Quick Reference Guide

- Cisco TelePresence MX Series
- Cisco TelePresence EX Series
- Cisco TelePresence Codec C Series
- Cisco TelePresence Profile Series
- Cisco TelePresence Quick Set C20
- Cisco TelePresence SX20 Quick Set
- Cisco Unified CM 9.0

Software versions TC6.x and Cisco Unified CM 9.0
January 2013

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 CM.

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

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 start using your Cisco TelePresence endpoints on Cisco Unified CM (CUCM).

This guide describes TC6.0 and CUCM 9.0, but most configurations will also apply to CUCM 8.6.2. Note that if you are configuring CUCM 8.6.2 you may find that some menus have changed.

Products covered by this guide

Cisco TelePresence endpoints:

- TC5.0 and later: MX200, MX300, EX90, EX60, Codec C90, Codec C60, Codec C40, Profiles w/ Codec C Series, Quick Set C20
- TC5.1 and later: SX20 Quick Set

Cisco Unified CM – CUCM9.0

Prerequisite

Users of this guide should be familiar with configuration of the Cisco Unified CM and Cisco TelePresence endpoints.

This document do not describe the basic configuration of the endpoint, such as user accounts, network configuration, date & time, etc. Refer to the user documentation:

▸ Cisco TelePresence Video Systems Getting Started Guide

This document do not describe configuration of the CUCM such as voice mail, shared lines, call forward, etc. Refer to the user documentation:

▸ Cisco Unified Communications Manager (CallManager)

Before you start

In most cases a factory reset of the endpoint is not needed before provisioning it to the Cisco Unified CM. 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 "How to factory reset the endpoint" on page 29.

About device packages

The CUCM device packages are available for download on the Cisco web site. See the Release Notes for details.

If previously used with TMS

When selecting Cisco Unified CM as the one to provisioning and providing the address book, make sure the endpoint is purged from Cisco TelePresence Management Suite (TMS).

Supported software versions

Before you start configuring, make sure the endpoints and Cisco Unified CM have the correct software installed.

Cisco Unified CM version 8.6.1.10000-43 or higher

Supported endpoints: MX200, EX Series (EX90, EX60), Quick Set C20, Codec C Series (C90, C60, C40) and Profiles using Codec C Series.

Cisco Unified CM version 8.6.2 or higher

Supported endpoints: SX20 Quick Set, MX Series (MX300, MX200), EX Series (EX90, EX60), Quick Set C20, Codec C Series (C90, C60, C40) and Profiles using Codec C Series.

Cisco Unified CM version 8.6.2.21020 or lower

If using a version lower than 8.6.2.21020, you need the Cisco Unified CM device pack from December 2011 to support MX300 and SX20.

Cisco TelePresence TC 5.0 and higher

Supported endpoints: MX Series (MX300, MX200), EX Series (EX90, EX60), Quick Set C20, Codec C Series (C90, C60, C40) and Profiles using Codec C Series.

Cisco TelePresence TC 5.1 and higher

Supported endpoints: SX20 Quick Set, MX Series (MX300, MX200), EX Series (EX90, EX60), Quick Set C20, Codec C Series (C90, C60, C40) and Profiles using Codec C Series.

To enable CTI monitoring support for CTS Manager

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

Option package for C20

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

Useful links

User documentation and software download for the TelePresence endpoints:

- http://www.cisco.com/go/telepresence/docs

User documentation and software download for Cisco Unified CM:.

- http://www.cisco.com/en/US/products/sw/voicesw/ps556/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/en/US/products/ps11422/prod_release_notes_list.html

CHAPTER 2

ENDPOINT CONFIGURATION

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

Preparations

You can use the Touch controller or the remote control to configure the system; alternatively, you can use the system's web interface or the command line interface with API commands.

All methods are described on the following pages.

Touch

Using the Touch controller

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

You must use the Touch controller, or the remote control with on-screen display, for the configurations until you know your system's IP address.

OSD

Using the remote control

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

You must use the Touch controller, or the remote control with on-screen display, for the configurations until you know your system's IP address.

Preparations (continued...)

You can use the Touch controller or the remote control to configure the system; alternatively, you can use the system's web interface or the command line interface with API commands.

All methods are described on the following pages.

Finding the IP address using the Touch controller

Tap *More > Settings ( ) > System Information* on the Touch controller. If an IPv4 or IPv6 address is assigned to the system, you will find it in the Network section.

Finding the IP address using the remote control

Use the remote control and go to *Home > Settings > System Information*. If an IPv4 or IPv6 address is assigned to the system, you will find it on the System Information page.

WEB

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*.

   The default user name is *admin* with no password set.

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.

Saving changes

Click the *ok* button, to the right of most menu items, to save and make the change take effect.

API

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. Log in with the appropriate username and password.

   The default user name is *admin* with no password set.
3. Issue the commands as described later in this guide.

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.

Setting up 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.

Contact your Cisco Unified CM (CUCM) provider if in doubt for any of the provisioning parameters.

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.

About the CTL file

Normally, you will not delete the old Certificate Trust List (CTL), but there are few cases were you will need to delete the file 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.

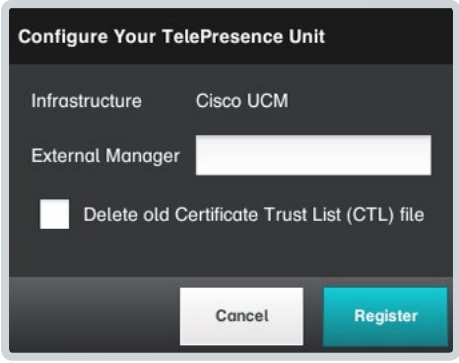
Touch

Running the Provisioning Wizard

If you are connecting the system for the first time, the Provisioning Wizard will start automatically. Otherwise, tap *More > Settings ( ) > Network Settings > Provisioning*.

Run the provisioning wizard

1. Click the *Start* button.
2. Choose *Cisco UCM* infrastructure and click *Next*.
3. *If required:* Enter the IP address or DNS name of the External Manager of the Cisco UCM cluster TFTP server in the *External Manager* input field. A soft keyboard appears when you tap the field.
4. *If required:* Check the *Delete old Certificate Trust List (CTL) file* check box. If no CTL file exist on the endpoint, this option will not be available.
5. Tap *Register* to complete the registration, or *Cancel* to abort the procedure.
6. When successfully registered a message will appear and display the URI for the endpoint.



OSD

Setting up provisioning

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

Configure the provisioning

1. Use the remote control and select *Home > Settings > Administrator Settings > Advanced Configuration > Provisioning*.
2. From the drop down list, set the *Provisioning Mode* to CUCM. The change will take effect immediately.
3. Go to the *ExternalManager* section and the IP address or DNS name of the External Manager of the Cisco UCM cluster TFTP server in the *External Manager* input field. Click *Save* to save the changes.

Setting up provisioning (continued...)

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.

WEB

Setting up provisioning

When logged on to the endpoint through the web interface, go to the *Configuration* tab and choose *Advanced Configuration*, then choose *Provisioning* from the left sidebar.

Configure the provisioning

1. Go to *Provisioning* section and set *Mode* to *CUCM*. Click *ok* to save the changes.
2. Go to the *ExternalManager* section and the IP address or DNS name of the External Manager of the Cisco UCM cluster TFTP server in the *Extermal Manager* input field. Click *ok* to save the changes.

API

Setting up provisioning

When logged on to the endpoint through the command line interface, run the following commands:

Configure the provisioning

`xConfiguration Provisioning Mode:` [must be CUCM]

`xConfiguration Provisioning ExternalManager Address:` [CUCM cluster TFTP server address]

`xConfiguration Provisioning ExternalManager Protocol:` [must be HTTP for UCM mode]

`xConfiguration Provisioning LoginName:` [leave blank, it is not needed for UCM mode]

`xConfiguration Provisioning Password:` [leave blank, it is not needed for UCM mode]

`xConfiguration Provisioning HttpMethod:` [both GET and POST work in UCM mode]

`xConfiguration Provisioning ExternalManager Path:` [leave blank, it is not needed for UCM mode]

`xConfiguration Provisioning ExternalManager Domain:` [leave blank, it is not needed for UCM mode]

Setting the call details

Some call details are configured at the endpoint.

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

The auto answer settings provisioned in Cisco Unified CM are ignored by the endpoint and must be set on the endpoint itself.

Touch

Setting the call details

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

On the Touch controller, tap *More > Settings ( ) > Administrator Settings > Call Settings*.

1. **Configure the auto answering**

   Set *Auto Answer* to On or Off, and if appropriate set the *Auto Answer Delay*. Tap the plus (+) or minus (-) buttons to increase or decrease the value.

2. **Configure the default call settings**

   Choose *Call Rate* and 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.

OSD

Setting the call details

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

1. **Configure the auto answering**

   Use the remote control and go to *Home > Settings > Administrator Settings > Advanced Configuration > Conference 1* and set to **IPv6**.

   Go to the *Auto Answer* section and set appropriate values for *Delay*, *Mode* and *Mute*.

   Click *Ok* to save the change.

2. **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.

Setting the call details *(continued...)*

Some call details are configured at the endpoint.

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

The auto answer settings provisioned in Cisco Unified CM are ignored by the endpoint and must be set on the endpoint itself.

WEB

Setting the call details

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

When logged on to the endpoint through the web interface, go to the *Configuration* tab and choose *Advanced Configuration*. Then open the *Conference 1* page from the left sidebar.

1. **Configure the auto answering**

   Go to the *Auto Answer* section and set appropriate values for *Delay*, *Mode* and *Mute*.

   Click *Ok* to save the change.

2. **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 *Ok* to save the change.

API

Setting the call details

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

When logged on to the endpoint through the command line interface, run the following commands:

1. **Configure the auto answering**

   `xConfiguration Conference 1 AutoAnswer Mode: <On/Off>` [must be set locally on the endpoint]

   `xConfiguration Conference 1 AutoAnswer Mute: <On/Off>` [must be set locally on the endpoint]

   `xConfiguration Conference 1 AutoAnswer Delay: <0..50>` [must be set locally on the endpoint]

2. **Configure the default call settings**

   `xConfiguration Conference 1 DefaultCall Rate: <64..6000>` [when used with CTMS; 2500 kbps or higher]

   `xConfiguration Conference 1 DefaultCall Protocol: SIP` [must be SIP for CUCM mode]

Setting the system password

The system password will restrict access to the codec.

The endpoint 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.

Make sure to keep a copy of the password in a safe place.

We strongly recommend that you set a password for the admin user, and to any other user with similar credentials, to restrict access to system configuration.

NOTE: The system password set on the endpoint must match the value set in the Cisco Unified CM in order for the Cisco TelePresence Manager (CTS-MAN) to discover the endpoint and provide *One Button to Push* scheduling to it. Refer to "Admin Username and Password" on page 21.

WEB

Setting the system password

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 on.

Set or change the system password

1. Click on your 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*.

API

Setting the system password

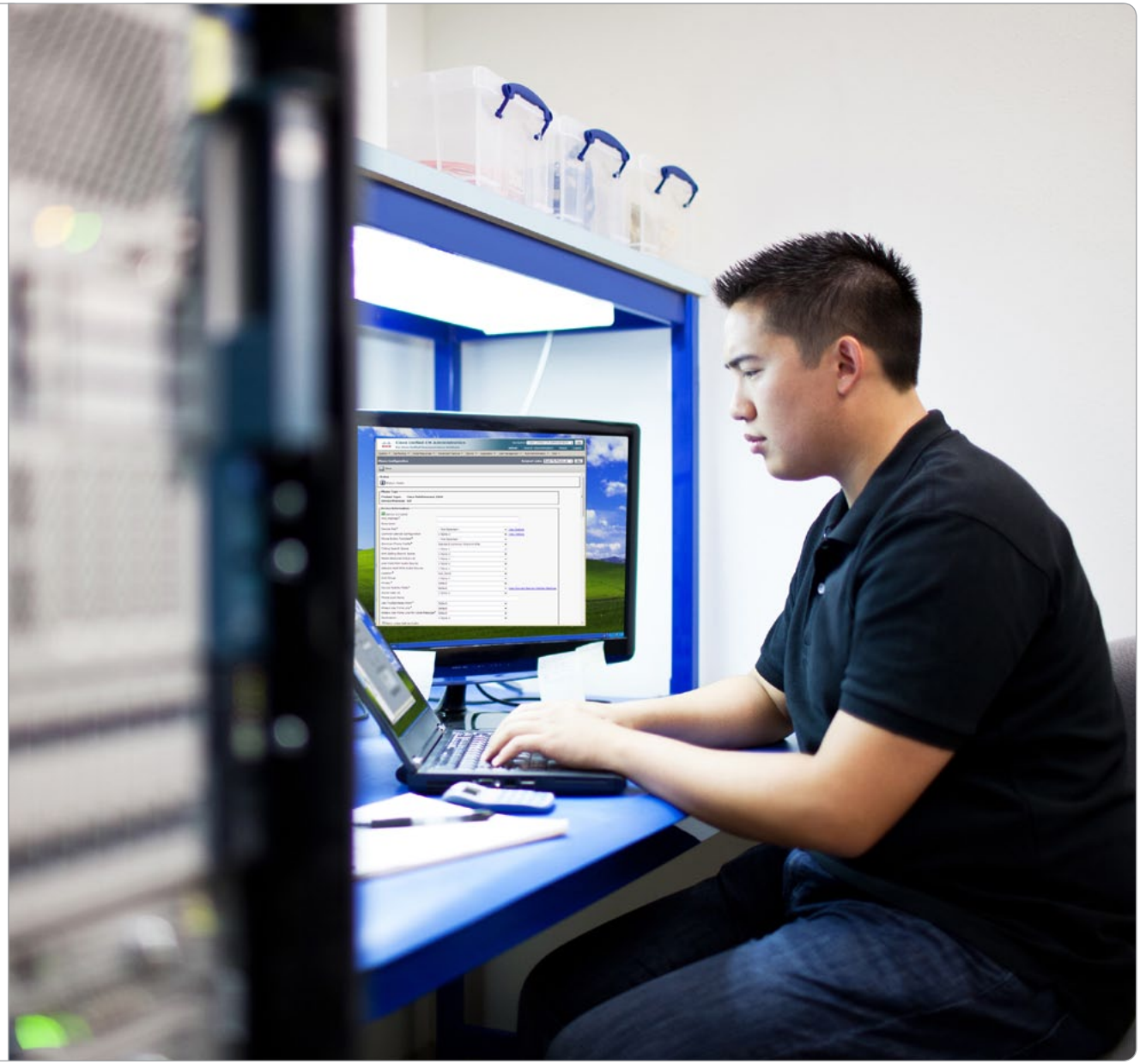
Log in to the endpoint through the command line interface with your username and current password. If a password is currently not set, use a blank password when logging on.

Set or change the system password

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

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

When the system password is set from the command line interface the codec must be restarted to make the password apply to the web interface.



CHAPTER 3

CUCM CONFIGURATION

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

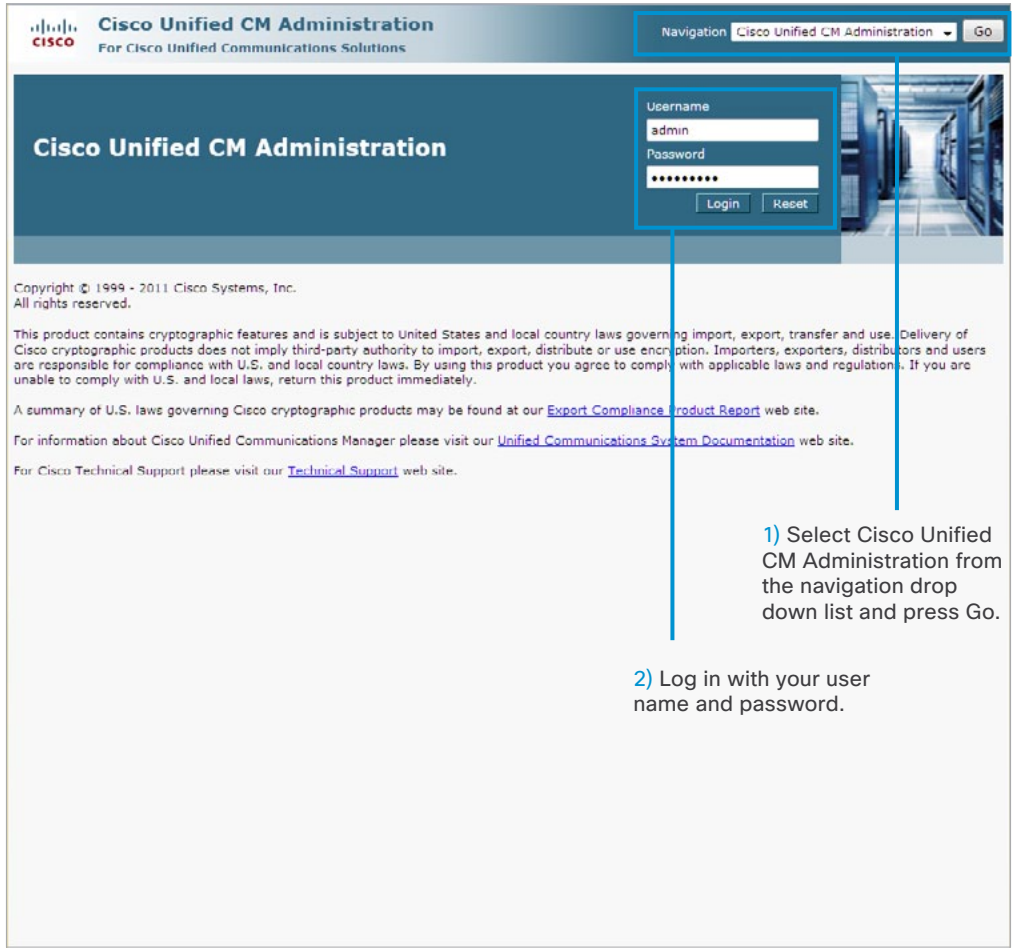
Logging in to Cisco Unified CM Administration

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. Log in with your username and password.

TIP: To bypass the first page and go directly to the *Cisco Unified CM Administration* page, you can add ccmadmin in the address bar:

- `http://your-cm-server-name/ccmadmin`, where your-cm-server-name is the host name of your CUCM.
- Or `xxx.xxx.xxx.xxx/ccmadmin`, where xxx is the IP address of your CUCM.



Creating a SIP profile

1. Navigate to *Device > Device Settings > SIP Profile*
2. Use the search options available on the page, or leave the search field blank and press *Find* to list all.
3. Locate the file you would like to copy and click the *Copy* button. This will take you to the *SIP Profile Configuration* page.

   You may give the profile a new name, or you can keep the default SIP profile name. If the latter, you will overwrite the template and use the modified profile as your default SIP profile.
4. Navigate to the *SIP Profile Information* section:

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

   Redirect by Application: Enable by checking the check box.

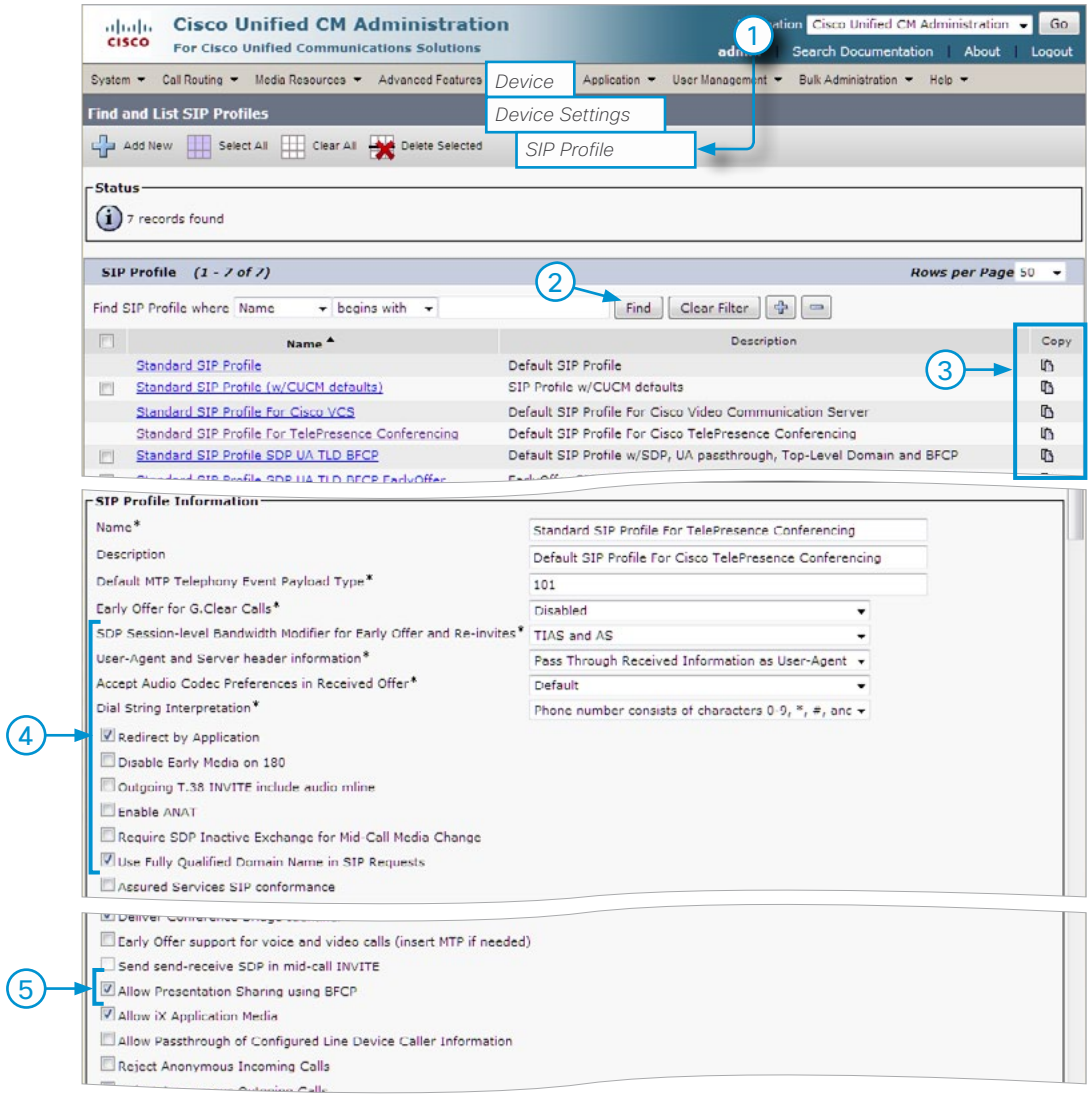
   Use Fully Qualified Domain Name in SIP Requests: Enable by checking the check box.
5. Navigate to the *Trunk Specific Configuration* section:

   Allow Presentation Sharing using BFCP: Enable by checking the check box.

Click *Apply Config*.

How to create a new SIP Profile

Log in to *Cisco Unified CM Administration* and navigate to *Device > Device Settings > SIP Profile*.



Creating a security profile

If you want to setup the CUCM for encrypted calls, follow the steps below:

CUCM must operate in mixed mode (cluster security mode) to enable secure (encrypted) communication.

You must define one device security profile for each endpoint type, and if you want to allow several authentication modes for the same endpoint type, you must define one profile for each mode.

1. Navigate to: *System > Security > Phone Security Profile*
2. Use the search options available on the page to locate the file.
3. You may *Copy* an existing profile or choose *Add New*.
4. Navigate to the *Phone Security Profile Information* section:

   Name: Enter a name of the profile.

   Description: Enter a description (optional).

   Device Security Mode: Set to Encrypted.

   Transport Type: Set to TLS.
5. Navigate to the *Phone Security Profile CAPF Information* section:

   Authentication Mode: Choose a value from the drop down list.

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

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

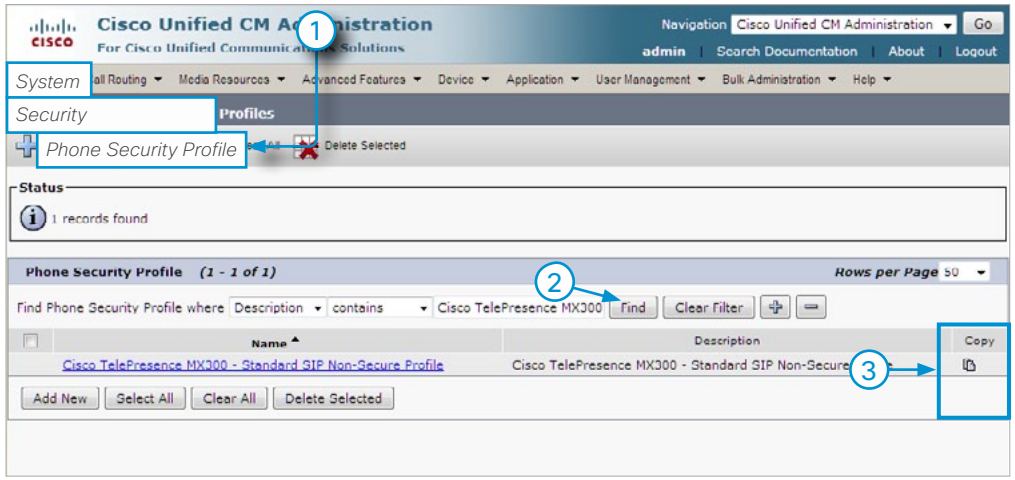
   By Existing Certificate (precedence to LSC/MIC): This option can only be used when a Locally Significant Certificate (LSC) is already stored on the endpoint, i.e. it cannot be used the first time the CAPF process runs.

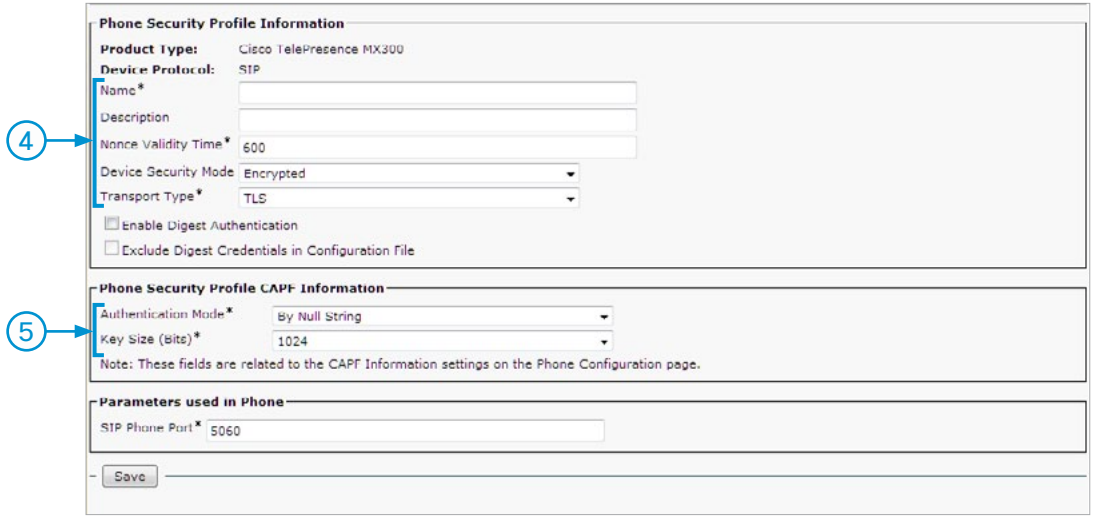
   Key-size: Choose the appropriate value from the drop down list.

Click *Save*.

How to create a security profile

Log in to *Cisco Unified CM Administration* and navigate to *System > Security > Phone Security Profile*





Manual registration of the endpoint

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

Adding a new device

1. Navigate to *Device* > *Phone*.

Add a New Phone (endpoint)

2. Click the *Add new* button and navigate to the *Create a phone using the phone type or a phone template* section:
   - From the *Phone Type* drop down list select the endpoint type.
   - Click the *Next* button.

Device Information

3. Navigate to the *Device Information* section:

   MAC Address: Enter the *MAC Address* of the endpoint.

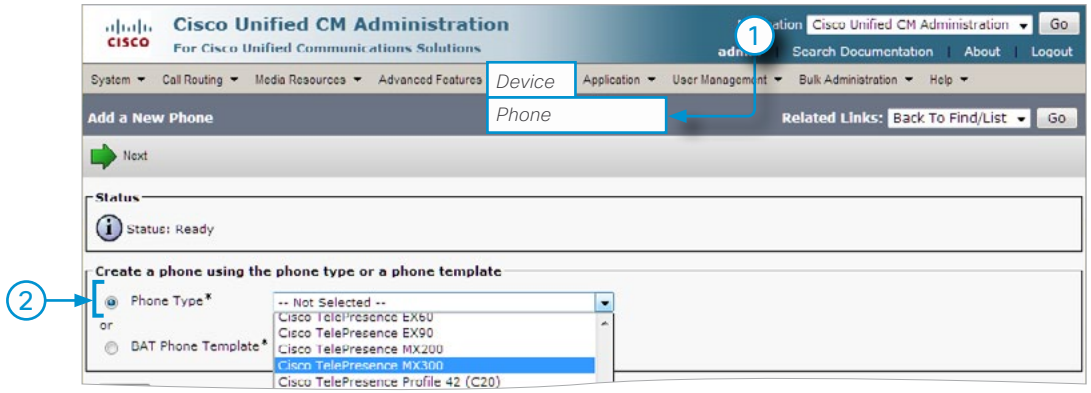
   Device Pool: Choose a Device Pool.

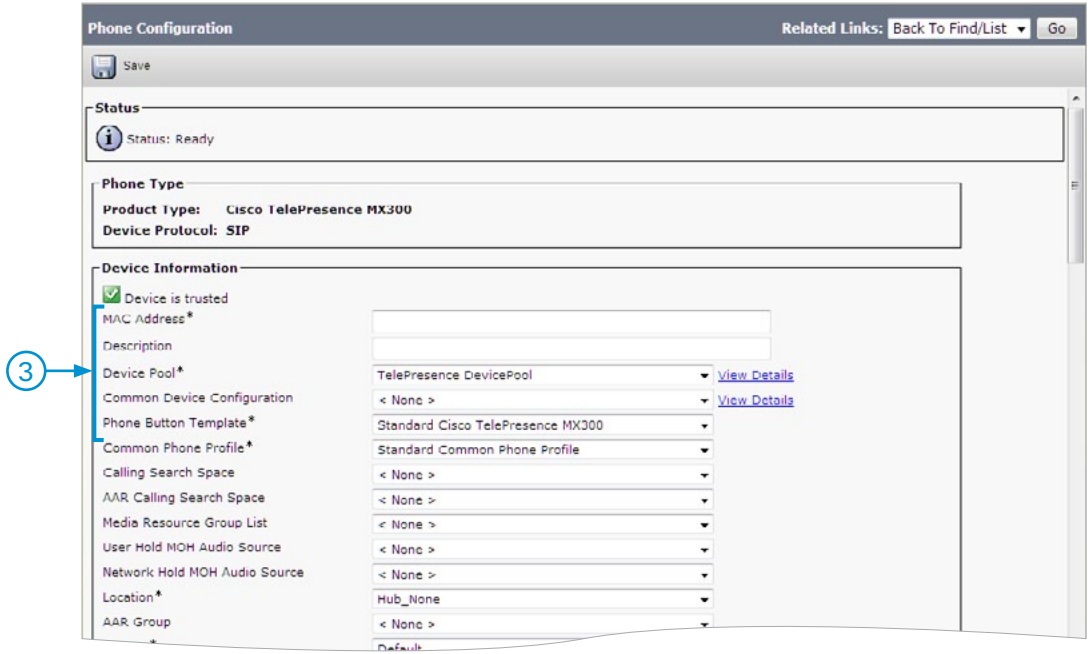
   Phone Button Template: Choose a Phone Button Template.

Click *Save*.

Adding a new device.

Log in to *Cisco Unified CM Administration* and navigate to *Device* > *Phone*.





Manual registration of the endpoint
(continued...)

Adding a new device *(continued...)*

Protocol Specific Information

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

   Device Security Profile: Choose the Device Security Profile you previously defined.

   SIP Profile: Choose the SIP Profile you previously defined.

Certification Authority Proxy Function (CAPF) Information

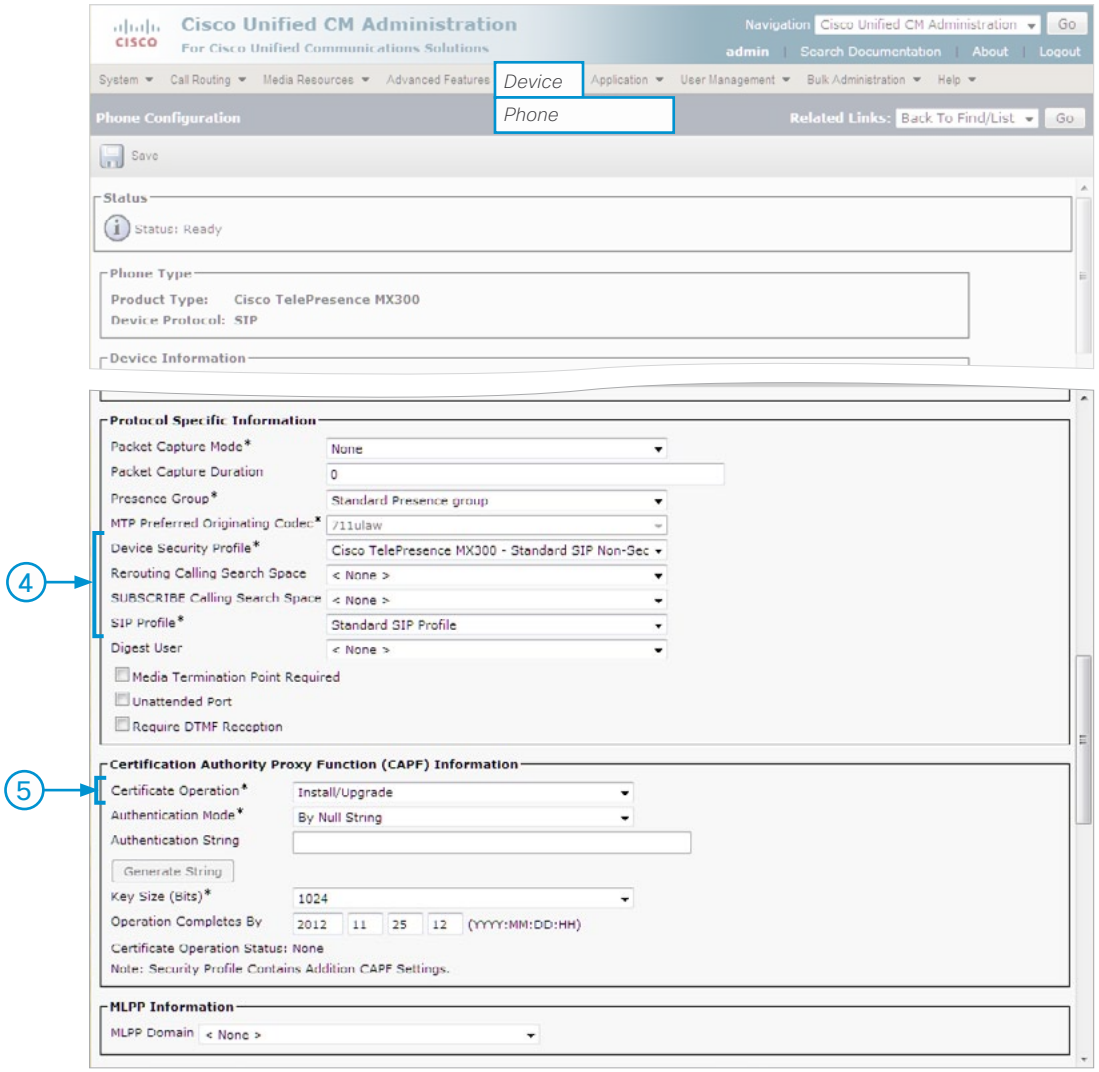
5. Navigate to the *Certification Authority Proxy Function (CAPF) Information* section:

   Certificate Operation: Set to *Install/Upgrade*.

Click *Save*.

Adding a new device.

Log in to Cisco *Unified CM Administration* and navigate to *Device* > *Phone*.



Manual registration of the endpoint
(continued...)

Adding a new device *(continued...)*

Product Specific Configuration Layout

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

6. Navigate to the *Product Specific Configuration Layout* section and configure the items according to your preferred settings.

   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. Maximum length: 64.

   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 phone's internal web pages and certain support capabilities, but will not degrade normal operation. Default: 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: Disabled.

   Default Call Protocol: This parameter sets the default call protocol of the device. This device only supports SIP when registering to Cisco Unified CM. Default: SIP.

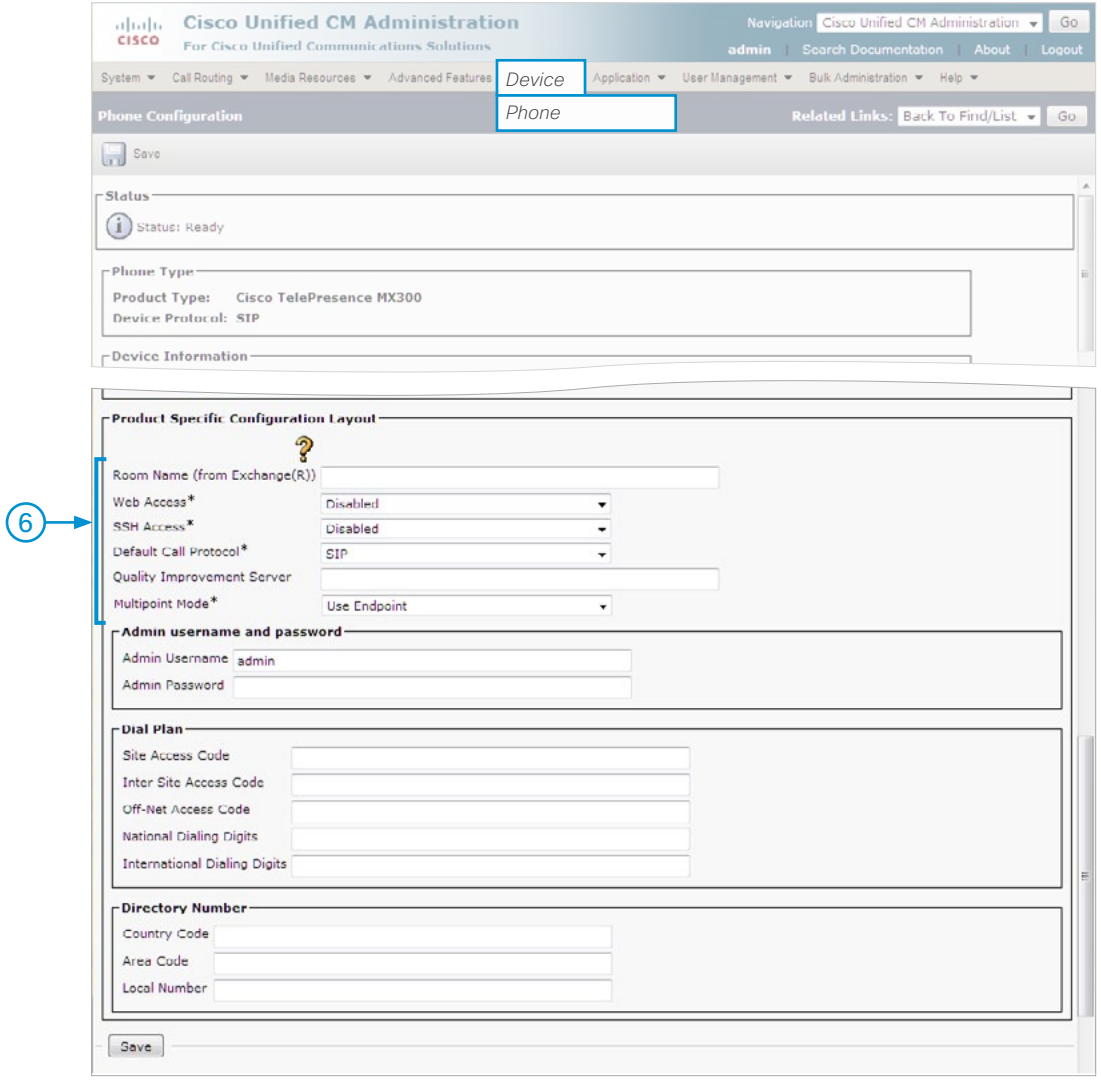
   Quality Improvement Server: Specifies a host name or IP address of a remote system to collect quality improvement reports from the device. Default: "" and Maximum length: 256.

   Multipoint Mode: Choose *Use Endpoint* to use the *built-in MultiSite* feature or choose *Use Media Resource Group List* to use the Conference Bridge feature on Cisco Unified CM. NOTE: Applies to endpoints having MultiSite capability and having the option installed.

Click *Save* and *Apply Config*.

How to configure the product specific configuration layouts for the endpoint.

Log in to *Cisco Unified CM Administration* and navigate to *Device* > *Phone*.



Manual registration of the endpoint
(continued...)

Adding a new device *(continued...)*

Admin Username and Password

7. Navigate to the *Product Specific Configuration Layout > Admin username and password* section, and configure the items accordingly to your preferred settings.

   Admin username and password: Configure the username and password, which must match the values set on the endpoint.

   Admin Username: Enter the username for the admin user.

   Default: admin

   Maximum length: 64

   Allowed values: Admin username cannot be one of the following: apache, daemon, nobody, root, shutdown. It must be between 1 and 64 characters long.

   Admin Password: Enter the password for the admin user.

   Default: “”

   Maximum length: 64

   Allowed values: Admin password can only contain printable characters from the ASCII character set, except a white space.

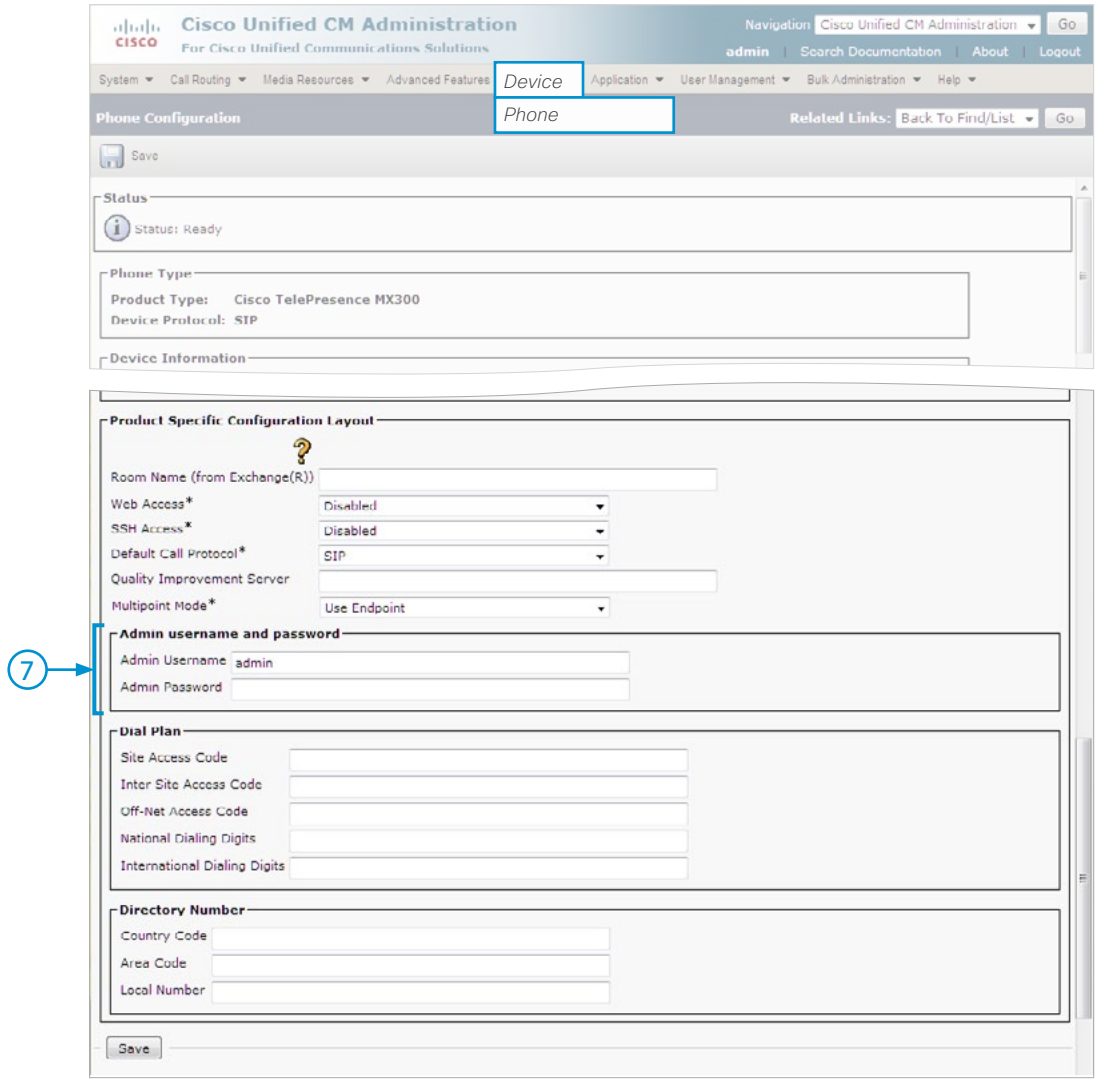
Click *Save* and *Apply Config*.

NOTE: The admin username and password will not be pushed to the endpoint, it must be set on both sides. 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.

- Refer to "Setting the system password" on page 13.
- The Cisco Unified CM user documentation: ▸http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

How to set the username and password for the endpoint.

Log in to Cisco *Unified CM Administration* and navigate to *Device > Phone*.



Manual registration of the endpoint
(continued...)

Adding a new device *(continued...)*

Dial Plan

Navigate to the *Product Specific Configuration Layout* > *Dial Plan* section, and configure the items accordingly to your preferred settings.

8. Configure the dial plan.

   Refer to Cisco TelePresence Manager documentation for more details.

Directory Number

Navigate to the *Product Specific Configuration Layout* > *Directory Number* section, and configure the items accordingly to your preferred settings.

9. Configure the directory number.

   Refer to Cisco TelePresence Manager documentation for more details.

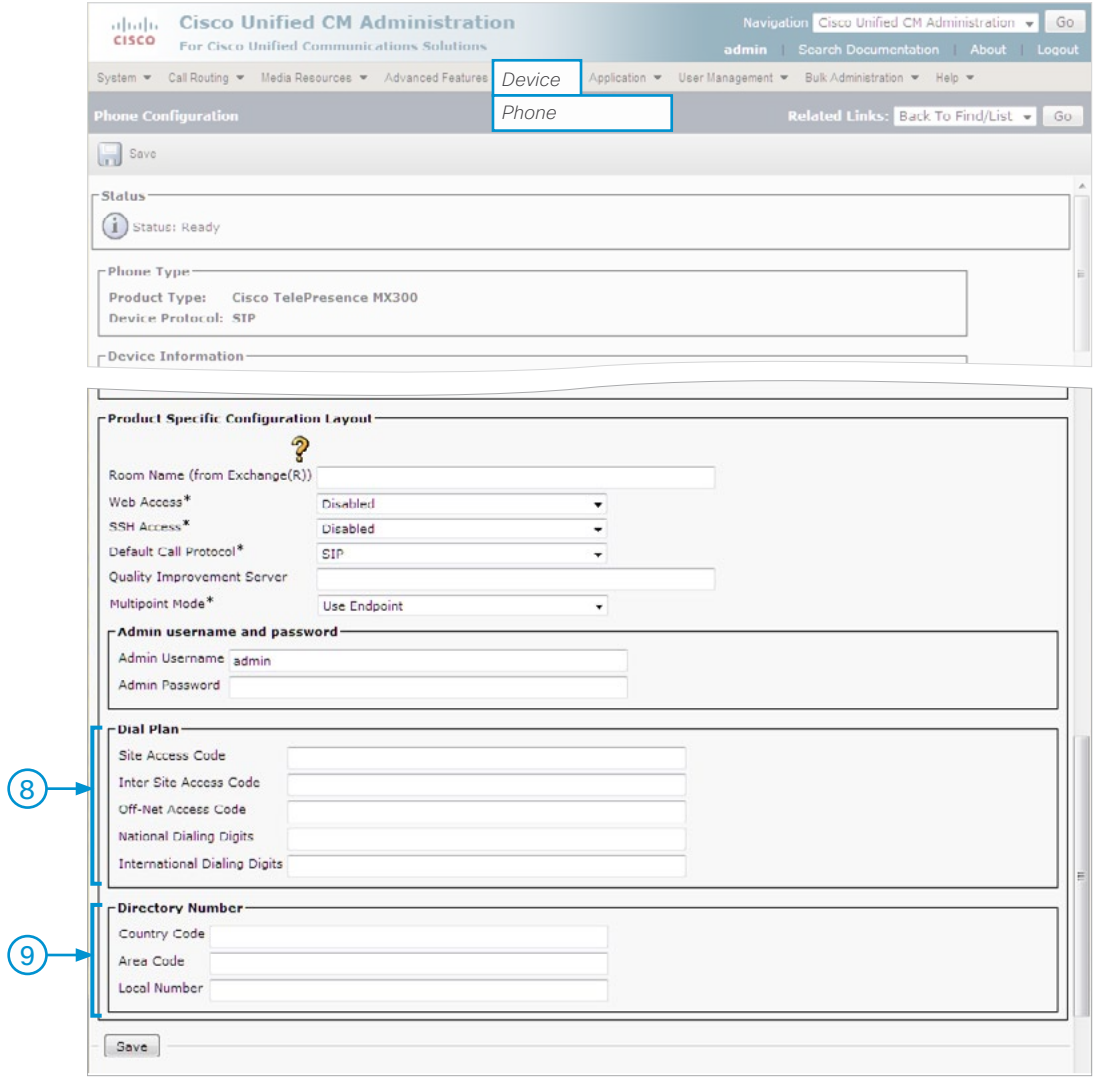
When done, click *Save* **and** *Apply Config***.**

Cisco TelePresence Manager documentation

The Cisco TelePresence Manager documentation is found on the Cisco web site. Go to: ▸ http://www.cisco.com/en/US/products/ps7074/tsd_products_support_series_home.html

How to configure the dial plan and directory number for the endpoint.

Log in to Cisco *Unified CM Administration* and navigate to *Device* > *Phone*.



Manual registration of the endpoint
(continued...)

Configuring the line number

1. Navigate to *Device* > *Phone*.

Search to find the previously defined endpoint

2. Use the search options to list the available TelePresence devices.
3. From the list, choose the endpoint you previously defined.

Association Information

4. Navigate to the *Association Information* section and click the *Line[1] - Add a new DN* to define the Line number.

Directory Number Information

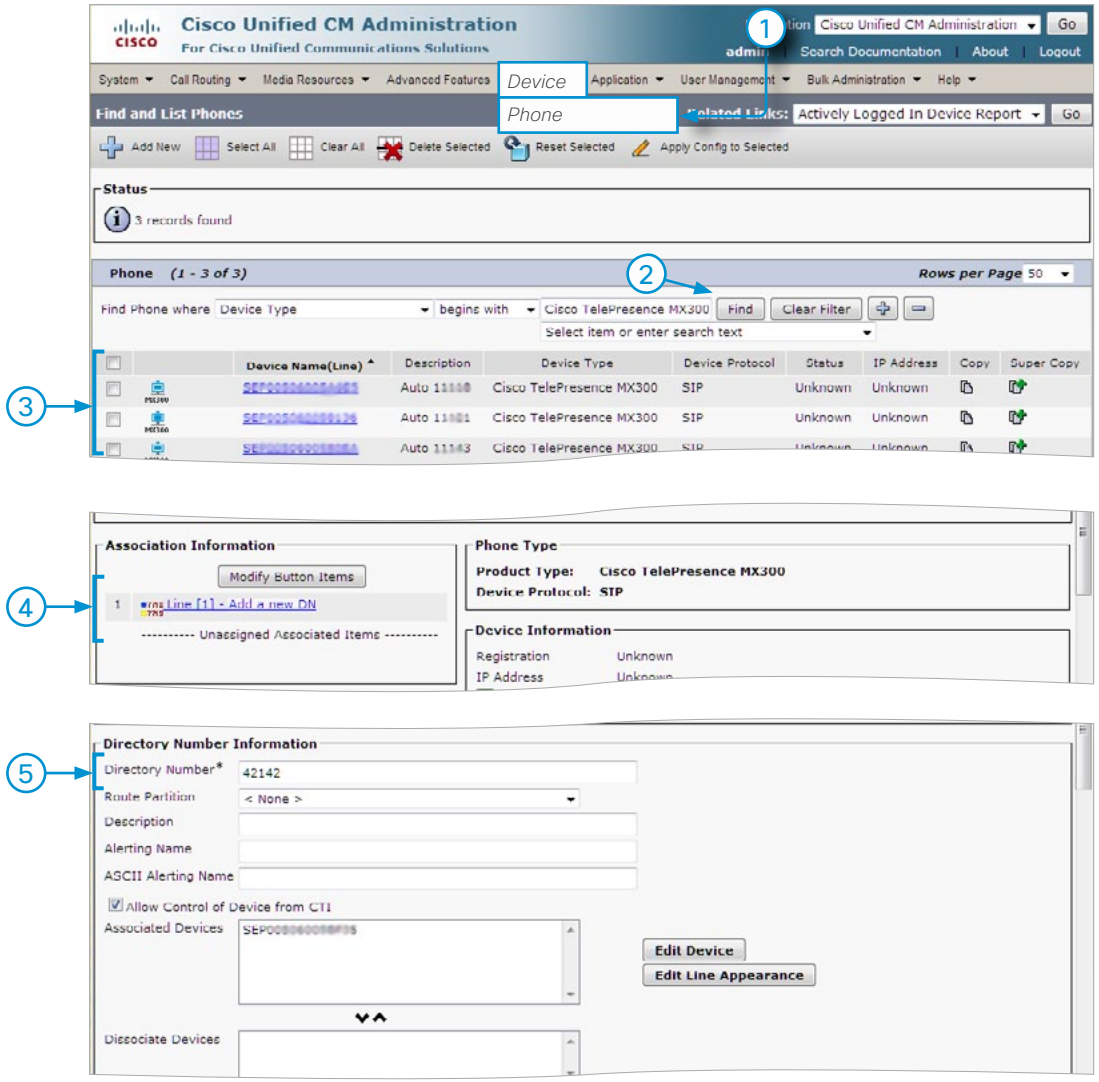
5. Navigate to the *Directory Number Information* section.

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

Click *Save* and *Apply Config*.

How to configure the line number.

Log in to Cisco *Unified CM Administration* and navigate to *Device* > *Phone*.



Auto-registration of the endpoint

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 Cisco Unified CM is set to mixed mode (cluster security mode).

Enable auto-registration

1. Navigate to *System* > *Cisco Unified CM*.

Search to find the Cisco Unified Communication Manager

2. Use the search options available on the page, or leave the search field blank and press *Find* to list all.
3. Select your Cisco Unified CM from the list.

Auto-registration Information

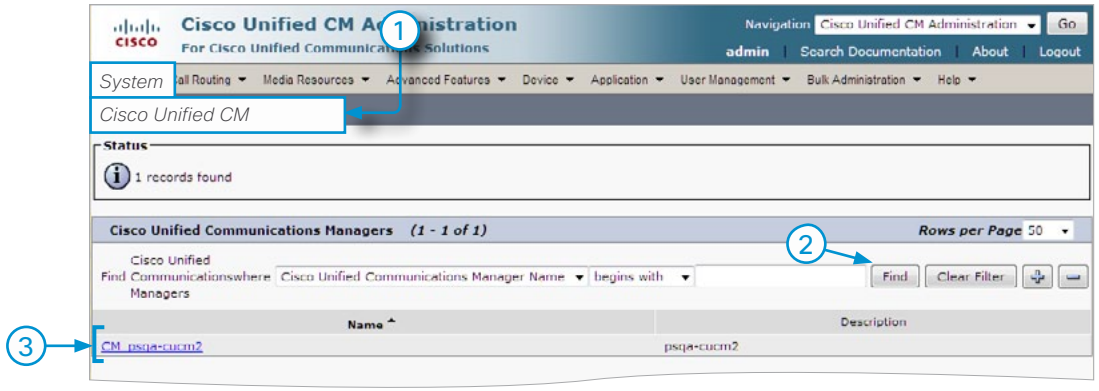
4. Navigate to the *Auto-registration Information* section.

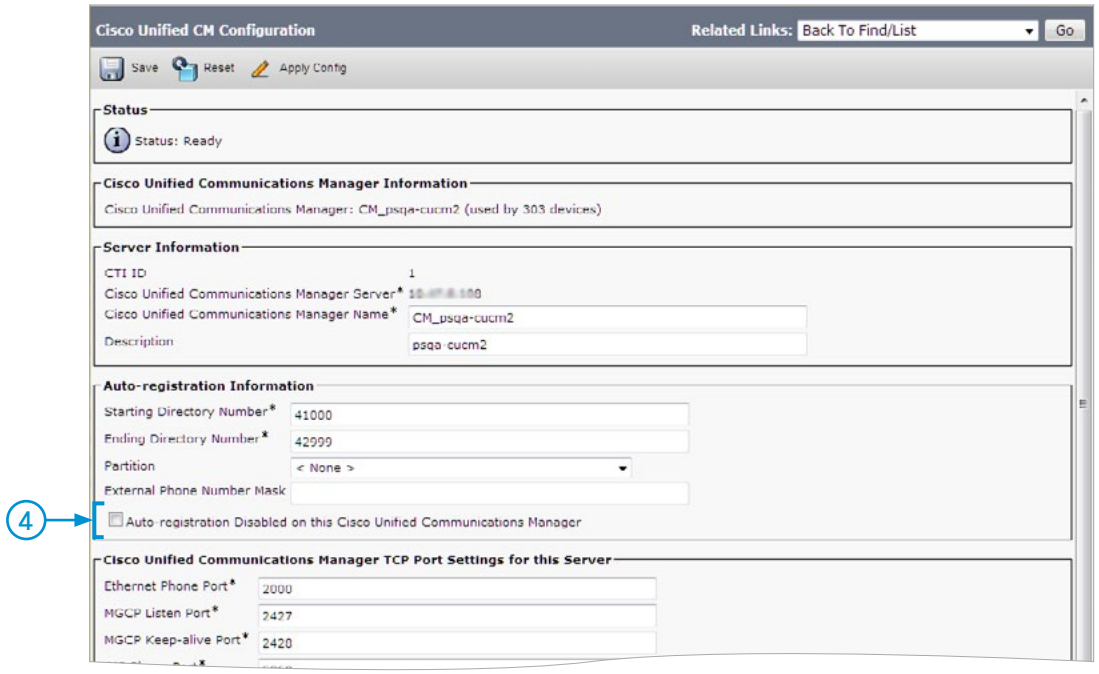
   Auto-registration Disabled on this Cisco Unified Communications Manager: Uncheck the check box to enable auto-registration.

Click *Save* and *Apply Config*.

Enable auto-registration of the TelePresence endpoint.

Log in to *Cisco Unified CM Administration* and navigate to *System* > *Cisco Unified CM*.





CHAPTER 4

SETTING PASSWORDS

This section explains about passwords on the TelePresence endpoints.

Setting the system password on the endpoint

The system password will restrict access to the codec.

You need to sign in to be able to use the web interface of your system.

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.

Make sure to keep a copy of the password in a safe place. You have to contact your Cisco representative if you have forgotten the password.

We strongly recommend that you set a password for the admin user, and to any other user with similar credentials, to restrict access to system configuration.

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 username and current password.
2. Click your username 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 username and password.
2. Go to the *Maintenance* tab and choose *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 on the endpoint

The menu password will restrict access to some menus.

When starting up the video conference system for the first time anyone can access the Administrator menu on the Touch controller because the menu password is not set.

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

You have to issue a command from the command line interface to set the menu password on the Touch; neither the Touch controller nor the web interface can be used.

Setting the menu password

1. Connect to the system through the network or its serial data port (if available) and open a command line interface (SSH or Telnet).

   See below how to find the system's IP address.

2. Sign in to the system with username and password. The user needs ADMIN rights.

3. Type the following command:

   ```
   xCommand SystemUnit MenuPassword Set
   Password: <password>
   ```

   The password format is a string with 0–255 characters.

To find the system's IP address tap *Settings ( ) > System Information* on the Touch controller.

CHAPTER 5

APPENDICES

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

How to factory reset the endpoint

You can reset the endpoint to its factory defaults by:

- The Touch controller, if you have one.
- The web interface, which available for all endpoints.
- The command line interface by issuing an API command.
- The power button (SX20/EX60/EX90).

It is not possible to undo a factory reset.

When factory resetting the endpoint the following happens:

- The call logs will be deleted.
- All system parameters will be reset to default values.
- All files that have been uploaded to the system will be deleted.
- The Release and Option keys will be preserved.
- Automatic restart of the system.

Notification on the main screen

The system will confirm the factory reset by displaying a notification on the main screen when up and running again. The notification disappears after approximately 10 seconds.

Basic configuration after the factory reset

This document do not describe the basic configuration of the endpoint, such as user roles, network configuration, date & time, or location settings, etc. You can read about these topics in the ▸ Cisco TelePresence Video Systems Getting Started Guide.

Touch

1. Tap gently on the Touch screen if the unit is in sleep mode.
2. Navigate to *Settings ( ) > Administrator > Reset.*
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.

WEB

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

Tap *Settings ( ) > System Information* on the Touch controller to find the system's IP address (IPv4 or IPv6).

API

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. Log 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.

Power button

Applies to SX20/EX60/EX90

1. Power down the system by pressing gently and hold the power button until the system shuts down. The power LED turns off.
2. Press gently and hold the power button for 10 seconds. During this period the power LED will remain off.
3. Release the button and within four seconds, press twice. During this period the power LED will blink.
4. The system will revert to the default factory settings and automatically restart. When up and running again the LED lights continuously.

If you failed to press the power button twice within the four seconds, the system will not revert to the default factory settings, and you will not see the confirmation message. If this happens, go back to Step 1.

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; on the Cisco TelePresence MX series, EX series, Codec C Series, Profile series and Quick Set C20 in release TC5.0. The Cisco TelePresence SX20 Quick Set is supported from release TC5.1. The Cisco TelePresence EX Series is supported in TE6.0.

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 series, EX series, Codec C Series, Profile series, Quick Set C20 and SX20 Quick Set.

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 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.

Figures 1 and 2 illustrate 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.

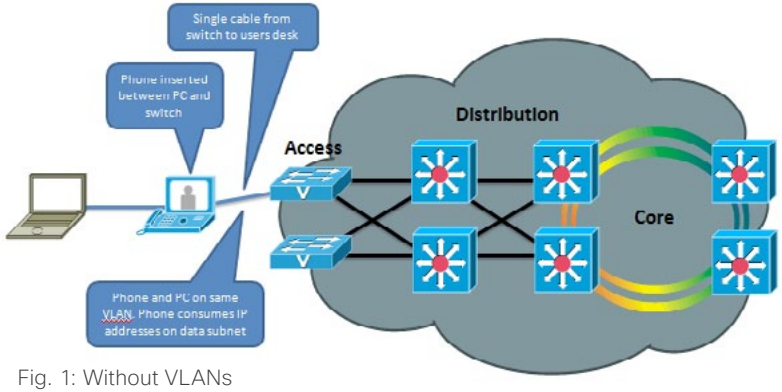


Fig. 1: Without VLANs

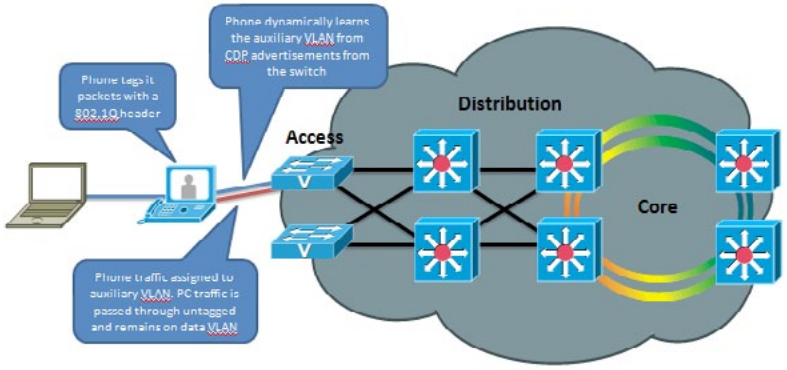


Fig. 2: With VLANs

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.

Fig. 3: Without CDP / AutoQoS

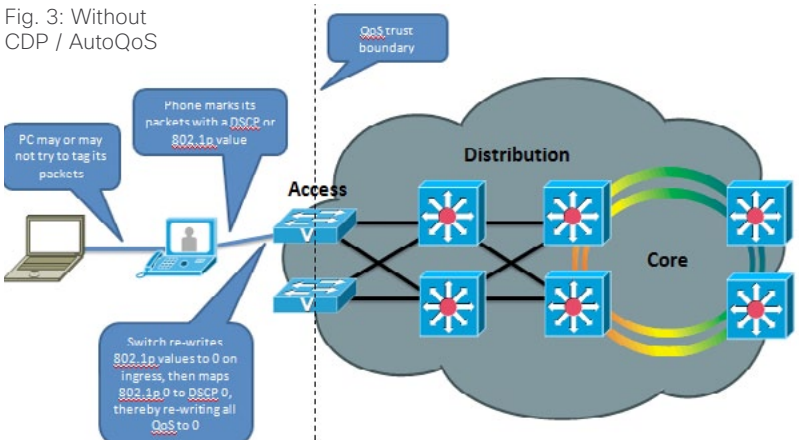
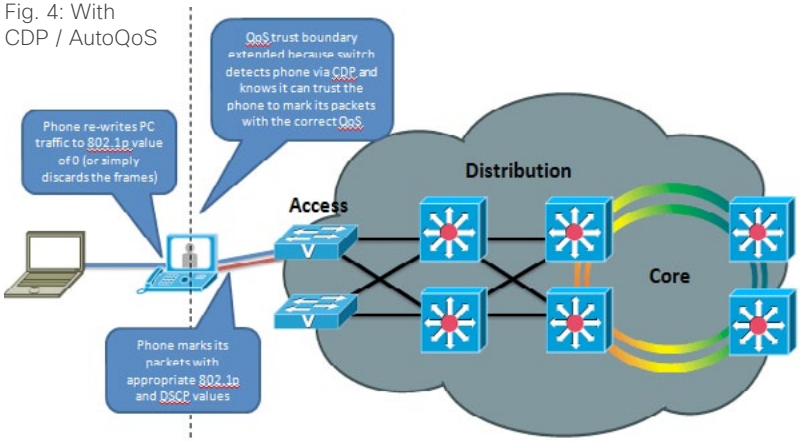


Fig. 4: With CDP / AutoQoS



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.

Figures 3 and 4 illustrate the concept of AutoQoS.

Further information about AutoQoS can be found at the following reference:

- Medianet Campus QoS Design guide: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1098057

Power over Ethernet (PoE) negotiation

The 802.3af standard provides for 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 more closely track its available power budget. Note that PoE is currently not used by the Cisco TelePresence endpoints, but is mentioned here as informational benefit to the reader since 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.

Further information about Medianet, CDP and LLDP-MED can be found at the following references:

- Medianet Campus QoS Design 4.0
  http://www.cisco.com/en/US/netsol/ns1094/index.html
- Using Cisco Discovery Protocol (CDP)
  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover_ps6350_TSD_Products_Configuration_Guide_Chapter.html
- Best Practices for Catalyst 4500/4000, 5500/5000, and 6500/6000 Series Switches Running CatOS Configuration and Management
  http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml#cdp
- LLDP-MED and Cisco Discovery Protocol White Paper
  http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html

CDP behavior in release TC5, and later

The following information applies to Cisco TelePresence MX series, EX series, Codec C Series, Profile series and Quick Set C20 running software release TC5.0, and later; and Cisco TelePresence SX20 Quick Set which is supported from release TC5.1, and later; and EX Series supported in TE6.0.

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

```
xConfiguration Provisioning Mode: Auto

xConfiguration Network 1 VLAN Voice Mode: Off
```

The endpoint then displays the Provisioning Wizard screen to prompt the user for what provisioning mode they would like to use: VCS, Callway or CUCM.

If CUCM is selected, then xConfiguration Provisioning Mode is automatically set to CUCM and xConfiguration Network 1 VLAN Voice Mode is automatically changed to Auto. Also the endpoint begins utilizing CDP to automatically discover its VLAN and begins tagging its packets with the appropriate VLAN ID. The endpoint also begins including DHCP Option 150 in its DHCP requests so that it can automatically discover the address of the Cisco Unified CM TFTP server.

If the xConfiguration Provisioning Mode is set to VCS or Callway, then xConfiguration Network 1 VLAN Voice Mode is left in its default state of Off, and the endpoint will ignore any CDP VLAN advertisements and not tag its packets with any VLAN ID. The endpoint also does not include DHCP Option 150 in its DHCP requests.

For TMS/VCS customers, this behavior preserves the functionality they had in previous software releases of these endpoints. If CDP is desired, then it may be manually enabled by setting the xConfiguration Network 1 VLAN Voice Mode parameter to Auto.

This may be done through:

- Touch user interface: *Administrator Settings -> Network Settings -> Link Settings.*
- Or the On-Screen Display Menu: *Settings -> Administrator Settings -> Advanced Configuration -> Network 1 -> VLAN Voice Mode.*
- Or the web interface: *Configuration -> Advanced Configuration -> Network 1 -> VLAN Voice Mode.*
- Or the API command: `xConfiguration Network 1 VLAN Voice Mode.`

For CUCM customers, this behavior does present an extra step in the first-time boot up process, but once CUCM mode has been chosen in the Startup 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 xConfiguration Network 1 VLAN Voice Mode parameter to Off.

For customers who do not have a CDP-capable Ethernet switch, but wish to use 802.1Q VLANs, the xConfiguration Network 1 VLAN Voice Mode parameter may be set to Manual, and the associated xConfiguration Network 1 VLAN Voice ID parameter may be set to the appropriate value.

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

Upgrades to TC5/TE6 from a previous release

For existing customers upgrading to release TC5.x from a previous release, the existing values for these parameters will be maintained, the Startup Wizard is not displayed, and no change in behavior will be seen by the user. Note however that the values for the xConfiguration Network 1 VLAN Voice Mode parameter have changed. In previous releases, the valid values for this parameter were Untagged or Tagged, with Untagged being the default. From release TC5.0, with the introduction of CDP support, the valid values for those parameters are now [Auto/Manual/Off]. During an upgrade, the previous values are automatically mapped to the new equivalent values.

NOTE: Management applications will need to be updated to use the new values (e.g. Off instead of Untagged, Manual instead of Tagged, or Auto) in xConfiguration API requests.

Table 1 illustrates the relationship between the old and new values.

NOTE: The DHCP process is actually done in the background prior to the Startup Wizard being displayed. This means that during the first-time boot up, or after a factory reset, the endpoint will initially obtain a DHCP lease in the native VLAN. If VLAN Voice Mode Auto is then chosen, and CDP indicates that a VLAN should be used, the endpoint will release the address it received in the native VLAN, restart its IP stack, and re-DHCP a new address in the auxiliary VLAN. This may result in temporary usage of IP addresses in the native VLAN during the first-time boot up.

Summary

This document has briefly introduced the history and benefits of the Cisco Discovery Protocol (CDP) and its behavior on the Cisco TelePresence MX series, EX series, Codec C Series, Profile series and Quick Set C20 running software release TC5.0 or later; and Cisco TelePresence SX20 Quick Set which is supported from release TC5.1; and the EX Series supported in TE6.0.

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 endpoints.

Prior Releases	*Release TC5.x/TE6.0*	*Comments*
	Auto	Auto mode was introduced in release TC5.0
Tagged	Manual	Manual is the same as Tagged in prior releases
Untagged	Off	Off is the same as Untagged in prior release

Table 1: Old and New VLAN Tagging Values

User documentation on the Cisco web site

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

EX Series:

TelePresence
> TelePresence Endpoints - Personal
> TelePresence Desktop
> Cisco TelePresence System EX Series

Or click: www.cisco.com/go/ex-docs

Codec C Series:

TelePresence
> TelePresence Solutions Platform
> TelePresence Integrator Products
> Cisco TelePresence System Integrator C Series

Or click: www.cisco.com/go/cseries-docs

Quick Set C20 and SX20 Quick Set:

TelePresence
> TelePresence Solutions Platform
> TelePresence Integrator Products
> Cisco TelePresence Quick Set Series

Or click: www.cisco.com/go/quickset-docs

MX Series:

TelePresence
> TelePresence Endpoints - Multipurpose
> Cisco TelePresence MX Series

Or click: www.cisco.com/go/mx-docs

Profile Series:

TelePresence
> TelePresence Endpoints - Multipurpose
> Cisco TelePresence System Profile Series

Or click: www.cisco.com/go/profile-docs

Cisco Unified Communication Manager (CallManager):

Voice and Unified Communications
> IP Telephony
> Unified Communications Platform
> Cisco Unified Communications Manager (CallManager)

Or click: http://www.cisco.com/en/US/products/sw/voicesw/ps556/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

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

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