



## CHAPTER 9

# Additional Installation Configurations for Cisco TelePresence Manager

---

Revised: June 11, 2009, OL-13673-04  
First Published: November 27, 2006

## Contents

- [Post-Install Guidelines for CTS-Manager, page 9-2](#)
- [Introduction, page 9-3](#)
- [Security Settings, page 9-3](#)
- [Digital Security Certificates, page 9-4](#)
  - [Generating Security Certificate Reports, page 9-5](#)
  - [Viewing Security Certificates, page 9-5](#)
  - [Deleting Security Certificates, page 9-5](#)
  - [Uploading Security Certificates, page 9-5](#)
- [LDAP Server, page 9-6](#)
- [Field Mappings, page 9-8](#)
- [Password, page 9-12](#)
- [Calendar Server, page 9-12](#)
- [Microsoft Exchange, page 9-17](#)
  - [Re-sync Operations, page 9-19](#)
- [IBM Domino, page 9-20](#)
- [System Settings, page 9-23](#)
- [Database - Status, Backup, and Restore, page 9-28](#)
  - [Settings, page 9-28](#)
  - [Changing the Backup Schedule, page 9-30](#)
  - [Backing Up Database Files, page 9-31](#)
  - [Viewing Backup History, page 9-32](#)
  - [To restore data from a backup:, page 9-34](#)

- [Discovery Service](#), page 9-34
- [MCU Devices](#), page 9-35
- [Access Management](#), page 9-37
- [Cisco TelePresence Multipoint Switch \(CTMS\)](#), page 9-38
- [Cisco Unified Video Conferencing \(CUVC\)](#), page 9-39
- [Concierges](#), page 9-41
- [Policy Management](#), page 9-44
- [Remote Account](#), page 9-46
- [System Configuration - System Settings](#), page 9-47
- [Application Settings](#), page 9-48
  - [Interoperability with Video Conferencing Settings](#), page 9-48
  - [Intercompany Setting](#), page 9-48
  - [Meeting Notification Email Settings](#), page 9-49
- [CTS-Manager Redundancy Failover Procedure](#), page 9-49

## Post-Install Guidelines for CTS-Manager

The purpose of this guide is to outline the information you will need to reference in order to configure the system after installing the CTS-Manager.

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

**Table 9-1** *Post-Install Guidelines for Configuring CTS-Manager*

Set-Up 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 as synchronizing system databases, managing security, and reconfiguring system settings	Current chapter.
Monitoring CTS-Manager	Describes the support features available when you log into CTS-Manager using a Concierge role.	<a href="#">Chapter 10, “Monitoring Cisco TelePresence Manager”</a>

If at any time you encounter problems, go to [Chapter 13, Troubleshooting Cisco TelePresence Manager](#) to see how to correct the problem.

# Introduction

The administrator makes use of the System Configuration window to perform additional tasks such as:

- upgrading system software
- synchronizing system databases,
- managing security
- reconfiguring system settings.

Figure 9-1 shows the system configuration tasks.

**Figure 9-1** Cisco Telepresence Manager System Configuration Window

**Host:** tsbu-ctm18

**System Information**

SKU:	CTS-MAN1.5
Hostname:	tsbu-ctm18
IP Address:	172.28.68.165
Subnet Mask:	255.255.252.0
MAC Address:	00:1a:4b:33:2f:ec
Hardware Model:	7835H2
Software Version:	1.5.0.0 (380)
OS Version:	UCOS 4.0.0.0-7

**Product Software Versions**

Product Name	Supported	Actual
Microsoft Exchange	[08.00.10685, 08.01.10240, 6.5.6944, 6.5.7226, 6.5.7638]	6.5.7638
Active Directory	[2003]	2003
Cisco Unified Communications Manager	[6.1.3]	7.0.1.11001(5)

**System Status**

**Today's Meetings:**

With Error:	2
In Progress:	0
Scheduled:	1

**Other Errors:** 4

## Security Settings

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

Figure 9-2 System Configuration Security Settings Window

System Configuration > Security Settings

Web Services Security: ☐ Secure ☒ Unsecure Apply Reset

Digital Security Certificates

Category: All Unit: All Filter

Showing 1 - 2 of 2 records

	Unit	Category	Certificate Name
<input type="radio"/>	CTM-trust	TRUST	tsbu-ctm23.pem
<input checked="" type="radio"/>	tomcat	OWN	tomcat.pem

Upload Download LSC View Delete

## Web Services Security

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



### Caution

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

## Digital Security Certificates

CTS-Manager supports the following security certificates:

- Tomcat—Security Keystore to store self-generated Apache Tomcat certificates.



### Note

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

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

## Generating Security Certificate Reports

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

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

## Viewing Security Certificates

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

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

## Deleting Security Certificates

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

**Note**

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

## Uploading Security Certificates

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

**Caution**

You cannot upload a certificate of the same name. You should delete the existing certificate before uploading a new one.

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

# LDAP Server

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



## Note

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

This window specifies LDAP Directory Server settings that are used by CTS-Manager to access the directory information. Open the LDAP Server window to see the following choices:

- [Settings for LDAP](#)
- [Field Mappings](#)

## Settings for LDAP

The Settings window is where you make changes to the LDAP server after first-time installation.

**Figure 9-3** LDAP Window Settings Tab

System Configuration > LDAP Server

**Settings** | Field Mappings

Service Status:	OK		
Host:	tsbu-sr6		*
Bind Method:	<input type="radio"/> Secure <input checked="" type="radio"/> Normal		
Port:	389		*
Default Context:	DC=srdev,DC=com	<input type="button" value="Fetch DNs"/>	*
Username:	cn=administrator,cn=users	<input checked="" type="checkbox"/> Append default context	*
Password:	.....		*
Certificate:		<input data-bbox="730 1339 824 1360" type="button" value="Browse..."/>	
Connection Pool Size:	1		*
User Containers:	cn=users	<input checked="" type="checkbox"/> Append default context	*
		<input type="checkbox"/> Append default context	
		<input type="checkbox"/> Append default context	
		<input type="checkbox"/> Append default context	
		<input type="checkbox"/> Append default context	

\* Required Fields

## 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`

Step 1

Test Connection.

Step 2

Apply.

Step 3

Reset



Note

container is the child of the other. This requirement includes specifying the default context.

Table 9-2 describes the settings for the LDAP Server window.

**Table 9-2 LDAP Server Settings**

Field or Button	Description or Settings
Service Status	Display-only status of the service.
Host	LDAP server host name.
Bind Method	Click the <b>Secure</b> or <b>Normal</b> radio button to select the binding method: <ul style="list-style-type: none"> <li>Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server.</li> <li>Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP.</li> </ul>
Port	The default port for secure connection is 636. The default port for normal connection in a single LDAP server deployment is 389. In cases where deployments consist of multiple LDAP Directory Servers, this port should be configured with 3268, which is the Global Catalog port. Secure Global Catalog port is 3269.
Default Context	The default context from which the LDAP queries are performed. To change the context string: <ul style="list-style-type: none"> <li>Click the Fetch DN's button and choose the context from the Fetch DN's drop-down list adjacent to this field.</li> </ul>

*LDAP Server Settings (continued)*

Field or Button	Description or Settings
Username	The username used to authenticate to the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: cn=adminstrator,cn=users,dc=<mydomain>,dc=com)
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.
Connection pool size	The number of concurrent connections used by the Cisco TelePresence Manager server to retrieve data from the LDAP server. This is primarily used for optimizing the server's access to the LDAP server.
User containers	<p>The containers from which queries are performed to retrieve user objects. More than one user container or user object can be specified. The Cisco Telepresence server uses the values entered to search through the containers in sequence to retrieve user and meeting room information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication.</p> <ul style="list-style-type: none"> <li>To append the default context, check the Append default context box next to the user container field.</li> </ul> <p><b>Note</b> If you have a LDAP peer domain configured you'll need to specify any user containers and context. For example, "cn=users,dc=domain2,dc=com". When specifying the container and context information for your peer domain, DO NOT check the Append default context box.</p>

## 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.

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 9-3](#) 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 9-4** LDAP Window Field Mappings Tab

The screenshot shows the 'System Configuration > LDAP Server' window with the 'Field Mappings' tab selected. It displays two sections: 'Person' and 'EnterpriseConfRoom'. Each section has a table with 'Object Class' and 'Attribute' columns. The 'Person' section has three rows: SchedulerName, EmailID, and DisplayName. The 'EnterpriseConfRoom' section has two rows: EmailID and DisplayName. A 'View Sample Data' button is located at the bottom right.

	Object Class	Attribute
SchedulerName:	Person	proxyaddresses
EmailID:	Person	proxyaddresses
DisplayName:	Person	displayname

	Object Class	Attribute
EmailID:	Person	proxyaddresses
DisplayName:	Person	displayname

[View Sample Data](#)

## 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 *proxyAddresses* 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 9-3](#) describes the settings for this window

**Table 9-3** LDAP Objects and Attributes

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

## IBM Domino Deployment s

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

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



### Caution

The object and attribute mappings for Domino/Directory Server deployments are listed in [Table 9-4](#) and cannot be changed after installing and configuring CTS-Manager.

**Figure 9-5** LDAP Window Field Mappings Tab

System Configuration > LDAP Server

Settings **Field Mappings**

**Person**

	Object Class	Attribute
SchedulerName:	Person	cn
EmailID:	Person	cn
DisplayName:	Person	cn

[View Sample Data](#)

**Table 9-4** LDAP Objects and Attributes

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

**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 Object Class field and the LDAP Attribute field do not need to be changed. Cisco TelePresence Manager may not function properly if the Object Class fields and LDAP Attribute fields are changed.

**Caution**

Setting the LDAP objects and attributes used by the Domino server requires experience using Directory Server and Domino software. Do not change the 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 Domino server administrator for your deployment before changing the default mappings in these screens.

## Password

Use the System Settings window to change the 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 9-6** System Configuration - System Settings Window Password Tab

The screenshot shows the 'System Configuration > System Settings' window with the 'Password' tab selected. The 'Username' field is populated with 'admin'. Below it are three password fields: 'Current Password', 'New Password', and 'New Password (verify)'. Each password field has a red asterisk icon to its right. At the bottom right of the form are 'Apply' and 'Reset' buttons.

- Step 1** To display the password fields, click on the tab, **Password**.
- Step 2** Type in your current password.
- Step 3** Then, to change password, go to **New Password** field and type your new password, using only English characters.
- Step 4** In the **New Password (verify)** field, repeat your new password to verify it.
- Step 5** To register the new password, click **Apply**.
- Step 6** To restore to the original password, click **Reset**.



**Note** Make sure you keep your password secure and that it follows standard password guidelines, minimum 6 letters.

## 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.

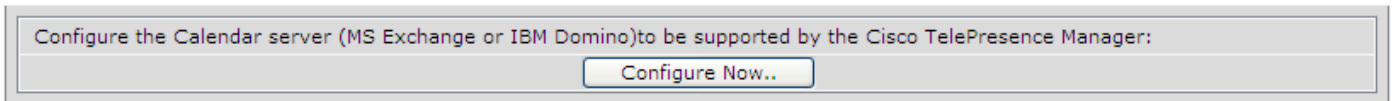
The Calendar Server wizard leads you through a four-step process to register a Calendar server with CTS-Manager.

**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.

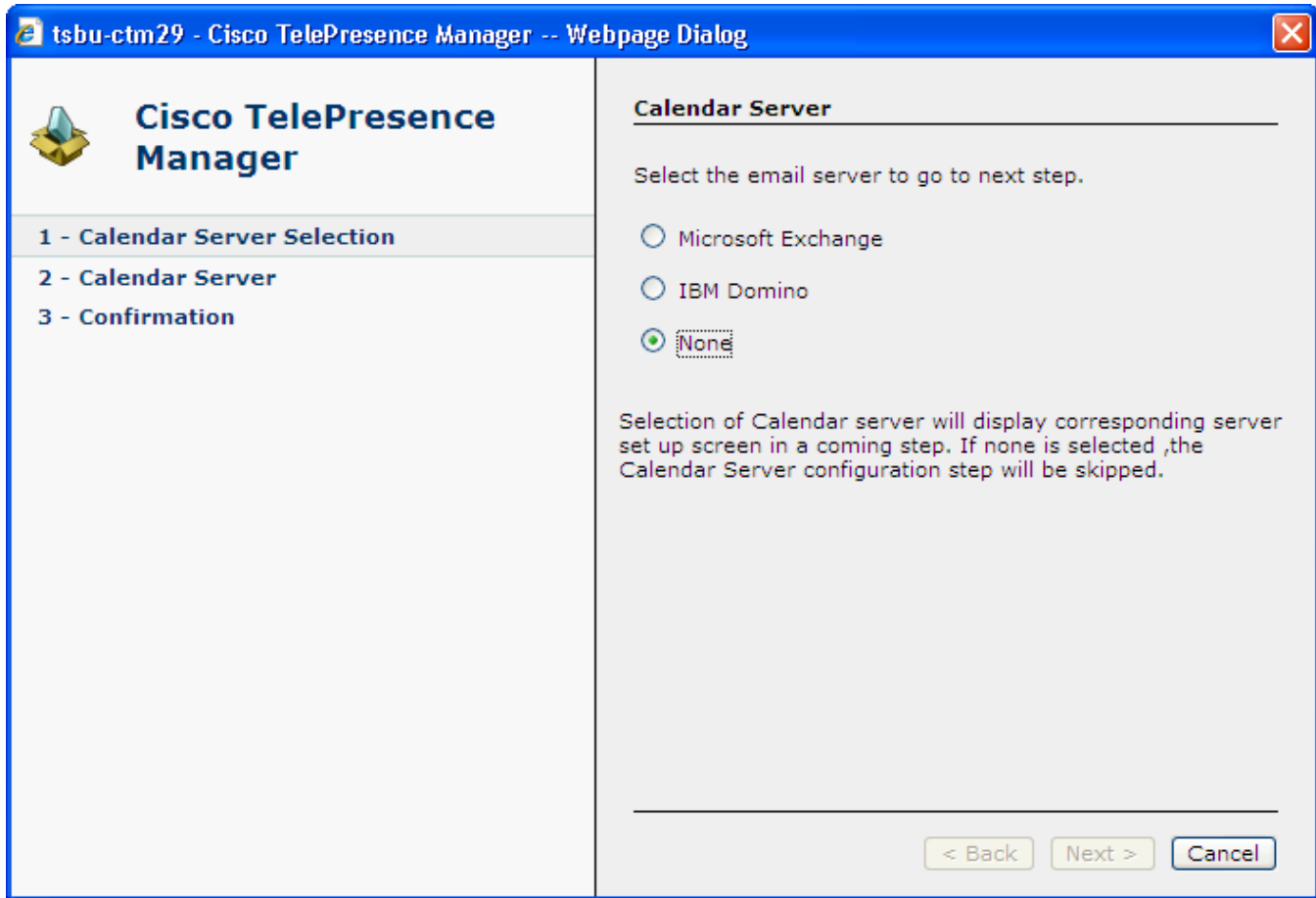
The No Calendar Server window displays the **Configure Now** button to initiate the Calendar Server wizard.

**Figure 9-7**      *Configure 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 9-8 Cisco TelePresence Manager - Calendar Server Selection Screen



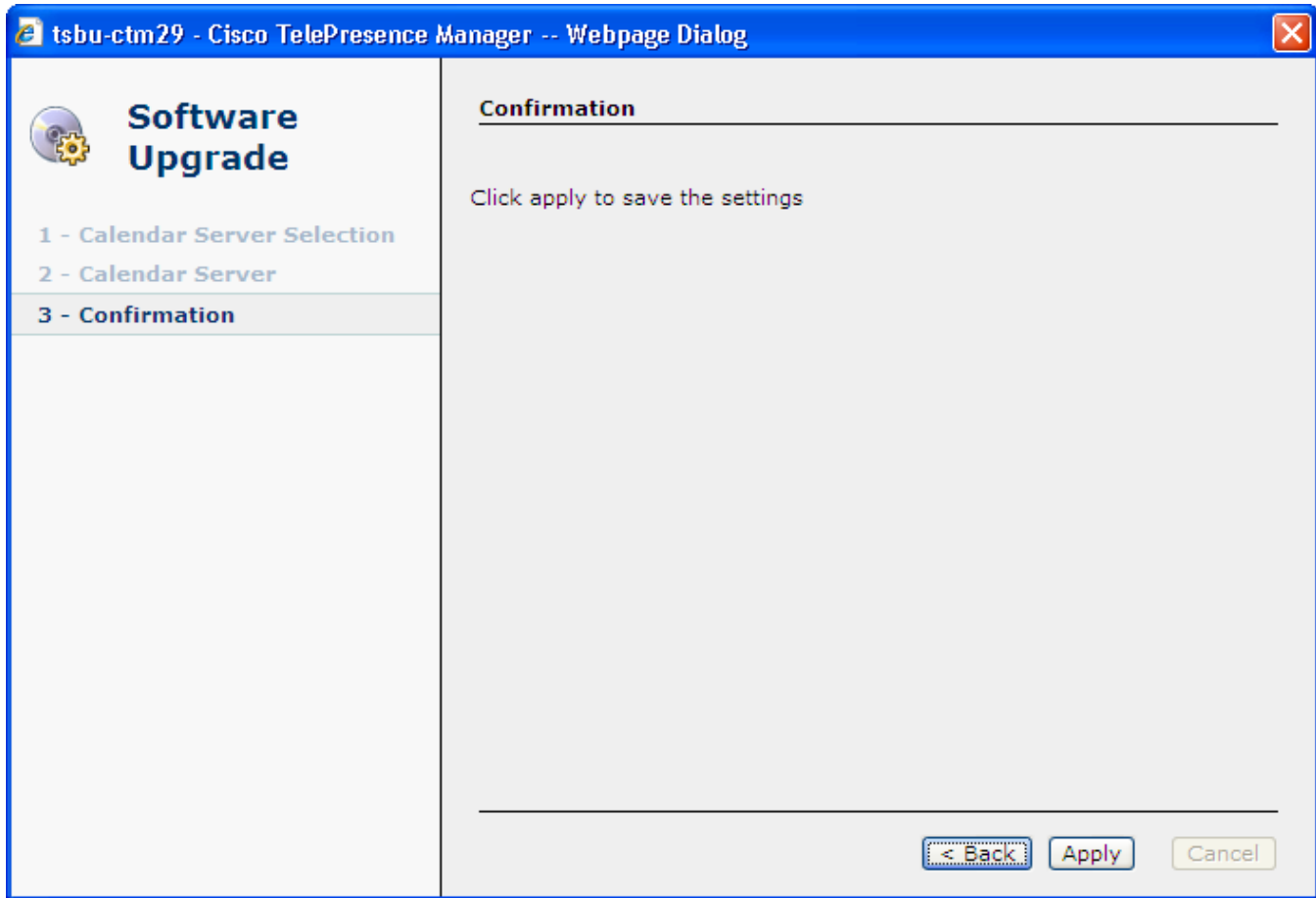
**Step 2** In the next step you need to specify the service logon information. The example below displays the information needed to use the Microsoft Exchange service.

**Figure 9-9** Cisco TelePresence Manager - Calendar Server Microsoft Exchange Screen

The screenshot shows a web browser window titled "tsbu-ctm29 - Cisco TelePresence Manager -- Webpage Dialog". The left sidebar contains the Cisco TelePresence Manager logo and a navigation menu with three items: "1 - Calendar Server Selection", "2 - Calendar Server" (which is highlighted), and "3 - Confirmation". The main content 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, each followed by a red asterisk indicating a required field: "Host:", "Bind Method:" (with radio buttons for "Secure" and "Normal", where "Normal" is selected), "Port:" (with the value "80" entered), "Domain Name:", "Logon Name:", "SMTP LHS:", "Password:", and "Certificate:" (with a "Browse..." button next to it). A "Test Connection" button is located below the input fields. At the bottom right of the main area are three buttons: "< Back", "Next >", and "Cancel".

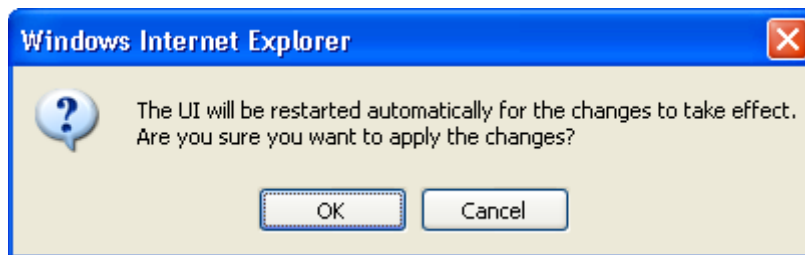
**Step 3** Click **Apply** to save the new Calendar server settings.

Figure 9-10 Cisco TelePresence Manager - Calendar Confirmation Screen



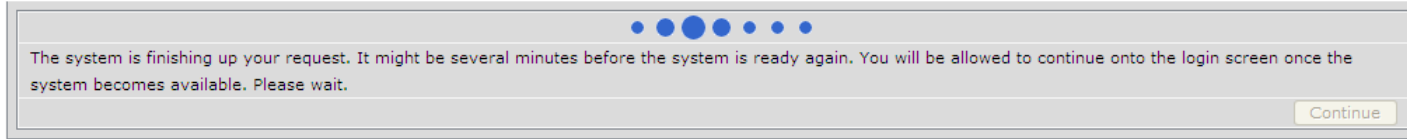
**Step 4** Then click **OK** to restart the CTS-Manager server.

Figure 9-11 Apply Changes Screen



**Step 5** Once the server has restarted, click **Continue** to re-launch the CTS-Manager server and log in.



**Figure 9-12**      **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.

To test the connection between this system and the Microsoft Exchange server as shown in [Figure 9-13](#):

- 
- 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**

CTS-Manager only supports Microsoft Windows Server 2003, Microsoft Exchange 2003 and 2007, Enterprise Edition.

**Figure 9-13** Microsoft Exchange Calendar Service Window

**System Configuration > Microsoft Exchange**

Service Status:	OK		
Mailbox Usage:	43.77% full (17508.0 of 40000.0 KB is used)		
Host:	tsbu-sr6	*	
Bind Method:	<input type="radio"/> Secure <input checked="" type="radio"/> Normal		
Port:	80	*	
Domain Name:	srdev.com	*	
Logon Name:	SuperUser		
SMTP LHS:	SuperUser	*	
Password:	*****	*	
Certificate:		Browse...	
Number of Meetings Per Query:	100	*	

\* Required Fields

[Test Connection](#) [Apply](#) [Reset](#)

**Synchronization Operations**

Subscription Status:  Room:  [Filter](#)

Showing 1 - 4 of 4 records

<input type="checkbox"/>	Room Name ▾	Last Synchronization Time (+)	Subscription Status
<input type="checkbox"/>	TelepresenceRoom34	✓ 12/08/2008 12:00 AM	Success
<input type="checkbox"/>	TelepresenceRoom32	✓ 12/08/2008 12:00 AM	Success
<input type="checkbox"/>	TelepresenceRoom31	✓ 12/08/2008 12:00 AM	Success
<input type="checkbox"/>	TelepresenceRoom33	✓ 12/08/2008 12:00 AM	Success

First < Previous Next > Last Rows Per Page: 10 ▾ [Re-sync](#) [Refresh](#)


(+) All times are shown in time zone America/Los\_Angeles (GMT -8.0)

Table 9-5 describes the information and operations accessible from this window.

**Table 9-5** Microsoft Exchange Server

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

**Table 9-5** Microsoft Exchange Server (continued)

Field	Description or Settings
Bind Method	Choose the <b>Secure</b> or <b>Normal</b> radio button to select the binding method, as follows: <ul style="list-style-type: none"> <li>Secure—CTS-Manager communicates with the Microsoft Exchange server in secure mode using HTTPS. This method requires enabling Secure Socket Layer (SSL) on the Microsoft Exchange server.</li> <li>Normal—CTS-Manager communicates with the Microsoft Exchange server in cleartext using HTTP.</li> </ul>
Port	Communication port number.
Domain Name	Domain name provided for the Microsoft Exchange server account, which can be changed. 
	<b>Note</b> This is the email domain name.
Logon Name	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> .
SMTP LHS	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>ctsappsmt@mycompany.com</i> enter <i>ctsappsmt</i> in this field.
Password	Password used to access the Microsoft Exchange server account, which can be changed.
Certificate	Use the field to provide a trust certificate for new Microsoft Exchange server.
Number of Meetings Per Query	The maximum number of meetings that Cisco TelePresence Manager can retrieve from the Exchange server for each query.

## Re-sync Operations

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

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

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

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

[Table 9-6](#) describes the information displayed in this area of the Microsoft Exchange window.

**Note**

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

**Table 9-6** *Microsoft Exchange Server Synchronization Report*

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

## IBM Domino

The IBM Domino window helps you manage the database that stores TelePresence meeting information. To test the connection between this system and the Domino server, as shown in [Figure 9-14](#)

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

**Figure 9-14 IBM Domino Calendar Service Window**

**System Configuration > IBM Domino**

Service Status:	OK
Mailbox Usage:	Unable to obtain necessary information
Host:	tsbu-ctmpc13 *
Bind Method:	<input type="radio"/> Secure <input checked="" type="radio"/> Normal
Port:	80 *
Organization Name:	CiscoDev *
Username:	ctm account *
Password:	***** *
Polling Interval (minutes):	1 *
Certificate:	<input type="text"/> Browse...

\* Required Fields Test Connection Apply Reset

**Synchronization Operations**

Subscription Status:  Room:  Filter

Showing 1 - 1 of 1 records

Domino Databases ▼	Last Synchronization Time (+)	Resynchronization Status	Associated Rooms
Telepres.nsf	✓ 12/08/2008 12:00 AM	Success	TelepresenceRoom15/Bldg 19 San Jose TelepresenceRoom14/Bldg 19 San Jose

Rows Per Page: 10 ▼
 Re-sync Refresh

(+) All times are shown in time zone America/Los\_Angeles (GMT -8.0)

Table 9-7 describes the information and operations accessible from this window.

**Table 9-7 IBM Domino Server**

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

**Table 9-7** *IBM Domino Server (continued)*

Field or Button	Description or Settings
Bind Method	Choose the Secure or Normal radio button to select the binding method, as follows: <ul style="list-style-type: none"> <li>Secure—CTS-Manager communicates with the Domino server in secure mode using HTTPS. This method requires enabling Secure Socket Layer (SSL) on the Domino server.</li> <li>Normal—CTS-Manager communicates with the Domino server in cleartext using HTTP.</li> </ul>
Port	Communication port number.
Organization Name	Domain name provided for the Domino server account, which can be changed.
Username	This is the account name used to log on to the Domino server.
Password	Password used to access the Domino server account, which can be changed. <b>Note</b> 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. <b>Note</b> A certificate is required in secure mode only.

## Re-sync Operations


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

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  to start the operation.

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

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

[Table 9-8](#) describes the information displayed in this area of the IBM Domino window.

**Table 9-8** *IBM Domino Server Synchronization Report*

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

**Table 9-8** *IBM Domino Server Synchronization Report*

Field	Description
Resynchronization Status	Status of the synchronization operation.
Associated Rooms	Name of the Cisco TelePresence meeting rooms associated with the Domino database.  <b>Note</b> The room name displayed is the name of the room in the Domino database. In order for CTS-Manager to successfully sync the room's meeting calendar, the room name must exactly match the room name in the Cisco TelePresence System profile registered in Unified CM.

## System Settings

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

- [IP Setting](#)
- [NTP Setting](#)
- [SNMP Setting](#)
- [Remote Account](#)
- [Password](#)
- [System Configuration - System Settings](#)

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 Setting

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 9-15](#) describes the fields and buttons.

**Figure 9-15** System Settings Window IP Settings Tab

System Configuration > System Settings

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

MAC Address:	00:1a:4b:33:2f:ec
Hostname:	tsbu-ctm18
Domain Name:	cisco.com
Primary DNS:	171.70.168.183
Secondary DNS:	
Ethernet Card:	eth0
DHCP:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IP Address:	172.28.68.165 *
Subnet Mask:	255.255.255.0 *
Default Gateway:	172.28.68.1 *

Apply Reset

To add new information, type it in the fields provided.


To change information, highlight and delete existing information and type in the new information.

To register new or modified settings, click

To restore the original settings, click .

Table 9-9 describes the information displayed in this area of the IP Settings window

**Table 9-9** 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.
Domain Name	Domain name for this Cisco TelePresence Manager.
Primary DNS	Primary DNS server IP address supplied for this Cisco TelePresence Manager.
Secondary DNS	Secondary DNS server IP address supplied for this Cisco TelePresence Manager.
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><b>Note</b> To modify the IP settings for this Cisco TelePresence Manager, click the radio button.</p> </div>



**Table 9-9** *IP Settings (continued)*

Field or Button	Description or Settings
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.

## NTP Setting

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 9-16** *System Settings Window NTP Settings Tab*

The screenshot shows the 'System Configuration > System Settings' window with the 'NTP Settings' tab selected. The tab bar includes 'IP Settings', 'NTP Settings', 'SNMP Settings', 'Remote Account', 'Password', and 'System'. The main area contains five rows for NTP servers. The first two rows have IP addresses entered: '64.104.222.16' and '64.104.193.12'. The remaining three rows are empty. At the bottom right, there are 'Apply' and 'Reset' buttons.

NTP Server	IP Address
NTP Server 1:	64.104.222.16
NTP Server 2:	64.104.193.12
NTP Server 3:	
NTP Server 4:	
NTP Server 5:	

- Step 1** To add an NTP server to the configuration, type 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 type in the new address.
- Step 3** To register new or modified settings, click [Apply](#).
- Step 4** To restore the original settings, click [Reset](#).

## SNMP Setting

SNMP is an industry-standard interface used by network management systems to capture system status and error information, including information provided by Unified CM. Use this window to enable and disable SNMP service and change the default configuration.

By default, SNMP service is disabled. Once SNMP is enabled, the following default SNMP settings are also enabled:

**Caution**

Editing SNMP settings from the CTS-Manager UI may cause some discrepancies. Please use the CLI commands to change these settings.

- One SNMP username set to “admin.” This name cannot be changed.
- SNMP service password set to “snmppassword.” The password can be changed. See Note below for additional information when performing a new installation.
- No trap receiver configured. Use the CLI snmp set command to configure a trap receiver. The fields collect trap receiver hostname or IP address and port, version, password, security level, authentication algorithm, and encryption.
- To view SNMP settings, click the SNMP Setting tab in the System Settings window.

**Figure 9-17** System Settings Window *SNMP Settings Tab*

System Configuration > System Settings

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

Engine ID: 0x80001f88030017a449c3e2

SNMP: Disabled

**SNMP Access Configuration**

Showing 0 - 0 of 0 records

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

**Trap Receiver Configuration**

Showing 1 - 1 of 1 records

IP Address/Hostname :Port	Version	Username/Community String	Password	Engine ID	Security Level	Authentication Algorithm	Encryption
No configured trap destinations.							

Note: Use CLI snmp set commands to change these settings.

Table 9-10 describes the fields for SNMP settings.

**Table 9-10** 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 command.  When SNMP is enabled, supply a password for the SNMP server in the area.

**Table 9-10** *SNMP Settings (continued)*

Field	Description or Settings
<b>SNMP Access Configuration</b>	<b>Use the CLI <code>snmp set</code> command to change these settings</b>
– Username	SNMP server username.
– Current Password	SNMP server password. The password must be 8 characters long. Enter it twice for verification.
<b>Trap Receiver Configuration</b>	<b>Use the CLI <code>snmp set</code> command to change these settings. See examples in following section.</b>
– IP Address/Hostname:Port	IP address or hostname and port number of the trap receiver
– Username	Trap receiver username.
– Current Password	Trap receiver password. The password must be 8 characters long. Enter it twice for verification.
– Authentication Algorithm	Choose Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) for authentication.

**Note**

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

## Technical Notes

CTS-Manager supports SNMP v3 and v2c. Together it supports ten SNMP users and five trap destination/receivers. A string of trap receiver settings is added to the `/etc/snmp/snmpd.conf` file to configure the trap receiver on the Cisco TelePresence Manager server. The string must include the following information, which is collected in the fields described in [Table 9-10](#) or is set by default:

- IP address and port number of the trap receiver
- Trap receiver username
- Trap receiver user password
- Trap sender engine ID
- Authentication method, either MD5 for Message Digest 5 or SHA for Secure Hash Algorithm
- Security model, which by default is `authNoPriv`
- SNMP version, which by default is version 3
- Included MIBs, which by default is ALL.

The following is an example trap receiver entry:

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

**Note**

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

Allowed:

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

Not allowed:

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

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

## 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 9-18 Database Window Settings Tab**

The screenshot shows the 'System Configuration > Database' window with the 'Settings' tab selected. The window contains a table with the following data:

Service Status:	OK
Current Database Size:	0.03% full (4.97 of 14648.44 MB is used)
Automatically Purge Data Older Than (months):	1

Below the table, there is a note: '\* Required Fields'. At the bottom right, there are 'Apply' and 'Reset' buttons. A footer note states: '(+) The system automatically purges data when database utilization exceeds 75% of the allocated disk space.'

Table 9-11 describes the information and settings that are accessible from the Database window Settings tab.

**Table 9-11**      **Database Settings**

Field	Description or Settings
Service Status	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.</p> <p>Data older than the specified number of months is purged.</p> <p>The purge cutoff date for this setting should be selected by balancing the number of months of data retention against the size of the database required to store the data created during that period. The default setting of 1 month is considered a reasonable midpoint.</p> <p><b>Note</b> Database utilization cannot exceed 75% of the allocated disk space, and takes precedence. If the number of months you have specified exceeds this percentage, older data is purged so as not to exceed 75%.</p>

## 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 9-19 System Configuration - Database Window Backup Tab

System Configuration > Database

Settings Backup Restore

Schedule (+): Daily @ 23:00 [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:

\* Required Fields [Backup Now](#) [Verify Remote Host](#) [Apply](#) [Reset](#)

Backup History

Showing 1 - 10 of 14 records

Time stamp (+) ▼	Status	Type	Hostname	Location
12/07/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-12-08-07-00-00.tar.gz
12/06/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-12-07-07-00-00.tar.gz
12/05/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-12-06-07-00-00.tar.gz
12/04/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-12-05-07-00-00.tar.gz
12/03/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-12-04-07-00-00.tar.gz
12/02/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-12-03-07-00-00.tar.gz
12/01/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-12-02-07-00-00.tar.gz
11/30/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-12-01-07-00-00.tar.gz
11/29/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-11-30-07-00-00.tar.gz
11/28/2008 11:00 PM	OK	Local		/common/dbbackup/CTMbackup.file.1.5.0.0.2008-11-29-07-00-00.tar.gz

First < Previous Next > Last Rows Per Page: 10 Refresh

(+) All times are shown in time zone America/Los\_Angeles null

## 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 timezone.
- Step 3** Choose the frequency of the backups by clicking the **Daily** or **Weekly** radio button.



**Note** If you click **Weekly**, check the box for the day of the week on which the backup should occur.

- Step 4** Click **OK** to register your settings, or **Cancel** to restore the original settings

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



**Note**

Backup schedules are now displayed in your local timezone.

## Backing Up Database Files

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.

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 **backup 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.

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

**Table 9-12 Remote Storage Host Fields**

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

### Viewing Backup History

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

[Table 9-13](#) describes the Backup History and Restore History fields.

**Table 9-13 Backup History and Restore History Fields**

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

## Restore

The Restore tab displays the history of the database restore operations. See [Table 9-13](#) for a description of the fields.



**Figure 9-20 Database Window Restore Tab**

**System Configuration > Database**

Settings Backup **Restore**

Restore Type:	<input checked="" type="radio"/> Local <input type="radio"/> Network
Restore Mode:	<input checked="" type="radio"/> Sftp <input type="radio"/> Ftp
Remote Storage Host :	<input type="text"/> *
Port:	<input type="text" value="22"/> *
Username:	<input type="text"/> *
Password:	<input type="text"/> *
Storage Path:	<input type="text"/> *

\* Required Fields

[Available Backups](#) [Verify Remote Host](#)

**Restore History**

Showing 0 - 0 of 0 records

Time stamp (+) ▼	Status	Type	Hostname	Location

First < Previous Next > Last Rows Per Page: 10 ▼ [Refresh](#)

(+) All times are shown in time zone America/Los\_Angeles null

## 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 login 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 **Restore Now** 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 9-12](#) for a description of the Remote Storage Host fields.

- 
- 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.
- 

## Discovery Service

To display and modify settings that associate CTS-Manager with Unified CM, choose Discovery Service in System Configuration.

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

To manually start the process that is periodically performed to discover new rooms added to 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.

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

**Figure 9-21** Discovery Service Window

[Table 9-14](#) describes fields, buttons, and settings.

**Table 9-14** *Cisco Unified Communications Manager Settings*

Field	Description or Settings
Service Status	Display-only status report of system services.  <b>Note</b> You may see a progress indicator in the status field, especially if many Cisco TelePresence meeting rooms are being managed by CTS-Manager. Each time this page is accessed, the status is updated, and the progress indicator will be seen while the system is discovering meeting rooms.
Host	Name of the Cisco Unified CM server host.
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.

## MCU Devices

The MCU Devices window provides the ability to add and delete MCU devices. There are two MCU devices supported by CTS-Manager—Cisco TelePresence Multipoint Switch (CTMS) and Cisco Unified Video Conference device (CUVC).

The MCU Devices support screen displays several attributes for each MCU device registered with Cisco TelePresence Manager.



### Caution

If the MCU devices has a reinstall the device must be registered through Cisco TelePresence Manager. There are no errors generated by the MCU device software change. The Cisco TelePresence Multipoint Switch Administrator must inform you of the change.

Figure 9-22 MCU Devices Window

System Configuration > Multipoint Conference Unit

MCU Devices

Service Status: **OK**

Showing 1 - 2 of 2 records

	Hostname ▾	Type ▾	Control State ▾	Description	IP Address
<input type="radio"/>	<a href="#">tsbu-ctm17</a>	CTMS	Scheduled	CTS Manager	172.28.68.164
<input type="radio"/>	<a href="#">tsbu-cuvc</a>	CUVC	Scheduled	CUVC	

First < Previous Next > Last Rows Per Page: 10 ▾ New... Edit... Delete Deallocate.. Refresh

Table 9-15 describes the MCU Device fields.

Table 9-15 MCU Devices

Field	Description or Settings
Hostname	The hostname or IP address of the MCU. Clicking the hostname hyperlink opens a new browser window, with the CTMS login page.
Type	The MCU Type is either CTMS or CUVC.
Control state	The Control state is either Scheduled or Non-Scheduled
Description	The Description field displays the MCU device description, added when the MCU device was added.
IP Address	The IP address of MCU.

### Deleting a MCU

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

To delete a MCU Device, click the radio button next to the device and click **Delete**.

### Refreshing the list of MCUs

Click the **Refresh** button to refresh the list of MCU 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. Refer to the CTS-Manager Release Note for the recommended versions.

# Access Management

From the Directory Server, it is possible to create groups, such as a Concierge group and an Admin group. Use this window to view and create roles for these groups. CTS-Manager supports two roles—a concierge and an administrator.

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

**Figure 9-23** Access Management Window

The screenshot shows the 'System Configuration > Access Management' window. The main section is titled 'Role to LDAP Group Mappings'. It features a 'Role:' dropdown menu set to 'All' and a 'Filter' button. Below this, a table displays the mappings. The table has two columns: 'Role' and 'LDAP FQDN'. A single row is visible, showing 'Concierge' as the role and 'CN=CTISConcierges,CN=Users,DC=srdev,DC=com' as the LDAP FQDN. The table is preceded by a radio button icon. At the bottom right, there are 'Add' and 'Delete' buttons. The text 'Showing 1 - 1 of 1 records' is displayed above the table.

Role	LDAP FQDN
Concierge	CN=CTISConcierges,CN=Users,DC=srdev,DC=com

## 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 CTS-Manager Administrator role. Only members of groups local to the IBM Domino Directory may be granted the Administrator role.

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

- Choose the role—All, Administrator, or Concierge—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 an 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 Concierge or Administrator role.

## Cisco TelePresence Multipoint Switch (CTMS)

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

## Adding a CTMS

To register additional CTMS devices with Cisco TelePresence Manager, click **New** to display the Registration dialog box, and choose CTMS from the Type drop-down field.

**Figure 9-24** Adding New CTMS - MCU Devices Window

**Table 9-16** Registering a CTMS with Cisco TelePresence Manager

Field	Description or Settings
Type	CTMS or CUVC are the only MCU types. If only CTMS appears in the drop-down list, Interop has not been enabled. Use the <a href="#">Application Settings</a> window to enable Interop.
MCU Host Name	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.

**Table 9-16**      *Registering a CTMS with Cisco TelePresence Manager (continued)*

Field	Description or Settings
Password	This is the account password used to log into the CTMS.
Control State	Specify whether the CTMS is available (scheduled) for meetings. The resources of a scheduled CTMS can be used when meetings are scheduled. Specifying a CTMS as Non-Scheduled means the CTMS will not be used when a meeting is scheduled.  <b>Note</b> CTMSs in a Scheduled state cannot be used to migrate meetings from other CTMSs.

## Editing CTMS Settings

To edit CTMS registration information, click the radio button next to the device and click **Edit**. The following table describes the CTMS settings that may be changed.

**Table 9-17**      *Editing Registered CTMS Configuration Settings*

Field	Description or Settings
Username	This is the account name used to log into the MCU.
Password	This is the account password used to log into the MCU.
Control State	Specify whether the MCU is available for meetings. The resources of a scheduled MCU can be used when meetings are scheduled. Specifying a MCU as Non-Scheduled means the MCU will not be used when a meeting is scheduled.  <b>Note</b> CTMSs in a Scheduled state cannot be used to migrate meetings from other CTMSs.

## Cisco Unified Video Conferencing (CUVC)

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


**Note**

Only one CUVC can be registered with CTS-Manager.

## Adding a CUVC

To add a CUVC device with Cisco TelePresence Manager, click **New** to display the Registration dialog box, and choose CUVC from the Type drop-down field.

**Table 9-18** Registering a CUVC with Cisco TelePresence Manager

Field	Description or Settings
Type	CTMS or CUVC are the only MCU types. If only CTMS appears in the drop-down list, Interop has not been enabled. Use the <a href="#">Application Settings</a> window to enable Interop. <b>Note</b> Only one CUVC may be registered with CTS-Manager.
MCU Host Name	This is the LHS of the complete Host name.
Control State	Specify whether the CUVC is available (scheduled) for meetings. The resources of a scheduled CUVC can be used when meetings are scheduled. Specifying a CUVC as Non-Scheduled means the CUVC will not be used when a meeting is scheduled.
Access Number Prefix for CTMS	The access number prefix for your CTMS is based on your enterprise dialing plan.
Access Number Prefix for Video Conferencing Participants	This access number prefix is based on your enterprise dialing plan.
Conference ID Length	The Conference ID can be 1-8 digits in length. The system-generated Conference ID is used to create an Interop Access Number used by the CTMS to establish the conference call. It is also used to create the Interop Access Number sent in an email to meeting participants, as the dial-in phone number. The Conference ID length is based on your enterprise dialing plan.
Multiple EMP Cards Support	Enabling EMP card support provides additional resources to support a greater number of video calls using the CUVC. CTS-Manager with EMP card support enabled allows up to 48 video calls per EMP card. <b>Note</b> If you are using a CUVC 3515 MCU this option is disabled.
Number of EMP Cards	Specify the number of EMP cards installed in the CUVC device.
Maximum Participants per Conference	Enter a numeric value for the maximum number of meeting participants that may dial into the conference call.
Minimum Participants per Conference	The minimum value for this field is 2. This value cannot exceed the Maximum Participants per Conference value.
Total Resources	This value should be greater than the Maximum Participants per Conference. <b>Note</b> If you have enabled EMP card support the values in the <b>Total Resources</b> field and the <b>Minimum Participants per Conference</b> field are calculated for you. The calculation is <i>Number of EMP Cards x Maximum Participants per Conference</i> .

## Editing CUVC Settings

To edit CUVC registration information, click the radio button next to the device and click **Edit**. The following table describes the CUVC settings that may be changed.



**Table 9-19**      *Editing Registered CUVC Configuration Settings*

Field	Description or Settings
Control State	Specify whether the CUVC is available for meetings. The resources of a scheduled CUVC can be used when meetings are scheduled. Specifying a CUVC as Non-Scheduled means the CUVC will not be used when a meeting is scheduled.  <b>Note</b> If there are scheduled interop meetings you can't change a CUVC state to non-scheduled.
Access Number Prefix for CTMS	The access number prefix for your CTMS is based on your enterprise dialing plan.
Access Number Prefix for Video Conferencing Participants	This access number prefix is based on your enterprise dialing plan.
Number of EMP Cards	This value in this field can be changed if Multiple EMP Card support is enabled.
Maximum Participants per Conference	Enter a numeric value for the maximum number of meeting participants that may dial into the conference call.  <b>Note</b> The value in this field affects the number of CTMS resources reserved for a specific conference call.
Minimum Participants per Conference	The minimum value for this field is 2. This value cannot exceed the Maximum Participants per Conference value.
Total Resources	This value should be greater than the Maximum Participants per Conference.

## Concierges

### Concierge Role

When a concierge logs into CTS-Manager, the following selections and information are available:

- System Information
- System Status
- Support
- Troubleshooting

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

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

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

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

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

**Figure 9-25** System Configuration - Concierge Window

**System Configuration > Concierges**

**Concierges**

ID	Phone Number	Description
<Unassigned>		System installed concierge

New... Edit... Delete

**Rooms that have not been assigned**

Showing 1 - 2 of 2 records

Status	Room Name	Room Phone	Description	IP Address
<input type="checkbox"/>	TelepresenceRoom15/Bldg 19 San Jose	16250	Telepresen...	<a href="#">172.28.69.216</a>
<input type="checkbox"/>	TelepresenceRoom14/Bldg 19 San Jose	16240	Telepresen...	<a href="#">172.28.69.215</a>

First < Previous Next > Last Rows Per Page: 10 Assign selected rooms to: <Unassigned> Apply

## Creating Concierges

To add a new Concierge, from this window, perform the following steps:

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



### Caution

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

**Figure 9-26** Adding a Concierge Window

The screenshot shows a web-based dialog box titled "tsbu-ctm30 - Cisco TelePresence Manager -- Webpage Dialog". The main heading inside is "New... Concierges". Below this, there are three input fields: "ID:" with a text box and a red asterisk, "Phone Number:" with a text box and a red asterisk, and "Description:" with a larger text area. Below these fields is a "Set as Default:" checkbox. At the bottom left, there is a legend: "\* Required Fields". At the bottom right, there are "Save" and "Close" buttons.

All Cisco TelePresence rooms must be assigned to a Concierge. If you haven't specified a Concierge for a room, the System installed <Unassigned> Concierge is the default Concierge for all rooms discovered in CTS-Manager. You can change the default Concierge to a specific Concierge by checking the Set as Default checkbox in the Concierge details window. Any Cisco TelePresence room discovered by CTS-Manager will be assigned to the new default Concierge. Each time you specify a different Concierge as the default, all future rooms discovered by CTS-Manager will be assigned to the new default.

## Assigning a Room to a Specific Concierge

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

- 
- Step 1** Check the box next to a room that has not been assigned.
  - Step 2** Select a concierge from the **Assign Selected Rooms** drop-down list.
  - Step 3** Click **Apply**.  
To edit the concierge assignment:
  - Step 4** Select the radio button next to the Concierge ID and click **Edit**.
  - Step 5** In the Edit Concierges window, you can change the phone number and other information identifying the concierge.
  - Step 6** To delete a Concierge, select the radio button next to the concierge ID and click **Delete**.
-

**Note**

CTS-Manager 1.5 supports a default concierge that is assigned to endpoints that have no specific concierge assignment. Earlier versions of CTS-Manager allowed more than one concierge to have the same phone number. If you are upgrading to version 1.5 from an earlier version that allows a concierge to share a phone number with another concierge, during the upgrade CTS-Manager 1.5 changes the phone number of one of the concierges and assigns that concierge to the endpoint.

## Policy Management

The Policy Management window lists the three default policies to support scheduling and conference termination:

**Figure 9-27** System Configuration - Policy Management Window

System Configuration > Policy Management			
Policy Management			
Showing 1 - 3 of 3 records			
	Policy Name ▼	Policy Type	Policy Description
<input type="radio"/>	Default	CONF_MAN	This is the Default Conference Management Policy
<input type="radio"/>	Default	CTS	This is the Default CTS Policy
<input type="radio"/>	Default	CTMS	This is the Default CTMS Policy
<div> <input type="button" value="First"/> <input type="button" value=" &lt; Previous"/> <input type="button" value="Next &gt;"/> <input type="button" value="Last"/> </div> <div>           Rows Per Page: <input type="text" value="10"/> </div> <div> <input type="button" value="New..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/> </div>			

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

Figure 9-28 CTMS Policy Window

Name:	Default
Type:	CTMS
Description:	This is the Default CTMS Policy
Switching Mode:	Speaker
Number of days pushed to CTMS:	14
* Required Fields	

- **CTS endpoint policy**—determines the number of days of scheduled meetings pushed to each endpoint. The default is 14 days, the range is from 1 to 30 max.

Figure 9-29 CTS Endpoint Policy Window

Name:	Default
Type:	CTS
Description:	This is the Default CTS Policy
Number of days pushed to phone:	14
* Required Fields	

- **Conference Manager policy**—specifies the following:
  - **Force Meeting Termination**—Setting this to “Yes” allows the endpoints and any MCU device to automatically terminate a conference call according to the scheduled meeting time. The default is “No”, so that meeting participants can continue a call past the scheduled end time of the meeting.
  - **Early Meeting Start in minutes**—Determines how many minutes before a meeting’s scheduled start time a participant can press the One-Button-to-Push to initiate a meeting.
  - **Late Meeting End in minutes**—Determines how many minutes a meeting may continue before the call is forced to terminate. This field is grayed out if Force Meeting Termination is set to No.

**Note**

“Early Meeting Start in minutes” affects both point-to-point meetings and multipoint meetings. All other settings affect only multipoint meetings.

**Figure 9-30** Conference Manager Policy Window

Name:	Default
Type:	CONF_MAN
Description:	This is the Default Conference Management Policy
Force Meeting Termination:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Early Meeting Start in minutes:	10
Late Meeting End in minutes:	0
Notify Meeting End Prior To Scheduled End in minutes:	10
* Required Fields	

Save Close

## 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 pass phrase generated by software in this CTS-Manager. The remote user uses the account name, the pass phrase, 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 9-31** System Settings Window Remote Account Tab

System Configuration > System Settings

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

Account Name:  \*

Duration (days):  \*

Add

To start the remote login account process:

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

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

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

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

This step generates a pass phrase.

To complete this process, the account name and pass phrase 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.

## System Configuration - System Settings

Use the System Configuration, System Settings window to restart CTS-Manager.

**Figure 9-32** System Settings Window System Tab

System Configuration > System Settings

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

Username: admin

Password:  \*

Restart Shutdown

**Step 1** To restart the system, click on the System tab.

- The username cannot be changed.

**Step 2** Enter your password.

**Step 3** Click on **Restart**.

This will restart the CTS-Manager system.

## Application Settings

The System Configuration Applications Settings window is used to set three different options: Interoperability with Video Conferencing, Intercompany, and Meeting Notification Email.

**Figure 9-33** Application Settings Window

System Configuration > Application Settings

**Interoperability with Video Conferencing**

Enable Feature: ☐ Yes ☒ No +

**Intercompany**

Enable Feature: ☐ Yes ☒ No

Provider ☒ Another Company Hosts ☐ Our Company Hosts

**Meeting Notification Email**

Enable Feature: ☒ Yes ☐ No

Copy Outgoing Email To:  ++

Apply Reset

(+) Interoperability with Video Conferencing can be enabled..  
 (++) All email generated by Cisco TelePresence Manager will be sent/copied to this address.

## Interoperability with Video Conferencing Settings

The default setting for inter operability with video conferencing is “Disable.” If the setting is grayed out and cannot be changed to “Enable,” there is at least one CTS endpoint or MCU device that is not interop-ready. All endpoints and CTMS MCUs must support interop before you can enable Interop settings. Make sure all devices discovered by CTS-Manager are running interop-enabled software releases.

If Interoperability with Video Conferencing has been set to “Enable” and is grayed out so that you can’t disable it, the CUVC, added through the MCU devices window, is included in at least one scheduled meeting. In order to disable interop services, you must first **Deallocate** the CUVC, and then **Delete** it from the MCU Devices window.

## Intercompany Setting

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



## Meeting Notification Email Settings

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.

You can also specify an additional email address. All emails generated by Cisco TelePresence Manager will also be sent to this address.

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

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

## 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 of Notes during a 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:

- To start the failover procedure, power off the primary CTS-Manager system.
- Power on the backup CTS-Manager system.
- Restore the last CTS-Manager database to the backup CTS-Manager, click **Available Backups** to complete this task

**Figure 9-34** System Configuration Database Restore Backup Window

The screenshot shows the 'System Configuration > Database' window in Cisco TelePresence Manager. The 'Restore' tab is active. The 'Restore Type' is set to 'Local'. The 'Remote Storage Host' is empty, and the 'Port' is set to '22'. There are input fields for 'Username' and 'Password'. The 'Storage Path' is also empty. There are buttons for 'Available Backups' and 'Verify Remote Host'. Below this is a 'Restore History' section showing 'Showing 0 - 0 of 0 records'.

Time stamp (+)	Status	Type	Hostname	Location
Showing 0 - 0 of 0 records				

- Next, perform a re-sync with Microsoft Exchange or IBM Domino database from the backup CTS-Manager.

**Figure 9-35** System Configuration - Microsoft Exchange Re-sync Window

The screenshot shows the 'System Configuration > Microsoft Exchange' window in Cisco TelePresence Manager. The 'SMTP LHS' is set to 'CTSMAN'. The 'Password' is masked with dots. There is a 'Certificate' field with a 'Browse...' button. The 'Number of Meetings Per Query' is set to '100'. There are buttons for 'Test Connection', 'Apply', and 'Reset'. Below this is a 'Synchronization Operations' section with a table showing synchronization results for three rooms.

Room Name	Last Synchronization Time (+)	Subscription Status
1003	02/23/2009 12:03 AM	Success
1009	02/23/2009 12:03 AM	Success
27990	02/23/2009 12:03 AM	Success

At the bottom, there are buttons for 'First', '< Previous', 'Next >', 'Last', 'Rows Per Page: 10', 'Re-sync', and 'Refresh'.

- After ensuring the information is correct, click **Re-sync** to complete the re-sync.



**Note**

This Re-sync in Exchange must be verified in an Exchange environment, not CTS-Manager.

## Warm Standby

### CTMS Warm Standby for Scheduled Meetings

Both the primary and backup CTMS systems are configured independently with different access 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 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-Man.
- Step 2** Power on the backup CTS-Manager.
- Step 3** Restore the last CTS-Manager database to the backup CTMS, click **Available Backups** to complete this task



#### 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.

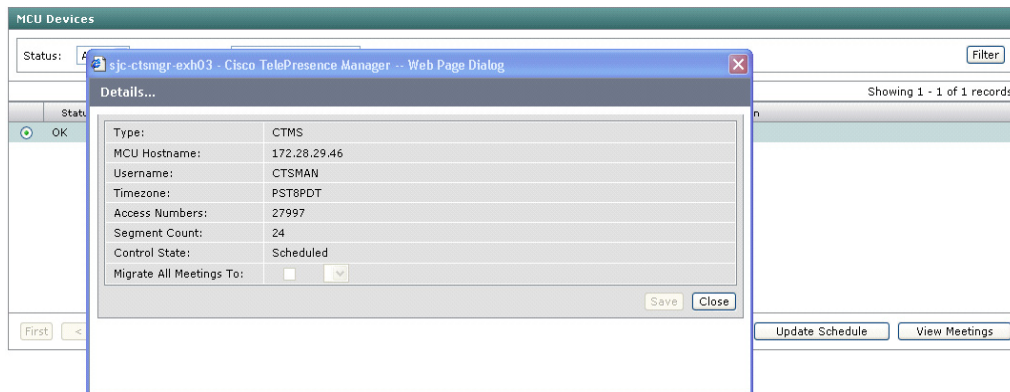
**Figure 9-36** System Configuration Database Restore Backup Window

The screenshot displays the Cisco TelePresence Manager interface. The left sidebar shows the navigation menu with 'System Configuration' expanded. The main content area is titled 'System Configuration > Database' and has three tabs: 'Settings', 'Backup', and 'Restore'. The 'Restore' tab is active, showing a form for restoring the database. The form includes a 'Restore Type' section with radio buttons for 'Local' (selected) and 'Network'. Below this is a 'Restore Mode' section with radio buttons for 'Sftp' (selected) and 'Ftp'. There are input fields for 'Remote Storage Host', 'Port' (with '22' entered), 'Username', 'Password', and 'Storage Path'. At the bottom of the form are two buttons: 'Available Backups' and 'Verify Remote Host'. Below the form is a 'Restore History' section with a table showing 0 records. The table has columns for 'Time stamp (+)', 'Status', 'Type', 'Hostname', and 'Location'. The top of the window shows the Cisco logo and the text 'Cisco TelePresence Manager', along with user information 'admin | Logout | Preferences | Help | About'.

## 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.

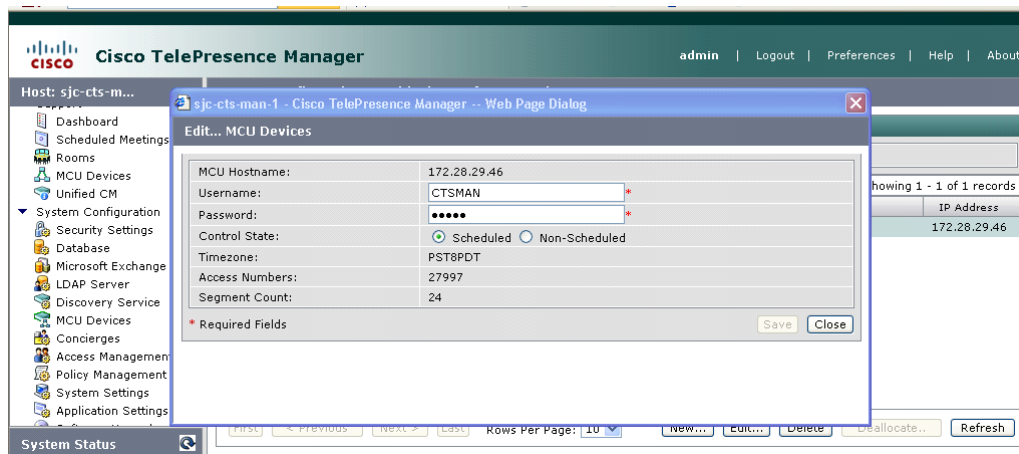
**Figure 9-37** System Configuration MCU Devices - Details Window



- Step 2** Change the Control State of primary CTMS to **Non-scheduled**

- Step 3** Change the Control State of the backup CTMS to **Scheduled**.

**Figure 9-38** System Configuration MCU Devices - Edit Window



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