

# CHAPTER 10

## Additional Installation Configurations for Cisco TelePresence Manager

---

First Published: September 27, 2010, OL-22226-01

### Contents

- [Post-Install Guidelines for CTS-Manager, page 10-2](#)
- [Introduction to the CTS-Manager Administration Software, page 10-3](#)
- [Licensing for CTS-Manager, page 10-6](#)
- [Security, page 10-12](#)
- [Digital Security Certificates, page 10-13](#)
  - [Generating Security Certificate Reports, page 10-13](#)
  - [Viewing Security Certificates, page 10-13](#)
  - [Deleting Security Certificates, page 10-13](#)
  - [Removing Security for Cisco TelePresence Manager, page 10-14](#)
  - [Uploading Security Certificates, page 10-14](#)
  - [Downloading LSCs, page 10-15](#)
- [LDAP Server, page 10-16](#)
- [Field Mappings, page 10-17](#)
- [Calendar Server, page 10-27](#)
- [Microsoft Exchange, page 10-31](#)
  - [Synchronization Operations, page 10-35](#)
- [IBM Domino, page 10-36](#)
- [System Settings, page 10-39](#)
- [Database - Status, Backup, and Restore, page 10-46](#)
  - [Settings, page 10-47](#)
  - [Changing the Backup Schedule, page 10-49](#)
  - [Backing Up CTS-Manager Data, page 10-50](#)

- Viewing Backup History, page 10-51
  - Restoring Backup Data, page 10-52
- Unified CM, page 10-53
- Bridges and Servers, page 10-57
  - Cisco TelePresence Multipoint Switch (CTMS), page 10-59
  - Cisco Unified Video Conferencing (CUVC), page 10-61
  - Cisco TelePresence Recording Server (CTRS), page 10-63
  - Cisco Multimedia Experience Engine (MXE), page 10-64
  - WebEx, page 10-65
- Access Management, page 10-68
- VC Rooms, page 10-72
- Live Desks, page 10-75
- Policies, page 10-78
- Application Settings, page 10-79
  - Meeting Notification Email, page 10-80
  - Studio Mode Recording, page 10-82
  - WebEx, page 10-83
  - Interoperability with Video Conferencing, page 10-83
  - Intercompany, page 10-84
  - Usage Survey, page 10-85
  - Start Meetings Early, page 10-93
  - Extend Meetings, page 10-93
- CTS-Manager Redundancy Failover Procedure, page 10-96

## Post-Install Guidelines for CTS-Manager

The purpose of this chapter is to outline the information you need to configure the system after installation.

The flow of tasks for additional configurations of CTS-Manager are provided in the following table.

**Table 10-1** *Post-Install Guidelines for Configuring CTS-Manager*

Setup Procedure Guidelines after Installing CTS-Manager	Description	Location
Additional Installation Procedures for CTS-Manager	The administrator makes use of the System Configuration window to perform system configuration tasks such as uploading licenses, synchronizing system databases, managing security, and reconfiguring system settings	Current chapter.

**Table 10-1** *Post-Install Guidelines for Configuring CTS-Manager (continued)*

<b>Setup Procedure Guidelines after Installing CTS-Manager</b>	<b>Description</b>	<b>Location</b>
Configuring Cisco TelePresence WebEx OneTouch for CTS-Manager	Describes how to set up Cisco TelePresence WebEx OneTouch in CTS-Manager, which allows WebEx participants to join TelePresence meetings.	<a href="#">Chapter 11, “Configuring Cisco TelePresence WebEx OneTouch for Cisco TelePresence Manager”</a>
Monitoring and Supporting CTS-Manager	Describes the support features available when you log into CTS-Manager using a Live Desk role.	<a href="#">Chapter 12, “Monitoring and Supporting Cisco TelePresence Manager”</a>
Email and Meeting Action Requirements	The Calendar service (either Microsoft Exchange or IBM Domino) sends an acceptance email to the meeting organizer, with the notice that the rooms have been reserved and placed on the calendar. CTS-Manager also sends either a Confirmation email or an Action Required email to the meeting organizer when a meeting is scheduled.	<a href="#">Chapter 13, “CTS-Manager Emails and Meeting Manager”</a>
Cisco WebEx OneTouch Configuration Guide for the Cisco TelePresence System	Describes the complete details on how to configure WebEx for the Cisco TelePresence System, including CTS-Manager.  CTS-Manager is used to configure and manage the Cisco WebEx bridging feature in Cisco TelePresence meetings.	Refer to the following URL: <a href="http://www.cisco.com/en/US/docs/telepresence/cts_admin/webex_solutions/guide/cts_webex_config.html">http://www.cisco.com/en/US/docs/telepresence/cts_admin/webex_solutions/guide/cts_webex_config.html</a>

If at any time you encounter problems, go to [Chapter 15, “Troubleshooting Cisco TelePresence Manager”](#) to see how to correct the problem.

## Introduction to the CTS-Manager Administration Software

CTS-Manager administration software is accessed through a web browser. All Cisco TelePresence administration software supports Microsoft Internet Explorer 6.x, 7.x, 8.x (Windows), Firefox 3.0 (Mac and Windows). CTS-Manager Administration software is accessed through the server’s hostname or IP address.

There are three levels of functionality when logging into CTS-Manager

- [Administrator Role, page 10-4](#)
- [SysAdmin Role, page 10-4](#)
- [Live Desk Role, page 10-4](#)

A meeting organizer who is not assigned to one of these roles only sees the details for meetings they have scheduled, and logs in through a special link in the confirmation email for their meetings.

## Administrator Role

When an administrator logs into the CTS-Manager, the following selections and information are available:

- System Status
- Monitor
- Support
- Configure
- Troubleshoot

The administrator performs the same tasks performed by a Live Desk, but has an additional system configuration task available. The administrator has a different login name and password from that of the Live Desk. The administrator's access privileges allow access to the internal workings of the system where the administrator can modify system settings such as passwords, IP addresses, and security settings. The administrator is also responsible for defining schedules to back up the database and for assigning a Live Desk to a meeting room.

In day-to-day operations, the administrator assists the Live Desk person with monitoring system status and, when problems occur, takes action to correct them by analyzing system error messages and debugging log files.

## SysAdmin Role

The SysAdmin has a special login account that allows access to two additional administrative tasks. These tasks are only visible by logging in using the SysAdmin password.

- System Settings
- Software Upgrade

This role is used mainly during installation of CTS-Manager. After installation, the administrator performs most administrative tasks.

## Live Desk Role

When a person designated as Live Desk logs into CTS-Manager, the following selections and information are available:

- System Status
- Monitor
- Support
- Troubleshoot

The Live Desk is the first person contacted when there are questions or problems pertaining to connecting meeting participants. Live Desks can be assigned rooms to monitor in the CTS-Manager application. Assigned Live Desks are easily reached by dialing the Help soft key on the Cisco IP phone in a Cisco TelePresence-enabled meeting room.

The administrator makes use of the Configure section to perform additional tasks such as:

- uploading licenses
- upgrading system software
- synchronizing system databases
- managing security
- reconfiguring system settings

Figure 10-1 shows the system configuration information displayed in the Troubleshoot > System Information window. The system configuration tasks in the Configure section are highlighted on the left.

**Figure 10-1** Troubleshoot > System Information Window

The screenshot shows the Cisco TelePresence Manager interface. The left sidebar contains a navigation menu with the following items: Monitor, Support, Configure, Access Management, Application Settings, Bridges and Servers, Database, LDAP Server, Licenses, Live Desks, Microsoft Exchange, Policies, Security, Software Upgrade, System Settings, Unified CM, and VC Rooms. The 'Configure' section is highlighted with a blue box, and an arrow points from this box to the 'System Configuration Tasks' label. Below the navigation menu, the 'System Status' section shows 'Today's Meetings' with counts for 'With Error', 'In Progress', and 'Scheduled', and 'Other Errors'.

The main content area is titled 'System Information' and contains two tables:

System Information							
SKU	Hostname	IP Address	MAC Address	License MAC Address	Hardware Model	Software Version	OS Version
CTS-MAN1.7	tsbu-docs-ctm	10.22.148.143	00:21:5e:c9:a6:3c	00215EC9A63C	784513	1.7.0.0 (620)	UCOS 4.0.0.0-31

Product Software Versions		
Product Name	Supported	Actual
Microsoft Exchange	[08.00.10685, 08.01.10240, 6.5.6944, 6.5.7226, 6.5.7638, 8.1.240.5, 8.2.176.2]	Unknown
Active Directory	[2003, 2008]	2008
Cisco Unified Communications Manager	[7.1.3 and later]	<a href="#">Actual Version</a>

© 2006-2010 Cisco Systems, Inc. All rights reserved.

# Licensing for CTS-Manager

CTS-Manager 1.7 and later has enforced licensing. Licensed features are enabled only when a valid license exists for the specific feature.

The primary licensed features in CTS-Manager include:

**Table 10-2 CTS-Manager Licensed Features**

Feature	License Type
Metrics Dashboard and Reporting API	Feature-based license
Scheduling API	Feature-based license
Room (required)	Count-based license
CTS Commercial Express	Both feature and device-based licenses



## Note

You are required to install the Room license. Without this license, your configured rooms will not be recognized by CTS-Manager and you will not be able to schedule meetings.

## Feature-Based Licenses

Optional feature-based licenses include:

**Table 10-1 Feature-Based Licenses**

License	Part Number
Metrics Dashboard and Reporting API	LIC-CTS-MAN-RPT
Scheduling API	LIC-CTS-MAN-API

The Metrics Dashboard license is enforced in the CTS-Manager Admin UI. If the license isn't uploaded to CTS-Manager, you can't enable and configure the usage survey and benefits report on the Configure > Application Settings > Usage Survey window.

For the Scheduling and Reporting APIs, the license is enforced at the API call. Whenever the administrator makes an API call, CTS-Manager returns the response if a valid license exists. If a license does not exist, a "License-not-found" error is returned.

The Scheduling API supports organizations that have other calendaring server types instead of MS Exchange or IBM Domino.

## Count-Based Licenses

Count-based licenses are based on the number of TelePresence and video conferencing (VC) devices (rooms with a TelePresence or VC system). Each TelePresence and VC device subscribes to a license. This count-based license is available in 3 license groups:

**Table 10-2 Count-Based Licenses**

License	Part Number
10 devices/rooms	LIC-CTS-MAN-10
50 devices/rooms	LIC-CTS-MAN-50
100 devices/rooms	LIC-CTS-MAN-100

Room licensing is common to Microsoft Exchange, IBM Domino, and the Scheduling API.

The Discover Rooms command in the Configure > Unified CM window checks and enforces the CTS room licensing. If there are more TelePresence rooms than available licenses, then the rooms above the designated license count will have no license to subscribe to. In this case, you must obtain more licenses in order for all rooms to subscribe. The syslogs and system error log tables provide warning notification when license count reaches a specific limit and when it is fully utilized. After loading additional licenses, it is not necessary to do Discover Rooms again.

## Getting Licenses for CTS-Manager

This section describes how the following customers get licenses:

- [New Customers, page 10-7](#)
- [Existing Customers Upgrading to CTS-Manager 1.7, page 10-8](#)

### New Customers

New customers purchasing CTS-Manager 1.7 or later, get licenses by doing the following:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Order CTS-Manager with server, choosing the number of rooms/devices for licensing plus optional reporting and/or scheduling API, as required. |
| <b>Step 2</b> | Receive CTS-Manager server. Included with the server is a Claim Certificate with a license Product Authorization Key (PAK).                   |
| <b>Step 3</b> | Install and initialize CTS-Manager.   |
| <b>Step 4</b> | Obtain the License MAC Address by logging in to CTS-Manager and going to the <b>Troubleshoot &gt; System Information</b> window.              |

**Note**

You can also obtain the License MAC Address by typing the **show status** command in the CTS-Manager command line interface (CLI). For information about how to access the CLI, refer to: [Starting a CLI Session, page 12-41](#).

- 
- |               |   |
|---------------|---|
| <b>Step 5</b> | Register the PAK with the License MAC Address at <a href="http://cisco.com/go/license">http://cisco.com/go/license</a> .  |
| <b>Step 6</b> | License file(s) arrive by email within one hour.  |
| <b>Step 7</b> | After installation of CTS-Manager, SysAdmin installs the license file(s). For more information, see <a href="#">Viewing and Uploading Licenses, page 10-8</a> . |

## Existing Customers Upgrading to CTS-Manager 1.7

Existing customers upgrading from CTS-Manager 1.5 or 1.6 to 1.7 or later, get licenses by doing the following:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Perform upgrade to CTS-Manager 1.7.   |
| <b>Step 2</b> | Log in to CTS-Manager<br>A message appears indicating that room licenses need to be installed.  |
| <b>Step 3</b> | Click <b>OK</b> in the message.<br>The Configure > Licenses > License Files window appears.   |
| <b>Step 4</b> | Click the <b>Get an Upgrade License</b> button and follow the instructions to get an upgrade license.<br>For more information, see <a href="#">Getting an Upgrade License, page 10-11</a> . |
| <b>Step 5</b> | License file arrives by email within one hour.  |
| <b>Step 6</b> | SysAdmin uploads the license file(s).<br>For more information, see <a href="#">Viewing and Uploading Licenses, page 10-8</a> .  |
- 

## Existing CTS-Manager 1.7 Customers Adding More Rooms or Licensed Features

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Order CTS-Manager rooms or feature licenses. Two options are available for ordering licenses: <ul style="list-style-type: none"><li>• LIC-CTS-MAN-xxx - paper-based license with normal lead times.</li><li>• L-LIC-CTS-MAN-xxx - eDelivery option where PAK is sent via email notification to eDelivery mailbox. Faster electronic delivery, shorter lead time. Log in to eDelivery to get your license: <a href="https://edelivery.cisco.com/esd/">https://edelivery.cisco.com/esd/</a>. For more information about eDelivery, refer to: <a href="http://www.cisco.com/web/partners/tools/edelivery.html">http://www.cisco.com/web/partners/tools/edelivery.html</a>.</li></ul> |
|---------------|---|

## Viewing and Uploading Licenses

The Configure > Licenses window in CTS-Manager allows you to view installed licenses and upload new licenses for different features.

The Licenses window has the following tabs:

- [Summary](#)—View existing licenses
- [License Files](#)—Upload new licenses

## Summary

The Configure > Licenses > Summary window lists both the feature-based and count-based licenses that are currently installed.

Licenses are generated by Cisco and shipped to the customer. There are two types of licenses:

- [Feature-Based Licenses](#)—Enable or disable a feature.

- **Count-Based Licenses**—Correspond to the number of CTS devices (rooms) used for TelePresence meetings, based on one license per room.

Licenses are tied to the MAC address of the CTS-Manager server. These licenses cannot be migrated to a new server. Therefore, when an existing CTS-Manager server is replaced with a new server, new licenses must be requested for the MAC address of the new server.

If a backup is restored onto another server, the server is not functional for the licensed feature until new licenses are uploaded. However, it is not necessary to migrate existing licenses from previous software.

The Syslogs and System error log tables provide warning notifications when the license count reaches specific limits and when it is completely used up.

If you are not able to set up TelePresence rooms, go to the Support > TelePresence Rooms window to make sure that a valid license is available for each room.

The name and the status of each license are displayed. A properly licensed feature will display a status of “LICENSE\_VALID.”

## Licensing Grace Period

A feature is in grace period when it was licensed at some point in the past, but a valid license is not currently available. You should upload a new license during this grace period. A feature remains in grace period for a maximum of 30 days, after which it becomes invalid and the feature’s functionality is disabled. Full functionality is restored after a valid license is uploaded.

**Figure 10-2** *Configure > Licenses > Summary Window*

Licenses

SummaryLicense Files

Feature-Based Licenses

Name	Status
LIC-CTS-MAN-RPT	LICENSE_VALID

Count-Based Licenses

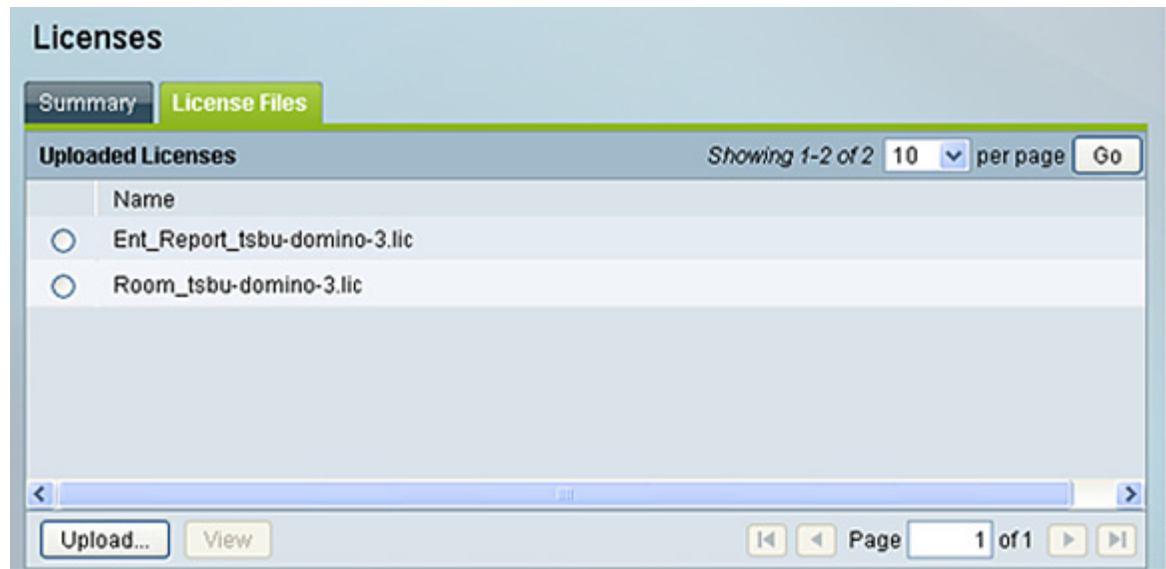
Name	Status	Total	Available
LIC-CTS-MAN-CTS	LICENSE_VALID	50	42

## License Files

The Configure > Licenses > License Files window lists which licenses are already loaded in the system and allows you to upload new licenses. CTS-Manager allows you to import FlexLM-based license files into the database and enforce licensing based on information stored in that database. Licenses can be imported any time after CTS-Manager is installed.

If you are upgrading to CTS-Manager 1.7 from a previous version, you must get an upgrade license to manage the rooms you currently have configured in CTS-Manager. For more information, see [Getting an Upgrade License](#).

**Figure 10-3** Configure > Licenses > License Files Window



## Uploading Licenses

To upload a license:

- 
- Step 1** Click **Upload**.
  - Step 2** In the License Upload window, click **Browse**, find the license you want to add and click **Open**.
  - Step 3** Click **Upload**.
  - Step 4** Click **Close** to close the License Upload window.
  - Step 5** To verify that your license has been uploaded properly, click the Summary tab.  
Your license should be listed with a status of "LICENSE\_VALID."
- 



### Note

License files sent from Cisco for install are text files. You can change the file name without using special characters or spaces. Do not change the contents of the file, otherwise the license install will fail.

## When You Need New Count-based (Room-based) Licenses

The following examples explain what happens when an administrator registers an 11th room with CTS-Manager which already has been set up with 10 rooms using a 10-room license group.

1. In a person-to-person meeting, the meeting organizer schedules a meeting between one room using the 10-room license group in CTS-Manager and the new 11th room. The 11th room is not recognized by CTS-Manager and the meeting organizer receives an “action required” email. In addition, the meeting appears in error on the phone UI of the licensed room, and no schedule appears on the phone in the 11th room.
2. In a multipoint meeting, the meeting organizer schedules a meeting between 3 rooms using the 10-room license group in CTS-Manager and the 11th room. The 11th room is not recognized by CTS-Manager and the meeting organizer receives a “confirmation” email for the three licensed rooms. The meeting appears in the schedule of the phone in all three licensed rooms, but not in the 11th room.

## CTS-Manager License Backup and Restore

License files are bundled as part of backup. The Restore process restores the backed-up license files. CTS-Manager validates licenses filed with the system Host ID during startup. The license file is removed if it does not match the Host ID of the system, and the corresponding feature is not enabled.

## Hardware Replacement and New Licensing

If it becomes necessary to replace CTS-Manager hardware, new licenses are requested for the new hardware as part of the RMA process. The administrator must run a fresh install and upload the new licenses in CTS-Manager.

Alternatively, the administrator can restore a previous backup on the new hardware from a remote location. During this process, CTS-Manager invalidates the licenses restored from the backup and the administrator must upload new licenses.

When you receive your new hardware, do a fresh install and upload the new licenses in the Configure > Licenses > License Files window, as detailed in [Uploading Licenses, page 10-10](#).

All licensed features will be non-functional until licenses are uploaded. During a Server replacement to re-host the licensing file, contact the Cisco licensing team ([licensing@cisco.com](mailto:licensing@cisco.com)) or the Cisco Technical Assistance Center (TAC).

## Getting an Upgrade License

CTS-Manager 1.7 and later requires a room license to manage the rooms configured. If you are upgrading from a previous version, the Get an Upgrade License button is displayed.

Follow the steps below to get a license for all rooms managed by CTS-Manager:

---

**Step 1** Click **Get an Upgrade License**.

The Get an Upgrade License window appears displaying the MAC Address and Upgrade Code for your CTS-Manager server.

**Step 2** Go to <http://cisco.com/go/license> and log in using your Cisco.com user account and password.

The Product License Registration page appears.

- Step 3** In the Migration License section at the bottom of the page, click **Register for Upgrade/Migrate License**.  
The Select Product page appears.
- Step 4** From the drop-down menu, select **Cisco TelePresence Manager** and click **Goto Upgrade/Migration License Portal**.  
The Upload Features page appears.
- Step 5** Copy and paste the MAC Address into the first field and the Upgrade Code into the next field and click the Agreement checkbox to accept the terms of the end-user license agreement.
- Step 6** Enter your contact information, making sure your email address is correct, and click **Continue**.
- Step 7** The license file will arrive via email in less than one hour.
- Step 8** Save the license file.



**Note** You can rename the file without special characters or spaces, but don't change the information in it.

- Step 9** In Cisco TelePresence Manager, go to the **Configure > Licenses** window, click the **License Files** tab and upload the license file. For more information, refer to [Uploading Licenses, page 10-10](#).



**Note** If you don't receive the license file after one hour or have problems uploading the license file, contact the Cisco Technical Assistance Center (TAC). If the number of room licenses you receive does not match the total licenses you purchased, email [licensing@cisco.com](mailto:licensing@cisco.com) with information about your license and your proof of purchase, including your Cisco sales order number or purchase order number.

## Security

The Security window assists with managing system security certificates and web services security.

**Figure 10-4** *Configure > Security Window*

**Security**

Web Services Security: ☐ Secure ☒ Unsecure

**Digital Security Certificates**

Category:  Unit:    
 Showing 1-3 of 3 10 per page

	Unit	Category	Certificate Name
<input type="radio"/>	CTM-trust	TRUST	example-1.com.pem
<input type="radio"/>	CTM-trust	TRUST	example-2.com.pem
<input type="radio"/>	tomcat	OWN	tomcat.pem

## Web Services Security

You can turn on web services security by choosing Secure mode. For more information refer to the Cisco TelePresence Security Solution documentation on Cisco.com, [http://www.cisco.com/en/US/docs/telepresence/security\\_solutions/security\\_solutions.html](http://www.cisco.com/en/US/docs/telepresence/security_solutions/security_solutions.html)

**Caution**

Cisco Unified CM and any CTMS registered with CTS-Manager must be configured and set to secure mode before downloading CAPF certs, LSCs, and setting CTS-Manager to secure mode. If secure mode is not established in this order, you may need to restart the CTI manager in Cisco Unified CM and restart CTS-Manager in order for secure mode to work properly.

## Digital Security Certificates

CTS-Manager supports the following security certificates:

- CTM-trust—CTS-Manager Security Keystore to store digital certificates for Microsoft Exchange or IBM Domino, Directory Server, and Cisco Unified CM.
- Tomcat—Security Keystore to store self-generated Apache Tomcat certificates.

**Note**

CTS-Manager does not support replacing the default Tomcat certificate with any other certificate.

## Generating Security Certificate Reports

You can generate a list of certificates containing a specific category and unit by supplying the following criteria:

- Choose All, Own, or Trust from the Category drop-down list.
- Choose All, CTM-trust, or Tomcat from the Unit menu.
- Click **Filter** to generate the list of certificates that match the search criteria.

## Viewing Security Certificates

To view the contents of a security certificate click the radio button next to the certificate unit name and click **View**.

The contents of the certificate can be copied and pasted in a text file.

## Deleting Security Certificates

To delete a CTM-trust type security certificate, click the radio button next to the certificate unit name and click **Delete**.

**Note**

CAPF-LSCs and CAPF-trust certificates and tomcat cannot be deleted. To remove them, set Web Security to “Unsecure.” Setting Web Security to unsecure triggers the deletion process.

## Removing Security for Cisco TelePresence Manager

To remove security for Cisco TelePresence Manager, complete the following steps:

- 
- Step 1** Remove the Cisco CTI Secure role from the Cisco TelePresence Manager application user by completing the following steps:
- Log in to the Cisco Unified CM Administration GUI.
  - Locate the existing Cisco TelePresence Manager application user by clicking the **Find** button.
  - Locate the user ID and click the hypertext link to select that user.
  - In the Roles pane, click the Standard CTI Secure Connection role to highlight it.
  - Click **Remove from User Group**.
- Step 2** Remove the security configuration from Cisco TelePresence Manager by performing the following actions:
- Log in to the Cisco TelePresence Manager Administration GUI.
  - Choose **Configure > Security**.
  - In the Web Security Settings area, click the **Unsecure** radio button.
  - Click **Apply**.

Cisco TelePresence Manager restarts and deletes the CAPF security certificates.

---

## Uploading Security Certificates

To display the Certificate Upload window, from which you can copy a security certificate to Cisco TelePresence Manager, click **Upload**.

**Caution**

You cannot upload a certificate that has the same name as an existing uploaded certificate. You must delete the existing certificate before uploading the new one. If a certificate has expired, you cannot upload it.

---

- 
- Step 1** In the Certificate Upload window, choose the category and unit for the certificate.
- Step 2** Click **Browse** to choose a location where a certificate file is located, and add it to the Certificate field.
- Step 3** Click **Upload** to copy the file.
- Step 4** Click **Close** to close the Certificate Upload window.
-

## Downloading LSCs

In this section, you download the CAPF Locally Significant Certificates (LSCs) from Cisco Unified CM to the Cisco TelePresence Manager.

You need the information that you created in previous steps in this section to download LSCs:

- CAPF Instance ID
- CAPF authentication string

In addition, you must have the following information:

- The TFTP server IP address
- The CAPF server IP address

To download LSCs, complete the following steps:

**Step 1** From the Cisco TelePresence Manager Administration GUI, choose **Configure > Security**.

**Step 2** Click the **Secure** radio button on the top of the screen and click the **Apply** button.

**Step 3** Click the **Download LSC** button.

The Download CAPF LSC window appears.

**Figure 10-5** Certificate Management Download CAPF LSC Window

### Download CAPF LSC

Unified CM:	example-ccm1	▼
CAPF Instance ID:	<input type="text"/>	
CAPF Auth. String:	<input type="text"/>	
TFTP Server Host:	<input type="text"/>	
TFTP Server Port:	69	
CAPF Server Host:	<input type="text"/>	
CAPF Server Port:	3804	
Certificate Install Directory:	/usr/local/ctis/.security/certs/capf-lsc/	
<input type="button" value="Download LSC"/> <input type="button" value="Close"/>		

**Step 4** Enter the following information in the fields that are displayed:

- CAPF Instance ID: Enter the ID that you obtained in the “Configuring Cisco Unified CM for Cisco TelePresence Manager Secure Communications” document.
- CAPF Auth. String: Enter the string that you obtained in the “Configuring Cisco Unified CM for Cisco TelePresence Manager Secure Communications” document
- TFTP Server Host: Enter the IP address of the TFTP server.



**Note**

If your Cisco Unified CM server is configured as the TFTP server, use the IP address of the Cisco Unified CM that is configured as the publisher.

- CAPF Server Port: Leave the default value
- CAPF Server Host: Enter the IP address of the CAPF server



**Note**

If you use your Cisco Unified CM publisher as the TFTP server, Cisco TelePresence Manager automatically enters the IP address of the publisher Cisco Unified CM in this field.

**Step 5** Click **Download LSC**.

**Step 6** Click **OK** to confirm your choice.

Cisco TelePresence Manager creates the LSCs and restarts the system. The Digital Security Certificate window displays the LSC certificates that Cisco TelePresence Manager created:

- CTSTMan.pem
- CAPF.pem

## LDAP Server

CTS-Manager uses Lightweight Directory Access Protocol (LDAP) to retrieve information related to users and conference rooms from Directory Server deployments. Enterprises typically use specialized databases called *directories* to store information related to users, meeting rooms, and so on. LDAP is a protocol for accessing directories.



**Note**

CTS-Manager only supports English language-based Active Directory installations.

The initial LDAP Server window gives details on the CTS-Manager LDAP system.

**Figure 10-6** *Configure > LDAP Server*

Hostname	User Name	Default context
example-ad01 (Default)	cn=administrator,cn=users,DC=uctm,DC=com	DC=uctm,DC=com

From this window, multiple new LDAP servers can be configured or existing ones can be edited and updated.

This window specifies LDAP Directory Server server settings that are used by CTS-Manager to access the directory information. Open the LDAP Server window to see the status of the server. This window also allows new settings or editing the settings and field mappings.

## Settings for LDAP

To add an LDAP server, click **New** and enter the appropriate information in the LDAP Servers window.

To edit an existing LDAP, click **Edit** and make the appropriate changes in the Edit LDAP Servers window.



### Note

For Firefox browser users: When clicking the certificate field in either the LDAP Servers or Edit LDAP Servers window, a file upload window opens for you to select the certificate to upload. This is the same window that appears when clicking the **Browse** button. You cannot type a path in the certificate field using Firefox.

## Multiple LDAP Peer Domains

If you have a LDAP peer domain configured you'll need to specify the additional user containers and context. You can do this with one of the User Container fields.

For example, `cn=users,dc=domain2,dc=com`

When specifying the container and context information for your peer domain, DO NOT check the Append default context box.

- 
- Step 1** To test the connection between this system and the LDAP server, click **Test Connection**.
  - Step 2** To register new or modified settings, click **Apply**.
  - Step 3** To restore the original settings, click **Reset**
- 



### Note

LDAP containers configured for use with CTS-Manager should not be specified in such a way where one container is the child of the other. This requirement includes specifying the default context.

[Table 10-3](#) describes the settings for the LDAP Server window.

## Field Mappings

The CTS-Manager server uses application objects and attributes that are internally mapped to the objects and attributes in the LDAP Directory Server. Most of these mappings are predefined and fixed. However, some of the information required for the Cisco TelePresence system may be stored in different attributes of the LDAP Directory Server, based on the enterprise deployment. The Field Mapping window provides a mechanism to map such objects and attributes used by the CTS-Manager server to the object and attributes defined in the LDAP Directory Server schema.

## Microsoft Exchange Deployments

The attributes are used by the Exchange server to store the user's e-mail and display name information. For most of the Exchange deployments, this information should not be changed. It is very unlikely that these mappings need to be changed. In case there is a requirement to authenticate users using a different attribute, please contact Cisco Support before changing these values.

CTS-Manager supports connection to multiple LDAP domains/servers that belong to a single Active Directory forest. Some of the setups with which CTS-Manager can work are peer-peer LDAP domain setup, and Parent-Child LDAP domain setup.

**Caution**

---

The object and attribute mappings for Exchange/Directory Server deployments are listed in [Table 10-5](#) and cannot be changed after installing and configuring Cisco TelePresence Manager. Cisco TelePresence Manager may not function properly if the Object Class fields are changed.

---

**Figure 10-7** New LDAP Window Mappings

### LDAP Servers

= Required fields

Host:

Bind Method: ☐ Secure ☒ Normal

Port:

Default Context:

Username:  ☐ Append default context

Password:

Certificate:

User Containers:  ☐ Append default context

☐ Append default context

☐ Append default context

☐ Append default context

☐ Append default context

---

### Person

	Object Class	Attribute	
Country:	<input type="text" value="Person"/>	<input type="text" value="c"/>	
EmailID:	<input type="text" value="Person"/>	<input type="text" value="mail"/>	
DeptID:	<input type="text" value="Person"/>	<input type="text" value="department"/>	
SchedulerName:	<input type="text" value="Person"/>	<input type="text" value="cn"/>	
DisplayName:	<input type="text" value="Person"/>	<input type="text" value="displayname"/>	
Title:	<input type="text" value="Person"/>	<input type="text" value="title"/>	
Location:	<input type="text" value="Person"/>	<input type="text" value="location"/>	
Email Address:	<input type="text"/>	<input type="button" value="View Sample Data"/>	

Table 10-3 lists the fields in the LDAP Server - New window. See Table 10-5 for the Person field information.

CTS-Manager requires the Active Directory domain level to be set to at least level 2. If the domain controller is null due to some configuration issue on the Active Directory server, CTS-Manager will not work.

**Table 10-3**      **New LDAP Server Settings**

Field or Button	Description or Settings
Host	LDAP server host name.
Bind Method	Click the <b>Secure</b> or <b>Normal</b> radio button to select the binding method: <ul style="list-style-type: none"> <li>Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server.</li> <li>Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP.</li> </ul>
Port	The default port for secure connection is 636. The default port for normal connection in a single LDAP server deployment is 389. In cases where deployments consist of multiple LDAP Directory Servers, this port should be configured with 3268, which is the Global Catalog port. Secure Global Catalog port is 3269.
Default Context	The default context from which the LDAP queries are performed. To change the context string: <ul style="list-style-type: none"> <li>Click the Fetch button and choose the context from the Fetch DNS drop-down list adjacent to this field.</li> </ul>
Username	The username used to authenticate to the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: cn=adminstrator,cn=users,dc=<mydomain>,dc=com) <b>Note</b> “cn=CTSMAN User” is another example. Note that the CTS-Manager Active Directory configuration requires using users that have Domain Admin privilege. The user, “CTSMAN User” only needs to be created with the Domain Users privilege.
Password	Password to access the LDAP server.
Certificate	The name of the LDAP certificate. This is only needed if you have chosen the Secure Bind Method. To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer, then click Browse to select it and upload it to CTS-Manager.

**Table 10-3**      *New LDAP Server Settings (continued)*

Field or Button	Description or Settings
User containers	<p>The containers from which queries are performed to retrieve user objects. More than one user container or user object can be specified. The Cisco Telepresence server uses the values entered to search through the containers in sequence to retrieve user and meeting room information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication.</p> <ul style="list-style-type: none"> <li>To append the default context, check the Append default context box next to the user container field.</li> </ul> <p><b>Note</b> If you have a LDAP peer domain configured you'll need to specify any user containers and context. For example, <code>"cn=users,dc=domain2,dc=com"</code>. When specifying the container and context information for your peer domain, DO NOT check the Append default context box.</p>
Test Connection	This allows you to test the connection configuration between this system and the LDAP server.

## Edit

To edit the LDAP mapping, click the radio button to select the LDAP server that you want to edit. Then click the **Edit** button. The LDAP Edit window appears. [Table 10-4](#) lists the field information. See [Table 10-5](#) for the Person field information.

Figure 10-8 Edit LDAP Window

**Edit... LDAP Servers**

**= Required fields**

Host:

Bind Method: ☒ Secure ☐ Normal

Port:

Default Context:

Username:  ☐ Append default context

Password:

Certificate:

User Containers:

<input type="text" value="o=TRQA"/>	<input type="checkbox"/> Append default context
<input type="text" value="o=newORG"/>	<input type="checkbox"/> Append default context
<input type="text"/>	<input type="checkbox"/> Append default context
<input type="text"/>	<input type="checkbox"/> Append default context
<input type="text"/>	<input type="checkbox"/> Append default context

---

**Person**

	Object Class	Attribute
Country:	<input type="text" value="Person"/>	<input type="text" value="c"/>
EmailID:	<input type="text" value="Person"/>	<input type="text" value="mail"/>
DeptID:	<input type="text" value="Person"/>	<input type="text" value="department"/>
SchedulerName:	<input type="text" value="Person"/>	<input type="text" value="cn"/>
DisplayName:	<input type="text" value="Person"/>	<input type="text" value="displayname"/>
Title:	<input type="text" value="Person"/>	<input type="text" value="title"/>
Location:	<input type="text" value="Person"/>	<input type="text" value="location"/>

Email Address:

Table 10-4 Edit LDAP Server Settings

Field or Button	Description or Settings
Host	LDAP server host name.
Bind Method	<p>Click the <b>Secure</b> or <b>Normal</b> radio button to select the binding method:</p> <ul style="list-style-type: none"> <li>Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server.</li> <li>Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP or DIIOP.</li> </ul>

**Table 10-4** *Edit LDAP Server Settings (continued)*

Field or Button	Description or Settings
Port	<p>The default port for secure connection is 636.</p> <p>The default port for normal connection in a single LDAP server deployment is 389.</p> <p>In cases where deployments consist of multiple LDAP Directory Servers, this port should be configured with 3268, which is the Global Catalog port.</p> <p>Secure Global Catalog port is 3269.</p>
Default Context	<p>The default context from which the LDAP queries are performed.</p> <p>To change the context string:</p> <ul style="list-style-type: none"> <li>Click the Fetch DNS button and choose the context from the Fetch DNS drop-down list adjacent to this field.</li> </ul>
Username	<p>The username used to authenticate to the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: cn=administrator,cn=users,dc=&lt;mydomain&gt;,dc=com)</p>
Password	<p>Password to access the LDAP server.</p>
Certificate	<p>The name of the LDAP certificate. This is only needed if you have chosen the Secure Bind Method.</p> <p>To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer. Then click Browse to select it and upload it to CTS-Manager.</p>
User containers	<p>The containers from which queries are performed to retrieve user objects. More than one user container or user object can be specified. The Cisco Telepresence server uses the values entered to search through the containers in sequence to retrieve user and meeting room information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication.</p> <ul style="list-style-type: none"> <li>To append the default context, check the Append default context box next to the user container field.</li> </ul> <p><b>Note</b> If you have a LDAP peer domain configured you'll need to specify any user containers and context. For example, "cn=users,dc=domain2,dc=com". When specifying the container and context information for your peer domain, DO NOT check the Append default context box.</p>

## Verifying Field Mapping Data

Verify that the data retrieved is as you expected. If data is incorrect, the application will not operate correctly.

Click **View Sample Data** to retrieve objects based on the mappings specified.

**Caution**

Setting the LDAP objects and attributes used by the Exchange server requires experience using Directory Server and Exchange software. **Do not change the *mail* value in the LDAP SchedulerName Attribute field.**

The majority of deployments do not require any changes to these attributes. Incorrectly changing these fields will result in Cisco TelePresence Manager not being able to function.

Consult the Cisco TelePresence Manager support team and the LDAP and Exchange server administrator for your deployment before changing the default mappings in these screens.

Table 10-5 describes the settings for the Person fields in both the New and Edit windows.

**Table 10-5** LDAP Person - Objects and Attributes

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
<b>Person</b>			
	SchedulerName:	Person	cn <b>Note</b> Do not change this value. If this value is changed incorrectly, meetings will not have the correct information.
	EmailID:	Person	mail
	DisplayName:	Person	displayname
<b>Note</b> The Object Class mappings need not be changed and are displayed ready only. Only the attribute mappings need to be changed if required.			

## IBM Domino Deployments

These attributes are used by the Domino LDAP server to retrieve the user's e-mail and display name information. For most of the Domino deployments, this information should not be changed.

CTS-Manager supports a Domino deployment with a single domain. CTS-Manager can be configured against one Domino server only. In a cluster environment, all resource reservation databases that contain a Cisco TelePresence room's reservations must be replicated to the Domino server that CTS-Manager is configured against. Users in Directory Assistance database configured with external LDAP servers are not supported.

View the data on a new or changed set up and then click the Apply to save the configuration.

**Note**

The object and attribute mappings for Domino/Directory Server deployments are listed in Table 10-7 and cannot be changed after installing and configuring CTS-Manager.

**Note**

Any ports that communicate with CTS-Manager can be verified by using Telnet.

Table 10-6 lists the information for the fields in the IBM LDAP Edit or New window.

**Table 10-6 IBM LDAP Server Settings**

Field or Button	Description or Settings
Host	LDAP server host name.
Bind Method	Click the <b>Secure</b> or <b>Normal</b> radio button to select the binding method: <ul style="list-style-type: none"> <li>Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server.</li> <li>Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP or DIIOP.</li> </ul>
Port	The default port for secure connection is 636. The default port for normal connection in a single LDAP server deployment is 389. In cases where deployments consist of multiple LDAP Directory Servers, this port should be configured with 3268, which is the Global Catalog port. Secure Global Catalog port is 3269.
Default Context	The default context from which the LDAP queries are performed. To change the context string: <ul style="list-style-type: none"> <li>Click the Fetch DN's button and choose the context from the Fetch DN's drop-down list adjacent to this field.</li> </ul>
Username	The username used to authenticate to the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: cn=administrator,cn=users,dc=<mydomain>,dc=com)
Password	Password to access the LDAP server.
Certificate	The name of the LDAP certificate. This is only needed if you have chosen the Secure Bind Method. To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer. Then click Browse to select it and upload it to CTS-Manager.

**Table 10-6 IBM LDAP Server Settings (continued)**

Field or Button	Description or Settings
User containers	<p>The containers from which queries are performed to retrieve user objects. More than one user container or user object can be specified. The Cisco Telepresence server uses the values entered to search through the containers in sequence to retrieve user and meeting room information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication.</p> <ul style="list-style-type: none"> <li>To append the default context, check the Append default context box next to the user container field.</li> </ul> <p><b>Note</b> If you have a LDAP peer domain configured you'll need to specify any user containers and context. For example, "<i>cn=users,dc=domain2,dc=com</i>". When specifying the container and context information for your peer domain, DO NOT check the Append default context box.</p>
Test Connection	Allows you to test the configuration connection

Table 10-7 describes the settings for the Person fields in both the New and Edit windows.

**Table 10-7 LDAP Person - Objects and Attributes**

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
<b>Person</b>			
	SchedulerName	Person	cn <b>Note</b> Do not change this value. If this value is changed incorrectly, meetings will not have the correct information.
	EmailID	Person	mail
	DisplayName	Person	cn

**Note** The Object Class mappings need not be changed and are displayed ready only. Only the attribute mappings need to be changed if required.

## Verifying Field Mapping Data

Verify that the data retrieved is as you expected. If data is incorrect, the application will not operate correctly.

Click **View Sample Data** to retrieve objects based on the mappings specified.

**Caution**

The Setting of the LDAP objects and attributes used by the Domino server requires experience using Directory Server and Domino software. Do not change the *mail* and *cn* values in the LDAP SchedulerName Attribute field.

The majority of deployments do not require any changes to these attributes. Incorrectly changing these fields will result in Cisco TelePresence Manager not being able to function.

Consult the Cisco TelePresence Manager support team and the LDAP and Domino server administrator for your deployment before changing the default mappings in these screens.

## Deleting Server

Before performing a delete on a DNS server, it is important to first change existing servers like Unified CM and other bridges or servers to IP from hostname before the DNS server is deleted. If the hostname is not changed first, the Unified CM and bridges or servers will be put in error status.

## Calendar Server

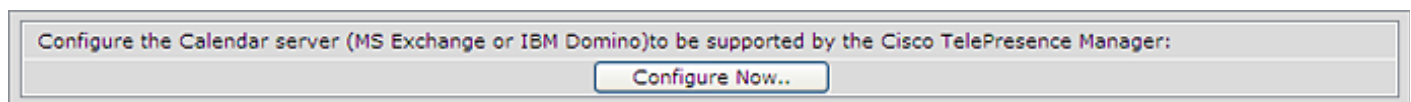
If you did not specify a Calendar server (either Microsoft Exchange or IBM Domino) during the initial installation, the Calendar Server window displays the Calendar Server wizard.

The Calendar Server wizard leads you through a four-step process to register a Calendar server with CTS-Manager.

**Note**

The LDAP server you specified during initial installation determines if you will be able to sync any Cisco TelePresence endpoints with the Calendar server you are registering. The LDAP server you are using must match the Calendar server you are registering.

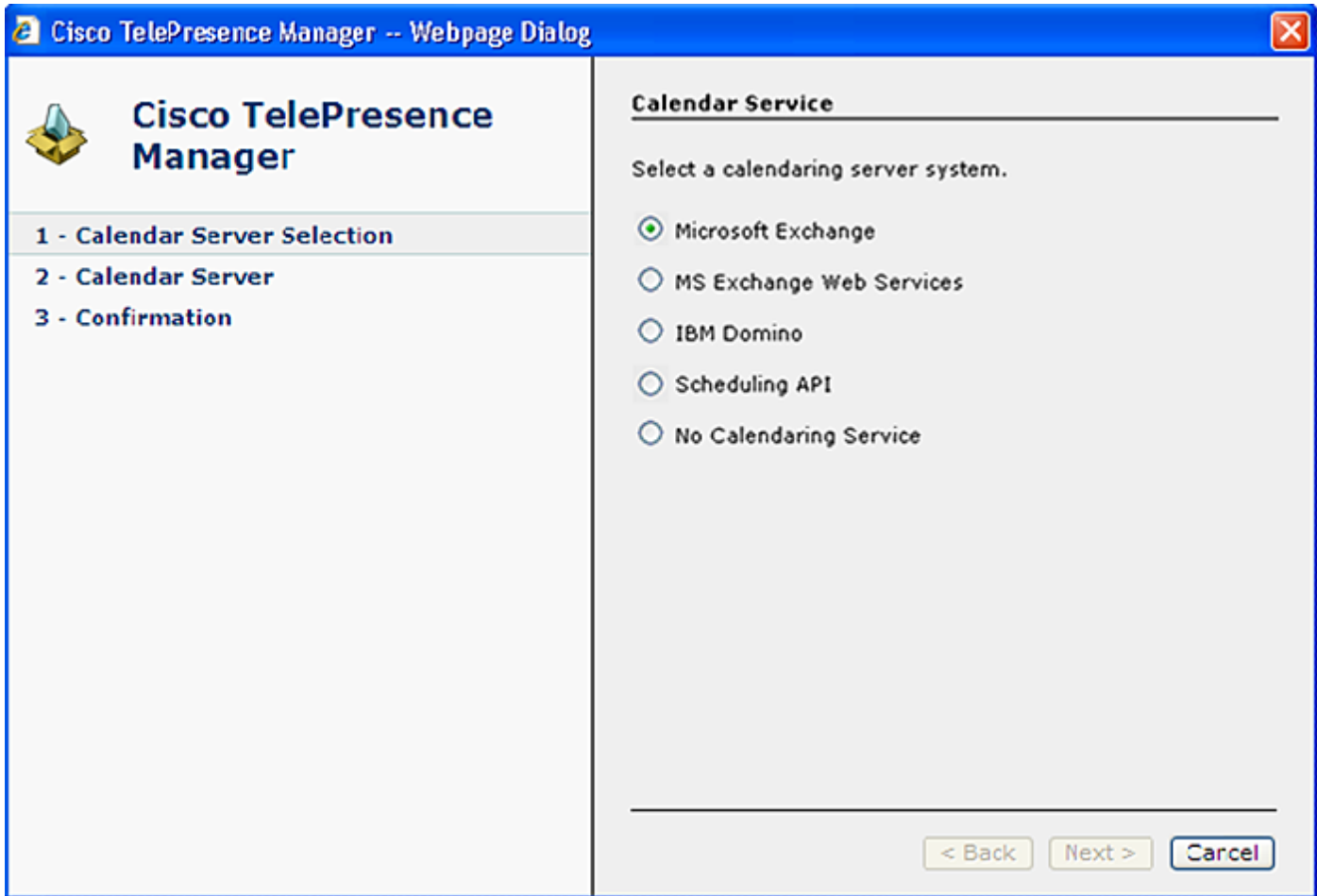
**Figure 10-9**      **Configure Calendar Server**



To configure the calendar server:

- Step 1**      The first step in registering a Calendar server with CTS-Manager is to choose either IBM Domino or Microsoft Exchange.

Figure 10-10 Cisco TelePresence Manager - Calendar Server Selection Screen



The screenshot shows a web-based configuration window titled "Cisco TelePresence Manager -- Webpage Dialog". On the left is a sidebar with the Cisco TelePresence Manager logo and a navigation menu with three items: "1 - Calendar Server Selection" (highlighted), "2 - Calendar Server", and "3 - Confirmation". The main content area is titled "Calendar Service" and contains the instruction "Select a calendaring server system." Below this are five radio button options: "Microsoft Exchange" (selected), "MS Exchange Web Services", "IBM Domino", "Scheduling API", and "No Calendaring Service". At the bottom right of the main area are three buttons: "< Back", "Next >", and "Cancel".

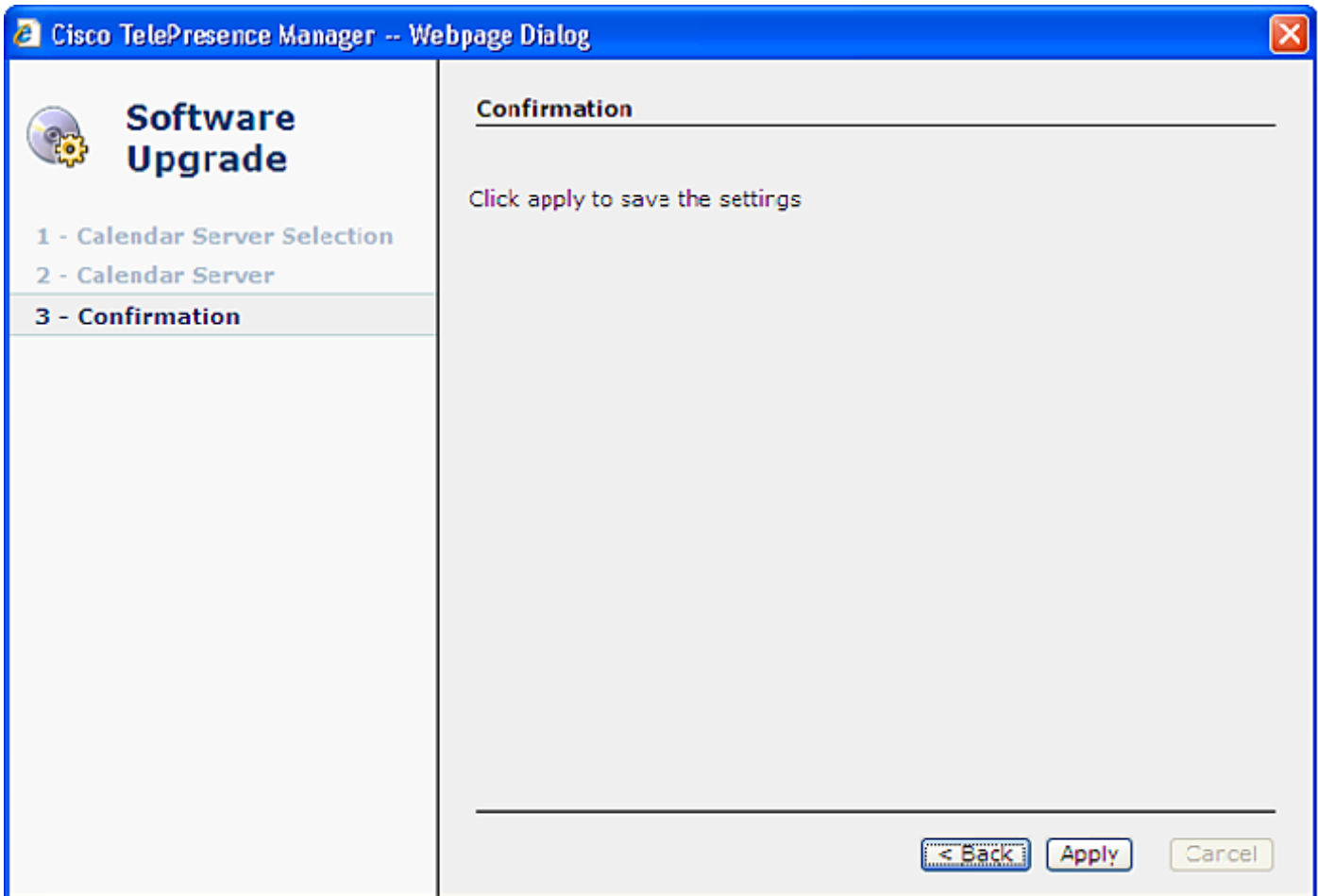
**Step 2** In the next step you need to specify the service logon information. The example below displays the information needed to use the Microsoft Exchange service.

Figure 10-11 Cisco TelePresence Manager - Calendar Server Microsoft Exchange Screen

The screenshot shows a web-based configuration window titled "Cisco TelePresence Manager -- Webpage Dialog". On the left is a sidebar with the Cisco TelePresence Manager logo and a navigation menu with three items: "1 - Calendar Server Selection", "2 - Calendar Server", and "3 - Confirmation". The main area is titled "Microsoft Exchange" and contains the following text: "Enter Microsoft Exchange resource properties. Connection to the Microsoft Exchange server must be tested and verified before you can advance to the next step." Below this text are several input fields: "Host:" (empty), "Bind Method:" (with radio buttons for "Secure" and "Normal", where "Normal" is selected), "Port:" (containing "80"), "Domain Name:" (empty), "Logon Name:" (empty), "SMTP LHS:" (empty), "Password:" (empty), and "Certificate:" (empty) with a "Browse..." button next to it. A "Test Connection" button is located below these fields. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

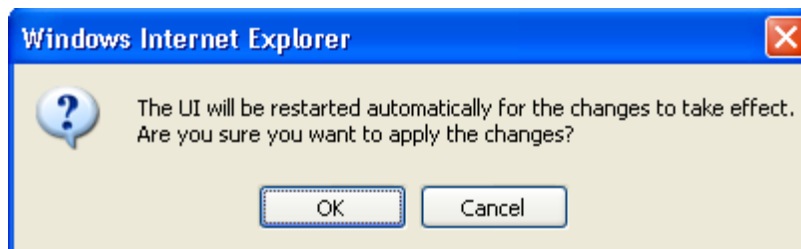
**Step 3** Click **Apply** to save the new Calendar server settings.

Figure 10-12 Cisco TelePresence Manager - Calendar Confirmation Screen

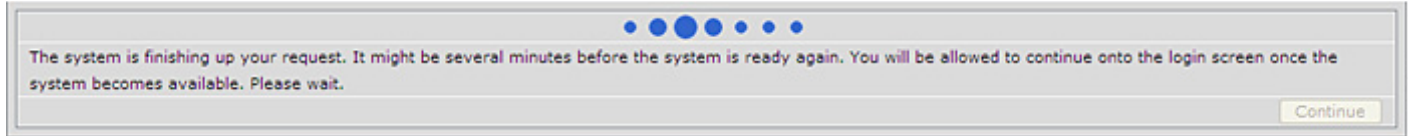


**Step 4** Then click **OK** to restart the CTS-Manager server.

Figure 10-13 Apply Changes Screen



**Step 5** Once the server has restarted, click **Continue** to go to the CTS-Manager login screen and log in.

**Figure 10-14** System Restart Notification Screen**Caution**

If the calendar service you are registering with does not match the LDAP server you specified during initial installation, the wizard will display all the Cisco TelePresence endpoints that will not sync with the new calendar service. You can proceed with the calendar service you have chosen, but meeting organizers will not be able to use the endpoints to schedule meetings.

## Microsoft Exchange

The Microsoft Exchange window helps you manage the database that stores meeting information.

To test the connection between CTS-Manager and the Microsoft Exchange server as shown in [Figure 10-15](#):

- 
- Step 1** Click **Test Connection**.
- Step 2** To register new or modified settings, click **Apply**.
- Step 3** To restore the original settings, click **Reset**.
- 

**Note**

If the Test Connection fails and a “Connection refused” message is displayed, the IIS server that hosts the WebDAV access is down. To fix this problem, restart the IIS server. In a scenario where there is a load balancer on the front end server, check the status of the IIS server on each server to which CTS-Manager can be load balanced.

**Figure 10-15** *Configure > Microsoft Exchange Window*

**Microsoft Exchange**

Service Status: **OK**

✱ = Required fields

Mailbox Usage: 0.17% full (3497.0 of 2097151.0 KB is used)

✱ Host:

Bind Method: ☐ Secure ☒ Normal

✱ Port:

✱ Domain Name:

Logon Name:

✱ SMTP LHS:

✱ Password:

Certificate:

---

**Synchronization Operations**

Subscription Status:  Room Name:

Showing 1-7 of 7 10 per page

<input type="checkbox"/>	Room Name ▾	Last Synchronization Time (*)	Subscription Status	Assigned Node
<input type="checkbox"/>	ROOM2	✓ 05/28/2010 12:03 PM	Success	sbu-bw-30
<input type="checkbox"/>		✗ Never synchronized	Error	sbu-bw-30
<input type="checkbox"/>	ROOM4	✓ 05/28/2010 12:03 PM	Success	sbu-bw-30
<input type="checkbox"/>	ROOM6	✓ 05/28/2010 12:03 PM	Success	sbu-bw-30
<input type="checkbox"/>	ROOM5	✓ 05/28/2010 12:03 PM	Success	sbu-bw-30
<input type="checkbox"/>	ROOM3	✓ 05/28/2010 12:03 PM	Success	sbu-bw-30
<input type="checkbox"/>	ROOM1	✓ 05/28/2010 12:03 PM	Success	sbu-bw-30

Page 1 of 1




(\*) All times are shown in time zone America/Los\_Angeles (GMT -7.0)

Table 10-8 describes the information and operations accessible from this window.

**Table 10-8** *Microsoft Exchange Server*

Field	Description or Settings
Service status	Display-only status report of system service.
Mailbox Usage	Meeting information is mailed to users. This display-only field reports the amount of storage space taken up by the e-mails as a percentage of total space available.
Host	Hostname provided for the Microsoft Exchange server account, which can be modified.
Bind Method	Choose the <b>Secure</b> or <b>Normal</b> radio button to select the binding method, as follows: <ul style="list-style-type: none"> <li>Secure—CTS-Manager communicates with the Microsoft Exchange server in secure mode using HTTPS. This method requires enabling Secure Socket Layer (SSL) on the Microsoft Exchange server.</li> <li>Normal—CTS-Manager communicates with the Microsoft Exchange server in cleartext using HTTP.</li> </ul>
Port	Communication port number.

**Table 10-8** Microsoft Exchange Server (continued)

Field	Description or Settings
Domain Name	<p>Domain name provided for the Microsoft Exchange server account, which can be changed.</p> <p> <b>Note</b> This is the email domain name.</p>
Logon Name	<p>This is the account name used to log on to the Microsoft Exchange server. The value is dependent on the AD/Exchange configuration. For example, it is either <i>ctsappaccount@mycompany.com</i> or <i>ctsappaccount</i>.</p>
SMTP LHS	<p>This is the left hand side (LHS) of the SMTP address for the account specified by the Logon Name. If the full SMTP address is <i>ctsappsmtplib@mycompany.com</i> enter <i>ctsappsmtplib</i> in this field.</p>
Password	<p>Password used to access the Microsoft Exchange server account, which can be changed.</p>
Certificate	<p>Use the field to provide a trust certificate for new Microsoft Exchange server.</p>
Configure EWS	<p>Use this button to bring up the Exchange Web Services window. Exchange needs to be configured for EWS when upgrading to Exchange 2007.</p> <p> <b>Note</b> EWS Authentication - must use the NTLMv1 authentication for releases 1.6.2 and earlier. The Axis2 Library supports NTLMv2 for releases 1.6.3 and later. NTLMv2 session is supported in 1.7.2 and later.</p> <p> <b>Note</b> For WebDav it was required to disable FBA. For EWS, FBA needs to be enabled.</p>

CTS-Manager and Microsoft Exchange server automatically renew subscriptions every 40 minutes. If there are any changes for room status in Exchange, CTS-Manager will not be notified of the change until that 40 minute update time. The exception is if CTS-Manager is forced to sync with the Exchange server by either doing a reboot or a restart.

Figure 10-16 Configure EWS Window

**Cisco TelePresence Manager**

1 - ExchangeWebServices  
2 - Confirmation

### MS Exchange Web Services

Enter configurations for the Microsoft Exchange Web Services.

Host:  \*

Bind Method: ☐ Secure ☒ Normal

Port:  \*

Domain Name:  \*

Username:  \*

Password:  \*

Certificate:  Browse... \*

**Test Connection**

- Host: the Microsoft Exchange Web Services server host name or IP address.
- Username/Password: Left hand side of the email address of the user account that has read access to the Exchange web services server. Password necessary for authentication.

\* Required Fields

< Back   Next >   Cancel

Table 10-9 Microsoft Exchange Web Services Fields

Field Name	Field Value
Host	The hostname or IP address of the Exchange server.
Bind Method	If you set this to secure you'll need to provide a security certificate.
Port	In Normal bind mode the port setting is 80. In Secure bind mode the port setting default is 443.
Domain Name	Enter the domain for the logon name.

**Table 10-9**      *Microsoft Exchange Web Services Fields*

Field Name	Field Value
Username	Enter the username for the Exchange EWS server.  <b>Note</b> If you are using Windows authentication, the format is: <b>domain\username</b> . If you are using basic authentication, the format is: <b>username@ldapdomainname.com</b>
Password	Enter the password for the CTS-Manager test account or Exchange administrative account, using English characters only.
Certificate	The full pathname to the Exchange security certificate. This is needed only if you are using the Secure Bind Mode.

## Synchronization Operations

The Synchronization Operations area tells you when information in the Microsoft Exchange server database was last updated with meetings scheduled for a particular room.

You can filter the list by selecting using the Subscription Status drop-down menu, entering a room name (optional) and clicking Filter.

When mismatched information in the databases causes meeting conflicts or there are other problems that prevent a meeting from being launched successfully, this area of the Microsoft Exchange window allows you to synchronize information between Microsoft Exchange and the CTS-Manager database. Synchronization takes time and system resources to accomplish and should be done only when necessary.

To synchronize information between Microsoft Exchange and the CTS-Manager database:

- 
- Step 1**    Check the boxes next to the rooms to select them. To synchronize information for all meeting rooms, check the box next to **Room Name** in the display header.
  - Step 2**    Click **Resync** to start the operation.  
  
Once you've begun the synchronization operation the Service Status field displays a **Sync progress** indicator showing the progress of the synchronization operation by percentage.
  - Step 3**    Once the synchronization operation completes, click **Refresh** to update the display.
- 

[Table 10-10](#) describes the information displayed in this area of the Microsoft Exchange window.



### Note

A maximum of 100 rooms are displayed per page. If you have more than 100 rooms registered with Cisco TelePresence Manager, you can click the Next button to display the additional rooms.

**Table 10-10**     *Microsoft Exchange Server Synchronization Report*

Field	Description
Room Name	Name of the meeting room. Click the arrow in the header of the Room Name column to sort the list in ascending or descending alphabetical order.
Last Synchronization Time	Time the synchronization operation was started.
Subscription Status	Status of the synchronization operation. Click the arrow in the header of the Room Name column to sort the list in ascending or descending alphabetical order.

## IBM Domino

The IBM Domino window helps you manage the database that stores TelePresence meeting information. To test the connection between this system and the Domino server, as shown in [Figure 10-17](#)

- 
- Step 1**     Click **Test Connection**.
- Step 2**     To register new or modified settings, click **Apply**.
- Step 3**     To restore the original settings, click **Reset**.
- 



### Note

Any ports to communicate with CTS-Manager can be verified by using Telnet.

---

**Figure 10-17** Configure > IBM Domino Window

**IBM Domino**

Service Status: **OK**

= Required fields

Mailbox Usage: Unable to obtain necessary information

Host:

Bind Method: ☒ Secure ☐ Normal

Port:

Organization Name:

Username:

Password:

Polling Interval (minutes):  \*

Certificate:

**Synchronization Operations**

Subscription Status:  Room Name:

Showing 1-1 of 1 10 per page

<input type="checkbox"/>	<a href="#">IBM Domino Databases</a>	Last Synchronization Time (+)	Resynchronization Status	Associated Rooms
<input type="checkbox"/>	yanas.nsf	✓ 05/28/2010 04:43 PM	Success	room1/newsite2 room2/newsite2 room6/newsite2 room8/newsite2

(+) All times are shown in time zone America/Los\_Angeles (GMT -7.0)

Table 10-11 describes the information and operations accessible from this window.


**Note**

The following parameters should already be known by your Domino administrator. Make sure the Domino Server configuration in CTS-Manager matches the configuration of your Domino Server.

**Table 10-11** IBM Domino Server

Field or Button	Description or Settings
Service status	Display-only status report of system service.
Mailbox Usage	Meeting information is mailed to users. This display-only field reports the amount of storage space taken up by the emails as a percentage of total space available.
Host	Hostname provided for the Domino server account, which can be modified.

Table 10-11 IBM Domino Server (continued)

Field or Button	Description or Settings
Bind Method	Choose the Secure or Normal radio button to select the binding method, as follows: <ul style="list-style-type: none"> <li>Secure—CTS-Manager communicates with the Domino server in secure mode using HTTP or DIIOP. This method requires enabling Secure Socket Layer (SSL) on the Domino server.</li> <li>Normal—CTS-Manager communicates with the Domino server in cleartext using HTTP or DIIOP.</li> </ul>
Port	Communication port number (HTTP or DIIOP).
Organization Name	Domain name provided for the Domino server account, which can be changed.  <p><b>Note</b> Organization Name is case sensitive.</p>
Username	Enter the account name used to log on to the Domino server. The format is determined by the Email ID fields in the Person object classes and attributes.
Password	Password used to access the Domino server account, which can be changed. <p><b>Note</b> Make sure the Internet password is used in the Password fields in the System Configuration&gt; IBM Domino window and the LDAP Server window.</p>
Polling Interval (minutes)	Specifies the time interval, in minutes from 1 to 360, to poll the Domino server for meeting information.
Certificate	Use the field to provide an IBM Domino trust certificate class file. Use the Domino CLI command, <b>tell diiop show config</b> , to find the class filename. <p><b>Note</b> A certificate is required in secure mode only.</p>

## Synchronization Operations

The Synchronization Operations area tells you when information in the Domino server database was last updated with meetings scheduled for a particular room.



### Tip

You can filter the list of rooms by their synchronization status by using the Subscription Status drop-down menu and clicking Filter.

When mismatched information in the databases causes meeting conflicts or there are other problems that prevent a meeting from being launched successfully, this area of the IBM Domino window allows you to synchronize information between Domino and the CTS-Manager database. Synchronization takes time and system resources to accomplish and should be done only when necessary.

To synchronize information between Domino and the CTS-Manager database:

**Step 1** Click **Resync** to start the operation.

Once you've begun the synchronization operation the Service Status field displays a Sync progress indicator showing the progress of the synchronization operation by percentage.

**Step 2** Once the synchronization operation completes, click **Refresh** to update the display.

Table 10-12 describes the information displayed in this area of the IBM Domino window.

**Table 10-12 IBM Domino Server Synchronization Report**

Field	Description
IBM Domino Databases	Name of the meeting room. Click the arrow in the header of the Room Name column to sort the list in ascending or descending alphabetical order.
Last Synchronization Time	Time the synchronization operation was started.
Resynchronization Status	Status of the synchronization operation.
Associated Rooms	Name of the Cisco TelePresence meeting rooms associated with the Domino database.  <b>Note</b> The room name displayed is the name of the room in the Domino database. In order for CTS-Manager to successfully sync the room's meeting calendar, the room name must exactly match the room name in the Cisco TelePresence System profile registered in Unified CM.

## System Settings

If you are the system administrator and know the SysAdmin password, you can open the System Settings window to see the following choices:

- [IP Settings, page 10-39](#)
- [NTP Settings, page 10-41](#)
- [SNMP Settings, page 10-42](#)
- [Remote Account, page 10-44](#)
- [Password, page 10-45](#)
- [System, page 10-46](#)

Use the tabs in this window to modify IP settings, configure a Network Time Protocol (NTP) server, enable or disable Simple Network Management Protocol (SNMP), set up a temporary account for access, change the system password, and restart the system.

## IP Settings

The IP Setting window lists information that is provided to CTS-Manager during first-time installation and configuration. Although it is typically not necessary to change IP settings, this window offers a place to modify some of them. [Figure 10-18](#) describes the fields and buttons.

**Figure 10-18** System Settings Window IP Settings Tab

**System Settings**

IP Settings | NTP Settings | SNMP Settings | Remote Account | Password | System

★ = Required fields

MAC Address: 00:1a:4b:34:96:0e

Hostname: example-domino-2

Domain Name:

Primary DNS:

Secondary DNS:

Ethernet Card: eth0

DHCP: ☐ Enable ☒ Disable

★ IP Address:


★ Subnet Mask:

★ Default Gateway:


- Step 1** To add new information, enter it in the fields provided.
- Step 2** To change information, highlight and delete existing information and enter the new information.
- Step 3** To register new or modified settings, click **Apply**.
- Step 4** To restore the original settings, click **Reset**.

Table 10-13 describes the information displayed in this area of the IP Settings window

**Table 10-13** IP Settings

Field or Button	Description or Settings
MAC Address	Display-only MAC address number supplied for this Cisco TelePresence Manager.
Hostname	Display-only hostname configured for this Cisco TelePresence Manager.
	 <p><b>Note</b> CTS-Manager hostname needs a DNS entry for email links to it to function properly.</p>
Domain Name	Domain name for this Cisco TelePresence Manager.
Primary DNS	Primary DNS server IP address supplied for this Cisco TelePresence Manager.
Secondary DNS	Secondary DNS server IP address supplied for this Cisco TelePresence Manager.

**Table 10-13** IP Settings (continued)

Field or Button	Description or Settings
Ethernet Card	Name supplied for the system Ethernet card.
DHCP	Enable and Disable radio buttons determine whether DHCP is enabled or disabled. When the Enable radio button is chosen, information in the IP address fields cannot be modified.  <div>  <b>Note</b> To modify the IP settings for this Cisco TelePresence Manager, click the <b>Disable</b> radio button. </div>
IP Address	IP address supplied for this Cisco TelePresence Manager.
Subnet Mask	Subnet mask used on the IP address.
Default Gateway	Default gateway IP address supplied for this Cisco TelePresence Manager.

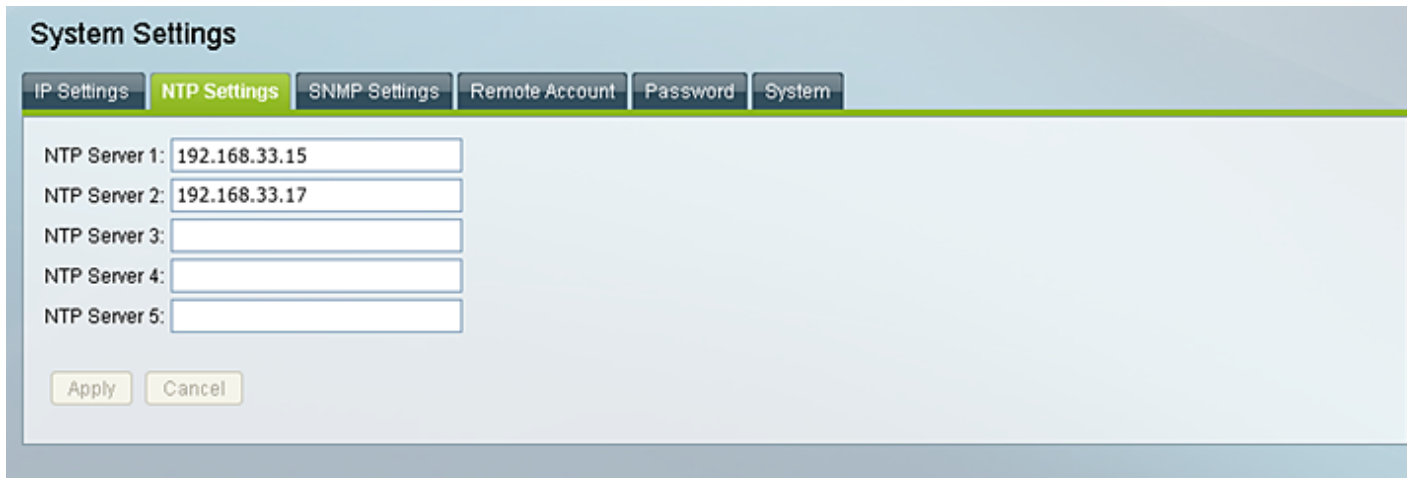
**Deleting Server**

Before performing a delete on a DNS server, it is important to first change existing servers like Unified CM and Conferencing Bridge to IP from hostname before the DNS server is deleted. If the hostname is not changed first, the Unified CM and Conferencing Bridge servers will be put in error status.

## NTP Settings

Click the NTP Setting tab in the System Settings window to list the configured IP address of the Network Time Protocol (NTP) servers.

NTP is used to synchronize the clocks on Cisco IP telephony servers with an external network time server that uses NTP.

**Figure 10-19** System Settings Window NTP Settings Tab


**System Settings**

IP Settings **NTP Settings** SNMP Settings Remote Account Password System

NTP Server 1: 192.168.33.15

NTP Server 2: 192.168.33.17

NTP Server 3:

NTP Server 4:

NTP Server 5:

Apply Cancel

- 
- Step 1** To add an NTP server to the configuration, enter the IP address in an NTP Server field.
- Step 2** To change an NTP server in the configuration, highlight and delete the IP address in the NTP Server field and enter the new address.
- Step 3** To register new or modified settings, click **Apply**.
- Step 4** To restore the original settings, click **Reset**.
- 

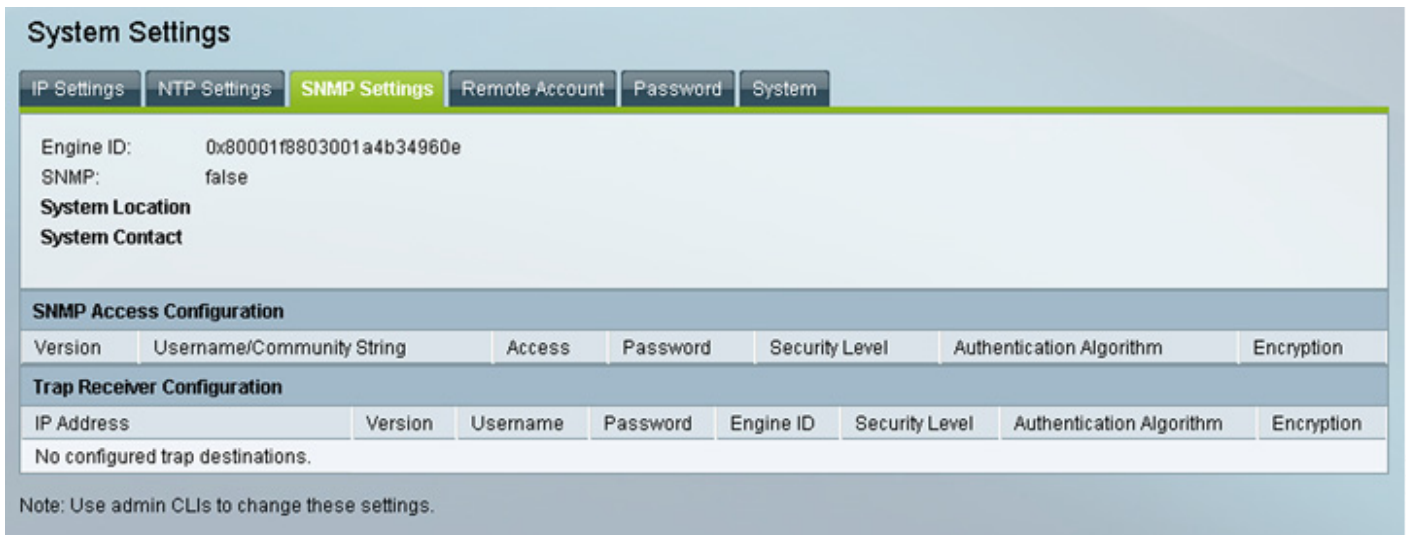
## SNMP Settings

SNMP is an industry-standard interface used by network management systems to capture system status and error information, including information provided by Unified CM. Use the CLI function to enable and disable SNMP Service and also configure communities and trap destinations.

Use the CLI commands to change these settings:

- No trap receiver configured. Use the CLI **snmp set** command to configure a trap receiver. The fields collect trap receiver hostname or IP address and port, version, password, security level, authentication algorithm, and encryption.
- No SNMP community or users are configured. Use the CLI **snmp set** command to configure users and communities.
- To view SNMP settings, click the **SNMP Setting** tab in the System Settings window.

**Figure 10-20** System Settings Window SNMP Settings Tab



**System Settings**

IP Settings | NTP Settings | **SNMP Settings** | Remote Account | Password | System

Engine ID: 0x80001f8803001a4b34960e  
 SNMP: false  
 System Location  
 System Contact

**SNMP Access Configuration**

Version	Username/Community String	Access	Password	Security Level	Authentication Algorithm	Encryption
No configured trap destinations.						

**Trap Receiver Configuration**

IP Address	Version	Username	Password	Engine ID	Security Level	Authentication Algorithm	Encryption
No configured trap destinations.							

Note: Use admin CLIs to change these settings.

Table 10-14 describes the fields for SNMP settings.

**Table 10-14** *SNMP Settings*

Field	Description or Settings
– Engine ID	The engine ID for the SNMP agent on this CTS-Manager. If you configure the trap receiver, this engine ID is used to create a trap user on the trap receiver system and to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.
– SNMP	The default is disable. To change setting to enable, you must use the CLI <b>Utility</b> command. When SNMP is enabled, supply a password for the SNMP server in the <b>Configuration</b> area.
<b>SNMP Access Configuration</b>	<b>Use the CLI <code>snmp set</code> command to change these settings</b>
– Username	SNMP server username.
– Current Password	SNMP server password. The password must be 8 characters long. Enter it twice for verification.
<b>Trap Receiver Configuration</b>	<b>Use the CLI <code>snmp set</code> command to change these settings. See examples in following section.</b>
– IP Address/Hostname:Port	IP address or hostname and port number of the trap receiver
– Username	Trap receiver username.
– Current Password	Trap receiver password. The password must be 8 characters long. Enter it twice for verification.
– Authentication Algorithm	Choose Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) for authentication.

**Note**

When performing a new installation, a default snmp “admin” user will not be created. The system created default “admin” user with the default password, “snmppassword” must be changed in the new installation. All customer created, modified snmp users and trap destinations will be migrated to a new installation.

## Technical Notes

CTS-Manager supports SNMP v3 and v2c. Together it supports ten SNMP users and five trap destination/receivers. A string of trap receiver settings is added to the `/etc/snmp/snmpd.conf` file to configure the trap receiver on the Cisco TelePresence Manager server. The string must include the following information, which is collected in the fields described in [Table 10-14](#) or is set by default:

- IP address and port number of the trap receiver
- Trap receiver username
- Trap receiver user password
- Trap sender engine ID
- Authentication method, either MD5 for Message Digest 5 or SHA for Secure Hash Algorithm

- Security model, which by default is *authNoPriv*
- SNMP version, which by default is version 3
- Included MIBs, which by default is ALL.

The following is an example trap receiver entry:

```
trapsess -e 0x80001f880474657374 -v 3 -m ALL -l authNoPriv -u traper -a MD5 -A changeme
171.71.232.113:162
```



#### Note

v3 Trap destination user cannot overlap with snmpv3 user. This is allowed only if both v3user and trap destination have same password:

Allowed:

```
set snmp user add 3 admin rw authNoPriv snmppassword.
```

```
set snmp trapdest add 3 admin 172.20.124.44 authNoPriv snmppassword 0x80001f8803001a64635cd4
```

Not allowed:

```
set snmp user add 3 admin rw authNoPriv snmppassword
```

```
set snmp trapdest add 3 admin 172.20.124.44 authNoPriv cisco123 0x80001f8803001a64635cd4
```

These fields can be viewed and configured using **get** and **set** commands on the */usr/sbin/snmpconfig* script. To test your configuration, run **snmptrapd come** with **net-snmp** on the trap receiver system. You can create the user in */etc/snmp/snmptrapd.conf* on the trap receiver system before starting **snmptrapd**.

## Remote Account

Use this window to set up limited access for remote users of this CTS-Manager. The remote account is intended for use by Cisco technical support personnel so they can access the system remotely to troubleshoot problems. Secure Shell (SSH) is used to access the system. The remote account is typically enabled for a brief period. Disabling the account will cause whoever is logged onto the system to be logged off. Only one remote account can be set up at a time, but more than one remote account can be active at the same time.

Login to the remote account is done using the account name and a passphrase generated by software in this CTS-Manager. The remote user uses the account name, the passphrase, and a utility available at an internal Cisco web site to generate a login name and password that allow access to this Cisco TelePresence Manager.

Figure 10-21 **Configure > System Settings > Remote Account Window**

**System Settings**

IP Settings | NTP Settings | SNMP Settings | **Remote Account** | Password | System

\* = Required fields

\* Account Name:

\* Duration (days):

Add

To start the remote login account process, perform the following steps:

**Step 1** Enter a name for the remote login account in the **Account Name** field.

This name can be anything you choose, using English characters.

**Step 2** Enter the number of days that the account should be active.

**Step 3** Click **Add**.

This step generates a passphrase.

To complete this process, the account name and passphrase are entered into a utility at the following Cisco Internal web site:

<https://remotesupporttool.cisco.com/logon.php>

For security reasons, if remote users fail to log off, they will be logged off automatically at the time listed in the Expires field.

## Password

Use the System Settings window to change the SysAdmin password for the Cisco TelePresence Manager. You must know the current password. Input the new password the second time for verification. Do not use anything other than English, as International words or characters are not supported in this release.

**Figure 10-22** *Configure > System Settings > Password*

The screenshot shows the 'System Settings' window with the 'Password' tab selected. The window has a title bar 'System Settings' and a tab bar with 'IP Settings', 'NTP Settings', 'SNMP Settings', 'Remote Account', 'Password' (selected), and 'System'. Below the tabs, there is a legend: '✱ = Required fields'. The form contains four fields: 'Username:' with the value 'admin', 'Current Password:', 'New Password:', and 'New Password (verify):'. Each of the last three fields has a small '✱' icon to its left. At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

**Step 1** To display the password fields, click the **Password** tab.

**Step 2** Enter your current password.

**Step 3** Then, to change password, go to the **New Password** field and enter your new password, using only English characters.

**Step 4** In the **New Password (verify)** field, repeat your new password to verify it.

**Step 5** To register the new password, click **Apply**.

**Step 6** To restore the original password, click **Reset**.



**Note**

Password should contain both upper and lower-case alphabetic and non-alphabetic characters. It should not be similar to the current password or be based on common words found in the dictionary.



**Note**

The password cannot be changed until at least 24 hours after it was created, unless you reinstall CTS-Manager.

## System

This window allows you to restart or shut down CTS-Manager.

**Figure 10-23** System Configuration System Settings

**Step 1** To restart the system, enter the password.

**Step 2** Click **Restart** to restart the system or **Shutdown** to shut down the CTS-Manager.

## Database - Status, Backup, and Restore

CTS-Manager uses an Informix database server to store information. The Database window allows the Administrator to view the database status and run backup and restore operations. Open the Database window to see the following choices:

- [Settings](#)
- [Backup](#)
- [Restore](#)

## Settings

The Settings window allows you to manage the size and age of meeting information in the Informix database. To register new settings, click **Apply**. To return to the original settings, click **Reset**.

**Figure 10-24 Database Window Settings Tab**

**Database**

**Settings** Backup Restore

✳ = Required fields

Service Status: OK

Current Database Size: 0.01% full (1.25 of 14648.44 MB is used)

✳ Automatically Purge Data Older Than (months): 1 +

Apply Cancel

(+) The system automatically purges data when database utilization exceeds 75% of the allocated disk space.

**Snapshots of Number of Meetings** Showing 1-6 of 6 10 per page Go

Date(+)	Past Meetings	Future Meetings
05/21/2010 11:55 PM	67	495
05/22/2010 11:55 PM	68	492
05/23/2010 11:55 PM	70	490
05/25/2010 11:55 PM	81	484
05/26/2010 11:56 PM	89	484
05/28/2010 10:55 AM	94	478

Page 1 of 1

(+) All times are shown in time zone America/Los\_Angeles (GMT -7.0)



### Note

CTS-Manager operates only on those recurring meetings that have a start time within 2 years in the past.

Table 10-15 describes the information and settings that are accessible from the Database window Settings tab.

**Table 10-15 Database Settings**

Field	Description or Settings
Service Status	Display-only status report of the Informix database server.

**Table 10-15** Database Settings (continued)

Field	Description or Settings
Current Database Size	Display-only report showing the size of the database as a percentage of the amount of total space available for a Cisco TelePresence Manager account in Directory Server. The number displayed should not exceed 75%.
Automatically purge data older than (months)	<p>Sets the number of months of storage for the information in the database.</p> <p>Data older than the specified number of months is purged.</p> <p>The purge cutoff date for this setting should be selected by balancing the number of months of data retention against the size of the database required to store the data created during that period. The default setting of 1 month is considered a reasonable midpoint.</p> <p><b>Note</b> Database utilization cannot exceed 75% of the allocated disk space, and takes precedence. If the number of months you have specified exceeds this percentage, older data is purged so as not to exceed 75%.</p>

The view at the bottom of the Database Settings window displays, for example, the status of past meetings for the past month and the future meetings scheduled for the next 12 months. If the list is longer than is what is showing, use the Next or Last button to view more data.

## Backup

Choose the Backup tab to display fields and settings that will assist you in scheduling backups of the database. It is important to keep the backup current in case you need to activate the backup CTS-Manager system.

Figure 10-25 Configure &gt; Database &gt; Backup

**Database**

Settings **Backup** Restore

✱ = Required fields

Schedule (+): Daily @ 23:55 [Change...](#)

Number of Backup Files to Keep: 2

Backup Type: ☒ Local ☐ Remote

Backup Mode: ☒ Sftp ☐ Ftp

Remote Storage Host:

Port: 22

Username:

Password:

Storage Path:

[Back Up Now](#) [Verify Remote Host](#) [Apply](#) [Cancel](#)

Showing 1-2 of 2 10 per page [Go](#)

Time (+) ▾	Status	Type	Hostname	Location
05/27/2010 11:55 PM	OK	Local	example-dom3	/common/dbbackup/CTMbackup.file.example-dom3.1.7.0.0.2010-05-28-06-55-00.tar.gz
05/26/2010 11:55 PM	OK	Local	example-dom3	/common/dbbackup/CTMbackup.file.example-dom3.1.7.0.0.2010-05-27-06-55-00.tar.gz


[Refresh](#) Page 1 of 1

(+) All times are shown in time zone America/Los\_Angeles (GMT -7.0)

## Changing the Backup Schedule

The backup schedule currently set is displayed in the Backup window.

To change the backup schedule:

- 
- Step 1** Click **Change**.
- Step 2** Choose the starting time from the Start Time drop-down list. This sets the backup time in your local time zone.
- Step 3** Choose the frequency of the backups by clicking the **Daily** or **Weekly** radio button.
-  **Note** If you click **Weekly**, check the box for the day of the week on which the backup should occur.
- 
- Step 4** Click **OK** to register your settings, or **Cancel** to restore the original settings
-

To register new or modified settings, click **Apply**. To restore the original settings, click **Reset**.

**Note**

Backup schedules are now displayed in your local time zone.

## Backing Up CTS-Manager Data

Data backups are performed on the Active partition. If you switch partitions after performing a backup you'll need to perform another backup for the new Active partition. As part of data backup, the following system information is backed up:

- Database data
- System SNMP configuration information
- System certificates
- License files

To back up files in the database:

- Step 1** From the drop-down list, choose the number of backup files to keep. If you choose 3, the last three backup files will be kept, but earlier backup files will be purged.

**Note**

If you are creating remote backups the number of backup files is not affected. CTS-Manager only keeps track of the number of backups made locally.

- Step 2** Choose the type of backup by clicking the **Local** or **Remote** radio button.

- Step 3** Test your connection to a remote host by clicking **Verify Remote Host**.

- Step 4** Click **Back Up Now** to begin the operation.

## Remote Storage Host Fields

A remote backup uses Secure FTP (SFTP) or FTP to store files remotely. If you choose to backup or restore using FTP, you do not need to supply a port number.

**Note**

FTP scripts for Upgrade, Backup and Restore use Expect scripts and perform on a best-effort basis, due to potential variations in the responses sent by the FTP server. Only username/password-based login is supported. Anonymous login is not supported. Secure FTP (SFTP) is the recommended mode of transferring files over the network.

**Note**

Backup files stored at remote location are stored in compressed form but are not encrypted. Ensure that the backup files are not publicly accessible by choosing a secure storage location.

You must fill in the following fields to gain access permissions to a remote host:

**Table 10-16 Remote Storage Host Fields**

Field	Description
Remote Storage Host	Pathname of the remote host.
Port	Port to access the remote host. The default is port 22 for SFTP.
Username	Login name for the remote server.
Password	Password to access the remote server.
Storage Path	The full pathname where you want to store the backup files.

## Viewing Backup History

The Database window Backup tab provides a history of database backups.

[Table 10-17](#) describes the Backup History and Restore History fields.

**Table 10-17 Backup History and Restore History Fields**

Field	Description
Timestamp	Date and time of backup. Click the arrow in the header of the Timestamp column to sort the list in ascending or descending order.
Status	Status of the backup.
Type	Type of backup, either local or remote.
Hostname	Name of host for the backup files.
Location	Pathname where the files are stored.

## Restore

The Restore tab displays the history of the database restore operations. As part of the data restore, the following data is restored from the CTS-Manager backup file:

- Database data
- System SNMP configuration information
- System Certificates
- License files


**Note**

CTS-Manager validates license files with system host ID during startup. If a license file does not match the host ID of the system, it is removed and its corresponding feature is in grace period.

OS parameters such as NTP, DNS are not backed up and thus not restored. It is expected that these parameters are configured by the administrator on the system during installation and later modified using CLI commands.


**Note**

Do not create mixed DNS and non-DNS environments. Identifying Unified CM node as publisher does not support mixed mode.

See [Table 10-17](#) for a description of the fields.

**Figure 10-26** *Configure > Database > Restore*

**Database**

Settings Backup **Restore**

✱ = Required fields

Restore Type: ☒ Local ☐ Network

Restore Mode: ☒ Sftp ☐ Flp

Remote Storage Host:

Port:

Username:

Password:

Storage Path:

Showing 0-0 of 0  per page

Time (+) ▾	Status	Type	Hostname	Location
No data to display				

(+) All times are shown in time zone America/Los\_Angeles (GMT-7.0)

## Restoring Backup Data

When you restore data from a backup file, all changes made to the database since the backup will be lost. These changes must be added by the Exchange Sync Up and Discovery functions of the Cisco TelePresence Manager server. The database Restore function should be run only as a last resort; for example, when the database is corrupted or the disk fails and has to be replaced.

The restore operation will stop the Informix database server, so some CTS-Manager operations might be impacted during the operation. While the restore operation is in progress, all other processes are stopped. The user interface will only display progress of the restore operation. When the restore operation is complete, the Cisco Telepresence Manager is automatically restarted and the login page is displayed. You will have to log in to resume use of the Cisco Telepresence Manager application.



### Note

You cannot restore the database from previous versions of CTS-Manager.

## To restore data from a backup:

Clicking **Available Backups** displays a window listing all the backups stored locally and remotely. If you want to restore from a backup stored remotely you must first click the Network Restore Type radio button. Then choose either the SFTP or FTP Restore Mode and enter required information to access the remote host. See [Table 10-16](#) for a description of the Remote Storage Host fields.

**Note**

The license files are bundled as part of backup. The Restore process restores backed up license files. However, when a CTS-Manager backup is restored onto another server, the server is not functional for the licensed features until new licenses are imported.

- 
- Step 1** Click the **Refresh** button to view the list of backups.
- Step 2** Click the radio button next to the backup filename that is to be used for the restore operation.
- Step 3** Click **Restore Now**. This action initiates a full restore of the database from the backup file.
- 

## Unified CM

The Configure > Unified CM window displays the settings that associate CTS-Manager with Cisco Unified CM, choose Configure > Unified CM. You can modify these settings.

This window provides Service Status and the listings of the Unified CM connections.

**Note**

Do not create mixed DNS and non-DNS environments. Identifying Unified CM node as publisher does not support mixed mode.

**Note**

If you change the settings in the Unified CM, you must select it and click Discover Rooms to register the new settings or wait until the next maintenance cycle has taken place, before the current status will be displayed in CTS-Manager.

Figure 10-27 Configure &gt; Unified CM Window

Unified CM

Service Status: **OK**

Showing 1-1 of 1 10 per page Go

Status	Hostname	IP Address	Application Username
<input type="radio"/> OK	<a href="#">example-dom-ccm1</a>	<a href="#">192.168.3.3</a>	exampleappuser

New... Edit... Delete Discover Rooms Refresh

Page 1 of 1


Click the radio button to select a Unified CM server. Once a Unified CM is selected, the buttons on the screen become usable. Refer to [Table 10-19](#) for a description of each button's function.

To manually start the process that is periodically performed to discover new rooms added to Cisco Unified CM, click **Discover Rooms**.

**Note**

This process consumes a large amount of system processor time. System operation will be noticeably slower from the time that the Discover Rooms button has been clicked until the process is completed.

Table 10-18 Discover Cisco Unified Communications Manager Settings

Field	Description or Settings
Status	<p>Display-only status report of system services.</p> <p><b>Note</b> You may see a progress indicator in the status field, especially if many Cisco TelePresence meeting rooms are being managed by CTS-Manager. Each time this page is accessed, the status is updated, and the progress indicator will be seen while the system is discovering meeting rooms.</p> <p> <b>Caution</b> An error status is displayed if the connection to the Unified CM server was lost due to a network outage or if the Unified CM server was down during the CTS-Manager maintenance cycle. You can resolve the error status by clicking <b>Discover Rooms</b>.</p>
New	This opens the Discovery Service window to add a new Cisco Unified Cm connection.
Edit	This opens the Discovery Service window to correct current settings.

**Table 10-18 Discover Cisco Unified Communications Manager Settings (continued)**

Field	Description or Settings
Delete	This deletes the current Cisco Unified CM connection.
Discover Rooms	This allows you to manually start the process that is periodically performed to discover new rooms added to Cisco Unified CM.
Refresh	This refreshes the window, ensuring the information is up to date.

Once you select a record and press **New** or **Edit**, the Unified CM Service window appears as shown in [Figure 10-28](#).

**Figure 10-28 Unified CM Service Window**

To test the connection between Cisco TelePresence Manager and Cisco Unified Communications Manager, click **Test Connection**.

To register new or modified settings, click **Save**. To restore the original settings, click **Reset**.

[Table 10-19](#) describes fields, buttons, and settings.

**Table 10-19 Discovery Service Cisco Unified CM Settings**

Field	Description or Settings
Host	Name of the Cisco Unified CM server host that was selected in the Discover window.
Username	Username for login to the Cisco Unified CM server.
Password	Password to access the Cisco Unified CM server.
Certificate	Use the field to provide a trust certificate for new Cisco Unified CM server.
Test Connection	Tests the connection between CTS-Manager and Cisco Unified CM server.
Save	Save the new settings.
Reset	Restore the original settings.

When a room is deleted from the application user profile, it is automatically deleted from CTS-Manager without re-discovery. It is removed from calendar server view, but remains in rooms view.

**Note**

---

Rooms should be deleted only after an administrator manually does a rediscovery. If the room has a large number of meetings, it is possible that the CTS-Manager performance will be impacted.

---

# Bridges and Servers

The Bridges and Servers window provides the ability to add and delete bridge and server devices. There are five devices supported by CTS-Manager:

- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco Unified Video Conference device (CUVC)
- Cisco TelePresence Recording Server (CTRS)
- Cisco Media Experience Engine (MXE)
- WebEx (WebEx) server



## Caution

If a bridge or server device is reinstalled, it must be registered again through Cisco TelePresence Manager. There are no errors generated by a bridge or server device software change. The administrator of the bridge or server device must inform you of the change.



## Note

When Interoperability with Video Conferencing is enabled, multipoint meetings require a CTMS and an MXE in a scheduled state.

**Figure 10-29** *Configure > Bridges and Servers*

Bridges and Servers						
Service Status:		OK				
						Showing 1-3 of 3 10 per page Go
	Status	Hostname	Type	Control State	Description	IP Address
<input type="radio"/>	OK	<a href="#">example-ctms-13</a>	CTMS	Scheduled	CTMS	192.168.19.7
<input type="radio"/>	OK	<a href="#">192.168.15.12</a>	CUVC	Scheduled	CUVC	192.168.15.12
<input type="radio"/>	OK	<a href="#">example.webex.com</a>	WebEx			http://example.webex.com/example
<div> <input type="button" value="New..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/> <input type="button" value="Deallocate.."/> <input type="button" value="Refresh"/> </div> <div> <input type="button" value="Previous"/> <input type="button" value="First"/> Page 1 of 1 <input type="button" value="Next"/> <input type="button" value="Last"/> </div>						

Table 10-20 describes the Conferencing Bridge Device fields.

**Table 10-20** *Bridges and Servers Devices*

Field	Description or Settings
Status	Display-only status report of system services.  <b>Note</b> You may see a progress indicator in the status field, especially if many Cisco TelePresence meeting rooms are being managed by CTS-Manager. Each time this page is accessed, the status is updated, and the progress indicator will be seen while the system is discovering meeting rooms. A CUVC always shows a status of OK
IP Address	The IP address of the bridge or server.
Hostname	The configured Hostname of the Conferencing Bridge. Clicking the hostname hyperlink opens a new browser window, with the CTMS login page.
Type	The Conferencing Bridge Type. Clicking the arrow allows you to sort ascending or descending.
Control State	The Control State is either Scheduled or Non-Scheduled. If Non-Scheduled is listed, the resource allocation function won't be used. The arrow allows you to sort ascending or descending.
Interop Quality	This area shows the selected SD (CIF) or HD (720p) quality. This is not the quality the device can support, but it is the video quality mode currently set in the Application Setting window.
Description	The Description field displays the Conferencing Bridge device description, added when the Conferencing Bridge device was added. CUVC is the default; CTMS is configured in the CTMS program.

## Adding a Bridge or Server Device

To register a bridge or server with Cisco TelePresence Manager, click **New** to display the New...Bridge or Server dialog box, and choose CTMS from the Type drop-down field.

Details on configuring specific bridges and servers, are available in the following sections:

- [VC Rooms, page 10-72](#)
- [Cisco Unified Video Conferencing \(CUVC\), page 10-61](#)
- [Cisco TelePresence Recording Server \(CTRS\), page 10-63](#)
- [Cisco Multimedia Experience Engine \(MXE\), page 10-64](#)
- [Live Desks, page 10-75](#)

## Editing Bridge or Server Settings

To edit a bridge or server device, click the radio button on the device line to select that device. Click the Edit button. The Edit...Bridge or Server window appears.

## Deleting a Bridge or Server

A bridge or server cannot be deleted if there are any associated scheduled meetings. If the bridge or server is a CUVC, with associated scheduled meetings, you must first Deallocate the CUVC resources before you can delete the device.

To delete a bridge or server device, click the radio button next to the device and click **Delete**.

## Deallocate a Bridge or Server

Go to the Application Setting window. In the Interoperability with Video Conferencing section, under the Enable Feature, select **No**.

Then in the Bridges and Servers window, click the radio button next to the selected device and click **Deallocate**.

## Refreshing the List of Bridges or Servers

Click the **Refresh** button to refresh the list of bridge or server devices.

**Note**

Once Interop has been enabled (see [Application Settings](#)), a CTMS device can only be added to CTS-Manager if it is interop-ready. An interop-ready device is defined as running a certain level of software release.

## Cisco TelePresence Multipoint Switch (CTMS)

A CTMS communicates with the Cisco TelePresence Manager. CTMS devices provide the functionality for three or more Cisco TelePresence rooms to attend a conference call. Cisco TelePresence Manager provides the scheduling information to the different CTMS devices and each CTMS provides the multipoint switching capabilities for the conference.

### Adding a CTMS


To add a CTMS device to Cisco TelePresence Manager:

- 
- Step 1** Go to the Configure > Bridges and Servers window.
  - Step 2** Click **New** to display the New Bridge or Server dialog box.
  - Step 3** Choose CTMS from the Type drop-down field.
  - Step 4** Enter the information, click **Save**.

After you add the CTMS, you can edit it later by selecting it and clicking the **Edit** button.

---

**Figure 10-30** Adding a CTMS Device**New...Bridge or Server**

 = Required fields

Type: CTMS ▾

Hostname:

Username:

Password:

Control State: ☐ Scheduled ☒ Non-Scheduled

**Table 10-21** CTMS Device Information

Field	Description or Settings
Type	Select CTMS from this pull-down list menu.
Hostname	The hostname or IP address of the CTMS. This is the LHS of the complete Host name.
Username	This is the account name used to log into the CTMS.
Password	This is the account password used to log into the CTMS.
Control State	Specify whether the CTMS is available (scheduled) for meetings. The resources of a scheduled CTMS can be used when meetings are scheduled. Specifying a CTMS as Non-Scheduled means the CTMS will not be used when a meeting is scheduled.  CTMS devices in a Scheduled state cannot be used to migrate meetings from other CTMS devices.

**Note**

To downgrade an existing CTMS to an software version earlier than 1.7, you must restart CTS-Manager to establish a fresh connection.

**Resource Allocation with CTMS Devices**

CTS-Manager chooses an available CTMS based on the time zone that is closest to the majority of the TelePresence endpoints participating in the meeting. If there are multiple available CTMS devices in the same time zone, CTS-Manager randomly chooses a CTMS based on its database record number.

## Cisco Unified Video Conferencing (CUVC)

CTS-Manager's support of CUVC enables video conferencing devices to join a scheduled Cisco TelePresence meeting. A CUVC is notified by and joins a Cisco TelePresence meeting through a CTMS. A CTMS device must be used to enable video conferencing devices to join, even if it is a point-to-point call.

There are two options for registering CUVC devices with CTS-Manager:

- Using a single CUVC device
- Using the CUVC Manager application to manage a pool of ports (participants) from multiple CUVC devices to enable TelePresence Interop meetings that transparently span conference bridges (dynamic cascading)

### Adding a CUVC

To add a CUVC device to Cisco TelePresence Manager:

- 
- Step 1** Go to the Configure > Bridges and Servers window.
- Step 2** Click **New** to display the Registration dialog box.
- Step 3** Choose CUVC from the Type drop-down field.
- Step 4** Enter the information, click **Save**.

After you add the CUVC, you can edit it later by selecting it and clicking the **Edit** button.

---



#### Note

If you do not find CUVC in the Type drop-down menu, go to Configure > Application Settings > Bridges and Servers and make sure Interoperability with Video Conferencing is enabled and either CUVC-CIF or CUVC-720p is selected for Interop Quality.

---

**Figure 10-31** Adding a CUVC Device

**New...Conference Bridges**

✱ = Required fields

Type:	CUVC ▼
Hostname:	<input type="text"/>
Control State:	<input type="radio"/> Scheduled <input checked="" type="radio"/> Non-Scheduled
Call-In Number Prefix for CTMS:	<input type="text"/>
Call-In Number Prefix for Video Conference Participants:	<input type="text"/>
Meeting Number Length:	1 ▼
Maximum Participants per Conference:	<input type="text"/>
Minimum Participants per Conference:	<input type="text"/>
Total resources:	<input type="text"/>

**Table 10-22** CUVC Device Information

Field	Description or Settings
Type	If only CTMS appears in the drop-down list, Interop has not been enabled. Use the <a href="#">Application Settings</a> window to enable Interoperability with Video Conferencing. <b>Note</b> Only one CUVC can be supported by one CTS-Manager.
Host Name	This is the LHS of the complete Host name.
Control State	Specify whether the CUVC is available (scheduled) for meetings. The resources of a scheduled CUVC can be used when meetings are scheduled. Specifying a CUVC as Non-Scheduled means an Interop meeting will not be available when a meeting is scheduled.
Call-In Prefix for CTMS	The call-in number prefix for your CTMS is based on your enterprise dialing plan.
Call-In Number Prefix for Video Conferencing Participants	This call-in number prefix is based on your enterprise dialing plan.
Meeting Number Length	The meeting number can be 1-8 digits in length. The system-generated meeting number is used to create an Interop Call-In Number used by the CTMS to establish the conference call. It is also used to create the Interop Call-In Number sent in an email to meeting participants, as the dial-in phone number. The meeting number length is based on your enterprise dialing plan.
Maximum Participants per Conference	Enter a numeric value for the maximum number of CUVC meeting participants that may dial into the conference call. <b>Note</b> The maximum number of participants depends on the maximum number of CUVC HD or SD video ports supported by the CUVC hardware, depending on how it's configured in CTS-Manager. Refer to the CUVC manual when determining the maximum video ports capacity. CTS-Manager supports use of a single CUVC device or pooling of multiple CUVC devices through the CUVC-M application. For more information about configuring this field to use multiple CUVC devices, see <a href="#">Configuring the Maximum Participants per Conference Field for Multiple CUVC Devices</a> , page 10-62
Minimum Participants per Conference	Enter a numeric value for the minimum number of CUVC meeting participants that may dial into the conference call. The minimum value for this field is 2. This value cannot exceed the Maximum Participants per Conference value.
Total Resources	This value should be equal to or greater than the Maximum Participants per Conference.
Type	If only CTMS appears in the drop-down list, Interop has not been enabled. Use the <a href="#">Application Settings</a> window to enable Interoperability with Video Conferencing. <b>Note</b> Only one CUVC or Cisco Unified Video Conferencing Manager (CUVC-M) can be supported by one CTS-Manager.

### Configuring the Maximum Participants per Conference Field for Multiple CUVC Devices

To configure the Maximum Participants per Conference field for multiple CUVC Devices:

- Step 1** Log into CUVC-M for the CUVC server you are adding.
- Step 2** Go to the Active Meeting Types window.

In the Maximum Available Ports column for the appropriate meeting type, the SD port count is displayed.

**Step 3** If Interop Quality in CTS-Manager is set to:

- a. CUVC-CIF (SD): Find the Maximum Available Ports number of the CIF meeting type in CUVC-M and enter that number in the Maximum Participants per Conference field for the CUVC device in CTS-Manager.
- b. CUVC-720p: Find the Maximum Available Ports number of the 720p meeting type in CUVC-M, divide it by 4 and enter it in the Maximum Participants per Conference field for the CUVC device in CTS-Manager.

For CUVC-720p, one additional step is required in CUVC-M: Go to the Meeting Type Detail window for the selected meeting type and make sure TelePresence Support is checked.

For more information about CUVC-M, go to the following URL:

[http://www.cisco.com/en/US/products/ps7088/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps7088/tsd_products_support_series_home.html)

## Cisco TelePresence Recording Server (CTRS)

The Cisco TelePresence Recording Server allows you to record video content such as training, executive messaging, and corporate communications using an existing TelePresence installation.



**Note**

Adding a CTRS is only required with the Commercial Express Bundle.

### Adding a CTRS Server

To add a CTRS to Cisco TelePresence Manager:

**Step 1** Click **New** to display the Registration dialog box.

**Step 2** Choose CTRS from the Type drop-down field.

**Step 3** Enter the information, click **Save**.

After you add the CTRS, you can edit it later by selecting it and clicking the **Edit** button.

**Figure 10-32** Adding a CTRS Device

**New...Bridge or Server**

✱ = Required fields

Type: CTRS ▾

Hostname:

Username:

Password:

**Table 10-23** Adding a CTRS Device

Field	Description or Settings
Type	Select CTRS from the pull-down list menu.
Hostname	The configured hostname of the CTRS device. This is the LHS of the complete hostname
Username	This is the account name used to log into the CTRS.
Password	This is the account password used to log into the CTRS.

## Cisco Multimedia Experience Engine (MXE)

The Cisco Media Experience Engine is a modular media processing system that provides interoperability between Cisco TelePresence and video conferencing devices, extending the reach of collaboration and communication within organizations. MXE provides 720p interoperability with video conferencing.

### Adding an MXE Device

To add an MXE device to Cisco TelePresence Manager:

- 
- Step 1** Go to the Configure > Bridges and Servers window.
  - Step 2** Click **New** to display the New...Bridge or Server dialog box.
  - Step 3** From the Type drop-down field, choose MXE.
  - Step 4** Enter the information, click **Save**.

After you add the MXE, you can edit it later by selecting it and clicking the **Edit** button.

---

**Note**

If MXE does not appear in the Type drop-down menu, go to the Configure > Application Settings > Bridges and Servers window and make sure Interoperability with Videoconferencing is enabled and MXE-HD is selected.

**Figure 10-33** Adding an MXE Device

**New...Conference Bridges**

✶ = Required fields

Type:

Hostname:

Username:

Password:

Control State: ☐ Scheduled ☒ Non-Scheduled

**Table 10-24** MXE Device Information

Field	Description or Settings
Type	Select MXE from the pull-down list menu.
Hostname	The configured hostname of the MXE device. This is the LHS of the complete hostname
Username	This is the account name used to log into the MXE.
Password	This is the account password used to log into the MXE.
Control State	Select either Scheduled or Non-Scheduled. Specify whether the MXE is available (scheduled) for meetings.  MXEs in a scheduled state cannot be used to migrate meetings from other MXEs.If Non-scheduled is selected, resource allocation is not available. Selecting Scheduled allows resource allocations.

## WebEx

Meeting organizers can add WebEx participants to their meeting. CTS-Manager is used to configure and manage the Cisco WebEx bridging feature in Cisco TelePresence meetings.

For the complete details on how to configure WebEx in CTS-Manager, refer to:

[Chapter 11, “Configuring Cisco TelePresence WebEx OneTouch for Cisco TelePresence Manager”](#).

## WebEx Proxy Server

To provide an extra level of security, you can choose to require communication between CTS-Manager and the Cisco WebEx scheduling server to go through a proxy server.

The following modes of proxy connection are available:

- Connection specifying the proxy server host and port (with no authentication).
- Connection specifying the proxy server host and port with authentication using username and password.

**Note**

Other forms of proxy connections (such as using a certificate, Kerberos, and NTLM authentication) are not supported.

## Adding a WebEx Server

To add a WebEx server to Cisco TelePresence Manager:

- 
- Step 1** Go to the Configure > Bridges and Servers window.
- Step 2** Click New to display the New... Bridges or Servers dialog box.
- Step 3** Choose WebEx from the Type drop-down field.
- Step 4** Enter the information and click **Test**.
- A message appears indicating the connection to the server is verified.
- Step 5** Click **Save**.

After you add the WebEx device, you can edit it later by selecting it and clicking the **Edit** button.

---

**Note**

If WebEx does not appear in the Type drop-down menu, make sure WebEx is enabled in the Bridges and Servers > Application Settings > Bridges and Servers window.

Figure 10-34 Adding a WebEx Server

The screenshot shows a configuration window titled "New Bridge or Server". It contains several input fields and a section for proxy server settings.

**Legend:** \* = Required fields

**Fields:**

- Type: WebEx (dropdown menu)
- Hostname: example.webex.com
- Site URL: https://example.webex.com/exam
- WebEx Admin Username: admin
- WebEx Admin Access Code: ••••••
- Certificate: (text field) [Browse... button]

**Connection Type:** ☒ Direct ☐ Via proxy server

**WebEx Proxy Server Settings**

- Host Name: (text field)
- Port: (text field)
- Require Authentication: ☐ Yes ☒ No
- User Name: (text field)
- Password: (text field)

**Buttons:** Test, Save, Close

**Table 10-25 WebEx Server Information**

Field	Description or Settings
Type	Select WebEx from the pull-down list menu.
Hostname	The configured hostname of the WebEx scheduling server.
Site URL	The address used to construct the URL that's used to access this meeting. This is the actual URL that CTS-Manager uses to communicate with WebEx. This is published in the email from CTS-Manager, and is displayed to users on the WebEx page of the CTS phone UI.
WebEx Admin Username	WebEx administrator's username (provided by the WebEx team)
WebEx Admin Access Code	WebEx administrator's access code (provided by the WebEx team)
Certificate	<p>Certificate from the hostname (WebEx scheduling server)</p> <p><b>Note</b> To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer. Then click Browse to select it and upload it to CTS-Manager. The certificate is required because communication with the WebEx server must use HTTPS. For detailed instructions on downloading the certificate with different browsers, see <a href="#">Obtaining the Cisco WebEx Site Security Server Certificate</a>, page 11-8.</p>
Connection Type	<p>Choose the type of connection to establish with the WebEx scheduling server: Direct or Via proxy server.</p> <p>Selecting the proxy server option allows you to filter IP traffic and increase security.</p>
<b>WebEx Proxy Server Settings</b>	
Host Name	Host name of proxy server
Port	Port number of proxy server
Requires Authentication	Yes or No. Select Yes if the proxy server requires authentication and then enter username and password.
Username	Username for proxy server
Password	Password for proxy server

## Access Management

From the Access Management window, it is possible to create groups, such as a Live Desk group and an Admin group. Use this window to view and create roles for these groups. CTS-Manager supports two basic roles—a Live Desk and an Administrator.

The roles have different levels of privilege and access when using CTS-Manager. For instance, members in the group mapped to the Live Desk role have limited privileges that allow them to view the meetings, rooms, and system error and log files. Members in the group mapped to the Administrator role have the privileges of the Live Desk role plus additional privileges that allow them to make configuration changes.

### Meeting Extension Premium User

Members of a group assigned to this role can also extend meetings beyond their scheduled end time using a single button on the phone. Specific settings are defined in the Configure > Application Settings > Meeting Options window. Members of the Meeting Extension Premium User can extend meeting times with a One Button To Push option on the phone.

### WebEx Roles

If you have enabled the WebEx feature, there are 3 additional roles:

- Premium WebEx User: always has WebEx with every meeting they schedule
- Permitted WebEx User: can request WebEx for specific meetings they schedule
- Non-Permitted WebEx User: is not permitted to request WebEx.

### Reporting API User

The reporting API user role can be assigned to a group that needs API access to the complete information gathered by the survey and benefits reporting feature.



#### Note

The Reporting API User role requires the Metrics Dashboard and Reporting API license to be uploaded to CTS-Manager. To upload the Metrics Dashboard and Reporting API license, go to the Configure > Licenses window, click the License Files tab and click Upload.

### Assigning Roles to Groups Using Domino Directory Assistance

If your Cisco TelePresence Manager deployment is working with an IBM Domino Server and Domino Directory Assistance, it is possible for the group to contain a user from an external directory. That type of external user cannot be granted the role of CTS-Manager Administrator. Only members of groups local to the IBM Domino Directory may be granted the Administrator role.

You can generate information about specific LDAP Group mappings, as follows:

- Choose the role from the **Role** drop-down list.
- Click **Filter**.



#### Caution

When assigning different Directory Server groups to a role, the Add window may not list the group or groups you want to add. This is a directory server limitation when the number of groups returned by the query exceeds 500. If this occurs, click the Manual radio button in the Add window, specify the Group FQDN you are searching for and assign either the Live Desk or Administrator role.

Figure 10-35 Access Management Window

**Access Management**

**LDAP Lookup Method to Authorize User Roles:**

☒ Include all the subgroups of the selected group  
☐ Look up only the selected group (no subgroups)

---

**Role to LDAP Group Mappings**

Role:

Showing 1-5 of 5  per page

	Role	LDAP FQDN
<input type="radio"/>	Reporting API User	CN= Reporting
<input type="radio"/>	Live Desk	CN= LiveDesk
<input type="radio"/>	Administrator	CN= Administrator
<input type="radio"/>	WebEx Premium User	CN= WebExPremium
<input type="radio"/>	WebEx Permitted User	CN= WebExPermitted

Page  of 1

208890

## LDAP Lookup Method to Authorize User Roles

This setting controls how CTS-Manager roles are assigned to LDAP groups.

Group Level options:

- **Include all the subgroups of the selected group**—All users in the selected group and all users in nested groups are assigned the role.
- **Look up only the selected group (no subgroups)**—Only users in the selected LDAP group are assigned the role. Users in groups within the selected group (nested groups) are ignored.

By default, CTS-Manager is set to include all subgroups of the selected group.



### Note

Cisco recommends organizations with thousands of LDAP groups to use the “Look up only the selected group” setting, otherwise users may experience a long delay when logging in to CTS-Manager.

Make the appropriate group-level selection for your organization, click **Apply** and then click **OK** to confirm your choice.

## Adding an LDAP Group to a Role

To add an LDAP group to a role in CTS-Manager:

- 
- Step 1** In the Access Management window, click **Add**.  
The LDAP Tree Selector window appears, as shown in [Figure 10-36](#).
- Step 2** Select a role from the Role drop-down menu
- Step 3** For Mode, click the Tree Selection radio button if you want to select an LDAP group from the list of all LDAP groups, or click the Manual radio button if you want to enter a specific group name in the FQDN text field.
- Step 4** Select the LDAP group(s) you want to assign to the selected role.

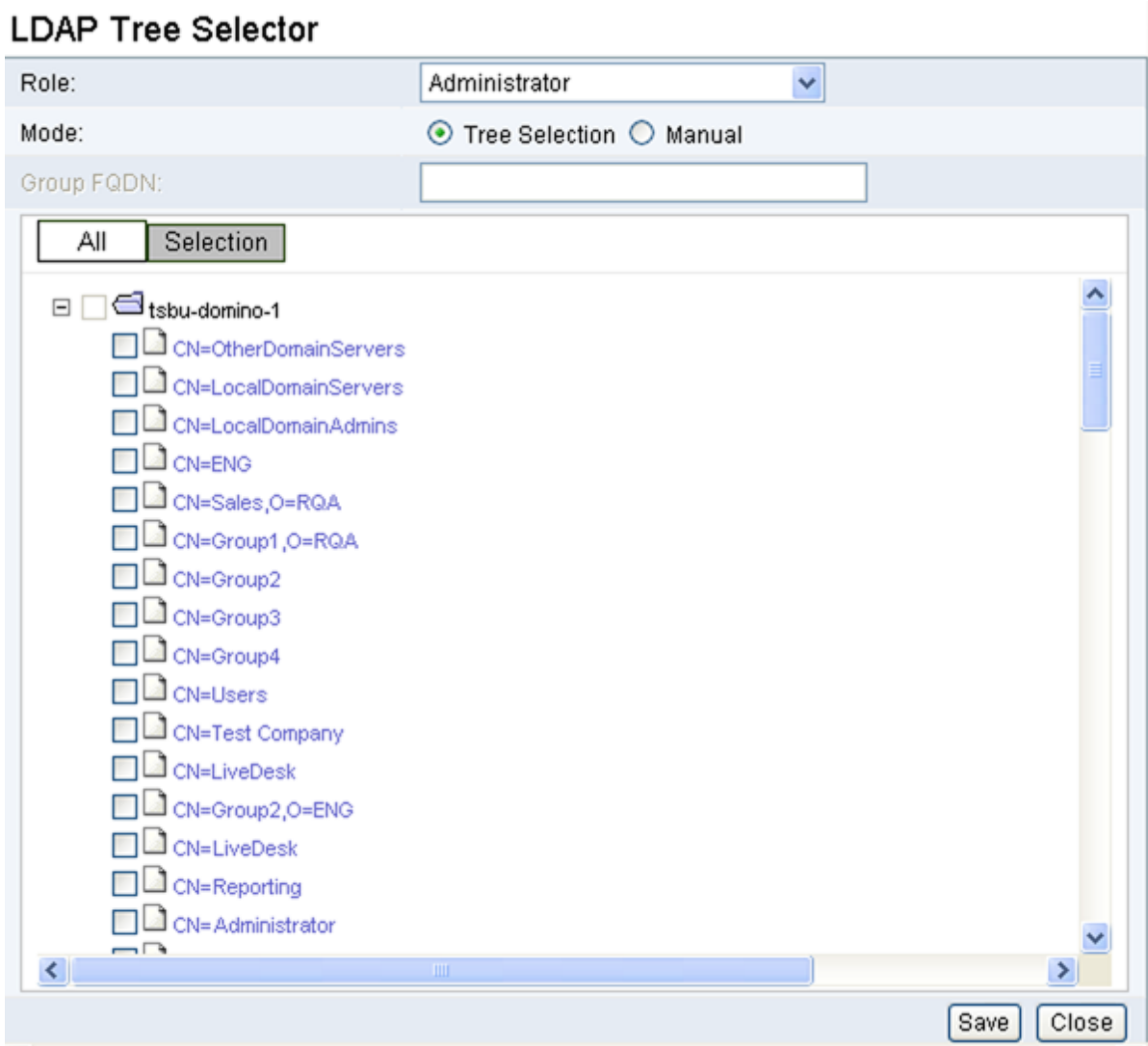


---

**Note** If you are selecting multiple LDAP groups in different directories, you can click the Selection button at any time to check which groups you currently have selected.

---

- Step 5** Click **Save**.  
The newly added role appears in the Access Management window.
-

**Figure 10-36 LDAP Tree Selector**

## VC Rooms


A CTS-Manager administrator can add video conferencing (VC) rooms to CTS-Manager, enabling easy scheduling of meetings that include video conferencing participants.

To add VC rooms to Cisco TelePresence Manager:

- 
- Step 1** Go to the Configure > VC Rooms window.
  - Step 2** Click **New** to display the New Video Conferencing Room dialog box.
  - Step 3** Enter the information, click **Save** and **Close**.

To reload the most current list of video conferencing rooms, click **Refresh**.

**Table 10-26 Video Conferencing Rooms Settings**

Field	Description or Settings
Email ID	<p>Email address of the video conferencing room.</p> <p>After you enter the email address, click <b>Validate</b> to ensure the email address is valid and to display the Name, Location and Country.</p> <div>  <p><b>Caution</b> The entire Email ID must not exceed 50 characters in length. If it exceeds 50 characters, clicking Save will cause one room license to be used but the VC room will be not be added to CTS-Manager.</p> </div>
Name	<p>Name of the video conferencing room.</p> <p><b>Note</b> This appears when the email ID is successfully validated.</p>
Location	<p>Physical location of the video conferencing room.</p> <p><b>Note</b> This appears when the email ID is successfully validated.</p>
Country	<p>Country where the video conferencing room is located.</p> <p><b>Note</b> This appears when the email ID is successfully validated.</p>
Segments required for the type of video conferencing room	<p>Set the number of segments for the video conferencing room.</p> <p>Select <b>1, 2, 3</b> or enter the number in the Other field.</p>
Phone	The phone number of the video conferencing room.
IP Address	The IP address of the video conferencing room.

## Importing Video Conference Rooms

You can import multiple video conferencing rooms at one time by creating a comma-separated values (.csv) text file with the rooms' information and uploading it to CTS-Manager.

To import video conferencing rooms:

- Step 1** Create a .csv text file in the following format:
- <fully qualified email address>, <number of segments>, <ip address>, <E.164 address (phone number)>
- Example: jsmith@example.com, 1, 10.22.146.142, 5023



**Note** The text file must have the .csv extension. Example: vc\_import.csv

- Step 2** Click **Import**.

The VC Rooms > Import window appears.

**Step 3** Click **Browse**.

The Choose file window appears.

**Step 4** Select the .csv text file and click **Open**.

**Step 5** Click **Import**.

**Step 6** To start the import, click **Start**.



**Note**

The email addresses the text file to be imported must exist in LDAP or the calendar server.

## Creating Resource Bundle Video Conference Rooms

A resource bundle room is a VC room that does not have any single VC endpoint corresponding to it, but contains extra segments for external VC endpoints to dial in. When a meeting organizer invites a resource bundle room, extra video conferencing segments are reserved for the external VC endpoints to dial in. This is useful when the meeting organizer wants to have an Interop meeting with some external VC endpoints that are outside of the organization



**Note**

A resource bundle room consumes only one room license.

To add a resource bundle room to Cisco TelePresence Manager:

**Step 1** Go to the **Configure > VC Rooms** window.

**Step 2** Click **New** to display the **New Video Conferencing Room** dialog box.

**Step 3** In the **Email ID** field, enter a valid email address to be used exclusively by this resource bundle room.



**Note**

CTS-Manager must read/write access to this email address.

**Step 4** In the **Segments required for the type of Video Conferencing Room** field, select or enter the number of desired segments.

**Step 5** (Optional) Enter **Phone** and **IP** address.

**Step 6** Click **Save** and **Close**.

To reload the most current list of video conferencing rooms, click **Refresh**.

## Scheduling Meetings with Video Conference Rooms

Scheduling TelePresence meetings with video conference (VC) rooms is just like scheduling meetings with TelePresence rooms.

To schedule a meeting with one or more video conference rooms:

**Step 1** Invite TelePresence rooms and VC rooms through Outlook or Lotus Notes, and wait for the confirmation email.

CTS-Manager automatically identifies the meeting as an Interop meeting, calculates and reserves required resources and emails the organizer with the video conference call-in information.

**Step 2** Forward the video conference call-in information to the video conference participants.

---

**Note**

A video conferencing meeting must have at least one TelePresence and one VC room. A meeting scheduled with only VC rooms will be marked as Not a TelePresence Meeting and CTS-Manager will not set up Interop or reserve any CTMS or Interop resources for the meeting.

---

**Caution**

Nonscheduled video conference room endpoints can join a scheduled meeting.

---

## VC meetings Scheduled Before Upgrading to CTS-Manager Release 1.7

Any meeting scheduled with a VC room as a participant before upgrading CTS-Manager to release 1.7, will remain a video conferencing interop meeting, with the following differences:

- No VC Interop tab is displayed in the Meeting Details window for the meeting.
- You cannot change the number of video conferencing end points joining the meeting from the Meeting Details window.
- In the Summary tab of the Meeting Details window:
  - A green checkmark appears next to Video Conferencing Interop.
  - If a VC room is added after upgrading to 1.7, a blue icon appears next to the VC room name.
  - Interop meetings scheduled in 1.7 have both the VC Room icon and the Video Conferencing Interop checkmark.
  - If VC room added in 1.6 is removed in 1.7, the Video Conferencing Interop checkmark remains.

**Note**

The CTS phone screen will display an interop icon for an Interop meeting.

---

## Live Desks

### Live Desk Role

When a person designated as Live Desk logs into CTS-Manager, the following selections and information are available:

- System Status
- Monitor
- Support
- Troubleshooting

The Live Desk is the first person contacted when there are questions or problems pertaining to connecting meeting participants. The Live Desk understands how to perform the following tasks:

- Scheduling meetings
- Using the Cisco IP phone in a Cisco TelePresence-enabled meeting room
- Using the tools supplied by the CTS-Manager to monitor the system and the schedule of upcoming meetings and to update meeting requests
- Gathering data to supply to the administrator when a problem cannot be easily solved

Live Desk personnel can be assigned rooms to monitor in the CTS-Manager application. Assigned Live Desks are easily reached by dialing the Live Desks soft key on the Cisco IP phone in a Cisco TelePresence-enabled meeting room.

The Live Desks window has two areas, a list of Live Desks and a list of rooms that need a Live Desk assigned to them. Use the areas in this window to assign a Live Desk to a meeting room.

A phone number is associated with the Live Desk, which is displayed on the Cisco TelePresence meeting room phone user interface when the Live Desk soft key is pressed. Meeting participants can dial the Live Desk and ask for help when problems occur with the Cisco TelePresence system.

**Figure 10-37** *Configure > Live Desks Window*

**Live Desks**

	ID	Phone Number	Description
<input checked="" type="radio"/>	2222 (Default)	4457878	test
<input type="radio"/>	<Unassigned>		System installed

**Rooms assigned to concierge '2222':**

Showing 1-2 of 2  per page

<input type="checkbox"/>	Status ▾	Room Name ▾	Room Phone	Description	IP Address
<input type="checkbox"/>	Error	Room18	16200	Room 18	192.168.33.17
<input type="checkbox"/>	Error	Room23	16199	Room 23	192.168.33.18

☐ Assign selected rooms to:     Page  of 1

## Creating Live Desk Personnel

To add a new person as a Live Desk, from this window, perform the following steps. The limit for the number of assigned Live Desk assignments is 10. The recommended range for the number of Live Desk assignments is 1 - 10.

**Note**

CTS-Manager supports 10 Live Desk concurrent login under steady State conditions. As more users login concurrently, the system performance will begin to degrade. Download of logs is recommended to be done with one user at a time. If the system is under maintenance or under high usage, these parameters will change.

- 
- Step 1** Click **New** to display the new Live Desks window.
- Step 2** In the New Live Desks window, enter an identifier for the Live Desk in the ID field
- Step 3** Enter a phone number in the Phone Number field.
- Step 4** You can choose to supply other information identifying the Live Desk person in the Description field.
- 

**Caution**

When putting information in the Live Desk Description Field do not use a Carriage Return or line feed, sometimes referred to as <CR> between words (do not hit return key).

**Figure 10-38 Adding a Live Desk Window**

All Cisco TelePresence rooms must be assigned to a Live Desk. If you haven't specified a Live Desk for a room, the System installed <Unassigned> Live Desk is the default Live Desk for all rooms discovered in CTS-Manager.

You can change the default Live Desk to a specific Live Desk by checking the Set as Default checkbox in the Live Desk details window. Any Cisco TelePresence room discovered by CTS-Manager will be assigned to the new default Live Desk. Each time you specify a different Live Desk as the default, all future rooms discovered by CTS-Manager will be assigned to the new default setting.

## Assigning a Room to a Specific Live Desk

Once Live Desks have been registered, the next step is to assign them meeting rooms:

- 
- Step 1** Check the box next to a room that has not been assigned.

- Step 2** Select a Live Desk from the **Assign Selected Rooms** drop-down list.
- Step 3** Click **Apply**.  
To edit the Live Desk assignment:
- Step 4** Select the radio button next to the Live Desk ID and click **Edit**.
- Step 5** In the Edit Live Desks window, you can change the phone number and other information identifying the Live Desk.
- Step 6** To delete a Live Desk, select the radio button next to the Live Desk ID and click **Delete**.

**Note**

CTS-Manager 1.7 supports a default Live Desk that is assigned to TelePresence rooms that have no specific Live Desk assignment. Earlier versions of CTS-Manager allowed more than one Live Desk to have the same phone number. If you are upgrading to version 1.7 from an earlier version that allows a Live Desk to share a phone number with another Live Desk, CTS-Manager 1.7 changes the phone number of one of the Live Desks during the upgrade and assigns that Live Desk to the TelePresence room.

## Policies

The Policies window lists the two available default policies that support scheduling and conference termination in CTS-Manager.

To edit a policy:

- Step 1** Select the radio button next to the policy you want to edit and click **Edit**.
- Step 2** Make changes to the policy and click **Save**.

**Figure 10-39** *Configure > Policies Window*

**Policy Management**

Showing 1-2 of 2 10 per page Go

	Policy Name ▾	Policy Type	Policy Description
<input type="radio"/>	CTMS	Default	This is the Default CTMS Policy
<input type="radio"/>	CTS	Default	This is the Default CTS Policy

New... Edit... Delete

Page 1 of 1

## CTMS policy

Describes the switching policy for multipoint meetings. The switching mode can be set to either Speaker or Room switching. You also use the policy management window to set the number of scheduled meetings pushed to CTMS devices. The default is to push 14 days of meetings, the range is 1 to 30 max.

**Figure 10-40** CTMS Policy Window

Edit...Policy Management	
⚙ = Required fields	
Name:	Default
Type:	CTMS
⚙ Description:	<input type="text" value="This is the Default CTMS Policy"/>
Switching Mode:	<input type="text" value="Speaker"/>
Number of days pushed to CTMS:	<input type="text" value="14"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

## CTS policy

Determines the number of days of scheduled meetings pushed to each TelePresence room. The default is 14 days, the range is from 1 to 30 max.

**Figure 10-41** CTS Policy Window

Edit...Policy Management	
⚙ = Required fields	
Name:	Default
Type:	CTS
⚙ Description:	<input type="text" value="This is the Default CTS Policy"/>
Number of days pushed to phone:	<input type="text" value="14"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

## Application Settings

The Configure > Applications Settings window is used to configure a variety of TelePresence meeting settings. It is organized into the following tabs:

- Email
- Bridges and Servers
- Usage Survey
- Meeting Options

## Email

In the Email tab you configure a variety of CTS-Manager email settings, including notification email settings and email prefixes settings.

**Figure 10-42** *Configure > Application Settings > Email Window*

**Application Settings**

Email Bridges and Servers Usage Survey Meeting Options

**Meeting Notification Email**

Enable Feature: ☒ Yes ☐ No

Enable Organizer Email: ☒ Yes ☐ No

Remove Meeting Link from Email: ☐ Yes ☒ No

Copy Outgoing Email To:

A copy of each email from Cisco TelePresence Manager will be sent to this address. Only one email address is allowed.

Text to Be Displayed in Email:

URL to Be Displayed in Email:

**Remove Email Prefixes from Meeting Subject on Phone**

Enable Feature: ☐ Yes ☒ No

FW:, RE:, Updated: will be removed from the meeting subject displayed on the TelePresence Phone

Apply Cancel

## Meeting Notification Email

**Enable Feature:** The default setting for Meeting Notification Email is “Yes.” If you change this setting to “No” you disable email notifications and Confirmation emails and Action Required emails are not sent to meeting organizers.



### Note

On a new install, email would be set to default, “Yes.” On a software upgrade, the email would be set to default, “Yes.” Optional FTS restores email option from preserved backup file.

**Enable Organizer Email:** This option shuts off or turns on the email to be sent to the meeting organizer.

**Remove Meeting Link from Email:** This removes or adds the meeting link to the email sent out from the CTS-Manager.

**Copy Outgoing Email To:** CTS-Manager will accept any email address as long as it matches the Exchange domain and/or any of the LDAP domains configured on CTS-Manager. Mail notifications will be sent to the Exchange server configured on CTS-Manager and it is up to this server to route the emails as configured. You can also specify an additional email address. All emails generated by Cisco TelePresence Manager will be sent to this address.

A secondary email address specified for IBM Domino installations is included in the BCC field when emails are generated.

A secondary email address specified for Microsoft Exchange installations is included in the CC field when emails are generated.

**Text to Be Displayed in Email:** Enter the text you want to appear in the email message header. Text can be up to 4096 characters in length.

**URL to Be Displayed in Email:** Enter the URL you want to appear in the email message header.

## System Alert Notification Emails

In addition to meeting confirmation and action required emails, system alert emails are sent to the address specified in the Copy Outgoing Email To field in certain situations. There are three different emails that contain the following information:

### No-Show Meetings and Meetings without Survey Responses

- Organizers of No-Show Meetings: Meetings that were scheduled but never took place.
- Meetings without Usage Survey Responses: Organizers of meetings for which surveys were not filled out.

### Mailbox Alert

- The CTS-Manager mailbox exceeded its size limit and is no longer able to send emails to meeting organizers.

### Certificate Expiry

- Security certificates that are about to expire.

For more information about System Alert Notifications, see [System Alert Notifications](#).

## Remove Email Prefixes from Meeting Subject on Phone

Select either **Yes** to remove the email prefixes, such as FW, RE or **NO** to keep the prefixes included in the meeting subject. When sorting by subject, this helps narrow down the meeting list.

## Bridges and Servers

In the Bridges and Servers tab, you configure Studio Mode Recording, WebEx, Interoperability with Video Conferencing and Intercompany features.

Figure 10-43 Configure &gt; Application Settings &gt; Bridges and Servers Window

**Application Settings**

Email Bridges and Servers Usage Survey Meeting Options

**Studio Mode Recording**  
 Enable Feature: ☒ Yes ☐ No  
 Studio Mode is enabled.  
 Once this feature is enabled, it cannot be disabled.

---

**WebEx**  
 Enable Feature: ☒ Yes ☐ No  
 Default User Type: ☒ Permitted ☐ Non-Permitted  
 This feature allows you to specify the default WebEx permission for new users.  
 New Users are assigned to one of the following WebEx user types by default  
 1. Permitted - Users are permitted to request WebEx for specific meetings  
 2. Not-Permitted - Users are not permitted to request WebEx

---

**Interoperability with Video Conferencing**  
 Enable Feature: ☒ Yes ☐ No  
 Once this feature is enabled, it cannot be disabled..  
 Interop Quality: ☐ CUVC-CIF ☒ CUVC-720p ☐ MXE-HD

---

**Intercompany**  
 Enable Feature: ☒ Yes ☐ No  
 Once this feature is enabled, it cannot be disabled.  
 Provider: ☒ Another Company Hosts ☒ Our Company Hosts

Apply Cancel

## Studio Mode Recording

The default setting for Studio Mode Recording is “No.” If recording is desired, select the “Yes” setting. This option allows the administrator to enable the studio mode recording support. Once this option is enabled, the user can enable this recording for a meeting from the meeting details view. The studio mode recording is mutually exclusive from Intercompany and Interop operation.



### Note

Interop and Intercompany meetings cannot be made as a studio mode recording meeting.

### Enabling recording globally

If a single meeting is set up and recording is enabled for the meeting, then if that meeting is modified as a recurring meeting all instances of that meeting will have recording enabled.

To enable recording globally:

- 
- Step 1** Schedule a single meeting with one room.
  - Step 2** From the Application setting, set Studio Mode Recording to Yes.
  - Step 3** From Microsoft Outlook or Lotus Notes, select this meeting and modify it as a recurring meeting.
  - Step 4** All instances now have recording enabled on them.
- 

## WebEx

This allows a meeting organizer or participant to start a simultaneous WebEx and Telepresence meeting with the simple push of a button on the Cisco IP phone.

**Enable Feature:** This allows you to enable WebEx. It is disabled by default.

**Default User Type:** This allows you to specify the default WebEx permissions which meeting organizers have for scheduling TelePresence meetings with WebEx enabled. There are two default options:

- Permitted WebEx User: can request WebEx for specific meetings they schedule
- Non-Permitted WebEx User: is not permitted to request WebEx.



### Note

For WebEx to work, all CTS endpoints and CTMS devices initially installed must have 1.7 software. If you install devices later that have software version 1.6 or earlier they will not be compatible with WebEx.

For the complete details on how to configure WebEx for the Cisco TelePresence System, including CTS-Manager, refer to the “Cisco WebEx OneTouch Configuration Guide for the Cisco TelePresence System” at the following URL:

[http://www.cisco.com/en/US/docs/telepresence/cts\\_admin/webex\\_solutions/guide/cts\\_webex\\_config.html](http://www.cisco.com/en/US/docs/telepresence/cts_admin/webex_solutions/guide/cts_webex_config.html)



### Note

A meeting cannot use both Interoperability with Video Conferencing with MXE-HD and WebEx OneTouch. If both are enabled, WebEx takes precedence and Interoperability with Video Conferencing is disabled.

## Interoperability with Video Conferencing

**Enable Feature:** The default setting for interoperability with video conferencing is “Disabled.” This feature cannot be disabled once it has been enabled.

If the setting is grayed out, and cannot be changed to “Yes” there is at least one CTS endpoint or bridge or server device that is not interop-ready. All endpoints and CTMS devices must support interop before you can enable Interop settings. Make sure all devices discovered by CTS-Manager are running interop-enabled software releases.

If Interoperability with Video Conferencing has been set to “Yes” and is grayed out so that you can’t disable it, the CUVC added through the Bridges and Servers window is included in at least one scheduled meeting. In order to disable interop services you must, from the Bridges and Servers window, first deallocate the CUVC and then delete it.

**Note**

When Interoperability with Video Conferencing is enabled, multipoint meetings require a CTMS and an MXE in a scheduled state.

**Interop Quality:** This allows you to select the correct resolution setting on a global basis. For all future meetings, CTS-Manager updates affected CTMS with the new resolution by pushing updated conference schedules.

Select “CIF” for SD Interop support. If this is selected, the Admin UI provides an option to add one CUVC at CIF. Only one CUVC is allowed.

Select “720p” or “MXE-HD” for HD Interop support. If “720p” is selected, the Admin UI provides an option to add one CUVC at 720p. Only one CUVC is allowed.

**Note**

To enable HD Interop, all endpoints must be running software version 1.6 or later.

The resolution type selection will be maintained by CTS-Manager and pushed to the CTMS on a per meeting basis.

Once HD Interop is configured at CTS-Manager, even if SD VC end points are joining through CUVC 7.0, CTS-Manager always reserves HD Interop resources.

**Note**

When upgrading from 1.6 to 1.7, either CUVC-CIF or CUVC-720p will be selected according to what was selected in 1.6.

## Intercompany

Enabling Intercompany allows you to schedule multipoint meetings between two different organizations. Once you enable the Intercompany feature it cannot be disabled.

**Note**

An Intercompany TelePresence meeting cannot be configured for Interop. If you enable Intercompany, you cannot add video conferencing (VC) rooms to your meeting.

The Provider setting allows you to select either “Another Company Hosts” or “Our Company Hosts.” You cannot select both. These options can be changed depending on whether the company is going to host meeting or be hosted. If multiple occurring meetings are set up with the company being host, this company will be the host for all the meetings.

### Another Company Hosts

If you select this feature, this allows another company to set up TelePresence meetings. You must provide the host with the rooms’ information that will be participating in the TelePresence calls. For example, if it is a room to a room call it still be a single (1) room. If it is a multi-room call, then, for example, a triple call would be 3.

### Our Company Hosts

If your company is hosting the meeting, the person setting up the meetings needs to reserve the rooms, and get dial-in and room information from the other company before setting up the TelePresence meeting.

## Usage Survey

The Usage Survey window provides your company the ability to form financial justifications for your deployment of Cisco TelePresence solutions. This feature allows the administrator to measure TelePresence usage, room utilization, ROI of TelePresence deployment, compute savings from travel elimination, and display meaningful data.

**Figure 10-44** *Configure > Application Settings > Usage Survey Window*

**Application Settings**

Email Bridges and Servers **Usage Survey** Meeting Options

**Enable Meeting Organizer Usage Survey and Benefits Report**

☒ Yes ☐ No

**Meeting Benefits Report Parameters**

⚙ = Required fields

⚙ Work Hours per Day:	<input type="text" value="10"/>	⚙ Trips Eliminated per Meeting:	<input type="text" value="6"/>
⚙ Work Days per Week:	<input type="text" value="5"/>	⚙ Travel Hours per Trip:	<input type="text" value="8"/>
⚙ Carbon Emissions per Trip (Tons):	<input type="text" value="0.18"/>	⚙ Cost per Trip (\$):	<input type="text" value="2200.0"/>
⚙ Employee Hourly Cost (\$):	<input type="text" value="93.75"/>		

**Survey Questions**

1. What is the purpose of this meeting?

2. What is the primary benefit of using Cisco TelePresence?

3. How many trips eliminated?

### Enable Meeting Organizer Usage Survey and Benefits Report

This feature provides basic information on room utilization, meeting benefits and survey results. It requires the Metrics Dashboard and Reporting API license.

To enable the usage survey and benefits report:

- Select the **Yes** radio button.



#### Note

“No” is selected by default which means the meeting organizer will not be able to fill out the survey or access the Monitor > Metrics Dashboard, Meeting Benefits or room utilization windows.

## Meeting Benefits Report Parameters

The Meeting Benefits Report Parameters are your company's benchmark numbers to apply to all TelePresence meetings to demonstrate how TelePresence meetings can help save your company money.

To set Meeting Benefits Parameters

- Enter the parameters appropriate for your company.



### Note

The above features are not available in the Usage Survey tab if the Metrics Dashboard and Reporting API license is not uploaded. To upload the Metrics Dashboard and Reporting API license, go to the **Configure > Licenses** window, click the **License Files** tab and click **Upload**.

## Survey Questions

You can create a survey based upon the information your company wants to gather.

After the meeting organizer receives the confirmation email for the scheduled meeting, they can answer the survey at any time, even after the meeting has ended.

Three survey questions and answers are included by default:

- [Purpose](#)
- [Benefit](#)
- [Trips](#)

### Purpose

This question captures the main purpose of the meeting.

#### Question:

- What is the purpose of this meeting?

#### Answers:

- Customer/Partner Demo
- Executive Meeting
- Executives and Customers
- Friends & Family
- Internal

### Benefit

This question captures the primary benefits of the meeting.

#### Question:

- What is the primary benefit of using Cisco TelePresence?

#### Answers:

- Avoid Travel
- Accelerate Time to Market
- Address Customer Issues

- Allow Business Continuity/Mitigate Crisis
- Connect Customers to Company Leaders
- Demonstrate Product to Customer
- Increase Employee Productivity

## Trips

This question captures the number of business trips eliminated by the meeting.

### Question:

- How many trips eliminated?

### Answer:

- *User enters a number*



#### Note

Results from Trips question are gathered through the reporting API and are not displayed on the Metrics Dashboard. This provides you with the ability to track how many trips are actually eliminated per meeting, which you can use as the basis for setting the Trips Eliminated per Meeting value in the **Configure > Application Settings > Usage Survey** window.

These questions and their possible responses are shown. These questions can be modified but not deleted.

You can add more questions, click the **Customize** button.

The Survey Customization Wizard opens.



#### Note

You can have up to ten questions. To collect the answers from additional questions, use the Reporting API.

When you are finished making changes in the Usage Survey window, click **Apply** to save your changes.



#### Note

You can modify any questions at any time. If you modify the possible answers for either of the first two questions, the previous answers will be visible on the Meeting Details page only if you select a time range before the modification; otherwise they will be blank.



#### Note

The above features are not available in the Usage Survey tab if the Metrics Dashboard and Reporting API license is not uploaded. To upload the Metrics Dashboard and Reporting API license, go to the **Configure > Licenses** window, click the **License Files** tab and click **Upload**.

## Survey Customization Wizard

The survey customization wizard guides you through the steps required to customize the usage survey. The first three questions are included by default, and you can add up to seven more.

**Figure 10-45** Usage Survey Customization Wizard

**Welcome to the Usage Survey Customization Wizard**

This wizard guides you through the steps required to customize your survey.

The first three questions gather data that will be displayed on the Metrics Dashboard. You can modify these questions but not delete them.

You can have up to ten questions. Use the provided API to collect the data from the additional questions. See Help for more details.

You can change any questions at any time. If you modify the choices for either of the first two questions, those modified choices will be displayed as new choices in the Metrics Dashboard.

**Delete**

1: What is the purpose of this meeting?

2: What is the primary benefit of using Cisco TelePresence?

3: How many trips eliminated?

How many total questions do you want? 4

Next Cancel

### Cannot Delete Questions 1 - 3

Questions 1 - 3 can be modified but not deleted. These responses appear on the Metrics Dashboard, after the meeting organizer fills out the survey for each meeting they schedule.

To add more questions to the survey, select the number of total questions that you want, the range is 1 to 10 (total 10 including the 3 default ones), with the default of 3.

Click **Next** to enter the data and go to the next window.

**Figure 10-46** Customize Your Purpose Question

You can customize this question or click Next to go to the next question.

To customize this question, do the following:

- 
- Step 1** In the Question field, change the default question, if you wish.
  - Step 2** (Optional) Click the checkbox for Include an “Other” option if you want to include a text box in the survey for the meeting organizer to enter text as an answer.
  - Step 3** Make any necessary changes to the answers and add any new ones if you need to.
  - Step 4** Click **Next**.
  - Step 5** Review and modify, if necessary, the next two default questions and their answers.
- 

**Note**

When customizing the Benefit question, you cannot modify the Avoid Travel answer because it is used to calculate reporting data in the Meeting Benefits section of the Metrics Dashboard. For more information, see [Meeting Benefits, page 12-16](#).

Figure 10-47 Customize Your Question

**Customize Your Question 4**

⚙ = Required fields

⚙ Question:

Response Type:  ▾

☐ Include an "Other" option with a free-form text entry

⚙ #1:

⚙ #2:

#3:

#4:

#5:

#6:

#7:

#8:

#9:

#10:

To create a new question, do the following:

- 
- Step 1** In the Question field, enter a question.
  - Step 2** From the Response Type drop-down menu, select a response type.
  - Step 3** (Optional) Click the checkbox for Include an "Other" option if you want to include a text box in the survey for the meeting organizer to enter text as an answer.
  - Step 4** Enter the possible responses for the question (up to ten).
  - Step 5** Click **Next**.
  - Step 6** Create additional new questions by following steps 1 through 5.
-

## Preview Your Questions

This window appears after you finish customizing all of your questions to show you your survey the way the meeting organizer will see it when they fill it out.

**Figure 10-48** *Preview Your Survey Questions Window*

**Preview Your Questions**

1. What is the purpose of this meeting?
2. What is the primary benefit of using Cisco TelePresence?
3. How many trips eliminated?
4. what is the meaning of life?

If you want to make changes to any of the questions, click **Back** until you reach the question you want to change and then click **Next** to get back to this window. When you are finished click **Finish**.

## Meeting Options

The Meeting Options tab on the Application Settings page contains the options to configure tentative room reservations, starting meetings early and the meeting extension settings.

[Figure 10-49](#) illustrates the default settings when the application is first installed.

The settings corresponding to a radio button selection are disabled unless the radio button is selected.

Figure 10-49 Configure &gt; Application Settings &gt; Meeting Options Window

**Application Settings**

Email Bridges and Servers Usage Survey **Meeting Options**

**Start Meetings Early**

☐ Do not allow meetings to start before the scheduled time

☒ Allow Meetings to start early, by (minutes): 10

---

**Extend Meetings**

☐ Do not end meetings until they are ended by the participants

☐ End meetings after the scheduled end time by (minutes) 0

☐ Allow all meeting organizers to extend meetings up to (minutes): 30

☐ Always extend ☒ Extend, if resources are available

☒ Allow these meeting organizers to extend meetings

Meeting Extension Premium Users (minutes): 60

As of Wed, 18 Aug 2010 18:54:14 +0000 there were 3 Meeting Extension Premium Users [Details..](#)

If resources are available all other meeting organizers can extend by (minutes): 30

Apply Cancel

## Enable Tentative Room Reservations

Enabling this feature allows CTS-Manager to process meetings for tentative room reservations for TelePresence rooms. Tentative room reservations are enabled on a per room basis. After enabling tentative room reservations, you must select the individual rooms you want to accept tentative room reservations by going to the **Support > TelePresence Rooms > Capability** window.



### Note

Upgrading from CTS-Manager 1.6 to 1.7: If you had tentative room reservations enabled in 1.6, this setting is maintained when upgrading to 1.7, but you must re-enable tentative reservations on each room individually in the **Support > TelePresence Rooms > Capability** window.



### Note

This option is supported only with Microsoft Exchange.

A tentative room reservation is a meeting invitation that has been viewed by the room owner or a proxy room owner, but not accepted yet. A room owner refers to a person who has a TelePresence system in their office or personal conference room, rather than a TelePresence system located in a regular conference room which has no owner. A proxy room owner is a person who is assigned the proper privileges by the room owner to reserve their room for meetings. A CTS-Manager tentative reservation is identical to an accepted reservation.

**Caution**

Once Enable Tentative Room Reservations is turned on, you cannot turn it off without reinstalling CTS-Manager.

This feature is set to “No” by default. The administrator must turn this feature on globally to incorporate all rooms hosted by CTS-Manager.

**Note**

A meeting participant must read the meeting invitation for it to appear on the phone UI. If a scheduled meeting is updated and the meeting invitation has not been read yet, the phone UI will not be updated. In this case, the room or proxy mode room calendar may show double bookings.

Once all room reservations are confirmed, the meeting appears in the Scheduled Meetings window and the phone UI within five minutes. If email alerts are turned on, confirmation or error emails are generated and sent within approximately 10-15 minutes.

Cisco recommends enabling tentative room reservations for private (office) rooms so if the scheduled meetings aren't in sync the result is ok.

## Start Meetings Early

This feature allows you to set a policy for starting meetings early.

You have two options:

**Do not allow meetings to start before the scheduled time:** Prohibits all meetings from starting before the scheduled time.

**Allow meetings to start early, by (minutes):** Allows meetings to start before the scheduled start time.

## Extend Meetings

This feature allows you to set a policy for extending multipoint meetings beyond the scheduled end time.

**Note**

This feature is not compatible with single-room or point-to-point meetings.

## Prerequisites

The following are required to enable the Extend Meetings feature:

- At least one CTMS version 1.7 or later.
- TelePresence endpoints must be version 1.7 or later.
- CTS-Manager 1.7 or later.
- All TelePresence endpoints must have a Connectivity status of OK.

To check the status of TelePresence endpoints, go to **Support > TelePresence Rooms** and click the **Status** tab.

- Default first option **Do not end meetings until they are ended by the participants** should be selected.

**Note**

Before setting this feature, make sure that the CTMS has sufficient capacity to support these extended schedules. If not, then additional CTMS resources need to be deployed.

Select one of the following meeting options, described below:

- **Do not end meetings until they are ended by the participants** - This option allows all meeting participants to be able to extend in-progress meetings. (This is the default setting).
- **End meetings after the scheduled end time (minutes)** - This option forces each meeting to end after the designated extended time. If you upgraded from the previous version of CTS-Manager, then the setting time appears in this field.
- **Allow all meeting organizers to extend meetings up to (minutes)** - Select either 30 or 60 (30 default) for every meeting.
  - **Always Extend** - Automatically extends every meeting.
  - **Extend, if resources are available** - Only extends the meeting if the necessary resources are available.
- **Allow these meeting organizers to extend meetings** - This allows the meeting that is in progress to continue after the scheduled end time. The two selections are:
  - **Meeting Extension Premium Users (minutes)** - select either 30 or 60 (60 default).  
 The following message appears after clicking the radio button to select this option and clicking **Apply**:  
*As of (date and time) there were X meeting Extension Premium Users [Details](#)*
  - **If resources are available all other meeting organizers can extend by (minutes)** - select either 0, 30 or 60 minutes. If you set this option to 0, only Meeting Extension Premium Users are able to extend meetings.

**Note**

When changing the Extend Meetings setting from allowing Meeting Extension Premium users to extend meetings to allowing all meeting organizers to extend meetings if resources are available, some meetings that immediately follow a meeting scheduled by a Meeting Extension Premium user, may be in an error state even if there are enough resources for them to take place. These errors will be corrected during the next CTS-Manager maintenance cycle. To avoid this potential situation, Cisco suggests making this change shortly before the maintenance cycle, so that if it does occur, it will be corrected as soon as possible.

Before enabling this option, you must do the following:

1. In LDAP create a group for the premium users you want to use this feature and the users to that group.
2. Disable meeting notification emails by going to: **Configure > Application Settings > Email**. In the Meeting Notification Email section, next to Enable Feature select **No** and click **Apply**.
3. Go to **Configure > Access Management** and add the LDAP group you created in step 1 to the Meeting Extension Premium User role.
4. Go to **Configure > Application Settings > Meeting Options**. In the Extend Meetings section, make sure the number of users in the Meeting Extension Premium User group is correct in the following section “As of <Current date and time> there were <total number of users in a premium group> Meeting Extension Premium Users Details.”

5. Select **Allow these meeting organizers to extend meetings** and configure its options, as described above.

After enabling the Click the **Apply** button if you change any of these settings. If any of the settings are changed from the default settings, a confirmation message appears informing you of the number of scheduled meetings that will need to be revalidated. After the revalidation is finished, click **OK** to close the message and save the changes. Click **Cancel** to close the message without saving the changes.

**Caution**

Changing meeting extension settings will require all scheduled meetings to be revalidated by CTS-Manager. The validation process can take from a few minutes to a few hours. You cannot make another change to your meeting extension settings until revalidation is complete. During this time, meeting confirmations may take longer than usual. It is recommended to make changes during off-peak hours.

### Displaying Meeting Extension Information in Meeting Details Window

The Administrator and Live Desk users are able to view the meeting extension information in the Meeting Details window. Meeting organizers are not able to see the settings in the Meeting Details window.

## Important Information About Resource Allocation

Depending on which meeting options you select, the resources are allocated differently:

- Start Meetings Early and Extend Meetings depend entirely on the available schedulable segments. CTMS resources are required and not guaranteed.
- Static meetings and scheduled meetings only utilize available ad hoc segments when the Extend Meetings feature's 3rd and 4th options are selected with "if resources are available".
- If the Extend Meetings feature's 3rd and 4th options are selected, scheduled meetings utilize schedulable segments.
- If the Extend Meetings feature's 3rd and 4th options are selected with "if resources are available, scheduled and static meetings utilize only available ad hoc segments.
- Back-to-back meetings:
  - If "Do not end meetings until they are ended by the participants" is selected and the first meeting uses all schedulable segments and a user starts the second meeting on time or early, the second meeting will start successfully from the phone, but the video will not be available and the following message will be displayed: "Please wait, temporarily at maximum number of callers." The video for the second meeting will start after the first meeting ends and release its resources.
  - If "End meetings after the scheduled end time by (minutes)" is selected and the first meeting uses all schedulable segments and a user starts the second meeting early, the second meeting will start successfully from the phone, but the video will not be available and the following message will be displayed: "Please wait, temporarily at maximum number of callers." The video for the second meeting will start after the first meeting reaches its scheduled end time.
- If "Do not end meetings until they are ended by the participants" is selected and the meeting continues beyond the scheduled end time and the schedulable segments are not enough to continue the meeting, then the meeting takes resources from Ad hoc segments.

# CTS-Manager Redundancy Failover Procedure

The Cisco TelePresence Manager configuration for a redundant system is to have a primary and a backup CTS-Manager system with a mirror configuration.

**Note**

If a redundant system is configured, make sure database backups are performed regularly.

## Cold Standby

In a redundant system, the primary CTS-Manager is active and the backup is powered off.

When a CTS-Manager primary system stops working, meetings scheduled during this down-time will not be pushed to the phone. Meetings can still be scheduled in the Exchange or Domino during the downtime and all meetings “one button to push” on the phone will not be affected. Once the backup CTS-Manager is online, meetings scheduled during the primary down-time will be processed and pushed to the phones.

**Note**

It is recommended to use the same hostname and the same IP address for CTS-Manager replacement server.

### CTS-Manager Failover Procedure

When the primary CTS-Manager fails, perform the following procedure:

- 
- Step 1** To start the failover procedure, power off the primary CTS-Manager system.
  - Step 2** Power on the backup CTS-Manager system.
  - Step 3** Restore the last CTS-Manager database to the backup CTS-Manager by clicking **Available Backups**, selecting an available backup file and clicking **Restore Now**.

**Figure 10-50** *Configure > Database > Restore Window*

**Database**

Settings Backup **Restore**

✱ = Required fields

Restore Type: ☒ Local ☐ Network

Restore Mode: ☒ Sftp ☐ Ftp

Remote Storage Host:

Port:

Username:

Password:

Storage Path:

Showing 1-1 of 1 10 per page

	Time (+) ▾	Status	Type	Hostname	Location
<input type="radio"/>	05/25/2010 06:07 PM	OK	Local		/common/dbbackup/CTMbackup.fileter.1.7

- Step 4** Next, perform a resync with the Microsoft Exchange or IBM Domino database from the backup CTS-Manager.

Figure 10-51 System Configuration - Microsoft Exchange Resync Window

**Microsoft Exchange**

Service Status: **OK**

✱ = Required fields

Mailbox Usage: 0.17% full (3497.0 of 2097151.0 KB is used)

✱ Host:

Bind Method: ☐ Secure ☒ Normal

✱ Port:

✱ Domain Name:

Logon Name:

✱ SMTP LHS:

✱ Password:

Certificate:

---

**Synchronization Operations**

Subscription Status:  Room Name:

Showing 1-7 of 7 10 per page

<input type="checkbox"/>	Room Name	Last Synchronization Time (+)	Subscription Status	Assigned Node
<input type="checkbox"/>	ROOM2	✓ 06/01/2010 06:00 PM	Success	bw-30
<input type="checkbox"/>		✗ Never synchronized	Error	bw-30
<input checked="" type="checkbox"/>	ROOM4	✓ 06/01/2010 06:00 PM	Success	bw-30
<input checked="" type="checkbox"/>	ROOM6	✓ 06/01/2010 06:00 PM	Success	bw-30
<input checked="" type="checkbox"/>	ROOM5	✓ 06/01/2010 06:00 PM	Success	bw-30
<input type="checkbox"/>	ROOM3	✓ 06/01/2010 06:00 PM	Success	bw-30
<input type="checkbox"/>	ROOM1	✓ 06/01/2010 06:00 PM	Success	bw-30

Page 1 of 1

**Step 5** Review the information to make sure it is correct, make any changes needed and click **Resync**.



**Note**

This Resync in Microsoft Exchange must be verified in on the Exchange server.

## Warm Standby

### CTMS Warm Standby for Scheduled Meetings

Both the primary and backup CTMS systems are configured independently with different call-in numbers, etc.

Each CTMS is configured in the CTS-Manager. Both primary and backup CTMS are powered on and connected to the network at all times. The meetings will only be scheduled on and serviced by the primary CTMS.

## CTS-Manager Redundancy Failover Procedure

With a redundant CTS-Manager system, make sure to configure two CTMS devices and register the primary with CTS-Manager in “Scheduled” mode and the backup in “Non-Scheduled” mode.



#### Note

Both CTMS are active, but meetings are to be scheduled on the primary “Scheduled” CTMS

When the primary CTS-Manager fails, perform the following procedure:

- Step 1** To start the failover procedure process, power off the primary CTS-Manager.
- Step 2** Power on the backup CTS-Manager.
- Step 3** Restore the last CTS-Manager database to the backup CTMS by clicking **Available Backups**, selecting an available backup file and clicking **Restore Now**.



#### Note

During a primary CTMS failure, all multipoint meetings in progress will be disconnected and no new meetings will be allowed to start. Migrating all meetings is only allowed to a non-scheduled CTMS.

**Figure 10-52** *Configure > Database > Restore Window*

**Database**

Settings Backup **Restore**

✱ = Required fields

Restore Type: ☒ Local ☐ Network

Restore Mode: ☒ Sftp ☐ Ftp

Remote Storage Host:

Port:

Username:

Password:

Storage Path:

**Available Backups** **Verify Remote Host**

## CTMS Redundancy Failover Procedure

- 
- Step 1** When the primary CTMS fails, log into CTS-Manager and migrate all scheduled meeting to the backup “non-scheduled” CTMS.
- Step 2** Change the Control State of primary CTMS to **Non-scheduled**
- Step 3** Change the Control State of the backup CTMS to **Scheduled**.
- 

**Figure 10-53** *Configure > Bridges and Servers Edit Window*

Edit...Bridge or Server	
* = Required fields	
Hostname:	example-ctms-4
* Username:	admin
* Password:	••••••••
Control State:	<input checked="" type="radio"/> Scheduled <input type="radio"/> Non-Scheduled
Timezone:	America/Los_Angeles
Call-In Numbers:	12001
Segment Count:	24
<input type="button" value="Save"/> <input type="button" value="Close"/>	

All scheduled multipoint meetings are moved to the backup CTS-Manager and “One Button to Push” entries are updated with the new CTMS call-in number and meeting number. The time it takes to update all meeting entries and update all phones will vary depending on the number of meetings and CTS endpoints.