



CHAPTER 8

Initializing Cisco TelePresence Manager

Revised: August 12, 2009, OL-13673-04
First Published: November 27, 2006

Contents

- [Introduction, page 8-1](#)
- [Post-Install Guidelines for CTS-Manager, page 8-2](#)
- [Initializing Cisco TelePresence Manager After Installation, page 8-3](#)
- [Required Information and Equipment, page 8-3](#)
- [Initialization for Microsoft Exchange Deployments, page 8-4](#)
- [Explanation of LDAP Access Setting Fields, page 8-5](#)
- [Explanation of Field Mappings Fields, page 8-8](#)
- [Explanation of Cisco Unified Communications Manager Fields, page 8-10](#)
- [Explanation of Microsoft Exchange Fields, page 8-11](#)
- [Explanation of Database Backup Schedule Fields, page 8-12](#)
- [Microsoft Exchange Calendar Service Window, page 8-13](#)
- [Initialization for IBM Domino Deployments, page 8-16](#)
- [Explanation of LDAP Access Setting Fields, page 8-18](#)
- [Explanation of LDAP User Auth Setting Fields, page 8-19](#)
- [Explanation of Cisco Unified Communications Manager Fields, page 8-21](#)
- [IBM Domino Calendar, page 8-22](#)
- [Explanation of IBM Domino Fields, page 8-22](#)
- [Dashboard for Verification of Installation Status, page 8-24](#)

Introduction

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

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

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

Post-Install Guidelines for CTS-Manager

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

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

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

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

Set-Up Procedure Guidelines after Installing CTS-Manager	Description	Location
Additional Configuration Procedures for CTS-Manager	The administrator makes use of the System Configuration window to perform system configuration tasks such as asynchronizing system databases, managing security, and reconfigure system settings	Chapter 10, “Monitoring Cisco TelePresence Manager”
Email and Meeting Action Requirements	The Calendar service (either Microsoft Exchange or IBM Domino) sends an acceptance email to the meeting organizer, with the notice that the rooms have been reserved and placed on the calendar. CTS-Manager also sends either a Confirmation email or an Action Required email to the meeting organizer when a meeting is scheduled	Chapter 11, “CTS-Manager Emails and End-User Web UI”

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

Initializing Cisco TelePresence Manager After Installation

This section contains the following topics pertaining to initialization:

- [Required Information and Equipment, page 8-3](#)
- [Initialization Procedure, page 8-4](#)

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

Required Information and Equipment

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

Additionally, Cisco TelePresence Manager must have network access to a computer running Windows Explorer version 6.0, Microsoft Exchange Server and Active Directory server or IBM Domino Server and Domino Directory Server, and Cisco Unified Communications Manager.

Initialization Procedure

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

Initialization for Microsoft Exchange Deployments

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

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

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

Figure 8-1 Initial Preferences Window

To assist Cisco TelePresence System Manager in showing date and time properly, specify the location in which the computer is located.


Note that time zones of the same offset might or might not observe daylight saving time (DST). Ensure that appropriate location is selected.

Browser's Location:	<input type="text"/>
Selected location observes DST:	<input type="checkbox"/>

[Continue](#)

- Step 3** At the product page that appears, click on **Cisco TelePresence Manager**.
- Step 4** At the login page, enter the username and password created during installation.
- The Cisco TelePresence Manager initial window appears with several fields already populated from the installation process. Review it and click **Next**.
- Step 5** The Calendar Server Selection window is displayed. See .
- Choose Microsoft Exchange for this deployment and click **Next**.

Figure 8-2 Calendar Server Selection Window

 <p>Cisco TelePresence Manager</p> <ul style="list-style-type: none"> 1 - Welcome 2 - Calendar Server Selection 3 - LDAP Access Setting 4 - LDAP User Auth Setting 5 - Field Mappings 6 - Unified CM 7 - Database Backup Schedule 	<p>Calendar Server</p> <p>Select the email server to go to next step.</p> <ul style="list-style-type: none"> <input type="radio"/> Microsoft Exchange <input type="radio"/> IBM Domino <input checked="" type="radio"/> None <p>Selection of Calendar server will display corresponding server set up screen in a coming step. If none is selected ,the Calendar Server configuration step will be skipped.</p>
---	---

- Step 6** The LDAP Access Setting window opens. See [Figure 8-3](#). Fill in the fields and click **Test Connection**.

The system tests the connection information. A popup window opens and displays “Connection Verified.” Click **OK**, then click **Next**.



Note

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

Figure 8-3 LDAP Access Setting Window

LDAP Access Setting

Enter host and user account information that allows Cisco TelePresence Manager to access the LDAP server. Connection to the LDA must be tested and verified before you can advance to the next step.

Host: *

Bind Method: ☐ Secure ☒ Normal

Port: *

Default Context: *

Username: ☒ Append default context *

Password: *

Certificate: *

- Host: the LDAP server host name or IP address.
- Port: the port on which the LDAP server is running.
- Default Context: the base DN (e.g. ou=department,o=building,o=state,dc=com). Use 'Fetch DNs' to pick from a list of DNs ex from the given host.
- User Name: FQDN of the user ID that has READ access to the server (e.g. cn=administrator). Check 'Append default context' just the RDN.

* = Required Fields

Explanation of LDAP Access Setting Fields

Lightweight Directory Access Protocol (LDAP) is a protocol definition for accessing directories. The LDAP Access Settings window specifies LDAP Active Directory server settings that are used by Cisco TelePresence Manager to access the directory information. This window contains the following fields:

- Host

The hostname is an alias that is assigned to an IP address for identification.

- Enter the hostname of the LDAP server.
- The hostname consists of up to 64 characters and can contain alphanumeric characters and hyphens, English characters only.

- Bind Method

The bind method is the type of security required.

- Secure—Secure Socket Layer (SSL) connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. You must complete the Certificate field on this window before you can proceed.
- Normal—The CTS-Manager communicates with the LDAP server in cleartext using HTTP. In normal mode, you do not need to complete the Certificate field.

- Port
 - The default port for secure SSL connection is 636.
 - The default port for normal SSL connection for multiple servers is 3268.
 - The default port for secure SSL connection for multiple servers is 3269 (when global catalogue is enabled).
 - The default port for normal connection for a single server is 389 (when global catalogue is enabled).
- Default Context

Default Context is the context from which the LDAP queries are performed. To change the default context, choose it in the Fetch DN's drop-down list adjacent to this field.
- Username

The username provides identification of the user to the LDAP server.

 - The format must be in the LDAP fully qualified domain name (FQDN) format.
 - Examples: cn=admin, cn=users, dc=<mydomain>, dc=com
- Append default context

Check this box to avoid typing in the LDAP Access username manually, keeping the requirements of the LDAP FQDN format. If this box is not checked, you must append the information in the Default Context field.
- Password

The user password allows access to the LDAP server.

The password must contain at least six characters and maximum of 31 characters and should be unique. It must start with a lowercase alphanumeric character and be English characters. International characters are not supported.
- Certificate

The certificate is a digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

Step 7 The LDAP User Auth Setting window is displayed. See [Figure 8-4](#).

Fill in the fields and click **Verify Container DN**.

The system tests the container information. A popup window opens and displays “User container <...> validated successfully.” Click **OK**, then **Next**.



Note

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

Figure 8-4 LDAP User Authorization Settings Window

Cisco TelePresence Manager

1 - Welcome
2 - Calendar Server Selection
3 - LDAP Access Setting
4 - LDAP User Auth Setting
5 - Field Mappings
6 - Cisco UCM
7 - Calendar Server
8 - Database Backup Schedule

LDAP User Auth Setting

Enter the user container Relative Distinguished Names (RDNs) for LDAP users. The RDNs must be validated successfully before you advance to the next step.

Default Context: DC=srdev,DC=com

User Containers: cn=users ☒ Append default context *

☐ Append default context

☐ Append default context

☐ Append default context

☐ Append default context

- Default Context: the DN that was entered in the previous screen.
- User Container: the DN of the container under which users can be found. Check 'Append default context' to enter just the RDN

* = Required Fields

LDAP User Authorization Setting Fields

The LDAP User Auth Setting window contains the following fields:

- User Containers

The FQDN format name of the LDAP container in which CTS-Manager can find the list of users.

- Append default context

Check this box to meet the requirements of the LDAP FQDN format, or type in the Default Context after the User Container name yourself.

Step 8 The Field Mapping window is displayed. See [Figure 8-5](#).

The fields should be populated with information you have already entered.

Figure 8-5 Field Mappings Window

System Configuration > LDAP Server

Settings
Field Mappings

Person

	Object Class	Attribute
SchedulerName:	Person	proxyaddresses
EmailID:	Person	proxyaddresses
DisplayName:	Person	displayname

EnterpriseConfRoom

	Object Class	Attribute
EmailID:	Person	proxyaddresses
DisplayName:	Person	displayname

View Sample Data

Explanation of Field Mappings Fields

The CTS-Manager server uses application objects and attributes that are internally mapped to the objects and attributes in the LDAP Directory Server. Most of these mappings are predefined and fixed. However, some of the information required for the Cisco TelePresence system may be stored in different attributes of the LDAP Directory Server, based on the enterprise deployment. The Field Mapping window provides a mechanism to map such objects and attributes used by the CTS-Manager server to the object and attributes defined in the LDAP Directory Server schema.



Note

The Login of the user is dependent on the Field Mapping of the EmailID attribute, the administrator must notify users if this Field Mapping has changed.



Caution

The object and attribute mappings for Exchange/Directory Server deployments are listed in [Table 8-2](#) and cannot be changed after installing and configuring Cisco TelePresence Manager. Cisco TelePresence Manager might not functions properly if the Object Class fields are changed. SchedulerName should not be changed unless Microsoft Exchange changes their mappings.

Table 8-2 LDAP Objects and Attributes

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
Person			
	SchedulerName	Person	proxyaddresses
	EmailID	Person	proxyAddresses

Table 8-2 LDAP Objects and Attributes (continued)

Application Object	Application Attribute	LDAP Object Class	LDAP Attribute
	DisplayName	Person	displayname
EnterpriseConfRoom			
	EmailID	Person	proxyAddresses
	DisplayName	Person	displayname



Note For more information about Field Mapping, see the Cisco TelePresence Manager online help.

Step 9 When all information has been entered, click **View Sample Data**.

A popup window opens and displays the data that has been entered, see [Figure 8-6](#). Review the information and verify that it is correct and complete, and click **Close**.

A popup window opens and displays the message “Does the data look correct to you?”

Click **OK**, then click **Next**.

Figure 8-6 System Configuration - LDAP Server Window

System Configuration > LDAP Server

Person		
SchedulerName --> Person:proxyaddresses	EmailID --> Person:proxyaddresses	DisplayName --> Person:displayname
smtp:Administrator@mycisco.com	smtp:Administrator@mycisco.com	Administrator

EnterpriseConfRoom	
EmailID --> Person:proxyaddresses	DisplayName --> Person:displayname
smtp:Administrator@mycisco.com	Administrator

Close

Step 10 The Cisco **Unified CM** window is displayed. See [Figure 8-7](#).

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

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



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

Figure 8-7 Cisco Unified CM Window

Explanation of Cisco Unified Communications Manager Fields

- **Host**
Host is the hostname or IP address of the Cisco Unified Communications Manager server host.
- **Username**
Username is the username for the application user for the Cisco Unified Communications Manager server.
- **Password**
The password allows the user to access the Cisco Unified Communications Manager.
- **Certificate**
The certificate is a digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

Step 11 The **Microsoft Exchange** window opens. See [Figure 8-8](#).

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

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



Note

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

Figure 8-8 Microsoft Exchange Window

Cisco TelePresence Manager

- 1 - Welcome
- 2 - Calendar Server Selection
- 3 - LDAP Access Setting
- 4 - LDAP User Auth Setting
- 5 - Field Mappings
- 6 - Cisco UCM
- 7 - Calendar Server**
- 8 - Database Backup Schedule

Microsoft Exchange

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

Host: *

Bind Method: ☐ Secure ☒ Normal

Port: *

Domain Name: *

Logon Name:

SMTP LHS: *

Password: *

Certificate: Browse... *

- Host: the Microsoft Exchange server host name or IP address.
- Logon Name: user account that has read access to the Exchange server. This account name is used to log on to an Active Directory domain.
- SMTP LHS/Password: Left hand side of the email address of the user account that has read access to the Exchange server. Password necessary for authentication.

* = Required Fields

Explanation of Microsoft Exchange Fields

- **Host**
Host is the hostname or IP address of the Microsoft Exchange Server host.
- **Bind Method**
The bind method indicates the desired level of security.
 - Secure—Secure Socket Layer (SSL) connection requires the Distinguished Encoding Rules (DER) Certificate for the Microsoft Exchange Server. You must complete the Certificate field on this window before you can proceed.
 - Normal—The Cisco TelePresence Manager communicates with the Microsoft Exchange Server in cleartext using HTTP.
- **Port**
The default value is 80, for secure mode the value is 443.
- **Domain Name**
This field requires a sequence of case-insensitive ASCII labels separated by dots (for example, “cisco.com”)—defined for subtrees in the Internet Domain Name System and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.
- **Logon Name**
The logon username should have read access to the Exchange server and rooms. This account name is used to logon to an Active Directory domain.
- **SMTP LHS**
Left hand side of the email address of the user account that has read access to the Exchange Server. Password is necessary for authentication.
- **Password**

The user password allows access to the Microsoft Exchange Server.

- **Certificate**

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



Note

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

Step 12 The Database Backup Schedule window opens. See [Figure 8-9](#).

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



Note

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

Figure 8-9 Database Backup Schedule Window

Cisco TelePresence Manager

- 1 - Welcome
- 2 - Calendar Server Selection
- 3 - LDAP Access Setting
- 4 - LDAP User Auth Setting
- 5 - Field Mappings
- 6 - Cisco UCM
- 7 - Calendar Server
- 8 - Database Backup Schedule**

Database Backup Schedule

Set database backup schedule and settings. A schedule must be set before the initialization process can be completed.

Schedule (GMT): !Set back-up schedule! Change...

Number of backup files to keep: 14

Backup Type: ☐ Local ☒ Remote

Backup Mode: ☒ Sftp ☐ Ftp

Remote Storage Host : *

Port: *

Username: *

Password: *

Storage Path: *

Verify Remote Host

• Schedule: Select a schedule at which the machine is likely to be under the least load.

* = Required Fields

Explanation of Database Backup Schedule Fields

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



Note

Cisco strongly recommends scheduling regular backups of the database.

The Database Backup Schedule window contains the following fields:

- **Schedule**

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

- **Start Time (UTC)**

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

- **Frequency**

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

- Number of backup files to keep

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

- **Backup Type**

Choose Local or Remote to designate the server for backups. If you choose Remote, you must fill in the following values for the remote server:

- **Remote Storage Host (SFTP)**

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

- **Port**

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

- **User Name**

Username for login of the remote server.

- **User Password**

Password for login to the remote server.

- **Storage Path**

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

Step 13 Click **Finish**, located at the bottom of the window.

The Cisco TelePresence Manager admin window appears at http://server_hostname_or_IP_address.

Microsoft Exchange Calendar Service Window

The Microsoft Exchange Calendar Service window helps you manage the database that stores meeting information.

To test the connection between this system and the Microsoft Exchange server as shown in [Figure 8-10Microsoft Exchange Calendar Service Window](#):

Step 1 Click **Test Connection**.

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

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

**Note**

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

Figure 8-10 Microsoft Exchange Calendar Service Window

System Configuration > Microsoft Exchange

Service Status:	OK		
Mailbox Usage:	43.77% full (17508.0 of 40000.0 KB is used)		
Host:	<input type="text" value="tsbu-sr6"/>	*	
Bind Method:	<input type="radio"/> Secure <input checked="" type="radio"/> Normal		
Port:	<input type="text" value="80"/>	*	
Domain Name:	<input type="text" value="srdev.com"/>	*	
Logon Name:	<input type="text" value="SuperUser"/>		
SMTP LHS:	<input type="text" value="SuperUser"/>	*	
Password:	<input type="password" value="....."/>	*	
Certificate:	<input type="text"/>	<input type="button" value="Browse..."/>	
Number of Meetings Per Query:	<input type="text" value="100"/>	*	

* Required Fields

Synchronization Operations

Subscription Status: Room:

Showing 1 - 4 of 4 records

<input type="checkbox"/>	Room Name ▾	Last Synchronization Time (+)	Subscription Status
<input type="checkbox"/>	TelepresenceRoom34	✓ 12/08/2008 12:00 AM	Success
<input type="checkbox"/>	TelepresenceRoom32	✓ 12/08/2008 12:00 AM	Success
<input type="checkbox"/>	TelepresenceRoom31	✓ 12/08/2008 12:00 AM	Success
<input type="checkbox"/>	TelepresenceRoom33	✓ 12/08/2008 12:00 AM	Success

Rows Per Page:

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

Table 8-3 describes the information and operations accessible from this window.

Table 8-3 Microsoft Exchange Server

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

Table 8-3 **Microsoft Exchange Server (continued)**

Field	Description or Settings
Bind Method	Choose the Secure or Normal radio button to select the binding method, as follows: <ul style="list-style-type: none"> Secure—CTS-Manager communicates with the Microsoft Exchange server in secure mode using HTTPS. This method requires enabling Secure Socket Layer (SSL) on the Microsoft Exchange server. Normal—CTS-Manager communicates with the Microsoft Exchange server in cleartext using HTTP.
Port	Communication port number.
Domain Name	Domain name provided for the Microsoft Exchange server account, which can be changed.
Logon Name	This is the account name used to log on to the Microsoft Exchange server. The value is dependent on the AD/Exchange configuration. For example, it is either <i>ctsappaccount@mycompany.com</i> or <i>ctsappaccount</i> .
SMTP LHS	This is the left hand side (LHS) of the SMTP address for the account specified by the Logon Name. If the full SMTP address is <i>ctsappsmt@mycompany.com</i> enter <i>ctsappsmt</i> in this field.
Password	Password used to access the Microsoft Exchange server account, which can be changed.
Certificate	Use the field to provide a trust certificate for new Microsoft Exchange server.
Number of Meetings Per Query	The maximum number of meetings that CTS-Manager can retrieve from the Exchange server for each query. Cisco recommends that once set it not be modified.

Re-sync Operations

The Re-sync Operations area tells you when information in the Microsoft Exchange server database was last updated with meetings scheduled for a particular room.

When mismatched information in the databases causes meeting conflicts or there are other problems that prevent a meeting from being launched successfully, this area of the Microsoft Exchange window allows you to synchronize information between Microsoft Exchange and the CTS-Manager database. Synchronization takes time and system resources to accomplish and should be done only when necessary.

To synchronize information between Microsoft Exchange and the CTS-Manager database:

-
- Step 1** Check the boxes next to the rooms to select them. To synchronize information for all meeting rooms, check the box next to **Room Name** in the display header.
- Step 2** Click **Re-sync** to start the operation.
- Once you've begun the Re-sync operation the Service Status field displays a **Sync progress** indicator showing the progress of the Re-sync operation by percentage.
- Step 3** Once the synchronization operation completes, click **Refresh** to update the display.
- Step 4** Once the synchronization operation completes, click **Refresh** to update the display.
-

Table 8-4 describes the information displayed in this area of the Microsoft Exchange window.

**Note**

A maximum of 100 rooms are displayed per page. If you have more than 100 rooms registered with Cisco TelePresence Manager you can click the Next button to display the additional rooms.

Table 8-4 **Microsoft Exchange Server Synchronization Report**

Field	Description
Room Name	Name of the meeting room. Click the arrow in the header of the Room Name column to sort the list in ascending or descending alphabetical order.
Last Synchronization Time	Time the synchronization operation was started.
Subscription Status	Status of the synchronization operation. Click the arrow in the header of the Room Name column to sort the list in ascending or descending alphabetical order.
Room Filter	This allows you to filter your rooms to be displayed.

Initialization for IBM Domino Deployments

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

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

**Note**

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

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

Figure 8-11 **Initial Preferences Window**

To assist Cisco TelePresence System Manager in showing date and time properly, specify the location in which the computer is located.

Note that time zones of the same offset might or might not observe daylight saving time (DST). Ensure that appropriate location is selected.

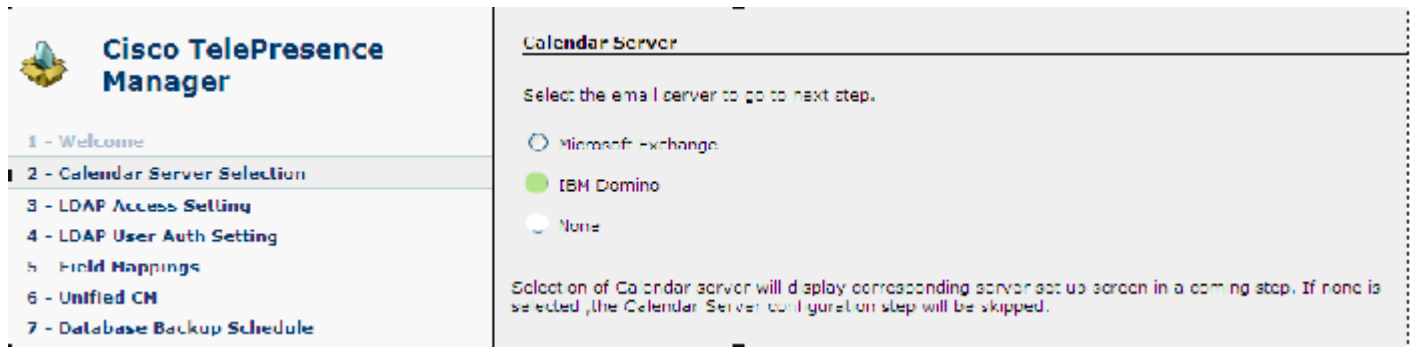
Browser's Location:	<input type="text"/>
Selected location observes DST:	<input type="checkbox"/>

Continue

- Step 3** At the product page that appears, click on **Cisco TelePresence Manager**.
- Step 4** At the login page, enter the username and password created during installation.
- The Cisco TelePresence Manager initial window appears with several fields already populated from the installation process and click **Next**.

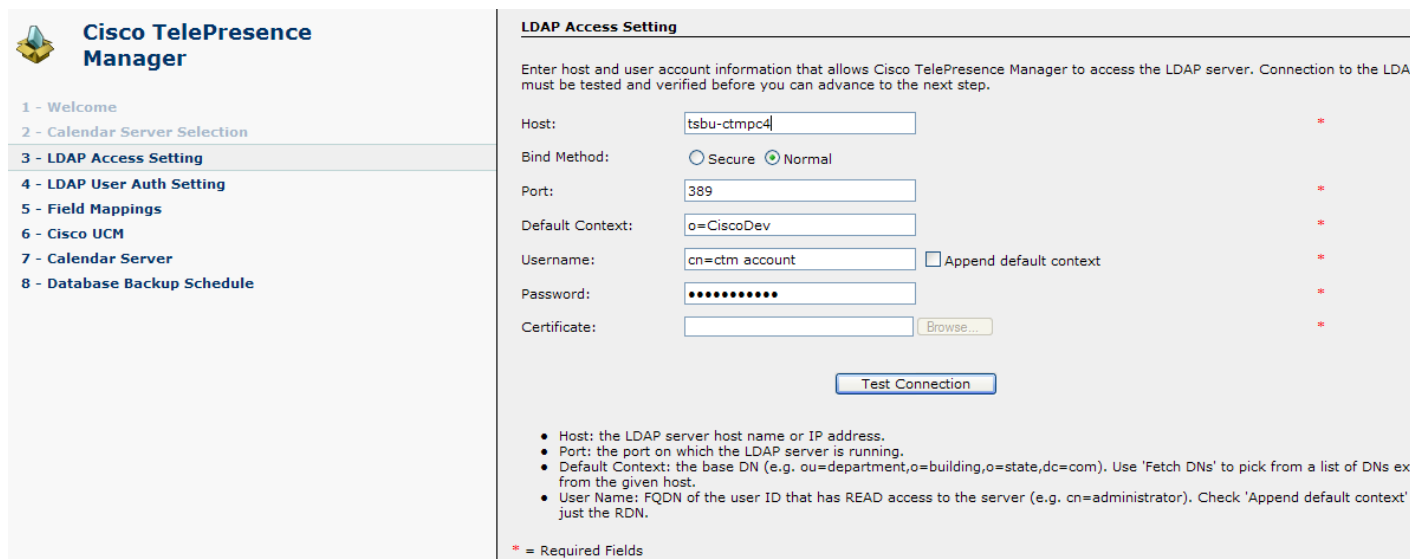
- Step 5** The Calendar Server Selection window is displayed. See [Figure 8-12](#).
Choose IBM Domino for this deployment and click **Next**.

Figure 8-12 Calendar Server Selection Window



- Step 6** The LDAP Access Setting window opens. See [Figure 8-13](#). Fill in the fields and click **Test Connection**.
The system tests the connection information. A popup window opens and displays “Connection Verified.” Click **OK**, then click **Next**.
- Note** If the system cannot verify the connection, the popup window directs the user to re-enter the information.

Figure 8-13 LDAP Access Setting Window



Explanation of LDAP Access Setting Fields

Lightweight Directory Access Protocol (LDAP) is a protocol definition for accessing directories. The LDAP Access Settings window specifies LDAP Active Directory server settings that are used by Cisco TelePresence Manager to access the directory information. This window contains the following fields:

- Host

The hostname is an alias that is assigned to an IP address for identification.

- Enter a hostname that is unique to your network.
- The hostname consists of up to 64 characters and can contain alphanumeric characters and hyphens, using English characters. International characters are not recognized.

- Bind Method

The bind method is the type of security required.

- Secure—Secure Socket Layer (SSL) connection requires the Distinguished Encoding Rules (DER) Certificate for the LDAP server. You must complete the Certificate field on this window before you can proceed.
- Normal—The Cisco TelePresence Manager communicates with the LDAP server in cleartext using HTTP. In normal mode, you do not need to complete the Certificate field.

- Port

- The default port for secure SSL connection is 636.
- The default port for normal connection for a single server is 389.

- Default Context

Default Context is the context from which the LDAP queries are performed. To change the default context, choose it in the Fetch DN's drop-down list adjacent to this field.

- Username

The username provides identification of the user to the LDAP server.

- The format must be in the LDAP fully qualified domain name (FQDN) format.
- Examples: cn=admin, cn=users, dc=<mydomain>, dc=com

- Append default context

Check this box to avoid typing in the LDAP Access username manually, keeping the requirements of the LDAP FQDN format. If this box is not checked, you must append the information in the Default Context field.

- Password

The user password allows access to the LDAP server.

The password must contain at least six characters and maximum 31 characters and should be unique using English characters only. It must start with a lowercase alphanumeric character. International characters are not valid.

- Certificate

The certificate is a digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

Step 7 The LDAP User Auth Setting window is displayed. See [Figure 8-14](#).

LDAP user containers should be added so that users are unique in these containers having no user overlap. If users belong to multiple user containers, for example, sales and HR, then only one container should be specified. If not the user, then the login to email link will fail. If the container at the organizational level is specified which will include everyone, then no other user container should be specified for the email link login to work. Fill in the fields and click **Verify Container DN**.

The system tests the container information. A popup window opens and displays “User container <...> validated successfully.” Click **OK**, then **Next**.

**Note**

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

Figure 8-14 LDAP User Authorization Settings Window

Cisco TelePresence Manager

1 - Welcome
2 - Calendar Server Selection
3 - LDAP Access Setting
4 - **LDAP User Auth Setting**
5 - Field Mappings
6 - Cisco UCM
7 - Calendar Server
8 - Database Backup Schedule

LDAP User Auth Setting

Enter the user container Relative Distinguished Names (RDNs) for LDAP users. The RDNs must be validated successfully before you advance to the next step.

Default Context: o=CiscoDev

User Containers: b=CiscoDev ☐ Append default context *

☐ Append default context

☐ Append default context

☐ Append default context

☐ Append default context

☐ Append default context

• Default Context: the DN that was entered in the previous screen.
• User Container: the DN of the container under which users can be found. Check 'Append default context' to enter just the RDN

* = Required Fields

Explanation of LDAP User Auth Setting Fields

The LDAP User Auth Setting window contains the following fields:

- User Containers

The FQDN format name of the LDAP container in which Cisco TelePresence Manager can find the list of users.


- Append default context

Check this box to meet the requirements of the LDAP FQDN format, or type in the Default Context after the User Container name yourself.

Step 8 The Field Mapping window is displayed. See [Figure 8-15](#).

The fields should be populated with information you have already entered.

Figure 8-15 Field Mappings Window



**Cisco TelePresence
Manager**

1 - Welcome

2 - Calendar Server Selection

3 - LDAP Access Setting

4 - LDAP User Auth Setting

5 - Field Mappings

6 - Cisco UCM

7 - Calendar Server

8 - Database Backup Schedule

Field Mappings

Select the object class and its attribute to map to the corresponding object field. Sample data must be visually verified before you advance to the next step.

Person

EmailID:

Person

DisplayName:

Person

Object Class

Attribute

cn

cn

View Sample Data

Explanation of Field Mappings Fields

These attributes are used by the Domino LDAP server to retrieve the user's e-mail and display name information. For most of the Domino deployments, this information does not have to be changed. If this information is stored in other attributes in the LDAP server, use the following steps to change the mapping:




Caution

The object and attribute mappings for Domino/Directory Server deployments are listed in [Table 8-5](#) and cannot be changed after installing and configuring CTS-Manager.

Table 8-5 LDAP Objects and Attributes

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



Note

For more information about Field Mapping, see the Cisco TelePresence Manager online help.

- Step 9

When all information has been entered, click **View Sample Data**.
A popup window opens and displays the data that has been entered, see [Figure 8-16](#). Review the information and verify that it is correct and complete, and click **Close**.
A popup window opens and displays the message “Does the data look correct to you?”
Click **OK**, then click **Next**.

Figure 8-16 System Configuration - LDAP Server

tsbu-ctm16 - Cisco TelePresence Manager -- Webpage Dialog

System Configuration > LDAP Server

Person	
EmailID --> Person:proxyaddresses	DisplayName --> Person:displayname
SMTP:Administrator@srdev.com	Administrator

EnterpriseConfRoom	
EmailID --> Person:proxyaddresses	DisplayName --> Person:displayname
SMTP:Administrator@srdev.com	Administrator

Close

Step 10 The Cisco **Unified CM** window is displayed. See [Figure 8-17](#).

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

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



Note

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

Figure 8-17 Cisco Unified CM Window

Cisco TelePresence Manager

- 1 - Welcome
- 2 - Calendar Server Selection
- 3 - LDAP Access Setting
- 4 - LDAP User Auth Setting
- 5 - Field Mappings
- 6 - Cisco UCM**
- 7 - Calendar Server
- 8 - Database Backup Schedule

Cisco UCM

Enter Cisco Unified Communications Manager resource properties. Connection to the Cisco UCM server must be tested and verified you can advance to the next step.

Host: *

Username: *

Password: *

Certificate: Browse... *

Test Connection

- Host: the Cisco CallManager appliance box hostname or IP address.
- User Name/Password: Application user name and password configured in CallManager to allow Cisco TelePresence Manager to

* = Required Fields

Explanation of Cisco Unified Communications Manager Fields

- **Host**

Host is the hostname or IP address of the Cisco Unified Communications Manager server host.

- **Username**

Username is the username for the application user for the Cisco Unified Communications Manager server.

- **Password**

The password allows the user to access the Cisco Unified Communications Manager.

- **Certificate**

The certificate is a digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

IBM Domino Calendar

The **IBM Domino** window next appears. See [Figure 8-18](#).

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

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



Note

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

Figure 8-18 IBM Domino Calendar Window

Cisco TelePresence Manager

- 1 - Welcome
- 2 - Calendar Server Selection
- 3 - LDAP Access Setting
- 4 - LDAP User Auth Setting
- 5 - Field Mappings
- 6 - Cisco UCM
- 7 - Calendar Server**
- 8 - Database Backup Schedule

IBM Domino

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

Host: *

Bind Method: ☐ Secure ☒ Normal

Port: *

Organization Name: *

Username: *

Password: *

Polling Interval(minutes): *

Certificate: *

- Host: the IBM Domino server host name or IP address.
- User Name/Password: user account that has read access to the Domino server.

* = Required Fields

Explanation of IBM Domino Fields

- **Host**

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

- **Bind Method**

The bind method indicates the desired level of security.

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

**Note**

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

- **Port**

The default value is 80.

- **Organization Name**

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

- **Username**

The username provides login access to the IBM Domino server.

- **Password**

The user password allows access to the IBM Domino server.

- **Polling Interval** (minutes)

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

- **Certificate**

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

**Note**

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

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

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

Dashboard for Verification of Installation Status

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

Figure 8-19 describes the dashboard report information. To update the reports, click **Refresh**.

Figure 8-19 Cisco TelePresence Manager Support - Dashboard Window

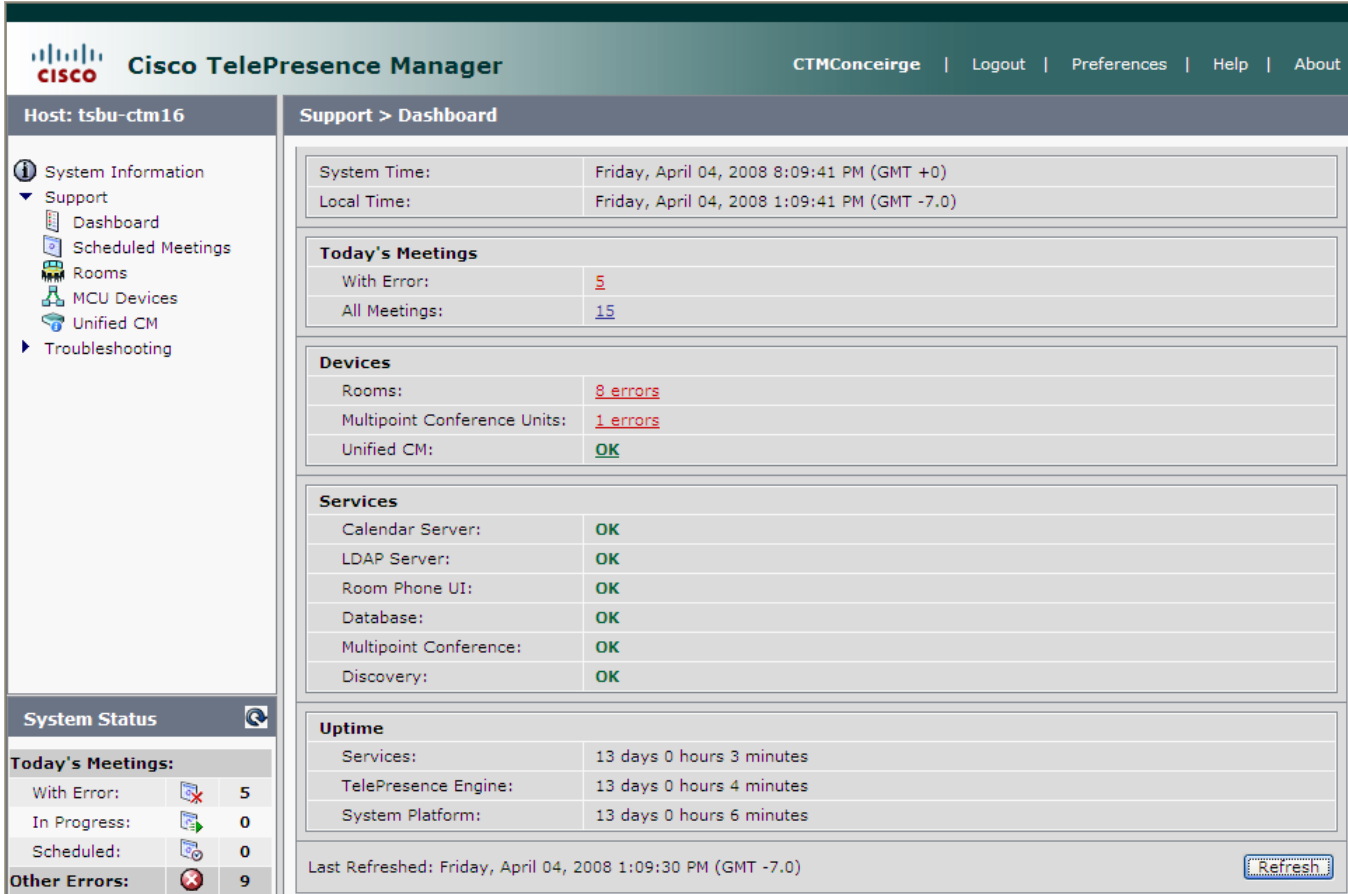


Table 8-6 Dashboard Report

Field	Description or Setting
System Time	Day, date, and time in coordinated universal time (UTC, formerly known as Greenwich mean time or GMT).
Local Time	Local day, date, and time.

Field	Description or Setting
Today's Meetings	<p>Status of current and upcoming meetings:</p> <ul style="list-style-type: none"> • With Error—Reports the number of meetings that have errors. • All Meetings—All meetings scheduled for today. <p>Click the link associated with each report to go to the Scheduled Meetings window.</p>
Devices	<p>Status report of the following devices:</p> <ul style="list-style-type: none"> • Cisco TelePresence rooms—Clicking the link displays the Status tab in the Support > Rooms window. • Multipoint Conference Units (MCUs)—Clicking the link displays the Support > Multipoint Conference Unit window and filters the list to those MCUs with an error status. • Cisco Unified CM—Clicking the link displays the Support > Unified CM window. <p>Note An error status may be reported if the connection to Cisco Unified CM was caused by a network outage. You can remove the error status by restarting CTS-Manager.</p>
Services	<p>Status report of following system services:</p> <ul style="list-style-type: none"> • Calendar Server • LDAP Server • Room Phone UI • Database • Multipoint Conference • Discovery <p>Status is either OK or is a highlighted link listing the number of errors. You can click a link to see further status information and resolve problems. You can also pass your mouse over a highlighted link to see a brief description of the error.</p>
Uptime	<p>Status reporting uptime since the last restart.</p> <ul style="list-style-type: none"> • Services refers to the list of services above. • TelePresence Engine refers to the Cisco TelePresence database engine. • System Platform refers to the hardware host for CTS-Manager.

