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 Communications Manager

Software versions TC7.0 and Cisco Unified CM 9.1.2
AUGUST 2014

Thank you for choosing Cisco TelePresence!

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

This part of the product documentation is aimed at administrators working with the setup of the TelePresence endpoints on Cisco Unified 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 register a Cisco TelePresence endpoint (C, EX, MX, SX, and Profile Series) on Cisco Unified CM (CUCM).

The software versions referred to in this document are the TelePresence endpoints TC7.0 and CUCM 9.1.2. Cisco recommends using the latest software versions to support all features and functions described in this guide.

Most configurations will also apply to CUCM 8.6.2, but some menus may have changed in newer versions of the CUCM. Make sure you have the latest device package.

Prerequisites

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

Recommended sequence when configuring

Note that we recommend doing the CUCM configuration before the endpoint provisioning, as access through HTTP (web interface) and SSH (command line) to the endpoint will be disabled by default when registering to CUCM.

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

About device packages

The Cisco Unified CM Device Package contains device configuration capabilities for the Cisco TelePresence endpoints (C, EX, MX, SX, and Profile Series). The device package is available for download on our web site.

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

Encrypted vs non-encrypted communication

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

About endpoints previously used with TMS

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

About endpoints factory reset

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 "Factory resetting the TelePresence endpoint" on page 49.

What's new in this version

This section provides an overview of the new and changed features for TC7.0 used with CUCM 8.6.2, and later. The CUCM must have a device package with support for TC7.0. See the TC Release Notes for detailed information.

Support for alternate phone book server

The CUCM will have support for both UDS (User Data Service) and TMS (TelePresence Management Suite) for directory integration.

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

NOTE: TMS will have support for this feature by software release 14.4, estimated for March 2014.

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

About software versions

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

CUCM versions vs endpoints supported

TelePresence endpoints supported on Cisco Unified CM version 8.6.1.10000-43 and higher: MX200, EX Series (EX90, EX60), Quick Set C20, Codec C Series (C90, C60, C40) and Profiles using Codec C Series.

TelePresence endpoints supported on Cisco Unified CM version 8.6.2 and higher: 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.

If using Cisco Unified CM version lower than 8.6.2.21020 you must have Cisco Unified CM device pack from December 2011 to support MX300 and SX20.

Endpoint software vs endpoints supported

TelePresence endpoints supported on TC5.0 and higher: MX Series (MX300, MX200), EX Series (EX90, EX60), Quick Set C20, Codec C Series (C90, C60, C40) and Profiles using Codec C Series.

TelePresence endpoints supported on TC5.1 and higher: 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.

Option package for C20

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

CTI monitoring support for CTS Manager

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

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

Limitations

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

Useful links

User documentation and software download for the TelePresence endpoints:

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

User documentation and software download for Cisco Unified CM:.

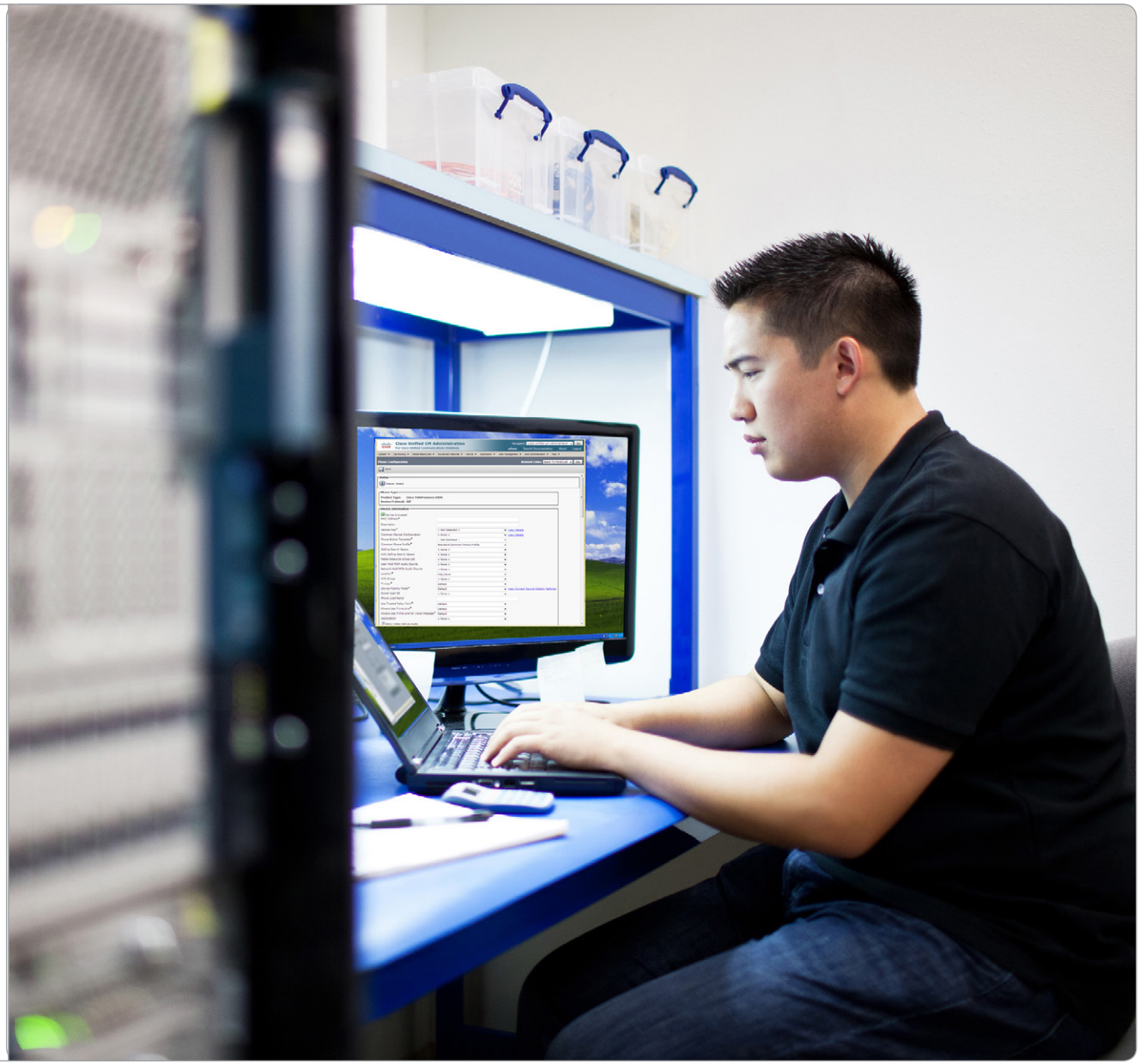
▸ http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

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 3

CUCM CONFIGURATION

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

Logging in to Cisco Unified CM Administration

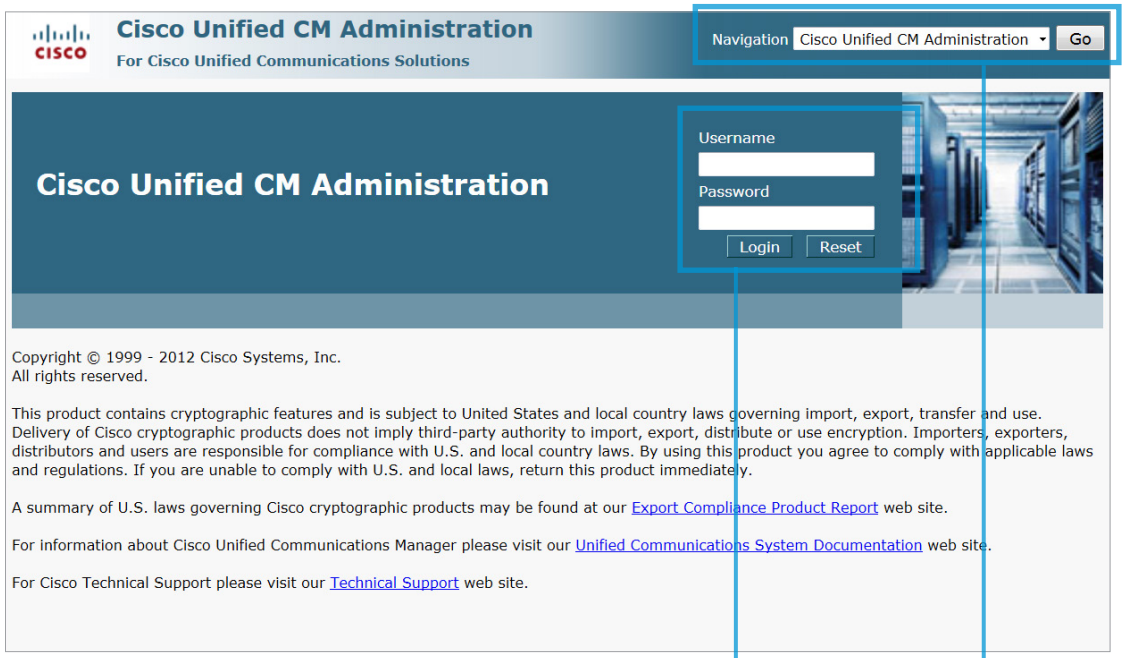
Open a web browser and enter the host name or IP address of the Cisco Unified CM and select *Cisco Unified Communications Manager* from the list of installed applications.

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

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

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

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



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

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

Mandatory Optional

Creating a SIP profile

You can copy a profile to use as a template.

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

SIP Profile configuration

Navigate to the *SIP Profile Information* section:

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

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

Redirect by Application: **Enable** by checking the checkbox.

Use Fully Qualified Domain Name in SIP Requests: **Enable** by checking the checkbox to enable the called endpoint to return the call using the received or missed call list (the history list). See also "Clusterwide Domain Configuration" on page 34.

Navigate to the *Trunk Specific Configuration* section:

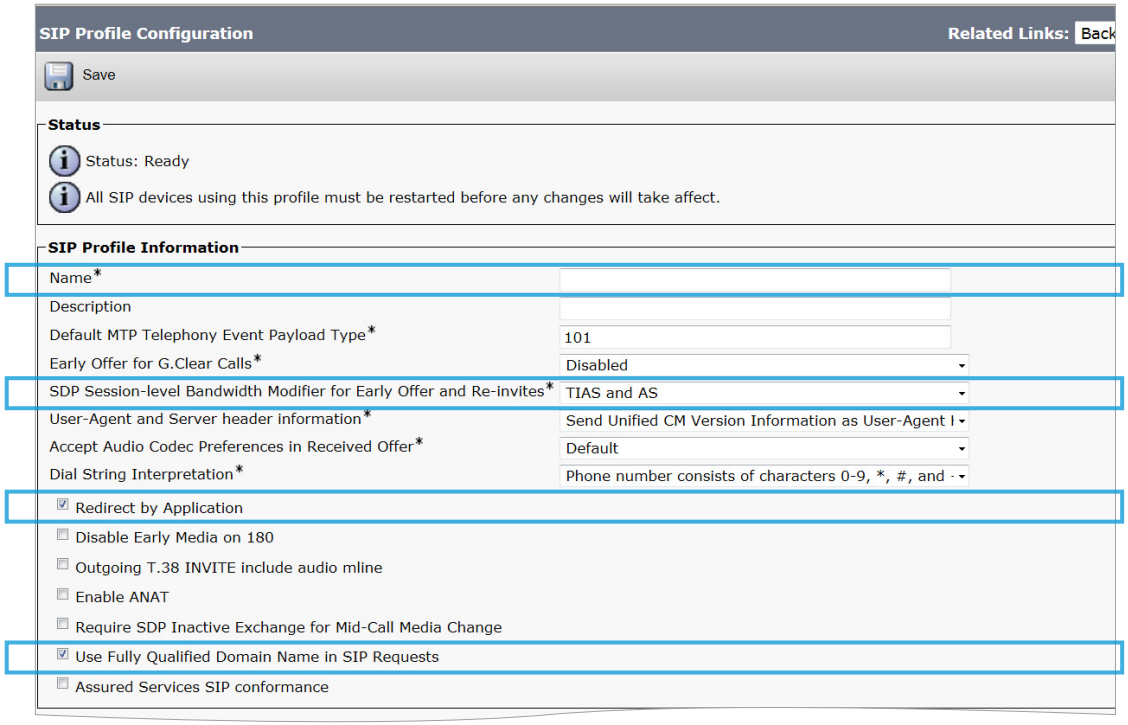
Allow Presentation Sharing using BFCP: **Enable** by checking the checkbox to allow presentation sharing.

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

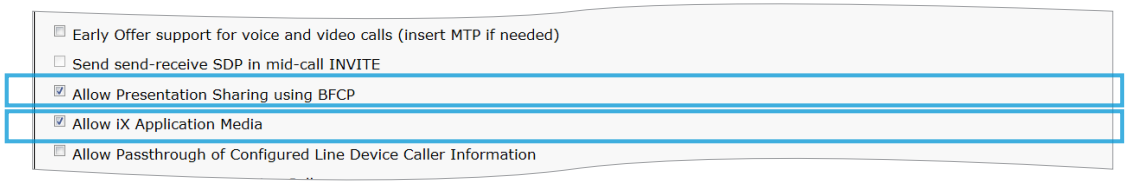
When done click **Save**.

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

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



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



Mandatory Optional

About the phone security profile

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

Releated information:

- CUCM must operate in mixed mode (cluster security mode) to enable secure communication.
- You must define one device security profile for each endpoint type.
- If you want to allow several authentication modes for the same endpoint type, you must define one profile for each mode.
- See the CUCM Security Guide for further information: ▸http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/9_1_1/secugd/CUCM_BK_C0395F44_00_cucm-security-guide-91.html

About the non-secure profile

The non-secure endpoints will use the **predefined non-secure profile**. If this is your option you can proceed to: "Manual registration of the endpoint" on page 13.

About the secure profile

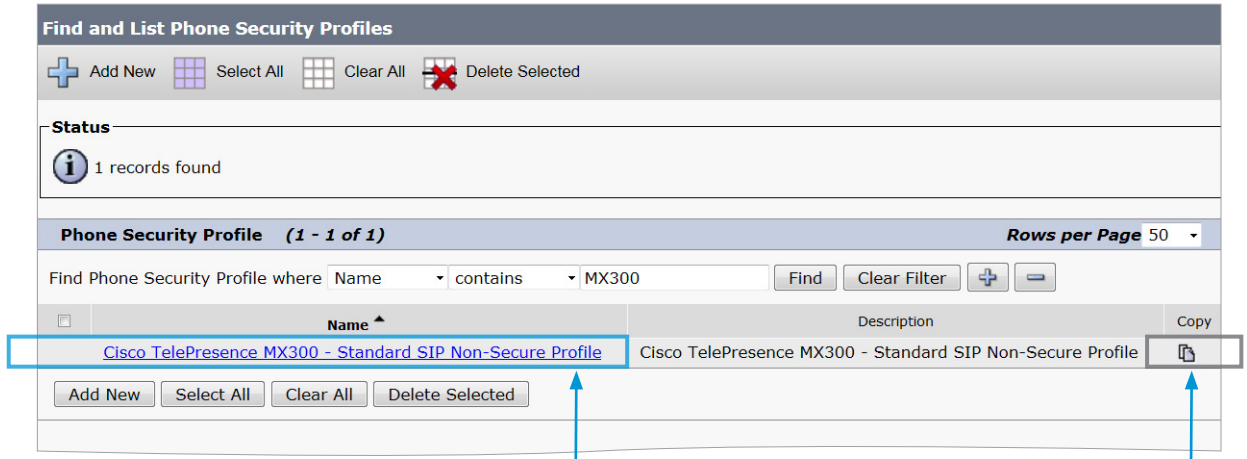
When configuring a secure device for the first time, you can copy a predefined non-secure profile to use as a template. This is the method used in this section.

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

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

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

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



Editing a security profile

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

Creating a security profile

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

Mandatory Optional

Creating a phone security profile

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

Phone security profile information

Only applicable when using secure (encrypted) communication.

Navigate to the *Phone Security Profile Information* section:

Name: Enter a name of the profile.

Description: Enter a description of the profile.

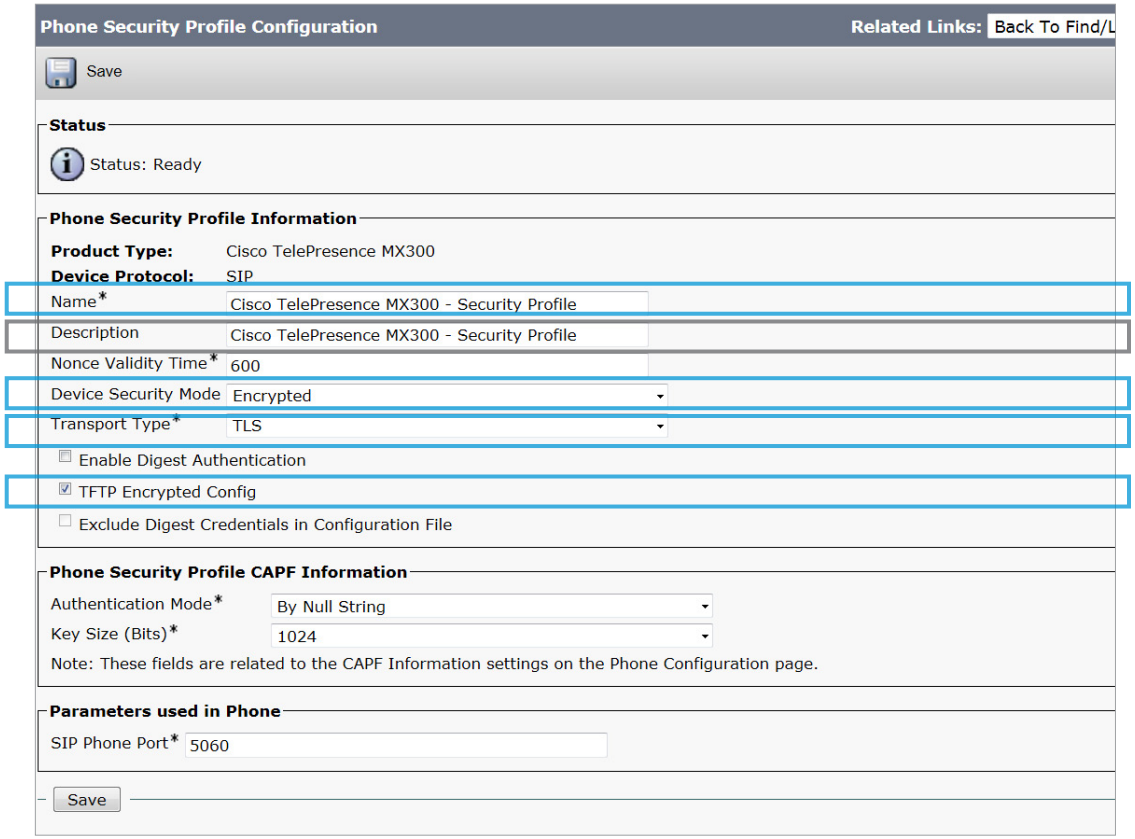
Device Security Mode: Set to Encrypted.

Transport Type: Set to TLS.

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

When done click **Save**.

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



Mandatory Optional

Creating a phone security profile

Phone security profile CAPF information

Only applicable when using secure (encrypted) communication.

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

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

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

By Authentication String: The CAPF process will commence when the correct authentication code is received from the endpoint. NOTE: The combination of encrypted configuration file and CAPF authentication mode "authenticating string" is not supported on the TelePresence endpoint side in software version TC6.2/TC6.3.

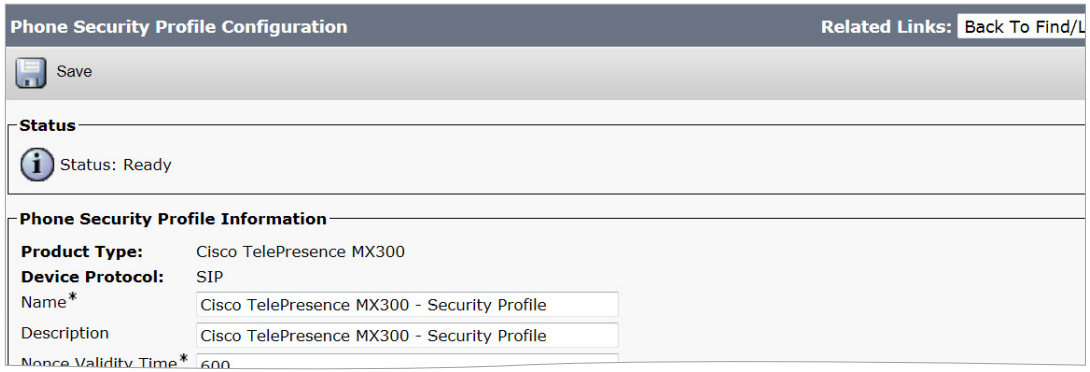
By Existing Certificate (precedence to LSC/MIC): This option can only be used when a Locally Significant Certificate (LSC) is already stored on the endpoint, i.e. it cannot be used the first time the CAPF process runs.

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

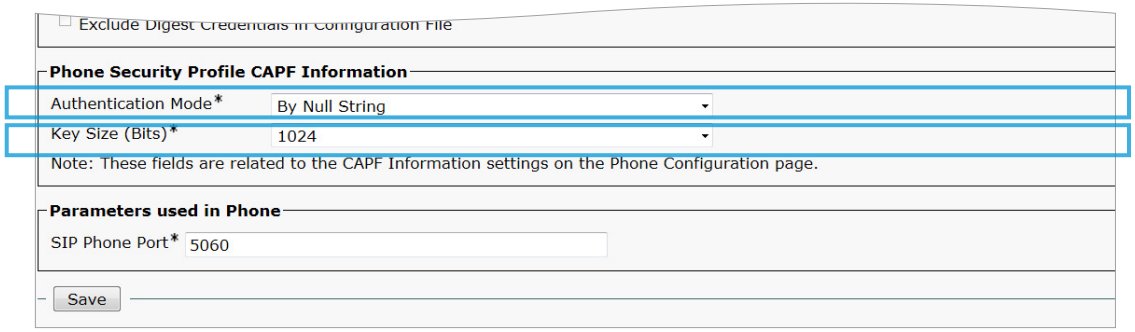
When done click **Save**.

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

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



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



Mandatory Optional

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 phone (endpoint)

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

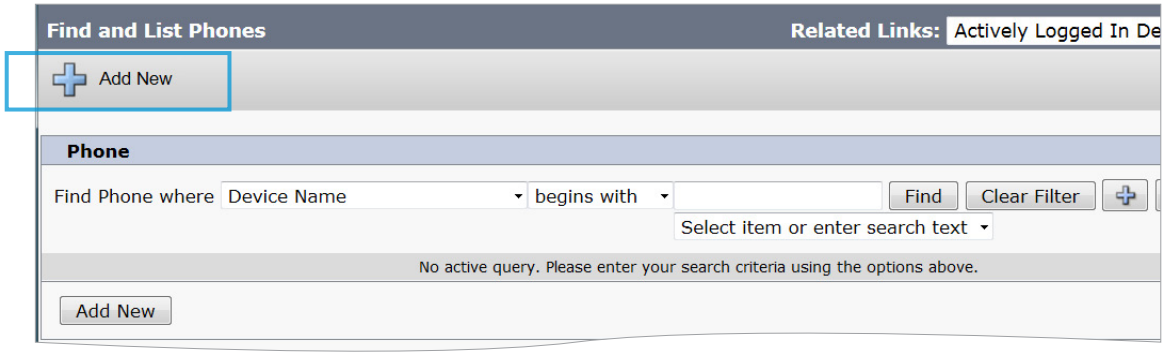
Navigate to *Create a phone using the phone type or a phone template* section.

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

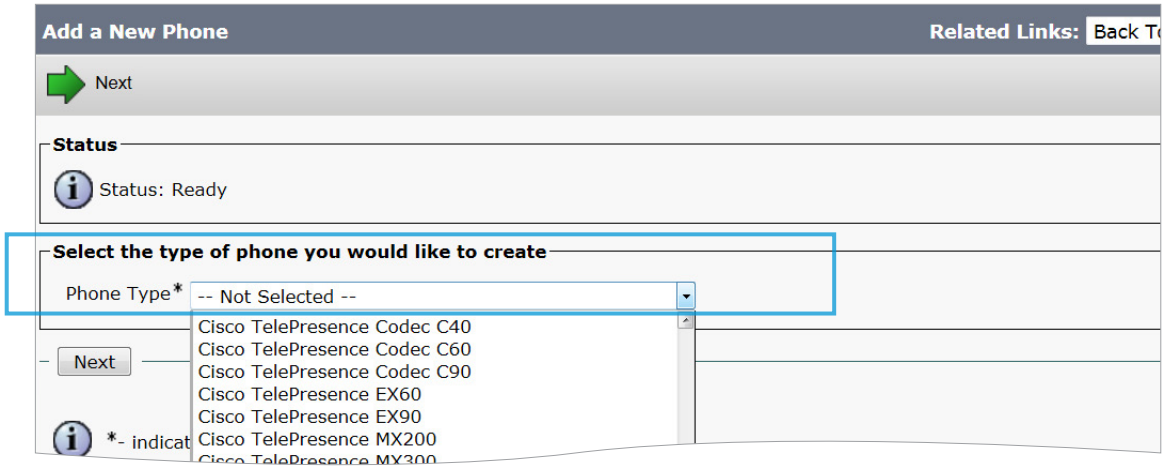
Click **Next**.

Navigate to: *Device* > *Phone*.

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



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



Mandatory Optional

Manual registration of the endpoint

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

Device information

Navigate to the *Device Information* section:

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

For information on how to find the MAC address, see: "Finding the MAC address of the endpoint" on page 50.

Device Pool: Choose a Device Pool.

Phone Button Template: Choose a Phone Button Template.

Protocol specific information

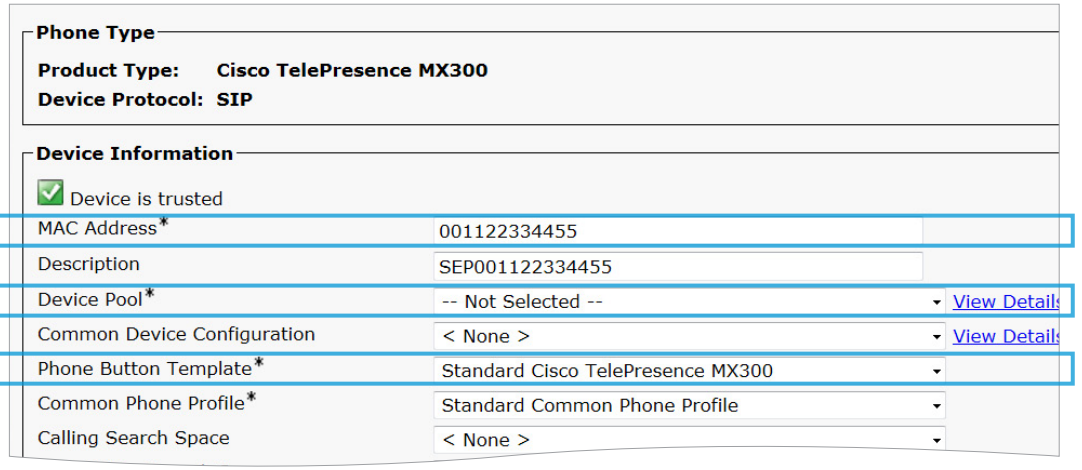
Navigate to the *Protocol Specific Information* section:

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

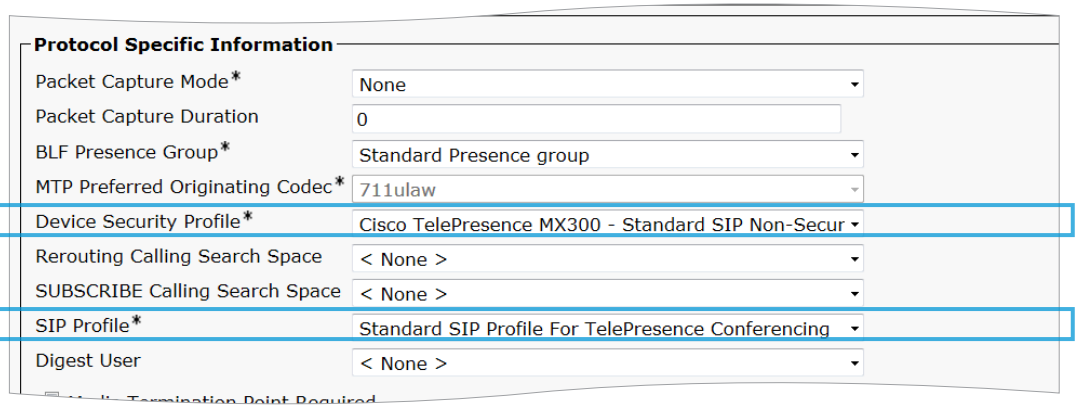
SIP Profile: Choose the SIP Profile you previously defined.

When done click **Save**.

Navigate to the **Device Information** section.



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



Mandatory Optional

Manual registration of the endpoint

Certification authority proxy function information

Only applicable when:

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

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

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

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

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

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

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

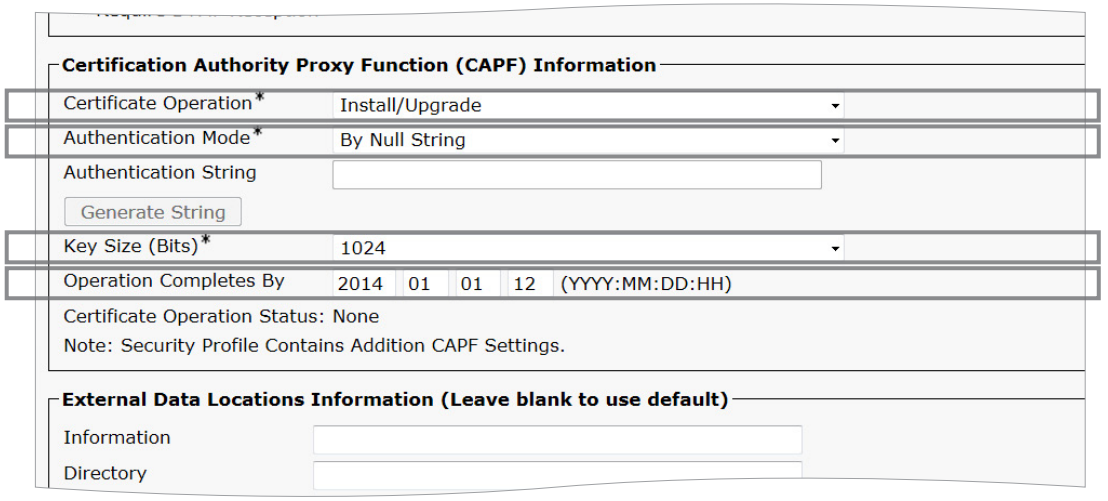
Key-size: Choose the appropriate value from the drop down list. The recommended key size is 1024.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

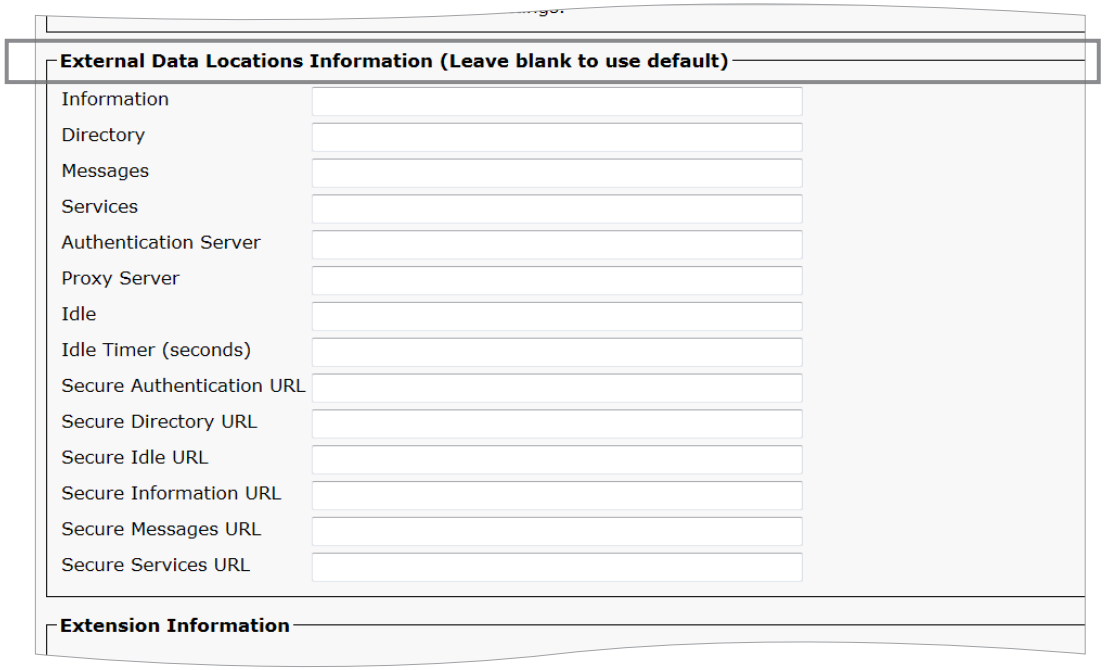
External Data Locations information

Navigate to the *External Data Locations Information* section:

Leave all fields blank to accept the default settings.

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

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



Mandatory Optional

Manual registration of the endpoint

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

Extension information

Navigate to the *Extension Information* section:

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

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

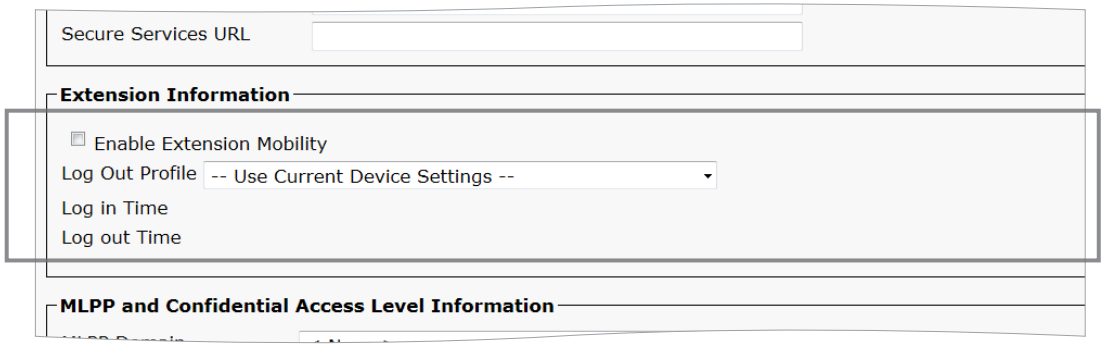
Log In Time: This field remains blank until a user logs in. When a user logs in, the time at which the user logged in displays in this field.

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

NOTE: For further details on how to setup Extension Mobility, refer to the Features and Services guide for CUCM. Go to: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

When done click **Save**.

Navigate to the **Extension Information** section.



Mandatory Optional

Manual registration of the endpoint

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

Product specific configuration layout

Navigate to the *Product Specific Configuration Layout* section:

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

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

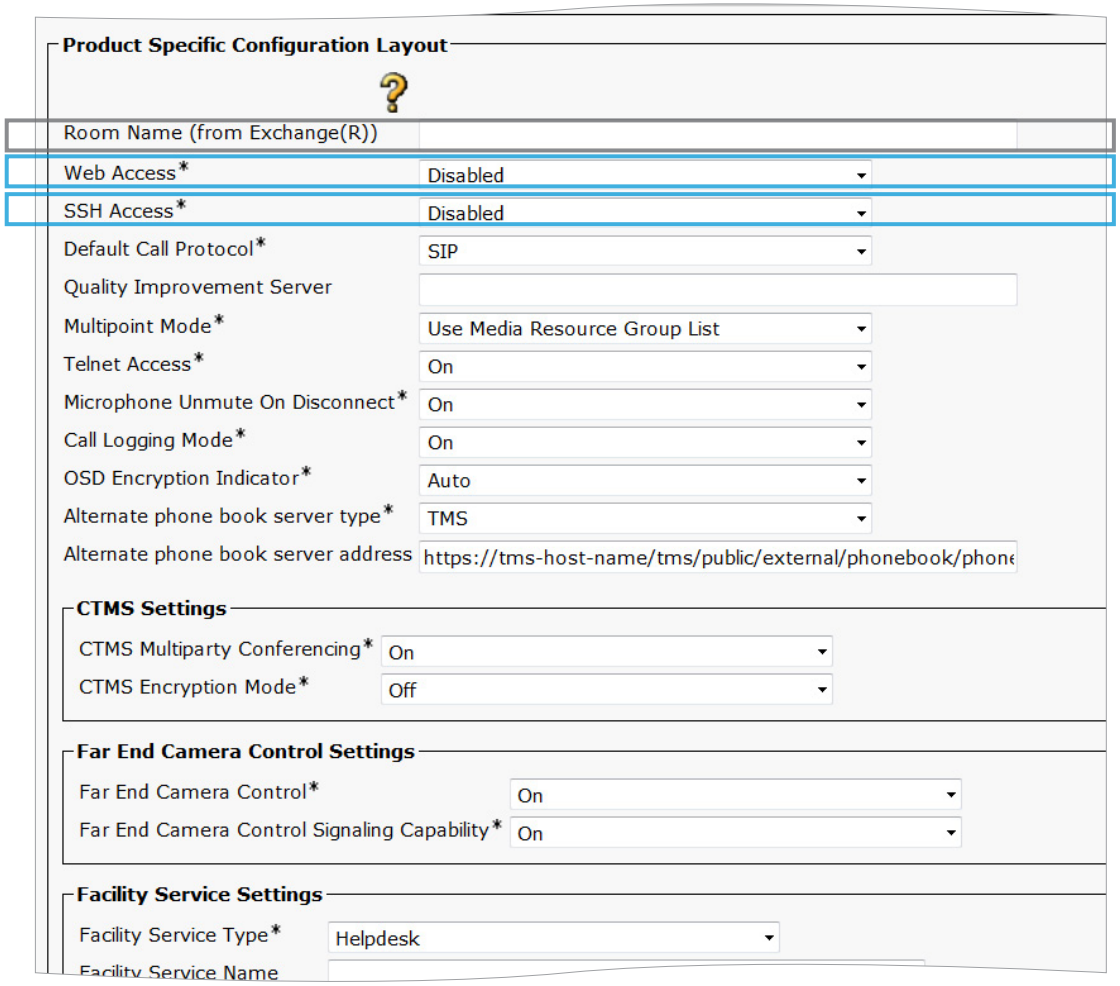
Web Access: This parameter indicates whether the device accepts connections from a web browser or other HTTP clients. Disabling the web server functionality of the device will block access to the TelePresence system's internal web pages and certain support capabilities, but will not degrade normal operation.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

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

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

When done click **Save**.

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout* section:

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

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

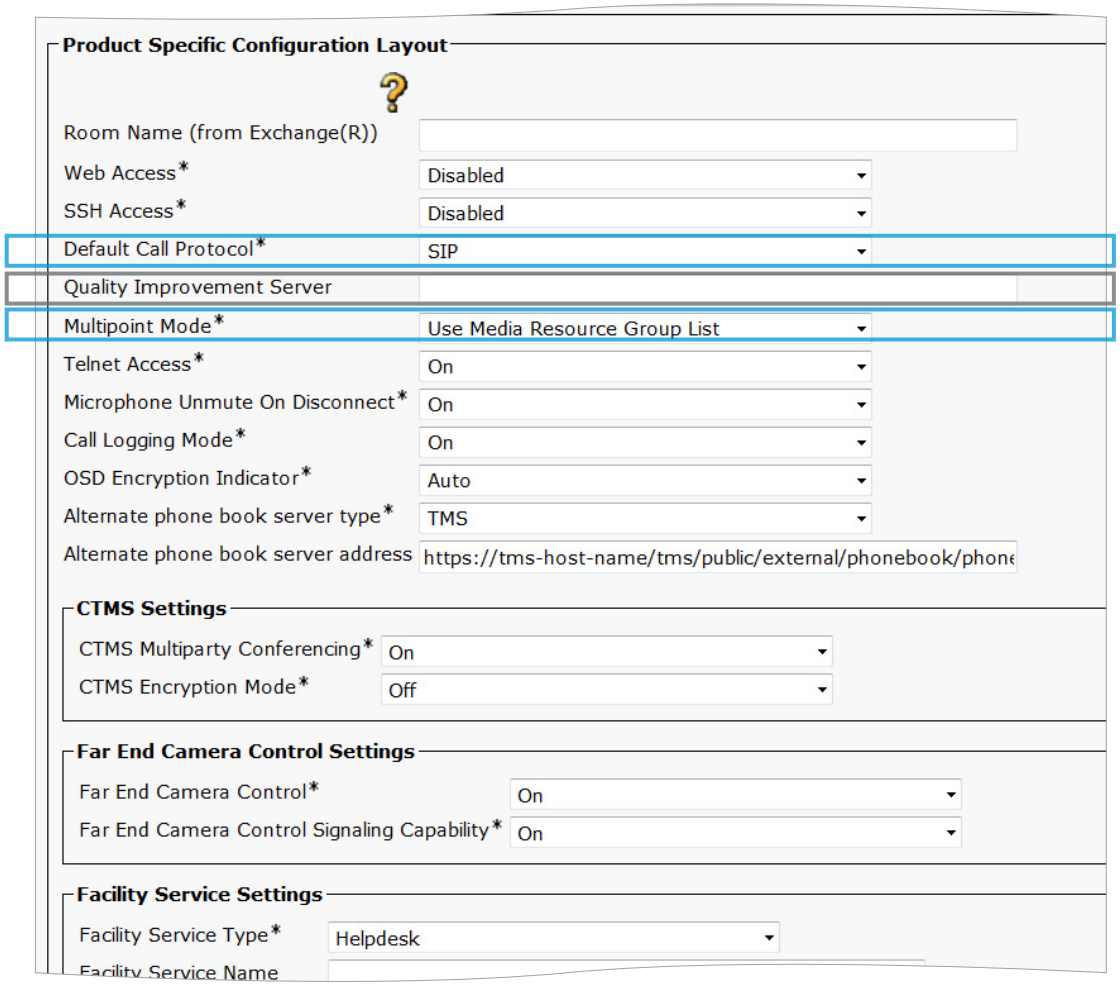
Multipoint Mode: Endpoints that do not have a bulit-in MultiSite feature can use the ad hoc conference bridge on Cisco Unified CM.

- Choose *Use Endpoint* to use the *built-in MultiSite* feature. NOTE: Applies to endpoints having MultiSite capability and having the option key installed.
- Choose *Use Media Resource Group List* to use the Conference Bridge (media resources) feature on Cisco Unified CM. This will enable the ad hoc conferencing feature and applies to non-MultiSite endpoints.

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

Navigate to the *Product Specific Configuration Layout* section:

Configure the product specific configuration layout settings as appropriate.

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

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

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

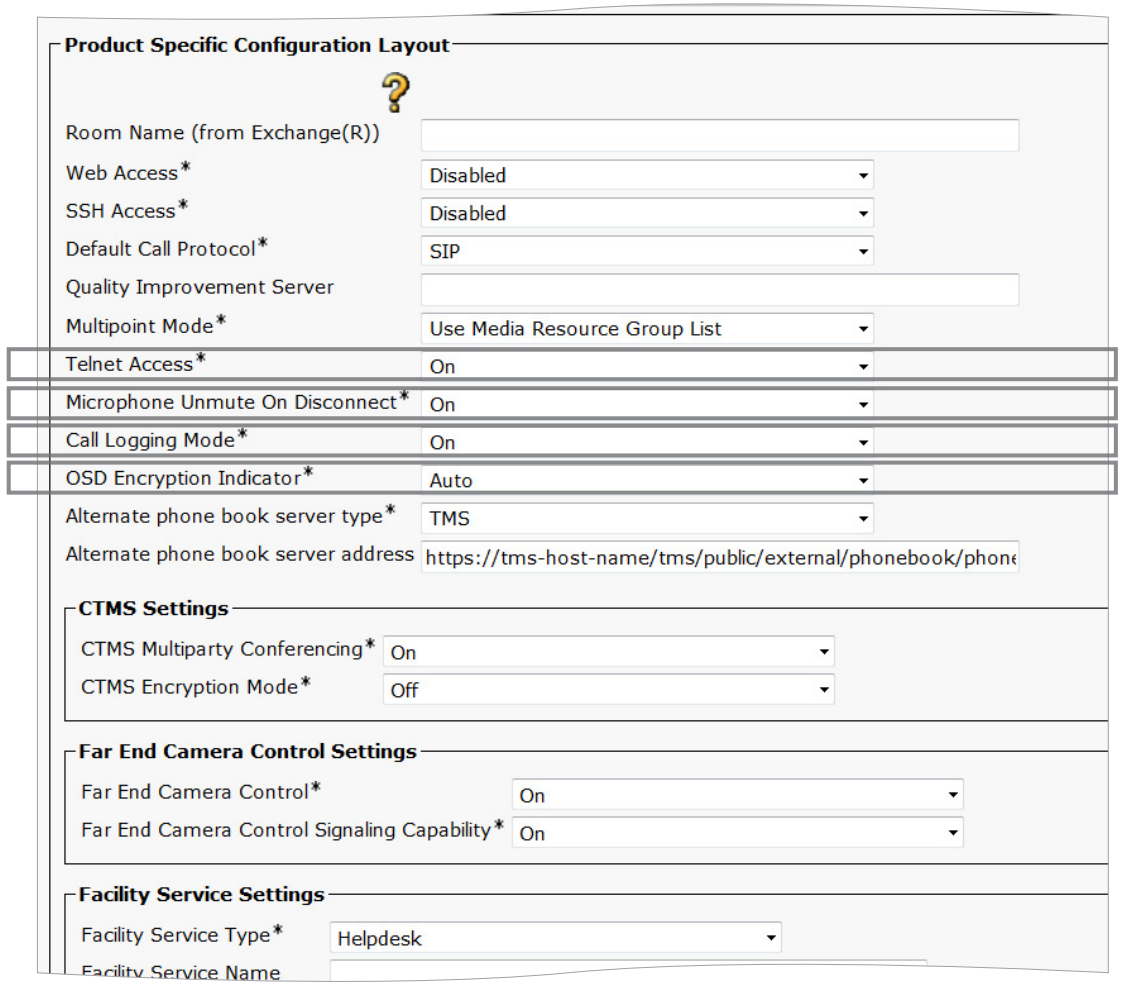
Call Logging Mode: Set the call logging mode (On/Off) for calls that are received or placed by the system. Default value is On.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Navigate to the *Product Specific Configuration Layout* section:

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

NOTE: TMS will have support for this feature by software release 14.4, estimated for March 2014.

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

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

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

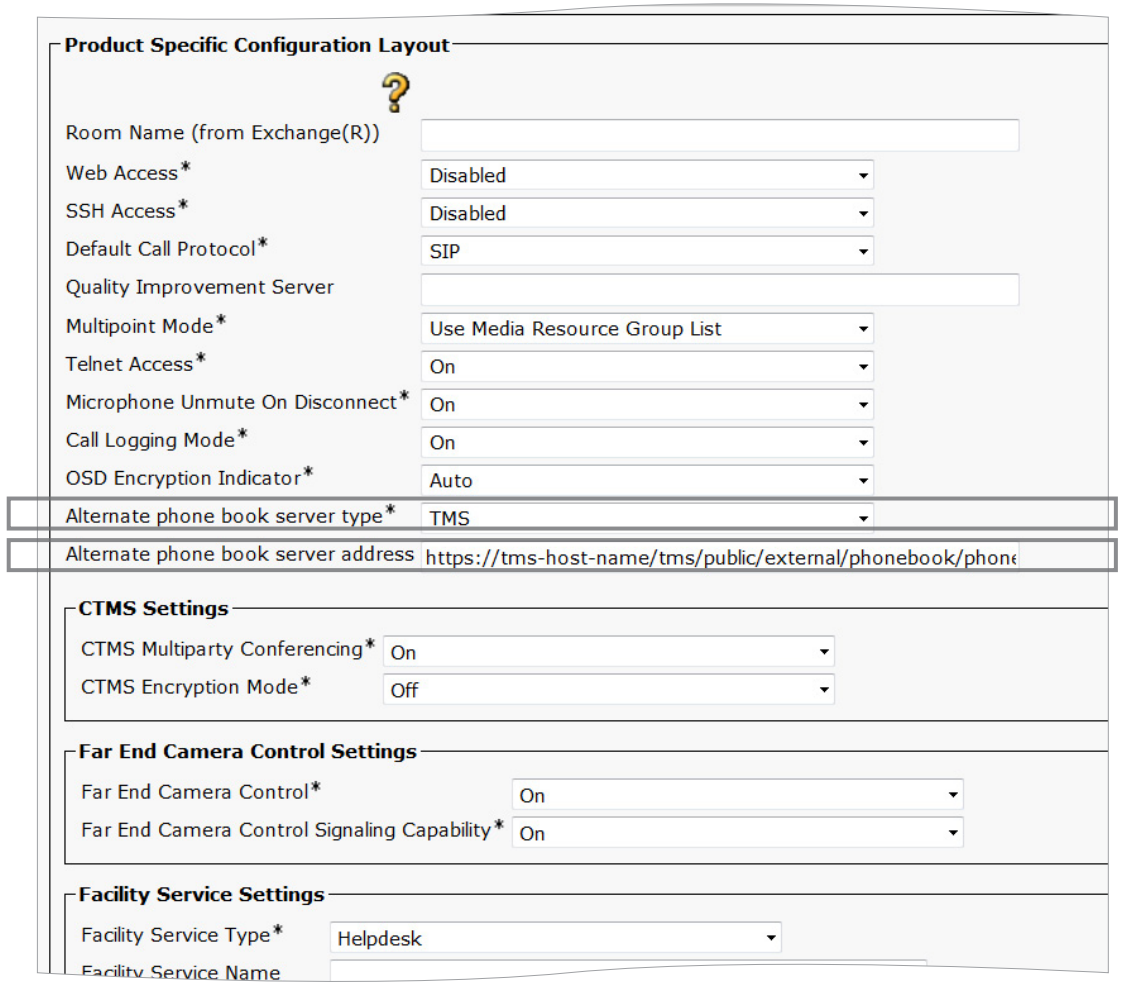
Alternate phone book server address: Enter the address to the phone book server. The field requires a full URL.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

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

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

Configure the product specific configuration layout settings as appropriate.

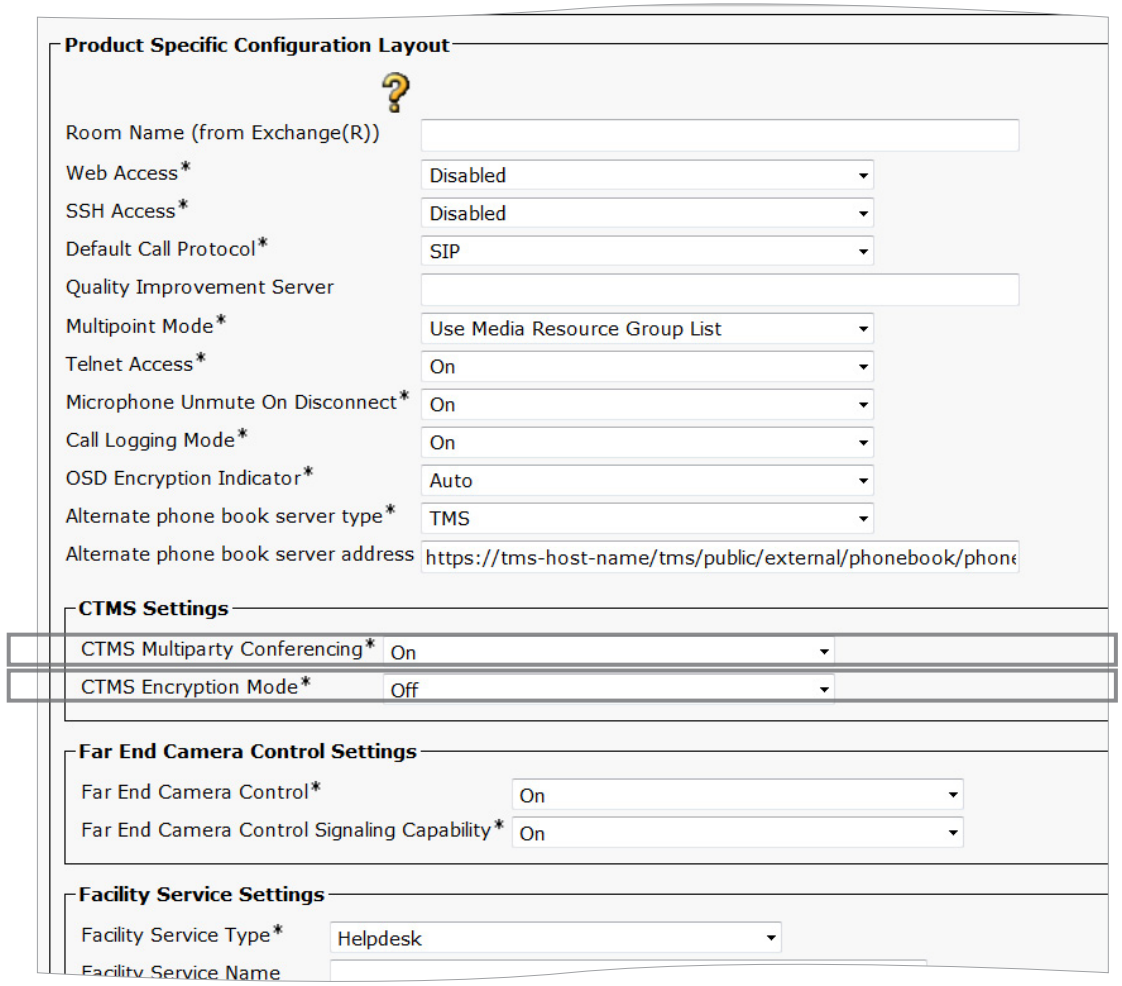
CTMS MultiParty Conferencing: Set the CTMS Multiparty Conferencing mode (On/Off). Default value is On.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

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

Configure the product specific configuration layout settings as appropriate.

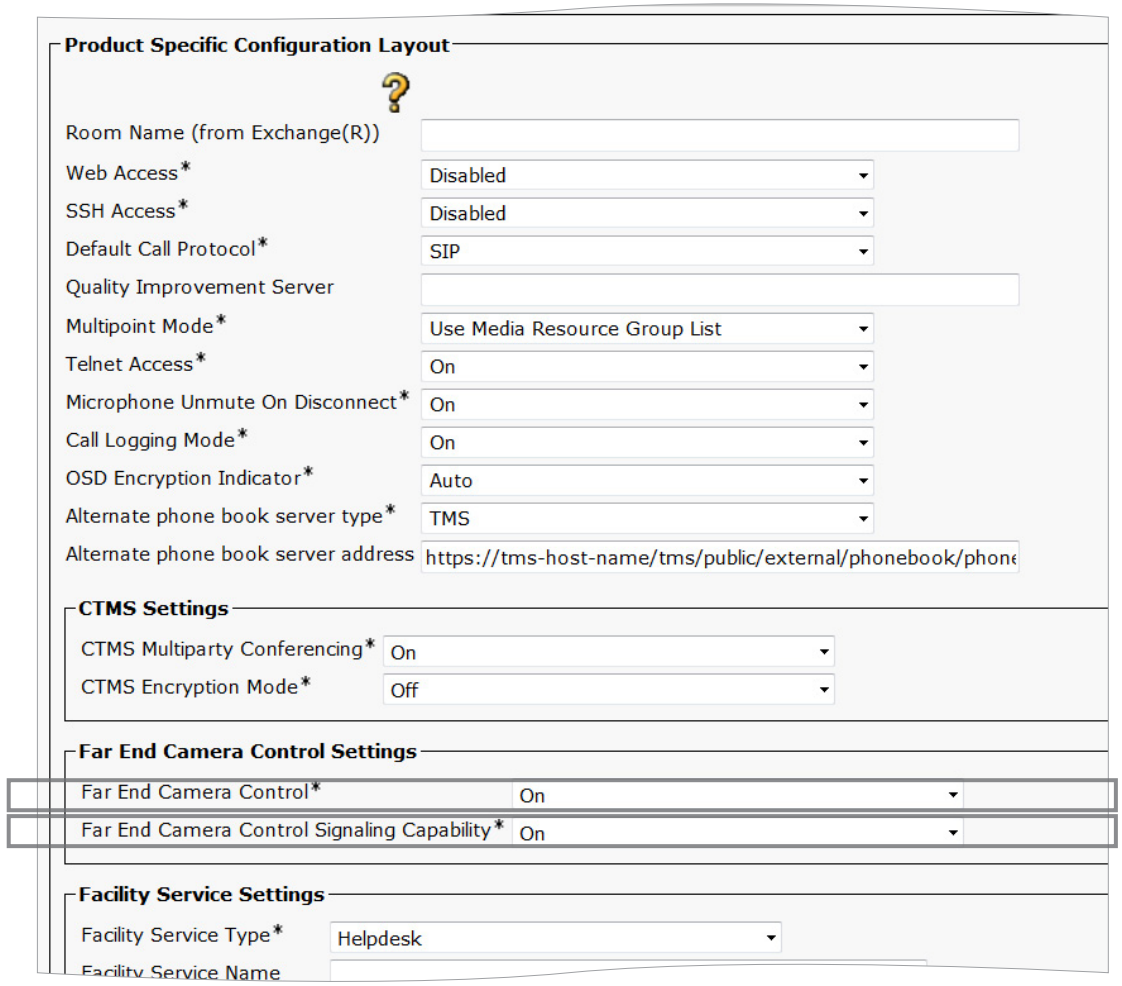
Far End Camera Control: Set the far end camera control mode (On/Off) to let the user on the endpoint (near end) decide if the remote side (far end) should be allowed to select video sources and control the near end camera (pan, tilt, zoom). Default value is On.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

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

Configure the product specific configuration layout settings as appropriate.

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

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

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

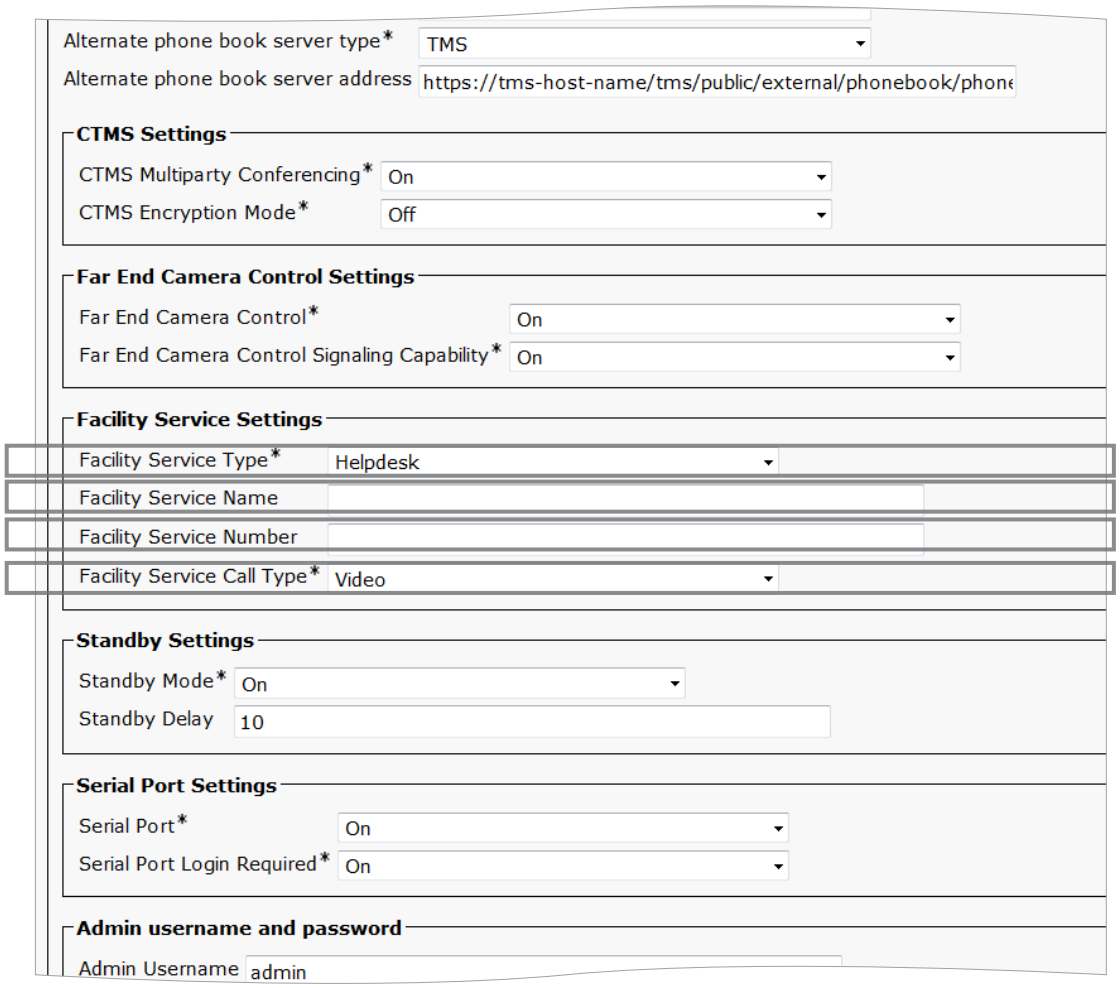
Facility Service Number: Enter the number of the facility service. Default value is "" (empty) and maximum length is 255 characters.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

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

Configure the product specific configuration layout settings as appropriate.

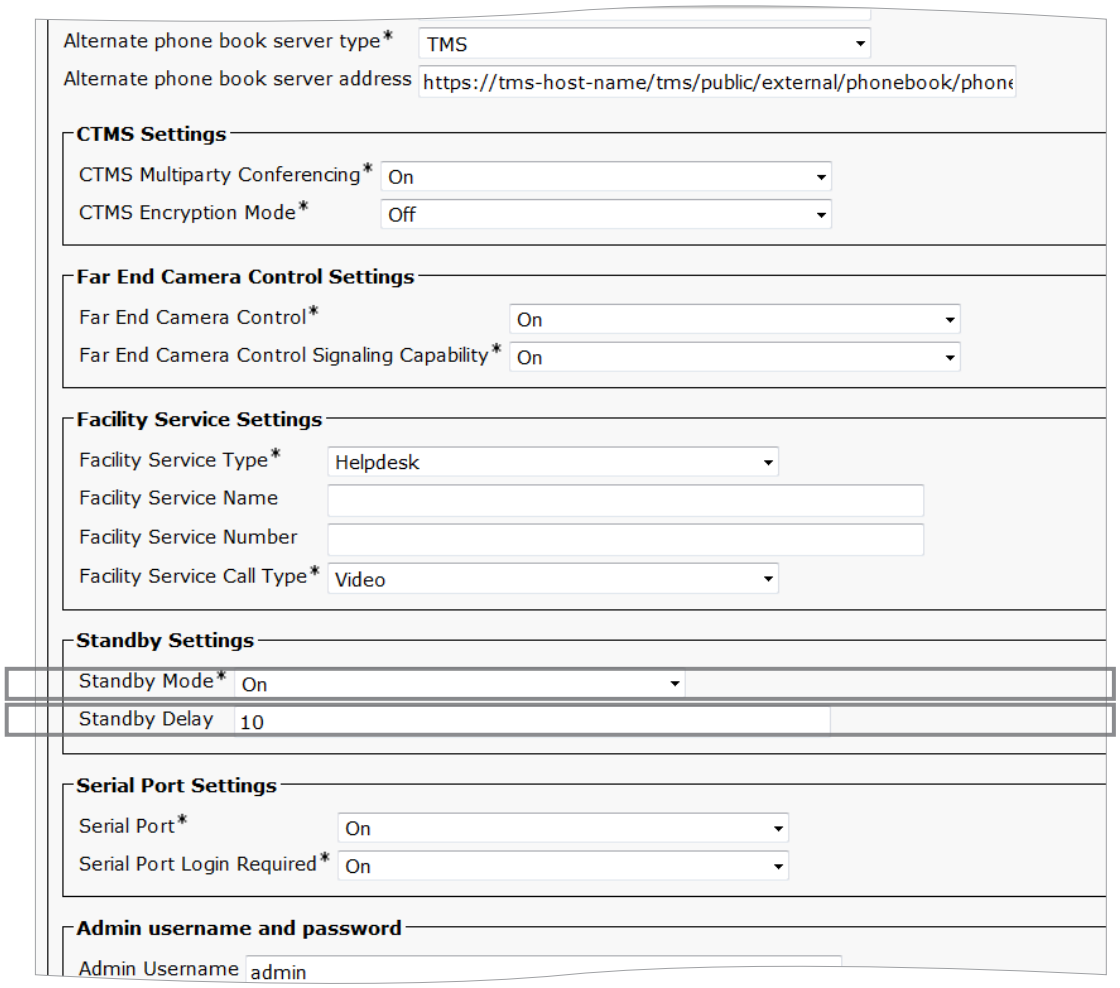
Standby Mode: Set the Standby Mode (On/Off) to determine whether the endpoint should go into standby mode or not. Default value is On.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

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

Configure the product specific configuration layout settings as appropriate.

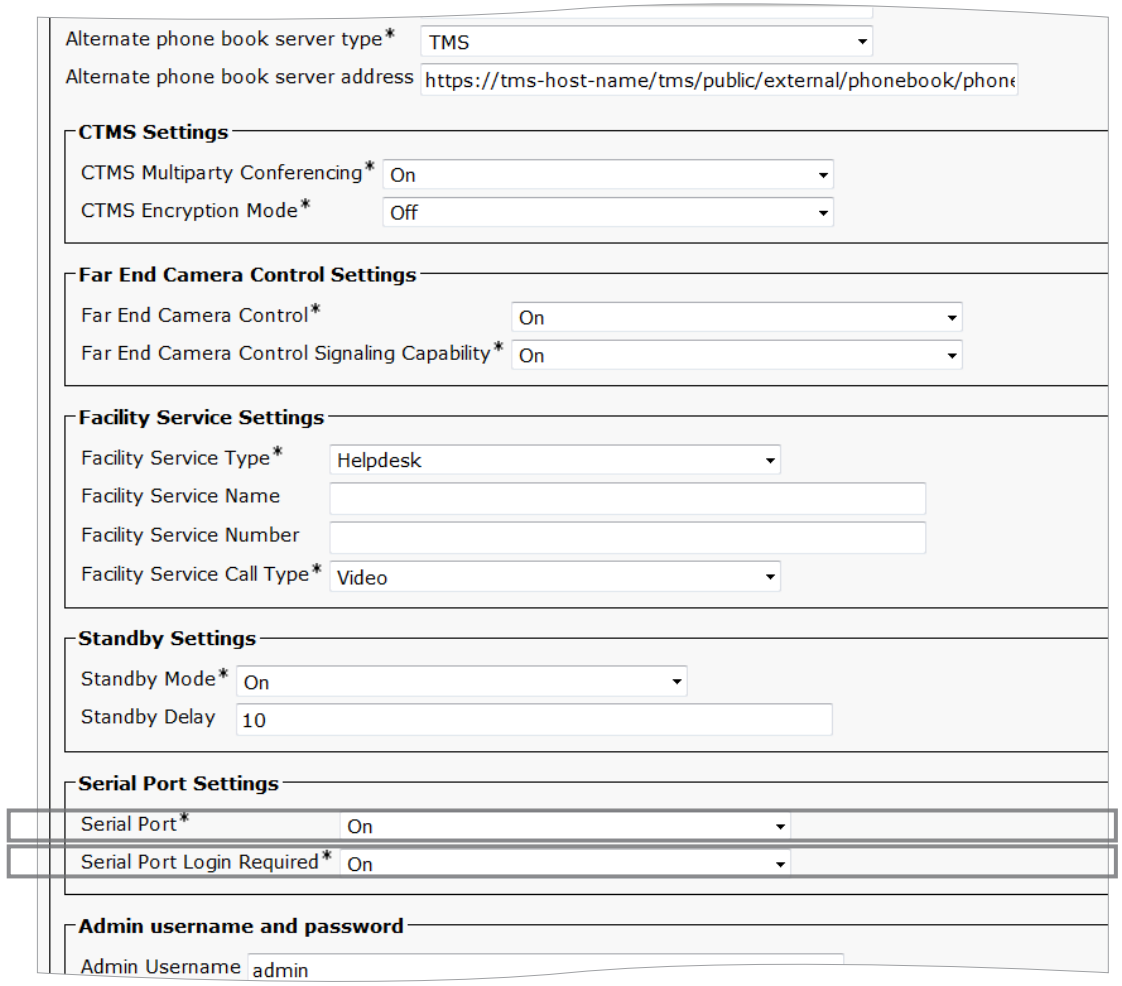
Serial Port: Set the serial port mode (On/Off) to enable/disable the serial port. Default value is On.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

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

Configure the product specific configuration layout settings as appropriate.

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

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

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

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

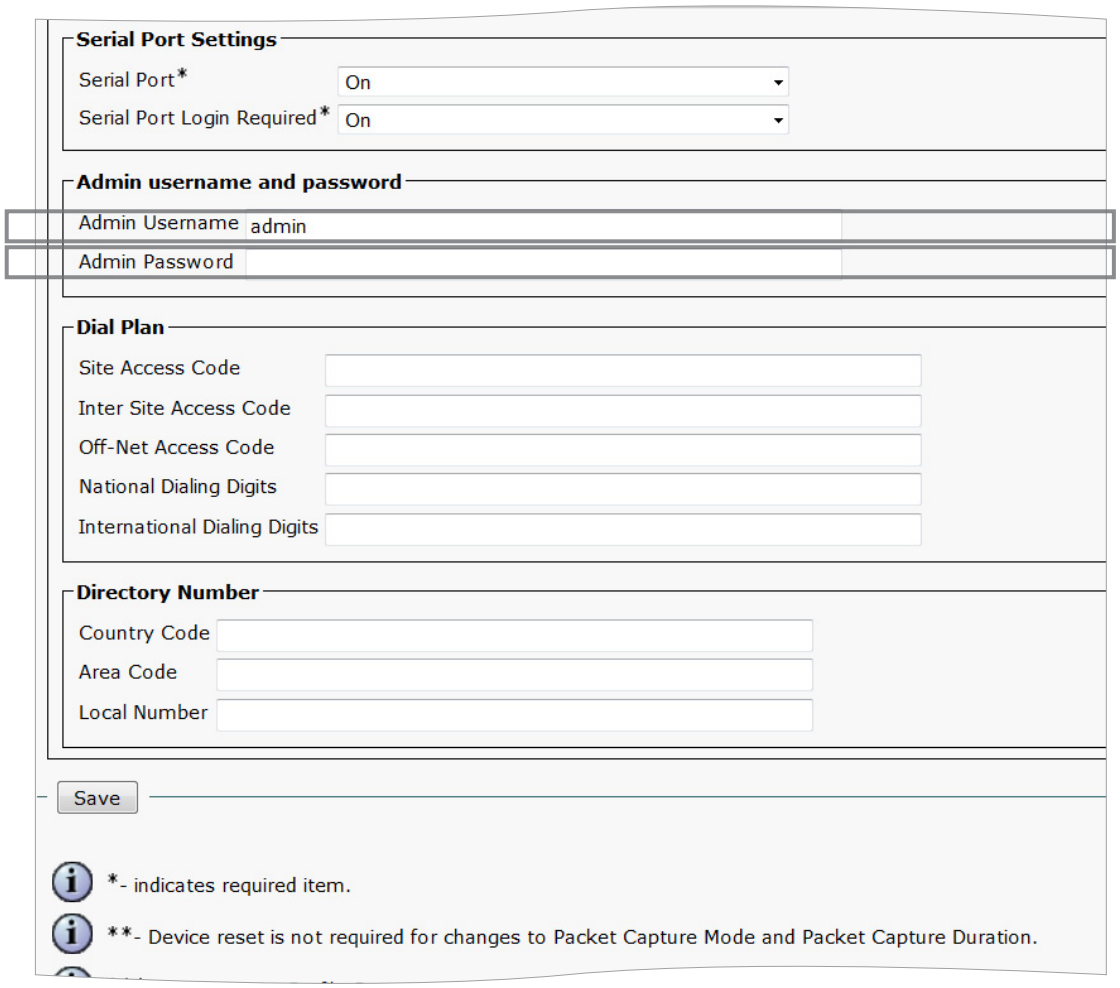
For further information:

- Refer to "About the phone security profile" on page 10.
- Refer to "Setting the system password" on page 37.

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

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

Configure the product specific configuration layout settings as appropriate.

Only applicable when using Cisco TelePresence Manager.

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

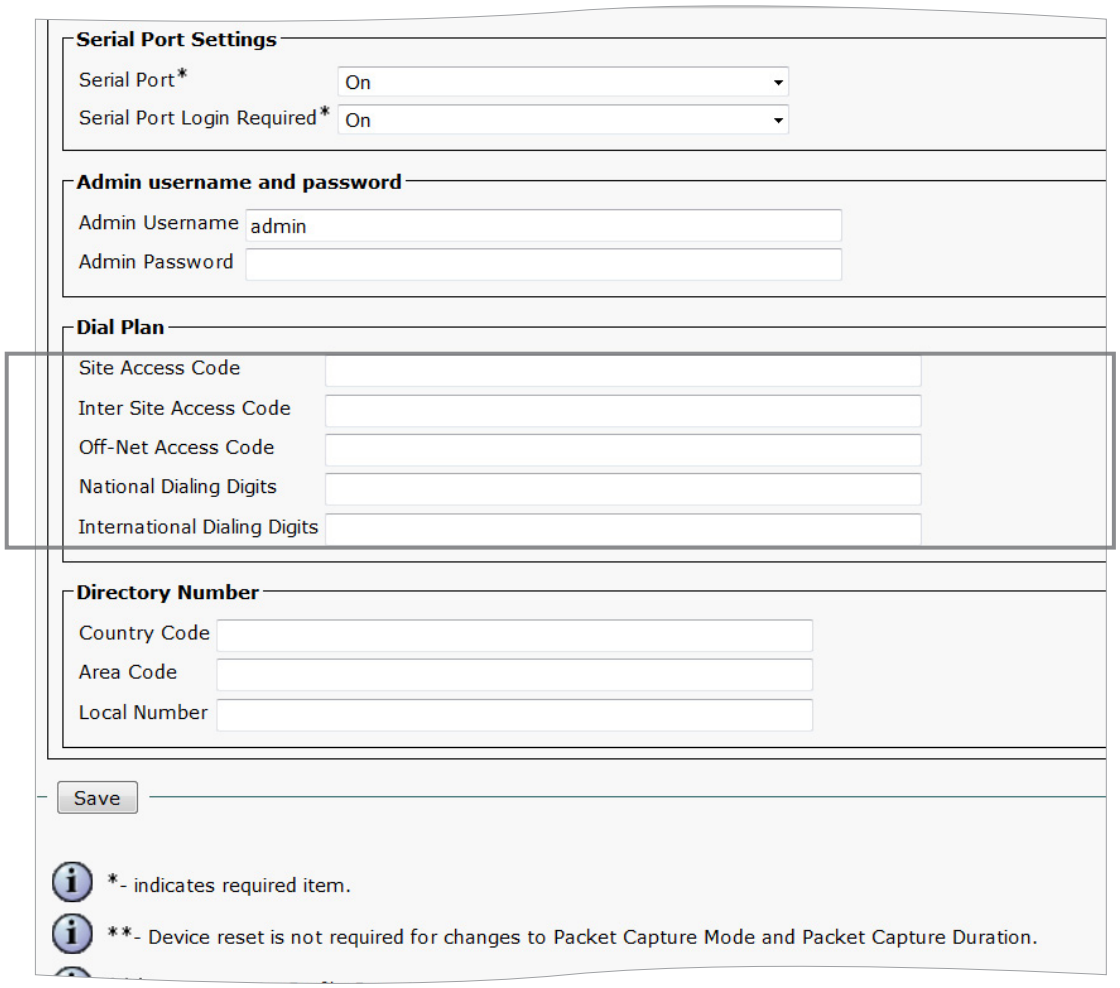
Configure the dial plan. Refer to Cisco TelePresence Manager documentation for more details.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Product specific configuration layout

Continued from the previous page...

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

Configure the product specific configuration layout settings as appropriate.

Only applicable when using Cisco TelePresence Manager.

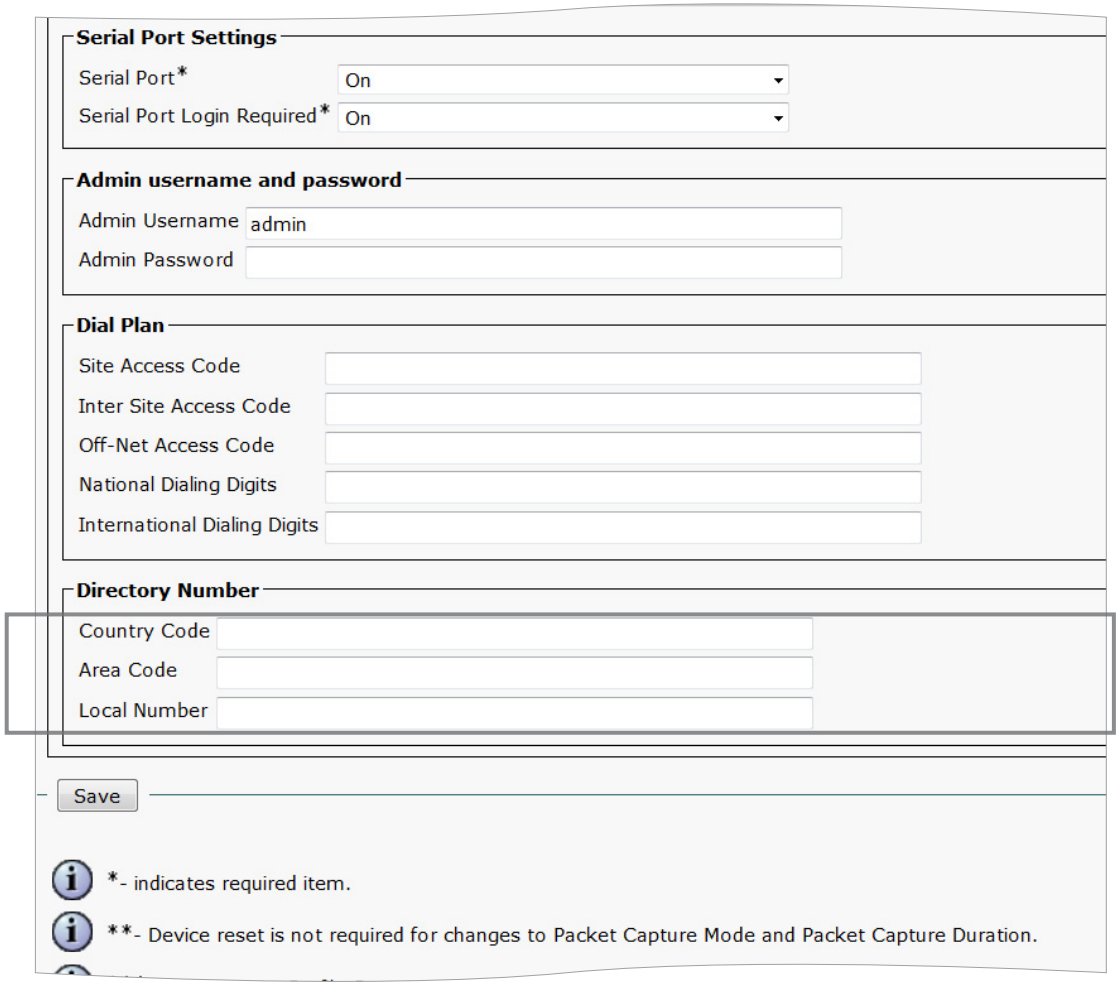
Configure the directory number. Refer to Cisco TelePresence Manager documentation for more details.

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

When done click **Save**.

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

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



Mandatory Optional

Manual registration of the endpoint

Adding the directory number

Navigate to the *Association Information* section:

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

Directory number information

Navigate to the *Directory Number Information* section.

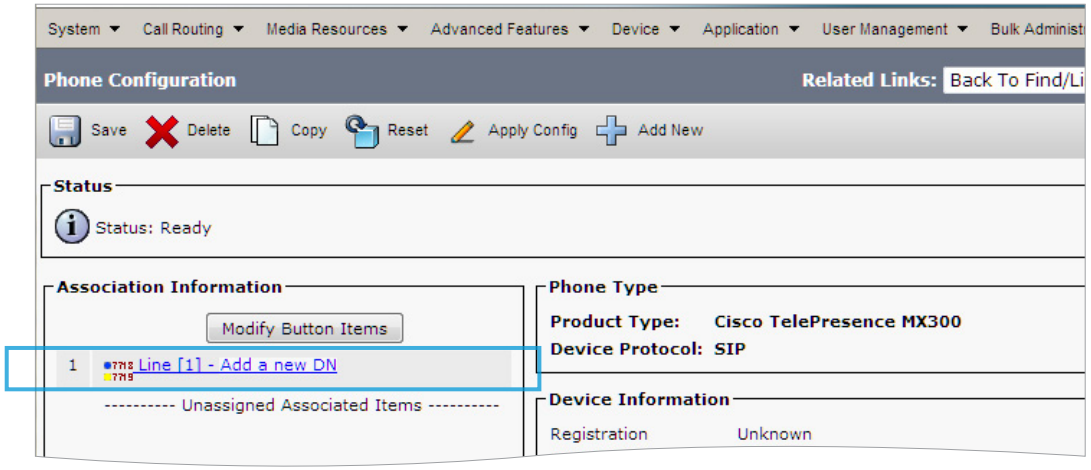
Directory Number: Enter the number of the endpoint, according to the E.164 Numbering Plan

Click **Save**.

Continues on the next page...

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

Navigate to the **Association Information** section.



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

Mandatory Optional

Manual registration of the endpoint

Configuring shared lines

Optional: To configure the CUCM for shared lines, navigate back to "Manual registration of the endpoint" on page 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 *Privacy* setting to *Off* for shared lines to function as intended. You can find this setting under *Device > Phone > Phone Configuration > Device Information*.

Display the name of the caller

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

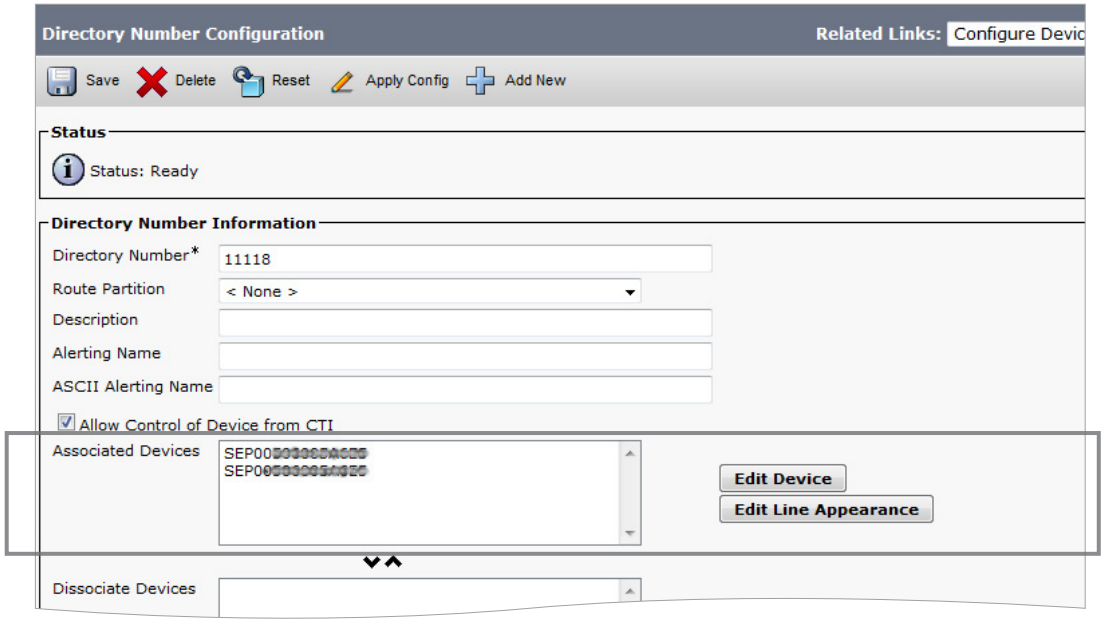
Display (Caller ID): Enter the name of the owner of the TelePresence system to allow the receiver of a call from the system to see the proper identity of the caller.

Display text for a line appearance is 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 may not see the proper identity og the caller.

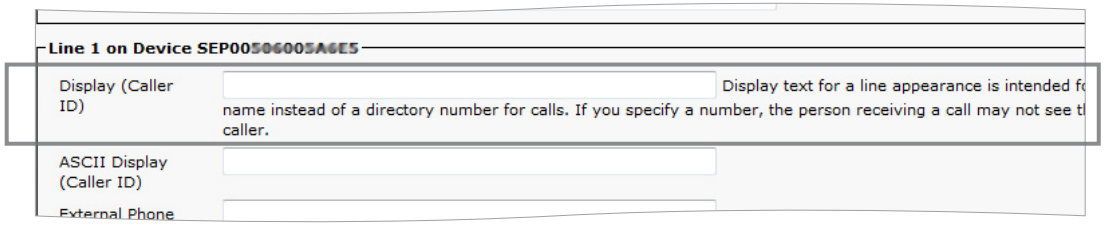
When done click **Save** and **Apply Config**.

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

Navigate to the **Association Information** section.



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



Mandatory Optional

Auto-registration of the endpoint

Only applicable when the CUCM is not set to mixed mode.

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).

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

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

Enable auto-registration

Navigate to the *Auto-registration Information* section.

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

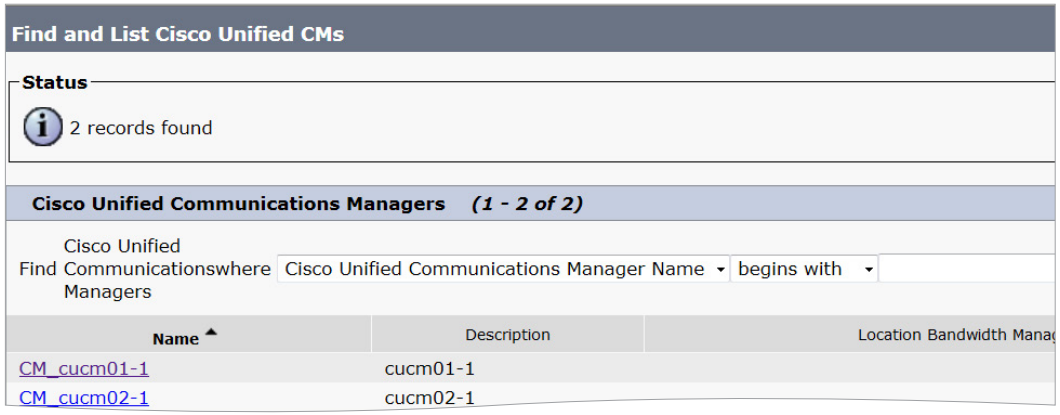
Ending Directory Number: Enter the highest number in the range of directory numbers.

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

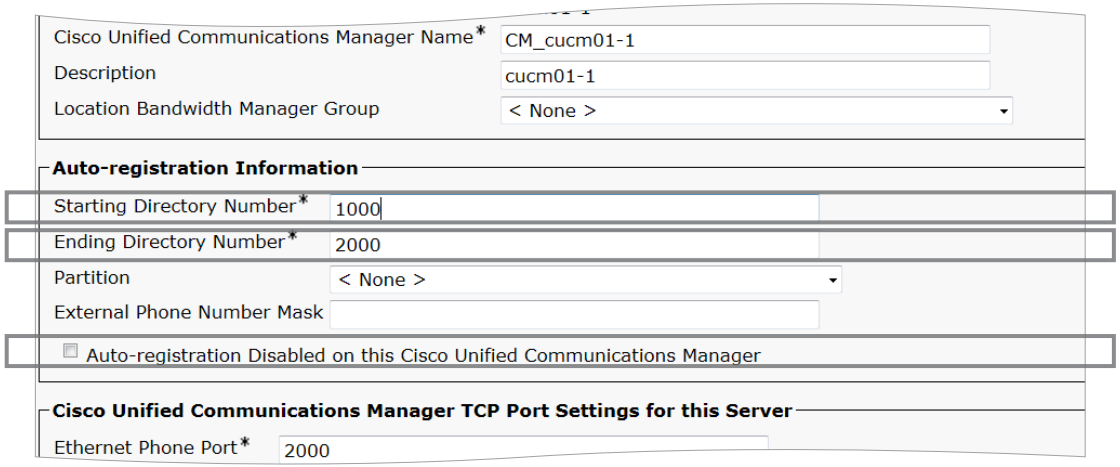
When done click **Save** and **Apply Config**.

Navigate to: *System > Cisco Unified CM*.

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



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



Mandatory Optional

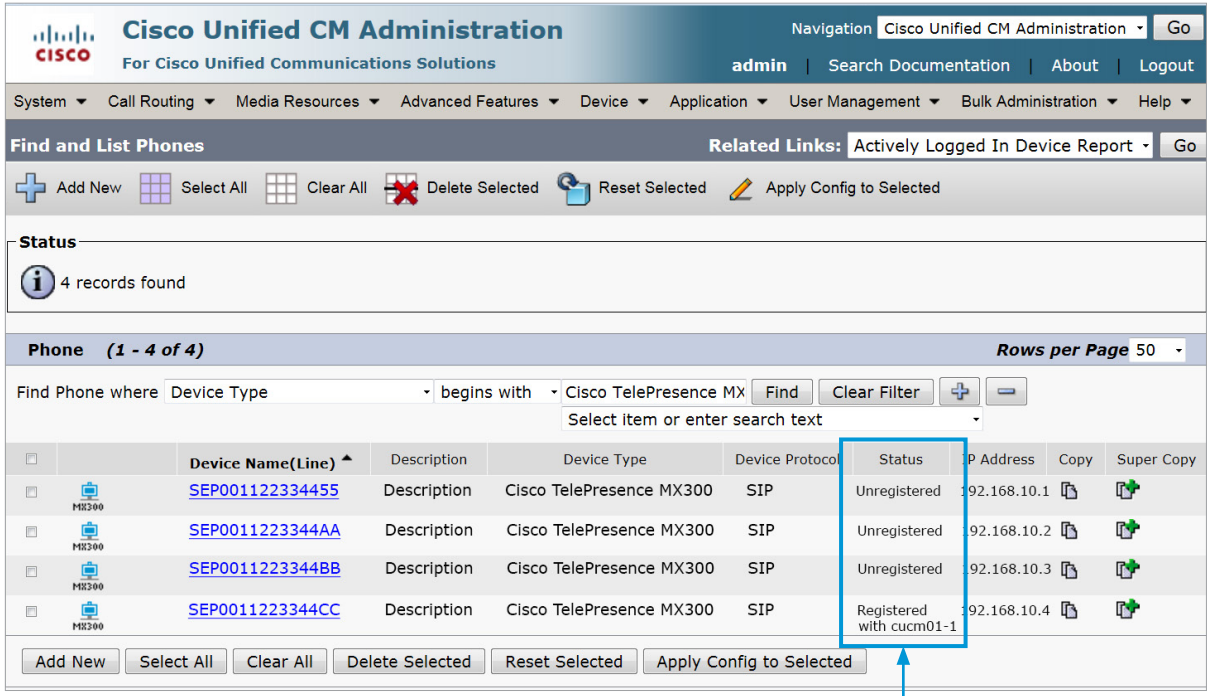
How to verify the endpoint registration

NOTE: Before you can verify the endpoint registration you must configure the TelePresence endpoint. See: "About endpoint configuration" on page 36

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

Navigate to: *Device* > *Phone*

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



The status of the endpoint registration.

Enterprice parameters

Navigate to: *System > Enterprice Parameters*

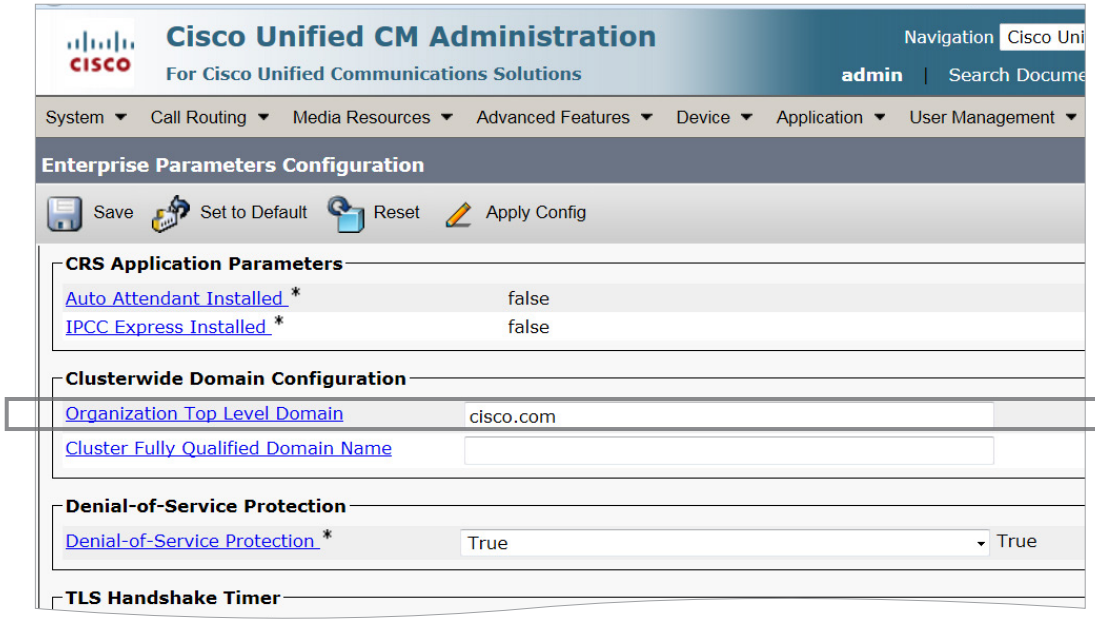
Clusterwide Domain Configuration

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

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

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

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



Mandatory Optional

CHAPTER 2

ENDPOINT CONFIGURATION

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

About endpoint configuration

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

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

NOTE: We recommend doing the CUCM configuration before the endpoint provisioning, as access through HTTP (web interface) and SSH (command line) to the endpoint will be disabled by default.

Endpoint diagnostic tools

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

Endpoint configuration in three steps

Setting the system password

We strongly recommend setting a password for the users to restrict access to system configuration. If no password is set there will be a notification on screen.

Go to: "Setting the system password" on page 37.

Setting the call details

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

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

Go to: "Setting the call details" on page 38.

Provisioning the endpoint to CUCM

Provisioning allows the video conferencing network administrators to manage many video systems simultaneously.

Go to: "Setting up provisioning" on page 39.

Finding the IP address

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

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

- Using the Touch controller: Tap *(Settings) > System Information* and see the *General* section.
- Using the remote control: Navigate to *Home > Settings > System Information* and see the *Network* section.

Setting the system password

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

If the endpoint is set up with an encrypted security profile

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

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

Access through HTTP and SSH

Access to the endpoint through HTTP (web interface) and SSH (command line) is disabled by default when the endpoint is registered to Cisco Unified CM.

If used with Cisco TelePresence Manager

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.

Using the web interface

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

Set or change the system password

1. Click on the username in the upper right corner and choose *Change password* in the drop down menu.
2. Enter the *Current password*, the *New password*, and repeat the new password in the appropriate input fields.

   The password format is a string with 0–64 characters.
3. Click *Change password*.

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

Using the command line interface

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

Set or change the system password

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

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

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

Setting the call details

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

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

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

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

Using the Touch panel

Tap *(Settings) > Administrator > Call Details*.

1. **Configure the auto answering**

   Set Auto Answer to the desired value.

   If appropriate set the *Auto Answer Delay*.

2. **Configure the default call settings**

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

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

Using the remote control

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

1. **Configure the auto answering**

   Navigate to *Home > Settings > Administrator Settings > Advanced Configuration > Conference 1 > AutoAnswer* and set appropriate values for auto answer *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.

Using the web interface

Navigate to *Configuration > Advanced Configuration > Conference*.

3. **Configure the auto answering**

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

   Click *Save* after each change.

4. **Configure the default call settings**

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

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

   Click *Save*.

Using the command line interface

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

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 up provisioning

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

For more information about the *external manager address* and *CTL files*, refer to "About endpoint provisioning" on page 46.

Using the Touch panel

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

Running the provisioning wizard

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

Using the remote control

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

Configuring the provisioning

1. Navigate to *Home* > *Settings* > *Administrator Settings* > *Advanced Configuration* > *Provisioning*.
2. Navigate to the *ExternalManager* section and enter the IP address or DNS name of the External Manager (the CUCM cluster TFTP server address). Click *Save*.
3. From the drop down list, set the *Provisioning Mode* to CUCM. The change will take effect immediately.

Using the web interface

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

Configuring the provisioning

1. Navigate to *Configuration* > *System Configuration* > *Provisioning*.
2. Navigate to *ExternalManager* section and enter the Address, which can be an IP address, DNS name, or the path of the External Manager (the CUCM cluster TFTP server address). Click *Save*.
3. Navigate to *Mode* and set the provisioning mode *CUCM*. Click *Save*.

Using the command line interface

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

Configuring the provisioning

`xConfiguration Provisioning Mode:`
[must be CUCM]

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

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

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

`xCommand Provisioning CUCM CTL Delete`
[If required: delete the CTL file]

Verifying the endpoint registration

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

Making a call

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

Use the interface of your choice:

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

Checking the system information

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

Using the web interface

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

Using the Touch controller

Tap *(Settings) > System Information* on the Touch and see the *SIP* section.

Using the remote control

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

Using the command line interface

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

```
xStatus SIP Profile 1 Registration 1 Status
xStatus SIP Proxy 1 Address
```

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

CHAPTER 4

ABOUT PASSWORDS

This section describes the use of passwords on TelePresence endpoints.

Setting the system password

The system password protects the video system. You have to sign in to be able to use the web and command line interfaces, and to get access to the Administrator settings from a Touch 8 control panel.

The *admin* user

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

We strongly recommend that you set a password for the *admin* user in order to restrict access to system configuration. Also set a password for any other user with similar credentials.

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

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

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

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

Other user accounts

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

You can read more about how to create and manage user accounts in the administrator guide for your endoint.

Changing your own system password

Perform the following steps to change the system password.

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

1. Sign in to the web interface with your user name and current password.
2. Click your user name in the upper right corner and choose *Change password* in the drop down menu.
3. Enter the *Current password*, the *New password*, and repeat the new password in the appropriate input fields.

   The password format is a string with 0–64 characters.
4. Click *Change password*.

Changing another user's system password

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

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

Setting the menu password

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

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

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

Note that the menu password, as from software version TC7.0, applies only to the on-screen Administrator Settings menu; it does not apply to the Administrator menu on the Touch 8 controller.

Setting the menu password from the web interface

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

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

Remote control and on-screen menu: Navigate to *Home > Settings > System information*.

Touch controller: Tap the upper, left corner of the Touch controller to open the drop down window. Then tap *Settings > System Information*.

Setting the menu password using the remote control

1. In the on screen menu, go to *Home > Settings > Administrator settings > Set menu password*.

   The password should be a string with 0–255 characters.

   To deactivate the password leave the password input field empty.
2. Enter the menu password in the input field. The password you enter is hidden; each character is replaced with a star (*).

   On the remote control, press the # key to toggle between lower or upper case characters and numbers: abc/ABC/123.
3. Select *Save* to save the changes, or *Cancel* to leave without saving.
4. Press *Home* ( ) to exit.

Setting a root password

You can protect the file system of your video system by setting a password for the root user.

The root user is disabled by default. You have to use the command line interface to enable the root user and set a root password.

Activate the root user and set the password

Perform the following steps to activate the root user and set a password for it:

1. Connect to the system through the network or the system's serial data port (if available) and open a command line interface (SSH or Telnet).
2. Sign in to the system with user name and password. The user needs ADMIN rights.
3. Type the following command:

   ```
   systemtools rootsettings on <password>
   ```

The root password is not the same as the system (admin) password.

CHAPTER 5

APPENDICES

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

About ad hoc conferencing

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

Configuration of Cisco Unified CM is described earlier in this guide. Refer to the *Multipoint Mode* setting in the "Product specific configuration layout" on page 18.

Verifying the setup

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

```
xStatus Conference Multipoint Mode
```

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

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

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

```
xStatus Conference UseBuiltInBridge
```

False: The CUCM ad hoc conferencing mode is used.

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

About shared lines

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

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

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

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

Configuration of Cisco Unified CM is described earlier in this guide. Refer to the *Shared Lines* setting in the "Configuring shared lines" on page 31.

About endpoint provisioning

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

Configuration of Cisco TelePresencce endpoint is described earlier in this guide. Refer to "About endpoint configuration" on page 36 and "Setting up provisioning" on page 39.

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 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.

The TelePresence endpoint user interfaces

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

NOTE: Access through HTTP (web interface) and SSH (command line interface) will be disabled when the endpoint has been succesfully registered to Cisco Unified CM 9.1.1 (using a dev.pack with support for TC6.3).

Using the Touch panel

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

Password protection

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

If the system does not wake up:

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

Finding the IP address

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

Using the remote control

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

Password protection

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

If the system does not wake up:

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

Finding the IP address

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

Using the web interface

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

Signing in to the web interface

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

If you are not able to connect to the system:

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

Using the command line interface

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

Signing in through SSH

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

If you are not able to connect to the system:

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

Collecting log files from a TelePresence endpoint

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

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

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

Downloading one file

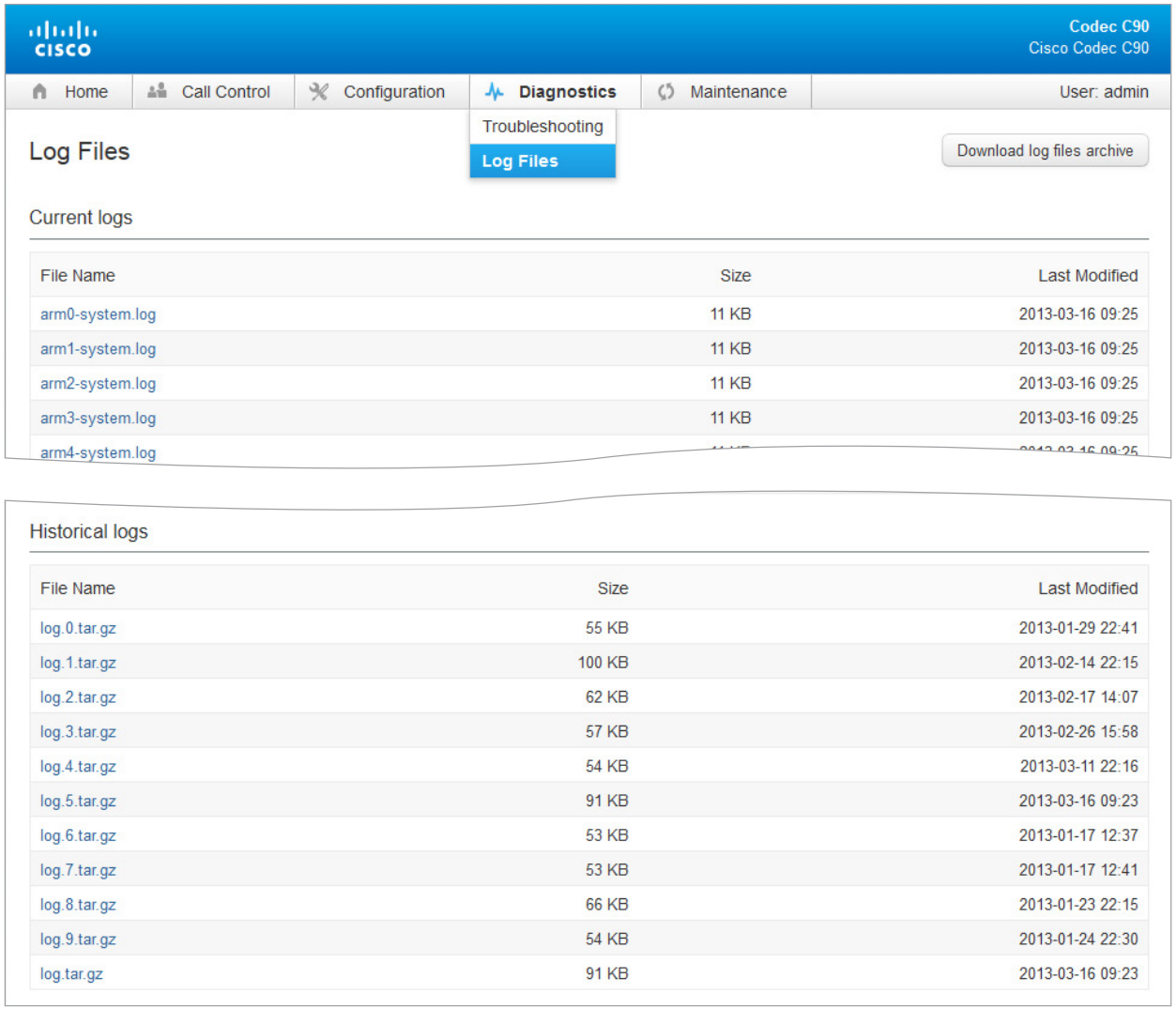
Click on a log file and follow the instructions in the dialog box to save or open the file (left or right click depending on your browser).

Downloading all files

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

How to collect the log files from a TelePresence endpoint.

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



Factory resetting the TelePresence endpoint

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 uploaded to the system will be deleted.
- The Release key and Option key will be preserved.
- Automatic restart of the system.

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

Useful information

Make sure to collect the call logs before factory resetting the endpoint.
Refer to "Collecting log files from a TelePresence endpoint" on page 48.

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

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

Using the Touch panel

1. Tap gently on the Touch 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.

Using the command line interface

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

Using the web interface

1. Open a web browser and enter the IP address of the video system in the address bar.
2. Navigate to *Maintenance > System Recovery > Factory Reset.*

   NOTE: Read the provided information carefully before proceeding.
3. Click *Perform a factory reset.*
4. The system will revert to the default factory settings and automatically restart. This will take a few minutes.

Using the 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.

   NOTE: If you failed to press the power button 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.

Finding the MAC address of the endpoint

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

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

Finding the MAC address on the System Information page

Using the web interface

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

Using the Touch controller

To find the system's MAC address tap *(Settings) > System Information* on the Touch and see the *Hardware* section.

Using the remote control

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

Finding the MAC address using a command line interface

To find the system's MAC address:

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

```
xStatus Network 1 Ethernet MacAddress
```

Finding the MAC address on the rating label

The rating label is found on the physical unit.

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

The rating label is found underneath the codec:

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

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

- Cisco TelePresence System EX60
- Cisco TelePresence System EX90

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

- Cisco TelePresence MX200
- Cisco TelePresence MX300

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

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 is supported on the following endpoints from software version TC5.0, and later: MX200, MX300, EX60, EX90, C20, C40, C60, C90, and Profile series. The SX20 was introduced at a later time and is supported from release TC5.1, and later.

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 its traffic belongs to, placing its traffic into

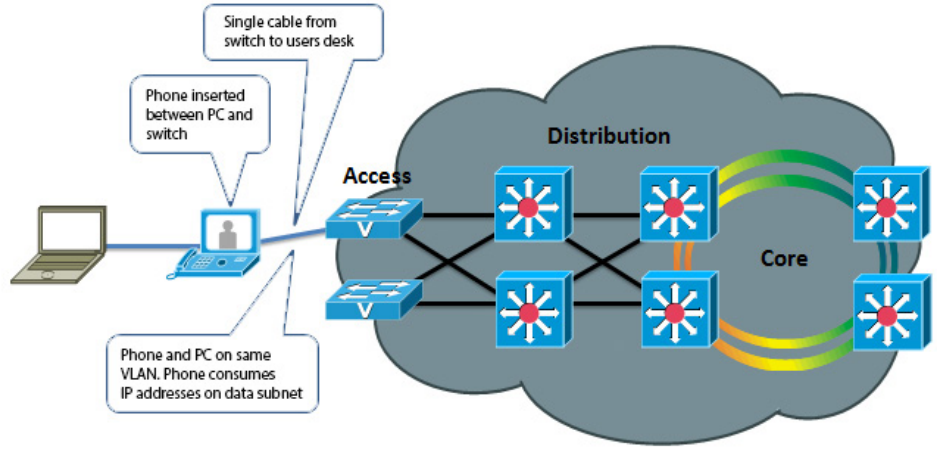


Fig. 1: Without VLANs

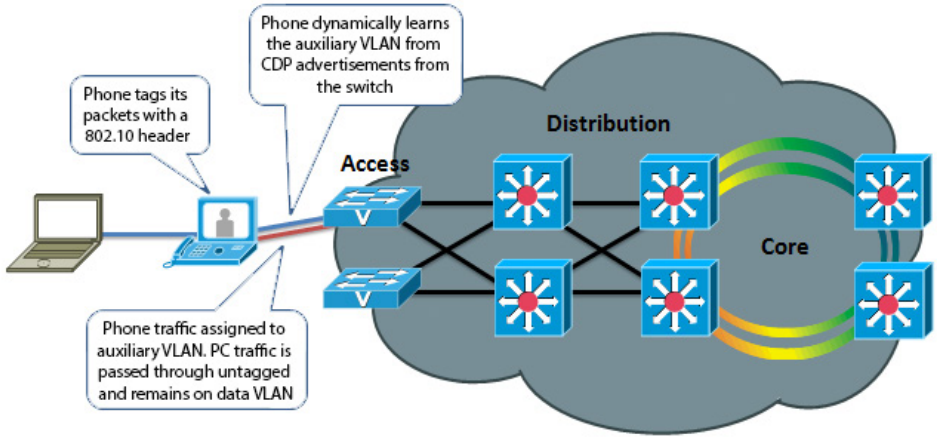


Fig. 2: With VLANs

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:

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 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

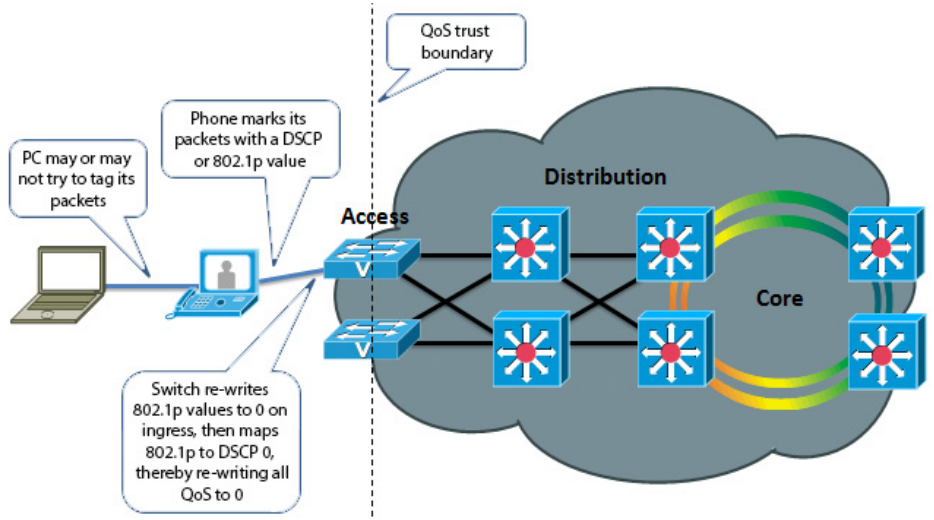


Fig. 3: Without CDP / AutoQoS

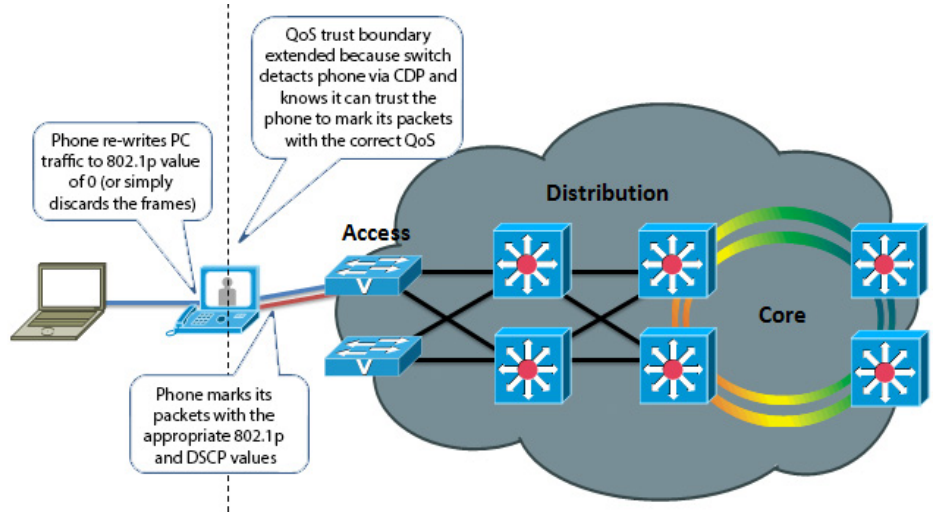


Fig. 4: With CDP / AutoQoS

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

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: Off

The provisioning mode can be set from the Touch 8 using the Startup Wizard, or you can manually set the parameters.

- When provisioning mode is set to *Cisco CUCM*, the *Network VLAN Voice Mode* must be set to *Auto* (the Startup Wizard on Touch 8 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 CM TFTP server.
- When provisioning mode is set to *Cisco VCS* or *WebEx TelePresence*, *the Network VLAN Voice Mode* must be set to *Off* (the Startup Wizard on Touch 8 will automatically set the VLAN voice mode) and the endpoint will not use CDP.

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 Startup Wizard, or by manually setting the parameters.

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 Network VLAN Voice Mode to Auto.

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 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.

Upgrading to TC5/TC6 from a previous release

For existing customers upgrading to release TC5/TC6 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 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.

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:

Collaboration Endpoints
> Smart Desktop Endpoints
> Cisco TelePresence System EX Series

Or click: ▸ www.cisco.com/go/ex-docs

Codec C Series:

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

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

Quick Set C20 and SX20 Quick Set:

Collaboration Endpoints
> TelePresence Integration Solutions
> Cisco TelePresence Quick Set Series

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

MX Series:

Collaboration Endpoints
> Collaboration Room Endpoints
> Cisco TelePresence MX Series

Or click: ▸ www.cisco.com/go/mx-docs

Profile Series:

Collaboration Endpoints
> Collaboration Room Endpoints
> Cisco TelePresence Profile Series

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

Cisco Unified Communication Manager (CallManager):

Unified Communications
> Call Control
> 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

Intellectual property rights

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