Cisco TelePresence Manager Release 1.9 Administration and Installation Guide

Release 1.9.x
May 29, 2012

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-22226-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

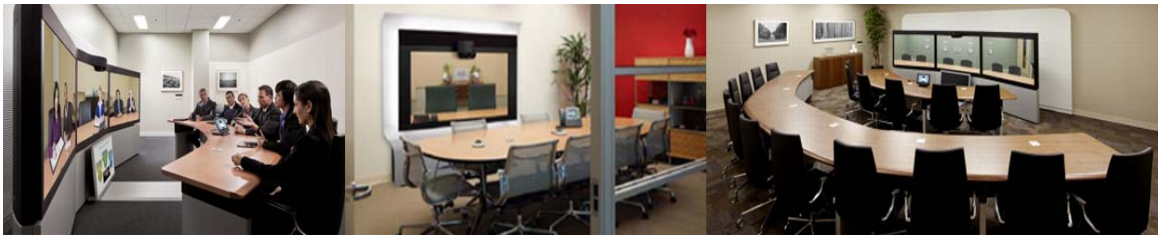
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco TelePresence Manager Release 1.8 Administration and Installation Guide
© 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xvii

Obtaining Documentation, Obtaining Support, and Security Guidelines xvii

Audience and Scope xvii

What's New in this Release xvii

New in Release 1.9: xvii

CHAPTER 1 **General Information About Cisco TelePresence Manager** 1-1

Contents 1-1

Overview of the Cisco TelePresence Manager Administration Guide 1-2

Terminology 1-3

Introduction to the Cisco TelePresence System 1-4

Making Point-to-Point Cisco TelePresence calls 1-4

Supported Endpoints 1-4

Components of the Cisco TelePresence System 1-5

Cisco TelePresence Manager Specifications and System Requirements 1-6

Installation Procedures Guidelines 1-8

CHAPTER 2 **Pre-Install System Setup for Cisco TelePresence Manager** 2-1

Contents 2-1

Introduction 2-1

System Components 2-1

Installation Considerations 2-2

Pre-Installation Procedure Guidelines for Initial Network Setup 2-3

CHAPTER 3 **Configuring Microsoft Exchange for Cisco TelePresence Manager** 3-1

Contents 3-1

Introduction 3-1

Pre-Configuration Setup Guidelines 3-2

Configuring Microsoft Exchange for CTS-Manager 3-3

Deploying with Microsoft Exchange 2003 3-3

Deploying with Microsoft Exchange 2007 - WebDAV 3-4

Deploying with Microsoft Exchange 2007 and 2010 EWS 3-9

Exchange Migration Guide 3-12
Migrating from Exchange Server 2003 to 2007 3-12
Continue Using WebDAV Protocol 3-13
Use EWS Access 3-13
Migrating from Exchange Server 2003 to 2010 3-15
Migrating from Exchange Server 2007 to 2010 3-15
Applying CTS-Manager Throttling Policy for Exchange 2010 SP1 3-16
Throttling Policy Parameter Definitions and Values 3-17
Restoring the Microsoft Throttling Policy for Exchange 2010 SP1 3-21

CHAPTER 4 **Configuring IBM Domino Server for Cisco TelePresence Manager** 4-1
Contents 4-1
Introduction 4-1
Important Considerations 4-1
Pre-Configuration Procedure Guidelines for IBM Domino Setup 4-2
Configuring IBM Domino for CTS-Manager 4-2
Directory Assistance in a Domino Deployment 4-4

CHAPTER 5 **Configuring Scheduling API for Cisco TelePresence Manager** 5-1
Contents 5-1
Introduction 5-1
Overview 5-1
Requirements 5-2
CTS-Manager Requirements 5-2
Licensing Requirements 5-3
LDAP Requirements 5-3
Important Considerations 5-3
Pre-Configuration Procedure Guidelines for Scheduling API Setup 5-3
Configuring Scheduling API for CTS-Manager 5-4

CHAPTER 6 **Configuring Cisco Unified Communications Manager for Cisco TelePresence Manager** 6-1
Contents 6-1
Introduction 6-1
Important Considerations 6-1
Pre-Configuration Procedure Guidelines for Cisco Unified CM Setup 6-2
Configuring Cisco Unified CM for CTS-Manager 6-3
For Deployments Using Microsoft Exchange or IBM Domino or Scheduling API 6-3

Configuring Cisco Unified CM Server Names 6-5
Logging into Cisco Unified CM Administrator 6-6
Configuring the Options File 6-6
Adding a Cisco TelePresence Device 6-7
Download Device Pack 6-7
Install Device Pack 6-8
Creating and Configuring a Cisco TelePresence Device 6-8
Adding a Cisco TelePresence Device 6-8
Configuring a Cisco TelePresence Device 6-9
Device Information for Cisco TelePresence Devices 6-9
Assigning a Directory Number to a TelePresence Device 6-13
Verifying a TelePresence Device is Registered to Unified CM 6-13
Adding a TelePresence Device to the Application User 6-14

CHAPTER 7 **Installing and Configuring Cisco PreQualification Assistant** 7-1
Contents 7-1
Introduction 7-2
Pre-Configuration Procedure Guidelines for Checking Initial Network Setup 7-2
Installing the PreQualification Assistant Tool 7-3
Running the Tool - Using the Tool Application Window 7-6
Menu Commands 7-8
File Menu Commands 7-8
System Menu Command 7-8
Host Configuration Window 7-9
Test Status Window 7-10
Using PreQualification Configuration Forms 7-11
Cisco Unified Communications Manager Configuration Form 7-11
Test(s) Enabled by the Host Configuration Form 7-12
Test Host Configuration Forms in a Generic Environment 7-13
LDAP (Generic) Test Configuration Form 7-14
Test Configuration Forms in a Microsoft Exchange Environment 7-16
LDAP Server (Active Directory) Test Configuration Form 7-18
Calendar Server (Microsoft Exchange) Host Configuration Form 7-20
Test Configuration Forms in an IBM Domino Environment 7-21
LDAP (Domino Directory) Host Configuration Form 7-23
Calendar Server (IBM Domino) Configuration Form 7-25
Cisco Unified Communications Manager Server (IBM Domino) Configuration Window 7-27
LDAP (Domino Directory) Host Configuration Form 7-29

Test Configuration Forms in a Microsoft Exchange Web Services (EWS) Environment 7-30
LDAP Server (Active Directory) Add/Edit Configuration Form 7-31
LDAP Server Microsoft Exchange EWS Calendar Server Configuration Form 7-33
WebEx Server 7-35

CHAPTER 8 **Configuring UCS Server and VMware for Cisco TelePresence Manager** 8-1
Contents 8-1
Introduction 8-1
Installation Guidelines 8-2
Requirements 8-3
Firmware Recommendation and Upgrade 8-3
Checking the Firmware Version on the UCS Server 8-3
Upgrading the Firmware on the UCS Server 8-4
Configuring RAID on the UCS Server 8-6
Installing VMware on the UCS Server 8-8
Installing the VMware Client and Setting Up the Datastore 8-9
Disabling LRO 8-11
Creating the Virtual Machine 8-11
Installing CTS-Manager 8-13
Upgrading VMware Tools 8-13
Installing the VMware License Key 8-14
Setting Automatic Startup for CTS-Manager 8-15

CHAPTER 9 **Installing or Upgrading Cisco TelePresence Manager** 9-1
Contents 9-1
Introduction 9-1
Installation Guidelines 9-2
Installing Cisco TelePresence Manager from DVD 9-3
Required Information and Equipment 9-3
Installation Procedure for Cisco TelePresence Manager 9-3
Installation Page Values Defined 9-4
Recovering Administrator and Security Passwords 9-7
Recovery Procedure 1: 9-7
Recovery Procedure 2: 9-8
System Log Error Detection 9-8
System Messages 9-8
System Error - AXL Error or Invalid Credential 9-10

Software Upgrade 9-10
Upgrading to Cisco TelePresence Manager 1.9 9-11
Switch Versions 9-11
Upgrade Software 9-11
Cisco TelePresence Manager Window 9-19
Header Pane 9-19
System Status Pane 9-19
Navigation Pane 9-20
Work Pane 9-21
Preferences 9-22

CHAPTER 10 **Initializing Cisco TelePresence Manager** 10-1
Content 10-1
Introduction 10-1
Post-Install Guidelines for CTS-Manager 10-2
Initializing CTS-Manager After Installation 10-3
Required Information and Equipment 10-3
Initialization Procedure 10-4
Log In and Set Time Zone 10-4
Server Roles 10-5
Select Configuration Options 10-5
Select Calendar Server 10-9
Configure LDAP Servers 10-10
Configure Unified CM 10-14
Configure Calendar Server 10-15
Configure Database Backup Schedule 10-19
Dashboard for Verification of Installation Status 10-21

CHAPTER 11 **Additional Installation Configurations for Cisco TelePresence Manager** 11-1
Contents 11-1
Post-Install Guidelines for CTS-Manager 11-2
Introduction to the CTS-Manager Administration Software 11-3
Administrator Role 11-3
SysAdmin Role 11-4
Live Desk Role 11-4
Licensing for CTS-Manager 11-6
Feature-Based Licenses 11-6
Count-Based Licenses 11-6

Getting Licenses for CTS-Manager 11-7
New Customers 11-7
Existing Customers Upgrading to CTS-Manager 1.9 11-8
Existing CTS-Manager 1.9 Customers Adding More Endpoints or Licensed Features 11-8
Viewing and Uploading Licenses 11-8
Summary 11-9
Licensing Grace Period 11-9
License Files 11-10
Uploading Licenses 11-11
When You Need New Count-based (Endpoint-based) Licenses 11-12
CTS-Manager License Backup and Restore 11-12
Hardware Replacement and New Licensing 11-12
Getting an Upgrade License 11-12
Security 11-13
LDAP Server 11-14
Settings for LDAP 11-14
Multiple LDAP Peer Domains 11-15
Field Mappings 11-15
Microsoft Exchange Deployments 11-15
Edit 11-18
Verifying Field Mapping Data 11-21
IBM Domino Deployments 11-22
Verifying Field Mapping Data 11-24
Deleting Server 11-25
Calendar Server 11-25
Microsoft Exchange 11-29
Synchronization Operations 11-30
IBM Domino 11-35
Synchronization Operations 11-36
System Settings 11-38
IP 11-39
NTP 11-40
SNMP 11-41
Configuring SNMP Traps on CTS-Manager 11-43
Modifying SNMP Trap Settings 11-45
Remote Account 11-46
Password 11-47
System 11-47
Cluster 11-48

Database - Status, Backup, and Restore 11-48
Settings 11-48
Backup 11-50
Changing the Backup Schedule 11-50
Backing Up CTS-Manager Data 11-51
Remote Storage Host Fields 11-51
Viewing Backup History 11-52
Restore 11-52
Restoring Backup Data 11-53
To restore data from a backup: 11-54
Unified CM 11-54
Bridges and Servers 11-58
Adding a Bridge or Server 11-59
Editing a Bridge or Server 11-60
Deleting a Bridge or Server 11-60
Migrating All Meetings from a CTMS 11-61
How Meeting Migration Works with CTMSs 11-61
Distributing All Meetings from a TS 11-62
Resource Allocation with CTMS and TS Devices 11-62
Refreshing the List of Bridges or Servers 11-63
Cisco TelePresence Multipoint Switch (CTMS) 11-63
Adding a CTMS 11-63
Cisco TelePresence Server (TS) 11-65
Adding a Cisco TelePresence Server 11-65
Cisco TelePresence Recording Server (CTRS) 11-67
Adding a CTRS Device 11-67
WebEx 11-68
Adding a WebEx Site 11-68
Deleting a WebEx Site 11-71
Collaboration Manager 11-72
Cluster Management 11-73
Access Management 11-73
LDAP Lookup Method to Authorize User Roles 11-75
Adding an LDAP Group to a Role 11-75
Alert Management 11-77
Device Groups 11-78
Grouping Devices 11-78
Editing Groups 11-80
Deleting Groups 11-80

Endpoints 11-81
Registering EX, MX or C-series Endpoints 11-81
Importing Endpoints 11-85
Creating Resource Bundle Endpoints 11-86
Scheduling Meetings with Video Conferencing, EX and C-Series Endpoints 11-87
VC meetings Scheduled Before Upgrading to CTS-Manager Release 1.7 or 1.8 11-87
Live Desks 11-88
Live Desk Role 11-88
Creating Live Desk Personnel 11-89
Assigning an Endpoint to a Specific Live Desk 11-90
Policies 11-91
CTMS Policy 11-91
CTS Policy 11-92
TS Policy 11-92
Application Settings 11-93
Email 11-94
Meeting Notification Email 11-94
Remove Email Prefixes from Meeting Subject on Phone 11-95
Additional Text in Email 11-95
System Alert Notification Emails 11-95
Bridges and Servers 11-96
Multipoint Conference Scheduling 11-96
Interoperability with Video Conferencing 11-97
TelePresence Call-In Number 11-98
Studio Mode Recording 11-98
WebEx 11-98
CTMS Network Multipoint 11-99
Intergroup Scheduling 11-99
Intercompany 11-100
Locales 11-100
Selecting and Publishing Locales for Meeting Manager and Meeting Organizer Email Notifications 11-100
Benefits Reporting 11-101
Usage Survey 11-103
Enable Meeting Organizer Usage Survey 11-103
Select a Locale to Preview or Customize Survey 11-103
Preview Survey Questions 11-104
Customizing the Survey 11-105
Preview Your Questions 11-110
Default Survey Questions 11-111

Meeting Options 11-112
Enable Tentative Room Reservations 11-112
Start Meetings Early 11-114
Extend Multipoint Meetings 11-114
Important Information About Resource Allocation 11-116
CTS-Manager Redundancy Failover Procedure 11-117
Cold Standby 11-117
Warm Standby 11-119
CTS-Manager Redundancy Failover Procedure 11-119
CTMS Redundancy Failover Procedure 11-120

CHAPTER 12 **Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager** 12-1
Contents 12-1
Introduction 12-1
Post-Install Guidelines for CTS-Manager 12-2
Before Configuring Cisco WebEx in CTS-Manager 12-2
Setting Up Cisco WebEx Administration Site Account 12-3
Specifying Cisco TelePresence Integration Options 12-3
Cisco WebEx First-Time Setup in CTS-Manager 12-4
Enabling WebEx and Selecting Default WebEx User Type 12-5
Configuring a Cisco WebEx Site 12-7
WebEx Proxy Server 12-7
Multiple WebEx Sites 12-9
Obtaining the Cisco WebEx Site Security Server Certificate 12-9
Obtaining Your Certificate Using Internet Explorer 12-9
Obtaining Your Certificate Using Firefox 12-10
Adding Your Certificate to CTS-Manager 12-10
Configuring Cisco WebEx Users in CTS-Manager 12-12
WebEx User Types 12-12
Configuring WebEx Users 12-13
First-Time Scheduling of TelePresence Meetings with WebEx 12-15
Using Calendar Client and Meeting Manager 12-15
Using Microsoft Outlook and the WebEx Productivity Tools Plug-in 12-20
Configuring Other Applications 12-23

CHAPTER 13 **Monitoring and Supporting Cisco TelePresence Manager** 13-1
Contents 13-1
Introduction 13-2

Post-Install Guidelines for CTS-Manager 13-2
Meetings 13-3
Process/Response Times for Scheduled Meetings 13-4
Modifying Meeting Details from a Calendar Client 13-4
Calendar Scheduling Limitation 13-5
Generating Scheduled Meeting Reports 13-5
Exporting Scheduled Meeting Data 13-7
Meeting Details 13-8
Summary 13-9
Bridges and Servers 13-9
CTMS Network 13-11
Intercompany 13-11
WebEx 13-13
Usage Survey 13-13
Meeting Options 13-13
Status Dashboard 13-14
Metrics Dashboard 13-16
Endpoint Utilization 13-18
Meeting Benefits 13-19
Meetings by Purpose 13-20
Meetings by Benefits 13-20
Scheduled Meetings 13-20
Ad Hoc Meetings 13-20
Meetings Avoided Travel 13-20
Travel Savings 13-20
Emissions Savings 13-21
Productivity Savings 13-21
Endpoints Added 13-21
TelePresence Utilization 13-21
Meeting Benefits 13-23
VC Utilization 13-24
Users 13-25
Current Logins 13-25
Meeting Organizers 13-26
Endpoints 13-27
Manually Updating Schedules on the Cisco TelePresence Endpoint Phone or Control Device 13-30
Viewing Scheduled Meetings for a Specific Endpoint 13-30
Tentative Room Reservation 13-31
Bridges and Servers 13-33

Summary 13-33
Generating Bridges or Servers Reports 13-33
Capability 13-40
Unified CM 13-42
Command Line Interface 13-43
Starting a CLI Session 13-43

CHAPTER 14 **Meeting Manager and CTS-Manager Emails** 14-1
Contents 14-1
Introduction 14-2
User Authentication 14-2
Point-to-Point Meeting 14-2
Multipoint Meeting 14-4
Video Conferencing Meeting 14-6
TelePresence Call-In and WebEx Meeting 14-8
Action Required Email 14-10
Video Conferencing Error Email 14-13
Meeting Manager 14-14
Summary 14-15
Intercompany 14-15
Intercompany Host Meeting Options 14-16
Intercompany Participant Meeting Options 14-17
WebEx 14-18
Usage Survey 14-22
Meeting Options 14-22
Allowing Other Users to Manage Your Meetings 14-23
System Alert Notification 14-24

CHAPTER 15 **Supported MIBs for Cisco TelePresence Manager** 15-1
Contents 15-1
Introduction 15-1
MIB Support 15-1

CHAPTER 16 **Troubleshooting Cisco TelePresence Manager** 16-1
Contents 16-1
Introduction 16-2
System Information 16-2

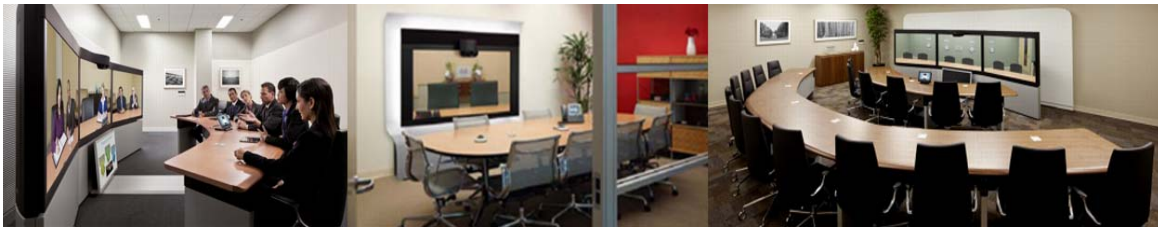
System Resources 16-3
System Messages 16-5
Log Files 16-6
Log Files 16-6
Log Levels 16-7
Archive 16-8
Scheduled Meeting and Endpoint Issues 16-10
Endpoint Phone/Display Device User Interface Issues 16-16
Cisco TelePresence Manager Database Issues 16-17
Bridges and Servers Issues 16-18
Cisco Unified Communications Manager (Unified CM) Issues 16-19
Calendar Server and LDAP Interface Issues 16-20
LDAP Server Issues 16-20
Microsoft Exchange Calendar Server Issues 16-21
IBM Domino Calendar Server Issues 16-24
Scheduling API Issues 16-26
Web Browser Error Messages 16-26
JavaScript Error Message 16-26
Safe ActiveX Checking Message 16-27
System Alert Notifications 16-27
The No-Show Meetings and Meetings without Usage Survey Responses 16-27
Mailbox Alert 16-28
Certificate Expiry 16-28

APPENDIX A **Cisco TelePresence Manager System Messages** A-1
Contents A-1
System Message Overview A-1
System Messages By ID Number A-4

APPENDIX B **Replacing a Cisco TelePresence System Codec** B-1
Overview B-1
Replacing a Cisco TelePresence System Codec B-1

APPENDIX C **Reconfiguring CTS-Manager and CTMS Addressing** C-1
Overview C-1
Before You Begin C-1
Changing IP Address and Hostname of CTS-Manager C-1

Changing IP Address of CTMS C-2



Preface

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

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 1.7.

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 for Release 1.9:

New in Release 1.9:

- **Network Multipoint for Scheduled Meetings**

  CTS-Manager now supports scheduled network multipoint meetings. A maximum of 11 CTMS devices and 440 segments are supported in a meeting. CTMS Network Multipoint is enabled by logging in to the CTS-Manager Administrative Web UI and going to the **Configure > Application Settings > Bridges and Servers** tab.

For more information, see the CTMS Network Multipoint 1.9 Design Guide for release 1.9, at the following URL:

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

- **WebEx OneTouch Meeting Scheduling with WebEx Productivity Tools for Microsoft Outlook**

  Meeting organizers can schedule TelePresence meetings with WebEx directly in Microsoft Outlook using the WebEx Productivity Tools plug-in. Logging into CTS-Manager is not required.

- **Device Grouping in CTS-Manager**

  You can group endpoints with CTMS devices, so that when a meeting is scheduled, CTS-Manager reserves devices from the same group as the endpoint(s). Grouping is especially useful for large geographically-dispersed companies with many endpoints and CTMS devices. Groups are created and managed by logging in to the CTS-Manager Administrative Web UI and going to **Configure** > **Device Groups**.

- **Virtualization Support**

  Multiple instances of CTS-Manager and CTMS can now be installed as virtual machines on the UCS C210 M2 server using VMware ESXi 4.1.

  - 1 CTS-Manager and 1 CTMS can be installed on a single UCS server.
  - CTS-Manager with up to 2 instances on a single server, for service provider deployments with no more then 50 endpoints under management per instance of CTS-Manager.

- **Support for CTX without external LDAP**

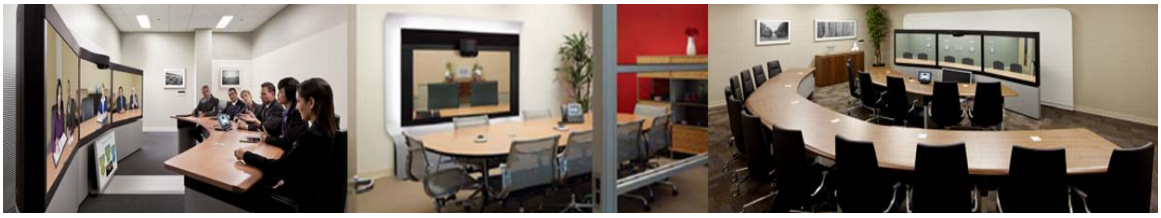
  CTX to CTS-Manager integration using scheduling API no longer requires and LDAP/AD server for authentication.

- **Clustering Support Discontinued**

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

- **MXE Support Discontinued**

  In earlier versions of the CTS-Manager release notes, CTMS 1.8 and Media Experience Exchange (MXE) 5600 with limited interoperability was supported. Based on recent testing, it has been determined that MXE 5600 interop with CTMS 1.8 or later is a solution Cisco can no longer recommend to customers. As a result, support for MXE 5600 is discontinued with CTS-Manager and CTMS 1.8 and 1.9. Existing customers are encouraged to migrate to TelePresence Server for interop.



CHAPTER 1

General Information About Cisco TelePresence Manager

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

Contents

- Overview of the Cisco TelePresence Manager Administration Guide, page 1-2
  - Terminology, page 1-3
- Introduction to the Cisco TelePresence System, page 1-4
  - Making Point-to-Point Cisco TelePresence calls, page 1-4
  - Components of the Cisco TelePresence System, page 1-5
- Cisco TelePresence Manager Specifications and System Requirements, page 1-6
- Installation Procedures Guidelines, page 1-8

Overview of the Cisco TelePresence Manager Administration Guide

Table 1-1 give a brief description of the contents of each chapter in the Cisco TelePresence Manager (CTS-Manager) Administration Guide.

Table 1-1 Administration Guide Chapter Descriptions

Chapter Title	Description
Chapter 1 General Information About 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 System Setup for Cisco TelePresence Manager	This chapter describes the pre-installation and installation features for CTS-Manager.
Chapter 3 Configuring Microsoft Exchange for Cisco TelePresence Manager	This chapter describes the steps needed to configure either Microsoft Exchange 2003 or 2007 and Active Directory.
Chapter 4 Configuring IBM Domino Server for Cisco TelePresence Manager	This chapter describes the steps needed to configure IBM Domino and Domino Directory Server for the CTS-Manager system.
Chapter 5 Configuring Scheduling API for Cisco TelePresence Manager	This chapter describes the steps needed to configure the CTS-Manager scheduling API.
Chapter 6 Configuring Cisco Unified Communications Manager for Cisco TelePresence 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 Cisco TelePresence Manager during installation.
Chapter 7 Installing and Configuring Cisco PreQualification Assistant	This chapter explains how to install and run the Cisco TelePresence Manager PreQualification Assistant tool. It is important to install and run the PreQualification assistant to ensure that the pre-installation setup is performed correctly.
Chapter 8 Configuring UCS Server and VMware for Cisco TelePresence Manager	This chapter explains how to configure the UCS server and VMware for Cisco TelePresence Manager
Chapter 9 Installing or Upgrading Cisco TelePresence Manager	Describes how to install or upgrade CTS-Manager.

Table 1-1 Administration Guide Chapter Descriptions

Chapter Title	Description
Chapter 10 Initializing Cisco TelePresence 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 (endpoint) information, and Cisco Unified Communications Manager for conference room (endpoint) availability and telephone support.
Chapter 11 Additional Installation Configurations for Cisco TelePresence Manager	Describes the configuration features available when you log into CTS-Manager using an Administrator role.
Chapter 12 Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager	Describes the steps for configuring WebEx OneTouch for CTS-Manager.
Chapter 13 Monitoring and Supporting Cisco TelePresence Manager	Describes the monitoring and support features available when you log into CTS-Manager using a Live Desk role.
Chapter 14 Meeting Manager and CTS-Manager Emails	Describes the different email notifications and meeting details window available to Meeting Organizers.
Chapter 15 Supported MIBs for Cisco TelePresence Manager	Provides the MIBs used by the CTS-Manager.
Chapter 16 Troubleshooting Cisco TelePresence Manager	Provides troubleshooting information for CTS-Manager Administrators.
Appendix A Cisco TelePresence Manager System Messages	Provides detailed information about the messages displayed in the Troubleshoot > System Messages window, including explanation and recommended action.

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.
- **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 were previously referred to as Cisco TelePresence rooms.
- **Interop**: Interoperability with video conferencing. The ability for TelePresence meetings to include Cisco TelePresence endpoints and traditional video conferencing/video telephony endpoints.
- **LDAP**: Lightweight Directory Access Protocol
- **VC**: Video conferencing
- **MXE**: Media Experience Engine

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.

Supported Endpoints

The following endpoint models are 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.
- **EX, MX and C-series** - With TC5.0 or later software and Unified CM version 8.6.1.20000-1 or later with device pack 8.6.1.21019-1 installed, these endpoints are discovered automatically. With TC5.0 or earlier software and Unified CM 8.5(1) or earlier, these endpoints must be added manually like video conferencing (VC) endpoints. Only endpoints with TC5.0 or later software support One-Button-to-Push.
  - A point-to-point meeting between an EX, MX or C-series endpoint and a CTS is supported if the CTS supports TIP. If the CTS does not support TIP, a multipoint scheduling device is required.

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. 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 endpoints 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, which is then displayed on the display device.
- **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 network.
- **Calendar server** - Each CTS endpoint has a corresponding mailbox on a calendar server to support scheduling through Outlook, Lotus Notes, or other groupware client. CTS-Manager monitors endpoint calendars and reports errors. CTS-Manager also uses the scheduling information to push meeting schedules to each CTS endpoint which is displayed on the IP phone.
- **LDAP/Active Directory** - Each CTS endpoint's room (endpoint) ID is stored in LDAP/Active Directory. CTS-Manager is the conduit between Active Directory and an endpoint. On login to CTS-Manager users are authenticated to LDAP/AD. No user IDs or passwords are stored in CTS-Manager.
- **Cisco TelePresence Multipoint Switch (CTMS)** - A CTMS provides the resources for multipoint (three or more endpoints) and WebEx meetings. CTS-Manager reports errors with a CTMS and specifies which CTMS is used for each scheduled 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 Media Experience Engine (MXE). This provides interoperability with many standards-based video conferencing systems installed today.
- **Cisco TelePresence Server** - Provides the resources for multipoint (three or more endpoints) meetings.

- **WebEx** - TelePresence Meetings with Webex are scheduled by CTS-Manager through a direct connection to the WebEx Scheduling Server. When the meeting organizer schedules TelePresence meetings with WebEx, the WebEx meeting ID and password are provided in the email sent to meeting organizers for them to forward to the meeting participants.
- 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 Specifications and System Requirements

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

For hardware support and upgrade path information, refer to the CTS-Manager 1.9 Release Notes available on Cisco.com:

http://www.cisco.com/en/US/docs/telepresence/cts_manager/1_9/release/ctm_rn1_9.html

Table 1-2 Product Specifications

Specifications	Description
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 and UCS platforms

Table 1-3 System Requirements

Specifications	Description
Groupware connectivity:	Microsoft • Microsoft Exchange Server: – 2003 SP2 (Windows Server 2003 Enterprise Edition SP2). – 2007 SP3 (Windows Server 2003 SP2 Enterprise Edition 64-bit). – 2007 SP3 (Windows Server 2008 SP2 Enterprise Edition 64-bit). – 2007 SP3 (Windows Server 2008 R2 Enterprise Edition 64-bit). **Note** 2007 is supported with WebDAV and EWS. – 2010 SP1, SP 2 (Windows Server 2008 SP2 Enterprise Edition 64-bit). – 2010 SP3 is supported with CTS-Manager 1.9.1 or later. **Note** The English language version of Microsoft Exchange is required. **Note** For best results, network latency between CTS-Manager and Microsoft Exchange should not exceed 30 ms one way or 60 ms round trip. • Microsoft Outlook client: 2003, 2007 and 2010 – Required Installation: cumulative time zone update for Microsoft Windows operating systems (December 2008 or newer). For more information, refer to: http://support.microsoft.com/kb/979306. – Microsoft Outlook 2003 SP3 is supported only with the following bug fixes installed sequentially, available from Microsoft: http://support.microsoft.com/kb/956310 11.0.8233.0 http://support.microsoft.com/kb/957142 11.0.8234.0 http://support.microsoft.com/kb/959628 11.0.8238.0 http://support.microsoft.com/kb/965495 11.0.8249.0 http://support.microsoft.com/kb/968689 11.0.8309.0 http://support.microsoft.com/kb/971366 11.0.8312.0 **Note** Microsoft Exchange with Entourage client is not supported.
	IBM • IBM Domino Server: 8.5.1 (Operating System: Windows Server 2003 Enterprise Edition SP2, Windows 2008) – The Resource Reservation database must be initially created using the Resource Reservation Template 7 or later. Reservation templates prior to version 7 cannot be upgraded. • IBM Lotus Notes Client: 8.5.1
	Other • Other Groupware integrations with CTS-Manager are allowed using the Cisco Developer CTS-Manager Scheduling-API. Information on the Scheduling API for customers or developers can be found at: http://developer.cisco.com.

Table 1-3 System Requirements (continued)

Specifications	Description
Cisco Unified Communications Manager	Cisco Unified CM 7.1.5, 8.5.1 and 8.6.2.21008-1 are required for TC 5.0 endpoints to be discoverable by CTS-Manager. Version 8.6.1a or 8.6.2 is required for CTMS Network Multipoint feature.
Lightweight Directory Access Protocol (LDAP) connectivity	Active Directory 2003 SP2, 2008 SP2, 2008 R2 Domino Directory, versions: 7.0.x, 8.0.x, 8.5 **Note** CTS-Manager LDAP user and SysAdmin need read permission to the Domino Directory.
Ethernet Cable	Connect to MCS server's NIC Port 1
Web browsers supported	Microsoft Internet Explorer 7.x, 8.x, 9.x (Windows) Firefox 11, 12 (Mac and Windows). **Note** Cisco cannot guarantee correct system behavior using unsupported browsers. When using Firefox, the height of the browser window must be equal to at least 50 percent of the height of the computer screen. If it is less than 50 percent, windows with secondary tabs and tables may not display properly.
Licensing	Licenses are required for the following features: • Endpoints: TelePresence endpoint (room) license. Licenses are available in groups of 10, 50 and 100 endpoints. All TelePresence endpoints must be licensed to be used with CTS-Manager. • Metrics Dashboard and Reporting API: Survey and benefits reports and meeting information for external metrics reporting solutions. • Scheduling API: Scheduling support for organizations that are not using MS Exchange or IBM Domino.
Cisco WebEx Productivity Tools Plug-in for Microsoft Outlook	• WebEx version FR26/FR29 or T28 • Exchange server 2007/2010 • Outlook version 2007/2010 for Windows

Note CTS-Manager is supported only in an enterprise intranet environment. NAT deployment is not supported.

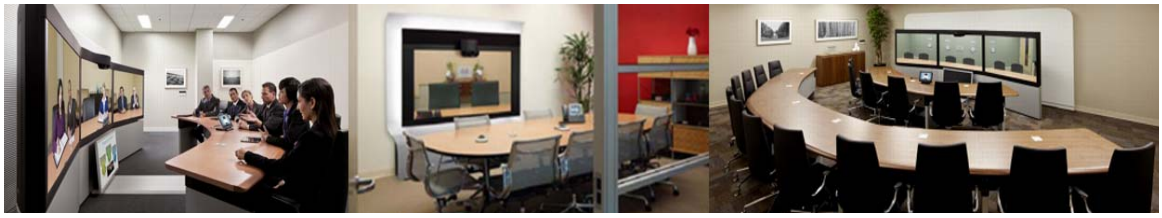
Installation Procedures Guidelines

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

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

Setup 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 Setup for Cisco TelePresence Manager"
Configure Microsoft Exchange for CTS-Manager	This chapter describes the steps needed to configure Microsoft Exchange and Active Directory for the CTS-Manager system.	Chapter 3, "Configuring Microsoft Exchange for Cisco TelePresence Manager"
Configure IBM Domino for CTS-Manager	This chapter describes the steps needed to configure IBM Domino and Domino server for the CTS-Manager system.	Chapter 4, "Configuring IBM Domino Server for Cisco TelePresence Manager"
Configure Scheduling API for CTS-Manager	This chapter describes the steps needed to configure the Scheduling API for the CTS-Manager system.	Chapter 5, "Configuring Scheduling API for Cisco TelePresence Manager"
Configuring Cisco Unified CM for CTS-Manager	Before installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-Manager system.	Chapter 6, "Configuring Cisco Unified Communications Manager for Cisco TelePresence Manager"
Install and Configure PreQualification Assistant	Install and configure the PreQualification Assistant to ensure that your pre-installation setup 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 7, "Installing and Configuring Cisco PreQualification Assistant"
Installing or Upgrading CTS-Manager software	Installing the CTS-Manager software. In addition, the installation requires information about your network and the rules for finding and exchanging information.	Chapter 9, "Installing or Upgrading Cisco TelePresence Manager"

Setup and Installation Procedures Guidelines	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 (endpoint) information, and Cisco Unified Communications Manager for conference room (endpoint) availability and telephone support	Chapter 10, "Initializing Cisco TelePresence Manager"
Additional Installation Procedures for CTS-Manager	The administrator makes use of the configuration windows to perform system configuration tasks such as uploading licenses, synchronizing system databases, managing security, and reconfigure system settings	Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager"
Configure WebEx OneTouch	This chapter describes the steps required to configure the WebEx OneTouch feature for CTS-Manager.	Chapter 12, "Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager"



CHAPTER 2

Pre-Install System Setup for Cisco TelePresence Manager

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

Contents

- Introduction, page 2-1
- System Components, page 2-1
- Pre-Installation Procedure Guidelines for Initial Network Setup, page 2-3

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 described in the next section.

System Components

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

- Cisco TelePresence System endpoints
- Cisco Unified Communications Manager
- LDAP server:
  - Active Directory
  - Domino Directory
- Calendar Server
  - Microsoft Exchange

  - IBM Domino
  - Other calendar server via Scheduling API
- Scheduling Client
  - Microsoft Outlook
  - IBM Lotus Notes
  - Other scheduling client via Scheduling API

For details on the software versions supported, refer to: Cisco TelePresence Manager Specifications and System Requirements, page 1-6

Installation Considerations

- When you install CTS-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 for easier management.
- To use HD Interop, all Cisco TelePresence System endpoints must be running software version 1.6 or later.

Pre-Installation Procedure Guidelines for Initial Network Setup

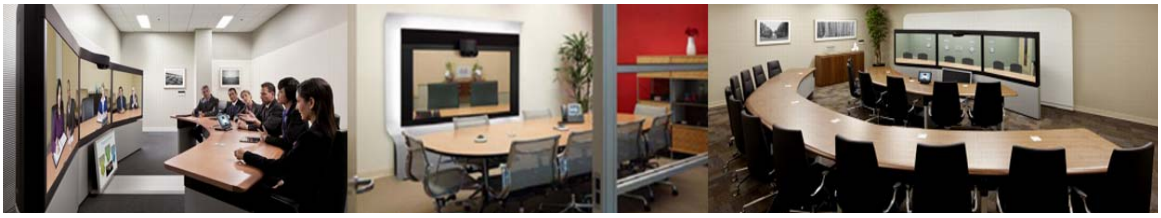
This table provides guidelines for the procedures you will need to reference in order to preconfigure the network **before** installing the Cisco TelePresence Manager.

Note The system will use either Microsoft or IBM, but not both. For Microsoft, see Configuring Microsoft Exchange for Cisco TelePresence Manager, page 3-1. For IBM, see Configuring IBM Domino Server for Cisco TelePresence Manager, page 4-1.

Table 2-1 Pre-Installation Guidelines for Setting up Initial System Network for CTS-Manager

Setup Procedure Guidelines before Installing CTS-Manager	Description	Location
Configure Microsoft Exchange	This chapter describes the steps needed to configure Microsoft Exchange and Active Directory for the CTS-Manager system.	Chapter 3, "Configuring Microsoft Exchange for Cisco TelePresence Manager"
Configure IBM Domino	This chapter describes the steps needed to configure IBM Domino and Domino server for the CTS-Manager system.	Chapter 4, "Configuring IBM Domino Server for Cisco TelePresence Manager"
Configure Scheduling API	This chapter describes the steps needed to configure the Scheduling API for the CTS-Manager system.	Chapter 5, "Configuring Scheduling API for Cisco TelePresence Manager"
Configuring Cisco Unified CM	Before installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-Manager system.	Chapter 6, "Configuring Cisco Unified Communications Manager for Cisco TelePresence Manager"
Install and run PreQualification Assistant	Install and run the PreQualification Assistant to ensure that your pre-installation setup 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 7, "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

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

Contents

- Introduction, page 3-1
- Pre-Configuration Setup Guidelines, page 3-2
- Configuring Microsoft Exchange for CTS-Manager, page 3-3
- Deploying with Microsoft Exchange 2003, page 3-3
- Deploying with Microsoft Exchange 2007 - WebDAV, page 3-4
- Deploying with Microsoft Exchange 2007 and 2010 EWS, page 3-9
- Exchange Migration Guide, page 3-12
  - Migrating from Exchange Server 2003 to 2007, page 3-12
  - Migrating from Exchange Server 2003 to 2010, page 3-15
  - Migrating from Exchange Server 2007 to 2010, page 3-15
- Applying CTS-Manager Throttling Policy for Exchange 2010 SP1, page 3-16
  - Throttling Policy Parameter Definitions and Values, page 3-17

Introduction

This chapter 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 describes the steps needed to configure Microsoft Exchange 2003, 2007 and 2010.

Note CTS-Manager supports the English language version of Microsoft Exchange only.

Table 3-1 Exchange Configuration Options

Exchange Version	Integration Method
2003	WebDav
2007	WebDav or EWS
2010	EWS

Note Microsoft Exchange with Entourage client is not supported.

It is recommended that Chapter 10, "Initializing Cisco TelePresence Manager" Manager, LDAP sections be reviewed to ensure that user set up is performed correctly.

Pre-Configuration Setup Guidelines

The purpose of this section is to reference the chapters you will next need in order to preconfigure 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 3-2 Microsoft Exchange Pre-Configuration Guidelines Before Installing CTS-Manager

Setup Procedures before Installing CTS-Manager	Description	Location
Configure Microsoft Exchange	This chapter describes the steps needed to configure Microsoft Exchange and Active Directory for the CTS-Manager system.	Current Chapter.
Next Steps After Microsoft Exchange Setup		
Configuring Cisco Unified CM.	Before installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-Manager system.	Chapter 6, "Configuring Cisco Unified Communications Manager for Cisco TelePresence Manager"
Install and Configure PreQualification Assistant	Install and run the PreQualification Assistant to ensure that your pre-installation setup 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 7, "Installing and Configuring Cisco PreQualification Assistant"

Configuring Microsoft Exchange for CTS-Manager

To configure 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

To deploy CTS-Manager 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 Log onto the **ctsmanaccount** account once to verify it is set up correctly.

Step 4 Create an account in Microsoft Exchange for each Cisco TelePresence System or video conferencing endpoint. You can use ‘Active Directory Users and Computers’ to create the room (endpoint) 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 support site 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 onto the room (endpoint) account once using Outlook Web Access (OWA), or Outlook. This must be done or the room mailbox will 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 the 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 on using the CTS-Manager account (e.g. ctsmanaccount)

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 sync 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.

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

After the meeting organizer cancels a meeting, the tentative or proxy room owner must log in to room (endpoint) mailbox, and remove the meeting from the calendar.

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". It is not available in version 2010. 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

To deploy CTS-Manager with Microsoft Exchange 2007 - WebDAV:

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 instructions to create the mailbox.

Step 2 Provide an adequate mailbox quota for the ctsmanaccount account. 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 onto the CTS-Manager mailbox once to verify the user mailbox is set up correctly.

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

Step 5 Create an account in Exchange for each Cisco TelePresence System or video conferencing 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 instructions to create the mailbox.

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

Step 6 The CTS-Manager account needs to have full access permissions to each room mailbox. Using EMS, run the following cmdlet:

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

Step 7 Set the DeleteSubject and AddOrganizerToSubject properties in the 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 Cisco recommends to not switch the room (endpoint) mailbox acceptance mode once it is set. If it is configured to auto-accept and then switched to manual proxy mode, the meeting will not appear in CTS-Manager nor will it be pushed to the phone UI. The user will have to manually accept the meeting again.

Step 9 Log onto the room mailbox once using Outlook Web Access (OWA) or Outlook 2007. This important step ensures the room mailbox is set up correctly in MS Exchange. In Exchange 2007, you won't be able to directly log onto the room* mailbox using the room username, because the user account of the room mailbox is disabled by default. There are two possible scenarios (based on the decision made in step 5):

Note *Only when mailbox is created as the 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 (endpoint) mailboxes. In this case, use the ctsmanaccount credentials 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 the ctsmanaccount user, click 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 onto the room (endpoint) account using either Outlook 2007 or Outlook Web Access:
  http://<exchange ip address>/owa/<endpoint_name@domain_name>. Again, here you will need to log on using the ctsmanaccount credentials.

b. The second scenario is where the ctsmanaccount was only given read permission to the room(endpoint) mailboxes. In this case, you must 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 these steps:

- i. Once logged on, click **Calendar** in the left pane.
- ii Click **Open a Shared Calendar** and enter the room (endpoint) name.
- iii The room calendar appears under **People's Calendar** in the left pane. Right-click the room name, and select **Properties**.
- iv. Click **Permissions** tab
- v. Click **Add** and select the ***ctsmanaccount*** account name.
- vi. In the **Permissions > Permission Level** drop-down field, select **Reviewer**.
- vii.In the **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. For Cisco TelePresence Manager to work, you must 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** in the warning message 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.

For Exchange 2007 installed on Windows 2003:

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

b. Select **WebDAV** and click the **Allow** button, if it is showing "Prohibited" for its status.

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

For Exchange 2007 installed on Windows 2008:

Refer to the following information from Microsoft on how to configure WebDAV for IIS7:

http://technet.microsoft.com/en-us/library/cc431377.aspx#Install_WebDAV

Note WebDAV is not available for IIS6.

Step 12 Verify that the Web Sites Authentication Method is configured correctly for Exchange website.

Note If using EWS Authentication with CTS-Manager 1.6.2 or earlier: Only Integrated Windows Authentication (NTLM) v1 authentication is supported. Please ensure that NTLMv1 authentication scheme is enabled for EWS site.

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 ***Exchange*** and select **Properties**.

c. Go to the **Directory Security** tab

d. In the 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 the 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 sync 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 renew 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 and 2010 EWS

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

- 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 the Recipient Policy Exchange server name, mailbox name, etc. These special characters are also not be supported by CTS-Manager.
Exchange 2007 Information:
http://technet.microsoft.com/en-us/library/dd285491.aspx

To deploy CTS-Manager with Microsoft Exchange 2007 and 2010 EWS:

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.

Caution If the CTS-Manager user logon name is different from the LHS of the email ID and there is no matching email ID for the user, Microsoft Exchange EWS will fail the mailbox quota test. To avoid this, add a secondary email ID that uses the CTS-Manager logon name as the LHS of the email ID appended with the SMTP domain.

Step 2 Provide an adequate mailbox quota for the ctsmanaccount. 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 onto the CTS-Manager mailbox once to verify the user mailbox is set up correctly.

Step 4 If a new endpoint needs to be added, the Admin needs to create the room in the calendaring server first with appropriate permissions for the CTS-Manager application account and then create associated device(s) in Unified CM. If the admin creates devices in Unified CM beforehand, then the endpoint would appear in error in CTS-Manager. Once the room is configured in the calendaring server, the admin can resync the endpoint in CTS-Manager to resolve the error.

Step 5 Create an account in Exchange for each Cisco TelePresence System or video conferencing 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 the Exchange Management Shell (EMS) cmdlet to create a room mailbox / account.

Step 6 The CTS-Manager account needs to have full access permissions to each room mailbox. Using EMS, run the following cmdlet:

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

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.

For Exchange 2007:

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

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

For Exchange 2010:

a. Set-CalendarProcessing -Identity “room5” -DeleteSubject $false

b. Set-CalendarProcessing -Identity “room5” -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.

For Exchange 2007:

Set-MailboxCalendarSettings -Identity TelepresenceRoom9 -AutomateProcessing AutoAccept

For Exchange 2010:

Set-CalendarProcessing -Identity “room1” -AutomateProcessing AutoAccept

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

Get-MailboxCalendarSettings -Identity TelepresenceRoom9 | fl

Note It is recommended not to switch room (endpoint) 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.

Step 9 Log onto the room (endpoint) 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 onto 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 onto each room (endpoint) 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 the **ctsmanaccount** tab at the top, enter the room account name, and click **Open**. The room (endpoint) mailbox opens in another window.
- Alternatively, you can log on to the room (endpoint) account using either Outlook 2007 or Outlook Web Access:
  http://<exchange ip address>/owa/<endpoint_name@domain_name>. Again, here you will need to log on using the ctsmanaccount credential.

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

- i. Once logged on, click **Calendar** in the left pane.
- ii Click **Open a Shared Calendar** and enter the room (endpoint) name.
- iii The room calendar would show up under **People's Calendar** on the left pane. Right-click the room(endpoint) name, and select **Properties**.
- iv. Click **Permissions** tab
- v. Click **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 endpoint 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 the ***EWS*** and select **Properties**.

c. Go to the **Directory Security** tab

d. In the 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 the 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 sync 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.

Step 13 If you installed Exchange 2010 SP1, you must apply the CTS-Manager Throttling Policy for Exchange 2010 SP1. For more information, see: Applying CTS-Manager Throttling Policy for Exchange 2010 SP1, page 3-16.

CTS-Manager and Microsoft EWS server automatically renew 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 forced to sync with the EWS server by either doing a reboot or a restart.

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

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

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

Exchange Migration Guide

CTS-Manager integrates with Exchange Server 2003, Exchange Server 2007 and Exchange Server 2010. This section highlights the steps required in CTS-Manager when an existing Exchange Server is upgraded. Please refer to official Microsoft documentation on how to:

- Migrate Exchange Server from a previous release to a newer version
- Set up Client Access Server (CAS) against previous version mailbox server

Migrating from Exchange Server 2003 to 2007

CTS-Manager accesses Exchange Server 2003 via the WebDAV protocol. This protocol is supported by Exchange Server 2007. In addition, Microsoft has introduced a new access method via Exchange Web Service (HTTP/SOAP) protocol.

Microsoft does not support in-place upgrade from Exchange Server 2003 to 2007. A separate Exchange Server 2007 must be installed and data can be migrated over time. Depending on the size of your installation, this process can take from hours to months. For more information, refer to the following documentation from Microsoft:
http://technet.microsoft.com/en-us/library/bb124008%28EXCHG.80%29.aspx

There are 2 possible migration paths for CTS-Manager:

- Continue Using WebDAV Protocol, page 3-13
- Use EWS Access, page 3-13

Continue Using WebDAV Protocol

If the CTS-Manager version is earlier than 1.6, this is the only upgrade path available.

To migrate to Exchange 2007 and continue using WebDAV:

Step 1 Set up Exchange Server 2007.

Step 2 Identify the CAS server to which CTS-Manager will integrate.

Step 3 Shut down CTS-Manager.

Step 4 Migrate CTS-Manager account mailbox to 2007 mailbox server at the minimum.

Note Cisco recommends migrating all TelePresence room (endpoint) mailboxes.

Step 5 Start up CTS-Manager.

Step 6 Log in to CTS-Manager.

Step 7 Go to **Configure > Microsoft Exchange**.

The connection to Exchange may be down. This is expected.

Step 8 Enter the connection parameters identified in step 2, click **Test Connection** and make sure that the test is successful.

Step 9 Click the **Apply** button and wait for CTS-Manager to sync up the data from all of the TelePresence mailboxes. This could take from few minutes to a few hours depending on the size of your deployment.

Note Please note that for step 4, if the downtime of CTS-Manager exceeds your company policy about permissible downtime, only the CTS-Manager account mailbox needs to be migrated. The TelePresence room (endpoint) mailboxes can still reside in Exchange 2003 Mailbox server. Ensure that those mailboxes are accessible from the CAS server identified in step 2. Please consult Microsoft documentation on how to set up a CAS server against a previous version's mailbox

Use EWS Access

This upgrade path is only available for CTS-Manager release 1.6 or later.

Upgrading CTS-Manager to the new EWS mode is recommended for the following reasons:

- Microsoft discontinued official support for the WebDAV protocol. An extension to the support agreement is required.
- EWS is a more secure implementation. CTS-Manager in EWS mode supports basic and integrated Windows authentication (NTLMv1 in CTS-Manager 1.6.2 or earlier, NTLM v1 and v2 in CTS-Manager 1.6.3 or later and NTLMv2 session in CTS-Manager 1.7.2 or later).
- EWS is more scalable.
- EWS ensures an easier future upgrade. In Exchange 2010, the WebDAV access to Exchange server has been disabled.

To migrate to Exchange 2007 and continue using EWS:

Step 1 Set up Exchange Server 2007.

Step 2 Identify the CAS server to which CTS-Manager will integrate.

Step 3 Shut down CTS-Manager.

Step 4 Migrate the CTS-Manager account mailbox to the 2007 mailbox server. Cisco recommends to also migrate all TelePresence room (endpoint) mailboxes.

Step 5 Start CTS-Manager.

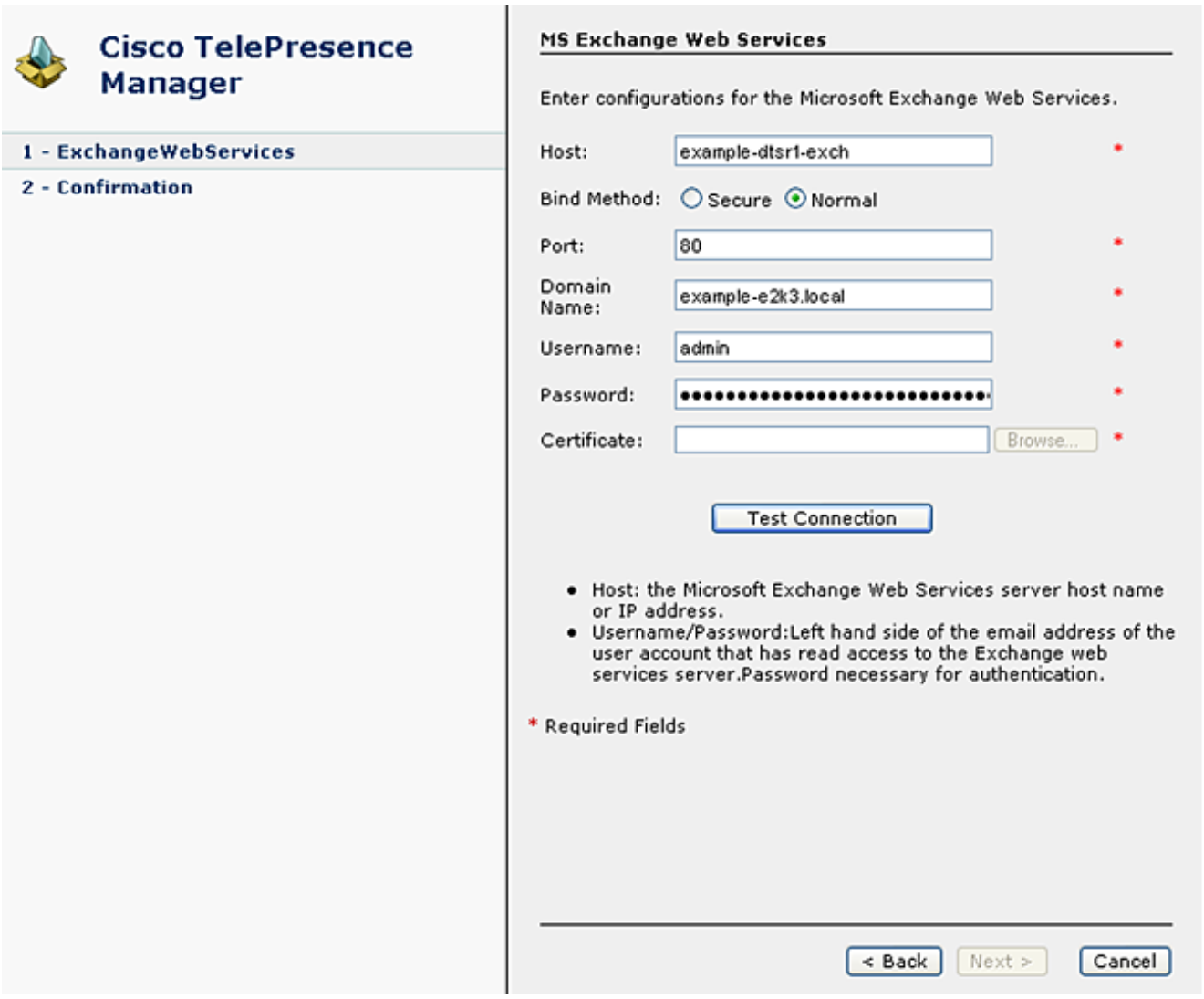
Step 6 Log in to CTS-Manager

Step 7 Go to the **Configure > Microsoft Exchange** window.

The connection to Exchange may be down. This is expected.

Step 8 Click **Configure EWS**. The MS Exchange Web Services window appears. See Figure 3-1 on page 3-14.

Figure 3-1 Configure EWS Window



Step 9 In the MS Exchange Web Services window, enter the connection parameters identified in step 2, click **Test Connection** and make sure that the test is a success.

Step 10 Click the **Apply** button and wait for CTS-Manager to sync up the data from all of the TelePresence mailboxes. This could take from a few minutes to a few hours depending on the size of your deployment.

Migrating from Exchange Server 2003 to 2010

Exchange Server 2010 discontinued WebDAV access; therefore CTS-Manager must be configured in EWS mode before the upgrade process.

Use the following procedure to migrate from Exchange 2003 to Exchange 2010:

Step 1 Install and configure the Exchange 2010 server.

Step 2 In CTS-Manager, go to **Configure > Microsoft Exchange**.

Step 3 Click the **Configure EWS** button in the right pane, enter and apply the Exchange 2010 CAS server configuration information.

Step 4 If running in secure mode, add the 2010 CAS server certificate.

Step 5 Click **Test Connection** and then click **Apply**.

CTS-Manager will sync all rooms.

Step 6 Shut down the CTS-Manager server.

This is important so that users do not use CTS-Manager during migration.

Step 7 Migrate all Cisco TelePresence endpoints to the Exchange 2010 server.

Verify that all Cisco TelePresence endpoints are of the type “RoomMailbox.”

This is required for Auto-Accept to be enabled.

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

Step 8 If you installed Exchange 2010 SP1, you must apply the CTS-Manager Throttling Policy for Exchange 2010 SP1. For more information, see: Applying CTS-Manager Throttling Policy for Exchange 2010 SP1, page 3-16.

Migrating from Exchange Server 2007 to 2010

Support for Exchange 2010 is introduced in release 1.7. This upgrade path is only available for CTS-Manager release 1.7 or later.

The migration path depends on how CTS-Manager is configured to access Exchange Server 2007.

- WebDAV mode
- EWS mode

Use the following procedure to migrate from Exchange 2007 to Exchange 2010:

Step 1 Install and configure the Exchange 2010 server.

Step 2 If CTS-Manager is running in 2007 WebDAV mode, configure EWS (see Deploying with Microsoft Exchange 2007 and 2010 EWS, page 3-9.) and move to 2007 EWS. If CTS-Manager is already running in EWS mode, go to step 3.

Step 3 Shut down CTS-Manager.

Step 4 Migrate the CTS-Manager account mailbox to the 2010 mailbox server.

Step 5 Set the Throttling policy for 2010 (see Applying CTS-Manager Throttling Policy for Exchange 2010 SP1, page 3-16).

Step 6 Move the Exchange 2007 rooms to Exchange 2010.

Note Cisco recommends migrating all TelePresence room mailboxes.

Step 7 Make sure the CTS-Manager account has full permission to the 2010 room mailboxes.

Step 8 Identify the 2010 CAS server to which CTS-Manager will integrate.

Step 9 Start up CTS-Manager.

Step 10 Log in to CTS-Manager.

Step 11 Go to **Configure > Microsoft Exchange** and click the **Configuration** tab.

Step 12 Change the Exchange server to 2010 CAS server.

Step 13 If running in secure mode, add the 2010 CAS server certificate.

Step 14 Click **Test Connection** and then click **Apply**.

Step 15 CTS-Manager will sync all rooms.

Applying CTS-Manager Throttling Policy for Exchange 2010 SP1

With Exchange 2010 SP1 update, Microsoft has enabled the client throttling policy feature by default. For more information, refer to: http://technet.microsoft.com/en-us/library/dd297964.aspx

If there's no throttling policy already configured, Microsoft will apply a default policy to all users. The default throttling policy is tailored for end-user load and not for an enterprise application like CTS-Manager.

In order for all CTS-Manager features to work, a custom throttling policy must be applied to the CTS-Manager application user.

Note This throttling policy is required for Exchange 2010 SP1.

To apply the CTS-Manager Throttling Policy for Exchange 2010 SP1:

Step 1 Log in to the CAS server for Exchange 2010.

Step 2 Open Exchange Management Shell application.

Step 3 Create a custom throttling policy:

a. **Run > New-ThrottlingPolicy Cisco_CTSManager_ThrottlingPolicy**

b. **Run > Set-ThrottlingPolicy -Identity Cisco_CTSManager_ThrottlingPolicy -EWSFastSearchTimeoutInSeconds 300 -EWSFindCountLimit 6000 -EWSMaxConcurrency $null -EWSMaxSubscriptions 5000 -EWSPercentTimeInAD 200 -EWSPercentTimeInMailboxRPC 300 -EWSPercentTimeInCAS 500**

Step 4 Assign the policy to CTS-Manager application user

a. **Run > $b = Get-ThrottlingPolicy Cisco_CTSManager_ThrottlingPolicy**

b. **Run > Set-Mailbox -Identity <superuser account> -ThrottlingPolicy $b**

Note If you encounter any errors after applying the CTS-Manager throttling policy, you can revert back to the Microsoft throttling policy. For more information, refer to: Restoring the Microsoft Throttling Policy for Exchange 2010 SP1, page 3-21.

Throttling Policy Parameter Definitions and Values

The default values used in the above steps satisfy most CTS-Manager deployments. If your deployment requires adjustments, you can adjust the **Set-ThrottlingPolicy** values and rerun step 3b above.

Caution Please contact the Cisco TelePresence support team before adjusting any of the default values.

The following tables describe the policy parameters and values for the **Set-Throttling Policy** command of Exchange 2010 SP1 for the following deployments:

- Throttling Policy Parameters for 300 or Fewer Rooms

- Throttling Policy Parameters for More than 300 Rooms.

Table 3-3 Throttling Policy Parameters for 300 or Fewer Rooms

Name	Description	CTS-Manager Default Policy Value	Note
EWSFastSearchTimeoutInSeconds	The length, in seconds, of an Exchange Web Services search before it times out. If the length of the search exceeds the specified value, the search ends, and the system returns an error.	300	Each CTS-Manager call has a default time out of 180 second. 300 is granted since each call could be phased out.
EWSFindCountLimit	The maximum number of FindItem or FindFolder requests that the CAS memory can store for the CTS-Manager application user. If the maximum number exceeds the specified value, the system returns an error. Requests made for an indexed page view are an exception. In this case, search results include only the number of items allowed by the policy limit. Results that are not currently viewable by the user can be accessed using FindItem or FindFolder requests.	6000	This parameter governs the maximum number of entries for all requests combined at a given time. CTS-Manager only requests for 200 entries to be returned
EWSMaxConcurrency	The maximum number of connections between an Exchange Web Services user and an Exchange server. (A connection begins when a connection request is received and ends after the entire response is sent.) If the maximum number of connections between the two entities is reached, the existing connections are unaffected, but any subsequent connection requests from the user are denied. The valid range is 0 through 2147483647 inclusive.	500	Due to the nature of EWS notification, you can't measure the number of concurrent requests. $null value is required to indicate that no throttling is necessary for this criteria.

Table 3-3 Throttling Policy Parameters for 300 or Fewer Rooms (continued)

Name	Description	CTS-Manager Default Policy Value	Note
EWSPercentTimeInAD	The portion of each minute, expressed as a percentage, that an Exchange Web Services user can dedicate to handling LDAP requests. For example, if you specify 100, the Exchange Web Services user can spend 100 percent of each minute on LDAP requests.	200	The value is higher than 100 since this counts for all concurrent requests at any given time.
EWSPercentTimeInMailboxRPC	The portion of each minute, expressed as a percentage, that an Exchange Web Services user can dedicate to handling mailbox remote procedure call (RPC) requests.	300	The value is higher than 100 since it counts for all concurrent requests at any given time.
EWSPercentTimeInCAS	The portion of each minute, expressed as a percentage, that an Exchange Web Services user can dedicate to handling CAS code.	500	The value is higher than 100 since this counts for all concurrent requests at any given time.
EWSMaxSubscriptions	The maximum number of active push and pull subscriptions that the CAS can store for a particular user. If the maximum number of subscriptions is reached, any subsequent subscription requests will fail and an event will be recorded in the Event Viewer log.	5000	This number should be set to (2 * the number of managed endpoints). Please allocate a number that allows for future growth.

Table 3-4 Throttling Policy Parameters for More than 300 Rooms

Name	Description	CTS-Manager Default Policy Value	Note
EWSFastSearchTimeoutInSeconds	The length, in seconds, of an Exchange Web Services search before it times out. If the length of the search exceeds the specified value, the search ends, and the system returns an error.	$null	Each CTS-Manager call has a default time out of 180 second. 300 is granted since each call could be phased out.
EWSFindCountLimit	The maximum number of FindItem or FindFolder requests that the CAS memory can store for the CTS-Manager application user. If the maximum number exceeds the specified value, the system returns an error. Requests made for an indexed page view are an exception. In this case, search results include only the number of items allowed by the policy limit. Results that are not currently viewable by the user can be accessed using FindItem or FindFolder requests.	$null	This parameter governs the maximum number of entries for all requests combined at a given time. CTS-Manager only requests for 200 entries to be returned
EWSMaxConcurrency	The maximum number of connections between an Exchange Web Services user and an Exchange server. (A connection begins when a connection request is received and ends after the entire response is sent.) If the maximum number of connections between the two entities is reached, the existing connections are unaffected, but any subsequent connection requests from the user are denied. The valid range is 0 through 2147483647 inclusive.	$null	Due to the nature of EWS notification, you can't measure the number of concurrent requests. $null value is required to indicate that no throttling is necessary for this criteria.

Table 3-4 Throttling Policy Parameters for More than 300 Rooms (continued)

Name	Description	CTS-Manager Default Policy Value	Note
EWSPercentTimeInAD	The portion of each minute, expressed as a percentage, that an Exchange Web Services user can dedicate to handling LDAP requests. For example, if you specify 100, the Exchange Web Services user can spend 100 percent of each minute on LDAP requests.	$null	The value is higher than 100 since this counts for all concurrent requests at any given time.
EWSPercentTimeInMailboxRPC	The portion of each minute, expressed as a percentage, that an Exchange Web Services user can dedicate to handling mailbox remote procedure call (RPC) requests.	$null	The value is higher than 100 since it counts for all concurrent requests at any given time.
EWSPercentTimeInCAS	The portion of each minute, expressed as a percentage, that an Exchange Web Services user can dedicate to handling CAS code.	$null	The value is higher than 100 since this counts for all concurrent requests at any given time.
EWSMaxSubscriptions	The maximum number of active push and pull subscriptions that the CAS can store for a particular user. If the maximum number of subscriptions is reached, any subsequent subscription requests will fail and an event will be recorded in the Event Viewer log.	$null	This number should be set to (2 * the number of managed endpoints). Please allocate a number that allows for future growth.

Restoring the Microsoft Throttling Policy for Exchange 2010 SP1

If for any reason, you encounter errors applying the CTS-Manager throttling policy for Exchange 2010 SP1, you can revert back to the default Microsoft throttling policy.

To restore the Microsoft throttling policy for Exchange 2010 SP1:

Step 1 Log in to the CAS server for Exchange 2010.

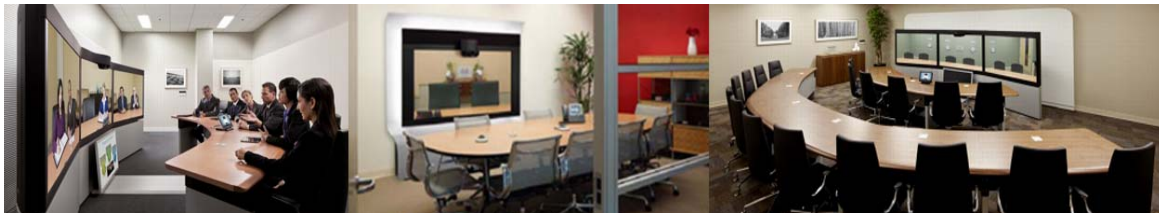
Step 2 Open Exchange Management Shell application.

Step 3 Remove Throttling policy association from CTS-Manager application user:

- **Run > Set-Mailbox -Identity <*superuser account*> -ThrottlingPolicy $null**

Step 4 Remove the custom policy:

- **Run > Remove-ThrottlingPolicy Cisco_CTSManager_ThrottlingPolicy**



CHAPTER 4

Configuring IBM Domino Server for Cisco TelePresence Manager

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

Contents

- Introduction, page 4-1
- Important Considerations, page 4-1
- Pre-Configuration Procedure Guidelines for IBM Domino Setup, page 4-2
- Configuring IBM Domino for CTS-Manager, page 4-2
- Directory Assistance in a Domino Deployment, page 4-4

Introduction

This chapter describes 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 should already be installed and configured.
- IBM Domino

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

Pre-Configuration Procedure Guidelines for IBM Domino Setup

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

Table 4-1 IBM Domino Pre-Configuration Guidelines Before Installing CTS-Manager

Setup Guidelines before Installing CTS-Manager	Description	Location
Configuring IBM Domino	This chapter describes 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 6, "Configuring Cisco Unified Communications Manager for Cisco TelePresence Manager"
Install and Configure PreQualification Assistant Tool	Install and configure the PreQualification Assistant to ensure that your pre-installation setup 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 7, "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 16, "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. CTS-Manager account). CTS-Manager LDAP user and SysAdmin need read permission to the Domino Directory.

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 endpoints. Additional mailbox quota allocated to this user is recommended if feasible.

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

The CTS-Manager account needs to have read permission for each resource reservation database which contains any Cisco TelePresence room (endpoint). 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 or video conferencing endpoint. The steps might involve creating a new resource reservation database, creating a new site profile document and adding Cisco TelePresence rooms for Domino.

Note The Resource Reservation database **must** be initially created using the Resource Reservation Template 7 or later. Reservation templates prior to version 7 cannot be upgraded.

Step 5 CTS-Manager displays 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 Configure > 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

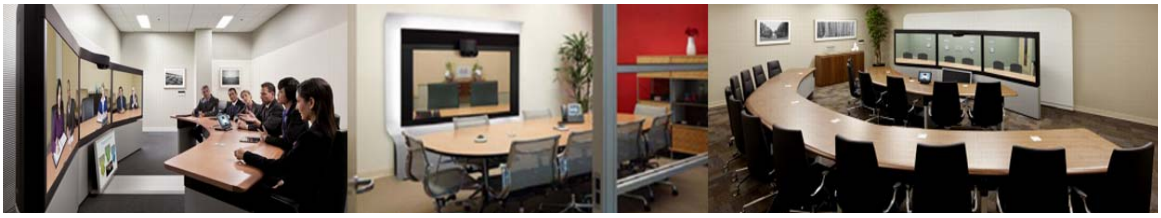
Directory Assistance in a Domino Deployment

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 Live Desk, 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, log into 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 Scheduling API for Cisco TelePresence Manager

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

Contents

- Introduction, page 5-1
- Important Considerations, page 5-3
- Pre-Configuration Procedure Guidelines for Scheduling API Setup, page 5-3
- Configuring Scheduling API for CTS-Manager, page 5-4

Introduction

This chapter describes the steps needed to configure the Scheduling API for Cisco TelePresence Manager.

Overview

The CTS-Manager Scheduling API (Scheduling API) interfaces Cisco TelePresence services to third-party Enterprise Calendaring Applications (ECA).

Currently, CTS-Manager supports Microsoft Exchange and IBM Domino calendaring. If you use any other calendar server, or if no calendar server is available, you must use the Scheduling API.

You can perform the following functions with the Scheduling API:

- Retrieve calendar data for CTS End points from the ECA.
- ECA uses **getTLiteMeetings** API call to sync meeting by comparing the lastModified attribute for each meeting to determine any meetings that have been modified.
- Schedule a TelePresence meeting providing a One-Button-To-Push number to start meetings on CTS endpoints.
- Cancel a TelePresence meeting
- Retrieve CTS endpoints room (endpoint) names

- Receive notifications from CTS-Manager based on certain events, such as meeting attribute change or CTS endpoints addition and deletion

CTS-Manager is not a calendaring solution. You use the ECA as the calendar application. You use the ECA to reserve Cisco TelePresence endpoints (Cisco TelePresence rooms) the same as you invite users or resources in the ECA. The Scheduling API then provides for the ECA to provide CTS-Manager information about the new meeting, including the Cisco TelePresence endpoint(s), in iCalendar (iCal) format.

Once CTS-Manager receives the meeting invitation, it performs the following tasks:

- It schedules the Cisco TelePresence Multipoint Switch (CTMS), Cisco TelePresence Recording Server (CTRS), WebEx, Cisco Unified Videoconferencing Manager (CUVC), and any other resources that are required for the meeting, based on the number of Cisco TelePresence end points that are invited and other options that are allowed or selected by the meeting organizer.
- It notifies the Cisco TelePresence endpoints of the schedule of meetings for that endpoint and provides the OBTP number that is used to start the meeting. These details are displayed on the Cisco Unified IP Phone immediately before the meeting starts.

For details on how to use the Scheduling API and which features of CTS-Manager are supported, refer to the Cisco TelePresence Manager Scheduling API Developer's Guide, available at:

http://developer.cisco.com/web/telesched/documentation.

Requirements

The following sections describe the software and licensing requirements for the Scheduling API and includes the following topics:

- CTS-Manager Requirements, page 5-2
- Licensing Requirements, page 5-3
- LDAP Requirements, page 5-3

CTS-Manager Requirements

To use the Scheduling API, you must deploy CTS-Manager in Scheduling API mode. This mode is available with CTS-Manager release 1.7 and later.

If your CTS-Manager release 1.7 is deployed in No Calendar mode, you can upgrade to Scheduling API mode by first migrating to CTS-Manager release 1.9 in No Calendar mode, then configuring your migrated CTS-Manager to be in Scheduling API mode. You make these changes using the CTS-Manager administrative GUI.

In all other cases, a fresh installation of release 1.9 is required for Scheduling API mode.

Note If you deploy CTS-Manager in Exchange or Domino calendaring mode, you cannot switch to Scheduling API mode and must reinstall the CTS-Manager application.

After you configure CTS-Manager in Scheduling API mode, you cannot configure any other mode (for example, calendar server mode).

If you perform a new installation, you lose all existing data when you migrate to the new release.

Licensing Requirements

After installing CTS-Manager, you must install the license for the Scheduling API. For detailed information about the license and how to install it, refer to Licensing for CTS-Manager, page 11-6.

LDAP Requirements

You must provide the Lightweight Directory Access Protocol (LDAP) server information during first-time setup of CTS-Manager. All Cisco TelePresence rooms (endpoints) and schedulers should be part of this LDAP server. The API will retrieve the scheduler display name and room display name from this LDAP server.

The LDAP administrator should create a new user account in the LDAP server. This account represents the ECA. When the ECA invokes the API, it uses this account to authenticate itself to CTS-Manager. During the first-time setup of CTS-Manager, you should use this account on the ECA configuration page. For more information, refer to Initializing Cisco TelePresence Manager, page 10-1.

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 include one or more of the following:

- Cisco Unified Communications Manager should already be installed and configured.

Note For a complete list of system requirements, refer to: Cisco TelePresence Manager Specifications and System Requirements, page 1-6

Pre-Configuration Procedure Guidelines for Scheduling API Setup

The purpose of this guide is to outline the chapters you will need to reference in order to preconfigure the Scheduling API before installing the CTS-Manager.

Table 5-1 Pre-Configuration Guidelines for Scheduling API Before Installing CTS-Manager

Setup Guidelines before Installing CTS-Manager	Description	Location
Configuring Scheduling API.	This chapter describes the steps needed to configure a scheduling API for the CTS-Manager system.	Current Chapter
Next Steps After Scheduling API configuration		

Table 5-1 Pre-Configuration Guidelines for Scheduling API Before Installing CTS-Manager (continued)

Setup Guidelines before Installing CTS-Manager	Description	Location
Configuring Cisco Unified CM.	Before installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-Manager system.	Chapter 6, "Configuring Cisco Unified Communications Manager for Cisco TelePresence Manager"
Install and Configure PreQualification Assistant Tool	Install and configure the PreQualification Assistant to ensure that your pre-installation setup 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 7, "Installing and Configuring Cisco PreQualification Assistant"

The procedures in the next section must be completed to configure the Scheduling API in Cisco TelePresence Manager.

If at any time you encounter problems, go to Chapter 16, "Troubleshooting Cisco TelePresence Manager" to see how to correct the problem.

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

Configuring Scheduling API for CTS-Manager

To configure the Scheduling API:

Step 1 Create a user account for the ECA in the LDAP server that will be configured in CTS-Manager.

Step 2 Designate one computer to be an ECA host. This machine will host the ECA.

Step 3 (Optional) Install and run the PreQualification tool. For complete details, see Installing and Configuring Cisco PreQualification Assistant, page 7-1.

Step 4 Install CTS-Manager. For complete details, see Installing or Upgrading Cisco TelePresence Manager, page 9-1.

Step 5 Initialize CTS-Manager in Scheduling API mode. During initialization, in the LDAP Servers page, use the ECA account details created for LDAP in Step 1 and in the Calendar Server configuration page, specify the ECA host that you configured in Step 2. For complete details, see Initializing Cisco TelePresence Manager, page 10-1.

Tip You can also initialize CTS-Manager in No Calendaring Service mode and configure the Scheduling API after initialization in the Configure > Scheduling API window.

Step 6 Install Apache Tomcat on the ECA host.

Step 7 Download the CTS-Manager certificate and import it into the keystore.

Step 8 Implement ECA using Scheduling API calls and deploy it as web app.

For more information, refer to the Cisco TelePresence Manager Scheduling API Developer's Guide, available at: http://developer.cisco.com.

Step 9 After you start the ECA, use the *getStatus* API to make sure that CTS-Manager is up and running, and to verify the user authentication between the ECA and CTS-Manager.

Step 10 If the API indicates that the CTS-Manager is running, continue to the next step.

Note You must invoke the *getStatus* API every few minutes to check CTS-Manager status. In case of an error, the ECA may choose to "bubble it up" (pass the error from the bottom of the calling hierarchy) and notify the administrator.

Step 11 Subscribe the ECA to CTS-Manager notifications.

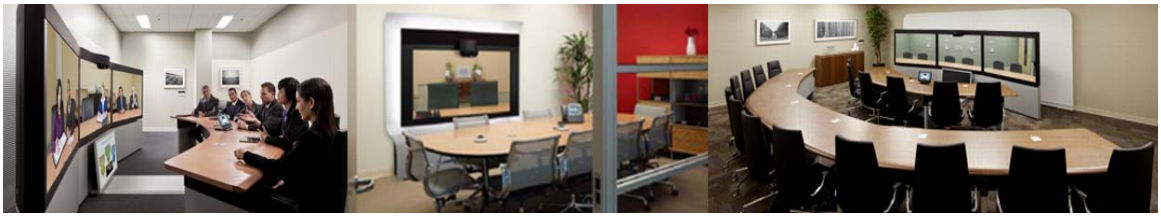
For more information, refer to the "Configuring the ECA to Receive Notifications" section in the Cisco TelePresence Manager Scheduling API Developer's Guide.

Step 12 Use the *getTRooms* API to retrieve TelePresence endpoints that are managed by CTS-Manager.

The ECA must use only these endpoints in iCal data when scheduling meetings. ECA can choose to cache these endpoints and validate iCal requests before submitting the requests to CTS-Manager.

Step 13 Invoke the remaining ECA APIs.

Whenever there is a request for scheduling a meeting, the ECA should generate iCal data conforming to RFC2445 and 2446 format for the meeting and then invoke the *scheduleTMeetings* API. When the iCal data is well formed and there are no errors, the TelePresence meeting is scheduled.



CHAPTER 6

Configuring Cisco Unified Communications Manager for Cisco TelePresence Manager

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

Contents

- Introduction, page 6-1
- Important Considerations, page 6-1
- Pre-Configuration Procedure Guidelines for Cisco Unified CM Setup, page 6-2
- Configuring Cisco Unified CM for CTS-Manager, page 6-3
- For Deployments Using Microsoft Exchange or IBM Domino or Scheduling API, page 6-3
- Logging into Cisco Unified CM Administrator, page 6-6
- Configuring the Options File, page 6-6
- Adding a Cisco TelePresence Device, page 6-7
- Creating and Configuring a Cisco TelePresence Device, page 6-8

Introduction

This section describes adding parameters to Cisco Unified Communications Manager (Cisco Unified CM) and researching information from the current installation of Cisco 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 describes the following applications:

- Cisco Unified CM should already be installed and configured. For more information refer to section *Logging into Cisco Unified CM Administrator, page 6-6* 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 easier to manage.

Pre-Configuration Procedure Guidelines for Cisco Unified CM Setup

This table provides a guideline for the procedures you will need to reference in order to preconfigure 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 preconfiguration.

Table 6-1 Pre-Configuration Guidelines for Setting Up Unified CM for CTS-Manager

Setup Procedure Guidelines before Installing CTS-MAN	Description	Location
Configuring Cisco Unified CM	Before CTS-Manager installation, you must verify that Cisco Unified Communications Manager is configured for the CTS-Manager system.	Current Chapter
Install and Configuring PreQualification Assistant	Install and run the PreQualification Assistant to ensure that your pre-installation setup 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 7, “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 16, "Troubleshooting Cisco TelePresence Manager"to see how to correct the problem.

For Deployments Using Microsoft Exchange or IBM Domino or Scheduling API

- 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.

- Unified CM Certificate
  - To get a Cisco Unified Communications Manager certificate do the following:
  1. Log into the Cisco Unified CM Administration application
  2. From the Navigation menu, select **Cisco Unified OS Administration** and click **Go**.
  3. From the Security menu click **Certificate Management**.
  4. Click the link for **tomcat.der**.
  5. In the Certificate Configuration window, click the **Download** button.
  - This saves a copy of the certificate on your computer. Make sure this file is accessible to the computer that has browser access to the Cisco TelePresence Manager server.

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

Step 1 Create an application user for CTS-Manager. Refer to section Logging into Cisco Unified CM Administrator, page 6-6 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.

Warning **Application user names must contain only ASCII characters to work correctly with CTS-Manager.**

Note Make sure that the application user you've created has all the endpoints assigned to it that you plan to use.

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 in the Cisco Unified CM Admin UI, by going to Device > Phone.

Note It is not required to add an IP phone associated with the CTS to the application user.

Note To secure CTS-Manager, add the "Standard CTI Secure Connection" group to the application user.

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

a. Go to Device > Phone and click the device name corresponding to the TelePresence endpoint device.

b. At the bottom of the Device Information section, check the **Allow Control of Device from CTI** checkbox.

c. In the Product Specific Configuration Layout section, enter the endpoint email address in the **Room Name** field.

Caution You cannot assign the same email address to more than one endpoint. If you do, you must fix the problem in Unified CM and then do a resync in the Microsoft Exchange or IBM Domino window in CTS-Manager.

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

e. In the Directory Number Information section of Directory Number Configuration, check the **Allow Control of Device from CTI** checkbox.

Step 3 For each IP phone device that is associated to TelePresence endpoint device, check the **Allow Control of Device from CTI** checkbox 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 the Cisco TelePresence Manager first time setup.

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

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

a. Assign the following roles to this user group:

- Standard AXL API access
- Standard CTI enabled
- Standard serviceability
- Standard CCM Admin Users
- Standard RealtimeandTracesCollection

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 the Cisco Unified CM Publisher node. Cisco CTIManager should be activated and running, but can 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 an endpoint'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 endpoint is added to Unified CM, restarting 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 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 Unified CM, do not set up a non-DNS and DNS in a mixed mode environment, i.e., where Unified CM is configured with DNS and CTS-Manager is configured with non-DNS environment. Unified CM 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 Unified CM node as publisher does not support mixed mode.

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

The **Configure > Unified CM** window opens. This window provides Service Status and the listings of the Unified CM connections.

Note If changing settings in the Unified CM, it is necessary to perform a Discovery in CTS-Manager to register the new settings. Otherwise, CTS-Manager won't display or connect to the correct settings.

Logging into 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 is compatible with 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 Cisco TelePresence device.

To configure the options file, follow these steps:

Step 1 Log into the Cisco Unified CM Administration application. See the "Logging into Cisco Unified CM Administrator" section on page 6-6.

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 6-7.

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 6-8.

Step 4 Assign a directory number to the Cisco TelePresence device. See the "Assigning a Directory Number to a TelePresence Device" section on page 6-13.

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

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

- Download Device Pack, page 6-7
- Install Device Pack, page 6-8

Download Device Pack

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 location on Cisco.com:

a. **Support**

The Support and Downloads page appears.

b. Under the Product Support tab, click **Voice & Unified Communications**

The Voice and Unified Communications window appears.

c. At the top of the Voice and Unified Communications window, click **Browse All Voice and Unified Communications Categories**

The Select Your Product or Technology page appears.

d. In the far-right column, click **IP Telephony**

e. Click **Call Control**

f. Scroll down (if necessary) and click **Cisco Unified Communications Manager (CallManager)**

The Introduction page appears.

Step 2 Click **Download Software.**

Step 3 (If needed) Enter your Cisco username and password and click **Log In**.

The Select a Product page appears.

Step 4 In the Cisco Unified Communications Manager (CallManager) section, click the version that corresponds to the Unified CM version you have configured in CTS-Manager.

Step 5 Click **Unified Communications Manager/CallManager Device Packages**.

Step 6 Click the latest release.

Note To register EX, MX and C-series endpoints, Unified CM 8.6.1.20000-1 and device pack 8.6.1.21019-1 are required.

The software download page for that release opens.

Step 7 Click **Download Now** to begin the download process.

Install Device Pack

To install a device pack, follow these steps:

Step 1 Log into 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.

Step 7 After installation is complete, restart.

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 (endpoint) so you can register it as a Cisco Unified IP phone:

- Adding a Cisco TelePresence Device, page 6-8
- Configuring a Cisco TelePresence Device, page 6-9
- Assigning a Directory Number to a TelePresence Device, page 6-13
- Verifying a TelePresence Device is Registered to Unified CM, page 6-13
- Adding a TelePresence Device to the Application User, page 6-14

Adding a Cisco TelePresence Device

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

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

Step 1 Log into 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 the **Cisco TelePresence** device you want to add.

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

Step 6 Proceed to Configuring a Cisco TelePresence Device.

Configuring a Cisco TelePresence Device

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 their 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.

Device Information for Cisco TelePresence Devices

Step 1 To configure a Cisco TelePresence device, enter the information appropriate for the device you are configuring using the information in the following sections:

- Cisco TelePresence System (CTS) Devices, page 6-9
- EX and C-series Devices, page 6-11

Cisco TelePresence System (CTS) Devices

Table 6-2 Cisco TelePresence System 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.

Table 6-2 Cisco TelePresence System Device Information (continued)

Field	Required?	Setting
Use Trusted Relay Point	—	Chose from the following: • Default • On • Off
Calling Party Transformation CSS	—	Leave field as <None>.

EX and C-series Devices

To register EX, MX and C-series devices, TC version 5 or later and Unified CM version 8.6.1.20000-1 or later are required. Endpoints with a previous TC firmware version must be upgraded to version 5 before they can be registered with Unified CM and be discovered by CTS-Manager.

The TC5.0.0 firmware for the endpoints is available in both .pkg and .cop formats.

- For TC4.x to TC5.0 upgrades, use the .pkg format. The .pkg file is uploaded directly onto each endpoint. Because it is a prerequisite that the endpoint run TC5.0 to be able to register with Unified CM, you must use the .pkg file to upgrade them first, and then provision them in Unified CM.

  For more information, go to the following link:
  http://www.cisco.com/cisco/software/release.html?mdfid=283645026&softwareid=280886992&release=TC5.0.0&rellifecycle=&relind=AVAILABLE&reltype=all

- For TC5.0.0 to TC5.0.x or later upgrades, use the .cop file format. The .cop file is installed on Unified CM, which extracts the .pkg file into the TFTP directory on the Unified CM and sets the Device Defaults to point to it so that all TC endpoints registered to Unified CM will be upgraded to that .pkg version.

  For more information, go to the following link:
  http://www.cisco.com/cisco/software/release.html?mdfid=283645026&softwareid=280886992&release=TC5.0.0-CUCM&rellifecycle=&relind=AVAILABLE&reltype=all

Table 6-3 Cisco TelePresence EX and C-series Device Information

Field	Required?	Setting
MAC Address	Yes	MAC address for the Cisco TelePresence EX or C-series primary codec.
Description	—	Short description of the device.
Device Pool	Yes	Default
Common Device Configuration	—	Leave field as< None>.
Phone Button Template	Yes	Standard_Cisco_TelePresence <endpoint model name>
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 (EX and C-Series Devices Only) In the Protocol Specific Information section:

- Set Device Security Profile to Standard SIP Non-secure for non-secure or create and select your own secure profile.
- Set Sip Profile to **Standard SIP Profile**

Step 4 (EX and C-Series, including MX200, Devices Only) In the Product Specific Configuration Layout section:

- For Room Name, enter the Exchange Conference Room Name from Microsoft Exchange

  This setting must be the email address used in Exchange (e.g. room1@cisco.com).

- (Optional) Web Access

  This indicates whether the device will accept connections from a web browser or

  other HTTP client. Disabling web access for the device blocks access to the phone's internal web pages and certain support capabilities, but does not degrade normal operation. A device RESET is required for this parameter to take effect.

- (Optional) SSH Access

  This parameter indicates whether the device accepts SSH connections. Disabling the SSH server functionality blocks certain support capabilities such as log file collection but does not degrade normal operation.

- Default Call Protocol

  This parameter sets the default call protocol of the device. This device only supports SIP when registering to Cisco Unified Communications Manager.

- Quality Improvement Server

  Specifies a hostname or IP address of a remote system to collect quality improvement reports from the device. Use the default hostname or IP address, unless otherwise directed by the specific device documentation.

- Admin Username and Password

  Admin Username and Password are required for CTS-Manager to discover endpoints and provide One-Button-to-Push scheduling to them.

  a. Enter a user ID for the admin user (default: **admin**).

  Note Username must be between 1 and 64 characters long and cannot be “apache”, “daemon”, “nobody”,”root”, or “shutdown”.

b. Enter a password for the admin user (default: “”).

Note Password must be between 1 and 64 characters long and can only contain printable ASCII characters, except space.

Caution You must configure Admin Username and Password individually on both Unified CM and the endpoint device. If the username and/or passwords do not match between Unified CM and the endpoint device, the endpoint will not be discoverable or schedulable by CTS-Manager. If you change these in the future, it is recommended that you do so immediately before a maintenance cycle. If you do it during another time, you must go to **Configure > Unified CM**, select the Unified CM to which the endpoint is registered and click **Discover Rooms**.

Step 5 Click **Save** to save your settings.

The Phone Configuration screen appears.

Proceed to Assigning a Directory Number to a TelePresence Device.

Assigning a Directory Number to a TelePresence Device

In the Phone Configuration screen for the TelePresence device you configured, do the following to assign a directory number to the TelePresence Device:

Step 1 Under Association Information, click **Add a new DN**

Step 2 Under Directory Number Information, enter a phone number for your TelePresence device in the Directory Number field.

Step 3 Click **Save**.

Step 4 Verify that the Associated Devices field contains information that begins with “SEP” (Example: SEP6C504EDA443C).

Step 5 In the Line 1 on Device section, toward the bottom of the page, enter a name for your endpoint in the Display (Internal Caller ID) field.

Note If this field is left blank, the endpoint name will not display properly in the WebEx participant’s list for TelePresence meetings with WebEx.

Step 6 Click **Apply Config**.

Step 7 Click **OK** to confirm.

Verifying a TelePresence Device is Registered to Unified CM

After assigning a directory number to a TelePresence device, you can verify that the device is now registered to Unified CM by doing the following:

Step 1 First, you must find the device:

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

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

b. 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

   a. Choose the appropriate search pattern for your text search (for example, “Begins with”).

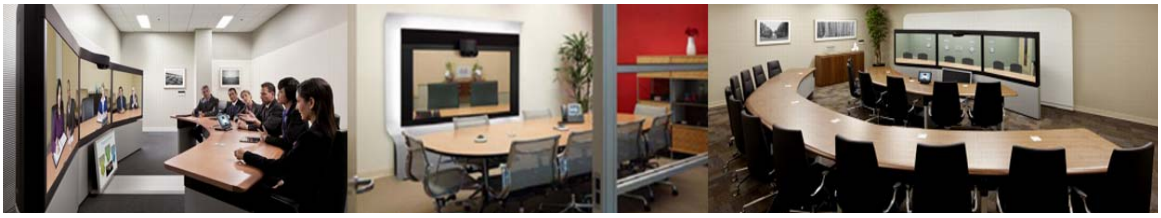
   b. Enter your search text in the **Find** field.

   c. Click **Find**.

Step 2 Under Device Name, the TelePresence device name should appear and under the Status column make sure that the device is shown as “Registered with” the name of the Unified CM.

Adding a TelePresence Device to the Application User

The final step to making a TelePresence device schedulable through CTS-Manager, is to add the TelePresence device to the application user used by CTS-Manager. For more information, refer to *Cisco Unified Communications Manager Configuration Guide for Cisco TelePresence System* for the steps to perform this.



CHAPTER 7

Installing and Configuring Cisco PreQualification Assistant

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

Contents

- Introduction, page 7-2
- Pre-Configuration Procedure Guidelines for Checking Initial Network Setup, page 7-2
- Installing the PreQualification Assistant Tool, page 7-3
- Running the Tool - Using the Tool Application Window, page 7-6
- Menu Commands, page 7-8
- File Menu Commands, page 7-8
- System Menu Command, page 7-8
- Using PreQualification Configuration Forms, page 7-11
- Calendar Server (Microsoft Exchange) Host Configuration Form, page 7-20
- Test Configuration Forms in an IBM Domino Environment, page 7-21
- Calendar Server (IBM Domino) Configuration Form, page 7-25
- Test Configuration Forms in a Microsoft Exchange Web Services (EWS) Environment, page 7-30
- WebEx Server, page 7-35

Introduction

This chapter 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 preconfiguration setup 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 that is used to configure CTS-Manager.

Pre-Configuration Procedure Guidelines for Checking Initial Network Setup

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

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

Table 7-1 Pre-Configuration Guidelines for Testing the System Network Setup for CTS-Manager

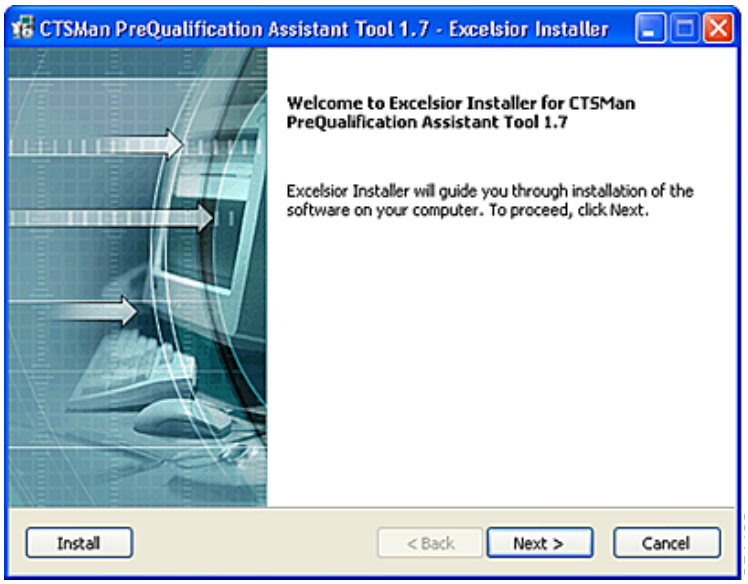
Setup Procedure Guidelines before Installing CTS-Manager	Description	Location
Install and configure PreQualification Assistant	Install, configure, and run the PreQualification Assistant to ensure that your preconfiguration setup is performed correctly. The data you enter into the Tool Test Configuration forms are used to verify connections to the servers and get data from them to be used to configure CTS-Manager	Current Chapter.
Next Step after Pre-Configuration		
(For installations on UCS server only) Configuring the UCS Server and VMware for Cisco TelePresence Manager	1	Chapter 8, "Configuring UCS Server and VMware for Cisco TelePresence Manager"
Install or Upgrade Cisco TelePresence Manager		Chapter 9, "Installing or Upgrading Cisco TelePresence Manager"

Installing the PreQualification Assistant Tool

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

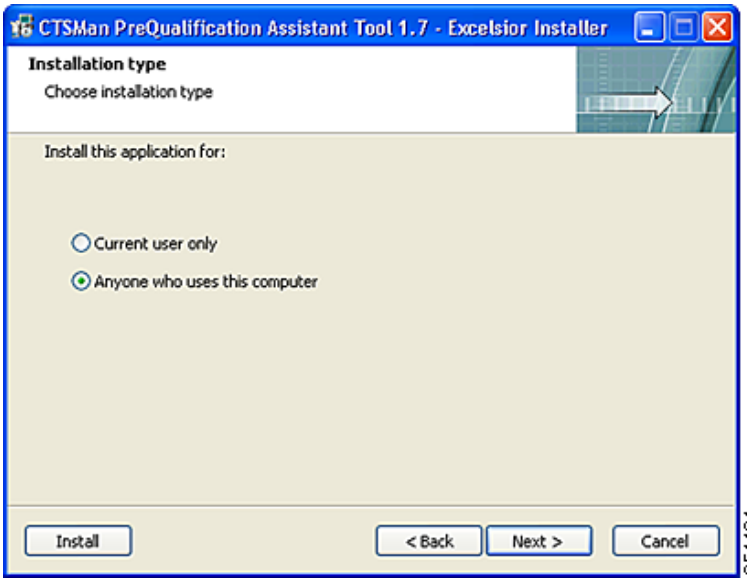
Step 1 Double-click the executable to begin the install process. After the Installer window appears, click the **Next** button.

Figure 7-1 PreQualification Assistant Installer Window



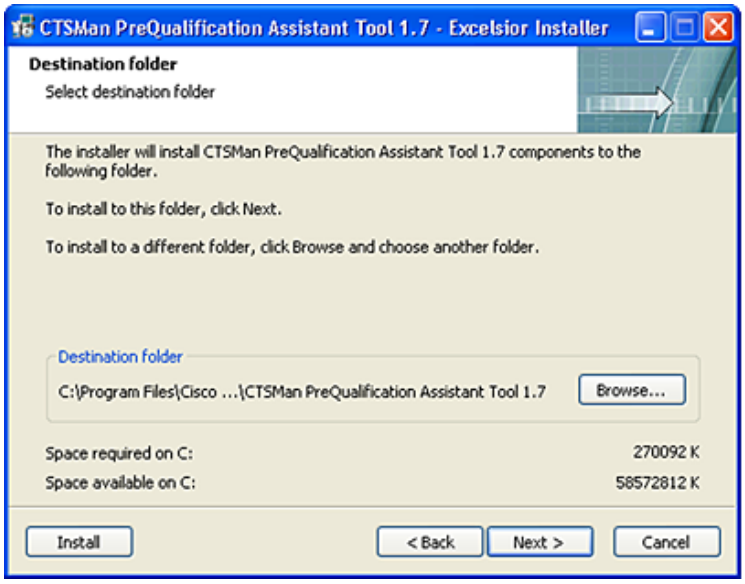
Step 2 Specify if the application is to be a personal profile or can be used by others. Then click the **Next** button.

Figure 7-2 Installation Type Window



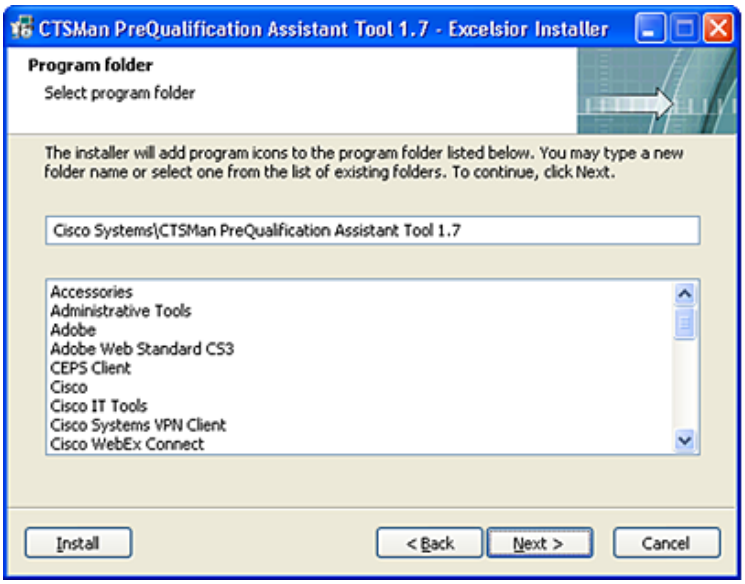
Step 3 Review and accept the destination folder defaults and click the **Next** button.

Figure 7-3 Destination Folder Window



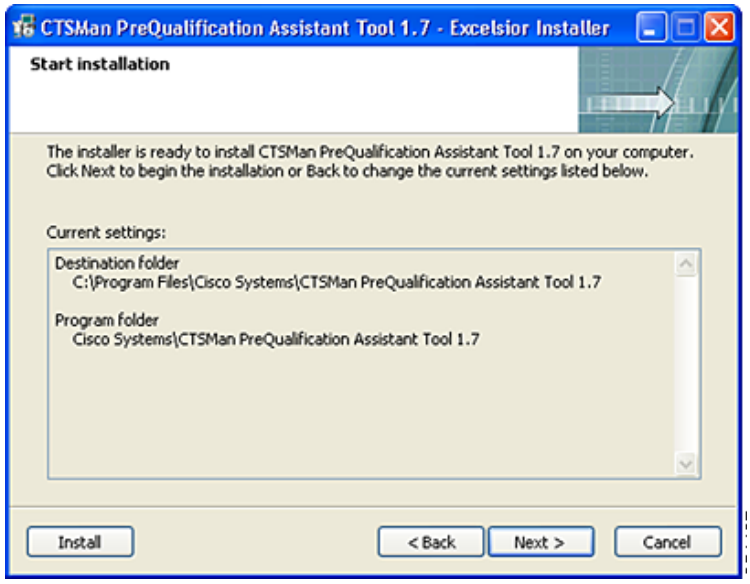
Step 4 Review the program folder destination, accept the defaults and click the **Next** button.

Figure 7-4 Program Folder Window



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

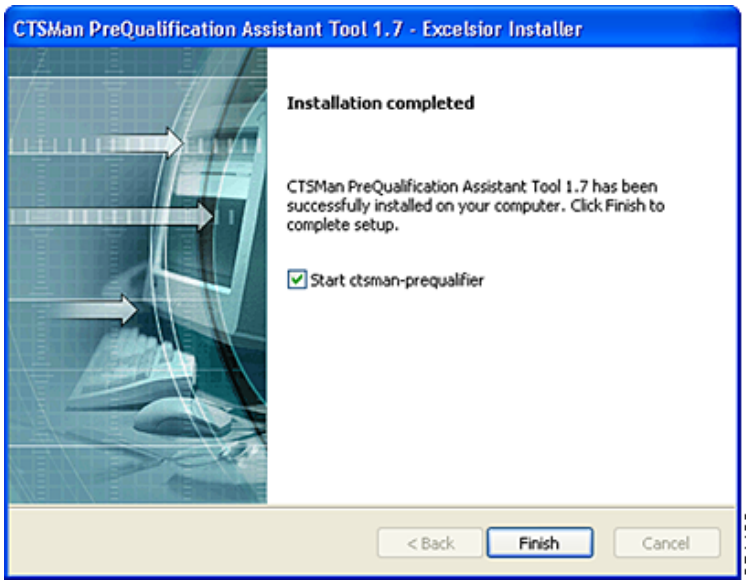
Figure 7-5 Start Installation Window



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 7-6 Installation Completed Window



Uninstalling a Previous Version

Uninstall previous versions using the PreQualification uninstaller.

Note The directory is not removed at the end of the uninstall.

To uninstall the CTS-Manager PreQualification Assistant Tool:

Step 1 Close the window.

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

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

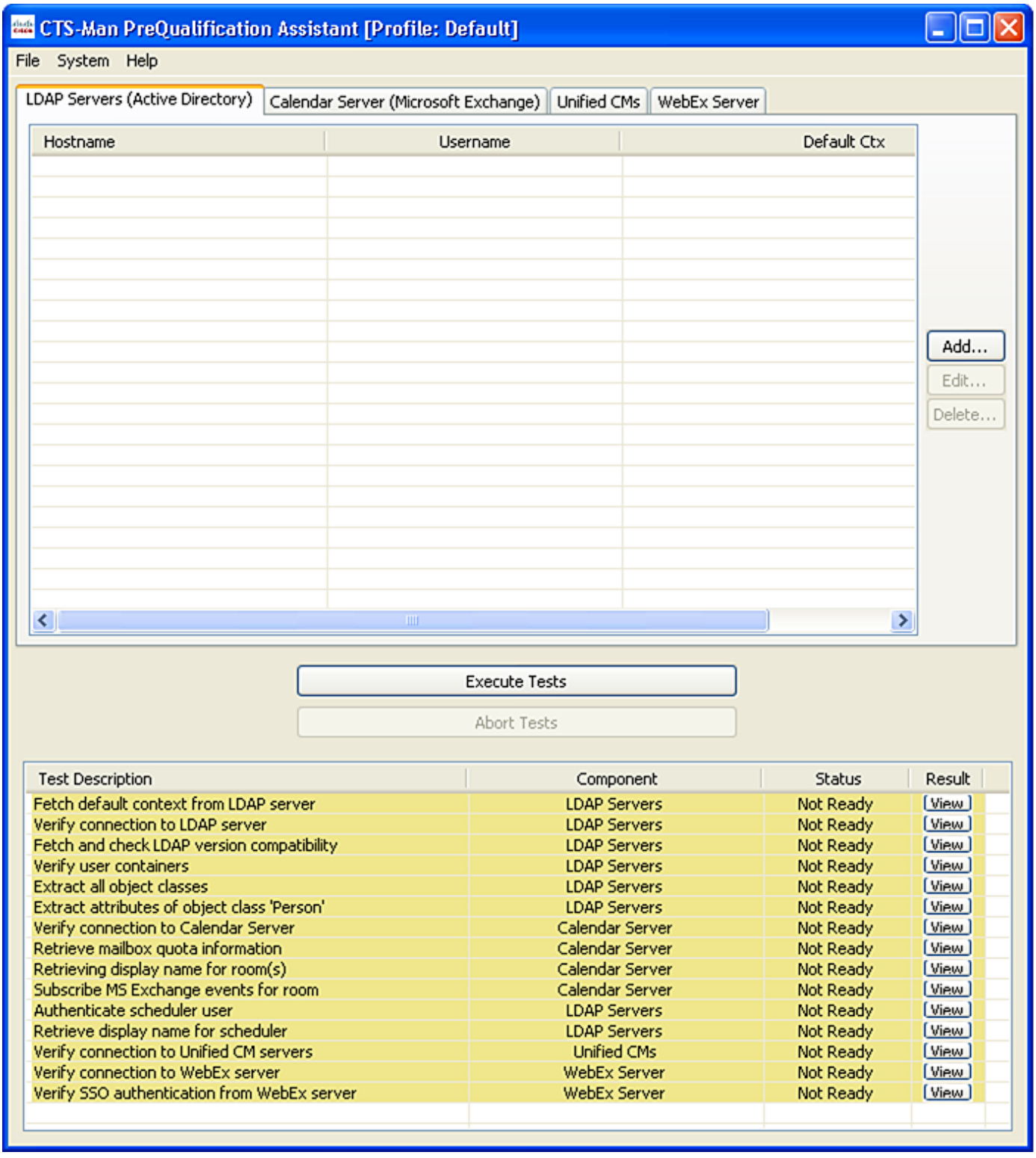
Running the Tool - Using the Tool Application Window

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 server, Cisco Unified CM servers and WebEx server. The four-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 7-7 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 the Execute Tests 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 describe 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.

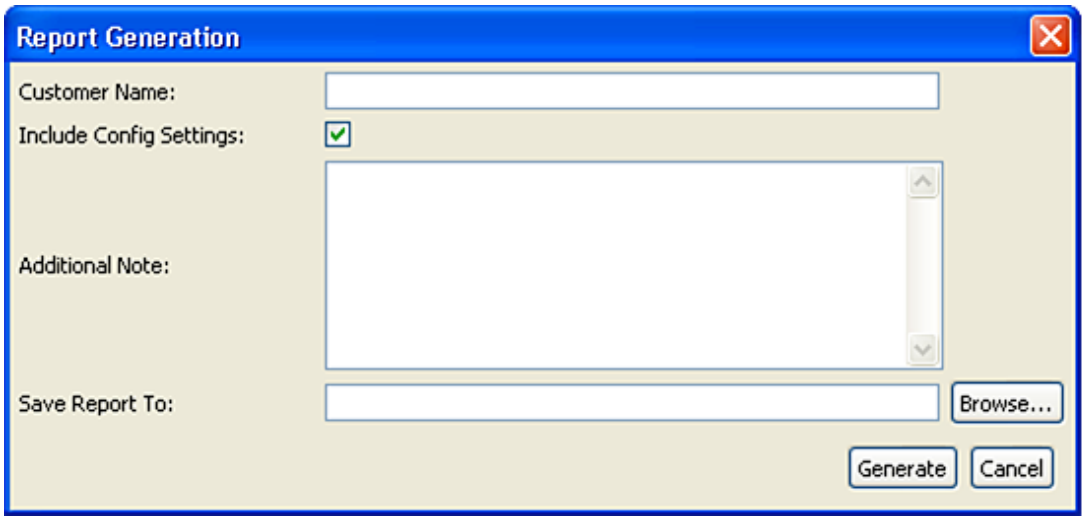
Figure 7-8 File Menu Commands

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 Tests 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 7-9.

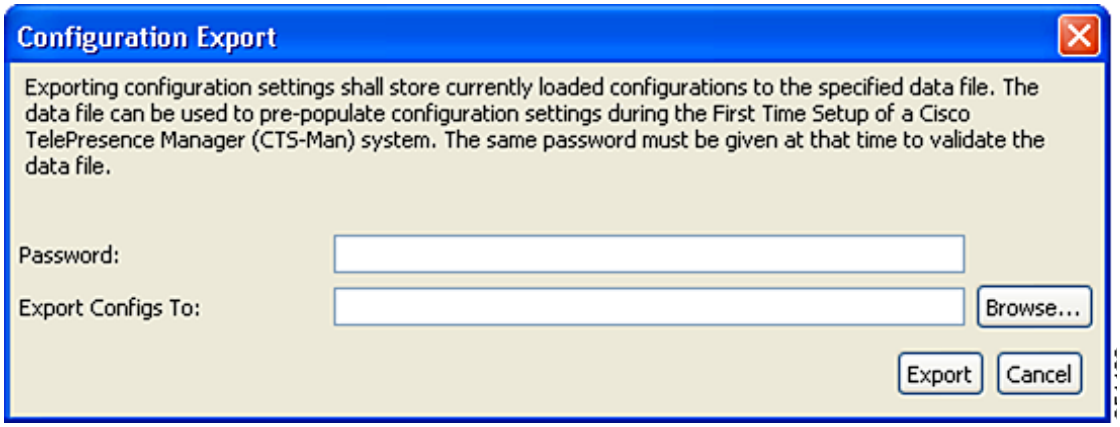
– If you check the **Include Config Settings** checkbox, the values you entered into the Host Configuration forms are collected and included in the zipped report.

Figure 7-9 Report Generation Window



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

Figure 7-10 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 Unified CM server configurations you've chosen from the Select Calendar Server command in the System menu.

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 7-11 The Test Status Window

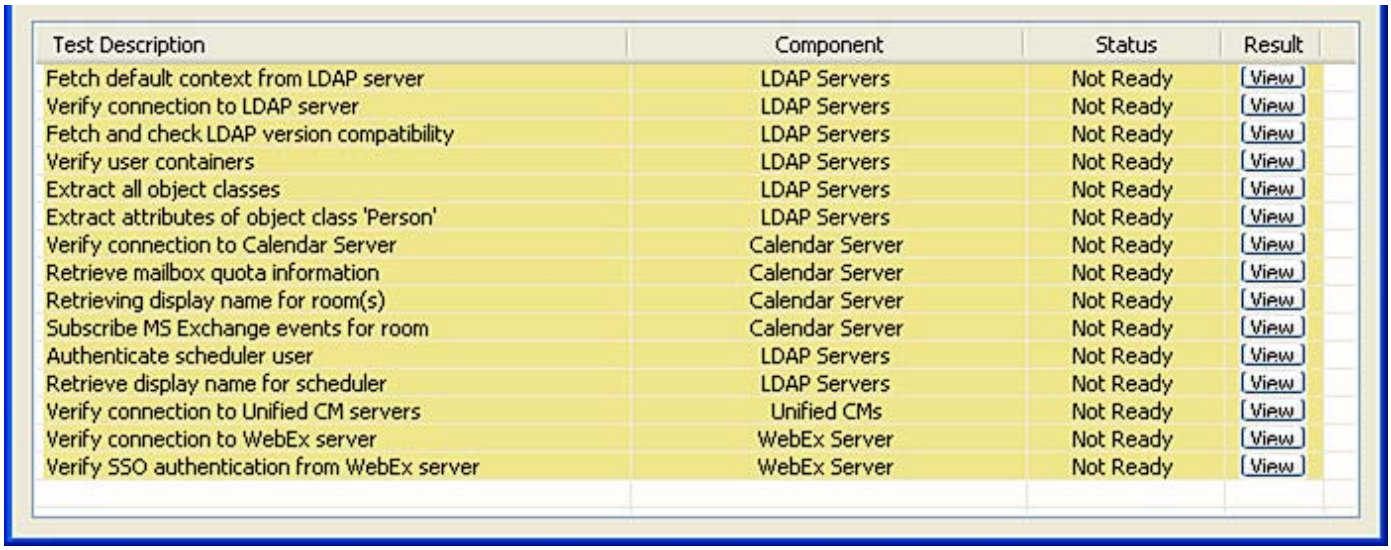


Table 7-2 Test Status Columns

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.

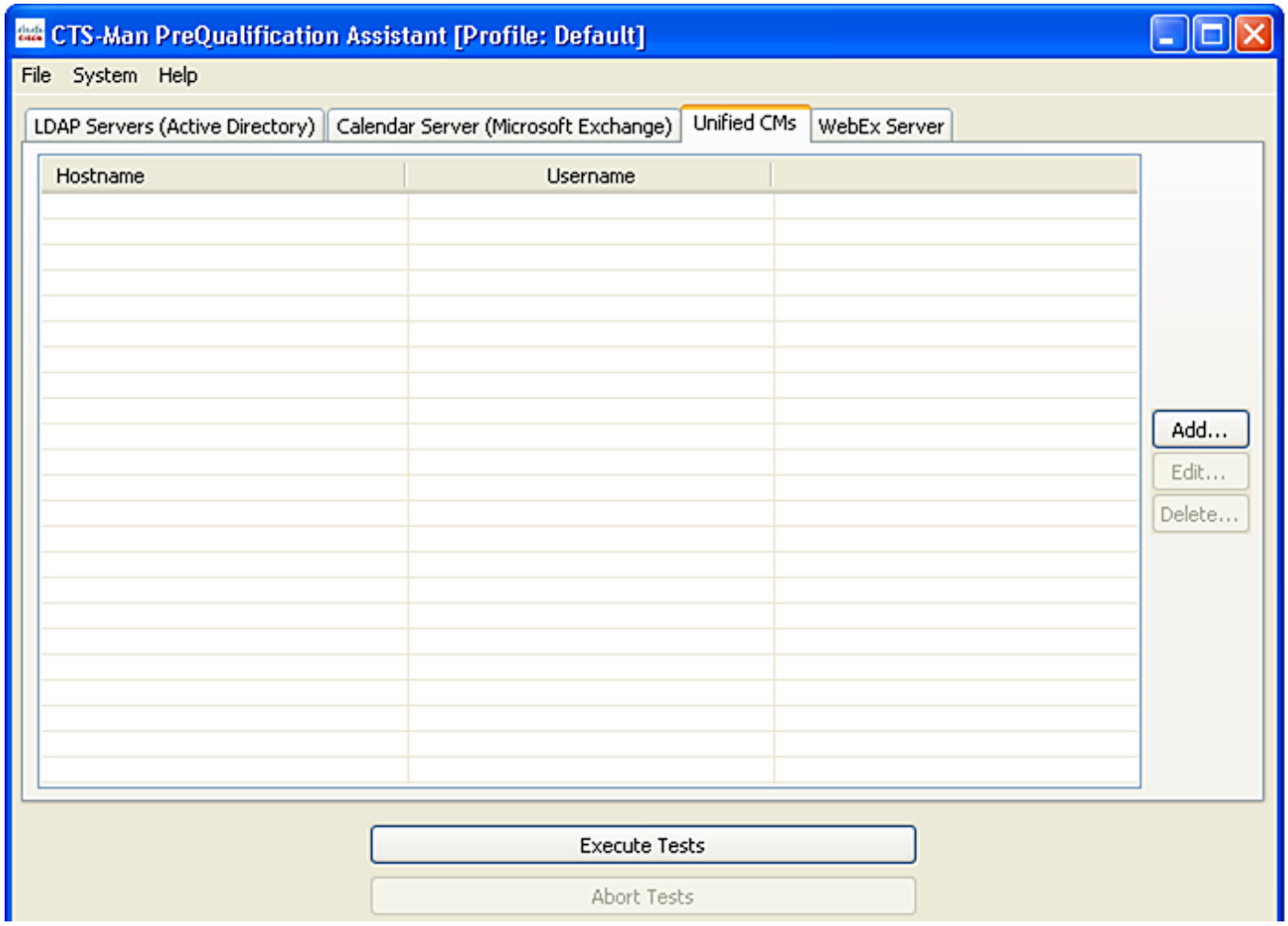
Using PreQualification Configuration Forms

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 Communications Manager Configuration Form

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

Figure 7-12 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 Unified CM 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 the **Edit** button to change the configuration.

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

When adding a Unified CM, click the **Add** button and the following Host Configuration window appears.

Figure 7-13 The Cisco Unified CM Add/Edit Configuration Form

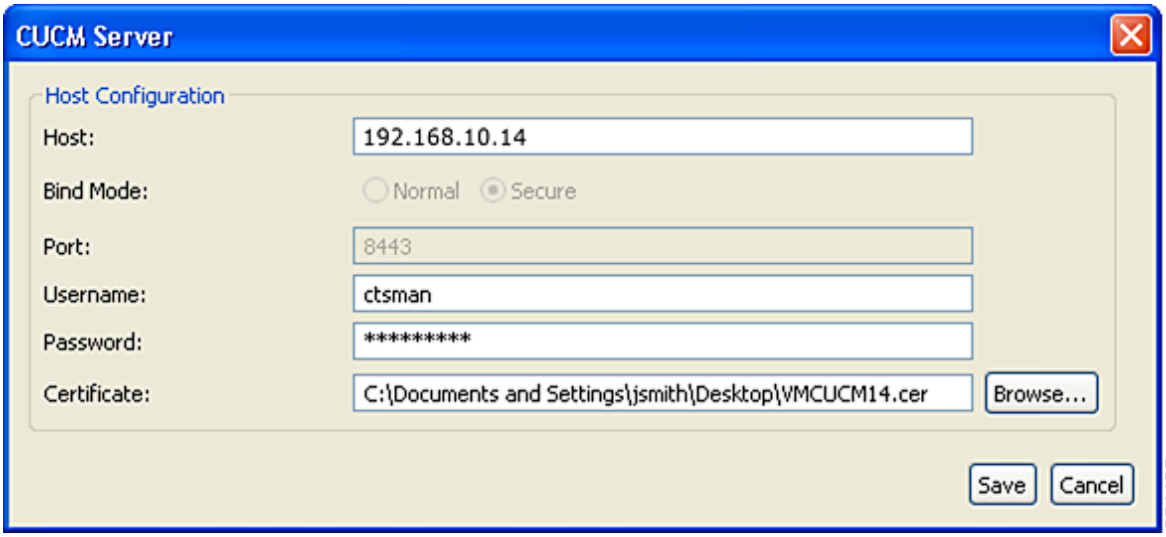


Table 7-3 The Cisco Unified CM Add/Edit Configuration Form Fields

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	Login 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 Unified CM or editing the configuration.

Test(s) Enabled by the Host Configuration Form

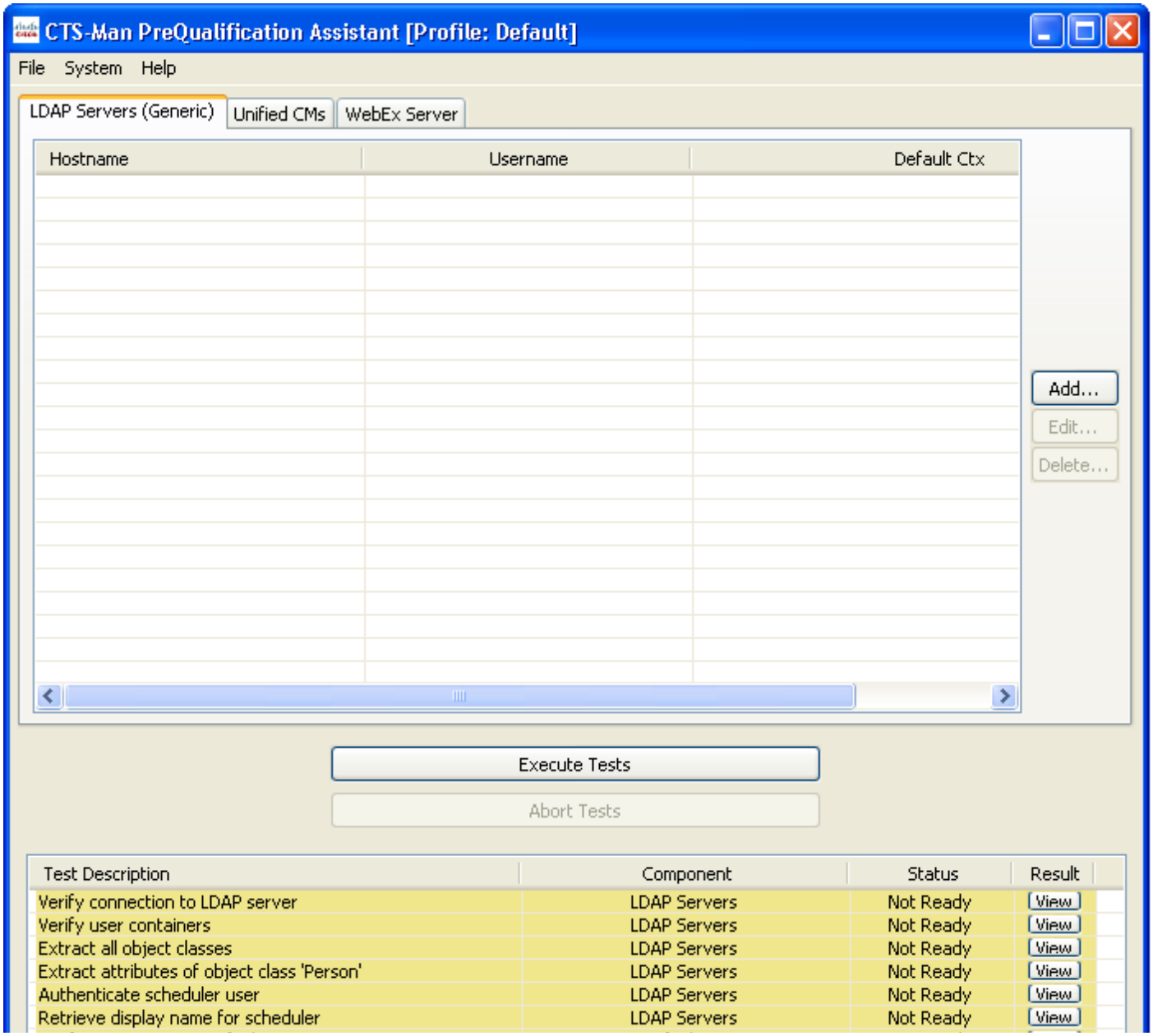
- Verify connection to Cisco Unified CM servers.

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 7-14 LDAP Server Generic Window



If it is necessary to change the configuration of one, highlight the line, and click the **Edit** button to change the configuration and the Host Configuration window appears, refer to Figure 7-15.

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

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

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

LDAP (Generic) Test Configuration Form

Figure 7-15 The LDAP Server (Generic) Add/Edit Configuration Form

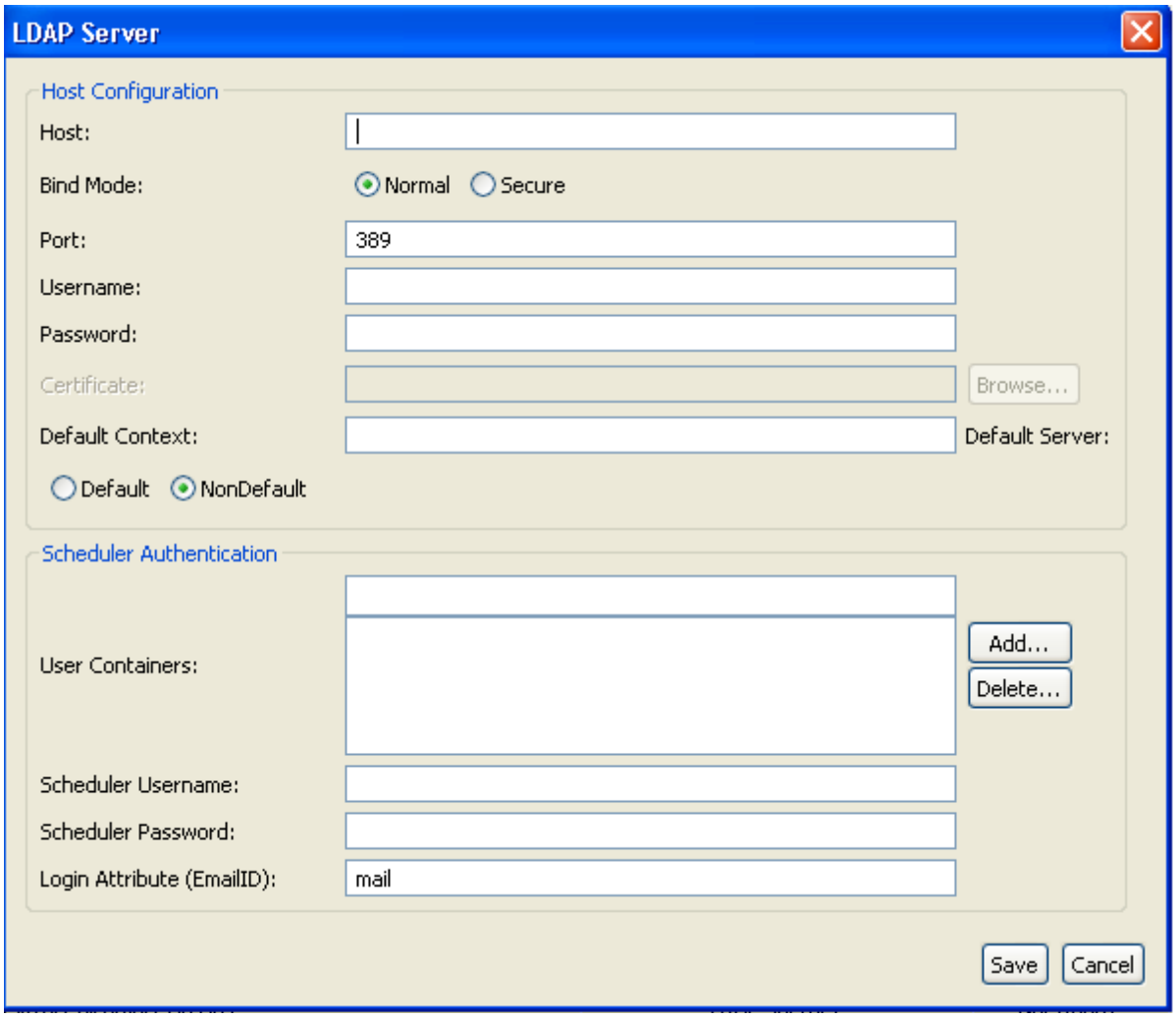


Table 7-4 The LDAP Server (Generic) Add/Edit Configuration Form Fields

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 login 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 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.

Table 7-4 The LDAP Server (Generic) Add/Edit Configuration Form Fields (continued)

Field Name	Field Value
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

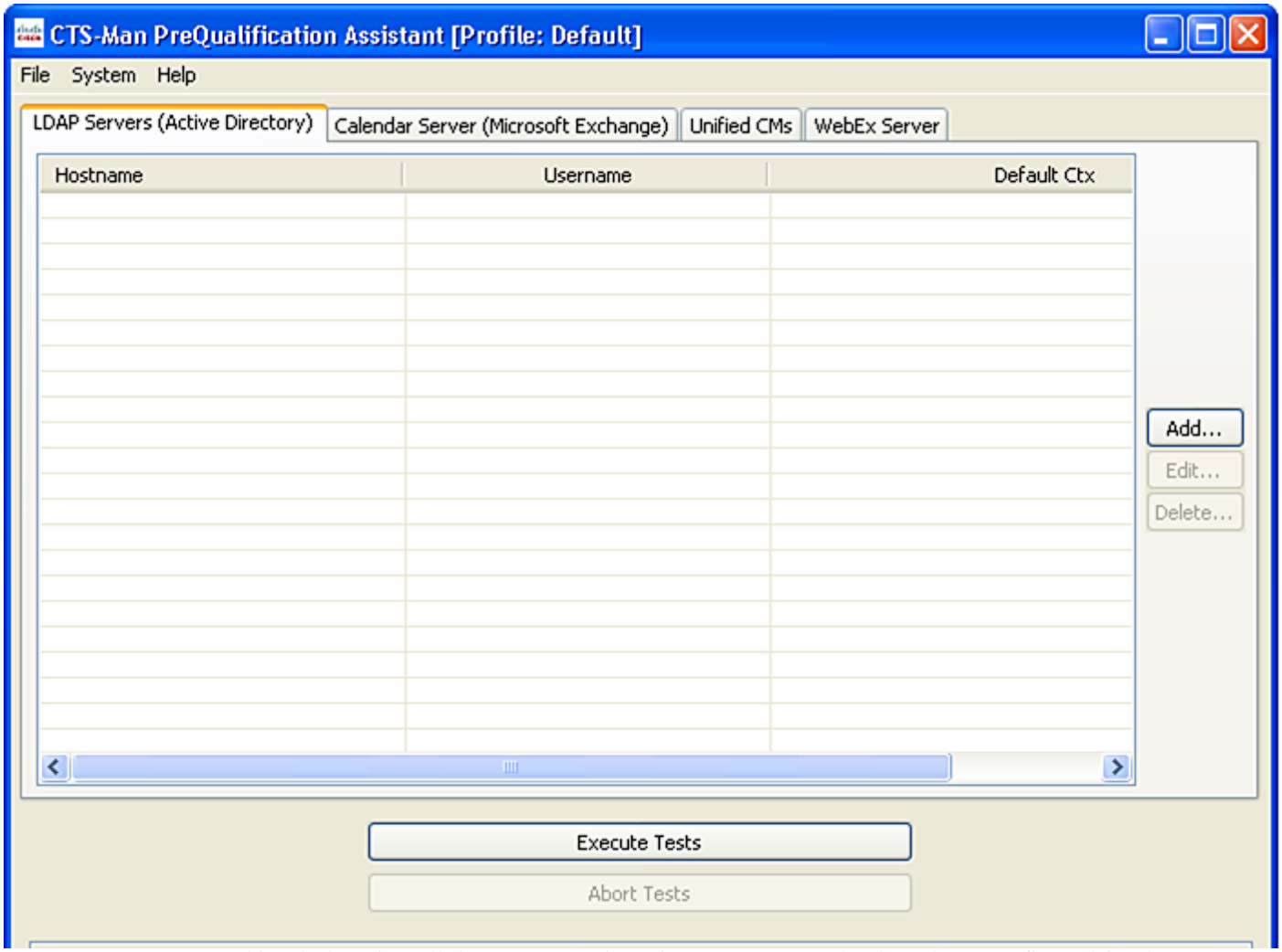
- Verify connection to LDAP server
- Verify user containers
- Extract all object classes
- Extract attributes of object class ‘Person’

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 7-16 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 the **Edit** button to change the configuration.

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

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

LDAP Server (Active Directory) Test Configuration Form

Figure 7-17 The LDAP Server (Active Directory) Add/Edit Configuration Form

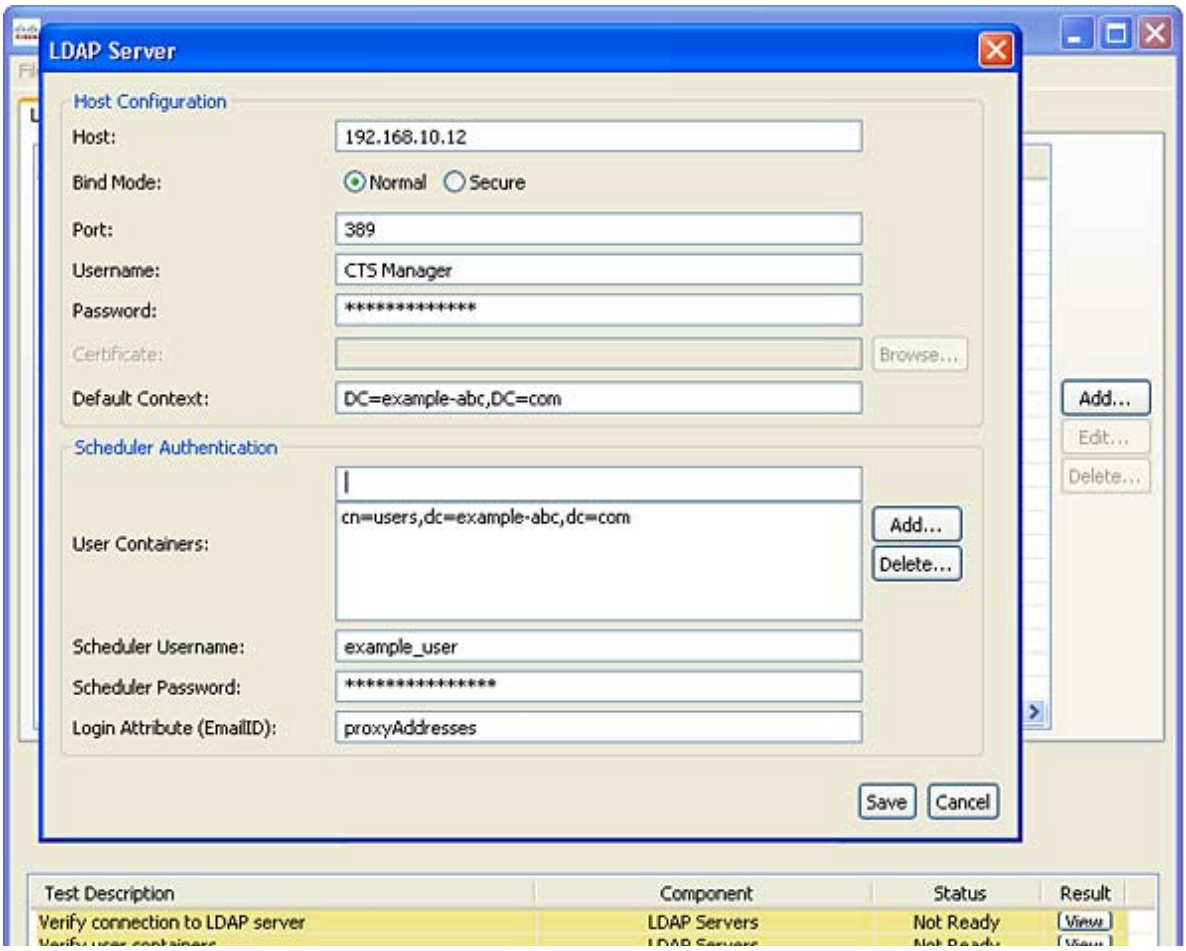


Table 7-5 The LDAP Server (Active Directory) Test Configuration Form Fields

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*

Table 7-5 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.
User Containers	The containers from which queries are performed to retrieve user objects. More than one user container or user object can be specified. Cisco TelePresence Manager uses the values entered to search through the containers in sequence to retrieve user and meeting room (endpoint) information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication. 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 7-18 The Calendar Server (Microsoft Exchange) Host Configuration Form

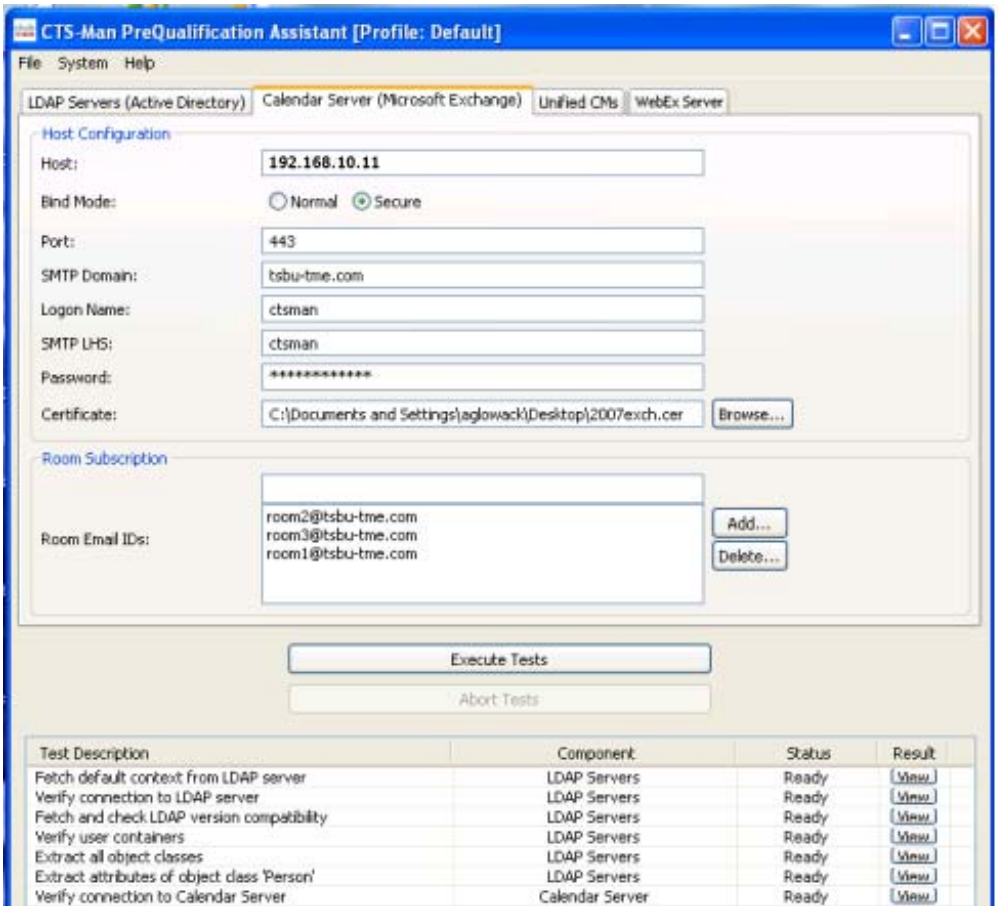


Table 7-6 The Calendar Server (Microsoft Exchange) Host Configuration Fields

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 (endpoints).
Password	Enter the password for the CTS-Manager test account or Exchange administrative account, using English characters only.

Table 7-6 The Calendar Server (Microsoft Exchange) Host Configuration Fields (continued)

Field Name	Field Value
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 (endpoints). 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

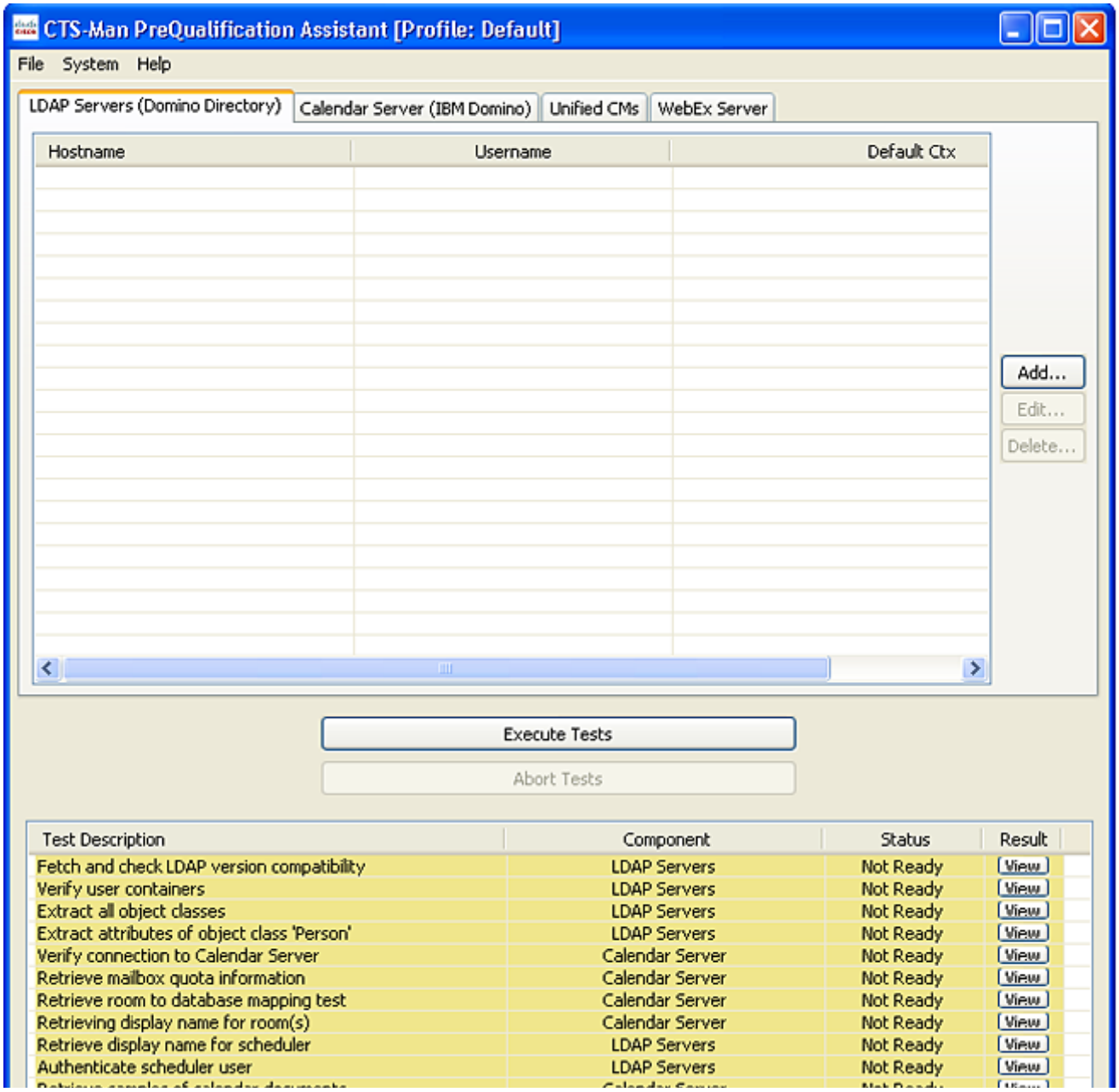
- Verify connection to Calendar Server
- Retrieve mailbox quota information
- Retrieving display name for room(s) (endpoints)
- Subscribe MS Exchange events for room (endpoint)

Test Configuration Forms in an IBM Domino Environment

You can use the PreQualification Assistant 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 7-19 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 the **Edit** button to change the configuration.

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

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

LDAP (Domino Directory) Host Configuration Form

Figure 7-20 The LDAP Server (Domino Directory) Add/Edit Configuration Form

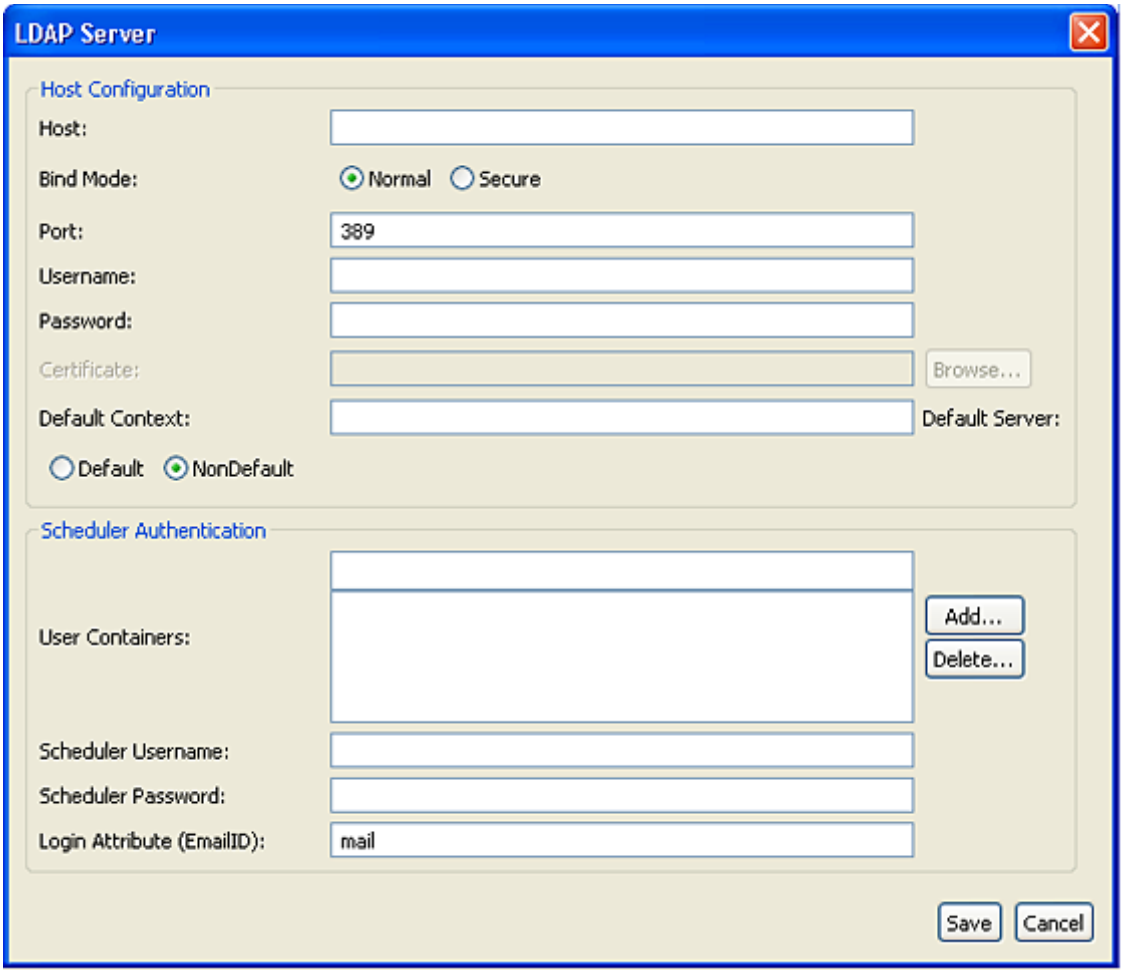


Table 7-7 The LDAP Server (Domino Directory) Test Configuration Form Fields

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 7-7 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 (endpoint) 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 Tests button

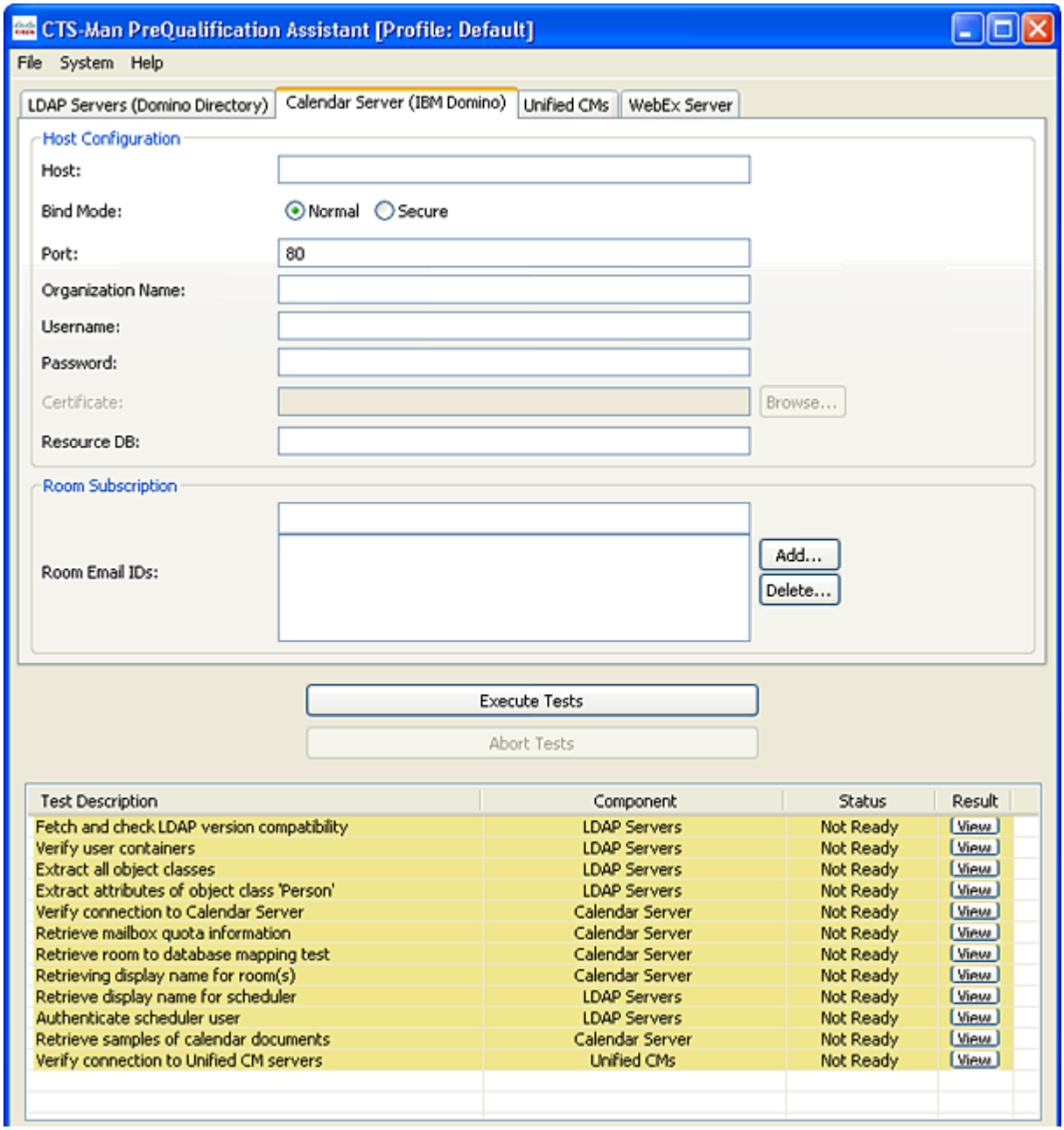
- Fetch and check LDAP version compatibility
- Verify user containers
- Extract all object classes
- Extract attributes of object class “Person”
- Retrieve display name for scheduler
- Authenticate scheduler user
- Verify connection to Unified CM servers

Calendar Server (IBM Domino) Configuration Form

You can use the PreQualification Assistant to test your LDAP Calendar server configurations when specifying a IBM Domino Calendar server. This applies when from the pull-down menu, the user selects **System > Select Calendar Server > IBM Domino**.

The Calendar Server (IBM Domino) window appears as shown in Figure 7-21

Figure 7-21 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 (endpoint) 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, enter the room email ID and click the **Add** button.

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

Table 7-8 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 account name used to log on to the Domino server. The format is determined by the Email ID fields in the Person object classes and attributes.
Password	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: *Testendpoint/Site1*

Test(s) Enabled by the Execute Tests button

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

Cisco Unified Communications Manager Server (IBM Domino) Configuration Window

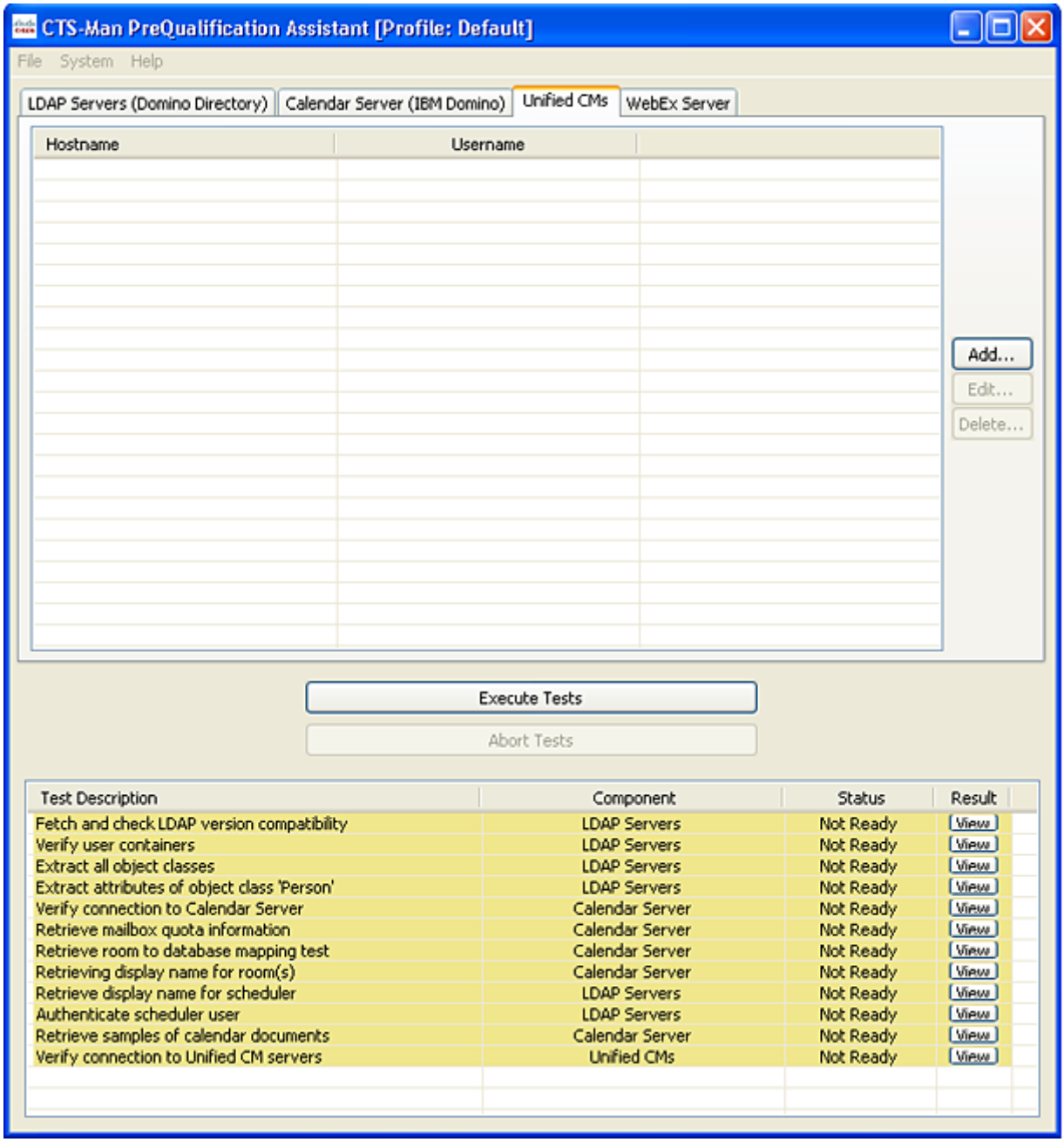
This window lists all the Cisco Unified CM (Unified CM) servers that have been configured for the CTS-Manager. If all of the Unified CM servers have been configured, use the Execute Tests button to make sure that they have been configured correctly.

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

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

When adding a Unified CM, click the **Add** button and the following Host Configuration window appears.

Figure 7-22 Unified Communications 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 the **Edit** button to change the configuration.

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

When adding an LDAP server, click the **Add** button and the following configuration window appears.

LDAP (Domino Directory) Host Configuration Form

Figure 7-23 The Cisco Unified CM Add/Edit Configuration Form

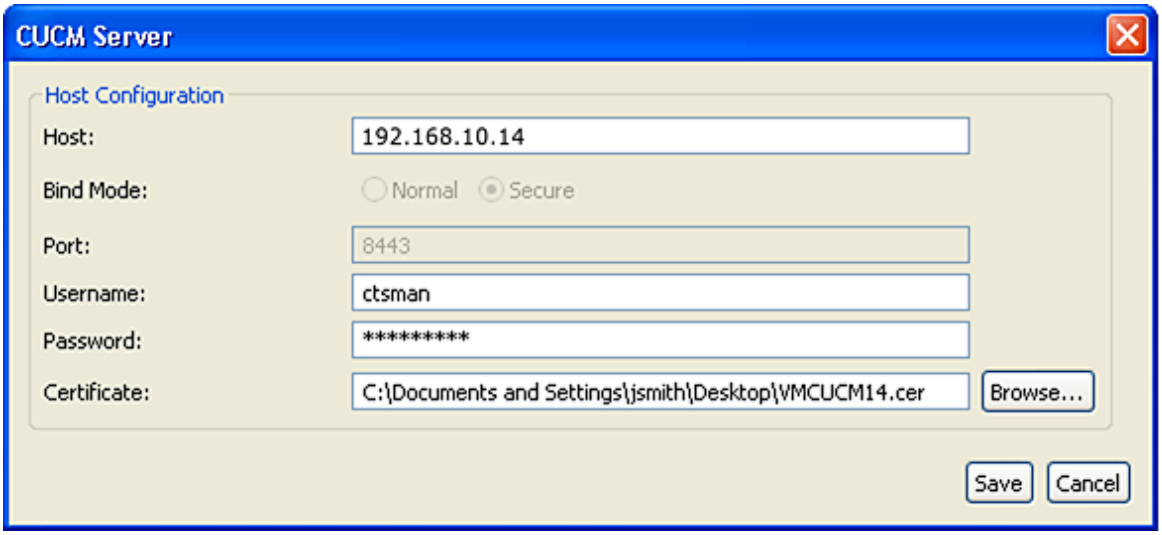


Table 7-9 The Cisco Unified CM Add/Edit Configuration Form Fields

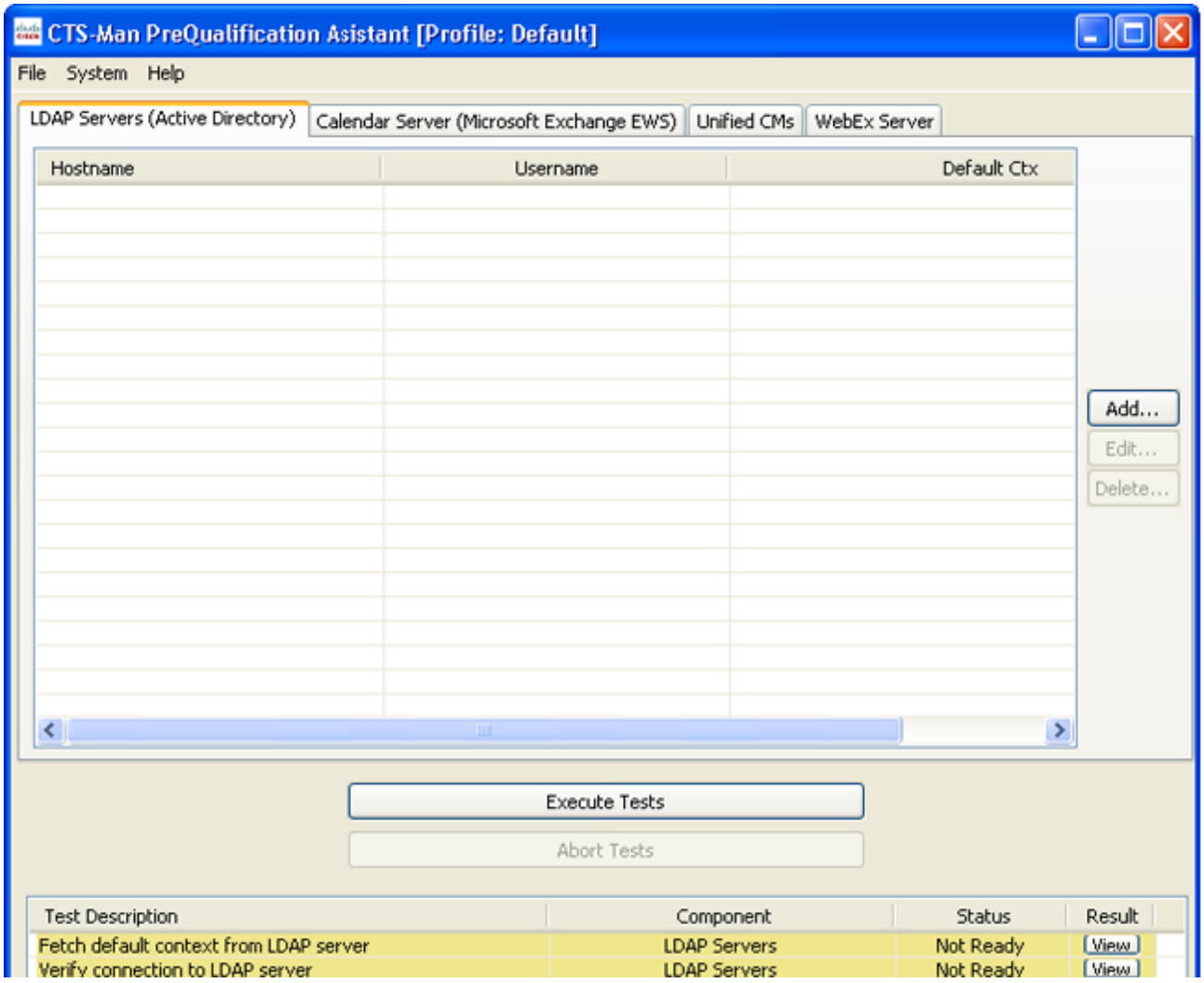
Field Name	Field Value
Host	The hostname or IP address of Cisco Unified CM
Bind Mode	This is always set to secure mode.
Port	This is always set to port 8443.
Username	Login account with Cisco Unified CM Application Username. The admin username is not needed.
Password	Password for Cisco Unified CM Admin 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 Unified CM or editing the configuration.

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 Calendar 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 7-24 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 the **Edit** button to change the configuration and the Host Configuration window appears, refer to Figure 7-25.

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

When adding another LDAP server, click 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 7-25 The LDAP Server (Active Directory) Add/Edit Configuration Form

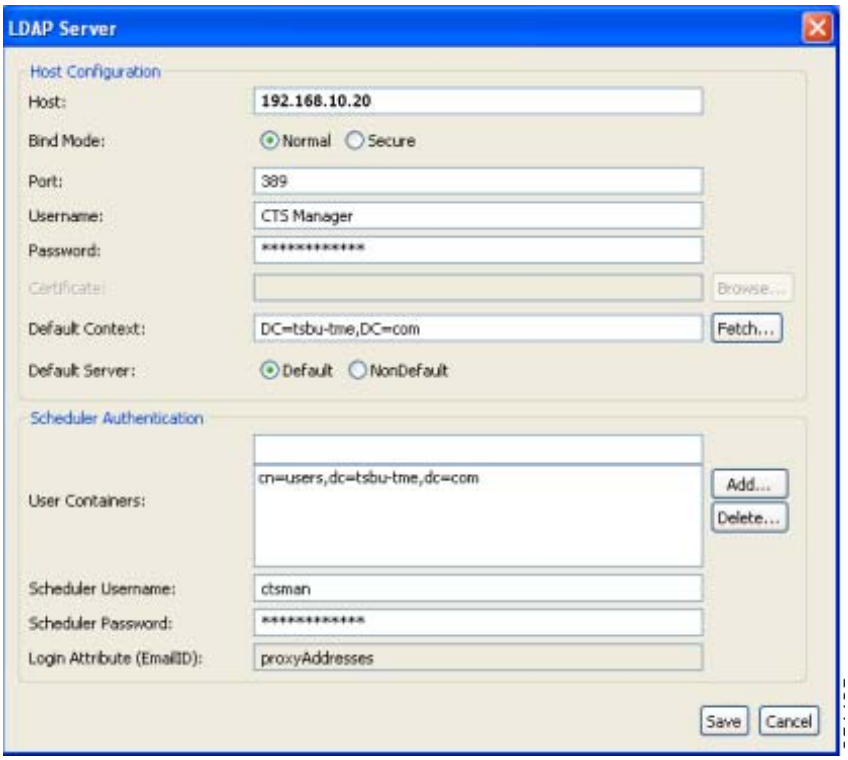


Table 7-10 LDAP Server (Active Directory) Test Configuration Form Fields

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.
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.*

Table 7-10 LDAP Server (Active Directory) Test 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 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 (endpoint) 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 Tests 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) (endpoints)
- Subscribe MSEWS events for room (endpoint)

- 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 7-26 appears. This window allows you to configure the calendar server for Microsoft Exchange EWS and add or delete room (endpoint) subscriptions.

Figure 7-26 LDAP Calendar Server Microsoft Exchange EWS Configuration Window

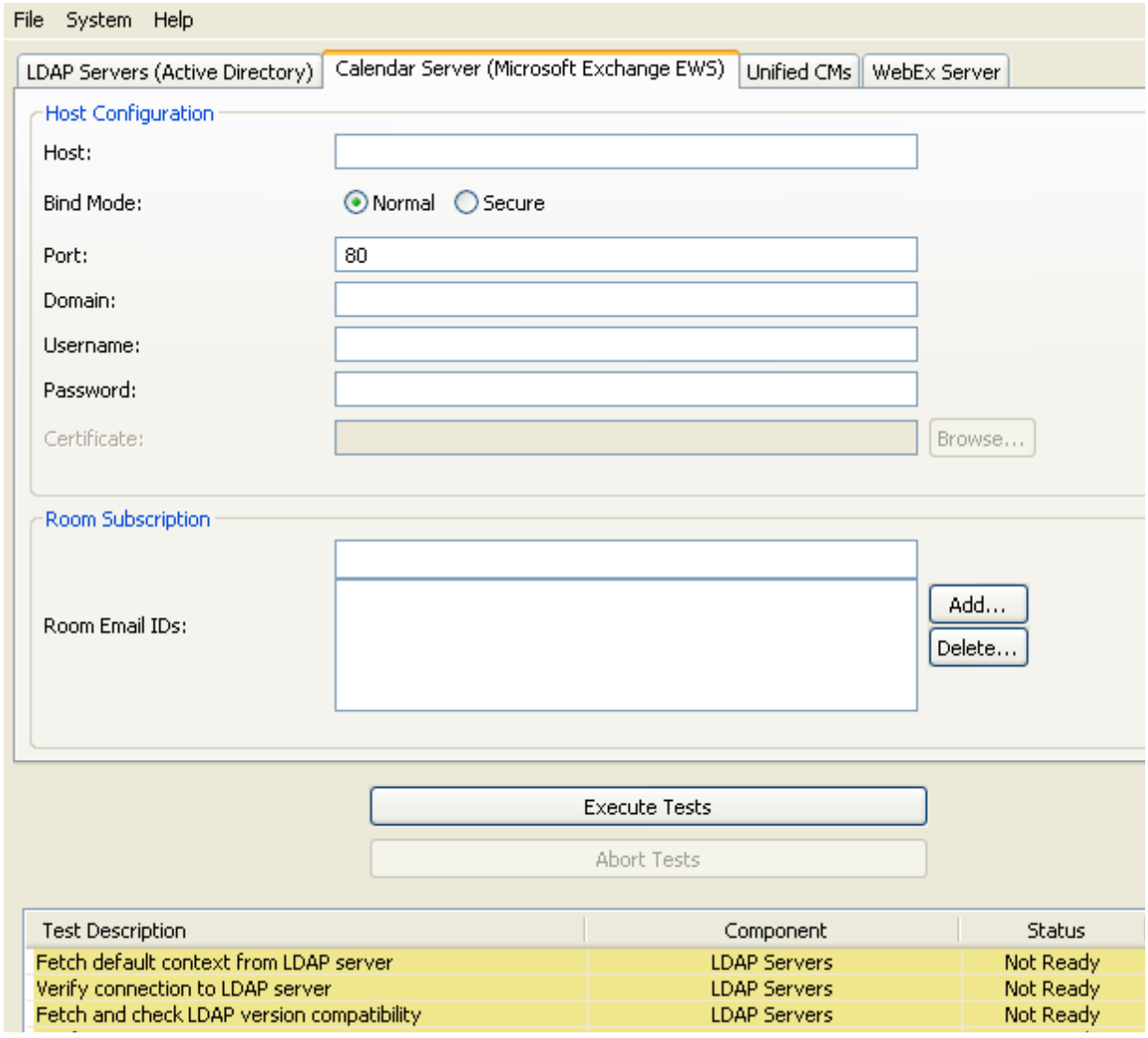


Table 7-11 Calendar Server (Microsoft Exchange) Host Configuration Form Fields

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.

Table 7-11 Calendar Server (Microsoft Exchange) Host Configuration Form Fields (continued)

Field Name	Field Value
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 for the Exchange EWS server. **Note** If you are using Windows authentication, the format is: **domain\username**. If you are using basic authentication, the format is: **username@ldapdomainname.com** ⚠ **Caution** If the CTS-Manager user logon name is different from the LHS of the email ID and there is no matching email ID for the user, Microsoft Exchange EWS will fail the mailbox quota test. To avoid this, add a secondary email ID that uses the CTS-Manager logon name as the LHS of the email ID appended with the SMTP domain.
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.

WebEx Server

On this tab you configure a connection to the WebEx scheduling server, necessary for enabling the WebEx feature in CTS-Manager. The purpose of this is to test connectivity to the WebEx site. This information is not imported into CTS-Manager during first-time setup.

Figure 7-27 WebEx Server Window

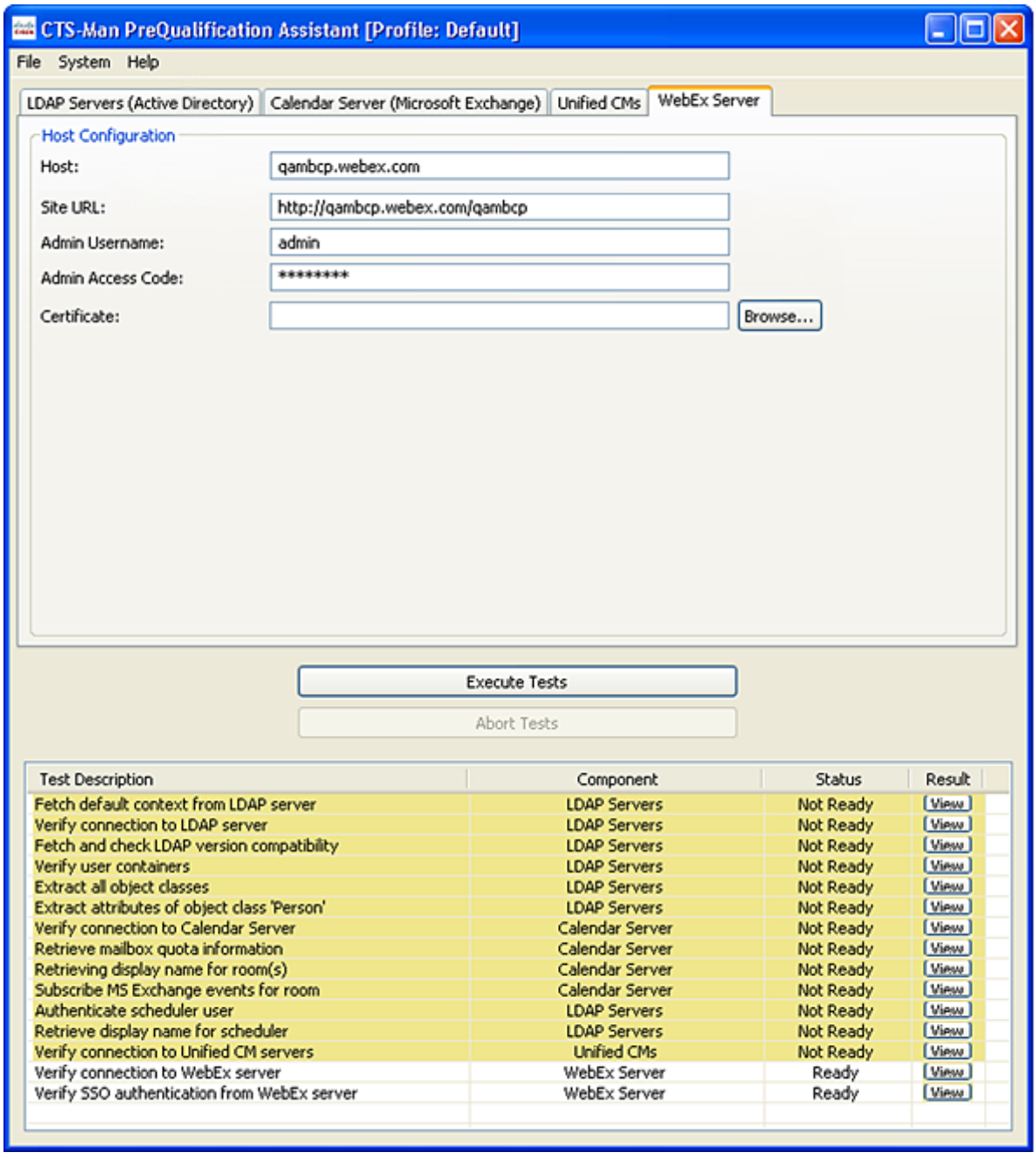
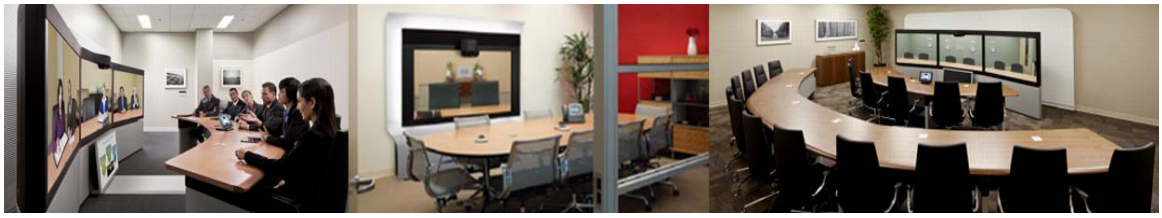


Table 7-12 WebEx Server Host Configuration Form Fields

Field	Description or Settings
Host	The configured hostname of the WebEx scheduling server.
Site URL	The address used to construct the URL that's used to access this meeting. This is the actual URL that CTS-Manager uses to communicate with WebEx. This is published in the email from CTS-Manager, and is displayed to users on the WebEx page of the CTS phone UI.
Admin Username	WebEx administrator's username (provided by the WebEx team)
Admin Access Code	WebEx administrator's access code (provided by the WebEx team)
Certificate	Certificate from the hostname (WebEx scheduling server) **Note** To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer, then click Browse to select it and upload it to CTS-Manager. For detailed instructions on downloading the certificate with different browsers, see First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15.



CHAPTER 8

Configuring UCS Server and VMware for Cisco TelePresence Manager

First Published: May 29, 2012

Contents

- Introduction, page 8-1
- Installation Guidelines, page 8-2
- Requirements, page 8-3
- Firmware Recommendation and Upgrade, page 8-3
  - Checking the Firmware Version on the UCS Server, page 8-3
  - Upgrading the Firmware on the UCS Server, page 8-4
- Configuring RAID on the UCS Server, page 8-6
- Installing VMware on the UCS Server, page 8-8
- Installing the VMware Client and Setting Up the Datastore, page 8-9
- Disabling LRO, page 8-11
- Creating the Virtual Machine, page 8-11
- Installing CTS-Manager, page 8-13
- Upgrading VMware Tools, page 8-13
- Installing the VMware License Key, page 8-14
- Setting Automatic Startup for CTS-Manager, page 8-15

Introduction

This chapter describes how to configure the UCS C-210 M2 server and VMware for Cisco TelePresence (CTS) Manager.

Note If you are going to install CTS-Manager on an MCS server, skip this chapter and go directly to Chapter 9, "Installing or Upgrading Cisco TelePresence Manager."

Installation Guidelines

The purpose of this section is to provide the information you need in order to install the CTS-Manager software.

The tasks required to install and configure CTS-Manager are provided in the following table.

Table 8-1 Installation Overview for CTS-Manager

Setup Procedures	Description	Location
Configuring the UCS Server and VMware for Cisco TelePresence Manager		Current chapter
Installing or Upgrading Cisco TelePresence Manager		Chapter 9, "Installing or Upgrading Cisco TelePresence Manager"
Initializing CTS-Manager	After installing the CTS-Manager software, the next process is to initialize 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 (endpoint) information, and Cisco Unified Communications Manager for conference room (endpoint) availability and telephone support	Chapter 10, "Initializing Cisco TelePresence Manager"
Additional Installation Procedures for CTS-Manager	The administrator makes use of the Configure section to perform system configuration tasks such as synchronizing system databases, managing security, and reconfiguring system settings	Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager"
Configuring Cisco TelePresence WebEx OneTouch for CTS-Manager	Describes how to set up Cisco TelePresence WebEx OneTouch in CTS-Manager, which allows WebEx participants to join TelePresence meetings.	Chapter 12, "Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager"
Next Step after Pre-Configuration		
Monitoring CTS-Manager	Monitoring and updating meeting schedules and monitoring the status of rooms (endpoints) and system services	Chapter 13, "Monitoring and Supporting Cisco TelePresence Manager"

Requirements

Before you begin, make sure you have the following items:

- Hostname and IP address for the VMware ESXi host (UCS server)
- Hostname and IP address for Cisco TelePresence Manager (Virtual machine)
- IP address of DNS server
- Subnet mask
- Default gateway
- Domain name
- IP address of NTP server
- Cisco UCS Server Configuration Utility CD
- VMware ESXi 4.0, 4.1 or 5.0/vSphere 5 Standard for 1 processor (Purchase from Cisco or VMware.)
  - When purchasing from Cisco, use the following SKU: VMW-VS5-STD-1A.
  - When downloading the VMware software, make sure to select ESXi 4.0, 4.1 or 5.0.
- OVF template file for CTS-Manager (Download from Cisco.com)
- PC running Microsoft Windows connected to the same network as the UCS server
- CTS-Manager 1.9 installation software
- Virtualization Support

  Multiple instances of CTS-Manager and CTMS can be installed as virtual machines on the UCS C210 M2 server using VMware ESXi 4.0, 4.1 or 5.0.
  - 1 CTS-Manager and 1 CTMS can be installed on a single UCS server.
  - CTS-Manager with up to 4 instances on a single server, for service provider deployments with no more than 50 endpoints under management per instance of CTS-Manager.

  For more information about virtualization, including sizing guidelines, application support and storage requirements, refer to the Cisco Unified Communications Virtualization Wiki:

  http://docwiki.cisco.com/wiki/Before_You_Buy_or_Deploy_-_Considerations_for_Design_and_Procurement#Useful_Links

Firmware Recommendation and Upgrade

For the best results, Cisco recommends UCS firmware version 1.2.2d or later.

Checking the Firmware Version on the UCS Server

To check the firmware version on the UCS server:

Step 1 Set up Cisco Integrated Management Controller (CIMC) for your UCS Server.

For more information, refer to:
http://www.cisco.com/en/US/products/ps10493/products_configuration_example09186a0080b10d66.shtml

Step 2 In the CIMC Configuration Utility, configure the IP address and save the changes:

- NIC mode: dedicated
- NIC redundancy: none

Step 3 Open a browser and go to the CIMC IP address.

Step 4 Log in to the CIMC

By default, the username is **admin** and the password is **password**.

Step 5 Go to **Admin > Firmware Management**.

The firmware version is displayed here. It is also displayed on the login page.

Step 6 If you want to upgrade the firmware, go to the next section: Upgrading the Firmware on the UCS Server, page 8-4

Upgrading the Firmware on the UCS Server

To upgrade the firmware on the UCS server:

Step 1 Download the firmware from Cisco:

a. Go to: http://cisco.com/support

b. Click the **Downloads** tab

c. Click in the Find field, enter **UCS** and click **Find**.

The Select a Product page appears.

d. Click the link for the **Cisco UCS C-210 M2 Rack-Mount Server Software**.

The Download Software page appears.

e. Click the link for **Unified Computing System (UCS) Server Firmware**.

The available firmware releases are displayed.

f. Select a firmware release and click **Download Now**.

g. Log in to Cisco.com (if required).

h. In the Download Cart page, click **Proceed With Download**.

The End User License Agreement page appears.

i. Click **Agree**.

j. Select one of the available download options.

k. Click the **Download** link.

Step 2 Log in to the CIMC (if not already logged in).

Step 3 Go to **Admin > Firmware Management**

Step 4 Click **Install CIMC Firmware through Browser Client**.

The Install Firmware window appears.

Step 5 Click **Browse**, select the firmware you downloaded and click **Install Firmware**.

Step 6 When a message appears indicating the upgrade is completed successfully, click **Activate CIMC Firmware**.

Step 7 The upgrade takes about 20 minutes.

Step 8 When the upgrade is complete, reboot the UCS server.

Configuring RAID on the UCS Server

This section describes the process for configuring RAID on the UCS server. RAID must be configured before installing VMware, setting up the virtual machine and installing CTS-Manager.

Note If the UCS server was purchased from the TelePresence Technology Group (TTG) or Voice Technology Group (VTG) at Cisco, the RAID will be preconfigured. In this case, skip this section and start in the Installing VMware on the UCS Server section.

To configure RAID on the UCS Server:

Step 1 Insert the Cisco UCS Server Configuration Utility CD and reboot UCS server.

Cisco UCS Server Configuration Utility version 1.0.0 screen appears.

Step 2 Wait for application to load and the License Agreement screen to appear.

Step 3 Click **I Accept** and click **Next**.

The My Server screen appears.

Step 4 Click RAID Configuration

The Choose RAID Controllers screen appears.

Step 5 Click **LSI MegaRAID SAS 9261-8i (External)** and click **Next**.

Step 6 The RAID Configuration screen appears.

Step 7 Click **Create custom or multiple RAID Arrays (advanced)** and click **Next**.

The Select Drives for Logical Drive screen appears.

Step 8 Select Disks **0** and **1** and click **Next**.

The Select Hotspare Drives screen appears.

Step 9 Click **Next**.

The Define Array Attributes screen appears.

Step 10 Set the fields the following way:

- RAID Level: **1**
- Stripe size: **64k** (only option)
- Read policy: **Read Ahead** (other options: No Read Ahead, Adaptive Read Ahead)
- Write Policy: **Write Through** (other option: Write Back)
- Cache Policy: **Direct IO** (other option: Cache IO)
- Size(MB): **139236**

Step 11 Click **Next**.

The Summary screen appears displaying RAID array information.

Step 12 Click **Create Array**.

The Array Definition Complete screen appears with the message “Virtual Drive Created Successfully”.

Step 13 Click **Create Another Array**.

The Choose RAID Controllers screen appears.

Step 14 Click **LSI MegaRAID SAS 9261-8i (External)** and click **Next**.

Step 15 Click **Create custom or multiple RAID Arrays (advanced)** and click **Next**.

The Select Drives for Logical Drive screen appears.

Step 16 Select disks **2** through **9** and click **Next**.

The Define Array Attributes screen appears.

Step 17 Set the fields the following way:

- RAID Level: **5**
- Stripe size: **64k** (only option)
- Read policy: **Read Ahead** (other options: No Read Ahead, Adaptive Read Ahead)
- Write Policy: **Write Through** (other option: Write Back)
- Cache Policy: **Direct IO** (other option: Cache IO)
- Size(MB): **974652**

Step 18 Click **Next**.

The Summary screen appears displaying RAID array information.

Step 19 Click **Create Array**.

The Array Definition Complete screen appears with the message “Virtual Drive Created Successfully.”

Step 20 Click **Finish**.

The My Server screen appears.

Step 21 Eject the CD.

Installing VMware on the UCS Server

This section describes how to install VMware on the UCS C-210 M2 server. VMware ESXi 4.0, 4.1 or 5.0 are supported for this version of CTS-Manager on the UCS C-210 M2 server.

To install VMware on the UCS server:

Step 1 Insert the VMware Installer CD.

Step 2 Reboot the UCS server by doing either of the following:

- If RAID on your UCS server was preconfigured by Cisco: Reboot the UCS server.
- If you configured RAID on your UCS (following the steps in the previous section): In the My Server screen, click **Exit** and then click **OK** to confirm and reboot the UCS server.

The VMware screen appears.

Step 3 Wait for the bootup process to complete. Do not press any keys.

The bootup is complete when the VMware ESXi Installer screen appears with a welcome message.

Step 4 Press **Enter** to install VMware.

The End User License Agreement (EULA) screen appears.

Step 5 Press **F11** to accept the agreement and continue.

The Select a Disk screen appears displaying the installed disks and their size.

Step 6 Use the arrow keys to select the disk for the RAID 1 array and press **Enter**.

Note The RAID 1 array is the smaller of the two RAID arrays.

The Confirm Install screen appears.

Step 7 Press **F11** to start the installation.

The installation begins.

The installation is finished when the Installation Complete screen appears.

Step 8 Eject the VMware CD.

Step 9 Press **Enter** to reboot the UCS server.

When bootup is complete, the VMware ESXi screen appears with the message:

"Download tools to manage this host from:" followed by a URL.

Step 10 Press **F2** to customize the system.

The System Customization screen appears.

Step 11 Select Configure Password (selected by default) and press **Enter**.

The Configure Password screen appears.

Step 12 In the New Password field, enter a password and press **Tab**.

Step 13 In the Confirm Password field, re-enter that password and press **Enter**.

Step 14 Select **Configure Management Network** and press **Enter**.

The Configure Management Network screen appears.

Step 15 Select Network Adaptors (selected by default) and press **Enter**.

The Network Adaptors screen appears.

Step 16 Select the adaptor which is connected and press **Enter.**

Step 17 Select IP configuration and press **Enter**.

The IP Configuration screen appears.

Step 18 Select **Set Static IP address and network configuration**.

Step 19 Enter IP address, Subnet Mask and Default Gateway and press **Enter**.

Step 20 Select **DNS Configuration** and press **Enter**.

Step 21 The DNS Configuration screen appears.

Step 22 Select **Use the following DNS server addresses and hostname**.

Step 23 Enter Primary DNS Server and Hostname (including domain name) and press **Enter**.

Step 24 In the Configure Management Network window, press **Esc** to return to the System Customization window.

Step 25 Select Test Management Network and press **Enter**.

The Test Management Network screen appears.

Step 26 Press **Enter**.

The VMware software will attempt to ping your default gateway, DNS server and hostname. The test should display "OK" for each ping attempt.

Step 27 Press **Enter**.

The System Customization window appears.

Step 28 Log out of the VMware ESXi Installer by pressing **Esc**.

The VMware ESXi screen appears.

Step 29 Note the IP address displayed on this screen. You will use this IP address to download the VMware vSphere client to your PC to create your virtual machine in the next section.

Installing the VMware Client and Setting Up the Datastore

This section describes how to install the VMware vSphere Client and create the datastore for the CTS-Manager virtual machine. To complete this section, you must use a PC that is connected to the same network as your UCS server.

To install the VMware client and set up the datastore:

Step 1 From your PC, open a web browser and go to the IP address displayed on the VMware ESXi screen at the end of the previous section.

The VMware ESXi Welcome page appears.

Step 2 Click Download vSphere Client and follow the on-screen instructions to install the vSphere Client on your PC.

Note During the installation, you have the option of installing the vSphere Host Update Utility. You can install this, but it is not required.

Step 3 Open the VMware vSphere Client.

Step 4 Log in to the ESXi host on the UCS server using the following information:

- IP address / name: IP address of UCS server (used in step 1)
- User name: **root**
- Password: VMware password created during installation on the UCS server

A Security Warning window appears, indicating that an untrusted SSL certificate is installed.

Step 5 Click the checkbox for "Install this certificate and do not display any security warnings" and click **Ignore**.

A VMware Evaluation Notice window appears, indicating that you must upgrade your ESX Host license. The initial evaluation license expires 60 days after installation.

Step 6 Click **OK** to close the VMware Evaluation Notice window.

The vSphere Client window opens with the UCS server (identified by IP address) displayed in the left-hand side of the window.

The next step is to align the datastore on which you will set up the CTS-Manager virtual machine, which improves disk performance and prevents disk blocks from being fragmented.

Step 7 Click the **Summary** tab.

Step 8 In the Datastore area, right-click the datastore with the largest capacity and select **Delete**.

A confirmation window appears.

Step 9 Click **Yes** to confirm you want to delete the datastore.

In the Recent Tasks area at the bottom of the window, the Remove Datastore task appears.

Step 10 Wait for the task to display a status of "Completed."

Step 11 Click the **Configuration** tab.

Step 12 In the Hardware area on the left, click **Storage**.

In the Datastores area, the remaining datastore is displayed.

Step 13 In the upper right above the Datastores area, click **Add Storage…**.

The Add Storage window opens and the Select Storage Type screen is displayed.

Step 14 Select **Disk/LUN** (selected by default) and click **Next**.

The Select Disk/LUN screen appears.

Step 15 Click the **Local LSI Disk** and click **Next**.

The Current Disk Layout screen appears confirming the disk partition you will create.

Step 16 Click **Next**.

The Properties screen appears.

Step 17 Enter a name for your datastore and click **Next**.

The Disk/LUN Formatting screen appears.

Step 18 From the Maximum file size drop-down list, choose **256 GB, Block size: 1 MB** and make sure **Maximize Capacity** is checked.

Step 19 Click **Next**.

The Ready to Complete screen appears.

Step 20 Click **Finish**.

In the Recent Tasks area at the bottom of the window, the Create VMFS Datastore task appears.

Step 21 Wait for the task to display a status of "Completed."

After completion, you have two datastores. The datastore with the smaller capacity is the RAID 1 configuration, where the VMware software is installed, and the datastore with the larger capacity is the RAID 5 configuration, where you will deploy the virtual machine and install CTS-Manager.

Disabling LRO

When running VMware ESXi 4.0, 4.1 or 5.0 on the UCS server, you may experience slow TCP performance of the virtual machine. You can resolve this by disabling Large Receive Offload (LRO) on the ESXi host.

To disable LRO:

Step 1 Log into the ESXi host on the UCS server with the VMware vSphere Client (if not already logged in).

Step 2 Click the UCS server icon in the left-hand side of the window.

Step 3 Click the **Configuration** tab.

Step 4 In the Software section, click **Advanced Settings**.

Step 5 Select **Net** and scroll down slightly more than half way.

Step 6 Set the following parameters from 1 to 0:

- Net.VmxnetSwLROSL
- Net.Vmxnet3SwLRO
- Net.Vmxnet3HwLRO
- Net.Vmxnet2SwLRO
- Net.Vmxnet2HwLRO

Step 7 Right-click the UCS server and select **Reboot**.

Your virtual machine should now have normal TCP networking performance.

Creating the Virtual Machine

This section describes how to deploy the Open Virtualization Format (OVF) template for CTS-Manager to create the virtual machine on which to install the CTS-Manager software. OVF is a standard for packaging and distributing virtual machines. The OVF template streamlines the process of setting provided by Cisco contains all the virtual machine settings required for CTS-Manager.

To create the virtual machine:

Step 1 Download the OVF template from Cisco:

a. Go to: http://cisco.com/support

b. Click the **Downloads** tab

c. Click in the Find field, enter **Cisco TelePresence Manager** and click **Find**.

The Select a Product page appears.

d. Click the link for the **Cisco TelePresence Manager Release 1.9**.

The Download Software page appears.

e. Find **CTSMAN_1.9_v1.0.ova** and click **Download Now**.

f. Log in to Cisco.com (if required).

g. In the Download Cart page, click **Proceed With Download**.

The End User License Agreement page appears.

h. Click **Agree**.

i. Select one of the available download options.

j. Click the **Download** link.

Step 2 Log into the ESXi host on the UCS server with VMware vSphere Client (if not already logged in).

Step 3 Select **File > Deploy OVF Template**.

The Deploy OVF Template window opens.

Step 4 Select **Deploy from File**.

Step 5 Click **Browse**

Step 6 Select the OVF template that you downloaded and click **Open**.

Step 7 Click **Next**.

The OVF Template Details page appears.

Step 8 Click **Next**.

Step 9 Enter a name for your virtual machine and click **Next**.

The Datastore page appears.

Step 10 Click the datastore (with the largest capacity) that you created in the Installing the VMware Client and Setting Up the Datastore section and click **Next**.

The Ready to Complete page appears.

Step 11 Click **Finish**.

Step 12 When the OVF template is deployed successfully, the Deployment Completed Successfully window appears.

Step 13 Click **Close**.

Installing CTS-Manager

This section describes how to install CTS-Manager on the virtual machine you created and configured.

To install CTS-Manager:

Step 1 Insert the installer DVD into your PC (unless the you downloaded the software from Cisco.com).

Note If a CDROM window appears asking what you want Windows to do, click **Cancel**.

Step 2 Log into the ESXi host on the UCS server with VMware vSphere Client (if not already logged in).

Step 3 In the left-hand side of the window, click the virtual machine you created for CTS-Manager and click the **Console** tab.

Step 4 Right-click the CTS-Manager virtual machine and choose **Power > Power On**.

Step 5 On the toolbar, click the button with the CD and Wrench icon and wait for the menu to pop up.

Step 6 Choose **CD/DVD Drive 1 > Connect to D:** (or the letter associated with the drive in which you inserted the DVD).

Note If you downloaded the CTS-Manager software to your PC from Cisco.com, select **Connect to ISO image on local disk. . .**, select the CTS-Manager .iso file and click **Open**.

Step 7 Right-click the CTS-Manager virtual machine and select **Guest > Send Ctrl + Alt + del**.

The CTS-Manager virtual machine reboots.

After bootup, the installer startup process begins in the console window.

Step 8 Click inside the console window to make it active, so you can use your keyboard during the installation process.

Note After clicking in the console window, you can no longer use your mouse. This is normal behavior, because you cannot use the mouse in the console. If at any time you need to regain control of your mouse, press **Ctrl+Alt**. To make the console window active again, click in the console window.

Step 9 Follow the rest of the installation as detailed in Installing Cisco TelePresence Manager from DVD, page 9-3 of Chapter 9, “Installing or Upgrading Cisco TelePresence Manager.”

Step 10 After completing the installation, press **Ctrl+Alt** to exit the console window and regain control of your mouse.

Step 11 Close the VMware vSphere Client by selecting **File > Exit**.

Upgrading VMware Tools

This section describes how to upgrade the VMware tools which is required after installing CTS-Manager.

To upgrade VMware tools:

Step 1 Log into the ESXi host on the UCS server with VMware vSphere Client.

Step 2 Make sure the virtual machine for CTS-Manager is powered on.

Step 3 Right-click the CTS-Manager virtual machine, and choose **Guest > Install/Upgrade VMware Tools**.

Step 4 In the popup window that appears, choose **Automatic Tools Upgrade** and click **OK**.

Step 5 In the Recent Tasks area at the bottom of the vSphere Client window, wait for the VMware Tools Installer Mount to display a status of Completed.

Installing the VMware License Key

This section describes how to install the VMware software license key. After installation, the VMware software works for 60 days. Before the 60 days have elapsed, you must install a license key to continue using the software.

When you purchase ESXi 4.1/vSphere 5, you receive a licensing confirmation email with your license key. You can also retrieve your license key from the vSphere License portal at: http://downloads.vmware.com/licensing/license.portal

To install the VMware license key:

Step 1 Log in to the VMware vSphere Client.

The VMware vSphere Client opens and a VMware Evaluation Notice window appears.

Step 2 Click **OK** to close the VMware Evaluation Notice window.

Step 3 Click the VMware host icon at the top of the left-hand column of the vSphere Client window.

Step 4 Click the **Configuration** tab.

Step 5 In the Software area in the middle-left side of the vSphere Client window, click **Licensed Features**.

The Licensed Features information for the ESX Server License Type appears.

Step 6 In the upper-right part of the window, click **Edit**.

The Assign License window appears.

Step 7 Click **Assign a new license key to this host** and click **Enter Key**.

Step 8 The Add License Key window appears.

Step 9 Enter the license key you received from VMware and click **OK**.

Step 10 Click **OK** again to close the Assign License window.

Setting Automatic Startup for CTS-Manager

You can configure your CTS-Manager virtual machine to automatically start when the UCS server is started. The advantage of enabling Automatic Startup is that in the event of a power outage, you only need to start up the UCS server to get CTS-Manager up and running again.

To set Automatic Startup for CTS-Manager:

Step 1 Log in to the VMware vSphere Client.

Step 2 Click the VMware host in the left side of the vSphere Client window to select it.

Step 3 Click the **Configuration** tab.

Step 4 In the Software area in the middle-left side of the vSphere Client window, click **Virtual Machine Startup/Shutdown**.

The Virtual Machine Startup and Shutdown information appears.

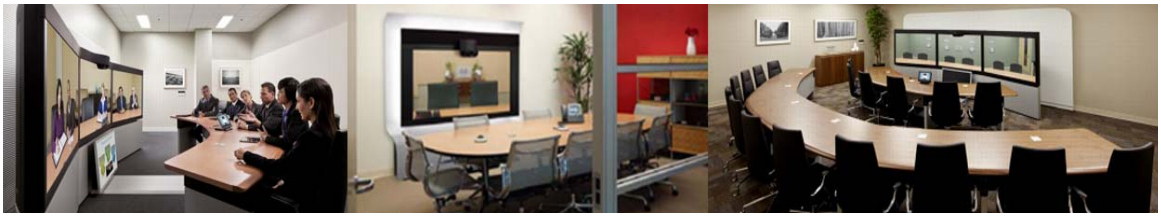
Step 5 In the upper-right part of the window, click **Properties**.

The Virtual Machine Startup and Shutdown window appears.

Step 6 Check **Allow virtual machines to start and stop automatically with the system**.

Step 7 Select the CTS-Manager virtual machine in the table and move it up to the Automatic Startup section.

Step 8 Click **OK**.



CHAPTER 9

Installing or Upgrading Cisco TelePresence Manager

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

Contents

- Introduction, page 9-1
- Installation Guidelines, page 9-2
- Installing Cisco TelePresence Manager from DVD, page 9-3
- Installation Procedure for Cisco TelePresence Manager, page 9-3
- Required Information and Equipment, page 9-3
- Recovering Administrator and Security Passwords, page 9-7
- System Log Error Detection, page 9-8
- Software Upgrade, page 9-10
- Upgrading to Cisco TelePresence Manager 1.9, page 9-11
- Cisco TelePresence Manager Window, page 9-19
- Preferences, page 9-22

Introduction

This chapter explains how to install the Cisco TelePresence Manager software in your network. After completing this installation, you will be able to schedule Cisco TelePresence meetings through existing Microsoft Outlook or Lotus Notes software, receive reminders, and connect to a remote meeting 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 communicate with your network. The purpose of this chapter is to walk you through each step using the Cisco TelePresence Manager installation DVD.

The installation requires information about your network and the rules for finding and exchanging information. Once this pre-installation data is set up, then you can install Cisco TelePresence Manager from DVD. In addition, you can use the Configure > Software Upgrade window to upgrade the system software.

Installation Guidelines

The purpose of this section is to provide the information you need in order to install the CTS-Manager software.

The tasks required to install and configure CTS-Manager are provided in the following table.

Table 9-1 Installation Overview for CTS-Manager

Setup Procedures	Description	Location
Installing or Upgrading Cisco TelePresence Manager		Current Chapter.
Initializing CTS-Manager	After installing the CTS-Manager software, the next process is to initialize 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 (endpoint) information, and Cisco Unified Communications Manager for conference room (endpoint) availability and telephone support	Chapter 10, "Initializing Cisco TelePresence Manager"
Additional Installation Procedures for CTS-Manager	The administrator makes use of the Configure section to perform system configuration tasks such as synchronizing system databases, managing security, and reconfiguring system settings	Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager"
Configuring Cisco TelePresence WebEx OneTouch for CTS-Manager	Describes how to set up Cisco TelePresence WebEx OneTouch in CTS-Manager, which allows WebEx participants to join TelePresence meetings.	Chapter 12, "Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager"
Next Step after Pre-Configuration		
Monitoring CTS-Manager	Monitoring and updating meeting schedules and monitoring the status of rooms (endpoints) and system services	Chapter 13, "Monitoring and Supporting Cisco TelePresence Manager"

Installing Cisco TelePresence Manager from DVD

The following section provides installation procedures for CTS-Manager.

Required Information and Equipment

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

- The Model 7845 Cisco Media Convergence Server or UCS C-210 M2 server included with Cisco TelePresence Manager, installed and connected to a Domain Name System (DNS) server and your network.
- DNS configuration for both forward and reverse name resolution is required for all servers configured in CTS-Manager, so that all server names can be resolved bidirectionally by DNS. This includes the server name for CTS-Manager itself.
- The information listed in Table 9-2 “Installation Window and Field Definitions” that includes your system-specific values and parameters.
- A management console 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.
- Endpoint license. If you do not have this license, you will not be able to add TelePresence endpoints to CTS-Manager. After installation and initialization, the SysAdmin must go to the Configure > Licenses window and click the License Files tab to upload the license.

Installation Procedure for Cisco TelePresence Manager

Step 1 Insert the CTS-Manager installation DVD into the DVD drive of the server and boot up 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.

Note Cisco recommends using the default selections (which are highlighted by a grey box). For example, on the DVD Found screen that appears after inserting the DVD, “Yes” is the default selection.

Caution Remove the DVD 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 When the DVD Found screen appears, select **Yes** to perform a media check of the DVD, or **No** to abort the installation.

Step 3 Once the media check passes, click **OK** to proceed.

The Product Deployment Selection screen appears, indicating Cisco TelePresence Manager suite will be installed.

Step 4 Click **OK** to proceed.

The installer checks for a prior installation of CTS-Manager software.

Step 5 If you choose **Yes** to continue the installation, the Platform Installation Wizard opens in the next window. Read and become familiar with the wizard conventions.

Step 6 Select **Proceed**.

Step 7 Fill in each window with the information defined in Table 9-2, "Installation Window and Field Definitions".

Step 8 When you are satisfied that the information is correct, click **OK** in the Platform 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.

Step 9 Proceed to Chapter 10, "Initializing Cisco TelePresence Manager," to initialize Cisco TelePresence Manager.

Installation Page Values Defined

Table 9-2 explains in detail the window and field definitions of the Cisco TelePresence Manager installation process in detail.

Table 9-2 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.
Apply Patch	
Yes:	Applies upgrade patch from the DVD as part of the installation.
No:	Proceeds with install without installing upgrade patch.
Back:	Goes back to previous screen.
Basic Install	
Continue	Proceeds with installation without importing any data.
Time zone Configuration	
OK	Proceeds with installation using the selected time zone.
Back	Goes back to the previous screen.

Table 9-2 Installation Window and Field Definitions (continued)

Installation Windows and Fields	Description and Usage
Help	Provides additional information about selecting time zones.
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.
MTU Configuration	
	This screen gives you the option to change the Maximum Transmission Unit (MTU). This is the size of the largest packet that a network protocol can send. It is recommended to use the default of 'No.'
DHCP Configuration	
	This screen gives you the option to choose DHCP to run on CTS-Manager. It is recommended to select the default of 'No.'
Status Network Configuration	
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).
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	

Table 9-2 Installation Window and Field Definitions (continued)

Installation Windows and Fields	Description and Usage
	This screen gives you the option to enable DNS for CTS-Manager. It is recommended to select the default of 'Yes.'
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. **Note** If you have a DNS server, Cisco requires 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.
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.
Administrative Login Configuration	
Admin ID	The username for the CTS-Manager Administrator. This is the administrator login that includes SysAdmin 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. **Note** The password cannot be changed until at least 24 hours after it was created, unless you reinstall CTS-Manager. **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.

Table 9-2 Installation Window and Field Definitions (continued)

Installation Windows and Fields	Description and Usage
Certificate Information	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 IP address of one or more NTP server. • NTP Servers 1 and 2 values are mandatory; NTP Servers 3–5 are optional. **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 will not operate properly.
NTP Servers 2–5	
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.
SMTP Host Configuration	Selecting **Yes** enables Simple Mail Transfer Protocol so CTS-Manager can send emails to meeting organizers or the SysAdmin.
Application User Configuration	Create an Application User name and password for logging in to the CTS-Manager administrative web pages.

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.

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

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 Messages

Go to Troubleshoot > System Messages to see a list of system messages. You can filter the list by starting and ending dates and message type All, Emergency, Alert, Critical, Error, Warning, Notice, Info and Debug as follows:

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

Figure 9-1 System Messages Window

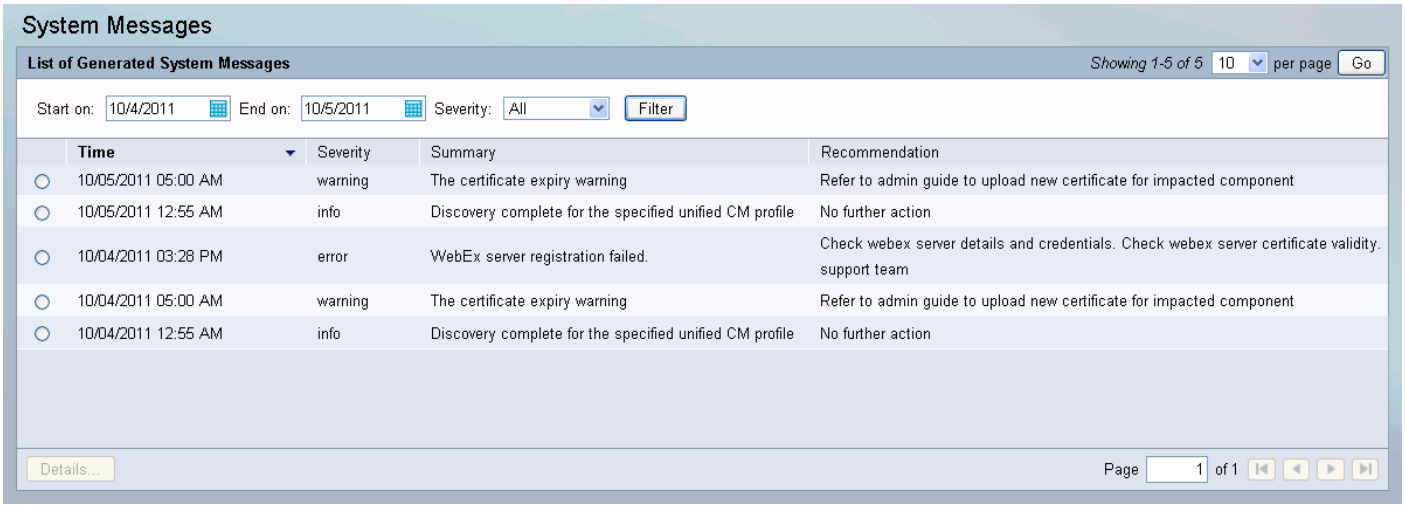


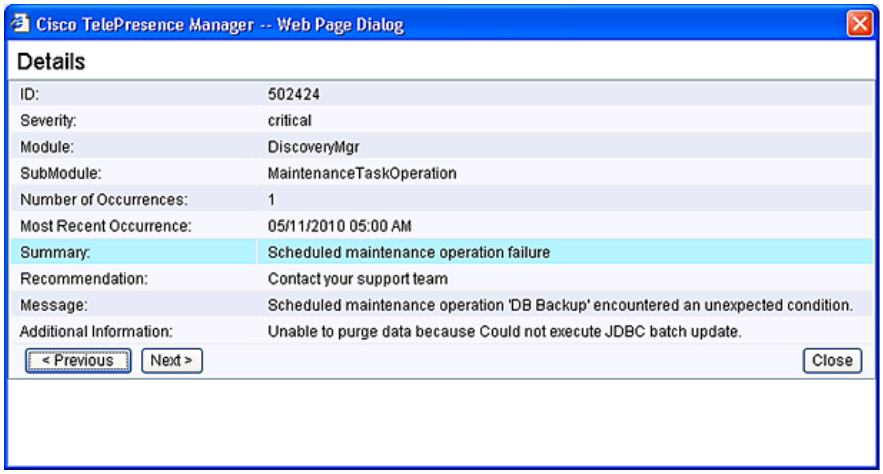
Table 9-3 lists the messages provided by the system.

Table 9-3 System Messages

Field	Description
Time(+)	Date and time the message was logged. You can sort the messages in ascending or descending order by the time stamp.
Severity	Message type.
Summary	Explanation of problem detected. Message identification number. You can sort the reports in ascending or descending order by ID.
Recommendation	Recommended course of action

To view the details of a system message, click its corresponding radio button and then click the **Details** button.

Figure 9-2 System Messages > Details Window



System Error - AXL Error or Invalid Credential

If the System Messages > Details message in the Syslog appears 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 6, "Configuring Cisco Unified Communications Manager for Cisco TelePresence Manager" to review what services need to be running on the Cisco UCM for CTS-Manager.

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 16, "Troubleshooting Cisco TelePresence Manager"

Software Upgrade

If you are the system administrator and know the SysAdmin password, you can access the Software Upgrade window to monitor and maintain system software by going to Configure > Software Upgrade. This window displays the version number of the system software. There are also two buttons to assist you in version maintenance between primary (active) and backup (inactive) and upgrading the system software, as follows:

Figure 9-3 Configure > Software Upgrade Window

- Switch Versions—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.

Note After successfully upgrading from CTS-Manager 1.7 or 1.8 to 1.9, the status message in the Most Recent Upgrade Attempt section, will display "Software versions switched" instead of "Upgrade completed sucessfully".

Note Secure FTP (SFTP) is the recommended mode for downloading the upgrade software over the network.

Caution For the upgrade to be successful, the NTP server(s) specified in the Configure > System Settings > NTP tab must be an IP address.

Upgrading to Cisco TelePresence Manager 1.9

Important notes about upgrading to CTS-Manager 1.9:

- Switching calendar application type, e.g. changing from Exchange to Domino, during upgrade is not supported. A fresh install is required to install Cisco TelePresence Manager to switch to Domino deployment.
- Software upgrade is only supported from CTS-Manager 1.7.x, and 1.8x.
- Data is automatically migrated during software upgrade, with the following exceptions:
  - 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.
- Make sure you have an endpoint license before you upgrade to CTS-Manager 1.9. If you do not have this license, you will not be able to add TelePresence rooms (endpoints) to CTS-Manager. After upgrade, the SysAdmin must go to the Configure > Licenses window and click the License Files tab to upload the license.
- After successfully upgrading from CTS-Manager 1.7 or 1.8 to 1.9, the upgrade status displays "Software versions switched" instead of "Upgrade completed successfully."

Note In rare instances, upgrades could take up to 5 hours or more. Please allow ample time and do not assume that the system has frozen during upgrades. Do not reboot.

Switch Versions

The hard drive on the CTS-Manager server is divided into two partitions. CTS-Manager is always using the software on the Active partition, while the other partition always contains the previous software version. The software image versions are identified in the Configure > Software Upgrade window.

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

- To switch between the software versions stored on the two 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 network host. Before starting this task, determine the source of the patch file.

To upgrade the CTS-Manager software:

Step 1 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.

Step 2 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 are required to log into the server.
- **Storage Path**—The file path to the patch file, e.g. */localview/ctm_patch*

Caution Performing FTP for Upgrade, Backup and Restore is provided 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 9-4 Software Upgrade - Source Selection Window

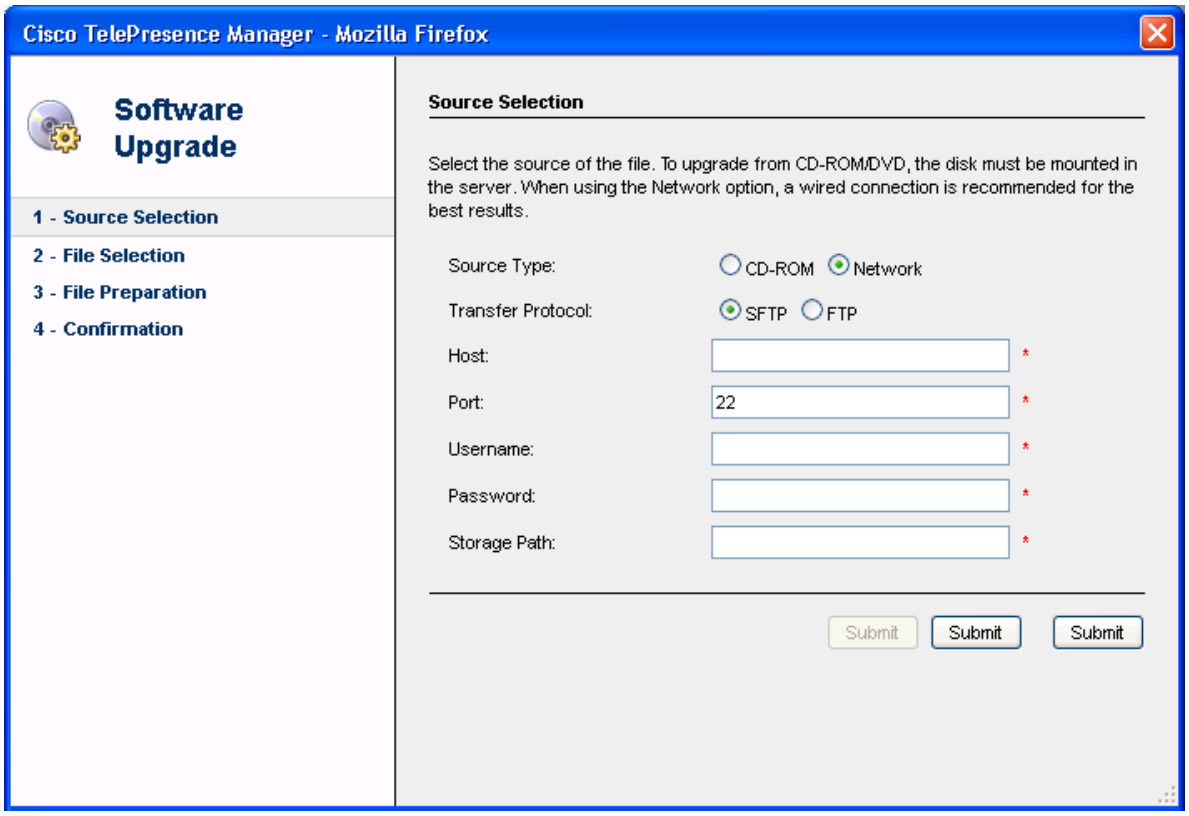
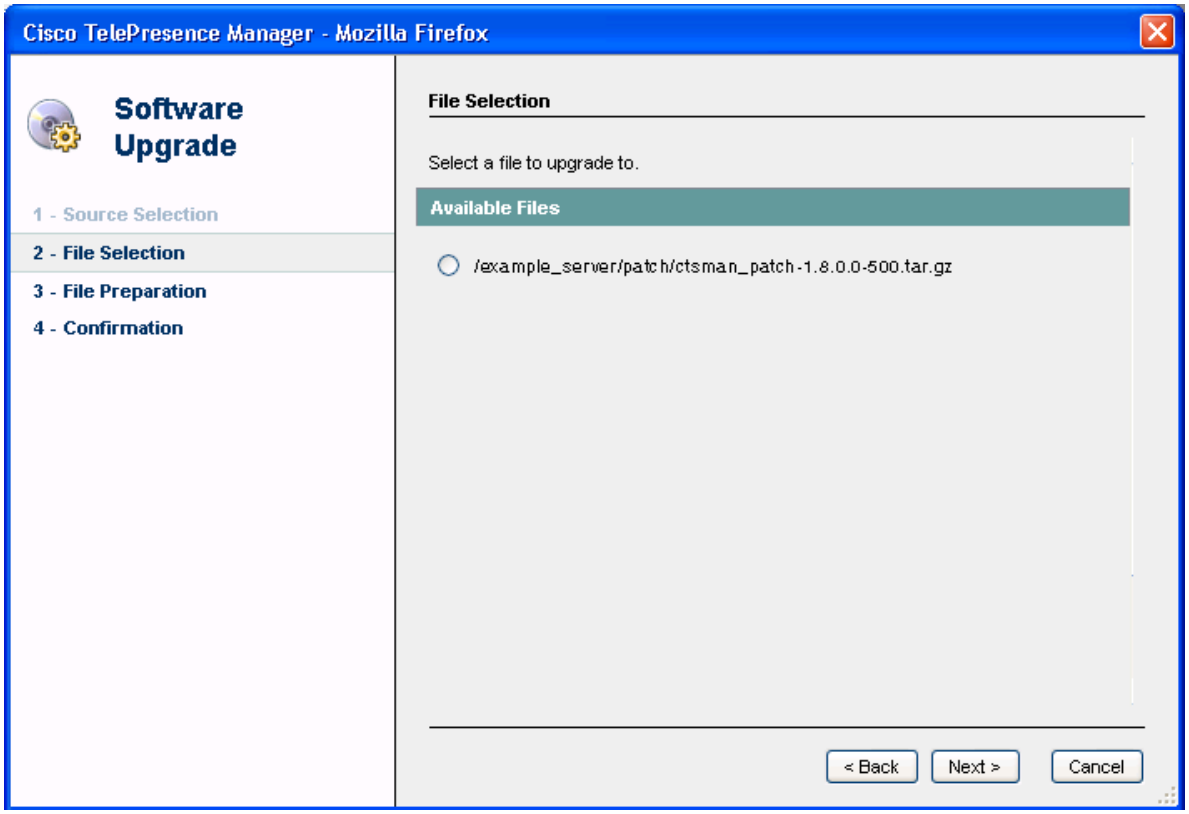
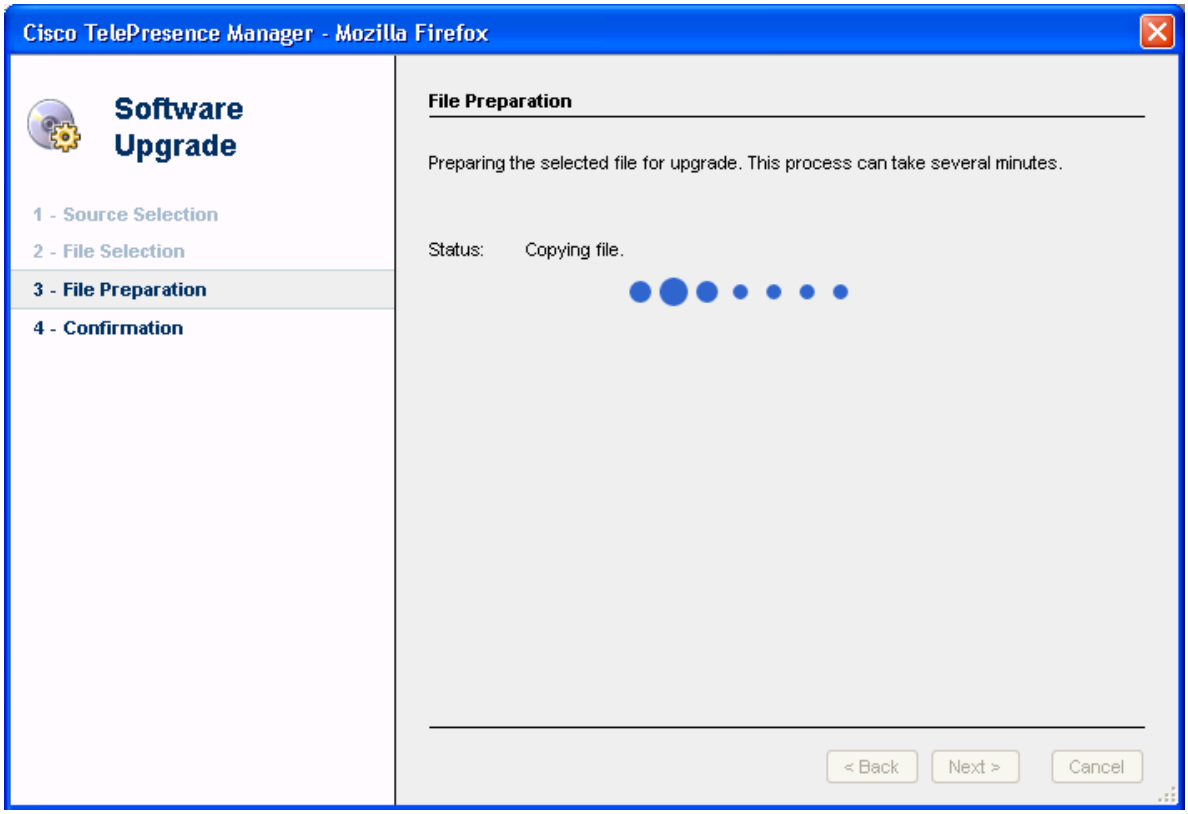


Figure 9-5 Software Upgrade - File Selection window



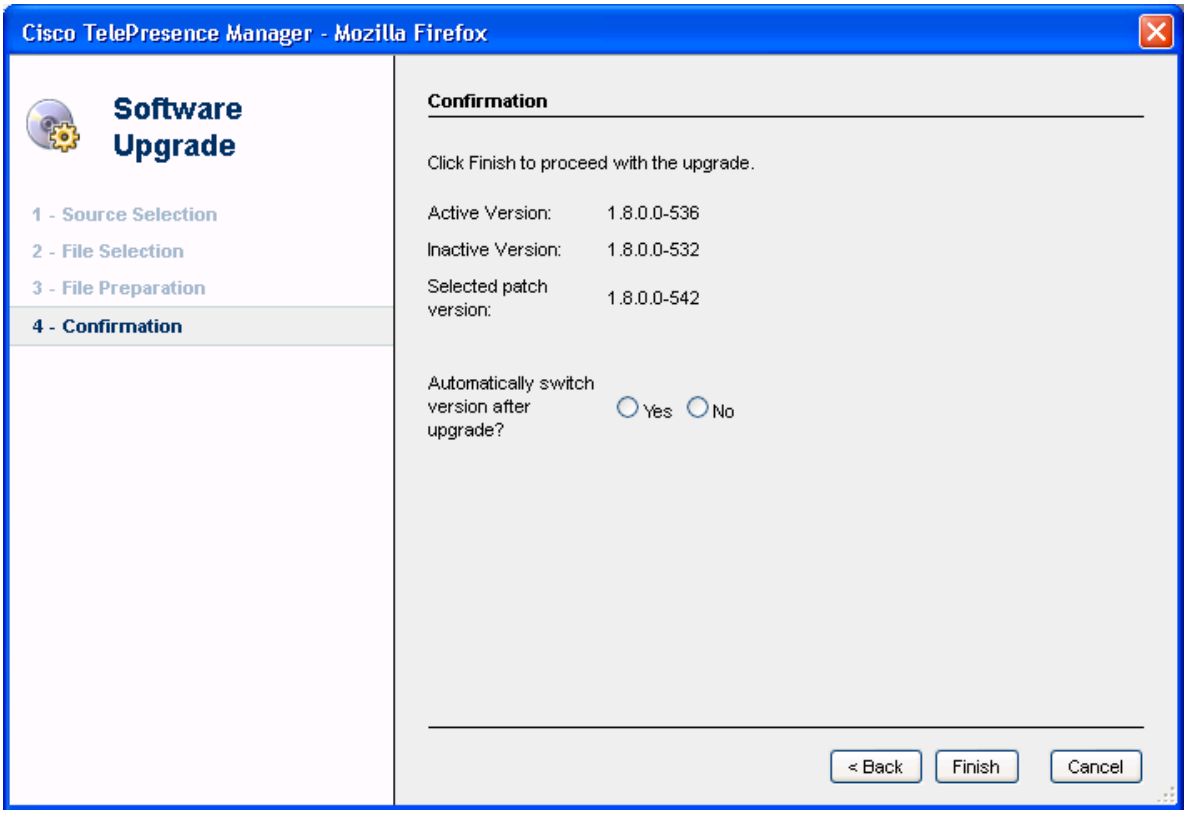
Step 3 In the File Selection page, choose the file to load by clicking its radio button. Then click **Next**.

Figure 9-6 Software Upgrade - Patch File Preparation 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.Once the file is loaded, the window displays a Confirmation message.

Figure 9-7 Software Upgrade - Confirmation Window



The software upgrade 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.

Step 4 Click **Yes** or **No** to make your choice and then click **Next** to finish the software upgrade task. A confirmation dialog box appears.

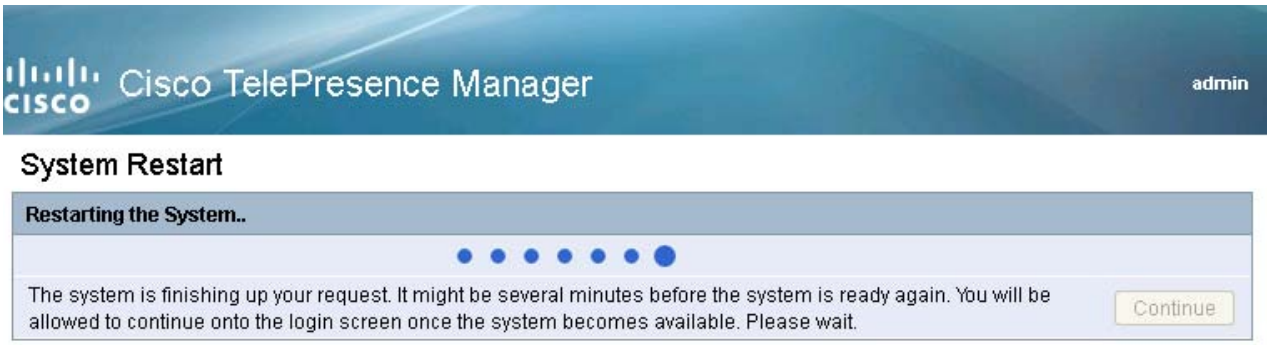
Note If you select Yes, the current active version will become the inactive version after upgrade is complete.

Step 5 Click **Finish** to proceed with the upgrade.

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

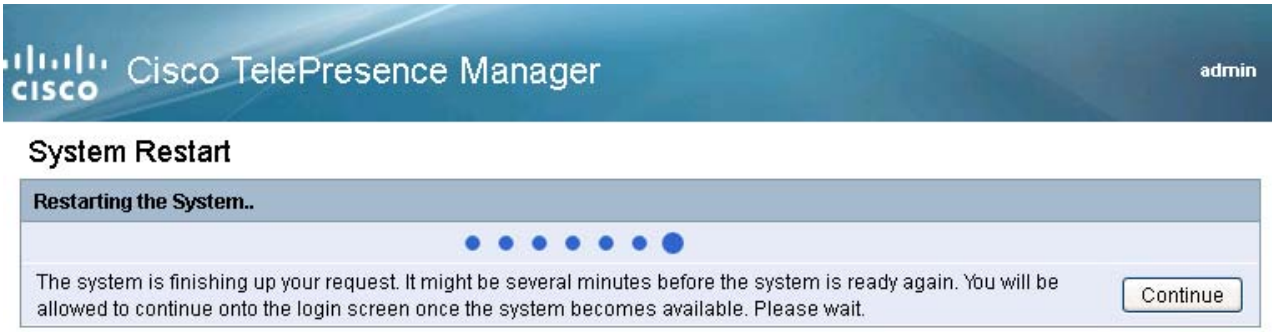
The software upgrade wizard closes revealing the Software Upgrade window in CTS-Manager. A progress indicator is displayed on the screen to show the upgrade is in progress. The Status field displays the current step being completed. When the final step is completed, CTS-Manager restarts.

Figure 9-8 Software Upgrade - CTS-Manager Restarting



While CTS-Manager is restarting, the Continue button is greyed out.

Figure 9-9 Software Upgrade - CTS-Manager Upgrade Completed Window



When CTS-Manager is restarted, the Continue will no longer be greyed out.

Step 6 Click **Continue** to go to the CTS-Manager login screen and log in to CTS-Manager.

If you are upgrading from release 1.6 of CTS-Manager, the SysAdmin must upload licenses to enable the license-based features. The Endpoint (Room) license is required in order to schedule TelePresence meetings.

Go to Licensing for CTS-Manager, page 11-6 for more information.

Figure 9-10 Software Upgrade - CTS-Manager Login Window

Cisco TelePresence Manager Window

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

Header Pane

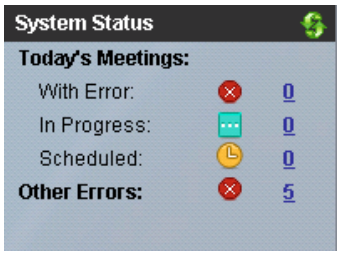
Figure 9-11 Cisco TelePresence Manager Header Pane

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

- **Preferences**—Display the Browser’s location information.
- **Log Out**—Log out of the system.
- **About**—Display licensing information.
- **Help**—Display online help for CTS-Manager.

System Status Pane

Figure 9-12 System Status Pane



System Status is always in view in the lower left corner of the CTS-Manager window. Both the Live Desk 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

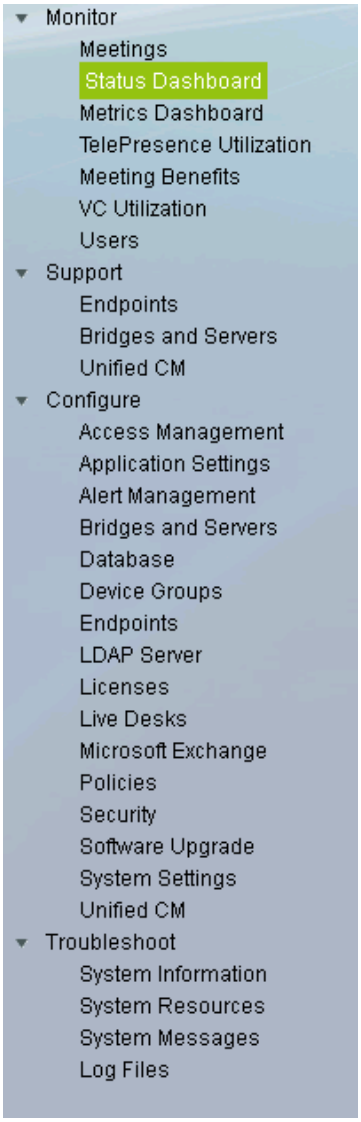
The Other Errors area displays a cumulative number of errors listed in the Dashboard.

Navigation Pane

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

- **Monitor**— This drop-down list contains commands available to a Live Desk, Administrator, or SysAdmin.
- **Support** — This drop-down list contains commands available to a Live Desk, Administrator, or SysAdmin.
- **Configure** — This drop-down list contains commands available to an Administrator or SysAdmin. If you log in as a SysAdmin the System Settings and Software Upgrade commands are included in the list.
- **Troubleshoot**— This drop-down list contains commands available to an Administrator or SysAdmin.

Figure 9-13 Navigation Pane



Work Pane

Figure 9-14 Work Pane

The frame to the right of the Navigation pane is the work 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.

Entering Information in Fields

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

Entering 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`**.

Entering Meeting Room (Endpoint) Names

The names of meeting rooms (endpoints) must be entered into CTS-Manager fields exactly as they are stored in your Microsoft Exchange, or IBM Domino database. If an endpoint is listed as **`M-Room 1/3 at Main`** in the Microsoft Outlook or Lotus Notes list of resources, that name must be entered 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

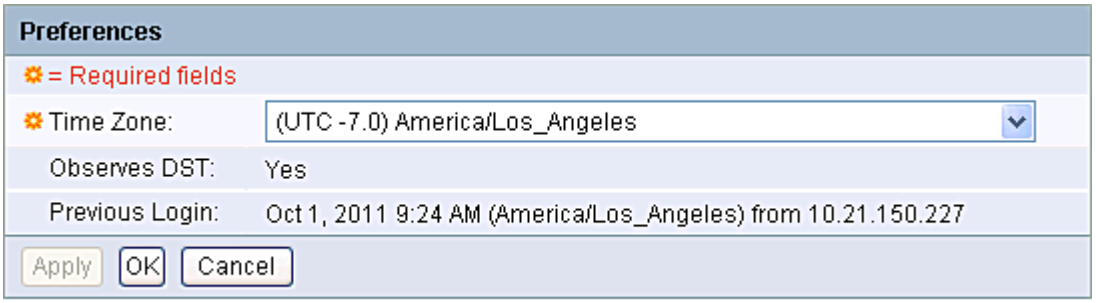
Clicking Preferences in the header pane displays the Preferences window.

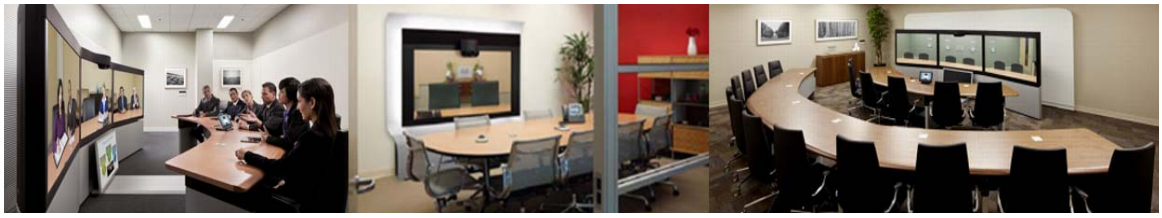
Figure 9-15 Preferences Link in the Header Pane

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

Note The time zone setting in the Preferences window is for the user only and does not affect the time zone setting of the CTS-Manager server, which is configured during installation.

Figure 9-16 Preferences window





CHAPTER 10

Initializing Cisco TelePresence Manager

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

Content

- Introduction, page 10-1
- Post-Install Guidelines for CTS-Manager, page 10-2
- Initializing CTS-Manager After Installation, page 10-3
- Required Information and Equipment, page 10-3
- Initialization Procedure, page 10-4
  - Log In and Set Time Zone, page 10-4
  - Select Configuration Options, page 10-5
  - Select Calendar Server, page 10-9
  - Configure LDAP Servers, page 10-10
  - Configure Unified CM, page 10-14
  - Configure Calendar Server, page 10-15
  - Configure Database Backup Schedule, page 10-19
- Dashboard for Verification of Installation Status, page 10-21

Introduction

After a first-time or fresh installation of Cisco TelePresence Manager, the next step is to initialize the program.

Note If you have upgraded to Cisco TelePresence Manager 1.9, you do not initialize the program but you must install an endpoint license. Without this license, your configured endpoints will not be recognized and you will not be able to schedule meetings. For more information, go to Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager".

Initializing Cisco TelePresence Manager enables access to information sources such as Microsoft Exchange Server for meeting requests from Microsoft Outlook, Active Directory for accessing user and conference room (endpoint) information, and Cisco Unified Communications Manager for room (endpoint) 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 section is to outline the information you need to initialize CTS-Manager after either a fresh or first-time installation.

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

Table 10-1 Post-Install Procedure Guidelines for Setting Up CTS-Manager

Setup Procedure Guidelines after Installing CTS-Manager	Description	Location
Initializing CTS-Manager	After first-time installation of the CTS-Manager software, the next process is initializing CTS-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 (endpoint) information, and Cisco Unified Communications Manager for conference room (endpoint) availability and telephone support	Current Chapter
Additional Configuration Procedures for CTS-Manager	The administrator makes use of the System Configuration window to perform system configuration tasks such as uploading licenses, synchronizing system databases, managing security, and reconfigure system settings	Chapter 11, “Additional Installation Configurations for Cisco TelePresence Manager”
Configuring Cisco TelePresence WebEx OneTouch for CTS-Manager	Describes how to set up Cisco TelePresence WebEx OneTouch in CTS-Manager, which allows WebEx participants to join TelePresence meetings.	Chapter 12, “Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager”

Table 10-1 Post-Install Procedure Guidelines for Setting Up CTS-Manager (continued)

Setup Procedure Guidelines after Installing CTS-Manager	Description	Location
Monitoring and Supporting CTS-Manager	Describes the support features available when you log into CTS-Manager using a Live Desk role.	Chapter 13, "Monitoring and Supporting Cisco TelePresence Manager"
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 (endpoints) 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 14, "Meeting Manager and CTS-Manager Emails"

If at any time you encounter problems, go to Chapter 16, "Troubleshooting Cisco TelePresence Manager" to see how to correct the problem.

Initializing CTS-Manager After Installation

This section contains the following topics pertaining to initialization:

- Required Information and Equipment, page 10-3
- Initialization Procedure, page 10-4

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 Internet 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.

You must also have an endpoint license in order to fully initialize CTS-Manager. If you do not have this license, you will not be able to add rooms (endpoints) to CTS-Manager. After installation and initialization, go to the Configure > License window and click the License Files tab to upload the license.

Initialization Procedure

To initialize CTS-Manager, follow these steps:

1. Log In and Set Time Zone, page 10-4
2. Select Configuration Options, page 10-5
3. Select Calendar Server, page 10-9
4. Configure LDAP Servers, page 10-10
5. Configure Unified CM, page 10-14
6. Configure Calendar Server, page 10-15
7. Configure Database Backup Schedule, page 10-19

Log In and Set Time Zone

To log in and set your time zone:

Step 1 Using Microsoft Explorer, go to the Cisco TelePresence Manager server name or IP address. See the following example.

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

Step 2 At the product page that appears, click **Cisco TelePresence Manager**.

Step 3 At the login page, enter the SysAdmin username and password and click **Log In**.

Note SysAdmin username and password are the Administrator ID and password that were created during installation of CTS-Manager.

The Time Zone Setting window appears.

Figure 10-1 Timezone Setting Window

Step 4 Select your location and locale using the drop-down menus and click **Continue**.

A window pops up asking you if you want to apply changes.

Step 5 Click **OK**.

The first-time setup welcome window appears displaying the following information about the CTS-Manager server hardware and software you have installed:

- SKU
- Hostname
- IP Address
- Subnet Mask
- MAC Address
- Hardware Model
- Software Versions
- OS Version

Step 6 Click **Next**.

The License Agreement window appears.

Step 7 Review the license agreement and check the check box next to I **accept the terms of the license agreement**.

Step 8 Click **Next**.

Step 9 The Server Roles window appears.

Server Roles

The Server Roles window allows you to choose how you want to deploy the CTS-Manager server.

The options are:

- A standalone server

  Choose this to set up CTS-Manager as a standalone server to manage up to 500 endpoints.

- A server in a cluster

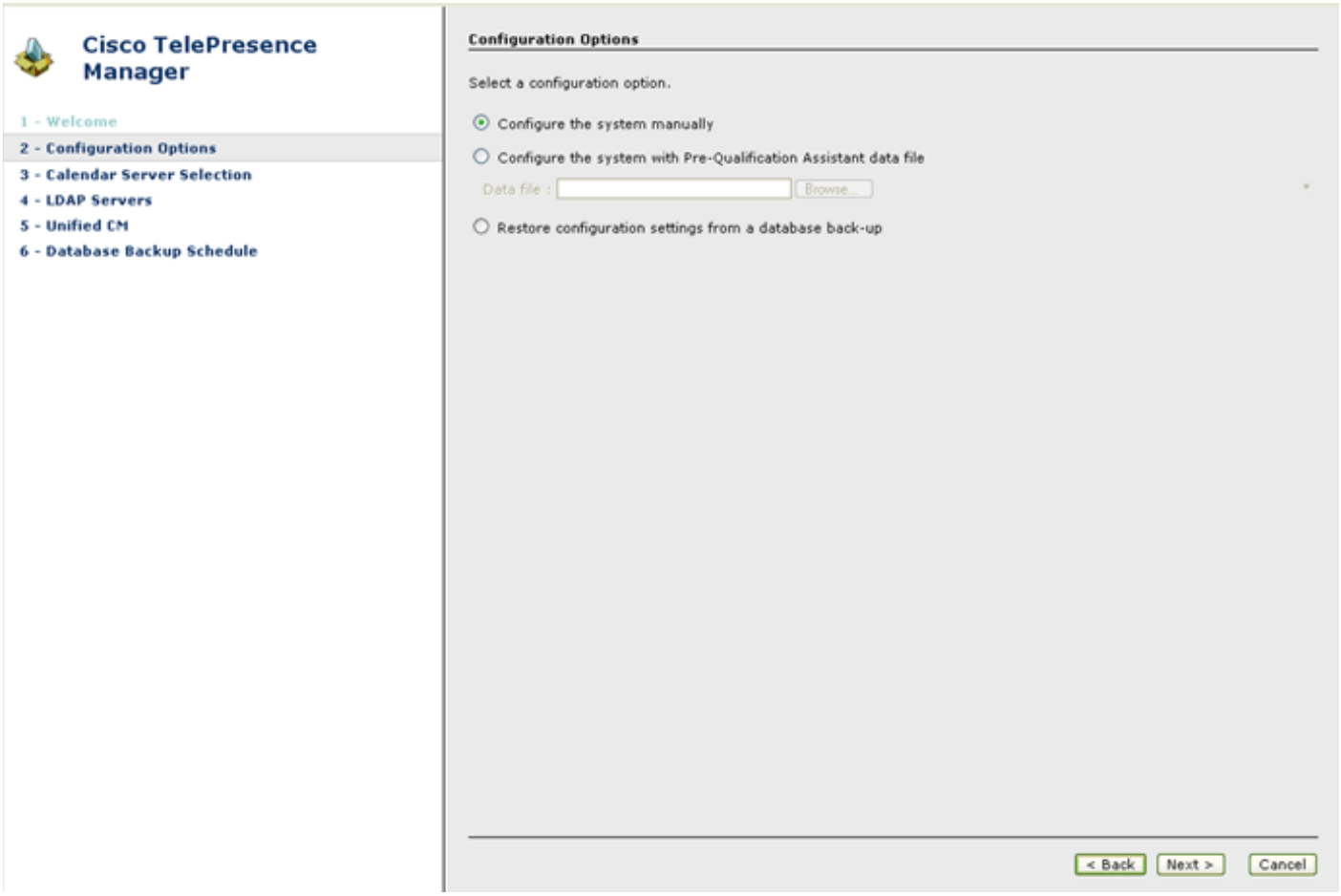
  Cisco no longer provides support for the clustering feature originally introduced in release 1.8. For questions, contact Ron Lewis: ronlewis@cisco.com.

Select a server role and click **Next**.

Select Configuration Options

The Configuration Options window allows you to configure the system manually or to restore the configuration settings from a database backup.

Figure 10-2 Configuration Options Window - Manual Configuration



The Configuration Options window provides three options for configuring CTS-Manager:

- Configure the System Manually, page 10-6
- Configure the System with PreQualification Assistant Data File, page 10-7
- Restore Configuration Settings from a Database Backup, page 10-8 (Not available for Commercial Bundle)

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 PreQualification data files.

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

If you are setting up Microsoft Exchange as your calendar server for the first time:

- Select **Configure the system manually** and click **Next**.

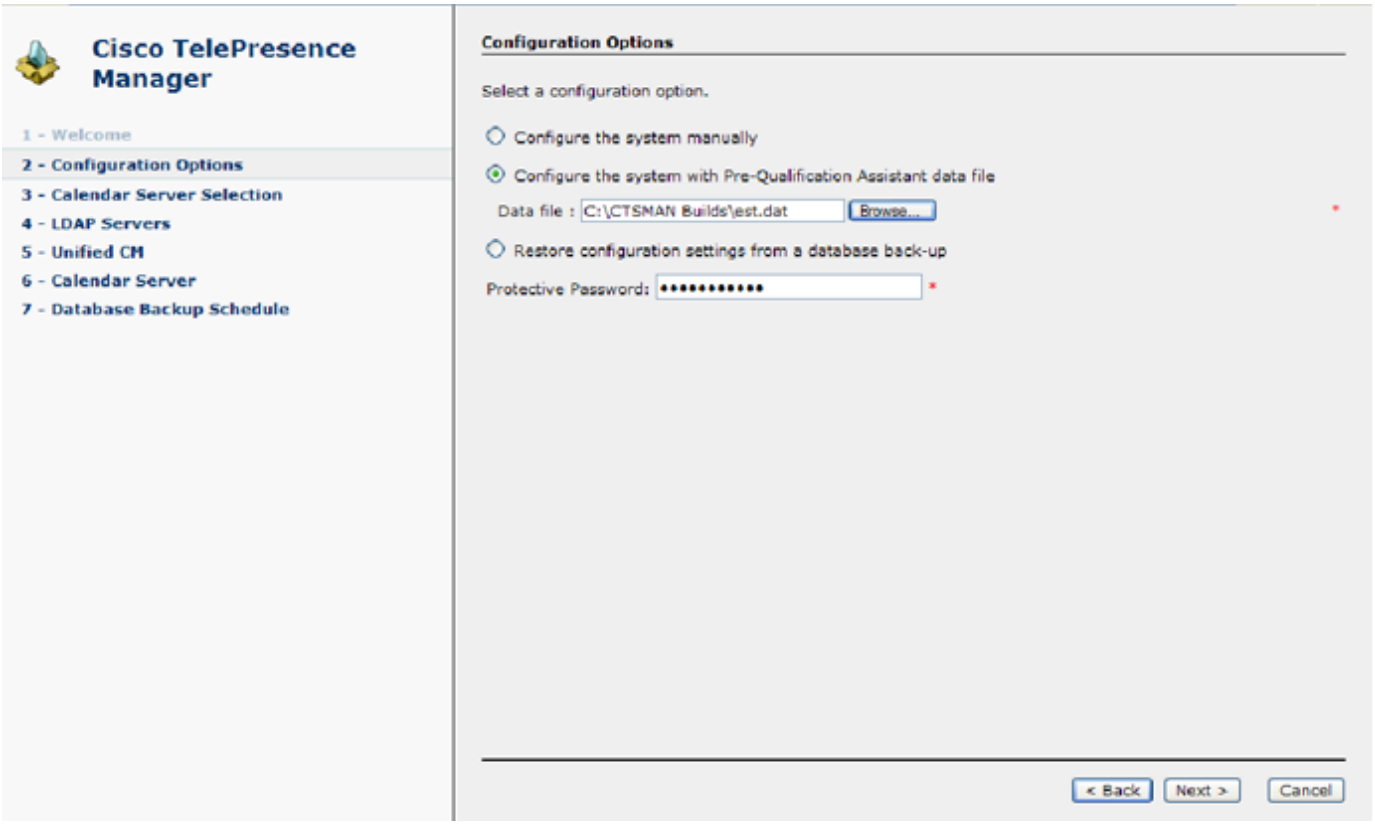
The Calendar Server window appears.

Go to Select Calendar Server, page 10-9 for more information

Configure the System with PreQualification Assistant Data File

If you choose to configure CTS-Manager using the PreQualification data, this option allows you to select the data file that you have previously set up. Refer to Chapter 7, "Installing and Configuring Cisco PreQualification Assistant"

Figure 10-3 Configuration Options - PreQualification Configuration



To configure the system using the Pre-Qualification Assistant data file:

Step 1 Click **Browse**, select the data file, and click **Open**.

Step 2 Enter the password you created when you exported the file from the PreQualification Assistant.

Step 3 Click **Next**.

The Calendar Server Selection window appears.

Go to Select Calendar Server, page 10-9.

Note If this option is selected, it is necessary to test the LDAP servers connections through the PreQualification Assistant.

Restore Configuration Settings from a Database Backup

This option allows you to select the data that you have previously backed up. Refer to Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager", section, Database - Status, Backup, and Restore for further details on backing up your system database.

Note This option is not available with the commercial bundle of CTS-Manager.

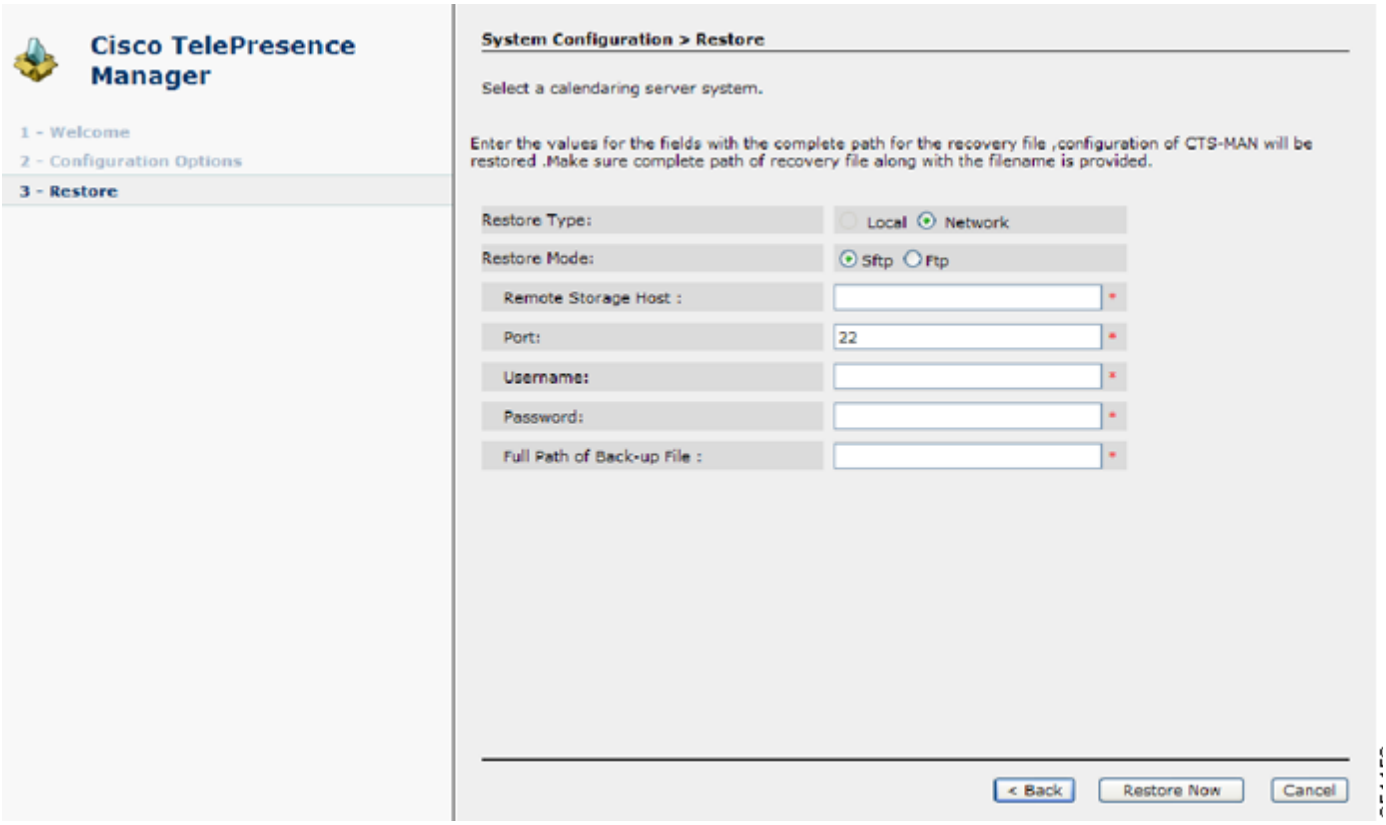
To restore configuration settings from a database backup:

Step 1 Select the **Restore configuration settings from a database backup** option and click **Next**.

Step 2 The Restore window appears.

Step 3 Fill in the fields by providing the path of the recovery file and the filename.

Figure 10-4 System Configuration - Restore Window



Step 4 After filling in the details, click the **Restore Now** button. The backup data is restored to the CTS-Manager server.

After selecting the configuration option and setting up the data, the next step is to set up the calendar server. Go to Select Calendar Server, page 10-9.

Select Calendar Server

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

- Microsoft Exchange
- MS Exchange Web Services (EWS)
- IBM Domino
- Scheduling API
- No Calendaring Service

To select a calendar server:

Step 1 Select a calendar server from the displayed options.

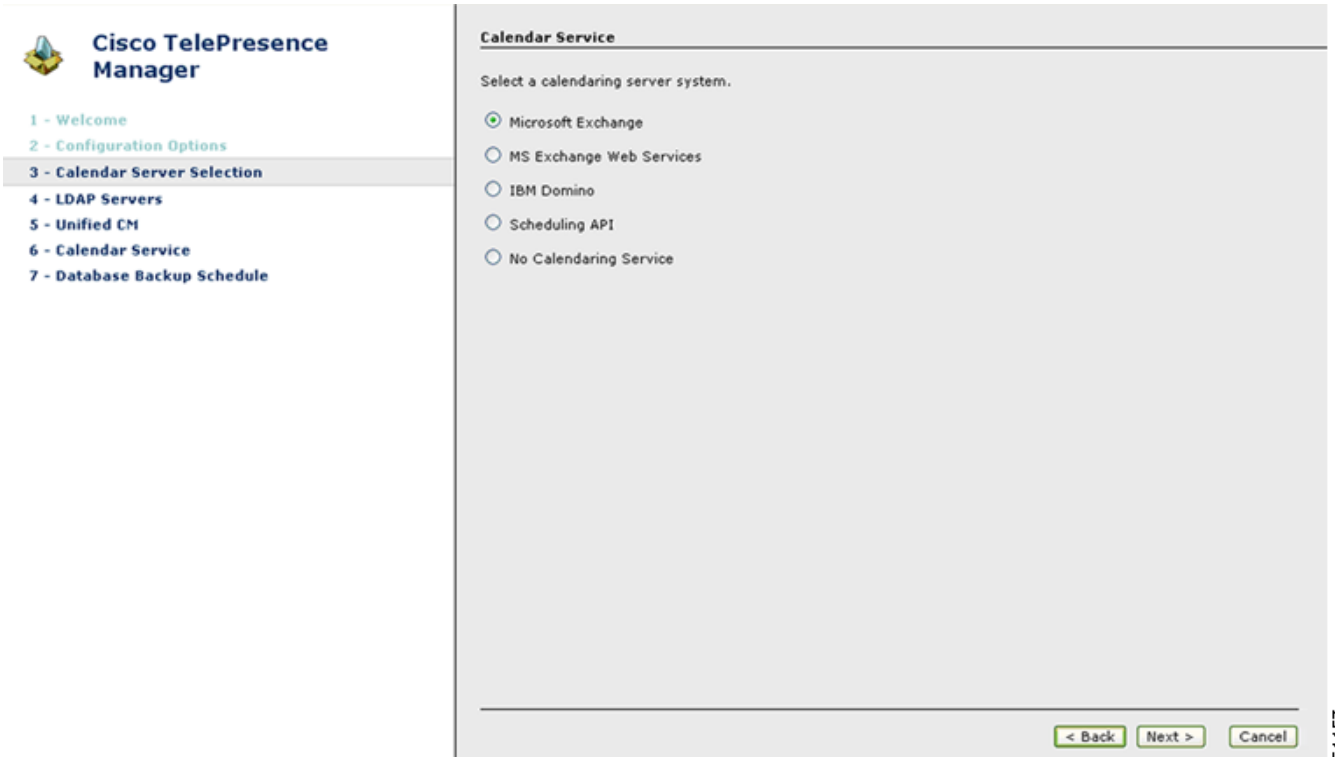
Note If you choose Scheduling API, review the license agreement and check the check box next to **I accept the terms of the license agreement**.

Step 2 Click **Next**.

The LDAP Servers window opens.

Go to Configure LDAP Servers, page 10-10.

Figure 10-5 Calendar Service Window



Configure LDAP Servers

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 LDAP servers, refer to Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager"

If you have selected the "Configure the system with PreQualification Assistant data file" option, you must select the server record and click 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 click the Next button.

To configure an LDAP Server:

Step 1 Select the first listed LDAP server, then click **Edit**. If adding a new LDAP server, click **New**.

Step 2 When the LDAP Servers popup window appears, make sure the existing information is correct or enter the new LDAP information. For further information, refer to LDAP Server, page 11-14. If necessary, make changes in the fields.

Click the **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**.

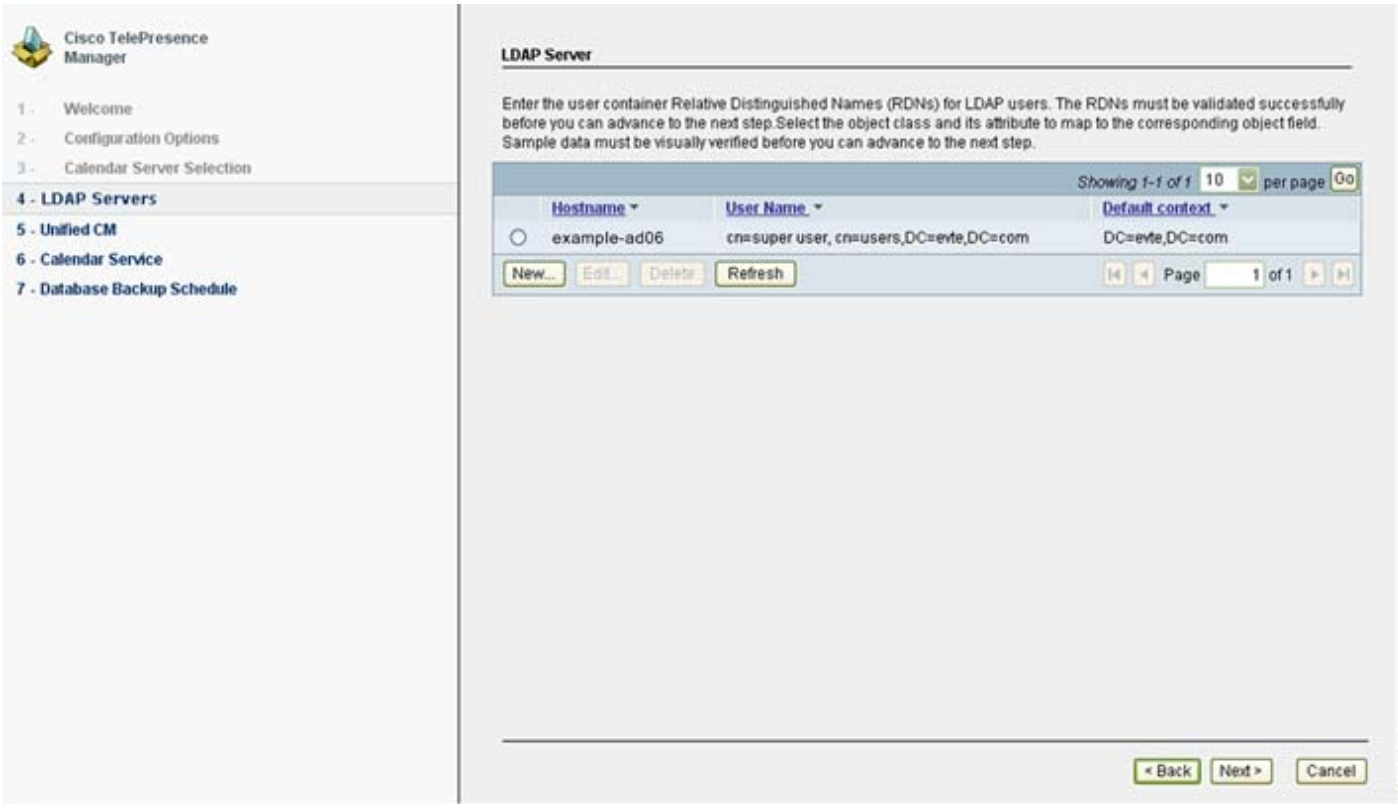
Step 3 The LDAP Server window re-appears. If you have more LDAP servers to test, repeat steps 1 through 3.

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

The Unified CM window appears. Go to Configure Unified CM, page 10-14.

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

Figure 10-6 LDAP Server Window for Microsoft Exchange



Exchange LDAP Mappings

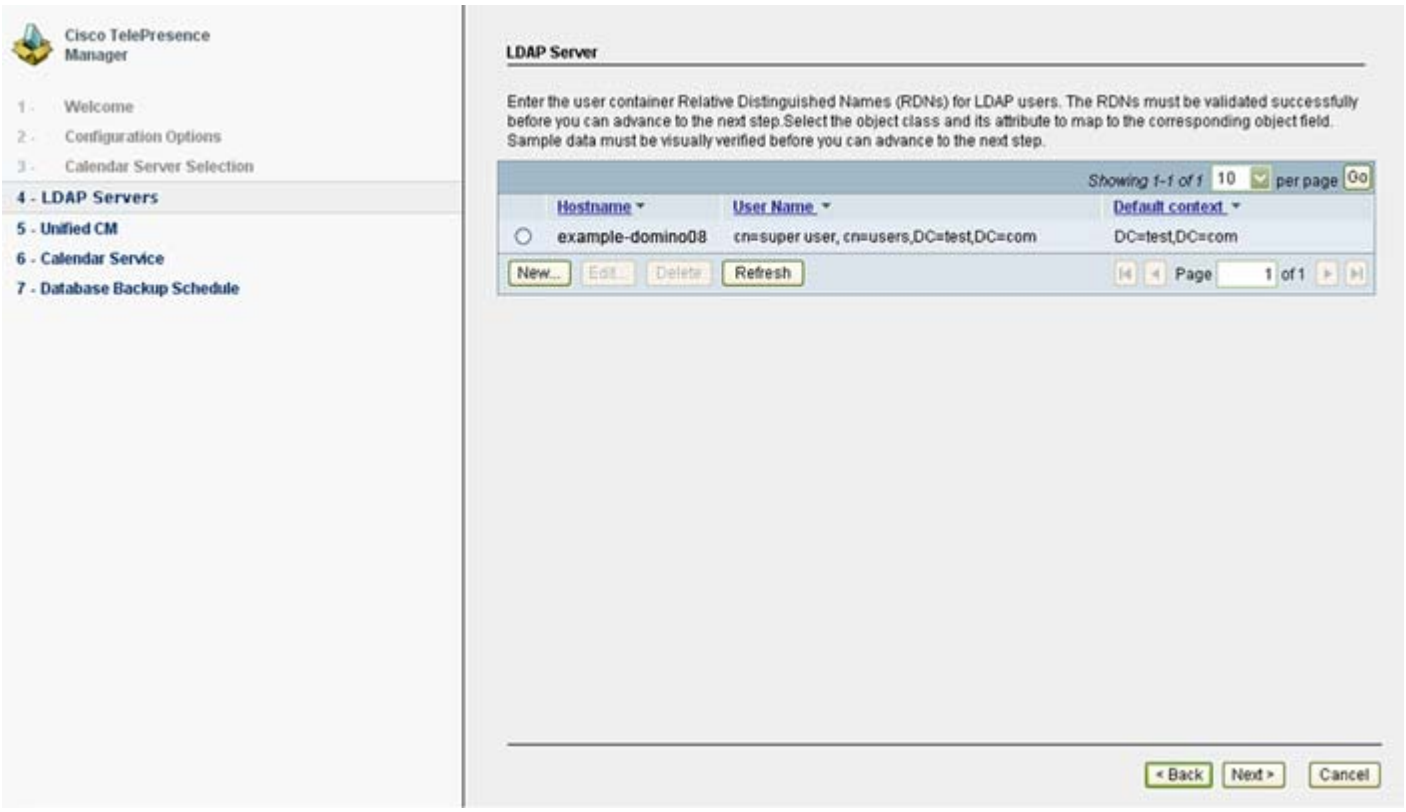
The following table describes the settings for the Person fields in both the New and Edit windows.

Table 10-2 LDAP Person - Objects and Attributes Microsoft Exchange

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
Person			
	Title	Person	title
	Location	Person	l
	DeptID	Person	department
	Country	Person	co

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

Figure 10-7 LDAP Servers Window for IBM Domino



Domino LDAP Mappings

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 does not have to be changed.

Caution The object and attribute mappings for Domino/Directory Server deployments are listed in Table 10-3 and cannot be changed after installing and configuring CTS-Manager.

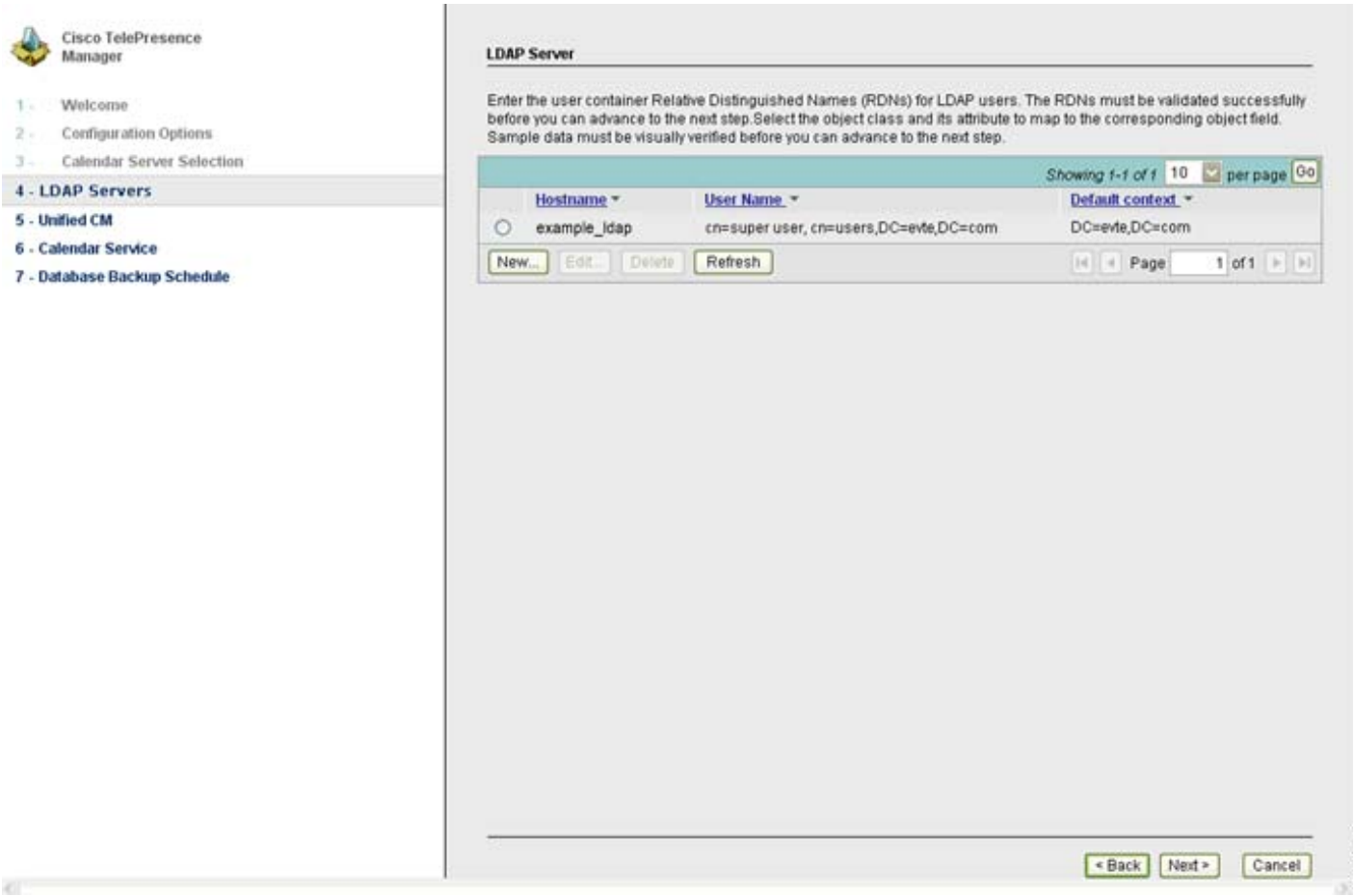
Table 10-3 LDAP Person - Objects and Attributes for IBM Domino

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
Person			
	Country	Person	c
	EmailID	Person	mail
	DeptID	Person	department

Table 10-3 LDAP Person - Objects and Attributes for IBM Domino (continued)

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
	SchedulerName	Person	cn **Note** Do not change this value. If this value is changed incorrectly, meetings will not have the correct information.
	DisplayName	Person	displayname
	Title	Person	title
	Location	Person	location

Figure 10-8 LDAP Servers Window for Scheduling API



Configure Unified CM

This window allows you to add a new Cisco Unified Communications Manager (Unified CM) server or review configured Unified CM server(s) and verify their setup.

To configure Unified CM:

Step 1 Select the first listed Unified CM server, then click **Edit**. If adding a new Unified CM server, click **New**.

Step 2 When the Unified CM Service window appears, make sure the existing information is correct or enter new information. For further information, refer to Unified CM, page 11-54. If necessary, make changes in this window.

- Click the **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**.

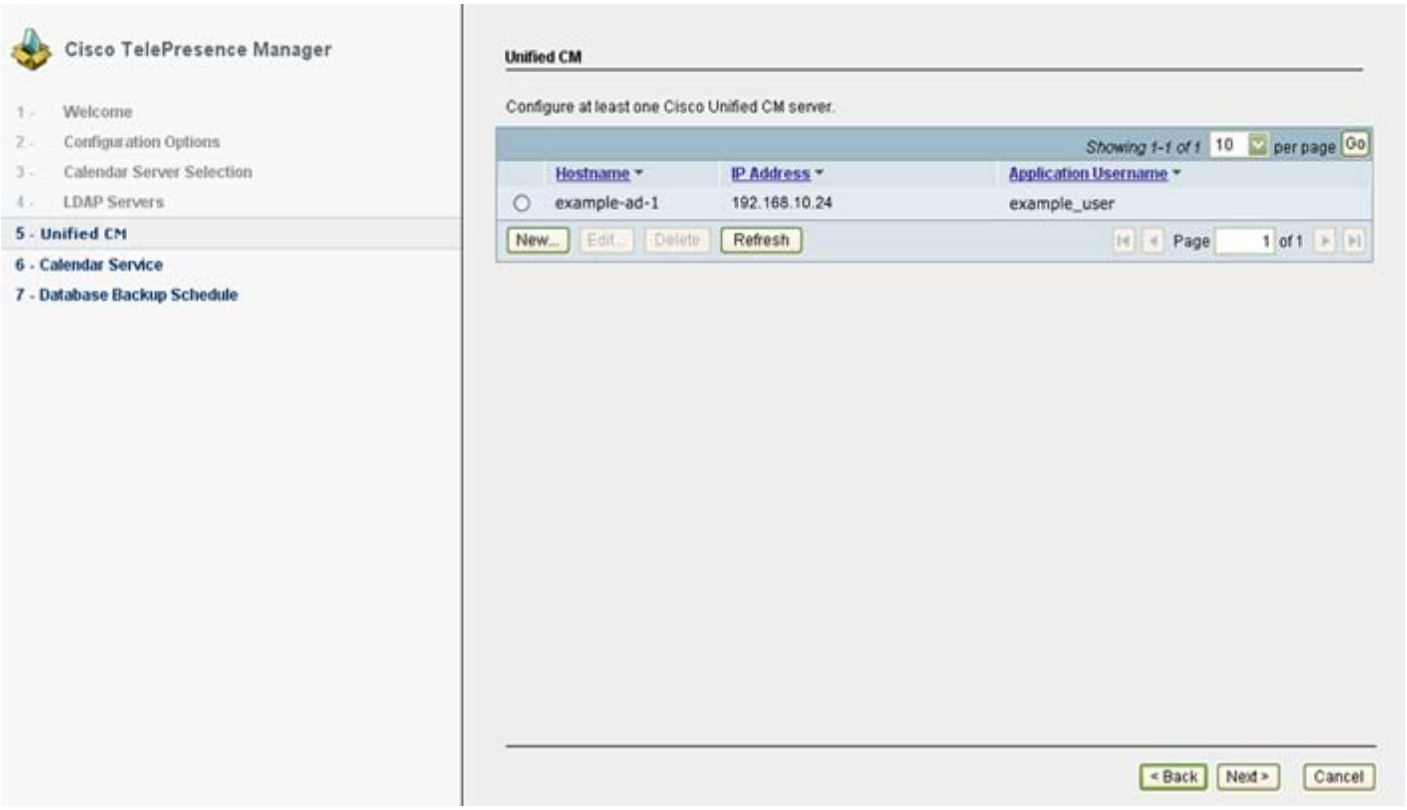
Step 3 The Unified CM Service window re-appears. If you have more server connections to test, repeat Steps 1 through 3.

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.

The calendar server window appears. Go to Configure Calendar Server, page 10-15.

Figure 10-9 Unified CM Window for Microsoft Exchange



Configure Calendar Server

This window allows you to review the calendar server that was configured, make changes if needed, and verify the configuration. Microsoft Exchange and Domino calendaring server examples are shown below. For further information about calendar server configurations, refer to Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager".

To configure the calendar server:

Step 1 Review the existing calendar server information or enter new calendar server information.

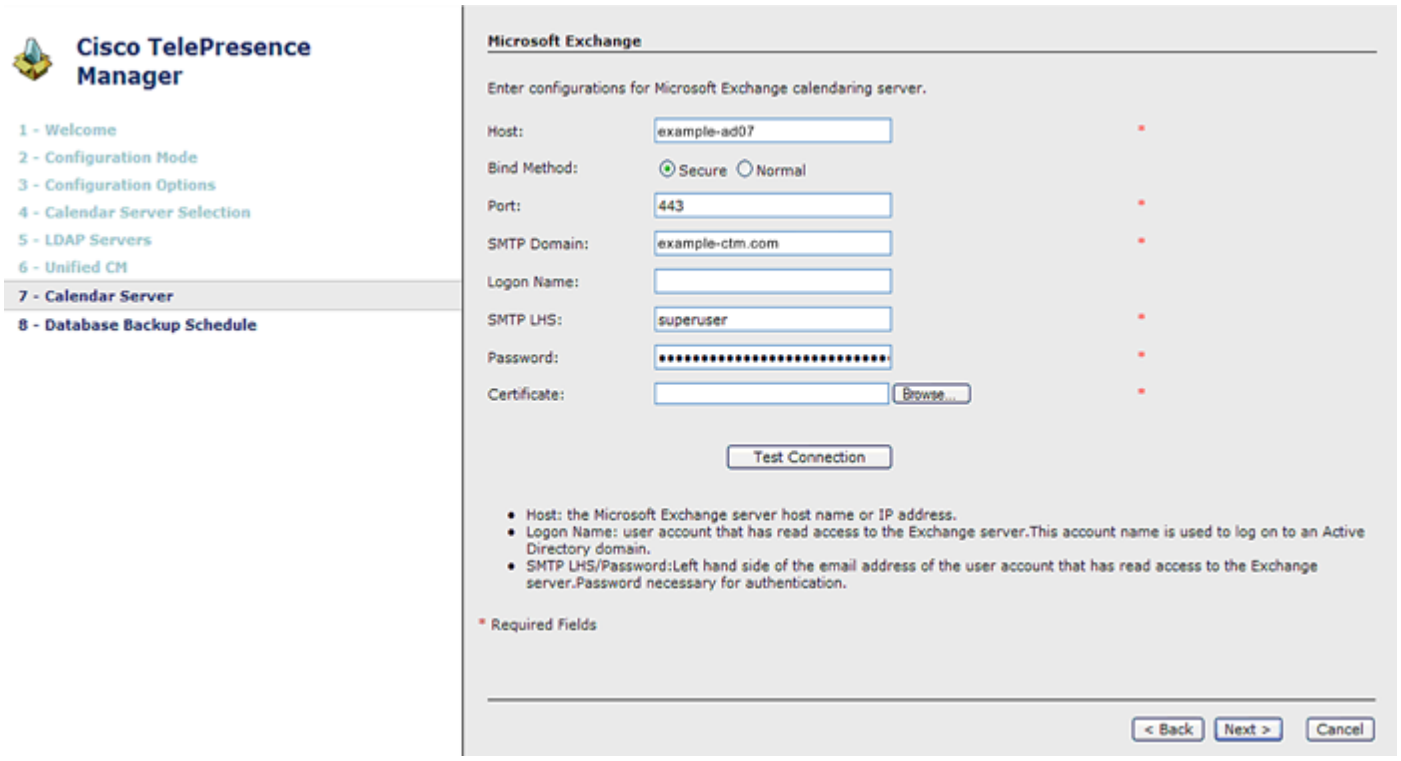
- For information about Microsoft Exchange fields, see Explanation of Microsoft Exchange Fields, page 10-16.
- For information about IBM Domino fields, see Explanation of IBM Domino Fields, page 10-17.
- For information about Scheduling API fields, see Explanation of Scheduling API Fields, page 10-19

Step 2 After filling in all of the fields, click **Test Connection** to verify this configuration.

Step 3 When the verification is completed, click the **Next** button.

The Database Backup Schedule window appears. Go to Configure Database Backup Schedule, page 10-19.

Figure 10-10 Calendar Server Window for Microsoft Exchange



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 (endpoints). 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**

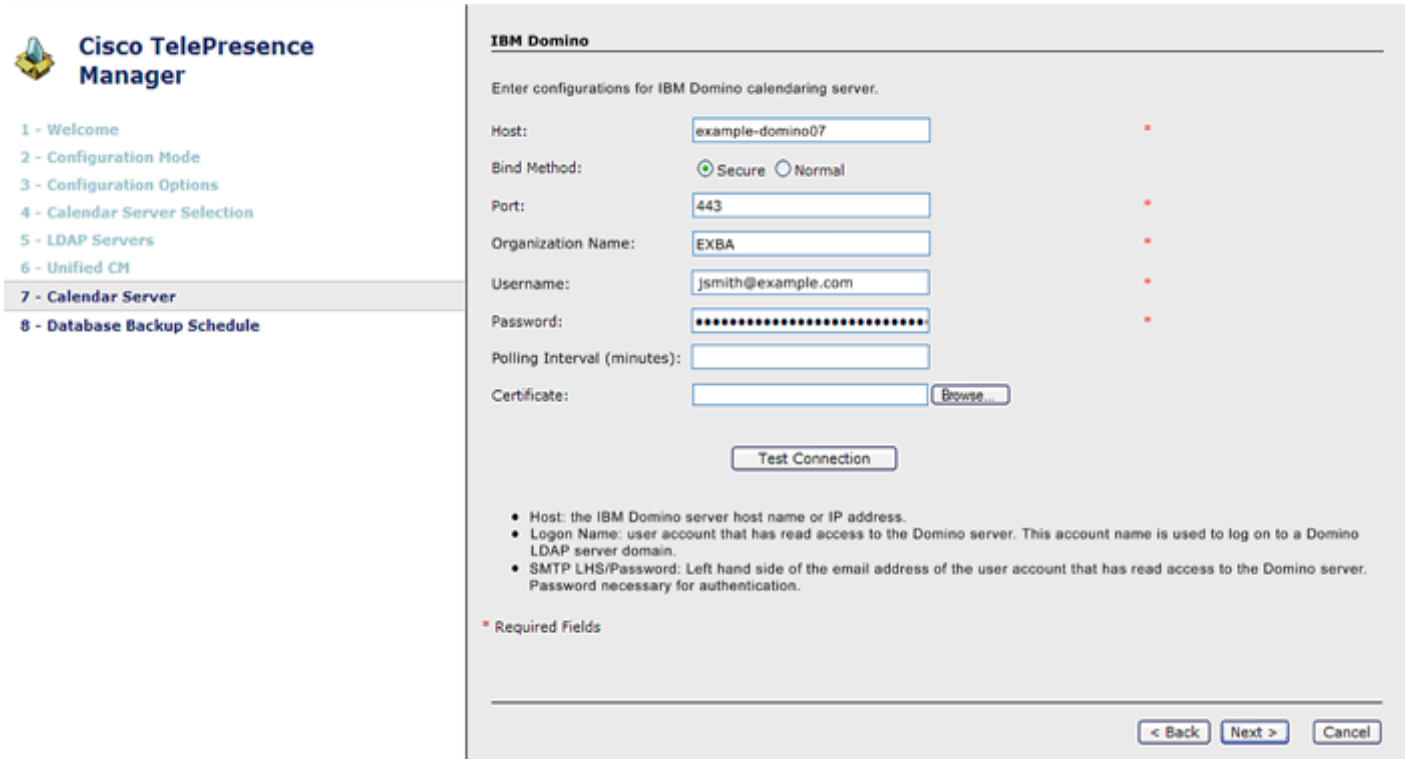
  The user password allows access to the Microsoft Exchange Server.

- **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.

Figure 10-11 Calendar Server Window for IBM Domino



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)**

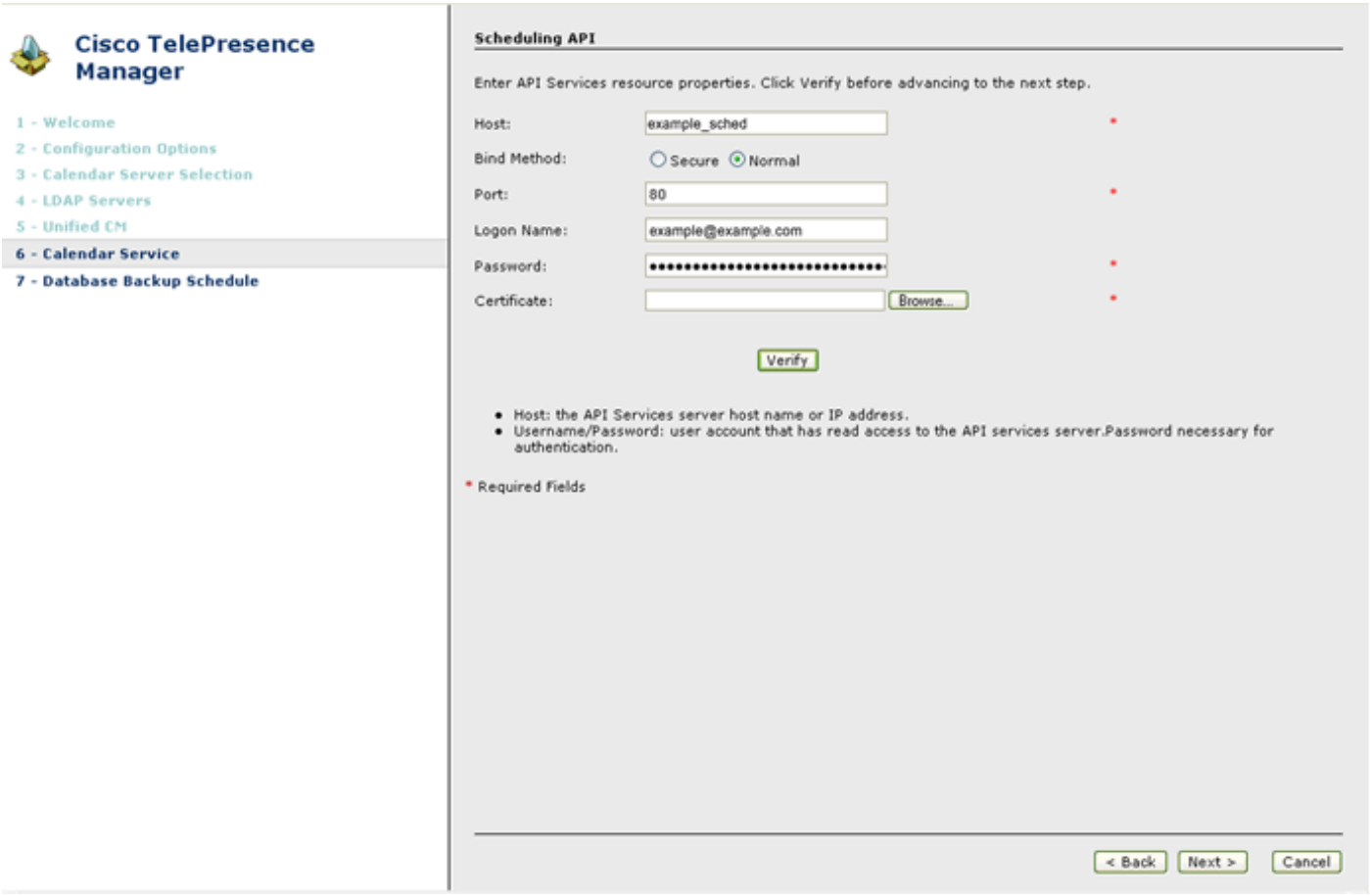
  This is the amount of time between intervals that the CTS-Manager will poll for Calendar information. The interval times for polling are from a minimum of 1 to a maximum of 360 minutes.

- **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.

Figure 10-12 Calendar Server Window for Scheduling API



Explanation of Scheduling API Fields

- **Host**

  Host is the hostname or IP address scheduling API server.

- **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 scheduling API server. You must complete the Certificate field on this window before you can proceed.
  - Normal—The CTS-Manager communicates with the scheduling API server in cleartext using HTTP.

- **Port**

  The default value is 80. You can use 80 or 8080.

- **Logon Name**

  The username provides login access to the calendar server.

- **Password**

  The user password allows access to the calendar 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.

- **Verify**

  Validates Logon Name and Password against the LDAP server.

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

Configure Database Backup Schedule

The Database Backup Schedule window allows you to set the database backup schedule. This schedule must be set in order to complete the initialization process.

To configure the database backup schedule:

Step 1 Fill in the Database Backup Schedule fields.

For information about these fields, see Explanation of Database Backup Schedule Fields, page 10-20.

Step 2 If you are setting up a remote backup, click **Verify Remote Host** to verify the login information.

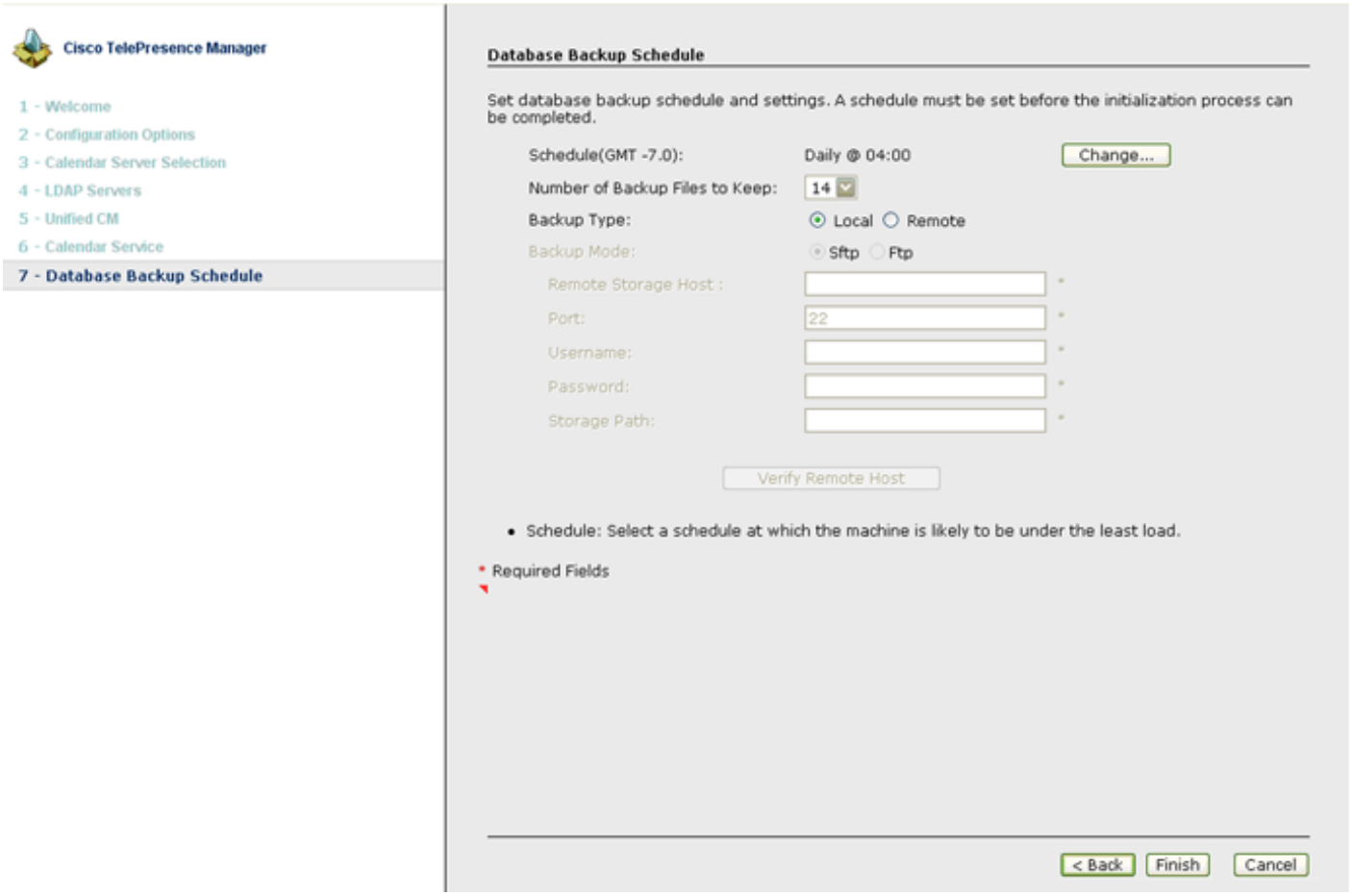
For additional information about Database Backup, refer to Database - Status, Backup, and Restore, page 11-48 in Chapter 11, “Additional Installation Configurations for Cisco TelePresence Manager.”

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.

Step 3 Click **Finish**.

The Cisco TelePresence Manager Status Dashboard window appears. Go to Dashboard for Verification of Installation Status, page 10-21.

Figure 10-13 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 to 14 (two week's worth of daily backups). The default is 14.

- **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 to 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.

Dashboard for Verification of Installation Status

The Status Dashboard window appears after initialization is complete, allowing you to verify installation and to check the status of the system services. In the future, you can come to this window to see a snapshot of meetings that are scheduled for the day. Click highlighted links in this window for quick access to other windows that provide meeting and room(endpoint)-scheduling functions.

Figure 10-15 describes the dashboard report information. To update the reports, click **Refresh**.

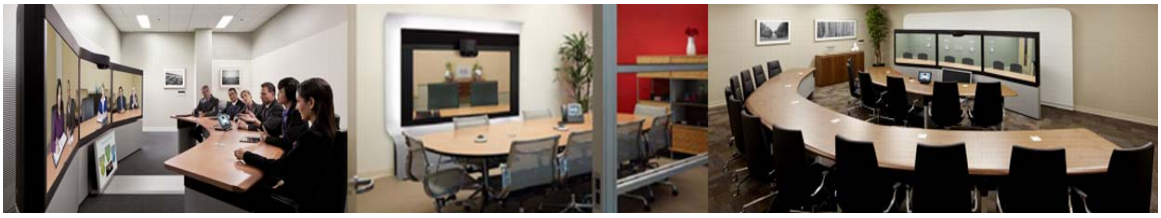
For additional configurations and an introduction to the CTS-Manager administration software, go to Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager".

Figure 10-14 Cisco TelePresence Manager Monitor > Status Dashboard Window

Figure 10-15 Status Dashboard Report

Field	Description or Setting
Today's Meetings	Status of current and upcoming meetings: • With Error—Displays the number of meetings that have errors. • All Meetings—All meetings scheduled for today. Click the link associated with each meeting or device's information to go to the Meetings window.
Devices	Status information for the following devices: • Bridges and Servers—Clicking the link displays the summary information in the Support > Bridges and Servers window and filters the list to those bridges and servers with an error status. • Application Servers—Clicking the link displays the summary information in the Cluster Management > Application Servers window. (Only appears if CTS-Manager is part of a cluster). Cisco no longer provides support for the clustering feature originally introduced in release 1.8. For questions, contact Ron Lewis: ronlewis@cisco.com. • Database Servers—Clicking the link displays the summary information in the Cluster Management > Database Servers window. (Only appears if CTS-Manager is part of a cluster). Cisco no longer provides support for the clustering feature originally introduced in release 1.8. For questions, contact Ron Lewis: ronlewis@cisco.com. • TelePresence Endpoints—Clicking the link displays the status information in the Support > Endpoints window. • VC Endpoints—Clicking the link displays the status information for VC endpoints in the Support > Endpoints window. • Unified CM—Clicking the link displays the information in the Support > Unified CM window. **Note** An error may occur if the connection to Unified CM was caused by a network outage. You can remove the error status by restarting Cisco TelePresence Manager.
Indicators	Status Indicators for: • Database Backup • Current Database Size • Mailbox is • Endpoint Mailbox Sync
Time	Status of the following times: • 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 for logged-in user.

Field	Description or Setting
Services	Status information for the following system services: • Calendar Service • WebEx (if enabled) • LDAP Server • Endpoint Control • Database • Multipoint Conference • Unified CM Status is either **OK** or is a highlighted link listing the number of errors. You can click a link to see further system log status information and troubleshoot problems. You can also roll your mouse over a highlighted link to see a brief description of the error.
Uptime	Status information about the elapsed running time since the last restart. • Services—Services displayed in the Services section. • TelePresence Engine—Cisco TelePresence database engine. • System Platform—Hardware host for CTS-Manager.



CHAPTER 11

Additional Installation Configurations for Cisco TelePresence Manager

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

Contents

- Post-Install Guidelines for CTS-Manager, page 11-2
- Introduction to the CTS-Manager Administration Software, page 11-3
- Licensing for CTS-Manager, page 11-6
- Security, page 11-13
- LDAP Server, page 11-14
- Field Mappings, page 11-15
- Calendar Server, page 11-25
- Microsoft Exchange, page 11-29
  - Synchronization Operations, page 11-30
- IBM Domino, page 11-35
- Access Management, page 11-73
- Alert Management, page 11-77
- Application Settings, page 11-93
  - Meeting Notification Email, page 11-94
  - WebEx, page 11-98
  - Multipoint Conference Scheduling, page 11-96
  - Interoperability with Video Conferencing, page 11-97
  - TelePresence Call-In Number, page 11-98
  - Studio Mode Recording, page 11-98
  - CTMS Network Multipoint, page 11-99
  - Intergroup Scheduling, page 11-99
  - Intercompany, page 11-100

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

Post-Install Guidelines for CTS-Manager

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

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

Table 11-1 Post-Install Guidelines for Configuring CTS-Manager

Setup Procedure Guidelines after Installing CTS-Manager	Description	Location
Additional Installation Procedures for CTS-Manager	The administrator makes use of the System Configuration window to perform system configuration tasks such as uploading licenses, synchronizing system databases, managing security, and reconfiguring system settings	Current chapter.
Configuring Cisco TelePresence WebEx OneTouch for CTS-Manager	Describes how to set up Cisco TelePresence WebEx OneTouch in CTS-Manager, which allows WebEx participants to join TelePresence meetings.	Chapter 12, "Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager"
Monitoring and Supporting CTS-Manager	Describes the support features available when you log into CTS-Manager using a Live Desk role.	Chapter 13, "Monitoring and Supporting Cisco TelePresence Manager"

If at any time you encounter problems, go to Chapter 16, "Troubleshooting Cisco TelePresence Manager" to see how to correct the problem.

Introduction to the CTS-Manager Administration Software

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

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

- Administrator Role, page 11-3
- SysAdmin Role, page 11-4
- Live Desk Role, page 11-4

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

Administrator Role

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

- System Status
- Monitor

- Support
- Configure
- Troubleshoot

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

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

SysAdmin Role

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

- System Settings
- Software Upgrade

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

Live Desk Role

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

- System Status
- Monitor
- Support
- Troubleshoot

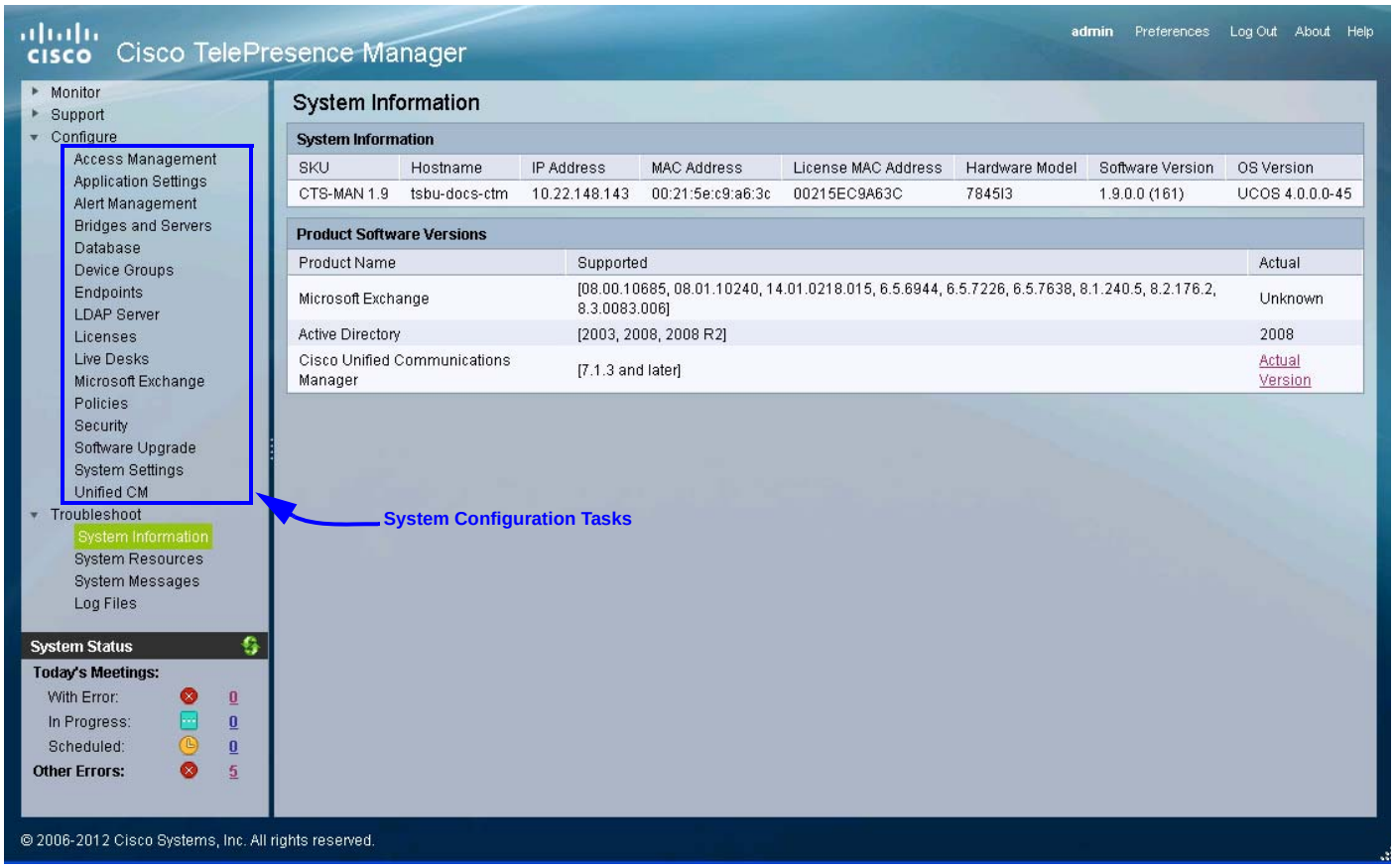
The Live Desk is the first person contacted when there are questions or problems pertaining to connecting meeting participants. Live Desks can be assigned rooms (endpoints) to monitor in the CTS-Manager application. Assigned Live Desks are easily reached by dialing the Help soft key on the endpoint phone/display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

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

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

Figure 11-1 shows the system configuration information displayed in the Troubleshoot > System Information window. The system configuration tasks in the Configure section are highlighted on the left.

Figure 11-1 Troubleshoot > System Information Window



Licensing for CTS-Manager

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

The primary licensed features in CTS-Manager include:

Table 11-2 CTS-Manager Licensed Features

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

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

Feature-Based Licenses

Optional feature-based licenses include:

Table 11-1 Feature-Based Licenses

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

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

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

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

Count-Based Licenses

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

Table 11-2 Count-Based Licenses

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

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

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

Getting Licenses for CTS-Manager

This section describes how the following customers get licenses:

- New Customers, page 11-7
- Existing Customers Upgrading to CTS-Manager 1.9, page 11-8

New Customers

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

Step 1 Order CTS-Manager with server, choosing the number of endpoints for licensing plus optional reporting and/or scheduling API, as required.

Step 2 Receive CTS-Manager server. Included with the server is a Claim Certificate with a license Product Authorization Key (PAK).

Step 3 Install and initialize CTS-Manager.

Step 4 Obtain the License MAC Address by logging in to CTS-Manager and going to the **Troubleshoot > System Information** window.

Note You can also obtain the License MAC Address by typing the **show status** command in the CTS-Manager command line interface (CLI). For information about how to access the CLI, refer to: Starting a CLI Session, page 13-43.

Step 5 Register the PAK with the License MAC Address at http://cisco.com/go/license.

Step 6 License file(s) arrive by email within one hour.

Step 7 After installation of CTS-Manager, SysAdmin installs the license file(s).
For more information, see Viewing and Uploading Licenses, page 11-8.

Existing Customers Upgrading to CTS-Manager 1.9

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

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

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

To get upgrade license do the following:

Step 1 Perform upgrade to CTS-Manager 1.9.

Step 2 Log in to CTS-Manager

A message appears indicating that room (endpoint) licenses need to be installed.

Step 3 Click **OK** in the message.

The Configure > Licenses > License Files window appears.

Step 4 Click the **Get an Upgrade License** button and follow the instructions to get an upgrade license.

For more information, see Getting an Upgrade License, page 11-12.

Step 5 License file arrives by email within one hour.

Step 6 SysAdmin uploads the license file(s).

For more information, see Viewing and Uploading Licenses, page 11-8.

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

Step 1 Order CTS-Manager endpoints (rooms) or feature licenses. Two options are available for ordering licenses:

- LIC-CTS-MAN-xxx - paper-based license with normal lead times.
- L-LIC-CTS-MAN-xxx - eDelivery option where PAK is sent via email notification to eDelivery mailbox. Faster electronic delivery, shorter lead time. Log in to eDelivery to get your license: https://edelivery.cisco.com/esd/. For more information about eDelivery, refer to: http://www.cisco.com/web/partners/tools/edelivery.html.

Viewing and Uploading Licenses

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

The Licenses window has the following tabs:

- Summary–View existing licenses
- License Files–Upload new licenses

Summary

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

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

- Feature-Based Licenses–Enable or disable a feature.
- Count-Based Licenses–Correspond to the number of CTS endpoints (rooms) used for TelePresence meetings, based on one license per endpoint.

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

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

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

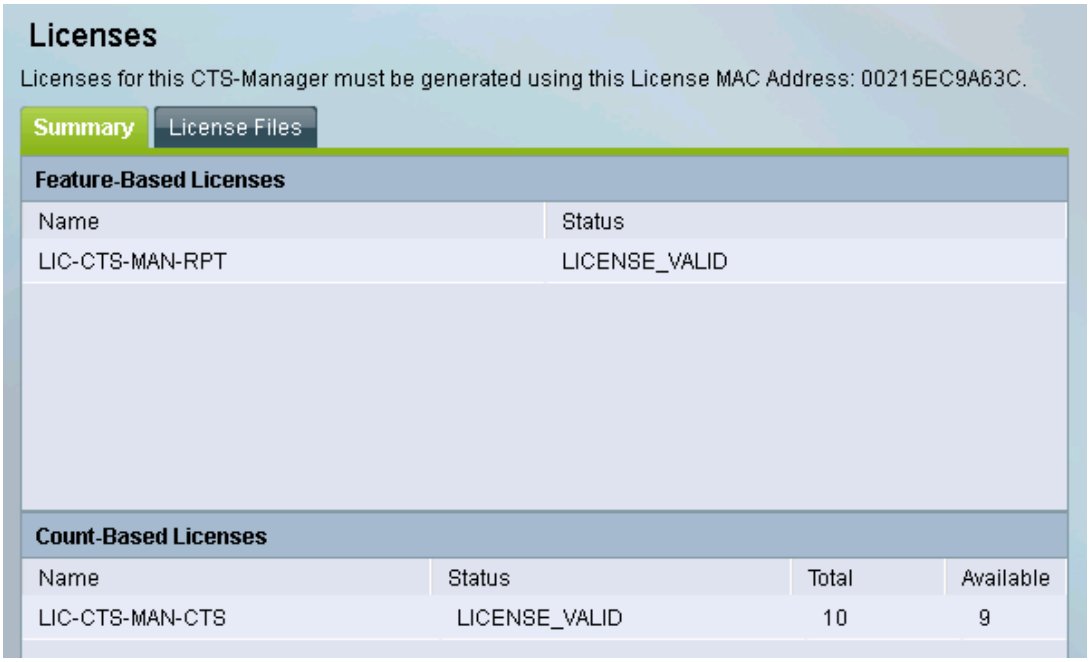
If you are not able to set up TelePresence endpoints, go to the Support > Endpoints window to make sure that each endpoint has a green checkmark in the “Licensed” column.

To check if the uploaded licenses are valid, go to the Configure > Licenses window. The name and the status of each license are displayed. A properly licensed feature will display a status of “LICENSE_VALID.”

Licensing Grace Period

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

Figure 11-2 Configure > Licenses > Summary Window



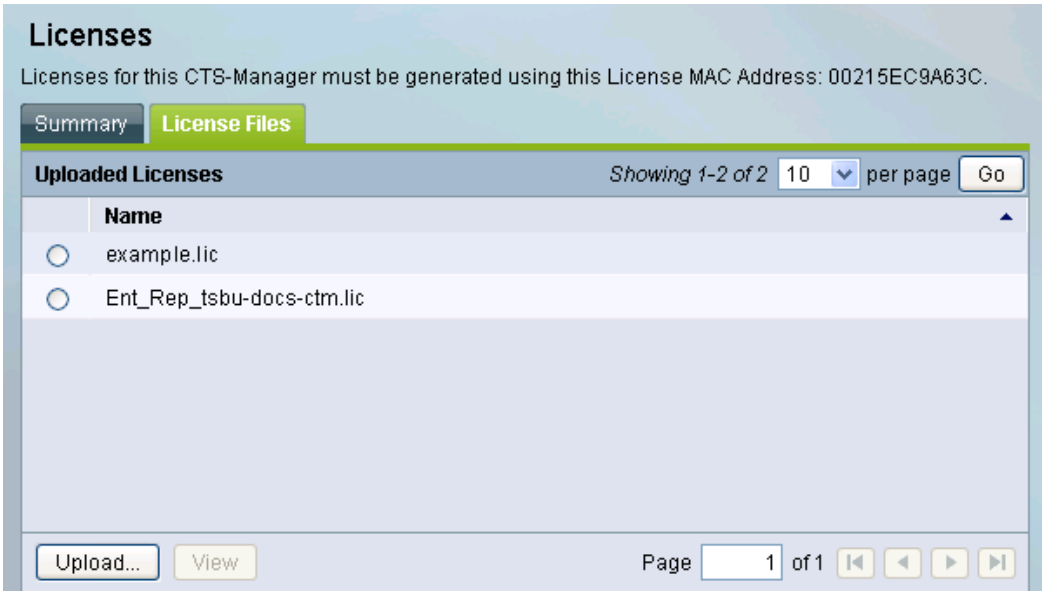
License Files

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

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

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

Figure 11-3 Configure > Licenses > License Files Window



Uploading Licenses

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

To upload a license:

Step 1 Click **Upload**.

Step 2 In the License Upload window, click **Browse**, find the license you want to add and click **Open**.

Step 3 Click **Upload**

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

Step 5 To verify that your license has been uploaded properly, click the Summary tab.

Your license should be listed with a status of "LICENSE_VALID."

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

When You Need New Count-based (Endpoint-based) Licenses

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

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

CTS-Manager License Backup and Restore

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

Hardware Replacement and New Licensing

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

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

When you receive your new hardware, do a fresh install and upload the new licenses in the Configure > Licenses > License Files window, as detailed in Uploading Licenses, page 11-11.

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

Getting an Upgrade License

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

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

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

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

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

The Product License Registration page appears.

Step 3 In the Migration License section at the bottom of the page, click **Register for Upgrade/Migrate License**.

The Select Product page appears.

Step 4 From the drop-down menu, select **Cisco TelePresence Manager** and click **Goto Upgrade/Migration License Portal**.

The Upload Features page appears.

Step 5 Copy and paste the MAC Address into the first field and the Upgrade Code into the next field and click the Agreement checkbox to accept the terms of the end-user license agreement.

Step 6 Enter your contact information, making sure your email address is correct, and click **Continue**.

Step 7 The license file will arrive via email in less than one hour.

Step 8 Save the license file.

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

Step 9 In Cisco TelePresence Manager, go to the **Configure > Licenses** window, click the **License Files** tab and upload the license file. For more information, refer to Uploading Licenses, page 11-11.

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

Security

The Configure > Security window allows you to manage system security certificates and web services security.

CTS-Manager supports these security types:

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

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

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

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

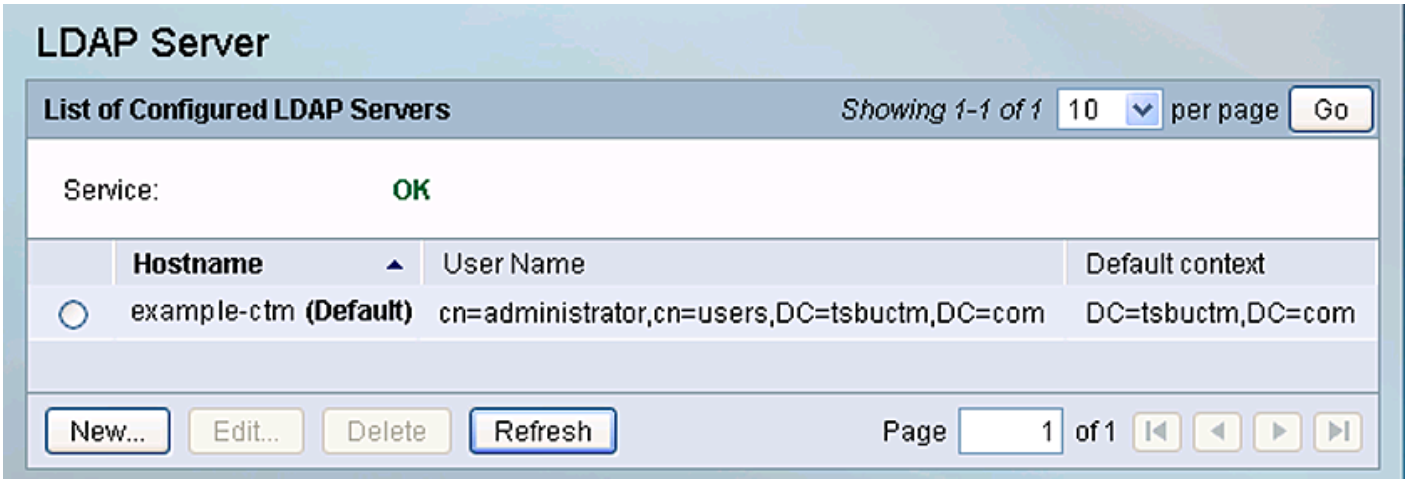
LDAP Server

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

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

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

Figure 11-4 Configure > LDAP Server



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

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

Settings for LDAP

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

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

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

Multiple LDAP Peer Domains

If you have a LDAP peer domain configured you'll need to specify the additional user containers and context. You can do this with one of the User Container fields.
For example, **`cn=users,dc=domain2,dc=com`**
When specifying the container and context information for your peer domain, DO NOT check the Append default context box.

Step 1 To test the connection between this system and the LDAP server, click **Test Connection.**

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

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

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

Table 11-3 describes the settings for the LDAP Server window.

Field Mappings

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

Microsoft Exchange Deployments

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

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

Caution The object and attribute mappings for Exchange/Directory Server deployments are listed in Table 11-5 and cannot be changed after installing and configuring Cisco TelePresence Manager. Cisco TelePresence Manager may not functions properly if the Object Class fields are changed.

Figure 11-5 New LDAP Window Mappings

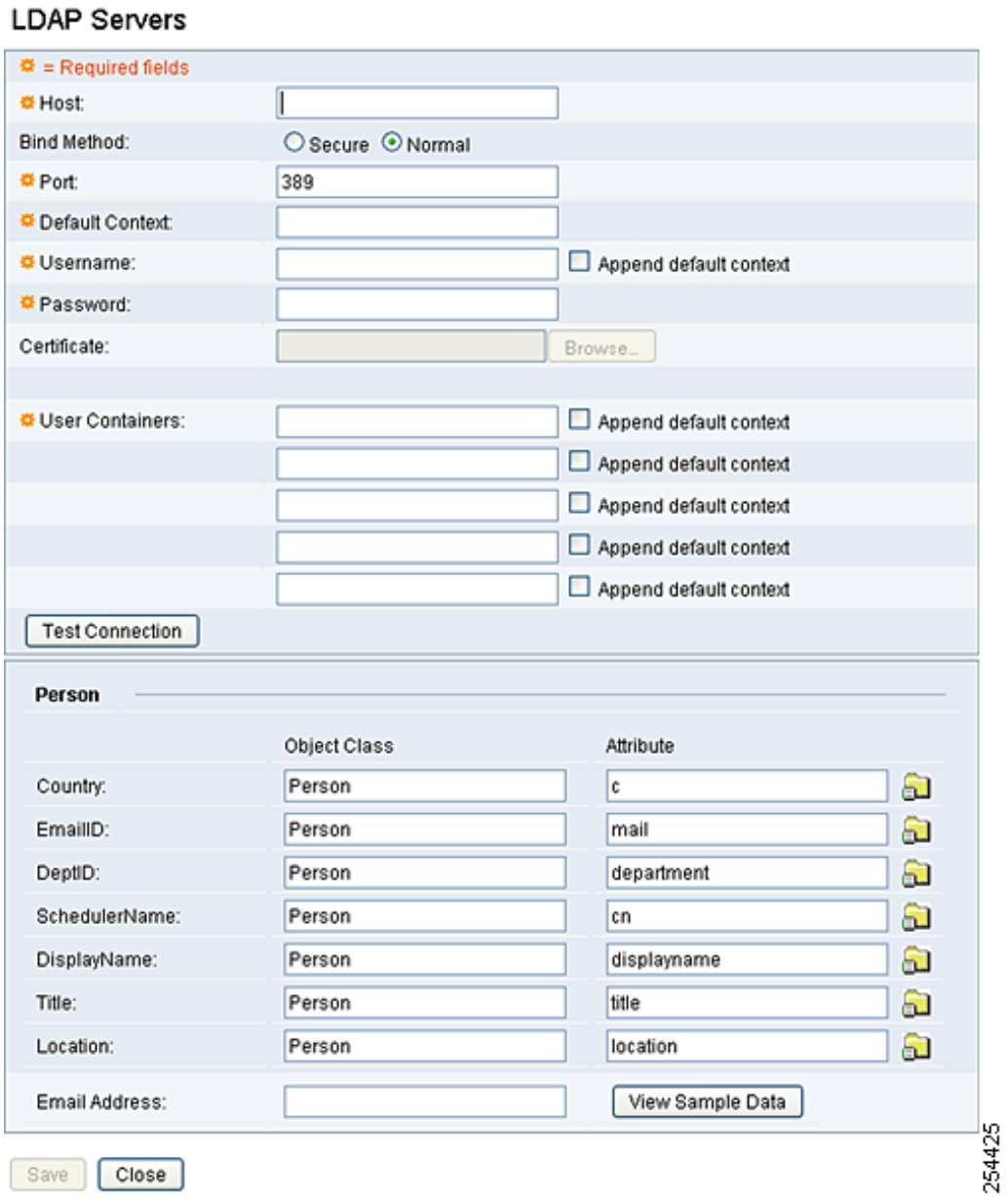


Table 11-3 lists the fields in the LDAP Server - New window. See Table 11-5 for the Person field information.

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

Table 11-3 New LDAP Server Settings

Field or Button	Description or Settings
Host	LDAP server host name.
Bind Method	Click the **Secure** or **Normal** radio button to select the binding method: • 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 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. To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer, then click Browse to select it and upload it to CTS-Manager.

Table 11-3 New LDAP Server Settings (continued)

Field or Button	Description or Settings
User containers	The containers from which queries are performed to retrieve user objects. More than one user container or user object can be specified. The Cisco Telepresence server uses the values entered to search through the containers in sequence to retrieve user and meeting room (endpoint) information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication. • To append the default context, check the Append default context box next to the user container field. **Note** If you have a LDAP peer domain configured you'll need to specify any user containers and context. For example, "*cn=users,dc=domain2,dc=com*". When specifying the container and context information for your peer domain, DO NOT check the Append default context box.
Test Connection	This allows you to test the connection configuration between this system and the LDAP server.

Edit

To edit the LDAP mapping, click the radio button to select the LDAP server that you want to edit. Then click the **Edit** button. The LDAP Edit window appears. Table 11-4 lists the field information. See Table 11-5 for the Person field information.

Figure 11-6 Edit LDAP Window

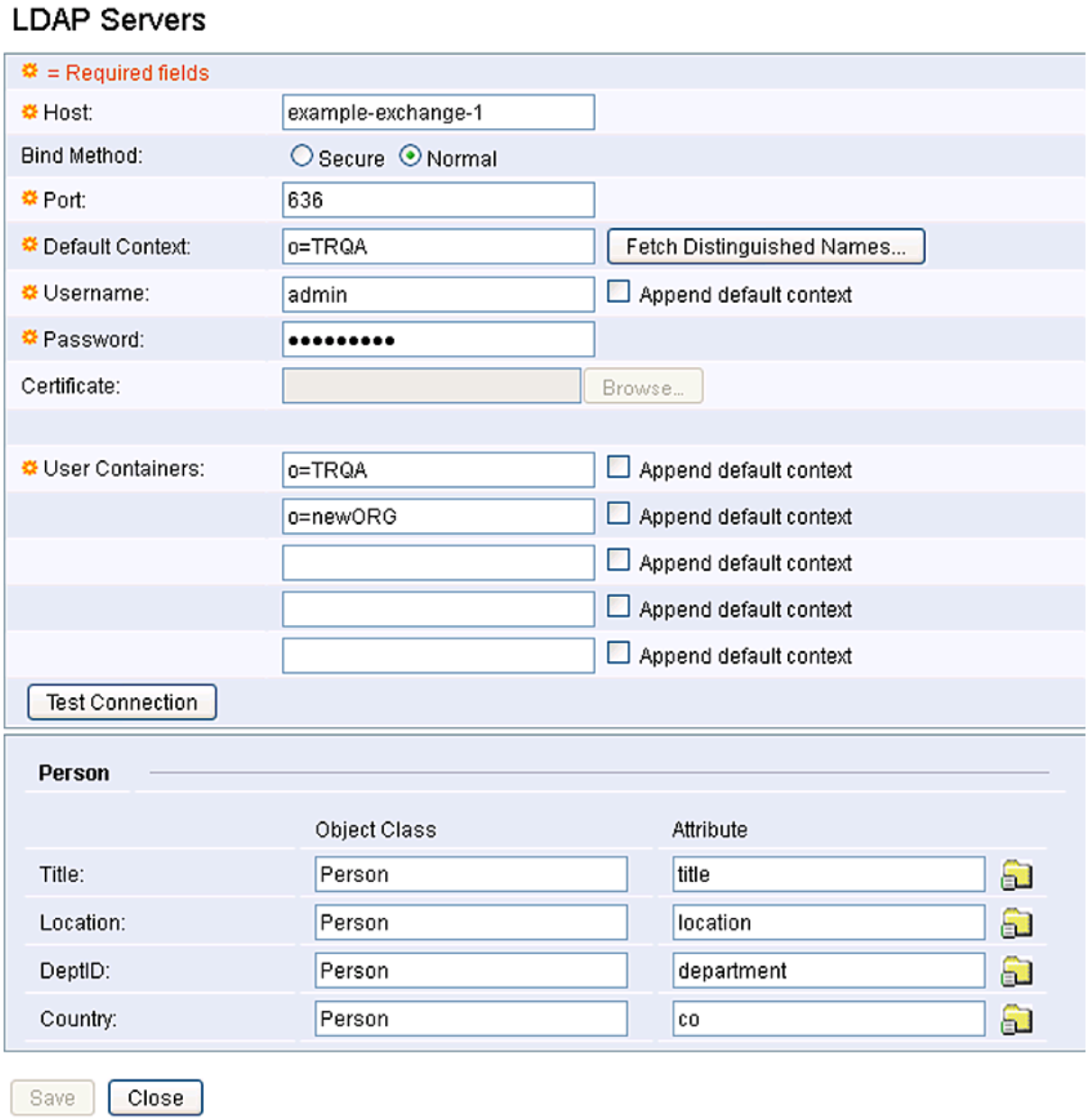


Table 11-4 Edit LDAP Server Settings

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

Table 11-4 Edit LDAP Server Settings (continued)

Field or Button	Description or Settings
Bind Method	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 or DIIOP.
Port	The default port for secure connection is 636. The default port for normal connection in a single LDAP server deployment is 389. In cases where deployments consist of multiple LDAP Directory Servers, this port should be configured with 3268, which is the Global Catalog port. Secure Global Catalog port is 3269.
Default Context	The default context from which the LDAP queries are performed. To change the context string: • Click the Fetch Distinguished Names button and choose the context from the Select a DN drop-down list adjacent to this field.
Username	The username used to authenticate to the LDAP server. This must be in the LDAP fully qualified domain name (FQDN) format. Example: cn=administrator,cn=users,dc=<mydomain>,dc=com)
Password	Password to access the LDAP server.
Certificate	The name of the LDAP certificate. This is only needed if you have chosen the Secure Bind Method. To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer. Then click Browse to select it and upload it to CTS-Manager.

Table 11-4 Edit 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 (endpoint) 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 11-5 describes the settings for the Person fields in both the New and Edit windows.

Table 11-5 LDAP Person - Objects and Attributes

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

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

IBM Domino Deployments

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

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

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

Note The object and attribute mappings for Domino/Directory Server deployments are listed in Table 11-7 and cannot be changed after installing and configuring CTS-Manager.

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

Table 11-6 lists the information for the fields in the IBM LDAP Edit or New window.

Table 11-6 IBM LDAP Server Settings

Field or Button	Description or Settings
Host	LDAP server host name.
Bind Method	Click the **Secure** or **Normal** radio button to select the binding method: • Secure—Secure SSL connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. • Normal—CTS-Manager communicates with the Microsoft Exchange or IBM Domino server in cleartext using HTTP or DIIOP.
Port	The default port for secure connection is 636. The default port for normal connection in a single LDAP server deployment is 389. In cases where deployments consist of multiple LDAP Directory Servers, this port should be configured with 3268, which is the Global Catalog port. Secure Global Catalog port is 3269.
Default Context	The default context from which the LDAP queries are performed. To change the context string: • Click the Fetch Distinguished Names 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. To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer. Then click Browse to select it and upload it to CTS-Manager.

Table 11-6 IBM LDAP Server Settings (continued)

Field or Button	Description or Settings
User Containers	The containers from which queries are performed to retrieve user objects. More than one user container or user object can be specified. The Cisco Telepresence server uses the values entered to search through the containers in sequence to retrieve user and meeting room (endpoint) information from the Directory Server. Additionally, these containers are used to retrieve user information for authentication. • 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 11-7 describes the settings for the Person fields in both the New and Edit windows.

Table 11-7 LDAP Person - Objects and Attributes

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

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

Verifying Field Mapping Data

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

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

Caution The Setting of the LDAP objects and attributes used by the Domino server requires experience using Directory Server and Domino software. Do not change the *mail* and *cn* values in the LDAP SchedulerName Attribute field.
The majority of deployments do not require any changes to these attributes. Incorrectly changing these fields will result in Cisco TelePresence Manager not being able to function.
Consult the Cisco TelePresence Manager support team and the LDAP and Domino server administrator for your deployment before changing the default mappings in these screens.

Deleting Server

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

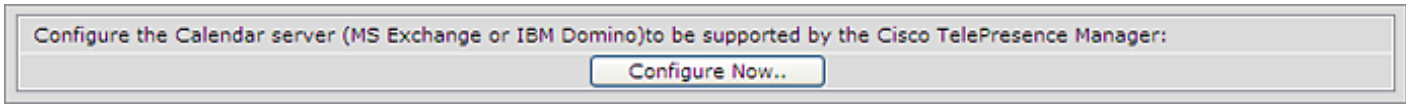
Calendar Server

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

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

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

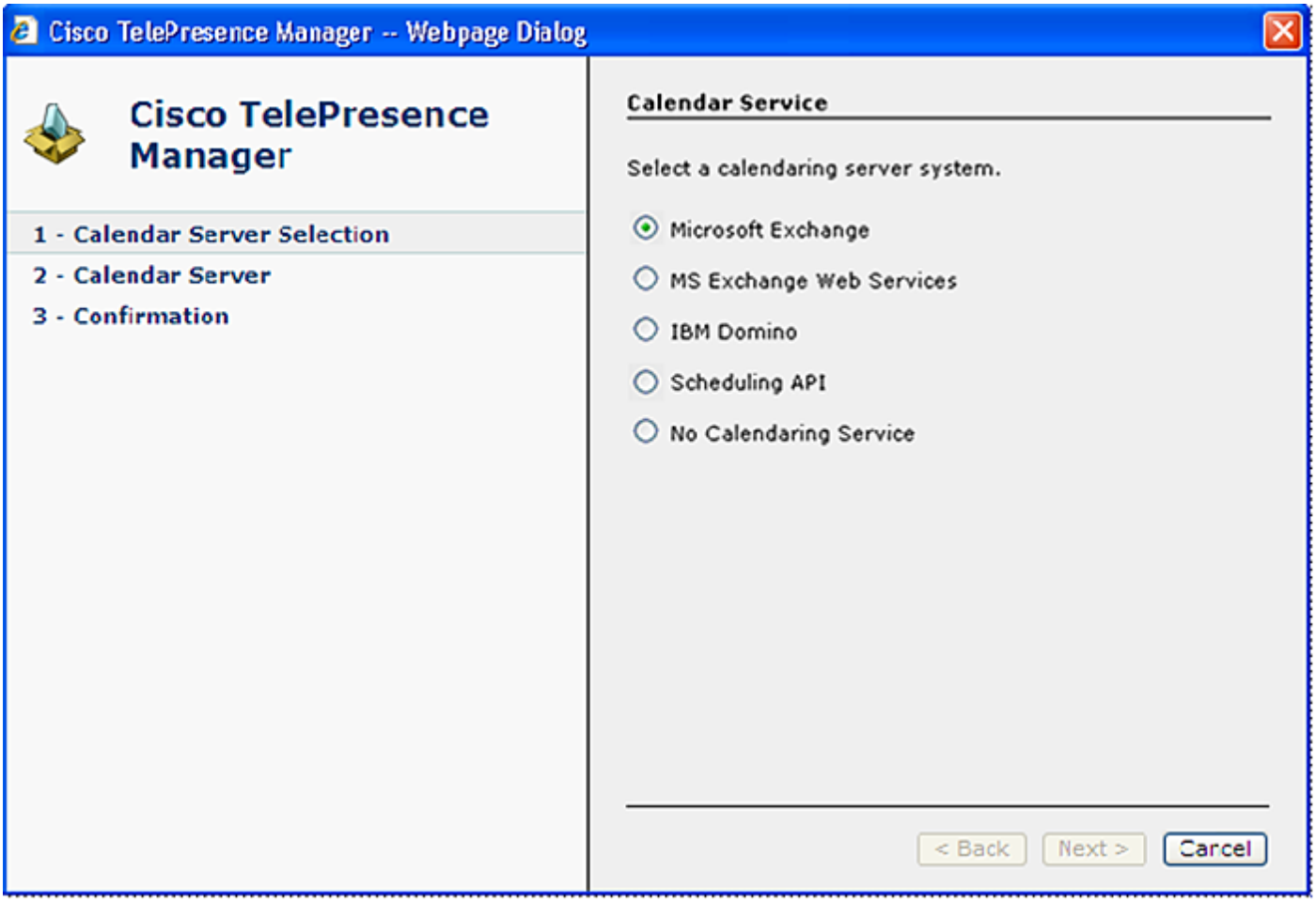
Figure 11-7 Configure Calendar Server



To configure the calendar server:

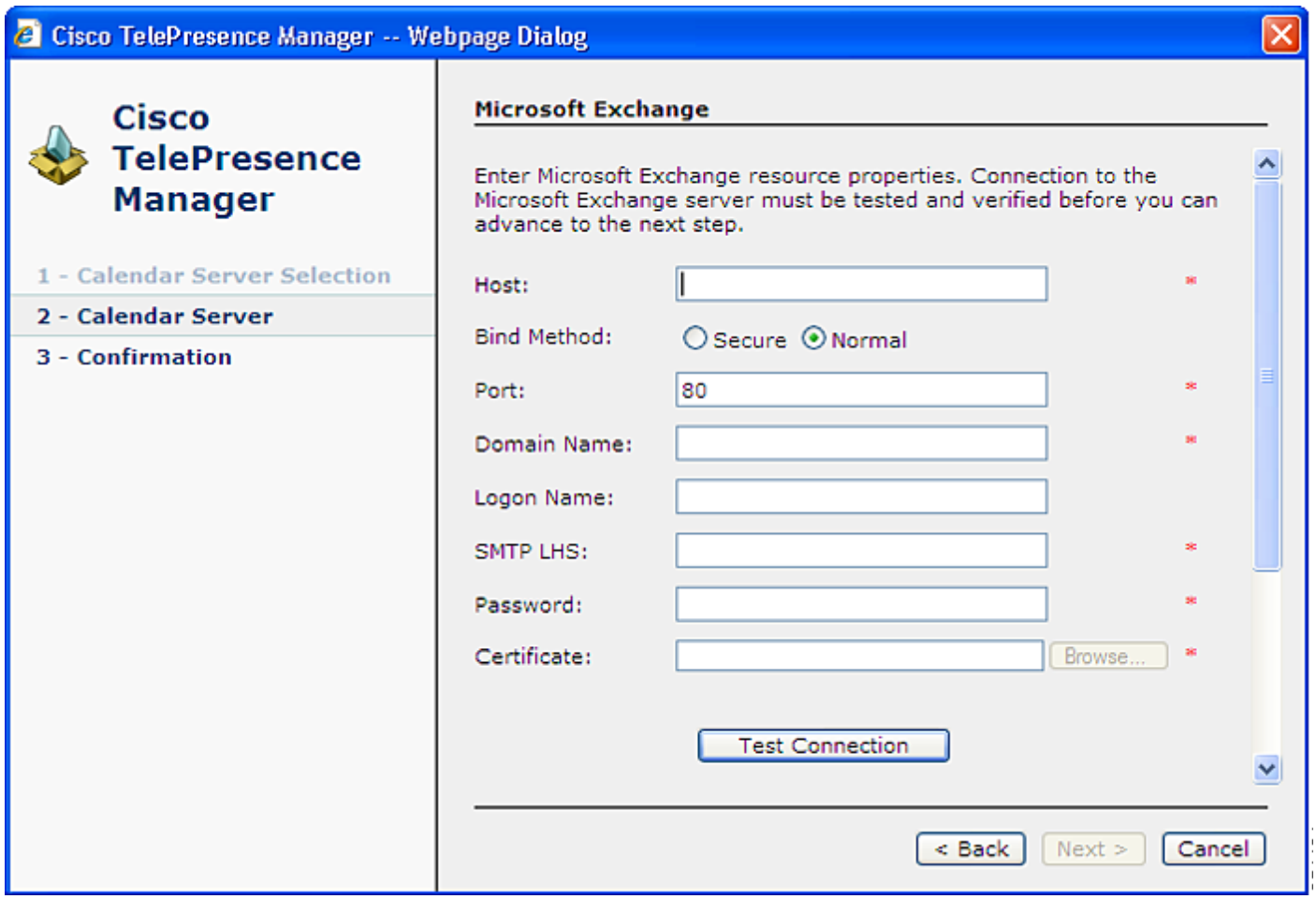
Step 1 The first step in registering a Calendar server with CTS-Manager is to choose either IBM Domino or Microsoft Exchange.

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



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

Figure 11-9 Cisco TelePresence Manager - Calendar Server Microsoft Exchange Screen

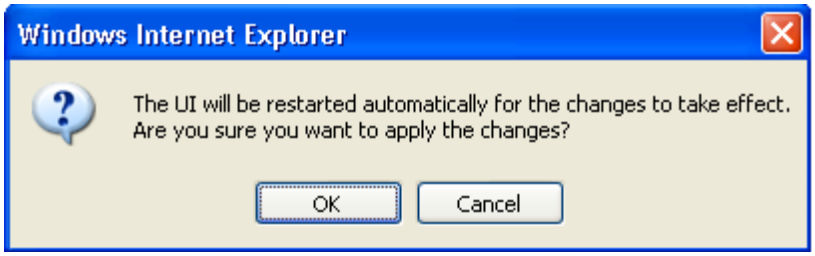


Step 3 Click **Apply** to save the new Calendar server settings.

Figure 11-10 Cisco TelePresence Manager - Calendar Confirmation Screen

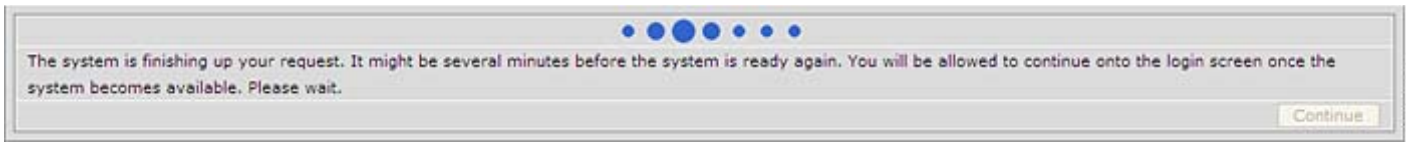
Step 4 Then click **OK** to restart the CTS-Manager server.

Figure 11-11 Apply Changes Screen



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

Figure 11-12 System Restart Notification Screen



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

Microsoft Exchange

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

It is divided into two tabs:

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

To test the connection between CTS-Manager and the Microsoft Exchange server as shown in Figure 11-13:

Step 1 Click the **Configuration** tab**.**

Step 2 Click **Test Connection.**

Step 3 To register new or modified settings, click **Apply.**

Step 4 To restore the original settings, click **Reset**.

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

Figure 11-13 Configure > Microsoft Exchange Window > Synchronization tab

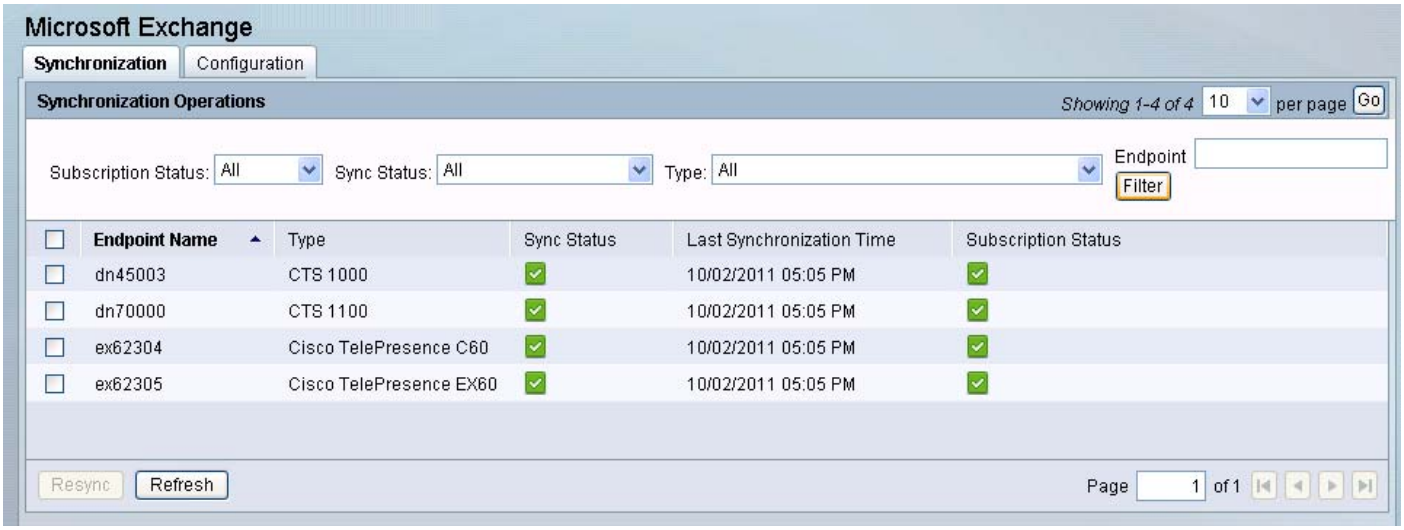


Table 11-8 describes the information and operations accessible from this window.

Synchronization Operations

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

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

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

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

Step 1 Check the boxes next to the endpoints to select them. To synchronize information for all endpoints, check the box next to **Endpoint Name** in the display header.

Step 2 Click **Resync** to start the operation.

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

Step 3 Once the synchronization operation completes, click **Refresh** to update the display.

Table 11-8 describes the information displayed in this area.

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

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

Field	Description or Settings
Endpoint Name	Name of the endpoint (room). Click the arrow in the header of the Endpoint Name column to sort the list in ascending or descending alphabetical order.
Type	Model of endpoint.
Sync Status	Status of the synchronization operation. Click the arrow in the header of the Endpoint Name column to sort the list in ascending or descending alphabetical order.
Last Synchronization Time	Choose the **Secure** or **Normal** radio button to select the binding method, as follows: • Secure—CTS-Manager communicates with the Microsoft Exchange server in secure mode using HTTPS. This method requires enabling Secure Socket Layer (SSL). on the Microsoft Exchange server. • Normal—CTS-Manager communicates with the Microsoft Exchange server in cleartext using HTTP.
Subscription Status	Display-only status information of system service.

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

Figure 11-14 Configure > Microsoft Exchange Window > Configuration tab

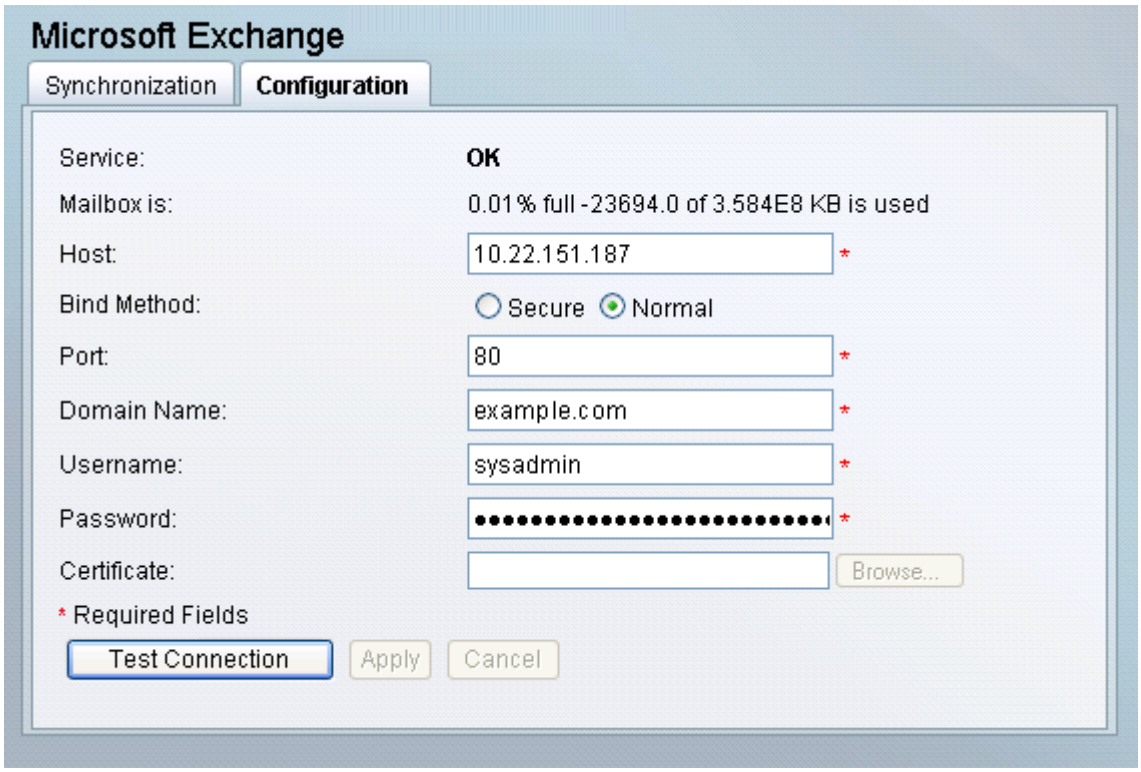


Table 11-9 Configure > Microsoft Exchange > Configuration tab information

Field	Description or Settings
Service	Display-only status report of system service.
Mailbox is	Meeting information is mailed to users. This display-only field reports the amount of storage space taken up by the e-mails as a percentage of total space available.
Host	Hostname provided for the Microsoft Exchange server account, which can be modified.
Bind Method	Choose the **Secure** or **Normal** radio button to select the binding method, as follows: • 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.

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

Field	Description or Settings
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.` **Caution** Logon Name is required for tentative room (endpoint) reservations to work.
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 NTLMv1 authentication for releases 1.6.2 and earlier. The Axis2 Library supports NTLMv2 for releases 1.6.3 and later. NTLMv2 session is supported in1.7.2 and later. **Note** For WebDav it was required to disable FBA. For EWS, FBA needs to be enabled.

Figure 11-15 Configure EWS Window

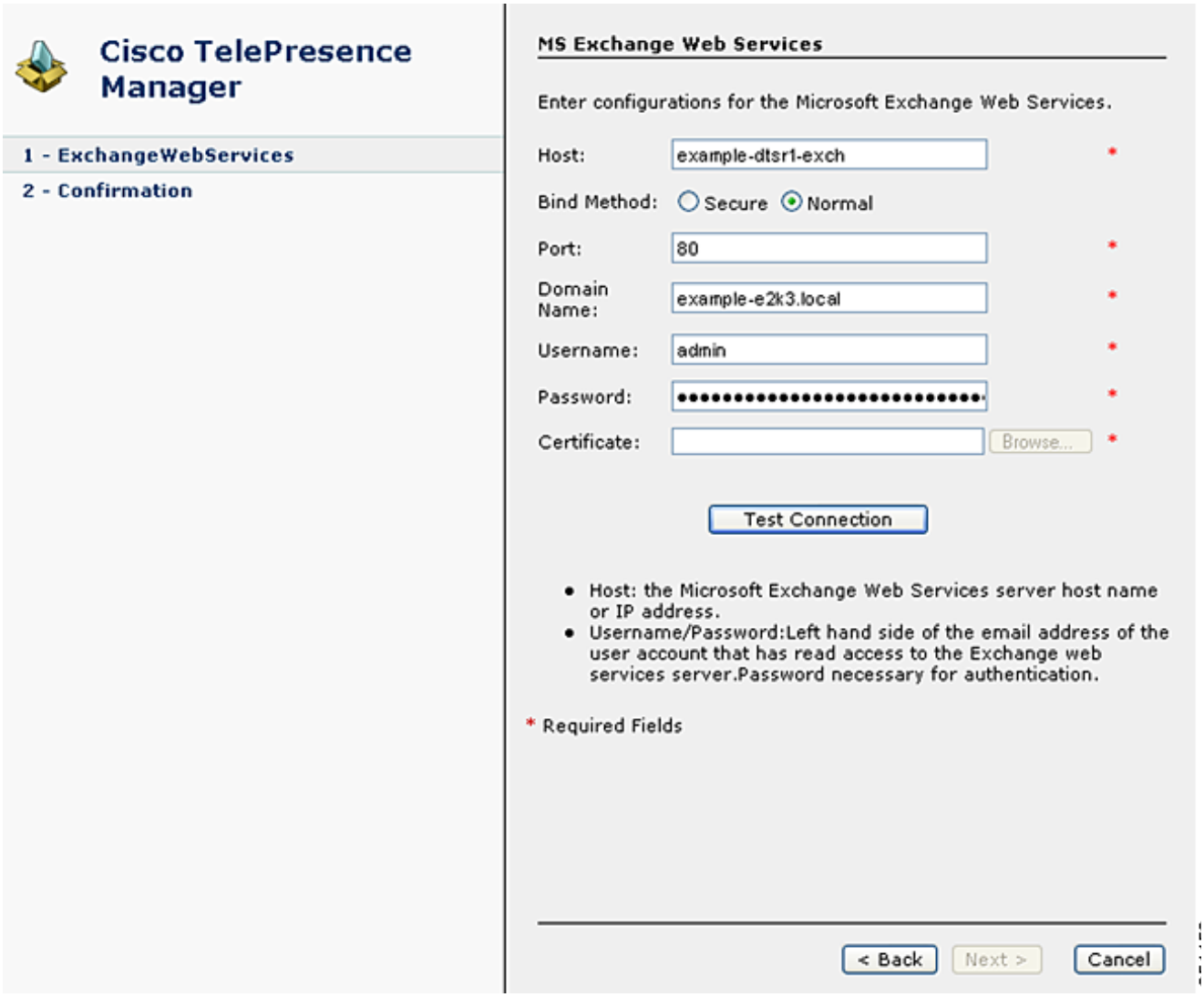


Table 11-10 Microsoft Exchange Web Services Fields

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

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

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

IBM Domino

The IBM Domino window helps you manage the database that stores TelePresence meeting information.

It is divided into two tabs:

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

To test the connection between this system and the Domino server, as shown in Figure 11-16

Step 1 Click **Test Connection.**

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

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

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

Figure 11-16 Configure > IBM Domino > Synchronization tab

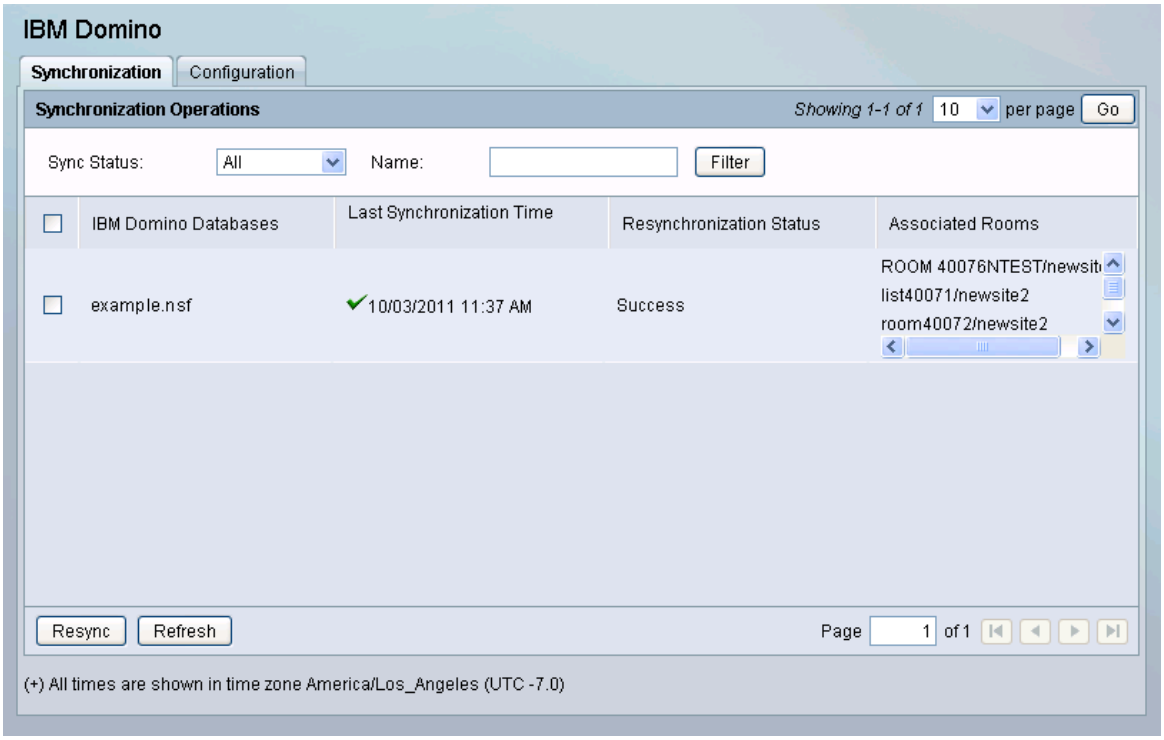


Table 11-12 describes the information and operations accessible from this window.

Synchronization Operations

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

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

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

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

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

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

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

Table 11-11 describes the information displayed in this area of the IBM Domino window.

Table 11-11 IBM Domino Server Synchronization Report

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

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

Figure 11-17 Configure > IBM Domino > Configuration tab

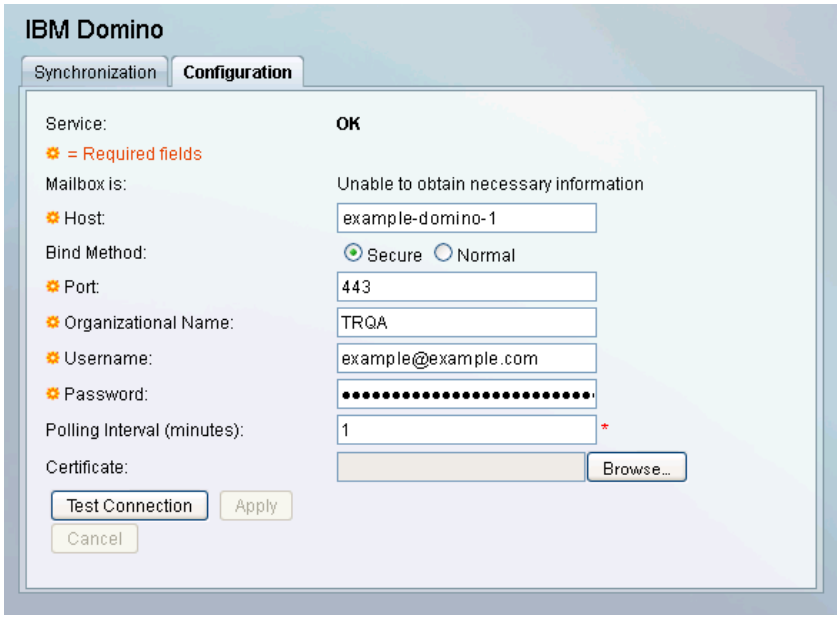


Table 11-12 IBM Domino Server > Configuration fields

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

Table 11-12 IBM Domino Server > Configuration fields

Field or Button	Description or Settings
Bind Method	Choose the Secure or Normal radio button to select the binding method, as follows: • Secure—CTS-Manager communicates with the Domino server in secure mode using HTTP or DIIOP. This method requires enabling Secure Socket Layer (SSL). on the Domino server. • Normal—CTS-Manager communicates with the Domino server in cleartext using HTTP or DIIOP.
Port	Communication port number (HTTP or DIIOP).
Organization Name	Domain name provided for the Domino server account, which can be changed. **Note** Organization Name is case sensitive.
Username	Enter the account name used to log on to the Domino server. The format is determined by the Email ID fields in the Person object classes and attributes.
Password	Password used to access the Domino server account, which can be changed. **Note** Make sure the Internet password is used in the Password fields in the System Configuration> IBM Domino window and the LDAP Server window.
Polling Interval (minutes)	Specifies the time interval, in minutes from 1 to 360, to poll the Domino server for meeting information.
Certificate	Use the field to provide an IBM Domino trust certificate class file. Use the Domino CLI command, **tell diiop show config**, to find the class filename. **Note** A certificate is required in secure mode only.

System Settings

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

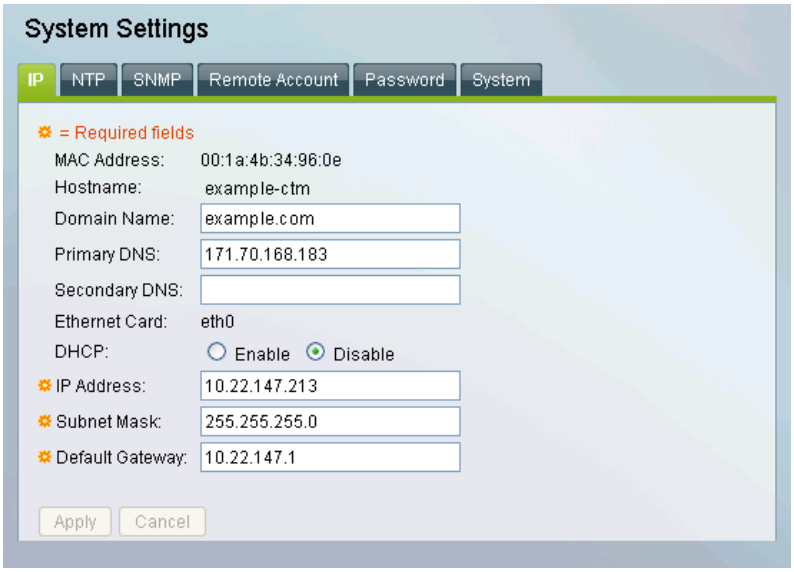
- IP, page 11-39
- NTP, page 11-40
- SNMP, page 11-41
- Remote Account, page 11-46
- Password, page 11-47
- System, page 11-47
- Cluster, page 11-48

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

IP

The IP Setting window lists information that is provided to CTS-Manager during first-time installation and configuration. Although it is typically not necessary to change IP settings, this window offers a place to modify some of them. Figure 11-18 describes the fields and buttons.

Figure 11-18 System Settings > IP Tab



Step 1 To add new information, enter it in the fields provided.

Step 2 To change information, highlight and delete existing information and enter the new information.

Step 3 To register new or modified settings, click **Apply.**

Step 4 To restore the original settings before clicking Apply, click **Cancel**.

Table 11-13 describes the information displayed in this area of the IP Settings window

Table 11-13 IP Settings

Field or Button	Description or Settings
MAC Address	Display-only MAC address number supplied for this Cisco TelePresence Manager.
Hostname	Display-only hostname configured for this Cisco TelePresence Manager. **Note** CTS-Manager hostname needs a DNS entry for email links to it to function properly.
Domain Name	Domain name for this Cisco TelePresence Manager.

Table 11-13 IP Settings (continued)

Field or Button	Description or Settings
Primary DNS	Primary DNS server IP address supplied for this Cisco TelePresence Manager.
Secondary DNS	Secondary DNS server IP address supplied for this Cisco TelePresence Manager.
Ethernet Card	Name supplied for the system Ethernet card.
DHCP	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.
IP Address	IP address supplied for this Cisco TelePresence Manager.
Subnet Mask	Subnet mask used on the IP address.
Default Gateway	Default gateway IP address supplied for this Cisco TelePresence Manager.

Deleting Server

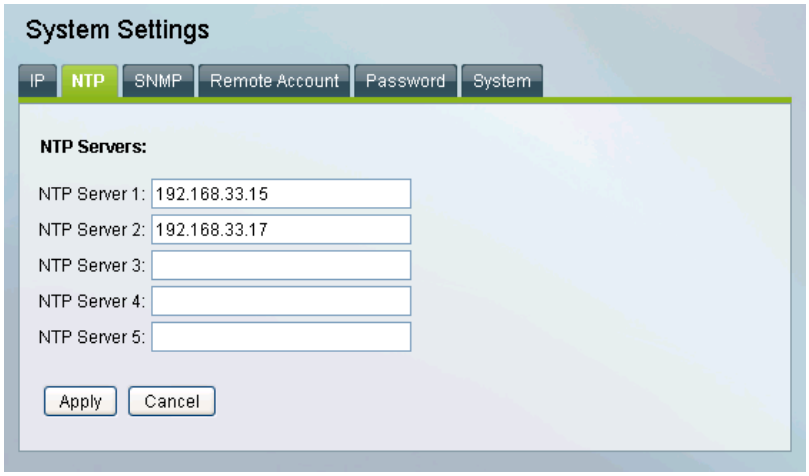
Before performing a delete on a DNS server, it is important to first change existing servers like Unified CM and Conferencing Bridge to IP from hostname before the DNS server is deleted. If the hostname is not changed first, the Unified CM and Conferencing Bridge servers will be put in error status.

NTP

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

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

Figure 11-19 System Settings > NTP Tab



Step 1 To add an NTP server to the configuration, enter the IP address in an NTP Server field.

Step 2 To change an NTP server in the configuration, highlight and delete the IP address in the NTP Server field and enter the new address.

Step 3 To register new or modified settings, click **Apply**.

Step 4 To restore the original settings before clicking Apply, click **Cancel**.

SNMP

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

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

Figure 11-20 System Settings > SNMP Tab

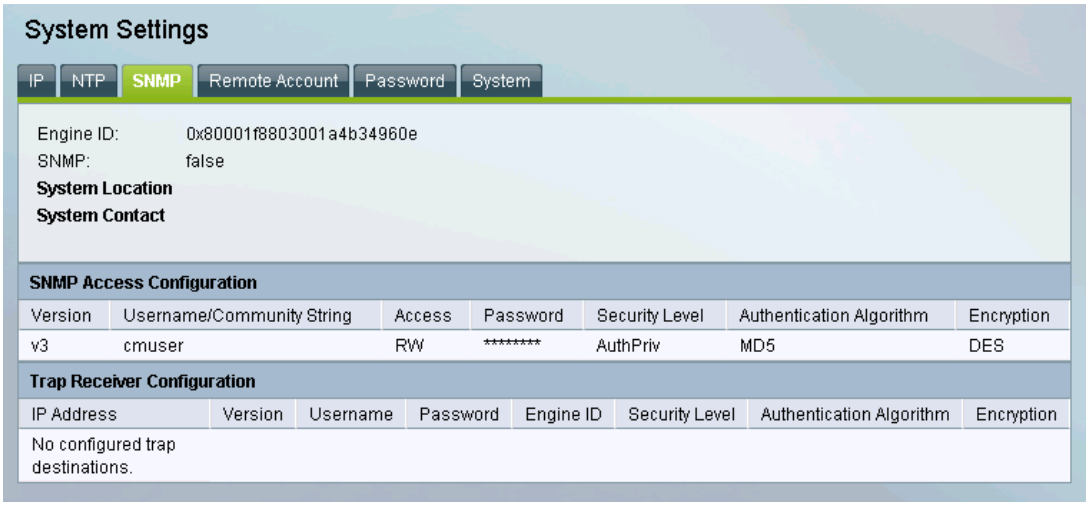


Table 11-14 describes the fields for SNMP settings.

Table 11-14 SNMP Settings

Field	Description or Settings
– Engine ID	The engine ID for the SNMP agent on this CTS-Manager. If you configure the trap receiver, this engine ID is used to create a trap user on the trap receiver system and to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.
– SNMP	The default is disable. To change setting to enable, you must use the CLI **Utility** command. When SNMP is enabled, supply a password for the SNMP server in the **Configuration** area.
SNMP Access Configuration	**Use the CLI 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 default "admin" user with the default password, "snmppassword" must be changed in the new installation. All customer-created SNMP users and trap destinations are migrated to the new installation.

Configuring SNMP Traps on CTS-Manager

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

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

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

Starting the SNMP Service

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

Step 1 Log in to the CTS-Manager CLI.

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

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

Configuring an SNMP User

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

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

set snmp user add v*ersion username access* [*passphrase*] [*level*]

Syntax Description

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

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

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

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

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

Configuring an SNMP Trap Destination

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

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

set snmp trapdest add *version username destination* [*passphrase*] [*level*] [*engineID*]

Syntax Description

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

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

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

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

Enabling CTS-Manager to Send SNMP Trap Notifications

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

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

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

SNMP Trap notifications are now enabled for CTS-Manager.

Modifying SNMP Trap Settings

You can modify existing SNMP trap destinations and user access.

To modify an SNMP trap destination, do the following:

Step 1 Delete the existing trap destination with the command:

set snmp trapdest del

After entering the above command, the CTS-Manager CLI lists all configured SNMP trap destinations and prompts you to specify the trap destination to delete.

Step 2 Configure the new SNMP trap destination with this command:

set snmp trapdest add *version username destination* [*passphrase*] [*engineID*] [*level*]

For details on the syntax, refer to Syntax Description, page 11-44.

The following example configures an SNMP v3 trap destination with the username **testusr**, at host **192.168.180.122**, passphrase **testpass**, and engine ID **0x8000DEECAFE8111BEEFADE**:

```
set snmp trapdest add 3 testusr 192.168.180.122 testpass 0x8000DEECAFE8111BEEFADE
```

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

Step 1 Delete an existing SNMP user with the command:

set snmp user del *version username*

Syntax Description

- *version* is the SNMP version, either 3 or 2c
- *username* is the SNMP username (SNMP v3) or community string (SNMP v2c)

The following example deletes the SNMP v3 user **testusr**:

```
set snmp user del 3 testusr
```

Step 2 Configure the new SNMP user with the command:

set snmp user add v*ersion username access* [*passphrase*] [*level*]

For details on the syntax, refer to Syntax Description, page 11-43.

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

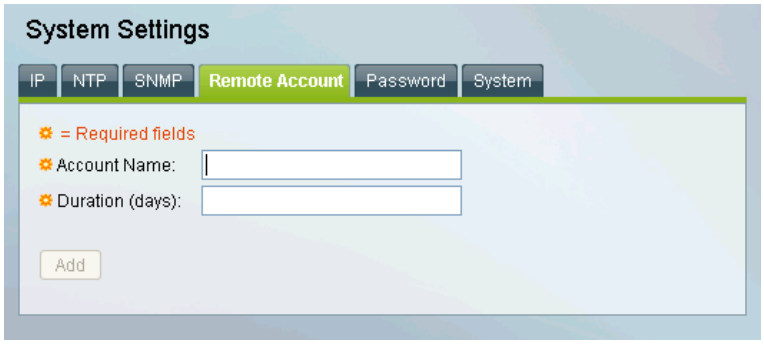
```
set snmp user add 3 newusr rw newpass
```

Remote Account

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

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

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



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

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

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

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

Step 3 Click **Add**.

This step generates a passphrase.

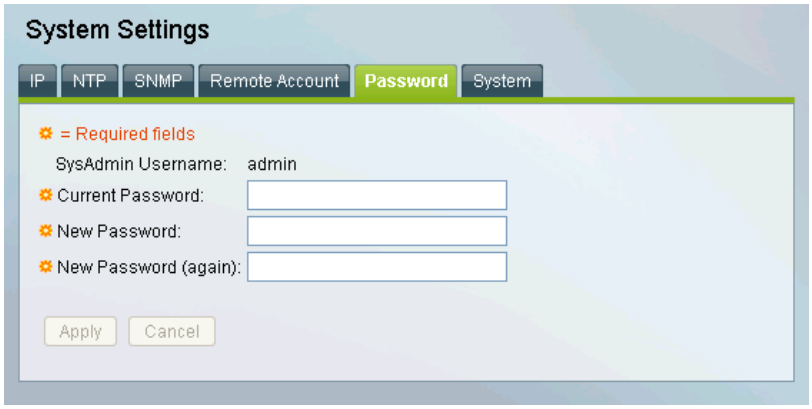
To complete this process, the account name and passphrase are entered into a utility at the following Cisco Internal web site:
https://remotesupporttool.cisco.com/logon.php

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

Password

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

Figure 11-22 Configure > System Settings > Password Tab



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

Step 2 Enter your current password.

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

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

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

Step 6 To restore the original password before clicking Apply, click **Cancel**.

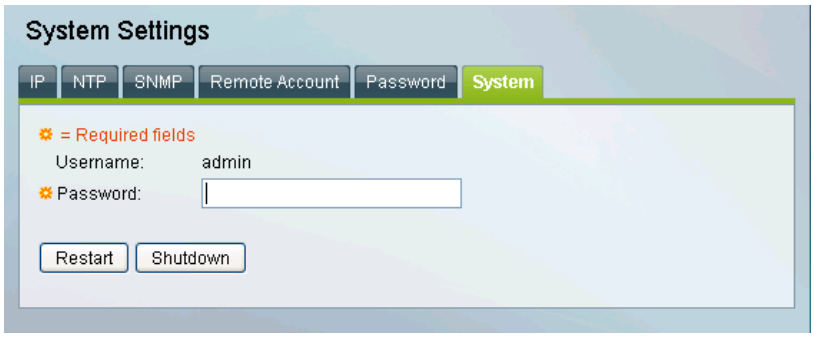
Note Password should contain both upper and lower-case alphabetic and non-alphabetic characters. It should not be similar to the current password or be based on common words found in the dictionary.

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

System

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

Figure 11-23 System Configuration System Settings



Step 1 To restart the system, enter the password.

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

Cluster

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

Database - Status, Backup, and Restore

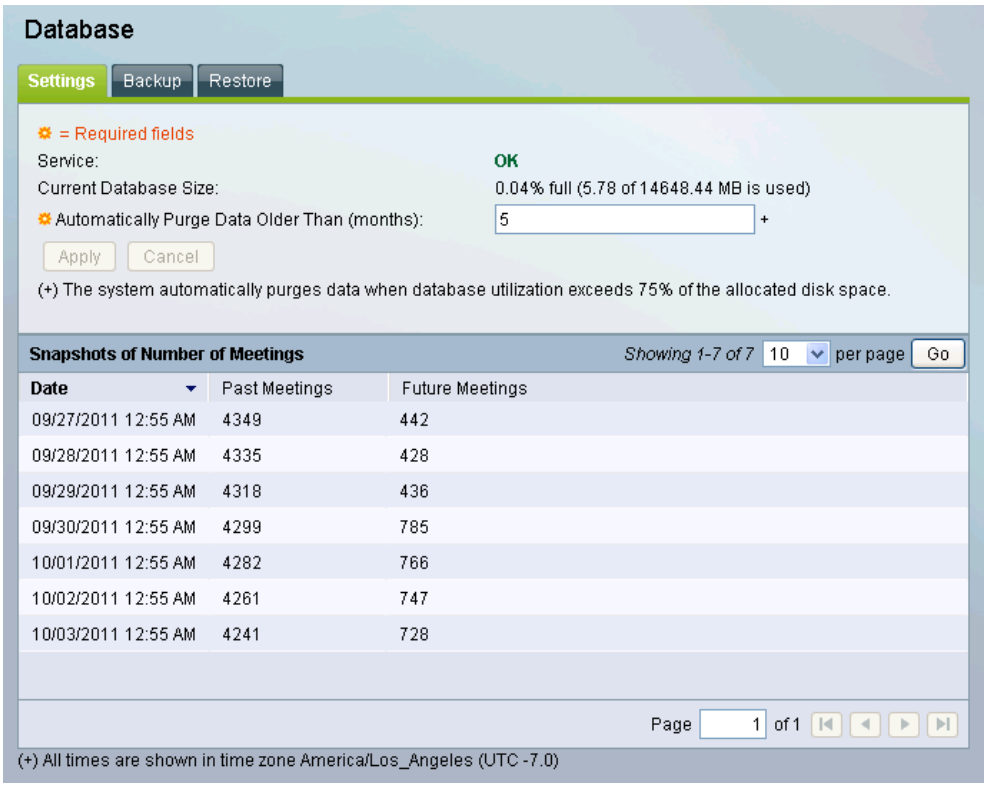
CTS-Manager uses an Informix database server to store information. The Database window allows the Administrator to view the database status and run backup and restore operations. Open the Database window to see the following choices:

- Settings
- Backup
- Restore

Settings

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

Figure 11-24 Database > Settings Tab



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

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

Table 11-15 Database Settings

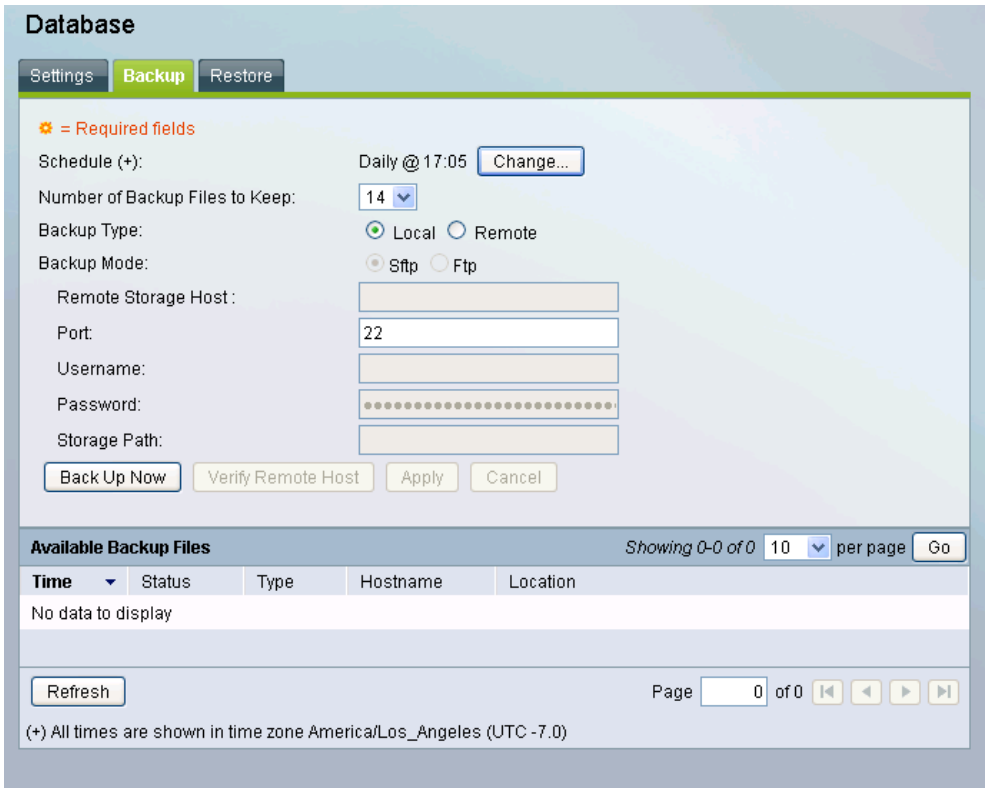
Field	Description or Settings
Service	Display-only status report of the Informix database server.
Current Database Size	Display-only report showing the size of the database as a percentage of the amount of total space available for a Cisco TelePresence Manager account in Directory Server. The number displayed should not exceed 75%.
Automatically Purge Data Older Than (months)	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 11-25 Configure > Database > Backup



Changing the Backup Schedule

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

To change the backup schedule:

Step 1 Click **Change**.

Step 2 Choose the starting time from the Start Time drop-down list. This sets the backup time in your local time zone.

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

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

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

To register new or modified settings, click **Apply.** To restore the original settings before clicking Apply, click **Cancel**.

Note Backup schedules are now displayed in your local time zone.

Backing Up CTS-Manager Data

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

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

To back up files in the database:

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

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

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

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

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

Remote Storage Host Fields

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

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

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

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

Table 11-16 Remote Storage Host Fields

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

Viewing Backup History

The Database window Backup tab provides a history of database backups, in the Available Backup Files section.

Table 11-17 describes the Backup History and Restore History fields.

Table 11-17 Backup History and Restore History Fields

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

Restore

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

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

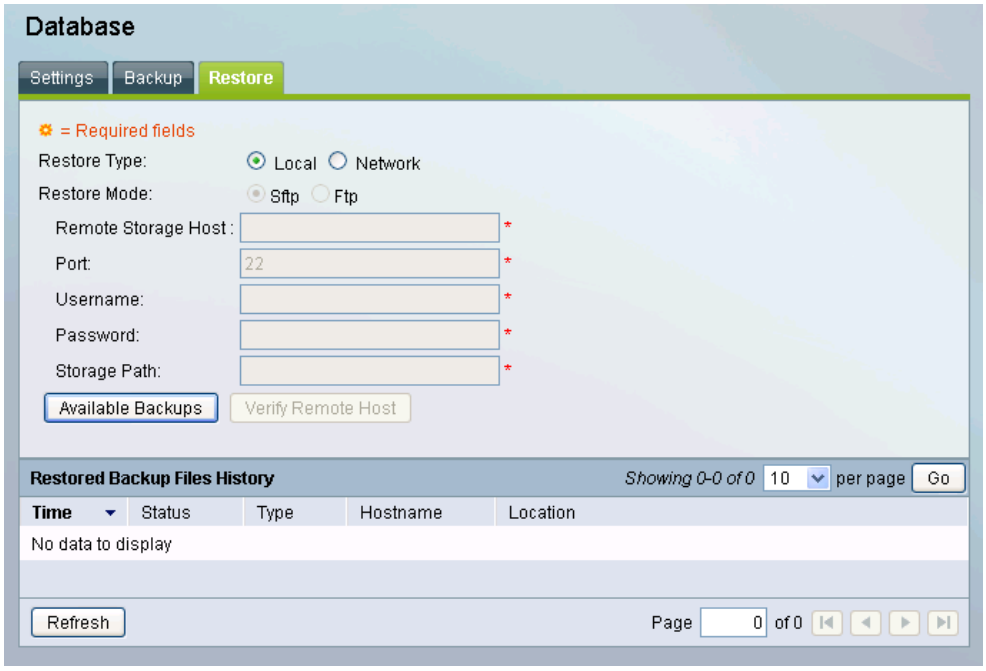
Note CTS-Manager validates license files with system host ID during startup. If a license file does not match the host ID of the system, it is removed and its corresponding feature is in grace period.

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

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

See Table 11-17 for a description of the fields.

Figure 11-26 Configure > Database > Restore Tab



Restoring Backup Data

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

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

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

To restore data from a backup:

Clicking **Available Backups** displays a window listing all the backups stored locally and remotely. If you want to restore from a backup stored remotely you must first click the Network Restore Type radio button. Then choose either the SFTP or FTP Restore Mode and enter required information to access the remote host. See Table 11-16 for a description of the Remote Storage Host fields.

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

Step 1 Click the **Refresh** button to view the list of backups.

Step 2 Click the radio button next to the backup filename that is to be used for the restore operation.

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

Unified CM

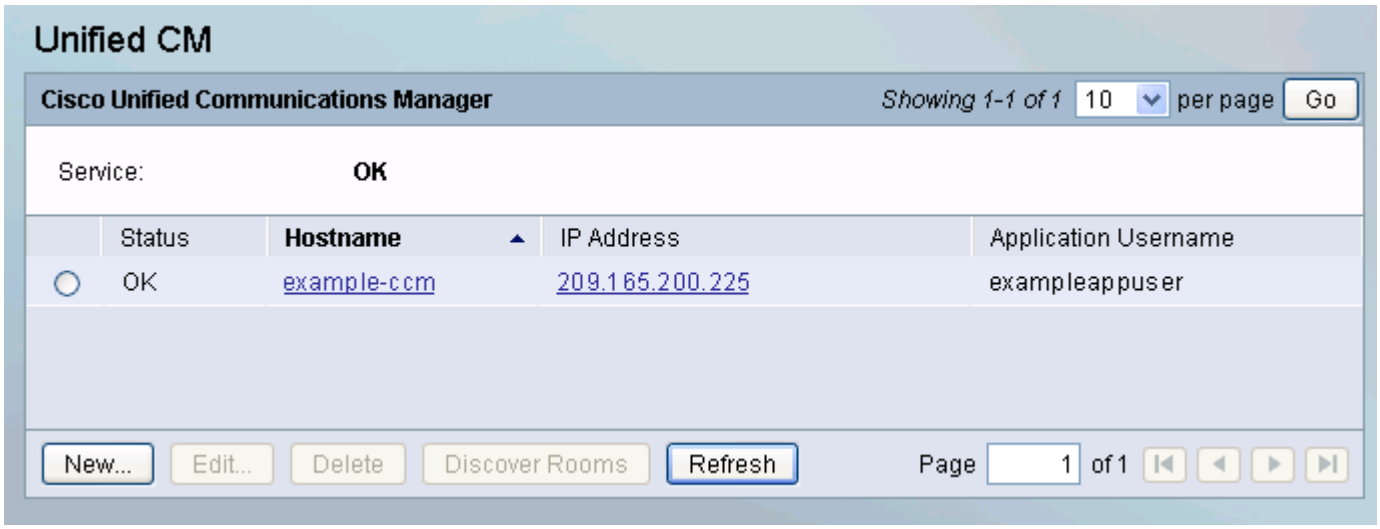
The Configure > Unified CM window displays the settings that associate CTS-Manager with Cisco Unified CM, choose Configure > Unified CM. You can modify these settings.

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

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

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

Figure 11-27 Configure > Unified CM Window



Click the radio button to select a Unified CM server. Once a Unified CM is selected, the buttons on the screen become usable. Refer to Table 11-19 for a description of each button's function.

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

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

Table 11-18 Discover Cisco Unified Communications Manager Settings

Field	Description or Settings
Status	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 (endpoints) are being managed by CTS-Manager. Each time this page is accessed, the status is updated, and the progress indicator will be seen while the system is discovering endpoints. **Caution** An error status is displayed if the connection to the Unified CM server was lost due to a network outage or if the Unified CM server was down during the CTS-Manager maintenance cycle. You can resolve the error status by clicking **Discover Rooms**.
New	This opens the Discovery Service window to add a new Cisco Unified Cm connection.
Edit	This opens the Discovery Service window to correct current settings.
Delete	This deletes the current Cisco Unified CM connection.

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

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

Once you select a record and press **New** or **Edit**, the Unified CM Service window appears as shown in Figure 11-28.

Figure 11-28 Unified CM Service Window

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

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

Table 11-19 describes fields, buttons, and settings.

Table 11-19 Discovery Service Cisco Unified CM Settings

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

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

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

Bridges and Servers

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

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

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

Figure 11-29 Configure > Bridges and Servers

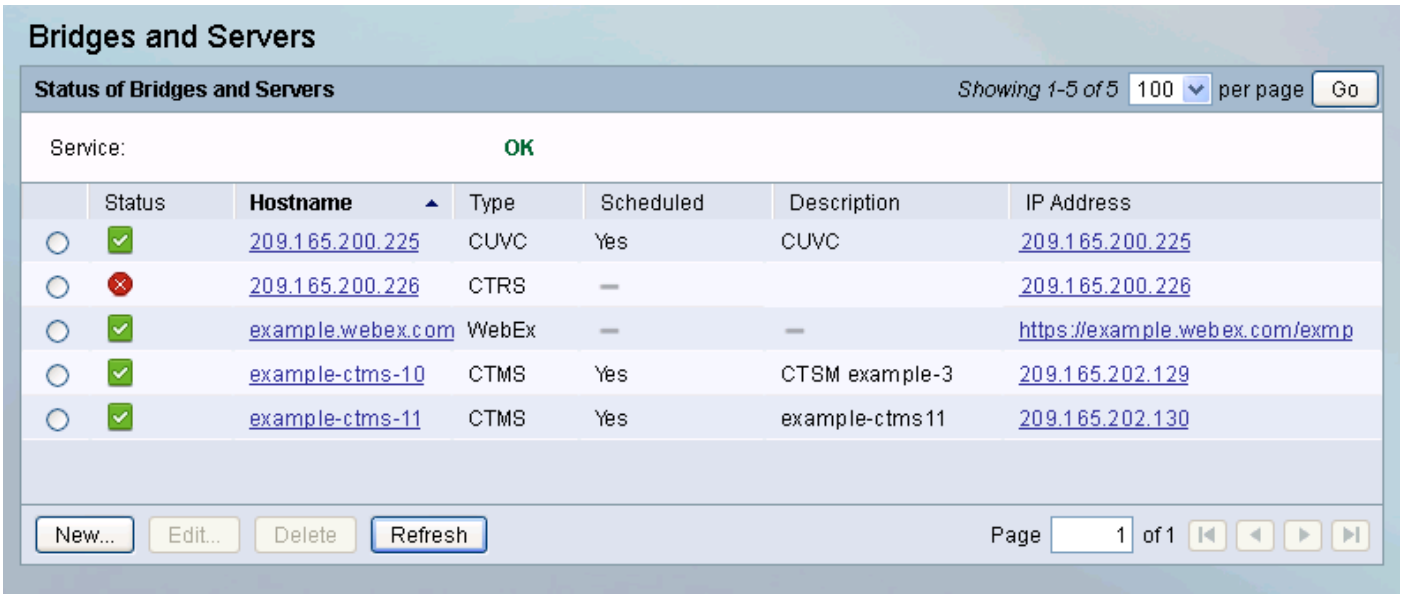


Table 11-20 describes the Bridges and Servers fields.

Table 11-20 Bridges and Servers Devices

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

Adding a Bridge or Server

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

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

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

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

Editing a Bridge or Server

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

Table 11-21 Edit Bridge or Server Devices

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

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

Deleting a Bridge or Server

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

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

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

Migrating All Meetings from a CTMS

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

To migrate all meetings from a CTMS to another CTMS:

Step 1 Click the radio button next to the CTMS from which you want to migrate all meetings.

Step 2 Click **Edit**.

The Edit Bridge or Server window opens.

Step 3 Select **Migrate All Meetings**.

Step 4 Select a CTMS to which to migrate.

Step 5 Click **Save**.

How Meeting Migration Works with CTMSs

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

How device group settings affect meeting migration

1. Default (Ungrouped) device group only

   Migrating individual and all meetings works the same as non-network multipoint meetings.
2. Multiple device groups and Intergroup Scheduling disabled

   Migration destinations must be CTMSs within the same device group
3. Multiple device groups and Intergroup Scheduling enabled

   Migration destinations can be CTMSs in any device group.

How CTMS Network Multipoint settings affect meeting migration

1. CTMS Network Multipoint disabled

   Meeting is cleared from the source CTMS and migrated to the destination CTMS. Endpoints receive updated One-Button-to-Push numbers for the destination CTMS.
2. CTMS Network Multipoint enabled

   Meeting is cleared from the source CTMS and migrated to the destination CTMS. Endpoints receive updated One-Button-to-Push numbers for the destination CTMS.

   – If the source CTMS is a leaf, the RP of the destination is updated to match the source's RP.

   – If the source CTMS is an RP, the leaves are updated with the new RP number of the destination.

   – If the source CTMS is used for the TelePresence Call-In Number, the meeting is updated with the new call-in number of the destination CTMS and a new email is sent to the meeting organizer with the new call-in number.

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

Distributing All Meetings from a TS

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

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

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

Step 1 Click the radio button next to the TS from which you want to migrate all meetings.

Step 2 Click **Edit**.

The Edit Bridge or Server window opens.

Step 3 Select **Distribute All Meetings**.

Step 4 Click **Save**.

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

Example

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

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

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

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

Resource Allocation with CTMS and TS Devices

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

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

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

Refreshing the List of Bridges or Servers

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

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

Cisco TelePresence Multipoint Switch (CTMS)

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

Adding a CTMS

To add a CTMS device to Cisco TelePresence Manager:

Step 1 Go to the Configure > Bridges and Servers window.

Step 2 Click **New** to display the New Bridge or Server dialog box.

Step 3 Choose CTMS from the Type drop-down field.

Step 4 Enter the information, click **Save**.

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

Figure 11-30 Adding a CTMS Device

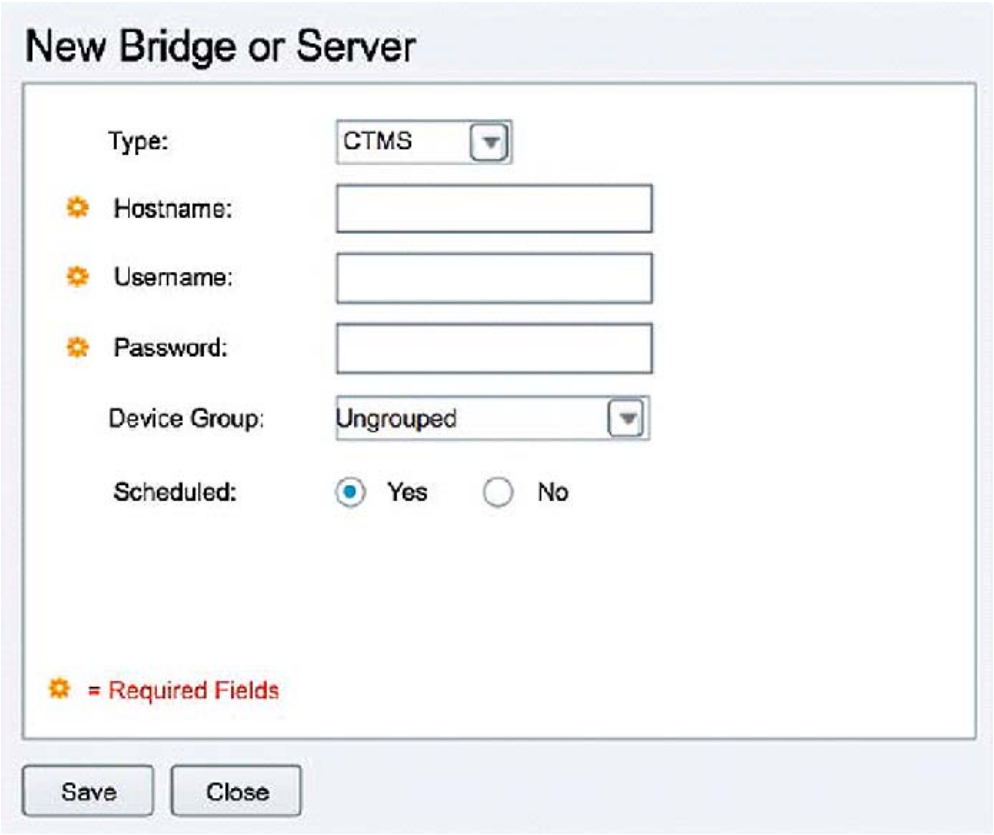


Table 11-22 Adding a CTMS Device

Field	Description or Settings
Type	Select CTMS from this pull-down list menu.
Hostname	The hostname or IP address of the CTMS. This is the LHS of the complete Host name.
Username	This is the account name used to log into the CTMS.
Password	This is the account password used to log into the CTMS.
Device Group	Select the group to which you want to assign the CTMS. If you do not select a group, you can do it later in the Configure > Device Groups page.
Scheduled	Choose either **Yes** or **No**, to specify whether the CTMS is available (scheduled) for meetings. The resources of a scheduled CTMS can be used when meetings are scheduled. Specifying a CTMS as Non-Scheduled means the CTMS will not be used when a meeting is scheduled. CTMS devices in a Scheduled state cannot be used to migrate meetings from other CTMS devices. ⚠ **Caution** When a CTMS is in a scheduled state, CTS-Manager schedules its resources, even if it is in an error state. When a CTMS is in a error state, scheduled meetings will fail. The only way to disable scheduling of a CTMS is to set Scheduled to **No**.

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

Cisco TelePresence Server (TS)

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

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

Adding a Cisco TelePresence Server

To add a Cisco TelePresence server to Cisco TelePresence Manager:

Step 1 Go to the Configure > Bridges and Servers window.

Step 2 Click **New** to display the New Bridge or Server window.

Step 3 Choose **TelePresence Server** from the Type drop-down field.

Step 4 Enter the information, click **Save**.

Step 5 Click **Refresh** to display the new TS in the Configure > Bridges and Servers window.

The new TS is displayed in the Configure > Bridges and Servers window.

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

Step 6 To verify the TS you just added configured correctly, select it and click the Edit button.

Segment Count should display the total capacity of ports on the TS.

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

Figure 11-31 Adding a TelePresence Server

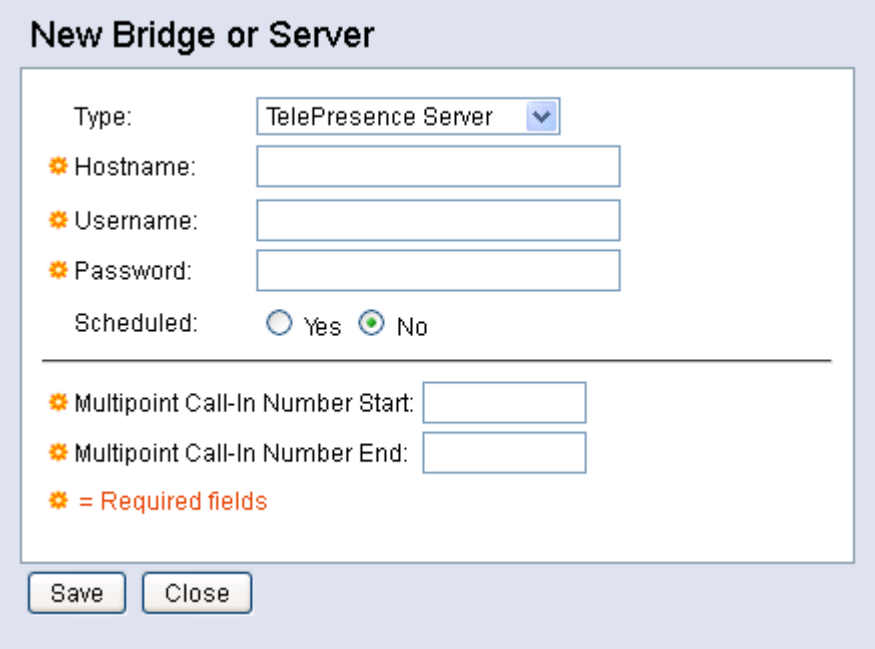


Table 11-23 TS Device Information

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

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

Multipoint Call-In Numbers on the TelePresence Server

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

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

Cisco TelePresence Recording Server (CTRS)

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

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

Adding a CTRS Device

To add a CTRS to Cisco TelePresence Manager:

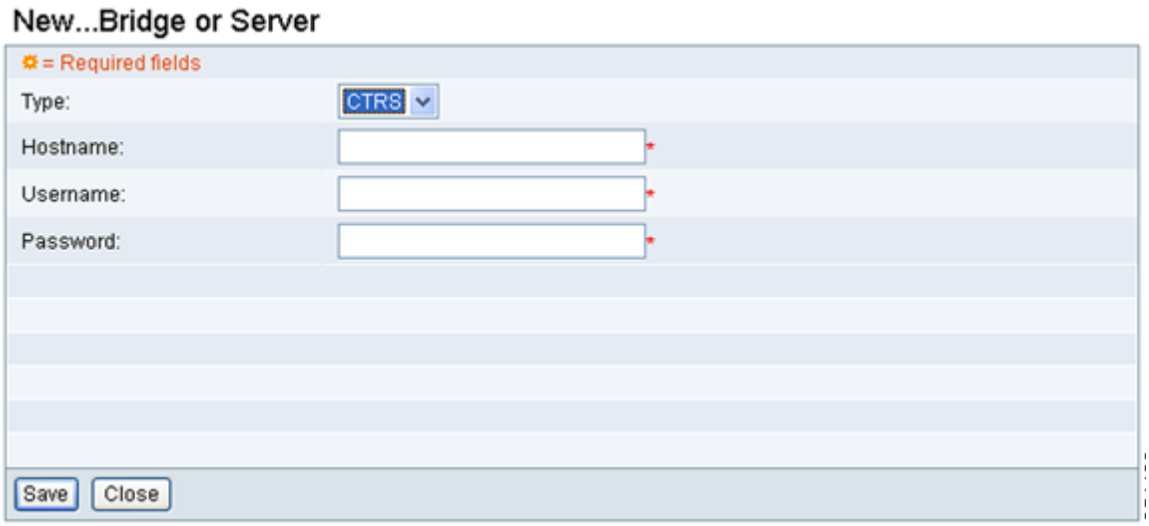
Step 1 Click **New** to display the Registration dialog box.

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

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

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

Figure 11-32 Adding a CTRS Device



WebEx

Table 11-24 Adding a CTRS Device

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

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

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

Chapter 12, "Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager".

Multiple WebEx Sites

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

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

First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15.

WebEx Proxy Server

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

The following modes of proxy connection are available:

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

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

Adding a WebEx Site

To add a WebEx site to Cisco TelePresence Manager:

Step 1 Go to the Configure > Bridges and Servers window.

Step 2 Click New to display the New... Bridges or Servers dialog box.

Step 3 Choose **WebEx** from the Type drop-down field.

Step 4 Enter the information and click **Test**.

A message appears indicating the connection to the server is verified.

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

Step 5 Click **Save**.

The New Bridge or Server window closes.

Step 6 Click the **Refresh** button.

The newly added WebEx site displays a status of "OK."

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

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

Figure 11-33 Adding a WebEx Site

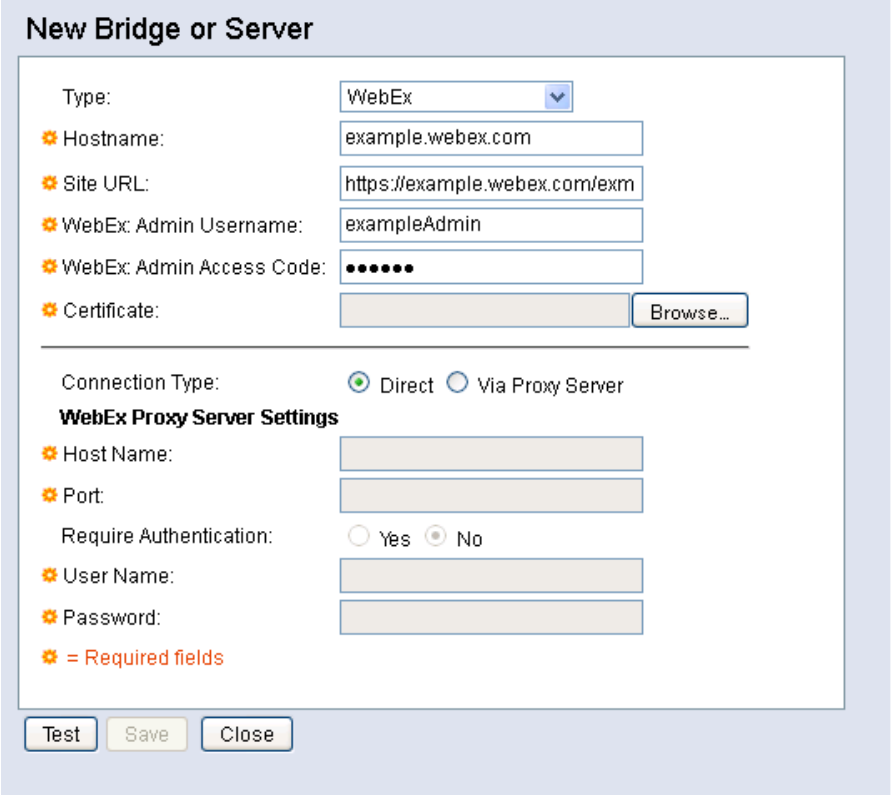


Table 11-25 WebEx Site Information

Field	Description or Settings
Type	Select WebEx from the pull-down list menu.
Hostname	A name identifying the WebEx site hostname to the administrator. This typically can be the same name as the hostname used in the site URL. **Note** Multiple WebEx sites can have the same hostname. This is not used to connect to the WebEx site and therefore is not validated during testing of connection.
Site URL	The address used to construct the URL that's used to access this meeting. This is the actual URL that CTS-Manager uses to communicate with WebEx. This is published in the email from CTS-Manager, and is displayed to users on the WebEx page of the CTS phone UI.
WebEx Admin Username	WebEx administrator's username (provided by the WebEx team)
WebEx Admin Access Code	WebEx administrator's access code (provided by the WebEx team)
Certificate	Certificate from the hostname (WebEx scheduling server) **Note** To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer. Then click Browse to select it and upload it to CTS-Manager. The certificate is required because communication with the WebEx site must use HTTPS. For detailed instructions on downloading the certificate with different browsers, see First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15.
Connection Type	Choose the type of connection to establish with the WebEx scheduling server: **Direct** or **Via Proxy Server**. Selecting the proxy server option allows you to filter IP traffic and increase security.
WebEx Proxy Server Settings	
Host Name	Host name of proxy server
Port	Port number of proxy server
Requires Authentication	Select Yes if the proxy server requires authentication and then enter username and password.
Username	Username for proxy server
Password	Password for proxy server

Deleting a WebEx Site

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

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

To delete a WebEx site:

Step 1 Select the WebEx site.

Step 2 Click **Delete**.

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

Collaboration Manager

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

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

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

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

Step 2 Select a meeting.

Step 3 Click **Open Collaboration Manager**.

Figure 11-34 Adding a Collaboration Manager

Table 11-26 Adding a Collaboration Manager

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

Cluster Management

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

Access Management

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

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

Meeting Extension Premium User

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

WebEx Roles

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

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

Reporting API User

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

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

Assigning Roles to Groups Using Domino Directory Assistance

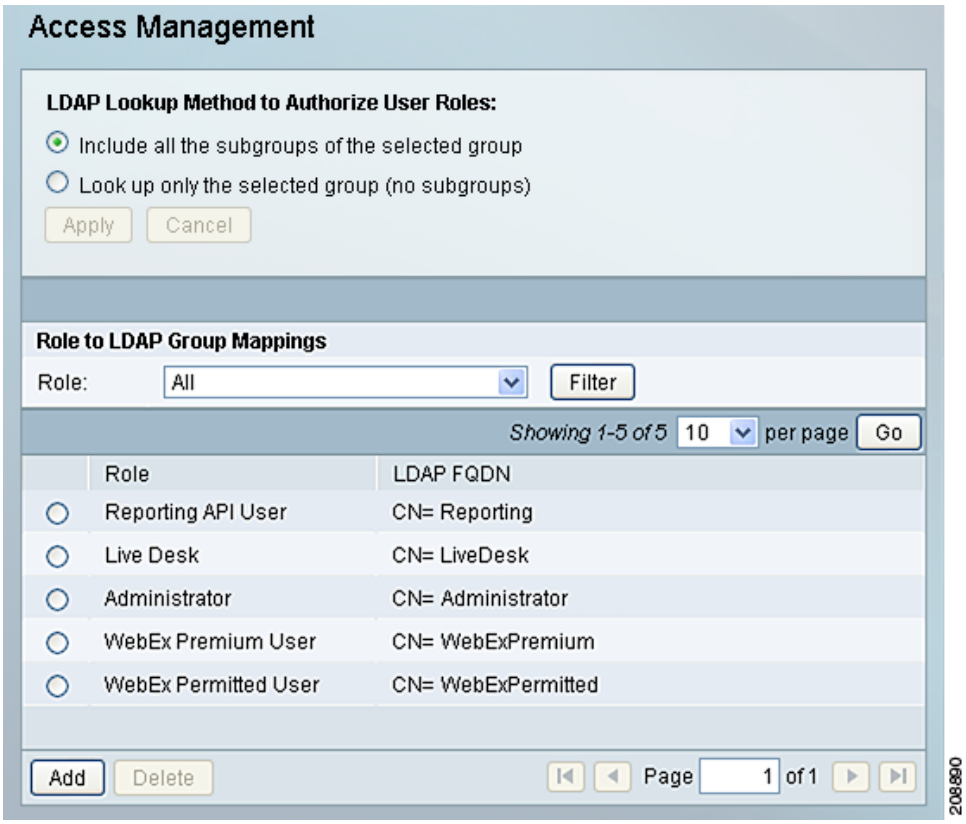
If your Cisco TelePresence Manager deployment is working with an IBM Domino Server and Domino Directory Assistance, it is possible for the group to contain a user from an external directory. That type of external user cannot be granted the role of CTS-Manager Administrator. Only members of groups local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

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

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

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

Figure 11-35 Access Management Window



LDAP Lookup Method to Authorize User Roles

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

Group Level options:

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

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

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

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

Adding an LDAP Group to a Role

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

Step 1 In the Access Management window, click **Add**.

The LDAP Tree Selector window appears, as shown in Figure 11-36.

Step 2 Select a role from the Role drop-down menu

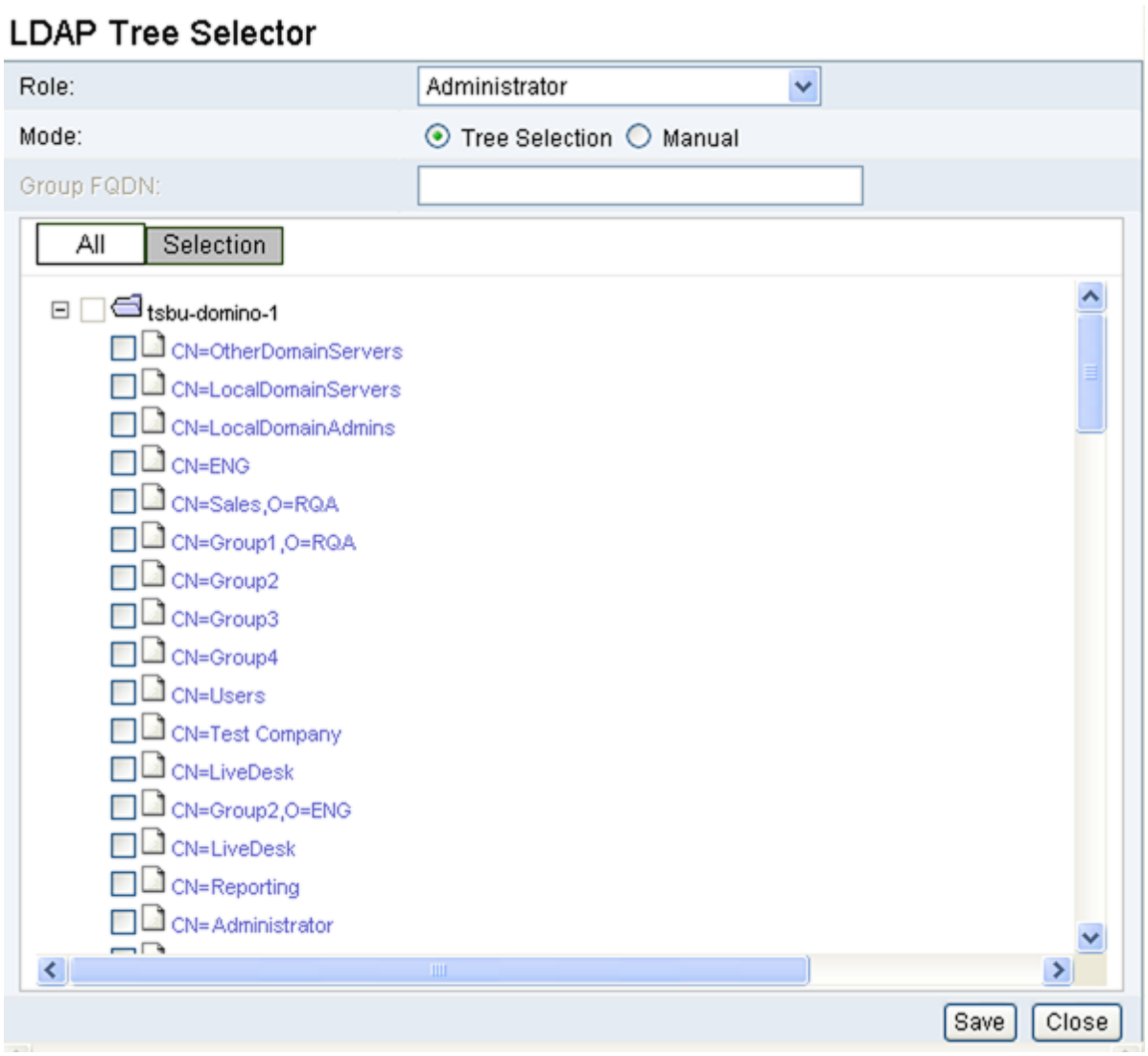
Step 3 For Mode, click the Tree Selection radio button if you want to select an LDAP group from the list of all LDAP groups, or click the Manual radio button if you want to enter a specific group name in the FQDN text field.

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

Step 4 Click **Save**.

The newly added role appears in the Access Management window.

Figure 11-36 LDAP Tree Selector



Alert Management

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

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

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

CTS-Manager sends alert emails under the following circumstances:

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

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

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

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

Table 11-27 Storage Parameters

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

Table 11-28 System Parameters

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

Device Groups

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

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

Note It is not required to create device groups.

Grouping Devices

To group devices, do the following:

Step 1 Log into the CTS-Manager Administrative UI.

Step 2 Go to **Configure > Device Groups**.

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

The New Group window appears.

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

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

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

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

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

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

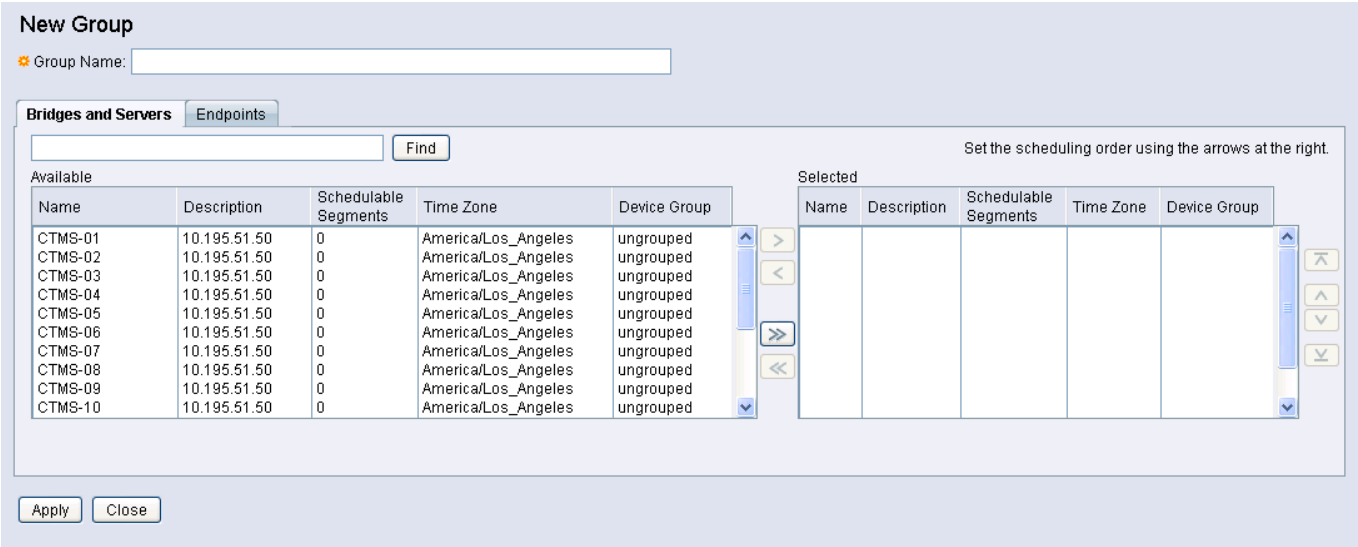
Tip The scheduling order allows you to prioritize the order in which CTS-Manager attempts to schedule CTMS resources. The CTMS at the top of the Selected list will be used first, followed by each CTMS in order from top to bottom. Scheduling order is followed on a best effort basis.

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

Figure 11-37 displays a sample New Group window.

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

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



Editing Groups

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

To edit a device group, do the following:

Step 1 Log into the CTS-Manager Administrative UI.

Step 2 Go to **Configure > Device Groups**.

Step 3 In the List of Device Groups section, select the group that you want to edit.

The list of devices in the selected group appears in the bottom half of the page.

Step 4 Click **Edit**.

The Edit Group window appears.

Step 5 Modify the name, add, remove or order devices following the steps in Grouping Devices, page 11-78.

Deleting Groups

To delete a device group, do the following:

Step 1 Log into the CTS-Manager Administrative UI.

Step 2 Go to **Configure > Device Groups**.

Step 3 In the List of Device Groups section, select the group that you want to delete.

The list of devices in the selected group appears in the bottom half of the page.

Step 4 Click **Delete**.

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

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

Endpoints

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

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

Registering EX, MX or C-series Endpoints

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

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

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

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

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

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

Figure 11-38 Configure > Endpoints

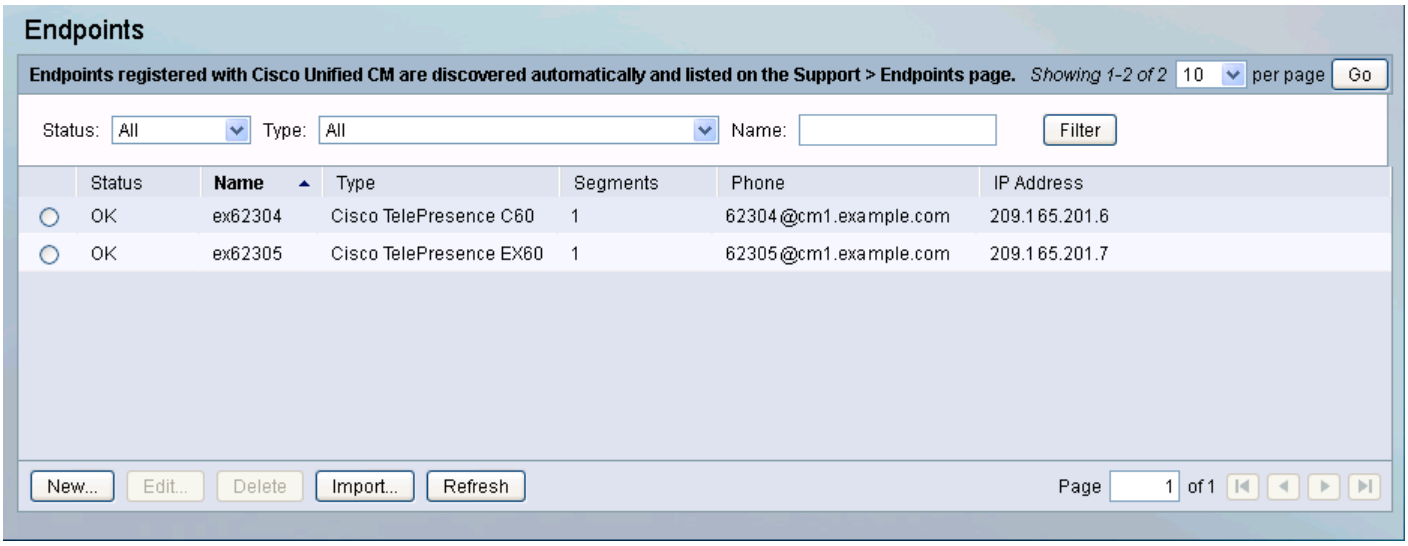


Table 11-29 Configure > Endpoints Information

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

To add an endpoint to Cisco TelePresence Manager:

Step 1 Go to the **Configure** > **Endpoints** window.

Step 2 Click **New** to display the New Endpoint dialog box.

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

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

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

Table 11-30 Endpoint Settings

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

Table 11-30 Endpoint Settings

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

Figure 11-39 Video Conferencing Endpoint

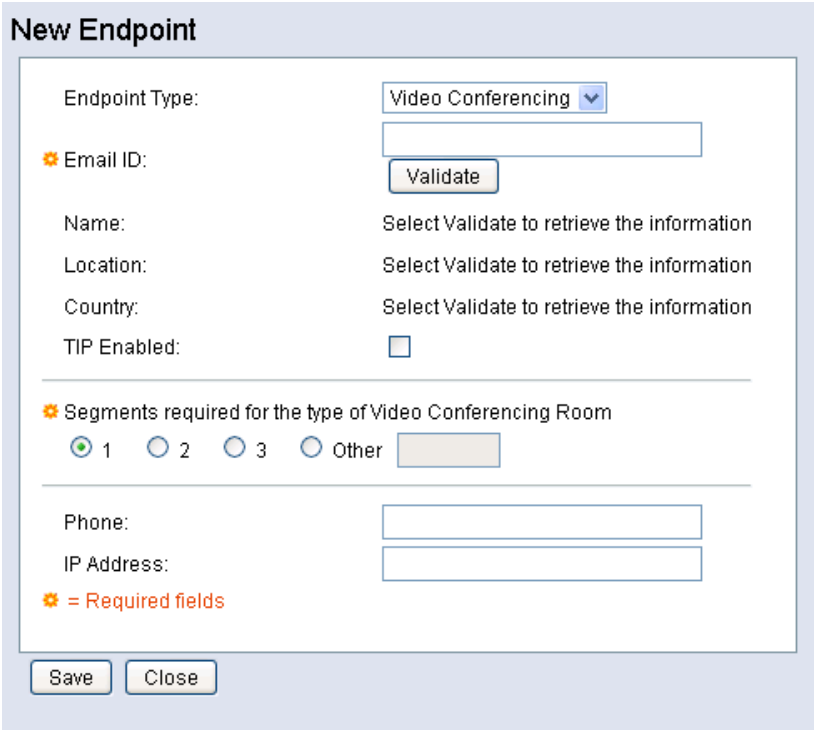


Figure 11-40 EX or C-Series Endpoint

Importing Endpoints

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

To import endpoints:

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

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

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

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

Step 2 Click **Import**.

The Import window appears.

Step 3 Click **Browse**.

The Choose file window appears.

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

Step 5 Click **Upload**.

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

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

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

Creating Resource Bundle Endpoints

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

Note A resource bundle endpoint consumes only one endpoint license.

To add a resource bundle endpoint to Cisco TelePresence Manager:

Step 1 Go to the Configure > Endpoints window.

Step 2 Click **New** to display the New Endpoint dialog box.

Step 3 For Endpoint Type, select **Video Conferencing**.

Step 4 In the Email ID field, enter a valid email address to be used exclusively by this resource bundle endpoint.

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

Step 5 In the Segments required for the type of Video Conferencing Room field, select or enter the number of desired segments.

Step 6 (Optional) Enter Phone and IP address.

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

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

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

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

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

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

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

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

Step 1 Invite TelePresence endpoints and VC/EX/C series endpoints through Outlook or Lotus Notes, and wait for the confirmation email.

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

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

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

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

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

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

- No VC Interop tab is displayed in the Meeting Details window for the meeting.
- You cannot change the number of video conferencing end points joining the meeting from the Meeting Details window.
- In the Summary tab of the Meeting Details window:
  - A green checkmark appears next to Video Conferencing Interop.
  - If a VC endpoint is added after upgrading to 1.7 or 1.8, a blue icon appears next to the VC endpoint name.
  - Interop meetings scheduled in 1.7 or 1.8 have both the VC Room icon and the Video Conferencing Interop checkmark.

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

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

Live Desks

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

Live Desk Role

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

- System Status
- Monitor
- Support
- Troubleshooting

The Live Desk understands how to perform the following tasks:

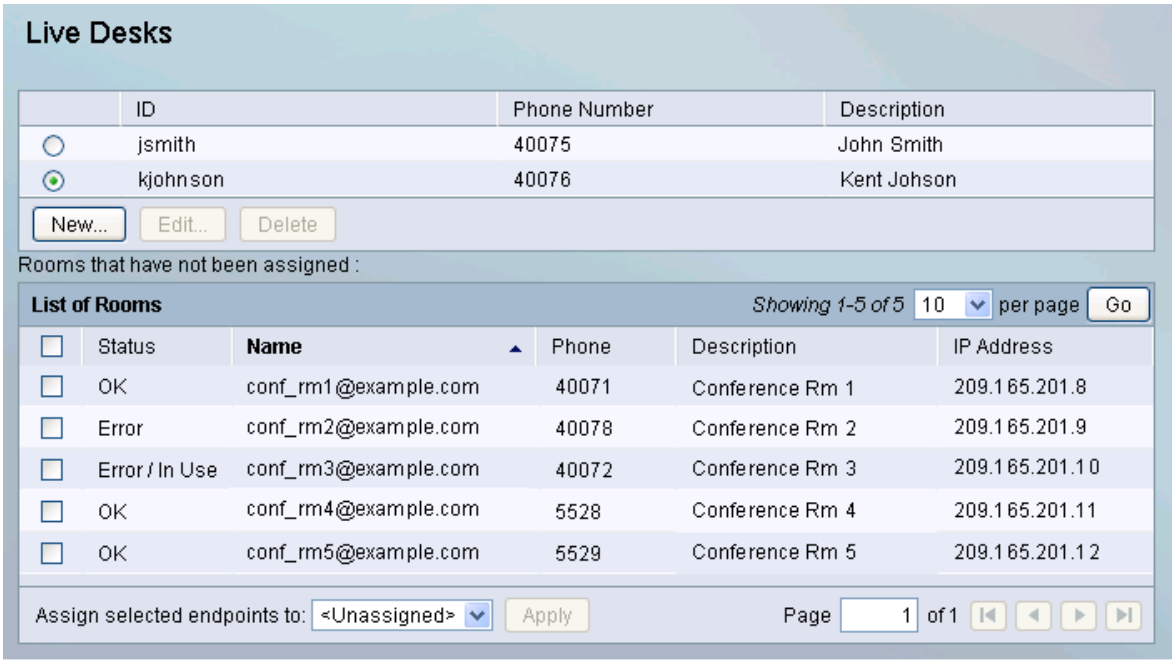
- Scheduling meetings
- Using the Cisco IP phone in a Cisco TelePresence-enabled endpoint
- Using the tools supplied by the CTS-Manager to monitor the system and the schedule of upcoming meetings and to update meeting requests
- Gathering data to supply to the administrator when a problem cannot be easily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

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

The Live Desks window has two areas, a list of Live Desks and a list of rooms (endpoints) that need a Live Desk assigned to them. Use the areas in this window to assign a Live Desk to an endpoint.

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

Figure 11-41 Configure > Live Desks Window



Creating Live Desk Personnel

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

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

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

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

Step 3 Enter a phone number in the Phone Number (Live Desk Number) field.

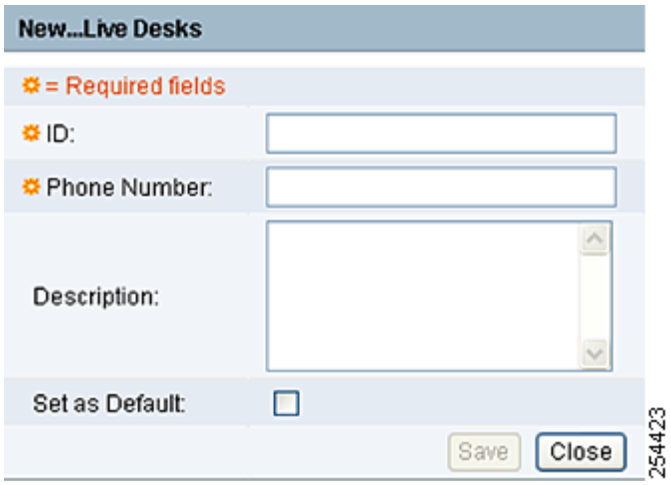
Step 4 You can choose to supply other information identifying the Live Desk person in the Description field.

Step 5 Click **Save** and then click **OK** in the confirmation window that appears.

Step 6 To see the new Live Desk you added, you must refresh the page.

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

Figure 11-42 Adding a Live Desk Window



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

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

Assigning an Endpoint to a Specific Live Desk

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

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

Step 2 Select a Live Desk from the **Assign Selected Rooms** drop-down list, at the bottom of the page.

Step 3 Click **Apply**.

To edit the Live Desk assignment:

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

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

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

Note Beginning in release 1.7, CTS-Manager supports a default Live Desk that is assigned to TelePresence rooms (endpoints) that have no specific Live Desk assignment. Earlier versions of CTS-Manager allowed more than one Live Desk to have the same phone number. If you are upgrading to version 1.9 from a version (earlier than 1.7) that allows a Live Desk to share a phone number with another Live Desk, CTS-Manager 1.9 changes the phone number of one of the Live Desks during the upgrade and assigns that Live Desk to the TelePresence room (endpoint).

Policies

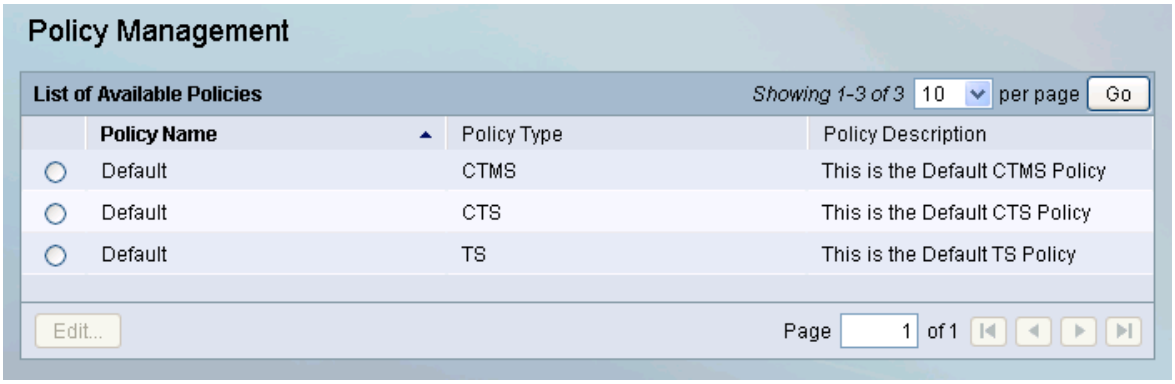
The Policies window lists the three available default policies that support scheduling and conference termination in CTS-Manager.

To edit a policy:

Step 1 Select the radio button next to the policy you want to edit and click **Edit**.

Step 2 Make changes to the policy and click **Save**.

Figure 11-43 Configure > Policies Window



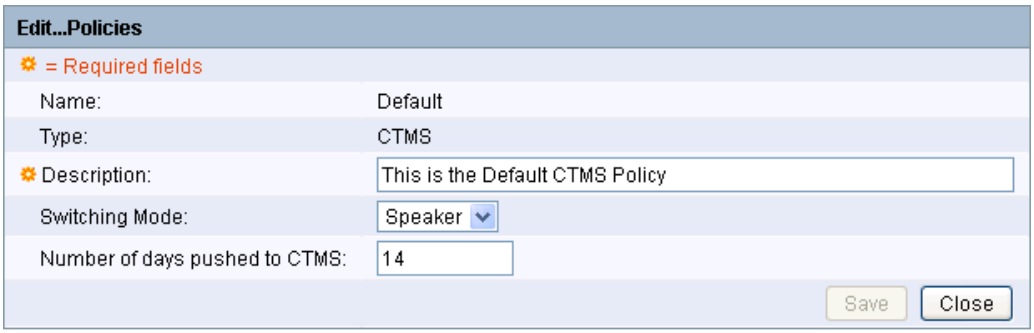
CTMS Policy

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

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

You also use the policy management window to set the number of scheduled meetings pushed to CTMS devices. The default is to push 14 days of meetings, the range is 1 to 30 max.

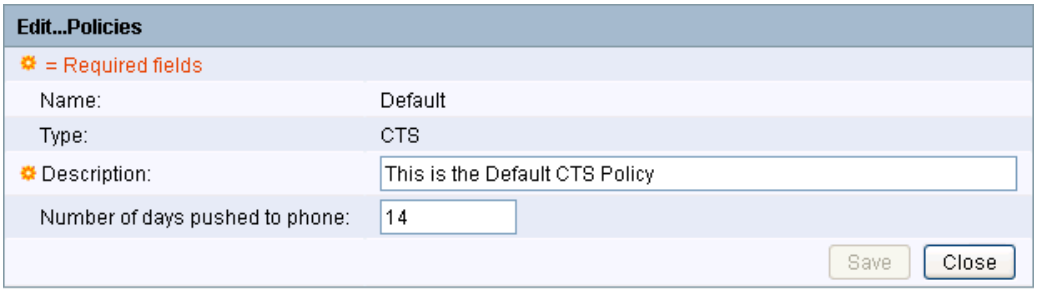
Figure 11-44 CTMS Policy Window



CTS Policy

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

Figure 11-45 CTS Policy Window

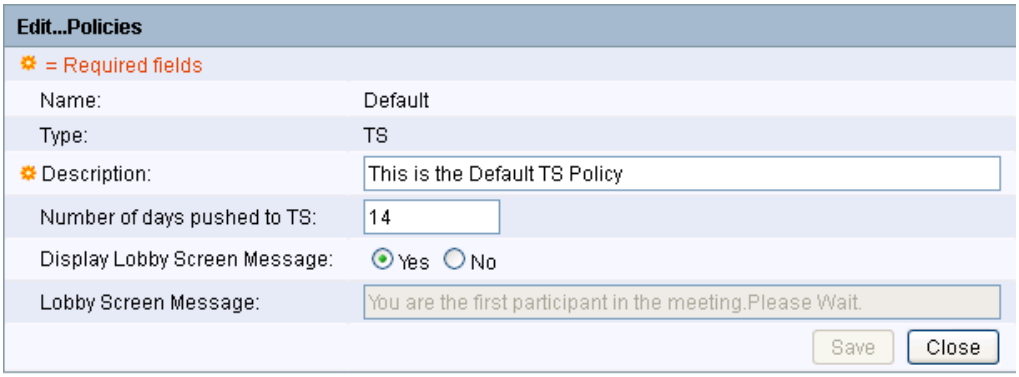


TS Policy

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

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

Figure 11-46 TS Policy Window



Application Settings

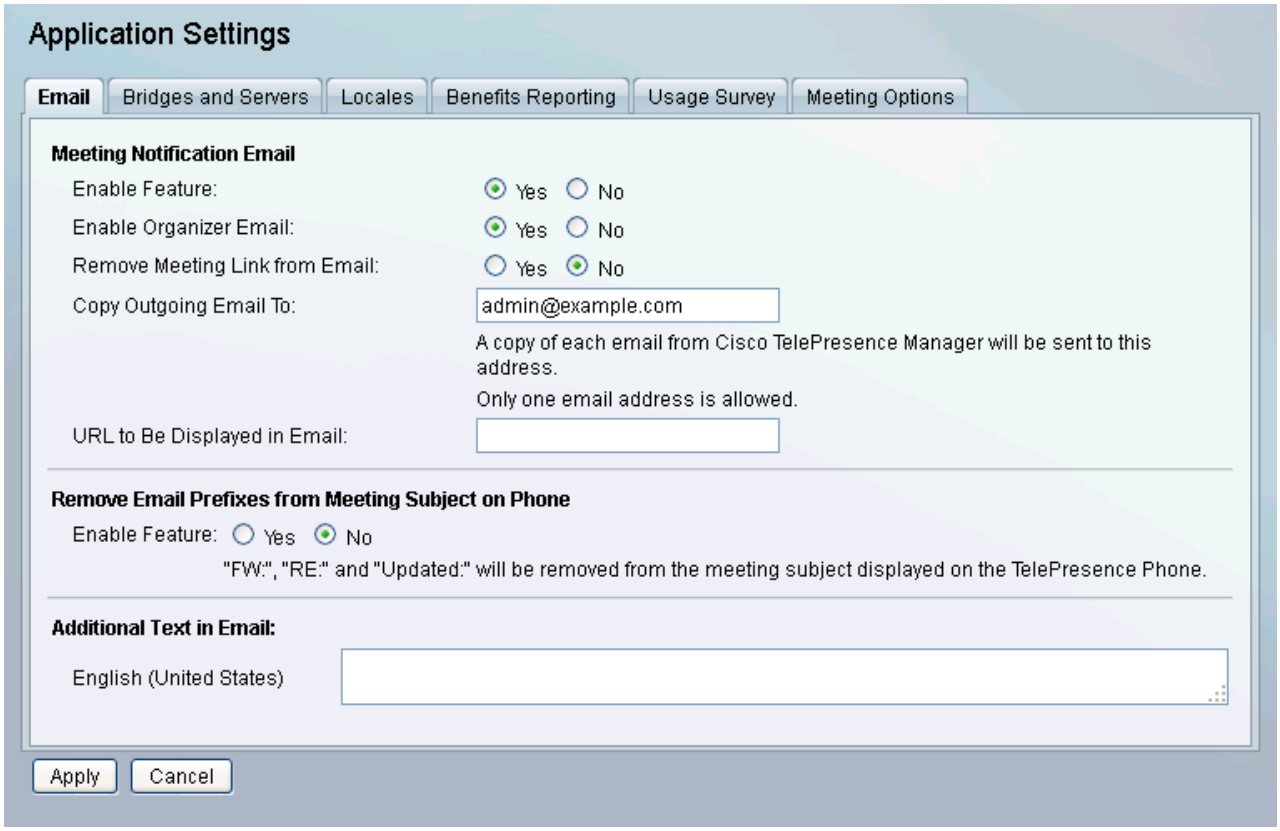
The Configure > Application Settings window is used to configure a variety of TelePresence meeting settings. It is organized into the following tabs:

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

Email

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

Figure 11-47 Configure > Application Settings > Email Window



Meeting Notification Email

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

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

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

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

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

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

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

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

Remove Email Prefixes from Meeting Subject on Phone

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

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

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

Additional Text in Email

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

System Alert Notification Emails

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

No-Show Meetings and Meetings without Survey Responses

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

Mailbox Alert

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

Certificate Expiry

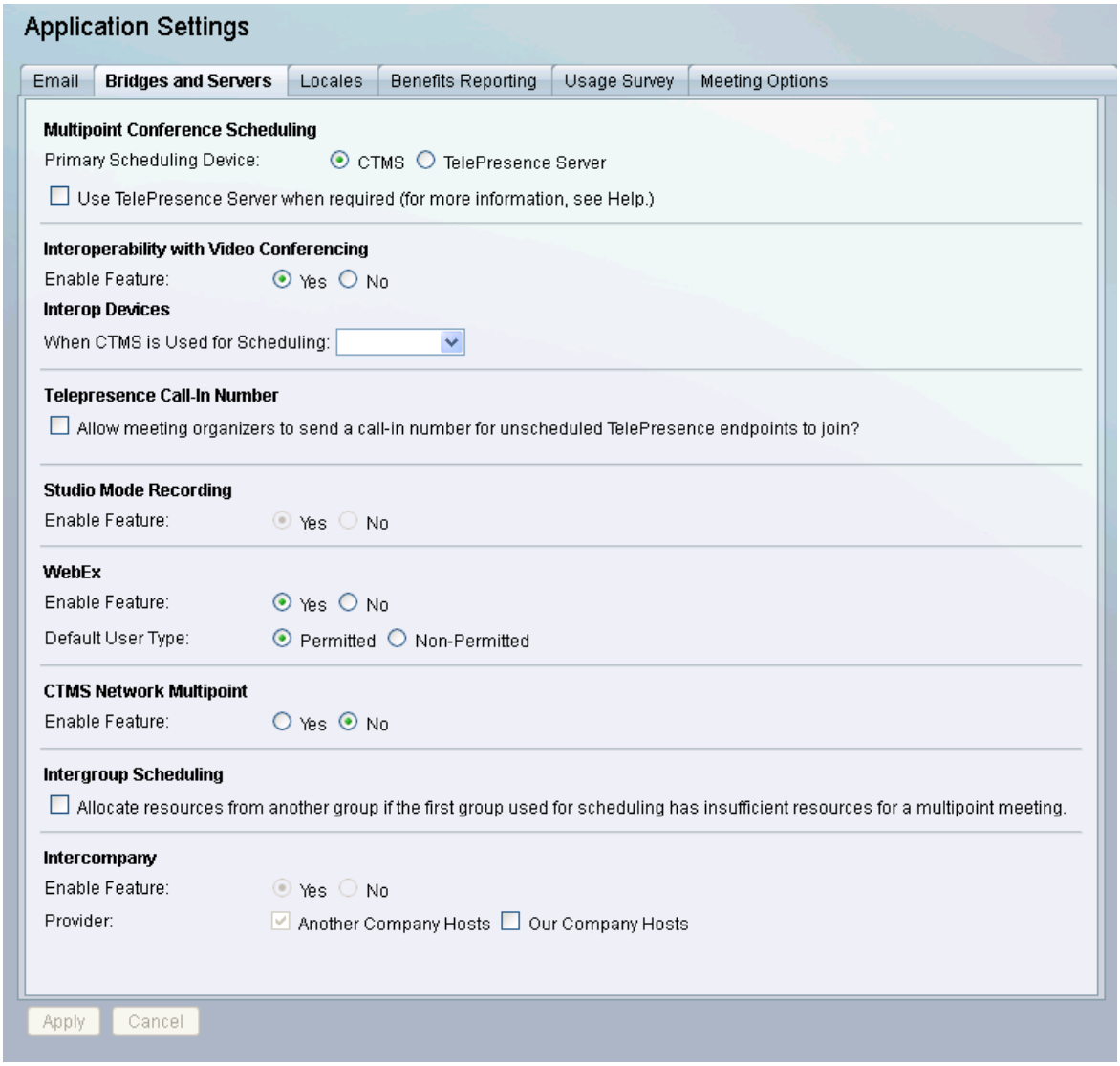
- Security certificates that are about to expire.

For more information about System Alert Notifications, see System Alert Notifications.

Bridges and Servers

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

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



Multipoint Conference Scheduling

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

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

- WebEx
- Intercompany

TelePresence Server supports interop with video conferencing without additional interop devices.

(add note about meeting extension feature of CTS-Manager is only compatible with CTMS).

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

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

Interoperability with Video Conferencing

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

When the setting is greyed out:

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

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

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

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

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

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

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

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

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

TelePresence Call-In Number

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

Studio Mode Recording

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

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

Enabling recording globally

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

To enable recording globally:

Step 1 In Microsoft Outlook or Notes, schedule a single meeting with one endpoint.

Step 2 Log in to the CTMS administration interface as an Administrator.

Step 3 Go to **Configure** > **Application Settings** > and click the **Bridges and Servers** tab.

Step 4 Set Studio Mode Recording to **Yes**.

Step 5 From Microsoft Outlook or Lotus Notes, select this meeting and modify it as a recurring meeting.

Step 6 All meeting instances now have recording enabled.

WebEx

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

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

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

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

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

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

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

http://www.cisco.com/en/US/docs/telepresence/cts_admin/webex_solutions/guide/cts_webex_config.html

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

CTMS Network Multipoint

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

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

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

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

Note This feature is only compatible with CTMS devices.

Intergroup Scheduling

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

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

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

For more information about Device Groups, go to Device Groups, page 11-78.

Intercompany

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

Note An Intercompany TelePresence meeting cannot be configured for Interop. If you enable Intercompany, you cannot add video conferencing (VC) endpoints to your meeting. EX and C series endpoints are supported only

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

Another Company Hosts

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

Our Company Hosts

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

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

Locales

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

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

- All emails sent to the meeting organizer
- Meeting Manager

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

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

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

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

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

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

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

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

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

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

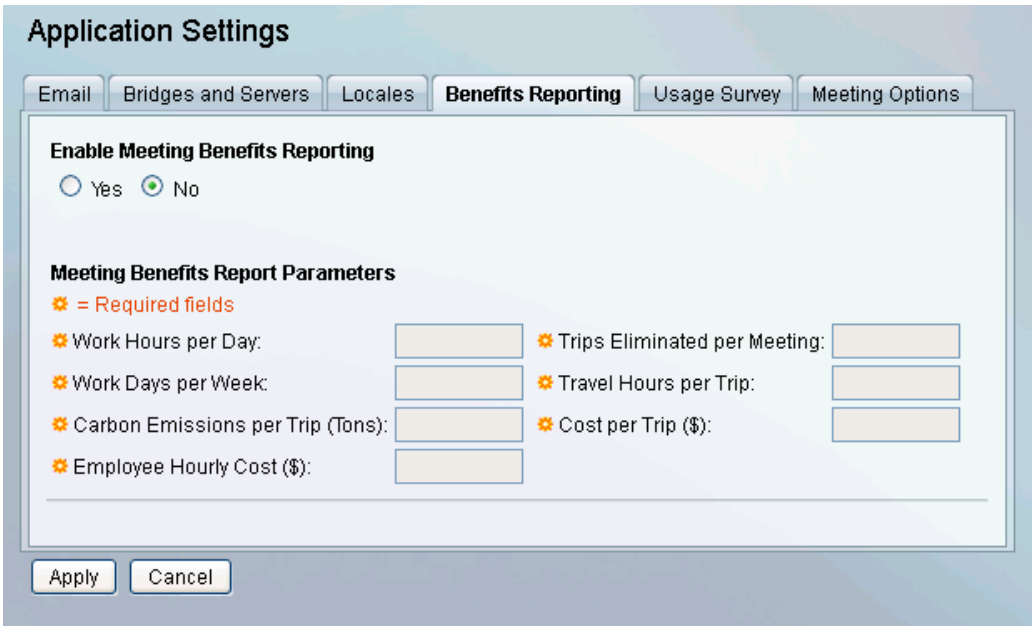
Step 5 To make selected locales available to meeting organizers, click **Publish All Locales**.

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

Benefits Reporting

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

Figure 11-49 Configure > Application Settings > Benefits Reporting



Enable Meeting Benefits Report

To enable the meeting benefits report feature:

- Select the **Yes** radio button.

Note "No" is selected by default which means the meeting organizer will not be able to fill out the survey or access the Monitor > Metrics Dashboard, Meeting Benefits or TelePresence and VC Utilization windows.

Meeting Benefits Report Parameters

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

To set Meeting Benefits Parameters:

- Enter the parameters appropriate for your company

Table 11-31 Meeting Benefits Parameters

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

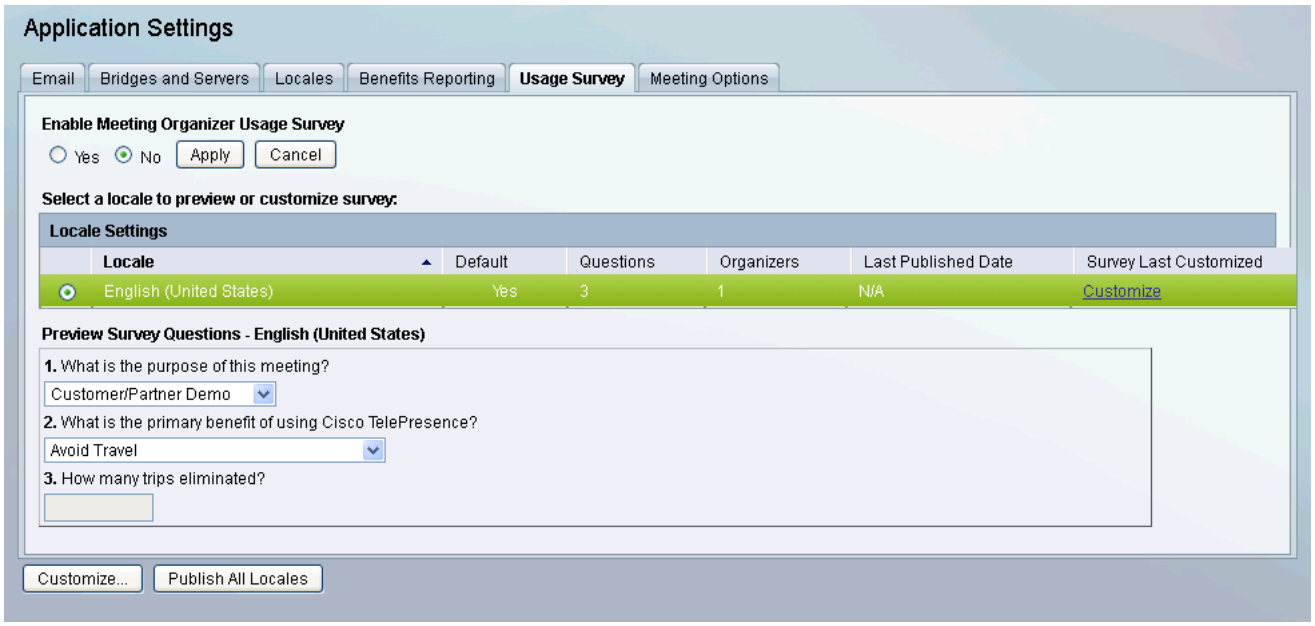
Usage Survey

The Application Settings > Usage Survey window allows you to create and customize a usage survey.

You can create a survey based upon what information your company wants to gather from each meeting. After the meeting organizer receives the confirmation email for the scheduled meeting, they can answer the survey at any time, even after the meeting has ended.

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

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



Enable Meeting Organizer Usage Survey

To enable the usage survey feature:

Step 1 Select the **Yes** radio button.

Step 2 Click **Apply**.

Note "No" is selected by default which means the meeting organizer will not be able to fill out the survey or access the Monitor > Metrics Dashboard, Meeting Benefits or TelePresence Utilization windows.

Select a Locale to Preview or Customize Survey

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

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

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

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

Preview Survey Questions

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

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

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

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

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

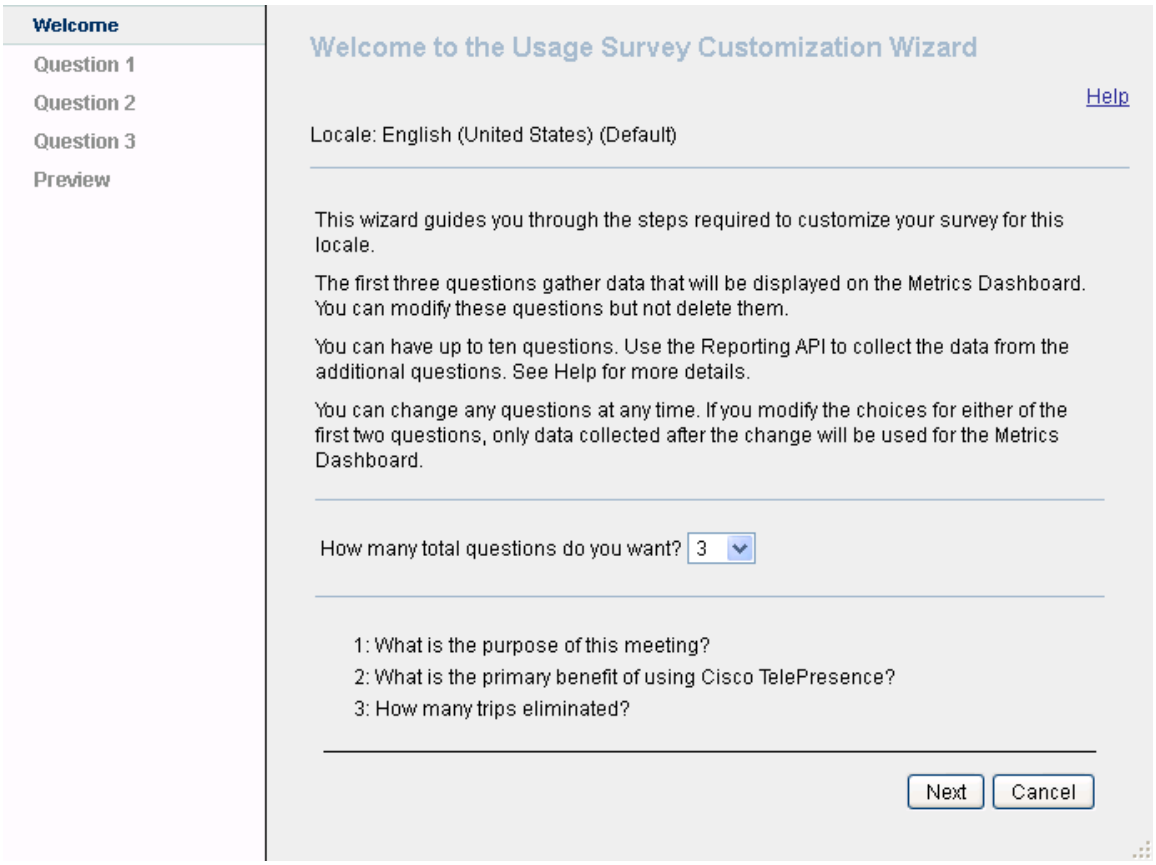
Customizing the Survey

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

The survey customization wizard guides you through the steps required to customize the usage survey.

The first three questions are included by default, and you can add up to seven more.

Figure 11-51 Usage Survey Customization Wizard



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

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

Survey Questions 1 - 3

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

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

Note If you modify the possible answers for either of the first two questions, the previous answers will be visible on the Meeting Details page only if you select a time range before the modification.

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

Results from question 3 are gathered through the reporting API and are not displayed on the Metrics Dashboard. This provides you with the ability to track how many trips are actually eliminated per meeting, which you can use as the basis for setting the Trips Eliminated per Meeting value in the Configure > Application Settings > Usage Survey window.

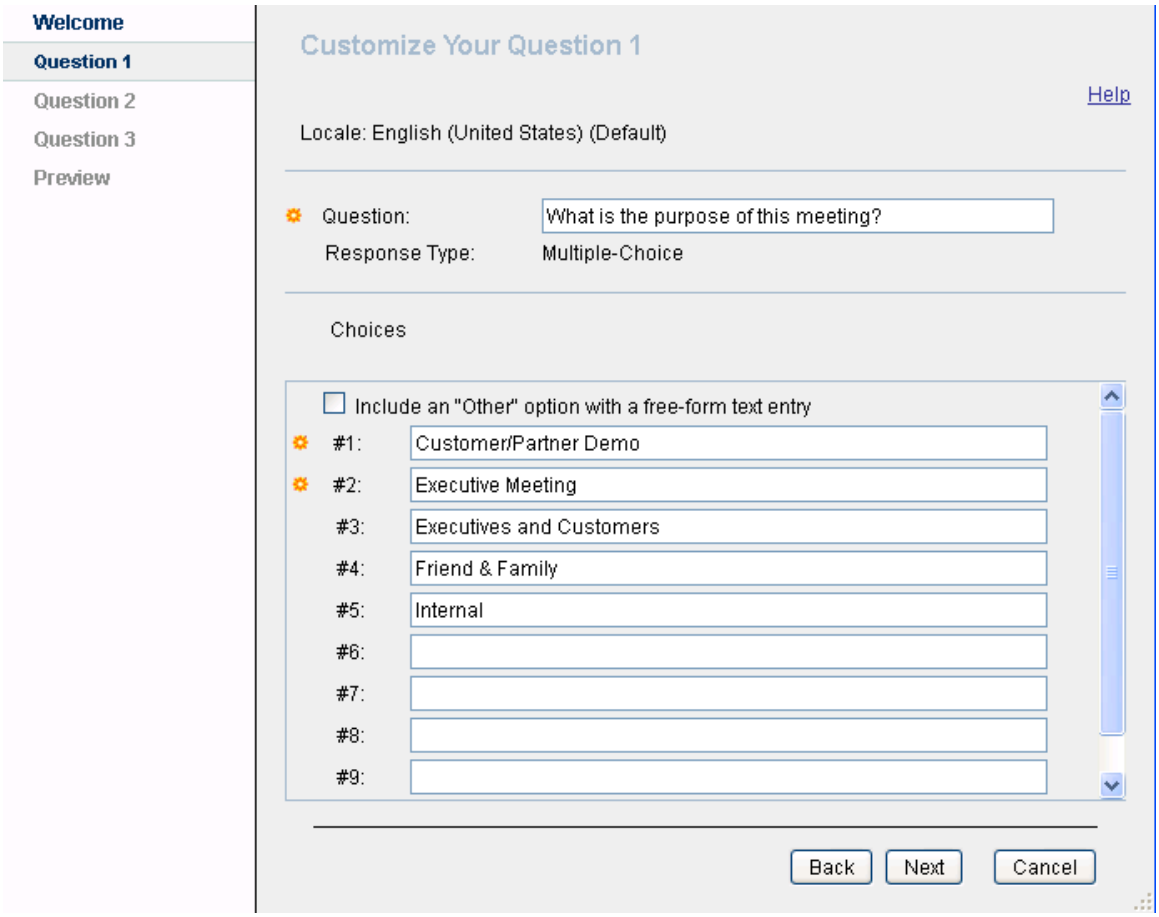
Additional Questions

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

- Multiple Choice
- Number
- Text

You can have up to 10 possible choices.

Figure 11-52 Customize Your Question 1



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

To customize this question, do the following:

Step 1 In the Question field, change the default question, if you wish.

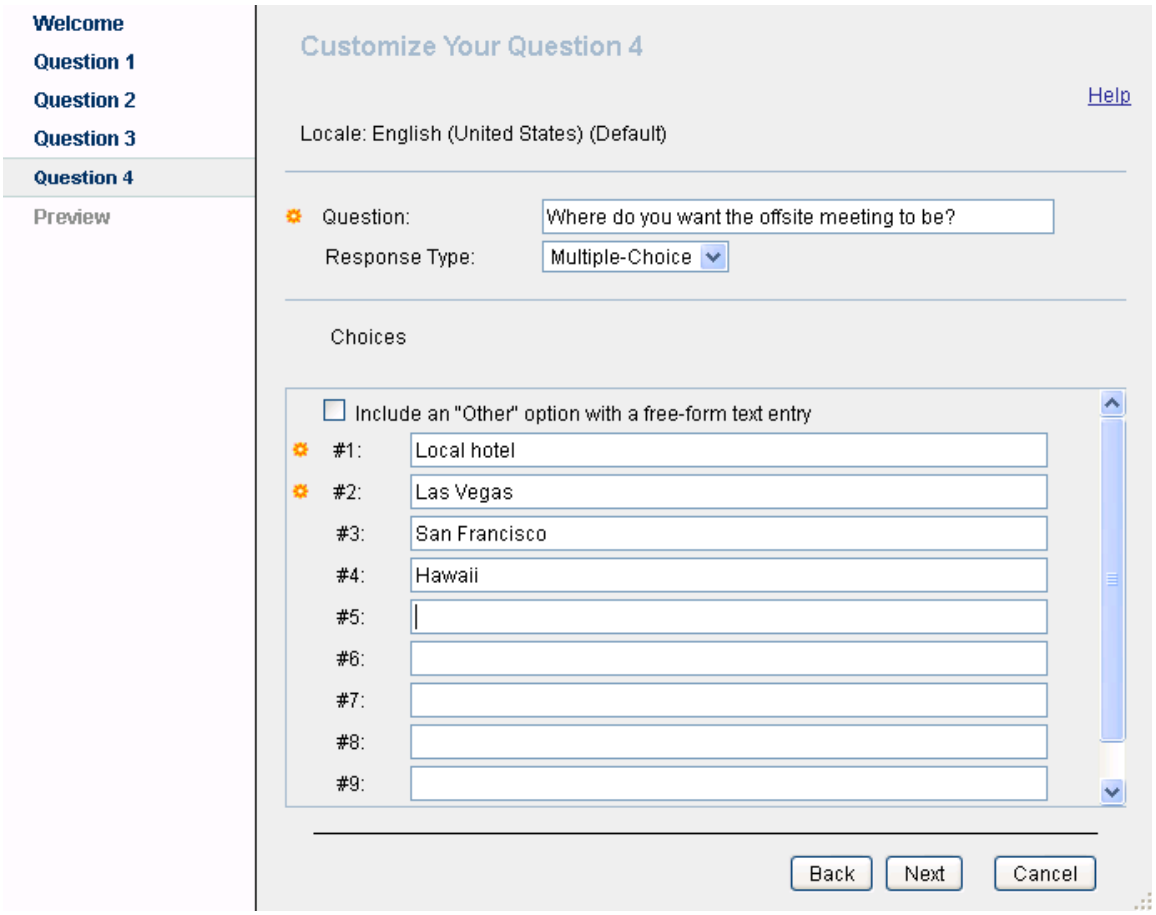
Step 2 Make any necessary changes to the answers and add any new ones if you need to.

Step 3 Click **Next**.

Step 4 Review and modify, if necessary, the next two default questions and their answers.

Note When customizing the question 2, you cannot modify the Avoid Travel answer because it is used to calculate reporting data in the Meeting Benefits section of the Metrics Dashboard. For more information, see Meeting Benefits, page 13-19.

Figure 11-53 Creating a New Question



To create a new question, do the following:

Step 1 In the Question field, enter a question.

Step 2 From the Response Type drop-down menu, select a response type.

Step 3 (Optional) Click the checkbox for Include an “Other” option if you want to include a text box in the survey for the meeting organizer to enter text as an answer.

Step 4 Enter the possible responses for the question (up to ten).

Step 5 Click **Next**.

Step 6 Create additional new questions by following steps 1 through 5.

Editing Additional Questions

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

Deleting Additional Questions

You can delete additional survey questions by doing the following:

Step 1 Go back to the Welcome page of the survey customization wizard (using the back button or opening the wizard again, if you are making changes to an existing survey).

Step 2 Click the checkbox next to the additional question you want to delete.

Step 3 Click **Next**.

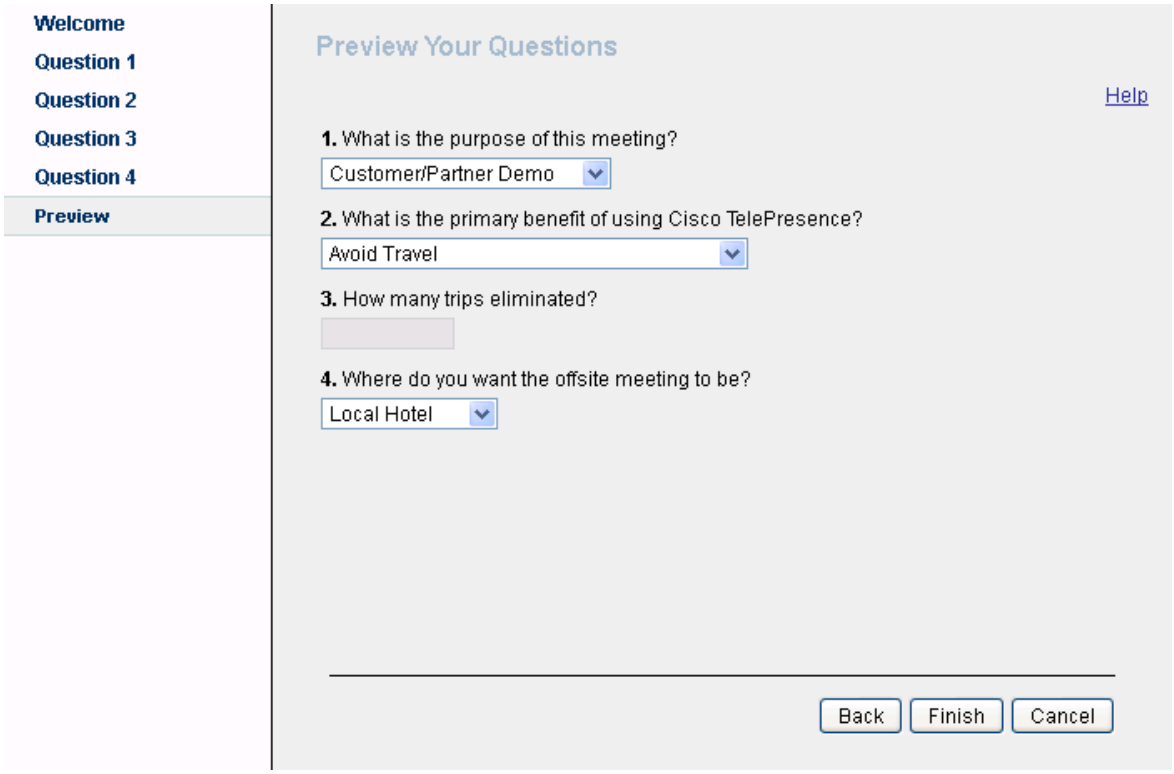
Step 4 If the survey is the default locale survey, a confirmation message appears. To delete the selected question, click **OK**.

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

Preview Your Questions

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

Figure 11-54 Preview Your Survey Questions



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

Publishing Your Survey

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

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

Changing the Default Survey

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

Step 1 Click the Default radio button for the locale survey you want to be the default.

Step 2 Click **Publish All Locales**.

Default Survey Questions

Three survey questions and answers are included by default:

- Question 1
- Question 2
- Question 3

Question 1

This question captures the main purpose of the meeting.

Question:

- What is the purpose of this meeting?

Answers:

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

Question 2

This question captures the primary benefits of the meeting.

Question:

- What is the primary benefit of using Cisco TelePresence?

Answers:

- Avoid Travel
- Accelerate Time to Market
- Address Customer Issues
- Allow Business Continuity/Mitigate Crisis
- Connect Customers to Company Leaders
- Demonstrate Product to Customer
- Increase Employee Productivity

Question 3

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

Question:

- How many trips eliminated?

Answer:

- *User enters a number.*

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

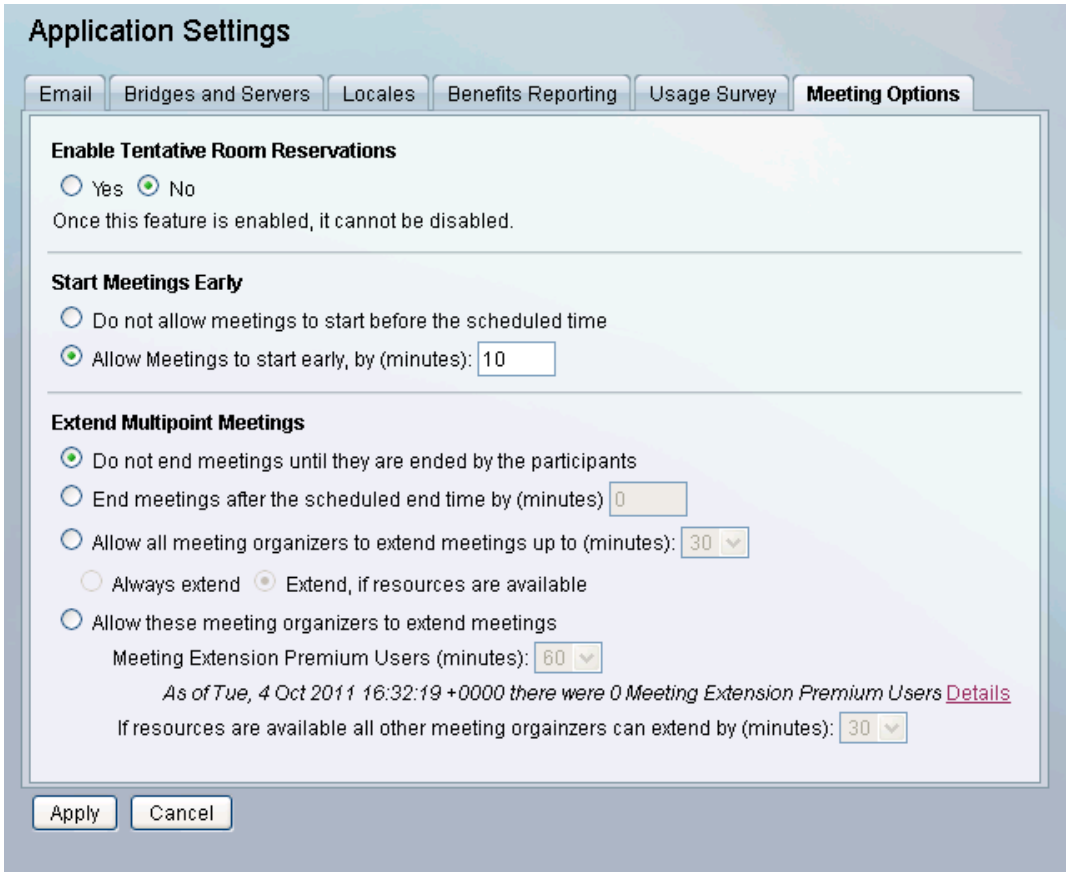
Meeting Options

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

Figure 11-55 illustrates the default settings when the application is first installed.

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

Figure 11-55 Configure > Application Settings > Meeting Options



Enable Tentative Room Reservations

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

This option is supported only with Microsoft Exchange.

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

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

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

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

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

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

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

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

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

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

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

Start Meetings Early

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

You have two options:

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

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

Note This feature is not compatible with TelePresence Server.

Extend Multipoint Meetings

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

To enable this feature, the following are required:

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

Note This feature is not compatible with single-endpoint or point-to-point meetings. It is also not compatible with TelePresence Server.

Prerequisites

The following are required to enable the Extend Meetings feature:

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

  To check the status of TelePresence endpoints, go to **Support > Endpoints** and click the **Status** tab.
- Default first option **Do not end meetings until they are ended by the participants** should be selected.

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

Select one of the following meeting options, described below:

- **Do not end meetings until they are ended by the participants** - This option allows all meeting participants to be able to extend in-progress meetings. (This is the default setting).
- **End meetings after the scheduled end time (minutes)** - This option forces each meeting to end after the designated extended time. If you upgraded from the previous version of CTS-Manager, then the setting time appears in this field.
- **Allow all meeting organizers to extend meetings up to (minutes)** - Select either 30 or 60 (30 default) for every meeting.

  - **Always Extend** - Automatically extends every meeting.
  - **Extend, if resources are available** - Only extends the meeting if the necessary resources are available.
- **Allow these meeting organizers to extend meetings** - This allows the meeting that is in progress to continue after the scheduled end time. The two selections are:
  - **Meeting Extension Premium Users (minutes)** - select either 30 or 60 (60 default).

    The following message appears after clicking the radio button to select this option and clicking **Apply**:

    As of (date and time) there were X meeting Extension Premium Users Details
  - **If resources are available all other meeting organizers can extend by (minutes) -** select either 0, 30 or 60 minutes. If you set this option to 0, only Meeting Extension Premium Users are able to extend meetings.

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

Before enabling this option, you must do the following:

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

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

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

Displaying Meeting Extension Information in Meeting Details Window

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

Important Information About Resource Allocation

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

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

CTS-Manager Redundancy Failover Procedure

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

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

Cold Standby

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

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

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

CTS-Manager Failover Procedure

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

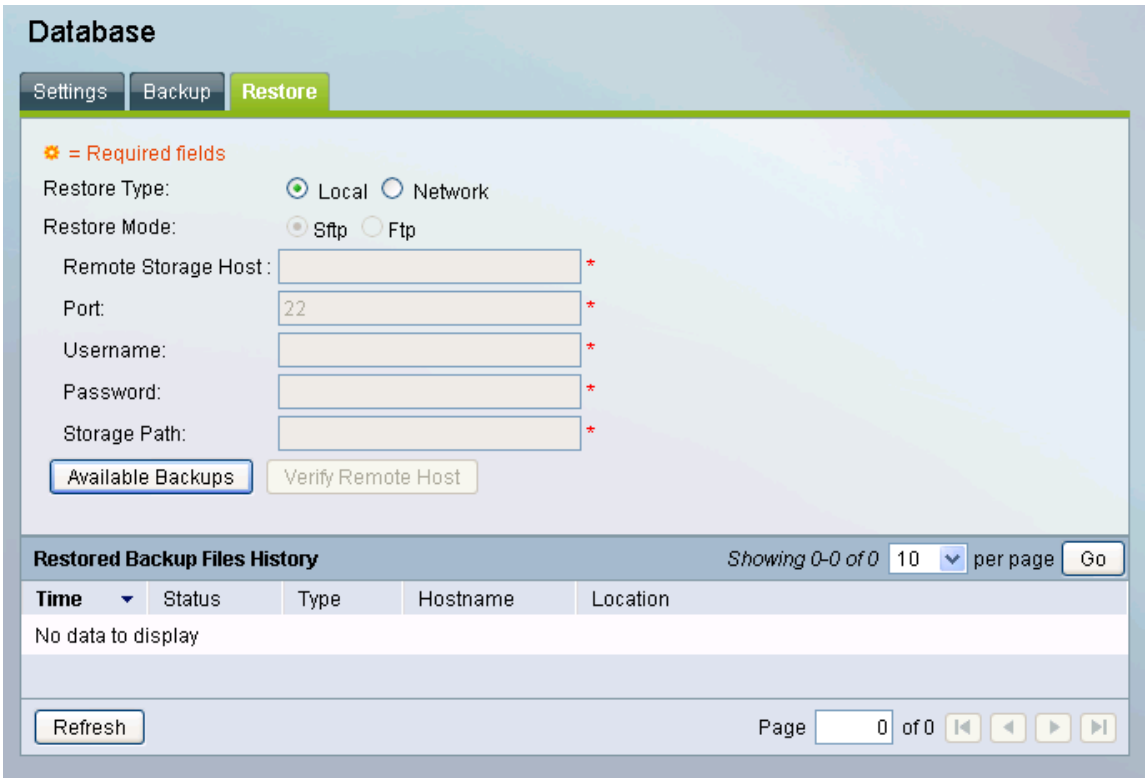
Step 1 To start the failover procedure, power off the primary CTS-Manager system.

Step 2 Power on the backup CTS-Manager system.

Step 3 Go to **Configure > Database** and click the **Restore** tab.

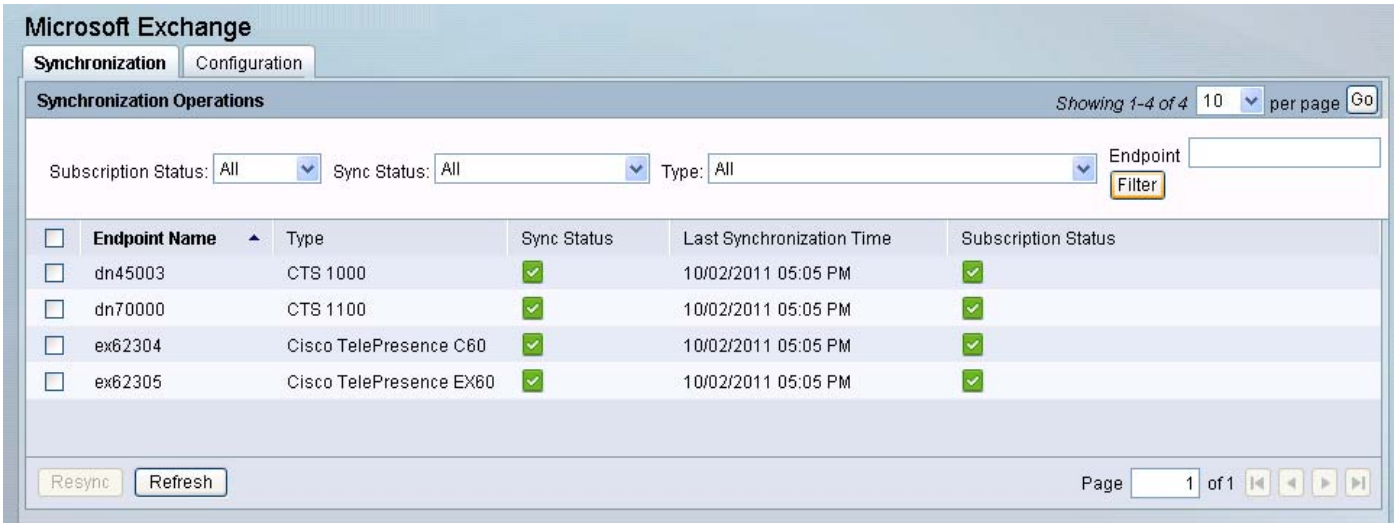
Step 4 Restore the last CTS-Manager database to the backup CTS-Manager by clicking **Available Backups,** selecting an available backup file and clicking **Restore Now.**

Figure 11-56 Configure > Database > Restore Window



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

Figure 11-57 Configure > Microsoft Exchange > Synchronization Tab



Step 6 Review the information to make sure it is correct, make any changes needed and click **Resync**.

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

Warm Standby

CTMS Warm Standby for Scheduled Meetings

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

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

CTS-Manager Redundancy Failover Procedure

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

Note Both CTMS are active, but meetings are to be scheduled on the primary "Scheduled" CTMS

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

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

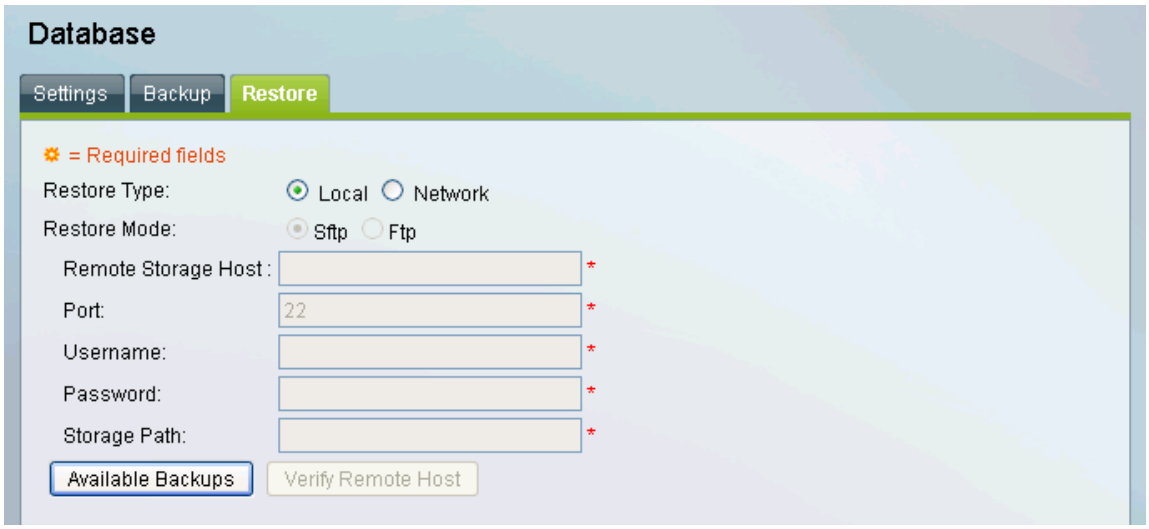
Step 2 Power on the backup CTS-Manager.

Step 3 Go to **Configure** > **Database** and click the **Restore** tab.

Step 4 Restore the last CTS-Manager database to the backup CTMS by clicking **Available Backups,** selecting an available backup file and clicking **Restore Now.**

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

Figure 11-58 Configure > Database > Restore



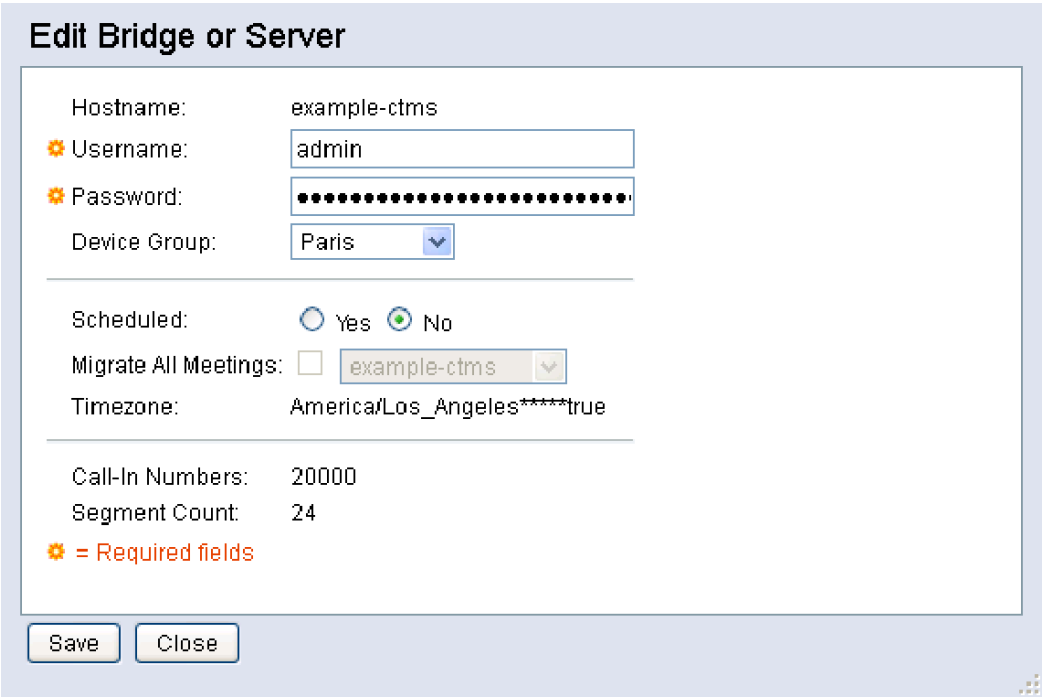
CTMS Redundancy Failover Procedure

Step 1 When the primary CTMS fails, log into CTS-Manager and migrate all scheduled meeting to the backup "non-scheduled" CTMS.

Step 2 Change the Scheduled option of the primary CTMS to **No**.

Step 3 Change the Scheduled option of the backup CTMS to **Yes**.

Figure 11-59 Configure > Bridges and Servers Edit Window



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

CHAPTER 12

Configuring Cisco WebEx OneTouch for Cisco TelePresence Manager

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

Note You must be running CTS-Manager, CTMS, CTS software release 1.7 or later to schedule TelePresence meetings with WebEx.

Contents

This chapter contains the following sections:

- Introduction, page 12-1
- Before Configuring Cisco WebEx in CTS-Manager, page 12-2
- Setting Up Cisco WebEx Administration Site Account, page 12-3
- Cisco WebEx First-Time Setup in CTS-Manager, page 12-4
- Configuring Cisco WebEx Users in CTS-Manager, page 12-12
- First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15
- Configuring Other Applications, page 12-23

Introduction

This chapter explains how to set up Cisco WebEx OneTouch in CTS-Manager, which allows WebEx participants to join TelePresence meetings. Beginning with release 1.9, CTS-Manager provides the following new feature:

- TelePresence meetings with WebEx can now be scheduled directly from Microsoft Outlook. For more information, refer to: Using Microsoft Outlook and the WebEx Productivity Tools Plug-in, page 12-20

Post-Install Guidelines for CTS-Manager

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

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

Table 12-1 Post-Install Guidelines for Configuring CTS-Manager

Setup Procedure Guidelines after Installing CTS-Manager	Description	Location
Configuring Cisco TelePresence WebEx OneTouch for CTS-Manager	Describes how to set up Cisco TelePresence WebEx OneTouch in CTS-Manager, which allows WebEx participants to join TelePresence meetings.	Current chapter
Monitoring and Supporting CTS-Manager	Describes the support features available when you log into CTS-Manager using a Live Desk role.	Chapter 13, "Monitoring and Supporting Cisco TelePresence Manager"

If at any time you encounter problems, go to Chapter 16, "Troubleshooting Cisco TelePresence Manager" to see how to correct the problem.

Before Configuring Cisco WebEx in CTS-Manager

Before configuring WebEx in CTS-Manager, you must have the following information:

Information	Description
WebEx hostname	A name identifying the WebEx site hostname to the administrator. This typically can be the same name as the hostname used in the site URL. **Note** Multiple WebEx sites can have the same hostname. This is not used to connect to the WebEx site and therefore is not validated during testing of connection.
WebEx Admin Username	WebEx site administrator's username (provided by the WebEx team).
WebEx Admin Access Code	WebEx site administrator's access code (provided by the WebEx team).
WebEx Site URL	URL for WebEx Scheduling Server (provided by the WebEx team).

Information	Description
WebEx Hostname Certificate	Security certificate of WebEx scheduling server. For more information, see First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15
Default WebEx user role setting for new users	You must decide whether you want new users to be Permitted or Non-Permitted users by default. For more information, see First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15.

Note To use WebEx in a scheduled network multipoint meeting, CTMS release 1.9 is required. WebEx uses one segment from the Rendezvous Point CTMS to establish the connection to the WebEx site.

Setting Up Cisco WebEx Administration Site Account

You have access to the Cisco WebEx Administration Site interface through your Cisco WebEx administrator using a unique Cisco WebEx administration URL and access code. As a site administrator, you can log in to access current Cisco WebEx user and administration guides for the services and features that have been configured on your Cisco TelePresence system.

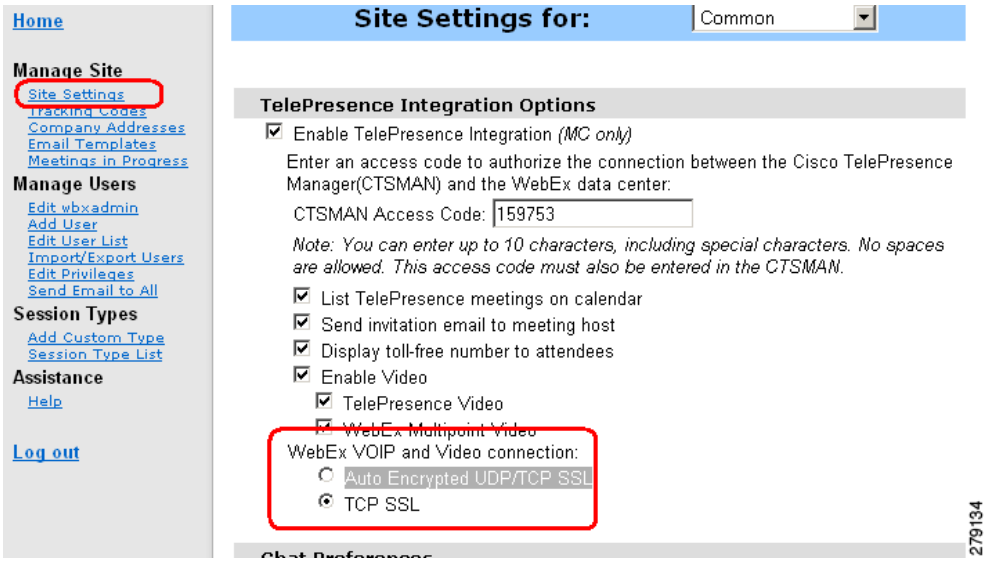
Specifying Cisco TelePresence Integration Options

To integrate Cisco TelePresence to Cisco WebEx on the Cisco WebEx site, follow these steps:

Step 1 Log in to the Cisco WebEx Site Administration interface.

Step 2 Choose **Manage Site** > **Site Settings**. The Site Settings screen appears, as shown in Figure 12-1.

Figure 12-1 Configuring Cisco WebEx Connection Settings



Step 3 Click to select **Enable Cisco TelePresence Integration (MC only)**. If not checked, Cisco WebEx will be disabled on this site.

Step 4 Enter your CTS Manager access code (SiteID and ConferenceID). This combined access code identifies a prefix number which is exclusively assigned to Cisco Telepresence deployments that are integrated with the Cisco WebEx solution. This code allows the CTMS to connect to the Cisco TelePresence gateway to initiate your meeting.

Step 5 Click to select **List Cisco TelePresence meetings on calendar** so that scheduled meetings appear on the Cisco WebEx calendar.

Step 6 Click to select **Send invitation email to meeting host**. This allows the meeting information email to be sent to the Cisco WebEx host after the meeting is scheduled.

Step 7 Click to select **Display toll-free number to attendees**.

Step 8 Click to select: **Enable Video**. This enables video on the Cisco WebEx meeting user interface. Click both **Cisco TelePresence Video** (CIF) and **Cisco WebEx Multipoint Video**.

Step 9 In the Cisco WebEx VOIP and Video Connection field, click to select **TCP SSL** (recommended). This selects the connection method between the Cisco WebEx client and the multimedia server (VOIP and video).

Step 10 Click **Save** to save your settings.

Cisco WebEx First-Time Setup in CTS-Manager

This section describes how to enable WebEx and select the default WebEx user type, as well as perform the one-time initial registration in CTS-Manager that specifies the Cisco WebEx account information so that you can add Cisco WebEx functionality to Cisco TelePresence meetings.

Before You Begin

You will need at least one CTMS configured in CTS-Manager before you can configure CTS-Manager for Cisco WebEx. The CTMS communicates with the Cisco WebEx Telephony Gateway to establish the audio portion of a Cisco WebEx meeting.

CTS-Manager requires that all scheduled CTMSes are registered with a WebEx Telepresence Gateway.

To register a CTMS with a WebEx Telepresence Gateway, log in to the CTMS administration UI and go to **Configure > WebEx**.

Complete the steps in Chapter 2, "Configuring Cisco WebEx OneTouch on the Cisco TelePresence Multipoint Switch."in the "Cisco WebEx OneTouch Configuration Guide for the Cisco TelePresence System" at the following URL:
http://www.cisco.com/en/US/docs/telepresence/cts_admin/webex_solutions/guide/cts_webex_ctms.html

Once you have configured the CTMS, proceed with the following tasks:

- Enabling WebEx and Selecting Default WebEx User Type, page 12-5
- Configuring a Cisco WebEx Site, page 12-7
- First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15

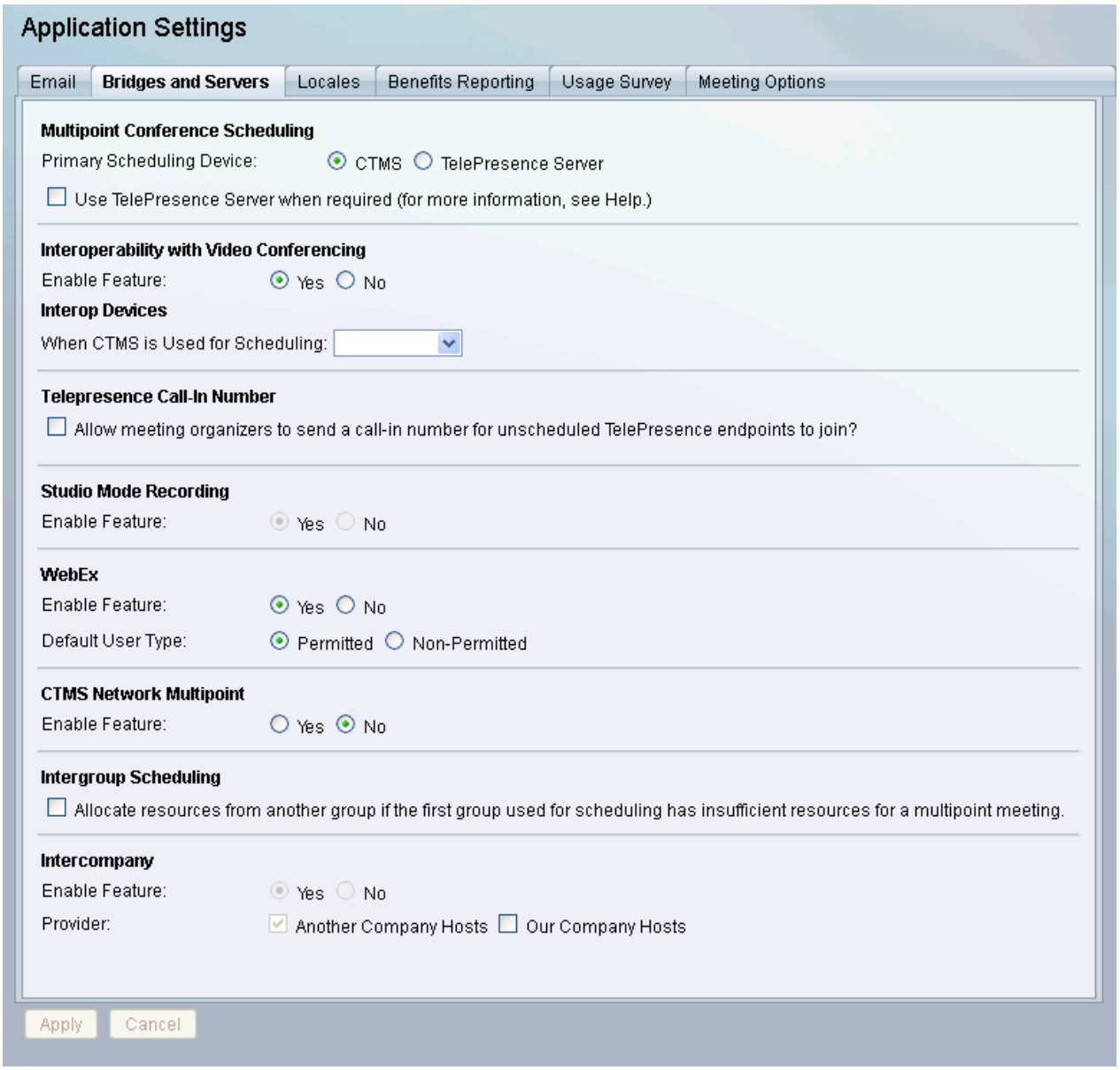
Enabling WebEx and Selecting Default WebEx User Type

To select Permitted and Non-Permitted Cisco WebEx user types, follow these steps in the CTS-Manager administration interface:

Step 1 Choose **Configure > Application Settings**.

Step 2 Select the **Bridges and Servers** tab. The Application Settings > Bridges and Servers window appears, as shown in Figure 12-2.

Figure 12-2 Enabling WebEx and Configuring Default User Type



Step 3 For WebEx Enable Feature, click the **Yes** radio button.

Step 4 For Default User Type, click one of the following radio buttons:

- **Permitted** (default)—These users are permitted to request Cisco WebEx for specific meetings using CTS-Manager.
- **Non-Permitted**—These users are not permitted to request Cisco WebEx; no Cisco WebEx meeting options are available to these users.

Note The default user type is the WebEx role assigned to users until the CTS-Manager administrator assigns them to a specific role using the Configure > Access Management window.

Step 5 In the Interoperability with Video Conferencing Interop Quality field, click the **CIF** radio button.

Step 6 Click **Apply** and then click **OK** in the confirmation window.

Configuring a Cisco WebEx Site

To configure a new site for Cisco WebEx, follow these steps:

Step 1 Log in to the CTS-Manager administration interface.

Step 2 Choose **Configure** > **Bridges and Servers**. The Bridges and Servers page appears.

Step 3 Click **New**. The New Bridge or Server page appears in a new window.

Step 4 From the Type drop-down menu, select **WebEx**.

Step 5 In the Hostname field, enter the hostname to uniquely identify the WebEx site being configured. For example: example.webex.com.

Step 6 In the Site URL field, enter your unique Cisco WebEx Site URL obtained from the Cisco WebEx administrator. For example: https://example.webex.com/example.

Step 7 In the WebEx Admin Username field, enter your Cisco WebEx Administration account username. For example, wbxAdmin. This is the user account that was created by your Cisco WebEx administator that grants you Cisco WebEx Administration Site privileges.

Step 8 In the WebEx Admin Access Code field, enter your Cisco WebEx Site Administration account access code. For example, 123456.

Step 9 Enter the rest of the information for the remaining fields. For more information, refer to Table 12-2 on page 12-8.

Step 10 Click **Save** to save your settings and close the New Bridge or Server page.

Step 11 Verify your settings by checking that the Service Status reads “OK” on the Bridges and Server page.

Step 12 Proceed to Obtaining the Cisco WebEx Site Security Server Certificate.

WebEx Proxy Server

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

The following modes of proxy connection are available:

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

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

Table 12-2 New Bridge or Server Window for WebEx Information

Field	Description or Settings
Type	Select WebEx from the pull-down list menu. **Note** If WebEx does not appear in the drop-down list, make sure WebEx is enabled in the Configure > Application Settings > Bridges and Servers window.
Hostname	A name identifying the WebEx site hostname to the administrator. This typically can be the same name as the hostname used in the site URL. **Note** Multiple WebEx sites can have the same hostname. This is not used to connect to the WebEx site and therefore is not validated during testing of connection.
Site URL	The address used to construct the URL that's used to access this meeting. This is the actual URL that CTS-Manager uses to communicate with WebEx. This is published in the email from CTS-Manager, and is displayed to users on the WebEx page of the CTS display device.
WebEx Admin Username	WebEx administrator's username (provided by the WebEx team)
WebEx Admin Access Code	WebEx administrator's access code (provided by the WebEx team)
Certificate	Certificate from the hostname (WebEx scheduling server) **Note** To get the certificate, open a web browser window and go to the hostname URL and download the certificate to your computer, then click Browse to select it and upload it to CTS-Manager. For detailed instructions on downloading the certificate with different browsers, see Obtaining the Cisco WebEx Site Security Server Certificate, page 12-9.
Connection Type	Choose the type of connection to establish with the WebEx scheduling server: Direct or Via Proxy Server. Selecting the proxy server option allows you to filter IP traffic and increase security.
WebEx Proxy Server Settings	
Host Name	Host name of proxy server
Port	Port number of proxy server
Requires Authentication	Yes or No. Select Yes if the Proxy server requires authentication and then enter username and password.
Username	Username for proxy server
Password	Password for proxy server

Multiple WebEx Sites

You can configure up to five WebEx sites to support more WebEx users for TelePresence meetings. The meeting organizer can, however, select any of the available WebEx sites to register with. The meeting organizer can only register one WebEx account on one of the available sites configured in CTS-Manager.

Obtaining the Cisco WebEx Site Security Server Certificate

Use the information in this section to obtain and add your Cisco WebEx site security server certificate to CTS-Manager:

- Obtaining Your Certificate Using Internet Explorer, page 12-9
- Obtaining Your Certificate Using Firefox, page 12-10
- Adding Your Certificate to CTS-Manager, page 12-10

Obtaining Your Certificate Using Internet Explorer

To obtain your Cisco WebEx site security certificate using Internet Explorer (IE), follow these steps:

Step 1 Open a new browser window.

Step 2 Enter the unique Cisco WebEx scheduling server hostname from CTS-Manager Host field in Step 5 of Configuring a Cisco WebEx Site and press Enter. (For example, https://qamctp.webex.com/qamctp)

Step 3 IE 7.x or earlier: In the bottom right-hand corner of the browser window, double-click the lock icon.

IE 8.x or later: Click the Certificate Error in the top of the browser after the URL and click **View certificates**.

The certificate window appears.

Step 4 Click the **Certification Path** tab.

Step 5 Select the top-level certificate (CA root, .e.g Verisign).

Step 6 Click **View Certificate**.

The Certificate window appears.

Step 7 Click the **Details** tab.

Step 8 Click **Copy to File**.

The Certificate Export Wizard window appears.

Step 9 Click **Next**.

Step 10 Select the **DER encoded binary** option and click **Next**.

Step 11 Click **Browse**.

The Save As window appears.

Step 12 Create a file name for the certificate.

Step 13 Navigate to the location where you want to save the certificate and click **Save**.

Step 14 Click **Next** and then click **Finish**.

When the export is complete, the message “The export was successful” appears.

Step 15 Click **OK** to close the message and **OK** again to close the Certificate window.

Step 16 Proceed to Adding Your Certificate to CTS-Manager.

Obtaining Your Certificate Using Firefox

To obtain your Cisco WebEx site security certificate using Firefox, follow these steps:

Step 1 Open a new browser window.

Step 2 Enter the Cisco WebEx scheduling server hostname from CTS-Manager Host field in Step 5 of Configuring a Cisco WebEx Site and press Enter. (For example, https://qamctp.webex.com/qamctp)

Step 3 For Firefox 4.x or earlier: In the bottom right-hand corner of the browser window, double-click the lock icon.

Step 4 For Firefox 5.x or later: In the upper left corner of the browser, before the URL, click the site name (in blue).

The site info popup window appears showing the security information for the site.

Step 5 Click the **More Information** button.

The Page Info window appears with the Security tab selected.

Step 6 Click **View Certificate**.

The Certificate Viewer window appears.

Step 7 Click the **Details** tab.

Step 8 Select the top level of the Certificate Hierarchy (e.g. Builtin Object Token: Verisign Class 3 Public Primary Certification Authority - G2).

Step 9 Click **Export**.

The Save Certificate To File window appears.

Step 10 (Optional) Modify the file name.

Step 11 Navigate to the location where you want to save the certificate and click **Save**.

Step 12 Click **Close** to close the Certificate Viewer window.

Step 13 Proceed to Adding Your Certificate to CTS-Manager.

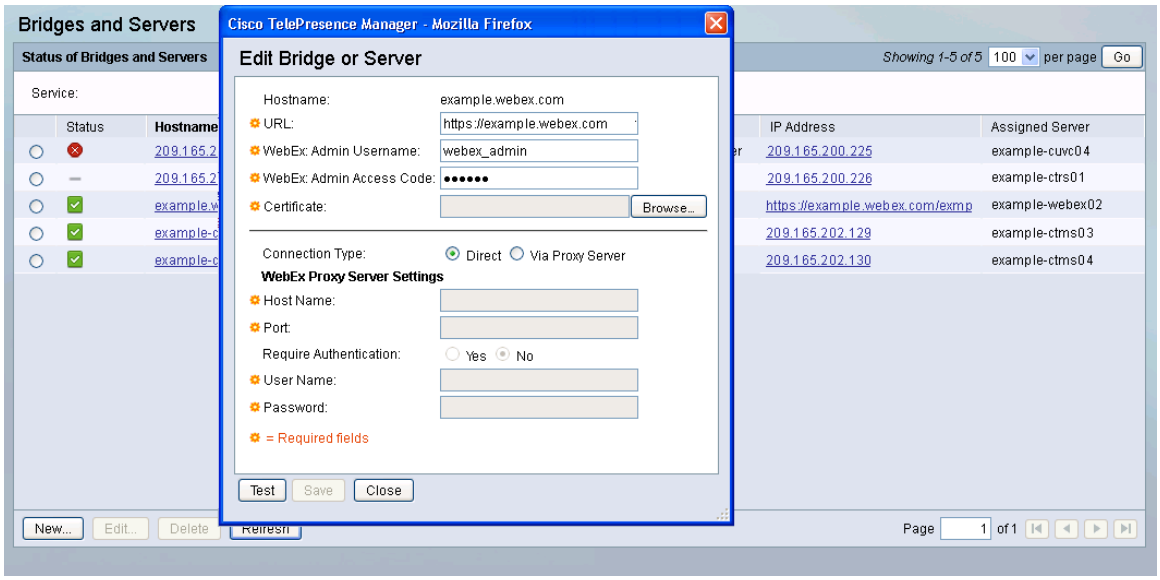
Adding Your Certificate to CTS-Manager

To add your certificate to CTS-Manager, follow these steps in the CTS-Manager administration interface:

Step 1 Choose **Configure** > **Bridges and Servers**. The Bridges and Servers page appears.

Step 2 Select the Cisco WebEx site and click **Edit**. The Edit Bridge or Server window appears showing your Cisco WebEx configuration settings, as shown in Figure 12-3.

Figure 12-3 Edit...Bridge or Server Dialog



Step 3 Click **Browse** to find and add the certificate you just obtained in Obtaining the Cisco WebEx Site Security Server Certificate.

Step 4 Click **Test**. The system checks for the certificate and responds with confirmation or an error message.

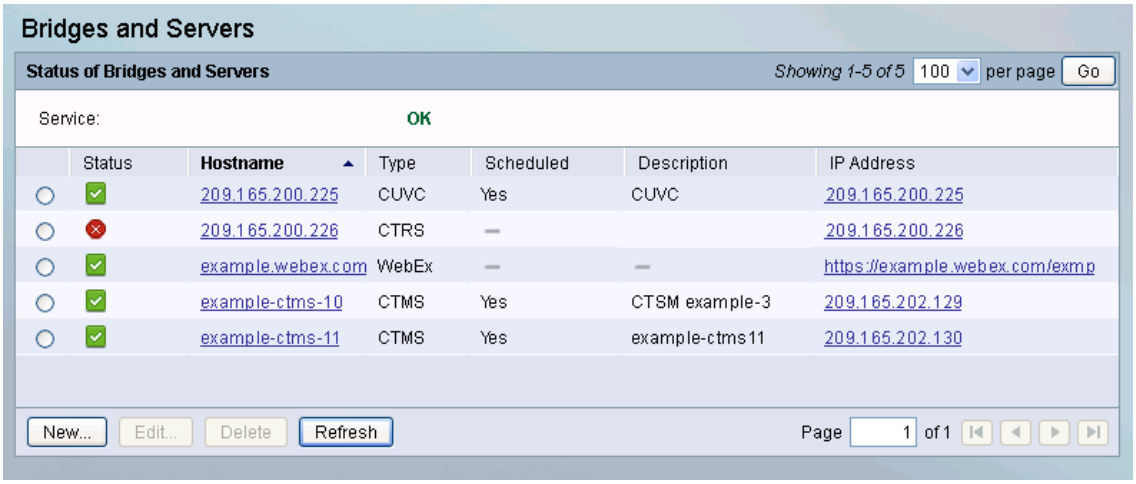
Step 5 Click **OK** to dismiss the message.

Tip If the certificate is not found and an error message appears, make sure that you browsed to the correct certificate in your local directory and try again.

Step 6 Click **Save** to save your settings and to dismiss the Edit Bridge or Server window.

Step 7 The Bridges and Servers window should show OK in for Service, as shown in Figure 12-4.

Figure 12-4 Service OK



Tip If you do not see the expected green OK, click your browser's reload or refresh button to update the system and see your changes.

Step 8 Proceed to Configuring Cisco WebEx Users in CTS-Manager.

Configuring Cisco WebEx Users in CTS-Manager

This section contains the following information:

- WebEx User Types, page 12-12
- Configuring WebEx Users, page 12-13

WebEx User Types

The meeting organizer can schedule meetings with options defined in Cisco TelePresence Manager based upon one of three possible WebEx user types configured in CTS-Manager:

- **Premium User—Cisco WebEx Always-On**. Use this option if you want to use Cisco WebEx Meeting Center for every Cisco TelePresence meeting. "Always-On" users select the Cisco TelePresence endpoints in the calendaring application and the Cisco WebEx session is automatically set up. A meeting confirmation e-mail is sent from Cisco TelePresence Manager with Cisco WebEx session details that the scheduler can forward to the Cisco WebEx attendees.

Note To prevent over-scheduling of CTMS resources, do not to add all users to the Premium user group, especially if you anticipate that the feature will not be used for most Cisco TelePresence meetings.

- **Permitted User—Enable Cisco WebEx Per Meeting**. This option requires the meeting organizer to add WebEx to a Cisco TelePresence meeting by doing the following:
  a. Select Cisco TelePresence endpoints in the Microsoft Outlook or Lotus Notes client.
  b. Add WebEx to the meeting in Microsoft Outlook using the WebEx Productivity Tools Plug-in or by clicking the WebEx button provided in the Cisco TelePresence Manager confirmation e-mail message by enabling the WebEx option in the Cisco TelePresence Manager. For more information, see First-Time Scheduling of TelePresence Meetings with WebEx, page 12-15.
  c. Receive a confirmation e-mail message from Cisco TelePresence Manager with the Cisco WebEx session details. The Cisco TelePresence meeting organizer forwards the e-mail to the Cisco WebEx attendees.

     When the meeting is scheduled, CTS-Manager pushes the schedule information, along with the Cisco WebEx meeting details, to the CTMS Conference Manager. This information is maintained in the Conference Manager until the meeting starts.
- **Non-Permitted User—Disallow Cisco WebEx**. You can configure CTS-Manager to disallow Cisco WebEx support entirely. Users configured in this mode may not use the Cisco WebEx feature, and may only schedule standard multipoint CTMS meetings.

Configuring WebEx Users

Using the Access Management window in CTS-Manager, you can configure the three different types of WebEx users mentioned in the previous section WebEx User Types, page 12-12. To assign a WebEx role, you must add the user group to the WebEx user role by following these steps in the CTS-Manager administration interface:

To configure WebEx users in CTS-Manager:

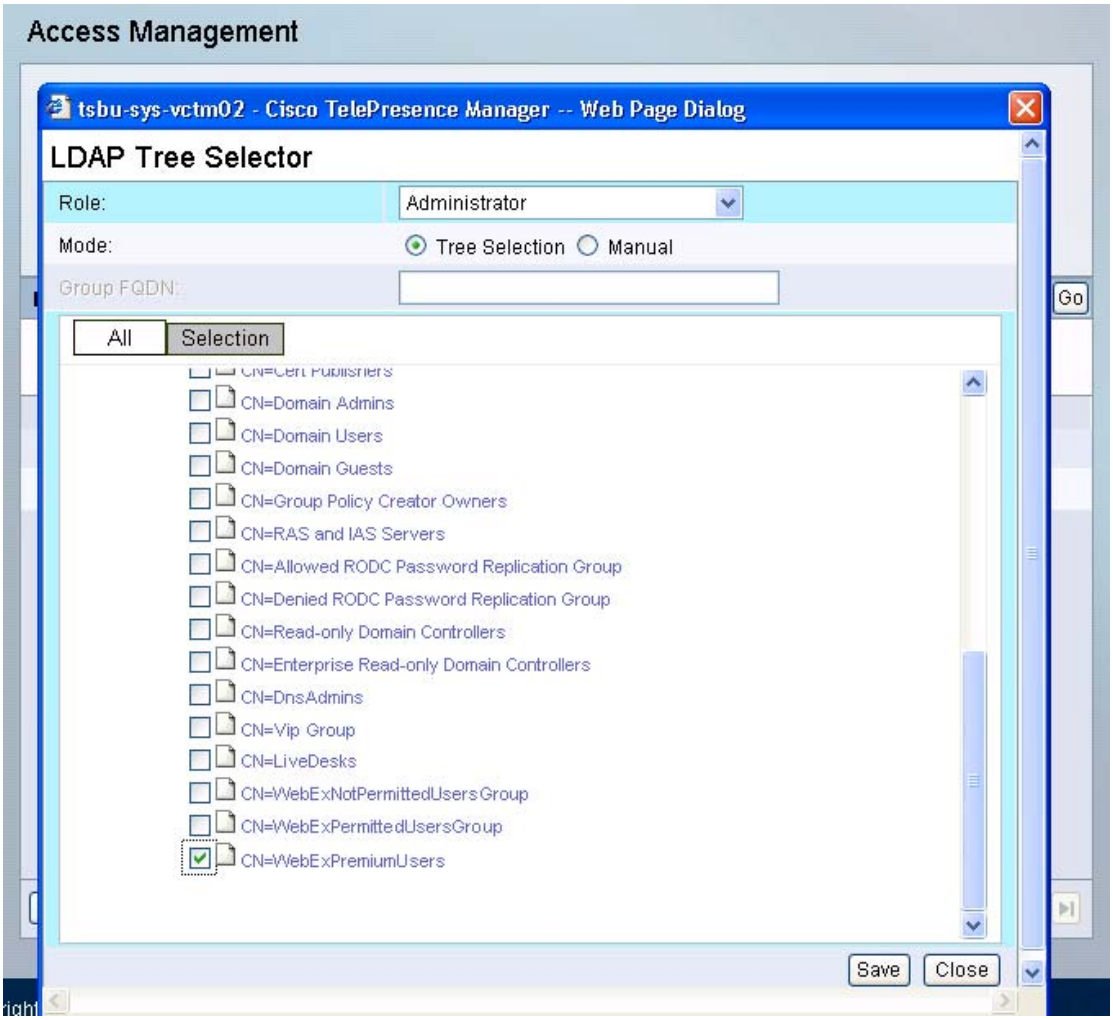
Step 1 Choose **Configure > Access Management** and click **Add**.

The LDAP Tree Selector window appears.

Step 2 From the Role drop-down menu, select the WebEx role you want to assign.

Step 3 Traverse the LDAP tree to find and select the user group by checking the box next to the user group name, as shown in Figure 12-5.

Figure 12-5 Assigning a User Group to WebEx User Role



Step 4 Click **Save**.

The user group is added to the selected WebEx user role.

Step 5 Proceed to First-Time Scheduling of TelePresence Meetings with WebEx.

First-Time Scheduling of TelePresence Meetings with WebEx

The first time a meeting organizer schedules a TelePresence meeting with WebEx, they register with the WebEx site. You can do first-time scheduling either of the following ways:

- Using Calendar Client and Meeting Manager, page 12-15

  You schedule the meeting in your calendar client, then log in to CTS-Manager to add WebEx to your meeting.

- Using Microsoft Outlook and the WebEx Productivity Tools Plug-in, page 12-20

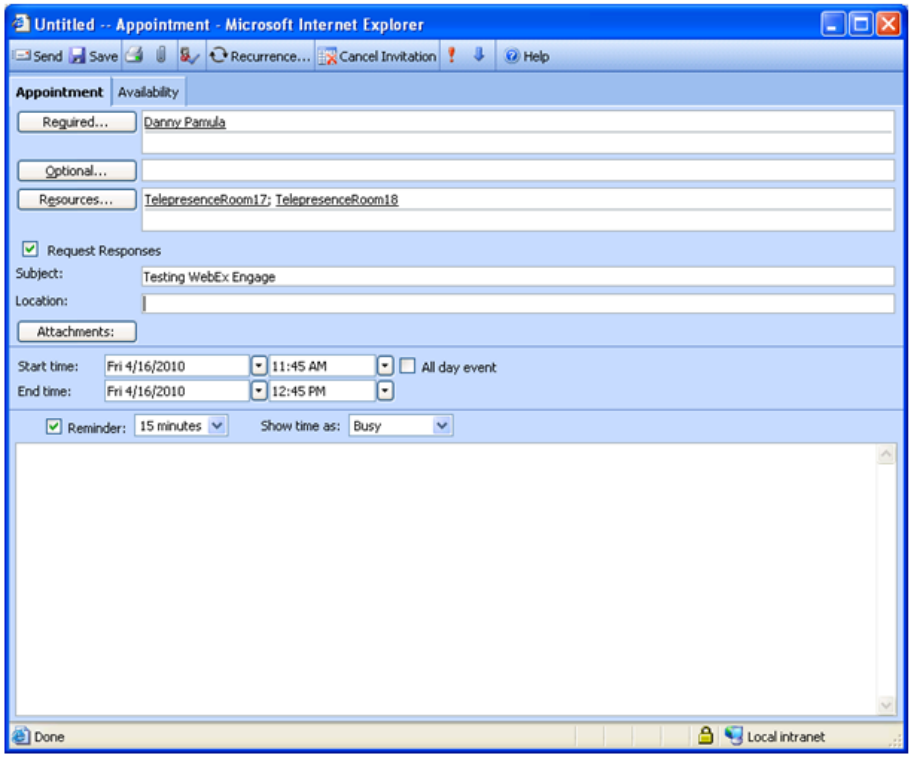
  You schedule and add WebEx to your meeting in Microsoft Outlook.

Using Calendar Client and Meeting Manager

To schedule a TelePresence meeting with WebEx using a calendar client and Meeting Manager, do the following:

Step 1 Schedule the meeting as usual with Microsoft Outlook, Lotus Notes or another supported client and include one or more Cisco TelePresence System (CTS) endpoints. See the Configuring Microsoft Exchange for Cisco TelePresence Manager, page 3-1 for instructions.

Figure 12-6 Schedule Meeting

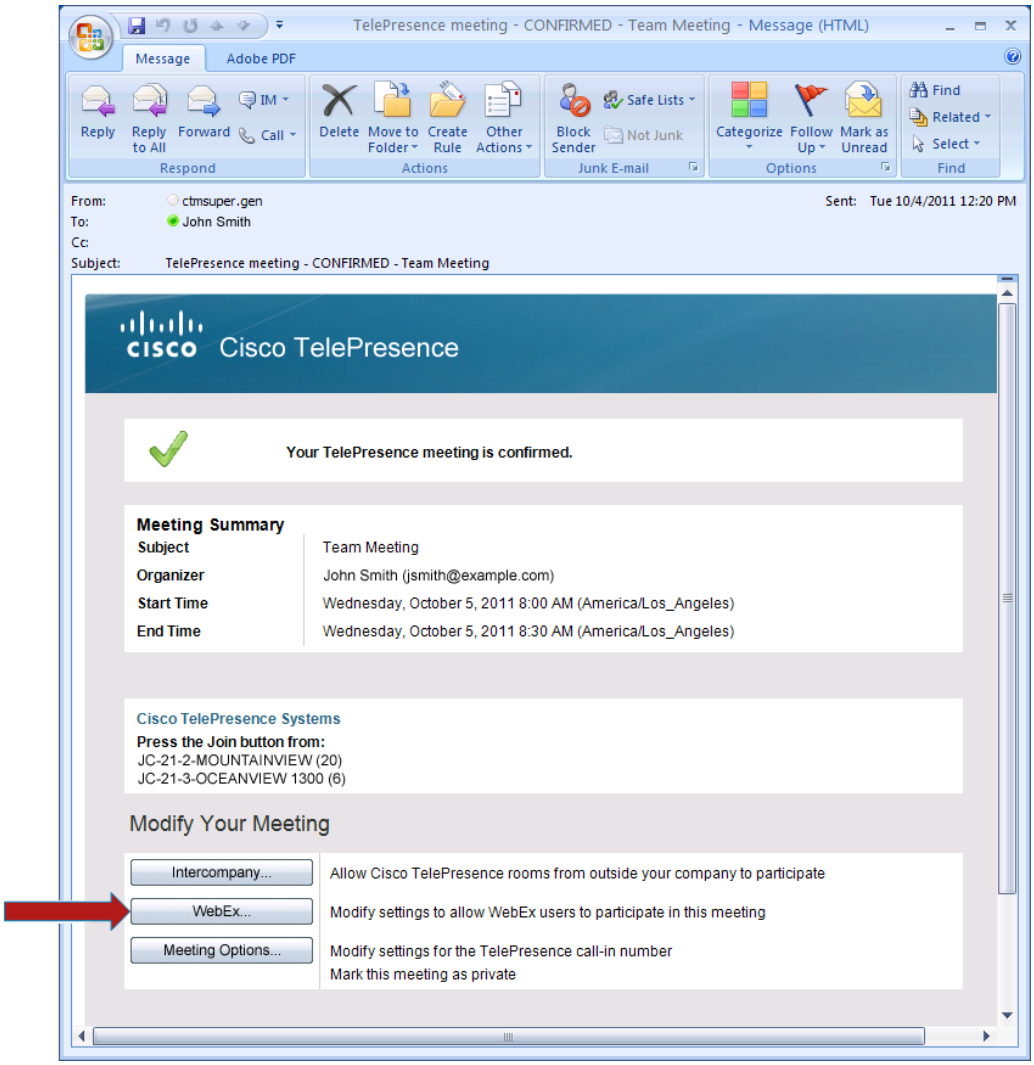


Step 2 Wait for email confirmation from CTS-Manager.

Step 3 To enable WebEx for the meeting, click the **WebEx** button in the email, as shown in Figure 12-7.

- The WebEx button does not appear if the meeting organizer is a WebEx Non-Permitted user.

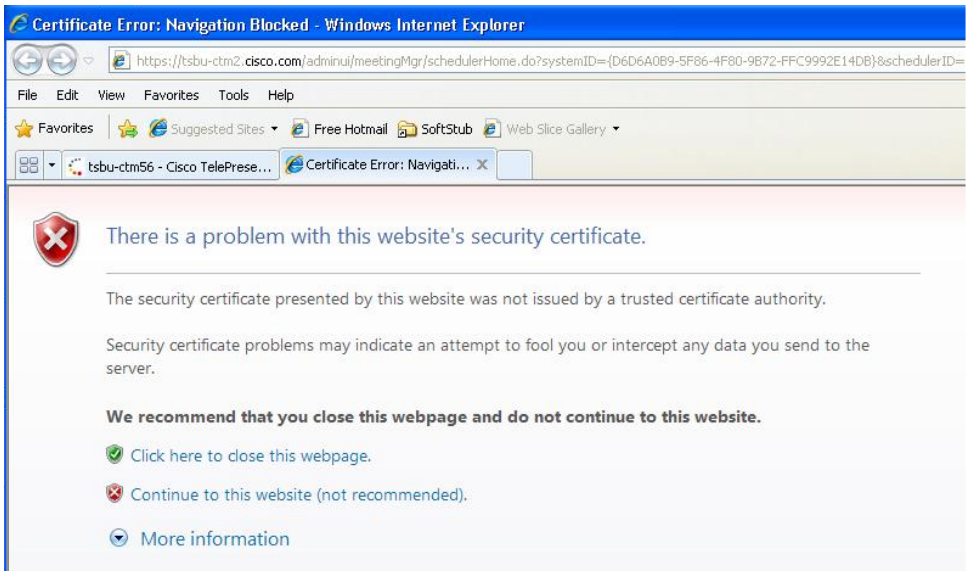
Figure 12-7 Click the WebEx Button in Meeting Email Confirmation



Step 4 Depending on which browser you use, you may be presented with a security warning message:

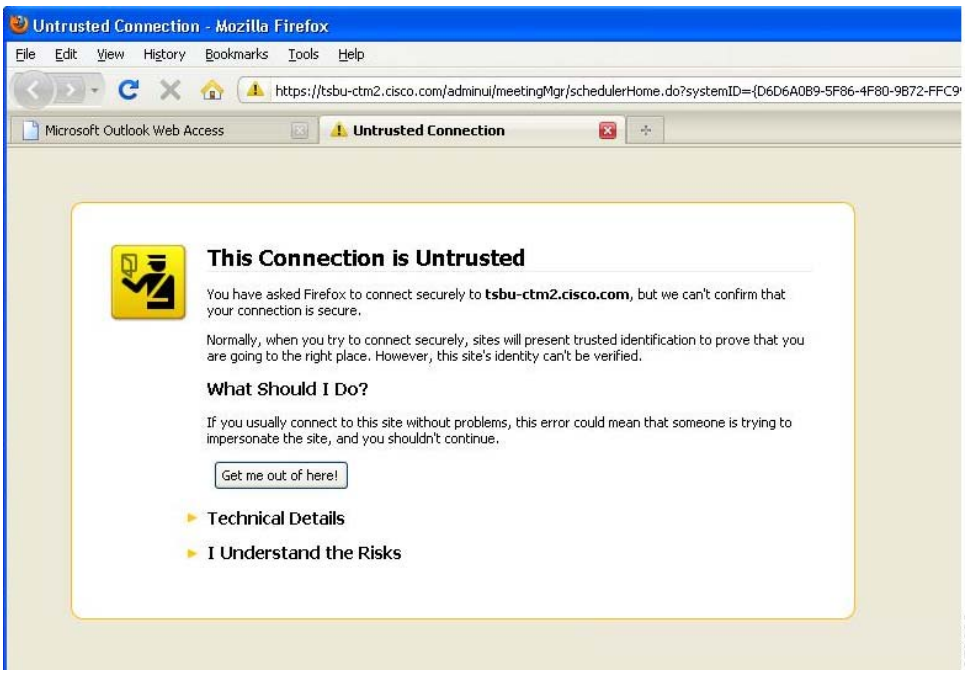
- If you are using Internet Explorer Version 8 and a security warning appears, click **Continue** to proceed, as shown in Figure 12-8.

Figure 12-8 Security Warning in Internet Explorer Version 8



- If you are using Firefox and a security warning appears, click **"I understand the risks**" to proceed, as shown in Figure 12-9.

Figure 12-9 Security Warning in Firefox



Step 5 Once you have dismissed any security warnings, the CTS-Manager log in window appears, as show in Figure 12-10.

Figure 12-10 CTS Manager Log In

Step 6 Log in to CTS-Manager using your enterprise email ID and password.

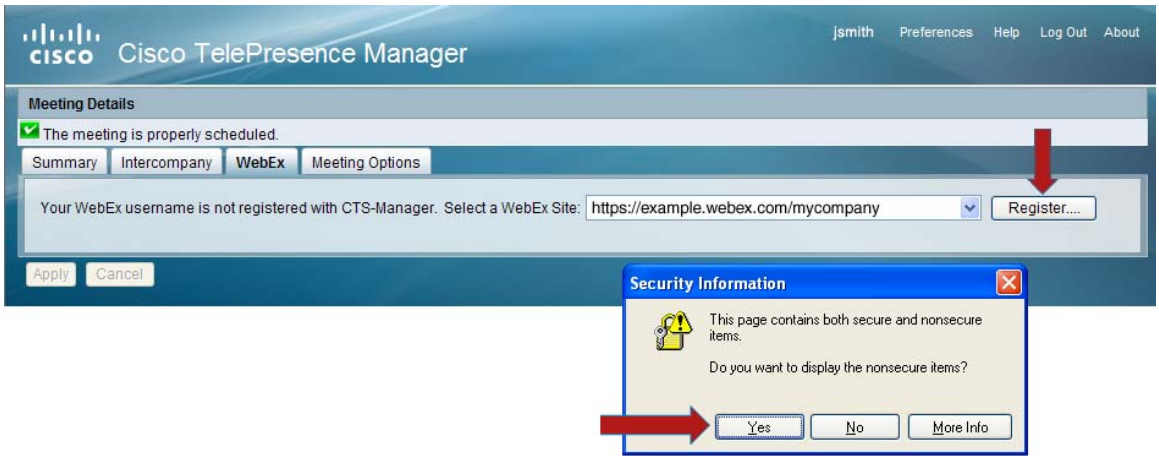
The meeting details window for your meeting appears, with the WebEx tab selected.

Step 7 The first time you schedule a meeting with WebEx, you must register your WebEx account with CTS-Manager by doing the following:

a. If there are multiple WebEx sites available, select the WebEx site on which you have an account.

b. Click **Register**.

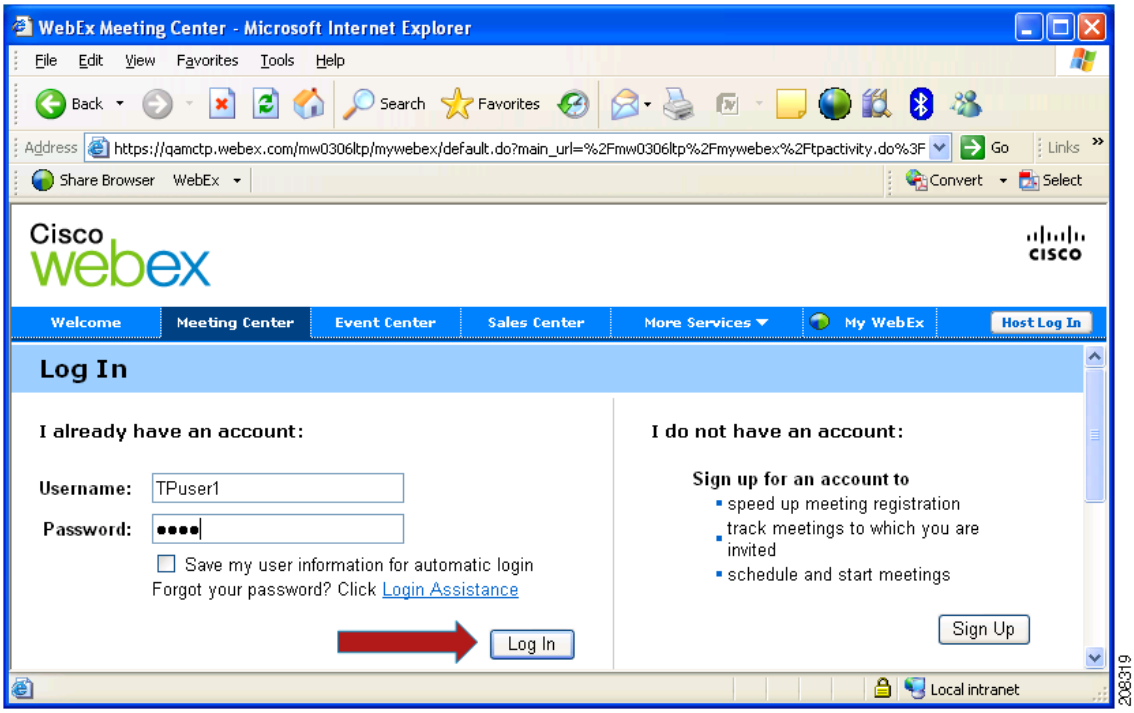
Figure 12-11 Authenticate with Cisco WebEx Internet Explorer Version 7



- If you are using Internet Explorer Version 8, click **Register** and click **No** at the security warning pop-up.
- If you are using Firefox, there is no security warning at this step; simply click **Register**.

This redirects you to the Cisco WebEx site. The Cisco WebEx login page appears, as shown in Figure 12-12.

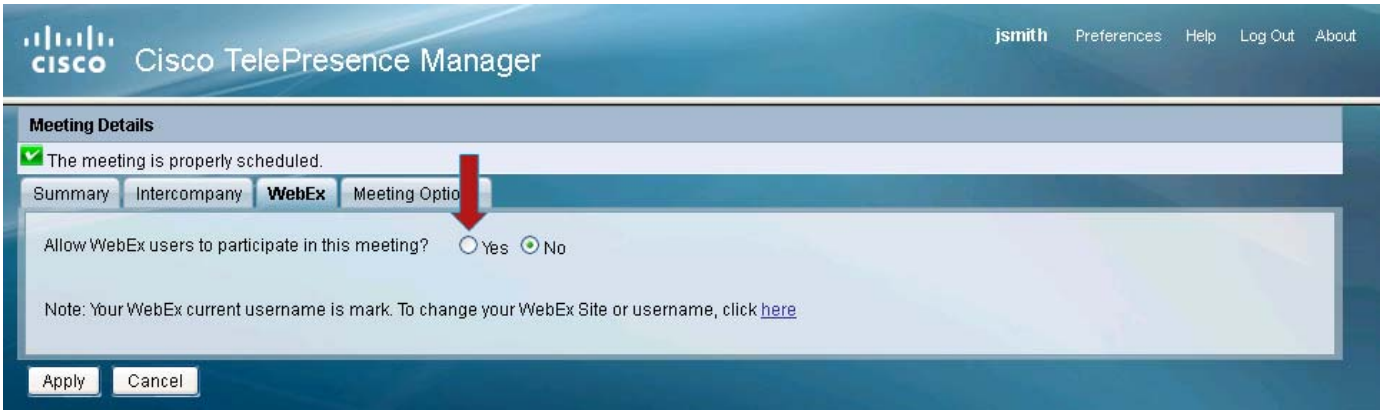
Figure 12-12 Log in to Cisco WebEx



c. Enter your Cisco WebEx username and password and click **Log In**.

Upon successful authentication, you are directed back to the CTS-Manager meeting details window with the WebEx tab selected, as shown in Figure 12-13.

Figure 12-13 Cisco WebEx Tab in CTS Manager Meeting Details



Step 8 Select the **Yes** radio button to allow WebEx users to participate in this meeting and click **Apply**.

WebEx OneTouch is now set up for the meeting organizer and enabled for the selected meeting. To schedule future meetings with WebEx, you will not need to log in to the Cisco WebEx site.

Using Microsoft Outlook and the WebEx Productivity Tools Plug-in

To use Microsoft Outlook and the WebEx Productivity Tools plug-in to schedule a TelePresence meeting with WebEx, do the following:

Step 1 Download and install the WebEx Productivity Tools plug-in.

a. Open a browser and go to the WebEx site on which you have an account.

b. On the left-hand side of the window, click **Support** and then **Downloads**.

Note If you do not see Support, make sure the Meeting Center tab is selected at the top of the window.

c. Next to the Productivity Tools description click **Download now (Login Required).**

d. Log in to your account using the username and password of your WebEx account.

e. Next to the Productivity Tools description click **Download now**.

f. Install the plug-in:

- For IE: the File Download window appears. Click **Run** and follow the on-screen instructions to install the plug-in.
- For Firefox: the Opening ptools.msi window appears. Click **Save File**. After the file is downloaded, open it and follow the on-screen instructions to install the plug-in.

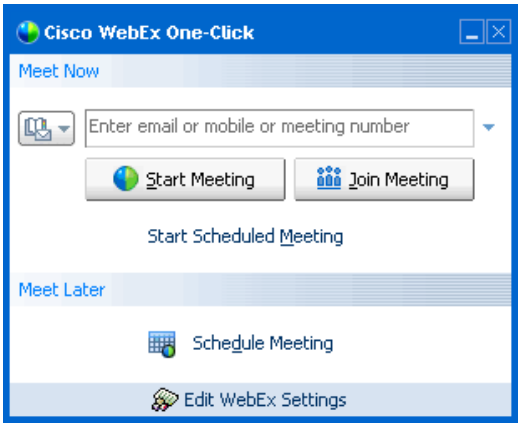
  When installation is complete, the WebEx Productivity Tools window appears.

Figure 12-14 WebEx Productivity Tools window

g. Enter your WebEx User Name and Password and click **Login**.

In a few moments, you will be logged into the WebEx server. When the installation is complete, the Cisco WebEx One-Click window appears.

Figure 12-15 Cisco WebEx One-Click window

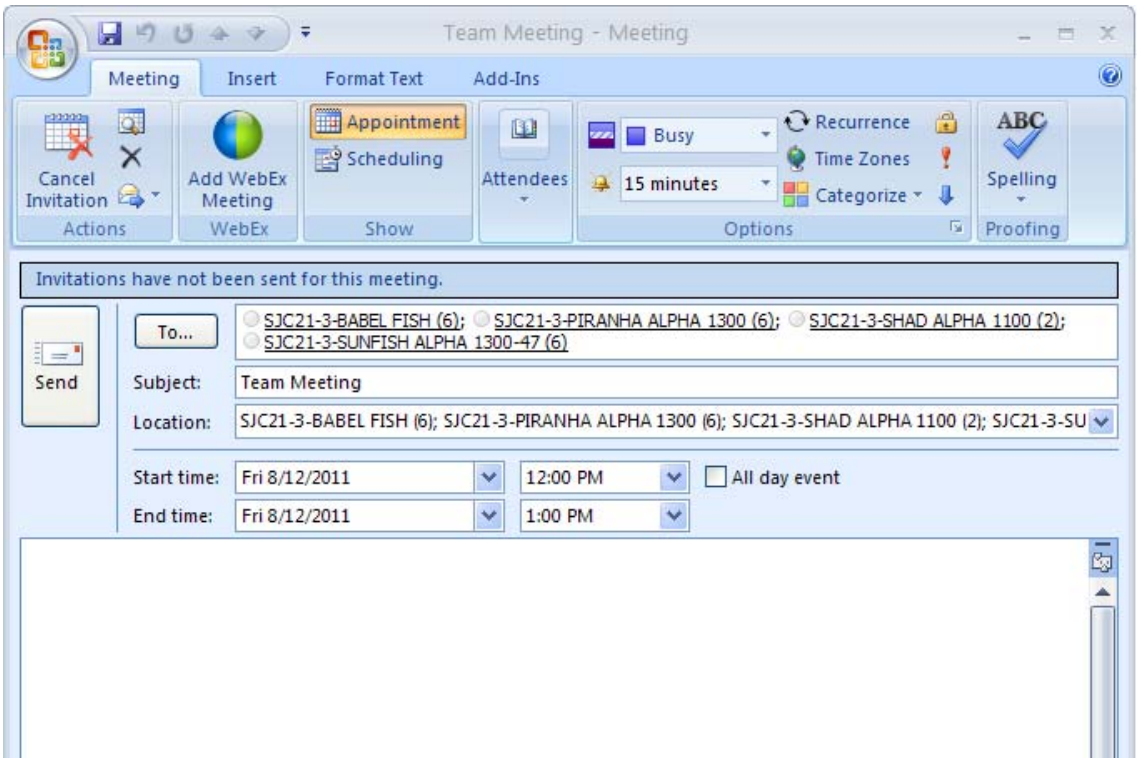


h. Close the Cisco WebEx One-Click window.

Step 2 Open Microsoft Outlook

Step 3 Schedule the meeting as usual and include one or more Cisco TelePresence System (CTS) endpoints.

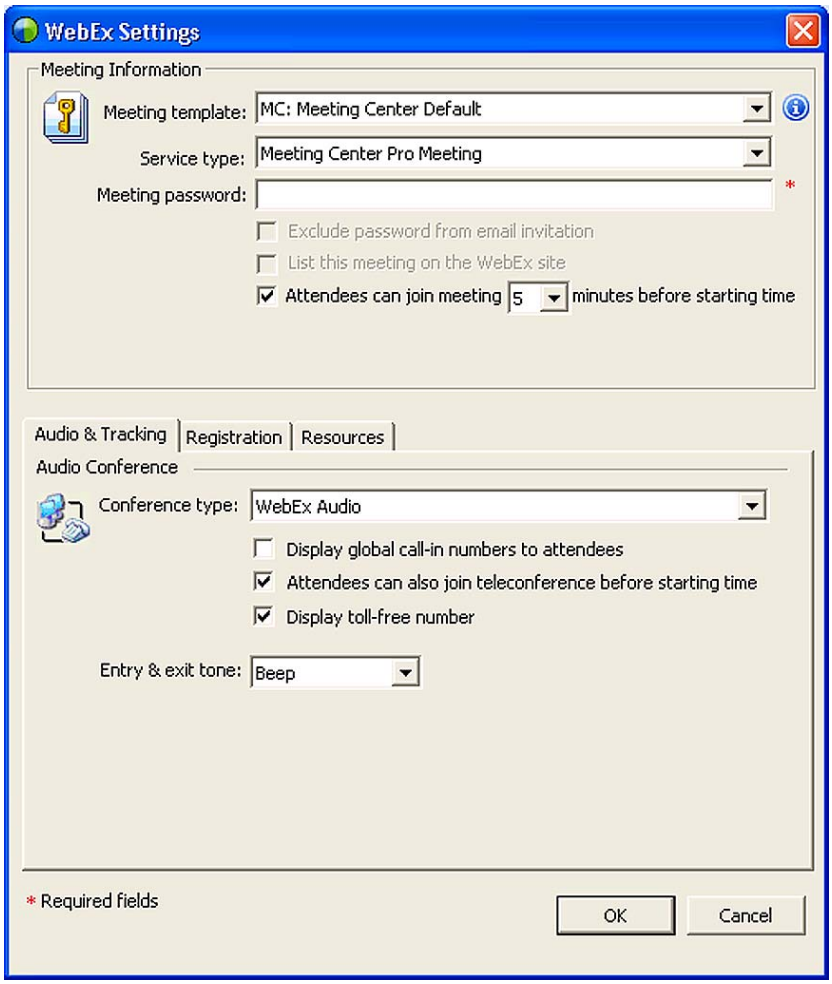
Figure 12-16 Schedule Meeting



Step 4 Click the **Add WebEx Meeting** button in the top part of the Meeting window.

Step 5 The WebEx Settings window appears.

Figure 12-17 WebEx Settings window



Step 6 (Optional) If you want to create a password for the meeting, enter it in the Meeting Password field.

Step 7 Make sure Service type is set to **Meeting Center Pro Meeting** and Conference type is set to **WebEx Audio** and click **OK**.

Note Both of these selections are required or WebEx will not work properly.

Step 8 Click **Send** to send the meeting invitation.

The WebEx information is added to the meeting invitation and then it is sent.

Step 9 After the meeting is confirmed, you will receive a meeting confirmation email from CTS-Manager which also includes the WebEx information along with the other meeting details.

Note After first-time scheduling, WebEx users configured as Premium Users have WebEx added to their Cisco TelePresence meetings automatically. WebEx Permitted Users must enable WebEx for each meeting. To prevent overscheduling Webex when the feature is used for most TelePresence Meetings, Cisco recommends to not add all users to the Premium user group. For more information about WebEx users, see WebEx User Types, page 12-12.

Notes About Using CTS-Manager and the WebEx Productivity Tools Plug-in for Adding WebEx to TelePresence Meetings

WebEx enabled via Outlook takes precedence over WebEx enabled via the Meeting Manager window of CTS-Manager. For example, if the meeting organizer schedules a TelePresence meeting and adds WebEx via CTS-Manager and later, enables WebEx using Outlook, the plug-in generated WebEx meeting information will replace the WebEx information enabled via CTS-Manager.

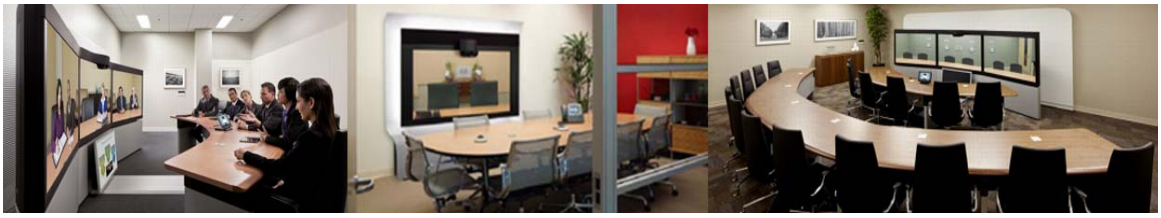
If the meeting organizer enables WebEx via the Outlook plug-in, they can only disable WebEx using the plug-in (by clicking **Cancel WebEx** in Outlook).

Configuring Other Applications

For the Cisco TelePresence WebEx OneTouch feature to work, other applications, including CTMS, must also be configured. For complete details on how to configure and use this feature, refer to the "Cisco WebEx OneTouch Configuration Guide for the Cisco TelePresence System" at the following URL:

http://www.cisco.com/en/US/docs/telepresence/cts_admin/webex_solutions/guide/cts_webex_config.html

This document also describes how to manage and monitor scheduled meeting interoperability between Cisco TelePresence System (CTS), Cisco TelePresence MultiPoint Switch (CTMS) multipoint meetings, CTS-Manager, Cisco Unified Communications Manager (Cisco Unified CM), and the Cisco WebEx meeting server.



CHAPTER 13

Monitoring and Supporting Cisco TelePresence Manager

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

Contents

- Introduction, page 13-2
- Post-Install Guidelines for CTS-Manager, page 13-2
- Meetings, page 13-3
- Status Dashboard, page 13-14
- Metrics Dashboard, page 13-16
- TelePresence Utilization, page 13-21
- Meeting Benefits, page 13-23
- VC Utilization, page 13-24
- Users, page 13-25
- Command Line Interface, page 13-43
- Bridges and Servers, page 13-33
- Unified CM, page 13-42
- Command Line Interface, page 13-43

Introduction

CTS-Manager monitoring features allow you to monitor:

- Scheduled meetings
- Status of system services
- Meeting benefits and survey results
- TelePresence and video conferencing endpoint utilization
- Users

Note The meeting benefits, survey results and endpoint utilization monitoring features require the Reporting API and Meeting Benefits license. For more information, see Licensing for CTS-Manager.

Post-Install Guidelines for CTS-Manager

The purpose of this chapter 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 13-1 Post-Install Guidelines for CTS-Manager

Setup Procedure Guidelines after Installing CTS-Manager	Description	Location
Monitoring and Supporting 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 and acceptance email to the meeting organizer, with the notice that the endpoints 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 14, "Meeting Manager and CTS-Manager Emails"

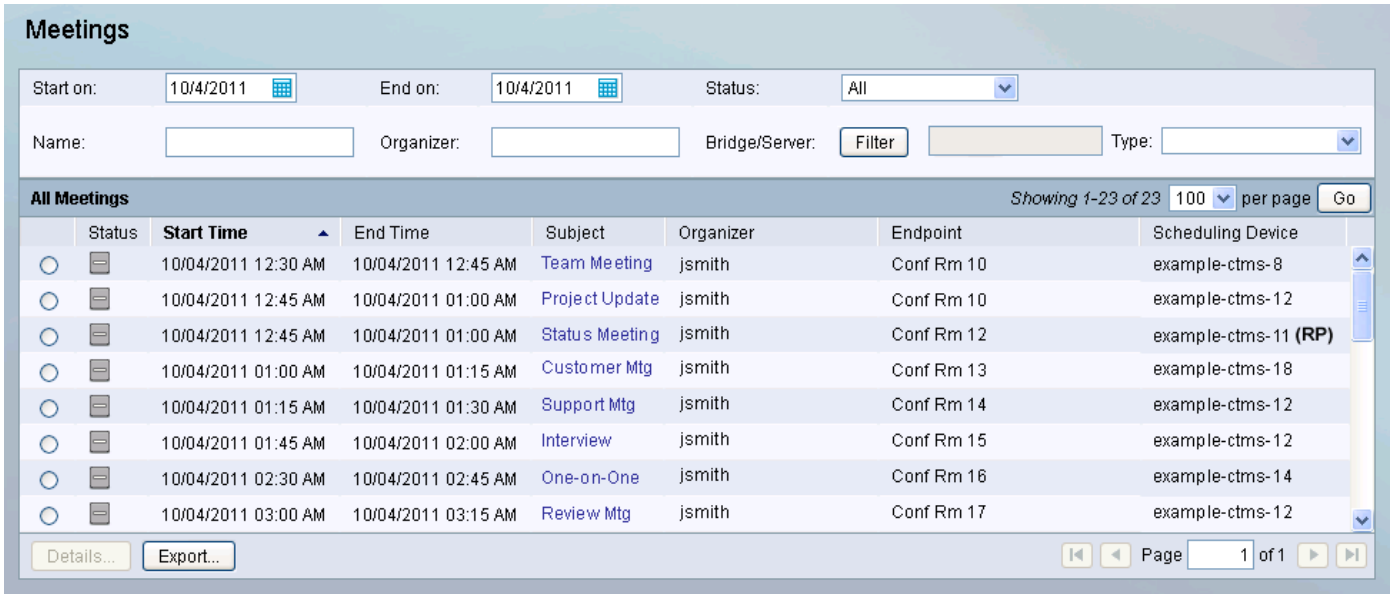
If at any time you encounter problems, go to Chapter 16, "Troubleshooting Cisco TelePresence Manager" to see how to correct the problem.

Meetings

The Monitor > Meetings window allows you to view information about the scheduled meetings, including:

- Status
- Start Time
- End Time
- Subject
- Organizer
- Endpoint
- Scheduling Device

Figure 13-1 Meetings window



When a 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.

The Rendezvous Point of a CTMS Network Multipoint meeting is indicated with **(RP)** next to the CTMS.

Note A maximum of 5 concurrent users can filter an endpoint.

The 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.

Warning **When a meeting organizer modifies their meeting in Microsoft Outlook, they must click the Send Update button for the changes to be sent to CTS-Manager.**

Note If meetings do not appear automatically in CTS-Manager, you must do a manual sync. Make sure you can ping the CTS-Manager hostname from the Exchange server.

Note If you remove an endpoint (room) from Microsoft Exchange and it is not removed from a meeting in CTS-Manager, schedule at least one meeting for the affected room in Exchange, then resync the endpoint in CTS-Manager by going to **Configure** > **Microsoft Exchange**, selecting the endpoint and clicking **Resync**.

Note When using the CTS-Manager Reporting API to retrieve information about meetings scheduled with a TelePresence Server, Call Detail Record (CDR) information is not available.

Call Detail Record Information for Point-to-Point Meetings with C, EX and MX-series Endpoints

Call Detail Record (CDR) information is available for point-to-point meetings scheduled with C, EX and MX-series endpoints in the following ways:

- Meetings that contain C, EX and MX-series endpoint(s) only:
  - CDR date is displayed after the meeting is completed.
  - Meetings that are in progress, display a status of “Scheduled”.
- Meetings that contain one or more C, EX or MX-series endpoints and one or more CTS endpoints:
  - If the meeting is started by a C, EX or MX-series endpoint, the CDR data will be available after the meeting is completed and meetings that are in progress, display a status of “Scheduled”.
  - If the meeting is started by a CTS, the CDR data for meeting Start Time and End Time are available in real time.

The CDR limitations of C, EX and MX-series endpoints are due to the fact that Meeting ID is not provided along with meeting start event.

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 rooms (endpoints) are in auto-accept mode. A room (endpoint) 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’s screen 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

- After modifying a meeting from Microsoft Outlook, you must click the Send Update button to send the updated information from Microsoft Exchange to CTS-Manager.
- If a meeting organizer updates the Subject field of a meeting scheduled with Lotus Notes that has already been synced with CTS-Manager, the phone’s screen is not updated.
- It is advisable to avoid modifications to a meeting a few minutes before its start time.

- If a meeting is changed within a few minutes of the meeting's start time (such as a time change, or endpoint change), the change may not appear on the endpoint phone's screen for that endpoint, or in the Scheduled Meetings window of CTS-Manager. This does not affect a user's ability to schedule a new meeting at the original (pre-modified) time.
- A notification email is not generated if a meeting is processed as part of a server startup.
- No notification email is generated if a meeting is deleted from Outlook or Lotus Notes.
- Modifications to an in-progress or completed meeting, except for time, are ignored.
- Time modifications to an in-progress/completed meeting will generate a new meeting with the new time. The in-progress/completed meeting will remain unchanged.
- In order for Exchange to alert CTS-Manager to scheduled meeting changes, it is advisable not to make changes to the scheduled meeting from the calendar/mailbox of the TelePresence endpoint. Doing this may cause Exchange to not send an invite to the meeting organizer and, as a result, CTS-Manager will not get the notification to process the meeting accordingly.

Note Tentative room reservations in CTS-Manager are not supported with 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 Enter the endpoint name in the **Name** field.

Step 2 Enter the user name of the meeting organizer in the **Organizer** field.

Step 3 From the **Status** drop-down list, choose the All, Needs Help, With Error, In Progress, Scheduled, Completed, No Show, Not TelePresence meeting status.

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

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

Step 5 Enter the name of the bridge or server.

Step 6 Click **Filter**.

Table 13-2 describes the Meetings information.

Table 13-2 Meetings Information

Field or Button	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 (displayed when moving your mouse pointer over the displayed icon). **Note** A meeting that has been started, is shown as In Progress. When a TelePresence meeting is ended, the meeting is shown as Completed. A meeting can be started multiple times before its scheduled end time. **Note** Meetings scheduled using a TelePresence Server only display the status of Scheduled. To determine if the meeting is In Progress or Completed, you must access the TelePresence server. **Note** In-progress point-to-point meetings between two EX or C series endpoints show as Scheduled until they are completed. If meeting includes a CTS, it will show as In Progress.
Subject	Information (such as the meeting subject) provided by the meeting organizer about the meeting. **Note** If the meeting organizer did not create a subject for the meeting, “No Subject” is displayed in this window and a dash (-) is displayed on the endpoint phone/display device.
Organizer	Login name of the person who scheduled the meeting. Click the arrow in the header of the Organizer column to sort the list in ascending or descending alphabetical order.
Endpoint	Endpoint (room) name as specified in the Microsoft Exchange or IBM Domino database.
Scheduling Device	Multipoint scheduling device used for meeting (if multipoint meeting). **Note** The Rendezvous Point of a CTMS Network Multipoint meeting is indicated with (RP) next to the CTMS.
Details	Click this button to view detailed information about a selected meeting. See Meeting Details, page 13-8 for more information.

Table 13-2 Meetings Information (continued)

Field or Button	Description or Setting
Export	Click this button to export your meeting data in tab-separated value (.tsv) format. Information includes: • Meeting type (single or recurring • Status • Endpoint • Organizer • Subject • MCU • Features enabled/disabled: – Video Conferencing – Intercompany – Recording – WebEx – Number to Dial Meeting Subject on Phone
Open Collaboration Manager	Click this button to open Cisco Prime Collaboration Manager (CM) for a selected meeting. Cisco Prime CM is a web-based user application for managing and troubleshooting end-to-end video collaboration, over a borderless network. It provides a real-time unified view of all Cisco TelePresence sessions that are in progress. The Collaboration Manager button does not appear unless it is configured in CTS-Manager. To configure Collaboration Manager, go to Configure > Bridges and Servers.

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 13-2 Viewing Exported Scheduled Meeting Data

	A	B	C	D	E	F	G	
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 [M All]**
2	2/10/2009 10:00	2/10/2009 10:30	Recurring Meeting (Instance)	No Show	TelepresenceRoom31 || TelepresenceRoom32 || TelepresenceRoom33	chen@example.com	3 days no end	
3	2/10/2009 11:00	2/10/2009 11:30	Single	Scheduled	TelepresenceRoom32 || TelepresenceRoom31	superuser@example.com	Testing again	
4	2/10/2009 15:00	2/10/2009 15:30	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom32 || TelepresenceRoom31	shrivastav@example.com	more than 800 occurrences	
5	2/11/2009 15:00	2/11/2009 15:30	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom31 || TelepresenceRoom32	shrivastav@example.com	more than 800 occurrences	
6	2/12/2009 11:30	2/12/2009 12:00	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom31 || TelepresenceRoom32	Motwani@example.com	Test 1	
7	2/12/2009 15:00	2/12/2009 15:30	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom32 || TelepresenceRoom31	shrivastav@example.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@example.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@example.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@example.com	3 days no end	
11	2/13/2009 14:32	2/13/2009 14:49	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom33 || TelepresenceRoom32	chen@example.com	daily no end	
12	2/13/2009 15:00	2/13/2009 15:30	Recurring Meeting (Instance)	Scheduled	TelepresenceRoom32 || TelepresenceRoom31	shrivastav@example.com	more than 800 occurrences	
13								
14	Report generated at: Tuesday, February 10, 2009 11:01 AM (America/Los_Angeles)							

Meeting Details

The meeting details window provides detailed information about a specific meeting and allows the administrator to make changes to the meeting's settings and correct possible errors.

To access the meeting details window:

Step 1 Click the radio button next to the scheduled meeting to select it.

Step 2 Click **Details**.

The meeting details window appears displaying summary information for the selected meeting.

Tip You can also click the meeting subject to open the meeting details window.

The Meeting Details window is divided into the following tabs:

- Summary
- Bridges and Servers
- CTMS Network
- Intercompany
- WebEx
- Usage Survey
- Meeting Options

Summary

The Summary tab provides basic information about the meeting.

Table 13-3 Meeting Details Summary 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.
Time	Displays the date, time and duration of the meeting.
Endpoints	Lists the endpoints that are participating in the meeting.
Notification Email	If the system is set up for email notification, clicking the Send Email button sends a meeting confirmation email to the meeting organizer.
WebEx	Displays the WebEx information (if used) for the meeting.
Intercompany	Displays the Intercompany information for the meeting.
Video Conferencing Interop	Displays the video conferencing interoperability information for the meeting.
Record Meeting	Displays the video recording information for the meeting (if a single-endpoint meeting).
Hide Meeting Subject	Displays whether the meeting subject will be displayed on the TelePresence phone or not.
Not a TelePresence Meeting	Indicates if the meeting is not a TelePresence meeting.

Bridges and Servers

The bridges and servers tab appears if the meeting is a multipoint meeting (three or more endpoints are scheduled). This window displays how many scheduling devices and endpoints are reserved for the meeting and allows the administrator to migrate the multipoint meeting from one CTMS to another and change the Cisco Media Experience Engine (MXE) assigned to the meeting, if Interoperability with Video Conferencing is enabled. If the meeting is a network multipoint meeting, two or more CTMS devices are displayed and the Rendezvous Point CTMS is noted with an '(RP)' next to it.

Note If an MXE video conference (VC) endpoint is added to a meeting with one CTS endpoint, it becomes a multipoint meeting, even though there are only two endpoints. 1 CTS and 1 MXE VC endpoint = multipoint meeting pushed to CTMS

Table 13-4 Bridges and Servers Tab

Field or Section Name	Description
Call-In Number	The call-in number for TelePresence endpoints to attend the meeting, if selected by the meeting organizer. If it is not selected by the meeting organizer the call-in number still exists, but is not published to the meeting organizer or participants.
Meeting Number	The unique ID number generated by CTS-Manager to identify the scheduled meeting.
Scheduling Device	The scheduling devices used for the meeting. The Rendezvous Point of a CTMS Network Multipoint meeting is indicated with **(RP)**. The CTMS to which the call-in number is associated is indicated with a phone icon. If a CTMS is part of a device group, the group is displayed in parentheses () next to the CTMS name. You have the option to migrate the meeting to a different scheduling device, by selecting it from the drop-down menu corresponding to the scheduling device from which you want to migrate. Network multipoint meetings only support CTMS devices, so migration will only be possible to another CTMS. Migration of CTMS devices for multipoint meetings is supported only with CTMS 1.9 or later. **Note** If you migrate a CTMS to a TS and your meeting has the following features: Studio Mode Recording, WebEx, Intercompany or Extend Multipoint Meetings, those features will be removed, because TS is not compatible with them.
Endpoint	The endpoints used for the meeting
Bridge Call-In Number	The call-in number for video conferencing endpoints to attend the meeting. **Note** Video conferencing is not permitted when Intercompany is in use or if Studio Mode Recording is enabled.
MXE Associated	The MXE used for the meeting (if applicable). **Note** If Interoperability with Video Conferencing is enabled, multipoint meetings require a CTMS and an MXE in a scheduled state.

Guidelines for Migrating CTMSs for Network Multipoint Meetings

When migrating CTMSs associated with a network multipoint meeting, follow these guidelines:

- Only one CTMS can be migrated at a time
- Destination CTMSs must be running release 1.9 or later software
- Destination CTMSs must have enough resources to support the meeting that is being migrated
- If it is a recurring meeting, the destination CTMSs must have enough resources to support all occurrences of the meeting that is being migrated
- If Intergroup Scheduling is disabled, the source and destination CTMSs must be in the same device group.
- To migrate all meetings on a CTMS, including NMP meetings, go to Configure > Bridges and Servers. For more information, see Editing a Bridge or Server, page 11-60.

CTMS Network

The CTMS Network tab appears only if the meeting is a network multipoint meeting. This window displays the scheduling devices and endpoints that are reserved for the meeting, including their device group and time zone. Also displayed is the number of CTMS segments reserved for the meeting.

Table 13-5 CTMS Network Tab

Field or Section Name	Description
Name	Name of device
Type	Type of device (CTMS or endpoint model). If the CTMS is a rendezvous point, **(RP)** will be displayed.
Device Group	Group to which the device belongs
Description	Description of the device
Time Zone	Time zone of the device

Intercompany

The Intercompany window provides the ability to schedule TelePresence meetings with other companies.

To enable this feature, click **Yes** and then click **Apply**.

Table 13-6 Intercompany Tab

Field or Section Name	Description
Does this meeting include TelePresence endpoints from another company?	Select Yes to enable Intercompany TelePresence for the meeting. **Note** Additional fields appear when Intercompany is enabled.
Which company will host the TelePresence multipoint bridge?	Select Our Company if your company will be hosting. Select Another Company if another company will be hosting. **Note** Selecting this option will reveal additional fields.
Enter the sum of TelePresence resources required by all other companies participating in this meeting. (This field appears only if Our Company is selected.)	If your company is hosting, you must get the total number of resources required from all other companies participating and enter the number in this field. 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
Enter the following information provided by the meeting host when Another Company is hosting	
Intercompany Call-In Number	This is the phone number your Cisco TelePresence endpoint phone/display device will call to join the meeting. This number is provided by the meeting Host's CTMS or your Service Provider's CTMS.

Table 13-6 Intercompany Tab

Field or Section Name	Description
Intercompany Meeting Number	This number is generated by the host's CTMS or your service Provider's CTMS
The host needs to know that your endpoints require Telepresence Resources.	If another company is hosting an Intercompany Cisco TelePresence meeting, the number of resources required for your endpoints to participate is listed. Provide this number to the host at the other company.

Note For a CTMS Network Multipoint Intercompany meeting, participants from the other companies (not hosting the meeting) always dial directly into Rendezvous Point (RP) CTMS.

Recurring Intercompany Meetings

If you make changes to a recurring intercompany meeting, those chnages are applied to all future instances of the meeting. It is not possible to change a single instance only.

WebEx

The WebEx window displays WebEx information for the meeting and provides the ability to enable or disable WebEx for the meeting.

Note If the meeting organizer's WebEx username is not registered with CTS-Manager, WebEx cannot be enabled for the meeting.

Allow WebEx users to participate in this meeting

Selecting **Yes** enables WebEx for this meeting. Selecting **No** disables Webex for this meeting.

WebEx Call-In Information

This section displays the WebEx information necessary for both the host and participants to join the meeting

Table 13-7 WebEx Tab

Field or Section Name	Description
Call-in Toll Free Number	Toll free number for WebEx participants.
Call-In Toll Number	Toll number for WebEx participants.
WebEx Meeting Host Key	Code for host to regain control of the meeting from an attendee.
WebEx Meeting ID	The unique ID number generated by WebEx to identify the scheduled meeting.
Meeting Password	Password for WebEx participants.
URL	URL for WebEx meeting.

Usage Survey

The Usage Survey window displays the survey, as set up by the administrator in the Configure > Application Settings > Usage Survey window.

Note This tab is not available if the Metrics Dashboard and Reporting API license has not been uploaded in the Configure > Licenses > License Files window.

Meeting Options

The meeting options window allows the meeting organizer to adjust other options for their meeting.

Note Meeting options are different for Intercompany Meeting. See the Intercompany, page 13-11 sections, for more information.

Mark this meeting as private: Allows you to show or hide the TelePresence meeting subject on the phone of the TelePresence endpoint.

Provide a call-in number for other participants?: Allows you to provide a call-in number for TelePresence endpoints that were not originally invited to the meeting to be able dial in to the meeting.

The following two options are available only for a meeting scheduled with one endpoint (room):

Is TelePresence Needed For This Meeting?: Allows you to enable or disable TelePresence for the meeting.

Is this meeting intended for recording a video to be distributed later?: Allows you to record the meeting for distribution later.

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

Status Dashboard

The Monitor > Status Dashboard window displays a concise list of system activity, including a snapshot of scheduled meetings for the day and 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 endpoint-scheduling functions.

To update the Status Dashboard, click the **Force refresh** icon.

Figure 13-3 Monitor > Status Dashboard

Table 13-8 Status Dashboard Fields and Descriptions

Field	Description or Setting
Today's Meetings	Status of current and upcoming meetings: • With Error—Displays the number of meetings that have errors. • All Meetings—All meetings scheduled for today. Click the link associated with each meeting or device's information to go to the Meetings window.
Devices	Status information for the following devices: • Bridges and Servers—Clicking the link displays the summary information in the Support > Bridges and Servers window and filters the list to those bridges and servers with an error status. • Application Servers—Clicking the link displays the summary information in the Cluster Management > Application Servers window. (Only appears if CTS-Manager is part of a cluster). Cisco no longer provides support for the clustering feature originally introduced in release 1.8. For questions, contact Ron Lewis: ronlewis@cisco.com. • Database Servers—Clicking the link displays the summary information in the Cluster Management > Database Servers window. (Only appears if CTS-Manager is part of a cluster). Cisco no longer provides support for the clustering feature originally introduced in release 1.8. For questions, contact Ron Lewis: ronlewis@cisco.com. • TelePresence Endpoints—Clicking the link displays the status information in the Support > Endpoints window. • VC Endpoints—Clicking the link displays the status information for VC endpoints in the Support > Endpoints window. • Unified CM—Clicking the link displays the information in the Support > Unified CM window. **Note** An error may occur if the connection to Unified CM was caused by a network outage. You can remove the error status by restarting Cisco TelePresence Manager.
Indicators	Status Indicators for: • Database Backup • Current Database Size • Mailbox is • Endpoint Mailbox Sync
Time	Status of the following times: • 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.

Table 13-8 Status Dashboard Fields and Descriptions (continued)

Field	Description or Setting
Services	Status information for the following system services: • Calendar Service • WebEx (if enabled) • LDAP Server • Endpoint Control • Database • Multipoint Conference • Unified CM Status is either **OK** or is a highlighted link listing the number of errors. You can click a link to see further system log status information and troubleshoot problems. You can also roll your mouse over a highlighted link to see a brief description of the error.
Uptime	Status information about the elapsed running time since the last restart. • Services—Services displayed in the Services section. • TelePresence Engine—Cisco TelePresence database engine. • System Platform—Hardware host for CTS-Manager.

Metrics Dashboard

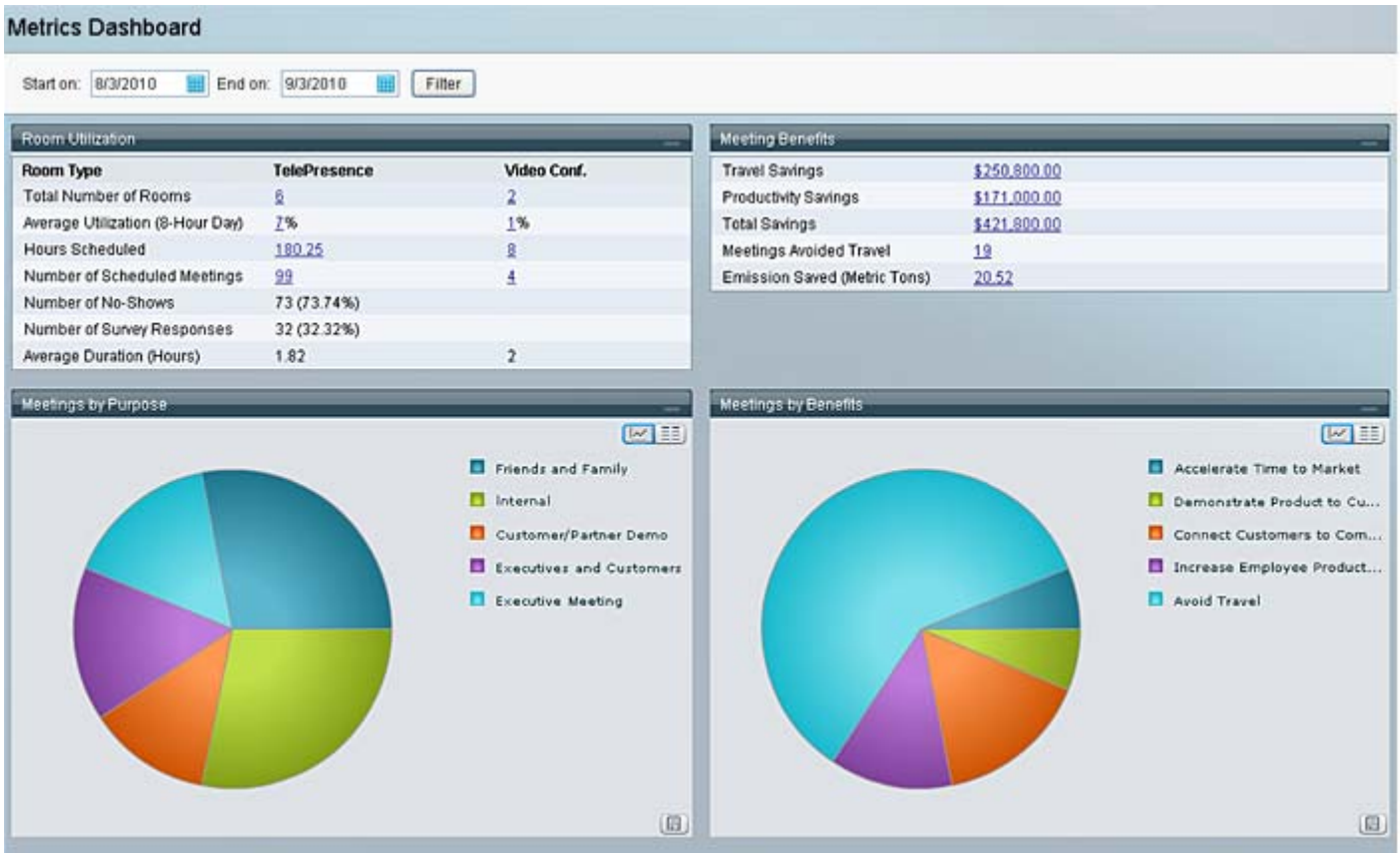
The Monitor > Metrics Dashboard window displays system-wide information about how TelePresence endpoints are used and the associated benefits of their usage.

Caution Changing parameters in the Meeting Benefit Report Parameters of the Configure > Application Settings Usage Survey window changes the Metric Dashboard data retroactively.

To view information for a specific range of time:

- Select dates for Start on and End on and click **Filter**.

Figure 13-4 Monitor > Metrics Dashboard



Note You can enter a date or click the calendar icon to select a date from the calendar.

Except for the Endpoint Utilization and Meeting Benefits information, the information in this window can be viewed in a graphical format. You can view the information either as a chart or a list (grid).

To view information as a chart, click the **View as Chart** button. This is the default view.

View as Chart

Note When viewing information in a pie chart, roll your mouse over the different colored areas to see the exact percentage for each area and the number of survey respondents that provided that answer. When viewing information in a line chart, roll your mouse over different points on the line to see the exact numbers for specific dates.

To view the information as a list, click the **View as Grid** button.

View as Grid

To open a chart as an image in a new window, click the **Show as Image** button.

Show as Image

The following information is available in the Metrics Dashboard:

- Endpoint Utilization, page 13-18
- Meeting Benefits, page 13-19

- Meetings by Purpose, page 13-20
- Meetings by Benefits, page 13-20
- Scheduled Meetings, page 13-20
- Ad Hoc Meetings, page 13-20
- Meetings Avoided Travel, page 13-20
- Travel Savings, page 13-20
- Emissions Savings, page 13-21
- Productivity Savings, page 13-21
- Endpoints Added, page 13-21

Note This window is only displayed if the Metrics Dashboard and Reporting API license has been uploaded in the Configure > Licenses > License Files window and Enable Meeting Organizer Usage Survey and Benefits Report is enabled in the Configure > Application Settings > Usage Survey window.

Endpoint Utilization

The Endpoint Utilization information helps you understand how TelePresence and video conferencing endpoints are used.

This information is calculated using the Meeting Benefit Report Parameters entered in the Configure > Application Settings > Usage Survey window.

Table 13-9 Endpoint Utilization Description

Endpoint Type	TelePresence / Video Conferencing
Total Number of Endpoints	Total number of TelePresence and video conferencing endpoints which are currently configured in CTS-Manager.
Average Utilization	Average percentage of TelePresence and video conferencing endpoints utilization based on the work hours per day and work days per week configured in the Configure > Application Settings > Usage Survey window.
Hours Scheduled	Total number of hours that TelePresence and video conferencing endpoints were scheduled as computed by CTS-Manager based on the number of meetings scheduled.
Number of Scheduled Meetings	Total number of scheduled TelePresence and video conferencing meetings as computed by CTS-Manager based on the number of scheduled meetings the within selected timeframe.
Number of No-Shows	Total number of scheduled meetings that never took place
Number of Survey Responses	Total number and percentage of survey responses for TelePresence meetings
Average Duration (Hours)	Average duration of TelePresence meetings in hours

Note This window is only displayed if the Metrics Dashboard and Reporting API license has been uploaded in the Configure > Licenses > License Files window and Enable Meeting Organizer Usage Survey and Benefits Report is enabled in the Configure > Application Settings > Usage Survey window.

Meeting Benefits

The Meeting Benefits information helps you understand how TelePresence meetings benefit your organization in terms of cost and productivity savings, as well as reduced environmental impact.

This information is calculated using the Meeting Benefit Report Parameters entered in the Configure > Application Settings > Usage Survey window.

Table 13-10 Meeting Benefits Description

Benefit	Value
Travel Savings	Total amount of money saved by using TelePresence instead of traveling as configured in the cost per trip and trips eliminated per meeting parameters in the Configure > Application Settings > Usage Survey window if the meeting organizer selects Avoid Travel as the response for required Benefit question in the usage survey. The meeting organizer must choose the Avoid Travel answer for the meeting to be counted as saving travel.
Productivity Savings	Total amount of money (in USD) saved through increased productivity when people avoid travel by using TelePresence based on the travel hours per trip, employee hourly cost, number of people who avoid travel per meeting and the number of meetings that avoided travel per the meeting, configured in the Configure > Application Settings > Usage Survey window. The meeting organizer must choose the Avoid Travel answer to the Benefit question for the meeting to be counted as saving travel, increasing productivity and saving emissions.
Total Savings	Total amount of money (in USD) saved by using TelePresence. This is the sum of travel savings and productivity savings.
Meetings Avoided Travel	Total number of meetings that replaced business trips, based on the number of meeting organizers who selected Avoid Travel for the Benefit question.
Emissions Saved (Metric Tons)	Total number of carbon emissions saved by using TelePresence, based on the carbon emissions per trip, the trips eliminated per meeting, as configured in the Configure > Application Settings > Usage Survey window, the number of people who avoided travel per meeting, and the number of meetings which avoided travel. The meeting organizer must choose the Avoid Travel answer to the Benefit question for the meeting to be counted as saving emissions.

Meetings by Purpose

The Meetings by Purpose information shows the percentage of survey respondents for all meetings that chose each purpose as the purpose for their meeting. This information is gathered from the meeting purpose question in the usage survey for each meeting and is displayed in a pie chart by default. In grid view, the number displayed in each row of the Value column corresponds to the number of survey respondents that provided that answer.

Meetings by Benefits

The Meetings by Benefits information shows the percentage of survey respondents for all meeting that chose each benefit as the benefit for their meeting. This information is gathered from the meeting benefit question in the usage survey for each meeting and is displayed in a pie chart by default. In grid view, the number displayed in each row of the Value column corresponds to the number of survey respondents that provided that answer.

Scheduled Meetings

The Scheduled Meetings information shows the number of daily scheduled meetings over time. The information is displayed in a line chart by default. You can view the information for the Past Week, Past Month and Past Quarter by clicking the appropriate link at the top of the chart. In grid view, the number displayed in each row of the Scheduled Meetings column corresponds to the number of scheduled meetings for that date.

Ad Hoc Meetings

The Ad Hoc Meetings information shows the number of daily ad hoc meetings over time. The information is displayed in a line chart by default. You can view the information for the Past Week, Past Month and Past Quarter by clicking the appropriate link at the top of the chart. In grid view, the number displayed in each row of the Ad Hoc Meetings column corresponds to the number of Ad Hoc meetings for that date.

Meetings Avoided Travel

The Meetings Avoided Travel information shows the number of meetings over time that replaced business trips. The information is displayed in a line chart by default. You can view the information for the Past Week, Past Month and Past Quarter by clicking the appropriate link at the top of the chart. In grid view, the number displayed in each row of the Meetings Avoided Travel column corresponds to the number of meetings that replaced business trips for that date.

Travel Savings

The Travel Savings information shows the amount of money (in USD) saved by using TelePresence instead of traveling. The information is displayed in a line chart by default. You can view the information for the Past Week, Past Month and Past Quarter by clicking the appropriate link at the top of the chart. In grid view, the number displayed in each row of the Travel Savings column corresponds to the amount of money (in USD) saved by using TelePresence instead of traveling on that date.

Emissions Savings

The Emissions Savings information shows the carbon emissions saved (in Metric Tons) by using TelePresence instead of traveling. The information is displayed in a line chart by default. You can view the information for the Past Week, Past Month and Past Quarter by clicking the appropriate link at the top of the chart. In grid view, the number displayed in each row of the Emissions Savings column corresponds to the amount of carbon emissions (in Metric Tons) saved by using TelePresence instead of traveling on that date.

Productivity Savings

The Productivity Savings information shows the amount of money (in USD) saved through increased productivity by using TelePresence. The information is displayed in a line chart by default. You can view the information for the Past Week, Past Month and Past Quarter by clicking the appropriate link at the top of the chart. In grid view, the number displayed in each row of the Productivity Savings column corresponds to the amount of money (in USD) saved in increased productivity by using TelePresence on that date.

Endpoints Added

The Endpoints Added information shows the number of endpoints added over time. The information is displayed in a line chart by default. You can view the information for the Past Week, Past Month and Past Quarter by clicking the appropriate link at the top of the chart. In grid view, the number displayed in each row of the Endpoints Added column corresponds to the number of endpoints added on that date.

TelePresence Utilization

The Monitor > TelePresence Utilization window displays information about how each TelePresence endpoint is currently used. You can export all TelePresence utilization data to a Tab-separated values (.tsv) file, by clicking **Export**.

Table 13-11 TelePresence Utilization Description

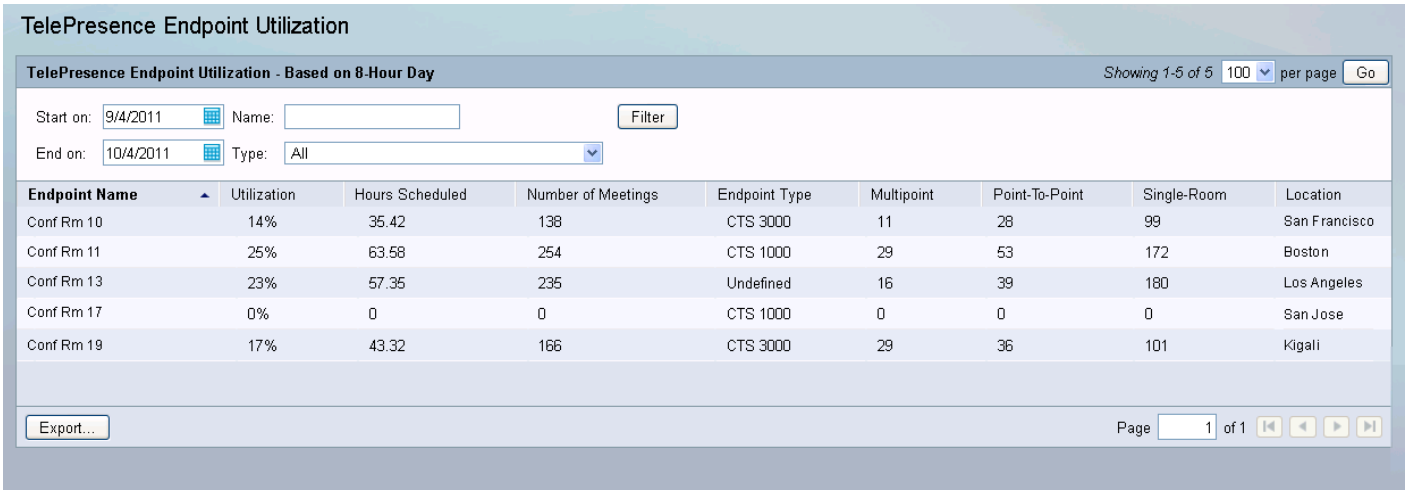
Endpoint Name	Name of TelePresence endpoint. **Note** An individual endpoint will appear twice in the following situation: The endpoint is initially discovered by CTS-Manager and is scheduled for meetings. Later, its Unified CM profile is changed and it is rediscovered by CTS-Manager.
Utilization	Percentage of the time during an 8-hour day that the TelePresence endpoint is being used.
Hours Scheduled	Number of hours TelePresence endpoint is currently scheduled
Number of Meetings	Total number of meetings using the TelePresence endpoint

Table 13-11 TelePresence Utilization Description (continued)

Endpoint Type	Type of TelePresence endpoint **Note** CTS submodel type is not displayed. Example: CTS1300-65 is displayed as CTS1300. **Note** When CTS configurations in Unified CM are changed, CTS-Manager rediscovers the devices and creates new endpoint entries. It marks any previous entries not rediscovered as deleted and removes their Telepresence equipment information. Because the TelePresence Utilization report shows historical utilization data for each endpoint, CTS Type information for old endpoints is displayed as 'Undefined'.
Multipoint	If the meeting is a multipoint meeting or not
Point-to-Point	If the meeting is an point-to-point meeting or not.
Single-Room	Description of TelePresence endpoint
Location	Location of TelePresence endpoint
Country	Country where TelePresence endpoint is located **Note** Country information is not available for meetings scheduled with Lotus Notes.

Note This window is only available if the Metrics Dashboard and Reporting API license has been uploaded in the Configure > Licenses > License Files window and Enable Meeting Organizer Usage Survey and Benefits Report is enabled in the Configure > Application Settings > Usage Survey window.

Figure 13-5 Monitor > TelePresence Utilization



Meeting Benefits

The Monitor > Meeting Benefits window displays information about the benefits for all TelePresence meetings. From this window you can modify the benchmark parameters used to generate this information, based on your company's approved benchmarks, by clicking Modify Parameters. You can also export all meeting benefits data to a Tab-separated values (.tsv) file, by clicking Export.

Table 13-12 Meeting Benefits Description

Benefit	Value
Travel Savings	Total amount of money saved by using TelePresence instead of traveling
Productivity Savings	Total amount of money (in USD) saved through increased productivity by using TelePresence.
Total Savings	Total amount of money (in USD) saved by using TelePresence.
Meetings Avoided Travel	Total number of meetings that replaced business trips
Emissions Saved (Metric Tons)	Total number of carbon emissions saved by using TelePresence

Note This window will only be displayed if the Metrics Dashboard and Reporting API license has been uploaded in the Configure > Licenses > License Files window and Enable Meeting Organizer Usage Survey and Benefits Report is enabled in the Configure > Application Settings > Usage Survey window.

Figure 13-6 Monitor > Meeting Benefits

VC Utilization

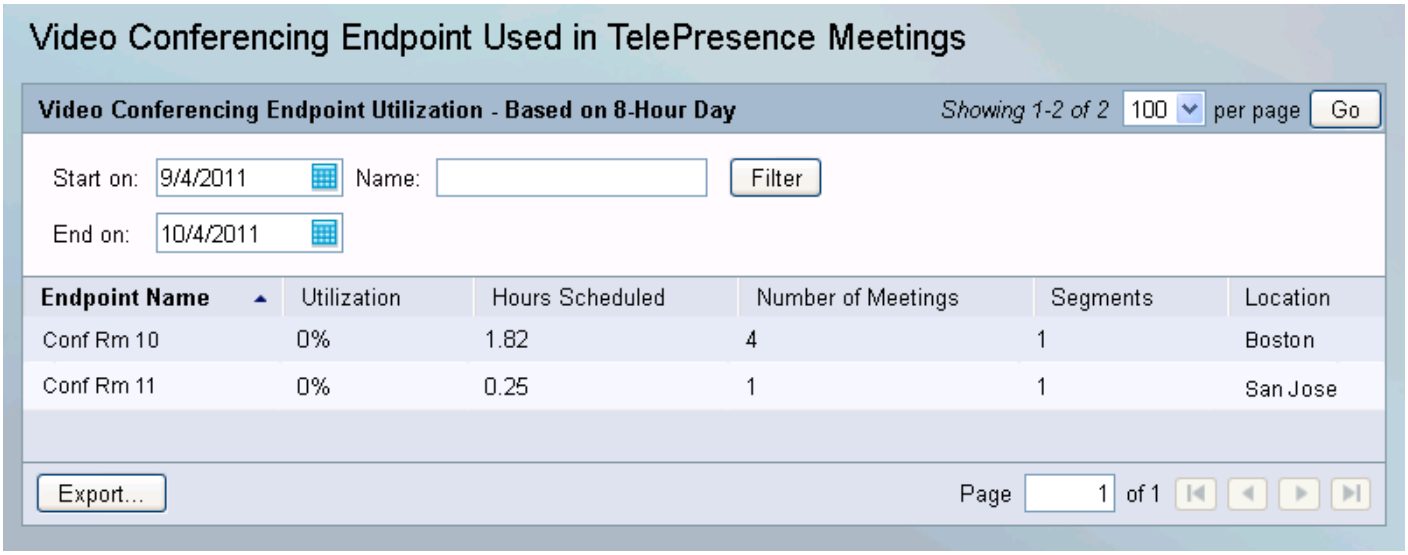
The VC Utilization window displays information about how each video conferencing endpoint is currently used. You can export all video conferencing utilization data to a Tab-separated values (.tsv) file, by clicking **Export**.

Table 13-13 VC Utilization Description

Endpoint Name	Name of video conferencing endpoint
Utilization	Percentage of the time during an 8-hour day that the video conferencing endpoint is being used
Hours Scheduled	Number of hours video conferencing endpoint is currently scheduled
Number of Meetings	Total number of meetings in the video conferencing endpoint
Segments	Number of segments of the video conferencing endpoint
Location	Location of video conferencing endpoint
Country	Country where video conferencing endpoint is located. **Note** Country information is not available for meetings scheduled with Lotus Notes.

Note This window will only be displayed if Interoperability with Video Conferencing is enabled in the Configure > Application Settings > Bridges and Servers window and there are video conferencing endpoints added to CTS-Manager in the Configure > Endpoints window.

Figure 13-7 Monitor > VC Utilization



Users

The Monitor > Users window displays information about Cisco TelePresence Manager users. It is divided into two tabs:

- Current Logins
- Meeting Organizers

Current Logins

Choose Support > Monitor > Current Logins to view information about who is currently logged into CTS-Manager, what their system role is and their IP address. You can filter this window to display information about the following users:

- All (all system roles)
- Administrator
- Meeting Organizer
- Live Desk
- SysAdmin

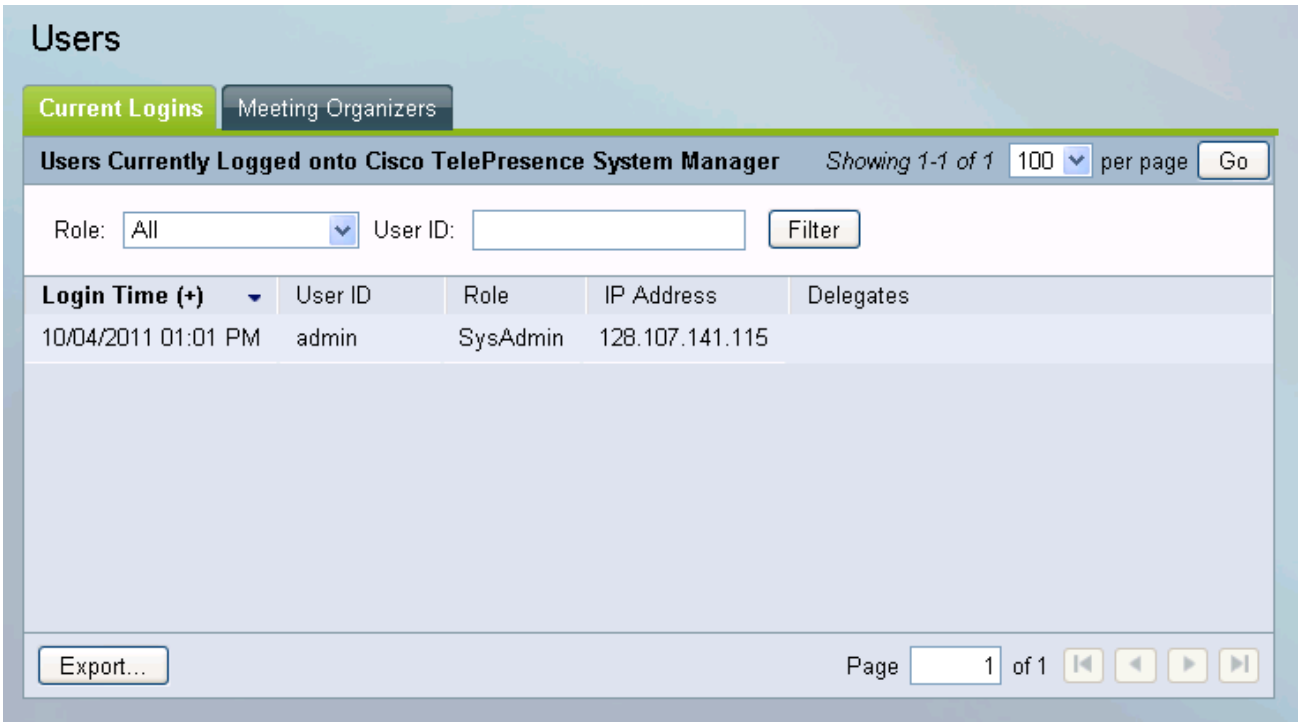
To further filter this list, you can enter a specific User ID. Once you've selected your filtering criteria, click **Filter**.

Note If a user closes their browser window without logging out of CTS-Manager first, they will remain logged in for 15 minutes until CTS-Manager detects their lack of activity and expires their session. Cisco recommends that users log out explicitly instead of closing their CTS-Manager browser window.

Table 13-14 Current Logins Description

Field	Description
Login Time(+)	Date and time user logged in.
User ID	User's CTS-Manager User ID.
Role	User's CTS-Manager role.
IP Address	IP address of where the user logged in.
Delegates	Other users to which the meeting organizer has given permission to manage their meetings.

Figure 13-8 Monitor > Users > Current Logins



Meeting Organizers

The Monitor > Users > Meeting Organizers window displays the meeting organizers of currently scheduled meetings.

This information can be exported to create lists of organizers, and additional information about them and the number of meetings that they set up.

Table 13-15 Meeting Organizers Description

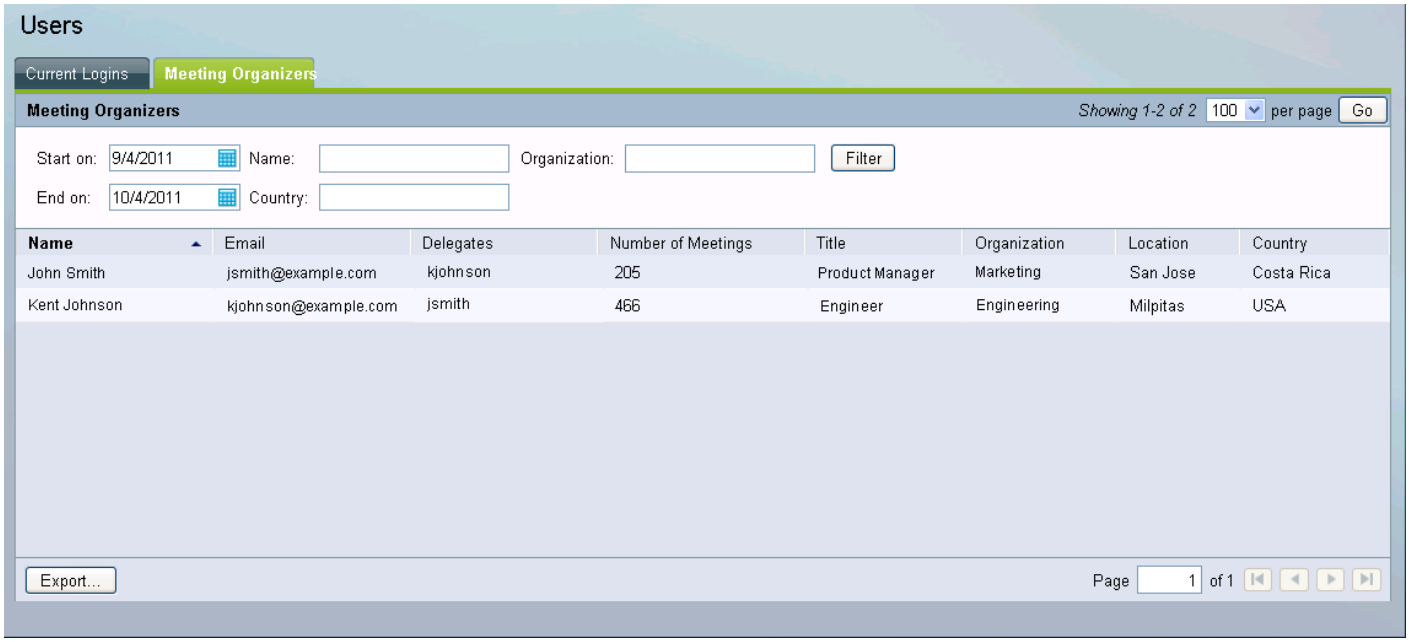
Field	Description
Name	Name of meeting organizer.
Email	Email address of meeting organizer.

Table 13-15 Meeting Organizers Description

Field	Description
Delegates	Other users to which the meeting organizer has given permission to manage their meetings.
Number of Meetings	Number of meetings that meeting organizer has scheduled.
Title	Meeting organizer's job title.
Organization	Organization of meeting organizer.
Location	Location of meeting organizer.
Country	Country of meeting organizer.

Note This window is only displayed if the Metrics Dashboard and Reporting API license has been uploaded in the Configure > Licenses > License Files window and Enable Meeting Organizer Usage Survey and Benefits Report is enabled in the Configure > Application Settings > Usage Survey window.

Figure 13-9 Monitor > Users > Meeting Organizers



Endpoints

The Support > Endpoints window displays information about endpoints. This window is divided into three, tabbed views.

- The **Summary** view displays the status of all Cisco TelePresence endpoints registered with Cisco TelePresence Manager, as well as Cisco Unified CM, Microsoft Exchange or IBM Domino. Table 13-16 on page 13-28 describes information in this window.

- The **Capability** view displays the availability of certain Cisco TelePresence features. Table 13-17 describes information in this window.

Generating Endpoint Reports

You can generate a report about specific meeting endpoints 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 An endpoint is in the Needs Help state if the Live Desk soft key on the endpoint phone/display device has been selected.

Step 2 Enter the endpoint name in the **Name** field.

Step 3 Click **Filter**.

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

Figure 13-10 Support > Endpoints > Summary

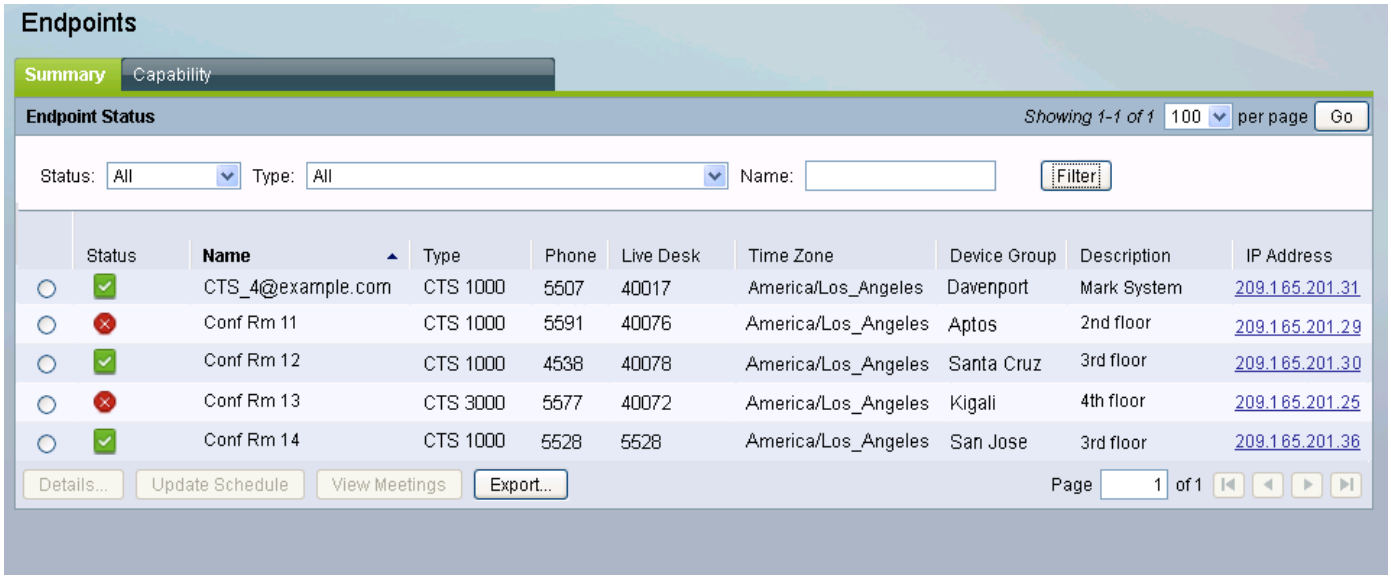


Table 13-16 Endpoints Summary

Field	Description or Setting
Status	Endpoint status: All, OK, Error, Needs Help, or In Use
Name	Name of the endpoint
Type	Type and model of endpoint

Table 13-16 Endpoints Summary (continued)

Field	Description or Setting
Phone	Endpoint phone number
Live Desk	Live Desk who is assigned to the endpoint as the help contact
Time Zone	Displays the Time Zone location of the TelePresence endpoint
Device Group	The group to which the endpoint is assigned. You can change this group in the Configure > Device Groups page.
Description	Endpoint 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 endpoint. Click the address to go to the endpoint administration login page
Unified CM	IP address of Cisco Unified CM
Assigned Server	Server managing the endpoint
Licensed	Green checkmark indicates the endpoint is licensed. Red X indicates it is not licensed
Connectivity with	
Unified CM	Status of connectivity between endpoint and Unified CM. A check indicates connectivity is supported. An “X” indicates a problem with the connection between Unified CM and the Cisco TelePresence endpoint.
CTS Manager	A check indicates connectivity is supported. An “X” indicates a problem with the connection between Cisco TelePresence Manager and the Cisco TelePresence endpoint.
Device Error	A check indicates communication is supported. An “X” indicates a problem with the Cisco TelePresence endpoint.
CUCM	
Email ID	A check indicates the Cisco TelePresence System email ID stored in Unified CM is valid. An “X” indicates a problem with the Cisco TelePresence System email ID stored in Unified CM.
Microsoft Exchange or IBM Domino	
Subscription	A check indicates a subscription between the TelePresence endpoint and Microsoft Exchange is supported. An “X” indicates a subscription problem between the TelePresence endpoint and Microsoft Exchange. A subscription error may be indicated by an “X” when there is no error.
Sync	A check indicates synchronization between the endpoint and Microsoft Exchange is supported. An “X” indicates a synchronization problem between the endpoint and Microsoft Exchange.

Manually Updating Schedules on the Cisco TelePresence Endpoint Phone or Control Device

To update an endpoint's IP phone/or control device 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 an endpoint.

Step 2 Click **Update Schedule**.

Viewing Scheduled Meetings for a Specific Endpoint

To obtain additional information about any meetings associated with an endpoint, perform the following steps:

Step 1 Click the radio button associated with an endpoint.

Step 2 Click **View Meetings**.

Figure 13-11 Support > Endpoints > Capability

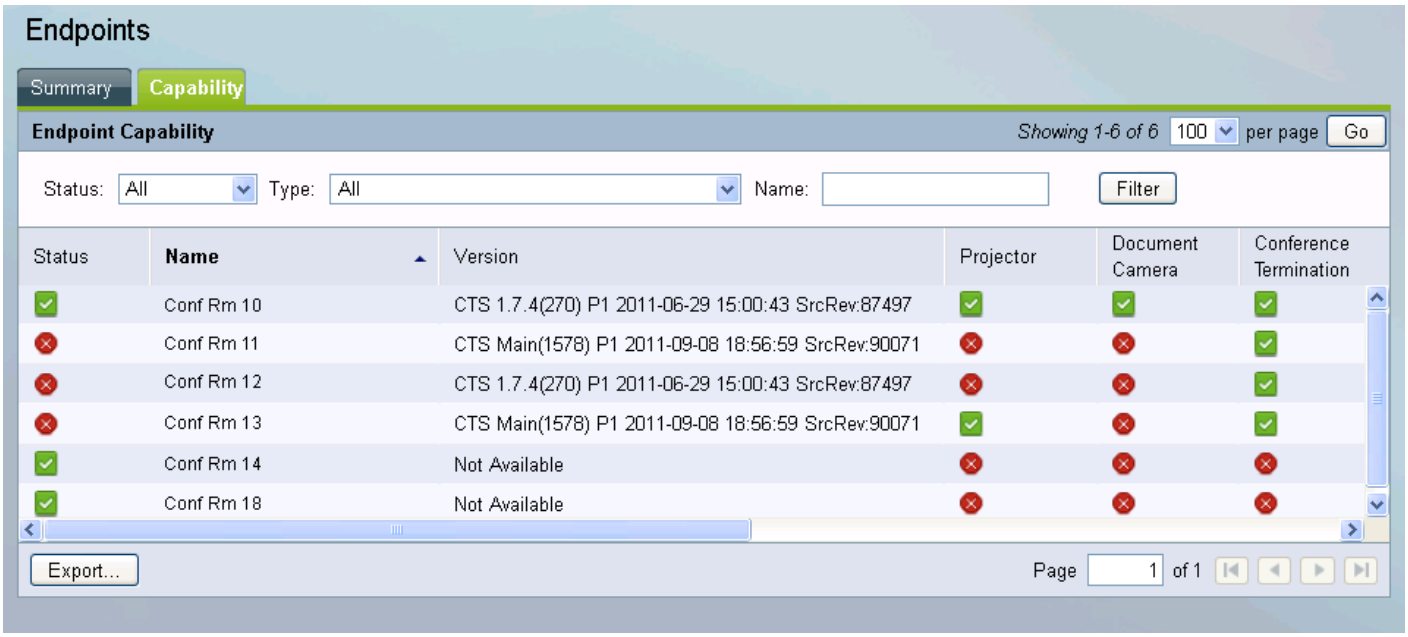


Table 13-17 Endpoints Capability Information

Field	Description or Setting
Status	Endpoint 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.
Endpoint Name	Endpoint device name.
Version	Displays the software release version for the endpoint. **Note** Versions of CTS prior to 1.5 only display "Not Available" in this field. This does not affect any functionality.
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.
Interop	A check specifies the endpoint supports SD (CIF) Interop calls.
HD Interop	A check specifies the endpoint supports HD (720p) Interop calls.
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.
Recording	A check specifies the endpoint supports recording.
Inter-Device Security	A check specifies the endpoint supports HTTPS communications.
WebEx	A check specifies the endpoint supports WebEx.
Tentative Reservation	A check specifies the endpoint supports tentative room reservations. (Microsoft Exchange only)

Tentative Room Reservation

The Tentative Room Reservation button allows you to enable tentative room reservations for individual TelePresence endpoints.

Note This option is supported only with Microsoft Exchange. Tentative Room Reservations must be enabled in the Configure > Application Settings > Meeting Options window.

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

To enable tentative room reservations for a TelePresence endpoint:

Step 1 Click **Tentative Room Reservation**.

A popup window displays each endpoint with a check box next to it.

Step 2 Check the check box next to the endpoint to select it.

Note Endpoints that are already checked currently have tentative reservations enabled.

Step 3 Click **Apply**.

A message appears, asking you to confirm your changes.

Step 4 Click **OK**.

Step 5 Click **Close**.

To disable tentative room reservations for a TelePresence endpoint, click **Tentative Room Reservation**, uncheck the endpoint you want to disable and follow steps 3 through 5 above.

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

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

Cisco recommends enabling tentative room reservations for private (office) endpoints.

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 (endpoint) (AAA) and 1 proxy room. The Proxy room accepts the meeting and the meeting is processed as a point-to-point meeting in CTS-Manager. Then the meeting is modified to a different time and the proxy room (endpoint) 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 endpoints (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 endpoints and conference room endpoints are set up with tentative enabled. if the meeting is not accepted, the proxy setting can be out-of-sync and double booking of the endpoint can occur. Thus, the best practice for public or conference endpoints is to not have this feature enabled and force a proxy confirmation acceptance.

Endpoint Subscription - Synchronization Change

As shown in the Support > Endpoints > Status window, an endpoint was successfully synchronized sometime in the past. Then the endpoint capability is changed, i.e., recording disabled. If performing a Discovery on this change, the result is the endpoint 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 endpoint which was successful in this case.

Bridges and Servers

The Support > Bridges and Servers window displays information about the bridges or servers associated with Cisco TelePresence Manager. The Bridges and Servers window is divided into two tabs:

- Summary
- Capability

Summary

The Summary tab lists the bridges or servers associated with CTS-Manager.

Generating Bridges or Servers Reports

You can generate a report about specific bridges or servers with the following steps:

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

Step 2 Enter the bridge or server hostname, IP address or Device Group in the field and select the corresponding item in the drop-down menu.

Step 3 Click **Filter**.

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

Step 5 Select a bridge or server and click **Update Schedule** to send the latest meetings schedule to the device.

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 bridge or server and click **View Meetings** to display a list of meetings assigned to that bridge or server.

Figure 13-12 Support > Bridges and Servers > Summary

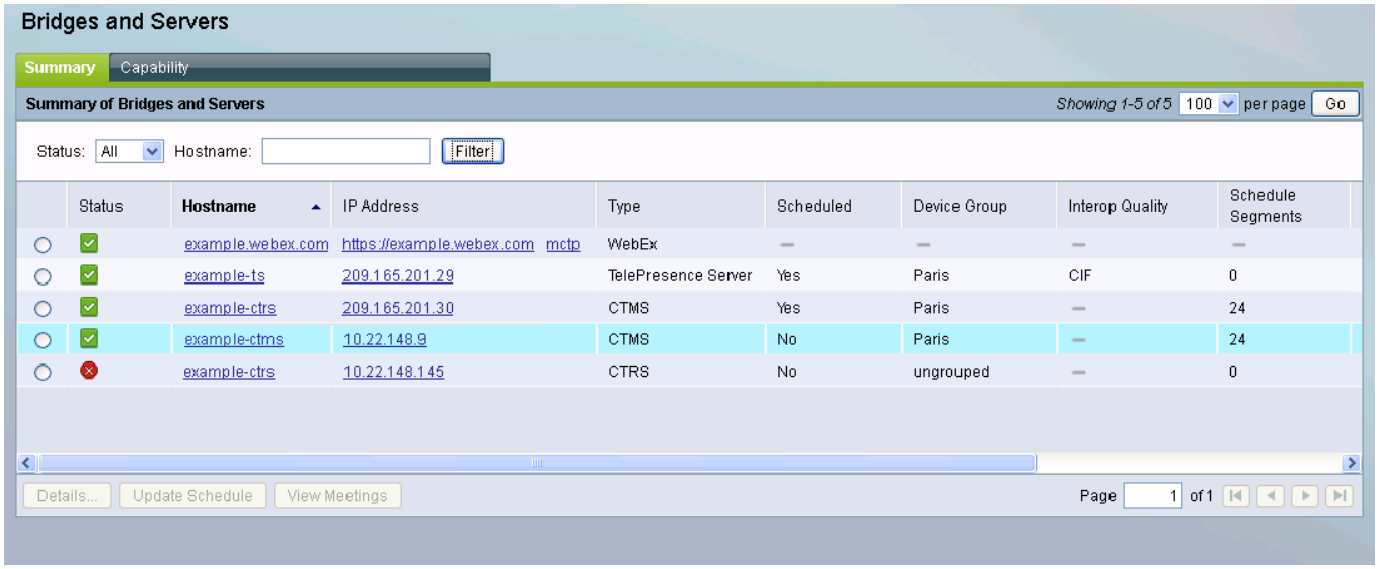


Table 13-18 Support > Bridges and Servers > Summary Tab

Field	Description or Settings
Status	Bridge or server status: All, OK, or Error. A CUVC device always shows a status of OK.
Hostname	The address of the bridge or server.
IP Address	The IP Address of the bridge or server.
Type	CTS-Manager supports the following types of bridges or servers: • Cisco TelePresence Multipoint Switch (CTMS) • Cisco Unified Video Conferencing (CUVC) • Cisco TelePresence Recording Server (CTRS) • TelePresence Server (TS) • WebEx Site • Collaboration Manager • Cisco Media Experience Engine (MXE)
Scheduled	If **Yes** is displayed, a bridge or server is available (schedulable) for meetings. **Note** Meetings scheduled using a TelePresence Server only display the status of Scheduled. To determine if the meeting is In Progress or Completed, you must access the TelePresence server.

Table 13-18 Support > Bridges and Servers > Summary Tab

Field	Description or Settings
Device Group	The group to which the CTMS is assigned. You can change this group in the Configure > Device Groups page. **Note** Only CTMS devices and endpoints can be grouped.
Interop Quality	Indicates either SD (CIF) or HD (720p or 1080p) resolution.
Schedule Segments	Indicates the number of segments that can be used for scheduling meetings.
Description	Information about the bridge or server.
Call-In Number	Call-in number for the bridge or server.

Figure 13-13 CTMS Details Window

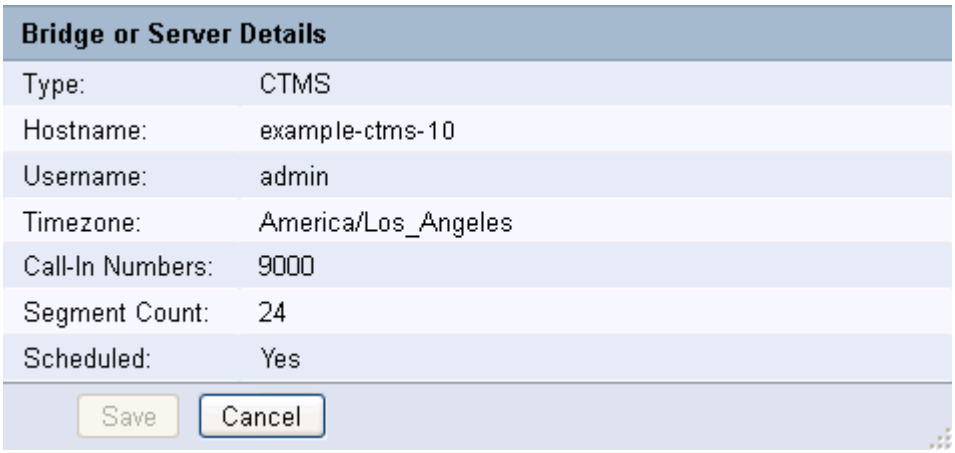


Table 13-19 CTMS Details Window Information

Field	Description or Settings
Type	The bridge or server type: CTMS.
Hostname	This is the address of the CTMS.
Username	Username used to log into the CTMS.
Timezone	Displays the time zone where the CTMS is located.
Call-In Numbers	The CTMS call-in number.
Segment Count	The number of resources available on the CTMS.
Scheduled	If **Yes** is displayed, the CTMS is available (schedulable) for meetings.

Note To migrate all meetings from a CTMS, go to **Configure > Bridges and Servers**, select the CTMS from which you want to migrate meetings, click **Edit**, select **Migrate All Meetings**, select a CTMS to migrate to and then click **Save**.

Figure 13-14 CUVC Details Window

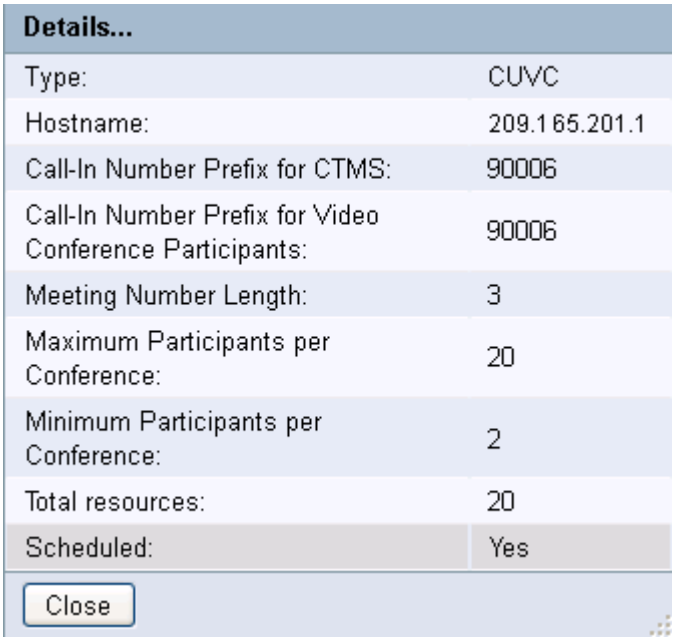


Table 13-20 CUVC Details Window Information

Field	Description or Settings
Type	The bridge or server type:CUVC **Note** Only one CUVC can be supported by a single CTS-Manager
Hostname	This is the LHS of the complete hostname.
Call-In Number Prefix for CTMS	The call-in number prefix for your CUVC is based on your enterprise dialing plan.
Call-In Number Prefix for Video Conferencing Participants	This call-in number prefix is based on your enterprise dialing plan.
Meeting Number Length	The meeting number can be 1-8 digits in length. The system-generated meeting number is used to create an Interop Call-In Number used by the CUVC to establish the conference call. It is also used to create the Interop Call-In Number sent in an email to meeting participants as the dial-in phone number. The meeting number length is based on your enterprise dialing plan.

Table 13-20 CUVC Details Window Information (continued)

Field	Description or Settings
Maximum Participants per Conference	Enter a numeric value for the maximum number of CUVC 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.
Scheduled	If **Yes** is displayed, the CUVC is available (schedulable) for meetings. If **No** is displayed Interop meetings using CUVC will not be schedulable.

Figure 13-15 CTRS Details Window for CTRS

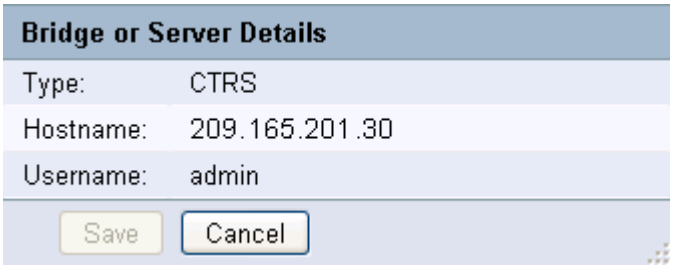


Table 13-21 CTRS Details Window Information

Field	Description or Settings
Type	The bridge or server type:CTRS
Hostname	The configured hostname of the CTRS device. This is the LHS of the complete hostname
Username	This is the account name used to log into the CTRS.

Figure 13-16 TelePresence Server Details Window

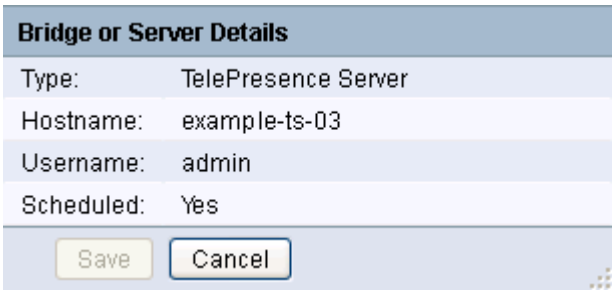


Table 13-22 TelePresence Server Details Window Information

Field	Description or Settings
Type	The bridge or server type: TelePresence Server
Hostname	Hostname of the TelePresence Server
Username	SysAdmin username of the TelePresence Server
Scheduled	If **Yes** is displayed, the TelePresence Server is available (schedulable) for meetings.

Figure 13-17 MXE Details Window

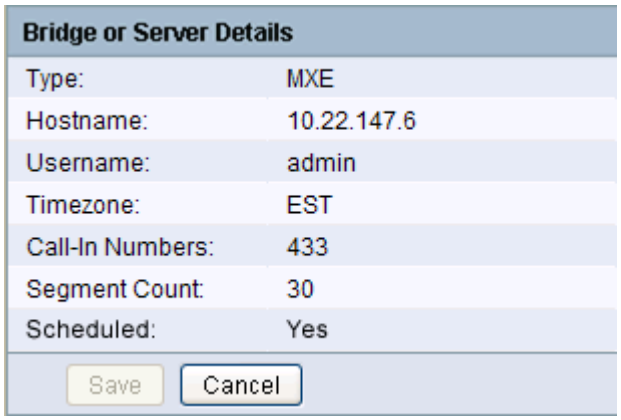


Table 13-23 MXE Details Window Information

Field	Description or Settings
Type	The bridge or server type: MXE
Hostname	The configured hostname of the MXE device.
Username	SysAdmin username of the MXE.
Timezone	Displays the time zone where the MXE is located.
Call-In Numbers	MXE call-in phone number(s).
Segment Count	Number of resources available on the MXE. Each VC endpoint requires two resources. If WebEx is included in the meeting, an additional resource is required.
Scheduled	If **Yes** is displayed, the MXE is available (schedulable) for meetings.

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

Figure 13-18 WebEx Details Window

Figure 13-19 WebEx Details Window

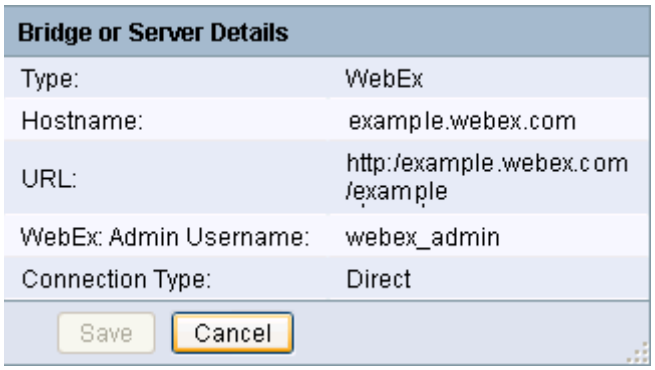


Table 13-24 WebEx Details Window Information

Field	Description or Settings
Type	The bridge or server type: WebEx **Note** If WebEx does not appear in the drop-down list, make sure WebEx is enabled in the Configure > Application Settings > Bridges and Servers window.
Hostname	A name identifying the WebEx site hostname to the administrator. This typically can be the same name as the hostname used in the site URL. **Note** Multiple WebEx sites can have the same hostname. This is not used to connect to the WebEx site and therefore is not validated during testing of connection.
URL	The address used to construct the URL that's used to access this meeting. This is the actual URL that CTS-Manager uses to communicate with WebEx. This is published in the email from CTS-Manager, and is displayed to users on the WebEx page of the CTS phone UI/display device.

Table 13-24 WebEx Details Window Information

Field	Description or Settings
WebEx Admin Username	WebEx administrator's username (provided by the WebEx team)
Connection Type	CTS-Manager connection to the WebEx site. Can be direct or via a proxy server.

Figure 13-20 Collaboration Manager Details Window

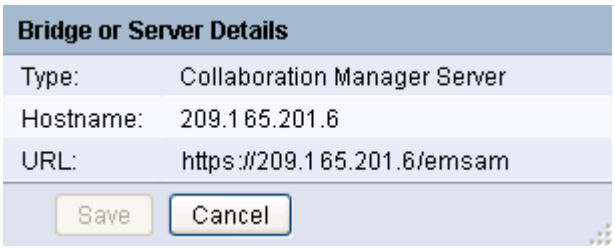


Table 13-25 Collaboration Manager Details Window

Field	Description or Settings
Type	Always Collaboration Manager
Hostname	The configured hostname of the collaboration manager server.
URL	The configured URL of the collaboration manager server.

Capability

The Capability tab identifies the Cisco TelePresence features available for each bridge or server device.

Figure 13-21 Support > Bridges and Servers > Capability

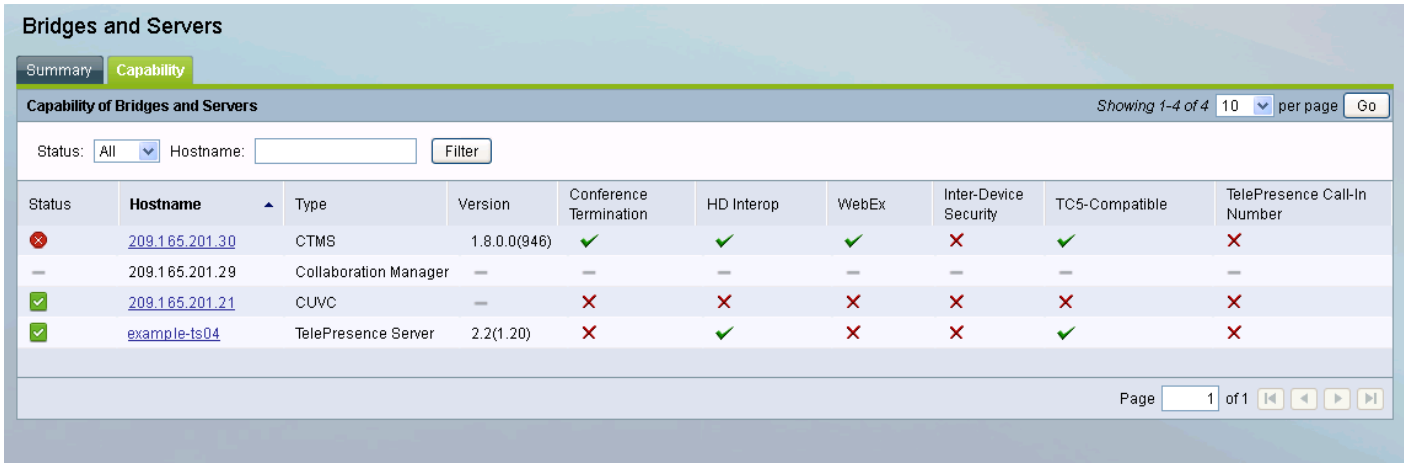


Table 13-26 Support > Bridges and Servers > Capability Information

Field	Description or Settings
Status	Bridge or Server 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 bridge or server device. Clicking the hostname hyperlink opens a new browser window, with the CTMS login page.
Type	The bridge or server type.
Version	Displays the software version running on the device. The version is not displayed for the CUVC device type.
Conference Termination	A check indicates the device supports conference termination. Refer to Policies, page 11-91 in Chapter 11, "Additional Installation Configurations for Cisco TelePresence Manager"
HD Interop	A check indicates the device supports HD (720p) video quality A check also indicates that the video quality of a scheduled meetings using this bridge or server are 720p quality. It doesn't, however, indicate the actual capability that this bridge or server can support. CUVC always shows "No" for HD Interop since CTS-Manager does not detect the true capability of CUVC. **Note** To enable HD Interop, all endpoints must be running software version 1.6 or later.
WebEx	A check indicates the device supports WebEx.
Inter-Device Security	A check indicates that connectivity between CTS-Manager and CTMS is secured via HTTPS.
TC5-Compatible	A check indicates the device supports endpoints running TC5.0 or later software.
Call-In Number	A check indicates the device supports the TelePresence Call-In Number feature.
Network Multipoint	A check indicates that the CTMS is running a software version that supports CTMS Network Multipoint. **Note** Only CTMS 1.9 or later supports Network Multipoint.

Unified CM

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

Figure 13-22 Support > Unified CM

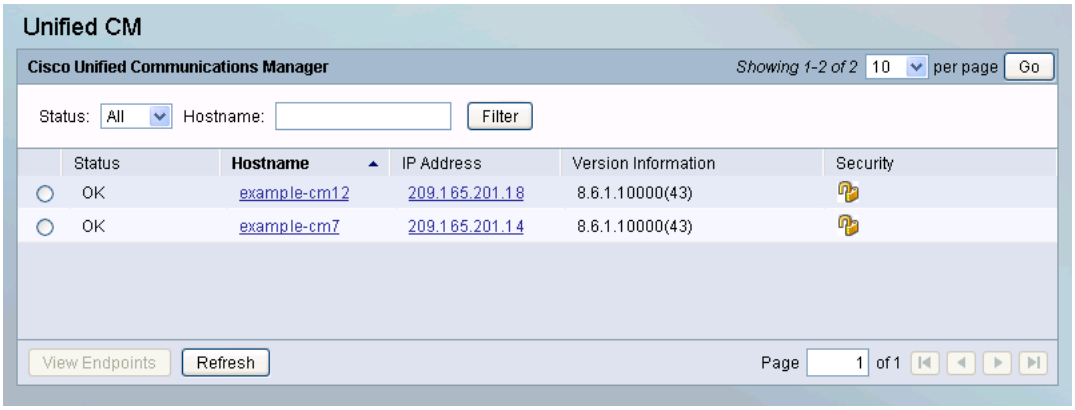


Table 13-27 describes fields and settings for the Cisco Unified CM.

Table 13-27 Unified CM Settings

Field	Description or Settings
Status	Display-only status report of system services. You may see a progress indicator in the status field, especially if many Cisco TelePresence endpoints are being managed by CTS-Manager. Each time this page is accessed, the status is updated, and the progress indicator will be seen while the system is discovering endpoints. **Caution** An error status is displayed if the connection to the Unified CM server was lost due to a network outage or if the Unified CM server was down during the CTS-Manager maintenance cycle. You can resolve the error status by going to the **Configure > Unified CM** window and clicking **Discover Rooms**.
Hostname	Name of the Cisco Unified CM server host.
IP Address	IP address of Cisco Unified CM server host.
Version Information	Version of Cisco Unified CM server host.
Security	Security setting of Cisco Unified CM server host.

Command Line Interface

Starting a CLI Session

The SysAdmin can access the CTS-Manager CLI remotely or locally:

- From a web client workstation, such as the workstation that you use for CTS-Manager administration, you can use SSH to connect securely to CTS-Manager.
- Using the monitor and keyboard that you used during installation, you can access the CTS-Manager CLI directly or by using a terminal server that is connected to the serial port. Use this method if a problem exists with the IP address.

Before You Begin

Ensure you have the following information that gets defined during installation:

- A primary IP address and hostname
- The SysAdmin ID
- The SysAdmin password

Note SysAdmin ID and password are the Administrator ID and password that are created during installation of CTS-Manager.

You will need this information to log in to the Cisco IPT Platform.

Perform the following steps to start a CLI session:

Step 1 Do one of the following actions depending on your method of access:

- From a remote system, use SSH to connect securely to the Cisco IPT Platform. In your SSH client, enter

  ssh *sysadminname@hostname*

  where ***sysadminname*** specifies the Administrator ID created during installation and ***hostname*** specifies the hostname that was defined during installation.

  For example, **ssh admin@ipt-1**.

- From a direct connection, you receive this prompt automatically:

  ```
  ipt-1 login:
  ```

  where **ipt-1** represents the host name of the system.

  Enter the SysAdmin ID.

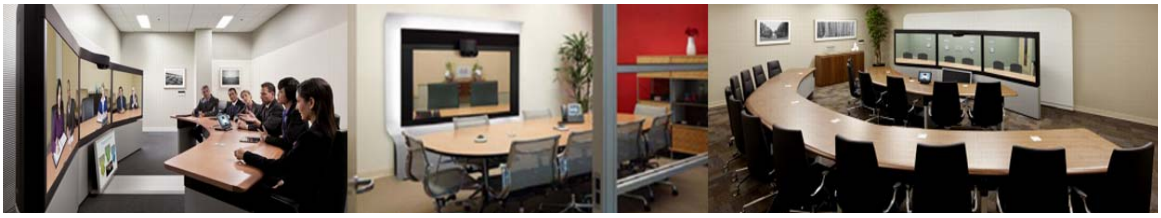
In either case, the system prompts you for a password.

Step 2 Enter your password.

The CLI prompt displays. The prompt represents the SysAdmin ID; for example: `admin:`

For all commands for the CTS-Manager, refer to the Cisco TelePresence Manager help or the CLI Book set at:

http://www.cisco.com/en/US/products/ps7074/tsd_products_support_series_home.html



CHAPTER 14

Meeting Manager and CTS-Manager Emails

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

Contents

- Point-to-Point Meeting, page 14-2
- Multipoint Meeting, page 14-4
- Video Conferencing Meeting, page 14-6
- TelePresence Call-In and WebEx Meeting, page 14-8
- Meeting Manager, page 14-14
  - Summary, page 14-15
  - Intercompany, page 14-15
  - WebEx, page 14-18
  - Usage Survey, page 14-22
  - Meeting Options, page 14-22
- System Alert Notification, page 14-24

Introduction

Cisco TelePresence meetings are scheduled between one or more endpoints. The calendar server sends an acceptance email to the meeting organizer, with the notice that the endpoints have been reserved and placed on the calendar. CTS-Manager sends either a Confirmation email or an Error email in which action is required from the meeting organizer.

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 logs into CTS-Manager using their Windows logon account (account name and password). For more information about confirmation emails refer to the various meeting sections below. For more information about the CTS-Manager Meeting Details window, refer to the Meeting Manager section.

The Action Required email specifies the error that caused the email to be generated, and a link to the Meeting Details window. For more information, refer to the Meeting Manager section.

User Authentication

In order to log in to CTS-Manager, the user needs to provide their Exchange or Domino email ID for authentication. For Exchange servers using multiple LDAP forests, the user account can reside in a remote forest. This will be associated with a disabled user account in the local forest using the Windows attribute “Associate External Account to Mailbox.” Only an associated user account can authenticate with CTS-Manager. User accounts which have read access to the mailbox but are not associated will not be able to authenticate with CTS-Manager.

Point-to-Point Meeting

The Point-to-Point meeting confirmation email is described in Table 14-1.

Figure 14-1 Point-to-Point Meeting Confirmation Email

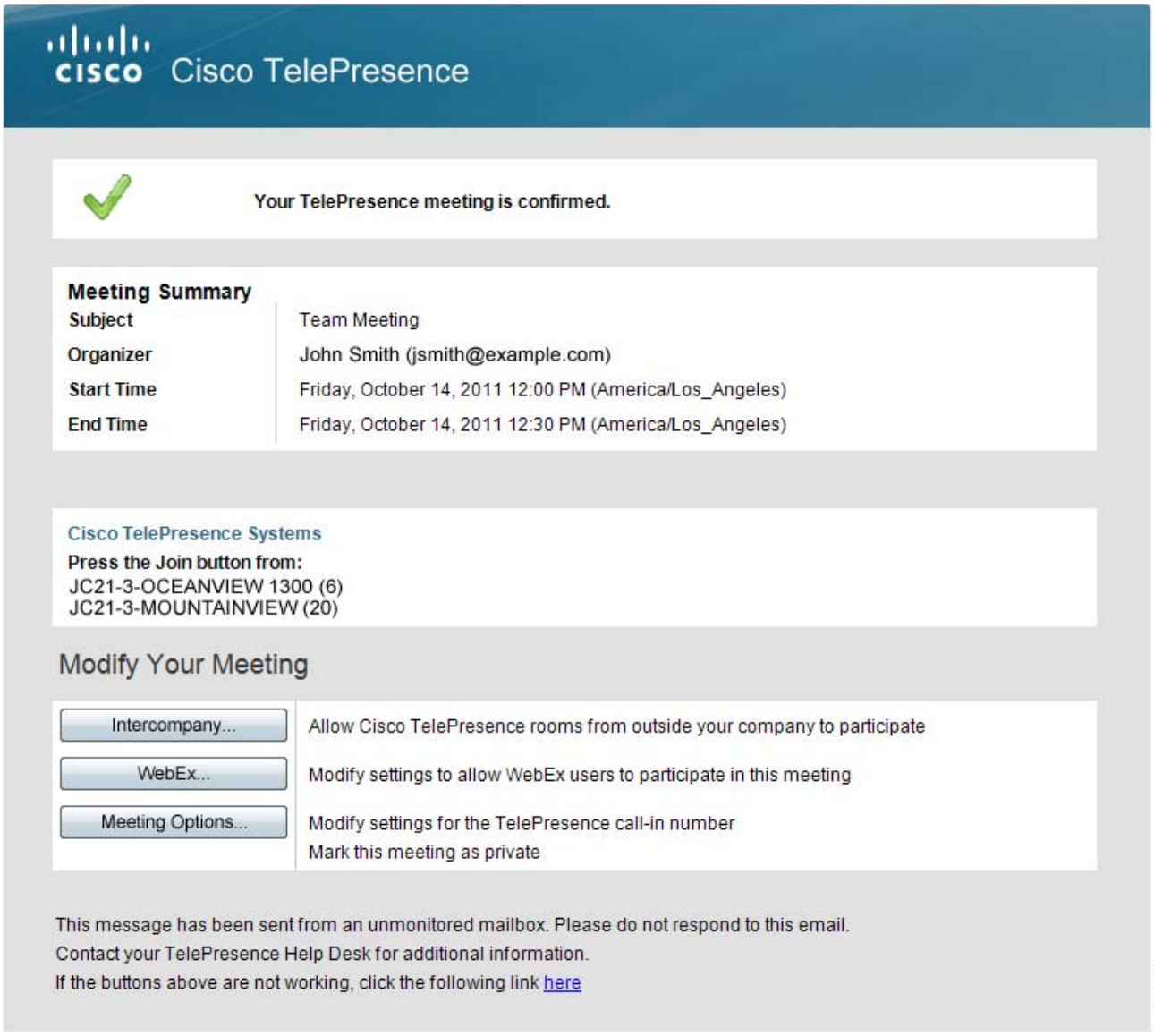


Table 14-1 Point-to-Point Meeting Confirmation Email

Email Section	Description
Confirmation Statement (below the email banner)	Your TelePresence meeting is confirmed.
Meeting Summary	This section displays information about the scheduled meeting, including subject, organizer, start time, end time and rooms (endpoints).

Table 14-1 Point-to-Point Meeting Confirmation Email

Email Section	Description
Modify Your Meeting	This section displays buttons that allow the meeting organizer to set various options that are available depending on how CTS-Manager is configured. These options include: Intercompany: clicking this button allows the organizer to go to the Intercompany window to enable Intercompany to allow TelePresence endpoints from outside your company to participate in the TelePresence meeting. Usage Survey: clicking this button allows the organizer to go to the Usage Survey window to complete the survey for this meeting. WebEx: clicking this button allows the organizer to go to the Meeting Options window to set WebEx so it can be used for this meeting. **Note** Firefox users may receive an error message when clicking the WebEx button. Click OK in the error message to continue on to the WebEx window. Meeting Options: clicking this button allows the organizer to go to the Meeting Options window to set the various options for this meeting.
Email footer	The URL displayed at the bottom of the email is the same link to the Meeting Details window which is also accessible through the buttons in the Modify Your Meeting section.

Multipoint Meeting

The Multipoint meeting confirmation email is described in Table 14-2.

Figure 14-2 Multipoint Meeting Confirmation Email

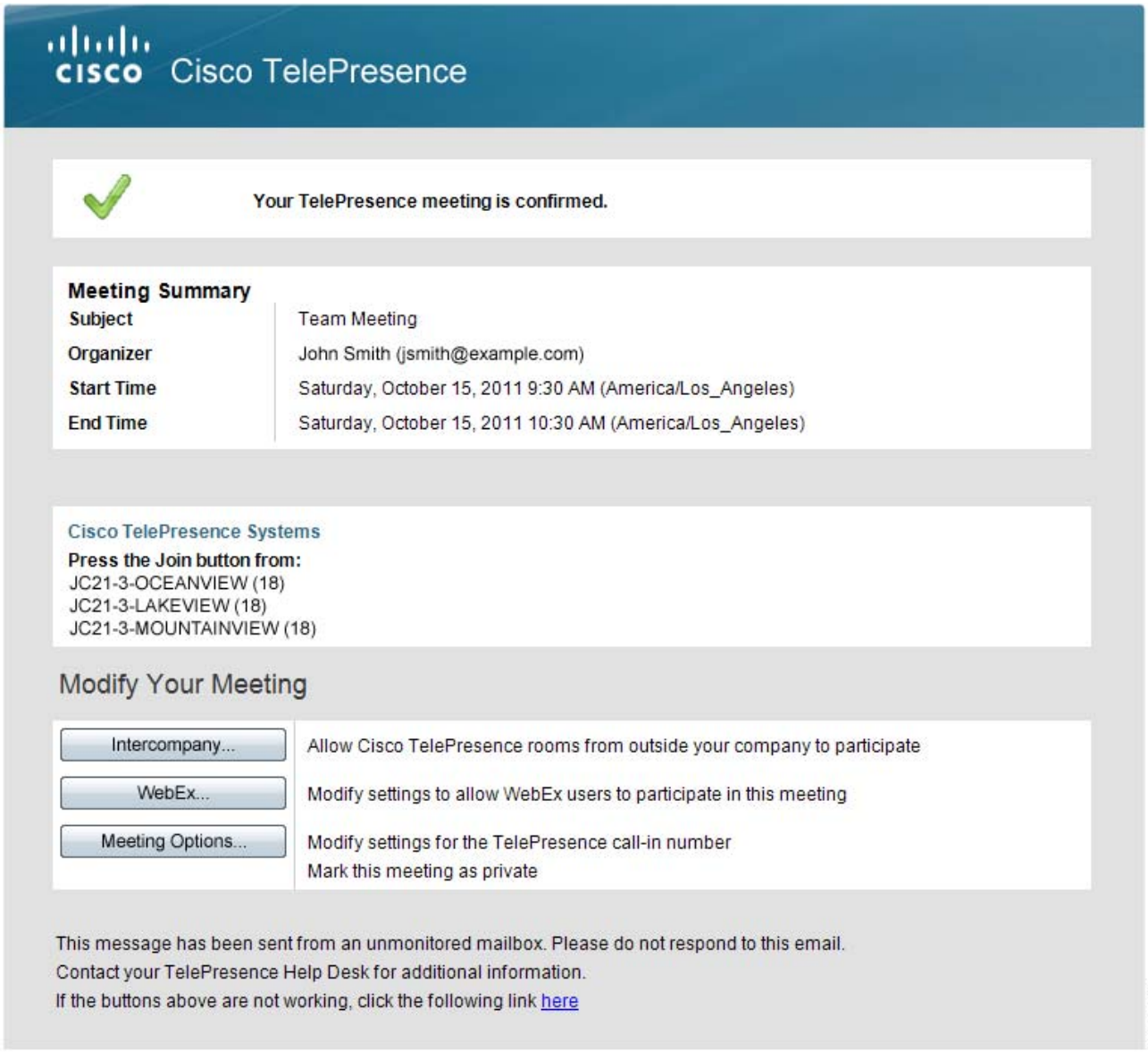


Table 14-2 Multipoint Meeting Confirmation Email

Email Section	Description
Confirmation Statement (below the email banner)	Your TelePresence meeting is confirmed.

Table 14-2 Multipoint Meeting Confirmation Email (continued)

Email Section	Description
Meeting Summary	This section displays information about the scheduled meeting, including subject, organizer, start time, end time and rooms (endpoints).
Modify Your Meeting	This section displays buttons that allow the meeting organizer to set various options that are available depending on how CTS-Manager is configured. These options include: Intercompany: clicking this button allows the organizer to go to the Intercompany window to enable Intercompany to allow TelePresence endpoints from outside your company to participate in the TelePresence meeting. Usage Survey: clicking this button allows the organizer to go to the Usage Survey window to complete the survey for this meeting. WebEx: clicking this button allows the organizer to go to the Meeting Options window to set WebEx so it can be used for this meeting. **Note** Firefox users may receive an error message when clicking the WebEx button. Click OK in the error message to continue on to the WebEx window. Meeting Options: clicking this button allows the organizer to go to the Meeting Options window to set the various options for this meeting.

Video Conferencing Meeting

The Video Conferencing meeting confirmation email is described in Table 14-3.

Figure 14-3 Video Conferencing Meeting Confirmation Email

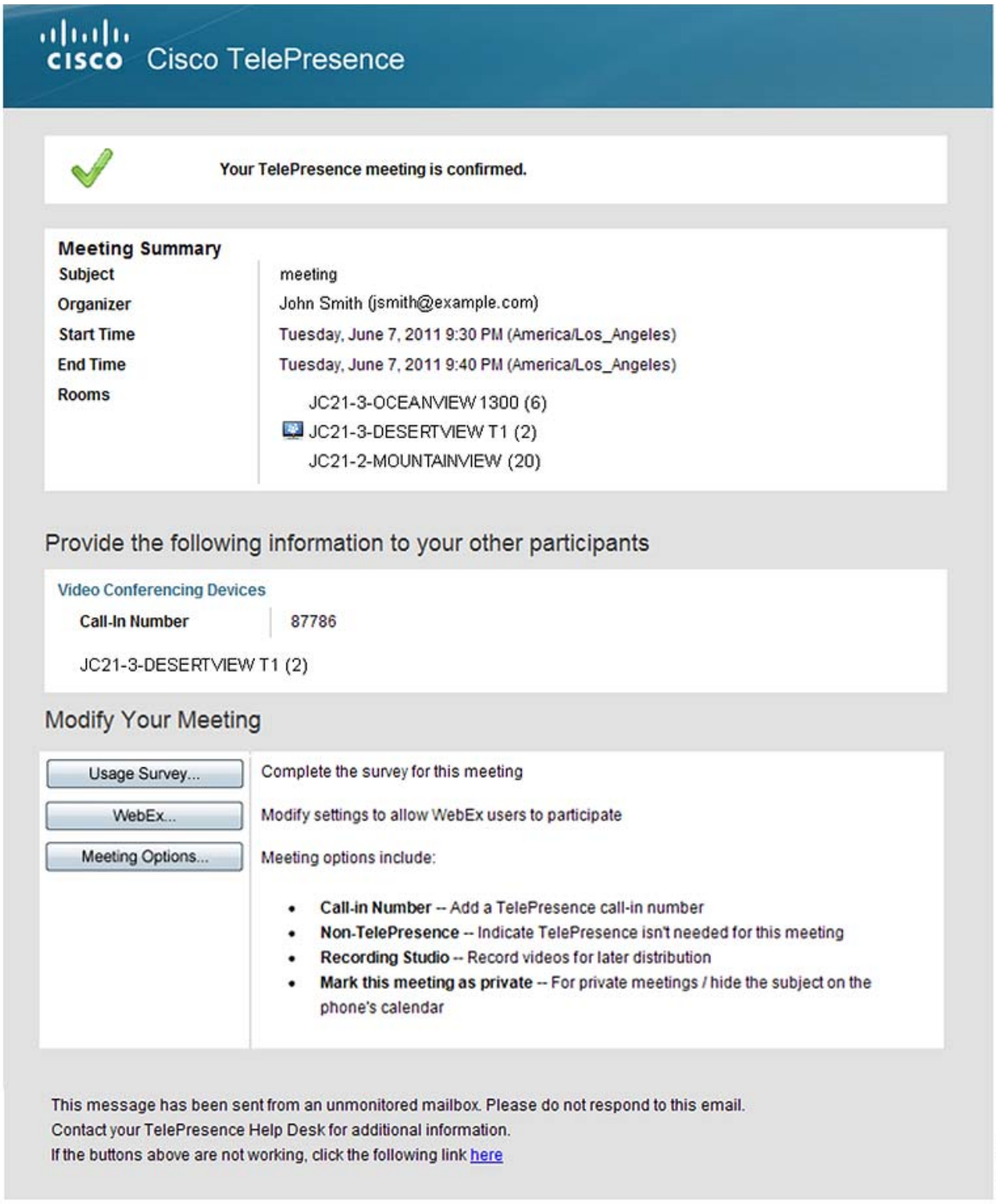


Table 14-3 Video Conferencing Meeting Confirmation Email

Email Section	Description
Confirmation Statement (below the email banner)	Your TelePresence meeting has been confirmed.
Meeting Summary	This section displays information about the scheduled meeting, including subject, organizer, start time, end time and rooms (endpoints).
Provide the following information to your other participants	This section displays the call-in phone number that the meeting organizer should send to the participants attending via a video conferencing endpoint.
Modify Your Meeting	This section displays buttons that allow the meeting organizer to set various options that are available depending on how CTS-Manager is configured. These options include: Usage Survey: clicking this button allows the organizer to go to the Usage Survey window to complete the survey for this meeting. WebEx: clicking this button allows the organizer to go to the Meeting Options window to set WebEx so it can be used for this meeting. **Note** Firefox users may receive an error message when clicking the WebEx button. Click OK in the error message to continue on to the WebEx window. Meeting Options: clicking this button allows the organizer to go to the Meeting Options window to set the various options for this meeting.

TelePresence Call-In and WebEx Meeting

A TelePresence Call-In Number and WebEx meeting confirmation email is described in Table 14-3.

Figure 14-4 TelePresence Call-In and WebEx Meeting Confirmation Email

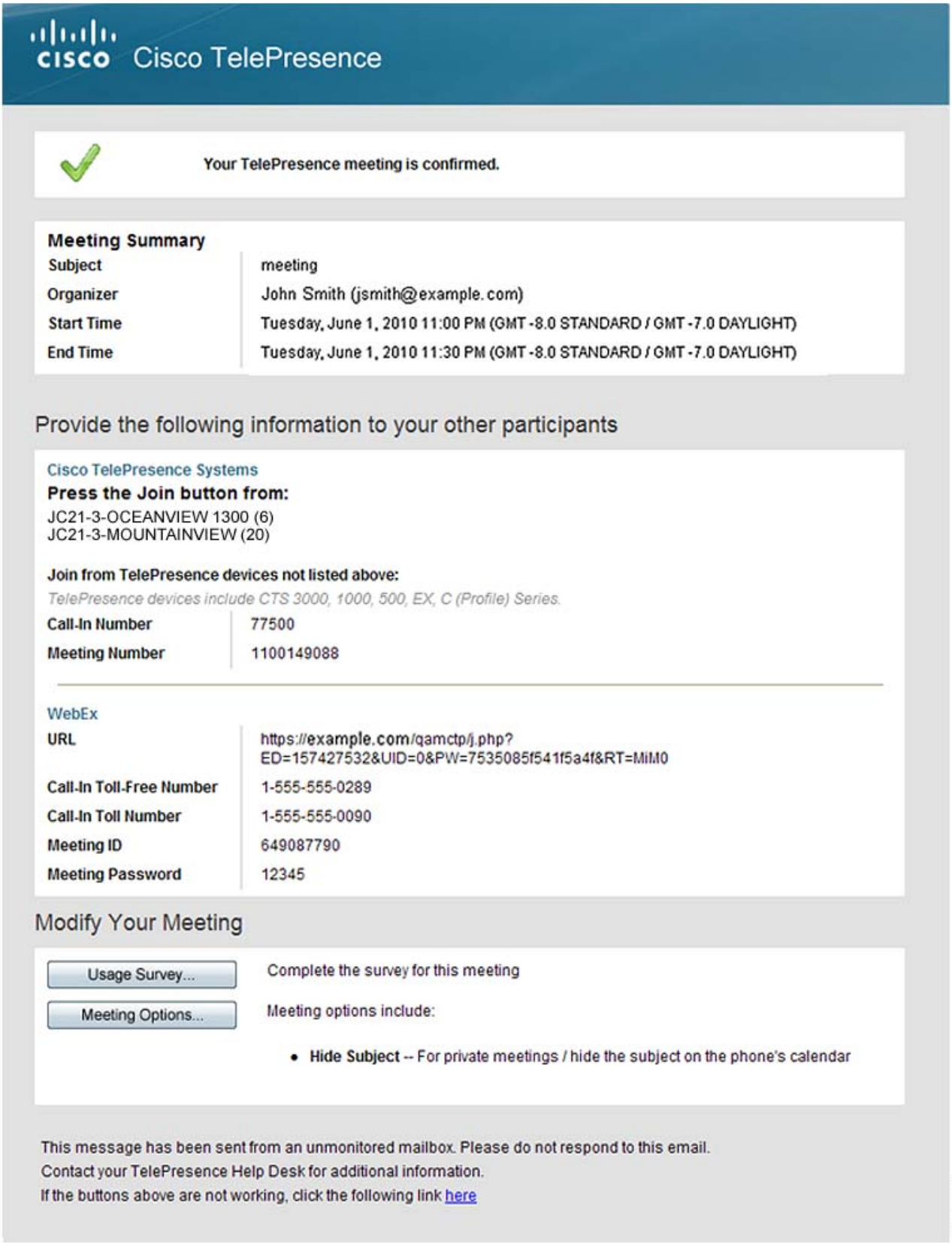


Table 14-4 TelePresence Call-In and WebEx Meeting Confirmation Email

Email Section	Description
Confirmation Statement (below the email banner)	Your TelePresence meeting has been confirmed.
Meeting Summary	This section displays information about the scheduled meeting, including subject, organizer, start time, end time and (rooms) endpoints.
Provide the following information to your other participants	This section displays the information that the meeting organizer should send to the participants attending via: • a video conferencing endpoint • a TelePresence endpoint that was not originally included in the meeting invitation • WebEx
Modify Your Meeting	This section displays buttons that allow the meeting organizer to set various options that are available depending on how CTS-Manager is configured. These options include: Usage Survey: clicking this button allows the organizer to go to the Usage Survey window to complete the survey for this meeting. Meeting Options: clicking this button allows the organizer to go to the Meeting Options window to set the various options for this meeting.

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 14-5.

- **501205 - Missing Required Endpoints**: A second Cisco TelePresence endpoint, 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 Figure 14-5. 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 an endpoint not being deleted properly from a calendar server, for example Microsoft Exchange. This can occur if the Meeting Organizer schedules a meeting that includes an endpoint in delegate mode. If the Meeting Organizer schedules the meeting and then deletes it before the endpoint delegate accepts the invitation, this Action Required email is sent to the Meeting Organizer.

- **501211 - Room (Endpoint) Not Compatible**: One or more Cisco TelePresence rooms (endpoints) are running software that is incompatible with the Cisco TelePresence Multipoint Switch.
- **501212 - Resource Not Available**: Not enough Multipoint Switch resources are available to support the multipoint meeting.
- **501213 - MCU Not Configured**: A Multipoint Switch has not been configured for the network.
- **501217 - CUVC Resource Not Available**: Insufficient Video Conferencing resources to setup multipoint meeting.

- **29105 - Inactive WebEx Account**: Inactive WebEx user account. Whether the account is reactivated or a new one is created, the meeting organizer must reauthenticate with WebEx.

Figure 14-5 Action Required Email

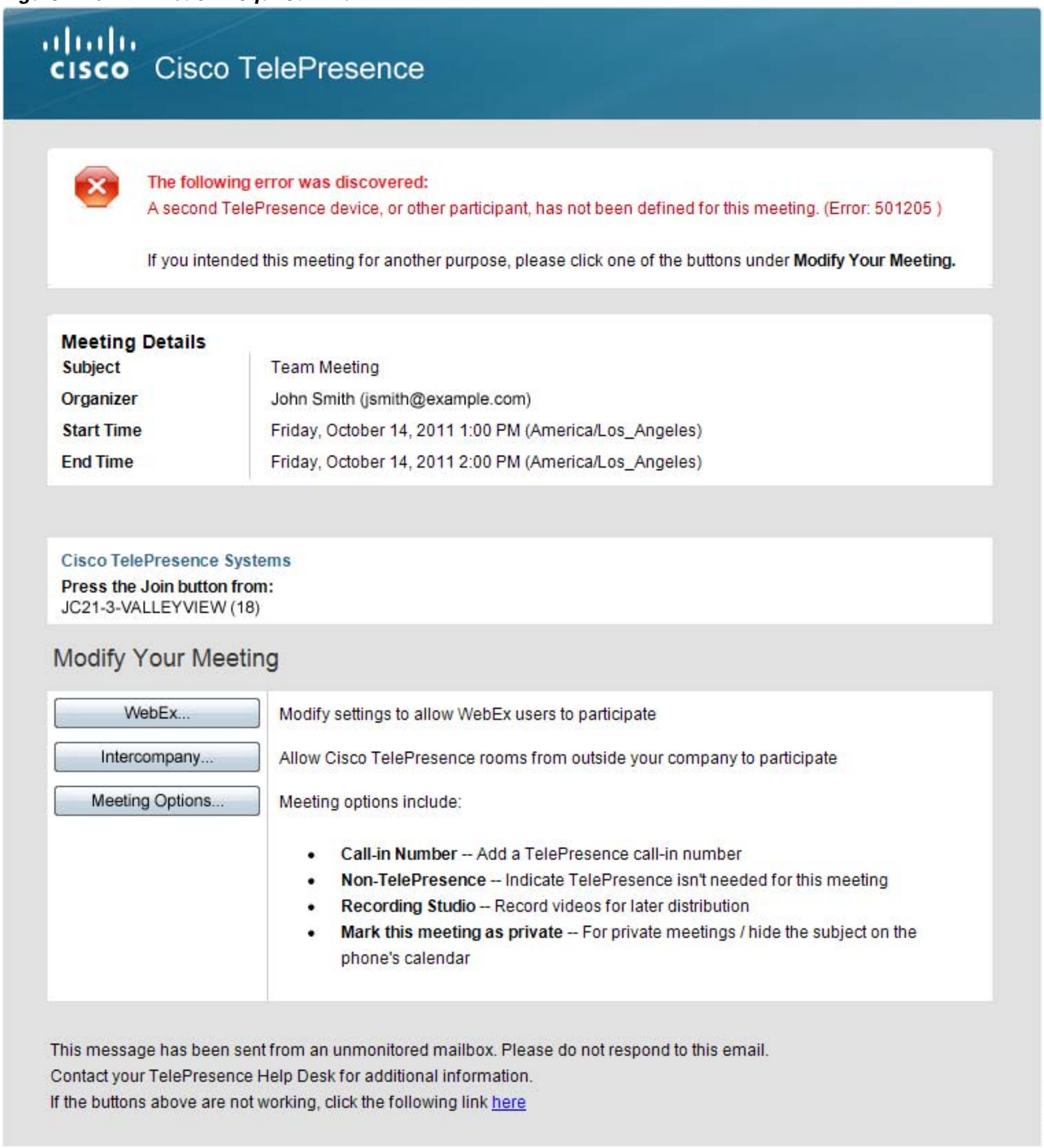


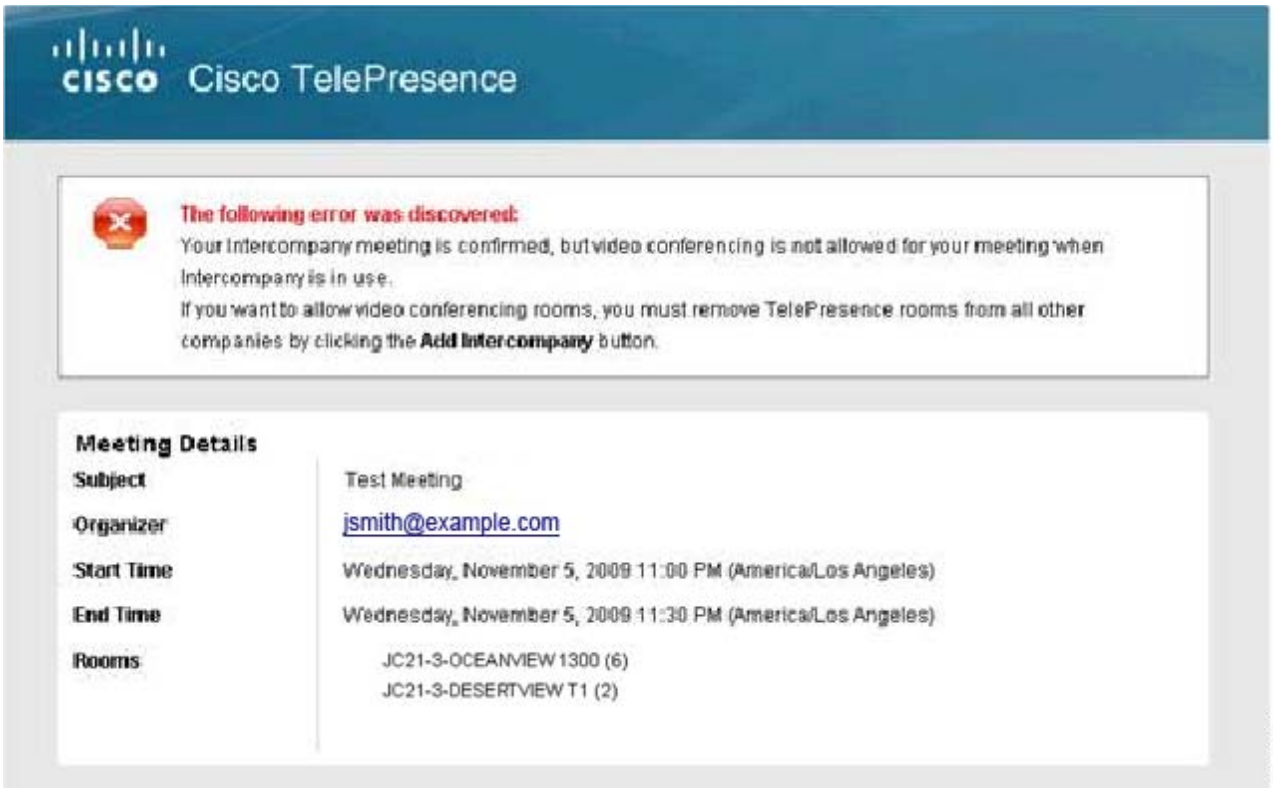
Table 14-5 Action Required Email

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.
Meeting Details	This section displays information about the scheduled meeting, including subject, organizer, start time, end time and endpoints.
Modify Your Meeting	This section displays buttons that allow the meeting organizer to set various options that are available depending on how CTS-Manager is configured. These options include: Intercompany: clicking this button allows the organizer to go to the Intercompany window to enable Intercompany to allow TelePresence endpoints from outside your company to participate in the TelePresence meeting. Usage Survey: clicking this button allows the organizer to go to the Usage Survey window to complete the survey for this meeting. WebEx: clicking this button allows the organizer to go to the Meeting Options window to set WebEx so it can be used for this meeting. **Note** Firefox users may receive an error message when clicking the WebEx button. Click OK in the error message to continue on to the WebEx window. Meeting Options: clicking this button allows the organizer to go to the Meeting Options window to set the various options for this meeting.
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 any occurrence with an icon showing a red X to resolve the error.
Email footer	The link displayed at the bottom of the email is the same link to the Meeting Manager window as the link in the Confirmation Statement above.

Video Conferencing Error Email

The error email is sent to the meeting organizer when the endpoint is not reserved for a meeting. Follow the instructions in the email header to schedule endpoints for a meeting.

Figure 14-6 Video Conference Meeting Error Email



System Alert Notification Emails

In addition to the emails sent to the meeting organizer, system alert emails are sent to the SysAdmin each day after the maintenance cycle providing information about:

- No-Show Meetings and Meetings without Survey Responses
- Mailbox Alert
- Certificate expiry

For more information about these emails, see System Alert Notifications.

Meeting Manager

The meeting manager window provides detailed information about a specific meeting and allows the meeting organizer to make changes to the meeting's settings. The meeting organizer accesses the Meeting Manager by clicking on of the e "Modify Your Meeting" buttons in the confirmation email for their meeting and then logs in to the Meeting Manager.

It is divided into the following tabbed sections:

- Summary
- Intercompany
- WebEx
- Usage Survey

- Meeting Options

Note After changing the settings in any of the tabbed sections of the Meeting Manager window, you must click **Apply** to save your changes.

In addition, the meeting organizer can specify other users to manage their meetings. For more information, refer to the Allowing Other Users to Manage Your Meetings section.

Summary

The Summary tab provides you the following fields:

Table 14-6 Meeting Details Summary 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.
Time	Displays the date, time and duration of the meeting.
Endpoints	Lists the endpoints that are participating in the meeting.
WebEx	Displays the WebEx information (if used) for the meeting.
Intercompany	Displays a green checkmark if WebEx is used in the meeting.
Video Conferencing Interop	Displays the video conferencing interoperability information for the meeting.
Record Meeting	Displays the video recording information for the meeting.
Hide Meeting Subject	Displays whether the meeting subject will be displayed on the TelePresence phone or not.
Not a TelePresence Meeting	Indicates if the meeting is not a TelePresence meeting.

Note If you have included only one Cisco TelePresence endpoint in a scheduled meeting, you enter a phone number to dial, by clicking the Meeting Options tab and entering the number in the Number to Dial field, If you mistakenly included only one Cisco TelePresence endpoint, use your calendar software (Microsoft Outlook or Lotus Notes) to add additional endpoints.

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

Intercompany

The Intercompany window allows you to enable the ability to schedule TelePresence meetings with other companies.

To enable this feature, click **Yes** and then click **Apply**.

Table 14-7 Meeting Details Intercompany Window

Field or Section Name	Description
Does this meeting include TelePresence endpoints from another company?	Select Yes to enable Intercompany TelePresence for the meeting. Additional fields appear when Intercompany is enabled.
Which company will host the TelePresence multipoint bridge?	Select Our Company if your company will be hosting. Select Another Company if another company will be hosting. Selecting this option will reveal additional fields.
Enter information provided by the meeting host (when Another Company is hosting)	
Multipoint Call-In Number	This is the phone number your Cisco TelePresence endpoint phone will call to join the meeting. This number is provided by the meeting Host's CTMS or your Service Provider's CTMS.
Meeting Number	This number is generated by the Host's CTMS or your Service Provider's CTMS
The host needs to know that your endpoints require Telepresence Resources	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

If you want to remove what has been configured before you save it and set new values, click **Cancel**.

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

Recurring Intercompany Meetings

If you make changes to a recurring intercompany meeting, those chnages are applied to all future instances of the meeting. It is not possible to change a single instance only.

Intercompany Host Meeting Options

If your company is considered the Intercompany Cisco TelePresence meeting host you need to configure your side of the meeting as the host. You'll need to obtain the Call-in Number and the Meeting Number from your CTS-Manager Administrator.

Enter the information and click **Apply** to set the values.

Table 14-8 Intercompany Host Meeting Options

Field Name	Description
Does this meeting include TelePresence rooms from another company?	Select Yes to allow TelePresence endpoints from another company to participate in this meeting. If you select Yes, three additional configuration options appear.
Enter information provided by the meeting host	
Which company will host the multipoint bridge?	Select the company that will host the TelePresence multipoint bridge.
Multipoint Call-in Number	The multipoint call-in number for the meeting.
Intercompany Meeting Number	The intercompany meeting number for the meeting.
Apply	Saves all settings.
Cancel	This removes what has been configured and reverts back to the last saved settings.

Intercompany Participant Meeting Options

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 to obtain the Call-In Number and the Meeting Number from your CTS-Manager Administrator or from the Host meeting organizer

Enter the information and click **Apply** to set the values.

Table 14-9 Intercompany Participant Meeting Options

Field Name	Description
Multipoint Call-In Number	This is the phone number your Cisco TelePresence endpoint phone will call to join the meeting. This number is provided by the meeting Host's CTMS or your Service Provider's CTMS.
Intercompany Meeting	The Meeting Number 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 TelePresence endpoints 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

WebEx

The WebEx window allows the meeting organizer to enable WebEx for their meeting and provides them with the WebEx information for both the host and par tic pants to join the meeting. The first time they schedule a TelePresence meeting with WebEx, they must register their WebEx ID user account with CTS-Manager. For more information, see First-time WebEx Setup.

Note This window is not available if the meeting organizer is not permitted to use WebEx.

Allow WebEx users to participate in this meeting

Selecting **Yes** and clicking **Apply** enables WebEx for the meeting. Selecting **No** and clicking **Apply** disables WebEx for the meeting.

WebEx Call-In Information

This section displays the WebEx information necessary for both the host and participants to join the meeting.

Table 14-10 Meeting Manager > WebEx Window

Field or Section Name	Description
Call-in Toll Free Number	Toll-free number for WebEx participants.
Call-In Toll Number	Toll number for WebEx participants.
WebEx Meeting Host Key	Code for host to regain control of the meeting from an attendee.
WebEx Meeting ID	The unique ID number generated by WebEx to identify the scheduled meeting.
Meeting Password	Password for WebEx participants.
URL	URL for WebEx meeting.

First-time WebEx Setup

If this is your first time setting up WebEx for a TelePresence meeting, you must register your WebEx ID user account with CTS-Manager. This makes using WebEx with future TelePresence meetings as easy as possible.

Note If you use the WebEx Productivity Tool plug-in for Microsoft Outlook to schedule your meeting, you do not need to go through this first-time setup.

To set up WebEx:

Step 1 If there is more than one WebEx site available, select the WebEx site to which you have been assigned.

Note If you are not sure which site to select, contact your help desk for assistance.

Step 2 Click **Register**.

The WebEx login window appears.

Note If a Security warning message appears: In Internet Explorer 6, click **Yes**. In Internet Explorer 8, click **No**

Step 3 Enter your WebEx Username and Password and click **Log In**.

Once you log in, you are redirected back to the Meeting Manager window for your meeting.

Note If a security warning message appears, click **No**.

Step 4 Click the WebEx tab, select the **YES** radio button, then click **Apply**.

WebEx is enabled and the following WebEx details appear:

- Call-in Toll-Free Number
- Call-in Toll Number
- WebEx Meeting Host Key
- WebEx Meeting ID
- Meeting Password
- URL

After a few minutes, you will receive an updated confirmation email with the WebEx information listed in the "Provide the following information to your other participants" section.

Step 5 Copy the WebEx information from the confirmation email.

Step 6 In your email program, create a new email addressed to your WebEx participants.

Step 7 Paste the WebEx information into the email and send it.

WebEx participants join the meeting by clicking the URL you sent in the email or copying and pasting it into their browser.

TelePresence participants join the meeting by pressing the button on their TelePresence phone.

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

Note The process of authenticating with WebEx maps your enterprise user account to your WebEx account. If your WebEx account changes after you log into WebEx the first time, you will use the Re-authenticate button to log into WebEx the next time with your new username and password and, after successful login, the mapping will be updated to your new WebEx account. Any WebEx account created for your company can be used to authenticate with WebEx, as long as the you know the correct username and password. If your WebEx account is reactivated, or a new one is created, you must reauthenticate with WebEx to be able to schedule WebEx-enabled TelePresence meetings.

Changing Your WebEx Site or Username

If you want to change your WebEx site or username, do the following:

Step 1 Contact your WebEx administrator to get your new WebEx site and username/password information.

Step 2 Open the confirmation email for an upcoming Cisco TelePresence meeting you scheduled. If you have no upcoming meetings, schedule one now.

Step 3 Click the **WebEx** button in the email.

Step 4 Log in to Cisco TelePresence Manager using your enterprise user ID and password.

The Meeting Manager window appears with the WebEx tab selected.

Step 5 Next to "To change your WebEx Site or username" click the **here** link.

Note If there is only one site available, you can only change your WebEx username

Step 6 If changing your WebEx site, select the new WebEx site.

Step 7 Click **Update WebEx Credential**.

The WebEx login window appears.

Note If a Security warning message appears: In Internet Explorer 6, click **Yes**. In Internet Explorer 8, click **No**

Step 8 Enter your WebEx username and password for the new WebEx site, provided by your WebEx administrator.

Step 9 Click **Log In**.

Once you log in, you are redirected back to the Meeting Manager window for your meeting.

Note One or more WebEx sites may be available, but you can only use one for scheduling WebEx-enabled TelePresence meetings. If you are not sure which one to use, contact your help desk.

Reactivating Your WebEx Account

If your WebEx account is inactive, you will not be able to schedule WebEx-enabled TelePresence meetings.

To reactivate your account:

Step 1 Contact your WebEx administrator to have your account reactivated.

Step 2 Open the confirmation email for an upcoming Cisco TelePresence meeting you scheduled. If you have no upcoming meetings, schedule one now.

Step 3 Click the WebEx button in the email.

Step 4 Log in to Cisco TelePresence Manager using your enterprise user ID and password.

Step 5 Select the WebEx site on which you have your account.

Step 6 Click the **Registe**r button and log in to WebEx using your reactivated account username and password.

After successful login, you are redirected to Cisco TelePresence Manager where you can enable WebEx for your TelePresence meeting.

WebEx Roles

The CTS-Manager administrator is responsible for assigning WebEx roles to users. Until the administrator assigns a role to a meeting organizer, their role is determined by the WebEx default user type configured in the Configure > Application Settings > Bridges and Servers window.

There are three types of WebEx users:

- WebEx Permitted User
- WebEx Premium User
- WebEx Non-Permitted User

WebEx Permitted User

If you are a WebEx Permitted user, you can request WebEx on a meeting-by-meeting basis.

Using Microsoft Outlook, you can use the WebEx Productivity Tools plug-in to add WebEx to your meeting.

Alternatively, you can enable WebEx for your meeting by doing the following:

Step 1 Click the WebEx tab, select the **YES** radio button, then click **Apply**.

WebEx is enabled and the following WebEx details appear:

- Call-in Toll-Free Number
- Call-in Toll Number
- WebEx Meeting Host Key
- WebEx Meeting ID
- Meeting Password
- URL

After a few minutes, you will receive an updated confirmation email with the WebEx information listed in the “Provide the following information to your other participants” section.

Step 2 Copy the WebEx information from the confirmation email.

Step 3 In your email program, create a new email addressed to your WebEx participants.

Step 4 Paste the WebEx information into the email and send it.

WebEx participants join the meeting by clicking the URL you sent in the email or copying and pasting it into their browser.

TelePresence participants join the meeting by pressing the button on their TelePresence phone.

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

WebEx Premium User

If the meeting organizer is a WebEx Premium user, every meeting they schedule includes WebEx.

All they have to do is provide the WebEx information to their meeting participants:

Step 1 Copy the WebEx information from the confirmation email.

Step 2 In your email program, create a new email addressed to your WebEx participants.

Step 3 Paste the WebEx information into the email and send it.

WebEx participants join the meeting by clicking the URL you sent in the email or copying and pasting it into their browser.

TelePresence participants join the meeting by pressing the button on their TelePresence phone.

Note All existing meetings scheduled by the user before they become a WebEx Premium User will remain unchanged. All meetings scheduled thereafter will have WebEx enabled. WebEx can be enabled for an existing meeting only by adding or deleting endpoints or changing the time of the meeting.

WebEx Non-Permitted User

If the meeting organizer is a WebEx Non-Permitted user, they are not permitted to use WebEx with any of their meetings.

In this case, the WebEx button in the confirmation email and the WebEx tab in the Meeting Manager window are not available.

Usage Survey

The Usage Survey window allows you to view and fill out the survey.

To fill out the survey:

Step 1 Select or enter an answer for each of the questions.

Step 2 Click **Apply**.

Meeting Options

The meeting options window allows you to adjust other options for your meeting.

Note Meeting options are different for an intercompany meeting. See the Intercompany Host Meeting Options and Intercompany Participant Meeting Options sections, for more information.

Mark this meeting as private: Allows you to show or hide the TelePresence meeting subject on the phone in the TelePresence endpoint.

Provide a call-in number for other participants?: Allows you to provide a call-in number for TelePresence endpoints that were not originally invited to the meeting to be able dial in to the meeting.

The following options are available only for a meeting scheduled with one endpoint:

Number to Dial: Enter a call-in number. The entire number must be 15 digits or less, and begin with a country prefix. You must enter only numbers. Other characters including dashes are not permitted.

Is this meeting intended for recording a video to be distributed later?: Allows you to record the meeting for distribution later.

Is TelePresence required for this meeting?: Allows you to disable TelePresence for the meeting. When TelePresence is disabled, Action Required emails will not be sent if any additional settings are changed.

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

Allowing Other Users to Manage Your Meetings

The meeting organizer can select up to five other users who can also manage the meeting organizer's meetings. The user(s) will receive the email notifications and have the ability to access Meeting Manager to view meeting details, change meeting options, as well as change preferences.

Note First-time WebEx authentication must be done by the meeting organizer.

In the emails and in the meeting details, delegates will see the meeting information based on the organizer's time zone and locale preferences, not the delegates' own.

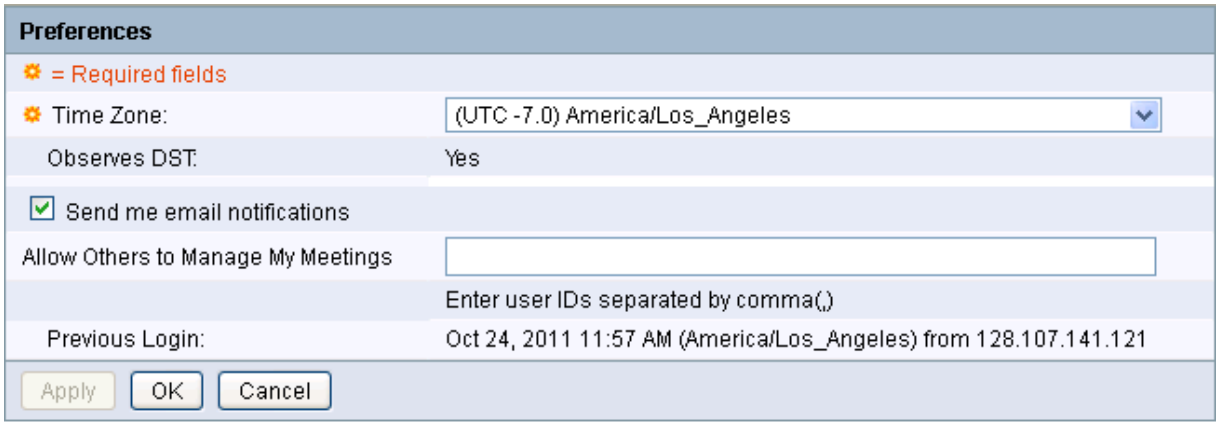
All feature options that are available to the meeting organizer are also available to the delegates for the organizer's meetings.

To allow other users to manage your meetings:

Step 1 In the Meeting Manager window, click **Preferences**.

The Preferences window opens.

Figure 14-7 Preferences



Step 2 In the Allow Others to Manage My Meetings field, enter the user ID of each user to whom you want to delegate management of your meetings. User IDs must be separated by a comma and must be valid LDAP user IDs.

example: jsmith, kjohnson, bjones

Step 3 (Optional) After you enter at least one delegate, if you don't want to receive email notifications for meetings that you schedule, uncheck **Send me email notifications**.

Step 4 (Optional) If you want to save the user IDs that you are entering and keep this window open while you find other user IDs to enter, click **Apply**.

Step 5 When you are finished, click **OK** to save changes and close the Preferences window.

System Alert Notification

Each day after the CTS-Manager maintenance cycle, the SysAdmin receives a system alert notification email if there are any meetings that were scheduled but never took place (no-show meetings), and meetings for which the survey was not completed by the meeting organizer.

This email displays the following information:

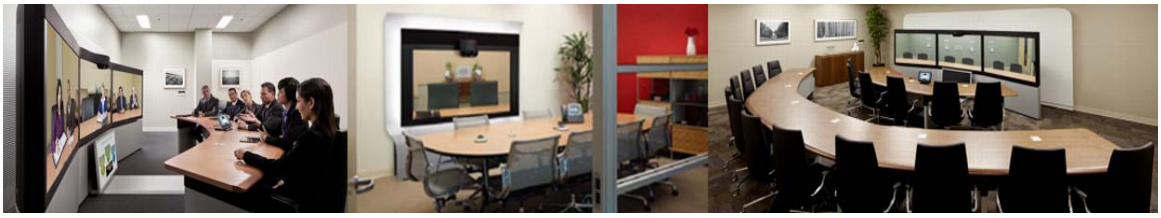
Table 14-11 Organizers of No-Show Meetings

Field Name	Description
Organizer Name	The meeting organizer who scheduled the meeting.
Meeting Count	The number of scheduled meetings that never took place.
Total Hours	The total number of hours associated with the meetings that never took place.

Table 14-12 Meetings without Usage Survey Responses

Field Name	Description
Organizer Name	The meeting organizer who scheduled the meeting.
Meeting Count	The number of scheduled meetings for which the Usage Survey has not been completed.

Note The Meetings without Usage Survey Responses information will not be available if the Metrics Dashboard and Reporting API license is not uploaded. To upload the Metrics Dashboard and Reporting API license, go to the **Configure > Licenses** window, click the **License Files** tab and click **Upload**.



CHAPTER 15

Supported MIBs for Cisco TelePresence Manager

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

Contents

- Introduction, page 15-1
- MIB Support, page 15-1

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 15-1 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	

Table 15-1 CTS-Manager Supported MIBs

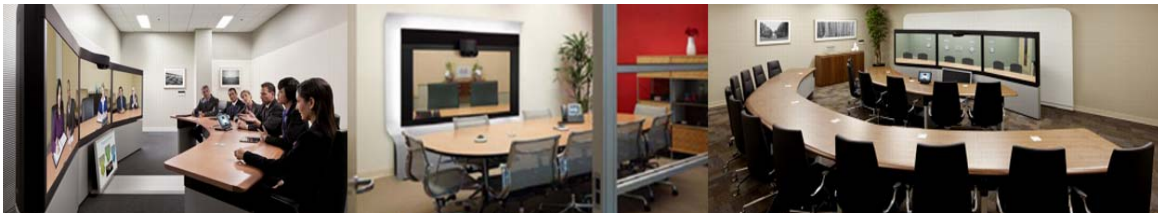
MIB	Support	Capability Location
SNMPv2-MIB	Fully	
TCP-MIB	Partially	ftp://ftpeng.cisco.com/pub/mibs/v2/CISCO-TCP-STD-CAPABILITY.my
UDP-MIB	Fully	
SNMP-FRAMEWORK-MIB	Fully	
SNMP-MPD-MIB	Fully	
SNMP-VACM-MIB (SNMP-VIEW-BASED-ACM-MIB	Fully	
SNMP-NOTIFICATION-MIB	Fully	
SNMP-TARGET-MIB	Fully	
SNMP-USER-BASED-SM-MIB	Fully	
HOST-RESOURCE-MIB	Fully	

Table 15-2 CTS-Manager Supported H/W MIBs

MIB	Support	Capability Location
IBM PLATFORM		
IBM-SYSTEM-AGENT-MIB		
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

Table 15-2 CTS-Manager Supported H/W MIBs

MIB	Support	Capability Location
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 16

Troubleshooting Cisco TelePresence Manager

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

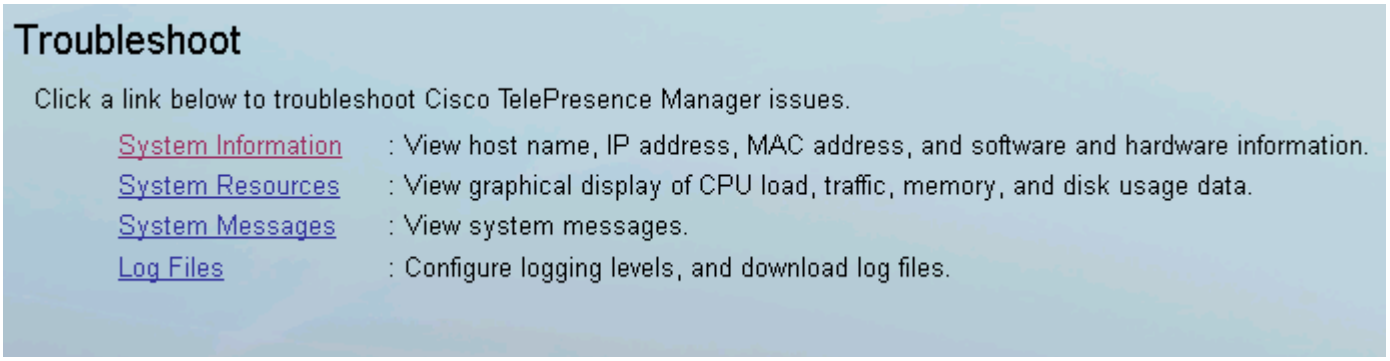
Contents

- Introduction, page 16-2
- System Information, page 16-2
- System Resources, page 16-3
- System Messages, page 16-5
- Log Files, page 16-6
- Scheduled Meeting and Endpoint Issues, page 16-10
- Endpoint Phone/Display Device User Interface Issues, page 16-16
- Cisco TelePresence Manager Database Issues, page 16-17
- Bridges and Servers Issues, page 16-18
- Cisco Unified Communications Manager (Unified CM) Issues, page 16-19
- Calendar Server and LDAP Interface Issues, page 16-20
  - LDAP Server Issues, page 16-20
  - Microsoft Exchange Calendar Server Issues, page 16-21
  - IBM Domino Calendar Server Issues, page 16-24
- Scheduling API Issues, page 16-26
- Web Browser Error Messages, page 16-26
  - JavaScript Error Message, page 16-26
  - Safe ActiveX Checking Message, page 16-27
- System Alert Notifications, page 16-27

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 16-1 shows the links available to assist you with these troubleshooting tasks.

Figure 16-1 Troubleshooting Window

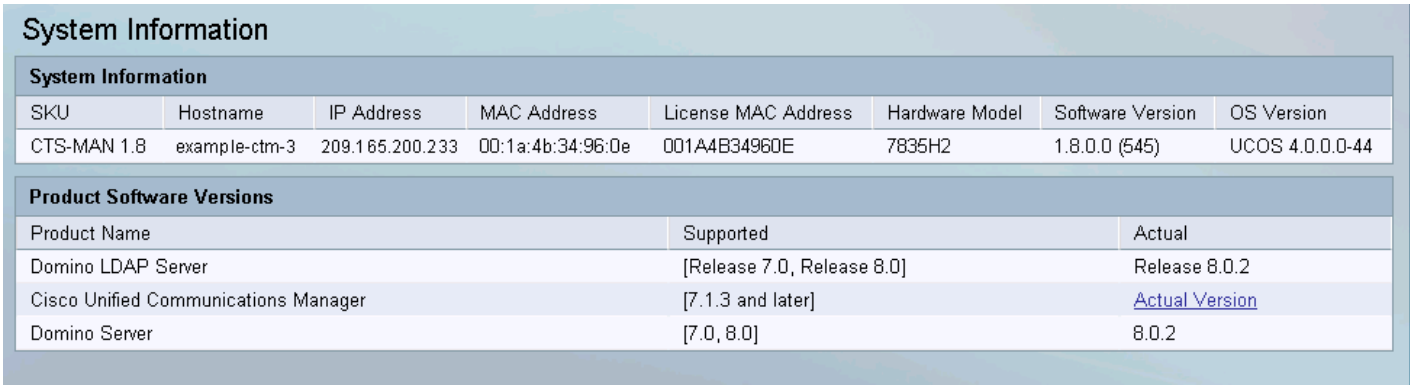


System Information

The System Information window displays 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.

Figure 16-2 Troubleshoot > System Information



System Resources

Table 16-1 System Information

SKU	CTS-Manager 1.9.x
Hostname	The name of the CTS-Manager server (e.g. example-ctm19).
IP Address	The IP address of the CTS-Manager server.
MAC Address	The MAC address of the CTS-Manager server (e.g. 00:18:fe:73:58:14).
License MAC Address	The MAC address of the CTS-Manager server that is used to get licenses.
Hardware Model	The hardware model of the CTS-Manager server (e.g. 7845H2).
Software Version	The version of CTS-Manager software running on the server (e.g. 1.9.0.0).
OS Version	The software version of the Cisco Unified Communications OS running on the CTS-Manager server (e.g. Cisco Unified CM OS 3.0.0.0-44).
Product Software Versions	Supported versions for Microsoft Exchange or Domino, Active Directory or Domino LDAP Server and Domino Server, and Cisco Unified CM.

This System Resources window displays eight graphs which provide system information.

Figure 16-3 System Resource Information Chart 1 - 4

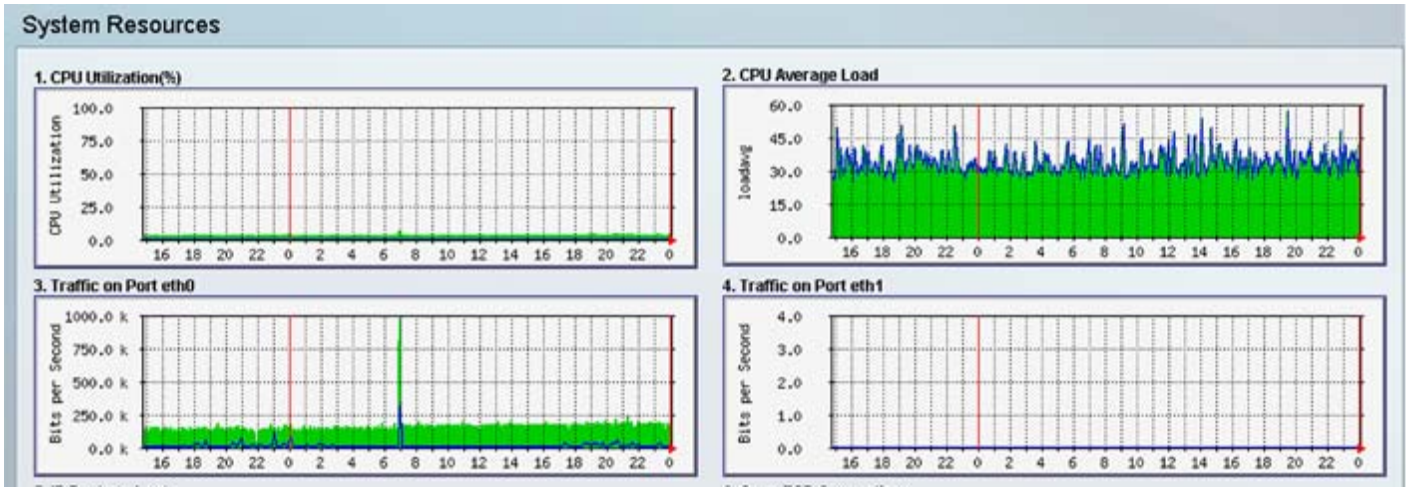
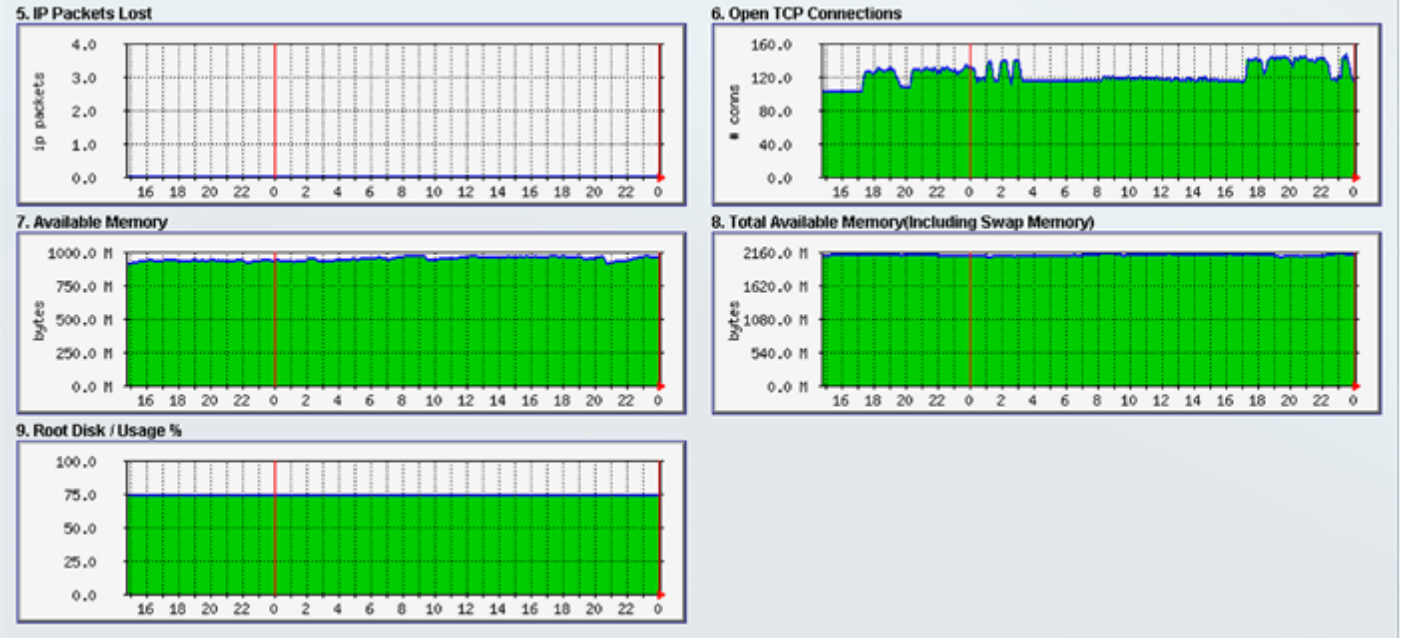


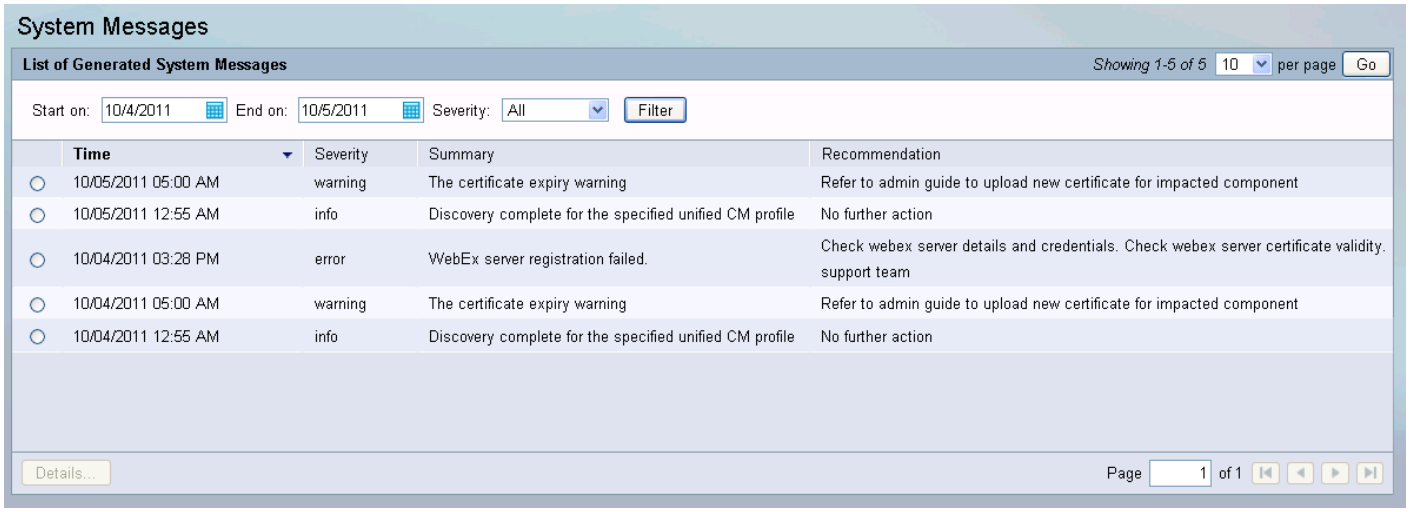
Figure 16-4 System Resource Information Chart 5 - 9



System Messages

The System Messages window displays system messages provided by the CTS-Manager.

Figure 16-5 Troubleshooting System Resources Window



Click the radio button and then click the **Details** button to view the details of the alert.

Table 16-2 System Messages Fields and Descriptions

Field	Description
Time (+)	Date and time the message was logged. You can sort the messages in ascending or descending order by the time stamp.
Severity	Message severity level. (All, Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug),.
Summary	Explanation of problem detected. Move your mouse pointer over a message field to see a complete description.
Recommendation	Recommended action to correct the problem.

To view details about a specific message:

Step 1 Select the message by clicking its radio button.

Step 2 Click **Details**.

The Details window for the selected message opens, providing additional information about the message.

Tip Each message has a unique ID number. To find out more information about each message, including its possible cause and any solutions, refer to Appendix A, "Cisco TelePresence Manager System Messages."

Log Files

In the Log Files window, you can download log files, set levels for logging system errors and archive logs:

- Log Files
- Log Levels
- Archive

Log Files

In the Log Files tab of the Log Files window you can download logs for the following services:

- Discovery
- Calendar
- Room Phone UI
- Admin UI
- Multipoint Conference
- TelePresence Engine Components
- WebEx
- Recording

Generating a List of Specific Log Types

Step 1 From the Service drop-down list, choose one of the following to specify the type of errors to display:

Note To display the errors for all services, select **All**. This is the default selection.

Step 2 Click **Filter** to generate the list.

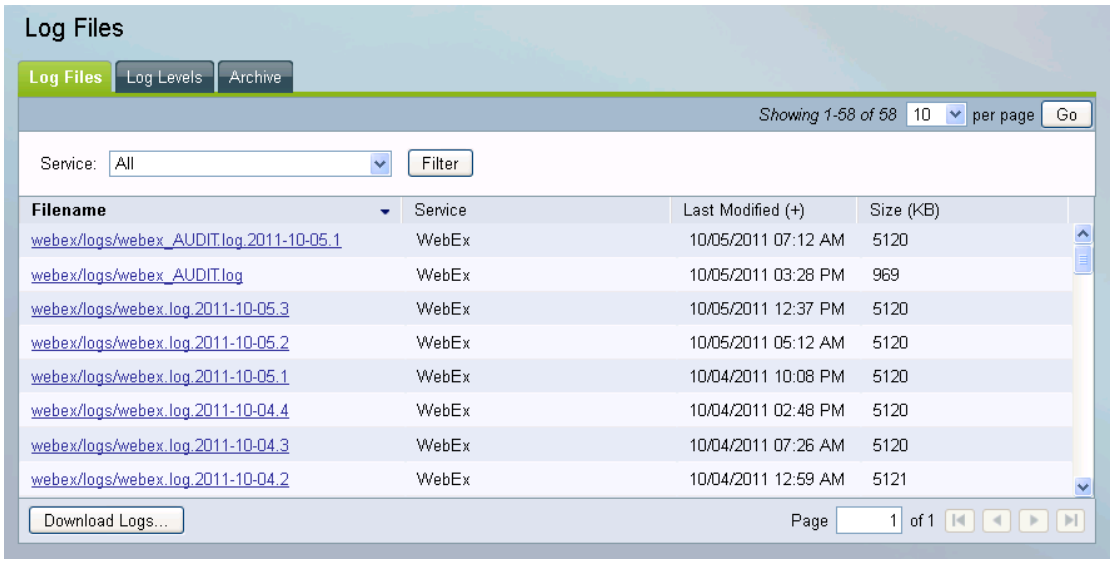
Note Log files are named with a .log extension. The log filename provides a link to the contents of the error log file. This window also shows the date the file was last modified and the size of the log file. The lists can be sorted by filename and time last modified.

Downloading Log Files

You can download log files individually or all together in a single compressed file:

- To download individual log files, click the name of the log file you want to download. You are prompted to either open or save the file.
- To download all log files, click **Download Logs**. All logs are compressed into a file that can be emailed, which makes it convenient to provide to Cisco technical support if you encounter a problem using CTS-Manager.

Figure 16-6 Troubleshoot > Log Files > Log Files



Log Levels

In the Log Levels tab of the Log Files window you can set levels for the following logs:

Services

- Unified CM
- Microsoft Exchange or IBM Domino
- Endpoint Phone UI
- Admin UI
- Multipoint Conference
- WebEx

TelePresence Engine

- Service Providers
- Data Access
- Interface

You can set the messages from these services to the following levels:

- DEBUG—Detailed/verbose information on internal system activity.
- ERROR—Errors that need to be addressed by user or if needed, brought to system support team notice.

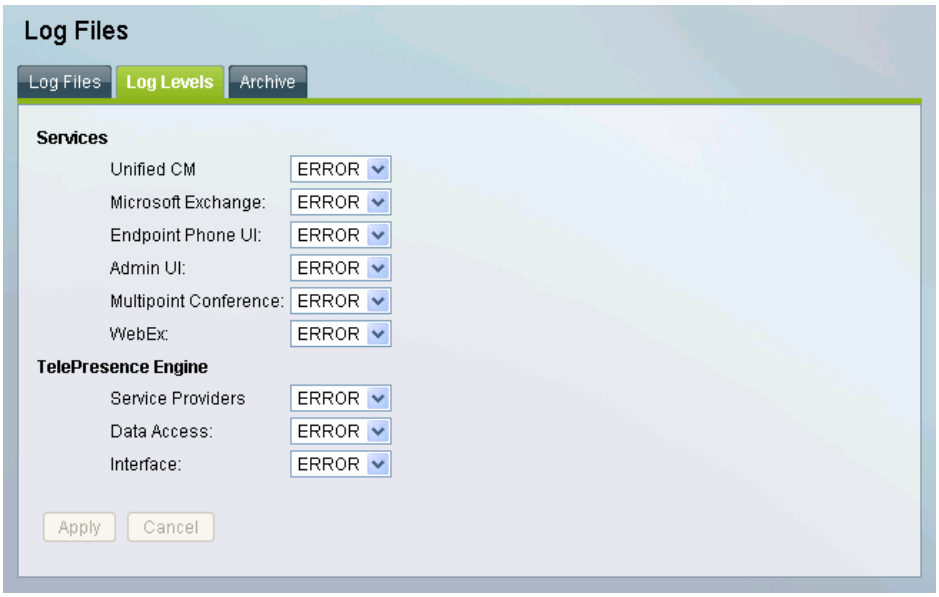
The default logging level is typically set to ERROR. There may be times when Cisco technical personnel will instruct you to modify the logging level for one or more of the services, to help them diagnose a problem. Be sure to reset the logging level immediately after the problem has been resolved, or else disk space may become filled with messages and negatively impact system performance.

Note If you set the debug level to DEBUG in a pre-1.9 version of CTS-Manager and then upgrade to CTS-Manager 1.9 or later, the debug level is set back to the default setting of ERROR.

Once you have made your logging level choices for each service:

- Click **Apply** to save new settings or click **Reset** to restore the original settings before you save your new settings.

Figure 16-7 Troubleshoot > Log File > Log Levels



Archive

In the Archive tab of the Log Files window you can configure where you want to archive logs.

Note Log files stored at remote location are stored in compressed form but are not encrypted. If you choose the Remote Storage option, ensure that the logs are not publicly accessible by choosing a secure storage location

Table 16-3 describes the archive configuration options.

Table 16-3 CTS-Manager Log Files Archive Settings

Field or Button	Description or Settings
Archive Logs to	Local Server: Log files are stored on this CTS-Manager Remote Storage: Log files are stored on a remote server.
Storage Type	When Remote Storage is selected, choose FTP or SFTP.
Host	Archive log remote storage location
Port	Port to access the remote host. The default is port 22 for SFTP.
Username	Login name for the remote server.

Table 16-3 CTS-Manager Log Files Archive Settings (continued)

Field or Button	Description or Settings
Password	Password to access the remote server.
Storage Path	The full pathname where you want to remotely store the log files.
Download Logs for	Date of the archive logs to download. Enter a date (mm/dd/yyyy) or click the calendar icon and click a date.
Download	To download the archive logs for the selected date, click **Download**.

Downloading Archive Log Files

You can download archive log files all together in a single compressed file by doing the following:

Step 1 In the Download Logs for field, enter a date or select one by clicking the calendar.

Step 2 Click Download.

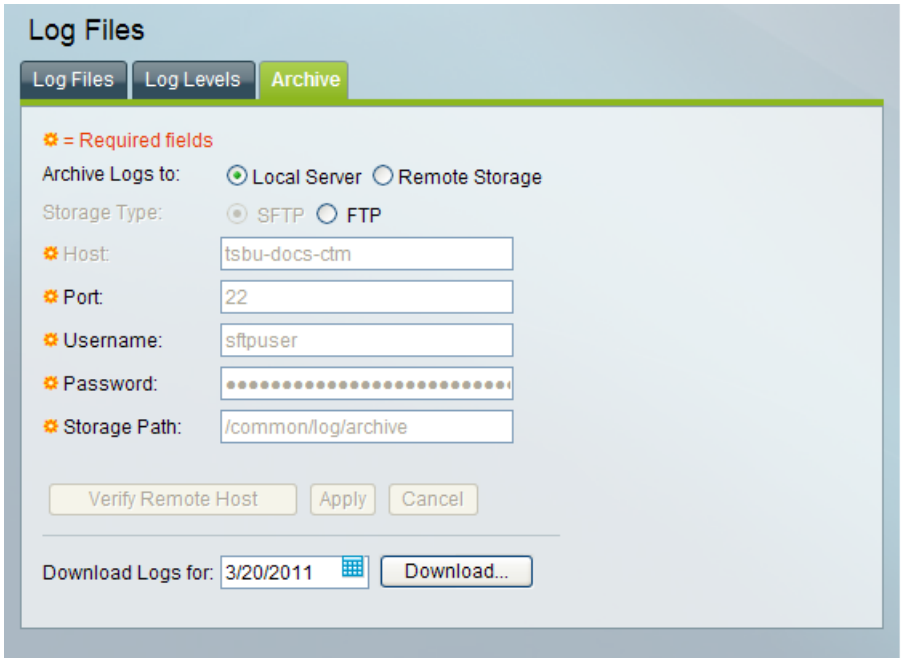
You are prompted to either open or save the file.

To test your connection to a remote host, click **Verify Remote Host**.

To save new or modified settings, click **Apply.**

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

Figure 16-8 Troubleshoot > Log Files > Archive



Scheduled Meeting and Endpoint Issues

Meeting information is retrieved via processing room (endpoint) 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 (endpoint) 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 (endpoint) meeting schedule using the Resync 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 Support > Endpoints window displays the endpoint status as “In Use” when a call is placed. The Configure > Meetings window displays meetings as “In Progress” or “Completed” reflecting the actual state of the call.

If the Live Desk is called, this condition will be reflected in the Room UI view as “Needs Help”.

Refer to troubleshooting information in Table 16-4 to solve common problems that prevent Cisco TelePresence meetings from being scheduled correctly.

Table 16-4 Scheduled Meeting and Endpoint 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 (endpoint) is in manual-accept mode and its 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 (endpoint) 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 (endpoint) is not in auto-accept mode.	Make sure reserved rooms (endpoints) are in auto-accept mode. If a room (endpoint) is in manual-accept mode, the meeting invitation must be accepted by its delegate using Microsoft Outlook or Lotus Notes.

Table 16-4 Scheduled Meeting and Endpoint Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Scheduled Meetings do not show the status “In Progress”, or endpoints do not show “In Use” when a call is placed.	Connectivity between the Cisco TelePresence system and CTS-Manager is lost.	Check the Support > Endpoints 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.
Endpoint 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 endpoint is not included in Cisco TelePresence Manager application user profile. • The phone associated with the Cisco TelePresence endpoint is not registered with the Unified CM. • More than one Cisco TelePresence phone could be configured with the same endpoint name.	Cisco TelePresence IP phone associated with participating endpoints must be added to the CTS-Manager Application User Profile. Update the CTS-Manager Application User Profile with correct endpoint data. Check the Support > Endpoints 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.

Table 16-4 Scheduled Meeting and Endpoint Issues (continued)

Problem or Message	Possible Causes	Recommended Action
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 endpoints are scheduled).	The endpoints 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 (endpoint) delegate has declined one instance (R1), all meeting instances show only one endpoint scheduled. If the recurring meeting is a multi-point meeting (R1, R2, & R3) and a room (endpoint) delegate has declined one instance (R1), all meeting instances show only two endpoints scheduled (R2 & R3).	• In Microsoft Exchange, select the check box for the endpoint(s) missing from the scheduled meeting and Resync. • In IBM Domino, click Resync to resync the database.
Endpoint Status reports a Subscription or Synchronization error with Microsoft Exchange	A discovery operation attempted to sync to a newly added room (endpoint) calendar before even one meeting was added to the calendar.	A room (endpoint) 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 (endpoint) calendar. 2. From the Configure > Microsoft Exchange window, select the endpoint showing the subscription error and click **Resync**.
Recurring or single meeting with only one endpoint (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 of the endpoints 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 of the endpoints (rooms) are removed from the scheduled meeting and the meeting is set to an Error status.	This is expected behavior. All rooms (endpoints) calendars are available for scheduled meetings.

Table 16-4 Scheduled Meeting and Endpoint Issues (continued)

Problem or Message	Possible Causes	Recommended Action
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 (Live Desk 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.
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 synchronized and must be rescheduled.	Verify the endpoints (rooms) are registered properly in the Configure > IBM Domino window. The endpoint name appearing in the Associated Rooms column must exactly match the room (endpoint) 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 endpoint 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.

Table 16-4 Scheduled Meeting and Endpoint Issues (continued)

Problem or Message	Possible Causes	Recommended Action
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.	Resync the endpoints with scheduled meeting errors or missing meetings. After the endpoint resync, Exchange may still display an error status. This can be fixed by either: • waiting for CTS-Manager to renew subscription to the affected endpoints (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
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 endpoint.
A deleted meeting still appears in the Scheduled Meetings window.	The meeting was deleted from the Exchange endpoint calendar, but the meeting is not deleted in CTS-Manager. This can happen if room (endpoint) reservations are managed using Outlook Auto Accept.	Delete the meeting from the room (endpoint) calendar. Refer to Microsoft Knowledge Base article 280854 for more information.
An endpoint shows a sync error with a calendar server.	1. A new endpoint with no scheduled meetings is included in a multipoint recurring meeting. 2. Meeting goes into error state, because of reduced bridge or server resources. 3. The meeting series is deleted through Outlook. 4. The new endpoint now has a ‘one room’ meeting error. 5. Exchange returns ‘0’ meetings for the new endpoint during daily maintenance, but the CTS-Manager database still contains a meeting for the endpoint.	Perform one of the following procedures to correct the endpoint sync error: • Create a meeting using this room (point-to-point, multipoint, single or recurring). The next daily maintenance corrects the sync error. • Perform a manual sync for the endpoint.

Table 16-4 Scheduled Meeting and Endpoint Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Scheduled meeting is in error state for a new endpoint.	A new endpoint 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.	Resync the endpoint with Exchange.
Meeting does not show up in CTS-Manager Web UI nor is it pushed to the phone UI.	Endpoint (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 endpoint (room) mailbox acceptance mode.
No clarification email sent when a meeting is modified to include only one endpoint.	If the meeting organizer is using OWA and deletes one of two endpoints 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.
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 an endpoint are deleted, CTS-Manager is not updated to reflect the meeting deletions in Exchange.	Create a new scheduled meeting for the endpoint to resync 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 endpoint, 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 endpoint (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.

Table 16-4 Scheduled Meeting and Endpoint Issues (continued)

Problem or Message	Possible Causes	Recommended Action
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 endpoints, CTS-Manager deletes all endpoints and meetings, adds new endpoints, 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.
If a recurring meeting is started at a local time which is shifted by the daylight savings time change (for example in the U.S., between March 14, 2:00 to 2:59 AM), future recurring meeting instances could be shown in a wrong local time.	Meeting is scheduled during the date and time that daylight savings time begins.	Modify the time of all future instances after daylight savings time has begun to the correct time.
After system upgrade to CTS-Manager 1.9 and after the maintenance cycle, most of the multipoint meetings are displaying the following error: "WARNING: The system is waiting for more information on this meeting from the calendar server. Try to view the meeting again after a few minutes."	This normally occurs if the meeting processing/resource allocation takes longer than 2 minutes, blocking other threads that are trying to acquire the lock on the same meeting. This can occur when there are many long recurring meetings (more than 300 occurrences) with many endpoints (70 or more).	Modify the meeting time and/or recurring pattern, so the meeting gets revalidated.

Endpoint Phone/Display Device User Interface Issues

Once a scheduled Cisco TelePresence meeting has been confirmed by participating endpoints (rooms) in Microsoft Exchange or IBM Domino, it should be listed on the endpoint phone/display device user interface in less than three minutes. Use Table 16-5 to troubleshoot problems between scheduled meetings and the phone user interface.

Table 16-5 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 endpoint (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 endpoint (room) name must exactly match the name (e-mail alias) provided in the Directory Server. • Remove duplicate endpoint (room) names configured in Unified CM. • Update the CTS-Manager Application User Profile with correct endpoint (room) data. • Change the CTS-Manager user account for Exchange or Domino so it has permissions to retrieve (read) endpoint (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 16-6 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.

Bridges and Servers Issues

CTS-Manager supports five types of bridges and servers. Table 16-7 documents any issues or anomalies between CTS-Manager and specific bridges or servers.

Table 16-7 Bridges and Servers 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.
CTS-Manager shows scheduled meeting failed due to insufficient resources.	Each room (endpoint) participating in a multipoint or interop call that is capable of 30fps requires 1 additional segment	Allocate enough resources in CTMS to provide for multipoint or interop calls with 30fps endpoints.

Cisco Unified Communications Manager (Unified CM) Issues

Table 16-8 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 Configure > Security 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 Configure > Discovery Service window.
Connection failed between secure CTS-Manager and secure CUCM (8.0.3). Troubleshoot > System Messages window displays the following error: “Provider is null” The Discovery log (accessible from the Troubleshoot > Log Files window) displays the following error:- ERROR cti.CTIAdapter (initJtapi:661) - Failed to create CTI Adapter :Unable to create provider -- Socket Closed com.cisco.jtapi.PlatformExceptionImpl: Unable to create provider -- Socket Closed at com.cisco		Log into the Cisco Unified CM Administration application for the CUCM and restart the “Cisco CTIManager” service.

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 16-10 and Table 16-11 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 16-9 LDAP Server Issues

Problem or Message	Recommended Action
Endpoint (room) is not synchronized 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 16-10 Microsoft Exchange Calendar Server Issues

Problem or Message	Possible Causes	Recommended Action
Extra endpoint has been added to a specific instance of a recurring meeting. **Note** This issue occurs with Exchange 2007.	1. 1. A meeting organizer schedules a recurring meeting with two or more endpoints (E1, E2 and E3). 2. 2. Meeting organizer deletes E1 from one instance of recurring meeting (M1). 3. Meeting organizer adds a fourth endpoint to master series (E4). 4. E1 has been re-added to M1.	1. Open the E1 room calendar and delete the scheduled meeting instance. 2. In Cisco TelePresence Manager, go to the Configure > Microsoft Exchange window, select the check box next to the room and click the Resync button. **Note** Refer to Microsoft Knowledge Base article 949294 for more information.
Endpoint Status reports a Subscription status error or a sync error with Microsoft Exchange	A Discovery operation attempted to sync to a newly added room (endpoint) calendar before even one meeting was added to the calendar.	A room (endpoint) 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 (endpoint) calendar. 2. From the Configure > Microsoft Exchange window, select the endpoint showing the subscription error and click **Resync**. 3. From the Support > Endpoints Summary tab, select the endpoint showing the Exchange subscription or sync error (on the Status tab), and click **Update Schedule**.

Table 16-10 Microsoft Exchange Calendar Server Issues (continued)

Problem or Message	Possible Causes	Recommended Action
Endpoint is not synchronized between Microsoft Exchange and Cisco TelePresence Manager.		• Cisco TelePresence Manager must have Full Access or Read Permission to the room's (endpoint's) mailbox. • The room (endpoint) mailbox must be created with English as the default language. • The room (endpoint) user must log into the room mailbox at least once. • The room (endpoint) email ID must be uniquely assigned to only one user (endpoint user). • Room's (endpoint'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 (endpoint) is configured for Auto-accept, or the Room Delegate has accepted the meeting invitation. • At least one meeting must be scheduled on a room (endpoint) calendar before syncing with CTS-Manager, or CTS-Manager will return a sync error condition for the endpoint

Table 16-10 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 (endpoint) 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 (endpoint) calendar mailbox setting to false.
Single meeting email confirmation may show incorrect local time zone for meeting start time.	Outlook desktop does not set the meeting time zone 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 endpoints included in the meeting.	Do not use OWA to schedule a meeting if you are logging in as one of the endpoints included in the scheduled meeting.

Table 16-10 Microsoft Exchange Calendar Server Issues (continued)

Problem or Message	Possible Causes	Recommended Action
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 Configure > 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.
The most recent changes to an individual instance of a recurring meeting are sometimes not displayed on the endpoint phone/display device.	When using Exchange 2007 and WebDAV, the Exchange Server sent different time zones that triggered the recurring meeting to be processed again.	Microsoft recommends using Exchange 2007 with EWS. **Note** WebDAV is not recommended for Exchange 2010.

IBM Domino Calendar Server Issues

Table 16-11 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.
Endpoint is not synchronized between Domino server and Cisco TelePresence Manager.		• The room (endpoint) user must log into the room mailbox at least once. • The room (endpoint) email ID must be uniquely assigned to only one user (room user). • Room's (endpoint'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 16-11 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 Configure > IBM Domino window).

Scheduling API Issues

Table 16-12 Scheduling API Issues

Problem or Message	Possible Causes	Recommended Action
Internet Explorer (IE) 8: When using IE 8 with CTS-Manager deployed with Scheduling API, the web UI and logs display no information.	Settings in IE 8 that only allow non-secure data to flow through and block the display of secured data.	Select **Tools** > **Internet Options**. Select the **Advanced** tab and click **Reset**.

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, page 16-26
- Safe ActiveX Checking Message, page 16-27

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 Alert Notifications

Each day after the CTS-Manager maintenance cycle, the following emails are sent to the email address specified in the Copy Outgoing Email To field in the Configure > Application Settings > Email window, if the appropriate conditions exist:

- No-Show Meetings and Meetings without Survey Responses
- Mailbox Alert
- Certificate Expiry

The No-Show Meetings and Meetings without Usage Survey Responses

This email is sent if there are any meetings that were scheduled but never took place (no-show meetings), and/or meetings for which the survey was not completed by the meeting organizer.

The following information is provided:

Table 16-13 Organizers of No-Show Meetings

Field Name	Description
Organizer Name	The meeting organizer who scheduled the meeting.
Meeting Count	The number of scheduled meetings that never took place.
Total Hours	The total number of hours associated with the meetings that never took place.

Table 16-14 Meetings without Usage Survey Responses

Field Name	Description
Organizer Name	The meeting organizer who scheduled the meeting.
Meeting Count	The number of scheduled meetings for which the Usage Survey has not been completed.

Note The Meetings without Usage Survey Responses information will not be available if the Metrics Dashboard and Reporting API license is not uploaded. To upload the Metrics Dashboard and Reporting API license, go to the **Configure > Licenses** window, click the **License Files** tab and click **Upload**.

Mailbox Alert

This email is sent if the CTS-Manager mailbox has exceeded it size limit and is no longer able to send emails to meeting organizers. In this situation, it is important to delete all emails no longer required. Cisco recommends setting policies to automatically purge emails when the mailbox reaches 75% of it's allocated threshold.

Note Refer to the documentation for your calendaring and messaging software for more information.

The following information is provided:

Table 16-15 Mailbox Quota Information

Field Name	Description
Mailbox Quota	The total available mailbox space.
Current Mailbox Size	The current mailbox size.

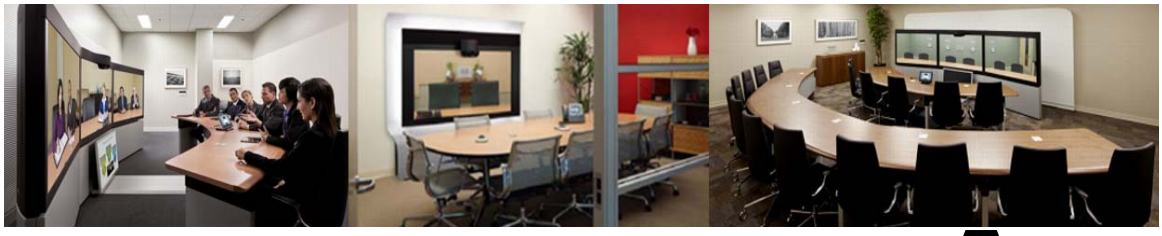
Certificate Expiry

This email is sent if one or more security certificates are about to expire. In this situation, it is important to replace the expiring certificate(s) as soon as possible, so CTS-Manager will continue to function properly.

The following information is provided:

Table 16-16 Certificate Expiry Information

Field Name	Description
Certificate Name	Name of expiring certificate
Certificate Unit	Unit of expiring certificate
Certificate Type	Type of expiring certificate
Certificate Expiration	Date certificate will expire



APPENDIX A

Cisco TelePresence Manager System Messages

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

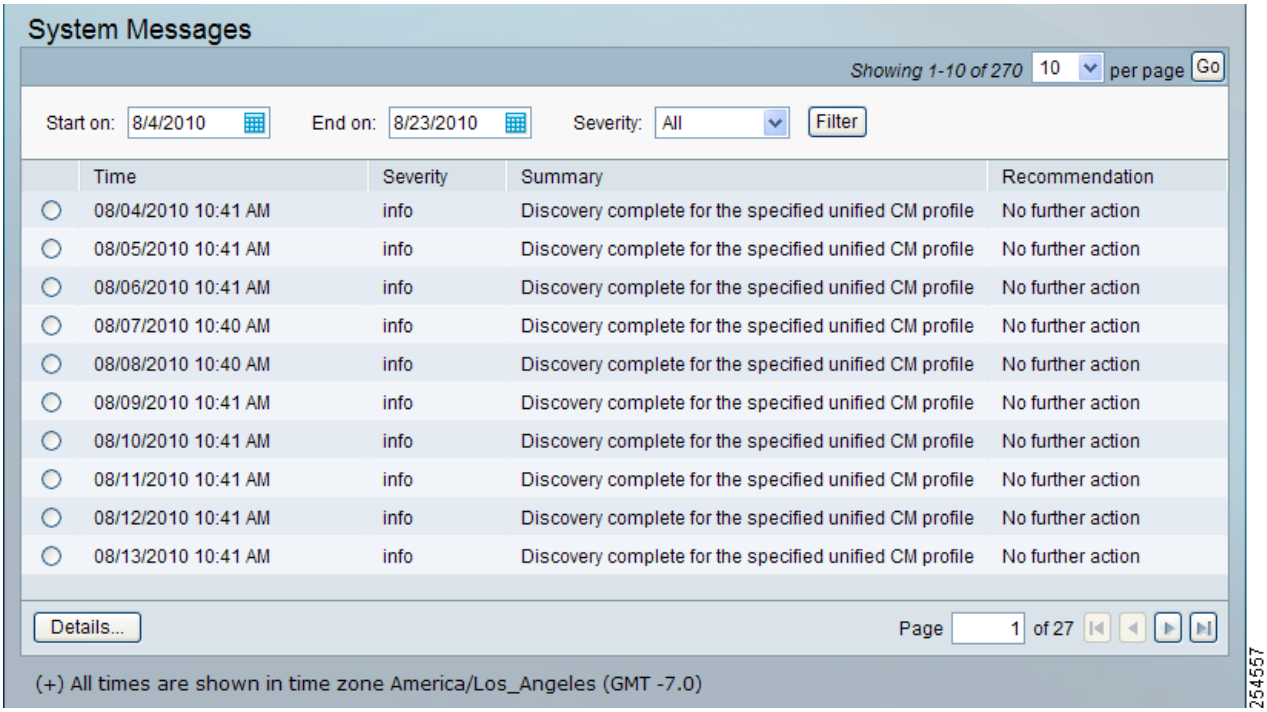
Contents

- System Message Overview, page A-1
- System Messages By ID Number, page A-4

System Message Overview

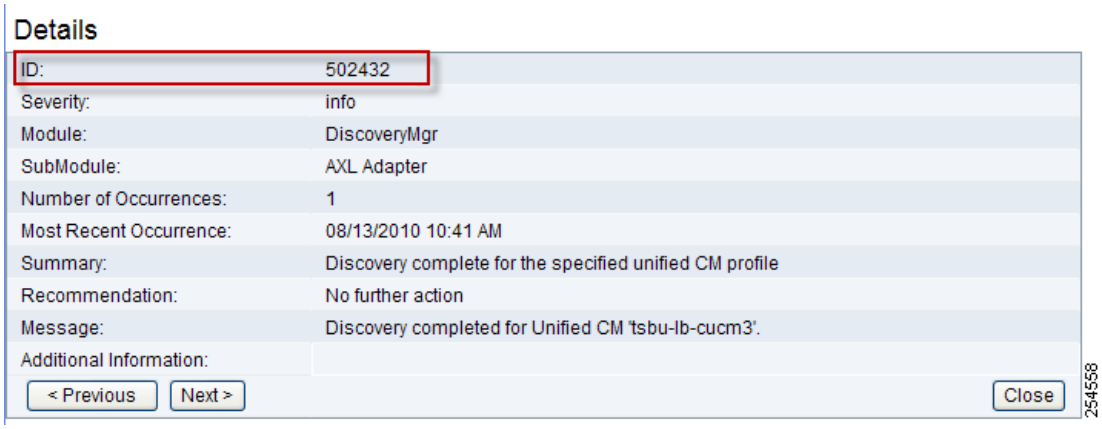
The CTS-Manager system messages appear in the Troubleshoot > System Messages window, which is shown in Figure A-1.

Figure A-1 System Messages Window



The messages in this appendix are organized by the unique ID number assigned to each message. To view the ID number for a message, you must click the radio button associated with the message, then click **Details...**. The ID number appears in the Details window, which is shown in Figure A-2.

Figure A-2 System Messages Details Window



Each ID number corresponds to a software module that generates the system message. Table A-1 maps the ID number ranges to their respective software modules.

Table A-1 ID Number Range and Software Module Mapping

ID Number Range	Software Module
501000-501099	General server
501200-501399	Schedule management module API
501400-501599	Resource management module API
501600-501699	Security management module API
501700-501799	Administrative management module API
501900-501999	Calendar generator module
502000-502099	Data access
502100-502199	LDAP
502300-502399	API layer
502400-502499	Discovery manager
502500-502599	Event subsystem
502600-502699	UI module
502700-502799	Certificate management module
502800-502899	Configuration management module
502900-502999	Licensing module
503000-503099	Groupware adapter module
503100-503299	Exchange adapter module
503500-503599	Email management module
503600-503799	Resource schedule management module

Table A-1 ID Number Range and Software Module Mapping (continued)

ID Number Range	Software Module
503800-503999	MCU module
504000-504099	Domino adapter module
504100-504199	Reporting module
504200-504299	WebEx module
505000-505199	External scheduling API module

Each system message has a severity level assigned to it. From the most to the least severe, the severity levels are as follows:

- Alert
- Critical
- Error
- Warning
- Notice
- Info(rmational)

Some system messages in this appendix include “$1,” “$2,” “$3,”and so on. These strings are variables. When these variables appear in the System Messages window, they are replaced by a text or numerical string that provides specific information about the condition that caused the message to display.

System Messages By ID Number

This section presents each CTS-Manager system message by ID number.

501000

Summary

Internal application error

Message

The system has encountered an unexpected condition ($1)

Module

General server

Severity

Error

Explanation

The system encountered the specified error.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501001

Summary

The system configuration file can not be processed

Message

Unable to parse system configuration file '$1' because $2

Module

General server

Severity

Error

Explanation

The server failed to parse the config/ctis.xml configuration file, and as a result, the web application could not start up.

Recommendation

The administrator should check the syntax of the ctis.xml file. This file should be changed by a qualified technician only. If possible, revert to its original content and restart the Tomcat server. If more assistance is needed, the administrator can contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501004

Summary

Unsupported software version

Message

Software version '$1' of third party component '$2' is not supported

Module

General server

Severity

Warning

Explanation

CTS-Manager does not support the software version extracted from the given component.

Recommendation

The administrator can upgrade the third-party component to a supported software version.

501007

Summary

Unable to restart host

Message

Unable to restart host because $1

Module

General server

Severity

Alert

Explanation

CTS-Manager could not restart the host as requested.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501008

Summary

Functionality not implemented

Message

The functionality '$1' is not yet implemented

Module

General server

Severity

Warning

Explanation

The specified functionality has not yet been implemented.

Recommendation

The administrator can determine if the functionality is implemented in the latest version of CTS-Manager software and if it is, upgrade the software to that version.

501009

Summary

Unable to initialize system

Message

Unable to initialize system because $1

Module

General server

Severity

Error

Explanation

The database maintenance manager could not initialize because a script for a backup, purge, or cron job is missing.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501010

Summary

Unexpected null parameter passed to an operation

Message

Operation '$1' encounters unexpected null parameter '$2'

Module

General server

Severity

Error

Explanation

A Microsoft Exchange component could not test a connection because one of the required parameters (host, super user account name/password, bind method) is null.

Recommendation

The administrator can check the information provided on the Microsoft Exchange configuration window in the CTS-Manager Administration UI.

501011

Summary

Software execution error

Message

Unable to dispatch API '$1' because $2

Module

General server

Severity

Error

Explanation

A CTS-Manager component is unable to communicate with the CTS-Manager engine.

Recommendation

The administrator can check for errors in the log file. If needed, contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501012

Summary

Unable to shutdown host

Message

Unable to shutdown host because $1

Module

General server

Severity

Error

Explanation

The server cannot be shut down because of the specified reason.

Recommendation

The administrator can verify the following:

- That their user account has the required privilege level to shut down the server.
- Associated error messages in the log file.

For further assistance, contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501013

Summary

Can not resolve IP address for a host

Message

Unable to determine IP address of host '$1'

Module

General server

Severity

Error

Explanation

The hostname might be incorrect.

Recommendation

The administrator can verify the following to ensure that they are correct:

- The server hostname.
- The DNS configuration.

501014

Summary
Web application stopped

Message
Service '$1' is shutting down

Module
General server

Severity
Informational

Explanation
The specified service is shutting down.

Recommendation
No action is required.

501015

Summary
Web application started

Message
Service '$1' is started and ready to process requests

Module
General server

Severity
Informational

Explanation
The specified service was started.

Recommendation
No action is required.

501016

Summary

Application run time error

Message

Object class '$1' does not have property '$2'

Module

General server

Severity

Error

Explanation

An internal programming error has occurred.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501017

Summary

Application run time error

Message

Unable to acquire '$1' lock on element '$2'. Current lock is '$3'

Module

General server

Severity

Error

Explanation

The system has detected concurrent activity on the indicated database element. This activity is causing the locking mechanism to function unexpectedly.

Recommendation

Although the CTS-Manager server might still function normally after this message is received, we recommend that the administrator collects the log files, then contacts the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501200

Summary

An error occurs when processing meeting data

Message

Invalid meeting (subject '$1') because field '$2' has invalid value '$3'

Module

Schedule management module API

Severity

Error

Explanation

A field for the specified meeting has an invalid value. This error could indicate an internal problem with CTS-Manager.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501201

Summary

An error occurs when processing meeting data

Message

Invalid single meeting (subject '$1') because field '$2' has invalid value '$3'

Module

Schedule management module API

Severity

Error

Explanation

The specified meeting is not a single meeting as expected. This error could indicate an internal problem with CTS-Manager.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501202

Summary

An error occurs when processing meeting data

Message

Invalid recurring meeting (subject '$1') because field '$2' has invalid value '$3'

Module

Schedule management module API

Severity

Error

Explanation

The specified meeting is not a master meeting as expected. This error could indicate an internal problem with CTS-Manager.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501205

Summary

Meeting is not valid for One-Button-To-Push

Message

A second TelePresence endpoint, or other participant, has not been defined for this meeting

Module

Schedule management module API

Severity

Warning

Explanation

The Microsoft Exchange component sent an automated email informing a meeting organizer that their meeting has only one TelePresence endpoint scheduled.

Recommendation

The meeting organizer can add another TelePresence endpoint to the meeting, or provide a dial number. To take these actions, they can click the appropriate option in the automated email.

501211

Summary

TelePresence equipment is running incompatible software

Message

One or more TelePresence endpoints are running incompatible software. $1

Module

Schedule management module API

Severity

Error

Explanation

The Microsoft Exchange component sent an automated email informing a meeting organizer that their meeting is scheduled with endpoint(s) that cannot support a multipoint conference.

Recommendation

The administrator can check the software version running on the TelePresence equipment in each endpoint, and verify that all software versions support multipoint meetings. If they find software that does not support multipoint meetings, they should upgrade the software.

501212

Summary

Insufficient multipoint switch resources

Message

Insufficient multipoint switch resources to support this multipoint meeting

Module

Schedule management module API

Severity

Error

Explanation

The Microsoft Exchange component sent an automated email informing a meeting organizer that there is no available conference bridge for their multipoint meeting.

Recommendation

The meeting organizer can verify that the conference bridge is configured properly, and at least one bridge is available for the multipoint meeting. They should also add a new conference bridge, if necessary, or reschedule the meeting to a different time.

501213

Summary

Conference bridge is not configured

Message

A conference bridge has not been configured for your network

Module

Schedule management module API

Severity

Error

Explanation

The Microsoft Exchange component sent an automated email informing a meeting organizer that a conference bridge was not configured for a multipoint meeting.

Recommendation

The meeting organizer can verify that the conference bridge is configured properly, and at least one bridge is available for multipoint meetings. They should add a new conference bridge, if necessary.

501214

Summary

Organizer does not have sufficient privileges to schedule meeting

Message

Organizer does not have sufficient privileges to schedule '$1' meetings

Module

Schedule management module API

Severity

Error

Explanation

The Microsoft Exchange component sent an automated email informing a meeting organizer that they do not have the privilege level required to schedule a multipoint meeting.

Recommendation

The administrator can verify that the meeting organizer was assigned the required privilege level. If necessary, they should add the meeting organizer to the user group that has the required privilege level.

501215

Summary

Target MCU in migration does not have enough resources

Message

Unable to allocate resources for meeting (subject '$1'). Unavailable dates '$2'

Module

Schedule management module API

Severity

Error

Explanation

Not enough resources are available to migrate all meetings from one conference bridge to another.

Recommendation

The administrator can verify that the target conference bridge is properly configured and available.

501216

Summary

Unable to migrate meetings

Message

Unable to migrate meeting(s) because $1

Module

Schedule management module API

Severity

Error

Explanation

An error occurred when migrating meetings from one conference bridge to another.

Recommendation

The administrator can check for the associated error message in the log file, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501217

Summary

Insufficient video conferencing resources

Message

Unable to add video conferencing endpoint to meeting because of insufficient resources. Please contact help desk

Module

Schedule management module API

Severity

Error

Explanation

Not enough video conferencing resources are available to add a video conferencing endpoint to the meeting.

Recommendation

The meeting organizer can reduce the number of video conferencing participants, or increase the number of video conferencing resources on the video conferencing bridge.

501221

Summary

Some meetings update failed

Message

Bulk execution was not successful

Module

Schedule management module API

Severity

Error

Explanation

Some meetings could not be updated. This issue could be caused by a CTS-Manager server error.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501222

Summary

Time zone map loading failure

Message

Unable to load/parse time zone map file '$1' because $2

Module

Schedule management module API

Severity

Critical

Explanation

The timezonemap.xml file resides in the /usr/local/ctis/config directory. This file associates a user calendaring time zone (from either Microsoft Exchange or Lotus Domino) with a system time zone. During system installation or upgrade, a problem occurred with this file.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501223

Summary

Unknown time zone

Message

Unknown time zone target '$1'

Module

Schedule management module API

Severity

Error

Explanation

The timezonemap.xml file associates a user calendaring time zone (from either Microsoft Exchange or Lotus Domino) with a system time zone. In this case, the system time zone in the timezonemap.xml file is incorrect. However, this error should not impede a user from scheduling their meeting.

Recommendation

The administrator can optionally pursue this issue by collecting the log files, then contacting the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501225

Summary

Unresolved time zone mapping

Message

Unable to find a matching time zone target time zone definition ID '$1', descriptor '$2', definition '$3’

Module

Schedule management module API

Severity

Error

Explanation

The timezonemap.xml file associates a user calendaring time zone (from either Microsoft Exchange or Lotus Domino) with a system time zone. CTS-Manager could not recognize the user time zone passed from the calendaring application. However, this error should not impede a user from scheduling their meeting.

Recommendation

The administrator can optionally pursue this issue by collecting the log files, then contacting the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501227

Summary

Duplicate endpoint entries configured in Cisco UCM

Message

Duplicate endpoint entries found in Cisco Unified Call Manager

Module

Schedule management module API

Severity

Error

Explanation

Two Cisco TelePresence System (CTS) devices have the same email address configured in Cisco Unified CM.

Recommendation

The administrator can locate the duplicate email addresses in the Cisco Unified CM configuration, and change one of addresses, thereby making it unique.

501228

Summary

Invalid License. Upload valid license

Message

Invalid License

Module

Schedule management module API

Severity

Error

Explanation

The Scheduling API license currently uploaded in CTS-Manager is invalid.

Recommendation

The administrator should upload a valid Scheduling API license to CTS-Manager using the Configure > Licenses window.

501230

Summary

LDAP group was added from access management

Message

LDAP group [$1] was added to [$2] role from access management tab

Module

Schedule management module API

Severity

Informational

Explanation

The mapping between a role and an LDAP group was created in the Configure > Access Management window.

Recommendation

No action is required.

501231

Summary

LDAP group was deleted from access management tab

Message

LDAP group [$1] was deleted from [$2] role from access management tab

Module

Schedule management module API

Severity

Informational

Explanation

The mapping between a role and an LDAP group was deleted in the Configure > Access Management window.

Recommendation

No action is required.

501400

Summary

Failed to perform the given concierge operation

Message

Unable to '$1' concierge because $2

Module

Resource management module API

Severity

Error

Explanation

CTS-Manager did not allow the Live Desk properties to be edited or an endpoint to be assigned to a Live Desk user.

Recommendation

The administrator should restart the CTS-Manager service. If this condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501401

Summary

Failed to delete MCU

Message

This device has '$1' future meetings scheduled. Migrate the meetings to another device first

Module

Resource management module API

Severity

Error

Explanation

A selected conference bridge has the specified number of meetings scheduled, and therefore, cannot be deleted.

Recommendation

The administrator can move the meetings from the conference bridge that they intend to delete to another conference bridge, then retry the deletion.

501402

Summary

Duplicate host name or IP address for a TelePresence device

Message

Another device with host name or IP address '$1' already exists

Module

Resource management module API

Severity

Error

Explanation

A TelePresence device with the specified hostname or IP address already exists. This condition prevents the addition of a new TelePresence device with the specified hostname or IP address.

Recommendation

The administrator can verify the hostname or IP address of the new TelePresence device. If a conflict exists, they can use a different hostname or IP address, then retry adding the new device.

501403

Summary

Duplicate configuration entry

Message

Duplicate entry. '$1' already exists

Module

Resource management module API

Severity

Error

Explanation

The specified configuration entry already exists. This condition prevents the new entry from being added.

Recommendation

The administrator can verify the new entry. If a conflict exists, they can create a unique value, then retry the entry.

501405

Summary

Failed to enable Interoperability feature

Message

Cannot enable Interoperability support because $1

Module

Resource management module API

Severity

Error

Explanation

A meeting participant tried to enable the interoperability feature, but the attempt failed. A likely cause is that the Cisco TelePresence Engine server process is not running.

Recommendation

The administrator can verify the status of and try to restart the server process using CLI commands. If further assistance is needed, they can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501406

Summary

Failed to disable Interoperability feature

Message

Cannot disable Interoperability support because $1

Module

Resource management module API

Severity

Error

Explanation

A meeting participant attempted to disable the interoperability feature, but the attempt failed. A likely cause is that the Cisco TelePresence Engine server process is not running.

Recommendation

The administrator can verify the status of and try to restart the server process using CLI commands. If further assistance is needed, they can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501408

Summary

Failed to enable Interoperability feature

Message

Cannot enable Interoperability support because managed Cisco TelePresence Multipoint Switch is not Interoperability capable

Module

Resource management module API

Severity

Error

Explanation

The managed CTMS does not support video conferencing interoperability.

Recommendation

The administrator can upgrade the CTMS software to a version that supports interoperability with video conferencing.

501409

Summary

Failed to enable Interoperability feature

Message

Cannot enable Interoperability support because managed CTS and CTMS are not Interoperability capable

Module

Resource management module API

Severity

Error

Explanation

The managed CTS does not support video conferencing interoperability.

Recommendation

The administrator can upgrade the CTS software to a version that supports interoperability with video conferencing.

501410

Summary

Failed to disable Interoperability feature

Message

Cannot disable Interoperability support when there exists a video conferencing MCU

Module

Resource management module API

Severity

Error

Explanation

If a video conferencing conference bridge is configured in the system, CTS-Manager does not allow the the video conferencing interoperability feature to be disabled.

Recommendation

The administrator can delete the video conferencing conference bridge, then try to disable this feature.

501412

Summary

Groupware subscription failure

Message

Endpoint '$1' does not support Interoperability. Groupware subscription will be denied.

Module

Resource management module API

Severity

Error

Explanation

The video conferencing interoperability feature is enabled, but the managed CTS might be running an older software version that does not support this feature. This condition prevents the groupware subscription from being configured.

Recommendation

The administrator can upgrade the CTS to a software version that supports interoperability with video conferencing.

501414

Summary

Groupware subscription failure

Message

More than one endpoint '$1' exists in managed state. Groupware subscription will be denied.

Module

Resource management module API

Severity

Critical

Explanation

Two endpoints have the same email ID, and as a result, CTS-Manager will not subscribe meeting events to these endpoints.

Recommendation

The administrator should rename one of the duplicate email IDs.

501415

Summary

Groupware subscription failure

Message

Endpoint '$1' not found in the system. Groupware subscription will be denied.

Module

Resource management module API

Severity

Error

Explanation

The system could not find the endpoint (room) in the Unified CM application profile because it was not configured or was misspelled.

Recommendation

The administrator can check the endpoint (room) configuration in the Unified CM application profile.

501416

Summary

Groupware subscription failure

Message

No telepresence device found for endpoint '$1'.

Module

Resource management module API

Severity

Error

Explanation

This message can appear if the TelePresence device does not have a valid license.

Recommendation

Go to Support > Endpoints. If the Licensed column displays a green check mark, the endpoint has a valid license. If the endpoint does not have a valid license, see the "Licensing for CTS-Manager" section on page 11-6 for complete information on obtaining and uploading licenses into CTS-Manager.

501417

Summary

Groupware subscription failure

Message

Endpoint '$1' does not support studio mode recording. Groupware subscription will be denied.

Module

Resource management module API

Severity

Error

Explanation

The studio mode recording feature is enabled, but the managed CTS might be running an older software version that does not support this feature. This condition prevents the groupware subscription from being configured.

Recommendation

The administrator can upgrade the CTS to a software version that supports studio mode recording.

501418

Summary

Groupware subscription failure

Message

Endpoint '$1' does not support HD Interoperability. Groupware subscription will be denied

Module

Resource management module API

Severity

Error

Explanation

The HD interoperability feature is enabled, but the managed CTS might be running an older software version that does not support this feature. This condition prevents the groupware subscription from being configured.

Recommendation

The administrator can upgrade the CTS to a software version that supports HD interoperability with video conferencing.

501419

Summary

Groupware subscription failure

Message

Enpdoint '$1' does not support WebEx. Groupware subscription will be denied

Module

Resource management module API

Severity

Error

Explanation

The Cisco WebEx feature is enabled, but the managed CTS might be running an older software version that does not support this feature. This condition prevents the groupware subscription from being configured.

Recommendation

The administrator can upgrade the CTS to a software version that supports Cisco WebEx.

501430

Summary

Email address not recognized

Message

The email address in the entry ['$1'] is invalid in the LDAP server or the calendar server

Module

Resource management module API

Severity

Error

Explanation

The email address provided for a video conferencing (VC) endpoint import is not present in the LDAP or calendar database.

Recommendation

The administrator can take the following action:

- Verify that the email address in the entry is correct.
- Verify that the associated user is in the LDAP and calendar databases.
- Reimport the device.

501431

Summary

Unknown error when importing Video Conferencing endpoints

Message

Encountered an unknown error when importing the entry ['$1']

Module

Resource management module API

Severity

Error

Explanation

When trying to import a video conferencing (VC) endpoint into CTS-Manager, an unknown error occurred.

Recommendation

The administrator can check the video conference endpoint file to ensure the information included therein is correct, then try to reimport the file.

501432

Summary

An earlier entry with the same email exists

Message

A duplicate email was encountered when parsing the entry ['$1']

Module

Resource management module API

Severity

Error

Explanation

A duplicate email address was detected in the video conferencing (VC) endpoint import, and as a result, the entry could not be processed.

Recommendation

The administrator should rename one of the duplicate email addresses.

501433

Summary

Email conflicts with an existing TelePresence endpoint.

Message

An existing TelePresence endpoint has the same email as the entry ['$1'].

Module

Resource management module API.

Severity

Error

Explanation

When importing a video conferencing (VC) endpoint, CTS-Manager detected an existing endpoint with the same email address.

Recommendation

The administrator should use a unique email address for the VC endpoint.

501434

Summary

Attempting to change Video Conferencing endpoint segment

Message

Changing segment is not allowed: the Video Conferencing endpoint already exits, and has a different segment from the entry ['$1']

Module

Resource management module API

Severity

Error

Explanation

When importing a video conferencing (VC) endpoints, CTS-Manager detected that the specified email address already exists. Instead of specifying a new email address, the administrator retained the same email address and changed the segment count.

Recommendation

The administrator must specify a new email address.

501435

Summary

Invalid video conferencing endpoint data

Message

Encountered an error when parsing the entry ['$1']. Please make sure the email, segment, IP, and phone number are all valid

Module

Resource management module API

Severity

Error

Explanation

When importing a video conferencing (VC) endpoint, CTS-Manager detected that the text file format was incorrect. The file must include a comma as a delimiter and the columns must be organized in the following order:

- Email
- Segment count
- IP address
- Phone number

Recommendation

The administrator should check the file to ensure that it adheres to the following format:

- Uses a comma as the delimiter.
- From left to right, the columns appear in the following order:
  - Email
  - Segment count
  - IP address
  - Phone number

501436

Summary

Interop quality selection not supported by the endpoints and conference bridges

Message

Cannot enable $1 because one or more endpoints or CTMS devices are not compatible with $2

Module

Resource management module API

Severity

Error

Explanation

After enabling the interoperability with video conferencing feature, an interoperability quality option that was not supported by all TelePresence devices was selected.

Recommendation

The administrator should check the Bridge and Servers tab, which is available in the Configure > Application Settings window, to identify the supported quality options.

501601

Summary

Unable to authenticate user

Message

Unable to authenticate user. Check authentication parameters

Module

Security management module API

Severity

Error

Explanation

A user tried to log into the CTS-Manager Administration UI but could not because CTS-Manager could not authenticate them.

Recommendation

The user should check their username and password, then retry their login.

501602

Summary

Unsupported authentication type

Message

Authentication type '$1' is not supported

Module

Security management module API

Severity

Error

Explanation

The indicated authentication type that was specified during configuration, for example, for LDAP to be authenticated against the directory server, is not supported.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501603

Summary

Unable to encrypt data

Message

Unable to encrypt data because $1

Module

Security management module API

Severity

Error

Explanation

A problem occurred while encrypting a string.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501604

Summary

Unable to decrypt data

Message

Unable to decrypt data. Possible causes: incorrect password or corrupted file. Correct the required information and try again

Module

Security management module API

Severity

Error

Explanation

A problem occurred while decrypting a string.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501605

Summary

Insufficient credential for authentication

Message

Insufficient credential '$1'. Requires credential '$2'

Module

Security management module API

Severity

Error

Explanation

A user tried to perform an unauthorized operation.

Recommendation

If appropriate, the user can work with the administrator to obtain the needed privilege level.

501606

Summary

Incorrect credential for authentication

Message

Access permitted to email ID '$1' only

Module

Security management module API

Severity

Error

Explanation

The meeting organizer only can access the URL provided in the automated emails sent by CTS-Manager. All other users who try to access the URL will be denied.

Recommendation

The meeting organizer only can access the provided URL.

501607

Summary

Password is not secure

Message

New password is too simple. Password should contain both mixed-case alphabetic and non-alphabetic characters. It should not be similar to the current password. It should not base on common words found in dictionary

Module

Security management module API

Severity

Error

Explanation

A CTS-Manager Administration UI user attempts to change the password for a SysAdmin account, and the new password does not meet the guidelines.

Recommendation

The user must specify a password that meets the following guidelines:

- Contain both mixed-case alphabetic and non-alphabetic characters.
- Not be similar to the current password.
- Not be based on common words found in the dictionary.

501608

Summary

Could not save the new password

Message

Password was change successfully, but could not be saved for future upgrade

Module

Security management module API

Severity

Error

Explanation

An internal error occurred and as a result, a new password could not be saved to platformConfig.xml.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501609

Summary

Failed to change password

Message

Unable to change password because current password does not match

Module

Security management module API

Severity

Error

Explanation

While changing their password, a CTS-Manager Administration UI user entered their current password incorrectly, and as a result, the new password could not be processed.

Recommendation

The user should reenter their current password.

501610

Summary

The certificate expiry warning

Message

'$1'. Certificate name '$2'. Unit '$3'. Type '$4'. Expiration: '$5'

Module

Security management module API

Severity

Warning

Explanation

A security certificate for the specified component will expire soon.

Recommendation

The administrator should upload a new certificate for the specified component. For more information on uploading a security certificate in CTS-Manager, see the "Security" section on page 11-13.

501611

Summary

Unable to find user in LDAP directory

Message

Unable to find user '$1' in LDAP directory

Module

Security management module API

Severity

Error

Explanation

This message can appear under the following conditions:

- A user tried to log into the CTS-Manager Administration UI but CTS-Manager could not find this user in the LDAP directory.
- In the Edit... LDAP Servers window, an administrator entered an email address in the Email Address field, then clicked **View Sample Data** but CTS-Manager could not find this user in the LDAP directory.

Recommendation

The user should verify their login credentials. If the problem persists, the user can contact the administrator to verify their credentials.

501612

Summary

Unable to authenticate user

Message

Invalid username or password. Please try again

Module

Security management module API

Severity

Error

Explanation

The CTS-Manager system administrator account credentials, which are managed by Microsoft Exchange, are invalid.

Recommendation

The administrator should verify their account credentials, then reenter the correct username and password.

501613

Summary

Unable to authenticate user

Message

Invalid username or password. Please try again

Module

Security management module API

Severity

Error

Explanation

The CTS-Manager system administrator account credentials, which are managed by IBM Domino, are invalid.

Recommendation

The administrator should verify their account credentials, then reenter the correct username and password.

501614

Summary

Unable to calculate check sum

Message

Unable to calculate check sum for file '$1' because $2

Module

Security management module API

Severity

Error

Explanation

The checksum could not be calculated for the specified file.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501615

Summary

Insufficient privilege

Message

Not enough privilege to perform the operation

Module

Security management module API

Severity

Error

Explanation

A user tried to access the CTS-Manager Reporting API but one of the following conditions existed:

- The user did not have the appropriate permission to access the Reporting API.
- A license required to access the Reporting API functionality has not been uploaded to CTS-Manager, or the license is invalid.

Recommendation

The administrator should take this action:

- If the user does not have the appropriate permission:
  - Work with the LDAP administrator to ensure that a user group for the Reporting API client user accounts exists on the LDAP server and that within this group, one or more user accounts for the Reporting API client exists.
  - In the Configure > Access Management window, ensure that the “Reporting API User” role is mapped to the LDAP user group that contains the Reporting API client user accounts.
  - Ensure that the user has the correct user account information.
- Ensure that the Reporting API license is uploaded in CTS-Manager and that the license is valid.

501616

Summary

mismatch admin user credential between joining node and primary node

Message

Joining node must have same admin user credential as the primary node

Module

Security management module API

Severity

Error

Explanation

The administrator tried to log into the joining node with the same account credentials as the primary node but was denied access because the joining node has different account credentials.

Recommendation

The administrator can modify the administrator account credentials for the joining node so that they match those for the primary node.

501617

Summary

Insufficient credential for authentication

Message

Invalid username or password. Please try again

Module

Security management module API

Severity

Error

Explanation

A user tried to log into the CTS-Manager Administration UI without providing a username, a password, or both.

Recommendation

If needed, the user should obtain the proper login credentials from the administrator, then retry their login. When logging in, the user must provide both username and password.

501618

Summary

Unable to login user due to max limit reached

Message

System is currently busy. Please try again later or contact your help desk

Module

Security management module API

Severity

Error

Explanation

A user tried to log into CTS-Manager but was denied access because a maximum number of users was already logged in.

Recommendation

The user should retry their login later or if the condition persists, contact the Live Desk.

501700

Summary

Incorrect configuration data

Message

Missing or unknown configuration component '$1'

Module

Administrative management module API

Severity

Error

Explanation

The configuration of the specified component is missing or does not exist.

Recommendation

The administrator can verify that the initial configuration setup has been performed and all values are properly specified.

501701

Summary

Incorrect configuration data

Message

Configuration component '$2' is missing parameter '$1'

Module

Administrative management module API

Severity

Error

Explanation

The specified component is missing the specified parameter.

Recommendation

The administrator can verify that the initial configuration setup has been performed and all values are properly specified.

501702

Summary

Unable to set configuration data

Message

Unable to set configuration parameter '$1' to value '$2' because $3

Module

Administrative management module API

Severity

Error

Explanation

CTS-Manager could not save the value of the specified parameter.

Recommendation

The administrator can check the DB component status using the **utils service list** command, and restart the service manager if needed.

501703

Summary

Unable to update schedule for endpoints

Message

Unable to update schedule for endpoints '$1' because $2

Module

Administrative management module API

Severity

Error

Explanation

CTS-Manager could not submit a schedule update request to the specified endpoints.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501704

Summary

Application data store run time error

Message

Unable to validate distinguished name

Module

Administrative management module API

Severity

Error

Explanation

CTS-Manager could not validate a distinguished name (DN) in the LDAP directory.

Recommendation

The administrator can check the DN configuration to make sure it is set up properly. If the problem persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501705

Summary

Unable to find user in the directory

Message

Unable to find user in the directory. Email address '$1' is invalid. Check the email parameter. Only one email address is allowed

Module

Administrative management module API

Severity

Error

Explanation

The directory was searched but the indicated email address was not found. As a result, the user could not be authenticated.

Recommendation

The administrator should verify that the email address is correct.

501901

Summary

Unable to authenticate the CTS device

Message

Unable to authenticate the CTS device

Module

Calendar generator module

Severity

Error

Explanation

The username and password specified for the CTS device do not match the login credentials.

Recommendation

The administrator can verify the configuration of the CTS device in the Cisco UCM application profile.

501902

Summary

Failed to push meeting calendar to CTS

Message

Unable to push calendar to the device '$1'

Module

Calendar generator module

Severity

Critical

Explanation

Calendar updates could not be propagated to the indicated CTS device.

Recommendation

The administrator should verify that the CTS device is registered with Cisco Unified CM. If the device is not registered, the administrator should contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

501903

Summary

Communication to CTS failure

Message

No communication link to CTS '$1

Module

Calendar generator module

Severity

Critical

Explanation

The indicated CTS device is not running, or the device has lost network connectivity.

Recommendation

The administrator should take the following action:

- Ensure that the CTS device is up and running.
- Ensure that the CTS device is reachable via the network.

501904

Summary

Application data store run time error

Message

Unable to update the SSH username/password from DB into cache because $1

Module

Calendar generator module

Severity

Critical

Explanation

The SSH username and password could not be retrieved from the DB, and as a result, they could not be updated.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502000

Summary

Application data store run time error

Message

Data access error: $1

Module

Data access

Severity

Error

Explanation

The indicated data access error occurred.

Recommendation

The administrator can verify that the database is up and running. If more assistance is needed, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502001

Summary

Application data store run time error

Message

Unable to parse meta schema file because $1

Module

Data access

Severity

Error

Explanation

An error occurred while parsing the metaschema file.

Recommendation

The administrator can verify that the installation and initial configuration has completed successfully. If more assistance is needed, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502002

Summary

Application data store run time

Message

Unable to load metaschema file '$1' because $2

Module

Data access

Severity

Error

Explanation

The metaschema file could not be loaded.

Recommendation

The administrator can take the following action:

- Verify that the installation and initial configuration was successfully completed.
- Verify that the disk is not corrupted.

If more assistance is needed, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502003

Summary

Application data store run time error

Message

Data store '$1' is not found in metaschema file

Module

Data access

Severity

Error

Explanation

The metaschema file might include an incorrect datastore value, which prevents the system from locating the datastore.

Recommendation

The administrator can verify that the installation and initial configuration was successfully completed. If more assistance is needed, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502004

Summary

Application data store run time error

Message

Unable to update metaschema file '$1' because $2

Module

Data access

Severity

Error

Explanation

The metaschema file might include an incorrect datastore value, which prevents the file from being updated and saved.

Recommendation

The administrator can take the following action:

- Verify that the installation and initial configuration has completed successfully.
- Verify that the values specified in the Field Mappings window are valid.

If more assistance is needed, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502005

Summary

Application data store run time error

Message

Data access initialization error: $1

Module

Data access

Severity

Error

Explanation

An error occurred during the initialization of the data access plug-ins.

Recommendation

The administrator can troubleshoot these areas:

- Database
- LDAP connectivity
- Initial setup

If more assistance is needed, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502006

Summary

Application data store run time error

Message

Unable to create database object because $1

Module

Data access

Severity

Error

Explanation

An error occurred while creating an object in the database.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502007

Summary

Application data store run time error

Message

Unable to write to database because $1

Module

Data access

Severity

Error

Explanation

An error occurred while updating an object in the database.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502008

Summary

Application data store run time error

Message

Unable to delete from database because $1

Module

Data access

Severity

Error

Explanation

An error occurred while deleting an object from the database.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502009

Summary

Application data store run time error

Message

Unable to get object because $1

Module

Data access

Severity

Error

Explanation

An error occurred while retrieving an object from the database.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502010

Summary

Application data store run time error

Message

Specified object '$1' not found in '$2' data store

Module

Data access

Severity

Error

Explanation

The specified object does not exist in the directory server.

Recommendation

The administrator can take the following action:

- Check the LDAP user container.
- Verify the LDAP content using an LDAP browser.

502011

Summary

Application data store run time error

Message

Invalid parameter specified '$1'

Module

Data access

Severity

Error

Explanation

The specified parameter is not valid.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502012

Summary

Error in purging database data during maintenance

Message

Unable to purge data because $1

Module

Data access

Severity

Error

Explanation

An error occurred while data was purged from the database during a regularly scheduled maintenance session.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502013

Summary

Data backup failure

Message

Unable to backup data because $1

Module

Data access

Severity

Critical

Explanation

The indicated error occurred during a data backup.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502014

Summary

Data restore failure

Message

Unable to restore data because $1

Module

Data access

Severity

Critical

Explanation

An error occurred while data was being restored.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502015

Summary

Unable to perform DB maintenance operations

Message

Unable to perform DB maintenance operations because $1

Module

Data access

Severity

Error

Explanation

An error occurred during a database backup, purge, or restore.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502016

Summary

DB maintenance operation failure

Message

Maintenance process returns code '$1'

Module

Data access

Severity

Error

Explanation

An error occurred during a database backup, purge, or restore.

Recommendation

The administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502017

Summary

Application data store run time error

Message

Unable to acquire connection to component '$1'

Module

Data access

Severity

Error

Explanation

An error occurred when getting a connection from the connection pool.

Recommendation

The administrator can take this action:

- Check the connection type (DB/LDAP).
- Verify the connectivity to the component.
- Restart the server.

If this condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502018

Summary

Application data store run time error

Message

Unable to close connection to component '$1'

Module

Data access

Severity

Error

Explanation

An error occurred when closing a connection from the connection pool.

Recommendation

The administrator can take this action:

- Check the connection type (DB/LDAP).
- Verify the connectivity to the component.

- Restart the server.

If this condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502019

Summary

Application data store run time error

Message

Unable to close JDBC statement because $1

Module

Data access

Severity

Error

Explanation

An error occurred when closing a Java Database Connectivity (JDBC) Structured Query Language (SQL) statement object.

Recommendation

The administrator can check to make sure that the database is running.

502020

Summary

Application data store runtime error

Message

Unable to instantiate class '$1’

Module

Data access

Severity

Error

Explanation

An error occurred when using pluggable methods during data access operations.

Recommendation

The administrator should verify that the installation and initial setup was properly completed. If this condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502021

Summary

Application data store run time error

Message

Unable to instantiate method '$1' of class '$2'

Module

Data access

Severity

Error

Explanation

An error occurred when using pluggable methods during data access operations.

Recommendation

The administrator should verify that the installation and initial setup was properly completed. If this condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502022

Summary

Application data store run time error

Message

Unable to retrieve field '$1' of class '$2'

Module

Data access

Severity

Error

Explanation

An error occurred when using pluggable methods during data access operations.

Recommendation

The administrator should verify that the installation and initial setup was properly completed. If this condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502023

Summary

Application data store run time error

Message

Unable to set value for field '$1' of class '$2'

Module

Data access

Severity

Error

Explanation

An error occurred when using pluggable methods during data access operations.

Recommendation

The administrator should verify that the installation and initial setup was properly completed. If this condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502024

Summary

Application data store run time error

Message

Object '$1' is already deleted

Module

Data access

Severity

Error

Explanation

An object to be deleted was already deleted.

Recommendation

If this condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502025

Summary

Application data store run time error

Message

Object handler not found for object '$1'

Module

Data access

Severity

Error

Explanation

The object handler for data access operations is not found.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502027

Summary

Application data store run time error

Message

Object attribute '$1' was not retrieved

Module

Data access

Severity

Error

Explanation

The requested attribute was not found in the object because the application did not retrieve all the attributes for the object or the correct attribute name was not used.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502028

Summary

Database is in maintenance cycle

Message

Database under maintenance: restore is in progress

Module

Data access

Severity

Notice

Explanation

A database operation was requested but not executed because the database is currently being restored.

Recommendation

The administrator can resubmit the request after the restoration of the database is completed.

502029

Summary

Application data store run time error

Message

Unknown predefined query named '$1'

Module

Data access

Severity

Error

Explanation

The indicated query was requested but could not be executed because the predefined query name was unknown.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502100

Summary
LDAP connection failure

Message
Unable to connect to LDAP Server '$1'

Module
LDAP

Severity
Alert

Explanation
CTS-Manager could not communicate with the indicated LDAP server.

Recommendation
The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502101

Summary
LDAP operation failure

Message
Unable to retrieve object '$1'

Module
LDAP

Severity
Critical

Explanation
CTS-Manager was not able to obtain the directory entry indicated in the system message.

Recommendation
The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502102

Summary
LDAP authentication failure

Message
Unable to authenticate to LDAP Server

Module
LDAP

Severity
Alert

Explanation
CTS-Manager could not authenticate the indicated LDAP server.

Recommendation
The administrator should verify that the LDAP parameters are properly configured.

502301

Summary
Application run time operation failure

Message
Unknown resource object interface '$1'

Module
API layer

Severity
Critical

Explanation
The specified object is no longer accessible.

Recommendation
The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502302

Summary

Application run time operation failure

Message

The parameter '$1' has invalid value '$2'

Module

API layer

Severity

Error

Explanation

The indicated parameter has the indicated invalid value.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502400

Summary

Unable to connect to Unified CM

Message

Unable to connect to Unified CM '$1' because $2'

Module

Discovery manager

Severity

Alert

Explanation

CTS-Manager could not connect with Unified CM for the indicated reason, and as a result, information from Unified CM could not be retrieved.

Recommendation

The CTS-Manager administrator should work with the network administrator to check the network connectivity with Unified CM.

502401

Summary

Authentication to Unified CM failure

Message

Unable to authenticate into Unified CM '$1' because $2

Module

Discovery manager'

Severity

Alert

Explanation

A digital certificate for Unified CM was not found in the CTS-Manager Security Keystore.

Recommendation

The administrator should upload a digital certificate for Unified CM.

502402

Summary

Unable to locate phone attached to CTS device

Message

Unable to locate phone attached to CTS device '$1''

Module

Discovery manager

Severity

Error

Explanation

An IP phone is not configured for the shared line with the indicated CTS device.

Recommendation

The administrator should configure the shared line with an IP phone.

502403

Summary

Unable to locate endpoint information attached to TelePresence equipment

Message

Unable to locate endpoint information attached to TelePresence equipment '$1''

Module

Discovery manager

Severity

Error

Explanation

Endpoint information for the indicated CTS device is missing.

Recommendation

The administrator should verify that the endpoint (room) information exists in Unified CM.

502404

Summary

Unified CM communication failure

Message

Unable to send AXL message to Unified CM '$1' because $2'

Module

Discovery manager

Severity

Alert

Explanation

CTS-Manager could not send an Administrative XML (AXL) request to Unified CM.

Recommendation

The administrator should take the following action:

- Work with the network administrator to verify connectivity between CTS-Manager and Unified CM.
- Ensure that the correct digital certificate for Unified CM is uploaded.
- Ensure that the credentials specified for the Unified CM Application user are correct.

502405

Summary

Unified CM data retrieving failure

Message

Unable to retrieve publisher and/or secondary servers from Unified CM '$1' because $2'

Module

Discovery manager

Severity

Critical

Explanation

The Unified CM node information could not be retrieved from the database.

Recommendation

The administrator should take this action:

- Check the *Software Compatibility Information for the Cisco TelePresence System* to ensure that the CTS-Manager and Unified CM software are compatible.
- Ensure that the specified node is a Unified CM Publisher node.

502406

Summary

Unable to authenticate and connect with Unified CM

Message

Unable to authenticate and connect with Unified CM '$1' because $2

Module

Discovery manager

Severity

Error

Explanation

The Unified CM server could not be authenticated because of invalid credentials and/or hostname were specified.

Recommendation

The administrator should verify the Unified CM App User credentials and Publisher node configuration.

502407

Summary

Communication to Unified CM failure

Message

Unable to create CTI adapter to Unified CM '$1' because $2

Module

Discovery manager

Severity

Critical

Explanation

The Unified CM server could not be authenticated because of an issue with Cisco CTIManager.

Recommendation

The administrator should take this action:

- Verify the Unified CM App User credentials.
- Verify that the Cisco CTIManager service is activated on the Unified CM Publisher node.

502409

Summary

CTS data store operation failure

Message

Unable to create or update TelePresence equipment '$1' because $2'

Module

Discovery manager

Severity

Critical

Explanation

The configuration for the specified CTS device could not be created in the database.

Recommendation

The administrator should ensure that the directory number (DN) for the specified CTS device is configured.

502411

Summary

CTI manager on Unified CM is down

Message

CTI manager on node '$1' is down message received for the Unified CM '$2"

Module

Discovery manager

Severity

Critical

Explanation

The Cisco CTIManager provider instance could not be created.

Recommendation

The administrator should restart the Cisco CTIManager on Unified CM.

502415

Summary

Unified CM communication failure

Message

Unable to connect to RIS manager on Unified CM '$1"

Module

Discovery manager

Severity

Alert

Explanation

A connection could not be made with the Real-Time Information Service (RIS) manager on the Unified CM server.

Recommendation

The administrator should check the Unified CM status to ensure that the RIS manager is functioning.

502418

Summary
Cisco UCM CTI provider in error state

Message
Unable to get list of addresses from CTI provider '$1"

Module
Discovery manager

Severity
Error

Explanation
The Unified CM CTI provider is in an error state.

Recommendation
The administrator should collect the Unified CM log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502419

Summary
Failed to get CTS IP addresses

Message
Unable to retrieve IP addresses for devices from Unified CM '$1' because $2'

Module
Discovery manager

Severity
Error

Explanation
The Unified CM Real-Time Information Service (RIS) web service is not running.

Recommendation
The administrator should activate the Simple Object Access Protocol (SOAP) web service.

502420

Summary

Failed to communicate with Cisco UCM

Message

Unable to discover TelePresence equipment from Unified CM '$1'

Module

Discovery manager

Severity

Error

Explanation

One of the Unified CM interfaces is down.

Recommendation

The administrator should collect the Unified CM log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502422

Summary

CTS configuration mismatching

Message

Directory number is not configured for device '$1"

Module

Discovery manager

Severity

Critical

Explanation

The directory number (DN) for the specified CTS device is not configured.

Recommendation

The administrator should configure the DN for the specified CTS device.

502423

Summary
Unified CM version not supported

Message
Unified CM version '$1' is not supported for Unified CM '$2"

Module
Discovery manager

Severity
Critical

Explanation
The Unified CM software version is not compatible with the CTS-Manager software version.

Recommendation
The administrator should refer to the *Software Compatibility Information for the Cisco TelePresence System* to determine the Unified CM and CTS-Manager software versions that are compatible and upgrade the software accordingly.

502424

Summary
Scheduled maintenance operation failure

Message
Scheduled maintenance operation '$1' encountered an unexpected condition'

Module
Discovery manager

Severity
Critical

Explanation
The system was unable to execute one of these operations:

- A scheduled maintenance for the database
- The discovery of a CTS device
- A Microsoft Exchange synchronization
- The pushing of calendar schedules

Recommendation
The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502425

Summary

Unified CM data retrieving failure

Message

Unable to discover time zone information from Unified CM '$1"

Module

Discovery manager

Severity

Error

Explanation

Time zone information was not configured or is not available in Unified CM.

Recommendation

If not already configured, the administrator should set up the time zone attributes in Unified CM. If this action does not resolve the issue, the administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502426

Summary

Unable to discover TelePresence capability information from end-points

Message

Unable to discover TelePresence capability information from end-points'

Module

Discovery manager

Severity

Error

Explanation

The system was unable to discover capability information from a CTS endpoint. The most likely cause of this issue is an older version of the CTS device, which does not support capability information.

Recommendation

The administrator should check the version of the CTS device and if needed, upgrade the device to a version that supports capability information.

502427

Summary

CTS misconfigured in Unified CM

Message

More than one IP Phone configured on shared DN with TelePresence equipment '$1"

Module

Discovery manager

Severity

Error

Explanation

In the Unified CM configuration, more than one IP phone is configured to share the same directory number (DN) as the specified CTS endpoint.

Recommendation

The administrator should check the CTS configuration in Unified CM and take one of these actions:

- Remove the extraneous IP phone(s) that share the same DN.
- Assign a new DN for each of the extraneous IP phone(s) so that the CTS endpoint has only one IP phone sharing the DN.

502428

Summary

CTI control disabled

Message

CTI control is disabled on the IP phone '$1"

Module

Discovery manager

Severity

Critical

Explanation

The specified Cisco IP Phone, which is configured for the CTS endpoint, has the CTI control set to disabled.

Recommendation

The administrator should check the configuration of the IP phone in the Unified CM Administration user interface and make sure CTI control is enabled.

502429

Summary

Failed to update Unified CM time zone in data store

Message

Unable to update time zone '$1' because $2'

Module

Discovery manager

Severity

Error

Explanation

An internal server error occurred.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502430

Summary

Insufficient CTS capability

Message

CTS device '$1' does not Interop with SD/HD VC end points. Check capability for details'

Module

Discovery manager

Severity

Error

Explanation

The indicated CTS does not support video conferencing interoperability.

Recommendation

The administrator should upgrade the CTS to a version that supports interoperability with video conferencing.

502432

Summary

Discovery complete for the specified unified CM profile

Message

Discovery completed for Unified CM '$1"

Module

Discovery manager

Severity

Informational

Explanation

The specified Unified CM profile was discovered.

Recommendation

No action is required.

502434

Summary

Endpoint discovery operation error

Message

Unable to parse AXL Throttling fault string - $1'

Module

Discovery manager

Severity

Error

Explanation

CTS-Manager received an Administrative XML (AXL) fault from Unified CM but was unable to extract information because of a malformed fault string or formatting error.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502435

Summary

Duplicate email address found for endpoints in Unified CM profile.

Message

Duplicate email address found for endpoint '$1''.

Module

Discovery manager

Severity

Error

Explanation

A duplicate email address for an indicated endpoint was found in a Unified CM profile.

Recommendation

The administrator should remove the duplicate email address(es) for the endpoint (room) in the Unified CM profile.

502436

Summary

Duplicate email address of a endpoint in Unified CM profile cleared.

Message

Endpoint duplicate email address cleared for endpoint '$1''.

Module

Discovery manager

Severity

Informational

Explanation

A duplicate email address for the indicated endpoint (room) was removed from the Unified CM profile.

Recommendation

No action is required.

502437

Summary

There are no endpoint licenses available

Message

There are no endpoint licenses available

Module

Discovery manager

Severity

Critical

Explanation

A valid endpoint license has not been uploaded to CTS-Manager via the Configure > Licenses window. Without this license, configured endpoints will not be recognized by CTS-Manager and meeting organizers will not be able to schedule meetings.

Recommendation

The administrator should acquire and upload a valid endpoint license. For information on performing these tasks, see "Licensing for CTS-Manager" section on page 11-6.

502438

Summary

Endpoints licenses are in grace period

Message

Endpoints licenses are in grace period.'

Module

Discovery manager

Severity

Informational

Explanation

The endpoint licenses are in a grace period. Before the licenses expire, which would cause the associated CTS endpoints to become nonfunctional, new licenses must be acquired.

Recommendation

The administrator should acquire and upload valid endpoint licenses. For information on performing these tasks, see "Licensing for CTS-Manager" section on page 11-6.

502439

Summary

There are not enough endpoint licenses available.

Message

There are not enough endpoint licenses available.'

Module

Discovery manager

Severity

Critical

Explanation

The number of endpoint licenses uploaded to CTS-Manager is not sufficient to cover the available endpoints. As a result, some endpoints are nonfunctional.

Recommendation

The administrator should acquire and upload endpoint licenses for the unlicensed endpoints. For information on performing these tasks, see "Licensing for CTS-Manager" section on page 11-6.

502440

Summary

Device ID of an endpoint gets updated by another Device ID. Possible endpoint email address duplication in Unified CM profile

Message

Device ID '$1' is replaced by Device ID $2'

Module

Discovery manager

Severity

Warning

Explanation

The device ID of an endpoint was updated by another device ID. The likely cause are duplications in the email addresses of the rooms (endpoints) in the Unified CM profile.

Recommendation

The administrator should check the Unified CM profile to determine if there are duplications in the email addresses of the endpoints. If duplicates exist, the administrator should remove them.

502500

Summary

Event system operation failure

Message

Unable to dispatch message/event because $1

Module

Event subsystem

Severity

Alert

Explanation

The ActiveMQ message system is unable to dispatch a message or event.

Recommendation

The administrator should check the state of the event service using the **utils service list** CLI command, then take the following action:

- If the event service is not running, the administrator should start it using the **utils service start** CLI command.
- If the event service is running, we recommend stopping it using the **utils service stop** CLI command then restarting it using **utils service start** CLI command.
- If the issue persists after taking the recommended action, the administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502601

Summary

Admin UI unable to retrieve meeting

Message

Your meeting ID '$1' has been removed from the system. Please contact your help desk for assistance.'

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to extract details for the indicated meeting because the meeting organizer ID or the meeting serial ID is null.

Recommendation

The meeting organizer should check the URL provided in their email notification. The URL cannot be altered.

502602

Summary

Admin UI unable to get certificate configuration file

Message

Unable to get certificate configuration file '$1"

Module

UI module

Severity

Error

Explanation

The cert-conf.xml file is not in the expected location. A problem could have occurred during installation.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502603

Summary

Admin UI certificate operation failure

Message

Unable to load certificate because $1'

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to load the indicated certificate into the system.

Recommendation

The administrator should note the details provided by the “$1” variable in “Message,” and retry the certificate upload to CTS-Manager.

502604

Summary

Admin UI certificate operation failure

Message

Unable to delete certificate unit '$1' of category '$2' because $3'

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to delete the indicated certificate because of the indicated issue.

Recommendation

The administrator should note the details provided by the “$3” variable in “Message,” and retry the certificate upload to CTS-Manager.

502605

Summary

Admin UI network operation failure

Message

Unable to $1 DHCP setting (CLI code '$2')'

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to enable or disable the DHCP setting.

Recommendation

The administrator should note the details provided by the “$2” variable in “Message,” and retry the configuration of the DHCP attribute.

502606

Summary

Admin UI network operation failure

Message

Unable to set IP address and/or subnet mask (CLI code '$1')'

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to save the configuration of a new IP address and/or subnet mask.

Recommendation

The administrator should note the details provided by the “$1” variable in “Message,” and retry the configuration of the IP address attributes.

502607

Summary

Admin UI network operation failure

Message

Unable to set default gateway (CLI code '$1')'

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to change default gateway setting.

Recommendation

The administrator should note the details provided by the “$1” variable in “Message,” and retry the configuration of the default gateway attribute.

502608

Summary

Admin UI SNMP operation failure

Message

Unable to set SNMP data command executed '$1' because $2'

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to execute the SNMP setting script to set new values for SNMP attributes.

Recommendation

The administrator should note the details provided by the “$2” variable in “Message,” and retry the execution of the SNMP setting script.

502609

Summary

Admin UI SNMP operation failure

Message

Unable to '$1' SNMP service because $2'

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to perform the indicated action because the SNMP service was deactivated.

Recommendation

The administrator should use the CTS-Manager CLI to restart the SNMP service. (To verify the status of the SNMP service, the administrator should enter the **utils service list** command. If the SNMP service is not running, the administrator can enter the **utils service restart** *service-name* command, where *service-name* is the name of the SNMP service, which the administrator can get from the output of the **utils service list** command.)

502610

Summary

Software upgrade already in progress

Message

Software upgrade already in progress

Module

UI module

Severity

Warning

Explanation

A software upgrade is attempted while another upgrade is in progress. Only one upgrade can take place at a time.

Recommendation

The administrator who is attempting the upgrade should wait until the in-progress upgrade is completed, then retry their upgrade.

502611

Summary

Software upgrade failure from Admin UI

Message

Unable to upgrade software because $1

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to upgrade the software because of the indicated reason.

Recommendation

The administrator should note the details provided by the “$1” variable in “Message,” and retry the upgrade.

502612

Summary
System is restarting

Message
System is restarting. Try again later.

Module
UI module

Severity
Warning

Explanation
The system is being restarted. Users are not allowed to log into the CTS-Manager Administration UI during the startup process.

Recommendation
The CTS-Manager Administration UI users must wait until the startup process is complete.

502613

Summary
Admin UI operation error

Message
Webapp home directory '$1' does not exist

Module
UI module

Severity
Error

Explanation
The indicated webapp home directory does not exist. It was probably not created during installation.

Recommendation
The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502614

Summary

System is being maintained

Message

System is being maintained. Try again later

Module

UI module

Severity

Warning

Explanation

Either a database restore or system restart is in progress. During these processes, users are not allowed to log into the CTS-Manager Administration UI, and this system message is displayed on the CTS-Manager Administration login window.

Recommendation

The CTS-Manager Administration UI users must wait until the system maintenance process is complete.

502615

Summary

Users cannot delete his own role mapping

Message

Cannot delete own role mapping '$1'

Module

UI module

Severity

Notice

Explanation

A CTS-Manager user whose role is Administrator is trying to delete the Administrator role mapping in the Configure > Access Management window. CTS-Manager users cannot delete their own role mappings. Only super users can perform this task.

Recommendation

An administrator with the super user privilege should delete the Administrator role mapping in the Configure > Access Management window.

502616

Summary

Invalid user FQDN

Message

FQDN '$1' is not a group FQDN

Module

UI module

Severity

Error

Explanation

An invalid user LDAP fully qualified domain name (FQDN) was specified during CTS-Manager access management configuration.

Recommendation

The CTS-Manager administrator should work with the LDAP administrator to verify the user LDAP FQDN, then retry the configuration in the Configure > Access Management window.

502617

Summary

Admin UI unable to create remote account

Message

Unable to create remote account '$1' because $2. Account name must contain only lower case alphabetic characters. Upper case, digit, and special characters are not allowed.

Module

UI module

Severity

Error

Explanation

CTS-Manager was unable to create the indicated remote account because of the indicated reason.

Recommendation

The administrator should note the details provided by the “$2” variable in “Message,” and try to create the remote account again.

502618

Summary

Admin UI meeting viewing operation failure

Message

Cannot view more than one meeting in the same session. Log out of session on meeting '$1' first.

Module

UI module

Severity

Error

Explanation

Viewing more than one meeting in the same CTS-Manger Administration UI session is not allowed.

Recommendation

The meeting organizer should log out of the CTS-Manger Administration UI session for the first meeting, then log back into the UI to view information for the second meeting.

502619

Summary

System is being restarted

Message

System is being restarted. Try again later.

Module

UI module

Severity

Warning

Explanation

A system restart is in progress. During this process, users are not allowed to log into the CTS-Manager Administration UI.

Recommendation

The CTS-Manager Administration UI users must wait a few minutes until the system restart process is complete.

502620

Summary

Admin UI meeting viewing operation failure

Message

Email ID '$1' specified in URL is different than ID '$2' found in database

Module

UI module

Severity

Error

Explanation

The email notification received by a meeting organizer includes a URL that has a different user ID than their own. When using the URL to view information about their meeting, the meeting organizer receives this message. In CTS-Manager software release 1.1, this condition could occur when switching between versions.

Recommendation

The meeting organizer should check the URL provided in the email notification to ensure that the user ID is their own. If the user ID is incorrect, they should contact the Live Desk.

502621

Summary

Admin UI meeting viewing operation failure

Message

Missing required URL parameter '$1' in email link

Module

UI module

Severity

Error

Explanation

The email notification received by a meeting organizer includes a URL that is missing a required parameter. When using the URL to view information about their meeting, the meeting organizer receives this message.

Recommendation

The meeting organizer should ensure that they are using the URL provided in the email notification for that particular meeting, then try to view the meeting information again. If they get the same message, they should contact the Live Desk.

502622

Summary

Admin UI network operation failure

Message

Unable to set primary DNS (CLI code '$1')

Module

UI module

Severity

Error

Explanation

The system was unable to set the requested primary Domain Name Service (DNS) for the platform, and the CLI displayed an error message.

Recommendation

The administrator should verify the primary DNS, then retry the configuration.

502623

Summary

Admin UI network operation failure

Message

Unable to set secondary DNS (CLI code '$1')

Module

UI module

Severity

Error

Explanation

The system was unable to set the requested secondary Domain Name Service (DNS) for the platform, and the CLI displayed an error message.

Recommendation

The administrator should verify the secondary DNS, then retry the configuration.

502624

Summary

Admin UI configuration operation failure

Message

Group FQDNs '$1' already belong to access role '$1'

Module

UI module

Severity

Error

Explanation

The indicated group LDAP fully qualified domain name (FQDN) is already mapped to another role.

Recommendation

The administrator should determine to which role the indicated group FQDN should be mapped, and take the appropriate action in the Configure > Access Management window.

502626

Summary

Admin UI network operation failure

Message

Unable to set domain (CLI code '$1')

Module

UI module

Severity

Error

Explanation

The system was unable to set the domain name specified in the IP Settings window.

Recommendation

The administrator should verify that the domain name is correct, then retry the configuration.

502627

Summary

Admin UI network operation failure

Message

Unable to delete the primary DNS (CLI code $1)

Module

UI module

Severity

Error

Explanation

The system was unable to delete the DNS name, and the CLI displayed an error message.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502628

Summary

Admin UI network operation failure

Message

Unable to delete the secondary DNS (CLI code '$1')

Module

UI module

Severity

Error

Explanation

The system was unable to delete the DNS name, and the CLI displayed an error message.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502629

Summary

Admin UI certificate operation failure

Message

Invalid certificate file name '$1'. Valid certificate file extensions are .cer and .der.

Module

UI module

Severity

Error

Explanation

The filename of the certificate being uploaded is invalid. The file extensions .cer and .der are supported.

Recommendation

The administrator should check the filename extension to ensure that it is a supported extension. If it is not, change the extension, then retry the upload.

502630

Summary

Admin UI meeting viewing operation failure

Message

Meeting query matches more than a maximum of $1 instances. Change search criteria and try again.

Module

UI module

Severity

Error

Explanation

While in the Monitor > Meetings window, an administrator or Live Desk administrator searched for meetings that matched specified criteria, and the search results exceeded the maximum number of meetings that can be viewed in this window.

Recommendation

The administrator or Live Desk administrator should change the search criteria to narrow down the number of meetings.

502632

Summary

Admin UI configuration operation failure

Message

Cannot enable Interoperability because some devices do not support Interoperability. Click on the links to view the errored devices.

Module

UI module

Severity

Error

Explanation

At least one CTS or CTMS device does not support interoperability. Enabling interoperability with video conferencing requires that all CTS and CTMS devices support the feature.

Recommendation

The administrator should click the links to determine which devices have errors, then upgrade those devices with a later software version that supports interoperability with video conferencing.

502633

Summary

Failed to update the meeting

Message

Unable to update meeting because ID '$1' was not found

Module

UI module

Severity

Error

Explanation

The indicated meeting does not exist in the CTS-Manager database. The meeting was possibly deleted after the meeting organizer accessed information about it in the CTS-Manager Administration UI.

Recommendation

The meeting organizer should refresh the browser in which the meeting information is being viewed. If the information still appears after the refresh, the meeting organizer should contact the Live Desk.

502644

Summary

Unable to make intercompany configuration for a meeting.

Message

Unable to enable Intercompany because one or more occurrences have video conferencing enabled.

Module

UI module

Severity

Error

Explanation

A recurring meeting was set up wherein the interoperability with video conferencing feature is enabled for one or more meetings in the series. The meeting organizer subsequently tried to enable the intercompany feature for a meeting wherein interoperability is already enabled, and this message appears.

Both interoperability and intercompany features are not supported in the same TelePresence meeting.

Recommendation

The meeting organizer can disable the interoperability feature, then enable the intercompany feature.

502650

Summary

An endpoint with the given email address already exits.

Message

A endpoint with the email address '$1' already exists.

Module

UI module

Severity

Error

Explanation

When configuring the email address for an endpoint, a previously specified email address is entered, which CTS-Manager does not allow.

Recommendation

The administrator should enter a unique email address for the endpoint.

502651

Summary

There are no endpoint licenses available.

Message

There are no endpoint licenses available.

Module

UI module

Severity

Error

Explanation

Endpoint-based license files have not been uploaded to CTS-Manager.

Recommendation

The administrator should acquire and upload valid endpoint license(s). For information on performing these tasks, see "Licensing for CTS-Manager" section on page 11-6.

502652

Summary

Admin UI certificate operation failure

Message

Invalid certificate file name '$1'. Valid certificate file extensions is .class.

Module

UI module

Severity

Error

Explanation

The filename of the IBM Domino certificate being uploaded is invalid. CTS-Manager supports the .class file extension only.

Recommendation

The administrator must upload an IBM Domino certificate with the .class file extension.

502653

Summary

An endpoint with the given directory number already exits.

Message

An endpoint with the directory number '$1' already exists.

Module

UI module

Severity

Error

Explanation

An endpoint with the indicated directory number (DN) already exists.

Recommendation

The administrator should specify a different DN for the endpoint.

502654

Summary

An endpoint with the given IP address already exits.

Message

An endpoint with the IP address '$1' already exists.

Module

UI module

Severity

Error

Explanation

An endpoint with the indicated IP address already exists.

Recommendation

The administrator should specify a different IP address for the endpoint.

502655

Summary

Meeting organizer updated delegate information

Message

User updated delegate information, Delegates changed to = '$1'.

Module

UI module

Severity

Info

Explanation

Meeting organizer added users to manage their meetings using the 'Allow other users to manage my meetings' field in the Meeting Manager > Preferences window.

Recommendation

No further action

502700

Summary

Failed to display certificate

Message

Failed to display requested certificate

Module

Certificate management module

Severity

Error

Explanation

From the Configure > Security window, an administrator tried to view the content of a certificate but was unsuccessful because CTS-Manager detected that the certificate has been corrupted.

Recommendation

The administrator should upload a new copy of the certificate.

502803

Summary

Unable to delete configuration policy

Message

Unable to delete configuration policy because $1

Module

Configuration management module

Severity

Error

Explanation

The configuration policy could not be deleted for the indicated reason.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502808

Summary

Duplicate name specified for a policy

Message

Configuration policy with name '$1' already exists

Module

Configuration management module

Severity

Error

Explanation

A configuration policy with the indicated name already exists, which CTS-Manager does not allow.

Recommendation

The administrator should specify a different name for the configuration policy.

502900

Summary

Invalid date format error

Message

Incorrect date format

Module

Licensing module

Severity

Error

Explanation

The feature-based license has an expiration date.

Recommendation

The administrator must acquire a permanent license for the feature, then upload the license file to CTS-Manager. To acquire a permanent license, the administrator can contact the Global Licensing Operations (GLO) team at licensing@cisco.com. (When using this contact method, response times may vary depending on business hours and peak volume times.) For information on uploading the permanent license, see the "License Files" section on page 11-10.

502901

Summary

Invalid total count quantity error

Message

'$1' is not a valid total count for feature '$2'

Module

Licensing module

Severity

Error

Explanation

A license for a feature-based feature is generated with a count value of more than 1.

Recommendation

To resolve this issue, the administrator can contact the Global Licensing Operations (GLO) team at licensing@cisco.com. (When using this contact method, response times may vary depending on business hours and peak volume times.)

502902

Summary

File upload copying error

Message

Failed to make local copy of uploaded file

Module

Licensing module

Severity

Error

Explanation

An error occurred while CTS-Manager was uploading and copying a license file.

Recommendation

The administrator should retry uploading the license file to CTS-Manager. If the problem persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502903

Summary

Query failed error

Message

Query failed

Module

Licensing module

Severity

Error

Explanation

A database error occurred during a licensing operation.

Recommendation

The administrator should retry the licensing operation. If the problem persists, the administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502904

Summary

Object update error

Message

Update to database object failed

Module

Licensing module

Severity

Error

Explanation

A database error occurred while updating an object.

Recommendation

The administrator should retry the update. If the problem persists, the administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502905

Summary

Feature ownership error

Message

Feature '$1' does not belong to '$2'

Module

Licensing module

Severity

Error

Explanation

An error occurred while CTS-Manager was retrieving feature details from the license file.

Recommendation

The administrator should retry the operation. If the problem persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502906

Summary

Vendor has no features error

Message

Vendor '$1' has no features available to it in the license file '$2'

Module

Licensing module

Severity

Error

Explanation

An error occurred while CTS-Manager was retrieving feature details from the license file.

Recommendation

The administrator should retry the operation. If the problem persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502907

Summary

Null feature specifier error

Message

Feature Specifier is null

Module

Licensing module

Severity

Error

Explanation

An error occurred while CTS-Manager was retrieving feature details from the license file.

Recommendation

The administrator should retry the operation. If the problem persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502908

Summary

Count not specified error

Message

No count is specified for feature '$1'

Module

Licensing module

Severity

Error

Explanation

The license file does not include count information.

Recommendation

The administrator should retry the operation. If the problem persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502909

Summary

Invalid vendor error

Message

Correct vendor keys were not specified

Module

Licensing module

Severity

Error

Explanation

The vendor information in the license file is invalid.

Recommendation

The administrator should retry the operation. If the problem persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

502910

Summary

The license file specified is invalid.

Message

Invalid license specified : '$1'

Module

Licensing module

Severity

Error

Explanation

The license file content is corrupted or incorrect.

Recommendation

The administrator should verify that the license file is intended for the CTS-Manager server. If the problem persists, the administrator can request a new license by contacting the Global Licensing Operations (GLO) team at licensing@cisco.com. (When using this contact method, response times may vary depending on business hours and peak volume times.) For information on uploading the new license, see the "License Files" section on page 11-10.

502911

Summary

The license file specified is duplicate

Message

Duplicate license specified : '$1'

Module

Licensing module

Severity

Error

Explanation

A license file with the same features already resides in CTS-Manager.

Recommendation

The administrator should verify that the license file that they are trying to upload is the correct one, then retry the upload if appropriate.

502912

Summary

Invalid License. Upload valid license

Message

Some license features invalid in License: $1

Module

Licensing module

Severity

Error

Explanation

One or more feature line items in the license file is invalid.

Recommendation

The administrator should verify that the license file is intended for the CTS-Manager server. If the problem persists, the administrator can request a new license by contacting the Global Licensing Operations (GLO) team at licensing@cisco.com. (When using this contact method, response times may vary depending on business hours and peak volume times.) For information on uploading the new license, see the "License Files" section on page 11-10.

503001

Summary

Groupware adapter can not be started

Message

Unable to start adapter '$1' because $2

Module

Groupware adapter module

Severity

Alert

Explanation

CTS-Manager was unable to start the indicated client adapter for the indicated reason.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

503002

Summary

Groupware adapter sync operation failed

Message

Unable to sync '$1'.

Module

Groupware adapter module

Severity

Error

Explanation

Information for the indicated Microsoft Exchange endpoint (room) could not be synchronized with endpoint information in the CTS-Manager database.

Recommendation

The administrator can manually synchronize the Microsoft Exchange room in the Microsoft Exchange window of the CTS-Manager Administration UI.

Note Synchronization takes time and system resources to accomplish and should be done only when necessary.

503003

Summary

Groupware adapter failed to process meeting

Message

Unable to process meeting '$1'

Module

Groupware adapter module

Severity

Error

Explanation

The meeting organizer scheduled a meeting in their calendaring application, but CTS-Manager was unable to process the meeting.

Recommendation

The meeting organizer can try to update the meeting in their calendaring application, which gives CTS-Manager another opportunity to process the meeting.

503004

Summary

Groupware adapter failed to update endpoint.

Message

Unable to update endpoint '$1'.

Module

Groupware adapter module

Severity

Error

Explanation

CTS-Manager was unable to update information for the indicated endpoint. This message could indicate a CTS-Manager internal error.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

503005

Summary

Endpoint event processing failure

Message

Unable to process '$1' event for endpoint '$2'

Module

Groupware adapter module

Severity

Error

Explanation

CTS-Manager was unable to process a specific endpoint event. This message could indicate a CTS-Manager internal error.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

503100

Summary

Groupware adapter failed to process meeting

Message

Unexpected error condition while processing your request because $1

Module

Exchange adapter module

Severity

Error

Explanation

The CTS-Manager Exchange adapter encountered an internal error.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

503101

Summary

Missing configuration parameter in groupware adapter configuration

Message

Missing configuration parameter '$1' in groupware adapter configuration

Module

Exchange adapter module

Severity

Error

Explanation

The indicated configuration parameter, which is required, is missing.

Recommendation

The administrator must specify the required parameter, then retry the operation.

503102

Summary

Microsoft Exchange server connection failure

Message

Unable to establish connection with Microsoft Exchange server because $1

Module

Exchange adapter module

Severity

Critical

Explanation

A connection between the CTS-Manager server and the Microsoft Exchange server could not be established.

Recommendation

The administrator should check the settings for Microsoft Exchange parameters in the Microsoft Exchange window of the CTS-Manager Administration UI.

503103

Summary

Configuration parameter has invalid format value

Message

Configuration parameter '$1' has invalid format value '$2'

Module

Exchange adapter module

Severity

Error

Explanation

The indicated configuration parameter format is incorrect.

Recommendation

The administrator should note the details provided by the “$2” variable in “Message,” and reenter the parameter value based on the indicated format.

503105

Summary

Endpoint subscription failure.

Message

Unable to subscribe endpoint(s) '$1'.

Module

Exchange adapter module

Severity

Critical

Explanation

Possible reasons for this messages are as follows:

- An account for the indicated endpoint might not exist in the active directory or Microsoft Exchange.
- The CTS-Manager account might not have the needed permission to read the endpoint (room) calendar.
- The connection to the Microsoft Exchange server might be down.
- The Microsoft Exchange account for the indicated endpoint could have been modified.

Recommendation

The administrator can take this action:

- Set up a endpoint (room) account in the active directory and/or Microsoft Exchange server.
- Ensure that the CTS-Manager account has read access for the endpoint's (room's)calendar.
- Wait for CTS-Manager to regain its connection to the Microsoft Exchange server, or restart CTS-Manager.

503106

Summary

Groupware adapter endpoint processing failure

Message

Unable to un-subscribe endpoint '$1' because $2.

Module

Exchange adapter module

Severity

Error

Explanation

The indicated endpoint could not be unsubscribed for one of the following reasons:

- The connection to the Microsoft Exchange server might be down.
- The Microsoft Exchange account for the indicated endpoint could have been modified.

Recommendation

The administrator can wait for CTS-Manager to regain its connection to the Microsoft Exchange server if the server was down.

503107

Summary

Groupware Adapter not able to read/search endpoint (room) mailbox

Message

Unable to search for endpoint '$1' because $2.

Module

Exchange adapter module

Severity

Error

Explanation

CTS-Manager could not search for the indicated endpoint for one of the following reasons:

- The connection to the Microsoft Exchange server might be down.
- The Microsoft Exchange account for the indicated endpoint could have been modified.

Recommendation

The administrator can check the security settings for the endpoint and if the Microsoft Exchange server was down, wait for CTS-Manager to regain its connection to the server.

503109

Summary

Groupware adapter endpoint processing failure

Message

Unable to renew subscription for endpoint '$1' because $2.

Module

Exchange adapter module

Severity

Error

Explanation

CTS-Manager could not renew the subscription for the indicated endpoint for one of the following reasons:

- The connection to the Microsoft Exchange server might be down.
- The Microsoft Exchange account for the indicated endpoint (room) could have been modified.

Recommendation

The administrator can check the security settings for the endpoint and if the Microsoft Exchange server was down, wait for CTS-Manager to regain its connection to the server.

503112

Summary

Mailbox process error

Message

Unable to calculate mailbox size because $1

Module

Exchange adapter module

Severity

Error

Explanation

The mailbox quota for the CTS-Manager account could not be read.

Recommendation

The administrator can take this action:

- Specify a mailbox quota for the CTS-Manager account.
- Check the Microsoft Exchange domain to ensure that it is valid and correctly populated.

503113

Summary

Mailbox exceeds quota limit

Message

Mailbox size '$2' is exceeding quota '$1'. Cleanup the account to free some space.

Module

Exchange adapter module

Severity

Error

Explanation

The current size of the mailbox for the CTS-Manager account exceeds the indicated quota.

Recommendation

The administrator should remove unneeded data from the mailbox to free up space.

503114

Summary

Invalid domain name on calendar server

Message

Invalid domain name '$1'

Module

Exchange adapter module

Severity

Error

Explanation

The indicated domain name is invalid. If this error occurs, it would typically occur during the test connection of the Microsoft Exchange settings in the CTS-Manager Administration UI.

Recommendation

The administrator should verify the domain in which the Exchange server exists, and enter the correct domain name in the Microsoft Exchange window of the CTS-Manager Administration UI.

503115

Summary

Invalid SMTP LHS name

Message

Invalid SMTP LHS name: name cannot contain space(s)

Module

Exchange adapter module

Severity

Error

Explanation

A Microsoft Exchange username is invalid. A likely cause is that the username includes space(s).

Recommendation

The administrator should work with the Exchange administrator to correct the invalid username.

503116

Summary

Exchange server connection succeeded

Message

Exchange server connection succeeded

Module

Exchange adapter module

Severity

Informational

Explanation

The connection between the CTS-Manager server and the Exchange server was successful.

Recommendation

No action is required.

503117

Summary

Duplicate endpoints with same device name

Message

Duplicate endpoints found with device name '$1'

Module

Exchange adapter module

Severity

Error

Explanation

Duplicate endpoints (rooms) were configured for the indicated CTS device.

Recommendation

The administrator should check the endpoint (room) configuration in the Unified CM application user profile.

503501

Summary

Problem in sending out email notification

Message

Email cannot be sent for meeting in validation state '$1'

Module

Email management module

Severity

Error

Explanation

An internal error occurred, and as a result, the system could not send an email notification to validate meeting details with an organizer.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

503503

Summary

Invalid meeting organizer

Message

Invalid meeting organizer (subject '$1') because field '$2' has invalid value '$3'

Module

Email management module

Severity

Error

Explanation

The email address for the indicated meeting organizer is invalid.

Recommendation

The administrator should check the email address for the meeting organizer to ensure that it is correct. If it is not, the administrator can work with the appropriate administrator to correct the address in the directory. If the problem persists, the administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

503504

Summary

Dropped email request

Message

Discarded email request '$1' after '$2' attempts

Module

Email management module

Severity

Error

Explanation

CTS-Manager attempted the indicated number of times to send an email notification for a meeting, but all attempts failed.

Recommendation

The administrator should take these actions:

- Check the email server configuration to ensure the specified values are correct.
- In the Meeting Details window, click **Send Email** to send the notification email manually.

503505

Summary

Email request has been shut off

Message

Too many email requests submitted for ID '$1'

Module

Email management module

Severity

Error

Explanation

An excessive number of email requests were submitted for the same meeting. In this type of situation, CTS-Manager shuts off the email request to counter a possible Denial-of-Service (DoS) attack.

Recommendation

The administrator should wait for the defensive code to finish processing. If the problem persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

503602

Summary

Requested time slot is beyond allowable range

Message

Requested time slot ('$1' minutes) is beyond allowable range of '$2' minutes

Module

Resource schedule management module

Severity

Error

Explanation

A meeting was scheduled with a duration of 0 minutes or more than 24 hours, both of which are outside of the allowable range.

Recommendation

The meeting organizer should schedule a meeting within the allowable duration range of 1 minute to 24 hours.

503603

Summary

Requested time range is outside scheduling window

Message

Requested time range ('$1' to '$2') is outside scheduling window ('$3' to '$4')

Module

Resource schedule management module

Severity

Error

Explanation

A meeting organizer tried to schedule a meeting more than 1 year in advance, which is outside of the allowable scheduling window.

Recommendation

The meeting organizer should schedule a meeting within the allowable scheduling window of 1 year.

503604

Summary

Not enough resources for a given time slot

Message

Time slot ('$1' to '$2') only has '$3' available resources so cannot reserve '$4' more

Module

Resource schedule management module

Severity

Error

Explanation

Not enough conference bridges were available during the indicated timeslot, so no more reservations can be made during the timeslot.

Recommendation

The administrator can add more conference bridges.

503607

Summary

Resource provisioning data store error

Message

Failed to record resource provision into database for meeting serialIds in '$1'

Module

Resource schedule management module

Severity

Error

Explanation

CTS-Manager is unable to save a meeting reservation in the database because of an internal issue.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

503608

Summary

Cleared resource provisioning data store error

Message

Cleared error in recording resource provision into database for meeting serialIds in '$1'

Module

Resource schedule management module

Severity

Notice

Explanation

CTS-Manager cleared the error for a multipoint meeting with a resource issue.

Recommendation

No action is required.

503609

Summary

Meeting re-validation started

Message

Meeting re-validation started

Module

Resource schedule management module

Severity

Informational

Explanation

CTS-Manager started its revalidation of a meeting that was modified, for example, a meeting that was extended by 30 minutes.

Recommendation

No action is required.

503610

Summary

Meeting re-validation completed

Message

Meeting re-validation completed

Module

Resource schedule management module

Severity

Informational

Explanation

CTS-Manager completed its revalidation of a meeting that was modified, for example, a meeting that was extended by 30 minutes.

Recommendation

No action is required.

503800

Summary

MCU is not reachable

Message

MCU '$1' is not reachable

Module

MCU module

Severity

Critical

Explanation

CTS-Manager was unable to communicate with the conference bridge or server.

Recommendation

The administrator should check for any connectivity issues with the bridge and check the conference bridge status.

503801

Summary

MCU authentication failure

Message

Unable to authenticate with MCU '$1'

Module

MCU module

Severity

Critical

Explanation

The indicated conference bridge or server could not be authenticated.

Recommendation

The administrator should verify that the authentication information configured in the CTS-Manager Administration UI and the bridge or server match.

503802

Summary

Operation failure in MCU

Message

MCU '$1' has encountered an unexpected condition

Module

MCU module

Severity

Critical

Explanation

The indicated conference bridge or server has encountered an unexpected error.

Recommendation

The administrator should check the bridge or server status in the CTS-Manager Administration UI.

503804

Summary

MCU Hostname not found

Message

Hostname or IP address not found for MCU '$1'

Module

MCU module

Severity

Critical

Explanation

The indicated conference bridge or server is unknown to CTS-Manager, and as a result, CTS-Manager will not process any of its requests.

Recommendation

The administrator should verify that the bridge or server is properly configured in the CTS-Manager Administration UI.

503805

Summary

Cisco TelePresence Multipoint Switch does not support Interoperability

Message

Cisco TelePresence Multipoint Switch '$1' does not support Interoperability

Module

MCU module

Severity

Error

Explanation

The indicated CTMS does not support the interoperability with video conferencing feature.

Recommendation

The administrator should upgrade the CTMS to a version that supports the interoperability feature.

503806

Summary

Pushing meeting calendar to MCU failure

Message

Meeting '$1' was not pushed to MCU '$2' because it has error(s)

Module

MCU module

Severity

Error

Explanation

Information for the indicated meeting could not be pushed to the indicated conference bridge or server.

Recommendation

The administrator should check the Meeting Details window in the CTS-Manager Administration UI for an error condition, and take the appropriate action.

504000

Summary

Problem in communicating with IBM Domino server

Message

IBM Domino connection error: $1

Module

Domino adapter module

Severity

Alert

Explanation

A connection between the CTS-Manager server and the IBM Domino server could not be established.

Recommendation

The administrator should verify IP connectivity to the Domino server and ensure that the DIIOP server task is running.

504001

Summary

Problem in communicating with IBM Domino server

Message

Connection was established, but the system could not open the IBM Domino resource database '$1'

Module

Domino adapter module

Severity

Error

Explanation

The indicated IBM Domino resource database could not be accessed.

Recommendation

The administrator should collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

504002

Summary

IBM Domino organization name is invalid

Message

IBM Domino organization name '$1' is invalid

Module

Domino adapter module

Severity

Error

Explanation

The indicated IBM Domino organization name is invalid.

Recommendation

The administrator should verify that the actual and configured Domino organization names match.

504100

Summary

Date range is too long in data query

Message

Date range is too long. It must be less than '$1' months

Module

Reporting module

Severity

Error

Explanation

When requesting meeting information using the CTS-Manager Reporting API, the dates specified exceeded the maximum range of 6 months.

Recommendation

The Reporting API developer should specify dates within the supported range of 6 months, and resubmit the query.

504101

Summary

Too many data query attempts for the same session

Message

Too many data query attempts for the same session

Module

Reporting module

Severity

Error

Explanation

A request for meeting information using the CTS-Manager Reporting API was denied because the Reporting API client made two consecutive calls to the Reporting API web service within a short time interval. A minimum interval of 5 minutes between two consecutive calls is established to prevent spikes in the CPU usage of CTS-Manager.

Recommendation

The Reporting API developer should wait 10 to 15 minutes, then resubmit the query.

504200

Summary

WebEx connectivity error

Message

Can not connect to WebEx Server '$1'

Module

WebEx module

Severity

Error

Explanation

The CTS-Manager server could not establish a connection with the WebEx site.

Recommendation

The administrator should take the following action:

- Verify that the specified URL, username, access code, and certificate are valid.
- Verify the HTTPS connectivity between CTS-Manager and the WebEx scheduling server.

504201

Summary

WebEx registration error

Message

Failed to register with WebEx Server

Module

WebEx module

Severity

Error

Explanation

CTS-Manager could not locate the Cisco WebEx account information, for example, the Cisco WebEx hostname URL. After this information is set up, it is pushed from CTS-Manager to the CTMS so that the audio portion of the Cisco WebEx meeting could be enabled.

Recommendation

The administrator should take the following action:

- Verify that the specified URL, username, access code, and certificate are valid.
- Verify the HTTPS connectivity between CTS-Manager and the WebEx scheduling server.

504202

Summary

WebEx reserve error

Message

An error occurred during WebEx Reserve with WebEx Server '$1'

Module

WebEx module

Severity

Error

Explanation

CTS-Manager made an API call to the WebEx site, and the call failed. Possible causes for the failure include network issues or changes in the connection details.

Recommendation

The administrator should take the following action:

- Verify that the specified URL, username, access code, and certificate are valid.
- Verify the HTTPS connectivity between CTS-Manager and the WebEx scheduling server.

504203

Summary

WebEx schedule failure

Message

An error occurred during WebEx Schedule with WebEx Server '$1'

Module

WebEx module

Severity

Error

Explanation

CTS-Manager made an API call to the WebEx site, and the call failed. Possible causes for the failure include network issues or changes in the connection details.

Recommendation

The administrator should take the following action:

- Verify that the specified URL, username, access code, and certificate are valid.
- Verify the HTTPS connectivity between CTS-Manager and the WebEx scheduling server.

504204

Summary

WebEx sync hosts error

Message

An error occurred during sync up of users with WebEx Server '$1'

Module

WebEx module

Severity

Error

Explanation

CTS-Manager made an API call to the WebEx site, and the call failed. Possible causes for the failure include network issues or changes in the connection details.

Recommendation

The administrator should take the following action:

- Verify that the specified URL, username, access code, and certificate are valid.
- Verify the HTTPS connectivity between CTS-Manager and the WebEx scheduling server.

504205

Summary

WebEx expire error

Message

An error occurred during WebEx Expire with WebEx Server '$1"

Module

WebEx module

Severity

Error

Explanation

CTS-Manager made an API call to the WebEx site, and the call failed. Possible causes for the failure include network issues or changes in the connection details.

Recommendation

The administrator should take the following action:

- Verify that the specified URL, username, access code, and certificate are valid.
- Verify the HTTPS connectivity between CTS-Manager and the WebEx scheduling server.

504206

Summary

Scheduler not registered with WebEx

Message

Meeting scheduler '$1' is not registered with WebEx Server '$2"

Module

WebEx module

Severity

Error

Explanation

The indicated meeting organizer does not have a Cisco WebEx account.

Recommendation

The administrator should inform the meeting organizer that they need to set up a Cisco WebEx account.

504207

Summary

WebEx site delete error

Message

WebEx Server cannot be deleted'

Module

WebEx module

Severity

Error

Explanation

When trying to delete the WebEx site configured in CTS-Manager, a problem occurred. A possible cause is that the WebEx site's resources were not removed, or deallocated, from all future meetings, thereby preventing CTS-Manager from deleting the server.

Recommendation

The administrator should verify that the WebEx site was deallocated. If it was not, the administrator deallocate the site, then retry deleting the server. If the condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

504208

Summary

WebEx deallocate error

Message

WebEx Deallocate failed to complete successfully'

Module

WebEx module

Severity

Error

Explanation

CTS-Manager was unable to remove the WebEx site's resources from all future meetings.

Recommendation

The administrator should retry the deallocation operation. If the condition persists, the administrator can collect the log files, then contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

505000

Summary
Operation successful

Message
Operation successful

Module
External scheduling API module

Severity
Informational

Explanation
The CTS-Manager Scheduling API successfully handled the requested operation.

Recommendation
No action is required.

505001

Summary
Endpoint is not managed

Message
Endpoint ($1) is not managed by CTS-Manager

Module
External scheduling API module

Severity
Critical

Explanation
While scheduling a meeting, a meeting organizer requested an endpoint that is not managed by CTS-Manager.

Recommendation
The Scheduling API developer should consider adding the endpoint to the list of endpoints that are managed by CTS-Manager.

505002

Summary

Function not yet implemented

Message

($1) is not yet implemented

Module

External scheduling API module

Severity

Error

Explanation

Assuming that an iCalendar object must consist of a single VEVENT component, this message can display under the following conditions:

- The VEVENT component is missing.
- The VEVENT is present but invalid.
- CTS-Manager has not implemented the VEVENT.

Recommendation

The Scheduling API developer should contact the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Note To receive Cisco technical support for the Scheduling API, your organization must purchase Cisco Developer Network (CDN) support services. If your organization has not yet purchased these services, you can find information on CDN support at http://developer.cisco.com.

505003

Summary

Invalid scheduling API request

Message

Request data ($1) is invalid. Message: ($2)

Module

External scheduling API module

Severity

Error

Explanation

When scheduling a single meeting, this message can display under the following conditions:

- The iCalendar string is null.
- There are no meetings in the input array of TMeeting objects, or the array, which includes at least one meeting, is null.
- The iCalendar string could not be parsed; a valid iCalendar string must be passed in.
- The endpoint (room) attendee email address could not be parsed; the valid managed endpoint (room) email address must be passed in.
- DTSTART or DTEND is specified in a non-DATE-TIME format. The format of these properties must be of value type DATE-TIME.

When scheduling a recurring meeting, this message can display under the following conditions:

- Neither RRULE nor RDATE properties are specified in the iCalendar string.
- The frequency specified in RRULE has an invalid value; specify a valid integer value for frequency.
- The date(s) are specified in non-DATE-TIME format. The format must be of value type DATE-TIME.

When cancelling one instance of a recurring meeting, this message can display under the following condition:

- The RECURRENCE-ID is specified in a non-DATE-TIME format. The format must be of value type DATE-TIME.

Recommendation

The Scheduling API developer should note the specifics of the message, and take the appropriate action. If the action entails checking property values, the Scheduling API developer should work with the appropriate person on their team to ensure that the property values are correct and in the format required by the Scheduling API. For complete information on the Scheduling API, see the *Cisco TelePresence Manager Scheduling API Developer's Guide,* which you can access on the Cisco Developer Network (CDN) at http://developer.cisco.com.

505004

Summary

Scheduling API request not support

Message

Request ($1) is not supported

Module

External scheduling API module

Severity

Error

Explanation

The CTS-Manager Scheduling API does not support the scheduling of recurring instances. Therefore, this message displays if the METHOD is set to REQUEST and RECURRENCE-ID is specified in the iCalendar string.

Recommendation

The Scheduling API developer should work with the appropriate person on their team to withdraw this request. For complete information on the Scheduling API, see the *Cisco TelePresence Manager Scheduling API Developer's Guide,* which you can access on the Cisco Developer Network (CDN) at http://developer.cisco.com.

505005

Summary

Invalid iCal component from scheduling API

Message

($1) is not supported. Message: ($2) is required

Module

External scheduling API module

Severity

Error

Explanation

When scheduling a single meeting, this message can display under the following conditions:

- Assuming that one VEVENT must be passed in the iCalendar string, one of the following conditions exists:
  - The VEVENT component is missing.
  - The iCalendar string includes more than one VEVENT component.
- Assuming that one VTIMEZONE must be passed in the iCalendar string, this string includes more than one VTIMEZONE component.

Recommendation

The Scheduling API developer should note the specifics of the message, and work with the appropriate person on their team to verify the components. For complete information on the Scheduling API, see the *Cisco TelePresence Manager Scheduling API Developer's Guide,* which you can access on the Cisco Developer Network (CDN) at http://developer.cisco.com.

505006

Summary

Invalid iCal data from scheduling API

Message

($1) with value ($2) is not allowed. Message: ($3)

Module

External scheduling API module

Severity

Error

Explanation

When scheduling a single meeting, this message can display under the following conditions:

- DTSTART or DTEND is specified in a non-UTC format. These properties must be specified in a UTC format.
- DTSTART or DTEND has a nonzero seconds value. These properties must have a seconds value of 00.
- STATUS is not set to CONFIRMED. When the iCalendar string is passed in the scheduleTMeeting API request, the value for the STATUS property must be CONFIRMED.
- METHOD is not set to REQUEST. When the iCalendar string is passed in the scheduleTMeeting API request, the value for the METHOD property must be REQUEST.
- VERSION property value is not set to 2.0. When the iCalendar string is passed in the API request, the value for the VERSION property must be 2.0.

When scheduling recurring meetings, this message can display under the following conditions:

- Assuming that the iCalendar string must include only one RRULE property and one RDATE property, one of the following conditions exist:
  - More than one RRULE property is specified.
  - More than one RDATE property is specified.
- The date(s) is specified in a non-UTC format. This property must be specified in a UTC format.

When cancelling a single meeting, recurring meetings, and a single instance of a recurring meeting, this message can display under the following conditions:

- STATUS is not set to CANCELLED. When the iCalendar string is passed in the scheduleTMeeting API request, the value for the STATUS property must be CANCELLED.
- METHOD is not set to CANCEL. When the iCalendar string is passed in the scheduleTMeeting API request, the value for the METHOD property must be CANCEL.

When cancelling a single instance of a recurring meeting, this message can display under the following conditions:

- RECURRENCE-ID is specified in a non-UTC format. This property must be specified in a UTC format.

Recommendation

The Scheduling API developer should note the specifics of the message, and check the corresponding property value. For complete information on these property values, see the *Cisco TelePresence Manager Scheduling API Developer's Guide,* which you can access on the Cisco Developer Network (CDN) at http://developer.cisco.com.

505007

Summary

Invalid iCal data from scheduling API

Message

Property ($1) with valid value is required. Current value: ($2)

Module

External scheduling API module

Severity

Error

Explanation

When scheduling a single meeting, this message can display under the following conditions:

- The UID, ORGANIZER, or SUMMARY property is missing.
- The DTSTART or DTEND property is missing or has an empty value. The iCalendar string must include one DTSTART property with a valid value and one DTEND property with a valid value.
- The STATUS property value is missing or is not set to CONFIRMED.
- The METHOD property is missing or has an empty value. This property must be set to REQUEST.
- The VERSION property is missing or has empty value. This property must be set to 2.0.

When scheduling a recurring meeting, this message can display under the following condition:

- The VTIMEZONE property is missing. The iCalendar string must include one VTIMEZONE property.

When cancelling a single instance of a recurring meeting, this message can display under the following condition:

- The RECURRENCE-ID property has empty value. The iCalendar string must include one RECURRENCE-ID property with a valid value

Recommendation

The Scheduling API developer should note the specifics of the message, and check the corresponding property value. For complete information on these property values, see the *Cisco TelePresence Manager Scheduling API Developer's Guide,* which you can access on the Cisco Developer Network (CDN) at http://developer.cisco.com.

505008

Summary

Invalid iCal data value type

Message

Property ($1) must be of value type ($2)

Module

External scheduling API module

Severity

Error

Explanation

The indicated property must be of the indicated value type.

Recommendation

The Scheduling API developer must specify the correct value type for the property.

505009

Summary

Number of meetings in a request exceeds the limit

Message

Maximum meetings allowed per request are ($1). Current value: ($2).

Module

External scheduling API module

Severity

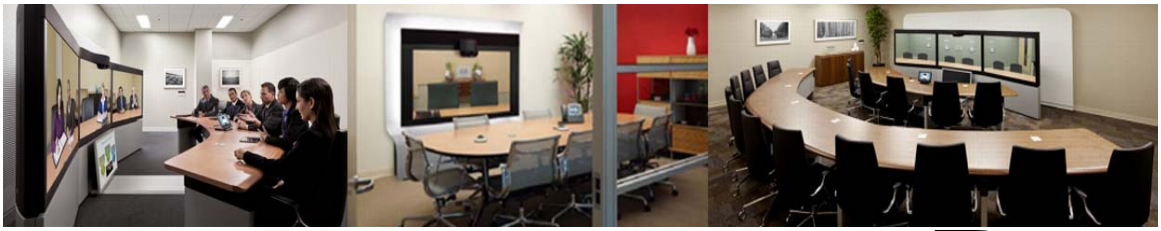
Error

Explanation

The CTS-Manager Scheduling API supports a maximum of 25 meetings in one request, and the maximum number of meetings in one request was exceeded.

Recommendation

The Scheduling API developer should reduce the number of meetings in the request to a maximum of 25.



APPENDIX B

Replacing a Cisco TelePresence System Codec

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

Overview

This appendix describes the process for replacing a Cisco TelePresence System (CTS) primary codec.

Before you install the codec, make sure you have the following:

- MAC address of replacement codec unit
- Computer attached to the network
- The Assembly, Use & Care, and Field-Replaceable Unit Guide for your CTS model

Note It is recommended to make this change as a planned activity during maintenance.

Caution Complete all steps before powering on any secondary codecs. This prevents the secondary codecs from being affected by any software and peripheral upgrades to the primary codec.

Replacing a Cisco TelePresence System Codec

To replace a Cisco TelePresence System codec, do the following:

Step 1 Replace the primary codec unit according to the procedures in the Field-Replaceable Unit Guide for your CTS model.

Step 2 Open a browser on a computer connected to the network.

Step 3 Log in to Cisco Unified CM Administration and set up the new codec.

For more information, refer to the Cisco Unified Communications Manager Administration Guide.

Step 4 Add the Room (endpoint) Email ID of the previous codec to the new codec.

Step 5 Make sure the new codec's status is registered.

Step 6 Delete the MAC address of the previous codec from the Cisco Unified CM application user profile that is used in CTS-Manager.

Step 7 Add the new codec to the application user profile and click **Save**.

Step 8 Power on the CTS system by turning the power switches to the On position on the PDUs and (if present) auxiliary control unit. Do not power on any secondary codecs.

Step 9 In the browser on the computer, go to the IP address of the primary codec unit.

Step 10 Enter the required information at the login screen.

The Cisco TelePresence Administrator window appears.

Step 11 Verify the status of the Cisco Unified Communications Manager (seen in the lower left portion of the window) is Enabled/Up.

Step 12 Select **Hardware Setup** to verify the cameras, displays, speakers, and microphones are working properly.

Step 13 Perform the Auto Adjust camera setup procedure. This sets the white balance to the correct levels.

Step 14 Log in to CTS-Manager as SysAdmin or Administrator.

Step 15 Go to **Configure > Application Settings**.

Step 16 Disable the Meeting Notification Email by selecting **No** for Enable Feature and clicking **Apply**.

Step 17 Go to **Configure > Unified CM**.

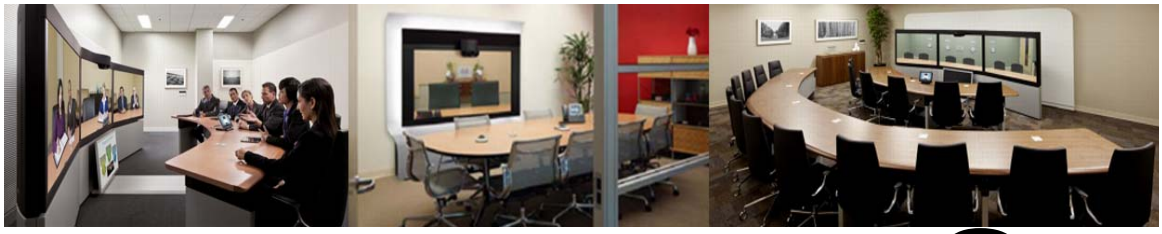
Step 18 Select the Unified CM that has the new codec.

Step 19 Click **Discover Rooms**.

The new codec with the existing endpoint name is added and the previous codec is removed from CTS-Manager.

Step 20 Power on any secondary codecs of the CTS system.

Note Make sure the old phone and codec are turned off.



APPENDIX C

Reconfiguring CTS-Manager and CTMS Addressing

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

Overview

This appendix describes the process for reconfiguring addressing for CTS-Manager and CTMS. It contains the following sections:

- Changing IP Address and Hostname of CTS-Manager, page C-1
- Changing IP Address of CTMS, page C-2

Before You Begin

Make sure you have the following before you begin:

- SysAdmin username and password for CTS-Manager
- Administrator username and password for CTMS
- Laptop computer attached to the network

Changing IP Address and Hostname of CTS-Manager

To change the IP address and hostname of CTS-Manager, do the following:

Step 1 Get the new IP address, which should be in the data VLAN, and new hostname, which should be with the new IP address in DNS.

Step 2 Log in to the CTS-Manager web UI and go to **Configure > System Settings > IP**

Step 3 In the IP Address field, replace the existing IP address with the new IP address and click **Apply**.

CTS-Manager restarts.

Step 4 After CTS-Manager has restarted, SSH to CTS-Manager using the new IP address and log in as the SysAdmin.

Step 5 Run the **Set Network Hostname <*new hostname*>** command.

Step 6 When CTS-Manager asks you to restart the system, select **Yes**.

CTS-Manager restarts.

Step 7 Log in to the CTMS web UI and go to **Configure > CTS Manager**

Step 8 In the Host field, change the IP address or hostname to the new IP address or hostname of CTS-Manager and click **Apply**.

Note In the Host field, you can use either hostname or IP address, but not both.

After restart, all CTS-Manager services will start and function normally with new IP and hostname.

Changing IP Address of CTMS

To change the IP address of CTMS, do the following:

Step 1 Get the new IP address, which should be from the voice VLAN, and hostname, which should be with the new IP address in DNS.

Step 2 Log in to the CTMS console as the admin and run following commands:

a. **set network gateway <***gateway IP***>**

b. **network IP eth0 <***new IP address***> <***mask IP***>**

CTMS restarts.

Step 3 Verify the new IP has been changed, by doing the following:

a. From the console, run the **show network eth0** command and verify the new IP address is displayed.

b. SSH to the CTMS, run the **cat/etc/hosts** command and verify the new IP address is displayed.

c. Log in to the CTMS web UI, go to **Troubleshoot > System Information** and verify the new IP address is displayed.

d. Log in to the CTS-Manager web UI, go to **Configure > Bridges and Servers**, and verify the new IP address is displayed.

Note The meeting organizer will not receive any new emails from CTS-Manager for future meetings after the IP address is changed.

Step 4 Log in to the Unified CM Administration web UI, go to **Device > Trunk** and change the IP address for Destination Address to the new IP address.

Note Make this change wherever the CTMS IP address is used.