Cisco TelePresence Management Suite

Administrator Guide

Last Updated: November 2020

Software Version 15.11

Contents

Introduction 13
Related Documents 13
Cisco TMS Overview 15
Web Page Features and Layout 15
Portal 17
Sitemap 17
Cisco TMS Components 17
Internet Information Services Web Server and Applications 18
The tmsng SQL Database 18
Windows Services 19
Cisco TMS Tools Application 20
Setting up Cisco TMS 21
Adding Release and Option Keys 21
Getting Your Cisco TMS Release Key 21
Entering Keys During Cisco TMS Upgrades 21
Entering Release Keys Post Installation 22
Entering Option Keys Post Installation 22
How Groups and Permissions Work 22
Group Membership 22
System Permissions 22
Setting Up Initial Group Permissions 23
Enabling Active Directory Lookup 24
Adding User Accounts and Profiles 24
Language setting 24
Cisco Collaboration Meeting Rooms Hybrid 25
Webex Site and User Credentials 25
Reviewing and Setting Defaults 25
General Settings 25
Network Settings 25
Mail Settings 27
Conference Settings 27
Using Configuration Templates 27
Creating a New Configuration Template 28
Viewing a Configuration Template 28
Editing a Template 28
Applying Templates to Systems 29

Creating a New Configuration Template from an Existing Template 29
Custom Configuration and Commands 29
Routing 31
Introduction to Routing 31
The Main Participant 32
Allocation 33
Protocols and Call Control 34
IP 34
ISDN 34
How Call Protocols are Prioritized 34
What Infrastructure Does Cisco TMS Use for Routing? 35
MCU 35
Gatekeeper 37
ISDN Gateway 37
Cisco Unified Communications Manager 38
How Zones Work 38
Setting up an IP Zone 39
Setting a Zone on One or More Systems 40
Setting up an ISDN Zone 41
Example 41
Creating area Code Rules 42
Setting a Zone on One or More Systems 42
System Management Overview 44
Supported Systems 44
System Types Supported by Cisco TMS 44
System Locations 44
How Endpoints are Managed by Cisco TMS 44
Cisco TMS Controlled 45
Cisco TMSPE Provisioned 45
Unified CM Registered 45
Unmanaged Endpoint 46
Changing Management Modes 46
Infrastructure Systems 46
Booking 46
Monitoring 46
Software Versions 46
Systems Behind a Firewall/NAT 47
Booking 47
Statistics and monitoring 47
Software Upgrades 47
Phone Books 47
Configuration Templates 48

Configuration Backup and Restore 48
System Replacement 48
How Systems are Added to Cisco TMS 48
Automatic Discovery 48
Manual Addition 49
Through Unified CM 49
Provisioning 49
Pre-registration 49
How Cisco TMS Communicates with Managed Systems 49
The Addresses that Systems Use to Contact Cisco TMS 50
System Connectivity Status 50
Calendar Push Behavior 51
How Persistent Settings Work 52
Adding and Managing Systems 53
Setting Up Default System Folders 53
Adding Systems 54
Prerequisites for all Systems 54
Using Automatic Discovery 55
Adding by IP addresses or DNS Names 55
System Discovery Order by Protocol 56
Pre-registering Endpoints 57
Adding Endpoints Behind a Firewall/NAT 57
Adding Unified CM and Registered Endpoints 58
Adding an Unmanaged Bridge 60
Adding Unmanaged Endpoints 61
Endpoint Support in Various Communication Modes 62
Managing Systems 65
Viewing and Editing a System 65
Changing Managed Endpoints Password 66
Assigning Email Addresses to Endpoint 66
Swapping a System 67
Upgrading Cisco TMS-Managed Endpoints 68
Purging a System 69
Navigator 69
Folder Actions 70
Navigating the Folder Tree 70
Endpoints 71
Cisco VCS 78
Unified CM 85
Cisco TelePresence Supervisor MSE 8050 88
TelePresence Conductor 92
Cisco Meeting Server 101

MCUs and TelePresence Server 112
Gateways 119
Content Servers and Recording Servers 122
Unmanaged Bridge 127
Unmanaged Endpoint 131
Add Systems 134
Folder and System Permissions 137
Ticketing Service 138
Ticket Statuses 139
In-page System Management 139
System Overview 140
Manage Dial Plan 140
Provisioning 141
Users 141
FindMe 148
Devices 150
Configuration Backup 150
Perform Backup 150
Perform Restore 150
Backup/Restore Activity Status 151
Configuration Templates 151
Configuration Templates Main Page 152
Select Settings for Configuration Template 152
Configuration Template Activity Status 155
System Upgrade 155
Cisco TMS Endpoints 155
Endpoints Managed by the Provisioning Extension 155
Upgrade Modes 156
Buttons for Upgrading 156
Select Software and Release Keys 157
Software Manager 157
System Upgrade Activity Status 158
Purge Systems 159
Event Notification Manager 159
Select Event Types 159
Bulk Room Email Mapping for Endpoints 160
Export Room Mailbox Address 160
Import Room Mailbox Address 160
System Status Reporting 161
Booking 162
Conference Basics 162
What is a Conference? 162

What is a Participant? 162
What is a Video Conference Master? 162
Routing and MCUs 163
Port Usage on MCUs 163
How are Conference Layout Options Controlled? 163
What is an Externally Hosted Conference? 163
Email Notifications 164
Booking a Conference 164
Booking a Conference with Remote Systems 166
Viewing and Editing Existing Conferences 167
Adding Recurrence to a Conference 167
Booking and Editing Conferences with Cisco TelePresence Conductor 168
New Conference 170
Basic Settings 170
Advanced Settings 172
Participants Tab 174
Webex Details Tab 176
Connection Settings Tab 176
MCU Settings Tab 177
TelePresence Conductor Settings Tab 177
Conference Information Tab 177
Webex Details Tab 178
MCU Settings 178
Cisco TelePresence Conductor Settings 185
List Conferences 186
Editing Conferences from This Page 186
Time Zone Display 187
Search 187
Advanced 187
Search Results 188
External Service 190
View Conference 190
List References 191
Conferences and References 191
Creating a Reference 191
Deleting References 191
Sorting References 191
Searching for References 191
Ad Hoc Booking 191
Displaying Systems 192
Checking Availability and Reserving Systems 192
Booking on Behalf of Someone Else 192
Entering a Billing Code 192

Participant Templates 192
Why Use Participant Templates 193
Creating a Participant Template 194
Adding a Participant Template to a Booking 198
Sample Participant Template Setups 198
Conference Templates 200
Editing and Using a Conference Template 200
Monitoring 201
Monitoring and Managing Conferences 201
Conference Control Center 201
Graphical Monitor 202
Operator Conferences 202
Conference Control Center 203
Enabling Ad Hoc Conference Monitoring 203
Finding and Displaying Conferences 204
Monitoring and Managing Conferences 204
Viewing Conference Events 207
Viewing System Tickets 207
Controlling Sound Alerts 207
Conference Event Log 207
Graphical Monitor 208
View Folders and Systems 208
Creating and Managing Phone Books 210
Phone Book Basics 210
The Role of Phone Book Sources 210
Hierarchical Phone Books 210
Default Source and Phone Book 210
Phone Book Routing 210
Phone Book Types 211
Corporate Directory 211
Global Directory 211
Local Directory 211
Setting the Phone Book Type For All Systems 211
Creating a Phone Book 212
Creating a Phone Book Hierarchy 213
Alternate Way of Generating Phone Book 213
Granting Access to Phone Books 213
Cisco TMS Users 213
Provisioning Users 213
Setting Phone Books on Systems 214
One Phone Book on Multiple Systems 214
Multiple Phone Books on a Single System 214

Setting Global Directory Update Frequency 214
Exporting Contacts to a File 214
Manage Phone Books 215
Sources 215
Access Control 216
Manage Phone Book Sources 216
Source Types and Configurations 216
Cisco Unified Communications Manager 224
Viewing contacts 224
Phone Book and Source Activity Status 224
Phonebook for Cisco Meeting Management 224
Add Cisco Meeting Management Server 225
Set Phone book/s on a Cisco Meeting Management Server 225
Edit Cisco Meeting Management Server 225
Delete Cisco Meeting Management Server 225
Reporting 226
Reporting Basics 226
Types of Data 226
How Log Purge Settings Affect Reporting 226
Creating a Report 226
Exporting Data to an Excel Sheet 228
Using Reporting Templates 228
Creating a Template 228
Viewing and Running Template Searches 228
Editing and Deleting a Template 229
Bridge Utilization 229
The Reporting Mechanism and Logs 229
Troubleshooting 229
Call Detail Records 230
What is a Call Detail Record? 230
Endpoints 230
MCUs 230
Gatekeeper and VCS 230
Users 231
TelePresence Content Servers 231
Gateways 231
Billing Code Statistics 231
Conferences 231
Conference Statistics 231
Conference Resources 231
Events 232
Scheduling Interfaces 232

Bridging Methods 232
System 233
Ticket Log 233
Feedback Log 233
Connection Error 233
System Connection 233
Authentication Failure 233
Boot 233
History 233
Administrative Tools 234
Configuration 234
General Settings 234
Network Settings 237
Email Settings 243
Edit Email Templates 244
Conference Settings 248
WebEx Hybrid Settings 256
Reporting Settings 258
Provisioning Extension Settings 258
Manage Ticket Error Levels 261
Manage Event Notification Error Levels 266
User Administration 266
Groups 267
Users 273
Default Groups 277
Default System Permissions 277
Locations 278
ISDN Zones 278
IP Zones 279
Billing Codes 280
Manage Billing Codes 280
Billing Codes Activity Status 282
Diagnostics 282
TMS Tickets 282
Provisioning Extension Diagnostics 282
Conference Diagnostics 283
Activity Status 284
Analytics Extension 285
TMS Server Maintenance 285
Identifying a Server Time Mismatch 285
Downloading Diagnostics Files 285
Viewing Free Disk Space 286

Viewing and Managing Database Files and Sizes 286
Purging Old Data and Logs 286
TMS Redundancy 287
TMS Services Status 287
Audit Log 288
Cisco TMS Tools 290
Configuration 290
Database Connection Settings 290
Directory Locations 292
Security Settings 293
Encryption Key 293
TLS Client Certificates 293
Advanced Security Settings 294
Additional Information about Security Settings 296
Utilities 296
Change User Domain 296
Generate Phone Book 296
Resolve Duplicate Keys 297
Diagnostic Tools 297
SNMP Connectivity Checking Tool 297
Scan Db for Encryption Key Mismatch 297
TMS Log Collector 298
Launch TMS Log Collector 299
Set to debug mode 299
Unsupported Cisco TMS version or Components not installed 302
TMS Redundant Deployment 303
Collect Logs 303
Export TMSXE Logs 303
Get TMS Logs 304
Troubleshooting 305
Troubleshooting 306
Using the Logs 306
Downloading Log Files 306
Locating the Logs on the Server 306
Log Overview 307
Changing the Log Level 310
Reading the Logs 311
Website Scenarios 312
Cisco TMS does not Load 312
System Scenarios 313
New Systems are not Automatically Discovered 313
System Information and Status Outdated 313

Scheduled Events not Starting 313
System Upgrade Fails 314
Tickets not Raised 315
Conference Scenarios 315
Call Does Not Start 315
Java Applet Scenarios 316
Username and Password Prompt Keeps Reappearing 316
Applet does not Load 316
Applet Is Slow to Load or will not Load Completely 316
Mozilla Firefox Blocks Java Plugin 317
Quicker Load of Monitor 317
Out of Memory 317
Increase Maximum Amount of Memory 317
Phone Book Scenarios 318
Phone Book (Corporate Directory) Errors 318
Polycom Endpoints do not Get Phone Books 318
Reporting Scenarios 319
Bridge Utilization Report 319
No CDRs from Endpoints Running Cisco Collaboration Endpoint Software, TC, and TE Software 319
No CDRs from Cisco TelePresence Server 320
No CDRs from Cisco TelePresence MCU 320
No CDRs from Polycom Endpoints 320
No Statistics for Legacy TANDBERG Systems 321
Cause Codes 321
Accessibility notice 326
Cisco Legal Information 327
Cisco Trademark 327

Introduction

Cisco TelePresence Management Suite (Cisco TMS) enables you to manage, deploy, and schedule your entire video network, including telepresence, from one platform.

Cisco TMS provides visibility and centralized control for on-site and remote video systems, and aims to make telepresence accessible and successful within an organization.

The primary audiences for Cisco TMS include:

- Administrators looking to maintain and operate a telepresence network.
- Consumers of a telepresence network who want interfaces for utilizing the telepresence deployment as a service, rather than as individual components.
- Business owners looking to analyze and track the use of their telepresence investment.

The user permissions feature lets the administrator configure Cisco TMS to present each user only with the functionality needed for their particular role.

About this guide

This administrator guide contains conceptual information, procedures, and reference information primarily aimed towards Cisco TMS administrators.

The contents of this guide are also available as web help while using Cisco TMS.

Click the question mark symbol in the upper right corner of any Cisco TMS page to access the context-sensitive help.



Related Documents

All documentation for the latest version of Cisco TMS can be found at http://www.cisco.com/en/US/products/ps11338/tsd_products_support_series_home.html.

Extension documentation is found at http://www.cisco.com/en/US/products/ps11472/tsd_products_support_series_home.html

Table 1 Related documents for the Cisco TMS Administrator Guide and Web Help

Title	Link
Cisco TelePresence Management Suite Installation and Upgrade Guide	http://cisco.com
Cisco TelePresence Management Suite Provisioning Extension Deployment Guide	http://cisco.com
Cisco TelePresence Conductor with Cisco TMS Deployment Guide	http://cisco.com
Cisco TelePresence Video Communication Server Administrator Guide	http://cisco.com
Cisco Unified Communications Manager documentation	http://cisco.com
Cisco TelePresence Supervisor MSE 8050 Printable Help	http://cisco.com
Cisco TelePresence Conductor Administrator Guide	http://cisco.com

Training

Training is available online and at our training locations. For more information on all the training we provide and where our training offices are located, visit www.cisco.com/go/telepresencetraining

Glossary

A glossary of TelePresence terms is available at: tp-tools-web01.cisco.com/start/glossary/

Cisco TMS Overview

This chapter provides a short introduction to the core functionality of Cisco TMS and a walkthrough of the main elements of the web application. A brief explanation of each of the main components and services that make up the Cisco TMS backend is also included.

Web Page Features and Layout 15
Cisco TMS Components 17

Web Page Features and Layout

Administrators have full access to Cisco TMS. Users with restricted permissions will not see or have access to all menus and options.

Table 2 User interface elements in Cisco TMS and their functions

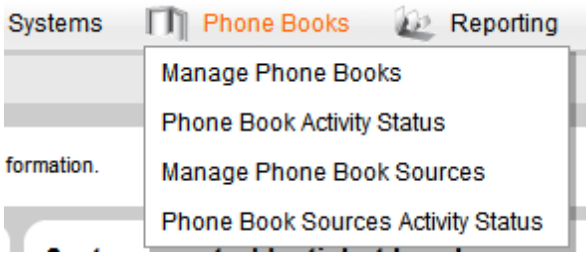
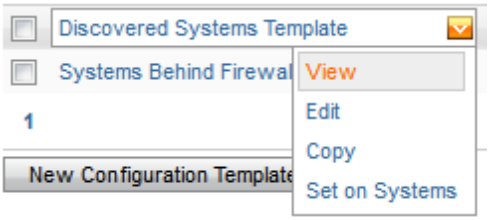
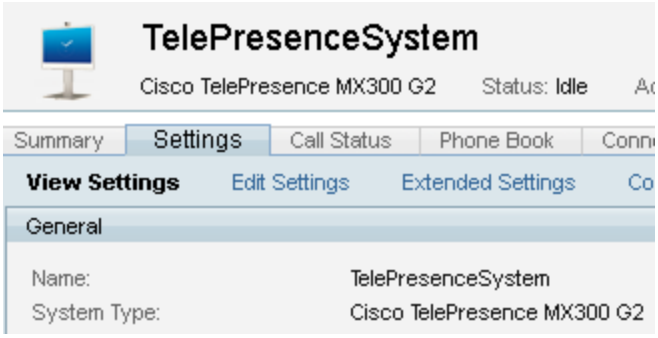
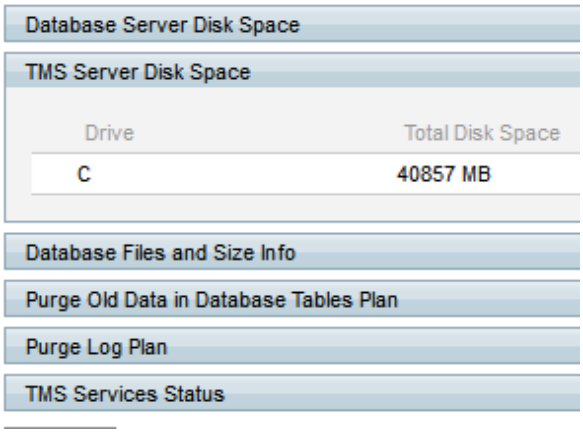
User interface element	Image	Description
Top-level menu		The Cisco TMS functionality is grouped by main categories in a top menu. Hover over each menu item to expand the sub-menu.
Search field		Use the search box at the top right of every page to find an individual telepresence system. You can search by: ▪ **System name** ▪ **Network address** ▪ **SIP URI** ▪ **H.323 ID** ▪ **E.164 Alias** ▪ **ISDN number** ▪ **MAC Address** ▪ **Hardware Serial Number** If you click on the system name in the search results you will be taken to the **View settings** page for the system in the Navigator, page 69.

Table 2 User interface elements in Cisco TMS and their functions (continued)

User interface element	Image	Description
Help		The help icon takes you to context-sensitive help for the page you are on.
Log out		The key icon logs you out of Cisco TMS.
Drop-down menus		Hovering over items in a list will display an orange drop-down menu icon when available.
Lists		You can re-sort most lists in Cisco TMS by clicking the title of the relevant column. A small triangle next to the column title will indicate whether the sorting is ascending or descending. Some lists may have hundreds or even thousands of entries. Rather than show them all in a single list, most lists in Cisco TMS are split into pages with **Previous** and **Next** links at the bottom
Tabs		Many pages in Cisco TMS have multiple views available, shown as tabs across the top. There can be multiple levels of tabs. In the screenshot to the left, there are multiple pages/views available, including Summary, Settings, Call Status, Connection, and Logs. The active tab is displayed in a darker blue and has additional views under it. The current view is highlighted.
Collapsible sections		Each collapsible section has a blue bar at the top. If the bar has arrow icons at the right edge, clicking on the blue bar will cause the section to either collapse or expand. This allows you to choose which areas of the screen to concentrate on or see more of.

Portal

The portal page provides an overview of the status of the videoconferencing network.

Systems

This section of the page lists the different types of systems that are registered in Cisco TMS.

Each system type is linked to a **Systems > Navigator** page. If you click on for example **Endpoints**, the **Systems > Navigator** page is opened in folder view sorted by *System Category*, showing all the endpoints in Cisco TMS.

For details, see Navigator, page 69.

Tickets

This section contains a list of systems grouped by their uppermost ticket level.

Note that each system is only counted once even though it may have more lower-level tickets.

The ticket levels are linked to the **Systems Ticketing Service** page. If you click on for example **Systems with uppermost ticket level Critical**, the **Systems Ticketing Service** page will be opened showing all systems with *Critical* as the uppermost ticket level. If the system has tickets of lower levels, these tickets will also be displayed.

The **Open Ticketing Service** link takes you to Ticketing Service, page 138.

Conferences and Reservations

This section of the portal page presents today's conferences and reservations.

The **Open Conference Control** Center link opens Conference Control Center, page 203.

System Usage

The System Usage graph shows the number of endpoints that have been in call per day as a blue area, and the number of booked endpoints per day as a green line.

Click **Show Conference Statistics** to see reporting on Conferences, page 231.

Sitemap

In Cisco TMS: **Portal > Sitemap**

This page gives an overview of all the main pages in Cisco TMS. The page covers all items from the main menu level to sub-menus.

When clicking on a menu name, a brief explanation of the contents on each page is shown.

Clicking on the **Go to ...** link below a page name takes you to that screen in Cisco TMS.

Cisco TMS Components

Cisco TMS consists of a set of standard components including:

- Internet Information Services (IIS) Server with webapps
- TMS Services
- tmsng SQL Database
- TMS Tools application

Some background knowledge of these components is required for administrators managing a Cisco TMS deployment and when troubleshooting. The components are described below.

Internet Information Services Web Server and Applications

Microsoft Internet Information Services (IIS) is used as the primary web server for hosting web content, web services, and web applications that make up the user and external service interfaces of Cisco TMS.

TMS sites are configured to run under a specific Application Pool to isolate them from other activity that may be hosted on the IIS Server.

Cisco TMS is developed using the Microsoft .NET platform. Some additional IIS components are therefore required for Cisco TMS to work properly. These components are installed by Windows during the Cisco TMS installation.

All web-related files are stored on the server in the location specified during the installation. Installation creates the virtual directories described below.

For IIS troubleshooting information, see Website Scenarios, page 312.

tms

This is the authenticated web application where all user facing web content is hosted. **http://<server>/tms** is the landing page for user interaction with Cisco TMS.

Authentication is required for all access to this application, and users authenticate through IIS. By default, both *Windows Authentication* and *Basic Authentication* are enabled.

tms/public

The tms/public component is a web application and directory structure for all content and services that must be accessible to systems without authentication. Examples of such content are call feedback and phone books.

Anonymous Authentication must be enabled for this component. All other authentication modes must be disabled.

external

External is the web application and directory structure for all content and services that use authentication at the web server level. It is primarily used for external facing APIs for server integrations.

cdm and pwx

Some managed system types have hardcoded URLs for where they can post information or query for services. Web applications are therefore set up at specific paths in the root level of the website to match these hardcoded URLs.

- **/cdm** is where CTS/TX systems post their feedback and status updates.
- **/pwx** is where Polycom devices post their feedback and status updates.

tmsagent

The tmsagent web application serves as a proxy to handle requests intended for the Cisco TelePresence Management Suite Provisioning Extension.

The tmsng SQL Database

All operational and system configuration data is stored in the SQL database, by default named **tmsng**. Software files for system upgrades and log files for the services are stored outside of this database.

The database runs on a Microsoft SQL Server. The SQL server can be on the same server as or remote from Cisco TMS, and all references to find the database server are via registry keys defined during setup on the server platform.

Users never directly authenticate or interact with the database. All interaction with the database is executed within the context of the application.

Note that if Cisco TelePresence Management Suite Provisioning Extension is used, this extension stores its information in several separate databases.

Important Note: Any modifications done to Cisco TMS database must only be made through the Cisco TMS web interface. Modifications made through SQL Management Studio should never be performed unless advised by Cisco. This can cause Cisco TMS performance issues, and/or loss of functionality and will result in a new installation or restoration of a previous backup.

For detailed SQL server requirements and best practices for database maintenance, see *Cisco TMS Installation and Upgrade Guide*.

Credentials and Permissions

During the installation of Cisco TMS, the sa account on the SQL server is automatically chosen to create and access the database, but by choosing a custom installation different credentials may be used. Note that the account used to run and upgrade Cisco TMS must have *db_owner* permissions to the tmsng database, while a user that also has access to **master.mdf** is required for creating the tmsng database the first time.

Windows Services

Cisco TMS relies on a set of Windows services to run at all times on the server or servers. The function of each of these services is described below.

TMSLiveService

This backend service:

- Starts and stops scheduled conferences.
- Monitors ongoing conferences and the updated status of those conferences.
- Executes commands against ongoing conferences.

LiveService acts as the backend for conference monitoring while the client-side applet, Conference Control Center, acts as the front-end for interacting with ongoing calls.

TMSDatabaseScannerService

This scanner service checks the connection status, call status, and system configuration of existing systems. It pauses for 15 minutes after a scan has finished.

If a system is unavailable, Cisco TMS will display the system as giving "No HTTP response" until the next scan, or until receiving another response from the endpoint.

To improve response times, Cisco TMS runs an additional connection status check every 30 seconds for infrastructure systems.

TMSSchedulerService

This service launches events at set times, such as:

- System restore
- System upgrade
- Active Directory phone book source updates

The service will also remind TMSLiveService to start a conference if needed.

TMSLiveService will keep track of all booked conferences, but lose this information if it is restarted.

TMSPLCMDirectoryService

This service is responsible for posting phone books to Polycom endpoints. They retrieve the phonebook from this service when requested via the remote control. This is similar to Corporate Directory in legacy TANDBERG endpoints.

TMSServerDiagnosticsService

This service runs scheduled checks on the health of the server platform itself. Current checks include:

- The server disk space. A ticket will be raised if less than 10% free space is available.
- The database size. A ticket will be raised if the database is at 90% of the maximum size.
- That all the other services are running. A ticket will be raised when one of the services is not running.

TMSSnmpService

This service is used for SNMP trap handling and polling including:

- A quick scanner that uses SNMP to query online managed systems on short intervals to detect whether any systems have become unreachable on the network unannounced.
- An SNMP trap handler that subscribes to the Windows SNMP Trap Service to collect and process SNMP traps sent by managed systems.
- A system discovery scan that uses SNMP broadcasts to discover new SNMP-capable systems on the network.

Cisco TMS Tools Application

TMS Tools is a helper application available from the **Start** menu on the Cisco TMS server. This application is used to modify database connection settings.

For more information, see Cisco TMS Tools, page 290.

Setting up Cisco TMS

As an administrator you need to tune Cisco TMS's behaviors to suit your organization's needs. This chapter provides instructions for configuring an initial setup, including user groups and permissions, key configuration settings, and configuration templates for endpoints.

Adding Release and Option Keys 21
How Groups and Permissions Work 22
Setting Up Initial Group Permissions 23
Enabling Active Directory Lookup 24
Adding User Accounts and Profiles 24
Reviewing and Setting Defaults 25
Using Configuration Templates 27

Adding Release and Option Keys

This is a description of how to install a license key which enables Cisco TelePresence Management Suite (Cisco TMS) features.

Release keys and option keys can be entered during installation, post-installation, or when upgrading. If no release key is entered during initial installation, Cisco TMS will run in a limited demo mode.

Getting Your Cisco TMS Release Key

To install or upgrade, you need a release key that is unique to your serial number and software version combination. You retrieve your release key by contacting Cisco.

Have your Cisco.com user ID and password available.

1. Go to **Cisco.com > Support**.
2. Open a Support Case using Cisco's Technical Assistance Center (TAC) Service Request Tool on the right side of this screen.

As an alternative, you can call Cisco's TAC

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
- EMEA: +32 2 704 55 55
- USA: 1 800 553-2447

Entering Keys During Cisco TMS Upgrades

Release key must be entered during installation to complete upgrades between major versions of Cisco TMS. When upgrading between minor versions, the existing release key is retained and reused automatically.

Adding a new release key can be done during installation. The Cisco TMS installation wizard will prompt you for a release key and option keys. Any previously entered keys will be shown.

Entering Release Keys Post Installation

If no release key was entered during installation, the server will run in trial mode. Add a release key by logging into Cisco TMS with **Site Administrator** privileges via the portal web page.

1. Go to **Administrative Tools > Configuration > General Settings**.
2. Enter your release key in the field labeled **TMS Release Key**.
3. Click the **Save** button.
   Changes take effect immediately. Your Cisco TMS release key will now appear in the bottom right corner of the application window.

Entering Option Keys Post Installation

Add an option key to an existing Cisco TMS installation by logging into Cisco TMS with **Site Administrator** privileges via the Portal webpage.

1. Go to **Administrative Tools > Configuration > General Settings > Licenses and Option Keys**.
2. Click the **Add Option Key** button.

If the key is verified successfully it will be added to the list of option keys displayed. Changes take effect immediately.

How Groups and Permissions Work

Administrators must plan their Cisco TMS deployment in terms of which features and permissions users need access to in Cisco TMS.

This is controlled through group membership, group permissions, and system permissions. All permissions in Cisco TMS are set on a group level.

A user can be a member of multiple groups. Users who belong to more than one group are granted all of the permissions for all of the groups to which they belong.

Group Membership

There are three ways to add members to a Cisco TMS group:

- Editing the group itself.
  On the **Edit Group** page, click the **Add Members** tab to specify users you want to add to the group. You can also edit a user's groups going to **Administrative Tools > User Administration > Users** and editing the user.
- Assigning the user to a group automatically when the user's profile is created.
  Groups set as *Default Group* are automatically added to any new user that logs in.

  Note that after installation, the Site Administrators group is a *Default Group*, which is what allows the administrator to log in and start configuring Cisco TMS. See Setting Up Initial Group Permissions, page 23 for instructions on changing this setting and verifying that only approved administrators are members of this group.
- Active Directory Groups.
  Cisco TMS lets you import existing groups from Active Directory. Active Directory group memberships are automatically updated in Cisco TMS groups when the user logs in.

Note that it is not possible to manually edit groups created from Active Directory.

System Permissions

Permissions in Cisco TMS are a combination of feature permissions and system permissions:

- User Groups have permissions to control which portions/features of Cisco TMS a user has access to.
- System Permissions are used to control what a user can do to a particular system. There are default system permissions, folder permissions that apply to all systems in a particular folder, and individual system permissions.

Default permissions are given to a system when first added to Cisco TMS. This is controlled in **Administrative Tools > User Administration > Default System Permissions**, where you can set which permissions each group gets on newly added systems.

Setting Up Initial Group Permissions

For an initial setup, a basic set of permissions must be established by:

- Making sure that new users will not automatically have administrator rights.
- Creating a default group for new users with the desired baseline permissions.

Follow the steps below to specify access control and feature availability for users:

1. Create a new group to use for all users:
   a. Go to **Administrative Tools > User Administration > Groups**.
   b. Click **New** to create a new group.
   c. Name your new group as desired. For example, "All company users".
   d. Click **Save**.
2. Change the Default Groups:
   a. Go to **Administrative Tools > User Administration > Default Groups**.
   b. Clear all the check boxes except **Users** and your new group.
   c. Click **Save**.
   Any person who logs into Cisco TMS will now automatically be added to your new group, and given the permissions for that group.
3. Assign the default permissions you want all Cisco TMS users to have to the new group:
   a. Click on the group name in the Edit Group listing.
   b. Click **Set Permissions**.
   c. Check each permission you wish group members to have.

      For a starting point that gives users full access except to Cisco TMS configuration, check all permissions except those under **Administrative Tools**. Check a section heading to enable all permissions in that section.
   d. Click **Save**.
4. Ensure only intended users have Site Administrator access:
   a. Go to **Administrative Tools > User Administration > Groups**.
   b. Click on the **Site Administrator** group and click **Edit**.
   c. In the Members list, ensure only the users you wish to have administrator rights are listed. If any other accounts are listed, select them and click **Remove**.
   d. Click **Save**.
5. Change the Default System Permissions:
   a. Go to **Administrative Tools > User Administration > Default System Permissions**.
   b. Uncheck all permissions for the **Users** group, and assign the permissions you would like for the new user group.
   c. Click **Save**.

You can create additional groups with more specific permissions when you settle on a complete configuration—the permissions can be changed at any time.

Enabling Active Directory Lookup

Enable Active Directory lookup to make user information replicate automatically from AD to Cisco TMS at given intervals.

To enable AD lookup:

1. Go to **Administrative Tools > Configuration > Network Settings > Active Directory**.
2. Set **Lookup User Information from Active Directory** to *Yes*.
3. Enter the appropriate information in the remaining fields.

If you choose not to activate AD lookup, each user logging in to Cisco TMS for the first time will be prompted to enter their first name, last name, and email address.

Adding User Accounts and Profiles

To log into the Cisco TMS web application, users must have a Windows username and password that the server is configured to trust. By default, any local Windows user account will work, as well as any Active Directory domain user account if the server is a member of an Active Directory domain.

The first user to sign into Cisco TMS is automatically made an administrator and will have full access to Cisco TMS.

For each user that successfully logs into Cisco TMS, a user profile is created based on their Windows username. A user is authenticated by their Windows credentials.

While it is possible to create a user profile in Cisco TMS manually, this does not create a Windows user account, and deleting a user profile in Cisco TMS does not alter the user's actual Windows user account.

Four personal information fields are mandatory:

- **Windows username**
- **First name**
- **Last name**
- **Email address**

If these are not filled in, the user will be prompted to complete them on first sign-in.

Language setting

Each user can choose their own language to use within Cisco TMS. The following languages are supported for the main Cisco TMS web interface:

- English
- French
- German
- Russian
- Japanese
- Chinese (Simplified)
- Korean

The Smart Scheduler and mail templates have more languages available. If another language than the above mentioned is selected, that user will see English when browsing pages that do not support their language selection.

Cisco Collaboration Meeting Rooms Hybrid

For bookings with Webex to work, the user performing the booking must have Webex credentials in their Cisco TMS profile. This ensures that the correct user is associated with the meeting in Webex and can log in and operate the Webex conference.

Note: If adding multiple Webex sites to Cisco TMS, ensure that the user's credentials are valid for the Webex site they will use for booking.

The remaining fields are not mandatory, but are used for other Cisco TMS features.

Webex Site and User Credentials

To be able to add Webex in telepresence conferences, a **Webex Site**, **Webex Username**, and **Webex Password** must be set up for the conference owner in Cisco TMS.

The information can be entered manually for each user, or retrieved from Active Directory (AD). We strongly recommend using AD to simplify this procedure.

Either method of entering the Webex information can be used in conjunction with Single Sign On (SSO). When SSO is enabled, entering the Webex password is not required.

Note that:

- When Active Directory lookup is enabled, any manually entered usernames will be overwritten when the user's data is synchronized again.
- When single sign-on is enabled, any passwords entered manually into Cisco TMS will be ignored.

Reviewing and Setting Defaults

Most settings in Cisco TMS are configured automatically or have suitable default values for most organizations.

Below are important settings you should review and configure as part of your initial setup to ensure they meet your needs and to ease the configuration of other Cisco TMS features.

General Settings

Table 3 Settings found in Administrative Tools > Configuration > General Settings

Setting	Description
System Contact/Email	When filled in, these display a Contact link on the bottom of all Cisco TMS pages so users can easily contact you for help or questions.
Release Key/Option Keys	You can enter your release key and option key here if you did not do so during installation. If upgrading from a trial version or adding new options, this is where license information is entered.

Network Settings

Table 4 Settings found in Administrative Tools > Configuration > Network Settings

SNMP Community Name	This is a comma separated list of common SNMP community names Cisco TMS will use when discovering and adding systems to Cisco TMS. If you use a customized SNMP Community Name on your existing systems, be sure to add it to this list.

Table 4 Settings found in Administrative Tools > Configuration > Network Settings (continued)

E-mail Addresses to Receive System and Network Notifications	You should enter your email address here so Cisco TMS can send you notifications about discovering non-registered endpoints, system event failures, and other administrative messages. Multiple email addresses must be comma separated.
Automatic System Discovery Mode	This feature is enabled by default. It automatically adds systems Cisco TMS discovers to a folder in System Navigator, and configures their management properties to work with Cisco TMS. Cisco TMS configures the systems with basic settings from the "Discovered Systems Template". Modify this template to specify default settings that you wish all new systems to have.
Active Directory	These settings allow Cisco TMS to use Active Directory for its user and group settings. If the Cisco TMS server is a member of a domain, it is highly recommended you enable these settings by entering a valid Windows Domain account. The account does not need to be an administrator account, just a normal user account. If Lookup User Information... is enabled, when a new user profile is created, Cisco TMS will automatically populate as many of the fields in the user profile as possible from Active Directory. Allow AD Groups simplifies Cisco TMS Groups by allowing you to use Groups from Active Directory as Cisco TMS User Groups which automates which Cisco TMS groups a user belongs to.
Scan SNMP Capable Systems to Allow Quick Discovery of Inaccessibility	This setting will allow Cisco TMS to more quickly detect whether a system has gone offline. Enabling this is recommended.
SNMP Broadcast/MultiCast Address(es)	This is/are the network addresse(s) that were configured in the Cisco TMS Installer. Cisco TMS will send a SNMP query to these addresses to find new systems. If your network spans multiple networks, add the broadcast address for each, separated by commas to allow Cisco TMS to find systems automatically. Do not worry if all networks are not represented here as systems can also be added manually and through systems contacting Cisco TMS. To turn this scan off, enter the localhost address 127.0.0.1.
Enforce Management Settings on Systems	This setting is enabled by default and should remain enabled. This setting is essential to ensure systems are properly configured to point to your Cisco TMS server. The setting should be disabled on any lab TMS servers, so that they do not change management settings on production systems.
Advanced Network Settings	To account for diverse network configurations, Cisco TMS supports the notion of two networks that can access Cisco TMS: ▪ Internal LAN: this is usually the same as your organization's internal network. ▪ Public Internet/Behind Firewall: you may have systems that you wish to manage outside the organization's firewall or proxy. The public hostname used should resolve to an IP forwarded to the Cisco TMS server's IP address. Each system added to Cisco TMS has a Connectivity parameter where you specify which network identity Cisco TMS should use when communicating with the system. Note that Cisco TMS is still only connected to one physical LAN port and only one IP Address. Cisco TMS does not support multihomed networking.

Table 4 Settings found in Administrative Tools > Configuration > Network Settings (continued)

TMS Server IPv4/IPv6 Addresses	These were configured during installation and should be the IP addresses used to reach your Cisco TMS server. Cisco TMS supports dual stack (that is, it can communicate simultaneously using IPv4 and IPv6 addresses)
TMS Server Fully Qualified Hostname	The fully qualified domain name used to access your Cisco TMS server from the internal, or local, network. This setting will be used with systems that support DNS and must be configured correctly. If the server has no hostname that is usable, enter the IP address that systems would use to reach Cisco TMS.
TMS Server Address (Fully Qualified Hostname or IPv4 Address):	The fully qualified domain name used to access your Cisco TMS server from an outside network, if different from the local hostname. This setting must be configured to use features such as SOHO/Behind Firewall support. If the server has no hostname that is usable, enter the IP address that systems would use to reach Cisco TMS.
Automatic Software Update	This functionality allows Cisco TMS to automatically check over a secure link for new software available for your systems, and notify you of your Service Contract status for your Cisco Systems. No personal information is sent during this communication except the system identifying information such as serial numbers and hardware identifiers. If you do not wish to have Cisco TMS check for software, you can disable this feature. If your network requires a web proxy to reach the internet, configure the properties for it here.

Mail Settings

Open **Administrative Tools > Configuration > Mail Settings**. These settings were configured during the Cisco TMS installation. However, if your mail server requires SMTP Authentication, specify the username and password here. The settings will be validated when you click **Save**.

You can also specify a different port for your SMTP server by using <ip address>:<port>. Example: 10.11.12.13:1234.

Conference Settings

These settings control most of the behaviors of Cisco TMS for scheduled calls and for monitoring of active calls.

Table 5 Settings found in Administrative Tools > Configuration > Conference Settings > Conference Create Options

Default Bandwidth	This is the default bandwidth suggested for H.323 and SIP calls when scheduling conferences.
Default ISDN Bandwidth	This is the default bandwidth suggested for ISDN calls when scheduling conferences.
Set Conferences as Secure by Default	Cisco TMS understands the ability for systems to support encryption or not, and this setting will control the default behavior for conferences. *If Possible* is the default and will enable encryption when all systems in a call support encryption. If one system in the call doesn't support encryption, the call will go through without encryption. **Note:** If an endpoint that supports encryption has encryption set to *Off* and is added to a conference which is encrypted, encryption will be set on the endpoint, and this setting will persist after the conference has ended, until set to *Off* on the endpoint itself.

Using Configuration Templates

A common administrative need is to apply a common group of settings to more than one system. Configuration templates in Cisco TMS allow you to define a set of configuration parameters to be applied to several systems in one

operation.

The template can include configuration choices for different system types, and Cisco TMS will only apply the settings that are valid for the individual system being updated.

As part of the default installation, Cisco TMS creates a template named **Discovered Systems Template**, containing a group of settings that will be automatically applied to all systems added to Cisco TMS by automatic system discovery, if enabled. For more information on system discovery, see How Systems are Added to Cisco TMS, page 48.

Administrators can define multiple templates, and may choose to apply them:

- manually per system
- automatically as systems are added to Cisco TMS
- every time the system is booted
- persistently at scheduled intervals. Note that the first application of the template will be performed immediately after saving. Subsequent applications will follow the configured schedule.

The software version and the current template data on which it is based on is as follows:

Cisco TMS 15.11	CE 9.12.1.4fe8516fb6e

Creating a New Configuration Template

To create a new configuration template:

1. Go to **Systems > Configuration Templates**.
2. Click **New Configuration Template**.
3. Enter a descriptive **Name** for the new template.
4. Select the settings you want to include in the template using the check boxes and drop-down menus. For field descriptions, see Configuration Templates, page 151.
5. Go to the **Select Advanced Settings** tab to add specific settings for certain systems by adding a filter, or leave the filter field empty to get a complete list of setting per system/system type.
   a. Choose the type of system and/or type a part of the setting you are looking for.
   b. Click **Search**.
   c. From the resulting list, select settings you want to add for the system type using the check boxes.
   d. Click **>** to move them to the list of selected settings.
   e. Click **Save**.
   Any setting selected in the **Select Advanced Settings** tab will now also be available in the **Template Settings** tab, to be used in the configuration template.

Viewing a Configuration Template

Click the action drop-down **View** for a configuration template to display the settings that will be set on the selected systems.

Editing a Template

This procedure uses the auto-created **Discovered Systems Template** as an example:

1. Open **Systems > Configuration Templates**.
2. Click on **Discovered Systems Template**.

   The **Type** for the settings in this template is *Other type* because they are Cisco TMS configuration settings, not configuration options from the device's commands itself.

3. Use the drop-down action button and click **Edit** to see the **Edit Settings** page.
   All templates have some common Cisco TMS settings added to them to start with, such as **Zones** and **Phone books**.
4. To add more settings to the template, click on the **Select Advanced Settings** tab.
   To see a list of all available settings, simply leave the Filter box blank and the drop down set to *All Systems* and click **Search**. From this view, you can chose from all the template settings available in Cisco TMS and add them to the list to be shown on the **Template Settings** tab.
5. Add or remove settings to the template by marking a setting's check box and using the arrow buttons to add or remove it from the list on the right.
6. Once the desired changes have been made, click on the **Template Settings** tab to return to the previous view.
7. On the **Template Settings** tab, enable or disable individual settings with their check boxes and set the values to use for each setting.
8. When finished, click **Save**.

Applying Templates to Systems

A template can be applied to one or many systems at once, but any one system can only have a single template applied to it at a time.

To apply a template to one or more systems:

1. Go to **Systems > Configuration Templates**.
2. Click the action drop-down button and select **Set on Systems**.
3. Select a system by clicking on it. Multiple systems can be selected by holding the `Shift` or `Control` keys when clicking on a system. Use the **< >** buttons to add and remove systems to the list.
   a. Add systems to the **Once** tab, to apply the template one single time.
   b. Add systems to the **Persistent** tab to make Cisco TMS re-apply the template according to the **Recurrence Interval** set for the template.
      Note that the first application of the template will be performed immediately after saving. Subsequent applications will follow the configured schedule.
4. Click **Set on Systems** to start the task.
   Applying the template to systems will be performed as a background task on the Cisco TMS server.
5. You can view the status of the job on the page **Systems > Configuration Templates > Configuration Template Activity Status**, see Configuration Template Activity Status, page 155 .

Creating a New Configuration Template from an Existing Template

1. Hover over the template you want to copy from, open the drop-down menu and select **Copy**.
   Cisco TMS will open the **Template Settings** page.
2. Modify the name and settings of the configuration template as desired.
3. Click **Save**.

Custom Configuration and Commands

For some systems, there is an option to add custom commands and configuration to the configuration templates. These behave differently from the predefined settings.

See the documentation for your system for the syntax.

- For configuration, the systems use XML from the **configuration.xml** document.
- For commands, the systems use XML from the **command.xml** document.

On Cisco TelePresence endpoints these files are available on the system's web server in the **Diagnostics** or **XML Files** section.

On Cisco VCS you can provide multiple custom configurations or commands by putting all of them in a single Command or Configuration root tag.

An example of custom configuration for E20, MXP Series, C Series and EX Series that changes the system name to "System name test" is

```
<Configuration><SystemUnit><Name>System name test</Name></SystemUnit></Configuration>
```

For Polycom HDX Endpoints you have the option of a **Custom Configuration** template setting. This template setting can be used when editing and creating a new template. An unlimited amount of commands and configurations can be added if you need functionality the stored settings do not provide. Separate the commands and configurations with a comma.

Routing

This chapter explains the methods used by Cisco TMS to route calls between systems using different protocols and networks, and how Cisco TMS selects network devices to optimize these connections.

Before you can configure routing in Cisco TMS, you must have an overview of your telepresence network dial plan, and which protocols and infrastructure your systems have in place.

Introduction to Routing 31
Protocols and Call Control 34
What Infrastructure Does Cisco TMS Use for Routing? 35
How Zones Work 38
Setting up an IP Zone 39
Setting up an ISDN Zone 41

Introduction to Routing

During the booking process, Cisco TMS tries to create a route between participants in a conference when one of the following actions takes place:

- The user clicks **Save Conference**.
- The user clicks the **Connection Settings** tab.
- A Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA) client saves a conference.

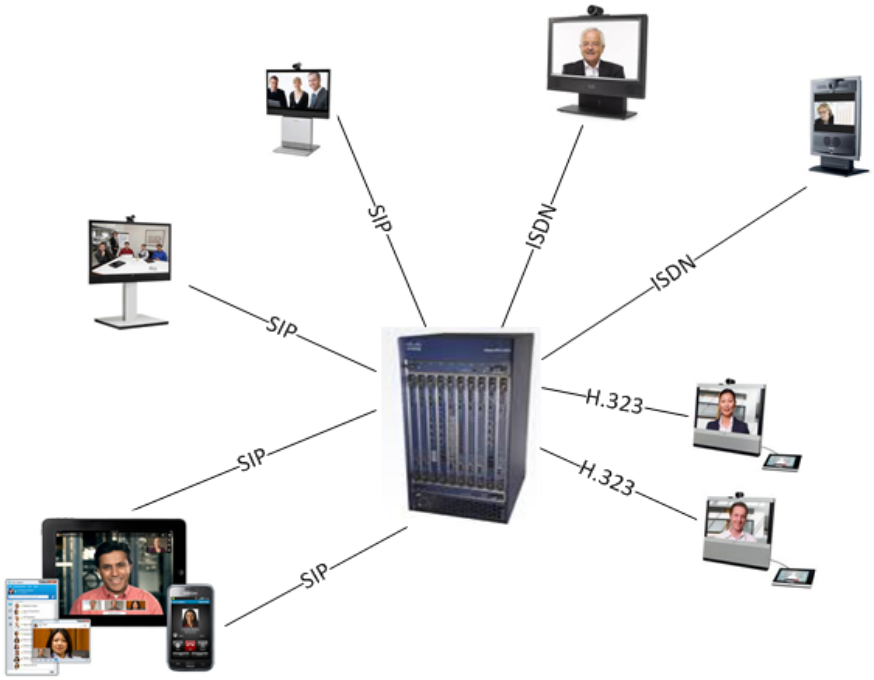
When a conference is saved, corresponding dial-in numbers for the conference are distributed via email to the organizer and/or participants. The route created by Cisco TMS is a suggestion and can be changed to another valid route during booking by clicking on the **Connection Settings** tab. If Cisco TMS is unable to create a route between all participants, the action fails, and an error is displayed. The administrator can then make changes, such as removing some participants, so that a route can be created.

Whenever a conference is edited and updated, Cisco TMS creates a completely new route (the old route is not taken into account when doing this). Even the smallest change to a conference could therefore create new dial-in numbers.

Cisco TMS will not take the initiative to reroute a conference. This means that for example:

- If you change your number range on a TelePresence Server that has future conferences already routed by Cisco TMS, all these future conferences on the TelePresence Server will assume the old dial plan. Run Conference Diagnostics, page 283 to identify issues with these future conferences.
- If a conference is booked on SIP for a SIP-enabled system, and then SIP is disabled for that system, Cisco TMS will understand that SIP is not enabled for this system any more but will not change the protocol for that call leg in the conference booked before the change to the system was made.

A conference can be split into several legs depending on how many participants there are, and each leg can use a different protocol.



This diagram shows a TelePresence conference that includes eight legs over multiple protocols.

Cisco TMS uses zones and distribution to define which MCUs will be used depending on the systems involved in a conference. Zones are also used for routing ISDN.

When booking using any Cisco TMS Extension that relies on the Cisco TMSBA, it is not possible to edit the route Cisco TMS has created for the conference. The only way to edit the route during booking is to use the Cisco TMS booking interface.

The Main Participant

The most important Cisco TMS concept in routing is the Main participant.

The Main participant is the system that hosts the conference. This can be either an MCU, or a system with multisite if there are more than two participants. If the conference is point-to-point then either system can be the Main. If booking from the Cisco TMS web interface, you can choose which participant you want to be the Main from the drop-down menu.

Cisco TMS decides which participant will be the Main based on the following criteria:

- The option selected in:
  - **Administrative Tools > Configuration > Conference Settings > External MCU Usage in Routing**
  - **Administrative Tools > Configuration > Conference Settings > Preferred MCU Type in Routing**
- Whether the conference includes immersive endpoints or MCUs with immersive capabilities.
- IP/ISDN Zones.
- Which gatekeeper systems are registered to.
- Which protocol each system supports, for example, whether a gateway or interworking is required.
- Encryption.
- Bandwidth.

If an external main participant is required, Cisco TMS compiles a prioritized list of possible main participants based on the criteria above. Cisco TMS chooses the first available participant to be the Main participant. If multiple bridges have the same priority, one of these is selected at random.

If you have manually added an MCU to the conference during booking, the route with this MCU is chosen.

The order in which Cisco TMS prioritizes the above criteria could change from one release of Cisco TMS to the next.

You can use scheduling logging at INFO level to see how Cisco TMS compiled the prioritized list. See Log Overview, page 307 for further details.

The following must be noted:

- There can only be one Main participant per conference.
- The Main participant can be changed once the conference has started using **Conference Control Center**. In this case the conference will be torn down, rerouted and reconnected.
- If one of two sides of a call leg is an MCU, the MCU is always the Main system.
- Cisco TMS communicates with the Main system to send conference disconnect and mute requests.
- Cisco TMS monitors the Main system to provide conference information for **Conference Control Center**.

The default is that the Main participant places all calls in a scheduled conference, however in One Button To Push conferences, systems dial into the Main participant instead. It is also possible to edit the connection settings for a conference during booking (if using the Cisco TMS booking interface) so that systems dial into the Main participant. This is not possible using the Cisco TMSBA. This option is not editable here for cascaded conferences.

Changes made to an ongoing conference in **Conference Control Center**, for example Mute All, or Disconnect, are actioned only on the Main participant, which then carries out that action on all the other participants. The only exceptions to this are Set Mic Off and Send Message, which are actioned on the individual participants.

Allocation

For a scheduled conference, allocation of systems takes place at the conference start time, unless you are using Early Join. Cisco TMS allocates the Main participant first, and then all other participants. If the Main participant cannot be allocated and MCU failover is unsuccessful, the conference itself will fail and no further allocation will take place.

Allocation means that Cisco TMS attempts to connect to the system to do the following:

- Encryption is set on the main participant.
- Feedback receivers are set on endpoints and bridges.
- The conference is created and the settings selected in the **MCU Settings** or **TelePresence Conductor Settings** tab in the booking page are applied to the bridge.
- Ad hoc calls that the endpoints are participating in are disconnected, unless the conference that is about to start is a One Button To Push or No Connect conference.

Cisco TMS will retry allocation according to the value set in **Administrative Tools > Configuration > Conference Settings > Allocation attempts for scheduled calls**.

If connection to the bridge or endpoint fails at any time, allocation of that system fails.

Once allocation for a system is successful,Cisco TMS sends the dial command for that participant. If dialing fails, Cisco TMS will retry according to the value set in **Administrative Tools > Configuration > Conference Settings >Connection Attempts for Scheduled Calls** unless the user has deliberately rejected the call.

Unmanaged Bridges

As Cisco TMS does not connect to an unmanaged bridge, much of the information above does not apply when an unmanaged bridge hosts a conference, even though it will still be the Main participant in the conference. For more details see What Infrastructure Does Cisco TMS Use for Routing?, page 35.

Protocols and Call Control

Both IP and ISDN are supported in Cisco TMS, as is interconnection between the two.

IP

Cisco TMS supports two call control devices:

- Cisco TelePresence Video Communication Server
- Cisco Unified Communications Manager.

Their respective capabilities are listed below:

- Cisco VCS
  - SIP registrar
  - H.323 gatekeeper
  - can route calls to a Unified CM
- Unified CM
  - SIP only
  - can trunk calls to a Cisco VCS

For further information on configuring Cisco VCS see:

Cisco TelePresence Video Communication Server Administrator Guide

To configure Cisco VCS with Unified CM see:

Cisco TelePresence Video Communication Server Cisco Unified Communications Manager Deployment Guide

Your choice of call control solution will dictate how Cisco TMS routes scheduled calls. For example, for systems registered to Unified CM, Cisco TMS will assume that the system can only use SIP.

ISDN

Cisco TMS supports:

- ISDN networks and configuring a dial plan.
- mixed networks and can route ISDN - > IP and IP -> ISDN.
- endpoints that have both IP and ISDN capability.
- connections between IP sites over ISDN.

How Call Protocols are Prioritized

Protocol priority depends on **Preferred Protocol in Routing** setting in Conference Settings page. By default this option is set to SIP hence the priority goes to SIP over H323. You can use zones to specify whether Cisco TMS prioritizes IP or ISDN, see How Zones Work, page 38 .

You can also configure the following settings in **Administrative Tools > Configuration > Conference Settings**:

- **Prefer H.323 ID over E.164 Alias**: choose whether to favor dialing H.323 ID or E.164 alias when using H.323.
- **Use Flat H.323 Dialing Plan When Routing Calls**: Cisco TMS assumes every system can dial every system.

The protocols that Cisco TMS will use to route individual systems in scheduling are set per system in **Systems > Navigator >** select a system **> Settings > TMS Scheduling Settings**.

What Infrastructure Does Cisco TMS Use for Routing?

MCU

An MCU (Multipoint Control Unit) is a conference bridge that can host a number of conferences at the same time depending on its port allocation. Participants can dial in, or the MCU can dial out to them. Cisco TMS supports the following types of MCU:

- Cisco TelePresence Server
- Cisco TelePresence MCU Series
- Cisco TelePresence MPS
- Unmanaged bridge
- Cisco Meeting Server

For new telepresence deployments, we recommend using Cisco Meeting Server for optimum performance.

You can specify what type of MCUCisco TMS will prefer in scheduled conferences here: **Administrative Tools > Configuration > Conference Settings > Preferred MCU Type in Routing**.

You can specify when the MCU should be used in routing here: **Administrative Tools > Configuration > Conference Settings > External MCU Usage in Routing**.

If you have several similar MCUs in Cisco TMS, the MCU will be selected based on which zone the conference participants belong to, and the capability set of the systems in the conference: conferences including immersive systems will use a Cisco TelePresence Server or an unmanaged bridge configured as **Immersive**, if available. Otherwise any MCU can be chosen by Cisco TMS.

Cisco TMS supports both scheduling of SIP-trunked bridges and bridges registered to an H.323 gatekeeper or SIP registrar.

When booking using any extension that relies on Cisco TMSBA, including Smart Scheduler, it is not possible to change the default conference settings in **Administrative Tools > Configuration > Conference Settings**.

Note: If a user adds MCU to Cisco TMS or user group, it may take up to 30 minutes to reflect the auto selection of bridges in Cisco TMS.

Number Allocation

When routing a conference, Cisco TMS allocates a random number in the assigned ranges to the conference in the following manner:

1. Cisco TMS tries to find an unused number or alias on a bridge within a 4 hour window around the conference (4 hours before the start time and 4 hours after the end time) for both new and an edited conference.
2. Cisco TMS checks for 4 hour window around the conference irrespective of the **Extend Conference Mode** settings.
3. If there are no unused numbers or aliases during that time frame, Cisco TMS tries a 2 hour window, then 1 hour, 45 minutes, 30 minutes, 15 minutes, and finally settles on a number or alias that is unique for the exact duration of the conference.

This is so that back-to-back meetings are not allocated with the same number or alias unless no other number is available, so participants are not at risk of dialing into the previous conference.

For recurrent bookings, Cisco TMS uses the same number or alias for all occurrences. When a single instance of a recurrent meeting is edited, this single exception occurrence can get a different dial-in number.

This also applies to bridges behind TelePresence Conductor if variable alias patterns are used.

Managed MCUs Only

Cisco TMS gives each MCU port a number (starting at 1 for the first port and so on), and an alias (SIP URI/H.323 ID/E.164 alias). The first number and the step are configurable for each MCU in **Extended Settings**. For recurrent bookings Cisco TMS uses the same port number for all occurrences.

Cisco TMS reads the number of ports from the bridge, it is not aware of whether it is SD or HD quality.To differentiate in this way we recommend using a TelePresence Conductor.

Distribution

Administrators can configure Cisco TMS to calculate routing across several MCUs either to reduce cost and/or bandwidth, or to achieve the highest quality. This is known as cascading. See Distribution (Routing Modes), page 176

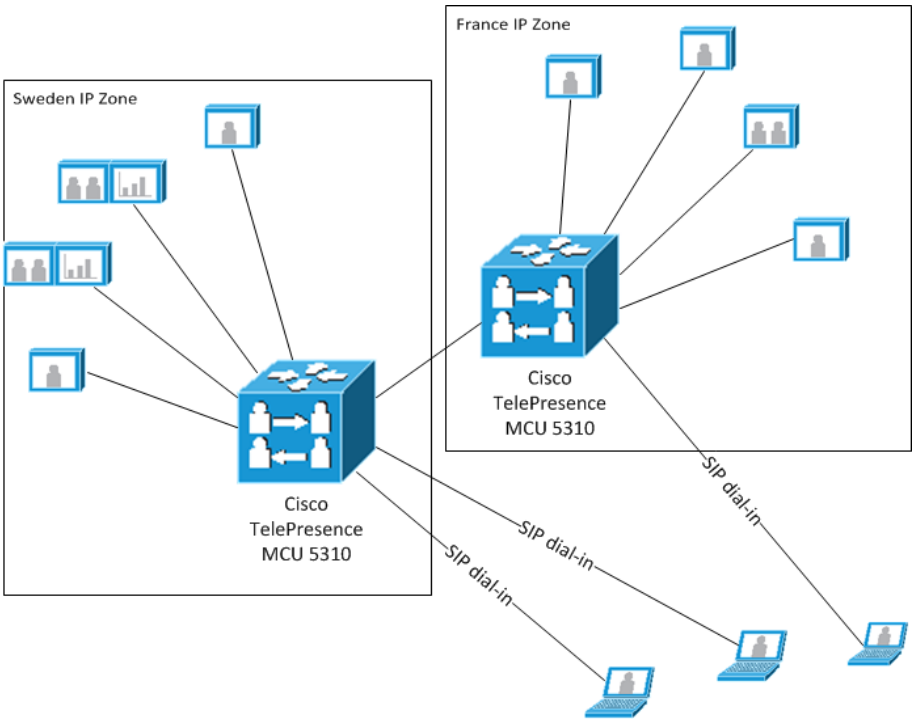
When Cisco TMS cannot fit all participants onto one MCU, the user is informed with an error during booking, as cascading does not happen automatically. The user must then choose between either Best Impression or Least Cost distribution, to cascade the call over two or more MCUs. For this reason cascading is only possible when booking using the Cisco TMS booking interface, it is not possible to cascade using the Cisco TMSBA. You cannot cascade MCU for ongoing conferences in Cisco TMS.

Note that the setting **Administrative Tools > Configuration > Conference Settings > Preferred MCU Type in Routing** is ignored when it comes to distribution.

Using different models of MCU in a cascade when manually configuring cascading is not supported in Cisco TMS.

When you book a distributed conference all MCUs generate a different conference dial-in number, all of these will be included in the confirmation email to participants. Once the number of participants corresponding to the number of available ports on the first MCU have dialed in, the next participant dialing in will get an error message and must try the next dial-in number listed.

This diagram illustrates a cascaded conference over two MCUs:



Note the following:

- Dial-ins do not have a designated IP zone.
- TelePresence Server only supports cascading if behind a TelePresence Conductor. Locally managed TelePresence Server's do not support cascading.
- Bridges added to Cisco TMS as external participants, rooms (now unmanaged endpoints) or phone book entries will not be included when creating a cascade.

Cisco TelePresence Conductor

If you are using a Cisco TelePresence Conductor in front of your MCUs, Cisco TMS lets the TelePresence Conductor decide which MCU(s) to use in a conference.

Unmanaged Bridges

Cisco TMS gives each unmanaged bridge port a number (starting at 1 for the first port and so on). The first address configured for the bridge is port number 1, the next, port number 2. For recurrent bookings Cisco TMS uses the same port number for all occurrences.

Unmanaged bridges are always the least prioritized bridge when selecting the main participant, unless the conference contains one or more multiscreen participants, in which case any unmanaged bridge configured as **Immersive** will be preferred over a non-immersive bridge.

It is only possible to schedule participants to dial in to an unmanaged bridge.

Gatekeeper

When Cisco TMS wants to create a route between two or more systems, it looks at whether systems are registered to the same or different gatekeepers.

The Systems are Registered to the Same Gatekeeper

Cisco TMS knows they can dial each other - the gatekeepers do not have to be registered in Cisco TMS and can even be unsupported third party or legacy systems such as the TANDBERG Gatekeeper. Cisco TMS just checks whether the gatekeeper IP address value is the same for both systems.

The Systems are Registered to Different Gatekeepers

Cisco TMS must know whether there is a relationship between the gatekeepers to understand whether the two systems can dial each other.

If the gatekeepers are registered in Cisco TMS, it will look at neighbor zones or cluster relationships on the gatekeepers to see if they can dial each other.

If the gatekeepers are not in Cisco TMS, it assumes there is no relationship between them and will use IP dialing.

If you configure an IP zone with a Domain URL, then Cisco TMS understands this can be used for systems to dial one another. (See How Zones Work, page 38.)

ISDN Gateway

An ISDN gateway allows an IP network to call out to ISDN and ISDN to call into an IP network.

Your gateway does not need to be added into Cisco TMS, you simply add gateway information to your IP zone so that Cisco TMS knows what prefix systems in that zone should dial for ISDN. (See How Zones Work, page 38).

Extended Settings DID Mapping for Cisco TelePresence MCUs

In the settings for a Cisco TelePresence MCU in Cisco TMS you can implement Direct Inbound Dial (DID) mapping to create a list of DID numbers that Cisco TMS can use as ISDN dial ins for scheduled conferences. Cisco TMS matches

the numbers up with the E.164 aliases already set up for conferences on this MCU. This means you can produce an ISDN dial-in number for a booked conference instead of using a TCS4 dial in.

If you do not set up DID mapping, you can set a dial-in ISDN number for the gateway in the IP zone. Cisco TMS then creates a dial in using the ISDN number of the gateway plus a * then the alias of the meeting you are going to join.

Note: The value of **ISDN Gateway DID Quantity** and **Numeric ID Quantity** fields must be same.

Cisco Unified Communications Manager

If a system is provisioned by Unified CM and there is a trunk to a Cisco VCS, Cisco TMS:

- will never use H.323 for the system even though it might support it.
- will never use IP dialing for the system.
- cannot verify that the trunk between the Unified CM and the Cisco VCS is set up correctly. Cisco TMS assumes that it will work and that the Cisco VCS is able to route calls to the Unified CM and vice versa.
- will always append the top level domain to calls going through the Unified CM - make sure the Cisco VCS accepts this kind of dial plan/numbering scheme.

How Zones Work

IP and ISDN zones are administratively defined concepts used to let Cisco TMS know which network a system is connected to. This feature ensures that users do not have to work out themselves whether calls are possible, which digits must be added for prefixes or telephone codes, or which network protocol to use.

During installation, Cisco TMS creates an IP zone and an ISDN zone, both named "Default". You need to add more zones after installation to implement a network that goes beyond one single location. The administrator defines the zones that represent their network, and systems in Cisco TMS are associated to these zones.

- Systems in the same IP zone will always connect using IP by default when they are booked via Cisco TMS.
- If you only want to use ISDN between systems in a location, they should be part of an ISDN zone.
- Systems that will never connect on ISDN (except through a gateway) should not be part of an ISDN zone.

Zones in Cisco TMS enable systems and MCUs to use the correct international dialing codes, protocols and communication technology when:

- using ISDN between countries (area codes within the same country).
- selecting whether a system should use IP or ISDN.
- inserting the correct prefix for IP systems when using an ISDN gateway.

Note: Cisco TMS also supports IP Zones for Cisco Meeting Server.

ISDN Zones

ISDN zones define the ISDN network in a location. A location is an area where all systems share the same ISDN dialing behavior. A location could be as small as a building or as large as an entire city or country, but all the systems assigned to a zone must share the following ISDN dialing information:

- **Country/Region** - Defines which dialing rules to use. For example, whether to dial 011 or 00 for international calls.
- **Area code** – Allows Cisco TMS to make determinations about long distance dialing.
- **Line prefixes** – Defines any prefix digits – such as dialing 9 to get an outside line from a PBX.
- **Digits to dial for internal calls** – How many digits to dial when making calls between systems in the same ISDN zone. For example, if you are using a PBX, it may only be necessary to dial the last 4 digits between two local systems.

- **Area Code Rules** – Used to further tweak the dialing behavior of Cisco TMS with regard to local and long distance calling.

How many ISDN Zones you need to represent your network depends on how many different ISDN dialing behaviors there are. If systems share identical settings for the properties above, they can share the same ISDN Zone.

All ISDN numbers in Cisco TMS are stored as "fully qualified numbers"; the number is entered and shown as the full number, including country code. For example: a US phone number is shown as +1 555 7094281, and a Norwegian phone number is shown as: +47 67125125. The same number can then be used by any system in the world because Cisco TMS (with ISDN zones) knows how to modify the number so that any system it manages can dial it properly. For more information see Setting up an ISDN Zone, page 41

IP Zones

An IP zone performs two roles:

- Creating the idea of locality in an IP network.
- Providing information for connecting from the IP network using gateways and URI dialing.

IP zones are purely logical entities and do not necessarily map to physical boundaries of network segments. Cisco TMS uses IP zones to determine which systems can be considered local or close to each other. This affects, for example, the choice of an MCU, where a local MCU may be preferred. IP zones also provide gateway and dialing information about the network a system is attached to. If an organization does not have widespread IP connectivity between sites and prefers to use ISDN when making certain connections, IP zones also provide controls for this. For more information see Setting up an IP Zone, page 39

IP-ISDN-IP Calls

These calls run through two different gateways and may have lower connect success rate and lower quality compared to other calls. Due to the reduced call quality, IP-ISDN-IP calls will be the lowest priority call route.

Between systems with no ISDN bandwidth, however, IP-ISDN-IP calls may be the only call alternative.

When placing a call between two systems in different IP Zones where **Prefer ISDN over IP calls to these IP Zones** is defined and neither system has ISDN bandwidth, **Allow IP-ISDN-IP** must be enabled for the zone for Cisco TMS to allow these IP calls by connecting the call through the ISDN Gateway defined in the zone. Without enabling this setting, the call will *not* be allowed in Cisco TMS.

Prerequisite

To use IP-ISDN-IP routing in Cisco TMS, your ISDN gateway must be configured to use * as a TCS-4 delimiter. This is the default setting on many gateways, but may need to be modified or set up on some.

For more information about TCS-4 dialing, see your ISDN gateway's documentation.

Setting up an IP Zone

When setting up an IP zone, you specify which prefixes to dial in order to use a gateway. By specifying the prefix rather than the gateway directly, Cisco TMS is given the flexibility to use load-balanced gateways, and even gateways not supported by Cisco TMS.

1. Go to **Administrative Tools > Locations > IP Zones**.
2. Click **New**.

3. Fill in the fields described in the table below.

Table 6 IP Zone settings

Sections and fields	Description
IP Zone	
Name	Set a name for the IP zone.
Gateway Resource Pool	
ISDN Zone	Specify which ISDN zone you want the below gateway prefixes to use. Note that the Gateway Resource Pool will not work correctly unless this setting has been specified.
URI Domain Name	Cisco TMS will always use URI dialing between two locations where this setting is filled in, thereby ignoring the IP/ISDN preferences defined at the bottom of this page.
Gateway Auto Prefix	The prefix needed to dial a video ISDN number from this IP zone using a Gateway.
Gateway Telephone Prefix	The prefix needed to dial an audio ISDN number from this IP zone using a Gateway.
Gateway 3G Prefix	The prefix needed to dial a 3G mobile phone number from this IP zone using a Gateway.
Dial-in ISDN Number	These numbers are used for generating TCS-4 numbers like +15551231234*99999 when Cisco TMS is routing a call: – from PSTN and into an IP zone. – from a 3G network and into an IP zone. After the settings are saved, these numbers will both be shown as qualified numbers.
Dial-in ISDN Number for 3G	
Allow IP-ISDN-IP	Check to allow IP-ISDN-IP calls, running through two different gateways. For more information, see IP-ISDN-IP Calls, page 39.
Prefer ISDN over IP calls to these IP Zones	Lists of IP zones to which: – ISDN is preferred over IP. – IP is preferred over ISDN. The lists are used when scheduling calls between IP zones. Move zones between lists by selecting them and clicking the arrow buttons.
Prefer IP calls over ISDN to these IP zones	

Setting a Zone on One or More Systems

1. Go to **Administrative Tools > Locations > IP Zones**.
2. Hover over the IP Zone Name in the list, and use the drop-down menu to select **Set On Systems**.
3. Choose the systems to associate with this particular IP zone.
4. Click **Save**.

Setting up an ISDN Zone

1. Go to **Administrative Tools > Locations > ISDN Zones**
2. Click **New**.
3. Fill in the fields described below.

Table 7 ISDN Zone settings

Section/field	Description
General	
ISDN Zone Name	Name of the ISDN zone.
Country/Region	Which country this zone is situated in. This enables Cisco TMS to choose the correct country code and international dialing prefixes.
Area Code	Which area code this ISDN zone is situated in. This enables Cisco TMS to choose the correct area code rules.
Line	
To access an outside line for local calls, dial	Prefix needed to obtain an outside line in this ISDN zone.
To access an outside line for long distance calls, dial	Prefix needed to obtain an outside line for long distance calls in this ISDN zone.
Internal Calls	
Number of digits to use for internal ISDN calls	Number of digits used for internal dialing between systems in the zone. The first digits in the number will be stripped from the number when dialing between systems in this ISDN zone.

Example

A Swedish phone number in Stockholm has a number layout that looks like this:

Country code (`+46`); Area code (`08`); local number (`12345678`)

The dialing pattern then needs to be like this:

- From within Stockholm: only dial the local number `12345678`
- From Gothenburg (within the country, outside the area code): dial `08 12345678`
- From outside of Sweden: dial: `+46 8 12345678`

The 0 in front of 8 (in the area code) has to be removed when dialing this number from outside the country. This is therefore seen as a prefix to dial between area codes rather than part of the area code itself.

The systems should only be configured with the local ISDN number: 12345678, but with the correct area and country code in the ISDN Zone. In the ISDN Zone the area code should be stored as just 8, since Cisco TMS will add a 0 in front of it when dialing between Swedish area codes, and add +46 when dialing from outside Sweden.

There are some exceptions to these rules, but Cisco TMS is configured to implement these exceptions:

- Some countries, like Norway, do not use area codes; the area code field in the ISDN zones in these countries should therefore be left empty. An example of a valid number is +47 12345678.

- Other countries, like Italy, include the leading zero in the area code even when being dialed into from outside the country. This means that the area codes in the Italian ISDN zones must include the leading zero. An example of a valid number is +39 02 12345678.
- There are also countries, such as Switzerland, that include the area code with the leading zero when dialing within an area code and when dialing within the country, but remove the leading zero when being dialed into from outside the country. Cisco TMS is configured to recognize this, which means that the area code for ISDN zones in Switzerland should only include the area code without the leading zero. For example: +41 33 1234567 and 033 1234567.

Creating area Code Rules

Area code rules are typically added to ISDN zones used in the US to set up 10-digit dialing and area code overlays. Area code rules determine how ISDN numbers are dialed from one area code (the area code set for the location) to other area codes.

In a US phone number, for example +1 (123) 456-7890, the area code consists of the digits in brackets (123), and the prefix consists of the digits 456 (in this example).

To add or edit an area code rule for a location:

1. Go to **Administrative Tools > Locations > ISDN Zones**.
2. Click on an existing zone to view it, or start creating a new zone by clicking **New** and following the instructions above.
3. Click **Area Code Rules** when viewing or editing an ISDN zone to open an overview of existing rules for area codes in ISDN zones.
4. Click on an existing rule, or start creating a new one by clicking **New**.
5. Fill in the fields described below:

Table 8 Settings for area code rules

Field	Description
When dialing from this area code to the following area code	Specify the area code this rule should apply for. For example, if you want the rule to apply every time dialing 555, specify 555 in this field.
With the following prefixes	The prefix is the first three digits of the base number. Leave blank if you want the rule to apply for all calls made to the area code in the above field.
Include Area Code	Check this if you want the rule to include the area code specified above in the call. For the US, check to enable 10-digit dialing.
Before dialing, also dial	Enter a string here to include in front of the dial string created by this area code rule (before the area code and prefixes specified in the first two fields above).
Strip digits for zone's local outside line access	Check to strip the outside line prefix (set in **Administrative Tools > Locations > ISDN Zones > Line** section) from the number you are going to dial.

6. Click **Save**.

When an area code rule is used, prefixes from the ISDN zone are still used, but domestic dialing behaviors (such as inserting a 1) are ignored by Cisco TMS.

Setting a Zone on One or More Systems

1. Go to **Administrative Tools > Locations > ISDN Zones**.
2. Hover over the zone and use the pull down arrow. Click **Set on System**.

3. Choose the systems to associate with this particular ISDN zone.
4. Click **Save**.

System Management Overview

This chapter presents the different system types that can be managed, explains the different ways they can be managed, and how Cisco TMS communicates with systems inside and outside the organization's network.

Supported Systems 44
How Endpoints are Managed by Cisco TMS 44
Infrastructure Systems 46
Systems Behind a Firewall/NAT 47
How Systems are Added to Cisco TMS 48
How Cisco TMS Communicates with Managed Systems 49
How Persistent Settings Work 52

Supported Systems

System Types Supported by Cisco TMS

All systems in your telepresence deployment can be added to Cisco TMS:

- telepresence endpoints
- Cisco VCS and legacy gatekeepers
- MCUs and TelePresence Server
- manager systems such as Unified CM and Cisco TelePresence Supervisor MSE 8050
- Cisco TelePresence Conductor
- gateways
- content and recording servers

Endpoints or bridges not directly supported by Cisco TMS or Cisco TMSPE can be added as Unmanaged Endpoints or Unmanaged Bridges, where Cisco TMS does not have any control over the system, but makes it available for booking.

System Locations

All systems that you add to Cisco TMS are given a system connectivity status based on their network location. These classifications determine the Cisco TMS functionality available to them.

- Systems on the organization's network have the most extensive management support. Infrastructure systems *must* be on the organization's network. The connectivity for these systems will be reported as *Reachable on LAN*.
- Endpoints in public behave similarly to endpoints on the organization's network.This system connectivity is described as *Reachable on Public Internet*.
- Endpoints behind a firewall/NAT are supported for booking, software upgrades, phone books, and reporting. System connectivity for these systems is reported as *Behind Firewall*.
- A system not reachable by Cisco TMS can be supported for booking. The system connectivity status for such systems is *Inaccessible*.

How Endpoints are Managed by Cisco TMS

How an endpoint is managed by Cisco TMS and which functionality is available for it depends on how it is added:

- Adding the endpoint directly to Cisco TMS provides the most extensive control of the system.
- Provisioning the endpoint using Cisco TMSPE does not add the endpoint itself to Cisco TMS.
- Adding endpoints already registered to Unified CM to Cisco TMS provides limited management options.
- Adding an endpoint as an Unmanaged Endpoint is normally done for any system that is not directly supported by Cisco TMS.

All management modes except Cisco TMSPE provisioning make the endpoints bookable in Cisco TMS.

Cisco TMS Controlled

Systems added to Cisco TMS without other application management layers have the most services available to them:

- View and edit system settings from the Cisco TMS web interface.
- Back up and restore configurations.
- Use persistent templates so that local changes on the system are regularly overwritten.
- Get tickets raised for the system in Cisco TMS when there is an issue.
- Upgrade software.
- Make phone books available.
- Monitor conferences using **Conference Control Center**.
- Get reporting on system usage.
- Book the system as a participant in conferences.

For instructions on adding systems to be controlled by Cisco TMS, see Adding Systems, page 54.

Cisco TMSPE Provisioned

The following features are available for systems provisioned by Cisco TMSPE:

- Software upgrades
- Phone books (note that this works differently than for Cisco TMS-controlled systems)
- Limited conference control/monitoring
- Reporting (User CDR)

Note that these systems cannot be booked as participants in conferences.

Also note that while it is possible to add endpoints to Cisco TMS after they have been provisioned, we do not recommend doing so. Regular phone book handling will not be possible, and the option to enforce management settings will be disabled.

For more information, see Provisioning, page 141.

Unified CM Registered

The following feature set is available to systems that are registered to Unified CM when added to Cisco TMS:

- Booking
- View settings
- Conference Control Center
- Phone Books
- Tickets

Fewer logs and less logging information will be available through Cisco TMS for systems registered to Unified CM.

For instructions on making sure your system is supported and adding it to Cisco TMS, see Adding Unified CM and Registered Endpoints, page 58.

Note: Cisco TMS supports the providing of CDRs for CUCM managed TC / CE endpoints that are added into Cisco TMS.

Unmanaged Endpoint

Adding an unsupported system as an unmanaged endpoint makes the system bookable in Cisco TMS, but gives no access to other features. Unmanaged endpoints are considered as single screen devices.

For instructions on adding these systems, see Adding Systems, page 54.

Changing Management Modes

For administrators migrating their call control infrastructure from Cisco VCS to Unified CM, Cisco TMS understands that a system being added from a Unified CM was already managed by Cisco TMS. It also recognizes that the two systems are the same and replaces the original system with the Unified CM-registered one, so that all the existing CDRs and scheduled future conferences are retained.

If a system that is direct-managed by Cisco TMS is registered to a Unified CM and then imported to Cisco TMS using **Add Systems > From List > Unified CM**, Cisco TMS recognizes that the two systems are in fact the same, and replaces the original system with the Unified CM-registered one, so all CDR and future conference data is retained.

Conference Diagnostics must be run after migrating an endpoint.

Infrastructure Systems

Infrastructure systems for call control and conferencing are supported for:

- Viewing and editing settings
- Reporting
- Monitoring
- Booking
- Ticketing

Note that infrastructure systems cannot be behind a NAT/firewall; they must be inside the organization's network.

Pre-registration is also not supported for infrastructure systems.

Booking

The booking of infrastructure systems such as MCUs and TelePresence Server is handled automatically; the user does not have to actively add an MCU, but may choose to do so, or to modify the automatic MCU selection.

The addition of systems like TelePresence Conductor or TelePresence Content Servers to a booking are optional.

Reservation

Note that if an MCU or gateway is booked with the conference type *Reservation*, all ports/resources on the unit are reserved, making the unit unavailable for further bookings during the scheduled time.

Monitoring

Cisco TMS constantly monitors the status of infrastructure systems by polling them every 30 seconds. For more information on how Cisco TMS polls systems, see TMSDatabaseScannerService, page 19.

Software Versions

Upgrading of infrastructure system software from the Cisco TMS interface is not possible.

If the software of an infrastructure system is downgraded to an earlier version, Cisco TMS may not be able to correctly read its settings. Purging the system from Cisco TMS and then re-adding it after the downgrade resolves this issue.

Systems Behind a Firewall/NAT

Systems behind a firewall or NAT are supported for booking, getting software upgrades, receiving phone books and being part of the statistics created in Cisco TMS.

Every 15 minutes and on boot, these systems send a Keep Alive signal which Cisco TMS responds to. Cisco TMS cannot contact the systems outside of these exchanges. The system status information for remote endpoints is therefore limited.

Unified CM

Note that Unified CM-registered systems must not be placed behind a firewall or NAT.

Booking

Some limitations apply when booking conferences that involve endpoints behind a firewall:

- Cisco TMS cannot make an endpoint behind a firewall dial out. The endpoint must therefore either be dialed into, or the person operating the endpoint must manually dial in to the conference.
- When booking conferences that include multiple endpoints behind a firewall as *Automatic Connect*, the conference must include an MCU or local endpoint with embedded multisite support.
  A point-to-point conference with *Automatic Connect* will not work for two systems behind a firewall/NAT, but will work as expected if one of the endpoints is local.

Statistics and monitoring

Statistics and monitoring of remote systems work the same way as for systems that are on the LAN, by sending HTTP feedback to Cisco TMS.

- Status and detailed call information (**status.xml** and **history.xml**) are sent to Cisco TMS every 15 minutes.
- Any changes to the configuration of the system (**configuration.xml**) will also be sent with the Keep Alive signal every 15 minutes.

Ad hoc calls will not be shown for systems behind a firewall, as TMSLiveService is not able to contact the system to get information about the call. For more information, see TMSLiveService, page 19.

Software Upgrades

When scheduling an upgrade for a system behind a firewall/NAT:

1. Cisco TMS will report that the upgrade went successfully, but the upgrade will have been put on hold.
2. The next time Cisco TMS receives a boot event from the system, the system will receive notice that an upgrade has been scheduled . In the reply to the boot event, Cisco TMS will send the endpoint a URL where it can get the software package.

   This URL is defined in **Administrative Tools > Configuration > Network Settings > General Network Settings** pane **> URL Where Software Packages Can Be Downloaded**.

For instructions on upgrading, see Upgrading Cisco TMS-Managed Endpoints, page 68.

Phone Books

The corporate phone book will work in the same way as if the system was located on a LAN; the endpoint will request phone book information from Cisco TMS, and the response will be returned as search results.

The legacy global phone book format is not supported for remote systems.

Configuration Templates

For remote systems, configuration templates may be applied on adding the system to Cisco TMS. If modified later, the update will be applied within 15 minutes.

Configuration Backup and Restore

Configuration backup and restore events are also scheduled and performed as responses to Keep Alive signals from the endpoint.

Note the following limitations to configuration backup support for remote systems:

- The **Compare Settings** tab in **Navigator** is not available.
- The **Backup/Restore Activity Status** list does not accurately report the status.

System Replacement

The **Replace System** feature is not available for remote systems. For more information about replacing systems, see Swapping a System, page 67.

How Systems are Added to Cisco TMS

When Cisco TMS successfully adds a system, the management settings needed for the system to communicate with Cisco TMS are automatically configured.

This applies to all system types except unmanaged bridges and unmanaged endpoints, and Cisco TMSPE-provisioned systems (which are not added to Cisco TMS, see below).

While accessing a web service on Cisco TMS (.asmx address) through IPV6 if you get an `Invalid URI` error in the Windows Server, then upgrade the .net framework to version 4.7 to rectify this error.

Automatic Discovery

New systems on the network are discovered in two ways:

- Boot and registration events over HTTP are detected by Cisco TMS.
- TMSSnmpService scans the network for SNMP-capable systems.

The **Automatic System Discovery Mode** setting controls what is done to the detected systems:

- If the setting is enabled, systems found during the scan will be added to the folder of your choice (by default, they will be added to **Discovered Systems**). Default configurations may also be applied.
- If disabled, discovered systems appear on a list of systems available to Cisco TMS, but are not added. These systems can be added manually by going to **Add Systems > From List**.

Note that Cisco TMS interprets a system that is not in any folder as being deleted (but not purged). If you have automatic system discovery enabled, but no default folder set up for discovered systems, the systems will be treated the same as if discovery was disabled.

Also note, when you add Unified CM to Cisco TMS, always add it with FQDN (Fully Qualified Domain Name). It helps Cisco TMS to communicate properly with Unified CM, specially when the Unified CM is in cluster.

By default, **Automatic System Discovery Mode** and **Automatic System Discovery for Endpoints Behind a Firewall/NAT**, are both disabled.

For instructions, see Using Automatic Discovery, page 55.

Manual Addition

If automatic system discovery is disabled, or does not work for the type of system you are adding, you can add systems for Cisco TMS control by manually entering IP addresses or an IP range, or DNS names. A persistent configuration template may be applied during this process.

Unmanaged bridges and unmanaged endpoints must also be manually added to Cisco TMS. Configurations for these systems must be manually set for each unit, as automatic configuration is not possible for unsupported systems.

For instructions, see:

- Adding by IP addresses or DNS Names, page 55
- Adding an Unmanaged Bridge, page 60
- Adding Unmanaged Endpoints, page 61

Through Unified CM

When a Unified CM is added to Cisco TMS, a list of telepresence endpoints registered to Unified CM is made available.

Administrators can use this list to add the endpoints to Cisco TMS for limited management.

For instructions, see Adding Unified CM and Registered Endpoints, page 58.

Provisioning

Provisioning using Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) is recommended as the most flexible and scalable way of registering and configuring large quantities of endpoints.

Note that this provisioning model does not actually add the endpoints themselves to Cisco TMS; the provisioning is user-based, not device-based. This also means that the configuration received by the endpoint will depend on the user signed in to the endpoint.

For more information on how provisioning works, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.

Pre-registration

Pre-registering endpoints in Cisco TMS is a legacy and smaller-scale alternative to provisioning. Up to 10 endpoints can be pre-registered at a time to any folder.

Pre-registration uses IP address, MAC address or, for legacy systems, serial number, to let the endpoint be recognized instantly when it comes online, added as a Cisco TMS-controlled system, and configured as specified during pre-registration.

Note that infrastructure systems may not be pre-registered.

See Pre-registering Endpoints, page 57 for instructions.

How Cisco TMS Communicates with Managed Systems

Cisco TMS uses HTTP/HTTPS when communicating with managed endpoints and infrastructure products. In addition, SNMP is used for communicating with some older endpoints, such as the Cisco TelePresence System MXP series.

Managed systems also initiate connections to Cisco TMS. Examples of such connections include phonebook requests, boot and registration events, and heartbeats from systems behind a firewall. Each Cisco TMS-managed system must therefore be configured with an External Manager Address, which is used for contacting Cisco TMS.

The Addresses that Systems Use to Contact Cisco TMS

You specify addresses that systems use for contacting Cisco TMS by going to **Administrative Tools > Configuration > Network Settings**.

- The IPv4, IPv6, and Fully Qualified Hostname addresses specified in the **Advanced Network Settings for Systems on Internal LAN** are used by systems that have their **System Connectivity** status set to *Reachable on LAN*.
- The Fully Qualified Hostname or IPv4 address specified in **Advanced Network Settings for Systems on Public Internet/Behind Firewall** is used by systems that have their **System Connectivity** status set to *Reachable on Public Internet* or *Behind Firewall*.

System Connectivity Status

The system connectivity status defines the network location of all systems managed by Cisco TMS. The status may be set by the administrator when adding the system, manually updated at a later stage, or modified automatically by Cisco TMS.

The available statuses are:

- *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations.
- *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237.
- *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237.
- *Behind Firewall*: This alternative will only be shown for endpoints that may be located behind a firewall/NAT. The system uses the same public network address setting as systems reachable on public internet.

By default, all systems are set to *Reachable on LAN*.

The **System Connectivity** status may be configured by going to **Systems > Navigator >** select a system **> Connection** tab **> System Connectivity**.

You can choose whether Cisco TMS will automatically modify your systems' connectivity status using **Administrative Tools > Configuration > Network Settings > Update System Connectivity for Systems**. If set to *Automatic*, Cisco TMS will change the status, if set to *Manual*, Cisco TMS will never change it from its current status.

Enforced Management Settings

If the **Enforce Management Settings on Systems** setting is set to *Yes* in **Administrative Tools > Network Settings > TMS Services**, Cisco TMS periodically pushes server information to systems:

- The Fully Qualified Hostname (if set) or the IP address (if the Fully Qualified Hostname is not set) is pushed to systems with **System Connectivity** status set to *Reachable on LAN*.
- The **TMS Server Address (Fully Qualified Hostname or IPv4 Address)** setting is pushed to systems with **System Connectivity** status set to *Reachable on Public Internet*.

Cisco TMS assumes that systems set to *Behind Firewall* are located behind a firewall or a router that uses network address translation (NAT). Cisco TMS is then unable to connect to the system, for example to instruct it to launch a call. Having a system set to *Behind Firewall* status will severely limit what you can do with the system in Cisco TMS.

Why Cisco TMS Changes the System Connectivity Status

If **Administrative Tools > Configuration > Network Settings > Update System Connectivity for Systems** is set to *Automatic*, Cisco TMS will in some cases change the **System Connectivity** status based on boot and registration

events sent by a system.

Whenever a system sends a boot or registration event, Cisco TMS compares the reported IP address with the value in the IP header's *Source IP Address* field.

If these two IP addresses are the same, Cisco TMS keeps the **System Connectivity** status the same as it was when the system was originally added to Cisco TMS.

If the two IP addresses are not the same, Cisco TMS will try to contact the system on the *Source IP Address* in the IP header:

- If the system responds to requests sent to this address, Cisco TMS compares the address the system used to reach Cisco TMS with the DNS addresses set in **Administrative Tools > Configuration > Network Settings**:
  - If the address used by the system is equal to the internal address (**Advanced Network Settings for Systems on Internal LAN > TMS Server Fully Qualified Hostname**) the system is set to *Reachable on LAN*. The same will be true if both the internal and the public addresses are set to the same DNS name.
  - If the address is equal to the public address only (**Advanced Network Settings for Systems on Public Internet/Behind Firewall > TMS Server Address (Fully Qualified Hostname or IPv4 Address)**), the system is set to *Reachable on Public Internet*.
- If the system does not respond to the request sent to the *Source IP Address* in the IP header, Cisco TMS changes its **System Connectivity** status to *Behind Firewall*.

Note: Admin must ensure to enter the correct IP and MAC address.

Examples

Here is an example registration event sent to Cisco TMS from a Cisco TelePresence System Integrator C Series system:

```
(...)
<PostEvent>
       <Identification>
              <SystemName>example_system</SystemName>
              <MACAddress>A1:B2:C3:D4:E5:06</MACAddress>
              <IPAddress>172.16.0.20</IPAddress>
              <ProductType>TANDBERG Codec</ProductType>
              <ProductID>TANDBERG Codec</ProductID>
              <SWVersion>TC4.1.2.257695</SWVersion>
              <HWBoard>101400-5 [08]</HWBoard>
              <SerialNumber>B1AC00A00000</SerialNumber>
       </Identification>
       <Event>Register</Event>
</PostEvent>
(...)
```

In the example above, the Cisco TelePresence Codec C90 reports its local IP address as `172.16.0.20`.

- A system is set to *Reachable on LAN*, and reports its IP address as: 172.16.0.20. The *Source IP Address* in the IP header is also: 172.16.0.20. Cisco TMS keeps the system as *Reachable on LAN*.
- A system is set to *Reachable on LAN*, and reports its IP address as: 172.16.0.20. The *Source IP Address* in the IP header is: 10.0.0.50. Cisco TMS then attempts to contact the system on 10.0.0.50. When the request times out, Cisco TMS changes the system to *Behind Firewall*.
- A system is set to *Reachable on Public Internet*, and reports its IP address as: 172.16.0.20. The *Source IP Address* in the IP header is: 10.0.0.50. Cisco TMS then attempts to contact the system on 10.0.0.50, and the network device at 10.0.0.50 is able to route the traffic back to the original system. The original system replies to Cisco TMS, and Cisco TMS keeps the system as *Reachable on Public Internet*.

Calendar Push Behavior

Cisco TMS sends lists of future bookings to endpoints that support the Meetings calendar feature. The bookings include subject, organizer, connection type, start time and so on.

The calendar pusher mechanism:

- updates all systems, waits for a minute, then starts again.
- pushes entries that are at most 72 hours in the future.
- pushes to all systems that have seen a calendar change since the last time it ran.

Endpoints present this Meetings calendar information in different ways depending on the model and software version.

How Persistent Settings Work

Persistent settings are a feature that allows the administrator to regularly enforce settings that are critical for operation on Cisco TMS-controlled endpoints and infrastructure systems throughout the network.

There are four persistent settings:

- **System Name**
- **H.323 ID**
- **E.164 alias**
- **SIP URI**

These settings can be specified either when the system is added or at a later stage by using the system's **Persistent settings** tab in **Navigator**.

The persistent settings will be set on the system every time Cisco TMS receives a boot event either via HTTP or SNMP.

Additionally, a persistent configuration template can be set for Cisco TMS-controlled endpoints and infrastructure systems. The template is set on the system at the same time every day, based on the first time the template was set on the system. For more information, see Using Configuration Templates, page 27.

Adding and Managing Systems

This chapter describes core tasks for managing your telepresence network, and reference material for all pages in the **Systems** menu.

Setting Up Default System Folders 53
Adding Systems 54
Managing Systems 65
Navigator 69
Ticketing Service 138
System Overview 140
Manage Dial Plan 140
Provisioning 141
Configuration Backup 150
Configuration Templates 151
System Upgrade 155
Purge Systems 159
Event Notification Manager 159
Bulk Room Email Mapping for Endpoints 160
System Status Reporting 161

Setting Up Default System Folders

As an administrator you can define any folder tree structure under the root folder. The folders are purely for organizational purposes, making it easier to locate systems and set system permissions. One system can appear in multiple folders.

The same folder tree is seen by all users, and is used throughout Cisco TMS. We therefore recommend choosing a scheme that is friendly and understandable for all user groups.

A commonly used model is basing the structure for endpoints on geography and organization, like the below example:



Infrastructure systems may be kept in separate folders.

To build your own folder structure:

1. Click on the **Company Name** folder in the tree.
   The right panel will update to show the contents of that folder.
2. Click **Edit This Folder** in upper right corner of the screen.
3. Rename the folder using the appropriate company name.
4. Click **Save**.
5. Add any additional folders:
   a. Click on the desired parent folder.
   b. Click **New Folder** on the right-hand side of the screen.
   c. Enter a name and, optionally, a description.
   d. Click **Save**.
   e. Repeat the above steps for as many folders as you wish to create.

You can add and delete folders at any time.

The root folder may not be deleted.

Adding Systems

The procedures described below are appropriate for most systems and system types.

Some systems require special procedures, see the following for further details:

- Adding Endpoints Behind a Firewall/NAT, page 57.
- Adding Unified CM and Registered Endpoints, page 58
- Adding an Unmanaged Bridge, page 60
- Adding Unmanaged Endpoints, page 61

For details of the layout and options of each of the Cisco TMS pages used in these procedures, see the reference section Add Systems, page 134.

Prerequisites for all Systems

- An administrator username and password for the system must be available for use by Cisco TMS.
  For most endpoints, this will be the default *admin* account.
- Network Services for HTTP and/or HTTPS must be enabled on the system.
- Endpoints that have a provisioning mode must be set to *TMS*.
- If your system relies on SNMP-based autodiscovery, its **NetworkServices SNMP CommunityName** must be set to a value listed in the Cisco TMS list of SNMP community names (see **Administrative Tools > Configuration > Network Settings > General Network Settings**).

  Note that SNMP for purposes beyond system discovery is only used for legacy systems.

Enforcing Settings from Cisco TMS

We strongly recommend enabling **Enforce Management Settings on Systems** in **Administrative Tools > Configuration > Network Settings > General Network Settings > TMS Services** before starting to add systems.

If you opt not to follow this recommendation, you must go to the system's **Settings > Edit Settings** tab in **Navigator** once the system has been added and click **Enforce Management Settings**, repeating this on-demand enforcement whenever settings change or need to be reset from Cisco TMS.

Note that if you add one or more systems to a second Cisco TMS instance in a test environment, you must only leave **Enforce Management Settings on Systems** in one Cisco TMS instance to avoid conflict.

Using Automatic Discovery

To enable automatic system discovery:

1. Go to **Administrative Tools > Configuration > Network Settings**.
2. Set **Automatic System Discovery Mode** to *On* and verify that **Default Folder for Discovered Systems** is set to an appropriate folder.
3. Click **Save**.

If you want to receive notifications by email each time a new system is discovered and added:

1. Go to **Administrative Tools > Configuration > Network Settings**.
2. In the Event Notification section, add your address to **E-mail Addresses to Receive System and Network Notifications**.

As systems on the network send HTTP events or are detected by the SNMP scanner service, they will now be added to the specified folder, and you will be notified.

To review the settings of these systems:

1. Go to **Systems > Navigator > [Name of your folder for discovered systems]**.

   The default folder is **Discovered Systems**.
2. Review and adjust the settings for each system as desired.
3. Verify on the system's **Permissions** tab that new user groups will have permissions for the system. Modify as required.
4. If desired, move the systems to a more permanent folder by selecting the system and clicking **Move/Copy** in the folder listing.

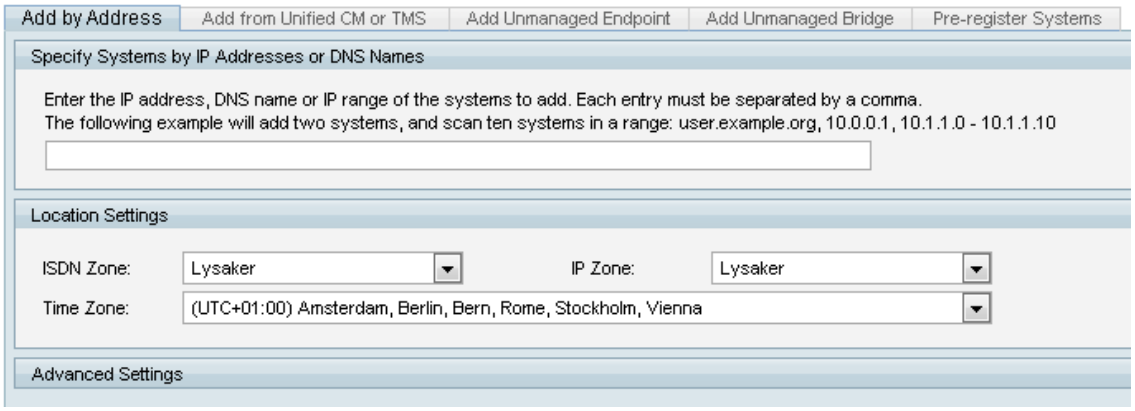
Adding by IP addresses or DNS Names

All types of infrastructure systems and endpoints can be added following the steps below. Note however that endpoints registered to Unified CM must not be added in this way, see Adding Unified CM and Registered Endpoints, page 58.

To add a system:

1. Go to **Systems > Navigator**.
2. Open **Discovered Systems** to verify that the system you are planning to add has not been added automatically by Cisco TMS already.
   - If the system has been added, go to the instructions for Using Automatic Discovery, page 55.
   - If the system is not in the **Discovered Systems** folder, select the folder to which you want to add the system.

3. Click **Add Systems**.



4. Enter either the IP address, the DNS name, an IP range, or a comma-separated list of IP addresses and/or DNS names.
   Note that adding very large ranges slows down the system discovery scan process.
5. Select **ISDN Zone**, **IP Zone** and **Time Zone** for the system from the drop-down lists.
6. Click the **Advanced Settings** section heading to expand it to add authentication details, configuration template, or SNMP discovery options.
   For an overview of the settings on this page, see Add Systems, page 134.
7. Click **Next** to start adding the system.
   A progress window will be shown as Cisco TMS connects to the address and determines the type of system being added, and the system's configuration.
8. You will now be prompted if a password is needed to access the system. Enter the password and click **Next**.
   A **Results** page is shown with a status for each system Cisco TMS tried to add. If Cisco TMS detected problems with any system's configuration, a message in the **Description** column states that the system has not yet been added.
   - To address errors immediately, click **Edit System**. Use the displayed information to make the necessary adjustments, then click **Save**.
     If the problem is resolved, the settings page will close and you will be returned to the **Results** page, which has been updated to state that the system was successfully added.
   - To address the error(s) later or ignore them altogether, click **Add System Despite Warnings** on the **Settings** or **Results** page.
   - When adding a TelePresence Server you will get an error stating that it is in remotely managed mode—ignore this.
9. Click **Finish Adding Systems** to return to the main **Navigator** view.
   Your new system will now be in the designated folder.

System Discovery Order by Protocol

When adding systems, Cisco TMS attempts to connect to them using SNMP first, trying all the community names defined in **Administrative Tools > Configuration > Network Settings > SNMP Community Name**. Cisco TMS tries connecting over SNMP for the period of time defined in **Network Settings > SNMP Timeout**.

Note that additional community names can be specified in **Advanced Settings** when adding systems.

If the system(s) cannot be contacted using SNMP, Cisco TMS then tries to connect to the systems using HTTP/HTTPS.

If there is no reply after the value defined in **Network Settings > Telnet/HTTP Connection Timeout** a 'System not found' error will be displayed.

Once successfully connected to the system using HTTP/HTTPS, Cisco TMS tries to get the system's systemunit.xml file, which includes the software version that identifies it as a particular system type.

If unable to get the systemunit.xml file, Cisco TMS goes through all system types it is aware of trying to match until it finds the right one. If it cannot find the right one, a 'System not found' error will be displayed.

Pre-registering Endpoints

Pre-registering endpoints ensures that they are added to Cisco TMS with a pre-defined configuration as soon as they are available on the network.

You can pre-register up to 10 endpoints at the same time:

1. Go to **Systems > Navigator** and locate or create the folder to which you want the systems added.
2. Click **Add Systems**.
3. Go to the **Pre-register Systems** tab.
4. Select the primary identifier to use for the systems; a MAC address, IP address, or serial number for legacy systems.
5. For each system, add the primary identifier.

   You may also choose to add a **System Name**, **H.323 ID**, **E.164 Alias**, **SIP URI**, and a **Password** if required.
6. Add location settings for the systems; IP/ISDN zone, and time zone.
7. Select whether to make any of the pre-registered settings persistent, whether to add a configuration template on first boot, and whether to set a persistent template.
8. Click **Add System(s)**.

   An entry for the system containing minimal information is added to the parent folder with **System Status** set to *Not Yet Activated*.

When the system comes online and registers, the status and system information are updated automatically. You can receive notification when this occurs by setting up an event notification for *Preregistered System Activated* in **Systems > Event Notification Manager**, see Event Notification Manager, page 159.

Pre-registration of infrastructure systems is not supported.

For similar functionality with more flexibility and scalability, we recommend large-scale provisioning using Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE), see Provisioning, page 141.

Adding Endpoints Behind a Firewall/NAT

Prerequisite

Before you can use a system behind a firewall/NAT in Cisco TMS, you must set a public DNS address on the Cisco TMS server:

1. Go to **Administrative Tools > Configuration > Network Settings**.
2. Under **Advanced Network Settings for Systems on Public Internet/Behind Firewall**, set **TMS Server Address** to be a public DNS address.
3. Click **Save**.

Adding to Cisco TMS While on the Network

The easiest way to add a system that will be located behind a firewall/NAT to Cisco TMS is to first connect the system to the organization's network so that you can add it following the steps in Adding Systems, page 54.

When the system has been added:

1. Go to **Systems > Navigator**, locate the system and open the **Settings** tab.
2. Set **System Connectivity** to *Behind Firewall*.

3. Click **Enforce Management Settings**.
   Cisco TMS will now set the management address on that system to Cisco TMS' external management address.

When the system is plugged in at the remote location, the system will send a boot event to Cisco TMS. From then on the system will be available.

Setting up from Behind the Firewall/NAT

If you want to add an endpoint behind a firewall/NAT and do not have the option of plugging it in on the organization's network first, you can either add it using automatic discovery, or, for increased security, pre-register it.

Enabling Automatic Discovery

This feature is off by default. To enable it:

1. Go to **Administrative Tools > Configuration > Network Settings**.
2. In the **Automatic System Discovery** section, make sure **Automatic System Discovery Mode for Endpoints Behind a Firewall/NAT** is set to *On*.
3. Verify that a default folder for discovered systems is set up.
4. Click **Save**.

Pre-registering the Endpoint

Follow the steps in Pre-registering Endpoints, page 57, using the endpoint's MAC address as the primary identifier.

Setting the Endpoint's External Management Address

You must set the external management address of Cisco TMS on the endpoint itself. Follow the instructions in your endpoint's documentation to set:

- **ExternalManager Address** to the address of the Cisco TMS server.
- **ExternalManager Path** to `TMS/public/external/management/systemmanagementservice.asmx`

When the endpoint is plugged in at the remote location with the correct external management address:

- Automatically discovered endpoints will be added to the default folder.
- Pre-registered endpoints will populate their entries in Cisco TMS with additional system information, and their system status will be set to *Alive*.

Adding Unified CM and Registered Endpoints

To add a Unified CM and endpoints registered to Cisco TMS, follow the procedures given in the listed order.

Multiple Unified CM are supported as long as the dial plan is flat between different Unified CM clusters.

Important Note: It is not supported to have provisioning mode as “Cisco TMS”, when the endpoint is registered with Unified CM.

Unified CM registered endpoints are managed only by Unified CM and not by Cisco TMS. The credentials for accessing endpoints are managed by Unified CM, and are synced to Cisco TMS on a regular cycle. Performing a Force Refresh on the Unified CM within Cisco TMS will also sync these credentials. For more information, refer to Unified CM Registered, page 45 features.

For a Unified CM cluster, it is required to add the publisher and all subscribers which contain the endpoints to be added to Cisco TMS.

Preparing the Unified CM

Activate these services on the Unified CM node(s) you want to add to Cisco TMS before you start:

- Cisco AXL Web Service on the Unified CM node.
- Cisco RIS Data Collector on the Unified CM Publisher node.
- Cisco CTIManager must be active on at least one of the nodes inside the Unified CM cluster.

Note: Cisco TMS uses **JSessionID** in CUCM AXL and RIS API request to align with the CUCM best practices guidelines. **JSessionID** allows CUCM clients to use a single session for making multiple AXL and RIS requests.

See *Cisco Unified Serviceability Configuration Guide* for instructions on service activation.

Follow this procedure in Unified CM:

1. Create an application user for Cisco TMS following the steps described in *Cisco Unified Communication Manager Configuration Guide for the Cisco TelePresence System*. Make sure to:
   - Save the credentials for the Cisco TMS initialization procedure that follows.
   - Assign all the rooms that you plan to use to the application user you create.
   - Assign all telepresence units to this user profile. The MAC Address of each unit and shared phone must be added to the user profile. Adding an IP phone associated with the CTS to the application user is not necessary.
   - Add the "Standard CTI Secure Connection" group to the application user to secure Cisco TMS. (This step is optional.)
2. Create an access control group group in Unified CM for Cisco TMS.
3. Assign the following roles to this access control group:
   - Standard AXL Read-only API Access (**Note**: This role is available from CUCM version 12.0.1.21002-2 onwards)
   - Standard AXL API Users
   - Standard CTI Enabled
   - Standard SERVICEABILITY
   - Standard CCM Admin Users
   - Standard RealtimeAndTraceCollection
4. Add the above application user to the newly created user group.

Adding Unified CM

Add Unified CM following the steps in Adding Systems, page 54.

Preparing to Add Endpoints

Cisco TMS support for Unified CM-registered systems relies on a special identifier for each system type being present in Cisco TMS. Identifiers for new endpoints will not be immediately available in Cisco TMS due to diverging release cycles. An updated list of supported systems is available on the **Extended Settings** tab for Unified CM in **Navigator**.

You can verify that your systems are supported as follows:

1. Go to **Systems > Navigator** and locate the Unified CM you just added.
2. Go to **Settings > Extended Settings**.
3. Make sure that all the endpoints you want to add are on the list of supported system types displayed on this tab.

For more information on how Unified CM-registered systems are supported in Cisco TMS, see How Endpoints are Managed by Cisco TMS, page 44.

CTS and TX Endpoints

The endpoints must already have been added to the Unified CM and configured with the same **Directory Number** as their associated phones as detailed in *Cisco Unified Communication Manager Configuration Guide for the Cisco TelePresence System*.

To prepare the systems, follow the steps below in Unified CM:

1. For each endpoint:
   a. Go to **Device > Phone** and click the endpoint's device name.
   b. Assign the same **DN** (Directory Number) as the IP phone that is associated with this endpoint.
   c. At the bottom of the **Device Information** section, select **Allow Control of Device from CTI**.
   d. In the **Product Specific Configuration Layout** section, enter a dummy email address in the **Room Name** field.
   This is a mandatory item but any email address can be used.
   e. In the Directory Number Information section of **Directory Number Configuration**, select **Allow Control of Device from CTI**.
   f. Set the field **SSH AdminLife** to *0* to prevent the command-line interface password from expiring.
   Cisco TMS uses this password to set up calls.
2. For each IP phone device that is associated to a telepresence device, select **Allow Control of Device from CTI** at the bottom of the **Device Information** section.

Endpoints Running Collaboration Endpoint Software, TE, and TC Software

Endpoints running Collaboration Endpoint Software, TE, and TC software must already have been added to the Unified CM as detailed in the Configuration guide for your version of Unified CM in *http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-system-ex-series/products-maintenance-guides-list.html*.

If an endpoint has previously been managed by Cisco TMS, see Changing Management Modes, page 46.

For each endpoint follow these steps in Unified CM:

1. Go to **Device > Phone** and search for the device name corresponding to the telepresence endpoint.
2. At the bottom of the **Product Specific Configuration Layout** section, ensure that **Web Access** and **SSH Access** are set to *Enabled*.

Adding the Systems

Unified CM and its nodes must be added to Cisco TMS before adding the endpoints from publisher and subscriber of Unified CM, following these steps:

1. In **Systems > Navigator** go to the folder where you want to add the endpoints.
2. Click **Add Systems**.
3. Go to the **From List** tab.
4. Click **Unified CM**.
5. Select the endpoints you want to add.
6. Click **Next**.
7. Click **Finish Adding Systems**.

Adding an Unmanaged Bridge

Cisco TMS supports adding unsupported legacy and third party bridges (including Cisco TelePresence Multipoint Switch) so they can be scheduled in conferences.

Prior to adding an unmanaged bridge to Cisco TMS, you must have created dedicated conferences for use with Cisco TMS scheduling on the bridge. These are known as Static Meetings on a Cisco TelePresence Multipoint Switch. Refer to your bridge's documentation for details of how to configure these conferences.

To add an unmanaged bridge:

1. Go to **Systems > Navigator**.
2. Select the folder to which you want to add the bridge, and click **Add Systems**.
3. Click the **Add Unmanaged Bridge** tab.
4. Enter the following **Basic Settings** for the bridge (the other settings are optional):
   a. **Name**
   b. **Max IP Bandwidth (kbps)**
   c. **Max Number of Video/Audio Calls**:
      - If *0* is entered in **Max Number of Audio Calls**, the value set as the **Max Number of Video Calls** will be the number of generic ports that can be used to book either video or audio participants.
      - If anything higher than *0* is entered in **Max Number of Audio Calls**, video and audio calls are counted separately and can not be used interchangeably.
   d. Check the **Immersive** checkbox if you want the bridge to be preferred in routing for conferences including multiscreen participants.
5. Add the **Bridge Addresses**:
   a. Select the number of bridge addresses up to a maximum of 25.
   b. Specify whether the bridge allows H.323, SIP or both.
   c. Specify the **E.164 Alias**, **H.323 ID** and/or **SIP URI** for pre-configured conference on the bridge. These are the 'static meeting' addresses referred to above.
6. Enter the **Location Settings** as appropriate.

Adding Unmanaged Endpoints

You can add a system as an unmanaged endpoint if the system type is not directly supported by Cisco TMS.

For more information about how unmanaged endpoints differ from other systems in Cisco TMS, see How Endpoints are Managed by Cisco TMS, page 44

To add an unmanaged endpoint:

1. Go to **Systems > Navigator**.
2. Select the folder to which you want to add the system, and click **Add Systems**.
3. Click the **Add Unmanaged Endpoint** tab.
4. Enter a name for what you are adding, and select a type.
5. Enter the **Endpoint Settings** and **Location Settings**. Some fields are mandatory:
   - Select **IP Zone**, **ISDN Zone**, and **Time Zone**.
   - Specify **Maximum IP Bandwidth**.
   - Specify **Gatekeeper Address**.
   - In order to use **SIP URI**, you must also set an **H.323 ID** or an **E.164 Alias**.
6. Click **Next**.

Endpoint Support in Various Communication Modes

Endpoint Name	Functionality	Communication Security Mode
Cisco CTS	All functionalities of CTS are supported only with HTTP in TMS.	Medium
	None of the functionalities of CTS are supported in TMS.	Medium-High or High
Cisco E20	All functionalities of E20 are supported with both HTTP and HTTPS.	Medium
	None of the functionalities of E20 are supported in TMS. It will be available for Booking. However Automatic connect, OBTP will not work.	Medium-High or High
Cisco TX9000	All functionalities of TX9000 are supported only with HTTP.	Medium
	None of the functionalities of TX9000 are supported in TMS.	Medium-High or High
Cisco IX5000	All functionalities of IX5000 are supported only with HTTPS.	Medium or Medium-High or High
Cisco Telepresence DX 80	All functionalities of DX 80 are supported only with HTTPS.	Medium-High or High
	All functionalities of DX 80 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence SX 80	All functionalities of SX 80 are supported only with HTTPS.	Medium-High or High
	All functionalities of SX 80 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence C 90	All functionalities of C 90 are supported only with HTTPS.	Medium-High or High
	All functionalities of C 90 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence SX 10	All functionalities of SX 10 are supported only with HTTPS.	Medium-High or High
	All functionalities of SX 10 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence C 20	All functionalities of C 20 are supported only with HTTPS.	Medium-High or High
	All functionalities of C 20 are supported with both HTTP and HTTPS.	Medium

Endpoint Name	Functionality	Communication Security Mode
Cisco Telepresence Mx300G2	All functionalities of Mx300G2 are supported only with HTTPS.	Medium-High or High
	All functionalities of Mx300G2 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence Mx200G2	All functionalities of Mx200G2 are supported only with HTTPS.	Medium-High or High
	All functionalities of Mx200G2 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence SX 20	All functionalities of SX 20 are supported only with HTTPS.	Medium-High or High
	All functionalities of SX 20 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence C 60	All functionalities of C 60 are supported only with HTTPS..	Medium-High or High
	All functionalities of C 60 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence EX 60	All functionalities of EX 60 are supported only with HTTPS.	Medium-High or High
	All functionalities of EX 60 are supported with both HTTP and HTTPS.	Medium
Cisco Telepresence DX70	All functionalities of DX 70 are supported only with HTTPS.	Medium-High or High
	All functionalities of DX 70 are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room Kit	All functionalities of Cisco Webex Room Kit are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room Kit are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room Kit Plus	All functionalities of Cisco Webex Room Kit Plus are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room Kit Plus are supported with both HTTP and HTTPS.	Medium

Endpoint Name	Functionality	Communication Security Mode
Cisco Webex Codec Plus	All functionalities of Cisco Webex Codec Plus are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Codec Plus are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room 55	All functionalities of Cisco Webex Room 55 are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room 55 are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room 55 Dual	All functionalities of Cisco Webex Room 55 Dual are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room 55 Dual are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room 70 Single	All functionalities of Cisco Webex Room 70 Single are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room 70 Single are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room 70 Dual	All functionalities of Cisco Webex Room 70 Dual are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room 70 Dual are supported with both HTTP and HTTPS.	Medium
Cisco Webex Codec Pro (For VCS managed endpoint) Cisco Webex Room Kit Pro (For CUCM managed endpoint)	All functionalities of Cisco Webex Codec Pro are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Codec Pro are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room Kit Mini	All functionalities of Cisco Webex Room Kit Mini are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room Kit Mini are supported with both HTTP and HTTPS.	Medium

Endpoint Name	Functionality	Communication Security Mode
Cisco Webex Room 70 Dual G2	All functionalities of Cisco Webex Room 70 Dual G2 are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room 70 Dual G2 are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room 70 Single G2	All functionalities of Cisco Webex Room 70 Single G2 are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room 70 Single G2 are supported with both HTTP and HTTPS.	Medium
Cisco Webex Desk Pro	All functionalities of Cisco Webex Desk Pro are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Desk Pro are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room 70 Panorama	All functionalities of Cisco Webex Room 70 Panorama are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room 70 Panorama are supported with both HTTP and HTTPS.	Medium
Cisco Webex Room Panorama	All functionalities of Cisco Webex Room Panorama are supported only with HTTPS.	Medium-High or High
	All functionalities of Cisco Webex Room Panorama are supported with both HTTP and HTTPS.	Medium

Managing Systems

This section describes common system-related administrative tasks:

- Viewing and Editing a System, page 65
- Changing Managed Endpoints Password, page 66
- Assigning Email Addresses to Endpoint, page 66
- Upgrading Cisco TMS-Managed Endpoints, page 68
- Swapping a System, page 67
- Purging a System, page 69

Note that these tasks only apply to systems added to Cisco TMS. Managing devices provisioned by Cisco TMSPE is covered by *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.

Viewing and Editing a System

When a system has been added to Cisco TMS, it can be managed using the web interface.

1. Go to **Systems > Navigator** and locate the system.
   The default view is the **System Summary** tab that contains a ticket list and an overview of the system and its key settings and status.
2. Click the other tabs for more details about the system. The available tabs vary by system type.
3. Click the **Settings** tab for a detailed view of the system's configuration.
   - The **Force Refresh** button at the bottom of the page allows you to immediately pull an updated configuration from the system.

     Note that this does not work for endpoints behind a firewall/NAT.
   - Go to **Edit Settings** in the menu bar to edit any of the system's settings and Cisco TMS properties.
   - Most systems can be rebooted from the **Edit Settings** screen by clicking **Boot**.

For a detailed reference of the tabs and settings available for the different system types, see Navigator, page 69.

Connection Settings

The **Connection** tab shows that the parameters Cisco TMS uses to communicate with the system. If Cisco TMS fails to reach the system when you go to **Edit Settings**, the **Connection** tab opens in its place.

To attempt reconnection with the system:

1. Update any connection setting as required.
2. Click **Save/Try**.

Changing Managed Endpoints Password

To change the password for managed endpoints, follow these steps:

1. On the endpoint, add a username and password and change the password for the "admin" username.
2. Go to **TMS web interface > Systems > Navigator > Find endpoint > Settings > Edit Settings**.
3. Click **Force Refresh**.
4. Type a new password.
5. Click **Save/Try**.

Note: This is not applicable for endpoints managed by Unified CM.

Assigning Email Addresses to Endpoint

Cisco TMS allows you to add, update or remove email address for the endpoint. Email address option is used to map an email address to the endpoint in Cisco TMS. Cisco TMS internally uses email address mapping to identify the endpoint while scheduling a conference. This is used only for ‘New Scheduling experience’ feature and is not a replacement for Cisco TMSXE's Systems Configuration. Valid email address formats are accepted.

Note: Endpoints must have unique email address mapped to it. No two endpoints can have the same email address mapped.

Cisco TMS also allows you to export or import bulk email address. For more information, refer Bulk Room Email Mapping for Endpoints, page 160.

Email address mapping can be done by using the following steps:

1. Go to the **TMS web interface > Systems > Navigator > Find endpoint > Settings > Edit Settings**.
2. Add or Update the valid **Email Address**.
3. Click **Save**.

Note: This is applicable for endpoints only.

Swapping a System

All systems get an ID (**TMS System ID**) when first added to Cisco TMS. This ID is used as the system reference for booking, permissions, and so on.

Should you need to replace a system due to theft, hardware failure, or similar, retaining the ID allows Cisco TMS to keep the links to existing bookings and permissions.

It is not possible to swap:

- remote endpoints.
- an endpoint with a bridge or vice versa.
- call control devices.
- gateways.
- recording servers.

While replacing bridges is possible, this is on a best effort basis and should be used with caution.

Conference Diagnostics must be run after any system has been replaced to check for any issues the replacement has introduced with future conferences.

Disallowing Booking

When a system in Cisco TMS is out of order, or awaiting a swap, we recommend preventing it from accepting new bookings:

1. Go **Systems > Navigator** and click on the system you wish to replace.
2. Open the **Connection** tab.
3. Set **Allow Bookings** to *No*.
4. Click **Save/Try**.

Note: Any booking details present on the endpoint outside of Cisco TMS will get overwritten by the booking details available in Cisco TMS, every 24 hours even if the booking is disallowed for a system on Cisco TMS.

Replacing the System

Follow this procedure to replace a system:

1. Go to **Systems > Navigator** and click on the system you wish to replace.
2. Click the **Connection** tab.
3. Click **Replace System**.
4. Search for the system in the folder tree or by typing part of the name in the search field and clicking **Filter**.
5. Click **Next**.
   A summary page is displayed.
6. Choose whether to keep the system name, call configuration, and all system logs.
7. Click **OK**.
8. The swap will now be completed and the old system purged from Cisco TMS.

Endpoints on the Same Cisco VCS

Note that if you wish to replace the connection settings of the current system with the connection settings of another system registered to the same Cisco VCS, a time delay for H.323 devices will influence the process.

This registration timeout setting in Cisco VCS is by default set to 1800 seconds (30 minutes). This means that when selecting **Keep call configuration (H.323 ID, E.164 alias and SIP URI) to system**, two settings will *not* be copied from the old system to the new and have to be set manually:

1. Go to **System > Navigator** and click on the system.
2. Open the **Settings** tab and click on the **Edit Settings** sub-menu.
3. Modify these settings:
   - **Requested Gatekeeper IP Address**
   - **Requested SIP Server Address**.

If you enter an IP address or DNS name that does not exist, for example because the system you are replacing is down, you may still update the network address of the current system. This will however result in a ticket indicating a connection error.

Upgrading Cisco TMS-Managed Endpoints

Note that when you schedule upgrades for more than nine endpoints, Cisco TMS will divide the endpoints into batches. The first batch always consists of 9 endpoints, subsequent batches include 10, until all endpoints have been upgraded.

The scheduled upgrade of a large number of endpoints can be resource intensive so we recommend doing this outside normal business hours.

Before you Start

Place the software package in the software directory in Cisco TMS. This location is defined in **TMS Tools > Configuration >** Software Directory, page 292, and the location is viewable in **Administrative Tools > General Settings**.

Uploading the Software to Cisco TMS

1. Go to **Systems > System Upgrade > Software Manager**.
2. Click **Upload New Software**.
3. Click **Browse** and locate the software package.
4. Click **Upload**.
   Verify that the package is visible in the list on the **Software Manager** page.

Upgrading the Endpoints

1. Go to **Systems > System Upgrade > System Upgrade**.
2. Locate the endpoint(s) you want to upgrade by using the folder view, selecting an alternate listing from the drop-down, or searching for the system on the **Search** tab.
3. Select the system(s) and click **Next**.
   The **Select Software and Release Keys** page opens.
4. Fill in:
   - The software version, using the drop-down list in the **Software** field.
   - The **Date** and **Start Time** you want for the scheduled upgrade.
   - For legacy systems a **Release Key** for the software may be required.

5. Click **Upgrade**.
   - For systems on the organization's network, you can now verify that the upgrade has been scheduled or initiated by going to **Systems > System Upgrade > System Upgrade Activity Status**.
   - Systems behind a firewall/NAT must now be booted. Cisco TMS will initiate the upgrade when receiving the boot event.
     See Systems Behind a Firewall/NAT, page 47 for background on how these upgrades work.

Applying the Same Upgrade to Endpoints with the Same Software Version

To select the same software file in the **Software** drop-down list for all systems with a similar software version:

1. Choose *Software* on one system.
2. Click the **Apply to all** link displayed to the right of the drop-down.
   All systems affected will have the same software file selected and will be highlighted.

Purging a System

Cisco TMS differentiates between deleting and purging a system.

- You can use a **Delete** operation to delete a system from a folder. It will still have an entry in the Cisco TMS database and may appear in one or more additional folders.
- If you **Purge** a system, its database entry is permanently removed.

Using the Navigator

1. Go to **Systems > Navigator** and locate a folder where the system is displayed.
2. Check the system you want to remove.
3. Click **Delete**.
   A confirmation prompt is displayed asking you whether you want to delete the system from the folder or purge it entirely from the database.
4. Click **Purge**.

Using the Purge Systems Page

1. Go to **Systems > Purge Systems**.
2. Select the system you want to remove.
3. Click **Purge Systems** at the bottom of the page.
   A list is displayed containing all selected systems and any future conferences they are scheduled to participate in.
4. Click **Purge** to confirm the operation.

Navigator

In Cisco TMS: **Systems > Navigator**

The **Navigator** is the hub for system management in Cisco TMS. This is where you add new systems and access systems that have already been added to view and modify their settings.

When clicking on a system name in **Navigator**, up to two icons are displayed in the upper right-hand corner:

	Go directly to the system's web interface.		Send an instant message to the endpoint that will be displayed on screen.

For more information about the available settings for each system type, see:

- Endpoints, page 71
- Cisco VCS, page 78
- Unified CM, page 85
- MCUs and TelePresence Server, page 112
- Gateways, page 119
- TelePresence Conductor, page 92
- Cisco TelePresence Supervisor MSE 8050, page 88
- Unmanaged Endpoint, page 131
- Unmanaged Bridge, page 127

The reference section below describes the **Navigator** framework.

Folder Actions

When a folder is selected in the tree view, up to six buttons are available.

Button	Description
In the upper right corner	
Edit This Folder	Rename the current folder and add a description. This button is only visible in folder view.
Folder and System Permissions	Adjust permissions for the folder and systems, including subfolders. See Folder and System Permissions, page 137 for an overview of the page that opens.
Below the list of systems	
Move/Copy	Move or copy the selected system(s) to other folder(s).
Delete	Remove the selected system(s) from its current folder in the system tree structure. Next, decide whether the system should be purged from Cisco TMS or just deleted from this folder. See Purge Systems, page 159 for more information.
New Folder	Add a new sub-folder to the current folder.
Add Systems	Start adding a new system to the current folder. See Add Systems, page 134 for an overview of the page that opens.

Navigating the Folder Tree

The drop-down menu on the top left contains multiple view options. *Folder View* is the default, where you can add and remove folders and systems and organize your videoconferencing systems in a tree structure. You can also restrict and control the permissions to folders, subfolders and systems for different groups.

- Expand and collapse the folders by clicking on **+** and **–**.
- Click on a folder to display all systems in that folder in the right side of the screen.
- Click on a system to display details for that system.
- One system can reside in several folders.

You can improve Navigator performance by going to **Administrative Tools > Configuration > General Settings** and setting **Show Systems In Navigator Tree** to *No*. Only folders will then be displayed on the left side of the screen, while systems can still be viewed in the main section of the screen when a folder is selected.

Additional views in the Navigator page

The drop-down menu above the folder list contains the below alternatives to the default folder view.

View option	System grouping
All Systems	Sorted alphabetically
System Type	By system type, for example: Cisco TelePresence MX300, Cisco Unified Communications Manager, TANDBERG Codec C60, and so on.
System Category	By system category: Endpoint, Gatekeeper, Gateway, MCU, and so on.
Manufacturer	By manufacturer: Cisco, TANDBERG, Polycom..
Time Zone	By system time zone.
ISDN Zone	By ISDN zone as configured in Cisco TMS.
IP Zone	By the IP zones they are configured with in Cisco TMS.
System Status	By system status. For an overview of all possible system statuses, see System Status Reporting, page 161.
Connection Status	By connection status, such as: ■ *No SNMP Response* ■ *OK* ■ *Wrong Username Password* ■ *Missing Password*
Software Version	By current software version; TC5.1.3, X7.2, CTS 1.8.0(55), and so on.
System Usage Type	By **System Usage Type**: ■ Meeting Room system ■ Personal Office System ■ Personal Home System ■ Roll About ■ Other
System Search	Search for systems by name or partial name.

Endpoints

In Cisco TMS: **Systems > Navigator** an endpoint is selected

For information about the configuration options and maintenance of each particular endpoint model, see the administrator documentation for the endpoint.

Summary

Table 9 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.
Service Contract Status	An overview of service contract status and updates for the selected system, including expiry date, release keys for the latest major software versions, and a link to check for software updates. Possible status messages are: ■ *Service contract is valid and ok* ■ *Service contract is ordered, but not invoiced* ■ *Service contract is expired* ■ *No service contract* ■ *Draft* ■ *New Revision* ■ *Bought by current partner* ■ *Unknown* This field is not applicable to or displayed for all systems.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
Phone Books	Any phone books set on the system (only displayed for endpoints, MCUs, and gateways that support phone books).
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.
Book conference with this system	This link does navigate to new conference web page without any participants added into it.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 10 Sections in View Settings and Edit Settings

Section	Description

Table 10 Sections in View Settings and Edit Settings (continued)

General	The most important settings for the system, such as: ▪ **Name** ▪ **System Type** ▪ **Network Address** ▪ **Location** ▪ **System Connectivity** For endpoints that support provisioning using Cisco TMSPE, a check box labeled **Provisioned** is displayed.
Configuration	Lists the system's software and hardware version and time of last backup and restore. For Unified CM-registered endpoints, only the software version will be displayed. For TelePresence Server: **Operation mode**: *Remotely Managed* or *Locally Managed* A TelePresence Server that is in *Remotely Managed* mode is only supported if it is managed by a TelePresence Conductor that is present in Cisco TMS.
Network Settings	In this section you will find H.323 gatekeeper and SIP server registration information, the NTP (Network Time Protocol) server setting and IP configuration information. For Unified CM-registered endpoints, only **SIP Mode**, **Requested SIP Server Address**, and **Active SIP Server Address** are displayed. For TelePresence Server and TelePresence MCUs that are SIP-trunked to a Unified CM, the SIP Mode is read from the bridge and displayed here.
Cisco Proximity Settings	Lists the options to configure Cisco Intelligent Proximity Settings for the endpoints that run on Collaboration Endpoint Software version 8.0 and newer.
Monitoring/SNMP Settings	In this section the trap host and management IP addresses and SNMP community are found. The trap host and management addresses should be the IP address of the Cisco TMS server that administrates the systems. Legacy Cisco TelePresence MXP endpoints use the management address to send traps.

Table 10 Sections in View Settings and Edit Settings (continued)

TMS Scheduling Settings	**Allow Booking**: Allows the system to be added to conferences. **Allow Webex Booking**: Allows bridges to host Webex conferences. **Allow Incoming IP Address Dialing**: Allows calls to the system to be routed using H.323 direct mode. **Allow Incoming H.323 Dialing**: Allows calls to the system to be routed using an E.164 alias or H.323 ID. **Allow Incoming SIP URI Dialing**: Allows calls to the system to be routed using a SIP URI. **Allow Incoming ISDN Dialing**: Allows calls to the system to be routed using ISDN. **Allow Incoming Telephone Dialing**: Allows calls to the system to be routed using ISDN. **Allow Outgoing IP Address Dialing**: Allows calls from the system to be routed using H.323 direct mode. **Allow Outgoing H.323 Dialing**: Allows calls from the system to be routed using an E.164 alias or H.323 ID. **Allow Outgoing SIP URI Dialing**: Allows calls from the system to be routed using a SIP URI. **Allow Outgoing ISDN Dialing**: Allows calls from the system to be routed using ISDN. Note the following: ■ Only the booking/dialing options applicable to a particular system will be displayed. ■ Unchecking the **Allow Booking** box only affects new conferences. ■ Changing any of the Dialing options could affect the routing of existing conferences. ■ If you change any of the Dialing options for a system we recommend running **Conference Diagnostics** to identify any resulting issues with existing conferences.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Clicking **Force Refresh** updates the information displayed from the system.

For Unified CM-registered endpoints, the refreshed status is read from Unified CM. The button has no effect for endpoints behind a firewall/NAT.

An **Enforce Management Settings** button is available for most direct-managed systems. Clicking this button will:

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
  For Unified CM-registered endpoints, this IP address will be set as the **Feedback Address** instead.
- Update settings for **Daylight Saving Time**, **Time Zone** and **IP address**, and the paths for **Phonebook Settings** and **External Services**.
- For legacy systems that communicate with Cisco TMS using SNMP, such as Cisco TelePresence MXP systems, the **Traphost IP Address** is also set. This is done automatically on all systems if **Enforce Management Settings on Systems** is enabled in **Administrative Tools > Configuration > Network Settings**, see Network Settings, page 237.

Extended Settings

Extended settings are not available for all endpoint types, but typically include read-only listings of:

- Option keys
- Display parameters
- System status

Compare Settings

This tab displays a comparative listing of the current settings on the system and any backed up configuration stored on the server. Any differences will be highlighted.

If settings are already stored on the server, two buttons will be available:

- **Make Backup**
- **Restore System**

If no settings have yet been stored on the server, only **Make Backup** will be available.

This tab is not available for endpoints behind a firewall/NAT and Unified CM-registered endpoints.

Persistent Settings

The **Persistent Settings** tab is only available for Cisco TMS-controlled endpoints. Here you can enter settings that Cisco TMS will preserve for the endpoint. If any of these settings are altered on the endpoint, Cisco TMS will overwrite those changes with the settings configured here.

These persistent settings are available:

- **Configuration Template**: have a custom settings template applied to the system daily. For further detail, see Configuration Templates, page 151.
- **System Name**: the endpoint's display name.
- **E.164 alias**
- **H.323 ID**
- **SIP URI**

Note that settings configured as persistent will be unavailable for editing on the **Edit Settings** tab.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Call Status

If the system is in a conference, information about the current connection is shown on this tab. Any conferences scheduled for the day are also listed on the tab.

On this tab you can:

- Make a call using the **Dial** button and choosing call protocol as appropriate. If the system supports calling several systems at once, additional fields will appear while entering addresses/numbers.
- Disconnect an ongoing call by clicking **Disconnect**.
- Get the latest information from the system by clicking **Refresh Page**.

Telepresence (Cisco TelePresence T3 only)

This tab lists the TelePresence Server and codecs associated with the Cisco TelePresence T3 system.

When the associated systems are registered in Cisco TMS, their name and status will be displayed, and a **Details** link will open each system's detail in a **Navigator** view.

Phone Book

This tab displays all endpoint phone books. Click **Server Phone Books** to go to phone book selection mode.

Use the arrow buttons to set phone books on the system or remove existing phone books.

The button **Go to Manage Phone Books** will open the page Manage Phone Books, page 215.

For guidance on working with phone books, see Creating and Managing Phone Books, page 210.

Connection

Table 11 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
SNMP Get Community Name	The SNMP get community name for the system. Only visible for systems that support SNMP community names.
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname* ■ *MAC Address*

Table 11 Connection parameters for system communication on the Connection tab (continued)

Field	Description
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. ■ *Behind Firewall*: This alternative will only be shown for endpoints that may be located behind a firewall/NAT. The system uses the same public network address setting as systems reachable on public internet. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Note: When the Endpoints password is changed through Cisco TMS, it takes time to get updated in Cisco TMS. The user has to wait for a while for the new password to be effective in Cisco TMS. During the time password is updated, the user has to navigate to the System page, where a warning message "`Wrong Username or Password. Note: If you have changed the password, wait for a few mins, then refresh the page for the password to be effective`" is displayed. The status, then is changed to "*Unknown*" and later after a few minutes, it will be changed to "*Idle*" state.

Cisco TMS allows updation of credentials for Cisco Unified Communications Manager managed endpoints

Cisco TMS now provides a **Connection** tab for Cisco Unified Communications Manager managed devices to update the credentials which are added in Cisco TMS. Whenever, the credentials are changed for Cisco Unified Communications Manager managed endpoint which are added in Cisco TMS then in Cisco TMS Cisco Unified Communications Manager managed endpoint the status will change to '**Wrong username or password**'. You must manually update the correct credentials in **Connection** tab of the endpoint in Cisco TMS.

Note: Any updates done to the credentials from Cisco Unified Communications Manager does not work for the Cisco Unified Communications Manager managed devices that are added in Cisco TMS until the credentials are updated manually in Cisco TMS.

Replace System

On this tab, you can replace the system with a new one that will have the exact same name, role and configurations.

For step-by-step instructions, see Swapping a System, page 67.

Inherent from Current System helps you to retain or replace the old system settings. The following options enable you to retain the old system settings and uncheck these options to replace the old system settings:

- System name
- Call configuration (H323 id, E164 Alas and SIP URI) to system

- Logs (Feedback log, History, Call log and Ticket log).

By default, these options are selected in the **Replace System** tab.

This tab is not available for endpoints behind a firewall/NAT and systems whose system connectivity status has been set to *Inaccessible*.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 12 The Logs contains all available logs for the system

Log	Description
Feedback Log	A detailed log describing all events that are registered for a particular system, including scheduling, errors, and encryption status. You will be able to see the 100 last events for the system.
History	All detected changes that have been made to the system in Cisco TMS.
Call Log	Call Detail Records (CDRs) for the selected system, if available. For more information, see Call Detail Records, page 230.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Cisco VCS

In Cisco TMS: **Systems > Navigator**Cisco VCS or a legacy gatekeeper/border controller is selected

For information about the configuration options and maintenance of Cisco VCS, see *Cisco TelePresence Video Communication Server Administrator Guide* for your version.

Summary

Table 13 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.

Table 13 The Summary tab presents the most important data for the system (continued)

Section	Description
Service Contract Status	An overview of service contract status and updates for the selected system, including expiry date, release keys for the latest major software versions, and a link to check for software updates. Possible status messages are: ■ *Service contract is valid and ok* ■ *Service contract is ordered, but not invoiced* ■ *Service contract is expired* ■ *No service contract* ■ *Draft* ■ *New Revision* ■ *Bought by current partner* ■ *Unknown* This field is not applicable to or displayed for all systems.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 14 Sections in View Settings and Edit Settings

Section	Description
General	The most important settings for the system, such as: ■ **Name** ■ **System Type** ■ **Network Address** ■ **Location** ■ **System Connectivity**
Configuration	Lists the system's software and hardware version and time of last backup and restore. For TelePresence Server: **Operation mode**: *Remotely Managed* or *Locally Managed* A TelePresence Server that is in *Remotely Managed* mode is only supported if it is managed by a TelePresence Conductor that is present in Cisco TMS.

Table 14 Sections in View Settings and Edit Settings (continued)

Network Settings	In this section you will find H.323 gatekeeper and SIP server registration information, the NTP (Network Time Protocol) server setting and IP configuration information. For TelePresence Server and TelePresence MCUs that are SIP-trunked to a Unified CM, the SIP Mode is read from the bridge and displayed here.
Monitoring/SNMP Settings	In this section the trap host and management IP addresses and SNMP community are found. The trap host and management addresses should be the IP address of the Cisco TMS server that administrates the systems. Legacy Cisco TelePresence MXP endpoints use the management address to send traps.
Gatekeeper Settings	Fields include **Routing Mode**, **Zone Mode**, and **Domain Name**. These settings are read-only in Cisco TMS and are not available under **Edit Settings**.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Clicking **Force Refresh** updates the information displayed from the system.

For Unified CM-registered endpoints, the refreshed status is read from Unified CM. The button has no effect for endpoints behind a firewall/NAT.

An **Enforce Management Settings** button is available for most direct-managed systems. Clicking this button will:

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
  For Unified CM-registered endpoints, this IP address will be set as the **Feedback Address** instead.
- Update settings for **Daylight Saving Time**, **Time Zone** and **IP address**, and the paths for **Phonebook Settings** and **External Services**.
- For legacy systems that communicate with Cisco TMS using SNMP, such as Cisco TelePresence MXP systems, the **Traphost IP Address** is also set. This is done automatically on all systems if **Enforce Management Settings on Systems** is enabled in **Administrative Tools > Configuration > Network Settings**, see Network Settings, page 237.

Extended Settings

In the extended settings for Cisco VCS, you can:

- Add new option keys and see the ones already added.
- View display parameters
- View system status

Compare Settings

This tab displays a comparative listing of the current settings on the system and any backed up configuration stored on the server. Any differences will be highlighted.

If settings are already stored on the server, two buttons will be available:

- **Make Backup**
- **Restore System**

If no settings have yet been stored on the server, only **Make Backup** will be available.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Registrations

All endpoints, gateways, and MCUs registered to the system.

Table 15 Sections and fields on the Registrations tab

Sections and fields	Description
Registration search	
Name or Alias	Find registrations that contains the search text in the name or alias.
Information	
Name	Name of system or SIP URI.
Alias	E.164 alias, H.323 ID, or SIP URI.
IP Address	The IP address of the registered system.
Type	Type of system, for example, SIP UA, H.323 Endpoint, or MCU.
Vendor Information	The system vendor and, in the case of SIP registrations, also the software version.
Peer	The IP address of the cluster peer where the system is registered. Cisco VCS only.

Active Calls

Under **Active Calls** you will find a list of all ongoing calls for systems registered to the Cisco VCS.

Table 16 Sections and fields on the Active Calls tab

Sections and fields	Description
Call search	
Address or Alias	Find active calls that contains the search text in source/destination address or alias.
Information	
Source Address	IP address for the calling system.
Source Alias	Alias, for example E.164 alias, for the calling system.
Destination Address	IP address for the called system.
Destination Alias	Alias, for example E.164 alias, for the called system.
Bandwidth	Bandwidth in kilobits per second (kbps) used for the call.
Call Type	Type of call. The options are: - *Traversal* - *NonTraversal* - *Unknown*
Duration	Duration of call at the time of opening the **Active Calls** tab.

Table 16 Sections and fields on the Active Calls tab (continued)

Sections and fields	Description
Call Protocol	Displays the call signaling protocol; either SIP or H.323.
Peer	The IP address of the cluster peer where the call is active. Cisco VCS only.

Services

This tab contains a list of prefixes of all services on MCUs and gateways registered to the system.

Table 17 Columns on the Services tab

Column	Description
Service Prefix	Digit pattern registered with Cisco VCS as a service.
Description	Type of service (gateway or MCU) with IP address and port for each service.
Predefined	▪ *True*–statically defined by Cisco VCS configuration. ▪ *False*–added by a system registered to Cisco VCS.
Out Of Zone	Whether the service may be used by calls originating outside of Cisco VCS's zone. Can be set to *True* or *False*.

Clustering

This tab allows you to administer your Cisco VCS clusters. A cluster consists of one master Cisco VCS and one or more peers that work together as if they were a single unit.

See *Cisco TelePresence Video Communication Server Cluster Creation and Maintenance Deployment Guide* for instructions on clustering.

All peers in a cluster must have the same software version and the same set of option keys, and configuration of certain elements must be identical. Changes to these configuration elements must be performed on the master Cisco VCS only and will be replicated automatically to the peers.

Table 18 Components of the Clustering tab

Sections, columns, and buttons	Description
Cluster Name	The name of the cluster. This setting is read only and can only be changed on the Cisco VCS.
Create Cluster	A cluster must be set up on Cisco VCS before it can be added to Cisco TMS.
Cluster Peers	
Name	The name of each Cisco VCS cluster peer.
IP Address	The IP address of this cluster peer.
Software Version	The software version of the Cisco VCS. All peers (members) of a Cisco VCS cluster must have the same software version and the same set of option keys.
Status	Shows the status of each cluster peer (member). For an overview of all possible system statuses, see System Status Reporting, page 161.

Table 18 Components of the Clustering tab (continued)

Sections, columns, and buttons	Description
Description	Comments from Cisco TMS regarding the peer.
Update Cluster in Cisco TMS	Updates cluster information in Cisco TMS with the current configuration read from the Cisco VCS. Only needed when Cisco TMS detects a mismatch between the two configurations. This page will indicate any mismatch found.
Delete Cluster	Delete entire cluster from Cisco TMS. This will not delete any cluster information from the Cisco VCS. That can only be done on the VCS itself.
Refresh	Refreshes this page.

Provisioning

For instructions on using this tab and setting up provisioning, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.

Table 19 Settings on the Provisioning tab

Field and buttons	Description
TMS Connection Settings	
Server Address	Specify Cisco TMS server address.
Encryption	Whether to use HTTPS communication.
Certificate Verification Enabled	When HTTPS communication is used, determine whether to check the validity of certificates and their hostnames. These fields will be grayed out if **Encryption** is set to *Off*.
Certificate Hostname Checking Enabled	
Username	Credentials for a user with Site Administrator permissions in Cisco TMS.
Password	
Base Group	User repository group to use as the base.
Services	
Enable Service	The available services are: ■ Users ■ FindMe ■ Phone Books ■ Devices
Polling Interval	How often to poll for status.
Base Group	User repository group to use as the base.
Status	The status of each service.

Table 19 Settings on the Provisioning tab (continued)

Field and buttons	Description
Save	Save the settings
Force Refresh	Sends the current settings available in Cisco VCS page, as the same settings on the Cisco VCS UI must be same as seen in Cisco TMS.
Set Default Connection Settings	Set default connection settings.
Check for Updates	Triggers Cisco VCS to search for the changes in the data-set from the last time that Cisco VCS checked for changes in it.
Perform full Synchronization	Use in special cases when groups are moved or databases are restored. This creates inconsistencies in the datasets on the Cisco VCS and Cisco TMSPE.

Connection

Table 20 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
SNMP Get Community Name	The SNMP get community name for the system. Only visible for systems that support SNMP community names.
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname* ■ *MAC Address*

Table 20 Connection parameters for system communication on the Connection tab (continued)

Field	Description
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 21 The Logs contains all available logs for the system

Log	Description
Feedback Log	A detailed log describing all events that are registered for a particular system, including scheduling, errors, and encryption status. You will be able to see the 100 last events for the system.
History	All detected changes that have been made to the system in Cisco TMS.
Call Log	Call Detail Records (CDRs) for the selected system, if available. For more information, see Call Detail Records, page 230.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Note: If Cisco VCS is added using non default port, then Cisco TMS does not discover SNMP Community Name.

Unified CM

In Cisco TMS: **Systems > Navigator**Unified CM is selected

For details on Unified CM management and configuration options, see Unified CM documentation.

Summary

Table 22 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.

Settings

View Settings and Edit Settings

Limited configuration options are available for Unified CM in Cisco TMS:

Table 23 View and Edit Settings for Unified CM

Section	Description
General	The most important settings for the system. The editable settings for Unified CM are: ■ **Time Zone** ■ **Username** ■ **System Type** ■ **System Contact** ■ **Alert System Contact When Booked** ■ **Description**
Configuration	Unified CM software version.

Extended Settings

This tab contains a list of all Cisco TMS-compatible telepresence endpoint types supported by this version of Unified CM. See Preparing to Add Endpoints, page 59 for further information.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Managed Systems

Telepresence systems managed by Unified CM are listed on this tab.

Table 24 Columns on the Managed Systems tab

Column	Description
System Name	System name in Cisco TMS. If the system is not in Cisco TMS, a warning about this will be displayed. Note: The system name is captured from the endpoints' description field of Unified CM. If the description field is empty, then Cisco TMS displays SEP+MAC address as System name.
System Type	The system type and model.
MAC Address	The MAC address of the system.
IP Address	The IP address of the system.

Clustering

This tab lists all the nodes in the cluster that the Unified CM is a member of. A green tick shows which is the primary node. Clicking the **View Details** link takes you to the system details for the corresponding nodes in **Systems > Navigator**.

Note that Cisco TMS creates a cluster by identifying member nodes in the **System > Servers** page of a Unified CM that are also present in Cisco TMS.

It is therefore essential that the **Host Name/IP Address** set for a Unified CM in the **System > Servers** page is the same as what is set for the Unified CM in the **IP Address** and **Hostname** fields on the **Connection** tab in Cisco TMS.

Connection

Table 25 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
SNMP Get Community Name	The SNMP get community name for the system. Only visible for systems that support SNMP community names.
Track system on network by	Set the preferred address for your system. The options are: ▪ *IP Address* ▪ *Hostname* ▪ *MAC Address*

Table 25 Connection parameters for system communication on the Connection tab (continued)

Field	Description
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 26 The Logs contains all available logs for the system

Log	Description
Feedback Log	A detailed log describing all events that are registered for a particular system, including scheduling, errors, and encryption status. You will be able to see the 100 last events for the system.
History	All detected changes that have been made to the system in Cisco TMS.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Cisco TelePresence Supervisor MSE 8050

In Cisco TMS: **Systems > Navigator**Cisco TelePresence Supervisor MSE 8050 is selected

For more detailed information about this system, see *Cisco TelePresence Supervisor MSE 8050 Printable Help* for your version.

Summary

Table 27 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.
Book conference with this system	This link does navigate to new conference web page without any participants added into it.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 28 Sections in View Settings and Edit Settings

Section	Description
General	The most important settings for the system, such as: ■ **Name** ■ **System Type** ■ **Network Address** ■ **Location** ■ **System Connectivity**
Configuration	Lists the system's software and hardware version and time of last backup and restore. For TelePresence Server: **Operation mode**: *Remotely Managed* or *Locally Managed* A TelePresence Server that is in *Remotely Managed* mode is only supported if it is managed by a TelePresence Conductor that is present in Cisco TMS.
Network Settings	In this section you will find H.323 gatekeeper and SIP server registration information, the NTP (Network Time Protocol) server setting and IP configuration information. For TelePresence Server and TelePresence MCUs that are SIP-trunked to a Unified CM, the SIP Mode is read from the bridge and displayed here.
Monitoring/SNMP Settings	In this section the trap host and management IP addresses and SNMP community are found. The trap host and management addresses should be the IP address of the Cisco TMS server that administrates the systems. Legacy Cisco TelePresence MXP endpoints use the management address to send traps.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Clicking **Force Refresh** updates the information displayed from the system.

For Unified CM-registered endpoints, the refreshed status is read from Unified CM. The button has no effect for endpoints behind a firewall/NAT.

An **Enforce Management Settings** button is available for most direct-managed systems. Clicking this button will:

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
  For Unified CM-registered endpoints, this IP address will be set as the **Feedback Address** instead.
- Update settings for **Daylight Saving Time**, **Time Zone** and **IP address**, and the paths for **Phonebook Settings** and **External Services**.
- For legacy systems that communicate with Cisco TMS using SNMP, such as Cisco TelePresence MXP systems, the **Traphost IP Address** is also set. This is done automatically on all systems if **Enforce Management Settings on Systems** is enabled in **Administrative Tools > Configuration > Network Settings**, see Network Settings, page 237.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Supervisor

Table 29 Columns on the Supervisor tab

Column	Description
Slot	Placement in chassis, numbered from left to right.
System Name	System name in Cisco TMS. If the system is not in Cisco TMS, a warning about this will be displayed.
Type	The type of blade.
Port Address	In the **Port A–D** columns, the IPv4 and/or IPv6 addresses of the blade's Ethernet ports are displayed.

Table 29 Columns on the Supervisor tab (continued)

Column	Description
Status	■ *Blade OK* ■ *Blade removed*: no blade is fitted in this slot. ■ *Blade absent*: there is no blade in this slot. ■ *Blade inserted badly*: ensure that this blade is firmly secured in the chassis. ■ *Blade shutting down*: the blade is in the process of shutting down. ■ *Attempting restart*: the Supervisor is in the process of attempting to restart the blade. ■ *Invalid blade ID*: ensure that the blade is pushed in firmly. ■ *Waiting for communications*: the blade has failed to make contact with the Supervisor. ■ *Lost communication*: the blade has lost contact with Supervisor. ■ *Temperature / Voltages / RTC Battery critical*: a problem is shown on the blade's Health status page. ■ *Blade shut down*: The blade is currently shut down (or restarting). ■ *Restart required*: shut down and restart this blade. ■ *Restarting*: this blade is restarting. ■ *Blade software version too old*: Upgrade this blade to the latest available software release.
View System Details	This link will be displayed for all systems added to Cisco TMS. Click to launch system details in a separate window.

Connection

Table 30 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
SNMP Get Community Name	The SNMP get community name for the system. Only visible for systems that support SNMP community names.

Table 30 Connection parameters for system communication on the Connection tab (continued)

Field	Description
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname* ■ *MAC Address*
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 31 The Logs contains all available logs for the system

Log	Description
History	All detected changes that have been made to the system in Cisco TMS.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

TelePresence Conductor

In Cisco TMS: **Systems > Navigator**TelePresence Conductor is selected

For information about the configuration options and maintenance of TelePresence Conductor, see *Cisco TelePresence Conductor Administrator Guide* for your version. For information about scheduling using Cisco TMS and a TelePresence Conductor, see *Cisco TelePresence Conductor with Cisco TMS Deployment Guide*.

Summary

Table 32 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.
Book conference with this system	This link does navigate to new conference web page without any participants added into it.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 33 Sections in View Settings and Edit Settings

Section	Description
General	The most important settings for the system, such as: ■ **Name** ■ **System Type** ■ **Network Address** ■ **Location** ■ **System Connectivity**
Configuration	Lists the system's software and hardware version and time of last backup and restore. For TelePresence Server: **Operation mode**: *Remotely Managed* or *Locally Managed* A TelePresence Server that is in *Remotely Managed* mode is only supported if it is managed by a TelePresence Conductor that is present in Cisco TMS.
Network Settings	In this section you will find H.323 gatekeeper and SIP server registration information, the NTP (Network Time Protocol) server setting and IP configuration information. For TelePresence Server and TelePresence MCUs that are SIP-trunked to a Unified CM, the SIP Mode is read from the bridge and displayed here.
Monitoring/SNMP Settings	In this section the trap host and management IP addresses and SNMP community are found. The trap host and management addresses should be the IP address of the Cisco TMS server that administrates the systems. Legacy Cisco TelePresence MXP endpoints use the management address to send traps.

Table 33 Sections in View Settings and Edit Settings (continued)

TMS Scheduling Settings	**Allow Booking**: Allows the system to be added to conferences. **Allow Webex Booking**: Allows bridges to host Webex conferences. **Allow Incoming IP Address Dialing**: Allows calls to the system to be routed using H.323 direct mode. **Allow Incoming H.323 Dialing**: Allows calls to the system to be routed using an E.164 alias or H.323 ID. **Allow Incoming SIP URI Dialing**: Allows calls to the system to be routed using a SIP URI. **Allow Incoming ISDN Dialing**: Allows calls to the system to be routed using ISDN. **Allow Incoming Telephone Dialing**: Allows calls to the system to be routed using ISDN. **Allow Outgoing IP Address Dialing**: Allows calls from the system to be routed using H.323 direct mode. **Allow Outgoing H.323 Dialing**: Allows calls from the system to be routed using an E.164 alias or H.323 ID. **Allow Outgoing SIP URI Dialing**: Allows calls from the system to be routed using a SIP URI. **Allow Outgoing ISDN Dialing**: Allows calls from the system to be routed using ISDN. Note the following: ▪ Only the booking/dialing options applicable to a particular system will be displayed. ▪ Unchecking the **Allow Booking** box only affects new conferences. ▪ Changing any of the Dialing options could affect the routing of existing conferences. ▪ If you change any of the Dialing options for a system we recommend running **Conference Diagnostics** to identify any resulting issues with existing conferences.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Clicking **Force Refresh** updates the information displayed from the system.

For Unified CM-registered endpoints, the refreshed status is read from Unified CM. The button has no effect for endpoints behind a firewall/NAT.

An **Enforce Management Settings** button is available for most direct-managed systems. Clicking this button will:

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
  For Unified CM-registered endpoints, this IP address will be set as the **Feedback Address** instead.
- Update settings for **Daylight Saving Time**, **Time Zone** and **IP address**, and the paths for **Phonebook Settings** and **External Services**.
- For legacy systems that communicate with Cisco TMS using SNMP, such as Cisco TelePresence MXP systems, the **Traphost IP Address** is also set. This is done automatically on all systems if **Enforce Management Settings on Systems** is enabled in **Administrative Tools > Configuration > Network Settings**, see Network Settings, page 237.

Extended Settings

The following values are set at the TelePresence Conductor level and apply to all aliases configured for the TelePresence Conductor in Cisco TMS:

Table 34 Numeric ID settings

Field	Description
Numeric ID Base	The first number Cisco TMS uses when creating the variable part of the alias. The combination of the non-variable part of the alias and this number will give the dial string that participants use to join the conference.
Numeric ID Step	Cisco TMS will add this number to the **Numeric ID Base** to avoid duplicated aliases. As conferences finish, the alias will be made available to new conferences.
Numeric ID Quantity	The number of times Cisco TMS will increase the number from the Numeric ID Base, using the Numeric ID Step increment. The default is: *Unlimited*.

The following tables show examples of aliases generated from example Numeric ID values for both Unified CM and Cisco VCS deployments:

Table 35 Numeric ID example

Field	Example value
Numeric ID Base	`000`
Numeric ID Step	`1`
Numeric ID Quantity	`999`

Table 36 Examples of aliases generated from example Numeric ID values

	Unified CM	Cisco VCS
Alias Pattern	`5%`	`meet.%@example.org`
First generated alias	`5000`	`meet.000@example.org`
Second generated alias	`5001`	`meet.001@example.org`
Last possible alias	`5999`	`meet.999@example.org`

The following settings can also be modified per conference during booking:

Table 37 Additional Extended Settings for TelePresence Conductor

Field	Description
Conference Layout	Set the default layout for all conferences. For more information about conference layouts, see Cisco TelePresence Conductor Administrator Guide.
Limit Ports to Number of Scheduled Participants	Limit ports to the number of scheduled audio and video participants for all conferences. No additional participants will be able to join conferences.

TelePresence Conductor

On this tab, you can create, modify, and view conference alias patterns for use when booking conferences with TelePresence Conductor. The alias provides a pattern which will create a conference address that participants will dial to join a conference.

You can also view and calculate resource usage for Service Preferences on the TelePresence Conductor.

Aliases

This page displays a list of all aliases configured in Cisco TMS for this TelePresence Conductor.

Click **New** to create a new alias.

Select one or more aliases and click **Delete** to remove them.

The **Alias Pattern** column displays the alias pattern you have created as a regular expression. This can be copied and used when configuring both the Cisco VCS search rules and the TelePresence Conductor aliases.

Hover over the **Name** field of an alias and select **View/Edit** to display the Alias Configuration.

Table 38 Alias configuration settings

Name	Give the alias a name, for example: `Scheduled meeting`.
Alias Pattern	The pattern can be fixed or can contain a variable, which is denoted by `%`. For Cisco VCS deployments, we strongly recommend that the alias pattern contains a domain. The alias pattern must match one of the following: ■ The route pattern on the Unified CM. ■ The pattern string of the search rule targeting the neighbor zone to the TelePresence Conductor on the Cisco VCS. Examples: ■ Variable for Unified CM deployments: `5%` ■ Variable for Cisco VCS deployments: `meet.%@example.org` ■ Fixed: `allhands@example.org`, `1234@example.org` Note that the variable part of the alias will be generated by Cisco TMS from the **Numeric ID Base** configured for the TelePresence Conductor in **Systems > Navigator >** select the TelePresence Conductor **> Extended Settings**.
Priority	Give the alias a priority. The alias or variable alias pattern with the lowest number has the highest priority, and will be used first when Cisco TMS creates a conference. If that alias or variable aliases are already in use, the alias or alias patterns with the next highest number will be used, and so on. The priority can be any number between 0 and 65535.
Description	Enter a description of this alias.
Prefer for Multiscreen	Cisco TMS uses aliases with this field checked when selecting aliases for conferences including immersive TelePresence systems. The alias with the highest priority will be chosen first. If all the immersive aliases are in use, a non-immersive alias will be used for the conference. When this field is checked, immersive participants using this alias will connect using the **Default Immersive Bandwidth** set in **Administrative Tools > Configuration > Conference Settings**. If checked, ensure that the TelePresence Conductor conference template that this alias is configured to use has **Allow multiscreen** set to *Yes*.

Table 38 Alias configuration settings (continued)

Allow Booking	If *No* is selected, this alias will not be used by Cisco TMS in any bookings. This setting could be used if you want to stop using a particular alias, but it has a number of future bookings and therefore cannot be deleted. Disabling booking using this setting will enable the alias to be deleted once the final booking has taken place.
Allow Booking with Webex	Set to *Yes* to allow this alias to be used in bookings including Cisco Collaboration Meeting Rooms Hybrid.
Max Participants per Conference	This number is read from the TelePresence Conductor. When booking a conference with this alias, if more than this number of participants is selected it will not be possible to save the conference. The number is a theoretical maximum: the actual number of possible participants in a conference could be much lower depending on how the associated TelePresence Conductor conference templates are set up. This field is only populated if there is a corresponding alias on the TelePresence Conductor.
Max Screens per Participant	The maximum number of screens per participant for this alias. This field is only populated if there is a corresponding alias on the TelePresence Conductor.
Regular Expression	The regular expression of the alias.
Service Preference	The Service Preference that this alias is linked to. This field will display *None* if there is no corresponding alias on the TelePresence Conductor.

Future Conferences for this Alias

This section displays a list of all current and future conferences this alias is booked in, with a link to the **View Conference** page for each conference.

An alias that is in use in a current or future conference cannot be deleted or have its pattern modified.

Service Preferences

This page displays a list of the Service Preferences configured on this TelePresence Conductor and shows the **Bridge Type**, **Capacity Adjustment** and **Aliases** that are connected to them.

Hover over the **Name** field of a Service Preference and select **Details** to display the **Service Preference Configuration** and the **Resource Cost Calculator**.

Service Preference Configuration

Capacity Adjustment

TelePresence Conductor reports the total capacity of a service preference to Cisco TMS. This setting allows you to specify what percentage of the total capacity will be available for scheduling conferences with this Service Preference.

We recommend using conference bridge pools that are reserved only for scheduling, in which case, do not change this setting. If, however, ad hoc and rendezvous conferences share the conference bridge pools being used for scheduling, setting the percentage to less than 100% reserves capacity for non-scheduled conferences.

It is also possible to set the percentage higher than 100%. If users regularly book more capacity than they use, for example 10 dial-ins for a conference where only 5 are ever used, you could set the Capacity Adjustment to 120% or higher.

Resource Cost Calculator

This tool helps you calculate what percentage of the total capacity of a service preference is used in different conference scenarios. You can enter:

- **Number of Conferences**
- **Participants per Conference**
- **Screens per Participant** (for multiscreen aliases only)

for each alias associated with the service preference. Cisco TMS will then calculate the resource that would be used if you were to set up these conferences.

No changes are made on the TelePresence Conductor when editing these values, the tool is purely to help you calculate how much resource will be used depending on the types of system used and number of participants.

Conference Bridges

This tab lists the bridges that are in the conference bridge pools on the selected TelePresence Conductor.

Table 39 Columns on the Conference Bridges tab

Column	Description
System Name	System name in Cisco TMS. If the system is not in Cisco TMS, a warning about this will be displayed.
Type	The system type and model.
Network Address	The IP address or hostname of the system.
View System Details	This link will be displayed for all systems added to Cisco TMS. Click to launch system details in a separate window.

Clustering

On this tab, you can view the primary and peer TelePresence Conductors and view the status of primary and peer TelePresence Conductor. If the nodes are reachable and Cisco TMS can communicate with them normally, the status is *OK*. Otherwise the status is *Inaccessible*.

Connection

Table 40 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.

Table 40 Connection parameters for system communication on the Connection tab (continued)

Field	Description
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
SNMP Get Community Name	The SNMP get community name for the system. Only visible for systems that support SNMP community names.
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname* ■ *MAC Address*
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Replace System

On this tab, you can replace the system with a new one that will have the exact same name, role and configurations.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 41 The Logs contains all available logs for the system

Log	Description
Feedback Log	A detailed log describing all events that are registered for a particular system, including scheduling, errors, and encryption status. You will be able to see the 100 last events for the system.

Table 41 The Logs contains all available logs for the system (continued)

Log	Description
History	All detected changes that have been made to the system in Cisco TMS.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

TelePresence Conductor Clustering

Clusters of TelePresence Conductor are used in the rare case of failure of an individual TelePresence Conductor (for example, due to a network or power outage). Each TelePresence Conductor is a peer of the other TelePresence Conductor in the cluster. Each peer knows about all conferences.

Adding and Configuring the Primary TelePresence Conductor

Perform the following tasks to add and configure a TelePresence Conductor cluster:

Task 1: Adding the Primary TelePresence Conductor

Decide which TelePresence Conductor is to be the primary TelePresence Conductor. In this example, we refer to the first TelePresence Conductor as the primary TelePresence Conductor.

Note: The configuration of this system is shared with all other subordinates as they are added to the cluster.

Perform the following steps to add the primary TelePresence Conductor:

1. Go to **Systems > Navigator**.
2. Click **Add Systems**. The **Add by Address** tab is displayed.
3. Enter the appropriate information in the fields. See Add Systems, page 134 for further details.
4. Click **Next**.
5. Click **Finish Adding Systems**.

Task 2: Configuring the Primary TelePresence Conductor

You must configure the primary TelePresence Conductor and add the TelePresence Conductor bridges to it before you add the subordinate TelePresence Conductor to the cluster. Perform the following steps to configure an alias and the TelePresence Conductor bridges:

Configure Alias

1. Select the primary TelePresence Conductor and click the **TelePresence Conductor** tab.
2. Click **New**.
3. Enter the appropriate values by following the steps explained in TelePresence Conductor Tab.
4. Ensure that there is no open ticket available for alias configuration under the **Summary** tab.

Configure TelePresence Conductor Bridges

Perform the following steps to configure the TelePresence Conductor bridges:

1. Select the primary TelePresence Conductor and click the **Conference Bridges** tab.
2. Make a note of the network address, in the **Network Address** section.

3. Go to **Systems > Navigator**.
4. Click **Add Systems**.
5. Under **Specify Systems by IP Addresses or DNS Names** tab enter the network address that is displayed in the **Conference Bridges** tab.
6. Click the **Advanced Settings** tab.
7. Enter the **Username** and **Password** of the bridge.
8. Click **Next**.

Task 3: Adding subordinate TelePresence Conductor

Perform the following steps to add the subordinate TelePresence Conductors:

1. Go to **Systems > Navigator**.
2. Click **Add Systems**. The **Add by Address** tab is displayed.
3. Enter the appropriate information in the fields. See Add Systems, page 134 for details.
4. Click **Next**.
5. Click **Finish Adding Systems**
6. Click **Next**.

You must preform the following steps on the primary and subordinate conductors to successfully complete the Conductor Cluster configuration:

1. Go to **Systems > Navigator**.
2. Select a TelePresence Conductor.
3. Click the **Settings** tab.
4. Click **Force Refresh**.

Cisco Meeting Server

In Cisco TMS: **Systems > Navigator** Cisco Meeting Server is selected

For information about the configuration options and maintenance of Cisco Meeting Server, see Cisco Meeting Server Guides for your version.

Summary

Table 42 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.

Table 42 The Summary tab presents the most important data for the system (continued)

Section	Description
System Status	An overview of system statuses and updates for the selected Cisco Meeting Server system. The possible status messages are: ■ *Call Bridge Uptime* ■ *CallLegs Active* ■ *CallLegs Max Active* ■ *CallLegs Completed* ■ *Audio Bit Rate Outgoing* ■ *Audio Bit Rate Incoming* ■ *Video Bit Rate Outgoing* ■ *Video Bit Rate Incoming* Note that Cisco TMS does not update the system statuses when Cisco Meeting Server connection status is *No HTTPS response*. In this case, the values for the above status messages are displayed as *ZERO*.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
Book conference with this system	This link does navigate to new conference web page without any participants added into it.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 43 Sections in View Settings and Edit Settings

Section	Description

Table 43 Sections in View Settings and Edit Settings (continued)

General	The most important settings for the system, such as: ■ **Name** ■ **System Type** ■ **Manufacturer** ■ **Network Address** ■ **System Connectivity** ■ **Track System by** ■ **TMS System ID** ■ **IP Zone** ■ **Time Zone** ■ **Status** ■ **Your Access** ■ **System Contact** ■ **Alert System Contact When Booked** ■ **Description** ■ **Folders with system** ■ **Web Bridge URI**: Web Bridge URI is included in the conference booking confirmation email and in the **Meeting Landing Page**. This option allows a user to click and join a meeting instantly. **Web Bridge URI** can only be configured, if the **Web Bridge URI** details are provided when a Cisco Meeting Server is added. You must enter the same URI that is configured for Cisco Meeting Server Web Bridge URI. Specify a port along with the URI, if the port is not same as the default port 443.
Configuration	Displays the system's software version.
Network Settings	**Alternate IP**: The IP address of an alternate bridge in the call bridge cluster is used for TMS to Cisco Meeting Server communication. The Webadmin and Callbridge services must be running. Select an alternate IP to be used for Cisco Meeting Server failover support. The **Alternate IP** drop-down list displays the IP addresses of the clustered call bridge nodes. **Alternate IP Username**: Enter the username of the selected Alternate IP. **Alternate IP Password**: Enter the password of the selected Alternate IP.
TMS Scheduling Settings	**Allow Booking**: Allows the system to be added to conferences. **Allow Incoming SIP URI Dialing**: Allows calls to the system to be routed using a SIP URI. **Allow Outgoing SIP URI Dialing**: Allows calls from the system to be routed using a SIP URI. Note that unchecking the **Allow Booking** box only affects new conferences. **Allow Incoming H.323 Dialing**: Allows calls to the system to be routed using H.323. **Allow Outgoing H.323 Dialing**: Allows calls from the system to be routed using a H.232. Both the options are enabled by default, however you have to manually enable them when you upgrade from Cisco TMS 15.3 to 15.4. Note that H.323 incoming and outgoing dialing works when VCS is configured to provide H.323 to SIP interworking in Cisco Meeting Server deployment. Disable both the options, if Cisco Meeting Server is registered with Cisco Unified Communications Manager.

Any errors and warnings on system settings are displayed in red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Click **Force Refresh** to update the information displayed from the system.

Extended Settings

Table 44 The Extended Settings tab presents the most important data for the system

Section	Description
Domain	Enter the domain name.
Numeric ID Base	The first number that Cisco TMS uses when creating the variable part of the alias. The combination of the non-variable part of the alias and this number will give the dial string that participants use to join the conference. The Numeric ID Base must be greater than zero and less than 19 characters. Note: When configuring a Numeric ID Base for Cisco Meeting Server, ensure that the Numeric ID does not begin with 0.
Numeric ID Quantity	The number of times Cisco TMS will increase the number from the Numeric ID Base and it will be increased by one.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Clustering

The **Clustering** tab appears only when a clustered Cisco Meeting Server is added.

Notes:

1. Cisco TMS does not support management of a cluster. However the alternate cluster node IP address is used for TMS to Cisco Meeting Server communication for conference allocation, if the primary node is unreachable.
2. In Cisco TMS when a standalone Cisco Meeting Server is moved to a cluster, you can perform **Force Refresh** operation on the Cisco Meeting Server. After **Force Refresh** operation is completed, **Clustering** tab is enabled from where you can check the list of nodes of primary Cisco Meeting Server. The future meetings that were created before clustering will continue to run without any issues.
3. The clustered Cisco Meeting Server node should be added via IP or FQDN format and must match the format of the addresses listed in Cisco Meeting Server under the Configuring the Cluster Call Bridges, page 108 section.

Connection

Table 45 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.

Table 45 Connection parameters for system communication on the Connection tab (continued)

Field	Description
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.
Hostname	The hostname for the system.
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname*
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 46 Contains all available logs for the system

Log	Description
History	All detected changes that have been made to the system in Cisco TMS.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Cisco Meeting Server Configuration

Cisco Meeting Server can now be added in Cisco TMS as a managed bridge to schedule a conference. The key benefits of using Cisco Meeting Server for scheduling are as follows:

- Unprecedented capacity to manage large number of calls on a Clustered Call Bridge.
- Automatic failover with no single point of failure for meetings that are about to begin, when an alternate IP is configured.

Note the following points before you add a Cisco Meeting Server in Cisco TMS:

- You must configure the cluster call bridges in Cisco Meeting Server and then add the primary Cisco Meeting Server in Cisco TMS.
- It is not mandatory to add the Cisco Meeting Server node where the master database is hosted in Cisco Meeting Server cluster as the primary managed node in TMS. The Cisco Meeting Server node that is added in Cisco TMS is identified as primary Cisco Meeting Server from TMS.
- It is mandatory to enter the **Username** and **Password**, to add a Cisco Meeting Server.
- Cisco TMS supports Cisco Meeting Server version 2.0 and above. Cisco Meeting Server can only be tracked by *IP Address* or *Hostname*.

Adding the Primary Cisco Meeting Server

Decide which Cisco Meeting Server is to be the primary Cisco Meeting Server.

Then perform the following steps to add the primary Cisco Meeting Server:

1. Go to **Systems > Navigator**.
2. Click **Add Systems**. The **Add by Address** tab is displayed.
3. Enter the appropriate information in the fields. See Add Systems, page 134 for further details.
4. In the **Advanced Settings** section, enter **Username** and **Password**.
5. Click **Next**.
6. Click **Finish Adding Systems**.

A Cisco Meeting Server can also be added by its IPv6 address when IPv6 is configured for the Cisco Meeting Server. Enter the address in `[IPv6 address]:port number` format to add the Cisco Meeting Server. Note that the port number is mandatory for IPv6.

If Cisco Meeting Server Web Admin is configured to listen on a specific port other than the default port (often in the case for single-server deployments), then port number is mandatory to add Cisco Meeting Server in Cisco TMS. The default port is 443.

Configuring Cisco Meeting Server

Perform the following tasks to configure the Primary Cisco Meeting Server:

Task 1: Enter the System Name

When a Cisco Meeting Server is added for the first time, the system name is displayed as *No Name*. Enter a system name:

1. Navigate to **Systems > Navigator >** Select a Cisco Meeting Server **> Settings > Edit Settings > General**.
2. Enter the system name in the **Name** field.
3. Click **Save**

Task 2: Configure the Dial Number

Perform the following steps to configure a Dial Number:

1. Navigate to **Systems > Navigator >** Select a Cisco Meeting Server **> Settings > Extended Settings**.
2. Enter appropriate details in **Domain**, **Numeric ID Base** and **Numeric ID Quantity** fields.
3. When selecting save, the TMS will run through a process to remove all existing TMS created coSpaces, and will create a new set of coSpaces for the desired numbering schema. This process could also be used to recreate any TMS created coSpace that may have been deleted from the Cisco Meeting Server through other means. To do so, a change to the numbering schema is not needed.
4. Click **Save**.

We recommend not to change the Dial Number settings frequently and only do so if necessary. Do the following before you make any changes in dial number configuration when it is required:

- Make change during a maintenance window only.
- If future conferences are scheduled, run the **Diagnostics Tool** after making the changes.
- Be aware that the **Save** button is disabled during an ongoing conference.

Cisco TMS checks the callProfile and callLegProfile that are created by Cisco TMS on Cisco Meeting Server, in every 24 hours. If the profiles are deleted, Cisco TMS recreates the profiles and reassociates them with the cospaces that are created by Cisco TMS. The Administrator can perform a **Force Refresh** in the **View Settings** page to initiate the process manually without waiting for 24 hours. System level profiles are used during the duration when Cisco TMS created profiles have got deleted.

Task 3: Configure Web Bridge URI

The **Web Bridge URI** option allows a user to click and join a conference instantly. This option can only be configured when **Web Bridge** is configured in Cisco Meeting Server.

Perform the following steps to configure **Web Bridge URI**:

1. Navigate to **Systems > Navigator >** select a Cisco Meeting Server **> Settings > Edit Settings > General**
2. Enter the URI in **Web Bridge URI** field.
   You must enter the same URI that is configured on Cisco Meeting Server for Web Bridge. After successfully configuring the URI on Cisco TMS, you can update the Web Bridge URI. Specify a port along with the URI, if the port is not same as the default port 443.
3. Click **Save**.

Preform the following steps to configure WebBridge URI for Cisco Meeting Server cluster on TMS:

1. Configure common domain-name (for example oneclick@domain.com) in Domain Controller for all Cisco Meeting Server clustered nodes.
2. Ensure that same Web Bridge port number is set for all Cisco Meeting Server clustered members. For example 470.
3. On all Cisco Meeting Server clustered members console, configure **Webbridge > Clickonce URL**. For example https://oneclick@domain.com:470.
4. Set the common domain-name in Cisco Meeting Server web interface, under **Configuration > General > External access > Web Bridge URI**. For example https://oneclick@domain.com:470.
5. When you add one of the clustered Cisco Meeting Server node in TMS, enter the **Web Bridge URI** in TMS with the common domain-name:port format. For example, https://oneclick@domain.com:470.

Configuring the Cluster Call Bridges

Cluster nodes of Cisco Meeting Server are used to support the failure of an individual Cisco Meeting Server (for example, due to network or power outage).

The alternate IPs are fetched from the Cisco Meeting Server, that are configured with clustered call bridges. Perform the following steps to configure cluster call bridges:

1. Go to **Systems > Navigator >** Select a Cisco Meeting Server **> Settings > Edit Settings**.
2. Select an alternate IP from the **Alternate IP** drop down list under **Network Settings** section.
3. Enter alternate IP username and password in **Alternate IP Username** and **Alternate IP Password** fields.
4. Click **Save**.

Ensure the Cisco TMS Connection Settings for Cisco Meeting Server node matches the clustered CB Address taken from Cisco Meeting Server (including port details).

When Cisco Meeting Server nodes is added to Cisco TMS, an IP address or FQDN is used followed by a port number.

- If the standard HTTPS port 443 is configured on the Cisco Meeting Server side for webadmin and is used to add the Cisco Meeting Server node to Cisco TMS, the connection details will not retain the default port details for 443.
- If the Clustered Call bridges are addressed in Cisco Meeting Server with port 443 specified, the following error is displayed in the Cisco TMS **Clustering** tab: "FQDN_or_IP_of_CMS_node is not part of the cluster call bridge nodes fetched from Cisco Meeting Server. Ensure that the clustering in Cisco Meeting Server is configured either with the hostname or IP address in both Cisco TMS and Cisco Meeting Server".

Note the following points:

- When the cluster nodes in Cisco Meeting Server are added using the IP address, ensure that the cluster nodes in TMS are also added using IP address. This rule is applicable for adding through IPv6 and host name.
- Cisco Meeting Server failover support on Cisco TMS, is intended to handle the conferences that are about to begin. The failover functionality does not work for an ongoing conference. If a meeting is allocated on an alternate Cisco Meeting Server due to a failover event, and the master Cisco Meeting Server becomes accessible again during the course of meeting, further operations from Cisco TMS to the conference will be to the master Cisco Meeting Server, and this may cause the operation to fail. For example: Dial- out commands. Only one **Alternate IP** configuration is supported by Cisco TMS. If both the master node and alternate IP are down, Cisco TMS does not use other clustered call bridges that are part of the clustered Cisco Meeting Server.
- During failover, the conference event logs show the primary Cisco Meeting Server instead of alternate Cisco Meeting Server. By default the details about the current failover can be seen in the `log-cmsfailover-liveservice` log.
- Only one Cisco Meeting Server cluster call bridge node has to be managed by Cisco TMS.
- If an existing Cisco TMS-managed Cisco Meeting Server needs to be clustered, first remove all individual Cisco Meeting Servers, except the one that shall be used as the primary server. After configuring the call cluster bridges in Cisco Meeting Server, perform a Force refresh on the Primary Cisco Meeting Server in Cisco TMS.
- To uncluster an existing Cisco TMS managed Cisco Meeting Server, first remove the managed Cisco Meeting Server node from Cisco TMS, then uncluster the call bridges in Cisco Meeting Server. Execute **database cluster remove** and **factory-reset app** on Cisco Meeting Server console to ensure that the node is completely unclustered.
- When one of the Cisco Meeting Server cluster member is managed by Cisco TMS, then other members of the cluster cannot be added in Cisco TMS as a managed bridge.
- To add an existing TMS managed standalone Cisco Meeting Server as part of Cisco TMS managed clustered Cisco Meeting Server node, first remove the managed stand-alone and clustered Cisco Meeting Server nodes from TMS and then add the clustered node back in TMS.

- During failover, when primary node of Cisco Meeting Server in Cisco TMS is unreachable, the secondary node becomes primary node. Cisco TMS does not update the changed status of the old primary node and continues to consider secondary node as primary node.

Cisco Meeting Server Profiles

Cisco TMS checks the callProfile and callLegProfile that are created by Cisco TMS on Cisco Meeting Server, in every 24 hours. If the profiles are deleted, Cisco TMS recreates the profiles and reassociates them with the cospaces that are created by Cisco TMS. Administrators can perform a **Force Refresh** in the **View Settings** page to initiate the process manually without waiting for 24 hours. System-level profiles are used for the period that the TMS-created profiles are deleted.

Scheduling

Cisco TMS admin can select the desired bandwidth for Cisco Meeting Server to host the conference, when Cisco Meeting Server is added as a participant and the conference is scheduled.

Note: Cisco TMS 15.6 release onwards, option to choose the bandwidth for conference hosted on Cisco Meeting Server has been enabled. If the client is upgrading from the previous Cisco TMS release, they will experience a difference in the quality of call hosted on Cisco Meeting Server. As the default bandwidth in earlier versions is 6144 kbps and in Cisco TMS 15.6 onwards default bandwidth is 512 kbps. Cisco TMS admin needs to explicitly select the desired **IP Bandwidth** while creating the conference from Cisco TMS portal.

The following features are not supported for Cisco Meeting Server in Cisco TMS:

- Webex enabled conferences
- **Conference Control Center**
  You can however view Cisco Meeting Server in the **Edit Conference** and **Add Participants** section for the conferences that are scheduled on other bridges.
- **ISDN Bandwidth** and **ISDN Restrict**
- Best Impression Routing
- Least Cost Routing
- Recording

You can only select the following options under **Booking > New Conference > Advanced Settings**, when you add Cisco Meeting Server and book a new conference:

- *Continuous Presence* in **Picture Mode**.
- *Automatic Best Effort* in **Extend Mode**.
- *If Possible* in **Secure**.

Support for Dial Out from an Unmanaged Cisco Meeting Server Cluster Call Bridge Node

This feature is applicable for Cisco Meeting Server 2.2 and below versions only and is not available for Cisco Meeting Server version 2.3 and above. For Cisco Meeting Server version 2.3, you must use Cisco Meeting Server Load Balancing feature.

Cisco TMS can now distribute a conference dial out among the CallBridge nodes which are not directly managed by Cisco TMS. This happens when one of the CallBridge nodes in a Cisco Meeting Server cluster CallBridge setup is managed by Cisco TMS.

By default Cisco Meeting Server outbound dial plan rules have global scope and it is common to all the CallBridge nodes in the cluster setup. Load balance among the clustered CallBridge nodes is achieved by creating the Outbound Dial Plan Rules with CallBridge scope. This makes the Outbound Dial Plan Rule specific to a single nominated CallBridge.

Cisco TMS internally uses Cisco Meeting Server feature to initiate dial-out from the unmanaged Cisco Meeting Server cluster CallBridge node based on the Outbound Dial Plan Rules.

The steps and configuration details are as follows:

1. Take a Cisco Meeting Server cluster with three nodes (For example: Cisco Meeting Server-1, Cisco Meeting Server-2, Cisco Meeting Server-3). On Cisco TMS add Cisco Meeting Server-1 as primary node and keep the **Alternate IP** field as **None**. So that Cisco Meeting Server-2 and Cisco Meeting Server-3 are unmanaged bridges for Cisco TMS.

2. Using Mozilla poster, perform the **POST** request operation, given below to create the Outgoing Calls Dial pattern:

```
URL:

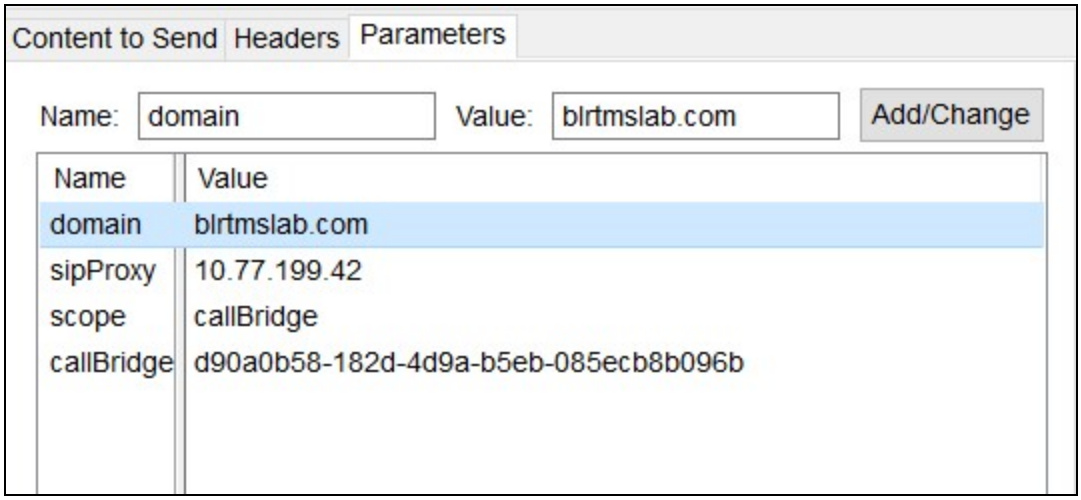
https<ip address of Cisco Meeting Server-2>/api/v1/outboundDialPlanRules/

Parameters:

domain = blrtmslab.com ( vcs domain)
sipProxy = 10.77.199.42 ( vcs IP address)
scope = callBridge
callBridge = 107c9daf-fde8-4dd7-b02c-22460357c5b1 ( callBridge ID of Cisco Meeting Server-2)
```

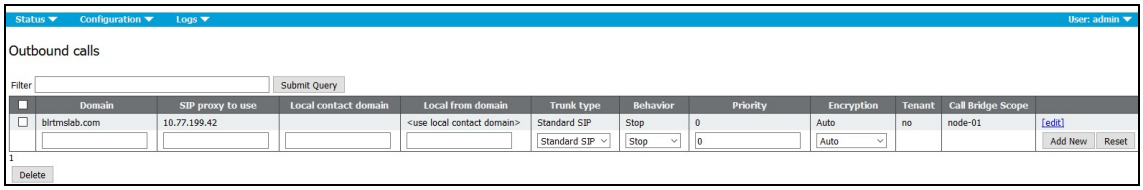
Note: **callBridge ID** can be generated by performing the **GET** operation like **https://<ip address of Cisco Meeting Server- 2>/api/v1/callBridges/**.

For parameters in Mozilla Poster, refer to the following screen shot:

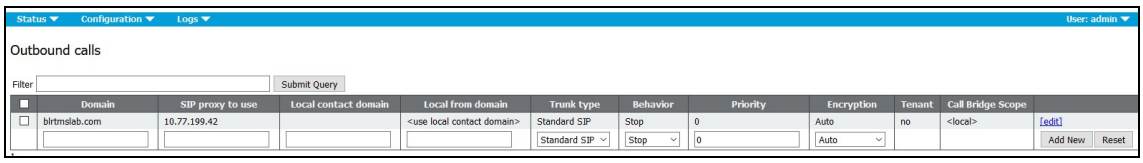


After the above operation is completed, from **POSTER**, the dial patterns on Cisco Meeting Server outgoing calls is displayed in the following screen shots:

On Cisco Meeting Server-1 (managed by Cisco TMS):



On Cisco Meeting Server-2 (not managed by Cisco TMS):



After this, schedule a meeting from Cisco TMS with Cisco Meeting Server cluster and one endpoint (which is registered to VCS with the above mentioned domain name). It can be seen that the outgoing calls are dialed from Cisco Meeting Server-2 which is not managed by Cisco TMS.

Refer the **Creating and modifying outbound dial plan rules** section in Cisco Meeting Server API Reference Guide for the configuration steps.

Support for Meeting Owner in Cisco Meeting Server Scheduled Meeting

Cisco TMS sets the name of the Cisco TMS user who schedules the meeting (or who the meeting is scheduled on behalf of) to the **meetingScheduler** field in Cisco Meeting Server co-space when a meeting is allocated. If this user is part of the Cisco Meeting Server users list, then the user is set as the owner for the co-space for the scheduled duration. It is updated only when the meeting is allocated on the co-space and is active only for the meeting duration.

Note: This feature is available only for Cisco Meeting Server 2.2 and above.

Support for handling Load Balancing on Cisco Meeting Server

Cisco TMS sets `activeWhenEmpty` parameter to **false** while creating the call object on Cisco Meeting Server, this helps Cisco TMS to control the load balancing on the Cisco Meeting Server conference created by Cisco TMS. For more information, refer to Cisco Meeting Server Release Notes 2.2.

Note: This feature is available only for Cisco Meeting Server 2.2 and above.

MCUs and TelePresence Server

In Cisco TMS: **Systems > Navigator** MCU or TelePresence Server is selected

Summary

Table 47 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.
Service Contract Status	An overview of service contract status and updates for the selected system, including expiry date, release keys for the latest major software versions, and a link to check for software updates. Possible status messages are: ▪ *Service contract is valid and ok* ▪ *Service contract is ordered, but not invoiced* ▪ *Service contract is expired* ▪ *No service contract* ▪ *Draft* ▪ *New Revision* ▪ *Bought by current partner* ▪ *Unknown* This field is not applicable to or displayed for all systems.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.

Table 47 The Summary tab presents the most important data for the system (continued)

Section	Description
Phone Books	Any phone books set on the system (only displayed for endpoints, MCUs, and gateways that support phone books).
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.
Book conference with this system	This link does navigate to new conference web page without any participants added into it.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 48 Sections in View Settings and Edit Settings

Section	Description
General	The most important settings for the system, such as: ▪ **Name** ▪ **System Type** ▪ **Network Address** ▪ **Location** ▪ **System Connectivity**
Configuration	Lists the system's software and hardware version and time of last backup and restore. For TelePresence Server: **Operation mode**: *Remotely Managed* or *Locally Managed* A TelePresence Server that is in *Remotely Managed* mode is only supported if it is managed by a TelePresence Conductor that is present in Cisco TMS.
Network Settings	In this section you will find H.323 gatekeeper and SIP server registration information, the NTP (Network Time Protocol) server setting and IP configuration information. For TelePresence Server and TelePresence MCUs that are SIP-trunked to a Unified CM, the SIP Mode is read from the bridge and displayed here.
Monitoring/SNMP Settings	In this section the trap host and management IP addresses and SNMP community are found. The trap host and management addresses should be the IP address of the Cisco TMS server that administrates the systems. Legacy Cisco TelePresence MXP endpoints use the management address to send traps.

Table 48 Sections in View Settings and Edit Settings (continued)

TMS Scheduling Settings	**Allow Booking**: Allows the system to be added to conferences. **Allow Webex Booking**: Allows bridges to host Webex conferences. **Allow Incoming IP Address Dialing**: Allows calls to the system to be routed using H.323 direct mode. **Allow Incoming H.323 Dialing**: Allows calls to the system to be routed using an E.164 alias or H.323 ID. **Allow Incoming SIP URI Dialing**: Allows calls to the system to be routed using a SIP URI. **Allow Incoming ISDN Dialing**: Allows calls to the system to be routed using ISDN. **Allow Incoming Telephone Dialing**: Allows calls to the system to be routed using ISDN. **Allow Outgoing IP Address Dialing**: Allows calls from the system to be routed using H.323 direct mode. **Allow Outgoing H.323 Dialing**: Allows calls from the system to be routed using an E.164 alias or H.323 ID. **Allow Outgoing SIP URI Dialing**: Allows calls from the system to be routed using a SIP URI. **Allow Outgoing ISDN Dialing**: Allows calls from the system to be routed using ISDN. Note the following: ■ Only the booking/dialing options applicable to a particular system will be displayed. ■ Unchecking the **Allow Booking** box only affects new conferences. ■ Changing any of the Dialing options could affect the routing of existing conferences. ■ If you change any of the Dialing options for a system we recommend running **Conference Diagnostics** to identify any resulting issues with existing conferences.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Clicking **Force Refresh** updates the information displayed from the system.

For Unified CM-registered endpoints, the refreshed status is read from Unified CM. The button has no effect for endpoints behind a firewall/NAT.

An **Enforce Management Settings** button is available for most direct-managed systems. Clicking this button will:

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
  For Unified CM-registered endpoints, this IP address will be set as the **Feedback Address** instead.
- Update settings for **Daylight Saving Time**, **Time Zone** and **IP address**, and the paths for **Phonebook Settings** and **External Services**.
- For legacy systems that communicate with Cisco TMS using SNMP, such as Cisco TelePresence MXP systems, the **Traphost IP Address** is also set. This is done automatically on all systems if **Enforce Management Settings on Systems** is enabled in **Administrative Tools > Configuration > Network Settings**, see Network Settings, page 237.

Extended Settings

These settings for both MCU and TelePresence Server can only be set in the Cisco TMS extended settings. They cannot be modified per conference or set directly on the systems, and they are ignored if TelePresence Conductor is managing the MCU or TelePresence Server.

Table 49 Numeric ID settings

Field	Description
Numeric ID Base	The first number in a sequence sent to conference participants from Cisco TMS. The number is used as the base for the numeric ID needed when dialing into the bridge hosting the conference. The numeric ID is included in the booking confirmation email message.
Numeric ID Step	Cisco TMS will add this number to the **Numeric ID Base** to avoid duplicated numeric IDs. As conferences finish, their IDs will be made available to new conferences.
Numeric ID Quantity	The maximum number of concurrent meeting IDs that can be generated.

Cisco TelePresence MCU

The following settings can also be modified per conference during booking.

Not all of the settings below are available for all Cisco TelePresence MCU models.

Table 50 Extended MCU settings

Setting	Description
Enable ISDN Gateway DID Mapping	DID (Direct Inbound Dialing) allows for inbound ISDN connections to MCUs without ISDN support. For instructions on setting up DID, see the documentation for your gateway. For more information, see Extended Settings DID Mapping for Cisco TelePresence MCUs, page 37.
Conference Layout	Defines the picture layout for the conference. There are several alternatives to select between. For more information about conference layouts, see the documentation for your MCU.
Visibility	Indicates the visibility of the conference on the auto attendant and the web interface. The options are: ■ *Public*: The conference will be listed in the auto attendant and be visible to all users of the web interface. ■ *Private*: The conference will not be listed in any auto attendant except for auto attendants specifically set to show it. The conference will also only be visible in the web interface to the conference owner and to the admin user.
Dual Video Stream	Enable an additional video stream, such as a presentation.
Content Mode	Determine the mode for sending content packet streams. The options are: ■ *Disabled*: Content is not transmitted. ■ *Passthrough*: Content is not decoded and is simply repackaged and sent out to each eligible endpoint in the conference. ■ *Hybrid*: The MCU sends out two content streams: a higher resolution one (passthrough), and a lower resolution stream transcoded and scaled down for any endpoints that are unable to support the higher stream. ■ *Transcoded*: A single transcoded content stream is sent.

Table 50 Extended MCU settings (continued)

Setting	Description
Register with Gatekeeper	Registers the conference with the H.323 registrar.
Conference SIP registration	Registers the conference with the SIP registrar.
Allow Chair Control	Floor and chair control is encompassed by the H.243 protocol. The options are: ■ *None*: The use of floor and chair controls is not allowed in this conference. ■ *Floor Control Only*: Only floor control is allowed in this conference. Chair control is not allowed. Any participant can 'take the floor' so long as no other participant has currently has done so. ■ *Chair and Floor Control*: Both floor and chair controls are allowed in this conference. Any participant can take the floor, and any chairperson participant can take the chair so long as no other participant has currently done so.
Allow Layout Control	Enable conference participants to control the conference layout using DTMF signals or far-end camera control.
Automatic Lecture Mode	When this feature is enabled for a conference, the MCU identifies the loudest speaker as the lecturer. The lecturer will see a normal continuous presence view or a custom layout, if defined. For the other participants, the view of the lecturer will override any custom layout. The options are: ■ *Disabled* ■ *After 10 seconds* ■ *After 30 seconds* ■ *After 1 minute* ■ *Immediately*
Ports to Reserve for ConferenceMe	If using the ConferenceMe feature on the MCU, ports can be reserved for it using this field.
Limit Ports to Number of Scheduled Participants	Limit ports to the number of scheduled audio and video participants. No additional participants will be able to join the conference.
Multicast Streaming Enabled	Allows multicast streaming for the conference.
Unicast Streaming Enabled	Allows unicast streaming for this conference.

TelePresence Server

The following settings can also be modified per conference during booking.

Table 51 Extended TelePresence Server settings

Field	Description
Register With Gatekeeper	Register the conference's numeric ID with the gatekeeper (if H.323 registration is enabled on TelePresence Server).
Conference SIP Registration	Register the conference's numeric ID with the registrar (if SIP registration is enabled on TelePresence Server).
Dual Video Stream	Enable an additional video stream, such as a presentation.
Limit Ports to Number of Scheduled Participants	Limit ports to the number of scheduled audio and video participants. No additional participants will be able to join the conference.
Lock Conference on Creation	Lock the conference when it is created. You can still add pre-configured participants before the conference starts, but no participants will be able to join (call in) when the conference is active. You can call out to invite participants into a locked conference.
Conference Lock Duration	Number of seconds during which the conference will be kept locked (if enabled above).
Use Lobby Screen for Conferences	Enable TelePresence Server to display lobby screens to participants. The lobby screen shows the conference title, start and end times (if applicable), and an optional lobby message. The message is set on a per conference basis. Participants see this screen when they join a conference, or when there is no video to display. This is set to On by default when a TelePresence Server is added to Cisco TMS.
Conference Lobby Message	Enter text to display on the lobby screen. Participants will see this text if **Use Lobby Screen for conferences** is enabled server-wide or for their particular conference.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Call Status

If the system is in a conference, information about the current connection is shown on this tab. Any conferences scheduled for the day are also listed on the tab.

On this tab you can:

- Disconnect an ongoing call by clicking **Disconnect**.
- Get the latest information from the system by clicking **Refresh Page**.

Connection

Table 52 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
SNMP Get Community Name	The SNMP get community name for the system. Only visible for systems that support SNMP community names.
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname* ■ *MAC Address*
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Replace System

On this tab, you can replace the system with a new one that will have the exact same name, role and configurations.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and

System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 53 The Logs contains all available logs for the system

Log	Description
Feedback Log	A detailed log describing all events that are registered for a particular system, including scheduling, errors, and encryption status. You will be able to see the 100 last events for the system.
History	All detected changes that have been made to the system in Cisco TMS.
Call Log	Call Detail Records (CDRs) for the selected system, if available. For more information, see Call Detail Records, page 230.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Gateways

In Cisco TMS: **Systems > Navigator** a gateway is selected

For detailed information about gateway configuration and specific settings, see the documentation for your gateway model and software version.

Summary

Table 54 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
Phone Books	Any phone books set on the system (only displayed for endpoints, MCUs, and gateways that support phone books).
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 55 Sections in View Settings and Edit Settings

Section	Description

Table 55 Sections in View Settings and Edit Settings (continued)

General	The most important settings for the system, such as: ■ **Name** ■ **System Type** ■ **Network Address** ■ **Location** ■ **System Connectivity**
Configuration	Lists the system's software and hardware version and time of last backup and restore. For TelePresence Server: **Operation mode**: *Remotely Managed* or *Locally Managed* A TelePresence Server that is in *Remotely Managed* mode is only supported if it is managed by a TelePresence Conductor that is present in Cisco TMS.
Network Settings	In this section you will find H.323 gatekeeper and SIP server registration information, the NTP (Network Time Protocol) server setting and IP configuration information. For TelePresence Server and TelePresence MCUs that are SIP-trunked to a Unified CM, the SIP Mode is read from the bridge and displayed here.
Monitoring/SNMP Settings	In this section the trap host and management IP addresses and SNMP community are found. The trap host and management addresses should be the IP address of the Cisco TMS server that administrates the systems. Legacy Cisco TelePresence MXP endpoints use the management address to send traps.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Clicking **Force Refresh** updates the information displayed from the system.

For Unified CM-registered endpoints, the refreshed status is read from Unified CM. The button has no effect for endpoints behind a firewall/NAT.

An **Enforce Management Settings** button is available for most direct-managed systems. Clicking this button will:

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
  For Unified CM-registered endpoints, this IP address will be set as the **Feedback Address** instead.
- Update settings for **Daylight Saving Time**, **Time Zone** and **IP address**, and the paths for **Phonebook Settings** and **External Services**.
- For legacy systems that communicate with Cisco TMS using SNMP, such as Cisco TelePresence MXP systems, the **Traphost IP Address** is also set. This is done automatically on all systems if **Enforce Management Settings on Systems** is enabled in **Administrative Tools > Configuration > Network Settings**, see Network Settings, page 237.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Phone Book

Use the arrow buttons to set phone books on the system or remove existing phone books.

The button **Go to Manage Phone Books** will open the page Manage Phone Books, page 215.

For guidance on working with phone books, see Creating and Managing Phone Books, page 210.

Connection

Table 56 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
SNMP Get Community Name	The SNMP get community name for the system. Only visible for systems that support SNMP community names.
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname* ■ *MAC Address*
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 57 The Logs contains all available logs for the system

Log	Description
History	All detected changes that have been made to the system in Cisco TMS.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Content Servers and Recording Servers

In Cisco TMS: **Systems > Navigator** a content server or recording server is selected

For information about the configuration options and maintenance of Cisco TelePresence Content Server, see *Cisco TelePresence Content Server Administration and User Guide* for your version.

Note: Cisco TMS will only utilize content server's H323 configuration for Scheduling.

Content Server in Gateway Mode

If a Content Server is configured in Gateway mode, Cisco TMS will create a unique alias for each scheduled recording, instead of using the number for the recording alias that has been selected.

This individual generated alias is a longer random number unique to the conference, and has the same settings as the selected recording alias. The reason Cisco TMS does this is so that if the Content Server drops out of the conference temporarily, or the conference disconnects, the conference will continue recording to the original file when reconnected, instead of creating a new recording file.

Content Server in Terminal Mode

If a Content Server is configured in Terminal mode, the recording alias number will be used, and if the Content Server drops out or the conference disconnects, a new file will be created each time instead of continuing with the same file as before.

Summary

Table 58 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.

Table 58 The Summary tab presents the most important data for the system (continued)

Section	Description
Service Contract Status	An overview of service contract status and updates for the selected system, including expiry date, release keys for the latest major software versions, and a link to check for software updates. Possible status messages are: ■ *Service contract is valid and ok* ■ *Service contract is ordered, but not invoiced* ■ *Service contract is expired* ■ *No service contract* ■ *Draft* ■ *New Revision* ■ *Bought by current partner* ■ *Unknown* This field is not applicable to or displayed for all systems.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.
Book conference with this system	This link does navigate to new conference web page without any participants added into it.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 59 Sections in View Settings and Edit Settings

Section	Description
General	The most important settings for the system, such as: ■ **Name** ■ **System Type** ■ **Network Address** ■ **Location** ■ **System Connectivity**

Table 59 Sections in View Settings and Edit Settings (continued)

Configuration	Lists the system's software and hardware version and time of last backup and restore. For TelePresence Server: **Operation mode**: *Remotely Managed* or *Locally Managed* A TelePresence Server that is in *Remotely Managed* mode is only supported if it is managed by a TelePresence Conductor that is present in Cisco TMS.
Network Settings	In this section you will find H.323 gatekeeper and SIP server registration information, the NTP (Network Time Protocol) server setting and IP configuration information. For TelePresence Server and TelePresence MCUs that are SIP-trunked to a Unified CM, the SIP Mode is read from the bridge and displayed here.
Monitoring/SNMP Settings	In this section the trap host and management IP addresses and SNMP community are found. The trap host and management addresses should be the IP address of the Cisco TMS server that administrates the systems. Legacy Cisco TelePresence MXP endpoints use the management address to send traps.
TMS Scheduling Settings	**Allow Booking**: Allows the system to be added to conferences. **Allow Webex Booking**: Allows bridges to host Webex conferences. **Allow Incoming IP Address Dialing**: Allows calls to the system to be routed using H.323 direct mode. **Allow Incoming H.323 Dialing**: Allows calls to the system to be routed using an E.164 alias or H.323 ID. **Allow Incoming SIP URI Dialing**: Allows calls to the system to be routed using a SIP URI. **Allow Incoming ISDN Dialing**: Allows calls to the system to be routed using ISDN. **Allow Incoming Telephone Dialing**: Allows calls to the system to be routed using ISDN. **Allow Outgoing IP Address Dialing**: Allows calls from the system to be routed using H.323 direct mode. **Allow Outgoing H.323 Dialing**: Allows calls from the system to be routed using an E.164 alias or H.323 ID. **Allow Outgoing SIP URI Dialing**: Allows calls from the system to be routed using a SIP URI. **Allow Outgoing ISDN Dialing**: Allows calls from the system to be routed using ISDN. Note the following: ▪ Only the booking/dialing options applicable to a particular system will be displayed. ▪ Unchecking the **Allow Booking** box only affects new conferences. ▪ Changing any of the Dialing options could affect the routing of existing conferences. ▪ If you change any of the Dialing options for a system we recommend running **Conference Diagnostics** to identify any resulting issues with existing conferences. Note that scheduling IP VCR is not supported by Cisco TMS.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Clicking **Force Refresh** updates the information displayed from the system.

For Unified CM-registered endpoints, the refreshed status is read from Unified CM. The button has no effect for endpoints behind a firewall/NAT.

An **Enforce Management Settings** button is available for most direct-managed systems. Clicking this button will:

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
  For Unified CM-registered endpoints, this IP address will be set as the **Feedback Address** instead.
- Update settings for **Daylight Saving Time**, **Time Zone** and **IP address**, and the paths for **Phonebook Settings** and **External Services**.
- For legacy systems that communicate with Cisco TMS using SNMP, such as Cisco TelePresence MXP systems, the **Traphost IP Address** is also set. This is done automatically on all systems if **Enforce Management Settings on Systems** is enabled in **Administrative Tools > Configuration > Network Settings**, see Network Settings, page 237.

Compare Settings

This tab displays a comparative listing of the current settings on the system and any backed up configuration stored on the server. Any differences will be highlighted.

If settings are already stored on the server, two buttons will be available:

- **Make Backup**
- **Restore System**

If no settings have yet been stored on the server, only **Make Backup** will be available.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Active Calls

A list of all ongoing recordings and playbacks. This tab is displayed for Cisco TelePresence IP VCR and Cisco TelePresence VCR MSE.

Table 60 Fields on the Active Calls tab

Field	Description
Type	■ *Recording*: The IP VCR is recording the call. ■ *Playback*: The IP VCR is playing back a recording. ■ *Auto Attendant*: The call is displaying an auto attendant menu.
Recording Name	The name of the recording.
Participant Name	Name of the system on the other side of the call.
Call Protocol	Displays the call signaling protocol; either SIP or H.323.
Address	Address of the system on the other side of the call.
Duration (s)	Duration of call at the time of opening the tab.
Call Direction	Direction of the call (incoming is from system to IP VCR, outgoing is from IP VCR to system).

Call Status

This tab is only displayed for Cisco TelePresence Content Server.

Table 61 Columns on the Call Status tab

Columns	Description
Port	Descriptive name of port.
Name	If the port is in use, an identifier of the caller will be shown. Unused ports will show as *[Idle]*.
ISDN Number	Port ISDN number if available.
E.164 Alias	Port E.164 alias if available.
Video Calls	Number of live video connections.
Audio Calls	Number of live audio connections.

Connection

Table 62 Connection parameters for system communication on the Connection tab

Field	Description
Current Connection Status	The current status of the system. Only visible if the system can be reached by Cisco TMS.
Authentication Status	Username and password status for the system.
IP Address	IP Address for the system.
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
SNMP Get Community Name	The SNMP get community name for the system. Only visible for systems that support SNMP community names.
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname* ■ *MAC Address*

Table 62 Connection parameters for system communication on the Connection tab (continued)

Field	Description
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 63 The Logs contains all available logs for the system

Log	Description
Feedback Log	A detailed log describing all events that are registered for a particular system, including scheduling, errors, and encryption status. You will be able to see the 100 last events for the system.
History	All detected changes that have been made to the system in Cisco TMS.
Call Log	Call Detail Records (CDRs) for the selected system, if available. For more information, see Call Detail Records, page 230.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Unmanaged Bridge

In Cisco TMS: **Systems > Navigator** an unmanaged bridge is selected

Unsupported legacy and third party bridges (including Cisco TelePresence Multipoint Switch) can be added to Cisco TMS as unmanaged bridges, and scheduled in conferences.

For instructions on setting a system up as an unmanaged bridge, see Adding an Unmanaged Bridge, page 60.

Features

- An unmanaged bridge can be configured as **Immersive** if it supports hosting conferences including multiscreen systems. Unmanaged bridges that are configured as immersive are preferred in routing if multiscreen systems are added to a conference.
- If the conference includes participants that are controlled by Cisco TMS or registered to Unified CM, some limited monitoring of scheduled conferences hosted on unmanaged bridges is available in **Conference Control Center**. You can send participants messages, view basic details for each participant, and add participants to the conference.
- SIP and H.323 dial-in participants are fully supported.
- A Network Integration license key must be obtained for each unmanaged bridge before adding it into Cisco TMS. Up to 25 meeting addresses can be configured for each bridge, reflecting conference addresses that must already be created on the bridge itself.

Limitations

Cisco TMS can never connect to unmanaged bridges or read or make changes to their configuration.

Therefore, ending an unmanaged bridge conference from Cisco TMS will result in the conference appearing as finished, but endpoints will stay connected. Unmanaged bridge conferences are listed in **Booking > List Conferences**.

The following features are not supported for unmanaged bridges in Cisco TMS:

- Cascading, Ad Hoc calls, ISDN, call termination, resource guarantees
- Dial-out participants
- CMR Hybrid
- Native API support for Cisco TelePresence Multipoint Switch
- Reporting
- Guaranteed encryption
- Participant templates
- Meeting extension
- Meeting end notifications
- Automatic disconnection of conferences at scheduled end time

Summary

Table 64 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.
Book conference with this system	This link does navigate to new conference web page without any participants added into it.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 65 Sections in View Settings and Edit Settings

Section	Description
General	The most important settings for the system, such as: ■ **Name** ■ **System Type** ■ **Network Address** ■ **Location** ■ **System Connectivity**
Call Settings	**Maximum IP Bandwidth**: The Maximum IP Bandwidth Cisco TMS will use at any one time for all concurrent conferences on the bridge. Refer to your bridge's documentation for details of its maximum IP bandwidth. **Max Number of Video Calls**: The number of video ports on the bridge. This is the number of concurrent video participants that Cisco TMS will allow to be scheduled. **Max Number of Audio Calls**: The number of audio ports on the bridge. This is the number of concurrent audio participants that Cisco TMS will allow to be scheduled. Note the following: ■ If *0* is entered in **Max Number of Audio Calls**, the value set as the **Max Number of Video Calls** will be used as generic ports that can be used to book either video or audio participants. ■ If anything higher than *0* is entered in **Max Number of Audio Calls**, video and audio calls are counted separately and can not be used interchangeably. **Number of bridge addresses**: The number of concurrent meeting IDs that Cisco TMS will use on the bridge. **Immersive**: Specify whether the bridge will be preferred when routing conferences including multiscreen participants. **E.164 Alias/H.323 ID/SIP URI**: The addresses you have already configured on the bridge, as appropriate up to the number specified in **Number of bridge addresses**. Conferences with these addresses must already have been set up on the bridge. Depending on the bridge model, they may be described as Static or Permanent Conferences; refer to your bridge documentation for details.
Network Settings	H.323 gatekeeper and SIP server addresses. These are optional but will help Cisco TMS route conferences optimally.

Table 65 Sections in View Settings and Edit Settings (continued)

TMS Scheduling Settings	**Allow Booking**: Allows the system to be added to conferences. **Allow Incoming H.323 Dialing**: Allows calls to the system to be routed using an E.164 alias or H.323 ID. **Allow Incoming SIP URI Dialing**: Allows calls to the system to be routed using a SIP URI. Note the following: ■ Unchecking the **Allow Booking** box only affects new conferences. ■ Changing any of the Dialing options could affect the routing of existing conferences. ■ If you change any of the Dialing options for a system we recommend running **Conference Diagnostics** to identify any resulting issues with existing conferences.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Connection

As Cisco TMS does not connect to an unmanaged bridge, the values you enter here are for information purposes only.

Table 66 Connection parameters for system communication on the Connection tab

Field	Description
IP Address	IP Address for the system.
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
Track system on network by	Set the preferred address for your system. The options are: ■ *IP Address* ■ *Hostname*

Table 66 Connection parameters for system communication on the Connection tab (continued)

Field	Description
System connectivity	Define the system's location on the network: ■ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ■ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ■ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 67 The Logs contains all available logs for the system

Log	Description
History	All detected changes that have been made to the system in Cisco TMS.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Unmanaged Endpoint

In Cisco TMS: **Systems > Navigator** an unmanaged endpoint is selected

Cisco TMS has limited control over and access to settings for unmanaged endpoints.

For instructions on setting a system up as an unmanaged endpoint, see Adding Unmanaged Endpoints, page 61.

For background on how endpoints are managed, see How Endpoints are Managed by Cisco TMS, page 44.

Summary

Table 68 The Summary tab presents the most important data for the system

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service, page 138 for more information.
This Week's Bookings	A list of all the scheduled conferences for this system for the next 7 days.
System Image	Add or replace an image to be associated with the system. If the system is an endpoint that supports snapshots, this is a simple way of visualizing which room it is located in.
System Contact	The details from the **System Contact** field in the **Settings** tab; name, email address, and phone number are displayed here.
Book conference with this system	This link does navigate to new conference web page without any participants added into it.

Settings

View Settings and Edit Settings

The menu options **View Settings** and **Edit Settings** display mostly the same settings in a read-only and editable view respectively. Note that some settings, such as software version, are read-only in either view.

Table 69 Sections in View Settings and Edit Settings

Section	Description
General	The most important settings for the system, such as: ▪ **Name** ▪ **System Type** ▪ **Network Address** ▪ **Location**
Network Settings	In this section you will find H.323 gatekeeper and SIP server registration information, the NTP (Network Time Protocol) server setting and IP configuration information.

Table 69 Sections in View Settings and Edit Settings (continued)

TMS Scheduling Settings	**Allow Booking**: Allows the system to be added to conferences. **Allow Webex Booking**: Allows bridges to host Webex conferences. **Allow Incoming IP Address Dialing**: Allows calls to the system to be routed using H.323 direct mode. **Allow Incoming H.323 Dialing**: Allows calls to the system to be routed using an E.164 alias or H.323 ID. **Allow Incoming SIP URI Dialing**: Allows calls to the system to be routed using a SIP URI. **Allow Incoming ISDN Dialing**: Allows calls to the system to be routed using ISDN. **Allow Incoming Telephone Dialing**: Allows calls to the system to be routed using ISDN. **Allow Outgoing IP Address Dialing**: Allows calls from the system to be routed using H.323 direct mode. **Allow Outgoing H.323 Dialing**: Allows calls from the system to be routed using an E.164 alias or H.323 ID. **Allow Outgoing SIP URI Dialing**: Allows calls from the system to be routed using a SIP URI. **Allow Outgoing ISDN Dialing**: Allows calls from the system to be routed using ISDN. Note the following: ■ Only the booking/dialing options applicable to a particular system will be displayed. ■ Unchecking the **Allow Booking** box only affects new conferences. ■ Changing any of the Dialing options could affect the routing of existing conferences. ■ If you change any of the Dialing options for a system we recommend running **Conference Diagnostics** to identify any resulting issues with existing conferences.

Any errors and warnings on system settings will show up as red or yellow boxes around the setting that is incorrect. Hover over the error code for a tooltip message about the problem, and how to address it.

Ticket Filters

You can add or remove ticket filters for the system, if you want to hide tickets of certain types.

For more on tickets, see:

- Ticketing Service, page 138
- Manage Ticket Error Levels, page 261

Connection

As Cisco TMS does not connect to an unmanaged endpoint, the values you enter here are for information purposes only.

Table 70 Connection parameters for system communication on the Connection tab

Field	Description
IP Address	IP Address for the system.

Table 70 Connection parameters for system communication on the Connection tab (continued)

Field	Description
MAC Address	MAC address for the system.
Hostname	The hostname for the system.
Track system on network by	Set the preferred address for your system. The options are: ▪ *IP Address* ▪ *Hostname*
System connectivity	Define the system's location on the network: ▪ *Inaccessible*: The system cannot connect to Cisco TMS or vice versa. No attempts to communicate will be made, but the system may be booked for future conferences. The setting is intended for use in case of temporary system downtime for maintenance and similar situations. ▪ *Reachable on LAN*: The system is located on the same LAN as Cisco TMS and will communicate using the IP address or FQDN configured in **Advanced Network Settings for Systems on Internal LAN** to communicate, see Network Settings, page 237. ▪ *Reachable on Public Internet*: The system is located outside the LAN, but is reachable on a public network address and uses the **TMS Server Address (FQDN or IPv4 Address)** to communicate with Cisco TMS, see Network Settings, page 237. For more information, see System Connectivity Status, page 50.
Allow Bookings	Allows the system to be added to conferences. Selecting *No* will stop the system from being booked in the future but will not affect existing conferences.

Permissions

The **Permissions** tab controls permissions for the use and administration of a specific system for Cisco TMS user groups. The permission levels that can be set are the same as can be set on folders. For details, see Folder and System Permissions, page 137 and Default System Permissions, page 277.

Logs

Table 71 The Logs contains all available logs for the system

Log	Description
History	All detected changes that have been made to the system in Cisco TMS.
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service, page 138.
Audit Log	Changes to attributes for this system. For more information, see Audit Log, page 288.

Add Systems

In Cisco TMS: **Systems > NavigatorAdd Systems** has been clicked

When clicking **Add Systems** in the **System Navigator**, five tabs are displayed:

- **Add by Address**
- **Add from Unified CM or TMS**
- **Add Unmanaged Endpoint**
- **Add Unmanaged Bridge**
- **Pre-register Systems**

Add by Address

Table 72 Sections on the Add by Address tab

Section	Description
Specify Systems by IP Addresses or DNS Names	In this field you can enter: ▪ single IP addresses or DNS names. ▪ a range of IP addresses. ▪ a comma separated list of IP and host addresses. This means that when entering user.example.org, 10.0.0.1, 10.1.1.0 - 10.1.1.10, two systems will be added (one by DNS name and one by IP address), and ten IP addresses in a range will be scanned and systems with those IP addresses will be added. Note: If Cisco VCS is configured to listen on a specific port other than the default port, then port number is mandatory to add Cisco VCS in Cisco TMS. The default port is **443**. Cisco VCS can be added as **IP:PORT** in Cisco TMS.
Location Settings	Specify the ISDN zone, IP zone, and time zone.
Advanced Settings	
Username **Password**	If the system(s) require authentication, enter the username and password. Note that for systems running Cisco TelePresence System Collaboration Endpoint Software, TC, and TE Software, the username must be 'admin'. If adding a Cisco TelePresence Content Server, use the windows administrator username and password.
SNMP Community Names	Specify the SNMP community names Cisco TMS will use when searching for systems. SNMP community names added here will work only once—add them permanently in **Administrative Tools > Configuration > Network Settings**, see Network Settings, page 237.
Persistent Template	Select a configuration template in Cisco TMS that will be set as persistent on the system(s). See Using Configuration Templates, page 27.
Usage Type	In **Usage Type**, specify whether the system is used as: ▪ *Meeting Room* ▪ *Personal Home* ▪ *Personal Office* ▪ *Roll About*

Add from Unified CM or TMS

Add systems registered to Unified CM, auto-discovered systems, or systems from other folders.

Table 73 Options on the Add from Unified CM or TMS tab

Menu option	Description
Unified CM	Select systems registered to a Unified CM from the list to add them into Cisco TMS. See Adding Unified CM and Registered Endpoints, page 58.
TMS	This list can be used to add automatically discovered systems to a particular folder, or add existing systems to additional folders. Only systems already entered into Cisco TMS or automatically discovered appear on this list. A system can be in multiple folders.. The **In Folder** column displays all the folders a system is in.

Add Unmanaged Endpoint

Configure meeting rooms or third party systems that you want to be bookable in Cisco TMS. For step-by-step instructions, see Adding Unmanaged Endpoints, page 61.

Section	Description
Endpoint Settings	Enter endpoint configuration settings. These fields are mandatory: ■ Select **IP Zone**, **ISDN Zone**, and **Time Zone**. ■ Specify **Maximum IP Bandwidth**. ■ Specify **Gatekeeper Address**. ■ In order to use **SIP URI**, you must also set an **H.323 ID** or an **E.164 Alias**.
Location Settings	Specify the ISDN zone, IP zone, and time zone.

Add Unmanaged Bridge

Configure unsupported third party or legacy bridges that you want to be bookable in Cisco TMS. For step-by-step instructions, see Adding an Unmanaged Bridge, page 60.

Section	Description
Basic Settings	Name the bridge and enter the mandatory settings: **Max IP Bandwidth**: specify the maximum IP bandwidth **Max Number of Video/Audio Calls**: Note the following: ■ If *0* is entered in **Max Number of Audio Calls**, the number for video calls will be used as generic ports that can be used to book either video or audio participants. ■ If anything higher than *0* is entered in **Max Number of Audio Calls**, video and audio calls are counted separately and can not be used interchangeably. Optionally, enter network, SIP Server and Gatekeeper addresses for the bridge, and check **Immersive** if the bridge supports conferences with multiscreen systems.
Bridge Addresses	Specify the maximum number of bridge addresses (to a limit of 25), the protocol used and the meeting aliases/numbers.
Location Settings	Specify the ISDN zone, IP zone, and time zone.

Pre-register Systems

Pre-registration lets Cisco TMS configure systems when they connect to the network for the first time. For step-by-step instructions, see Pre-registering Endpoints, page 57.

Section	Description
Select System Identifier	Specify the system name and one of the following primary identifiers: ■ *MAC Address*—recommended for most systems. Must be used for remote systems unless they support using *Serial Number*. ■ *IP*—do not use for systems that will be placed behind a router or firewall that uses Network Address Translation (NAT). ■ *Serial Number*—only supported by legacy TANDBERG MXP Series and Polycom HDX endpoints.
Enter Location Settings	Specify the ISDN zone, IP zone, and time zone.
Set Templates	If you want a template to be applied when systems become online, you can select a pre-created template from the **First Boot Template** list on the **Set templates** pane. This template can be modified any time in **Systems > Configuration Templates**, see Configuration Templates, page 151. You can also configure a persistent template for the system here, by making values from the list of pre-registered systems persistent: ■ **Keep Name Persistent** ■ **Keep E.164 Alias Persistent** ■ **Keep H.323 ID Persistent** ■ **Keep SIP URI Persistent**

Unified CM

Systems registered to Unified CM must *not* be pre-registered in Cisco TMS. See Adding Unified CM and Registered Endpoints, page 58.

Folder and System Permissions

In Cisco TMS: **Systems > NavigatorFolder and System Permissions** has been clicked

The **Folder and System Permissions** button in **Navigator** opens two sections of permission settings for the active folder. If the folder does not contain any systems, only the **Folder Permissions** section will be displayed.

When adding, moving, or copying a system, the permissions you specify on a folder level will merge with the system permission settings for groups in Default System Permissions, page 277.

The permissions on these pages are displayed differently, but map as shown in the table below.

Table 74 Mapping of folder and system permissions

Folder Permissions	Default System Permissions
Read	Read, Book
Edit	Read, Book, Edit Settings, Manage Calls
Set Permissions	–

For more on this, see Default System Permissions, page 277.

Folder Permissions

For a group to get read access and other permissions for a folder, *Read* must be checked on the parent folders.

Read	See the folder and its contents, for example which systems are added to the folder.
Edit	Edit name of and description for the folder. The **Edit this folder** button is hidden to a group if this permission is removed.
Set Permissions	Set permissions for *Read*, *Edit* and *Set Permissions*. The **Folder and system permissions** button is hidden to a group if this permission is removed.

Checking **Apply folder permissions to all subfolders** makes all subfolders inherit parent folder permissions.

Cisco TMS allows a user to edit a conference or to add systems to it when the user is having booking permission to the folders that are used at the time of scheduling the conference.

System Permissions

System permissions can also be set for each system individually, by using the **Permissions** tab for the system, and in the Default System Permissions, page 277.

Read	Makes the system visible in **Systems > Navigator**. Enables reading of the **System Summary** and **View settings** tabs. If not set, the system will not be visible for this group in the **Systems > Navigator** folder view.
Book	Book systems in the folder (from **Ad Hoc Booking** and **New Conference** pages in Cisco TMS).
Edit Settings	Use the **Edit Settings** tab for systems in the folder.
Manage Calls	Use the **Call Status** tab where calls can be initiated and disconnected.
Set Permissions	Use the **Permissions** tab for systems in the folder. Note that a user/group does not have access to set system permissions if the permissions are disabled at the folder level. For more information, see **Permissions tab**.

Checking **Apply system permissions to all systems in subfolders** makes all systems in subfolders inherit parent folder permissions.

Ticketing Service

In Cisco TMS: **Systems > Ticketing Service**

The **Ticketing Service** scans the system and checks for any configuration errors when you add a new system to Cisco TMS, and each time an existing system has its configuration read by the system scanner or is manually refreshed.

When an error is discovered, Cisco TMS raises a new ticket for the system that includes a ticket ID, a description, and a severity level. The default severity levels for tickets are set in **Administrative Tools > Configuration > Manage Ticket Error Levels**, see Manage Ticket Error Levels, page 261.

The left pane contains a systems list and a drop-down to select the sorting mode:

- *Sort by ticket severity*: quickly identify the systems with the most severe errors and fix them first. This is the default sorting mode.
- *Sort by ticket type*: quickly identify systems with the same type of error, and potentially fix the error for several systems at the same time.

You can hover over each system to display the ticket type description.

Ticket Statuses

Table 75 Possible ticket statuses

Status	Description
Open	The error has not yet been handled (this is the default status).
Fixed	The error has been fixed.
Acknowledged	A user has acknowledged the error.
Invalidated	The ticket has been invalidated by the ticketing service. This happens if a system goes offline and Cisco TMS can no longer verify that the ticket is valid. The only valid ticket when Cisco TMS cannot connect to a system is the *TMS connection error* ticket.

In-page System Management

You can rectify errors directly on the **Ticketing Service** page by clicking on items in the left-hand listing:

- Clicking on a system opens a Navigator-like system management view.
- Clicking on a group header when *Sort by ticket type* is selected will open a multiple systems overview:
  - If the system fields associated with a ticket are editable, the overview will contain editable fields.
  - If not, a read-only overview will be displayed.

The system management view has three tabs; **Edit Settings**, **Ticket Filters**, and **Ticket Log**.

On the top of each tab, the **Tickets** section is displayed.

Tickets

This section contains a list of current tickets grouped by status. Clicking on the title of each ticket displays the action menu entries described below:

Table 76 Action menu options for tickets

Action	Description
Ignore ticket type for this system	Stop displaying the selected ticket type for this system.
Ignore ticket type for all systems	Stop displaying the selected ticket type for all systems.
Acknowledge ticket	Stop displaying the selected ticket as an open error. If a ticket is acknowledged, you can change the message given to the ticket.
Clear this ticket	Manually clear a ticket. This action is only available for certain types of tickets which cannot be automatically cleared by Cisco TMS, such as user defined tickets and *Low battery on remote*.

Below the list of tickets, two links are available:

- **Add custom ticket** link at the bottom of the **Tickets** pane can be used to create a custom ticket for one system and one occasion where a ticket does not exist in Cisco TMS.
  Clicking the link launches a pop-up window where you can enter a description and severity level. The ticket will then be accessible through the ticketing service. Using this feature to report issues helps create a structured routine for solving issues.

- **Open system in System Navigator** takes you directly to the system in Navigator, where you can modify all supported settings for the system.

Edit Settings

The settings available for editing on this tab will depend on the ticket type:

- If the ticket type is *Connection Error*, Cisco TMS will bring up the **Connection** tab from Navigator.
- For other ticket types, Cisco TMS will bring up the **Edit Settings** view from Navigator.

The settings and information displayed also depend on the system type. Overall, the actions and settings available correspond to those available in Navigator, page 69.

Ticket Filters

Add and manage filters for ticket types on this tab. Here you can manage all filters hiding tickets for the selected system, and global filters for all systems.

Ticket Log

The tab **Ticket Log** contains a list of all tickets that have been raised on the system. The list is sorted by ticket status first, and by date fixed second.

Hover over the ticket type to see the ticket description as a tooltip.

System Overview

In Cisco TMS: **Systems > System Overview**

On this page, you can compare specific parameters on specific systems by having them presented in a table view. The table can also be exported to Excel for further processing.

- All available systems are listed in a folder view to the left.
- All available parameters are listed to the right.

After selecting the desired combination of systems and parameters, click **View** at the bottom of the page.

When a table has been generated, **Export to Excel** becomes available.

Manage Dial Plan

In Cisco TMS: **Systems > Manage Dial Plan**

Table 77 Settings on the Manage Dial Plan page

Setting	Description
System Name	The system's display name in Cisco TMS.
H.323 ID	The alphanumeric H.323 identifier to use for contacting the system, if applicable.
E.164 Alias	The numeric E.164 alias to use for contacting the system, if applicable.
SIP URI	The SIP address to use for contacting the system, if applicable.

Table 77 Settings on the Manage Dial Plan page (continued)

Setting	Description
Persistent	Checking this option will set all these settings as persistent: ■ **System Name** ■ **H.323 ID** ■ **E.164 Alias** ■ **SIP URI** ■ **Persistent Template**
System Identifier	Whether to track the system by *IP Address* or *MAC Address*.
Persistent Template	Drop-down list of available configuration templates. See Configuration Templates, page 151.

The settings on this page can be applied only to Cisco TMS-controlled systems.

Provisioning

In Cisco TMS: **Systems > Provisioning**

This menu section will only be available in Cisco TMS if Cisco TelePresence Management Suite Provisioning Extension is installed and activated on the system.

A reference to buttons, settings, and menu items is presented below. For guidance on installation, configuration, and deployment of Cisco TMSPE, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.

Users

In Cisco TMS: **Systems > Provisioning > Users**

On the left-hand side of the screen, two sections can be accessed using the accordion buttons **Users and Groups** and **Configuration Templates**.

Users and Groups

Selecting a user or group will display the settings for that user or group in the right hand pane of the Users window.

Table 78 Buttons in the Users and Groups section

Button	Description
Buttons on the left	
Add Group	Enter a display name to manually create a new user group .
Add User	Enter user details to manually create a new user.
Reload	Update the list of groups and users if imported from Active Directory or LDAP.
Buttons on the right	
Rename Group...	Edit the display name of the group.
Edit User	Edit the user details.
Delete	Delete the group/user.

Table 78 Buttons in the Users and Groups section (continued)

Button	Description
Send Account Information	Send an email message containing account information to all the users in the selected group or the selected user.
Move Group	Move a group into another group folder.
Move User	Move a user into another group.
Toggle Details	Click to view more user details.
Go to Group	View the group to which the selected user belongs.

Collaboration Meeting Room Templates

These templates predefine settings for the Collaboration Meeting Rooms users can create from the Cisco TMSPE User Portal. Templates are applied to user groups.

Before creating CMR templates, you must complete the TelePresence Conductor setup. For guidance on deploying Collaboration Meeting Rooms with Cisco TMSPE, see *Cisco TMSPE Deployment Guide* for Unified CM or Cisco VCS depending on your environment.

Table 79 Buttons in the Collaboration Meeting Room Template section.

Button	Description
New Template	Create a new template.
TelePresence Conductor Settings	Add a new TelePresence Conductor peer to use for CMR templates, or change connection settings for existing TelePresence Conductor peers. It is not possible to connect more than one TelePresence Conductor peer from a cluster per template. Click the **TelePresence Conductor Multiparty Licensing** icon to view Multiparty Licenses status. Click **Synchronize Now** button within the **TelePresence Conductor Multiparty Licensing** dialog to do manual synchronization. This allows the admin to re-organize the CMR setup and does not have to wait for nightly synchronization, for the changes to be effective.
Regenerate CMRs	Updates, adds, and deletes CMR information on the TelePresence Conductor based on current CMR templates in Cisco TMSPE.
Check Sync Status	CMR templates will be marked as out of sync between TelePresence Conductor and Cisco TMSPE when one or more of the following is true: ▪ The template has been updated ▪ User information has been updated, or one or more users have been deleted ▪ Something on the CMR has been altered. The sync status check is performed automatically as the page is loaded. To check again, click **Check Sync Status** . To synchronize CMRs, click **Regenerate CMRs**.

Table 79 Buttons in the Collaboration Meeting Room Template section. (continued)

Verify Templates	This verification checks whether: ■ the TelePresence Conductor selected for each CMR template is active. ■ **Service Preference** is correct according to what is available from the TelePresence Conductor. ■ **Maximum Conference Quality** and **Maximum Content Quality** are configured and correspond between the CMR and TelePresence Conductor. The check is not performed automatically. Click the button to run the verification if: ■ Changes have been done on the TelePresence Conductor ■ Alarms have been raised in Cisco TMSPE ■ Users report failure to create new CMRs
Export Room Data	Generate a **.csv** file with CMR information from each user that can be opened in for example Excel.

New Template

When creating a new template, the available fields and values will depend on settings on TelePresence Conductor.

- For more detail on TelePresence Conductor settings, see *Cisco TelePresence Conductor Administrator Guide*.
- For examples with a Cisco Unified Communications Manager setup, see *Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide*.
- For examples with a Cisco VCS setup, see *Cisco TelePresence Conductor with Cisco VCS Deployment Guide*.

Table 80 Collaboration Meeting Room template configuration fields

Field	Description
Template Name	Assign a descriptive name to each template to ease the selection and maintenance of templates as the list grows. For example, include a descriptor for video quality, geographical location, or other signifier that clearly conveys what the template does.
TelePresence Conductor	Select the TelePresence Conductor to use with the template from the drop-down list.
Service Preference	Select a Service Preference that has already been created on TelePresence Conductor.

Table 80 Collaboration Meeting Room template configuration fields (continued)

Field	Description
Multiparty License Mode	Select the multiparty license type from the following options: ■ Personal Multiparty ■ Shared Multiparty The **Multiparty License Mode** field appears when the following conditions are met: ■ A conductor is selected in **TelePresence Conductor** field. ■ A valid service is selected in **Service Preference** field which is mapped with a TelePresence Server. The default **Multiparty License Mode** is Personal Multiparty.
SIP Alias Pattern	Create a pattern for alphanumeric dialing matching Cisco VCS search rules. Create a pattern for alphanumeric dialing if supported by your Unified CM deployment. The pattern must match your dial plan. For example: `{username}@meeting.example.com` The recommended variables are: ■ {username} ■ {email} ■ {office_phone} ■ {mobile_phone} {display_name}, {first_name}, and {last_name} are also supported variables, but will typically lead to conflict during room creation in organizations where many may share the same name. We strongly recommend using a unique identifier to minimize the risk of conflict and ensure alias predictability for users. In the event of alias conflict when a user creates a new room, Cisco TMSPE will create a numeric alias only if enabled, or fail to create a room if no aliases can be generated.
Numeric Alias Pattern	Whether to add a numeric alias for each room in addition to the alphanumeric alias. The selected pattern must match the dial plan of your call control device. Check to display the below settings.
Type	Select whether to base the numeric alias pattern on: ■ number ranges (*Generate a Number*) . ■ a RegEx pattern (*Office Phone* or *Mobile Phone*).

Table 80 Collaboration Meeting Room template configuration fields (continued)

Field	Description
Number Ranges	Enter one or more number ranges to use for the numeric aliases. Ranges must be written with a hyphen and no spaces, and multiple ranges must be separated by commas. Note that: ■ Both parts of the range must contain the same number of digits. For example, `01-99` will work, but `1-99` will not . ■ Ranges may overlap within and across templates. Duplicate numbers will not be generated. ■ Numbers will be assigned randomly within the range, but if there are multiple ranges, the ranges will be consumed sequentially. ■ A single number range cannot span more than one million numbers. Example: `100000-123456, 200000-234567`
Prefix	Enter a string of numbers that will constitute the first part of all numeric aliases.
RegEx	To create the last part of the numeric alias, you may opt to use the user's office phone number or mobile phone number. Either choice requires that each user has the specified type of phone number available in Active Directory. Use the Regex field to specify which part or parts to extract from the phone number. Keep in mind that using parts of a phone number will not always generate a unique number. We strongly recommend using a unique identifier to minimize the risk of conflict and ensure alias predictability for users. In the event of alias conflict when a user creates a new room, Cisco TMSPE will create an alphanumeric alias if a pattern exists, or fail to create a Collaboration Meeting Room if no aliases can be generated. **Example:** If the regex result contains one or more match groups, the result will be all match groups concatenated. If there are no match groups, the result will be the entire match result. In this example we will match against the phone number `123.456.7890`. ■ Given the regex `\d{4}` which will match the last four digits without any capture groups. The result will be `7890`. ■ Given the regex `(\d{3})\.\d{4}` which will match `456.7890` but also has one match groups which matches `456`. The result will be `456`. ■ Given the regex `((?<=\.\d)\d{2}(?=\.))(?:\.)(\d{4})` which will match `56.7890` with two match groups `56` and `7890`. The result will be `567890`.
Maximum Conference Quality	From the range of available video qualities, select the maximum quality that users will have access to when you assign them this template.
Content Sharing	Whether to allow content (presentation) sharing in rooms based on this template.

Table 80 Collaboration Meeting Room template configuration fields (continued)

Field	Description
Maximum Content Quality	From the range of available qualities for content (presentation) sharing, select the maximum quality that users will have access to. The **Maximum Content Quality** setting is not applicable to CMRs that are hosted on MCU.
Minimum Host PIN Length **Allow Guest Role** **Minimum Guest PIN Length** **Guest Lobby**	These settings control the requirements and options for PIN protection of CMRs based on the template: ■ First, enter the minimum number of digits for the host role's PIN in **Minimum Host PIN Length**. If you leave the setting as 0, the CMR owner is not required to use a PIN for any participants. ■ Select whether to allow the role of guest for CMRs based on this template.: – The guest role has more limited privileges than the host role. – If **Allow Guest Role** is disabled, all participants will have the same privileges and PIN requirements as the host. ■ If **Allow Guest Role** is enabled: – Enter the minimum number of digits for the guest PIN in **Minimum Guest PIN Length**. If you leave the setting as 0, the CMR owner is not required to use a PIN for the guest role. – Choose whether to enable **Guest Lobby**, which means guests must wait in the lobby unless at least one host is present in the CMR.
Limit Number of Participants	Choose whether to set a maximum number of participants that will be allowed in the Collaboration Meeting Room.
Maximum Participants	Set a maximum number of participants to allow if **Limit Number of Participants** is enabled. The upper limit for number of participants allowed in a CMR is controlled by Cisco TelePresence Conductor. For more detail, see documentation for Cisco TelePresence Conductor.
Limit Conference Duration	Choose whether to set a maximum duration for meetings in the CMR. Enable this setting to prevent meetings where participants forget to disconnect, so that the meeting continues.
Maximum Minutes	Set a maximum meeting duration in minutes if **Limit Conference Duration** is enabled.
Allow Multiscreen	Choose whether to allow participating telepresence systems to use more than one screen.
Maximum Screens	Set a maximum number of screens allowed per participant if **Allow Multiscreen** is enabled.
Allow Cascading	Choose whether to allow the user of this CMR to seamlessly expand an ongoing meeting if there is an available bridge in your environment. This requires reserving one or more bridge ports or connections for cascading, which will always be available to the CMRs defined by this template.
Number of Cascades	Set a number of MCU ports or TelePresence Server connections to reserve for cascading if enabled.

Table 80 Collaboration Meeting Room template configuration fields (continued)

Field	Description
Optimize Resources	Select whether to allow TelePresence Conductor to free up any allocated resources not used by participants once the meeting has started. This setting is enabled by default.
Include Webex	If CMR Hybrid is deployed, choose whether to enable the creation of instant Webex meetings connected to the CMR. For this option to work, you must first go to **Administrative Tools > Configuration > Provisioning Extension Settings > Collaboration Meeting Room** and set **Allow Webex Connections** to *Yes*.
Advanced Parameters	Configure bridge-specific JSON objects for advanced conference parameters on creation. For examples of JSON, see Cisco TelePresence Conductor Administrator Guide.

User Settings

Table 81 Buttons in the User Settings section.

Button	Description
Edit	Edit the patterns.
Reload	Update patterns set at a higher group level.

Table 82 Address patterns for user configuration

Pattern	Description
Video Address Pattern	The Video URI is used to generate video URIs. A video URI is used for your users FindMe addresses and can be used in phone books. Example Video URI: `{username}@example.org`
Caller ID Pattern	The Caller ID is used to generate caller IDs. A Caller ID is used as the callback number when a FindMe call is routed through an ISDN gateway. Example: `{office_phone}`
Device Address Pattern	The Device Address is used to generate device addresses that will be set on provisioned devices. Example: `{username}.{device.model}@example.org`
Image URL Pattern	An image URL is a pointer to an image of the user that can be displayed in the Cisco TMSPE and FindMe user interfaces and in phone books on devices that support the feature. The supported extensions are **.jpg**, .**jpeg**, and **.png**. Example: `http://yourimageserver/users/{username}.png`

For further help with configuring the patterns, click on the help link in the **Edit** > **User Settings** popup window.

User Import

Click **Configure** to display the **Type** field.

Select the type of directory server to import groups and users from:

- *Active Directory (AD)*
- *Active Directory with Kerberos (secure AD)*
- *Lightweight Directory Access Protocol (LDAP)*

and enter the server settings.

Configuration Templates

Click **Assign Templates** to select which template to assign to the group.

Provisioned Devices

Devices the user has logged on to are listed here.

Configuration Templates

Table 83 Configuration template creation and management

Button	Description
Buttons on the left	
Add Schema...	Browse to add a configuration template schema.
Add Template...	Create a new configuration template from a template schema.
Buttons on the right	
Rename Template...	Change the display name of the template.
Delete Template	Delete the template.
Delete Schema	Delete the schema.
Copy Configurations...	Copy configurations from another template to this one.
Edit Configurations...	Add and remove configurations and edit their values.

The information displayed in the right hand pane will be different depending on whether a schema or a template has been selected.

FindMe

In Cisco TMS: **Systems > Provisioning > FindMe**

The left-hand side of the screen consists of three sections accessed using the accordion buttons: **Accounts and Groups**, **Location Templates**, and **Device Templates**.

Accounts and Groups

Select an account or group to display its settings in the right hand pane of the FindMe window.

Table 84 Buttons in the Accounts and Groups section

Button	Description
Add Group	Enter a display name to create a FindMe group.
Add Account	Add account detail to create a FindMe account.

Table 84 Buttons in the Accounts and Groups section (continued)

Button	Description
Edit in FindMe User Portal	Launch the FindMe User Portal in a new browser window and edit the user's FindMe profile directly.
Assign Templates	Assign location templates to groups.
Edit	Change the display name.
Delete	Delete the template.

- Click on a group to view which location templates are assigned to it.
- Click on an account to view which locations and devices are associated with it.

Location Templates

Select a location template to display its settings in the right-hand pane of the FindMe window.

Table 85 Buttons in the Location Templates section

Button	Description
Add Location Template	Enter a display name and ring duration to create a location template.
Add Device Template	Enter a display name, device type and device address pattern to create a device template.
Assign Templates	Assign device templates to location templates.
Edit	Rename the template and modify the ring duration.

Select a template to display the device templates and assigned groups settings for that location template in the right hand pane of the FindMe window.

Device Templates

Select a device template to display its settings in the right-hand side of the FindMe page.

Table 86 Buttons in the Location Templates section

Button	Description
Add Device Template	Enter a display name, device type and device address pattern to create a device template.
Assign Templates	Assign device templates to location templates.
Edit	Rename the template and modify the ring duration.

Select a template will display the location templates for that device template in the right hand pane of the FindMe window.

Regenerate Locations and Devices

In all three sections, a **Regenerate Locations and Devices...** button is available. This button generates locations and devices associated with the selected group (and any subgroups) or template, based on the configured location and device templates. In the dialog that opens, choose one of the following:

- **Yes**—apply the templates and overwrite any edits made by users.
- **No**—apply the templates, but keep existing user edits.
- **Cancel**—do not apply the templates.

Devices

In Cisco TMS: **Systems > Provisioning > Devices**

This page displays all devices which have been provisioned.

- Use the filter drop-down menu and search field and click **Filter** to choose which devices to display.
- Use the bottom toolbar to select or deselect all entries for deletion.
- Click **Export All** to download a comma-separated list of devices for further processing in a third-party application.

Configuration Backup

In Cisco TMS: **Systems > Configuration Backup**

This feature allows the user to backup all the settings of several systems. Backup for later restoring of the systems settings is done in one operation.

Perform Backup

In Cisco TMS: **Systems > Configuration Backup > Perform Backup**

On this page you can create system configuration backups on the Cisco TMS server.

For systems that are already backed up on the server, the date of the previous backup is shown next to the system name.

To view the settings from the last backup:

1. Go to **Systems > Navigator**.
2. Click on a system.
3. Click on the **Settings** tab.
4. Click **Compare Settings**.
   Any modified settings since the backup will be highlighted. The **System Setting** column shows the current settings and the **Server Setting** column shows the settings in the backup.

To create a new backup:

1. Select systems (double-click the first folder to select all).

   You can see how many systems you have selected to do backup from on the right.
2. Click **Make Backup**.

Perform Restore

In Cisco TMS: **Systems > Configuration Backup > Perform Restore**

On this page you can restore settings from a previously created backup. Only systems with a backup on the Cisco TMS server are available for selection on this page.

Immediate Restore

To restore the system settings immediately, select systems in the left-hand section and click **Restore**.

Scheduled Restore

To schedule recurrent restore of settings:

1. Select systems in the left-hand section.
2. In the **Restore Event Time** section on the right:
   a. Set **Restore time**.
   b. Set **Recurrence** to *Once* or *Daily*.
3. Click **Restore**

Note:
Backup and Restore option is applicable for system configurations that a system supports (endpoint, bridge or any other system). Some fields like Email Address, System Contact, Description in System Navigator are not supported configurations in system and cannot be backed up or restored.

Email Alert

You can choose to receive an email notification when the restore has completed or failed.

Select your preferred alternative in the **Send Email Alert** section.

Monitoring

To monitor the progress and status of the restore, go to **Systems > Configuration Backup > Backup/Restore Activity Status**, see Backup/Restore Activity Status, page 151.

Backup/Restore Activity Status

In Cisco TMS: **Systems > Configuration Backup > Backup/Restore Activity Status**

On the **Backup/Restore Activity Status** page information is provided on the status of scheduled backups and restores.

Ongoing and upcoming scheduled events are displayed automatically.

- Search for past events by modifying the **Start Date** and **End Date** fields, then click **Search**.
- Check *Show only mine* to display only events scheduled by the currently logged in user.

  To apply this to the list below, click **Refresh**.
- Click the linked description of any event to see a detailed activity log.
  - For Conference Diagnostic Activity, the status and event description for the selected dates are displayed
- To cancel a scheduled event, select it and click **Delete**.

Click to refresh

Note that the activity status pages do not automatically refresh while open. To update the status view, click **Refresh**.

Configuration Templates

In Cisco TMS: **Systems > Configuration Templates > Configuration Templates**

On this page you can create, edit, copy and delete configuration templates for Cisco TMS-controlled systems.

By using configuration templates, you can download a specific set of settings to several systems in one operation. This ensures homogenous settings among different systems.

A configuration template can contain any setting from any system category. Systems will ignore any template settings they do not support.

Note: If template contain both **System Based Template** and **Cisco TMS Commands** and if any of the System Based Template entry is rejected, then Cisco TMS Commands will not be applied and the task will be marked as failed. Cisco TMS Admin needs to either fix the rejected items in current template or move Cisco TMS Commands to a separate template and retry.

Note that Cisco TMSPE has its own configuration templates which are managed elsewhere. If you are looking for information on configuring Cisco TMSPE provisioned endpoints, see Provisioning, page 141.

Configuration Templates Main Page

This page lists all available configuration templates.

As a part of the default installation, Cisco TMS created a template called **Discovered Systems Template**.

A drop-down menu is available when hovering over each template on the list

Table 87 Drop-down menu options for configuration templates

Menu entry	Description
View	Open a read-only view of the template. Buttons to edit, copy, or set the template on systems will be available from this view.
Edit	Open an editable view of the template, the **Select Settings for Configuration Template** page (described below).
Copy	Use this template to start a new template.
Set on Systems	Open the **Set Configuration Template on Systems** page, where you can select systems from the main folder structure and set the template on the systems as a one-time operation or as a persistent template.

The button **New Configuration Template** opens the **Select Settings for Configuration Template** page,

Select Settings for Configuration Template

Give each template a descriptive name.

Three tabs are available for setting up a template, described below.

Template Settings

Table 88 General configuration template settings that can be applied to most systems

Field	Description
Allow Bookings	*None*: No setting specified. *On*: Make the system available for booking. *Off*: Make the system unavailable for booking.
DNS Domain Name	The system's DNS Domain Name.
DNS Server Address	The system's DNS Address.
H.323 Call Setup Mode	*None*: *Gatekeeper*: The system will use a gatekeeper to make a H.323 call. *Direct*: An IP address must be dialed in order to make a H.323 call.

Table 88 General configuration template settings that can be applied to most systems (continued)

Field	Description
H.323 Gatekeeper Address	Defines the H.323 gatekeeper address.
H.323 Gatekeeper Discovery Mode	*None*: *Manual*: The system will use a specific gatekeeper identified by the **H.323 Gatekeeper Address**. *Auto*: The system will automatically try to register to any available gatekeeper.
IP Zone for the system	*None*: The list of IP Zones defined in your Cisco TMS.
ISDN Zone for the system	*None*: The list of ISDN Zones defined in your Cisco TMS.
Management Address	Address of the system's external manager, which can be the address of the Cisco TMS, Cisco VCS or Unified CM. Which of these alternatives are dependent on how you want your endpoint to be provisioned.
Phone Book 1	*None*: No phone book selected The list of all available phone books in Cisco TMS is available for selection.
Phone Book 2	
Phone Book 3	
SIP Mode	*None*: No setting specified. *On*: Enable the system for incoming and outgoing SIP calls. *Off*: Disable incoming and outgoing SIP calls from the system.
SIP Proxy IP Address	The manually configured outbound proxy for the signaling, or the SIP registrar.
SIP Server Discovery	*None*: *Auto*: The **SIP Proxy IP Address** is retrieved from the DHCP service, if available. *Manual*: The manually configured **SIP Proxy IP Address** will be used.
Time Zone	*None*: No time zone specified. The list of all available time zones in Cisco TMS is available for selection. Select the time zone that applies to the systems you are setting the configuration on.

Select Advanced Settings

On this tab you can search for system-specific settings to add to the general template from the **Template Settings** tab.

- *Personal Systems* are endpoints running Cisco TelePresence TE Software.
- *Group Systems* are endpoints running Cisco TelePresence TC Software.

After selecting and saving the advanced settings you want, you can go back to the **Template Settings** tab to edit each of the advanced settings. All settings on the tab will be sorted alphabetically.

Table 89 Fields on the Select Advanced Settings tab

Field	Description
Filter	Enter the name of the setting you want to add to your configuration template. Leave this field blank and select a specific system type to see all available settings for that system type.
All Systems	Select the system you want the search to apply to. You can search and select different settings for different system types to apply to one configuration template. **TMS Commands**: General settings that can be applied to all systems.

Once filters have been applied, a list of all available settings matching the filter criteria is displayed on the left-hand side on the screen. On the right side is a list of settings selected for your template. You can use the arrow buttons to add and remove settings.

Each list entry includes a named setting and the system type it is valid for.

Setting a password

To set a password on CE, TC and TE systems, the correct setting is *Password* for **System Type**: *Other Type*. The setting *Admin Password* for **System Type**: *Other Type* applies only to legacy endpoints.

Setting a time zone

If you set the time zone for a system using a configuration template where you have specified the system type, the time zone will be updated on the system itself, but not for the system in Cisco TMS. Therefore we recommend setting the time zone using system type: 'Other Type' on the **Template Settings** tab. This will update the time zone for the system itself and in Cisco TMS.

Persistent Scheduling

Use this page to set the time/intervals for recurring configuration.

All configuration templates are set up with persistent scheduling as a default. Applying a configuration template only once (overriding the recurrence) is done in the **Set Configuration Template on Systems** page, available when clicking **Set on Systems**.

Table 90 Settings for recurring configuration

Field	Description
Apply at	Set the time of day for the configuration.
Recurrence Interval	The options are *Daily* or *Weekly*.
On Each	This field is only active when **Recurrence Interval** has been set to *Weekly*. Specify which day the configuration is to occur.
Apply on System Boot	Select this if you want the configuration template applied each time the systems boot.

Configuration Template Activity Status

In Cisco TMS: **Systems > Configuration Templates > Configuration Template Activity Status**

The **Configuration Template Activity Status** page shows the status of ongoing configuration templates being set on systems.

Note that the events created by Cisco TMS cannot be deleted from **Configuration Template Activity Status** page. You can only delete an event that a user has created.

Follow the steps to delete an event:

1. Select the event that you want to delete.
2. Click **Delete**.
3. Click **OK** to confirm the action.

There are two types of entries for persistent templates:

- A first entry for when the template has been set on the system. No recurrence is set for these entries.
- A second entry for the template with recurrence set to every day.

Ongoing and upcoming scheduled events are displayed automatically.

- Search for past events by modifying the **Start Date** and **End Date** fields, then click **Search**.
- Check *Show only mine* to display only events scheduled by the currently logged in user.

  To apply this to the list below, click **Refresh**.
- Click the linked description of any event to see a detailed activity log.
  - For Conference Diagnostic Activity, the status and event description for the selected dates are displayed
- To cancel a scheduled event, select it and click **Delete**.

Click to refresh

Note that the activity status pages do not automatically refresh while open. To update the status view, click **Refresh**.

System Upgrade

In Cisco TMS: **Systems > System Upgrade**

On this page, you can upgrade the software on endpoints managed by Cisco TMS and endpoints provisioned by Cisco TMSPE.

Software upgrade is supported for endpoints only. Software upgrade is not supported for Unmanaged Endpoints and Unified CM-registered endpoints.

Cisco TMS Endpoints

For Cisco TMS-managed endpoints you can choose from a drop-down list of display options similar to the display options in Navigator, page 69. You can also search for specific endpoints by opening the **Search** tab.

Endpoints Managed by the Provisioning Extension

For endpoints provisioned by Cisco TMSPE you can either choose to *Order by Software Version* or *List All*, which includes all endpoints belonging to users on the **Systems > Provisioning > Users** page.

- For instructions on upgrading Cisco Jabber Video for TelePresence, see *Cisco Jabber Video for Telepresence Administrator Guide*.
- For instructions on upgrading and maintaining endpoints provisioned by Cisco TMSPE, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.

Upgrade Modes

Select the upgrade mode from the drop-down list at the bottom of the **System Upgrade** page.

Table 91 Available upgrade modes

Mode	Description
Basic	Cisco TMS will select a software package that is compatible with the software already installed on the endpoint. This mode will work for most upgrades and support only encrypted files.
Advanced	You must manually select a package from the list of compatible packages. This mode supports both encrypted and non-encrypted files.
Expert	Select from all software packages available on the Cisco TMS server. Note that this mode requires knowledge of the software packages that can be uploaded to the different endpoints.

Buttons for Upgrading

At the bottom of the page, the following buttons are available:

Table 92 Buttons at the bottom of the System Upgrade page

Button	Description
Next	Display the **Select Software and Release Keys** page (see below).
Auto Select	Automatically select the endpoints that have newer software versions available (based on update checks for endpoints registered with Cisco) and display a list of these endpoints along with the software packages and release keys. This feature will only be available if **Automatically Check for Updates** has been set to *Yes*, see Network Settings, page 237.
Check for Updates	Automatically downloads the software updates and the corresponding release keys for legacy endpoints that are registered with the upgrade web service at Cisco. The URL of the software update service is set in **Administrative Tools > Configuration > Network Settings > Service URL**. The update check will run in the background until completed. Progress for the background event can be seen in the **Activity Status** page, where you can see which systems the update check failed for. When the upgrade check is completed, the **Auto Select** button on the **System Upgrade** page can be used to automatically select the systems that have new software updates available.
Upgrade	Start upgrade, after filling in the required information on the **Select Software and Release Keys** page (see below). You can follow the progress of the software upgrades from the **System Upgrade Activity Status** page. You can also use this to perform software downgrade. **Note:** This button is only visible when an endpoint has already been selected for upgrade.

Some buttons are only available if **Automatically Check for Updates** has been set to *No*, see Network Settings, page 237:

Table 93 Buttons when no automatic check for updates is configured

Button	Description
Import Log	Import a log of the software and release keys of all your Cisco systems. The **Systems Upgrade** page will then list all the systems in the log and the software and release keys to the systems. After importing the log you can upgrade the endpoints by clicking the **Upgrade** button.
Generate Log	Generate a Release Key report from the page. The list will contain information about the systems shown and the software packages selected for each system. **Note:** This button is only visible when an endpoint has already been selected for upgrade.

Select Software and Release Keys

The **Select Software and Release Keys** page is displayed when one or more endpoints have been selected for upgrade and **Next** has been clicked.

Table 94 Fields on the Select Software and Release Keys page

Field	Description
Release Key	Consult the device documentation to determine if a release key is required for upgrade.
Software	A drop-down list of available software packages.
Date	Date of the scheduled upgrade.
Start time	Start time of the scheduled upgrade on the selected date.

Software Manager

In Cisco TMS: **Systems > System Upgrade > Software Manager**

This page is used to manage all available software packages for upgrade of :

- Cisco-controlled systems
- Cisco TMSPE-provisioned systems

For instructions on upgrading, see Upgrading Cisco TMS-Managed Endpoints, page 68.

Note that this software manager *cannot* be used for software packages intended for:

- Systems managed by Cisco Unified CM.
- Systems added to Cisco TMS Unmanaged Endpoints.

Valid Formats

Clicking **Upload New Software** lets you browse your server or network for the software files. The supported extensions for file upload are **.zip**, ***.pkg**, ***.exe**, ***.dmg**, ***.gz** and ***.cop.sgn**.

If you have access to the Cisco TMS server, you may also choose to copy software packages directly into the destination directory of the server, instead of using this web interface.

Notes:

1. You can copy the software files for upgrades manually to **C:\Program Files (x86)\TANDBERG\TMS\wwwtms\public\data\SystemSoftware** on the server. Do not include the **COP.SGN** file else the upgrade will fail. The **.cop.sgn** file can only be uploaded via **Upload New Software** option.

2. Cisco TMS supports using SuperCOP files for upgrading all endpoints that support CE 9.x software.
   Note: Endpoint upgrade using **.loads** extension file is supported only if the **Upgrade Mode** is '**Expert**'. The **.loads** file uploaded via SuperCOP files have the **Target** and **Version** fields which are displayed as **Unknown**. SuperCOP files with size more than 2 GB are not supported. If the SuperCOP file is more than 2 GB, then you must use individual COP file for each endpoint.

The destination directory for the software is visible in the **Software Directory** field on the **Administrative Tools > Configuration > General Settings** page. To change the directory location, you must use the Cisco TMS Tools application, see Software Directory, page 292

Fields in the Software List

The list is only visible if at least one software package has been uploaded to Cisco TMS). Each uploaded file will be added to the software list.

Table 95 Software list fields

Field	Description
File Name	The file name of the uploaded software package.
Target	The system type that the software is valid for.
Version	The version of the software.
Encryption Support	Encryption Support will show *No encryption* if the software package uploaded does not support encryption, and *With encryption* if it does.

Overwriting and Deleting Software

- If you upload a software package that is already on the list, Cisco TMS will overwrite the old one with the one you are currently uploading. You will not be prompted. The actual overwriting will be done immediately after the upload is finished.
- When a software package is no longer needed, you can remove it from the server by selecting it from the list and clicking **Delete**.

System Upgrade Activity Status

In Cisco TMS: **Systems > System Upgrade > System Upgrade Activity Status**

This page shows you the status of scheduled and ongoing system upgrades.

Ongoing and upcoming scheduled events are displayed automatically.

- Search for past events by modifying the **Start Date** and **End Date** fields, then click **Search**.
- Check *Show only mine* to display only events scheduled by the currently logged in user.

  To apply this to the list below, click **Refresh**.
- Click the linked description of any event to see a detailed activity log.
  - For Conference Diagnostic Activity, the status and event description for the selected dates are displayed
- To cancel a scheduled event, select it and click **Delete**.

Click to refresh

Note that the activity status pages do not automatically refresh while open. To update the status view, click **Refresh**.

Purge Systems

In Cisco TMS: **Systems > Purge Systems**

This functionality lets you remove and purge systems which you no longer wish to see in Cisco TMS from the Cisco TMS database.

Beware that purged systems will also be removed from all ongoing and pending scheduled meetings.

Note that the system list will include any auto-discovered systems that have not been added to Cisco TMS.

To purge:

1. Select the system you want to remove.
2. Click **Purge Systems** at the bottom of the page.
   A list is displayed containing all selected systems and any future conferences they are scheduled to participate in.
3. Click **Purge** to confirm the operation.

Event Notification Manager

In Cisco TMS: **Systems > Event Notification Manager**

Use the event notification manager to subscribe users to system events so that they are notified by email whenever the event occurs on that system.

Select **Edit** in the pulldown menu for a user, and the **Edit Event Notification** page for that user will be displayed.

Any event notifications the user is already subscribed to are shown in the right hand panel. Up to 1000 notifications are displayed at a time.

To add new event notifications:

1. Select the folder, systems and event types, and use the arrow button to move them to the right-hand list of stored notifications.
2. Click **Apply**.
   The user will now be notified by email when the selected events occur.

To remove event notifications, select them and use the arrow button to remove them from the list. Only 1000 notifications can be selected and deleted at a time.

Select Event Types

Table 96 Event types for which notifications can be configured

Event type	Description
Authentication Failure	Authentication failure on Telnet access.
Boot	System boot.
Connected	System has connected.
Connection Error	System could not connect.
Disconnected	System has disconnected.
Downspeeding	Sent when call rate drops due to ISDN errors or H.323 packet loss (MXP Series).
Encryption Status	Encrypted off/DES/AES.
Flow Control	Sent when call rate drops due to H.323 packet loss. (MXP Series).

Table 96 Event types for which notifications can be configured (continued)

Event type	Description
Gatekeeper Registration	System has registered or failed to register to a gatekeeper.
Got Response	A system has returned from a Lost Response state.
IP Conflict	The system's IP Address is in conflict with the IP Address of another device in the network.
Link Down	ISDN link down.
Link Up	ISDN link up.
Lost Response	A system is unavailable.
Low Battery on Remote Control	Low battery on system's remote control. (Polycom VSX only.)
Other	Other events not explicitly supported by Cisco TMS
Pre-registered System Activated	A pre-registered system has been detected and activated.
Scheduling	The system is scheduled by Cisco TMS, or a scheduled conference is changed or deleted.
Scheduling error	An error has occurred in a scheduled conference.
System type Changed	Cisco TMS has registered a change in system type for a system.
Upgrade	System software upgraded.
User Assistance Requested	The user has requested assistance.

Bulk Room Email Mapping for Endpoints

Cisco TMS allows you to export or import bulk email address by using .CSV format file to map the email address. The group must be enabled for Bulk Room Email Mapping and any user within that group can perform this activity.

Note: This feature is for Conferencing Connector and this is used only for '@meet scheduling experience' feature. For more information, refer Deployment Guide for Cisco Webex Hybrid Calendar Service.

Export Room Mailbox Address

Follow the procedure to **Export** the .CSV format file:

1. Go to the **TMS web interface > Systems > Bulk Room Email Mapping.**
2. Click **Export**. A **.CSV** format file will be saved. The file includes the following fields for the systems that supports email address mapping:
   - System Name
   - TMS System ID
   - Room mailbox Address
   - Folder Name
   - IP Address

Import Room Mailbox Address

Follow the procedure to **Import** the .CSV format file to map the Room Mailbox Address:

1. Go to the **TMS web interface > Systems > Bulk Room Email Mapping.**
2. Select a **.CSV** format file. The file must include the following mandatory fields:
   - TMS System ID
   - Room mailbox Address
3. Click **Import**.
4. Click **Activity Status** to view the progress.

Notes:

1. Activity Status displays the **Activity Description** and **Activity log**. The results of the activity will be captured in the Activity Log.
2. Admin can check the activity status from **Administrative Tools > Activity Status**. After the upload is completed, a pop-up about this information is displayed.
3. When the .CSV file is imported, only email addresses are updated to the endpoint.

Before backing up the endpoint, export the .CSV file. After the backup is restored to the system, the admin can use the .CSV file to update the old email address for the endpoint. For more information, refer to **Note** in Scheduled Restore, page 150.

System Status Reporting

Table 97 System statuses can be seen in for example Systems > Navigator

Status	Description
Idle	Cisco TMS can communicate with this system, and the system has no active calls registered.
In Call	The system is in a scheduled or ad hoc call.
Unknown	Cisco TMS cannot determine the status of this system. Systems that are recently pre-registered or systems behind a firewall may be found in this state.
Not Yet Activated	Pre-registered systems waiting to be added to a Cisco TMS are found in this state.
Network address missing	No IP address is set on the system. Cisco TMS will therefore not be able to track the system on IP address.
Alive	Cisco TMS can communicate with the system, but is unabled to determine whether there are active calls on the system.
No SNMP response	Cisco TMS is failing to communicate with this system using SNMP. This communication may fail if **SNMP Community Name** is set incorrectly in the system's **Connection** tab in **Systems > Navigator**. *No SNMP response* is a detailed status of the *No Response* status.
No HTTP response	A system that Cisco TMS cannot communicate with using HTTP or HTTPS. *No HTTP response* is a detailed status of the *No Response* status.
No Telnet response	Cisco TMS is failing to communicate with this system using the telnet protocol. *No telnet response* is a detailed status of the *No Response* status.
Wrong username or password	Cisco TMS is using the wrong credentials and cannot communicate with this system. Use the **Connection** tab of the system to correct the username and/or password used to communicate with the system. *Wrong username or password* is a detailed status of the *No Response*status.

Note: The system status values are cached values, and may be up to two minutes old.

Booking

This chapter explains Cisco TMS conference concepts, describes the tasks related to booking, and details the entries in the **Booking** menu.

Conference Basics 162
Booking a Conference 164
New Conference 170
List Conferences 186
List References 191
Ad Hoc Booking 191
Participant Templates 192
Conference Templates 200

Conference Basics

What is a Conference?

A conference is a call between two or more participants. The conference can be:

- point to point
- hosted by a participant that supports multisite
- hosted by an MCU
- externally hosted, that is, hosted by a participant outside of Cisco TMS, see What is an Externally Hosted Conference?, page 163

What is a Participant?

In Cisco TMS, a participant is any system capable of dialing in or being dialed out to during a conference on one of several protocols – depending on which protocols are supported in the conference. Supported protocols depend on how the conference is being hosted and what infrastructure equipment is in place.

Table 98 Examples of protocols and participants

SIP	H.323	ISDN
Cisco Jabber Video for TelePresence	Cisco TelePresence System Codec C Series	Audio dial in (telephone)
Cisco IP Video Phone E20	Cisco TelePresence System MXP Series	ISDN-capable video systems

What is a Video Conference Master?

Video Conference Master is the participant that drives the conference. This participant will be prompted to start the conference if the conference is set up as a manual connect, and will be prompted to extend the conference just before it is due to end (if this setting has been configured in **Administrative Tools > Configuration > Conference Settings**). Not all systems support this feature.

Routing and MCUs

Cisco TMS handles routing automatically. When booking conferences it is not necessary to specify network protocols or MCUs.

You can modify the defaults selected by Cisco TMS on a per conference basis during booking.

If a booking requires an MCU and no MCU is available, an error will be shown.

Port Usage on MCUs

Each call leg will consume one port, in addition extra ports are used for these reasons:

- Streaming (multicast/unicast): If either multicast or unicast, or both, are enabled, streaming takes up one port.
- ConferenceMe: Usually one port per conference. This can be configured in the **MCU Settings** tab during booking.
- Duovideo/presentation: There are four content mode options on a Cisco TelePresence MCU. Of these, *Hybrid* and *Transcoded* take up a port, the others do not.
- Cascading: One port is used for each leg of the cascade.

How are Conference Layout Options Controlled?

Table 99 Layout control on different conference bridge types and alternatives

MCU	Layout
Cisco TelePresence MCU	Uses settings in **Systems > Navigator >** select a Cisco TelePresence MCU **> Settings** tab **> Extended Settings > Conference Layout**. These settings can be modified on a per conference basis during booking: **Booking > New Conference >** Add participants **> MCU Settings** tab **> Conference Layout**.
Cisco TelePresence Server	Does not use any Cisco TMS layout settings. Layout is determined on the TelePresence Server itself depending on which immersive systems are in the call.
Cisco TelePresence Conductor	Does not use any Cisco TMS layout settings. Uses the layout settings defined in the alias templates on the TelePresence Conductor itself.
Cisco TelePresence MPS	Uses the settings in **Administrative Tools > Configuration > Conference Settings > Conference Create Options > Default Picture Mode**. These settings can be modified on a per conference basis during booking: **Booking > New Conference > Advanced Settings > Picture Mode**.

What is an Externally Hosted Conference?

An Externally Hosted Conference is a conference that has been created outside of your Cisco TMS. For example, if another company is hosting a conference and has provided a dial-in video address, you can schedule endpoints in your organization by booking an Externally Hosted Conference in Cisco TMS, making the endpoints dial in to the conference as *One Button To Push* or *Automatic Connect* if desired.

Making a conference externally hosted limits the set of available booking and monitoring features, as Cisco TMS does not control the conference host in any way.

The following Cisco TMS booking features and participants cannot be used with an Externally Hosted Conference:

- Webex
- MCUs
- Guaranteed encryption (**Secure** cannot be set to *Yes*)
- Recording participants
- Non-SIP dial-in participants
- Dial-out participants

Setting **Picture Mode** or **Extend Mode** will also not affect an Externally Hosted Conference.

When monitoring an Externally Hosted Conference in Conference Control Center, features are similarly limited. From CCC, you can add participants and change the end time for the Cisco TMS participants. At end time, these participants will not be disconnected and in Cisco TMS the Externally Hosted Conference will be listed as finished. Cisco TMS cannot extend the Externally Hosted Conference itself.

Cisco TMS disconnects an ongoing extended Externally Hosted Conference, based on the following Meeting Types:

- OBTP: Cisco TMS sends an OBTP to the endpoint. If the participants of the ongoing meeting accept it, then the ongoing conference gets disconnected. Based on the importance of the existing conference, a participant can also decline it.
- Automatic Connect: The new meeting scheduled by Cisco TMS automatically gets connected and the existing meeting gets disconnected.
- Manual Connect: The user of the master endpoint has to click **OK** to get connected to the new meeting.

Note: The **Early Join** option is not available for any type of externally hosted meeting.

Email Notifications

All users involved in booking a conference receive booking confirmation and error notification email messages when the conference is booked, updated, or deleted. This includes the following:

- Conference creator: The user who books the conference.
- Conference owner.
- Any other user who has ever updated the conference.

Editing a recurrent conference series will generate emails sent to all users involved in booking the conference and who have edited the recurrent series or any of the instances.

Editing an instance of a recurrent conference series will generate emails to any users that have edited the series or that instance.

Booking a Conference

There are several ways to schedule a conference in Cisco TMS. **Booking > New Conference** provides advanced setup options for a conference during booking. This page is used in the procedure described below. **Booking > List Conferences > New Conference** also links to the **Booking > New Conference** page.

Other booking options:

- The Smart Scheduler is a light-weight scheduler aimed at a general audience. For more information see the Cisco TMSPE Deployment Guide.
- **Booking > Ad Hoc Booking** allows booking of scheduled conferences for the systems displayed, either as **Reservation Only** or **Automatic Call Launch** conferences.
- **Monitoring > Conference Control Center > New Conference** button displays a New Conference pop-up window from which you can create a conference, adding participants once the conference has been created.

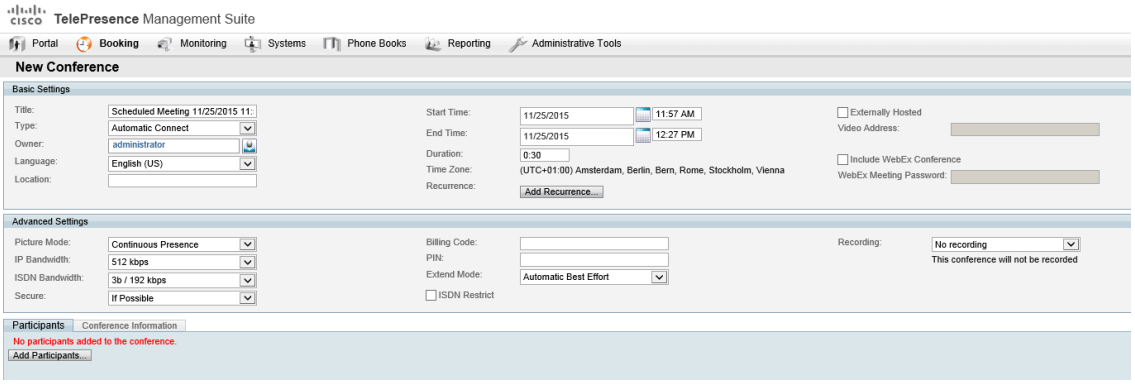
Note: When a conference is created or edited using Cisco TMS Conference Control Center, no confirmation e-mail is sent.

To add systems not managed by Cisco TMS to conferences, there are two options:

1. **Booking > New Conference > Add Participant** button **> External** tab. This option is intended for systems that cannot be booked directly from Cisco TMS, such as provisioned devices. Do not add infrastructure systems as external participants.
2. Create a Participant Template, (**Booking > Participant Template**) and add that as a representation of a participant during the booking. This option was originally intended for the MPS but can be used to add a non-managed system/participant to Cisco TMS or to define more complex or different settings to a participant that the ordinary bookings allow.

To book a conference from **Booking > New Conference**:

1. Enter the basic settings:



   a. Edit the conference title, which will help administrators and users to identify the conference in all Cisco TMS interfaces, and in email notifications.

      Note: Single and double quotes in the **Title** field will be discarded.

   b. Set the start time, and the duration or end time.

   c. Click **Recurrence Settings** to create a series of meetings that are tied together, such as a weekly or daily meeting.

   d. Check **Externally Hosted** if you already have a video address for the meeting generated outside of Cisco TMS. This limits the available options for booking and monitoring.

   e. Check the **Include Webex Conference** to add a Webex meeting and participants to your TelePresence conference. Create a **Webex Meeting Password** that Webex participants must use to access the conference.

2. If necessary, modify any fields in the **Advanced Settings** section, which is pre-populated with values that are set in **Administrative Tools > Configuration > Conference Settings, page 248**.
3. Optionally, add notes about the conference in **Conference Information**.

4. In the **Participants** tab, click **Add Participants** to display the Add Participants pop-up window (ensure you have allowed pop-up windows in your internet browser):

   - Click the tabs to list participants by type. If you have used scheduling before, the default tab is **Last Used** with quick access to the systems you have used recently.
   - Participant availability is displayed based on existing scheduled and ad hoc meetings. The colored vertical lines represent your current requested time for the scheduled meeting.
   - Hover over any system or the blocks in the planner view with the mouse for additional detail about the system or scheduled meeting.
   - Add participants to the meeting by selecting their checkbox and clicking the **>** button. Adding an MCU is optional as Cisco TMS will handle this for you automatically.
   - Use the **External** tab to add systems not managed by Cisco TMS:
     - For dial-out participants, enter their contact information, and Cisco TMS will automatically connect them to the conference at the scheduled time.
     - For dial-in participants, Cisco TMS will reserve the capacity needed and provide you with precise dial-in information to forward to the participant.

       Note: When external participants are added to the conference, the default protocol that is listed depends on the protocol that is chosen as **Preferred Protocol in Routing** in the **Conference Settings** page.
5. Click **OK** when all participants have been added.
   You will be returned to the conference page, with the participant section of the page now showing your selected participants, and some additional tabs. These additional tabs allow advanced scheduling tasks such as altering routing, or setting specific MCU or TelePresence Conductor conference settings for the conference.
6. Optionally, use the **Video Conference Master** drop-down list to determine which system should drive the conference. See What is a Video Conference Master?, page 162.
7. Click **Save Conference**.
   When the conference is saved, Cisco TMS will calculate the routing to determine the best way to connect your selected participants:

   - If Cisco TMS is able to complete the request, you will see the **Confirmation** page, which shows the conference details. These include the list showing how each participant is scheduled to connect, and, if appropriate, the exact dial string the participants must dial.
     You will also receive an email confirmation with an ICS attachment that can be saved to an Outlook (or compatible) calendar.
   - If Cisco TMS is unable to complete the booking request, you will be returned to the **New Conference** page. An error message states why it was not possible to save the meeting.
     Edit the conference settings to try to resolve the issue and save the conference again.

Caution: If you have used Cisco TMS **to schedule a conference which will be hosted on an MCU, you must use** Cisco TMS **to manage the conference. Never make changes to this conference directly on the MCU. This includes changes to layout, and moving participants from one conference to another.**

Booking a Conference with Remote Systems

Some limitations apply when booking conferences that involve endpoints behind a firewall:

- Cisco TMS cannot make an endpoint behind a firewall dial out. The endpoint must therefore either be dialed into, or the person operating the endpoint must manually dial in to the conference.
- When booking conferences that include multiple endpoints behind a firewall as *Automatic Connect*, the conference must include an MCU or local endpoint with embedded multisite support.
  A point-to-point conference with *Automatic Connect* will not work for two systems behind a firewall/NAT, but will work as expected if one of the endpoints is local.

The following limitation is applied while booking conferences that involve only dial-ins:

- To schedule a meeting with conference type as **Manual Connect** in Cisco TMS, atleast one endpoint is required otherwise the conference will get saved as **No Connect**. It is also applicable, if meetings are scheduled using BAPI and conference type is set to **Manual Connect** on Cisco TMS.

Viewing and Editing Existing Conferences

To view or edit a conference:

1. Open **Booking > List Conferences**.
2. Use the options to search for conferences.
3. To view a conference, click on the title, or open the drop-down menu that appears when you hover over the conference title, and select **View**.
   You will see a page similar to the **New Conference** page.
4. Click on the tabs in the lower segment of the window to see the information saved for this conference.
   If the conference is scheduled for the future, you can click the **Edit** button to modify the meeting using the same options as when creating a new conference. The conference will be updated and new confirmation email messages will be distributed.

Note: When an occurrence in the series is in progress and you try to modify the series, Cisco TMS changes the ongoing occurrence into a single meeting and separates it from the series.

Adding Recurrence to a Conference

1. In **Booking > New Conference**, click **Add Recurrence...**.
2. Select the **Start Time** and the duration for each instance of the meeting.
3. Set up the **Recurrence Pattern**.
4. Choose the **Range of Recurrence**.
5. Click **OK** to apply the recurrence to the conference and exit the dialog.
   You will be taken back to the conference booking page where the recurrence pattern and range are now displayed.

To change the conference from a recurrent series to a single instance conference, click **Remove Recurrence**. This will revert the conference back to the start/end date and time in the **New Conference** dialog.

To access the recurrence dialog for an existing conference:

1. Go to **Booking > List Conferences**.
2. Select **Edit** from the pulldown menu, and when prompted, choose to *Edit the series*.
3. Click **Edit Recurrence...**.

Adding Exceptions

1. Click **Exceptions...** to change the date of individual occurrences in the series.
   The occurrences are shown in dark blue.
2. Select an occurrence in the **Recurrence Exceptions** calendar.
   The range of dates that the selected occurrence can be moved within is highlighted.
3. Click one of the highlighted dates to move the occurrence to.
   The exception shows in light blue.

   You cannot move an occurrence past the previous or subsequent occurrence in the series.

To reset all occurrences back to the original recurrence pattern, click **Reset Exceptions**.

Note the following when working with recurrence:

- The maximum number of occurrences in a series is limited to 100.
- The final occurrence in a series cannot take place later than the number of days defined in the **Booking Window** set in **Administrative Tools > Configuration > Conference Settings**.
- Adding CMR Hybrid to a recurrent conference will limit the available recurrence patterns.
- You cannot add Webex to single instances of a recurrent series.
- Note that when editing a single instance of a recurrent series, it is not possible to change the conference owner. This means you cannot change the time zone for an instance.

Booking and Editing Conferences with Cisco TelePresence Conductor

Booking a Conference

1. Book a conference as normal in Cisco TMS using **Booking > New Conference**.
   You do not need to add the TelePresence Conductor to the conference manually if it is set as the preferred MCU in **Conference Settings**.

   If you have multiple TelePresence Conductors in Cisco TMS, the one in the IP zone matching the majority of endpoints will be selected automatically.

2. Once you have added the participants to the conference, click the **Connection Settings** tab to display the **TelePresence Conductor Settings** tab and fill in the fields as appropriate:

Table 100 Alias configuration settings

Field	Description
Alias	Select the alias you want to use as your conference dial-in address. The aliases displayed in the drop-down have been configured in **Systems > Navigator >** select a TelePresence Conductor **> TelePresence Conductor** tab **> Aliases**. For reference, see TelePresence Conductor, page 95 .
Variable	If the alias is not fixed, you can change the variable part to contain something appropriate for your conference. As you type in the **Variable** field, you will see the preview change to reflect what you are typing. The variable can contain any alphanumeric characters. An example of a variable might be the name of the person who is hosting the conference. The **Variable** field is pre-populated by Cisco TMS with the first available Numeric ID set in the **Extended Settings** for the TelePresence Conductor in **Systems > Navigator**. If you do not change the variable, the auto-generated address which you can see in the **Preview** field will be used for the conference. Click **Check Address Availability** to see whether your chosen variable alias is available at the time chosen. If you change the variable, but want to go back to a Cisco TMS-generated variable, click **Regenerate Address**.
Address Preview	A preview of the address that participants will use to dial into the conference. As you change the variable, the blue part of the address in this field will change.
Description	This field contains the description added for the alias here: **Systems > Navigator >** select a TelePresence Conductor **> Aliases tab > Edit Aliases** This field is not displayed if there is no description for the alias you have selected.
Conference Layout	Set the layout for the conference.
Limit Ports to Number of Scheduled Participants	Limit ports to the number of scheduled audio and video participants. No additional participants will be able to join the conference.

3. To check that your chosen alias is available, click **Check Address Availability**.
4. Click **Save Conference**.

Note that the following scheduling options are not supported for TelePresence Conductor in Cisco TMS:

- Media port reservation—do not enable this on the MCUs.
- Cisco TMS Conference templates
- Participant templates
- Distribution
- TelePresence Conductor conference type Lecture. Only conference templates using the Meeting conference type are supported.

Note: IP dialing is not supported when scheduling conferences with a TelePresence Conductor.

Editing a Conference

Edit the conference in Cisco TMS using **Booking > List Conferences**.

In addition, you can change the conference address from the **TelePresence Conductor Settings** tab.

Note: Cisco TMS will auto-select an alias when first calculating the route after a conference has been booked. Any subsequent changes to the participant list will not affect the selection of alias.

New Conference

In Cisco TMS: **Booking > New Conference**

The **New Conference** page has a Basic Settings, page 170 section, an Advanced Settings, page 172 section, and a lower tabbed area.

Basic Settings

Table 101 Basic settings when booking a new conference

Field	Description
Title	The title of the conference with date and time. You can type the title yourself or leave the default title, date and time, which is copied from the field **Default Conference Title** in the **Administrative Tools > Configuration > Conference Settings**.
Private	This option indicates whether your conference is marked as a **Private** meeting. When the scheduled meeting is marked as **Private**, irrespective of any meeting type (OBTP or Automatic connect), the scheduled meeting title on the endpoint meeting list, is named as **Private Meeting**. The original meeting title cannot be viewed by the room users while browsing the meeting list in the endpoint. Cisco TMS Admin will be able to view the original meeting title and know whether the meeting is a **Private** meeting or not. Meeting that is marked as private, indicates as **Yes** for private field in Meeting Landing Page, List and View Conference pages. Note: On the endpoint calendar, only the customized private meeting title is displayed. The original meeting title will be displayed instead of **Private** meeting at the start of meeting and as well as for an ongoing meeting, if the original title is sent by the bridge. Setting a meeting as private can be done only via Cisco TMSXE or BAPI client and not via Cisco TMS portal.

Table 101 Basic settings when booking a new conference (continued)

Field	Description
Type	How the conference will connect: ■ *Automatic Connect*: Cisco TMS will automatically connect all the participants at the specified time and date. ■ *One Button to Push*: Conference dial-in information will be presented automatically on endpoints that support One Button to Push an email with conference information including the dial-in number will be sent to the conference owner to forward to these participants. Note that *One Button to Push* is supported by those systems that are supported by Cisco TMS. ■ *Manual Connect*: At the specified time and date, the system listed as the Video Conference Master will be prompted to begin the call. The call will connect automatically when the Video Conference Master initiates the call. ■ *No Connect*: This option will reserve the system(s) and generate the call route, but will not connect the conference. These are the alternative ways to connect if this option is chosen: – The conference can be started by clicking **Connect** for the participants in **Conference Control Center**. – I there are only two participants in the conference, one can call the other. – If the conference is booked with an MCU, all participants must dial in. ■ *Reservation*: This option will reserve the system(s) but will not initiate any connections or generate a call route. If the booking contains one or more MCUs, all ports on the MCU(s) will be reserved for the conference.
Owner	The default owner of the conference is the user that is logged on. If the permission for **Book on behalf of** is set in **Administrative Tools > User Administration > Groups** for the group the user is a member of, the user can book meetings on behalf of the other users. The users booked on behalf of, will be conference owners. Information about the conference owner is used in the **Conference Control Center** and **List Conferences** pages. The owner of the conference will receive a booking confirmation by email for the booked meeting. The email contains information about the start time, end time, participants and call route for the conference.
Language	Specify the language for all conference emails, and in-video meeting end notifications.
Location	A textual description of the physical location(s) of the conference.
Start Time	Set the start date and time of the conference.
End Time	Set the end date and time of the conference. Cisco TMS ends the conference nine seconds before the actual end time. As, Cisco TMS takes some time to cleanup and release the resources.
Duration	Set the duration of the conference.
Add Recurrence	Make the conference a recurrent series. For further details see: Adding Recurrence to a Conference , page 167.
Externally Hosted	To schedule endpoints in Cisco TMS for a conference created outside of Cisco TMS, you can book an Externally Hosted Conference. You must then provide the exact video address of the address in the **Video Address** field below. Beware that some features are not supported when booking an Externally Hosted Conference, such as Webex and guaranteed encryption. For details, see What is an Externally Hosted Conference?, page 163.

Table 101 Basic settings when booking a new conference (continued)

Field	Description
Video Address	This field is only available when **Externally Hosted** is checked. You must provide the exact SIP video address that endpoints will need to dial to join the conference. This field is not validated, as the SIP video address may have different formats and the conference host of an Externally Hosted Conference is not controlled by Cisco TMS in any way.
Include Webex Conference	Add a Webex meeting and participants to your TelePresence conference.
Webex Meeting Password	The default Webex password is numeric and the length is a minimum of six digits. However, the Webex Administrator can configure the requirements to create a password that can be a combination of the following conditions: ▪ Mixed case ▪ Minimum password length ▪ Minimum number of numeric value ▪ Minimum number of alpha ▪ Minimum number of special characters ▪ Do not allow dynamic web page text for meeting password ▪ Do not allow meeting passwords from a list related to words like Cisco, password, Webex etc.

Advanced Settings

Table 102 Advanced settings when booking a new conference

Field	Description
Picture mode	▪ *Voice Switched*: Only the participant who is talking will be seen, and if another participant starts talking, the picture will switch to them. ▪ *Continuous Presence*: A split screen showing all participants equally. ▪ *Enhanced Continuous Presence*: The participant who is speaking shows largest with the other participants shown around the main picture.
IP Bandwidth	**IP Bandwidth** is preset in **Administrative Tools > Configuration > Conference Settings > Conference Create Options** section, **Default Bandwidth** field. This bandwidth will be the default used in a scheduled conference but can be changed during booking. Systems that have an upper limit lower than **IP Bandwidth** will connect using their maximum bandwidth. IP Bandwidth range is from 64kbps to 6144kbps. Bandwidth restrictions put in place by call control infrastructure will override this setting. **Note:** This does not apply to CTS and TX systems – it is not possible to specifiy the bandwidth a CTS or TX system uses in a call from Cisco TMS.

Table 102 Advanced settings when booking a new conference (continued)

Field	Description
ISDN Bandwidth	**ISDN Bandwidth** is preset in **Administrative Tools > Configuration > Conference Settings > Conference Create Options** section, **Default ISDN Bandwidth** field. This bandwidth will by default be used in a scheduled conference but can be changed during booking. Systems that have an upper limit lower than **ISDN Bandwidth**, will connect using their maximum bandwidth. The first digits denote the number of b-channels. The second number is the bandwidth in kbps. The range is from 64kbps to 4096kbps.
Secure	If **Secure** is set to *Yes*, and the conference is hosted on a TelePresence Conductor or bridge, participants can be scheduled in the conference whether they support encryption or not. Encryption should always be set to **Yes** on the bridge/TelePresence Conductor. For point-to-point or multisite conferences, if **Secure** is set to *Yes*, Cisco TMS will only allow the conference to be booked if every leg of the call is secure. This includes checking whether the endpoint supports secure signaling. External Participants are always considered to be **Unsecure**, if there is no bridge in the conference. **Note:** If an endpoint that supports encryption has encryption set to *Off* and is added to a conference which is encrypted, encryption will be set on the endpoint, and this setting will persist after the conference has ended, until set to *Off* on the endpoint itself.
Billing Code	Billing codes are only supported for Cisco TelePresence MXP systems. Specify a billing code to apply for the scheduled conference. How billing codes are applied depends on the settings **Billing Code for Scheduled Calls** and **Enable Billing Code Selection Popup** in Conference Settings, page 248: ▪ *No*–billing codes entered during booking will not be applied. ▪ *Optional*–any billing code can be entered during booking. ▪ *Required*–a billing code matching the list in **Administrative Tools > Billing Codes > Manage Billing Codes** must be entered during booking. See Manage Billing Codes, page 280. If **Enable Billing Code Selection Popup** is set to *Yes*, the user may access a list of valid billing codes directly from the booking page. Note that regardless of setting, the characters ; and = cannot be used as part of a billing code.
PIN	Adding a numeric PIN prevents uninvited participants from joining the conference. The PIN will be included in the conference information email message that is sent to the organizer after booking and must be forwarded to dial-in participants. Changing the PIN after a conference has started is not supported and may prevent participants from joining.

Table 102 Advanced settings when booking a new conference (continued)

Field	Description
Extend Mode	■ *None*: Ensure that meetings are never automatically extended . ■ *Endpoint Prompt*: Display a non-configurable Extend Meeting message on the Video Conference Master both 5 minutes and 1 minute prior to the end time of the conference. ■ *Automatic Best Effort*: Enable automatic extension of scheduled conferences by 15 minutes up to a maximum of 16 times. The meeting will be extended irrespective of the number of participants connected in the conference only for the first auto extension. The subsequent extensions happen only if more than one participants are connected in the conference. The meeting extension happens only, when there are no conflicting meetings for any of the participants within the next 15 minutes, unless **Resource Availability Check on Extension** is set to *Ignore*.
ISDN Restrict	If checked, the conference will use ISDN restrict (56kbps). A restricted call is a call to a 56 kbps network.
Recording	Use the drop-down menu to select a recording alias from the Cisco TelePresence Content Server you want to record the conference from. Displayed below each Content Server registered to Cisco TMS are the default system recording aliases that all users can see, and a list of Personal Recording Aliases that are owned by the currently logged in user. Naming the recording aliases appropriately on the Content Server will assist users in finding and using the correct one. **Note:** This option is only visible if a Content Server is available.

Participants Tab

Add Participants launches the **Add Participants** window. This is where you add participants to a conference and check availability information.

Add Participants Window

In Cisco TMS: **Booking > New Conference**

Use the query section, if shown, to search for participants on each page.

Table 103 Tabs in the Add Participants window

Tab	Description
Last Used	A list of the ten last participants selected by the logged in user for previous bookings.
Endpoints	Endpoints registered in Cisco TMS can be added as participants here.
Users	Users listed here have been added or imported to Cisco TelePresence Management Suite Provisioning Extension through **Systems > Provisioning > Users**. Participants added from this list will not be connected automatically to the conference, but will receive an email with details on how to connect. The email will be generated automatically when the conference is saved. The Page Size on this tab is limited to 1000.

Table 103 Tabs in the Add Participants window (continued)

Tab	Description
MCUs	MCUs (including Cisco TelePresence Conductor and Cisco TelePresence Server) that are registered in Cisco TMS are shown in this tab.
Phone Books	Phone book participants can be added here. You can use the **Query** field to search for names and/or select a phone book from the drop-down list. The page size on this tab is limited to 1000. This page loads the records based on page size. It allows you to load as many records from the database in a single page. Also, you can use the search functionality to fetch the particular record from database directly even when the record is not loaded on the page. Phone books that contain only *Search Only* sources are not displayed in this window.
External	Use this tab to add dial in and dial out participants, specifying protocol type, audio/video type and number of participants. You can specify a name for each participant. You cannot save a conference, when only one external participant is added in the conference. When you add only one external participant and schedule the conference, Cisco TMS does not allow you to save this conference. An error message "Cannot Save the conference. It has only one External Participant" is displayed. **Note:** Infrastructure systems must not be added here.
Templates	Participant Templates are intended for use by administrators, therefore users can only view the Participant Templates tab if they have been granted group permissions to do so. It is possible to create a new participant template from this tab. For more details, see Participant Templates, page 192.
Equipment	Add equipment registered in Cisco TMS.

Table 104 Checkboxes and buttons in the Add Participants window

Checkbox/Button	Description
Details (link)	Opens the system details window for a selected system.
Default Booking Tab	Check this box to make the tab you are currently on the default which will be shown every time you open the **Add Participants** window.
Show Availability	■ If checked, free/busy information will be shown for systems. ■ If unchecked, system information will be shown.
Always Add My Primary System	Add your primary system automatically to every conference.
Add My Primary System	Add your primary system to this conference. This button is grayed out if the user has no primary system defined.

When participants have been added, more buttons and links are displayed.

Video Conference Master is the participant that drives the conference. This participant will be prompted to start the conference if the conference is set up as a manual connect, and will be prompted to extend the conference just before it is due to end (if this setting has been configured in **Administrative Tools > Configuration > Conference Settings**). Not all systems support this feature.

Webex Details Tab

This tab displays if you have added Cisco Collaboration Meeting Rooms Hybrid to the conference. No details are shown until the conference has been saved.

Connection Settings Tab

This tab appears after participants are added to the conference and contains information on how the call will be set up. Depending on the participants, it is possible to view or change several settings here, including:

- direction of calls.
- protocol.
- dial strings.

By clicking on the **Settings** link to the right of each participant, additional settings can be configured per participant, including:

- Bandwidth
- For conferences hosted on a bridge:
  - You can mute audio and video on connect for each separate participant.
  - For dial-out participants, you can set **DTMF Tones**.
- Editing the **Dial String** field changes the dial string dialed by that participant, but will not change anything on the remote end, for example allocated ports on bridges.

Select Main

The Main participant is the system that hosts the conference. This can be either an MCU, or a system with multisite if there are more than two participants. If the conference is point-to-point then either system can be the Main. If booking from the Cisco TMS web interface, you can choose which participant you want to be the Main from the drop-down menu.

For more details see The Main Participant, page 32.

Routing

Call direction depends on both conference type and the type of endpoint. For One Button to Push conferences, the call direction is always from the endpoint.

Cascaded MCU calls and recording calls are always scheduled and initiated by Cisco TMS. For more information see Protocols and Call Control, page 34

Distribution (Routing Modes)

Table 105 Distribution types

Type	Description
No distribution	Only one MCU will be used in the conference.

Table 105 Distribution types (continued)

Type	Description
Least Cost Routing	Cisco TMS will try to reduce call cost and/or bandwidth on all protocols by using multiple MCUs. Cisco TMS will ensure that systems use local MCUs wherever possible using zones, for more information see How Zones Work, page 38. For example, if Cisco TMS has access to one MCU in Sweden and one MCU in France, and there are three participants located in Sweden and three participants located in France, *Least Cost Routing* mode would use the Sweden MCU to call the participants in Sweden, the France MCU to call the participants in France and then connect the two MCUs together with only one connection.
Best Impression	For large conferences, if one single MCU does not have enough resources to call all participants, *Best Impression* routing will use multiple MCUs to connect all participants. *Best Impression* connects MCUs as follows: it will identify the MCU with the most available video ports, and fill it up with participants, and then continue on the MCU with the next highest number of available video ports, fill it with participants and so on.

System availability

Some of the tabs contain free/busy information for systems in the default view.

Participants that are already booked in a conference at the time you have chosen are marked red. Participants with *No Response* status are also marked red. A tooltip for each participant provides more detailed information.

Availability information can be shown for:

- Endpoints
- Single-use Participant Templates

Adding and removing participants

To add a participant you can either:

- Select the participant and click the **>** button.
- Double-click on the participant.
- Select all the participants you want added, then click **OK**.

To remove a participant, select it and click the **<** button.

MCU Settings Tab

If an MCU or TelePresence Server is hosting the conference, this tab will be visible. For more information see MCU Settings, page 178.

TelePresence Conductor Settings Tab

If a TelePresence Conductor is hosting the conference, this tab will be visible. For more information see Cisco TelePresence Conductor Settings, page 185.

Conference Information Tab

Table 106 Fields on the Conference Information tab

Field	Description

Table 106 Fields on the Conference Information tab (continued)

Send Email To	Specify who will receive the booking confirmation by email. Email addresses can be separated by semicolon, comma or space. Note: You must use the same separator when multiple email addresses are added (For example: a@cisco.com, b@cisco.com, c@cisco.com) and combination of separators are not allowed (For example: a@cisco.com, b@cisco.com ; c@cisco.com d@cisco.com). This field supports 255 characters.
Email Message	This field can contain conference-specific data such as a meeting agenda. The information will be included in the booking confirmation email.
Conference Notes	Additional notes can be added here, which will be viewable in Conference Control Center but not in the booking confirmation email.
Reference Name	A reference can be added to the conference, which may contain information about a customer to bill for the conference. Click **New Reference** to add one, then fill in the information you want: 1. **Reference Name**: Name of Reference. (Mandatory field). 2. **Reference Code**: A code for the reference. (For example Customer number) 3. **Comment**: Field for any comment for reference. 4. **Contact Information**: Enter a contact person, with a phone number here. For more information see List References, page 191.

Webex Details Tab

This tab contains details about the Webex meeting, including the links to click on to access the meeting as either host or participant.

MCU Settings

When an MCU is booked in a conference, an **MCU Settings** tab will appear on the booking page.

Cisco TelePresence MCU

Not all of the settings below are available for all Cisco TelePresence MCU models.

Table 107 Extended MCU settings

Setting	Description
Enable ISDN Gateway DID Mapping	DID (Direct Inbound Dialing) allows for inbound ISDN connections to MCUs without ISDN support. For instructions on setting up DID, see the documentation for your gateway. For more information, see Extended Settings DID Mapping for Cisco TelePresence MCUs, page 37.
Conference Layout	Defines the picture layout for the conference. There are several alternatives to select between. For more information about conference layouts, see the documentation for your MCU.

Table 107 Extended MCU settings (continued)

Setting	Description
Visibility	Indicates the visibility of the conference on the auto attendant and the web interface. The options are: ■ *Public*: The conference will be listed in the auto attendant and be visible to all users of the web interface. ■ *Private*: The conference will not be listed in any auto attendant except for auto attendants specifically set to show it. The conference will also only be visible in the web interface to the conference owner and to the admin user.
Dual Video Stream	Enable an additional video stream, such as a presentation.
Content Mode	Determine the mode for sending content packet streams. The options are: ■ *Disabled*: Content is not transmitted. ■ *Passthrough*: Content is not decoded and is simply repackaged and sent out to each eligible endpoint in the conference. ■ *Hybrid*: The MCU sends out two content streams: a higher resolution one (passthrough), and a lower resolution stream transcoded and scaled down for any endpoints that are unable to support the higher stream. ■ *Transcoded*: A single transcoded content stream is sent.
Register with Gatekeeper	Registers the conference with the H.323 registrar.
Conference SIP registration	Registers the conference with the SIP registrar.
Allow Chair Control	Floor and chair control is encompassed by the H.243 protocol. The options are: ■ *None*: The use of floor and chair controls is not allowed in this conference. ■ *Floor Control Only*: Only floor control is allowed in this conference. Chair control is not allowed. Any participant can 'take the floor' so long as no other participant has currently has done so. ■ *Chair and Floor Control*: Both floor and chair controls are allowed in this conference. Any participant can take the floor, and any chairperson participant can take the chair so long as no other participant has currently done so.
Allow Layout Control	Enable conference participants to control the conference layout using DTMF signals or far-end camera control.
Automatic Lecture Mode	When this feature is enabled for a conference, the MCU identifies the loudest speaker as the lecturer. The lecturer will see a normal continuous presence view or a custom layout, if defined. For the other participants, the view of the lecturer will override any custom layout. The options are: ■ *Disabled* ■ *After 10 seconds* ■ *After 30 seconds* ■ *After 1 minute* ■ *Immediately*

Table 107 Extended MCU settings (continued)

Setting	Description
Ports to Reserve for ConferenceMe	If using the ConferenceMe feature on the MCU, ports can be reserved for it using this field.
Limit Ports to Number of Scheduled Participants	Limit ports to the number of scheduled audio and video participants. No additional participants will be able to join the conference.
Multicast Streaming Enabled	Allows multicast streaming for the conference.
Unicast Streaming Enabled	Allows unicast streaming for this conference.

Cisco TelePresence Server

Table 108 Extended TelePresence Server settings

Field	Description
Register With Gatekeeper	Register the conference's numeric ID with the gatekeeper (if H.323 registration is enabled on TelePresence Server).
Conference SIP Registration	Register the conference's numeric ID with the registrar (if SIP registration is enabled on TelePresence Server).
Dual Video Stream	Enable an additional video stream, such as a presentation.
Limit Ports to Number of Scheduled Participants	Limit ports to the number of scheduled audio and video participants. No additional participants will be able to join the conference.
Lock Conference on Creation	Lock the conference when it is created. You can still add pre-configured participants before the conference starts, but no participants will be able to join (call in) when the conference is active. You can call out to invite participants into a locked conference.
Conference Lock Duration	Number of seconds during which the conference will be kept locked (if enabled above).
Use Lobby Screen for Conferences	Enable TelePresence Server to display lobby screens to participants. The lobby screen shows the conference title, start and end times (if applicable), and an optional lobby message. The message is set on a per conference basis. Participants see this screen when they join a conference, or when there is no video to display. This is set to On by default when a TelePresence Server is added to Cisco TMS.
Conference Lobby Message	Enter text to display on the lobby screen. Participants will see this text if **Use Lobby Screen for conferences** is enabled server-wide or for their particular conference.

Cisco TelePresence MPS Settings

Conference Layout	**Auto**: When set to Auto the most suitable conference layout will automatically be selected depending on the total number of participants in the actual conference. **Voice Switched**: Full Screen voice switched will show the current speaker in full screen to all the other participants, regardless of how many participants there are in the conference. Current speaker will see the previous speaker. **Custom Selection**: Select a specific Conference Layout for the conference. The different selections are illustrated to the right. **CP Auto**: When set to CP Auto there will be a dynamic change in layout dependent on the number of sites in the conference. The **CP Auto** will start with VS- > CP4- > CP9- > CP16.
Welcome picture and Sound (Show Welcome Message)	When selected, a Welcome screen and audio message will be shown to each new participant of the conference.
Allow G.728	The MPS supports high quality audio even on low call rate. On low call rate the MPS will prioritize G.722.1. Video participants not supporting this, will receive low quality audio G.728 instead, when **Allow G.728** is selected. To ensure high quality audio on low call rate, unselect **Allow G.728** and video participants not able to support G.722.1, will receive G.722 instead. ■ *On*: The MPS supports high quality audio even on low call rate. On low call rate the MPS will prioritize G.722.1. The video participants which do not support G.722.1 will receive low quality audio G.728 instead when this feature is enabled. ■ *Off*: Ensure high quality audio on low call rate. Video participants who are not able to support G.722.1 will receive G.722 instead.
NetworkID	Used to identify port or interface number within a network module. Enter a value between 1 and 32 ■ Specify which IP network to use, only 1 and 2 are valid values (optional). ■ Specify which V.35 port to use (mandatory).
Video Custom Format (Custom Formats)	■ *On*: Support custom formats such as SIF and VGA resolutions. Allow true resolution to be maintained, rather than being scaled to another format. This is of particular benefit to users of NTSC and VGA resolutions, ensuring that their images are not scaled to fit with the PAL standard. ■ *Off*: Set to Off when support for custom formats is not needed.
Entry/Exit Tones	When selected, a tone signal will be heard each time a participant is entering or leaving the conference.
Floor To FullScreen	This function only applies for the Continuous Presence 5+1 and 7+1 layout. When selected, the participant requesting the floor will be shown in full screen to all the other video participants, regardless of current speaker. The same will happen if the conference administrator **Assign Floor** to a site. When unselected, the participant requesting the floor will be shown in the larger quadrant of the 5+1 or 7+1 layout.
Telephone Indication	■ *On*: Display Telephone Indicator when there are telephone (audio only) participants connected to the conference. When the telephone participant is speaking, the indicator will be outlined. ■ *Off*: Disable the Telephone Indicator.
Participant Identifier Timeout	Set the number of seconds (1 - 30 seconds) the Participant Identifier will be visible, if set to auto. The identifier will re-appear at every picture changing event.

Network Error Handling	■ *None*: Disable error handling. ■ *IPLR*: Use if one or more sites are experiencing network errors. ■ *FURBlock* (Fast Update Request Block): Use if one or more sites are experiencing network errors.
FUR Filter Interval	Denotes the number of seconds between Fast Update Requests, for example the minimum time between FURs that will refresh the picture.
Far End Telephone Echo Suppression	Analog telephone lines, speaker phones and telephone headsets may all cause echoes. The Far End Telephone Echo Suppression function eliminates some or the entire experienced echo. ■ *Off*: Set to **Off** to disable Far End Telephone Echo Suppression. ■ *Normal*: Set to **Normal** to remove weak echo. ■ *High*: Set to **High** to remove strong echo.
Bandwidth management	■ *Manual*: Disables automatic regulations of sites to Low rate encoder, based on video rate reports. ■ *Auto*: Enables automatic regulations of sites to Low rate encoder, based on video rate reports.
Password Out	■ *On*: When dialing out from a password protected conference, the participant is met with the **Password Enquiry** screen and sound, asking for a password. This setting can be used to ensure that only authorized participants are able to join the conference also when dialing out from the conference. ■ *Off*: No password is required when dialing out.
Dual Video Stream	The MCU supports DuoVideo^{TF}, H.239 and BFCP: ■ *On*: Set to **On** to enable a Dual Video Stream protocol for this conference. Both DuoVideo^{TF} and H.239 or BFCP are supported in the same conference. ■ *Off*: When set to **Off**, Dual Video Stream will not be supported in this conference.
Cascading Mode	Join two or more conferences together: ■ *Auto*: Automatically determine which conference is "master" and which conference(s) are "slaves". The "master" conference will have control of the video layout. When left in Auto mode, the conference dialing in to the other conferences will become the "master". ■ *Master*: Set to **Master** when this conference is the one controlling the video layout for the whole conference. It is not recommended to have more than one 'master' in a conference. ■ *Slave*: Set to **Slave** when another conference manually has been assigned 'master'. The slave will be forced to Full Screen voice switched mode.
Conference Selfview	■ *On*: Set to **On** to enable Conference Selfview. The users will see themselves in the picture when more than one participant is in the conference. ■ *Off*: Set to **Off** to disable Conference Selfview.

AudioLeveling (AGC)	Ensures that all participants will receive the same audio level from all other participants, regardless of the levels transmitted. AGC - Automatic Gain Control. In most conferences, the participants will speak at different levels. As a result, some of the participants are harder to hear than others. The Audio Leveling corrects this problem by automatically increasing the microphone levels when "quiet" or "distant" people speak, and by decreasing the microphone levels when "louder" people speak. 1. *On*: When set to **On** the MCU maintains the audio signal level at a fixed value by attenuating strong signals and amplifying weak signals. Very weak signals, i.e. noise alone, will not be amplified. 2. *Off*: Set to **Off** to disable Audio Leveling (AGC).
Legacy Level	When connecting older videoconferencing endpoints to the MCU, problems can occur since older equipment sometimes does not handle modern capabilities. When selected, some capabilities are not being sent from the MCU. See the software release document for more information.
Minimum Bandwidth Threshold	If a participant calls in with a lower bandwidth than the Minimum Bandwidth Threshold, the participant will receive audio only (not live video) as well as a poster saying the bandwidth is to too low. After 10 seconds the participant will receive low rate video. The Minimum Bandwidth Threshold can be modified during a conference. The system will move calls below the defined Minimum Bandwidth Threshold to a low rate encoder. **Note:** Once a participant is moved to the low rate encoder, they will not be moved back even if the Minimum Bandwidth Threshold is lowered.
Speaker Indication	■ *On*: Set to **On** to enable a Speaker Indicator (a colored line) to be displayed around the sub-picture that will indicate who the currently speaking participant is. ■ *Off*: Set to **Off** to disable the colored line to be displayed.
Chair Control	■ *On*: The conference will support H.243 and BFCP Chair Control functionality initiated from the participants connected to the conference. ■ *Off*: Disable Chair Control.
IPLR Robust Mode	■ *IPLR* (Intelligent Packet Loss Recovery) If one or more sites are experiencing network errors. ■ *Auto*: When set to **Auto**, the IPLR Robust Mode is turned on for each encoder when needed. ■ *On*: When set to **On**, the IPLR Robust Mode is on for all encoders.
Voice Switch Timeout	Defines the number of seconds between 1 and 10, a participant must speak before it gets the speaker indication and is shown as the speaker to the other endpoints. A long timeout might be suitable in noisy environments and in conferences with many participants.
Optimal Voice Switch	■ *On*: Enable Optimal video format in Voice Switch mode, if the connected endpoints allow this. Icons and text will not be available. ■ *Off*: Use normal transcoding when doing Voice switch. **Note:** Optimal Voice Switch is only available on IP.

Web Snapshots	Web snapshots are shown in the upper right corner of the web interface, and will show snapshots of the video from the participants and dual video stream. The snapshots are updated in accordance to the refresh rate (placed above the snapshot). 1. *On*: The Conference Snapshot and Dual Video Stream Snapshot will show the video transmitted from the MCU to the participants. 2. *Off*: A picture notification that Web Snapshots is disabled will appear.
Encryption Mode	■ *Auto*: Set to **Auto** to use the highest level of encryption available on each of the participants connected in the conference. This means that there can be a mix of DES and AES encrypted connections in the same conference. ■ *AES 128*: Allow only participants with AES 128 bit encryption capabilities. Participants without this capability will not be able to join the conference. ■ *DES*: Allow only participants with DES 56 bit encryption capabilities. Participants without this capability will not be able to join the conference.
Secondary Rate	■ *On*: Make the conference support two outgoing bandwidths if needed, in addition to the low rate video. ■ *Off*: Disable Secondary Rate.
CPAutoswitching	The **CP Autoswitching** enables you to swap non speaking sites with the least active sites in the picture. This lets you see all participants in a conference, even if they are not speaking.
Video Format (Video Optimization Mode)	Defines the video format for Continuous Presence (CP) mode. ■ *Auto*: (Best Impression^{TF}) In Continuous Presence mode the MPS will select Motion (CIF) if the call rate is below 256 kbps and sending 4:3 aspect ratio. When sending 16:9 aspect ratio the MPS will select Motion (w288p) if the call rate is below 512 kbps. At call rates of 256 kbps and higher the MPS will select Sharpness (4CIF) when sending 4:3 aspect ratio. When sending 16:9 aspect ratio the MPS will select Sharpness (w576p) at call rates of 512 kbps and higher. ■ *Motion*: Set to Motion to prioritize motion and show up to 30 fps in CIF resolution and transmit the highest common format, preferably H.264 CIF when sending 4:3 aspect ratio or H.263+ w288p when sending 16:9 aspect ratio. ■ *Sharpness*: Set to Sharpness to prioritize crisp and clear picture and transmit the highest common format, preferably H.263+ 4CIF when sending 4:3 aspect ratio or H.263+ w576p when sending 16:9 aspect ratio. In Full Screen Voice Switched Conference layout, the MCU will prioritize H.264 CIF as the highest common format.
Allow Incoming Calls	When selected, incoming calls are automatically answered. If unselected, all incoming calls will be rejected.
Telephone Noise Suppression (Telephone Filter)	■ *On*: Attenuates the noise which normally is introduced when adding mobile phones to a conference and the background noise normally heard when the telephone participant is not speaking. ■ *Off*: Disable Telephone Noise Suppression.
Timeout Participants from Call List	■ *On*: When set to **On** all participants that have been disconnected from the conference will be cleared from the Call List within 2 minutes. ■ *Off*: Set to **Off** to disable the Timeout Participants from Call List.

Participant Identifier	■ *Auto*: Let the System Name of a participant to be displayed the number of seconds set in Participant Identifier Timeout. ■ *On*: Enable the System Name for each participant to be displayed in the picture during the conference. ■ *Off*: Set to **Off** to disable the System Name to be displayed.
Lecture Mode	■ *On*: Set to **On** to enable the Lecturer to be displayed in full screen to the other participants. The Lecturer is the participant which is assigned floor. The Lecturer will see a scan of all the participants in a full screen view or one of the supported sub-picture views. To enable the scan of other sites the CP Autoswitching must be set. ■ *Off*: Set to **Off** to disable the Lecturer, the participant which is assigned floor, to be view in full screen.
FUR Block Sites	■ *FURBlock* (Fast Update Request Block) if one or more sites are experiencing network errors. ■ *Auto*: FUR's from sites that send too many will be blocked. ■ *On*: FUR's from all sites will be blocked.
Protect	■ *On*: Only predefined Protected Numbers are allowed to join this conference. The **Protected Numbers** field will be shown, and numbers can be configured from the Dial-in Configuration in the **MCU Conference Overview**. ■ *Off*: Protect mode disabled.
Encoder Selection Policy	■ *Best Bit Rate*: Make the MPS prioritize the video quality for sites based on bit rate. The system will move participants with a Low Video Rate to a secondary encoder, if it is available. If no sites are moved, the system will move sites with Low Video Standard. ■ *Best Video Standard*: Make the MPS prioritize sites based on video standard. The system will move participants with a Low Video Standard to a secondary encoder, if it is available. If no sites are moved, the system will move sites with Low Video Rate. ■ *Best Resolution*: Make the MPS prioritize the video quality for sites based on resolution. The system will move participants with a Low Resolution to a secondary encoder, if it is available. If no sites are moved, the system will move sites with low video rate.

Cisco TelePresence Conductor Settings

In Cisco TMS: **Booking > New Conference**

Table 109 Alias configuration settings

Field	Description
Alias	Select the alias you want to use as your conference dial-in address. The aliases displayed in the drop-down have been configured in **Systems > Navigator >** select a TelePresence Conductor **> TelePresence Conductor** tab **> Aliases**. For reference, see TelePresence Conductor, page 95 .

Table 109 Alias configuration settings (continued)

Field	Description
Variable	If the alias is not fixed, you can change the variable part to contain something appropriate for your conference. As you type in the **Variable** field, you will see the preview change to reflect what you are typing. The variable can contain any alphanumeric characters. An example of a variable might be the name of the person who is hosting the conference. The **Variable** field is pre-populated by Cisco TMS with the first available Numeric ID set in the **Extended Settings** for the TelePresence Conductor in **Systems > Navigator**. If you do not change the variable, the auto-generated address which you can see in the **Preview** field will be used for the conference. Click **Check Address Availability** to see whether your chosen variable alias is available at the time chosen. If you change the variable, but want to go back to a Cisco TMS-generated variable, click **Regenerate Address**.
Address Preview	A preview of the address that participants will use to dial into the conference. As you change the variable, the blue part of the address in this field will change.
Description	This field contains the description added for the alias here: **Systems > Navigator >** select a TelePresence Conductor **> Aliases tab > Edit Aliases** This field is not displayed if there is no description for the alias you have selected.
Conference Layout	Set the layout for the conference.
Limit Ports to Number of Scheduled Participants	Limit ports to the number of scheduled audio and video participants. No additional participants will be able to join the conference.

List Conferences

In Cisco TMS: **Booking > List Conferences**

The **List Conferences** page displays a list of conferences based on search criteria. You can save a default search that will be displayed when you access the page.

Editing Conferences from This Page

To edit conferences from this page and to view some of the options, the logged-in user must be a member of a group with the following permissions set in **Administrative Tools > User Administration > Groups**:

Table 110 Required group booking permissions for editing conferences

Booking field	Permissions
List Conferences - All	*Read; Update*
List Conferences - Mine	*Read; Update*
Misc	*Booking; New Conference Page*

Time Zone Display

Conferences are listed with the time zone of the currently logged-in user. Viewing or editing a conference displays the time zone that the conference was booked in.

Note that the time zone of a scheduled conference cannot be changed in Cisco TMS.

Search

Table 111 Conference search fields

Field	Description
Find	This free-text field searches the following to return any conferences containing the characters entered: ■ Conference ID ■ Conference title ■ Email address ■ Email message ■ Conference Notes If you type an ID (integers only) here, the search will check conference IDs only. This ID search will ignore dates and any other values set in the **Search** and **Advanced** sections.
Status	Select the status of the conferences you are searching for. Searching on *Conference Request* will display a list of conferences awaiting approval or rejection by the logged-in user.
Start Date	Search for conferences that occur on or after this date.
End Date	Search for conferences that occur up to and including this date.
All users/User	Search for conferences owned by all users or a specific user. This includes conferences booked on behalf of other users.

Advanced

Table 112 Advanced conference search fields

Field	Description
Type	Select one or more conference types to search on.

Table 112 Advanced conference search fields (continued)

Filter	Filter on recorded or defective conferences. A *Defective* conference in Cisco TMS has been booked by an external client that encountered a resource conflict or routing problem. A defective conference retains all properties of the booking request without setting up routing or consuming telepresence resources. Until all issues are resolved, Cisco TMS will not initiate a defective conference or send it to endpoints. ■ In the case of a routing issue, all endpoints in the booking will be set to *Busy* for the scheduled time, keeping the reservation while the administrator or user resolves the issue. ■ In the rare case of an endpoint reservation conflict, the endpoints will not be set to *Busy* for the defective booking. Defective conferences can be corrected by the organizer or the administrator: ■ Users who book conferences that are saved as defective will be notified by email and can resolve most issues by changing their request and rescheduling from their client. ■ Administrators can locate and resolve defective conferences in Cisco TMS by going to **Administrative Tools > Diagnostics > Conference Diagnostics** or **Booking > List Conferences**. Conferences that are defective because of configuration errors or a permanent lack of routing resources must be resolved by an administrator. When scheduling a series where only some occurrences have a resource conflict or routing issue, Cisco TMS will only store the problematic occurrences as defective, leaving the remaining occurrences unaffected.
Filter Systems	Clicking this button displays the **Systems > Navigator** folder list in a popup window. Select the systems to filter on and click **Save** to display a list of all conferences containing those systems.
Save as Default	Save the filters and settings to see these results as default when the page is launched. This search will remain as default until a new one is saved. The settings saved are: ■ Date range relative to now. For example, if your date range spans a 5 day period beginning 2 days before today and ending 3 days after today, and you load the same search on a day next week, the search will span 2 days before the day next week to 3 days after the day next week. ■ User selection. This is only saved if *All Users* or the logged in user is selected. This setting is not saved if you search on another user. ■ **Type** ■ **Filter** ■ **Systems**

Search Results

Hover over the conference title in the search results. Depending on the status of the conference and the permissions set for the logged in user, (see Editing Conferences from This Page, page 186), a drop-down menu will appear with options as described below:

Table 113 Conference drop-down menu options

Menu option	Description
View	View the conference in the View Conference, page 190 page.
Edit	Opens the **Edit Conference** page for the selected conference.
Meeting Details	Opens the **Meeting Information Page** for an ongoing or upcoming meeting. When multiple video addresses are displayed in **Meeting Information Page**, only the first video address can be accessed.
End	End an ongoing conference.
Copy	Copy the conference to create a new booking.
Approve	Approve the conference if it was booked by another user and requires your approval. The user must be a member of a group that has *Approve Meeting* permissions set in **Administrative Tools > User Administration > Groups** for this option to be visible.
Reject	Reject the conference if it was booked by another user and requires your approval. This means the conference will not start. The user must be a member of a group that has *Reject Meeting* permissions set in **Administrative Tools > User Administration > Groups** for this option to be visible.
Create as Template	Create a conference template from this conference for future use. See Conference Templates, page 200.

Note: Only View and Meeting Details are applicable for a non-ongoing Conferencing Connector meeting. Also, View, Meeting Details and End are applicable for an ongoing Conferencing Connector meeting.

Table 114 Buttons on the List Conferences page

Button	Description
Delete	Delete selected meetings. Note that ongoing conferences cannot be deleted and attempting to delete an ongoing conference will end it.
Export Log	Export the list of conferences as a **.xls** file. All conferences that are listed will be included—it is not possible to explicitly select conferences to export.
Export Details Log	The same as **Export Log**, but with these two extra fields: ▪ Participants ▪ Log When a participant/s name is changed in CUCM or in Cisco TMS for a future meeting, then Cisco TMS updates the changed name of the participant of the future meeting in the **Export Details Log** of Cisco TMS. ▪ For CUCM managed participant/s, it may take maximum upto one minute for the updated device name to be reflected in **Export Details Log**. ▪ For TMS managed participant/s, it may take maximum upto four hours for the updated device name to be reflected in **Export Details Log**.
New Conference	Click to be redirected to the New Conference, page 170 page.

Table 115 Conference status icons

Icon	Conference Description
	Active, and all participants are connected
	Active, but no participants are connected
	Active, but only some of the participants are connected
	Finished
	Pending
	Rejected
	Requested, and awaiting approval
	Deleted

Table 116 Reservation status icons

Icon	Reservation Description
	Active
	Finished
	Pending
	Rejected
	Requested, and awaiting approval

External Service

Webex column has been replaced as **External Service** in Cisco TMS **List Conference** page. External Service column displays the following information based on the type of external service involved in the meeting.

Table 117 External Service information

Type of Meeting	External Service
Meeting booked by Calendar Connector application.	Calendar Connector
Meeting not booked by Calendar Connector application and Webex is involved in the conference.	CMR Hybrid Webex
Meeting not booked by Calendar Connector application and Webex is not involved in the conference.	Blank

View Conference

In Cisco TMS: **Booking > List Conferences > select conference view**

In **List Conferences**, hover over a conference and select view to see settings, participants, conference information and logs for this specific conference.

Note that to be able to view and edit bookings from this page, the user must have permissions to see their own conferences set in **Administrative Tools > User Administration > Groups**, see Groups, page 267.

See New Conference, page 170 for descriptions of most of the fields, settings, and tabs available on this page.

Event Log

An **Event Log** tab is available in the lower tabbed area of the conference page when editing or viewing a conference. For more information, see Conference Event Log, page 207.

List References

In Cisco TMS: **Booking > List References**

A reference is information which can be associated with one or more conferences. A reference can include a reference name, reference code, a comment and contact information. It can be used whenever a conference needs to be associated with a specific code/name/other info.

This page shows all the references that have been created and saved in Cisco TMS.

Conferences and References

Conferences can be associated with a reference by choosing them in the **Conference Information** tab while booking conferences in the **New Conference** page. A conference can only be associated with one reference. References can be created without any connection to booked conferences.

Creating a Reference

To create a new reference:

1. Click **New**.
2. Fill in the necessary information.
3. Click **OK**.

Deleting References

To delete references:

1. Select the check boxes next to the references you want to delete.
2. Click **Delete**.

Sorting References

Click **Reference Code** or **Reference Name** at the top of the list to change the sorting of the reference list. By default, they will be sorted ascending by code.

Searching for References

Type in the **Query Search References** field and click **Search**. Every reference that matches the word or contains the search term in the **Reference Code** or **Reference Name** fields will be listed.

Ad Hoc Booking

In Cisco TMS: **Booking > Ad Hoc Booking**

The **Ad Hoc Booking** page allows you to launch calls quickly by choosing currently available systems. You can also schedule future conferences on this page.

Availability information is not displayed for conferences not booked with Cisco TMS.

Displaying Systems

You can select which systems to display on this page by clicking **Filter on Folders** to show all the folders and systems in Cisco TMS, and selecting the check boxes next to each folder.

Note: To view MCUs and TelePresence Server on this page, go to **Administrative Tools > Configuration > Conference Settings** and set **Show Network Products in Ad Hoc Booking** to *Yes*.

To define how much system information is displayed on the page:

1. Click **Select Fields** to launch the **Select Fields** pop-up window.
2. Select the parameters you want to be visible.
3. Click **Save**.

Checking Availability and Reserving Systems

To set up an automatic call or reserve systems from Cisco TMS:

1. Specify the **Start Date**, **End Date**, **Start Time** and **End Time**.
   Leaving these fields as default will launch the call immediately.
2. Click **Search** to check availability during the specified period.
3. Select the check boxes next to the systems you want to use.
4. Now either:
   a. Click **Automatic Call Launch** to start a conference at the specified start time.
   b. Click **Reservation Only** to reserve the systems for the same period.
5. Your reservations will be shown in green, while reservations by other users will be shown in red.

Booking on Behalf of Someone Else

By default, bookings are made under the logged in user's account.

To make a reservation or launch an automated call on behalf of someone else:

1. In the **Book For** field, click on the user selector icon next to your name
2. Select the other person from the list.

You can also search for the user:

1. Type the user's name into the **Filter users by name** field.
2. Click **Search**.
3. In the search results, click on the name of the person you wish to book on behalf of.

Entering a Billing Code

To apply a billing code to a conference during booking, enter a billing code in the **Billing Code** field.

The search does not use this field.

Participant Templates

In Cisco TMS: **Booking > Participant Templates**

Participant templates are saved sets of connection settings that can be created to represent a single participant, or a type of participant that uses a specific connection settings.

Notes:

- Cisco TMS does not allow users to create **Participant Templates** with TelePresence Conductor or Cisco Meeting Server. However, preconfigured **Participant Templates** of endpoints can be used with TelePresence Conductor or Cisco Meeting Server while scheduling a meeting.
- Cisco TMS endpoints can handle maximum bandwidth upto 6000 kbps and Cisco Meeting Server conference bandwidth supports maximum upto 6144 kbps. Hence in Participant Templates bandwidth , the selection has to be based upon the appropriate bandwidth supported by the endpoints. Endpoints cannot handle Cisco Meeting Server Conference Bandwidth.
- When you are using participant templates, bandwidth settings of the endpoints should not be set more than maximum supported bandwidth of endpoint. Call may fail if the correct bandwidth is not selected.
  Example: Maximum bandwidth for DX70/ DX80 endpoint is 3072.

Why Use Participant Templates

The main uses for participant templates are:

- Saving a participant with customized dial settings as a template for easy reuse in booking, instead of manually configuring them for each booking.
- Setting specialized parameters that are not available in the Cisco TMS booking page.

  Examples include serially connected bridge ports and bridge participants that can only connect through a specific network interface.

  Once created, a participant template can be added to a conference like any other participant.

Note that participant templates are only available when booking directly in Cisco TMS, they cannot be used with Smart Scheduler, Cisco TMSXE, or any other application using Cisco TelePresence Management Suite Extension Booking API.

Customized Participants

When adding a participant to a conference, Cisco TMS calculates the best way to call that participant based on the conference settings and the information available to Cisco TMS about the participant.

Should the organizer booking a meeting need to add additional information, or override the default call settings like the dial direction or the number to be dialed for the participant, these settings can be

- modified on a per-conference/per-participant basis using the **Connection Settings** tab
- specified once and reused as many times as needed by creating a participant template

Templates can represent endpoints controlled by Cisco TMS or external participants. For examples of how participant templates might be used for customized participants, see examples 1-3 in Sample Participant Template Setups, page 198.

Special Use Participants

Booking some participant types or scenarios require additional parameters that are not available for editing in the Cisco TMS booking pages, such as:

- Having a participant use a specific dial-in number.
- Booking direct connected leased line endpoints
- Using the dynamic dial-in number features of the legacy Cisco TelePresence MPS bridge

Note that these special uses are not supported on all device types, and most are specific features for the Cisco TelePresence MPS series of bridges.

For examples of how participant templates might be used to define special use participants, see examples 4-5 in Sample Participant Template Setups, page 198.

Creating a Participant Template

Note that the available settings change as you make selections, and that not all visible settings apply to all systems.

1. Go to **Booking > Participant Templates** and click **New**.

2. Specify the **Dial Settings** as described in the table below.

Table 118 Dial settings for participant templates

Field	Description
Name	Specify a name for the template. This name will represent the template when used in bookings.
Reusable	This setting is disabled by default. Cisco TMS then treats the participant as any other system and performs an availability check during booking that prevents the template from being double booked. Enabling this setting disables the scheduling availability check for the template. This allows the same template to be used multiple times in the same conference or in overlapping conferences. For example, if using a template to define a class of external dial-in participants that require the use of a specific bridge, enable this setting. **Note**: When a participant template is created using Cisco Meeting Server , then the '**Reusable**' option will not work for Dialouts. **Workaround**: In **Cisco TMS>Participant Template>Number Settings**, after the telephone number add "**-**" followed by the name of the end user as the unique sequence. The name part of the sequence should be removed in the Search rules of Call Manager.
Protocol	Specify the call protocol to use for this participant: – *ISDN – H320* – a H.320 system reachable via ISDN – *IP – H323* – a H.323 system reachable via IP – *IP – SIP* – a SIP participant reachable via IP – *V.35* – a participant connected via a V.35 Serial interface on an MPS bridge – *G.703* – a participant connected via a leased-line interface on an MPS bridge – *IP* – a participant using IP Address direct dialing into a Cisco TelePresence MCU bridge – *ISDN – H221* – a system reachable by ISDN that does not support bonding and requires both ISDN numbers be supplied. Requires the system to support H.221 dialing
Type	– *Audio*: Audio only—specifies a telephone call. – *Video*: Both audio and video.
Call Restrict	Specify whether ISDN restricted (Nx56kbs) rates will be used with this call.
Endpoint	Associate a Cisco TMS-controlled endpoint with this template. The endpoint will be booked with the template's parameters when the template is booked. When no endpoint is specified, the booked participant will be treated as an external participant.

Table 118 Dial settings for participant templates (continued)

Field	Description
Direction	– *Dial Out*: The main participant will dial out to the participant at conference start time using the specified connection settings and commands. The main participant is an MCU, TelePresence Server, or endpoint with multisite capabilities, see The Main Participant, page 32. – *Dial In*: The main participant uses the template's setting to reserve resources for the system to dial in to the conference at the scheduled time.
Bandwidth	The bandwidth to allocate for the participant can be fixed, or set to *Conference Bandwidth* to follow the overall conference setting.
Number	The number or alias to be dialed for this participant. This field will go through the regular Cisco TMS routing logic, which means ISDN numbers must be in their fully qualified format. To force Cisco TMS to use the number provided as-is, enclose the number in square brackets.
Extension Number	Specify an extension number to add to the dialed number if required, such as a TCS-4 string.
Second Number	Used when the protocol is set to *ISDN - H.221* and the direction is *Dial Out*. Enter the second ISDN number to be dialed. This field will go through the regular Cisco TMS routing logic, which means ISDN numbers must be in their fully qualified format. To force Cisco TMS to use the number provided as-is, enclose the number in square brackets.
DTMF Tones	Enter the string of DTMF digits to be sent after a call has connected, if needed. A DTMF sequence is used for dialing systems with keypad/tone navigation menus, such as an audio bridge. The sequence may contain the digits 0-9, the star/asterisk character (*), the hash/pound character (#), and the comma character (,). Note: This feature is available only for Cisco Meeting Server 2.4.
MCU	If set, the selected bridge will be included in the conference when this participant is booked. If left as *Not Selected*, the default Cisco TMS routing logic is used to select the main participant. Note that this field must be set if using functionalities that require a specific bridge for the participant, such as V.35, G.703, specific ISDN network, or MPS-specific dial-in methods.
MCU Number	Only applicable when the selected bridge is Cisco TelePresence MPS. Specify which existing meeting alias on the MCU to use when this template is booked. If this field is left blank, the default Cisco TMS routing logic is used to determine the conference alias.
MCU Interface	Only applicable when the selected bridge is Cisco TelePresence MPS. Specify which MCU interface to use to connect to the system. The protocol can be V.35, G.703, ISDN, or IP - H.323.

Table 118 Dial settings for participant templates (continued)

Field	Description
Dial In Method	Specify the method for assigning the dial-in number a participant will be assigned: – *Conference Number*: The template will use the common conference number and will not get a unique number to dial. If the selected bridge is not Cisco TelePresence MPS, this is the only valid option. – *Participant Number per Conference*: Only applicable when the selected bridge is Cisco TelePresence MPS. The participant will have a unique dial-in number for the conference, and the number may change each time the template is scheduled. – *Participant Number Fixed*: Only applicable when the selected bridge is Cisco TelePresence MPS. The participant is assigned a unique dial-in number for the conference, which is used each time the template is scheduled.
Caller ID	Only applicable when the selected bridge is Cisco TelePresence MPS. Enter the number the calling participant will be seen as by the bridge when receiving the call. **Protect** must be set to *On* for the conference for this field to be valid, causing only participants whose caller ID match the predefined list to be allowed to join. The **Protect** setting can be configured: – in the MPS interface (**Overview > MCU > Create Conference**). – on the conference in Cisco TMS after the MPS has been added, on the **MCU Settings** tab. – in the MCU defaults for the system in **Navigator**.
ISDN Zone	Set ISDN and IP zones for the template. These fields are not applicable if an endpoint is specified in the template. For further details, see Locations, page 278.
IP Zone	

3. If desired, go to the **Identification** tab, write a description of the template and associate it with a reference; see List References, page 191 for more information.

Adding a Participant Template to a Booking

When creating or modifying a booking:

1. Click **Add Participants**.
2. Click on the **Templates** tab.
3. Select the participant template or templates to add.
4. Click **OK**.

With any booking involving dial-in participants, make sure the required dial-in information is distributed to all participants.

Sample Participant Template Setups

Example 1: Third-party audio bridge

You frequently have to call a third-party telephone audio bridge as part of your scheduled calls that requires you to dial a set DTMF string when you connect.

Template solution:

- **Protocol**: *ISDN – H320*
- **Type**: *Audio*
- **Direction**: Dial-Out
- **Number**: The telephone number of the bridge
- **DTMF**: All digits to dial upon connection

Whenever this template is scheduled, an external ISDN dial out will be added to the conference with the number and DTMF fields already populated.

Example 2: Special network access

You frequently need to setup a call for the CEO's office system where you must use a specific bridge for the call because only that bridge has the special network access needed for the call.

Template solution:

- **Endpoint**: Set to the CEO's office system
- Specify the call protocol
- **MCU**: The specific bridge desired

Whenever this template is scheduled, the CEO's system and the selected bridge will be added to the conference, forcing the conference to use that bridge.

Example 3: Lower bandwidth to reduce cost

Your default conference bandwidth is 1024kbps, but to keep costs down when calling the Singapore office, you want the participant bandwidth for that single participant to be 384kbs when you schedule it for the monthly manager's meeting.

Template solution:

- Specify the desired protocol and call direction
- **Bandwidth**: 384kbps
- Endpoint: Set the Singapore office system

Whenever this template is scheduled, the Singapore system will be included in the booking, and the bandwidth for that participant alone will be set to 384kbps.

Example 4: Connection to a particular ISDN interface

You have a Cisco TelePresence MPS bridge with ISDN interfaces connected to both public and private ISDN networks and need to define a dial-out participant that can only be connected to via the specific private ISDN network connected to your MPS.

Template solution:

- **MCU**: Set the specific MPS bridge
- Specify the ISDN port where the private network is connected to the bridge

Whenever this template is scheduled, MPS will be added to the call, and Cisco TMS will modify the dial string provided to MPS to use the selected interface.

Example 5: Direct connected endpoint via V.35

You have a Cisco TelePresence MPS bridge with direct connected endpoints via a V.35 network interface that you wish to schedule within meetings.

Template solution:

- **Protocol**: *V.35*
- Selecting the MCU and interface where the participant is connected
- Create one template for each direct connected endpoint

Whenever such a template is scheduled, the specified MPS bridge will be added as the bridge for the meeting, and the participant will be connected and represented for the specified V.35 interface on the bridge.

Conference Templates

In Cisco TMS: **Booking > Conference Templates**

If you create conferences using the same settings and participants on a regular basis, you can input these settings into a conference template and use this instead of starting from scratch to save time.

To create a new template:

1. Click **New**
2. Enter the basic and advanced settings for the conference
3. Add participants
4. Click **Save Template**

Note that TelePresence Conductor is not supported on **Conference Template**.

Editing and Using a Conference Template

1. Hover over the name of the template you want to use and choose **Use as Conference** from the drop down menu.
   A **New Conference** page will appear pre-populated with the settings from your conference template.
2. Make any changes that you want to and specify the start and end time of the conference.
3. Click **Save**.

Monitoring

This chapter describes the **Conference Control Center**, which is used to monitor and edit conferences in Cisco TMS, and also the **Graphical Monitor**, which provides a visual interpretation of your video network. Also included are related tasks and reference material for these menu items.

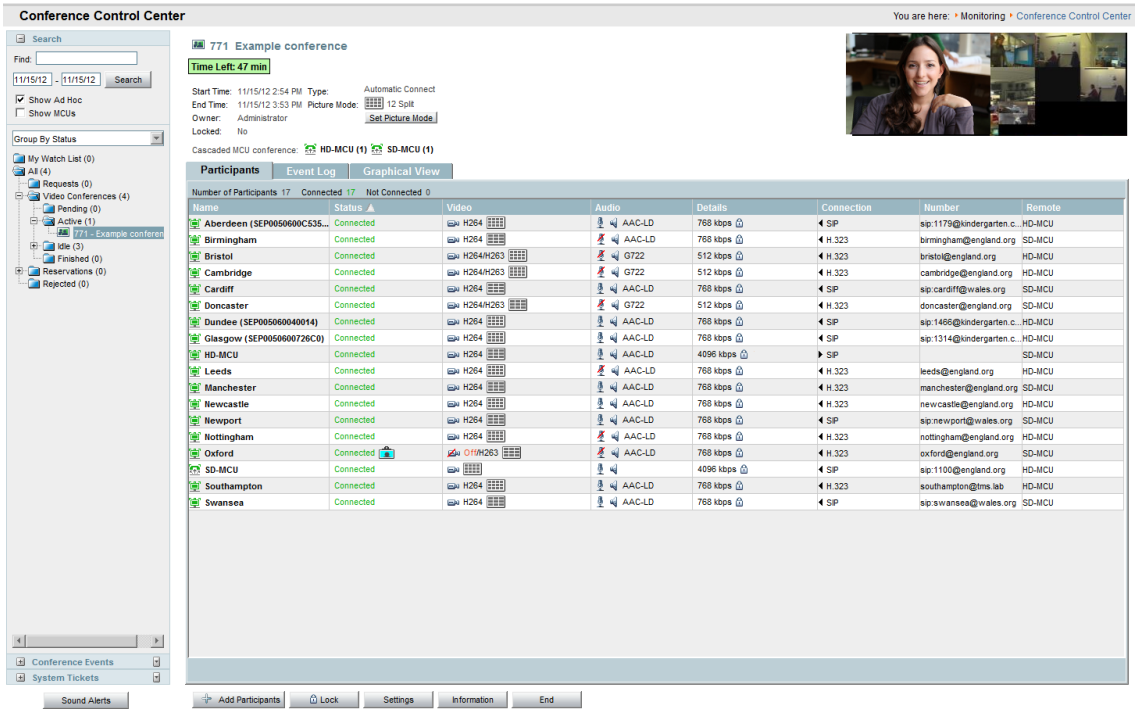
The monitoring tools require that Java Runtime Environment is installed on each client computer. To install or upgrade Java, go to www.java.com.

Monitoring and Managing Conferences 201
Operator Conferences 202
Conference Control Center 203
Graphical Monitor 208

Monitoring and Managing Conferences

Conference Control Center

The **Conference Control Center** (CCC) is a dashboard-like interface that allows you to monitor the status of the conferences running on the network and if required, control and interact with the systems in the conference.



Here you can also create operator conferences: ad hoc conferences that allow conference operators to work with individual participants in a conference outside the conference they are participating in.

This means that if a site is having a problem or has questions, an operator can start a new conference and add themselves and the problem site(s) to the special conference. Once this conference is over, the operator can send the site back to their originally scheduled call.

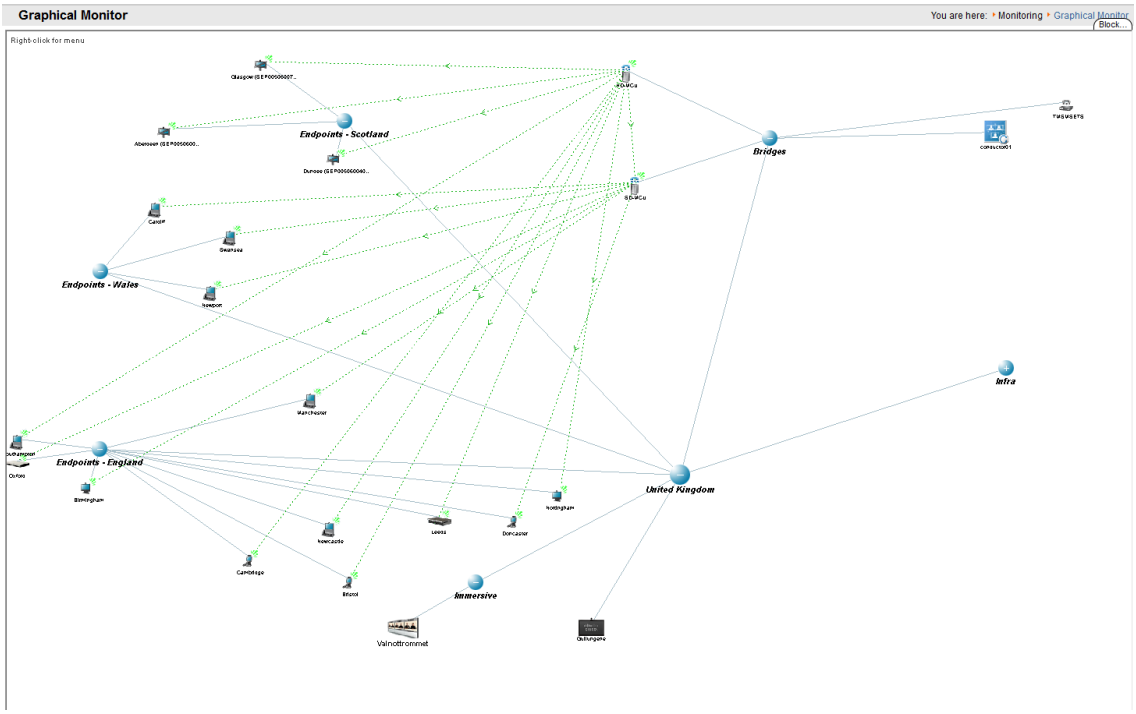
For more information, see Operator Conferences, page 202 .

Notes:

1. If a point to point conference is escalated onto a bridge on the fly, information in CCC will no longer be correct - you may see duplicate conference information.
2. If an ongoing conference is created from CCC page and is not answered, then Cisco TMS does not redial the conference. However, when a future conference is created from CCC page and is not answered, Cisco TMS redials the conference.
3. When the call is in ringing state and disconnected from CCC or Bridge it triggers reconnect of the call.

Graphical Monitor

The **Graphical Monitor** is an interactive live map of your conferencing network. Using animation and colors, it shows a live view of your network including active calls, and systems that are unreachable. The view is based on the folder structure set up in the System Navigator.



Operator Conferences

Operator conferences are ad hoc conferences that can be used by conference operators to work with individual participants in a conference outside their normally scheduled call.

If a site is experiencing a problem or has questions, an operator can start a new conference and add themselves and the problem site(s) to this conference. When the problem has been resolved, or the question answered, the operator can put the participant back in their original conference again.

- Operator conferences can be created on the fly with a single click.
- You can click on participants to move them to an operator conference without disconnecting the site.

- If no operator conference exists, a new one can be created automatically.
- Operators can have a default system for themselves that can be automatically added to the conference when an operator conference is started.
- Operators can move a participant or multiple participants in and out of an operator conference as they wish from the Conference Control Center.
- Multiple operator conferences can run simultaneously.
- Participants moved to an operator conference are still shown as participants in the scheduled meeting, but with special icons to signal that they have been moved.
- Operator conferences will automatically clear themselves out if no longer used by the operator's system.

Creating an Operator Conference

There are two ways to create an operator conference:

1. Select the **Show MCUs** check box in the upper right corner of the screen, then right-click on an MPS or MCU and select **Create Operator Conference**
2. Right-click on a participant in a conference with an MPS or MCU as the main system and select **Move to Operator**.

Participant(s) moved to an operator conference are marked as moved in the original conference.

Note: The participant will only be moved out of their original conference when the operator is successfully connected to the operator conference, eliminating the possibility of the participant being moved into an empty conference.

The participant(s) can be moved back by right-clicking on the participant either in the original or in the operator conference and select **Move back**. If the operator conference is ended with participants in it, the participant(s) are automatically moved back to their conference.

The operator conference is auto-extended, and it can be ended either explicitly from **Conference Control Center** or by just disconnecting the operator's endpoint.

If the original conference is ended while participant(s) are moved out from the conference, the operator will be notified by a warning event in CCC. When the original conference is ended, moved participants will behave as ad hoc participants and not moved participants in the operator conference.

Even though a participant is moved out from a conference, messages from the original conference will still be sent to the participant's endpoint.

Note: Participants sending dual video stream or cascaded conferences can not be moved out from a conference.

Conference Control Center

In Cisco TMS: **Monitoring > Conference Control Center**

The **Conference Control Center** (CCC) is a tool for managing and monitoring all conferences booked in Cisco TMS or through an extension using Cisco TelePresence Management Suite Extension Booking API, including Cisco TMSXE and Smart Scheduler, and conferences scheduled directly on conference bridges.

Enabling Ad Hoc Conference Monitoring

Conference Control Center can also monitor calls on your network that have not been scheduled through Cisco TMS).

Caution: This monitoring is highly resource intensive and may considerably slow down the Cisco TMS **server in a large deployment.**

To enable the monitoring of ad hoc calls:

1. Go to **Administrative Tools > Configuration > Network Settings**.
2. Set **Enable ad hoc conference discovery** to *Yes*
3. Check **Show Ad Hoc** in the search area of the CCC page.

Finding and Displaying Conferences

The folder view on the left side of the screen shows a list of all the meetings booked and registered in Cisco TMS.

The **Search** area lets you narrow, expand, and sort the displayed list of conferences:

- Enter a number in the **Find** field to make CCC search in conference IDs.
- Search in text format to look for conferences with titles or participants that match the search string.
- Check **Show Ad Hoc** to include ad hoc calls if you have already enabled ad hoc conference monitoring.

Use the *Group By...* dropdown menu to sort the conferences by current state, date, owner, or MCUs:

- Conferences with no connected participants are placed in the **Idle** folder.
- Conferences where the main participant is not a conference bridge or TelePresence Conductor are placed in the **Other** folder.
- Right-clicking a folder allows you to **Set as Default Start Folder** for Conference Control Center. Note that custom folders (grouped by date, user, and so on) cannot be used as the start folder.
- Right-click a conference to **Add to Watch List** or **Remove from Watch List**.
- Select a conference from inside this folder view to display its properties in the main pane. You can also right-click a conference to get the option to **Open in New Window**.

Monitoring and Managing Conferences

For each ongoing conference, snapshots from the conference and presentation will be displayed if available.

Table 119 Available actions for conferences depend on their status..

Button	Description
Set Picture Mode	In the conference information near the top of the screen, set the picture mode for the conference based on what is available on the conference bridge.
Add Participants	Adding participants works the same as when booking from New Conference, see Add Participants Window, page 174.
Lock/Unlock	Locking a conference makes the conference bridge disallow more participants from dialing in. An administrator can still add participants through Cisco TMS.
Settings	Opens conference settings, see New Conference, page 170.
Accept	Accept or reject the conference, if booked by a user that cannot approve bookings.
Reject	
End	Ends the ongoing conference. This is not available for permanent conferences scheduled directly on conference bridges.

Managing Participants

A **Participants** tab is available for each conference.

Different buttons/commands for participants will be displayed depending on the functionality available on each system. Tooltips are available for each button when hovering. Actions are also available when right-clicking each participant.

Table 120 Actions for participants in CCC

Icon	Name	Description
	**View Details**	Open a separate window with the system's **Navigator** page.
	**View Web**	Shows you the web interface of the system.
	**Mute Audio**	Mute/unmute the participant from the bridge. (Only available for Multipoint calls).
	**Unmute Audio**	
	**Microphone On/Off**	Mute or unmute the participant's microphone in this conference. Note: For conferences involving a bridge, the Microphone On/Off status may not be accurately reflected, as not all call scenarios allow the bridge to accurately report if the participant is remotely muted. This limitation is based on the limitations of the bridge and participant types involved.
	**Set Floor**	Give the floor to the selected participant and release it.
	**Release Floor**	
	**Set Important**	Set this participant as the focused participant. For example, this participant will be considered the loudest participant in the conference even if they are not speaking.
	**Remove Important**	Cancel the **Set Important** setting.
	**Disconnect**	Disconnect the selected participant.
	**Send Message**	Send a message to the participant. Depending on the main participant, the message may be displayed on the video screen or the system's touch-screen panel.
	**Remove**	Remove the selected participant from the conference.
	**Connect**	Connect the selected participant.
	**Connect All**	Connect all participants (only available from the main participant).
	**Cancel Connect**	Cancel the connection to the selected participant.
	**Disconnect All**	Disconnect all participants in the conference (only available from the main participant).
	**Mute Outgoing Audio**	Mute and unmute outgoing audio to this participant.
	**Unmute Outgoing Audio**	

Table 120 Actions for participants in CCC (continued)

Icon	Name	Description
	**Mute Video**	Mute and unmute video for this participant.
	**Unmute Video**	
	**Status Duo Video**	Hover to see content stream information for MCUs in conferences. This is not available for all MCUs and software versions.
	**Block FUR**	Block and unblock fast update requests from remote participant. Applies to the legacy Cisco TelePresence MPS only.
	**Unblock FUR**	
	**Change Display Name**	Change the participant's display name.
	**Show Snapshot**	Show snapshots for this participant.
	**Contact Information**	This information is collected from the **System Contact** field in **Systems > Navigator >** select system **Settings > General**.
	**Move to operator conference**	Move the participant from the current conference to an operator conference, see Operator Conferences, page 202.
	**Move Back**	Moves the participant back to the original conference.
	**Dial Settings**	Show connection settings for this participant.
	**Get Back**	You can drag-and-drop participants from one conference to another on the same MCU. Select the participant and click the **Get Back** button to bring the participant back to the original conference. This functionality is only available with Cisco TelePresence MCU Series and the legacy Cisco TelePresence MPS.
	Layout drop-down menu	Change the layout of the receiving video for this participant. Only available for some conference bridges and software verisons.
	+participant name	If an MCU is used in a conference, click the button **+participant name** directly above the action buttons to display transmit and receive statistics for video and audio for this system. When applicable, content stream information will also be displayed.

Viewing connections

To see the connections in an ongoing or finished conference, open the **Graphical View** tab for the conference.

- Arrows on the lines indicate call direction.
- Colors indicate connection status.

You can perform the same commands on participants in this view as on the **Participants** tab, but you can only select one participant.

Viewing Conference Events

Each conference has an **Event Log** tab. For more information about this, see Conference Event Log, page 207.

In **Conference Events** in the left-hand panel, events from all pending and active conferences are shown:

- Right-click on events to acknowledge or clear the event, or open the affected conference.
- Click the drop-down icon in the **Conference Events** header and select **My Conferences List** to display only events from conferences on your watch list.

Conference events are indicated in the folder view, in the conference list, and in the conference details if the event is tied to a participant.

Viewing System Tickets

The **System Tickets** area in the left-hand panel contains tickets from relevant systems. A detailed list and display options are available from the drop-down icon on the **System Tickets** header.

Controlling Sound Alerts

Click **Sound Alerts** to configure alerts for errors and other events in active and/or opened conferences.

Sound alert settings are stored per user.

Conference Event Log

To see an audit trail of changes to a booking, or connection issues in an ongoing conference, look at the conference event log. This log can be found in two places in Cisco TMS:

- when viewing or editing an already booked conference, on the **Event Log** tab in the lower half of the screen.
- on the **Event Log** tab for each conference in **Conference Control Center** (CCC).

The log lists all changes to the conference since it was booked. The contents of the logs are identical in the two locations, but CCC includes additional options for running diagnostics and opening the list as text.

Reading the Log

In CCC you will always read the event log on an instance basis. In **List Conferences**, to view the event log for the series you need to edit the series rather than the instance. Note that an instance's Event Log always contains both the series' events and the instance's events.

The Event Log identifies whether changes were made to conferences series or single instances by using the prefixes: 'Conference' or 'Instance' in log entries.

The log includes a timestamp, the user that made the change, and details of any changes to:

- start and end time
- conference type
- recurrence pattern
- Webex included in the conference of not
- picture mode
- participants. Adding or removing a recording alias will be logged as (recording) participant added or removed

For the user field, note that any changed performed through Cisco TMSBA will be logged as originating from the service user.

The user **nt authority\network service** indicates automatic actions taken or initiated by Cisco TMS, such as:

- dial attempts from the main participant
- automatic messages sent to participants
- automatic extensions to the meeting

During the conference, the following will also be logged:

- participants connecting and disconnecting, including ad hoc participants
- actions performed through **Conference Control Center**, including muting of participants and messages sent to participants

For changes not mentioned above, the log will generally state "Conference updated".

All changes to ongoing conferences will be logged on an instance level.

Conference Registration and Diagnostics

The message "Conference registered" will be logged 15 minutes prior to the scheduled start time, when the conference is handed over from schedulerservice to liveservice (see Windows Services, page 19 for more detail on these).

At the same time, or at booking time if the start time is less than 15 minutes and more than one minute ahead in time, Cisco TMS runs diagnostics on the conference. The diagnostics service checks all systems for system tickets that can affect confernece setup, checks that the routed calls are still valid call alternatives, and whether dial in numbers exist. Any problems discovered during this check will create an event in the event log.

When viewing the event log in CCC, this diagnostic check can also be run manually by clicking **Run Diagnostics**.

Creating Exceptions and Recreating Conferences

The log captures whether an instance is an exception, or no longer an exception, and the number of exceptions in a series.

If the person updating a conference series chooses to overwrite all exceptions in a series, or a change is made to a series while an instance is ongoing, the old instances will be deleted and new instances with new conference IDs will be created.

The event log for the new instances will say "Conference recreated", and log messages from before series recreation will only be available on the deleted instances.

Graphical Monitor

In Cisco TMS: **Monitoring > Graphical Monitor**

This page provides powerful features for monitoring a network of conferencing systems and infrastructure.

View Folders and Systems

What is displayed here reflects a visual representation of your **System > Navigator** folder structure. Folders can be opened or closed by double-clicking on the icons or by right clicking on the folder and selecting **Open**, **Open All** or **Close**.

Systems can be displayed and zoomed in on by clicking directly on the icon representing the system. By right clicking in an empty space on the **Graphical Monitor** page, a menu is displayed:

Arrange

Automatically arrange the position of the folders and systems for the best fit in the graphical monitor.

Expand All

Expand and display all sub-folders.

Show Control Panel

Choose between different presentation options. Moving the **Zoom** slide bar, the size of the picture can be increased or made smaller. Checking **In Call** will display only systems that are in a call, whereas checking **No Response** will show only systems that are turned off, not connected to the network, or have some kind of network problem.

Select **Idle / Alive** to display only systems that are alive or idle.

Options

Table 121 Graphical Monitor user settings

Field	Description
User Arrange	Allows the user to arrange icons freely by clicking and dragging them.
Locked	Locks the positions of the icons.
Auto Arrange	Automatically arrange the folders and systems in the graphical monitor.
Show name	The system names will be shown next to each system.
Show Network Address	The system IP addresses will be shown for each system.
Visible Characters	Choose how many characters will be displayed for each system.
Font Size	■ *Small* ■ *Normal* ■ *Large*
Label Color	Label text coloring options for each system. ■ *Dark Gray* ■ *Blue* ■ *Orange*
Update Frequency	Define the update rate of the graphical monitor in seconds, when checking system status of each system. Choose within an interval from one to sixty seconds.
Animation	Define the speed of the animation of systems in call, and when opening and closing folders. Choose between: ■ *Fast* ■ *Normal* ■ *Slow*
Show Call Animation	Enable/disable the animation of the systems in a call. Note that having animations enabled requires more resources from the Cisco TMS client.
Show Call Lines	Enable/disable the lines drawn between systems registered in Cisco TMS that are in a call together.
Rotate when moving folder	When un-checking this check box you will be able to move the child-nodes in the tree without rotating or rearranging the systems in the node.

Creating and Managing Phone Books

This chapter covers core phone book concepts and describes the creation and management of phone books and their sources in Cisco TMS.

The chapter also includes reference material for all entries in the **Phone Books** menu.

Phone Book Basics 210
Phone Book Types 211
Creating a Phone Book 212
Granting Access to Phone Books 213
Setting Phone Books on Systems 214
Exporting Contacts to a File 214
Manage Phone Books 215
Manage Phone Book Sources 216
Phone Book and Source Activity Status 224
Phonebook for Cisco Meeting Management 224

Phone Book Basics

The Role of Phone Book Sources

Phone books in Cisco TMS are containers for one or more phone book sources. The phone book source supplies a list of contacts that are made available to endpoints through phone books. Multiple sources connected to one phone book will be merged together.

A multitude of different source types are supported, including Active Directory users and Unified CM users. For an extensive list with descriptions and configuration options, see Manage Phone Book Sources, page 216.

Hierarchical Phone Books

Phone book sources are always imported as flat lists of contacts. However, phone books may contain other phone books in a hierarchical structure based on, for example, geography or organizational structure.

All or parts of the hierarchical phone book may then be set on the different systems. Any phone books below the specified level will be included recursively, while parent phone books will be excluded.

Note that hierarchical phone books are not supported by the legacy global directory phone book format.

For instructions on setting up such a structure, see Creating a Phone Book Hierarchy, page 213.

Default Source and Phone Book

As part of the default installation, Cisco TMS creates a simple phone book that contains all the systems that are managed by Cisco TMS and assigns it to all systems automatically discovered by Cisco TMS.

Phone Book Routing

In **Administrative Tools > Configuration > General Settings**, there is a setting called **Route Phone Book Entries**.

- *Yes* is the default setting, which means that endpoints will only display addresses that they are capable of dialling. For example, on an H.323-only endpoint, ISDN numbers and SIP addresses will not be displayed.
- *No* means that the endpoints will display all addresses and numbers in the phone book regardless of their dialling capabilities.

Note that enabling this setting causes additional server load and may lead to slower phone book searches for users.

For more information on routing, for example how numbers are displayed in phone books, see Routing, page 31.

Phone Book Types

Depending on the endpoint type, up to three different phone book types may be available to endpoints, two of which are managed by Cisco TMS.

Corporate Directory

Most Cisco endpoints rely on this live XML search service on the Cisco TMS server.

Corporate Directory settings will be modified on supported systems:

- Every time a change is done to the **Set on system** list. See Setting Phone Books on Systems, page 214.
- By a background service that by default will run every four hours if enabled. To enable this background service:
  a. Go to **Administrative Tools > Configuration > Network Settings**.
  b. In the **TMS Services** section, set **Enforce Management Settings on Systems** to *Yes*.
  c. Click **Save**.

Corporate directories can be flat or have a hierarchical structure.

Global Directory

Legacy TANDBERG MXP endpoints may also use Global Directory, an HTTP-transmitted file that merges multiple phone books into one and displays a maximum of 400 contacts.

The directory (the **globdir.prm** file) is transmitted to the endpoint over HTTP at two different events:

- Every time a change is done to the **Set on system** list. See Setting Phone Books on Systems, page 214.
- At the intervals specified in **Phone Book Update Frequency**. See General Settings, page 234.

Global directory phone books always have a flat structure.

Local Directory

Endpoints usually have some contact entries entered directly on the endpoint itself, referred to as a local directory, phone book, contacts, or favorites. These are not managed by Cisco TMS. However, a local directory can be imported as a phone book source, see Manage Phone Book Sources, page 216.

You can also view the local directory in Cisco TMS:

1. Go to **Systems > Navigator** and locate the system.
2. Click on the **Phone Book** tab.

Setting the Phone Book Type For All Systems

To set which type of phone book will be used:

1. Go to **Administrative Tools > Configuration > General Settings**.
2. In the **General Settings** section, set **Cisco System Phone Books** to one of the following:
   - *Use centralized TMS phone books only (corporate phone book)*
   - *Use both centralized and downloaded phone books (both)*
   - *Use global phone books downloaded to systems only (global phone book)*

   We recommend opting for *corporate phone book* or *both*, as the downloaded phone book is only supported by legacy TANDBERG endpoints.

   The default setting is *both*, which will make the global directory available should the corporate directory live search fail.
3. Click **Save**.

Creating a Phone Book

To create a phone book in Cisco TMS, you need one or more phone book sources. You can use an existing source as is, configure an existing source, or set up a new one. The procedure below includes the creation of a new phone book source:

1. Go to **Phone Books > Manage Phone Book Sources**.
2. Click **New**.
3. Select a phone book source type from the drop-down.
   See Manage Phone Book Sources, page 216 for a reference to source types.
4. Enter a name for the new source.
   Note: The phone book name must not contain special characters like "%", "&", "@" and ":"
5. Click **Save**.
   Configuration fields will appear on the lower half of the screen, depending on the type of source you selected.
6. Fill in the required fields.
   See Manage Phone Book Sources, page 216 for a reference to configuration fields and options.
7. Click **Save**.
8. Set the **Update Frequency** for the new source by selecting from the drop-down list.
   Repeat the above steps for as many sources as you want included in the phone book.
9. Go to **Phone Books > Manage Phone Books**.
10. Click **New**.
11. Enter a name for the new phone book.
12. Click **Save**.
    A new section with three tabs will appear on the lower half of the screen.
13. Click **Connect**.
    A list of all available phone book sources appears.
14. Use the checkboxes to select one or more sources for the phone book.
    You can combine as many sources as you want.
15. Configure the **Update Type** for each of the sources you want to include. This does not apply to the *Manual List* source type.
    - *Import to TMS*
    - *Search only*: Note that you cannot schedule entries from phone book sources with this type, and that these sources will be filtered out from the **Phone Books** tab that appears when adding participants to conferences.
16. Click **OK**.

The phone book has now been created. To make it available to Cisco TMS-controlled systems, you must:

1. Set up access control, see Granting Access to Phone Books, page 213.
2. Set phone books on the systems, see Setting Phone Books on Systems, page 214.

Creating a Phone Book Hierarchy

For ease of distribution and browsing, you may want to create a hierarchy of phone books.

Restructuring hierarchical phone books, once they are created, is not supported. We therefore strongly recommend to plan the phone book structure out in detail before creating it in Cisco TMS.

To create a phone book inside of another phone book:

1. In **Phone Books > Manage Phone Books**, open or create the phone book you want to be the top level container for your hierarchy.
2. While the top level phone book is open, click **New** to create a new phone book inside it.
3. Create as many nested phone books inside the top-level phone book as you need, making sure to always create each new phone book from the appropriate parent in the structure.

All levels of the phone book hierarchy may, but do not need to, be connected to one or more phone book sources.

Alternate Way of Generating Phone Book

The procedures described above are the recommended ways of creating phone book sources and phone books in Cisco TMS. However, it is also possible to generate a phone book using the Cisco TMS Tools application. For more information, see Generate Phone Book, page 296.

Granting Access to Phone Books

Only Site Administrators and Video Unit Administrators can set phone book read and update permissions.

Cisco TMS Users

These permissions determine the ability of the selected group of users to read and update contacts and to update the name of or delete the selected phone book.

1. Go to **Phone Books > Manage Phone Books** and open or create the phone book to which you want to grant users access.
2. Open the tab **Access Control**.
3. Select **TMS User Groups**
4. Specify the access for each group by checking *Read* and/or *Update*.
5. Click **Save**.

By default, Site Administrators and Video Unit Administrators have all permissions set for all phone books.

Note that permissions for reading the list of phone books in Cisco TMS, creating and deleting phone books, and granting update on new phone books are all set elsewhere, see Groups, page 267.

Provisioning Users

When Cisco TMSPE is installed, provisioning users can be granted access as follows:

1. Go to **Phone Books > Manage Phone Books** and open or create the phone book to which you want to grant users access.
2. Open the tab **Access Control**.
3. Select **Provisioning Directory Groups**.
4. Expand the root directory and select the directory groups that are to have access to this phone book.

5. Check **Apply settings to "(current phone book)" and all underlying phone books** if required.
6. Click **Save**.

Setting Phone Books on Systems

This section relates to setting phone books on systems managed by Cisco TMS. For instructions on how to provide phone books to provisioned endpoints, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.

One Phone Book on Multiple Systems

To set one phone book on a group of systems:

1. Go to **Phone Books > Manage Phone Books**
2. Select a phone book in the left-hand navigation section.
3. Click **Set on Systems**.
4. In the two-section view that appears, use the arrows to add or remove endpoints from the right-hand list.
5. Click **OK**.

To verify that the update has been completed, go to **Phone Books > Monitor Phone Book Activity Status**. See Phone Book and Source Activity Status, page 224 for detail.

Multiple Phone Books on a Single System

To set one or more phone books on a specific system:

1. Go to **Systems > Navigator** and select the system to update.
2. Click on the **Phone Book** tab.
3. In the two-section view that appears, use the arrows to add or remove phone books from the right-hand list.
4. Click **Save**.

To verify that the update has been completed, go to **Phone Books > Monitor Phone Book Activity Status**. See Phone Book and Source Activity Status, page 224 for detail.

Setting Global Directory Update Frequency

For legacy systems that are using the phone book as a global directory:

1. Go to **Administrative Tools > General Settings**.
2. In the field **Phone Books Update Frequency**, specify how often you want the phone book to be posted to the endpoints.
3. Click **Save**.

If corporate directory is used, the systems will read the phone book directly from Cisco TMS, and the update frequency can be ignored.

Exporting Contacts to a File

1. Create a *File Based Phone Book Source* with a blank text file that will be used to export the contacts to.
2. Create a phone book .
3. Click **Connect** for this phone book.
4. Select the sources you want to export contacts from.

5. For **Update Type** for these sources, select either *Import to Cisco TMS* or *Import to Cisco TMS and Export to phone book source*.
6. Now select the *File Based Phone Book* source you want to export to.
7. For **Update Type** for this source, select *Import to Cisco TMS and Export to Phone Books Source*.

The first line of the tab delimited text file of the export destination File Based Phone Book source will contain the headers of Name, ISDNNumber, ISDNNumber2, ISDNBandwidth, Restrict, Telephone, SIP, H.323, IPBandwidth, and ExternalId.

The remaining lines will contain the actual phone book contacts. The **ExternalId** column will contain a unique id for the phone book entry.

Manage Phone Books

In Cisco TMS: **Phone Books > Manage Phone Books**

The **Manage Phone Books** page consists of a **Directory** pane on the left-hand side displaying the phone books and a **Workspace** pane to the right.

Workspace buttons

Clicking **New** initiates the creation of a new phone book. After a phone book has been created and populated, select it to modify the configuration, or to click on any of the following buttons:

- **Edit** to change the name.
- **Delete**, then confirm, to delete the phone book. This does not delete any connected sources.
- **Set on Systems** to distribute the phone book to specific endpoints. See Setting Phone Books on Systems, page 214 for further instructions.

Sources

The **Sources** tab displays information for each source connected to the selected phone book. On the **Sources** tab you can create, update, and delete connections to phone book sources.

Settings

Table 122 Source settings for phone books

Field	Description
Name	The name of the source with a link to Manage Phone Book Sources, page 216, where you can modify configurations for the source.
Type	The type of phone book source. For an overview, see Manage Phone Book Sources, page 216.
Update Type	This field indicates how the contacts are shared. Options: ▪ *Search only*: Enable searching in, for example, large H.350 directories directly without importing the contacts to a Cisco TMS phone book. Note that you cannot schedule entries from phone book sources with this type, and that these sources will be filtered out from the **Phone Books** tab that appears when adding participants to conferences. ▪ *Import to Cisco TMS*: Import all contacts to the Cisco TMS phone book. ▪ *Import to Cisco TMS and export to phone book source*: Import all contacts to the Cisco TMS phone book and take the complete phone book (consisting of multiple sources) and export what was not imported to the source.
Update Frequency	The frequency of the update between the source and the phone book. This frequency is set in Manage Phone Book Sources, page 216.

Connection buttons

- **Connect** opens the list of possible phone book sources to add to your phone book.
- **Update** forces an update of one or more selected sources.
- **Disconnect** removes one or more selected sources from the phone book.
- **Manage Phone Book Sources** takes you to Manage Phone Book Sources, page 216.

Access Control

On the **Access Control** tab you can set read and update access to phone books for Cisco TMS user groups by clicking on the respective links with these names. If Cisco TMSPE is installed, you can also grant access to phone books for provisioning users here.

For instructions, see Granting Access to Phone Books, page 213.

Manage Phone Book Sources

In Cisco TMS: **Phone Books > Manage Phone Book Sources**

On the left side of the **Manage Phone Book Sources** page is the **Phone Book Sources** pane displaying the sources. One or more phone book sources must be available before you can populate phone books.

Workspace buttons

Clicking **New** initiates the creation of a new phone book source. After a source has been created, select it to modify the configuration, or to click on any of the following buttons:

- **Edit** to change the name.
- **Delete**, then confirm, to delete the source.
- **Force Refresh** to update the phone book source.

When a source is already selected, you must click **Sources** in the left-hand pane to display the **New** button.

Source Types and Configurations

When configuring a phone book source, the available fields vary depending on source type. The following fields are common to all source types:

Table 123 Available settings for all phone book source types

Field name	Description
Default Bandwidth for Imported Contacts	The bandwidth to set on the imported contacts. This applies to bandwidth at which calls are made. Only imported contacts without bandwidth or with bandwidth set to *Auto* will have bandwidth set from this field. For Manual List this field is called **Default Bandwidth for New Contact Methods**.
Update Frequency	Select how often Cisco TMS will synchronize with the phone book source. This field does not apply to manual lists. Note that importing from large AD sources or provisioning user bases can be resource intensive both for the source server and for Cisco TMS. Updates that take a long time to complete may also block other scheduled tasks. We therefore recommend updating a maximum of four times per day, as most sources are relatively static.

Cisco TMS Endpoint

Dynamically fetch all managed systems or a subset of managed systems to create a source.

Settings

Table 124 Endpoint phone book source settings

Field	Description
Select Folder to Import Contacts from	Cisco TMS will import all contacts in this folder and its subfolders.
Include Subfolders	When creating a phone book source of **Type***Cisco TMS Endpoints*, the checkbox **Include Subfolders** is selected by default. When de-selected it does not import contacts from the subfolders of the folder selected to import contacts from.

Manual List

Create a manually maintained list. Contacts are added and edited directly through the Cisco TMS interface by going to the **View/Edit Contacts** tab.

Contact methods

For each contact displayed, you will on the initial view see the contact's name and originating phone book source. You will also see any contact methods. Each contact method displays the following fields:

Table 125 Contact methods for the manual phone book source type

Field	Description
Type	■ *Voice*: Call set up using standard telephone protocols. (Non-video connection; cell-phone or telephone number.) ■ *IP*: Call set up using direct IP communication to the contact. No gatekeepers or SIP registrars will be involved. ■ *SIP*: Call set up using the Session Initiation Protocol (SIP). ■ *H.323*: Call set up using the H.323 protocol. ■ *ISDN*: Call set up using ISDN. ■ *ISDN2*: number to be paired with an ISDN number for 2B calls (128 Kb/s). ■ *Tel3G*: Deprecated.
Address	The address for each system with the selected type (see above).
Restrict ISDN	A restricted call is a call to a 56 kb/s network. ■ *True*: The ISDN is restricted. ■ *False*: The ISDN is not restricted.
Description	Information you can enter when editing each contact.
Bandwidth	The selected bandwidth for this contact and type.

Table 125 Contact methods for the manual phone book source type (continued)

Field	Description
Icon for Manual list	Use this button to edit contact.
Icon for Manual list	Use this button to delete contact.

Adding a New Contact Method for a Contact

To manually add a new contact method for an already existing contact in your manual list phone book:

1. Open your manual list.
2. Go to the **View/Edit Contacts** tab.
3. Find the contact where you want to add a new method.
4. Click the icon for the contact.
5. Click the **Add contact method**.
6. Enter the fields, see table above.
7. Click **Add**.
8. Repeat to add more methods.
9. Click **Done.**

Adding a New Contact

1. Open your manual list.
2. Go to the **View/Edit Contacts** tab.
3. Click the **Add contact** at the bottom of the screen.
4. Enter the name of the contact.
5. Click **Save**.
6. Click **Add contact method**.
7. Enter the information for the contact.
8. Click **Add**.

One-time import

On the **One-time Import** tab you can fetch contacts from any other source to the manual list source by picking an originating source in the **Select source to copy from** drop-down list.

The result of the import, once completed, is visible in the **View/Edit Contacts** tab.

Active Directory

Import IP Phone and telephone numbers from Microsoft Active Directory to create a source.

Settings

Table 126 Active Directory phone book source settings

Field	Description
IP Address/DNS	The IP address or hostname of an Active Directory Domain Controller or Global Catalog server.
Username	The username for the account to use when logging on to the external source to import/export contacts. The format must be `DOMAIN\username` or `username@DOMAIN`.
Password	The password for the above account.
Default Country Code	Cisco TMS needs country codes for telephone numbers. If the contacts in your directory are stored without a country code specified, provide it here.
Advanced Settings	
LDAP Port Number	If your domain controller is responding on a different port than the standard (389), you can specify the port number here. If you want to connect to a Global Catalog server, you can use port 3268.
Search Base (DN)	This allows you to specify a distinguished name (DN) for an Active Directory container you want to use as the top level of your import. If you set this to blank, the DN for the domain where the domain controller specified in **IP Address/DNS** resides will be used. Example: `OU=Norway,OU=Europe,DC=EXAMPLE,DC=COM`.
Search Scope	Select *One Level* if you want to import contacts found in the container specified in **Search Base (DN)**. If you want to expand the import to also return contacts in all sub containers, select *Recursive*.
Custom LDAP Filter	If you want the import to filter out contacts based on specific user properties in Active Directory, you can supply an LDAP filter. The structure of such a filter is defined in NWG RFC 3377; "The String Representation of LDAP Search Filters". Example: "sn=A*", which would return all contacts with a surname starting with the letter A. See the Active Directory Schema specification for property names.
Import IP Phone	Import Active Directory attribute **ipPhone**, with a dialing protocol of **H323**.
Import Home Phone	Import Active Directory attribute **homePhone**, with a dialing protocol of **ISDN**.
Import SIP	Import Active Directory attribute **MSRTCSIP-PrimaryUserAddress**, with a dialing protocol of **SIP**.
Import Mobile Phone	Import Active Directory attribute **mobile**, with a dialing protocol of **ISDN**.
Import Telephone	Import Active Directory attribute **telephoneNumber**, with a dialing protocol of **ISDN**.

H.350 Directory and H.350 User Directory

H.350 is a standard for communicating with an LDAP-based global directory of calling addresses in various video and VoIP formats.

- H.350 Directory source: Search for H.350 commObjects and import them.
  Two-way synchronization is supported, but Cisco TMS can only update contacts in the H.350 directory that were created by Cisco TMS.
- H.350 User directory source: Search for H.350 commURI properties and import the commObjects they point to.
  Only import is supported for this source.
  Note: By default, `commURI` attribute is not available in OpenLDAP. You must first install the `commURIOject` schema for this user attribute to become available.

To configure openLDAP, see **LDAP Server Configuration for Device Authentication** section in Cisco TelePresence Video Communication Server Administrator Guide.

Settings

Table 127 H.350 phone book source settings

Field	Description
IP Address/DNS	The IP address or hostname of an Active Directory Domain Controller or Global Catalog server.
Username	The username for the account to use when logging on to the external source to import/export contacts.
Password	The password for the above account.
New contacts will be put in (RDN)	This entry specifies where in the H.350 directory contacts made in Cisco TMS should be stored when exporting to the H.350 directory. A Relative Distinguished Name should be used when specifying this. Example: if DN is set to `OU=VideoConferencing,DC=EXAMPLE,DC=COM` and `OU=ExampleUnit` is specified here, then the new contacts will be stored in `OU=ExampleUnit,OU=VideoConferencing,DC=EXAMPLE,DC=COM`
Advanced Settings	
LDAP Port Number	If your domain controller is responding on a different port than the standard (389), you can specify the port number here. If you want to connect to a Global Catalog server, you can use port 3268.
Search Base (DN)	This allows you to specify a distinguished name (DN) for an Active Directory container you want to use as the top level of your import. If you set this to blank, the DN for the domain where the domain controller specified in **IP Address/DNS** resides will be used. Example: `OU=Norway,OU=Europe,DC=EXAMPLE,DC=COM`
Search Scope	Select *One Level* if you want to import contacts found in the container specified in **Search Base (DN)**. If you want to expand the import to also return contacts in all sub containers, select *Recursive*.
Custom LDAP Filter	If you want the import to filter out contacts based on specific user properties in Active Directory, you can supply an LDAP filter. The structure of such a filter is defined in NWG RFC 3377; "The String Representation of LDAP Search Filters". Example: "sn=A*", which would return all contacts with a surname starting with the letter A. See the Active Directory Schema specification for property names.
Field to use for Display Name in TMS	If you want to use another property than **commUniqueId** as the display name in Cisco TMS, you can supply the name of this property here. You can use H.350 properties or properties defined in a custom scheme on your LDAP server. Example: *DisplayName*.

Table 127 H.350 phone book source settings (continued)

Field	Description
Field on User Object to Prefix Display Name in TMS	The display name for the imported contact is normally provided as a postfix to the commURI. If you want to use the value of an LDAP property on the object containing the commURI as a prefix to the display name of the imported contact, you can specify that here.

Wrong number of entries imported from LDAP

If an incorrect number of entries is returned to your phone book source from your LDAP server, your server might be set up to return a limited number of entries. The truncation happens on the LDAP server, usually because it does not implement the paged LDAP extension. For guidance, see the documentation for your LDAP server..

File Based Phone Book

Connect to a local or online file to create a phone book source.

Note: Cisco TMS does not support 'File Based Phone Book' source in High/Medium-High mode.

Settings

Table 128 File-based phone book source settings

Field	Description
Force Default Bandwidth	By checking this check box, Cisco TMS will force default bandwidth for all imported contacts. Any bandwidths configured in the phone book source will be overridden by the value selected as **Default Bandwidth for Imported Contacts**. (Not only on contacts without bandwidth or with bandwidth set to *Auto*, see field above.)
Use Local File or File from URL	Radio buttons to decide the location of the file which contains the phone book to be imported/exported to/from Cisco TMS.
File Path	When opting for local file, the file path must be provided by clicking the **Browse Files** button.
URL	When opting for file from URL, specify the URL where the file is located.
Username (Empty = anonymous)	Only available when using file from URL. Username required to access the file. Leave blank if no username is required or a local file is used.
Domain	Only available when using file from URL. Domain required accessing the file.
Password	Only available when using file from URL. Password required accessing the file. Leave blank if no password is required or a local file is used.

Importing contacts to file-based phone book sources

When choosing to create a File Based Phone Book Source, it is possible to set up and import contacts from a comma-separated file located on a web server or a local directory on the Cisco TMS server.

For example if a phonebook.txt file containing the phone book information is placed on your Cisco TMS server:

1. Under **File Path**, click **Browse Files**.
   You now get a list of the files in the **~\TANDBERG\TMS\wwwTMS\data\ExternalSourceFiles** folder on your Cisco TMS server.

2. Click **Browse...**.
3. Browse to the correct file and select it.
4. Click **Open** to create a copy of the file in the **~\TANDBERG\TMS\data\ExternalSourceFiles** folder.
5. Select the **phonebook.txt** file from the list and click **Use**.
6. If the file is not empty, you can display the phone book contacts from this source by clicking **View Contacts**. Click on the arrow to the left of each entry to expand the details for that entry.

Structure requirements for imported files

Files for import must contain comma-separated values and have either a **.txt** or **.csv** extension. The first row must contain column headers describing the contents of each column.

- The column headers must be named as follows:
  `Id, Name, ISDNNumber, ISDNNumber2, ISDNBandwidth, Restrict, Telephone, SIPAlias, IPNumber, IPAddress, IPBandwidth.`

  Note that IPNumber may contain an H.323 ID or an E.164 alias.
- The column headers and data entries must all be separated by a comma.
- All columns do not need to be included or contain data, but the **Name** column cannot be empty.
- We strongly recommend using the Id column, you can use any string or number of less than 512 characters. This is used as identification in later imports.

An example of a comma-separated file is shown below, where the first row contains the headers (note that only some of the columns contain data):

```
Id,Name,ISDNNumber,SIPAlias,IPNumber,IPAddress
1,Test Entry,+1 (555)1231234,system@example.com,system@example.com,10.0.0.5
2,Test Entry2,+1 (555)1111111,system2@example.com,system2@example.com,10.0.0.6
```

Gatekeeper

Import registrations on a gatekeeper to create a phone book source.

Note: Importing SIP entries is not supported.

Settings

Table 129 Gatekeeper phone book source settings

Field	Description
Select Gatekeeper	Select a gatekeeper from the gatekeepers currently added to Cisco TMS.
Include Zone Prefix from GK	Check this to include the zone prefix from the gatekeeper on imported contacts.
User Defined Prefix	Prefix to add to imported contacts.
User Defined Postfix	Postfix to add to imported contacts.

Other TMS Phone Book

Import contacts from a Cisco TMS phone book as a source to create nested phone books.

Settings

Table 130 Other TMS phone book source settings

Field	Description
Select TMS Phone Book	Select one of the phone books in Cisco TMS you want to import contacts from.

TMS User Phone Book

Create a source from all users registered in Cisco TMS. Only default bandwidth and update frequency are configurable for this phone book source.

Cisco TMS Provisioning Directory

When Cisco TelePresence Management Suite Provisioning Extension is used, the provisioning user base can be used for one or more phone book sources.

Settings

Table 131 Provisioning phone book source settings

Field	Description
Root Directory Group	Specify the root directory group in the Provisioning Directory that contacts will be imported from when creating a Cisco TMS Provisioning Directory source.
Advanced Settings	
Import Provisioned Devices	Import provisioned devices for each user.
Import Office Phone	If an office phone number is included in the user directory, import it to the phone book source.
Import Mobile Phone	If a mobile phone number is included in the user directory, import it to the phone book source.

System Local Phone Book

Import the local directory from an endpoint. This feature is only supported for legacy endpoints, including Cisco TelePresence MXP.

Settings

Table 132 System Local phone book source settings

Field	Description
Force Default Bandwidth	Check to make Cisco TMS force default bandwidth for all imported contacts. Any bandwidths configured in the phone book source will be overridden by the value selected as **Default Bandwidth for Imported Contacts**. (Not only on contacts without bandwidth or with bandwidth set to *Auto*, see above.)
Select a System	Select the system from the drop down list that you want to import the local Phone Book from.

Cisco Unified Communications Manager

Use a Cisco TMS-managed Unified CM for a phone book source.

Settings

Table 133 Unified CM phone book source settings

Field	Description
Select Cisco Unified Communications Manager	Choose a Cisco TMS-managed Unified CM from the drop-down.
Advanced Settings	
Prefix for Imported Numbers	Add this prefix to all numbers imported from Unified CM.
Suffix for Imported Numbers	Add this suffix to all numbers imported from Unified CM.

Viewing contacts

After selecting a phone book source you can to search and view contacts by going to the **View/Edit Contacts** tab.

To search:

1. Enter the name of the person you are looking for in the search field.
2. In Number of Contacts select how many search results to display. Note that this field does not apply to sources of the *Manual List* type, where you adjust the number of contacts displayed in the bottom row of the search results.
3. Click **Search**.

If the search returned more results than are displayed, the bottom row of the search results will inform you of this.

Phone Book and Source Activity Status

In Cisco TMS: **Phone Books > Phone Book Activity Status** and **Phone Book Source Activity Status**

The **Phone Book Activity Status** page tracks all events created when Cisco TMS posts a phone books to systems.

The **Phone Book Sources Activity Status** page tracks all events created when phone books are synchronized with phone book sources.

Ongoing and upcoming scheduled events are displayed automatically.

- Search for past events by modifying the **Start Date** and **End Date** fields, then click **Search**.
- Check *Show only mine* to display only events scheduled by the currently logged in user.

  To apply this to the list below, click **Refresh**.
- Click the linked description of any event to see a detailed activity log.
  - For Conference Diagnostic Activity, the status and event description for the selected dates are displayed
- To cancel a scheduled event, select it and click **Delete**.

Click to refresh

Note that the activity status pages do not automatically refresh while open. To update the status view, click **Refresh**.

Phonebook for Cisco Meeting Management

Cisco TMS allows Cisco Meeting Management to access the corporate directory in Phone books. You can perform the following functions:

- Add a Cisco Meeting Management Server
- Set your phone book/s on Cisco Meeting Management Server
- Edit a Cisco Meeting Management Server
- Delete a Cisco Meeting Management Server

The Cisco Meeting Management Server can be configured from **Phone books> Phonebook for Cisco Meeting Management**.

Note: You have to set access permissions in **Administrative Tools> Users> Groups** in order to use this feature, where you can configure and set Phone books on the Cisco Meeting Management Server.

Add Cisco Meeting Management Server

1. Click **New** to configure a Cisco Meeting Management Server.
2. Enter the **Server name**and **MAC address**.
3. Click **Save** to add the Cisco Meeting Management in Cisco TMS. The Cisco Meeting Management server is added in the left side of the screen.

Set Phone book/s on a Cisco Meeting Management Server

This functionality allows you to select phone book/s that has to be set on the Cisco Meeting Management Server.

1. Select the phone book/s from '**Available Phone Books**' pane.
2. Click . The selected phone book/s are moved to '**Phone Books Set on System**' pane.
3. Click **Save**.
   Or
   Click '**Go to Manage Phone Books**'. You will be re-directed to **Manage Phone Books** page, where you can create new phone book/s or manage your company phone books.

Edit Cisco Meeting Management Server

1. Click **Edit** to make the required modifications to server name and MAC address.
2. Click **Save** to save the modifications.

Delete Cisco Meeting Management Server

1. Select the Cisco Meeting Management Server to be deleted.
2. Click **Delete**. A message ' Do you want to delete <Cisco Meeting Management Server name> from Cisco TMS? The Cisco Meeting Management Server is deleted from Cisco TMS.

Reporting

This chapter explains how Cisco TMS collects data about systems and calls, and details the statistics that are available under the **Reporting** menu.

Reporting Basics 226
Creating a Report 226
Using Reporting Templates 228
Bridge Utilization 229
Call Detail Records 230
Billing Code Statistics 231
Conferences 231
System 233

Reporting Basics

The reporting pages all work in similar ways and share core functionality.

For more flexible reporting options, we recommend adding Cisco TelePresence Management Suite Analytics Extension (Cisco TMSAE) to your deployment, see Analytics Extension, page 285.

Types of Data

- Call Detail Records, page 230 track the frequency and duration of calls in your telepresence deployment.
- Billing Code Statistics, page 231 show which billing codes are applied to conferences.
- Conferences, page 231 are tracked per user, type, and so on.
- System, page 233 reporting catches errors and other events from systems.

How Log Purge Settings Affect Reporting

Many of the statistics calculations are based on call logs. If logs are purged after a specific time, calculations that span earlier dates will be misleading.

To view or modify the settings for log purging:

1. Go to **Administrative Tools > TMS Server Maintenance**.
2. Expand the **Purge Old Data in Database Tables Plan** section.
3. Click **Edit** to modify any entry.
4. Click **Update** for each entry that you modify.

Creating a Report

All report query forms contain default values to search for. You can view and modify these defaults in Reporting Settings, page 258.

To generate a custom report:

1. Enter the start and end time for your search. Depending on the type of report, you may have the option of adding both a date and a specific time of day.
2. Specify additional search criteria:

Table 134 Search criteria for Reporting search

Calculate By	Define how the report should be calculated and set the unit on the y-axis of the graph. You can generate reports based on: – *Duration* – *Number of Occurrences* – *Utilization*—display the percentage of time the video systems were in use on average in the given time range.
Call Protocols	To see calls made using a specific call protocol, select the desired protocol. If you want to see all calls and disregard which call protocol was used, select *All Call Protocols*.
Conference Type	Define what type of conferences should be used for generating the report. You can generate reports for: – *Scheduled Conferences* – *Ad Hoc Conferences* – *All Conferences*
Graph Types	Set the displayed unit on the x-axis of the graph: – *Date Range*: · When calculated by *Duration*, the total duration in minutes of calls that took place in the given time range will be plotted for each day in the given date range. · When calculated by *Number of Occurrences*, the chart will show the number of calls that took place in the given time range. · When calculated by *Utilization*, the chart will show the percentage of time that the video systems were in use on average in the given time range – *Day of the Month*: This graph will plot the distribution of calls by day of the month. · When calculated by *Duration*, the duration of calls in the given time range for each day of the month will be summarized within the date range. Example: If 500 minutes of video calls took place in the specified time range on January 11, and 900 minutes on February 11, and your date range spans January and February, the value for day 11 in the chart will be 1400 minutes. · When calculated by *Number of Occurrences*, the chart will show the distribution of the number of calls by day of the month. · When calculated by *Utilization*, the chart will show how the average utilization varies by day of the month. – *Day of the Week*: This graph will show how the duration, number of calls, and utilization varies by day of the week. – *Time of Day*: This graph will show how the duration, number of calls and utilization varies over time for the specified time range.
System Category	Select which types of systems to include statistics data for.

3. In some report query forms, a **Filter Systems** button is available for selecting which specific systems to include:
   - If no systems are specified, all available systems will be included.
   - Click the button to select the desired systems from a navigator view.
4. Click **Search** to generate the report.
5. Click **Save as Template** if you want to reuse the same search at a later time. See Using Reporting Templates, page 228 for more information.
6. Use the tabs below the query area to choose how you want the search results to be presented:
   - **Chart** view: a graphical representation of the data.
   - **Data** view: the actual data that make up the report, such as the call history, event log, or conference history in a table format.

Exporting Data to an Excel Sheet

Under the **Data** tab, click on **Export Excel** to export all data to an Excel sheet.

The exported **.csv** file will include additional information that will not be present in the **Data** tab.

Using Reporting Templates

In Cisco TMS: **Reporting > Reporting Templates**

Creating a Template

Creating a reporting template can be done on most of the reporting pages in Cisco TMS:

1. Click on the **Save as Template** button in the query field.
2. Enter a unique name for your template.
3. Click **Save**.
4. The saved search will then be available in the **Reporting Templates** page.

Viewing and Running Template Searches

You can run all template searches in both the **My Templates** and the **All Templates** tabs. The dates will be adjusted to the current date, with the same time interval as the saved query.

To run a template search:

1. View the available templates by doing one of the following:
   - On any page under the **Reporting** menu, click the **List Templates** button to see all saved templates for the page in a popup window.
   - Go to **Reporting > Reporting Templates**, which lists all searches saved as templates. You will also see who created the template and from which reporting page.
2. Hover over the desired template, click the drop-down button and select **Run Reporting Template** in the drop-down menu.

Automatically Running a Template Search

All reporting template searches can be run automatically:

1. In your browser's address field, input the URL for the reporting page you want, appending `&RunStatTemp=<template name>`.
2. Press `Enter`, and the requested template search will be run.

For example, when entering `http://<servername>/tms/default.aspx?pageId=29&RunStatTemp=CDR_All_systems_monthly`, the template search called **CDR_All_systems_monthly** will be run on the **Call Detail Record** page.

Editing and Deleting a Template

You can edit and delete only templates that you have created.

To edit:

1. Select **Edit** in the drop-down menu for the template you want to modify.
2. Modify the template search as desired.
3. Click **Save as Template**.
4. A prompt will ask you whether to overwrite the existing template.
   - Click **Yes** to update the original template.
   - Click **No** to save the modified search as a new template:
     1. Enter a name for the new template.
     2. Click **Save**.
   - Click **Cancel** to return to the template editing view.

To delete:

1. Select the check boxes next to the template or templates you want to delete.
2. Click **Delete**.
3. Confirm that you want to delete the templates by clicking **OK**.

Bridge Utilization

The Bridge Utilization page contains reporting information on how much Cisco TMS-managed bridges are being used. The only supported bridges are direct-managed TelePresence Servers and TelePresence MCUs.

Two graphs and a table show how much your bridges are being used. The upper graph compares the total capacity with the peak call count for a given point in time. The lower graph presents the same information as a percentage (peak calls divided by capacity). The table contains the selected information as raw data.

Note that:

- The report contains data from video calls only.
- Permanent conferences are only included in the reporting data from the day that they are ended and onwards.

The Reporting Mechanism and Logs

The data is collected using an extract, transform and load (ETL) process in the SQL database.

The ETL job:

- runs daily at 04:05am. It processes data from 00:00 til 23:59 the previous day. Calls ending at 00:05 will therefore affect tomorrow's data, not today's.
- is not database intensive.

The ETL log is available as part of the **Download Diagnostic Files** download bundle. The data is kept for 30 days. It is a self-cleaning log that contains log level information only.

Troubleshooting

For troubleshooting assistance see Bridge Utilization Report, page 319 in the Troubleshooting chapter.

Call Detail Records

In Cisco TMS: **Reporting > Call Detail Record**

The pages in the **Reporting > Call Detail Record** menu section contain reporting options for call detail records from all supported Cisco TMS-managed systems.

What is a Call Detail Record?

A call detail record is created as a call (videoconference or audio) ends. Different systems generate their CDRs and share them with Cisco TMS using different mechanisms. For this reason, data is sometimes processed and interpreted differently, which may lead to discrepancies in CDRs from different systems that participated in the same call.

Key information in a CDR includes:

- Call participants (systems)
- Duration
- Encryption mode and protocols used

CDR-based reports are commonly used in planning and reviewing how a telepresence network deployment is used. CDRs may reveal where more telepresence resources are needed, as well as potential under utilization of existing equipment. Below are brief descriptions of the different types of systems for which Cisco TMS statistics can be generated, and how they are retrieved.

Note that CDRs in Cisco TMS should be considered best effort, and the quality of the data presented relies on the quality of data received from the systems.

Endpoints

Endpoints managed by Cisco TMS will generate a CDR and communicate it to Cisco TMS immediately after the call ends.

Reports based on endpoint CDRs can be generated either in the **Endpoints and MCUs** page, where you also have the option of seeing the two different CDRs accumulated, or in the **Endpoints** page.

Note that both of these reports only include endpoints managed by . Cisco TMS. Statistics for provisioned endpoints are available in the Users, page 231 page.

Cisco TMS provides CDRs for Cisco Unified Communications Manager managed TC / CE endpoints that are added into Cisco TMS.

MCUs

The Cisco TMS Database Scanner Service requests MCU CDRs at regular intervals.

Reports based on MCU CDRs can be generated either in the **Endpoints and MCUs** page, where you also have the option of seeing the two different CDRs accumulated, or in the **MCUs** page.

External participants will appear only in MCU CDR reports, not in endpoint reports.

Note that the minimum value of 1% is displayed in MCU Utilization chart. If the calculated value is less than 1% then the data is not sufficient to be displayed in the MCU Utilization chart and it is considered as 0% utilization.

Gatekeeper and VCS

Cisco VCS sends call data and other events to Cisco TMS as the events occur. On the **Gatekeeper CDRs** page, you can create reports based on this call data.

The chart shows the amount of calls handled by each device type. To get call data for a specific Cisco VCS, click on a bar in the chart, or select a system in the **Data** tab.

Users

The **User CDR** page is only available if Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) is installed and activated.

These CDRs are listed per user.

Note the following:

- User CDRs are only generated for outgoing calls.
- User CDRs are only generated on the Cisco VCS the endpoint making the outbound call is registered to.
- User CDRs are only shown on the Cisco TMS server receiving the call disconnect feedback from the Cisco VCS the endpoint making the outbound call is registered to. Cisco VCSs under heavy load could fail to send feedback events to Cisco TMS, and there is no retry mechanism.
- Cisco TMS's "Resolve users from numbers in gatekeeper log" scheduled task will resolve feedback events to Cisco TMSPE users. As this task runs every five minutes, there is a short delay before a User CDR is created.
- Cisco TMS filters out the zero duration calls when resolving feedback from the Cisco VCS.

As with other CDRs in Cisco TMS, User CDRs should be considered best effort.

TelePresence Content Servers

If you have TelePresence Content Servers managed by Cisco TMS, CDR-based reports for these are available in the **Content Server** page.

Select a bar in the chart view to see a **Content Server Activity Log** for each server.

Gateways

CDR-based reports for gateways are available in the **Gateway** page.

The chart shows activity filtered by call protocol.

Billing Code Statistics

In Cisco TMS: **Reporting > Billing Code Statistics**

On the **Billing Code Statistics** page you can generate, view statistics for and export CDRs (call detail records) for selected billing codes. This includes billing codes for both scheduled and unscheduled calls.

Data can be collected for defined time intervals for a selected billing code. Only 20 billing codes can be shown in the chart. Use the **Paging** drop-down to view more.

Conferences

In Cisco TMS: **Reporting > Conferences**

The pages in the **Reporting > Conferences** menu section contain reporting options for scheduled and unscheduled conferences in Cisco TMS.

Conference Statistics

On the **Conference Statistics** page you can generate statistics for scheduled and ad hoc conferences for a specified time interval. This does not include permanent conferences configured directly on bridges.

Conference Resources

On the **Conference Resources Overview** page you can display reports for each Cisco TMS-registered resource used in the conference. Such resources include endpoints, MCUs, gateways, and Cisco VCS.

Data can be collected for defined time intervals on selected systems.

Use the **Paging** drop-down to navigate through the generated chart.

Events

On the **Conference Events Overview** page you can obtain a detailed log that describes all events registered in a conference. These events typically include like scheduling, encryption status, any errors, and so on.

The chart will indicate which conferences have encountered errors, as the bars representing conferences will change color to red if any of the following events have been logged:

- Boot
- Link Down
- Connection Error
- Lost Response
- Downspeed

Only the 20 last conferences will be shown in the generated chart.

Scheduling Interfaces

On the **Scheduling Interfaces** page you can view which tools are most and least used for scheduling. The chart shows the amount of time each user has scheduled, in minutes per user, for the specified time period and which tool has been used for scheduling the calls.

Possible scheduling interfaces include:

- The page New Conference, page 170
- Smart Scheduler
- Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE)
- Cisco TelePresence Management Suite Extension for IBM Lotus Notes (Cisco TMSXN)
- Any third-party application using Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA)

Bridging Methods

This report is useful in observing which bridging methods, that is, multisite options, are used in your telepresence network.

On the **Bridging Methods** page you can display the distribution of the following different types of conferences (**Call Type**) set up by each system in Cisco TMS.

- *Point-to-point*: The endpoint was in a point-to-point call with another endpoint.
- *Multipoint*: The endpoint was in a multipoint conference, either involving an external MCU or another endpoint with internal MCU (multisite option).
- *Internal MCU*: The endpoint was in a multipoint conference using its internal MCU.
- *Internal MCU cascaded*: The endpoint was in a cascaded multipoint conference using its internal MCU.

Display Cascaded, Multiway, and Normal MCU Conferences

You can also display the distribution on cascaded, multiway, and normal MCU conferences for an MCU:

- *External MCU*: The MCU was used in a multipoint conference.
- *External MCU cascaded*: The MCU was used in a cascaded multipoint conference, the other MCU(s) in the conference was either another MCU or an endpoint with internal MCU.
- *Multiway*: The MCU was used in a multiway conference.

System

In Cisco TMS: **Reporting > System**

The pages in the **Reporting > System** menu section contain reporting options for data from managed systems. This means that none of these reports cover provisioned endpoints. Many of these reporting options are also only supported only by certain types of endpoints.

Ticket Log

The **Ticket Log** reports on all system tickets that have been raised on systems in Cisco TMS, with the network address, the time the ticket was raised, and a ticket description.

Feedback Log

The **Feedback Log** reports events like scheduling, errors, and encryption status from systems in Cisco TMS.

For Cisco TMS to receive events from systems that rely on SNMP, the traphost IP address for the system must be set to the IP address of the Cisco TMS server under **Monitoring/SNMP Settings**. For further details, see the description of the relevant system type in Navigator, page 69.

Connection Error

The **Connection Error** page gives a detailed log that describes connection errors only with a cause code. This is useful information to determine if there are network connection problems towards systems in Cisco TMS.

To view the log for a specific system, select the check box next to the system, then click on the **View** button at the bottom of the page.

System Connection

The **System Connection** page displays all management connection and Cisco VCS registration attempts for a system.

Authentication Failure

The **Authentication Failure** page gives information about all failed login attempts on systems that require a password when accessing the systems by Telnet, HTTP or SNMP.

Boot

The **Boot** page displays statistics for all boot events on systems registered in Cisco TMS.

History

The **History** page provides a consolidated list of changes that have occurred with the registered systems in Cisco TMS. This is the same data that is shown when you select the **System History** tab per system in system navigator, except that you here get an overview across all systems.

Administrative Tools

This chapter contains reference material for all pages in the **Administrative Tools** section of Cisco TMS, which contains tools for configuration, user administration, call routing, and billing code management.

Configuration 234
User Administration 266
Locations 278
Billing Codes 280
Diagnostics 282
Activity Status 284
Analytics Extension 285
TMS Server Maintenance 285
Audit Log 288

Configuration

In Cisco TMS: **Administrative Tools > Configuration**

The Configuration menu is where you can make changes to settings for the Cisco TMS application and set defaults for conferences, email, the network, errors, and any extension products you have installed.

General Settings

In Cisco TMS: **Administrative Tools > Configuration > General Settings**

Table 135 Settings in the General Settings section

Field	Description
TMS Release Key	This is the release key for your Cisco TMS installation. The release key must be provided when contacting Cisco for support or new option keys.
Default Time Zone	Specify the default time zone for users and systems in Cisco TMS. Users will see their own time zone when: ▪ Booking a new conference. ▪ Listing existing conferences. When editing or viewing the details of a booking created for a different time zone, the time zone of the conference will be displayed, and the user will be notified of this.
Default ISDN Zone	Specify the default ISDN zone for systems in Cisco TMS.
Default IP Zone	Specify the default IP zone for systems in Cisco TMS.

Table 135 Settings in the General Settings section (continued)

Field	Description
Software Directory	The Software Directory on your Cisco TMS server where system software used for system upgrades is stored. This location is edited using the Cisco TMS Tools program accessed on the server itself, see .
System Contact Name	The name of the Cisco TMS system contact. This name will be displayed in the footer of Cisco TMS on all pages.
System Contact Email Address	The email address of the Cisco TMS system contact. The system contact name in the footer of Cisco TMS will be a clickable email link when this address is set.
Global Phone Book Sort	Specify how global phone book entries should be sorted when sent to systems from Cisco TMS: ■ *Default TMS Sort*: sort in accordance with Cisco TMS server language. ■ *System Specific Sort*: sort in accordance with system language.
Route Phone Book entries	This setting applies to the phone books specified in **Cisco System Phone Books**. ■ *Yes* is the default setting, which means that endpoints will only display addresses that they are capable of dialling. For example, on an H.323-only endpoint, ISDN numbers and SIP addresses will not be displayed. ■ *No* means that the endpoints will display all addresses and numbers in the phone book regardless of their dialling capabilities.
Cisco System Phone Books	Select which type of phone book should be used: ■ *Use centralized TMS phone books only (corporate phone book)* ■ *Use both centralized and downloaded phone books (both)* ■ *Use global phone books downloaded to systems only (global phone book)* We recommend opting for *corporate phone book* or *both*, as the downloaded phone book is only supported by legacy TANDBERG endpoints. The default setting is *both*, which will make the global directory available should the corporate directory live search fail. See Phone Book Types, page 211 for more information.
Phone Books Update Frequency	Specify how often global phone books should be downloaded to systems. Note that this is only relevant for legacy endpoints. The options are: ■ *Not Set* ■ *Every Hour* ■ *Every Day*
Phone Books Update Time of Day	If **Phone Books Update Frequency** is set to *Every Day*, set the time here.

Table 135 Settings in the General Settings section (continued)

Field	Description
Alternate System Name Rules for Endpoints (order of name to use)	Specify how to display system names in Cisco TMS. The options are: ■ *Use System Name only (displays "No Name" if blank)*: Cisco TMS will display the name of the system or *No Name* if no system name is set. ■ *System Name/Network Address*: Cisco TMS will display the **System Name** if not blank; otherwise it will display the **Network Address**. ■ *H.323 ID/System Name/Network Address*: Cisco TMS will display the **H.323 ID** if set. If **H.323 ID** is not set, Cisco TMS will display the **System Name**, if not blank. If the **System Name** is blank, the **Network Address** is displayed. ■ *H.323 ID/E.164 alias/System Name/Network Address*: Cisco TMS will display the **H.323 ID** if set. If the **H.323ID** is not set, Cisco TMS will display the **E.164 Alias**. If no E.164 alias is set, the **System Name** is displayed, if not blank. If the **System Name** is blank, the **Network Address** is displayed.
Provisioning Mode	This setting can be used to activate or deactivate Cisco TelePresence Management Suite Provisioning Extension if the extension has been installed. The options are: ■ *Off* ■ *Provisioning Extension* See *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* for information on installing and activating the extension. **Note**: If you are no longer using Cisco TMSPE, moved or uninstalled it, then you must change the **Provisioning Mode** to **Off** before you move or uninstall Cisco TMSPE.
Analytics Extension Admin URL	This setting can be used to modify the URL to the Cisco TelePresence Management Suite Analytics Extension (Cisco TMSAE) web interface. The setting is only available if the extension has been installed. See *Cisco TelePresence Management Suite Analytics Extension Installation Guide* for information on installing and configuring the extension.
Enable Login Banner	The text entered here will be displayed to each user when entering Cisco TMS. If the user is inactive for one hour or more and then starts using Cisco TMS, the text will be displayed again. To enable: 1. Select *Yes*. 2. Click **Edit Login Banner**. 3. Enter the text you want users to see. 4. Click **Save** in the Login Banner window. 5. Click **Save** on the page.
Show Systems In Navigator Tree	If set to *Yes*, all systems will be viewable in the **Navigator** tree (left hand section in **Systems > Navigator**). If set to *No*, only folders will be viewable in the **Navigator** tree. After selecting a folder, the systems will be viewable in the right hand section.

Licenses and Option Keys

Note: Adding more than 5000 systems licenses will generate a warning that utilizing more than 5000 systems is not supported. This warning will be displayed every time the **General Settings** page is accessed. Contact tms-marketing@cisco.com if you have a deployment that exceeds or is likely to exceed 5000 systems.

Table 136 Description of Licenses and Option Keys section

Section name	Description
Licenses	An overview of the number of licenses that are in use and how many are available.
Active Application Integration Clients	This section is only visible if there are active Cisco TMSBA clients. Lists all currently active application integration clients. The table displays: ■ **Session ID** (if applicable, only clients using Cisco TMSBA version 13 or later will use this). ■ **Network Address** (either the hostname or IP address, in redundant Cisco TMS deployments this could be the load balancer address). ■ **Last Access** timestamp.
Option Keys	A list of all the option keys that have been added to Cisco TMS.

Click **Add Option Key** to add option keys to Cisco TMS. Click **Delete** to delete selected option keys from Cisco TMS.

Network Settings

In Cisco TMS: **Administrative Tools > Configuration > Network Settings**

Table 137 Settings on the Network Settings page

Sections and fields	Description
General Network Settings	
Telnet/HTTP Connection Timeout (in seconds)	The number of seconds Cisco TMS will wait for a system's Telnet or HTTP service to reply before timing out.
Telnet/HTTP Command Timeout (in seconds)	The number of seconds Cisco TMS will wait for a system to respond to a Telnet or HTTP command before timing out.
SNMP Timeout (in seconds)	The number of seconds Cisco TMS will wait for a response to an SNMP query.

Table 137 Settings on the Network Settings page (continued)

Sections and fields	Description
SNMP Community Name	The defaults used by Cisco TMS are: ■ `public` ■ `Public` ■ `RVGET2` ■ `RVGK` Enter multiple community names in a comma-separated list. The maximum length for SNMP community name in the database is 255 characters. Hence, either you can have one item of up to 255 characters or multiple items that add up to 255 characters including commas.
Override DNS	If set to *Yes*, Cisco TMS will use IP addresses instead of DNS names to communicate with systems.
DNS Timeout (in seconds)	The number of seconds Cisco TMS will wait for a response to a DNS query before timing out.
Default System Identifier type to track systems	Choose whether Cisco TMS will use *IP Address*, *MAC Address*, or *Hostname* to contact managed systems.
URL where software packages can be downloaded	**Note:** *This functionality only applies to legacy systems.* This field is not used for endpoints running software version TC 6.x and later; instead the address set for Cisco TMS in the **Advanced Network Settings for Systems on Internal LAN** section below is used, with the correct path automatically appended. Specify which URL will be used when performing software upgrades on endpoints behind a firewall/NAT. The endpoint will contact this URL to download the software package. The default directory **TMS/public/data/software** is where Cisco TMS retrieves the list of packages found in **Systems > System Upgrade > Software Manager**.
Event Notifications	
Email Addresses to Receive System and Network Notifications	Specify which email addresses will receive email when an event notification is created. Enter multiple addresses in a comma-separated list.
SNMP Traphost IP Address	*Legacy systems only.* If using one or more external traphosts to which you upload the Cisco TMS MIB file, provide a comma-separated list of IP addresses that will receive SNMP traps from Cisco TMS when an applicable event notification is received.
SNMP Version for Traps	This field is not editable. Cisco TMS uses SNMPv2 exclusively.
Automatic System Discovery	

Table 137 Settings on the Network Settings page (continued)

Sections and fields	Description
Automatic System Discovery Mode	Cisco TMS is capable of automatically discovering and registering systems. Systems must be configured to send HTTP events or SNMP traps to Cisco TMS for this feature to work. If set to *Off*, systems will not be added to any folder, but will still be auto-discovered. Auto-discovered systems will be viewable by going to **Systems > Navigator > Add Systems > Add from Unified CM or TMS > TMS** and can be added to a folder from there. Each time a system is discovered, an email notification will be sent to the email address specified in **Email Addresses to Receive System and Network Notifications**.
Default Configuration Template for Discovered Systems	You can set Cisco TMSto apply a default configuration template to discovered systems. The default *Discovered Systems Template* applies the following: ▪ default IP Zone ▪ phone books You can override this by selecting another template in the drop-down menu, editing the default template, or creating a new template.
Default Folder for Discovered Systems	Add discovered systems to this folder in **Systems > Navigator**.
Automatic System Discovery Mode for Endpoints behind a Firewall/NAT	To automatically discover and register endpoints behind a firewall/NAT, each endpoint must be configured to send feedback to Cisco TMS. Each time a system is discovered, an email notification will be sent to the email address specified in **Email Addresses to Receive System and Network Notifications**.
Default Template for Discovered Endpoints behind a Firewall/NAT	See **Default Configuration Template for Discovered Systems** above.
Active Directory	
Lookup User Information from Active Directory	If enabled, any user logging into Cisco TMS or using the booking API (Cisco TMSBA) will generate a lookup for user and group information in Active Directory. If disabled, the remaining fields in this section will be grayed out.
GC server or AD forest DNS name	Specify the GC (global catalog) server or AD forest DNS name If the forest structure is too complex, then port 3268 is required to set the connection to GC (global catalog). Use the port 3268 followed by the domain name and a colon. For example `[domain.com:3268]`
AD Lookup Account - Username	Specify the username, password, and domain that Cisco TMS will use to connect to Active Directory.
AD Lookup Account - Domain	
AD Lookup Account - Password	

Table 137 Settings on the Network Settings page (continued)

Sections and fields	Description
Allow AD Groups	When set to *Yes*, Cisco TMS groups can be mapped to Active Directory groups in **Administrative Tools > User Administration > Groups**, see Groups, page 267.
AD synchronization schedule	Specify day of the week and time for Active Directory synchronization of users and groups.
Test connection to Active Directory	Click **Save and Test connection** to test. If the connection to Active Directory is successful, you will see the message: "Successfully connected to Active Directory <AD name >".
TMS Services	
Scan SNMP Capable Systems to Allow Quick Discovery of Inaccessibility	*Legacy systems only.* Enable to make Cisco TMS regularly poll all SNMP-capable systems. The frequency is set in the field below.
System Alive-Status Scan Interval (in seconds)	Specify the frequency of the polling.
Maximum Number of Missed SNMP Responses Before System Is Set to Inaccessible	Specify the number of consecutive failed SNMP poll requests to accept before attempting connection via HTTP. If both connections fail, Cisco TMS will set the connection status to *No SNMP Response*. In networks with high packet loss, this field should be increased from the default, which is 2. As SNMP is a UDP protocol, packet delivery is not guaranteed.
System Force Refresh Interval (in hours)	Control how often Cisco TMS retrieves configurations from managed systems and enforces settings if **Enforce Management Settings on Systems** is set to *Yes*.
SNMP Broadcast Interval (in minutes)	*Legacy systems only.* Specify how many minutes Cisco TMS will wait between successive SNMP scans for system discovery, system status, and call status.
SNMP Broadcast/Multicast Address(es)	Specify the IPv4 broadcast address(es) of the subnet, or the IPv6 multicast address(es) the TMS SNMP Service (TMSSnmpService) is scanning. By default, the SNMP service scans the entire IPv4 network for systems by broadcasting to the IP address "255.255.255.255". ■ If you wish to narrow the broadcast range, change this value. Example: Set the address to "10.0.255.255" to receive responses from systems connected to this subnet only. ■ To scan multiple ranges, use comma separation.

Table 137 Settings on the Network Settings page (continued)

Sections and fields	Description
Enforce Management Settings on Systems	When enabled: ■ The Cisco TMS server address configured in **Advanced Network Settings for Systems on Internal LAN** will be enforced on all systems as a feedback address. This address is also used for phone books and management on Cisco TMS-controlled endpoints. ■ Cisco TMS will use the frequency set in **Administrative tools > Configuration > Network settings > TMS Services > System Force Refresh Interval (in hours)**. **Daylight Saving Time** and **Time Zone** are also enforced on Cisco TMS-controlled endpoints.
Enforce Now	Click to enforce the management settings mentioned above immediately. This has the same effect as clicking **Enforce Management Settings** at the bottom of the **System > Navigator >** Select system **> Settings tab > Edit Settings** page.
Enable Ad Hoc Conference Monitoring	■ If set to *Yes*, Cisco TMS will discover and monitor ad hoc calls for systems managed by Cisco TMS, and they will be viewable in Conference Control Center, page 203. ■ If set to *Only for MCUs*, only ad hoc conferences on MCUs will be shown in **Conference Control Center**. To lower the load on Cisco TMS in large deployments, disable this setting or set to *Only for MCUs*.
Update System Connectivity for Systems	Specify whether Cisco TMS will automatically change a system's connectivity status (for example: *Reachable on LAN*, *Behind Firewall*) if it detects changes to connectivity. ■ *Automatic*: Cisco TMS will change the system's connectivity status as it detects it. ■ *Manual*: Cisco TMS will not change the status. Administrators may change a system's connectivity status themselves by going to **Systems > Navigator >** select a system **> Connection** tab **> System Connectivity**. See also Why Cisco TMS Changes the System Connectivity Status, page 50.
Advanced Network Settings for Systems on Internal LAN	

Table 137 Settings on the Network Settings page (continued)

Sections and fields	Description
TMS Server IPv4 Address	When enforcing management settings on endpoints controlled by Cisco TMS, these addresses will be applied in the following order of preference: ■ FQDN ■ IP address For endpoints controlled by Cisco TMS, these addresses are used as the traphost address, phone book server address, external manager address and external services address. For Cisco TMSPE-provisioned and Unified CM-registered systems the addresses are used as the 'feedback 3' address.
TMS Server IPv6 Address	
TMS Server Fully Qualified Hostname	
Advanced Network Settings for Systems on Public Internet/Behind Firewall	
TMS Server Address (Fully Qualified Hostname or IPv4 Address)	The public FQDN or IP address of the Cisco TMS server, that must be reachable for remote systems. This address is used as the phone book server address, external manager address, and external services address on remote systems.
Automatic Software Update	
Automatically Check for Updates	*Legacy systems only.* ■ If enabled, Cisco TMS will check cisco.com every two days to see if there are new software updates available for legacy systems. The software and corresponding release keys will be downloaded to the location specified in Cisco TMS Tools: **Administrative Tools > General Settings > Software Directory**. ■ If disabled, the **Import Log** button is displayed on the **System Upgrade** page. This enables the import of a list of software and release keys for use when upgrading systems. Once systems have been selected for upgrade, the **Import Log** and **Generate Log** buttons are both displayed in the **Select Software and Release Keys** page. For more details, see System Upgrade, page 155.
Service URL	This is the URL of the software update service at cisco.com and must not be changed.
Web Proxy Address	If there is a proxy server on your network, enter its address here.
Web Proxy Username	A valid username and password for Cisco TMS to use to authenticate to the proxy server.
Web Proxy Password	

Email Settings

In Cisco TMS: **Administrative Tools > Email Settings**

Email

Table 138 Settings in the Email section

Field	Description
Enable Sending of Email	Allow Cisco TMS to send emails to users.
Email Content Type	Allows to choose the type of email that contains the conference details. ■ Plain Text – Sends a plain text email. ■ HTML – Sends an HTML email. ■ Both(Multipart) – Sends plain text and HTML type email in one message. However, it is up to the email client to choose which type of email is displayed to the user.
From Email Address	The email address Cisco TMS will use when sending email notifications. This address will show in the **From** field of the recipient's email client.

SMTP

Table 139 Settings in the SMTP section

SMTP Server	The IP-address or hostname of your SMTP (Mail) server. The default port is 25, but this can be changed by adding :<port number> after the IP address of the server.
SMTP Server Authentication Username (if needed)	A valid username for Cisco TMS to use to connect to the SMTP server if authentication is required.
SMTP Server Authentication Password (if needed)	The password of the account specified in the Username field.

Content

Table 140 Settings in the Content section

Primary SIP Protocol Handler	Identify the protocol handler and application name to list first and second for SIP URI links in conference invitation email, which will allow users to join the conference directly from the email message. For example, entering `sip` and `Jabber` will create a link called "Jabber" that uses the **sip://** protocol handler.
Secondary SIP Protocol Handler	
Web Client URL	Enter a URL and name for a web-based telepresence client if one is available in your environment. Make sure to include the full URL with protocol (http or https) and include a name for the web client, or the link will not be displayed correctly.

Table 140 Settings in the Content section (continued)

Base URL for Icons	The location used for images in HTML e-mail messages is displayed here. The default location will be overwritten on any subsequent upgrades of Cisco TMS. To add or modify image files, opt for a custom location. Make sure this is a trusted location in your organization, or the user's email client may suppress the images.

The **Booking invite preview** updates as you type in the **Handler** and **App** fields, and shows exactly what users will see when they receive the booking invitation email. The links in the preview are clickable.

Edit Email Templates

In Cisco TMS: **Administrative Tools > Configuration > Edit Email Templates**

You can use this page to change the layout and text for all email templates in Cisco TMS. For a reference to the required settings for sending email from Cisco TMS, see Email Settings, page 243.

Template Types

While Cisco TMS allows you to customize any system-generated email including notifications to administrators, this documentation primarily covers the templates used for messages to end users about booking.

Each template exists in two versions, one in HTML and one in plain text. Which version is displayed to the end user depends on:

- The **Email Content Type** setting in **Administrative Tools > Configuration > Email Settings**. The default and recommended setting is *Multipart*, which lets the email client decide.
- The capabilities and configuration of the recipient's mail client. For example, some mobile clients will only display text.

How Templates are Constructed

Both versions of the template are built up of the same types of variable tags and share the same phrase file.

Tag	Description
`{...}`	Curly brackets indicate a phrase tag. You can create, add, and remove phrase tags to any template without restrictions.
`<...>`	Angle brackets indicate a defined content tag. You can move or remove content tags, but not modify or create them, and all content tags are not valid for all templates.
`<SECTION: ...>`	Section tags indicate a content section that will be displayed under defined criteria. For example, `<SECTION:RECURRENCE_INFO>` will only be displayed if the conference is booked with recurrence. Section tags must always be accompanied by a closing tag.
`<FOREACH: ...>`	Foreach tags indicate a content section that will be repeated as many times as there are contents that meet the criteria. For example, `<FOREACH:LOCATION>` will list every telepresence endpoint scheduled for a conference. FOREACH tags must always be accompanied by a closing tag.
`<VAL: ...>`	Value tags indicate a single value that will be displayed if it exists. For example, `<VAL:ADMINISTRATOR>` will include the name of the Cisco TMS administrator/contact person if this information has been configured in Cisco TMS. VAL tags are self-contained and do not require closing.
`<UPPERCASE>`	Enclosing any phrase in this tag will make it display as uppercase. You can use it in plain text templates as well as HTML. The UPPERCASE tag must always be accompanied by a closing tag.

Tag	Description
`<ADD:ICALENDAR_ATTACHMENT>`	Include .ical attachment with email message. This tag can be placed anywhere in the template and is self-contained.
`<VAL:TMS_ICONS_BASE_URL>`	This tag applies the **Base URL for Icons** setting from **Administrative Tools > Configuration > Email Settings > Content**, where all graphics must be located.

In addition to content and phrase tags, HTML templates contain HTML markup and inline styling. If you want special characters such as angle brackets to be visible in the email message, you must use HTML character encoding. For example, use `>` when you want to show >.

Customizing the Templates

How to customize a template depends on what aspects you want to modify:

- Look and feel: The HTML templates use inline styling. To change this, you must modify the markup of each template. Any custom graphics must be added to the location specified in **Administrative Tools > Configuration > Email Settings > Content**.
- Wording: All modifiable wording is in the phrase files that are available in the right-hand pane. You can create your own phrase tags in these phrase files and add them to the corresponding template.
- Content organization: To change the order in which content is presented, you can rearrange and/or remove tags. Note that VAL tags must normally appear inside of a SECTION or FOREACH tag.

While editing email templates, you can:

- See how the message will look in the **Preview** section, making sure to click **Refresh** after changes.
- Revert to the last saved version of a template by clicking **Discard Changes**.
- Delete all modifications to a template by clicking **Revert to Default**.

Booking Email Templates

There are four default booking-related email templates in Cisco TMS

- Booking Invite
- Booking Cancel
- Booking Event
- Booking Failure

Booking Invite Legacy and Booking Cancel Legacy are legacy templates. These legacy templates remain supported for customers who are already using them, but for new users, we strongly recommend using the above templates exclusively.

Booking Invite

```
<VAL:TMS_ICONS_BASE_URL> // Applies the "Base URL for Icons" setting.
<ADD:ICALENDAR_ATTACHMENT> // Adds an .ical invitation to the email notification.

<FOREACH:API_ERROR> // Repeated for each error from Cisco TMSBA (Booking API).
       <VAL:API_ERROR> // The error message.

<SECTION:MEETING_PARTIAL_FAILURE> // Used if a series has defective occurrences.
       <VAL:MEETING_PARTIAL_FAILURE_DESCRIPTION>

       <SECTION:MEETING_PARTIAL_FAILURE_FEW> // Used if there are less than 4 defective occurrences.
              <VAL:MEETING_DEFECTIVE_DATES> // Dates of the occurrences, with suggested actions.
       <SECTION:MEETING_PARTIAL_FAILURE_MANY> // Used if there are more than 3 defective occurrences.
```

```
<SECTION:MEETING_WEBCONF_ERROR> // Used if the Webex part of a booking failed.
       <VAL:MEETING_WEBCONF_ERROR> // The Webex error text.

<SECTION:MEETING_WEBCONF_WARNING> // Any warnings regarding Webex booking.
       <VAL:MEETING_WEBCONF_WARNING> // The Webex-related warning text.

<FOREACH:API_WARNING> // Repeated for each warning from Cisco TMSBA (Booking API).
       <VAL:API_WARNING> // The warning text.

<SECTION:MAIL_HEADING_MCU_FAILOVER> // Used in the case of an MCU failover.

<SECTION:MUST_BE_APPROVED> // Used if the booking is pending approval.


<SECTION:NO_SETUP_BUFFER_WARNING> // Used if Early Join is disabled and {NO_SETUP_BUFFER_MESSAGE} is not
empty in phrase file
       <SECTION:NO_SETUP_BUFFER_WARNING_TEXT> // The relevant text from the phrase file, if available.

<FOREACH:API_INFO> // Informational messages from Cisco TMSBA (Booking API).
       <VAL:API_INFO>

<SECTION:RESERVATION_ONLY> // Used if the conference is of type Reservation.

<SECTION:BOOKEDBYOWNER> // Used if the conference was booked by the conference owner.
       <VAL:OWNER> // The owner.

<SECTION:BOOKEDONBEHALF> // Used if the conference was booked on behalf of the conference owner.
       <VAL:BOOKED_BY> // The person who performed the booking.
       <VAL:OWNER> // The owner.

<SECTION:MEETING_TITLE>        // Used for the conference title, if available.
       <VAL:MEETING_TITLE> // The conference title.

<SECTION:RECURRENCE_ICON> // Includes an icon if conference is recurrent.
<SECTION:RECURRENCE_INFO> // Used if conference is recurrent.
       <VAL:RECURRENCE_INFO> // The recurrence pattern information.

<VAL:MEETING_DATE_TIME> // The conference date and time.
<VAL:MEETING_TIME_ZONE> // The conference time zone.
<VAL:OWNEREMAILADDRESS> // Use meeting owner email address
<VAL:OWNERPHONENUMBER> //  Use meeting owner phone number

<SECTION:MEETING_MESSAGE> // Displays the text from the Meeting Message field, if available.
       <VAL:MEETING_MESSAGE> // The meeting message (agenda).
<SECTION:NO_MEETING_MESSAGE> // Used if no meeting message (agenda) is available.

<SECTION:MEETING_WEBCONF_DETAILS> // Used if conference includes Webex.
       <VAL:ATTENDANT_URL> // The attendant URL
       <SECTION:WEBCONF_PASSWORD> // The Webex password if not hidden.
              <VAL:WEBCONF_PASSWORD>
       <SECTION:WEBCONF_HIDDEN_PASSWORD> // Used if the Webex password is hidden.
       <VAL:WEBCONF_ID>

<SECTION:TELEPRESENCE> // Used if the conference has a telepresence component.
       <SECTION:TP_ONLY_TITLE> // Used for telepresence-only conferences.
       <SECTION:TP_COMBINED_TITLE> // Used for CMR Hybrid conferences.
       <SECTION:JOIN_FROM_LINKS> // Used if protocol handlers or a web client URL have been defined.
              <SECTION:JOIN_WITH_APPS> // Used if protocol handlers are defined.
                     <SECTION:SIP_HANDLER1> // LPrimary protocol handler, if defined.
                            <VAL:SIP_HANDLER1_URI>
                            <VAL:SIP_HANDLER1_LABEL>
                     <SECTION:SIP_HANDLER2> // Secondary protocol handler, if defined.
                            <VAL:SIP_HANDLER2_URI>
                            <VAL:SIP_HANDLER2_LABEL>
```

```
                        <SECTION:WEB_CLIENT1> // Web client, if defined.
                                <VAL:WEB_CLIENT1_URL>
                                <VAL:WEB_CLIENT1_LABEL>
                <SECTION:VIDEO_ADDRESS> // Used if there is at least one video address.
                        <SECTION:VIDEO_ADDRESS_TITLE> // Used if there is only one protocol.
                        <FOREACH:VIDEO_ADDRESS_PROTOCOL> // Repeated for each protocol available.
                                <SECTION:PROTOCOL> // Used if there is more than one protocol.
                                        <VAL:PROTOCOL>
                                <FOREACH:ZONE> // Repeated for every TMS zone used in a video address.
                                        <SECTION:ZONE> // Used if there is more than one zone.
                                                <VAL:ZONE>
                                        <FOREACH:VIDEO_ADDRESS> // Repeated for every video address.
                                                <VAL:VIDEO_ADDRESS>
                <SECTION:CMS_WEBBRIDGE_ADDRESS; // The conference is hosted on CMS and webbridge URI is configured.
                                        <VAL:CMS_WEBBRIDGE_ADDRESS>
                <SECTION:MEETING_CONFERENCEME> // The conference is on a ConferenceMe-enabled TelePresence MCU.
                        <VAL:CONFERENCEME_URL> // The ConferenceMe URL.
                <SECTION:MEETING_CONFERENCESTREAMING> // Used if conference is on a streaming-enabled TelePresence MCU.
                        <VAL:CONFERENCESTREAMING_URL> // The streaming URL.
                <SECTION:MEETING_PASSWORD> // Used if conference has a PIN code.
                        <VAL:MEETING_PASSWORD> // The conference PIN.
                <SECTION:LOCATIONS> // Used if telepresence endpoints are scheduled.
                        <FOREACH:LOCATION> // Repeated for each scheduled telepresence endpoint.
                                <VAL:LOCATION> // The endpoint name.

        <SECTION:WEBEX_AUDIO> // Used if conference includes Webex.
                <SECTION:WEBCONF_LOCAL_CALL_IN_TOLL_NUMBER> // Used if the country has a local call-in toll number.
                        <VAL:WEBCONF_LOCAL_CALL_IN_TOLL_NUMBER> // The call-in toll number.
                <SECTION:WEBCONF_LOCAL_CALL_IN_TOLL_FREE_NUMBER> // Used if the country has a local call-in toll-free
number
                        <VAL:WEBCONF_LOCAL_CALL_IN_TOLL_FREE_NUMBER> // The call-in toll-free number.
                 <VAL:WEBCONF_ACCESS_CODE> // The access code for the Webex conference.
                <SECTION:WEBCONF_GLOBAL_CALL_IN_NUMBER_URL> // Used if the Webex conference has a global call-in URL.
                        <VAL:WEBCONF_GLOBAL_CALL_IN_NUMBER_URL> // The global call-in URL.
                <SECTION:WEBCONF_TOLL_FREE_RESTRICTIONS_LINK> // A link to the restrictions on toll-free calls.

        <SECTION_WEBEX_HELP> // Used if conference includes Webex.
                <VAL:PRESENTER_URL> // The presenter URL.

        <SECTION:TMS_CONFERENCE_URL> // Used if a Cisco TMS conference URL is configured.
                <VAL:TMS_CONFERENCE_URL> // The Cisco TMS conference URL URL.

        <SECTION:MEETING_RECORDING_FOOTER> // Used if recording is set up for the meeting.
                <VAL:RECORDING_URL> // The recording URL.

        <SECTION:WEBEX_NOTICE> // Used if the meeting includes Webex.
```

Legacy sections and values

```
        <SECTION:MEETING_RECORDING> // Used if recording is set up for the conference.
                <VAL:RECORDING_URL> // The recording URL.
```

Option Value

```
        <VAL:NUMERIC_ID> // To be used if the meeting includes a numeric  dial number and can be used only inside
        <FOREACH:VIDEO_ADDRESS> section of the Booking invite.
```

Booking Cancel

Used when a conference is cancelled.

```
        <SECTION:MEETING_TITLE> // Used if conference has a title.
                <VAL:MEETING_TITLE> // The conference title.
```

```
<SECTION:RECURRENCE_INFO> // Used if conference is recurrent.
       <VAL:RECURRENCE_INFO> // The recurrence pattern information.
<VAL:MEETING_DATE_TIME> // The conference date and time.
<VAL:MEETING_TIME_ZONE> // The conference time zone.
<VAL:OWNEREMAILADDRESS>  // The conference owner email address
<VAL:OWNERPHONENUMBER>  //  The conference owner phone number

<VAL:OWNER> // The conference owner.
<VAL:DELETED_BY_EMAILADDRESS>  // Email address of the user who deleted the conference
<VAL:DELETED_BY_PHONENUMBER>  //  Phone number of the user who deleted the conference
```

Booking Event

```
<SECTION:ERROR> // Used if event is an error.
       <VAL:MESSAGE>

<SECTION:WARNING> // Used if event is a warning.
       <VAL:MESSAGE>

<SECTION:INFO> // Used if event is informational.
       <VAL:MESSAGE>

<VAL:PROPOSED_ACTION> // Proposed action for the user.
<VAL:FAILURE_DESCRIPTION> // A description of the problem.

<VAL:MEETING_TITLE> // The meeting title.
<SECTION:RECURRENCE_INFO> // Used if conference is recurrent.
       <VAL:RECURRENCE_INFO> // The recurrence pattern information.
<VAL:MEETING_DATE_TIME> // The conference date and time.
<VAL:MEETING_TIME_ZONE> // The conference time zone.

<SECTION:HOST> // Used if the conference has a host.
        <VAL:HOST> // The host.

<SECTION:ADMINISTRATOR> // Used if an administrator is defined with contact information in Cisco TMS.
       <VAL:ADMINISTRATOR> // The administrator's name.
       <VAL:EMAIL> // The administrator's email adress.
```

Booking Failure

Used when booking fails.

```
<VAL:PROPOSED_ACTION> // The proposed action for dealing with the  conference.
<VAL:FAILURE_DESCRIPTION> // A description of the problem.

<VAL:MEETING_TITLE> // The meeting title.
<SECTION:RECURRENCE_INFO> // Used if conference is recurrent.
       <VAL:RECURRENCE_INFO> // The recurrence pattern information.
<VAL:MEETING_DATE_TIME> // The conference date and time.
<VAL:MEETING_TIME_ZONE> // The conference time zone.

<VAL:HOST> // The host.

<SECTION:ADMINISTRATOR> // Used if an administrator is defined with contact information in Cisco TMS.
       <VAL:ADMINISTRATOR> // The administrator's name.
       <VAL:EMAIL> // The administrator's email adress.
```

Conference Settings

In Cisco TMS: **Administrative Tools > Configuration > Conference Settings**

On this page you can specify settings that will apply to all scheduled conferences in Cisco TMS as default. Changes can be made to individual conference settings during booking.

Conference Display

Table 141 Settings in the Conference Display section

Field	Description
Show Network Products in Ad Hoc Booking	Specify whether infrastructure products such as gateways, MCUs and VCSs will be visible in Ad Hoc Booking.

Conference Creation

Table 142 Settings in the Conference Creation section

Field	Description
Default Conference Title	The default title used for all booked meetings is set to *Scheduled Meeting*. You can also edit the default title by clicking on the text box. If you want a time and date stamp in the title, enter *%DATE% %TIME%* together with the title.
Default Scheduled Call Duration (in minutes)	Specify the default conference duration for scheduled calls.
Default Immersive Bandwidth	This bandwidth will be used between any two immersive participants in a scheduled conference (T3, T1, CTS, TX, IX or TelePresence Server systems, Cisco Meeting Server and TelePresence Conductor aliases with **Prefer for Multiscreen** selected). This is to ensure that immersive conferences have sufficient bandwidth for multiple codecs/screens. Other system types in the same conference will use the bandwidth defined in the **Default Bandwidth** setting.
Default IP Bandwidth	The default IP bandwidth for scheduled conferences. It is possible to adjust this bandwidth during booking.
Default ISDN Bandwidth	The default ISDN bandwidth for scheduled conferences. It is possible to adjust this bandwidth during booking.
Default Picture Mode	Specify the default picture mode for scheduled conferences: ■ *Voice Switched* ■ *Continuous Presence* ■ *Enhanced Continuous Presence* This setting does not apply to Cisco TelePresence MCU, Cisco TelePresence Server and Cisco TelePresence Conductor.

Table 142 Settings in the Conference Creation section (continued)

Field	Description
Default Reservation Type for Scheduled Calls	Specify the default reservation type for scheduled conferences: ■ *Automatic Connect*: The conference is routed and launched automatically. ■ *One Button to Push*: The conference is routed and ready to launch using One Button to Push on supported endpoints. ■ *Manual Connect*: Conference routing is set up, and the video conference master must launch the conference. ■ *No Connect*: Routing for the conference is set up, and participants must connect themselves. ■ *Reservation*: Only the systems are reserved. No routing is attempted.
Set Conferences as Secure by Default	Specify that scheduled conferences will be booked as encrypted by default. If set to *Yes*, you can change individual conferences to be unencrypted during booking. **Note:** If an endpoint that supports encryption has encryption set to *Off* and is added to a conference which is encrypted, encryption will be set on the endpoint, and this setting will persist after the conference has ended, until set to *Off* on the endpoint itself.
Auto Generate PIN on New Conferences	Specify that you want Cisco TMS to auto-generate a conference PIN for scheduled calls.
Auto Generated PIN Length	Specify the number of digits Cisco TMS will include when auto-generating a conference PIN. The default value is 3.
Billing Code for Scheduled Calls	Specify whether to apply billing codes to scheduled calls. ■ *No*–billing codes entered during booking will not be applied. ■ *Optional*–any billing code can be entered during booking. ■ *Required*–a billing code matching the list in **Administrative Tools > Billing Codes > Manage Billing Codes** must be entered during booking. See Manage Billing Codes, page 280.
Enable Billing Code Selection Popup	■ *Yes*: A button will be displayed next to the field **Billing Code** in **Booking > New Conference > Advanced Settings**. The button launches the **Billing Code Selection Popup**. ■ *No*: The button will not be displayed.
Booking Window (in days)	Specify the maximum number of days into the future that users are allowed to schedule conferences.
Default Conference Language	Specify the language for all conference email, and in-video meeting end notifications.

Conference Connection

Table 143 Settings in the Conference Connection section

Field	Description
Allocation Attempts for Scheduled Calls	The number of times Cisco TMS will attempt to allocate the call on the bridge. The default value is 4.
Connection Attempts for Scheduled Calls	The number of times Cisco TMS will keep trying to connect if a call is not initially successful. Cisco TMS will not continue trying to connect if the user rejects the call. The default value is 4.
Connection Timeout for Scheduled Calls and Allocation (in seconds)	The number of seconds to wait for a successful allocation and connection. If a system does not respond within this time, the call will be disconnected and retried the number of times set in **Connection Attempts for Scheduled Calls** and **Allocation Attempts for Scheduled Calls**. The default value is 30. Cisco TMS will wait at least as long as the value set here. Note that the timeout is not capped so it could take longer that the value set here before the next allocation is attempted.
Allow Participants to Join Early	Set to *Yes* to enable a best-effort feature that starts conferences 5, 10 and 15 minutes before the scheduled start time. Participants can then join the conference up to 5, 10 and 15 minutes early. Note: If two back-to-back meetings are created with early join option enabled and use same endpoints, then editing (reducing) of first meeting's end-time is possible before the early-join start time of second meeting (not permitted to set any time within early join period of second meeting).
Join Early time for participants (in minutes)	Select the early join time of the meeting that is 5, 10 or 15 minutes.
Ignore Scheduled Meeting and Continue Active Call	If this feature is set to *Yes*, then Cisco TMS will not disconnect the active call on an endpoint at the time of a scheduled meeting allocation. The Endpoint will still get the scheduled meeting's incoming call and the endpoint can choose to join or ignore the incoming call. This feature works only: ▪ When the next scheduled meeting type is **Automatic Connect**. ▪ When the call direction is from bridge to endpoint. This feature is for the following scenarios: ▪ Endpoint has ongoing adhoc call which conflicts with a scheduled call. ▪ Endpoint has ongoing scheduled call which conflicts with another scheduled call where the **Resource Availability Check on Extension** option is set to **Ignore** in **Administrative Tools > Configuration > Conference Settings > Conference Extension**.

Conference Extension

Table 144 Settings in the Conference Extension section

Field	Description
Contact Information to Extend Meetings	Cisco TMS displays a Meeting End notification on systems before the end of a conference. The message will be displayed according to the minutes entered in the setting **Show Message X Minutes Before End**. This field allows you to customize what follows the Meeting End notification. You can enter contact information such as the telephone number or name of a contact person who can extend the meeting for you. The text configured here applies to both the in-video warnings about conference end sent from bridges to all participants in a conference, and to Meeting End notifications sent to individual participants by Cisco TMS.
Supply Contact Information on Extend Meeting Scheduling Conflict	Select *Yes* if you want participants to see contact information when a meeting extension is not possible due to a booking conflict.
Extend Conference Mode	▪ *None*: Ensure that meetings are never automatically extended . ▪ *Endpoint Prompt*: Display a non-configurable Extend Meeting message on the Video Conference Master both 5 minutes and 1 minute prior to the end time of the conference. ▪ *Automatic Best Effort*: Enable automatic extension of scheduled conferences by 15 minutes up to a maximum of 16 times. The meeting will be extended irrespective of the number of participants connected in the conference only for the first auto extension. The subsequent extensions happen only if more than one participants are connected in the conference. The meeting extension happens only, when there are no conflicting meetings for any of the participants within the next 15 minutes, unless **Resource Availability Check on Extension** is set to *Ignore*.
Maximum Number of Automatic 15-minute Extensions	The number of times the conference will automatically extend by 15 minutes when **Extend Conference Mode** is set to *Endpoint Prompt* or *Automatic Best Effort*. The maximum number possible is 16.

Table 144 Settings in the Conference Extension section (continued)

Field	Description
Resource Availability Check on Extension	▪ *Best Effort*: Conferences will only automatically extend beyond the scheduled end time on a best effort basis if all resources are available for the next 15 minutes. ▪ *Ignore*: – Cisco TMS will ignore the resource availability check, and conferences will automatically extend beyond the scheduled end time regardless of whether all the resources are available or not. The only exception to this is if the port used on the main participant clashes with another conference that takes place during that extended time – in that case the conference will not be extended. – Use this setting with caution: participants may be unable to join new conferences or could be downgraded from video to audio if resources are still in use by the previous conference. However, conferences will always be allocated: if extending the conference would block a new conference from being able to start (for example, by using the same URI on the bridge), the extension will not take place. – Do not use this setting if your conferences are of **Type**: *Automatic Connect*.

Conference Ending

Table 145 Settings in the Conference Ending section

Field	Description
Message Timeout	The default time (in seconds) that a message should be shown on an endpoint. The default value is 10.
Show Message X Minutes Before End	Specify how many minutes before the end of a conference the Meeting End notification will appear. This message can be shown multiple times by separating the minutes with a comma. For example 1,5 will display the message 5 minutes and 1 minute before the conference is scheduled to end. If the **Show In-Video Warnings About Conference Ending** setting is disabled, Meeting End notifications including the **Contact Information to Extend Meetings** text will still be displayed for individual participants. Not all systems can display individual Meeting End notifications. **Note:** For TelePresence MPS bridges, only 10, 5 and 1 can be entered here and will be displayed as a number icon on the screen. All other systems can be configured with any number intervals, and will show the Meeting End notification followed by the text string entered in **Contact Information to Extend Meetings**.
Show Reconnect Message Box on Endpoints	If enabled, Cisco TMS will display a reconnect message on Cisco systems if a scheduled call disconnects before the conference end time. The message will be displayed ten seconds after Cisco TMS has discovered the disconnected call, and only if the call is not disconnected by Cisco TMS.

Table 145 Settings in the Conference Ending section (continued)

Field	Description
Show In-Video Warnings About Conference Ending	If enabled, remote participants will receive an in-video warning about conference ending. The warning will be displayed according to the minutes entered in the setting **Show Message X Minutes Before End**. This setting applies only to multipoint conferences hosted on a bridge.
Show Messages On Endpoints About Conference Starting In X Minutes	If enabled, conference participants will be notified on their endpoint at predefined intervals of 5 and 1 minute(s) before the conference start time, that the conference is about to start.
Endpoint message anonymization	Optionally hide the username/ID of the administrator in messages. ■ *None*: Username/ID will be published. ■ *End conference messages*: Username/ID of the administrator will be hidden in the end conference messages ■ *All messages*: Username/ID of the administrator will be hidden in all messages sent.

Advanced

Table 146 Settings in the Advanced section

Field	Description
External MCU Usage in Routing	Specify whether Cisco TMS will use an external MCU when booking a conference. ■ *Only if needed* - Prefer the embedded MCU on the endpoint if available. ■ *Always, except point to point* - Always use an external MCU, except for point to point calls. ■ *Always* - Always use an external MCU, including point to point calls.
Preferred MCU Type in Routing	Define which MCU type Cisco TMS will prefer as default when creating a conference. When booking Immersive TelePresence conferences, a TelePresence Server, TelePresence Conductor, Cisco Meeting Server, or immersive unmanaged bridge (in that order) will always be preferred by Cisco TMS regardless of the setting here, as long as enough resource is available. Note that other factors can affect and override this setting, for more details see The Main Participant, page 32.
Preferred Protocol in Routing	Specify the protocol that is used in routing a conference either H.323 or SIP protocol. On an upgrade, H.323 is set as the default protocol and for new installations SIP is set as the default protocol.

Table 146 Settings in the Advanced section (continued)

Field	Description
Use Flat H.323 Dialing Plan When Routing Calls	The Flat H.323 Dial Plan option is used to disable the Gatekeeper neighbor checking logic in call routing. *On*: Configures Cisco TMS to assume a 'flat' dial plan, where all aliases can be dialed without prefixes no matter which Gatekeeper a device is registered to. When set to *On*, no Gatekeeper comparison is done in call routing. This is useful for situations where Cisco TMS is not managing the Gatekeepers so the neighbor checking can not be performed, or where Gatekeepers are not direct neighbors to each other (hierarchical or multi-legged paths). Neighbor Zone prefixes read from Gatekeepers are not used in call routing when this option is set to *On*. *Off*: Cisco TMS determines whether gatekeepers are compatible by checking whether the call participants are registered to the same gatekeeper, or whether the gatekeepers are direct neighbors. Cisco TMS determines whether an alias can be reached between gatekeepers and will insert E.164 dialing prefixes for neighbor zones if required by the gatekeeper's configuration. If Cisco TMS fails this neighbor check, it is assumed the call can not be made with H.323 aliases and alias options will not be given as a valid call routes.
Prefer H.323 ID over E.164 Alias	▪ *Yes*: H.323 ID will be favored over E.164 aliases when routing H.323 calls. ▪ *No*: E.164 aliases will be favored over H.323 ID when routing H.323 calls.
Send Warning When Ad Hoc Conferences Exceed This Duration (in hours)	A conference event is triggered in **Conference Control Center** when the duration of an Ad Hoc conference has exceeded the set time limit (in hours). Set to 0 to disable (no event will be triggered).
Send Warning When Auto Attendant Conferences Exceed This Duration (in seconds)	A conference event is triggered in **Conference Control Center** when the duration of an MCU Auto Attendant conference has exceeded the set time limit (in seconds). Set to 0 to disable (no event will be triggered).
Automatic MCU Failover	▪ *Off*: Cisco TMS will not initiate automatic MCU failover. ▪ *If conference start fails*: Cisco TMS will automatically try another MCU if conference setup fails during conference start. ▪ *If conference start or MCU polling fails*: Cisco TMS will automatically try another MCU if conference setup fails during conference start, or if the MCU is unresponsive during the conference. For failover threshold, see the field below. We do not recommend using this setting, as Cisco TMS could disconnect all participants from a conference if the network connection to the hosting MCU is lost for a short time, despite the conference having continued with no problem. This setting is ignored for conferences hosted on a TelePresence Conductor. **Note:** Automatic MCU Failover is only supported for scheduled conferences where the main participant is an MCU or a TelePresence Conductor. It is not supported for cascaded conferences hosted on direct managed MCUs.

Table 146 Settings in the Advanced section (continued)

Field	Description
Automatic MCU Failover Threshold (seconds after first poll failure)	Specify the number of seconds Cisco TMS will wait after the first poll failure before MCU failover is executed.

WebEx Hybrid Settings

In Cisco TMS: **Administrative Tools > Configuration > WebEx Hybrid Settings**

On the **WebEx Hybrid Settings** page, you add Webex sites to Cisco TMS and configure them.

Note that to be able to add WebEx Hybrid in telepresence conferences, a **WebEx Site**, **WebEx Username**, and **WebEx Password** must also be set up for each conference owner in Cisco TMS, and your telepresence deployment must be set up to support CMR Hybrid.

- For information on the user settings for WebEx Hybrid, see Users, page 273.
- For guidance on setting up CMR Hybrid with Cisco TMS, see *Cisco Collaboration Meeting Rooms Hybrid Configuration Guide*.

Caution: **Cisco Meeting Server users should not enable WebEx Hybrid. As WebEx Hybrid settings are exclusively set for integration of legacy bridges/TelePresence Conductor/ Server and not for Cisco Meeting Server.**

WebEx Configuration

Table 147 General WebEx Hybrid settings for Cisco TMS

Field	Description
Enable WebEx Hybrid	▪ *Yes*: Conferences can include Webex. ▪ *No*: Conferences cannot include Webex.
Add WebEx Hybrid to All Conferences	▪ *Yes*: All conferences will include WebEx Hybrid by default. In the booking pages, the **Include WebEx Hybrid Conference** checkbox will be checked, but can be cleared. ▪ *No*: This checkbox is by default cleared.
Get WebEx Username from Active Directory	Enable AD lookup before selecting this field. To enable AD lookup, see Enabling Active Directory Lookup, page 24. The AD attribute used to look up the Webex username must correspond to the username in WebEx Hybrid. ▪ *Disabled*: Username lookup is disabled. ▪ *Username (SamAccountName)* ▪ *Email (mail)* ▪ *Custom Attribute*: If the Webex Username matches a different attribute in AD, enter the name of the attribute here.

WebEx Sites

The list of sites displays the site name and hostname for each site added. A green checkmark indicates the default Webex site.

The default site is automatically set on *new* Cisco TMS users if the **Get WebEx Username from Active Directory** option is enabled.

WebEx Site Configuration

Click the **Add Site** button to display these settings.

Table 148 Configuration options for each WebEx site

Field	Description
Site URL	The site URL. This is a combination of the **Hostname** and **Site name**. Example: `https://hostname.webex.com/sitename`.
Hostname	The name of the host server for the Webex site above.
Site Name	The name of the Webex site.
Webex Participant Bandwidth	Use this field to specify the available bandwidth for the Webex participants. For specification on value, see the MCU documentation.
Default Site	The default site is automatically set on *new* Cisco TMS users if the **Get WebEx Username from Active Directory** option is enabled.
TSP Audio	■ *Yes*: Enable this if your Webex site is set to use PSTN (Public switched telephone network). PSTN gives the conferences an extra port for audio during conferences. (TSP - Telephony Service Provider). The audio line used will not be encrypted. ■ *No*: SIP will be used for both video and audio.
Use Web Proxy	■ *Yes*: Enable this if your network uses a web proxy to exit the intranet. A **Web Proxy Configuration** will be displayed with three fields: – **Web Proxy Address** (mandatory) – **Web Proxy Username** – **Web Proxy Password** ■ *No*: WebEx Hybrid can be reached without using a proxy.
Enable SSO	Enable this if configuring CMR Hybrid to use single sign-on. For instructions, see *Cisco Collaboration Meeting Rooms Hybrid Configuration Guide*
Connection Status	This field displays the status of the connection between Cisco TMS and the Webex site.

SSO Configuration

Table 149 Configuration options for single sign-on (SSO)

Field	Description
Certificate	This field displays the certificate that ensures safe transfer of data between Cisco TMS and WebEx Hybrid for single sign-on. This certificate must be sent to the Webex administrator to set up the trust relationship between Cisco TMS and WebEx Hybrid.
Upload Certificate	Browse to upload certificate. For guidance on certificates, see *Cisco Collaboration Meeting Rooms Hybrid Configuration Guide*.

Table 149 Configuration options for single sign-on (SSO) (continued)

Field	Description
Certificate Password	Provided by the Webex Cloud Services team.
Partner Name	Usually the name of the company deploying Cisco Collaboration Meeting Rooms Hybrid. Must be determined or approved by the Webex team, because the value must be unique. Provided by the Webex Cloud Services team.
Partner Issuer (IdP ID)	Identity Provider ID. This value is normally determined by the Cisco TMS administrator, because the Identity Provider is Cisco TMS. Provided by the Webex Cloud Services team.
SAML Issuer (SP ID)	Service Provider ID. This value is normally determined by Webex, because the Service Provider is Webex. Provided by the Webex Cloud Services team.
AuthContextClassRef	This is the authentication context. The IdP authenticates the user in different contexts, such as X509 cert, Smart card, IWA, username/password). Provided by the Webex Cloud Services team.

Reporting Settings

In Cisco TMS: **Administrative Tools > Configuration > Reporting Settings**

On this page you define general settings used by the statistics found in Reporting, page 226.

Table 150 Settings for reports generated in Reporting

Field	Description
Reporting History (in days)	Set the default date range used for statistics. Only data for the last Statistics History days will be shown by default.
Reporting Default Start Time	The default start time for statistics.
Reporting Default End Time	The default end time for statistics.

Provisioning Extension Settings

In Cisco TMS: **Administrative Tools > Configuration > Provisioning Extension Settings**

This page will only be available in Cisco TMS if Cisco TelePresence Management Suite Provisioning Extension is installed and activated on the system. For more information, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* for your environment.

Table 151 Buttons on the Provisioning Extension Settings page

Button	Description
Save	Save all changes to settings within the section.
Cancel	Cancel any unsaved changes to settings within the section.
Restore Default	Restore all settings in the section to the default.

Account Information Email

Table 152 Settings for account information email sent to users

Field	Description
Sender Address	The email address that the users will receive their provisioning account email messages from.
Subject	The subject of the provisioning account information email sent to users.
Body	Template for the message body. The following placeholders are supported: ■ `{display_name}` - the display name of the recipient ■ `{username}` - provisioning username ■ `{password}` - provisioning password ■ `{video_address}` - the SIP URI of the recipient
SMTP Hostname	Hostname of the SMTP server.
SMTP Port	Port to use for the SMTP server.
SMTP Username	Username for the SMTP server.
SMTP Password	Password for the SMTP server.

User Repository

Table 153 Settings for the Cisco TMSPEuser repository

Field	Description
Enable Password Generation	If set to *Yes*, new passwords will be generated automatically.
Password Length	The number of characters that generated password will have.
Password Generation Scheme	Passwords can be generated as one of the following: ■ *Numeric* ■ *Alphanumeric*
Enable automatic email sending to imported user	Specify whether account information should be automatically emailed to new users upon import from Active Directory. The default setting is *No*.

Collaboration Meeting Room

Table 154 Settings for Collaboration Meeting Room

Field	Description
Allow Webex Connections	Enable **Allow Webex Connections** to make CMR templates contain an option to **Include Webex**. This setting requires CMR Hybrid to be deployed. For further detail about adding Webex to a CMR, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* for your environment.

Table 154 Settings for Collaboration Meeting Room (continued)

Field	Description
Allow Active Meeting Manager	Set to *Yes* to enable Active Meeting Manager in CMR self-service portal. Set to *No* to disable Active Meeting Manager in CMR self-service portal.

Smart Scheduler

Table 155 Settings for Multiple Protocol Support

Field	Description
Add Video Call-In-SIP	Set to *Yes* to enable video call in for SIP users. By default, this option is selected for video call in participants.
Add Video Call-In-IP	Set to *Yes* to enable video call in for IP users.
Add Video Call-In-ISDN	Set to *Yes* to enable video call in for ISDN users.
Add Audio Call-In-ISDN	Set to *Yes* to enable Audio call in for ISDN users.
Add Audio Call-In-SIP	Set to *Yes* to enable Audio call in for SIP users. By default, this option is selected for audio call in participants.
Add Audio Call-In-IP	Set to *Yes* to enable Audio call in for IP users.

FindMe

Table 156 Settings for FindMe

Field	Description
Enable FindMe	Set to *Yes* to enable FindMe functionality. Note that this requires a FindMe option key to be installed on Cisco VCS.
Provisioned Devices	Specify whether devices should be automatically added to FindMe as they are provisioned: ■ *Add to user's device list* – when a device is first provisioned, it will be added to the user's FindMe device list. ■ *Set as default device for user's active location* – when a device is first provisioned, it will be added to the user's active FindMe location as a default device ("Initial Ring" in the FindMe user portal). It will also be added to the user's device list. ■ *Do not include* – devices will not be automatically added to FindMe when provisioned.

Cisco TMS Connection

Table 157 Settings for connecting Cisco TMSPE to Cisco TMS

Field	Description
HTTPS	Set to *Yes* for secure communication with Cisco TMS.

Table 157 Settings for connecting Cisco TMSPE to Cisco TMS (continued)

Field	Description
Connection Timeout	Timeout in seconds when connecting to Cisco TMS.
Receive Timeout	Receive timeout for Cisco TMS in seconds.
Hostname	The hostname of the Cisco TMS server. You only need to edit this field if the hostname has previously been erroneously configured as something other than `localhost`.
Username	Username of an account that is a member of the site administrator's group in Cisco TMS.
Password	Password for the above account.

LDAP Connection

Table 158 LDAP connection settings

Field	Description
Follow Referrals	Set to *Yes* to follow naming referrals automatically.
LDAP Connection Timeout	Timeout in milliseconds when connecting to the LDAP server.

Active Directory Connection

Table 159 AD connection settings

Field	Description
Connection Timeout	Timeout in milliseconds when connecting to Active Directory.
Filter Template	Define a filter template for the user import from Active Directory. Append `%s` as a placeholder for the search filter that can be defined per group.
Follow Referrals	Set to *Yes* to follow naming referrals automatically.

Manage Ticket Error Levels

In Cisco TMS: **Administrative Tools > Configuration > Manage Ticket Error Levels**

Change the ticket error levels to reflect the importance you want to give the errors in Cisco TMS.

Note: The error levels are common for all users in Cisco TMS and cannot be defined per user.

Changing the error levels will affect how the tickets are shown in Cisco TMS and in the Ticketing Service. Setting a ticket type to *Not an error* will stop Cisco TMS from showing this ticket.

If you only want to stop Cisco TMS showing tickets for selected systems rather than all systems of a particular type, you can use ticket filters instead. See Ticketing Service, page 138 for more information.

Table 160 Ticket errors with descriptions

Ticket error	Description

Table 160 Ticket errors with descriptions (continued)

Active Gatekeeper Address Blank	The gatekeeper settings are configured incorrectly. The active gatekeeper address is blank.
Aliases Not Associated With Working Service Preference	One or more aliases do not match any conference aliases on TelePresence Conductor.
Approaching Limit for Provisioning Licenses	This ticket applies to Cisco TMSPE. There are only (no) available provisioning licenses left (out of a total of (no) licenses). When there are no more licenses, additional clients/devices will be denied registration. Note that this ticket will not be cleared automatically and must either be acknowledged or deleted.
Auto Answer Off	Auto answer is switched off on the system. This means that Cisco TMS will not be able to auto connect incoming calls on this system.
Bandwidth Error	No bandwidth is defined on the system
Blank System Name	The name of the system is blank.
Certificate Validation Error	There is an error with the system's certificate.
E.164 Alias or H.323 ID, but no IP Bandwidth	An E.164 alias or H.323 ID is specified on system, but the system is configured without IP Bandwidth.
E.164 Alias, but no IP Bandwidth	An E.164 number is specified on system, but the system is configured without IP Bandwidth.
Gatekeeper Configuration Error	The gatekeeper settings are configured incorrectly.
Gatekeeper ID Registration Disabled	Gatekeeper ID registration has been disabled.
Gatekeeper Mode Off	The system has gatekeeper mode off. It is not possible to use E.164 aliases for dialing this system.
Gatekeeper Registration Failure	The system has failed to register on the gatekeeper.
Hostname Mismatch	The hostname of the system in Cisco TMS does not match the hostname of the system itself.
HTTP Error	There is a problem with the HTTP communication between Cisco TMS and the system.
HTTPS Connection Error	Cisco TMS could not contact the system using HTTPS.
Incorrect Authentication Information	The authentication information stored in Cisco TMS for this system is incorrect.
Incorrect Feedback Address	The feedback address on the system is incorrectly configured. Call status and reporting may be incorrect.

Table 160 Ticket errors with descriptions (continued)

Incorrect Management Address	The management address on the system is incorrectly configured. Call status and reporting may be incorrect.
Incorrect Provisioning Mode	The **Provisioned** setting in Cisco TMS **Systems > Navigator >** Select system **> Settings > General** pane does not match the Provisioning Mode setting on the system. Either: ■ The field Provisioned is disabled in Cisco TMS for this system but on the system itself, the Provisioning Mode is set to VCS. Provisioning Mode on the system must be set to TMS. Go to **Systems > Navigator >** Select system **> Settings > Edit Settings > General** pane. Correct the field **Provisioned**. Click **Enforce Management Settings** to apply the new setting, or correct the Provisioning Mode manually on the system. or ■ The field Provisioned is enabled in Cisco TMS for this system but on the system itself, the Provisioning Mode is set to TMS. Provisioning Mode on the system must be set to VCS. Correct the Provisioning Mode manually on the system.
Incorrect SNMP CN	The system has an incorrect SNMP Community Name
Incorrect SNMP Traphost	The SNMP Traphost on the system is incorrectly configured. Call status and reporting may be incorrect for this system
Invalid MCU Prefix Configuration	If the **MCU Service Prefix** and **Prefix for MCU Registrations** settings in the MCU are defined, both prefixes must be the same value so Cisco TMS can properly resolve cascaded MCU conferences.
IP Bandwidth Configuration Error	System is set up to accept IP calls, but there is no IP Bandwidth available.
IP Zone Not Set	IP Zone is not set for this system. Cisco TMS may therefore not be able to book H.323 calls with this system.
ISDN Configuration Error	The ISDN settings on the system are configured incorrectly.
ISDN Zone Not Set	ISDN Zone is not set for this system. Cisco TMS will therefore not be able to book ISDN calls with this system.
Low Battery on Remote Control	The endpoint has indicated that the batteries on the remote control need changing.
Low Diskspace on System	The system is running out of disk space.
Low Diskspace on TMS Web Server	The Cisco TMS server is running out of disk space.
Missing E.164 Alias	At least one E.164 alias is missing.
Missing E.164 Alias and H.323 ID	At least one port is missing both an E.164 Alias and H.323 ID.
Missing ISDN Number	The system is configured with ISDN Bandwidth, but no ISDN number is set on system.

Table 160 Ticket errors with descriptions (continued)

New Movi Client software available	There is a new version of the Jabber Video client available. The ticket will tell you where to download the setup file.
New Software Available	There is a new software version available. The software package is downloaded automatically from the Cisco software repository. The release key is included in the ticket.
No Bookable Aliases Configured	You have not configured any bookable Cisco TelePresence Conductor aliases.
No ISDN Bandwidth	The system is configured with an ISDN number, but there is no ISDN Bandwidth available.
No Ports Defined	There are no ports defined on this system. Cisco TMS is unable to read out port information from this system.
No Service Contract	There is no valid and active service contract registered for this system.
No System Contact Assigned	No system contact has been assigned for this system.
No TMS CP Services	Applies only to Legacy Systems. There are no Cisco TMS CP Services defined on the MCU. It is therefore not possible to book continuous presence conferences with this MCU.
No TMS ECP Services	Applies only to Legacy Systems. There are no Cisco TMS ECP Services defined on the MCU. It is therefore not possible to book enhanced continuous presence conferences with this MCU.
No TMS VS Services	Applies only to Legacy Systems. There are no Cisco TMS VS Services defined on the MCU. It is therefore not possible to book voice switched conferences with this MCU.
No TMS-archiving Lines Defined	Applies only to Legacy Systems. There are no reserved Cisco TMS-archiving lines defined for Cisco TMS to use.
No TMS-transcoding Lines Defined	Applies only to Legacy Systems. There are no reserved Cisco TMS-transcoding lines defined for Cisco TMS to use.
Organization Top Level Domain is not set	The Organization Top Level Domain is not set in Unified CM, so Cisco TMS may be unable to schedule or receive feedback about calls involving systems managed by Unified CM.
Pending Configuration Changes for System	There are pending configuration changes stored in Cisco TMS that have not yet been applied to the system.
Persistent Name Not the Same as Name on System	The persistent name is not the same as the name on the system. Cisco TMS is unable to set the persistent name.
Persistent Setting Mismatch	The system settings differ from configured persistent settings.
Port Count Exceeds License	The number of Cisco TMS ports defined exceeds the license.

Table 160 Ticket errors with descriptions (continued)

Provisioning Extension Critical Error	A critical Cisco TMSPE Diagnostics error.
Provisioning Extension Warning	There are a number of warnings from Cisco TMSPE diagnostics on the local Cisco TMSPE or on the Cisco VCS.
Scheduling Error	A scheduling error has occurred.
Service Contract Expired	The service contract for this system has expired. Without a valid service contract you will not be entitled to new software updates. Note that the current software version for this system is (vers. no.) and the latest version available from the Cisco software repository is (vers. no.)
Service Contract Expiring	The service contract for this system is about to expire. The ticket will include the expiration date.
SIP Registration Problem	There is a SIP registration problem.
SIP Server Registration Failure	The system has failed to register to the SIP Server.
Site Administrator Set as Default Group	The site administrator group is set as the default group for new users, which means all new users will have full administrator rights in Cisco TMS.
Software Version Incompatible	The software version on the system is incompatible with this version of Cisco TMS.
SSH Password Expiry Enabled	Applies only to CTS systems. SSH password expiry is enabled on this system. TMS uses SSH to control certain functionality, therefore if the password expires, this functionality will stop working. Please disable password expiry.
System Has Reached Resource Limit	The system has reached the limit of resources (calls/traversal calls/registrations) as given by option key(s). Note that this ticket will not be cleared automatically and must either be acknowledge or deleted.
System Is Not Registered with Unified CM	Applies to Unified CM-registered systems. Unified CM thinks this system is unregistered, this could be because the system has disconnected from the network, is switched off, or is misconfigured. You need to log on to Unified CM to continue troubleshooting this problem.
System Must Be Restarted	Settings have changed on the system, and the system must be restarted for changes to take effect.
System Settings Not Found	The default settings for the system are not set.
TelePresence Conductor Bridges Not Found in TMS	The systems which are managed by this TelePresence Conductor are not registered in Cisco TMS. This means that some features will not be available.
TelePresence Server is in Remotely Managed Mode but is Not Managed By a TelePresence Conductor	The TelePresence Server is in **Operation Mode**: *Remotely Managed*, but must be set to **Operation Mode**: *Locally Managed* when not behind a TelePresence Conductor.
The System's Unified CM Is Not Available	Applies to Unified CM-registered systems. The Unified CM this system is registered to is not available.

Table 160 Ticket errors with descriptions (continued)

This System is Running a Software Version that is Not Supported	The software version running on this system is not supported in this version of Cisco TMS.
This TelePresence Conductor is Running a Software Version that is Not Supported	The software version running on this TelePresence Conductor is not supported in this version of Cisco TMS.
Time Zone Mismatch	The time zone set in Cisco TMS for the system is different from the time zone on system.
Time Zone Not Set	The time zone has not been set. It will not be possible to book this system.
TMS Connection Error	There is a connection problem between Cisco TMS and the system.
TMS Database file is running out of space	The Cisco TMS Database File is Running Out of Space.
TMS Encryption key mismatch	The encryption key set in TMS Tools does not match the encryption key used by Cisco TMS to decrypt the authentication data.
TMS Server Time Out of Sync	The current time on the SQL Server is more than 30 seconds out of sync with the server time on the Cisco TMS Server.
TMS Service Not Running	One of the TMS Services is not running – the ticket will specify which one.
Tracking Method Incompatible with IP Assignment	The system is currently set to track by *IP Address* in the **Connection** tab, but the system is configured locally to use DHCP addressing. In this configuration, if the system's IP address changes, Cisco TMS will no longer be able to track the system.
Unable to Communicate with the Provisioning Extension	Cisco TMS is unable to communicate with the Cisco TMSPE.
Unified CM Server Time Is Out of Sync with TMS Server Time	The sever time on the Unified CM is different to the Cisco TMS server time.

Manage Event Notification Error Levels

In Cisco TMS: **Administrative Tools > Configuration > Manage Event Notification Error Levels**

On this page you can change the event notification error levels to customize the importance of different errors in Cisco TMS.

Note: The error levels are common for all users in Cisco TMS and cannot be defined per user.

User Administration

In Cisco TMS: **Administrative Tools > User Administration**

Here administrators can manage users, groups and permission levels.

Cisco TMS user permissions are controlled on a group level and every user can be a member of several groups. The total permission level for an end user will be the sum of all permissions assigned to all groups that the Cisco TMS user is a member of.

A new user is automatically added to a set of groups (see Default Groups, page 277) the first time the user accesses Cisco TMS, as the Windows Username of the user is automatically detected from Active Directory lookup. For more details, see Users, page 273.

Groups

In Cisco TMS: **Administrative Tools > User Administration > Groups**

On this page you can manage groups and their permissions for pages and functionality. You must have **Site Administrator** or **Video Unit Administrator** rights to create a File Based Phone Book using a local file.

Note: Security groups can only be imported to Cisco TMS.

Pre-defined Groups

Site Administrator

The permissions for this group cannot be changed and is per default set to full access to all menus, functionality, folders and systems in Cisco TMS. Only people who will be responsible for Cisco TMS are to be members of this group. Only members of the **Site Administrator** group have the rights to edit the **Configuration** pages under **Administrative Tools**, and can change for example the IP address of the server and alter the option keys.

Users

All new Cisco TMS users are members of this group by default. You cannot add or remove users belonging to the **Users** group. The permissions for this group can be changed by a **Site Administrator**. It is recommended that the access rights assigned to this group represents the lowest level you want any person in your organization to have. This applies to both what pages in Cisco TMS you want them to have access to, as well as which systems they are allowed to use.

Video Unit Administrator

This group has full administrative rights to all video conferencing systems (including gateways, gatekeepers and MCUs) in your network. The permissions can be changed.

Typically persons who are technically responsible are members of this group. **Video Unit Administrators** do not have the rights to edit the **Configuration** pages – otherwise, they have the same rights as the **Site Administrator**.

Group Administration

The **Groups** page shows **Name**, **Description** and type of groups that are present in Cisco TMS. There are three types of groups in Cisco TMS:

- **Removable** groups are created by users and can be removed.
- **Default Group**s are described above. They cannot be removed.
- **AD Group**s are imported from Active Directory. For more on this, see below.

Viewing Members of a Group

1. Move the cursor over the group name.
2. Click **View**.
3. A list of group members will now be displayed.

Editing a Group

To edit a group when you have the necessary permissions to do so:

1. Move the cursor over the group name.
2. Click **Edit**.
3. Now you can change the name, description, or who is a member of a group.
   - To remove members:
     1. Go to the **Group members** tab
     2. Select the user(s) you want to remove from the group.
     3. Click **Remove** button.
   - To add members:
     1. Go to the **Add members** tab
     2. Select the user(s) you want to add to the group.
     3. Click **Add**.
4. Click **Save** when finished.

Adding a New Group

1. Click **New** at the bottom of the page.
2. Enter a name and a description for the group.
3. Add Cisco TMS-registered users to the group.
4. Click **Save**.

Setting Permissions for Groups

1. Move the cursor over the group name.
2. Click **Set Permissions**.
3. Now you can set permissions for specific functionality and pages in Cisco TMS. Select or deselect the check boxes as desired.
4. Click **Save** when finished.

The tables below explain which permissions can be set for different functionalities within each menu in Cisco TMS.

Portal

Table 161 Cisco TMS portal page permissions

Page/feature	Permission	Action available to group
Portal	**Read**	Access the page.
Sitemap	**Read**	Access the page.

Booking

Table 162 Booking permissions

Page/feature	Permission	Action available to group

Table 162 Booking permissions (continued)

List Conferences -- All	*Read*	View meetings for all users in **List Conferences** and **Conference Control Center**. Use this setting to limit read access for conference information in **Ad hoc Booking**, the **Add Participant** availability table and so on.
	Update	Create, edit and delete meetings for all users.
	Export Log	Export log from **List Conferences** page to Excel/spreadsheet format.
List Conferences -- Mine	*Read*	View only your own meetings and those you have booked on behalf of someone else in **List Conferences** and **Conference Control Center**.
	Update	Edit and delete own meetings only. A Cisco TMSBA service user must have this permission.
List References	*Read*	Access the page.
	Update	Create, edit and delete references.
Participant Template	*Read*	Access the page.
	Update	Create, edit and delete templates.
Misc	*Booking*	Permission to book new conferences. A Cisco TMSBA service user must have this permission.
	Ad Hoc Booking Page	Access the page.
	Advanced Settings	Access **Advanced Settings** in **Booking > New Conference**.
	Approve Meeting	Approve or reject scheduled meetings. If not enabled, all meetings booked by a user in this group will need approval by a user that has this permission. A Cisco TMSBA service user will usually need this permission.
	Book on behalf of	Book on behalf of other users. A Cisco TMSBA service user must have this permission.
	New Conference Page	Access to the **New Conference** page. The *Booking* permission is required to create a new conference.

Monitoring

Table 163 Monitoring permissions

Page/feature		
Misc	*Conference Control Center*	Access the page.
	Graphical Monitor	Access the page.

Systems

Table 164 Permissions related to the Systems menu

Page/feature	Permission	Action available to group
Navigator	*Read*	Access the page.
	Read TelePresence Conductor Aliases	View the TelePresence Conductor Aliases tab.
	Create/Update/Delete TelePresence Conductor Aliases	Create, edit and delete TelePresence Conductor aliases.
Ticketing Service	*Read*	Access the page.
System Overview	*Read*	Access the page.
Manage Dial Plan	*Read*	Access the page.
Provisioning	*Directory*	Access the page.
	Users	Access the page.
	FindMe	Access the page.
Configuration Backup	*Configuration Backup*	Access the page.
	Configuration Restore	Access the page.
	View Backup Status	Access the page.
System Upgrade	*System Upgrade*	Access the page.
	Software Manager	Access the page.
Purge Systems	*Purge Systems*	Delete/purge systems from the Cisco TMS database.
History	*Read*	Access the page.
Event Notification Manager	*Read*	Access the page.
	Update	Edit notifications to all users.
	Own Notifications	Edit notifications for own user only.

Phone Books

Table 165 Permissions related to the Phone Books menu

Page/feature	Permission	Description
Phone Books	*Read*	Access the list of Phone Books in for example **Phone Books > Manage Phone Books** page.
	Create/Delete	Create, edit and delete phone books available for you to update.
	Grant Update on New Phone Books	Enter and edit entries in new phone books. This does not give permissions to update existing phone books. **Note:** To update or delete existing phone books, the group permissions must be set for each of those phone books. See Manage Phone Books, page 215.
	Set On System	Set phone books on systems.
	Connect to Source	Set up a connection between a phone book and a phone book source.
Phone Book Sources	*Read*	Read access to the **Phone Book Sources** page.
	Create	Create new phone book sources.
	Update	Edit existing phone book sources.
	Delete	Delete phone book sources.
	One-time Import	Perform one-time import to a manual list source.

Reporting

Table 166 Reporting permissions

Page/feature	Permission	Description
Reporting	*Call Detail Record*	Access the page.
	Conference Statistics	Access the page.
	Network Statistics	Access the page.
	System Statistics	Access the page.
	Billing Codes	Access the page.

Administrative Tools

Table 167 Permissions related to the Administrative Tools menu

Page/feature	Permission	Description
Configuration	*Read*	Access the page.
	Update	Edit configurations.

Table 167 Permissions related to the Administrative Tools menu (continued)

Page/feature	Permission	Description
Users	*Read*	Access the page.
	Create	Create new users.
	Update	Update existing users.
	Delete	Delete existing users.
	Set Groups	Set groups to users.
Groups	*Read*	Access the page.
	Create	Create new groups.
	Update	Update existing groups.
	Delete	Delete existing groups.
	Set Permissions	Set permissions for existing groups.
	Set Default Group	Define which groups are default groups.
IP zones	*Read*	Access the page.
	Create	Create new IP Zones.
	Update	Edit existing IP Zones.
	Delete	Delete existing IP Zones.
ISDN zones	*Read*	Access the page.
	Create	Create new ISDN Zones.
	Update	Edit existing ISDN Zones.
	Delete	Delete existing ISDN Zones.
Billing Codes	*Read*	Access the page.
	Create	Create new Billing Codes.
	Update	Edit existing Billing Codes.
	Delete	Delete existing Billing Codes.
	Set on System	Set existing Billing Codes on systems.
	Import	Access to importing Billing Codes.
Activity Status	*Read*	Access the page.
	Delete	Delete an event log.
TMS Server Maintenance	*Read*	Access the page.
TMS Tickets	*Read*	Access the page.
Provisioning Extension Settings	*Read/Update*	Access the page and edit configurations.
Provisioning Extension Diagnostics	*Read/Update*	Access the page and edit configurations.
Audit Log	*Read*	Access the page.

Adding Active Directory groups

Instead of creating your own Cisco TMS groups you can add existing groups from Active Directory.

To start using Active Directory groups:

1. Go to **Administrative Tools > Configuration > Network Settings**.
2. In the **Active Directory** section, set **Allow AD groups** to *Yes*.

   Import from AD and **Update Groups From AD** buttons will now be displayed in **Administrative Tools > User Administration > Groups**.

To add a group from Active Directory:

1. Click **Import from AD**.
2. Type the name (or parts of the name) of the group.
3. Click **Search**.
4. Select the check box next to the group you want to add.
5. Click **Import selected**.
6. The added AD group(s) will be shown as selected after they have been added to Cisco TMS Groups.

When you add an Active Directory group to Cisco TMS it will initially have no members. The membership in these groups is updated when:

- a user logs on.
  Only AD users who have signed in to Cisco TMS will show up as members of the Active Directory groups. The Active Directory groups may have members that have not yet used Cisco TMS.
- you click **Update From AD** or **Update Users From AD** in **Administrative Tools > User Administration > Users**.
- you click **Update Groups From AD** on the group page.
  This updates AD group memberships for all users in Cisco TMS.

Note that you cannot manage membership in Active Directory groups from within Cisco TMS.

Users

In Cisco TMS: **Administrative Tools > User Administration > Users**

On the **Users** page you can manage contact information, user preferences, and the group memberships that control the user's permission levels.

- Users can be created manually or imported from Active Directory. Cisco TMS will also automatically authenticate any local user accounts on the Cisco TMS server.
- To enable AD synchronization and/or set up automatic synchronization, go to **Administrative tools > Configuration > Network Settings > Active Directory**, see Network Settings, page 237.

Active Directory Synchronization

The first time a user logs on to Cisco TMS, the **Username** parameter is retrieved from Active Directory. Cisco TMS will also retrieve user information such as email address and first and last name. If the information is not available, the user will be prompted by a popup window to fill in user information and user preferences. You may not change the **Username** while logged into Windows.

Synchronization with AD retrieves new users and updated information, and deletes any users in Cisco TMS that have been removed from AD. If AD lookup is enabled, the following buttons for manual synchronization are available:

- **Update from AD** in the user details page allows you to retrieve updated information about the selected user from Active Directory.

- **Synchronize all user with AD** on the **Users** page initiates a manual, complete synchronization.

Adding a New User or Changing User Details

To manually add a new user, or update the details for an existing user:

1. Click **New** or click on an existing user in the list.

2. Enter user information. If Active Directory lookup is enabled and the user is found in AD, some fields will be read-only.

Table 168 User settings

Field	Description
Windows Username	The user's Windows Username. This field must be filled in.
First Name	The user's first name. This field must be filled in.
Last Name	The user's last name. This field must be filled in.
Email Address	The email where meeting bookings and event notifications will be sent. The format must be `handle@example.com`. This field must be filled in.
Language	This setting controls: – the language that this user will see in the **User Settings** pop-up window, available to users by clicking on their username at the bottom left of any Cisco TMS page. The rest of the Cisco TMS web interface will be in the language selected during installation, or in US English if that language is not available. – the user's locale, including time format and first day of the week. For example, US, UK, and AU English will use the same text strings, but different date and time formats.
Office Telephone	The user's office telephone number.
Mobile Telephone	The user's mobile telephone number.
Primary System	The user's preferred video system.
Webex Username	The user's Webex username. If **Get Webex Username from Active Directory** is enabled, any username entered here will be overwritten the next time data is synchronized from AD for the user. For more about AD username retrieval, see WebEx Hybrid Settings, page 256.
Webex Password	The user's Webex password. If single sign-on is enabled for CMR Hybrid, any password entered here will be ignored.
Webex Site	The Webex site that the user will use for their CMR Hybrid conferences.

Table 168 User settings (continued)

Field	Description
Time Zone	Set the user's time zone to present the correct time and date information to users. Users will see their own time zone when: – Booking a new conference. – Listing existing conferences. When editing or viewing the details of a booking created for a different time zone, the time zone of the conference will be displayed, and the user will be notified of this.
IP Zone	Used to identify network resources when no Cisco TMS endpoints are participating in a conference. Note that if the user's IP zone does not contain any network resources, this setting should be set to the zone nearest to the user that does have network resources.

3. Click **Save** when all the requested information has been provided.

Deleting a User

1. Check the box for the user or users you want to remove.
2. Click the **Delete** button.

Default Groups

In Cisco TMS: **Administrative Tools > User Administration > Default Groups**

In the **Default groups** page you can define to which groups a new user automatically will be assigned when logging in to Cisco TMS for the first time.

By default, all users will be member of the **Users** group. Membership to additional groups may be set by selecting the check boxes next to a group and clicking **Save**.

Cisco TMSdoes not overrule membership in AD groups. Therefore it is not possible to set AD groups as default groups in Cisco TMS.

Default System Permissions

In Cisco TMS: **Administrative Tools > User Administration > Default System Permissions**

On this page you define default system permissions for each group in Cisco TMS to the systems in **Systems > Navigator**.

Note: Changes made to **Default System Permissions** will only affect systems that are added *after* the change to settings. Existing systems in **Navigator** will keep their original permission settings.

The permissions that can be set as system defaults for each user group in Cisco TMS are listed in the table below.

Table 169 Possibly default system permissions for groups

Permission	Description
Read	Group members can view configuration settings.
Book	Group members can book conferences.
Edit Settings	Group members can edit configuration settings.
Manage Calls	Group members can manage calls set up with the recently added systems.
Set Permissions	Group members can change permissions for the recently added systems.

When adding, moving, or copying a system, the permissions you specify on a folder level will merge with the system permission settings for groups in Default System Permissions, page 277.

The permissions on these pages are displayed differently, but map as shown in the table below.

Table 170 Mapping of folder and system permissions

Folder Permissions	Default System Permissions
Read	Read, Book
Edit	Read, Book, Edit Settings, Manage Calls
Set Permissions	–

To make settings for a folder or system that override these defaults, go to **Systems > Navigator** and click the **Folder and System Permissions** button, see Folder and System Permissions, page 137.

Locations

In Cisco TMS: **Administrative Tools > Locations**

This is where you define ISDN and IP zones so that Cisco TMS will know which calls are possible, which prefixes and area codes are needed, and what protocols to use.

For more information see How Zones Work, page 38.

ISDN Zones

In Cisco TMS: **Administrative Tools > Locations > ISDN Zones**

On this page, a list of any existing ISDN zones is presented, and new zones can be created:

- Hover over each zone in the list to access the drop-down menu with options to **View**, **Edit**, or **Set on Systems**.
- Click **New** to create a new ISDN zone.

Settings

When creating or editing an ISDN zone in Cisco TMS, the following fields are available:

Table 171 ISDN Zone settings

Section/field	Description
General	
ISDN Zone Name	Name of the ISDN zone.
Country/Region	Which country this zone is situated in. This enables Cisco TMS to choose the correct country code and international dialing prefixes.
Area Code	Which area code this ISDN zone is situated in. This enables Cisco TMS to choose the correct area code rules.
Line	
To access an outside line for local calls, dial	Prefix needed to obtain an outside line in this ISDN zone.
To access an outside line for long distance calls, dial	Prefix needed to obtain an outside line for long distance calls in this ISDN zone.

Table 171 ISDN Zone settings (continued)

Section/field	Description
Internal Calls	
Number of digits to use for internal ISDN calls	Number of digits used for internal dialing between systems in the zone. The first digits in the number will be stripped from the number when dialing between systems in this ISDN zone.

Area Code Rules

When viewing or editing an ISDN zone, clicking **Area Code Rules** brings up a page where you can add and edit area code rules for the United States.

When creating or editing an area code rule, the following fields are available:

Table 172 Settings for area code rules

Field	Description
When dialing from this area code to the following area code	Specify the area code this rule should apply for. For example, if you want the rule to apply every time dialing 555, specify 555 in this field.
With the following prefixes	The prefix is the first three digits of the base number. Leave blank if you want the rule to apply for all calls made to the area code in the above field.
Include Area Code	Check this if you want the rule to include the area code specified above in the call. For the US, check to enable 10-digit dialing.
Before dialing, also dial	Enter a string here to include in front of the dial string created by this area code rule (before the area code and prefixes specified in the first two fields above).
Strip digits for zone's local outside line access	Check to strip the outside line prefix (set in **Administrative Tools > Locations > ISDN Zones > Line** section) from the number you are going to dial.

IP Zones

In Cisco TMS: **Administrative Tools > Locations > IP Zones**

On this page, a list of any existing IP zones is presented, and new zones can be created:

- Hover over each zone on the list to access the drop-down menu with options to **View**, **Edit**, or **Set on Systems**.
- Click **New** to start creating a new IP zone.

When creating or editing an IP zone, the below settings are available. With these settings you specify which prefixes to dial in order to use a gateway. Specifying the prefix rather than the gateway directly creates the flexibility to use load-balanced gateways, and even gateways not supported by Cisco TMS.

Table 173 IP Zone settings

Sections and fields	Description
IP Zone	
Name	Set a name for the IP zone.

Table 173 IP Zone settings (continued)

Sections and fields	Description
Gateway Resource Pool	
ISDN Zone	Specify which ISDN zone you want the below gateway prefixes to use. Note that the Gateway Resource Pool will not work correctly unless this setting has been specified.
URI Domain Name	Cisco TMS will always use URI dialing between two locations where this setting is filled in, thereby ignoring the IP/ISDN preferences defined at the bottom of this page.
Gateway Auto Prefix	The prefix needed to dial a video ISDN number from this IP zone using a Gateway.
Gateway Telephone Prefix	The prefix needed to dial an audio ISDN number from this IP zone using a Gateway.
Gateway 3G Prefix	The prefix needed to dial a 3G mobile phone number from this IP zone using a Gateway.
Dial-in ISDN Number **Dial-in ISDN Number for 3G**	These numbers are used for generating TCS-4 numbers like +15551231234*99999 when Cisco TMS is routing a call: ■ from PSTN and into an IP zone. ■ from a 3G network and into an IP zone. After the settings are saved, these numbers will both be shown as qualified numbers.
Allow IP-ISDN-IP	Check to allow IP-ISDN-IP calls, running through two different gateways. For more information, see IP-ISDN-IP Calls, page 39.
Prefer ISDN over IP calls to these IP Zones **Prefer IP calls over ISDN to these IP zones**	Lists of IP zones to which: ■ ISDN is preferred over IP. ■ IP is preferred over ISDN. The lists are used when scheduling calls between IP zones. Move zones between lists by selecting them and clicking the arrow buttons.

Billing Codes

In Cisco TMS: **Administrative Tools > Billing Codes**

Create and manage billing codes, and set them on systems, in these pages.

Manage Billing Codes

In Cisco TMS: **Administrative Tools > Billing Codes > Manage Billing Codes**

Billing codes are only supported for Cisco TelePresence MXP systems.

On this page you can create, edit and delete billing codes, and set them on systems.

Using billing codes, you can:

- Ensure that only users with the correct billing code can make calls from a particular system.
- Monitor system usage based on the billing codes which are entered when calls are made. This can be useful for distributing the cost.

There are two ways to use billing codes:

- Require that a billing code must be entered on a system before a call can be made.
- Request a billing code when a call is attempted on a system, but still allow the call to proceed if no billing code is entered.

When a billing code is used, the Call Detail Record (CDR) for the conference will contain the billing code. For more information, see Billing Code Statistics, page 231.

It is not necessary to enter a billing code when a system is receiving a call.

Creating a New Billing Code

To create a new billing code:

1. Click **New**.
2. Enter a name and description for your new billing code.

   The characters ; and = are not permitted.
3. Click **Save** to finish, or **Add New** to create more billing codes before saving.

Applying a Billing Code

To set a billing code on a system:

1. Click **Set On Systems** and then select the systems or folders the billing code will be set on.
2. Select the way you want the billing code to be used for the selected system(s):
   a. **Require billing code before making calls (codes are checked)**: calls cannot be made without entering the correct billing code.
   b. **Ask for billing code before making calls (codes are not checked)**: entering the correct billing code is optional, and not necessary to make a call.
3. Click **OK** to commit the changes.

Disabling a billing code

To disable the use of billing codes on one or more systems:

1. Repeat the selection of systems as described above.
2. Select **Turn off billing code use**.
3. Click **OK** to commit changes.

Importing Billing Codes from a File

You can also import billing codes from a file instead of adding them manually.

In the **Manage Billing Codes** page:

1. Click **Import**.
2. Browse to the file on your local machine.
3. Click **Upload**.

Note that the valid file format is **.txt**, and each row in the file must contain a billing code. Optionally you can add a comma followed by a description, as in this example:

```
101, Description for billing code 1
102, Description for billing code 2
103, Description for billing code 3
```

Billing Codes Activity Status

In Cisco TMS: **Administrative Tools > Billing Codes > Billing Codes Activity Status**

Billing codes are only supported for Cisco TelePresence MXP systems.

On this page you can monitor the billing code update progress for the systems in Cisco TMS.

Ongoing and upcoming scheduled events are displayed automatically.

- Search for past events by modifying the **Start Date** and **End Date** fields, then click **Search**.
- Check *Show only mine* to display only events scheduled by the currently logged in user.

  To apply this to the list below, click **Refresh**.
- Click the linked description of any event to see a detailed activity log.
  - For Conference Diagnostic Activity, the status and event description for the selected dates are displayed
- To cancel a scheduled event, select it and click **Delete**.

Click to refresh

Note that the activity status pages do not automatically refresh while open. To update the status view, click **Refresh**.

Diagnostics

In Cisco TMS: **Administrative Tools > Diagnostics**

View TMS tickets and get diagnostic tools for conferences and Cisco TMSPE in these pages.

TMS Tickets

In Cisco TMS: **Administrative Tools > Diagnostics > TMS Tickets**

This page shows all open Cisco TMS tickets. Tickets flag information, warnings and error messages. Go to **Manage Ticket Error Levels, page 261** to define which tickets will be shown on this page.

Table 174 Available actions for each ticket

Action	Description
Acknowledge	This will acknowledge a ticket, causing it not be displayed as an open error any more.You can add a comment to the ticket when you acknowledge it. Information tickets will be removed from the list when acknowledged.
Delete	This will permanently delete the ticket from Cisco TMS.

Provisioning Extension Diagnostics

In Cisco TMS: **Administrative Tools > Diagnostics > Provisioning Extension Diagnostics**

After you have installed and enabled Cisco TMSPE, diagnostics run automatically at regular intervals. No configuration is required by the administrator. It is also possible to manually initiate a diagnostics health check.

Tests are run on the following:

- The connection between Cisco VCS and Cisco TMS.
- The synchronization between the services.
- The connection between the services.
- The display of alarms and events and their dispatch to Cisco TMS as tickets.

To run diagnostics manually, click **Run Health Check**. This button initiates diagnostics on all modules of Cisco TMSPE. The **System Status** list and the list of all the active Cisco VCSs will be updated.

Alarms

This section displays a list of alarms raised by Cisco TMSPE. For more details on each alarm, click the **Details** button on the right side.

All alarms and warnings raised by Cisco TMSPE Diagnostics generates a ticket in Cisco TMS.

System Status

In this table, a colored circle indicates which diagnostics run on which system. No colored circle indicates that the test does not apply.

The circles can be:

- Green: Status is OK.
- Orange: The diagnostics task has not started yet.
- Red: The system has a warning or a critical error.
- Gray: The diagnostics task is idle or disabled.
- Blue: The diagnostics task is in-progress.

Diagnostics are run on these systems:

- User Repository
- Device Repository
- User Preference, imported from the user repository
- Phone Book
- FindMe, if in use
- Diagnostics
- CMR (Collaboration Meeting Room)

VCS Communication

This section displays information for each Cisco VCS and cluster names.

Last Call Time is the date and time of the last communication between the Cisco VCS and the Cisco TMS.

Conference Diagnostics

In Cisco TMS: **Administrative Tools > Diagnostics > Conference Diagnostics**

This page allows administrators to identify and fix problems with existing conferences.

When to Run Diagnostics

As the task is resource intensive we recommend running it outside of normal business hours. The task can take a long time to run, depending on the number of future conferences.

While diagnostics can be used at any time, it is particularly useful after you have made changes to your deployment such as:

- Dial plan:
  - Endpoints that were H.323 are moved to SIP.
  - The number range is changed on a bridge.

- Infrastructure:
  - Conference bridges are moved behind TelePresence Conductor.
  - MCUs are swapped for TelePresence Server.
  - Migrating from a Cisco VCS to a Unified CM-based deployment.

  Note that the Diagnostic Tool runs only on the conferences that are scheduled for the next seven days.

How the Diagnostics Work

When **Run Diagnostics** is clicked, Cisco TMS checks the following for future scheduled conferences that are scheduled to launch for a period of seven days from the selected start date.

- All participants exist in the database and are bookable.
- The route is valid (all participants are still routable—for more information see Introduction to Routing, page 31).
- Date selection option in Conference Diagnostics - You are able to select a date range for Conference Diagnostics. By default, the diagnostics are run for a period of seven days from the selected start date. You can only edit start date and the end date is disabled.

When an issue is found, the diagnostics status of the conference is set to *Reported*.

Go to the **Activity Status** page to view task progress, or click **Refresh** to update the page. The diagnostics task is executed by SchedulerService and runs asynchronously.

Autocorrecting Conferences

Click **Autocorrect** to make Cisco TMS attempt to fix selected conferences automatically.

Scenario	Autocorrect outcome
The conference route is no longer valid.	Conference is re-routed, disregarding any manual choices made when the conference was first booked. This can result in: ■ New dial-in numbers for the conference. ■ Removal of manually configured distribution.
Any occurrence of a recurrent series needs correction.	All occurrences are re-routed, any exceptions deleted.
One or no participants left after autocorrection.	No action. These conferences will show the status *Autocorrection Failed*.
Participants have been deleted from the Cisco TMS database or are no longer routable for other reasons.	Participants removed from conference.
Unable to resolve the problem for a conference	**Status** will show as *Autocorrection Failed* and the conference must be manually edited.

During and after running diagnostics, you can click **Refresh** to update the status of conferences.

Click **Run Diagnostics** to remove conferences with diagnostics status *Fixed* from the list.

Activity Status

In Cisco TMS: **Administrative Tools > Activity Status**

This page contains information about events for all systems registered in Cisco TMS.

Ongoing and upcoming scheduled events are displayed automatically.

- Search for past events by modifying the **Start Date** and **End Date** fields, then click **Search**.
- Check *Show only mine* to display only events scheduled by the currently logged in user.

  To apply this to the list below, click **Refresh**.
- Click the linked description of any event to see a detailed activity log.
  - For Conference Diagnostic Activity, the status and event description for the selected dates are displayed
- To cancel a scheduled event, select it and click **Delete**.

Click to refresh

Note that the activity status pages do not automatically refresh while open. To update the status view, click **Refresh**.

Analytics Extension

In Cisco TMS: **Administrative Tools > Analytics Extension**

The **Analytics Extension** menu item and web page will only be visible if a license has been added for Cisco TelePresence Management Suite Analytics Extension (Cisco TMSAE)

Cisco TMSAE is an online analytical processing (OLAP) system for Cisco TelePresence Management Suite (Cisco TMS) that provides advanced reporting functionality on your video network. It integrates with Business Intelligence (BI) applications, custom built applications, and other applications capable of connecting to an OLAP cube. The most communly used client is Microsoft Excel.

Cisco TMSAE consists of three elements:

- The application software, installed onto an existing Cisco TMS Server.
- The data warehouse databases, installed onto an existing Microsoft SQL Server.
- The clients used to access the data.

For information on installing, managing, and using Cisco TMSAE, see the product documentation.

TMS Server Maintenance

In Cisco TMS: **Administrative Tools > TMS Server Maintenance**

This page displays server information and provides tools for general management and housekeeping of the Cisco TMS and database servers.

Click **Refresh** to refresh all data on the page.

Identifying a Server Time Mismatch

The **Database Server Date and Time Settings** section displays the date and time of the Cisco TMS server, the database server, and any mismatch between the two.

If such a mismatch is found, you must correct this in the Windows Date and Time settings on the server whose time is incorrect.

Downloading Diagnostics Files

Click **Download Diagnostics Files** to create and download a diagnostics zip file that can be sent to Cisco Technical Support to assist with troubleshooting .

The zip file created will contain the recent Cisco TMS log files and, if installed, the Cisco TelePresence Management Suite Analytics Extension and Cisco TelePresence Management Suite Provisioning Extension log files, an XML file of Cisco TMS's configuration settings and any Cisco TMS-related entries found in the Windows event log.

Viewing Free Disk Space

To display the free disk space for each partition on the database server, you must enable the OLE Automation Procedures option on the SQL server. For SQL Server 2016 and 2012 instances, OLE Automation Procedures are disabled by default.

To enable this option, run the following SQL statements on your SQL Server:

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'Ole Automation Procedures', 1;
GO
RECONFIGURE;
GO
```

The **Database Server Disk Space** section displays the free disk space for each partition on the web server.

Note that if using an account other than sa to connect to the tmsng database, that account must have the 'sysadmin' server role.

Viewing and Managing Database Files and Sizes

The **Database Files and Size Info** section provides an overview of database names, servers, and path information about the databases, as well as the current size and maximum size of each database, and what it stores.

Database management must be handled through an external tool such as Microsoft SQL Server Management Studio.

For guidance on setting up a database maintenance plan, see *Cisco TMS Installation and Upgrade Guide*.

Purging Old Data and Logs

The **Purge Old Data in Database Tables Plan** section displays information about the database tables used for logs, and caching information in Cisco TMS.

The **Purge Log Plan** section displays information about log files on the web server. For descriptions of all Cisco TMS debug logs, see Log Overview, page 307.

The overviews show how many entries each log file or database table currently has and how many days the entries will be kept before they will be purged automatically.

To modify the purge settings for any entry:

1. Click on the **Edit** link for the desired entry.
2. Check **Enabled** to initiate automatic cleanup. If left unchecked, the log will never be purged.
3. Set the **Number of Days to Keep Data** before the data is purged.
4. Click **Update** to save the setting.

Purge Old Data in Database Tables Plan

Table 175 Database tables affected

Database Table	Description
Endpoint/MCU Call Log	Call detail records for conferences involving endpoints/MCUs, as displayed in **Reporting > Call Detail Record > All Endpoints and MCUs**.
Gateway/Gatekeeper Call Log	Call detail records for conferences involving gateways/gatekeepers, as displayed in **Reporting > Call Detail Record > Gateway**, **Gatekeeper and VCS**.

Table 175 Database tables affected (continued)

Database Table	Description
Feedback Log	Events like scheduling, errors, and encryption status from systems in Cisco TMS. The **Number of Days to Keep Data** field for this entry affects the **Logs** tab for each system in **Navigator**. For a company with several hundred endpoints, the size of this log file can become substantial, and we recommend that you regularly purge old data.
LiveSnapshot	This table contains snapshots of monitored conferences in Cisco TMS.
Scheduler Events	All scheduled events.
Scheduled Calls	These fields show the number of entries in the scheduled calls database. Note that this setting is disabled by default.
Ticket Log	This log contains tickets for systems in Cisco TMS.

TMS Redundancy

This section is visible only if the setting **Administrative Tools > Configuration > General Settings > Enable TMS Redundancy** is set to *Yes*.

Table 176 Section available with a redundant setup

Section	Description
Probe URL	The URL that the Network Load Balancer (NLB) must be configured to probe in order to monitor the status of the nodes.
Server Status	This section lists the following: ■ The status of each node. ■ The last time a timestamp notification was logged. ■ The last time the node status changed from active to passive or passive to active.
Failover Activity Log	The table lists whether the node became *Active* or *Retired*, the date and time, and the reason: ■ *Manual*: an administrator forced a manual failover by clicking **Force Manual Failover**. ■ *Automatic*: the active node detected that its services became unresponsive or disabled, or the passive node detected that the active node's services became unresponsive or disabled. To clear all past data from the tables, click **Clear Lists**. Click **Force Manual Failover** to force a failover.

TMS Services Status

The TMS Services status section displays information about all Cisco TMS services which are running towards the Cisco TMS database and the status of the probe URL in redundant deployments. For more information on the windows services, see Windows Services, page 19.

Click **Clear List** to remove obsolete data from the list, such as services listed under a server name that is no longer in use.

Redundant Deployments

In a redundant deployment, the services will be listed for each node, with a **Status**:

- *Service Running* for those on the active node.
- *Service on Standby* for those on the passive node.

The TMSProbeURL status displays as a service in this table. It will show once for each node: if it does not display as *Service Running* this could indicate a problem with the Network Load Balancer's probes. See Cisco TelePresence Management Suite Installation and Upgrade Guide for your version of Cisco TMS for more details.

Note: In a Cisco TMS redundant deployment where Cisco VCS is configured to provision users, currently Cisco TMS displays NLB management IP address in the Provisioning Extension Diagnostics page, instead of Cisco VCS IP address.

Audit Log

In Cisco TMS: **Administrative Tools > Audit Log**

The **Audit Log** lists changes made to objects in Cisco TMS.

The changes or operations which are listed in the log are:

- *Create*
- *Update*
- *Delete*

The **Object Types** you can view change information for are:

- *Folders*
- *Groups*
- *Systems*
- *System Backups*
- *TMS Settings*
- *Users*
- *Purge Log Plan*
- *Phone Book*

All audit log settings are configured in **TMS Tools**. To enable auditing and to view and purge audit log data, go to **TMS Tools > Security Settings > Advanced Security Settings > Auditing**.

Table 177 Audit log columns

Column	Description
Date and Time	Date and time the changes were made.
Username	The username of the user who made the change.
Object Operation	Type of change that was made to the object. You can display the operation types listed above.
Object Category	Type of object the changes were made to. You can display the object types listed above.
Object Name	Name of the system to which the change was made. This field can be used for doing a free text search.

Table 177 Audit log columns (continued)

Attribute Name	Name of the attribute that was changed.
New Value	Current value of the **Attribute Name** if applicable.
Service Name	Name of the service (TMSWeb, TMSWebPublic or other services).
Origin Host-Address	IP address of the host machine from which the change was made. If a service user made the change, this field will be blank. This field is not visible in redundant deployments.

You can filter the audit log by specifying:

- **Start Time** and **End Time**
- **User Type**
- **User Name**
- **Object Name**
- **Object Type**
- **Origin Host-Address**
- **Operation Name**

You can configure access to the audit log on a per user group basis:

1. Go to **Administrative Tools > User Administration > Groups**.
2. In the drop-down menu for the group, click **Set permissions**.
3. Under **Administrative Tools**, select the **Audit Log** check box.

To limit the size of the audit log you can specify how frequently the audit log data is purged from the database:

1. Go to **TMS Tools > Security > Advanced Security**.
2. In **Auditing**, check **Purge Old Audit Log Data in Database**.
3. Edit **Number of Days to Keep Data**.
4. Click **Save**.

Cisco TMS Tools

Cisco TMS Tools is an administrator program installed as part of Cisco TMS which runs on the Cisco TMS server under **Start > Programs > Cisco TelePresence Management Suite >TMS Tools**. Here you can make configuration changes, change the security level of your Cisco TMS deployment, and run troubleshooting tools.

Changes made in Cisco TMS Tools can restrict access to parts of the Cisco TMS application and in some cases stop the application from working altogether.

Changes to settings in Cisco TMS Tools must be made by an experienced Windows and Cisco TMS administrator.

Configuration 290
Security Settings 293
Utilities 296
Diagnostic Tools 297

Configuration

Database Connection Settings

This is where you specify the location of the Cisco TMS or Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) SQL databases, and the credentials Cisco TMS uses to connect to them.

Cisco TMS Database Connection

Prerequisites for Windows Authentication and the Cisco TMS Database

If you intend to use **Windows Authentication**, ensure that the following accounts have *db_owner* rights to the database before you edit the Cisco TMS database settings:

- The account you use to log into the Cisco TMS server.
- The account that the TMS services log on as.
- The IIS AppPool account.

Before selecting **Windows Authentication** in Cisco TMS Tools, complete the following steps for Cisco TMS to use Windows authentication towards the SQL database:

1. Create a new Active Directory service account, for example tms-databaseservice.
2. In SQL Server, create a new login for tms-databaseservice.
3. In SQL Server, create a new user for the tmsng database.
   a. Associate the user with the tms-databaseservice login.
   b. Assign the user *db_owner* permissions.

4. In SQL Server, create a new login for the user account that runs Cisco TMS's IIS App pool. The default account is IIS APPPOOL\TMSNet40AppPool.

   You can verify which user account Cisco TMS's IIS App pool runs under by opening its log-web file;the first entry will contain the Cisco TMS version number followed by the user account in brackets.
   Note: If you are using an external SQL Server; The IIS APPPOOL\TMSNet40AppPool user identity in IIS must be changed to a domain user (can be the same user created in Step 3 -- that is: *tms-databaseservice*) via *IIS* > *Application Pools* > right-click *TMSNet40AppPool* and choose *Advanced Settings* > *Process Model* > *Identity*.

5. In SQL Server, create a new user for the tmsng database.
   a. Associate the user with the login you created in step 4 above.
   b. Assign the user *db_owner* permissions.
6. On the Windows Server hosting Cisco TMS, add the service account user to the NTFS permission with '**Modify**' permission to the data location path. The default path is **C:\Program Files (x86)\TANDBERG\TMS\data**.
7. Change all six TMS services so that they log on as tms-databaseservice, and restart them.
8. Restart IIS.

You can now disable SQL Server authentication in SQL Server, so that it uses Windows Authentication only.

Note: You must re-enable SQL authentication in SQL server, if you chose to disable it, and set authentication back to SQL in Cisco TMS Tools before upgrading Cisco TMS.

Database Settings

Table 178 Database settings in Cisco TMS Tools

Field	Description
Database Server\Instance	This field shows the database server and instance which Cisco TMS is currently using. Change this setting to point the Cisco TMS application to a different server or instance.
Database Name	The Cisco TMS database name is **tmsng** by default. This must be changed if the database name has been changed in SQL, but we do not recommend changing the database name as you can only upgrade a TMS database with the name tmsng. Upgrades attempted on a database which is not called tmsng will fail. **Note:** Changing the database name in this field will not change the name of the database in SQL. Modifying this database name to something different to the database name in SQL will cause Cisco TMS to lose connection with this database and stop working altogether.

Authentication

Windows Authentication

Windows Authentication improves the security and management of the database by using centrally managed accounts instead of local SQL server/database accounts.

When you change the **Cisco TMS Database Connection Settings** to **Windows Authentication** and click **Save**, Cisco TMS Tools checks that the account running the services and the IIS app pool account are able to connect to the database using Windows authentication.

Settings in Cisco TMS Tools which require database access will be grayed out if the user you are logged into the server as does not have appropriate SQL server access.

SQL Server Authentication

The sa account and password must be used during installation of Cisco TMS. Afterwards the account can be changed here to one with lesser privileges which Cisco TMS will use to access the database using SQL Server authentication.

MultiSubnetFailover option for SQL connection

Cisco TMS Admin can select **Enable the use of 'MultiSubnetFailover' for SQL Connection** option respectively for **High Availability Group Listener** or **Microsoft SQL Server Failover Cluster**. The feature can be configured from **Cisco TMS Tools>Configuration> Cisco TMS Database Connection**.

During Microsoft SQL Server failover, Cisco TMS attempts to connect to **Microsoft SQL Server Failover Cluster** or **High Availability Group Listener**. If **Enable the use of 'MultiSubnetFailover' for SQL Connection** option is selected, MultiSubnetFailover allows faster failover and significantly reduce the failover time.

Note : If **Enable the use of 'MultiSubnetFailover' for SQL Connection** option is selected for a SQL connection other than **High Availability Group Listener** or **Microsoft SQL Server Failover Cluster**, it may result in a negative performance impact and is not supported.

For more information, refer to https://support.microsoft.com/en-us/help/2870437/connection-times-out-when-you-use-alwayson-availability-group-listener.

Cisco TMSPE Database Connection

Table 179 Cisco TMSPE database connection settings

Field	Description
Database Server\Instance	This field shows the database server and instance which Cisco TMSPE is currently using. Change this setting to point Cisco TMSPE to a different server or instance.
Database Name	The Cisco TMSPE database name which is *tmspe* . This is not editable.

Authentication

- Windows Authentication can be set by using the format domain\username in the **Username** field.
- A username string without a \ will ensure that SQL authentication is used.

Directory Locations

Software Directory

You can specify the location where the software for system upgrades is stored by editing the Software Directory. The directory you specify here must be a subfolder of \wwwTMS\ and the TMS service accounts must have write access to it. The System Upgrade feature can use the software stored in this location to upgrade Cisco systems.

This location path can also be viewed in **Administrative Tools > Configuration > General Settings > Software Directory** in the Cisco TMS application.

If the field is left blank, Cisco TMS will use the default value: **C:\Program Files (x86)\TANDBERG\TMS\wwwtms\Public\Data\SystemSoftware**.

If upgrading from an earlier version of Cisco TMS the path which was used in the previous version will not be changed.

Security Settings

Encryption Key

To improve security, all credentials stored in the database are encrypted. During installation of Cisco TMS, you are asked to either generate or provide an encryption key.

The **Key** field displays the key that Cisco TMS will use to decrypt that data in the database.

Caution: **If you delete or modify this key** Cisco TMS **will no longer be able to use these credentials to launch conferences, manage systems, retrieve feedback data from systems, or send emails.**

The Scan Db for Encryption Key Mismatch, page 297 tool can be run to identify all the credentials which cannot be decrypted by the current encryption key, and set all these credentials to blank or the default username and password for that system if Cisco TMS is aware of this.

TLS Client Certificates

When Cisco TMS is initiating an outbound connection to systems and if the system requests a client certificate from Cisco TMS, then it will provide TLS certificates configured here to verify its identity.

When initiating outbound connection to systems Cisco TMS can provide TLS certificates to verify its identity.

Listed here you will see the certificates currently available in the server's trust store which can be selected to be used as described above.

If there are no certificates listed here, check that the account you are using to run Cisco TMS Tools has read access to the private keys of the certificates.

You must also ensure that all accounts the Cisco TMS services are logged on as have read access to the private keys of the certificates.

Caution: **If the selected certificate or the private key used by** Cisco TMS **is not accessible, then Cisco TMS portal will not be accessible.**

To add a certificate under Cisco TMS Tool, perform the following steps:

1. Open **mmc.exe** from the start menu.
2. Select **File > Add/ Remove snap-in**, **Add or remove snap-in** dialog appears.
3. From **Available snap-ins:**, choose *Certificates*.
4. Click **Add**, **Certificate snap-in** dialog appears, then choose *Computer Account*.
5. Click **Next**, **Select Computer** dialog appears.
6. Click **Finish**.
7. Click **OK** in the **Add or remove snap-in** dialog.
8. In mmc.exe, expand **Console Root > Certificates (Local Computer) > Personal > Certificates** to find the newly added certificate.
9. Right click on the certificate of interest and select **All Tasks > Manage Private Keys**, a dialog for setting permissions on the private keys of the selected certificate appears.
10. Click **Add**, **Select Users, Computers, Service Accounts, or Groups** window appears.
11. Enter SERVICE in the text box below **Enter the object name to select (examples):**

    Note: If you login with admin credentials, user will not be prompted for the credentials while adding new account. If you login with non-admin account and try to add permission to certificate private key, then it will prompt for credentials to ensure that admin is modifying.
12. If server prompts for credentials, enter the admin username and password or the appropriate user credentials.
13. Click **Check Names** > **OK**.

14. In the **Select Users, Computers, Service Accounts, or Groups** dialog. Make sure that the read permission is checked under **Allow column for SERVICE**.

    Note: If **SERVICE** account is already listed under setting permission, make sure that it has Read permission.

15. Click **Apply** > **OK** in certificate permissions dialog.

You can view the newly added certificate in **TMS Tools > Security Settings > TLS Certificates**.

For more information about managing certificates, see *Microsoft Technet: Manage Certificates*.

Advanced Security Settings

It is possible to run Cisco TMS in a reduced functionality, high security mode by making changes to these settings.

- The settings must only be modified by a Cisco TMS administrator.
- Incorrect application of these settings can stop Cisco TMS from working altogether.

Table 180 Cisco TMS Tools advanced security settings

Sections and fields	Description
Optional Features Control	
Disable Provisioning	■ Removes the **Systems > Provisioning** menu option from the Cisco TMS application. ■ Stops the TMS Provisioning Extension Service from running. ■ The **Administrative Tools > Configuration > General Settings > Provisioning Mode** option becomes grayed out so that provisioning can not be activated from here.
Disable SNMP	■ Disables SNMP communication in the Cisco TMS application. ■ All SNMP fields in **Administrative Tools > Configuration > Network Settings** become grayed out—if de-selected the previous values will be reinstated.
Auditing	
Enable Auditing	If checked, Cisco TMS will log all updates, create and delete operations on Cisco TMS settings, systems, folders, users and groups. The log is located in **Administrative Tools >** Audit Log, page 288.
Purge Old Audit Log Data in Database	Displays the number of audit log entries in the database and how many days the entries will be kept before they will be purged automatically. If checked, **Number of Days to Keep Data** can be edited.
Transport Layer Security Options	

Table 180 Cisco TMS Tools advanced security settings (continued)

Sections and fields	Description
Communication Security	You can set the level of security required for communication for all Cisco TMS connections. Note that the following security settings impacts only Cisco TMS outbound connections. Unsupported TLS versions for Cisco TMS inbound connections can be disabled via Windows registry. For guidance, see the TLS/SSL Settings article. ■ *Medium:* Cisco TMS prefers HTTPS, using TLS 1.0, TLS 1.1 and TLS 1.2 for communication, but falls back to HTTP. It remembers the last used protocol for the system in the previous communication and going forward continues with the same protocol. Insecure protocols like Telnet and SNMPv2 are also used. ■ *Medium-High:* Cisco TMS will communicate using SSL for connections. SSL includes HTTPS and SSH, using TLS 1.1 and TLS 1.2. TLS 1.0 is not used by Cisco TMS. ■ *High:* Cisco TMS will communicate only using SSL for connections and will check that valid and signed certificates are present during communications, using only TLS 1.2 with proper Certificate validation. TLS 1.0 and TLS 1.1 are not used by Cisco TMS. For more information on security settings best practices, see Additional Information about Security Settings, page 296. Note that the following phone book types are not supported in *Medium-High* and *High* security mode. ■ *File Based Phone Book* ■ *H.350 Directory* ■ *H.350 User Directory* Note that the following services are not supported in *Medium-High* and *High* security mode. ■ PLCMDirectoryService ■ SNMPservice Irrespective of the chosen setting, end points can still reach Cisco TMS using HTTP. However, you can block this usage of HTTP by configuring IIS. For detailed information on configuring IIS, see *Cisco TMS Installation and Upgrade Guide*. For new installations and upgrades, the default security level will be set to Medium. If you are upgrading and had **Validate Certificates** enabled, you need to decide which option is most suitable for your setup. Note that, you must use FQDN to add a device in high security mode.
Enable Certificate Revocation Check	Checks the validity of certificates for all systems that Cisco TMS communicates with, using built-in Windows mechanisms for revocation checks.
Banners	

Table 180 Cisco TMS Tools advanced security settings (continued)

Sections and fields	Description
Banners on Web Pages, emails and Documents	Adds banners to: ■ The Cisco TMS application web site. ■ Microsoft Excel documents exported from Cisco TMS. ■ Cisco TMS/ Cisco TMSXE email templates.
Top Banner	Enter text to display in the top banner.
Bottom Banner	Enter text to display in the bottom banner.
Banner Color	Enter a color to add to the text of both top and bottom banners. On the Color Preview pane, you can see the preview of the color entered. You must either type a color name or an HTML color code.

Additional Information about Security Settings

- Cisco TMS does not control support for SSLv3 and below versions, and 3DES.

  - For guidance to disable SSLv3 and below versions, and 3DES, see the Microsoft article on Cryptographic Algorithms and Protocols.

- Cisco TMS does not control Ciphers.

  - For guidance on supported Ciphers, see the Microsoft article on Cipher Suites.

  - For guidance to configure the set of supported Ciphers, see the Microsoft article on Configuring Cipher Suite Priority Order.

- Cisco TMS does not control RC4 Ciphers. For guidance to disable the RC4 Cipher Suites, see the Microsoft article on disabling RC4.

Note: For more information about Microsoft issue with it's ciphers when a Windows machine acts as a client with an OpenSSL device acting as a server, refer to https://www.cisco.com/c/en/us/support/docs/conferencing/telepresence-management-suite-tms/212421-windows-ciphers-cause-tls-issue-between.html

Utilities

Change User Domain

If the Windows domain the Cisco TMS server is a member of has changed name, or the Cisco TMS server is not in a domain and the server hostname has changed, you can make Cisco TMS aware of this change here.

The changes made will only apply to usernames in Cisco TMS, not to user accounts on the domain itself.

Generate Phone Book

Here you can generate a phone book with folders and corresponding phone book sources based on the folder structure of **Systems > Navigator**.

Caution: **We recommend creating phone books from phone book sources in** Cisco TMS**. See** Creating and Managing Phone Books, page 210**.**

1. Open Cisco TMS Tools on the Cisco TMS server.
2. From the **Utilities** menu, select **Generate Phone Book**
3. Enter a name for the phone book.
4. Click **OK**.

A background job is scheduled to generate the phone book and its sources.

The phone book will be visible in Cisco TMS under **Phone Books > Manage Phone Books**.

Carrying out the above procedure more than once will not overwrite any previously created phone books or sources. A duplicate set of phone books and sources will be generated, and any unwanted phone books and sources generated in this way will have to be manually deleted one at a time.

Resolve Duplicate Keys

Customers affected by the duplicate external primary key issue found in Cisco TMS 14.4 and 14.4.1 can use this tool to identify conference series that have duplicate external primary keys, and select which is the correct conference. (For more information on the issue itself, see Cisco TelePresence Management Suite Software Release Notes (14.4.2).)

This tool should only be used if, after upgrading to 14.4.2 or later, this critical ticket appears in Cisco TMS: "Conferences with duplicate external primary keys found".

When the tool is accessed, all affected conferences are loaded into the page. Conferences with the same external primary key are grouped together, and the title, owner, recurrence pattern, and a link to open the conference or series in **Cisco TMS > Booking > List Conferences** are displayed.

Select the correct conference from each group of conferences as only one conference in the group should exist in Cisco TMS. Once you click **SELECT**, the remaining conferences in the group are deleted.

If it is not clear which conference is the correct one, review the Exchange resource calendars for the systems involved in the conference. If most or all of the resource calendars are in agreement with one of the duplicate conferences, that is probably the correct one to select.

If it is still not possible to identify the correct conference, contact the conference owner.

Click **VIEW LOG** for a list of the conferences that have been selected/deleted. This log (**log-tmstools-duplication-resolution.txt**) is located in the tmsdebug logs folder and contained in the **Download Diagnostic Files** download bundle.

Diagnostic Tools

SNMP Connectivity Checking Tool

When certain legacy systems are added into Cisco TMS, SNMP is used. If you are unable to add a system into Cisco TMS you can use this tool to check whether Cisco TMS can contact the system using SNMP.

- **IP Address**: IP address of the system you want to check
- **SNMP Read Community Name**: The community name set in **Cisco TMS > Administrative Tools > Configuration > Network Settings > General Network Settings > SNMP Community Name** which corresponds with the community name set on the system itself.
- **SNMP Timeout (ms)**: Number of seconds before Cisco TMS will give up trying to contact the system via SNMP.

Scan Db for Encryption Key Mismatch

- **Scan**: Scan the SQL database to get a list of all the credentials which have been encrypted and are affected by the encryption key having been changed (see).

- **Cleanup**: Set all data found in the scan to default credentials for that system, or remove the values completely.
- **Cancel**: Stop the scan while it is running.

A Cisco TMS ticket is generated if the encryption key has been changed; the ticket is removed on cleanup.

Note that phone book source and Webex credentials are not reset during cleanup.

TMS Log Collector

Cisco TMS Log Collector is a stand-alone tool that allows you to set Cisco TMS/TMSXE/TMSPE logs level to debug mode and also collect the logs based on the components installed on your server.

The two main functionalities of this tool are:

- Enable Log Selection :
  - It lists the components (Cisco TMS/TMSXE/TMSPE) that are installed on your windows server, so that you can select the available components logs and set to debug mode.
  - After you set the selected services to debug mode, the system restarts respective IIS (web related services) and Cisco TMS/TMSXE/TMSPE/ services.
  - Once the selected components are set to debug mode, you get an option to reset the logs to the original mode.
  - When you reset the logs back to the original mode, the system restarts respective IIS (web related services) and Cisco TMS/TMSXE/TMSPE/ services.

  Notes:

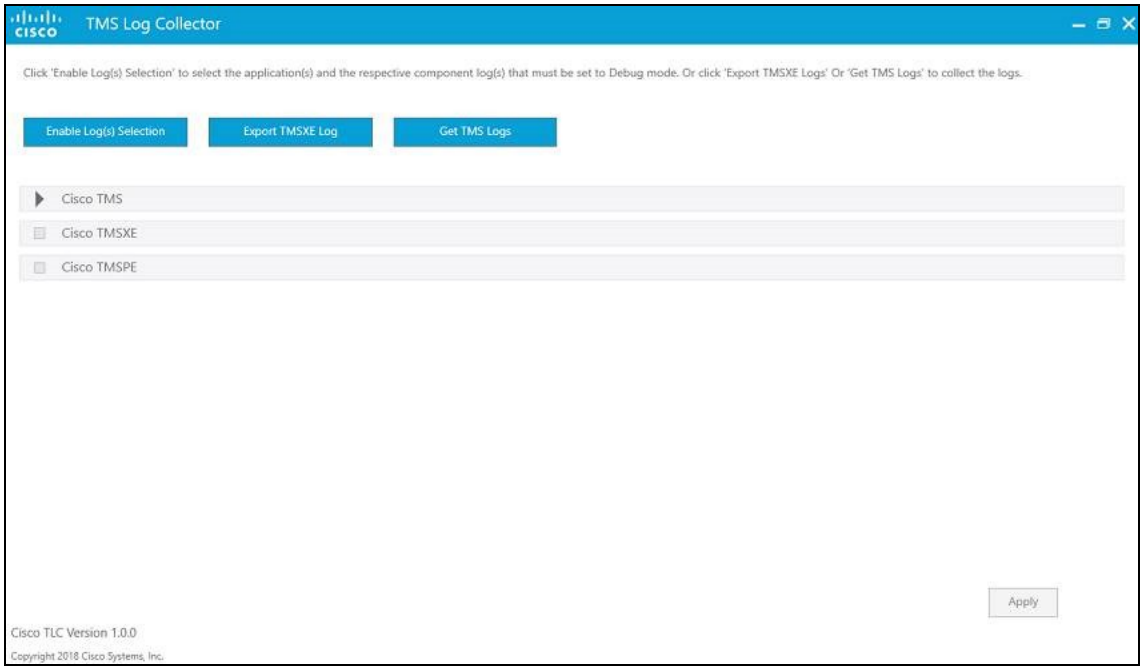
  - If there are any services which have been set to Debug mode manually without using the tool then those services will be in the disable mode(you cannot change the mode for those logs using this tool).
  - The IIS service is restarted only for web components.
  - **Warning**: When the Tool is in use, Cisco TMS/TMSXE/TMSPE Service Config files should not be updated manually.
- Collect Logs:
  - Option to collect and download Cisco TMS/TMSXE/TMSPE logs.
  - Export TMSXE Logs : You can export Cisco TMSXE Logs to the selected destination.
  - Get TMS Location: This option allows you to navigate to Cisco TMS portal page from where you can download the logs(Cisco TMSPE logs can also be collected along with Cisco TMS logs).

Notes:

- This tool works from Cisco TMS version 15.0, TMSXE 5.0 and TMSPE 1.5 onwards.
- This tool works only with Windows Server Admin credentials/permissions.
- If Cisco TMS and TMSXE are installed in different systems, then Cisco TMS Log Collector tool has to be installed and run in the respective systems.
- Cisco TMS provides a bundled installer with Cisco TMS Log Collection Utility .
- For more information about installation of Cisco TMS Log Collector, refer to Cisco TMS Bundle section in Cisco TelePresence Management Suite Installation and Upgrade Guide.
- For more information about uninstallation of Cisco TMS Log Collector, refer to Moving or Uninstalling Cisco TMS section in Cisco TelePresence Management Suite Installation and Upgrade Guide.

Launch TMS Log Collector

1. Launch **TMS Log Collector**. Cisco TMS/TMSXE/TMSPE components that are installed in the server are listed in Disable mode.

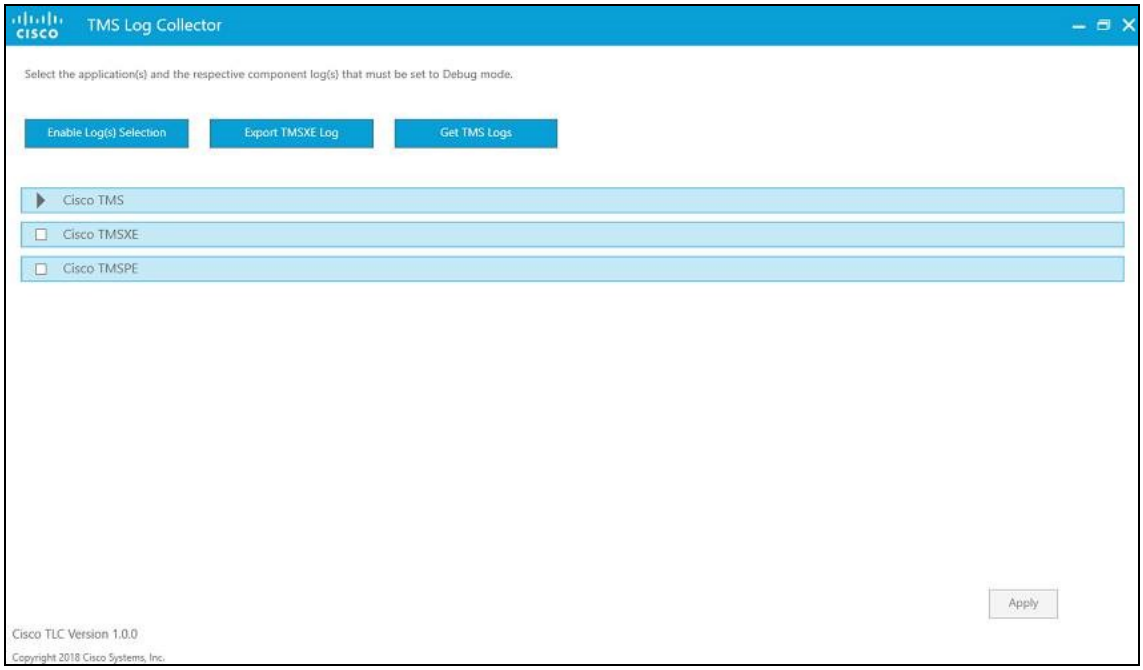


Note: **CiscoLogBackup** folder is created for backup of the Service files. When the tool is closed, this folder is removed automatically and it must not be manually deleted.

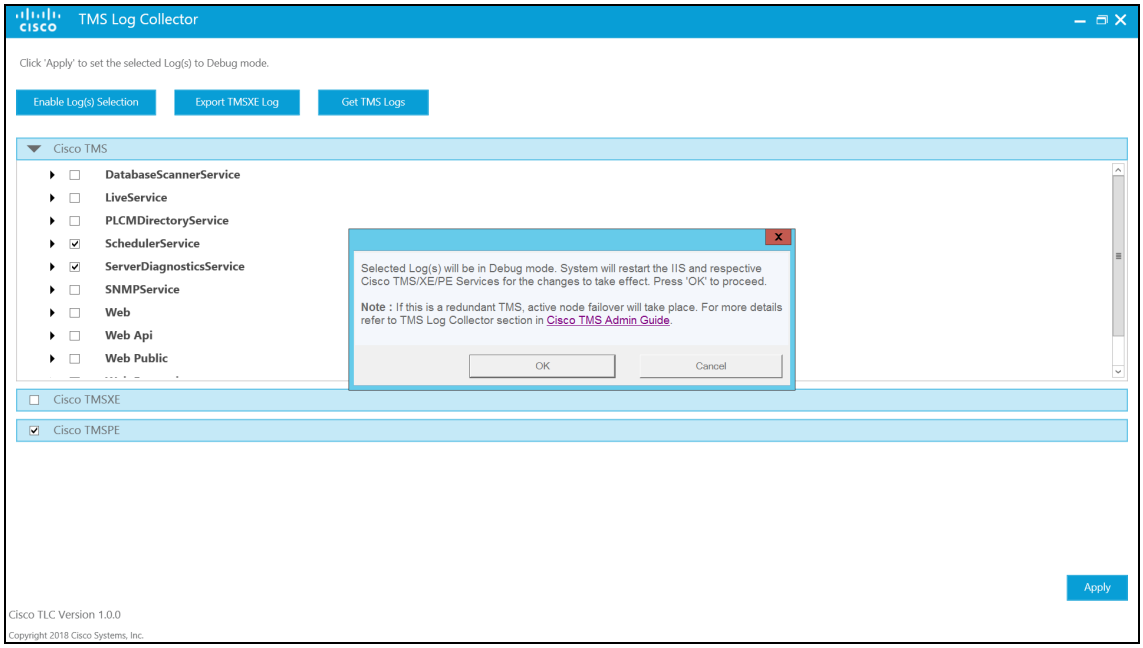
Set to debug mode

Follow the procedure to set the services to debug mode:

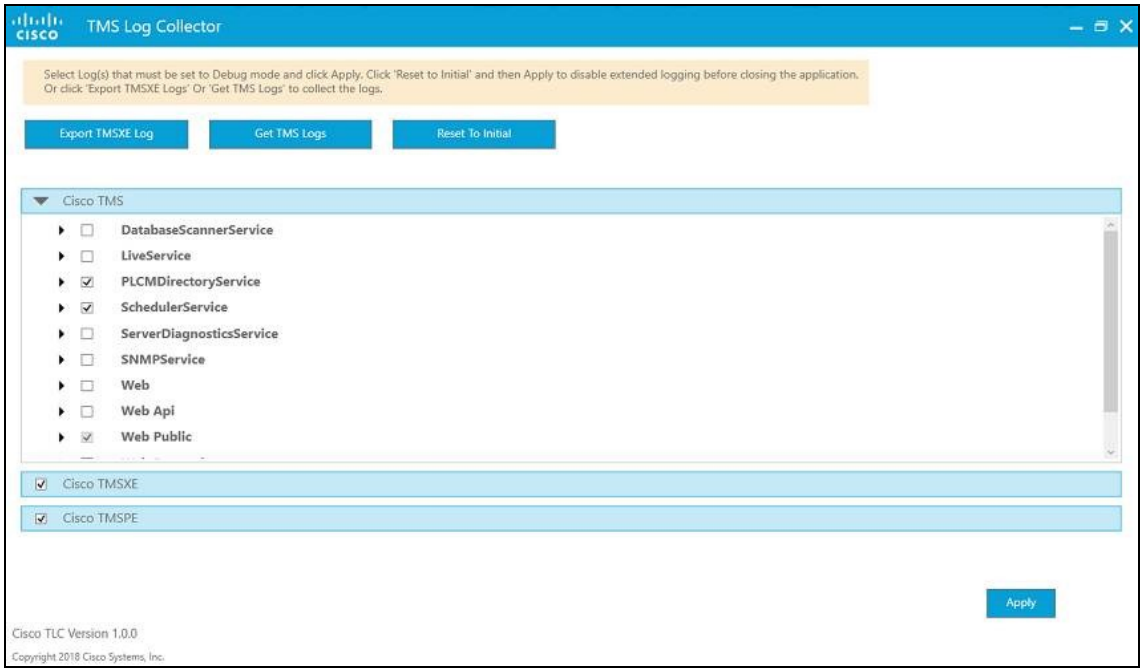
1. Click **Enable Log(s) Selection** to enable component services.
2. Select the respective service log that must be set to Debug mode.



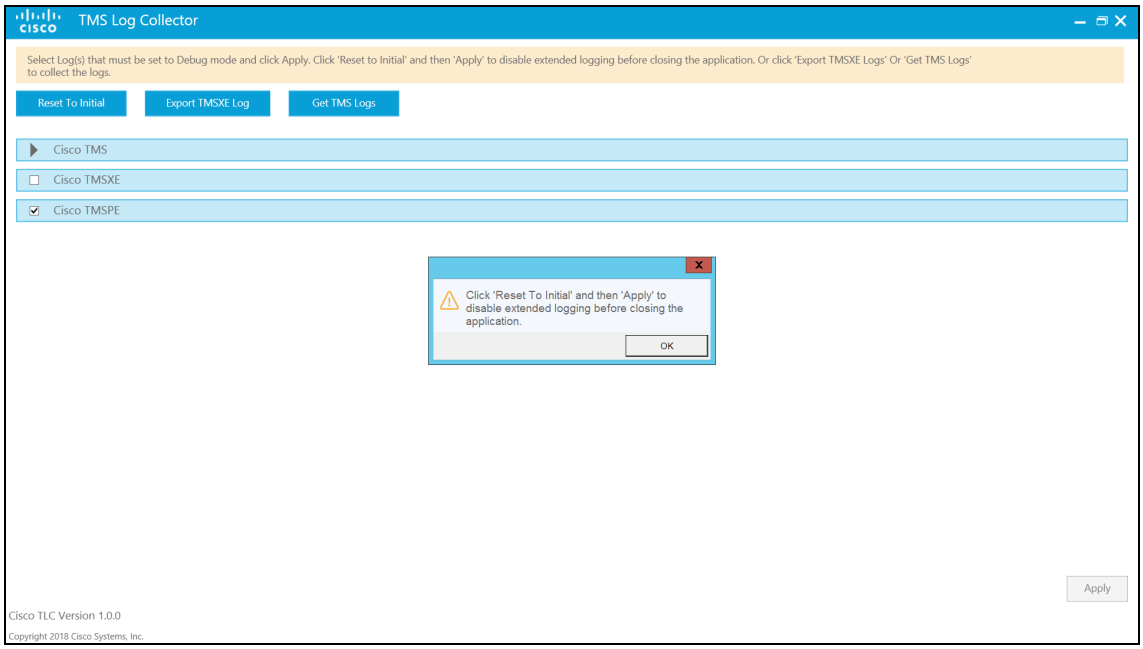
3. Click **Apply**. The selected logs are set to Debug mode.



4. Click **OK**. The logs are set to debug mode and the system restarts the IIS and respective Cisco TMS/TMSXE/TMSPE services. **Reset To Initial button** is enabled.

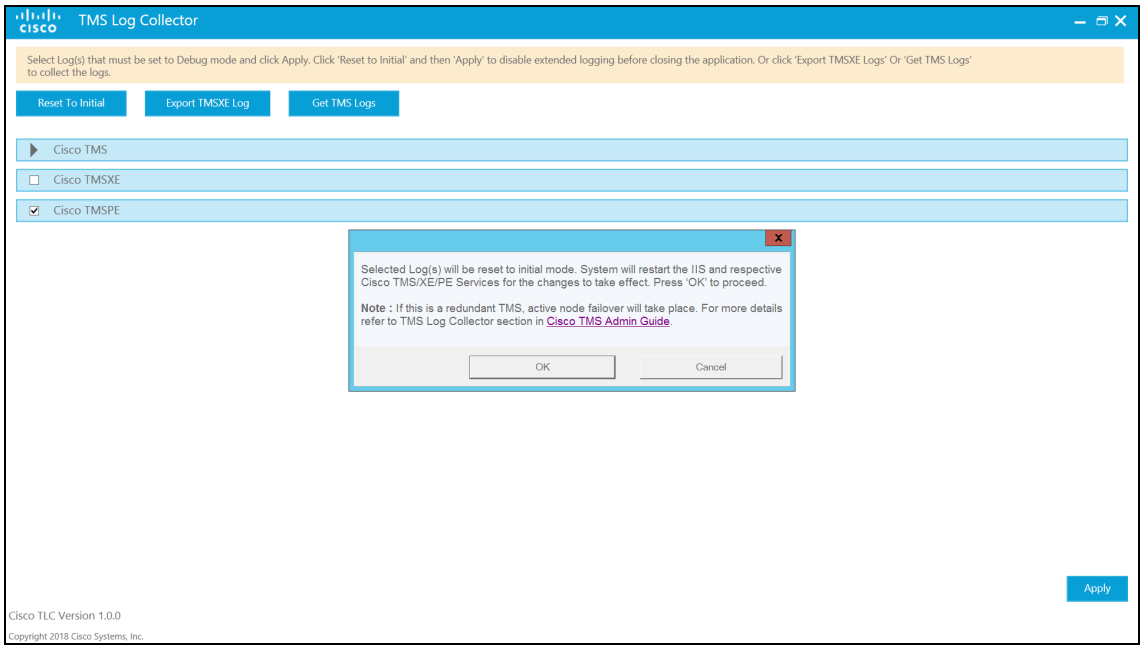


5. If you try to close the tool when it is in Debug mode, it will not allow you to close unless you reset the logs to their original mode.



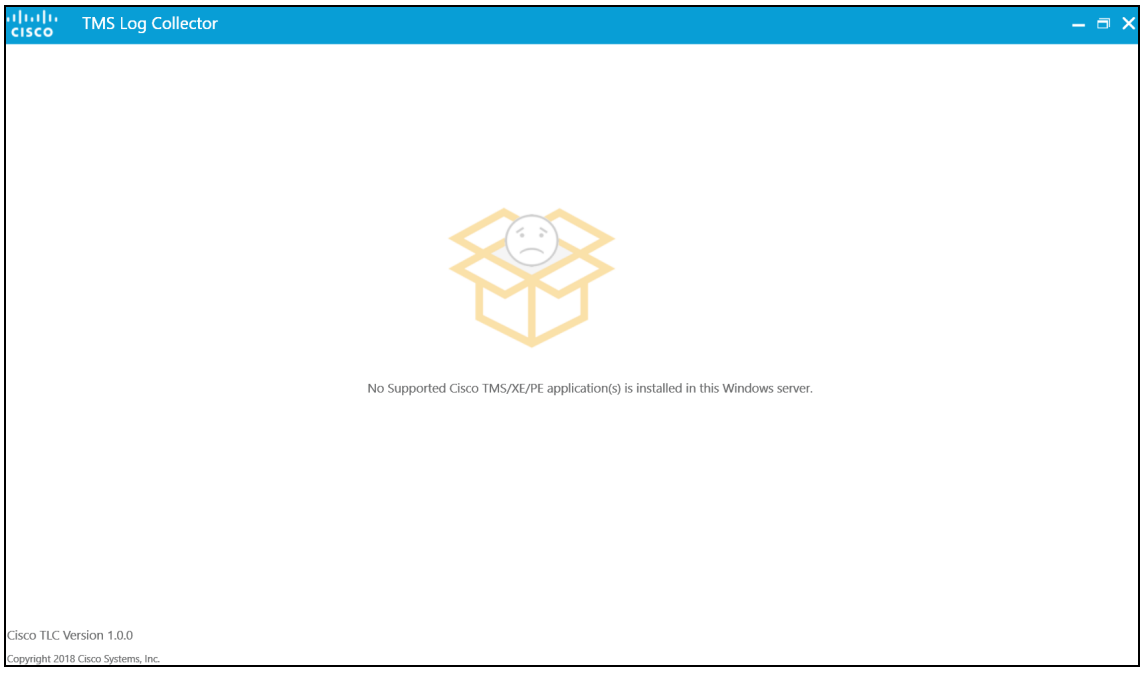
Note: For more information about the procedure to collect logs, refer to Collect Logs, page 303.

6. Click **Reset To Initial** and click Apply to reset logs level to the original mode and the system restarts the IIS and respective Cisco TMS/TMSXE/TMSPE services.
Note: The original mode is the mode in which the logs were before using the tool.



Unsupported Cisco TMS version or Components not installed

- If tool is opened on a server which does not have any of Cisco TMS or TMSXE or TMSPE installed or on a server where Cisco TMS version less than 15.0, TMSXE 5.0 and TMSPE 1.5 is installed, then the following screenshot is displayed.



TMS Redundant Deployment

For redundant set ups, you have to install TMS Log Collector tool in the server where troubleshooting steps will be performed. To prevent a failover as services will be restarted, it is recommended to stop services in the passive node prior to setting the debug level in the active node.

To prevent failover on passive node, perform the following steps:

1. Login to Remote Desktop in passive node.
2. Click on **Start** menu, search for Services and click on it.
3. Search for following Cisco TMS services and disable/stop them:

   - TMSDatabaseScannerService
   - TMSLiveService
   - TMSPLCMDirectoryService
   - TMSSchedulerService
   - TMSServerDiagnosticsService
   - TMSSNMPService

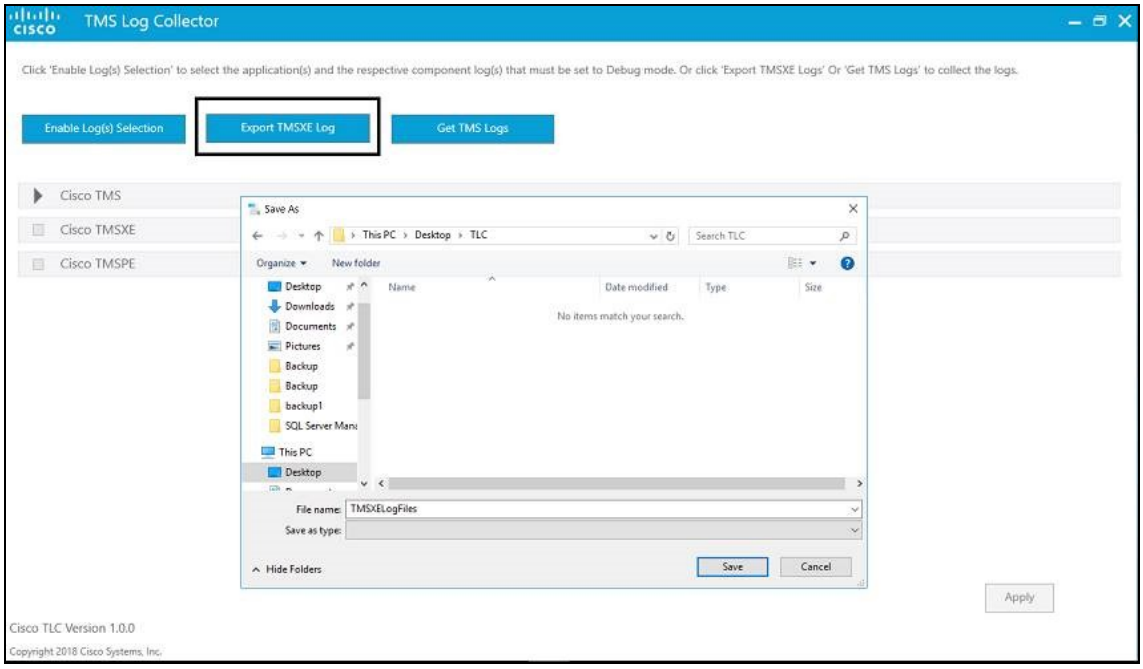
   Note: If Cisco TMSPE is installed, disable TMS Provisioning Extension Service.
4. Login to Remote Desktop in active node.
5. Install TMS Log Collector tool in Active node.
6. Set required services to Debug mode and collect all the required logs.
7. Close TMS Log Collector tool.
8. Re-login to remote desktop in passive node and enable all the services which are set to 'Disable' For more information, refer to Step 3.

Collect Logs

Export TMSXE Logs

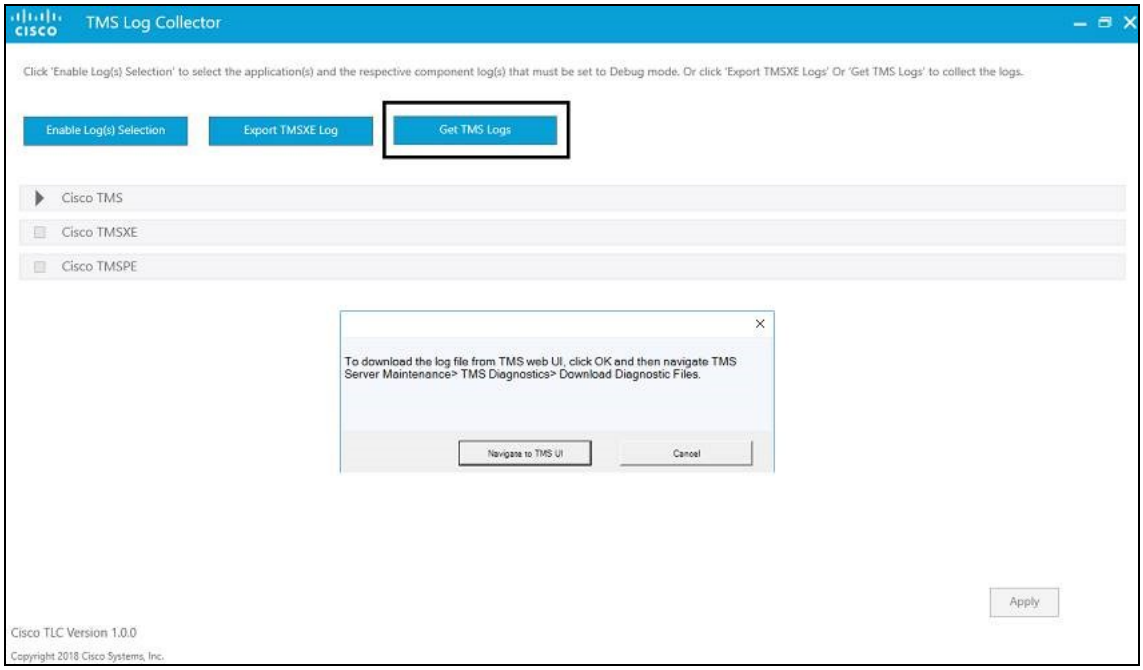
You can do the following:

- Export TMSXE logs to a selected destination.
- Change to the path where the log will be zipped and downloaded.
- Change the default zip file name, as needed.

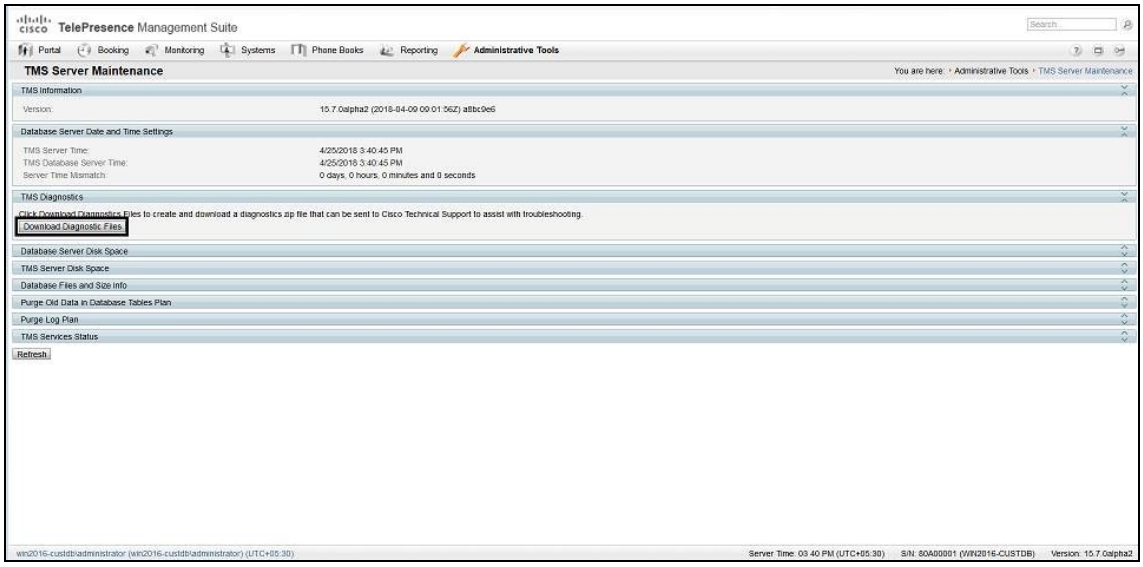


Get TMS Logs

1. Click **Get TMS logs**.



2. Click **Navigate to TMS UI** option in the pop-up and it will navigate you to the respective TMS page as displayed in the following screenshot. The location from where you download the logs is displayed.



Troubleshooting

When you open this tool, TMS Log Collector.txt will be generated in the path where it is installed. This log file is used to troubleshoot the issue with the TMS Log Collector tool.

Troubleshooting

This chapter addresses how to troubleshoot the various components of Cisco TMS.

Instructions on troubleshooting extension products can be found in the documentation for each extension.

Using the Logs 306
Website Scenarios 312
System Scenarios 313
Conference Scenarios 315
Java Applet Scenarios 316
Phone Book Scenarios 318
Reporting Scenarios 319
Cause Codes 321

Using the Logs

All Cisco TMS components and services include logging features. This section details where to find the logs, which logs are available, how to change the log levels, and reading the logs.

Downloading Log Files

1. Go to **Administrative Tools > TMS Server Maintenance**.
2. Click **Download Diagnostic Files**.

An archive containing the available log files will be downloaded to the client computer. Not all logs are enabled by default or at a sufficiently verbose level for troubleshooting. See Changing the Log Level, page 310 for instructions.

Extract IIS Logs with Cisco TMS Diagnostic files

Cisco TMS introduces a new functionality where you can include the most recent seven days of IIS logs within the Cisco TMS logs bundle. Cisco TMS supports the download of IIS logs which are stored on the local machine.

1. Select **Include IIS Logs** option and click **Download Diagnostic Files**. This downloads the IIS Log files along with Cisco TMS logs. By default, the IIS log file resides in **C:\inetpub\logs\LogFiles**.

Note: After installation of Cisco TMS, if the log location is changed, then you need to change the IIS log location in registry. Also, you have to set permission to "**IIS APPPOOL\TMSNet40AppPool**" for the newly changed IIS log location.

Locating the Logs on the Server

You can also access the logs directly on the server. The default log location is:

Program Files (x86)\TANDBERG\TMS\data\Logs.

There are two log folders; **Install** and **TMSDebug**.

Modifying the Log Location

The environment variable `TMSLOGFILES` is set by the Cisco TMS installer.

- To change the log location, we strongly recommend changing it by using this variable.
- Note that the log location must *not* be inside any of the Cisco TMS web sites.

Log Overview

All Cisco TMS logs have a **.txt** extension.

Install

Table 181 Logs created by the Cisco TMS installer

Log name	Description
Install_log	Keeps a record of all installations, any uninstallations, and upgrades since the software was first installed on the server.
Databaselog	Keeps a record of database schema patches applied during upgrades. If applying a patch fails, the log will detail which patch failed and contain a stack trace.
TMSInstallDllFilesInfo	One log per installation/upgrade performed on this server.

TMSDebug

The following table details all logs created by the various modules of Cisco TMS and the default log levels. All configuration file paths are derived from **C:\Program Files (x86)\TANDBERG\TMS**.

Table 182 Cisco TMS logs with configuration files and default log level

Log name	Description	Level	Configuration file
log-api	Logs the activity of the REST API for configurations.	WARN	**\wwwTMS\api\Web.CONFIG**
log-cmsfailover-liveservice	Logs the failover information when Cisco Meeting Server failover occurs.	INFO	**\Services\TMSLiveService.exe.CONFIG**
log-conductorfailover-liveservice	Logs the failover information when Conductor failover occurs.	INFO	**\Services\TMSLiveService.exe.CONFIG**
log-etl	Logs the activity of the ETL job that collects data for the Bridge Utilization report. Not configurable.	INFO	
log-feedback-web-public-tms	Logs the feedback from Managed endpoints. To activate, set "FeedbackLogger" to DEBUG.	OFF	**\wwwTMS\public\Web.CONFIG**

Table 182 Cisco TMS logs with configuration files and default log level (continued)

Log name	Description	Level	Configuration file
log-lcdpanel	LCD panel log. Cisco TelePresence Management Server appliance only. Not configurable.		
log-liveservice	Keeps a record of TMSLiveService, page 19	WARN	**\Services\TMSLiveService.exe.CONFIG**
log-livesignals	Additional LiveService logging. Only activate when requested by Cisco support. To activate, set "SignalProcessingLog" to INFO.	WARN	**\Services\TMSLiveService.exe.CONFIG**
log-plcmdir	Logs the activity of TMSPLCMDirectoryService, page 20	WARN	**\Services\TMSPLCMDirectoryService.exe.CONFIG**
log-schedulerservice	Logs the activity of TMSSchedulerService, page 19	WARN	**\Services\TMSSchedulerService.exe.CONFIG**
log-scheduling-liveservice	Keeps a record of LiveService routing decisions. To activate, set "SchedulingLogger" to INFO or DEBUG.	OFF	**\Services\TMSLiveService.exe.CONFIG**
log-scheduling-schedulerservice	Keeps a record of SchedulerService routing decisions. To activate, set "SchedulingLogger" to INFO or DEBUG.	OFF	**\Services\TMSSchedulerService.exe.CONFIG**
log-scheduling-web-external	Keeps a record of Cisco TMSBA routing decisions. To activate, set "SchedulingLogger" to INFO or DEBUG.	OFF	**\wwwTMS\external\Web.config**

Table 182 Cisco TMS logs with configuration files and default log level (continued)

Log name	Description	Level	Configuration file
log-scheduling-web-tms	Keeps a record of routing decisions for bookings created using the Cisco TMS web interface. To activate, set "SchedulingLogger" to `INFO` or `DEBUG`.	`OFF`	**\wwwTMS\Web.config**
log-systemapi-web-tms	Logs manual actions initiated by users within Cisco TMS.	`OFF`	**\wwwTMS\Web.CONFIG**
log-systemapi-web-public-tms	Logs feedback from controlled systems, such as CDRs. To enable: Set `FeedbackLogger` to `DEBUG` to log incoming communication.	`OFF`	**\wwwTMS\public\Web.CONFIG**
log-systemapi-web-external	This log is only used by internal Cisco TMS APIs.	`OFF`	**\wwwTMS\external\Web.CONFIG**
log-systemapi-databasescannerservice	These logs record outgoing communication initiated by the services. To enable: ▪ Set `SystemAPILogger` to `DEBUG` to log outgoing communication.	`OFF`	**\services\TMSDatabaseScannerService.exe.CONFIG**
log-systemapi-liveservice		`OFF`	**\services\TMSLiveService.exe.CONFIG**
log-systemapi-schedulerservice		`OFF`	**\services\TMSSchedulerService.exe.CONFIG**
log-systemapi-SNMPservice		`OFF`	**\services\TMSSNMPService.exe.CONFIG**
log-TMSAgentDiagnostics	This log is no longer in use.		
log-tmsagentproxy	Logs the activity of the Cisco TMSPE IIS Proxy.	`WARN`	**\wwwProvisioning\Web.config**
log-TMSDatabaseScanner	Logs the activity of TMSDatabaseScannerService, page 19	`WARN`	**\Services\TMSDatabaseScannerService.exe.CONFIG**
log-TMSServerDiagnosticsService	Logs the activity of TMSServerDiagnosticsService, page 20	`WARN`	**\Services\TMSServerDiagnosticsService.exe.CONFIG**
log-TMSSNMPservice	Logs the activity of TMSSnmpService, page 20	`WARN`	**\Services\TMSSSNMPService.exe.CONFIG**

Table 182 Cisco TMS logs with configuration files and default log level (continued)

Log name	Description	Level	Configuration file
log-tmstools-duplication-resolution	Logs the activity of the Resolve Duplicate Keys tool. Logs which conferences were kept and which were deleted.	INFO	**\TMSTools\TMSTools.exe.CONFIG**
log-web	Logs all web interface activity.	WARN	**\wwwTMS\Web.CONFIG**
log-web-cdm	Logs errors in feedback from CTS endpoints.	WARN	**\cdm\Web.CONFIG**
log-webex-web-tms	Logs Cisco Collaboration Meeting Rooms Hybrid activities.	OFF	**\wwwTMS\Web.CONFIG**
log-web-external	Logs activities that use password protected APIs, such as Cisco TMSBA.	WARN	**\wwwTMS\external\Web.CONFIG**
log-webex-web-external	Logs the communication with the Webex API. To activate, set "WebexApiLogger" to DEBUG.	OFF	**\wwwTMS\external\Web.CONFIG**
log-web-public	Logs all activities that use public APIs, such as phone books and feedback.	WARN	**\wwwTMS\public\Web.CONFIG**
log-xml	Logs feedback parsing errors.	WARN	**\wwwTMS\public\Web.config**
phonebook-stats.txt	Logs all corporate directory queries from endpoints.	WARN	**\wwwTMS\public\Web.config**
log-phonebook-request-response	Logs requests and responses for phonebook queries from endpoints.	DEBUG	**\wwwTMS\public\Web.config**
log-bookingapi-request-response	Logs requests and responses for Cisco TMS Booking API interactions. To activate, set "BookingApiLogger" to DEBUG.	OFF	**\wwwTMS\external\Web.config**

Changing the Log Level

There are four log levels available for each log file, with the default values and location of the relevant configuration file listed in the table above.

The available values are:

- `OFF`: Disables logging for the component.
- `WARN`: Only logs warnings and errors.
- `INFO`: Contains the same as WARN with additional, non-critical, log entries.
- `DEBUG`: This log level is very verbose, and should only be activated if instructed to do so by a Cisco support representative. Debug logging is normally only used in advanced troubleshooting scenarios, and disabled as soon as the troubleshooting session ends.

To change the log level:

1. Locate the appropriate configuration file listed for the log in Log Overview, page 307.
2. Create a backup copy of the configuration file before making any modifications to it.
3. Open a text editor as an administrator.
4. Open the configuration file in the text editor.
5. Locate the `<log4net>` element, the `<root>` or `<logger>` element for appropriate log file desired, and then the `<level>` element.
   The `<root>` element is for the primary service log. The `<logger>` elements are for secondary logs for the service.
   Example: SystemApiLogger.
6. Update the element with the desired value, for example from `<level value="WARN"/>` to `<level value="DEBUG"/>`.
7. Locate and modify any other required elements as stated in Log Overview, page 307.
8. Save and close the file.
   - For all logs related to services, you must restart the relevant Windows service for the change to take effect.
   - For all IIS-based logs, the new log level takes effect immediately.

We strongly recommend reverting the log level back to its initial value after debugging, as increasing the log level significantly increases the size of the log.

The steps to revert are the same as above.

Reading the Logs

The Cisco TMS version and the user account the component uses are logged every time the component starts.

Example log entries:

```
2013-06-19 20:14:29,108 [6] WARN  Tandberg.TMS.Framework.AccessControl.AclService - Access denied to:
SystemRead
```

```
2013-06-20 14:53:04,503 [75] ERROR ASP.global_asax - System.Web.Services.Protocols.SoapException:
Unspecified Error
at Tandberg.TMS.External.SoapExceptionThrower.Throw(ExceptionContext exceptionContext)
       at Tandberg.TMS.External.SoapExceptionThrower.Throw(Exception e, String actor)
at Tandberg.TMS.Global.Application_AuthenticateRequest(Object sender, EventArgs e)
at System.Web.HttpApplication.SyncEventExecutionStep.System.Web.HttpApplication.IExecutionStep.Execute()
at System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously)
```

The first log entry is from a **log-web** file. It is logged as a WARN (warning), and shows that a user tried to access a page they do not have access to. The attempt was denied by the Access Control List mechanism of Cisco TMS, and a corresponding log entry was created. In general, a WARN log entry is not critical and indicates no loss of data or functionality.

The second log entry is from a **log-web-external** file. It is logged as an ERROR, and a full stack trace is displayed. In general, an ERROR followed by a stack trace indicates that data or functionality has been lost. In this specific case, the root cause of the ERROR is that a Cisco TMSBA client tried to create a new booking, but had syntactical errors in the conference object it provided. Cisco TMS then discards the booking and logs an ERROR, and unless the client re-tried the save operation using a valid conference object, the conference is lost.

IIS Logs

Cisco TMS uses Windows Server's Internet Information Services (IIS) as its web server. The IIS logs could be useful for troubleshooting certain kinds of Cisco TMS problems, for example:

- CDR data is missing.
- Intermittent phone book problems.
- The Cisco TMS web interface loads very slowly.

In default IIS installations, the logs are found in the **C:\inetpub\logs\LogFiles** folder. When correlating IIS log entries with Cisco TMS log entries, note that IIS log entries are in UTC.

For assistance on configuring the IIS logs, see the following Microsoft TechNet article:

http://technet.microsoft.com/en-us/library/cc732079%28v=ws.10%29.aspx

Purging IIS Logs

Note that IIS logs are not part of the Cisco TMS purge log plan. We recommend setting up your own purge plan or manually removing these logs at regular intervals.

Website Scenarios

This section describes troubleshooting scenarios involving Cisco TMS as a website.

Cisco TMS does not Load

In the event of Cisco TMS not loading, the problem might be network, web server, or database related. Troubleshooting steps for possible web server and database issues are included below.

Basic Steps

Web Server

- Verify that IIS is running.
- Check whether you can access the default webpage **http://<tms_server_name>**.
- See the logs in **c:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug\log-web.txt**.

Database

- Check the Database Scanner log for a stack trace declaring that the SQL server is unavailable.
- Go to the **Services** panel on your database server:
  - Verify that SQL Server is running.
  - If you are running a named instance on a remote server, make sure that the SQL Server browser service is also running.
  - As a troubleshooting measure, you can also restart these services.
- Verify that the information Cisco TMS uses to connect to the database is correct. For this, we recommend using Cisco TMS Tools, page 290.

Advanced steps

Web server

- Verify that the virtual directories described in the Internet Information Services Web Server and Applications, page 18 section:
  - Exist on the Cisco TMS server.
  - Point to valid directories on the server.
- Check that the permission settings are correct according to the list above.
- Verify that IIS allows for running .NET extensions.

Web Server Symptoms

- The corporate directory on Cisco endpoints does not work.
- Endpoint statistics reports are empty.

System Scenarios

This section covers possible issues with systems using Cisco TMS.

New Systems are not Automatically Discovered

If new systems on the network are not automatically discovered, try the steps below.

Basic Steps

- Make sure no SNMP tool outside of Cisco TMS is running on the server
- Verify that the system's management address (feedback receiver if an infrastructure system) is set to **http://<FQDNofTMS>/tms/public/feedback/code.aspx**. If the address is set up to use HTTPS, this must be enabled in Cisco TMS IIS.
- Check the logs for symptoms or error messages at **C:\Program Files\TANDBERG\TMS\data\Logs\TMSDebug\log-TMSSNMPservice.txt** on the server.

System Information and Status Outdated

If system information and system status in Cisco TMS are outdated; systems not responding still have the status *In Call* or *Idle*, try the steps below.

Basic Steps

- Check the logs for symptoms or error messages at **C:\Program Files\TANDBERG\TMS\data\Logs\TMSDebug\log-TMSDatabaseScanner.txt** on the server.
- Restart TMSDatabaseScanner. For more information about this Windows service, see TMSDatabaseScannerService, page 19.

Scheduled Events not Starting

If scheduled events do not start, try the steps below.

Basic Steps

- Check the logs for symptoms or error messages at **C:\Program Files\TANDBERG\TMS\data\Logs\TMSDebug\log-schedulerservice.txt** on the server.
- Restarting TMSSchedulerService. For more information about this Windows service, see TMSSchedulerService, page 19.

System Upgrade Fails

Upgrades Fail with a "100% Event failed" Message

When a scheduled upgrade task fails with a "100% Event failed" error in the **System Upgrade Activity Status**, click the **Description** field to view the specific error message.

Unable to Connect to the Remote Server

Error: "The event failed to complete. Details: hostAddress: 10.1.2.3, description: GetDocument Failed. URL: https://10.1.2.3/getxml?location=/Configuration/, base exception: Unable to connect to the remote server"

Basic Steps

This error message indicates that Cisco TMS was unable to connect to the endpoint to initiate the upgrade.

- If **Communication Security** in Cisco TMS Tools is set to *Medium* , HTTP or HTTPS must be enabled in the endpoint. **If Communication Security** in Cisco TMS Tools is set to *Medium-High* or *High*, HTTPS must be enabled in the endpoint.
- Enabling these services could require a reboot of the endpoint for Cisco TMS to pick up the change.

Software Directory not Accessible

"The event failed to complete. Details: Software Directory not accessible via IIS/HTTP."

Basic Steps

This error message indicates that Cisco TMS was unable to create a software upgrade URL it could provision the endpoint with.

1. Verify that the **Software Directory** (configurable in **TMS Tools**) is a subfolder of **C:\Program Files (x86)\TANDBERG\TMS\wwwTMS**
2. Restart IIS and SchedulerService.

Upgrades Hang in a "25% Executing" State

Endpoints that run Collaboration Endpoint Software or TC software version 6.0 and above have the ability to provide feedback to Cisco TMS about the upgrade process, so that Cisco TMS can provide an accurate status in the **System Upgrade Activity Status**.

When a scheduled upgrade task hangs in a "25% Executing" state, it indicates that the endpoint is unable to get the new software package from the URL Cisco TMS provisioned it with.

Basic Steps

Using a web browser, go to **http://ip.address.of.endpoint/status.xml**. Verify that:

- Within the <Provisioning> element, there is a <URL> element showing a URL pointing to the Cisco TMS server.
- The URL displayed is accessible using a web browser.

The URL is built using one of the addresses in **Administrative Tools > Network Settings > Advanced Network Settings for Systems on Internal LAN** as the base, and with the folders defined in **Administrative Tools > General Settings >Software directory** appended to the base.

Upgrades Hang in a "60% Executing" State

When an upgrade task stays at "60% Executing", the endpoint is either ready to install, or currently installing the software package it just downloaded from Cisco TMS. Cisco TMS will not move an upgrade task out of a "60% Executing" state unless the endpoint sends an event to Cisco TMS stating that the upgrade either succeeded or failed.

Basic Steps

Ensure that:

- The endpoint's feedback URL and management address are pointing to Cisco TMS. A **Force Refresh** of the endpoint in **Systems > Navigator** will create a ticket if one or both are incorrect.
- The software upgrade is either in progress, has aborted, or has completed. Consult your endpoint documentation for information on how to verify results of the software upgrade.

Tickets not Raised

If there is less than 10% free disk space or the database is larger than 90% of its maximum size, and no tickets are raised, try the steps below.

Basic Steps

- Check the logs for symptoms or error messages at **C:\Program Files\TANDBERG\TMS\data\Logs\TMSDebug\log-TMSServerDiagnosticsService.txt** on the server.
- Restart TMSServerDiagnosticsService. For more information about this Windows service, see TMSServerDiagnosticsService, page 20.

Conference Scenarios

This section covers possible issues with Cisco TMS conferences.

Call Does Not Start

If the log in the **Conference Control Center** is almost empty, containing only one line that says "Created", or several related to conference changes but none to the launching of the conference, try the steps below.

Basic Steps

- Check the logs for symptoms or error messages at **C:\Program Files\TANDBERG\TMS\data\Logs\TMSDebug\log-liveservice.txt** on the server.

Advanced Steps

Using Wireshark, verify that Cisco TMS is sending commands to all systems involved in the call.

Java Applet Scenarios

The **Conference Control Center** and **Graphical Monitor** use a Java applet for displaying dynamic information. This section covers possible troubleshooting scenarios involving the Java applet and how to resolve them.

Username and Password Prompt Keeps Reappearing

The Java Applet will require the users to authenticate themselves if the Cisco TMS server is not part of the domain (or trusted by the domain) that the user is logged into.

Basic Steps

Insert the username and password when prompted for each session.

Advanced Steps

Make the Cisco TMS server part of the domain and verify the same.

Applet does not Load

Java Runtime Environment may not be installed on the computer, and the computer does not have direct access to the Internet to download it automatically.

If the applet is installed, but not loading, a proxy server might be preventing the Java applet from retrieving the necessary data from the Cisco TMS server. To open the Java console, right-click the Java icon in the systray and select Open Console. Error messages stating "Unknown source" will be displayed. To solve this problem, try one or more of the points below.

Basic Steps

- If Java is not installed, go to http://www.java.com/ to download and install Java.
- If using the server's IP address when accessing Cisco TMS, try again with the hostname for the Cisco TMS server.
- Configure the Java client through the Java Control Panel to use Direct Connection rather than using the browser's proxy settings.

Applet Is Slow to Load or will not Load Completely

The applet will normally be finished loading within 5 seconds of opening the page. If you experience a significantly higher loading time, try the points below.

Basic Steps

- Turn off caching in Java and delete the existing temporary files:
  a. Open the **Java Control Panel**.
  b. Click the General tab.
  c. Click **Settings**, click **View Applets**.
  d. De-select **Enable Caching** in the lower left corner.
  e. Click **OK**.
  f. Click **Delete Files**.
  g. Select all check boxes.
  h. Click **OK**.

i. Click **OK**.
j. Click **OK**.

- Remove old or duplicate Java clients from Internet Explorer:
  a. Click **Tools** in the Internet Explorer menu.
  b. Click the Programs tab.
  c. Click **Manage Add-ons**.
  d. Disable all old or duplicate Java plug-ins.
- Remove Google Desktop. We have seen issues where Google Desktop is conflicting with the Java plug-in and significantly increasing the loading time of Java applets. Other desktop search engines have not displayed the same symptoms.
- If using Java JRE version 6, update 15 or later, you will need to de-select **Enable the next generation Java plug-in...** under **Advanced** on the Java Control Panel to make the Graphic Monitor work as expected.

Mozilla Firefox Blocks Java Plugin

Mozilla Firefox version 17.0 and above prompts you to activate Java plugin every time you open **Conference Control Center**. Follow the steps given below, to permanently activate Java plugin.

In Mozilla Firefox:

1. Click the **Open menu** icon.
2. Click **Add-ons**.
3. Select **Plugins** tab on the left panel.
4. Select **Java(TM) Platform SE** version 8 and above from the plugins list.
5. Click the drop down list and select *Always Activate* option.

Quicker Load of Monitor

When Cisco TMS is upgraded, users may experience that loading of **Conference Control Center** and **Graphical Monitor** are slowed down. This is caused by old versions of the .jar files in the Java Applet cache.

To fix the problem;

1. Open the Java Control Panel (in your computer's Control Panel)
2. Click the **General** tab.
3. Click **View...**
4. Go to**Temporary Internet Files**.
5. Delete files with extension .jar.

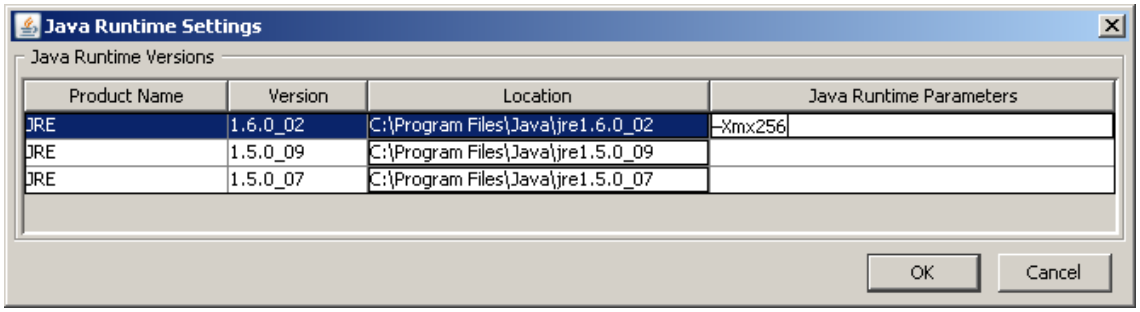
Out of Memory

Depending on the number of systems in your Cisco TMS installation and the number of ongoing conferences, users might experience memory problems with **Conference Control Center** or **Graphical Monitor**. The reason for this is that Java Applets as a default are only allowed to use 64 MB of memory. If you are having problems with out of memory exceptions you will experience that the Applets might 'hang' or seem very slow and find traces of **OutOfMemory** exceptions in the **Sun Java Console** found under the **Tools** menu in Internet Explorer. To avoid the problem you can increase the maximum amount of memory these Applets can use.

Increase Maximum Amount of Memory

Open the **Java Control Panel** (in your computer's Control Panel), click the **Java** tab and click **View...** on the **Java Applet Runtime Settings**. The **Java Runtime Settings** will show you the runtime versions currently installed on your

machine. Find the most recent 'Version' and add **-Xmx256** to the **Java Runtime Parameters** box (see screenshot below). This will increase the maximum amount of memory the Applets can use from the default value of 64 MB to a maximum of 256 MB. You can of course change the value to any amount you see fit.



Phone Book Scenarios

This section covers troubleshooting scenarios related to Cisco TMS phone books as they may present both client-side and in Cisco TMS.

Phone Book (Corporate Directory) Errors

Table 183 Possible errors displayed on endpoint due to problems with corporate directory

Message	Explanation or suggested solution
Request timed out, no response	The Cisco TMS server is busy, try again.
Warning: directory data not retrieved: 404	▪ The endpoint is configured with the IP address of a different web server than the Cisco TMS server. ▪ The corporate directory path on the endpoint is wrong.
Warning: directory data not retrieved: 401	▪ The "Public" virtual directory on the Cisco TMS server is not configured to allow Anonymous Access. ▪ The most common problem here is that anonymous access is set, but the account used has been overwritten by a group policy. The default IUSR user is a part of the guest account, and typically group policies disable this account.
Cisco TMS: No phonebook(s) set on this system	▪ No phonebook(s) set on this system in Cisco TMS. Configure the endpoint to subscribe to phonebooks in Cisco TMS. ▪ Using NAT on the endpoint can lead to Cisco TMS not recognizing the system and will not allow it to retrieve any phone books.
Request timed out, no response	The endpoint is configured with the IP address of a non existing web server.
No contact with server	The IIS is restarting or in a state where corrupted messages are received.

Polycom Endpoints do not Get Phone Books

If Polycom endpoints are not receiving phone book data, try the steps below.

Basic Steps

- Check the Phone Book and Source Activity Status, page 224 pages for detail on phone books failing.
- Check the logs for symptoms or error messages at **C:\Program Files\TANDBERG\TMS\data\Logs\TMSDebug\log-plcmdir.txt** on the server.
- Verify that the required ports for the endpoint are open on the Cisco TMS server. For details, see *Cisco TMS Product Support*.

Reporting Scenarios

This section covers troubleshooting scenarios related to Cisco TMS reporting functionality.

Bridge Utilization Report

Data Inconsistencies

Past Data Inconsistencies

A bridge that was replaced with a bridge of a different capacity, or reconfigured in the past, for example from HD to Full HD, will lead to inaccurate past data and could lead to more than 100% usage being reported.

Purging bridges does not delete their historical Bridge Utilization data. The same applies when transitioning to a TelePresence Conductor-managed bridge.

If the ETL job fails, a TMS ticket will be generated: check the ETL log that is available in the **Download Diagnostic Files** zip in **TMS Server Maintenance**.

Reconnected Bridge Call

In some scenarios, if participants in a multipoint conference lose connection to a bridge and reconnect, the new connection may use a different port on the bridge. If the initial port has not yet been released, the participant can occupy two ports. This results in the bridge reporting a misleading participant count to Cisco TMS.

Port Usage Imprecision

Depending on port availability, participants may have their connection downgraded (video to audio) or upgraded (audio to video) during a conference.

Any participant that has used a video port at any point during a conference will be reported as a video participant when the conference ends. This means that a conference could be reported to have more video participants than the available video ports on the bridge.

The report is based on actual call data provided by the managed bridges and does not consider the number of ports originally scheduled.

No CDRs from Endpoints Running Cisco Collaboration Endpoint Software, TC, and TE Software

Basic Steps

Verify that:

- The endpoint is on a software version supported by Cisco TMS.
- The endpoint has the correct management address
- The Cisco TMS server's IIS has Anonymous Authentication enabled for /tms/public, and that an Active Directory group policy isn't restricting the IUSR account.

Advanced Steps

Capture a Wireshark trace on the Cisco TMS server, and pre-filter it on the endpoint's IP address. To successfully get a CDR from a Cisco endpoint, you should then see this sequence of events:

1. The endpoint POSTs to **/tms/public/feedback** that it is in a call. The endpoint continuously sends feedback to Cisco TMS while the call is ongoing.
2. When the call has ended, the endpoint POSTs a call item to **/tms/public/feedback**. Example call item from Cisco TelePresence SX20 running TC 5.1.1 software:

```
<Call item="175">
       <CallId item="1">48</CallId>
       <Protocol item="1">H323</Protocol>
       <Direction item="1">Incoming</Direction>
       <CallType item="1">Video</CallType>
       <RemoteNumber item="1">h323:1234</RemoteNumber>
       <CallbackNumber item="1">h323:example@example.com</CallbackNumber>
       <DisplayName item="1">example@example.com </DisplayName>
       <CallRate item="1">1920</CallRate>
       <DisconnectCause item="1">Undefined reason</DisconnectCause>
       <DisconnectCauseCode item="1">21</DisconnectCauseCode>
       <DisconnectCauseOrigin item="1">Q850</DisconnectCauseOrigin>
       <StartTime item="1">2012/05/30 14:45:23</StartTime>
       <Duration item="1">11</Duration>
       <Encryption item="1">Aes-128</Encryption>
       <BookingId item="1"></BookingId>
</Call>
```

3. Cisco TMS parses and processes the call item and creates a CDR from it. Most values are taken verbatim from the call item posted to Cisco TMS; some values, such as cause codes, can be discarded by Cisco TMS and set to "unknown" if they do not follow ITU-T standards.

No CDRs from Cisco TelePresence Server

Basic Steps

Verify that:

1. TelePresence Server is running a software version supported by Cisco TMS.
2. Cisco TMS IIS has Anonymous Authentication enabled for **/tms/public**, and that an Active Directory group policy is not restricting the IUSR account.

No CDRs from Cisco TelePresence MCU

Basic Steps

Make sure you are running software version 4.3 or later, which supports asynchronous processing of CDRs.

No CDRs from Polycom Endpoints

Basic steps

Verify that:

- The Polycom endpoint is on a software version supported by Cisco TMS.
- The Polycom endpoint has the correct management address.
- The Cisco TMS server's operating system has either MSXML 4.0 or MSXML 6.0 installed.

- The Cisco TMS server's IIS has Anonymous Authentication enabled for **/pwx**, and that an Active Directory group policy is not restricting the IUSR account.

Advanced Steps

Capture a Wireshark trace on the Cisco TMS server, and pre-filter it on the endpoint's IP address.

To successfully get a CDR from a Polycom, you should then see this sequence of events:

1. When the call is set up, the endpoint POSTs a status to **/pwx/nx_status.asp** on the Cisco TMS server so that Cisco TMS starts monitoring the call.
2. When the call is ended, the endpoint POSTs a status that includes "type=disconnected". Example status message posted to **/pwx**:

   ```
   id=sa_sabre&event=sa_cxn_state&serial=1234567890123456&conf_id=14948&cxn_
   id=1&direction=incoming&display_name=endpoint@example.com&number=123456&rate=512&cxn_
   type=h323&type=disconnected&hangup_type=local&cause_code=16&rollover_cod
   ```
3. Cisco TMS then GETs a **/localcdr.csv** file from the endpoint. The .csv file is parsed and processed by Cisco TMS, which creates its own CDR based upon the data received from the Polycom.

Note that some data cannot be received from Polycom endpoints and will therefore be reported as *Unknown*.

An administrator can manually filter unused Polycom feedback, when the load balancer receives feedback through an HTTP connection. You will not be able to filter HTTP content on a HTTPS connection, as the content would be encrypted on HTTPS connetcion. The HTTP content filter can be set to block, if feedback is sent from a Polycon devices where the HTTP content contains id=sa_sabre&event=sa_exchangeSrvr_state or id=sa_sabre&event=sa_sip_state. The availability of this function and it's configuration method are dependent upon the network load balancer.

The Polycom CDR configuration files are located at C:\Program Files (x86)\TANDBERG\TMS\pwx when you use Cisco TMS version 13.0 to 14.5. For Cisco TMS version 14.6 and above, theconfiguration files are located at C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\public\pwx.

No Statistics for Legacy TANDBERG Systems

If Cisco TMS is not displaying statistics for legacy systems, try the steps below.

Basic Steps

- Make sure no SNMP tool outside of Cisco TMS is running on the server
- Verify that the system's management address (feedback receiver if an infrastructure system) is set to **http://<FQDNofTMS>/tms/public/feedback/code.aspx**. If the address is set up to use HTTPS, this must be enabled in Cisco TMS IIS.
- Check the logs for symptoms or error messages at **C:\Program Files\TANDBERG\TMS\data\Logs\TMSDebug\log-TMSSNMPservice.txt** on the server.

Advanced Steps

Using Wireshark, verify that Cisco TMS is receiving SNMP data from the system.

Cause Codes

Table 184 Cause codes based on the ITU-T standard

Code	Description
0	Cisco specific. Not part of ITU-T standard.

Table 184 Cause codes based on the ITU-T standard (continued)

1	This cause indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned.
2	This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular transit network, while it does exist, does not serve the equipment which is sending this cause.
3	This cause indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This cause is supported on a network dependent basis.
5	This cause indicates the erroneous inclusion of a trunk prefix in the called party number. This number is supposed to be stripped from the dialed number being sent to the network by the customer premises equipment.
6	This cause indicates that the channel most recently identified is not acceptable to the sending party for use in this call.
7	This cause indicates that the user has been awarded the incoming call, and that the incoming call is being connected to a channel already established to that user for similar calls (for example packet-mode x.25 virtual calls.
8	This cause indicates the call is being pre-empted.
9	This cause indicates that the call is being pre-empted and the circuit is reserved for reuse by the pre-empting exchange.
16	This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.
17	This cause is used when the called user has indicated the inability to accept another call. This cause code may be generated by the called user or by the network. Please note that the use equipment is compatible with the call.
18	This cause is used when a called party does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated (in Q.931 by the expiry of either time T303 or T310.
19	This cause is used when a user as provided an alerting indication but has not provided a connect indication within a prescribed period of time. **Note:** This cause is not necessarily generated by the customer premise equipment, but may be generated by internal network timers.
20	This cause value is used when a mobile station has logged off, radio contact is not obtained with a mobile station or if a personal telecommunication user is temporarily not addressable at any user-network interface.
21	This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible. This cause may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection.
22	This cause is returned to a calling party when the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If the network does not support this cause, cause no: 1, unallocated (unassigned) will be used instead.
26	This cause indicates that the user has not been awarded the incoming call.

Table 184 Cause codes based on the ITU-T standard (continued)

27	This cause indicates that the destination cannot be reached because the interface to the destination is not functioning correctly. The signaling message was unable to be delivered due to a hardware failure.
28	This cause indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete.
29	This cause is returned when a facility requested by the user cannot be provided by the network.
30	This cause is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY.
31	This cause is used to report a normal event only when no other cause in the normal class applies.
34	This cause indicates that there is no appropriate circuit/channel presently available to handle the call. **Note:** If you receive this call, try another data-service, such as dropping from a 64K to 56K data rate.
35	This cause indicates that the call has been queued for service by the next available device.
38	This cause indicates that the network is not functioning correctly and that the conditions are likely to last a relatively long period of time. A call that is attempted soon afterwards will most likely not connect successfully.
39	This cause is included in a STATUS message to indicate that a permanently established frame mode connection is out-of-service (for example due to equipment or section failure) [see Annex A/Q.933].
40	This cause is included in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information. [See Annex A/Q.933].
41	This cause indicates that the network is not functioning correctly and that the condition is not likely to last a very long period in time. A call that is attempted almost immediately afterwards will most likely connect successfully.
42	This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.
43	This cause indicates that the network could not deliver access information, low layer compatibility, high layer compatibility, or sub-address as indicated in the diagnostic.
44	This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.
46	This cause indicates that there are no circuits that can be pre-emptied or that the called user is busy with a call of equal or higher preemptable level.
47	This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.
49	This cause is used to report that the requested Quality of Service can't be provided (delay can't be supported).
50	This cause indicates that the requested supplementary service could not be provided due to user oversight. This cause code is often caused by the CPE being configured for the wrong switch type.
52	This cause indicates that because of call screening provided by the network, the calling user is not permitted to make a call.
53	This cause indicates that although the calling party is a member of the CUG for the outgoing CUG call, outgoing calls are not allowed for this member of the CUG.
54	This cause indicates that the called user will not accept the call delivered in the SETUP message.

Table 184 Cause codes based on the ITU-T standard (continued)

55	This cause indicates that although the calling party is a member of the CUG for the incoming CUG call, incoming calls are not allowed for this member of the CUG.
57	This cause indicates that the user has requested a bearer capability which is implemented by their equipment but the user is not authorized to use.
58	This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but which is not available at this time.
62	This cause indicates an inconsistency in the designated outgoing access information and subscriber class.
63	This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.
65	This cause indicates that the equipment sending this cause does not support the bearer capability requested.
66	This cause indicates that the equipment sending this cause does not support the channel type requested.
69	This cause indicates that the equipment sending this cause does not support the requested supplemental service.
70	This cause indicates that on equipment has requested an unrestricted bearer service but that the equipment sending the cause only supports the restricted version of the requested bearer capability.
79	This cause is used to report a service r option not implemented but only when no other cause in this class applies.
81	This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.
82	This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if the user only subscribed to channels 1 to 12 and channel 13 through 23 is requested by either side, this cause is generated.
83	This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).
84	This cause indicates that the network has received a call resume request. The call resume request contained a call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.
85	This cause indicates that the network has received a call resume request containing a Call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.
86	This cause indicates that the network has received a call resume request. The request contained a call identity information element which once indicated a suspended call, however, that the call was cleared while suspended (either a network time-out or remote user.
87	This cause indicates that the called user for the incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber calling a CUG subscriber.
88	This cause indicates that the equipment sending this cause has received a request to establish a call which has low layer compatibility, high layer compatibility, or other compatibility attributes (for example data rate) which cannot be accommodated.
90	This cause indicates that the specified CUG does not exist.
94	This cause indicates that a transit network identification was received which is of an incorrect format as defined in Annex C/Q.931.

Table 184 Cause codes based on the ITU-T standard (continued)

95	This cause is used to report an invalid message event only when no other cause in the invalid class applies.
96	This cause indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message before that message can be processed.
97	This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined of defined but not implemented by the equipment sending this cause.
98	This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.
99	This cause indicates that the equipment sending this cause has received a message which includes information element(s)/parameter(s) not recognized because the information element(s)/parameter name (s) are not defined or are defined but not implemented by the equipment sending the cause. This cause indicates that the information element(s)/parameter(s) were discarded. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.
100	This cause indicates that the equipment sending this cause has received and information element which it has implemented; however, one or several fields in the information elements are coded in such a way which has not been implemented by the equipment sending this cause.
101	This cause indicates that a message has been received which is incompatible with the call state.
102	This cause indicates that a procedure has been initiated by the expiry of a timer in association with Q.931 error handling procedures.
103	This cause indicates that the equipment sending this cause has received a message which includes parameters not recognized because the parameters are not defined or are defined but not implemented by the equipment sending this cause.
110	This cause indicates that the equipment sending this cause has discarded a received message which includes a parameter that is not recognized.
111	This cause is used to report a protocol error event only when no other cause in the protocol error class applies.
127	This cause indicates that there has been internetworking which does not provide causes for actions. The precise cause for a message being sent is not known.
128	This cause is used when the called user has indicated the inability to accept another call.
129	This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.
130	This cause indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned.
131	This cause indicates that the destination can not be reached caused by an unknown reason.
132	This cause indicates that the destination can not be reached caused by a generic error.
133	This cause indicates that the gatekeeper rejected the call.
134	This cause indicates that the gatekeeper could not find the number.
135	This cause indicates that the gatekeeper timed out the call.
136	This cause indicates that the gatekeeper is not active.

Table 184 Cause codes based on the ITU-T standard (continued)

255	Cisco specific. Not part of ITU-T standard.
1000 range	Used for mapping TC & TE codes. Cisco TMS adds 1000 to the number sent by the endpoint. For standard cause codes this corresponds to the numbers for the cause codes listed above.

Accessibility notice

Cisco is committed to designing and delivering accessible products and technologies.

The Voluntary Product Accessibility Template (VPAT) for Cisco TelePresence Management Suite is available here:

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

You can find more information about accessibility here:

www.cisco.com/web/about/responsibility/accessibility/index.html

Cisco Legal Information

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.

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2014- 2020 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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. (1721R)