



- Quick Reference Guide**
- Cisco TelePresence MX Series
  - Cisco TelePresence EX Series
  - Cisco TelePresence SX Series
  - Cisco TelePresence Codec C Series
  - Cisco TelePresence Quick Set C20
  - Cisco TelePresence Profile Series
  - Cisco Unified Communications Manager

Software versions TC7.2 and  
Cisco Unified Communications Manager 10.5.1  
NOVEMBER 2014

Thank you for choosing Cisco TelePresence!

Your Cisco product has been designed to give you many years of safe, reliable operation.

This part of the product documentation is aimed at administrators working with the setup of the TelePresence endpoints on Cisco Unified Communications Manager.

Our main objective with this guide is to address your goals and needs. Please let us know how well we succeeded! Go to the feedback page, click [here...](#)

May we recommend that you visit the Cisco web site regularly for updated versions of this guide. Go to:

▶ <http://www.cisco.com/go/telepresence/docs>

How to use this guide

The top menu bar and the entries in the Table of contents are all hyperlinks. You can click on them to go to the topic.

## Table of contents

<b>Introduction.....</b>	<b>4</b>	Extension information .....	20
Introduction .....	5	Product specific configuration layout .....	21
Prerequisites.....	5	Adding the directory number .....	35
Recommended sequence when configuring .....	5	Directory number information.....	35
About device packages.....	5	Configuring shared lines.....	36
Encrypted vs non-encrypted communication .....	5	Display the name of the caller .....	36
About endpoints previously used with TMS.....	5	Auto-registration of the endpoint .....	37
About endpoints factory reset.....	5	Enable auto-registration .....	37
About software versions.....	6	How to verify the endpoint registration.....	38
Endpoints supported in TC7.2 .....	6	Specify the home cluster service for the end user .....	39
CUCM versions vs endpoints supported .....	6	Associate a user with an access control group .....	40
Option package for C20 .....	6	Add the user to an access control group .....	40
CTI monitoring support for CTS Manager .....	6	Enterprise parameters .....	41
Limitations .....	6	Clusterwide Domain Configuration .....	41
Useful links .....	6	<b>Endpoint configuration.....</b>	<b>42</b>
What's new in this version .....	7	About endpoint configuration .....	43
CUCM support for endpoints outside of the enterprise network via Expressway.....	7	Endpoint diagnostic tools .....	43
Support for product specific configuration .....	7	Endpoint configuration in three steps.....	43
<b>CUCM configuration .....</b>	<b>8</b>	Setting the system password .....	44
Logging in to Cisco Unified CM Administration .....	9	Setting the call details.....	45
Creating a SIP profile .....	10	Setting up CUCM provisioning.....	46
SIP Profile configuration .....	10	Setting up provisioning from CUCM via Expressway (Mobile and Remote Access).....	47
About the phone security profile .....	11	Verifying the identity of the Expressway .....	47
About non-secure and secure profiles .....	11	Verifying the endpoint registration.....	49
Creating a phone security profile.....	12	Making a call.....	49
Phone security profile information.....	12	Checking the system information .....	49
Phone security profile CAPF information .....	13	<b>About passwords.....</b>	<b>50</b>
Manual registration of the endpoint .....	14	Setting the system password .....	51
Adding a new phone (endpoint) .....	14	Changing your own system password .....	51
Device information.....	15	Changing another user's system password.....	51
Protocol specific information.....	17	Setting the menu password .....	52
Certification authority proxy function information .....	18	Setting the menu password from the web interface.....	52
External Data Locations information.....	19	Setting the menu password using the remote control.....	52



**Appendices..... 53**  
About ad hoc conferencing ..... 54  
About shared lines ..... 54  
About endpoint provisioning ..... 54  
The TelePresence endpoint user interfaces ..... 55  
    Using the Touch panel ..... 55  
    Using the web interface ..... 55  
    Using the TRC5 remote control ..... 55  
    Using the command line interface ..... 55  
Collecting log files from a TelePresence endpoint ..... 56  
Factory resetting the TelePresence endpoint ..... 57  
Finding the MAC address of the endpoint ..... 58  
Creating a remote support user ..... 59  
Understanding Cisco Discovery Protocol on the  
Cisco TelePresence endpoints ..... 60  
User documentation on the Cisco web site ..... 63  
**Cisco contacts ..... 64**

## CHAPTER 1

### INTRODUCTION

This chapter gives an overview of what is important to know before you start to configure the Cisco Unified Communications Manager and the TelePresence endpoints.



## Introduction

This document describes the tasks you must perform to register a Cisco TelePresence endpoint (C, EX, MX, SX, and Profile Series) on Cisco Unified Communications Manager (CUCM).

Note that endpoints can register to CUCM also when the endpoint is not within the enterprise network. In such cases you will need a VCS Expressway for secure firewall traversal and line-side support for CUCM registrations. This feature is also referred to as Cisco Unified Communications Mobile and Remote Access, and is a core part of the Cisco Collaboration Edge Architecture.

The software versions referred to in this document are the TelePresence endpoints TC7.2 and CUCM 10.5.1. Cisco recommends using the latest software versions to support all features and functions described in this guide.

Most features/configurations also applies to CUCM versions 8.6.2 and 9.1.2, but some menus may have changed in newer versions of the CUCM. Make sure you have the latest device package.

## Prerequisites

Users of this guide are assumed to be familiar with the basics of the user interface of the CUCM and the Cisco TelePresence endpoints.

## Recommended sequence when configuring

Note that we recommend doing the CUCM configuration before the endpoint provisioning.

1. *First*, configure the CUCM.
2. *Next*, provision the endpoint.

Be aware that HTTP (web interface) and SSH (used for command line) may be disabled in the endpoint configuration on CUCM. This will prevent access to the endpoint's web interface and command line interface. See "[Product specific configuration layout](#)" on page 21 how to enable/disable Web access and SSH access.

## About device packages

The Cisco Unified CM Device Package contains device configuration capabilities for the Cisco TelePresence endpoints. The device package is available for download on our web site.

Go to: <http://software.cisco.com/download/navigator.html> and navigate to Unified Communications > Call Control > Cisco Unified Communications Manager (CallManager) and choose the desired version, then choose Unified Communications Manager/CallManager Device Packages.

To find which device packages are available for which CUCM version and endpoint, go to: [http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/compat/devpack\\_comp\\_mtx.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html)

## Encrypted vs non-encrypted communication

The deployment is considered non-secure with a standard phone profile (non-encrypted file exchange). When higher security is required choose a phone security profile to obtain encrypted file exchange and secure transport between the endpoint and CUCM.

## About endpoints previously used with TMS

If the endpoint has previously been used with Cisco TelePresence Management Suite (TMS), make sure the endpoint is purged from TMS unless you still want TMS to be able to manage this endpoint's bookings. In the latter case, please see [Cisco TelePresence Management Suite Administrator Guide](#) for instructions on how to handle endpoint migration to CUCM in TMS.

## About endpoints factory reset

In most cases a factory reset of the endpoint is not needed before provisioning it to the CUCM. But, in some cases it is recommended to factory reset the endpoint before provisioning:

- When the system has been used with Cisco TelePresence Management Suite (TMS), or a similar system.
- When the system is re-deployed to another user.
- When changing the security configuration.
- When moving the system to another security environment.

Factory reset is described in the Appendices section. Refer to "[Factory resetting the TelePresence endpoint](#)" on page 57.

## About software versions

Before you start configuring, make sure the endpoints and CUCM have the correct software installed, and the correct device package installed on CUCM (see the previous page for details).

### Endpoints supported in TC7.2

TelePresence endpoints supported in TC7.2:

- SX Series (SX10, SX20, SX80)
- MX Series (MX200, MX300, MX200 G2, MX300 G2, MX700, MX800)
- EX Series (EX90, EX60)
- Quick Set C20 and Codec C Series (C90, C60, C40)
- Profiles using Codec C Series

### CUCM versions vs endpoints supported

All TelePresence endpoints that are supported in TC7.2 are also supported in CUCM 8.6.2, 9.1.2 and 10.5.1. Use the latest device package to be sure all endpoints are covered.

**NOTE:** Endpoint registration to CUCM via VCS Expressway (Cisco Unified Communications Mobile and Remote Access) requires CUCM version 9.1.2 SU1 or later.

You can find an overview of which device packages are available for which CUCM version and endpoint in the CUCM device pack compatibility matrix on our web site. Go to:

▶ [http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/compat/devpack\\_comp\\_mtx.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/devpack_comp_mtx.html)

### Option package for C20

Note that the C20 must have high definition/premium resolution option to interoperate with CTMS.

### CTI monitoring support for CTS Manager

To enable CTI monitoring support for CTS Manager you will need:

- Cisco Unified Communications Manager version 8.6.2 or later.
- Cisco TelePresence MultiPoint Switch – CTMS 1.8 or later.
- Cisco TelePresence Manager – CTS-MAN 1.8 or higher.

### Limitations

CUCM 9.0 does not support Directory URI provisioning of the TelePresence endpoint. You will need CUCM 9.1 or later.

### Useful links

User documentation and software download for the TelePresence endpoints:

▶ <http://www.cisco.com/go/telepresence/docs>

User documentation and software download for CUCM:

▶ <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>

Cisco support and software download page:

▶ <http://www.cisco.com/cisco/web/support/index.html>

Cisco TelePresence TC Release Notes:

▶ <http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-integrator-c-series/products-release-notes-list.html>

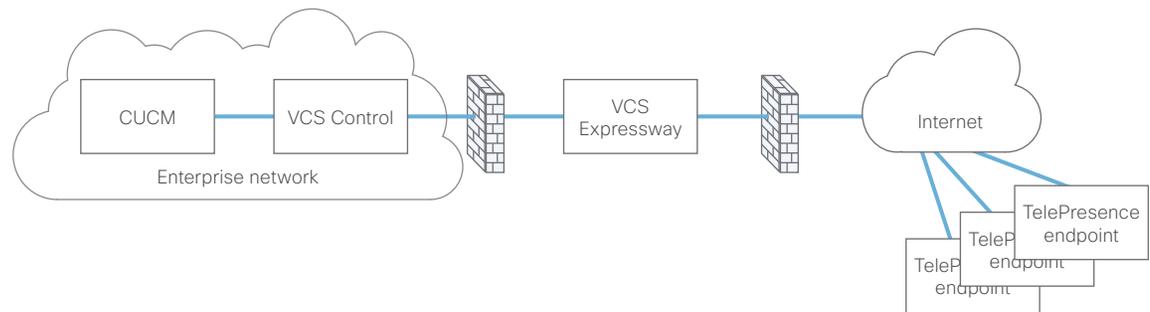
## What's new in this version

This section provides an overview of the new and changed features since the previous version of this guide was issued (TC7.0 on CUCM version 9.1.2). The CUCM must have a device package with support for TC7.2. See the [TC Release Notes](#) for detailed information.

### CUCM support for endpoints outside of the enterprise network via Expressway

Note that endpoints can register to CUCM also when the endpoint is not within the enterprise network. In such cases you will need a VCS Expressway for secure firewall traversal and line-side support for CUCM registrations. See illustration below.

This feature is also referred to as Cisco Unified Communications Mobile and Remote Access, and is a core part of the Cisco Collaboration Edge Architecture.



### Support for product specific configuration

Additional product specific configurations can be provisioned from CUCM, e.g.

- Default volume
- Max total upstream rate
- Max total downstream rate
- System name
- Standby action

## CHAPTER 3

### CUCM CONFIGURATION

This chapter describes the steps required to configure the Cisco Unified Communications Manager for TelePresence endpoints.



## Logging in to Cisco Unified CM Administration

Open a web browser and enter the host name or IP address of the Cisco Unified CM and select *Cisco Unified Communications Manager* from the list of installed applications.

1. Select *Cisco Unified CM Administration* from the *Navigation* drop down list and press **Go**.
2. Enter your *user name* and *password* and click **Login**.

**TIP:** You can bypass the first page and go directly to the *Cisco Unified CM Administration* login page (the graphic shown on this page):

- `http://your-cm-server-name/ccmadmin`
- `http://<ip address>/ccmadmin`

Navigate to: *Cisco Unified Communication Manager* > *Cisco Unified CM Administration*.

Copyright © 1999 - 2012 Cisco Systems, Inc. All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

**1** Select *Cisco Unified CM Administration* from the *Navigation* drop down list and press **Go**.

**2** Enter your *user name* and *password* and click **Login**.

Mandatory  Optional

## Creating a SIP profile

You can copy a profile to use as a template.

Click *Find* to list all profiles. Select the one you would like to copy and choose *Copy*; or click *Add New* to add a new profile. This will open the *SIP Profile Configuration* page.

### SIP Profile configuration

Navigate to the *SIP Profile Information* section:

*Name*: Enter the **Name** for the profile.

*Use Fully Qualified Domain Name in SIP Requests*:

**Enable** by checking the checkbox to enable the called endpoint to return the call using the received or missed call list (the history list). See also "[Clusterwide Domain Configuration](#)" on page 41.

*SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*: Set to **TIAS and AS**.

Navigate to the *Trunk Specific Configuration* section:

*Allow Presentation Sharing using BFCP*: **Enable** by checking the checkbox to allow presentation sharing.

*Allow IX Application Media*: **Enable** by checking the checkbox. This will enable the ActiveControl feature, if available on the endpoint.

When done click **Save**.

Navigate to: *Device > Device Settings > SIP Profile*.

Add New or Copy a profile and navigate to the **SIP Profile Information** section.

Navigate to the **Trunk Specific Configuration** section.

Mandatory  Optional

## About the phone security profile

Security profiles must be defined when using secure (encrypted) communication, else you will use the default *non-secure phone security profile* for your product.

Note the following:

- CUCM must operate in mixed mode (cluster security mode) to enable secure communication.
- You must define one device security profile for each endpoint type.
- If you want to allow several authentication modes for the same endpoint type, you must define one profile for each mode.
- See the CUCM Security Guide for further information: [http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/security/10\\_0\\_1/secugd/CUCM\\_BK\\_C68276B4\\_00\\_cucm-security-guide-100.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/10_0_1/secugd/CUCM_BK_C68276B4_00_cucm-security-guide-100.html)

## About non-secure and secure profiles

A profile's security mode is defined by the *Device Security Mode* parameter (see next page). TelePresence endpoints support **Non-secure** and **Encrypted** modes; they do not support Authenticated mode. Endpoints connected to CUCM via Expressway support only **Non-secure** mode.

### Non-secure profile

The non-secure endpoints will use the **predefined non-secure profile**. If this is your option you can proceed to: "[Manual registration of the endpoint](#)" on page 14.

### Secure (Encrypted) profile

When configuring a secure device for the first time, you can copy a predefined non-secure profile to use as a template. This is the method used in this section.

You may also choose *Add New*, and then choose the type of TelePresence endpoint for the *phone security profile*.

The page content will be the same using one or another method, but the default values may vary.

Navigate to: *System > Security > Phone Security Profile.*

Click **Add New** on the *Find and List Phone Security Profiles* page.

### Editing a security profile

The non-secure endpoints will use the predefined non-secure profile. No action required.

### Creating a security profile

When registering a **secure device** for the first time, copy the predefined non-secure profile to use as a template.

Mandatory  Optional

## Creating a phone security profile

### Phone security profile information

Only applicable for secure (encrypted) profiles; not applicable for endpoints connected to CUCM via Expressway.

Navigate to the *Phone Security Profile Information* section:

*Name:* Enter a name of the profile.

*Description:* Enter a description of the profile.

*Device Security Mode:* Set to Encrypted.

*Transport Type:* Set to TLS.

*TFTP Encrypted Config:* Check this check box to enable TFTP encrypted configuration.

When done click **Save**.

Navigate to: *System > Security > Phone Security Profile*.

Navigate to the **Phone Security Profile Information** section.

**Phone Security Profile Configuration**
Related Links: [Back To Find/L](#)

Save

**Status**

Status: Ready

**Phone Security Profile Information**

**Product Type:** Cisco TelePresence MX300

**Device Protocol:** SIP

**Name\*** Cisco TelePresence MX300 - Security Profile

**Description** Cisco TelePresence MX300 - Security Profile

**Nonce Validity Time\*** 600

**Device Security Mode** Encrypted

**Transport Type\*** TLS

Enable Digest Authentication

TFTP Encrypted Config

Exclude Digest Credentials in Configuration File

**Phone Security Profile CAPF Information**

**Authentication Mode\*** By Null String

**Key Size (Bits)\*** 1024

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

**SIP Phone Port\*** 5060

Save

■ Mandatory ■ Optional

## Creating a phone security profile

### Phone security profile CAPF information

Only applicable for secure (encrypted) profiles; not applicable for endpoints connected to CUCM via Expressway.

Navigate to the *Phone Security Profile CAPF Information* section:

*Authentication Mode:* Choose the appropriate value from the drop down list.

*By Null String:* The Certificate Authority Proxy Function (CAPF) process will start automatically. This is the default value.

*By Authentication String:* The CAPF process will commence when the correct authentication code is received from the endpoint.

**NOTE:** The combination of encrypted configuration file and CAPF authentication mode "authenticating string" is not supported on the TelePresence endpoint side in software version TC6.2/TC6.3.

*By Existing Certificate (precedence to LSC/MIC):* This option can only be used when a Locally Significant Certificate (LSC) is already stored on the endpoint, i.e. it cannot be used the first time the CAPF process runs.

*Key-size:* Choose the appropriate value from the drop down list. *The recommended key size is 1024.*

When done click **Save**.

Navigate to: *System > Security > Phone Security Profile.*

Navigate to the **Phone Security Profile CAPF Information** section.

**Phone Security Profile Configuration**
Related Links: [Back To Find/L](#)

Save

**Status**

Status: Ready

**Phone Security Profile Information**

**Product Type:** Cisco TelePresence MX300

**Device Protocol:** SIP

**Name\***

**Description**

**Nonce Validity Time\***

**Device Security Mode**

**Transport Type\***

Enable Digest Authentication

TFTP Encrypted Config

Exclude Digest Credentials in Configuration File

**Phone Security Profile CAPF Information**

**Authentication Mode\***

**Key Size (Bits)\***

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

**SIP Phone Port\***

Mandatory  Optional

## Manual registration of the endpoint

**i** Manual registration of the TelePresence endpoint is required when the CUCM is set to mixed mode (cluster security mode).

### Adding a new phone (endpoint)

Click *Add New* to add a new phone (endpoint).

Navigate to *Create a phone using the phone type or a phone template* section.

- From the drop down list, choose the type of TelePresence endpoint you are going to register.

Click **Next**.

Navigate to: *Device > Phone*.

Click **Add New** on the *Find and List Phones* page.

Navigate to **Create a phone using the phone type or a phone template** section.

Mandatory  Optional

## Manual registration of the endpoint

### Device information

Navigate to the *Device Information* section:

*MAC Address:* Enter the *MAC Address* of the TelePresence endpoint. Format: XXXXXXXXXXXX, 12-character, hexadecimal (0-9 and A-F) number.

For information on how to find the MAC address, see: "[Finding the MAC address of the endpoint](#)" on page 58.

*Device Pool:* Choose a Device Pool.

*Phone Button Template:* Choose a Phone Button Template.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page).*

Navigate to the **Device Information** section.

**Phone Type**

**Product Type:** Cisco TelePresence MX300  
**Device Protocol:** SIP

---

**Device Information**

Device is Active  
 Device is trusted

MAC Address*	001122334455	
Description	SEP001122334455	
Device Pool*	-- Not Selected --	<a href="#">View Details</a>
Common Device Configuration	< None >	<a href="#">View Details</a>
Phone Button Template*	Standard Cisco TelePresence MX300	
Common Phone Profile*	Standard Common Phone Profile	<a href="#">View Details</a>
Calling Search Space	< None >	
AAR Calling Search Space	< None >	
Media Resource Group List	< None >	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	
Location*	Hub_None	
AAR Group	< None >	
User Locale	< None >	
Network Locale	< None >	
Privacy*	Default	
Device Mobility Mode*	Default	<a href="#">View Current Dev Mobility Settings</a>
Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)	
Owner User ID*	myuserid	<b>Find</b>
Phone Load Name		

Mandatory  Optional

## Manual registration of the endpoint

### Device information

Continued from the previous page...

Only applicable for TelePresence endpoints connected to CUCM via Expressway.

Navigate to the *Device Information* section:

If the TelePresence endpoint is connected to CUCM via Expressway, the following fields are mandatory:

*Owner:* Choose *User* to define that it is a personal endpoint.

*Owner User ID:* Enter the User ID of the appropriate user. Refer to the [CUCM administrator guide](#) for details about CUCM end user management.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page).*

Navigate to the **Device Information** section.

**Phone Type**

**Product Type:** Cisco TelePresence MX300  
**Device Protocol:** SIP

---

**Device Information**

Device is Active  
 Device is trusted

MAC Address*	<input type="text" value="001122334455"/>	
Description	<input type="text" value="SEP001122334455"/>	
Device Pool*	-- Not Selected --	<a href="#">View Details</a>
Common Device Configuration	< None >	<a href="#">View Details</a>
Phone Button Template*	Standard Cisco TelePresence MX300	
Common Phone Profile*	Standard Common Phone Profile	<a href="#">View Details</a>
Calling Search Space	< None >	
AAR Calling Search Space	< None >	
Media Resource Group List	< None >	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	
Location*	Hub_None	
AAR Group	< None >	
User Locale	< None >	
Network Locale	< None >	
Privacy*	Default	
Device Mobility Mode*	Default	<a href="#">View Current Dev Mobility Settings</a>
Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)	
Owner User ID*	<input type="text" value="myuserid"/> <input type="button" value="Find"/>	
Phone Load Name	<input type="text"/>	

Mandatory  Optional

## Manual registration of the endpoint

### Protocol specific information

Navigate to the *Protocol Specific Information* section:

*Device Security Profile:* If using a non-secure communication choose the default *non-secure phone security profile* for your product. If using a secure (encrypted) communication choose the *phone security profile* you previously defined.

*SIP Profile:* Choose the SIP Profile you previously defined.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page).*

Navigate to the **Protocol Specific Information** section.

Protocol Specific Information	
Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco TelePresence MX300 - Standard SIP Non-Secur
Rerouting Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile For TelePresence Conferencing
Digest User	< None >

Mandatory  Optional

## Manual registration of the endpoint

### Certification authority proxy function information

**Only applicable when:**

1. Registering an endpoint for the first time; and the endpoint is configured for secure (encrypted) communication.
2. Registering an endpoint after it has been factory reset; and the endpoint is configured for secure (encrypted) communication.

**Not applicable for TelePresence endpoints connected to CUCM via Expressway.**

Navigate to the *Certification Authority Proxy Function (CAPF) Information* section:

*Certificate Operation:* If using a secure profile, set to *Install/Upgrade*. Only required the first time the endpoint is registering. After the certificate has been downloaded to the endpoint, this setting will automatically resume to *No pending Operation*.

*Authentication Mode:* Choose the appropriate value from the drop down list.

*By Null String:* The Certificate Authority Proxy Function (CAPF) process will start automatically. This is the default value.

*By Authentication String:* The CAPF process will commence when the correct authentication code is received from the endpoint.

*By Existing Certificate (precedence to LSC/MIC):* This option can only be used when a Locally Significant Certificate (LSC) is already stored on the endpoint, i.e. it cannot be used the first time the CAPF process runs.

*Key-size:* Choose the appropriate value from the drop down list. The recommended key size is 1024.

*Operation Completes By:* Make sure the date and time are set to a future date and time. If set to the past the installation/upgrade will not be performed.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Certification Authority Proxy Function (CAPF) Information** section.

**Certification Authority Proxy Function (CAPF) Information**

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Size (Bits)*	1024
Operation Completes By	2014 01 01 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None  
Note: Security Profile Contains Addition CAPF Settings.

**External Data Locations Information (Leave blank to use default)**

Information	<input type="text"/>
Directory	<input type="text"/>

Mandatory  Optional

## Manual registration of the endpoint

### External Data Locations information

Navigate to the *External Data Locations Information* section:

Leave all fields blank to accept the default settings.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page).*

Navigate to the **External Data Location Information** section.

**External Data Locations Information (Leave blank to use default)**

Information	<input type="text"/>
Directory	<input type="text"/>
Messages	<input type="text"/>
Services	<input type="text"/>
Authentication Server	<input type="text"/>
Proxy Server	<input type="text"/>
Idle	<input type="text"/>
Idle Timer (seconds)	<input type="text"/>
Secure Authentication URL	<input type="text"/>
Secure Directory URL	<input type="text"/>
Secure Idle URL	<input type="text"/>
Secure Information URL	<input type="text"/>
Secure Messages URL	<input type="text"/>
Secure Services URL	<input type="text"/>

**Extension Information**

Mandatory  Optional

## Manual registration of the endpoint

### Extension information

Navigate to the *Extension Information* section:

*Enable Extension Mobility:* Check this check box to enable extension mobility.

*Log Out Profile:* Choose a device profile for the endpoint that will be used when no one is logged in to the device by using Cisco Extension Mobility.

*Log In Time:* This field remains blank until a user logs in. When a user logs in, the time at which the user logged in displays in this field.

*Log Out Time:* This field remains blank until a user logs in. When a user is logged in, the time at which the system will log out the user displays in this field.

**NOTE:** For further details on how to setup Extension Mobility, refer to the Features and Services guide for CUCM. Go to: <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page).*

Navigate to the **Extension Information** section.

**Secure Services URL**

**Extension Information**

Enable Extension Mobility

Log Out Profile -- Use Current Device Settings --

Log in Time

Log out Time

**MLPP and Confidential Access Level Information**

MLPP Profile

MLPP Security

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Navigate to the *Product Specific Configuration Layout* section:

If registered to TMS (Cisco TelePresence Management Suite) or CTSMAN (Cisco TelePresence Manager), configure the product specific configuration layout as appropriate.

*Room Name (from Exchange(R))*: This is the Exchange Conference Room Name. It is used for scheduling meetings where this TelePresence system participates. This setting must match the e-mail address used in Exchange exactly. Example: room123@example.com. Default value is "" (empty) and maximum length is 64 characters.

*Web Access*: This parameter indicates whether the device accepts connections from a web browser or other HTTP clients. Disabling the web server functionality of the device will block access to the TelePresence system's internal web pages and certain support capabilities, but will not degrade normal operation. Default value is *Disabled*.

**NOTE:** For the Web Access configuration change to take effect, please make sure to *Save* and *RESET* the device (do not use Restart or Apply Config).

*SSH Access*: This parameter indicates whether the device accepts SSH connections. Disabling the SSH server functionality of the device will block certain support capabilities such as log file collection but will not degrade normal operation. Default value is *Disabled*.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

Product Specific Configuration Layout	
	Parameter Value
Room Name (from Exchange(R))	
Web Access*	Enabled
SSH Access*	Enabled
Default Call Protocol*	SIP
Quality Improvement Server	
Multipoint Mode*	Use Media Resource Group List
Telnet Access*	Off
Microphone Unmute On Disconnect*	On
Call Logging Mode*	On
OSD Encryption Indicator*	Auto
Alternate phone book server type*	UDS
Alternate phone book server address	
Default Volume	70
Max Total Downstream Rate	10000
Max Total Upstream Rate	10000
System Name	
<b>CTMS Settings</b>	
CTMS Multiparty Conferencing*	On
CTMS Encryption Mode*	Off
<b>Far End Camera Control Settings</b>	
Far End Camera Control*	On
Far End Camera Control Signaling Capability*	On

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout* section:

If registered to TMS (Cisco TelePresence Management Suite) or CTSMAN (Cisco TelePresence Manager), configure the product specific configuration layout as appropriate.

*Default Call Protocol:* This parameter sets the default call protocol of the device. This device only supports SIP when registering to CUCM. Default value is SIP.

*Quality Improvement Server:* Specify a host name or IP address of a remote system to collect quality improvement reports from the device. Default value is "" (empty) and maximum length is 256 characters.

*Multipoint Mode:* Endpoints that do not have a built-in MultiSite feature can use the ad hoc conference bridge on CUCM.

- Choose *Use Endpoint* to use the *built-in MultiSite* feature.

**NOTE:** Applies to endpoints having MultiSite capability and having the option key installed.

- Choose *Use Media Resource Group List* to use the Conference Bridge (media resources) feature on CUCM. This will enable the ad hoc conferencing feature and applies to non-MultiSite endpoints.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page).*

Navigate to the **Product Specific Configuration Layout** section.

Product Specific Configuration Layout		Parameter Value	Override Common S
Room Name (from Exchange(R))			
Web Access*	Enabled		
SSH Access*	Enabled		
Default Call Protocol*	SIP		
Quality Improvement Server			
Multipoint Mode*	Use Media Resource Group List		
Telnet Access*	Off		
Microphone Unmute On Disconnect*	On		
Call Logging Mode*	On		
OSD Encryption Indicator*	Auto		
Alternate phone book server type*	UDS		
Alternate phone book server address			
Default Volume	70		
Max Total Downstream Rate	10000		
Max Total Upstream Rate	10000		
System Name			
<b>CTMS Settings</b>			
CTMS Multiparty Conferencing*	On		
CTMS Encryption Mode*	Off		
<b>Far End Camera Control Settings</b>			
Far End Camera Control*	On		
Far End Camera Control Signaling Capability*	On		
<b>Facility Service Settings</b>			

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout* section:

Configure the product specific configuration layout settings as appropriate.

*Telnet Access:* Set the network services Telnet mode (On/Off). Default value is On.

*Microphone Unmute On Disconnect:* Set the microphone mute mode (On/Off) to determine if the microphones shall be unmuted automatically when calls are disconnected. Default value is On.

- *Off:* If muted during a call, let the microphones remain muted after the call is disconnected.
- *On:* Unmute the microphones after the call is disconnected.

*Call Logging Mode:* Set the call logging mode (On/Off) for calls that are received or placed by the system. Default value is On.

*OSD Encryption Indicator:* Define for how long the encryption indicator (a padlock) will be shown on screen (Auto/AlwaysOn/AlwaysOff). The setting applies to both encrypted and non-encrypted calls, i.e. both to secure and non-secure conferences. Default value is Auto.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page).*

Navigate to the **Product Specific Configuration Layout** section.

Product Specific Configuration Layout		Parameter Value	Override Common S
Room Name (from Exchange(R))			
Web Access*	Enabled		
SSH Access*	Enabled		
Default Call Protocol*	SIP		
Quality Improvement Server			
Multipoint Mode*	Use Media Resource Group List		
Telnet Access*	Off		
Microphone Unmute On Disconnect*	On		
Call Logging Mode*	On		
OSD Encryption Indicator*	Auto		
Alternate phone book server type*	UDS		
Alternate phone book server address			
Default Volume	70		
Max Total Downstream Rate	10000		
Max Total Upstream Rate	10000		
System Name			
<b>CTMS Settings</b>			
CTMS Multiparty Conferencing*	On		
CTMS Encryption Mode*	Off		
<b>Far End Camera Control Settings</b>			
Far End Camera Control*	On		
Far End Camera Control Signaling Capability*	On		
<b>Facility Service Settings</b>			

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Navigate to the *Product Specific Configuration Layout* section:

If you want the endpoint to use the phone book from TMS (Cisco TelePresence Management Suite) configure the product specific configuration layout as appropriate.

**NOTE:** TMS supports this feature from software release 14.4.

**NOTE:** CUCM will have support for this feature in a device package which will be released sometime after TC7.

*Alternate phone book server type:* By default the endpoint uses the UDS server on the UCM it is registered to, but if you wish to use an alternate phone book server, this parameter combined with an alternate phone book address will override the default setting of the endpoint.

- Set to TMS if using the phone book from the Cisco TelePresence Management Server.
- Set to UDS if using the directory from the User Data Service in CUCM.

*Alternate phone book server address:* Enter the address to the phone book server. The field requires a full URL.

- Example with UDS:  
https://uds-host-name:8443/cucm-uds/users.
- Example with TMS:  
https://tms-host-name/tms/public/external/phonebook/phonebookservice.asmx.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

Product Specific Configuration Layout		Parameter Value	Override Common S
Room Name (from Exchange(R))			
Web Access*	Enabled		
SSH Access*	Enabled		
Default Call Protocol*	SIP		
Quality Improvement Server			
Multipoint Mode*	Use Media Resource Group List		
Telnet Access*	Off		
Microphone Unmute On Disconnect*	On		
Call Logging Mode*	On		
OSD Encryption Indicator*	Auto		
Alternate phone book server type*	UDS		
Alternate phone book server address			
Default Volume	70		
Max Total Downstream Rate	10000		
Max Total Upstream Rate	10000		
System Name			
<b>CTMS Settings</b>			
CTMS Multiparty Conferencing*	On		
CTMS Encryption Mode*	Off		
<b>Far End Camera Control Settings</b>			
Far End Camera Control*	On		
Far End Camera Control Signaling Capability*	On		
<b>Facility Service Settings</b>			

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Navigate to the *Product Specific Configuration Layout* section:

If you want the endpoint to use the phone book from TMS (Cisco TelePresence Management Suite) configure the product specific configuration layout as appropriate.

*Default Volume:* Set the default speaker volume. The volume returns to this value when you switch on or restart the video system.

*Max Total Downstream Rate:* Specify the maximum overall receive bit rate allowed (kbps).

*Max Total Upstream Rate:* Specify the maximum overall transmit bit rate allowed (kbps).

*System Name:* Specify a host name for the endpoint.

When done click **Save**.

### About Max Total Downstream/Upstream Rate

In a point-to-point call, the downstream and upstream rates will not exceed 6000 kbps.

When using a video system's built-in MultiSite feature (optional) to host a video conference, the total rate will be divided fairly among all active calls. The maximum total rate is 10000 kbps.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

**Product Specific Configuration Layout**

	Parameter Value	Override Common S
Room Name (from Exchange(R))	<input type="text"/>	
Web Access*	Enabled	
SSH Access*	Enabled	
Default Call Protocol*	SIP	
Quality Improvement Server	<input type="text"/>	
Multipoint Mode*	Use Media Resource Group List	
Telnet Access*	Off	
Microphone Unmute On Disconnect*	On	
Call Logging Mode*	On	
OSD Encryption Indicator*	Auto	
Alternate phone book server type*	UDS	
Alternate phone book server address	<input type="text"/>	
Default Volume	70	
Max Total Downstream Rate	10000	
Max Total Upstream Rate	10000	
System Name	<input type="text"/>	

**CTMS Settings**

CTMS Multiparty Conferencing\*

CTMS Encryption Mode\*

**Far End Camera Control Settings**

Far End Camera Control\*

Far End Camera Control Signaling Capability\*

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout > CTMS Settings* section.

**Only applicable when using Cisco TelePresence Multipoint Switch (CTMS).**

Configure the product specific configuration layout settings as appropriate.

*CTMS MultiParty Conferencing:* Set the CTMS Multiparty Conferencing mode (On/Off). Default value is On.

*CTMS Encryption Mode:* Set the CTMS Encryption Mode (On/Off). Default value is Off.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page).*

Navigate to the **Product Specific Configuration Layout** section.

Product Specific Configuration Layout		Parameter Value	Override Common S
Room Name (from Exchange(R))			
Web Access*	Enabled		
SSH Access*	Enabled		
Default Call Protocol*	SIP		
Quality Improvement Server			
Multipoint Mode*	Use Media Resource Group List		
Telnet Access*	Off		
Microphone Unmute On Disconnect*	On		
Call Logging Mode*	On		
OSD Encryption Indicator*	Auto		
Alternate phone book server type*	UDS		
Alternate phone book server address			
Default Volume	70		
Max Total Downstream Rate	10000		
Max Total Upstream Rate	10000		
System Name			
<b>CTMS Settings</b>			
CTMS Multiparty Conferencing*	On		
CTMS Encryption Mode*	Off		
<b>Far End Camera Control Settings</b>			
Far End Camera Control*	On		
Far End Camera Control Signaling Capability*	On		
<b>Facility Service Settings</b>			

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout > Far End Camera Control Settings* section.

Configure the product specific configuration layout settings as appropriate.

*Far End Camera Control:* Set the far end camera control mode (On/Off) to let the user on the endpoint (near end) decide if the remote side (far end) should be allowed to select video sources and control the near end camera (pan, tilt, zoom). Default value is On.

*Far End Camera Control Signal Capability:* Set the far end control (H.224) signal capability mode (On/Off). Default value is On.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

Product Specific Configuration Layout		Parameter Value	Override Common S
Room Name (from Exchange(R))			
Web Access*	Enabled		
SSH Access*	Enabled		
Default Call Protocol*	SIP		
Quality Improvement Server			
Multipoint Mode*	Use Media Resource Group List		
Telnet Access*	Off		
Microphone Unmute On Disconnect*	On		
Call Logging Mode*	On		
OSD Encryption Indicator*	Auto		
Alternate phone book server type*	UDS		
Alternate phone book server address			
Default Volume	70		
Max Total Downstream Rate	10000		
Max Total Upstream Rate	10000		
System Name			
<b>CTMS Settings</b>			
CTMS Multiparty Conferencing*	On		
CTMS Encryption Mode*	Off		
<b>Far End Camera Control Settings</b>			
Far End Camera Control*	On		
Far End Camera Control Signaling Capability*	On		
<b>Facility Service Settings</b>			

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout > Facility Service Settings* section.

Configure the product specific configuration layout settings as appropriate.

*Facility Service Type:* Choose a facility service type (Helpdesk/Other/Concierge/Emergency/Security/Catering/Transportation). If the endpoint has a *Touch 8*, note that only the Helpdesk option is available on the Touch controller. Facility services are not available when using the remote control and on-screen menu. Default value is Helpdesk.

**NOTE:** A facility service is not available unless both the FacilityService Service Name and the FacilityService Service Number settings are properly set.

*Facility Service Name:* Enter the name of the facility service. Default value is "" (empty) and maximum length is 255 characters.

*Facility Service Number:* Enter the number of the facility service. Default value is "" (empty) and maximum length is 255 characters.

*Facility Service Call Type:* Choose the call type (Video/Audio). Default value is Video.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

**Far End Camera Control Settings**

Far End Camera Control\*

Far End Camera Control Signaling Capability\*

**Facility Service Settings**

Facility Service Type\*

Facility Service Name

Facility Service Number

Facility Service Call Type\*

**Standby Settings**

Standby Mode\*

Standby Delay

Standby Action\*

**Serial Port Settings**

Serial Port\*

Serial Port Login Required\*

**Admin username and password**

Admin Username

Admin Password

**Dial Plan**

Site Access Code

Inter Site Access Code

Off-Net Access Code

National Dialing Digits

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout > Standby Settings* section.

Configure the product specific configuration layout settings as appropriate.

*Standby Mode:* Set the Standby Mode (On/Off) to determine whether the endpoint should go into standby mode or not. Default value is On.

*Standby Delay:* Set the Standby Delay to define how long the system shall be in idle mode before it goes into standby mode. Default value is 10 minutes and the value space is 1-480 minutes.

*Standby Action:* Define the camera position when going into standby mode.

- Set to Privacy Position in order to turn the camera to a sideways position when entering standby mode.
- Set to None to leave the camera in its current position when entering standby mode.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

<b>Far End Camera Control Settings</b>	
Far End Camera Control*	On
Far End Camera Control Signaling Capability*	On
<b>Facility Service Settings</b>	
Facility Service Type*	Helpdesk
Facility Service Name	
Facility Service Number	
Facility Service Call Type*	Video
<b>Standby Settings</b>	
Standby Mode*	On
Standby Delay	10
Standby Action*	Privacy Position
<b>Serial Port Settings</b>	
Serial Port*	On
Serial Port Login Required*	On
<b>Admin username and password</b>	
Admin Username	admin
Admin Password	.....
<b>Dial Plan</b>	
Site Access Code	
Inter Site Access Code	
Off-Net Access Code	
National Dialing Digits	

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout > Serial Port Settings* section.

Configure the product specific configuration layout settings as appropriate.

*Serial Port:* Set the serial port mode (On/Off) to enable/disable the serial port. Default value is On.

*Serial Port Login Required:* Set the login mode (On/Off) to determine if login shall be required when connecting to the serial port. Default value is On.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

<b>Far End Camera Control Settings</b>	
Far End Camera Control*	On
Far End Camera Control Signaling Capability*	On
<b>Facility Service Settings</b>	
Facility Service Type*	Helpdesk
Facility Service Name	
Facility Service Number	
Facility Service Call Type*	Video
<b>Standby Settings</b>	
Standby Mode*	On
Standby Delay	10
Standby Action*	Privacy Position
<b>Serial Port Settings</b>	
Serial Port*	On
Serial Port Login Required*	On
<b>Admin username and password</b>	
Admin Username	admin
Admin Password	.....
<b>Dial Plan</b>	
Site Access Code	
Inter Site Access Code	
Off-Net Access Code	
National Dialing Digits	

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

**Not applicable for endpoints with a non-secure security profile; not applicable for endpoints connected to CUCM via Expressway.**

Navigate to the *Product Specific Configuration Layout* section > *Admin username and password* section.

Configure the product specific configuration layout settings as appropriate.

*Admin Username:* Set the username. Must be *admin* if using a Secure Profile in CUCM; or must match the value set on the endpoint if you are using Cisco TelePresence Manager (CTS-MAN).

*Admin Password:* Set the password. Set to the desired value if using a Secure Profile in CUCM; or match the value set on the endpoint if you are using Cisco TelePresence Manager (CTS-MAN).

**NOTE:** When the TelePresence endpoint is set up with an encrypted security profile, the endpoint will read the *admin* password from the CUCM. The password can not be blank and the user name must be *admin*.

**NOTE:** The admin username and password set on CUCM must match the system password set on the endpoint in order for the Cisco TelePresence Manager (CTS-MAN) to discover the endpoint and provide *One Button to Push* scheduling to them.

For further information:

- Refer to "[About the phone security profile](#)" on page 11.
- Refer to "[Setting the system password](#)" on page 44.

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

The screenshot shows a configuration page with several sections:

- Far End Camera Control Settings:**
  - Far End Camera Control\* (On)
  - Far End Camera Control Signaling Capability\* (On)
- Facility Service Settings:**
  - Facility Service Type\* (Helpdesk)
  - Facility Service Name (text input)
  - Facility Service Number (text input)
  - Facility Service Call Type\* (Video)
- Standby Settings:**
  - Standby Mode\* (On)
  - Standby Delay (10)
  - Standby Action\* (Privacy Position)
- Serial Port Settings:**
  - Serial Port\* (On)
  - Serial Port Login Required\* (On)
- Admin username and password:**
  - Admin Username (admin)
  - Admin Password (masked with dots)
- Dial Plan:**
  - Site Access Code (text input)
  - Inter Site Access Code (text input)
  - Off-Net Access Code (text input)
  - National Dialing Digits (text input)

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout* section > *Dial Plan* section.

Configure the product specific configuration layout settings as appropriate.

**Only applicable when using Cisco TelePresence Manager.**

The Cisco Unified CM Dial Plan specifies dial plan details for certain countries other than North America and describes deployment and installation of these dial plans.

Configure the dial plan. Refer to Cisco TelePresence Manager documentation for more details.

The Cisco TelePresence Manager documentation is found on the Cisco web site. Go to: <http://www.cisco.com/c/en/us/support/conferencing/telepresence-manager/tsd-products-support-series-home.html>

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

Standby Mode*	On
Standby Delay	10
Standby Action*	Privacy Position
<b>Serial Port Settings</b>	
Serial Port*	On
Serial Port Login Required*	On
<b>Admin username and password</b>	
Admin Username	admin
Admin Password	.....
<b>Dial Plan</b>	
Site Access Code	
Inter Site Access Code	
Off-Net Access Code	
National Dialing Digits	
International Dialing Digits	
<b>Directory Number</b>	
Country Code	
Area Code	
Local Number	
<b>Osd</b>	
Todays Bookings*	Off

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout* section > *Directory Number* section.

Configure the product specific configuration layout settings as appropriate.

**Only applicable when using Cisco TelePresence Manager.**

Configure the directory number. Refer to Cisco TelePresence Manager documentation for more details.

The Cisco TelePresence Manager documentation is found on the Cisco web site. Go to: <http://www.cisco.com/c/en/us/support/conferencing/telepresence-manager/tsd-products-support-series-home.html>

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

Standby Mode*	On
Standby Delay	10
Standby Action*	Privacy Position
<b>Serial Port Settings</b>	
Serial Port*	On
Serial Port Login Required*	On
<b>Admin username and password</b>	
Admin Username	admin
Admin Password	.....
<b>Dial Plan</b>	
Site Access Code	
Inter Site Access Code	
Off-Net Access Code	
National Dialing Digits	
International Dialing Digits	
<b>Directory Number</b>	
Country Code	
Area Code	
Local Number	
<b>Osd</b>	
Todays Bookings*	Off

Mandatory  Optional

## Manual registration of the endpoint

### Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout* section > *OSD* section.

Configure the product specific configuration layout settings as appropriate.

*Todays Bookings*: Choose whether to show today's bookings on screen or not. Default value is Off.

This setting is not available for all endpoints, and it requires that it is possible to book the endpoint by an external booking system, for example the Cisco TelePresence Management Suite (TMS).

When done click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Product Specific Configuration Layout** section.

<b>Standby Mode*</b>	On
<b>Standby Delay</b>	10
<b>Standby Action*</b>	Privacy Position
<b>Serial Port Settings</b>	
<b>Serial Port*</b>	On
<b>Serial Port Login Required*</b>	On
<b>Admin username and password</b>	
<b>Admin Username</b>	admin
<b>Admin Password</b>	.....
<b>Dial Plan</b>	
<b>Site Access Code</b>	
<b>Inter Site Access Code</b>	
<b>Off-Net Access Code</b>	
<b>National Dialing Digits</b>	
<b>International Dialing Digits</b>	
<b>Directory Number</b>	
<b>Country Code</b>	
<b>Area Code</b>	
<b>Local Number</b>	
<b>Osd</b>	
<b>Todays Bookings*</b>	Off

Mandatory  Optional

## Manual registration of the endpoint

### Adding the directory number

Navigate to the *Association Information* section:

Click *Line[1] - Add a new DN* to define the directory number.

### Directory number information

Navigate to the *Directory Number Information* section.

*Directory Number*: Enter the number of the endpoint, according to the E.164 Numbering Plan

Click **Save**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Association Information** section.

The screenshot shows the Cisco Phone Configuration interface. At the top, there are navigation tabs: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, and Bulk Administration. Below these is the 'Phone Configuration' header with a 'Related Links: Back To Find/...' button. A toolbar contains icons for Save, Delete, Copy, Reset, Apply Config, and Add New. The main content area is divided into sections: 'Status' (Status: Ready), 'Association Information' (containing a table with one row: '1 Line [1] - Add a new DN'), 'Phone Type' (Product Type: Cisco TelePresence MX300, Device Protocol: SIP), and 'Device Information' (Registration: Unknown). A blue box highlights the 'Association Information' table.

Navigate to the **Directory Number Information** section.

The screenshot shows the Cisco Directory Number Information interface. It features a 'Status: Ready' indicator at the top. The 'Directory Number Information' section is highlighted with a blue box and contains the following fields: 'Directory Number\*' (value: 11118) with an 'Urgent Priority' checkbox, 'Route Partition' (value: < None >), 'Description', 'Alerting Name', and 'ASCII Alerting Name'.

Mandatory  Optional

## Manual registration of the endpoint

### Configuring shared lines

*Optional:* To configure the CUCM for shared lines, navigate back to "Manual registration of the endpoint" on page 14 and repeat the steps for manual registration of another endpoint and assign the next endpoint to the *same* directory number.

*Associated Devices:* When one directory number has been set up to be shared between more than one endpoint you will see the MAC addresses of the devices listed in the *Associated Devices* section.

Additionally you must set the *Privacy* setting to *Off* for shared lines to function as intended. You can find this setting under *Device > Phone > Phone Configuration > Device Information*.

### Display the name of the caller

*Optional:* Navigate to the *Line # on Device <MAC address>* section.

*Display (Caller ID):* Enter the name of the owner of the TelePresence system to allow the receiver of a call from the system to see the proper identity of the caller.

Display text for a line appearance is intended for displaying text such as a name instead of a directory number for calls. If you specify a number, the person receiving a call may not see the proper identity of the caller.

When done click **Save** and **Apply Config**.

Navigate to: *Device > Phone > Phone Configuration (continued from the previous page)*.

Navigate to the **Directory Number Information** section.

**Directory Number Information**

Directory Number\* 11118  Urgent Priority

Route Partition < None >

Description

Alerting Name

ASCII Alerting Name

External Call Control Profile < None >

Allow Control of Device from CTI

Associated Devices

SEP...  
SEP...

Edit Device  
Edit Line Appearance

Navigate to the **Device Information** section.

**Device Information**

Device is trusted

Network Locale < None >

Privacy\* Off

Navigate to the **Line # on Device <MAC address>** section.

**Line 1 on Device SEP...**

Display (Caller ID)  Display text for a line appearance instead of a directory number for calls. If you specify a number, the person receiving the call may not see the proper identity of the caller.

ASCII Display (Caller ID)

Mandatory  Optional

## Auto-registration of the endpoint

Only applicable when the CUCM is not set to mixed mode; not applicable for endpoints connected to CUCM via Expressway.

Configuration of the CUCM for auto-registration of the endpoint is described on this page.

**i** Auto-registration of the TelePresence endpoint is not possible when the CUCM is set to mixed mode (cluster security mode).

Use the search options available on the page, or leave the search field blank and press *Find* to list the available CUCMs.

- Choose the one you would like to configure; this will take you to the *Cisco Unified CM Configuration* page.

### Enable auto-registration

Navigate to the *Auto-registration Information* section.

*Starting Directory Number:* Enter the lowest number in the range of directory numbers.

*Ending Directory Number:* Enter the highest number in the range of directory numbers.

*Auto-registration Disabled on this Cisco Unified Communications Manager:* Uncheck the checkbox to enable auto-registration.

When done click **Save** and **Apply Config**.

Navigate to: *System > Cisco Unified CM.*

Click **Find** and choose the CUCM from the list.

**Find and List Cisco Unified CMs**

**Status**

**i** 2 records found

**Cisco Unified Communications Managers (1 - 2 of 2)**

Cisco Unified  
Find Communications where  Cisco Unified Communications Manager Name  begins with

Name ^	Description	Location Bandwidth Manager
<a href="#">CM_cucm01-1</a>	cucm01-1	
<a href="#">CM_cucm02-1</a>	cucm02-1	

Navigate to the **Auto-registration Information** section.

Location Bandwidth Manager Group

**Auto-registration Information**

Universal Device Template

Universal Line Template

Starting Directory Number\*

Ending Directory Number\*

Auto-registration Disabled on this Cisco Unified Communications Manager

**Cisco Unified Communications Manager TCP Port Settings for this Server**

Ethernet Phone Port\*

MGCP Listen Port\*

MGCP Keep-alive Port\*

Mandatory  Optional

## How to verify the endpoint registration

**NOTE:** Before you can verify the endpoint registration you must configure the TelePresence endpoint. See: "[About endpoint configuration](#)" on page 43.

After the endpoint has been provisioned you can check the status on the *Phone* page to verify if the endpoint has been registered to CUCM.

Navigate to: *Device > Phone*

Search for the endpoint or click *Find* to list all.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go  
admin | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

**Find and List Phones** | Related Links: [Actively Logged In Device Report](#) | Go

+ Add New | Select All | Clear All | Delete Selected | Reset Selected | Apply Config to Selected

**Status**  
4 records found

**Phone (1 - 4 of 4)** | Rows per Page 50

Find Phone where Device Type begins with Cisco TelePresence MX | Find | Clear Filter

	Device Name(Line)	Description	Device Type	Device Protocol	Status	IP Address	Copy	Super Copy
<input type="checkbox"/>	<a href="#">SEP001122334455</a>	Description	Cisco TelePresence MX300	SIP	Unregistered	92.168.10.1		
<input type="checkbox"/>	<a href="#">SEP0011223344AA</a>	Description	Cisco TelePresence MX300	SIP	Unregistered	92.168.10.2		
<input type="checkbox"/>	<a href="#">SEP0011223344BB</a>	Description	Cisco TelePresence MX300	SIP	Unregistered	92.168.10.3		
<input type="checkbox"/>	<a href="#">SEP0011223344CC</a>	Description	Cisco TelePresence MX300	SIP	Registered with cucm01-1	92.168.10.4		

Add New | Select All | Clear All | Delete Selected | Reset Selected | Apply Config to Selected

The status of the endpoint registration.

## Specify the home cluster service for the end user

The enterprise network may consist of multiple CUCM clusters. One, and only one, CUCM cluster should be defined as an end user's Home Cluster.

Navigate to the *Service Settings* section.

Check the *Home Cluster* check box if the end user is homed to this cluster.

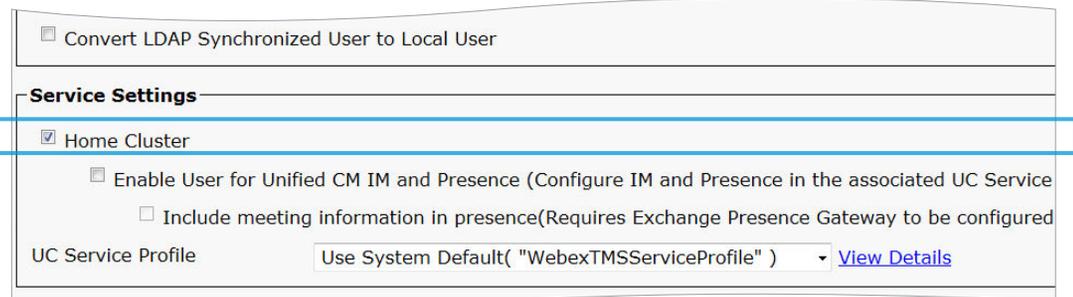
Click **Save**.

Navigate to: *User Management > End User*

Click **Find** and choose the appropriate user from the list. The End User Configuration window opens.



Navigate to the **Service Settings** section.



Mandatory  Optional

## Associate a user with an access control group

Only applicable for endpoints connected to CUCM via Expressway.

### Add the user to an access control group

The access control group(s) that a user belongs to defines the user's level of access.

Navigate to the *Permissions Information* section, and choose *Add to Access Control Group*.

Check the *Standard CCM End Users* check box.

When done click **Add Selected**, and you will return to the End User Configuration window.

The selected access control group is now added to the list of groups shown in the Permissions Information section.

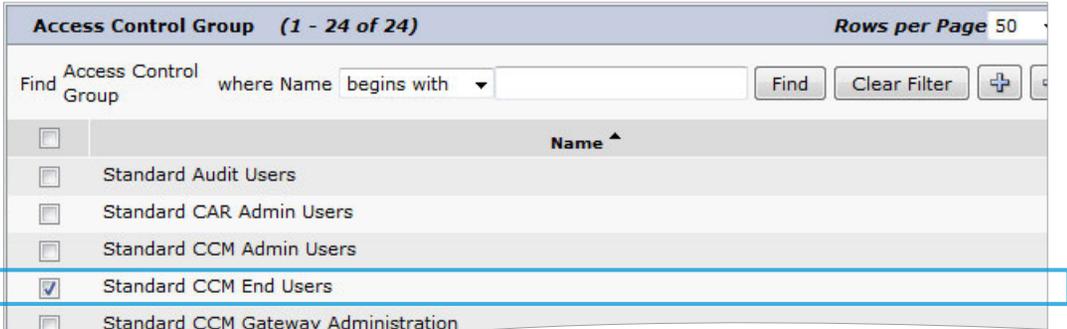
Click **Save**.

Navigate to: *User Management > End User*

Click **Find** and choose the appropriate user from the list. The End User Configuration window opens.



Navigate to the **Permissions Information** section, and click **Add to Access Control Group** to open the Access Control Group window.



Access Control Group (1 - 24 of 24)		Rows per Page 50
Find	Access Control Group	where Name begins with <input type="text"/> <b>Find</b> <b>Clear Filter</b> <b>+</b>
<input type="checkbox"/>	Name ^	
<input type="checkbox"/>	Standard Audit Users	
<input type="checkbox"/>	Standard CAR Admin Users	
<input type="checkbox"/>	Standard CCM Admin Users	
<input checked="" type="checkbox"/>	Standard CCM End Users	
<input type="checkbox"/>	Standard CCM Gateway Administration	

Mandatory  Optional

## Enterprise parameters

### Clusterwide Domain Configuration

If the inbound call does not provide a host or domain in the caller's information, the configured Organizational Top-Level Domain will be used in the identity headers. This enables the called endpoint to return a call using the received or missed call list (the history list).

See also "[Use Fully Qualified Domain Name in SIP Requests](#)" on page 10 for further details.

*Organization Top Level Domain:* Enter a valid domain (for example, cisco.com) to define the top level domain for the organization.

Navigate to: *System > Enterprise Parameters*

Navigate to the **Clusterwide Domain Configuration** section.

The screenshot shows the Cisco Unified CM Administration interface. The breadcrumb navigation is *System > Enterprise Parameters*. The page title is **Enterprise Parameters Configuration**. Below the title are buttons for **Save**, **Set to Default**, **Reset**, and **Apply Config**. The configuration is organized into sections:

- CRS Application Parameters**
  - [Auto Attendant Installed](#) \* false
  - [IPCC Express Installed](#) \* false
- Clusterwide Domain Configuration** (highlighted)
  - [Organization Top Level Domain](#) cisco.com
  - [Cluster Fully Qualified Domain Name](#) [Empty field]
- Denial-of-Service Protection**
  - [Denial-of-Service Protection](#) \* True (dropdown menu)
- TLS Handshake Timer**

Legend:  Mandatory  Optional

## CHAPTER 2

### ENDPOINT CONFIGURATION

This chapter describes the steps required to configure the TelePresence endpoints for use with Cisco Unified Communications Manager.



## About endpoint configuration

This section gives an overview of the steps required for registering a TelePresence endpoint to CUCM.

You can use the Touch controller, remote control, web interface, or the command line interface to configure the endpoint. Your TelePresence system is shipped with either a Touch panel or a remote control.

**NOTE:** We recommend doing the CUCM configuration before the endpoint provisioning.

Be aware that HTTP (web interface) and SSH (used for command line) may be disabled in the endpoint configuration on CUCM. This will prevent access to the endpoint's web interface and command line interface. See "[Product specific configuration layout](#)" on page 21 how to enable/disable Web access and SSH access.

### Endpoint diagnostic tools

If having trouble using the TelePresence endpoint diagnostic tools when the endpoint is provisioned to CUCM, check that the SIP listen port is set to Off (default). Log in to the web interface of the endpoint and go to: *Configuration > System Configuration > SIP > ListenPort*.

### Endpoint configuration in three steps

#### Setting the system password

It is mandatory to set a password for the users to restrict access to system configuration. If no password is set there will be a notification on screen.

Go to: "[Setting the system password](#)" on page 44.

#### Setting the call details

The *call rate* will not be set by CUCM. Set the call rate to match the network capabilities to achieve the desired call quality.

Go to: "[Setting the call details](#)" on page 45.

#### Setting up provisioning

The endpoint can be provisioned either from CUCM, or from CUCM via Expressway.

Go to: "[Setting up CUCM provisioning](#)" on page 46, or "[Setting up provisioning from CUCM via Expressway \(Mobile and Remote Access\)](#)" on page 47.

### Finding the IP address

If using the web interface or the command line interface you will need the IP address of the endpoint.

Use the Touch controller or remote control to find the address.

- Using the Touch controller: Tap the upper left corner of the Touch panel, followed by *Settings > System Information*. Then see the *General* section.
- Using the remote control: Navigate to *Home > Settings > System Information* and see the *Network* section.

## Setting the system password

The system password will restrict access to the TelePresence endpoint and is set from the web interface or the API. The endpoint is delivered with a default user account (*admin*) with full credentials and no password is set.

### If the endpoint is set up with an encrypted security profile

**NOTE:** If the TelePresence endpoint is set up with an encrypted security profile the endpoint will read the *admin* password from the CUCM; given that:

- **Endpoint:** A user with administrator rights must exist on the endpoint and the user name must be *admin*. The password will be provisioned by CUCM unless the password was blank on CUCM.
- **CUCM:** The user name must be *admin* and the password cannot be blank.

### Access through HTTP and SSH

Be aware that HTTP (web interface) and SSH (used for command line) may be disabled in the endpoint configuration on CUCM. This will prevent access to the endpoint's web interface and command line interface. See "[Product specific configuration layout](#)" on page 21 how to enable/disable Web access and SSH access.

### If used with Cisco TelePresence Manager

**NOTE:** The system password set on the endpoint must match the value set in the CUCM in order for the Cisco TelePresence Manager (CTS-MAN) to discover the endpoint and provide *One Button to Push* scheduling to it.

### Using the web interface

Log in to the endpoint through the web interface with your username and current password. If a password is currently not set, use a blank password when logging in.

#### Set or change the system password

1. Click on the username in the upper right corner and choose *Change password* in the drop down menu.
2. Enter the *Current password*, the *New password*, and repeat the new password in the appropriate input fields.  
The password format is a string with 0-64 characters.
3. Click *Change password*.

The new system password will apply when you log in through the web interface or command line interface.

### Using the command line interface

Open a command line interface (e.g. PuTTY) and log in to the endpoint (codec) with your username and current password. If a password is currently not set, use a blank password when logging in.

#### Set or change the system password

```
xCommand SystemUnit AdminPassword Set
Password: *****
```

The password format is a string with 0-64 characters.

The new system password will apply when you log in through the command line interface. The endpoint (codec) must be restarted to make the password apply to the web interface.

## Setting the call details

If in doubt for any of the parameters below, contact your system administrator or your service provider.

The *call rate* will not be set by CUCM. Set the call rate to match the network capabilities to achieve the desired call quality.

When used with Cisco TelePresence Multipoint Switch (CTMS), the recommended value is 2500 kbps, or higher.

Note that the call protocol must be SIP in CUCM and CUCM via Expressway mode. H.323 is not supported.

### Using the Touch panel

Tap the upper left corner of the Touch panel, followed by *Settings > Administrator > Call Details*.

You have to sign in with administrator credentials to open the Administrator menu.

#### Configure the default call settings

Set the *Default Call Rate* to the appropriate value. Tap the plus (+) or minus (-) buttons to increase or decrease the value.

In Cisco UCM mode the *Default Call Protocol* is automatically set to SIP, and H.323 is not supported.

### Using the TRC5 remote control

Navigate to *Home > Settings > Administrator Settings > Advanced Configuration > Conference 1*.

#### Configure the default call settings

Use the remote control and go to the *DefaultCall* section and set the *Rate* to the appropriate value.

In Cisco UCM mode the *Default Call Protocol* is automatically set to SIP, and H.323 is not supported.

Click *Ok* to save the change.

### Using the web interface

Navigate to *Configuration > Advanced Configuration > Conference*.

#### Configure the default call settings

Go to the *DefaultCall* section and set the *Rate* to the appropriate value.

In Cisco UCM mode the *Default Call Protocol* is automatically set to SIP, and H.323 is not supported.

Click *Save*.

### Using the command line interface

Open a command line interface (e.g. PuTTY) and log in to the endpoint (codec).

#### Configure the default call settings

```
xConfiguration Conference 1
DefaultCall Rate: <64..6000>
```

```
xConfiguration Conference 1
DefaultCall Protocol: SIP
```

## Setting up CUCM provisioning

Please contact your Cisco Unified Communications Manager (CUCM) provider if in doubt for any of the provisioning parameters.

For more information about the *external manager address* and *CTL files*, refer to "[About endpoint provisioning](#)" on page 54.

### Using the Touch panel

If you are connecting the system for the first time, the Provisioning Wizard will start automatically. Otherwise, tap the upper left corner of the Touch panel, followed by *Settings > Administrator > Provisioning*.

You have to sign in with administrator credentials to open the Administrator menu.

### Running the provisioning wizard

1. If the wizard is not already started, click *Start*.
2. Choose *Cisco UCM* as the infrastructure and click *Next*.
3. **If required:** Enter the IP address or DNS name of the *External Manager* (the CUCM cluster TFTP server address) in the input field <sup>1</sup>.
4. **If required:** Check *Delete old certificate files (CTL, ITL)*. If no CTL or ITL file exist on the endpoint, this option will not be available.
5. Tap *Register* to complete the registration.
6. When successfully registered to CUCM a message will appear and you will see the address (URI) of the endpoint.

### Using the TRC5 remote control

If the system is in sleep mode, press any key on the remote control to wake up the system.

### Configuring the provisioning<sup>2</sup>

1. Navigate to *Home > Settings > Administrator Settings > Advanced Configuration > Provisioning*.
2. Navigate to *Mode*, select *CUCM* from the drop down list, and press the *OK* key. The change will take effect immediately.
3. **If required:** Navigate to *ExternalManager > Address* and enter the IP address or DNS name of the External Manager (the CUCM cluster TFTP server address)<sup>1</sup>. Click *Save*.

### Using the web interface

Open a web browser, enter the IP address of the endpoint, and log in with your user name and password.

### Configuring the provisioning<sup>2</sup>

1. Navigate to *Configuration > System Configuration > Provisioning*.
2. Navigate to *Mode* and set the provisioning mode to *CUCM*. Click *Save*.
3. **If required:** Navigate to *ExternalManager > Address* and enter IP address or DNS name of the External Manager (the CUCM cluster TFTP server address)<sup>1</sup>. Click *Save*.
4. **If required:** Delete the certificate files (CTL/ITL). Navigate to *Configuration > Security* and click *Delete CTL/ITL*.

### Using the command line interface

Open a command line interface (e.g. PuTTY) and log in to the endpoint (codec).

### Configuring the provisioning<sup>2</sup>

1. `xConfiguration Provisioning Mode: CUCM`
2. **If required:**  
`xConfiguration Provisioning ExternalManager Address: <the CUCM cluster TFTP server address>`
3. **If required:** delete the CTL file  
`xCommand Provisioning CUCM CTL Delete`

<sup>1</sup> The DHCP server may be set up to provide the External Manager address automatically (DHCP Option 150). If so, you should not enter an address manually. A manually added address will override the address provided by DHCP.

<sup>2</sup> Keep the default setting for the other Provisioning parameters.

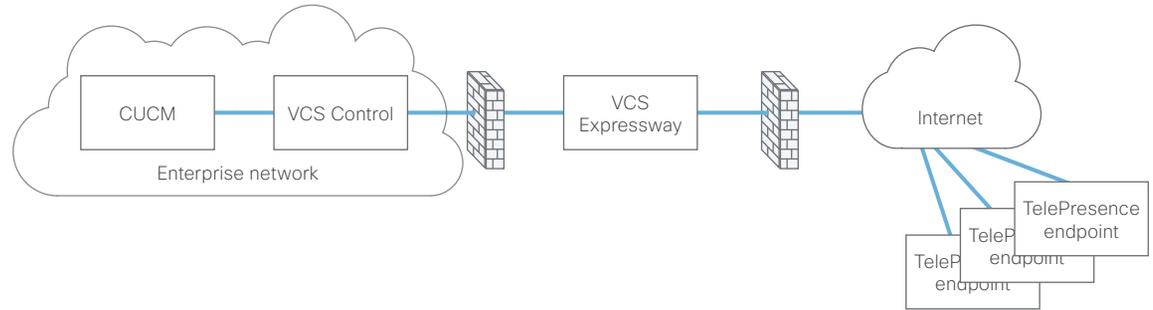
## Setting up provisioning from CUCM via Expressway (Mobile and Remote Access)

Endpoints can have their registration, call control and provisioning provided by Cisco Unified Communications Manager (CUCM) also when the endpoint is not within the enterprise network.

In such cases you will need a VCS Expressway for secure firewall traversal and line-side support for CUCM registrations (see illustration to the right).

This feature is also referred to as Cisco Unified Communications Mobile and Remote Access, and is a core part of the Cisco Collaboration Edge Architecture.

Refer to the *Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide* for details about setting up the infrastructure.



### Verifying the identity of the Expressway

The endpoint must verify the identity of the VCS Expressway it is connecting to. To do this, the certificate authority that was used to sign the VCS Expressway's server certificate must be in the endpoint's list of trusted CAs.

The endpoints ship with a list of default CAs which cover the most common providers (Verisign, Thawte, etc.). If the relevant CA is not included, it must be added.

### If required: Add a CA to the endpoint's list of trusted CAs

1. Open the endpoint's web interface, navigate to [Configuration > Security](#) and open the [CAs](#) tab.
2. Click [Browse...](#) and find the file containing the CA's certificate (file format: .PEM) on your computer.
3. Click the [Add certificate authority...](#) to store the new CA certificate on your system.

See *Managing the list of trusted certificate authorities* in the endpoint's administrator guide for more details.

## Setting up provisioning from CUCM via Expressway

Upon ordering this service, you have received a *Username, Domain and Password*.

Please contact your Cisco Unified Communications Manager (CUCM) provider if in doubt for any of the provisioning parameters.

For more information about the *external manager address* and *CTL files*, refer to "[About endpoint provisioning](#)" on page 54.

### Using the Touch panel

If you are connecting the system for the first time, the Provisioning Wizard will start automatically. Otherwise, tap the upper left corner of the Touch panel, followed by *Settings > Administrator > Provisioning*.

You have to sign in with administrator credentials to open the Administrator menu.

### Running the provisioning wizard

1. If the wizard is not already started, click *Start*.
2. Choose *Cisco UCM via Expressway* as the infrastructure and click *Next*.
3. Enter *Username, Domain and Password* in the corresponding input fields.
4. **If required:** Check *Manually override Expressway address*, and enter the IP address or DNS name of the *External Manager* (the CUCM cluster TFTP server address) in the input field<sup>1</sup>.
5. **If required:** Check *Delete old certificate files (CTL, ITL)*. If no CTL or ITL file exist on the endpoint, this option will not be available.
6. Tap *Register* to complete the registration.
7. When successfully registered to CUCM a message will appear and you will see the address (URI) of the endpoint.

### Using the TRC5 remote control

If the system is in sleep mode, press any key on the remote control to wake up the system.

### Configuring the provisioning<sup>2</sup>

1. Navigate to *Home > Settings > Administrator Settings > Advanced Configuration > Provisioning*.
2. Navigate to *Mode*, select *Edge* from the drop down list, and press the *OK* key. The change will take effect immediately.
3. Navigate to *LoginName*, and enter the username that you received when ordering the service.
4. Navigate to *Password*, and enter the password that you received when ordering the service.
5. Navigate to *ExternalManager > Domain*, and enter the domain that you received when ordering the service.
6. **If required:** Navigate to *ExternalManager > Address* and enter the IP address or DNS name of the External Manager (the CUCM cluster TFTP server address)<sup>1</sup>. Click *Save*.

### Using the web interface

Open a web browser, enter the IP address of the endpoint, and log in with your user name and password.

### Configuring the provisioning<sup>2</sup>

1. Navigate to *Configuration > System Configuration > Provisioning*.
2. Navigate to *Mode* and set the provisioning mode to *Edge*. Click *Save*.
3. Navigate to *LoginName*, and enter the username that you received when ordering the service. Click *Save*.
4. Navigate to *Password*, and enter the password that you received when ordering the service. Click *Save*.
5. Navigate to *ExternalManager > Domain*, and enter the domain that you received when ordering the service. Click *Save*.
6. **If required:** Navigate to *ExternalManager > Address* and enter IP address or DNS name of the External Manager (the CUCM cluster TFTP server address)<sup>1</sup>. Click *Save*.
7. **If required:** Delete the certificate files (CTL/ITL). Navigate to *Configuration > Security* and click *Delete CTL/ITL*.

### Using the command line interface

Open a command line interface (e.g. PuTTY) and log in to the endpoint (codec).

### Configuring the provisioning<sup>2</sup>

1. `xConfiguration Provisioning Mode: Edge`
2. `xConfiguration Provisioning LoginName: <the username that you received when ordering the service>`
3. `xConfiguration Provisioning Password: <the password that you received when ordering the service>`
4. `xConfiguration Provisioning ExternalManager Domain: <the domain that you received when ordering the service>`
5. **If required<sup>1</sup>:**  
`xConfiguration Provisioning ExternalManager Address: <the CUCM cluster TFTP server address>`
6. **If required:** delete the CTL file  
`xCommand Provisioning CUCM CTL Delete`

<sup>1</sup> Normally, the External Manager address is determined by DNS lookup in the provided Domain. If so, you should not enter an address manually. A manually added address will override the address determined by DNS lookup.

<sup>2</sup> Keep the default setting for the other Provisioning parameters.

## Verifying the endpoint registration

After having provisioned the endpoint to CUCM you should verify that the registration was successful.

### Making a call

Make a call from the TelePresence endpoint to see if the registration was successful.

Use the interface of your choice:

- The touch controller
- The remote control
- The web interface
- The command line interface

### Checking the system information

When checking the system information, the **SIP Status** should show *Registered* and the **SIP Proxy** should display the address of the CUCM.

#### Using the web interface

Navigate to *Home > System Information* and see the *SIP* section.

#### Using the Touch controller

Tap the upper left corner of the Touch panel, followed by *Settings > System Information*. Then see the *SIP* section.

#### Using the remote control

Navigate to *Home > Settings > System Information* and see the *SIP* section.

#### Using the command line interface

Open a command line interface (e.g. PuTTY), log in to the endpoint (codec), and run the following API commands:

```
xStatus SIP Profile 1 Registration 1 Status
```

```
xStatus SIP Proxy 1 Address
```

or: `xStatus SIP -` to see a complete overview.

## CHAPTER 4

### ABOUT PASSWORDS

This section describes the use of passwords on TelePresence endpoints.



## Setting the system password

The system password protects the video system. You have to sign in to be able to use the web and command line interfaces, and to get access to the Administrator settings from a Touch control panel.

### The *admin* user

The video system is delivered with a default user account with full credentials. The user name is *admin*, and initially, no password is set for the default user.



**It is mandatory to set a password for the *admin* user in order to restrict access to system configuration.** Also set a password for any other user with similar credentials.

Make sure to keep a copy of the password in a safe place. You have to factory reset the unit if you have forgotten the password.

A warning, saying that the system password is not set, is shown on screen until a password is set for the *admin* user.

### About access to administrator settings when using a TRC5 remote control and the on-screen menu

Note that the on-screen Administrator Settings menu that is available when using a remote control, is NOT protected by the system password; you have to set a menu password (see next page).

### Other user accounts

You can create as many user accounts as you like for your video system.

You can read more about how to create and manage user accounts in the [Administrator guide for the endpoint](#).

### Changing your own system password

Perform the following steps to change the system password.

If a password is currently not set, use a blank *Current password*; to remove a password, leave the *New password* fields blank.

1. Sign in to the web interface with your user name and current password.
2. Click your user name in the upper right corner and choose *Change password* in the drop down menu.
3. Enter the *Current password*, the *New password*, and repeat the new password in the appropriate input fields.  
The password format is a string with 0-64 characters.
4. Click *Change password*.

### Changing another user's system password

If you have administrator access rights, you can change all users' passwords by performing the following steps:

1. Sign in to the web interface with your user name and password.
2. Go to the *Configuration* tab and select *User Administration*.
3. Choose the appropriate user from the list.
4. Enter a new password and PIN code.
5. Click *Save*.

## Setting the menu password

The menu password protects the Administrator Settings menu that is available on-screen when using the remote control.

When starting up the video conference system for the first time anyone can access these settings, because the menu password is not set.



**We strongly recommend that you set a menu password, because the administrator settings may severely affect the behavior of the system.**

Note that the menu password, as from software version TC7.0, applies only to the on-screen Administrator Settings menu; it does not apply to the Administrator menu on the Touch controller.

### Setting the menu password from the web interface

1. Sign in to the web interface with your user name and current password.
2. Go to [Configuration > System Configuration](#).
3. Click [Set/Change Administrator Settings menu password](#) to open the menu password dialog.
4. Enter the password in the input field.
5. Click [Save](#) to set/change the password.



Use the remote control and on-screen menu, or the Touch controller to find the IP address (IPv4 or IPv6).

Remote control and on-screen menu: Navigate to [Home > Settings > System information](#).

Touch controller: Tap the upper, left corner of the Touch controller to open the drop down window. Then tap [Settings > System Information](#).

### Setting the menu password using the remote control

1. In the on screen menu, go to [Home > Settings > Administrator settings > Set menu password](#).  
The password should be a string with 0-255 characters.  
To deactivate the password leave the password input field empty.
2. Enter the menu password in the input field. The password you enter is hidden; each character is replaced with a star (\*).  
On the remote control, press the # key to toggle between lower or upper case characters and numbers: abc/ABC/123.
3. Select [Save](#) to save the changes, or [Cancel](#) to leave without saving.
4. Press [Home](#) (🏠) to exit.

## CHAPTER 5

### APPENDICES

The appendices section provides you with additional information that you may find useful as system administrator.



## About ad hoc conferencing

To enable ad hoc conferencing the CUCM must be set up with a Conference Bridge (media resources), and the conference bridge must be added as a Cisco TelePresence MCU in CUCM.

Configuration of CUCM is described earlier in this guide. Refer to the *Multipoint Mode* setting in the "[Product specific configuration layout](#)" on page 22.

### Verifying the setup

The ad hoc conference setup can be verified by running the following command on the endpoint (codec):

```
xStatus Conference Multipoint Mode
```

*CUCMMediaResourceGroupList*: Multiparty conferences (ad hoc conferences) will be hosted by the CUCM configured conference bridge.

Any other result *<Auto/Off/MultSite/MultiWay>* indicates that the codec is not configured for ad hoc conferences on CUCM.

The codec built in bridge setup can be verified by running the following command on the endpoint:

```
xStatus Conference UseBuiltInBridge
```

*False*: The CUCM ad hoc conferencing mode is used.

*True*: The internal built in bridge on the endpoint is used. Calls will not escalate to any external media resource.

## About shared lines

CUCM considers a directory number to be a shared line if the number appears on more than one device in the same partition, allowing the call to be accepted on more than one device. The other endpoints will display a notification on the user interface when the call is answered.

With shared lines several devices in the same partition can share the same directory number. The different devices sharing the same number receive status from the other appearances on the line.

For example, you can set up a shared line so that many devices share the same number and the first available operator picks up the call (help desk). Assisted call handling, where an administrator manages the calls for an executive (call forward and barge in) is another example. Also multiple devices belonging to one person can share the same line, thus allowing him/her to pick up a call on one device and resume it on another (single number reach).

To enable *barge in* to a video conference, the CUCM must be configured for ad hoc conferencing, else the call will be setup as audio only using the CUCM built in Audio bridge. If *barge in* is used on a non-multisite endpoint (EX60, MX200, MX300, C20) a conferencing bridge must be defined.

Configuration of CUCM is described earlier in this guide. Refer to the *Shared Lines* setting in the "[Configuring shared lines](#)" on page 36.

## About endpoint provisioning

Provisioning allows the video conferencing network administrators to manage many video systems simultaneously. In general, you only have to input the credentials of the provisioning server to each video system; the rest of the configuration is done automatically.

Configuration of Cisco TelePresence endpoint is described earlier in this guide. Refer to "[About endpoint configuration](#)" on page 43, "[Setting up CUCM provisioning](#)" on page 46, and "[Setting up provisioning from CUCM via Expressway \(Mobile and Remote Access\)](#)" on page 47.

### About the External Manager address

If the network does not offer DHCP Option 150, the External Manager Address must be added manually. Note that any input in the field will override the setting provided by DHCP.

When the infrastructure is set to *Cisco UCM*; then CDP (Cisco Discovery Protocol) will be enabled and if CDP is successful, the endpoint will discover DHCP Option 150. In this case you can leave the External Manager Address field blank, as the DHCP server will provide the address automatically.

When the infrastructure is set to *Cisco UCM via Expressway*, the External Manager address is determined by DNS lookup in the domain that is configured on the endpoint. If successful, you can leave the External Manager Address field blank.

### About CTL and ITL files

Normally, you will not delete the old Certificate Trust List (CTL) or Initial Trust List (ITL), but there are few cases where you will need to delete these files from the endpoint such as:

- When changing the CUCM IP address.
- When moving the endpoint between CUCM clusters.
- When you need to re-generate or change the CUCM certificate.

## The TelePresence endpoint user interfaces

You can use the Touch controller, the remote control, the web interface, or the command line interface to configure the endpoint.

**NOTE:** Access through HTTP (web interface) and SSH (command line interface) may be disabled when the endpoint has been successfully registered to Cisco Unified Communications Manager 10.5.1 (using a dev.pack with support for TC7.2). See "[Product specific configuration layout](#)" on page 21 how to enable/disable Web access and SSH access.

### Using the Touch panel

If no menu is displayed on the Touch controller, tap the display to wake up the system.

#### Password protection

The system may be password protected. Please contact your system administrator if you can not access the system.

#### If the system does not wake up:

- Make sure the Touch controller is connected to the endpoint, either directly or by the network.
- Make sure the endpoint is connected to power and switched on.
- If the system has just been switched on, wait for a few minutes to allow the system to start up.
- Make sure the Touch controller is properly paired with the endpoint.
- If in doubt, read the Installation guide for your product.

#### Finding the IP address

- Tap the upper left corner of the Touch panel, followed by *Settings > System Information* and navigate to the Network section.

### Using the TRC5 remote control

If no menu is displayed on screen, press any key on the remote control to wake up the system.

#### Password protection

The system may be password protected. Please contact your system administrator if you can not access the system.

#### If the system does not wake up:

- Make sure the remote control has working batteries.
- Make sure the endpoint is connected to power and switched on.
- If the system has just been switched on, wait for a few minutes to allow the system to start up.
- If in doubt, read the Installation guide for your product.

#### Finding the IP address

- Go to *Home > Settings > System Information* and navigate to the Network section.

### Using the web interface

When you know the IP address you can configure the endpoint from the web interface.

#### Signing in to the web interface

1. Open a web browser and enter the system's IP address in the address bar.
2. Enter your user name and password and click Sign In.

#### If you are not able to connect to the system:

- Make sure the endpoint and computer are connected to the same network.
- Make sure the endpoint is connected to power and switched on.
- If the system has just been switched on, wait for a few minutes to allow the system to start up.
- If in doubt, read the Installation guide for your product.

### Using the command line interface

When you know the IP address you can configure the endpoint from a command line interface by API commands.

#### Signing in through SSH

1. Start a command line interface (for example PuTTY). Enter the host name (or IP address) of the codec and set connection type to SSH.
2. Enter your user name and password to sign in.

#### If you are not able to connect to the system:

- Make sure the endpoint and computer are connected to the same network.
- Make sure the endpoint is connected to power and switched on.
- If the system has just been switched on, wait for a few minutes to allow the system to start up.
- If in doubt, read the Installation guide for your product.

## Collecting log files from a TelePresence endpoint

The log files are Cisco specific debug files which may be requested by the Cisco support organization if you need technical support.

The *Current logs* files are time stamped event log files.

All current log files are archived in a time stamped *Historical logs* file each time the system reboots. If the maximum number of historical log files is reached, the oldest one will be overwritten.

### Downloading one file

Click on a log file and follow the instructions in the dialog box to save or open the file (left or right click depending on your browser).

### Downloading all files

You can also download all log files as a bundle; click **Download logs archive** and follow the instructions.

Use the drop down list if you want to include the call history in the archive. You can choose whether to include the full call history or to make the caller/callee anonymous.

The log files shown in the illustration serve as examples. Your system may have other files.

How to collect the log files from a TelePresence endpoint.

Open a web browser and log in to the Cisco TelePresence endpoint. Navigate to *Diagnostics > Log files*.

**Download log archive**

A full archive of the logs on the device is useful for diagnosing problems. This archive includes all current and historical logs, in addition to current system configuration, system status and diagnostics information. Call history is not included by default.

Download logs archive...

**Extended logging**

To help diagnose network issues and problems during call setup, the system can enter a timed extended logging mode. This mode is resource intensive, and populates the existing logs with more detailed information. The extended logging mode can optionally include a full or partial capture of all network traffic.

Start extended logging...

Extended logging is inactive.

**Current Logs**

File Name	Size	Last Modified
arm0-system.log	11 KB	2014-03-31 21:36
arm1-system.log	11 KB	2014-03-31 21:36
arm2-system.log	11 KB	2014-03-31 21:36

**Historical logs**

File Name	Size	Last Modified
log.0.tar.gz	22 KB	2014-02-24 16:28
log.1.tar.gz	31 KB	2014-02-24 16:36
log.2.tar.gz	34 KB	2014-02-24 22:31
log.3.tar.gz	40 KB	2014-02-25 10:50

## Factory resetting the TelePresence endpoint

When factory resetting the endpoint the following happens:

- The call logs will be deleted.
- Passwords and system parameters will be reset to default values.
- All files uploaded to the system will be deleted.
- The previous (inactive) software image will be deleted.
- Option keys and release keys will be preserved.
- Automatic restart of the system.

**NOTE:** It is not possible to undo a factory reset.

### Useful information

Make sure to collect the call logs before factory resetting the endpoint. Refer to "[Collecting log files from a TelePresence endpoint](#)" on page 56.

After the factory reset a notification will display on the main screen for about 10 seconds.

After the factory reset you will need to re-configure the endpoint. Refer to: [Cisco TelePresence Video Systems Getting Started Guide](#)

### Using the Touch panel

1. Tap gently on the Touch panel if the unit is in sleep mode.
2. Tap the upper left corner of the Touch panel, followed by *Settings > Administrator > Reset*.  
You have to sign in with administrator credentials to open the Administrator menu.
3. Tap the *Factory Reset* button.
4. The system will revert to the default factory settings and automatically restart. This will take a few minutes.

### Using the command line interface

1. Start a command line interface (for example PuTTY). Enter the host name (or IP address) of the codec and set connection type to SSH.
2. Sign in with the appropriate username and password.
3. Run the following command: `xCommand SystemUnit FactoryReset Confirm: Yes`
4. The system will revert to the default factory settings and automatically restart. This will take a few minutes.

### Using the web interface

1. Open a web browser and enter the IP address of the video system in the address bar.
2. Navigate to *Maintenance > System Recovery > Factory Reset*.  
**NOTE:** Read the provided information carefully before proceeding.
3. Click *Perform a factory reset*.
4. The system will revert to the default factory settings and automatically restart. This will take a few minutes.

## Finding the MAC address of the endpoint

The MAC (Media Access Control) address can be found:

- On the System Information page (using the web interface, Touch controller or remote control).
- By running an API command using a command line interface.
- On the rating label of the TelePresence endpoint.

### Finding the MAC address on the System Information page

#### Using the web interface

To find the system's MAC address, navigate to *Home > System Information* and see the *General* section.

#### Using the Touch controller

To find the system's MAC address tap the upper left corner of the Touch panel, followed by *Settings > System Information*. Then see the *Hardware* section.

#### Using the remote control

To find the system's MAC address, navigate to *Home > Settings > System Information* and see the *Hardware* section.

### Finding the MAC address using a command line interface

To find the system's MAC address:

1. Open a command line interface (e.g. PuTTY) and log in to the endpoint (codec)
2. Run the following API command:  

```
xStatus Network 1 Ethernet MacAddress
```

### Finding the MAC address on the rating label

The rating label is found on the physical unit.

If the product is already mounted (wall/rack) it will be more convenient to use one of the other methods described on this page to find the MAC address.

The rating label is underneath the codec:

- Cisco TelePresence Quick Set C20
- Cisco TelePresence Codec C40, C60, C90
- Cisco TelePresence SX20 Quick Set
- Cisco TelePresence SX80

The rating label is on the rear side of the unit:

- Cisco TelePresence System EX60, EX90
- Cisco TelePresence SX10 Quick Set

The rating label is on the rear side, behind the back cover:

- Cisco TelePresence MX200, MX300
- Cisco TelePresence MX200 G2, MX300 G2

The rating label is on the rear side of the panel; remove the left side cover to find it:

- Cisco TelePresence MX700, MX800

If you have a Cisco TelePresence Profile Series, please use one of the other methods to find the MAC address, as the codec is mounted inside the column of the unit.

## Creating a remote support user

In cases where you need to diagnose problems on the video system you can create a remote support user.

The remote support user will be granted read access to the system and will have access to a limited set of commands that can aid troubleshooting.

You will need assistance from Cisco Technical Assistance Center (TAC) to acquire the password for the remote support user.



The remote support user should only be enabled for troubleshooting reasons when instructed by Cisco TAC.

### How to create a remote support user for a TelePresence endpoint.

Open a web browser and log in to the Cisco TelePresence endpoint. Navigate to *Maintenance > System Recovery*. Choose the *Remote Support User* tab.

#### System Recovery

In order to recover the system when experiencing a severe issue, a Software Recovery Swap or a Factory Reset can be performed. These recovery methods should only be attempted by a system administrator or in contact with Cisco technical support. The preferred recovery method is to perform a Software Recovery Swap and Factory Reset as last resort.

Backup   Software Recovery Swap   Factory Reset   Remote Support User

In order to diagnose problems on the TelePresence device, you might require extended privileges. This is obtained by creating a remote support user below, and then giving the supplied token to Cisco Support. The token will allow them to create a privileged support user on this device. This user will be valid for 7 days.

The system does not have an active remote support user.

Create user   Delete user

Expiry:

2014-04-14 08:28:31 UTC

Token:

```
FhUsRByooPauNo02HgtXEeBzfCuR/KGRJ2FMJYH+26/X9
wIXeEXPJkS10Ewaf1AbLQLvqMyjWntDrubcKD94UijA9t
c5Qy4Iq2dF874FF8iJaVs2M0sPhHkb2jHZuk5z4cJNvs
m5eoJHGasTXZIkYrqqZYGTA8fbvzuapq9mBbiUq8Y4Rda
6uLbSjVjhIDDz9a9obSgiqLR5NUBXhIITiG16h4P4mc6j
KnS1WISh5cdzTmS6fx2q16uguX+EXLKG/gPvIBtJc1109
RYfgNF1S5FX/uVrNFYGFxsV12u6AFYIORmd8vz3qigPcJ
3ev8EdequB0r176ChxGLMZKLoig==
```

The system has an active remote support user.

Create user   Delete user

#### Create remote support user

1. Open a case with Cisco TAC.
2. Click [Create user](#).
3. Copy the text in the *Token* field and send to Cisco TAC.
4. Cisco TAC will generate a *password*.

The remote support user is valid for seven days, or until it is deleted.

#### Delete remote support user

Click [Delete user](#).

## Understanding Cisco Discovery Protocol on the Cisco TelePresence endpoints

### Introduction

Cisco Discovery Protocol (CDP) is a proprietary layer-2 management protocol developed by Cisco in the early 1990s to provide enhanced automation of network discovery and management. It is broadly deployed on millions of existing Cisco products and provides countless benefits to network administrators for managing router and switch interfaces. With the introduction of IP Telephony in the late 1990s and early 2000s, CDP was enhanced to provide additional automation capabilities for IP-based telephones, including automatic VLAN discovery, Power over Ethernet (PoE) negotiation, Quality of Service (QoS) automation, location awareness (to automate the discovery of the physical location of an IP telephone for management and emergency services purposes), Ethernet speed and duplex mismatch detection, and more.

**NOTE:** The IETF, IEEE and TIA, in cooperation with Cisco and numerous other networking vendors, have since created the IEEE 802.1AB standard, known as Link-Layer Discovery Protocol (LLDP), with extensions developed for Media Endpoint Discovery (LLDP-MED) for voice and video endpoints. LLDP-MED will eventually subsume CDP, but this may take years to unfold due to the enormous installed-base and widespread use of CDP.

### History

Cisco acquired TANDBERG in April 2010. The TANDBERG portfolio of video endpoints compliments Cisco's existing TelePresence and Unified Communications solutions. CDP support was introduced on the Cisco E20 in release TE4.0 and on the other TelePresence endpoints in TC5.0.

CDP was supported on the following endpoints in software version TC5.0: MX200, MX300, EX60, EX90, C20, C40, C60, C90, and Profile series. Endpoints that have been introduced in later TC releases support CDP.

However, because there is already an installed-base of these endpoint models (prior to the Cisco acquisition) that are not running CDP, introducing CDP in a software release requires careful consideration of how the new automation functionality will affect that existing installed-base.

Enabling CDP by default could cause undesired behavior for those existing deployments when they upgrade to a CDP-enabled release and the devices suddenly begin using VLAN automation, so CDP is being introduced in a phased approach.

### Benefits provided by CDP

As mentioned in the introduction above, CDP provides numerous automation benefits for network administrators deploying IP-based voice and video endpoints on their networks. This section briefly highlights some of the most pertinent benefits for IP-based voice/video endpoints like the Cisco TelePresence MX, EX, SX, C90, C60, C40, C20, and Profile series.

### Automatic VLAN discovery

Virtual LANs (VLANs) allow a network administrator to introduce IP-based telephones and video terminals onto their network without the need for re-addressing their existing data subnets, or adding additional Ethernet ports to their switches. Leveraging the 802.1Q standard, a device such as the endpoint can tag its Ethernet

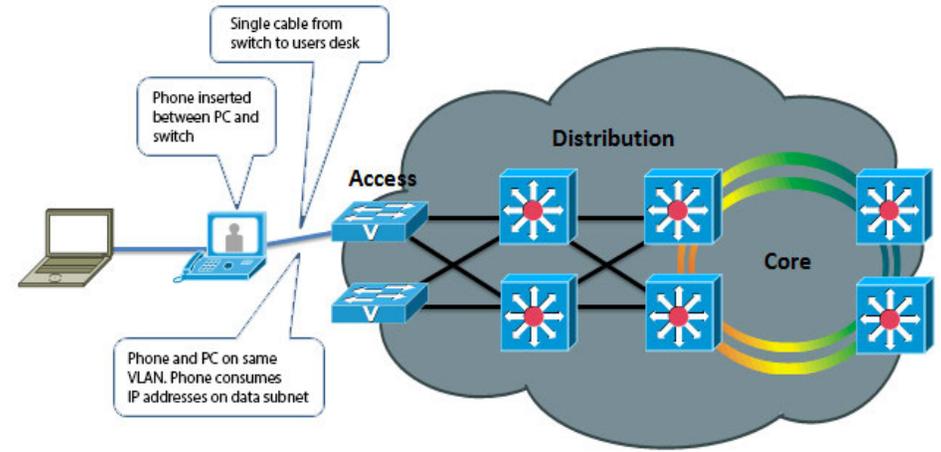


Fig. 1: Without VLANs

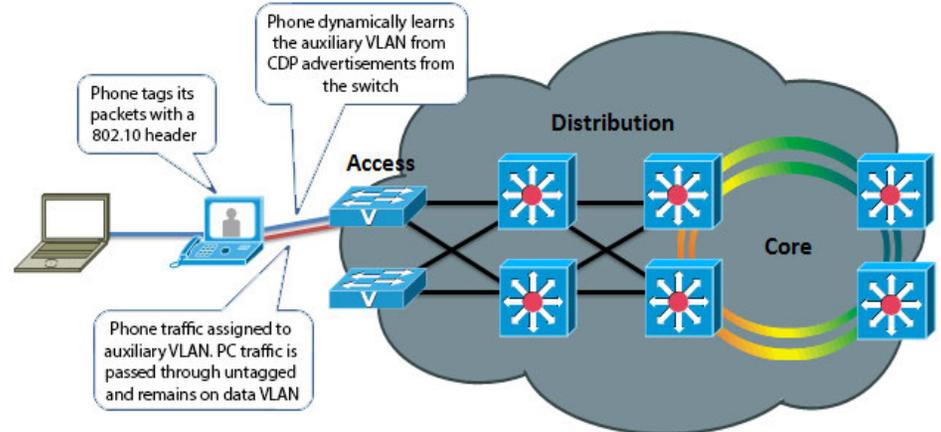


Fig. 2: With VLANs

frames with the VLAN ID that its traffic belongs to, placing its traffic into the voice/video VLAN (known as the auxiliary VLAN); while Ethernet frames sent by a PC are not tagged, and therefore end up in the data VLAN (known as the native VLAN). This allows the endpoint to be inserted in between an existing PC and the Ethernet switch to which it is attached, allowing for a single Ethernet port per user, thereby eliminating the need to add additional ports in the wiring closet, and allowing the endpoint to be assigned to a different (new) IP sub net rather than consuming IP addresses in the existing PC VLAN. VLANs also allow the network administrator to apply different security and Quality of Service (QoS) policies on a per-VLAN basis.

Figure 1 and 2, on the previous page illustrates, these concepts.

Without CDP (or LLDP-MED), the user must manually configure each endpoint with the 802.1Q VLAN ID it should use. CDP automates this task, allowing the Ethernet switch to advertise to the endpoint the ID of the VLAN it should belong to.

### Automatic Quality of Service

Quality of Service is essential for a well-performing network, providing preferential service to latency, jitter or loss sensitive applications like voice and video; deferential service to misbehaving applications such as viruses and other undesirable network traffic; and fair treatment to routine, non-time sensitive traffic such as e-mail or web browsing. However, QoS can be complex to configure and manage, and the administrator needs to be assured that the traffic entering the network is marked with the correct QoS values. For user-facing devices such as PCs, IP-based telephones and video terminals, the administrator must establish a demarcation point where QoS markings coming in from

these devices are either not trusted—and instead overwritten to an administratively configured value—or trusted to set their own QoS values and the Ethernet switch will honor those values. This demarcation point, or trust boundary, ensures that if the user accidentally, or intentionally, tampers with the QoS values assigned to these devices, those QoS values will be remarked by the administrator as they ingress the network.

CDP provides a method of automatically extending this trust boundary (at the administrators' discretion) so that the phone or video terminal can mark its packets with the desired QoS values, and the switch will trust the phones packets (because the administrator knows that the specific model of phone in question can be trusted to behave properly and cannot be tampered with) and forwards those packets on into the network. This functionality is known as AutoQoS on the Cisco Catalyst line of Ethernet switches.

Figure 3 and 4, to the right, illustrates the concept of AutoQoS.

Further information about AutoQoS can be found at the following reference, Medianet Campus QoS Design guide:

▶ [http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN\\_and\\_MAN/QoS\\_SRND\\_40/QoS\\_Campus\\_40.html](http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoS_Campus_40.html)

### Power over Ethernet (PoE) negotiation

The 802.3af standard provides Power over Ethernet to devices such as IP-based telephones and video terminals. CDP provides additional benefit by allowing the endpoint to indicate to the Ethernet switch how much power it requires—and for the switch to advertise to the endpoint how much power is available—thereby allowing more granular level of negotiation between the switch and the endpoint, and allowing the Ethernet switch to

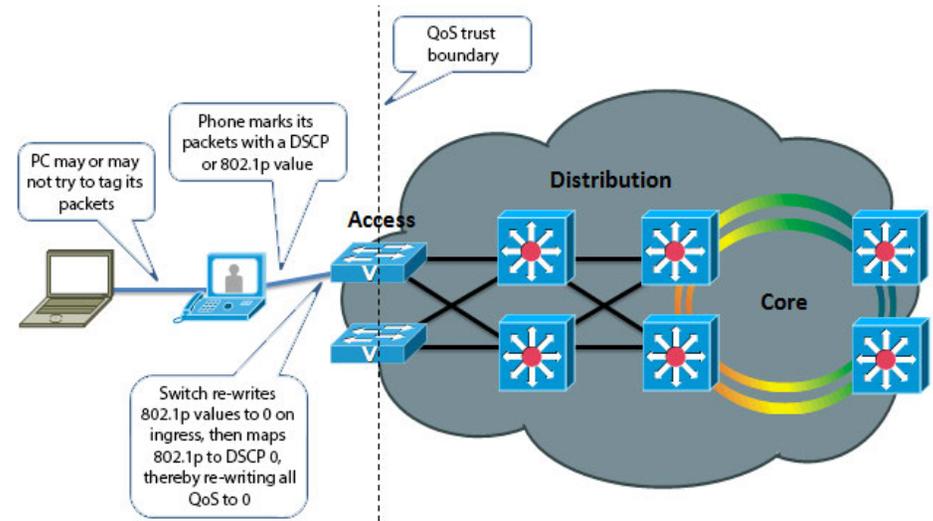


Fig. 3: Without CDP / AutoQoS

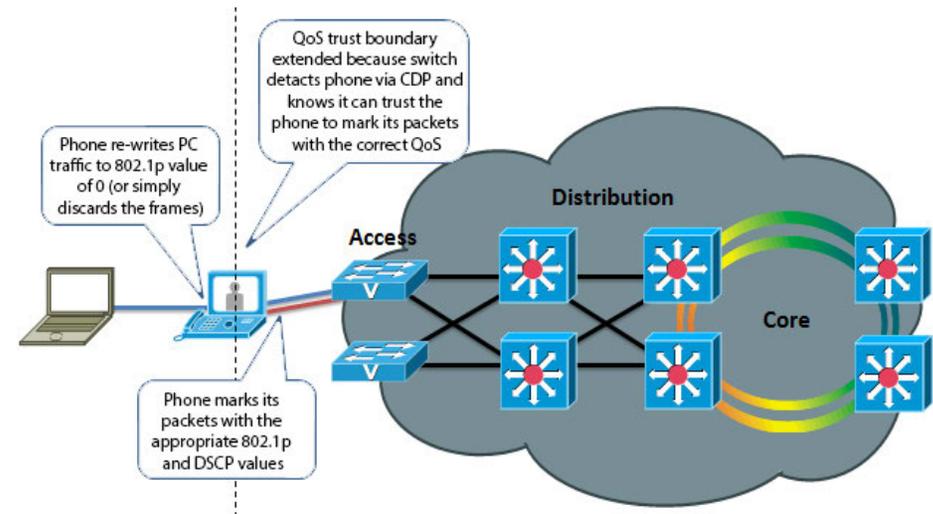


Fig. 4: With CDP / AutoQoS

more closely track its available power budget.

Note that PoE is currently used only by the Cisco TelePresence SX10; it is not used by the other TelePresence endpoints. PoE is widely used by many other models of Cisco Unified IP Phones, Wireless Access Points, surveillance cameras, and myriad other devices.

### Location awareness

With the introduction of IP-based telephones, a new level of mobility was afforded in that an IP endpoints could be plugged in anywhere in the network, obtain an IP address, and start making calls, reducing the costs associated with physically patching telephone cables when moving an employee from one office to another. However, certain management functions and emergency services rely on knowing the precise location of a telephone. CDP allows for network management applications to identify the physical location of a phone (by detecting what Ethernet port that phone is attached to, and hence, where it physically is located). This information is then leveraged by applications such as Cisco Emergency Responder to direct telephone calls made to emergency services personnel to the correct dispatch office. There are many other real and potential uses for location information.

### Ethernet speed/duplex mismatch detection

Ethernet devices use the 802.3 auto negotiation procedure to automatically negotiate their speed and duplex settings. However, a very common problem is that one side or the other is accidentally configured for the wrong settings, resulting in packet loss. For example, the network administrator has configured all the Gigabit Ethernet ports on the switch for auto negotiation, but the user accidentally sets the port on his or her PC, IP phone or video terminal to a manually configured value, such as 100Mbps / Full duplex. This can result in a mismatch between the switch and the endpoint, resulting in a large percentage of loss on that interface. CDP does not automate the resolution of such a condition, but it does detect it and cause an alarm to be generated on the switch, notifying the administrator of the condition so that he or she may take steps to resolve it.

### Future Medianet applications

The above benefits of CDP have been available for years from Cisco. Medianet is a new concept aimed at further extending and automating the interactions between endpoints and the network in order to deliver additional end-to-end optimization of multimedia traffic across an intelligent internetwork. CDP is one protocol, among others, that will be leveraged by future generations of Cisco IOS Software and Cisco Medianet-ready endpoints to deliver on this vision. Available Medianet applications at the time this document was written include end-to-end tracing of the path a video session takes through a network in order to pinpoint the source of packet loss, optimizing the routing of video packets over alternate paths in order to maximize the throughput of the network, enhanced Session Admission Control in order to control the amount of video sessions admitted onto the network, and more.

### CDP behavior in release TC5, and later

When the Cisco TelePresence endpoint is booted for the first time, or after a factory reset has been performed, the following settings are applied by default:

- xConfiguration Provisioning Mode: Auto
- xConfiguration Network 1 VLAN Voice Mode: Auto

The provisioning mode can be set from the Touch user interface using the Provisioning Wizard, or you can manually set the parameters.

- When provisioning mode is set to *Cisco CUCM*, the *Network VLAN Voice Mode* must be set to *Auto* (the Provisioning Wizard on Touch will automatically set the VLAN voice mode). The endpoint starts utilizing CDP to automatically discover its VLAN and starts to tag its packets with the appropriate VLAN ID. It will also include DHCP Option 150 in its DHCP requests so that it can automatically discover the address of the Cisco Unified Communications Manager TFTP server.

Once these parameters are set they will remain persistent through subsequent reboots. If a user later wishes to change them, they may do so by re-running the Provisioning Wizard, or by manually setting the parameters.

This behavior does present an extra step in the first-time boot up process, but once CUCM mode has been chosen in the Provisioning Wizard, CDP will automatically kick in and the phone will join the auxiliary (voice/video) VLAN. If the customer does not wish to use the CDP, then it may be manually disabled by setting the Network VLAN Voice Mode to Off.

For customers who do not have a CDP-capable Ethernet switch, but wish to use 802.1Q VLANs, the Network VLAN Voice Mode may be set to Manual, and the associated Network VLAN Voice ID may be set to the appropriate value.

### Summary

This document has briefly introduced the history and benefits of the Cisco Discovery Protocol (CDP) and its behavior on the Cisco TelePresence video endpoints.

CDP is a powerful mechanism for automating the application of VLANs and Quality of Service for voice/video devices. Existing Cisco customers are encouraged to begin exploring its benefits and preparing their networks so they can begin leveraging VLANs, AutoQoS and VLAN-based security policies for their Cisco video endpoints.

## User documentation on the Cisco web site

The user documentation is found here: [▶ http://www.cisco.com/go/telepresence/docs](http://www.cisco.com/go/telepresence/docs)  
Depending on which product you have, select the following in the right pane:

### EX Series:

- Collaboration Endpoints
  - > Collaboration Desk Endpoints
    - > TelePresence System EX Series
      - > TelePresence System EX Series

Or click: [▶ http://www.cisco.com/go/ex-docs](http://www.cisco.com/go/ex-docs)

### Codec C Series and Quick Set C20:

- Collaboration Endpoints
  - > TelePresence Integration Solutions
    - > TelePresence Integrator C Series
      - > TelePresence Integrator C Series

Or click: [▶ http://www.cisco.com/go/cseries-docs](http://www.cisco.com/go/cseries-docs)

### SX Series:

- Collaboration Endpoints
  - > TelePresence Integration Solutions
    - > TelePresence SX Series
      - > TelePresence SX Series

Or click: [▶ http://www.cisco.com/go/sx-docs](http://www.cisco.com/go/sx-docs)

### MX Series:

- Collaboration Endpoints
  - > Collaboration Room Endpoints
    - > TelePresence MX Series
      - > TelePresence MX Series

Or click: [▶ http://www.cisco.com/go/mx-docs](http://www.cisco.com/go/mx-docs)

### Profile Series:

- Collaboration Endpoints
  - > Collaboration Room Endpoints
    - > TelePresence Profile Series
      - > TelePresence Profile Series

Or click: [▶ http://www.cisco.com/go/profile-docs](http://www.cisco.com/go/profile-docs)

### Cisco Unified Communication Manager (CallManager):

- Unified Communications
  - > Call Control
    - > Unified Communications Manager (CallManager)

Or click: [▶ http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html](http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html)

### Document categories

The documents are organized in the following categories:

#### User guides:

*Maintain and Operate > End-User Guides*

#### Quick reference guides:

*Maintain and Operate > End-User Guides*

#### Installation guides:

*Install and Upgrade > Install and Upgrade Guides*

#### Getting started guide:

*Install and Upgrade > Install and Upgrade Guides*

#### Administrator guides:

*Maintain and Operate > Maintain and Operate Guides*

#### API reference guides:

*Reference Guides > Command references*

#### Physical interface guides:

*Maintain and Operate > End-User Guides*

#### Regulatory compliance and safety information:

*Install and Upgrade > Install and Upgrade Guides*

#### TC software release notes:

*Release and General Information > Release Notes*

#### TC software licensing information:

*Release and General Information > Licensing Information*

#### Video conferencing room guidelines:

*Design > Design Guides*

#### Knowledge base articles and frequently asked questions:

*Troubleshoot and Alerts > Troubleshooting Guides*

#### CAD drawings:

*Reference Guides > Technical References*

### Intellectual property rights

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, EXPRESSED 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](http://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.

TANDBERG is now a part of Cisco. TANDBERG® is a registered trademark belonging to TANDBERG ASA.

### Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: [▶ http://www.cisco.com/web/siteassets/contacts](http://www.cisco.com/web/siteassets/contacts)

Corporate Headquarters  
 Cisco Systems, Inc.  
 170 West Tasman Dr.  
 San Jose, CA 95134 USA