CHAPTER 9

Additional Installation Configurations for Cisco TelePresence Manager

Revised: October 27, 2009, OL-13673-06

Contents

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

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 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 Live Desk role.	Chapter 10, "Monitoring Cisco TelePresence Manager"

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

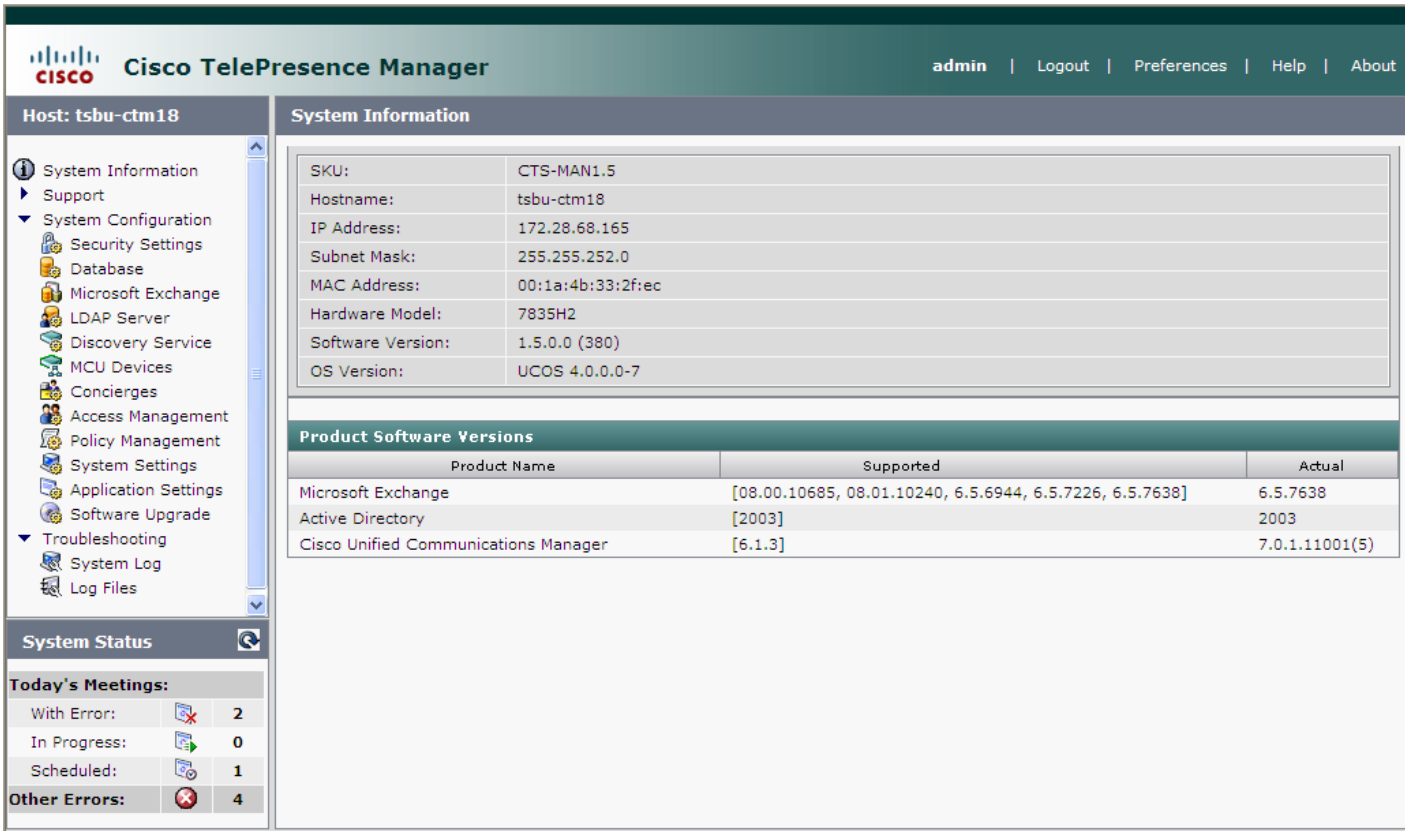
Introduction

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



Today's Meetings:	
With Error:	2
In Progress:	0
Scheduled:	1
Other Errors:	4

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

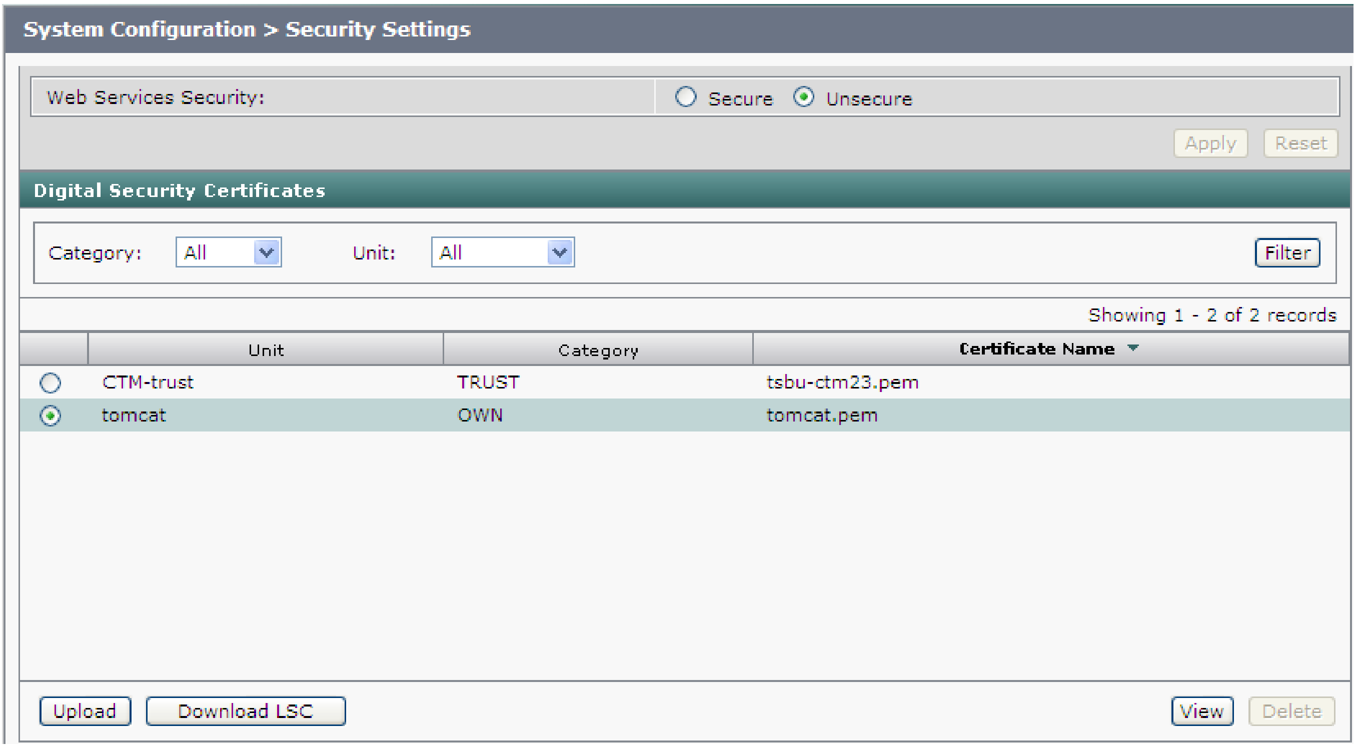
Product Software Versions

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)

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

Digital Security Certificates

Category: All Unit: All

Showing 1 - 2 of 2 records

	Unit	Category	Certificate Name
○	CTM-trust	TRUST	tsbu-ctm23.pem
●	tomcat	OWN	tomcat.pem

Web Services Security

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

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 must delete the existing certificate before uploading a new one. If a certificate has expired, you cannot attempt to upload it.

Step 1 In the Certificate Upload window, choose the category and unit for the certificate.

Step 2 Click **Browse** to choose a location where a certificate file is located, and add it to the Certificate field.

Step 3 Click **Upload** to copy the file.

Step 4 Click **Close** to close the Certificate Upload window.

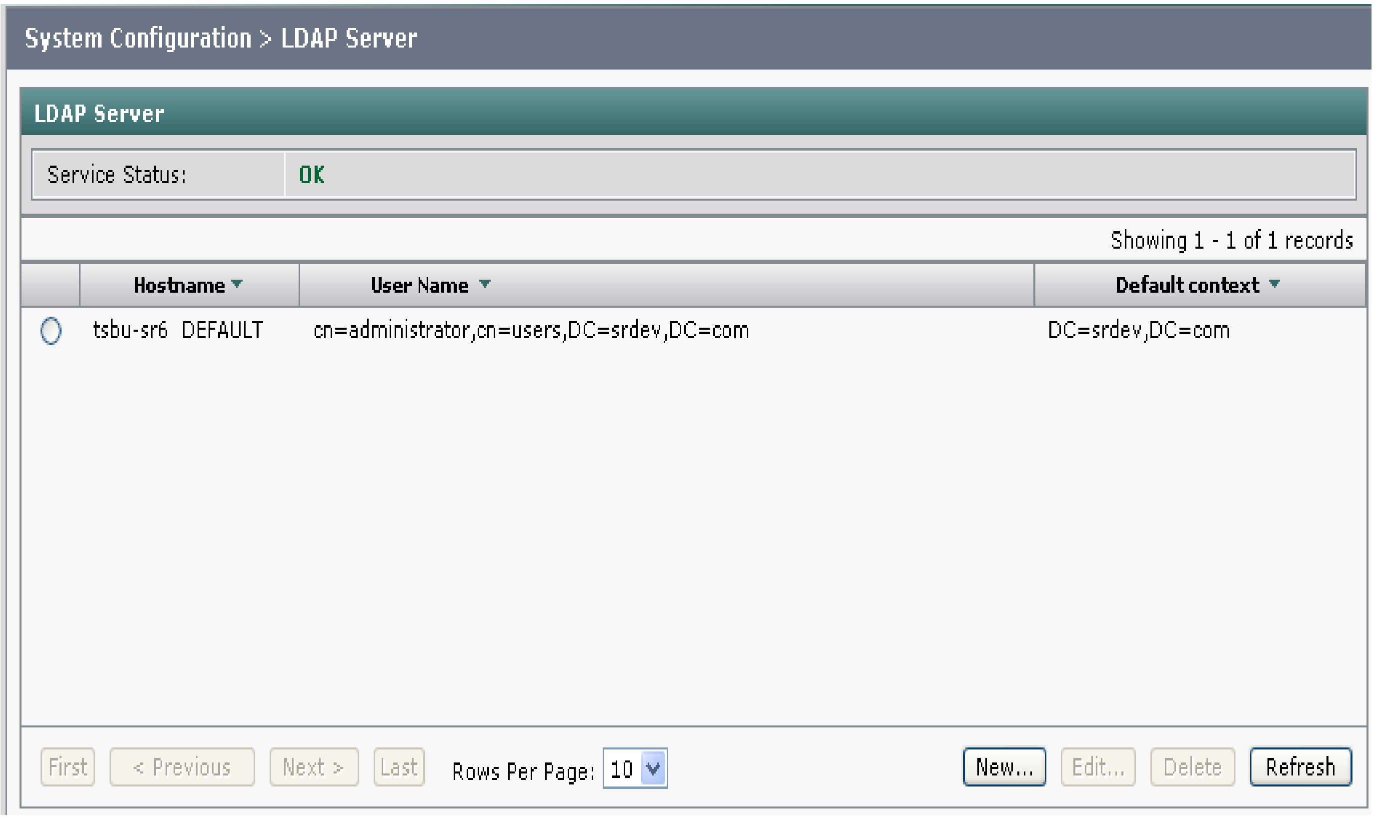
LDAP Server

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

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

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

Figure 9-3 System Configuration>LDAP Server



System Configuration > LDAP Server

LDAP Server

Service Status: OK

Showing 1 - 1 of 1 records

	Hostname	User Name	Default context
○	tsbu-sr6 DEFAULT	cn=administrator,cn=users,DC=srdev,DC=com	DC=srdev,DC=com

Rows Per Page: 10

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

Note Microsoft Exchange WebDAV and EWS environments: CTS-Manager 1.6.2 and earlier support only one LDAP server. 1.6.3 and later support unlimited LDAP servers.

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 the status of the server. This window also allows new settings or editing the settings and field mappings.

Settings for LDAP

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

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 9-2 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

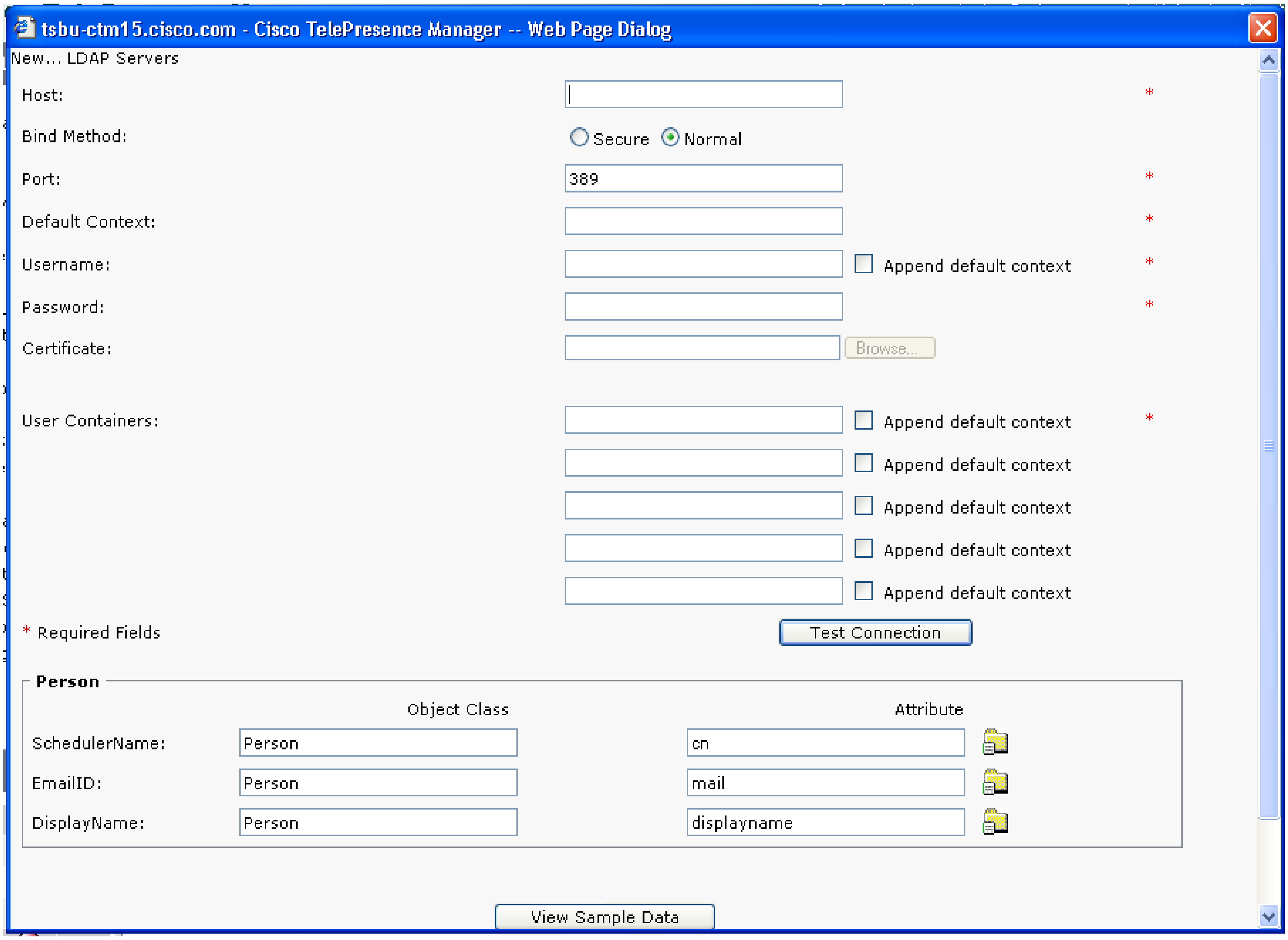
The attributes are used by the Exchange server to store the user's e-mail and display name information. For most of the Exchange deployments, this information should not be changed. It is very unlikely that these mappings need to be changed. In case there is a requirement to authenticate users using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

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

Note WebDAV and EWS environments: CTS-Manager 1.6.2 and earlier support only one LDAP server. 1.6.3 and later support unlimited LDAP servers.

Caution The object and attribute mappings for Exchange/Directory Server deployments are listed in Table 9-4 and cannot be changed after installing and configuring Cisco TelePresence Manager. Cisco TelePresence Manager may not functions properly if the Object Class fields are changed.

Figure 9-4 New LDAP Window Mappings



tsbu-ctm15.cisco.com - Cisco TelePresence Manager -- Web Page Dialog

New... LDAP Servers

Host: *

Bind Method: ○ Secure ● Normal

Port: 389 *

Default Context: *

Username: □ Append default context *

Password: *

Certificate: Browse...

User Containers: □ Append default context *
□ Append default context
□ Append default context
□ Append default context
□ Append default context

* Required Fields

Test Connection

Person

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

View Sample Data

Table 9-2 lists the fields in the LDAP Server - New window. See Table 9-4 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 9-2 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: • 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: • Click the Fetch DNS 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=CTSMan User" is another example. Note that the CTS-Manager Active Directory configuration requires using users that have Domain Admin privilege. The user, "CTSMan User" only needs to be created with the Domain Users privilege.
Password	Password to access the LDAP server.
Certificate	The name of the LDAP certificate. This is only needed if you have chosen the Secure Bind Method.

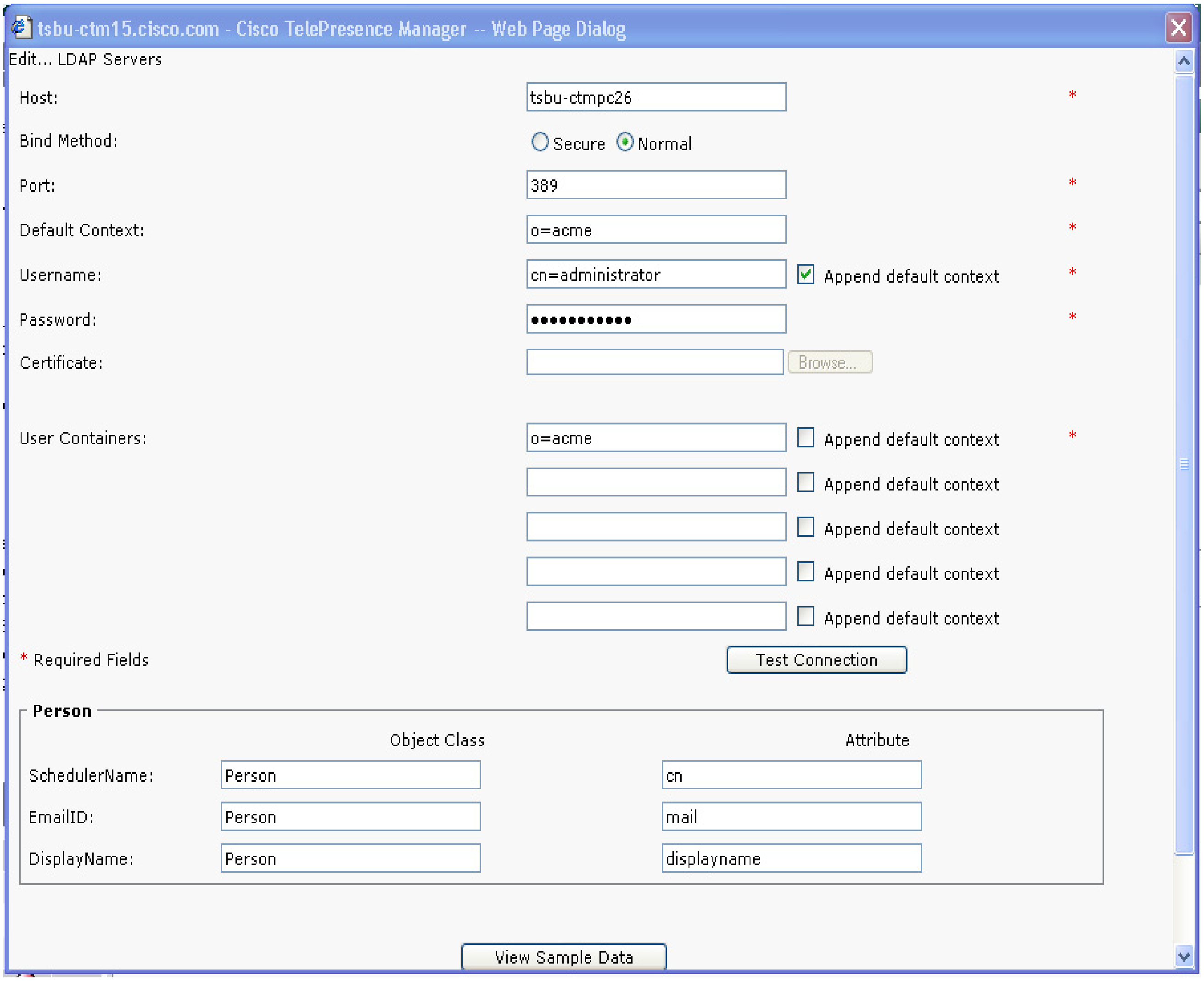
Table 9-2 New LDAP Server Settings (continued)

Field or Button	Description or Settings
User containers	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. • To append the default context, check the Append default context box next to the user container field. **Note** 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.
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 9-3 lists the field information. See Table 9-4 for the Person field information.

Figure 9-5 Edit LDAP Window



tsbu-ctm15.cisco.com - Cisco TelePresence Manager -- Web Page Dialog

Edit... LDAP Servers

Host:	tsbu-ctmpc26		*
Bind Method:	○ Secure ● Normal		
Port:	389		*
Default Context:	o=acme		*
Username:	cn=administrator	☑ Append default context	*
Password:	••••••••••••		*
Certificate:		Browse...	
User Containers:	o=acme	□ Append default context	*
		□ Append default context	
		□ Append default context	
		□ Append default context	
		□ Append default context	

* Required Fields

Person

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

Table 9-3 Edit 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: • 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.

Table 9-3 Edit LDAP Server Settings (continued)

Field or Button	Description or Settings
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: • Click the Fetch DNS 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)
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.
User containers	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. • To append the default context, check the Append default context box next to the user container field. **Note** 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.

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 9-4 describes the settings for the Person fields in both the New and Edit windows.

Table 9-4 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.

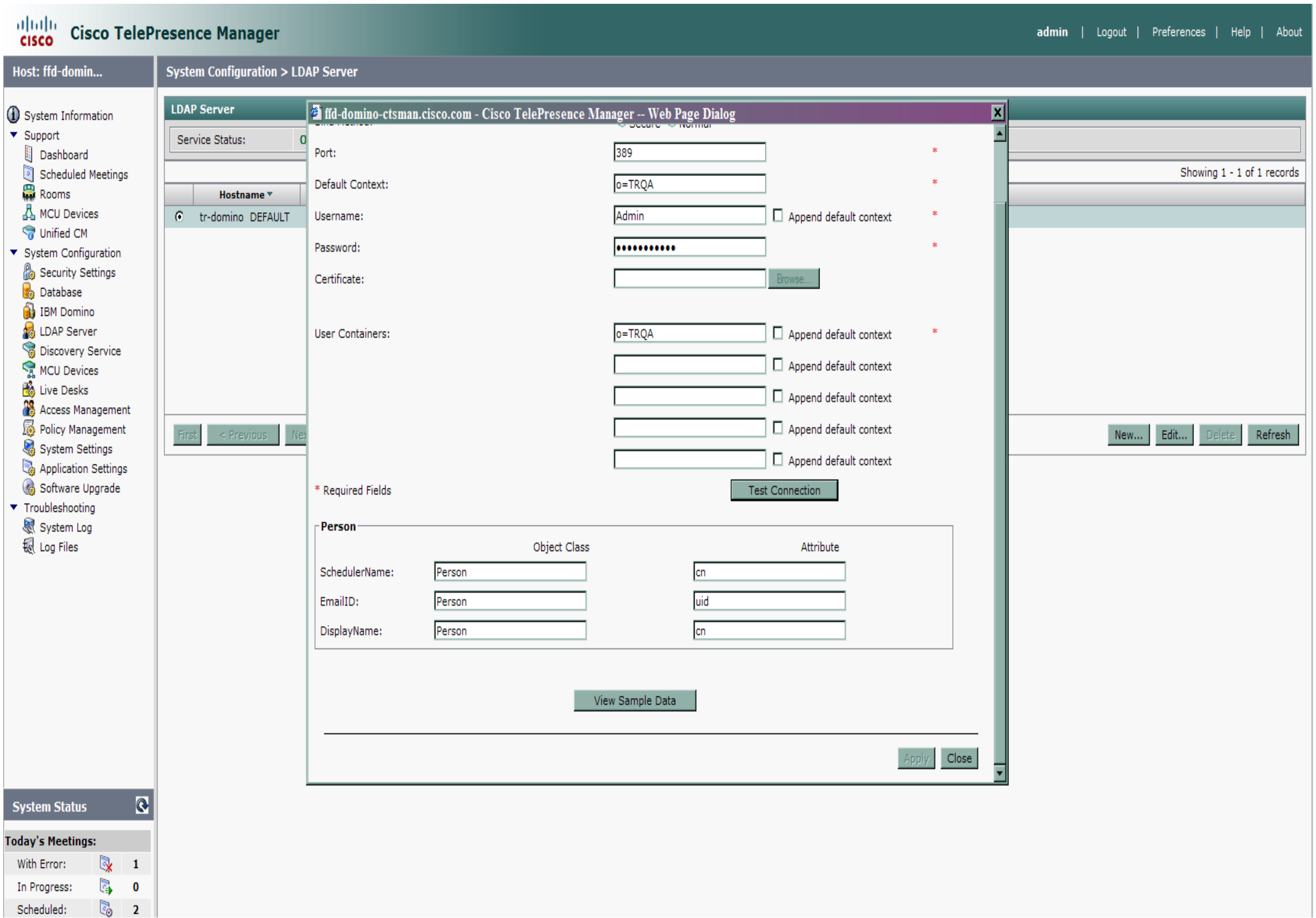
IBM Domino Deployments

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

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

Note The object and attribute mappings for Domino/Directory Server deployments are listed in Table 9-6 and cannot be changed after installing and configuring CTS-Manager.

Figure 9-6 IBM LDAP New/Edit Field Mappings Window



tr-domino DEFAULT

Port: 389 *

Default Context: o=TRQA *

Username: Admin ☐ Append default context *

Password: ●●●●●●●●●●● *

Certificate:

User Containers: o=TRQA ☐ Append default context *

☐ Append default context

☐ Append default context

☐ Append default context

☐ Append default context

* Required Fields

Person

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

Today's Meetings:

With Error:	1
In Progress:	0
Scheduled:	2

Table 9-5 lists the information for the fields in the IBM LDAP Edit or New window.

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

Table 9-5 IBM LDAP Server Settings

Field or Button	Description or Settings
Host	LDAP server hostname.
Bind Method	Click the **Secure** or **Normal** radio button to select the binding method: • Secure—CTS-Manager commnicates with the Domino server in secure mode using HTTPS or DIIOP. This method requires enabling Secure Socket Layer (SSL) on the Domino server. • Normal—CTS-Manager communicates with the IBM Domino server in cleartext using HTTP or DIIOP.

Table 9-5 IBM LDAP Server Settings (continued)

Field or Button	Description or Settings
Port	Communication port number (HTTP or DIIOP) The default port for secure connection is 636. The default port for normal connection in a single LDAP server deployment is 389.
Default Context	The default context from which the LDAP queries are performed. Example: o=dominotest
Username	The username used to authenticate to the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: "Admin User" **Note** LDAP username configured in CTS-Manager should have minimum Reader access on Domino directory. We recommend creating a user with Reader access.
Password	Password to access the LDAP server.
Certificate	The name of the LDAP certificate. **Note** A certificate is required for secure bind method only.
User Containers	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. Add Domino Containers, but do not check the Append default context checkbox. Example foe container: o=SalesOrg.
Test Connection	Allows you to test the configuration connection

Table 9-6 describes the settings for the Person fields in both the New and Edit windows.

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.

Table 9-6 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.

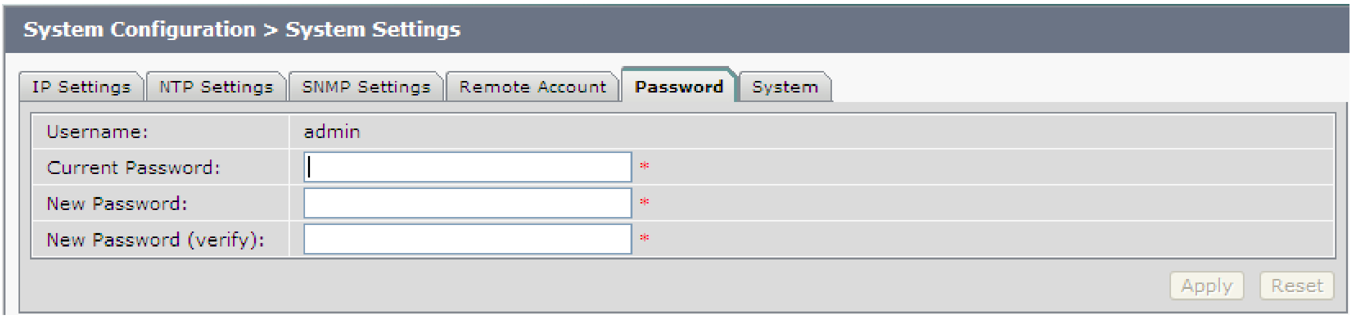
Deleting Server

Before deleting a DNS server, it is important to first change existing CUCM servers and conferencing bridges from hostname to IP before the DNS server is deleted. If the hostname is not changed first, the CUCM servers and conferencing bridges will be put into an error status.

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 9-7 System Configuration - System Settings Window Password Tab



Username: admin
Current Password: *
New Password: *
New Password (verify): *

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

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.

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

Calendar Server

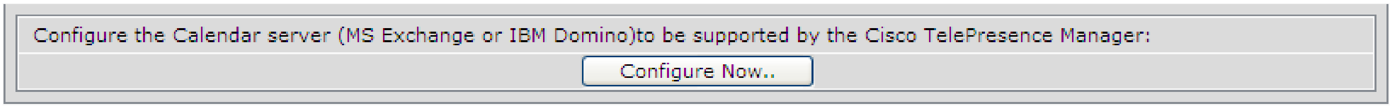
If you did not specify a Calendar server (either Microsoft Exchange or IBM Domino) during the initial installation, the Calendar Server window displays the Calendar Server wizard.

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.

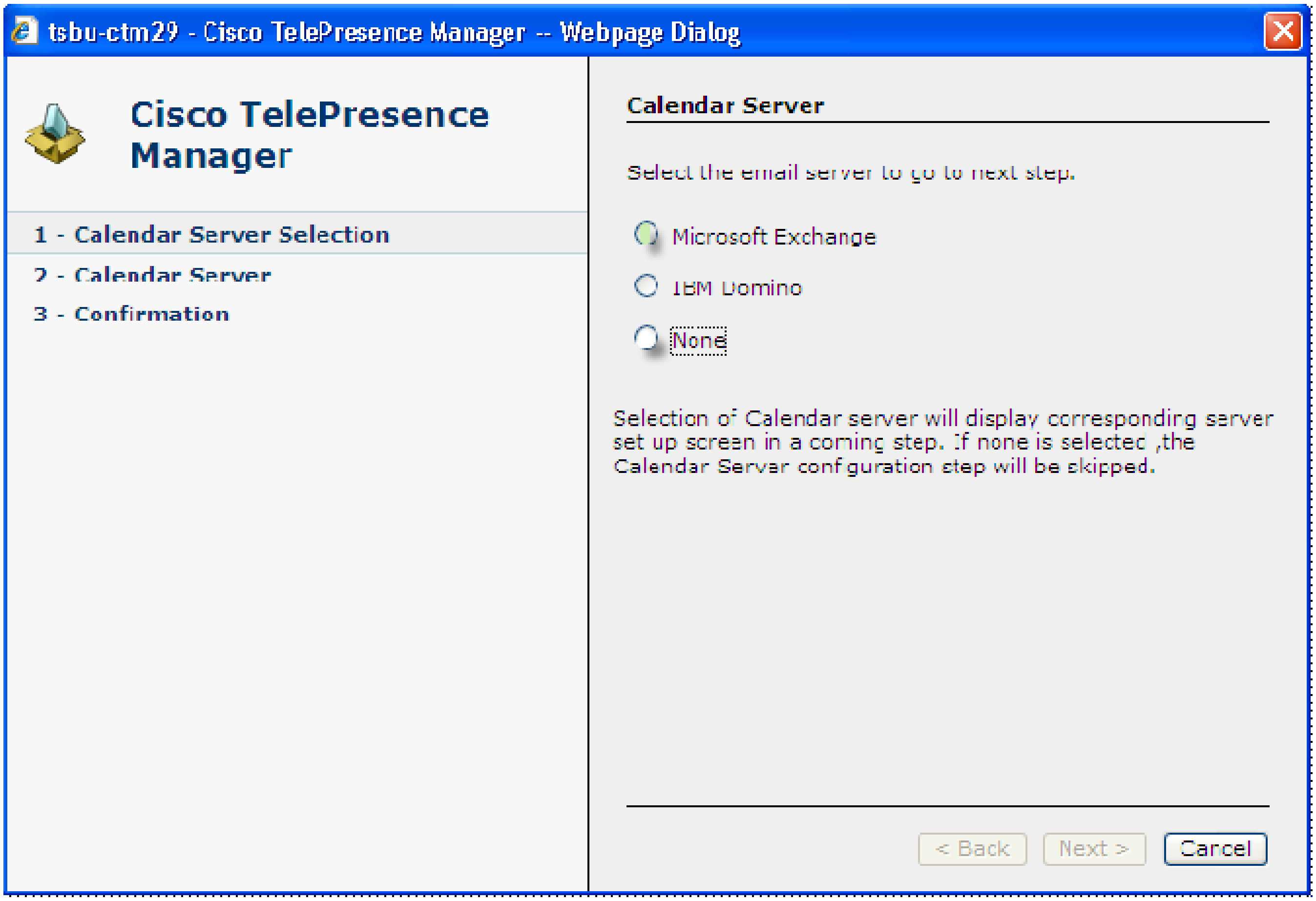
Figure 9-8 Configure Calendar Server



Configure the Calendar server (MS Exchange or IBM Domino)to be supported by the Cisco TelePresence Manager:

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

Figure 9-9 Cisco TelePresence Manager - Calendar Server Selection Screen



tsbu-ctm29 - Cisco TelePresence Manager -- Webpage Dialog
Cisco TelePresence Manager
1 - Calendar Server Selection
2 - Calendar Server
3 - Confirmation
< Back
Next >
Cancel

Calendar Server

Select the email server to go to next step.

○ Microsoft Exchange

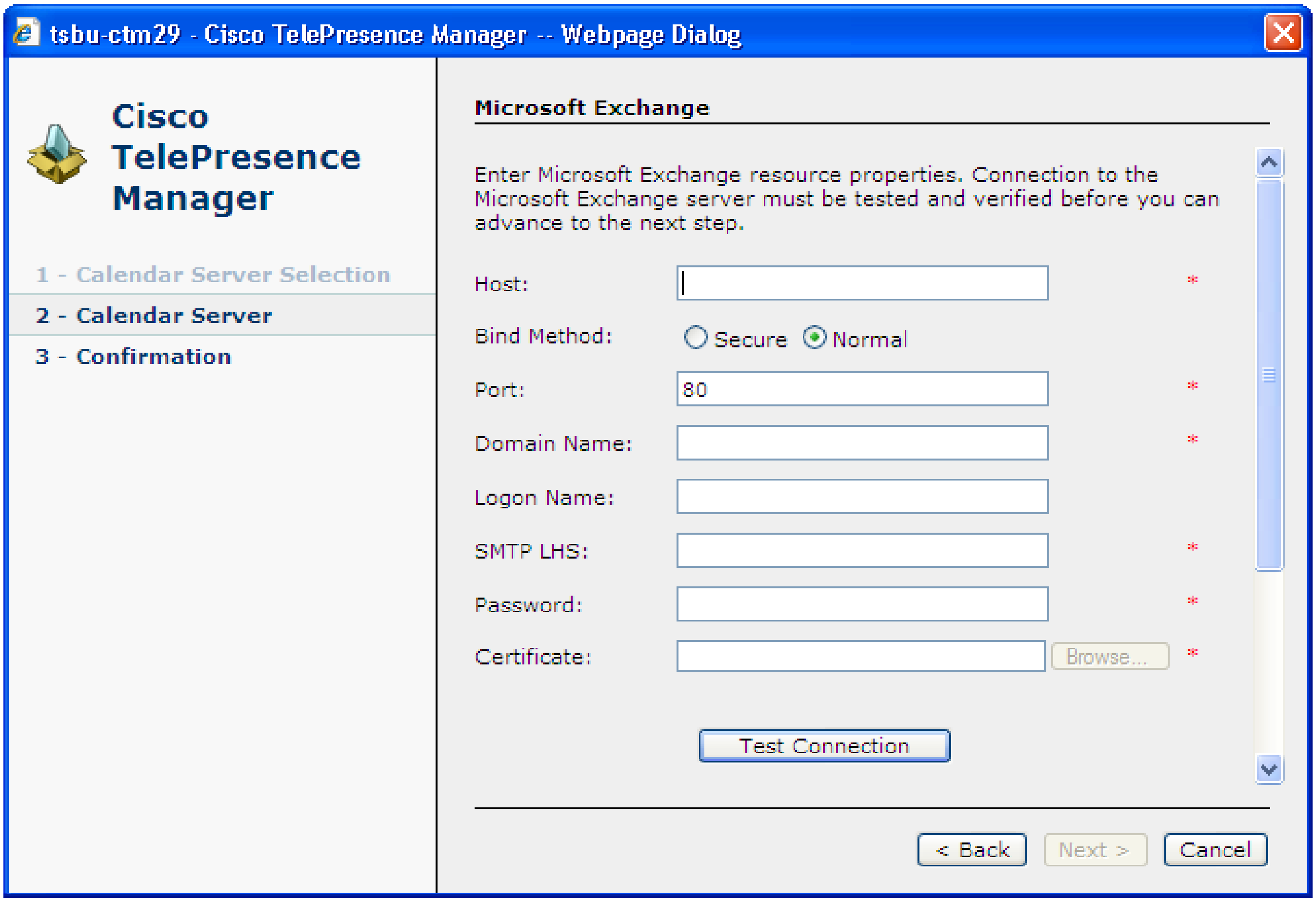
○ IBM Domino

○ None

Selection of Calendar server will display corresponding server set up screen in a coming step. If none is selectec ,the Calendar Server conf guration step will be skipped.

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 9-10 Cisco TelePresence Manager - Calendar Server MicroSoft Exchange Screen



tsbu-ctm29 - Cisco TelePresence Manager -- Webpage Dialog

Cisco TelePresence Manager

1 - Calendar Server Selection
2 - Calendar Server
3 - Confirmation

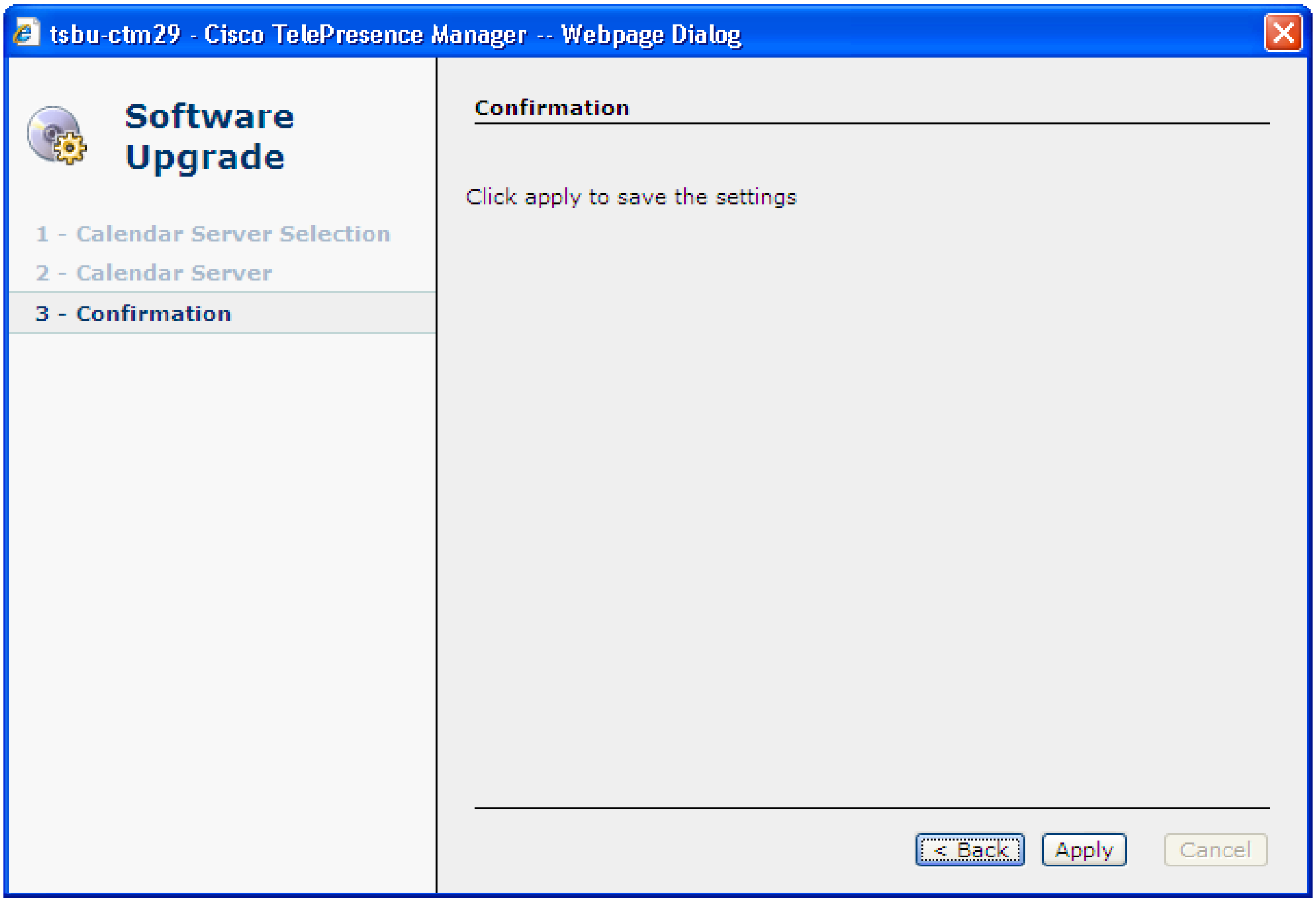
Microsoft Exchange

Enter Microsoft Exchange resource properties. Connection to the Microsoft Exchange server must be tested and verified before you can advance to the next step.

Host: *
Bind Method: ○ Secure ● Normal
Port: 80 *
Domain Name: *
Logon Name:
SMTP LHS: *
Password: *
Certificate: Browse... *

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

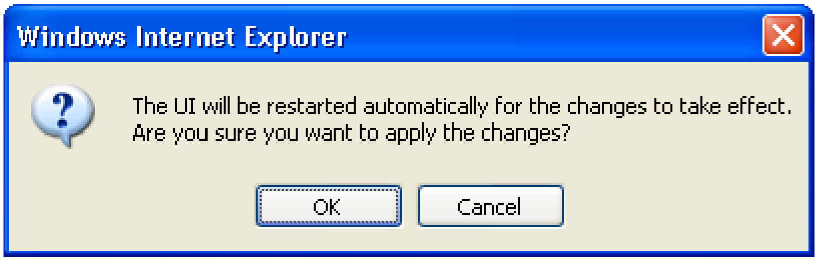
Figure 9-11 Cisco TelePresence Manager - Calendar Confirmation Screen


tsbu-ctm29 - Cisco TelePresence Manager -- Webpage Dialog
Software Upgrade
1 - Calendar Server Selection
2 - Calendar Server
3 - Confirmation
Confirmation
< Back
Apply
Cancel

Click apply to save the settings

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

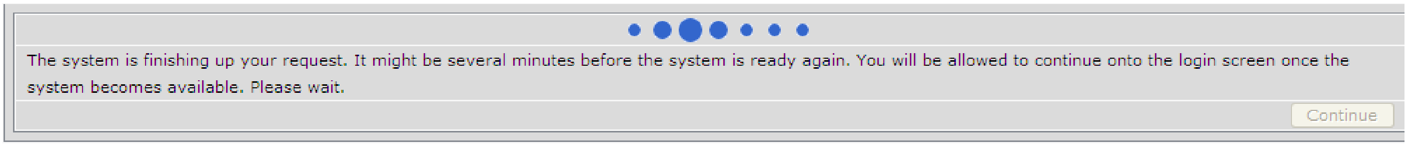
Figure 9-12 Apply Changes Screen



The UI will be restarted automatically for the changes to take effect.
Are you sure you want to apply the changes?

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

Figure 9-13 System Restart Notification Screen



The system is finishing up your request. It might be several minutes before the system is ready again. You will be allowed to continue onto the login screen once the system becomes available. Please wait.

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 9-14:

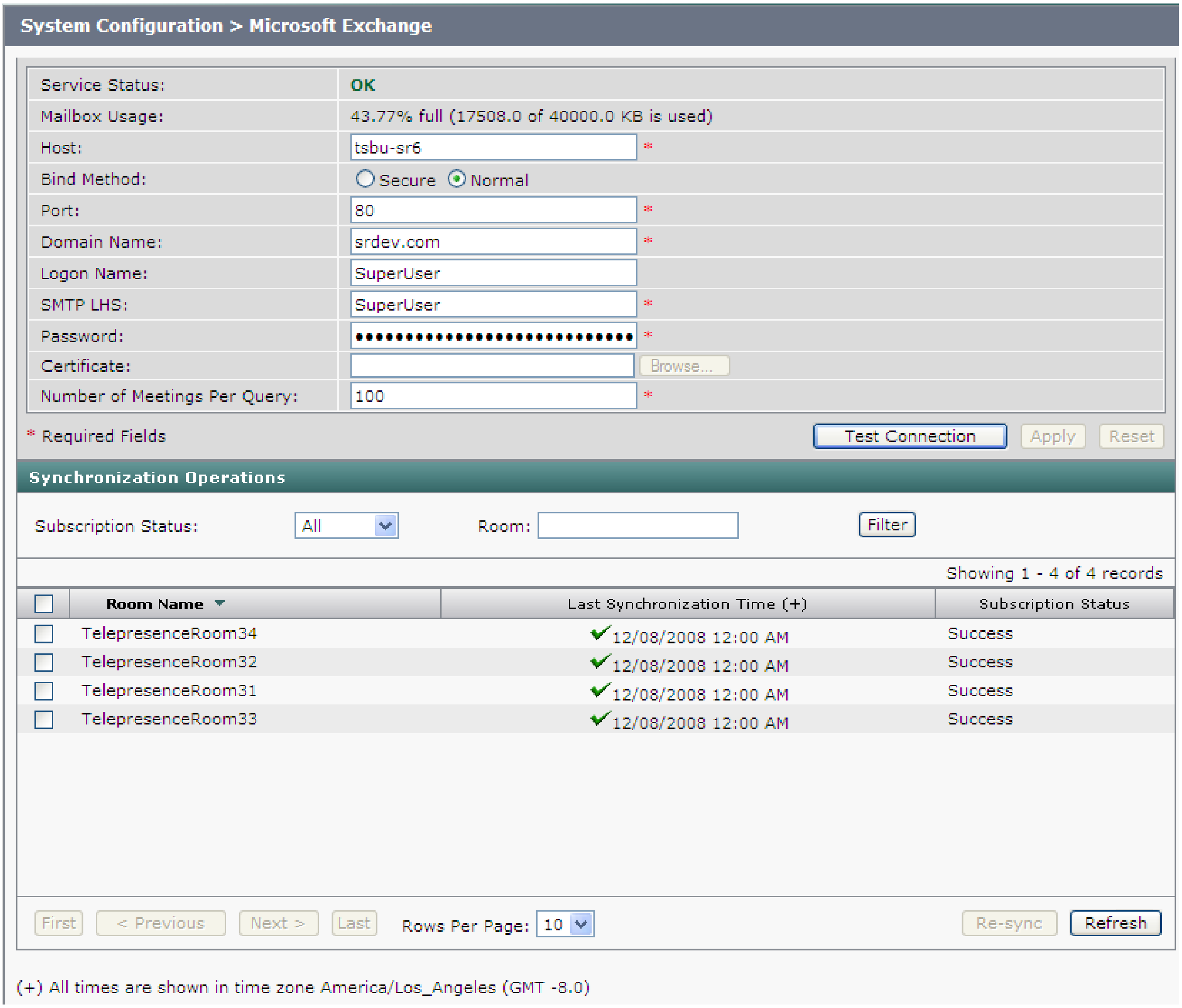
Step 1 Click **Test Connection.**

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. Entourage client is not supported.

Figure 9-14 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:	○ Secure ● Normal
Port:	80 *
Domain Name:	srdev.com *
Logon Name:	SuperUser
SMTP LHS:	SuperUser *
Password:	••••••••••••••••••••••••••••• *
Certificate:	Browse...
Number of Meetings Per Query:	100 *

* Required Fields

Synchronization Operations

Subscription Status: All Room:

Showing 1 - 4 of 4 records

□	Room Name ▼	Last Synchronization Time (+)	Subscription Status
□	TelepresenceRoom34	✓12/08/2008 12:00 AM	Success
□	TelepresenceRoom32	✓12/08/2008 12:00 AM	Success
□	TelepresenceRoom31	✓12/08/2008 12:00 AM	Success
□	TelepresenceRoom33	✓12/08/2008 12:00 AM	Success

Rows Per Page: 10

(+) 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 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 9-7 Microsoft Exchange Server (continued)

Field	Description or Settings
Bind Method	Choose the **Secure** or **Normal** radio button to select the binding method, as follows: • 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. **Note** 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 *ctsappaccount@mycompany.com* or *ctsappaccount.*
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 *ctsappsmtp@mycompany.com* enter *ctsappsmtp* 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.
Configure EWS	Use this button to bring up the Exchange Web Services window. Exchange needs to be configured for EWS when upgrading to Exchange 2007. **Note** EWS Authentication - must use the NTLM v1 authentication for version 1.6.2 and earlier. The Axis2 Library supports NTLM v2 for version 1.6.3 and later. **Note** This button is visible only during initial configuration. **Note** For WebDav (Exchange 2007 only) it was required to disable FBA. For EWS, FBA needs to be enabled.

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

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 9-8 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 9-8 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 9-15

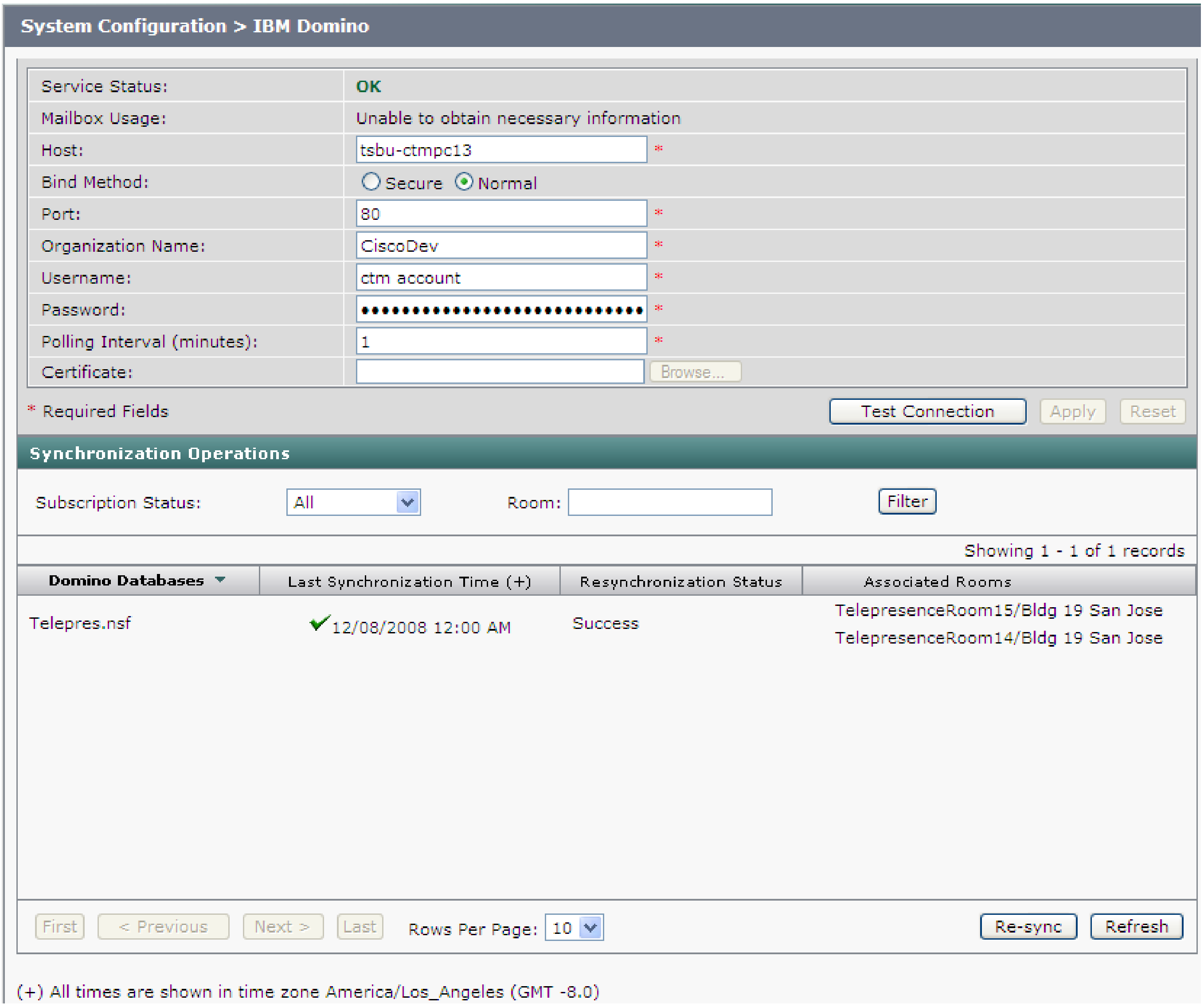
Step 1 Click **Test Connection.**

Step 2 To register new or modified settings, click **Apply.**

Step 3 To restore the original settings, click **Reset**.

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

Figure 9-15 IBM Domino Calendar Service Window



System Configuration > IBM Domino

Service Status:	OK
Mailbox Usage:	Unable to obtain necessary information
Host:	tsbu-ctmpc13 *
Bind Method:	○ Secure ● Normal
Port:	80 *
Organization Name:	CiscoDev *
Username:	ctm account *
Password:	•••••••••••••••••••••••••••••• *
Polling Interval (minutes):	1 *
Certificate:	

* Required Fields

Synchronization Operations

Subscription Status: All
Room:

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

(+) All times are shown in time zone America/Los_Angeles (GMT -8.0)

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

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

Table 9-9 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.
Bind Method	Choose the Secure or Normal radio button to select the binding method, as follows: • Secure—CTS-Manager communicates with the Domino server in secure mode using HTTPS 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.

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

Table 9-10 describes the information displayed in this area of the IBM Domino window.

Table 9-10 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.
Resynchronization Status	Status of the synchronization operation.
Associated Rooms	Name of the Cisco TelePresence meeting rooms associated with the Domino database. **Note** 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:

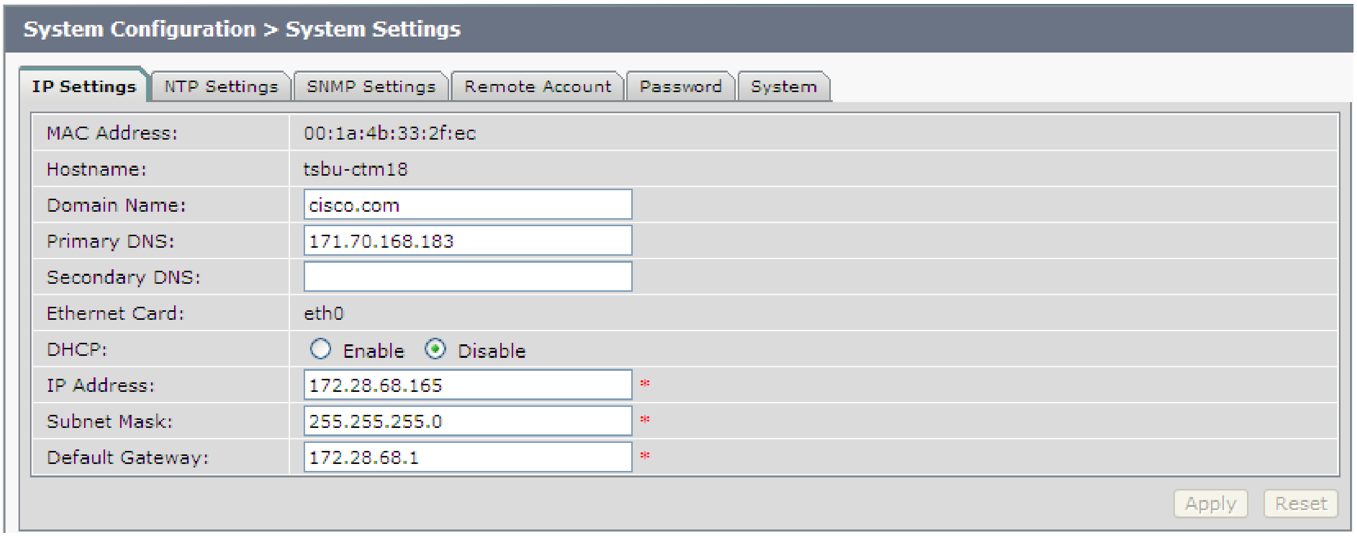
- IP Setting
- NTP Setting
- SNMP Setting
- Remote Account
- Password
- System Configuration - System Settings

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 9-16 describes the fields and buttons.

Figure 9-16 System Settings Window IP Settings Tab



System Configuration > System Settings

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:	○ Enable ● Disable
IP Address:	172.28.68.165 *
Subnet Mask:	255.255.255.0 *
Default Gateway:	172.28.68.1 *

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 **Apply.**

To restore the original settings, click **Reset**.

Table 9-11 describes the information displayed in this area of the IP Settings window

Table 9-11 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	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. **Note** To modify the IP settings for this Cisco TelePresence Manager, click the **Disable** radio button.

Table 9-11 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.

Deleting Server

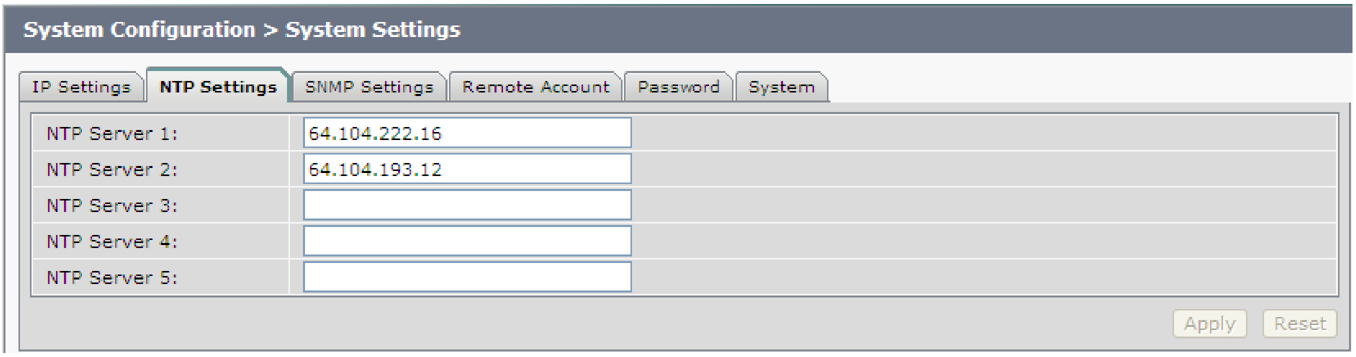
Before deleting a DNS server, it is important to first change existing servers like CUCM and MCU to IP from hostname before the DNS server is deleted. If the hostname is not changed first, the CUCM and MCU servers will be put in error status.

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 9-17 System Settings Window NTP Settings Tab



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**.

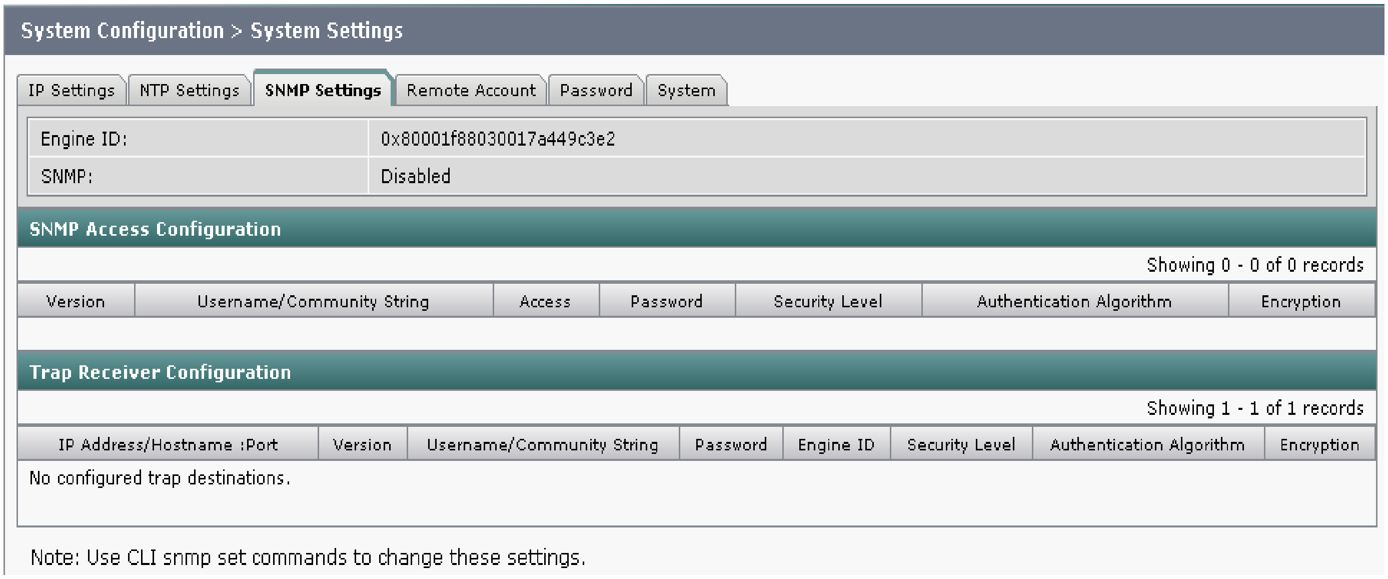
SNMP Setting

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 the CLI function to enable and disable SNMP Service and also configure communities and trap destinations.

Use the CLI commands to change these settings:

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

Figure 9-18 System Settings Window SNMP Settings Tab



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

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 9-12 describes the fields for SNMP settings.

Table 9-12 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 snamp 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 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 9-12 or is set by default:

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

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

The following is an example trap receiver entry:

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

Note v3 Trap destination user cannot overlap with snmpv3 user. This is allowed only if both v3user and trap destination have same password:
Allowed:
set snmp user add 3 admin rw authNoPriv snmppassword.
set snmp trapdest add 3 admin 172.20.124.44 authNoPriv snmppassword 0x80001f8803001a64635cd4

Not allowed:
set snmp user add 3 admin rw authNoPriv snmppassword
set snmp trapdest add 3 admin 172.20.124.44 authNoPriv cisco123 0x80001f8803001a64635cd4

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

Database - Status, Backup, and Restore

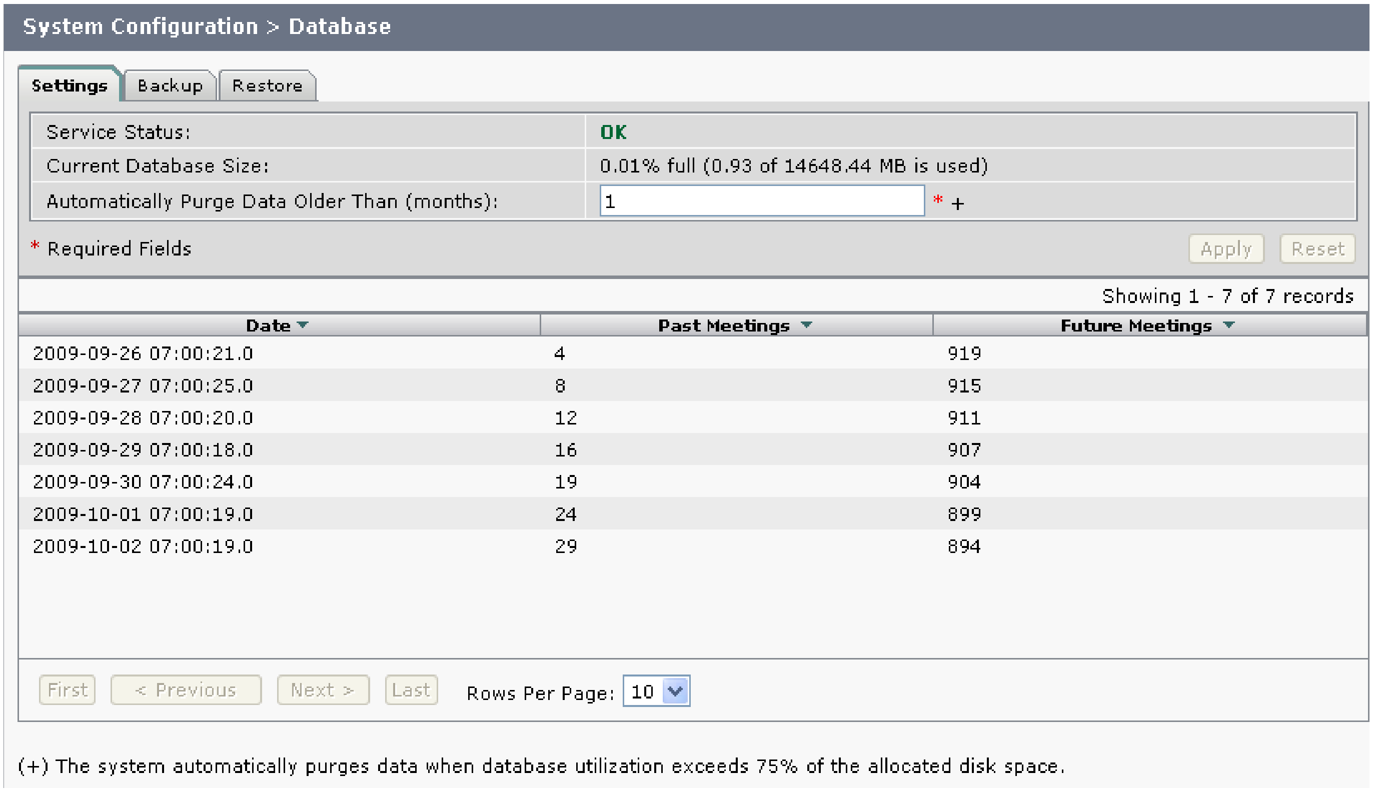
CTS-Manager uses an Informix database server to store information. The Database window allows the Administrator to view the database status and run backup and restore operations. Open the Database window to see the following choices:

- 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 9-19 Database Window Settings Tab



System Configuration > Database

Service Status:	OK
Current Database Size:	0.01% full (0.93 of 14648.44 MB is used)
Automatically Purge Data Older Than (months):	1 * +

* Required Fields

Showing 1 - 7 of 7 records

Date	Past Meetings	Future Meetings
2009-09-26 07:00:21.0	4	919
2009-09-27 07:00:25.0	8	915
2009-09-28 07:00:20.0	12	911
2009-09-29 07:00:18.0	16	907
2009-09-30 07:00:24.0	19	904
2009-10-01 07:00:19.0	24	899
2009-10-02 07:00:19.0	29	894

Rows Per Page: 10

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

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

Table 9-13 describes the information and settings that are accessible from the Database window Settings tab.

Table 9-13 Database Settings

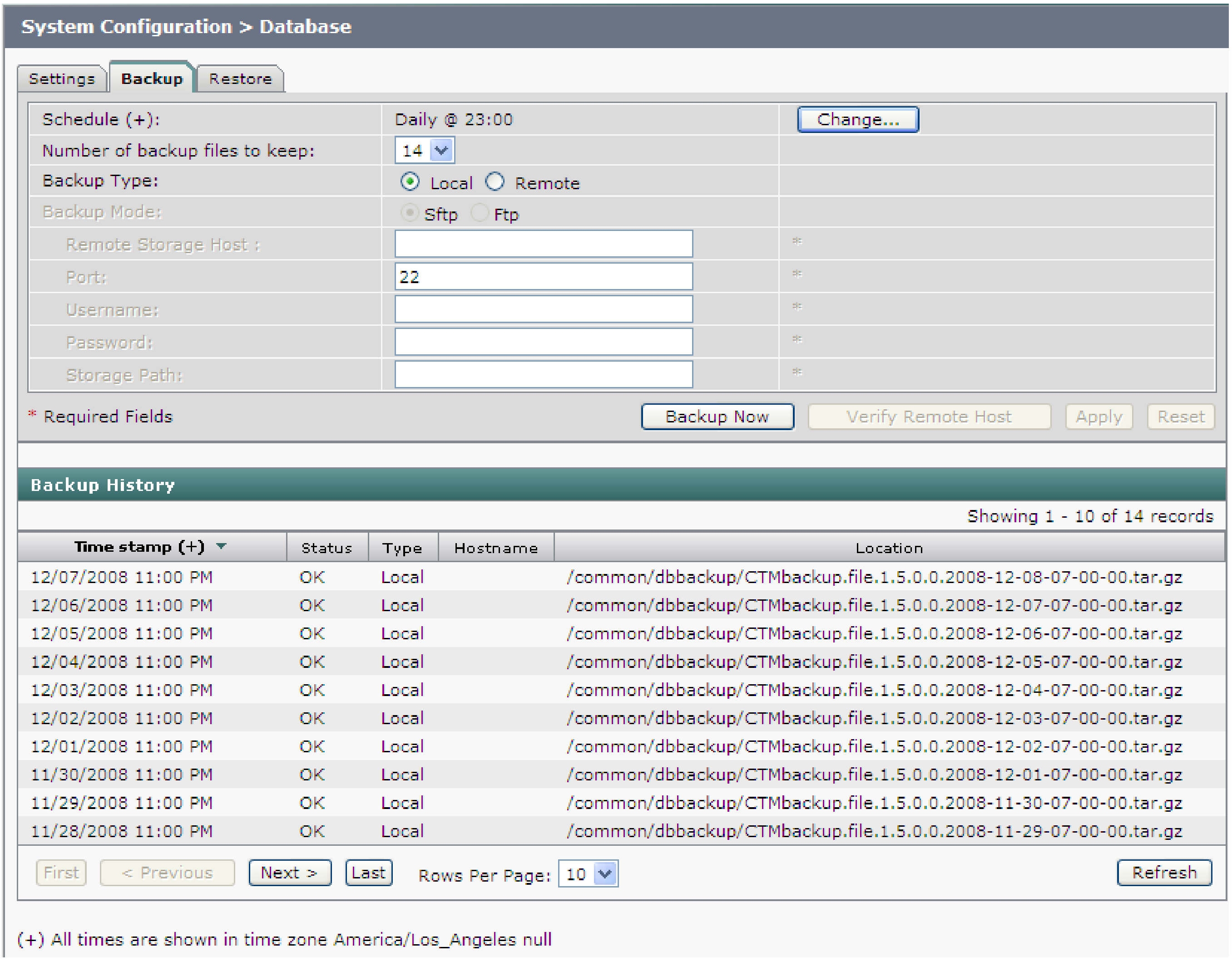
Field	Description or Settings
Service Status	Display-only status report of the Informix database server.
Current Database Size	Display-only report showing the size of the database as a percentage of the amount of total space available for a Cisco TelePresence Manager account in Directory Server. The number displayed should not exceed 75%.
Automatically purge data older than (months)	Sets the number of months of storage for the information in the database. Data older than the specified number of months is purged. 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. **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%.

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 9-20 System Configuration - Database Window Backup Tab



Schedule (+):	Daily @ 23:00	
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

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

Rows Per Page: 10

(+) 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 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

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 9-14 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 9-15 describes the Backup History and Restore History fields.

Table 9-15 Backup History and Restore History Fields

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

Restore

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

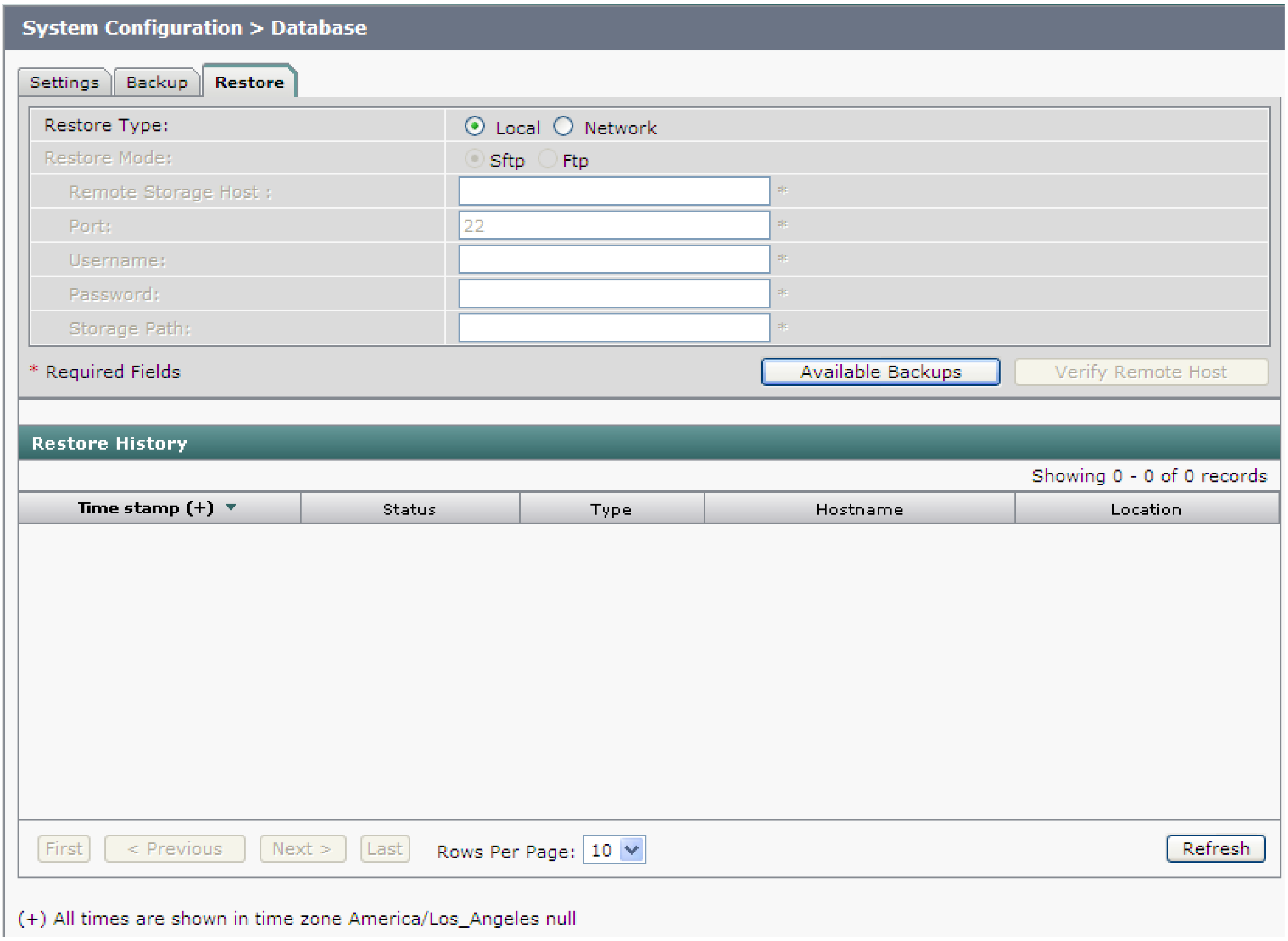
- Database data
- System SNMP configuration information
- System Certificates

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 CUCM node as publisher does not support mixed mode.

See Table 9-15 for a description of the fields.

Figure 9-21 Database Window Restore Tab



System Configuration > Database

Restore Type:	● Local ○ Network
Restore Mode:	● Sftp ○ Ftp
Remote Storage Host :	*
Port:	22 *
Username:	*
Password:	*
Storage Path:	*

* Required Fields

Restore History

Showing 0 - 0 of 0 records

Time stamp (+) ▼	Status	Type	Hostname	Location

Rows Per Page: 10

(+) 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 9-14 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.

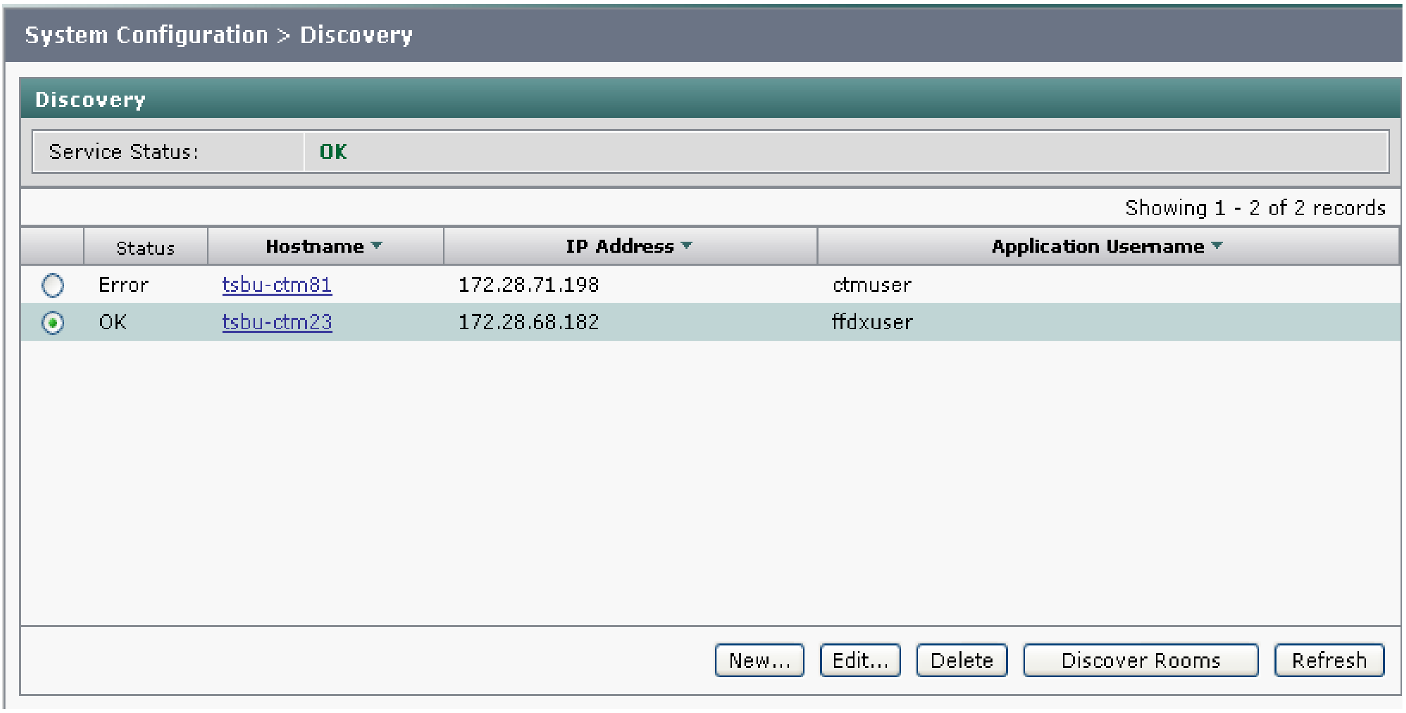
Step 3 Click **Restore Now**. This action initiates a full restore of the database from the backup file.

Discovery Service

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

The System Configuration>Discovery window opens. This window provides Service Status and the listings of the CUCM connections.

Note If changing settings in the CUCM, it is necessary to perform a Discovery in CTS-Manager to get the new settings registered. Otherwise, CTS-Manager won’t display or connect to the correct settings.


System Configuration > Discovery

Discovery

Service Status: OK

Showing 1 - 2 of 2 records

	Status	Hostname	IP Address	Application Username
○	Error	tsbu-ctm81	172.28.71.198	ctmuser
●	OK	tsbu-ctm23	172.28.68.182	ffdxuser

Click the radio button to select a host record. Once a record is selected, the buttons on the screen become active. Refer to Table 9-17 for a description of each button's function.

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

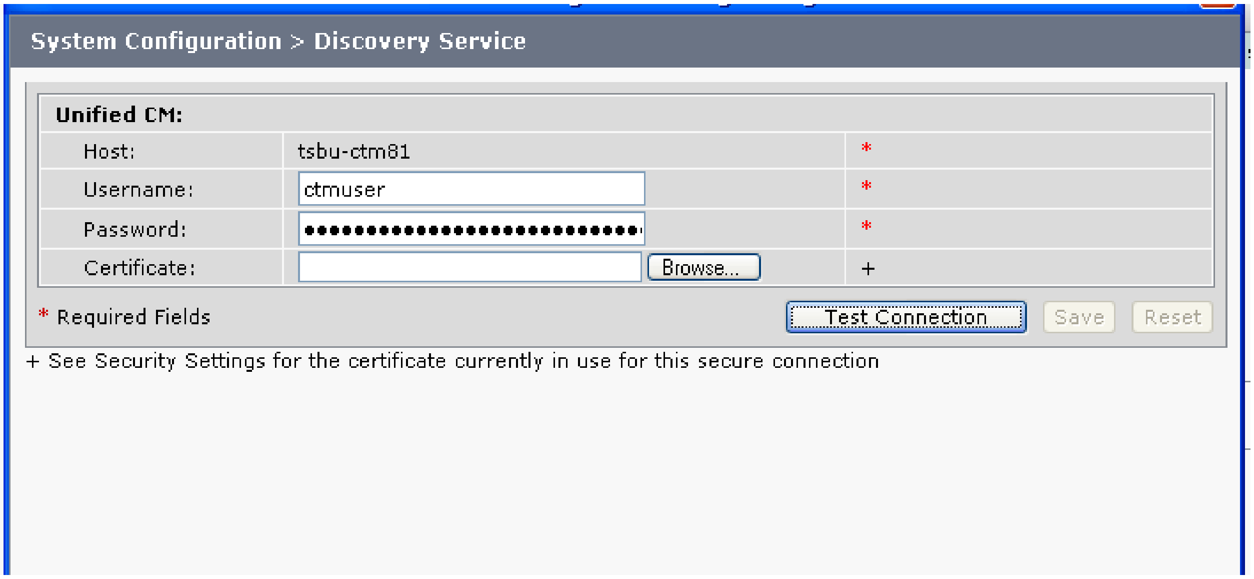
Note This process consumes a large amount of system processor time. System operation will be noticeably slower from the time that the Discover Rooms button has been clicked until the process is completed.

Table 9-16 Discover Cisco Unified Communications Manager Settings

Field	Description or Settings
Service Status	Display-only status report of system services. **Note** 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.
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.
Discover Rooms	This allows you to manually start the process that is periodically performed to discover new rooms added to Cisco UCM.
Refresh	This refreshes the window, ensuring the information is up to date.

Once you select a record and press **New** or **Edit**, the Discovery Service window appears as shown in Figure 9-22.

Figure 9-22 Discovery Service Window



System Configuration > Discovery Service

Unified CM:

Host:	tsbu-ctm81	*
Username:	ctmuser	*
Password:	●●●●●●●●●●●●●●●●●●●●●●●●●●●	*
Certificate:	Browse...	+

+ 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**.

Note When adding a Cisco Unified CM server that has a secure profile, you must also add a certificate. If you do not add a certificate, clicking Test Connection causes the following error message: 'Unable to create provider null'.

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

Table 9-17 describes fields, buttons, and settings.

Table 9-17 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. **Note** Do not import the Cisco Unified CM certificate (callManager.der) from the certificate list in the Cisco Unified Operating Administration application into CTS-Manager. You can only import Tomcat.der into CTS-Manager. You can find Tomcat.der in the Security > Certificate Management window in the Cisco Unified Operating System Administration application.
Test Connection	Tests the connection between CTS-Manager and CUCM server.

Table 9-17 Discovery Service Cisco Unified CM Settings (continued)

Field	Description or Settings
Save	Save the new settings.
Reset	Restore the original settings.

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

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

MCU Devices

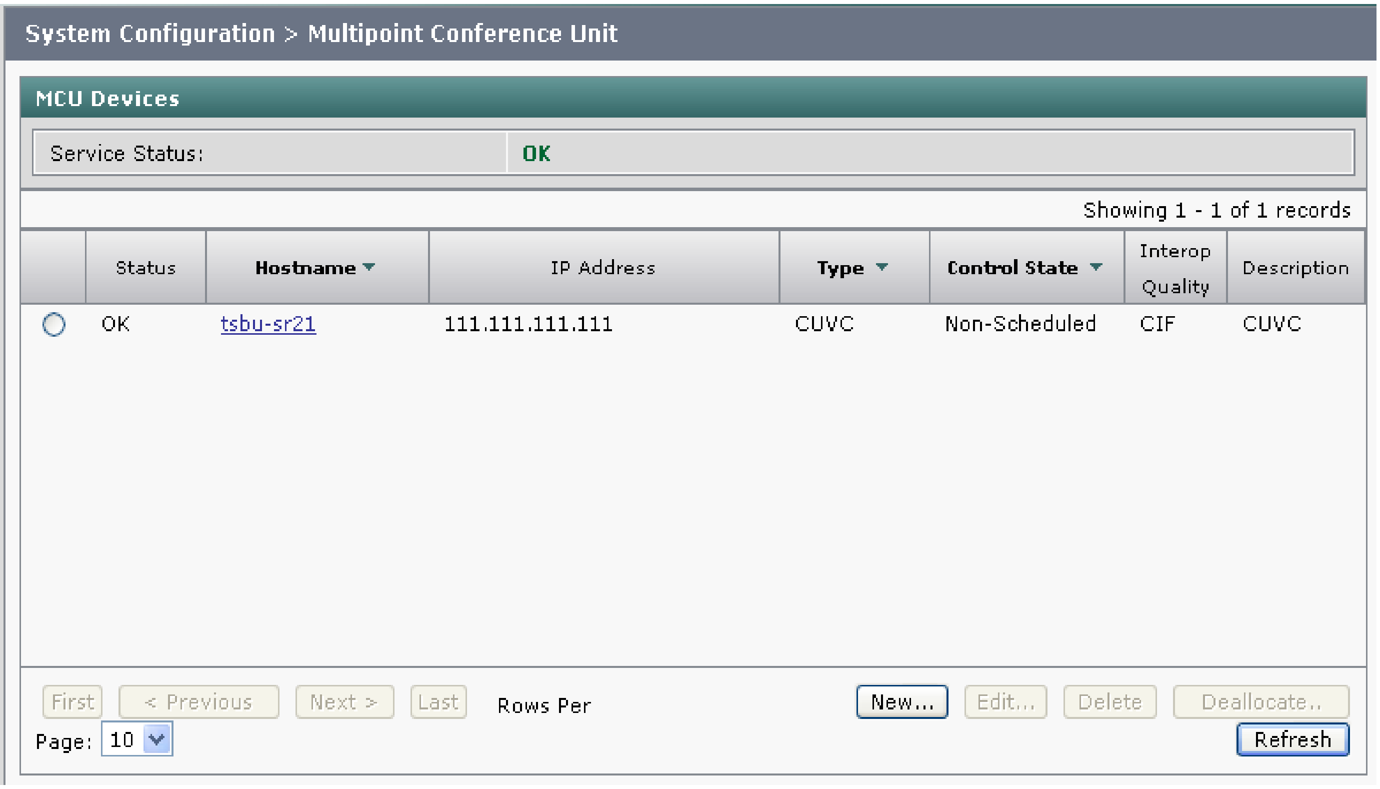
The MCU Devices window provides the ability to add and delete MCU devices. There are two MCU devices supported by CTS-Manager—Cisco TelePresence Multipoint Switch (CTMS) and Cisco Unified Video Conference device (CUVC). A CTMS communicates with CTS-Manager and the CTS-Manager provides the scheduling information to the different CTMSs and each CTMS provides the multipoint switching capabilities for the conference.

Specifying a CUVC as Non-Scheduled means the CUVC will not be used when a meeting is scheduled.

The MCU Devices support screen displays attributes for each MCU device configured with CTS-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 9-23 System Configuration>MCU Devices Window



Service Status: OK

Showing 1 - 1 of 1 records

	Status	Hostname	IP Address	Type	Control State	Interop Quality	Description
○	OK	tsbu-sr21	111.111.111.111	CUVC	Non-Scheduled	CIF	CUVC

Rows Per Page: 10

Table 9-18 describes the MCU Device fields.

Table 9-18 MCU Devices

Field	Description or Settings
Service Status	Allows the user to select MCU status: All, OK, or Error.
Status	MCU status: All, OK, or Error. **Error**: • Can indicate username and password mismatch between CTS-Manager and CTMS. • Network connectivity issue between CTS-Manager and CTMS. **Note** A CUVC always shows a status of OK
IP Address	The IP address of MCU.
Hostname	The configured Hostname 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. Clicking the arrow allows you to sort ascending or descending.
Control State	The Control State is either Scheduled or Non-Scheduled. If Non-Schedules is listed, the resource allocation function won't be used. The arrow allows you to sort ascending or descending.

Table 9-18 MCU Devices

Field	Description or Settings
Interop Quality	This area shows the selected CIF or 720p quality. This is not the quality the device can support, but it is the video quality mode currently set in the Application Setting window.
Description	The Description field displays the MCU device description, added when the MCU device was added. CUVC is the default; CTMS is configured in the CTMS program.

New MCU CTMS Device

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

Table 9-19 describes the fields that need to be filled out.

Table 9-19 Add a New MCU CTMS Device

Field	Description or Settings
Type	The selection is available from a pull-down list menu. CTMS or CUVC are the only MCU types. If only CTMS appears in the drop-down list, Interoperability with Video Conferencing has not been enabled. Use the Application Settings window to enable this feature.
MCU Hostname	The configured Hostname of the MCU. This is the LHS of the complete Host name
Username	This is the account name used to log into the CTMS.
Password	This is the account password used to log into the CTMS.
Control State	Select either Scheduled or Non-Scheduled. Specify whether the CTMS is available (scheduled) for meetings. CTMSs in a Scheduled state cannot be used to migrate meetings from other CTMSs.If Non-Scheduled is selected, resource allocation is not available. Selecting Scheduled allows resource allocations.

Edit the MCU setting

To edit a MCU Device, click the radio button on the device line to select that device. Click the Edit button. The Edit...MCU Devices window appears. Table 9-20 describes the fields that can be changed.

Table 9-20 Edit MCU CUVC Devices

Field	Description or Settings
Username	This is the account name used to log into the CTMS.

Table 9-20 Edit MCU CUVC Devices

Field	Description or Settings
Password	This is the account password used to log into the CTMS.
Control State	Select either Scheduled or Non-Scheduled. Specify whether the CTMS is available (scheduled) for meetings. CTMSes in a Scheduled state cannot be used to migrate meetings from other CTMSes. If Non-Scheduled is selected, resource allocation is not available. Selecting Scheduled allows resource allocations.

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.**

Deallocate a MCU

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

Then in the MCU, click the radio button next to the selected device and then click **Deallocate**

Refreshing the list of MCUs

Click the **Refresh** button to refresh the list of MCU devices.

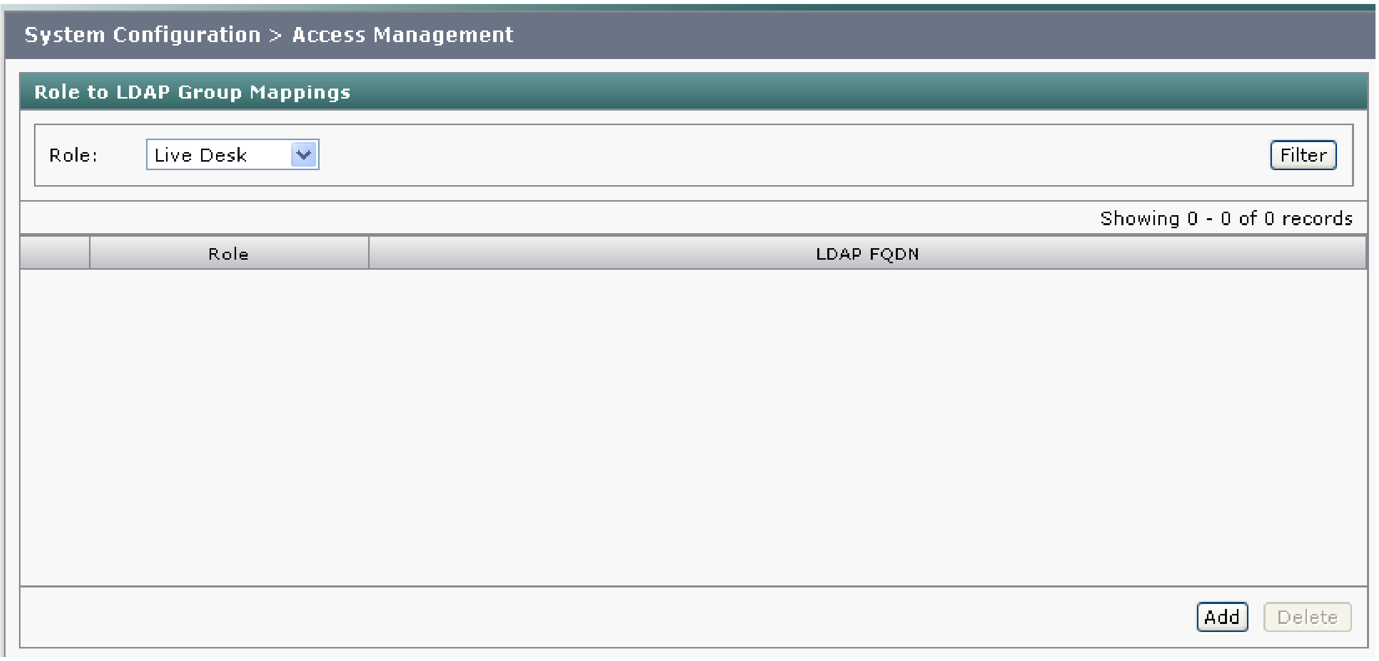
Note Once Interop has been enabled (see Application Settings), a CTMS device can only be added to CTS-Manager if it is interop-ready. An interop-ready device is defined as running a certain level of software release.

Access Management

From the Directory Server, 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 roles—a Live Desk and an administrator.

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

Figure 9-24 Access Management Window



System Configuration > Access Management

Role to LDAP Group Mappings

Role: Live Desk

Showing 0 - 0 of 0 records

	Role	LDAP FQDN

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 Live Desk—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 Live Desk or Administrator role.

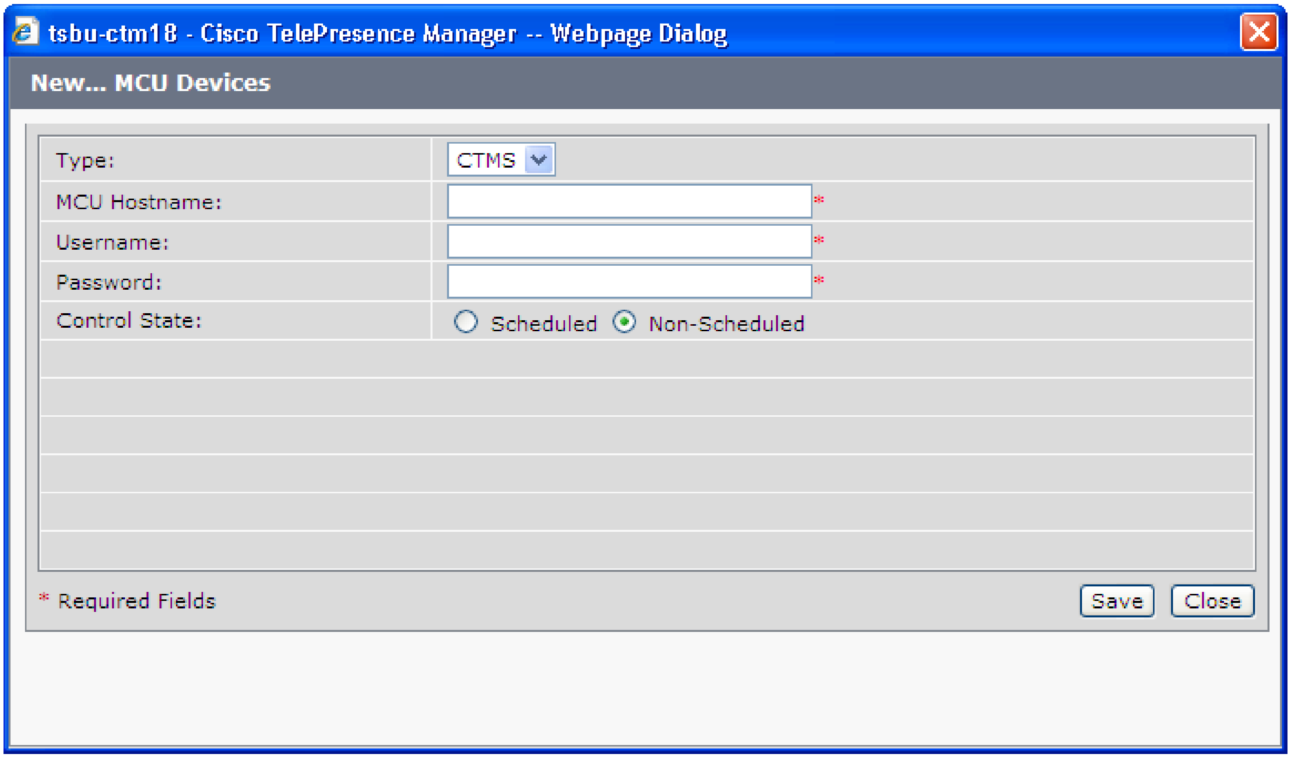
Cisco TelePresence Multipoint Switch (CTMS)

A CTMS communicates with the Cisco TelePresence Manager. CTMSes 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 9-25 Adding New CTMS - MCU Devices Window



tsbu-ctm18 - Cisco TelePresence Manager -- Webpage Dialog

New... MCU Devices

Type:	CTMS
MCU Hostname:	*
Username:	*
Password:	*
Control State:	○ Scheduled ● Non-Scheduled

* Required Fields

Table 9-21 describes the fields in the New MCU Devices window.

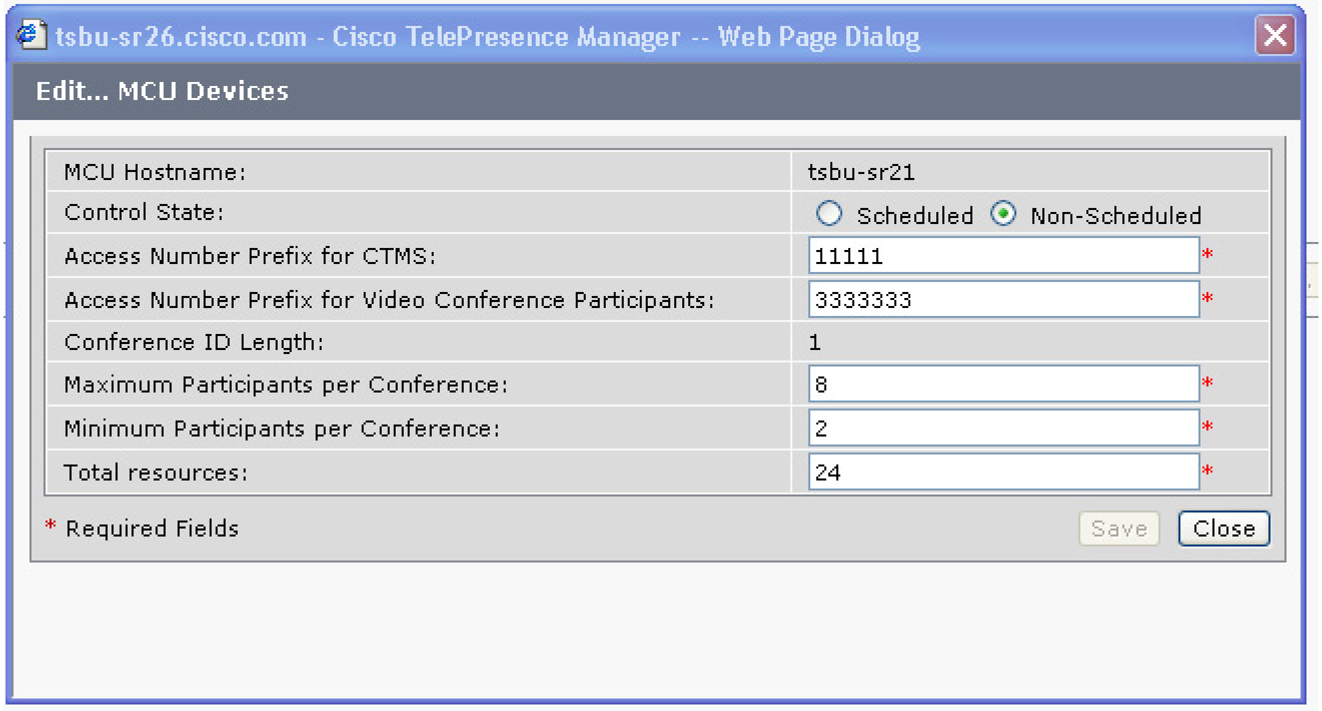
Table 9-21 Registering a CTMS with Cisco TelePresence Manager

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 Application Settings 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.
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. **Note** 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.

Figure 9-26



tsbu-sr26.cisco.com - Cisco TelePresence Manager -- Web Page Dialog

Edit... MCU Devices

MCU Hostname:	tsbu-sr21
Control State:	○ Scheduled ● Non-Scheduled
Access Number Prefix for CTMS:	11111 *
Access Number Prefix for Video Conference Participants:	3333333 *
Conference ID Length:	1
Maximum Participants per Conference:	8 *
Minimum Participants per Conference:	2 *
Total resources:	24 *

* Required Fields

Table 9-22 describes the fields in the Edit MCU Devices window.

Table 9-22 Edit MCU CTMS Devices

Field	Description or Settings
Control State	The Control State is either Scheduled or Non-Scheduled. Specify whether the MCU CTMS is to be available for meetings. The resources of a scheduled MCU CTMS can be used when meetings are scheduled. Specifying a MCU CTMS as Non-Scheduled means it will not be used when a meeting is scheduled. CTMSs in a Scheduled state cannot be used to migrate meetings from other CTMSs.
Access Number Prefix for CTMS:	The access number prefix for your CTMS is based on your enterprise dialing plan.
Access Number Prefix for Video Conference Participants:	This access number prefix is based on your enterprise dialing plan.

Table 9-22 Edit MCU CTMS Devices

Field	Description or Settings
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.
Maximum Participants per Conference:	The Maximum number of participants per conference is 8.
Minimum Participants per Conference:	The Minimum number of participants per conference is 2.
Total Resources:	This field needs to have the total number of resources available to the device.This value should be greater than the Maximum Participants per Conference.

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 9-23 Configuring 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 Application Settings window to enable Interoperability with Video Conferencing. **Note** Only one CUVC can be supported by one 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 an Interop meeting will not be available when a meeting is scheduled.
Access Number Prefix for CTMS	The access number prefix for your CTMS is based on your enterprise dialing plan.

Table 9-23 Configuring a CUVC with Cisco TelePresence Manager (continued)

Field	Description or Settings
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.
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.
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 Application Settings window to enable Interoperability with Video Conferencing. **Note** Only one CUVC can be supported by one CTS-Manager.

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 9-24 Editing Registered CUVC Configuration Settings

Field	Description or Settings
Control State	Specify whether the CUVC is available (scheduled) for meetings. The resources of a scheduled CUVC can be used when meetings are scheduled. Specifying a CUVC as Non-Scheduled means an Interop meeting will not be available when a meeting is scheduled
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.
Maximum Participants per Conference	Enter a numeric value for the maximum number of meeting participants that may dial into the conference call. **Note** 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.

Live Desks

Live Desk Role

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

- System Information
- System Status
- Support
- Troubleshooting

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

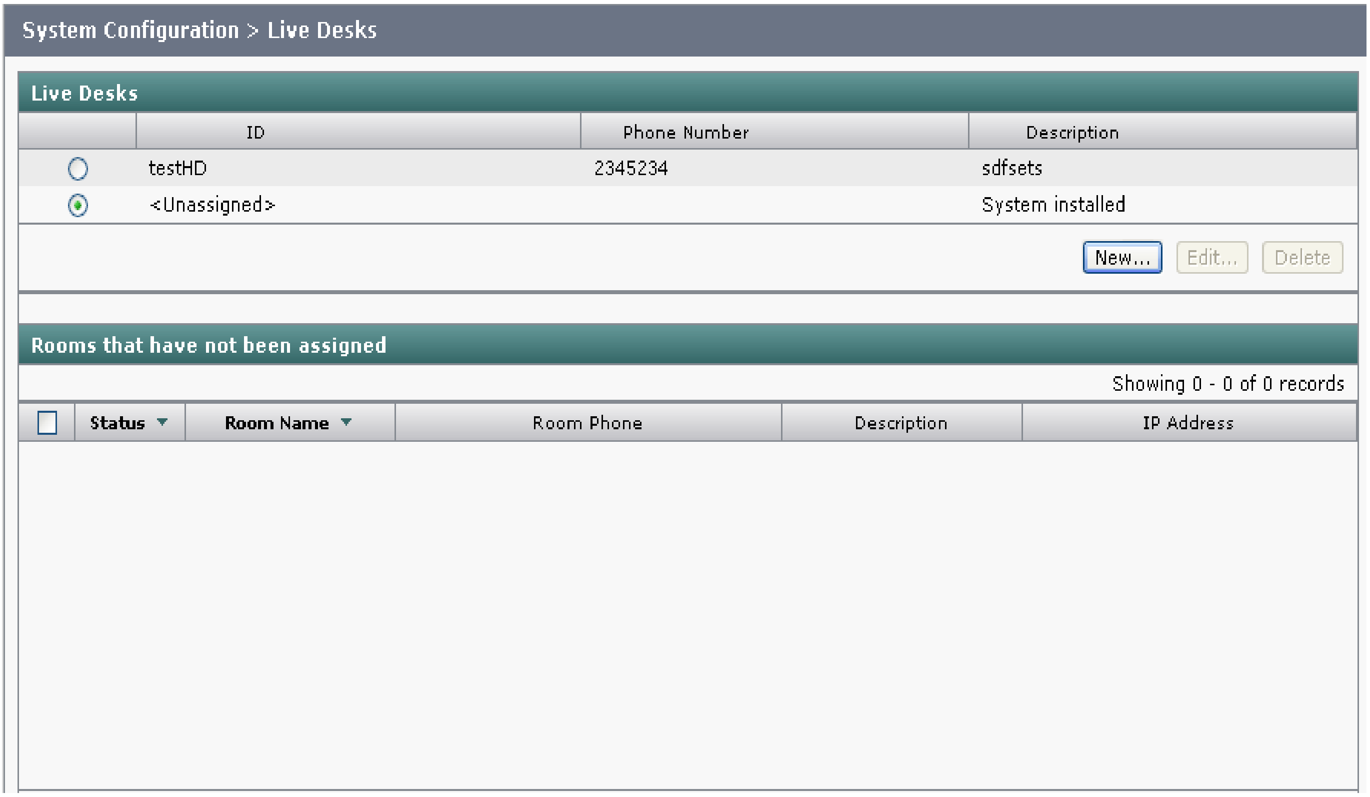
- Scheduling meetings
- Using the Cisco IP phone in a Cisco TelePresence-enabled meeting room
- Using the tools supplied by the CTS-Manager to monitor the system and the schedule of upcoming meetings and to update meeting requests
- Gathering data to supply to the administrator when a problem cannot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

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

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

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

Figure 9-27 System Configuration - Live Desk Window



System Configuration > Live Desks

Live Desks

	ID	Phone Number	Description
○	testHD	2345234	sdfsets
●	<Unassigned>		System installed

Rooms that have not been assigned

Showing 0 - 0 of 0 records

□	Status ▼	Room Name ▼	Room Phone	Description	IP Address

Creating Live Desk Personnel

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

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

Step 1 Click **New** to display the new Live Desks window.

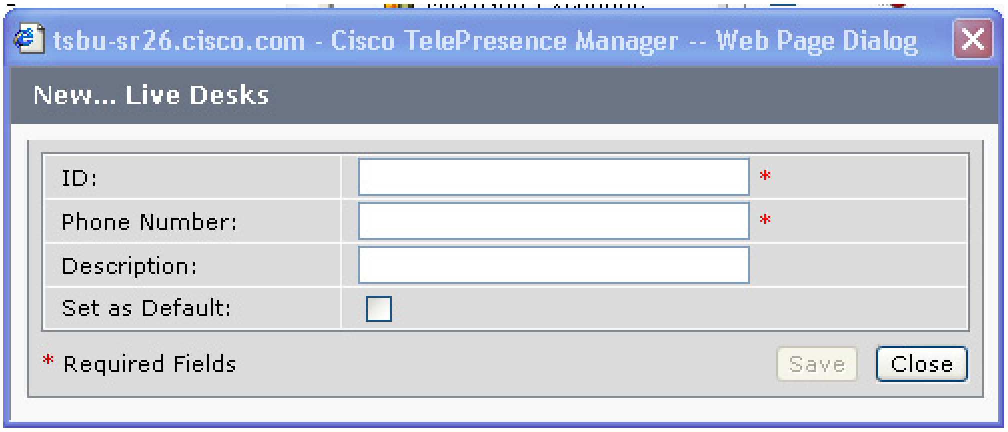
Step 2 In the New Live Desks window, enter an identifier for the Live Desk in the ID field

Step 3 Enter a phone number in the Phone Number field.

Step 4 You can choose to supply other information identifying the Live Desk person in the Description field.

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

Figure 9-28 Adding a Live Desk Window



tsbu-sr26.cisco.com - Cisco TelePresence Manager -- Web Page Dialog

New... Live Desks

ID:	*
Phone Number:	*
Description:	
Set as Default:	□

* Required Fields

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

Assigning a Room to a Specific Live Desk

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

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

Step 2 Select a Live Desk from the **Assign Selected Rooms** drop-down list.

Step 3 Click **Apply**.

To edit the Live Desk assignment:

Step 4 Select the radio button next to the Live Desk ID and click **Edit**.

Step 5 In the Edit Live Desks window, you can change the phone number and other information identifying the Live Desk.

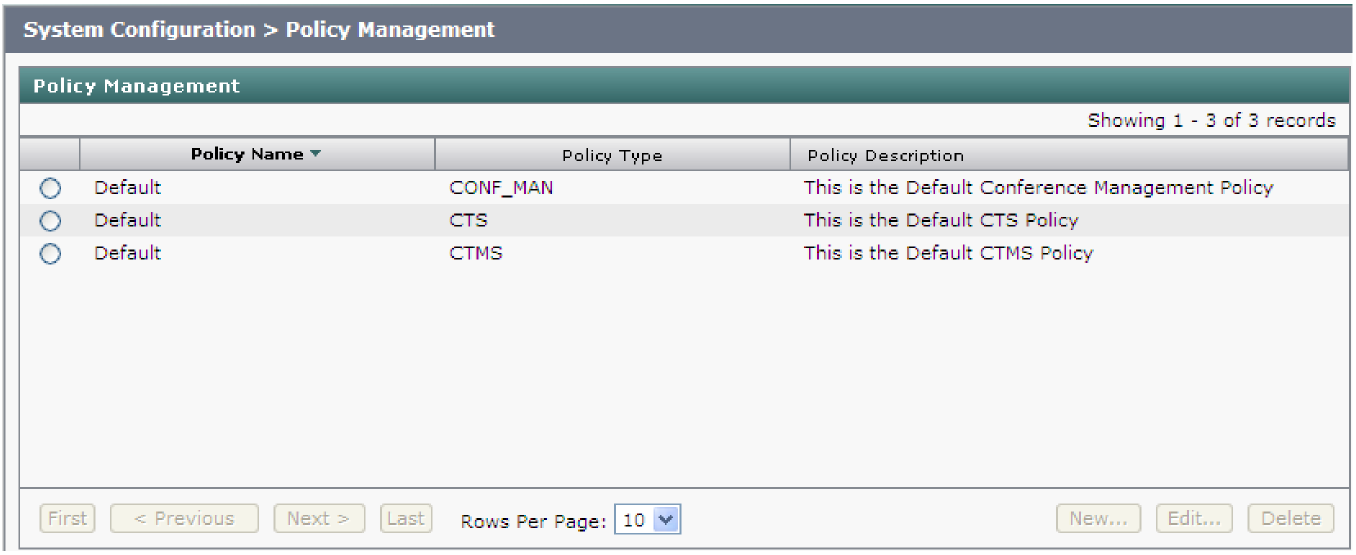
Step 6 To delete a Live Desk, select the radio button next to the Live Desk ID and click **Delete**.

Note CTS-Manager 1.6 supports a default Live Desk that is assigned to 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 1.6 from an earlier version that allows a Live Desk to share a phone number with another Live Desk, during the upgrade CTS-Manager 1.6 changes the phone number of one of the Live Desks and assigns that Live Desk to the endpoint.

Policy Management

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

Figure 9-29 System Configuration - Policy Management Window



System Configuration > Policy Management

Policy Management

Showing 1 - 3 of 3 records

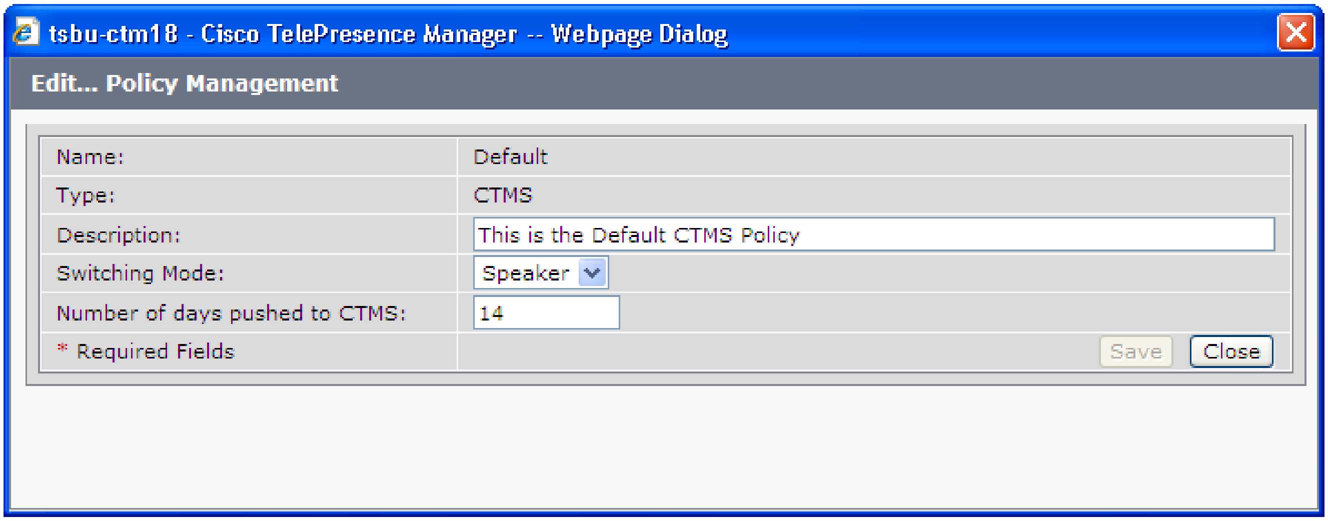
	Policy Name	Policy Type	Policy Description
○	Default	CONF_MAN	This is the Default Conference Management Policy
○	Default	CTS	This is the Default CTS Policy
○	Default	CTMS	This is the Default CTMS Policy

Rows Per Page: 10

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 9-30 CTMS Policy Window



tsbu-ctm18 - Cisco TelePresence Manager -- Webpage Dialog

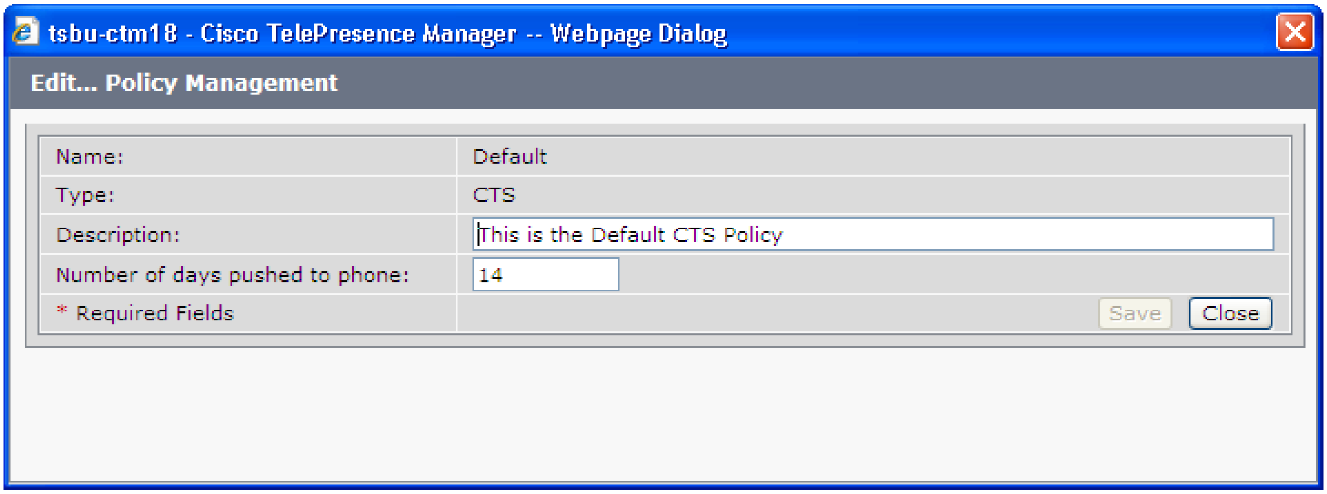
Edit... Policy Management

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 9-31 CTS Endpoint Policy Window


tsbu-ctm18 - Cisco TelePresence Manager -- Webpage Dialog
Edit... Policy Management

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

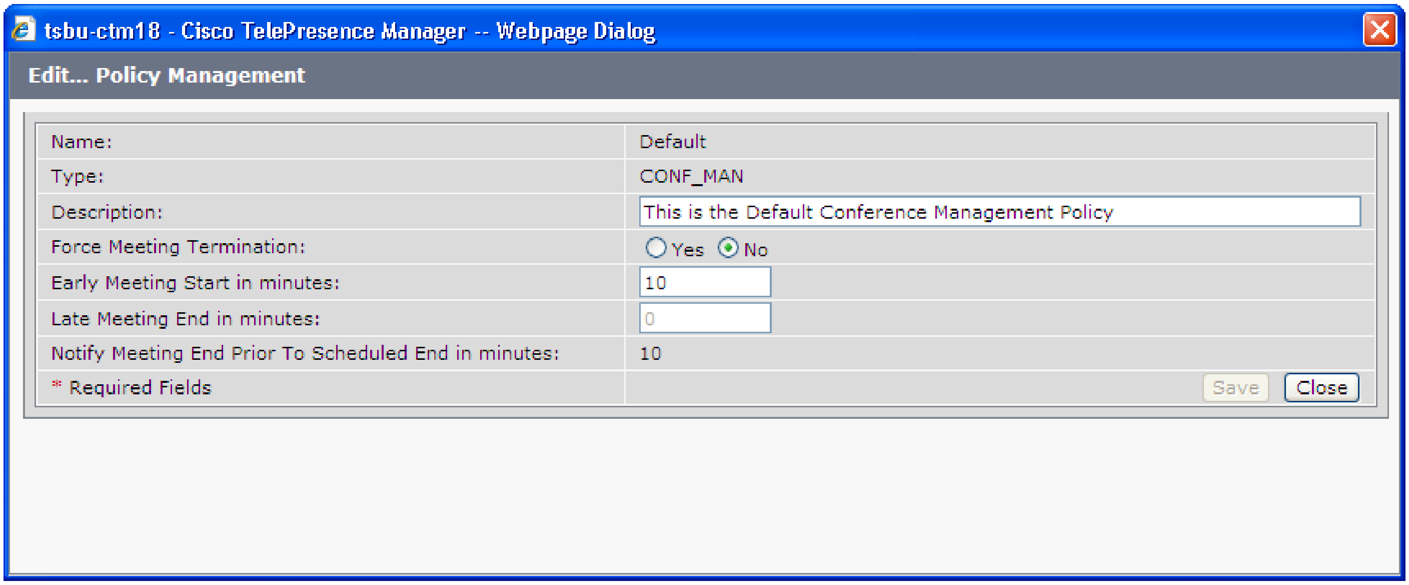
Conference Manager policy

The 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 9-32 Conference Manager Policy Window



tsbu-ctm18 - Cisco TelePresence Manager -- Webpage Dialog

Edit... Policy Management

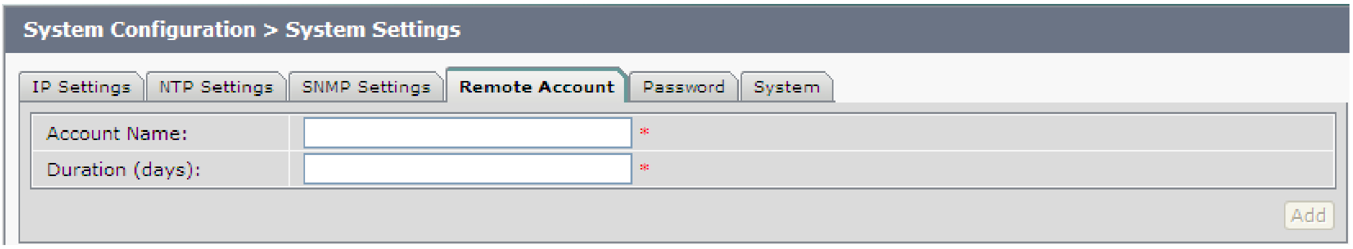
Name:	Default
Type:	CONF_MAN
Description:	This is the Default Conference Management Policy
Force Meeting Termination:	○ Yes ● No
Early Meeting Start in minutes:	10
Late Meeting End in minutes:	0
Notify Meeting End Prior To Scheduled End in minutes:	10
* Required Fields	Save Close

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 9-33 System Settings Window Remote Account Tab



System Configuration > System Settings

Account Name:	*
Duration (days):	*

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.

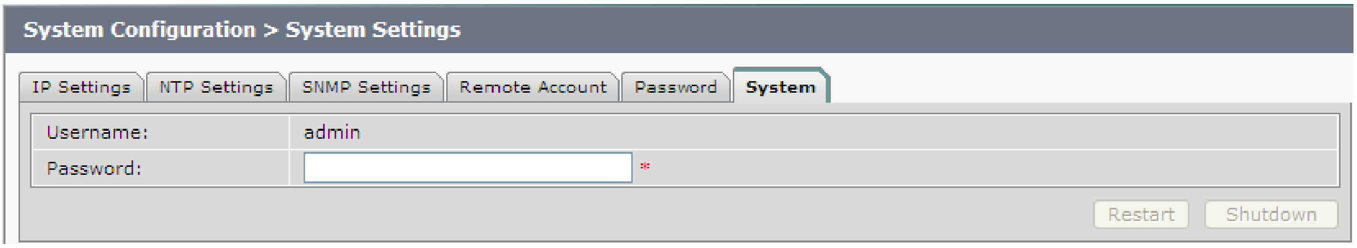
To complete this process, the account name and pass phrase are entered into a utility at the following Cisco Internal web site:
https://remotesupporttool.cisco.com/logon.php

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 9-34 System Settings Window System Tab



System Configuration > System Settings

Username: admin
Password: *

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

- The username cannot be changed.

Step 2 Enter your password.

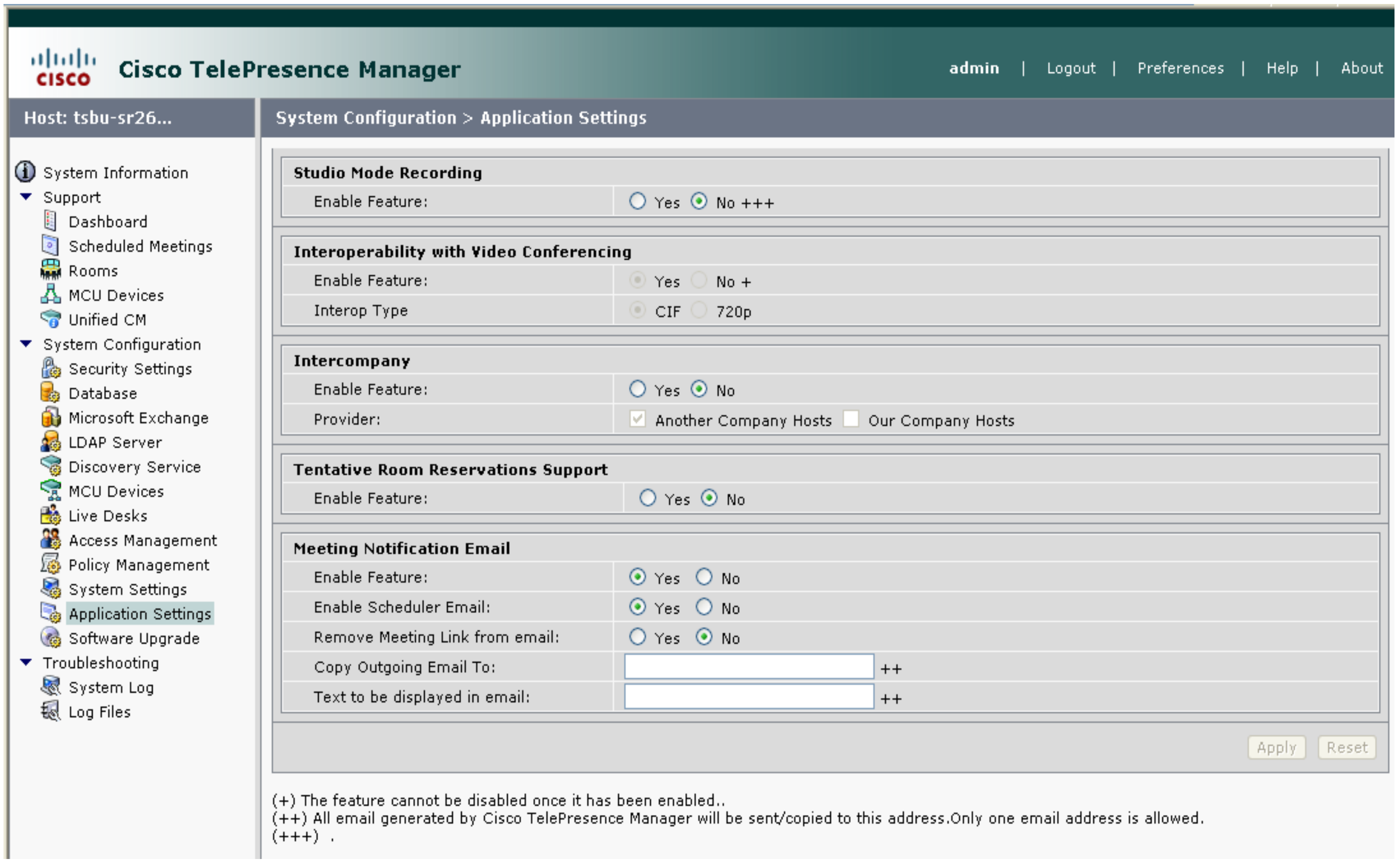
Step 3 Click **Restart**.

This will restart the CTS-Manager system.

Application Settings

The System Configuration Applications Settings window is used to set five different options: Studio Mode Recording, Interoperability with Video Conferencing, Intercompany, Tentative Room Reservations Support, and Meeting Notification Email.

Figure 9-35 Application Settings Window



System Configuration > Application Settings

Studio Mode Recording

Enable Feature:	○ Yes ● No +++

Interoperability with Video Conferencing

Enable Feature:	● Yes ○ No +
Interop Type	● CIF ○ 720p

Intercompany

Enable Feature:	○ Yes ● No
Provider:	☑ Another Company Hosts □ Our Company Hosts

Tentative Room Reservations Support

Enable Feature:	○ Yes ● No

Meeting Notification Email

Enable Feature:	● Yes ○ No
Enable Scheduler Email:	● Yes ○ No
Remove Meeting Link from email:	○ Yes ● No
Copy Outgoing Email To:	++
Text to be displayed in email:	++

(+) The feature cannot be disabled once it has been enabled..
(++) All email generated by Cisco TelePresence Manager will be sent/copied to this address.Only one email address is allowed.
(+++) .

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.

Recording enabled globally

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

The steps in this would be:

- Schedule a single meeting with one room.
- From the Application setting, select Recording to Yes.
- From Outlook, select this meeting and modify it into a recurring meeting.
- All instances now have recording enabled on them.

Interoperability with Video Conferencing Settings

Enable Feature: The default setting for interoperability with video conferencing is "Disable." This feature cannot be disabled once it has been enabled.

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, from the MCU Devices window, first Deallocate the CUVC and then Delete it.

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

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

Select "720p" for HD Interop support with CUVC 7.0. If this is selected, the Admin UI provides an option to add one CUVC at 720p. Only one CUVC is allowed.

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

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

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

Intercompany Setting

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

Note An Intercompany TelePresence meeting cannot be configured for Interop.

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

Another Company Host

If you select this feature, this allows another company to set up TelePresence meetings. You must provide the host with the rooms' information that will be participating in the TelePresence calls. For example, if it is a room-to-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 Host

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

Tentative Room Reservations Support

A tentative room reservation is a meeting invite that has been viewed by room owner but not accepted yet. CTS-Manager tentative reservation is identical to accepted reservation.

Enabling this feature allows the CTS-Manager to process meetings for tentative room reservations, i.e., place a room in proxy mode. This option is supported only for Exchange and not for Domino.

Tentative acceptance is off by default, the administrator needs to turn on this feature globally to incorporate all rooms hosted by CTS-Manager.

Note If a user has not read a meeting invite for a meeting, it would not show up on the phone UI. If the meeting invite is updated and is not viewed, the phone UI would be out-of-sync. The room or proxy mode room calendar may show double bookings.

Once Tentative room reservations are turned on, this feature cannot be turned off. A re-install is required to change the on to off option.

Once all room reservations are confirmed the meeting should appear 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 are sent approximately within 10-15 minutes.

The best practice for tentative room reservations is to enabled it for private (office) rooms so if the meetings scheduled aren't in sync the result is ok.

Tentative meeting not enabled

The following describes the behavior of the CTS-Manager when the tentative meeting is not enabled.

If the user creates a meeting with 1 auto-accept room (AAA) and 1 proxy room. The Proxy room accepts the meeting and the meeting is processed as a point-point meeting in CTS-Manager. Then the meeting is modified to a different time and the proxy room has not opened the meeting invite or clicked on the tentative or accept buttons. The meeting schedule in CTS-Manager is modified with a new time with both rooms shown and marked as scheduled without error. However, the proxy room calendar does not have the modified meeting time updated. To have the times sync, the proxy room must accept the modified time.

Problems can occur if public rooms and conference rooms are set up with tentative enabled. if the meeting is not accepted, the proxy setting can be out-of-sync and double booking for the room can occur. Thus, the best practice for public or conference rooms is to not have this feature enabled and force a proxy confirmation acceptance.

.

Meeting Notification Email Settings

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 Scheduler Email: This option shuts off or turns on the email to be sent to the scheduler.

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

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

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

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

Text to be displayed in email: Enter the text you want to appear in the email message header.

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.

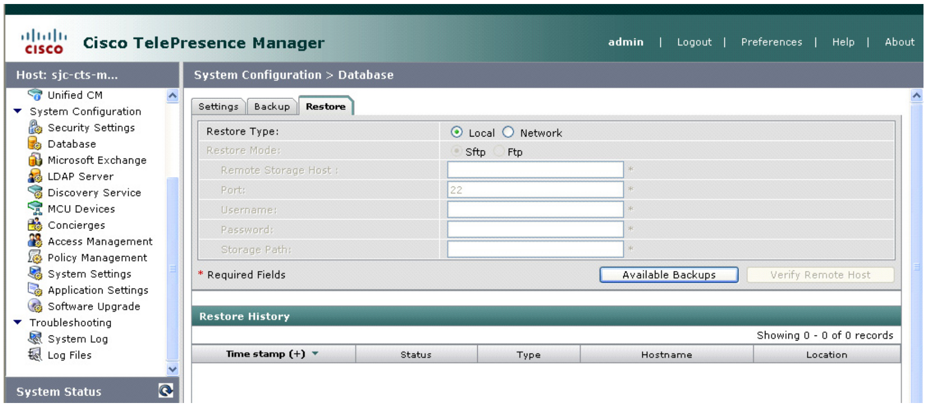
Note It is recommended to use the same hostname and the same IP address for CTS-Manager replacement server.

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 9-36 System Configuration Database Restore Backup Window



Restore Type:	● Local ○ Network
Restore Mode:	● Sftp ○ Ftp
Remote Storage Host :	*
Port:	22 *
Username:	*
Password:	*
Storage Path:	*

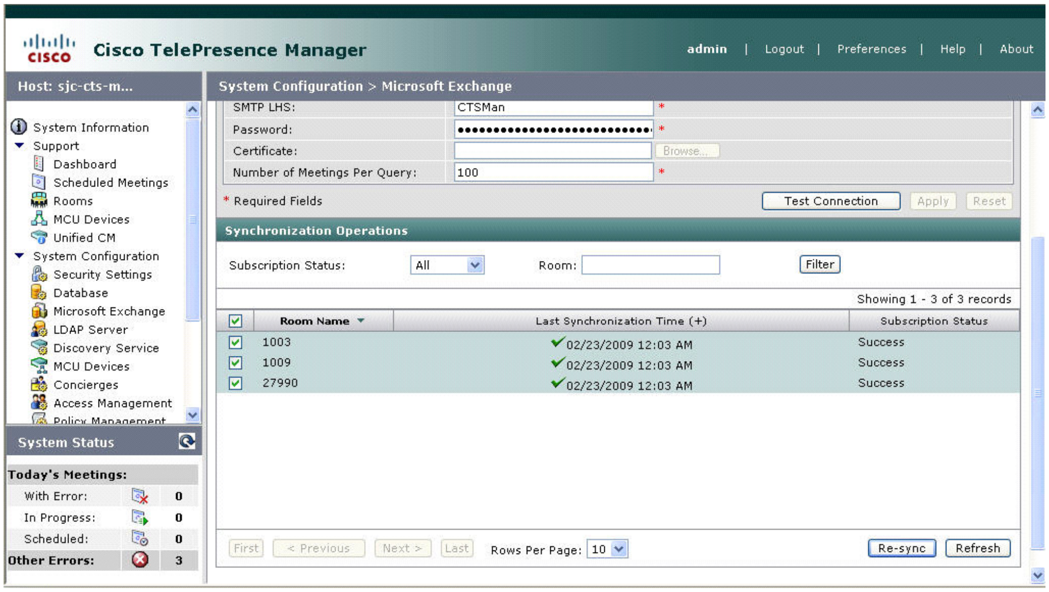
* Required Fields

Showing 0 - 0 of 0 records

Time stamp (+)	Status	Type	Hostname	Location

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

Figure 9-37 System Configuration - Microsoft Exchange Re-sync Window



SMTP LHS:	CTSMan *
Password:	•••••••••••••••••••••••••••• *
Certificate:	
Number of Meetings Per Query:	100 *

* Required Fields

Subscription Status: All   Room:

Showing 1 - 3 of 3 records

☑	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

Rows Per Page: 10

Today's Meetings:	
With Error:	0
In Progress:	0
Scheduled:	0
Other Errors:	3

- 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:

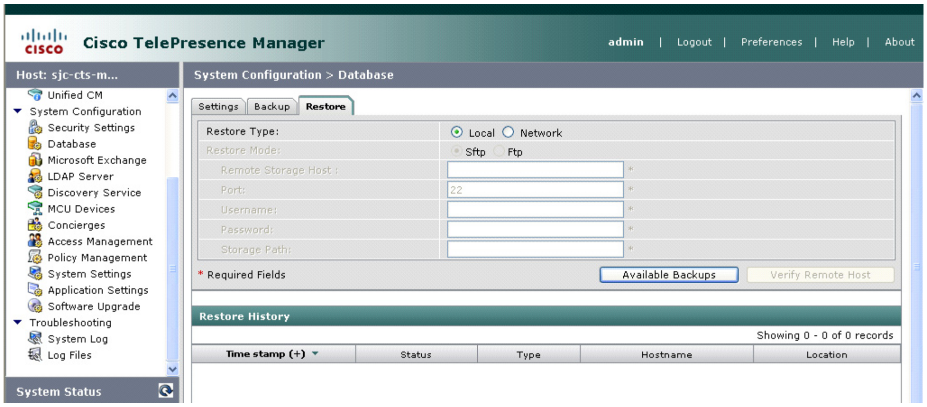
Step 1 To start the failover procedure process, power off the primary CTS-Man.

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 9-38 System Configuration Database Restore Backup Window



Restore Type: ● Local ○ Network
Restore Mode: ● Sftp ○ Ftp
Remote Storage Host : *
Port: 22 *
Username: *
Password: *
Storage Path: *
* Required Fields

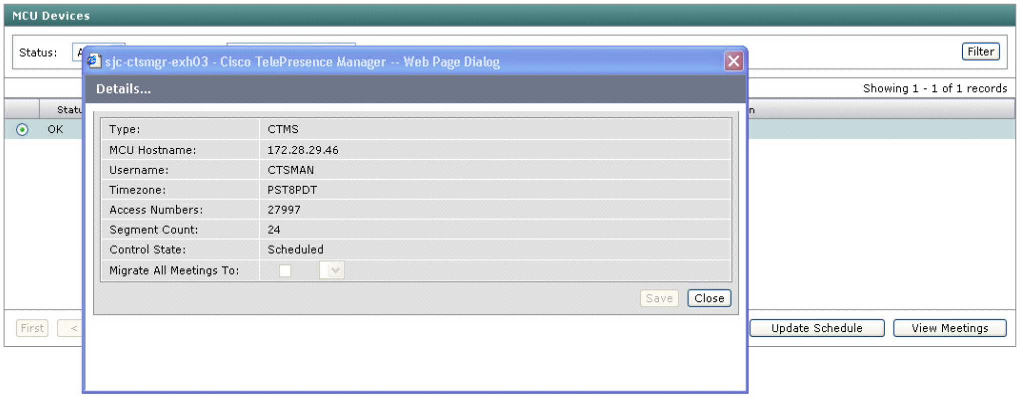
Showing 0 - 0 of 0 records

Time stamp (+)	Status	Type	Hostname	Location

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 9-39 System Configuration MCU Devices - Details Window

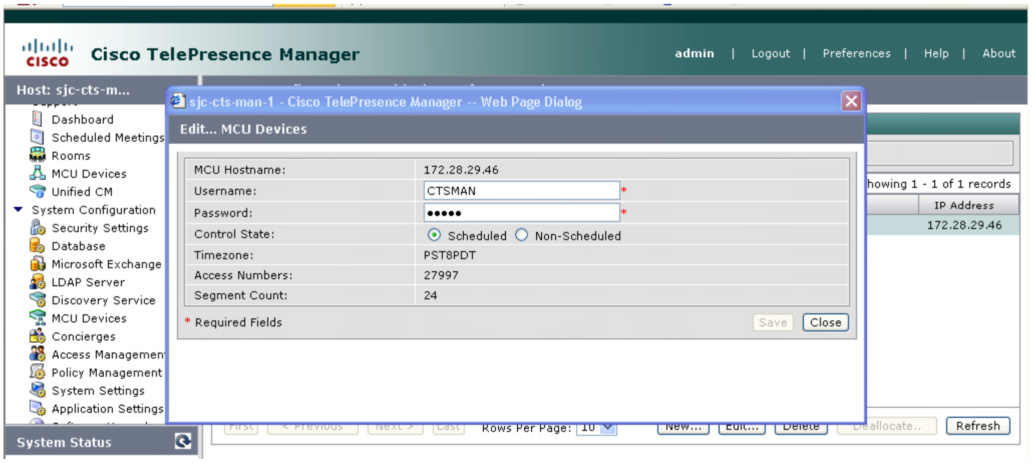

MCU Devices
Status:
Filter
Showing 1 - 1 of 1 records
Statu
OK
First
<
Update Schedule
View Meetings
sjc-ctsmgr-exh03 - Cisco TelePresence Manager -- Web Page Dialog
Details...
Save
Close

Type:	CTMS
MCU Hostname:	172.28.29.46
Username:	CTSMAN
Timezone:	PST8PDT
Access Numbers:	27997
Segment Count:	24
Control State:	Scheduled
Migrate All Meetings To:	□

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 9-40 System Configuration MCU Devices - Edit Window



MCU Hostname:	172.28.29.46
Username:	CTSMAN *
Password:	●●●●● *
Control State:	● Scheduled ○ Non-Scheduled
Timezone:	PST8PDT
Access Numbers:	27997
Segment Count:	24

* Required Fields

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.

Hardware Replacement

If it becomes necessary to replace CTS-Manager hardware, the administrator must run a fresh install of CTS-Manager on the new server hardware.

Alternatively, the administrator can restore a previous backup on the new server from a remote location.

For more information, contact Cisco Technical Assistance Center (TAC).