Cisco TelePresence Manager Release 1.6 Administration and Installation Guide

Release1.6.x
October 30, 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-13673-04

Cisco TelePresence Manager Release 1.6

CONTENTS

Preface

Revised: Nov 13, 2009, OL-13673-06

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Audience and Scope

The *Cisco TelePresence Manager Administration and Installation Guide* is directed to the administrator that configures, monitors, and maintains the Cisco TelePresence Manager application, and troubleshoots problems that may occur.

What's New in this Release

This section describes new and changed information in Cisco TelePresence Manager beginning with Release 1.6.

- Studio mode recording - allows an administrator to turn on global studio mode recording if all managed CTS endpoints are upgraded to the supported version. CTS is configured using the CTS UI, with a preferred recording server which would dial out to meetings, allowing the one button to push recording for the meeting
- Concierge changed to Live Desk

- Tentative Room Reservations - CTS-Manager now processes room reservations which are in tentative state. A tentative state implies meeting invite has been viewed by room/CTS-500 owner but not accepted yet. CTS-Manager would treat a tentative reservation as an accepted reservation
- Support for MS Exchange 2003/2007 deployments using Windows 2008 platform
- Enhancement Email Management - more support to email notifications on a global basis, admin can turn off or on email notifications
- Hardware MIB- new hardware MIBs are supported in 1.6 release
- Support for MS Exchange 2007 Web Services using FBA (Form Based Authentication)
- SD Interop supported with CIF; HD Interop with CUVC 7.0 supports 720p
- Support for multiple CUCM Clusters - supports One Button To Push in CUCM multi-cluster deployment. The ens user does not need to dial any special number to dial across the clusters in that CTS-Manager will formulate the numbers dialed by CTS end points to go across clusters based on CUCM configurations.
- Support for multiple LDAP Domains/Forests in MS Exchange Deployments - CTS-Manager supports interacting with a maximum of 5 LDAP servers per deployment
- Optional First Time Setup using the Pre-Qualifier tool.

End User License Agreement

Revised: February 25, 2009, OL-13673-04

Note It is important that you read and understand the conditions of the end user license agreement. Downloading, installing, and using Cisco and Cisco-supplied software constitute acceptance of the agreement.

You can display the end user license agreement from two places, the login window and the About window.

Figure 1 Cisco TelePresence Manager Login Screen

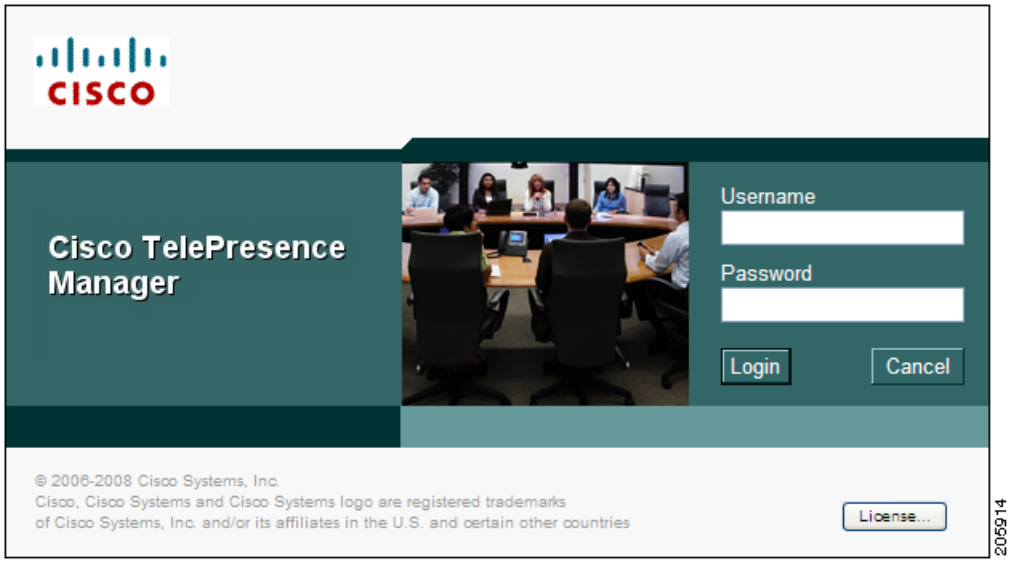


Figure 2 Cisco TelePresence Manager License Screen

CHAPTER 1

General Information about the Cisco TelePresence Manager

Revised: January 28, 2010, OL-13673-06

Contents

Overview of the CTS-Manager Administration Guide

Table 1-1 give a brief description of the contents of each chapter in the Administration Guide.

Table 1-1 Administration Guide Chapter Descriptions

Chapter Title	Description
Chapter 1 General Information About the Cisco TelePresence Manager	This chapter provides a general description of hardware and software components used within the Cisco TelePresence Manager system. It includes overviews of Point-to-Point calls, meeting scheduling, multipoint calls, Interoperability with legacy endpoints, and Intercompany Cisco TelePresence calls and administration roles.
Chapter 2 Pre-Install Set Up for CTS-Manager	This chapter describes the pre-setup and installation features for CTS-Manager.
Chapter 3 Configuring Microsoft Exchange	This chapter covers the steps needed to configure either Microsoft Exchange 2003 or 2007and Active Directory.
Chapter 4 Configuring IBM Domino and Domino Server	This document covers the steps needed to configure IBM Domino and Domino Directory Server for the CTS Manager system.
Chapter 5 Configuring CUCM for CTS Manager	This chapter describes adding parameters to Cisco Unified Communications Manager and gathering information from the current installation of Cisco Unified Communications Manager that will be used to configure the Cisco TelePresence Manager during installation.
Chapter 6 Installing and Configuring PreQualification Assistant Tool	This chapter explains how to install and run the Cisco TelePresence Manager PreQualification Assistant tool. It is important to install and run the pre-qualification assistant to ensure that the pre-installation set up is performed correctly.
Chapter 7 Installing or Upgrading CTS Manager	Describes how to install or upgrade CTS Manager.
Chapter 8 Initializing CTS Manager	The final process is initializing Cisco TelePresence Manager to enable access to information sources such as Microsoft Exchange Server for meeting requests from Microsoft Outlook, Active Directory for accessing user and conference room information, and Cisco Unified Communications Manager for conference room availability and telephone support.
Chapter 9 Installing Additional Configurations for CTS Manager	Describes the configuration features available when you log into CTS-Manager using an Administrator role.
Chapter 10 Monitoring CTS Manager	Describes the monitoring and support features available when you log into CTS-Manager using a Concierge role.

Table 1-1 Administration Guide Chapter Descriptions

Chapter Title	Description
Chapter 11 CTS-MAN Emails and End-User Web UI	Describes the different email notifications and meeting details window available to Meeting Organizers.
Chapter 12 Supported MIBs for CTS Manager	Provides the MIBs used by the CTS Manager.
Chapter 13 Troubleshooting	Provides troubleshooting information for CTS-Manager Administrators.
Appendix A - removed CTS-Manager Pre-Qualifying Tool	This section has been moved to Chapter 6.
CTS-Manager CLI Command Set (formerly Chapter 7) - removed	This chapter has been removed and is now a separate CLI book set.

Terminology

The following terms are used in this guide:

- **Audio call**: An audio call refers to a call placed to or from an audio-only telephone for the purpose of conferencing the audio call into a Cisco TelePresence meeting.

Note Audio calls are placed or answered with the CTS phone's handset on-hook.

- **Cisco TelePresence call**: A Cisco TelePresence call is placed between two or more CTS endpoints.
- **Cisco TelePresence meeting**: A Cisco TelePresence meeting refers to two or more endpoints connected by a Cisco TelePresence call.
- **Conference**: A conference refers to a Cisco TelePresence meeting that includes an audio call.
- **CUVC** - Cisco Unified Video Conferencing
- **Endpoint**: An endpoint, or 'CTS endpoint' refers to the combination of hardware and software that comprise a Cisco TelePresence System. Examples of a CTS endpoint are the CTS 3200 and the CTS 500. CTS endpoints are also referred to as Cisco TelePresence rooms, in the case of a CTS 3000 or CTS 3200 endpoint.
- **LDAP** - Lightweight Directory Access Protocol
- **MCU** - Multipoint Conference Unit

Introduction to the Cisco TelePresence System

The Cisco TelePresence System is composed of several hardware and software components. The Cisco TelePresence System also gets information and services with peripheral components such as Cisco Unified Communications Manager (Unified CM), and calendar services such as Microsoft Exchange or IBM Domino. Together all the peripheral and CTS components offer the features and services needed to schedule, place, and manage Cisco TelePresence calls and maintain all the Cisco TelePresence System components.

The following sections provide a general overview of the components that make up the Cisco TelePresence System.

Making Point-to-Point Cisco TelePresence calls

Placing a call between two CTS endpoints is similar to making a simple audio call. If you know the phone number of the endpoint you can dial it directly using the CTS IP phone.

CTS Endpoints

There are five CTS endpoint models supported by Cisco Unified CM.

- **CTS 500** - For data sheets and other product literature refer to the product page. For hardware installation information refer to the Cisco TelePresence System 500 Assembly, Use & Care, and Field-replaceable Unit Guide.
- **CTS 1100** - For data sheets and other product literature refer to the product page. For hardware installation information refer to the Cisco TelePresence System 1100 Assembly, Use & Care, and Field-replaceable Unit Guide.
- **CTS 1300** - For data sheets and other product literature refer to the product page. For hardware installation information refer to the Cisco TelePresence System 1300 Assembly, Use & Care, and Field-replaceable Unit Guide.
- **CTS 3000** - For data sheets and other product literature refer to the product page. For hardware installation information refer to the Cisco TelePresence System 3000 Assembly, Use & Care, and Field-replaceable Unit Guide.
- **CTS 3200** - For data sheets and other product literature refer to the product page. For hardware installation information refer to the Cisco TelePresence System 3200 Assembly, Use & Care, and Field-replaceable Unit Guide.

Each endpoint is configured and maintained through Unified CM and the CTS Administration software. The CTS Administration software is installed on each endpoint and is accessible by browser. All Cisco TelePresence Administration software supports Internet Explorer 6.0. For information about installing, configuring, and maintaining CTS endpoints refer to the CTS Administrator's Guide.

Components of the Cisco TelePresence System

In order to schedule meetings in advance you need to include CTS Manager in your Cisco TelePresence system. CTS Manager works with Microsoft Exchange or IBM Domino servers to schedule Cisco TelePresence meeting rooms and enable One -Button -To -Push meeting access.

CTS Manager communicates with the following components:

- **CTS endpoints** - CTS-Manager polls endpoints and reports errors to your CTS-Manager Administrator. CTS-Manager also pushes an endpoint's meeting schedule to the endpoint, then pushes to the IP phone.
- **Cisco Unified CM** - CTS-Manager works with Cisco Unified CM to maintain current configurations for each endpoint, and to discover new endpoints as they are added to your Cisco TelePresence system.

- **Calendar server (Exchange or Domino)** - Each CTS endpoint has a corresponding mailbox on a calendar server to support scheduling through Outlook or Lotus Notes. CTS-Manager monitors endpoint calendars and reports errors. CTS-Manager also uses the scheduling information to push meeting schedules to each CTS endpoint and then pushes to the IP phone.
- **Active Directory** - Each CTS endpoint's room ID is stored in Active Directory. CTS-Manager is the conduit between Active Directory and an endpoint.
- **Cisco TelePresence Multipoint Switch (CTMS)** - A CTMS provides the resources for multipoint (three or more endpoints) calls. CTS-Manager reports errors with a CTMS and specifies which CTMS is used for each Cisco TelePresence meeting. Cisco TelePresence supports the ability to conference existing standards-based video conference sessions into a Cisco TelePresence meeting by integrating the Cisco TelePresence Multipoint Switch (CTMS) with Cisco Unified Video conferencing Systems (CUVC). This provides interoperability with virtually all standards-based video conferencing systems installed today.
- For data sheets and other product literature refer to the product page. For hardware installation and CTMS maintenance refer to the Cisco TelePresence Multipoint Switch administration guide.

Cisco TelePresence Manager Product Specifications

Table 1-2 gives product specifications and Table 1-3 provides system requirements of the Cisco TelePresence Manager. Table 1-4 provides the flow of tasks you need follow to install the CTS_MAN system.

Table 1-2 Product Specifications

Specifications	Description
Product compatibility	Cisco MCS 7845-H2 and MCS 7845-I2 Media Convergence Servers
Software compatibility	Microsoft Internet Explorer 6.0 **Note** CTS Manager Release 1.5 does not support Microsoft Internet Explorer 7.x.
Protocols	HTTP, HTTPS, Administrative XML (AXL)/SOAP, Simple Network Management Protocol (SNMP), and CTI
Connectivity	IP
Reliability and availability	High availability through Cisco 7845 Media Convergence Server platform

Table 1-3 System Requirements

Specifications	Description
Groupware connectivity	• Microsoft Exchange Server: – 2003 SP2 (Windows Server 2003 Enterprise Edition SP2) – 2007 SP1 and 2007 SP2 (on Windows 2003 Enterprise Edition SP2 [64 bit] – 2007 SP1 and 2007 SP2 (on Windows 2008 Enterprise Edition [64 bit] – supported versions: [8.0.685.25, 08.00.0685.018, 08.00.10685, 08.01.0, 08.1.240.5, 08.1.240.6, 08.01.10240, 08.02.0176.002, 6.5.6944, 6.5.7226, 6.5.7638] • Microsoft Outlook Client: 2003 and 2007 • IBM Domino Server: 8.0.x and 7.0.x (Operating System: Windows Server 2003 Enterprise Edition SP2) • IBM Notes Client: 8.0.x, 7.0.x, and 6.5.x
Cisco Unified Communications Manager version	Cisco Unified CM 6.1.3 or later
Lightweight Directory Access Protocol (LDAP) connectivity	Active Directory 2003 SP2, 2008 Domino Directory, versions: 7.0.x, 8.0.x
Ethernet Cable	Connect to NIC Port 1
Web browser supported	Microsoft Internet Explorer 6.0

Installation Procedures Guideline

The flow of tasks you need to perform in order to configure the Cisco TelePresence network and install and configure the CTS-MAN are provided in the following table:

Table 1-4 Install and Configuration Procedures Guidelines for setting up CTS-MAN System

Set-Up and Installation Procedures Guidelines	Description	Location
Pre-Install Procedures	Provides Cisco TelePresence Manager with the contact and access information it requires to connect to and talk with your network.	Chapter 2, "Pre-Install System Set Up for Cisco TelePresence Manager"
Configure Microsoft Exchange for CTS-MAN	This chapter covers the steps needed to configure Microsoft Exchange and Active Directory for the CTS-MAN system.	Chapter 3, "Configuring Microsoft Exchange for Cisco TelePresence Manager"
Configure IBM Domino for CTS-MAN	This chapter covers the steps needed to configure IBM Domino and Domino server for the CTS-MAN system.	Chapter 4, "Configuring IBM Domino Server for Cisco TelePresence Manager"
Configuring Cisco Unified CM for CTS-MAN	Before installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-MAN system.	Chapter 5, "Configuring Cisco Unified CM for Cisco TelePresence Manager"
Install and Configure PreQualification Assistant	Install and configure the PreQualification Assistant to ensure that your pre-installation set up is performed correctly. The data you enter into the Tool Test Configuration forms are used to verify connections to the servers and retrieve data from them to be used to configure CTS manager	Chapter 6, "Installing and Configuring Cisco PreQualification Assistant"
Installing or Upgrading CTS-MAN software	Installing the CTS Manager software. In addition, the installation requires information about your network and the rules for finding and exchanging information.	Chapter 7, "Installing or Upgrading Cisco TelePresence Manager"

Set-Up and Installation Procedures Guidelines	Description	Location
Initializing CTS-MAN	After installing the CTS-MAN software, the next process is initializing Cisco TelePresence Manager to enable access to information sources such as Microsoft Exchange Server for meeting requests from Microsoft Outlook, Active Directory for accessing user and conference room information, and Cisco Unified Communications Manager for conference room availability and telephone support	Chapter 8, "Initializing Cisco TelePresence Manager"
Additional Installation Procedures for CTS-MAN	The administrator makes use of the configuration windows to perform system configuration tasks such as as synchronizing system databases, managing security, and reconfigure system settings	Chapter 9, "Additional Installation Configurations for Cisco TelePresence Manager"
Monitoring CTS-MAN	Monitoring and updating meeting schedules and monitoring the status of rooms and system services	Chapter 10, "Monitoring Cisco TelePresence Manager"
Email notifications and End User Web UI	The Calendar service (either Microsoft Exchange or IBM Domino) sends an acceptance email to the meeting organizer, with the notice that the rooms have been reserved and placed on the calendar. CTS-Manager also sends either a Confirmation email or an Action Required email to the meeting organizer when a meeting is scheduled	Chapter 11, "CTS-Manager Emails and End-User Web UI"

CHAPTER 2

Pre-Install System Set Up for Cisco TelePresence Manager

Revised: January 28, 2010, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

The Cisco TelePresence meeting solution combines audio, video, and interactive elements to create the feeling of being “in person” with participants in remote locations.

To enable these features, you must ensure the system components are meeting the system version requirements. These are covered in the next section.

System Components and Versions

Before you proceed with CTS Manager installation, the servers and applications within your telecommunications network must be configured so that Cisco TelePresence Manager can find the resources and information needed to initialize the installation. These servers and applications may include one or more of the following:

- Your Cisco TelePresence System endpoints should be fully installed and configured before installing Cisco TelePresence Manager.
- Cisco Unified Communications Manager (Version 5.1 or 6.1.3) should already be installed and configured.

The following versions are supported by Cisco TelePresence Manager 1.6

LDAP:

- Active Directory 2003 SP2, 2008 (32 bit and 64 bit versions). Only supported for Exchange calendar server and no calendar mode deployments.
- Domino Directory 7.0.x, 8.0.x. Only supported for Domino Calendar server deployments.

Note Active Directory is NOT supported for Domino Calendar server deployment with CTS-Manager

Microsoft Exchange:

- Microsoft Exchange versions 2003 SP2, Exchange 2007 SP1, Exchange 2007 SP2—
  - Versions:8.0.685.25, 08.00.0685.018, 08.00.10685, 08.01.0, 08.1.240.5, 08.1.240.6, 08.01.10240, 08.02.0176.002, 6.5.6944, 6.5.7226, 6.5.7638

Note NOTE: 2007 is supported with WebDAV and EWS.

Note Microsoft Exchange with Entourage client is not supported.

- Scheduling Clients supported
  - Outlook Versions 2003 SP2, 2007 SP2
- This release of Cisco TelePresence Manager is designed to work with Microsoft Internet Explorer version 6.1.3 or later. Cisco cannot guarantee correct system behavior using unsupported browsers
- IBM Domino (Version 7.0.x, 8.0.x) (Operating System: Windows Server 2003 Enterprise Edition SP2)
- Scheduling Clients supported
  - Outlook Version 2003 SP2, Outlook Version 2007 SP2
  - Lotus Notes versions: 6.5.x, 7.0.x, and 8.0.x
- MCS-7845-H2-CTS1 or MCS-7845-I2-CTS1 can be used as your Cisco Media Convergence Server.
- When you install Cisco TelePresence Manager, the Cisco Media Convergence Server hard drive is formatted, and any existing data on the drive is overwritten.
- Cisco recommends you configure the system using static IP addressing so it will be easy to manage.

Pre-Installation Procedure Guidelines for Initial Network Set-up

This table provides a guideline for the procedures you will need to reference in order to pre-configure the network **before** installing the Cisco TelePresence Manager.

Note The system will use either Microsoft or IBM not both. So only Chapter 3 or Chapter 4 needs to be referenced when doing the pre-configuration set-up.

Table 2-1 Pre-Configuration Guidelines for Setting Up Initial System Network for CTS-MAN

Set-Up Procedure Guidelines before Installing CTS-MAN	Description	Location
Configure Microsoft Exchange	This chapter covers the steps needed to configure Microsoft Exchange and Active Directory for the CTS-MAN system.	Chapter 3, "Configuring Microsoft Exchange for Cisco TelePresence Manager"
Configure IBM Domino	This chapter covers the steps needed to configure IBM Domino and Domino server for the CTS-MAN system.	Chapter 4, "Configuring IBM Domino Server for Cisco TelePresence Manager"
Configuring Cisco Unified CM	Before installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-MAN system.	Chapter 5, "Configuring Cisco Unified CM for Cisco TelePresence Manager"
Install and run PreQualification Assistant	Install and run the PreQualification Assistant to ensure that your pre-installation set-up is configured correctly. The data you enter into the Tool Test Configuration forms are used to verify connections to the servers and get data from them to be used to configure CTS-MAN.	Chapter 6, "Installing and Configuring Cisco PreQualification Assistant"

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

CHAPTER 3

Configuring Microsoft Exchange for Cisco TelePresence Manager

Revised: January 28, 2010, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

This document explains how to set up the Microsoft Outlook messaging software to be able to receive reminders and allow users to connect to a remote meeting site with the touch of a button.

To enable these features, you must provide CTS-Manager with the contact and access information it requires to connect to and talk with your network.

This chapter covers the steps needed to configure either Microsoft Exchange 2003, 2007, or EWS and Active Directory.

- Microsoft Exchange versions—The following versions are supported by Cisco TelePresence Manager 1.6
  - 2003 SP2, Exchange 2007 SP1, Exchange 2007 SP2
  - Active Directory 2003 SP2, 2008 (32 bit and 64 bit versions)
  - Versions:8.0.685.25, 08.00.0685.018, 08.00.10685, 08.01.0, 08.1.240.5, 08.1.240.6, 08.01.10240, 08.02.0176.002, 6.5.6944, 6.5.7226, 6.5.7638 with SP2

Note NOTE: 2007 is supported with WebDAV and EWS.

Note Microsoft Exchange with Entourage client is not supported.

- Scheduling Clients supported
  - Outlook Versions 2003 SP2, 2007 SP2
- This release of Cisco TelePresence Manager is designed to work with Microsoft Internet Explorer version 6.1.3 or later. Cisco cannot guarantee correct system behavior using unsupported browsers.
- Cisco recommends you configure the system using static IP addressing so it will be easy to manage.

It is recommended that Chapter 8, "Initializing Cisco TelePresence Manager" Manager, LDAP sections be reviewed to ensure that user set up is performed correctly.

Pre-Configuration Set-Up Guidelines

The purpose of this section is to reference the chapters you will next need in order to pre-configure supporting software before installing the Cisco TelePresence Manager.

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

Table 3-1 Pre-Configure Guidelines Before Installing CTS-Manager

Set-Up Procedures before Installing CTS-Manager	Description	Location
Configure Microsoft Exchange	This chapter covers the steps needed to configure Microsoft Exchange and Active Directory for the CTS-Manager system.	Current Chapter.
Next Steps After Microsoft Exchange Set-up		
Configuring Cisco Unified CM.	Before installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-Manager system.	Chapter 5, "Configuring Cisco Unified CM for Cisco TelePresence Manager"
Install and Configure PreQualification Assistant	Install and run the Pre-qualification Assistant to ensure that your pre-installation set up is performed correctly. The data you enter into the Tool Test Configuration forms are used to verify connections to the servers and get data from them in order to configure CTS Manager	Chapter 6, "Installing and Configuring Cisco PreQualification Assistant"

Configuring Microsoft Exchange for CTS-Manager

- If you are using secure mode, a certificate request must exist. If a certificate was not requested when Microsoft Exchange was installed, you can follow the procedure described in the tutorial found at the following Microsoft Exchange URL:
  http://www.msexchange.org/tutorials/Securing-Exchange-Server-2003-Outlook-Web-Access-Chapter5.html
  - See the sections "Installing the Microsoft Certificate Service" and "Creating the Certificate Request."
- Make a copy of the certificate and place it in a folder accessible to the computer with browser access to the Cisco TelePresence Manager server.

Note Only one certificate can be used. Do not reuse it or give it a new name and then try to upload it to CTS-Manager. Also, if a certificate is expired, it cannot be uploaded.

- A copy of the certificate for Active Directory exists. To request a certificate for Active Directory, follow the below steps:
  1. By default, the certificate file is named _.crt. An enterprise certificate authority (CA) automatically publishes the root certificates, and enterprise domain controllers automatically enroll for all domain controller certificates.
  2. Make sure the certificate, the CA, and the CA web interface are all installed on the same server. Using Internet Explorer, connect to *https://<CA server>/certsrv*.
  3. Authenticate as the administrator, making sure you specify the proper domain, for example, demotest\administrator. The Active Directory domain needs to be set to at least level 2.
  4. Choose **Download CA Certificate**, using Distinguished Encoding Rules as the encoding method.

Deploying with Microsoft Exchange 2003

Step 1 Create an account in Microsoft Exchange 2003 for CTS-Manager, e.g. **`ctsmanaccount`**.

Step 2 Provide an adequate mailbox quota for the ctmmanaccount. Cisco recommends providing at least 1 GB of mailbox quota for a deployment of up to 125 Cisco TelePresence System endpoints. Additional mailbox quota is recommended if feasible.

Step 3 Login to the ctsmanaccount once to verify it is set up correctly.

Step 4 Create an account in Microsoft Exchange for each Cisco TelePresence System endpoint. You can use 'Active Directory Users and Computers' to create the room accounts, or use any custom script to create the room account. If the room is already created, use the information from the Cisco Unified CM and skip this step.

Caution In Microsoft Exchange software, some special characters are not supported in Recipient Policy Exchange server name, mailbox name, etc. These special characters will also not be supported by CTS-Manager.
Refer to the Microsoft KB for specific information on characters:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;841091
Exchange 2007 Information
http://technet.microsoft.com/en-us/library/dd285491.aspx

Step 5 Log into the room account once using Outlook Web Access (OWA), or Outlook. This must be done or the room mailbox may not be set up properly in Exchange.

Step 6 The CTS-Manager account (e.g. ctsmanaccount) must have read permission on the Calendar folder for each room's mailbox. You can use Outlook to set Calendar Properties (the Permissions tab), or use Active Directory ("Full mailbox access" permissions).

Step 7 Verify the CTS-Manager account has permissions for all room accounts.

a. Use a supported browser and log onto the room account with OWA (http://<exchange ip address>/exchange/<roomaccountname>)

b. Log in using the CTA-Manager account (e.g. ctmmanaccount)

c. Validate the setup by sending a test email to any user in the same domain. Validate the user receives the email.

Step 8 Synchronize the system clock in the CTS Manager server to the same NTP server used by Exchange. Enter the hostname or IP address of one or more NTP servers. NTP Server 1 value is mandatory; NTP Servers 2-5 are optional. Thus, CTS-Manager and Exchange need to point to the same NTP and synch with the NTP to avoid having the room calendar not updating correctly.

Note Cisco strongly recommends that you enter the NTP server by which Cisco Unified CM synchronizes its clock as the primary NTP server. If these servers are out of synchronization, CTS-Manager may not update and delete unwanted meetings.

Deploying with Microsoft Exchange 2007 - WebDAV

Microsoft Exchange management tools can be found in the start menu in the Exchange server - "Start > All Programs > Microsoft Exchange Server 2007". There are 2 tools available as options:

- Exchange Management Console – GUI version which has online help.
- Exchange Management Shell – shell version that can be useful for scripting.

Caution In Microsoft Exchange software, some special characters are not supported in Recipient Policy Exchange server name, mailbox name, etc. These special characters will also not be supported by CTS-Manager.
Exchange 2007 Information:
http://technet.microsoft.com/en-us/library/dd285491.aspxhttp://technet.microsoft.com/en-us/library/dd285491.aspx

Step 1 Create a user account in Exchange for CTS-Manager (e.g. `ctsmanaccount`).

.The user account is created from "Exchange Management Console" using the User Mailbox by doing the following:

a. Select Recipient Configuration > Mailbox, right-click and select "New Mailbox"

b. Select "User Mailbox" type and follow the dialog to create the mailbox.

Step 2 Provide an adequate mailbox quota for the ctmmanaccount. Cisco recommends providing at least 1 GB of mailbox quota for a deployment of up to 125 Cisco TelePresence System endpoints. Additional mailbox quota is recommended if feasible.

Step 3 Log into the CTS-Manager mailbox once to verify the user mailbox is set up correctly.

Step 4 IF a new room needs to be added, Admin needs to create the room in Calendaring server first with appropriate permissions for CTS-Manager application account and then create associated device(s) in CUCM. If admin ends up creating room in CUCM beforehand, then the room would appear in error in CTS Manager. Once room is configured in Calendaring server, admin can resync the room in CTS Manager and at that point error goes away.

Step 5 Create an account in Exchange for each Cisco TelePresence System endpoint. Use one of the following methods:

a. In "Exchange Management Console" (EMC), select "Recipient Configuration > Mailbox", right-click and select "New Mailbox." Select "Room Mailbox" type and follow the dialogs to create the mailbox.

b. Run "Exchange Management Shell" (EMS) cmdlet to create a Room mailbox / account.

Step 6 The CTS-Manager account needs to have full access on the Calendar folder of each room mailbox, or at minimum it needs to have read permission. Using EMS, run one of the 2 cmdlets in the following based on your preference:

a. Add-mailboxpermission -identity "TelepresenceRoom9" -accessRights FullAccess -user ctmperf\ctsmanaccount

b. Add-mailboxpermission -identity "TelepresenceRoom9" -accessRights ReadPermission -user ctmperf\ctsmanaccount

You can check the current permission setting of a Room by running one of the following cmdlets:

- Get-mailbox -server tsbu-ctmpc19 | get-mailboxpermission
- Get-mailboxpermission –identity TelepresenceRoom9

Step 7 Set the "DeleteSubject" and "AddOrganizerToSubject" properties in room mailbox calendar to **False**. This sets the parameters for the meeting to be displayed on the IP Phone.

a. Set-MailboxCalendarSettings -Identity TelepresenceRoom9 -DeleteSubject $false

b. Set-MailboxCalendarSettings -Identity TelepresenceRoom9 -AddOrganizerToSubject $false

Step 8 It is recommended to set Auto-accept to ON using EMS.

Note This works only with room mailbox, not with user mailbox. Also CTS-Manager will not process meetings that are tentative. Meetings that are accepted if Microsoft AAA Agent is off will only access proxy if accepted.

Set-MailboxCalendarSettings -Identity TelepresenceRoom9 -AutomateProcessing AutoAccept

c. Check if Auto-accept has been configured for the room.

Get-MailboxCalendarSettings -Identity TelepresenceRoom9 | fl

Note It is recommended not to switch room mailbox acceptance mode once set. If it is configured auto-accept then switched to manual proxy mode the meeting does not show up in CTS-Manager Web UI nor is it pushed to the phone UI. The user will have to manually re-accept the meeting again.

Step 9 Log into room mailbox once using Outlook Web Access (OWA) or Outlook 2007. This is an important step, as room mailbox will not be setup appropriately in MS Exchange. In Exchange 2007, you won't be able to directly log on to the room* mailbox using the room username, because the user account of the room mailbox is disabled by default. There are 2 possible scenarios (based on the decision made in step 5):

Note *Only when mailbox is created as "Room Mailbox" type. If mailbox is created as "User Mailbox" type, then it would be the same step as it is with Exchange 2003 to log on to the mailbox.

a. The CTS-Manager user (e.g. ctsmanaccount) has been given full access to the room mailboxes. In this case, use ctsmanaccount credential to log on to each room mailbox.

- First log into ctsmanaccount mailbox using OWA, using a supported web browser (IE 6.x) and typing: http://<exchange ip address>/owa/. Once logged on as ctsmanaccount user, click on the "ctsmanaccount" tab on the top, enter the room account name, and click "Open". It would open the room mailbox in another window.
- Alternatively, you can log on to room account using either Outlook 2007 or Outlook Web Access:
  http://<exchange ip address>/owa/<room_name@domain_name>. Again, here you will need to log on using ctsmanaccount credential.

b. The second scenario is where the ctsmanaccount was only given read permission to the room mailboxes. In such case, you need to have a third user account which has "full access" to the room mailboxes, let's say this user is "Joe Smith." Use Joe Smith credential to log on to his mailbox using Outlook 2007, then follow the below steps:

- i. Once logged on, click on the **Calendar** on the left pane.
- ii Click **Open a Shared Calendar …** and enter the room name.
- iii The room calendar would show up under **People's Calendar** on the left pane. In the screen-shot, the room is TelepresenceRoom10. Right-click on the room name, and select **Properties**.
- iv. Click **Permissions** tab
- v. Click on **Add** and select ***ctsmanaccount*** account name.
- vi. In "Permissions" > "Permission Level" drop-down field, select **Reviewer**.
- vii.In "Permissions" > "Read" section, check **Full Details**.
- viii. Click **OK**.
- ix. Repeat step ii to viii for each Room that will be managed by CTS-Manager.

Step 10 Form-based authentication (FBA) is enabled by default in Exchange 2007. In order for Cisco TelePresence Manager to work, disable FBA.

a. Go to EMC > Server Configuration > Client Access > Outlook Web Access > Exchange (Default Web Site) > Properties > Authentication tab

b. Select "Use one or more standard authentication method."

c. Check “Integrated Windows Authentication” and/or “Basic Authentication (password is sent in clear text)” boxes.

d. Click **OK** on the warning dialog box that says IIS restart is required.

e. Run “iisreset /noforce” from a command prompt, or go to “Services Manager” and restart “IIS Admin service.”

Step 11 Open IIS Manager and enable WebDAV.

a. Go to “Internet Information Services” > [server_name] > “Web Service Extension”

b. Select “WebDAV” and click the “Allow” button, if it is showing “Prohibited” in Status.

a. Click the “Allow” button, if it is showing “Prohibited” in Status.

Step 12 Verify that the Web Sites Authentication Method is configured correctly for “Exchange” web site.

Note If using EWS Authentication - CTS Manager only supports Integrated Windows Authentication (NTLM) v1 authentication only. Please ensure that NTLM v1 authentication scheme are enabled for EWS site. The Axis2 Library does not support NTLM v2 at this time The Axis2 Library does not support NTLM v2 at this time.

Step 13 Repeat these steps for the “Default Web Site” setting:

a. In “IIS Manager,” go to “Internet Information Services” > [*server_name*] > “Web Sites” > “*Exchange*”

b. Right-click on the ***Exchange*** and select **Properties**.

c. Go to “Directory Security” tab

d. In “Authentication and access control” section:

- Click the **Edit** button
- Check the desired authentication access method - “Integrated Windows Authentication” and/or “Basic Authentication (password is sent in clear text)” boxes.
- Click **OK**

e. This step is required **only if** you need to configure CTS- Manager with the non-secure binding to the Exchange server. In “Secure communications” section:

- Click the **Edit** button
- Uncheck the “Require secure channel (SSL)” box, and click **OK**.

f. Click **OK** on all the dialog boxes that follow.

Step 14 Synchronize the system clock in the CTS Manager server to the same NTP server used by Exchange. Enter the hostname or IP address of one or more NTP servers. NTP Server 1 value is mandatory; NTP Servers 2-5 are optional. Thus, CTS-Manager and Exchange need to point to the same NTP and synch with the NTP to avoid having the room calendar not updating correctly.

Note Cisco strongly recommends that you enter the NTP server by which Cisco Unified CM synchronizes its clock as the primary NTP server. If these servers are out of synchronization, CTS-Manager may not update and delete unwanted meetings.

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 forced to sync with the Exchange server by either doing a reboot or a restart.

Deploying with Microsoft Exchange 2007 EWS

Microsoft Exchange management tools can be found in the start menu in the Exchange server - "Start > All Programs > Microsoft Exchange Server 2007". There are 2 tools available as options:

- Exchange Management Console – GUI version which has online help.
- Exchange Management Shell – shell version that can be useful for scripting.

Caution In Microsoft Exchange software, some special characters are not supported in Recipient Policy Exchange server name, mailbox name, etc. These special characters will also not be supported by CTS-Manager.
Exchange 2007 Information:
http://technet.microsoft.com/en-us/library/dd285491.aspxhttp://technet.microsoft.com/en-us/library/dd285491.aspx

Step 1 Create a user account in Exchange for CTS-Manager (e.g. `ctsmanaccount`).

.The user account is created from "Exchange Management Console" using the User Mailbox by doing the following:

a. Select Recipient Configuration > Mailbox, right-click and select "New Mailbox"

b. Select "User Mailbox" type and follow the dialog to create the mailbox.

Step 2 Provide an adequate mailbox quota for the ctmmanaccount. Cisco recommends providing at least 1 GB of mailbox quota for a deployment of up to 125 Cisco TelePresence System endpoints. Additional mailbox quota is recommended if feasible.

Step 3 Log into the CTS-Manager mailbox once to verify the user mailbox is set up correctly.

Step 4 IF a new room needs to be added, Admin needs to create the room in Calendaring server first with appropriate permissions for CTS-Manager application account and then create associated device(s) in CUCM. If admin ends up creating room in CUCM beforehand, then the room would appear in error in CTS Manager. Once room is configured in Calendaring server, admin can resync the room in CTS Manager and at that point error goes away.

Step 5 Create an account in Exchange for each Cisco TelePresence System endpoint. Use one of the following methods:

a. In "Exchange Management Console" (EMC), select "Recipient Configuration > Mailbox", right-click and select "New Mailbox." Select "Room Mailbox" type and follow the dialogs to create the mailbox.

b. Run "Exchange Management Shell" (EMS) cmdlet to create a Room mailbox / account.

Step 6 The CTS-Manager account needs to have full access on the Calendar folder of each room mailbox, or at minimum it needs to have read permission. Using EMS, run one of the 2 cmdlets in the following based on your preference:

a. Add-mailboxpermission -identity “TelepresenceRoom9” -accessRights FullAccess -user ctmperf\ctsmanaccount

b. Add-mailboxpermission -identity “TelepresenceRoom9” -accessRights ReadPermission -user ctmperf\ctsmanaccount

You can check the current permission setting of a Room by running one of the following cmdlets:

- Get-mailbox -server tsbu-ctmpc19 | get-mailboxpermission
- Get-mailboxpermission –identity TelepresenceRoom9

Step 7 Set the “DeleteSubject” and “AddOrganizerToSubject” properties in room mailbox calendar to **False**. This sets the parameters for the meeting to be displayed on the IP Phone.

a. Set-MailboxCalendarSettings -Identity TelepresenceRoom9 -DeleteSubject $false

b. Set-MailboxCalendarSettings -Identity TelepresenceRoom9 -AddOrganizerToSubject $false

Step 8 It is recommended to set Auto-accept to ON using EMS.

Note This works only with room mailbox, not with user mailbox. Also CTS-Manager will not process meetings that are tentative. Meetings that are accepted if Microsoft AAA Agent is off will only access proxy if accepted.

Set-MailboxCalendarSettings -Identity TelepresenceRoom9 -AutomateProcessing AutoAccept

c. Check if Auto-accept has been configured for the room.

Get-MailboxCalendarSettings -Identity TelepresenceRoom9 | fl

Note It is recommended not to switch room mailbox acceptance mode once set. If it is configured auto-accept then switched to manual proxy mode the meeting does not show up in CTS-Manager Web UI nor is it pushed to the phone UI. The user will have to manually re-accept the meeting again.

Step 9 Log into room mailbox once using Outlook Web Access (OWA) or Outlook 2007. This is an important step, as room mailbox will not be setup appropriately in MS Exchange. In Exchange 2007, you won’t be able to directly log on to the room* mailbox using the room username, because the user account of the room mailbox is disabled by default. There are 2 possible scenarios (based on the decision made in step 5):

Note *Only when mailbox is created as “Room Mailbox” type. If mailbox is created as “User Mailbox” type, then it would be the same step as it is with Exchange 2003 to log on to the mailbox.

a. The CTS-Manager user (e.g. ctsmanaccount) has been given full access to the room mailboxes. In this case, use ctsmanaccount credential to log on to each room mailbox.

- First log into ctsmanaccount mailbox using OWA, using a supported web browser (IE 6.x) and typing: http://<exchange ip address>/owa/. Once logged on as ctsmanaccount user, click on the “ctsmanaccount” tab on the top, enter the room account name, and click “Open”. It would open the room mailbox in another window.
- Alternatively, you can log on to room account using either Outlook 2007 or Outlook Web Access:
  http://<exchange ip address>/owa/<room_name@domain_name>. Again, here you will need to log on using ctsmanaccount credential.

b. The second scenario is where the ctsmanaccount was only given read permission to the room mailboxes. In such case, you need to have a third user account which has "full access" to the room mailboxes, let's say this user is "Joe Smith." Use Joe Smith credential to log on to his mailbox using Outlook 2007, then follow the below steps:

- i. Once logged on, click on the **Calendar** on the left pane.
- ii Click **Open a Shared Calendar …** and enter the room name.
- iii The room calendar would show up under **People's Calendar** on the left pane. In the screen-shot, the room is TelepresenceRoom10. Right-click on the room name, and select **Properties**.
- iv. Click **Permissions** tab
- v. Click on **Add** and select ***ctsmanaccount*** account name.
- vi. In "Permissions" > "Permission Level" drop-down field, select **Reviewer**.
- vii.In "Permissions" > "Read" section, check **Full Details**.
- viii. Click **OK**.
- ix. Repeat step ii to viii for each Room that will be managed by CTS-Manager.

Step 10 Verify that the Web Sites Authentication Method is configured correctly for "EWS" web site.

Step 11 Repeat these steps for the "Default Web Site" setting:

a. In "IIS Manager," go to "Internet Information Services" > [*server_name*] > "Web Sites" > "*EWS*"

b. Right-click on the ***EWS*** and select **Properties**.

c. Go to "Directory Security" tab

d. In "Authentication and access control" section:

- Click the **Edit** button
- Check the desired authentication access method - "Integrated Windows Authentication" and/or "Basic Authentication (password is sent in clear text)" boxes.
- Click **OK**

Note EWS Authentication - CTS Manager only supports Integrated Windows Authentication (NTLM) v1 authentication only. Please ensure that NTLM v1 authentication scheme are enabled for EWS site. The Axis2 Library does not support NTLM v2 at this time.

e. This step is required **only if** you need to configure CTS- Manager with the non-secure binding to the Exchange server. In "Secure communications" section:

- Click the **Edit** button
- Uncheck the "Require secure channel (SSL)" box, and click **OK**.

f. Click **OK** on all the dialog boxes that follow.

Step 12 Synchronize the system clock in the CTS Manager server to the same NTP server used by Exchange. Enter the hostname or IP address of one or more NTP servers. NTP Server 1 value is mandatory; NTP Servers 2-5 are optional. Thus, CTS-Manager and Exchange need to point to the same NTP and synch with the NTP to avoid having the room calendar not updating correctly.

Note Cisco strongly recommends that you enter the NTP server by which Cisco Unified CM synchronizes its clock as the primary NTP server. If these servers are out of synchronization, CTS-Manager may not update and delete unwanted meetings.

CTS-Manager and Microsoft EWS server automatically renews subscriptions every 20 minutes. If there are any changes for room status in EWS, the CTS-Manager will not be notified of the change until that 20 minute update time. The exception is if CTS-Manager is forces to sync with the EWS server by either doing a reboot or a restart

Migrating from Exchange 2003 to Exchange 2007

In Exchange 2003, there is no distinction between "User Mailbox" and "Room Mailbox" types. All mailboxes are created as "User Mailbox" in Exchange 2003. When you migrate the TelePresence room mailbox accounts from Exchange 2003 to Exchange 2007, you need to convert them into "Room Mailbox" type, especially if they are to be configured with Auto-Accept enabled.

Use the following procedure to migrate from Exchange 2003 to Exchange 2007:

Step 1 Install and configure the Exchange 2007 server.

Step 2 Migrate the CTS-Manager User mailbox to the Exchange 2007 server.

Step 3 Point CTS-Manager to the Exchange 2007 server.

Once step 1-3 are complete, the system will reboot.

Step 4 After the system has completed rebooting, shut down the CTS-Manager server.

This is important so that users may not use the system during migration.

Step 5 Migrate all Cisco TelePresence endpoints to the Exchange 2007 server.

Verify that all Cisco TelePresence endpoints are of type RoomMailbox, otherwise AutoAccept cannot be enabled.

After the migration is completed, add full access permission for the delegates to any proxy.

CHAPTER 4

Configuring IBM Domino Server for Cisco TelePresence Manager

Revised: January 28, 2010, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

This document covers the steps needed to configure IBM Domino and Domino Directory Server for the Cisco TelePresence Manager.

Important Considerations

Before you proceed with CTS-Manager installation, the servers and applications within your telecommunications network must be configured so that Cisco TelePresence Manager can find the resources and information needed to initialize the installation. These servers and applications for the IBM include the following:

These servers and applications may include one or more of the following:

- Cisco Unified Communications Manager (Version 6.1.3 or better) should already be installed and configured.
- BM Domino (Version 7.0.x, 8.0.x) (Operating System: Windows Server 2003 Enterprise Edition SP2)
  - Domino Directory Versions 7.0.x or 8.0.x. Only supported for Domino Calendar server deployments.

Note Active Directory is NOT supported for Domino Calendar server deployment with CTS-Manager

- Scheduling Clients supported
  - Lotus Notes versions: 6.5.x, 7.0.x, and 8.0.x
- This release of Cisco TelePresence Manager is designed to work with Microsoft Internet Explorer version 6.0. Cisco cannot guarantee correct system behavior using unsupported browsers.

Pre-Configuration Procedure Guidelines for IBM Domino Set-up

The purpose of this guide is to outline the chapters you will need to reference in order to pre-configure the IBM Domino before installing the CTS-Manager.

Table 4-1 Pre-Configuration Guide for IBM Domino before Setting Up CTS-Manager

Set-Up Guidelines before Installing CTS-Manager	Description	Location
Configuring IBM Domino	This chapter covers the steps needed to configure IBM Domino and Domino server for the CTS-Manager system.	Current Chapter
Next Steps After IBM Domino configuration		
Configuring Cisco Unified CM.	Before installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-Manager system.	Chapter 5, "Configuring Cisco Unified CM for Cisco TelePresence Manager"
Install and Configure PreQualification Assistant Tool	Install and configure the Pre-qualification Assistant to ensure that your pre-installation set up is configured correctly. The data you enter into the Tool Test Configuration forms are used to verify connections to the servers and get data from them to be used to configure CTS-Manager.	Chapter 6, "Installing and Configuring Cisco PreQualification Assistant"

The procedures in the next section must be completed before installing and initializing 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.

For additional information on setting up the Cisco TelePresence System, refer to the CTS Administration Guide.

Configuring IBM Domino for CTS-Manager

Step 1 Create an account in IBM Domino for CTS- Manager (e.g. ctsman account).

Use information on http://www-12.lotus.com/ldd/doc/domino_notes/7.0/help7_admin.nsf/Main?OpenFrameSet to create user account. Refer to 'Setting up Notes users' section for specific details.

Note Internet password for this account MUST be set.

Step 2 Provide an adequate mailbox quota for the CTS-Manager account.

Note Cisco System recommends setting up a CTS-Manager account with at least 1 GB of mailbox quota for a deployment of up to 50 rooms. Additional mailbox quota allocated to this user is recommended if feasible.

Step 3 Login to the CTS-Manager account once to verify it is setup correctly.

The CTS-Manager account needs to have read permission for each resource reservation database which contains any Cisco TelePresence room. Select the specific resource reservation database and right click to select *Database>Access Control*. Choose the account as specified below and set permissions per the instructions.

The CTS-Manager account also needs to have editor permissions to its own mailbox. This is required to allow storing copies of emails sent out in "Sent Items" folder.

Step 4 Create a room resource in IBM Domino for each TelePresence room. The steps might involve creating a new resource reservation database, creating a new site profile document and adding Cisco TelePresence rooms for Domino. The Resource Reservation database must be created using the Resource Reservation Template 7 and later.

Note You can create a room resource only using an administrative privilege account.

Step 5 CTS Manager display user and resource display name when displaying meeting details to end user. The display name is done by performing a full text search against domino. Once a display name is obtained, CTS Manager will cache that information and retrieve the value from the cache.

Subsequent name resolution consults the value of this cache. A full text search operation might fail with an error "NotesException: Notes error: Maximum allowable documents exceeded for a temporary full text index" on an unindexed domino directory database.

If you encounter this issue, there are several workarounds:

- 1. Indexed the domino directory (names.nsf) on the Domino Calendar Server, the server to be used to configure as "Host" in CTS-Manager under System Configuration>IBM Domino.
- 2. Increase the parameter Temp_Index_Max_Doc that limits the number of records to search . This value needs to be set to a value higher than the number of user or resource whichever is higher. For more information on this parameter and other related parameter, please check the following link: http://www.ibm.com/developerworks/lotus/documentation/notes-ini/ptot.html

Step 6 CTS-Manager uses Java Notes API to retrieve schedule information. Make sure the following server tasks are running on the Domino server.

- DIIOP Server
- HTTP Server

- LDAP Server

Directory Assistance in a Domino Deployment

Directory Assistance provides seamless authentication and authorization of Domino users existing outside the Domino directory. In order to support external LDAP users logging into CTS-Manager as a Concierge, your Domino Administrator must configure Directory Assistance to authenticate users in the external directory. In addition, users, with login privileges, must have their member groups assigned to the CTS-Manager Access Management roles.

Please refer to your Domino Administration documentation on how to configure Directory Assistance to use an external LDAP directory.

In order to verify that DA is configured correctly, perform an ldap search pointing to the Domino LDAP directory using the search filter and based dn of the external directory. This should return the user details in the external directory.

In addition, if the external directory also has a mail server setup (e.g. Exchange), DA will resolve the email ids of the external users. To verify this, login to the Domino client as a Domino user and try scheduling a meeting with the external user as the invitee. External users should be found in the meeting scheduling view.

CHAPTER 5

Configuring Cisco Unified CM for Cisco TelePresence Manager

Revised: January 28, 2010, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

This section describes adding parameters to Cisco Unified Communications Manager and researching information from the current installation of Cisco Unified Communications Manager that will be used to initialize the Cisco TelePresence Manager installation. For more information refer to *Cisco Unified Communications Manager Configuration Guide for Cisco TelePresence System.*

Important Considerations

Before you proceed with CTS Manager installation, the servers and applications within your network must be configured so that Cisco TelePresence Manager can find the resources and information needed to initialize the installation. This section cover the following applications:

- Cisco Unified Communications Manager (Version 6.1.3 or later) should already be installed and configured. For more information refer to section *Logging into the Cisco Unified CM Administrator, page 5-5* or refer to the *Cisco Unified Communications Manager Configuration Guide for Cisco TelePresence System*.

Note If you see the test connection failure message, you may need to specify IP addresses for your Cisco Unified Communications Manager server(s) if this is a non-DNS environment, as well as other network devices. You can change any server name values in Cisco Unified Communications Manager. Cisco recommends you configure the system using static IP addressing so it will be easy to manage

Pre-Configuration Procedure Guidelines for Cisco Unified CM Set-up

This table provides a guideline for the procedures you will need to reference in order to pre-configure the Cisco Unified Communications Manager **before** installing the Cisco TelePresence Manager.

Note The system uses either Microsoft or IBM not both. So either Chapter 3 or Chapter 4 needs to be referenced when doing the pre-configuration.

Table 5-1 Pre-Configuration Guideline for Setting Up CUCM for CTS-MAN

Set-Up Procedure Guidelines before Installing CTS-MAN	Description	Location
Configuring Cisco Unified CM	Before CTS-MAN installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-MAN system.	Current Chapter
Install and Configuring Pre-Qualification Assistant	Install and run the Pre-qualification Assistant to ensure that your pre-installation set-up is configured correctly. The data you enter into the Tool Test Configuration forms are used to verify connections to the servers and retrieve data from them to be used to configure CTS manager	Chapter 6, “Installing and Configuring Cisco PreQualification Assistant”

Configuring Cisco Unified CM for CTS-Manager

The procedures in the next section must be completed before installing and initializing 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.

For Deployments Using Microsoft Exchange 2003, 2007, and IBM Domino

- A Cisco Unified Communications Manager certificate must be accessible for CTS-Manager to communicate with Unified CM.

Note Only one certificate can be used. Do not reuse it or give it a new name and then try to upload it to CTS-Manager. Also, if a certificate is expired, it cannot be uploaded.

- CUCM Certificate
  - A Cisco Unified Communications Manager certificate is available from Internet Explorer, with the file extension .der. This certificate was generated when you first installed Cisco Unified Communications Manager.
  - Make a copy of the certificate and place it in a folder that is accessible to the computer that has browser access to the Cisco TelePresence Manager server.

Note Deleting a CUCM won't delete the CTS-Trust certificate corresponding to that CUCM. If the administrator adds the deleted CUCM back, then he/she doesn't need to upload the trust certificate again as it is already there in the system. If the administrator tires to upload it again, an error will be detected.

Step 1 Create an application user for CTS-Manager. Refer to section Logging into the Cisco Unified CM Administrator, page 5-5 or to your *Cisco Unified Communications Manager Configuration Guide for Cisco TelePresence System* for the steps to perform this. Save these credentials for the CTS-Manager initialization procedure that follows.

Assign all TelePresence units/IP phone devices to this user profile. MAC Address of each unit and shared phone should be added to the user profile. Add TelePresence endpoints and IP phone devices in the Cisco Unified CM Admin UI, by going to "Device > Phone."

Step 2 For each TelePresence endpoint device, follow these steps:

a. a.At the bottom of the "Device Information" section, check "**Allow Control of Device from CTI**" box.

b. b.In the "Product Specific Configuration Layout" section, enter the room email id in the "**Room Name**" field.

c. a.Assign the same DN as the IP phone that is associated to this TelePresence endpoint device.

d. In the "Directory Number Information" section of "Directory Number Configuration," check "**Allow Control of Device from CTI**" box .

Step 3 For each IP phone device that is associated to TelePresence endpoint device, check "**Allow Control of Device from CTI**" box at the bottom of the "**Device Information**" section.

Step 4 Go to "User Management > Application User," and create an application user in Cisco Unified CM for Cisco TelePresence Manager. Save these credentials for use during Cisco TelePresence Manager first time setup.

Step 5 Assign all TelePresence endpoints and their associated IP phone devices to this application user. MAC Address of each unit and IP phone should be added to the user profile.

Step 6 Create user group in the CiscoUnified CM for Cisco Telepresence Manager.

a. Assign following roles to this user group:

- Standard AXL API access
- Standard CTI enabled
- Standard serviceability
- Standard CiscoUnified CM administrative users

b. Add the above application user to the newly created user group.

Step 7 Verify all required services are activated and running on the Cisco Unified CM node. It is required to have "Cisco AXL Web Service" activated on the Cisco Unified CM Publisher node. Similarly, "Cisco RIS Data Collector" should be running on Cisco Unified CM Publisher node. "Cisco CTIManager" should be activated and running, but could be running on any node inside the same Cisco Unified CM Cluster. Please refer to the Cisco Unified CM Configuration Guide for details on service activation and start/stop.

Step 8 Download the certificate for Cisco Unified CM using IE Browser. User is prompted with a certificate when browser is pointed to Cisco Unified CM server. You can save cert file on local machine. This would be used later while configuring the CTS Manager during first time setup. You cannot upload a certificate twice even if you change the name of the certificate.

Note If a room's display name is changed once CTS-Manager is up and running, CTS Manager reads new display name once every 24 hours, so the new name will display after this 24 hour period. In addition, when a new room is added to CUCM, a restart on CTS Manager is also not required.

Configuring Cisco Unified CM Server Names

Step 1 Log into Cisco Unified Communications Manager as an Administrator.

Step 2 Choose the **Server** option from the **System** menu.

Step 3 Click **Find** to discover all the servers in your Cisco Unified Communications Manager cluster.

Step 4 In the Cisco TelePresence Manager's System Configuration -> Cisco UCM Host field, use only IP address in a non-DNS environment. If DNS is configured and accessible, use either hostname or IP address.

As you add a CUCM, do not set up the non-DNS and DNS in a mixed mode environment, i.e., where CUCM is configured with DNS and CTS-Manager is configured with non-DNS environment. CUCM is configured with DNS but has IP address in the Server Config. In a typical deployment, all applications are in either DNS or non-DNS. Identifying a CUCM node as publisher does not support mixed mode.

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

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.

Logging into the Cisco Unified CM Administrator

To log into the Cisco Unified CM Administration application, follow these steps:

Step 1 Open a web browser.

Note The Cisco Unified CM Administration program operates on the Microsoft Internet Explorer version 6 or a later version web browser.

Step 2 Access a web server that is supported by the Cisco Unified CM Administration application from any user PC in your network.

Step 3 In the address bar of the web browser, enter the following URL:

```
https://CCM-server-name
```

Where *CCM-server-name* is the name or IP address of the server.

Note You may need to specify the address of the server where Cisco Unified CM is installed. If your network uses DNS services, you can specify the hostname of the server. If your network does not use DNS services, you must specify the IP address of the server.

Step 4 Log in with your assigned administrative privileges.

Step 5 Select **Cisco Unified Communications Manager Administration** in the Navigation field at the upper right corner of the page and click **Go** to return to the Cisco Unified CM Administration home page.

Configuring the Options File

Cisco Unified CM is customized with an options file to configure support for the CTS.

To configure the options file, follow these steps:

Step 1 Log in to the Cisco Unified CM Administration application. See the "Logging into the Cisco Unified CM Administrator" section on page 5-5.

Note You must be running Cisco Unified CM version 6.1.3, or a later release.

Step 2 Add the Cisco TelePresence device pack to Cisco Unified CM. The device pack adds functionality to Cisco Unified Communications Manager so that you can create a Cisco TelePresence device. See the "Adding a Cisco TelePresence Device" section on page 5-6.

Step 3 Create a Cisco TelePresence device to register the Cisco TelePresence device as a Cisco Unified IP Phone. See the "Creating and Configuring a Cisco TelePresence Device" section on page 5-7.

Step 4 Assign a directory number to the Cisco TelePresence device. See the "Adding a Cisco TelePresence Device" section on page 5-6.

Step 5 Create a Cisco Unified IP Phone 7975 device type.

Note Auto registration cannot be used to create the device type.

Adding a Cisco TelePresence Device

Us the information in the following sections to add a CTS device:

Download Device Packs

If the Cisco TelePresence device is not listed on the Cisco Unified Communications Manager phone list, you must add the device. The Cisco TelePresence device is included in the latest device packs for Cisco Unified CM.

To download device packs, follow these steps:

Step 1 Go to the following path on Cisco.com:

Support > Voice and Unified Communications > Call Control > Download Software

Step 2 Enter your Cisco username and password and select your release.

Table 5-2 contains available software device packs:

Table 5-2

Cisco Unified CM Version	Device Package	Release Date
7.0	cmterm-devicepack7.0.2.21009-1.cop.sgn	May 15, 2009
6.1	cmterm-devicepack6.1.3.3102-1.cop.sgn	April 28, 2009
6.0	cmterm-devicepack6.0.1.3121-1.cop.sgn	May 15, 2009

Install the Device

To install the device, follow these steps:

Step 1 Log in to the Cisco Unified CM Administration application.

Step 2 At the Cisco IPT Platform Administration window, choose **Software Installation/Upgrade**.

Note For an explanation of how to access the Cisco IPT Platform Administration window, see the *Cisco IP Telephony Platform Administration Guide for Cisco Unified Mobility Manager, Release 1.2.*

Step 3 From the **Source** drop-down list, choose the source for the device pack.

Step 4 Click **Next**. The Options/Upgrades window appears.

Step 5 Choose the appropriate file from the drop-down list and click **Next**. The system compiles a checksum value.

Step 6 Click **Save** to accept the checksum value and start installation.

The installation process can take several minutes. An on-screen log reports status of the installation. Once the device pack is installed, you can begin configuring the Cisco TelePresence device.

Creating and Configuring a Cisco TelePresence Device

The following sections describe how to create and configure a Cisco TelePresence device so you can register it as a Cisco Unified IP phone:

- Adding a New Phone as a Cisco TelePresence Device, page 5-7
- Finding a Phone, page 5-8
- Configuring Cisco TelePresence Devices, page 5-8

Adding a New Phone as a Cisco TelePresence Device

Note Before you begin this procedure, note the MAC address of the Cisco TelePresence device.

To add a new phone as a Cisco TelePresence device, follow these steps from the Cisco Unified Communications Manager Administration menu bar:

Step 1 Log in to the Cisco Unified CM Administration application.

Step 2 From the Device drop-down menu, select **Phone**. The Find and List Phones Page appears.

Step 3 Click the **Add New** button at the bottom of the window. The Add a New Phone window appears.

Step 4 In the Add a New Phone window, click the **Phone Type** drop-down list and choose **Cisco TelePresence**.

Step 5 Click **Next** to display the Phone Configuration window.

Step 6 Proceed to Configuring Cisco TelePresence Devices.

Finding a Phone

To find a phone, follow these steps:

Step 1 Log in to the Cisco Unified CM Administration application.

Step 2 From the Device drop-down menu, select **Phone**. The Find and List Phones Page appears containing a list of configured phones.

Step 3 If a list of configured phones is not displayed, click the plus sign (**+**) under **Find and List Phones**.

To find all phones that are registered in the database, follow these steps:

a. Choose **Device Name** from the list of fields.

b. Choose "**is not empty**" from the list of patterns.

c. Click **Find**.

Or

d. Choose the appropriate search pattern for your text search (for example, "Begins with").

e. Enter your search text in the **Find** field.

Configuring Cisco TelePresence Devices

Note You must restart your system after you have completed the configuration tasks in this section.

This section describes how to configure Cisco TelePresence devices and associated parameters.

To configure the Cisco TelePresence device, perform the tasks in this section. When you are finished configuring your settings, click **Save** and follow the prompts to restart the system.

Before You Begin

Verify that the Phone Type and Device Protocol lists contain the following information:

- Phone Type—**Cisco 7970** or **Cisco 7975**
- Device Protocol—**SIP**

:

Device Information

To configure device information, follow these steps:

Step 1 Enter device information using the information in Table 5-3 as a guide.

Table 5-3 Cisco TelePresence Device Information

Field	Required?	Setting
MAC Address	Yes	MAC address for the Cisco TelePresence primary codec.
Description	—	Short description of the device.
Device Pool	Yes	Any
Common Device Configuration	—	Leave field as< None>.
Phone Button Template	Yes	Standard_Cisco_TelePresence
Common Phone Profile	Yes	Standard Common Phone Profile
Calling Search Space	—	Leave field as <Any>.
Media Resource Group List	—	Leave field as <None>.
Location	Yes	Hub_None
User Locale	—	Leave field as <None>.
Network Locale	—	Leave field as <None>.
Owner User ID	—	Leave field as <None>.
Phone Load Name	—	Specify required version of Cisco TelePresence System if no device default is set.
Use Trusted Relay Point	—	Chose from the following: • Default • On • Off
Calling Party Transformation CSS	—	Leave field as <None>.

Step 2 Make sure that the following check boxes at the bottom of the Device Information section are marked as indicated:

- **Use Device Pool Calling Party Transformation CSS**—Checked
- **Is Active**—Checked
- **Retry Video Call as Audio**—Checked
- **Ignore Presentation Indicators**—Unchecked
- **Allow Control of Device from CTI**—Checked
- **Logged Into Hunt Group**—Checked
- **Remote Device**—Unchecked

Step 3 Click **Save** to save your settings.

CHAPTER 6

Installing and Configuring Cisco PreQualification Assistant

Revised: January 28, 2010, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

This document explains how to install and configure the Cisco TelePresence Manager PreQualification Assistant tool.

It is important to install and run the PreQualification Assistant to ensure that the pre-configuration set-up is performed correctly. The data you enter into the Tool Test Configuration forms are used to verify connections to the servers and validate data from them to be used to configure CTS-Manager.

Pre-Configuration Procedure Guidelines for Checking Initial Network Set-up

This table provides a guideline for the procedures you will need to reference in order to check the set-up of the the network **before** installing the Cisco TelePresence Manager.

This table also lists the next couple to tasks to be performed when installing the CTS-Manager system.

Table 6-1 Pre-Configuration Guideline for Testing the Set-Up of the System Network for CTS-Manager

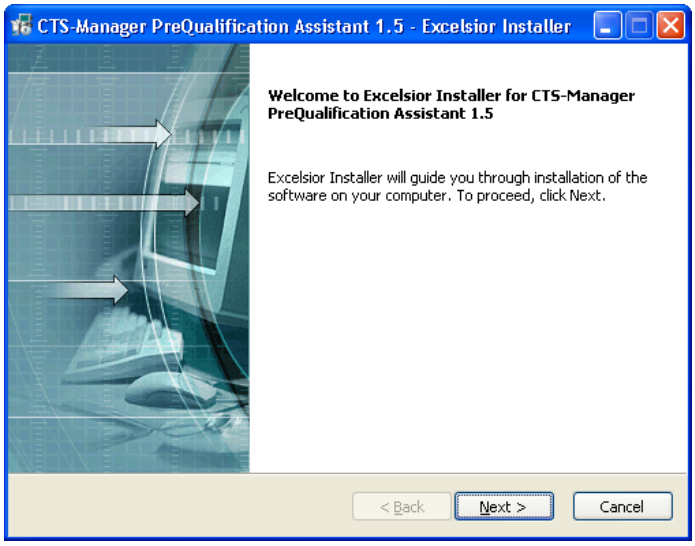
Set-Up Procedure Guidelines before Installing CTS-Manager	Description	Location
Install and configure PreQualification Assistant	Install, configure, and run the PreQualification Assistant to ensure that your pre-configuration set-up is performed correctly. The data you enter into the Tool Test Configuration forms are used to verify connections to the servers and get data from them to be used to configure CTS-Manager	Current Chapter.
Installing or Upgrading CTS-Manager software	The installation requires information about your network and the rules for finding and exchanging information. This information was set up during the pre-configuration tasks.	Chapter 7, "Installing or Upgrading Cisco TelePresence Manager"
Initializing CTS-Manager	After installing the CTS-Manager software, the next process is initializing Cisco TelePresence Manager to enable access to information sources such as Microsoft Exchange Server for meeting requests from Microsoft Outlook, Active Directory for accessing user and conference room information, and Cisco Unified Communications Manager for conference room availability and telephone support	Chapter 8, "Initializing Cisco TelePresence Manager"

Installing the PreQualification Assistant Tool

After you have downloaded the PreQualification executable, use the following procedures to install the tool.

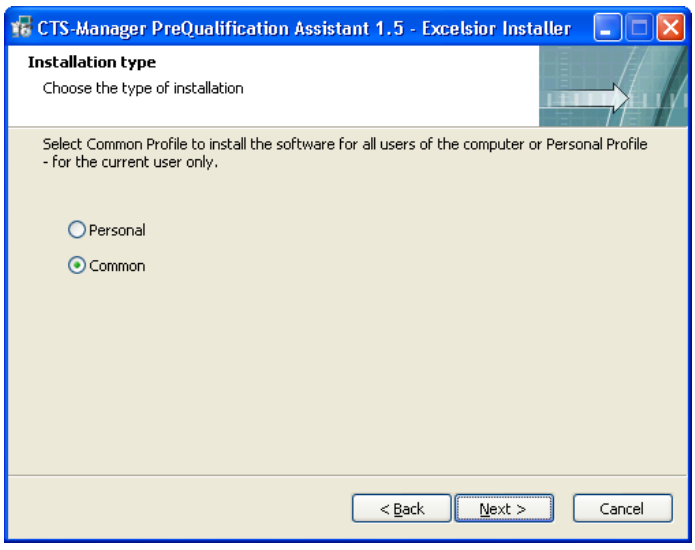
Step 1 Double-click the executable to begin the install process. After the Installer window appears, click the **Next** button.

Figure 6-1 Excelsior Installer Window



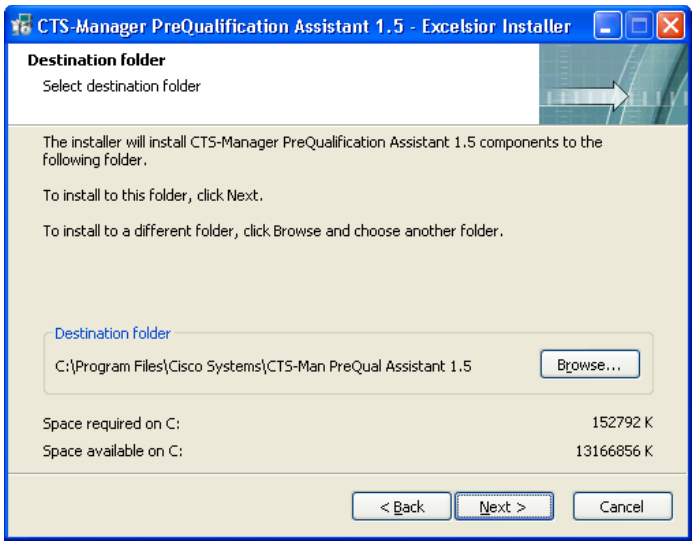
Step 2 Specify if the application is to be a personal profile or can be used by others. Then click the **Next** button.

Figure 6-2 Installation Type Window



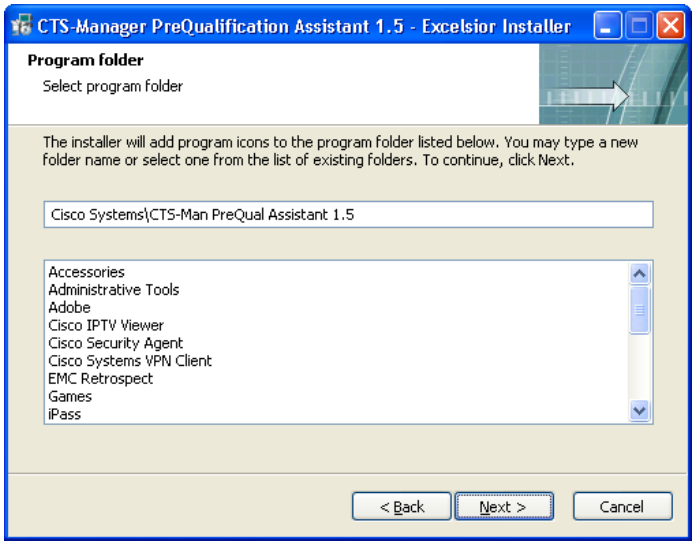
Step 3 Review and accept the destination folder defaults and click the **Next** button.

Figure 6-3 Destination Folder Window



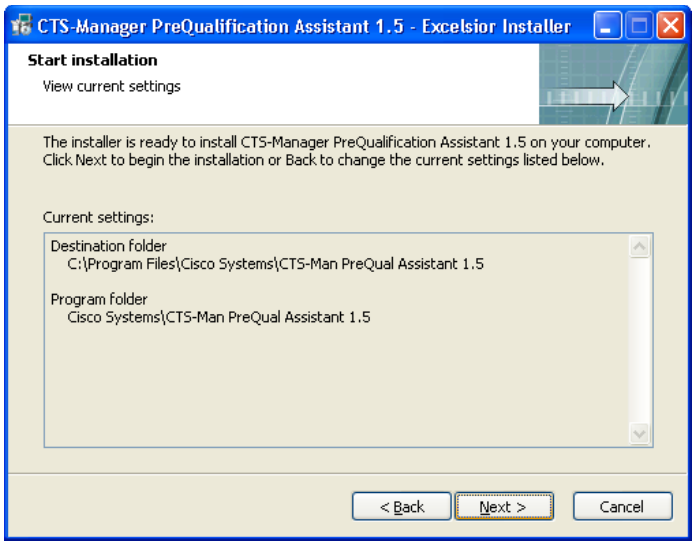
Step 4 Review the program folder destination, accept the defaults and click the **Next** button.

Figure 6-4 Program Folder Window



Step 5 In the Start Installation window, review the folder information and if correct, click the **Next** button.

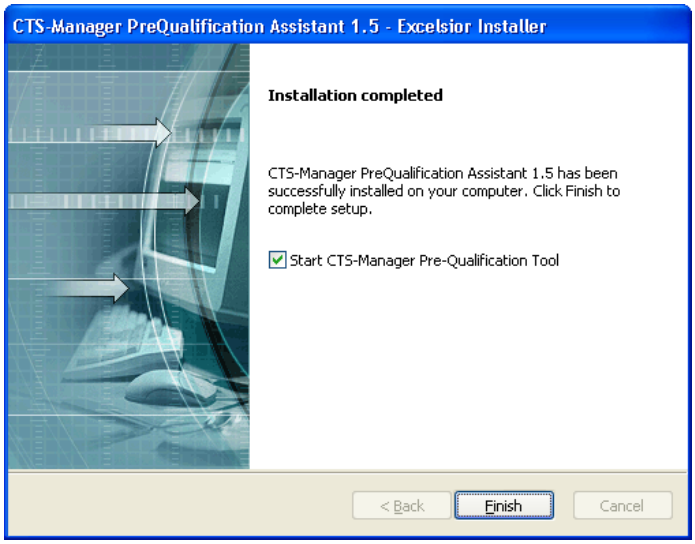
Figure 6-5 Start Installation Window



Step 6 If you are ready to finalize the installation, click **Finish** button.

Note Uncheck the **Start** checkbox if you don't want to launch the tool immediately after completing the installation.

Figure 6-6 Installation Completed Window



Uninstall Old Version

Uninstall older versions using the PreQualification uninstall. Notice that the uninstall UI shows the message that the directory is not removed at the end of the uninstall.

Step 1 Close the window.

Step 2 Open the PC TaskManager window on the PC and notice that both the uninstall processes are still running.

Step 3 In the Task Manager window, to to the processes Tab and look for the PreQualification UI. Highlight it and click on the End Process.

Step 4 Go to the Control Panel, Add or Remove Programs. Remove the PreQualification program.This will terminate the directory and it can be removed.

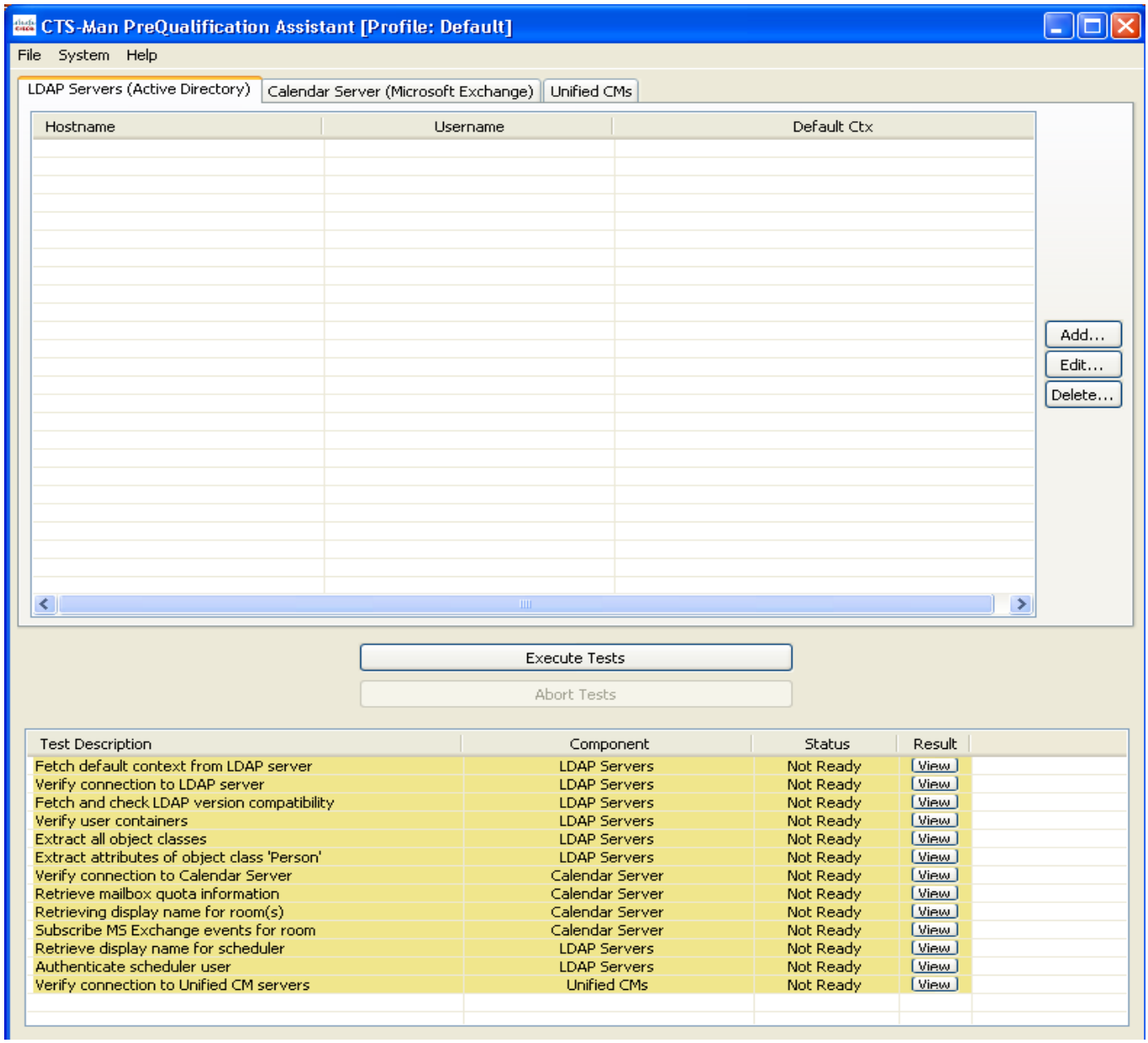
Running the Tool - Using the Tool Application Window

The CTS-Manager PreQualification tool allows administrators to determine if any changes are needed to their network to support a CTS-Manager installation.

The Tool runs a series of tests to determine if your LDAP server, Calendar server, and Cisco Unified CM configurations meet the requirements to support CTS-Manager. The set of tests you run are determined by the Calendar server running on your network (IBM Domino or Microsoft Exchange). You can also run a set of tests without specifying a Calendar server.

In order to run a series of tests you need to provide the Tool with configuration information for your LDAP servers, Calendar servers, and Cisco Unified CM servers. The three tabbed window displays the information that is configured for the servers. To add, edit or delete this information, use the Add, Edit, or Delete buttons to access the host configurations forms used to enter configuration data.

Figure 6-7 Tool Application Window



The Tool application runs a series of tests to determine if your LDAP server, Calendar server, and Cisco Unified CM server configurations meet the requirements to support CTS-Manager. The set of tests you run are determined by the Calendar server running on your network (IBM Domino, Microsoft Exchange (Active Directory), or Microsoft Exchange EWS). You can also run a set of tests without specifying a Calendar server.

The lower part of the window displays the status of each test after clicking on the Execute Test button. Once you have run a set of tests you can view the results of each test in a Test Result window. The test results contain troubleshooting data needed to prepare your LDAP servers, Calendar server, and Cisco Unified CM servers to work with CTS-Manager.

If additional analysis is required to prepare your network, you can create a zip file for technical support that includes all the test results.

The Tool application window has three main areas which are explained in the following sections.

Menu Commands

The following sections cover the commands in the File menu.

File Menu Commands

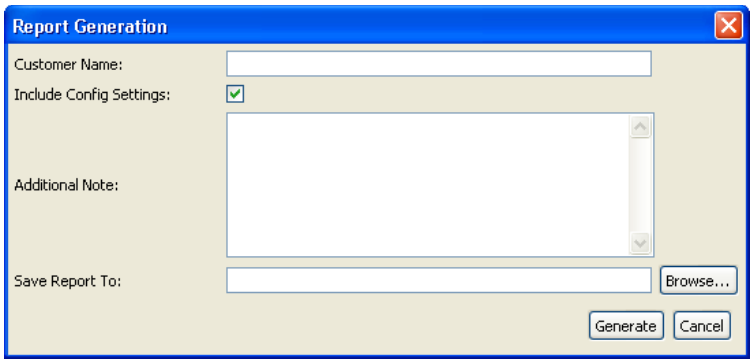
- The **New Profile** command saves all the Test form field values you have entered to a profile that can be used again.
- The **Delete Profile** command asks you to confirm your deletion of the active profile.
- The **Load Profile** command lists the saved profiles. You can choose which profile you want to use to run the PreQualification tests.

Figure 6-8 File Menu Commands

System Menu Command

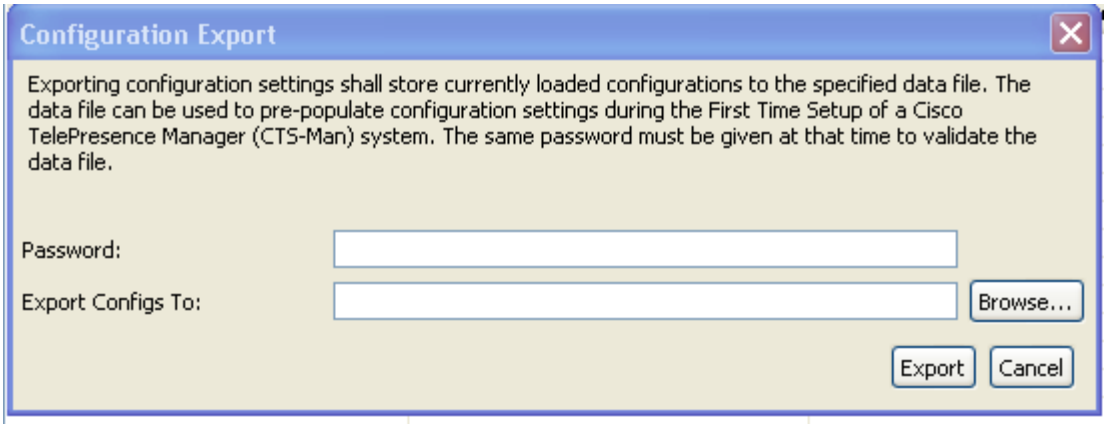
- The **Select Calendar Server** lists the Calendar servers. Choose either None, Microsoft Exchange, Domino, or Microsoft Exchange EWS to display the corresponding Test Configuration forms.
- The **Execute Tests** command performs the same function as the Execute Test button displayed above the Test Status list at the bottom of the application window.
- The **Collect Logs** command collects all the tests you've run into a zip file to make it easy to transport the results to Cisco Technical Support, refer to Figure 6-9.
  - If you check the **Include Config Settings** checkbox, the values you entered into the Host Configuration forms are collected and included in the zipped report.

Figure 6-9 Report Generation Window



- The **Export Configurations** selection allows you to export all the configurations you have saved to a data file.

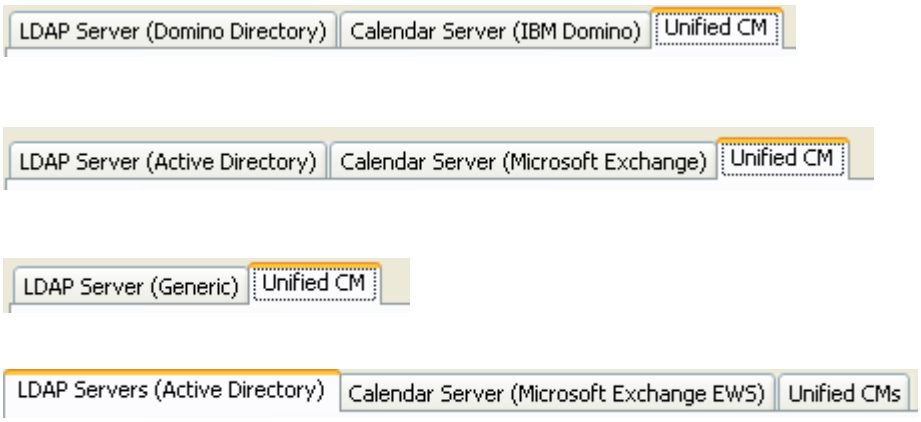
Figure 6-10 LDAP Configuration Export Window



Host Configuration Window

The PreQualification Configuration window presents four areas, selected by individual tabs. The tabs display the LDAP server, Calendar server and CUCM server configurations you've chosen from the Select Calendar Server command in the System menu.

Figure 6-11 The Forms Tabs Window



Note The Test and Add/Edit Configuration Form fields and how they are used are described in the Using PreQualification Configuration Forms section.

Test Status Window

The bottom of the application window lists the tests available. This will change depending on which server type is chosen. The Component area lists which tests are available for each server type.

Figure 6-12 The Test Status Window

Test Description	Component	Status	Result
Fetch and check LDAP version compatibility	LDAP Servers	Not Ready	View
Verify user containers	LDAP Servers	Not Ready	View
Extract all object classes	LDAP Servers	Not Ready	View
Extract attributes of object class 'Person'	LDAP Servers	Not Ready	View
Verify connection to Calendar Server	Calendar Server	Not Ready	View
Retrieve mailbox quota information	Calendar Server	Not Ready	View
Retrieve room to database mapping test	Calendar Server	Not Ready	View
Retrieving display name for room(s)	Calendar Server	Not Ready	View
Retrieve display name for scheduler	LDAP Servers	Not Ready	View
Authenticate scheduler user	LDAP Servers	Not Ready	View
Retrieve samples of calendar documents	Calendar Server	Not Ready	View
Verify connection to Unified CM servers	Unified CMs	Not Ready	View

Table 6-2 Test Status Columns

Test Description	This column describes the test.
Component	This column displays the type of test available on the different servers.

Status	This column displays the status of the test. The statuses are: • **Not Ready** - All the required Test Configuration Form fields do not have values. • **Ready** - All the required Test Confutation Form fields have the required vales entered. • **Not Applicable** - The test will not be run, because the LDAP/Calendar server does not need the test results • **Failed** - The test did not pass. Refer to the Test Results window by clicking the **View** button to the right of the failed test. • **Passed** - The test passed. There are no configuration changes needed to support the test results.
Result	This column contains the View buttons for viewing the results for each test.

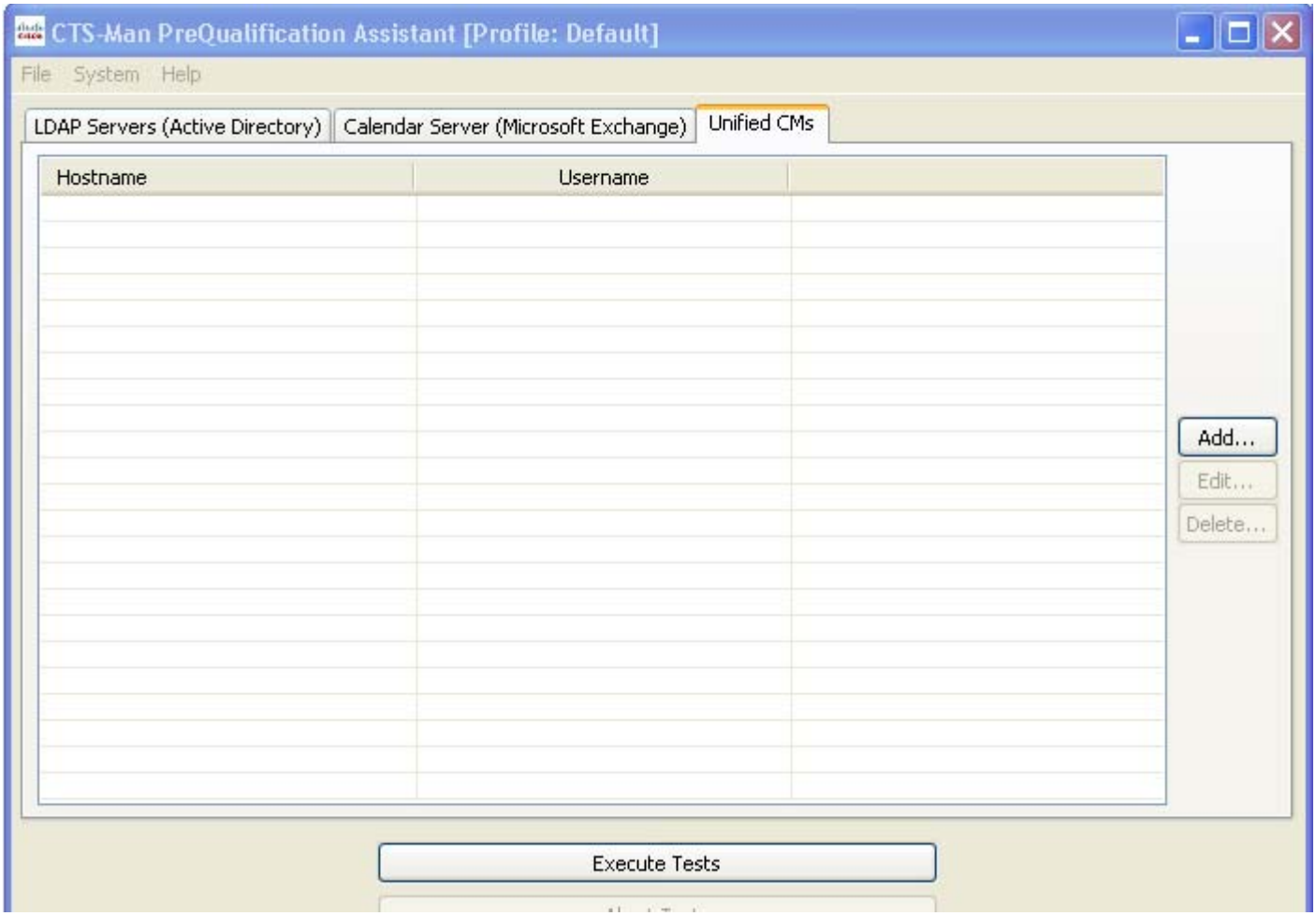
Using PreQualification Configuration Forms

There are three Test Configuration forms (LDAP server, Calendar server, and Cisco Unified CM). There are also four network environments (Exchange calendar server, Domino calendar server, Microsoft Exchange EWS, and no calendar server). There are set up windows, Add servers, Edit server configuration forms which are used to collect the data required to run the relevant tests for each network environment The sections below define the different windows and configuration forms for each network environment.

Cisco Unified Call Manager Configuration Form

The Cisco Unified CM (CUCM) Configuration form requires the same data for all three network environments.

Figure 6-13 The Cisco Unified CM List Configuration Form



This window lists all the Cisco Unified CM servers that have been configured for the CTS-Manager. If all of the CUCM servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

If it is necessary to change the configuration of one, highlight the line, and click on the Edit button to change the configuration.

To remove one, highlight it and then click on the Delete button.

When adding a CUCM, click on the Add button and the following Host Configuration window appears.

Figure 6-14 The Cisco Unified CM Add/Edit Configuration Form

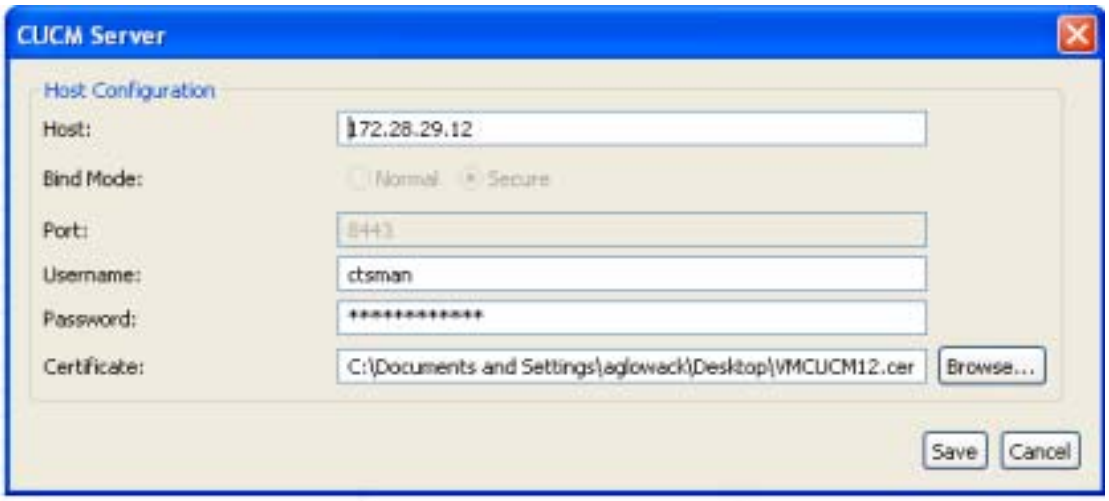


Table 6-3 The Cisco Unified CM Add/Edit Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of Cisco Unified CM
Bind Mode	This is always set to secure mode.
Port	This is always set to port 8443.
Username	Logon account with Cisco Unified CM Application User account name. The admin username is not needed.
Password	Password for Cisco Unified CM. Again, the Application User account
Certificate	The full pathname to the Cisco Unified CM security certificate.
Save	Use this button to save the configuration.
Cancel	Cancel from this window if not adding a new CUCM or editing the configuration.

Test(s) Enabled by the Host Configuration Form

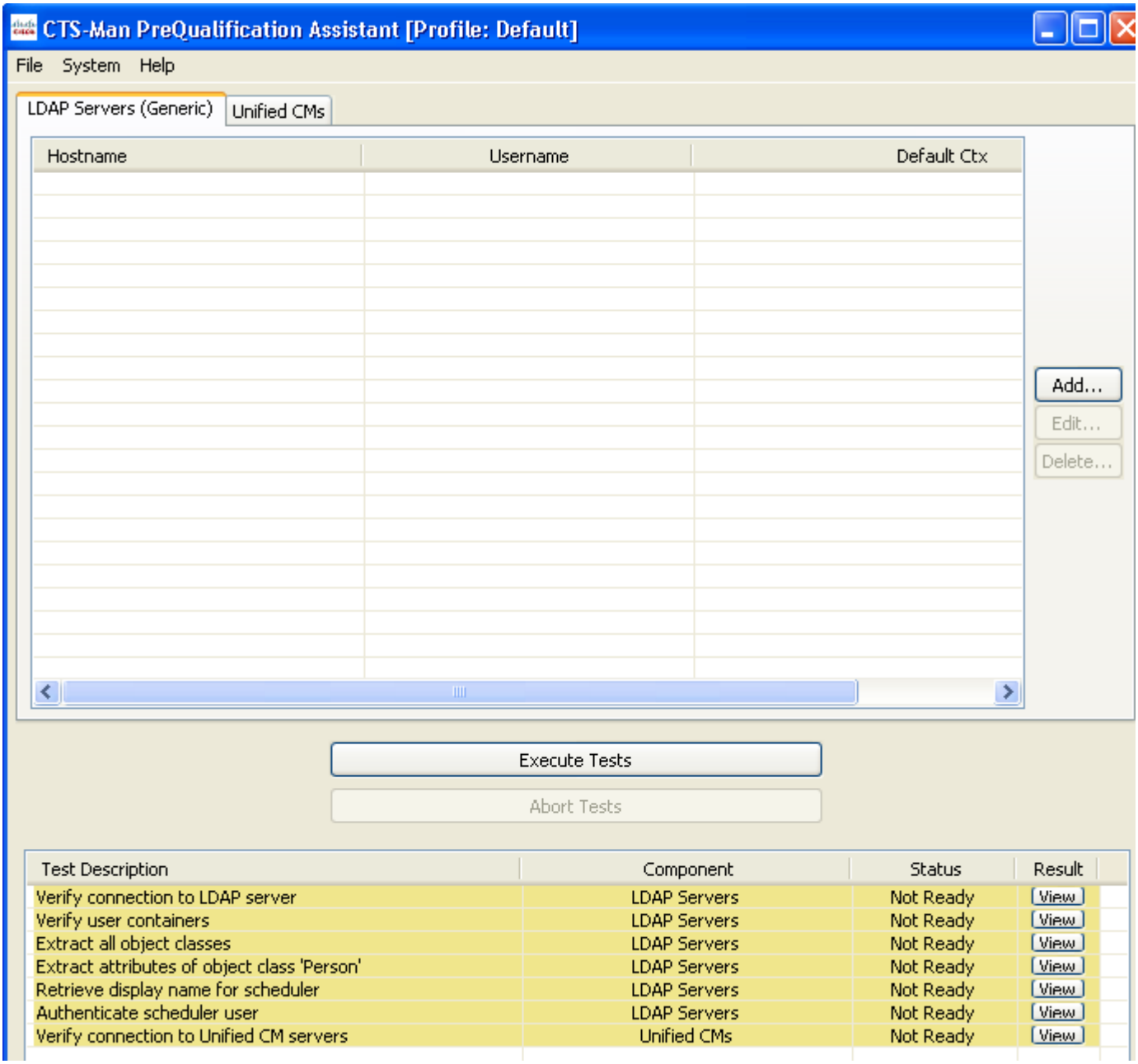
- Verify connection to Cisco Unified CM servers.

Test Host Configuration Forms in a Generic Environment

You can use the PreQualification Tool to test your LDAP server without specifying a calendar server. This applies when the user selects Calender Server, “None.”

This window lists all the generic LDAP servers that have been configured for the CTS-Manager. If all of the servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

Figure 6-15 LDAP Server Generic Window



If it is necessary to change the configuration of one, highlight the line, and click on the Edit button to change the configuration and the Host Configuration window appears, refer to Figure 6-16.

To remove one, highlight it and then click on the Delete button.

When adding another LDAP server, click on the Add button and the following configuration window appears.

Select the Unified CM's tab. This window lists all the generic CUCMs that have been configured for the CTS-Manager. If all of the CUCMs have been configured, use the Execute Tests button to make sure that they have been configured correctly.

LDAP (Generic) Test Configuration Form

Figure 6-16 The LDAP Server (Generic) Add/Edit Configuration Form

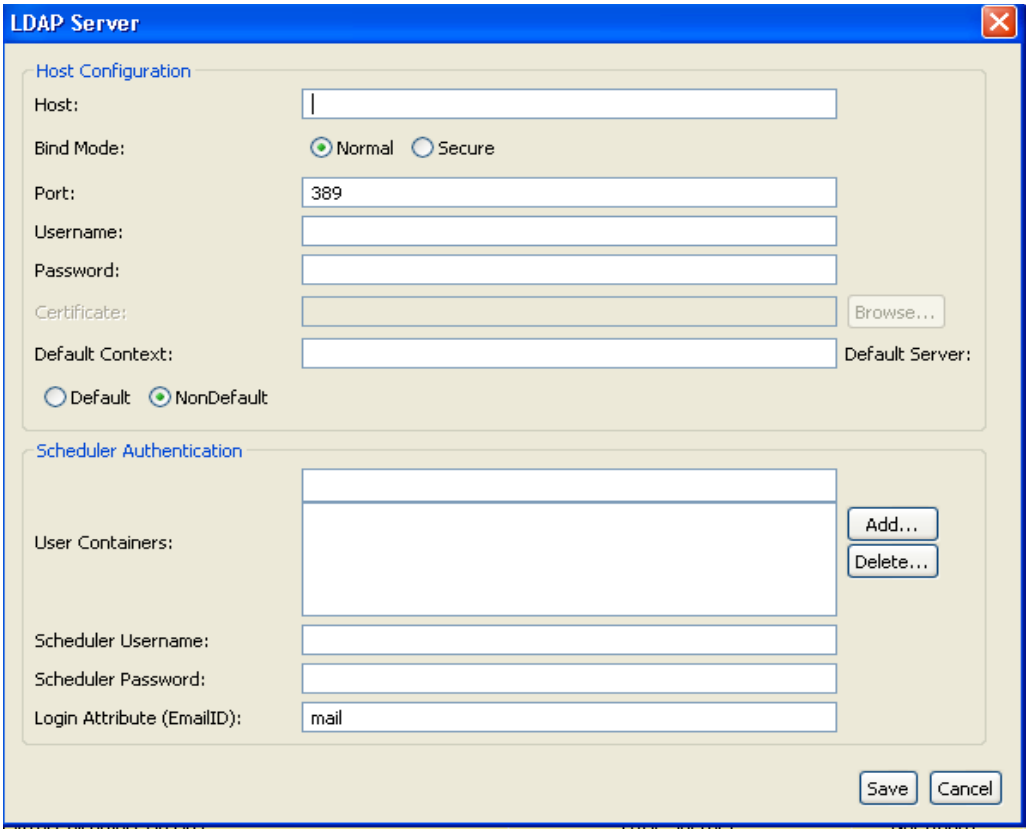


Table 6-4 The LDAP Server (Generic) Add/Edit Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of the LDAP server.
Bind Mode	If you set this to secure you'll need to provide a security certificate.
Port	In Normal bind mode the port setting is 389. In Secure bind mode the port setting default is 636.
Username	Enter the Active Directory user account username as the user fully qualified domain name (not the logon name). **Note** You also include the default context in the Username field. Examples are: *cn=administrator, cn=users, dc=mycompany, dc=com.*

Table 6-4 The LDAP Server (Generic) Add/Edit Configuration Form Fields (continued)

Field Name	Field Value
Password	Password for LDAP server with administrative privileges.
Certificate	The full pathname to the LDAP security certificate. This is needed only if you are using the Secure Bind Mode.
NonDefault or Default Context	The NonDefault button is selected as the default. To change this, select Default and enter the default context in the form: *o=ciscoDev*
Scheduler Authentication	
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. User containers are entered in the Entry field above the User Containers field. Use the Add button to add a user container to the list. To delete a user container from the list, select the specific user container and click Delete.
Scheduler Username	When the user selects “None” option, then this is not needed for generic LDAP environment, otherwise use your logon name.
Scheduler Password	When the user selects “None” option, then this is not needed for generic LDAP environment, otherwise use the same as the Password for LDAP server with administrative privileges
Login Attribute (EmailID)	For “None” option use “mail” or for Exchange 2007 use “proxy Address.”

Test(s) Enabled by this Test Configuration Form

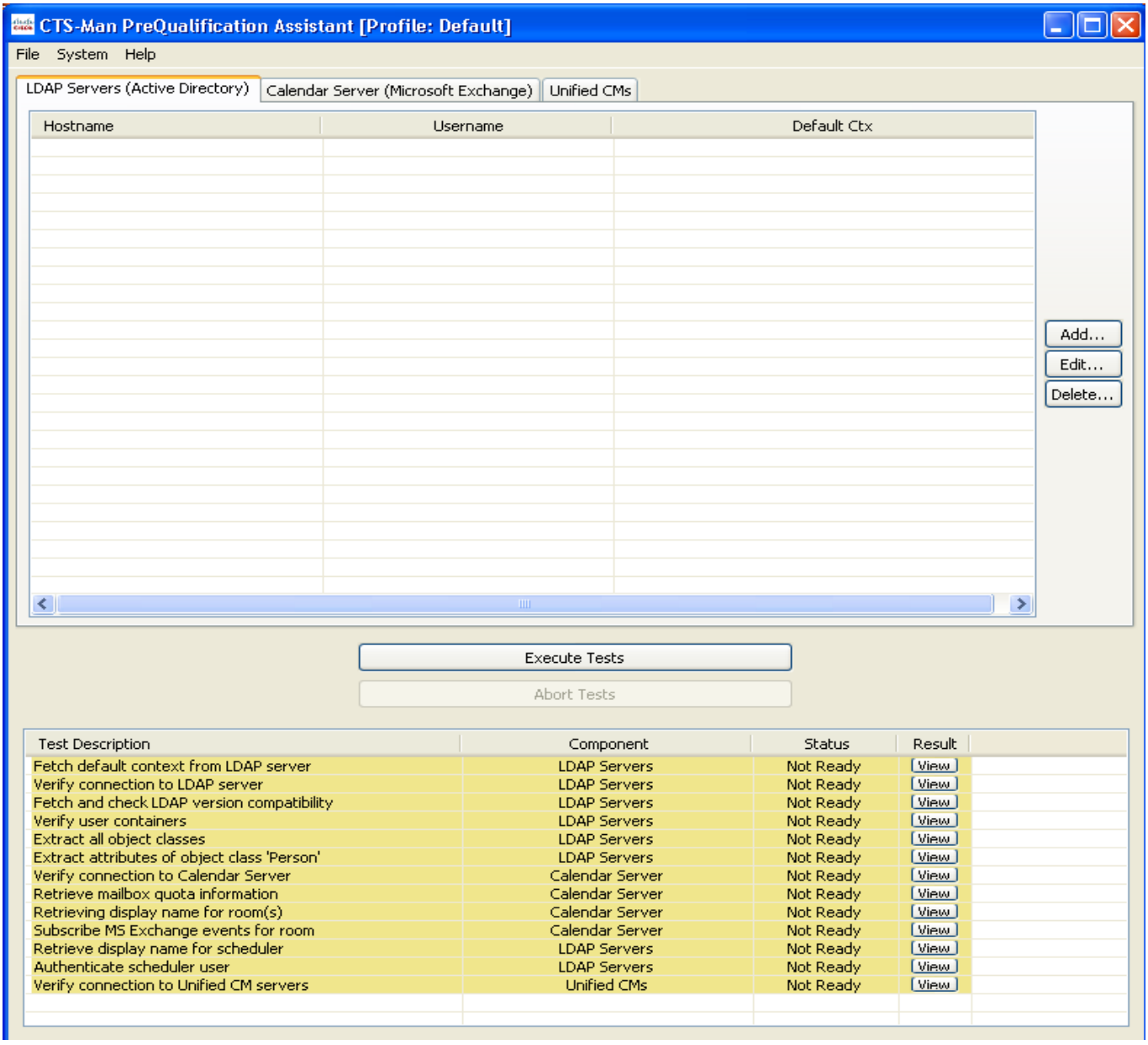
- Verify connection to LDAP server
- Verify user containers
- Extract all object classes
- Extract attributes of object class ‘Person’

Test Configuration Forms in a Microsoft Exchange Environment

You can use the PreQualification Tool to test your LDAP server when specifying a Microsoft (Active Directory) calendar server. This applies when the user selects Calender Server, “Microsoft Exchange.”

This window lists all the LDAP servers that have been configured for the CTS-Manager. If all of the servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

Figure 6-17 LDAP Server Microsoft Active Directory Window



This window lists all the LDAP (Active Directory) servers that have been configured for the CTS-Manager. If all of the LDAP servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

If it is necessary to change the configuration of one, highlight the line, and click on the Edit button to change the configuration.

To remove one, highlight it and then click on the Delete button.

When adding a LDAP server, click on the Add button and the following configuration window appears.

LDAP Server (Active Directory) Test Configuration Form

Figure 6-18 The LDAP Server (Active Directory) Add/Edit Configuration Form

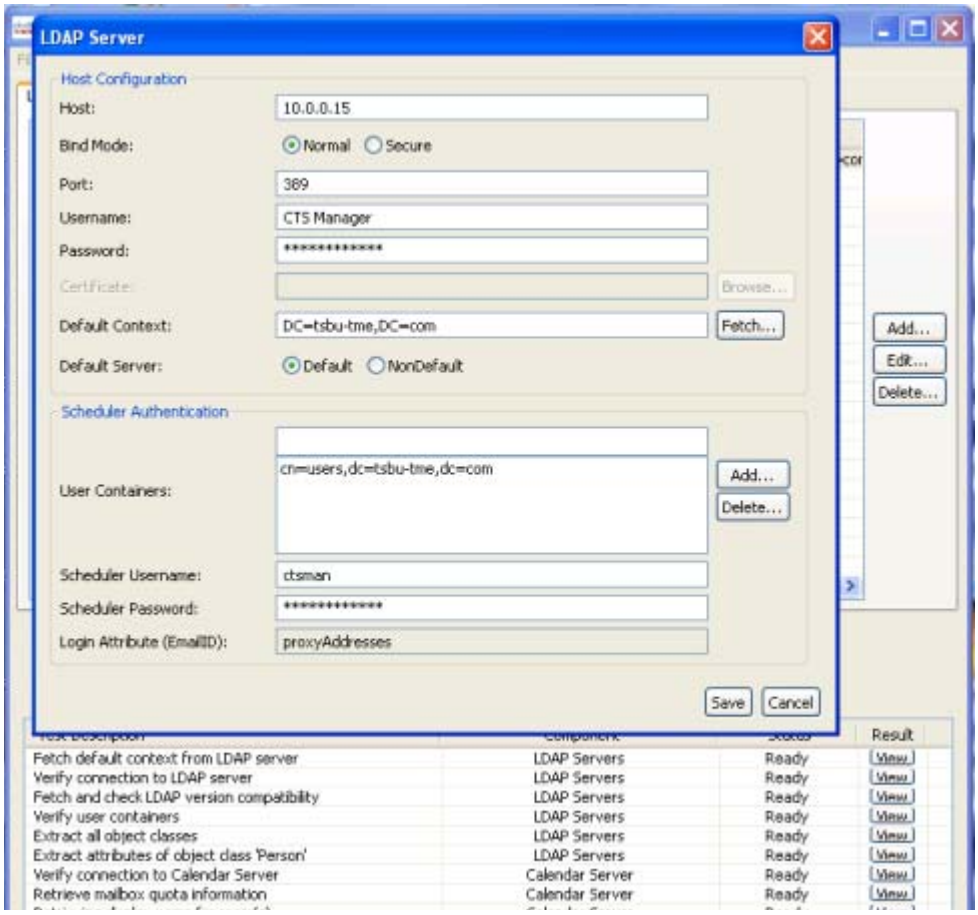


Table 6-5 The LDAP Server (Active Directory) Test Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of the LDAP server.
Bind Mode	If you set this to secure you'll need to provide a security certificate.
Port	In Normal bind mode the port setting is 389. In Secure bind mode the port setting default is 636.
NonDefault or Default Context	The NonDefault button is selected as the default. To change this, select enter the default context in the form *dc=mycompany, dc=com*
Username	Enter the Username as the user fully qualified domain name. **Note** You also include the default context in the Username field. Examples are: *cn=administrator, cn=users, dc=mycompany, dc=com.*
Password	Password for LDAP server with administrative privileges.
Certificate	The full pathname to the LDAP security certificate. This is needed only if you are using the Secure Bind Mode.
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. User containers are entered in the Entry field above the User Containers field. Use the Add button to add a user container to the list. To delete a user container from the list, select the specific user container and click Delete.
Scheduler Username	The scheduler username is the value of an end user ID.
Scheduler Password	When the user selects "None" option, then this is not needed for generic LDAP environment, otherwise use the same as the Password for LDAP server with administrative privileges
Login Attribute (EmailID)	For "None" option use "mail"

Test(s) Enabled by this Test Configuration Form

- Verify connection to LDAP server
- Verify user containers
- Extract all object classes
- Extract attributes of object class “Person”
- Retrieve display name for scheduler
- Authenticate scheduler user

Calendar Server (Microsoft Exchange) Host Configuration Form

Figure 6-19 The Calendar Server (Microsoft Exchange) Host Configuration Form

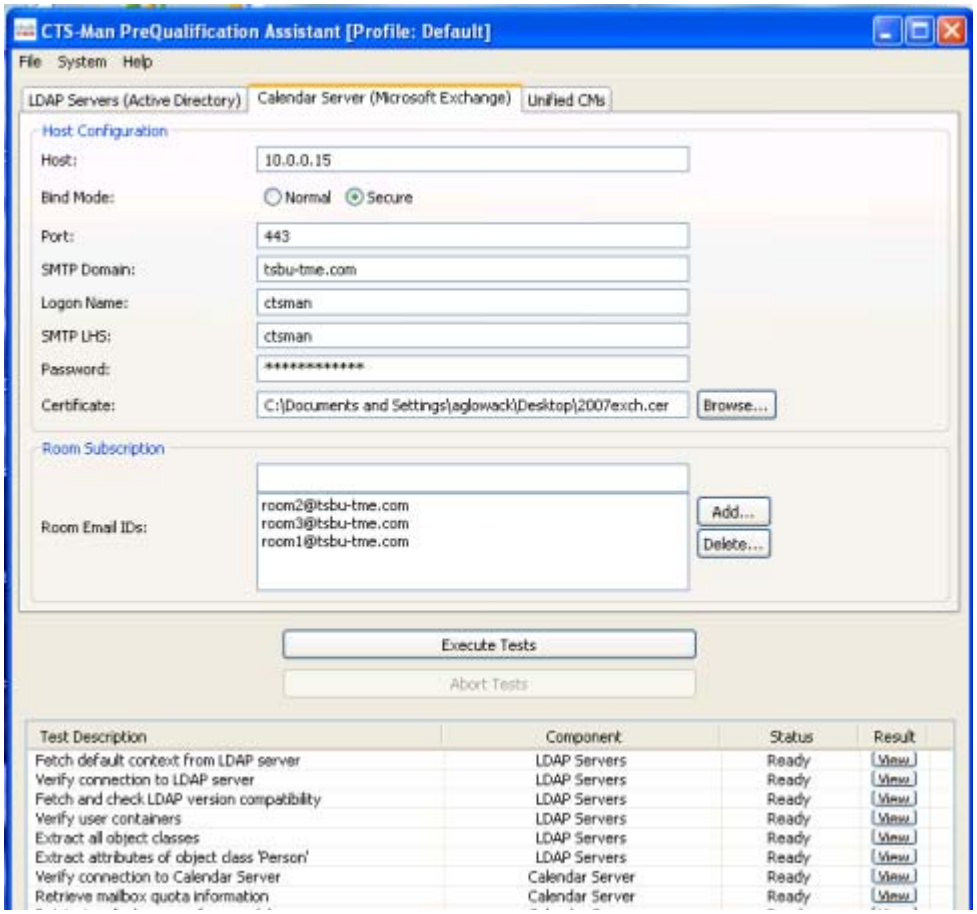


Table 6-6 The Calendar Server (Microsoft Exchange) Host Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of the Exchange server.
Bind Mode	If you set this to secure you'll need to provide a security certificate.
Port	In Normal bind mode the port setting is 80. In Secure bind mode the port setting default is 443.
SMTP LHS	Enter the CTS-Manager account or test account for full access or read access to rooms.
Password	Enter the password for the CTS-Manager test account or Exchange administrative account, using English characters only.
Certificate	The full pathname to the Exchange security certificate. This is needed only if you are using the Secure Bind Mode.
Logon Name	Enter the logon name for the full access or read access privileges to rooms. Enter the logon name in the same form as the SMTP LHS.
Domain	Enter the domain for the logon name.
Room Email IDs	Enter the full email address for each CTS endpoint, up to 5.

Test(s) Enabled by this Test Configuration Form

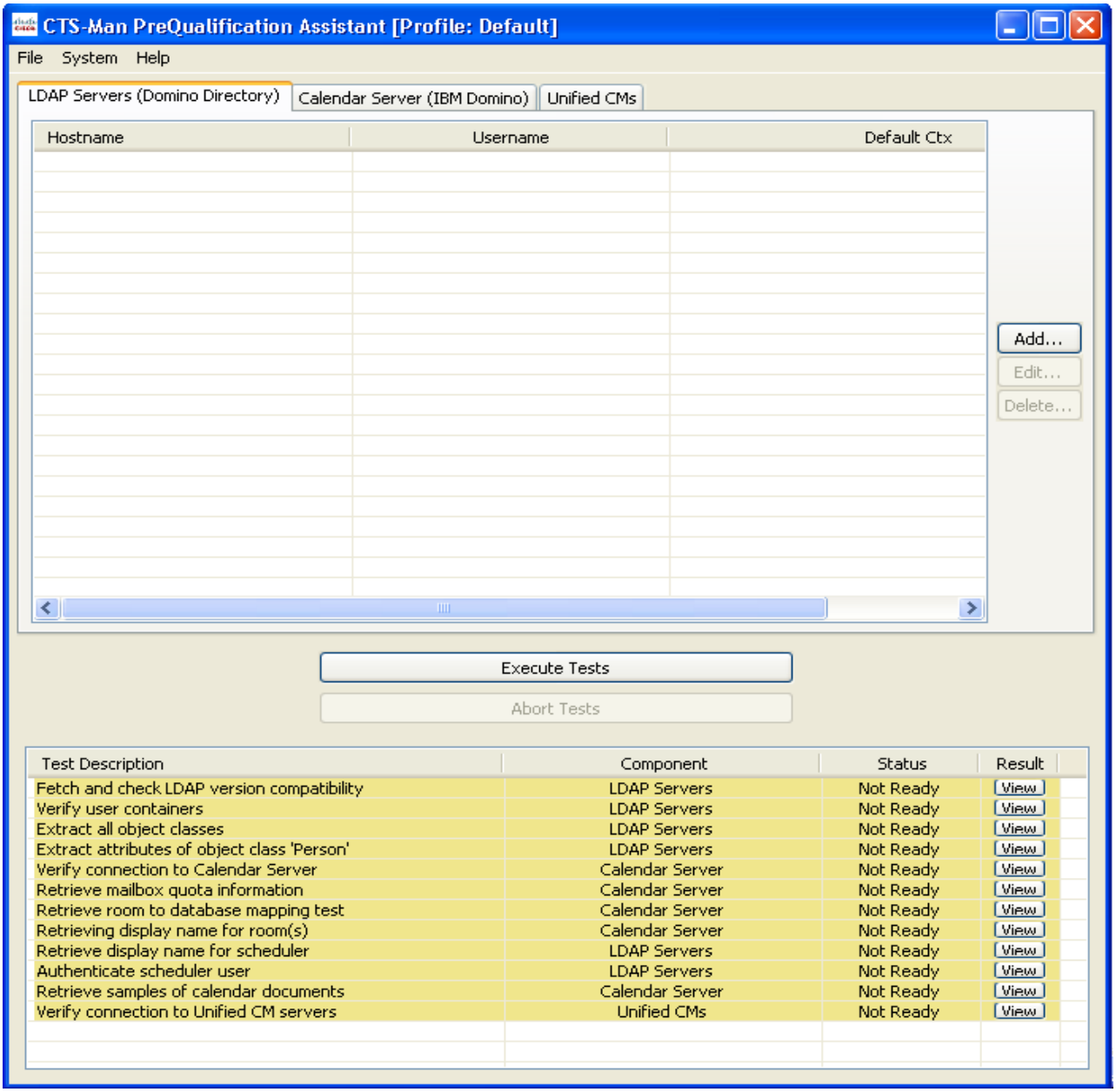
- Verify connection to Calendar Server
- Retrieve mailbox quota information
- Retrieving display name for room(s)
- Subscribe MS Exchange events for room

Test Configuration Forms in an IBM Domino Environment

You can use the PreQualification Tool to test your LDAP server when specifying a IBM Domino calendar server. This applies when the user selects Calender Server, "Microsoft Exchange."

This window lists all the LDAP servers that have been configured for the CTS-Manager. If all of the servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

Figure 6-20 LDAP Server IBM Domino Window



This window lists all the LDAP (Domino Directory) servers that have been configured for the CTS-Manager. If all of the LDAP servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

If it is necessary to change the configuration of one, highlight the line, and click on the Edit button to change the configuration.

To remove one, highlight it and then click on the Delete button.

When adding a LDAP server, click on the Add button and the following configuration window appears.

LDAP (Domino Directory) Host Configuration Form

Figure 6-21 The LDAP Server (Domino Directory) Add/Edit Configuration Form

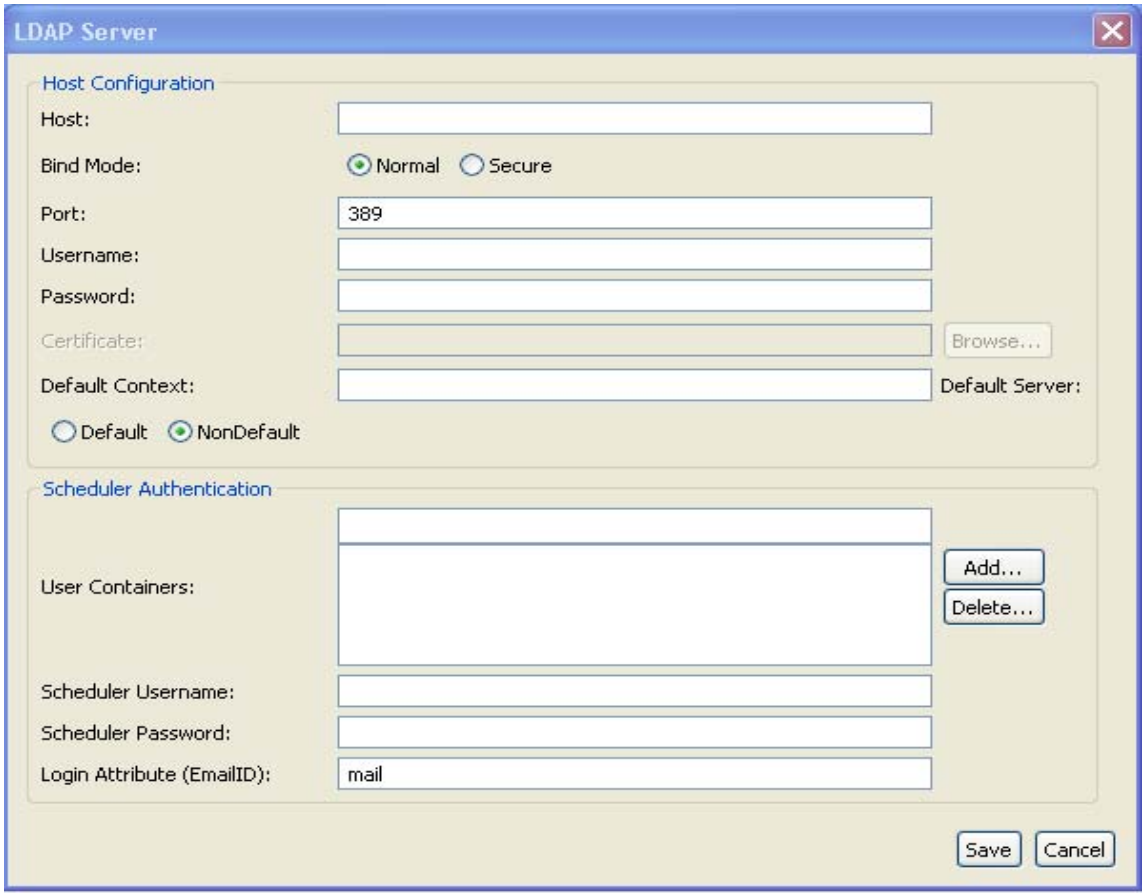


Table 6-7 The LDAP Server (Domino Directory) Test Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of the LDAP server.
Bind Mode	If you set this to secure you'll need to provide a security certificate.
Port	In Normal bind mode the port setting is 389. In Secure bind mode the port setting default is 636.
Username	Enter the Active Directory user account username (not the logon name) in the form *cn=ctm account* **Note** You must also include the default context in the Username field. For example, *cn=ctm account,o=ciscoDev.*
Password	Password for LDAP server with read privileges.

Table 6-7 The LDAP Server (Domino Directory) Test Configuration Form Fields (continued)

Field Name	Field Value
Certificate	The full pathname to the LDAP security certificate. This is needed only if you are using the Secure Bind Mode.
Default Context	Enter the default context in the form *o=ciscoDev*
Scheduler Authentication	
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. User containers are entered in the Entry field above the User Containers field. Use the Add button to add a user container to the list. To delete a user container from the list, select the specific user container and click Delete.
Scheduler Username	The scheduler username is the value of an end user ID (the logon name).
Scheduler Password	When the user selects “None” option, then this is not needed for generic LDAP environment, otherwise use the same as the Password for LDAP server with administrative privileges
Login Attribute (EmailID)	For this field use “mail”.

Test(s) Enabled by the Execute Test button

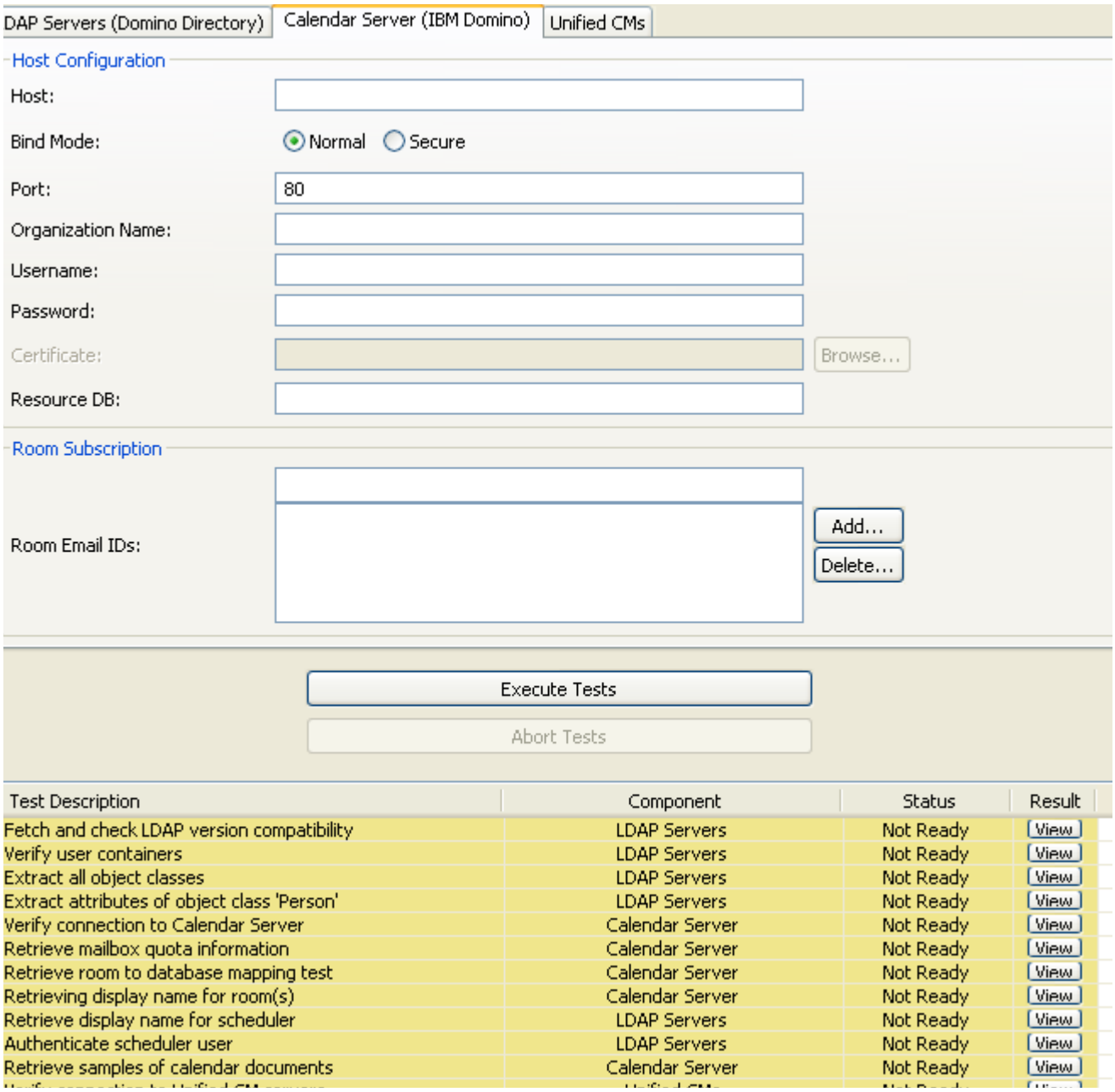
- Fetch and check LDAP version compatibility
- Verify user containers
- Extract all object classes
- Extract attributes of object class “Person”
- Retrieve display name for scheduler
- Authenticate scheduler user
- Verify connection to Unified CM servers

Calendar Server (IBM Domino) Configuration Form

You can use the PreQualification Tool to test your LDAP Calender server configurations when specifying a IBM Domino Calendar server. This applies when from the pull-down menu, the user clicks **Select Calender Server, “IBM Domino.**”

The Calender Server (IBM Domino) window appears as shown in Figure 6-22

Figure 6-22 The Calendar Server (Domino Directory) Add/Delete Configuration Form



This window lists the Calendar server that has been configured for the CTS-Manager. If the server and the room subscriptions have been configured, use the Execute Tests button to make sure that they have been configured correctly.

If it is necessary to add the room email ID, type in the room email ID and click on the Add button.

To remove one, highlight it and then click on the Delete button.

Table 6-8 The Calendar Server (IBM Domino) Host Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of the Domino Calendar server.
Bind Mode	If you set this to secure you'll need to provide a security certificate.
Port	In Normal bind mode the port setting is 80. In Secure bind mode the port setting default is 443.
Organization Name	Enter the Domino Organization name.
Username	Enter the username in the form "John Test."
Password	Enter the password for the username. The user must have a minimum of read permission on the resource database being used to test.
Certificate	The full pathname to the Domino security certificate. This is needed only if you are using the Secure Bind Mode.
Resource DB	Enter the name of the resource DB. For example, *Telepres.nsf.*
Room Subscription	
Room Email IDs	Enter the full email id for each CTS endpoint. The format for each Email id is: *Testroom/Site1*

Test(s) Enabled by the Execute Tests button

- Verify connection to Calendar Server
- Retrieve mailbox quota information
- Retrieve room to database mapping test
- Retrieving display name for room(s)
- Retrieve samples of calendar documents

Cisco Unified Call Manager Server (IBM Domino) Configuration Window

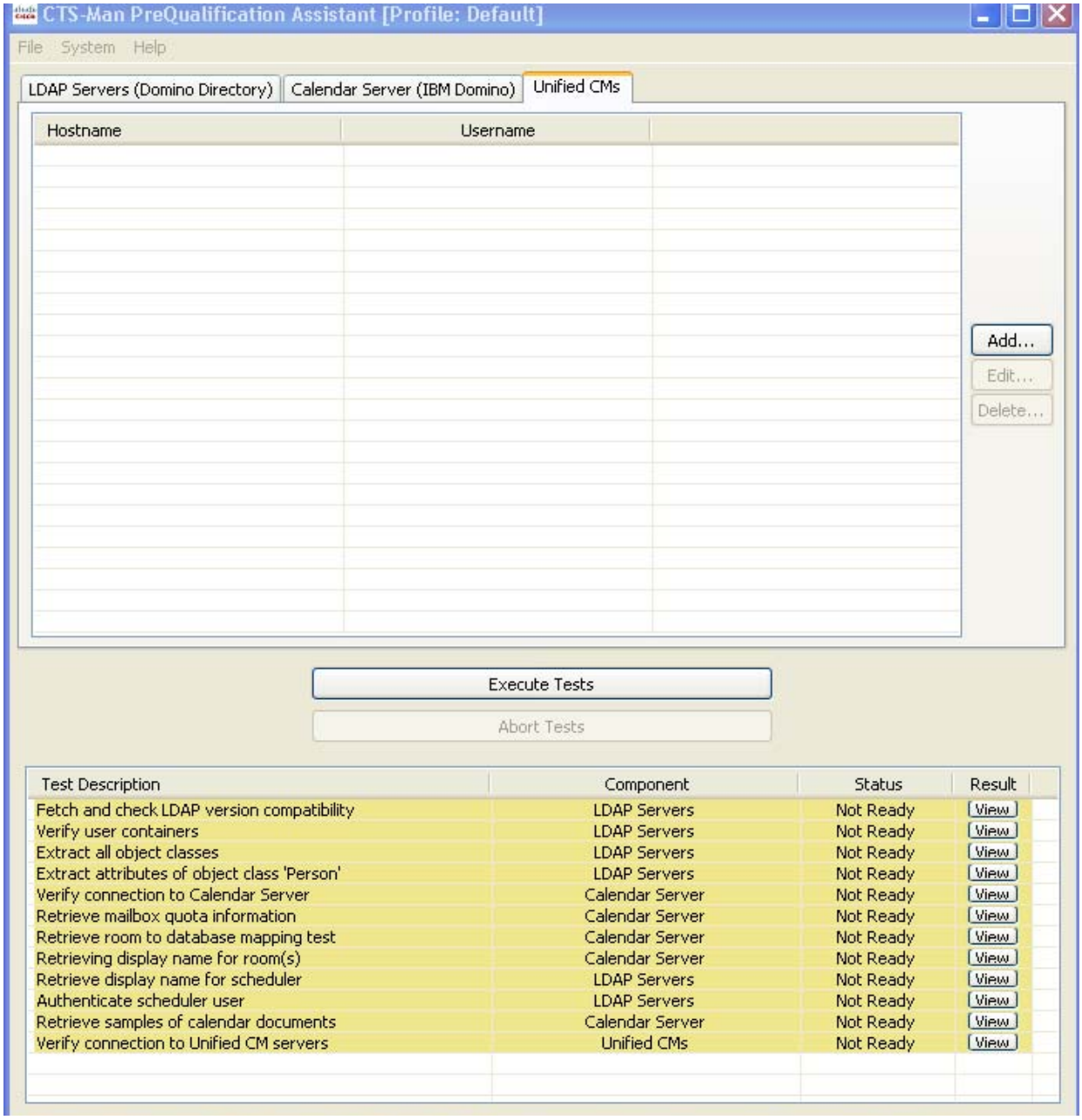
This window lists all the Cisco Unified CM (CUCM) servers that have been configured for the CTS-Manager. If all of the CUCM servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

If it is necessary to change the configuration of one, highlight the line, and click on the Edit button to change the configuration.

To remove one, highlight it and then click on the Delete button.

When adding a CUCM, click on the Add button and the following Host Configuration window appears.

Figure 6-23 Unified Call Manager Server (IBM Domino) Window



This window lists all the LDAP (Domino Directory) servers that have been configured for the CTS-Manager. If all of the LDAP servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

If it is necessary to change the configuration of one, highlight the line, and click on the Edit button to change the configuration.

To remove one, highlight it and then click on the Delete button.

When adding a LDAP server, click on the Add button and the following configuration window appears.

LDAP (Domino Directory) Host Configuration Form

Figure 6-24 The Cisco Unified CM Add/Edit Configuration Form

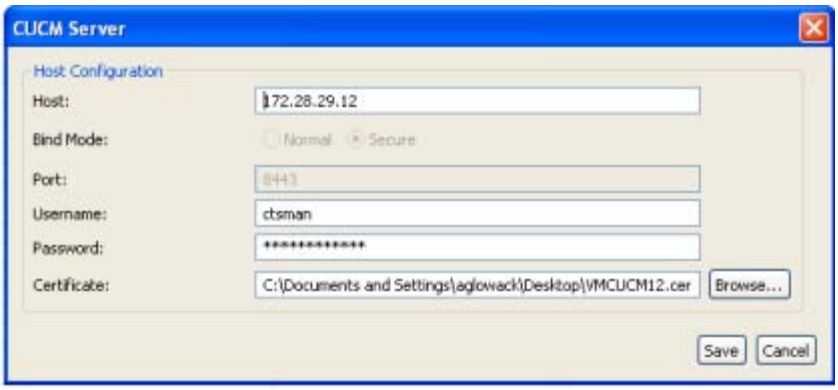


Table 6-9 The Cisco Unified CM Add/Edit Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of Cisco Unified CM
Bind Mode	This is always set to secure mode.
Port	This is always set to port 8443.
Username	Logon account with Cisco Unified CM Application User name. The admin username is not needed.
Password	Password for Cisco Unified CM Admin account.
Certificate	The full pathname to the Cisco Unified CM security certificate.
Save	Use this button to save the configuration.
Cancel	Cancel from this window if not adding a new CUCM or editing the configuration.

Test(s) Enabled by the Execute Test button

Test(s) Enabled by the Execute Test button

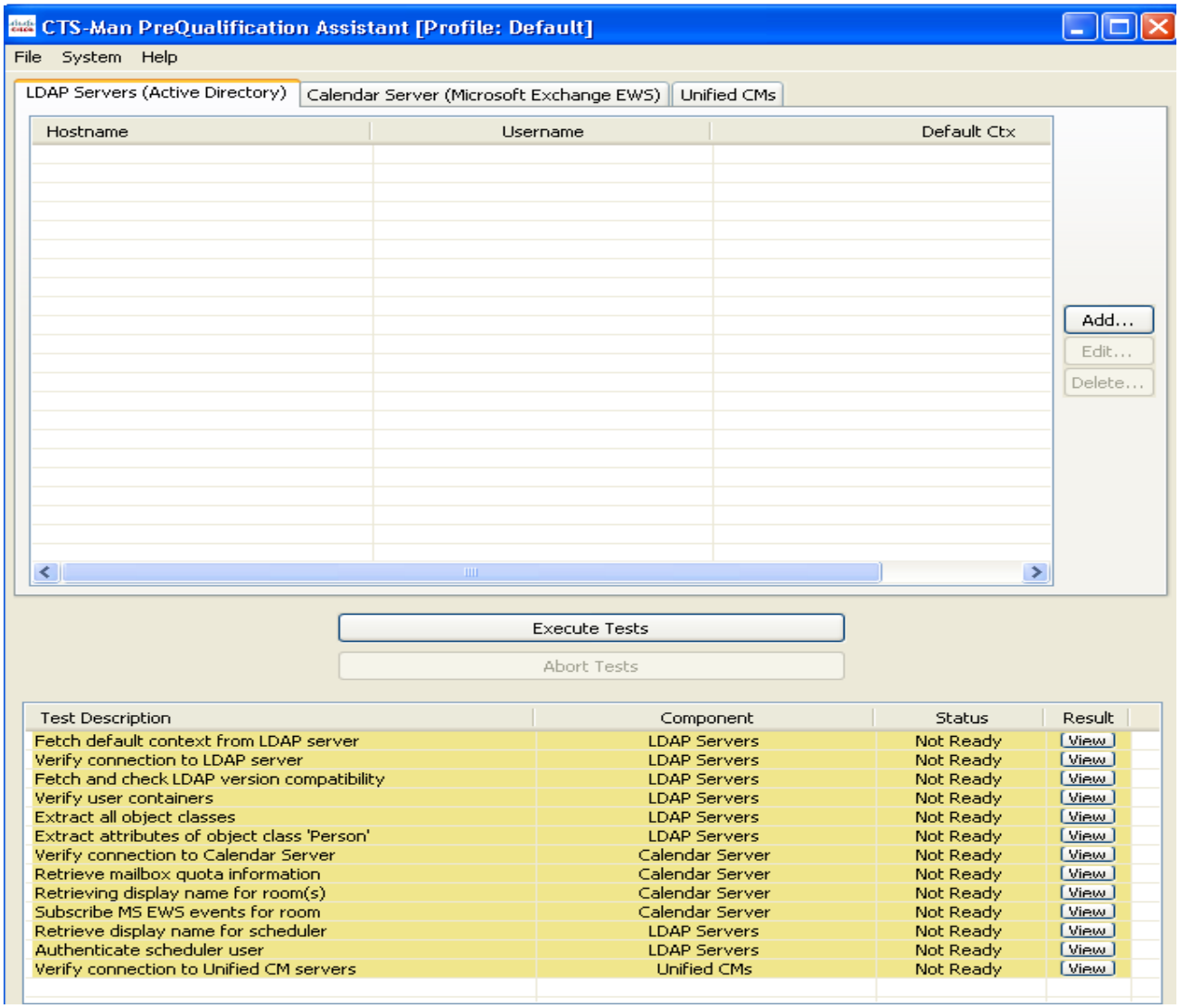
- Verify connection to Unified CM servers

Test Configuration Forms in a Microsoft Exchange Web Services (EWS) Environment

You can use the PreQualification Tool to test your LDAP server when specifying a Microsoft Exchange EWS calendar server. This applies when the user selects Calender Server, "Microsoft Exchange EWS."

This window lists all the LDAP servers that have been configured for the CTS-Manager. If all of the servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

Figure 6-25 LDAP Servers with Microsoft Exchange EWS Calendar Server window



This window lists all the Microsoft LDAP servers that have been configured for the CTS-Manager. If all of the servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

If it is necessary to change the configuration of one, highlight the line, and click on the Edit button to change the configuration and the Host Configuration window appears, refer to Figure 6-26.

To remove one, highlight it and then click on the Delete button.

When adding another LDAP server, click on the Add button and the following configuration window appears.

LDAP Server (Active Directory) Add/Edit Configuration Form

This is the same configuration form that appears when adding any Microsoft Exchange server.

Figure 6-26 The LDAP Server (Active Directory) Add/Edit Configuration Form

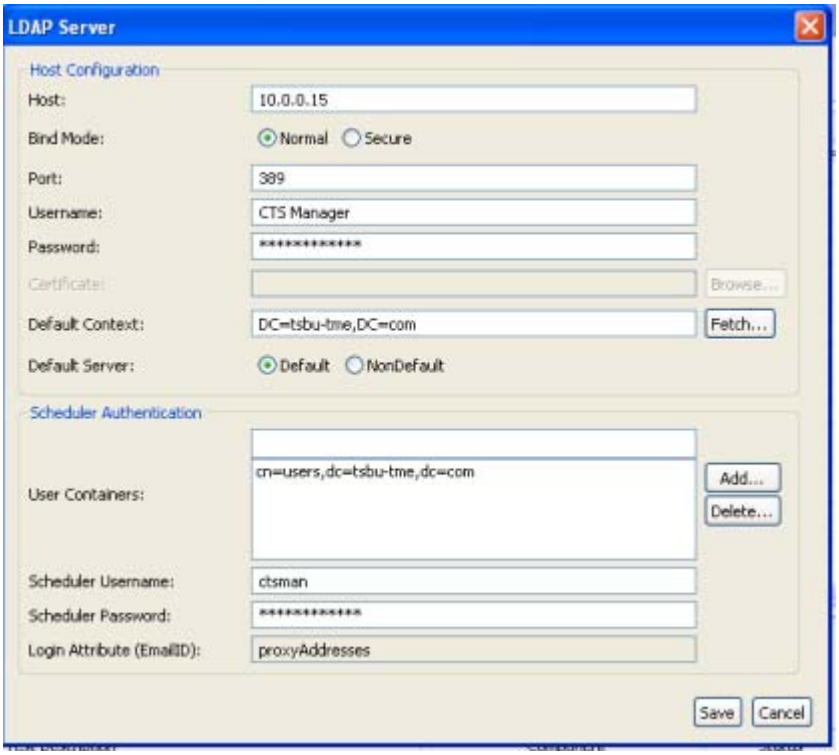


Table 6-10 The LDAP Server (Active Directory) Test Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of the LDAP server.
Bind Mode	If you set this to secure you'll need to provide a security certificate.
Port	In Normal bind mode the port setting is 389. In Secure bind mode the port setting default is 636.

Table 6-10 The LDAP Server (Active Directory) Test Configuration Form Fields (continued)

Field Name	Field Value
Username	Enter the Username as the user fully qualified domain name. **Note** You also include the default context in the Username field. Examples are: *cn=administrator, cn=users, dc=mycompany, dc=com.*
Password	Password for LDAP server with administrative privileges.
Certificate	The full pathname to the LDAP security certificate. This is needed only if you are using the Secure Bind Mode.
NonDefault or Default Context	The NonDefault button is selected as the default. To change this, select enter the default context in the form *dc=mycompany, dc=com*
Scheduler Authentication	
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. User containers are entered in the Entry field above the User Containers field. Use the Add button to add a user container to the list. To delete a user container from the list, select the specific user container and click Delete.
Scheduler Username	The scheduler username is the value of an end user ID.
Scheduler Password	The password associated with the scheduler username.
Login Attribute (EmailID)	Use the “proxyAddresses” EmailID attribute.

Test(s) Enabled by the Execute Test Button

- Fetch default context from LDAP server
- Verify connection to LDAP server
- Fetch and check LDAP version compatibility
- Verify user containers
- Extract all object classes

- Extract attributes of object class “Person”
- Verify connection to Calendar Server
- Retrieve mailbox quota information
- Retrieving display name for room(s)
- Subscribe MSEWS events for room
- Retrieve display name for scheduler
- Authenticate scheduler user
-

LDAP Server Microsoft Exchange EWS Calendar Server Configuration Form

When you select the Calendar Server tab, Figure 6-27 appears. This window allows you to configure the calendar server for Microsoft Exchange EWS and add or delete room subscriptions.

Figure 6-27 LDAP Calendar Server Microsoft Exchange EWS Configuration Window

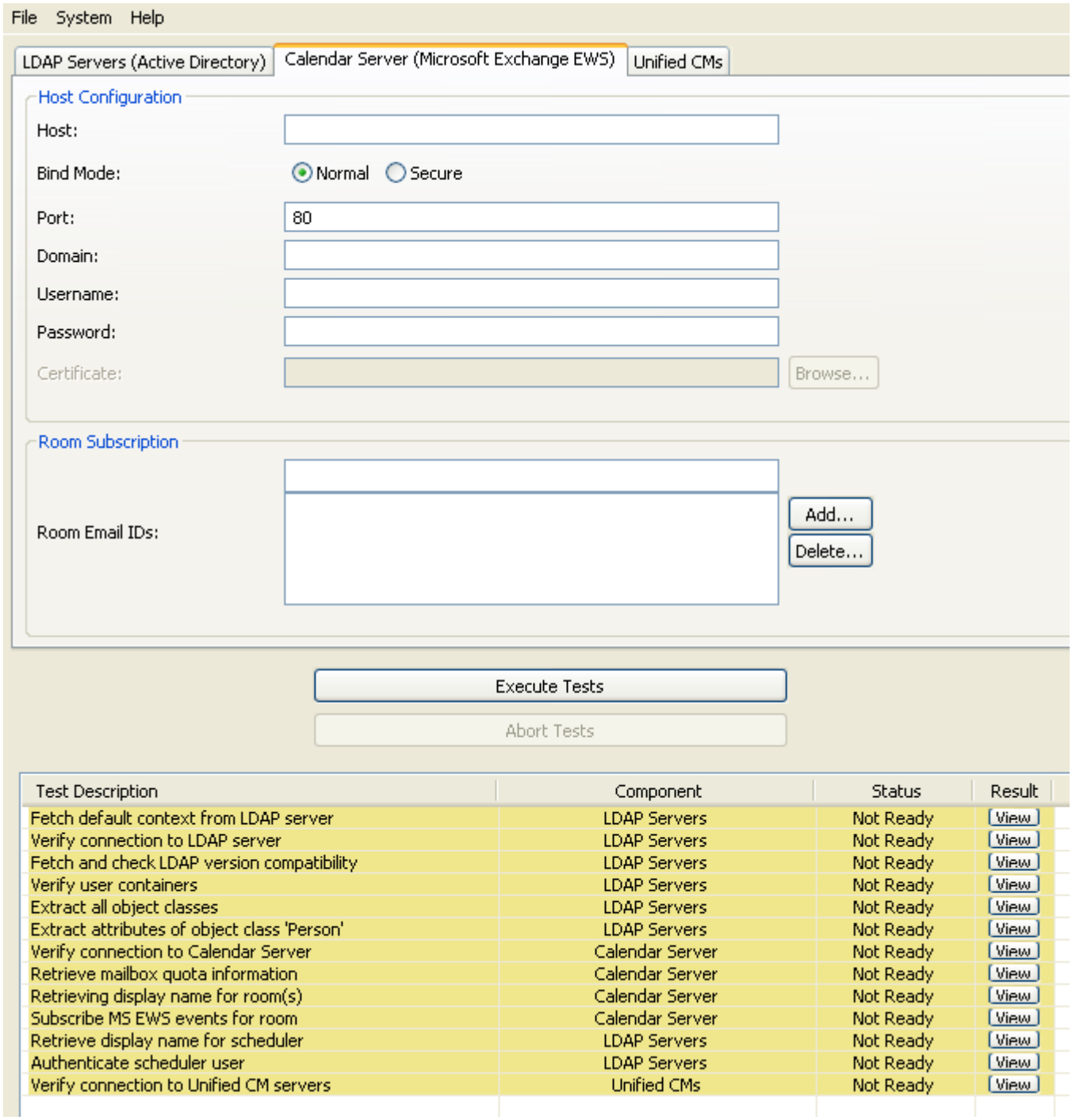


Table 6-11 The Calendar Server (Microsoft Exchange) Host Configuration Form Fields

Field Name	Field Value
Host	The hostname or IP address of the Exchange server.
Bind Mode	If you set this to secure you'll need to provide a security certificate.
Port	In Normal bind mode the port setting is 80. In Secure bind mode the port setting default is 443.
Domain	Enter the domain for the logon name.
Username	Enter the Username as the user fully qualified domain name. **Note** You also include the default context in the Username field. Examples are: *cn=administrator, cn=users, dc=mycompany, dc=com.*
Password	Enter the password for the CTS-Manager test account or Exchange administrative account, using English characters only.
Certificate	The full pathname to the Exchange security certificate. This is needed only if you are using the Secure Bind Mode.
Room Subscription	
Room Email IDs	Enter the full email address for each CTS endpoint, up to 5.

CHAPTER 7

Installing or Upgrading Cisco TelePresence Manager

Revised: January 28, 2010, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

This document explains how to install the Cisco TelePresence Manager software in your network. You will then be able to schedule Cisco TelePresence system meetings through existing Microsoft Outlook messaging software or IBM Domino software, receive reminders, and connect to a remote meeting site with the touch of a button.

To enable these features, you must provide Cisco TelePresence Manager with the contact and access information it requires to connect to and talk with your network. The purpose of this guide is to walk you through each step using the Cisco TelePresence Manager installation DVD and the accompanying wizard help windows.

The installation requires information about your network and the rules for finding and exchanging information.Once this pre-installation data is set up, then the Cisco TelePresence Manager program can be installed from DVD .In addition, the administrator can use the System Configuration window to upgrading system software,

System Information

The System Information window to see a quick summary of information about your Cisco TelePresence System. The window is divided into two areas:

- System Information lists model numbers, hostname, addresses, and hardware and software version information.
- Product Software Versions lists software currently configured in the system. It includes product names and version numbers.

Table 7-1 System Information

SKU	CTS-Manager1.5.x
Hostname	The name of the CTS-Manager server (e.g. tsbu-ctm19).
IP Address	The IP address of the CTS-Manager server.
Subnet Mask	The subnet mask of the CTS-Manager server (e.g. 255.255.255.0).
MAC Address	The MAC address of the CTS-Manager server (e.g. 00:18:fe:73:58:14).
Hardware Model	The hardware model of the CTS-Manager server (e.g. 7835H2).
Software Version	The version of CTS-Manager software running on the server (e.g. 1.5.0.0).
OS Version	The software version of the Cisco Unified Communications OS running on the CTS-Manager server (e.g. CUCOS 3.0.0.0-44).

Installation Guidelines

The purpose of this guide is to reference the information you will need in order to install the CTS-Manager software.

The flow of tasks you need to perform to install and configure the CTS-Manager are provided in the following table.

Table 7-2 Install Guide for setting up CTS-Manager

Set-Up Procedure Guidelines after Installing CTS-Manager	Description	Location
Initializing CTS-Manager	After installing the CTS-Manager software, the next process is initializing Cisco TelePresence Manager to enable access to information sources such as Microsoft Exchange Server for meeting requests from Microsoft Outlook, Active Directory for accessing user and conference room information, and Cisco Unified Communications Manager for conference room availability and telephone support	Chapter 8, "Initializing Cisco TelePresence Manager"
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 reconfigure system settings	Chapter 9, "Additional Installation Configurations for Cisco TelePresence Manager"
Monitoring CTS-Manager	Monitoring and updating meeting schedules and monitoring the status of rooms and system services	Chapter 10, "Monitoring Cisco TelePresence Manager"

Installing Cisco TelePresence Manager from DVD

The following section covers installation procedures for the CTS-Manager.

Required Information and Equipment

To install the Cisco TelePresence Manager system files, the following equipment and information are needed:

- The Model 7845 Cisco Media Convergence Server that came with Cisco TelePresence Manager, installed and connected to a Domain Name System (DNS) server and your network.
- The information, listed in Table 7-3, "Installation Window and field Definitions" that includes your system-specific values and parameters.
- A management console able to access the Model 7845 Cisco Media Convergence Server.

- The DVD included in your Cisco TelePresence Manager documentation and installation packet. Use the Installation Wizard included on this disk.

Introduction to the CTS-Manager Administration Software

CTS-Manager Administration software is accessed through your browser. All Cisco TelePresence administration software supports Internet Explorer 6.0. CTS-Manager Administration software is accessed through the server's host name or IP address.

Logging Into CTS-Manager

When doing a login to the account to access the CTS-Manager functions, use:

- your email ID if using Microsoft Exchange
- your own corporate login attribute (mail) if using IBM Domino.

There are three levels of functionality when logging into CTS-Manager. Any user not in these access categories will only see their own meeting details.

Administrator Role

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

- System Information
- System Status
- Support
- System Configuration
- Troubleshooting

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

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

Superuser Role

The system superuser has a special login account that allows access to two additional administrative tasks. These tasks are only visible by logging in using the superuser password. This role is used mainly during installation of CTS-Manager. After installation of CTS-Manager, this role will default to administrator.

- System Settings

- Software Upgrade

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

Installation Procedure for Cisco TelePresence Manager

Step 1 Insert the CTS-Manager installation DVD in the server.

There may be a short delay while the installer validates the integrity of the files on the DVD and configures the server for the operating system and the CTS-Manager software.

Caution Remove the DVD from the DVD drive after the installation/upgrade is complete. Leaving the DVD in the drive can prevent CTS- Manager from restarting properly after rebooting the server.

Step 2 The installer checks for a prior installation of CTS-Manager software. Choose **Yes** to continue, or **No** to abort the installation.

Step 3 If you choose **Yes** to continue the installation, the Installation Wizard opens in the next window. Read and become familiar with the wizard conventions.

Step 4 Click **Proceed**.

Step 5 Fill in each window with the information defined in Table 7-3, "Installation Window and field Definitions".

Step 6 When you are satisfied that the information is correct, click **OK** in the Configuration Confirmation window to begin the installation process. Be patient while the process takes place.

When the installation is complete, the server reboots. The installer then checks for network connectivity and access to a DNS server. If it cannot find these connections, an error message is displayed. If the installation process completes successfully, the message "The Installation of the Cisco TelePresence Manager Has Completed Successfully" is displayed.

Caution Remove the DVD from the DVD drive after the installation/upgrade is complete. Leaving the DVD in the drive can prevent Cisco TelePresence Manager from restarting properly after rebooting the server.

Installation Page Values Defined

Table 7-3 explains in detail the window and field definitions of the Cisco TelePresence Manager installation process in detail.

Table 7-3 Installation Window and field Definitions

Installation Windows and Fields	Description and Usage
Installation Wizard	
Proceed:	The installation wizard requests necessary configuration information before installing CTS-Manager files.
Skip:	Skip this wizard and install CTS-Manager files without configuration information. After the files are installed and the system reboots, the installation program will request configuration information.
Cancel:	Cancel this installation.
Autonegotiation Window Configuration	
NIC Speed	The speed of the server network interface card (NIC), in megabits per second. • The possible speeds are 10, 100, and 1000 mbps. **Default is 100 mbps**. **Note** Cisco recommends a NIC speed of at least 100 mbps for best performance.
Duplex Configuration	The duplex setting of the server NIC. • The possible settings are Half and Full. **Default is Full**. **Note** Cisco recommends full duplex for best performance.
DHCP Configuration Window and Fields	
Host Name	A hostname is an alias that is assigned to an IP address to help identify it. • Enter a hostname that is unique to your network. • The hostname can consist of up to 64 characters and can contain alphanumeric characters and hyphens.
IP Address	The IP address uniquely identifies a server on your network. • Enter the IP address in the form *ddd.ddd.ddd.ddd*, where *ddd* can have a value from 0 to 255 (except 0.0.0.0).

Table 7-3 Installation Window and field Definitions (continued)

Installation Windows and Fields	Description and Usage
IP Mask	The IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address. • Enter the IP mask in the form *ddd.ddd.ddd.ddd,* where *ddd* can have a value from 0 to 255 (except 0.0.0.0). Valid example: 255.255.240.0. Invalid example: 255.255.240.240.
GW Address	GW Address are for static configurations. A network point that acts as an entrance to another network. Outbound packets are sent to the gateway that will forward them to their final destination. • Enter the IP address of the gateway in the format *ddd.ddd.ddd.ddd,* where *ddd* can have a value from 0 to 255 (except 0.0.0.0). **Note** If you do not have a gateway, you must still fill in this field by setting it to 255.255.255.255. Not having a gateway may limit you to communicating only with devices on your subnet.
DNS Client Configuration	You will be prompted to enter DNS server information. A DNS server is a device that resolves a hostname into an IP address or an IP address into a hostname. • If you do not have a DNS server, choose **No**. When DNS is disabled, you should enter only IP addresses (not hostnames) for all network devices in your CTS-Manager network. **Note** If you have a DNS server, Cisco recommends choosing **Yes** to enable DNS. Disabling DNS limits the system's ability to resolve some domain names.
Primary DNS	CTS-Manager contacts this DNS server first when attempting to resolve hostnames. This field is mandatory if DNS is set to **yes**.
Secondary DNS (optional)	When a primary DNS server fails, CTS-Manager will attempt to connect to the secondary DNS server. • Enter the IP address in dotted decimal format as *ddd.ddd.ddd.ddd,* where *ddd* can have a value from 0 to 255 (except 0.0.0.0).
Domain	A sequence of case-insensitive ASCII labels separated by dots (for example, "cisco.com")—defined for subtrees in the Internet Domain Name System and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.

Table 7-3 Installation Window and field Definitions (continued)

Installation Windows and Fields	Description and Usage
Administrative Login Configuration	
Admin ID	The username for the CTS-Manager Administrator. This is the administrator login that includes superuser permissions. • Ensure that the name is unique. It is recommended to start with a lowercase alphanumeric character and can contain alphanumeric characters (uppercase and lowercase), hyphens, and underscores. ⚠ **Caution** The admin ID cannot be changed after installation without reinstalling CTS-Manager. Record it for safekeeping.
Password / Confirm	A password that allows the administrator to log into CTS-Manager. • The password must be at least six characters long and maximum of 31 characters. It is recommended to start with a lowercase alphanumeric character, using English characters only. International characters are not supported in this version. This field can be changed at Cisco TelePresence Manager web interface. Record it for safekeeping. **Recovering Administrator and Security Passwords** If you lose the administrator password or security password, two different procedures can be followed to reset these passwords. These procedures are in the section following this table.
Certificate Signing Request Configuration	A certificate signing request (CSR) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. • These values create a CSR for the server where the certificate will be installed.
Organization	Your company or organization name.
Unit	Your business unit, group, or organizational unit name.
Location	The physical location of the organization, most often a city.
State	The region, state, province, or other region where the organization resides.
Country	Your company or organization country of record.
Network Time Protocol Client Configuration	NTP is used to synchronize the clocks on Cisco IP telephony servers with an external network time server that uses NTP.
NTP Server 1	Enter the hostname or IP address of one or more NTP server.
NTP Servers 2–5	• NTP Server 1 value is mandatory; NTP Servers 2–5 are optional. **Tip** Cisco strongly recommends that you enter the NTP server by which Cisco Unified CM synchronizes its clock as the primary NTP server. If these servers are out of synchronization, CTS-Manager will not operate properly.
Database Access Security Configuration	Cisco TelePresence Manager uses the security password to communicate with its database.
Security Password / Confirm	• The password must be at least six characters long and a maximum of 31 characters. It is recommended to start with a lowercase alphanumeric character., using English characters only.

Recovering Administrator and Security Passwords

If you lose the administrator password or security password, two different procedures can be followed to reset these passwords.

Note During this procedure, you must remove and then insert a valid DVD in the disk drive to prove that you have physical access to the system.

Recovery procedure 1:

Step 1 Log in to the system with the following username and password:

Username: **pwrecovery**

Password: **pwreset**

Step 2 The Welcome to platform password reset window displays.

Step 3 Press any key to continue.

Step 4 If you have a DVD in the disk drive, remove it now.

Step 5 Press any key to continue. The system tests to ensure that you have removed the DVD from the disk drive.

Step 6 Insert a valid DVD into the disk drive. The system tests to ensure that you have inserted the disk.

Step 7 After the system verifies that you have inserted the disk, you see a prompt to enter one of the following options:

a. Enter **a** to reset the administrator password.

b. Enter **s** to reset the security password.

c. Enter **q** to quit.

Step 8 Enter a new password of the type that you chose.

Step 9 Reenter the new password.

Step 10 After the system verifies the strength of the new password, the password gets reset, and you're prompted to press any key to exit the password reset utility.

Recovery procedure 2:

If your password is lost, reinstall Cisco TelePresence Manager to regain access.

System Log Error Detection

When a problem is detected, you must collect system errors and logs files so they can be analyzed for prompt resolution

System Log

Choose the System Log window to see a list of system messages. You can filter the list by starting and ending dates and message type All, Fatal, Severe, Moderate, Warning, and Info, as follows:

- Use the Calendar icon to choose dates, or type the dates in the **Start On** and **End On** fields using the MM/DD/YYYY date format.
- Click **Filter** to generate the list.

Figure 7-1 System Log Window

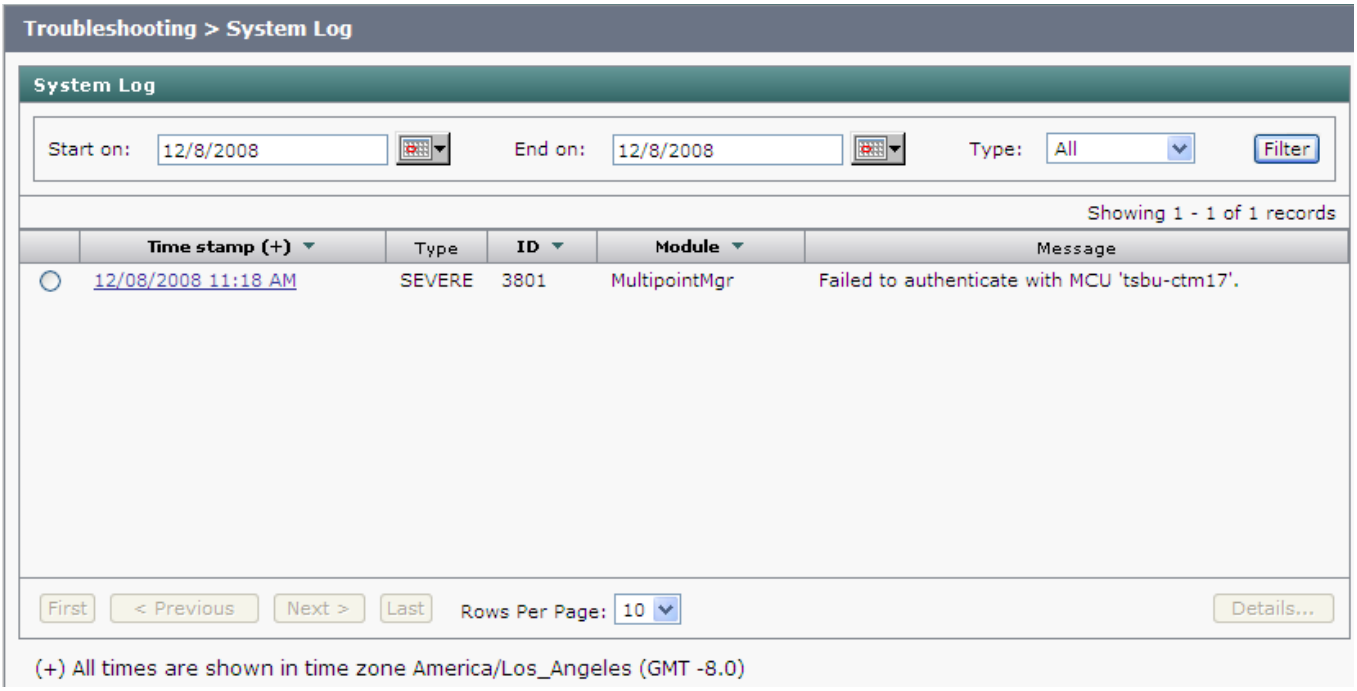


Table 7-4 lists the error information provided by the system.

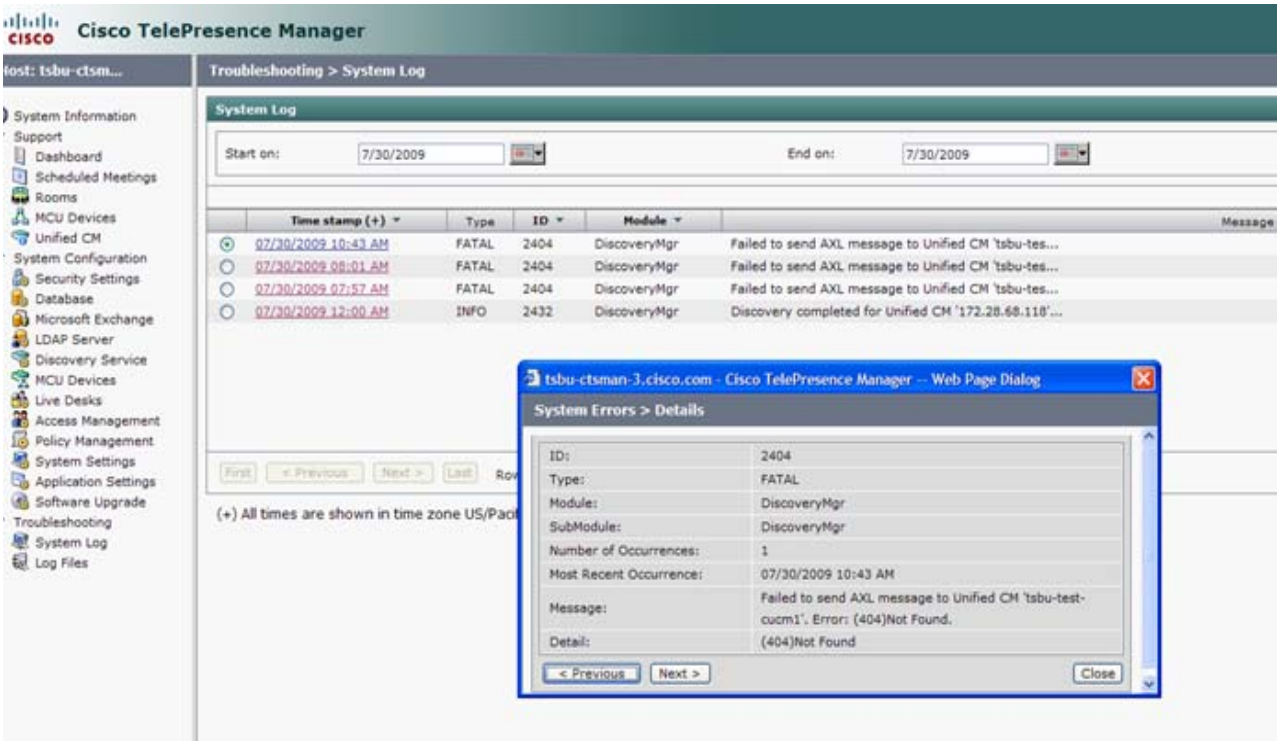
Table 7-4 System Error Report

Field	Description
Timestamp	Date and time the message was logged. You can sort the messages in ascending or descending order by the time stamp.
Type	Message type.
ID	Message identification number. You can sort the reports in ascending or descending order by ID.
Module	Component within CTS-Manager that generated the error.
Message	Explanation of problem detected. Move your mouse pointer over a message field to see a complete description.

System Error - AXL Error or Invalid Credential

If the System Errors>Details message in the Syslog appears as seen in Figure 7-2, or the Invalid Credentials message appears when testing connections, the user should make sure that all the required services are running. Also, the user may need to refer to Chapter 5, "Configuring Cisco Unified CM for Cisco TelePresence Manager" to review what services need to be running on the Cisco UCM for CTS-Manager.

Figure 7-2 System Log - System AXL Error Message

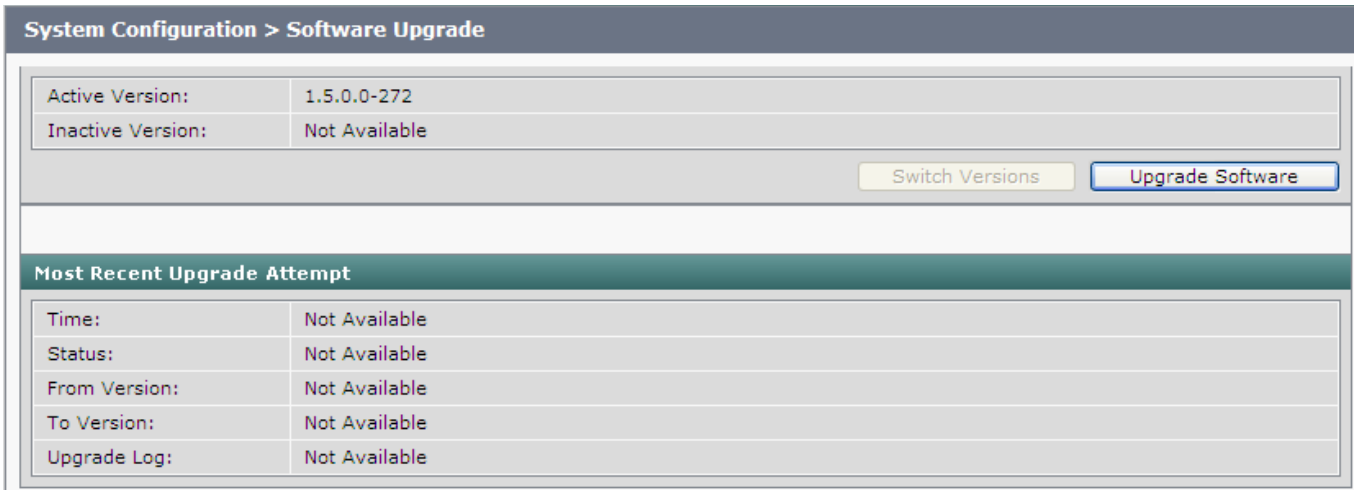


If it is necessary to drill down further into error data, go to the Log files. For further information about Log details, go to Chapter 13, "Troubleshooting Cisco TelePresence Manager"

Software Upgrade

If you are the system administrator and know the superuser password, you can access the Software Upgrade window to monitor and maintain system software. This window reports the version number of the system software. There are also two buttons to assist you in version maintenance between primary and backup and upgrading the system software, as follows:

Figure 7-3 System Configuration - Software Upgrade Window



- Switch Version—The hard drive on the server on which this CTS-Manager is installed is partitioned into two areas. Each area can contain a system image. The **Switch Version** button allows you to switch between the Active and Inactive versions of the system software.
- Upgrade Software—This button loads a patch file for upgrading system software. The Cisco-supplied patch file can be stored on a CD-ROM or a Secure FTP (SFTP) host network. A wizard displays dialog boxes to prompt you through the process.
  In addition to SFTP, FTP is also supported on a best-effort basis due to variations of behavior between different FTP servers. Only username/password-based login is supported. Anonymous login is not supported.
  Secure FTP (SFTP) is the recommended mode for downloading the upgrade software over the network.

Upgrading to Cisco TelePresence Manager 1.6

Switching calendar application type, e.g. changing from Exchange to Domino, during Cisco TelePresence Manager upgrade is not supported. A fresh install is required to install Cisco TelePresence Manager for Domino deployment.

- Software upgrade is only supported from CTS-Manager 1.4 or 1.5 to 1.6.
- Data are automatically migrated during software upgrade, with the exceptions of:
  - custom email templates
  - log files
- Perform a backup before performing a CTS-Manager upgrade and another backup after upgrade is completed and verified.
- If for any reason you must revert to a previous release after the upgrade is completed, you can switch to the old partition from CTS-Manager.

Note In rare instances, upgrades could take up to 5 hours or more - do not think the system is frozen during upgrades - do not reboot.

Switch Version

The hard drive on the CTS-Manager server is divided into two partitions. CTS-Manager is always using the Active partition and contains the Active software version. The software image versions are identified in the System Configuration> Software Upgrade window.

You may find it necessary to switch the version of the CTS-Manager software.

- To switch between the two software versions stored in the partitions, click the **Switch Version** button.

The system will swap the software versions and reboot. Screens will describe activity.

Upgrade Software

This task upgrades the CTS-Manager software by loading and applying a patch file from either a CD-ROM or an SFTP/FTP host network. Before starting this task, determine the source of the patch file.

- To start the software upgrade process, click the **Upgrade Software** button.
  The Source Selection dialog box appears.

Note Once you have launched the Upgrade Wizard the upgrade process cannot be started by any other user logged into the same Cisco TelePresence Manager server.

- Click the **CD-ROM** or **Network** radio button to choose the location of the patch file.

  If you chose CD-ROM, click **Next** to go to the File Selection window.

  If you chose Network, provide the following information, and then click **Next** to go to the File Selection window.

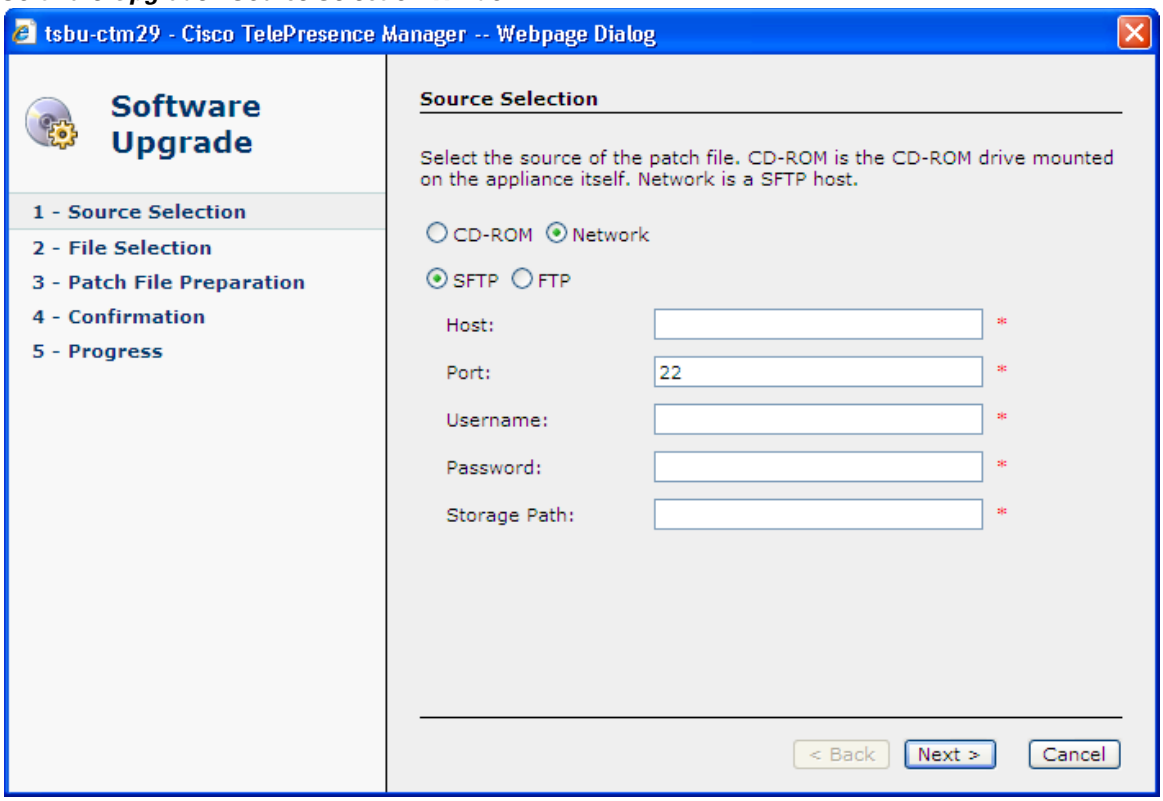
  - **Host**—The hostname of the network server.
  - **Port**—The port. By default, port 22 is used to access the server; supply the correct port number, if required.

  Note If you choose to perform the software upgrade using FTP you do not need to supply a port number.

  - **Username and Password**—The user account and password needed to log into the server.
  - **Storage Path**—The file path to the patch file, e.g. */localview/ctm_patch*

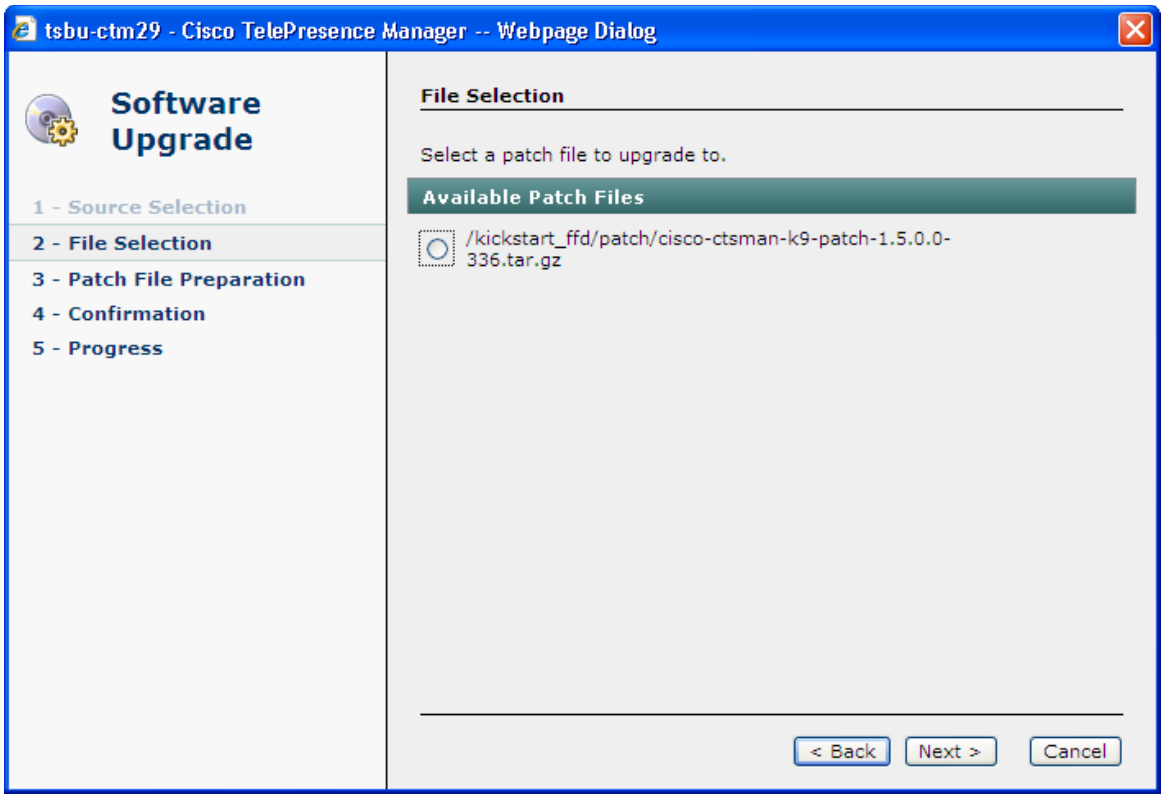
Caution Perform FTP for Upgrade, Backup and Restore on a best-effort basis, due to potential variations in the responses sent by the FTP server. Only username/password-based login is supported. Anonymous login is not supported.
Secure FTP (SFTP) is the recommended mode of transferring files over the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

Figure 7-4 Software Upgrade - Source Selection Window



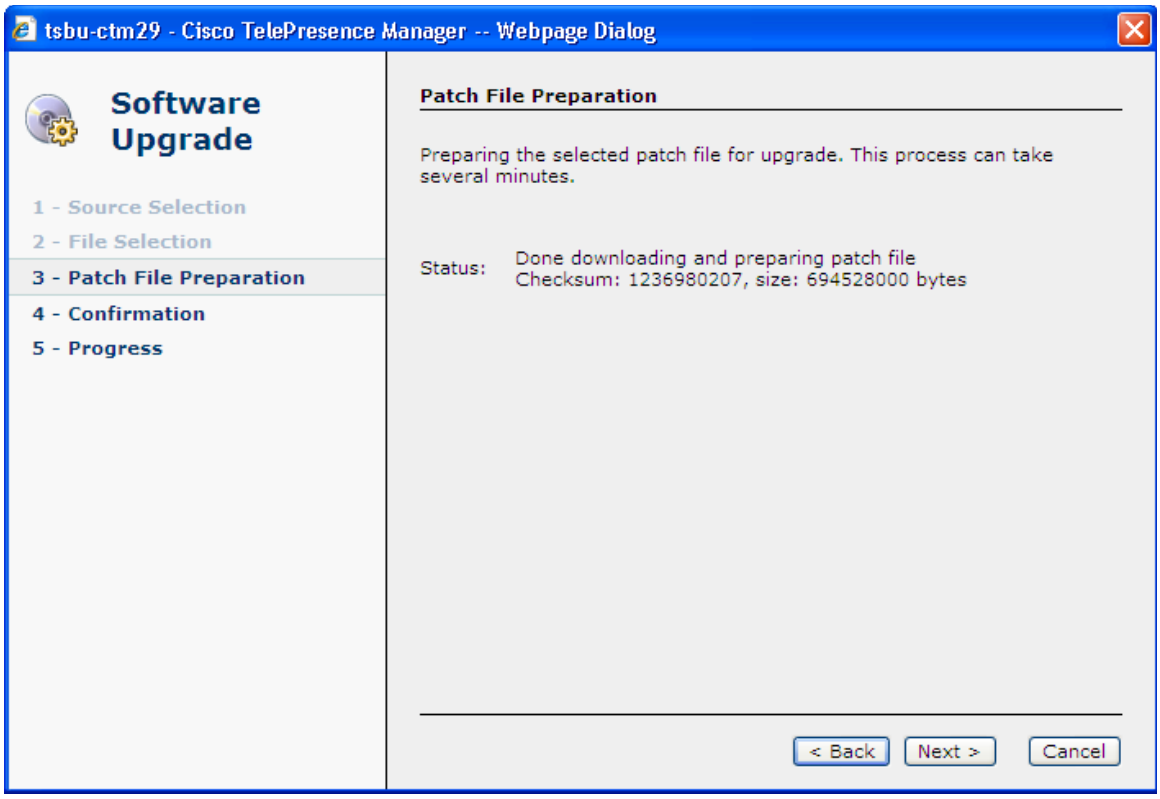
- At the File Selection window, choose the file to load by clicking its radio button. Then click **Next**.

Figure 7-5 Software Upgrade - File Selection window



- The Patch File Preparation window appears. Watch this window to monitor the progress of the file download. Buttons will be inactive until the patch file is loaded.

Figure 7-6 Software Upgrade - Patch File Preparation Window

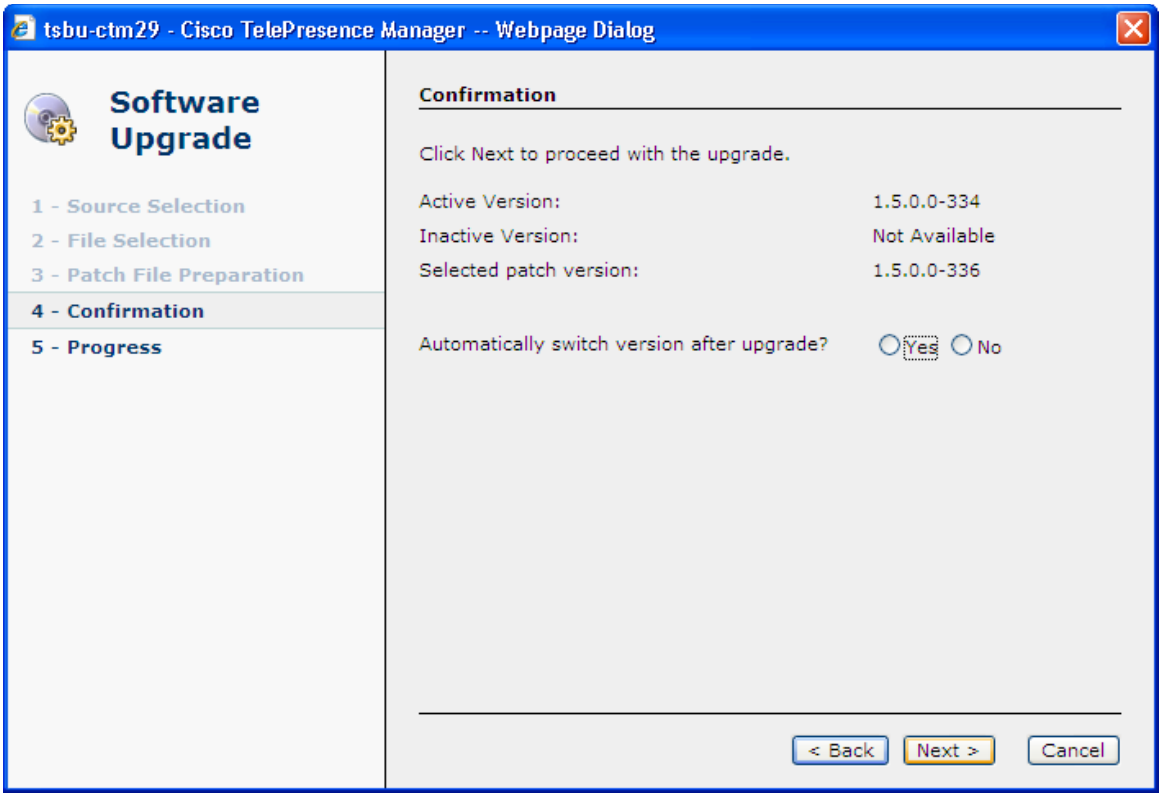


- Once the file is loaded, the window displays a Confirmation message.

  The software wizard displays the software versions that are installed and provides active Yes and No radio buttons so you can choose to switch the newly loaded software to the active partition.

  - Click **Yes** or **No** to make your choice. Then click **Next** to finish the software upgrade task.

Figure 7-7 Software Upgrade - Confirmation Window

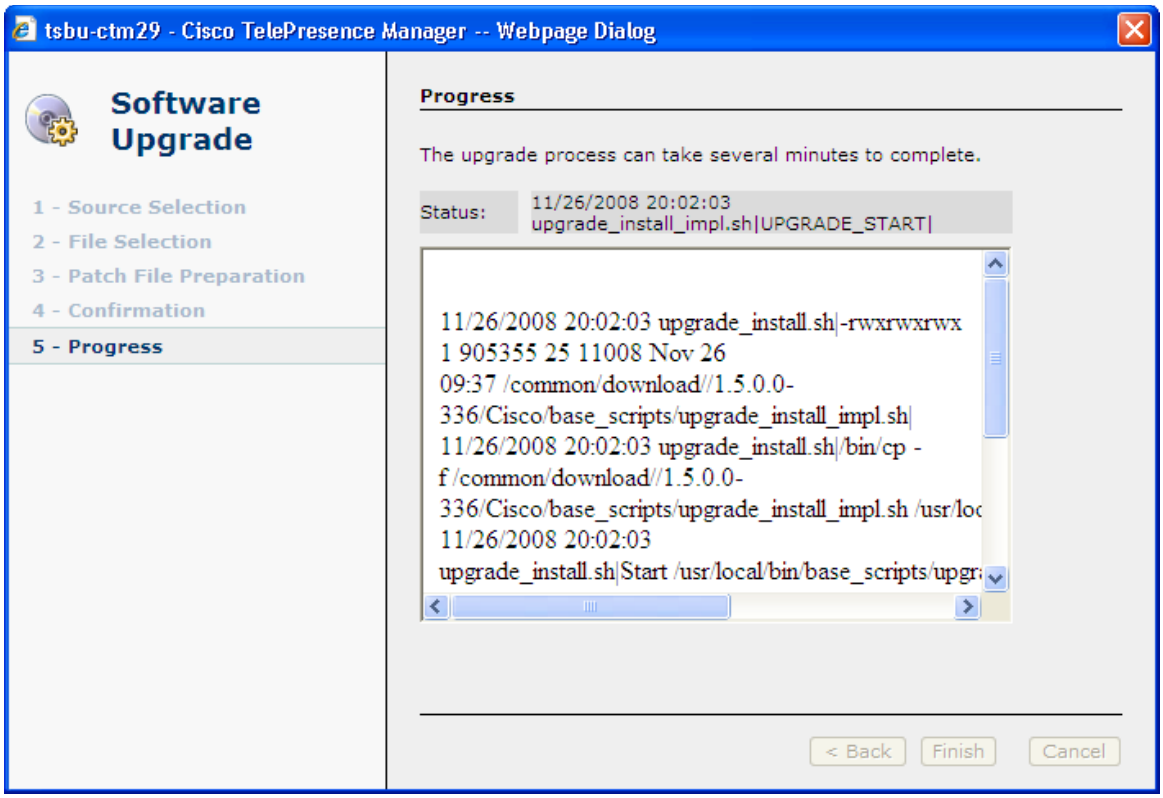


Note When you click **Yes** , you can still cancel the upgrade.

Caution Once you click **Next** to confirm, you cannot cancel the upgrade.

The install wizard displays a dialog window that logs the progress of the update.

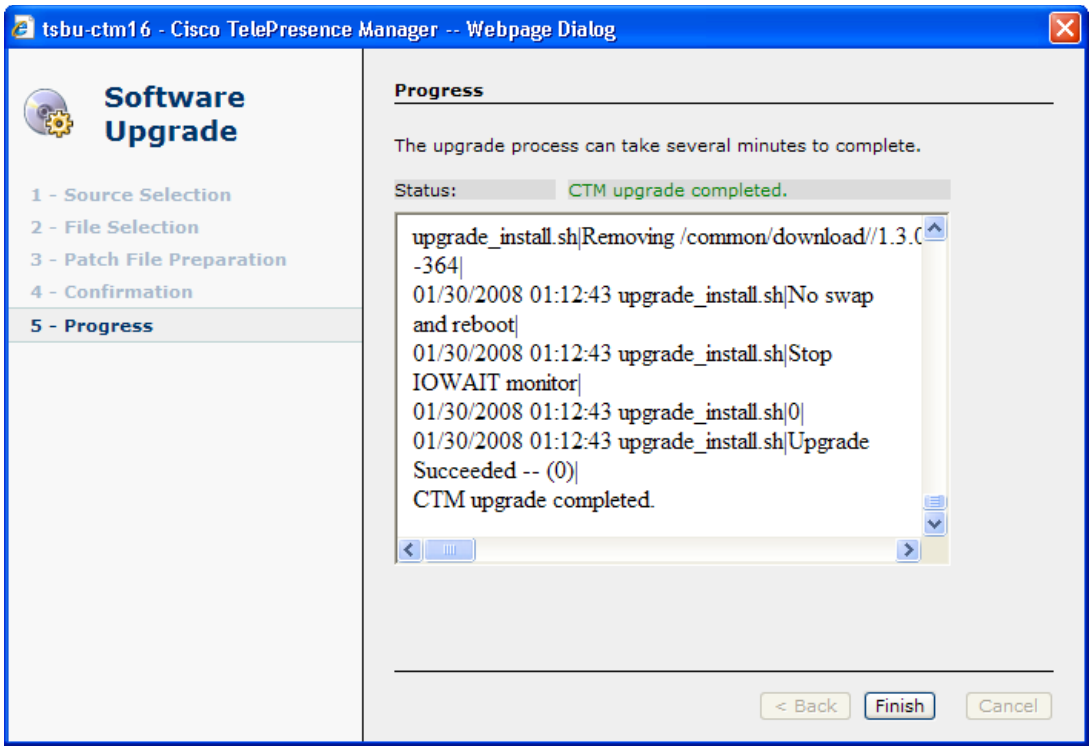
Figure 7-8 Software Upgrade - Progress Window



- When the log indicates that the files have been switched, click **Finish** to complete this task.

Note If you selected to automatically switch to the new version, a message is displayed letting you know there is no connectivity to the server during the switch.

Figure 7-9 Software Upgrade - CTM Upgrade Completed Window



Cisco TelePresence Manager Window

The Cisco TelePresence Manager window is divided into several panes with different functionality.

Header Pane

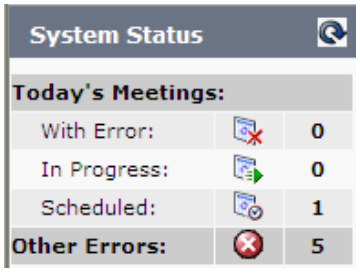
Figure 7-10 Cisco TelePresence Manager Header Pane

A header at the top of all CTS-Manager windows shows either “admin” or the login name of the concierge currently logged in and provides four links:

- **Logout**—Click to log out of the system.
- **Preferences**—Click to display the Browser’s location information.
- **Help**—Click to display online help for using the CTS-Manager.
- **About**—Click to display licensing information.

System Status Pane

Figure 7-11 System Status Pane



System Status is always in view in the lower left corner of the CTS-Manager window. Both the concierge and the administrator must closely monitor this area for notification of system errors and changes in the status of today's meetings.

The icons and numbers are links. They will take you to a window in the CTS-Manager that helps you identify problems for the With Error state or see more information about meetings in the In Progress and Scheduled states.

The following meeting states are displayed for Today's Meetings:

- With Error
- In Progress
- Scheduled

The Other Errors area displays a cumulative number of errors listed in the Dashboard.

Navigation Pane

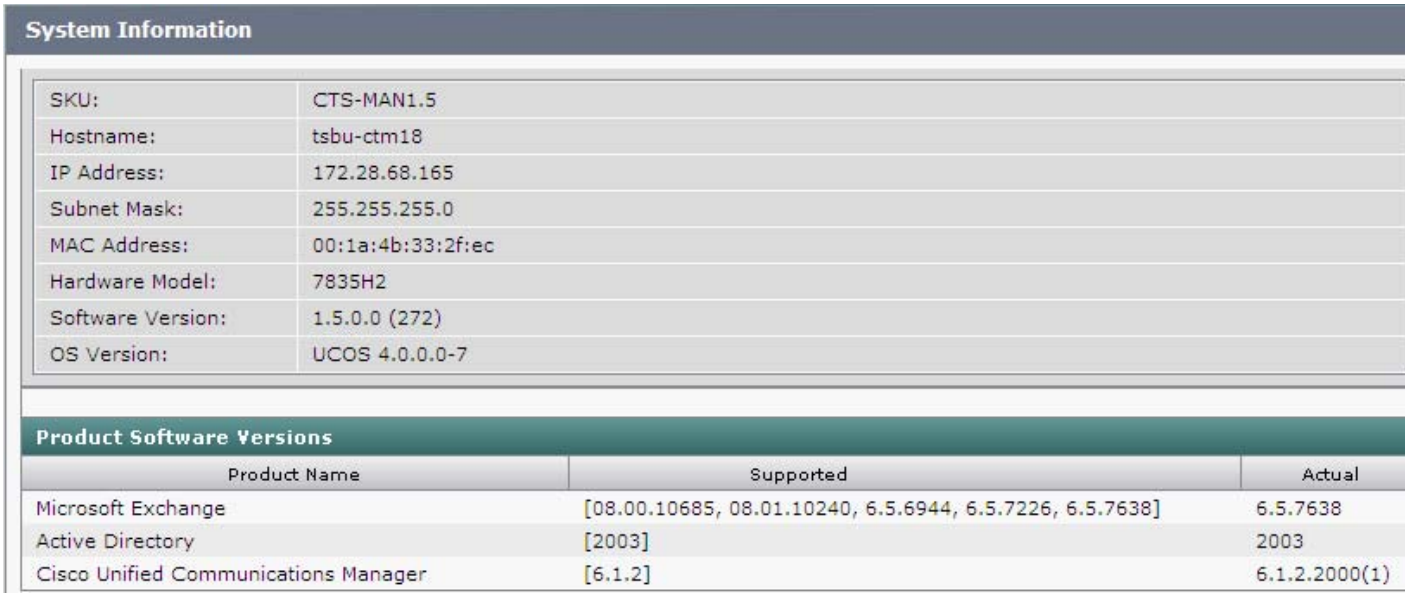
Figure 7-12 Navigation Pane

The navigation pane contains the list of commands you can run within Cisco TelePresence Manager. The commands are divided into three drop-down lists:

- **Support** — This drop-down list contains commands available to a Concierge, Administrator, or Superuser.
- **System Configuration** — This drop-down list contains commands available to an Administrator or Superuser. If you log in as a Superuser the System Settings and Software Upgrade commands are included in the list.
- **Troubleshooting** — This drop-down list contains commands available to an Administrator or Superuser.

Work Pane

Figure 7-13 Work Pane



The frame to the right of the Navigation pane is the content area. The gray bar above the content area shows the navigational path so you can see where you are at any time.

The following sections describe objects, functions, and information displayed in the Work pane associated with a specific command.

Tabs

Some windows have tabs that you click to display additional functionality related to a command.

Filtering Information

Some windows provide fields where you can enter criteria to filter the information contained is a report. Click the Filter button to display the reports using the criteria you specify. The settings are temporary; when you exit the page, the criteria are removed.

Obtaining Additional Information and Help

To access additional information or relevant windows, click a highlighted link.

Navigating Long Lists

When there is a long list of data in a window, you can navigate through it using Next, Last, First, and Previous buttons at the bottom of the window. The Rows Per Page drop-down list also found at the bottom of the window can be used to change the number of rows displayed. Choose 10, 20, 50, or 100 rows per page. The setting is temporary, and when you exit the page the default setting is restored.

Copying and Pasting Information

You can place information displayed by the CTS-Manager in a file using standard copy-and-paste functions.

Typing Information in Fields

For information provided in fields, use the mouse to highlight and delete existing information. Type in new information.

New or modified information is applied using the Apply button.

To back out of changes and return to original settings, use the Reset button.

Typing Telephone Numbers

Telephone numbers must be entered into CTS-Manager fields exactly as they will be dialed by the IP phone. For example, if you need to dial 9 to get an outside telephone line and you are calling a different area code or international dialing code, you must provide all the required numbers to the CTS-Manager in the exact sequence in which they should be dialed. The following is an example: **`915105550100`**.

Typing Meeting Room Names

The names of meeting rooms must be typed into CTS-Manager fields exactly as they are stored in your Microsoft Exchange, or IBM Domino database. If a room is listed as **`M-Room 1/3 at Main`** in the Microsoft Outlook or Lotus Notes list of resources, that name must be typed exactly the same way in the CTS-Manager. Otherwise, the system will not be able to match records and an error occurs.

Viewing All Information

Sometimes only a portion of text is visible and is completed by ellipses. You can see the full text in a tooltip by slowly passing the mouse pointer over the partial text. You can do this in any field in the user interface where text is cut off.

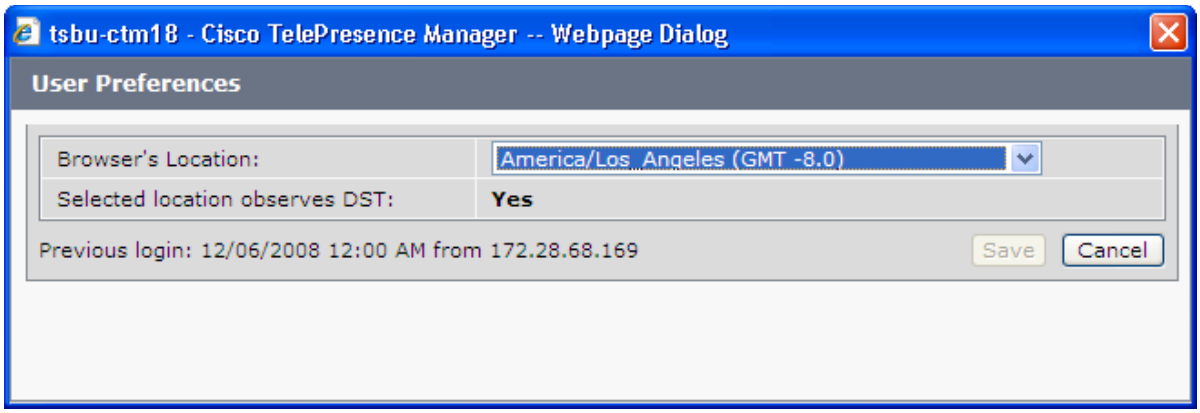
Preferences

Clicking Preferences in the header pane displays the Preferences window.

Figure 7-14 Preferences Link in the Header Pane

The first time you login you need to specify the timezone you are in. This localizes Cisco TelePresence Manager's meeting times to your location. You can use the Preferences window to change the timezone.

Figure 7-15 Preferences window



CHAPTER 8

Initializing Cisco TelePresence Manager

Revised: January 28, 2010, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

After installing the Cisco TelePresence Manager, the next step is to initialize the program.

The next process is initializing Cisco TelePresence Manager to enable access to information sources such as Microsoft Exchange Server for meeting requests from Microsoft Outlook, Active Directory for accessing user and conference room information, and Cisco Unified Communications Manager for conference room availability and telephone support.

The tasks for initializing the Cisco TelePresence Manager are described in the following sections.

Post-Install Guidelines for CTS-Manager

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

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

Table 8-1 Post-Install Procedure Guidelines for setting up CTS-Manager

Set-Up Procedure Guidelines after Installing CTS-Manager	Description	Location
Initializing CTS-Manager	After installing the CTS-Manager software, the next process is initializing Cisco TelePresence Manager to enable access to information sources such as Microsoft Exchange Server for meeting requests from Microsoft Outlook, Active Directory for accessing user and conference room information, and Cisco Unified Communications Manager for conference room availability and telephone support	Current Chapter

Set-Up Procedure Guidelines after Installing CTS-Manager	Description	Location
Additional Configuration 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 reconfigure system settings	Chapter 10, "Monitoring Cisco TelePresence Manager"
Email and Meeting Action Requirements	The Calendar service (either Microsoft Exchange or IBM Domino) sends an acceptance email to the meeting organizer, with the notice that the rooms have been reserved and placed on the calendar. CTS-Manager also sends either a Confirmation email or an Action Required email to the meeting organizer when a meeting is scheduled	Chapter 11, "CTS-Manager Emails and End-User Web UI"

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

Initializing Cisco TelePresence Manager After Installation

This section contains the following topics pertaining to initialization:

To initialize Cisco TelePresence Manager, you must enter contact and access information for your Microsoft Exchange Server, Lightweight Directory Access Protocol (LDAP) server, and Cisco Unified CM in a series of one-time-only, post-installation initialization windows.

Required Information and Equipment

To set up and initialize Cisco TelePresence Manager, you need the information previously entered or created during pre-installation.

Additionally, Cisco TelePresence Manager must have network access to a computer running Windows Explorer version 6.1.3, Microsoft Exchange Server and Active Directory, (set to level 2) server, Microsoft EWS server, or IBM Domino Server and Domino Directory Server, and Cisco Unified Communications Manager.

Initialization Procedure

The system administrator can access and change the information after initialization from the Configuration tab of the Cisco TelePresence Manager web interface.

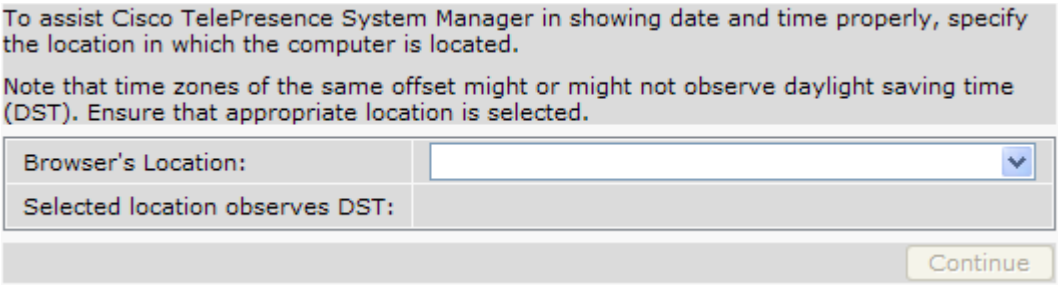
Initialization for Microsoft Exchange Deployments

Step 1 At the console running Microsoft Explorer, type the Cisco TelePresence Manager server name or the IP address. See the following example.

```
https:// server hostname or IP address
```

Step 2 The Initial Preferences window is displayed. Choose the timezone from the drop-down menu. The timezone you choose should be the one you are located in. Click **Continue**.

Figure 8-1 Initial Preferences Window



Step 3 At the product page that appears, click on **Cisco TelePresence Manager**.

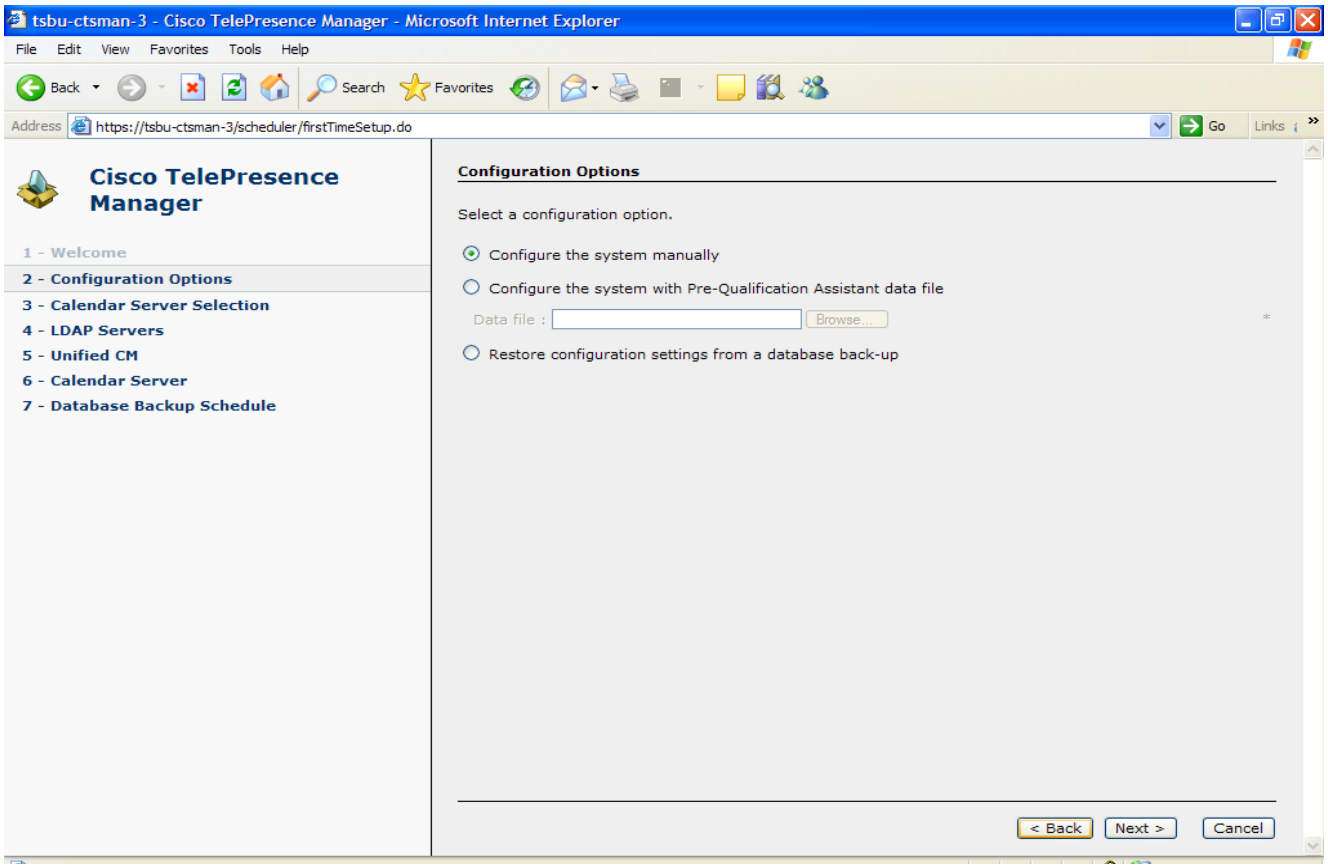
Step 4 At the login page, enter the username and password created during installation.

The Cisco TelePresence Manager initial window appears with several fields already populated from the installation process.

CTS-Manager Configuration Options

The initial window to open is the Configuration Options window. This window allows you to configure the system manually or to restore the configuration settings from a database back-up.

Figure 8-2 Configuration Options Window



This windows offers three options for configuring your CTS-Manager:

- Configure the system manually
- Configure the system with the Pre-Qualification Assistant data
- Restore configuration settings from a database back-up.

Configure the System Manually

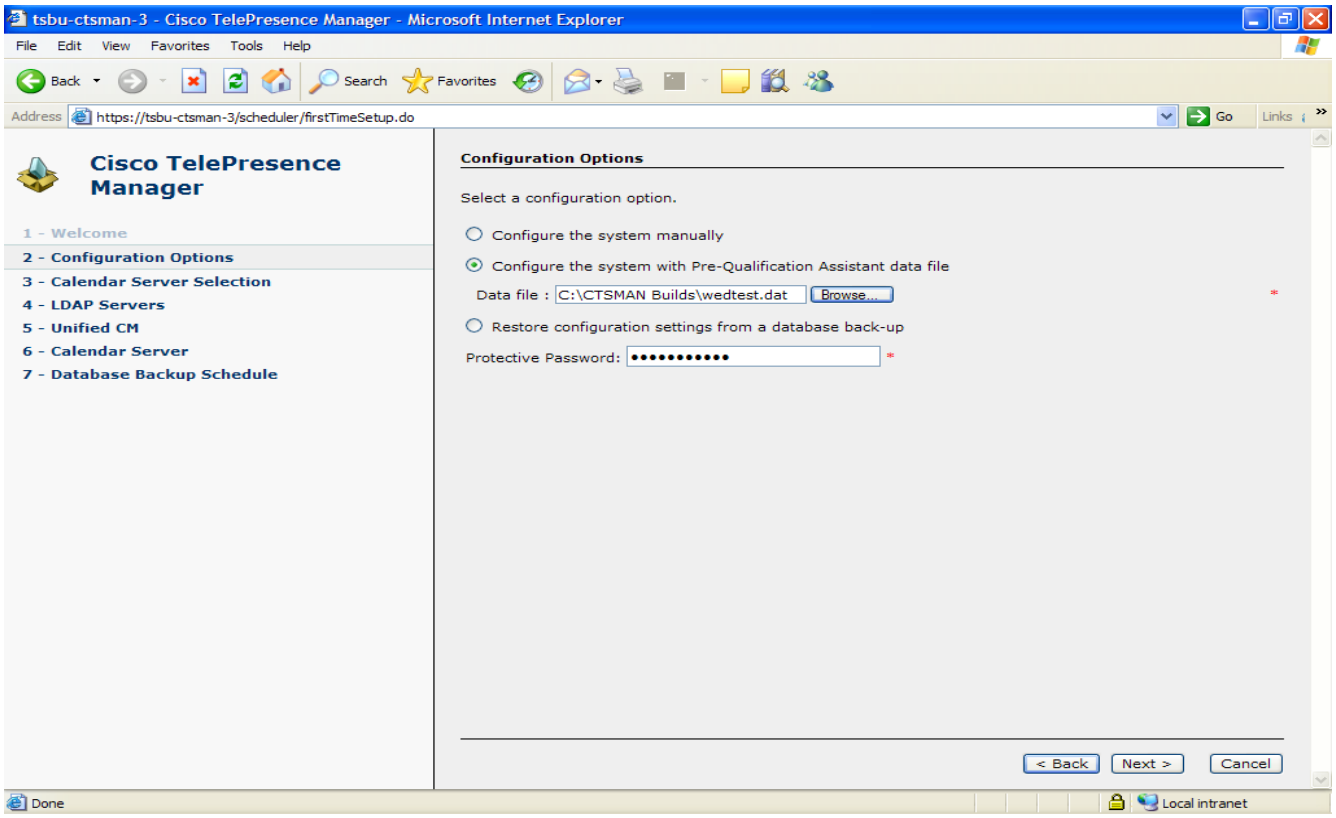
This option allows you to set up your configurations for a First Time Setup. You are not able to do a restore or use the Pre-Qualification data files.

You will have to add the server information in all the screens.

Configure the system with Pre-Qualification Assistant Data File

If selecting the FTS using the Pre-Qualification data, this option allows you to select the data file that you have previously set up. Refer to Chapter 6, "Installing and Configuring Cisco PreQualification Assistant"

Figure 8-3 FTS Configuration Option - Pre-Qualification



Step 1 Use the Browse button to find the location of the data file and select it.

Step 2 Put in your admin or superuser password.

Step 3 Click **Next**.

Note If this option is selected, it is necessary to test the LDAP servers connections through the Pre-Qualification Assistant tool.

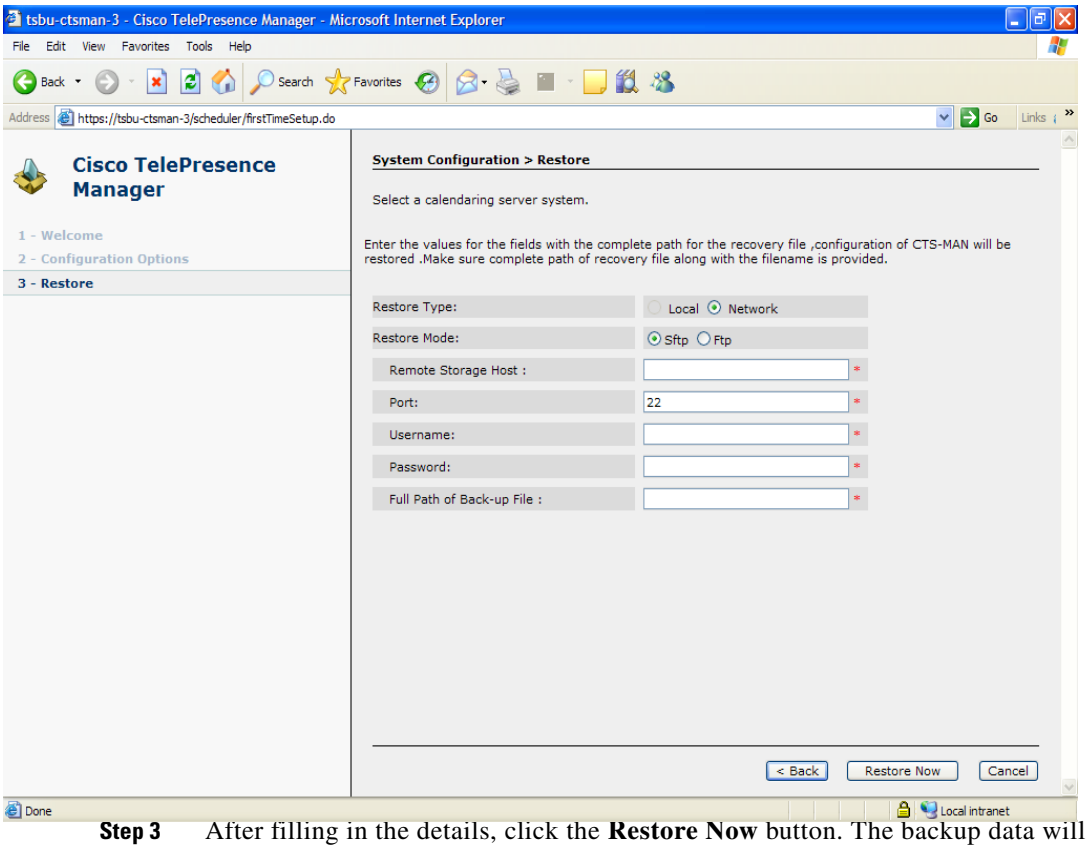
Restore Configuration Settings from a Database Back-up

If selecting the FTS using the restore option, this option allows you to select the data that you have previously backed up. Refer to Chapter 9, "Additional Installation Configurations for Cisco TelePresence Manager", section, Database - Status, Backup, and Restore for further details on backing up your system database.

Step 1 Select the **Restore** configuration settings from a database back-up option. Click on the **Next** button.

Step 2 The System Configuration>Restore window appears. This window is where you need to fill in the fields of the path of the recovery file and the file name.

Figure 8-4 FTS Configuration - Restore Window



Step 3 After filling in the details, click the **Restore Now** button. The backup data will be restored to the CTS-Manager system.

After selecting the configuration option and setting up the data, the next step is to set up the Calendar server option.

Calendar Server Option

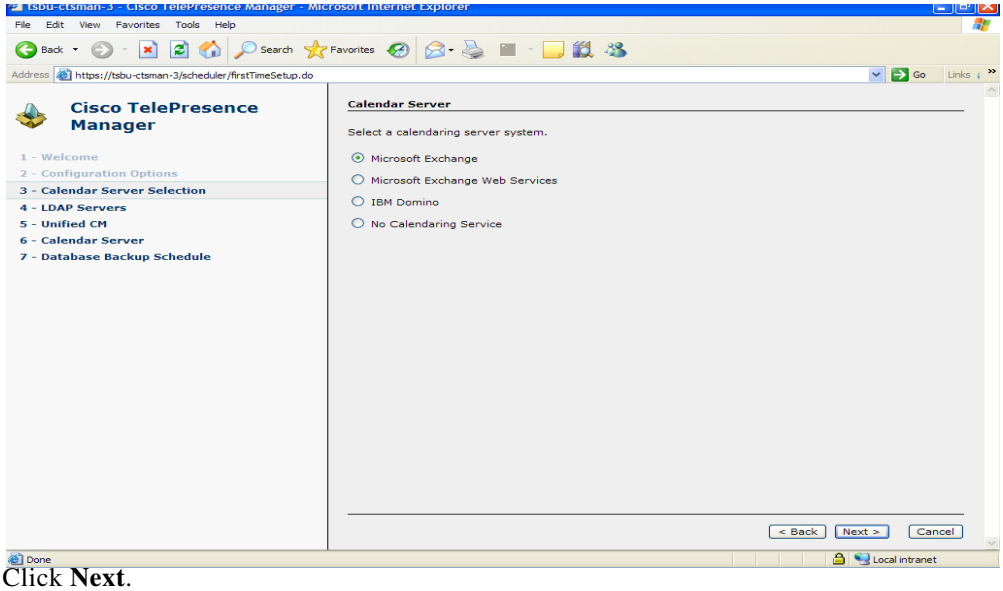
The Calendar Server Selection allows you to select the calendaring server for your system. The options are:

- Microsoft Exchange
- Microsoft Exchange Web Services (EWS)
- IBM Domino
- No Calendering Service

Step 1 The Calendar Server Selection window is displayed. See Figure 8-5.

Choose Microsoft Exchange for this deployment and click **Next**.

Figure 8-5 Calendar Server Selection Window



Step 2 Click **Next**.

Step 3 The LDAP Servers window opens. See Figure 8-6.

Verifying the LDAP Servers Configuration

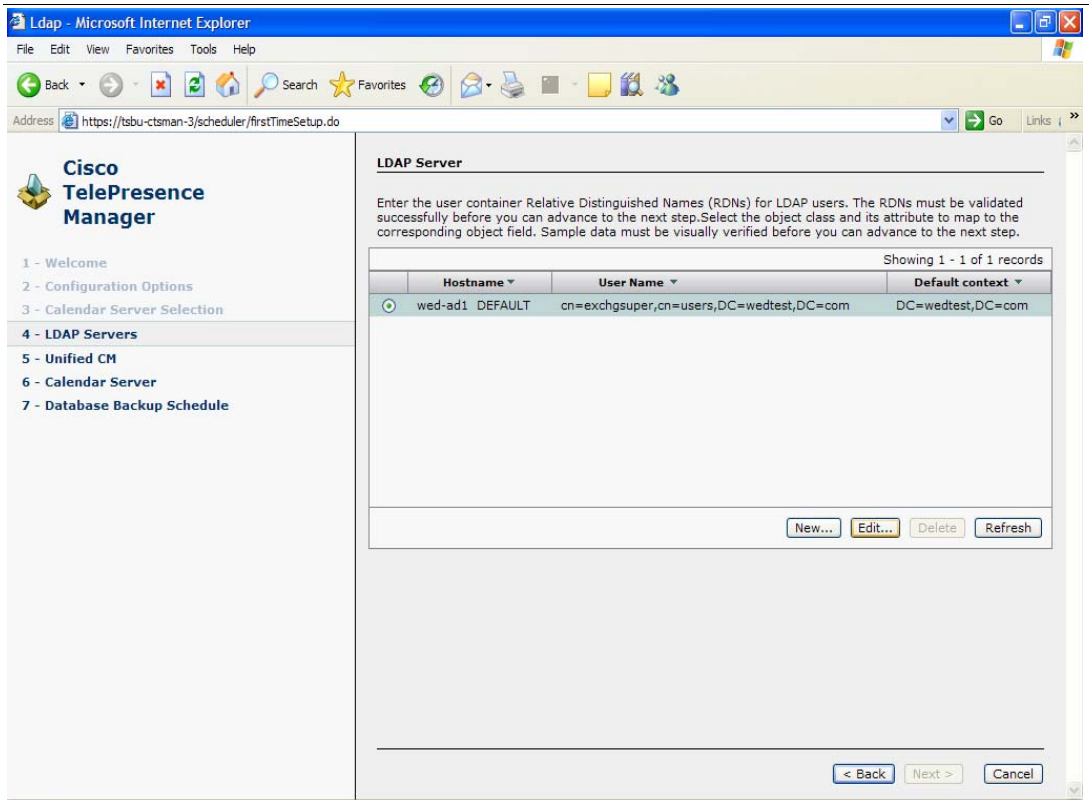
Lightweight Directory Access Protocol (LDAP) is a protocol definition for accessing directories. This window provides you with the records of the LDAP servers that have been set up. To add new ones or to edit the one listed, select the record that is listed, then click either the **New** or **Edit** button. For more information about setting up servers, refer to Chapter 9, "Additional Installation Configurations for Cisco TelePresence Manager"

If you have selected the Configure the system with Pre-Qualification Assistant data file option, you must select the server record and click on Edit. The next window that appears gives you the setup information, you must test the connection. You have to do this with all the LDAP servers that you have configured before you can select the Next button.

In the LDAP server window example Figure 8-6, it shows one record.

Figure 8-6 LDAP Servers Window

Note



Step 1 Select the first listed record, then click on **Edit**. Or, if adding a new one click **New**.

Step 2 When the popup window LDAP Server Settings appears, make sure the information is correct. For further information, refer to Chapter 9, Settings for LDAP. If necessary, make changes in the fields. If this is a new server, put in the information in all the fields.

Click on **Test Connection** button.

- The system tests the connection information. A popup window opens and displays the message "Connection to <....> Server was Verified." Click **OK**, then click **Next**.

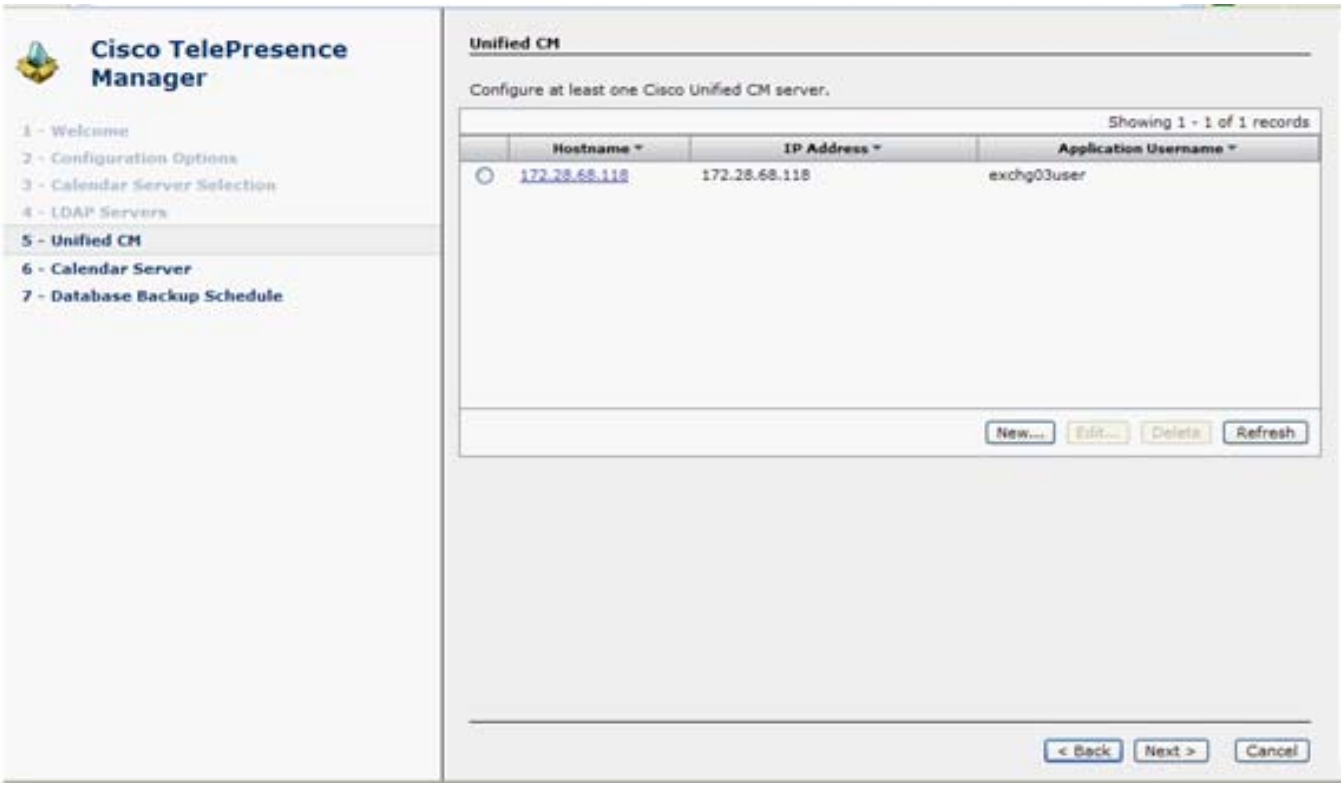
Step 3 The LDAP Server window re-appears. If you have more records to test, repeat Step 1 through Step 3.

Step 4 If all the server settings have been tested, click the **Next** button.

Cisco Unified Call Manager (CUCM) Server Configuration

This window allows you to review the CUCM server(s) that was configured and verify the set up through the Pre-Qualification Assistant.

Figure 8-7 Cisco Unified CM Configuration Window



Verifying the Cisco Unified Communications Manager Configuration

Step 1 Select the first listed record, then click on **Edit**. Or, if adding a new one, click **New**.

Step 2 When the popup window CUCM Server Settings appears, make sure the information is correct. For further information, refer to Chapter 9, Settings for CUCM. If necessary, make changes in this window.

- Click on **Test Connection** button. The system tests the connection information. A popup window opens and displays the message "Connection to <....> Server was Verified." Click **OK**, then click **Next**.

Step 3 The CUCM Server window re-appears. If you have more records to test, repeat Step 1 through Step 3.

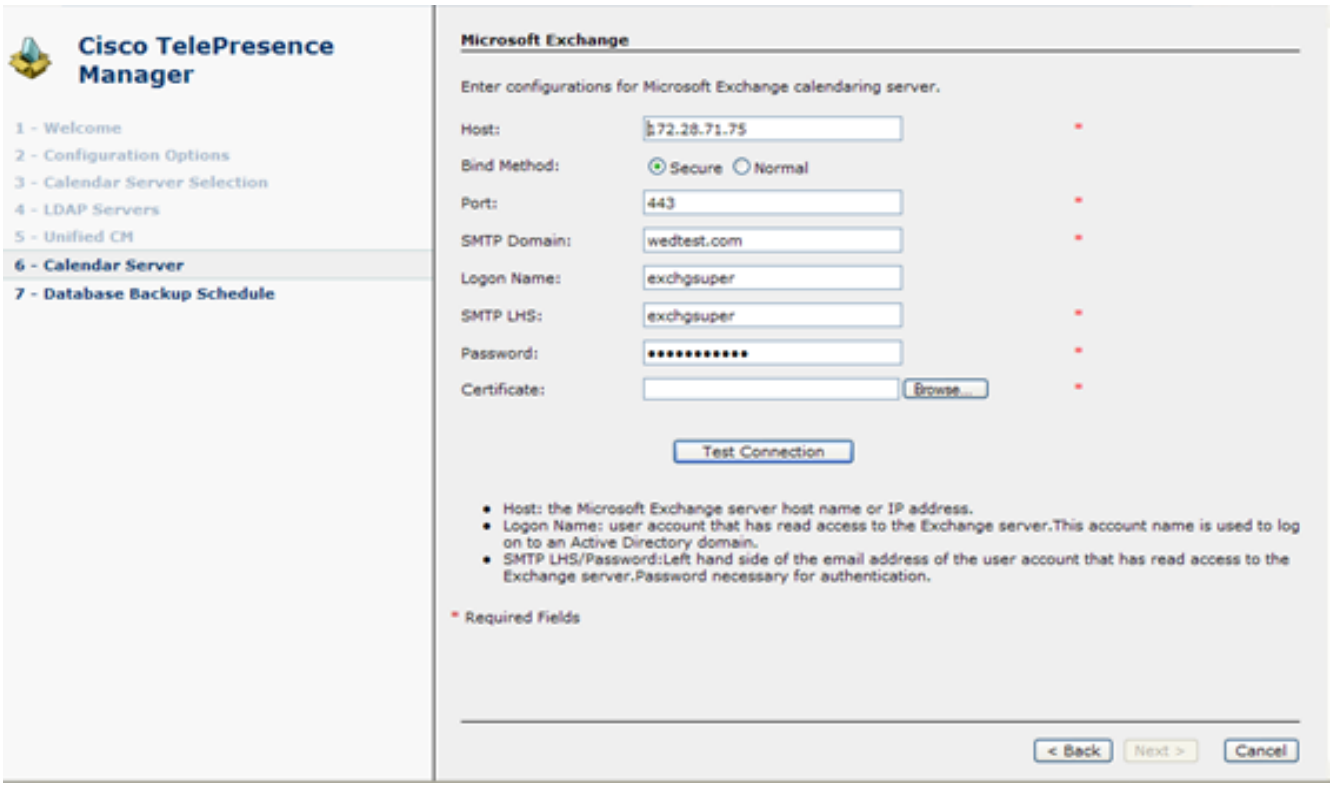
Step 4 If all the server settings have been tested, click the **Next** button.

Note If the system cannot verify the connection, the popup window directs the user to re-enter the information.

Calendar Server Configuration

This window allows you to configure the Calendar server that was configured and verify the set up. This example covers a Microsoft Exchange calendaring server. For further information about Calendar server configurations, refer to Chapter 9, "Additional Installation Configurations for Cisco TelePresence Manager".

Figure 8-8 Calendar Server Configuration Window



Explanation of Microsoft Exchange Fields

- **Host**

  Host is the hostname or IP address of the Microsoft Exchange Server host.

- **Bind Method**

  The bind method indicates the desired level of security.

  - Secure—Secure Socket Layer (SSL) connection requires the Distinguished Encoding Rules (DER) Certificate for the Microsoft Exchange Server. You must complete the Certificate field on this window before you can proceed.
  - Normal—The Cisco TelePresence Manager communicates with the Microsoft Exchange Server in cleartext using HTTP.

- **Port**

  The default value is 80, for secure mode the value is 443.

- **SMTP Domain Name**

  This field requires a sequence of case-insensitive ASCII labels separated by dots (for example, “cisco.com”)—defined for subtrees in the Internet Domain Name System and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.

- **Logon Name**

  The logon username should have read access to the Exchange server and rooms. This account name is used to logon to an Active Directory domain.

- **SMTP LHS**

  Left hand side of the email address of the user account that has read access to the Exchange Server. Password is necessary for authentication.

- **Password**

  The user password allows access to the Microsoft Exchange Server.

- **Certificate**

  A certificate is a digital representation of user or device attributes, including a public key, that is signed with an authoritative private key. In a self-signature, the signature can be verified using the public key contained in the certificate.

Note Click the **Browse...** button to choose the Microsoft Exchange Server SSL certificate. If you selected Secure bind method, this value is required.

Click on the **Test Connection** button to verify this configuration. When the verification is completed, click on the **Next** button.

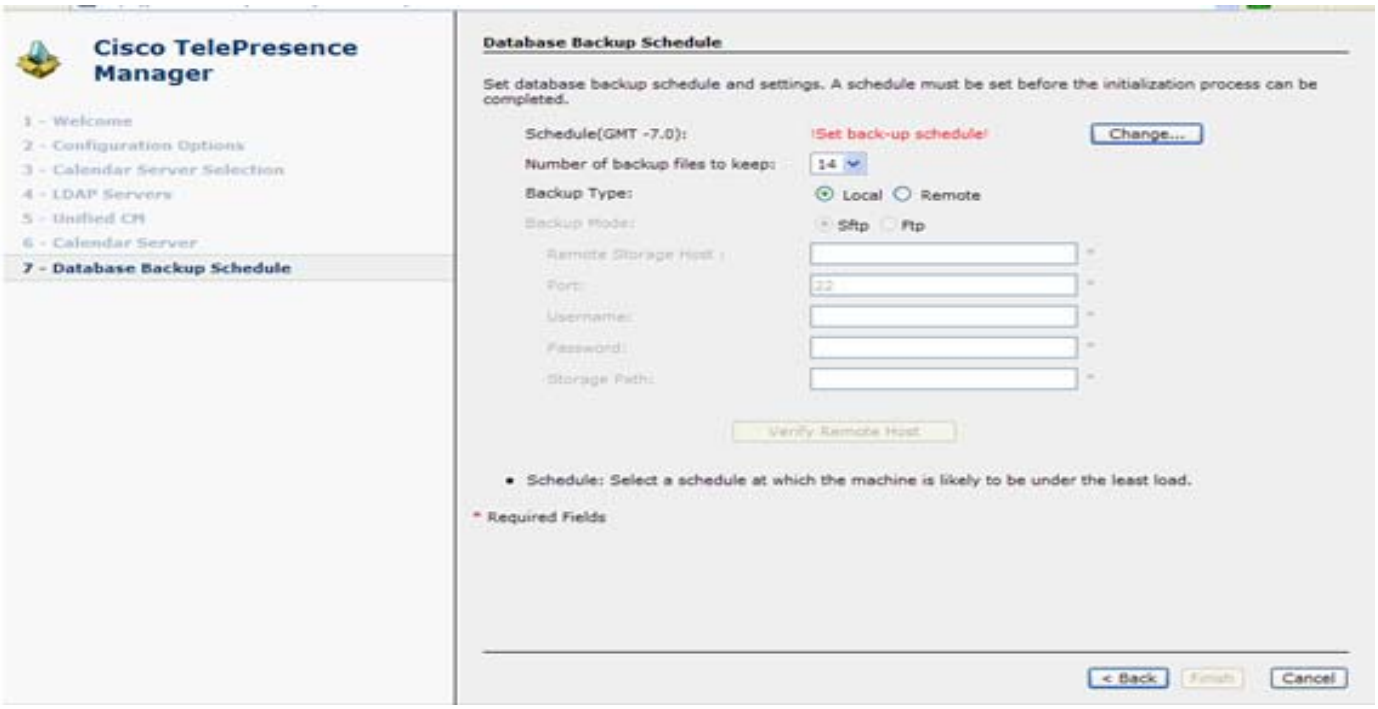
Database Back-up Schedule

The Database Backup Schedule window opens. See Figure 8-9.

Fill in the fields. If you are setting up a remote backup, click **Verify Remote Host** to verify the login information. For additional information about Database Backup, refer to Chapter 9, “Additional Installation Configurations for Cisco TelePresence Manager”, Database - Status, Backup, and Restore section.

Note The default is set to a daily backup schedule with the backup information stored to the local drive. Cisco recommends that you back up your data to a different drive.

Figure 8-9 Database Backup Schedule Window



Explanation of Database Backup Schedule Fields

The Cisco Unified Communications Manager uses an Informix Database server to store information. This window allows the administrator to set up regular backup operations of the database.

Note Cisco strongly recommends scheduling regular backups of the database.

The Database Backup Schedule window contains the following fields:

- **Schedule**

  Click **Change...** to set the backup schedule. The following choices are available:

  – **Start Time** (UTC)

  Enter the hour and minute, in UTC 24-hour format, for when you want your backup to begin. UTC is the atomic clock version of Universal Time (UT), formerly known as Greenwich Mean Time. Time zones around the world are expressed as positive and negative offsets from UT. For example, Midnight Pacific Standard Time (+8 UT) is 08:00 UT.

  – **Frequency**

  Choose **Daily** or **Weekly** database backups. If you choose Weekly, select the radio button beside the day of the week on which you want your backup to occur.

- Number of backup files to keep

  From the drop-down menu, choose the number of backup files to keep before deleting. Choices range from 1 (default) to 14 (two week's worth of daily backups).

- **Backup Type**

Choose Local or Remote to designate the server for backups. If you select Local, the backup files are stored on your local server.

If you choose Remote, you must fill in the following values for the remote server:

- **Remote Storage Host** (SFTP)

  The network path to the remote Secure File Transfer Protocol (SFTP) storage host.

- **Port**

  Port number designated for the backup process. The default is port 22.

- **User Name**

  Username for login of the remote server.

- **User Password**

  Password for login to the remote server.

- **Storage Path**

  The file path to the location where you want to store the backup data.

Step 5 Click **Verify Remote Host** to ensure that the path is valid.

Step 6 Click **Finish,** located at the bottom of the window.

The Cisco TelePresence Manager admin window appears at http://*server hostname or IP address*.

Microsoft Exchange Calendar Service Window

The Microsoft Exchange Calendar Service 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 8-10:

Step 1 Click **Test Connection.**

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

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

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

Figure 8-10 Microsoft Exchange Calendar Service Window

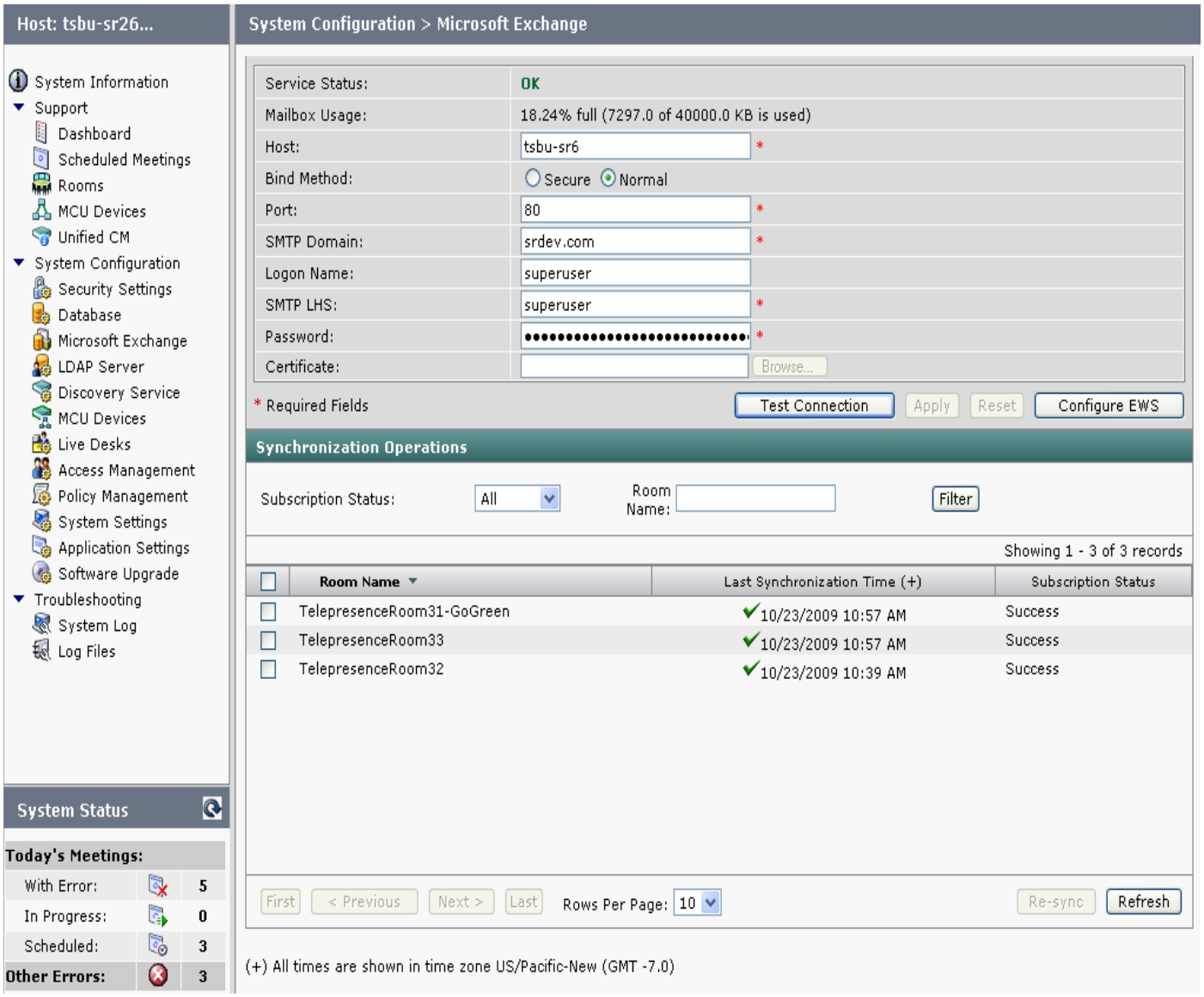


Table 8-2 describes the information and operations accessible from this window.

Table 8-2 Microsoft Exchange Server

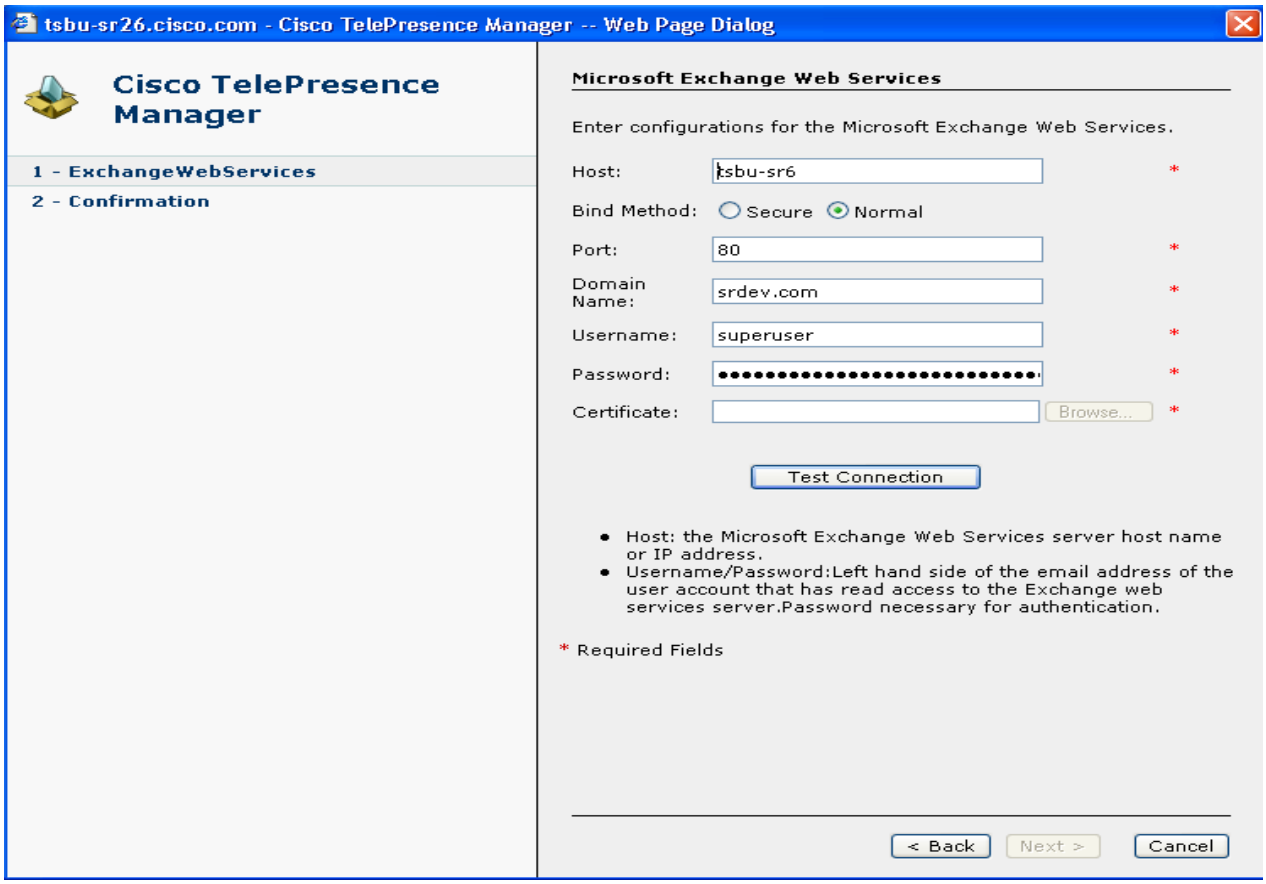
Field	Description or Settings
Service status	Display-only status report of system service.
Mailbox Usage	Meeting information is mailed to users. This display-only field reports the amount of storage space taken up by the e-mails as a percentage of total space available.
Host	Hostname provided for the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

Table 8-2 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. For Microsoft EWS, use port 80.
Domain Name	Domain name provided for the Microsoft Exchange server account, which can be changed.
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.The user password allows access to the LDAP server. The password must contain at least six characters and maximum 31 characters and should be unique using English characters only. It must start with a lowercase alphanumeric character. International characters are not valid.
Certificate	Use the field to provide a trust certificate for new Microsoft Exchange server.
Configure EWS	Select a pop up window to configure the Exchange Web Service.

Refer to Figure 8-11 for the Microsoft EWS configuration window.

Figure 8-11 Exchange Web Service Configuration Window



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.

Step 4 Once the synchronization operation completes, click **Refresh** to update the display.

Table 8-3 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 8-3 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.
Room Filter	This allows you to filter your rooms to be displayed.

Initialization for IBM Domino Deployments

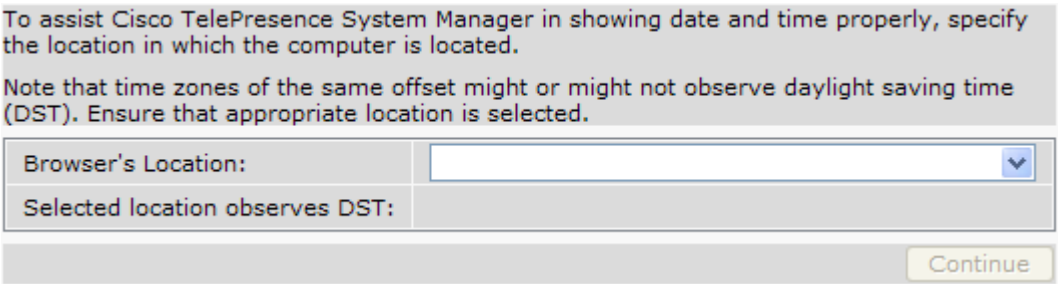
Step 1 At the console running Microsoft Explorer, type the Cisco TelePresence Manager server name or the IP address. See the following example if upgrading your system to 1.5 release.

`https://7835 server hostname or IP address`

Note If Installing a new CTS-Manager system, the server hardware version is 7845.

Step 2 The Initial Preferences window is displayed. Choose the timezone from the drop-down menu. The timezone you choose should be the one you are located in. Click **Continue**.

Figure 8-12 Initial Preferences Window



Step 3 At the product page that appears, click on **Cisco TelePresence Manager**.

Step 4 At the login page, enter the username and password created during installation.

The Cisco TelePresence Manager initial window appears with several fields already populated from the installation process and click **Next**.

Step 5 The Calendar Server Selection window is displayed. See Figure 8-13.

Choose IBM Domino for this deployment and click **Next**.

Figure 8-13 Calendar Server Selection Window

The LDAP Access Setting window opens. See Figure 8-14.

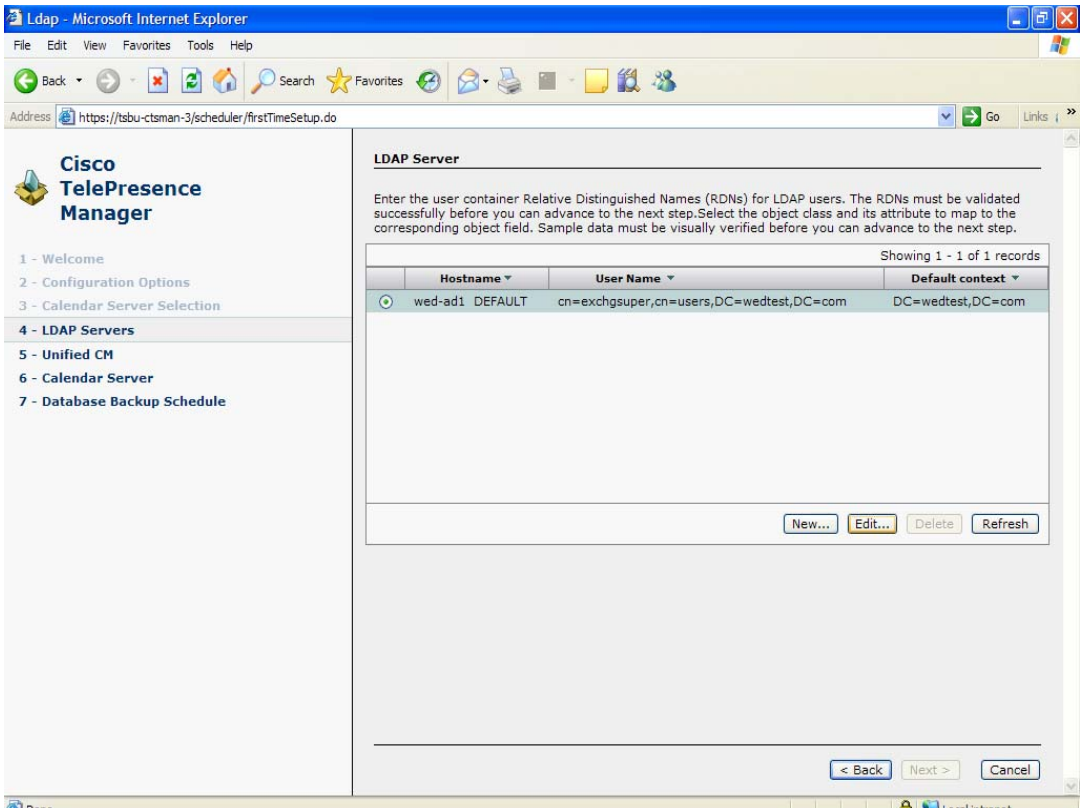
Verifying the LDAP Servers Configuration

Lightweight Directory Access Protocol (LDAP) is a protocol definition for accessing directories. This window provides you with the records of the LDAP servers that have been set up. To add new ones or to edit the one listed, select the record that is listed, then click either the **New** or **Edit** button. For more information about setting up servers, refer to Chapter 9, "Additional Installation Configurations for Cisco TelePresence Manager"

If you have selected the Configure the system with Pre-Qualification Assistant data file option, you must select the server record and click on Edit. The next window that appears gives you the setup information, you must test the connection. You have to do this with all the LDAP servers that you have configured before you can select the Next button.

In the LDAP server window example Figure 8-6, it shows one record.

Figure 8-14 LDAP Access Setting Window



Step 1 Select the first listed record, then click on **Edit**. Or, if adding a new one click **New**.

Step 2 When the popup window LDAP Server Settings appears, make sure the information is correct. For further information, refer to Chapter 9, Settings for LDAP. If necessary, make changes in the fields.

Click on **Test Connection** button.

- The system tests the connection information. A popup window opens and displays the message "Connection to <....> Server was Verified." Click **OK**, then click **Next**.

Step 3 The LDAP Server window re-appears. If you have more records to test, repeat Step 1 through Step 3.

Step 4 If all the server settings have been tested, click the **Next** button.

Note If the system cannot verify the container information, the popup window directs the user to re-enter the information.

The 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 does not have to be changed.

Caution The object and attribute mappings for Domino/Directory Server deployments are listed in Table 8-4 and cannot be changed after installing and configuring CTS-Manager.

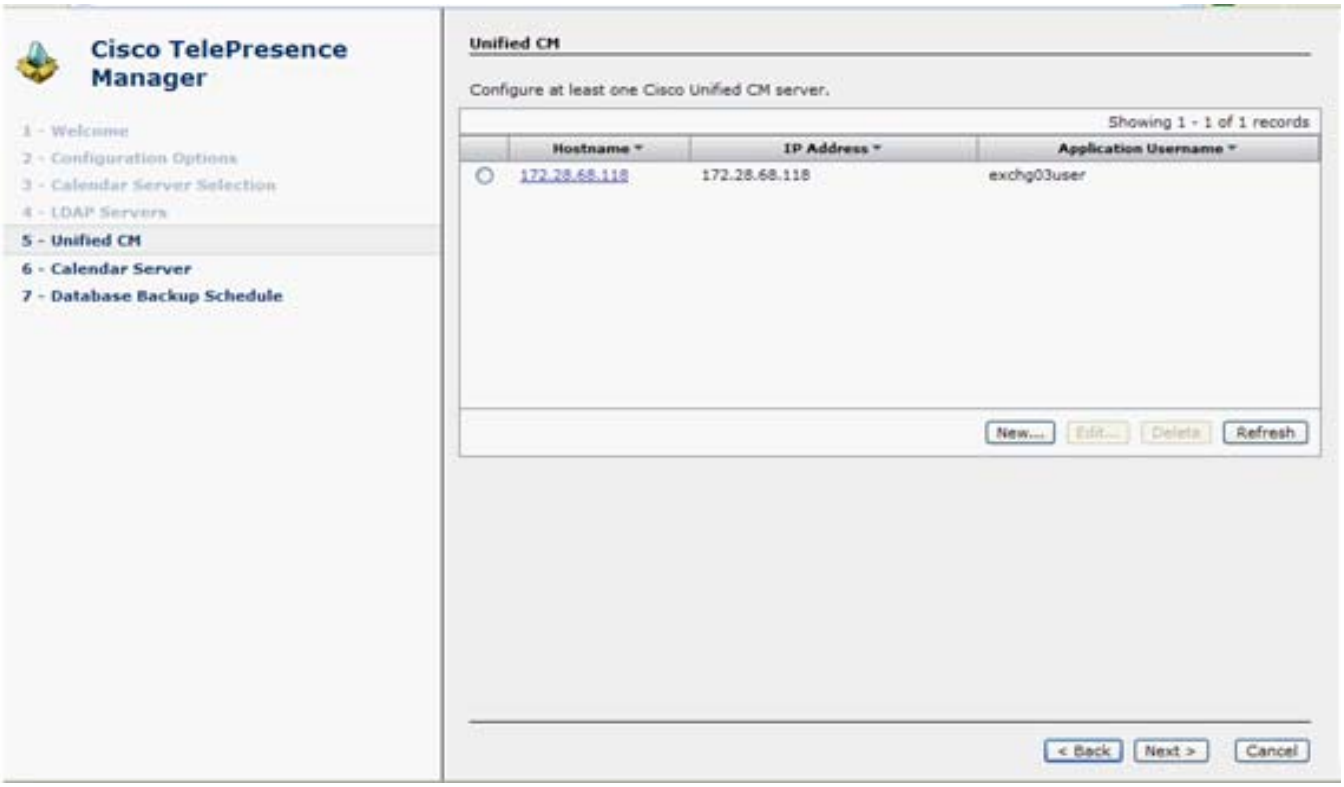
Table 8-4 LDAP Objects and Attributes

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
Person			
	EmailID	Person	cn
	DisplayName	Person	cn
(for releases after 1.5)	Mail	Person	cn

Cisco Unified Call Manager (CUCM) Server Configuration

This window allows you to review the CUCM server(s) that was configured and verify the set up through the Pre-Qualification Assistant.

Figure 8-15 Cisco Unified CM Configuration Window



Verifying the Cisco Unified Communications Manager Configuration

Step 1 Select the first listed record, then click on **Edit**. Or, if adding a new one, click **New**.

Step 2 When the popup window CUCM Server Settings appears, make sure the information is correct. For further information, refer to Chapter 9, Settings for CUCM. If necessary, make changes in this window.

- Click on **Test Connection** button. The system tests the connection information. A popup window opens and displays the message "Connection to <....> Server was Verified." Click **OK**, then click **Next**.

Step 3 The CUCM Server window re-appears. If you have more records to test, repeat Step 1 through Step 3.

Step 4 If all the server settings have been tested, click the **Next** button.

Note If the system cannot verify the connection, the popup window directs the user to re-enter the information.

IBM Domino Calendar

The **IBM Domino** window next appears.

Fill in the fields and click **Test Connection**.

The system tests the connection information. A popup window opens and displays the message "Connection to <....> Server was Verified." Click **OK**, then click **Next**.

Note If the system cannot verify the connection, the popup window directs the user to reenter the information.

Explanation of IBM Domino Fields

- **Host**

  Host is the hostname or IP address of the IBM Domino host.

- **Bind Method**

  The bind method indicates the desired level of security.

  - Secure—Secure Socket Layer (SSL) connection requires the Distinguished Encoding Rules (DER) Certificate for the IBM Domino server. You must complete the Certificate field on this window before you can proceed.
  - Normal—The CTS-Manager communicates with the IBM Domino server in cleartext using HTTP.

Note If you selected Secure bind method, this value is required.

- **Port**

  The default value is 80.

- **Organization Name**

  This field requires a sequence of case-insensitive ASCII labels separated by dots (for example, "cisco.com")—defined for subtrees in the Internet Organization Name System and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.

- **Username**

  The username provides login access to the IBM Domino server.

- **Password**

  The user password allows access to the IBM Domino server.

- **Polling Interval** (minutes)

  This is the amount of time between intervals that the CTS-Manager will poll for Calendar information. The interval times for polling are from minimum of 1 to a maximum of 360 minutes.

- **Certificate**

  A certificate is a digital representation of user or device attributes, including a public key, that is signed with an authoritative private key. In a self-signature, the signature can be verified using the public key contained in the certificate.

Note Click the **Browse...** button to choose the IBM Domino server SSL certificate. If you selected Secure bind method, this value is required.

After filling in all the fields, click on the **Test Connection** to make sure that all the data in the fields have been properly entered.

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

Dashboard for Verification of Installation Status

Go to the Dashboard window to verify installation and to check the status of the system services. In addition, you would choose Dashboard to provide a snapshot of meetings that are scheduled for the day in addition to showing the status of system services. This is a good place to monitor meetings and equipment. Click highlighted links in this window for quick access to other windows that provide meeting and room-scheduling functions.

Figure 8-16 describes the dashboard report information. To update the reports, click **Refresh**.

Figure 8-16 Cisco TelePresence Manager Support - Dashboard Window

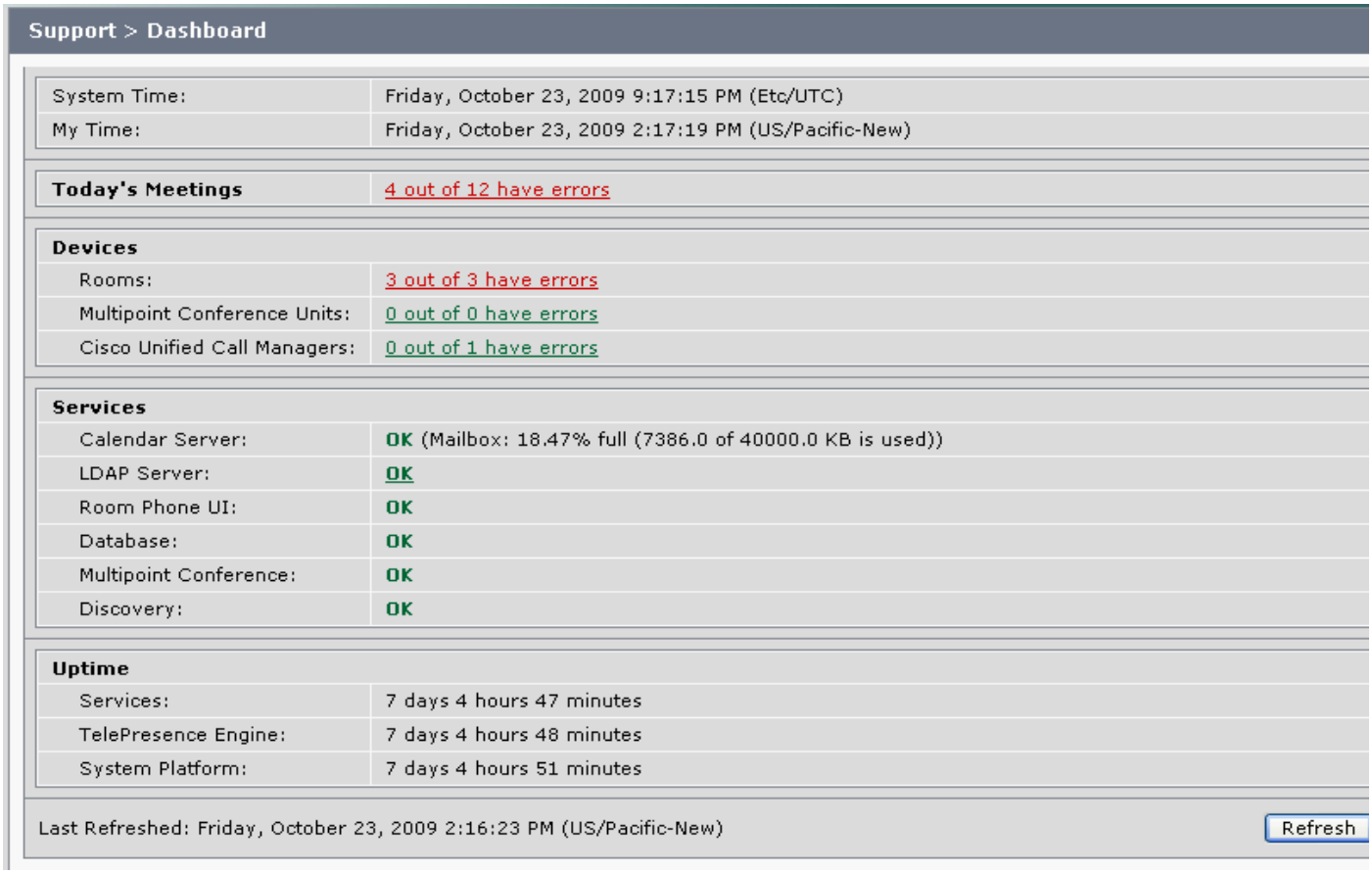


Table 8-5 Dashboard Report

Field	Description or Setting
System Time	Day, date, and time in coordinated universal time (UTC, formerly known as Greenwich mean time or GMT).
My Time	Local day, date, and time.
Today's Meetings	Status of current and upcoming meetings: • With Error—Reports the number of meetings that have errors. • All Meetings—All meetings scheduled for today. Click the link associated with each report to go to the Scheduled Meetings window.

Field	Description or Setting
Devices	Status report of the following devices: • Cisco TelePresence rooms—Clicking the link displays the Status tab in the Support > Rooms window. • Multipoint Conference Units (MCUs)—Clicking the link displays the Support > Multipoint Conference Unit window and filters the list to those MCUs with an error status. • Cisco Unified CM—Clicking the link displays the Support > Unified CM window. **Note** An error status may be reported if the connection to Cisco Unified CM was caused by a network outage. You can remove the error status by restarting CTS-Manager.
Services	Status report of following system services: • Calendar Server • LDAP Server • Room Phone UI • Database • Multipoint Conference • Discovery Status is either **OK** or is a highlighted link listing the number of errors. You can click a link to see further status information and resolve problems. You can also pass your mouse over a highlighted link to see a brief description of the error.
Uptime	Status reporting uptime since the last restart. • Services refers to the list of services above. • TelePresence Engine refers to the Cisco TelePresence database engine. • System Platform refers to the hardware host for CTS-Manager.

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

Set-Up Procedure Guidelines after Installing CTS-Manager	Description	Location
Additional Installation Procedures for CTS-Manager	The administrator makes use of the System Configuration window to perform system configuration tasks such as as synchronizing system databases, managing security, and reconfiguring system settings	Current chapter.
Monitoring CTS-Manager	Describes the support features available when you log into CTS-Manager using a 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.

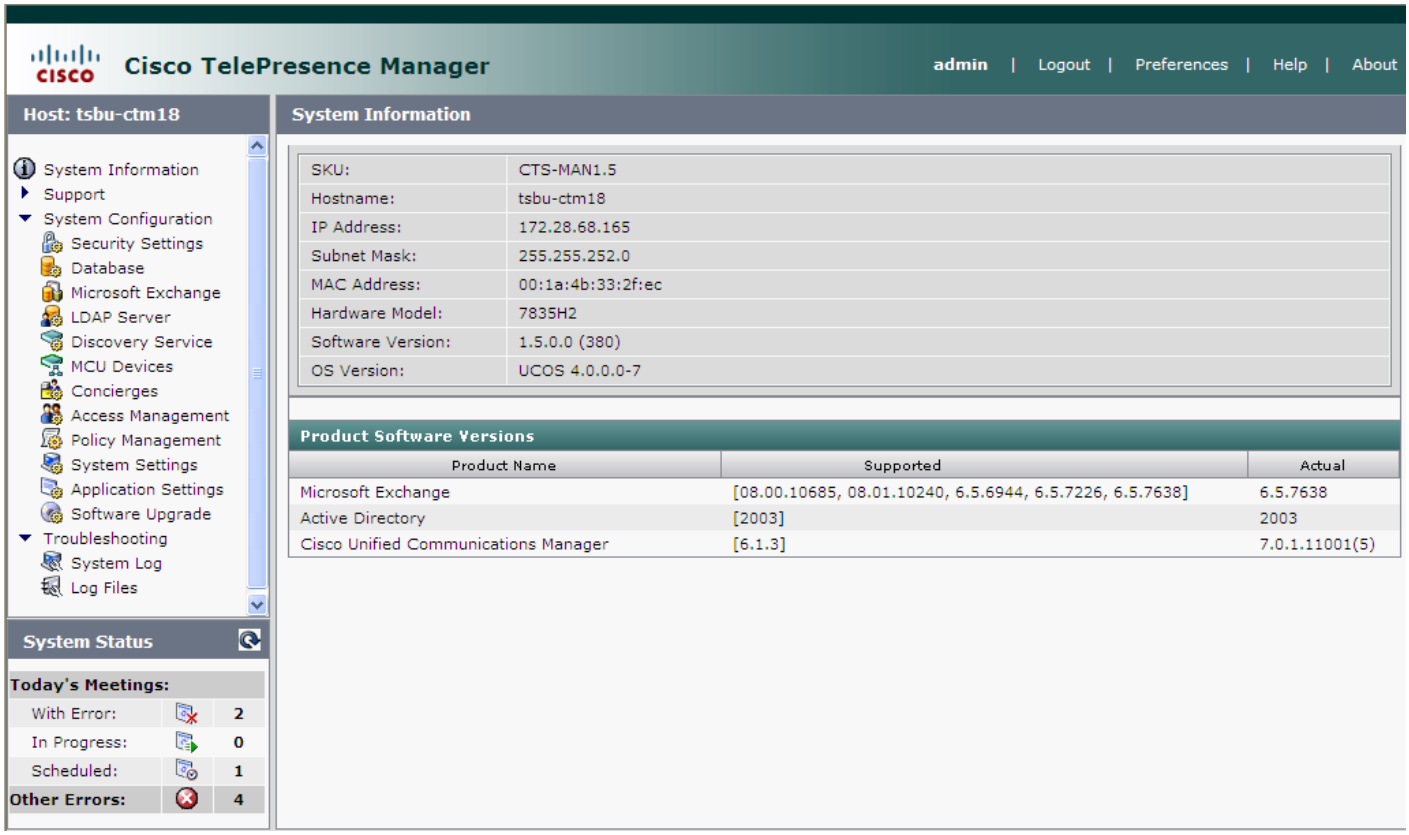
Introduction

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.

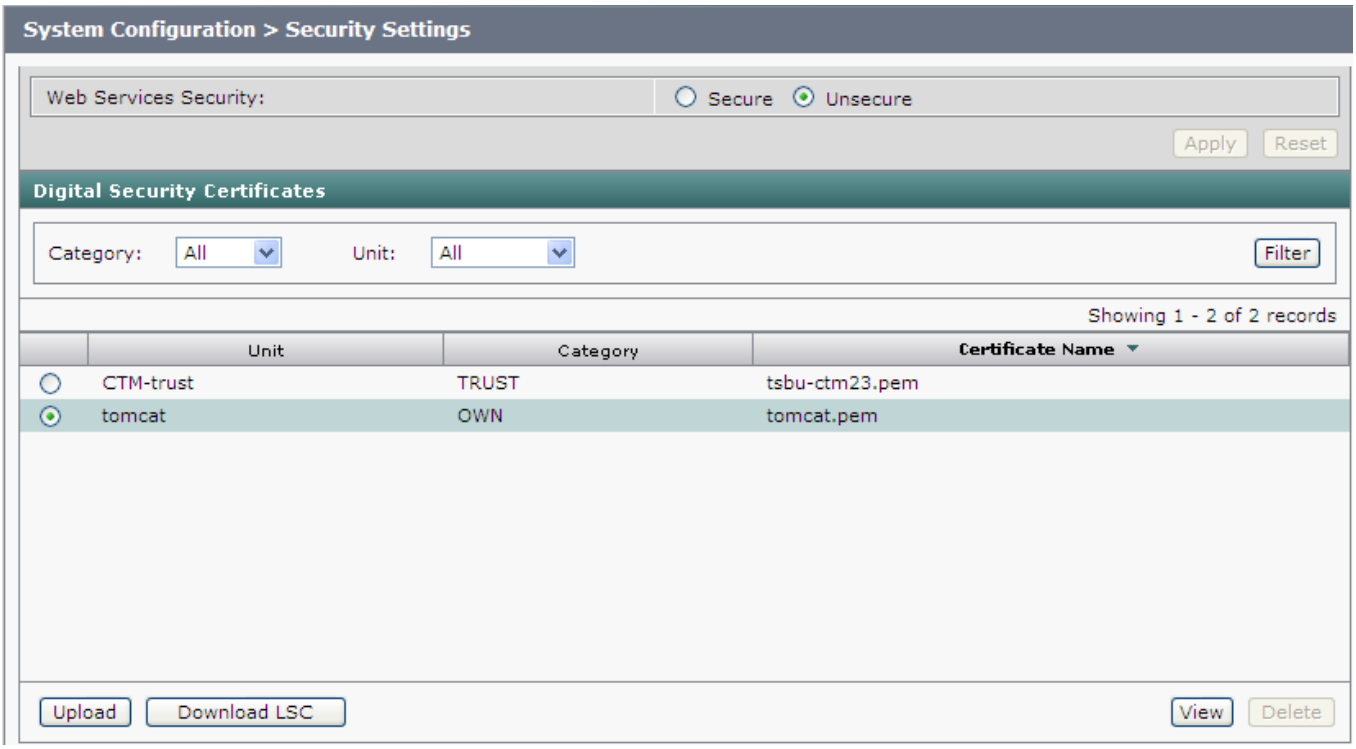
Figure 9-1 Cisco Telepresence Manager System Configuration Window



Security Settings

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

Figure 9-2 System Configuration Security Settings Window



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.

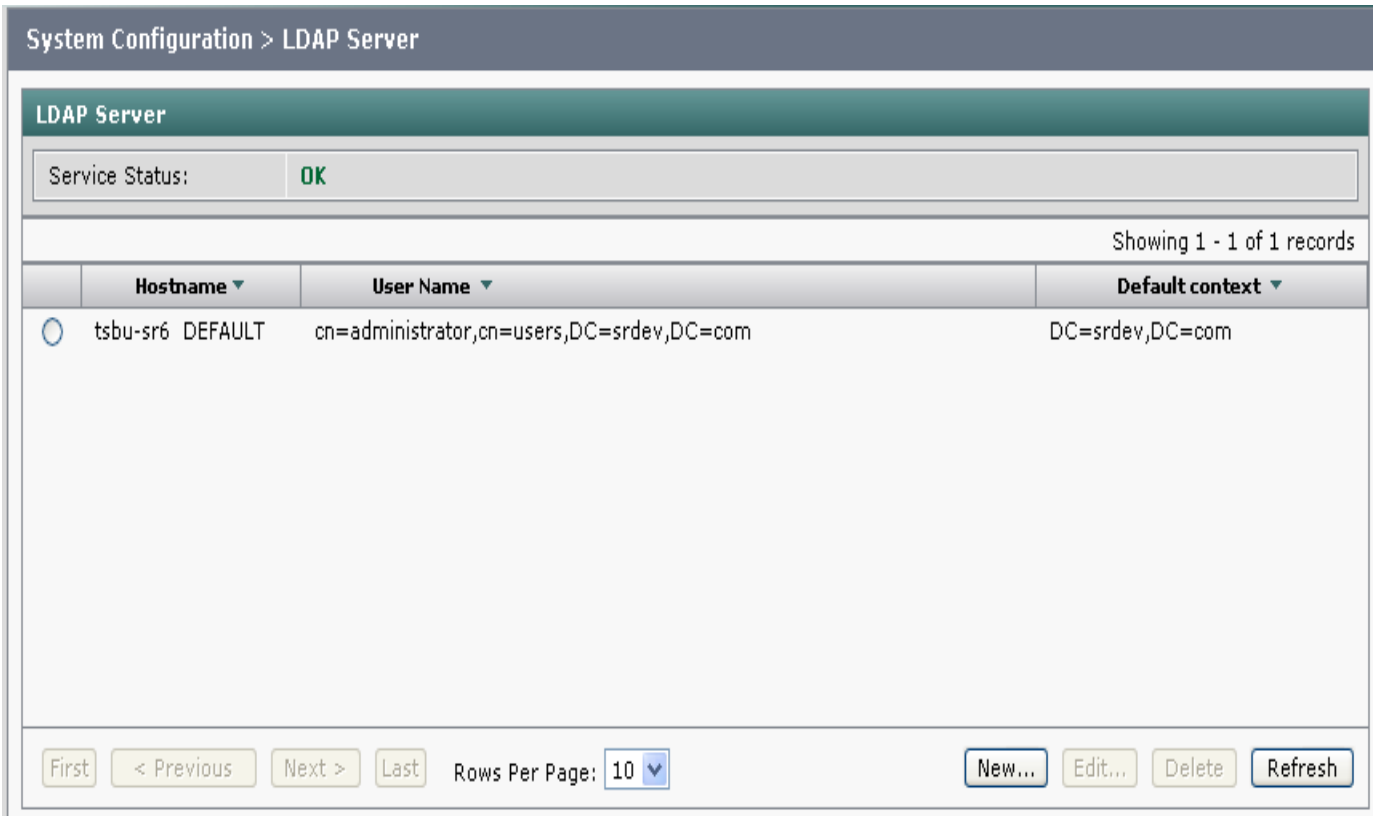
LDAP Server

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



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

This window specifies LDAP Directory Server server settings that are used by CTS-Manager to access the directory information. Open the LDAP Server window to see the 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 a single Active Directory forest. Some of the setups with which CTS-Manager can work are peer-peer LDAP domain setup, and Parent-Child LDAP domain setup.

Caution The object and attribute mappings for Exchange/Directory Server deployments are listed in Table 9-4 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

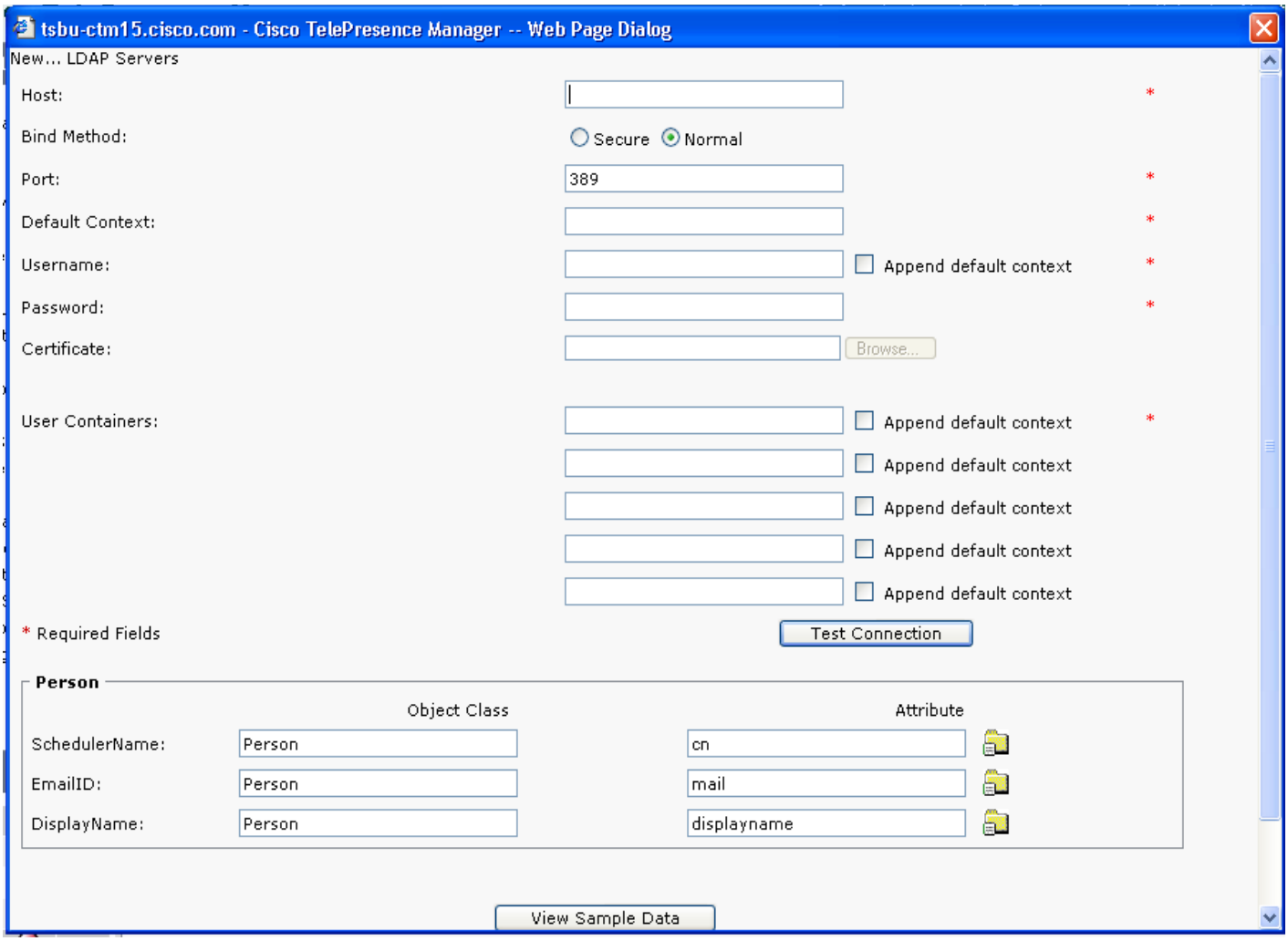


Table 9-2 lists the fields in the LDAP Server - New window. See Table 9-4 for the Person field information.

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 on the radio button to select the LDAP server that you want to edit. Then click on 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

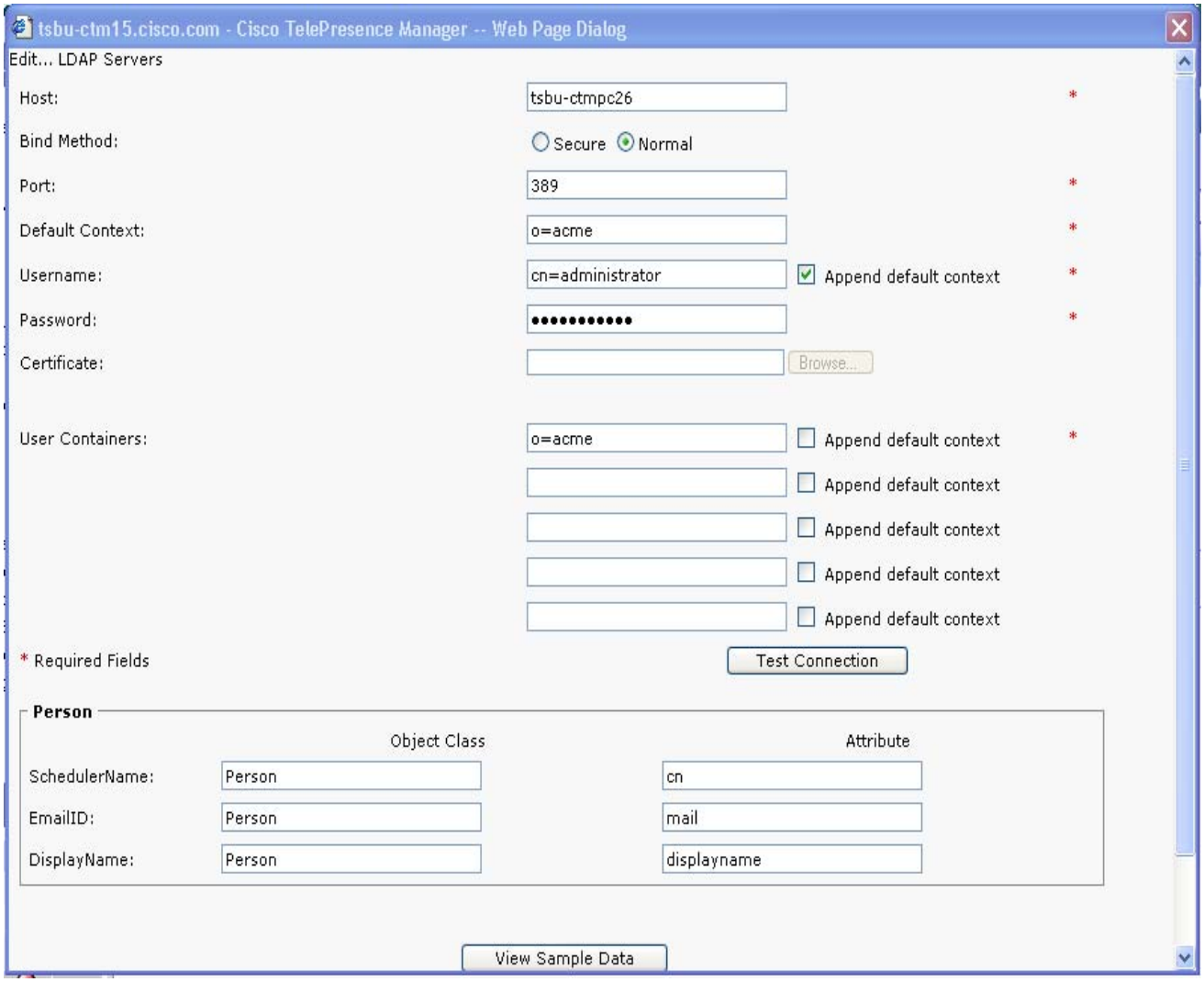


Table 9-3 Edit LDAP Server Settings

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

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

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

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

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

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

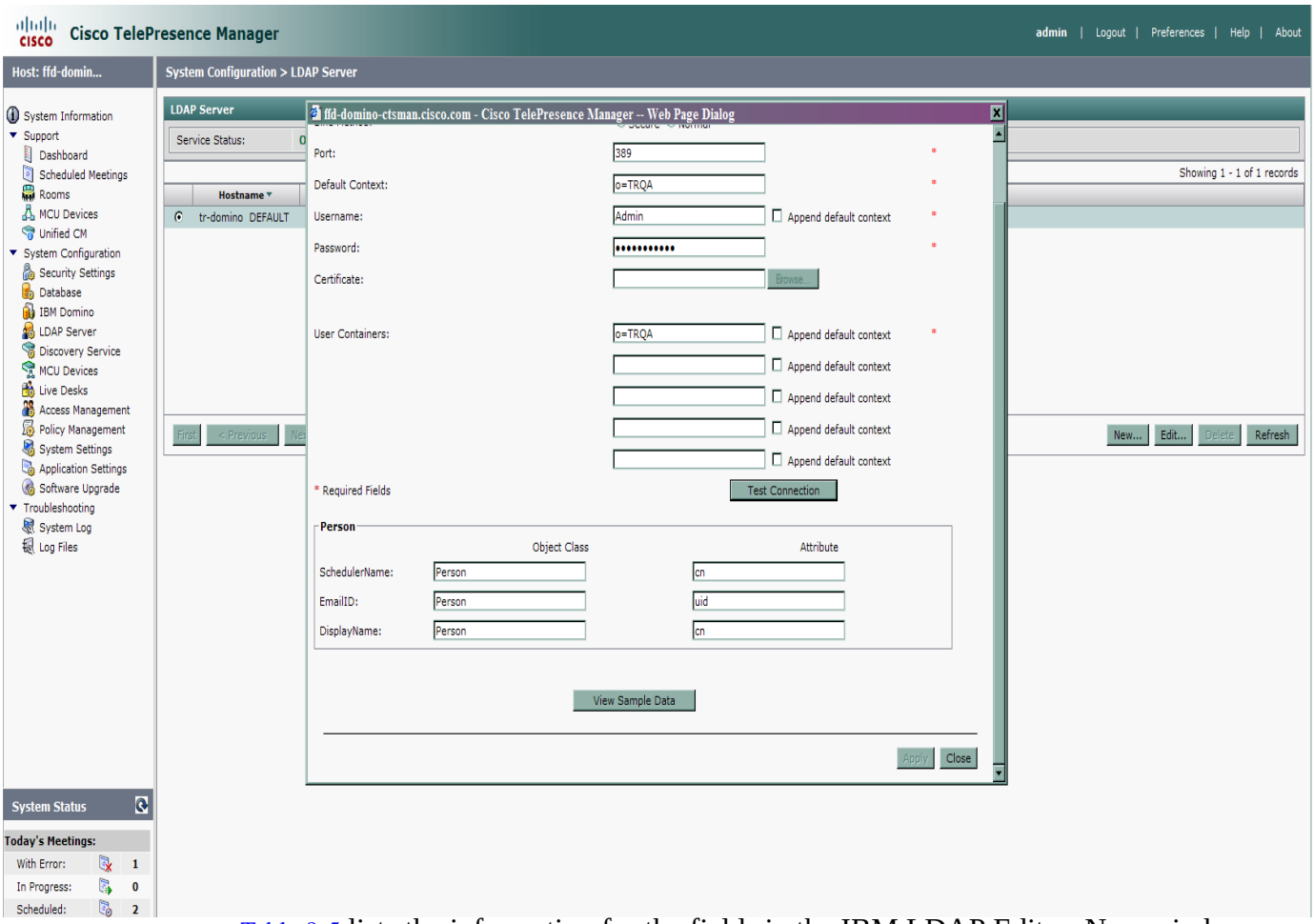


Table 9-5 lists the information for the fields in the IBM LDAP Edit or New window.

Table 9-5 IBM LDAP Server Settings

Field or Button	Description or Settings
Host	LDAP server host name.
Bind Method	Click the **Secure** or **Normal** radio button to select the binding method: • 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 9-5 IBM 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.
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.

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.

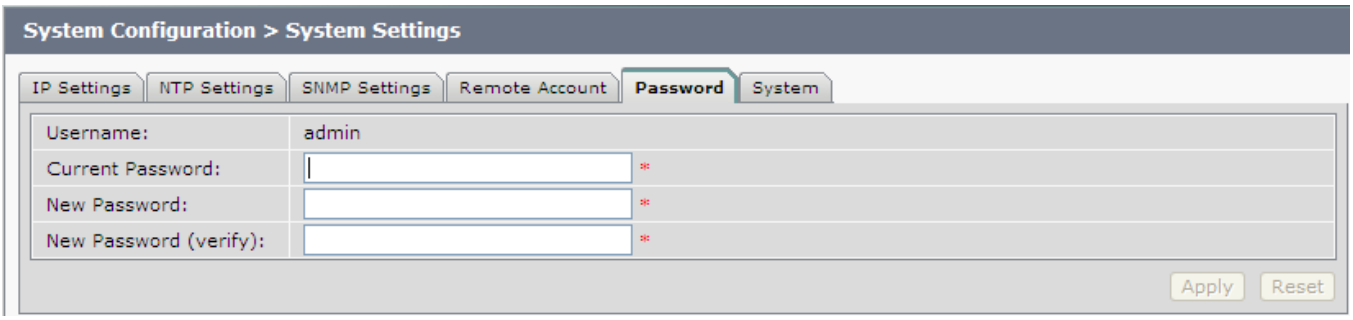
Deleting Server

Before performing a delete on 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.

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



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

Step 2 Type in your current password.

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

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

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

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

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

Calendar Server

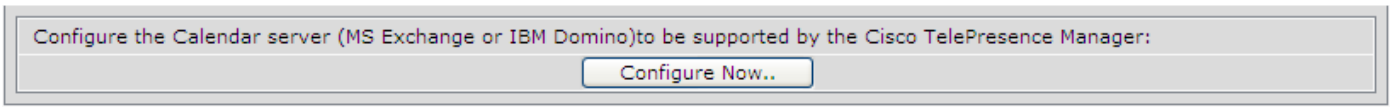
If you did not specify a Calendar server (either Microsoft Exchange or IBM Domino) during the initial installation, the Calendar Server window displays the Calendar Server wizard.

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

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

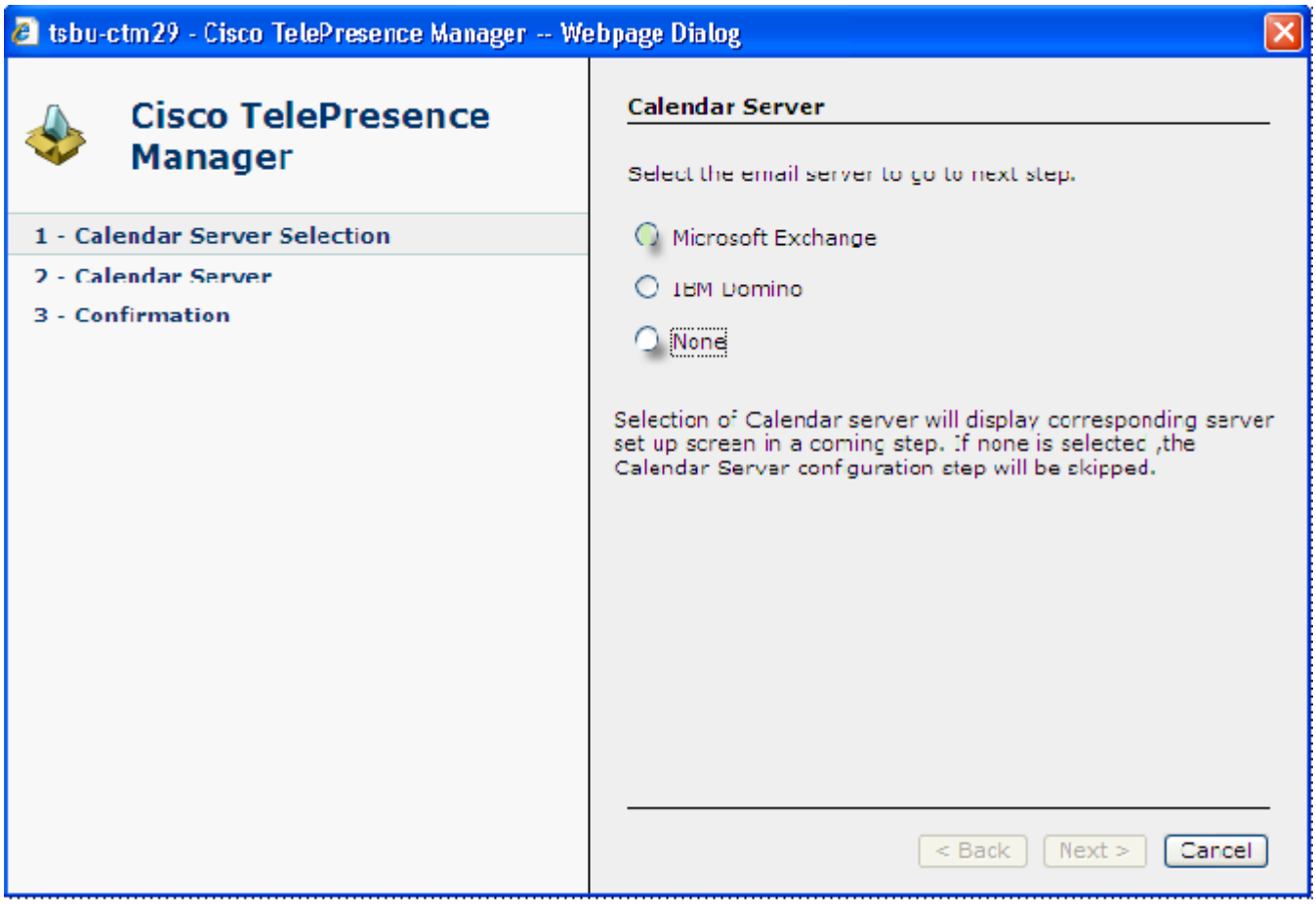
The No Calendar Server window displays the **Configure Now** button to initiate the Calendar Server wizard.

Figure 9-8 Configure Calendar Server



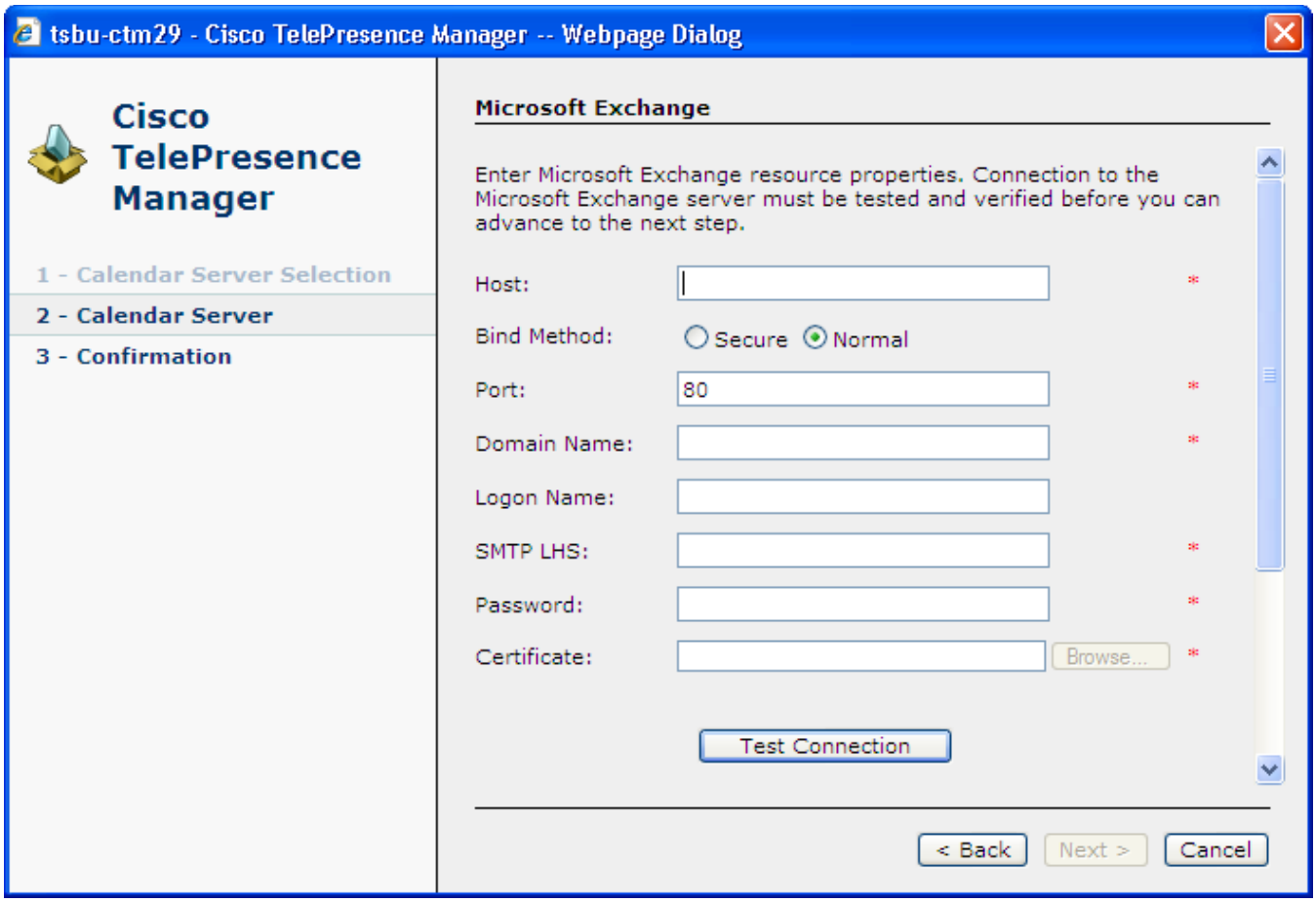
Step 1 The first step in registering a Calendar server with CTS-Manager is to choose either IBM Domino or Microsoft Exchange.

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



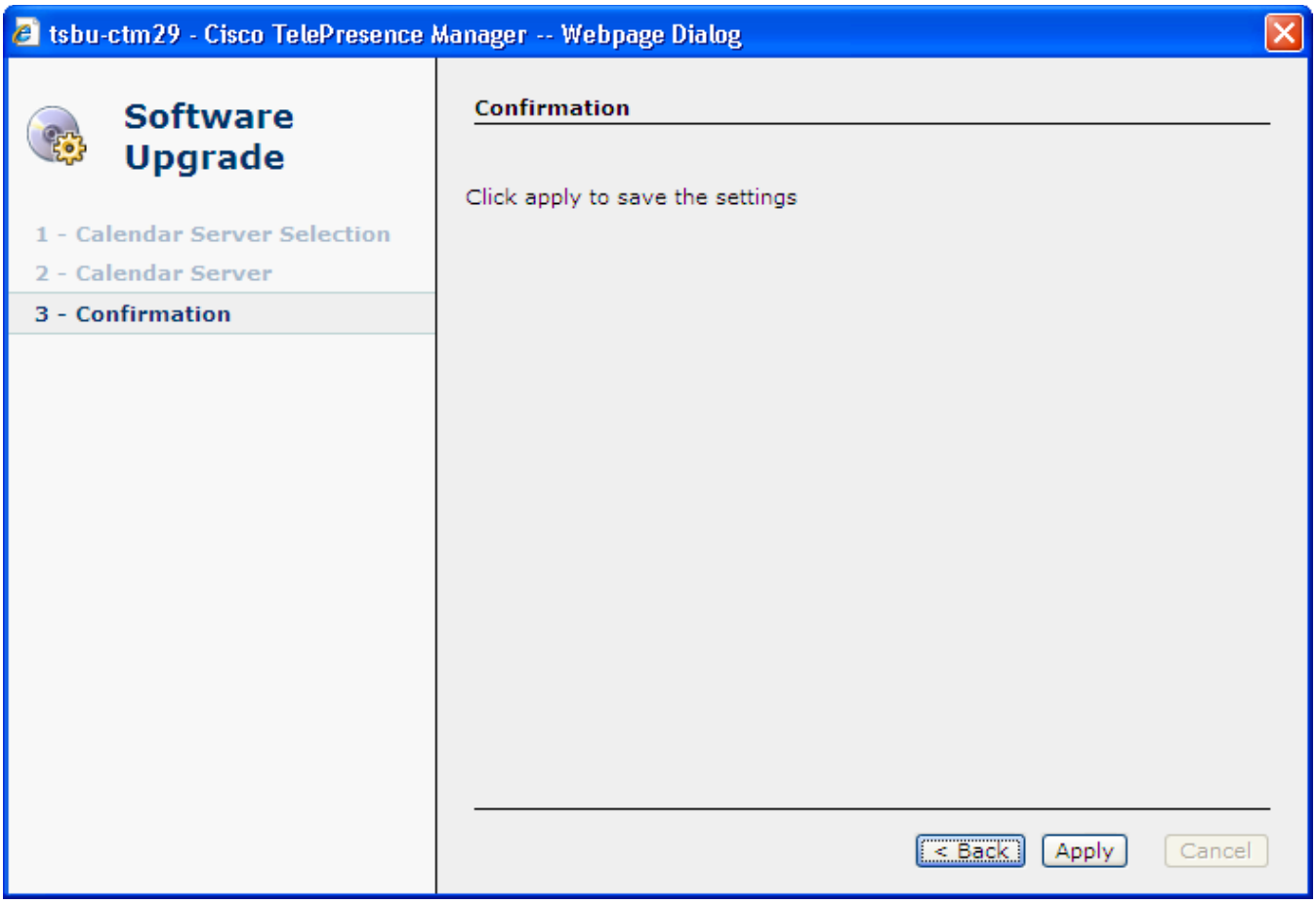
Step 2 In the next step you need to specify the service logon information. The example below displays the information needed to use the Microsoft Exchange service.

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



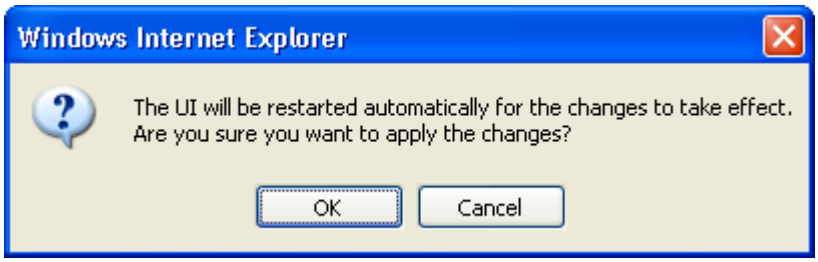
Step 3 Click **Apply** to save the new Calendar server settings.

Figure 9-11 Cisco TelePresence Manager - Calendar Confirmation Screen



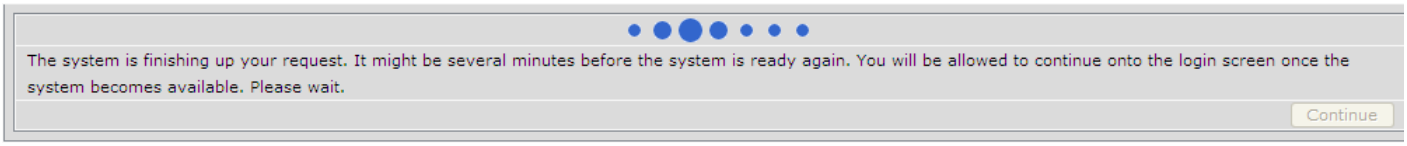
Step 4 Then click **OK** to restart the CTS-Manager server.

Figure 9-12 Apply Changes Screen



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



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

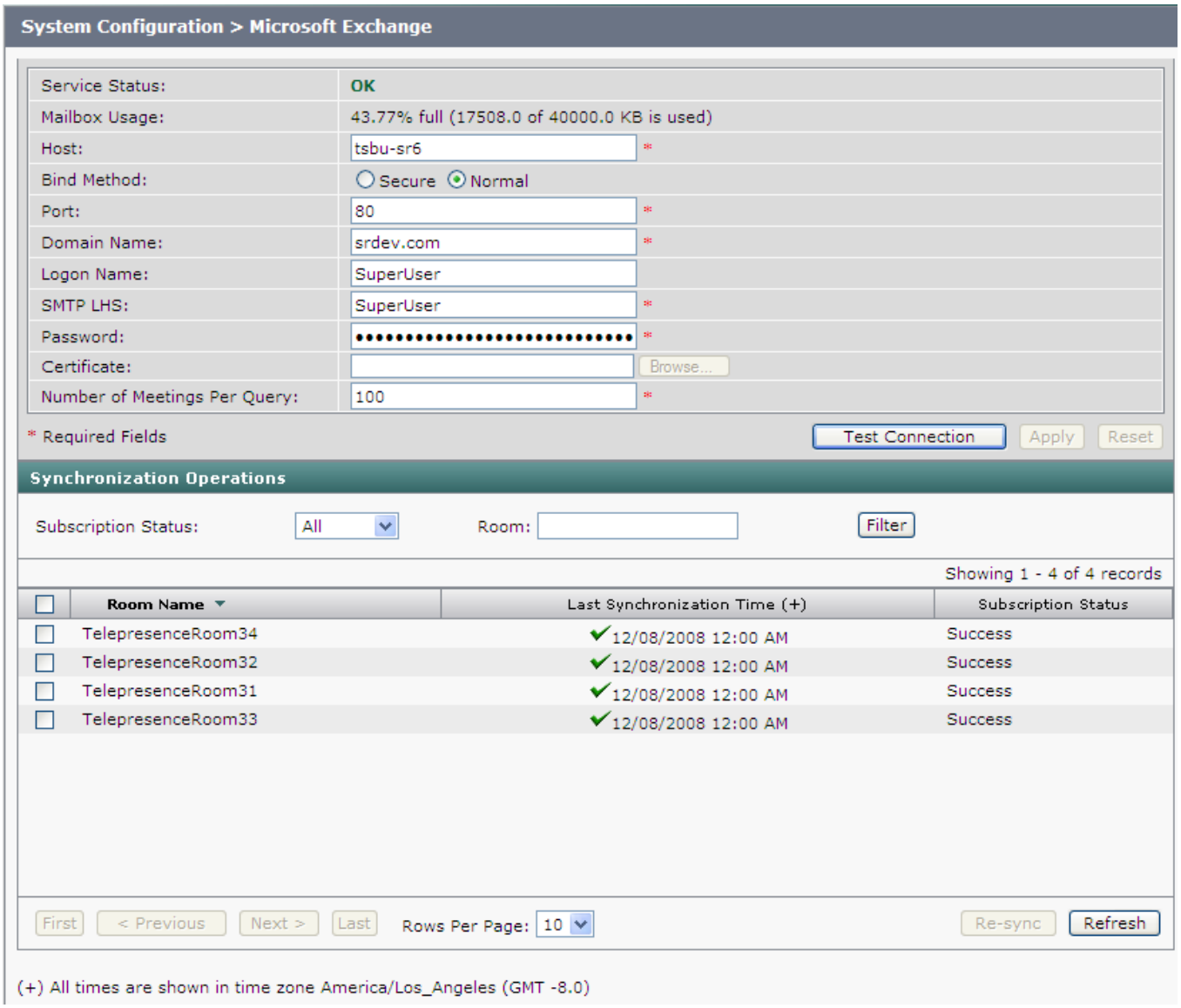


Table 9-7 describes the information and operations accessible from this window.

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. The Axis2 Library does not support NTLM v2 at this time. **Note** For WebDav 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**.

Figure 9-15 IBM Domino Calendar Service Window

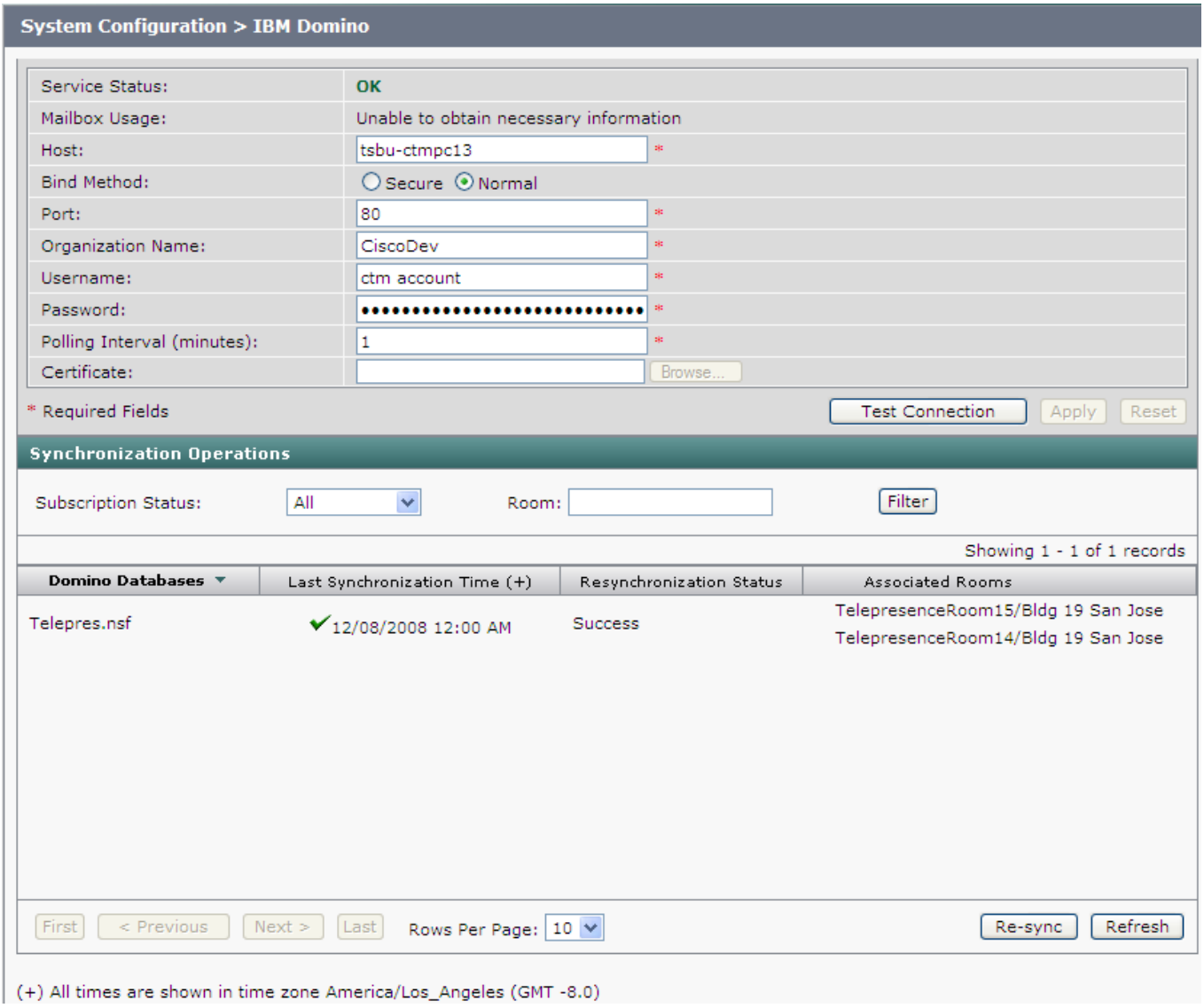


Table 9-9 describes the information and operations accessible from this window.

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. This method requires enabling Secure Socket Layer (SSL). on the Domino server. • Normal—CTS-Manager communicates with the Domino server in cleartext using HTTP.
Port	Communication port number.
Organization Name	Domain name provided for the Domino server account, which can be changed.
Username	This is the account name used to log on to the Domino server.
Password	Password used to access the Domino server account, which can be changed. **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. **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:

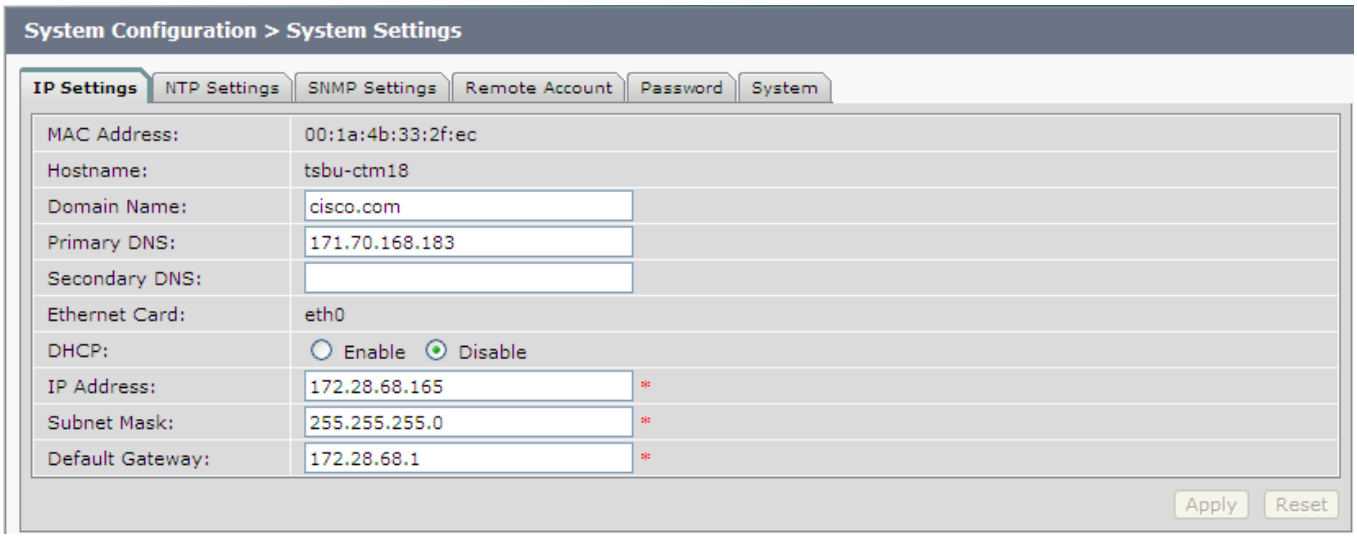
- IP Setting
- NTP Setting
- SNMP Setting
- Remote Account
- Password
- System Configuration - System Settings

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



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

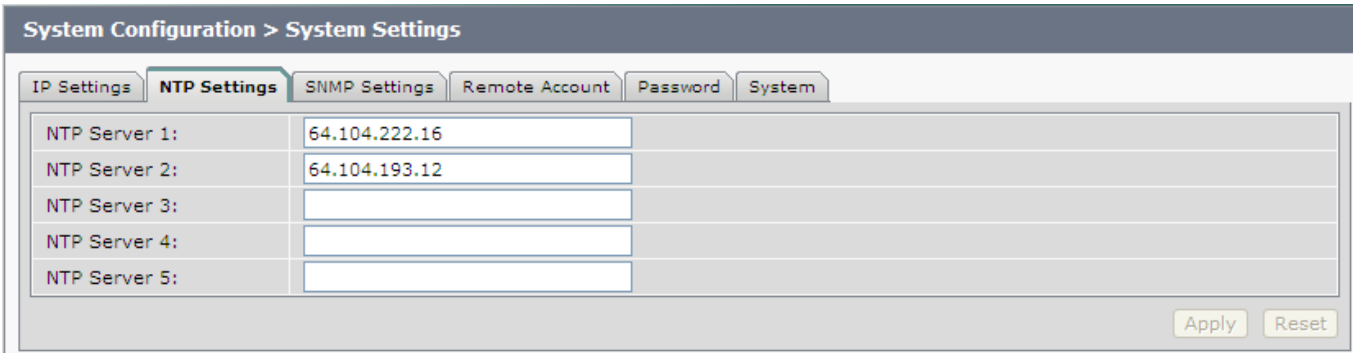
Before performing a delete on a DNS server, it is important to first change existing servers like CUCM and MCU to IP from hostname before the DNS server is deleted. If the hostname is not changed first, the CUCM and MCU servers will be put in error status.

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



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

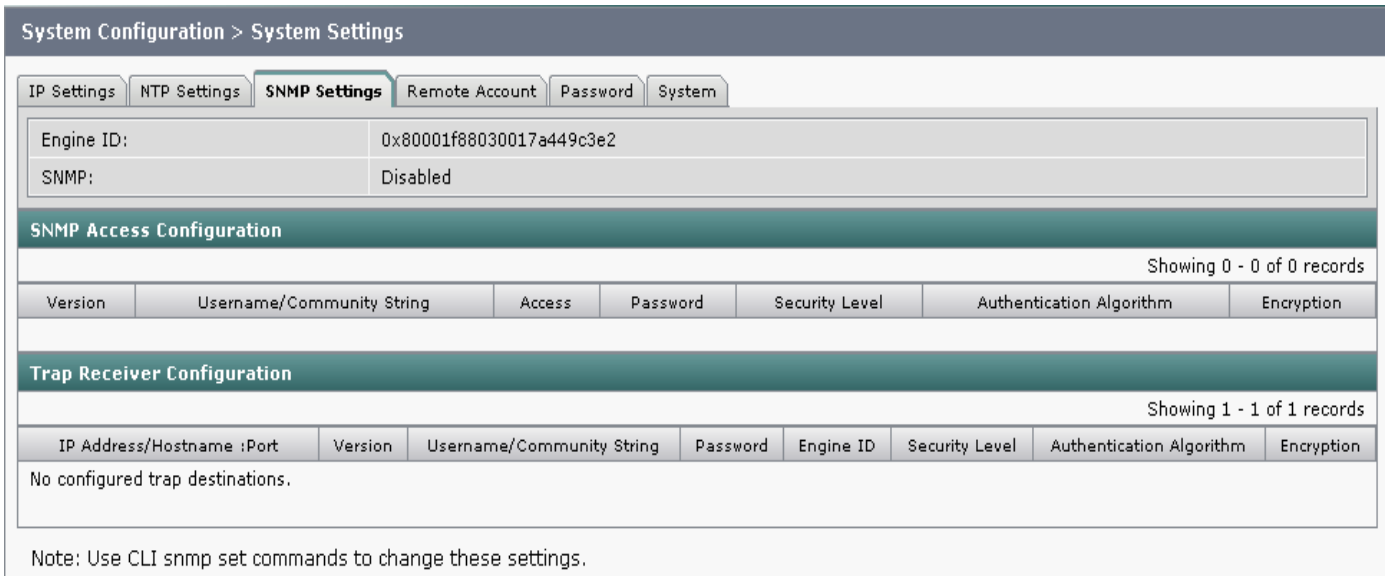


Table 9-12 describes the fields for SNMP settings.

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

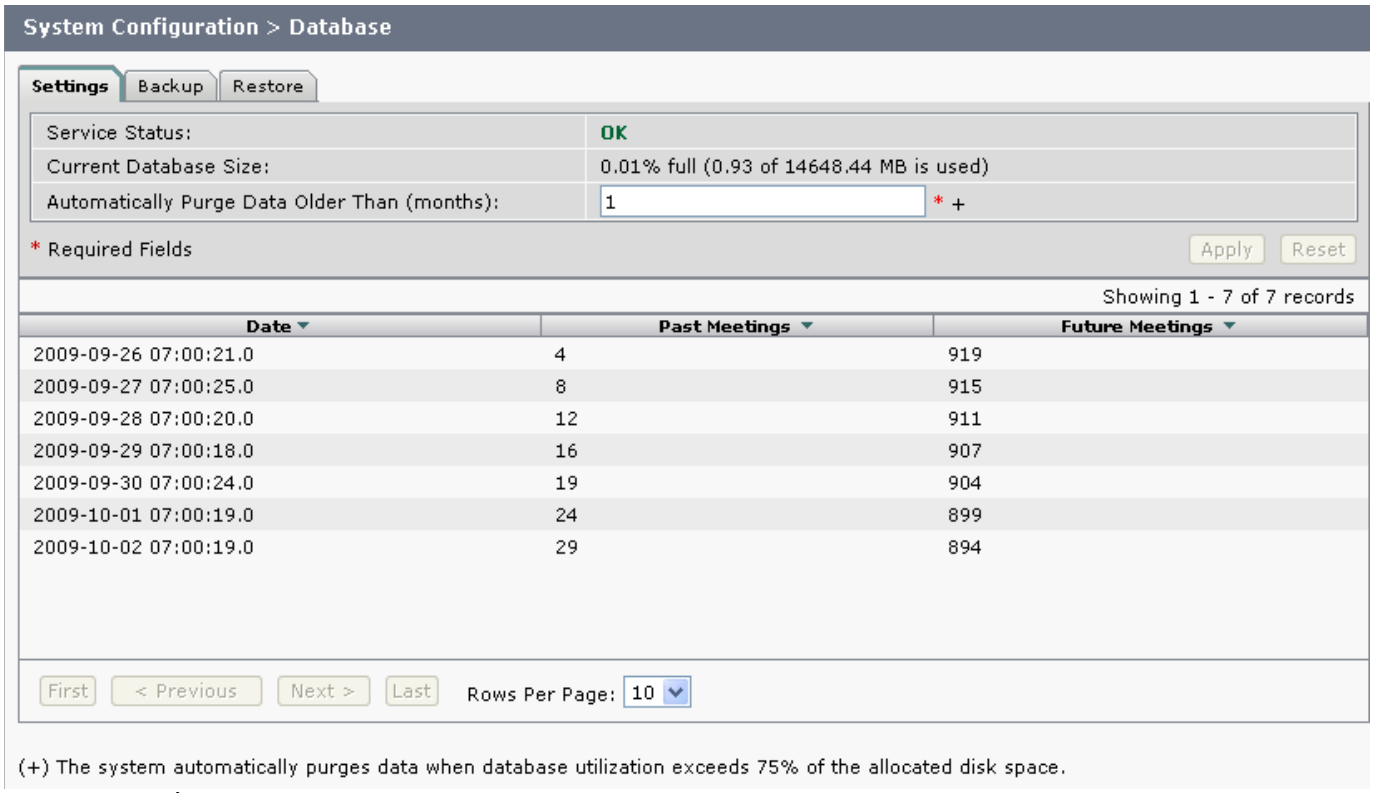
CTS-Manager uses an Informix database server to store information. The Database window allows the Administrator to view the database status and run backup and restore operations. Open the Database window to see the following choices:

- 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



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

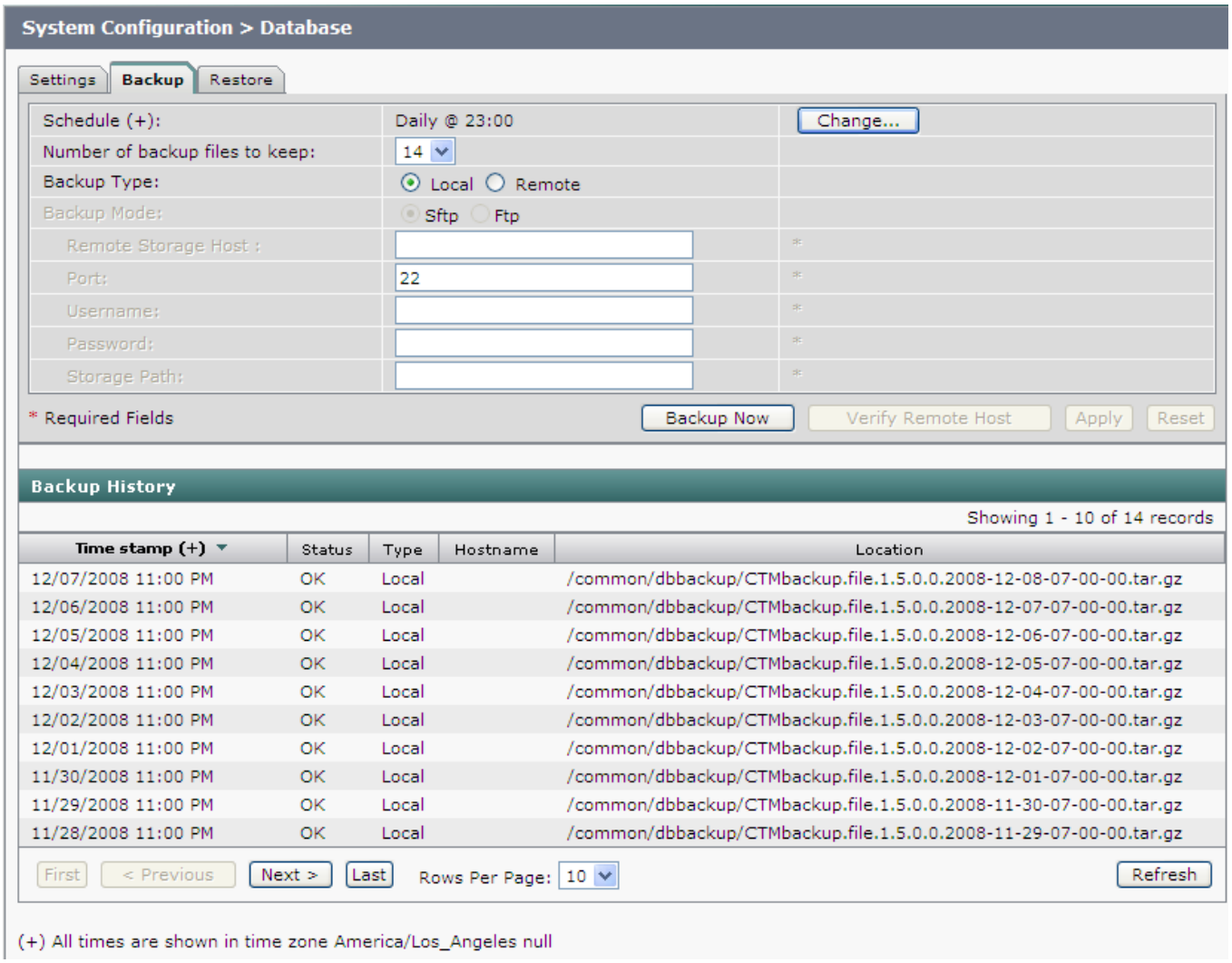
Field	Description or Settings
Service Status	Display-only status report of the Informix database server.
Current Database Size	Display-only report showing the size of the database as a percentage of the amount of total space available for a Cisco TelePresence Manager account in Directory Server. The 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



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:

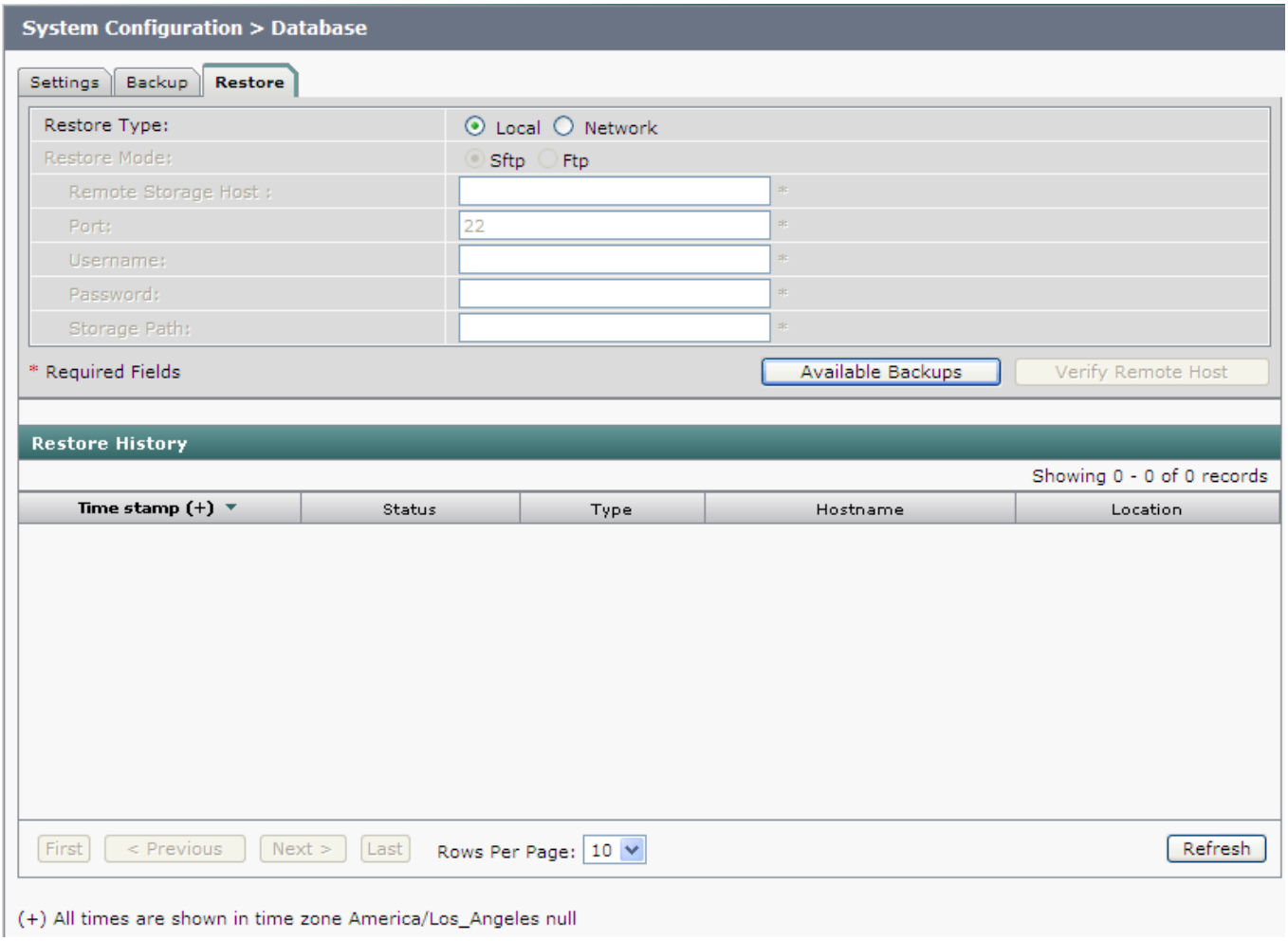
- Database data
- System SNMP configuration information
- System Certificates

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



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.

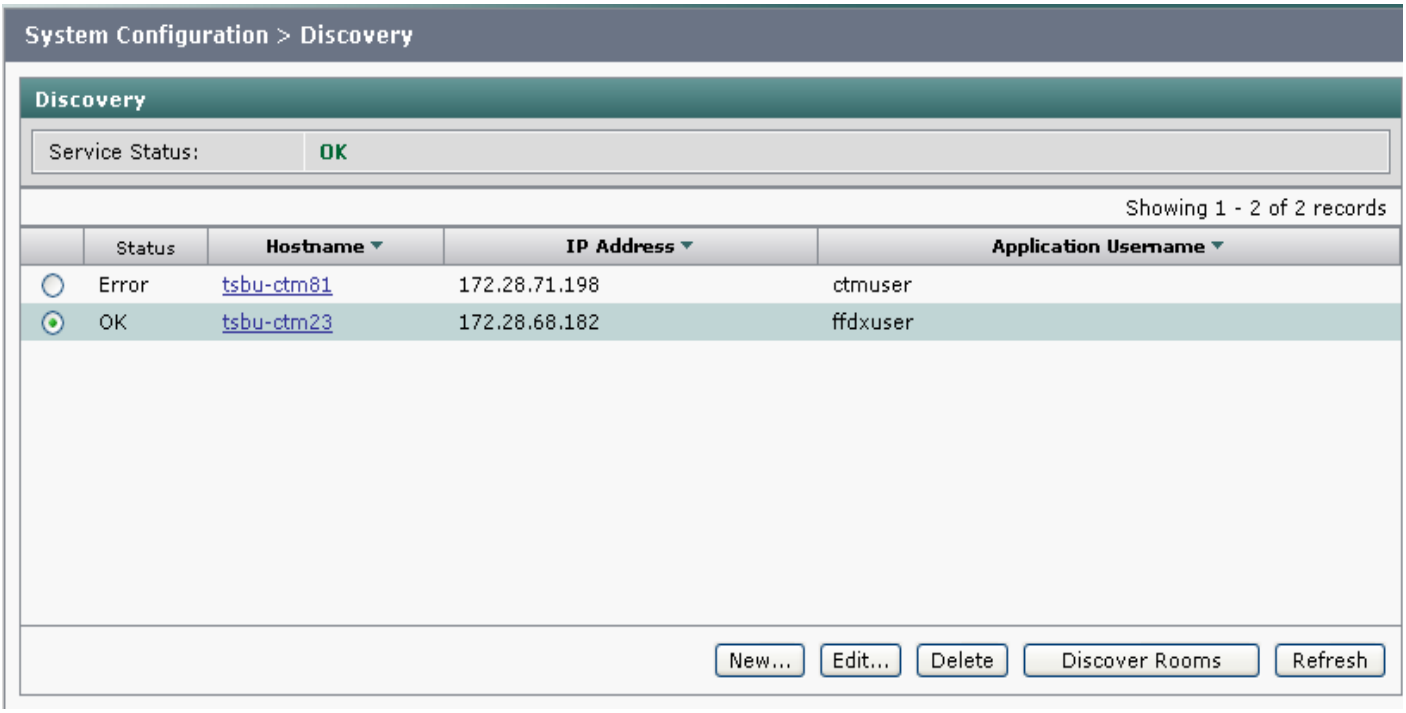
Step 3 Click **Restore Now**. This action initiates a full restore of the database from the backup file.

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.



Click on the radio button to select a host record. Once a record is selected, the buttons on the screen become usable. 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**.

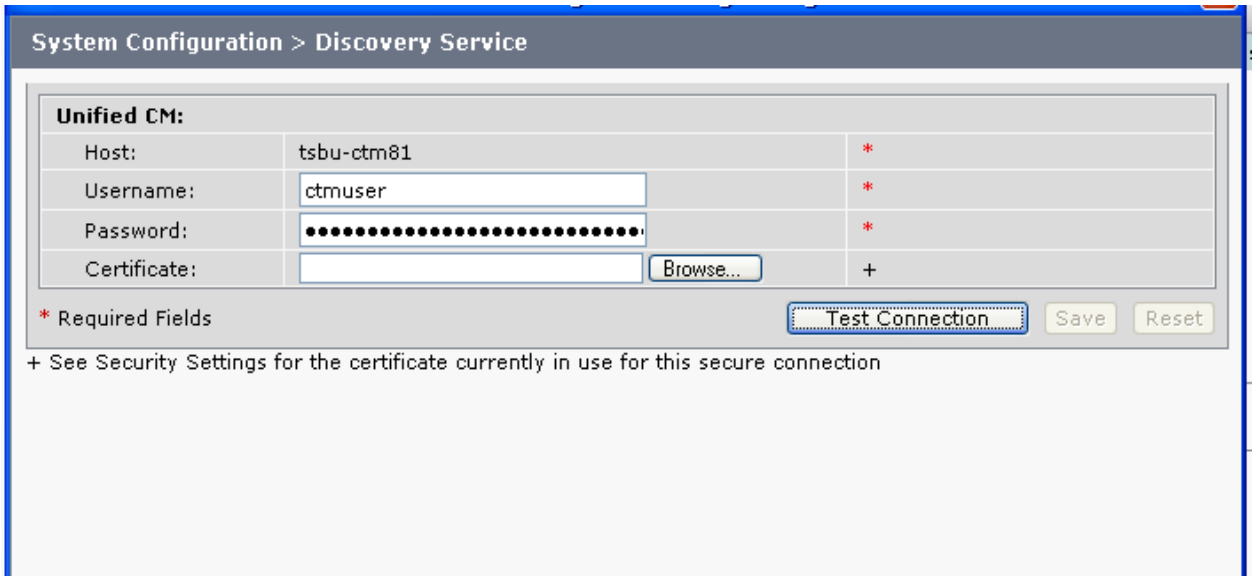
Note This process consumes a large amount of system processor time. System operation will be noticeably slower from the time that the Discover Rooms button has been clicked until the process is completed.

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



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

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

Table 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.
Test Connection	Tests the connection between CTS-Manager and CUCM server.
Save	Save the new settings.
Reset	Restore the original settings.

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

Note Rooms should be deleted only after an administrator manually does a 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

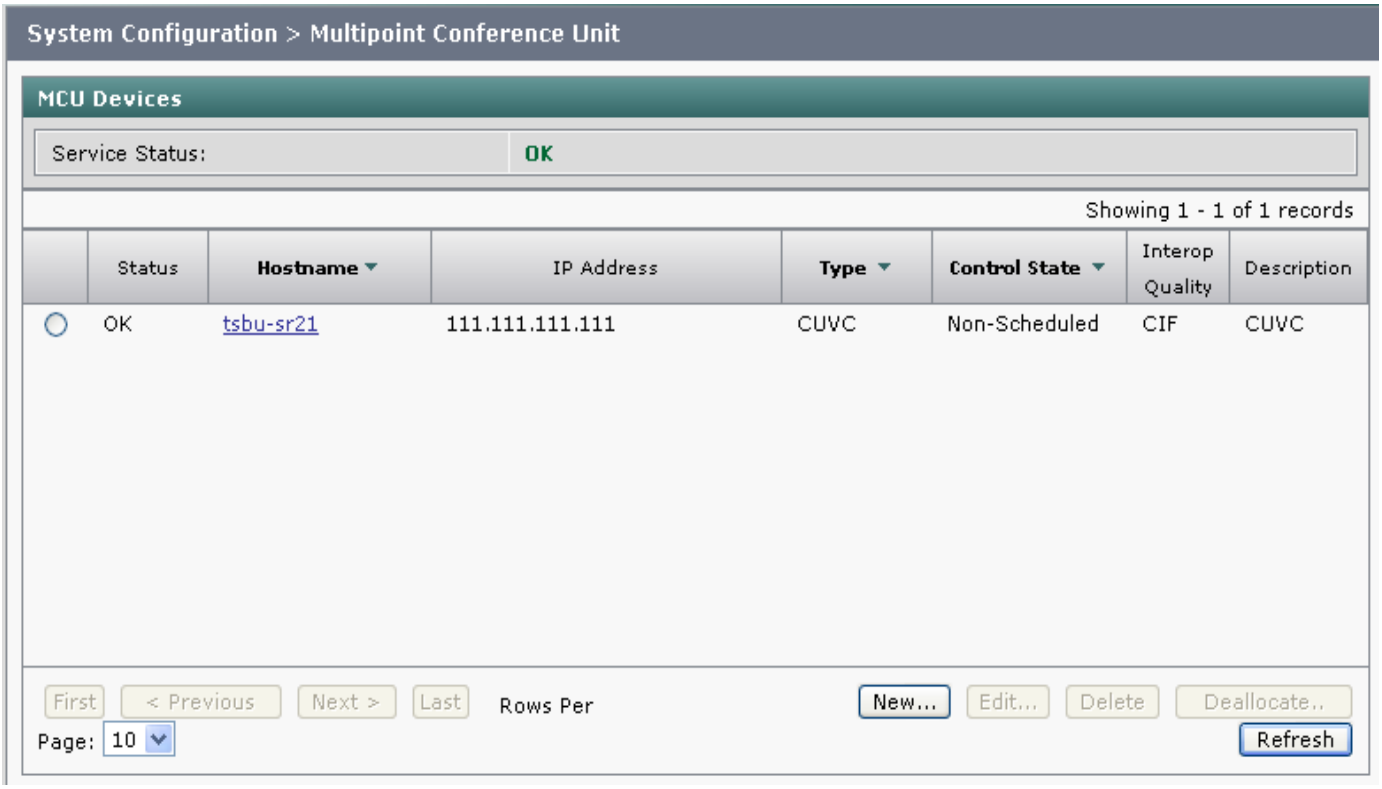


Table 9-18 describes the MCU Device fields.

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.
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.

Table 9-19 Add a New MCU CTMS Device

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. 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.
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.

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.

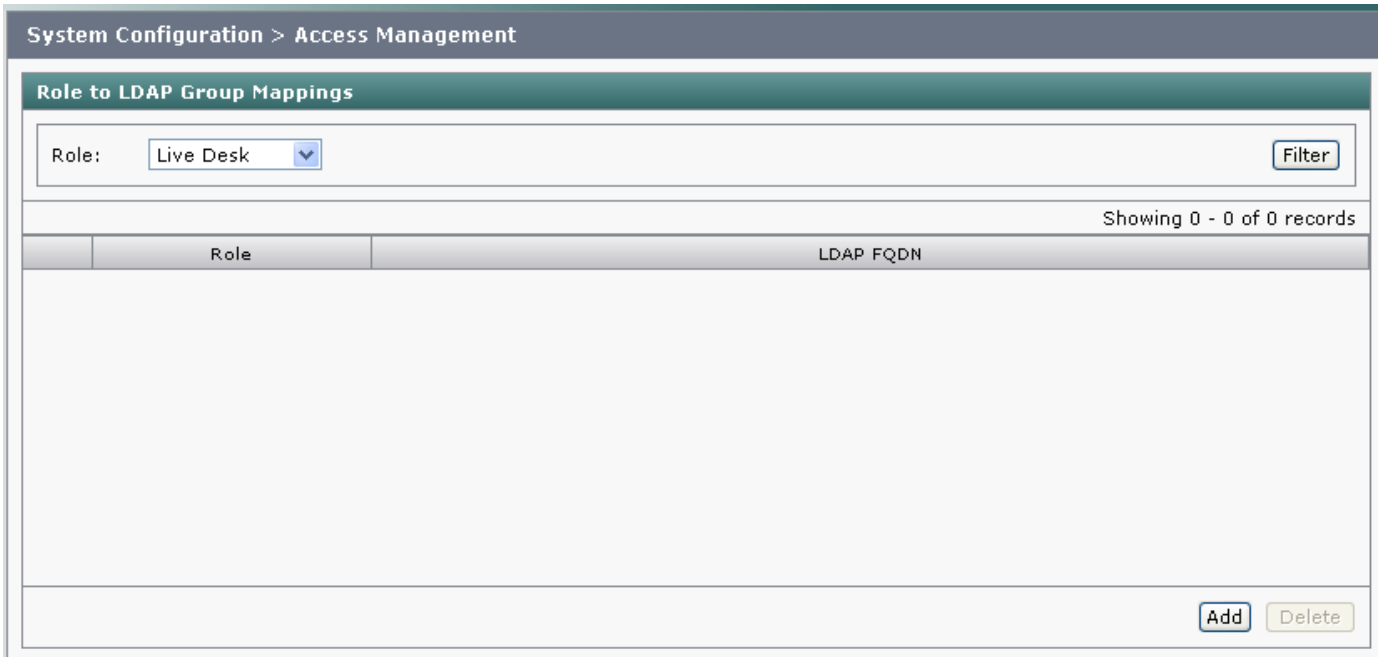
Note Once Interop has been enabled (see Application Settings), a CTMS device can only be added to CTS-Manager if it is interop-ready. An interop-ready device is defined as running a certain level of software release.

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



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

Adding a CTMS

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

Figure 9-25 Adding New CTMS - MCU Devices Window

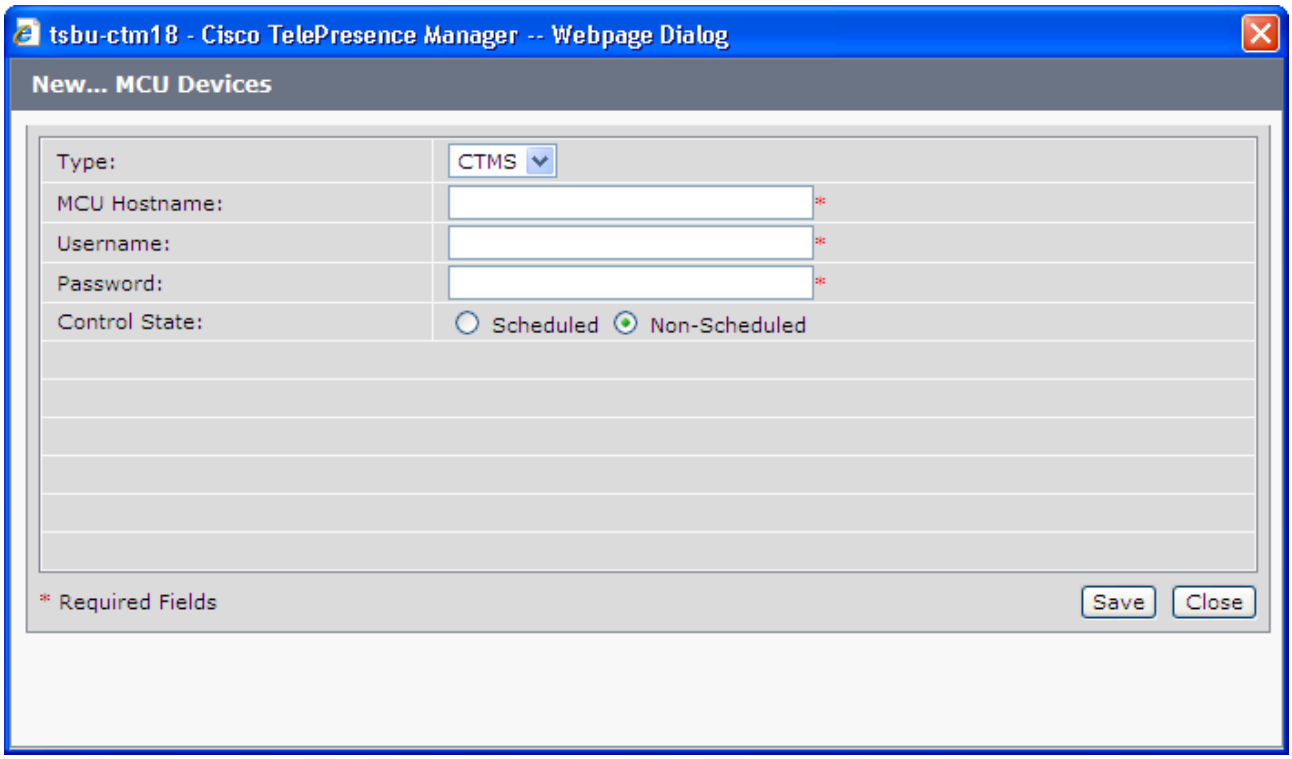


Table 9-21 describes the fields in the New MCU Devices window.

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

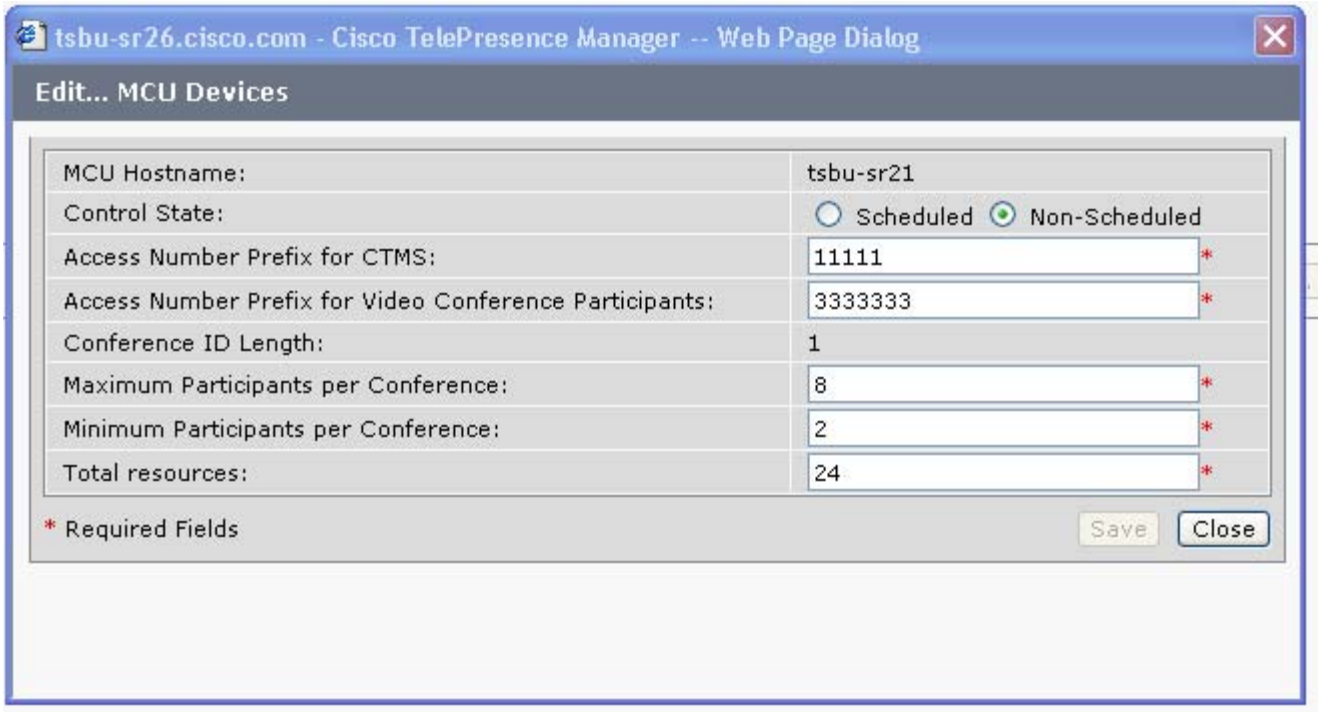


Table 9-22 describes the fields in the Edit MCU Devices window.

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.
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.
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.

Table 9-24 Editing Registered CUVC Configuration Settings (continued)

Field	Description or Settings
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:

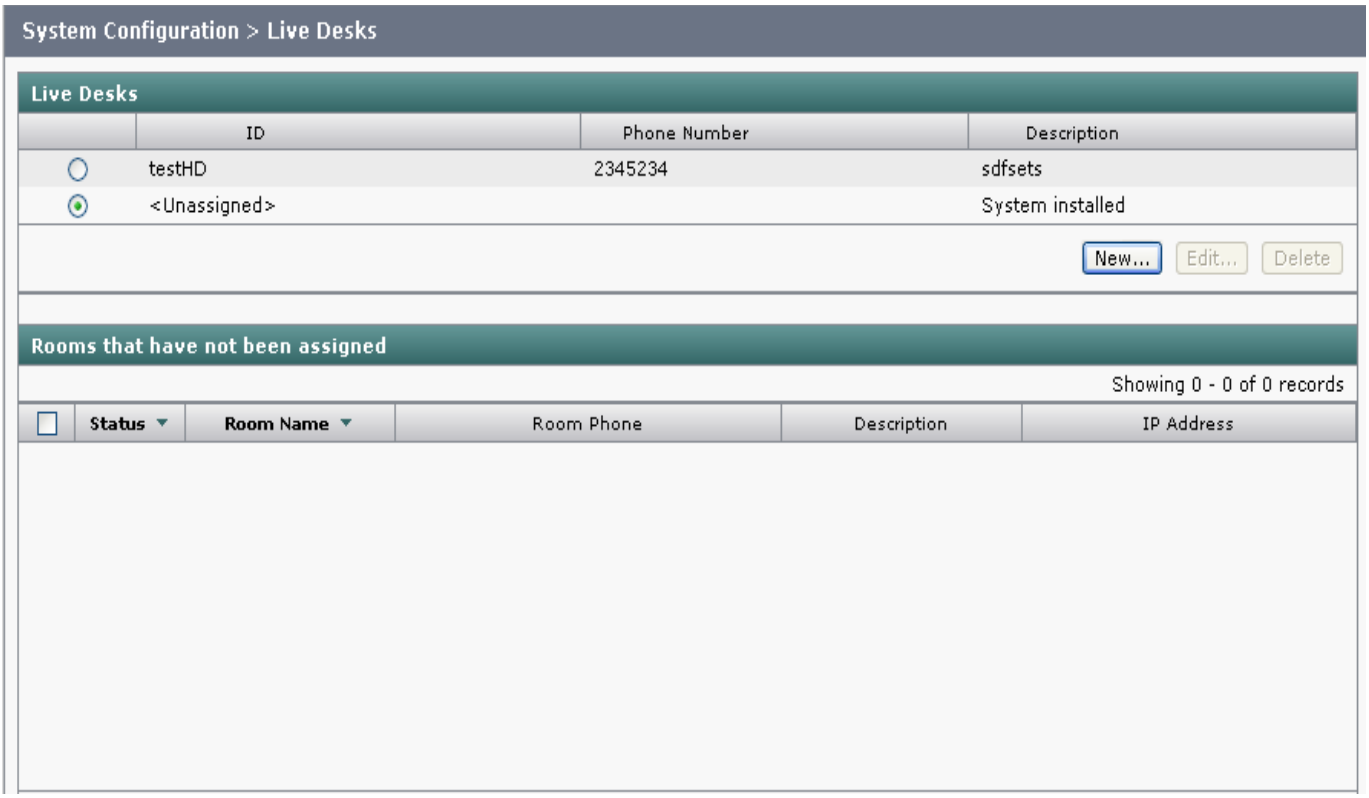
- Scheduling meetings
- Using the Cisco IP phone in a Cisco TelePresence-enabled meeting room
- Using the tools supplied by the CTS-Manager to monitor the system and the schedule of upcoming meetings and to update meeting requests
- Gathering data to supply to the administrator when a problem cannot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



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

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.

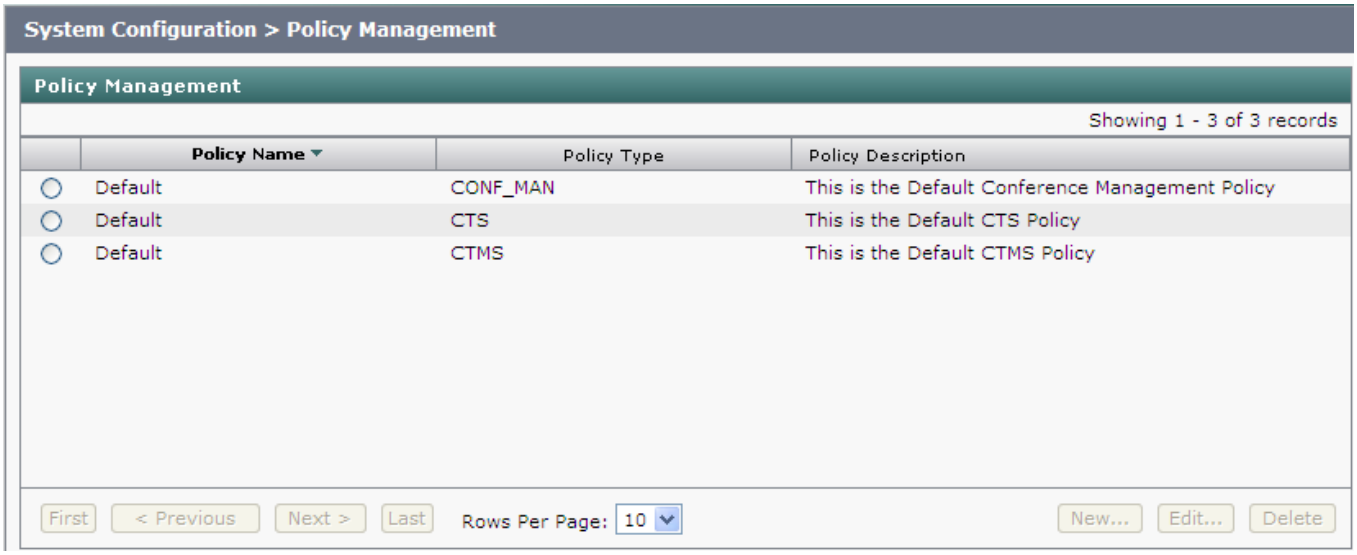
Step 6 To delete a Live Desk, select the radio button next to the Live Desk ID and click **Delete**.

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:

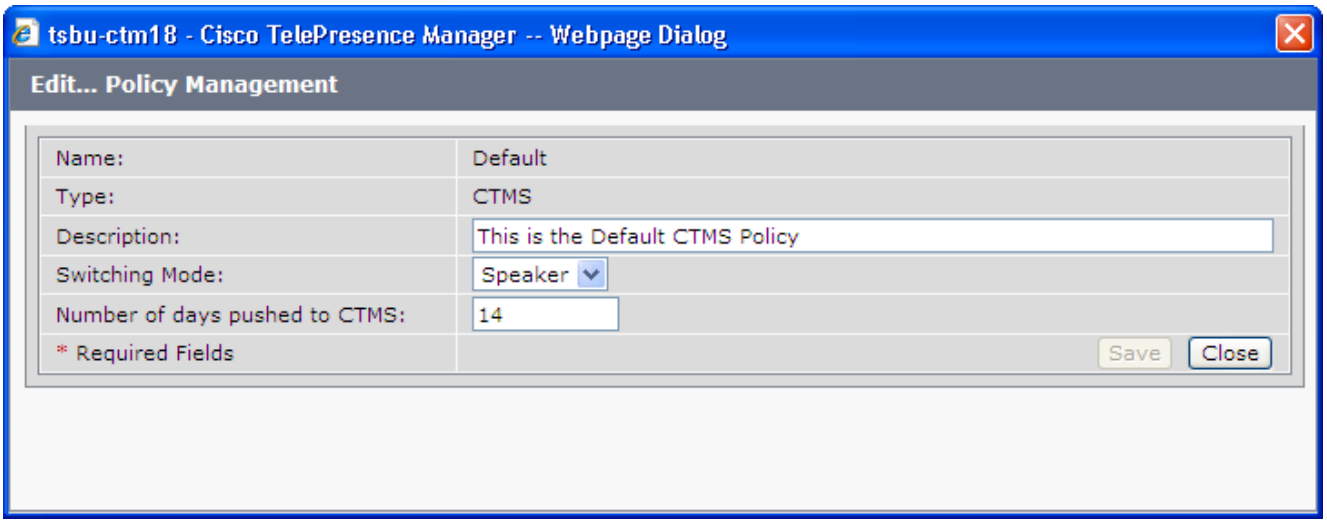
Figure 9-29 System Configuration - Policy Management Window



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.

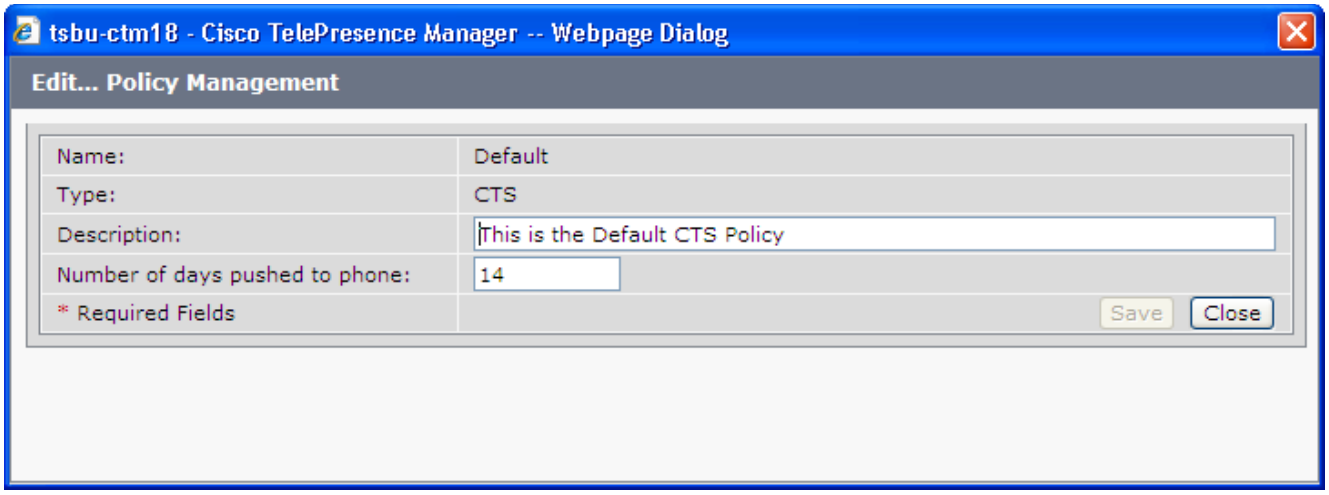
Figure 9-30 CTMS Policy Window



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



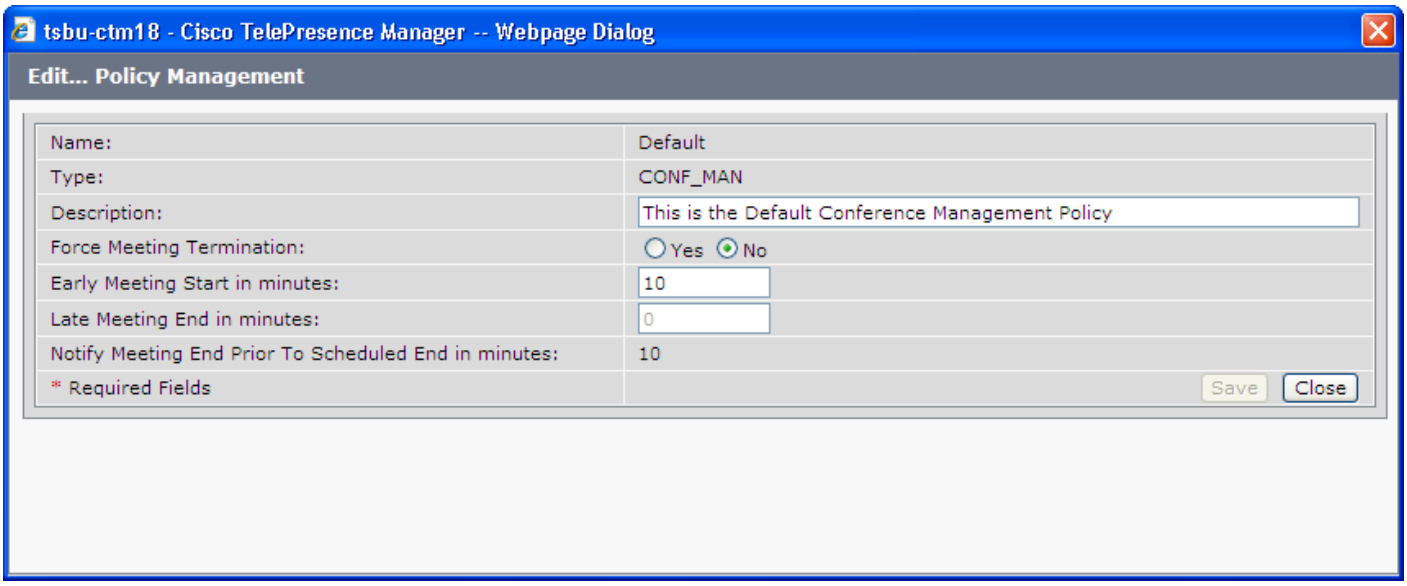
Conference Manager policy

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

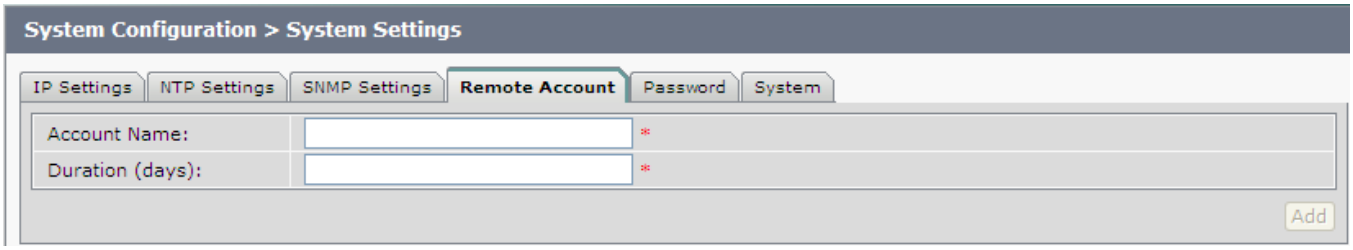


Remote Account

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



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.

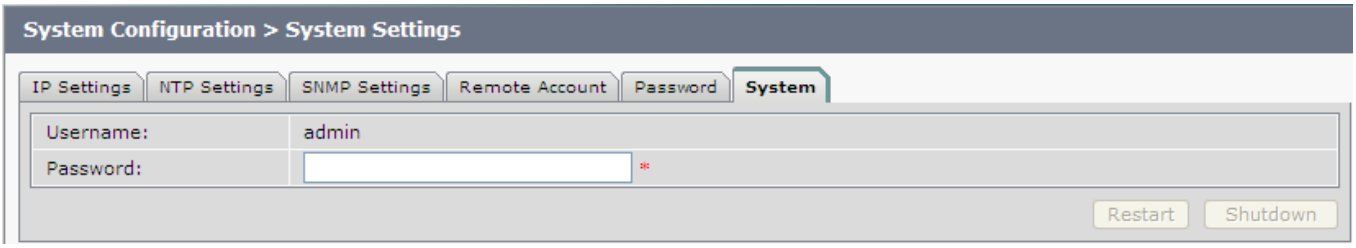
To complete this process, the account name and pass phrase are entered into a utility at the following Cisco Internal web site:
https://remotesupporttool.cisco.com/logon.php

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



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

- The username cannot be changed.

Step 2 Enter your password.

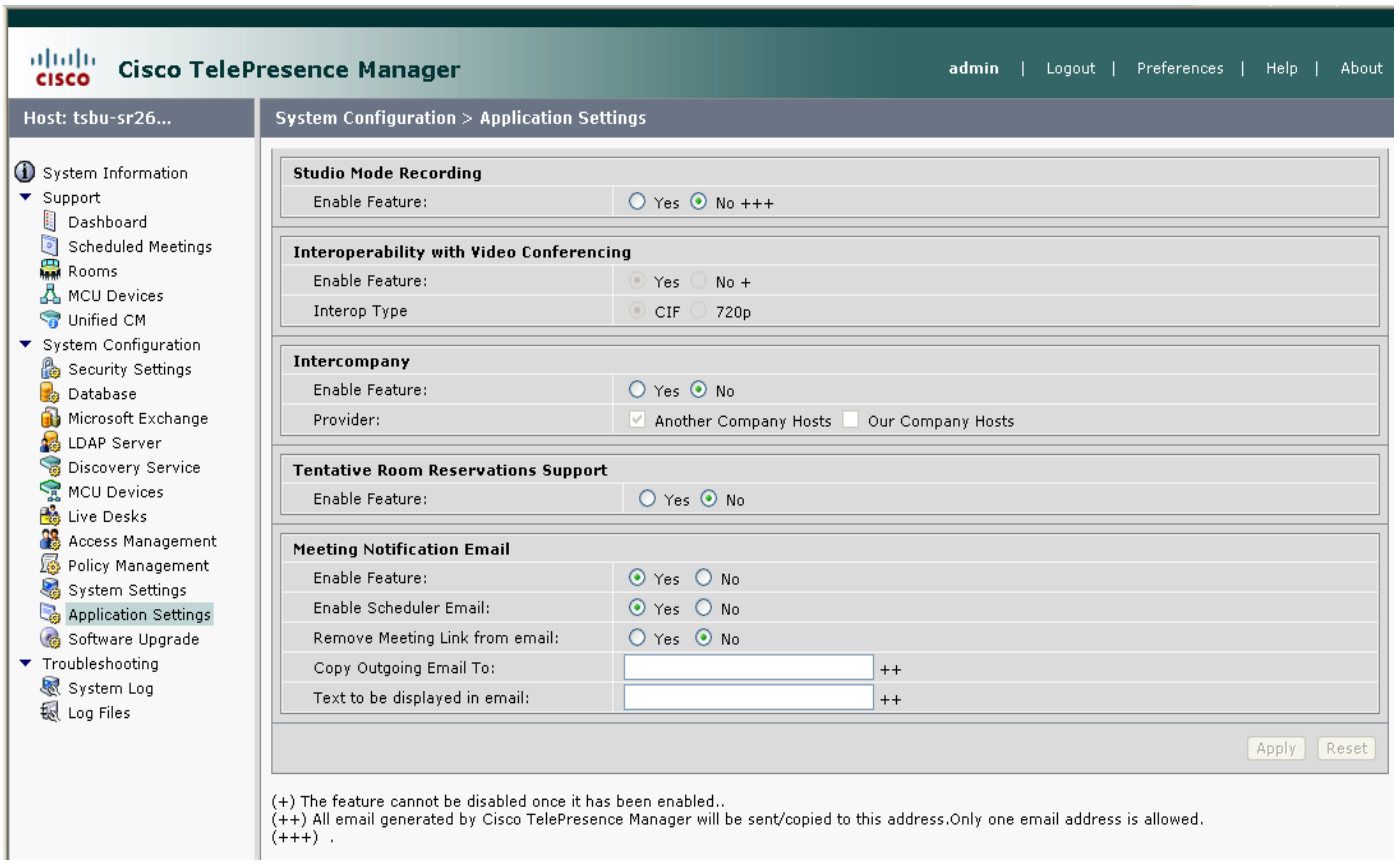
Step 3 Click on **Restart**.

This will restart the CTS-Manager system.

Application Settings

The System Configuration Applications Settings window is used to set 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



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.

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 a room call it sill 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.

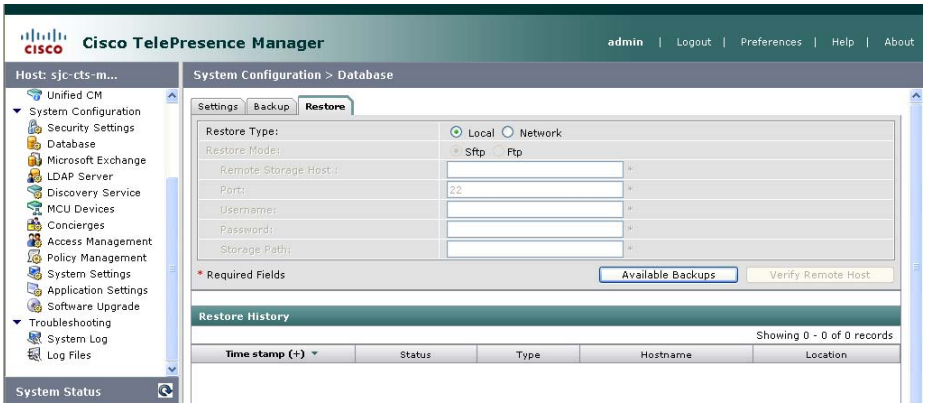
Note It is recommended to use the same hostname and the same IP address for CTS-Manager replacement server.

CTS-Manager Failover Procedure

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

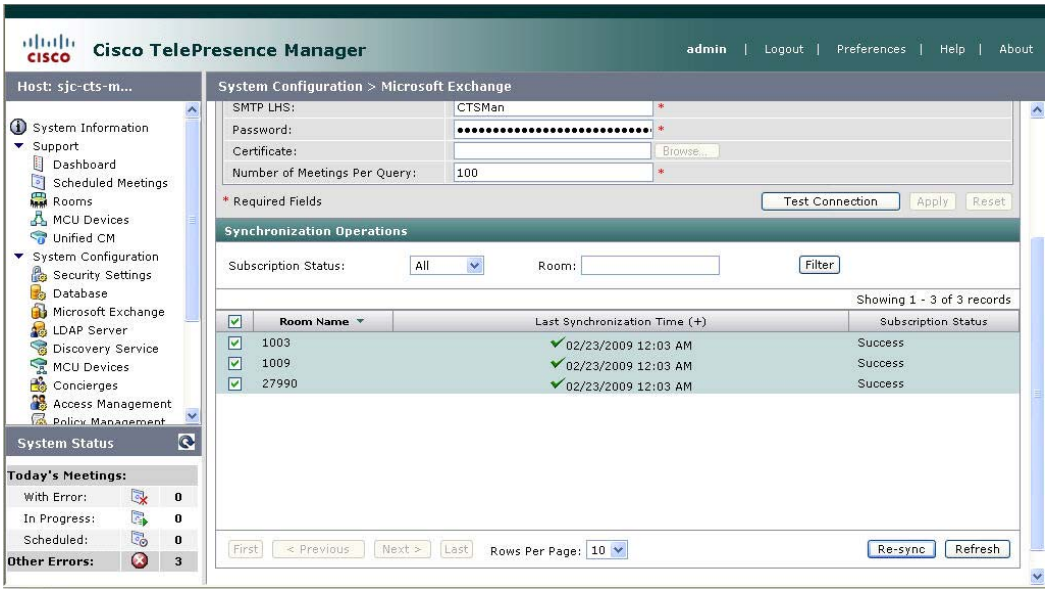
- To start the failover procedure, power off the primary CTS-Manager system.
- Power on the backup CTS-Manager system.
- Restore the last CTS-Manager database to the backup CTS-Manager, click **Available Backups** to complete this task

Figure 9-36 System Configuration Database Restore Backup Window



- 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



- 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:

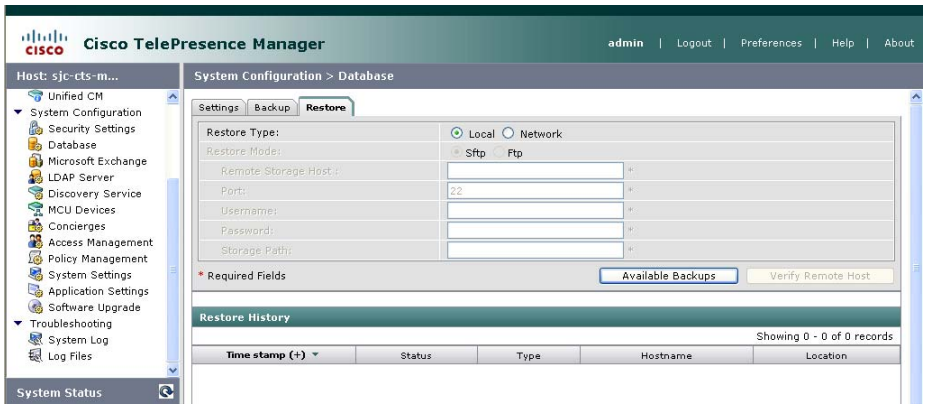
Step 1 To start the failover procedure process, power off the primary CTS-Man.

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.

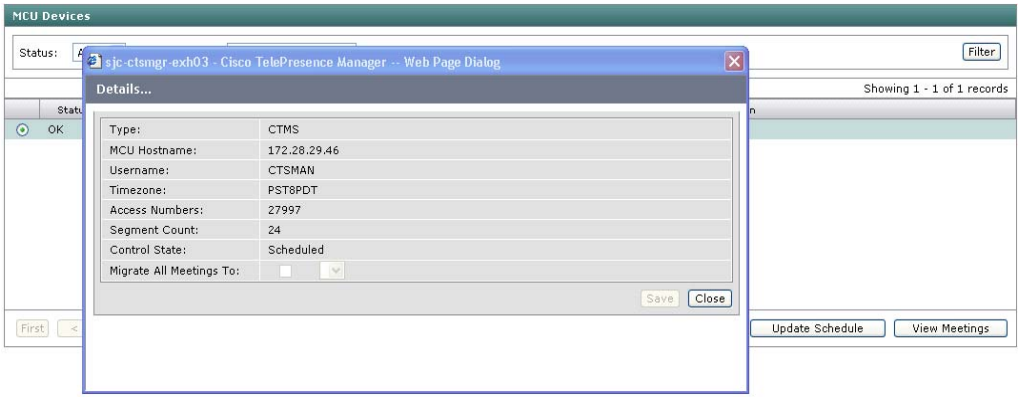
Figure 9-38 System Configuration Database Restore Backup Window



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



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

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.

.

CHAPTER 10

Monitoring Cisco TelePresence Manager

Revised: Nov 13, 2009, OL-13673-06

Contents

Introduction

System monitoring tasks consist primarily of monitoring and updating meeting schedules and monitoring the status of rooms and system services.

Post-Install Guidelines for CTS-Manager

The purpose of this guide is to outline the information you will need to reference in order to continue 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.

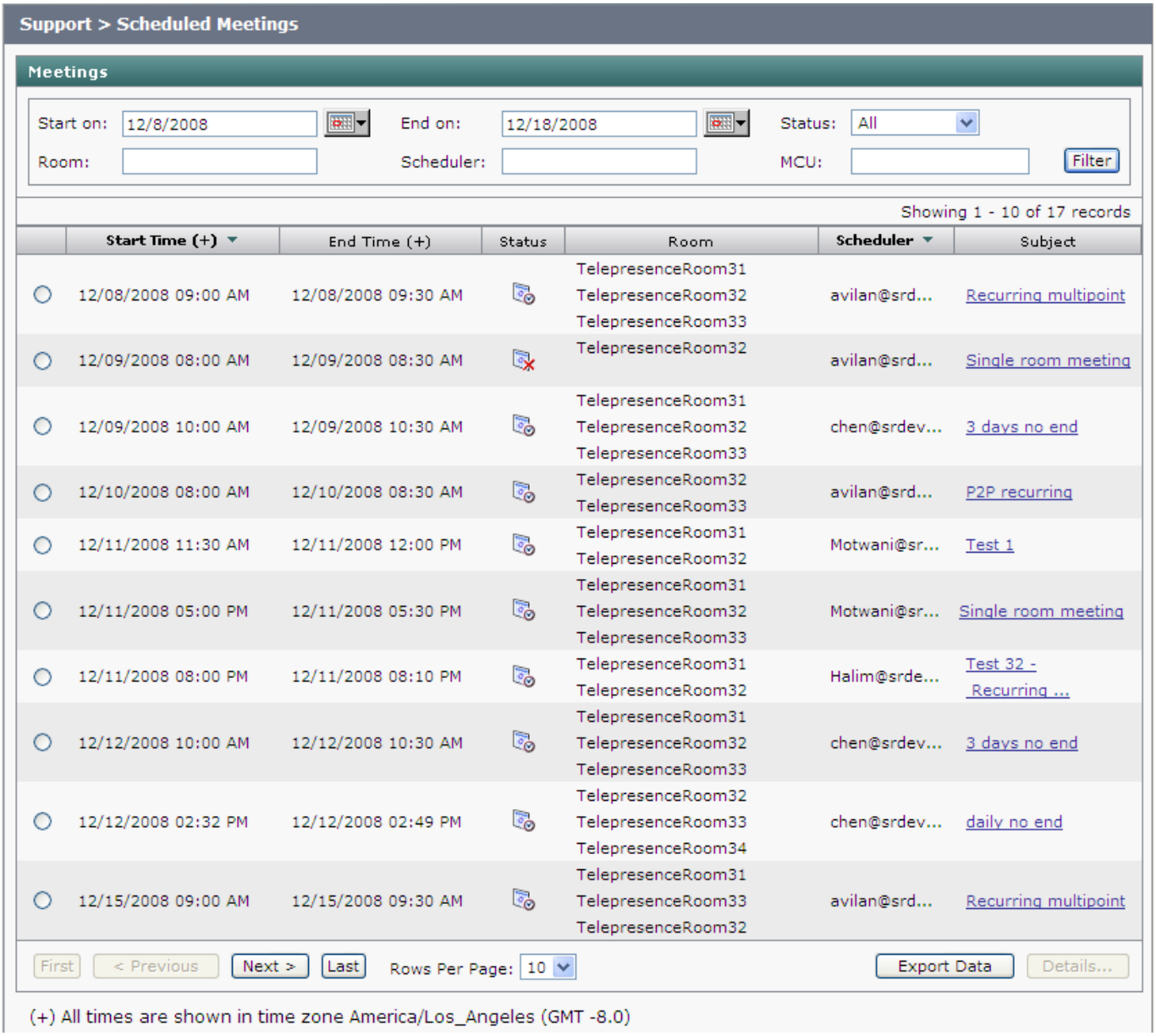
Table 10-1 Post-Install Guidelines for Configuring CTS-Manager

Configuring Procedures Guidelines after Installing CTS-Manager	Description	Location
Monitoring CTS-Manager	Describes the support features available when you log into CTS-Manager using a Live Desk role.	Current Chapter
CTS-Manager Emails and End-User Web UI	The Calendar service (either Microsoft Exchange or IBM Domino) sends an acceptance email to the meeting organizer, with the notice that the rooms have been reserved and placed on the calendar. CTS-Manager also sends either a Confirmation email or an Action Required email to the meeting organizer when a meeting is scheduled	Chapter 11, "CTS-Manager Emails and End-User Web UI"

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

Scheduled Meetings

Figure 10-1 Scheduled Meetings window



When a Cisco TelePresence meeting is scheduled using Microsoft Outlook or IBM Lotus Notes, an e-mail is generated to confirm the meeting and provide a link to meeting details. The CTS-Manager must be reachable from an Exchange Server for Meeting Notification to work.

Note When filtering for a room, a maximum of 5 concurrent users is supported.

The Scheduled Meetings window provides another way to view and modify meeting details.

In the current version of CTS-Manager, it is possible to search from 1 to 15000 meeting records.

Note If meetings do not show up automatically on CTS-Manager, then you need to do a manual sync. Make sure from the Exchange server that you can ping the CTS-Manager hostname.

Process/Response Times for Scheduled Meetings

Microsoft Exchange or IBM Domino calender servers typically confirm a meeting request within one minute if all the affected meeting rooms are in auto-accept mode. A meeting room in proxy mode must have a delegate respond to a meeting invite. This can affect the response time for a scheduled meeting. Once all room reservations are confirmed the meeting should appear in the Scheduled Meetings window and the phone UI within 15 minutes. If email alerts are turned on, confirmation or error emails are generated and sent within 10-15 minutes.

Modifying Meeting Details from a Calendar Client

- If a meeting organizer updates the Subject field of a meeting scheduled with Lotus Notes that has already been sync'd with CTS-Manager, the update is not reflected in phone user interface.
- If a meeting is modified within a few minutes of the meeting's starting time (such as a time change, or room change), the modification may not appear on the room phone screen or in the Cisco TelePresence Manager's Scheduled Meetings window. This does not affect any user's ability to schedule a new meeting at the original time (pre-modified) time.
- A notification email is not generated if a meeting is processed as part of a server startup.

Note A tentative room meeting process in CTS-Manager does not work for the Domino Calendar server at this time.

Calendar Scheduling Limitation

CTS-Manager only displays endpoint scheduling information for a 12 month window. If a meeting organizer schedules a recurring meeting with meeting instances that extend outside this window, those meeting instances are added to the CTS-Manager database as the calendar date moves forward. If a meeting organizer schedules a future meeting outside the present 12 month window the meeting is not displayed in CTS-Manager until the meeting falls inside the 12 month window.

Generating Scheduled Meeting Reports

You can generate a report about specific scheduled meetings or activity between specific dates by supplying any or all of the following details:

Step 1 Type the meeting room name in the **Room** field.

Step 2 Type the user name of the meeting organizer in the **Scheduler** field.

Step 3 From the **Status** drop-down list, choose the All, Needs Help, With Error, In Progress, Scheduled, Completed, or No Show meeting status.

Note A meeting is in the Needs Help state if the Live Desk soft key on the room phone has been selected.

Step 4 Use the Calendar icon to choose beginning and ending dates, or type the dates in the Start On and End On fields using the MM/DD/YYYY date format.

Step 5 Type the name of the MCU.

Step 6 Click **Filter**.

Table 10-2 describes the Scheduled Meetings information.

Table 10-2 Scheduled Meetings Information

Field	Description or Setting
Start Time	The scheduled starting time for a meeting. Click the arrow in the header of the Start Time column to sort the time from earliest to latest or latest to earliest.
End Time	The scheduled ending time for a meeting.
Status	Meeting status: All, With Error, In Progress, Scheduled, Completed, or No Show.
Room	Meeting room name as specified in the Microsoft Exchange or IBM Domino database.
Scheduler	Login name of the person who scheduled the meeting. Click the arrow in the header of the Scheduler column to sort the list in ascending or descending alphabetical order.
Subject	Information (such as the meeting subject) provided about the meeting.

Note If a meeting does not appear in the list Scheduled Meetings and it is a recurring meeting, check the starting date of the first occurrence of the meeting. If the meeting was scheduled to begin more than two years in the past, reschedule future occurrences.

Exporting Scheduled Meeting Data

You can use the **Export Data** button to export your scheduled meeting data to a tab-separated values (.tsv) file. The meeting data exported includes the meetings appearing in the Scheduled Meetings window.

Use the filter to display only the scheduled meetings you want to export. You can export as many as 500 meetings. The exported data file is a tab-delimited text file.

Figure 10-2 Viewing Exported Scheduled Meeting Data

	A	B	C	D	E	F	G	H
1	**Start Time [Start on: 2/10/2009]**	**End Time [End on: 02/13/2009]**	**Instance Type**	**Status [Matches: All]**	**Room [Matches: All]**	**Scheduler [Matches: All]**	**Subject**	**MCU [Matches: All]**
2	2/10/2009 10:00	2/10/2009 10:30	Recurring Meeting (Instance)	No Show	TelepresenceRoom31 || TelepresenceRoom32 || TelepresenceRoom33	chen@srdev.com	3 days no end	
3	2/10/2009 11:00	2/10/2009 11:30	Single	Scheduled	TelepresenceRoom32 || TelepresenceRoom31	superuser@srdev.com	Testing again	
4	2/10/2009 15:00	2/10/2009 15:30	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom32 || TelepresenceRoom31	shrivastava@srdev.com	more than 800 occurrences	
5	2/11/2009 15:00	2/11/2009 15:30	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom31 || TelepresenceRoom32	shrivastava@srdev.com	more than 800 occurrences	
6	2/12/2009 11:30	2/12/2009 12:00	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom31 || TelepresenceRoom32	Motwani@srdev.com	Test 1	
7	2/12/2009 15:00	2/12/2009 15:30	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom32 || TelepresenceRoom31	shrivastava@srdev.com	more than 800 occurrences	
8	2/12/2009 17:00	2/12/2009 17:30	Recurring Meeting (Instance)	With Error	TelepresenceRoom31 || TelepresenceRoom33 || TelepresenceRoom32	Motwani@srdev.com	Recording test - 3 rooms recurring	
9	2/12/2009 20:00	2/12/2009 20:10	Recurring Meeting (Instance)	With Error	TelepresenceRoom31 || TelepresenceRoom32	Halim@srdev.com	Test 32 - Recurring weekly no end date with 2 rooms	
10	2/13/2009 10:00	2/13/2009 10:30	Recurring Meeting (Instance)	With Error	TelepresenceRoom31 || TelepresenceRoom33 || TelepresenceRoom32	chen@srdev.com	3 days no end	
11	2/13/2009 14:32	2/13/2009 14:49	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom33 || TelepresenceRoom32	chen@srdev.com	daily no end	
12	2/13/2009 15:00	2/13/2009 15:30	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom32 || TelepresenceRoom31	shrivastava@srdev.com	more than 800 occurrences	
13								
14	Report generated at: Tuesday, February 10, 2009 11:01 AM (America/Los_Angeles)							
15	Report generated by: admin							
16	Report generated from: tsbu-ctm18							
17	All times are shown in time zone: America/Los_Angeles							

Meeting Details

To see meeting details, click the radio button next to a scheduled meeting and click **Details**.

For more information about the Meeting Details window refer to Chapter 11, "CTS-Manager Emails and End-User Web UI".

Rooms

Choose Rooms to display information about the Cisco TelePresence meeting rooms. The Rooms Support window is divided into three, tabbed views.

- The **Summary** view displays the status of all the Cisco TelePresence rooms registered with Cisco TelePresence Manager. Table 10-3 on page 10-8 describes information in this window.

- The **Status** view displays the different error types for Cisco Unified CM, each Cisco TelePresence System registered with Cisco TelePresence Manager, and Microsoft Exchange or IBM Domino connection errors. Table 10-4 describes information in this window.
- The **Capability** view displays the availability of certain Cisco TelePresence features. Table 10-5 describes information in this window.

Generating Room Reports

You can generate a report about specific meeting rooms and meeting status, as follows:

Step 1 Choose the status—All, OK, Error, Needs Help, or In Use—from the **Status** drop-down list.

Note A room is in the Needs Help state if the Live Desk soft key on the room phone has been selected.

Step 2 Type the meeting room in the **Room** field.

Step 3 Click **Filter**.

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.

Figure 10-3 Room Window Summary Tab

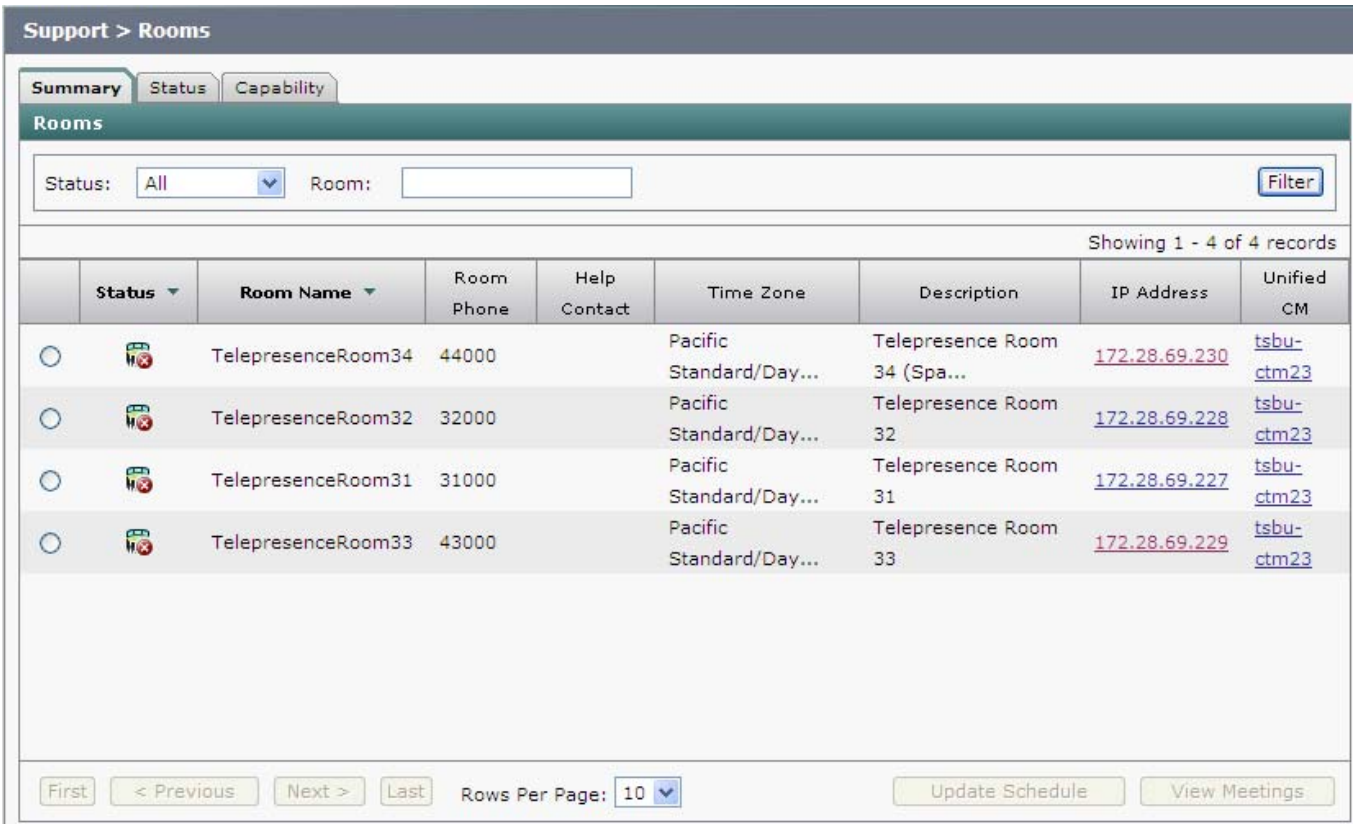


Table 10-3 Room Summary

Field	Description or Setting
Status	Room status: All, OK, Error, Needs Help, or In Use. Click the arrow in the header of the Status column to sort the list in ascending or descending alphabetical order.
Room Name	Meeting room name.
Room Phone	Meeting room telephone number.
Help Contact	Live Desk who is assigned to the room.
Time Zone	Displays the Time Zone location of the endpoint.
Description	Meeting room description. If text is truncated in this field, move your mouse pointer over the text to see the entire description.
IP Address	IP address of the Cisco TelePresence System. Click the address to go to the Cisco TelePresence System Administration login page.
Cisco Unified CM	IP address of Cisco Unified CM Click the address to go to the Cisco Unified CM Administration login page.

Manually Updating Room Schedules on the Cisco TelePresence Room Phone

To update a room's IP phone with what is currently scheduled in the Microsoft Exchange or IBM Domino database, perform the following steps:

Step 1 Click the radio button associated with a room.

Step 2 Click **Update Schedule**.

Viewing Scheduled Meetings for a Specific Room

To obtain additional information about any meetings associated with a room, perform the following steps:

Step 1 Click the radio button associated with a room.

Step 2 Click **View Meetings**.

Figure 10-4 Room Window Status Tab

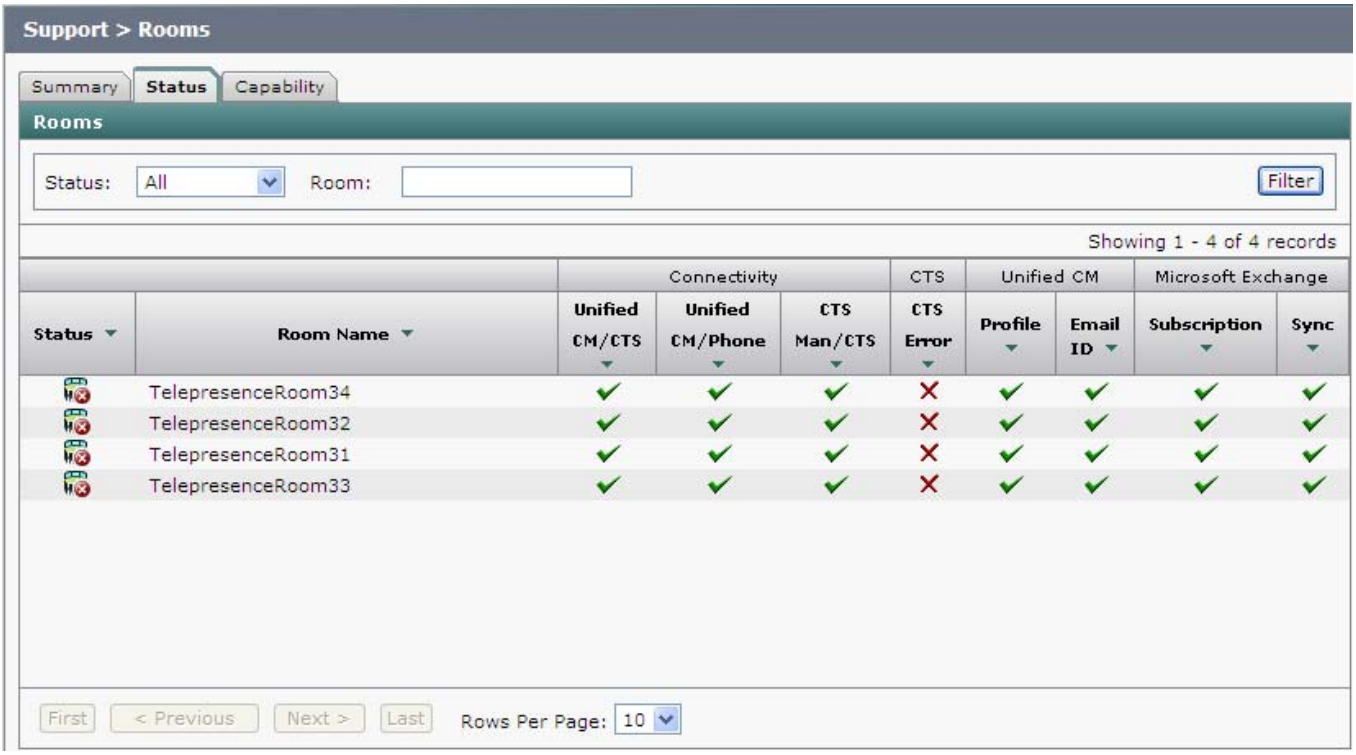


Table 10-4 Room Status

Field	Description or Setting
Status	Room status: All, OK, Error, Needs Help, or In Use. Click the arrow in the header of the Status column to sort the list in ascending or descending alphabetical order.
Room Name	Meeting room name.
Connectivity	
Cisco Unified CM/CTS	An **X** indicates a problem with the connection between Cisco Unified CM and the Cisco TelePresence room.
Cisco Unified CM/Phone	An **X** indicates a problem with the connection between Cisco Unified CM and the IP phone in the TelePresence meeting room.
CTS Man/CTS	An **X** indicates a problem with the connection between the Cisco TelePresence Manager and the Cisco TelePresence room.
CTS	
CTS Error	An **X** indicates a communication problem between the Cisco TelePresence meeting room and Cisco Unified CM.
Cisco Unified CM	
Profile	An **X** indicates a problem with the Cisco TelePresence System user profile stored in Cisco Unified CM.
Email ID	An **X** indicates a problem with the Cisco TelePresence System email ID stored in Cisco Unified CM.
Microsoft Exchange	
Subscription	An **X** indicates a subscription problem between the TelePresence meeting room and Microsoft Exchange. **Note** A subscription error may be indicated by an **X** when there is no error. This can be caused when an invalid email address is assigned in Unified CM, that does not match the email address in Microsoft Exchange.
Sync	An **X** indicates a synchronization problem between the room and Microsoft Exchange.
IBM Domino	
Subscription	An **X** indicates a polling problem between the TelePresence meeting room and the Domino server **Note** A subscription error may be indicated by an **X** when there is no error. This can be caused when an invalid email address is assigned in Unified CM, that does not match the email address in IBM Domino.
Sync	An **X** indicates a synchronization problem between the TelePresence meeting room and the Domino server.

Figure 10-5 Room Window Capability Tab

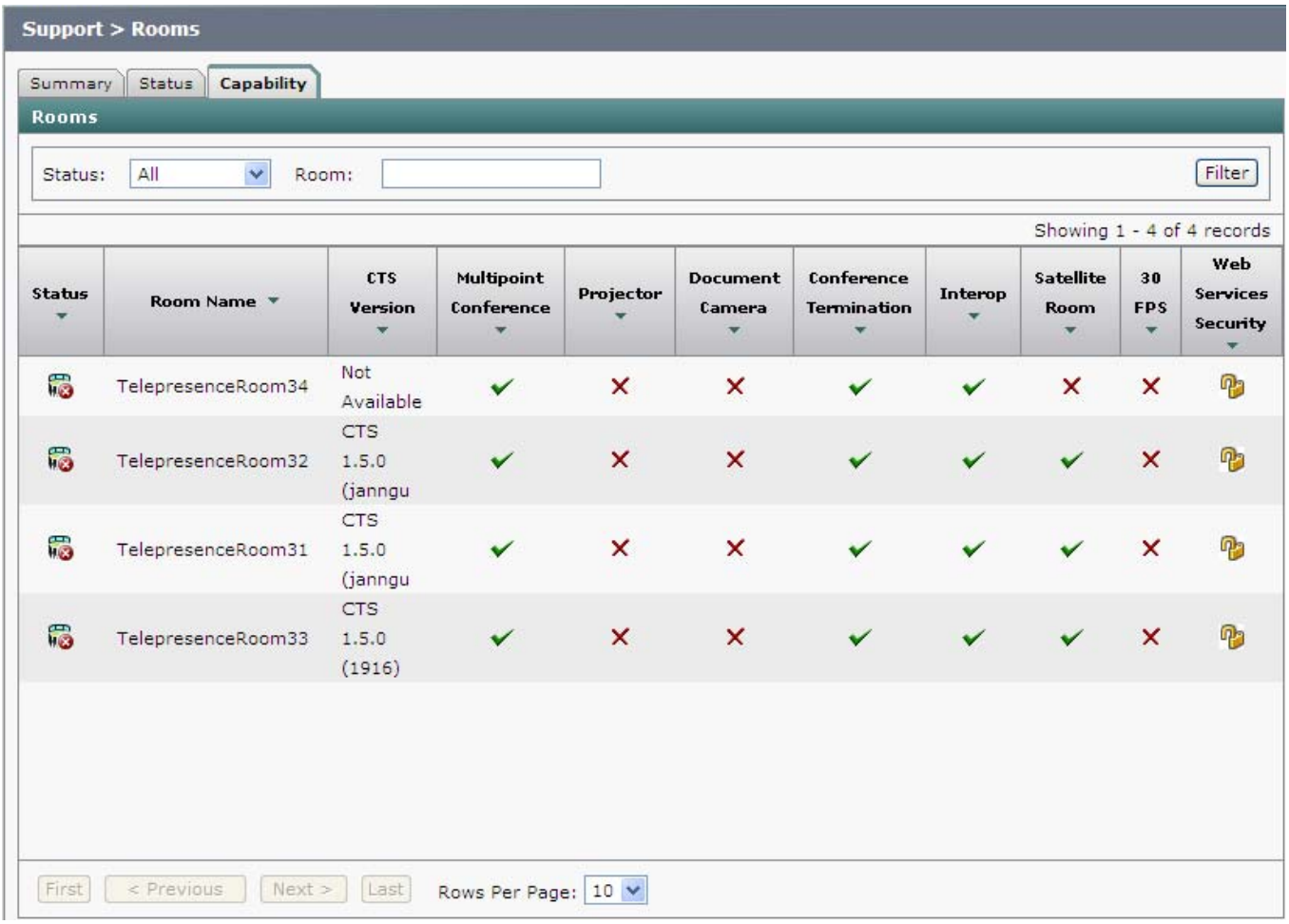


Table 10-5 Room Capability

Field	Description or Setting
Status	Room status: All, OK, Error, Needs Help, or In Use. Click the arrow in the header of the Status column to sort the list in ascending or descending alphabetical order.
Room Name	Meeting room name.
CTS Version	Displays the software release version for the CTS endpoint. **Note** Versions of CTS prior to 1.5 only display "Not Available" in this field. This does not affect any functionality.
Multipoint Conference	A check specifies the endpoint supports multipoint meetings.
Projector	A check specifies the endpoint includes a working projector.
Document Camera	A check specifies a document camera is installed.
Conference Termination	A check specifies the endpoint supports conference termination. Refer to in Monitoring Cisco TelePresence Manager for more information about conference termination.
Interop	A check specifies the endpoint supports Interop calls.

Table 10-5 Room Capability (continued)

Field	Description or Setting
Satellite Room	A check specifies the endpoint is using a satellite connection.
30 FPS	A check specifies the endpoint supports 30 frames per second data streaming for presentations.
Web Services Security	A check specifies the endpoint supports HTTPS communications.

Room Subscription - Synchronization Change

As shown in the Room Capability, a room was successfully synchronized sometime in the past. Then the Room Capability is changed, i.e., recording disabled. If performing a Discovery on this change, the result is the room subscription shows error, but the synchronization is in ok state. The synchronization status has historical value as it shows the result of the last synchronization on that room which was successful in this case.

If a new cluster is added which has devices which are not Interop or Recording capable, then both the subscription and the synchronization will show error status.

MCU Devices

The MCU Devices (Multipoint Conference Unit) 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).Specifying a CUVC as Non-Scheduled means the CUVC will not be used when a meeting is scheduled.

A CTMS communicates with Cisco TelePresence Manager. Cisco TelePresence Manager provides the scheduling information to the different CTMSs and each CTMS provides the multipoint switching capabilities for the conference. For information about CUVC configuration, see Cisco Unified Communications Manager in the section following the MCU information.

The support MCU Devices window is described in two sections, one for Summary and one for Capability:

Summary Tab

The Summary tab lists the MCU devices associated with CTS-Manager.

Generating Multipoint Conference Unit Reports

You can generate a report about specific MCU devices with the following steps:

Step 1 Choose the status—All, OK, or Error—from the **Status** drop-down list.

Step 2 Type the MCU Hostname in the **MCU** field.

Step 3 Click **Filter**.

Step 4 Select a MCU and click **Details** to display a detailed report about the MCU device.

Step 5 Select a MCU and click **Update Schedule** to send the latest meetings schedule to the MCU.

Note The Update Schedule button is not available when you select a CUVC device, because there is no direct communication between a CUVC and CTS-Manager.

Step 6 Select a MCU and click **View Meetings** to display a list of meetings assigned to that MCU.

Figure 10-6 MCU Window Summary Tab

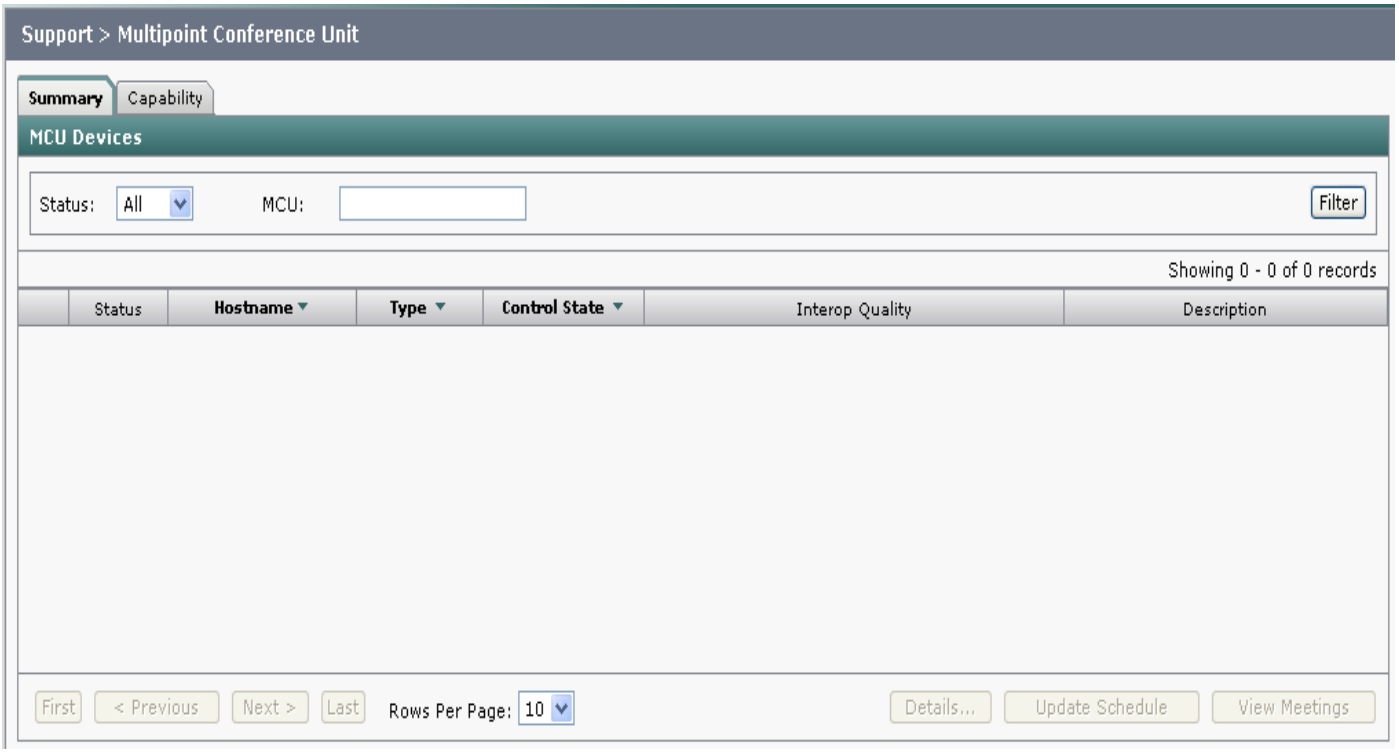


Table 10-6 Support>Multipoint Conference Unit Summary Window

Field	Description or Settings
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
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.

Table 10-6 Support>Multipoint Conference Unit Summary Window

Field	Description or Settings
Control State	The Control State is either Scheduled or Non-Scheduled. If Non-Schedules is listed, the resource allocation function won't be used.
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. CUVS is the default; CTMS is configured in the CTMS program.
Details	Click radio button to select the MCU, then view the details of the MCU.
Update Schedule	Click radio button to select the MCU, then select Update Schedule to get the most current schedule on that MCU.
View Meetings	Click radio button to select the MCU, then view the details of the meeting on that MCU .

Figure 10-7 CTMS Details Window

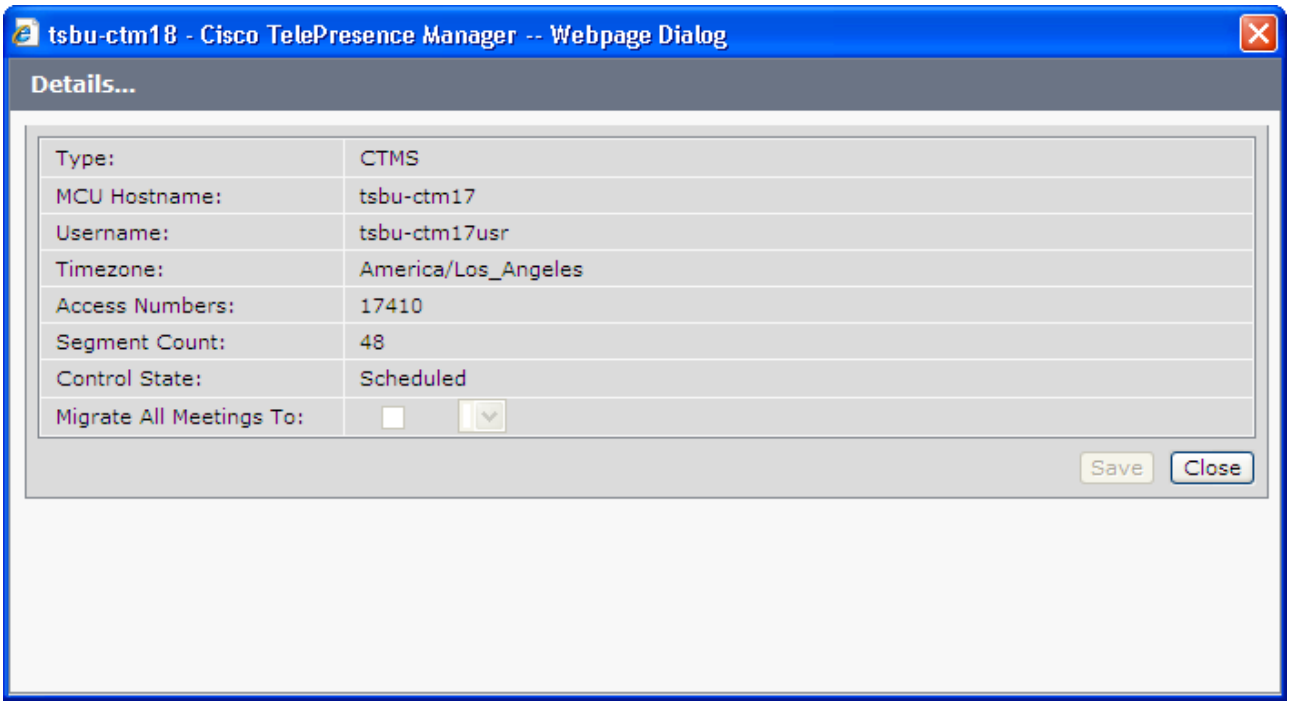


Table 10-7 Details Window for a CTMS

Field	Description or Settings
Type	This is always CTMS.
MCU Hostname	This is the address of the MCU.
Username	Username used to log into the MCU.
Timezone	Displays the timezone where the MCU is located.
Access Numbers	The MCU dial-in phone number.
Segment Count	The number of resources available on the MCU.
Control State	Scheduled or Non-scheduled. A MCU is available for meetings if it is in a Scheduled Control state.
Migrate All Meetings To	All meetings scheduled to use the MCU can be migrated to a Non-scheduled MCU. Click the checkbox and choose another MCU from the drop-down list.

Figure 10-8 CUVC Details Window

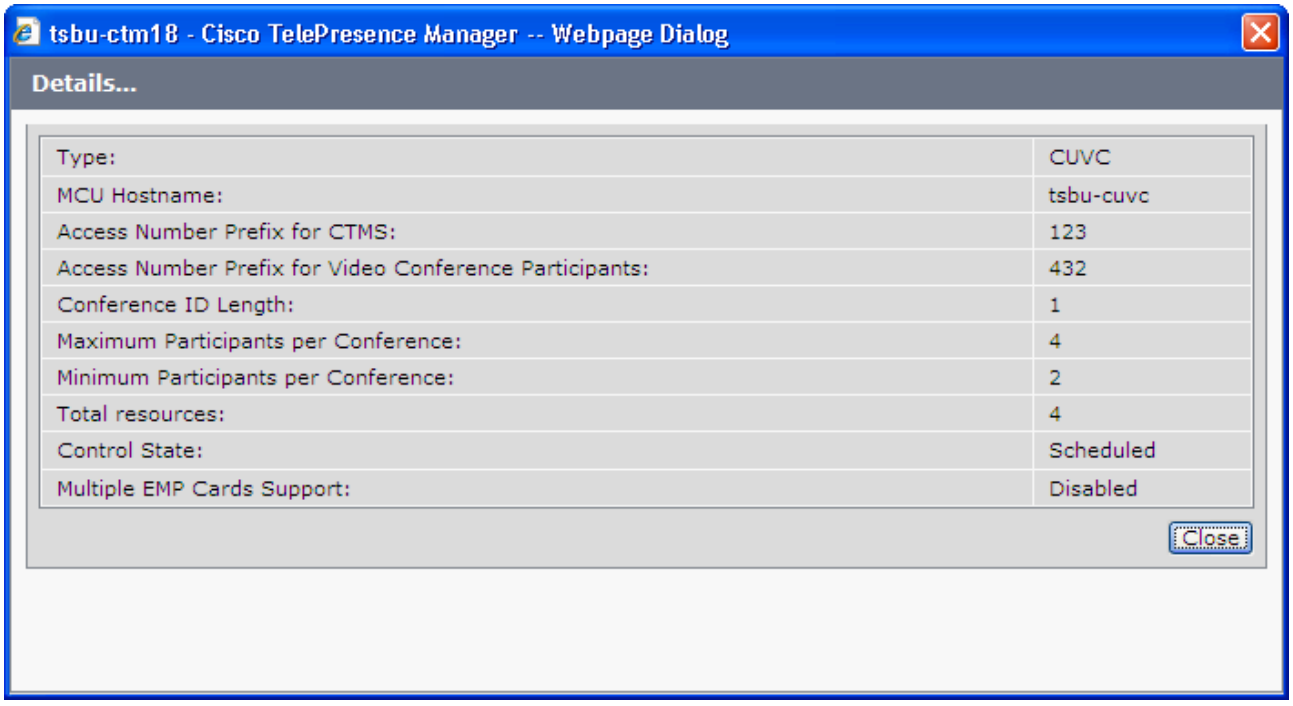


Table 10-8 Details Window for a CUVC

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 Hostname	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.
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.
Field	**Description or Settings**

Capability Tab

The Capability tab identifies the Cisco TelePresence features available for each MCU device, refer to Figure 10-9.

Figure 10-9 MCU Window Capability Tab

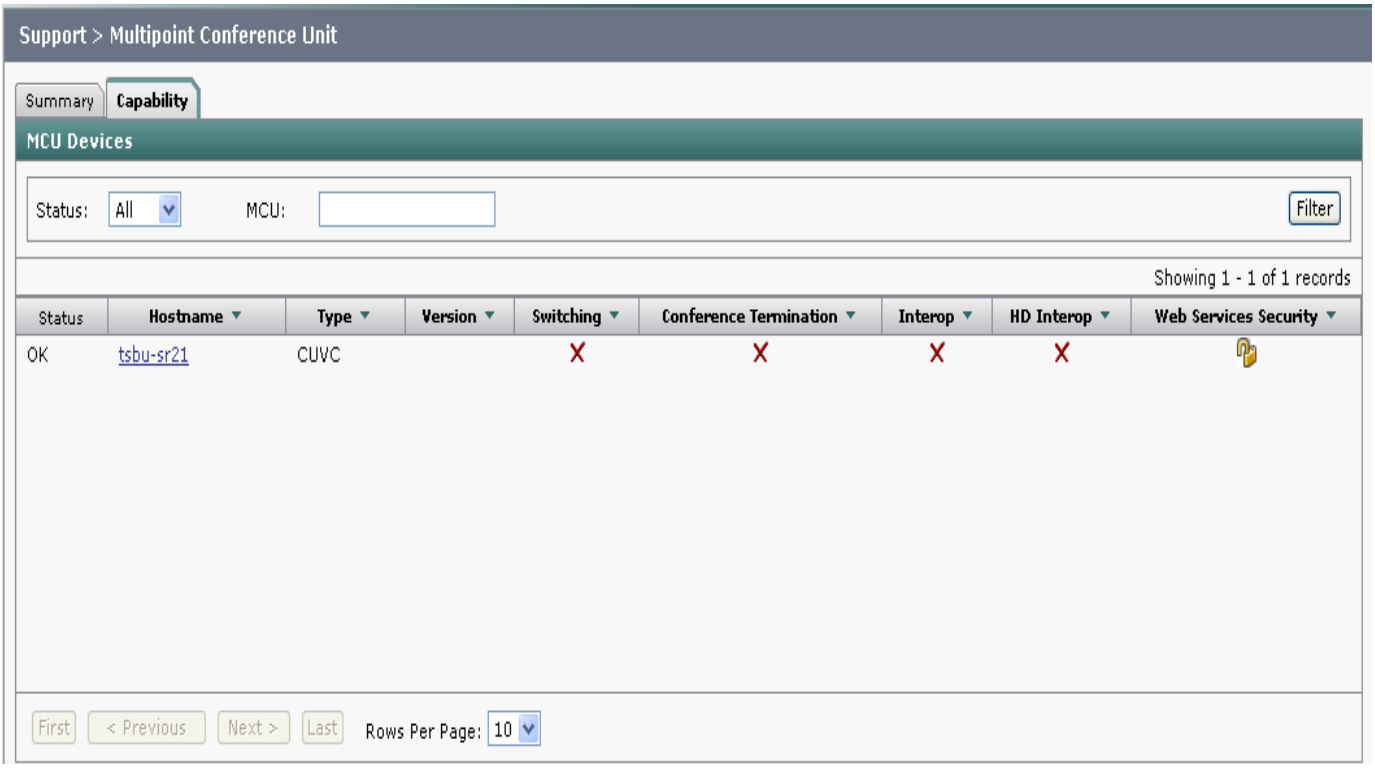


Table 10-9 MCU Capability

Field	Description or Settings
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.
Hostname	The configured hostname for the MCU device. Clicking the hostname hyperlink opens a new browser window, with the CTMS login page.
Type	Identifies the MCU as either CTMS or CUVC.
Version	Displays the software version running on the device. The version is not displayed for the CUVC MCU device type.
Switching	A check specifies the device supports either speaker or room switching.
Conference Termination	A check specifies the device supports conference termination. Refer to Policy Management in Additional Installation Configurations for CTS-Manager.

Table 10-9 MCU Capability

Field	Description or Settings
Interop	A check specifies the device is running a software version that supports CIF video quality. CUVC always shows No for Interop since CTS-Manager does not detect true capability of CUVC.
HD Interop	A check specifies the device is running a software version that supports 720p video quality A check indicates that the video quality of the scheduled meeting is at 720p quality. It doesn't specify that the actual capability that this MCU can support. CUVC always shows No for HD Interop since CTS-Manager does not detect true capability of CUVC.
Web Services Security	A lock specifies the endpoint supports HTTPS communications.

Cisco Unified Communications Manager

To display settings that associate the Cisco TelePresence Manager with Cisco Unified CM, choose Support > Unified CM.

Figure 10-10 Cisco Unified CM Window

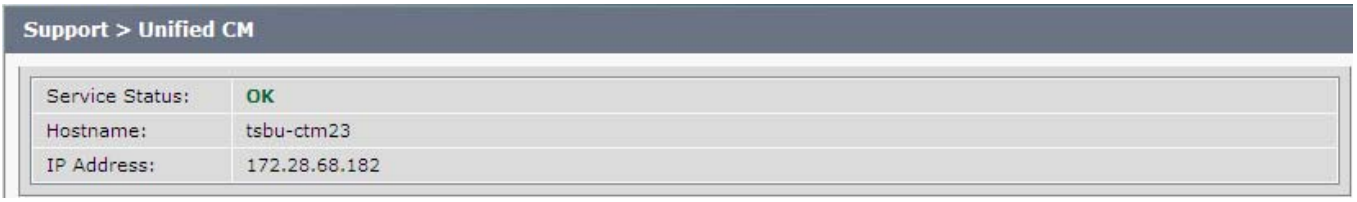


Table 10-10 describes fields and settings for the CUCM

Table 10-10 Cisco Unified Communications Manager Settings

Field	Description or Settings
Service Status	Display-only status report of system services. 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. **Caution** An error status may be reported if the connection to Cisco Unified CM was caused by a network outage. You can remove the error status by clicking Discover Rooms on the System Configuration > Discovery Service page.
Hostname	Name of the Cisco Unified CM server host.
IP Address	IP address of Cisco Unified CM server host.

Command Line Interface

For all commands for the CTS-Manager, refer to the Cisco TelePresence Manager CLI Book set,
http://www.cisco.com/en/US/products/ps7074/tsd_products_support_series_home.html

CHAPTER 11

CTS-Manager Emails and End-User Web UI

Revised: January 28, 2010, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

Cisco TelePresence meetings are scheduled between two or more conference rooms. The Calendar service (either Microsoft Exchange or IBM Domino) sends an acceptance email to the meeting organizer, with the notice that the rooms have been reserved and placed on the calendar. CTS-Manager also sends either a Confirmation email or an Action Required email to the meeting organizer when a meeting is scheduled.

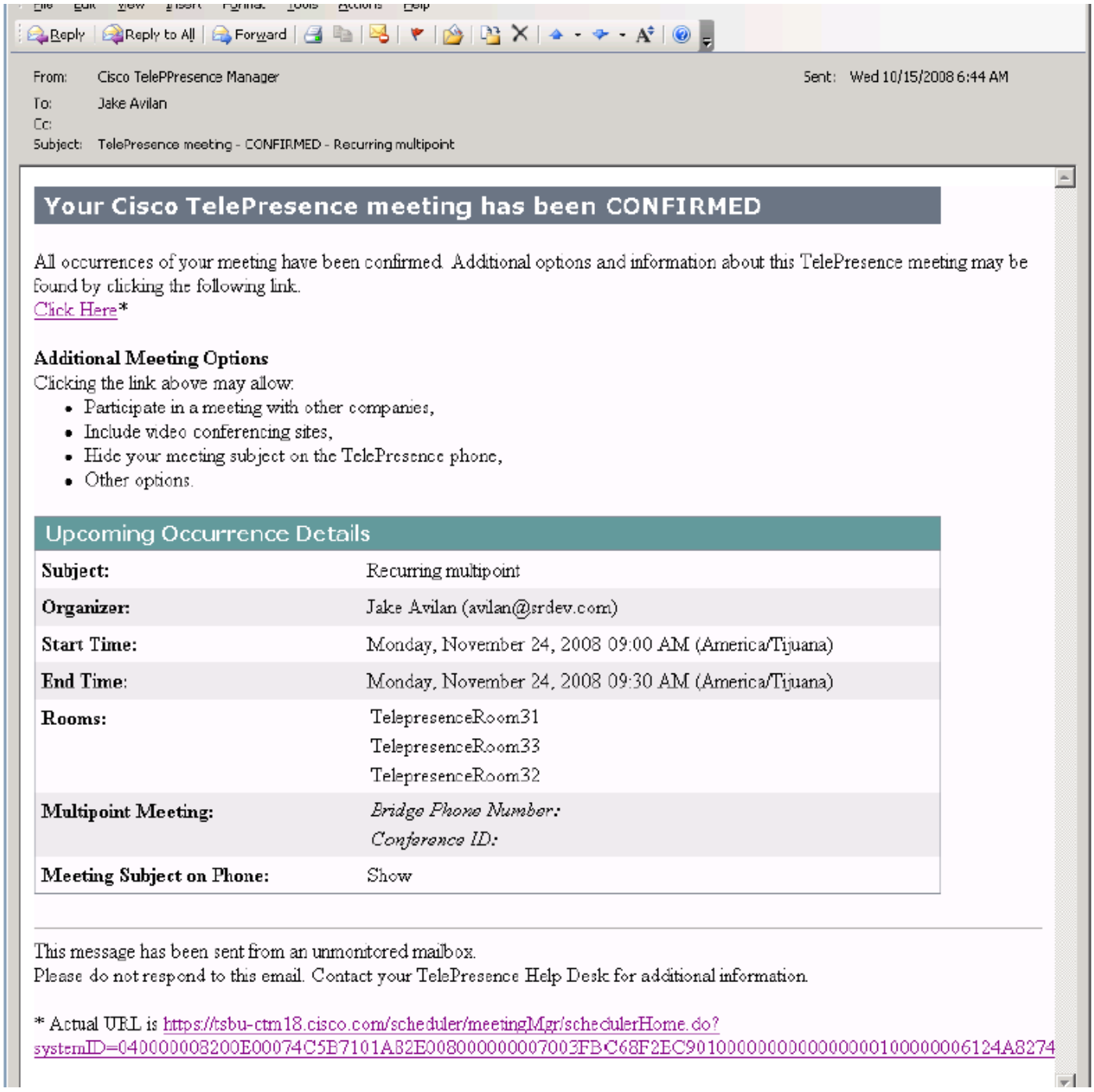
The Confirmation email provides additional information about the scheduled Cisco TelePresence meeting, including a link to the CTS-Manager Meeting Details window. In order to access the Meeting Details window the meeting organizer must log into CTS-Manager using their Windows logon account (account name and password). For more information about Confirmation emails refer to the Point-to-Point Meetings and Multipoint Meetings sections below. For more information about the CTS-Manager Meeting Details window refer to the section Confirmation Meeting Details Window.

The Action Required email specifies the error that caused the email to be generated, and a link to the Meeting Details window.

Point-to-Point Meetings

The Point-to-Point meeting confirmation email is described in Table 11-1.

Figure 11-1 Point to Point Meeting Confirmation Email



Reply | Reply to All | Forward

From: Cisco TelePPresence Manager
Sent: Wed 10/15/2008 6:44 AM
To: Jake Avilan
Cc:
Subject: TelePresence meeting - CONFIRMED - Recurring multipoint

Your Cisco TelePresence meeting has been CONFIRMED

All occurrences of your meeting have been confirmed. Additional options and information about this TelePresence meeting may be found by clicking the following link.
Click Here*

Additional Meeting Options
Clicking the link above may allow:

- Participate in a meeting with other companies,
- Include video conferencing sites,
- Hide your meeting subject on the TelePresence phone,
- Other options.

Upcoming Occurrence Details

Subject:	Recurring multipoint
Organizer:	Jake Avilan (avilan@srdev.com)
Start Time:	Monday, November 24, 2008 09:00 AM (America/Tijuana)
End Time:	Monday, November 24, 2008 09:30 AM (America/Tijuana)
Rooms:	TelepresenceRoom31 TelepresenceRoom33 TelepresenceRoom32
Multipoint Meeting:	*Bridge Phone Number:* *Conference ID:*
Meeting Subject on Phone:	Show

This message has been sent from an unmonitored mailbox.
Please do not respond to this email. Contact your TelePresence Help Desk for additional information.

* Actual URL is https://tsbu-ctm18.cisco.com/scheduler/meetingMgr/schedulerHome.do?systemID=040000008200E00074C5B7101A82E00800000000007003FBC68F2EC901000000000000000001000000006124A8274

Table 11-1 Point-to-Point Meeting Confirmation Email

Email Section	Description
Confirmation Statement (below the email banner)	This section confirms the meeting is properly scheduled and contains the link to the Meeting Details window.
Upcoming Occurrence Details **Note** If this is a single instance meeting, rather than a recurring meeting this section is labeled "Meeting Details".	This section displays information about the scheduled meeting, including some options that are set in the Meeting Details window.
Email footer	The URL displayed at the bottom of the email is the same link to the Meeting Details window as the link in the Confirmation Statement above.

Multipoint Meetings

The Multipoint meeting confirmation email is described in Table 11-2.

Figure 11-2 Multipoint Meeting Confirmation Email

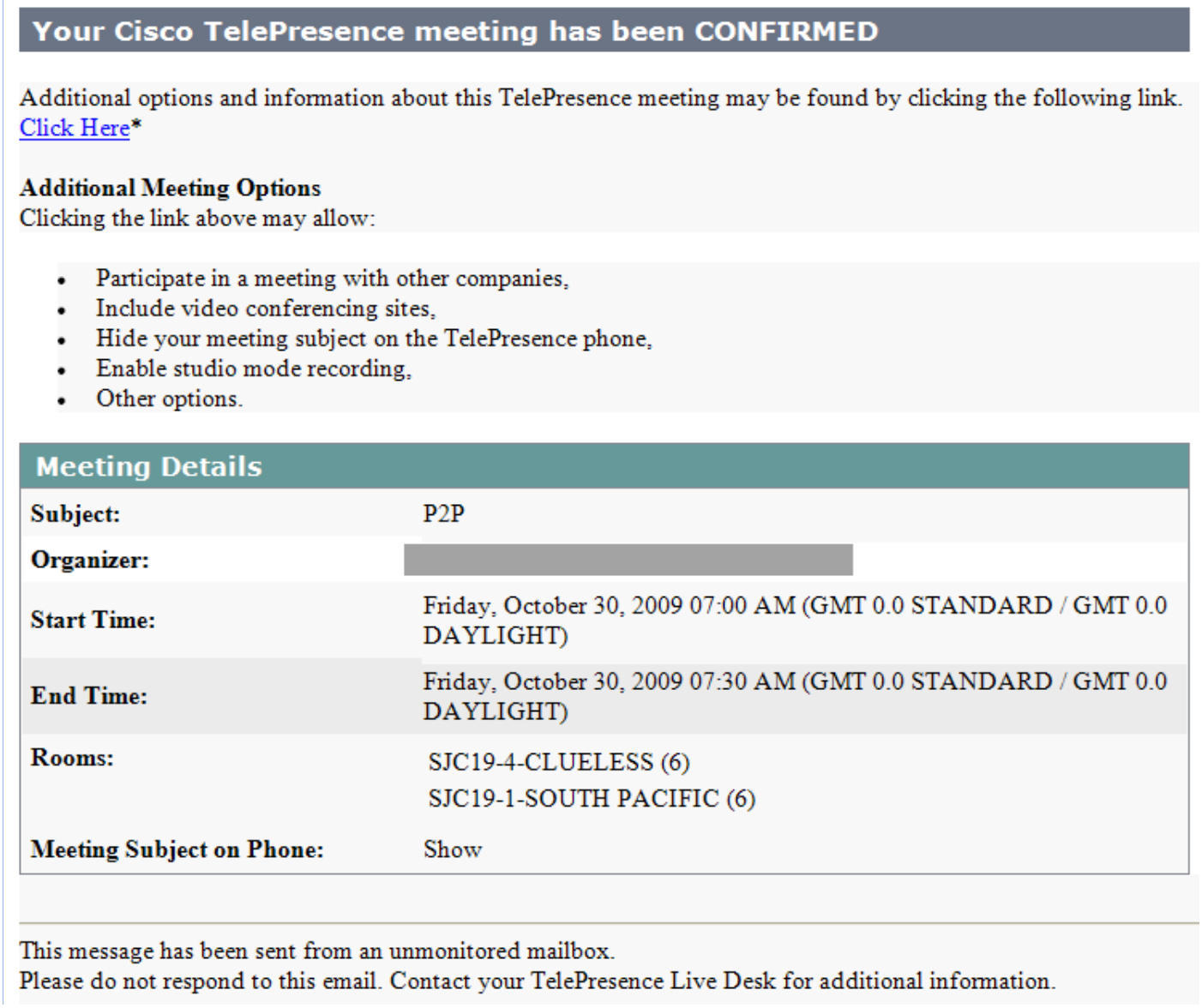


Table 11-2 Multipoint Meeting Confirmation Email

Email Section	Description
Confirmation Statement (below the email banner)	This section confirms the meeting is properly scheduled and contains the link to the Meeting Details window.

Table 11-2 Multipoint Meeting Confirmation Email

Email Section	Description
Upcoming Occurrence Details **Note** If this is a single instance meeting, rather than a recurring meeting this section is labeled "Meeting Details."	This section displays information about the scheduled meeting, including some options that are set in the Meeting Details window. In addition to the standard meeting information, this section contains the Multipoint Bridge Phone Number and the meeting's Conference ID.
Email footer	The URL displayed at the bottom of the email is the same link to the Meeting Details window as the link in the Confirmation Statement above.

Action Required Email

Action Required emails may be sent to the Meeting Organizer to alert them of the following error conditions. The Action Required email is described in Table 11-3.

- **1205 - Missing Required Rooms**: A second Cisco TelePresence room, or other participant has not been defined for the meeting.
  This is the only type of error a Meeting Organizer can correct without administrative assistance. You can see an example of this email in Table 11-3. You or the Meeting Organizer can correct this error using the Meeting Details window, but the recommended way to resolve the error is to use the calendar client used to create the meeting.

  Note This type of Action Required error can also be caused by a room not being deleted properly from a calendar server, for example Microsoft Exchange. This can occur if the Meeting Organizer schedules a meeting that includes a room in delegate mode. If the Meeting Organizer schedules the meeting and then deletes it before the room delegate accepts the invitation, this Action Required email is sent to the Meeting Organizer.

- **1211 - Room Not Compatible**: One or more Cisco TelePresence rooms are running software that is incompatible with the Cisco TelePresence Multipoint Switch.
- **1212 - Resource Not Available**: Not enough Cisco TelePresence Multipoint Switch resources are available to support the multipoint meeting.
- **1213 - MCU Not Configured**: A Cisco TelePresence Multipoint Switch has not been configured for the network.
- **1217 - CUVC Resource Not Available**: Insufficient Video Conferencing resources to setup multipoint meeting.

Figure 11-3 Action Required Email

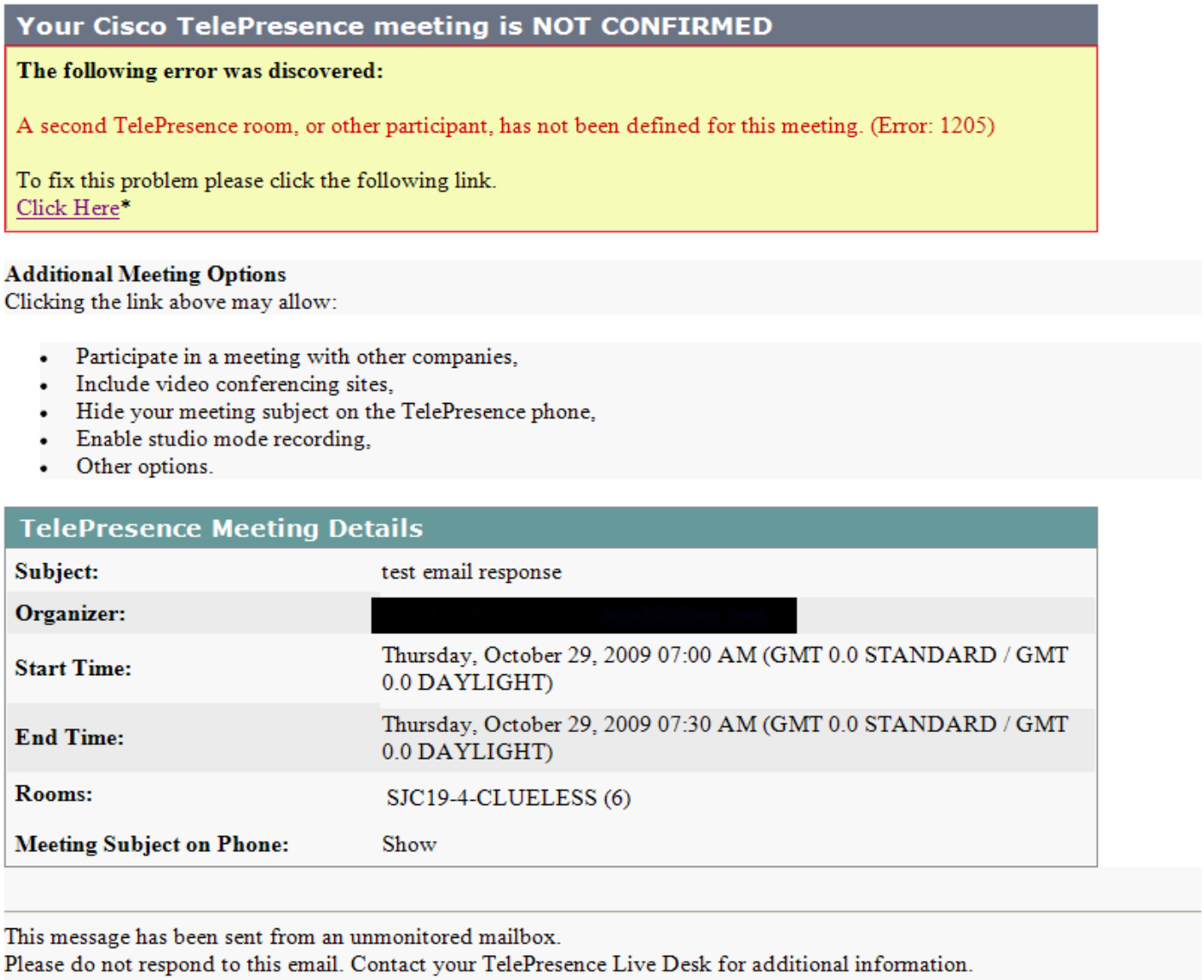


Table 11-3 Action Required Email

Email Section	Description
Confirmation Statement (below the email banner)	This section describes the error to be corrected before the meeting can be confirmed, and contains the link to the Meeting Details window. The error can usually be corrected using the Meeting Details window.
Upcoming Occurrence Details **Note** If this is a single instance meeting, rather than a recurring meeting this section is labeled "Meeting Details".	This section displays information about the scheduled meeting, including some options that are set in the Meeting Details window.

Table 11-3 Action Required Email

Email Section	Description
Occurrences with Errors	If this is a recurring meeting, all the instances that have an error are displayed in a list. Only some instances of a recurring meeting may be in error if the meeting organizer, using the Calendar client has edited some of the instances. Clicking the date/timestamp link takes you to the Meeting Details window for that meeting instance. Only the first 50 meeting instances with errors are listed in the email, but all instances with errors are listed in the Meeting Details window. **Note** The upcoming instance of a recurring meeting may not be one of the occurrences causing the error. When you log into Cisco TelePresence Manager from the upcoming meeting link, or any of the occurrences causing the link you will see all the occurrences of the meeting listed in the left-hand column. Click on any occurrence with an icon showing a red X to resolve the error.
Email footer	The URL displayed at the bottom of the email is the same link to the Meeting Details window as the link in the Confirmation Statement above.

Confirmation Meeting Details Window

For description purposes the Meeting Details window is divided into the following sections:

- Meeting Details
- Occurrence Details

Meeting Details

This web page allows you to specify options not available via your Calender Application and allows you to correct possible errors. Proceed to the Occurrence Details pane of this webpage to continue to set up options for your room configuration.Table 11-4 provides the Fields and Section Names with descriptions for this window.

Occurrence Details Pane

When the Meeting Details - Occurrence Details field is initially displayed you will see the following fields:

- Rooms tab
- VD Interop tab
- Intercompany tab
- Meeting Options tab

Figure 11-4 Default Rooms Tab Field

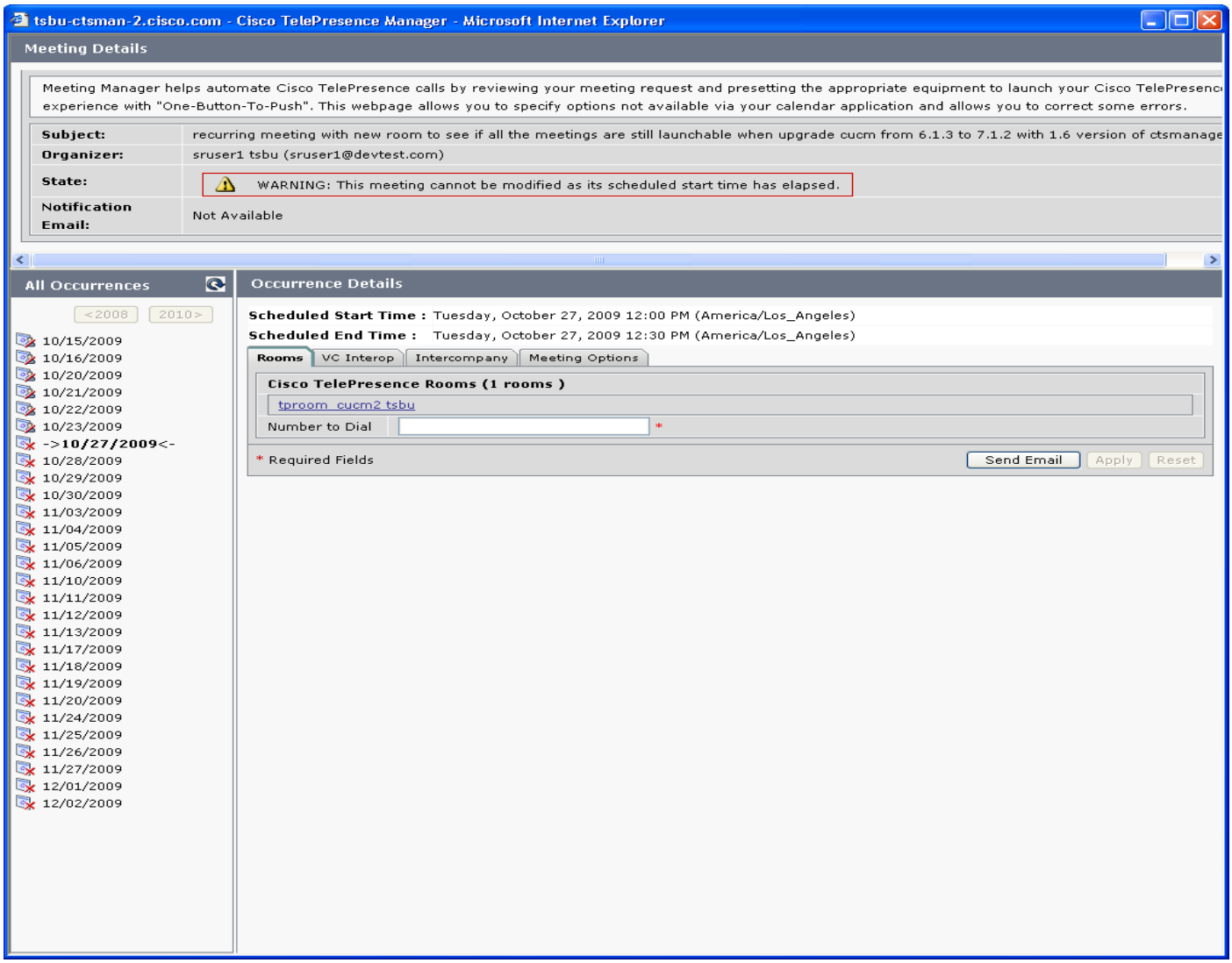


Table 11-4 Meeting Details window

Field or Section Name	Description
Subject	The person scheduling the meeting enters the information in the Subject field.
Organizer	This field displays the name and email address of the person scheduling the meeting.
State	Gives the state of the current meeting if it is properly scheduled. If it is not, then provides a warning message.
Notification Email	Provides you with the last email sent and the time stamp whether or not the meeting is successfully set up.
All Occurrences	This column lists all the occurrences of your recurring meeting. Each meeting instance is a link. Meeting icons showing a red X refer to those meeting instances with errors. Click the link to show the meeting details for that instance.
Occurrence Details	
Scheduled Start Time	Displays the start date and time of the meeting.
Schedule End Time	Displays the end date and time of the meeting.

Rooms Details Option

If you have included only one Cisco TelePresence room in a scheduled meeting you need to use the Meeting Details - Rooms tab window to supply a phone number. If you mistakenly included only one Cisco TelePresence room the meeting organizer should use the Calendar client to add additional rooms.

Table 11-5 Action Required Meeting Details Window

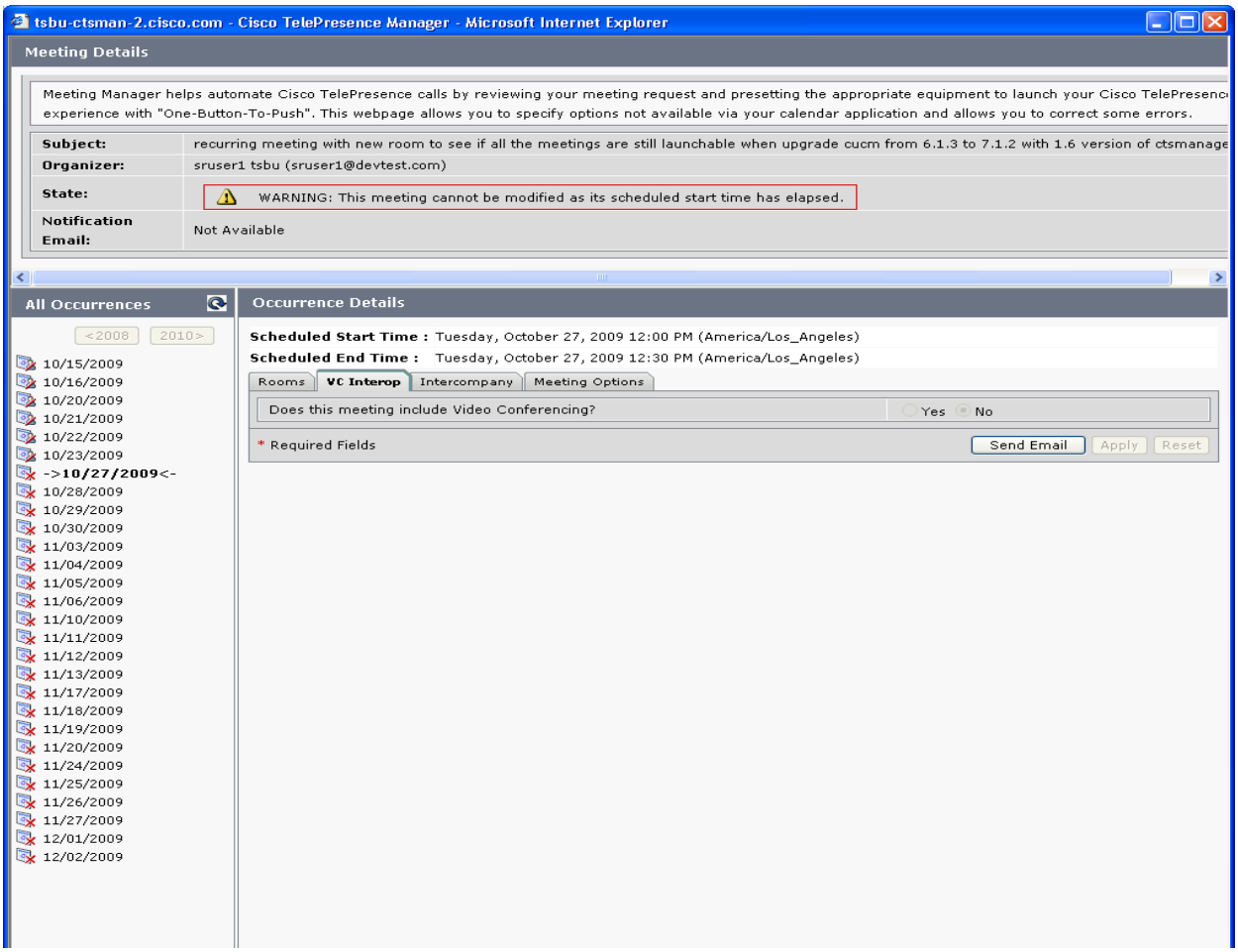
Field Name	Description
Number to Dial	Enter the phone number to be dialed to establish a connection from the Cisco TelePresence room phone.

VC Interop Options

Video Interoperability options available are Include Video Conferencing - **Yes** or **No**.

If select **No**, the following window appears, click **Send Email** if Notification Email is set up for this.

Figure 11-5 Video Interop Options - No Video Conferencing



Video Interoperability options available are Include Video Conferencing - **Yes** or **No**.

If select **Yes**, the following window appears, click **Send Email** if Notification Email is set up for this.

Figure 11-6 Video Interop Options - Yes Video Conferencing

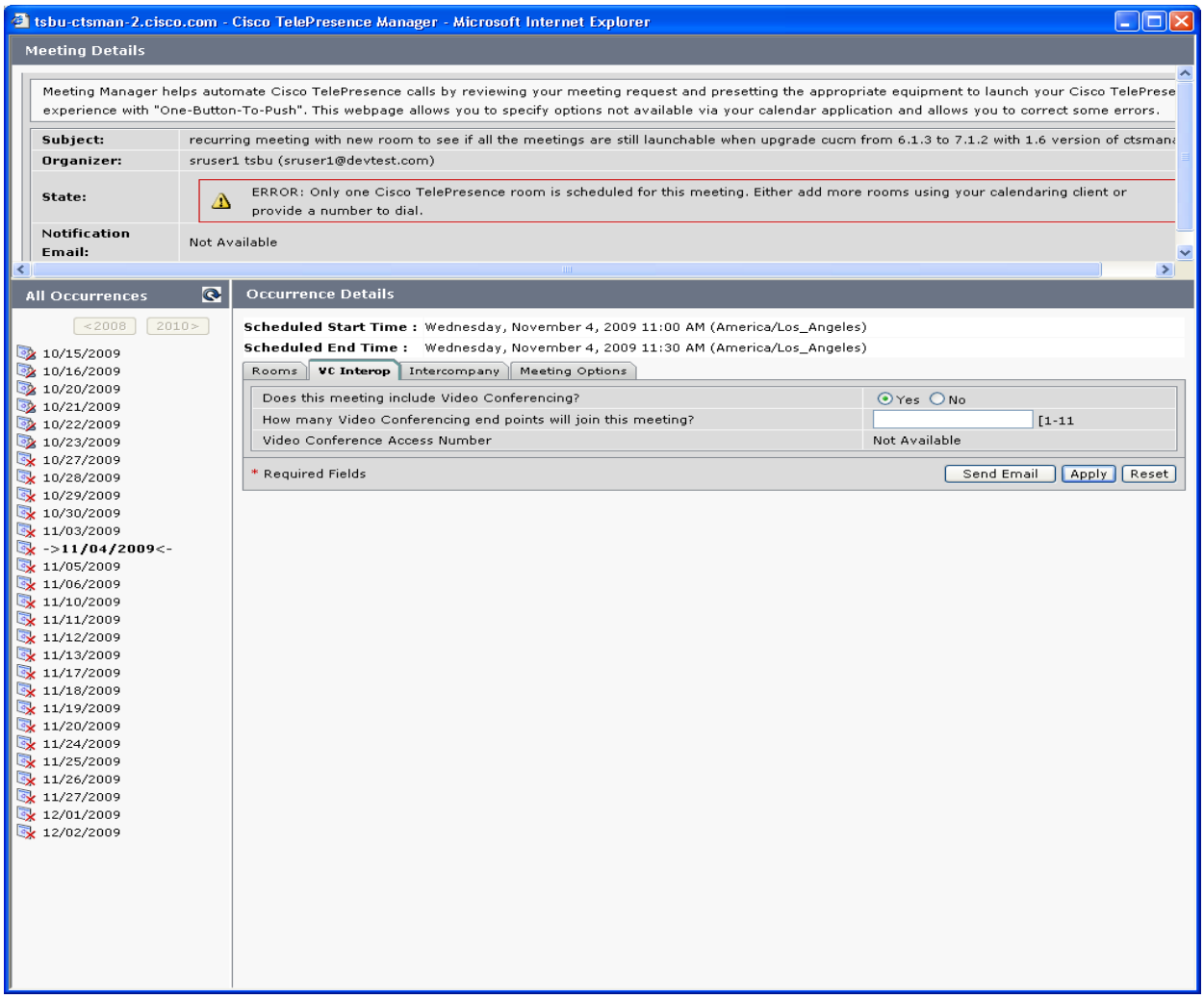


Table 11-6 Video Interoperability Options

Field Name	Description
How many Video Conferencing endpoints will join this meeting?	Enter the number of video conferencing devices that will participate in the meeting.The range is 1 - 11.
Video Conference Access Number	This number is previously configured in the CUVC prefix and is generated by CTS-Manager in this window.
Send Email	If the system is set up for email notification, the Send Email button will send confirmation of video conferencing.

Table 11-6 Video Interoperability Options

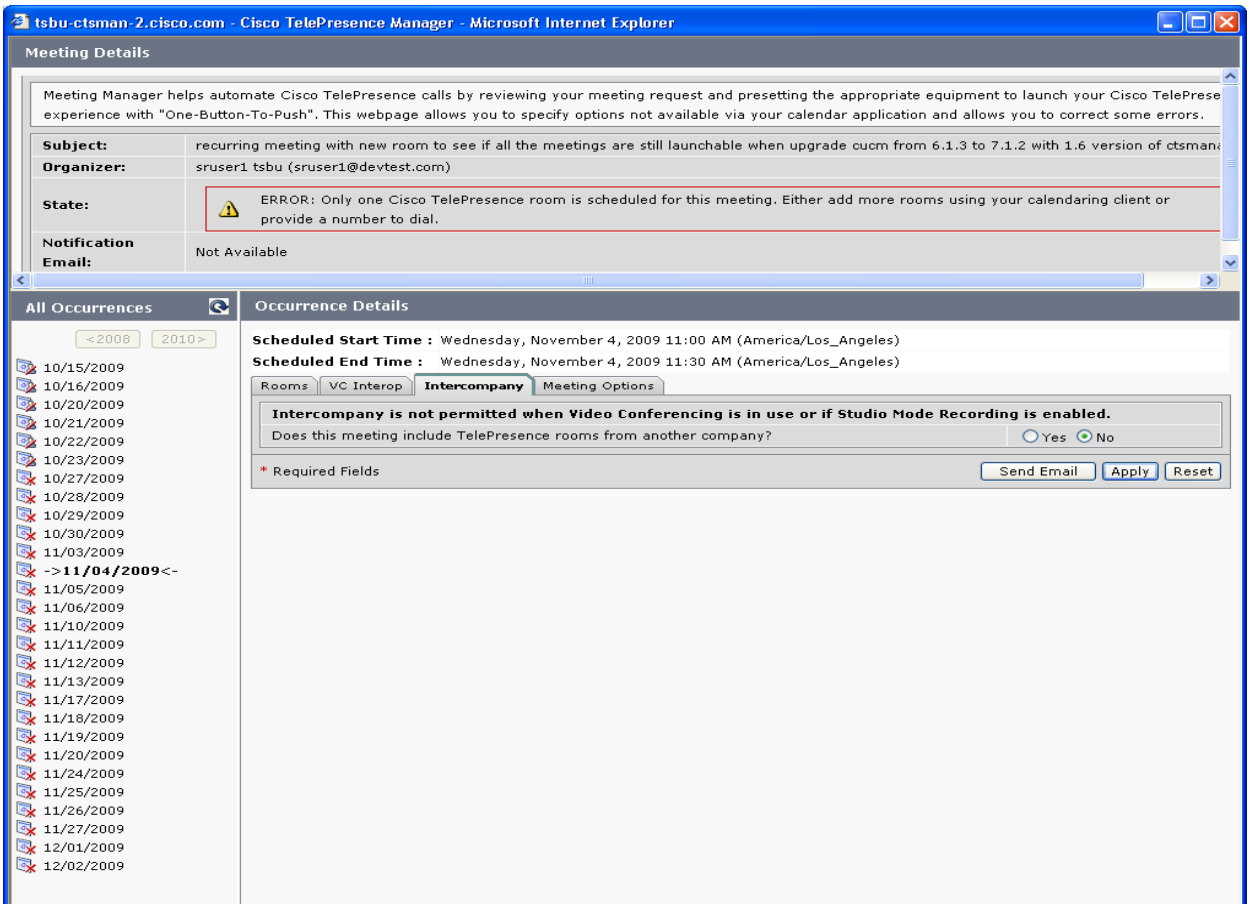
Field Name	Description
Apply	If the number of end points that join in the meeting are changes, use the Apply button to save the changed number.
Reset	This removes what has been configured and allows you to set new values.

Intercompany Host Meeting Options

Intercompany options available are "Does this meeting include TelePresence rooms from another company- **Yes** or **No**."

If select **No**, as shown in the following window , click **Send Email** if Notification Email is set up for this.

Figure 11-7 Intercompany Host Meeting Options

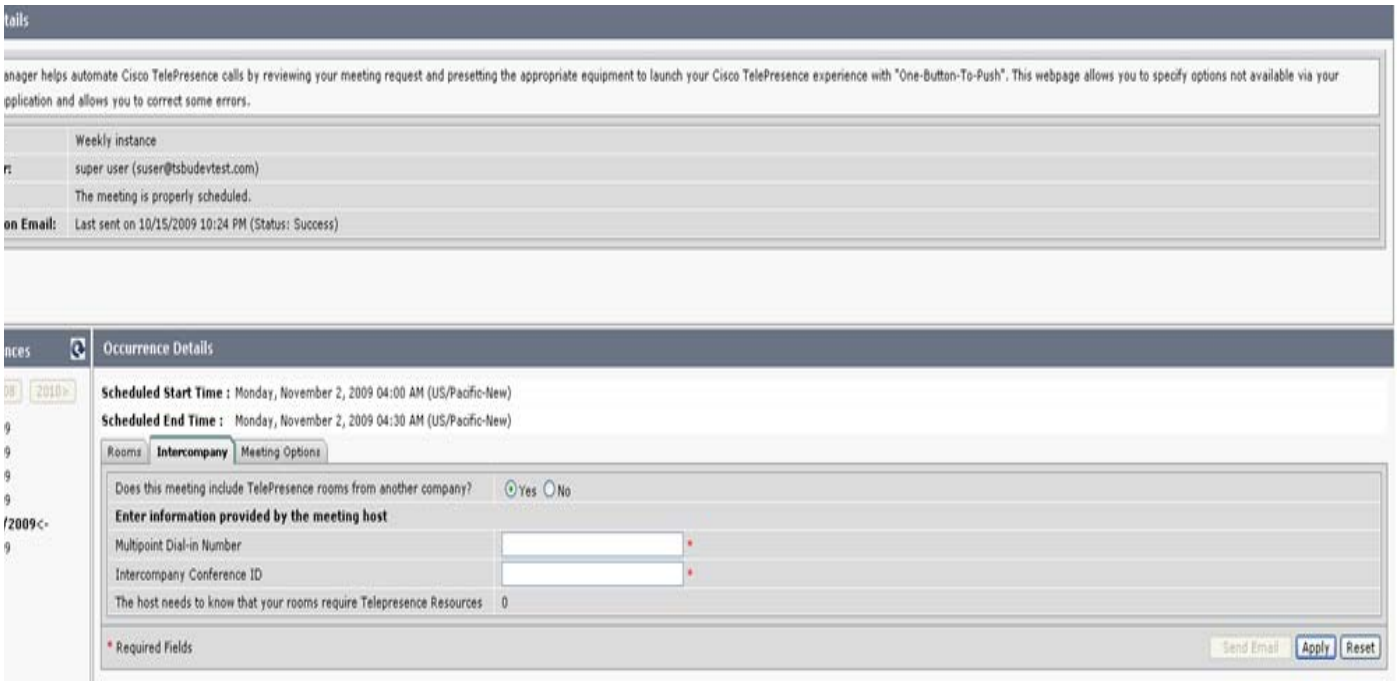


Intercompany hosting options available are Does this meeting include TelePresence rooms from another company? - **Yes** or **No**.

If select **Yes**, the following window appears, click **Send Email** if Notification Email is set up for this.

Intercompany Participant Meeting Options

Figure 11-8 Meeting Details - Intercompany Meeting Set-up Window



If another company is considered the Intercompany Cisco TelePresence meeting host you need to configure your side of the meeting as a participant. You'll need obtain the Dial-in Number and the Conference ID from your CTS-Manager Administrator or from the Host meeting organizer

Enter the information and click **Apply** to set the values.

Table 11-7 Intercompany Participant Meeting Options

Field Name	Description
Multipoint Dial-in Number	This is the phone number your Cisco TelePresence room phone will call to join the meeting. This number is provided by the meeting Host's CTMS or your Service Provider's CTMS.
Intercompany Conference ID	The Conference ID is generated by the Host's CTMS or your Service Provider's CTMS.
The sum of Cisco TelePresence resources required by all other companies.	If your company is hosting an Intercompany Cisco TelePresence meeting, the number of resources required to include all the participating companies is listed. The sum of the resources needed can be determined by adding the values below for each CTS endpoint participating in the meeting: CTS-500 = 1 resource CTS-1000 = 1 resource CTS-1100 = 1 resource CTS-1300 = 1 resource CTS-3000 = 3 resources CTS-3200 = 3 resources

Meeting Options Tab

Clicking the Meeting Options tab in the Meeting Details window displays the following fields:

Figure 11-9 Meeting Options Tab

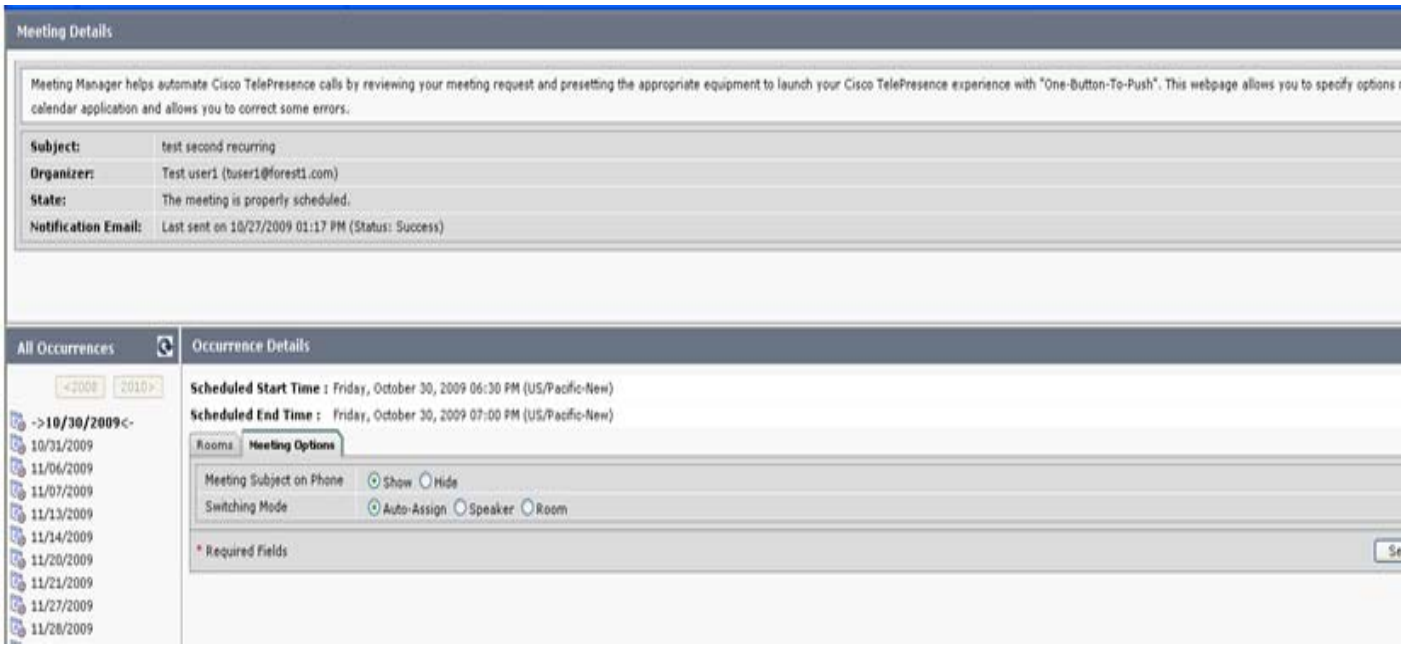


Table 11-8 Meeting Options Tab

Field or Section Name	Description
Meeting Subject on Phone	Choose **Hide** if you don't want the meeting subject to be displayed on the Cisco TelePresence room phone. Select **Show** if you do want the subject displayed. **Note** This option is displayed in the Upcoming Occurrence Details section of the Confirmation email.
Switching Mode	The Switching Mode can be either "**Auto-Assign**," "**Speaker**" or "**Room**." Switching Mode only affects CTS-3000 and CTS-3200 endpoints. If the Switching Mode is set to "**Room**" all the participant displays of the endpoint are switched each time the meeting participant who is speaking changes to a meeting participant at a different endpoint. If the Switching Mode is set to "**Speaker**" only the corresponding participant display (left, center, or right) is switched; the remaining participant displays are not switched. Using the "**Speaker**" switching mode provides the ability to view up to three different remote endpoints at the same time. If you choose "**Auto-Assign**," switching mode is determined by the default CTMS policy. The default CTMS policy is configured on the System Configuration > Policy Management page.

CHAPTER 12

Supported MIBs for Cisco TelePresence Manager

Revised: October 11, 2009, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

The following section provides the list of MIBs that are supported in the Cisco TelePresence Manager.

MIB Support

The following MIBs are supported by CTS-Manager. MIBs only partially supported list their capability files.

Table 12-1 CTS-Manager Supported MIBs

MIB	Support	Capability Location
CISCO-CDP-MIB	Partially	ftp://ftpeng.cisco.com/pub/mibs/v2/CISCO-CDP-CAPABILITY.my
CISCO-SYSLOG-MIB	Partially	ftp://ftpeng.cisco.com/pub/mibs/v2/CISCO-SYSLOG-CAPABILITY.my
IF-MIB	Partially	ftp://ftpeng.cisco.com/pub/mibs/v2/CISCO-IF-CAPABILITY.my
IP-MIB(v2)	Partially	ftp://ftpeng.cisco.com/pub/mibs/v2/CISCO-IP-CAPABILITY.my
RFC1213-MIB	Fully	
SNMPv2-MIB	Fully	
TCP-MIB	Partially	ftp://ftpeng.cisco.com/pub/mibs/v2/CISCO-TCP-STD-CAPABILITY.my
UDP-MIB	Fully	
SNMP-FRAMEWORK-MIB	Fully	
SNMP-MPD-MIB	Fully	
SNMP-VACM-MIB (SNMP-VIEW-BASED-ACM-MIB	Fully	
SNMP-NOTIFICATION-MIB	Fully	
SNMP-TARGET-MIB	Fully	
SNMP-USER-BASED-SM-MIB	Fully	
HOST-RESOURCE-MIB	Fully	

Table 12-2 CTS-Manager Supported H/W MIBs

MIB	Support	Capability Location
IBM PLATFORM		
IBM-SYSTEM-AGENT-MIB		

Table 12-2 CTS-Manager Supported H/W MIBs

MIB	Support	Capability Location
IBM-SYSTEM-ASSETID-MIB		
IBM-SYSTEM-HEALTH-MIB		
IBM-SYSTEM-LMSENSOR-MIB		
IBM-SYSTEM-MEMORY-MIB		
IBM-SYSTEM-MIB		
IBM-SYSTEM-NETWORK-MIB		
IBM-SYSTEM-POWER-MIB		
IBM-SYSTEM-PROCESSOR-MIB		
IBM-SYSTEM-RAID-MIB		
IBM-SYSTEM-TRAP-MIB		
HP PLATFORM		
CPQIDA-MIB		1.3.6.1.4.1.232.3
CPQHOST-MIB		1.3.6.1.4.1.232.11
CPOSTDEO-MIB		1.3.6.1.4.1.232.1
CPQTHRSH-MIB		1.3.6.1.4.1.232.10
CPQSTSYS-MIB		1.3.6.1.4.1.232.8
CPQSINFO-MIB		1.3.6.1.4.1.232.2
CPQHLTH-MIB		1.3.6.1.4.1.232.6
CPQIDE-MIB		1.3.6.1.4.1.232.14

CHAPTER 13

Troubleshooting Cisco TelePresence Manager

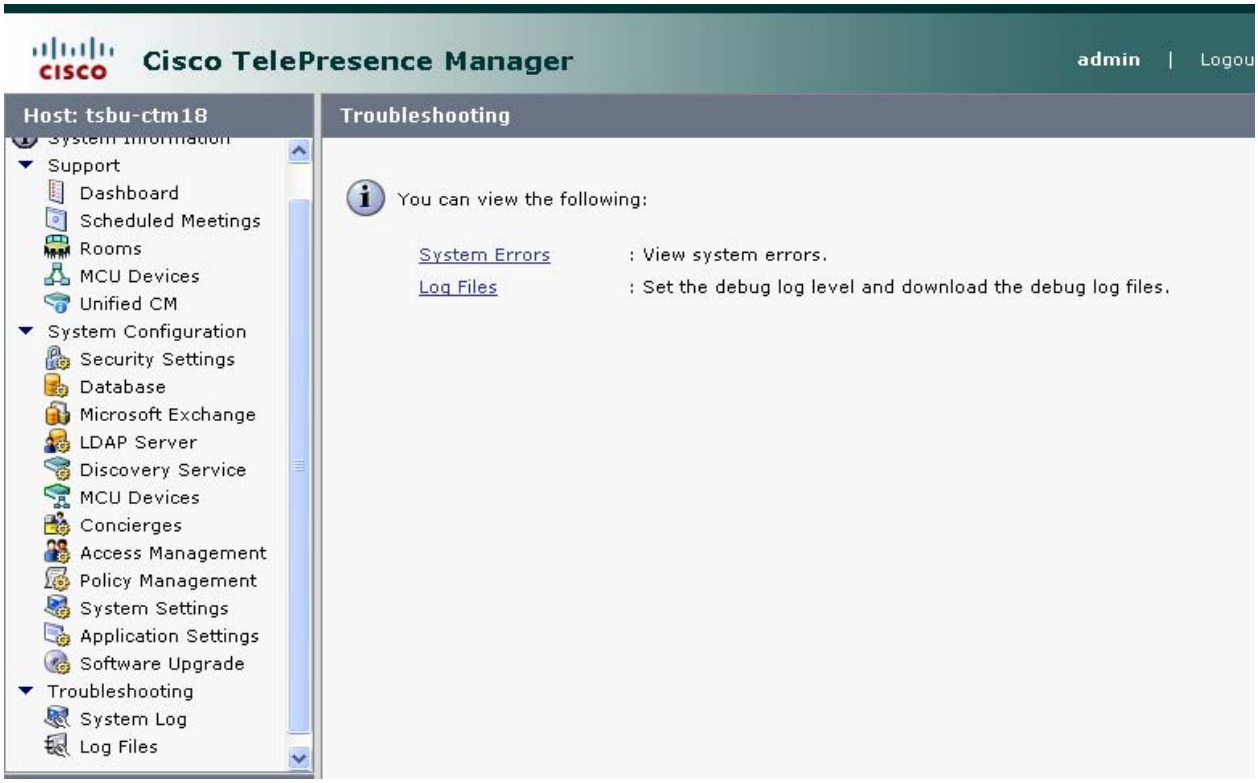
Revised: October 30, 2009, OL-13673-06
First Published: November 27, 2006

Contents

Introduction

Troubleshooting meeting connections and network problems is one of the more important responsibilities of the Cisco TelePresence system administrator. When a problem is detected, you must collect system errors and logs files so they can be analyzed for prompt resolution. Figure 13-1 shows the links available to assist you with these troubleshooting tasks.

Figure 13-1 Troubleshooting Window



System Log

Choose the System Log window to see a list of system messages. You can filter the list by starting and ending dates and message type All, Fatal, Severe, Moderate, Warning, and Info, as follows:

- Use the Calendar icon to choose dates, or type the dates in the **Start On** and **End On** fields using the MM/DD/YYYY date format.
- Click **Filter** to generate the list.

Figure 13-2 System Log Window

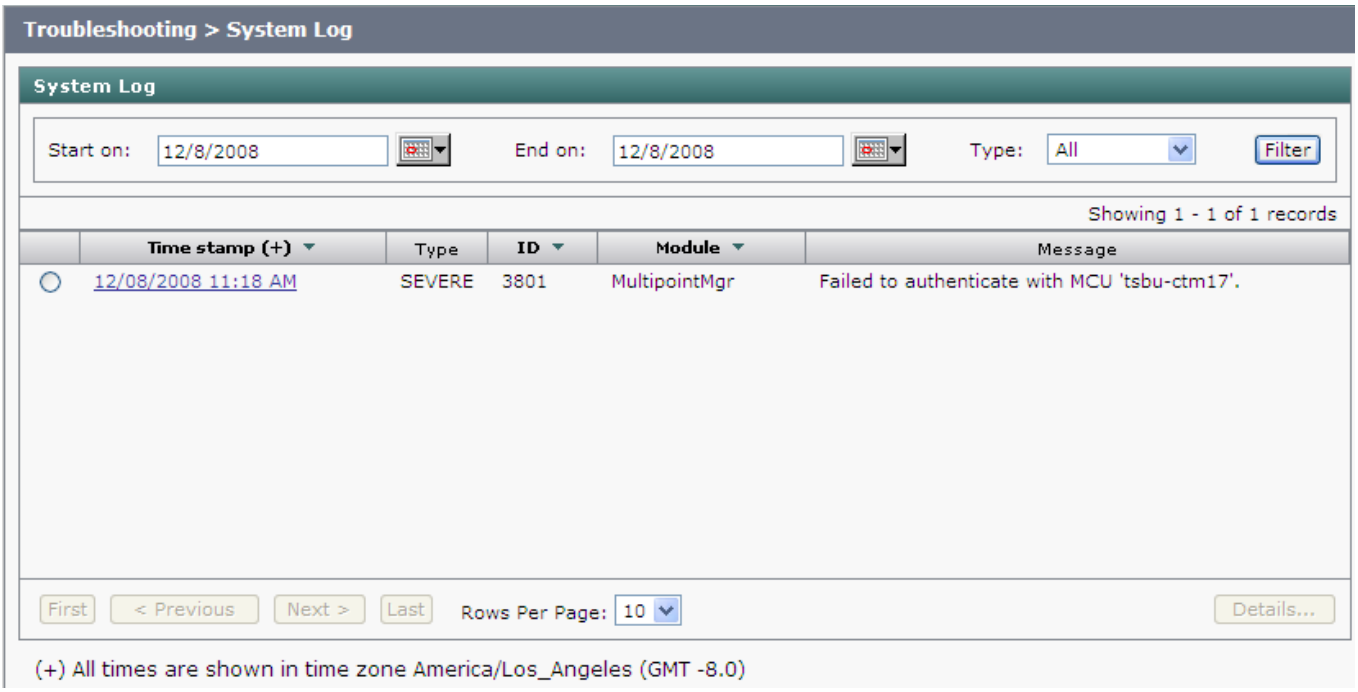


Table 13-1 lists the error information provided by the system.

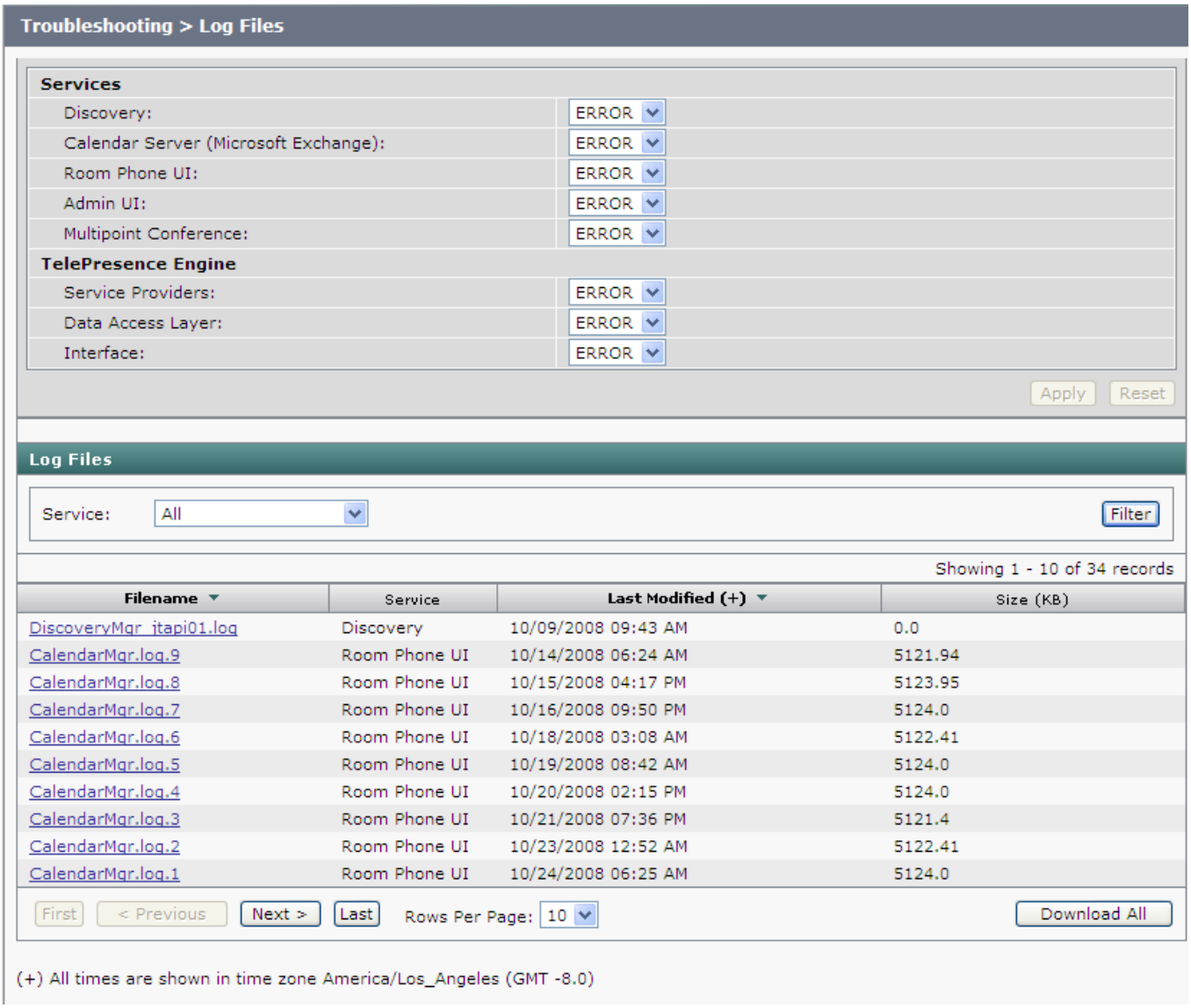
Table 13-1 System Error Report

Field	Description
Timestamp	Date and time the message was logged. You can sort the messages in ascending or descending order by the time stamp.
Type	Message type.
ID	Message identification number. You can sort the reports in ascending or descending order by ID.
Module	Component within CTS-Manager that generated the error.
Message	Explanation of problem detected. Move your mouse pointer over a message field to see a complete description.

Log Files

At the Log Files window, you can set the level for logging system errors from the following services that contribute messages:

Figure 13-3 Log File Window



Services

- Discovery Service
- Calendar Service
- Room Phone UI Service
- Admin UI Service
- Multipoint Conference

TelePresence Engine

- Service Providers
- Data Access Layer

- Interface

You can set the message types from these services to the following levels:

- **DEBUG**—Detailed errors and information messages.
- **ERROR**—Errors that are likely to terminate system activity.
- **FATAL**—Errors that will automatically terminate system activity.

Note The default logging level is typically set to **ERROR**. There may be times when Cisco technical personnel will instruct you to modify the logging level for one or more of the services, to help them diagnose a problem. Be sure to reset the logging level immediately after the problem has been resolved, or else disk space may become filled with messages and negatively impact system performance.

Once you have made your logging level choices for each service:

- Click **Apply** to register new or modified settings, or click **Reset** to restore the original settings.

You can generate a list of specific error types.

- From the Service drop-down list, choose one of the following to specify the type of errors to display:
  - **All**
  - **Discovery**
  - **Groupware Adapter**
  - **Room Phone UI**
  - **Admin UI**
  - **Multipoint Connection**
  - **TelePresence Engine**
- Click **Filter** to generate the list.

Log files are named with a .log extension. The log filename provides a link to the contents of the error log file. This window also shows the date the file was last modified and the size of the log file. The lists can be sorted by filename and time last modified.

- To update the error log, click the **Refresh** button.

Download All Files

Use the Download All button to collect all log data for Cisco technical support personnel when submitting a case for problem solution. The data is automatically compressed in a file that can be sent via email.

Scheduled Meeting and Room Issues

Meeting information is retrieved via processing room notifications from a Microsoft Exchange or an IBM Domino Calendar server. A notification is generated when a meeting is added, modified, or deleted.

The Cisco TelePresence Manager database is periodically synchronized with the Calendar server to retrieve and maintain room schedules. Synchronization resolves any problems that might have occurred when Exchange or Domino connectivity was not available and notifications were not received. If required, you can also trigger a manual synchronization of the room meeting schedule using the Re-sync Operation in the Microsoft Exchange or IBM Domino window.

Meeting information is stored in the database, and the Room Phone UI service is notified when it is time to send the meeting schedule to the phone user interface.

The Rooms window displays the room status as “In Use” when a call is placed. The Scheduled Meeting window displays meetings as “In Progress” or “Completed” reflecting the actual state of the call.

If the concierge is called, this condition will be reflected in the Room UI view and Scheduled Meeting view as “Needs Help”.

Refer to troubleshooting information in Table 13-2 to solve common problems that prevent Cisco TelePresence meetings from being scheduled correctly.

Table 13-2 Scheduled Meeting and Room Issues

Problem or Message	Possible Causes	Recommended Action
Detailed view of Meetings reports that the Cisco TelePresence meeting is “Pending for more information from Exchange”.	This message appears when one of the two following conditions occurs: • When Cisco TelePresence Manager receives notice of an event, it waits 30 seconds to see if any further event details are forthcoming from Microsoft Exchange and then validates the meeting. • If the room is in manual-accept mode and the room’s delegate has accepted a meeting only tentatively or has not responded to meeting e-mail notification	• Wait a few moments and view Meetings status again to see if the meeting has been validated. • Advise the room delegate to respond to meeting e-mail notification.
The meeting organizer receives no e-mail to confirm the meeting is scheduled.	This problem occurs when a room is not in auto-accept mode.	Make sure reserved rooms are in auto-accept mode. If a room is in manual-accept mode, the meeting invitation must be accepted by the room’s delegate using Microsoft Outlook or Lotus Notes.
Scheduled Meetings do not show the status “In Progress”, or Rooms do not show “In Use” when a call is placed.	Connectivity between the Cisco TelePresence system and CTS-Manager is lost.	Check the Rooms window for status. The SSH username and password should be configured for the Cisco TelePresence system. See the *Unified CM Installation Guide for Cisco TelePresence* for more help. Verify that the Calendar service is running on the Cisco TelePresence system.

Table 13-2 Scheduled Meeting and Room Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Room status indicates an error condition.	Place your mouse over the status to see the error described in a tooltip. This problem can occur when: • The phone associated with the Cisco TelePresence meeting room is not included in Cisco TelePresence Manager application user profile. • The phone associated with the Cisco TelePresence meeting room is not registered with the Unified CM. • More than one Cisco TelePresence phone could be configured with the same room name.	Cisco TelePresence IP phone associated with participating rooms must be added to the CTS-Manager Application User Profile. Update the CTS-Manager Application User Profile with correct room data. Check the Rooms window for status. Check the IP connectivity between the equipment and CTS-Manager. Missing Secure Shell username and password for the Cisco TelePresence IP phone should be configured in the Unified CM configuration.
A recurring meeting is not listed in the Scheduled Meetings window	The first occurrence of the meeting is scheduled more than one year in the past.	Reschedule the meeting so that the start date for the recurring meeting is less than one year in the past.
Two instances of the same meeting (either a single meeting or an instance of a recurring meeting) are listed in the Scheduled Meetings window.	The date or time of the meeting was modified after the start time of the meeting, but before the meeting was initiated or the before the meeting end time has occurred.	This is expected behavior. The meeting instance with the new start date or start time is treated as a new meeting.
A recurring point-to-point meeting listed in the Scheduled Meetings window displays an Error status. OR A recurring multipoint meeting is listed in the Scheduled Meetings window as a point-to-point meeting (only two rooms are scheduled).	The rooms included in the meeting are in manual-accept mode (delegates must accept meeting invitations). If the recurring meeting is a point-to-point meeting (R1 & R2) and a room delegate has declined one instance (R1), all meeting instances show only one room scheduled. If the recurring meeting is a multi-point meeting (R1, R2, & R3) and a room delegate has declined one instance (R1), all meeting instances show only two rooms scheduled (R2 & R3).	• In Microsoft Exchange, select the checkbox for the room(s) missing from the scheduled meeting and Re-sync. • In IBM Domino, click Re-sync to re-sync the database.

Table 13-2 Scheduled Meeting and Room Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Room Status reports a Subscription or Synchronization error with Microsoft Exchange	A Discovery operation attempted to sync to a newly added Room calendar before even one meeting was added to the calendar.	A Room calendar must contain at least one scheduled meeting in order for Cisco TelePresence Manager to successfully subscribe and sync. To remove the error status: 1. Schedule at least one meeting on the Room calendar. 2. From the System Configuration > Microsoft Exchange window, select the room showing the subscription error and click **Re-sync**. 3. From the Support > Rooms Summary tab, select the room showing the Exchange subscription or sync error (on the Status tab), and click **Update Schedule**.
Recurring or single meeting with only one room is displayed with an Error status after meeting start time has passed.	If a meeting organizer deletes a meeting that was 1. not launched, 2. after the meeting start time all but one rooms are removed from the scheduled meeting and the meeting is set to an Error status. If the meeting was a recurring meeting and the meeting series was deleted after the first instance of the meeting was 1. not launched, 2. after the 1st meeting instance start time all but one rooms are removed from the scheduled meeting and the meeting is set to an Error status.	This is expected behavior. All rooms calendars are available for scheduled meetings.
Meeting Confirmation email refers to upcoming meeting instance, not to meeting instance whose details were updated.	The **Send Email** button in the Meeting Details window is available to any user (Concierge or Administrator) logging into Cisco TelePresence Manager. If you make changes to a future instance of a recurring meeting and click **Send Email**, the confirmation email sent to the Meeting Organizer refers to the upcoming meeting and not to the future instance that was changed.	The Meeting Organizer must click the link in the Confirmation email to open the Meeting Details window and select the future meeting instance to see the changes made.

Table 13-2 Scheduled Meeting and Room Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Meeting instances in a recurring meeting are not listed in the Action Required emails.	Action Required emails list only the first 50 instances of a recurring meeting.	To view additional instances of a recurring meeting, the Meeting Organizer must click the link in the Action Required email and display the Meeting Details window.
A scheduled meeting is not listed in the Scheduled Meetings window. (For IBM Domino deployment.)	The date of a scheduled meeting must fall between two days prior to the current date and two calendar years in the future (-2 days — +12 months), in order for Cisco TelePresence Manager to sync the meeting between the Domino database and the Cisco TelePresence Manager database. **Note** If a meeting is scheduled while Cisco TelePresence Manager is down, and more than two days pass before CTS-Manager is restarted, the meeting will not be sync'd and must be rescheduled.	Verify the rooms are registered properly in the System Configuration > IBM Domino window. The room name appearing in the Associated Rooms column must exactly match the room names added to the profile in Unified CM. **Note** In Cisco Unified CM the Product Specific Configuration Layout window refers to "Room Name (from Exchange)". This is the room name that must match the room name in the Domino server database in order for CTS-Manager to successfully sync.
A deleted meeting still appears in CTS-Manager. (For IBM Domino deployment.)	The CTS-Manager database is set to delete scheduled meetings according to the (Polling Interval * 3). The Polling Interval is set in the IBM Domino window. If the scheduled meeting does not fall within two days prior to the current date and two calendar years in the future (-2 days — +12 months), the meeting is not deleted from the CTS-Manager database.	Please wait the prescribed amount of time to ensure the meeting is deleted.
Scheduled meetings show an error. OR New meetings are not appearing in the Scheduled Meetings window.	After the Microsoft Exchange server is down, CTS-Manager does not regain a connection.	Re-sync the rooms with scheduled meeting errors or missing meetings. After the room re-sync Exchange may still display an error status. This can be fixed by either: • waiting for CTS-Manager to renew subscription to the affected rooms (occurs every 55 minutes) OR • restarting the CTS-Manager server.
New meetings are not processed by CTS-Manager after a software upgrade.	The Domino or Exchange server was down during the upgrade and the initialization process did not complete properly.	• Initiate Discovery manually to initialize the processes. OR • Restart CTS-Manager

Table 13-2 Scheduled Meeting and Room Issues (continued)

Problem or Message	Possible Causes	Recommended Action
An Action Required email does not list the error for all instances of a recurring meeting (Domino Calendar Server issue).	If a recurring meeting is created with two endpoints, and is then modified by removing one endpoint for all meeting instances, the Action Required email does not list out all the meeting instances.	This is expected behavior. The meeting organizer should modify the meeting series using Lotus Notes and add a second Cisco TelePresence room.
A deleted meeting still appears in the Scheduled Meetings window.	The meeting was deleted from the Exchange room calendar, but the meeting is not deleted in CTS-Manager. This can happen if room reservations are managed using Outlook Auto Accept.	Delete the meeting from the room calendar. Refer to Microsoft Knowledge Base article 280854 for more information.
A room shows a sync error with a calendar server.	1. A new room with no scheduled meetings is included in a multipoint recurring meeting. 2. Meeting goes into error state, because of reduced MCU resources. 3. The meeting series is deleted through Outlook. 4. The new room now has a 'one room' meeting error. 5. Exchange returns '0' meetings for the new room during daily maintenance, but the CTS-Manager database still contains a meeting for the room.	Perform on of the following procedures to correct the room sync error: • Create a meeting using this room (P2P, multipoint, single or recurring). The next daily maintenance corrects the sync error. • Perform a manual sync for the room.
Scheduled meeting is in error state for a new room.	A new room is included in two separate meetings and one of the meetings is deleted. **Note** In this scenario a Clarification email may be sent to the meeting organizer for a 'missing rooms' issue. The email should not have been sent.	Re-sync the room with Exchange.
Meeting does not show up in CTS-Manager Web UI nor is it pushed to the phone UI.	Room mailbox attending the meeting has been switched between auto-accept mode and manual accept mode.	Re-accept the meeting manually again. It is recommended not to switch room mailbox acceptance mode.
No clarification email sent when a meeting is modified to include only one room.	If the meeting organizer is using OWA and deletes one of two rooms for a scheduled meeting no clarification email is sent.	Refer to Microsoft Knowledge Base article 916160 for more information.
Only one instance of a yearly recurring meeting is seen in CTS-Manager.	The meeting organizer did not specify an end date.	Update meeting to include an end date.
Two different meetings appear as scheduled for the same time slot.	One of the meeting's scheduled had its "Show time as" attribute set to "free".	Do not set the "Show time as" attribute to "free". Reschedule the meeting.

Table 13-2 Scheduled Meeting and Room Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Both past and present scheduled meetings are updated when enabling interoperability.	When enabling interoperability for a scheduled meeting and the meeting organizer chooses “all future occurrences”, all past and present meeting instances have interop enabled.	This is standard functionality.
Deleted scheduled meetings still appear in CTS-Manager.	If all meetings for a room are deleted CTS-Manager is not updated to reflect the meeting deletions in Exchange.	Create a new scheduled meeting for the room to re-sync CTS-Manager and Exchange.
Meetings scheduled past a one year duration only show the first year of scheduled meetings.	CTS-Manager only displays the first 365 days of any scheduled meeting.	Meetings scheduled prior to CTS-Manager 1.4 will continue to display meeting dates past a 365 day window. Meetings scheduled using CTS-Manager 1.4 only display meeting dates for the first 365 days.
CTS-Manager shows extra meeting instances for some recurring meetings.	An additional room, in proxy mode is added to an existing recurring meeting by the Meeting Organizer, who then makes additional changes to the series. The room delegate then accepts the invite to the meeting using an out-of-date meeting invitation.	Make sure the room delegate uses the latest meeting invitation when accepting the invitation.
A meeting organizer may receive two emails from CTS-Manager for a non-recurring multipoint meeting.		Use AAA for acceptance.
A meeting state is displayed as complete even if some participants remain active.	Meetings scheduled between endpoints supporting secure mode (earlier than 1.5) and 1.5 endpoints, that have been modified to be an intercompany meeting may not end the call properly for 1.5 endpoints.	Manually end the call from each version 1.5 endpoint.
After changing the hostname or IP address of Cisco Unified Communications Manager (Unified CM) with same configuration in CTS-Manager, the custom meeting data is lost.	1. Cisco Unified CM’s IP address is changed so that the IP address in CTS-Manager needs to be changed. 2. Cisco Unified CM is restored on a different server and now CTS-Manager is configured with new Cisco Unified CM IP address. In such cases, even though there is no change in the CTS conference rooms, CTS-Manager deletes all rooms and meetings, adds new rooms, and syncs again with the Exchange/Domino. This causes all custom data to be lost.	Change Cisco Unified CM to use the previous configuration; restore using the CTS-Manager backup so that all the custom changes to the meetings are restored.

IP Phone User Interface Issues

Once a scheduled Cisco TelePresence meeting has been confirmed by participating rooms in Microsoft Exchange or IBM Domino, it should be listed on the IP phone user interface in less than three minutes. Use Table 13-3 to troubleshoot problems between scheduled meetings and the phone user interface.

Table 13-3 IP Phone User Interface Issues

Problem or Message	Possible Causes	Recommended Action
The Cisco TelePresence IP phone displays the standard idle screen instead of the meeting list managed by CTS-Manager.	This problem can occur when: • There is no connectivity between the Cisco TelePresence IP phone and Cisco TelePresence Manager. • The scheduled meeting is outside the user-specified time window. • The Secure Shell username and password for the Cisco TelePresence IP phone in the Unified CM configuration are missing. • CTS-Manager has not sent required information to the Cisco TelePresence IP phone. • The network is not properly configured or is down.	• Check the dashboard for phone status. • Only meetings within the user-specified time window are displayed on the phone user interface. The administrator can configure the number of days displayed. • Verify that the Calendar service is running in the Cisco TelePresence system.
A scheduled meeting does not appear on the Cisco TelePresence phone user interface.	• The room name configured in Unified CM does not match the actual room name (e-mail alias) configured in the Directory Server. • Duplicate room names are configured. • Cisco TelePresence IP phone associated with participating rooms has not been added to the CTS-Manager Application User Profile. • The Exchange or Domino user account for CTS-Manager does not have permission to retrieve calendar data.	• The room name must exactly match the name (e-mail alias) provided in the Directory Server. • Remove duplicate room names configured in Unified CM. • Update the CTS-Manager Application User Profile with correct room data. • Change the CTS-Manager user account for Exchange or Domino so it has permissions to retrieve (read) room and calendar data.
A proposed meeting was deleted from Microsoft Outlook, but it still appears on the Cisco TelePresence phone user interface.	This problem can occur when: • Outlook Web Access (OWA) is used to schedule meetings because OWA does not receive delete updates. • CTS-Manager is not synchronized with the Exchange database.	• Log into Microsoft Outlook and use that application to delete the meeting. • Use the Re-Sync Operations under Microsoft Exchange to resynchronize the database and meeting schedule.

Cisco TelePresence Manager Database Issues

Status for database services is displayed on the Dashboard window.

You can verify the CTS-Manager database status using the following CLI command:

utils service list

The result should indicate the CTS-Manager database as running.

You can start the CTS-Manager database using the following CLI command:

utils service start Cisco DB

You can stop the CTS-Manager database using the following CLI command:

utils service stop Cisco DB

Caution Use this command with extreme caution: The CTS-Manager server must be stopped before stopping the CTS-Manager database.

Table 13-4 CTS-Manager Database Issues

Problem or Message	Possible Causes	Recommended Action

Remote access user names cannot be created with a number.	CLI returns the following error:
	`admin:utils remote_account create rootuser1`
	`Executed comand unsuccessfully`
	`Invalide account name`
	
	The Admin UI returns the following error:
	`"Cisco TelePresence Manager has detected error conditions while processing your request.`
	`Code 2617`
	`ID: REMOTE_ACCT_CREATE_ERROR`
	`Module: AUI`
	`Message: Failed to create remote account 'rootuser1'. Error: 'Invalid account name'.`
		Do not create user names that include a number as part of the name.

Multipoint Conference Unit (MCU) Issues

CTS-Manager supports two types of MCUs, CTMS and CUVC. Table 13-5 documents any issues or anomalies between CTS-Manager and an MCU.

Table 13-5 MCU Issues

Problem or Message	Possible Causes	Recommended Action
A CUVC status is always “OK”.	CUVC status is not monitored by CTS-Manager.	When registering a CUVC with CTS-Manager you must manually confirm all configuration settings.
The value entered in the Max/Min Participants per Conference fields are not validated by CTS-Manager when you click the Save button.		You must manually determine and enter the correct value in these fields.

Cisco Unified Communications Manager (CUCM) Issues

Table 13-6 Cisco Unified CM Issues

Problem or Message	Possible Causes	Recommended Action
The following message appears in the Support > Cisco Unified CM window “Cisco Unified CM version 6.1.1 is not supported.”	CTS-Manager is running in secure mode. If Web Services Security is set to ‘Secure’ on the System Configuration > Security Settings window you must be running Cisco Unified CM 6.1.2 or higher to support security.	Set Web Services Security to ‘Unsecure’ or upgrade Cisco Unified CM to 6.1.2 or higher and run Discovery from the System Configuration > Discovery Service window.

Calendar Server and LDAP Interface Issues

Status for the Calendar Server (Microsoft Exchange or IBM Domino), and the LDAP server is displayed in the Dashboard window. If problems are indicated, verify the attribute mappings specified during installation CTS-Manager. See Settings in the LDAP Server window under System Configuration.

Caution The object and attribute mappings for Exchange/Directory Server and Domino/Directory Server deployments are listed in Table 13-8 and Table 13-9 and **should not** be changed after installing and configuring Cisco TelePresence Manager.

Caution The Object Class field and Attribute fields should not be changed. Cisco TelePresence Manager might not function properly if these fields are changed.

For deployments with multiple Directory Server deployments, LDAP uses port 3268 (the Global Catalog port) by default. For a single server deployment, port 389 is generally used, but you can reconfigure this port at the LDAP Server window under System Configuration.

LDAP Server Issues

Table 13-7 LDAP Server Issues

Problem or Message	Possible Causes	Recommended Action
Room is not sync'd between Microsoft Exchange and Cisco TelePresence Manager.		• LDAP user container DN must be configured correctly for all domains. • LDAP field mapping should be set to default settings.

Microsoft Exchange Calendar Server Issues

Table 13-8 Microsoft Exchange Calendar Server Issues

Problem or Message	Possible Causes	Recommended Action
Extra room has been added to a specific instance of a recurring meeting. **Note** This issue occurs with Exchange 2007.	1. A meeting organizer schedules a recurring meeting with two or more rooms (R1, R2 and R3). 2. Meeting organizer deletes R1 from one instance of recurring meeting (M1). 3. Meeting organizer adds a fourth room to master series (R4). 4. R1 has been re-added to M1.	1. Open the R1 room calendar and delete the scheduled meeting instance. 2. In Cisco TelePresence Manager, go to the Configuration>Microsoft Exchange window, select the checkbox next to the room and click the Re-sync button. **Note** Refer to Microsoft Knowledge Base article 949294 for more information.
Room Status reports a Subscription status error or a sync error with Microsoft Exchange	A Discovery operation attempted to sync to a newly added Room calendar before even one meeting was added to the calendar.	A Room calendar must contain at least one scheduled meeting in order for Cisco TelePresence Manager to successfully subscribe and sync. To remove the error status: 1. Schedule at least one meeting on the Room calendar. 2. From the System Configuration > Microsoft Exchange window, select the room showing the subscription error and click **Re-sync**. 3. From the Support > Rooms Summary tab, select the room showing the Exchange subscription or sync error (on the Status tab), and click **Update Schedule**.

Table 13-8 Microsoft Exchange Calendar Server Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Room is not sync'd between Microsoft Exchange and Cisco TelePresence Manager.		• Cisco TelePresence Manager must have Full Access or Read Permission to the Room's mailbox. • The Room mailbox must be created with English as the default language. • The Room user must log into the Room mailbox at least once. • The Room email ID must be uniquely assigned to only one user (Room user). • Room's email ID must be configured correctly in Cisco Unified CM and Exchange. • The Cisco TelePresence System MAC address must be added to the User Profile in Unified CM. • Each Cisco TelePresence System may have only one corresponding IP Phone, that shares the same DN with the Cisco TelePresence System and whose MAC address has been defined in the Cisco Unified CM User Profile. • The Cisco TelePresence Manager's clock must be in sync with the Exchange system clock. • UDP port 3621 cannot be blocked by a firewall between Exchange Cisco TelePresence Manager. • Forms Based Authentication must not be enabled for WebDAV for the Exchange website in the Exchange server that is registered with Cisco TelePresence Manager. • Verify the room is configured for Auto-accept, or the Room Delegate has accepted the meeting invitation. • At least one meeting must be scheduled on a room calendar before syncing with CTS-Manager, or CTS-Manager will return a sync error condition for the room

Table 13-8 Microsoft Exchange Calendar Server Issues (continued)

Problem or Message	Possible Causes	Recommended Action
In the Microsoft Exchange window, clicking **Test Connection** returns an error.		• Verify Exchange 2007 has a Client Access role. • For IIS Manager on the Exchange server, make sure **SSL is required** is not checked for the default web site when you are not using secure mode. • In Exchange Management Console, make sure **Exchange (Default Website)** is not configured with FBA. **Note** FBA must be disabled for Cisco TelePresence manager to sync meeting information with Exchange. If a new Room mailbox is added to a new Exchange server that has FBA enabled, you can either disable FBA on the second Exchange server, or use the initial Exchange server as the front-end server and point Cisco TelePresence Manager to that server.
In the Scheduled Meetings window the Meeting Subject is deleted. **Note** This issue occurs with Exchange 2007.	By default, the Exchange mailbox calendar attributes **AllBookInPolicy**, **DeleteSubject**, and **AddOrganizerToSubject** are set to true. These attribute flags set to true delete the meeting subject and replace it with the organizer's username.	In order to display the original subject of the meeting, set **DeleteSubject** and **AddOrganizerToSubject** in the room calendar mailbox setting to false.
Single meeting email confirmation may show incorrect local timezone for meeting start time.	Outlook desktop does not set the meeting timezone for a single occurrence meeting.	Refer to Microsoft Knowledge Base article 925376 for more information.
Meeting shows with error "waiting for more info from Exchange". **Note** This issue occurs with Exchange 2007.	This can be caused if OWA is used to schedule the meeting, and the meeting organizer is logged into OWA as one of the rooms included in the meeting.	Do not use OWA to schedule a meeting if you are logging in as one of the meeting rooms included in the scheduled meeting.
CTS-Manager cannot connect to MS Exchange.	The Windows logon name used to log into the MS Exchange server is different from the SMTP LHS.	In the System Configuration > Microsoft Exchange window specify both the logon name and the SMTP LHS if they are different. **Note** After upgrading CTS-Manager make sure both the logon name and the SMTP LHS are specified.

IBM Domino Calendar Server Issues

Table 13-9 IBM Domino Calendar Server Issues

Problem or Message	Possible Causes	Recommended Action
Failed to authenticate. Check authentication parameters. Username: short form of email address. Password: Internet password	This problem can occur when the incorrect password is specified for the Domino server, or the LDAP server configured with Domino.	Make sure the Internet password is used in the Password fields in the System Configuration> IBM Domino window and the LDAP Server window.
Room is not sync'd between Domino server and Cisco TelePresence Manager.		• The Room user must log into the Room mailbox at least once. • The Room email ID must be uniquely assigned to only one user (Room user). • Room's email ID must be configured correctly in Cisco Unified CM and Domino. • The Cisco TelePresence System MAC address must be added to the User Profile in Cisco Unified CM. • Each Cisco TelePresence System may have only one corresponding IP Phone, that shares the same DN with the Cisco TelePresence System and whose MAC address has been defined in the Cisco Unified CM User Profile. • The Cisco TelePresence Manager's clock must be in sync with the Domino system clock.

Table 13-9 IBM Domino Calendar Server Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Clicking **Test Connection** returns an error.		The following services should be added to the list of server tasks to load automatically when the IBM Domino servers is started: • RNRMGR • DIIOP • HTTP • LDAP • Router • Calconn In addition to the above services: • the Resource Reservations Database must be local to the Domino server • The Resource Reservation Database must be using the Resrc7.ntf or Resrc8.ntf template. • The appropriate Security Settings should be applied to the Domino server. • Verify the Host, Port, Organization Name, Username, and Password are correct. • Verify the server is reachable from the Cisco TelePresence Manager host by performing a telnet to the Domino port.
Meeting Organizer unable to log into Cisco TelePresence Manager using the link in the Action Required email.	• Meeting Organizer is not using the internet password. • Meeting Organizer is not entering their login name correctly.	• Verify the Meeting Organizer's password is set as the Domino internet password. • On the Cisco TelePresence Manager login page, the Meeting Organizer must enter their Username in the standard Lotus Notes format <username>/<organization name> (The organization name must match the value in the Organization Name field on the System Configuration > IBM Domino window).

Web Browser Error Messages

The only version of Microsoft Internet Explorer supported on CTS-Manager is version 6. Use information in the following sections to help you resolve web browser problems.

JavaScript Error Message

Error Message `JavaScript is not enabled on this browser. Log-in is not allowed.`

Explanation CTS-Manager must have JavaScript enabled in the web browser in order to work. Without it, the login screen will appear and users can enter a username and password, but the Login button is disabled.

Recommended Action Users must enable JavaScript in their web browser to log into the Cisco TelePresence Manager user interface.

To enable JavaScript, perform the following steps on Microsoft Internet Explorer:

Step 1 Click **Tools**. Select **Internet Options** from the choices.

Step 2 Click the **Security** tab.

Step 3 Select the zone in which the CTS-Manager server resides. This zone is usually the Local intranet.

Step 4 Click the Custom Level button.

Step 5 Scroll down to the Active scripting section and click **Enable**.

Step 6 Click **OK** to apply the changes.

Safe ActiveX Checking Message

Error Message `WARNING: Your security settings do not allow the use of safe ActiveX controls installed on your computer. Most features will not work properly.`

Explanation CTS-Manager uses XMLHttpRequest technology. In Microsoft IE Version 6, this technology is implemented as a safe ActiveX control, and it is bundled with IE by default. However, if ActiveX controls have been disabled in the browser, CTS-Manager will not work correctly. For example, the status pane will not display any meeting counts.

Recommended Action Enable safe ActiveX control in the web browser so CTS-Manager works correctly.

To enable safe ActiveX control, perform the following steps on Microsoft IE Version 6:

Step 1 Click **Tools**. Select **Internet Options** from the choices.

Step 2 Click the **Security** tab.

Step 3 Select the zone in which the CTS-Manager server resides. This zone is usually the Local intranet.

Step 4 Click the **Custom Level** button.

Step 5 Scroll down to the ActiveX controls and plug-ins section.

Step 6 Enable the following items:

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

Step 7 Click **OK** to apply the changes.

System Error Messages

Table 13-10 lists messages that are displayed by CTS-Manager, along with possible causes and solutions for correcting the problem that caused the message.

When reading the following messages, consider that "$1" or "$2" are placeholder tokens. When the message actually appears in the application, the tokens will be replaced by text or a value.

Table 13-10 Cisco TelePresence Manager Error Messages

Code	Message	Explanation	Recommended Actions
1000	Internal server error: $1.	A bucket for all untyped errors. The detail message would contain the actual error.	Contact support.
1001	Failed to parse config file '$1'. Error: $2.	The server fails to parse the config/ctis.xml configuration file. The webapp would fail to start up.	Check syntax of ctis.xml. This file should be changed by qualified technicians only. If possible, revert to its original content and restart Tomcat server. Contact support for further assistance.
1004	Version $1 is not supported for component: $2.	CTS-Manager does not support the version extracted from the given component.	Deploy CTS-Manager with supported versions of Exchange and LDAP only.
1005	The operation is unsupported on OS '$1'.	The current operation is not supported on the given platform.	Contact support. Users should not see this error at all as we only deploy on Linux.
1007	Failed to restart host. Error: '$1'.	CTS-Manager fails to restart the machine as requested. The detail message is given.	Contact support.
1008	The functionality '$1' is not yet implemented.	The given functionality has not been implemented yet.	Upgrade CTS-Manager.
1009	Error in initialization: '$1'.	Database maintenance manager fails to initialize due to missing scripts for either backup, purge or cron job.	Contact support. The installation process has failed.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
1010	One or more arguments are null.	Exchange component is failing to test connection because one of the required parameters (host, super user account name/password, bind method) is null.	Check information provided on the Exchange configuration screen.
1011	Unable to dispatch API call.	CTS-Manager component is unable to communicate with the CTS-Manager Engine.	Check for any errors in the logfile. Contact support.
1012	Failed to shutdown host. Error: '$1'.	The server can not be shut down due to the specified reason.	Verify that user has the right permission to shutdown the server, check for any errors in the logfile. Contact support.
1013	Failed to determine IP address of host $1	Hostname may be incorrect	Verify hostname
1014	System service '$1' is shutting down.	Not an error. An info message is logged indicating a system service is being shut down.	Nothing to do.
1015	Service '$1' is started and ready to process requests.	Not an error. An info message is logged indicating a system service was started.	Nothing to do.
1016	Object class '$1' does not have property '$2'.	Internal programming error.Very Unlikely to happen.	Contact support.
1200	Invalid meeting. Error: Field '$1' ($2) is invalid.	A field in the given meeting has invalid value.	Contact support.
1201	Invalid single meeting. Error: '$1' ($2) is invalid.	The given meeting is not a single meeting as expected.	Contact support.
1202	Invalid master meeting. Error: '$1' ($2) is invalid.	The given meeting is not a master meeting as expected.	Contact support.
1203	Invalid exception meeting. Error: '$1' ($2) is invalid.	The given meeting is not a exception meeting as expected.	Contact support.
1204	Too many TelePresence rooms.	Used by Exchange component in its email notification to inform meeting organizers that a meeting has more than two TelePresence rooms scheduled.	Remove extra TelePresence rooms from the meeting.
1205	Missing required number of TelePresence rooms.	Used by Exchange component in its email notification to inform meeting organizers that a meeting has less than two TelePresence rooms scheduled.	Add another TelePresence room to the meeting, or provide a dial number using the URL in the confirmation email.
1208	Recurring meeting instance: '$1'.	An error occurred while calculating the instances for a recurring meeting.	Contact support.
1209	Missing Conference ID and Bridge Number for the Multipoint meeting.	Used by Exchange component in its email notification to inform meeting organizers that a multipoint meeting is missing a conference id or bridge phone number. This is an unlikely case to happen.	Verify that MCU is configured properly, and at least one is available for multipoint meeting allocation.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
1210	Missing required number of TelePresence rooms for the Multipoint meeting.	Used by Exchange component in its email notification to inform schedulers that a meeting has less number of rooms than what is required for a multipoint meeting. This is an unlikely case to happen.	Contact support.
1211	Selected TelePresence rooms are incompatible for multiroom conference. Contact help desk.	Used by Exchange component in its email notification to inform schedulers that a meeting is scheduled with room(s) that can not support multipoint conference.	Check the version of TelePresence equipment of each room and verify that it is a version which can support multipoint meeting. Upgrade if necessary.
1212	Insufficient resources to setup multiroom conference. Contact help desk.	Used by Exchange component in its email notification to inform schedulers that there is no available MCU for a multipoint meeting.	Verify that MCU is configured properly, and at least one is available for multipoint meeting allocation. Add a new MCU if necessary, or reschedule the meeting to a different time.
1213	Resources not setup to support multiroom conference. Contact help desk.	Used by Exchange component in its email notification to inform schedulers that there is no MCU configured for a multipoint meeting.	Verify that MCU is configured properly, and at least one is available for multipoint meeting allocation. Add a new MCU if necessary.
1214	Scheduler does not have enough privileges to setup this TelePresence meeting. Contact help desk.	Used by Exchange component in its email notification to inform schedulers that they don't have enough privilege for scheduling a multipoint meeting.	Verify that the scheduler has been assigned with the required user privilege. Add the scheduler to the user group that has the required privilege if necessary.
1215	Resource allocation error. $1	There is not enough resource available to migrate all meetings from one MCU to another MCU.	Verify that the target MCU has the proper configuration and that it is available.
1216	Meeting migration error. $1	An error occurred when attempting to migrate meetings from one MCU to another MCU	Check the error message in the logfile. Contact support.
1217	Insufficient Video Conferencing resources to setup multipoint conference.	There are not enough Video Conferencing resources available to have a Video Conferencing meeting.	Reduce the number of Video Conference participants or increase the number of Video Conferencing resources on the Video Conferencing MCU.
1221	Bulk execution failed	Some meetings update failed.	Contact Support.
1222	Failed to load/parse time zone map file '$1'. Error: $2.	The time zone map file maps a user calendaring time zone (from either Exchange or Domino) to a system time zone. The time zone map file is timezonemap.xml under /usr/local/ctis/config. The error would indicate the actual message in the Error portion of the message.	An internal error. Something has occurred during system installation or upgrade. Contact support.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
1223	Unknown time zone target '$1'.	The time zone map file maps a user calendaring time zone (from either Exchange or Domino) to a system time zone. The time zone map file is timezonemap.xml under /usr/local/ctis/config. The error is indicating that a system time zone in the mapping is wrong.	An internal error. Something has occurred during system installation or upgrade. Contact support.
1225	Unable to find a matching time zone target time zone definition ID: '$1', Descriptor: '$2', Definition: '$3'.	CTS-Manager fails to recognize the user time zone passed from the calendaring application.	Contact support with the error message so that the time zone mapping file can be updated and patched.
1226	A unique conference ID is not available in the requested time window.	All the Video Conferencing Access Numbers exhausted in this time slot.	Modify the meeting to use another time slot and try to convert the meeting to a Video Conferencing meeting.
1227	Duplicate room entries found in Cisco Unified CM.	Two CTS devices have same email address configured in Cisco Unified CM.	Correct the email address and make it unique for the devices having same email address.
1400	Fail to $1 concierge. Error: $2.	CTS-Manager fails to perform the given operation for a concierge. The detail error message is given.	Most likely real cause would be DB operation error. DB might be down. Contact support.
1401	This device has $1 future meetings scheduled. Please migrate the meetings to another device first and try again.	Selected MCU has some future meetings scheduled and therefore it can't be deleted.	Migrate the meetings from the MCU (to be deleted) to another MCU and try the deletion again.
1402	A device with hostname $1 already exists. Please use a different hostname and try again.	A device with the same hostname and/or IP address already exists, therefore it doesn't allow the addition of the new device.	Check the hostname configuration for any conflict. Correct it and try the addition again.
1403	Duplicate entry. $1 already exists.Please use a different name and try again.	A configuration entry with the same value already exists, therefore it doesn't allow the addition of the new entry.	Check the entry value uniqueness to make sure it does not have any conflict with any existing configuration. Correct it and try the addition again.
1405	Failed to enable Interoperability support. Error: $1.	User operation of enabling Interoperability support has failed.	Most likely cause is the Cisco TelePresence Engine server process is not running. Verify its status using CLI command. Contact support if unable to start this server process.
1406	Failed to disable Interoperability support. Error: $1.	User operation of disabling Interoperability support has failed.	Most likely cause is the Cisco TelePresence Engine server process is not running. Verify its status using CLI command. Contact support if unable to start this server process.
1408	Managed CTMS is not Interop capable. Cannot enable Interop support.	The managed CTMS does not support Video Conferencing Interoperability.	Upgrade the CTMS to a version that supports Interoperability with Video Conference.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
1409	Managed CTS is not Interop capable, cannot enable Interop support.	The managed CTS does not support Video Conferencing Interoperability.	Upgrade the CTS to a version that supports Interoperability with Video Conference.
1410	Cannot disable Interoperability support when there exists an Interoperability MCU.	CTS-Manager does not allow disabling of Video Conferencing Interoperability if there is a Video Conferencing MCU configured in the system.	Delete the Video Conferencing MCU and try disabling Interoperability support.
1411	Only one CUVC is allowed in system.	CTS-Manager allows only one CUVC.	If a new CUVC must be added, first remove the existing CUVC.
1412	Room $1 does not support Interoperability. Groupware subscription will be denied.	While Video Conferencing Interoperability is enabled a managed CTS is downgraded to not support Interoperability.	Upgrade the CTS to a version that supports Interoperability with Video Conference.
1601	Failed to authenticate. Check authentication parameters.	Self-explanatory.	Check user name and password and try again.
1602	Unsupported authentication type '$1'.	The authentication specified during configuration (e.g.: for LDAP against Directory Server) is not supported.	Contact support.
1603	Error during encryption: '$1'.	An error occurred while encrypting a string. The detail error message is given.	Contact support.
1604	Error during decryption: '$1'.	An error occurred while decrypting a string. The detail error message is given.	Contact support.
1605	Insufficient credential '$1'. Requires credential '$2'.	User does not have sufficient privilege to access an URL.	Obtain correct credential and try again.
1606	Access permitted to email ID '$1' only.	Only scheduler is permitted to access the URL given in the email notification. Any other user trying to log in will be rejected with this error.	Use scheduler's credential to log in.
1607	New password is too simple. New password should contain both mixed-case alphabetic and non-alphabetic characters. It should not base on common words found in dictionary.	Self-explanatory. Happened when user changes super user password.	Use better formed password and try again.
1608	Password was change successfully, but could not be saved for future upgrade.	Could not save new password to platformConfig.xml due to some internal error.	Contact support.
1609	Could not change password: current password does not match.	Users must enter the old password correctly before they are allowed to change to new password.	Enter the correct old password.
1611	Unable to find username '$1' in the directory	Incorrect username specified in login screen	Enter correct username

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
1612	Failed to authenticate.Check authentication parameters.Username:LHS of email address.Password:AD password	CTS-Manager superuser account credentials inside MS-Exchange are invalid	Enter correct username/password
1613	Failed to authenticate.Check authentication parameters.Username:short form of email address.Password:Internet password.	CTS-Manager superuser account credentials inside IBM-Domino are invalid	Enter correct username/password
1700	Unknown configuration component '$1'.	Configuration for the specified component does not exist.	Ensure that the first time configuration setup is done and all the values are properly specified.
1701	No parameter '$1' found under configuration component '$2'.	Specific configuration parameter for a component does not exist in stored configuration.	Ensure that the first time configuration setup is done and all the values are properly specified.
1702	Failed to set parameter '$1' to value '$2'. Error: '$3'.	CTS-Manager is unable to save the given parameter due to the given detail error message. This is likely to be caused by DB error.	Check DB component status using CLI command. Restart it if necessary. Restart Tomcat after DB is running.
1703	Failed to update schedule to rooms '$1'. Error: '$2'.	CTS-Manager fails to submit a schedule update request to the given rooms.	Check room equipment and try again.
1704	Failed to validate DN '$1'.	CTS-Manager fails to validate specified DB in LDAP directory	Check DN configuration.
1705	Failed to validate email '$1'. The specified email does not exist	Extra email address specified under custom settings is not valid	Correct email address in specified field
1901	Failed to authenticate the TB device:	Username/password does not match for Telepresence Equipment	1. Configure username/password in Cisco Unified CM for specified telepresence equipment. 2. Run Cisco Unified CM Discovery for SR to sync configured username/password.
1902	Failed to send message to the TB device:	Could not deliver updated calendar to Telepresence Equipment due to loss of connectivity	1. Verify if Telepresence equipment is registered with Cisco Unified CM. 2. If Telepresence Equipment is not registered inside, contact Cisco TAC
1903	No Communication link on TB:	Web Service on TelepresenceEquipment is not running	1. Use Telepresence Equipment Troubleshooting guide to ensure the webservice is running
1904	Failed to update the SSH username/password from DB into cache.	Failed to retrieve SSH username password from DB	1. Use trouble shooting section to verify database connectivity

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
2000	Data Access Error: $1.	General error in data access operations	Look into the specific error message. Based on the message, verify if database is running, verify using 'Test Connection' if Directory Server is running, troubleshoot the specific message.
2001	Metaschema Parsing Error: $1.	An error occurred while parsing metaschema file.	Ensure that the installation and first time configuration has completed successfully.
2002	Error loading Metaschema file: $1.	The metaschema file is not loaded.	Ensure that the installation and first time configuration has completed successfully. Ensure that the disk is not corrupted.
2003	Datastore '$1' not found in Metaschema file.	Datastore values are not proper in metaschema file.	Ensure that the installation and first time configuration has completed successfully.
2004	Error updating override metaschema file.	Unable to write the values specified in the FieldMapping tab to the metaschema file.	Ensure that the installation and first time configuration has completed successfully. Ensure that the values specified in the FieldMappings tab are valid.
2005	Data Access Initialization Error: $1.	An error occurred during data access plugins initialization.	Evaluate specific message and troubleshoot database, LDAP connectivity and first time setup.
2006	Error in object creation: $1.	An error occurred during object creation in the database.	Evaluate object to be created and troubleshoot based on specific message.
2007	Error during object write: $1.	An error occurred during object update in the database.	Evaluate object to be updated and troubleshoot based on specific message.
2008	Error during object delete: $1.	An error occurred during object deletion in the database.	Evaluate object to be deleted and troubleshoot based on specific message.
2009	Error during object get: $1.	An error occurred during object retrieval from the database.	Evaluate object to be retrieved and troubleshoot based on specific message.
2010	Specified object '$1' not found in '$2' datastore.	The specified object does not exist in the data store	Evaluate object to be retrieved and troubleshoot based on specific message.
2011	Invalid Parameter Specified: '$1'.	The specified parameter is not valid.	Contact support.
2012	Error in Data Purge.	Error in Data Purge.	Evaluate message and contact support.
2013	Error in Data Backup.	Error in Data Backup.	Evaluate message and contact support.
2014	Error in Data Restore.	Error in Data Restore.	Evaluate message and contact support.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
2015	Error in DB Maintenance Operations.	Error during database maintenance operation (Backup/Restore/Purge)	This is an error which is not handled by the categories mentioned above. Evaluate specific message and contact support.
2016	Error returned by spawned process: $1.	Error returned by script spawned by the server Java process	Evaluate the specific message. Contact support if required.
2017	Error acquiring connection: $1.	Error in getting a connection from connection pool	Check connection type (DB/LDAP) and verify connectivity. If problem persists, may require server restart. Contact support.
2018	Error closing connection: $1.	Error in closing a connection from connection pool	This may not be severe, but needs to be monitored. Check connection type (DB/LDAP) and verify connectivity. If problem persists, may require server restart. Contact support.
2019	Error closing statement: $1.	Error in closing a JDBC SQL statement object.	This may not be severe, but needs to be monitored. Check if database is running.
2020	Error instantiating class: $1.	Error in using pluggable methods during data access operations	Ensure the installation and first time setup is properly completed. This may be resolved by server restart. Contact support before doing this.
2021	Error instantiating method '$1' for class: '$2'.	Error in using pluggable methods during data access operations	Ensure the installation and first time setup is properly completed. This may be resolved by server restart. Contact support before doing this.
2022	Error retrieving field '$1' for class: '$2'.	Error in using pluggable methods during data access operations	Ensure the installation and first time setup is properly completed. This may be resolved by server restart. Contact support before doing this.
2023	Error setting value for field '$1' for class: '$2'.	Error in using pluggable methods during data access operations	Ensure the installation and first time setup is properly completed. This may be resolved by server restart. Contact support before doing this.
2024	Specified object '$1' is already deleted.	An object specified to be deleted is already deleted.	This is a warning to be monitored. Contact support.
2025	Object handler not found for specified object: '$1'.	The object handler for data access operations is not found.	This is a fatal error. Contact support.
2027	Attribute '$1' was not retrieved.	The requested attribute is not found in the object, either because application does not retrieve all the attributes for the object or it does not use the correct attribute name.	This is a severe error, but need not be fatal. Contact support.
2301	Unknown object interface '$1'.	An object specified is not accessible anymore.	This is a severe error, but need not be fatal. Contact support.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
2302	The parameter '$1' with value '$2' is not valid.	Specified value for a parameter is not valid.	Evaluate the parameter. If it is a configurable parameter, ensure proper value is specified.
2400	Failed to connect to Cisco Unified CM. Error: $1	Failure in retrieving information from Cisco Unified CM.	Cisco AXL WebService should be in running state.
2401	Failed to authenticate into Cisco Unified CM: Error: $1.	No Digital certificate found in truststore.	Upload updated Digital cert for Cisco Unified CM.
2402	Failed to locate attached phone to TelePresence device.	No Phone configured on shared line with telepresence equipment.	Configure shared line with IP Phone.
2403	Failed to locate room information attached to TelePresence equipment.	Missing Room information for Telepresence Equipment.	Configure Room information using steps specified in CTS-Manager Configuration guide
2404	Failed to send AXL Message to Cisco Unified CM. Error: $1.	Failure in sending information request to Cisco Unified CM. 1. Incorrect digital certificate is uploaded. 2. Incorrect credentials specified in Cisco Unified CM Application user.	1. Fix the certificate. 2. Correct Cisco Unified CM AppUser credentials.
2405	Failed to retrieve publisher and/or subscriber nodes.	Failure in discovering Cisco Unified CM Node information from DB. 1. Incompatible Cisco Unified CM version 2. Specified Node is not a Cisco Unified CM publisher.	1. Use compatible Cisco Unified CM version. 2. Publisher node hostname should be used.
2406	Failed to authenticate and connect with Cisco Unified CM '$1'. Error: $2.	Invalid credentials and/or hostname. 1. Incorrect Cisco Unified CM App User credentials 2. Incorrect publisher node hostname is specified.	1. Correct App User credentials and publisher node configuration.
2407	Failed to create CTI Adapter to Unified CM '$1'. Error: $2.	Failure in authenticating and connecting with CTIManager.	1. Verify Cisco Unified CM App User credentials 2. Verify CTIManager service is activated on the publisher node.
2409	Failed to create or update TelePresence equipment information.	Failure in creating Telepresence Equipment in DB.	1. Ensure DN is configured.
2411	CTI Manager on Cisco Unified CM is down.	Failure in creating provider instance.	1. CTIManager is not running.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
2415	Failed to connect to RIS Manager.	Failure in retrieving ip address from CiscoUnified CM.	1. SOAP Webservice for RIS should be running. 2. Check Cisco Unified CM AppUser has correct privileges.
2418	Failed to get list of addresses from CTI Provider.	Cisco Unified CM CTI Provider in error state.	Contact Cisco TAC for Unified CM issues.
2419	Failed to retrieve IP Address for requested device.	Cisco Unified CM RIS WebService is not running.	Active SOAP webservice.
2420	Failed to discovery TelePresence equipment.	One of the Unified CM interface is down.	Contact Cisco TAC for Unified CM issues.
2422	Directory number is not configured.	Directory number is not configured.	Configure Directory number.
2423	Incompatible Cisco Unified CM Configured. Please verify the supported Unified CM version inside Supported versions table.	Incompatible Cisco Unified CM version.	Correct Cisco Unified CM version.
2424	Failure inside scheduled maintenance operation.	Execution of scheduled maintenance for Database or TelepresenceEquipment Discovery or Exchange sync or Calendar schedule push failed.	Contact Cisco TAC for detailed investigation.
2425	Failed to discover timezone information from Cisco Unified CM.	TimeZone information not configured or available in Cisco Unified CM.	Contact Cisco TAC for Cisco Unified CM issues.
2426	Failed to discover telepresence capability information from endpoints.	Failure in discovering capability information from Telepresence equipment endpoints. It is most likely due to an older version of the Telepresence equipment not having the support for capability information.	Check the version of Telepresence equipment, and upgrade to a later version if necessary.
2427	More than one IP Phone configured on shared DN with telepresence equipment.	There is more than one IP phones that share the same DN as the specified Telepresence equipment endpoint.	Remove extra IP Phones or assign them with new DN, such that the Telepresence equipment endpoint only has one IP phone sharing its DN.
2428	CTI Control is disabled for the IP Phone.	The specified Cisco IP Phone that is configured for the Telepresence equipment endpoint is not set with CTI control enabled.	Verify the IP phone configuration in Unified CM Admin, and configure it to allow CTI control.
2429	Failed to update time zone '$1'. Error: $2.	An internal server error.	Contact support.
2430	CTS device '$1' does not support Interoperability.	The CTS does not support Video Conferencing Interoperability.	Upgrade the CTS to a version that supports Interoperability with Video Conference.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
2500	Failed to send message/event.	ActiveMQ message system is failing.	Contact Cisco TAC for detailed investigation.
2601	Error getting detail for meeting ID '$1'.	CTS-Manager fails to extract meeting detail because either the scheduler ID or the meeting serial ID is null.	Check the URL that is provided in the email notification. The URL cannot be altered in anyway.
2602	Error getting certificate configuration file '$1'.	The cert-conf.xml does not exist under catalina.home. Something occurred during installation.	Contact support.
2603	Error loading certificate named: '$1'.	CTS-Manager fails to load the given certificate into the system.	Take corrective action according to the detail message and try again.
2604	Error deleting certificate unit '$1' of category '$2'. Error: '$3'.	CTS-Manager fails to delete the given cert.	Take corrective action according to the detail message and try again.
2605	Error $1 DHCP setting. CLI error code: $2.	CTS-Manager fails to enable/disable DHCP setting. Detail error message is given.	Take corrective action according to the detail message and try again.
2606	Error setting IP address and/or subnet mask. CLI error code: $1.	CTS-Manager fails to set new IP settings.	Take corrective action according to the detail message and try again.
2607	Error setting default gateway. CLI error code: $1.	CTS-Manager fails to change default gateway setting.	Take corrective action according to the detail message and try again.
2608	Error setting SNMP data. Command executed: '$1'. Error: '$2'.	CTS-Manager fails to execute SNMP setting script to set new SNMP setting.	Take corrective action according to the detail message and try again.
2609	Failed to '$1' SNMP service. Error: '$2'.	CTS-Manager fails to use ControlCenter to perform the given action on SNMP daemon.	Try to use CLI to activate/deactivate SNMP service. Contact support.
2610	Software upgrade already in progress.	Users attempt to start another software upgrade while there is an upgrade going on. There can be only one upgrade at any time.	Wait until the current upgrade completes and try again.
2611	Failed to upgrade software. Error: '$1'.	CTS-Manager fails to upgrade software due to the given error message.	Take corrective action according to the detail message and try again.
2612	System is restarting. Try again later.	The system is being restarted. Users are disallowed to log in while the system is being restarted.	Wait a few minutes and try to log in again.
2613	Webapp home directory '$1' does not exist.	The webapp directory does not exist. Something has occurred during installation.	Users should not see this error. Contact support.
2614	System is being maintained. Try again later.	Either a database restore or system restart is in progress. Users are prevented from logging in, and this error is shown on the log-in page.	Wait a few minutes and try to log in again.
2615	Cannot delete own role mapping: '$1'.	Users whose role is Administrator is trying to delete his own role mapping on the Access Management screen.	Users cannot delete his own role mapping. Super User can delete anything.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
2616	FQDN '$1' is not a group FQDN.	Users enter an invalid user FQDN in the Role to LDAP mapping dialog box (during Access Management configuration).	Check the entered FQDN and try again.
2617	Failed to create remote account '$1'. Error: '$2'. Account name must contain only lower case alphabetic characters. Upper case, digit, and special characters are not allowed.	CTS-Manager fails to create the requested remote account. Detail error message is given.	Take corrective action according to the detail message and try again.
2618	Cannot view more than one meeting in the same session. Log out of session on meeting '$1' first.	Viewing more than one meeting in the same UI session is not allowed.	Log out of the session on the other meeting first and try again.
2619	Server is being restarted. Try again later.	An attempt to view the UI while server is being restarted.	Wait a few minutes and try to log in again.
2620	Email ID '$1' specified in URL is different than ID '$2' found in database.	The URL that is used to view a meeting contains a different user ID than the meeting scheduler. This request will be blocked with this error shown in the UI.	Make sure the user uses the exact same URL that is provided in the CTS-Manager generated email. After verifying the URL, if it still fails, contact support. In CTS-Manager 1.1, this could occur when switching between versions.
2621	Missing required URL parameter '$1'. Contact Administrator.	The URL that is used to view a meeting is missing a required parameter to retrieve the meeting information.	Make sure the user uses the exact same URL that is provided in the CTS-Manager generated email. After verifying the URL, if it still fails, contact support.
2622	Error setting primary DNS. CLI error code: $1	Failed to set requested primary DNS on the platform, CLI returned an error	Verify DNS name again
2623	Error setting secondary DNS. CLI error code: $1	Failed to set requested secondary DNS on the platform, CLI returned an error	Verify DNS name again
2624	Duplicate entry. Role '$1' for this Group FQDN already exists	Duplicate name specified for a rile.	Verify the role name again
2626	Error setting Domain. CLI error code: $1.	Failed to set the domain name	Refer to Domino installation and verify domain name
2627	Error deleting the primary DNS. CLI error code: $1	Failed to delete the DNS name, CLI returned an error	Contact Cisco TAC for detailed investigation.
2628	Error deleting the secondary DNS. CLI error code: $1	Failed to delete the DNS name, CLI returned an error	Contact Cisco TAC for detailed investigation.
2629	Invalid certificate type named: '$1'.Valid Certificate file extensions .cer and .der.	Incorrect cert file is used	Self explanatory

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
2630	Meeting query results in more than max $1 instances. Change search criteria and try again.	User has requested more than max allowed meetings inside meetings view.	Change search criteria to narrow down the number of meetings inside meetings view.
2632	Failed to enable Interoperability. Some devices do not support Interoperability. Click on the links to view the error devices.	At least a CTS or CTMS does not support Interoperability. Enabling Video Conferencing Interoperability support requires all CTS and CTMS support Interoperability.	Upgrade the CTS or CTMS that does not support Interoperability to a version that supports Interoperability.
2633	Error updating meeting. Meeting ID not found '$1'.	The meeting does not exist in the CTS-Manager. It was possibly deleted after the meeting is displayed on the UI.	Refresh the Admin UI web page. If the meeting still exists and the problem persists, contact support.
2644	Failed to enable Intercompany. One or more occurrences have Video Conferencing enabled.	The recurrent meeting has one or more instances as interop meeting .	Change the interop instances to be normal or non-interop meetings and then try to make the meeting as an intercompany meeting.
2700	Failed to display requested certificate :	Invalid Certificate	Reload a new certificate and try again.
2803	Error during configuration policy delete: $1.	Failed to delete configuration policy	Contact Cisco TAC for detailed investigation.
2808	A configuration policy with this policy name $1 already exists.	Duplicate name specified for a policy	Self explanatory
3001	Unable to start adapter '$1'. Error: '$2'.	CTS-Manager fails to start one of its client adapters. The adapter name and detail message is given.	This is a fatal error. Contact support.
3002	Failed to sync '$1'.	CTS-Manager fails to perform synchronization for the given Exchange room or database.	Using the Exchange or Domino configuration UI, try to manually start the sync for the given room or database. If unsuccessful then contact support.
3003	Failed to process meeting '$1'.	CTS-Manager fails to process a meeting with given subject or system ID.	Update the meeting using the calendaring tool (Outlook or Lotus Notes) to see if the meeting can be processed again. Contact support.
3004	Failed to update room '$1'.	CTS-Manager fails to update some information on the given room.	Contact support.
3005	Failed to process '$1' event for room '$2'.	CTS-Manager fails to process a specific room event.	Contact support.
3100	Unexpected Error: $1.	CTS-Manager Exchange Adapter has encountered internal error.	Contact Cisco TAC for detailed investigation.
3101	Missing Config Param Error: $1.	Required configuration parameter is missing.	Specify the required parameter and retry operation.
3102	Exchange Connection Error: $1.	Connection to Exchange could not be established.	Make sure specified connection are correct, Exchange host is reachable.

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
3103	Param Format Error: $1. Given value:($2).	Specified Exchange Adapter parameter format is incorrect.	Correct the parameter based on message and retry operation.
3105	Room Subscription Error: Room:($1). Message:($2)	Room account does not exist in AD/Exchange, CTS-Manager account does not have proper permission to read room calendar, connection to Exchange might be down, room account on Exchange modified.	Setup room account in AD/Exchange, give CTS-Manager account read access to room's calendar, wait for CTS-Manager to regain connection to Exchange else restart CTS-Manager.
3106	Room Unsubscription Error: Room:($1). Message:($2)	Connection to Exchange might be down, room account on Exchange modified.	Wait for CTS-Manager to regain connection to Exchange else restart CTS-Manager.
3107	Room Search Error: Room:($1). Message:($2)	Connection to Exchange might be down, room account on Exchange modified.	Wait for CTS-Manager to regain connection to Exchange else restart CTS-Manager.
3109	Room Renewal Error: Room:($1). Message:($2)	Connection to Exchange might be down, room account on Exchange modified.	Wait for CTS-Manager to regain connection to Exchange else restart CTS-Manager.
3111	Lock Error: Cannot acquire lock on element:($1).	Error in resolving deadlocks in server application threads.	This is a severe error, but need not be fatal. Contact support.
3112	Mailbox Error: Error during mailbox size computation:($1).	CTS-Manager is unable to read mailbox quota.	Specify specific mailbox quota for CTS-Manager account in Directory Server.
3113	Mailbox Quota Error: Cleanup account on Exchange. Quota:($1) Current size:($2).	Super user mailbox has filled up to the quota.	Cleanup super user account on Exchange.
3114	Invalid Domain Name	The specified domain name is invalid. Users would see this error during Test Connection of Exchange settings.	Correct the domain name and try Test Connection again.
3115	Invalid User Name. User name cannot contain space(s).	Invalid User Name. Exchange user name cannot contain space(s).	Correct the user name.
3116	Exchange connection succeeded	Not an error condition.	
3501	Email cannot be sent for meeting in validation state '$1'.	Internal error.	Contact support.
3502	Unknown email request '$1'.	Internal error	Contact support
3503	Invalid meeting scheduler (subject '$1'). Error: field '$2' has invalid value '$3'.	Internal error	Contact support
3504	Discarded email request '$1' after '$2' attempts.	CTS-Manager has attempted too many times to send email for a meeting but all have failed.	Contact support
3505	Too many email requests submitted for ID '$1'.	CTS-Manager under possible DoS attack. Too many email requests for the same meeting are being submitted.	Contact support

Table 13-10 Cisco TelePresence Manager Error Messages (continued)

Code	Message	Explanation	Recommended Actions
3601	Room display segments information is missing.	Room does not have any display segment information.	This is a severe error, but it should never happen. Contact support.
3800	MCU is not reachable:	CTS-Manager is unable to communicate with the MCU	Check for any connectivity issue and check the MCU status.
3801	Failed to authenticate with MCU:	MCU is unable to find CTS-Manager hostname/IP address or unable to authenticate the CTS-Manager, therefore it will not process any request from this CTS-Manager.	Verify that the MCU is configured properly with the correct CTS-Manager settings.
3802	An error occurred at MCU:	MCU has reported an error. The error detail is given in the message.	Take corrective action according to the detail message and try again.
3803	MCU failed to authenticate:	CTS-Manager is unable to authenticate the MCU, therefore it will not process any request from this MCU	Verify that the authentication information that are entered in CTS-Manager and MCU match.
3804	HostName or IP Address not found for MCU:	MCU is unknown to CTS-Manager, therefore it will not process any request from this MCU	Verify that this MCU is configured properly in CTS-Manager.
3805	CTMS '$1' does not support Interoperability.	The CTMS does not support Interoperability.	Upgrade the CTMS to a version that supports Interoperability.
3806	A meeting '$1' has error. Meeting is not pushed to MCU '$2'.	Meeting does not have the required information.	Contact Support.
4000	Domino Connection Error: $1.	Failed to connect to Domino server	Verify IP connectivity to Domino server, DIIOP task should be running
4001	Domino connection was established, but couldn't open the specified Domino resource database	Domino resource may be inaccessible for various reasons.	Contact Cisco TAC for detailed investigation.
4002	Domino Domain value '$1' specified is not correct.	Domino domain value is incorrect	Verify if Domino domain name is correct or has changed