Cisco TelePresence Management Suite

Administrator Guide

Version 14.3

D13741.20

August 2013

Contents

Introduction 11

Cisco TMS overview 12

Web page features and layout 13
- Portal 14
- Sitemap 15

Cisco TMS components 16
- Internet Information Services web server and applications 16
- The tmsng SQL database 17
- Windows services 17
- TMS Tools application 19

Setting up Cisco TMS 20

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 21
- Entering option keys post installation 21

How groups and permissions work 23
- Group membership 23
- System permissions 23

Setting up initial group permissions 24

Adding user accounts and profiles 25
- Language setting 25
- WebEx Enabled TelePresence 25
- WebEx site and user credentials 26

Reviewing and setting defaults 27
- General settings 27
- Network settings 27
- Mail settings 29
- Conference settings 29

Using configuration templates 30
- Creating a new configuration template 30
- Viewing a configuration template 30
- Editing a template 30
- Applying templates to systems 31
- Creating a new configuration template from an existing template 31
- Custom configuration and commands 32

Setting up WebEx Single Sign On 33
- Entering settings for your WebEx sites 33
- Obtaining certificates for use with WebEx 34
- Setting up SSO and installing the certificate 35

Enabling Active Directory lookup 37

Routing 38

Introduction to routing 39
- The Main participant 40

Protocols and call control 42
- IP 42
- ISDN 42

    How call protocols are prioritized 42
What infrastructure does Cisco TMS use for routing? 44
    MCU 44
    Distribution 44
    Cisco TelePresence Conductor 45
    Gatekeeper 45
    ISDN Gateway 46
    Cisco Unified Communications Manager 46
How zones work 47
Setting up an IP Zone 49
    Setting a zone on one or more systems 49
Setting up an ISDN zone 50
    Example 50
    Creating area code rules 51
    Setting a zone on one or more systems 52

System management overview 53

Supported systems 54
    System types supported by Cisco TMS 54
    System locations 54
How endpoints are managed by Cisco TMS 55
    Cisco TMS controlled 55
    Cisco TMSPE provisioned 55
    Cisco Unified CM registered 56
    Room 56
    Changing management modes 56
Infrastructure systems 57
    Booking 57
    Monitoring 57
    Software versions 57
Systems behind a firewall/NAT 58
    Booking 58
    Statistics and monitoring 58
    Software upgrades 58
    Phone books 59
    Configuration templates 59
    Configuration backup and restore 59
    System replacement 59
How systems are added to Cisco TMS 60
    Automatic discovery 60
    Manual addition 60
    Through Cisco Unified CM 60
    Provisioning 61
    Pre-registration 61
How Cisco TMS communicates with managed systems 62
    The addresses that systems use to contact Cisco TMS 62
    System connectivity status 62
How persistent settings work 65

Adding and managing systems 66

Setting up default system folders 67
Adding systems 68

- Using automatic discovery 68
- Adding by IP addresses or DNS names 68
- Pre-registering endpoints 70
- Adding rooms or equipment 70
- Adding endpoints behind a firewall/NAT 71
- Adding Cisco Unified CM and registered endpoints 72

Managing systems 75
- Viewing and editing a system 75
- Swapping an endpoint 75
- Upgrading Cisco TMS-controlled endpoints 77
- Purging a system 77

Navigator 79
- Folder actions 79
- Navigating the folder tree 80
- Endpoints 81
- Cisco VCS, legacy gatekeepers, and border controllers 86
- Cisco Unified CM 93
- Cisco TelePresence Supervisor MSE 8050 96
- TelePresence Conductor 99
- MCUs and TelePresence Server 103
- Gateways 109
- Content servers and recording servers 112
- Rooms and equipment 116
- Add Systems 119
- Folder and System Permissions 122

Ticketing Service 124
- Ticket statuses 124
- In-page system management 124

System Overview 126

Manage Dial Plan 127

Provisioning 128
- Users 128
- FindMe 130
- Devices 131

Configuration Backup 132
- Perform Backup 132
- Perform Restore 132
- Backup/Restore Activity Status 133

Configuration Templates 134
- Configuration Templates main page 134
- Select Settings for Configuration Template 134
- Configuration Template Activity Status 137

System Upgrade 138
- Cisco TMS systems 138
- Systems managed by the Provisioning Extension 138
- Upgrade modes 138
- Buttons for upgrading 138
- Select Software and Release Keys 139
- Software Manager 139
- System Upgrade Activity Status 140

Purge Systems 142

Event Notification Manager 143
Select Event Types 143
System status reporting 145

Booking 146

Conference Basics 147
What is a conference? 147
What is a participant? 147
What is a Video Conference Master? 147
Routing and MCUs 147
Port usage on MCUs 147
How are conference layout options controlled? 148
Booking a conference 149
Booking a conference with remote systems 151
Viewing and editing existing conferences 151
Booking and editing conferences with Cisco TelePresence Conductor 152
New Conference 154
Basic Settings 154
Advanced Settings 155
Participants tab 157
WebEx Details tab 158
Connection Settings tab 158
MCU Settings tab 160
TelePresence Conductor Settings tab 160
Conference Information tab 160
Webex Details tab 160
MCU Settings 160
Cisco TelePresence Conductor Settings 167
List Conferences 169
Time zone display 169
Query 169
List Conference 170
View Conference 171
List References 172
Conferences and references 172
Creating a reference 172
Deleting references 172
Sorting references 172
Searching for references 172
Ad Hoc Booking 173
Displaying systems 173
Checking availability and reserving systems 173
Booking on behalf of someone else 173
Entering a billing code 174
Participant Templates 175
Settings 176
Conference Templates 177
Editing and using a conference template 177

Monitoring 178

Monitoring and managing conferences 179
Conference Control Center 179

Graphical Monitor 179
Map Monitor 180
Operator conferences 181
Conference Control Center 182
Search field and folder view 182
Conference Overview 183
Conference Events 187
System Tickets 187
Sound Alerts button 187
Graphical Monitor 189
View folders and systems 189
Map Monitor 191
Setting up an organization in Map Monitor 191
Options in the background menu 191
System icons 193
System status 193

Creating and managing phone books 194

Phone book basics 195
The role of phone book sources 195
Hierarchical phone books 195
Default source and phone book 195
Phone book routing 195
Phone book types 196
Corporate directory 196
Global directory 196
Local directory 196
Setting the phone book type for all systems 196
Creating a phone book 198
Creating a phone book hierarchy 198
Alternate way of generating phone book 199
Granting access to phone books 200
Cisco TMS users 200
Provisioning users 200
Setting phone books on systems 201
One phone book on multiple systems 201
Multiple phone books on a single system 201
Setting global directory update frequency 201
Exporting contacts to a file 202
Manage Phone Books 203
Sources 203
Access Control 204
Manage Phone Book Sources 205
Source types and configurations 205
Cisco Unified Communications Manager 212
Viewing contacts 213
Phone Book and Source Activity Status 214

Reporting 215

Reporting basics 216
Types of data 216
How log purge settings affect reporting 216

Creating a report 217
Exporting data to an Excel sheet 218
Using reporting templates 219
Creating a template 219
Viewing and running template searches 219
Editing and deleting a template 219
Call Detail Records 221
What is a call detail record? 221
Endpoints 221
MCUs 221
Gatekeeper and VCS 221
Users 222
Content Servers 222
Gateways 222
Billing Code Statistics 223
Conferences 224
Conference Statistics 224
Conference Resources 224
Events 224
Scheduling Interfaces 224
Bridging Methods 225
System 226
Ticket Log 226
Feedback Log 226
Connection Error 226
System Connection 226
Authentication Failure 226
Boot 226
FTP Audit 227
Low Battery on Remote Control 227
Network 228
Packet Loss Log 228
Packet Loss Conference 228
Bandwidth Usage 228
Network History 228
Return on Investment 229
Calculating ROI 229
CO2 Savings 230
Calculating CO2 Savings 230
Administrative Tools 231
Configuration 232
General Settings 232
Network Settings 234
Email Settings 239
Edit Email Templates 240
Conference Settings 246
WebEx Settings 251
Statistics Settings 254
Provisioning Extension Settings 254
Manage Ticket Error Levels 256
Manage Event Notification Error Levels 261

User Administration 262
Groups 262
Users 268
Default Groups 270
Default System Permissions 271
Locations 272
ISDN Zones 272
IP Zones 273
Billing Codes 275
Manage Billing Codes 275
Billing Codes Activity Status 276
Activity Status 277
Analytics Extension 278
TMS Server Maintenance 279
Database Server Date and Time Settings 279
TMS Diagnostics 279
Database Server Disk space 279
TMS Server Disk space 279
Database Files and Size Info 279
Purge Old Data in Database Tables Plan 279
TMS Tickets 282
Provisioning Extension Diagnostics 283
Alarms 283
System Status 283
VCS Communication 283
Audit Log 285
TMS Tools 287
Configuration 288
Database Connection Settings 288
Directory Locations 290
Security Settings 291
Encryption Key 291
TLS Client Certificates 291
Advanced Security Settings 291
Utilities 293
Change User Domain 293
Generate Phone Book 293
Diagnostic Tools 294
SNMP Connectivity Checking Tool 294
Scan Database for Encryption Key Mismatch 294
Redundant deployments 295
Preliminary information 296
Communication with managed systems 296
Supported configurations 296
Licensing 296
Database redundancy 296
Cisco TelePresence Management Suite Provisioning Extension 296
Deploying with a load balancer 297
Recommended hardware 297
Active directory and user authentication requirements 297

Communication with managed systems 297
Architectural overview and network diagram 298
Installing and configuring 299
The network load balancer, protocols and probes 300
Scheduled tasks 301
Live Service and the Conference Control Center 302
Upgrading Cisco TMS 303
Recovery in case of a failing node 304
Deploying a hot standby 305
Setting up the primary Cisco TMS server 305
Setting up the secondary Cisco TMS server 306
Synchronizing local files 306
Optional: Enable TLS client certificates 306
Upgrading Cisco TMS 307
Recovery if the primary server fails 307
Database redundancy 309
Database mirroring 309
Failover clustering 310
Backups 310
Example ACE configuration 311
Local files for synchronization 315

Troubleshooting 316

Using the logs 317
Downloading log files 317
Locating the logs on the server 317
Log overview 317
Changing the log levels 319
Reading the logs 320
Website scenarios 322
Cisco TMS does not load 322
System scenarios 324
New systems are not automatically discovered 324
System information and status outdated 324
Scheduled events not starting 324
Tickets not raised 324
Conference scenarios 326
Call does not start 326
Java applet scenarios 327
Username and password prompt keeps reappearing 327
Applet does not load 327
Applet is slow to load or will not load completely 327
Troubleshooting monitoring 328
Phone book scenarios 330
Phone book (Corporate Directory) errors 330
Polycom endpoints do not get phone books 330
Reporting scenarios 331
No CDRs from endpoints running Cisco TC and TE software 331
No CDRs from Cisco TelePresence MCU 331
No CDRs from Cisco TelePresence Server 332
No CDRs from Polycom endpoints 332
No statistics for legacy TANDBERG systems 332

Cause Codes 334

Bibliography 338

338

Accessibility notice 339

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.

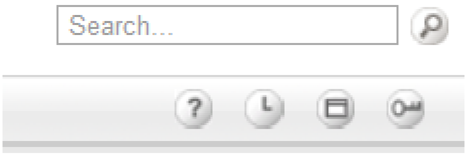
The primary audiences for Cisco TMS include:

- 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.



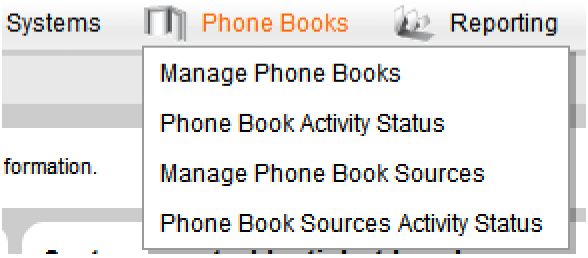
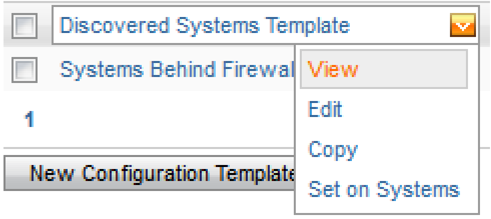
Cisco TMS overview

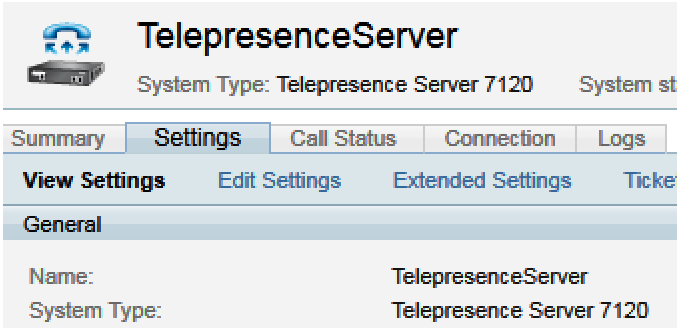
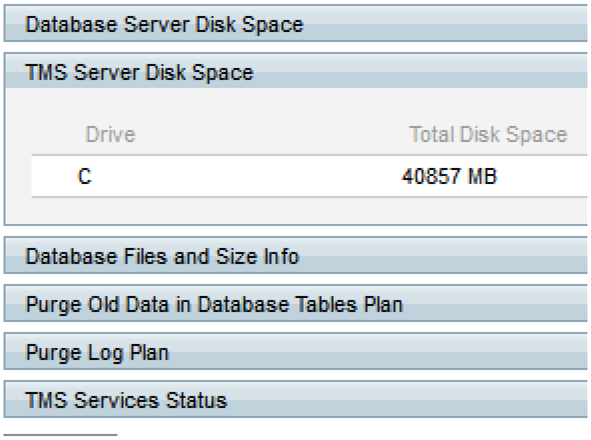
This chapter provides a short introduction to the core functionality of Cisco TMS and a walkthrough of the main elements of the web application. A brief explanation of each of the main components and services that make up the Cisco TMS backend is also included.

Web page features and layout 13
Cisco TMS components 16

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.

User interface element	Image	Description
Top-level menu	 Systems Phone Books Reporting Manage Phone Books Phone Book Activity Status Manage Phone Book Sources Phone Book Sources Activity Status formation.	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 [p.79].
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	 Discovered Systems Template Systems Behind Firewal 1 New Configuration Template View Edit Copy Set on Systems	Hovering over items in a list will display an orange drop-down menu icon when available.

User interface element	Image	Description
Lists	 □ Name ▽ Type	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	 TelepresenceServer System Type: Telepresence Server 7120 System st Summary Settings Call Status Connection Logs **View Settings** Edit Settings Extended Settings Ticke General Name: TelepresenceServer System Type: Telepresence Server 7120	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	 Database Server Disk Space TMS Server Disk Space Drive Total Disk Space C 40857 MB Database Files and Size Info Purge Old Data in Database Tables Plan Purge Log Plan TMS Services Status	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 [p.79].

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 [p.124].

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 [p.182].

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 [p.224].

Sitemap

In Cisco TMS: **Portal > Sitemap**

This page gives an overview over 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 [p.322].

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 for systems supporting the Cisco OneButtonToPush calendar service.
- **/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 2008 or 2005. 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 a separate database.

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 and Sony endpoints. Polycom endpoints 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.

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 TMS Tools [p.287].

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 23
Setting up initial group permissions 24
Adding user accounts and profiles 25
Reviewing and setting defaults 27
Using configuration templates 30
Setting up WebEx Single Sign On 33
Enabling Active Directory lookup 37

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 [p.24] 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.

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. The user is authenticated by his 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.

WebEx Enabled TelePresence

For bookings with WebEx to work, the user performing the booking must have WebEx credentials in his Cisco TMS profile. This ensures that the correct user "owns" 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 used for other features

The remaining fields are not mandatory, but are used for other Cisco TMS features. Later, if you are using Active Directory, you can configure Cisco TMS to populate these fields automatically for new users, see Setting up WebEx Single Sign On [p.33].

WebEx site and user credentials

For each user to be able to use WebEx in telepresence conferences, **WebEx Site**, **WebEx Username** and **WebEx Password** must be entered in Cisco TMS.

There are two alternative ways to enter this information:

- Using Single Sign On.
- Entering the information manually.

Using Single Sign On

The Cisco TMS administrator can either have the WebEx username imported from Active Directory or manually enter this on behalf of the users. When using Single Sign On, the WebEx password is not required.

To enable SSO, see Setting up WebEx Single Sign On [p.33]

Not using Single Sign On

If SSO is not used, each user must enter this information manually. Go to the personal information page, click the link in the lower left corner of Cisco TMS and enter:

- **WebEx site**.
- **WebEx Username**.
- **WebEx Password**.

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

Open **Administrative Tools > Configuration > General Settings**. Important settings that should be reviewed at this time are listed below:

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.
Enable Auditing	This setting enables Audit logging where Cisco TMS keeps detailed logs of all changes to systems, users, and other key elements of Cisco TMS. The Audit Log is accessible in the Administrative Tools Menu. This is disabled by default, but security conscious installs may want to enable it from the start. This feature will cause the Cisco TMS database to grow significantly faster.
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

Open **Administrative Tools > Configuration > Network Settings**. Significant settings that should be reviewed at this time are listed below:

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.
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. For further detail on AD Groups, refer to the *Cisco TelePresence Management SuiteAdministrator Guide*.
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.
TMS Server IPv4/IPv6 Addresses	These were configured during installation and should be the IP addresses used to reach your Cisco TMS server.
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.
Secure-Only Device Communication	This is *Off* by default and should only be enabled in specific customer scenarios.

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

Open **Administrative Tools > Configuration > Conference Settings > Conference Create Options**. These settings control most of the behaviors of Cisco TMS for scheduled calls and for monitoring of active calls. Significant settings that you may wish to update are:

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 to *On* 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 [p.60].

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

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 [p.134].
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. By adding systems to the **Once** tab, templates will be applied only once.
   b. By adding systems to the **Persistent** tab, templates will be set persistenlty according to the **Recurrence Interval** set for the template.
4. Click **Set on Systems** to start the task.
   Applying the template to systems will be performed as a backgroun 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**, seeConfiguration Template Activity Status [p.137] .

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.

Setting up WebEx Single Sign On

Enabling Single Sign On allows users to book and participate in conferences with WebEx without entering a password.

The WebEx username in each Cisco TMS user profile (see Adding user accounts and profiles [p.25]) is passed to the WebEx site to complete bookings that include WebEx.

Here is a description of the conference booking process for a WebEx user using SSO:

1. Add a user's WebEx username to their Cisco TMS profile. There are two alternatives:
   a. Ensure AD look up is configured in Cisco TMS. Enabling Active Directory lookup [p.37].
      i. Go to **Administrative Tools > Configuration > WebEx Settings** and configure **Get WebEx Username from Active Directory**.

   or

   b. Enter the WebEx username manually without replicating from AD.
2. Enter one or more WebEx Sites that will use SSO individually in Cisco TMS.
   a. Your WebEx Administrator must send you the configuration information to use in Cisco TMS for your WebEx Site.
   b. The WebEx site configuration on Cisco TMS must be set to allow SSO. See WebEx Settings [p.251].
   c. The WebEx site itself (see WebEx Help) must be set up to allow SSO.
3. At this stage the WebEx team enables SSO on your WebEx site by installing the public certificate (provided by the Cisco TMS administrator). This is done by the WebEx team in the WebEx cloud (SuperAdmin site), which is only accessible by this team.
4. Configure your WebEx site (Admin site) to enable partner delegated authentication.
5. Enable SSO in Cisco TMS.
6. Install a certificate on Cisco TMS and on WebEx to ensure secure communication. The Cisco TMS administrator must generate the certificate and send it to WebEx team.

Entering settings for your WebEx sites

1. Go to **Administrative Tools > Configurations > WebEx Settings**.
2. Click **Add Site**.
3. Enter **Hostname**.
4. Enter **Site Name**.
5. Fill in the fields below as appropriate.

Field description for the **WebEx Site Configuration**.

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.

Field	Description
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*: Set to *Yes* 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). By setting this to *Yes*, the audio line used will not be encrypted. *No*: SIP will be used for both video and audio.
Use Web Proxy	*Yes*: Set to *Yes* if your network uses a web proxy to exit the intranet. When selecting *Yes* a **Web Proxy Configuration** will be displayed with three fields: ■ **Web Proxy Address** where **Web Proxy Address**is mandatory. ■ **Web Proxy Username** ■ **Web Proxy Password** *No*: WebEx can be reached without using a proxy.
Enable SSO	To enable Single Sign On, see Setting up WebEx Single Sign On [p.33] *Yes*: Set to *Yes* if your network uses SSO. No: Your network does not use SSO.
Connection Status	This field displays the status of the connection between Cisco TMS and the WebEx site.

Obtaining certificates for use with WebEx

Choose one of the following:

- Use the SSL certificate generated by Cisco TMS during installation. If you chose not to enable HTTPS during installation, there will be no certificate available to use in this process.
- Generate your own certificate.

Generating the SSL certificate

If you want to use the SSL certificate generated by Cisco TMS, start by exporting the SSL certificate using IIS Manager, Server Certificates both the private and public key.

1. Export the private key:
   a. Double-click the TMS certificate.
   b. Click the **Details** tab.
   c. Click the **Copy to File** button.
   d. Select *Yes*.
   e. Export the private key
   f. Enter a Certificate password.
   Save this password to use later in the procedure.

   g. Select **Personal Information Exchange - PKCS #12 (.PFX)**
   h. Click **Next** and finish the procedure.

2. Export the public key:
   a. Double-click the TMS certificate.
   b. Click the **Details** tab.
   c. Click the **Copy to File** button.
   d. Select *No*.
      Do not export the private key.
   e. Select **Base-64 encoded X.509 (.CER)**.
   f. Click **Next** and finish the procedure.
3. Give the certificate to the WebEx SSO team to enable SSO for your WebEx site.

Generating a certificate using OpenSSL

1. Generate a private key using the following command:
   ```
   openssl genrsa -out tms-privatekey.pem 2048
   ```
2. Generate a certificate signing request (CSR) using the private key above:
   ```
   openssl req -new -key tms-privatekey.pem -config openssl.cfg -out tms-certcsr.pem
   ```
3. Enter the data requested, including:
   - Country
   - State or province
   - Organization name
   - Organization unit
   - Common name (this is Cisco TMS FQDN (Fully Qualified Domain Name))
   - (Optional) Email address, password, company name
4. Send the TMS certificate signing request file, **tms-certcsr.pem** to be signed by a well-known certificate authority (CA) or a self-created certificate authority such as OpenSSL or Windows CA.
   You should receive the signed certificate, **tms-cert.der** back from the CA.
5. Convert the signed certificate from .der to .pem using the following OpenSSL command:
   ```
   openssl x509 -inform der -in tms-cert.cer -out tms-cert.pem
   ```
6. Combine the signed certificate .pem with the private key:
   ```
   openssl pkcs12 -export -inkey tms-privatekey.pem -in tms-cert.pem -out tms-cert-key.p12 -nametms-cert-key
   ```

You now have a Cisco TMS certificate that contains the private key for SSO configuration to upload to Cisco TMS **Administration Tools > Configuration > WebEx Settings**.

Setting up SSO and installing the certificate

In this section you need to collaborate with the WebEx Cloud Service Team. The cloud services team provisions (creates) your WebEx site. For SSO configuration, cloud services is responsible for configuring SSO and uploading the certificate provided by the Cisco TMS administrator for your WebEx site.

Before configuring SSO in Cisco TMS, you must request the following information from the Webex Cloud Services team configure it in both Cisco TMS and in the WebEx cloud:

- **Partner Name**
  This value must be determined or approved by the WebEx team, because it is unique among all WebEx customers.
- **Partner Issuer (IdP ID)**
  This is the Identity Provider. This value is normally determined by the TMS administrator, because the Identity Provider is TMS.
- **SAML Issuer (SP ID)**
  This is the Service Provider. This value is normally determined by WebEx, because the Service Provider is WebEx.
- **AuthnContextClassRef**
  This is the authentication context. The IdP authenticates the user in different contexts, for example X509 cert, Smart card, IWA, username/password.

Enabling SSO

1. Give this public key certificate (.CER) to the WebEx SSO team who will install it for your WebEx site and assist you in determining the values for the SSO configuration of your Cisco TMS.
2. Go to **Administrative Tools > Configurations > WebEx Settings**.
3. Set **Enable SSO** to *Yes*.
   The **SSO Configuration** section is displayed.

Configuring SSO and installing the certificate

1. Go to the **SSO Configuration** section.
2. Click **Browse** to upload the private key certificate (PFX).
3. In **Certificate Password**, enter the password for the private key.
4. Enter the following fields:
   a. **Partner Name**.
   b. **Partner Issuer**.
   c. **SAML Issuer**.
   d. **AuthnContextClassRef**.
5. Click **Save**.

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.

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 39
Protocols and call control 42
What infrastructure does Cisco TMS use for routing? 44
How zones work 47
Setting up an IP Zone 49
Setting up an ISDN zone 50

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.

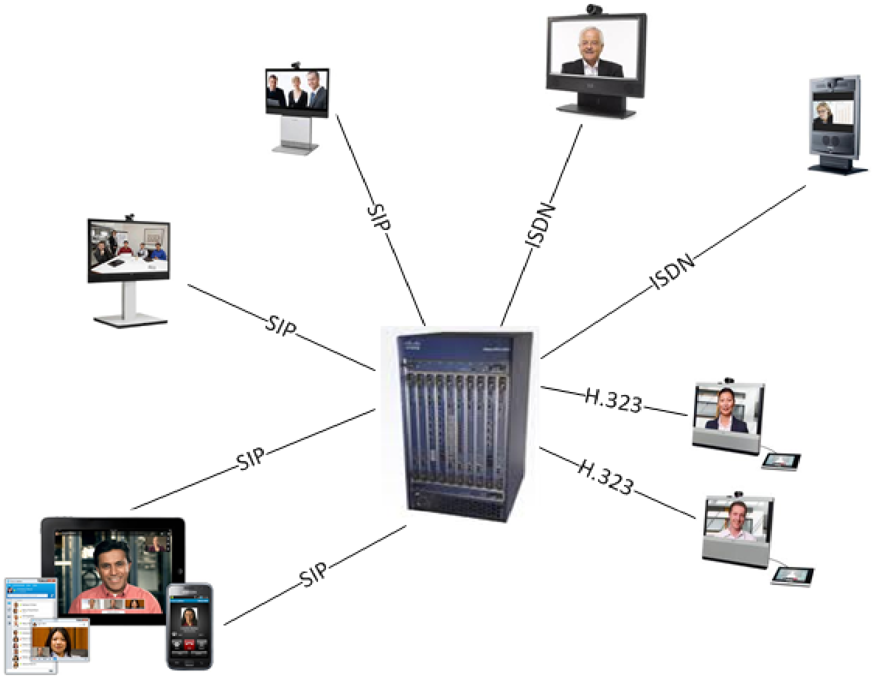
Whenever a conference is edited and updated, Cisco TMS creates a completely new route (the old route is not taken into account when doing this). Even the smallest change to a conference could therefore create new dial-in numbers.

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 and must be updated manually.
- 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.

Cisco TMS is able to route both IP and ISDN. Cisco TMS prioritizes IP if a system is capable of both. Over IP, H.323 is priorotized over SIP.

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.

Note that the weighting given to these criteria can change from one release of Cisco TMS to the next.

Cisco TMS evaluates all possible routes using all possible Main participants (endpoints/MCUs already in the call and any other MCUs in Cisco TMS). It attaches a weight to every (conference-wide rather than call leg) route. If you have manually added an MCU to the conference during booking, the route with this MCU is chosen. If not, the route with the lowest weight is chosen. The dropdown for changing the Main participant during booking is ordered based on these weights.

The following must be noted:

- There can only be one Main participant per conference.
- You cannot change the Main participant once the conference has started.
- The Main participant can never be disconnected as this will tear down the whole conference.
- 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** are actioned only on the Main participant, which then carries out that action on all the other participants, for example Mute All, or Disconnect.

Protocols and call control

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

IP

In a modern Cisco telepresence deployment there are two call control solutions: you can choose either Cisco TelePresence VCS or Cisco Unified Communications Manager.

Their respective capabilities are listed below:

- Cisco TelePresence VCS
  - SIP registrar
  - H.323 gatekeeper
  - can route calls to a Cisco Unified CM
- Cisco Unified Communications Manager
  - 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 Cisco Unified CM see:

Cisco TelePresence Video Communication Server Cisco Unified Communications Manager Deployment Guide

Cisco TMS also supports legacy call control systems:

- TANDBERG Gatekeeper
- TANDBERG Border Controller
- Some third party gatekeepers

Your choice of call control solution will dictate how Cisco TMS routes scheduled calls. For example, for systems registered to Cisco 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

By default Cisco TMS prioritizes H.323 over SIP, and IP over ISDN. You can use zones to specify whether Cisco TMS prioritizes IP or ISDN, see How zones work [p.47] .

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.

You can specify which protocols are allowed for individual systems in scheduling 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 many different models of MCU. In a modern Cisco TelePresence deployment we recommend the following for optimum performance:

- Cisco TelePresence MCU Series
- Cisco TelePresence Server

Note that 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). For recurrent bookings Cisco TMS uses the same port number and alias for all recurrences.

You can specify what type of MCU Cisco 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 if available. Otherwise any MCU can be chosen by Cisco TMS.

Note that a directly managed MCU must be registered to an H.323 gatekeeper or SIP registrar for Cisco TMS to be able to schedule it. For example, scheduling of SIP-trunked bridges is not supported in Cisco TMS.

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**.

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) [p.159]

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.

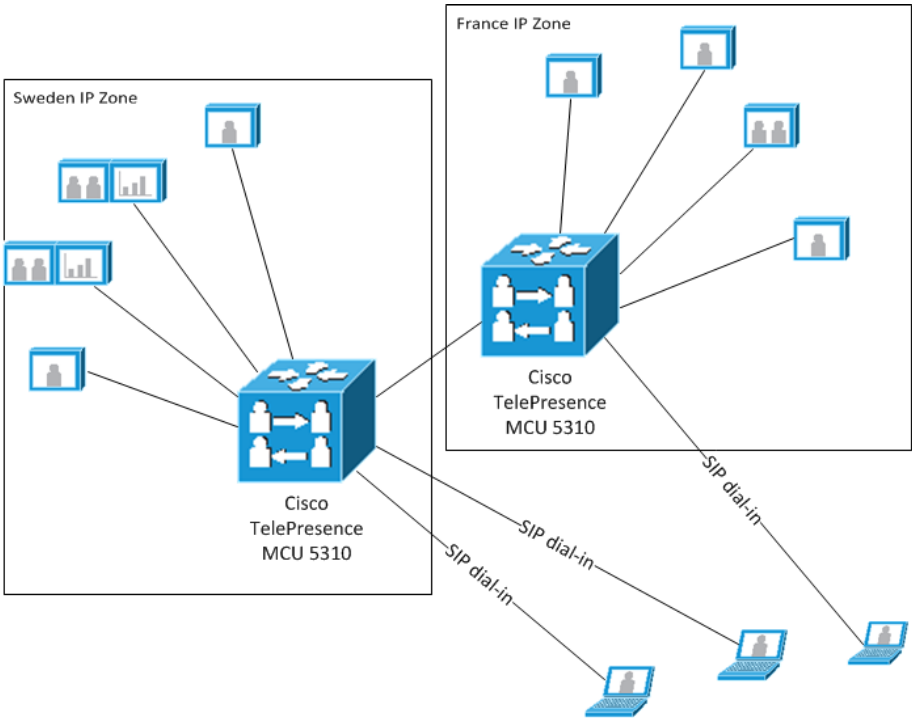
Note that the setting **Administrative Tools > Configuration > Conference Settings > Preferred MCU Type in Routing** is ignored when it comes to distribution.

Not all MCUs are supported for use in cascading: for example the TelePresence Server.

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 that dial-ins do not have a designated IP zone.

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.

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.

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 gatekeepers. 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 [p.47].)

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 [p.47]).

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.

Cisco Unified Communications Manager

If a system is provisioned by Cisco 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 Cisco 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 Cisco Unified CM and vice versa.
- does not support MCUs or Cisco TelePresence Servers SIP-trunked to the Cisco Unified CM. These must be registered to the Cisco VCS.
- will always append the top level domain to calls going through the Cisco Unified CM - make sure the Cisco VCS accepts this kind of dial plan/numbering scheme.
- only supports one Cisco Unified CM cluster (one top level domain).

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.

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 [p.50]

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 [p.49]

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.

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 [p.48].
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.

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:

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 54
How endpoints are managed by Cisco TMS 55
Infrastructure systems 57
Systems behind a firewall/NAT 58
How systems are added to Cisco TMS 60
How Cisco TMS communicates with managed systems 62
How persistent settings work 65

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 Cisco Unified CM and Cisco TelePresence Supervisor MSE 8050
- Cisco TelePresence Conductor
- gateways
- content and recording servers

Endpoints or equipment not directly supported by Cisco TMS or Cisco TMSPE can be added as *Room* or equipment, which does not provide control of 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 Cisco Unified CM to Cisco TMS provides limited management options.
- Adding an endpoint as Room or Equipment 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 [p.68].

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 [p.128].

Cisco Unified CM registered

The following feature set is available to systems that were registered to Cisco Unified CM prior to addition to Cisco TMS:

- Booking
- View settings
- Conference Control Center
- Tickets

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

For instructions on making sure your system is supported and adding it to Cisco TMS, see Adding Cisco Unified CM and registered endpoints [p.72].

Room

Adding an unsupported system as a room or equipment makes the system bookable in Cisco TMS, but gives no access to other features.

For instructions on adding these systems, see Adding systems [p.68].

Changing management modes

Directly migrating from one management mode to another is not supported.

To migrate for example a Cisco TMS-controlled endpoint to be provisioned by Cisco TMSPE or registered to Cisco Unified CM:

1. Purge the endpoint from Cisco TMS.
2. Follow the appropriate instructions to register the endpoint to Cisco Unified CM or provision it with Cisco TMSPE.
3. Manually update any future bookings that include the 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 content and recording 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 three minutes. For more information on how Cisco TMS polls systems, see TMSDatabaseScannerService [p.18].

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.

Cisco Unified CM

Note that Cisco 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 [p.17].

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-controlled endpoints [p.77].

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 an endpoint [p.75].

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 rooms and Cisco TMSPE-provisioned systems (which are not added to Cisco TMS, see below).

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.

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 [p.68].

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.

Rooms and equipment 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 [p.68]
- Adding rooms or equipment [p.70]

Through Cisco Unified CM

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

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

For instructions, see Adding Cisco Unified CM and registered endpoints [p.72].

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 [p.70] 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 and FTP are 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 SOHO systems. 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 [p.234].
- *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 [p.234].
- *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*.

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*.

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 [p.30].

Adding and managing systems

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

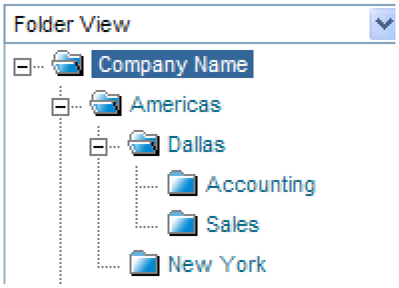
Setting up default system folders 67
Adding systems 68
Managing systems 75
Navigator 79
Ticketing Service 124
System Overview 126
Manage Dial Plan 127
Provisioning 128
Configuration Backup 132
Configuration Templates 134
System Upgrade 138
Purge Systems 142
Event Notification Manager 143
System status reporting 145

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 Adding endpoints behind a firewall/NAT [p.71] for instructions on adding endpoints behind a firewall/NAT.
- See Adding Cisco Unified CM and registered endpoints [p.72] for instructions on preparing and adding these systems.

For instructions on adding TelePresence Conductor and registered MCUs to Cisco TMS see *Cisco TelePresence Conductor with Cisco TMS Deployment Guide*.

For detail about the layout and options of the pages used in these procedures, see the reference section Add Systems [p.119].

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:

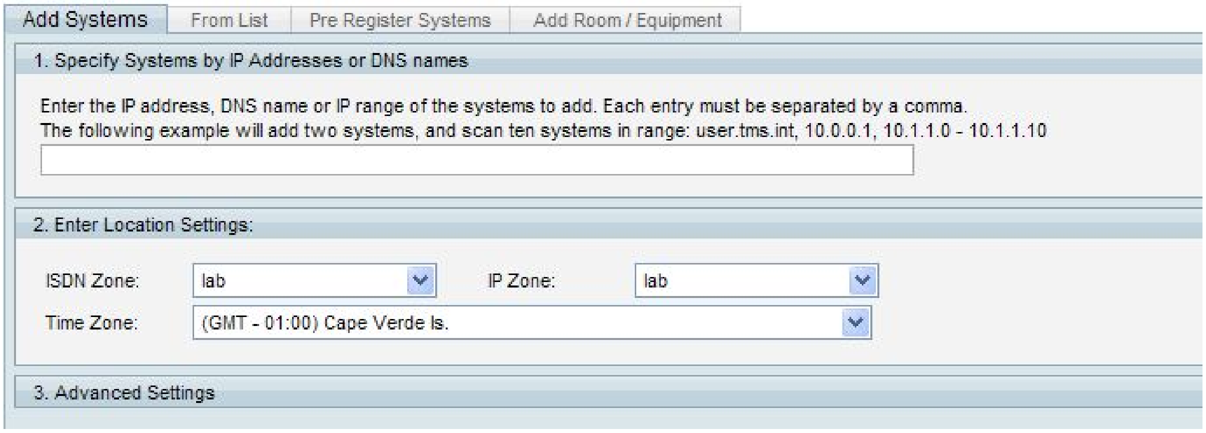
1. Go to **Systems > Navigator > [Name of your folder for discovered systems]**.
   The default folder is **Discovered Systems**.
2. Review and adjust the settings for each system as desired.
3. Verify on the system's **Permissions** tab that new user groups will have permissions for the system. Modify 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 Cisco Unified CM must not be added in this way, see Adding Cisco Unified CM and registered endpoints [p.72].

To add a system:

1. Go to **Systems > Navigator**. Select a folder for the system.
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 [p.68].
   - 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**.



1. Specify Systems by IP Addresses or DNS names

Enter the IP address, DNS name or IP range of the systems to add. Each entry must be separated by a comma.
The following example will add two systems, and scan ten systems in range: user.tms.int, 10.0.0.1, 10.1.1.0 - 10.1.1.10

2. Enter Location Settings:

ISDN Zone: lab
IP Zone: lab
Time Zone: (GMT - 01:00) Cape Verde Is.

3. Advanced Settings

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 **Time Zone**, **IP Zone**, and **ISDN Zone** for the system from the drop-down lists.
6. Click the **Advanced Settings** section heading to expand it if you need to add authentication details, configuration template, or SNMP discovery options.
   Do not fill in the **Admin Password** field.
   For an overview of the settings on this page, see Add Systems [p.119].
7. Click the **Next** button at the bottom of the page 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 Conductor you will see a number of errors. This is expected, just click on **Add System Despite Warnings**.
   - When adding a TelePresence Server you will get an error mentioning 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.

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 [p.143].

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 [p.128].

Adding rooms or equipment

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

For more information about how rooms differ from other systems in Cisco TMS, see How endpoints are managed by Cisco TMS [p.55]

To add an endpoint as a room:

1. Go to **Systems > Navigator**.
2. Select the folder to which you want to add the room or piece of equipment, and click **Add Systems**.
3. Click the **Add Room/Equipment** tab.
4. Enter a name for what you are adding, and select a type.
5. Click on the **Advanced** section heading to expand it. Some fields are mandatory:
   - Select **IP Zone**, **ISDN Zone**, and **Time Zone** for the room.
   - 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**.

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 [p.68].

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 SoHo** 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 [p.70], 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 Cisco Unified CM and registered endpoints

To add a Cisco Unified CM and endpoints registered to it to Cisco TMS, follow the procedures below in the order they are listed.

Preparing the Cisco Unified CM

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

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

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

Follow this procedure in Cisco 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 a user group in Cisco Unified CM for Cisco TMS.
3. Assign the following roles to this user group:
   - Standard AXL API Access
   - Standard CTI Enabled
   - Standard SERVICEABILITY
   - Standard CCM Admin Users
   - Standard RealtimeAndTraceCollection
4. Add the above application user to the newly created user group.

Adding Cisco Unified CM

Add Cisco Unified CM following the steps in Adding systems [p.68], making sure to check **Discover Non-SNMP Systems**.

Preparing to add endpoints

Cisco TMS support for Cisco 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 Cisco Unified CM in **Navigator**.

You can verify that your systems are supported as follows:

1. Go to **Systems > Navigator** and locate the Cisco 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 Cisco Unified CM-registered systems are supported in Cisco TMS, see How endpoints are managed by Cisco TMS [p.55].

CTS and TX endpoints

The endpoints must already have been added to the Cisco 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 Cisco 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 TE and TC software

Endpoints running TE and TC software must already have been added to the Cisco Unified CM as detailed in the document *Cisco TelePresence Administering TC Endpoints on CUCM8.6*.

If an endpoint has previously been managed by Cisco TMS, you must purge it from the database before re-adding it as a Cisco Unified CM-registered endpoint. See Purge Systems [p.142].

For each endpoint follow these steps in Cisco 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

Cisco Unified CM must be added to Cisco TMS before you can add the endpoints, 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**.

Managing systems

This section describes common system-related administrative tasks:

- Viewing and editing a system [p.75]
- Upgrading Cisco TMS-controlled endpoints [p.77]
- Swapping an endpoint [p.75]
- Purging a system [p.77]

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 on the other tabs for more details about the system. The available tabs vary by system type.
3. Click on 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 [p.79].

Connection settings

The **Connection** tab shows 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 will open in its place.

To attempt reconnection with the system:

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

Swapping an endpoint

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 an endpoint due to theft, hardware failure, or similar, retaining the ID allows Cisco TMS to keep the links to existing bookings and permissions.

A system *must* be swapped with a system of a similar type, software, and management model. For example, a Cisco TelePresence System EX90 running TC 6.1 that is controlled by Cisco TMS must be replaced with a new Cisco TMS-controlled EX90 running TC 6.1.

It is not possible to swap:

- Cisco TMS-controlled endpoints with endpoints registered to Cisco Unified CM
- infrastructure systems
- remote endpoints

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**.

Replacing the endpoint

Follow this procedure to replace an endpoint:

1. Go to **Systems > Navigator** and click on the system you wish to replace
2. Click the **Connection** tab.
3. Click **Replace System**.
4. Do one of the following:
   - Enter the IP or DNS address of the replacement system.
   - Browse to an existing system in Cisco TMS by clicking **Select System…**.
5. Click **Next**.
   A summary page is displayed.
6. Choose whether to keep the system name, call configuration, apply last configuration backup, and keep all logs of the system. You can also choose to purge the replacement system from Cisco TMS.
7. Click **OK**.
8. The swap will now be completed.

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-controlled endpoints

Before you start, you must place the software package on a drive available from Cisco TMS.

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:
   - A **Release Key** for the software, unless this has been correctly pre-populated by Cisco TMS.
   - The software version, using the drop-down list in the **Software** field.
   - The **Date** and **Start Time** you want for the scheduled upgrade.
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 [p.58] for background on how these upgrades work.

Applying the same upgrade to endpoints with 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 four 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.
🖧	Explore the files and folders on legacy systems using FTP.	🗔	Open a telnet connection to a legacy system.

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

- Endpoints [p.81]
- Cisco VCS, legacy gatekeepers, and border controllers [p.86]
- Cisco Unified CM [p.93]
- MCUs and TelePresence Server [p.103]
- Gateways [p.109]
- TelePresence Conductor [p.99]
- Cisco TelePresence Supervisor MSE 8050 [p.96]
- Rooms and equipment [p.116]

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 [p.122] 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 [p.142] 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 [p.119] 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, and so on.
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 [p.145].
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.

View option	System grouping
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

This tab presents a summary of the most important data for the system.

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service [p.124] for more information.
System Settings	The selected system's network address, E.164 alias, IP URI, H.323 ID, and ISDN numbers as relevant. More settings are viewable and editable in the **Settings** tab.
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.
Conferences	Upcoming conferences where the system is scheduled to participate.
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.

Section	Description
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 Cisco 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.
Call Settings	Here you will find for example the maximum ISDN and IP bandwidth, auto answer settings, and the H.323 ID, E.164 alias, and SIP URI of the system.
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 Cisco Unified CM-registered endpoints, only **SIP Mode**, **Requested SIP Server Address**, and **Active SIP Server Address** are displayed.
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	Settings to allow or deny bookings and incoming or outgoing calls for the system.

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

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
  For Cisco 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 [p.234].

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 Cisco 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 [p.134].
- **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 [p.124]
- Manage Ticket Error Levels [p.256]

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 [p.203].

For guidance on working with phone books, see Creating and managing phone books [p.194].

Connection

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.

Field	Description
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *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 [p.234]. - *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 [p.234]. - *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 [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.221].
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

Cisco VCS, legacy gatekeepers, and border controllers

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

This tab presents a summary of the most important data for the system.

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service [p.124] for more information.
System Settings	The selected system's network address, E.164 alias, IP URI, H.323 ID, and ISDN numbers as relevant. More settings are viewable and editable in the **Settings** tab.
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.
Conferences	Upcoming conferences where the system is scheduled to participate.
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.

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.
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.
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.

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
- 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 [p.234].

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server. For Cisco 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 [p.234].

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 [p.124]
- Manage Ticket Error Levels [p.256]

Registrations

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

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.

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.
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.

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.

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 [p.145].
Description	Comments from Cisco TMS regarding the peer.
Save Cluster settings	Save any changes to the cluster settings.
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*.

Field	Description
VCS Provisioning Mode	Depending on your version of Cisco VCS, two options may be available: ▪ *Provisioning Extension*—use Cisco TMSPE. ▪ *TMS Agent Legacy*—no longer supported by Cisco TMS.
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	

Field	Description
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.

Connection

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *MAC Address*

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 [p.234]. For more information, see System connectivity status [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.221].
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

Bandwidth (legacy only)

The **Bandwidth** tab is only available for legacy gatekeepers and contains a list of:

- Sub Zones, including the IP address and IP subnet mask of the sub zone.
- Pipes
- Links for the Gatekeeper/Border Controller

See chapter 4 **Bandwidth Control** in the documentation that came with your TANDBERG Gatekeeper, for a detailed explanation of configuration of **Sub Zones**, **Pipes** and **Links**.

Cisco Unified CM

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

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

Summary

This tab presents a summary of the most important data for the system.

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service [p.124] for more information.
System Settings	The selected system's network address, E.164 alias, IP URI, H.323 ID, and ISDN numbers as relevant. More settings are viewable and editable in the **Settings** tab.
Conferences	Upcoming conferences where the system is scheduled to participate.
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 Cisco Unified CM in Cisco TMS:

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

Extended Settings

This tab contains a list of all Cisco TMS-compatible telepresence endpoint types supported by this version of Cisco Unified CM. See Preparing to add endpoints [p.73] 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 [p.124]
- Manage Ticket Error Levels [p.256]

Managed Systems

This tab lists telepresence systems managed by Cisco Unified CM.

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 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.

Connection

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.

Field	Description
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *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 [p.234]. For more information, see System connectivity status [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

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

This tab presents a summary of the most important data for the system.

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service [p.124] for more information.
System Settings	The selected system's network address, E.164 alias, IP URI, H.323 ID, and ISDN numbers as relevant. More settings are viewable and editable in the **Settings** tab.
Conferences	Upcoming conferences where the system is scheduled to participate.
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.

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.
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.
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.

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
- 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 [p.234].

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 [p.124]
- Manage Ticket Error Levels [p.256]

Supervisor

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.
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

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *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 [p.234]. For more information, see System connectivity status [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

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*.

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.

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.

Call Settings	**Max Number of Concurrent Scheduled Calls** lets administrators limit the number of concurrent scheduled calls that Cisco TMS can schedule on this TelePresence Conductor. Changing this setting does not in any way affect the resource allocation on TelePresence Conductor itself, but allows administrators to save some resources for ad hoc calls. This field is set to *Unlimited* as default, which means that Cisco TMS will not limit the number of concurrent scheduled calls that it books. Here you will find for example the maximum ISDN and IP bandwidth, auto answer settings, and the H.323 ID, E.164 alias, and SIP URI of the system.
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.
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	Settings to allow or deny bookings and incoming or outgoing calls for the system.

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.

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
- 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 [p.234].

Extended Settings

Field	Description
First Meeting ID	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.
Meeting ID Step	Cisco TMS will add this number to the **First meeting ID** to avoid duplicated numeric IDs. As conferences finish, their IDs will be made available to new conferences.
Meeting ID Quantity	The maximum number of concurrent meeting IDs that can be generated.

Aliases

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.

View Aliases

The **Regular Expression** 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.

Edit Aliases

Click **Create** for a new line where you can enter the details for your alias.

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 `%`. We strongly recommend that the alias pattern contains a domain. The alias pattern must match the pattern string of the search rule targeting the neighbor zone to the TelePresence Conductor on the Cisco VCS. Examples: ■ Variable: `meet.%.scheduled@example.org`, `1234.%.scheduled@example.org` ■ Fixed: `allhands@example.org`, `1234@example.org`
Priority	Give the alias a priority. The alias with the lowest number has the highest priority, and will be used first when Cisco TMS creates a conference. If that alias is already in use, the alias with the next highest number will be used, and so on. The priority can be any number between 1 and 65535.
Is Immersive	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.
Description	Enter a description of this alias.
In Use	A green check mark indicates that this alias is booked in current or future conferences and therefore cannot be deleted or have its pattern modified. Clicking on **Details** gives the ID of all conferences the alias is booked in. If this is the first alias you are creating, this column will be blank.

Managed Systems

This tab lists bridges, that is, MCUs and TelePresence Servers, that are managed by the selected TelePresence Conductor.

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 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.

Connection

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *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 [p.234]. For more information, see System connectivity status [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

MCUs and TelePresence Server

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

Summary

This tab presents a summary of the most important data for the system.

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service [p.124] for more information.
System Settings	The selected system's network address, E.164 alias, IP URI, H.323 ID, and ISDN numbers as relevant. More settings are viewable and editable in the **Settings** tab.
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.
Conferences	Upcoming conferences where the system is scheduled to participate.
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).

Section	Description
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.

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.
Call Settings	Here you will find for example the maximum ISDN and IP bandwidth, auto answer settings, and the H.323 ID, E.164 alias, and SIP URI of the system.
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.
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	Settings to allow or deny bookings and incoming or outgoing calls for the system.

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.

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
- 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 [p.234].

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.

Field	Description
First Meeting ID	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.
Meeting ID Step	Cisco TMS will add this number to the **First meeting ID** to avoid duplicated numeric IDs. As conferences finish, their IDs will be made available to new conferences.
Meeting 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.

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 on routing in Cisco TMS, see Routing [p.38].
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.
Register with Gatekeeper	Registers the conference with the H.323 registrar.

Setting	Description
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* ■ *Immediately*
Multicast Streaming Enabled	Allows multicast streaming for the conference.
Unicast Streaming Enabled	Allows unicast streaming for this 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.
Ports to Reserve for ConferenceMe	If using the ConferenceMe feature on the MCU, ports can be reserved for it using this field.

TelePresence Server

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

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).

Field	Description
Dual Video Stream	Enable an additional video stream, such as a presentation.
Display warning on conference end	Display *This conference is about to end* warning.
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 [p.124]
- Manage Ticket Error Levels [p.256]

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

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *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 [p.234]. For more information, see System connectivity status [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.221].
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

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

This tab presents a summary of the most important data for the system.

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service [p.124] for more information.
System Settings	The selected system's network address, E.164 alias, IP URI, H.323 ID, and ISDN numbers as relevant. More settings are viewable and editable in the **Settings** tab.
Conferences	Upcoming conferences where the system is scheduled to participate.
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.

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.
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.
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.

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
- 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 [p.234].

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 [p.124]
- Manage Ticket Error Levels [p.256]

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 [p.203].

For guidance on working with phone books, see Creating and managing phone books [p.194].

Connection

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *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 [p.234]. For more information, see System connectivity status [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

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.

Summary

This tab presents a summary of the most important data for the system.

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service [p.124] for more information.
System Settings	The selected system's network address, E.164 alias, IP URI, H.323 ID, and ISDN numbers as relevant. More settings are viewable and editable in the **Settings** tab.
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.
Conferences	Upcoming conferences where the system is scheduled to participate.
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.

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.
Call Settings	Here you will find for example the maximum ISDN and IP bandwidth, auto answer settings, and the H.323 ID, E.164 alias, and SIP URI of the system.
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.
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	Settings to allow or deny bookings and incoming or outgoing calls for the system. 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.

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
- 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 [p.234].

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 [p.124]
- Manage Ticket Error Levels [p.256]

Active Calls

A list of all ongoing recordings and playbacks. This tab is displayed for Cisco TelePresence IP VCR and Cisco TelePresence VCR MSE.

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 (Cisco TCS only)

This tab is displayed for Cisco Telepresence Content Server.

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

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *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 [p.234]. For more information, see System connectivity status [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.221].
Ticket Log	Open and closed tickets for this system. For more information on tickets, see Ticketing Service [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

Rooms and equipment

In Cisco TMS: **Systems > Navigator** a room or piece of equipment is selected

Cisco TMS has limited control over and access to settings for rooms and equipment.

For background on how rooms are managed compared to other endpoints, see How endpoints are managed by Cisco TMS [p.55].

For instructions on setting a system up as room or equipment, see Adding rooms or equipment [p.70].

Summary

This tab presents a summary of the most important data for the system.

Section	Description
Tickets	Open tickets on the selected system. See Ticketing Service [p.124] for more information.
System Settings	The selected system's network address, E.164 alias, IP URI, H.323 ID, and ISDN numbers as relevant. More settings are viewable and editable in the **Settings** tab.
Conferences	Upcoming conferences where the system is scheduled to participate.
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.

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.
Call Settings	Here you will find for example the maximum ISDN and IP bandwidth, auto answer settings, and the H.323 ID, E.164 alias, and SIP URI of the system.
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.
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	Settings to allow or deny bookings and incoming or outgoing calls for the system.

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.

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

- Set the **Management IP address** to the IP address of the current Cisco TMS server.
- 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 [p.234].

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 [p.124]
- Manage Ticket Error Levels [p.256]

Phone Book (rooms only)

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 [p.203].

For guidance on working with phone books, see Creating and managing phone books [p.194].

Connection (rooms only)

On the **Connection** tab and sub-menu, you can change the connection parameters used by Cisco TMS to communicate with the system:

Field	Description
Current Connection Status	The current status of the system.
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.
Track system on network by	Set the preferred address for your system. The options are: 1. *IP Address* 2. *Hostname* 3. *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 [p.234]. For more information, see System connectivity status [p.62].
Allow Bookings	Make the system available for booking by setting to *Yes*.

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 an endpoint [p.75].

Radio button	Description
Change system Network Address to	Enter the network address of the system that will replace the current system.
Switch or replace with existing system	Browse to a replacement system that has already been added to or auto-discovered by Cisco TMS.

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 [p.122] and Default System Permissions [p.271].

Logs

Use this tab to access 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 [p.124].
Audit Log	Changes to attributes for this system. For more information, see Audit Log [p.285].

Add Systems

In Cisco TMS: **Systems > NavigatorAdd Systems** has been clicked

When clicking **Add Systems** in the **System Navigator**, four different tabs are available:

- **Add Systems**
- **From List**
- **Pre-register Systems**
- **Add Room/Equipment**

Add Systems tab

The initial tab to open is **Add Systems**.

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 from a start to an end IP-address ■ a comma separated list of IP addresses and host addresses This means that when entering user.TMS.int, 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 systems in a range will be scanned.
Enter Location Settings	Specify the ISDN zone, IP zone, and time zone.

Advanced Settings	Click on the pane heading to expand and collapse this pane, which contains the sections below.
Set authentication settings	If the system(s) requires authentication, enter the username and password. Do not fill in the **Admin Password** field. If adding a recording server or content server, make sure to add the credentials for the API.
Persistent settings	Select a configuration template in Cisco TMS that will be set as persistent on the system(s). See Using configuration templates [p.30].
Discovery options	■ Specify the SNMP community names Cisco TMS will use when searching for the systems to speed up detection. SNMP community names for all systems must be registered in **Administrative Tools > Configuration > Network Settings**, seeNetwork Settings [p.234] . ■ Select **Discover Non-SNMP Systems** if the system does not support SNMP. ■ Select **Add unsupported systems** when adding systems which are not supported by Cisco TMS, such as PCs and network infrastructure devices. You can add such systems in order to make them available for booking in the **Booking > Ad Hoc Booking** page, see Ad Hoc Booking [p.173].
Other	In **Usage type**, specify whether the system is used as: ■ *Meeting Room* ■ *Personal Home* ■ *Personal Office* ■ *Roll About*

From List

Add auto-discovered systems, systems from other folders, or systems registered to Cisco Unified CM on this tab.

Menu option	Description
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. One system may appear in multiple folders, displayed in the **In Folders** column.
Unified CM	Systems registered to Cisco Unified CM are added to Cisco TMS here. See Adding Cisco Unified CM and registered endpoints [p.72].

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 [p.70].

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 [p.134]. 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**

Cisco Unified CM

Systems registered to Cisco Unified CM must *not* be pre-registered in Cisco TMS. See Adding Cisco Unified CM and registered endpoints [p.72].

Add Room/Equipment

On the **Add Rooms/Equipment** tab you can add meeting rooms or equipment that you want to be bookable in Cisco TMS. For step-by-step instructions, see Adding rooms or equipment [p.70].

Section	Description
Enter Details	Name the system and select one of the supported types for users' reference: - *Room* - *Digital Camera* - *Projector* - *DVD Player* - *Document Camera* - *VCR* - *Laptop* - *Video Camera* - *Other Equipment*
Advanced	Click on the **Advanced** section header to expand and collapse. The below settings are only relevant if adding an unsupported system.
Enter Location Settings	Specify the ISDN zone, IP zone, and time zone.

Section	Description
Enter Configuration Details	Enter further configuration details. Some fields are mandatory for rooms/equipment: ▪ Select **IP Zone**, **ISDN Zone**, and **Time Zone** for the room. ▪ 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**.

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 [p.271].

The permissions on these pages are displayed differently, but map as shown in the table below.

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 [p.271].

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.

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 [p.271].

Read	Read the **System Summary** and **View settings** pages for systems in the folder.

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 [p.256].

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

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:

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 [p.79].

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**

On this page, you can select systems and modify the following settings:

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.
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 [p.134].

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.

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.
Send Account Information	Send an email containing account information to all the users in the group/the 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 the user belongs to.

User Settings

Buttons in the **User Settings** section.

Button	Description
Edit	Edit the patterns.
Reload	Update patterns set at a higher group level.

The address patterns for configuration are described below:

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}@company.com`
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}@company.com`
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

Add and manage templates for each device.

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.

Button	Description
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.

Button	Description
Add Group	Enter a display name to create a FindMe group.
Add Account	Add account detail to create a FindMe account.
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.

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.

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**

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 [p.133].

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.
- 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 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 [p.128].

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

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

Field	Description
Name	A descriptive name for the configuration template.

Three tabs are available for setting up a template, described below.

Template Settings

This tab contains general 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.
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 Cisco 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.

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.

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.

Note: 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**.

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 will show the status of ongoing configuration templates being set on systems. You can delete a process by selecting it and clicking the **Delete** button.

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.
- 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 systems controlled by Cisco TMS and systems provisioned by Cisco TMSPE.

Software upgrade is not supported for rooms and Cisco Unified CM-managed systems .

Cisco TMS systems

For Cisco TMS-controlled systems you can choose from a drop-down list of display options similar to the display options in Navigator [p.79]. You can also search for specific systems by opening the **Search** tab.

Systems managed by the Provisioning Extension

For systems provisioned by Cisco TMSPE you can either choose to *Order by Software Version* or *List All*, which includes all systems 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 systems provisioned by Cisco TMSPE, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide*.

Upgrade modes

In the drop-down list at the bottom of the **System Upgrade** page, three upgrade modes are available:

Mode	Description
Basic	Cisco TMS will select a software package that is compatible with the software already installed on the system. This mode will work for most upgrades.
Advanced	You must manually select a package from the list of compatible packages.
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 systems.

Buttons for upgrading

At the base of the page, the following buttons are available:

Button	Description
Next	Display the **Select Software and Release Keys** page (see below).
Auto Select	Automatically select the systems that have newer software versions available (based on update checks for systems registered with Cisco) and display a list of these systems 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 [p.234].

Button	Description
Check for Updates	Automatically downloads the software updates and the corresponding release keys for systems that are registered with the upgrade web service at Cisco. If there are systems in Cisco TMS that are not registered or could not be identified by the upgrade check, an XML file with the unknown system will be generated. The file is accessible by clicking the **View unknown systems file** link in the warning message displayed after the check.
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. **Note:** This button is only visible when a system has already been selected for upgrade.

Some buttons are only available if **Automatically Check for Updates** has been set to *No*, see Network Settings [p.234]:

Button	Description
Import Log	Import a log of the software and release keys to all your Cisco systems, if you have received one. 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 systems by clicking the **Upgrade** button.
Generate Log	Generate a Release Key report from the page. The list will contain info about the systems shown and the software packages selected for each system.

Select Software and Release Keys

The **Select Software and Release Keys** page is displayed when one or more systems have been selected for upgrade and **Next** has been clicked.

Field	Description
Release Key	If this field has not been pre-populated by Cisco TMS, you must fill it in manually. Major version numbers require new release keys.
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-controlled endpoints [p.77].

Note that this software manager *cannot* be used for software packages intended for:

- Systems managed by Cisco Unified CM.
- Systems added to Cisco TMS as rooms or equipment.

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**, and ***.gz**.

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.

The destination directory for the software is visible in the **Software FTP Directory** field on the **Administrative Tools > Configuration > General Settings** page. To change the directory location, you must use the TMS Tools application, see .

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.

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.
ISDN/IP Bandwidth	Legacy field for TANDBERG Classic software version support.
Video Mode - Encryption Support	Video mode is a legacy field for TANDBERG Classic software version support relating to NTSC/PAL. 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.
- 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**

The event notification manager lets users subscribe to events, and be notified by email whenever the event occurs. Subscription requires the user to have access rights to the events.

To use the event notification wizard in Cisco TMS follow these steps

1. Select the user for whom to set a certain event notification level.
2. Click on the **Edit** link.
3. Check to select the system(s) and events to be notified of, and use the arrow button to move them to the right-hand list of stored notifications.
4. Click **Save**.
   You will now be notified by email when the selected events happen.

Select Event Types

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. (TANDBERG Classic only).
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. (TANDBERG Classic, Polycom VSX, Viewstation and Ipower only.)
Other	Other events not explicitly supported by Cisco TMS
Pre-registered System Activated	A pre-registered device has been detected and activated.
Scheduling	The systems is scheduled by Cisco TMS, or a scheduled conference is changed or deleted.
Scheduling error	An error has occurred in a scheduled conference.

Event type	Description
System Activity	FTP session in use on system.
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.

System status reporting

The following system statuses can be seen for systems in Cisco TMS, for example in **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 SOHO systems 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.

Booking

This chapter explains Cisco TMS conference concepts, describes the tasks related to booking, and details the entries in the **Booking** menu.

Conference Basics 147
Booking a conference 149
New Conference 154
List Conferences 169
List References 172
Ad Hoc Booking 173
Participant Templates 175
Settings 176
Conference Templates 177

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

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.

Some 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 TelePresence 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.

If the conference includes a Cisco TelePresence T1 or T3 and a Cisco TelePresence MCU MSE 8710 or Cisco TelePresence Server 7010, the Video Conference Master is the telepresence system that can add participants during the meeting.

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?

Layout options define how participants are arranged on the screen of the other participants in a conference.

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**.

Booking a conference

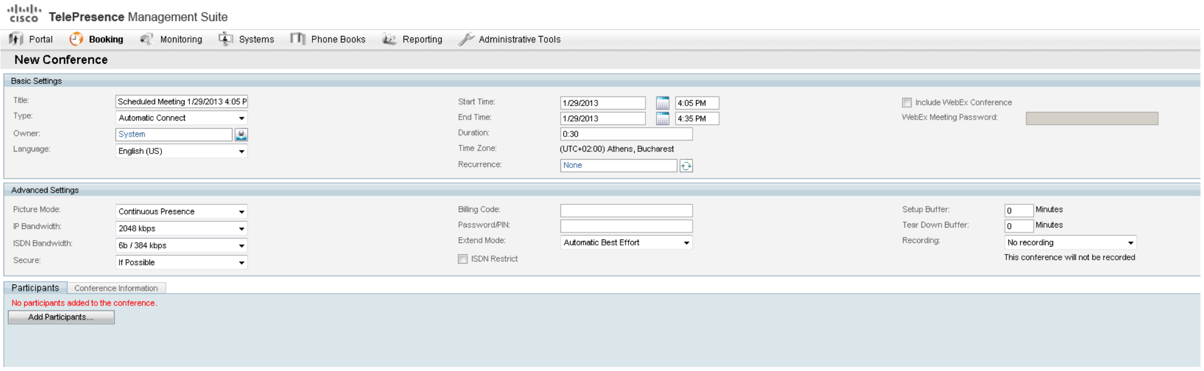
There are several ways to schedule a conference in Cisco TMS. **Booking > New Conference** provides advanced setup options for a conference during booking. This page is used in the procedure described below. **Booking > List Conferences > New Conference** also links to the **Booking > New Conference** 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.

To book a conference from **Booking > New Conference**:

1. Enter the basic settings:



New Conference

Basic Settings

Title: Scheduled Meeting 1/29/2013 4:05 P
Type: Automatic Connect
Owner: System
Language: English (US)

Start Time: 1/29/2013 4:05 PM
End Time: 1/29/2013 4:35 PM
Duration: 0:30
Time Zone: (UTC+02:00) Athens, Bucharest
Recurrence: None

□ Include WebEx Conference
WebEx Meeting Password:

Advanced Settings

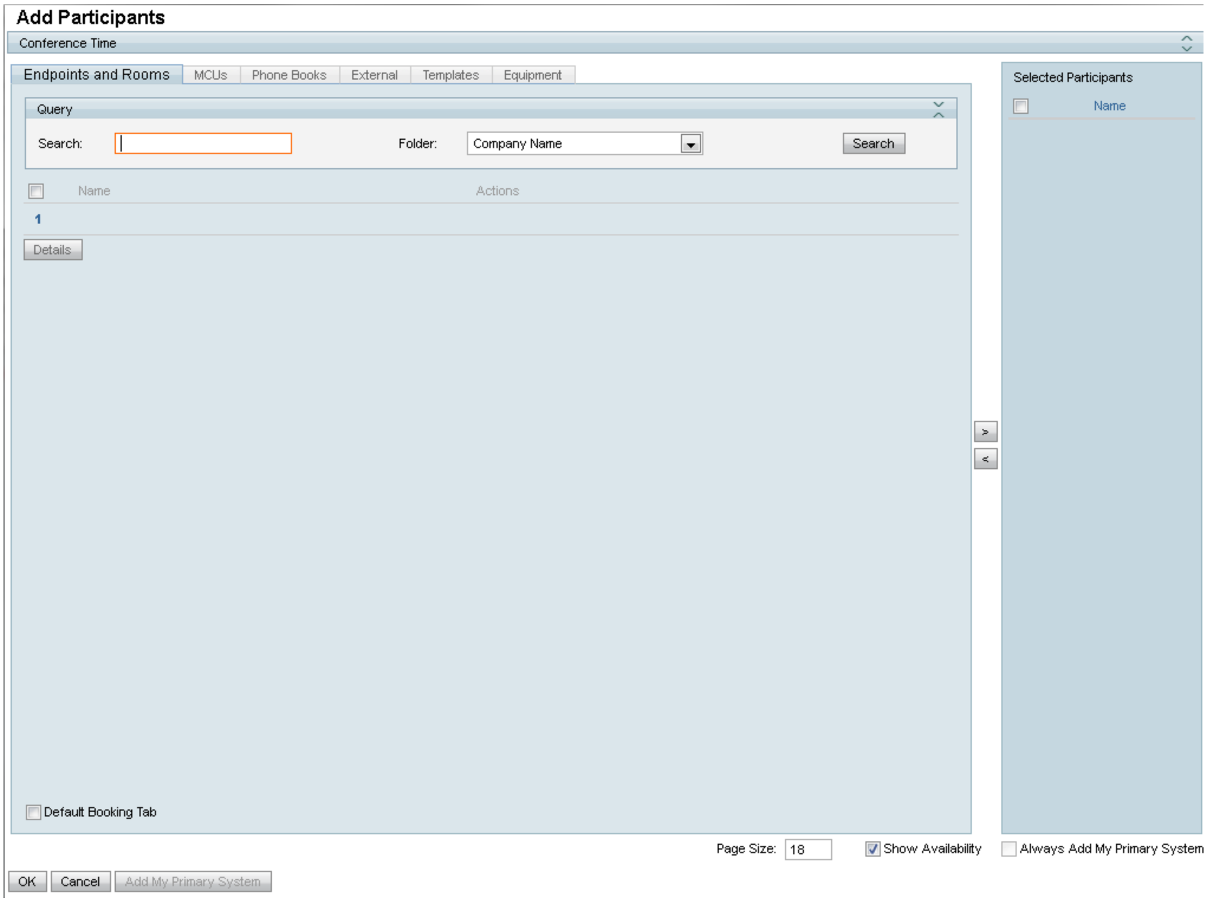
Picture Mode: Continuous Presence
IP Bandwidth: 2048 kbps
ISDN Bandwidth: 6b / 384 kbps
Secure: If Possible

Billing Code:
Password/PIN:
Extend Mode: Automatic Best Effort
□ ISDN Restrict

Setup Buffer: 0 Minutes
Tear Down Buffer: 0 Minutes
Recording: No recording
This conference will not be recorded

No participants added to the conference.

   a. Edit the conference title, which will help administrators and users to identify the conference in all Cisco TMS interfaces, and in email notifications.
   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 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 [p.246]**.
3. Optionally, add notes about the conference in **Conference Information**.
4. In the **Participants** tab, click **Add Participants** to display the Add Participants popup window (ensure you have allowed popup windows in your internet browser):



Folder: Company Name

Page Size: 18

☑ Show Availability

- 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.

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? [p.147].
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

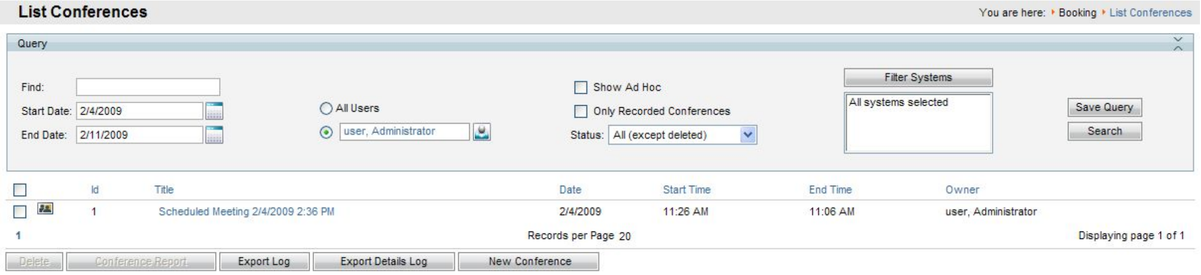
Some limitations apply when booking conferences that involve endpoints behind a firewall:

- 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.

Viewing and editing existing conferences

To view or edit a conference:

1. Open **Booking > List Conferences**



List Conferences

You are here: Booking List Conferences

Query

Find:

Start Date: 2/4/2009

End Date: 2/11/2009

○ All Users

● user, Administrator

□ Show Ad Hoc

□ Only Recorded Conferences

Status: All (except deleted)

All systems selected

□		Id	Title	Date	Start Time	End Time	Owner
□		1	Scheduled Meeting 2/4/2009 2:36 PM	2/4/2009	11:26 AM	11:06 AM	user, Administrator

1 Records per Page 20 Displaying page 1 of 1

2. Use the query 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.

Booking and editing conferences with Cisco TelePresence Conductor

Booking a conference

1. Book a conference as normal in Cisco TMS using **Booking > New Conference**. See Booking a conference [p.149] for instructions.
   You do not need to add the TelePresence Conductor to the conference manually if it is set as the default MCU in **Conference Settings**.
2. Once you have added the participants to the conference, click on the **Connection Settings** tab to display the **TelePresence Conductor Settings** tab and fill in the fields as appropriate:

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 **> Aliases** tab **> Edit Aliases**. For reference, see Aliases [p.100] .
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 Meeting 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.
Address Preview	A preview of the address which participants will use to dial into the conference. As you change the variable part, the blue part of the address shown in this field will change.
Description	This field contains the description added for the alias in **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.

3. To check that your chosen alias is available, click **Check Address Availability**.
4. Click **Save Conference**.

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.

Editing a conference

Edit the conference as normal in Cisco TMS using **Booking > List Conferences**. See Viewing and editing existing conferences [p.151] for instructions.

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 [p.154] section, an Advanced Settings [p.155] section, and a lower tabbed area.

Basic Settings

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**.
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. ▪ *Manual Connect*: At the specified time and date, the system listed as the VC.Master will be prompted to begin the call. The call will connect automatically when the VC.Master initiates the call. ▪ *No Connect*: This option will reserve the room(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	The language the conference is booked in. The confirmation email will be sent out in the language the conference is booked in.
Start Time	Set the start date and time of the conference.
End Time	Set the end date and time of the conference.
Duration	Set the duration of the conference.

Field	Description
Recurrence	Click **Recurrence Settings** to modify. - *Daily* includes settings for subsequent days or skipping weekends. - *Weekly* includes settings for how often and which day of the week you want the meeting to occur. - *Monthly* can be set to *Same day of month* or patterns such as: *first Monday* or *first weekday*. - Enter a **Number of recurrences** or an **End by Date**. When using recurrences, a meeting is limited to 100 total instances. 1. To create a custom recurrence pattern or make exceptions, use the calendar at the bottom of the pop up. If a change is made in the input fields that control the pattern, the calendar will reflect these changes. Click on a previously selected date to remove it from the series, and click on an unselected date to add it to the series. 2. Click **OK** to save the recurrence pattern.
Include WebEx Conference	Add a WebEx meeting and participants to your TelePresence conference.
WebEx Meeting Password	Create a password WebEx participants must use to access the conference. This must be numeric and a minimum of six digits.

Advanced Settings

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.

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*, Cisco TMS will only allow systems that support encryption to participate 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 to *On* on the endpoint, and this setting will persist after the conference has ended, until set to *Off* on the endpoint itself.
Billing Code	The user can specify which billing code the conference is to have. For more information, see Billing Codes [p.275].
Password/PIN	Setting up a password for a booked MCU ensures that the conference is protected from random dial-in participants. The participants will be asked to enter the password before being connected to the conference. The password is sent together with other conference information in the invitation email. Passwords must be numeric.
Extend Mode	■ *Off*: Ensure that meetings are never automatically extended . ■ *Endpoint Prompt*: Display a non-configurable Extend Meeting message on the VC 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 extension will only happen if there is at least 1 participant still connected, and there are no conflicting meetings for any of the participants or the MCU within the next 15 minutes.
ISDN Restrict	If checked, the conference will use ISDN restrict (56kbps). A restricted call is a call to a 56 kbps network.
Setup Buffer	If specified, the conference can be connected from 0 to 30 minutes before the meeting is scheduled to start. This is to ensure that the conference connects and makes it possible for dial-in participants to connect before the meeting begins.
Tear Down Buffer	If specified, the conference will not be disconnected for 0 to 30 minutes after the meeting is scheduled to end.
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 TelePresence 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 TelePresence Content Server will assist users in finding and using the correct one. **Note:** This option is only visible if a TelePresence 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.

Tabs

Tab	Description
Last Used	A list of the ten last participants selected by the logged in user for previous bookings.
Endpoints and Rooms	Endpoints and rooms 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.
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.
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. **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 [p.175].
Equipment	Add equipment registered in Cisco TMS.

Checkboxes and buttons

Checkbox/Button	Description
Details	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.

Checkbox/Button	Description
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.

Details opens the system details window for a selected system.

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.

If the conference includes a Cisco TelePresence T1 or T3 and a Cisco TelePresence MCU MSE 8710 or Cisco TelePresence Server 7010, the Video Conference Master is the telepresence system that can add participants during the meeting.

WebEx Details tab

This tab displays if you have added WebEx Enabled TelePresence 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 change several settings here, including:

- direction of calls.
- protocol.
- numbers dialed. Changing this will not change the number that the MCUor remote end will answer to.

By clicking on the **Settings** link to the right of each participant, additional settings can be configured, for example the bandwidth. For dial-out participants, **DTMF Tones** can be set in the **Number Settings** section.

For conferences with an MCU, it is possible to mute audio and video on connect for each separate participant.

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 [p.40].

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 [p.42]

Distribution (Routing Modes)

Type	Description
No distribution	Only one MCU will be used in the conference.
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 [p.47]. 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
- Rooms
- 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 [p.160].

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 [p.167].

Conference Information tab

Field	Description
Send Email To	Specify who will receive the booking confirmation by email. Email addresses can be separated by semicolon, comma or space.
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 [p.172].

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.

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 on routing in Cisco TMS, see Routing [p.38].
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.
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.

Setting	Description
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* ■ *Immediately*
Multicast Streaming Enabled	Allows multicast streaming for the conference.
Unicast Streaming Enabled	Allows unicast streaming for this 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.
Ports to Reserve for ConferenceMe	If using the ConferenceMe feature on the MCU, ports can be reserved for it using this field.

Cisco TelePresence Server

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.
Display warning on conference end	Display *This conference is about to end* warning.
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).

Field	Description
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 do 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**

Conference Address

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 **> Aliases** tab **> Edit Aliases**. For reference, see Aliases [p.100] .

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 Meeting 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.
Address Preview	A preview of the address which participants will use to dial into the conference. As you change the variable part, the blue part of the address shown in this field will change.
Description	This field contains the description added for the alias in **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.

List Conferences

In Cisco TMS: **Booking > List Conferences**

List and search for conferences on this page, based on specific criteria entered in the **Query** area. The conferences that match the search criteria are listed and can be sorted in the grid below.

Note: The user must have permissions to see their own conferences set in **Administrative Tools > User Administration > Groups** in order to edit bookings from this page.

Time zone display

On this page, bookings will be listed with the time zone of the currently logged-in user. However, when opening a booking to view or edit it, you will see the time zone that the conference was booked in.

Note that the time zone of a scheduled conference cannot be changed in Cisco TMS.

Query

Hover over fields to see a tooltip description.

Query field	Description
Find	A free-text search field, in which you can search through: ▪ Conference ID ▪ Conference title ▪ Email address ▪ Email message ▪ Comments for any conference. If an ID (integers only) is typed here, the search will check conference IDs only. This ID search will ignore dates and any other values set in the query section.
Start Date	Show conferences after this date. When changing start date, end date will automatically change with the same interval of days as before the change was made.
End Date	Show conferences up to this date. To change interval of days between start and end date, end date has to be changed.
All users/User	Show conferences belonging to all users/Show conferences belonging to the selected user.
Show Ad Hoc	Check this to show ad hoc, as well as scheduled conferences in the list.
Only Recorded Conferences	Only find conferences which include a Cisco TelePresence Content Server.
Status	Select the status of the conferences you are searching for.
Filter Systems	Click **Filter Systems** to display the list of all systems in Cisco TMS. Select the systems you want to view conferences for, and click **Save**. Conferences where one or more of the specified systems are participants will be listed in the query result.

Save Query	The settings saved are: ■ date interval ■ **Filter Systems** selections ■ **Status** ■ **Show Ad Hoc** ■ **Only Recorded Conferences** Only one query will be remembered at a time. This is the query that will be default the next time you enter the page.
Search	Click this button to run the query.

List Conference

Hover over the conference title in the search results, and depending on the status of the conference, a drop down menu will appear with options as described below.

Menu entry	Description
View	View the conference details.
Edit	Edit the conference details. The user must have access to the booking page for this option to be visible.
End	End an ongoing conference. The user must have permissions to edit conferences for this option to be visible.
Copy	Copy a conference so it can be used for a new booking. The user must have access to the booking page for this option to be visible.
Approve	Approve the conference . The user must have permissions to approve conferences for this option to be visible.
Reject	Reject the conference, which means that the conference will not start. The user must have permissions to reject conferences for this button to be visible.
Create as Template	Use the conference to create a template, a useful feature for frequently reused conferences.The user must have access to the booking page for this option to be visible.

Buttons on List Conferences page

Button	Description
Delete	Delete selected meetings. Note that ongoing conferences cannot be deleted. The user must have permissions to edit conferences for this button to be visible.
Conference Report	Generate reports for selected conferences. The report will be exported as a PDF file, where each conference will start on a new page.
Export Log	Export the list of conferences as a .csv file. All conferences that are listed will be included—it is not possible to explicitly select a conference.

Button	Description
Export Details Log	Export a detailed log (including two extra fields) of the conferences, listed as a .csv file. All conferences that are listed will be included—it is not possible to explicitly select a conference. The two extra fields are: ▪ Participants ▪ Log
New Conference	Click to be redirected to the **New Conference** page. The user must have permissions to make bookings for this button to be visible.

Conference status icons

Icon	Description
🟩	This conference is active and all participants are connected.
🟥	This conference is active but no participants are connected.
🟨	This conference is active but only some of the participants are connected.
✓	This conference has finished.
🕒	This conference is pending
✗	This conference has been rejected.
?	This conference has been requested and is awaiting approval.
🗑	This conference has been deleted.
🟢	This reservation is active.
✓	This reservation has finished.
🕒	This reservation is pending.
❌	This reservation has been rejected.
❓	This reservation has been requested and is awaiting approval.

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.

See New Conference [p.154] for descriptions of the fields, settings, and tabs available on this page.

Note: The user must have permissions to see their own conferences set in **Administrative Tools > User Administration > Groups** in order to edit bookings from this page. See Groups [p.262].

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** popup 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**

Templates represent external systems not managed by Cisco TMS but can also be set for systems managed by Cisco TMS. Participant templates make it possible to control how unmanaged systems are added to a conference. They can be used instead of external participants that dial in to a conference, or by giving more details to dial out participants. Settings in a participant template provide detailed control of how an unmanaged system is added to a conference. It is even possible to specify which MCU will call the unmanaged system.

To create a new participant template, click **New**.

The available settings in the **Dial Settings** tab are as shown in the table below.

In the **Identification** tab, you can write a description of the template and associate it with a **Reference**. For more information see List References [p.172].

Settings

Field	Description
Name	The user can specify a name for the template.
Reusable	1. *Yes*: The template can be added to one or several conferences several times. 2. *No*: The template can only be added once to one conference at a time.
Protocol	Specify the protocol that the unmanaged system will use in the conference.
Type	1. *Audio*: voice only, no picture 2. *Video*: both voice and picture)
Call Restrict	Specifies whether the unmanaged system will dial or be dialed at a restricted bandwidth (56 kbps).
Endpoint	If you select an endpoint, this endpoint will be booked when using the template in a booking.
Direction	1. *Dial Out*: the MCU dials out to the unmanaged system. 2. *Dial In*: the MCU allocates a port so that the unmanaged system can dial in to the conference.
Bandwidth	The bandwidth to use for the unmanaged system.
Number	Here the number of the unmanaged system should be entered. Only shown for dial outs.
Extension Number	If an extension number must be dialed to reach the unmanaged system, it must be entered here. Only shown for dial outs.
Second Number	Only shown if protocol is set to H.221 and it's a dial out. Enter the second number of the unmanaged system here.
DTMF Tones	Any DTMF (Dual Tone Multi Frequency) tones to be dialed after connection must be entered here.
MCU	Specify which MCU to use when connecting to the unmanaged system.
MCU Interface	Specify which MCU interface to use to connect to the unmanaged system. Examples of interfaces are ISDN1 and ISDN2.
Dial In Method (Only for Dial Ins)	Only shown if dial in and MCU are chosen. Dial in methods include: 1. *Conference Number*: The Participant Template will use the common conference number, this means that it will not have a unique number to dial. 2. *Participant Number per Conference*: The Participant Template will have a unique number within a conference. The number may change every time the Participant Template is in a conference. 3. *Participant Number Fixed*: The Participant Template will have a unique number within a conference. The number will always be the same for all conferences for this Template.
Caller ID	If the MCU of a conference is set to Protect On, all dial ins will be asked for a caller id before they are allowed to connect to the conference. Caller id may for example be the last digits in its ISDN number (if it dials in on ISDN). The Protect On parameter applies only to the Cisco MPS MCU, and is set on an MCU in a conference by using the MCU Settings tab in Cisco TMS Booking menu. The drop-down box is named Protect.
ISDN Zone	You can set ISDN and IP zones for unmanaged systems. For further details, see Locations [p.272].
IP Zone	

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**

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** and **Map Monitors**, which provide visual interpretations of your video network. Also included are related tasks and reference material for these menu items.

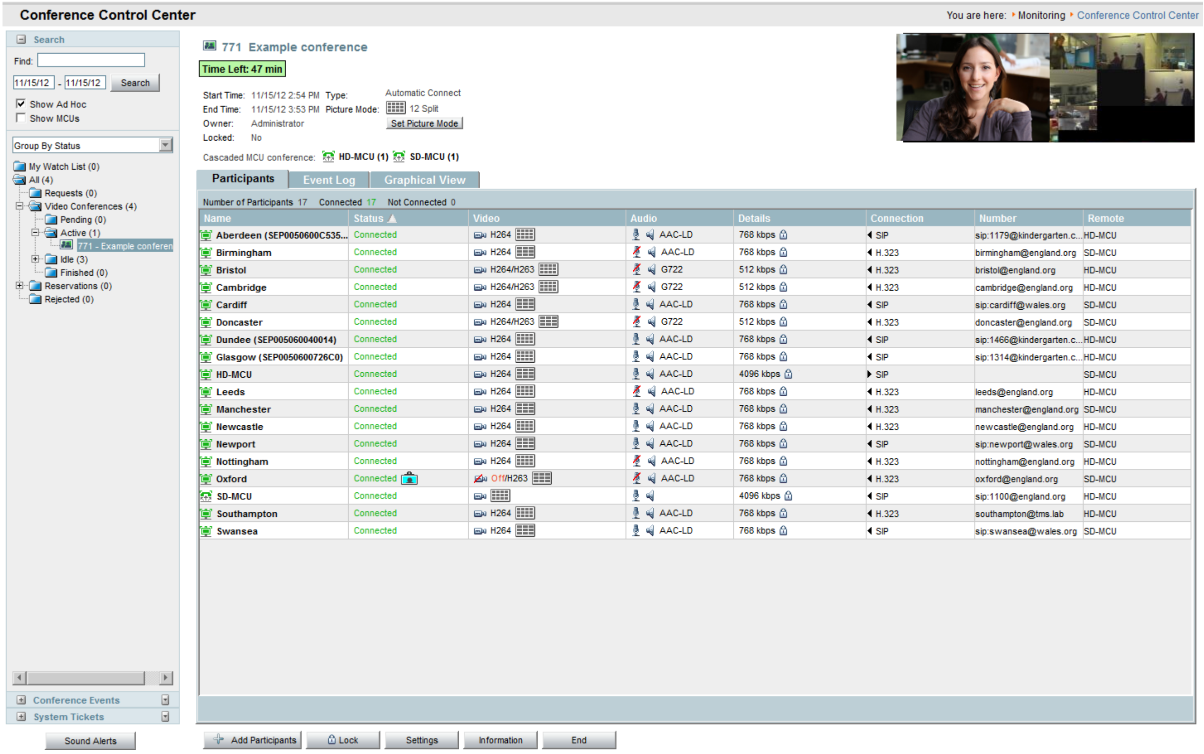
The monitoring tools require that Java Runtime Environment is installed on each client computer. To install or upgrade Java, go to www.java.com.

Monitoring and managing conferences 179
Operator conferences 181
Conference Control Center 182
Graphical Monitor 189
Map Monitor 191

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.



Conference Control Center

You are here: ‣ Monitoring ‣ Conference Control Center

Find:

11/15/12 - 11/15/12

☑ Show Ad Hoc
□ Show MCUs

Group By Status

771 Example conference

Time Left: 47 min

Start Time: 11/15/12 2:54 PM Type: Automatic Connect
End Time: 11/15/12 3:53 PM Picture Mode: 12 Split
Owner: Administrator
Locked: No

Cascaded MCU conference: HD-MCU (1) SD-MCU (1)

Number of Participants 17 Connected 17 Not Connected 0

Name	Status ▲	Video	Audio	Details	Connection	Number	Remote
Aberdeen (SEP0050600C535...	Connected	H264	AAC-LD	768 kbps	◀ SIP	sip:1179@kindergarten.c...	HD-MCU
Birmingham	Connected	H264	AAC-LD	768 kbps	◀ H.323	birmingham@england.org	SD-MCU
Bristol	Connected	H264/H263	G722	512 kbps	◀ H.323	bristol@england.org	HD-MCU
Cambridge	Connected	H264/H263	G722	512 kbps	◀ H.323	cambridge@england.org	HD-MCU
Cardiff	Connected	H264	AAC-LD	768 kbps	◀ SIP	sip:cardiff@wales.org	SD-MCU
Doncaster	Connected	H264/H263	G722	512 kbps	◀ H.323	doncaster@england.org	SD-MCU
Dundee (SEP005060040014)	Connected	H264	AAC-LD	768 kbps	◀ SIP	sip:1466@kindergarten.c...	HD-MCU
Glasgow (SEP0050600726C0)	Connected	H264	AAC-LD	768 kbps	◀ SIP	sip:1314@kindergarten.c...	HD-MCU
HD-MCU	Connected	H264	AAC-LD	4096 kbps	▶ SIP		SD-MCU
Leeds	Connected	H264	AAC-LD	768 kbps	◀ H.323	leeds@england.org	HD-MCU
Manchester	Connected	H264	AAC-LD	768 kbps	◀ H.323	manchester@england.org	SD-MCU
Newcastle	Connected	H264	AAC-LD	768 kbps	◀ H.323	newcastle@england.org	HD-MCU
Newport	Connected	H264	AAC-LD	768 kbps	◀ SIP	sip:newport@wales.org	SD-MCU
Nottingham	Connected	H264	AAC-LD	768 kbps	◀ H.323	nottingham@england.org	HD-MCU
Oxford	Connected	Off/H263	AAC-LD	768 kbps	◀ H.323	oxford@england.org	SD-MCU
SD-MCU	Connected			4096 kbps	◀ SIP	sip:1100@england.org	HD-MCU
Southampton	Connected	H264	AAC-LD	768 kbps	◀ H.323	southampton@tms.lab	HD-MCU
Swansea	Connected	H264	AAC-LD	768 kbps	◀ SIP	sip:swansea@wales.org	SD-MCU

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.

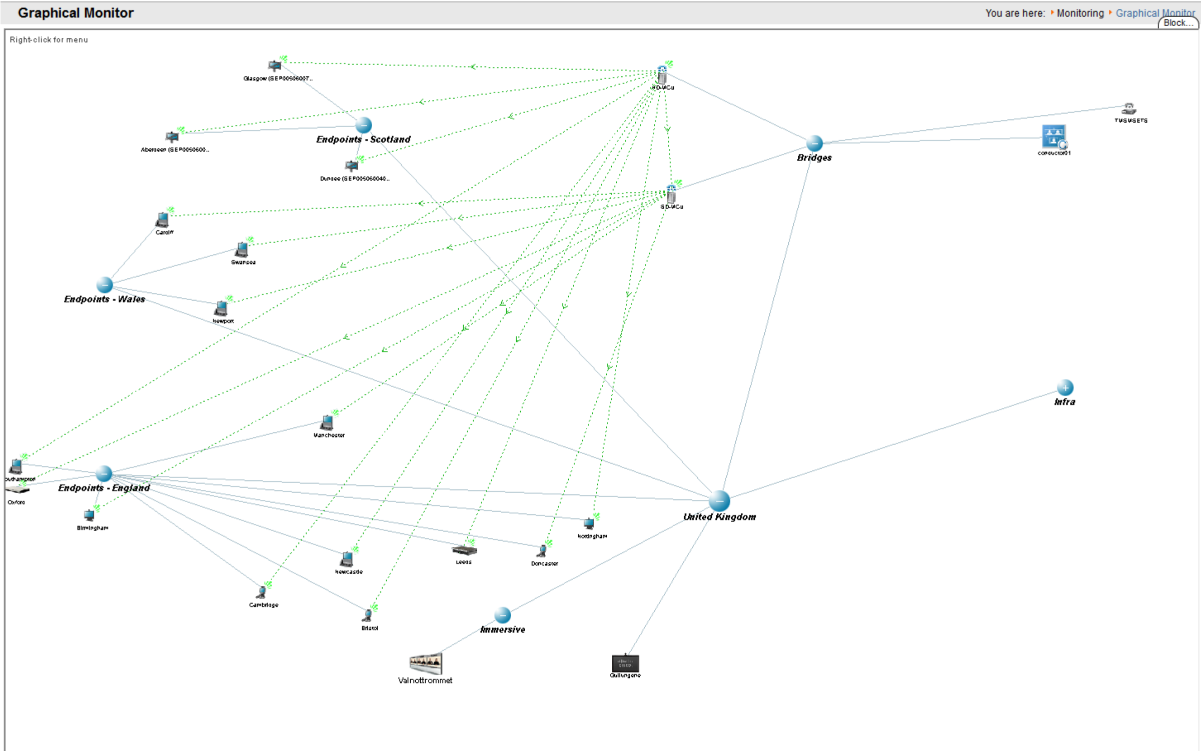
This means that if a site is having a problem or has questions, an operator can start a new conference and add themselves and the problem site(s) to the special conference. Once this conference is over, the operator can send the site back to their originally scheduled call.

For more information, see Operator conferences [p.181] .

Note: 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.

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.



Map Monitor

The **Map Monitor** is a variant of the Graphical Monitor where instead of all systems being shown on one page, each folder has its own page and administrators can overlay graphics behind the icons and images. This is very useful for showing geography or system location information.

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 through any of the booking interfaces listed below:

- **Booking > New Conference** in Cisco TMS
- Any extension using Cisco TelePresence Management Suite Extension Booking API, including Cisco TMSXE and Smart Scheduler
- Any call not initiated by Cisco TMS on a system or MCU that is registered to Cisco TMS

Conference Control Center can also monitor ad hoc calls (not booked by Cisco TMS). To enable this:

1. Go to **Administrative Tools > Configuration > Network Settings**.
2. Set **Enable ad hoc conference discovery** to *Yes*
3. Select **Show Ad Hoc** in the left hand panel of the CCC page.

Search field and folder view

The folder view on the left side of the screen shows a list of all the meetings booked and registered in Cisco TMS. It is possible to narrow down or expand the list of conferences by using the **Find** and **Date** fields in the search area.

Note: If the search string entered is an integer, the system searches by conference ID. If the search string is in text format, conferences with a matching conference title or matching conference participant names will be shown.

The *Group By...* dropdown box below the **Find** fields is used to sort the conferences by status, date or owner.

Any conference that has no connected participants will be in the **Idle** rather than the **Active** folder.

Selecting a conference

Select a conference by clicking on it. The window to the right will then show the conference details.

Right-click the conference and select **Open in new window** to display the information in a separate window.

Ending or deleting a conference

Use the **Delete** button to end or delete conferences, or right click the meeting title and select **End** or **Delete**.

Default start folder

To set a folder as the default start folder, right click and select *Set as default start*. This is only possible for static folders, you can't set this option for folders created from an MCU, or grouped by date or user..

Showing ad hoc calls

Selecting the **Show Ad Hoc** check box allows monitoring and management of ad hoc calls including systems which are managed by Cisco TMS.

Show MCUs

Selecting the **Show MCUs** check box will display each MCU registered in Cisco TMS as a separate folder in the folder list. Pending, active and finished conferences are displayed under the main MCU for that conference. Conferences with a main system that is not an MCU are shown in the **Other** folder.

My Watch List

The **My Watch List** folder in the folder view contains conferences which are selected and added by you from the folders beneath. If you wish to add a conference to put on this list and follow it up more closely, right-click on a conference in the folder view and select **Add to Watch List**. The conference is then copied to the **My Watch List** folder. To remove a conference from the list, right-click on the conference and select **Remove from Watch List**.

Conference Overview

When a folder containing conferences is selected in the folder view , a conference list including all conferences in that folder will appear in the **Conference Overview** on the right side of the screen.

Conference details can be accessed as follows:

- Double-click on the conference in the **Conference Overview**.
- Right-click on the conference in **Conference Overview** and use the context menu.
- Select the conference in the **Conference Overview**, then click the appropriate button at the bottom of the screen.
- Browse your way through the folder menu until you can select the conference you want to view.

Conference Details

After you have accessed the conference, (see above) you will be able to view information on the conference and perform different actions regarding the conference.

Conference information

Field	Description
Title	Meeting ID and Meeting title.
Start Time	The start time of the meeting.
End Time	The end time of the meeting.
Owner	The name of the owner of the conference (not necessarily the person who booked the meeting).
Locked	Use the **Lock/Unlock** button at the bottom of the page to change. Options: ■ *Yes*: The MCU in the conference will not allow any more participants to dial in. The administrator will be able to add participants. ■ *No*: The MCU will allow participants to dial in to the conference.

Type	How the call will connect.
Picture Mode	The picture mode of the conference

Conference actions

Field	Description
Set Picture Mode	This option allows you to set the picture mode for the conference. You will be able to select between all the layouts available on a Cisco TelePresence MCU.
Add Participants	Add participants to the conference. The add page gives you the same options as the add page in booking. Use the button at the bottom of the screen.
Lock/Unlock	By locking a conference the MCU will not allow any more participants to dial in to the conference.
Settings	This is where the information and settings for the conference can be edited See the New Conference [p.154] section for more information about these settings.
Accept	Accept the meeting, if it was booked by a user that cannot approve meetings.
Reject	Reject the meeting, if it was booked by a user that cannot approve meetings.
End	Ends the conference. Not available for permanent conferences.

Conference view also displays snapshots from the conference and Duo-video snapshots if available. Sound alerts will be given if a participant is disconnected or a new participant joins the conference.

Participants tab

This screen will give you an overview of the participants in the conference.

Right click on a participant to view and edit its settings.

For ongoing conferences there are buttons and a right-click menu and available when one or more participants are selected. Only commands which are supported by all selected participants are visible.

It is possible to drag-and-drop participants from one conference to another on the same MCU (Cisco TelePresence MCU and Cisco TelePresence MPS only).

- Drag the participant from the Participants list to the other conference displayed in the tree view (left).
- To move the participant back to the original conference:
  a. Select the participant.
  b. Click the **Get back** button.

Commands available for participants

You will see different buttons/commands depending on the functionality available on the selected system.

To see the name of the command/button, mouse over and read the tool tip.

Icon	Name	Description
📄	**View Details**	Gives you detailed information about a system's settings.
🌐	**View Web**	Shows you the web interface of the system.

Icon	Name	Description
🚫	**Mute Audio**	Mutes the audio of a participant. (Only available for Multipoint calls).
🎤	**Unmute Audio**	Unmutes the participant.
🎤 🚫	**Microphone On/Off**	Sets microphone(s) on/off for that participant in this conference.
↖	**Set Floor**	Gives the floor to the selected participant.
↘	**Release Floor**	Releases the **Set Floor** setting for the selected participant.
👥	**Set Important**	When you make a participant "important", it sets this participant as the focused participant. For example, this participant is considered the loudest participant even if they are not speaking.
👥	**Remove Important**	Cancels the **Set Important** setting.
📵	**Disconnect**	Disconnects the selected participant.
✉	**Send Message**	Sends a message that will appear on the video system of the selected participant.
÷	**Remove**	Removes the selected participant from the conference.
📞	**Connect**	Connects the selected participant.
📞	**Connect All**	Connects all participants (only available from the video conference master participant).
📵	**Cancel Connect**	Cancels the connection to the selected participant.
📵	**Disconnect All**	Disconnects all participants in the conference (only available from the video conference master participant).
🚫	**Mute Outgoing Audio**	Mutes outgoing audio to this participant.
🔈	**Unmute Outgoing Audio**	Removes the mute setting for outgoing audio for this participant.
🚫	**Mute Video**	Mutes the video of a participant.
📹	**Unmute Video**	Unmutes video for this participant.
📹	**Status Duo Video**	Mouse over to see content stream information for MCUs in conferences. This applies only to Cisco TelePresence MCU 4.2 and newer.
🚫	**Block FUR**	Blocks fast update requests from remote participant.
🗐	**Unblock FUR**	Unblocks fast update requests from remote participant.

Icon	Name	Description
name	**Change Display Name**	Changes participant's display name.
	Show Snapshot	Shows snapshots for this participant.
	Contact Information	This information is collected from **Systems > Navigator >** select system **Settings > General > System Contact** field.
←	**Move to operator conference**	Moves the participant from the current conference to an operator conference.
→	**Move Back**	Moves the participant back to the original conference.
	Dial Settings	Shows connection settings for this participant.
→	**Get back**	Brings a participant that has been moved from a conference back to the original conference.
	Drop down menu	Layout drop down menu found on the button bar and only for Cisco TelePresence MCUs. Changes the layout of the receiving video for this participant.
	+participant name	If an MCU is used in a conference, button **+participant name** directly above the action buttons contains additional information for each participant. Select one participant and click the button. The transmit and receive statistics for video and audio for this system will be displayed. When applicable, button will show content stream information.

Event Log tab

This tab contains a list of all the events that occurred during the conference. This list can be presented in a printer friendly version by clicking **Open as Text** at the bottom of the screen.

Fifteen minutes before the conference starts (or at booking time if the start time is less than 15 minutes and more than one minute ahead in time) conference diagnostics are run on a conference. The diagnostics service checks all systems in the conference for system tickets that can affect setup of the conference. It also checks if the routed calls are still valid call alternatives, and if MCU dial in numbers exist. Any problems it discovers will create an event in the event log.

Run Diagnostics button

It is possible to run the conference diagnostics manually from the **Event Log** tab by clicking on the **Run Diagnostics** button.

Graphical View tab

This tab, seen when clicking on a conference in **Conference Details** gives you a nice graphical overview of how the different sites are connected together. The lines show how they are connected, the arrow on the line shows the direction of the call and the color of the line indicates status of the connection. All commands available on the **Participants** tab are also available in this view, but only one participant can be selected.

Conference Events

In **Conference Events**, events from pending and active conferences are shown.

When right-clicking on a system event, the following choices are available:

- **Acknowledge Event**
- **Clear Event**
- **Open Conference**
- **Open Conference in New Window**

Show My Watch List events

By clicking the drop-down icon to the right in the **Conference Events** header you get the choices **My Conferences List** which shows only events from the conferences in the **My Watch List** folder.

Show lists and events

Open Detailed List, **Show/Hide Acknowledged Events** and **Show/Hide Viewed Events** show an event marked as viewed when a user has opened the conference details page after the event occurred).

Conference events are marked in the folder view, in the conference list and in the conference details if the event is tied to a participant.

System Tickets

System Tickets shows conference and system tickets from Cisco TelePresence MCUs and Cisco TelePresence MPSs. The panel can be collapsed and expanded by clicking on the show/hide +/- icon in the headers.

Open Detailed List

By clicking the drop-down icon to the right in the **System Tickets** header, you will get the choice **Open Detailed List**, which shows a detailed event list in the right side of the screen.

Show Acknowledged Events

Choose whether to show tickets that have been acknowledged.

By right-clicking on a system event in the list, you will get three choices.

- **Acknowledge Ticket**
- **View system details** (opens the system page from the system navigator in a pop-up).
- **Open Detailed List** (displays a detailed event list on the right side of the screen).

Moving the mouse over the tickets will show a tool-tip with the details of the ticket.

Sound Alerts button

Clicking the **Sound Alerts** button opens the **Sound Alert** pop-up window.

For active conferences you can set alert for

- **Error Events**
- **Warning Events**
- **Info Events**

For opened conferences you can set sound alert for

- **Participant Connected or Added**
- **Participant Disconnected or Removed**

Alert sounds can be turned on and of by respectively checking or un-checking check boxes.

Test the sound alerts by clicking on the **Test** button by the alert description.

These settings are stored on a per user level.

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

Change the user settings of the Graphical Monitor:

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*

Field	Description
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.

Map Monitor

In Cisco TMS: **Monitoring > Map Monitor**

This page provides an overview of the physical locations of the systems in your network. Each folder can be associated with its own background picture (for example country map, map of an office building and so on) where the conferencing systems are placed on top of the picture.

Setting up an organization in Map Monitor

Only the administrator in Cisco TMS can organize the conferencing systems. Other users can see the systems on the map, but cannot create/delete folders, move systems between folders or place the systems on the background pictures.

In order for the Map Monitor to be used effectively, the folders created in Cisco TMS should correspond to the physical location of the conference systems. For example a conference system in an international company ExampleCompany located in Chicago should have a tree structure corresponding to: ExampleCompany/ ExampleCompanyUS/ ExampleCompanyChicago. The three folders should be associated with one background picture each. Suitable background pictures to be associated with the three folders would be: a world map, a US map, and a layout map of the office space in Chicago. The layout map would show all the rooms in the Chicago office, and the icons for each conference system would be placed in the right room.

Organizing folders and icons

In order to move a conference system or a folder, simply drag the icon by holding down the left mouse button and release to place the icon. If the conference system should be moved in to another folder, just drop the icon on the folder. To move a system upwards in the folder hierarchy, drag and drop the system to the icon (blue circle with white triangle) located in the upper left corner of the map window. The folder structure is the same as in the rest of Cisco TMS, and any changes in the folder hierarchy or movement of conferencing systems is automatically updated in the rest of Cisco TMS.

Assigning background images

Every folder can be assigned its own background image. To change the background image:

1. Right-click inside the window.
2. From the context menu, choose **Select Map**

Options in the background menu

Control Panel

By right-clicking on the background of the **Map Monitor** menu and selecting **Show Control Panel** you can choose between different presentation options:

- Move the **Zoom** slide bar to increase or decrease the size of the picture.
- Select **In Call** to display only systems that are in call.
- Select **No Response** to display only systems that are for example turned off, not connected to the network or with some kind of network problem.
- Select **Idle / Alive** to display only systems that are alive or idle.

Options

By selecting **Options** you can change the user settings of the **Map Monitor**.

Field	Description
Show Name	The system name will be shown for all systems in the graphical monitor.
Show Network Address	The system IP addresses will be shown for all systems in the graphical monitor
Visible Characters	Allows you to choose how many characters will be displayed for each system.
Font Size	The options are: 1. *Small* 2. *Normal* 3. *Large*
Label Color	Coloring of the label text for each system. The options are: 1. *Dark Grey* 2. *Blue* 3. *Orange*
Animation	Choose the speed of the animation of systems in call. This animation is shown as circles around the systems in call with systems not registered in the Cisco TMS. The options are: 1. *Fast* 2. *Normal* 3. *Slow*
Update Frequency	This option defines 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.
Show Call Animation	This option defines turns the animation of the systems in a call on or off. **Note:** Using animation requires more resources from the Cisco TMS-client.
Show Call Lines	This option turns on/off the visual presentation of the line between two systems which are in call. The two systems must be registered in Cisco TMS.
Gray Maps	Click this button to show the maps in grey scale. This will enhance the contrast between the systems and the map, since the systems will still be in color.

Up one level

This setting is only available when having expanded one of the system folders represented by the blue icons with subsystems. The option will then bring you up one level.

Zoom In

Each time this options is chosen the map with Cisco TMS systems is enlarged one step.

Zoom Out

Each time this options is chosen the size of the map with Cisco TMS systems is decreased one step.

Select Map

This menu option lets you decide which map should be shown in the background of the Map Monitor.

Upload Map

This menu option lets you upload your own maps. The format of the map should be .gif.

System icons

The System icons are used both in the **Graphical Monitor** and the **Map Monitor**. All systems have icons corresponding to the different system types supported by Cisco TMS. In addition to resembling the systems the icons also indicate different system statuses

System status

If a system is in a call, the system icon changes to reflect this:

- The Set-Top icon displays a green dot in the camera.
- The Table-Top, Meeting System and Videoconference System icon display green screens.
- The Cisco TelePresence MCU displays green dots in the front panel.
- If the call is encrypted, there will also be a small padlock down to the right of the system icon.
- A system that is in a call with a system not in Cisco TMS will have a flashing circle around the icon.
- Selected third party products will also have green screens to indicate that they are in a call.
- If a system has a status of *No response*, it is marked with a red cross.
- Unknown endpoints are shown with a question mark.

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 195
Phone book types 196
Creating a phone book 198
Granting access to phone books 200
Setting phone books on systems 201
Exporting contacts to a file 202
Manage Phone Books 203
Manage Phone Book Sources 205
Phone Book and Source Activity Status 214

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 Cisco Unified CM users. For an extensive list with descriptions and configuration options, see Manage Phone Book Sources [p.205].

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 [p.198].

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 [p.38].

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 [p.201].
- 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 and TANDBERG Classic 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 [p.201].
- At the intervals specified in **Phone Book Update Frequency**. See General Settings [p.232].

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 [p.205].

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 [p.205] for a reference to source types.
4. Enter a name for the new source.
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 [p.205] 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*:
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 [p.200].
2. Set phone books on the systems, see Setting phone books on systems [p.201].

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 TMS Tools application. For more information, see Generate Phone Book [p.293].

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 [p.262].

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 [p.214] 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 [p.214] 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

You can set up the *File Based Phone Book* source to use for exporting phone book contacts to a file on a directory on your Cisco TMS server or another web server. Cisco TMS will then create a tab delimited file.

1. Create a phone book .
2. Click **Connect** for this phone book.
3. Select the sources you want to export contacts from.
4. For **Update Type** for these sources, select either *Import to Cisco TMS* or *Import to Cisco TMS and Export to phone book source*.
5. Now select the *File Based Phone Book* source you want to export to.
6. For **Update Type** for this source, select *Import to Cisco TMS and Export to Phone Books Source*.

The first line of the file will contain the headers; Name, ISDNNumber, ISDNNumber2, ISDNBandwidth, Restrict, Telephone, SIP, H.323, IPBandwidth, 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 [p.201] 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

Field	Description
Name	The name of the source with a link to Manage Phone Book Sources [p.205], where you can modify configurations for the source.
Type	The type of phone book source. For an overview, see Manage Phone Book Sources [p.205].
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. ■ *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 [p.205].

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 [p.205].

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 [p.200].

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:

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.
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

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:

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.
✎ 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

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.

Field	Description
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 IP phone contacts from the directory.
Import Home Phone	Import home phone contacts from the directory.
Import SIP	Import SIP contacts from the directory.
Import Mobile Phone	Import mobile phone contacts from the directory.
Import Telephone	Import telephone contacts from the directory.

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.

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.

Field	Description
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*.
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.

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\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

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

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

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 and TANDBERG Classic.

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 Cisco Unified CM for a phone book source.

Settings

Field	Description
Select Cisco Unified Communications Manager	Choose a Cisco TMS-managed Cisco Unified CM from the drop-down.
Advanced Settings	
Prefix for Imported Numbers	Add this prefix to all numbers imported from Cisco Unified CM.
Suffix for Imported Numbers	Add this suffix to all numbers imported from Cisco 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.
- 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**.

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 216
Creating a report 217
Using reporting templates 219
Call Detail Records 221
Billing Code Statistics 223
Conferences 224
System 226
Network 228
Return on Investment 229
CO2 Savings 230

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 [p.278].

Types of data

- Call Detail Records [p.221] track the frequency and duration of calls in your telepresence deployment.
- Billing Code Statistics [p.223] show which billing codes are applied to conferences.
- Conferences [p.224] are tracked per user, type, and so on.
- System [p.226] reporting catches errors and other events from systems.
- Network [p.228] statistics report on network and bandwidth usage.
- Return on Investment [p.229] and CO2 Savings [p.230] calculate return on investment and environmental savings for your video equipment.

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 Statistics Settings [p.254].

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:

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 [p.219] 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.
   - **Report** view: a format suitable for printing; click **Export to PDF** to save or print the report. The PDF will contain both the chart and the query data used to calculate the chart.

Exporting data to an Excel sheet

Under the **Data** tab, click on **Export Excel** to export all data to an Excel sheet.

The exported Excel sheet 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**.

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 [p.222] page.

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.

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.

CDRs for provisioned users and their endpoints are generated and accumulated by the Cisco VCS that each endpoint is registered to. Cisco VCS pushes CDRs to Cisco TMS at regular intervals.

These CDRs are listed per user.

Content Servers

If you have content servers and/or recording 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.

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.

Only the 20 last conferences will be shown in 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 [p.154]
- 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 [p.79].

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, FTP, HTTP or SNMP.

Boot

The **Boot** page displays statistics for all boot events on systems registered in Cisco TMS.

FTP Audit

The **FTP Audit** page gives an overview of all FTP (File Transfer Protocol) activities towards a system. This report is only supported by legacy systems.

Low Battery on Remote Control

The **Low Battery on Remote Control** page shows the number of low battery events on all Cisco TMS endpoints' remote controls in the specified time interval.

Network

In Cisco TMS: **Reporting > Network**

The pages in the **Reporting > Network** menu section contain reporting options for network activity involving Cisco TMS-managed systems. Note that all reporting options are not supported by all system types or endpoint types.

Packet Loss Log

The **Packet Loss Log** page shows all packet loss info sent by systems to Cisco TMS. This report is only supported by legacy TANDBERG MXP endpoints.

Every 30 seconds systems will send a message to Cisco TMS if there is a packet loss during this period. The log will contain the accumulated packet loss and the accumulated packet sent.

Packet Loss Conference

The **Packet Loss Conferences** page displays all conferences with packet loss.

Bandwidth Usage

Bandwidth/Average use of Bandwidth displays a graph showing the average use of bandwidth within a time period for a selected system, measured in kilobits per second and displayed per protocol (IP, ISDN, and SIP).

The protocol will be listed as *Unknown* for some third-party endpoints and in other cases where the endpoint is not providing this information to Cisco TMS.

Network History

The **Network 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.

Return on Investment

In Cisco TMS: **Reporting > Return on Investment**

The **Return on Investment Global** and **Local** pages show you how much of your company's total investments in video have been paid back in terms of savings on traveling costs over a defined period of time.

Only meetings lasting longer than the amount specified in **Administrative Tools > Configuration > Statistics Settings** under **Statistics ROI/CO2 Minimum Call Duration** will be included in the calculation. The default value is 60 minutes.

Calculating ROI

1. Set the start and end date of the calculation, starting with the date of the first telepresence hardware purchase.
2. Specify the average number of participants joining a video meeting at each endpoint. The graph is calculated by average traveling cost for every participant at N-1 endpoints.
3. Specify the average cost for one employee going on a business trip.
4. Enter the average cost of the video systems in your network (including infrastructure systems like gatekeepers and MCUs).
5. Enter the average number of endpoints used per conference.
6. Click **Calculate**.

Method for calculation of ROI

The average number of participants that would have traveled will be calculated by multiplying the number of participants per endpoint with the number of endpoints in a conference minus one. For example, if the average number of participants in front of each endpoint is five, and the average number of endpoints is three, then the average number of would be travelers is given by 5 * (3-1) = 10.

The black line in the graph will show a calculation of the Average System Cost multiplied with the number of systems in Cisco TMS. The green graph will show a calculation of the number of systems in calls in the specified period, multiplied with the average number of participants that would have traveled, multiplied with the average cost of a business trip for one employee.

CO_2 Savings

In Cisco TMS: **Reporting > CO_2 Savings**

On the **CO_2 Savings** page you can calculate how many kilograms CO_2 emissions you save by using video conferencing instead of traveling.

Calculating CO_2 Savings

To calculate:

1. Set the start and end dates for the calculation.
2. Specify the average number of participants joining a video meeting at each endpoint. The graph is calculated by average CO_2 cost for every participant at N-1 endpoints.
3. Specify the average CO_2 cost in kilograms per business trip.
4. Specify the average number of endpoints used in a conference.
5. Using the **Filter Systems** button, select the systems you want to include in the calculations. If none are selected, all systems in Cisco TMS will be included. Note that CO_2 savings are calculated based on endpoint usage only.
6. Click **Calculate**.

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 232
User Administration 262
Locations 272
Billing Codes 275
Activity Status 277
Analytics Extension 278
TMS Server Maintenance 279
TMS Tickets 282
Provisioning Extension Diagnostics 283
Audit Log 285

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**

General Settings

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.
Software FTP Directory	The Software FTP Directory on your Cisco TMS server where system software used for system upgrades is stored. This location is edited using the 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.

Field	Description
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 [p.196] 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.
Alternate System Name Rules for Endpoints and Rooms (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.
Enable Auditing	If set to *Yes*, 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 [p.285]**. This setting can be overridden in **TMS Tools >** .
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.

Field	Description
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

The first part of this section contains an overview of how many licenses are in use and how many are available.

The second part of the section contains a list of current option keys which have been added to Cisco TMS.

Click **Add Option Key** to add option keys to Cisco TMS.

Network Settings

In Cisco TMS: **Administrative Tools > Configuration > Network Settings**

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.
FTP Timeout (in seconds)	The number of seconds Cisco TMS will wait for a response when trying to initiate an FTP connection (for software upload, or similar), before it times out.
SNMP Timeout (in seconds)	The number of seconds Cisco TMS will wait for a response to an SNMP query. You can set this value to 1, but it can be increased if you experience problems with receiving SNMP feedback from systems.

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.
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	Specify which URL will be used when executing software upgrades on systems behind a firewall/NAT. The endpoint will contact this URL to download the software package that it is upgrading to. We recommend using the default directory **TMS/public/data/software** as this is where Cisco TMS retrieves its list of packages (**Systems > System Upgrade > Software Manager**). Otherwise you may schedule an upgrade with a package found in the list that is not found on the alternate URL you have specified. **Note:** 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.
Event Notifications	
Email Addresses to Receive System and Network Notifications	Specify which email addresses will receive an email when an event notification message is created. Enter multiple addresses in a comma separated list.
SNMP Trap host IP Address	The IP addresses listed here (comma separated list) will receive SNMP Traps from Cisco TMS when an event notification message contained in the MIB file which is included in the Cisco TMS software package, is created.
SNMP Version for Traps	The SNMP version Cisco TMS uses for Trap notifications. Only SNMPv2 is supported, and this field is not editable.
Automatic System Discovery	
Automatic System Discovery Mode	Cisco TMS is capable of automatically discovering and registering systems. To do this, the systems need to be configured to send HTTP events or SNMP traps to Cisco TMS. Set to *On* to enable this feature. 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 > From List** and can be added to a folder from here. 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**.

Sections and fields	Description
Default Configuration Template for Discovered Systems	When Cisco TMS discovers an unknown system, you can set it to apply a default configuration template to the system. The default: *Discovered Systems Template* does the following when a system is discovered by Cisco TMS: ■ Moves the system into the **Discovered Systems** folder. ■ Sets the default IP Zone. ■ Sets the Time Zone. ■ Sets Phone Books on the system. To override this, select another template in the drop-down menu.
Default Folder for Discovered Systems	Discovered systems will be added to this folder in **Systems > Navigator**.
Automatic System Discovery Mode for Endpoints behind a Firewall/NAT	Cisco TMS is capable of automatically discovering and registering systems behind a firewall/NAT. To do this, the systems need to be configured to send feedback to Cisco TMS. Set to *On* to enable this feature or set to *Off* to disable it. 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	When Cisco TMS discovers an unknown system behind a firewall/NAT, you can set it to apply a default configuration template to the system. The default template will move the system into the **Discovered Systems** folder and set the default Phone Book on the system. To override this, select another template in the drop-down menu.
Active Directory	
Lookup User Information from Active Directory	Specify that Cisco TMS should look for user and group information in Active Directory.
GC server or AD forest DNS name	Specify the GC (global catalog) server or AD forest DNS name.
AD Lookup Account - Username	Specify the username Cisco TMS will use to connect to Active Directory.
AD Lookup Account - Domain	Specify the domain Cisco TMS will use to connect to Active Directory.
AD Lookup Account - Password	The password that corresponds with the username in the **AD Lookup Account - Username** field.
Allow AD Groups	When set to *Yes*, Active Directory groups can be imported to Cisco TMS, in **Administrative Tools > User Administration > Groups**, see Groups [p.262].
AD synchronization schedule	Schedule which day of the week and at what time the Active Directory sync of users and groups will happen.
Test connection to Active Directory	When you have configured the settings above, click **Save and Test connection**. If the connection to Active Directory is successful, you will see the message: "Successfully connected to Active Directory <AD name >".
TMS Services	

Sections and fields	Description
Scan SNMP Capable Systems to Allow Quick Discovery of Inaccessibility	When this is set to *On*, Cisco TMS will regularly poll all SNMP-capable systems to check that they are accessible. The frequency is set in the field below.
System Alive-Status Scan Interval (in seconds)	Specify how frequently in seconds Cisco TMS will poll SNMP-capable systems for Alive-Status.
Maximum Number of Missed SNMP Responses Before System Is Set to Inaccessible	Specifies the number of consecutive SNMP requests a system can fail to respond to before the system's connection status is set to *No SNMP Response*. After this number of missed responses, Cisco TMS attempts a full connect to the system via HTTP before changing the connection status to *No SNMP Response*. **Note:** As SNMP is a UDP protocol, packet delivery is not guaranteed. In a network with high packet loss, this field should be set higher than the default (which is 2).
System Force Refresh Interval (in hours)	Control how often Cisco TMS updates itself with managed systems' configuration. The parameter set is the minimum time (in hours) between each Database Scanner service scan of the systems in Cisco TMS. Updated configuration is written to the Cisco TMS database. When **Administrative tools > Configuration > Network settings > TMS Services >Enforce Management Settings on Systems** is set to *Yes*, Cisco TMS will enforce management settings on the managed systems at the same time.
SNMP Broadcast Interval (in minutes)	Specify how many minutes Cisco TMS will wait between successive SNMP scans. Cisco TMS sends an SNMP request to the specified Broadcast/Multicast addresses to detect new systems on the network. Based on the response from systems in the network, **System Status** and **Call Status** are updated for all currently managed systems.
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: it sends a broadcast to the IP address "255.255.255.255". Change this value if you wish to narrow the broadcast range. If, for example, you set the address to "10.0.255.255", the TMS SNMP service will receive responses from systems connected to the "10.0" subnet. Use comma separation to scan multiple ranges.
Enforce Management Settings on Systems	When enabled this will set the address systems use for phone books and feedback to the Cisco TMS server address configured in the **Advanced Network Settings for Systems on Internal LAN** section below. This will happen at the frequency set in **Administrative tools > Configuration>Network settings > TMS Services >System Force Refresh Interval (in hours)**. The **Daylight Saving Time** and **Time Zone** for the system will also be corrected. This has the same effect as clicking **Enforce Management Settings** at the bottom of the **System > Navigator >** Select system **> Settings tab > Edit Settings** page. For more information, see the Navigator [p.79].
Enforce Now	Clicking this button will enforce the management settings mentioned above immediately.

Sections and fields	Description
Enable Ad Hoc Conference Discovery	If set to *Yes*, Cisco TMS will discover and monitor ad hoc calls for systems registered in Cisco TMS, and they will be viewable in Conference Control Center [p.182]. 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, set this to either *No* or *Only for MCUs*.
Update System Connectivity for Systems	Specify whether Cisco TMS will change a system's connectivity status (for example: *Reachable on LAN*, *Behind Firewall*) if it detects that this has changed. ▪ *Automatic*: Cisco TMS will change the system's connectivity status as it detects it. ▪ *Manual*: Cisco TMS will not change any system's connectivity status. If set to *Manual*, administrators will have to change a system's connectivity status themselves by going to **Systems > Navigator >** select a system **> Connection** tab **> System Connectivity**.
Advanced Network Settings for Systems on Internal LAN	
TMS Server IPv4 Address	The local IPv4 address of the Cisco TMS Server. For direct-managed systems this address is used as the trap host address, phone book server address, external manager address and external services address on systems that do not support DNS and that are using IPv4 on the same LAN as the Cisco TMS server. For TMSPE-provisioned and Unified CM-registered systems this address is used as the 'feedback 3' address. By default this value is set to the local IPv4 address of the Cisco TMS server.
TMS Server IPv6 Address	The local IPv6 address of the Cisco TMS Server. For direct-managed systems this address is used as the trap host address, phone book server address, external manager address and external services address on systems that do not support DNS and that are using IPv4 on the same LAN as the Cisco TMS server. For TMSPE-provisioned and Unified CM-registered systems this address is used as the 'feedback 3' address. By default this value is set to the local IPv6 address of the Cisco TMS server.
TMS Server Fully Qualified Hostname	The fully qualified hostname of the Cisco TMS Server. For direct-managed systems this address is used as the trap host address, phone book server address, external manager address and external services address on systems that do not support DNS and that are using IPv4 on the same LAN as the Cisco TMS server. For TMSPE-provisioned and Unified CM-registered systems this address is used as the 'feedback 3' address. **Note:** When using both IPv4 and IPv6 in a network, the hostname of Cisco TMS must be reachable from both.
Advanced Network Settings for Systems on Public Internet/Behind Firewall	

Sections and fields	Description
TMS Server Address (Fully Qualified Hostname or IPv4 Address)	The public address of the Cisco TMS Server. This address is used as the trap host address, phone book server address, external manager address and external services address on remote systems. Make sure this field contains an address that remote systems can reach.
Automatic Software Update	
Automatically Check for Updates	If set to *Yes*, Cisco TMS will check cisco.com every 2 days to see if there are new software updates available for all the registered Cisco systems. If so, the software and corresponding release keys are downloaded to the location specified **in Administrative Tools > General Settings > Software FTP Directory** (set in **TMS Tools**). **Note:** When setting **Automatically Check for Updates** to *No*, the buttons **Generate log**, **Import Log** and **Import Excel** will be available on the **System Upgrade** page, to enable import of a list of software and release keys to be used for upgrade of systems. For more detail, see System Upgrade [p.138].
Service URL	This is the URL of the software update service at cisco.com and should 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 for Cisco TMS to use to authenticate to the proxy server.
Web Proxy Password	A valid password for Cisco TMS to use to authenticate to the proxy server.
Secure-Only Device Communication	
Secure-Only Device Communication	If set to *On*, Cisco TMS will communicate using HTTPS only with systems that support this capability. When **Secure-Only Device Communication** is set to *On*, HTTPS must be enabled on your systems.
Validate Certificates	When this box is ticked, Cisco TMS will check that all systems that contact it (to access the corporate phone book or give feedback) have a trusted valid signed certificate.

Email Settings

In Cisco TMS: **Administrative Tools > Email Settings**

Field	Description
Enable Sending of Email	Allow Cisco TMS to send emails to users.
Email Content Type	Choose whether emails will be sent as: ■ *Plain Text* ■ *HTML* ■ *Both (Multipart)*
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.

Field	Description
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.
Base URL for Icons:	Location for images used in HTML emails
SIP Protocol Handler:	The value that identifies which application should open SIP URI links

Edit Email Templates

In Cisco TMS: **Administrative Tools >Configuration > Edit Email Templates**

Use this page to change the layout and text for all email templates in Cisco TMS. Each template has a plain text and an HTML version which you can edit.

The **Edit** section contains:

- The email template layout in HTML or TXT format, which contains tags described below.
- The phrase file where you can alter the text for tags for each language.

When editing email templates, you can:

- Click **Refresh** in the **Preview** section to see how the message will look.
- Click **Discard Changes** to discard your unsaved changes.
- Click **Revert to Default** to reset the edited template/phrase file back to the default.

Explanation of tags

- {...} Curly brackets indicate a phrase tag that you can add to the phrase file and the template.
- <...> Angle brackets indicate a tag that can only be moved or removed from templates; you cannot create new tags of this type.

Note: If you want HTML characters such as angle brackets to be visible in the e-mail, you must use HTML character encoding. Example: use `&gt;` when you want to show `>`.

These are all the tags that can be used in the booking email templates:

Booking Invite

Sections and values

Tag	Description
<FOREACH:API_ERROR>	Display errors requested via the Cisco TMS Booking API (Cisco TMSBA).
<VAL:API_ERROR>	Error message that can be inserted by the Cisco TMSBA.

Tag	Description
<SECTION:MEETING_WEBCONF_ERROR>	Placeholder for errors generated when booking WebEx.
<VAL:MEETING_WEBCONF_ERROR>	WebEx meeting error reference.
<SECTION:MEETING_WEBCONF_WARNING>	WebEx meeting warning reference.
<VAL:MEETING_WEBCONF_WARNING>	WebEx meeting warning reference.
<FOREACH:API_WARNING>	Display warnings requested via the Cisco TMSBA.
<VAL:API_WARNING>	Warning message that can be inserted by Cisco TMSBA.
<SECTION:MAIL_HEADING_MCU_FAILOVER>	If the conference has had to failover to a new MCU, new dial in/dial out details will be provided here for the new MCU.
<SECTION:MUST_BE_APPROVED>	If the user does not have rights to make a booking it can be requested and then approved by an administrator.
<FOREACH:API_INFO>	Info added from the Cisco TMSBA.
<VAL:API_INFO>	Info message that can be inserted by Cisco TMSBA.
<SECTION:RESERVATION_ONLY>	If the meeting is Reservation Only.
<SECTION:BOOKEDBYOWNER>	The name of the conference owner.
<VAL:OWNER>	The user the meeting was booked by.
<SECTION:BOOKEDONBEHALF>	If the meeting was booked on behalf of somebody.
<VAL:BOOKED_BY>	The user the meeting was booked by.
<SECTION:MEETING_TITLE>	If the meeting has a title.
<VAL:MEETING_TITLE>	The conference meeting title.
<SECTION:RECURRENCE_ICON>	If the conference is recurring show an icon.
<SECTION:RECURRENCE_INFO>	If the conference is recurring show the recurrence pattern.
<VAL:RECURRENCE_INFO>	Gives a human readable sentence representing the recurrence.
<VAL:MEETING_DATE_TIME>	Conference date and time.
<VAL:MEETING_TIME_ZONE>	Conference time zone.
<SECTION:MEETING_RECORDING>	If the conference includes recording.
<VAL:RECORDING_URL>	The URL to connect to the Recording Server page for the conference. This will show the recording after the conference and will also offer live streaming if the Recording Server is configured to do so.
<SECTION:MEETING_MESSAGE>	If there is a conference message.
<VAL:MEETING_MESSAGE>	The message entered in **Booking > New Conference > Conference Information**.
<SECTION:NO_MEETING_MESSAGE>	If there is no conference message.

Tag	Description
<SECTION:MEETING_WEBCONF_DETAILS>	If the conference includes WebEx.
<VAL:ATTENDANT_URL>	The URL to join a WebEx conference as a participant (as opposed to host).
<SECTION:WEBCONF_PASSWORD>	If the WebEx password should be shown.
<VAL:WEBCONF_PASSWORD>	The WebEx password.
<SECTION:WEBCONF_HIDDEN_PASSWORD>	If the WebEx password should not be shown.
<VAL:WEBCONF_ID>	The WebEx conference number, this can be entered on your WebEx site to find the conference if you don't click the link in the email.
<SECTION:TELEPRESENCE>	If the conference includes TelePresence.
<SECTION:TP_ONLY_TITLE>	If it is a TelePresence only conference .
<SECTION:TP_COMBINED_TITLE>	If it is a WebEx and TelePresence conference .
<SECTION:VIDEO_ADDRESS>	If there is at least one video address.
<SECTION:VIDEO_ADDRESS_TITLE>	If there is only one protocol.
<FOREACH:VIDEO_ADDRESS_PROTOCOL>	Repeated for every available protocol.
<SECTION:PROTOCOL>	If there is more than one protocol.
<VAL:PROTOCOL>	The connection protocol: H.323, SIP ... This is repeated for each dial in number.
<FOREACH:ZONE>	Repeated for every TMS zone used in a video address.
<SECTION:ZONE>	If there is more than one zone.
<VAL:ZONE>	Repeated for each dial in number, the zone for the MCU/endpoint that the number is dialing into.
<FOREACH:VIDEO_ADDRESS>	Repeated for every video address.
<VAL:VIDEO_ADDRESS>	Repeated for each dial in number: the address for that number.
<SECTION:MEETING_CONFERENCEME>	If there is ConferenceMe.
<VAL:CONFERENCEME_URL>	The URL to reach the conference on Cisco MCU's ConferenceMe.
<SECTION:MEETING_CONFERENCESTREAMING>	Conference streaming details for Cisco MCU.
<VAL:CONFERENCESTREAMING_URL>	The URL to reach the conference using the web-based streaming client on Cisco MCUs.
<SECTION:MEETING_PASSWORD>	If the conference has a password.
<VAL:MEETING_PASSWORD>	The conference password.
<SECTION:LOCATIONS>	If telepresence endpoints are scheduled.
<FOREACH:LOCATION>	Repeated for every telepresence endpoint scheduled.

Tag	Description
<VAL:LOCATION>	Telepresence endpoints are viewed as locations you can go to if you want to join the conference . For a conference including a Cisco TMS-managed system and 4 dial ins, the Cisco TMS-managed system would be a location.
<SECTION:WEBEX_AUDIO>	If the conference includes WebEx.
<SECTION:WEBCONF_LOCAL_CALL_IN_TOLL_NUMBER>	If the country has a local call in toll number.
<VAL:WEBCONF_LOCAL_CALL_IN_TOLL_NUMBER>	WebEx conference reference.
<SECTION:WEBCONF_LOCAL_CALL_IN_TOLL_FREE_NUMBER>	If the country has a local call in toll-free number.
<VAL:WEBCONF_LOCAL_CALL_IN_TOLL_FREE_NUMBER>	WebEx conference reference.
<VAL:WEBCONF_ID>	WebEx conference reference.
<SECTION:WEBCONF_GLOBAL_CALL_IN_NUMBER_URL>	If the WebEx conference has a global call in URL.
<VAL:WEBCONF_GLOBAL_CALL_IN_NUMBER_URL>	WebEx conference reference.
<SECTION:WEBCONF_TOLL_FREE_RESTRICTIONS_LINK>	WebEx conference reference.
<SECTION_WEBEX_HELP>	If the conference includes WebEx.
<SECTION:TMS_CONFERENCE_URL>	If the Cisco TMS address is configured.
<VAL:TMS_CONFERENCE_URL>	The URL of conference details in Cisco TMS.
<SECTION:MEETING_RECORDING_FOOTER>	If the conference includes recording.
<VAL:RECORDING_URL>	The URL of the recording.
<SECTION:WEBEX_NOTICE>	The disclaimer every WebEx conference must include stating that participants could be recorded for example.
<ADD:ICALENDAR_ATTACHMENT>	Adds an Icalender attachment to the mail.

Legacy sections and values

The following legacy sections and values remain supported:

Tag	Description
<SECTION:MEETING_WARNING>	If the conference has a WebEx error.
<VAL:MEETING_WARNING>	The warning will always be: "WebEx could not be booked".
<SECTION:MAIL_HEADING>	If there is no MCU failover.
<VAL:MEETING_ID>	The conference ID.
<SECTION:NUMERIC_ID>	If the conference includes Cisco TelePresence MCUs.

Tag	Description
<VAL:NUMERIC_ID>	Numeric ID for the conference on the Cisco MCU.
<VAL:MEETING_DATE>	Date format: StartDate - EndDate.
<VAL:MEETING_TIME>	Time format: StartTime - EndTime, TimeZone.
<SECTION:MEETING_TYPE>	If the conference has a type: (Automatic Connect, One Button to Push, Manual Connect, No Connect, Reservation).
<VAL:MEETING_TYPE>	The conference type (see above).
<VAL:OWNERLASTNAME>	The conference owner's last name.
<VAL:OWNERFIRSTNAME>	The conference owner's first name.
<VAL:OWNERUSERNAME>	The conference owner's Cisco TMS username.
<SECTION:MEETING_VCMASTER>	If the conference has a Video Conference master.
<VAL:MEETING_VCMASTER>	The Video Conference master.
<SECTION:MEETING_REFERENCE>	If the conference has a reference.
<SECTION:REFERENCE_NAME>	The reference name.
<VAL:REFERENCE_NAME>	Reference information if a reference was configured during booking.
<SECTION:REFERENCE_CODE>	If the reference includes a code.
<VAL:REFERENCE_CODE>	Reference information if a reference was configured during booking.
<SECTION:REFERENCE_COMMENT>	If the reference includes a comment.
<VAL:REFERENCE_COMMENT>	Reference information if a reference was configured during booking.
<SECTION:REFERENCE_CONTACT>	If the reference includes a contact.
<VAL:REFERENCE_CONTACT>	Reference information if a reference was configured during booking.
<SECTION:NO_CONNECT>	If the conference type is No Connect.
<FOREACH:PARTICIPANT>	Repeated for every participant (grouped by name).
<VAL:PARTICIPANT_NAME>	Particpant = video system, external dial in, phonebook entry, the name as stored in Cisco TMS.
<SECTION:PARTICIPANT_NUMBERS>	If the participants have dial in numbers.
<VAL:PARTICIPANT_NUMBERS>	The dial in number for the participant.
<SECTION:PARTICIPANT_TIME>	In a section because not every participant has a time zone for example, an external dial in/out.
<VAL:PARTICIPANT_TIME>	The relative time for this user: the conference time in their time zone.
<SECTION:CALL_ROUTE>	If the conference has a route.
<SECTION:OBTP_ROUTE_DETAIL>	If the conference is One Button To Push.
<FOREACH:PAIR>	Repeated for every route pair (grouped).
<VAL:PAIR_FROMNAME>	The name of the endpoint doing the dialing.

Tag	Description
<SECTION:PAIR_MANUALCALL>	If this is a One Button To Push conference and the participant does not support it.
<VAL:PAIR_TONAME>	The name of the endpoint being dialed.
<VAL:PAIR_CONNECTNUMBER>	The number that "from" will dial to reach "to".
<SECTION:MEETING_WEBCONF>	Only included if there is WebEx in the conference.
<VAL:WEBCONF_TYPE>	WebEx conference reference.
<VAL:WEBCONF_HOST_KEY>	The WebEx host key, required to start the conference as organizer.
<VAL:PRESENTER_URL>	The URL to join the conference as organizer.

Booking Cancel

Sections and Values

Tag	Description
<SECTION:MEETING_TITLE>	If the conference has a title.
<VAL:MEETING_TITLE>	The conference title.
<VAL:MEETING_DATE_TIME>	The date and time of the conference.
<VAL:MEETING_TIME_ZONE>	The conference time zone.
<VAL:OWNER>	The owner of the conference.

Legacy sections and values

Tag	Description
<VAL:MEETING_ID>	The conference title.
<VAL:MEETING_DATE>	The conference date.
<VAL:MEETING_TIME>	The conference start time and duration.
<VAL:OWNERLASTNAME>	The conference owner's last name.
<VAL:OWNERFIRSTNAME>	The conference owner's first name.
<VAL:OWNERUSERNAME>	The conference owner's username.
<VAL:DELETED_BY_LASTNAME>	Conference deleted by - lastname.
<VAL:DELETED_BY_FIRSTNAME>	Conference deleted by - firstname.
<VAL:DELETED_BY_USERNAME>	Conference deleted by - username.

Booking Event

Sections and values

Tag	Description
<SECTION:ERROR>	This mail is used by the Cisco TMS Booking API (Cisco TMSBA) and provides an e-mail with the Cisco TMS email template layout with specific messages inserted by the Cisco TMSBA. This can include errors, warnings or information.
<VAL:MESSAGE>	Message specified by Cisco TMSBA.
<SECTION:WARNING>	Message specified by Cisco TMSBA.
<VAL:MESSAGE>	Message specified by Cisco TMSBA.
<SECTION:INFO>	Message specified by Cisco TMSBA.
<VAL:MESSAGE>	Message specified by Cisco TMSBA.
<SECTION:MEETING_TITLE>	The conference title.
<VAL:MEETING_TITLE>	The conference title.
<VAL:MEETING_DATE_TIME>	The conference date and start time.
<VAL:MEETING_TIME_ZONE>	The conference time zone.
<SECTION:HOST>	The user that booked the conference.
<VAL:HOST>	The user that booked the conference.
<SECTION:ADMINISTRATOR>	The Cisco TMS contact person - not included if this is not configured in Cisco TMS.
<VAL:ADMINISTRATOR>	The Cisco TMS contact person - not included if this is not configured in Cisco TMS.
<VAL:EMAIL>	The Cisco TMS contact person's email address.

Conference Settings

In Cisco TMS: **Administrative Tools > Configuration > Conference Settings**

On this page you can specify settings which will apply to all scheduled conferences in Cisco TMS as default. Changes can be made to individual conference settings during booking.

Conference display options

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 create options

Field	Description
Default Conference Title	The default title used for all booked/scheduled meetings. The title can also be edited in the Booking/Scheduling wizard. By default this is set to *Scheduled Meeting*. 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 or TS systems). 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 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.
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 rooms 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 to *On* on the endpoint, and this setting will persist after the conference has ended, until set to *Off* on the endpoint itself.

Field	Description
Extend Scheduled Meetings Mode	■ *Off*: Ensure that meetings are never automatically extended . ■ *Endpoint Prompt*: Display a non-configurable Extend Meeting message on the VC 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 extension will only happen if there is at least 1 participant still connected, and there are no conflicting meetings for any of the participants or the MCU within the next 15 minutes.
Auto Generate Password on New Conferences	Specify that you want Cisco TMS to auto-generate a conference password/PIN for scheduled calls.
Auto Generated Password Length	Specify the number of digits Cisco TMS will include when auto-generating a conference password/PIN.
Billing Code for Scheduled Calls	Specify whether billing codes are required for scheduled calls. The options here are: ■ *No* ■ *Optional* ■ *Required*: Users will not be able to schedule a call without entering a valid billing code. See Billing Codes [p.275].
Enable Billing Code Selection Popup	■ *Yes*: A button will be displayed next to the field **Billing Code** in **Booking > New Conference > Advanced Settings**. Clicking on the button will open 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 Setup Buffer (in minutes)	Specify the amount of time before the scheduled start time that a conference will be set up, and the time that it will continue to run after the scheduled end time. Change the default setup buffer from zero to your preferred value.
Default Tear Down Buffer (in minutes)	**CAUTION:** Do not enable setup and teardown buffers if using Smart Scheduler, Cisco TMSXE, or any other application that makes use of the Cisco TelePresence Management Suite Extension Booking API, as the API does not support these buffers.
Conference Connection/Ending Options	
Connection Attempts for Scheduled Calls	The number of times Cisco TMS will keep trying to connect if a call is not initially successful. The number of allocation attempts (how many times Cisco TMS will attempt to allocate the call on the bridge) will also follow the number set here.
Connection Timeout for Scheduled Calls	The number of seconds to wait for a successful connection. If a system does not connect within this time, the call will be disconnected and retried the number of times set in **Connection Attempts for Scheduled Calls**.

Field	Description
Participant Connection State During Setup Buffer	Specify which participants will be connected automatically to the conference before it starts. The alternatives are: ■ *Connect no participants during buffer* ■ *Connect all non-recording participants during buffer* ■ *Connect all participants during buffer*
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.
Message Timeout	The default time (in seconds) that a message should be shown on an endpoint.
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 (Non Master) 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.
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.

Field	Description
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 Conference Options	
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 select as default when creating a conference. When booking Immersive TelePresence conferences, a Cisco TelePresence Server will always be preferred by Cisco TMS (if enough resource is available) regardless of the setting here.
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.

Field	Description
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 by a TelePresence Conductor. **Note:** Automatic MCU Failover is only supported for scheduled, non-cascaded MCU conferences.
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 Settings

In Cisco TMS: **Administrative Tools > Configuration > WebEx Settings**

This is where you configure the settings for the WebEx sites.

WebEx site and user credentials

For each user to be able to use WebEx in telepresence conferences, **WebEx Site**, **WebEx Username** and **WebEx Password** must be entered in Cisco TMS.

There are two alternative ways to enter this information:

- Using Single Sign On.
- Entering the information manually.

Using Single Sign On

The Cisco TMS administrator can either have the WebEx username imported from Active Directory or manually enter this on behalf of the users. When using Single Sign On, the WebEx password is not required.

To enable SSO, see Setting up WebEx Single Sign On [p.33]

Not using Single Sign On

If SSO is not used, each user must enter this information manually. Go to the personal information page, click the link in the lower left corner of Cisco TMS and enter:

- **WebEx site**.
- **WebEx Username**.
- **WebEx Password**.

WebEx Configuration

Field	Description
Enable WebEx	*Yes*: Conferences can be booked with Webex. *No*: Conferences cannot include Webex.
Add WebEx to All Conferences	*Yes*: All conferences will be booked with WebEx. In the booking pages Include WebEx Conference check box will by default be checked, but can be cleared. *No*: This check box 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 [p.37]. The AD attribute used to look up the WebEx username must correspond to the username in WebEx. *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

Column	Description
Site Name	Displays the name of the WebEx site.
Hostname	Displays the name of the host server for the WebEx site above.
Default Site	A green check mark indicates if this is 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

In the **WebEx Settings** page, click the **Add Site** button to display this page.

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.

Field	Description
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*: Set to *Yes* 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). By setting this to *Yes*, the audio line used will not be encrypted. *No*: SIP will be used for both video and audio.
Use Web Proxy	*Yes*: Set to *Yes* if your network uses a web proxy to exit the intranet. When selecting *Yes* a **Web Proxy Configuration** will be displayed with three fields: ■ **Web Proxy Address** where **Web Proxy Address**is mandatory. ■ **Web Proxy Username** ■ **Web Proxy Password** *No*: WebEx can be reached without using a proxy.
Enable SSO	To enable Single Sign On, see Setting up WebEx Single Sign On [p.33] *Yes*: Set to *Yes* if your network uses SSO. No: Your network does not use SSO.
Connection Status	This field displays the status of the connection between Cisco TMS and the WebEx site.

SSO Configuration

Field	Description
Certificate	This field displays the certificate that ensures safe transfer of data between Cisco TMS and WebEx during Single Sign On. This certificate must be sent to the WebEx administrator to set up the trust relationship between Cisco TMS and WebEx.
Upload Certificate	Browse to upload certificate. To create certificates, see Setting up WebEx Single Sign On [p.33].
Certificate Password	Password provided by WebEx.
Partner Name	This value must be determined or approved by the WebEx team, because it must be unique among all WebEx customers. Usually it is the name of the company deploying WebEx Enabled TelePresence. Value provided by WebEx.
Partner Issuer (IdP ID)	This is the Identity Provider. This value is normally determined by the Cisco TMS administrator, because the Identity Provider is Cisco TMS. Value provided by WebEx.

Field	Description
SAML Issuer (SP ID)	This is the Service Provider. This value is normally determined by WebEx, because the Service Provider is WebEx. Value provided by WebEx.
AuthContextClassRef	This is the authentication context. The IdP authenticates the user in different contexts, e.g., X509 cert, Smart card, IWA, username/password). Value provided by WebEx.

Statistics Settings

In Cisco TMS: **Administrative Tools > Configuration > Statistics Settings**

On this page you define general settings used by the statistics found in Reporting [p.215].

Field	Description
Statistics History (in days)	Set the default date range used for statistics. Only data for the last Statistics History days will be shown by default.
Disable Statistics Report	Setting to *Yes* disables the **Reporting** tab where statistics can be exported to PDF. This will speed up the reporting pages.
Statistics ROI Average System Cost	The average investment cost for a video system, used in the calculator for Return on Investment [p.229].
Statistics ROI Average Travelling Cost	The average cost of a business trip.
Statistics ROI/CO_2 Average Number of Participants per Endpoint	The average number of participants joining a video conference at each endpoint.
Statistics ROI/CO_2 Minimum Call Duration	Select a minimum duration in seconds for calls used in ROI statistics. All calls below this limit will be ignored by the ROI statistics.
Statistics CO_2 Cost Per Travel Per person (kg CO_2)	The average CO_2 cost of a business trip.
Statistics Default Start Time	The default start time for statistics.
Statistics 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*.

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

Field	Description
Sender Address	The email address 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.
Send Automatically on User Import	Specify whether account information should be automatically emailed to new users upon import from Active Directory. The default setting is *No*.

User 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*

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

Field	Description
HTTPS	Set to *Yes* for secure communication with Cisco TMS.
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

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

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 [p.124] for more information.

Description of ticket errors

Ticket error	Description
Accepts ISDN Calls but no Bandwidth	The system is set up to accept ISDN calls or telephone calls but there is no ISDN Bandwidth available.
Active Gatekeeper Address Blank	The gatekeeper settings are configured incorrectly. The active gatekeeper address is blank.
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.
CTS Native Interop Call Routing is Enabled but Organization Top Level Domain is Not Set	When Cisco CTS Native Interop Call Routing is enabled in Cisco TMS and Organization Top Level Domain is not set in Unified CM, Cisco TMS may be unable to schedule or receive feedback about calls involving systems managed by Unified CM.
Default Alias Is Fixed	You have set a Cisco TelePresence Conductor alias which does not have a variable part, which means you can only book one conference at a time.
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.
FTP Configuration Error	There is a problem with the FTP communication between Cisco TMS and the system.
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.
Gatekeeper Registration Problem	No valid service prefix is set.
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 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 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.
Low Max Participants on Service	Applies only to Radvision MCUs. The number of maximum participants for service is low.
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.
Missing Option Key(s)	This system is a cluster peer and its option keys do not match the master's option keys. To ensure that the configuration replication is successful, all cluster peers must have the same option keys.
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 Default Alias Configured	You have not configured a default Cisco TelePresence Conductor Alias.
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	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	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	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	There are no reserved Cisco TMS-archiving lines defined for Cisco TMS to use.
No TMS-transcoding Lines defined	There are no reserved Cisco TMS-transcoding lines defined for Cisco TMS to use.

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.
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.
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 Cisco Unified CM-registered systems. Cisco 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 Cisco 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.

System(s) Managed by Cisco TelePresence Conductor 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.
The System's Unified CM Is Not Available	Applies to Cisco Unified CM-registered systems. The Cisco Unified CM this system is registered to is not available.
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**

On the **User Administration** pages Cisco TMS 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 [p.270]) 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 [p.268].

Groups

In Cisco TMS: **Administrative Tools > User Administration > Groups**

On this page you can manage groups and their permissions for pages and functionality.

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 Groups** are described above. They cannot be removed.
- **AD Groups** 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:
     i. Go to the **Group members** tab
     ii. Select the user(s) you want to remove from the group.
     iii. Click **Remove** button.
   - To add members:
     i. Go to the **Add members** tab
     ii. Select the user(s) you want to add to the group.
     iii. 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

Page/feature	Permission	Action available to group
Portal	**Read**	Access the page.
Sitemap	**Read**	Access the page.

Booking

Page/feature	Permission	Action available to group
List Conferences -- All	*Read*	See meetings for all users in the **List Conferences** page. Use this setting to limit read access for conference information in **Free/busy Overview**, **Ad hoc Booking**, **Add Participant** availability table and similar situations.
	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*	See own meetings only in the **List Conferences** page.
	Update	Create, edit and delete own meetings only in the **List Conferences** page.
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*	Access the page.
	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.
	Book on behalf of	Book on behalf of other users.
	New Conference Page	Book meetings in the **New Conference** page.
	Free Busy Page	Read access to the **Free/busy** page.

Monitoring

Page/feature		
Misc	*Conference Control Center*	Access the page.
	Graphical Monitor	Access the page.
	Map Monitor	Access the page.
	Update Map Monitor	Access the page.

Systems

Page/feature	Permission	Action available to group
Navigator	*Read*	Access the page.
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.
Network 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

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 [p.203].
	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

Page/feature	Permission	Description
Reporting	*Call Detail Record*	Access the page.
	Conference Statistics	Access the page.
	Network Statistics	Access the page.
	Return On Investment	Access the page.
	System Statistics	Access the page.
	Billing Codes	Access the page.

Administrative Tools

Page/feature	Permission	Description
Configuration	*Read*	Access the page.
	Update	Edit configurations.

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 users.
	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 permission levels, that is, which group the user belongs to.

Adding a new user

If you need to add new users:

1. Click **New**.
2. Enter user contact information.
3. Click **Save** when all the requested information has been provided.

Deleting a user

1. Select the check box next to the user
2. Click the **Delete** button.

Updating from Active Directory

The button **Update from AD** in the user details page is only available if you are using Active Directory lookup. Click the button to get updated information about the selected user from Active Directory.

Synchronize all users with AD

To update information on all users, click **Synchronize all user with AD** on the **Users** page. Cisco TMS will use AD to update information on all Cisco TMS users. Users removed from AD will also be deleted in Cisco TMS.

Note that:

- The first time you log on to Cisco TMS, the **Username** parameter is retrieved from Active Directory, provided that the parameters in the **Active Directory** group have been configured in **Administrative Tools > Configuration > Network Settings**, see Network Settings [p.234]. Cisco TMS will also detect new 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.
- Synchronizing all users with AD can be done automatically. Go to **Administrative tools > Configuration > Network Settings > Active Directory** section, **AD synchronization schedule** fields.

To view the settings for a user, click on the name in the grid, or click on the marked area and select **View** from the drop down menu. You will see details like name, email address, Windows username, which groups and type of groups the user belongs to and so on. A complete list is shown in the table below.

Editing user settings

Choose **Edit** from the drop down menu for a user in the Users page or click on **Edit** when viewing a user's settings. The table below explains all available settings for a Cisco TMS user.

Note that some of these settings (for example **First Name**, **Last Name**, and **Email Address**) will be read only if Active Directory lookup is enabled and the user being edited can be found in Active Directory.

Field	Description
Windows Username	The user's Windows Username.
First Name (cannot be empty)	The user's first name.
Last Name	The user's last name.
Email Address (cannot be empty)	The email where meeting bookings and event notifications will be sent. The format must be `xxx@yyy.zz`.

Field	Description
Language	Change the language that this user will see in the **User Settings** pop-up window (available to users by clicking on their username in the bottom left of the Cisco TMS web interface). The rest of the Cisco TMS web interface will be in the language selected during installation. English (US) is the default language for Cisco TMS. **Note:** English (US), English (UK) and English (AU) use the same text strings, but different date and time formatting (12 hour clock with AM/PM for the US and AU as opposed to a 24 hour clock for the UK).
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.
WebEx Password	The user's WebEx password.
WebEx Site	The WebEx site the user will use.
SIP URI	The user's SIP address.
Time Zone	This option is used 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	This is the user's IP zone, and is 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.

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 following permissions can be set as system defaults for each user group in Cisco TMS:

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 [p.271].

The permissions on these pages are displayed differently, but map as shown in the table below.

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 [p.122].

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 [p.47].

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:

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.

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:

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.

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.

Sections and fields	Description
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 [p.48].
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	

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**

On this page you can create, edit and delete billing codes, and set them on systems.

Billing codes are used to restrict or monitor the use of systems.

There are two ways to use billing codes:

- Require that a billing code is entered on a system before a call can be made.
- Request a billing code when a call is attempted on a system, but calls can still be made if no billing code is entered.

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.

When a billing code is used, the Call Detail Record (CDR) for the conference will contain the billing code. For more on this, see Billing Code Statistics [p.223].

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.
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 use of a billing code, repeat the selection of systems as described above, and then select **Turn off billing code use.** 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**

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.
- 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**.

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.
- 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**

The **TMS Server Maintenance** page is for general management and housekeeping of the Cisco TMS server. The following fields can be viewed

Database Server Date and Time Settings

Displays time and mismatch in time between the database server and the web server.

TMS Diagnostics

To assist Cisco Technical Support with troubleshooting Cisco TMS related issues, click **Download Log Files** to create and download a diagnostics zip file.

The zip file created will contain the recent Cisco TMS debug log files, an XML file of Cisco TMS's configuration settings and any Cisco TMS related entries found in the Windows application event log.

Database Server Disk space

Displays free disk space for each partition on the database server. For this to work, the OLE Automation Procedures option needs to be enabled. For new SQL Server 2005 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
```

TMS Server Disk space

Displays free disk space for each partition on the web server.

Database Files and Size Info

This section displays information about the database.

Purge Old Data in Database Tables Plan

This section displays information about the database tables used for logs and caching information in Cisco TMS. The overview shows how many entries each table in the database currently has and how many days the entries will be kept before they will be purged automatically.

Click on the **Edit** link and select the check box to enable automatic cleanup.

Enter the number of days for each entry to be kept in the table in the field **Number of Days to Keep Data**.

Table	Description
Endpoint/MCU Call Log	This log contains call detail records for conferences involving endpoints/MCUs.
Gateway/Gatekeeper Call Log	This log contains call detail records for conferences involving gateways/gatekeepers.
Feedback Log	This log contains events and traps from all systems that send events to Cisco TMS. For more information, see the System [p.226] reporting section about traps from systems and **Navigator**. **Note:** For a company with several hundred endpoints, the size of this log file can become substantial, and we recommend that old data be purged regularly.
Scheduled Conference Cache	This table contains temporary information used for conference booking. The Scheduled Conference Cache will always be enabled.
LiveSnapshot	This table contains snapshots of monitored conferences in Cisco TMS.
Audit Log	This log contains the audit log for all Create, Delete and Update actions carried out in Cisco TMS on Systems, Folders, Users, Groups and Cisco TMS. For more information about audit logs in Cisco TMS see Audit Log [p.285].
Packet Loss Log	This log contains the endpoint's loss of packets reported to Cisco TMS.
Scheduler Events	This table contains the 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.
User Call Log	This log contains details for users in conferences listed in the Gateway/GateKeeper Call Log.

Purge Log Plan

Displays information about the log files on the web server

Log file	Description
Web	Debug information about user interaction.
Live Service	Debug information for all conferences.
Polycom Directory	Debug information for Polycom endpoints using Cisco TMS Phone Book.
Scheduler Service	Debug information for the Windows Service TMSSchedulerService that starts background jobs like configuration backup, software upgrades, database re-indexing and so on.
Database scanner	Debug information for the Windows Service TMSDatabaseScannerService that periodically queries the registered systems in Cisco TMS and updates the Cisco TMS database with the systems current configuration and call status.
SNMP Scanner	Debug information for SNMP feedback.
Public Web	Debug information for HTTP feedback from systems, phone books, and so on.
TMS Server Diagnostics Service	Debug/log information from the TMSServerDiagnostics service.

Clicking on **Edit** will allow the user to enable automatic cleanup and manage how long these logs shall be kept.

TMS Services Status

Displays information about all Cisco TMS services which are running towards the Cisco TMS database. For more information, see Windows services [p.17].

Service	Description
TMSLiveService	Controls the setup and control of all conferences in Cisco TMS.
TMSSchedulerService	Controls scheduled events, for example the purging of logs.
TMSPLCMDirectoryService	Controls setting of phone books on Polycom endpoints.
TMSSNMPService	Handles SNMP traps, and scans the network for new systems.
TMSDatabaseScannerService	Periodically queries the registered systems in Cisco TMS and updates the Cisco TMS database with the systems current configuration and call status.
TMSServerDiagnostics	Monitors the health of the Cisco TMS server and verifies that the services are running, that there is enough disc space on the Cisco TMS server and that the size of the database is sufficient. The server creates tickets if any problem arises. The tickets can be found on the TMS Tickets [p.282] page.

Clear List clears the list of services that are not running and the corresponding tickets. Also use this button if you change the name of the server Cisco TMS is running on and you get obsolete services and tickets with the old server name. The list will then be repopulated by services on the new server name.

TMS Tickets

In Cisco TMS: **Administrative Tools > TMS Tickets**

This page shows all open Cisco TMS tickets. Tickets flag information, warnings and error messages. Go to **Manage Ticket Error Levels [p.256]** to define which tickets will be shown on this page.

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 > 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

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.

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*

Before you can view audit logging data, you must go to **Administrative tools > Configuration > General Settings** and set **Enable Auditing** to *Yes*.

You can override this setting by going into **TMS Tools > Advanced Security Settings** and selecting **Auditing Always Enabled**. When this setting is enabled, the **Enable Auditing** option in **General Settings** will be grayed out.

The audit log contains:

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.
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.

You can filter the audit log by specifying:

- **Start Date** and **End Date**
- **User**
- **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 **Administrative Tools > TMS Server Maintenance**.
2. Expand the section **Purge Old Data in Database Tables Plan**.
3. Click **Edit** next to the **Audit Log** field.
4. Edit the **Number of Days to Keep Data** field.
5. Click **Update**.

TMS Tools

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 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 TMS Tools must be made by an experienced Windows and Cisco TMS administrator.

Configuration 288
Security Settings 291
Utilities 293
Diagnostic Tools 294

Configuration

Database Connection Settings

This is where you specify the location of the Cisco TMS or Cisco TMS Provisioning Extension (TMSPE) SQL databases, and the credentials Cisco TMS uses to connect to them.

TMS Database Connection Settings

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 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 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 TMS’s IIS App pool.
   - In Windows 2003 (IIS 6), the default account is NT AUTHORITY\NETWORK SERVICE.
   - In Windows 2008 (IIS 7), the default account is IIS APPPOOL\TMSNet40AppPool.

   You can verify which user account TMS’s IIS App pool runs under by opening TMS’s log-web file; the first entry will say “TMS Version 14.2 (IIS APPPOOL\TMSNet40AppPool)”.
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. Change all six TMS services so that they log on as tms-databaseservice, and restart them.
7. 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 TMS Tools before upgrading Cisco TMS.

Database Settings

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.

Field	Description
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.

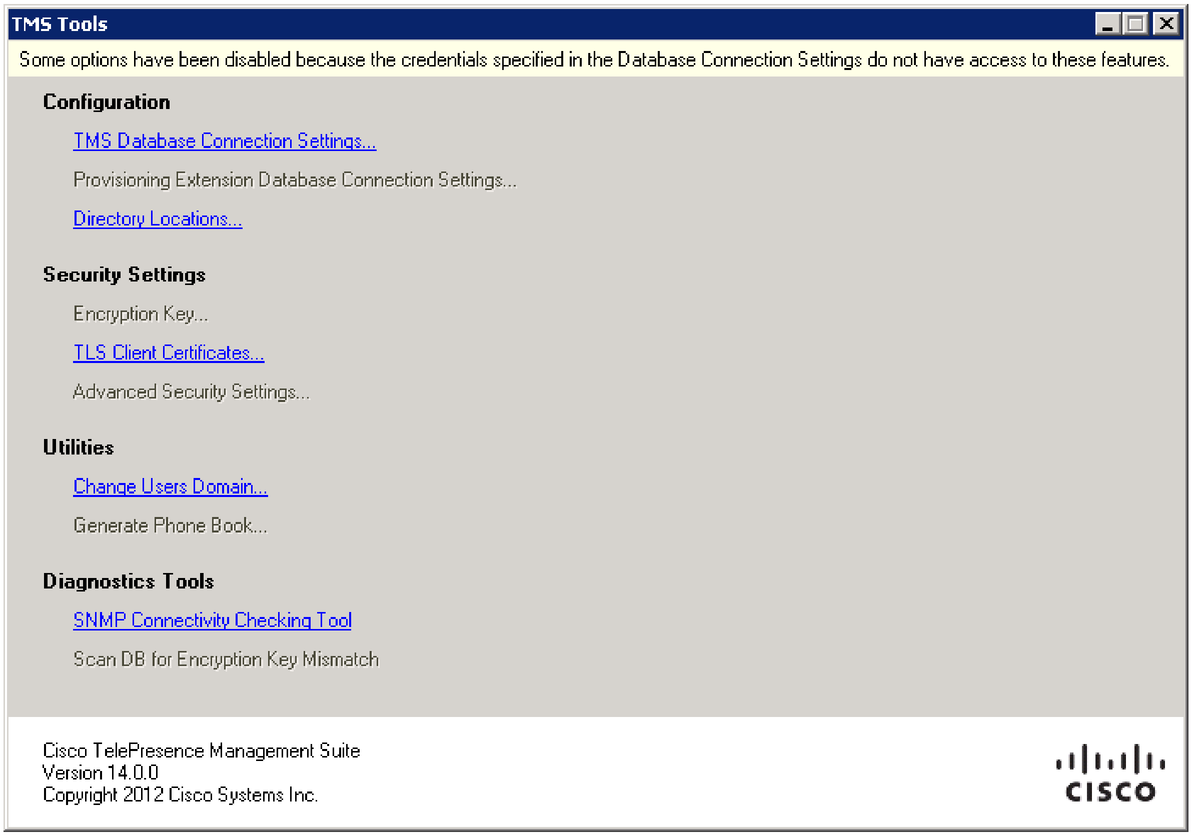
Authentication

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 **TMS Database Connection Settings** to **Windows Authentication** and click **OK**, 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.

The following settings in 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:



TMS Tools

Some options have been disabled because the credentials specified in the Database Connection Settings do not have access to these features.

Configuration

TMS Database Connection Settings...

Provisioning Extension Database Connection Settings...

Directory Locations...

Security Settings

Encryption Key...

TLS Client Certificates...

Advanced Security Settings...

Utilities

Change Users Domain...

Generate Phone Book...

Diagnostics Tools

SNMP Connectivity Checking Tool

Scan DB for Encryption Key Mismatch

Cisco TelePresence Management Suite
Version 14.0.0
Copyright 2012 Cisco Systems Inc.

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.

Provisioning Extension Database Connection Settings

Database 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 is *tmspe* by default. This must be changed here if the database name has been changed in SQL, but we do not recommend changing the database name as you can only upgrade a database with the name **tmspe**. Upgrades attempted on a database which is not called **tmspe** 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 Cisco TMSPE to stop working altogether.

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 FTP Directory

You can specify the location where the software for system upgrades is stored by editing the Software FTP 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 FTP 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 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 (for example, admin and TANDBERG for MXP systems).

TLS Client Certificates

When initiating outbound connections 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 personal 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 TMS Tools has read access to the private keys of the certificates.

You must also ensure that all accounts the TMS services are logged on as have read access to the private keys of the 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.

These settings must only be modified by a Cisco TMS administrator.

Incorrect application of these settings can stop Cisco TMS from working altogether.

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.

Sections and fields	Description
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	
Auditing Always Enabled	■ Ensures that auditing of all actions carried out in the Cisco TMS application is enabled . ■ Overrides the setting under **Administrative Tools > General Settings > Enable Auditing**.
Transport Layer Security Options	
Require Client Certificates for HTTPS API	■ Requires systems to provide a certificate for identity verification when they access the Public IIS folder on the Cisco TMS server (to access the Corporate Phone Book or provide CDR feedback). Cisco TMS will then check the hostname it has for the system against the common name (CN) field in the certificate. ■ Enables and grays out the following settings in **Administrative Tools > Configuration > Network Settings > Secure-Only Device Communication**: ● **Secure-Only Device Communication** ● **Validate Certificates** If disabling this setting after first enabling it, the **Secure-Only Device Communication** section is no longer grayed out, but the settings remain enabled until manually modified. **Note:** You must implement certificate management in your video network before this setting will have any effect.
Enable Certificate Revocation Check	Checks the validity of certificates for all systems which Cisco TMS communicates with, using built-in Windows mechanisms for revocation checks.
Banners	
Banners on Web Pages and Documents	Adds banners to: ■ The Cisco TMS application web site. ■ PDF and Microsoft Excel documents exported from Cisco TMS.

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 [p.194].

1. Open 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.

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 Database 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.
- **Close**: Close the window.

A 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.

Redundant deployments

Cisco TMS supports deployment in a redundant configuration, increasing the availability of the application.

This chapter describes the requirements, configuration, and limitations of deploying Cisco TMS in the two supported redundant scenarios:

- Deployment with a load balancer
- Deploying a hot standby

It is assumed that the reader has an understanding of Cisco TMS, Cisco TMS installation, and Windows Server operating systems, as well as an advanced level of understanding of computer networking and network protocols.

Preliminary information 296
Deploying with a load balancer 297
Deploying a hot standby 305
Database redundancy 309
Example ACE configuration 311
Local files for synchronization 315

Preliminary information

Communication with managed systems

Understanding how Cisco TMS communicates with managed systems is key to understanding Cisco TMS redundancy. For a detailed description see How Cisco TMS communicates with managed systems [p.62].

Supported configurations

For a fully redundant Cisco TMS deployment with an automatic failover process, you must set up two Cisco TMS servers with a network load balancer (NLB) in front. Cisco recommends using a Cisco ACE 4710 Application Control Engine Appliance for load-balancing IP traffic between the two Cisco TMS servers, therefore this document describes how to deploy Cisco TMS with an ACE 4710 appliance.

This chapter also describes how to deploy two Cisco TMS servers using a Hot Standby model.

Regardless of which of the two redundancy models you choose to deploy, no more than two Cisco TMS servers can be used. Deploying more than two Cisco TMS servers in a redundant setup is neither tested nor supported by Cisco.

Deploying two Cisco TMS servers will increase Cisco TMS availability, but will not in any way increase Cisco TMS scalability.

Other models of load balancer with alternative configurations may work with Cisco TMS, but have not been tested by Cisco.

Licensing

Only one live database can be used in a redundant Cisco TMS implementation, therefore both servers will use the same Cisco TMS serial number and the same set of release and option keys.

Database redundancy

Cisco TMS relies heavily on its SQL database, so a fully resilient Cisco TMS solution will also utilize one of the high-availability technologies offered by SQL Server 2008. Thoroughly documenting SQL Server 2008 high-availability alternatives is beyond the scope of this chapter, but the two relevant SQL Server redundancy models are briefly discussed in the Database redundancy [p.309] section along with references to the relevant Microsoft documentation.

Cisco TelePresence Management Suite Provisioning Extension

Implementing Cisco TMSPE in a redundant environment is described in the Cisco TelePresence Management Suite Provisioning Extension Deployment Guide.

Deploying with a load balancer

Configuring two Cisco TMS servers (also referred to as "nodes" in this context) with a network load balancer (NLB) provides a truly redundant Cisco TMS setup with fully automatic fail-over.

This deployment can be combined with a high-availability SQL Server option as discussed in the Database redundancy [p.309] section.

Requests from the systems managed by Cisco TMS pass transparently through the NLB so that the traffic appears to come directly from the managed systems. (See How Cisco TMS communicates with managed systems [p.62].

Recommended hardware

We recommend using the Cisco ACE 4710 Application Control Engine Appliance. The ACE is the only load balancer that has been tested and verified to work with Cisco TMS.

Fully documenting how to set up and manage an ACE appliance is outside the scope of this document, but a sample Cisco TMS-compatible ACE configuration has been included in Example ACE configuration [p.311] for your reference.

(See the Cisco ACE 4700 Series Application Control Engine Appliance documentation for further information.)

Active directory and user authentication requirements

- Both Cisco TMS servers must be members of the same Windows domain.
- All Cisco TMS users must be imported from and authenticated using Active Directory.
- Using local user accounts is not supported for this redundancy model.

Communication with managed systems

When deploying two Cisco TMS servers behind a load balancer such as the Cisco ACE 4710 Application Control Engine Appliance, one virtual IP address must be assigned to the NLB and one IP address assigned to each of the two Cisco TMS servers.

A DNS entry must be created pointing to the NLB's virtual IP address.

The NLB's hostname and IP address(es) must be entered in the fields on the **Network Settings** page in Cisco TMS discussed in The addresses that systems use to contact Cisco TMS [p.62].

See Deploying with a load balancer [p.297] for instructions on implementing this configuration.

Once the IP addresses and hostname values in **Network Settings** have been changed, the Database Scanner service enforces the new network settings on the managed systems. The systems then start directing traffic to the NLB, which forwards the requests to the Cisco TMS servers.

All communication between Cisco TMS and the managed systems will now go through the NLB. This is accomplished by keeping the Cisco TMS servers and the managed systems on different VLANs while the servers use the NLB as their default gateway.

Cisco TMS's logic for determining whether a system is *Reachable on LAN*, *Reachable on Public Internet* or *Behind Firewall* dictates how you set up the load balancer. As it is limiting to have systems in a *Behind*

Firewall status, the load balancer should be configured so that all traffic from managed systems appears to Cisco TMS as coming directly from the managed systems and not from the NLB. Alternatively you can choose to manually set your systems' connectivity status by setting: **Administrative Tools > Configuration > Network Settings > Update System Connectivity for Systems** to *Manual*. However we recommend leaving this setting as *Automatic*, rather than managing system connectivity manually.

Architectural overview and network diagram

Example configuration

In the example below the following values are used:

Table 1: VLAN200

Device	IP address	Hostname
ACE Virtual IP	10.0.200.40	tms.example.com
tms01	10.0.200.50	tms01.example.com
tms02	10.0.200.60	tms02.example.com
SQL Server	10.0.200.70	sql01.example.com

Table 2: VLAN100

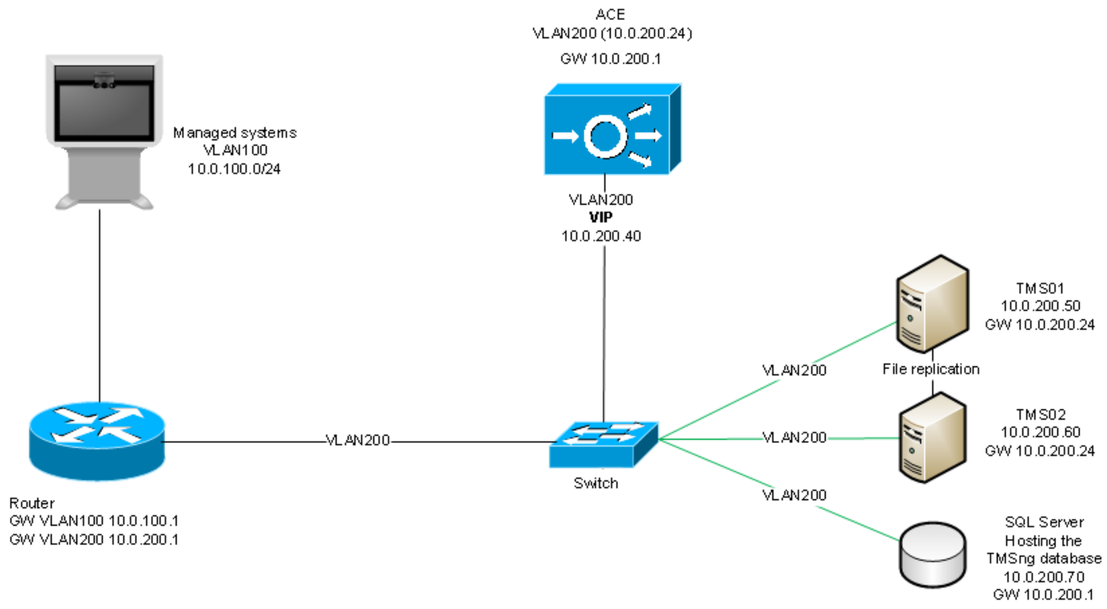
Device	IP address	Hostname
Managed systems and users	10.0.100.0/24	

- There are two Virtual LANs, VLAN200 and VLAN100.
- The ACE is configured on VLAN200.
- The two Cisco TMS servers (tms01 at 10.0.200.50 and tms02 at 10.0.200.60) are configured on VLAN200.
- All clients (managed systems and users) are configured on VLAN100. Clients must not be on the same VLAN as the load balanced Cisco TMS servers.
- All traffic to the virtual IP address of the ACE is forwarded to one of the two Cisco TMS servers.
- All managed systems and users use the ACE’s virtual IP address when communicating with Cisco TMS.
- The default gateway of both Cisco TMS servers is set to the ACE’s IP address on VLAN200 to ensure that all traffic to and from Cisco TMS is load balanced.

Database

- The two Cisco TMS servers share a common, external tmsng database.
- As both Cisco TMS servers simultaneously read and write data to the database the server hosting SQL Server needs more powerful hardware than if it only served one Cisco TMS server.
- The database server talks directly to the Cisco TMS servers, bypassing the ACE load balancer.

Transparent Source Network Address Translation



Installing and configuring

Installing Cisco TMS on tms01

1. Prior to installing Cisco TMS, set up an SQL Server instance on an external server.
2. Install Cisco TMS on the first node, using the instructions provided in the Cisco TelePresence Management Suite Installation and Getting Started Guide.
3. Use the "Custom” installation mode, and point Cisco TMS to the external database server.
4. Make a note of the encryption key generated during the installation.
5. If enabling HTTPS during installation, use a certificate issued to tms.example.com.
6. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.

Installing Cisco TMS on tms02

1. Check that the operating system including service pack level on tms02 is exactly the same as on tms01.
2. Check that both servers are configured with the same time zone.
3. Install Cisco TMS using the same external database server and installation directory as when setting up tms01. Install the same version of Cisco TMS.
4. Enter the encryption key generated during the installation on tms01.
5. If HTTPS was enabled during installation on tms01, use the same certificate used on tms01.
6. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.

Setting up the network load balancer

Once the second node is operational, set up the network load balancer. For the Cisco ACE 4710 Application Control Engine Appliance, this includes configuring:

- Virtual Servers
- Real Servers
- Server Farms
- Health Monitoring
- Stickiness

See Example ACE configuration [p.311] for a reference ACE configuration.

Configuring Cisco TMS

On one of the nodes:

1. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
2. Change the following IP address(es) and hostnames to the NLB's virtual IP address(es) and hostname:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**

On both nodes:

1. Go to **Control Panel** on the Windows server.
2. In **Network Settings** change the default gateway to be the NLB’s IP address.
3. Verify that the Cisco TMS servers can reach the managed systems and vice versa.

Synchronizing local files

Some customizable files used by Cisco TMS are stored in the Windows server's local file system rather than in the tmsng database. The folders these files are stored in must be kept synchronized between the two nodes. See Local files for synchronization [p.315] for a full list of the folders that must be synchronized.

Use your preferred method of synchronizing the folders; for example you could create a shell script that uses xcopy/robocopy to copy files between the two nodes.

Optional step: Enabling use of TLS Client Certificates

If you choose to use TLS client certificates in your deployment you must ensure that:

- The same options are selected in TMS Tools on both servers.
- The TLS certificates imported to both servers are identical.
- Both servers use the same mechanism for certificate revokation.

For more information see TMS Tools [p.287].

The network load balancer, protocols and probes

HTTP/HTTPS/SNMP: Sticky connections

Configure the NLB to forward HTTP and HTTPS connections as well as SNMP traps to the Cisco TMS servers using sticky connections.

Using sticky connections ensures that new connections from a client IP address are assigned to the same Cisco TMS node that received previous connections from that address.

Traffic must be forwarded to one single server, not both servers.

Other protocols

Other protocols such as SSH and FTP are always initiated from the Cisco TMS side. No special configuration of the NLB is required for these protocols.

Probes

A probe is a request sent from the NLB to a node to check whether a particular service is still responding.

Whenever a probe fails, the load balancer, assuming that the node is at least partially inoperative, directs all traffic to the other node and notifies the network administrator.

We recommend probing the Cisco TMS web application (**/tms**)

Create a new domain service account specifically for probing.

This service account does not need any specific rights in Cisco TMS itself and can be a member of the “Users” group only. It must, however, be allowed by IIS to authenticate and log in to Cisco TMS.

If using Cisco TMSPE, see *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* for guidance on probing Cisco TMSPE services.

See Example ACE configuration [p.311] for a sample configuration.

Scheduled tasks

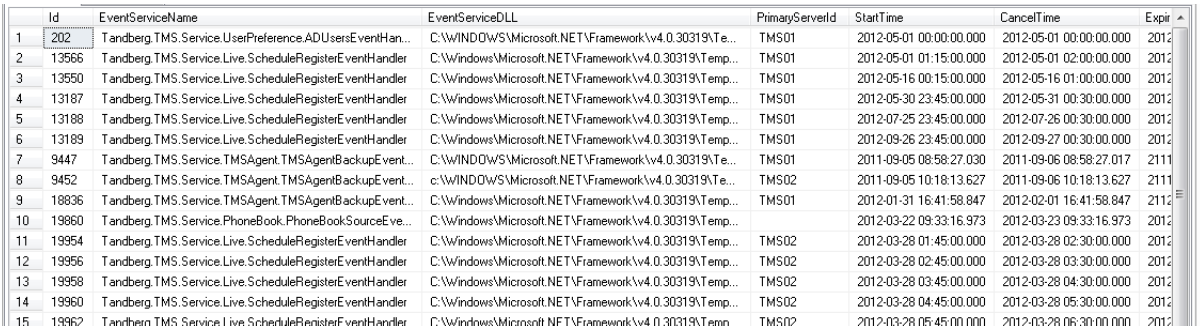
Some tasks in Cisco TMS are scheduled.

Examples include:

- Updating phone book sources from gatekeeper registration lists
- Pushing configuration templates to managed systems
- Mirroring user directories

Such tasks are assigned randomly to one of the two Cisco TMS nodes.

To see which node has been assigned a task, go to the PrimaryServerId column of the SchedulerEvent table in the tmsng database:



	Id	EventServiceName	EventServiceDLL	PrimaryServerId	StartTime	CancelTime	Expir
1	202	Tandberg.TMS.Service.UserPreference.ADUsersEventHan...	C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Te...	TMS01	2012-05-01 00:00:00.000	2012-05-01 00:00:00.000	2012
2	13566	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-05-01 01:15:00.000	2012-05-01 02:00:00.000	2012
3	13550	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-05-16 00:15:00.000	2012-05-16 01:00:00.000	2012
4	13187	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-05-30 23:45:00.000	2012-05-31 00:30:00.000	2012
5	13188	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-07-25 23:45:00.000	2012-07-26 00:30:00.000	2012
6	13189	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-09-26 23:45:00.000	2012-09-27 00:30:00.000	2012
7	9447	Tandberg.TMS.Service.TMSAgent.TMSAgentBackupEvent...	C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Te...	TMS01	2011-09-05 08:58:27.030	2011-09-06 08:58:27.017	2111
8	9452	Tandberg.TMS.Service.TMSAgent.TMSAgentBackupEvent...	c:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Te...	TMS02	2011-09-05 10:18:13.627	2011-09-06 10:18:13.627	2111
9	18836	Tandberg.TMS.Service.TMSAgent.TMSAgentBackupEvent...	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS01	2012-01-31 16:41:58.847	2012-02-01 16:41:58.847	2112
10	19860	Tandberg.TMS.Service.PhoneBook.PhoneBookSourceEve...	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...		2012-03-22 09:33:16.973	2012-03-23 09:33:16.973	2012
11	19954	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 01:45:00.000	2012-03-28 02:30:00.000	2012
12	19956	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 02:45:00.000	2012-03-28 03:30:00.000	2012
13	19958	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 03:45:00.000	2012-03-28 04:30:00.000	2012
14	19960	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp...	TMS02	2012-03-28 04:45:00.000	2012-03-28 05:30:00.000	2012
15	19962	Tandberg.TMS.Service.Live.ScheduleRegisterEventHandler	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temp	TMS02	2012-03-28 05:45:00.000	2012-03-28 06:30:00.000	2012

- If the PrimaryServerId field for a given task is empty, the task will be executed by the first node that polls the database for tasks after the task is scheduled to start.
- If the PrimaryServerId field for a given task shows a node that is operational, that node will pick up the task as soon as the task is scheduled to start.
- If the PrimaryServerId field for a given task shows a node that is not operational, the other node will pick up the task after 60 seconds and execute it.

Cisco TMS does not directly assign tasks to nodes based on server load. The other node picks up a task if the original node is under such a heavy load that it is unable to poll the database for new tasks—this offers a similar balancing mechanism.

The other node will not pick up and re-execute the task if the original assignee fails during execution of that task.

Live Service and the Conference Control Center

When a conference is booked in Cisco TMS, it is allocated to the Live Service on one of the two nodes. The Live Service collects data about the conference, which will display in **Monitoring > Conference Control Center** in Cisco TMS.

If a conference is owned by the Live Service on tms01, but the load balancer forwards feedback from one of the participants in the conference to tms02, tms02 uses a remote procedure call (RPC) to pass the information to tms01.

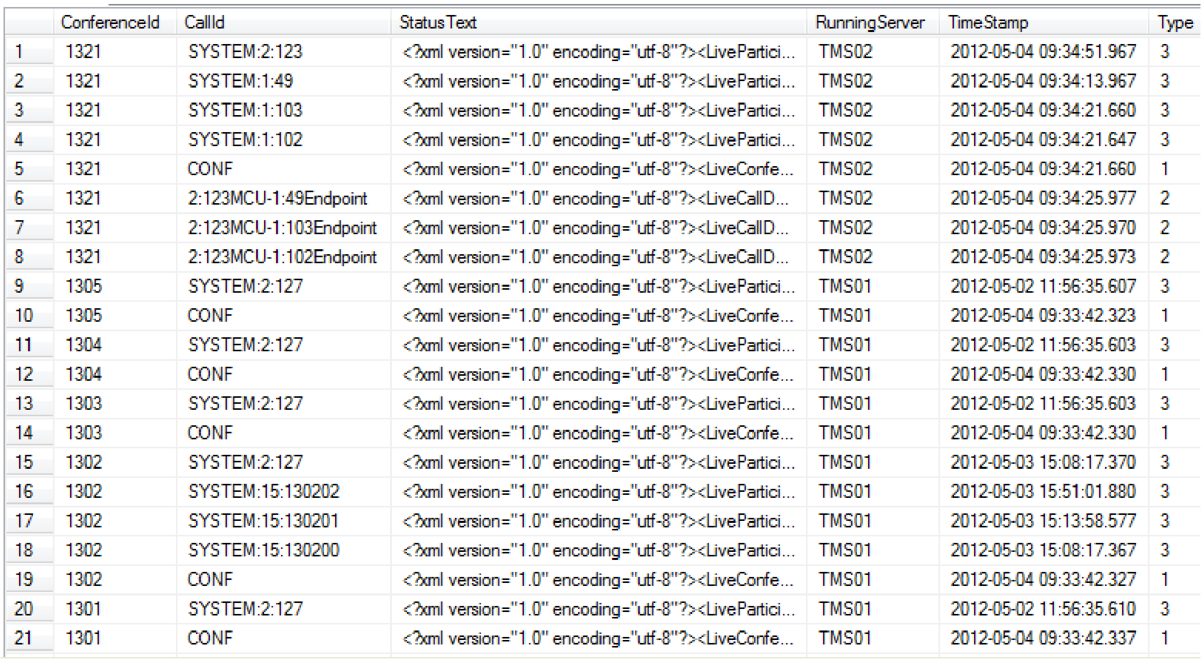
If a user logged on to tms01 makes a change to an ongoing conference owned by tms02 in **Conference Control Center** (CCC):

1. Tms01 sends the change to tms02 using RPC.
2. Tms02's Live Service then instructs the systems involved to make the change.

Live Service uses TCP port 8085 for RPC. If changes made in CCC are slow to propagate from one node to the other:

1. Check that a firewall is not blocking traffic on port 8085.
2. Verify that both Cisco TMS servers are listening on port 8085:
   - Open a cmd shell and execute a `netstat -a -n | findstr :8085` command on both servers
   - Try to connect using telnet (`telnet tms01.example.com 8085`) and check that the connections are not refused .

To check which node owns an ongoing conference and its participants, see the RunningServer column of the LiveStatusData table in the tmsng database. This field contains either “tms01” or “tms02”.



	ConferenceId	CallId	StatusText	RunningServer	TimeStamp	Type
1	1321	SYSTEM:2:123	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS02	2012-05-04 09:34:51.967	3
2	1321	SYSTEM:1:49	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS02	2012-05-04 09:34:13.967	3
3	1321	SYSTEM:1:103	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS02	2012-05-04 09:34:21.660	3
4	1321	SYSTEM:1:102	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS02	2012-05-04 09:34:21.647	3
5	1321	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS02	2012-05-04 09:34:21.660	1
6	1321	2:123MCU-1:49Endpoint	<?xml version="1.0" encoding="utf-8"?><LiveCallD...	TMS02	2012-05-04 09:34:25.977	2
7	1321	2:123MCU-1:103Endpoint	<?xml version="1.0" encoding="utf-8"?><LiveCallD...	TMS02	2012-05-04 09:34:25.970	2
8	1321	2:123MCU-1:102Endpoint	<?xml version="1.0" encoding="utf-8"?><LiveCallD...	TMS02	2012-05-04 09:34:25.973	2
9	1305	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-02 11:56:35.607	3
10	1305	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.323	1
11	1304	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-02 11:56:35.603	3
12	1304	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.330	1
13	1303	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-02 11:56:35.603	3
14	1303	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.330	1
15	1302	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-03 15:08:17.370	3
16	1302	SYSTEM:15:130202	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-03 15:51:01.880	3
17	1302	SYSTEM:15:130201	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-03 15:13:58.577	3
18	1302	SYSTEM:15:130200	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-03 15:08:17.367	3
19	1302	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.327	1
20	1301	SYSTEM:2:127	<?xml version="1.0" encoding="utf-8"?><LivePartici...	TMS01	2012-05-02 11:56:35.610	3
21	1301	CONF	<?xml version="1.0" encoding="utf-8"?><LiveConfe...	TMS01	2012-05-04 09:33:42.337	1

Conferences that are scheduled to start more than 15 minutes into the future are stored in the SchedulerEvent table as described in the Scheduled tasks [p.301] section above. You can then see which node will control the conference by examining the PrimaryServerId value.

Conferences scheduled to start less than 15 minutes into the future are not written to the SchedulerEvent table, but are directly assigned to the Live Service on the node the conference was scheduled on.

Upgrading Cisco TMS

Upgrading Cisco TMS to a later software version must be done during a maintenance window, as upgrading will make Cisco TMS unavailable to users for a short period of time.

As the two Cisco TMS nodes share a common database, they must run the same software version at all times. It is therefore not possible to upgrade one node at a time and keep the other node operational to serve systems and users.

1. Log in to both Cisco TMS Windows servers.
2. Disable file replication to temporarily stop synchronizing local files.
3. Stop all the TMS services, as well as the IIS service on both nodes.
4. Upgrade one of the nodes to the new software version. This will upgrade the tmsng database.
5. Log in to the Cisco TMS web application on this server to verify that it works correctly.

The probes on the NLB will now report that only the first Cisco TMS server is operational so all traffic will automatically be directed to this node. Users and managed systems can now use Cisco TMS again.

1. Upgrade the second Cisco TMS node.
2. The installer will detect that the database has already been upgraded, and offer to continue using the updated database: select **Yes**. The installer will then update the binaries and leave the database alone.
3. Log in to the Cisco TMS web application on this server to verify that it works correctly.
4. Enable file replication.

Check that the network settings have not been changed during the install process:

1. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
2. Check that the following IP address(es) and hostnames are set to the NLB's virtual IP address(es) and hostname:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**

Recovery in case of a failing node

No immediate action is required in the event of a server failure, as the NLB will automatically detect the failure and direct all traffic to the other node.

Troubleshoot the failing node’s software and hardware as you normally would, and bring it back online once it is operational.

The NLB will detect that the node is up again and traffic will then be forwarded to both nodes as normal.

Deploying a hot standby

Keeping an additional Cisco TMS server as a warm spare in case of failure is known as the "Hot Standby" redundancy model.This requires manual intervention if there is a failure on the primary Cisco TMS server, and is therefore a switchover solution rather than a failover solution.

One Cisco TMS server is active at any given time with this redundancy model. The hot standby server must be kept up to date with security patches and other upgrades so that it is ready for activation within a few minutes if the primary server fails.

Note that the hot standby redundancy model requires the tmsng database to be located on an external SQL server, and that the two Cisco TMS servers must be in the same Windows domain.

In the instructions below the following examples are used:

Server	DNS Name	IP Address
Primary Cisco TMS Server (tms01)	tms01.example.com	10.0.0.10
Secondary Cisco TMS Server (tms02)	tms02.example.com	10.0.0.11

The examples assume that you use IPv4. If you also use IPv6, change the IPv6 addresses accordingly.

Setting up the primary Cisco TMS server

Prior to installing Cisco TMS:

1. Set up an SQL server instance on an external server.
2. Set up a DNS entry: tms.example.com pointing to the IP address of the primary server tms01 (10.0.0.10).
3. Install Cisco TMS on tms01 using the instructions provided in the Cisco TMS Installation and Getting Started Guide, but:
   a. Use the "Custom" installation mode.
   b. Point Cisco TMS to the external database server you used in step 1.
4. Make a note of the encryption key generated during the installation.
5. If enabling HTTPS during installation, use a certificate issued to tms.example.com.
6. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.

All users and managed systems must use tms.example.com when connecting to Cisco TMS. The server's own hostname (tms01.example.com) must not be used.

After verifying that the installation of Cisco TMS was successful:

1. In Cisco TMS go to **Administrative Tools > Configuration > Network Settings**.
2. Enter *tms.example.com* in the **TMS Server Fully Qualified Hostname** and **TMS Server Address (Fully Qualified Hostname or IPv4 Address)** fields.

Do not use local user accounts when logging in to Cisco TMS. All user accounts must be domain accounts, so that they are available if you have to swap to the secondary server, tms02.

Setting up the secondary Cisco TMS server

1. Check that the operating system including service pack level on tms02 is exactly the same as on tms01.
2. Check that the servers are both configured with the same time zone; failure to do this will mean that the start and end times of scheduled conferences are incorrect in the case of a switchover.
3. Run the Cisco TMS installer on tms02:
   a. Choose the *Custom* installation mode and enter the IP address of the external SQL server when prompted.
   b. Install to the same directory as on tms01 and use the same log directory as on tms01. This is important because the log directory path is stored as an Environment Variable in Windows and not in the SQL database.
   c. Enter the encryption key generated during the installation on tms01.
   d. If HTTPS was enabled during installation on tms01, use the same certificate used on tms01.
4. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.
5. On tms02 go to **Administrative Tools > Configuration > Network Settings > Advanced Network Settings for Systems on Internal LAN**. Make sure the IP address is tms01 (10.0.0.10) and the hostname is tms.example.com as the installer could have changed these values.
6. Open the Services Management Console on tms02:
   - Stop all the Cisco TMS services - they all have names starting with TMS.
   - Stop the Internet Information Services (IIS) service called World Wide Web Publishing Service.
   - Set the Startup Type of the IIS and TMS services to “Manual”.

Tms02 is now ready to act as a warm spare in the case of a failure on tms01.

Note that in **Administrative Tools > Server Maintenance > TMS Service Status** you will see the services for both servers. Click on **Clear List** to remove the stopped services on tms02 from the list.

Synchronizing local files

Some customizable files used by Cisco TMS are stored in the Windows server's local file system rather than in the tmsng database. The folders these files are stored in must be kept synchronized between the two nodes. See Local files for synchronization [p.315] for a full list of the folders that must be synchronized.

Use your preferred method of synchronizing the folders. One way to do this is:

1. Create a shell script that uses xcopy/robocopy to copy files to the corresponding folders on tms02.
2. Use the Windows Task Scheduler on tms01 to run the script each hour.

If you swap the two servers in the event of a failure on the primary server, change the synchronization mechanism you set up for keeping the folders on tms01 and tms02 in synch so that it now synchronizes from tms02 to tms01.

Optional: Enable TLS client certificates

If you choose to use TLS client certificates in your deployment you must ensure that:

- The same options are selected in TMS Tools on both servers.
- The TLS certificates imported to both servers are identical.

- Both servers use the same mechanism for certificate revokation.

For more information see TMS Tools [p.287].

Upgrading Cisco TMS

You must keep the Cisco TMS software versions on the primary and secondary servers consistent. After upgrading the primary server, you must upgrade the secondary server as soon as possible. If the primary server fails while the secondary server is on an older software version, you will not be able to swap the servers until you have upgraded the secondary server to the newer Cisco TMS software version.

1. Disable file replication to temporarily stop synchronizing local files.
2. Upgrade the primary server.
3. Upgrade the secondary server.
4. After the server has rebooted, log in to the Cisco TMS web application to verify that it works correctly.
5. In the Cisco TMS application go to **Administrative Tools > Configuration > Network Settings**.
6. Check that the following IP address(es) and hostnames are set to IP address: 10.0.0.10 and hostname: tms.example.com:
   - **Event Notification > SNMP Traphost IP Address**
   - **Advanced Network Settings for Systems on Internal LAN**: all fields
   - **Advanced Network Settings for Systems on Public Internet/Behind Firewall**
7. Stop the TMS services and set them to Manual again.
8. Enable file replication.

Recovery if the primary server fails

If the primary server: tms01 fails and becomes unusable, changing the secondary server: tms02 into an operational state will take no more than a few minutes.

1. Unplug tms01 from the network.
2. Change the IP address of tms02 to the old IP address of tms01, for example 10.0.0.10.
3. Verify that tms02 is reachable on its new IP address.
4. Open the TMS Tools application and go to **Configuration > Change DB Connect Settings**.
5. Click **OK** to verify that tms02 still has the correct password, as the password to the database might have changed since you initially set up tms02.
6. In the Services Management Console:
   a. Change the Startup Type of all the TMS services and the World Wide Web Publishing Service to *Automatic*.
   b. Start the services.

Tms02 is now the active Cisco TMS server. As you have instructed managed systems to use tms.example.com when communicating with Cisco TMS, no reconfiguration is needed on the managed systems themselves.

To verify that tms02 operates correctly:

1. Schedule a short conference two minutes into the future.
2. See that it launches and is torn down as expected.

3. Check that you can monitor it using the **Conference Control Center**.
4. Check that Cisco TMS generates a call detail record (CDR) for the conference.

To verify that Cisco TMS is communicating with systems:

1. Wait approximately 20 minutes for the TMS Database Scanner Service to complete a full run.
2. Go to **Systems > System Overview** in Cisco TMS.
3. Select all the systems in the tree to the left, and select **Network Settings > TMS To System Connectivity** in the tree to the right.
4. Click **View** and then check that no systems have their **Status** set to *NoResponse*.

Note that in **Administrative Tools > Server Maintenance > TMS Service Status** you will see the services for both servers. Click on **Clear List** to remove the stopped services on tms01 from the list.

Before connecting tms01 to your network:

1. Change its IP address to tms02's old value, for example 10.0.0.11.
2. Disable all the TMS services and IIS.

Once the problem with tms01 has been fixed, it will become the warm spare in case tms02 ever goes down.

Note: Do not add tms01 back to the network before changing its IP address to a new value. This will lead to IP address conflicts that will cause unpredictable behavior in Cisco TMS.

Database redundancy

Two of the SQL Server 2008 high-availability alternatives are appropriate for Cisco TMS: database mirroring and failover clustering.

Database mirroring

Database mirroring increases database availability by maintaining a hot spare database on another SQL Server instance. The primary SQL Server instance is referred to as the principal database. The principal database has a secure channel to a mirror database residing on another SQL Server instance, preferably located on another physical server.

In the database mirroring model, there are two types of transfer mechanisms, synchronous and asynchronous.

Synchronous transfer

If you are using synchronous mirroring, a transaction is not considered successfully completed until it is committed in both the principal and mirror databases. This guarantees that the two databases are always consistent. However, network speed and distance will affect database response times.

Asynchronous transfer

If performance is more important than data consistency, data transfers can be set up as asynchronous operations, but some data will then be lost in the case of a catastrophic failure in the principal database server.

Network requirements for asynchronous mirroring:

Minimum bandwidth = 10Mbps

Latency < 50ms

Jitter < 1ms

Packet drops < 1%

Changing the database connection string

The SQL Server database mirroring feature supports automatic failovers between the principal and mirror databases in the case of a failure on the principal database. However Cisco TMS does not,so the database configuration must be manually changed in Cisco TMS. If you are using the NLB redundancy model, this must be done on both Cisco TMS nodes:

1. Go to the TMS Tools application **> Configuration > Change Database Connection Settings**.
2. Change the **Database Server\Instance** to point to the mirror database and click **OK**.
3. Restart all the TMS services as well as IIS to complete the manual failover operation.

Placing the principal and mirror databases in two different physical locations while using synchronous mirroring is not supported by Cisco TMS, as transactions take too long to complete, causing slow responses in the application.

See the following Microsoft Developer Network (MSDN) article for documentation on how to set up a mirrored database in SQL Server 2008: SQL Server 2008 Database Mirroring Overview

Failover clustering

Database failover clustering is a server level redundancy model where two or more servers (called nodes) share resources. If one or more nodes fail, the remaining nodes in the cluster automatically pick up all services from the failing nodes. Only one node manages a particular SQL Server instance at any given time.

Each failover cluster instance has a logical resource group that includes:

- Network name
- IP address
- SQL Server Database Engine service

Clients use the network name and IP address as identifiers to connect to the instance, regardless of which node currently serves the instance.

During installation, point Cisco TMS to the clustered instance's network name or IP address.

No further reconfiguration is necessary on the Cisco TMS server .

No additional steps are required when upgrading Cisco TMS.

Requirements

Two or more servers running Windows Server 2008 Enterprise or Datacenter edition.

Each server must have:

- Two network interfaces
- Shared disk storage such as a storage area network (SAN)

The following white paper from Microsoft gives an in-depth description on planning, implementation, and administration of an SQL Server 2008 failover cluster: SQL Server 2008 Failover Clustering

Backups

We recommend scheduling a regular automated backup of the tmsng database.

Example ACE configuration

After initial configuration of your Cisco ACE 4710 Appliance Control Engine load balancer, you can copy and paste this sample configuration to your ACE. All IP addresses, DNS names, usernames, and passwords must be amended to reflect your actual configuration prior to applying the settings to your load balancer.

```
!Assigning a recourse class for use as the default class (minimum required configuration)
resource-class TMS
limit-resource all minimum 10.00 maximum unlimited
limit-resource conc-connections minimum 10.00 maximum unlimited
limit-resource sticky minimum 10.00 maximum unlimited

!The software version used on the ACE: A5 1.2
boot system image:c4710ace-t1k9-mz.A5_1_2.bin

!Configuring the hostname of the loadbalancer
hostname loadbalancer

!Creating and assigning configuration to the Admin Context
context Admin

!Putting the Admin context into the resource class TMS
member TMS

!Creating access lists, here nothing is restricted
access-list ALL line 8 extended permit ip any any
access-list ALL line 9 extended permit icmp any any

!Creating Probes for health check of the TMS (change username/password)
probe https BOOKING-PROBE-TMS
description Checking to see if the booking module is running. running against port 443
port 443
interval 10
passdetect interval 10
ssl version all
credentials tms-service my_password
request method get url /tms/booking
expect status 200 400
probe https CITIES-PROBE-TCP-443
port 443
interval 10
passdetect interval 45
receive 20
ssl version all
expect status 200 400
append-port-hosttag
open 20
probe http PROBE-HTTP-80
port 80
interval 10
passdetect interval 45
receive 2
request method get url /tms
expect status 200 499
open 2

!This probe logs into TMS on HTTPS for verification (change username/password)
probe https TMS-Monitoring-443
description Monitor the TMS application
port 443
```

```
ssl version all
credentials tms-service my_password
request method get url /tms
expect status 200 400

!This probe logs into TMS on HTTP for verification (change username/password)
probe http TMS-Monitoring-80
credentials tms-service my_password
request method get url /tms
expect status 200 400
probe https TMS-WEBSERVICES-443
description Check if the booking services are running on 443
port 443
interval 10
ssl version all
credentials tms-service my_password
request method get url /TMS/external/booking/bookingservice.asmx
expect status 200 400

!Configuring the real servers
rserver host TMS01
description ***TMS01.EXAMPLE.COM***
ip address 10.0.200.50
inservice
rserver host TMS02
description ***TMS02.EXAMPLE.COM***
ip address 10.0.200.60
inservice

!Creating server farms
serverfarm host SFARM-TMS-WEB-161
description ** TMS-WEB-161 VIP **
probe PROBE-HTTP-80
rserver TMS01
inservice
rserver TMS02
inservice
serverfarm host SFARM-TMS-WEB-162
description ** TMS-WEB-162 VIP **
probe PROBE-HTTP-80
rserver TMS01
inservice
rserver TMS02
inservice
serverfarm host SFARM-TMS-WEB-443
description ** TMS-WEB-443 VIP **
probe BOOKING-PROBE-TMS
probe TMS-Monitoring-443
probe TMS-WEBSERVICES-443
rserver TMS01 443
inservice
rserver TMS02 443
inservice
serverfarm host SFARM-TMS-WEB-80
description ** TMS-WEB-80 VIP **
probe PROBE-HTTP-80
rserver TMS01 80
inservice
```

```
rserver TMS02 80
inservice

!Adding sticky sessions to all server farms
sticky ip-netmask 255.255.255.255 address source L7-CLASS-TMS-WEB-161-STICKY
timeout 10
serverfarm SFARM-TMS-WEB-161
sticky ip-netmask 255.255.255.255 address source L7-CLASS-TMS-WEB-162-STICKY
timeout 10
serverfarm SFARM-TMS-WEB-162
sticky ip-netmask 255.255.255.255 address source L7-CLASS-TMS-WEB-443-STICKY
timeout 10
serverfarm SFARM-TMS-WEB-443
sticky ip-netmask 255.255.255.255 address source L7-CLASS-TMS-WEB-80-STICKY
timeout 10

!Adding the virtual IP address to the virtual servers
serverfarm SFARM-TMS-WEB-80
class-map match-all L4-CLASS-TMS-WEB-161
match virtual-address 10.0.200.40 tcp eq 161
class-map match-all L4-CLASS-TMS-WEB-162
match virtual-address 10.0.200.40 tcp eq 162
class-map match-all L4-CLASS-TMS-WEB-443
match virtual-address 10.0.200.40 tcp eq https
class-map match-all L4-CLASS-TMS-WEB-80
match virtual-address 10.0.200.40 tcp eq www
class-map type http loadbalance match-any default-compression-exclusion-mime-type
description DM generated classmap for default LB compression exclusion mime types.
match http url .*gif
match http url .*css
match http url .*js
match http url .*class
match http url .*jar
match http url .*cab
match http url .*txt
match http url .*ps
match http url .*vbs
match http url .*xsl
match http url .*xml
match http url .*pdf
match http url .*swf
match http url .*jpg
match http url .*jpeg
match http url .*jpe
match http url .*png

!Making sure we can access the ACE remotely
class-map type management match-any remote_access
match protocol xml-https any
match protocol icmp any
match protocol telnet any
match protocol ssh any
match protocol http any
match protocol https any
match protocol snmp any
policy-map type management first-match remote_mgmt_allow_policy
class remote_access
permit
```

```
class class-default
permit

!Setting load balancing properties
policy-map type loadbalance first-match L4-CLASS-TMS-WEB-161-STICKY
class class-default
sticky-serverfarm L7-CLASS-TMS-WEB-161-STICKY
policy-map type loadbalance first-match L4-CLASS-TMS-WEB-162-STICKY
class class-default
sticky-serverfarm L7-CLASS-TMS-WEB-162-STICKY
policy-map type loadbalance first-match L4-CLASS-TMS-WEB-443-STICKY
class class-default
sticky-serverfarm L7-CLASS-TMS-WEB-443-STICKY
policy-map type loadbalance first-match L4-CLASS-TMS-WEB-80-STICKY
class class-default
sticky-serverfarm L7-CLASS-TMS-WEB-80-STICKY

!Setting virtual server properties
policy-map multi-match L4-POLICY-TMS-WEB
class L4-CLASS-TMS-WEB-162
loadbalance vip inservice
loadbalance policy L4-CLASS-TMS-WEB-162-STICKY
loadbalance vip icmp-reply
class L4-CLASS-TMS-WEB-161
loadbalance vip inservice
loadbalance policy L4-CLASS-TMS-WEB-161-STICKY
loadbalance vip icmp-reply
class L4-CLASS-TMS-WEB-80
loadbalance vip inservice
loadbalance policy L4-CLASS-TMS-WEB-80-STICKY
loadbalance vip icmp-reply
class L4-CLASS-TMS-WEB-443
loadbalance vip inservice
loadbalance policy L4-CLASS-TMS-WEB-443-STICKY

!Configuring virtual interface VLAN
interface vlan 200
description client
no ipv6 normalization
no ipv6 icmp-guard
ip address 10.0.200.24 255.255.255.0
no normalization
no icmp-guard
access-group input ALL
access-group output ALL
service-policy input remote_mgmt_allow_policy
service-policy input L4-POLICY-TMS-WEB
no shutdown

!END
```

Local files for synchronization

During installation of Cisco TMS, customizable files are added which must be synchronized between the two servers when using a redundant deployment.

The files include software and images which can be uploaded to Cisco TMS, and images created by Cisco TMS.

In a default installation the files are located here:

C:\Program Files\TANDBERG\TMS\Config\System\

C:\Program Files\TANDBERG\TMS\Data\GenericEndpoint\

C:\Program Files\TANDBERG\TMS\Data\SystemTemplate\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Map\

C:\Program Files\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

Note: Directories are created on first use, which means that the directory might not exist when setting up file replication between nodes.

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 317
Website scenarios 322
System scenarios 324
Conference scenarios 326
Java applet scenarios 327
Phone book scenarios 330
Reporting scenarios 331
Cause Codes 334

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 Log 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 levels [p.319] for instructions.

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

The Cisco TMS installer creates the following logs:

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\**.

Log name	Description	Level	Configuration file
event-stats	Logs feedback event statistics. Only activate when requested by Cisco support. Set to INFO to activate logging	WARN	**\wwwTMS\public\Web.CONFIG**
log-api	Logs the activity of the REST API for configurations.	WARN	**\wwwTMS\api\Web.CONFIG**
log-lcdpanel	LCD panel log. Cisco TelePresence Management Server appliance only. Not configurable.		
log-liveservice	Keeps a record of TMSLiveService [p.17]	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 [p.18]	WARN	**\Services\TMSPLCMDirectoryService.exe.CONFIG**
log-schedulerservice	Logs the activity of TMSSchedulerService [p.18]	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**

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-TMSAgentDiagnostics	This log is no longer in use.		
log-tmsagentproxy	Logs the activity of the Cisco TMSPE IIS Proxy.	**WARN**	**\wwwTMS\tmsagent\Web.config**
log-TMSDatabaseScanner	Logs the activity of TMSDatabaseScannerService [p.18]	**WARN**	**\Services\TMSDatabaseScannerService.exe.CONFIG**
log-TMSServerDiagnosticsService	Logs the activity of TMSServerDiagnosticsService [p.18]	**WARN**	**\Services\TMSServerDiagnosticsService.exe.CONFIG**
log-TMSSNMPservice	Logs the activity of TMSSnmpService [p.18]	**WARN**	**\Services\TMSSSNMPService.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-web-external	Logs activities that use password protected APIs, such as Cisco TMSBA.	**WARN**	**\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**

Changing the log levels

There are four log levels available for each log file, with the default values and location of the corresponding 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 being instructed to by a Cisco support representative. Debug logging is normally only used in advanced troubleshooting scenarios, and should be 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 [p.317].
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>`** element within, and then the **`<level>`** element.
6. Update the element with the desired value, for example from **`<level value="WARN"/>`** to **`<level value="DEBUG"/>`**.
7. 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 - Acces
s denied to: SystemRead
```

```
2013-06-20 14:53:04,503 [75] ERROR ASP.global_asax - System.Web.Services.Protocols.SoapEx
ception: 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.IExecutio
nStep.Execute()
at System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchron
ously)
```

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

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 TMS Tools [p.287].

Advanced steps

Web server

- Verify that the virtual directories described in the Internet Information Services web server and applications [p.16] 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.

Database

Run an osql script towards the database and see whether it returns any data. This script will return the number of systems in the Cisco TMS database. Depending on the SQL configuration, run one of the commands below from the Cisco TMS server itself.

1. `osql -E -d tmsng -Q "select count(*) from objsystem"`
2. `osql -E -S .\SQLTMS -d tmsng -Q "select count(*) from objsystem"`

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 in 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.
- Restart TMSSnmpService. For more information about this Windows service, see TMSSnmpService [p.18].

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 [p.18].

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 [p.18].

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 [p.18].

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.
- Restart TMSLiveService. See TMSLiveService [p.17] for more information on this Windows service.

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**, **Graphical Monitor** and **Map Monitor** all 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.

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.

Advanced steps

The proxy server may need to be configured to allow this kind of traffic from the Cisco TMS server to the clients.

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 and Map Monitor work as expected.

Troubleshooting monitoring

Quicker load of Monitor

When Cisco TMS is upgraded, users may experience that loading of **Conference Control Center**, **Graphical Monitor** and **Map 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.

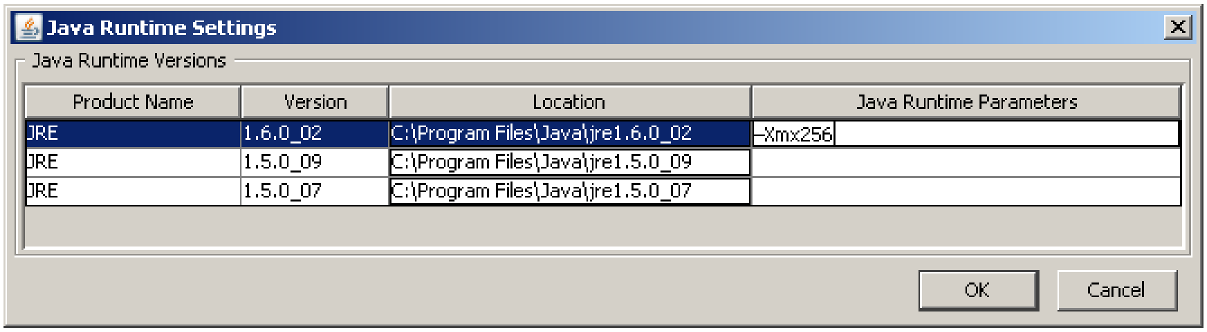
Out of memory

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**, **Graphical Monitor** or **Map 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.



Product Name	Version	Location	Java Runtime Parameters
JRE	1.6.0_02	C:\Program Files\Java\jre1.6.0_02	–Xmx256
JRE	1.5.0_09	C:\Program Files\Java\jre1.5.0_09	
JRE	1.5.0_07	C:\Program Files\Java\jre1.5.0_07	

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

You can get the following errors on the endpoint if corporate directory is not working properly:

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 [p.214] 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.
- Restart TMSPLCMDirectoryService. For more information about this Windows service, see TMSPLCMDirectoryService [p.18].
- 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.

No CDRs from endpoints running Cisco 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 MCU

Basic steps

Make sure you are running software version 4.3 or later, which supports asynchronous processing of CDRs.

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 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&directio
   n=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*.

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.
- Restart TMSSnmpService. For more information about this Windows service, see TMSSnmpService [p.18].

Advanced steps

Using Wireshark, verify that Cisco TMS is receiving SNMP data from the system.

Cause Codes

Code	Description
0	Cisco specific. Not part of ITU-T standard.
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.
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.
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.

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.
255	Cisco specific. Not part of ITU-T standard.

Bibliography

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

Title	Reference	Link
Cisco TelePresence Management Suite Installation Guide	D14389	http://cisco.com
Cisco TelePresence Management Suite Provisioning Extension Deployment Guide	D14941	http://cisco.com
Cisco TelePresence Conductor with Cisco TMS Deployment Guide	D15001	http://cisco.com
Cisco TelePresence Video Communication Server Administrator Guide	D14049	http://cisco.com
Cisco Unified Communications Manager documentation	—	http://cisco.com
Cisco TelePresence Supervisor MSE 8050 Printable Help	D14840	http://cisco.com
Cisco TelePresence Conductor Administrator Guide	D14826	http://cisco.com
SQL Server 2008 Database Mirroring Overview	—	http://msdn.microsoft.com
SQL Server 2008 Failover Clustering	—	http://download.microsoft.com

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

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.