

CHAPTER 11ex

ten

Additional Installation Configurations for Cisco TelePresence Manager

First Published: May 29, 2012, OL-22226-02

Contents

- [Post-Install Guidelines for CTS-Manager, page 11-2](#)
- [Introduction to the CTS-Manager Administration Software, page 11-3](#)
- [Licensing for CTS-Manager, page 11-6](#)
- [Security, page 11-13](#)
- [LDAP Server, page 11-14](#)
- [Field Mappings, page 11-15](#)
- [Calendar Server, page 11-25](#)
- [Microsoft Exchange, page 11-29](#)
 - [Synchronization Operations, page 11-30](#)
- [IBM Domino, page 11-35](#)
- [Access Management, page 11-73](#)
- [Alert Management, page 11-77](#)
- [Application Settings, page 11-93](#)
 - [Meeting Notification Email, page 11-94](#)
 - [WebEx, page 11-98](#)
 - [Multipoint Conference Scheduling, page 11-96](#)
 - [Interoperability with Video Conferencing, page 11-97](#)
 - [TelePresence Call-In Number, page 11-98](#)
 - [Studio Mode Recording, page 11-98](#)
 - [CTMS Network Multipoint, page 11-99](#)

- Intergroup Scheduling, page 11-99
 - Intercompany, page 11-100
 - Usage Survey, page 11-103
 - Start Meetings Early, page 11-114
 - Extend Multipoint Meetings, page 11-114
- Bridges and Servers, page 11-58
 - Cisco TelePresence Multipoint Switch (CTMS), page 11-63
 - Cisco TelePresence Server (TS), page 11-65
 - Cisco TelePresence Recording Server (CTRS), page 11-67
 - Cisco TelePresence Recording Server (CTRS), page 11-67
 - WebEx, page 11-68
 - WebEx, page 11-68
 - Collaboration Manager, page 11-72
- Cluster Management, page 11-73
- Database - Status, Backup, and Restore, page 11-48
 - Settings, page 11-48
 - Changing the Backup Schedule, page 11-50
 - Backing Up CTS-Manager Data, page 11-51
 - Viewing Backup History, page 11-52
 - Restoring Backup Data, page 11-53
- Device Groups, page 11-78
- Endpoints, page 11-81
- Live Desks, page 11-88
- Policies, page 11-91
- Unified CM, page 11-54
- System Settings, page 11-38
- CTS-Manager Redundancy Failover Procedure, page 11-117

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 11-1 *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.
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.	Chapter 12, “Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager”
Monitoring and Supporting CTS-Manager	Describes the support features available when you log into CTS-Manager using a Live Desk role.	Chapter 13, “Monitoring and Supporting Cisco TelePresence Manager”

If at any time you encounter problems, go to [Chapter 16, “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 11-3](#)
- [SysAdmin Role, page 11-4](#)
- [Live Desk Role, page 11-4](#)

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 room (endpoint).

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 (endpoints) to monitor in the CTS-Manager application. Assigned Live Desks are easily reached by dialing the Help soft key on the endpoint phone/display device in a Cisco TelePresence-enabled meeting room (endpoint).

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 11-1 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 11-1 Troubleshoot > System Information Window

System Information

SKU	Hostname	IP Address	MAC Address	License MAC Address	Hardware Model	Software Version	OS Version
CTS-MAN 1.9	tsbu-docs-ctm	10.22.148.143	00:21:5e:c9:a6:3c	00215EC9A63C	7845I3	1.9.0.0 (161)	UCOS 4.0.0 0-45

Product Software Versions

Product Name	Supported	Actual
Microsoft Exchange	[08.00.10685, 08.01.10240, 14.01.0218.015, 6.5.6944, 6.5.7226, 6.5.7638, 8.1.240.5, 8.2.176.2, 8.3.0083.006]	Unknown
Active Directory	[2003, 2008, 2008 R2]	2008
Cisco Unified Communications Manager	[7.1.3 and later]	Actual Version

System Status

Today's Meetings:

- With Error: 0
- In Progress: 0
- Scheduled: 0

Other Errors: 5

© 2006-2012 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 11-2 CTS-Manager Licensed Features

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



Note

You are required to install the Endpoints license. Without this license, your configured endpoints 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 11-1 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 11-2 Count-Based Licenses

License	Part Number
10 endpoints	LIC-CTS-MAN-10
50 endpoints	LIC-CTS-MAN-50
100 endpoints	LIC-CTS-MAN-100

Room (endpoint) 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 endpoints licensing. If there are more TelePresence endpoints than available licenses, then the endpoints above the designated license count will have no license to subscribe to. In this case, you must obtain more licenses in order for all endpoints 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 11-7](#)
- [Existing Customers Upgrading to CTS-Manager 1.9, page 11-8](#)

New Customers

New customers purchasing CTS-Manager 1.9 or later, get licenses by doing the following:

-
- Step 1** Order CTS-Manager with server, choosing the number of endpoints for licensing plus optional reporting and/or scheduling API, as required.
 - Step 2** Receive CTS-Manager server. Included with the server is a Claim Certificate with a license Product Authorization Key (PAK).
 - Step 3** Install and initialize CTS-Manager.
 - Step 4** Obtain the License MAC Address by logging in to CTS-Manager and going to the **Troubleshoot > System Information** 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 13-43](#).

-
- Step 5** Register the PAK with the License MAC Address at <http://cisco.com/go/license>.
 - Step 6** License file(s) arrive by email within one hour.
 - Step 7** After installation of CTS-Manager, SysAdmin installs the license file(s). For more information, see [Viewing and Uploading Licenses, page 11-8](#).

Existing Customers Upgrading to CTS-Manager 1.9

Upgrading from CTS-Manager 1.7 or 1.8 to 1.9 is supported. CTS-Manager versions 1.7 and later require device and feature licenses.

No upgrade license or key is required for upgrading from 1.7 or 1.8, as long as customers have an installed device and feature license and a current support contract.



Caution

Customers upgrading from CTS-Manager 1.7 or later are only required to get an upgrade license if the License MAC for the CTS-Manager they are upgrading has changed due to a hostname or IP address change.

To get upgrade license do the following:

-
- Step 1** Perform upgrade to CTS-Manager 1.9.
 - Step 2** Log in to CTS-Manager
A message appears indicating that room (endpoint) licenses need to be installed.
 - Step 3** Click **OK** in the message.
The Configure > Licenses > License Files window appears.
 - Step 4** Click the **Get an Upgrade License** button and follow the instructions to get an upgrade license.
For more information, see [Getting an Upgrade License, page 11-12](#).
 - Step 5** License file arrives by email within one hour.
 - Step 6** SysAdmin uploads the license file(s).
For more information, see [Viewing and Uploading Licenses, page 11-8](#).
-

Existing CTS-Manager 1.9 Customers Adding More Endpoints or Licensed Features

-
- Step 1** Order CTS-Manager endpoints (rooms) or feature licenses. Two options are available for ordering licenses:
 - LIC-CTS-MAN-xxx - paper-based license with normal lead times.
 - 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: <https://edelivery.cisco.com/esd/>. For more information about eDelivery, refer to: <http://www.cisco.com/web/partners/tools/edelivery.html>.

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 endpoints (rooms) used for TelePresence meetings, based on one license per endpoint.

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 License 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 endpoints, go to the Support > Endpoints window to make sure that each endpoint has a green checkmark in the “Licensed” column.

To check if the uploaded licenses are valid, go to the Configure > Licenses window. 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 11-2 *Configure > Licenses > Summary Window*

Licenses

Licenses for this CTS-Manager must be generated using this License MAC Address: 00215EC9A63C.

Summary License 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	10	9

License Files

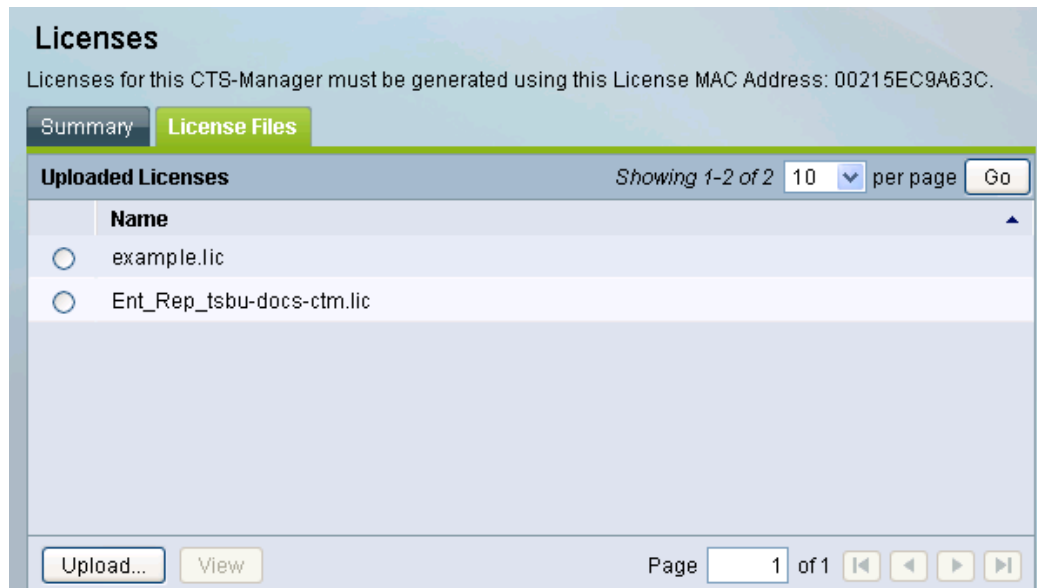
The Configure > Licenses > License Files window lists which licenses are already loaded in the system and allows you to upload new licenses. CTS-Manager allows you to import FlexLM-based license files into the database and enforce licensing based on information stored in that database. Licenses can be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



Note

Licensed must be generated using the License MAC Address of CTS-Manager, which is displayed at the top of the License Files window.

If you are upgrading to CTS-Manager 1.9 from a previous version, you must get an upgrade license to manage the endpoints you currently have configured in CTS-Manager. For more information, see [Getting an Upgrade License](#).

Figure 11-3 *Configure > Licenses > License Files Window*

Uploading Licenses

CTS-Manager licenses must be in text based ASCII format only. When licenses are generated from Cisco Licensing Site and saved from the browser or from the email client, some of the clients save the files as type of unicode text document. This introduces control characters which are not readable in during upload to CTS-Manager. Please ensure that the files are saved in ASCII Text format before attempting to upload in CTS Manager.

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 (Endpoint-based) Licenses

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

1. In a person-to-person meeting, the meeting organizer schedules a meeting between one endpoint using the 10-endpoint license group in CTS-Manager and the new 11th endpoint. The 11th endpoint 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/display device of the licensed endpoint, and no schedule appears on the phone/display device of the 11th endpoint.
2. In a multipoint meeting, the meeting organizer schedules a meeting between 3 endpoints using the 10-endpoint license group in CTS-Manager and the 11th endpoint. The 11th endpoint is not recognized by CTS-Manager and the meeting organizer receives a “confirmation” email for the three licensed endpoints. The meeting appears in the schedule of the phone/display device of all three licensed endpoints, but not in the 11th endpoint.

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 11-11](#).

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) or the Cisco Technical Assistance Center (TAC).

Getting an Upgrade License

CTS-Manager 1.7 and later requires a endpoint license to manage the endpoints 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 endpoints 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 11-11](#).



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 endpoint licenses you receive does not match the total licenses you purchased, email 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 Configure > Security window allows you to manage system security certificates and web services security.

CTS-Manager supports these security types:

- **Inter-device**—Secures communication between Cisco TelePresence devices, which include Cisco TelePresence Manager (CTS-Manager), Cisco TelePresence Recording Server (CTRS), and Cisco TelePresence Multipoint Switch (CTMS).
- **Browser**—Secures communication between the CTS-Manager web server and the browser through which you access the CTS-Manager Administrative UI. Browser security eliminates website security certificate warnings, which you receive if your web server is not secure.

You can set up either inter-device security or browser security on CTS-Manager, but not both at the same time.

For information on how to set up inter-device and browser security, see the Cisco TelePresence Security Solutions for Release 1.8, which you can access at this location:

http://www.cisco.com/en/US/docs/telepresence/security_solutions/1_8/CTSS.html.

LDAP Server

CTS-Manager uses Lightweight Directory Access Protocol (LDAP) to retrieve information related to users and conference rooms (endpoints) from Directory Server deployments. Enterprises typically use specialized databases called *directories* to store information related to users, meeting rooms (endpoints), 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 11-4 *Configure > LDAP Server*

Service:	OK	
Hostname	User Name	Default context
example-ctm (Default)	cn=administrator,cn=users,DC=tsbuctm,DC=com	DC=tsbuctm,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 11-3](#) 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 11-5](#) 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 11-5 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"/>	

254425

Table 11-3 lists the fields in the LDAP Server - New window. See Table 11-5 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 11-3 **New LDAP Server Settings**

Field or Button	Description or Settings
Host	LDAP server host name.
Bind Method	Click the Secure or Normal radio button to select the binding method: <ul style="list-style-type: none"> Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP.
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"> Click the Fetch button and choose the context from the Fetch DNS drop-down list adjacent to this field.
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 Note “cn=CTSTMan User” is another example. Note that the CTS-Manager Active Directory configuration requires using users that have Domain Admin privilege. The user, “CTSTMan 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 11-3 ***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 (endpoint) information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication.</p> <ul style="list-style-type: none"> To append the default context, check the Append default context box next to the user container field. <p>Note 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	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 11-4](#) lists the field information. See [Table 11-5](#) for the Person field information.


Figure 11-6 Edit LDAP Window


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	
Title:	<input type="text" value="Person"/>	<input type="text" value="title"/>	
Location:	<input type="text" value="Person"/>	<input type="text" value="location"/>	
DeptID:	<input type="text" value="Person"/>	<input type="text" value="department"/>	
Country:	<input type="text" value="Person"/>	<input type="text" value="co"/>	

Table 11-4 Edit LDAP Server Settings

Field or Button	Description or Settings
Host	LDAP server host name.

Table 11-4 *Edit LDAP Server Settings (continued)*

Field or Button	Description or Settings
Bind Method	<p>Click the Secure or Normal radio button to select the binding method:</p> <ul style="list-style-type: none"> Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP or DIIOP.
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"> Click the Fetch Distinguished Names button and choose the context from the Select a DN drop-down list adjacent to this field.
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=adminstrator,cn=users,dc=<mydomain>,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>

Table 11-4 Edit 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 (endpoint) information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication.</p> <ul style="list-style-type: none"> To append the default context, check the Append default context box next to the user container field. <p>Note 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>

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 11-5 describes the settings for the Person fields in both the New and Edit windows.

Table 11-5 LDAP Person - Objects and Attributes

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
Person			
	SchedulerName:	Person	cn Note Do not change this value. If this value is changed incorrectly, meetings will not have the correct information.
	EmailID:	Person	mail
	DisplayName:	Person	displayname
Note 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 endpoint'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 11-7](#) 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 11-6](#) lists the information for the fields in the IBM LDAP Edit or New window.

Table 11-6 IBM LDAP Server Settings

Field or Button	Description or Settings
Host	LDAP server host name.
Bind Method	Click the Secure or Normal radio button to select the binding method: <ul style="list-style-type: none"> Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP or DIIOP.
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"> Click the Fetch Distinguished Names button and choose the context from the Fetch DN's drop-down list adjacent to this field.
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 11-6 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 (endpoint) information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication.</p> <ul style="list-style-type: none"> To append the default context, check the Append default context box next to the user container field. <p>Note 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 11-7 describes the settings for the Person fields in both the New and Edit windows.

Table 11-7 LDAP Person - Objects and Attributes

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
Person			
	SchedulerName	Person	cn Note 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

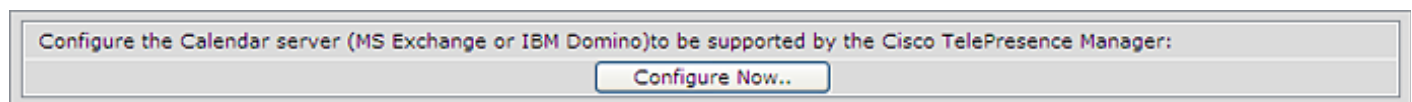
If you did not specify a Calendar server (either Microsoft Exchange or IBM Domino) during the initial installation, the Calendar Server window displays the Calendar Server wizard.

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

**Note**

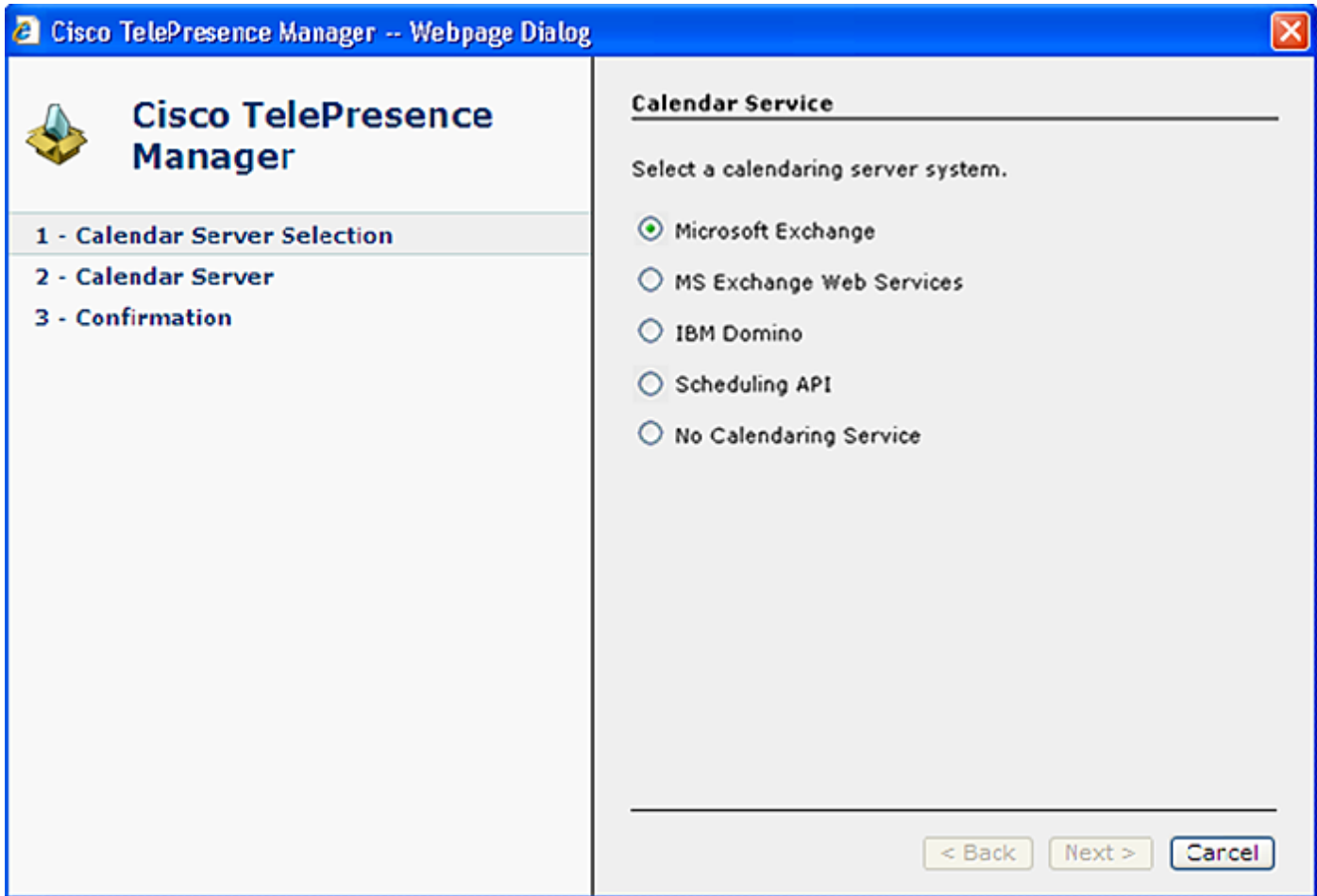
The LDAP server you specified during initial installation determines if you will be able to sync any Cisco TelePresence endpoints with the Calendar server you are registering. The LDAP server you are using must match the Calendar server you are registering.

Figure 11-7 **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 11-8 Cisco TelePresence Manager - Calendar Server Selection Screen

The screenshot shows a web-based configuration window titled "Cisco TelePresence Manager -- Webpage Dialog". On the left, there 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 area on the right is titled "Calendar Service" and contains the instruction "Select a calendaring server system." Below this, there are five radio button options: "Microsoft Exchange" (which is selected), "MS Exchange Web Services", "IBM Domino", "Scheduling API", and "No Calendaring Service". At the bottom right of the main area, there are three buttons: "< Back", "Next >", and "Cancel".

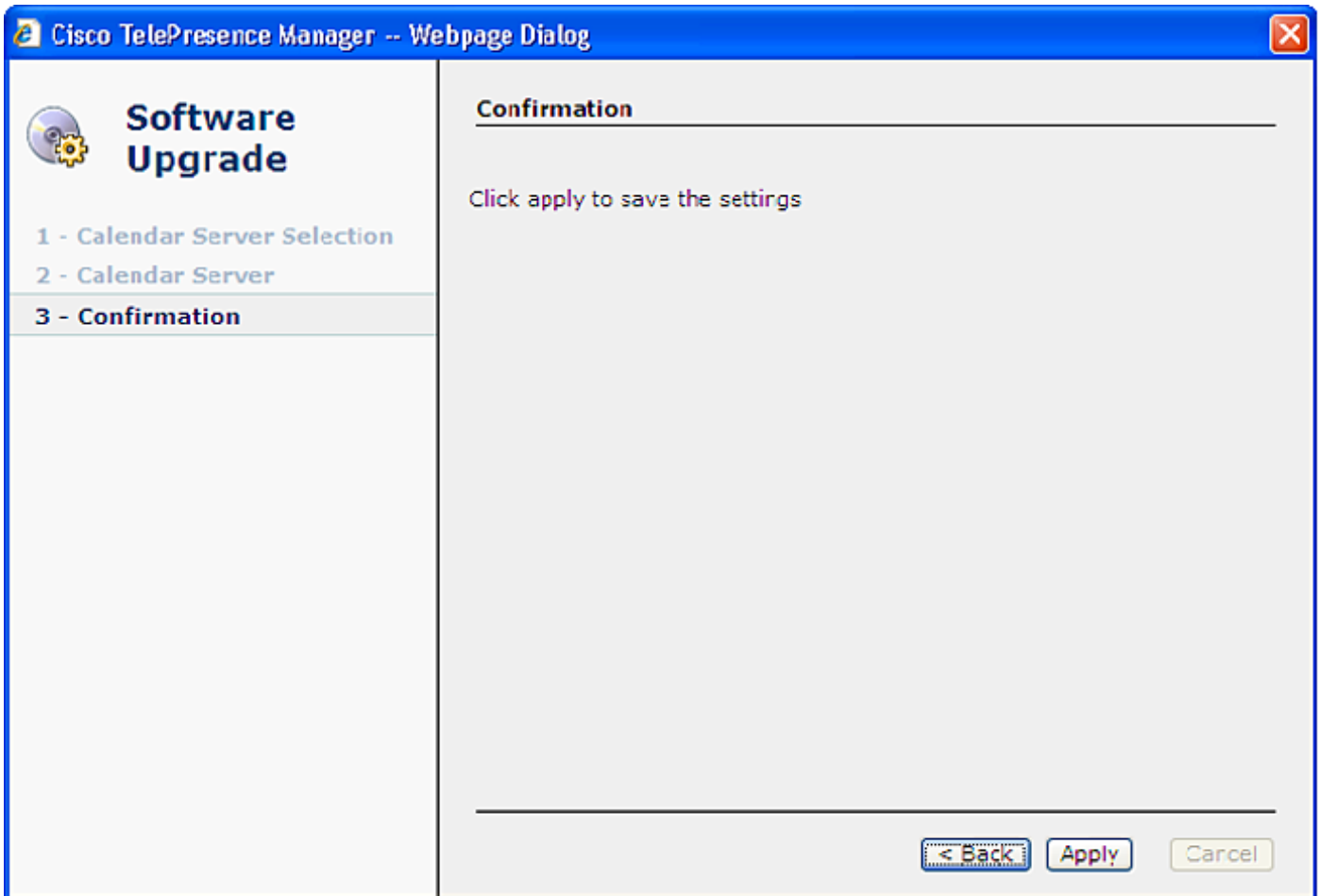
Step 2 In the next step you need to specify the service logon information. The example below displays the information needed to use the Microsoft Exchange service.

Figure 11-9 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".

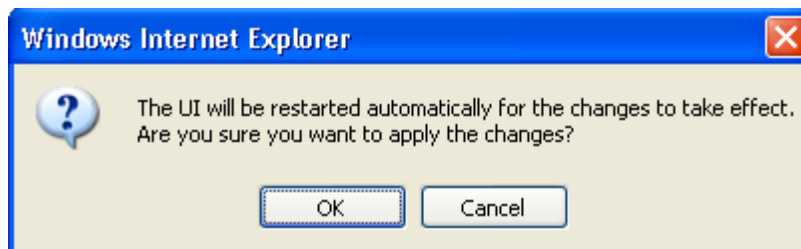
Step 3 Click **Apply** to save the new Calendar server settings.

Figure 11-10 Cisco TelePresence Manager - Calendar Confirmation Screen

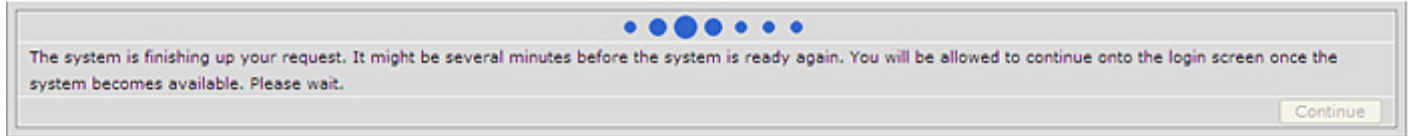


Step 4 Then click **OK** to restart the CTS-Manager server.

Figure 11-11 Apply Changes Screen



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

Figure 11-12 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.

It is divided into two tabs:

- Synchronization: Displays synchronization information for endpoints.
- Configuration: Displays configuration information for the Exchange server.

To test the connection between CTS-Manager and the Microsoft Exchange server as shown in [Figure 11-13](#):

-
- Step 1** Click the **Configuration** tab.
- Step 2** Click **Test Connection**.
- Step 3** To register new or modified settings, click **Apply**.
- Step 4** 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 11-13 *Configure > Microsoft Exchange Window > Synchronization tab*

Microsoft Exchange

Synchronization Configuration

Synchronization Operations Showing 1-4 of 4 10 per page Go

Subscription Status: All Sync Status: All Type: All Endpoint

Filter

<input type="checkbox"/>	Endpoint Name	Type	Sync Status	Last Synchronization Time	Subscription Status
<input type="checkbox"/>	dn45003	CTS 1000	✓	10/02/2011 05:05 PM	✓
<input type="checkbox"/>	dn70000	CTS 1100	✓	10/02/2011 05:05 PM	✓
<input type="checkbox"/>	ex62304	Cisco TelePresence C60	✓	10/02/2011 05:05 PM	✓
<input type="checkbox"/>	ex62305	Cisco TelePresence EX60	✓	10/02/2011 05:05 PM	✓

Resync Refresh

Page 1 of 1

Table 11-8 describes the information and operations accessible from this window.

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 endpoint.

You can filter the list by selecting using the Subscription Status drop-down menu, entering a room (endpoint) 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 endpoints to select them. To synchronize information for all endpoints, check the box next to **Endpoint 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 11-8 describes the information displayed in this area.

**Note**

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

Table 11-8 *Configure > Microsoft Exchange Window > Synchronization tab fields*

Field	Description or Settings
Endpoint Name	Name of the endpoint (room). Click the arrow in the header of the Endpoint Name column to sort the list in ascending or descending alphabetical order.
Type	Model of endpoint.
Sync Status	Status of the synchronization operation. Click the arrow in the header of the Endpoint Name column to sort the list in ascending or descending alphabetical order.
Last Synchronization Time	Choose the Secure or Normal radio button to select the binding method, as follows: <ul style="list-style-type: none"> 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. Normal—CTS-Manager communicates with the Microsoft Exchange server in cleartext using HTTP.
Subscription Status	Display-only status information of system service.

CTS-Manager and Microsoft Exchange server automatically renew subscriptions every 40 minutes. If there are any changes for endpoint 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 11-14 *Configure > Microsoft Exchange Window > Configuration tab*

Microsoft Exchange

Synchronization Configuration

Service: OK

Mailbox is: 0.01% full - 23694.0 of 3.584E8 KB is used

Host: 10.22.151.187 *

Bind Method: ☐ Secure ☒ Normal

Port: 80 *

Domain Name: example.com *

Username: sysadmin *

Password: *

Certificate: Browse...

* Required Fields

Test Connection Apply Cancel

Table 11-9 *Configure > Microsoft Exchange > Configuration tab information*


Field	Description or Settings
Service	Display-only status report of system service.
Mailbox is	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 Secure or Normal radio button to select the binding method, as follows: <ul style="list-style-type: none"> 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. Normal—CTS-Manager communicates with the Microsoft Exchange server in cleartext using HTTP.
Port	Communication port number.
Domain Name	Domain name provided for the Microsoft Exchange server account, which can be changed.
	 <p>Note This is the email domain name.</p>

Table 11-9 **Configure > Microsoft Exchange > Configuration tab information**




Field	Description or Settings
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> <div>  <p>Caution Logon Name is required for tentative room (endpoint) reservations to work.</p> </div>
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>ctsappsmtplhs@mycompany.com</i> enter <i>ctsappsmtplhs</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> <div>  <p>Note 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> </div> <div>  <p>Note For WebDav it was required to disable FBA. For EWS, FBA needs to be enabled.</p> </div>

Figure 11-15 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... *

- 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 11-10 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 11-10 Microsoft Exchange Web Services Fields (continued)

Field Name	Field Value
Username	Enter the username for the Exchange EWS server. Note If you are using Windows authentication, the format is: domain\username . If you are using basic authentication, the format is: username@ldapdomainname.com
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.

IBM Domino

The IBM Domino window helps you manage the database that stores TelePresence meeting information. It is divided into two tabs:

- Synchronization: Displays synchronization information for endpoints.
- Configuration: Displays configuration information for the Exchange server.

To test the connection between this system and the Domino server, as shown in [Figure 11-16](#)

-
- 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 11-16 *Configure > IBM Domino > Synchronization tab*

IBM Domino

Synchronization Configuration

Synchronization Operations Showing 1-1 of 1 10 per page Go

Sync Status: All Name: Filter

Sync Status	Name	Last Synchronization Time	Resynchronization Status	Associated Rooms
<input type="checkbox"/>	IBM Domino Databases			
<input type="checkbox"/>	example.nsf	✓ 10/03/2011 11:37 AM	Success	ROOM 40076NTEST/newsit list40071/newsite2 room40072/newsite2

Resync Refresh

Page 1 of 1

(*) All times are shown in time zone America/Los_Angeles (UTC -7.0)

Table 11-12 describes the information and operations accessible from this window.

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 (endpoint).



Tip

You can filter the list of endpoints 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 11-11 describes the information displayed in this area of the IBM Domino window.

Table 11-11 IBM Domino Server Synchronization Report

Field	Description
IBM Domino Databases	Name of the endpoint. Click the arrow in the header of the IBM Domino Database 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 endpoints (rooms) associated with the Domino database. Note The endpoint name displayed is the name of the room (endpoint) in the Domino database. In order for CTS-Manager to successfully sync the endpoint's meeting calendar, the room (endpoint) name must exactly match the endpoint name in the Cisco TelePresence System profile registered in Unified CM.



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.

Figure 11-17 Configure > IBM Domino > Configuration tab

Table 11-12 IBM Domino Server > Configuration fields

Field or Button	Description or Settings
Service	Display-only status report of system service.
Mailbox is	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 11-12 IBM Domino Server > Configuration fields

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"> 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. Normal—CTS-Manager communicates with the Domino server in cleartext using HTTP or DIIOP.
Port	Communication port number (HTTP or DIIOP).
Organization Name	Domain name provided for the Domino server account, which can be changed.  Note Organization Name is case sensitive.
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. Note Make sure the Internet password is used in the Password fields in the System Configuration> IBM Domino window and the LDAP Server window.
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, tell diiop show config , to find the class filename. Note A certificate is required in secure mode only.

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, page 11-39](#)
- [NTP, page 11-40](#)
- [SNMP, page 11-41](#)
- [Remote Account, page 11-46](#)
- [Password, page 11-47](#)
- [System, page 11-47](#)
- [Cluster, page 11-48](#)

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

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 11-18](#) describes the fields and buttons.

Figure 11-18 System Settings > IP Tab

System Settings

IP NTP SNMP Remote Account Password System

✱ = Required fields

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

Hostname: example-ctm

Domain Name: example.com

Primary DNS: 171.70.168.183

Secondary DNS:

Ethernet Card: eth0

DHCP: ☐ Enable ☒ Disable

✱ IP Address: 10.22.147.213

✱ Subnet Mask: 255.255.255.0

✱ Default Gateway: 10.22.147.1

Apply Cancel

-
- 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 before clicking Apply, click **Cancel**.
-

[Table 11-13](#) describes the information displayed in this area of the IP Settings window

Table 11-13 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>Note 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.

Table 11-13 IP Settings (continued)

Field or Button	Description or Settings
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.
Ethernet Card	Name supplied for the system Ethernet card.
DHCP	<p>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.</p> <div>  <p>Note To modify the IP settings for this Cisco TelePresence Manager, click the Disable radio button.</p> </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

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 11-19 **System Settings > NTP Tab**

The screenshot shows the 'System Settings' window with the 'NTP' tab selected. The 'NTP Servers' section contains five input fields for NTP Server 1 through NTP Server 5. The first two fields are populated with the IP addresses 192.168.33.15 and 192.168.33.17, respectively. Below the input fields are 'Apply' and 'Cancel' buttons.

NTP Servers:	
NTP Server 1:	192.168.33.15
NTP Server 2:	192.168.33.17
NTP Server 3:	
NTP Server 4:	
NTP Server 5:	

Buttons: 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 before clicking Apply, click **Cancel**.
-

SNMP

SNMP is an industry-standard interface used by network management systems to capture system status and error information, including information provided by Unified CM. CTS-Manager supports the Cisco SNMP service.

In order to configure the SNMP service on CTS-Manager, you must use the CTS-Manager Command Line Interface (CLI).

Figure 11-20 System Settings > SNMP Tab

System Settings

IP NTP **SNMP** 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
v3	cmuser	RW	*****	AuthPriv	MD5	DES

Trap Receiver Configuration

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

Table 11-14 describes the fields for SNMP settings.

Table 11-14 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 Utility command. When SNMP is enabled, supply a password for the SNMP server in the Configuration area.
SNMP Access Configuration	Use the CLI snmp set command to change these settings
– Username	SNMP server username.
– Current Password	SNMP server password. The password must be 8 characters long. Enter it twice for verification.
Trap Receiver Configuration	Use the CLI snmp set command to change these settings. See examples in following section.
– 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 default “admin” user with the default password, “snmppassword” must be changed in the new installation. All customer-created SNMP users and trap destinations are migrated to the new installation.

Configuring SNMP Traps on CTS-Manager

SNMP provides the ability to send traps, or notifications, to inform the system administrator when one or more conditions have occurred. Traps are network packets that contain information about a component of CTS-Manager. The information is status or error-related.

To configure SNMP traps on CTS-Manager, you must complete all of the following steps:

- Start the SNMP service
- Configure an SNMP user
- Configure an SNMP trap destination
- Enable CTS-Manager to send SNMP trap notifications

Starting the SNMP Service

To start the SNMP service, you must do the following:

Step 1 Log in to the CTS-Manager CLI.

Step 2 Run the **utils service start** command:

```
utils service start Cisco SNMP Service
```

Configuring an SNMP User

To configure an SNMP user on CTS-Manager, you must do the following:

Step 1 In the CTS-Manager CLI, configure an SNMP user with the command:

```
set snmp user add version username access [passphrase] [level]
```

Syntax Description

- *version* is the SNMP version, either 3 or 2c (both SNMP v3 and v2c are supported)
- *username* is the SNMP username (SNMP v3) or community string (SNMP v2c)
- *access* defines which SNMP tasks can be accessed; values are r (read), w (write), and rw (read and write)
- *passphrase* (optional) is the SNMP v3 user passphrase
- *level* (optional) is the SNMP v3 level; value is one of the following:
 - *authNoPriv* (default) is authentication with no encryption. The correct authentication key is required to write messages, but no encryption/decryption key is required to read the contents of the message.

- *authPriv* is authentication with encryption. The correct authentication key is required to write messages and the correct encryption/decryption key is required to read the contents of the message.
- *noauthNoPriv* is no authentication with no encryption. Neither an authentication key nor encryption/decryption key is required to write and read messages.



Note The *passphrase* and *level* parameters are not required for SNMP v2c.

The following example configures an SNMP v3 user, with the username **testusr**, granting read and write access, and with the passphrase **testpass**:

```
set snmp user add 3 testusr rw testpass
```

Configuring an SNMP Trap Destination

To configure an SNMP trap destination on CTS-Manager, you must do the following:

- Step 1** In the CTS-Manager CLI, configure an SNMP trap destination with the command:
- ```
set snmp trapdest add version username destination [passphrase] [level] [engineID]
```

### Syntax Description

- *version* is the SNMP version, either 3 or 2c
- *username* is the SNMP username (SNMP v3) or community string (SNMP v2c)
- *destination* is the destination host, in the format n.n.n.n[:port]
- *passphrase* (optional) is the SNMP v3 user passphrase
- *level* (optional) is the SNMP v3 level; value is one of the following:
  - *authNoPriv* (default) is authentication with no encryption. The correct authentication key is required to write messages, but no encryption/decryption key is required to read the contents of the message.
  - *authPriv* is authentication with encryption. The correct authentication key is required to write messages and the correct encryption/decryption key is required to read the contents of the message.
  - *noauthNoPriv* is no authentication with no encryption. Neither an authentication key nor encryption/decryption key is required to write and read messages.
- *engineID* (optional) is the SNMP v3 engine ID to use for the trap

The following example configures an SNMP v3 trap destination with the username **testusr**, at host **64.101.180.49:162**, passphrase **testpass**, and engine ID **0x8000DEECAFE8111BEEFADE**:

```
set snmp trapdest add 3 testusr 64.101.180.49:162 testpass authpriv
0x8000DEECAFE8111BEEFADE
```

- Step 2** Configure the SNMP client device according to the instructions for that device. For instructions on configuring a CTS Release 1.8 or later endpoint, for example, see the [SNMP Settings](#) sections of the *Cisco TelePresence Administration Guide for CTS Software Release 1.8*.

## Enabling CTS-Manager to Send SNMP Trap Notifications

The final step to configuring an SNMP trap on CTS-Manager is to enable CTS-Manager to send SNMP trap notifications.

To enable CTS-Manager to send SNMP trap notifications, you must do the following:

- Using an SNMP client, set the **clognotificationsenabled** MIB to **True**.

SNMP Trap notifications are now enabled for CTS-Manager.

## Modifying SNMP Trap Settings

You can modify existing SNMP trap destinations and user access.

To modify an SNMP trap destination, do the following:

- 
- Step 1** Delete the existing trap destination with the command:
- ```
set snmp trapdest del
```
- After entering the above command, the CTS-Manager CLI lists all configured SNMP trap destinations and prompts you to specify the trap destination to delete.
- Step 2** Configure the new SNMP trap destination with this command:
- ```
set snmp trapdest add version username destination [passphrase] [engineID] [level]
```
- For details on the syntax, refer to [Syntax Description, page 11-44](#).
- The following example configures an SNMP v3 trap destination with the username **testusr**, at host **192.168.180.122**, passphrase **testpass**, and engine ID **0x8000DEECAFE8111BEEFADE**:
- ```
set snmp trapdest add 3 testusr 192.168.180.122 testpass 0x8000DEECAFE8111BEEFADE
```
-

To modify SNMP user access to CTS-Manager SNMP traps, do the following:

-
- Step 1** Delete an existing SNMP user with the command:
- ```
set snmp user del version username
```
- Syntax Description**
- *version* is the SNMP version, either 3 or 2c
  - *username* is the SNMP username (SNMP v3) or community string (SNMP v2c)
- The following example deletes the SNMP v3 user **testusr**:
- ```
set snmp user del 3 testusr
```
- Step 2** Configure the new SNMP user with the command:
- ```
set snmp user add version username access [passphrase] [level]
```
- For details on the syntax, refer to [Syntax Description, page 11-43](#).
- The following example configures an SNMP v3 user, with the username **newusr**, granting read and write access, and with the passphrase **newpass**:
- ```
set snmp user add 3 newusr rw newpass
```

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 11-21 *Configure > System Settings > Remote Account Tab*

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 11-22 *Configure > System Settings > Password Tab*

The screenshot shows the 'System Settings' window with the 'Password' tab selected. The 'SysAdmin Username' is set to 'admin'. There are three password fields: 'Current Password', 'New Password', and 'New Password (again)'. A legend indicates that fields with a red asterisk are required. At the bottom, there are 'Apply' and 'Cancel' buttons.

- 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 (again)** field, repeat your new password to verify it.
- Step 5** To register the new password, click **Apply**.
- Step 6** To restore the original password before clicking Apply, click **Cancel**.



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

For standalone CTS-Manager deployments, this window allows you to restart or shut down CTS-Manager.

Figure 11-23 System Configuration System Settings

System Settings

IP NTP SNMP Remote Account Password **System**

★ = Required fields

Username: admin

★ Password:

Restart Shutdown

-
- Step 1** To restart the system, enter the password.
- Step 2** Click **Restart** to restart or **Shutdown** to shut down the CTS-Manager.
-

Cluster

Cisco no longer provides support for the clustering feature originally introduced in release 1.8. For questions, contact Ron Lewis: ronlewis@cisco.com.

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 11-24 Database > Settings Tab

Database

Settings Backup Restore

✱ = Required fields

Service: **OK**

Current Database Size: 0.04% full (5.78 of 14648.44 MB is used)

✱ Automatically Purge Data Older Than (months): +

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

Snapshots of Number of Meetings Showing 1-7 of 7 10 per page

Date	Past Meetings	Future Meetings
09/27/2011 12:55 AM	4349	442
09/28/2011 12:55 AM	4335	428
09/29/2011 12:55 AM	4318	436
09/30/2011 12:55 AM	4299	785
10/01/2011 12:55 AM	4282	766
10/02/2011 12:55 AM	4261	747
10/03/2011 12:55 AM	4241	728

Page of 1

(+) All times are shown in time zone America/Los_Angeles (UTC -7.0)

**Note**

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

Table 11-15 describes the information and settings that are accessible from the Database window Settings tab.

Table 11-15 Database Settings

Field	Description or Settings
Service	Display-only status report of the Informix database server.
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. 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>Note 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 11-25 *Configure > Database > Backup*

Database

Settings **Backup** Restore

✱ = Required fields

Schedule (+): Daily @ 17:05 [Change...](#)

Number of Backup Files to Keep: 14

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](#)

Available Backup Files Showing 0-0 of 0 10 per page [Go](#)

Time	Status	Type	Hostname	Location
No data to display				

[Refresh](#) Page 0 of 0 [◀](#) [▶](#)

(+) All times are shown in time zone America/Los_Angeles (UTC -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 before clicking Apply, click **Cancel**.



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 11-16 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, in the Available Backup Files section.

[Table 11-17](#) describes the Backup History and Restore History fields.

Table 11-17 Backup History and Restore History Fields

Field	Description
Time	Date and time of backup. Click the arrow in the header of the Time 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 11-17](#) for a description of the fields.

Figure 11-26 *Configure > Database > Restore Tab*

Database

Settings Backup **Restore**

* = Required fields

Restore Type: ☒ Local ☐ Network

Restore Mode: ☒ Sftp ☐ Ftp

Remote Storage Host: *

Port: *

Username: *

Password: *

Storage Path: *

Restored Backup Files History Showing 0-0 of 0 10 per page

Time	Status	Type	Hostname	Location
No data to display				

Page 0 of 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 11-16](#) 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 11-27 Configure > Unified CM Window

The screenshot shows the 'Unified CM' configuration window. At the top, it says 'Cisco Unified Communications Manager' and 'Showing 1-1 of 1' with a dropdown set to '10' and a 'Go' button. Below this, there's a 'Service:' label with a radio button and the text 'OK'. A table follows with columns: Status, Hostname, IP Address, and Application Username. The table contains one row with the following data: Status is 'OK' (with a radio button), Hostname is 'example-ccm', IP Address is '209.165.200.225', and Application Username is 'exampleappuser'. At the bottom, there are buttons for 'New...', 'Edit...', 'Delete', 'Discover Rooms', and 'Refresh'. To the right of these buttons is a 'Page' indicator showing '1 of 1' and navigation arrows.

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 11-19](#) for a description of each button's function.

To manually start the process that is periodically performed to discover new endpoints (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 11-18 Discover Cisco Unified Communications Manager Settings


Field	Description or Settings
Status	<p>Display-only status report of system services.</p> <p>Note You may see a progress indicator in the status field, especially if many Cisco TelePresence meeting rooms (endpoints) 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 endpoints.</p> <p> Caution 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 Discover Rooms.</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.
Delete	This deletes the current Cisco Unified CM connection.

Table 11-18 Discover Cisco Unified Communications Manager Settings (continued)

Field	Description or Settings
Discover Rooms	This allows you to manually start the process that is periodically performed to discover new endpoints 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 11-28](#).

Figure 11-28 Unified CM Service Window

+ See Security Settings for the certificate currently in use for this secure connection

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 11-19](#) describes fields, buttons, and settings.

Table 11-19 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.
Close	Close the window.

When a room (endpoint) 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 (endpoints) should be deleted only after an administrator manually does a rediscovery. If the endpoint 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, edit, deallocate and delete bridge and server devices. There are seven devices supported by CTS-Manager:

- Cisco TelePresence Multipoint Switch (CTMS)
- Cisco TelePresence Server (TS)
- Cisco Collaboration Manager
- Cisco TelePresence Recording Server (CTRS)
- 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.

Figure 11-29 *Configure > Bridges and Servers*

Bridges and Servers

Status of Bridges and Servers

Showing 1-5 of 5100 per pageGo

Service:OK

	Status	Hostname	Type	Scheduled	Description	IP Address
<input type="radio"/>		209.165.200.225	CUVC	Yes	CUVC	209.165.200.225
<input type="radio"/>		209.165.200.226	CTRS	—		209.165.200.226
<input type="radio"/>		example.webex.com	WebEx	—	—	https://example.webex.com/exmp
<input type="radio"/>		example-ctms-10	CTMS	Yes	CTSM example-3	209.165.202.129
<input type="radio"/>		example-ctms-11	CTMS	Yes	example-ctms11	209.165.202.130

New...Edit...DeleteRefresh

Page1 of 1

Table 11-20 describes the Bridges and Servers fields.

Table 11-20 *Bridges and Servers Devices*

Field	Description or Settings
Status	Display-only status report of system services. Note You may see a progress indicator in the status field, especially if many Cisco TelePresence endpoints 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 endpoints.
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.
Scheduled	Indicates whether the bridge or server is available (scheduled) for meetings. The resources of a scheduled bridge or server can be used when meetings are scheduled. If a bridges or server is non-scheduled, it means it will not be used when a meeting is scheduled. The arrow allows you to sort ascending or descending.
Device Group	The group to which the CTMS is assigned. You can change this group in the Configure > Device Groups page. Only CTMS devices and endpoints can be grouped. For more information about device groups, see Device Groups .
Description	The Description field displays the bridge or server device description, added when the Conferencing Bridge device was added. A CTMS description is configured in the CTMS administrative WEB UI.
IP Address	The IP address of the bridge or server.

Adding a Bridge or Server

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:

- [Cisco TelePresence Multipoint Switch \(CTMS\), page 11-63](#)
- [Cisco TelePresence Server \(TS\), page 11-65](#)
- [Cisco TelePresence Recording Server \(CTRS\), page 11-67](#)
- [WebEx, page 11-68](#)
- [Collaboration Manager, page 11-72](#)



Note

In release 1.9, support for CUVC is discontinued. Existing scheduled meetings will continue to work, but new meetings cannot be scheduled.

Editing a Bridge or Server

To edit a bridge or server device, click the radio button associated with the device to select that device and click the **Edit** button. The Edit...Bridge or Server window appears. [Table 11-21](#) describes the fields that can be changed.

Table 11-21 Edit Bridge or Server Devices

Field	Description or Settings
Username	This is the account name used to log into the bridge or server.
Password	This is the account password used to log into the bridge or server.
Scheduled	Select either Yes or No to specify whether the bridge or server is available (scheduled) for meetings. CTMSs in a scheduled state cannot be used to migrate meetings from other CTMSs. If No is selected, resource allocation is not available. Selecting Yes for Scheduled allows resource allocations. TSs must always be in a Schedule state.
Deallocate (CUVC)	Select the checkbox to specify that the CUVC's resources are removed from all future meetings.
Migrate All Meetings (CTMS)	All meetings scheduled to use a CTMS can be migrated to a non-scheduled CTMS. For more information about how meeting migration works, see Migrating All Meetings from a CTMS .
Distribute All Meetings (TS)	All meetings scheduled to use a TS can be migrated to other scheduling devices. Set Scheduled to No , check the check box and click Save . Note When distributing all meetings, CTS-Manager will try to schedule these meetings again on the available scheduling devices. Make sure you do this during off-peak hours and when there are enough scheduling resources available. If email notification is turned on, the organizer of each meeting will receive a new confirmation email.

After editing the information for your bridge or server, click **Save**.

Deleting a Bridge or Server

A bridge or server cannot be deleted if there are any associated scheduled meetings. To delete a CTMS, you must migrate all of its meetings to another scheduling device. To delete a TS, you must distribute all of its meetings to another scheduling device. To delete a CUVC, with associated scheduled meetings, you must first deallocate the CUVC before you can delete the device.

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



Note

To delete a WebEx site, CTS-Manager must have connectivity to the WebEx site to properly deallocate the meetings associated with it.

Migrating All Meetings from a CTMS

Migrating all meetings, moves all meetings scheduled to use the selected CTMS to a non-scheduled CTMS. Click the checkbox and choose another CTMS from the drop-down list.

To migrate all meetings from a CTMS to another CTMS:

-
- Step 1** Click the radio button next to the CTMS from which you want to migrate all meetings.
 - Step 2** Click **Edit**.
The Edit Bridge or Server window opens.
 - Step 3** Select **Migrate All Meetings**.
 - Step 4** Select a CTMS to which to migrate.
 - Step 5** Click **Save**.
-

How Meeting Migration Works with CTMSs

When preparing to migrate individual or all meetings from one CTMS to another, it's important to understand how device groups and CTMS Network Multipoint affect the migration process.

How device group settings affect meeting migration

1. Default (Ungrouped) device group only
Migrating individual and all meetings works the same as non-network multipoint meetings.
2. Multiple device groups and Intergroup Scheduling disabled
Migration destinations must be CTMSs within the same device group
3. Multiple device groups and Intergroup Scheduling enabled
Migration destinations can be CTMSs in any device group.

How CTMS Network Multipoint settings affect meeting migration

1. CTMS Network Multipoint disabled
Meeting is cleared from the source CTMS and migrated to the destination CTMS. Endpoints receive updated One-Button-to-Push numbers for the destination CTMS.
2. CTMS Network Multipoint enabled
Meeting is cleared from the source CTMS and migrated to the destination CTMS. Endpoints receive updated One-Button-to-Push numbers for the destination CTMS.
 - If the source CTMS is a leaf, the RP of the destination is updated to match the source's RP.
 - If the source CTMS is an RP, the leaves are updated with the new RP number of the destination.
 - If the source CTMS is used for the TelePresence Call-In Number, the meeting is updated with the new call-in number of the destination CTMS and a new email is sent to the meeting organizer with the new call-in number.



Note

In order to migrate a network multipoint meeting, the destination CTMS must be compatible with CTMS Network Multipoint.

Distributing All Meetings from a TS

Distributing all meetings, moves all meetings scheduled to use the selected TS to other available scheduling devices.



Note

If there are no other scheduling devices available, this removes TS from all future meetings. Meetings currently in progress will continue to have TS resources.

To distribute all meetings from a TS to another scheduling device:

-
- Step 1** Click the radio button next to the TS from which you want to migrate all meetings.
 - Step 2** Click **Edit**.
The Edit Bridge or Server window opens.
 - Step 3** Select **Distribute All Meetings**.
 - Step 4** Click **Save**.
-



Caution

In the Configure > Application Settings > Bridges and Servers tab, you can configure primary and secondary multipoint conference scheduling device settings. Either TS or CTMS can be configured as the primary or secondary. If TS is defined as the primary and CTMS is not selected as the secondary (even if a CTMS has been added in the Configure > Bridges and Servers window), the Distribute All Meetings command will deallocate all meetings on the selected TS.

Example

You have two TS devices (TS1 and TS2). Both have Scheduled set to Yes. Both have 16 ports.

1. Select TS1 and do Distribute All Meetings. (All future scheduled meetings will use TS2).

TS1 will be set to non-scheduled. All scheduled meetings are removed from TS1 and moved to TS2.

2. To find out if the distribution is successful, go to the Monitor > Meetings window to see if there are any meetings in error due to lack of resources.

Resource Allocation with CTMS and TS Devices

For 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.

For resource allocation with TS devices, CTS-Manager randomly chooses a TS based on its database record number.

With release 1.9 of CTS-Manager, you can prioritize scheduling of CTMS devices in device groups. To do this, you must create a device group and add CTMS devices to it. After you add CTMS devices to a group, you can set the scheduling order of those devices. For more information, see [Device Groups](#), page 11-78.

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)

CTMS devices provide the functionality for three or more endpoints to participate in a scheduled meeting. Cisco TelePresence Manager provides the scheduling information to the different CTMS devices and each CTMS provides the multipoint switching capabilities for the meeting.

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 11-30 Adding a CTMS Device

Table 11-22 Adding a CTMS Device

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.
Device Group	Select the group to which you want to assign the CTMS. If you do not select a group, you can do it later in the Configure > Device Groups page.
Scheduled	<p>Choose either Yes or No, to 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.</p> <p>CTMS devices in a Scheduled state cannot be used to migrate meetings from other CTMS devices.</p> <div>  <p>Caution When a CTMS is in a scheduled state, CTS-Manager schedules its resources, even if it is in an error state. When a CTMS is in a error state, scheduled meetings will fail. The only way to disable scheduling of a CTMS is to set Scheduled to No.</p> </div>

**Note**

To downgrade an existing CTMS to a software version earlier than 1.9, you must restart CTS-Manager to establish a fresh connection.

Cisco TelePresence Server (TS)

TS software 2.2 or later is required for CTS-Manager.

**Note**

CTS-Manager supports secure communication with TelePresence Server on port 443 only and non-secure communication on port 80 only. Refer to your TS documentation on how to set up secure communication.

Adding a Cisco TelePresence Server

To add a Cisco TelePresence server 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 window.
- Step 3** Choose **TelePresence Server** from the Type drop-down field.
- Step 4** Enter the information, click **Save**.
- Step 5** Click **Refresh** to display the new TS in the Configure > Bridges and Servers window.
The new TS is displayed in the Configure > Bridges and Servers window.

**Note**

A TS may initially be displayed with a status of 'Not registered' (red 'x' icon). After the Username and Password are validated by CTS-Manager, the status changes to 'Registered' (green check mark icon). This process may take up to 3 minutes. If the status is still 'Not registered' after 3 minutes, edit the TS and verify the Username and Password are correct.

- Step 6** To verify the TS you just added configured correctly, select it and click the Edit button.
Segment Count should display the total capacity of ports on the TS.
After you add the TelePresence Server, you can edit it later by selecting it and clicking the **Edit** button.

Figure 11-31 Adding a TelePresence Server

New Bridge or Server

Type: TelePresence Server ▼

✱ Hostname:

✱ Username:

✱ Password:

Scheduled: ☐ Yes ☒ No

✱ Multipoint Call-In Number Start:

✱ Multipoint Call-In Number End:

✱ = Required fields

Table 11-23 TS Device Information

Field	Description or Settings
Type	Select TelePresence Server from this pull-down list menu.
Hostname	The configured hostname of the TS device. This is the LHS of the complete hostname. Note Make sure the hostname is registered in DNS and can be resolved by CTS-Manager.
Username	This is the account name used to log into the TS. Note A user account must be created on the TS with API privileges with the same username and password. username and password must match.
Password	This is the account password used to log into the TS. Note Make sure you enter the correct password. If you enter the wrong password, an error status will appear after up to 3 minutes.
Scheduled	Select either Yes or No to specify whether the TS is schedulable for meetings. If No is selected, meetings cannot be scheduled using this device.
Multipoint Call-In Number Start	The first number of the numeric ID range allocated to this device, based on your enterprise dialing plan.
Multipoint Call-In Number End	The last number of the numeric ID range allocated to this device, based on your enterprise dialing plan.

**Caution**

The Multipoint Call-In Number range must be between: 1 and 2147483647 and must include only positive numbers. Using numbers that are outside of this range will cause no resources to be available for scheduling meetings that require the TS.

Multipoint Call-In Numbers on the TelePresence Server

Each conference on a TS must have a unique numeric ID. CTS-Manager randomly generates a numeric ID within the start and end number range when it is configured in CTS-Manager. One-Button-to-Push uses this TS call-in number. For more information about TelePresence Number, see http://www.cisco.com/en/US/docs/telepresence/cts_manager/1_8/call_in_number.html

**Caution**

The specific Multipoint Call-In Number range cannot be used by any other TS. CTS-Manager does not validate the dial plan associated with the number range.

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 Device

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 11-32 Adding a CTRS Device

New...Bridge or Server

⚙ = Required fields

Type:	CTRS ▼
Hostname:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>

WebEx

Table 11-24 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.

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 12, “Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager”](#).

Multiple WebEx Sites

You can add multiple WebEx sites to support WebEx users with accounts on different WebEx scheduling servers. When multiple WebEx sites are configured in CTS-Manager and WebEx is enabled, WebEx Permitted and Premium users will be able to register themselves to one of the WebEx sites the first time they schedule a WebEx meeting. It is important to communicate with these users which server they should use.

For more information about first-time WebEx meeting scheduling, refer to:

[First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15](#).

WebEx Proxy Server

To provide an extra level of security, an enterprise might require communication between the enterprise and the Cisco WebEx cloud to go through a proxy server. In such a case, the administrator must configure CTS-Manager to connect to WebEx site through the 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 using Basic authentication using username and password



Note

No other form of proxy authentication (such as Digest, NTLM, certificate based, Kerberos) is supported. A proxy server supporting multiple protocols should have basic authentication as the default authentication mechanism between CTS-Manager and WebEx.

Adding a WebEx Site

To add a WebEx site 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.

**Note**

If the message “No trusted certificate found” appears, an expired WebEx certificate may exist in CTS-Manager. Go to **Configure > Security** and verify that the WebEx certificate is valid (by checking its expiration date). If the certificate is expired, manually remove it and then add the new WebEx site again.

Step 5 Click **Save**.

The New Bridge or Server window closes.

Step 6 Click the **Refresh** button.

The newly added WebEx site displays a status of “OK.”

**Note**

After you add the WebEx site, you can edit it later by selecting it and clicking the Edit button. Only the authentication credentials can be edited. If the site URL needs to be changed, the original site needs to be deleted and a new site added.

**Note**

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

Figure 11-33 Adding a WebEx Site

New Bridge or Server

Type: WebEx

* Hostname: example.webex.com

* Site URL: https://example.webex.com/exm

* WebEx: Admin Username: exampleAdmin

* WebEx: Admin Access Code: •••••

* Certificate: Browse...

Connection Type: ☒ Direct ☐ Via Proxy Server

WebEx Proxy Server Settings

* Host Name:

* Port:

Require Authentication: ☐ Yes ☒ No

* User Name:

* Password:

* = Required fields

Test Save Close

284070

Table 11-25 WebEx Site Information

Field	Description or Settings
Type	Select WebEx from the pull-down list menu.
Hostname	<p>A name identifying the WebEx site hostname to the administrator. This typically can be the same name as the hostname used in the site URL.</p> <p>Note Multiple WebEx sites can have the same hostname. This is not used to connect to the WebEx site and therefore is not validated during testing of connection.</p>
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>Note 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 site must use HTTPS. For detailed instructions on downloading the certificate with different browsers, see First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15.</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>
WebEx Proxy Server Settings	
Host Name	Host name of proxy server
Port	Port number of proxy server
Requires Authentication	Select Yes if the proxy server requires authentication and then enter username and password.
Username	Username for proxy server
Password	Password for proxy server

Deleting a WebEx Site

When deleting a WebEx site, CTS-Manager must first connect to the WebEx site to deallocate the scheduled WebEx meetings. If CTS-Manager cannot connect to the WebEx site, the site cannot be deleted.

**Caution**

Deleting a WebEx site will remove WebEx from all upcoming scheduled meetings. Meeting organizers will receive a new confirmation email for their TelePresence meetings with WebEx, but the email will not indicate that WebEx has been removed from the meeting. TelePresence meetings with WebEx that are currently in progress will continue to have WebEx.

To delete a WebEx site:

Step 1 Select the WebEx site.

Step 2 Click **Delete**.

CTS-Manager connects to the WebEx site, deallocates the meetings and then deletes the WebEx site.

Collaboration Manager

To register a Collaboration Manager server with Cisco TelePresence Manager, click **New** to display the New...Bridges or Servers dialog box, and choose Collaboration Manager from the Type drop-down field.

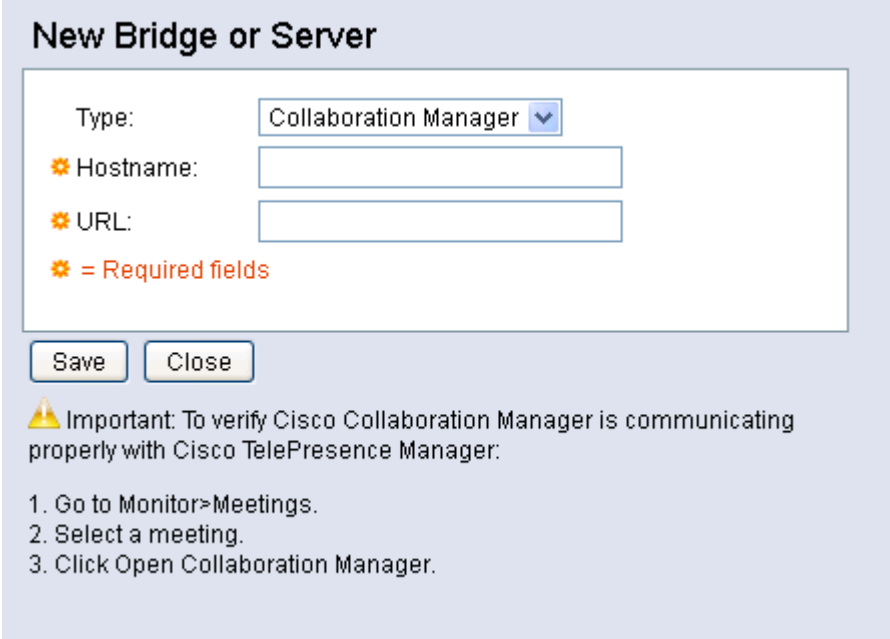
Provide the following information and click **Save**.

After Cisco Collaboration Manager is configured, you access it by doing the following:

Step 1 Go to **Monitor > Meetings**.

Step 2 Select a meeting.

Step 3 Click **Open Collaboration Manager**.

Figure 11-34 Adding a Collaboration Manager


New Bridge or Server

Type: Collaboration Manager

✱ Hostname:

✱ URL:

✱ = Required fields

Save Close

⚠ Important: To verify Cisco Collaboration Manager is communicating properly with Cisco TelePresence Manager:

1. Go to Monitor>Meetings.
2. Select a meeting.
3. Click Open Collaboration Manager.

Table 11-26 Adding a Collaboration Manager

Field	Description or Settings
Type	Select Collaboration Manager from this pull-down list menu.
Hostname	The configured Hostname of the Collaboration Manager server. This is the LHS of the complete Hostname
Username	This is the account name used to log into the Collaboration Manager.

Cluster Management

Cisco no longer provides support for the clustering feature originally introduced in release 1.8. For questions, contact Ron Lewis: ronlewis@cisco.com.

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 (endpoints), 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 11-35 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:

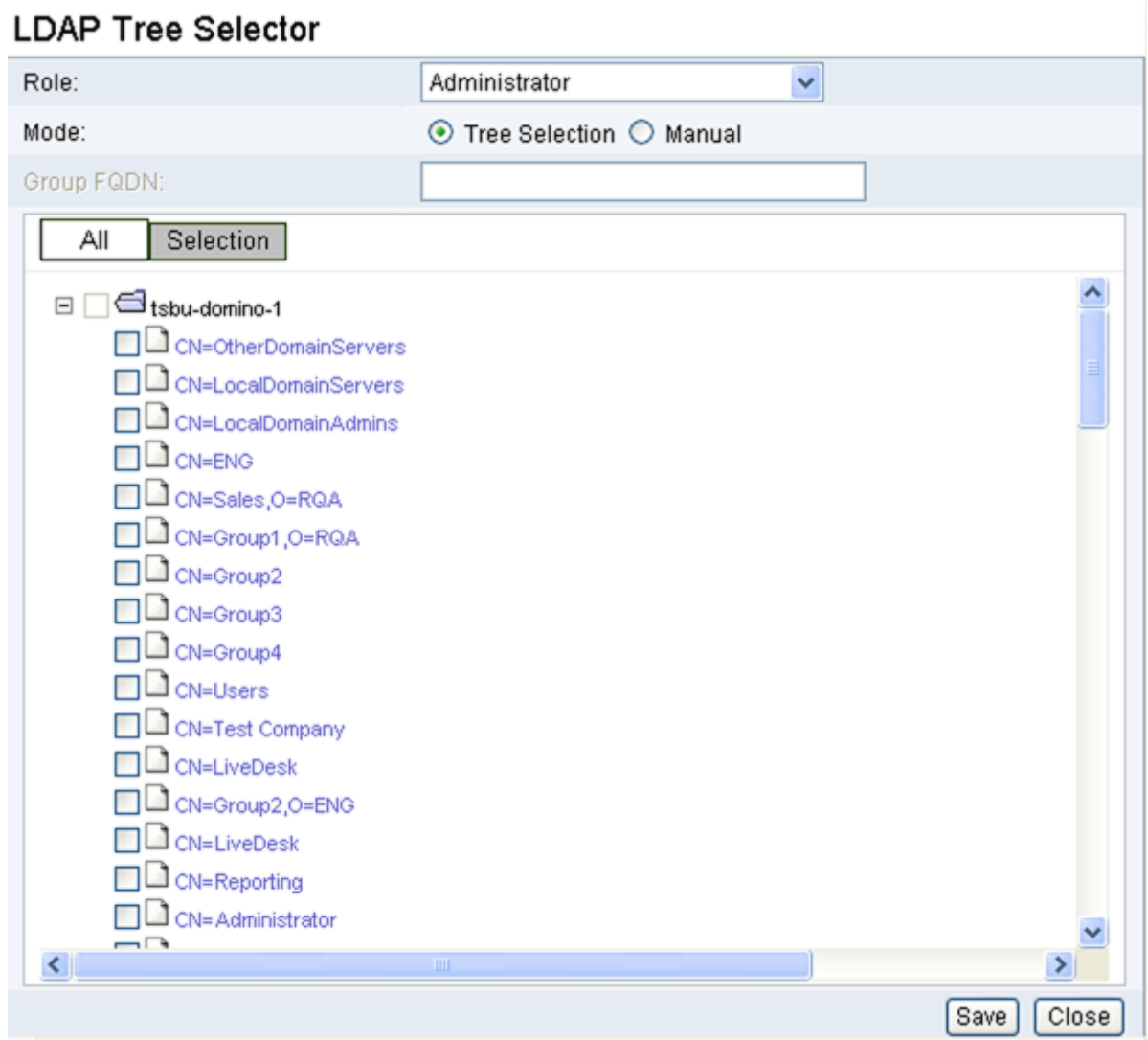
-
- Step 1** In the Access Management window, click **Add**.
The LDAP Tree Selector window appears, as shown in [Figure 11-36](#).
- Step 2** Select a role from the Role drop-down menu
- Step 3** For Mode, click the Tree Selection radio button if you want to select an LDAP group from the list of all LDAP groups, or click the Manual radio button if you want to enter a specific group name in the FQDN text field.



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

Figure 11-36 LDAP Tree Selector



Alert Management

The Alert Management window allows you to set the threshold that determines when CTS-Manager sends email notifications that its hard disk is approaching or has exceeded the configured threshold or critical level.

The alert is sent to the email address configured in the **Copy Outgoing Email To** field in the Configure > Application Settings > Email window.

In the Disk Threshold Percentage field, enter the percentage of used disk space that will determine when CTS-Manager will send alert emails and click **Apply**.

CTS-Manager sends alert emails under the following circumstances:

- When the disk usage reaches 5% below the configured Disk Threshold Percentage, CTS-Manager sends an email indicating the disk usage is approaching the threshold.

- When the disk usage exceeds the configured Disk Threshold Percentage, CTS-Manager sends an email indicating the disk usage has exceeded the threshold.
- When the disk usage exceeds 90%, CTS-Manager sends an email indicating the disk usage has exceeded the critical level.

CTS-Manager resends the alert every 24 hours until the disk usage issue is resolved.

Included in each email, are the storage and system parameters for the CTS-Manager server.

Table 11-27 Storage Parameters

Parameter	Description
Total Disk	Total disk capacity
Total Disk Used	Total disk space used
Total Disk Available	Total disk space available
Total Disk Used	Total percentage of disk space used

Table 11-28 System Parameters

Parameter	Description
SKU	CTS-Manager product version
Hostname	Configured hostname of the CTS-Manager server
IP Address	IP address of the CTS-Manager server
Hardware Model	Hardware model of the CTS-Manager server
Software Version	CTS-Manager software version

Device Groups

You can group endpoints with CTMS devices, so that when a meeting is scheduled, CTS-Manager reserves devices from the same group as the endpoint(s). Grouping is especially useful for large geographically-dispersed companies with many endpoints and CTMS devices.

By default, all devices are part of a group called 'Ungrouped'. The Ungrouped group displays all endpoints, CTMSs, TelePresence Servers and WebEx sites registered to CTS-Manager, however only endpoints and CTMSs can be part of a new group.



Note

It is not required to create device groups.

Grouping Devices

To group devices, do the following:

- Step 1** Log into the CTS-Manager Administrative UI.
- Step 2** Go to **Configure > Device Groups**.

Step 3 In the List of Device Groups section, click **New**.

The New Group window appears.

Step 4 In the Group Name field, enter a name for your device group.



Tip

Cisco recommends creating a meaningful name such as one based on geographical location.

Step 5 To add CTMS devices to the group, select the Bridges and Servers tab. To add Endpoints, select the Endpoints tab.

Step 6 From the Available devices list on the left, select devices and click the right-pointing single arrow to move them to the Selected list on the right.



Note

To add all available devices, click the right-pointing double arrow. To remove devices from the group, select the device and click the left-pointing single arrow.

Step 7 When adding CTMS devices, you can specify the scheduling order for each CTMS by selecting it in the Selected list and clicking one of the up or down arrows at the right side of the window.



Tip

The scheduling order allows you to prioritize the order in which CTS-Manager attempts to schedule CTMS resources. The CTMS at the top of the Selected list will be used first, followed by each CTMS in order from top to bottom. Scheduling order is followed on a best effort basis.

Step 8 When you are finished adding devices, click **Apply**.

[Figure 11-37](#) displays a sample New Group window.



Note

CTMS Devices can also be added to an existing group when they are configured in the Configure > Bridges and Servers page. Endpoints can also be added to an existing group when they are configured in the Configure > Endpoints page.

Figure 11-37 Creating a New Device Group—Sample New Device Group Window

New Group

Group Name:

Bridges and Servers **Endpoints**

Set the scheduling order using the arrows at the right.

Available					Selected				
Name	Description	Schedulable Segments	Time Zone	Device Group	Name	Description	Schedulable Segments	Time Zone	Device Group
CTMS-01	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-02	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-03	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-04	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-05	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-06	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-07	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-08	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-09	10.195.51.50	0	America/Los_Angeles	ungrouped					
CTMS-10	10.195.51.50	0	America/Los_Angeles	ungrouped					

Editing Groups

You can edit groups, so as you expand or modify your device deployment you can easily modify groups without having to delete and recreate them.

To edit a device group, do the following:

-
- Step 1** Log into the CTS-Manager Administrative UI.
 - Step 2** Go to **Configure > Device Groups**.
 - Step 3** In the List of Device Groups section, select the group that you want to edit.
The list of devices in the selected group appears in the bottom half of the page.
 - Step 4** Click **Edit**.
The Edit Group window appears.
 - Step 5** Modify the name, add, remove or order devices following the steps in [Grouping Devices, page 11-78](#).
-

Deleting Groups

To delete a device group, do the following:

-
- Step 1** Log into the CTS-Manager Administrative UI.
 - Step 2** Go to **Configure > Device Groups**.
 - Step 3** In the List of Device Groups section, select the group that you want to delete.
The list of devices in the selected group appears in the bottom half of the page.
 - Step 4** Click **Delete**.

- Step 5** A confirmation message appears, telling you that devices in the group you are about to delete will be moved to the 'Ungrouped' group.

**Note**

Deleting a group does not delete any CTMS devices or endpoints. It only moves them to the 'Ungrouped' group.

Endpoints

A CTS-Manager administrator can register video conferencing (VC) and EX, MX or C-series endpoints to CTS-Manager, enabling easy scheduling of meetings that include participants using these types of endpoints.

EX, MX or C-series endpoints with TC5.0 or later support One-Button-to-Push (OBTP). Endpoints with TC4.x or earlier function as VC endpoints and do not support OBTP.

Registering EX, MX or C-series Endpoints

For EX, MX or C-series endpoints with TC4.x or earlier software:

- Select **Video Conferencing** as the endpoint type.

For EX, MX or C-series endpoints with TC5.0 or later software:

- Select **EX or C Series** as the endpoint type.

EX, MX or C-series endpoints running TC5 or later that are registered to a Unified CM running version 8.6(1) or later are automatically discovered by CTS-Manager. In this case, it is not necessary to add the endpoints in this window.

**Note**

EX, MX and C-series endpoints do not support the Live Desk feature.

Figure 11-38 *Configure > Endpoints*

Endpoints

Endpoints registered with Cisco Unified CM are discovered automatically and listed on the **Support > Endpoints** page. Showing 1-2 of 2 10 per page Go

Status: Type: Name:

	Status	Name	Type	Segments	Phone	IP Address
<input type="radio"/>	OK	ex62304	Cisco TelePresence C60	1	62304@cm1.example.com	209.165.201.6
<input type="radio"/>	OK	ex62305	Cisco TelePresence EX60	1	62305@cm1.example.com	209.165.201.7

Page 1 of 1

Table 11-29 *Configure > Endpoints Information*

Field	Description
Status	Display-only status report of system services
Name	Name of endpoint
Type	Model of endpoint
Segments	Number of endpoint segments
Phone	Phone number of endpoint
IP Address	IP address of endpoint

To add an endpoint to Cisco TelePresence Manager:

- Step 1** Go to the **Configure > Endpoints** window.
- Step 2** Click **New** to display the New Endpoint dialog box.
- Step 3** Enter the information, click **Save** and **Close**.
- To reload the most current list of endpoints, click **Refresh**.

**Note**

An endpoint displays as the Type “Other” if the model type does not exist in Unified CM.

Table 11-30 **Endpoint Settings**


Field	Description or Settings
Endpoint Type	Video Conferencing or EX or C Series.
Email ID	<p><Room/Endpoint mailbox ID>@<exchange or domino domain name>.</p> <p>For EX or C Series endpoints, after you enter the email ID, click Validate to ensure the email address is valid.</p>
Name (Video Conferencing endpoint only)	<p>Name of the video conferencing endpoint.</p> <p>Note This appears when the email ID is successfully validated.</p>
Location (Video Conferencing endpoint only)	<p>Physical location of the video conferencing endpoint.</p> <p>Note This appears when the email ID is successfully validated.</p>
Country (Video Conferencing endpoint only)	<p>Country where the video conferencing endpoints located.</p> <p>Note This appears when the email ID is successfully validated.</p>
TIP enabled (Video Conferencing endpoint only)	<p>Select this checkbox if this video conferencing endpoint is compatible with TelePresence Interoperability Protocol (TIP).</p> <p>Note TIP-enabled endpoints can use CTMS version 1.8 or later or TS for resource allocation. With endpoints that are not TIP-enabled, multipoint meetings require a CTMS.</p> <p>TIP-enabled endpoints do not require Interoperability with Video Conferencing to be enabled.</p> <p> Caution TelePresence Call-In Number must be enabled and set to always include a call-in number for TIP-enabled endpoint participants to dial into a meeting.</p>
Segments required for the type of video conferencing endpoint (Video Conferencing endpoint only)	<p>Set the number of segments for the video conferencing endpoint. Select 1, 2, 3 or enter the number in the Other field.</p>

Table 11-30 **Endpoint Settings**

Field	Description or Settings
IP Address	IP address of the endpoint.
Username (EX or C Series only)	Username of the EX or C series endpoint
Password (EX or C Series only)	Password of the EX or C series endpoint
Phone	Phone number of the endpoint. For EX and C series endpoints only, after you enter the username and password, click Validate . The phone (directory) number for the endpoint will appear.
Device Group (EX and C Series only)	Select the group to which you want to assign the endpoint. If you do not select a group, you can do it later in the Configure > Device Groups page.

Figure 11-39 **Video Conferencing Endpoint**

New Endpoint

Endpoint Type: Video Conferencing ▾

✱ Email ID: Validate

Name: Select Validate to retrieve the information

Location: Select Validate to retrieve the information

Country: Select Validate to retrieve the information

TIP Enabled: ☐

✱ Segments required for the type of Video Conferencing Room

☒ 1 ☐ 2 ☐ 3 ☐ Other

Phone:

IP Address:

✱ = Required fields

Save Close

Figure 11-40 EX or C-Series Endpoint

Importing Endpoints

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

To import endpoints:

Step 1 Create a .csv text file in the following format:

- **For EX or C series endpoints running TC5.0 or later software:**
 <fully qualified email address>, <number of segments>, <ip address>, <E.164 address (phone number)>, obtp, <username>, <password>
 Example:5033@ex1.com, 1, 10.22.146.142, 5033, obtp, admin, jpwd
- **For TIP-enabled video conferencing endpoints:**
 <fully qualified email address>, <number of segments>, <ip address>, <E.164 address (phone number)>, tiponly
 Example:5022@ex1.com, 1, 10.22.146.142, 5022, tiponly

- **For non-TIP-enabled video conferencing endpoints, or EX or C series endpoints running pre-TC5.0 software:**
 <fully qualified email address>, <number of segments>, <ip address>, <E.164 address (phone number)>
 Example: 5023@ex1.com, 1, 10.22.146.142, 5023

**Note**

The text file must have the .csv extension. Example: endpoint_import.csv. If the information is formatted incorrectly or includes an email ID that is already in use, the import will not be successful.

Step 2 Click **Import**.

The 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 **Upload**.

A message appears indicating the number of endpoints that will be imported from the file.

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

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

Creating Resource Bundle Endpoints

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

**Note**

A resource bundle endpoint consumes only one endpoint license.

To add a resource bundle endpoint to Cisco TelePresence Manager:

Step 1 Go to the Configure > Endpoints window.**Step 2** Click **New** to display the New Endpoint dialog box.**Step 3** For Endpoint Type, select **Video Conferencing**.**Step 4** In the Email ID field, enter a valid email address to be used exclusively by this resource bundle endpoint.**Note**

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

Step 5 In the Segments required for the type of Video Conferencing Room field, select or enter the number of desired segments.**Step 6** (Optional) Enter Phone and IP address.

Step 7 Click **Save** and **Close**.

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

Scheduling Meetings with Video Conferencing, EX and C-Series Endpoints

Scheduling TelePresence meetings with video conferencing (VC) or EX/C-series endpoints running TC4.x or earlier software endpoints is just like scheduling meetings with TelePresence endpoints.

A point-to-point meeting between an EX or C-series endpoint and a CTS is supported under the following circumstances:

- CTS is running software release 1.7.4 or later.
- CTS supports TIP and a CTMS has available resources.

A multipoint meeting with one or more EX or C-series endpoints requires a CTMS.

To schedule a meeting with VC, EX or C-series endpoints:

Step 1 Invite TelePresence endpoints and VC/EX/C series endpoints 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 meeting with video conferencing, EX or C-series endpoints must have at least one CTS endpoint. A meeting scheduled without a CTS endpoint will be marked as Not a TelePresence Meeting and CTS-Manager will not set up video conferencing interop or reserve any CTMS or interop resources for the meeting.



Caution

Unscheduled video conferencing, EX or C-series endpoints can join a scheduled meeting.

VC meetings Scheduled Before Upgrading to CTS-Manager Release 1.7 or 1.8

Any meeting scheduled with a VC endpoint (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 endpoint is added after upgrading to 1.7 or 1.8, a blue icon appears next to the VC endpoint name.
 - Interop meetings scheduled in 1.7 or 1.8 have both the VC Room icon and the Video Conferencing Interop checkmark.

- If VC room added in 1.6 is removed in 1.7 or 1.8, the Video Conferencing Interop checkmark remains.

**Note**

The TelePresence phone/display device will display an interop icon for an Interop meeting.

Live Desks

The Live Desk is the first person contacted when there are questions or problems pertaining to connecting meeting participants in a meeting.

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 understands how to perform the following tasks:

- Scheduling meetings
- Using the Cisco IP phone in a Cisco TelePresence-enabled endpoint
- 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 endpoints 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 (endpoints) that need a Live Desk assigned to them. Use the areas in this window to assign a Live Desk to an endpoint.

A phone number is associated with the Live Desk, which is displayed on the Cisco TelePresence endpoint phone/display device when the Live Desk soft key is pressed. Meeting participants can dial the Live Desk and ask for help if problems occur with the Cisco TelePresence system.

Figure 11-41 Configure > Live Desks Window

Live Desks

	ID	Phone Number	Description
<input type="radio"/>	jsmith	40075	John Smith
<input checked="" type="radio"/>	kjohnson	40076	Kent Johson

Rooms that have not been assigned :

List of Rooms Showing 1-5 of 5 10 per page

<input type="checkbox"/>	Status	Name	Phone	Description	IP Address
<input type="checkbox"/>	OK	conf_rm1@example.com	40071	Conference Rm 1	209.165.201.8
<input type="checkbox"/>	Error	conf_rm2@example.com	40078	Conference Rm 2	209.165.201.9
<input type="checkbox"/>	Error / In Use	conf_rm3@example.com	40072	Conference Rm 3	209.165.201.10
<input type="checkbox"/>	OK	conf_rm4@example.com	5528	Conference Rm 4	209.165.201.11
<input type="checkbox"/>	OK	conf_rm5@example.com	5529	Conference Rm 5	209.165.201.12

Assign selected endpoints to: Page 1 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 (Live Desk Number) field.
- Step 4** You can choose to supply other information identifying the Live Desk person in the Description field.
- Step 5** Click **Save** and then click **OK** in the confirmation window that appears.
- Step 6** To see the new Live Desk you added, you must refresh the page.



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 11-42 Adding a Live Desk Window

All Cisco TelePresence endpoints (rooms) must be assigned to a Live Desk. If you haven't specified a Live Desk for an endpoint, the System installed <Unassigned> Live Desk is the default Live Desk for all endpoints 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 (endpoint) 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 (endpoints) discovered by CTS-Manager will be assigned to the new default setting.

Assigning an Endpoint to a Specific Live Desk

Once Live Desks have been registered, the next step is to assign them endpoints (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, at the bottom of the page.
 - 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

Beginning in release 1.7, CTS-Manager supports a default Live Desk that is assigned to TelePresence rooms (endpoints) 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 1.9 from a version (earlier than 1.7) that allows a Live Desk to share a phone number with another Live Desk, CTS-Manager 1.9 changes the phone number of one of the Live Desks during the upgrade and assigns that Live Desk to the TelePresence room (endpoint).

Policies

The Policies window lists the three 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 11-43 *Configure > Policies Window*

The screenshot shows the 'Policy Management' window. It contains a table titled 'List of Available Policies' with columns for Policy Name, Policy Type, and Policy Description. There are three rows, each with a radio button in the first column. The first row is for 'Default' CTMS, the second for 'Default' CTS, and the third for 'Default' TS. Below the table is an 'Edit...' button. At the bottom right, it says 'Page 1 of 1' with navigation arrows.

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

Showing 1-3 of 3 10 per page Go

Edit...

Page 1 of 1

CTMS Policy

Describes the switching policy for multipoint meetings. The switching mode can be set to either Speaker or Room (endpoint) switching:

- **Speaker:** Individual speakers are displayed on the screen when that meeting participant becomes the active speaker.
- **Room:** All speakers in a particular room are displayed on screen when any participant in that room is the active speaker.

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 11-44 CTMS Policy Window

Edit...Policies	
✱ = Required fields	
Name:	Default
Type:	CTMS
✱ Description:	This is the Default CTMS Policy
Switching Mode:	Speaker ▼
Number of days pushed to CTMS:	14
<div>Save Close</div>	

CTS Policy

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

Figure 11-45 CTS Policy Window

Edit...Policies	
✱ = Required fields	
Name:	Default
Type:	CTS
✱ Description:	This is the Default CTS Policy
Number of days pushed to phone:	14
<div>Save Close</div>	

TS Policy

Determines the number of days of scheduled meetings pushed to each TelePresence Server. The default is 14 days. The range is from 1 to 30 max. Also you can view, enable or disable the lobby screen message. The lobby screen is the message that appears when an endpoint joins the meeting.


Note

The lobby screen message can only be configured on the TS.

Figure 11-46 TS Policy Window

Edit...Policies	
⚙️ = Required fields	
Name:	Default
Type:	TS
Description:	<input type="text" value="This is the Default TS Policy"/>
Number of days pushed to TS:	<input type="text" value="14"/>
Display Lobby Screen Message:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Lobby Screen Message:	<input type="text" value="You are the first participant in the meeting. Please Wait."/>
<div>Save Close</div>	

Application Settings

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

- Email
- Bridges and Servers
- Locales
- Benefits Reporting
- 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 11-47 *Configure > Application Settings > Email Window*

Application Settings

Email Bridges and Servers Locales Benefits Reporting 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.

URL to Be Displayed in Email:

Remove Email Prefixes from Meeting Subject on Phone

Enable Feature: ☐ Yes ☒ No

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

Additional Text in Email:

English (United States)

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.

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

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.

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.

With this feature enabled, prefixes are automatically removed from the subject line of TelePresence email subject line that is displayed on the TelePresence phone/display device.

For example: "Re: TelePresence Meeting" would change to "TelePresence Meeting"

Additional Text in Email

This feature allows you to add custom additional text to appear in the email notification header. You can add specific text for each selected locale in CTS-Manager. Text can be up to 4096 characters in length.

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](#).

Bridges and Servers

In the Bridges and Servers tab, you can configure multipoint conference scheduling, interoperability with video conferencing, TelePresence call-in number, recording, WebEx, and Intercompany settings.

Figure 11-48 *Configure > Application Settings > Bridges and Servers Tab*

Application Settings

Email **Bridges and Servers** Locales Benefits Reporting Usage Survey Meeting Options

Multipoint Conference Scheduling
 Primary Scheduling Device: ☒ CTMS ☐ TelePresence Server
☐ Use TelePresence Server when required (for more information, see Help.)

Interoperability with Video Conferencing
 Enable Feature: ☒ Yes ☐ No

Interop Devices
 When CTMS is Used for Scheduling:

Telepresence Call-In Number
☐ Allow meeting organizers to send a call-in number for unscheduled TelePresence endpoints to join?

Studio Mode Recording
 Enable Feature: ☐ Yes ☐ No

WebEx
 Enable Feature: ☒ Yes ☐ No
 Default User Type: ☒ Permitted ☐ Non-Permitted

CTMS Network Multipoint
 Enable Feature: ☐ Yes ☒ No

Intergroup Scheduling
☐ Allocate resources from another group if the first group used for scheduling has insufficient resources for a multipoint meeting.

Intercompany
 Enable Feature: ☐ Yes ☐ No
 Provider: ☒ Another Company Hosts ☐ Our Company Hosts

Apply Cancel

Multipoint Conference Scheduling

This section appears only if you have both CTMS and TelePresence Server (TS) devices. You can select the device that will be used as the primary scheduling device. This is the device that CTS-Manager attempts to use first when allocating resources for a meeting. Either CTMS or TS can be used, as long as they are configured in CTS-Manager and in a scheduled state. If you have both CTMS and TS devices, you can check the checkbox below the Primary Scheduling Device, so that when the Primary Scheduling Device is out of segments or incompatible with certain features, CTS-Manager will automatically select the other type of scheduling device.

If you have the following features enabled and select TS as the primary scheduling device, you must select “Use CTMS when required.”

- WebEx
- Intercompany

TelePresence Server supports interop with video conferencing without additional interop devices. (add note about meeting extension feature of CTS-Manager is only compatible with CTMS).

**Note**

To use these features with TS as the primary scheduling device, requires a CTMS device and “Use CTMS when required” must be selected.

To add a CTMS or TS to CTS-Manager, go to Configure > Bridges and Servers.

Interoperability with Video Conferencing

Enable Feature: This allows you to enable interoperability with video conferencing. It is disabled by default. This feature cannot be disabled once it has been enabled.

When the setting is greyed out:

- (CTMS only) If it is disabled and grayed out, there is at least one TelePresence endpoint or bridge or server device that is not interop-ready. All TelePresence endpoints and CTMS devices (if selected under Multipoint Conference Scheduling) must support interop before you can enable Interop settings. Make sure all devices discovered by CTS-Manager are running interop-enabled software releases.

**Note**

When Interoperability with Video Conferencing is enabled, multipoint meetings require a CTMS in a scheduled state or a TS.

Interop Devices: The interop device that is used is selected based on the device used for scheduling of a meeting. If CTMS is used for scheduling, the device selected for “When CTMS is Used for Scheduling” will be used for Interop. If TelePresence Server is used for scheduling, it will be used as the interop device.

**Caution**

Support for CUVC in scheduled interop meetings is no longer supported in CTS-Manager 1.9. Existing meetings scheduled with CUVC interop will continue to work, but new meetings with CUVC interop are no longer supported.

For CTMS, you select the device and resolution setting on a global basis by using the “When CTMS is Used for Scheduling” menu. For all future meetings, updates affected CTMSs with the new setting by pushing updated conference schedules.

**Note**

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

The device and resolution setting selection is maintained by CTS-Manager and pushed to CTMS for each individual meeting.

Once HD Interop is configured in CTS-Manager, CTS-Manager always reserves HD Interop resources.

**Note**

When upgrading from 1.7 or 1.8 to 1.9, the CUVC option will no longer be available.

TelePresence Call-In Number

The TelePresence Call-In Number feature allows a meeting organizer to permit Cisco TelePresence endpoints that were not in the meeting's original invitation to join the meeting. For more information, see http://www.cisco.com/en/US/docs/telepresence/cts_manager/1_8/call_in_number.html

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 recording is enabled for a single meeting and that meeting is changed to a recurring meeting, all occurrences of that meeting will have recording enabled.

To enable recording globally:

-
- Step 1** In Microsoft Outlook or Notes, schedule a single meeting with one endpoint.
 - Step 2** Log in to the CTMS administration interface as an Administrator.
 - Step 3** Go to **Configure > Application Settings >** and click the **Bridges and Servers** tab.
 - Step 4** Set Studio Mode Recording to **Yes**.
 - Step 5** From Microsoft Outlook or Lotus Notes, select this meeting and modify it as a recurring meeting.
 - Step 6** All meeting instances now have recording enabled.
-

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.

**Tip**

You can assign specific LDAP groups to have different WebEx permissions in the **Configure > Access Management** window.

**Note**

For WebEx to work, all CTS endpoints and CTMS devices initially installed must have 1.7 or later software. In addition, all CTMSs must have WebEx configured.

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

**Note**

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

CTMS Network Multipoint

CTMS Network Multipoint allows multipoint meetings that exceed the resources of a single CTMS to automatically reserve resources on one or more additional CTMSs, allowing for larger-scale multipoint meetings.

Enable Feature: This allows you to enable Network Multipoint. It is disabled by default.

For details on how to configure and deploy CTMS Network Multipoint and how this feature works, refer to Chapter 2, “Network Multipoint Design for Scheduled Meetings,” in the CTMS Network Multipoint Design Guide for release 1.9 at the following URL:

http://www.cisco.com/en/US/docs/telepresence/multipoint_switch/1_9/design/guide/CTMS_Network_Multipoint_Design.html

**Note**

This feature is only compatible with CTMS devices.

Intergroup Scheduling

This allows resources from another device group to be allocated if the first device group used for scheduling has insufficient resources for a multipoint meeting. Device groups are configured on the **Configure > Device Groups** page.

This feature is automatically enabled, when CTMS Network Multipoint is enabled, but can be disabled later.

To enable this feature, click the checkbox for ‘Allocate resources from another group if the first group used for scheduling has insufficient resources for a multipoint meeting.’

For more information about Device Groups, go to [Device Groups, page 11-78](#).

Intercompany

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) endpoints to your meeting. EX and C series endpoints are supported only.

The Provider setting allows you to select “Another Company Hosts” and/or “Our Company Hosts.” You can select both if you want meeting organizers to have both capabilities. The meeting organizer can choose one or the other depending on whether your company is going to host the meeting or the meeting will be hosted by another company. The host designated for a recurring meeting will be the host for all occurrences of that meeting.

Another Company Hosts

If you select this feature, this allows another company to set up TelePresence meetings. You must provide the host with the endpoints’ information that will be participating in the TelePresence calls. For example, if it is a room-to-room call it will 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 endpoints, and get dial-in and endpoint information from the other company before setting up the TelePresence meeting.



Caution

Once this feature is enabled, the only way to disable it is to reinstall CTS-Manager.

Locales

The Application Settings > Locales window allows you to install locales for Meeting Manager and meeting organizer email notifications.

A Locale is the language used in a specific country/region. When a locale is installed, the following things are available in that locale to the meeting organizer who selects that locale when using CTS-Manager:

- All emails sent to the meeting organizer
- Meeting Manager



Warning

The Locales feature is not currently available. It will be available in a future release of Cisco TelePresence Manager.

Selecting and Publishing Locales for Meeting Manager and Meeting Organizer Email Notifications

To select and publish locales for Meeting Manager organizer email notifications:

Step 1 From the list of available locales on the left, choose the locale(s) you want to select for use with Meeting Manager and meeting organizer email notifications.

The selected locales appear in the selected column, on the right and also appear in the Locale Settings section at the bottom of the window.

Step 2 In the Locale Settings section, select a default locale that meeting organizers will see when they log into Meeting Manager for the first time. Click the Default radio button for the locale you want to be the default.

**Note**

The meeting organizer can switch to another of the available locales the first time or any subsequent time they log in Meeting Manager.

Step 3 (Optional) You can create a customized survey for each selected locale. To customize a survey, click the **Customize** link for the locale(s) you want to customize.

Step 4 To save the selected locales, click **Apply**.

This saves the locale settings in CTS-Manager, but the new locales are not available yet to meeting organizers. If you want to customize a usage survey, click the

Step 5 To make selected locales available to meeting organizers, click **Publish All Locales**.

**Note**

You have the option of adding additional text in the emails that CTS-Manager sends to meeting organizers for each locale. To add the additional text, click the **Email** tab and enter the text in the Additional Text in Email field(s).

Benefits Reporting

The Application Settings > Benefits Reporting window allows your company to form financial justifications for your deployment of Cisco TelePresence solutions. This feature allows the administrator to measure TelePresence usage, endpoint utilization, ROI of TelePresence deployment, compute savings from travel elimination, and display meaningful data. The benefits information is displayed in the Monitor > Metrics Dashboard, and Meeting Benefits windows.

Figure 11-49 *Configure > Application Settings > Benefits Reporting*
Enable Meeting Benefits Report

To enable the meeting benefits report feature:

- 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 TelePresence and VC 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

Table 11-31 *Meeting Benefits Parameters*

Benefit	Description
Work Hours per Day	Number of hours in normal work day
Work Days per Week	Number of days in normal work week
Carbon Emissions per Trip (Tons)	Number of carbon emissions in average business trip
Employee Hourly Cost (\$)	Average hourly cost for each employee
Trips Eliminated per Meeting	Average number of business trips eliminated by a TelePresence meeting
Travel Hours per Trip	Average number of travel hours for each trip
Cost per Trip	Average cost for each trip

Usage Survey

The Application Settings > Usage Survey window allows you to create and customize a usage survey. You can create a survey based upon what information your company wants to gather from each meeting. 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.

Answers from the first three questions appear in the Metrics Dashboard. To collect the answers from additional questions, use the Reporting API.

Figure 11-50 *Configure > Application Settings > Usage Survey Window*

Application Settings

Email Bridges and Servers Locales Benefits Reporting **Usage Survey** Meeting Options

Enable Meeting Organizer Usage Survey

☐ Yes ☒ No

Select a locale to preview or customize survey:

Locale Settings					
Locale	Default	Questions	Organizers	Last Published Date	Survey Last Customized
<input checked="" type="radio"/> English (United States)	Yes	3	1	N/A	Customize

Preview Survey Questions - English (United States)

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

To enable the usage survey feature:

- Step 1** Select the **Yes** radio button.
- Step 2** Click **Apply**.



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 TelePresence Utilization windows.

Select a Locale to Preview or Customize Survey

In the Locale Settings section, you can see information about the usage surveys for each locale, including:

- Default: The survey that meeting organizers will see if they use the default locale.
- Questions: The number of questions in the survey
- Organizers: The number of meeting organizers using the locale
- Last Published Date: The last date/time the survey was published
- Survey Last Customized: The last date/time the survey was customized.

**Note**

If a survey has not yet been customized, a Customize link will appear.

**Caution**

The Locales feature is not currently available. It will be available in a future release of Cisco TelePresence Manager.

Preview Survey Questions

Three survey questions are included by default and their results are displayed on the Metrics Dashboard:

- Purpose - For capturing the main purpose of the meeting
- Benefit - For capturing the primary benefits of the meeting
- Trips - For capturing how many business trips the meeting is eliminating

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

To add more questions, click the **Customize** button.

**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**.

Customizing the Survey

To customize the usage survey, click **Customize**.

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 11-51 Usage Survey Customization Wizard

Welcome

Question 1

Question 2

Question 3

Preview

Welcome to the Usage Survey Customization Wizard

[Help](#)

Locale: English (United States) (Default)

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

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 Reporting 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, only data collected after the change will be used for the Metrics Dashboard.

How many total questions do you want?

1: What is the purpose of this meeting?

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

3: How many trips eliminated?

[Next](#) [Cancel](#)

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

Click **Next** to go to the first default question.

Survey 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.

Survey Questions 1 and 2 are multiple choice questions that require at least two possible choices (answers). You can have up to 10 possible choices. You can change the questions and any of the choices, but the questions must remain multiple choice. You can add a free-form text box answer, where the meeting organizer can type their own answer, by clicking the checkbox for **Include an “Other” option with a free-form text entry**.

**Note**

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.

Question 3 is a number question that requires one choice (answer). You cannot add any additional choices. You can change the question, but the question must remain a number question.

Results from question 3 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.

Additional Questions

For additional survey questions, you can define the type of question. The possible question response types are:

- Multiple Choice
- Number
- Text

You can have up to 10 possible choices.

Figure 11-52 *Customize Your Question 1*

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** Make any necessary changes to the answers and add any new ones if you need to.
 - Step 3** Click **Next**.
 - Step 4** Review and modify, if necessary, the next two default questions and their answers.
-

**Note**

When customizing the question 2, 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 13-19](#).

Figure 11-53 Creating a New Question

Welcome

Question 1

Question 2

Question 3

Question 4

Preview

Customize Your Question 4 [Help](#)

Locale: English (United States) (Default)

Question: Where do you want the offsite meeting to be?

Response Type: Multiple-Choice

Choices

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

#1: Local hotel

#2: Las Vegas

#3: San Francisco

#4: Hawaii

#5:

#6:

#7:

#8:

#9:

Back Next Cancel

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.

Editing Additional Questions

After you initially create an additional question and click Next to go to the next/previous question or the preview page, you can go back to the question later to make changes the actual question, but the response type cannot be changed. To change the response type of an additional survey question, you must delete and recreate it.

Deleting Additional Questions

You can delete additional survey questions by doing the following:

-
- Step 1** Go back to the Welcome page of the survey customization wizard (using the back button or opening the wizard again, if you are making changes to an existing survey).
 - Step 2** Click the checkbox next to the additional question you want to delete.
 - Step 3** Click **Next**.
 - Step 4** If the survey is the default locale survey, a confirmation message appears. To delete the selected question, click **OK**.

The question is deleted and the first question of the survey appears.

Preview Your Questions

When you click Next on the last question of your survey, you preview your survey before you finish customizing it. If you find anything you want to change, simply click the Back button until you reach the question you want to change, make the changes and click Next the appropriate number of times to arrive back at the preview page to review your changes. This window appears after you finish customizing all of your questions.

Figure 11-54 Preview Your Survey Questions

Preview Your Questions [Help](#)

1. What is the purpose of this meeting?

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

3. How many trips eliminated?

4. Where do you want the offsite meeting to be?

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**.

Publishing Your Survey

To make your customized survey available to all meeting organizers, you must publish it.

To publish your survey, click **Publish All Locales**.

Changing the Default Survey

To change the default survey that meeting organizers will see when they log into Meeting Manager for the first time:

-
- Step 1** Click the Default radio button for the locale survey you want to be the default.
 - Step 2** Click **Publish All Locales**.
-

Default Survey Questions

Three survey questions and answers are included by default:

- [Question 1](#)
- [Question 2](#)
- [Question 3](#)

Question 1

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
- Friend & Family
- Internal

Question 2

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

Question 3

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

Question:

- How many trips eliminated?

Answer:

- *User enters a number.*

**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**.

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 11-55 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 11-55 *Configure > Application Settings > Meeting Options*

Application Settings

Email Bridges and Servers Locales Benefits Reporting Usage Survey **Meeting Options**

Enable Tentative Room Reservations

☐ Yes ☒ No

Once this feature is enabled, it cannot be disabled.

Start Meetings Early

☐ Do not allow meetings to start before the scheduled time

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

Extend Multipoint Meetings

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

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

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

☐ Always extend ☒ Extend, if resources are available

☐ Allow these meeting organizers to extend meetings

Meeting Extension Premium Users (minutes):

As of Tue, 4 Oct 2011 16:32:19 +0000 there were 0 Meeting Extension Premium Users [Details](#)

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

Apply Cancel

Enable Tentative Room Reservations

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

This option is supported only with Microsoft Exchange.

**Caution**

For tentative room reservations to work, the Logon Name for Microsoft Exchange must be provided in the Configure > Microsoft Exchange > Configuration tab.

**Note**

Upgrading from CTS-Manager 1.7 to 1.9: If you had tentative room reservations enabled in 1.6, this setting is maintained when upgrading to 1.9, but you must re-enable tentative reservations on each room individually in the Support > Endpoints > Capability window.

A tentative room reservation is a meeting invitation that has been viewed by the room (endpoint) owner or a proxy room (endpoint) owner, but not accepted yet. ‘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 endpoint for meetings. A CTS-Manager tentative reservation is identical to an accepted reservation.

(Microsoft Exchange Only) Cancelling a Meeting that Contains a Tentative or Proxy Room (Endpoint)

After the meeting organizer cancels a meeting, tentative or proxy room owners may have to log in to the room (endpoint) calendar and remove the meeting from the calendar:

- Exchange 2003: Tentative or proxy room owner must log in to room (endpoint) mailbox, and remove the meeting from the calendar.
- Exchange 2007/2010:
 - If the **Autoprocessing** parameter for the room (endpoint) is set to ‘None’, the tentative or proxy room owner must log in to the room (endpoint) mailbox, and remove the meeting from the calendar.
 - If the **Autoprocessing** parameter for the room (endpoint) is set to ‘AutoUpdate’, no action is required by the tentative or proxy room owner, because the meeting is automatically removed when the meeting organizer cancels the meeting.

**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 endpoints 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 (endpoint) 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.



Note

This feature is not compatible with TelePresence Server.

Extend Multipoint Meetings

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

To enable this feature, the following are required:

- At least one CTS that supports this feature
- All CTMS devices must support this feature



Note

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

Support for TelePresence Server

CTS-Manager 1.9.1 or later supports Extend Multipoint Meetings with TelePresence Server. TelePresence Server only supports the options that always extend meetings. For meetings that use TelePresence Server, no button is displayed on the phone or display device prompting the meeting organizer/participant to extend the meeting. The meeting is extended automatically.

Prerequisites

The following are required to enable the Extend Meetings feature:

- At least one CTMS version 1.7 or later or TelePresence Server (if using CTS-Manager 1.9.1 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 > Endpoints** 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 must 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). (Not supported with TelePresence Server)

- **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. (Not supported with TelePresence Server)
- **Allow all meeting organizers to extend meetings up to (minutes)** - Select either 15, 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. (Not supported with TelePresence Server)
- **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 15, 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 15, 30 or 60 minutes. (Not supported with TelePresence Server)



Note When switching from the “Meeting Extension Premium Users” option to the “If resources are available” option, 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.

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** Go to **Configure > Database** and click the **Restore** tab.
 - Step 4** 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 11-56 *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: *

Restored Backup Files History Showing 0-0 of 0 10 per page

Time	Status	Type	Hostname	Location
No data to display				

Page 0 of 0

Step 5 Next, perform a resync with the Microsoft Exchange or IBM Domino database from the backup CTS-Manager.

Figure 11-57 *Configure > Microsoft Exchange > Synchronization Tab*

Microsoft Exchange

Synchronization Configuration

Synchronization Operations Showing 1-4 of 4 10 per page

Subscription Status: Sync Status: Type: Endpoint

<input type="checkbox"/>	Endpoint Name	Type	Sync Status	Last Synchronization Time	Subscription Status
<input type="checkbox"/>	dn45003	CTS 1000	✓	10/02/2011 05:05 PM	✓
<input type="checkbox"/>	dn70000	CTS 1100	✓	10/02/2011 05:05 PM	✓
<input type="checkbox"/>	ex62304	Cisco TelePresence C60	✓	10/02/2011 05:05 PM	✓
<input type="checkbox"/>	ex62305	Cisco TelePresence EX60	✓	10/02/2011 05:05 PM	✓

Page 1 of 1

Step 6 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 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** Go to **Configure > Database** and click the **Restore** tab.
- Step 4** 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 11-58 *Configure > Database > Restore*

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 Scheduled option of the primary CTMS to **No**.
- Step 3** Change the Scheduled option of the backup CTMS to **Yes**.
-

Figure 11-59 *Configure > Bridges and Servers Edit Window*

Edit Bridge or Server

Hostname: example-ctms

✱ Username: admin

✱ Password:

Device Group: Paris

Scheduled: ☐ Yes ☒ No

Migrate All Meetings: ☐ example-ctms

Timezone: America/Los_Angeles****true

Call-In Numbers: 20000

Segment Count: 24

✱ = Required fields

Save 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.