Deployment Guide

- Cisco TelePresence MX Series
- Cisco TelePresence SX Series
- Cisco Unified Communications Manager

Software versions CE8.0 and
Cisco Unified Communications Manager 11.0.1
DECEMBER 2017

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...

We recommend that you visit the Cisco website regularly for updated versions of this guide. Go to:
▸ https://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. Click them to go to the topic.

Table of contents

Introduction 3
Introduction 4
Prerequisites 4
Recommended sequence when configuring 4
Device packages 4
Encrypted vs nonencrypted communication 4
Endpoints previously used with TMS 4
Endpoints factory reset 4
About software versions 5
Endpoints supported in CE8.0 5
CUCM versions vs endpoints supported 5
Limitations 5
Useful links 5
What's new in this version 6

CUCM configuration 7
Sign in to Cisco Unified CM Administration 8
Creating a SIP profile 9
SIP Profile configuration 9
Set the Default SIP Message Size 10
About the phone security profile 11
About non-secure and secure profiles 11
Creating a phone security profile 12
Phone security profile information 12
Phone security profile CAPF information 12
Manual registration of the endpoint 13
Adding a new phone (endpoint) 13
Device information 14
Protocol-specific information 14
Certification authority proxy function 14
External Data Locations information 15
Extension information 15
Product-specific configuration layout 16
Add directory number 20
Directory number information 20
Configuring shared lines 21
Display caller name 21
Auto-registration of the endpoint 22
Enable auto-registration 22
How to verify the endpoint registration 23
Specify the home cluster service for the end user 24
Associate a user with an access control group 24
Add the user to an access control group 24
Enterprise parameters 24
Clusterwide Domain Configuration 24

Endpoint configuration 25
About endpoint configuration 26
Endpoint diagnostic tools 26
Endpoint configuration in three steps 26
Finding the IP address 26
Setting the system passphrase 27
Access through HTTP 27
Endpoints with a secure (encrypted) security profile 27
Endpoints with a non-secure security profile 27
Setting the call details 28
Endpoint provisioning 29
Setting up CUCM provisioning 29
Setting up provisioning from CUCM via Expressway (Mobile and Remote Access) 30
Verifying the identity of the Expressway 30

Appendices 32
Ad hoc conferencing 33
Shared lines 33
Network Time Protocol (NTP) 34
Finding the MAC address of the endpoint 35
Understanding Cisco Discovery Protocol on the Cisco TelePresence endpoints 36
User documentation on the Cisco web site 39

Cisco contacts 40

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 how to register Cisco TelePresence MX and SX series endpoints on Cisco Unified Communications Manager (CUCM).

Endpoints can register to CUCM also when the endpoint is not within the enterprise network. In such cases, you need Cisco Expressway infrastructure 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.

This guide covers the software versions TelePresence endpoints CE8.0 and CUCM 11.0.1. We recommend using the latest software versions to support all features and functions.

Most features and configurations also apply to CUCM versions 8.6.2, 9.1.2, and 10.5(1), but some menus may have changed in newer versions. Make sure that you have the latest device package.

Prerequisites

We assume that you are familiar with the basics of the user interface of the CUCM and the Cisco TelePresence endpoints.

Recommended sequence when configuring

1. First you configure the CUCM.
2. Then you set up the endpoint for CUCM provisioning.

Check that you have access to the endpoint through HTTP in the endpoint configuration on CUCM. If using a command line interface, check that SSH is enabled. See "Product-specific configuration layout" on page 16 to enable and disable web access and SSH access.

Device packages

The CUCM Device Package contains device configuration capabilities for the Cisco TelePresence endpoints. The device package is available on our website. Go to: https://software.cisco.com/download 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: Cisco Unified Communications Manager Device Package Compatibility Matrix

Encrypted vs nonencrypted communication

The deployment is considered nonsecure with the standard phone profile (nonencrypted 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.

Endpoints previously used with TMS

If the endpoint has previously been used with Cisco TelePresence Management Suite (TMS), make sure that it is purged from TMS.

For instructions on how to handle endpoint migration to CUCM in TMS, see Cisco TelePresence Management Suite Administrator Guide

Endpoints factory reset

Usually a factory reset of the endpoint is not needed before provisioning it to the CUCM.

Factory reset is recommended before provisioning:

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

Factory reset is described in the Administrator guide for your product.

https://www.cisco.com/go/mx-docs

https://www.cisco.com/go/sx-docs

About software versions

Before you start configuration, make sure that 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 CE8.0

- SX Series (SX10, SX20, SX80)
- MX Series (MX200 G2, MX300 G2, MX700, MX800)

CUCM versions vs endpoints supported

All TelePresence endpoints that are supported in CE8.0 are also supported in CUCM 8.6.2, 9.1.2, 10.5.1, and 11.0.1. Use the latest device package to be sure that all endpoints are covered.

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

Overview of the device packages for CUCM: Cisco Unified Communications Manager Device Package Compatibility Matrix

Limitations

- CUCM 9.0 does not support Directory URI provisioning of the TelePresence endpoint. You need CUCM 9.1 or later.
- When a user changes the locale on the endpoint to a locale that is not supported in CUCM and the endpoint is reprovisioned from CUCM, the locale on the endpoint is reset to English.

Useful links

User documentation and software download for the TelePresence endpoints:

https://www.cisco.com/go/telepresence/docs

User documentation and software download for CUCM:

https://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:

https://www.cisco.com/cisco/web/support

Cisco TelePresence CE Release Notes:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/products-release-notes-list.html

What's new in this version

December 2017

Updated the article "Network Time Protocol (NTP)" on page 34 in the Appendices section.

August 2017

Added an article about "Network Time Protocol (NTP)" on page 34 in the Appendices section.

December 2015

This section provides an overview of the new and changed features since the previous version of this guide was issued (TC7.2 on CUCM version 10.5.1). The CUCM must have a device package with support for CE8.0. See the CE Software Release Notes for detailed information.

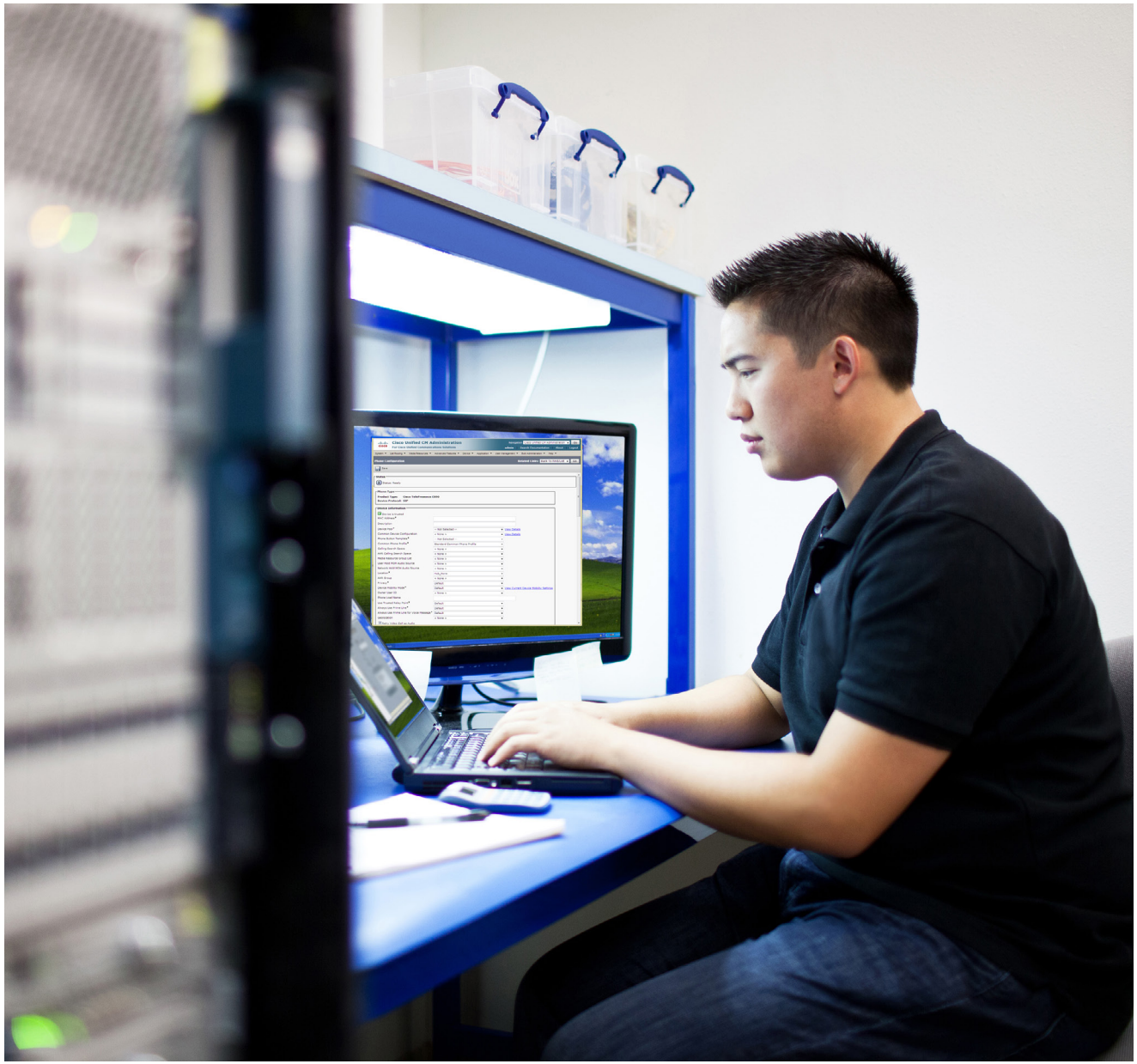
https://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/products-release-notes-list.html

Proximity

The Proximity feature allows the users to connect their PC / MAC, iOS or Android device to an endpoint wirelessly. Depending on what services has been enabled for Proximity, the user can get locally or remotely shared content to their Android or iOS device, and/or access endpoint call control. When Proximity is connected with the Cisco Proximity app for PC or MAC, the user can wirelessly share images of their laptop screen locally if the system is not in a call and remotely if the system is in a call.

Write Back

The first time an endpoint is provisioned from CUCM, all settings are pushed from CUCM to the endpoint. Anything that was set on the endpoint before the provisioning will be overwritten by CUCM. If you change settings on the endpoint after the first CUCM provisioning, these changes will be written back to CUCM. Likewise, if you push new changes from CUCM to the endpoint, settings on the endpoint will be overwritten. This way, the endpoints will always get the latest settings, whether they are set from CUCM or originally changed at the endpoint side.



CHAPTER 3

CUCM CONFIGURATION

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

Sign in to Cisco Unified CM Administration

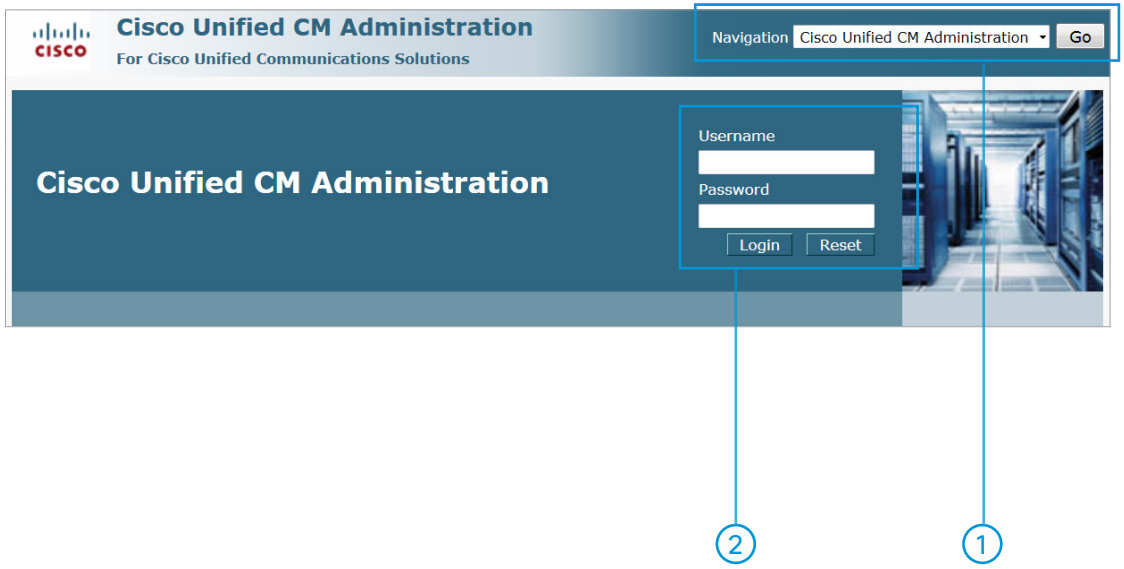
Open a web browser and enter the hostname or IP address of the Cisco Unified CM and select *Cisco Unified Communications Manager* from the list of installed applications.

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

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

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

NOTE: In this guide, we have chosen to describe the settings that are important when endpoints are provisioned to CUCM. Adjust other settings as needed, or leave them with the default value.



Creating a SIP profile

You can copy a profile to use as a template.

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

Copy a profile to use as a template: Click *Find* to list all profiles, then select a profile and click *Copy*. This action opens the *SIP Profile Configuration* page.

Or: Click *Add New* to create a new profile. This action opens 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:

Select **Enable** 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 24.

SDP Session-level Bandwidth Modifier for Early Offer and Reinvites:

Set to **TIAS and AS**.

Navigate to the *Trunk Specific Configuration* section:

Allow Presentation Sharing using BFCP:

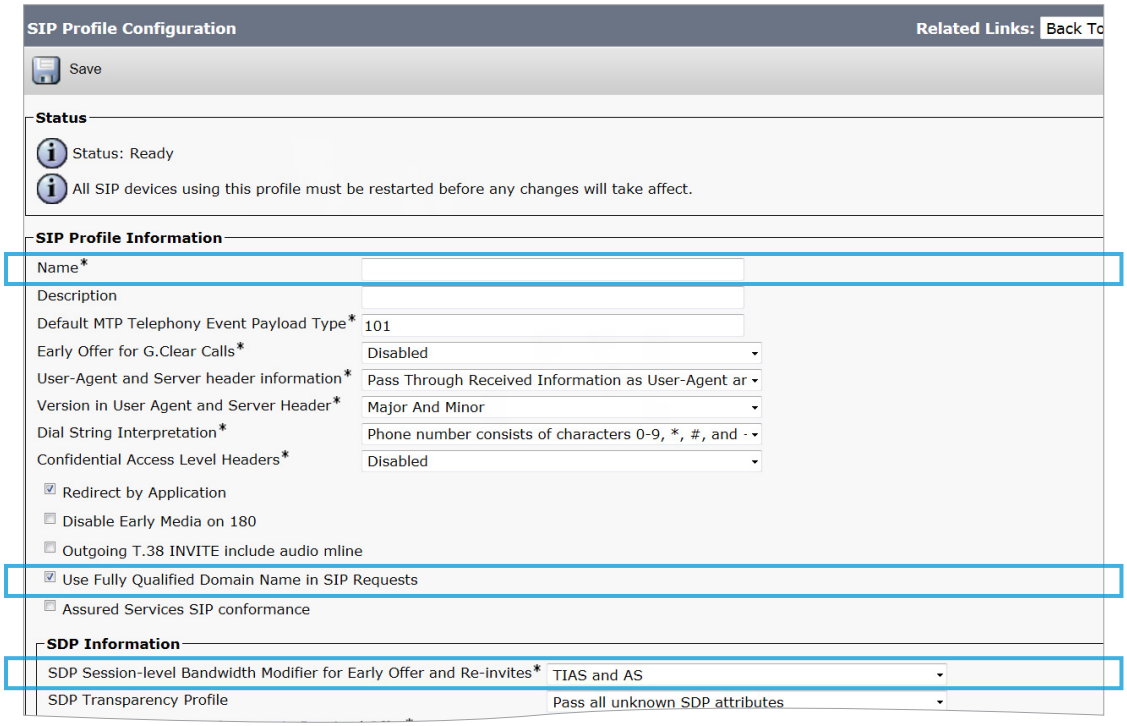
Select **Enable** to allow presentation sharing.

Allow IX Application Media:

Select **Enable** to enable the ActiveControl feature, if available on the endpoint.

When done click **Save**.

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

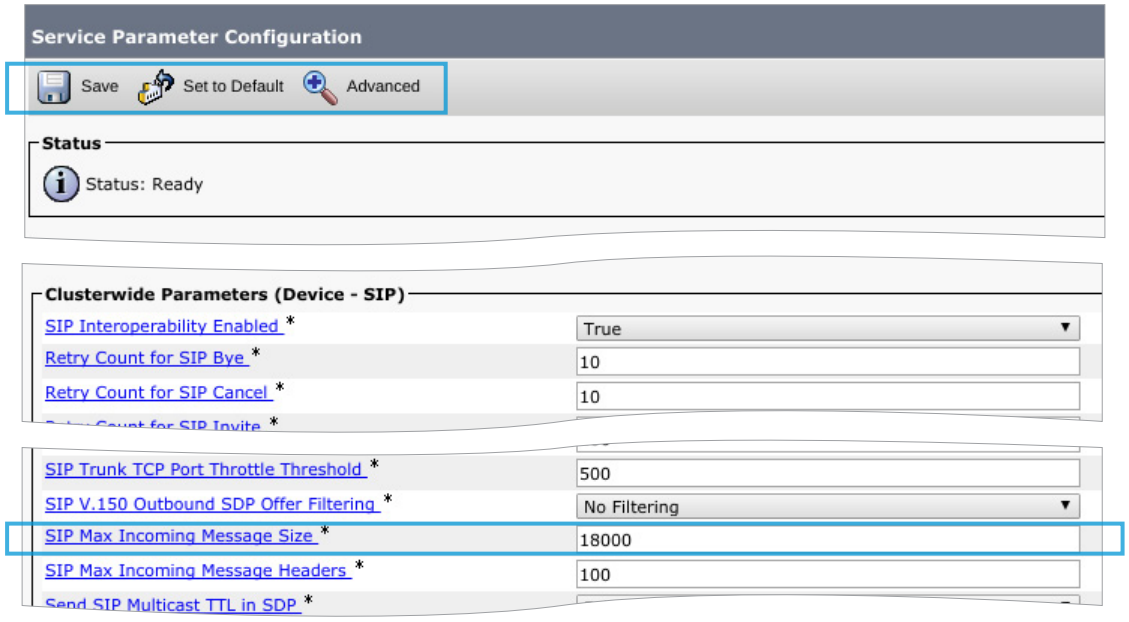


Navigate to the **Trunk Specific Configuration** section.

Set the Default SIP Message Size

The default SIP message size needs to be set to a high enough value for Multistream to work. Multistream is a feature that enables the endpoint to send and receive multiple streams of video at different resolutions.

1. In CUCM, choose *System > Service Parameters*.
2. Choose the active server from the Server drop-down list.
3. Choose *Cisco CallManager (Active)* from the Service drop-down list.
4. Click *Advanced* in the toolbar, since the message size is not shown in the default view.
5. Scroll to the *Clusterwide Parameters (Device - SIP)* section.
6. Set the *SIP Max Incoming Message Size* parameter. We recommend setting the paramter to 18000.
7. Click **Save**.



About the phone security profile

Security profiles must be defined when using secure (encrypted) communication, else use the non-secure profile. Note the following:

- CUCM must operate in mixed mode (cluster security mode) to enable secure communication.
- Define one device security profile for each endpoint type.
- If you want to allow several authentication modes for the same endpoint type, define one profile for each mode.

See the CUCM Security Guide for further information

About non-secure and secure profiles

TelePresence endpoints support **Non-secure** and **Encrypted** modes. They do not support Authenticated mode. When endpoints are connected to CUCM by Expressway, they support only **Non-secure** mode.

Non-secure profile

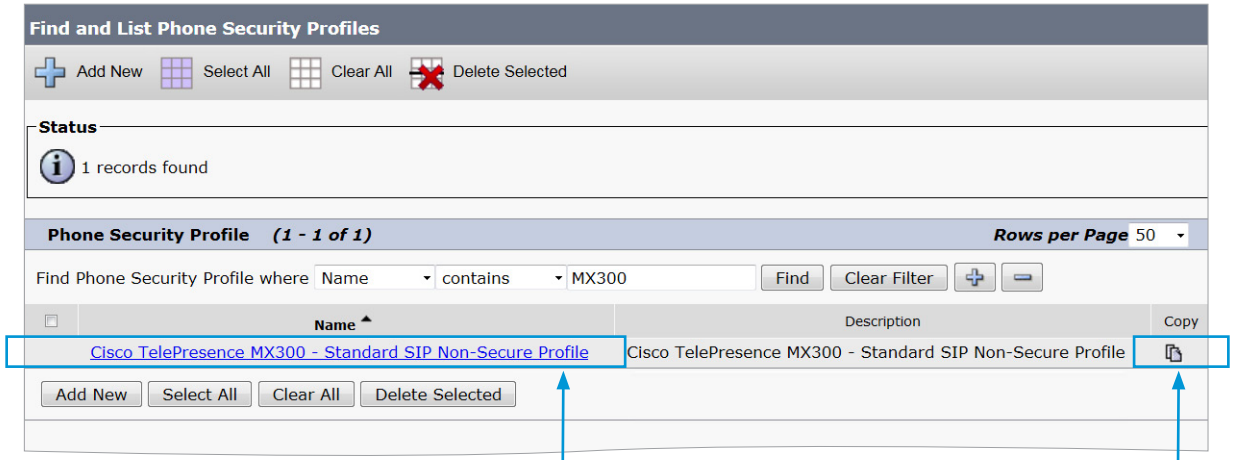
The non-secure endpoints use the **predefined non-secure profile**. See "Manual registration of the endpoint" on page 13.

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 method is 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 is the same using either method, but the default values may vary.



Editing a security profile

The non-secure endpoints 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.

Creating a phone security profile

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

1. Navigate to *System > Security > Phone Security Profile*.
2. **Copy** an existing profile or click **Add New** on the *Find and List Phone Security Profiles* page.

Then continue to set up the profile. When done with the profile, click **Save** to confirm the changes.

Phone security profile information

Navigate to the *Phone Security Profile Information* section and fill in the applicable information:

Name:

Enter the profile name.

Description:

Enter the profile description.

Device Security Mode:

Set to Encrypted.

Transport Type:

Set to TLS.

TFTP Encrypted Config:

Check this check box to enable TFTP encrypted configuration.

Phone security profile CAPF information

Navigate to the *Phone Security Profile CAPF Information* section and fill in the applicable information:

Authentication Mode:

Choose the appropriate value from the drop-down.

By Null String: The Certificate Authority Proxy Function (CAPF) process starts automatically.

By Authentication String: The CAPF process commences 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. In other words, it cannot be used the first time the CAPF process runs.

Key-size:

Choose the appropriate value from the drop-down. The recommended key size is 1024.

Manual registration of the endpoint

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

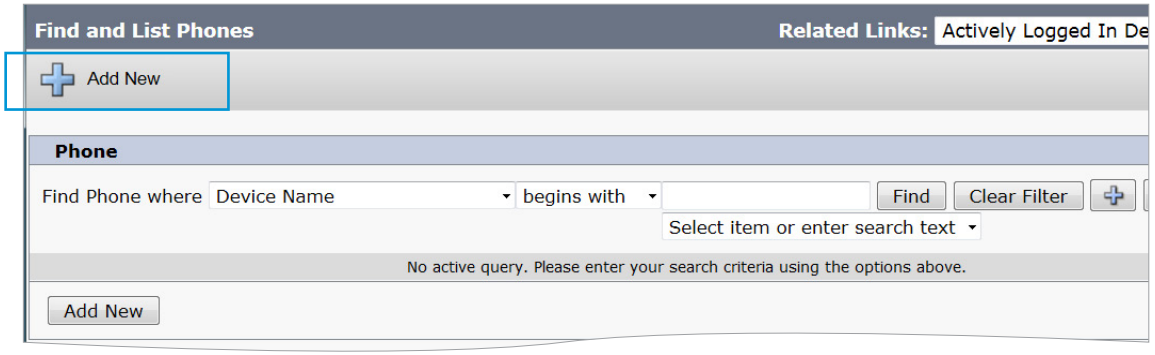
Adding a new phone (endpoint)

1. Navigate to *Device > Phone*.
2. Click *Add New* to add a new phone (endpoint).
3. Navigate to *Create a phone using the phone type or a phone template* section.
4. From the drop-down, choose the type of TelePresence endpoint you are going to register.
5. Click **Next**.

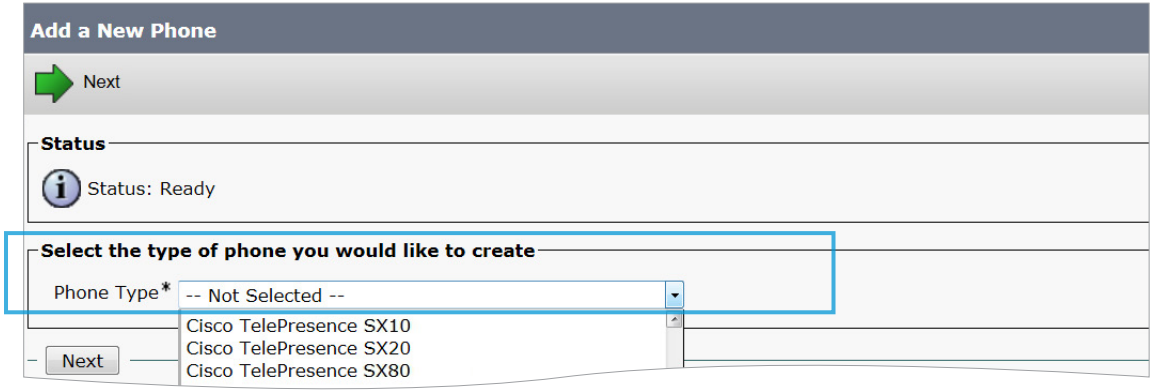
Then set the configurations described on the next pages.

When you have set the configurations, remember to click **Save** to confirm the changes.

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



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



Adding a new phone (endpoint) continued...

Device information

MAC Address:

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

See: "Finding the MAC address of the endpoint" on page 35.

Device Pool:

Choose a Device Pool.

Phone Button Template:

Choose a Phone Button Template.

If the TelePresence endpoint is connected to CUCM by 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 user management.

Protocol-specific information

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.

Certification authority proxy function

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.
3. TelePresence endpoints are not connected to CUCM by Expressway.

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.

By Null String: The Certificate Authority Proxy Function (CAPF) process starts automatically.

By Authentication String: The CAPF process starts 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. In other words, it cannot be used the first time the CAPF process runs.

Key-size:

Choose the appropriate value from the drop-down. The recommended key size is 1024.

Adding a new phone (endpoint) continued...

Operation Completes By:

Make sure that the date and time are set to a future date and time. If set to the past, the installation or upgrade is not performed.

External Data Locations information

Navigate to the *External Data Locations Information* section:

Leave all fields blank to accept the default settings.

Extension information

Enable Extension Mobility:

Select to enable Extension Mobility.

Log Out Profile:

Choose a device profile for the endpoint that is used when no one is signed in to the device by using Cisco Extension Mobility.

Log In Time:

This field remains blank until a user logs in. When a user signs in, the log in time is displayed in this field.

Log Out Time:

This field remains blank until a user logs in. When a user is signed in, the time at which the system signs out the user is displayed in this field.

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

Adding a new phone (endpoint) continued...

Product-specific configuration layout

Navigate to the *Product Specific Configuration Layout* section and configure the settings described on the following pages.

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

NOTE: TMS supports Alternate phone book feature from software release 14.4.

NOTE: CUCM will have support for Alternate phone book feature in a device package which will be released sometime after TC7.

Room Name (from Exchange(R)):

The Exchange Conference Room Name is used for scheduling meetings where this TelePresence system participates. This setting must match the email address used in Exchange exactly. Example: `room1@example.com`. Default value is <empty> and maximum length is 64 characters.

Web Access:

Enable or disable whether the device accepts connections from a web browser or other HTTP clients. Disabling the web server functionality of the device blocks access to the TelePresence system's web interface and certain support capabilities, but do 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 blocks certain support capabilities such as log file collection, but do not degrade normal operation. Default value is *Disabled*.

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 bulit-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 with MultiSite capability and 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.

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 whether the microphones are 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 how long the encryption indicator (a padlock) is shown on screen (Auto/AlwaysOn/AlwaysOff). Default value is Auto.

The setting applies to both encrypted and non-encrypted calls, i.e. both to secure and non-secure conferences.

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 overrides 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`.

Adding a new phone (endpoint) continued...

Admin username and password settings

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

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 cannot 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 for them.

For further information:

"About the phone security profile" on page 11

"Setting the system passphrase" on page 27

Far End Camera Control Settings

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) is 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.

Facility Service Settings

Facility Service Type:

Choose a facility service type (Helpdesk/Other/Concierge/Emergency/Security/Catering/Transportation). If the endpoint has a Touch controller, note that only the Helpdesk option is available. 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.

Adding a new phone (endpoint) continued...

Serial Port Settings

Serial Port:

Set the serial port mode (On/Off) to enable or disable the serial port. Default value is On.

Serial Port Login Required:

Set the login mode (On/Off) to determine if login is required when connecting to the serial port. Default value is On.

Standby Settings

Standby Mode:

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

Standby Delay:

Set the Standby Delay to define how long the system is in idle mode before going 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.

Proximity Settings

Proximity Mode:

Set the Proximity Mode field (On/Off) to determine whether the proximity app can pair with the endpoint. Default value is On for MX Series endpoints. Default value is Off for SX Series endpoints.

Call Control:

Set the Call Control field (Enabled/Disabled) to determine whether the proximity app can handle call control for the endpoint. Default value is Disabled.

Proximity Content Share From Clients:

Set the Proximity Content Share From Clients field (Enabled/Disabled) to allow the proximity app to send content as a presentation from the device to the TelePresence endpoint. Default value is Disabled.

Proximity Content Share To Clients:

Set the Proximity Content Share To Clients field (Enabled/Disabled) to allow the proximity app to receive presentation slides from the TelePresence endpoint. Default value is Disabled.

Adding a new phone (endpoint) continued...

Dial Plan settings

Only applicable when using Cisco TelePresence Manager.

The CUCM 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 Management Suite Administrator Guide for more details.

Directory Number settings

Only applicable when using Cisco TelePresence Manager.

Configure the directory number. Refer to Cisco TelePresence Manager Administration and Installation Guide for more details.

OSD settings

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).

Adding a new phone (endpoint) continued...

Add directory number

Navigate to the *Association Information* section:

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

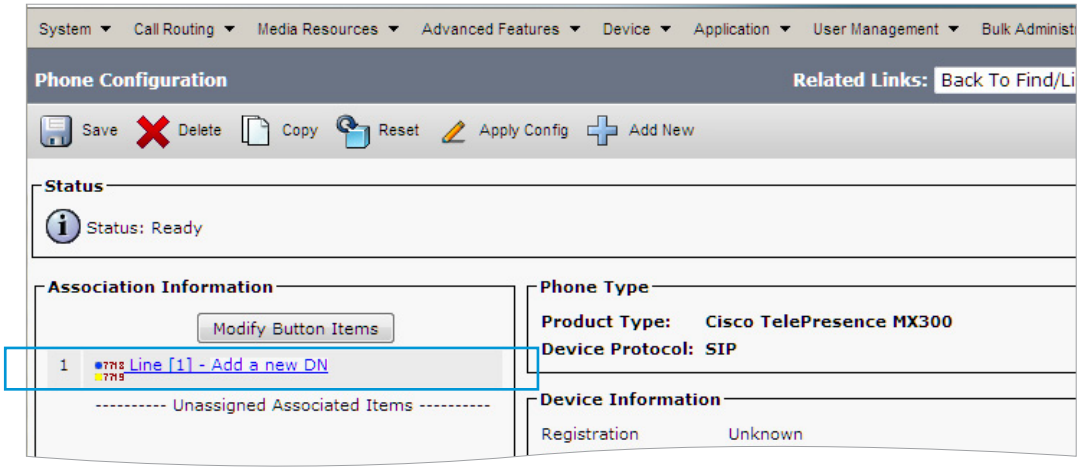
Directory number information

Navigate to the *Directory Number Information* section.

Directory Number:

Enter the number of the endpoint, according to the E.164 Numbering Plan.

Navigate to the **Association Information** section.



Adding a new phone (endpoint) continued...

Configuring shared lines

Optional: To configure the CUCM for shared lines, navigate back to "Manual registration of the endpoint" on page 13 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 caller name

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

Display (Caller ID):

Enter the TelePresence system's owner's name 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 inteded for displaying text, such as a name, instead of a directory number for calls. If you specify a number, the person receiving a call from this device may not see the callers proper identity.

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

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.

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 *System > Cisco Unified CM > Auto-registration Information*.

Starting Directory Number:

Enter the lowest number in the range of directory numbers.

Ending Directory Number:

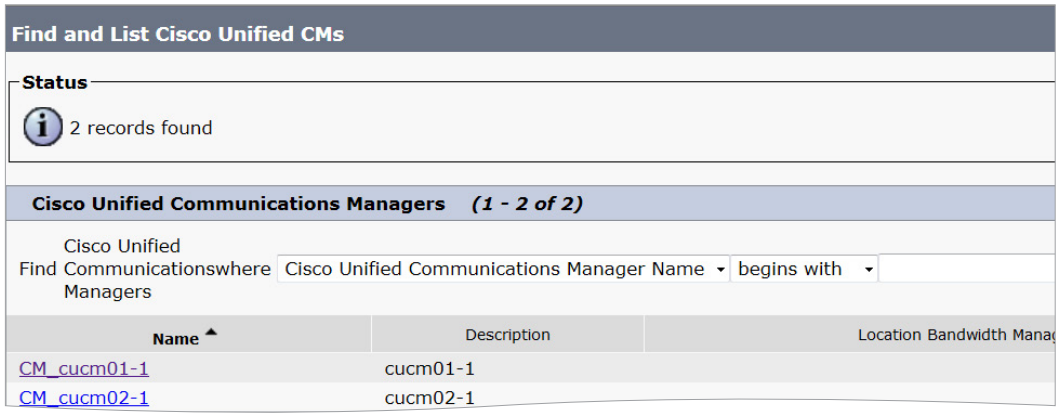
Enter the highest number in the range of directory numbers.

Auto-registration Disabled on this Cisco Unified Communications Manager:

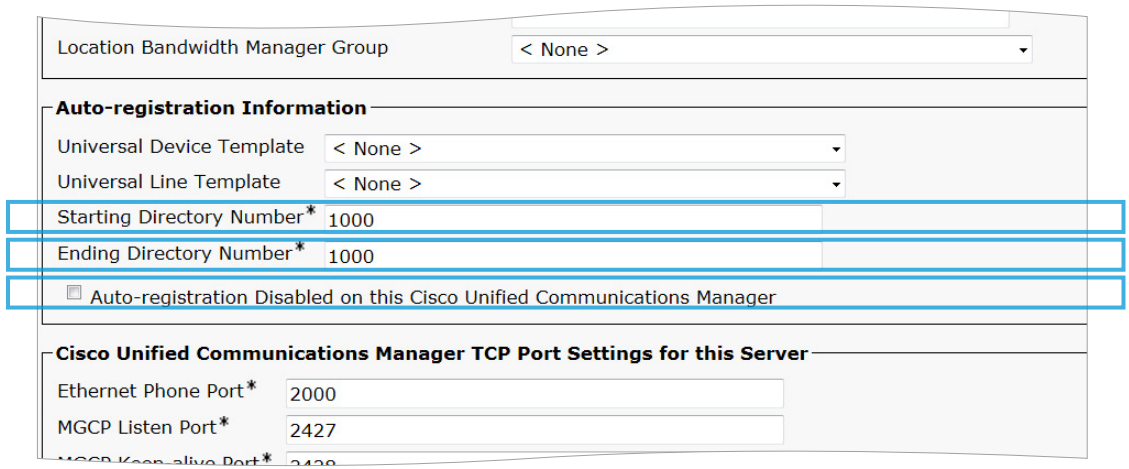
Uncheck the checkbox to enable auto-registration.

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

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



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



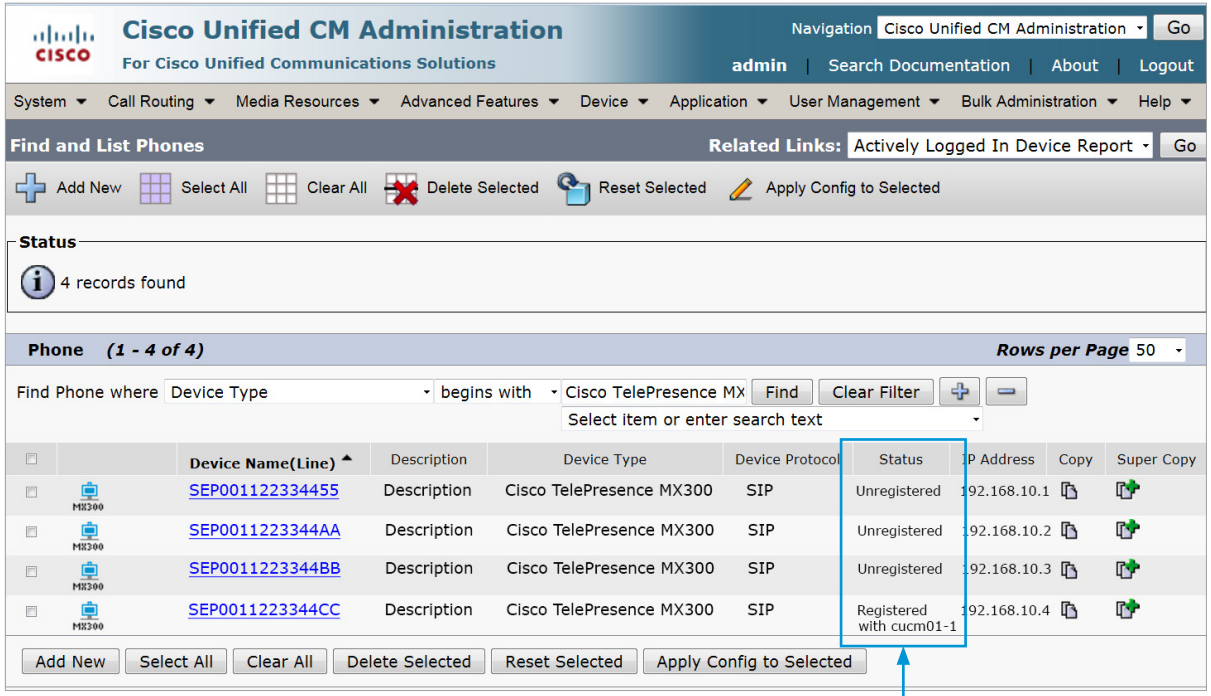
How to verify the endpoint registration

NOTE: Before you can verify the endpoint registration you must configure the TelePresence endpoint. See: "About endpoint configuration" on page 26.

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

Navigate to: *Device > Phone.*

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



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 *User Management > End User > Service Settings*.

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

Click **Save**.

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 access level.

Navigate to *User Management > End User > Permissions Information*, and choose *Add to Access Control Group*.

Select *Standard CCM End Users*.

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**.

Enterprise parameters

Clusterwide Domain Configuration

If an 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 "Use Fully Qualified Domain Name in SIP Requests:" on page 9 for further details.

Navigate to *System > Enterprice Parameter > Clusterwide Domain Configuration*.

Organization Top Level Domain:

Enter a valid domain (for example, cisco.com) to define the top level domain for the organization.

Click **Save**.

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

You can use the Touch controller, remote control, web interface, or the command line interface to configure the endpoint. We recommend using the web interface for the configuration.

NOTE: You should do the CUCM configuration before the endpoint provisioning.

When the endpoint is provisioned from CUCM, it will overrride some settings on 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 16 for how to enable/disable Web access and SSH access.

Endpoint diagnostic tools

If you are 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 passphrase

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

Go to: "Setting the system passphrase" on page 27.

Setting the default 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 28.

Setting up provisioning

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

Go to: "Setting up CUCM provisioning" on page 29, or "Setting up provisioning from CUCM via Expressway (Mobile and Remote Access)" on page 30.

You can also read about provisioning in the Getting Started Guide for the endpoint

https://www.cisco.com/go/mx-docs

https://www.cisco.com/go/sx-docs

Finding the IP address

If you are using the web interface or the command line interface, you will need the endpoint's IP address.

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

- Touch controller: Tap the gear wheel icon in the upper left corner of the Touch panel, followed by *Settings > System Information*. Then open the *System Info* section.
- Remote control: Navigate to the information icon in the upper left corner and select *System Information*.

Setting the system passphrase

The system passphrase restricts access to the TelePresence endpoint. The endpoint is delivered with a default user account (*admin*) with full credentials and no passphrase set.

The passphrase for the default *admin* user should be provisioned by CUCM or set locally on the endpoint, depending on the endpoint's security profile.

It is mandatory to set a passphrase for the *admin* user in order to restrict access to system configuration. You should also set a passphrase for any other user with similar credentials.

You have to factory reset the unit if you have forgotten the passphrase.

To learn more about passphrases see the *Administrator Guide* for your product:

https://www.cisco.com/go/mx-docs

https://www.cisco.com/go/sx-docs

Access through HTTP

HTTP (web interface) may be disabled on the endpoint configuration on CUCM. This will prevent access to the endpoint's web interface. See "Product-specific configuration layout" on page 16 to enable/disable Web access.

Endpoints with a secure (encrypted) security profile

If the TelePresence endpoint is set up with an encrypted security profile, CUCM will provision the passphrase for the endpoint's default *admin* user to the endpoint, provided that:

- A user with user name *admin* and administrator rights exists on the endpoint.
- The passphrase provisioned by CUCM is not blank.

Endpoints with a non-secure security profile

If the TelePresence endpoint is set up with a non-secure security profile, you must set the passphrase for the endpoint's default *admin* user locally on the endpoint; CUCM will not provision the passphrase.

Set or change the *admin* passphrase locally

Open a web browser, enter the endpoint's IP address, and sign in with your user name and passphrase. If a passphrase is currently not set, use a blank passphrase when signing in.

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

The new system passphrase will apply when you sign in through the web interface or the command line interface, or use the administrator settings on the Touch controller.

If used with Cisco TelePresence Manager

The system passphrase 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.

Setting the call details

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

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

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

Configure the default call settings

Open a web browser, enter the endpoint's IP address, and sign in with your user name and password. If a password is currently not set, use a blank password when logging in.

1. Navigate to *Configuration > System Configuration > Conference*.
2. Go to the *DefaultCall* section and set the *Rate* to the appropriate value.
3. In Cisco UCM mode the *Default Call Protocol* is automatically set to SIP. H.320 and H.323 are not supported.
4. Click *Save*.

Endpoint provisioning

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

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 External Manager Address field will override the setting provided by DHCP.

When the infrastructure is set to *Cisco UCM*; then CDP (Cisco Discovery Protocol) is 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.

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 were 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.

Setting up CUCM provisioning

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

Configure the provisioning[1]

Open a web browser, enter the endpoint's IP address, and log in with your user name and password. If a password is currently not set, use a blank password when logging in.

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)[2]. Click *Save*.
4. If required: Delete the certificate files (CTL/ITL). Navigate to *Configuration > Security*, open the *CUCM* tab, and click *Delete CTL/ITL*.

[1] Keep the default setting for the other Provisioning parameters.

[2] 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.

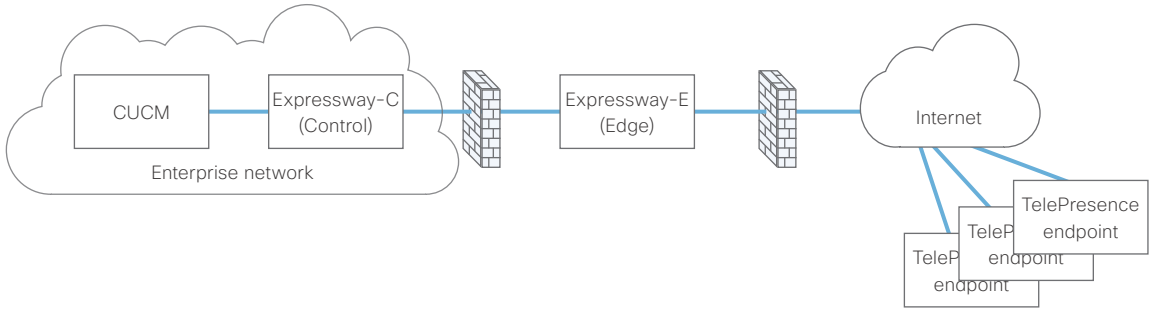
Setting up provisioning from CUCM via Expressway (Mobile and Remote Access)

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 Cisco Expressway infrastructure 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 Expressway-E'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 video system.

See *Managing the list of trusted certificate authorities and Manage pre-installed certificates for CUCM via Expressway provisioning* 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 you are in doubt of any of the provisioning parameters.

For more information about the *external manager address* and *CTL files*, refer to "Endpoint provisioning" on page 29.

Configuring the provisioning[1]

Open a web browser, enter the endpoint's IP address, and sign in with your user name and passphrase. If a passphrase is currently not set, use a blank passphrase when logging in.

1. Navigate to *Configuration > System Configuration > Provisioning*.
2. Navigate to *Mode* and set the provisioning mode to *Edge*.
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 IP address or DNS name of the External Manager (the CUCM cluster TFTP server address).[2]
7. If required: Delete the certificate files (CTL/ITL). Navigate to *Configuration > Security*, open the *CUCM* tab, and click *Delete CTL/ITL*.

[1] Keep the default setting for the other Provisioning parameters.

[2] 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.

CHAPTER 5

APPENDICES

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

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 the CUCM is described earlier in this guide. Refer to the *Multipoint Mode* setting in the "Product-specific configuration layout" on page 16.

Verifying the setup

The ad hoc conference setup can be verified by checking the System Status page in the endpoint's web interface.

1. Sign in to the web interface
2. Navigate to *Configuration > System Status > Conference* and check the *Multipoint Mode* status

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

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

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. This allows 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.

This can be useful in several scenarios:

- Help desk: You can set up a shared line so that many devices share the same number and the first available operator picks up the call.
- Call forward and barge in: Can be used for assisted call handling, for example when an administrator manages the calls for an executive.
- Single number reach: 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.

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.

For share lines configuration see "Configuring shared lines" on page 21

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is used to synchronize the system's date and time to one or more reference time servers.

If you you want to set the NTP server address(es) manually you must do this on the CUCM, and not on the codec itself. When you configure a Phone NTP Reference for the endpoint the NTP Reference must be in Unicast Mode.

If the codec receives one or more Unicast NTP servers from the CUCM, the NTP Mode will be set to *Manual* on the codec, and it will use those NTP servers.

If the codec does not receive any valid NTP servers, it will clear the NTP server list and set the NTP Mode to *Auto*, and obtain the address from the network's DHCP server (if available).

The affected settings on the endpoint (codec):

- NetworkServices NTP Mode <Auto/Manual/Off>
- NetworkServices NTP Server [1..3] Address <String>

Finding the MAC address of the endpoint

Using the web interface

To find the system's MAC (Media Access Control) 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 *System Information*. Then see the *General* section.

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 (Media Access Control) address.

The rating label is underneath the codec:

- Cisco TelePresence SX20 Quick Set
- Cisco TelePresence SX80

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

- Cisco TelePresence SX10 Quick Set

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

- 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

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 sub nets, or adding additional Ethernet ports to their switches. Leveraging the 802.1Q standard, a device such as the endpoint can tag its Ethernet frames with the VLAN ID that

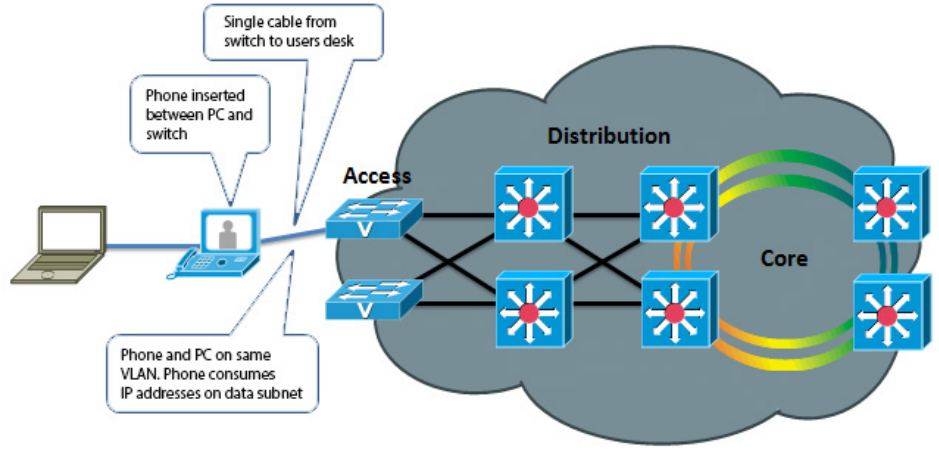


Fig. 1: Without VLANs

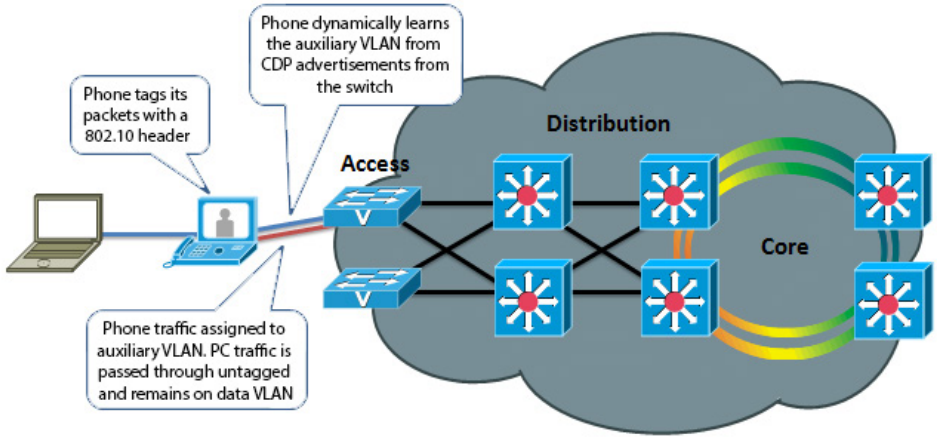


Fig. 2: With VLANs

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 accidently, 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:

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_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. This allows for more granular level of

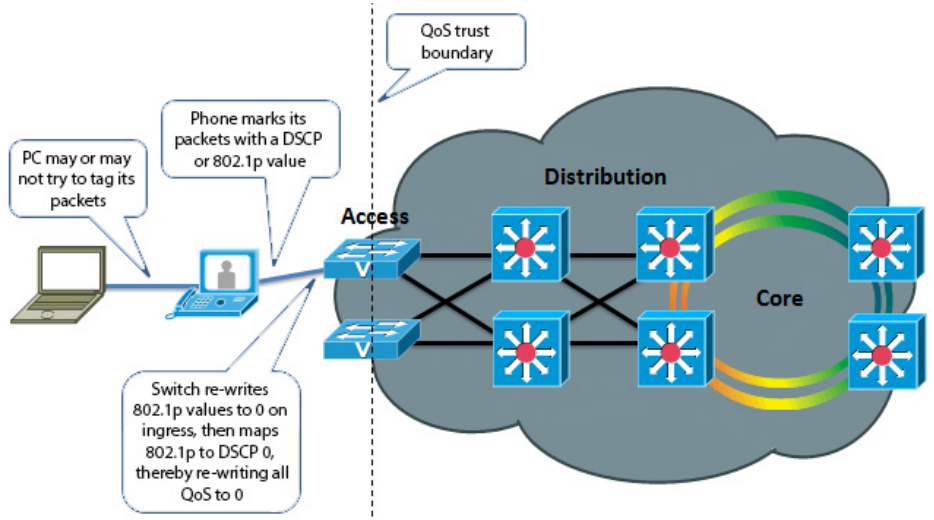


Fig. 3: Without CDP / AutoQoS

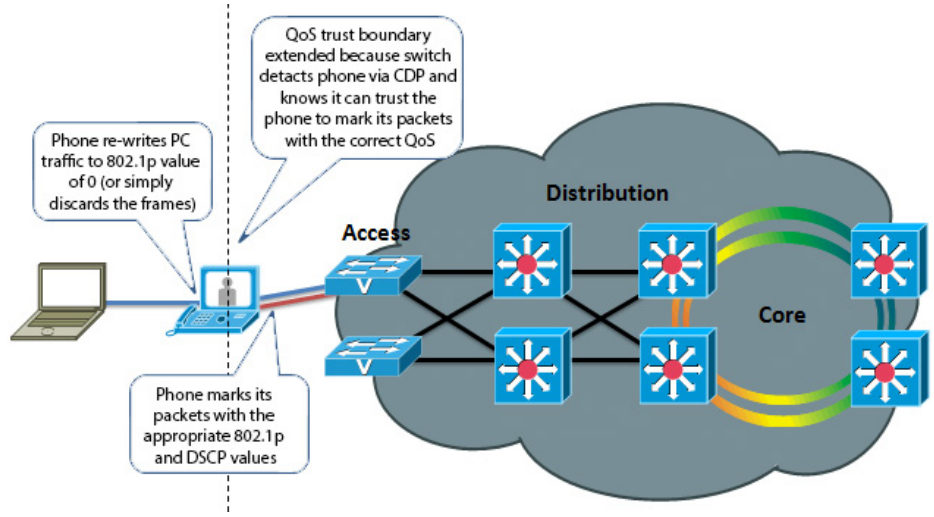


Fig. 4: With CDP / AutoQoS

negotiation between the switch and the endpoint, and allows the Ethernet switch to 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 accidently 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 accidently sets the port on his or her PC, IP phone or video terminal to a manually configured value, such as 100 Mbps / 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 Setup Assistant, 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 Setup Assistant, 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 Setup Assistant, CDP will automatically kick in and the endpoint 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

Cisco TelePresence

User documentation for the Cisco TelePresence products is available at https://www.cisco.com/go/telepresence/docs

Choose a product category in the right pane until you find the correct product. This is the path you have to follow:

Collaboration Room Endpoints >
Cisco TelePresence MX Series

TelePresence Integration Solutions >
Cisco TelePresence SX Series

Alternatively, use the following short-link to find the documentation:

https://www.cisco.com/go/mx-docs

https://www.cisco.com/go/sx-docs

Cisco Unified Communication Manager (CallManager)

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

Or click: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

The documents are organized in the following categories:

Install and Upgrade > Install and Upgrade Guides

- *Installation guides:* How to install the product
- *Getting started guide:* Initial configurations required to get the system up and running
- *RCSI guide:* Regulatory compliance and safety information

Maintain and Operate > Maintain and Operate Guides

- *Getting started guide:* Initial configurations required to get the system up and running
- *Administrator guide:* Information required to administer your product
- *Administering CE Endpoints on CUCM:* Tasks to perform to start using the product with the Cisco Unified Communications Manager (CUCM)

Maintain and Operate > End-User Guides

- *User guides:* How to use the product
- *Quick reference guides:* How to use the product
- *Physical interface guide:* Details about the product's physical interface, including the connctor panel and LEDs.

Reference Guides | Command references

- *API reference guides:* Reference guide for the Application Programmer Interface (API)

Reference Guides > Technical References

- *CAD drawings:* 2D CAD drawings with measurements

Design > Design Guides

- *Video conferencing room guidelines:* General guidelines for room design and best practice
- *Video conferencing room guidelines:* Things to do to improve the perceived audio quality

Software Downloads, Release and General Information > Licensing Information

- *Open source documentation:* Licenses and notices for open source software used in this product

Software Downloads, Release and General Information > Release Notes

- *Software release notes*

Cisco contacts

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

Go to: https://www.cisco.com/go/contacts

Corporate Headquarters

Cisco Systems, Inc.

170 West Tasman Dr.

San Jose, CA 95134 USA