CISCO CALL MANAGER (CUCM) GUIDE

How to Install, Configure, and Maintain the Cisco IP Telephony System



Vinicius Buscacio

CISCO CALL MANAGER (CUCM) GUIDE

Vinicius Buscacio

Copyright © 2019 by Vinicius Buscacio

ISBN:
ISBN-13:

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator,” at the e-mail below.

Techbook Publishing
Vinicius Buscacio
http://www.buscacio.net
vinicius@buscacio.net

Ordering Information
Quantity sales. Special discounts are available on quantity purchases by corporations, associations, and others. For details, contact the publisher at the e-mail above.

Warning and Disclaimer
This book is designed to provide information about Cisco Unified Communications Manager. Every effort has been made to make this book as complete and as accurate as possible, but no warranty of fitness is implied.

The information is provided on an as-is basis. The author and Techbook Publishing shall have neither liability nor responsability to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it. The opinions expressed in this book belong to the author and are not necessarily those of Techbook Publishing.

Trademark Acknowledgments
All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Techbook Publishing or Vinicius

Buscacio cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

DEDICATION

To my wife Paula Buscacio without whose sympathy and encouragement this work would never been done.

CONTENTS

Introduction - CUCM
- Cisco Unified Communications Manager
- This book
- My experience

Chapter 1 - Cisco Call Manager History
- Selsius Systems
- A Cisco Company
- First Version from Cisco
- The evolution
- Cisco Call Manager 3.1
- Cisco CallManager 3.3
- Cisco CallManager 4
- From Windows to Linux
- 2007: Cisco Unified Communications Manager 6.0
- From Hardware to Virtual
- 2012 - Cisco Unified Communications Manager 9.0
- 2013 - Cisco Unified Communications Manager 10.0
- 2014 - Cisco Unified Communications Manager 11.0
- 2017 - Cisco Unified Communications Manager 12.0
- CUCM status in 2019

Chapter 2 - CUCM Topologies
- CUCM Publisher x CUCM Subscriber
- Single site
- Multiple sites
- Multiple sites with SRST
- Intercluster Trunk

Chapter 3 - CUCM installation
- Installing VMware ESXi
- NTP Server
- Accessing the VMware vSphere Client
- Preparing the CUCM Publisher Virtual Machine
- CUCM Publisher Installation
- First access

CUCM Subscriber Installation
Start the Services
Chapter 4 - Initial configurations
License Install
Hostname/IP Address
CUCM Groups
NTP Reference
Date/Time Group
Regions
SRST Reference
Device Pool
Enterprise Parameters
Service Parameters
Chapter 5 - Call Permission
What are Partitions and Calling Search Spaces
Creating Partitions
Creating Calling Search Spaces
PT/CSS Examples
CSS on Phones x CSS on Extensions
Inbound CSS to Gateways and Trunks
Default CSS and PT to Auto-Registration
Auto-Registration Default CSS
Auto-Registration Default PT
Troubleshooting PT/CSS problems
Troubleshooting Phone call with DNA
Troubleshooting Gateway/Trunk call with DNA
Chapter 6 - Phones Registration
Power on the Cisco Phone
Voice VLAN x Data VLAN
IP Helper Address
DHCP Server
Creating the Phone on CUCM
Registration Troubleshooting
Chapter 7 - Voice Gateways
H.323 Gateway
MGCP Gateway

SCCP Gateways
Voice Cards and ATAs
ISDN Circuit
R2 Digital Circuit
Chapter 8 - Trunks
SIP Trunks
H.225 Trunks
Intercluster Trunk
Chapter 9 - Call Routing
Call Routing on CUCM
Call Routing Redundancy on CUCM
Call Routing on Cisco Gateways
Call Routing Redundancy on Cisco Gateways
Chapter 10 - Digits Manipulation
Digits Manipulation on CUCM
Digits Manipulation on Voice Gateways
Chapter 11 - SRST
What is SRST Mode?
Configuring SRST Mode
Testing SRST
Verify SRST
Chapter 12 - CUCM Users
Local User
LDAP Synchronized User
Application User
Create an Admin user on CUCM
Chapter 13 - Media Resources
Conference Bridge
Transcoder
Music on Hold
Media Resource Group
Media Resource Group List
Chapter 14 - Features
Pickup group
Hunt Group
Meet-me number

Conference Now
Extension Mobility
Remote Destination
Chapter 15 - BULK Administration
Update Phones using BULK
Export all phones details using BULK
Insert phones using BULK
File Upload
Insert Phone Specific Details
Insert Phone All Details
Chapter 16 - Call Detail Records
Search for call logs
Export CDR automatically to external Billing Server
Chapter 17 - Real Time Monitoring Tool
Install and access RTMT
Basic checks with RTMT
Collecting Traces with RTMT
SIP Call traces on RTMT
Chapter 18 - Backup and Restore
Backup
Restore
External Tools
Chapter 19 – Appendix
Making a non-bootable ISO image bootable
CUCM Database Synchronization Check
CUCM Database Synchronization Recovery
Verify all Extensions created on CUCM
Verify all Extensions created on CUCM but not associated with Phones
Verify if a number exist at any place on CUCM
Insert Phones via BULK with Handheld Barcode Scanner
Verify an T1 or E1 status on the Voice Gateway
Check ISDN Status on a Voice Gateway
Troubleshoot ISDN Status on a Voice Gateway
Display active calls on a Voice Gateway
Troubleshoot calls on a ISDN Gateway
Troubleshoot calls on a R2 Digital Gateway

Troubleshoot calls on a SIP Trunk
Troubleshoot calls on a H.323 Gateway
Troubleshoot calls CUCM
Troubleshoot SIP calls on CUCM
Preparing CUCM MoH File with Audacity
Preparing CUCM MoH File with ffmpeg command
Preparing CUCM MoH File with online sites

INTRODUCTION - CUCM

What is Cisco Unified Communications Manager, formerly Cisco Call Manager?

Cisco Unified Communications Manager

Cisco Unified Communications Manager, or just “Cisco Call Manager” as many people still call it (including myself), is the Core of the Cisco Unified Communications infrastructure; the primary server in a topology for Voice, Video and Unified Communications.

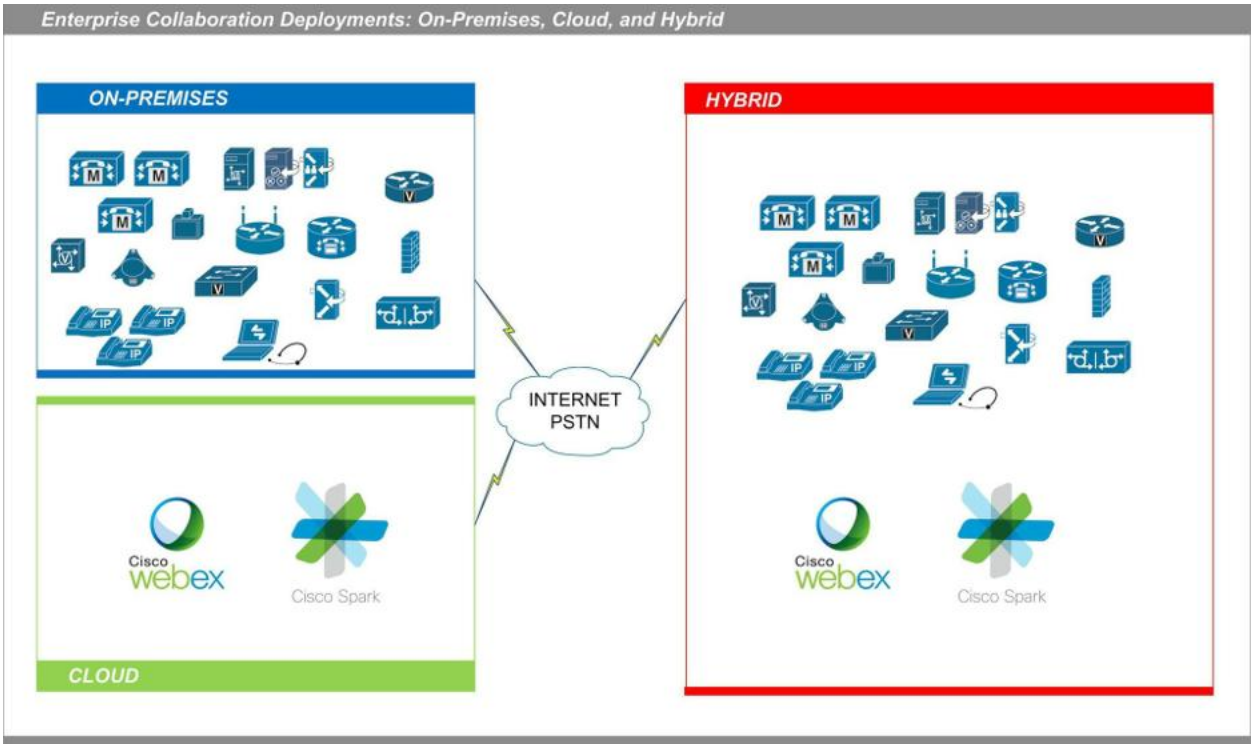


Figure 01 - Cisco Enterprise Collaboration Deployment Models

This topology is based on a robust network infrastructure, as required in an enterprise environment nowadays.

This book

This book will cover the main aspects of a CUCM environment, like

topologies, devices, implementation steps, integrations with PSTN, Cisco Phones requirements and configurations, call permission, digit manipulation, remote site support with SRST, CUCM End Users, Features, Monitoring, Backup, Restore and other relevant information.

My experience

I've been working with Cisco IP VoIP since 2006, installing Cisco 1750 routers with FXO and FXS cards.

The first CUCM implementation I did was in 2007, a CUCM 6.0 in a project with 90 Cisco phones including integration with a Siemens Hipath 4000 PBX, where I used an MGCP E1 with QSIG to connect not only the calls but also features like Calling and Called Name, Callback, and Call Forwarding.

Since then, I have been implementing and supporting almost all CUCM version, starting at Call Manager 3.1 (where we had to restart the Windows Server sometimes when the Music on Hold crashed) on MCS Servers until the newest CUCM versions, with VMware ESXi running on Cisco UCS Servers. I also worked with Cisco Presence/Jabber, Cisco Unity Voicemail, VCS-C and VCS-E Servers, video conference endpoints (SX20, DX Series) and other integrations.

I hope my experience can help you understand the fascinating Unified Communications environment from Cisco.

CHAPTER 1 - CISCO CALL MANAGER HISTORY

It is essential to know where we come from to know where we are going.

Selsius Systems

In 1997, Selsius Systems, a telecommunications company in Dallas, Texas, developed and marketed one of the first IP telephony systems. It was called "Selsius-CallManager".

It was an IP PBX system consisting of:

- Ethernet phones
- a server-based call control application
- Voice over IP gateways
- Voicemail system
- Automated attendant console
- Softphones

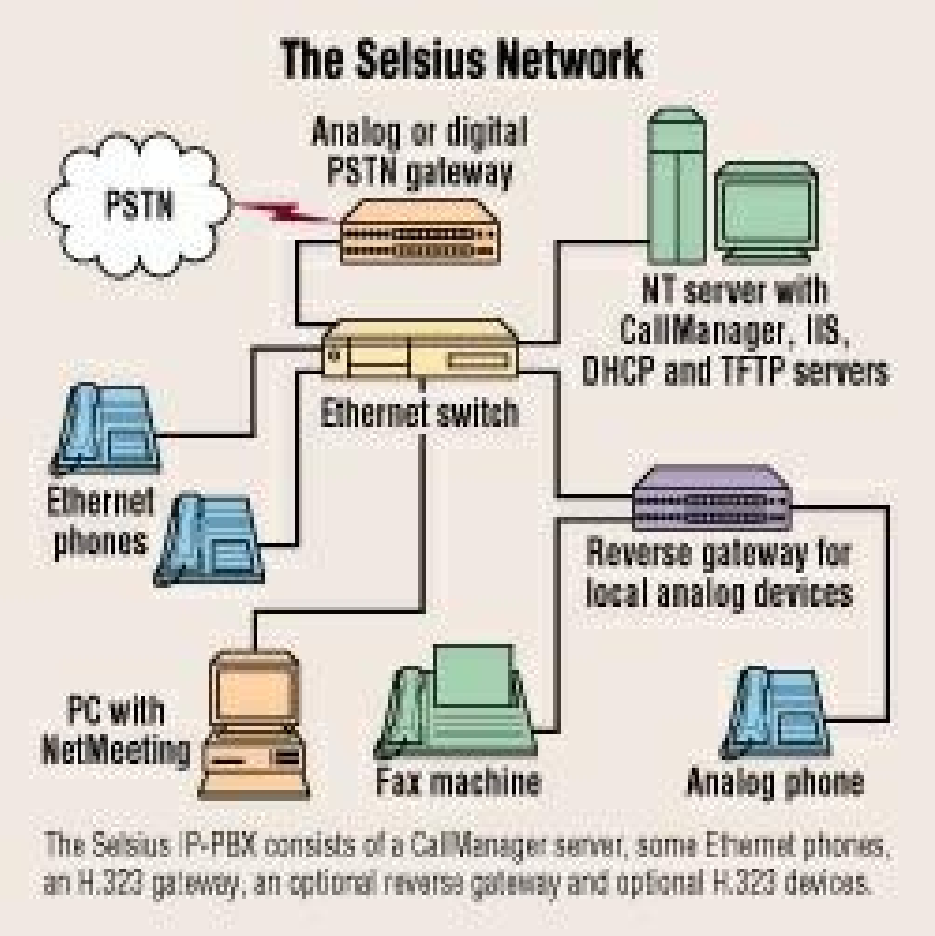


Figure 02 - The Selsius Network Topology

The Selsius-Manager was running on Windows NT, with IIS, DHCP and TFTP servers included. The SCCP protocol was used to control phones.

Phones were called “Selsius Ethernet Phones”, and they decided to use the letters “SEP” + the MAC Address of the phones as identifiers. Therefore, until today, Cisco Phones uses names like “SEP0020E7F24007”.



Figure 03 - Selsius Ethernet Phone

Also, it was possible to use Microsoft Netmeeting (software that came with Windows 95/97) as an H.323 client.



Figure 04 - Microsoft Netmeeting

Selsius-CallManager 2.0 was released in 1998. Then, Cisco buys Selsius.

A Cisco Company

In October 1998, Cisco bought Selsius systems for US$ 145 million.



The New York Times

ARCHIVES 1998

COMPANY NEWS; CISCO AGREES TO BUY SELSIUS SYSTEMS FOR $145 MILLION

By DOW JONES OCT. 15, 1998

The networking giant Cisco Systems Inc. has agreed to acquire Selsius Systems Inc., a maker of switches that route phone calls over company intranets, for $145 million in cash and stock. Costs associated with the deal will lower second-quarter earnings by 3 to 6 cents a share, Cisco said. Cisco, based in San Jose, Calif., has annual revenue of $8.46 billion. Selsius, a privately held company based in Dallas, was sold by the Intecom Inc. unit of Lagardere S.C.A. of France.

Figure 05 - NY Times - Cisco buy Selsius, October 1998

From this point, Cisco started to work faster to increase the Call Manager development.

First Version from Cisco

In 2000, Cisco released its first Call Manager version, “Cisco Call Manager 3.0”. Clustering was introduced at this time, and MGCP support was added.



Figure 06 - Cisco Call Manager 3.0 screen

As the system was basically a Windows Server 2000, the following had to be installed manually:

- Microsoft Windows 2000 Server;

- Microsoft SQL Server 7.0 Standard Edition, Service Pack 2;
- DC Directory 2.4;
- and finally, Cisco CallManager Release 3.0.

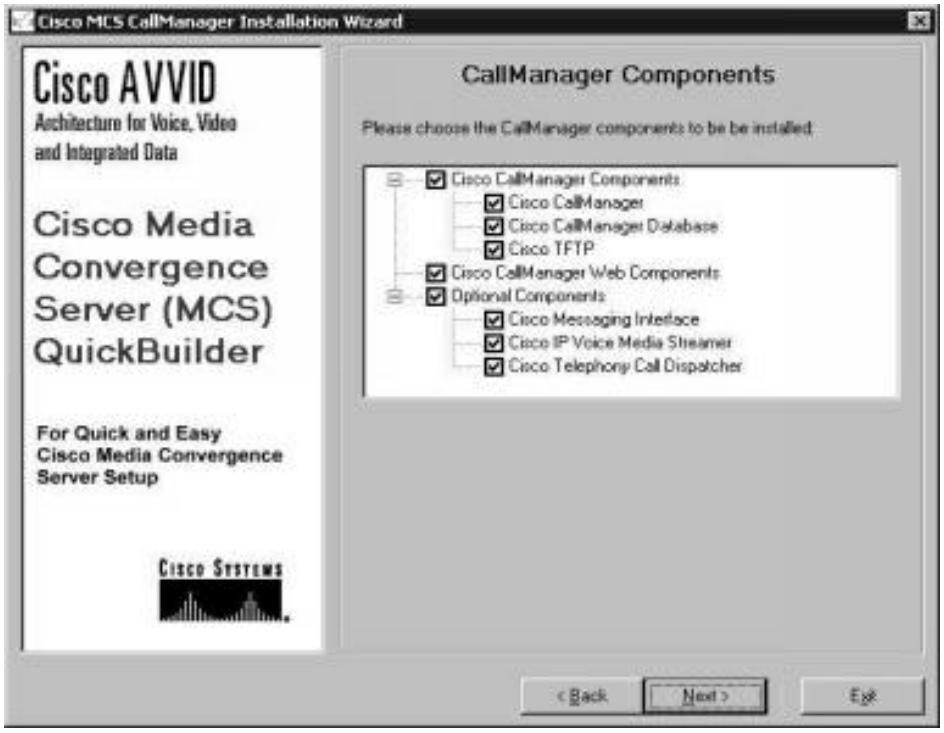


Figure 07 - Cisco AVVID installation

As the server was a regular Windows Server (despite the information that it was a "special, limited edition of Windows 2000, intended for use with Cisco CallManager only"), the documentation contained some warnings like this:

> **Caution:** Be aware that installing or using **Netscape Navigator** on the Cisco CallManager server can cause severe performance problems. Cisco strongly recommends against installing Netscape Navigator or any other application software on the Cisco CallManager server.

Warnings like this nowadays look bizarre. Indeed, many people used “third-party software” on Call Manager servers, like Microsoft Office.

The evolution

After the first Cisco version of the Call Manager, the development of new business functionalities started to grow faster. Each new version released, new updates and features including productivity tools were added.

Cisco Call Manager 3.1

In 2001, Cisco released “Cisco Call Manager 3.1”. This CallManager release was built on the 3.0 release, supporting more gateway devices, IP phones, and features, including:

- Music on hold (MOH)
- Support for digital interfaces on [MGCP] gateways
- Added support for XML and HTML applications in Cisco IP Phones
- Extension mobility
- Call preservation between IP phones and MGCP gateways
- TAPI (Telephony Application Programming Interface) is introduced

Same year, Cisco released “Cisco Call Manager 3.2”.



Figure 08 - Cisco Call Manager 3.2 screen

There were many enhancements on the Cisco CallManager 3.2:

- more scalable, distributable, and highly available enterprise IP telephony call-processing solution.
- Multiple Cisco CallManager servers are clustered and managed as a single entity
- Client user interface internationalization and localization
- Auto-answer at destination IP phone's speaker, enabling hands-free intercom service
- H.323 performance improvement, enabling 1000 H.323 calls per server in a cluster
- Cisco Analog Telephone Adapter, ATA-186 integration
- MGCP protocol extensions, including T1/E1 PRI and T1-CAS (E&M)
- Drop last conference party
- Web Attendant consult transfer
- Message Waiting Indication (MWI) enhancements

Cisco CallManager 3.3

Cisco added even more features to version 3.3:

- QSIG support
- IP Manager/Assistant (IPMA)
- Scalability to 30,000 phones per cluster
- Improved H.323 features and support
- Support for multiple H.323 gatekeepers

Cisco CallManager 4

The following years, Cisco kept improving the Call Manager, still running on top of Windows Servers. In Call Manager 4.0, released in 2004, customers were pleased with a number of new features. Previously, IP phones were restricted to only 2 calls per any given line appearance. This restriction was eliminated, and IP phones now had a user configurable maximum (up to 200) number of calls per line appearance.

Some new features and enhancements added during this release were:

- Hunt group
- Privacy for shared lines
- Call barge
- Improved security with media encryption between phones
- Multi-Level Administration (MLA) allowed delegated administration
- Direct transfer allowed user to select two calls from the same line and connect them together
- Call join allowed users to select several calls from a line and conference them together
- Additional QSIG features added



Figure 09 - Cisco Call Manager 4.0 - Phone configuration screen

In 2004, the Cisco Call Manager 4.1 was released. Two years later, in 2006, version 4.2. This version, however, was released with the name change, as the “Cisco Unified Call Manager 4.2”.

From Windows to Linux

Released in 2006, Cisco Unified Call Manager 5.0 was the first version running on Linux. The system was much more straightforward, as there was a single installation procedure to install the operating system and all necessary software as a simple appliance like we have today.

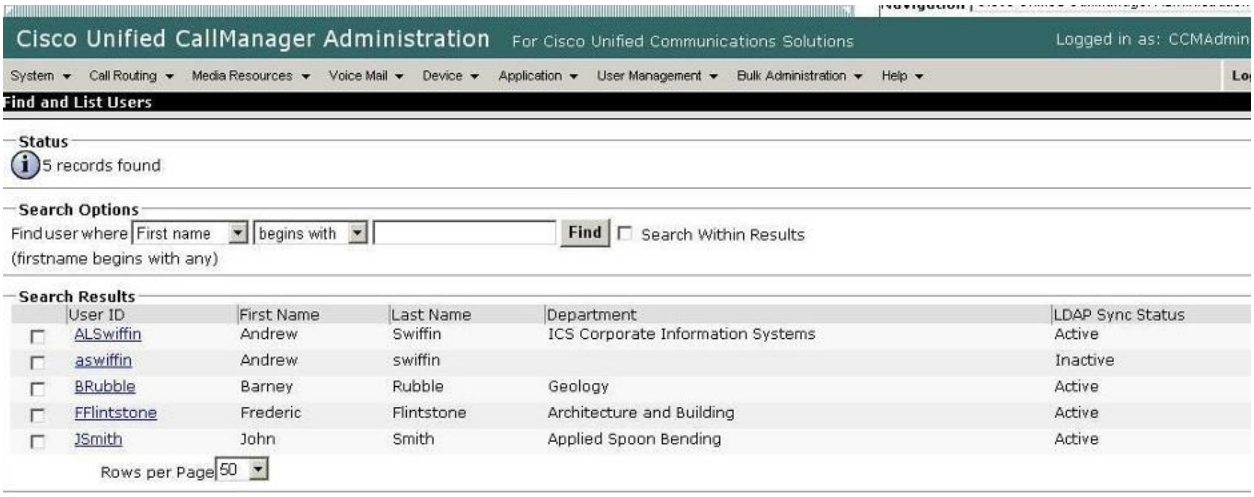


Figure 10 - Cisco Call Manager 5.0

It was also the first version with support to SIP endpoints.

2007: Cisco Unified Communications Manager 6.0

In 2007, Cisco renamed the product for the last time, now to "Unified Communications Manager" (CUMC). Starting with this version, Cisco Unified Communications Manager does not support Windows platform anymore. Furthermore, we have the same visual as we have on modern versions today (or at least until CUCM 12).

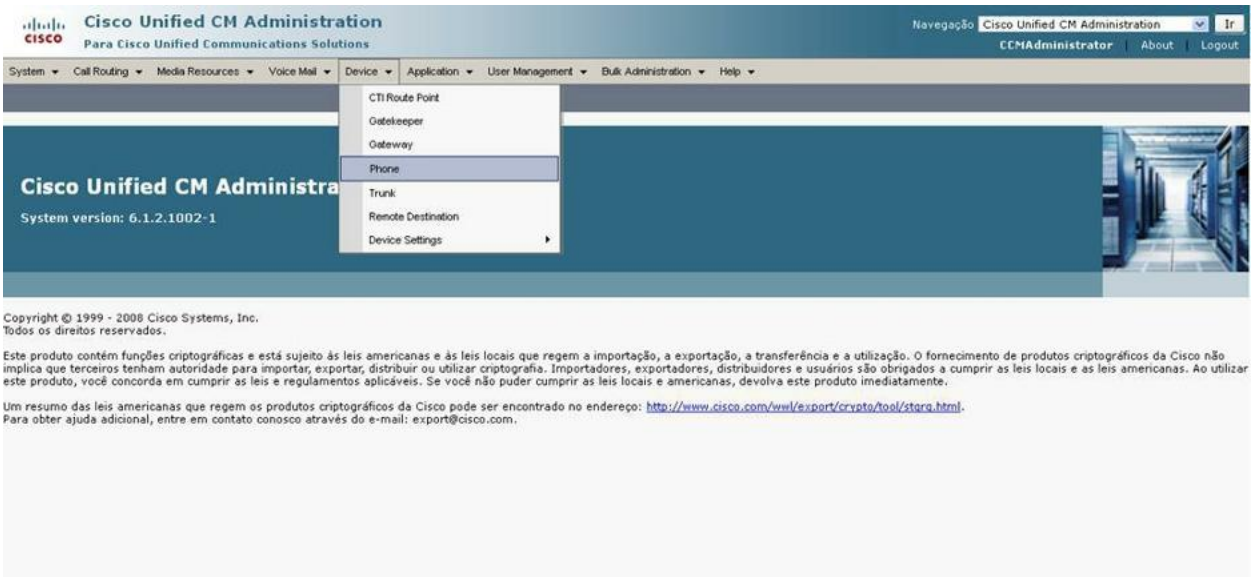


Figure 11 - Cisco Call Manager 6.0

In 2008, Cisco released the "Cisco Unified Communications Manager 7.0".

This version was supposed to have Windows and Linux version, but the Windows version was canceled.

Here, Cisco did a unification of “7.0” line, where servers like Unity and Presence “jumped” directly to version 7.0 from 2.0, to match the CUCM (CUCM 7.0 - Unity 7.0 - Presence 7.0).The system database was changed to IBM Informix.

From Hardware to Virtual

In 2010, the CUCM 8.0 was the first version to support virtualization on VMware ESXi - at that time, version 4.0. This was a significant change in the CUCM environment because from this point on, all CUCM servers started gradually to support only virtualized systems. The MCS servers were abandoned, and all hardware was now Cisco UCS Servers.

On CUCM 8.0, it was also added the IPv6 Support.



Figure 12 - Cisco UCS Server

2012 - Cisco Unified Communications Manager 9.0

- Improvements to SIP Phones, especially for third-parties

2013 - Cisco Unified Communications Manager 10.0

- Better encryption
- Video on Hold

2014 - Cisco Unified Communications Manager 11.0

- Native Call Queuing

2017 - Cisco Unified Communications Manager 12.0

- actual version (Jan 2019)

CUCM status in 2019

According to Gartner Report 2018, Cisco is still the leader on the Unified Communications.



Figure 13 - Cisco Gartner Report

Cisco's UC solutions are available from resellers globally. These solutions represent an attractive proposition for midsize, large and multinational corporations requiring strong voice, video or conferencing capabilities. –
Gartner Report - Magic Quadrant for Unified Communications, Published 25 July 2018

The CUCM is used in large global companies, but also to midsize business looking for a very flexible and professional phone system with integrated collaboration infrastructure for voice and video calling.

Cisco is still improving the system, now including cloud integrations to the regular on-premises system.

CHAPTER 2 - CUCM TOPOLOGIES

Understand the topologies possibilities and limitations is essential to having a stable and scalable system.

CUCM Publisher x CUCM Subscriber

The first thing to understand on a CUCM topology is that there are two servers roles: Publisher and Subscriber:

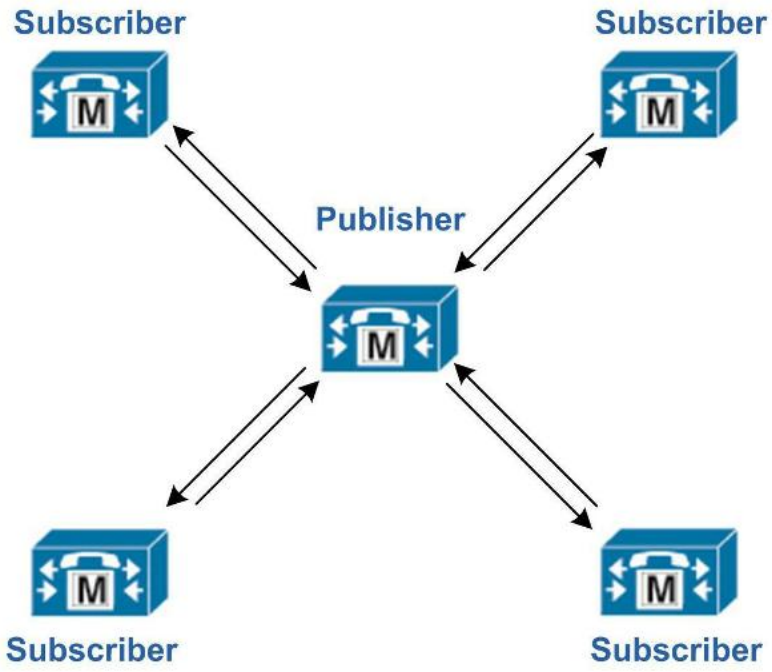


Figure 14: CUCM Publisher and Subscriber Synchronization

The Publisher is the primary server. It is the only one with read and write permissions on the System Database, and there is only one Publisher on each CUCM Cluster.

The Subscriber is the secondary server. Each Subscriber has a local copy of the CUCM Publisher database and has only read access to it. You can have

more than one Subscriber Server on each cluster (actually, you can have up to 8).

Functionality	CUCM Publisher	CUCM Subscriber
Can write data on the system database?	Yes	No, it needs Publisher communication to any database change
How many can be available on a Cluster?	1	from 0 up to 8
Can register Phones?	Yes	Yes
Can process calls?	Yes	Yes
Can provide Phones with TFTP Services?	Yes	Yes
Can register Voice Gateways?	Yes	Yes
Can provide Music on Hold?	Yes	Yes
Can provide Advanced Services?	Yes	Yes
Can provide Extension Mobility?	Yes	Yes
Can be used to manage the system?	Yes	Yes
Have a copy of all system database?	Yes	Yes

Table 1: Publisher and Subscriber comparison

As you can see on this table, the only difference between CUCM Publisher and Subscriber is that only Publisher can write data on the system database. All other functions are available on both servers.

When you create a phone on a Subscriber web page, in the background, the Subscriber is contacting the Publisher and sending him all the information he needs to write this change on the Database. Then, all Subscribers receive a copy of this new information, including the Subscriber which started this process.

When your Publisher server is down, it’s not possible to change system configurations, like creating a new phone or updating a user line. There are

only minor databases changes allowed during a Publisher outage, like registering an Extension Mobility change (if correctly configured), but as a general rule, no changes on the database are available until the Publisher came back online. The Publisher always has the "correct" database in a CUCM system. If at any point there is a Subscriber with a database version higher than the Publisher, you'll have a database problem and your system will not work correctly until you solve this (check this book Appendix to see how to solve this problem).

Single site

If you have a single site, all you need is a Publisher server, a PoE Switch, the Cisco Phones, and a Voice Gateway to connect to the PSTN.

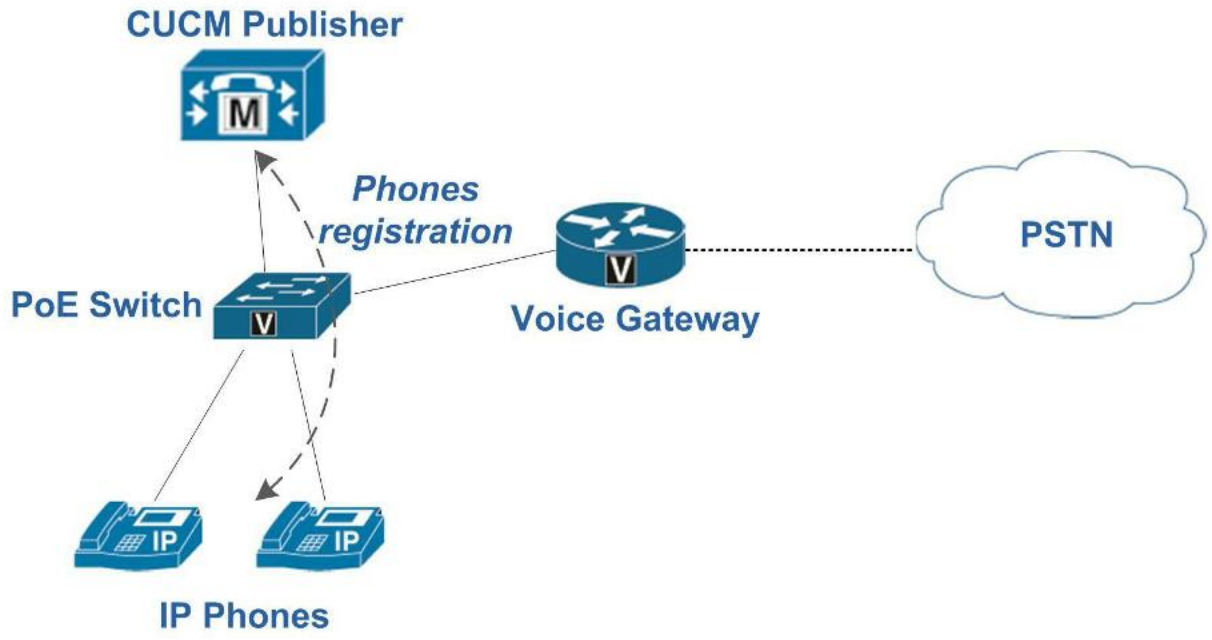


Figure 15: Phones registered on CUCM Publisher

However, depending on how many phones you have on your environment, it can be a good idea to create a Subscriber on this site to have redundancy for a hardware failure.

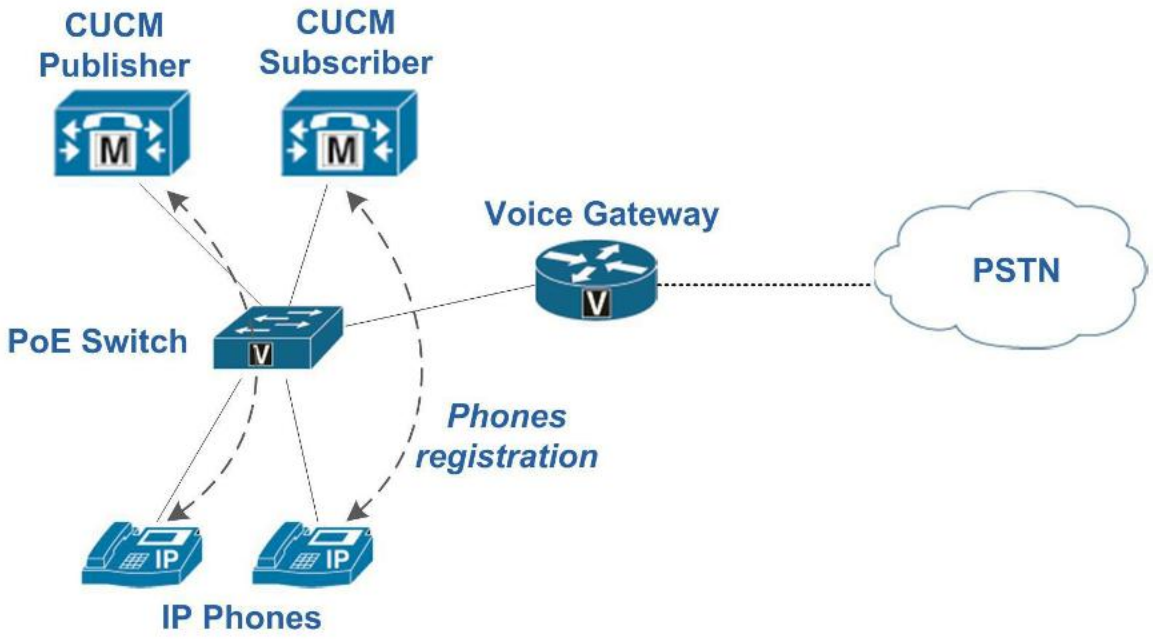


Figure 16: Phones registered on CUCM Publisher and Subscriber

On the other hand, if you have a small environment, you can have a Call Manager Express solution, where your Cisco router can act as an IP PBX system with basic functionality. The Phones register itself directly on the router.

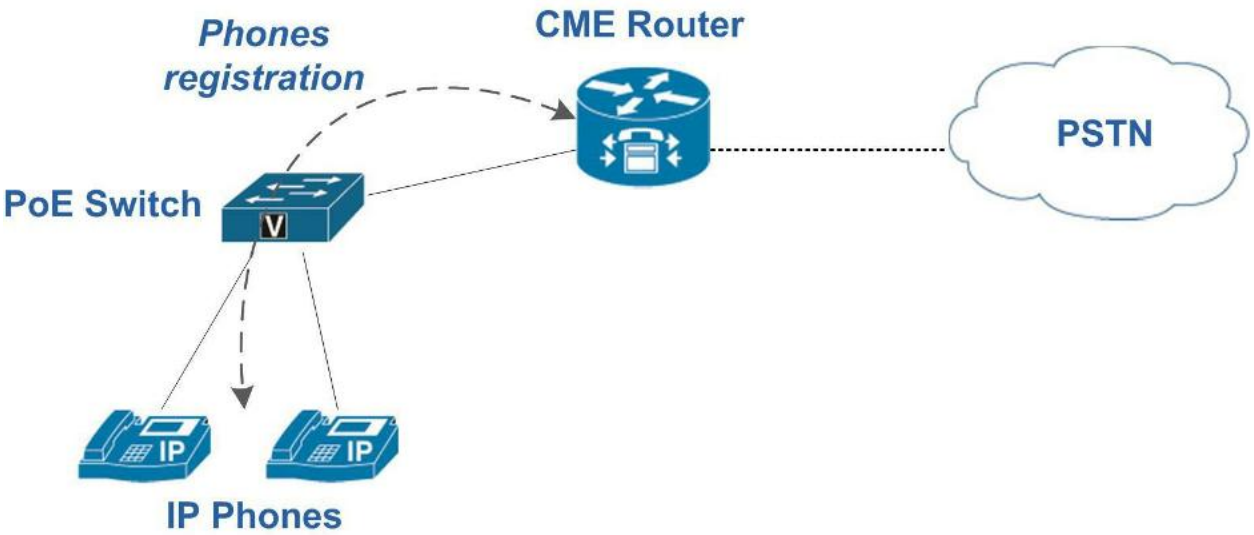


Figure 17: Phones registered on CME Router

Despite being an “Express” system, it can support up to 450 phones, depending on your hardware model. The hardware available to support Phones are:

Multiple sites

When you have multiple sites connected via WAN or VPN, you can have a local CUCM Subscriber server on the remote location, processing all local calls and phones registration, and using the WAN/VPN to synchronize the CUCM Database with the CUCM Publisher.

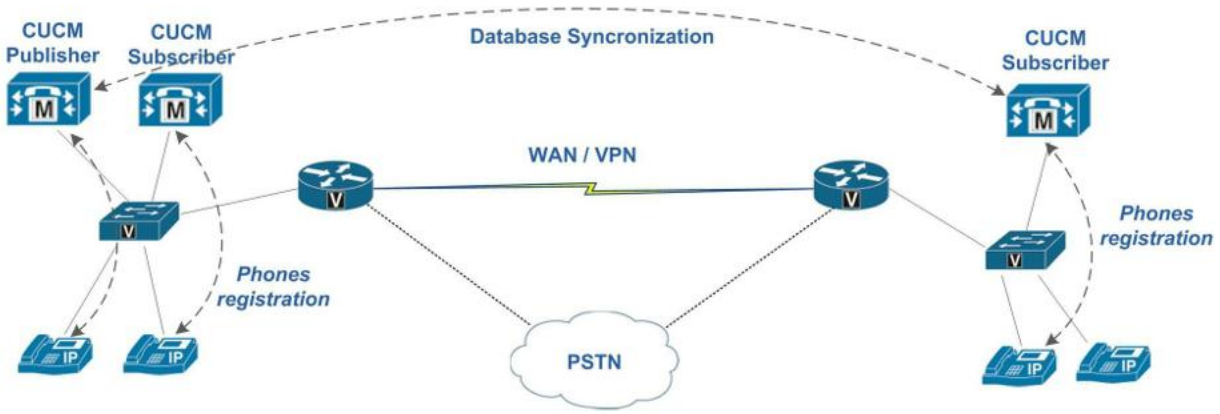


Figure 18: Phones registered on CUCM Cluster via WAN/VPN

On this topology, when you have a WAN/VPN failure, you cannot make any CUCM changes on the remote CUCM server until the link with CUCM Publisher is back online.

Multiple sites with SRST

Another possibility is to use the functionality Cisco Unified Survivable Remote Site Telephony, or just SRST. It enables the local router to act as a Telephony system during a WAN failure and register the phones, providing temporary support for these remote phones.

On this topology, the normal situation is to have the Remote Phones registered on the CUCM Cluster via WAN/VPN.

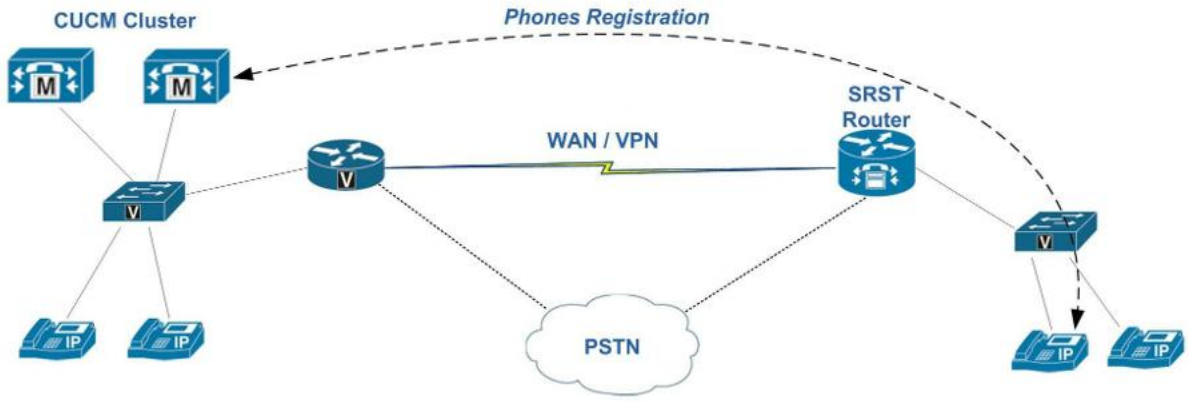


Figure 19: Phones registered on CUCM Cluster via WAN/VPN

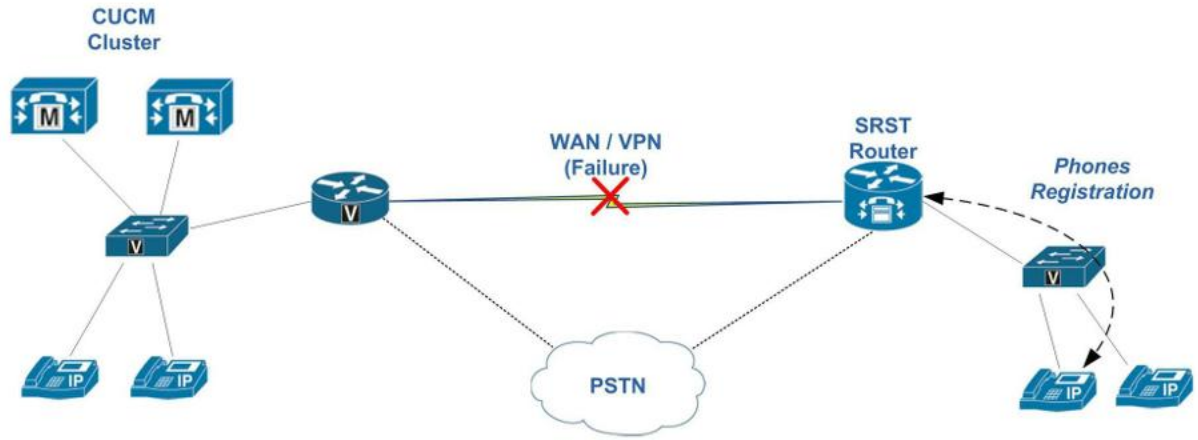


Figure 20: Phones registered on CME on WAN/VPN Failure

We will discuss SRST in chapter 11.

Intercluster Trunk

Intercluster Trunk is used to connect different CUCM Clusters via VoIP. These Cluster can be from different companies or the same company with huge IP Telephony systems.

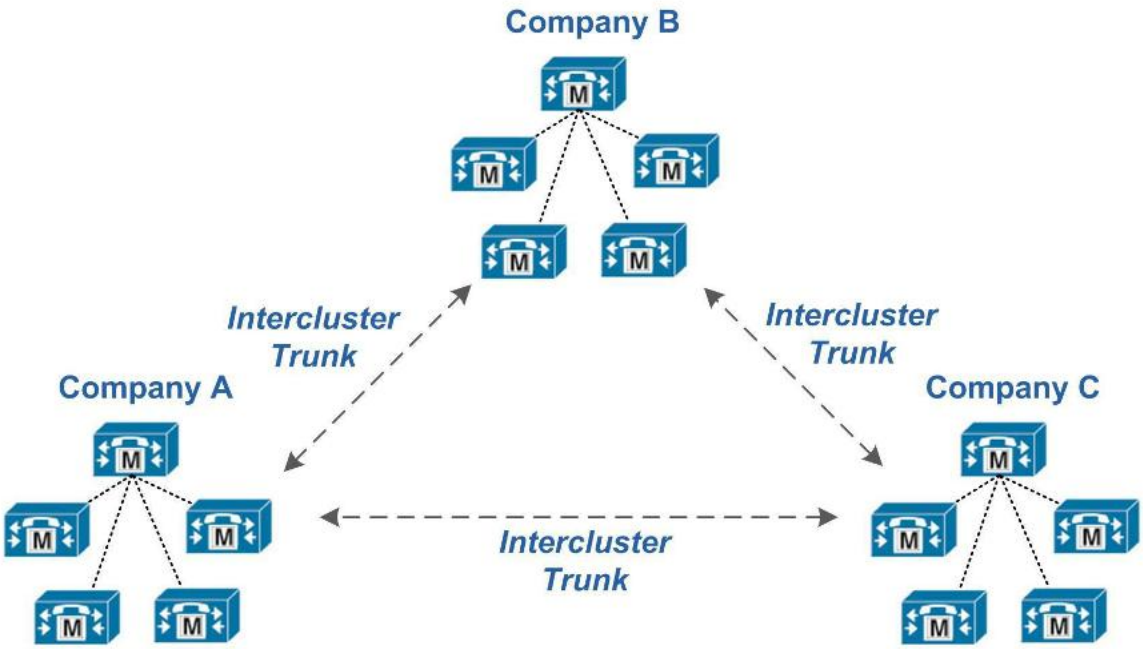


Figure 21: Intercluster Trunk

This Intercluster Trunk can be done via:

- SIP Trunk
- Intercluster Trunk (Gatekeeper Controlled)
- Intercluster Trunk (Non-Gatekeeper Controlled)

These trunks can be used to route voice and video calls. We will discuss these Trunks in chapter 8.

CHAPTER 3 - CUCM INSTALLATION

The CUCM installation is simple; it's just necessary to follow the steps needed; the most important thing is to have a good NTP Server available.

Installing VMware ESXi

As we saw in the first chapter, Cisco now delivers the CUCM server on its hardware, Cisco UCS Series. The server comes with VMware ESXi pre-installed and with all ISO files pre-loaded. Also, virtual machines like CUCM, CUC, CUP, and others come pre-installed, just needing to power on the virtual machines and proceed to the network configuration (Hostname, IP address, etc.).

> **Note:** If you're accessing a Cisco UCS server, ignore these steps below and go directly to the next session, "Connecting to the Network."

If you're planning to have your lab to install CUCM to test, you'll need to install a VMware ESXi on your server. You can get a free copy of Free vSphere Hypervisor on the vmware.com website. Check if your server is on the Hardware Compatibility List. As an example, I have a small Dell PowerEdge T110 II with 24GB RAM.



Figure 22: my small Dell PowerEdge T100 II Server

This server is enough to run six virtual machines like Call Manager, Unity, and Presence (for lab purposes only).

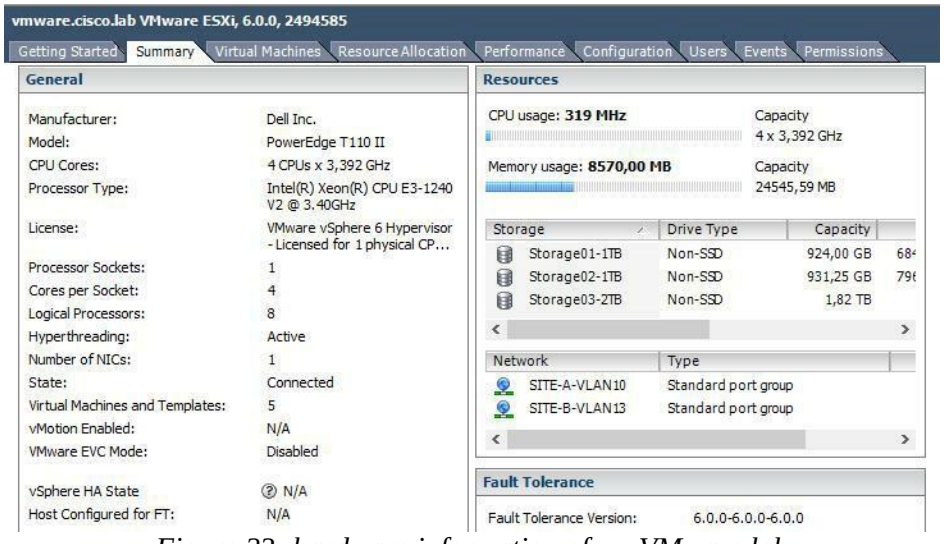


Figure 23: hardware information of my VMware lab

To install VMware ESXi on your lab, download the ISO file from VMware,

burn it on a CD, insert it on your server and follow the installation instructions.

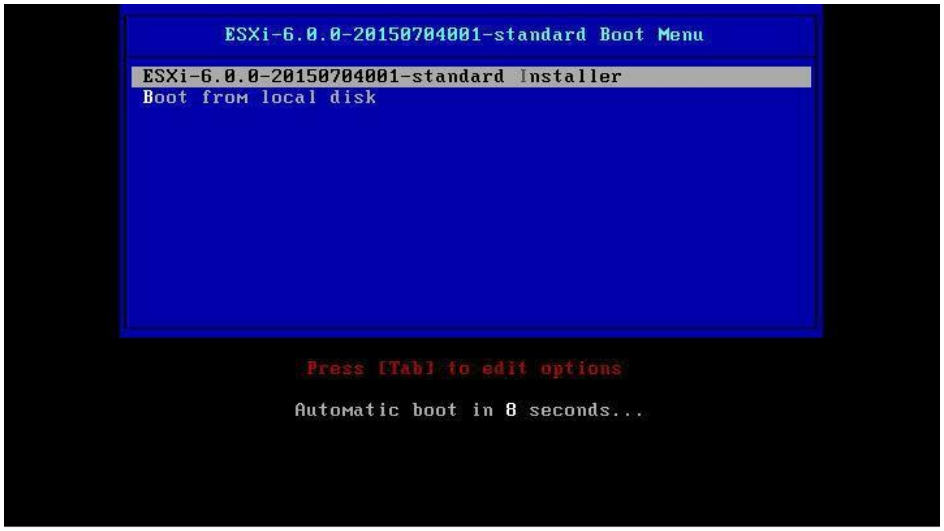


Figure 24: VMware ESXi 6.0 installation process

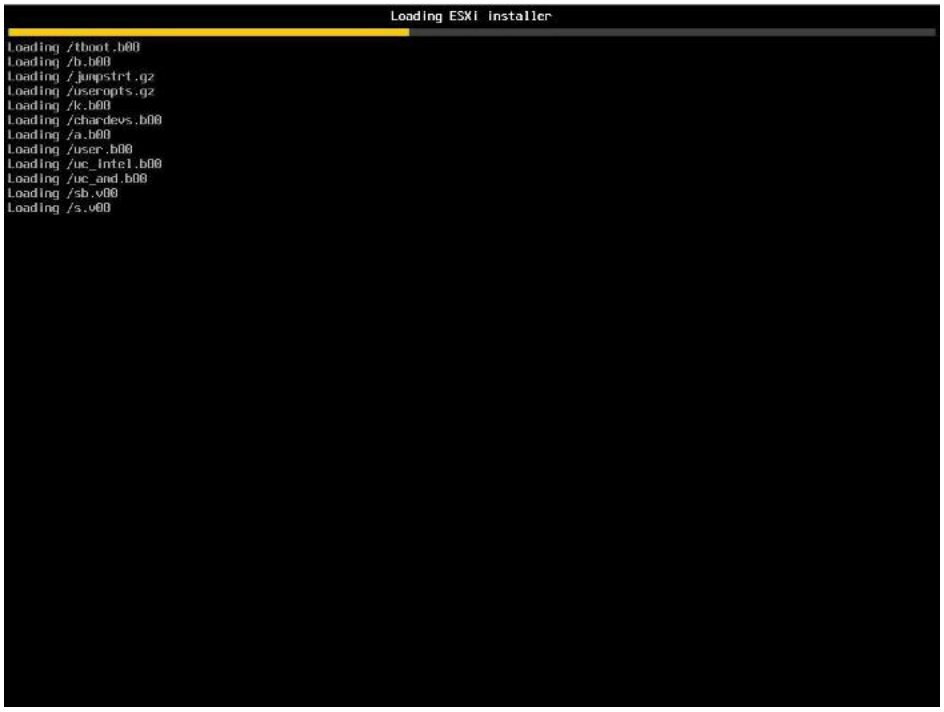


Figure 25: VMware ESXi 6.0 installation process



Figure 26: VMware ESXi 6.0 installation process

Here, press “Enter” to proceed.



Figure 27: VMware ESXi 6.0 installation process

Now, press F11 to accept the EULA.

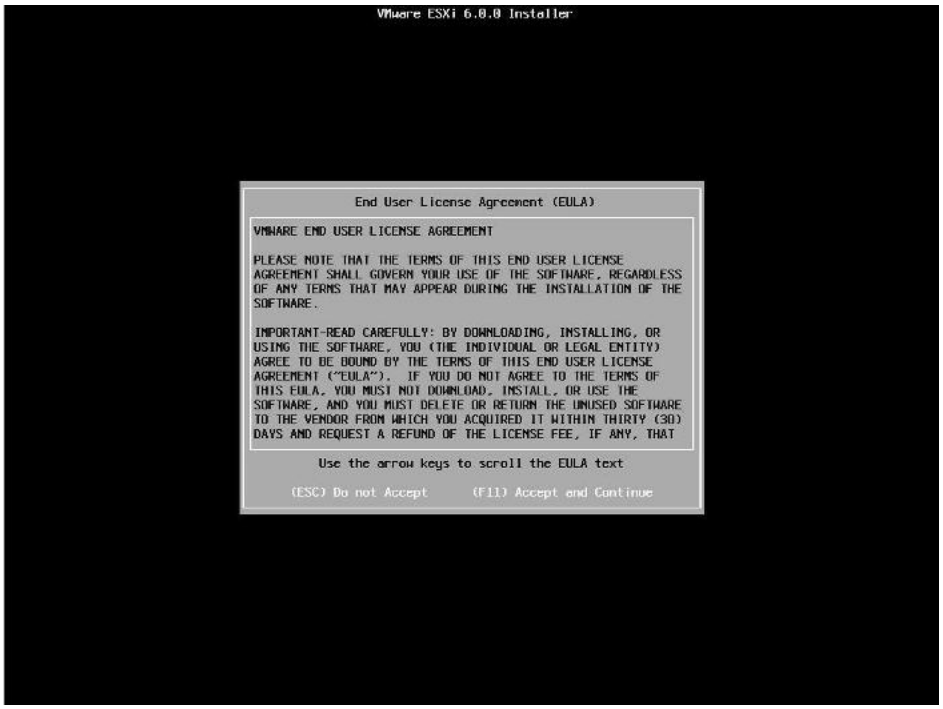


Figure 28: VMware ESXi 6.0 EULA

Select the disk you want to install the VMware ESXi operating system.



Figure 29: VMware ESXi 6.0 Installation disk selection

Select your keyboard layout.

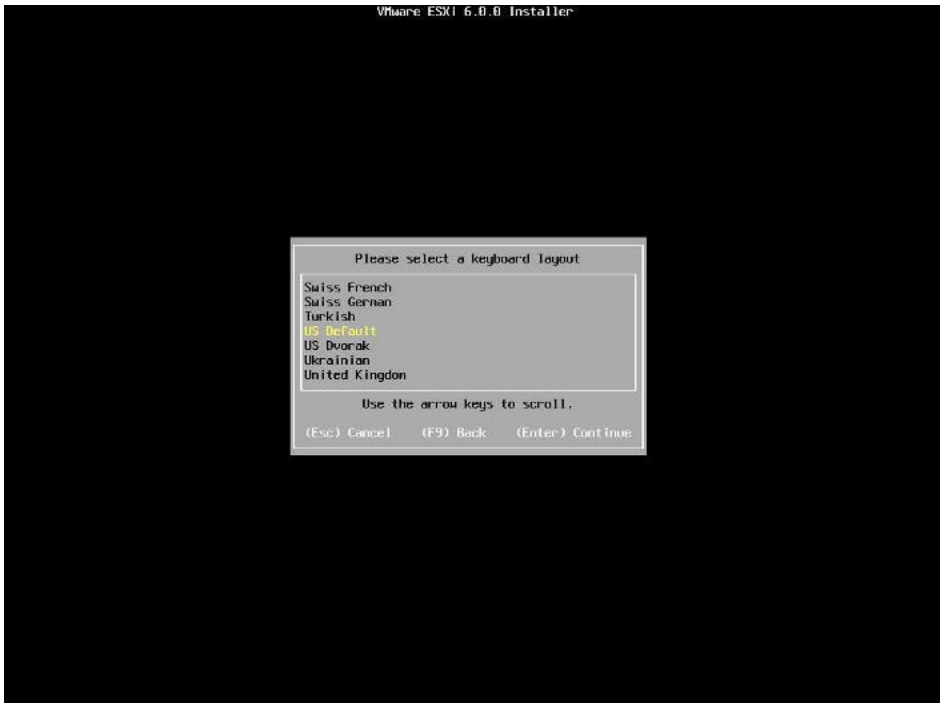


Figure 30: VMware ESXi 6.0 Keyboard Layout selection

Then, create your “root” password.

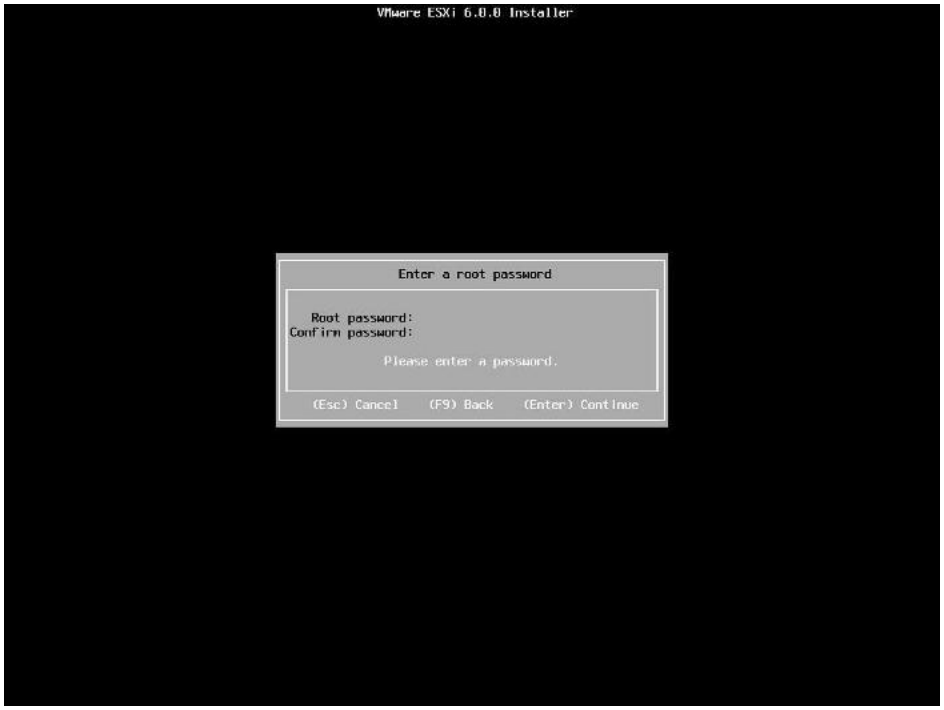


Figure 31: VMware ESXi 6.0 Root Password creation

The installation process will continue.



Figure 32: VMware ESXi 6.0 Installation process

After some minutes, the installation will finish.



Figure 33: VMware ESXi 6.0 Installation completed

The VMware ESXi will boot with a 60 day temporary license. After, you can

access the system via vSphere Client and activate the license you received from VMware when you were downloading the ESXi server at their site.

Connecting the EXSi Server to the network

To connect your VMware ESXi to your network for the first time, you'll need to connect a keyboard, mouse, and monitor to complete the initial network setup. Connect to the server, and you'll see the VMware console screen:

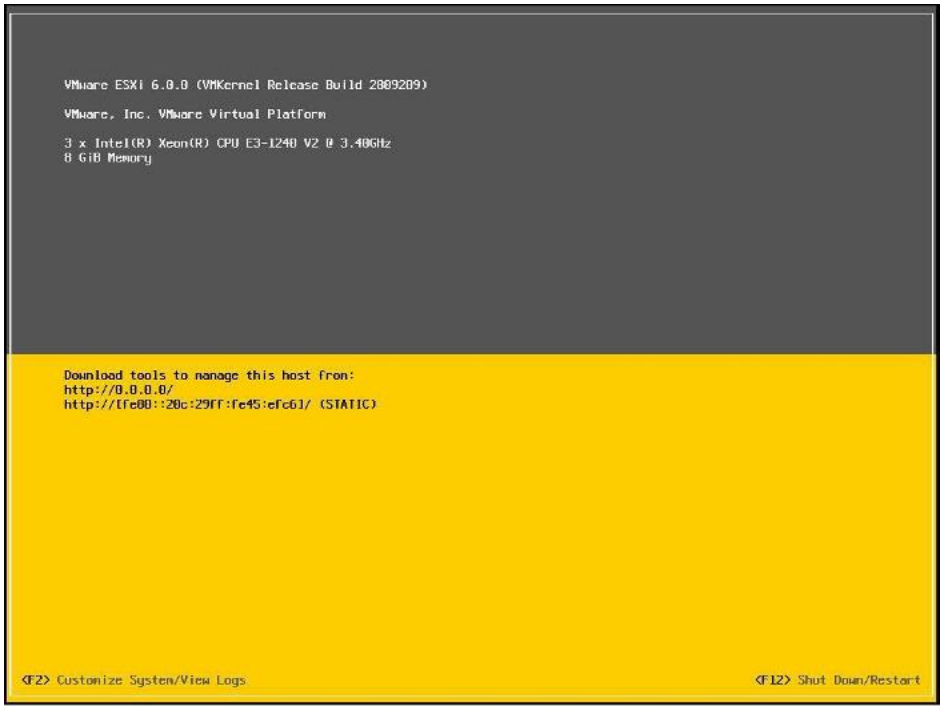


Figure 34: VMware ESXi 6.0 console access

Press F2 to customize the system, and you'll be prompted for the username and password. The default username is "root"; type the password you created during the installation process.

If this is a Cisco UCS Server, the default password to the "root" user is "password". If this doesn't work, check your product documentation.

Then, on the next screen, select "Configure Management Network".

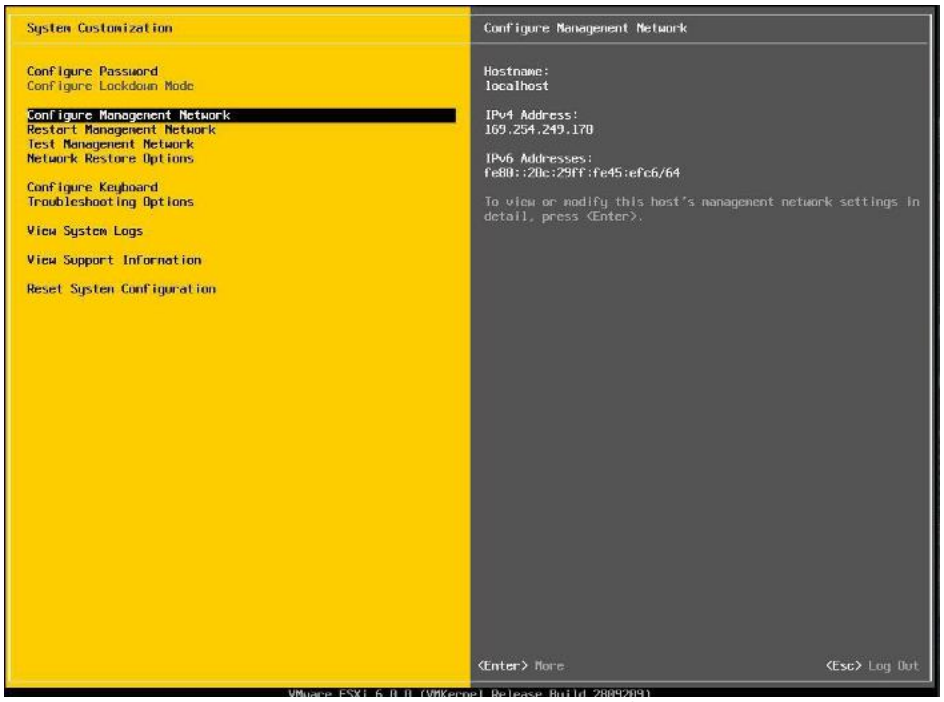


Figure 35: VMware ESXi 6.0 network configuration screen

Now, select the IPv4 Configuration.



Figure 36: VMware ESXi 6.0 IPv4 configuration screen

Finally, select "Set static IPv4 address and network configuration" (use the Spake key to select it); type the IP Address, subnet mask and default

gateway, and press Enter to confirm.

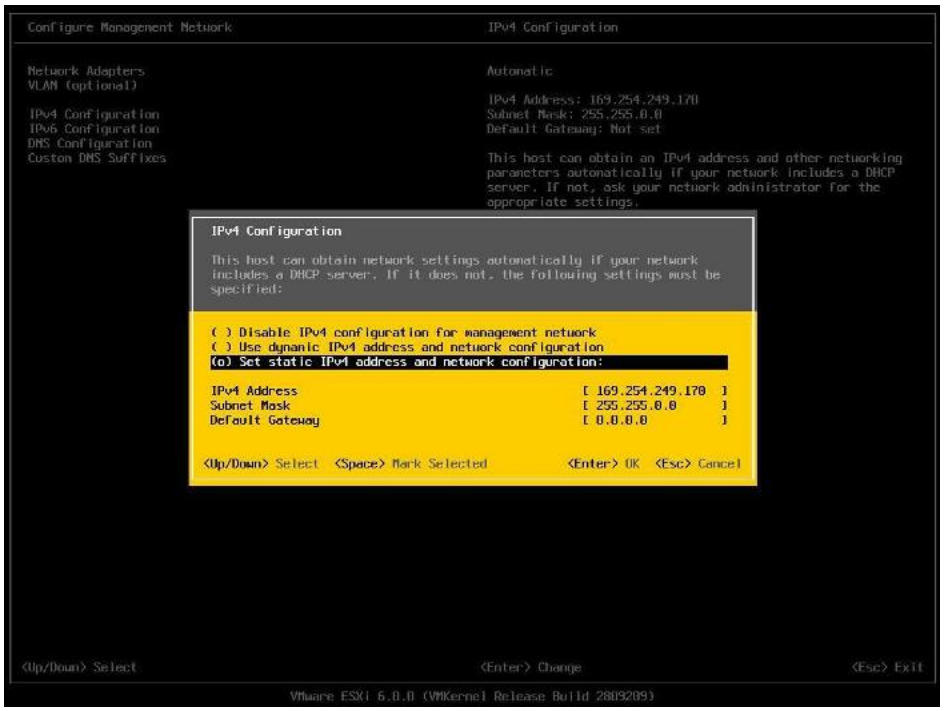


Figure 37: VMware ESXi 6.0 IPv4 configuration screen

After your network configuration is ready, you can proceed to the next step and access your VMware ESXi web page, where you'll find the download link for your VMware vSphere Client.



Figure 38: VMware ESXi 6.0 Welcome page

Click on the link "Download vSphere Client for Windows" to download it from vmware.com Website. The download size is at about 370 MB on

version 6.0. After the download, install it, and you'll be ready to manage your VMware ESXi Server.



Figure 39: VMware vSphere Client installation wizard

This is a very basic "Next/Next/Finish" process, select the installation folder, and you're done.

NTP Server

The next step is to provide an NTP server on your network, or at least provide network access to an NTP server available on the internet.

Usually, I use a Cisco Router or Switch with Internet access to have a good NTP Server locally. If your network provides direct internet access with a basic NAT configuration on your Firewall, with no port blocking, point your Cisco device to an NTP server online (I recommend https://www.ntppool.org/en servers).

However, if your Internet Firewall is blocking all non-authorized Internet access, you'll probably need to allow the TCP traffic on port 123 explicitly, as the NTP protocol uses this. Ask your firewall support team to enable it.

After your firewall passes NTP traffic, the Cisco configuration is straightforward. Follow the commands you'll need to use:

```
ntp server 0.pool.ntp.org
ntp server 1.pool.ntp.org
ntp server 2.pool.ntp.org
ntp server 3.pool.ntp.org
```

If your device doesn’t have access to a DNS server to resolve these names, you can ping these hostnames on your computer and type directly the IP Address instead of the FQDN. You can also use an NTP server you prefer, but if you don’t have any other available, I recommend this Pool from NTP.org. I’m using it for years, and it works very well.
A widespread mistake on the Cisco NTP configuration is to enable the command NTP master:

```
ntp master 2
```

This command is only necessary if your device doesn’t have access to an NTP server and you would like to use your device internal clock as a NTP source (not recommended).

When your NTP Server is ready, then you can proceed to the CUCM Publisher installation.

Accessing the VMware vSphere Client

Open the VMware vSphere Client and connect to your VMware server.

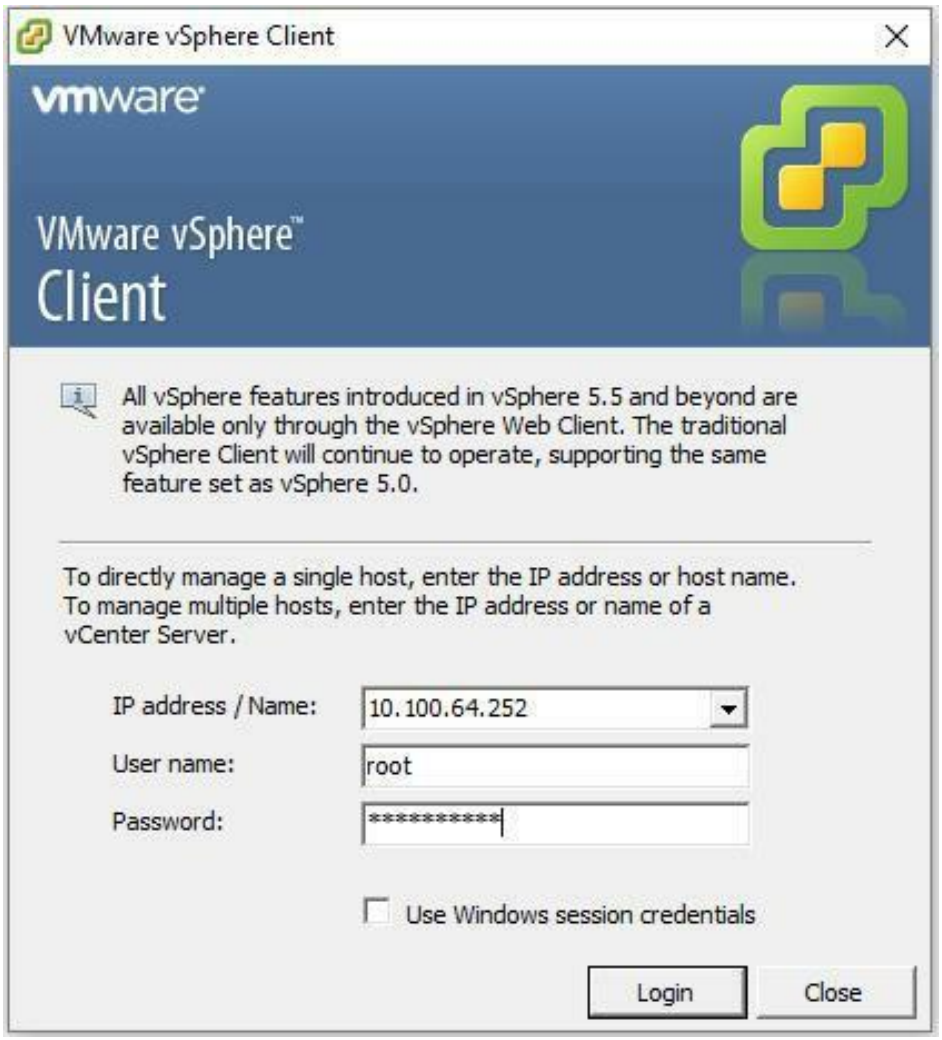


Figure 40: VMware vSphere Client

For example, I'm connecting to VMware ESXi server 10.100.64.252. The default Cisco UCS login/password are "root" and "password", but you may check your server documentation to confirm it.

When connected, go to the tab "Configuration" > "Storage". On the right side, you'll see your storages, where you need to have your CUCM installation ISO file. If you're accessing a Cisco UCS servers, all these ISO files will be here, but in your home lab, you need to load these ISO files here.

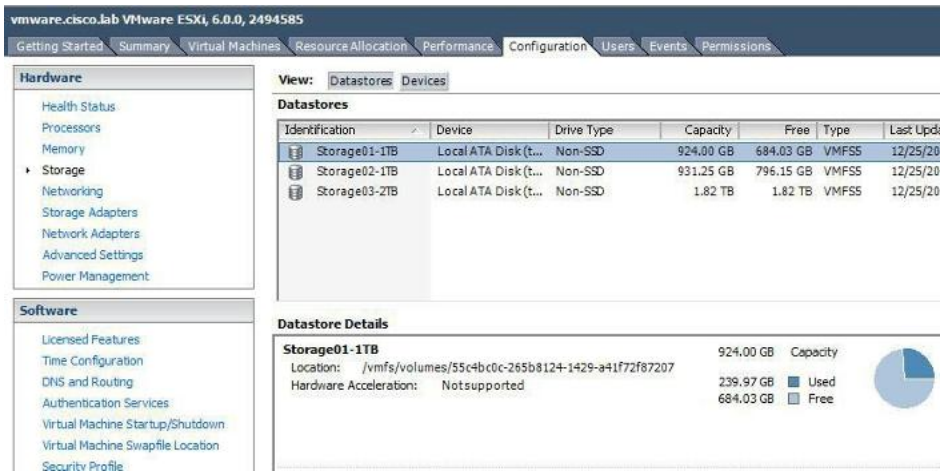


Figure 41: VMware Storage

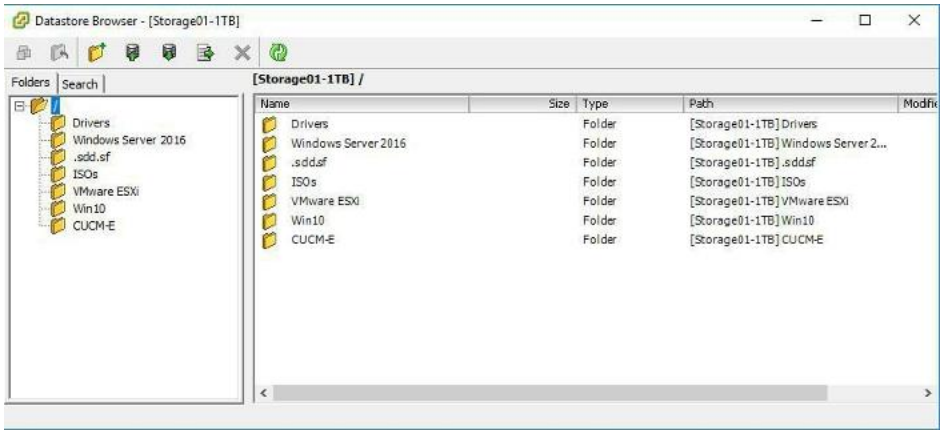


Figure 42: VMware Storage

Preparing the CUCM Publisher Virtual Machine

To prepare the virtual machine, you need to verify the hardware requirements for the system you are planning to install. You have two ways to develop the virtual machine:

- Manually create the VM with correct hardware requirements;
- Load an OVA file which automatically generates the VM.

If you have access to the OVA file, it's with no question the best option to create your virtual machine. With this file, you go directly to the menu "File" > "Deploy OVF Template..." and follow the wizard to create your virtual machine automatically.

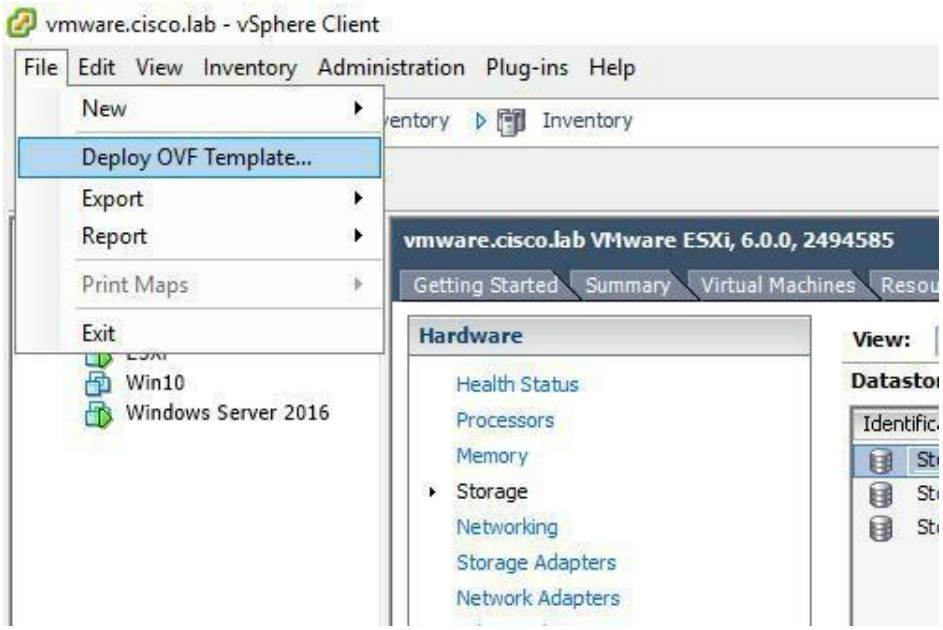


Figure 43: Deploy OVF Template

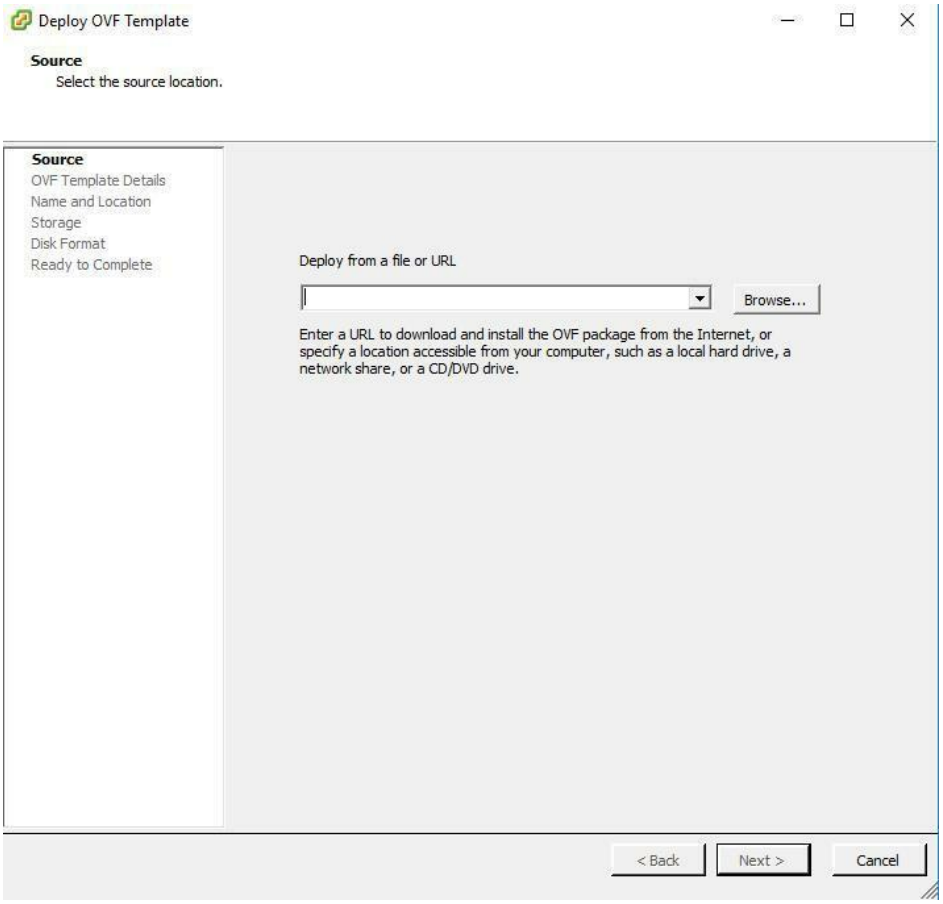
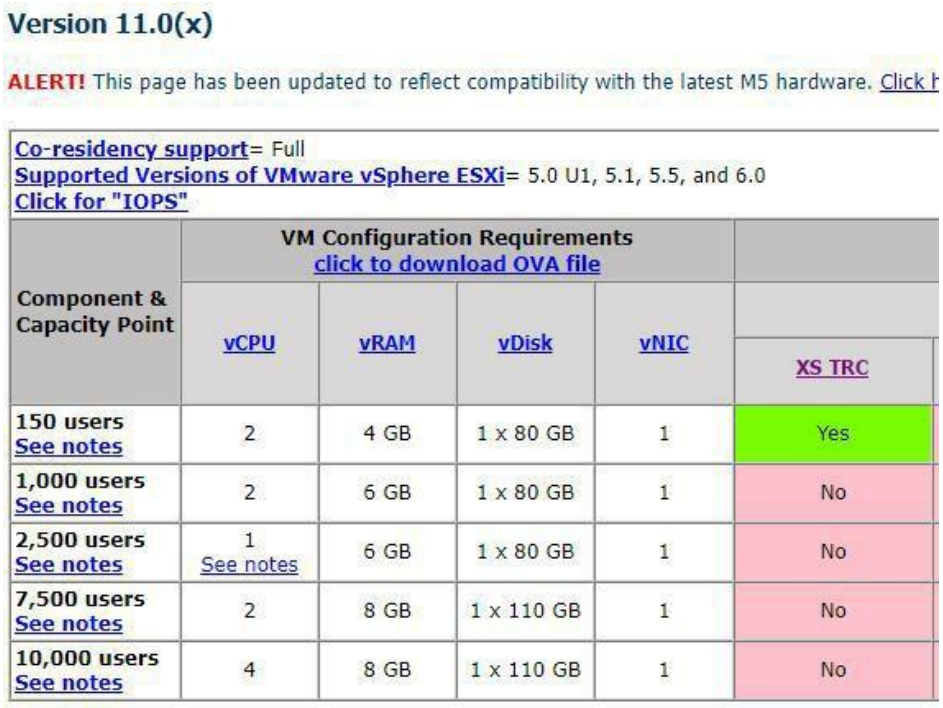


Figure 44: Deploy OVF Template Wizard

If you have an active SmartNet Contract, go to the Cisco website and search for “Virtual Server Template (OVA file)” to find the correct OVA file for your installation.

But if you don’t have access to these OVA files, you need to create the virtual machine manually. To do it, check a Cisco Website “Virtualization for Cisco Unified Communications Manager (CUCM)”, where you can find the correct information to each CUCM system.



Version 11.0(x)

ALERT! This page has been updated to reflect compatibility with the latest M5 hardware. Click h

Co-residency support= Full
Supported Versions of VMware vSphere ESXi= 5.0 U1, 5.1, 5.5, and 6.0
Click for "IOPS"

Component & Capacity Point	VM Configuration Requirements click to download OVA file				
	vCPU	vRAM	vDisk	vNIC	XS TRC
150 users See notes	2	4 GB	1 x 80 GB	1	Yes
1,000 users See notes	2	6 GB	1 x 80 GB	1	No
2,500 users See notes	1 See notes	6 GB	1 x 80 GB	1	No
7,500 users See notes	2	8 GB	1 x 110 GB	1	No
10,000 users See notes	4	8 GB	1 x 110 GB	1	No

Figure 45: VM Hardware requirements for CUCM 11.0

According to this information, to create a basic CUCM 11 virtual machine to support 150 users, we will use:

vCPU	2 CPU
vRAM	4 GB
vDisk	1 x 80 GB
vNIC	1 NIC

Table 2: Hardware Requirements for VM

With this information in hand, go to “File” > “New” > “Virtual Machine”.

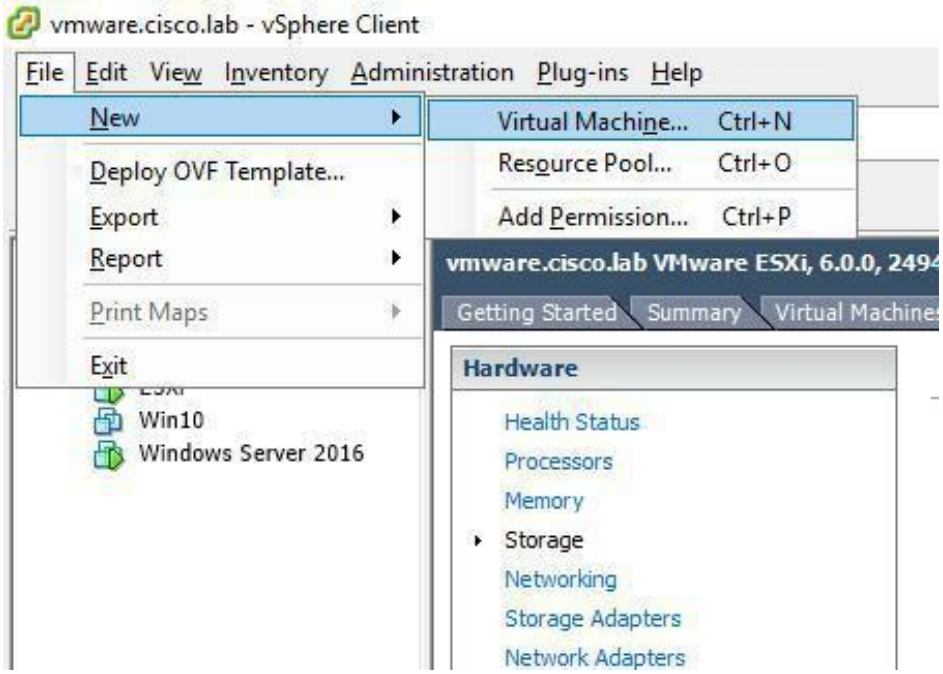


Figure 46: New Virtual Machine Wizard

Select the virtual machine type “Typical” and click “Next”.

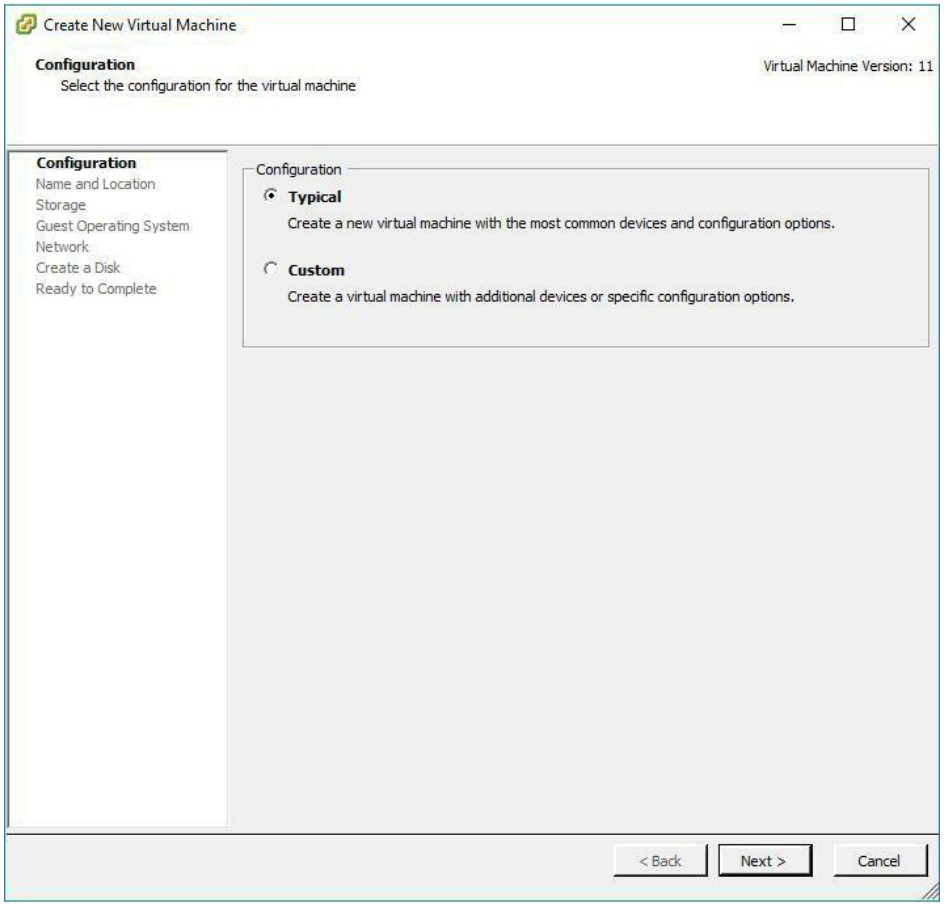


Figure 47: New Virtual Machine Wizard

Here you type the Virtual Machine name. This is not the VM hostname, but only an identifier on VMware ESXi screen.

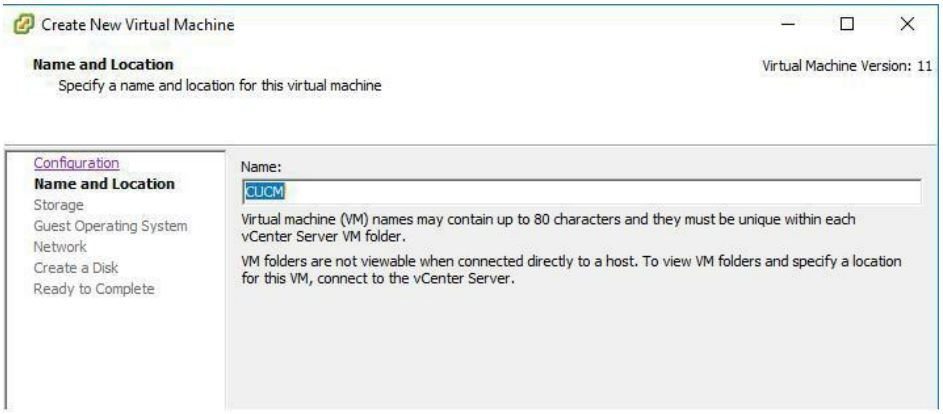


Figure 48: Virtual Machine Name

Now, select which Storage to use. On this storage, the VMware will create a folder where all VM files will be allocated.

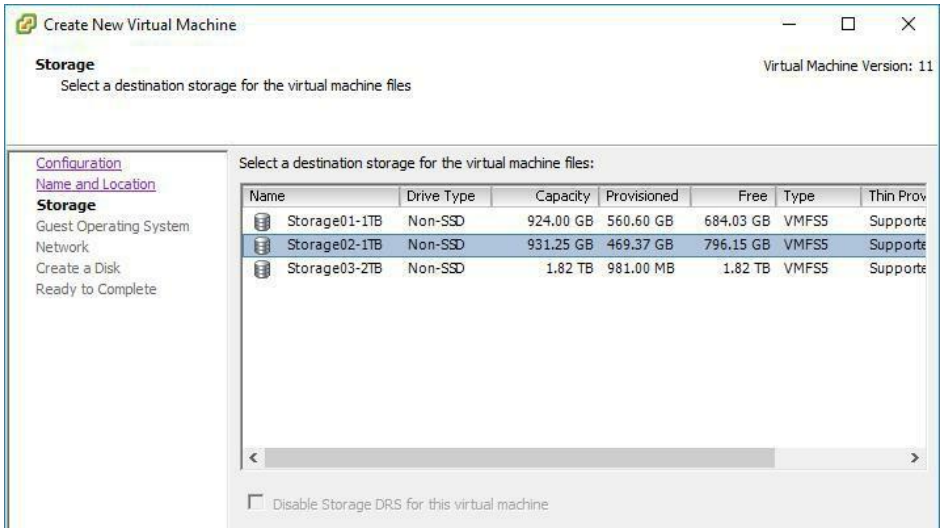


Figure 49: Virtual Machine Storage

Now you're going to select the virtual machine network interface. In your server, you will probably be using the default "VM Network", which is an untagged default VLAN, unless you want to create a trunk between VMware ESXi server and your switch. In my case, I'm using "SITE-A-VLAN-10", as I already have an 802.1q trunk between my server and my switch.

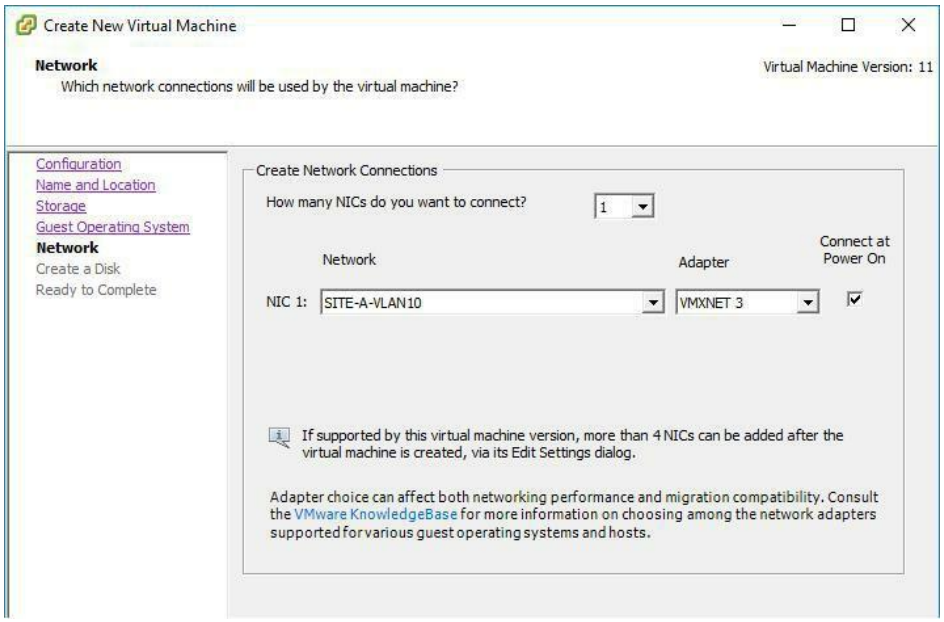


Figure 50: Virtual Machine Network

Now we need to create the disk and select the disk size. To our lab environment, as we will support only 150 phones, 80GB is enough.

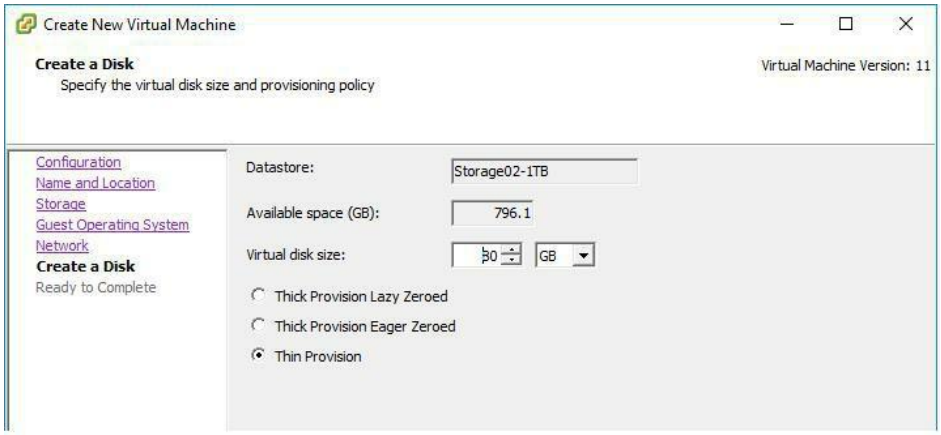


Figure 51: Virtual Machine Disk creation

About the disk type, according to VMware documentation, the options are:

Thick Provision Lazy Zeroed	A thick disk has all space allocated at creation time. This space may contain stale data on the physical media. Before writing to a new block a zero has to be written, increasing the IOPS on new blocks compare to Eager disks. The entire disk space is reserved and unavailable for use by other virtual machines.
Thick Provision Eager	An eager zeroed thick disk has all space allocated and wiped clean of any previous contents on the physical media at creation time. Such disks may take longer time during creation compared to other

Zeroed	disk formats. The entire disk space is reserved and unavailable for use by other virtual machines.
Thin Provision	Space required for thin-provisioned virtual disk is allocated and zeroed on demand as the space is used. Unused space is available for use by other virtual machines.

Table 3: Virtual Machine Disk types

In a production environment, Cisco recommends the option “Thick Provision Lazy Zeroed” to have a better performance. But to our lab environment, we can use “Thin Provision” to save disk space.

When asked to specify the guest operating system to use, select “Red Hat Enterprise Linux 7 (64-bit)”.

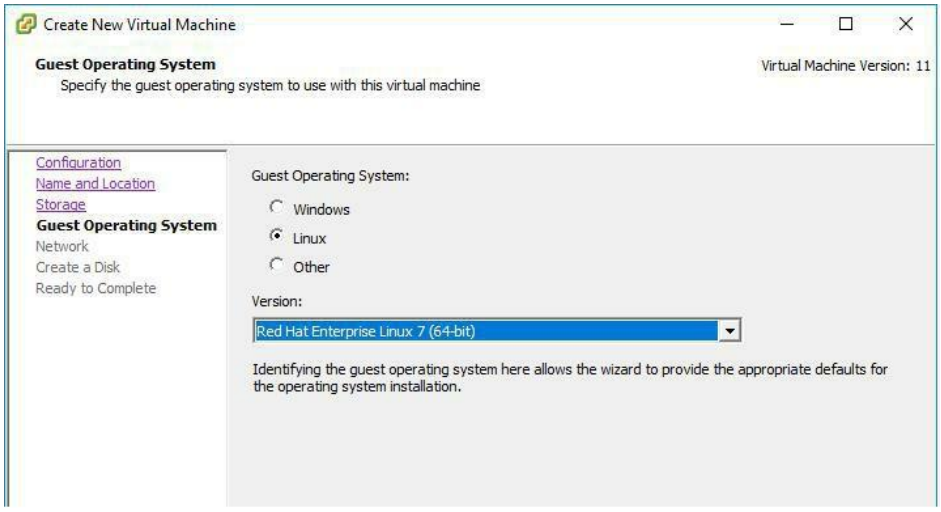


Figure 52: Selecting the guest operating system

Now the VM creation is completed, but we still need to edit some hardware options. Click “Finish” to proceed.

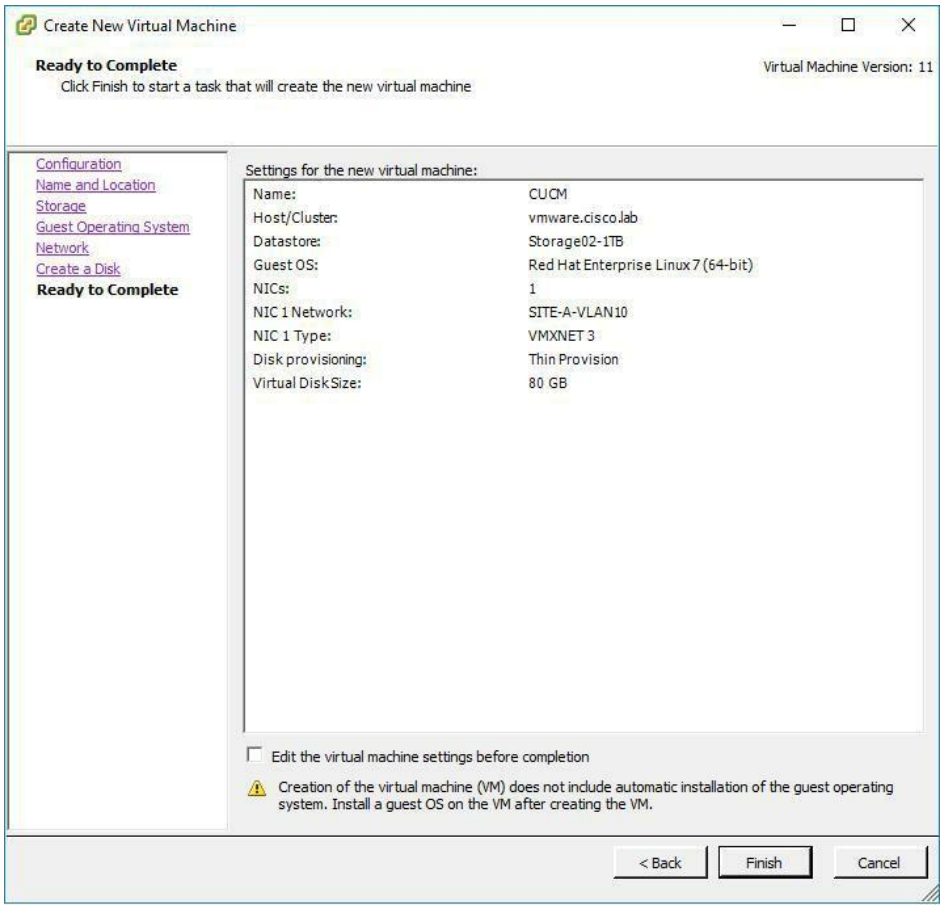


Figure 53: Finishing the VM creation

To edit the VM settings, right-click on the VM name, then select “Edit Settings...”

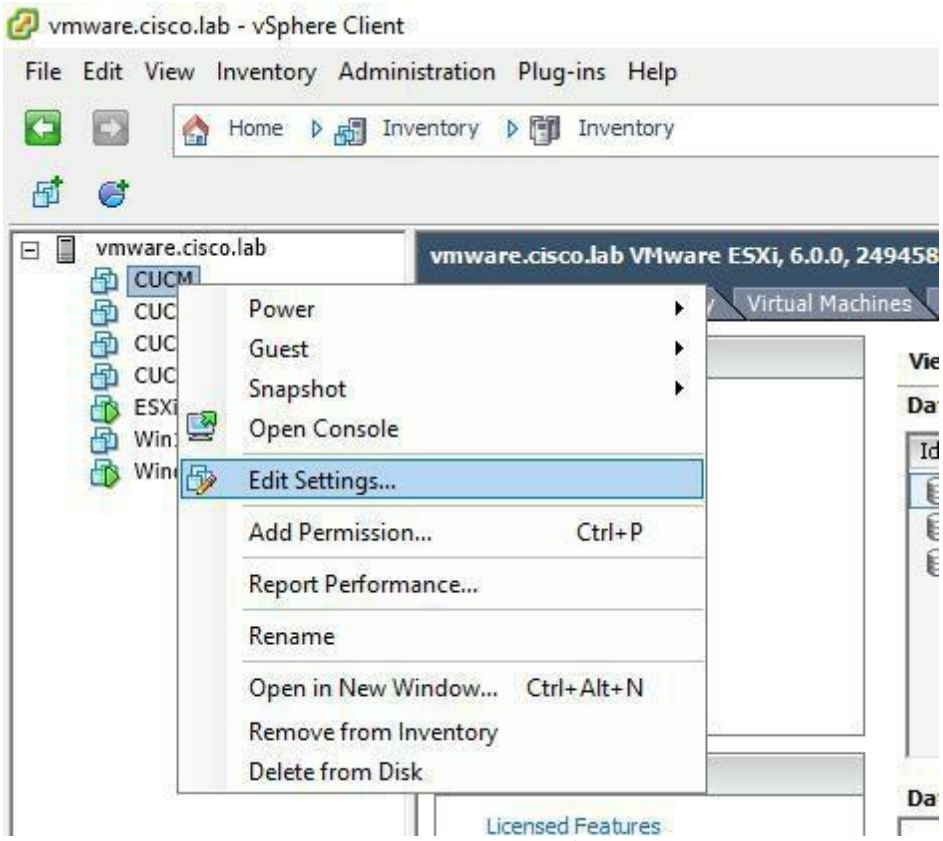


Figure 54: Edit Settings from VM

Increase the memory size to 4GB and the CPUs to 2.

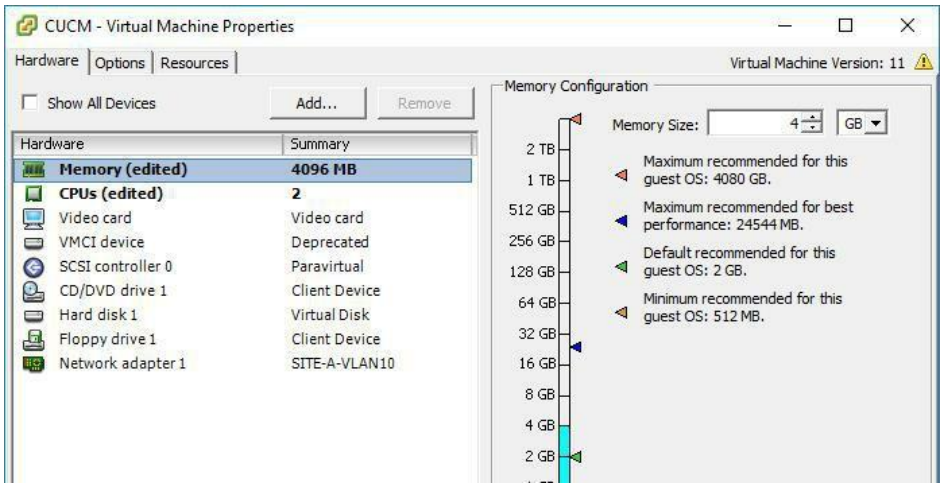


Figure 55: VM Memory Configuration

Then, go to “CD/DVD drive 1” and select the option “Connect and power on”; change the Device Type to “Datastore ISO File” and click “Browse” to select your CUCM ISO boot file.

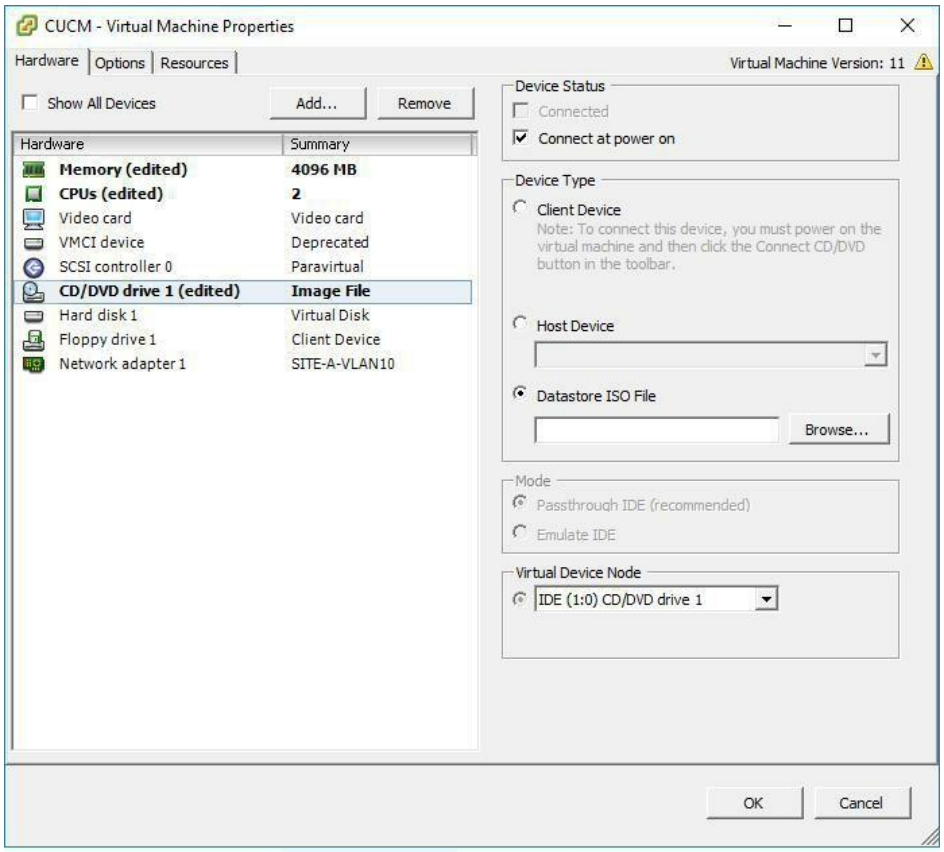


Figure 56: VM CD/DVD Configuration

Select the CUCM boot file, then click “OK”.

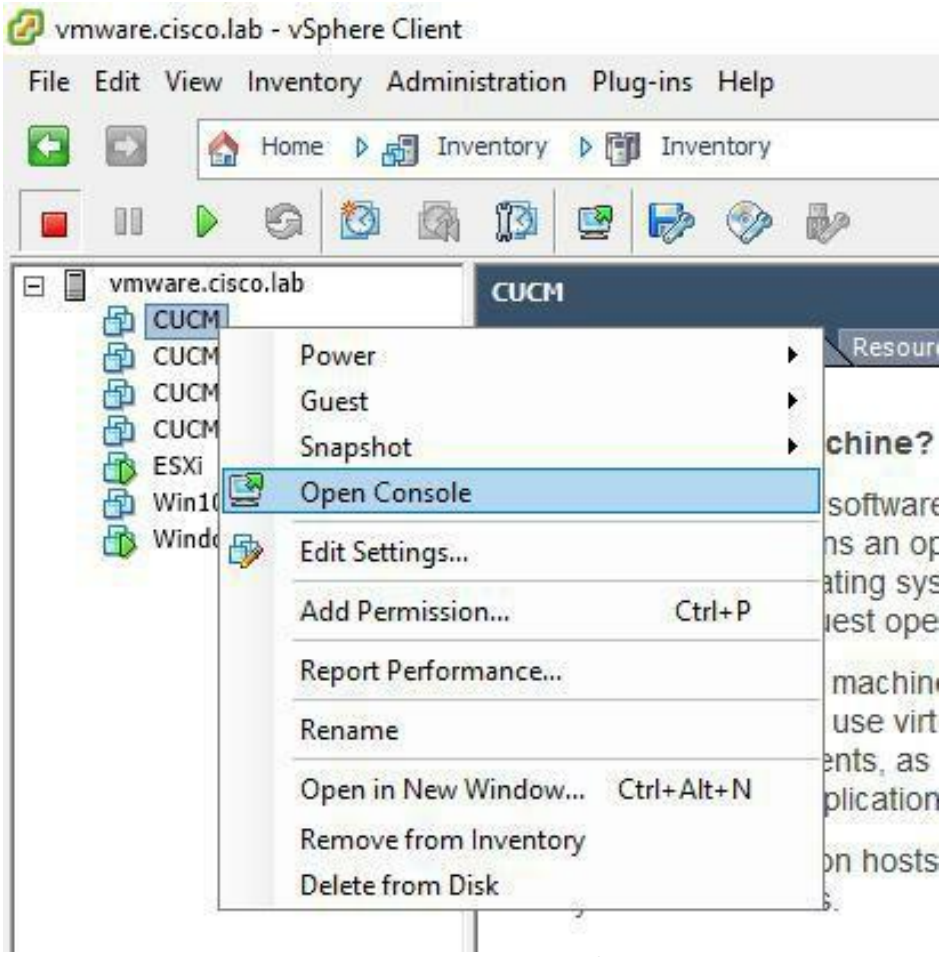


Figure 57: VM CD/DVD Configuration

Now we're ready to start the CUCM Publisher installation. Click "OK" to close this window.

> **Note:** If you only have non-bootable CUCM files, on the appendix of this book (Chapter 19) there is a tutorial showing how to create a bootable CUCM ISO file from a non-bootable CUCM ISO file. Please do not use this in a production environment, but only for lab purposes.

CUCM Publisher Installation

Before starting the installation process, the last things I would prepare are the username and passwords to be used during the process. You will need two

usernames and three passwords:

Administrator Login (and password)	This is the operating system administrator and password. Used to access the server via SSH and also via Web to the OS Admin web page. Necessary a username and password.
Security Password	This is the database password. It will be necessary to install the Publisher and the Subscriber; it must be the same on all CUCM nodes. It is also used during the backup restore process. Necessary only the password.
Application User (and password)	This is the CUCM Web administration. It will be used to manage everything related to telephony. Necessary a username and password.

Table 4: CUCM usernames and passwords

Now that you have all usernames and passwords in hand, let's start the installation process. Right-click on your CUCM VM and select "Open Console".

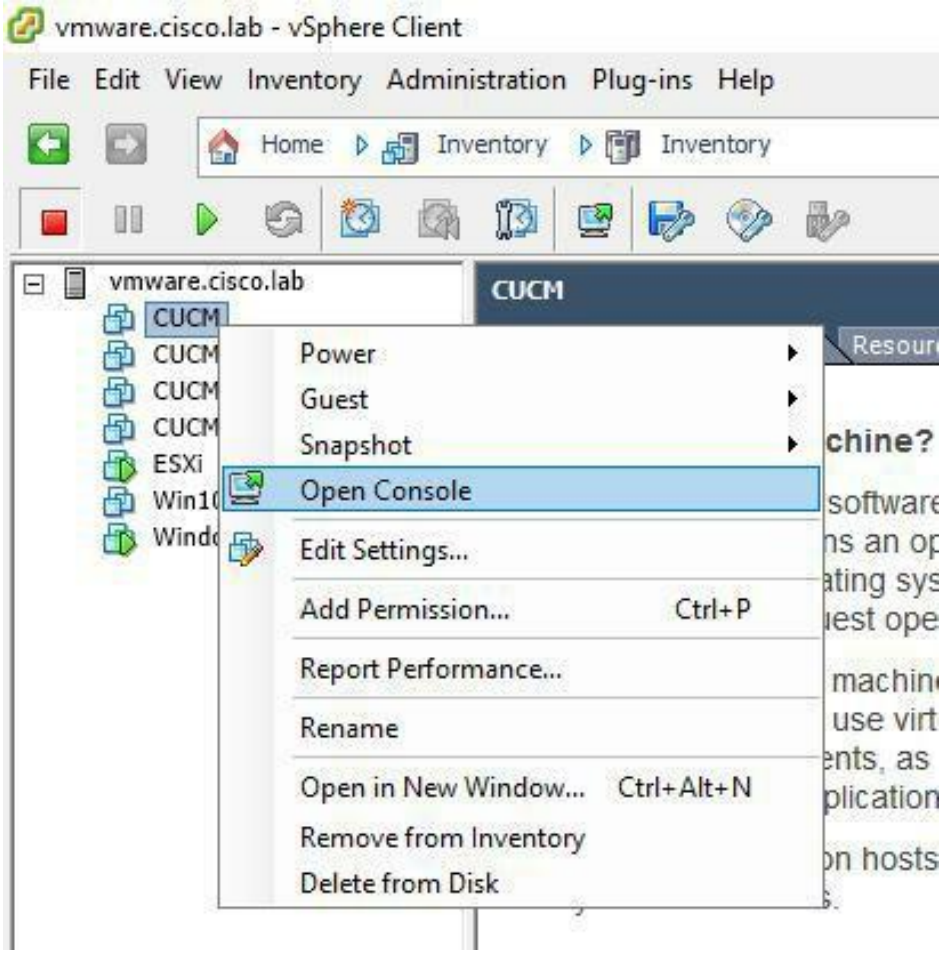


Figure 58: Open Console from VM

A pop-up window will appear with the server console. This is like connecting a monitor with mouse and keyboard directly in the computer. Press the green button “Play” to start the virtual machine.

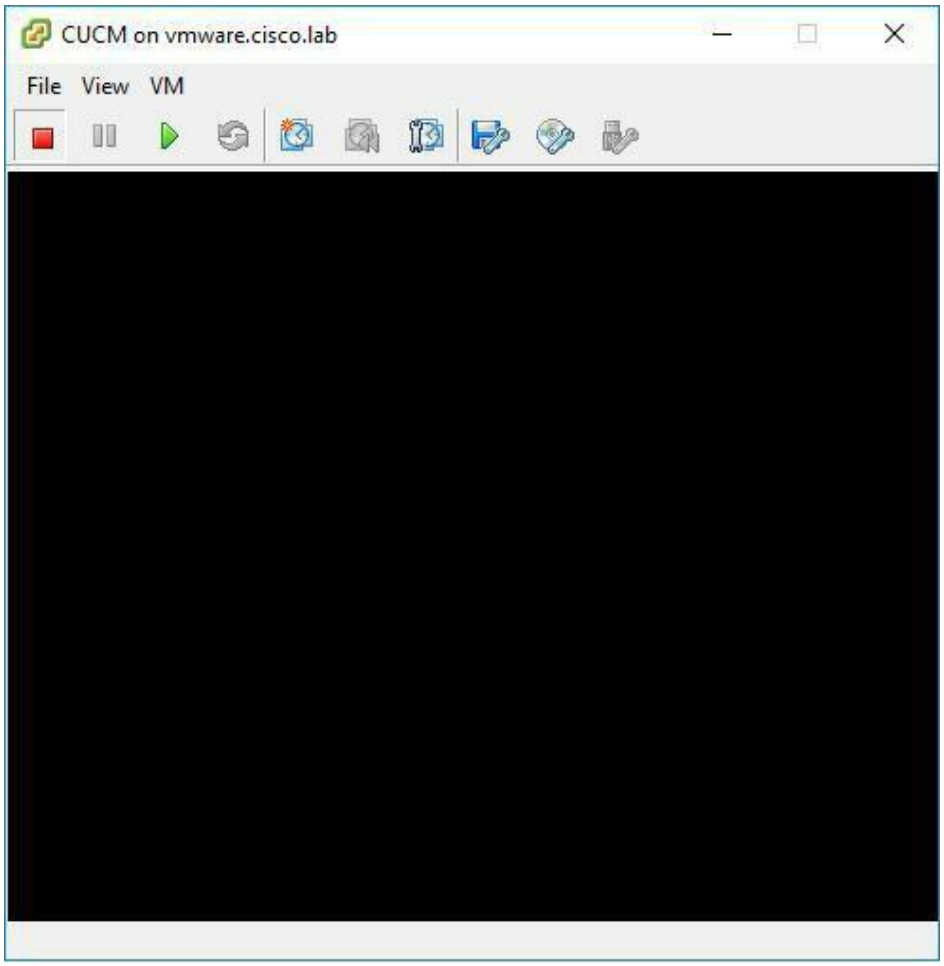


Figure 59: VM Console window

The CUCM VM will start the boot process.

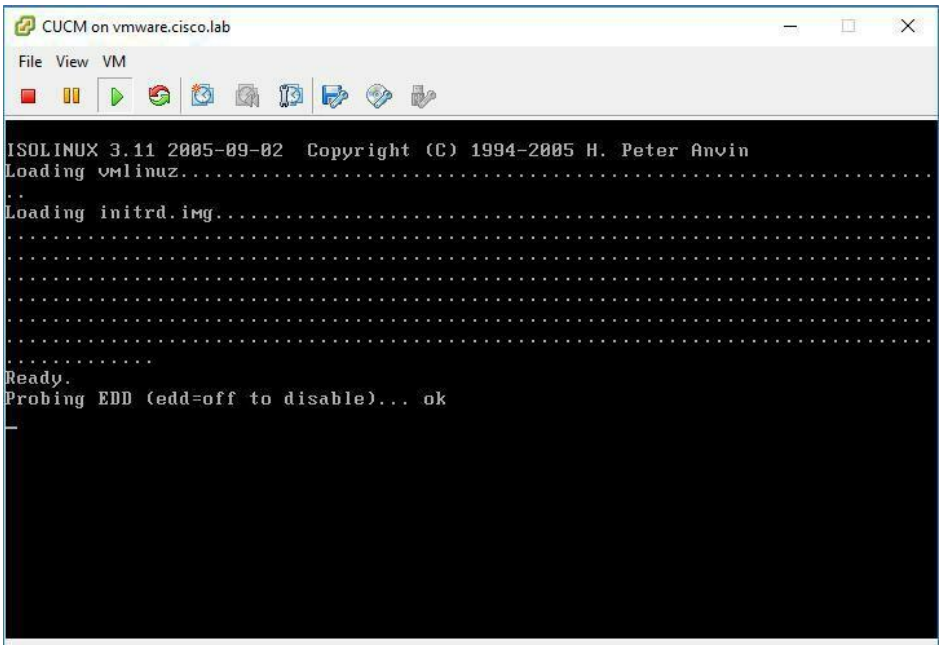


Figure 60: CUCM VM booting

For those who know Red Hat Linux, this is the Anaconda installer. To navigate, use the keyboard keys TAB, ENTER and the arrow keys.

In this first screen, the system is asking if you would like to perform a media check, to verify if your ISO file has any error. I usually skip this test.

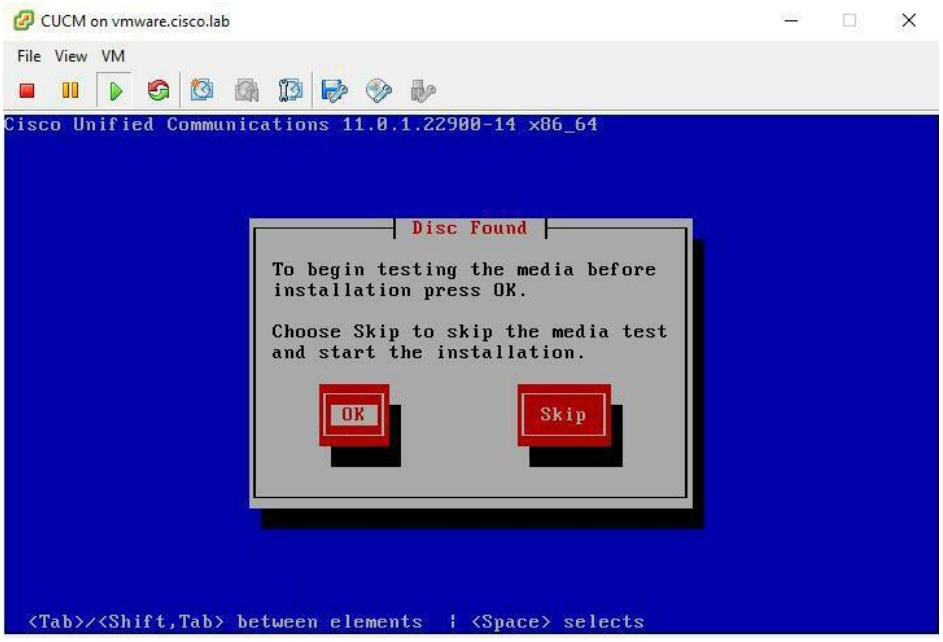


Figure 61: CUCM media test

According to the VM hardware created, these are the products available in

this installation. If you want to install the Cisco Unity Connection, you can use the same ISO File, just changing the VM hardware requirements.

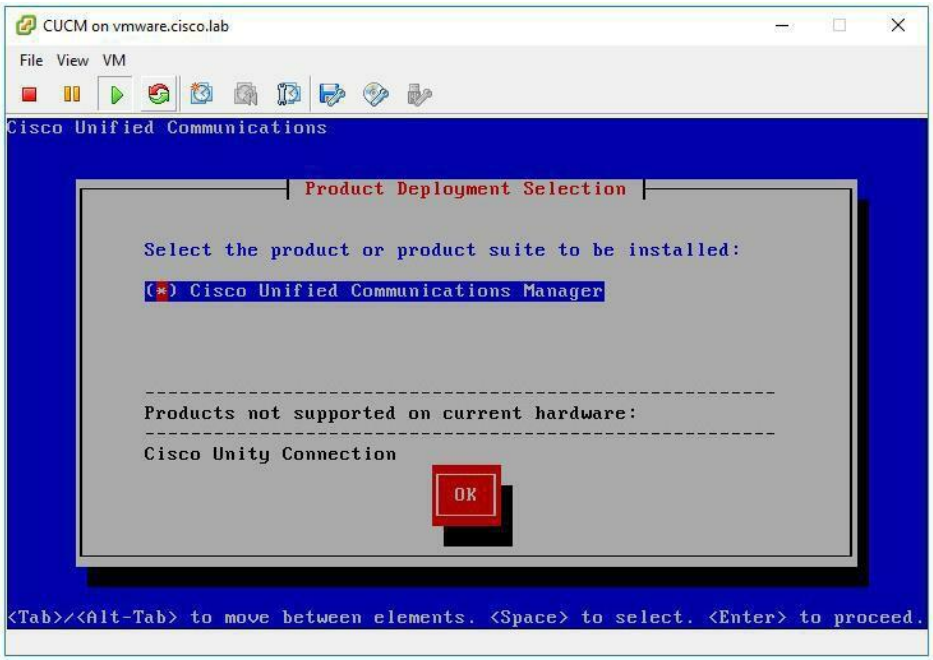


Figure 62: CUCM Installation product selection

Here the system will display the version you're installing.

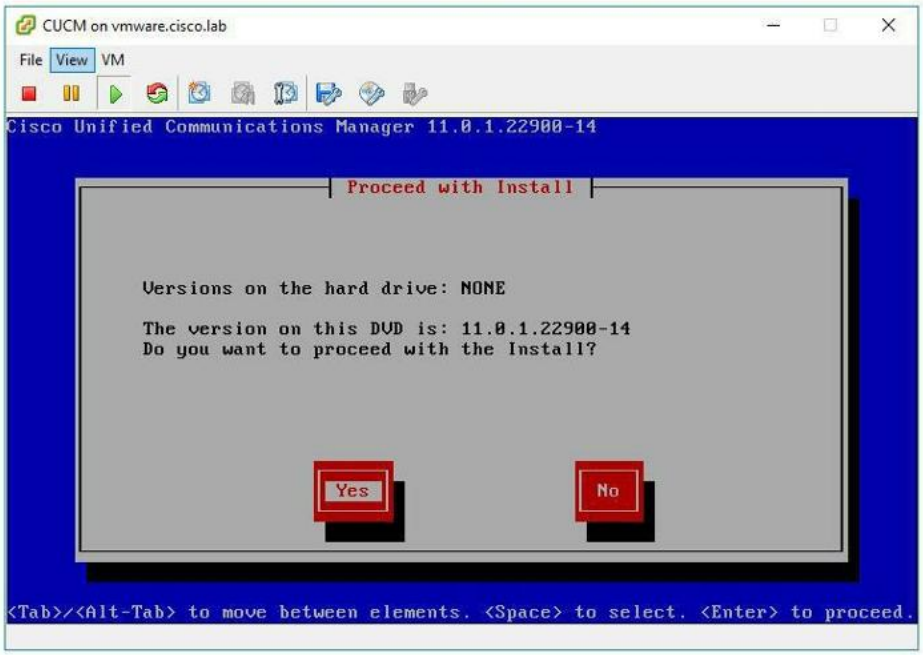


Figure 63: CUCM Version to be installed

Now you have two options: run the configuration wizard now or later. At the end of the process, the results are the same. I prefer to select the option “skip”, so the system will proceed with some installation tasks and will only ask me information later, but as I said, there is no difference at the end.

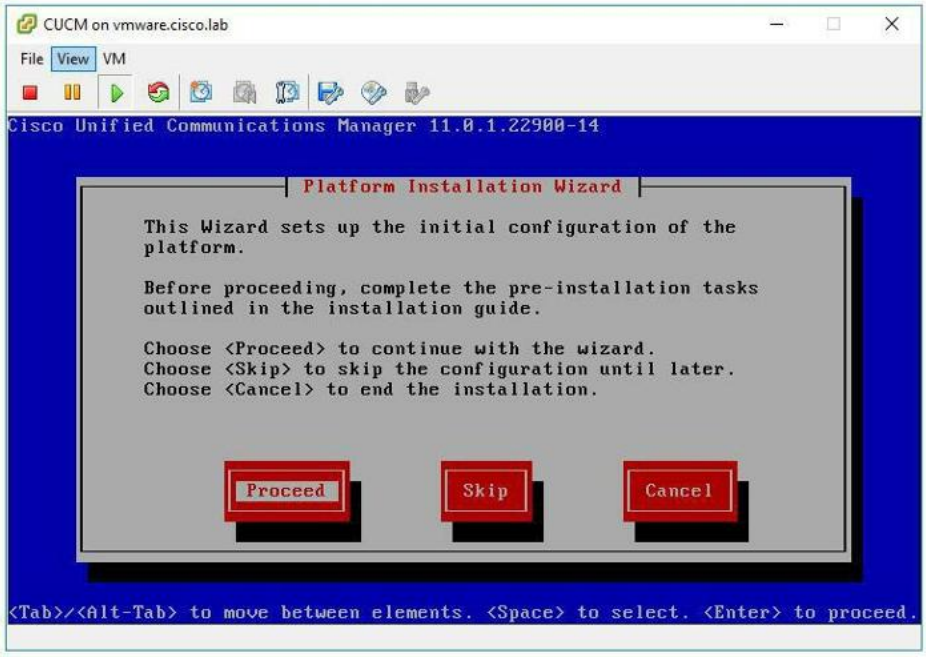


Figure 64: CUCM Platform Installation Wizard

As I create the VM manually, sometimes the system can ask to reinitialize the hard drives. If this message appears to you, select “Re-initialize all”.

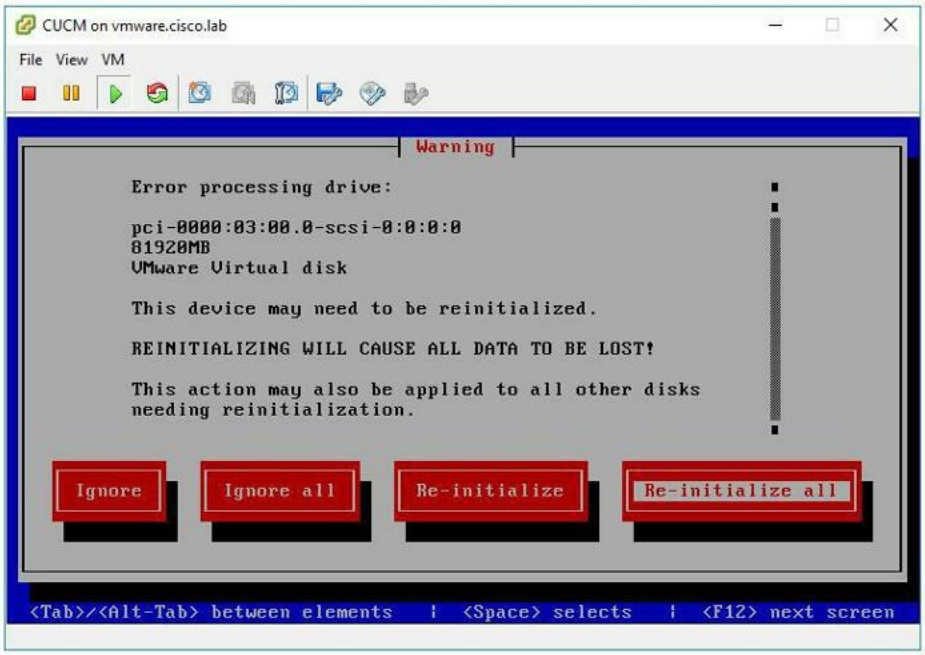


Figure 65: Disk Initialization warning

After some minutes, the system reboots and starts the Platform Installation Wizard.

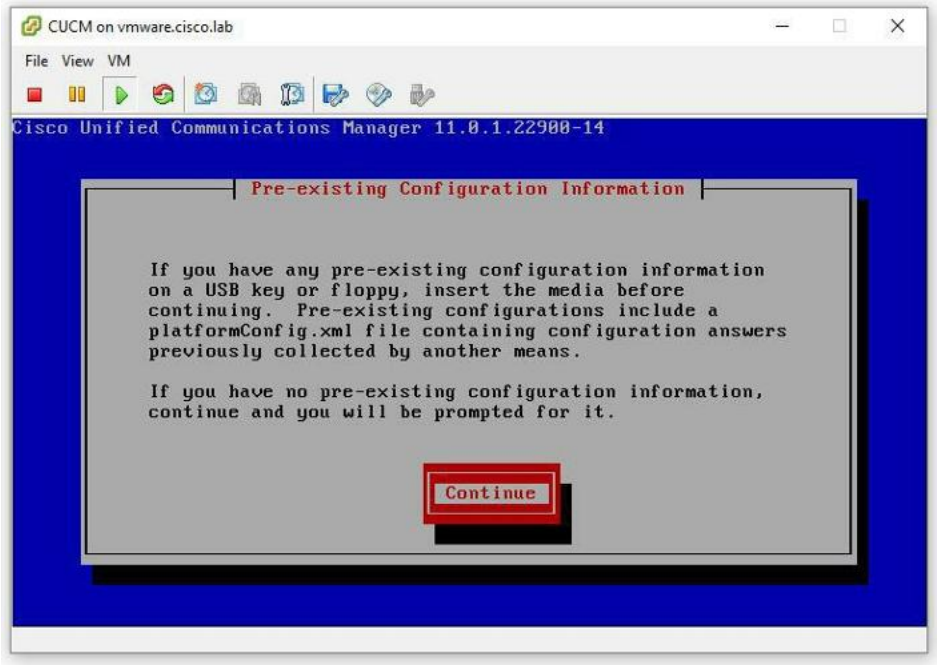


Figure 66: Pre-existing Configuration Information

Now, the CUCM Platform Installation Wizard will only inform you that the configuration process will start. Just click “Proceed”.

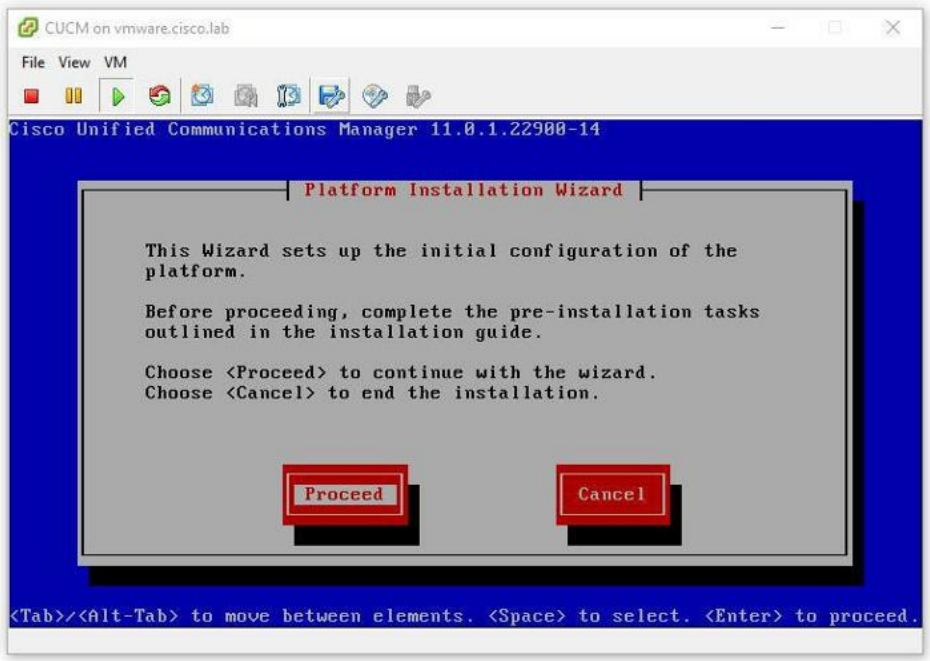


Figure 67: CUCM Platform Installation Wizard

The system asks if you have a patch to apply. If you don't have any, select "No".

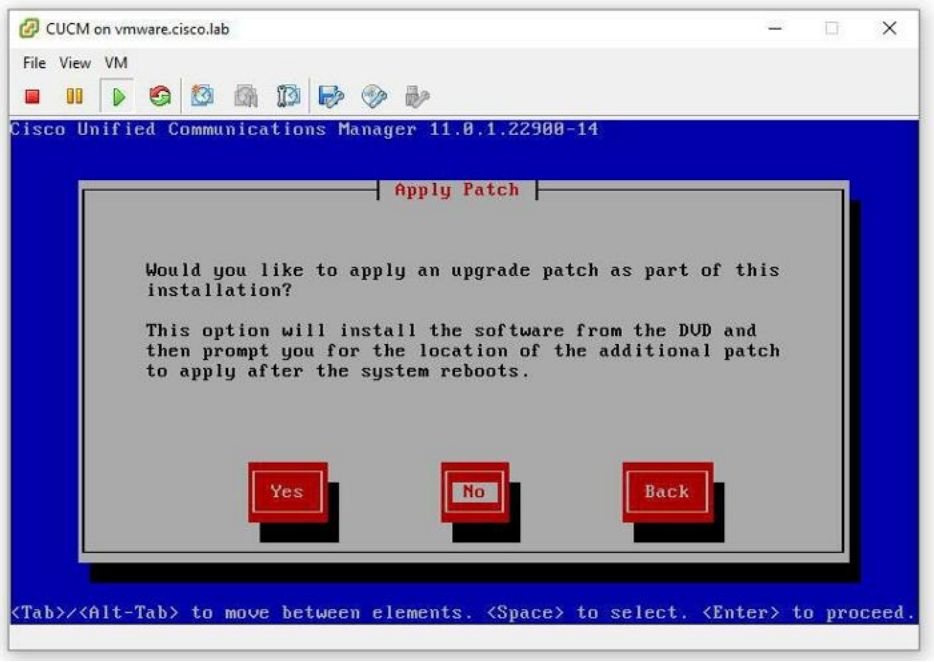


Figure 68: CUCM Apply Patch window

As we don't have a patch, the system will confirm that it is a "Basic Install".

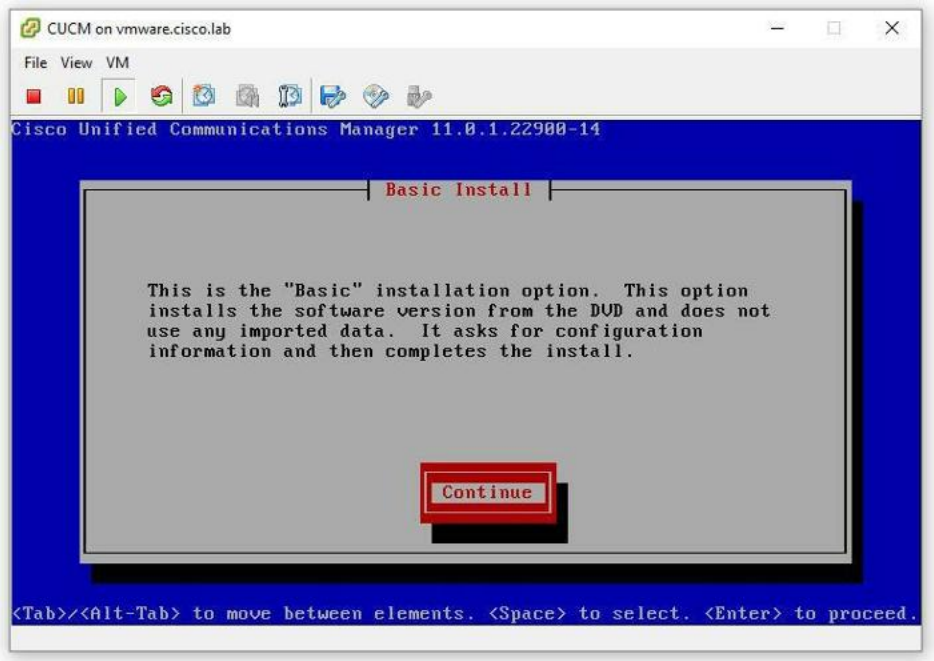


Figure 69: CUCM Basic Install Window

Select the correct timezone configuration and click “OK”.

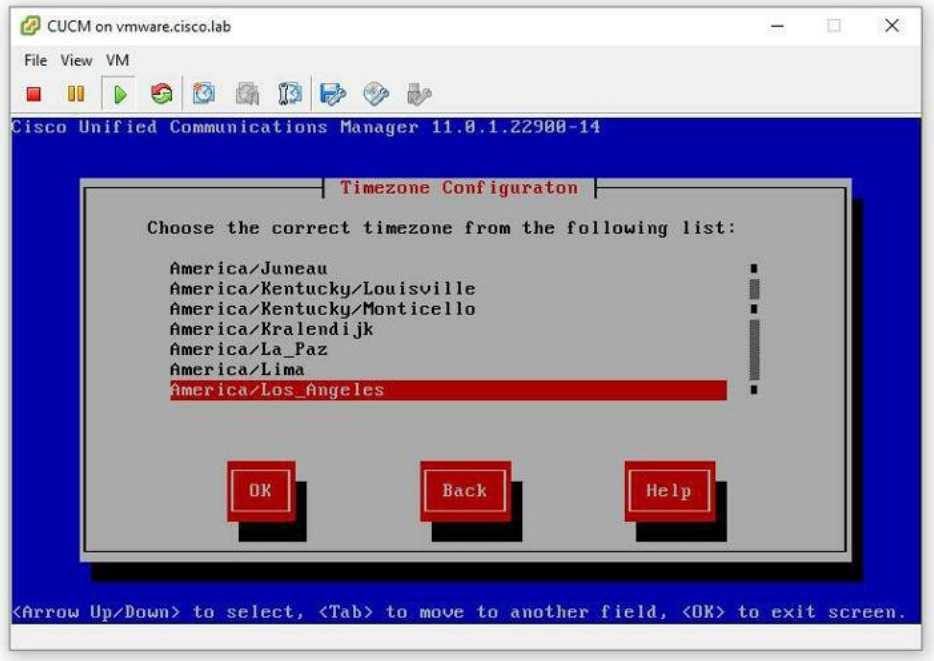


Figure 70: CUCM Timezone Configuration Window

The system will inform you that the network interface card will receive speed and duplex information from the Host (your physical server).

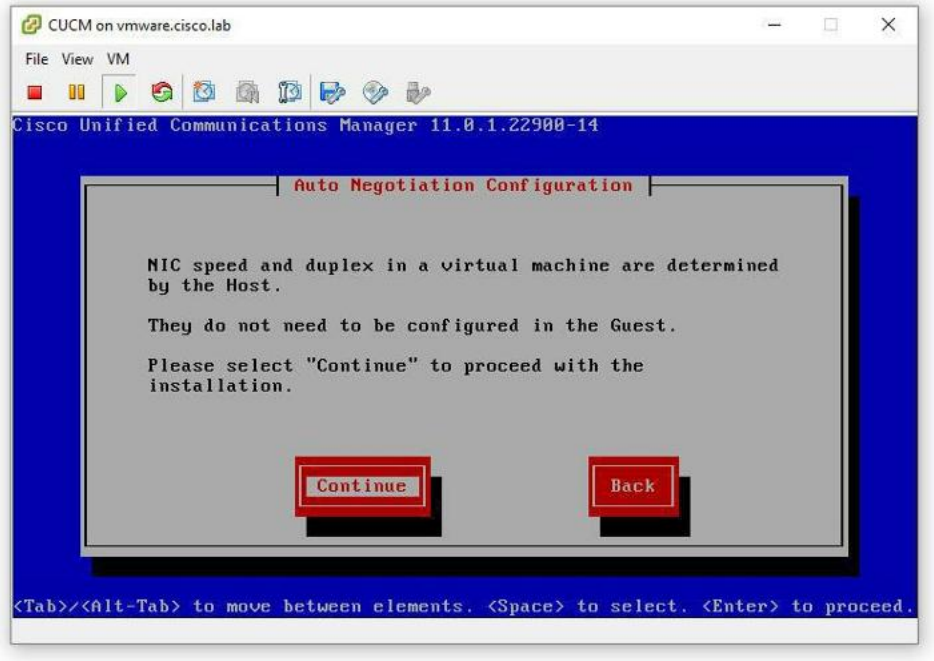


Figure 71: CUCM Network Auto Negotiation Window

If you want to change the default MTU size from 1500, select “Yes”. If not, select “No” (recommended).

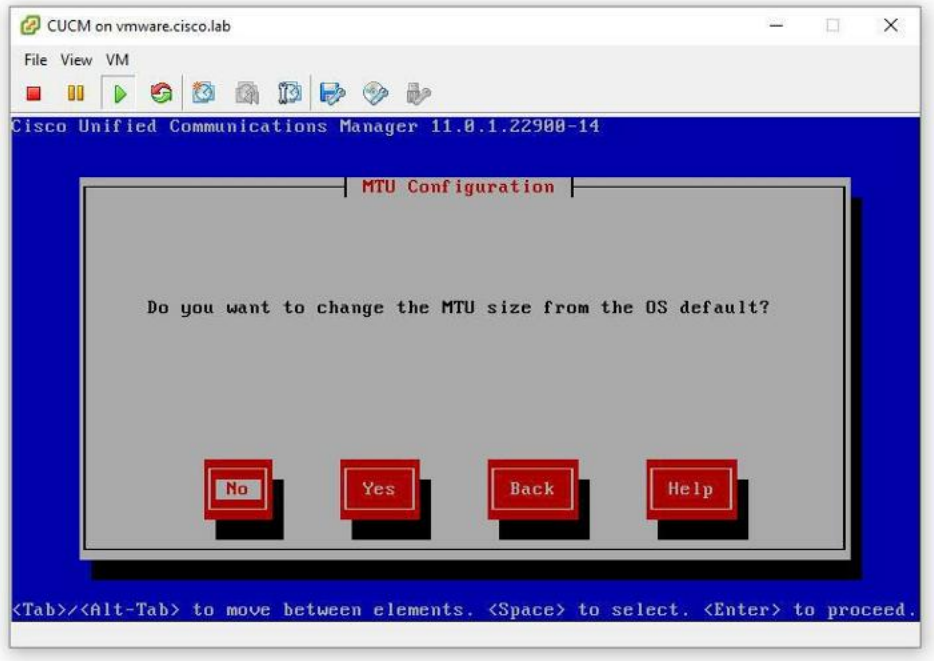


Figure 72: CUCM Network MTU Window

Now the installation will ask if you want to use DHCP Client on your CUCM Server (!!!). Of course, the recommended is always to select “No” and

configure manual IP Address to your server.

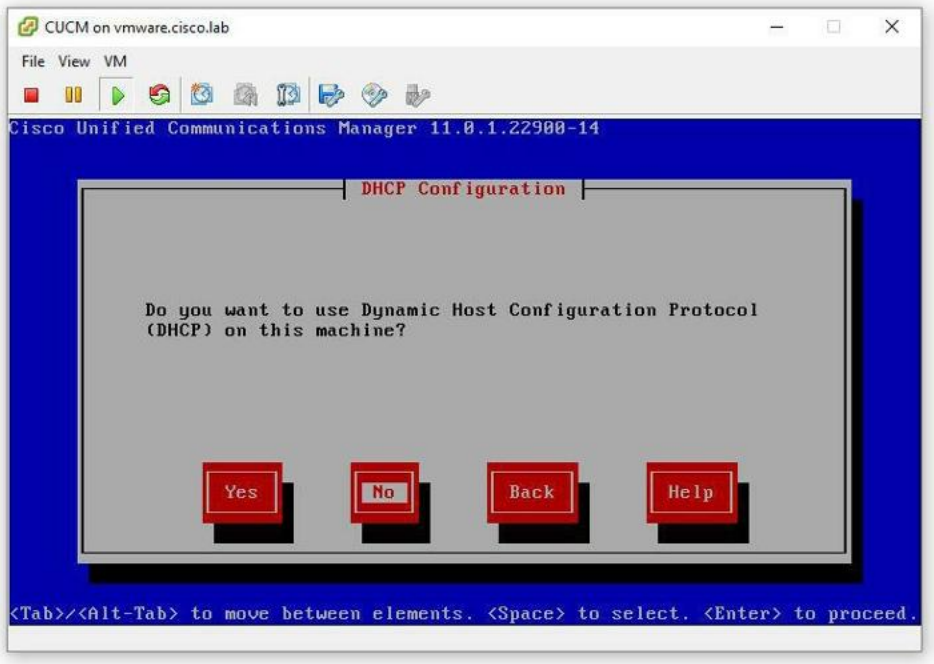


Figure 73: CUCM Network DHCP Configuration Window

Type your network configuration (Hostname, IP Address, Network Mask and Gateway).

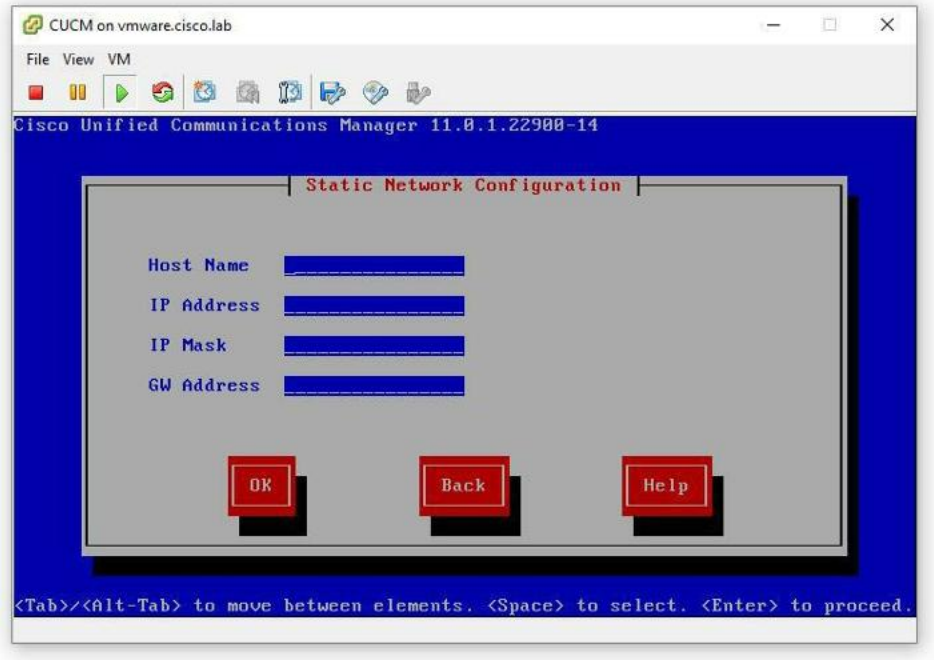


Figure 74: CUCM Static Network Configuration Window

The system now asks if you want to enable DNS Client on this machine. I think it's always a bad idea to enable any DNS dependency on CUCM, as you will create a point of failure on your telephony system.

What usually happens is: if you depend on DNS name resolution, a failure on your DNS servers can impact the phones registration and other services.

So it is strongly recommended to select "No" at this point.

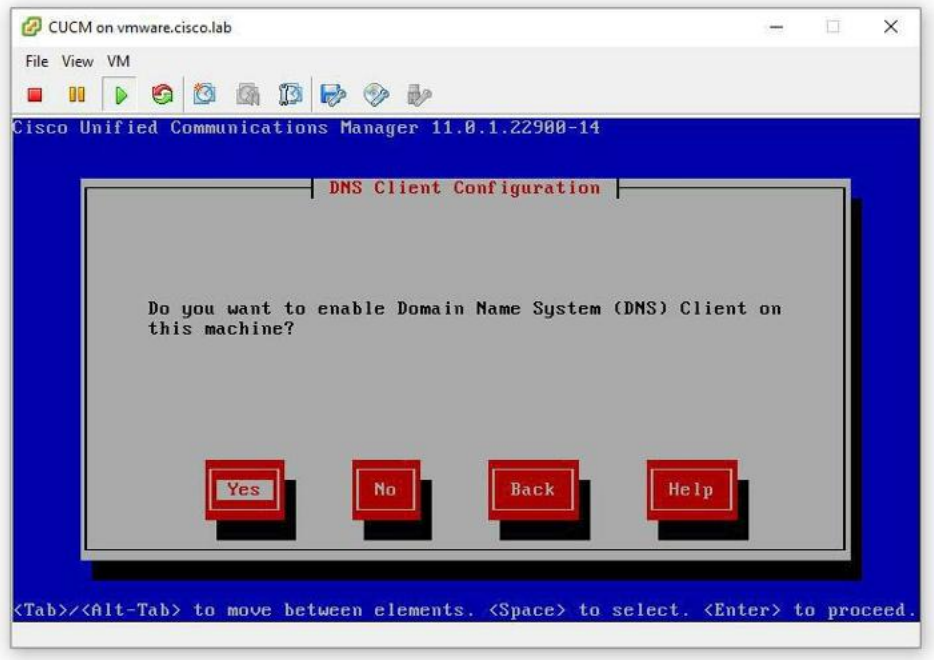


Figure 75: CUCM DNS Client Configuration Window

Now, create the username and password for the "Administrator Login". This will be used to access the server via SSH and also some of the web pages. Usually, a lot of people create it as "Administrator" or "CUCMAdministrator", but feel free to use what you want.

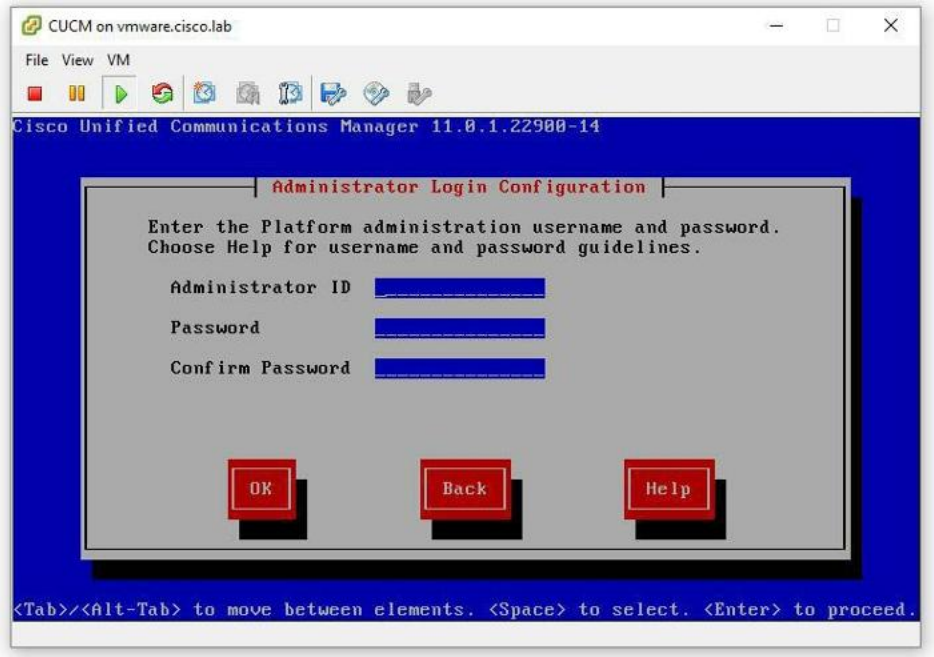


Figure 76: CUCM Administration Login Configuration Window

The CUCM will ask about the Certificate Information. You can type what you want, as it is only the HTTPS Certificate. As an example, in my lab, I use "LAB" in all fields. In your company, you can use the company name and information to fill it.

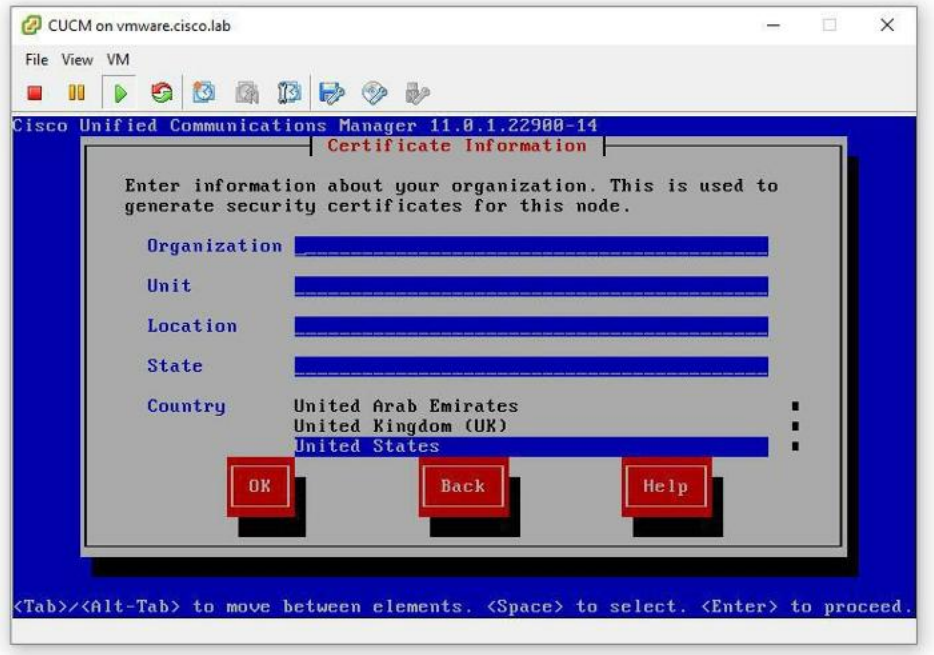


Figure 77: CUCM Certificate Information Configuration Window

Now the system will ask if this is the First Node in the cluster. This is a crucial question, as:

- If you select “Yes”, this VM will be the Publisher node of your Cluster;
- If you select “No”, this VM will be a Subscriber node of your cluster.

If you select this information incorrectly, you cannot change it later, and you will need to restart the installation from scratch.

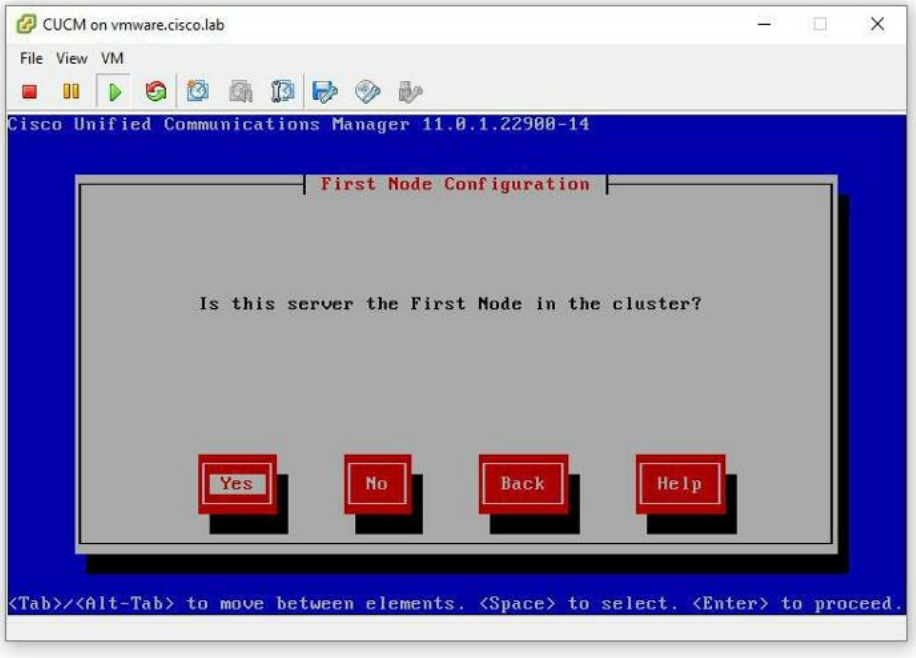


Figure 78: CUCM First Node Configuration Window

Here you need to type the IP address of your NTP server. You can press “Test” to validate if you want. After, select “Proceed”.

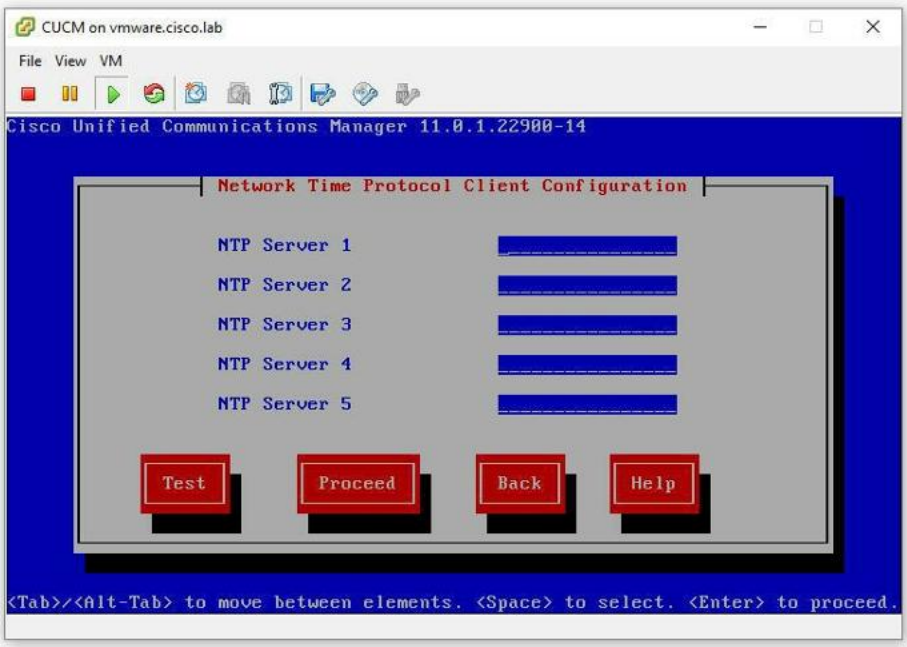


Figure 79: CUCM NTP Configuration Window

Now the system will ask you about the Security Password.

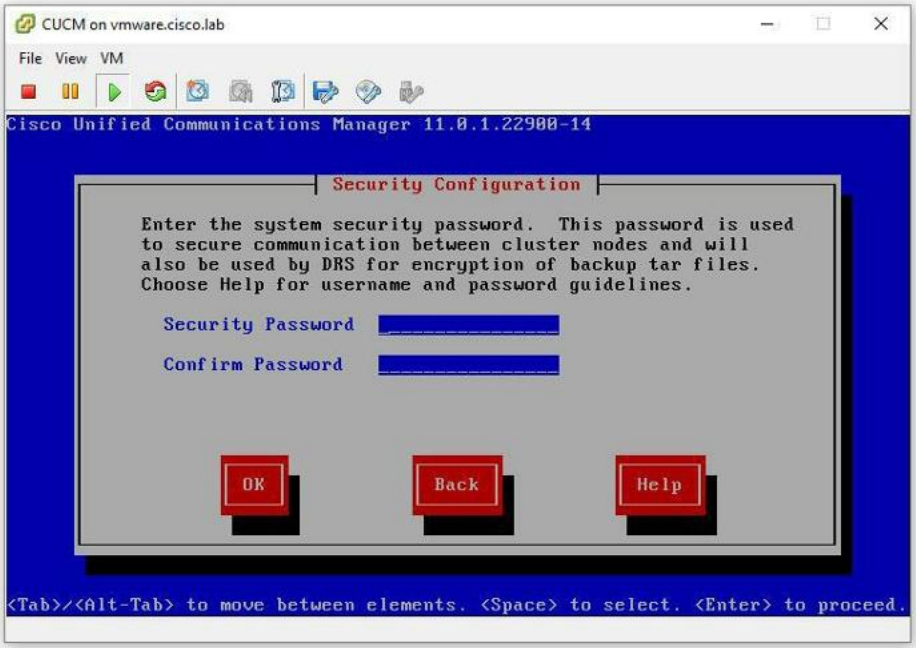


Figure 80: CUCM Security Password Configuration Window

If you want to enable an SMTP host on this server, select “Yes”, if not, select “No”. I usually do not use this SMTP option.

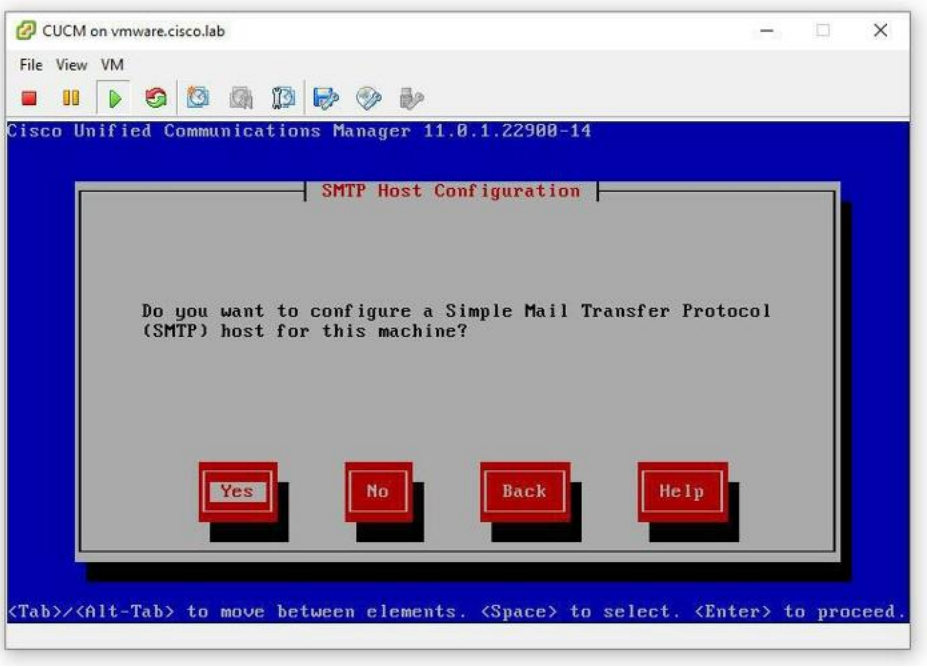


Figure 81: CUCM SMTP Host Configuration Window

Now you must select the “Smart Call Home” feature. According to Cisco, this feature:

> Smart Call Home offers proactive diagnostics and real-time alerts on select Cisco devices and provides higher network availability and increased operational efficiency. This proactive, support capability is provided at no additional cost with an active service contract and entitlement for the designated products.

Even when I have an active SmartNet contract, I have never used this feature. Then, I select “Disable All Call Home on System Startup”, but if you want, you can try it.

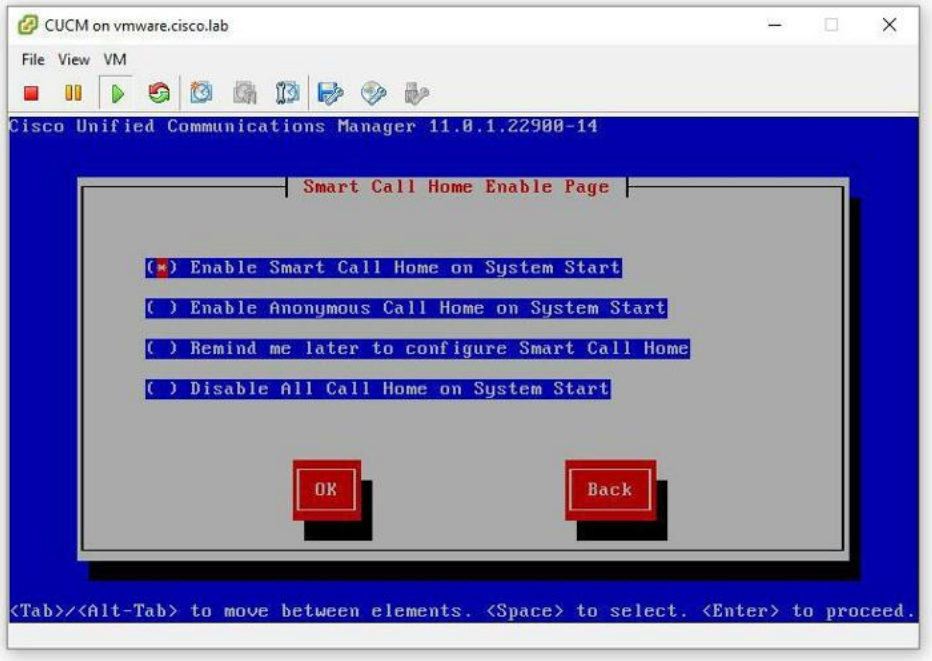


Figure 82: CUCM Smart Call Home Configuration Window

Finally, the system will ask you the “Application User Configuration”.

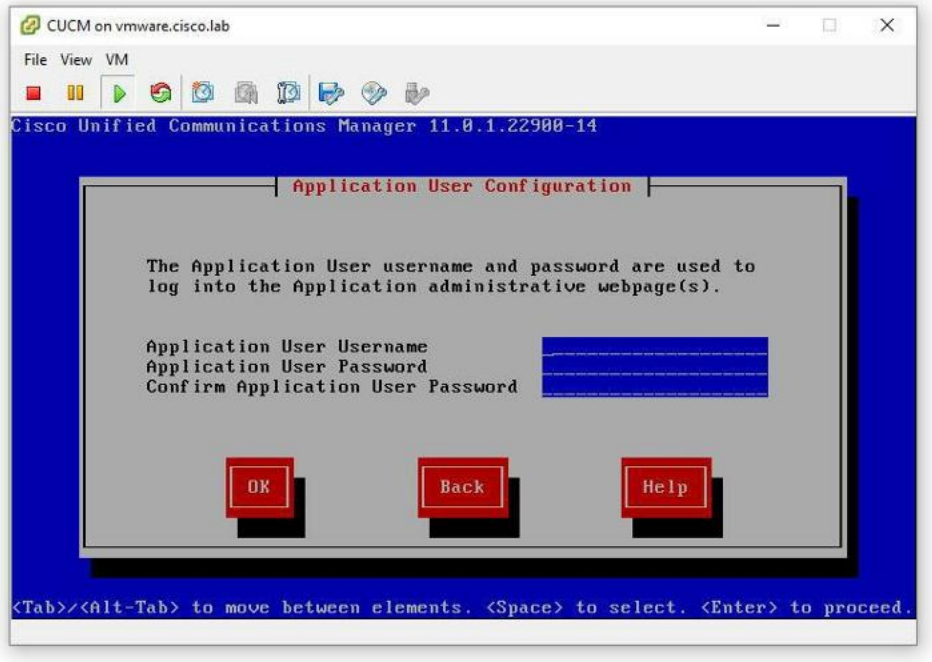


Figure 83: CUCM Application User Configuration Window

Then, the configuration is completed.

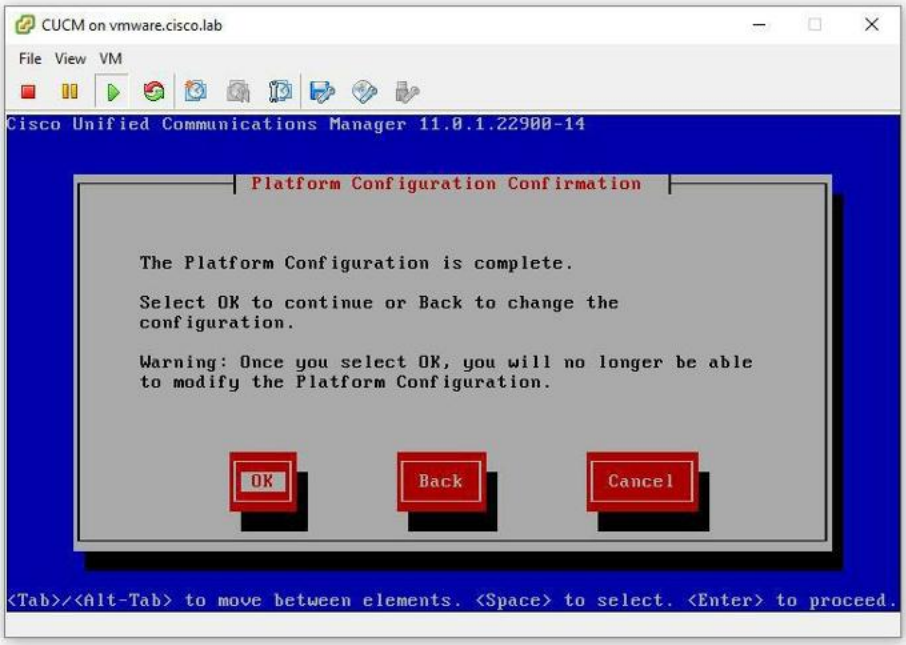


Figure 84: CUCM Platform Configuration Confirmation Window

Usually, it can take from 25 to 50 minutes to finish this process.

First access

Access via Web

The CUCM management is done via web access (HTTPS) and SSH. The SSH is only used for systems maintenance like database recovery, network changes, and others. Except for these situations, all configurations are done via HTTPS access.

When you open the CUCM IP address via HTTPS, you will see a page like this:

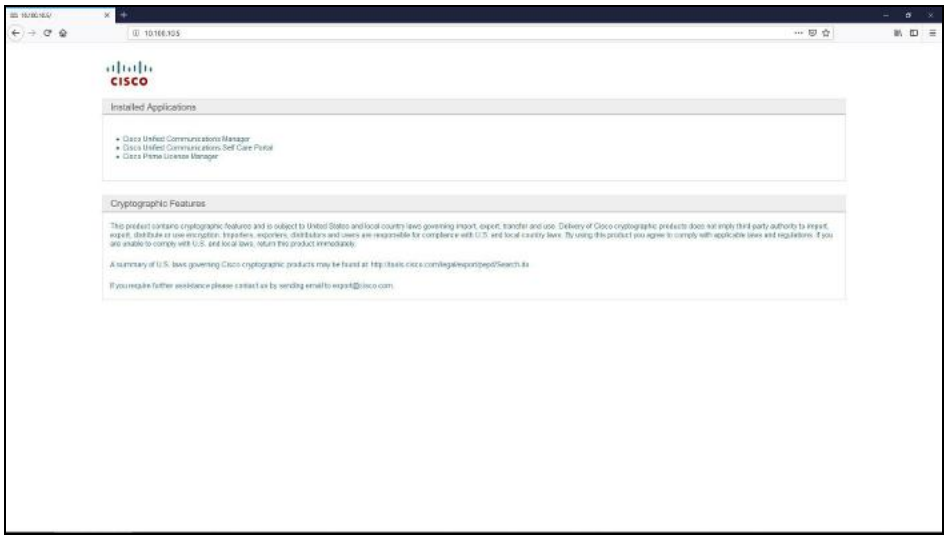


Figure 85: CUCM Initial Web Page

Just click on the first link to proceed (Cisco Unified Communications Manager). You will be advised about a certificate error, accept it to continue. Then you'll see a login screen:

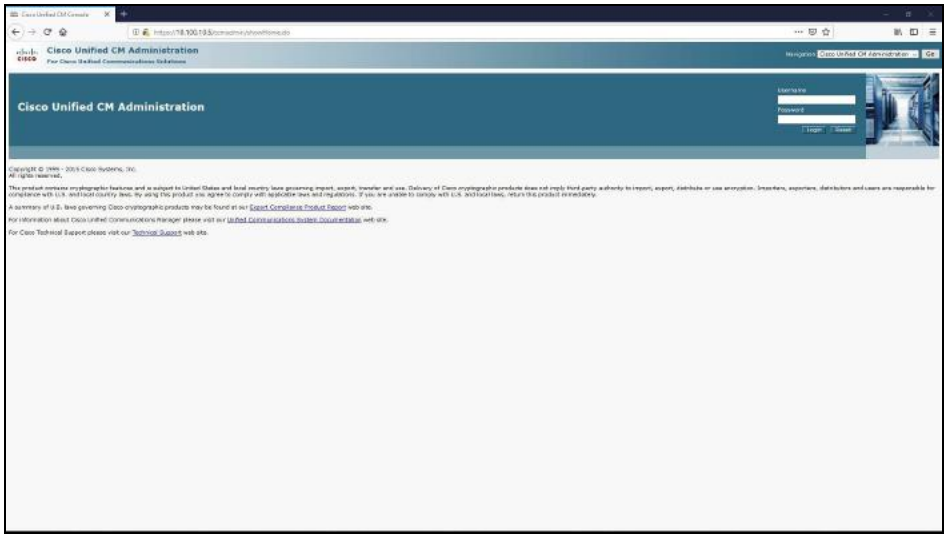


Figure 86: CUCM Initial Web Page

This is the main page of CUCM, where we will do all our configurations. At top right corner insert the credentials you have created on during the installation.

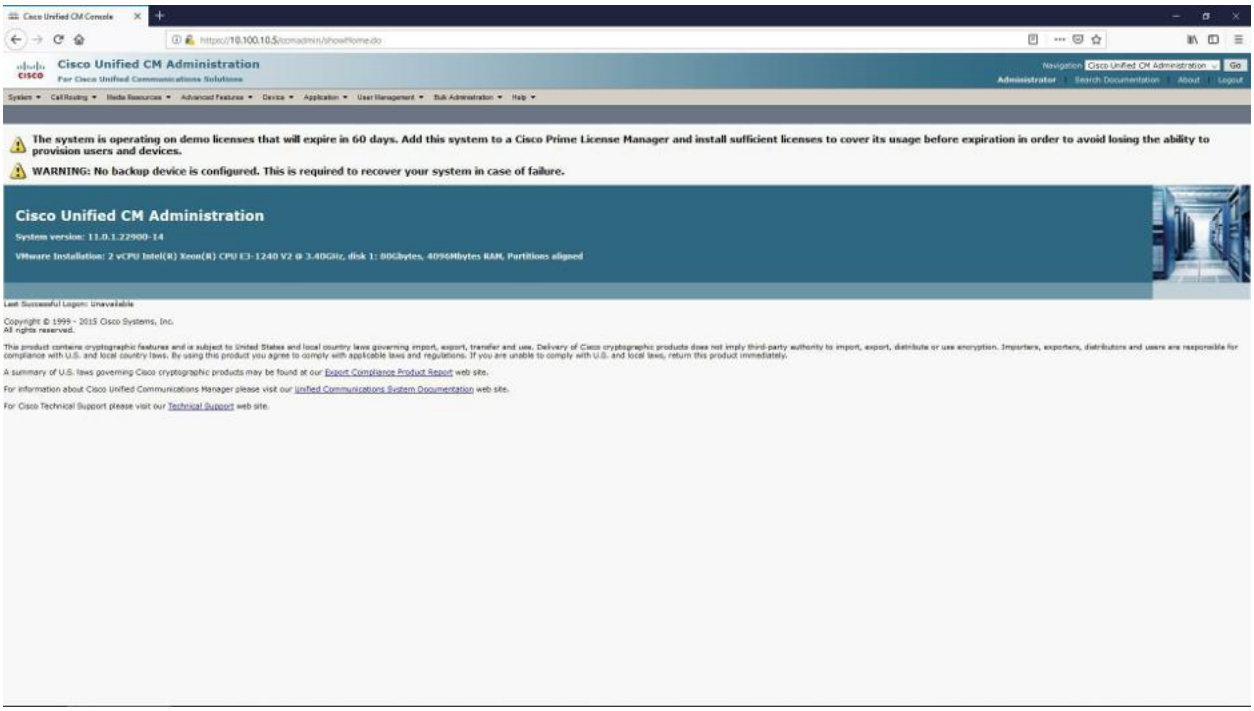


Figure 87: CUCM Initial Web Page

This is where you will do all your CUCM configuration. But first, let's test our SSH Access.

Access via SSH

The CUCM Server also has an SSH connection. This is necessary to do some system maintenance, like change the network information (IP, network mask, default gateway, DNS), change and test the NTP server configuration, test network connectivity and also check and repair the system database. To access it, open a regular SSH connection using your SSH client (like PuTTY, SecureCRT or other) directly to port 22 on CUCM. You'll need the administration credentials created during the system installation.

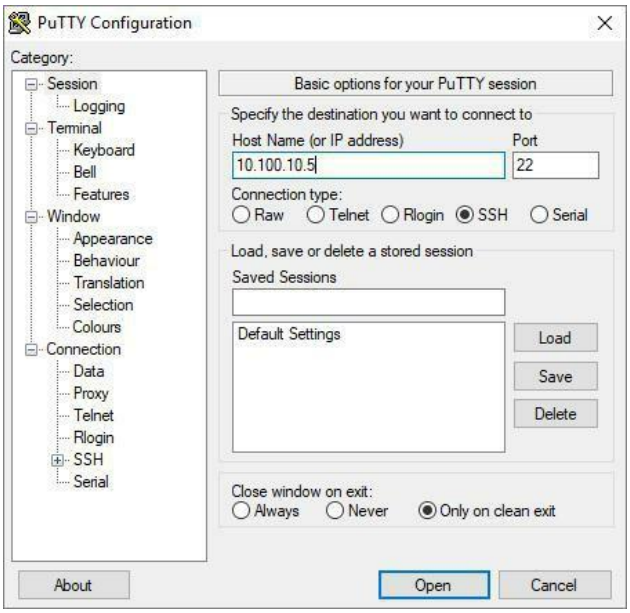


Figure 88: Accessing the CUCM SSH console via PuTTY

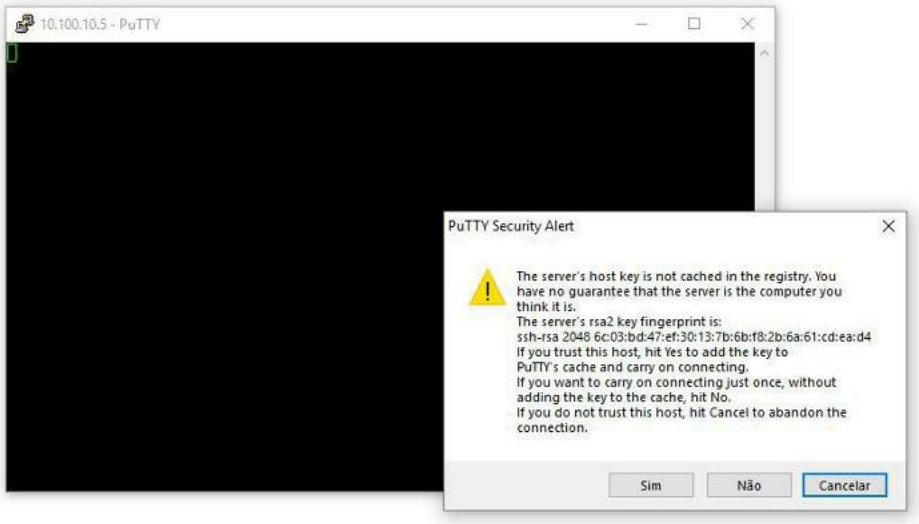


Figure 89: Accessing the CUCM SSH console via PuTTY

In the first access, accept the server host keys to proceed. Then, log in with the username and password created during the install process.

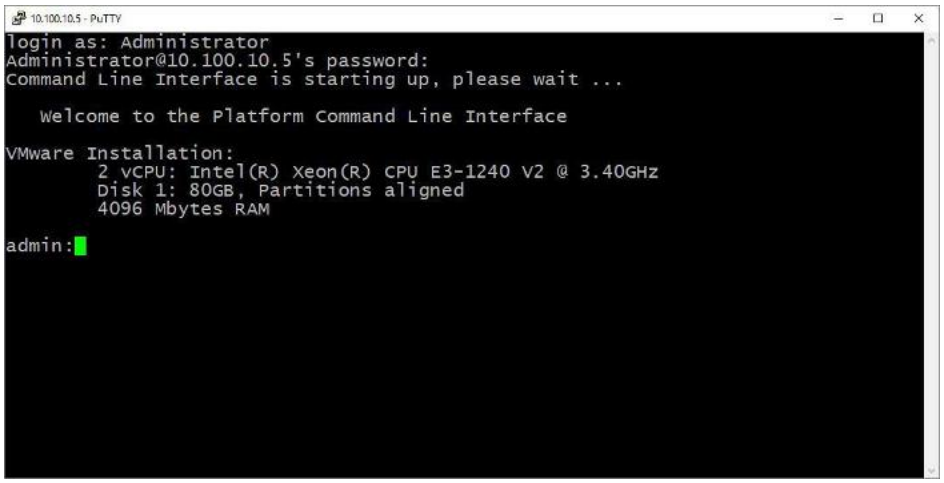


Figure 90: Accessing the CUCM SSH console via PuTTY

Despite being very similar to a regular Linux Server, this SSH shell won't provide you with Linux commands like ifconfig, ping or others available on a Bash environment. Cisco provides this shell with only specific CUCM commands. Some useful commands are:

utils dbreplication runtimestate	To check the Database status. Needs to be run on the CUCM Publisher.
utils network ping 10.20.3.4	Ping to host 10.20.3.4
utils ntp status	Verify NTP servers and status
utils ntp restart	Restart NTP service
show version active	Display the running CUCM version
show version inactive	Display the inactive CUCM version (if an upgrade has already happened on this server)
show network eth0	Display the network configuration
show date	Display the current clock and date
show status	Display general information like hostname, date and clock, timezone, CUCM version, uptime, CPU load, memory, disk usage
utils system shutdown	Shutdown the CUCM server
utils system restart	Restart the CUCM server
utils system switch-version	Change the CUCM active version, if an upgrade was done on the system

utils ntp config	Display the current NTP servers configured
utils ntp restart	Restart the NTP process
utils ntp status	Show the status of the NTP process

Table 5: some CUCM SSH commands available

You can also use the question mark "?" to discover all available commands, as in a Cisco router/switch.

More information on how to troubleshoot the database status are on the Appendix of this book.

CUCM Subscriber Installation

Preparing to create the CUCM Subscriber

Before starting the CUCM Subscriber server, you need to prepare the CUCM Publisher to receive it. To do it, on the CUCM Administration page, go to "System" > "Server" > "Find". You will see the CUCM Publisher server.

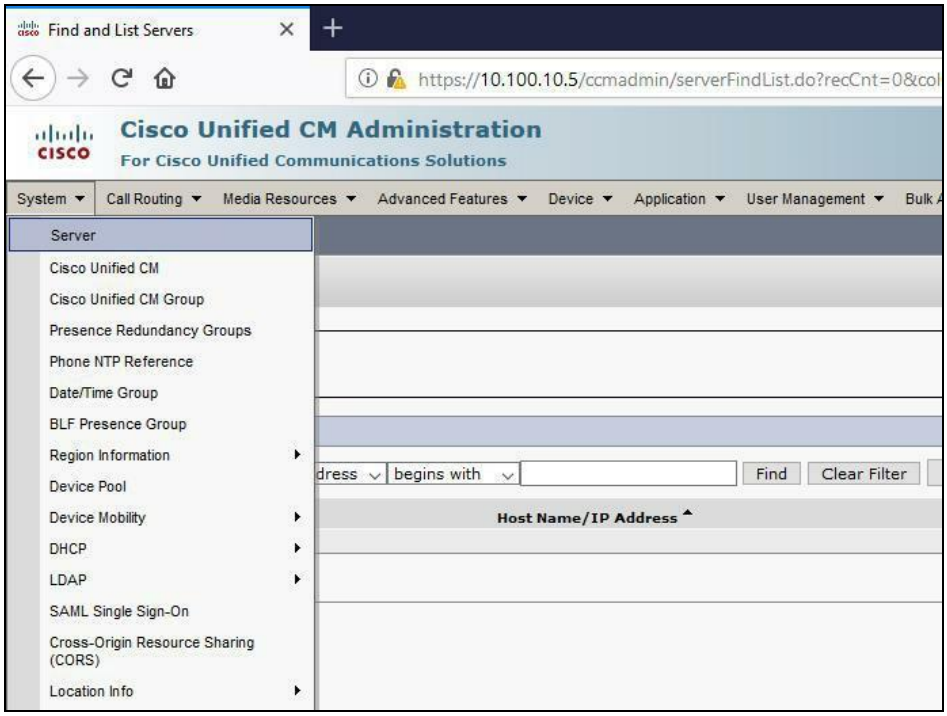


Figure 91: CUCM System > Server Menu

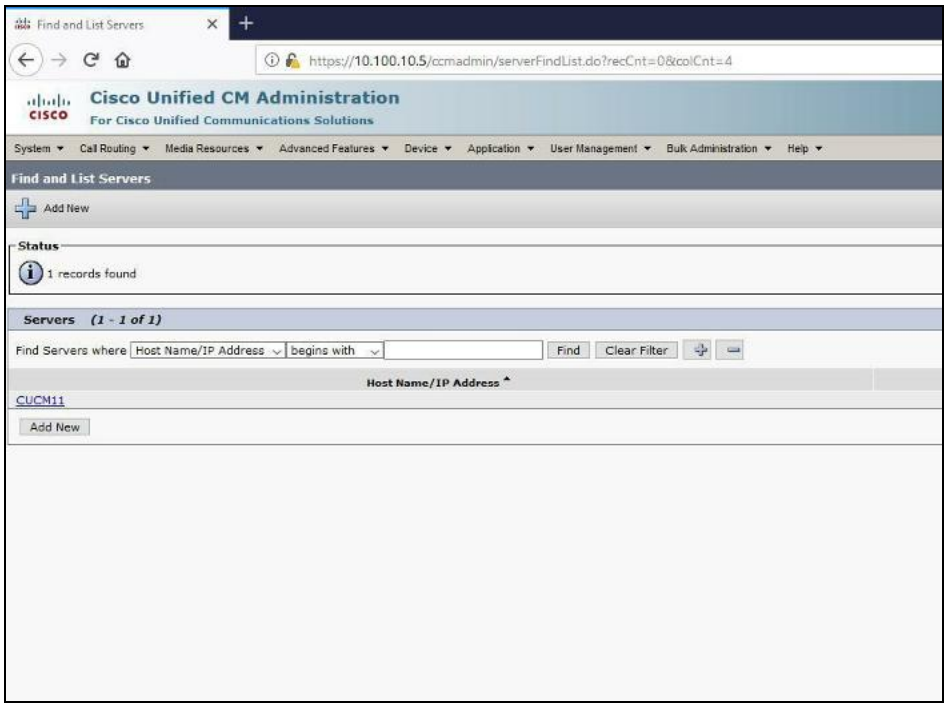


Figure 92: CUCM System > Server Menu

Click on the CUCM Publisher link, and then rename it to its own IP Address.

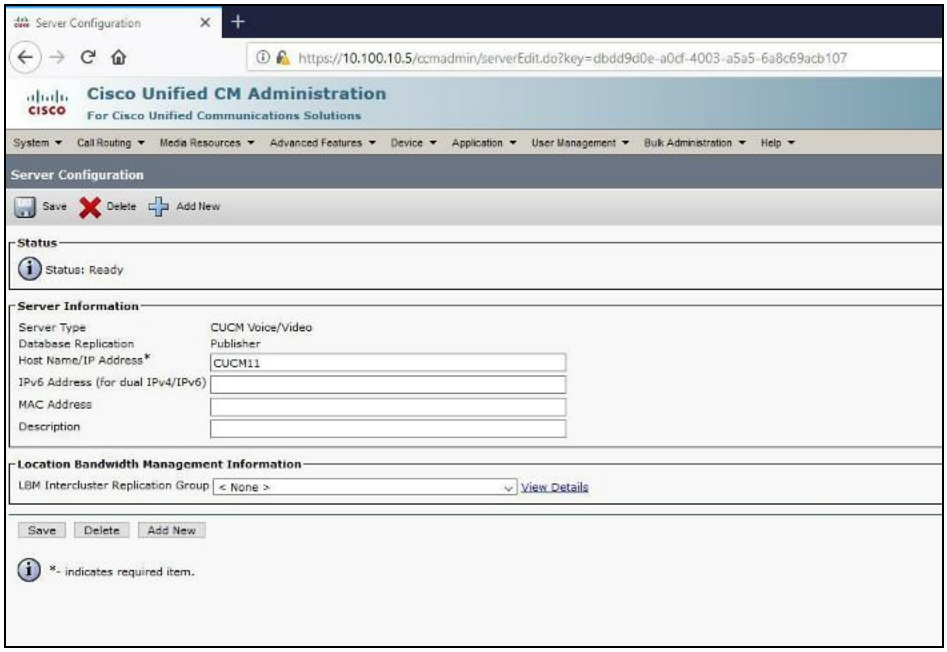


Figure 93: CUCM System > Server Menu > Publisher

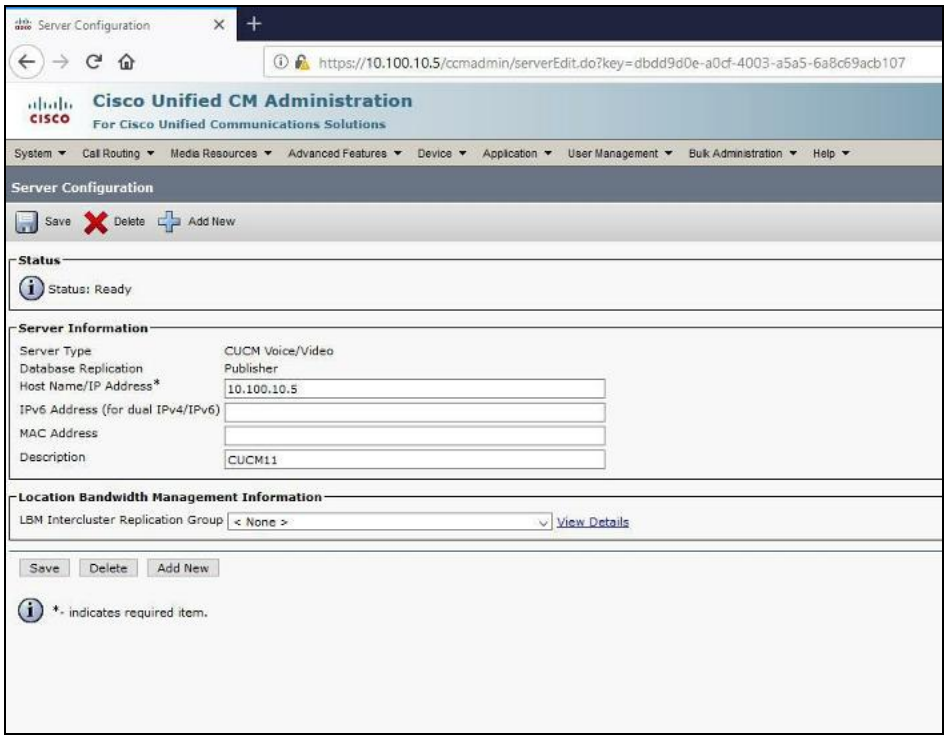


Figure 94: CUCM System > Server Menu > Publisher

Press the button “Save” to save this configuration. Now, let’s create our CUCM Subscriber server. Click “Add New” Button.



Figure 95: CUCM System > Server Menu > Add New

The server type is the default “CUCM Voice/Video”. Press “Next”.

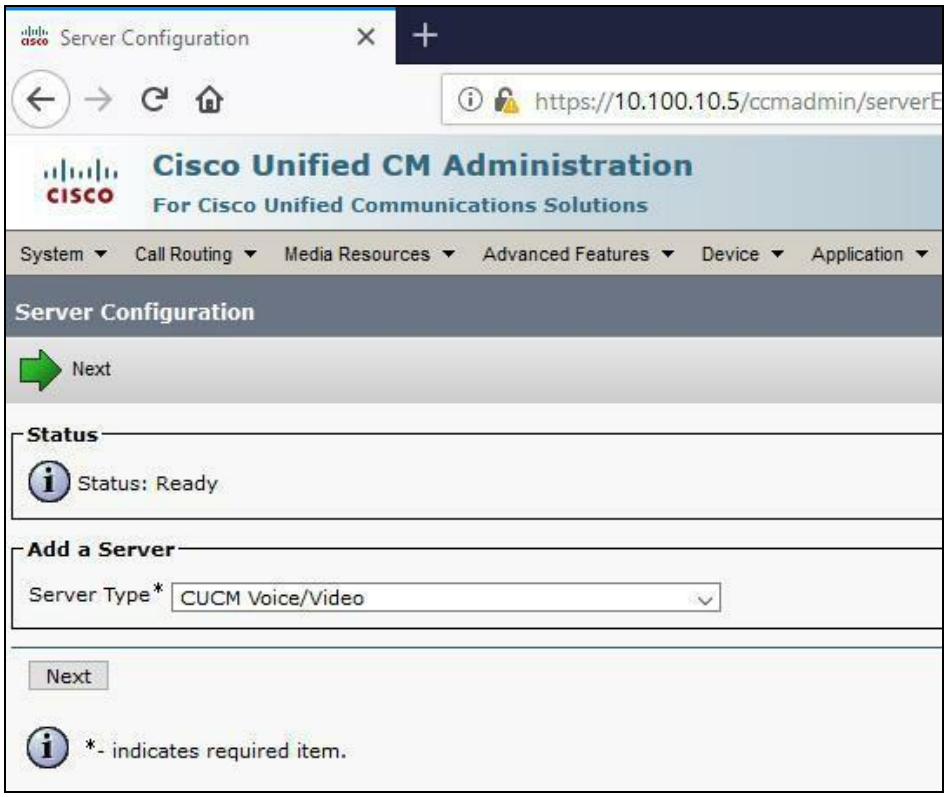


Figure 96: CUCM System > Server Menu > Add New > Server Type

Now, type the IP Address of your CUCM Subscriber server. If you want, also create a Description. In my example, I'm using 10.100.10.6 to my Subscriber.

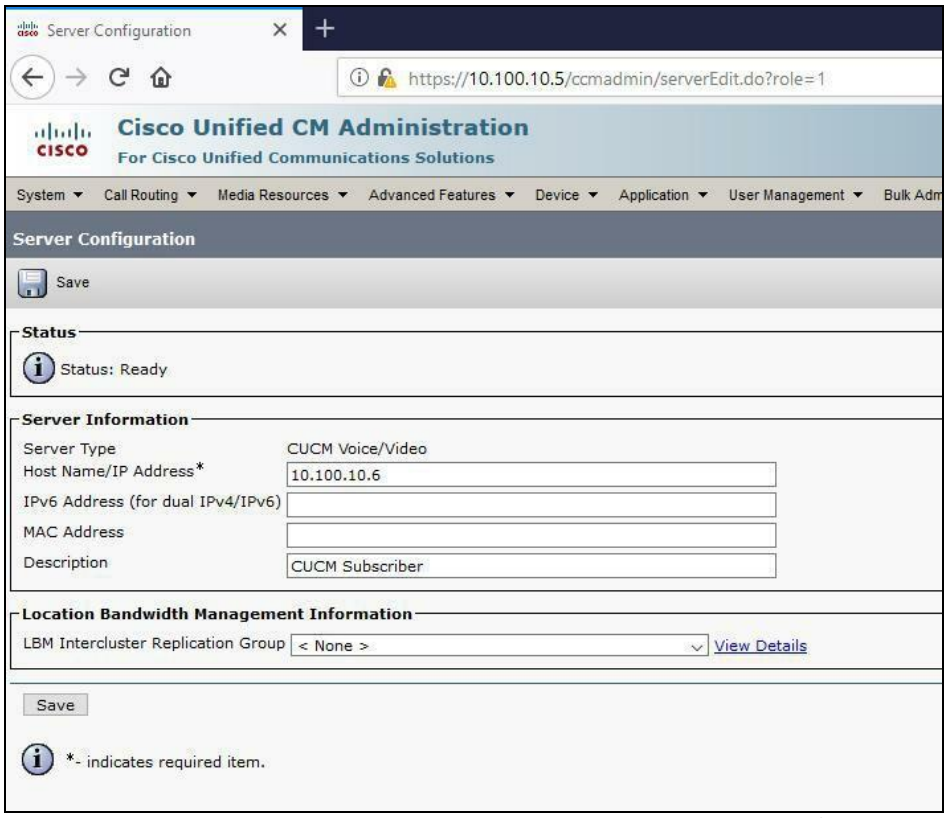


Figure 97: CUCM System > Server Menu > Add New > Server Information

Press “Save” and you’re done.

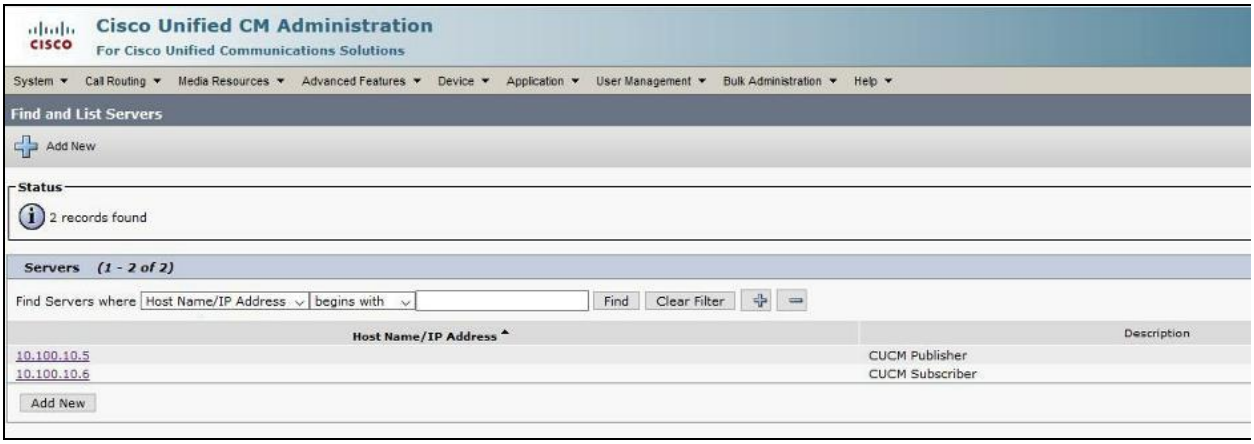


Figure 98: CUCM System > Server Menu > Find

Now you can proceed to the CUCM Subscriber installation.

Create the CUCM Subscriber and start it

Create the CUCM Subscriber Virtual Machine with the same hardware configuration as you did on the CUCM Publisher, then, start the VM.

The CUCM Subscriber creation is almost the same as the CUCM Publisher. All the answers you used on the Publisher installation are practically the same on the Subscriber, except the server IP Address (of course) and the “First Node Configuration Window”, where you should select “No”.



Figure 99: First Node Configuration Window on Subscriber

The installation will warn you that you need to configure the CUCM Subscriber on the First Node, as we did already.

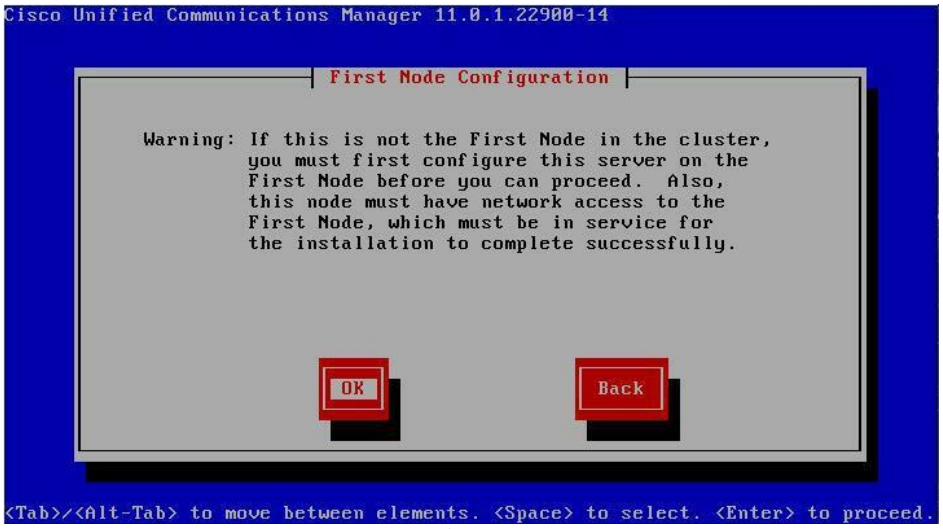


Figure 100: First Node Configuration Window on Subscriber

Now the installer will warn you that CUCM Subscriber needs to have network connectivity to CUCM Publisher during the installation process.

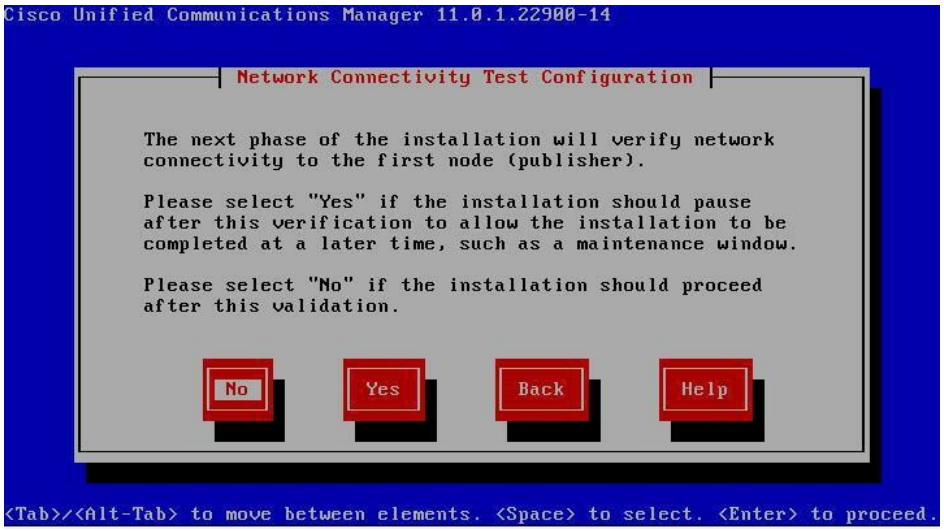


Figure 101: First Node Network Connectivity Test on Subscriber

Here you need to type the Publisher Hostname, Publisher IP Address and Database Security Password to proceed.

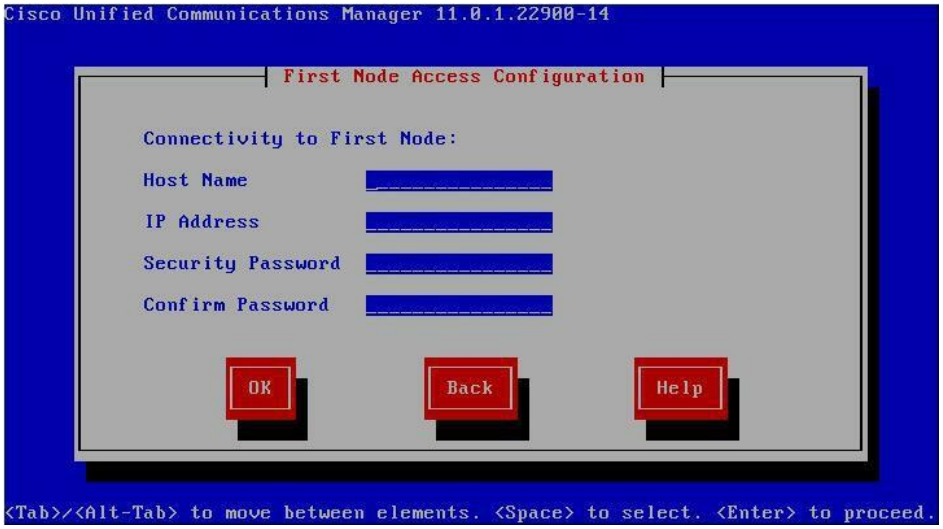


Figure 102: First Node Access Configuration on Subscriber

The installation will proceed. If any error happens, the system will advise you which configuration are missing to complete the Subscriber installation.

Start the Services

The CUCM server starts with all system services stopped. So you need to enable them manually. If you're installing it for lab purposes, I recommend starting all services at once. In a production environment, you need to start only the services you want.

To start the Services, at the top right corner of CUCM screen, select “Cisco Unified Serviceability” and then click “Go”.

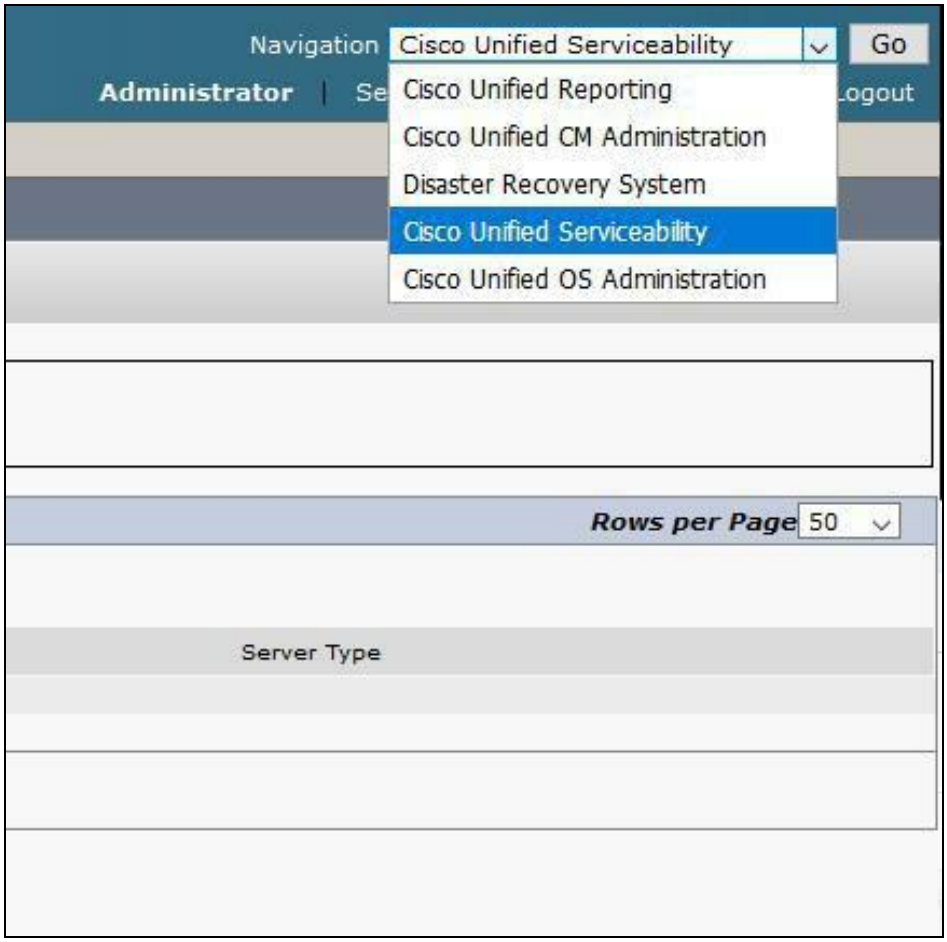


Figure 103: Cisco Unified Serviceability Menu

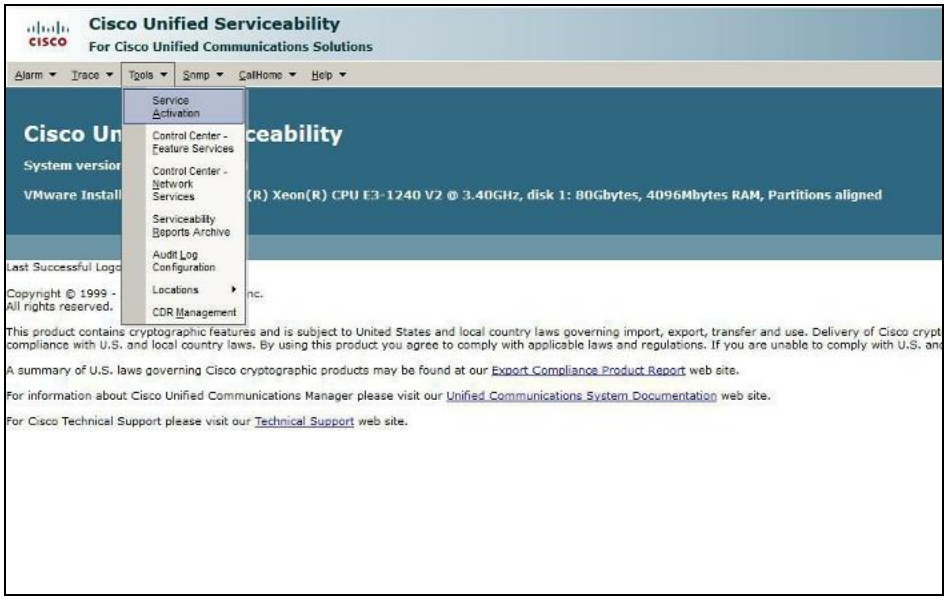


Figure 104: Cisco Unified Serviceability Service Activation

Select the server you want to enable the services, then click “Go”.

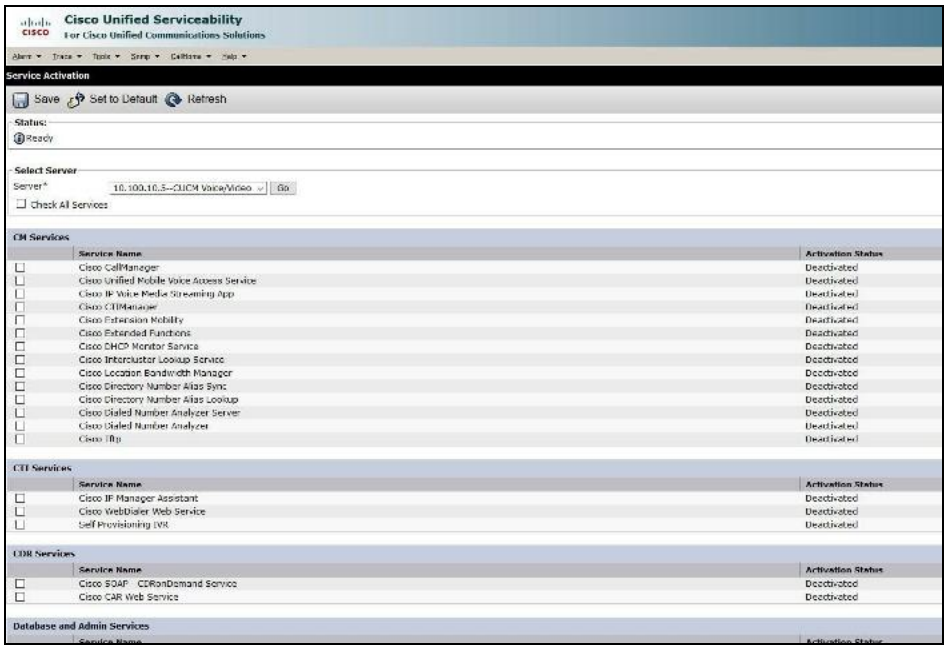


Figure 105: Cisco Unified Serviceability Service Activation

If you don’t know exactly what you need, I recommend you enable all services except the Cisco DHCP Monitor Service, as usually the DHCP Server is not used on the CUCM Server. For lab purposes, you can enable all services. Just click on “Check All Services” and click “Save”. You need to repeat this process to both servers.

Some of the primary services are:

Service	Functionality
Cisco CallManager	Register the phones, place and receive calls
Cisco Tftp	Provide XML configuration files to Cisco Phones via TFTP protocol
Cisco DHCP Monitor Service	DHCP Server to Phones. Not necessary, can be configured on other network devices
Cisco Extension Mobility	Enable the server to act as a Extension Mobility server (covered in Chapter 14)
Cisco Dialed Number Analyzer Server and Cisco Dialed Number Analyzer	Enable the Cisco DNA, a service useful to troubleshoot call errors.

Table 6: CUCM Main services

Now our servers are ready. In the next chapter, we will start the basic configurations.

CHAPTER 4 - INITIAL CONFIGURATIONS

After the installation, we need to proceed to some basics configurations on our CUCM environment.

License Install

The license on a CUCM system is not installed on the CUCM itself, but on another server called “Prime License Manager”. This server is installed automatically as part of the installation of Cisco Unified Communications Manager and Cisco Unity Connection. You may choose to run Cisco Prime License Manager on one of these servers (CUCM or CUC) or to install a dedicated server only for licensing.

I usually don’t install a dedicated server to run Cisco PLM. But if you decide to do it, the hardware requirements are straightforward. Follow what’s necessary on version 11.0:

Requirement	Details
CPU	1 vCPU with 1800 Mhz reservation
Memory	4 GB (RAM) with 4 GB reservation
Hard Drive	1 - 50 GB disk

Table 7: Hardware Requirements for Cisco PLM 11.0

To install the licenses on CUCM, open your server and click on “Cisco Prime License Manager”, or open directly the URL:

https://CUCM_IP_ADDRESS/elm-admin)

Technet24

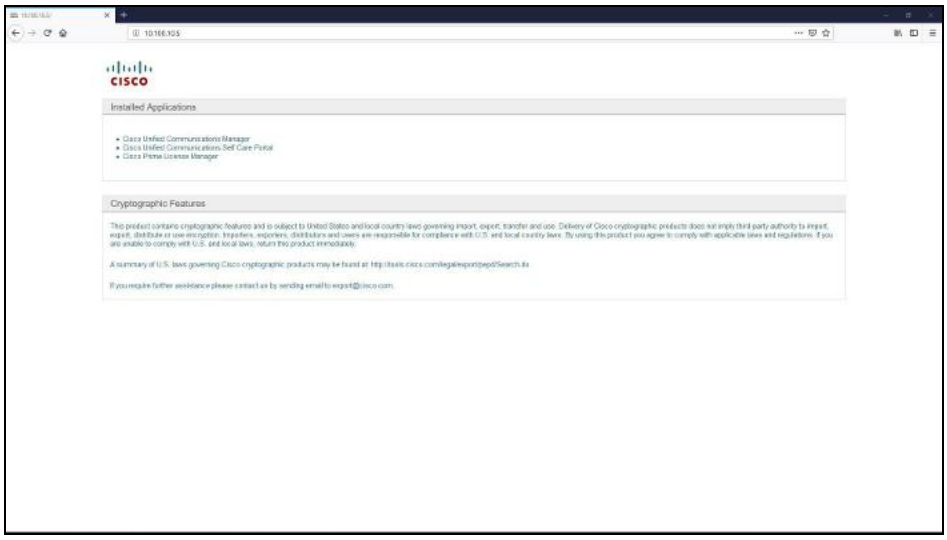


Figure 106: CUCM Inicial Web Screen

In the past, I had some problems accessing this ELM site using Google Chrome and Internet Explorer, it only worked on Mozilla Firefox. But I think this problem is solved now.

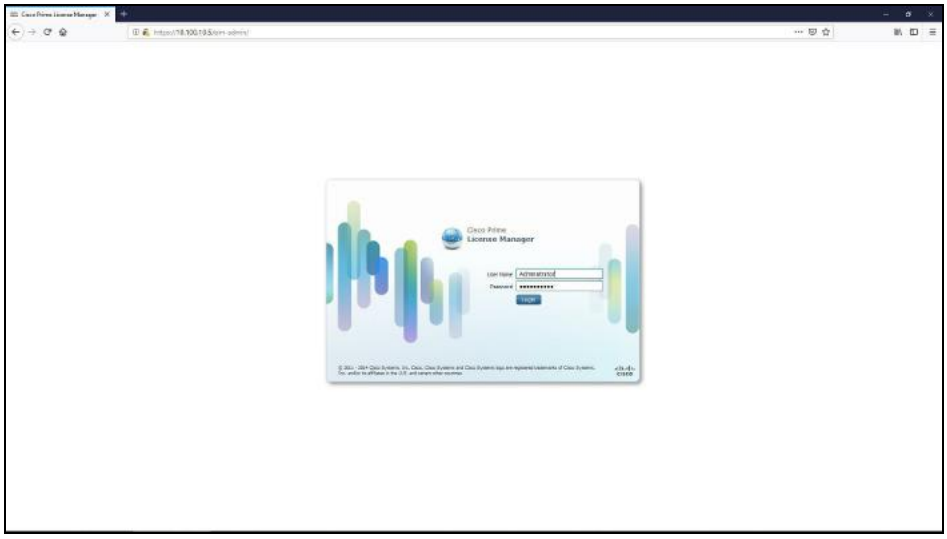


Figure 107: Cisco ELM

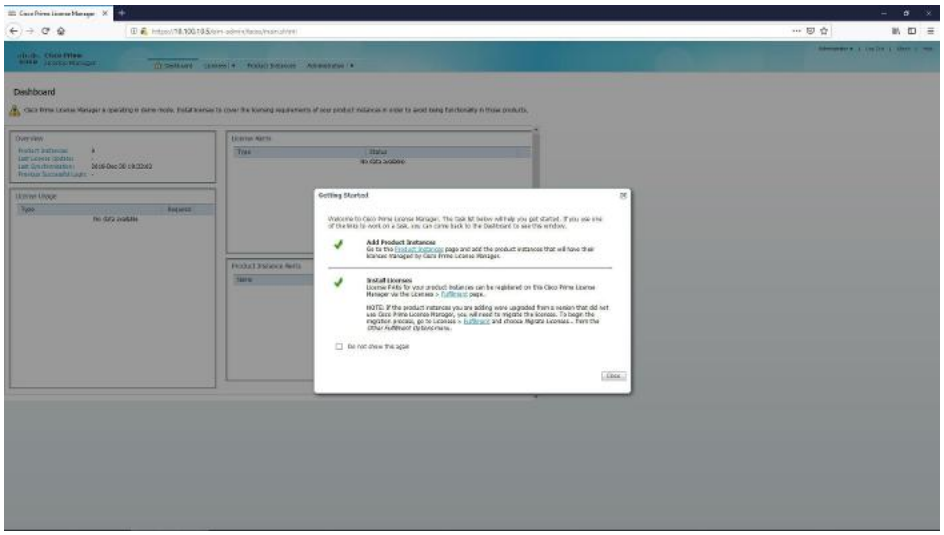


Figure 108: Cisco PLM Inicial Screen

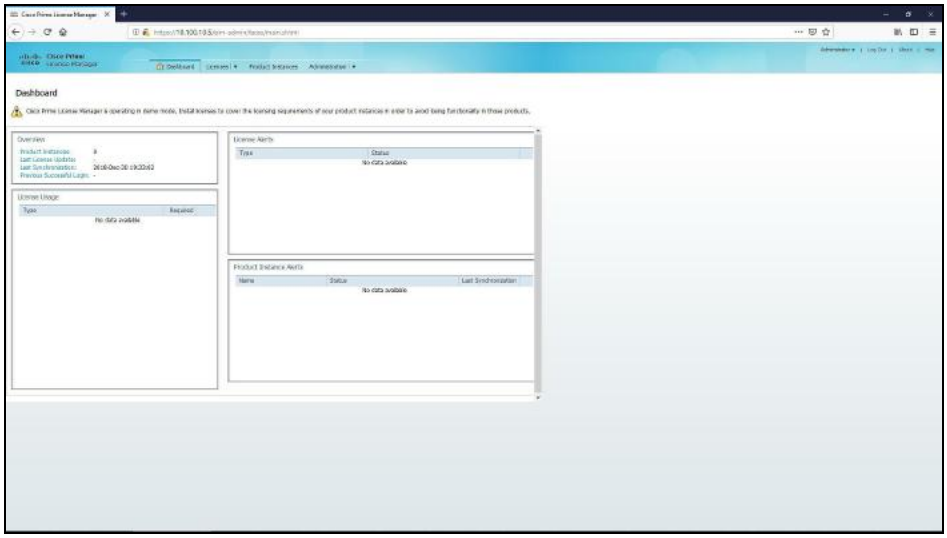


Figure 109: Cisco PLM Dashboard

To synchronize the CUCM with the PLM, go to “Product Instances”, then click “Add”.

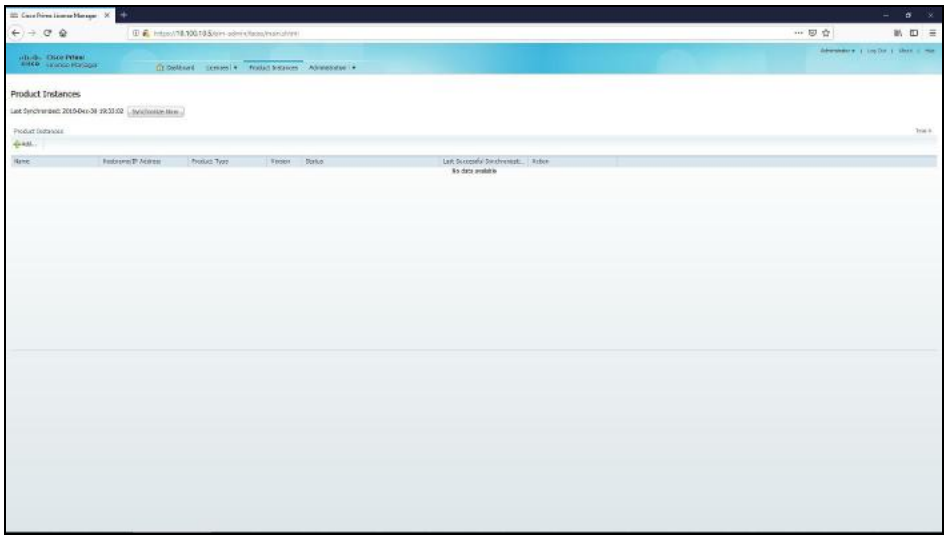


Figure 110: Cisco PLM Product Instances

Now, type the product (CUCM) information.

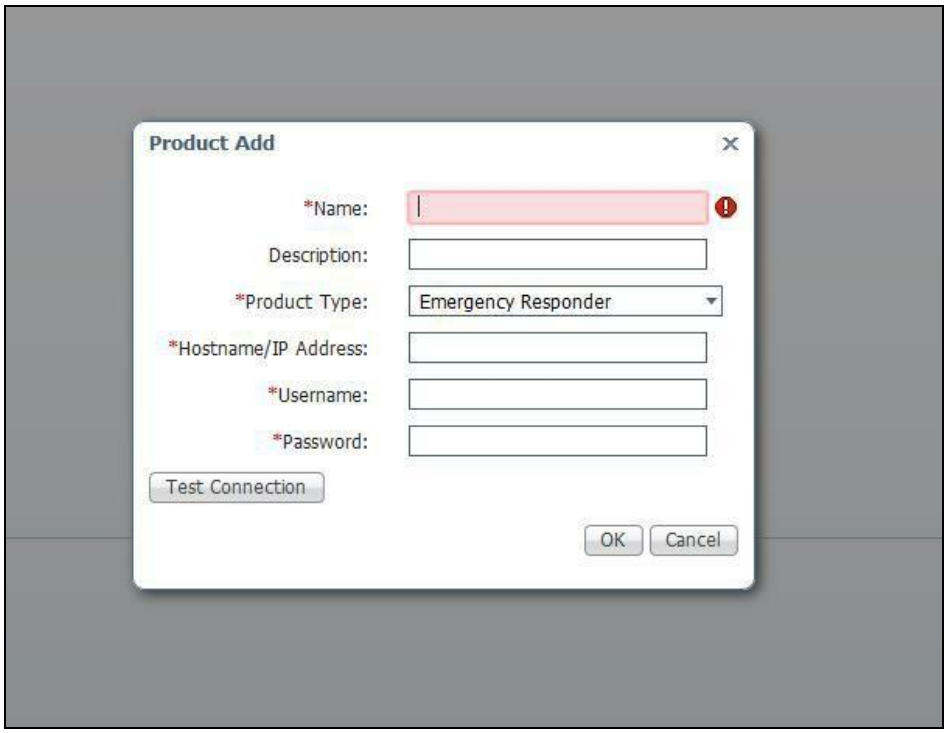


Figure 111: Cisco PLM Add Product

You can test the product synchronization with the button “Test Connection” to validate the credentials.

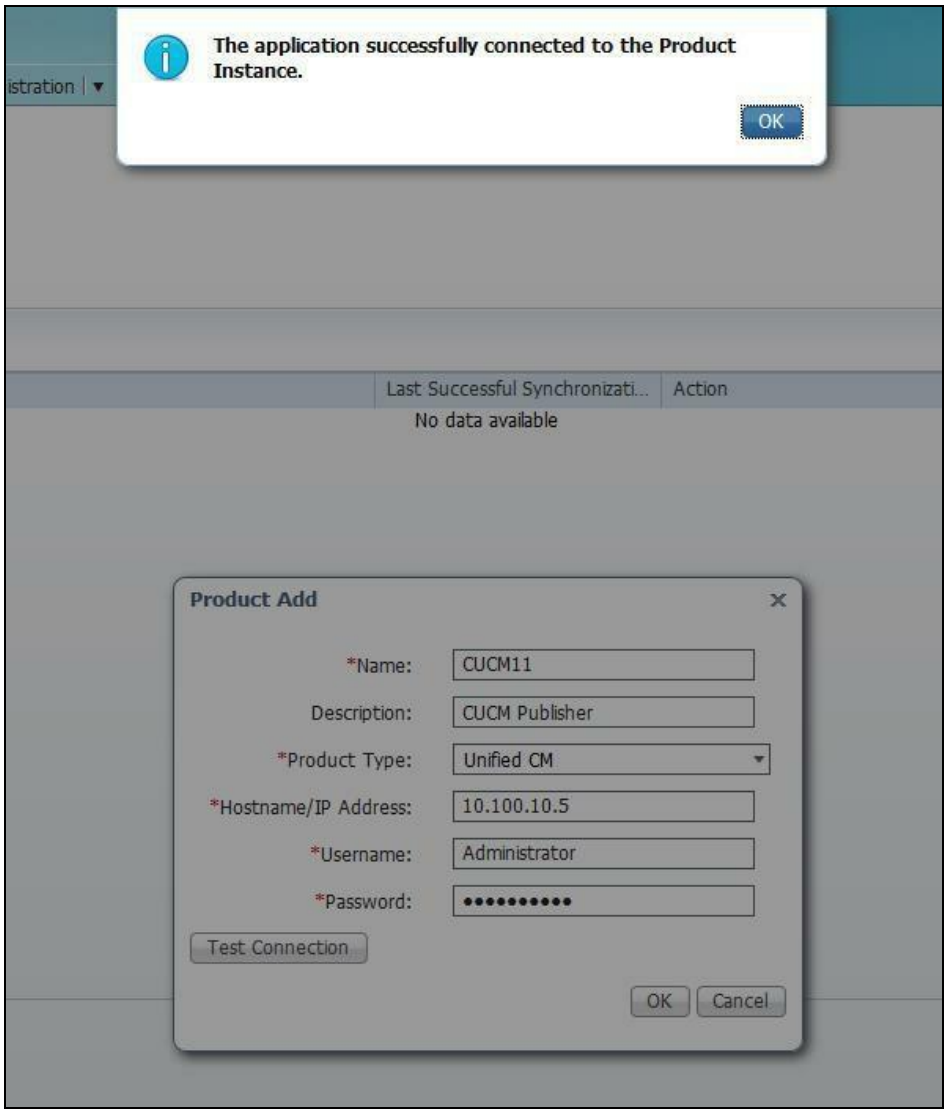


Figure 112: Cisco PLM Add Product Instance

After that, the CUCM will be listed on the Product Instances. Click "Synchronize Now" to refresh and validate the connection.

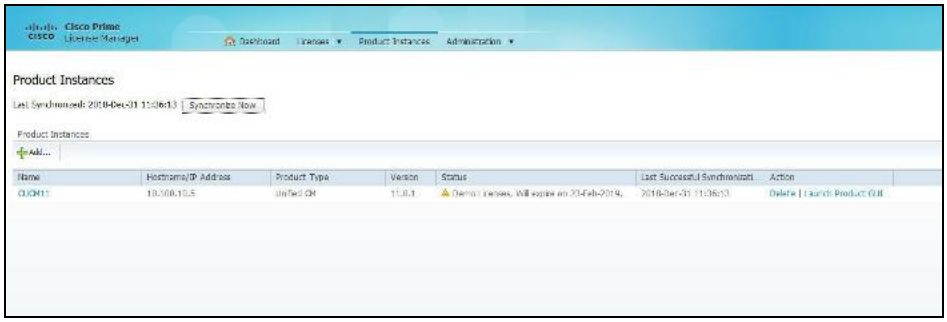


Figure 113: Cisco PLM Product Instances

There are two methods to install the license: Online (via PAK) or Offline (via Generate Request and Fulfill Licenses from File).

If your Cisco PLM has access to the Internet, the online process is more comfortable and faster. To do it, click on the first option on the left, “Fulfill the Licenses from PAK”. This will open a window to insert the PAK number.

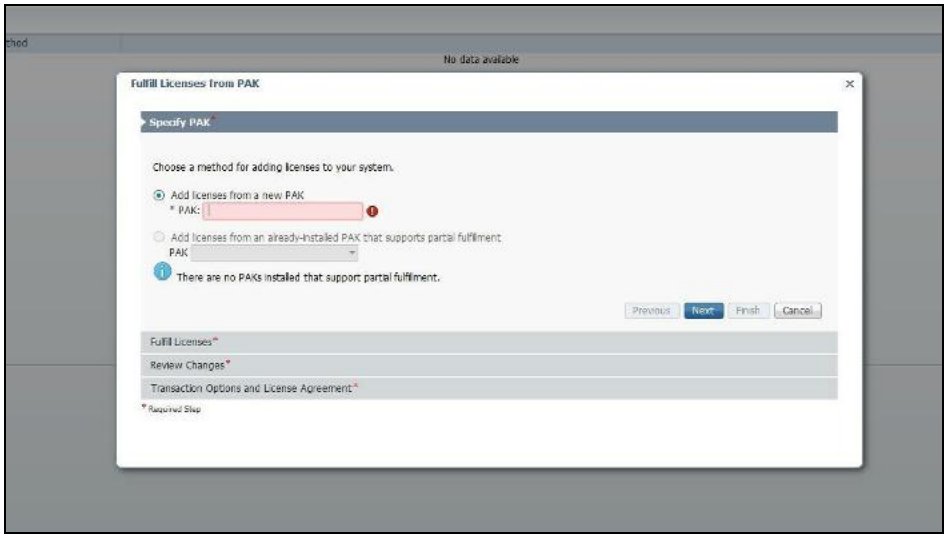
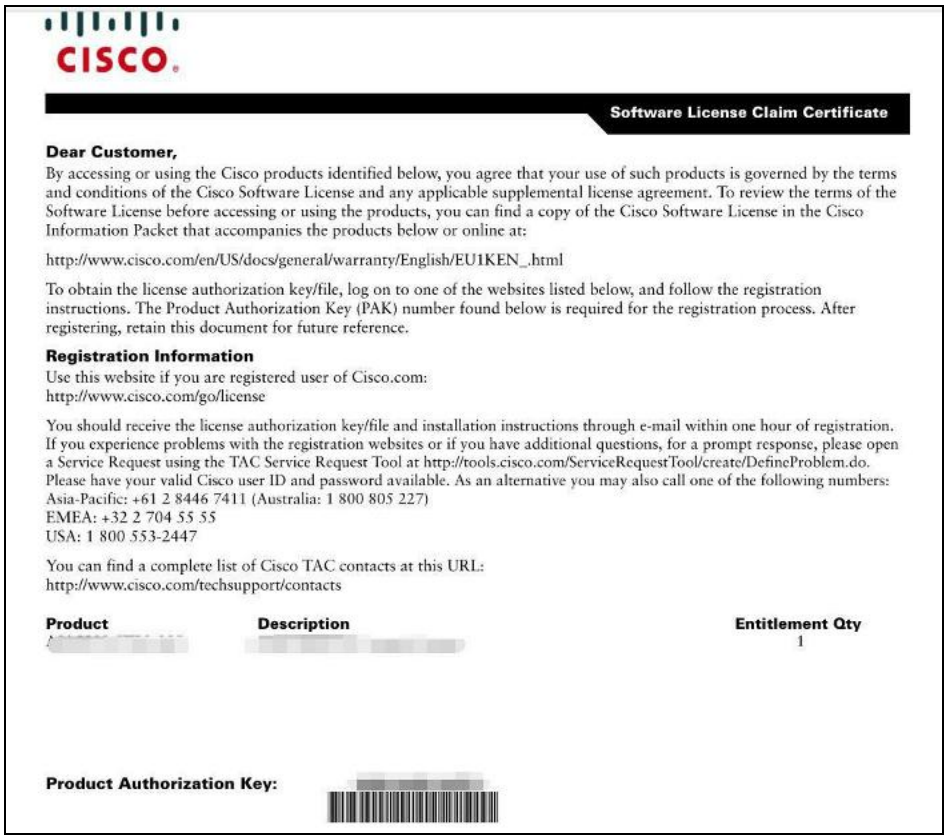


Figure 114: Cisco PLM Add License via PAK

Add the PAK number in this window and then follow the wizard to load these licenses. You’ll need a Cisco.com login to complete this process.

What is PAK Number?

PAK Number is a code you receive when you buy the licenses from Cisco. Typically, there is a printed paper with this code, as below:



Software License Claim Certificate

Dear Customer,

By accessing or using the Cisco products identified below, you agree that your use of such products is governed by the terms and conditions of the Cisco Software License and any applicable supplemental license agreement. To review the terms of the Software License before accessing or using the products, you can find a copy of the Cisco Software License in the Cisco Information Packet that accompanies the products below or online at:

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

To obtain the license authorization key/file, log on to one of the websites listed below, and follow the registration instructions. The Product Authorization Key (PAK) number found below is required for the registration process. After registering, retain this document for future reference.

Registration Information

Use this website if you are registered user of Cisco.com:
http://www.cisco.com/go/license

You should receive the license authorization key/file and installation instructions through e-mail within one hour of registration. If you experience problems with the registration websites or if you have additional questions, for a prompt response, please open a Service Request using the TAC Service Request Tool at http://tools.cisco.com/ServiceRequestTool/create/DefineProblem.do. Please have your valid Cisco user ID and password available. As an alternative you may also call one of the following numbers:
Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

You can find a complete list of Cisco TAC contacts at this URL:
http://www.cisco.com/techsupport/contacts

Product	Description	Entitlement Qty
		1

Product Authorization Key:

Figure 115: Cisco PAK File

But if your PLM server doesn't have access to the Internet, you need to install the license using the Offline method. The process (today) is:

- Go to "Other Fulfillment Options" > "Generate License" to obtain a code;
- Copy this code to a TXT file;
- Go to the Cisco Web Site and Cisco Software Central (https://software.cisco.com/) and select "Tradicional Licensing";
- On the "Product License Registration" site, select "Add New PAKs/Tokens";
- Follow the wizard to load the PAK file;
- Then, associate the PAK.

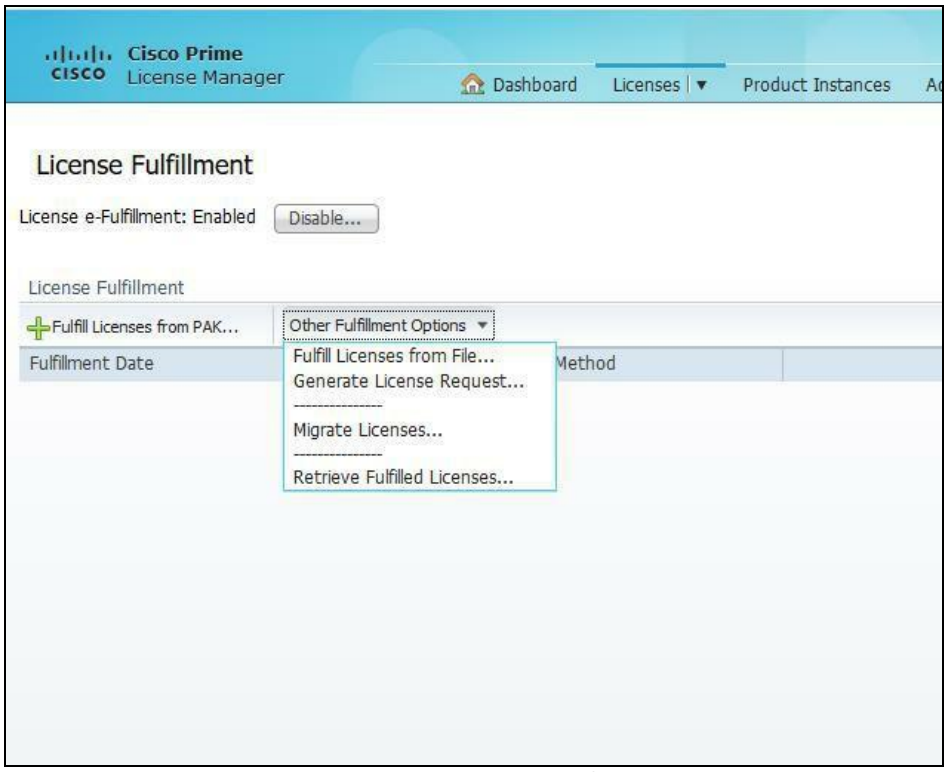


Figure 116: Cisco PLM Other Fulfillment Options

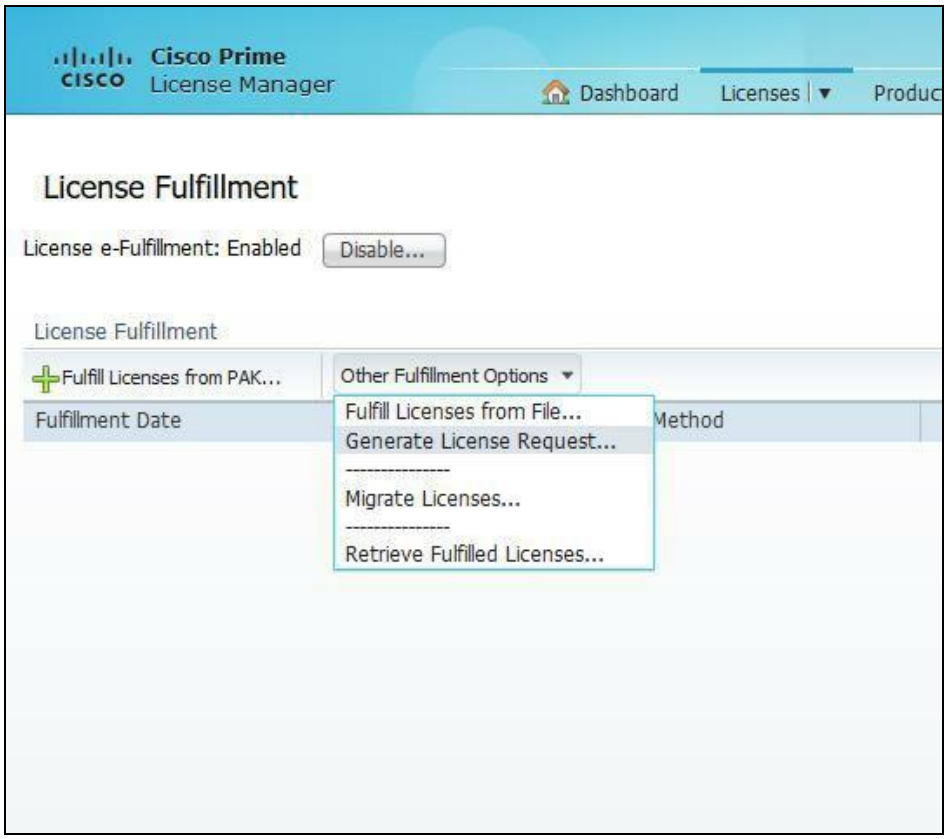


Figure 117: Cisco PLM Generate License Request

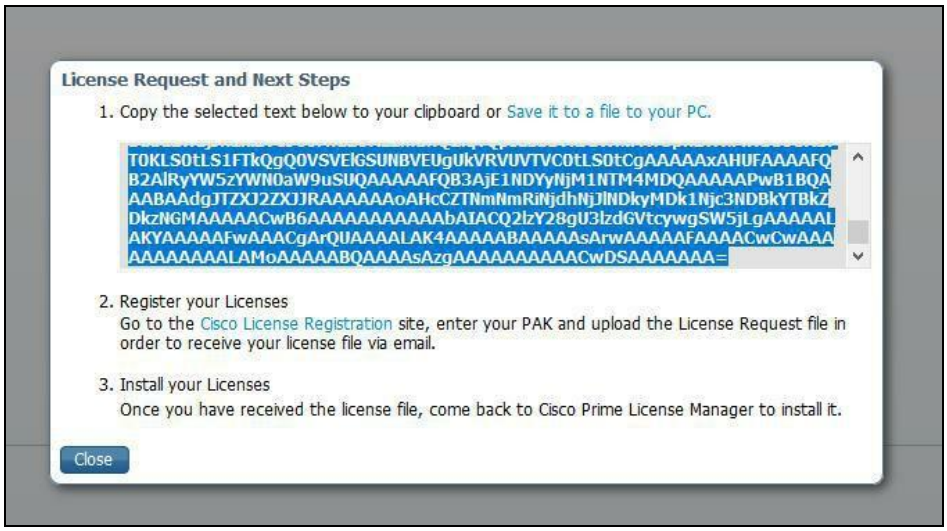


Figure 118: Cisco PLM License Request

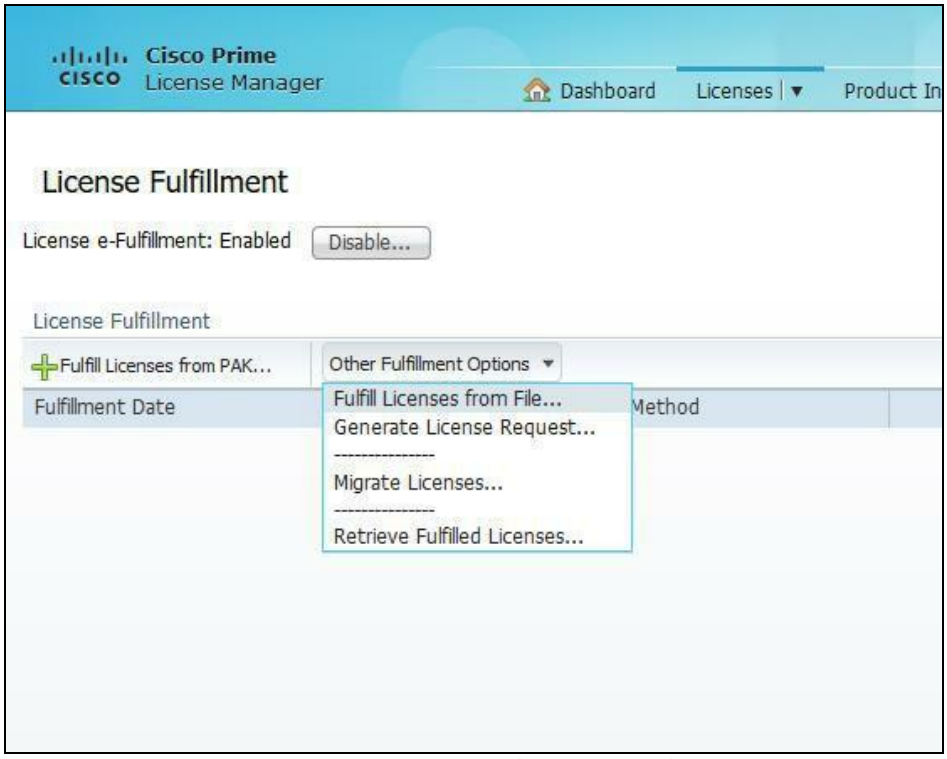


Figure 119: Cisco PLM Fulfill Licenses from File

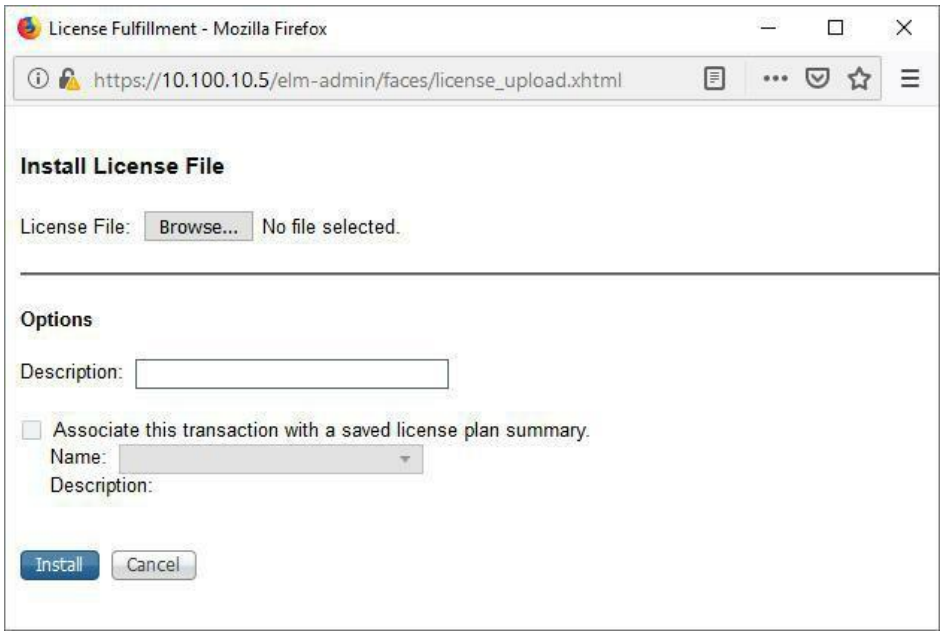


Figure 120: Cisco PLM Install License File

Hostname/IP Address

After the installation, the CUCM starts with some configurations relying on DNS resolution, and this is a bad idea. More than that, this is by far one of the most common points of failure: if a problem occurs on DNS servers, this can affect the telephony system in many ways.

So, it's highly recommended to remove this DNS dependency. To do it, we need to remove anything related to DNS entries or hostnames and replace it with IP Addresses. We did part of this configuration in chapter 3, section "Preparing to create the CUCM Subscriber". If you haven't done this process, you need to:

- Go to CUCM Admin Page (https://CUCM_IP_ADDRESS/ccmadmin/);
- Menu System > Server;
- Click "Find";
- Click on your server hostname;
- Change it to the server IP Address;
- Create a Description (optional);
- Click "Save" to finish.

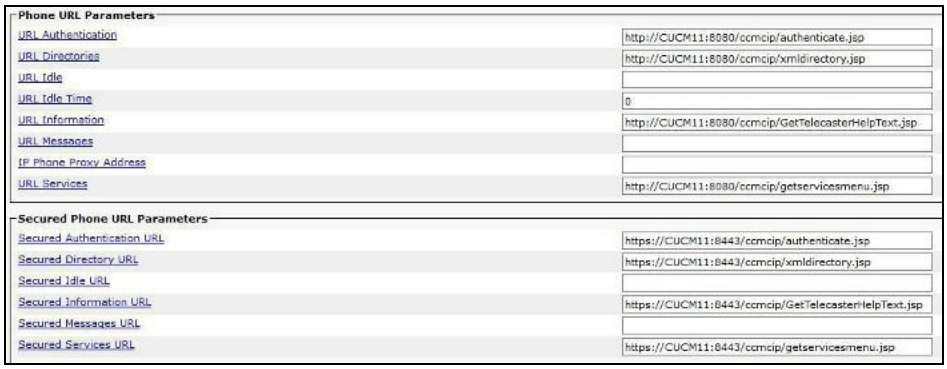


Figure 121: CUCM Server Edit

Repeat this process to all subscribers servers.

The other configurations using DNS dependency are in Enterprise Parameters. Go to:

- Menu System > Enterprise Parameters;
- Look for the following options:
    - URL Authentication
    - URL Directories
    - URL Information
    - URL Services
    - Secured Authentication URL
    - Secured Directory URL
    - Secured Information URL
    - Secured Services URL

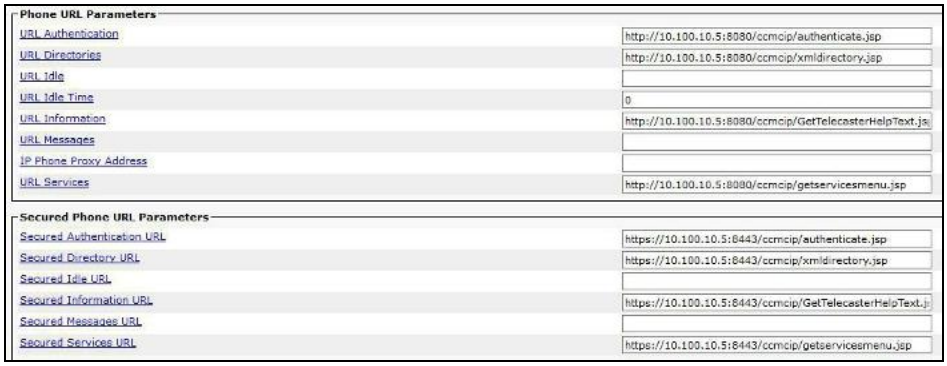


Figure 122: CUCM Enterprise Parameters

All those options will be pointing to the CUCM Publisher hostname you have created during the system installation. Change all to the IP Address of the CUCM instead.

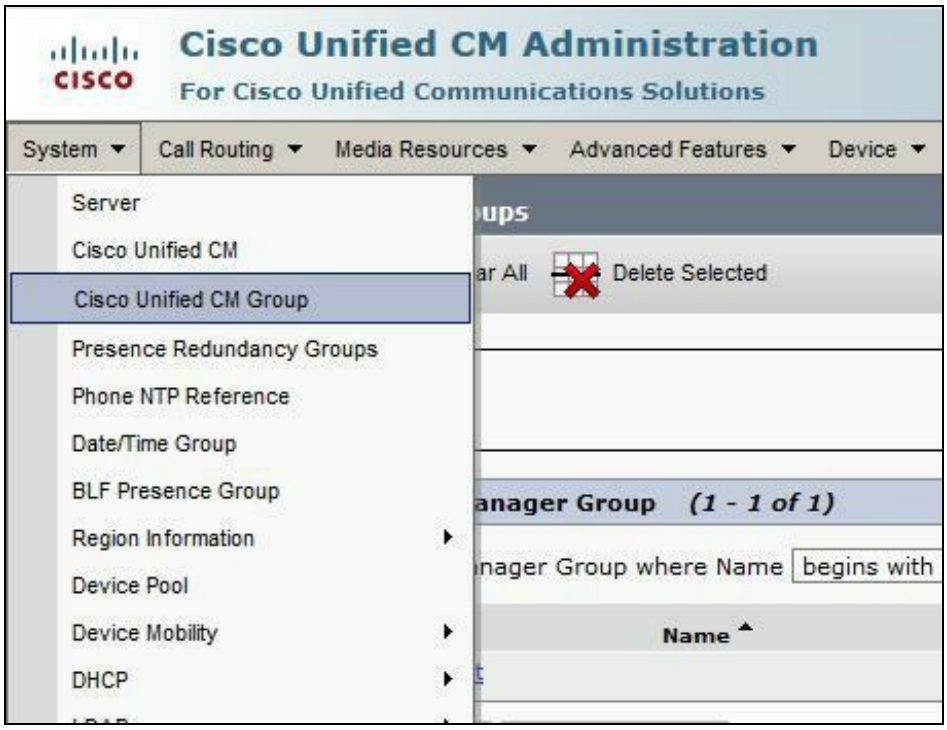


Figure 123: CUCM Enterprise Parameters

In my example, I changed the hostname “CUCM11” to my Publisher IP “10.100.10.5”.

CUCM Groups

CUCM Groups enables you to create the CUCM groups where the phones will register and in which order. For example, you can create a CUCM Group “PUBLISHER-FIRST”, where your CUCM Publisher is the first on your list and other “SUBSCRIBER-FIRST” with the Subscriber as the first option.

Let’s imagine a company with three sites: Site A (with Publisher Server), Site B (with Subscriber Server 01) and Site C (with Subscriber Server 02). We can create the following CUCM Groups:

Location	CUCM Group	First CUCM	Second CUCM	Third CUCM
Site A	SiteA_cmg	Publisher	Subscriber 01	Subscriber 02
Site B	SiteB_cmg	Subscriber 01	Subscriber 02	Publisher
Site C	SiteC_cmg	Subscriber 02	Publisher	Subscriber 01

Table 8: CUCM Groups with CUCM order

With this configuration, you’ll have a redundant topology. You need also

make sure that phones will primarily register on the most closer CUCM available, especially if is there LAN connectivity between a CUCM server and the phones. To create CUCM Groups, go to Menu System > Cisco Unified CM Group.

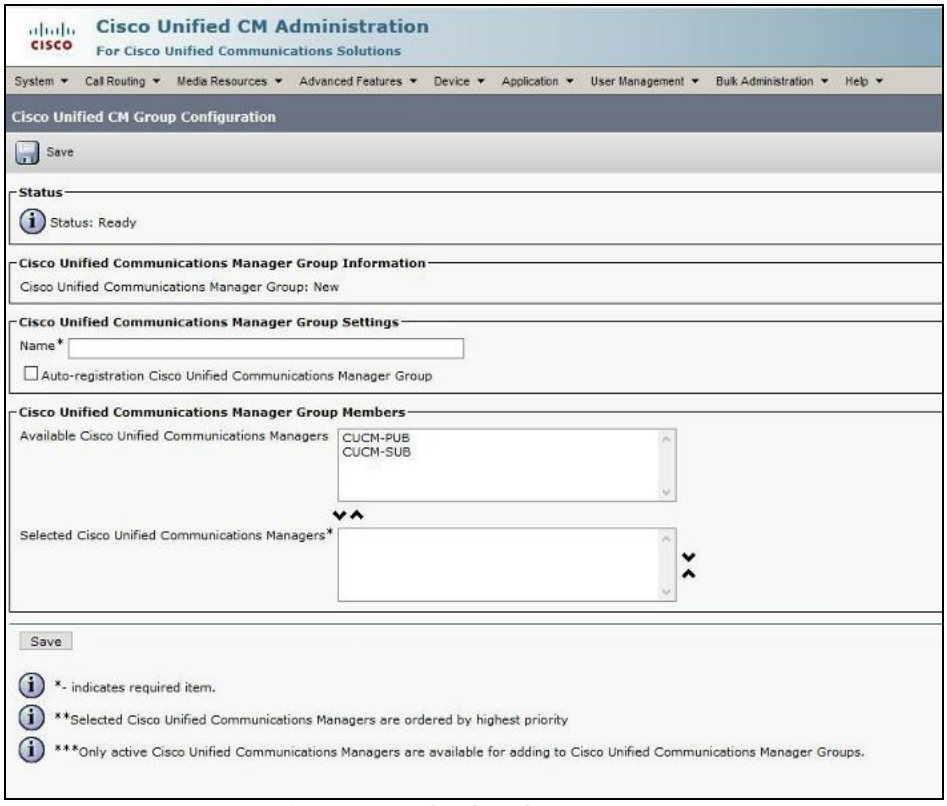


Figure 124: CUCM Groups Menu

Click Add New and create how many CUCM Groups you need. Select the CUCM Servers and click on the Down Arrow to move them from the box “Available Cisco Unified Communications Managers” to the box “Selected Cisco Unified Communications Managers”.

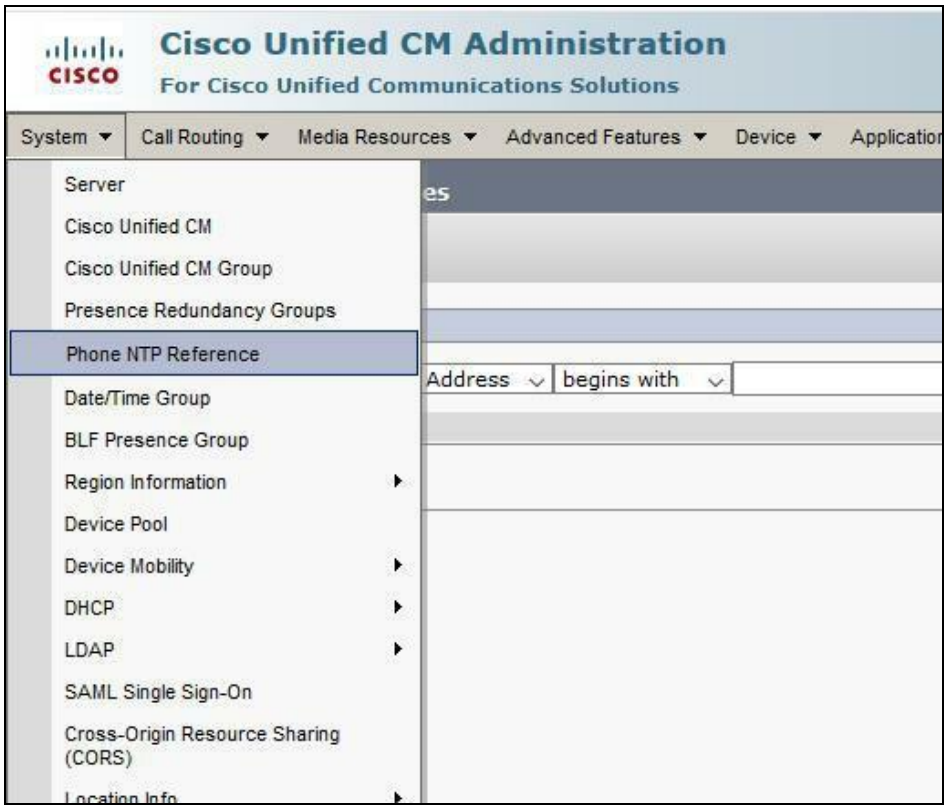


Figure 125: CUCM Group creation window

NTP Reference

NTP Reference is used to create NTP servers for Phones. We have created some NTP server reference to the CUCM server during the server installation. However, this configuration applies only to the CUCM server itself. To provide NTP reference to Cisco Phones, we need to insert these NTP references here.

You can use the same NTP servers you have used during the CUCM installation.

To create the NTP reference, go to “System” > “Phone NTP Reference”.

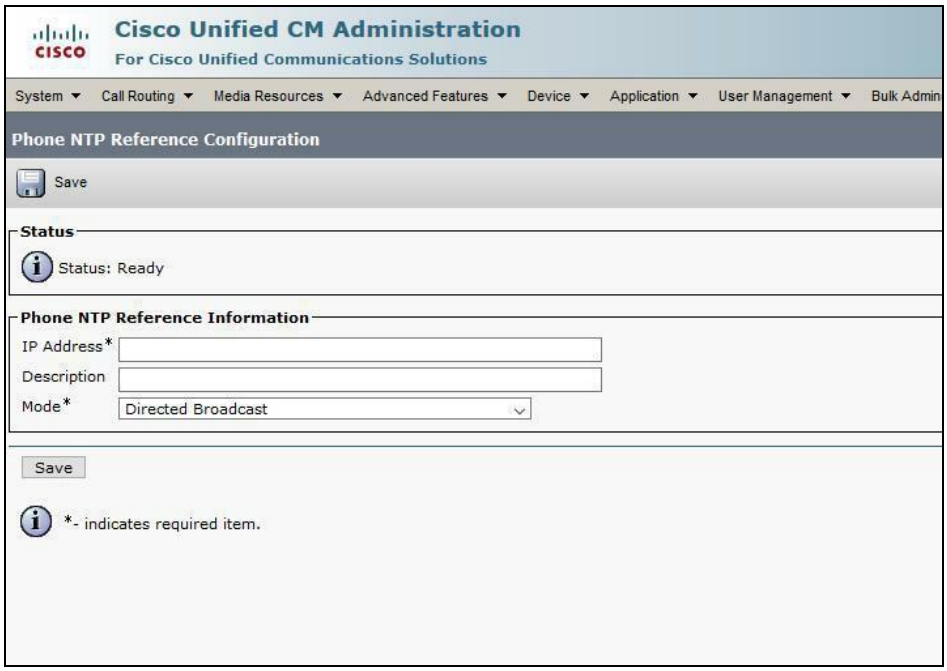


Figure 126: Phone NTP Reference Menu

Now, click “Add New”. Type the IP Address of your NTP Reference, a description (optional), and click “Save”.

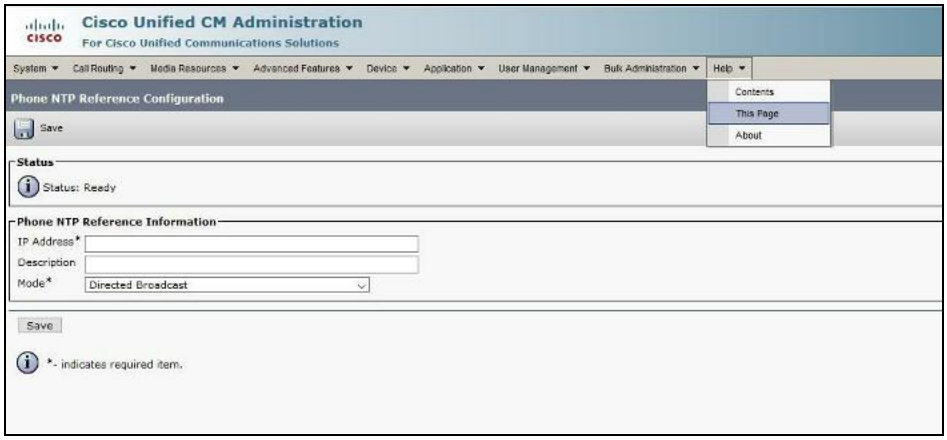


Figure 127: Phone NTP Reference creation

About the NTP Mode, you can select any you want. But if you would like more details, I'll take the opportunity to introduce you to the CUCM Help Menu. On the last Menu Option, click “Help” > “This Page”.

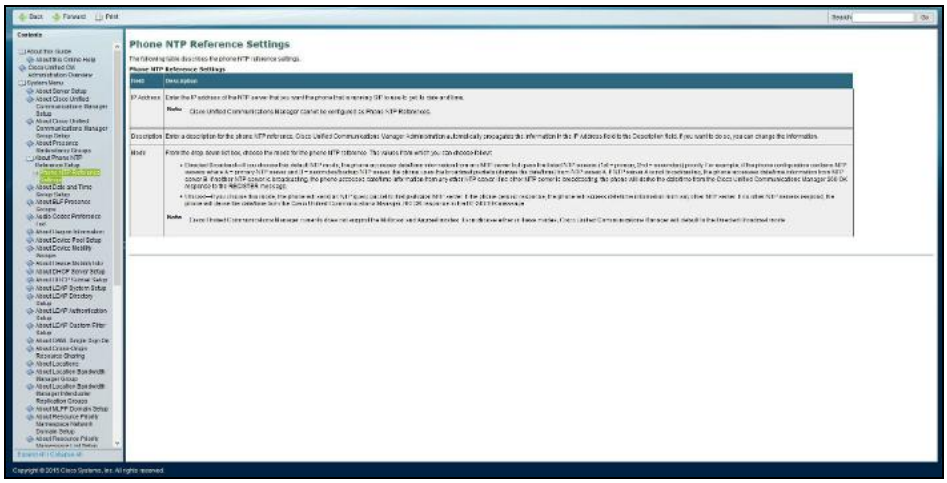


Figure 128: Accessing the CUCM Help page

This will open the CUCM Help. It's a handy web page with all the information about the CUCM options. Also, as you were configuring the NTP Reference and clicked on "This Page", the CUCM Help will open directly on the page with the information of the Phone NTP Reference. This is very helpful, and it works on any CUCM page you are - click on "Help" > "This page", and you'll see the specific information on this page.

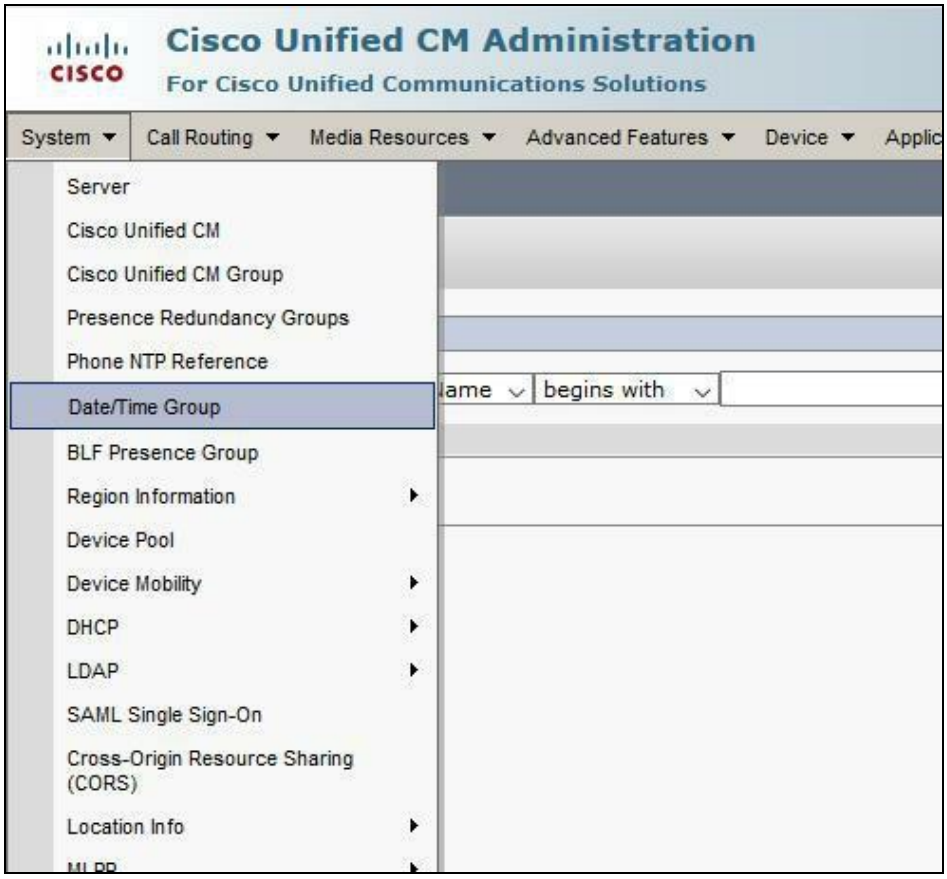


Figure 129: CUCM Help page

Date/Time Group

Date/Time Groups are created to provide date and time to your phones. If your phones are all located in the same time zone, you need one Date/Time Group, but if not, you need to create different groups to match the time zone of all your locations.

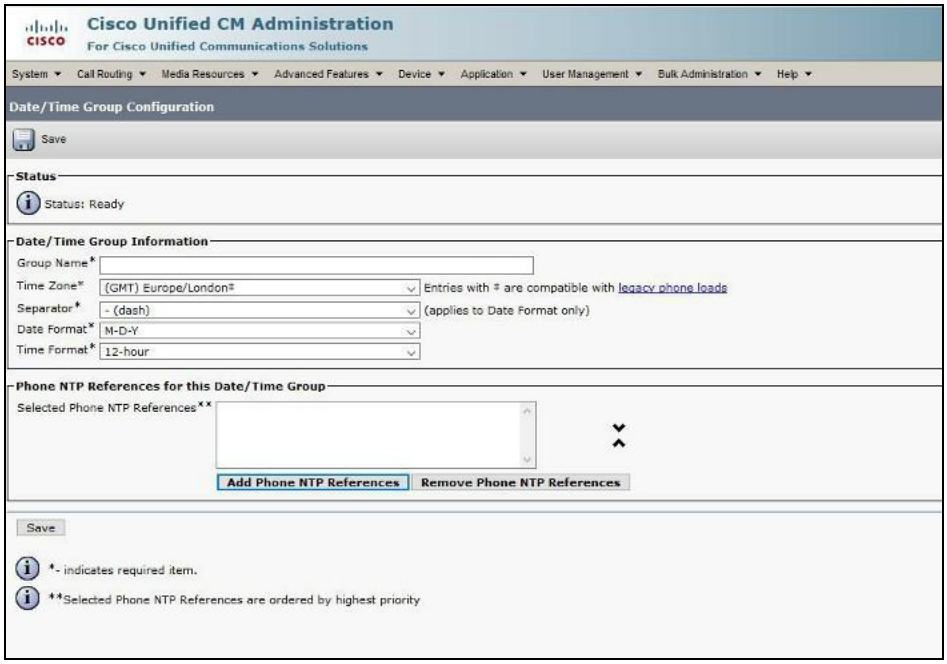


Figure 130: Date/Time Group Menu

Now, create the Date/Time group: type a name, select the time zone, the date separator (dash, slash or dot), the date format (month/day/year order) and the time format (12 or 24 hours). This formatting will appear on the phone screen using this Date/Time Group. If you have created an NTP Reference, you can associate it here.

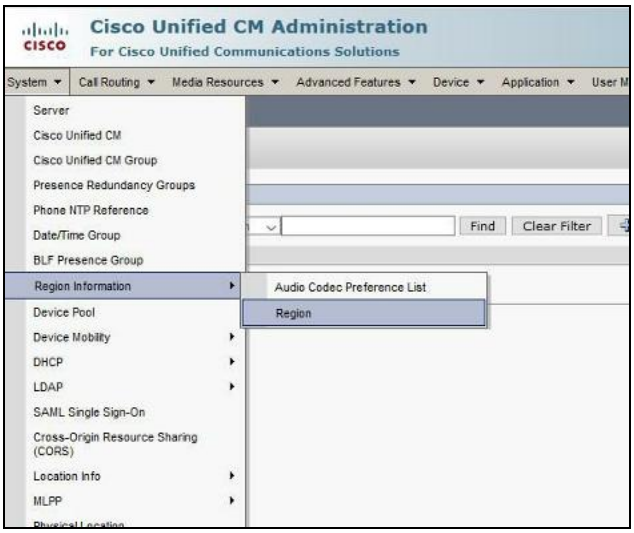


Figure 131: Date/Time Group Configuration

Usually, you need to create one Date/Time Group for each time zone you will have phones. For example, if you have three sites, but they are all in the same time zone, you will need to create only one Date/Time Groups. If you don't create these, some phones can display incorrect clock and date.

Regions

Regions are used to select which codec the phone calls will use. Here you will configure the relationship between regions, including the codec using inside its own. Example:

Region	Codec
Site A calls Site A	Call will use G.711
Site B calls Site B	Call will use G.711
Site C calls Site C	Call will use G.711
Site A calls Site B (and vice versa)	Call will use G.729
Site A calls Site C (and vice versa)	Call will use G.729
Site B calls Site C (and vice versa)	Call will use G.729

Table 9: CUCM Region Relationship Example

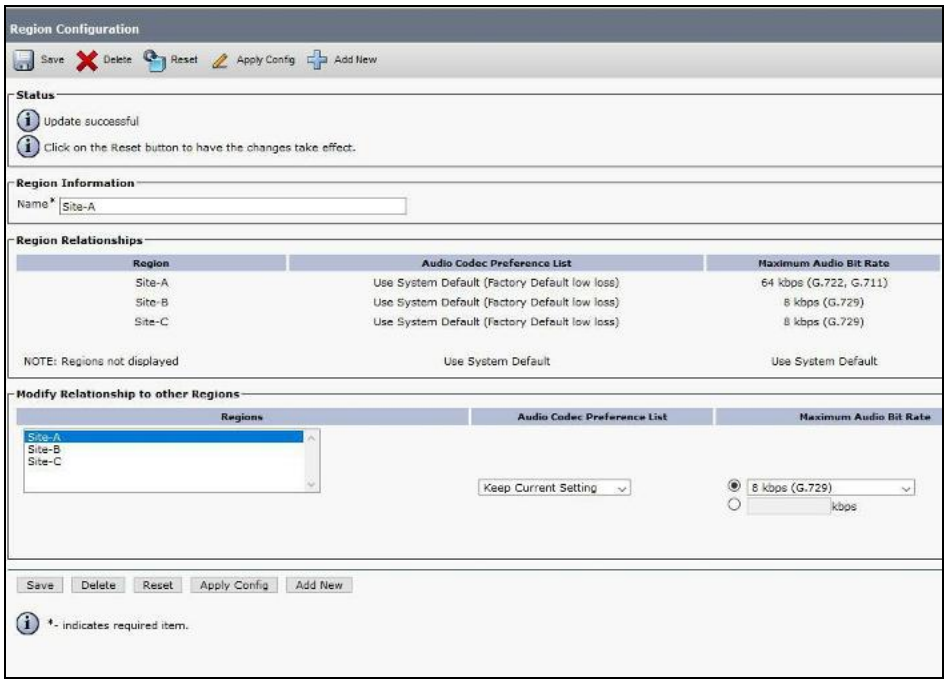


Figure 132: CUCM Region Menu

After creating the Regions you need, open it and select the Codec Relationship between regions. To do it, on the box “Modify Relationship to other Regions”, select a Region, and in “Maximum Audio Bit Rate”, select the Codec you want to use. Click “Save” and repeat this process for each region you need (you can select multiple regions to apply the same configuration at the same time).

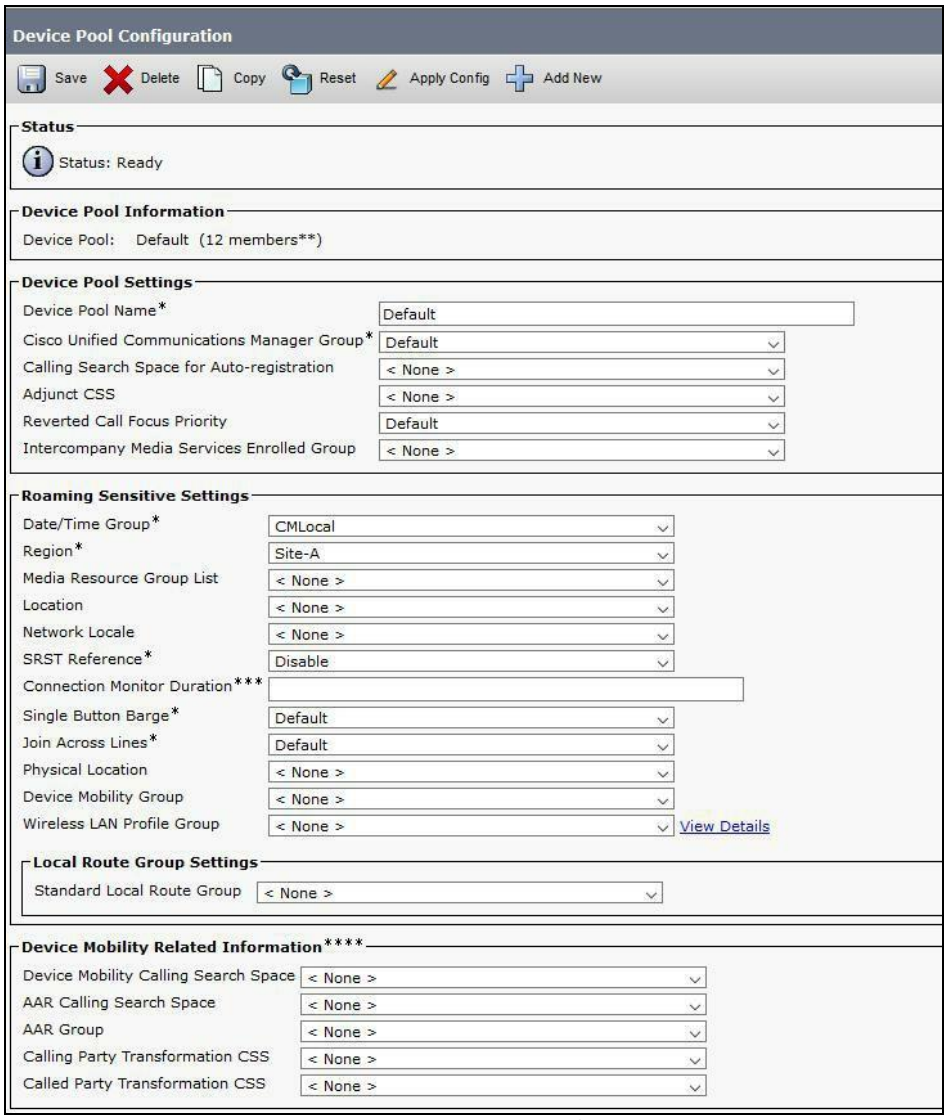


Figure 133: CUCM Region Configuration Menu

You need to create one Region for each site you have. If you don't create it, you will lose the ability to control which codec each call will use.

SRST Reference

If you have remote sites with WAN/VPN links without a CUCM Server available locally, it's possible to have phone outage situations in case of WAN failures. To avoid this, a good Cisco IP Telephony Project must always include Routers with the SRST functionality. This will provide remote sites with Survivable Remote Site Telephony (SRST) features.

With SRST, the Cisco Phones on remote sites will be able to register on the SRST Router locally when there is WAN failure and register back again to

CUCM automatically when the WAN link is restored.
We will see how to create an SRST Gateway in chapter 11, but you will only create an SRST Reference if you have a remote site without a CUCM Server locally but with a Cisco Router with the SRST functionality available. Also, you need to check the SRST licensing on your Cisco Voice Gateway.

Device Pool

Finally, Device Pools are used to aggregate all configurations we have created (CUCM Groups, Date/Time Groups, Region, SRST Reference and others, to apply it to a group of devices like Phones, Gateways, Trunks, and others.

To create it, go to menu “System” > “Device Pool > Add New”.

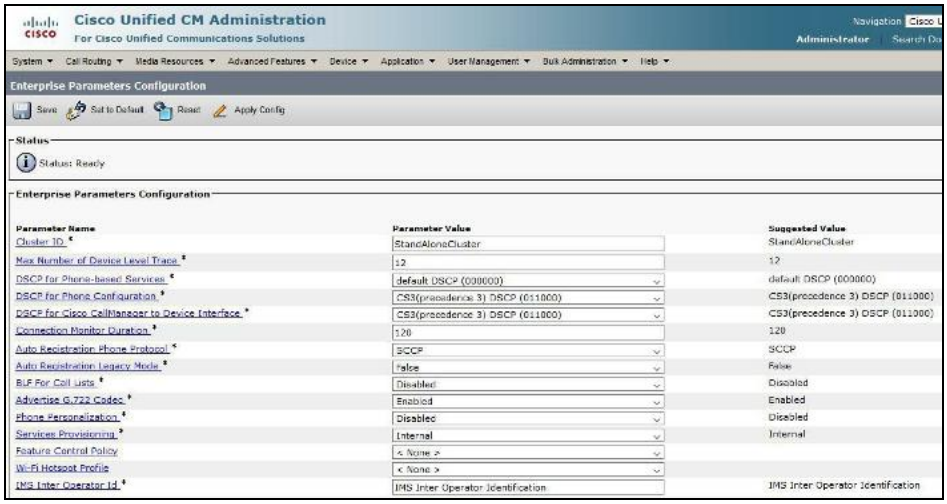


Figure 134: CUCM Region Configuration Menu

Create a Device Pool for any group of devices with similar configurations. It’s common to have one Device Pool to each site, but sometimes on large deployments, a single site can have more than one Device Pool.

Enterprise Parameters

Enterprise Parameters are configurations that apply to all system globally. Some of these configurations are:

Configuration	Default Settings	Description
Auto Registration Phone Protocol	SCCP	Default protocol (SCCP or SIP) to Auto Registration Feature

Advertise G.722 Codec	Enabled	Enable the G.722 codec automatically on devices compatible
Wi-Fi Hotspot Profile	<None>	Wifi SSID for Wireless Phones
CDR File Time Interval	1	Time interval for CDR Files
Default Network Locale	United States	Default phone tones for Network hold, transfer, etc
Default User Locale	English United States	Default phone tones for User hold, transfer, etc
URL Authentication	http://CUCM-IP-ADDRESS:8080/ccmcip/authenticate.jsp	URL for Phones authentication (Extension Mobility)
URL Directories	http://CUCM-IP-ADDRESS:8080/ccmcip/xmldirectory.jsp	URL for Corporate Directory
Enable IPv6	False	Enable or Disable IPv6 Protocol

Table 10: CUCM Region Configuration Menu

The settings above are just part of all configurations available. As these are very critical configurations, you should change them only if you know what you're doing. Also, the CUCM shows on the right side of the configuration what was the default settings for each parameter.

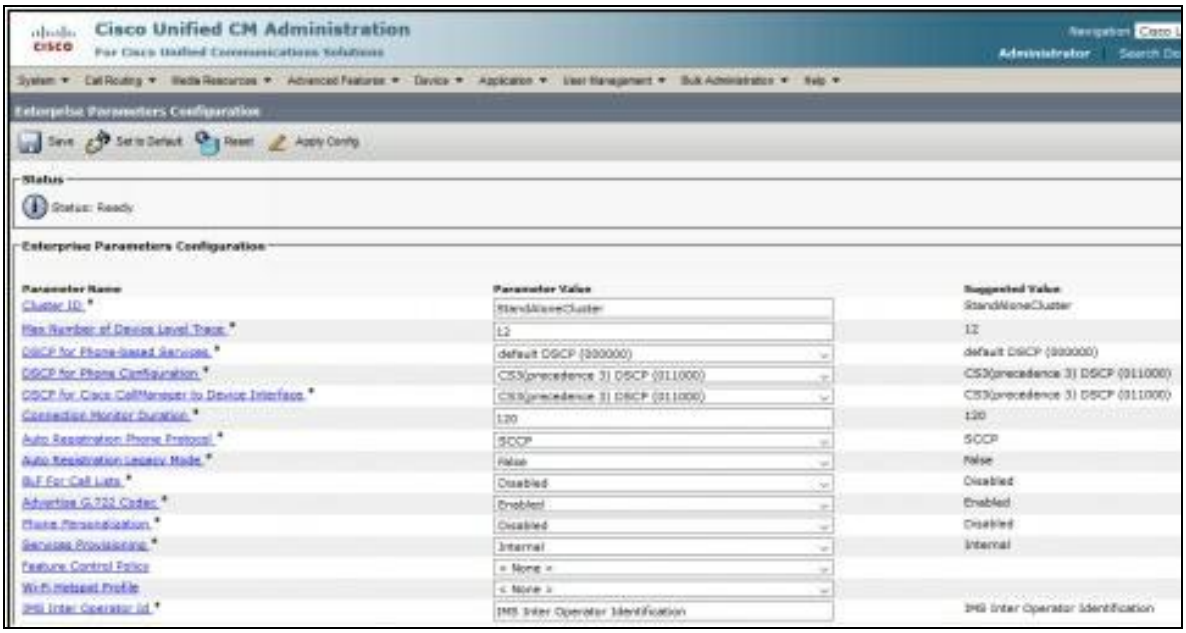


Figure 135: Enterprise Parameters

All the configurations on this screen; you can click on a setting, and a Pop-up will open explaining what precisely this configuration is related to.

Service Parameters

Service Parameters are very similar to Enterprise Parameters. The main difference is that the Enterprise Parameter is global configurations applied to the cluster, while Service Parameters are specific Service configurations, used only to each server.

To open it, go to Menu “System” > “Service Parameters” > Select the server > then, select the Service you want to edit:



Figure 136: Cisco Call Manager option under Service Parameters

As the Enterprise Parameters, there is a lot of configurations available. Some of the main configs are under “Call Manager” service:

Configuration	Default Settings	Description
CDR Enabled Flag	False	Enable or Disable the CDR - Call Detailed Record - to log information about all calls
CDR Log Calls with Zero Duration Flag	False	Enable or Disable the log of calls with Zero seconds
T302 Timer	15000	Interdigit Timeout - Timeout in milliseconds to wait until a call is routed (default is 15 seconds, usually I change it to 4000 ms / 4 seconds).
H225 T302 Timer	15000	Same as above, but to H.323 calls
Block OffNet To OffNet Transfer	False	Offnet to Offnet transfer are calls to outside of your company - like calling someone mobile phone and transfer him to another external mobile phone - by default, this is allowed on CUCM
Suppress MOH to Conference Bridge	True	Disable MoH on Conference Bridge
Drop Ad Hoc Conference	Never	Specified when a conference should terminate

Maximum Ad Hoc Conference	4	Maximum participants on a single Ad-hoc conference (when a user dials to all participants from his phone) - Usually I change it to 8
DSCP for Audio Calls	46	QoS parameters for Audio Calls
G.722 Codec Enabled	Enabled for All Devices	Enable or Disable the G.722 Codec
iLBC Codec Enabled	Enabled for All Devices	Enable or Disable the iLBC Codec

Table 11: some of the CUCM Service Parameters

The configurations above are only a small piece of all possible configurations available. Do not change any setting that you aren't sure.

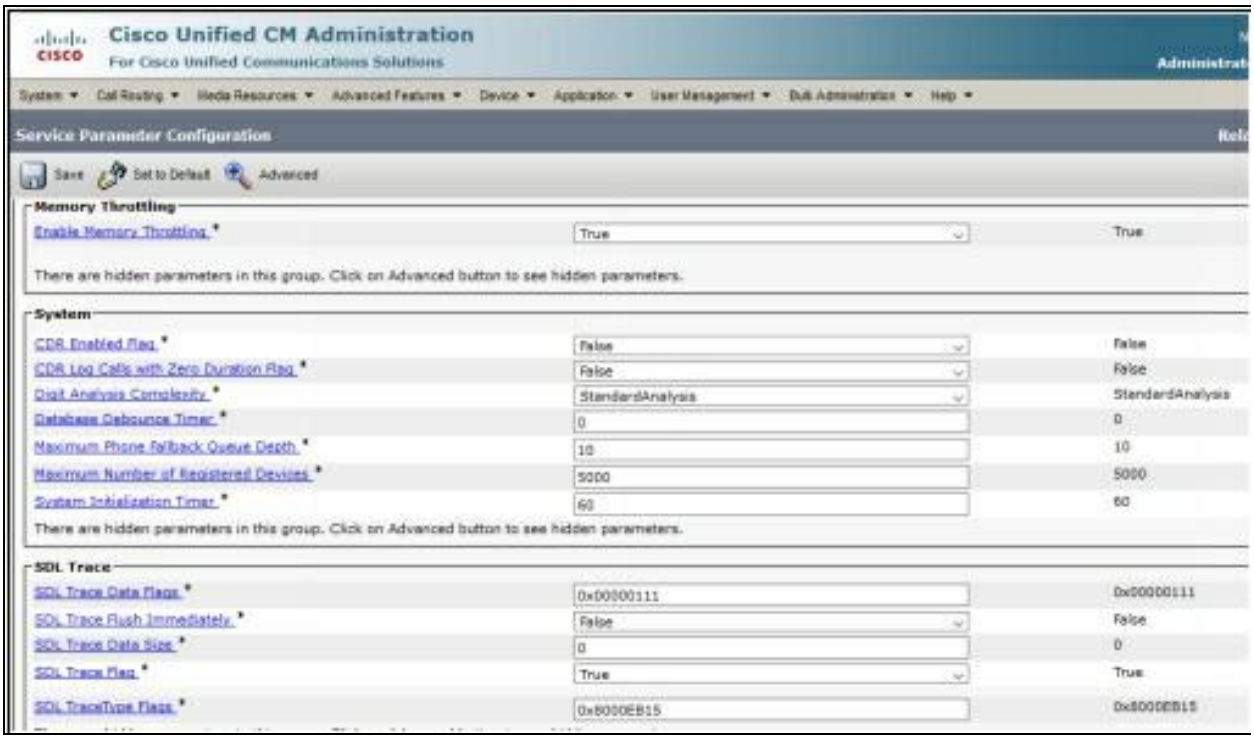


Figure 137: Service Parameters

If you change anything and cause a problem, you can always check the default settings and return to it.

Parameter Value	Suggested Value
40	20
56	40
5	5
2000	2000
10	10

Figure 138: Suggested Values

CHAPTER 5 - CALL PERMISSION

How to allow or block calls on CUCM

What are Partitions and Calling Search Spaces

Partition and Calling Search Spaces are the most critical configuration on CUCM when we talk about call permission. With PT and CSS, we can allow or block calls to and from users, gateways, phones, trunks, and other devices.

Despite being critical to CUCM call permissions, sometimes this topic is very confusing.

Partitions can be seen as a collection of objects like:

- Directory numbers
- Route patterns
- Translation patterns

All those can belong to specific partitions. Example: we can create a partition "Internal_PT" to place all our internal extensions.

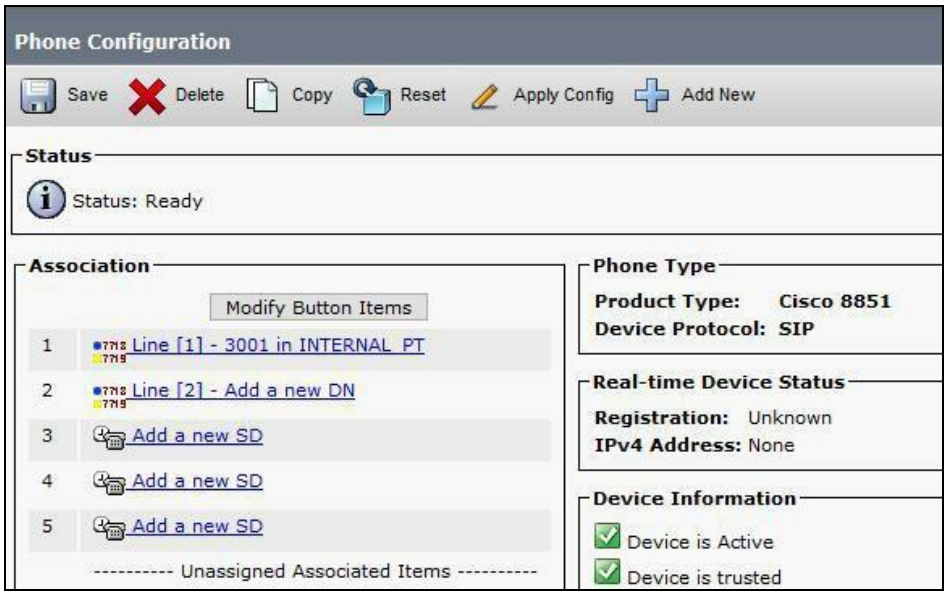


Figure 139: Extension 3001 in Partition "INTERNAL_PT"

Calling Search Spaces are an ordered list of route partitions. Example: we can create a CSS "Internal_CSS" to allow only internal calls, and associate only the "Internal_PT" with this CSS.

CSS Name	Internal_CSS
Partitions associated with this CSS	Internal_PT

Table 12: CSS and PT association

CSS determine which partitions calling devices must search when they attempt to complete a call. It's critical to understand this point, as a lot of calling problems in CUCM can be solved by checking this. To reach a destination, the called party's partition must belong to the calling party's CSS.

Another way of thinking is: CSS is related to permission to place a call, and Partition is associated with receiving a call.

You can again assign different CSS's to:

- phones
- directory numbers
- translation patterns
- call forward all
- call forward no answer
- call forward busy
- gateways
- trunks

Creating Partitions

To create Partitions, go to menu “Call Routing > Class of Control > Partition > Add New”:

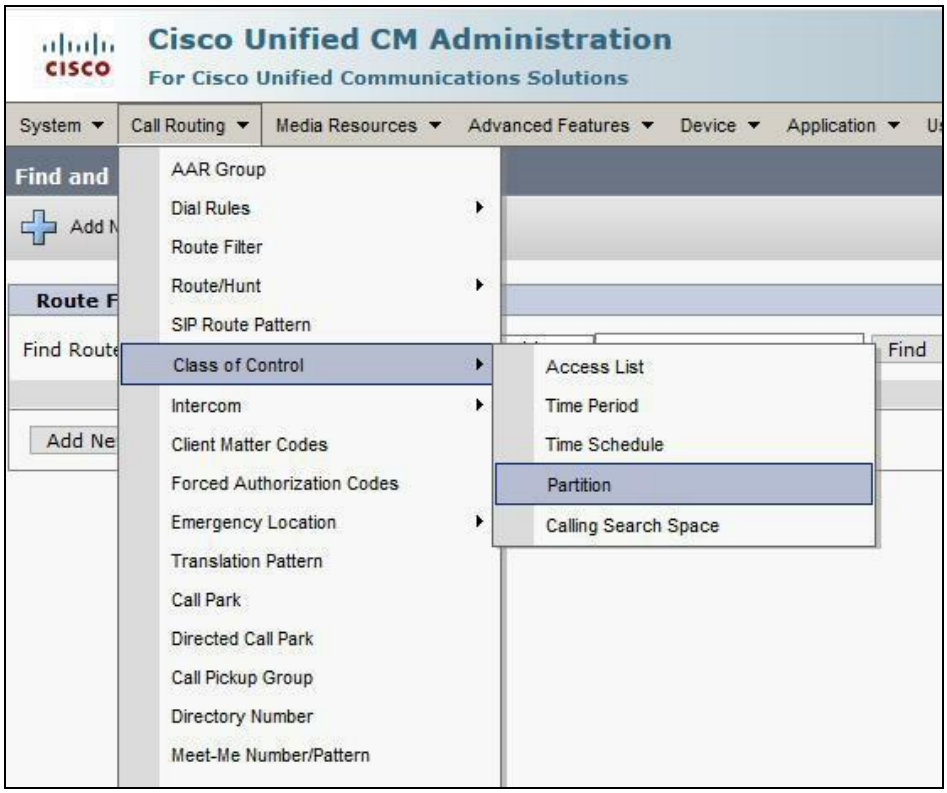


Figure 140: Partition Menu

You can create multiple partitions at once. Just type all partitions names and press Enter to create the next (one partition per line):

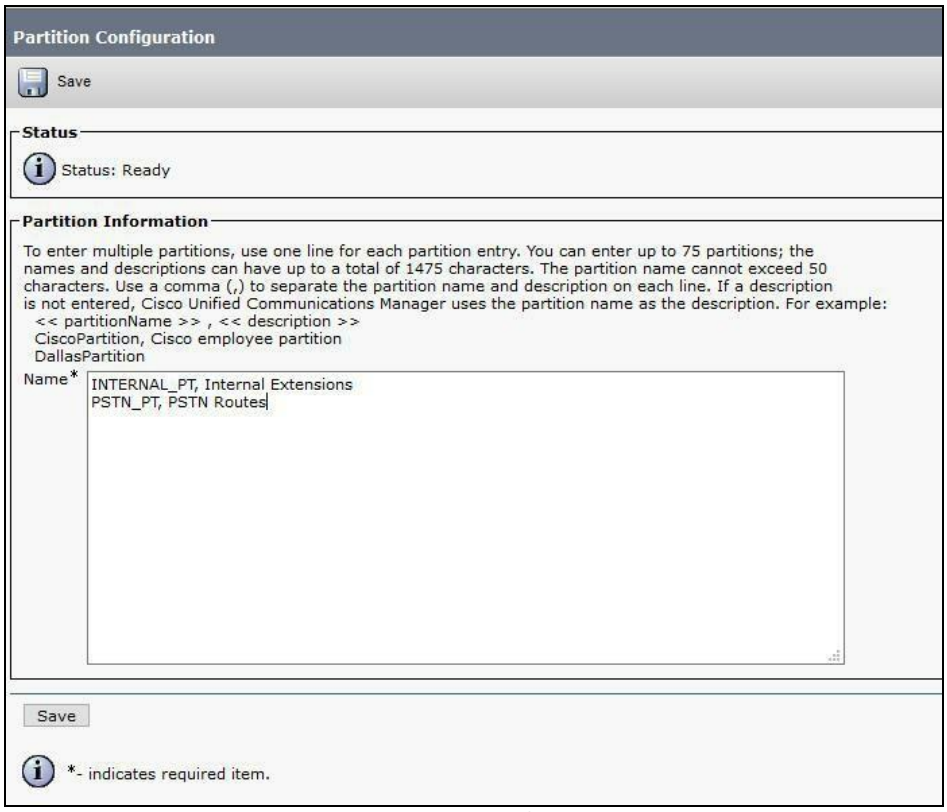


Figure 141: Partition Configuration Window

You can also create a description for each partition by inserting a comma and then the description. In the end, click “Save”.

Creating Calling Search Spaces

To create CSS, go to menu “Call Routing > Class of Control > Calling Search Space > Add New”:

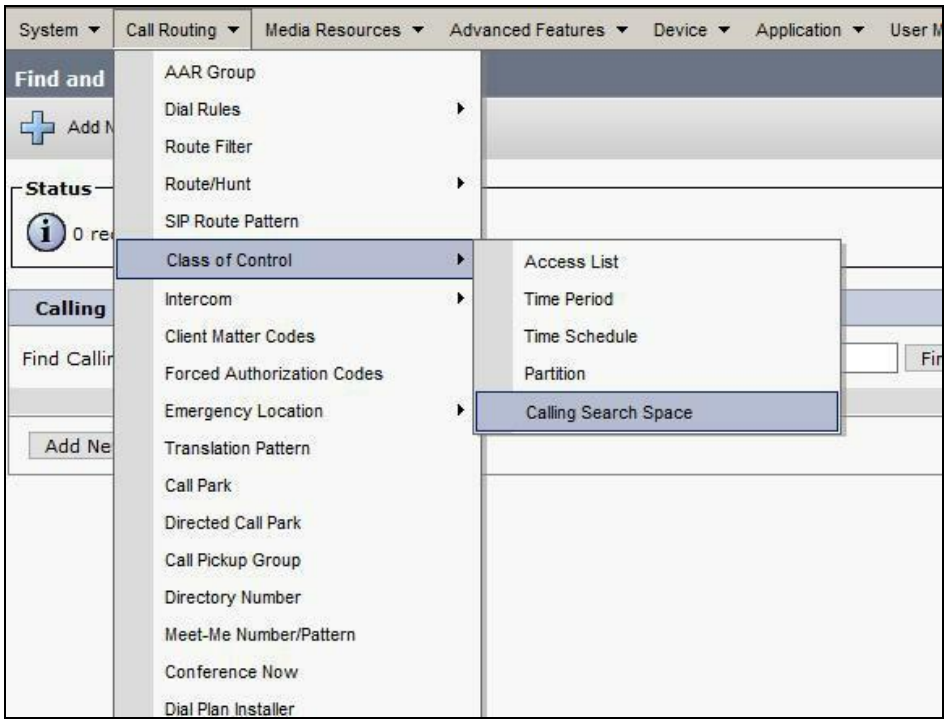


Figure 142: Calling Search Space Menu

Type the CSS name and a description (optional). Then, on this screen, select the Partitions you want to add on this CSS.

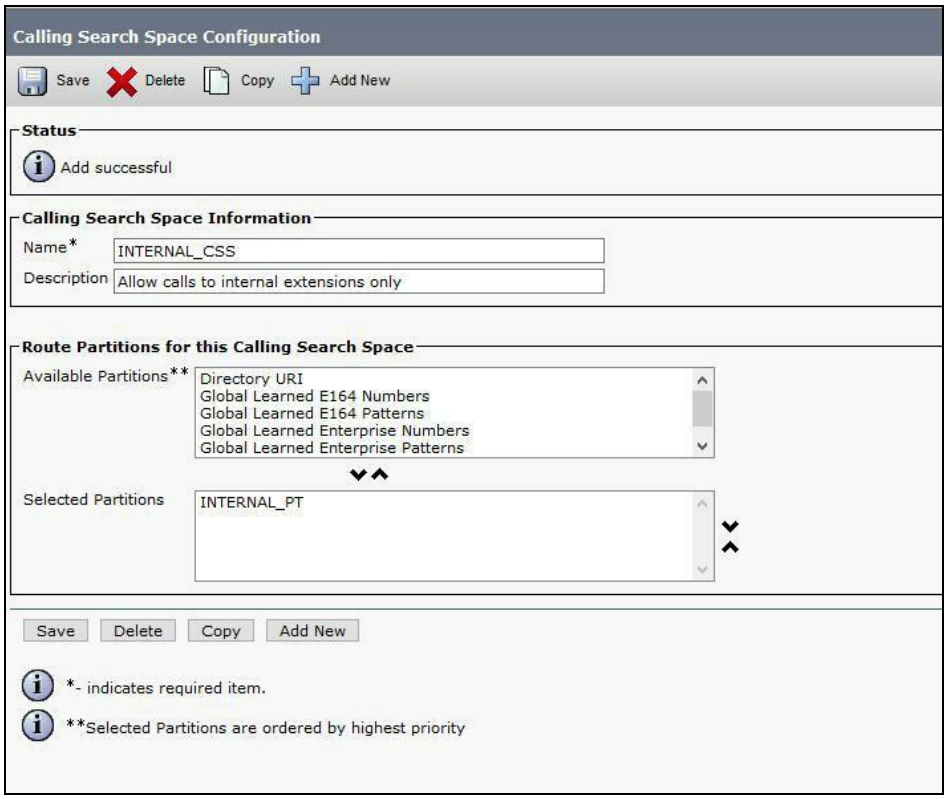


Figure 143: Calling Search Space "INTERNAL_CSS" associated with Partition "INTERNAL_PT"

Note: It's not necessary to use the letters "PT" or "CSS" at the end of a partition/calling search space name, but I like using it to make it easier to identify during the configuration process. Some people want to use these letters in front of the PT/CSS names, while others do not use this anywhere. .

PT/CSS Examples

Let's imagine a CUCM System with the following PT and CSS scheme:

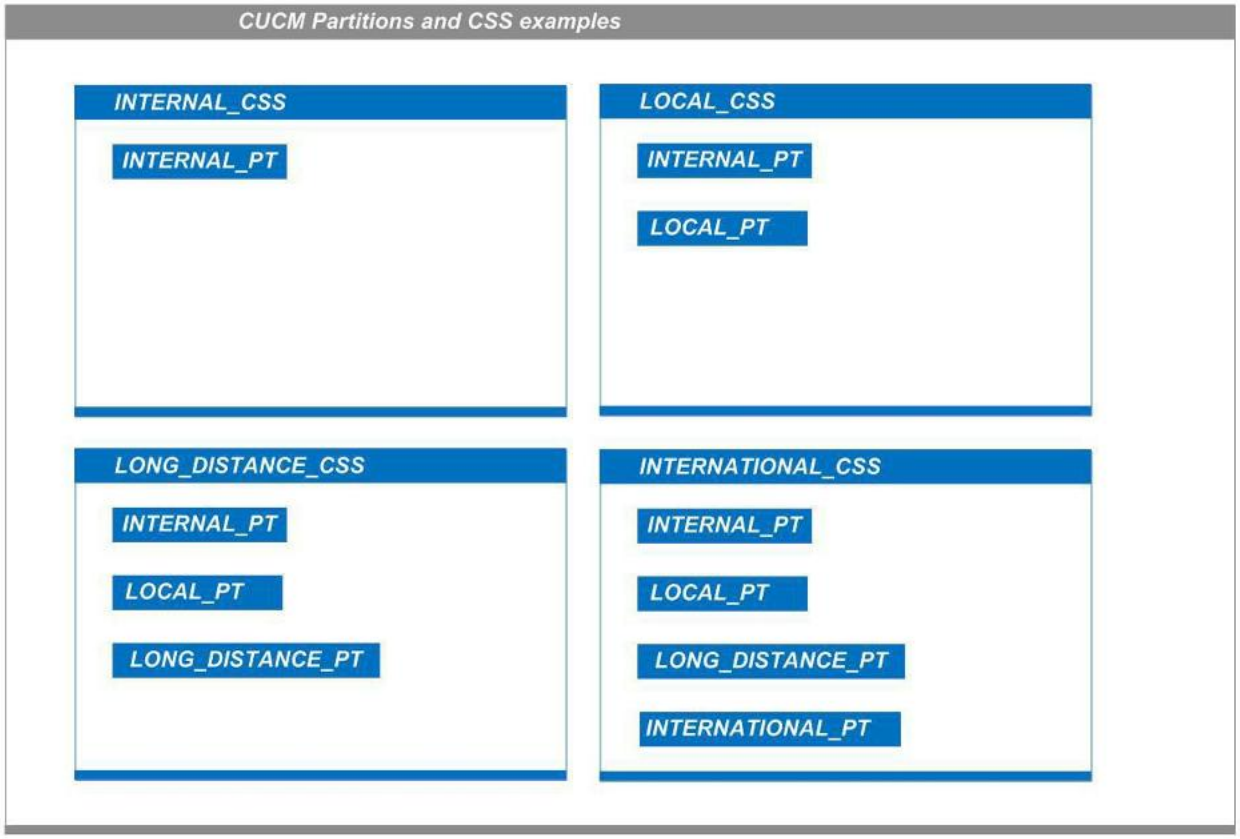


Figure 144: Partition and CSS example

There are four partitions and four calling search spaces created:

Partition Name	Usage
INTERNAL_PT	Internal extensions
LOCAL_PT	Local PSTN Route Patterns
LONG_DISTANCE_PT	Long distance PSTN Route Patterns

INTERNATIONAL_PT	International PSTN Route Patterns

Table 13: Partitions examples

To match these partitions, the following CSS will be created:

CSS Name	Usage
INTERNAL_CSS	Allow calls to Internal extensions
LOCAL_CSS	Allow calls to Internal extensions and Local PSTN numbers
LONG_DISTANCE_CSS	Allow calls to Internal extensions, Local PSTN numbers and Long distance PSTN numbers
INTERNATIONAL_CSS	Allow calls to Internal extensions, Local PSTN numbers, Long distance PSTN numbers and International PSTN numbers

Table 14: Calling Search Space examples

With that plan ready, the next steps are:

- Associate all internal extensions with partition “INTERNAL_PT”;
- Associate all route patterns to local PSTN numbers with partition “LOCAL_PT”;
- Associate all route patterns to long distance PSTN numbers with partition “LONG_DISTANCE_PT”;
- Associate all route patterns to international PSTN numbers with partition “INTERNATIONAL_PT”,
- Associate the CSS to each user phone with appropriate calling permissions (CSS).

To associate a user phone with the correct CSS, go to Menu “Device > Phone”, select his phone, and look for “Calling Search Space”:

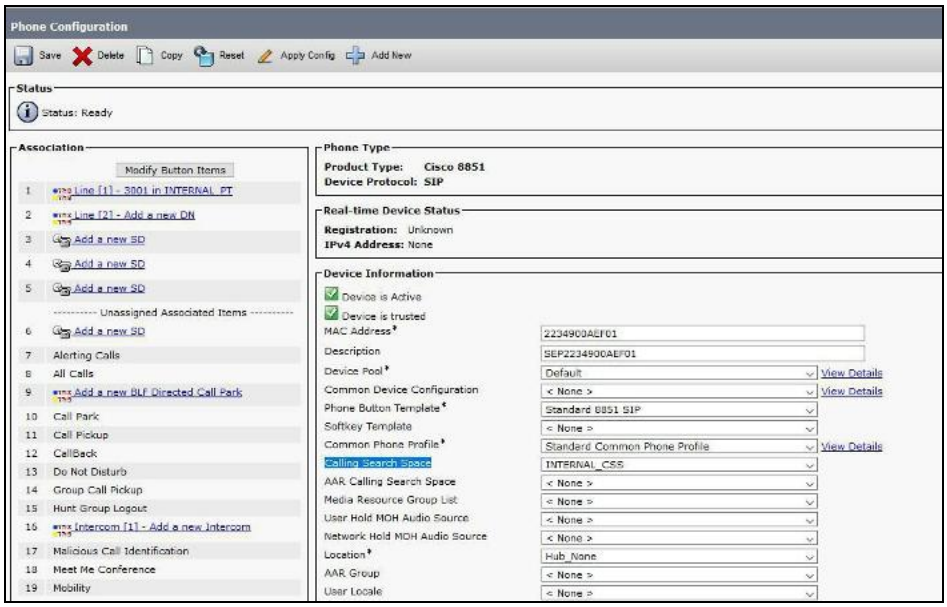


Figure 145: Calling Search Space inside Phone Configuration window

This is enough to allow this user to call all phones inside Partition "INTERNAL_PT".

CSS on Phones x CSS on Extensions

You can apply CSS directly on the phone, as seen in the example below. However, in more complex situations, you can use the CSS directly to the extension. To do this, open the directory number configuration window and select the CSS you want to apply:

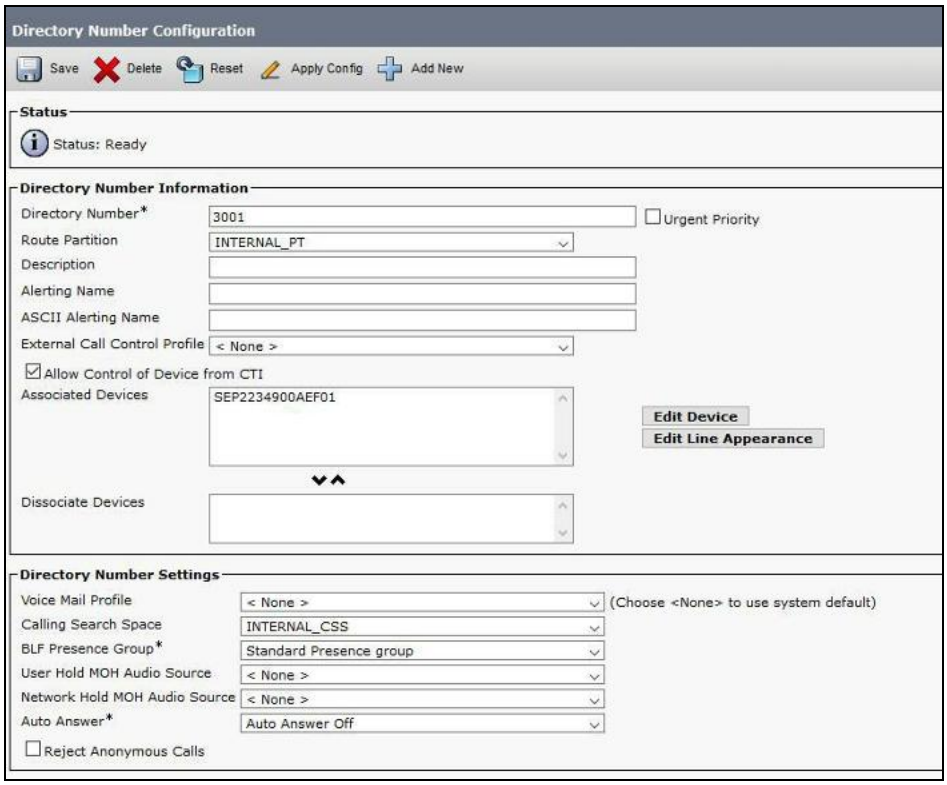


Figure 146: Calling Search Space inside DN Configuration window

This allows more complex scenarios, like shared lines or phones with more than one line. You can for example:

- apply a CSS allowing only internal calls on the Device, and use a CSS which would enable external PSTN calls to only one of the user's line; or:
- apply the same CSS on the device and the phone; or:
- apply the CSS only to the lines and no CSS on the device.

There are a lot of combinations possible. It depends on your environment if you have a simple CUCM Cluster with 50 phones or more complex company with more than 20.000 phones to manage. The combination of CSS on the line and device allow different combinations to all there scenarios.

Inbound CSS to Gateways and Trunks

When a Gateway or Trunk receives a call from another system, it will look for the destination of that call based on the CSS it is allowed to reach. You need to apply the correct CSS to make these inbound calls work.

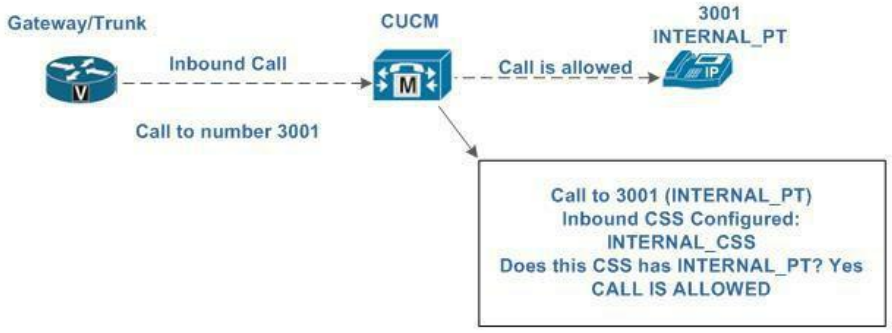


Figure 147: Inbound call allowed by CUCM

If the configured CSS does not have permission to call the destination of the call, the call will be blocked with a message "Your call cannot be completed as dialed. Please consult your directory and call again. This is a recording."

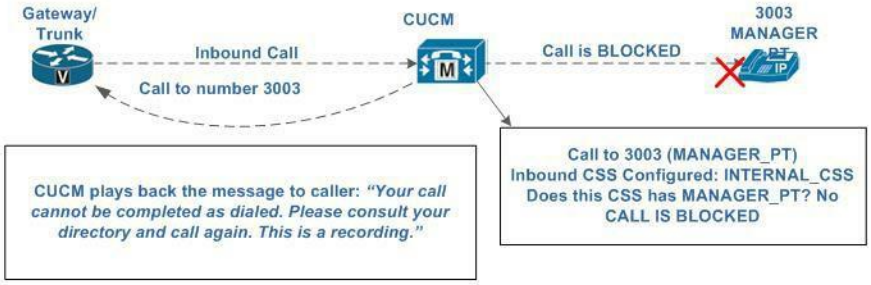


Figure 148: Inbound call blocked by CUCM

The Inbound Calls configuration is done inside the Gateway/SIP Trunk, on the "Inbound Calls" section:

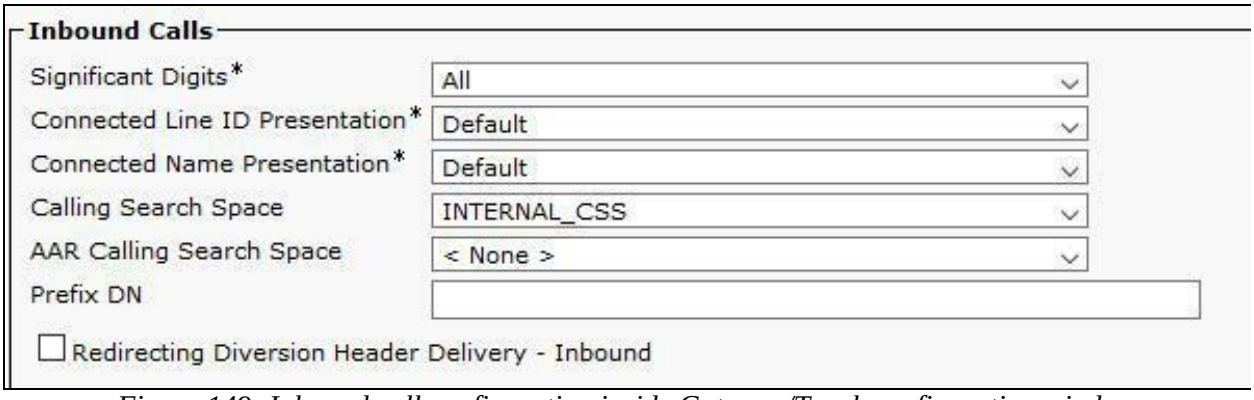


Figure 149: Inbound call configuration inside Gateway/Trunk configuration window

Default CSS and PT to Auto-Registration

If you are using Auto-Registration (we will see it in Chapter 6), you will need

to select the default PT/CSS for auto-registered phones and lines.

Auto-Registration Default CSS

To edit the "Universal Device Template" field, go to “User Management > User/Phone Add > Universal Device Template”:

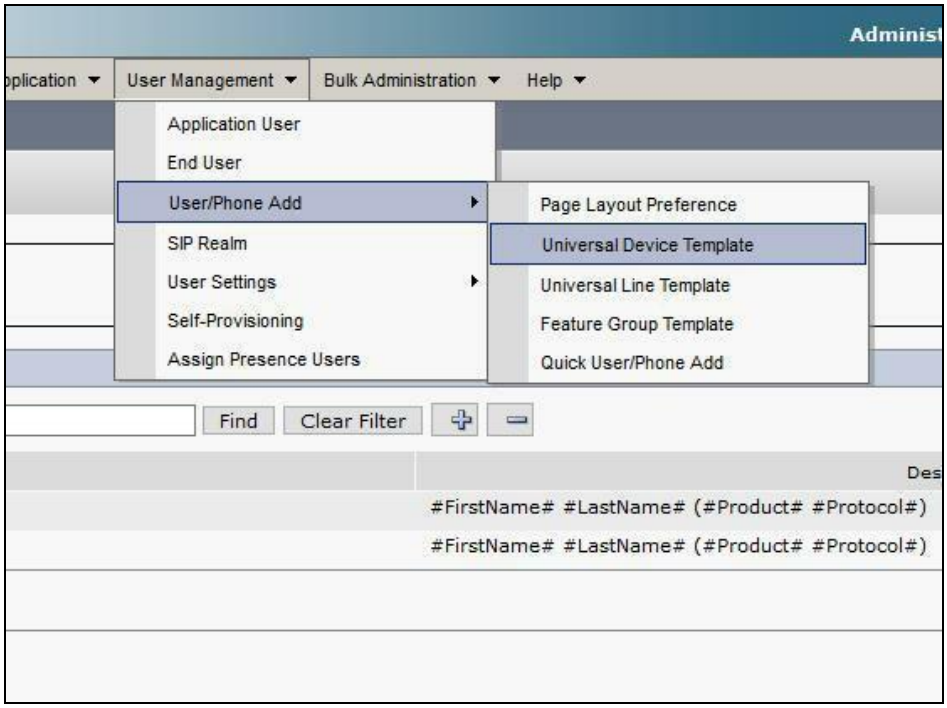


Figure 150: Universal Device Template Menu

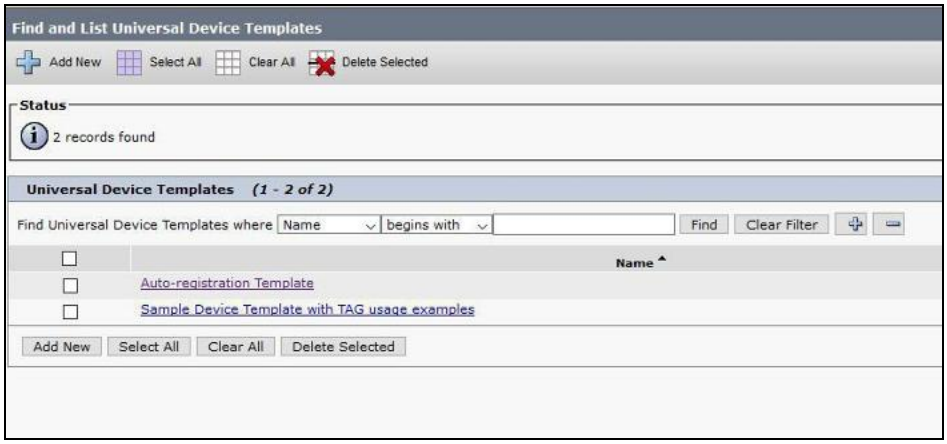


Figure 151: Existing Universal Device Templates

Click on “Auto-registration Template” to edit it. Open the “Device Routing” Menu and select the CSS you want the auto-registrations phone to use.

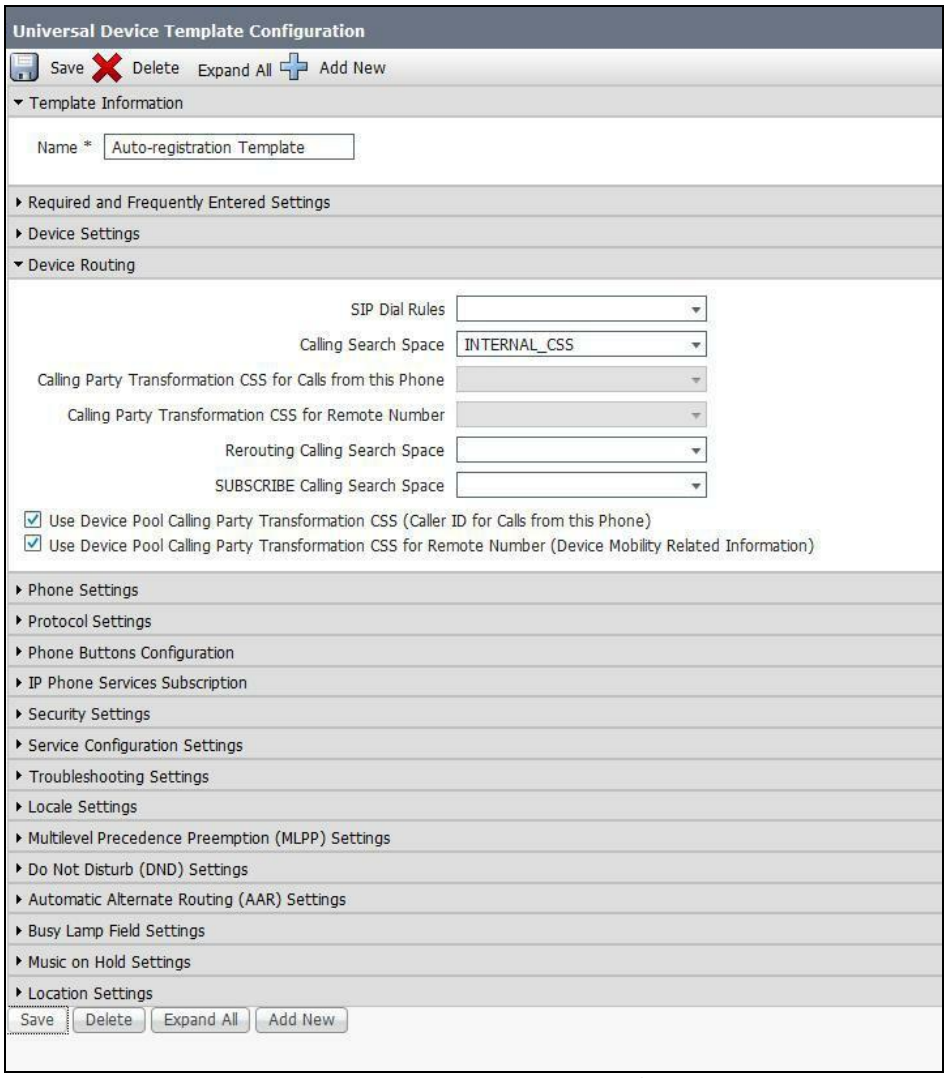


Figure 152: Universal Device Template Configuration window

You can use this window to edit other phones configurations like Device Pool, Extension Mobility, Softkey Template, etc.

Auto-Registration Default PT

To edit the default Partition where the Auto-registration lines will be created, go to menu “User Management > User/Phone Add > Universal Line Template”:

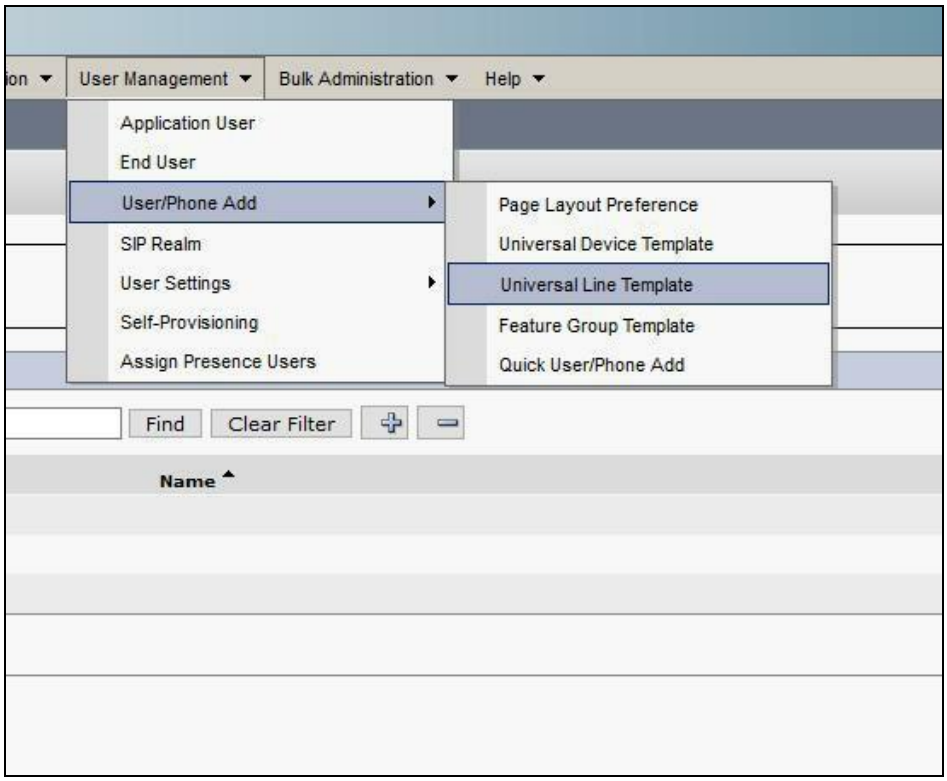


Figure 153: Universal Line Template Menu

Select “Sample Line Template with TAG usage examples” (or you can create your own if you want). Now, select the Route Partition you want to use.

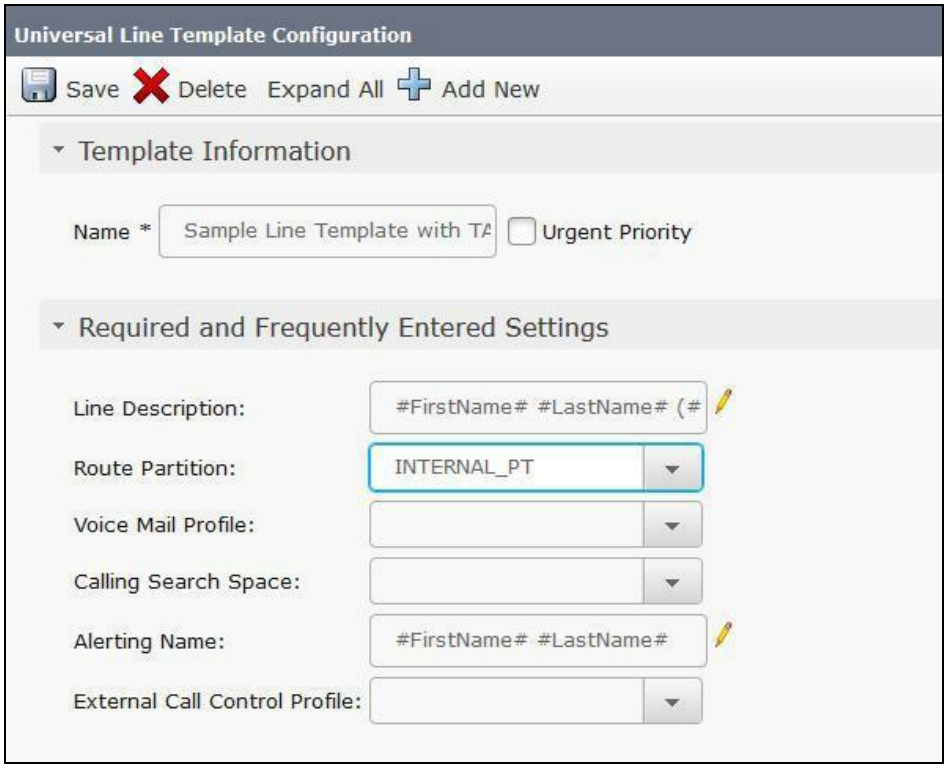


Figure 154: Universal Line Template Configuration window

With this configuration, all extensions automatically created in Auto-Registration feature will use this combination of Partition and Calling Search Space.

Troubleshooting PT/CSS problems

Cisco Dialed Number Analyzer (DNA) is a tool inside CUCM to test and troubleshoot call permissions. It simulates a call inside CUCM and will give you a result if this call is allowed or not.

To open it, go to URL https://CUCM-IP-ADDRESS/dna

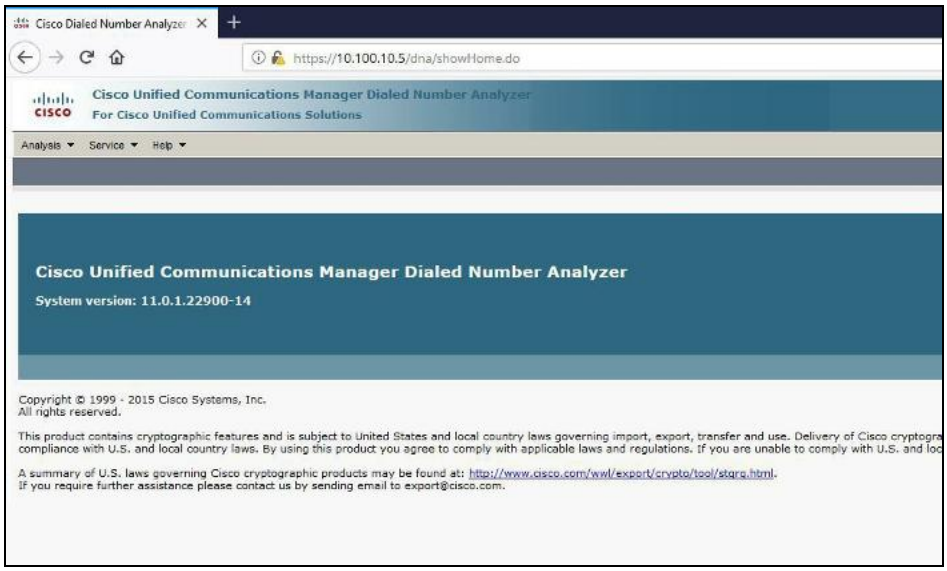


Figure 155: Cisco Dialed Number Analyser (DNA) page

> **Note:** If this page does not open, check if the services “Cisco Dialed Number Analyzer Server” and “Cisco Dialed Number Analyzer” are activated under menu "Cisco Unified Communications Manager Serviceability > Tools > Service Activation".

In the Analysis Menu, usually the most important options to test are:

- Phones
- Gateways
- Trunks

Let’s see how to test the calls:

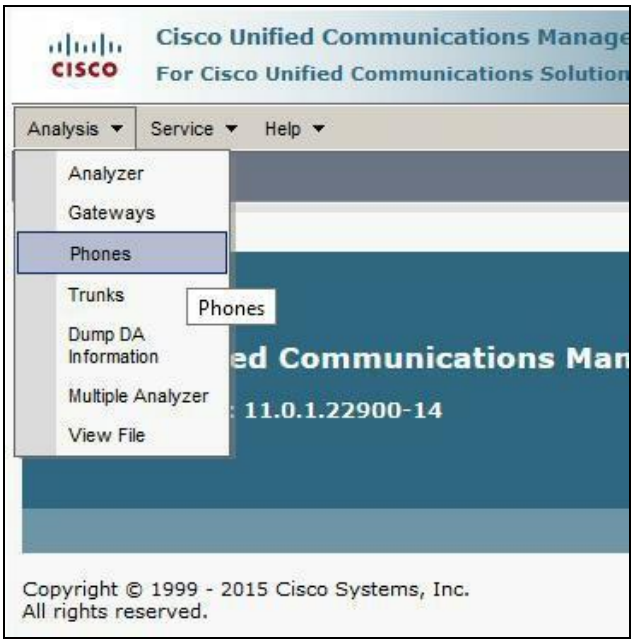


Figure 156: Cisco Dialed Number Analyser (DNA) Analysis Menu

Troubleshooting Phone call with DNA

To test a call from a Phone in DNA, click on menu “Analysis > Phone”. Click “Find” and select the phone you want to test. The following window will open:

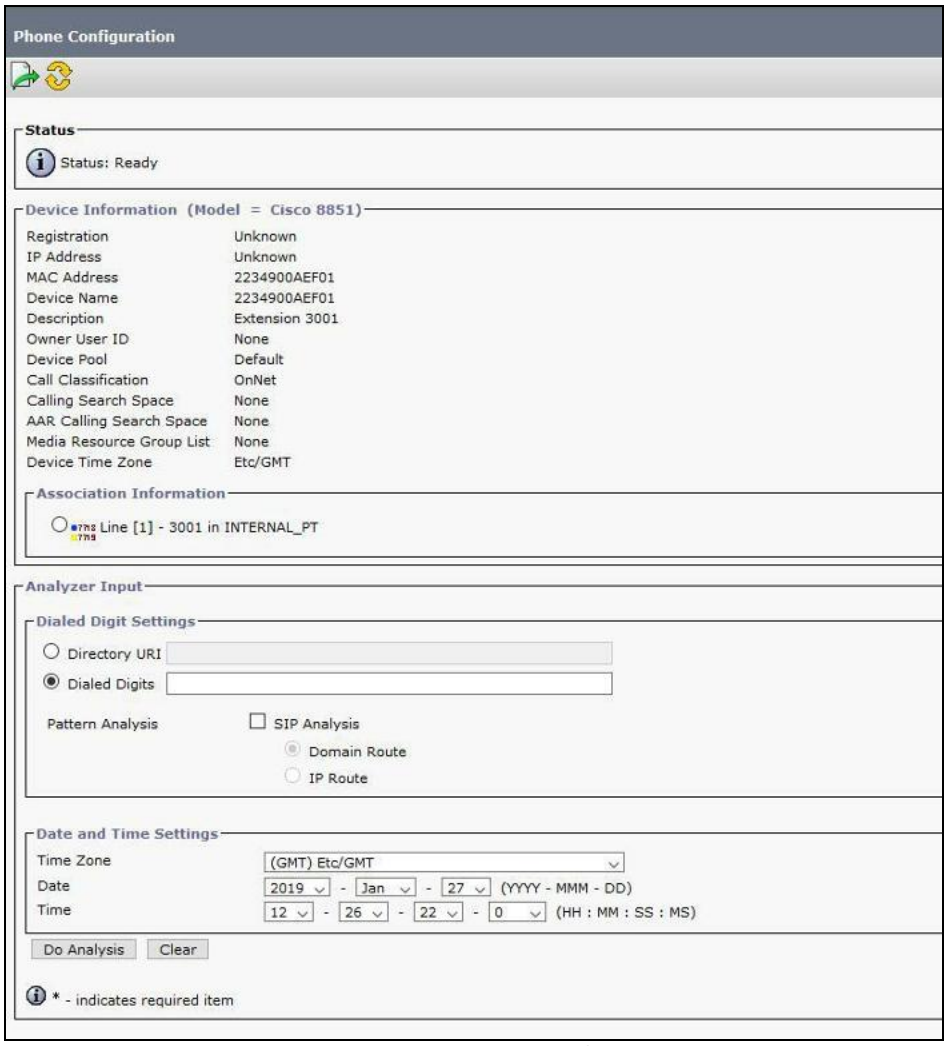


Figure 157: Cisco DNA Phone Configuration window

Here, select the line you want to simulate the call on “Association Information”; then, type the destination of this call on “Dialed Digits” and click “Do Analysis”. A pop-up window will open with the results of your test (please check if your pop-up blocker is blocking the page).

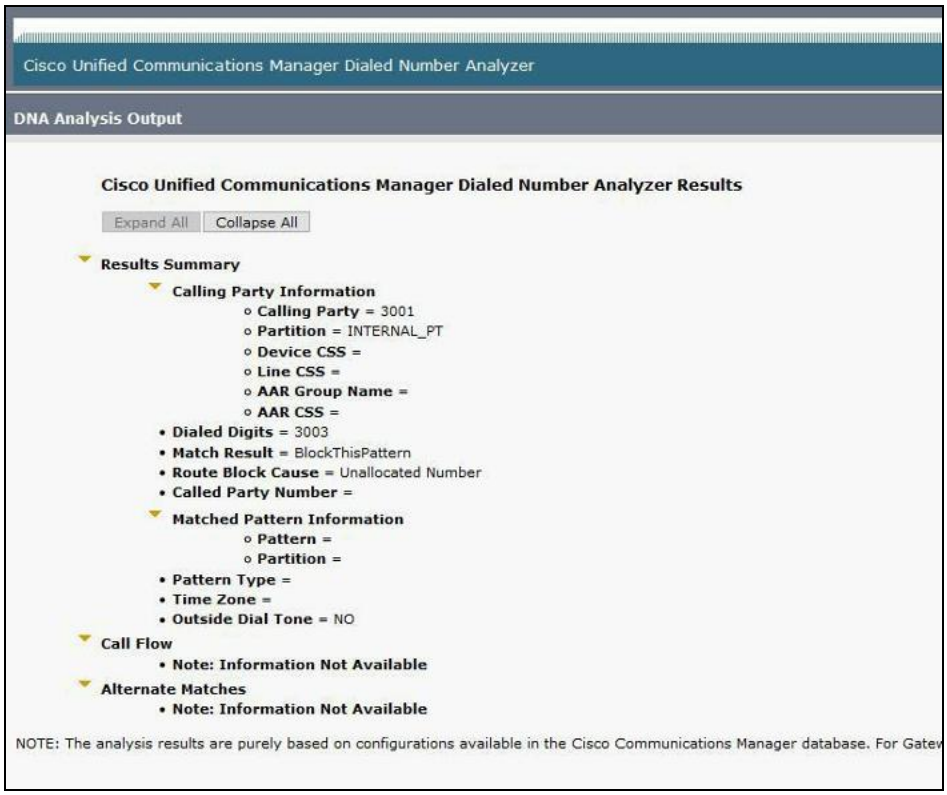


Figure 158: Cisco DNA Analysis Output window

In this example, I have simulated a call from extension 3001 to extension 3003. The result of this test was “BlockThisPattern”, and the cause was “Unallocated number”.

This happened because extension 3003 is located in Partition “MANAGER_PT”. As extension 3001 is using INTERNAL_CSS and this CSS does not have “MANAGER_PT”, this call is not allowed.

Now, let’s test the opposite: extension 3003 calling 3001:

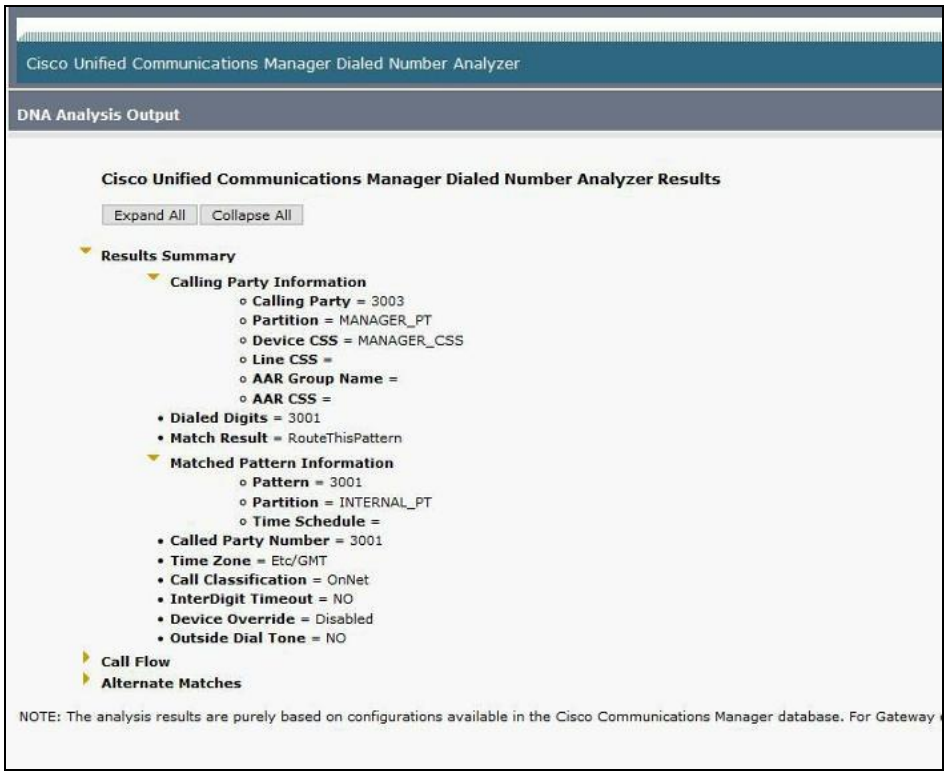


Figure 159: Cisco DNA Analysis Output window

Now, the match result is “RouteThisPattern”, and the extension 3003 can dial 3001.

This happened because extension 3001 is located in “INTERNAL_PT” and extension 3003 is using “MANAGER_CSS”, which has access to this “INTERNAL_PT”.

Troubleshooting Gateway/Trunk call with DNA

You can also use Cisco DNA to test inbound and outbound calls from Gateways and Trunks. The process is almost the same as we did testing the call from a Phone. Go to menu “Analysis > Gateway (or Trunk) > Select the device you want to test > Type the source of the call (Calling Party) and the destination (Dialed Digits) > click “Do Analysis”:

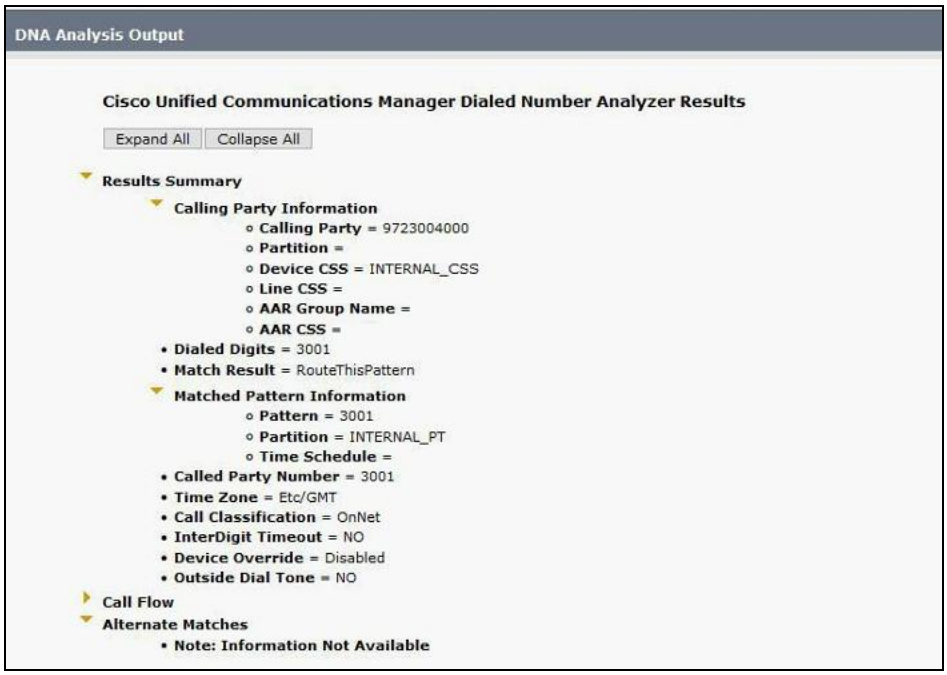


Figure 160: Cisco DNA Analysis Output window

In this example, the external line 9723004000 sent an incoming call to our gateway, and it allowed (RouteThisPattern) the call to extension 3001, as our gateway is using the CSS “INTERNAL_CSS” and it has access to extension 3001 (INTERNAL_PT).

Cisco DNA is handy to simulate and troubleshooting all types of calls, and I recommend that you have it enabled on at least one of your CUCM servers.

CHAPTER 6 - PHONES REGISTRATION

There are some steps until a Cisco Phone can register on CUCM. We need to understand these steps to troubleshoot any problem related to phones registration.



Figure 161: Cisco Phone registering

Power on the Cisco Phone

Obviously, the phone needs the power to turn on. The energy necessary to have a Cisco Phone working can be provided in 3 ways: Power Over Ethernet (PoE), Power Supply or Power Injector.

Power Over Ethernet (PoE)

This is by far the most common solution. You connect a phone to a network cable, and it turns on. But how does this magic happen? The answer is simple: a network Switch (Cisco or not) is providing power to the phones using an IEEE Standard called Power Over Ethernet.

Power Over Ethernet (PoE) switches can deliver up to 30 watts to each PoE devices. There are 5 PoE Classes, from Class 0 to 4:

Class 0	Up to 15.4 W

Class 1	Up to 4 W
Class 2	Up to 7 W
Class 3	Up to 15.4 W
Class 4	Up to 30.00 W

Table 15: Power Over Ethernet Classes

These switches are capable to power many PoE-enabled devices like Phones, Wireless Access-Points, IP Cameras, and other. You need to check every switch documentation to know how many phones it can support. Also, when buying your Cisco Switch, a precise calculation is needed on how much power you need. It is not rare to face problems in projects by not having enough energy to power on all your devices.

You can ask your Cisco Sales support to do it for you, but it is always good to have at least a general idea on those calculations. You multiply the power necessary to each phone with the number of phones per switch.

Cisco provides a tool called “Cisco Power Calculator”, available at https://cpc.cloudapps.cisco.com/cpc/launch.jsp (Cisco Login required).

Power Supply



Figure 162: Cisco CP-PWR-CUBE-3 and CP-PWR-CUBE-4

Power Supply can be useful, especially to remote sites or situations where a PoE Switch for a small number of phones is missing. Cisco has the CP-PWR-CUBE-3 and CP-PWR-CUBE-4 models available. You need to check which power supply is the compatible with your phone model.

Power Supply	Phone Series Supported
CP-PWR-CUBE-3	7800, 7900 and 69xx Series
CP-PWR-CUBE-4	8900 and 9900 Series

Table 16: Power Cube – Phones Supported

Power Injector



Figure 163: Cisco Power Injector

Although not-so-common nowadays, there is an option to buy a power injector, where you can inject power between your not-PoE Switch and your phone. The topology will look like this:

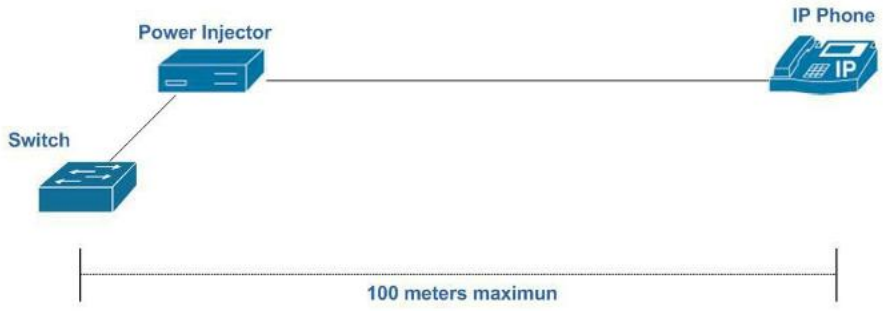


Figure 164: Cisco Power Injector Topology

The device can be connected on the users desk or on your rack. The maximum cable length between your switch and your phone will still be maximum 100 m, so this device cannot be considered to be a signal repeater.

After the phone is turned on, the next step will be the VLAN configuration.

Voice VLAN x Data VLAN

It is not necessary to create a Voice VLAN to your Cisco Phones, but it is highly recommended. With a dedicated VLAN for voice, you can isolate your voice traffic from the data traffic and make it easier to apply QoS and Traffic

Shaping, if necessary.

To create a Voice VLAN, create a normal VLAN on your switches, and apply it to the interfaces connected to phones. Example:

```
interface gigabitEthernet 0/2
switchport mode access
switchport access vlan 20
switchport voice vlan 30
```

On the configuration above, the switchport gigabitEthernet 0/2 is configured as Data VLAN 20 and Voice VLAN 30. This method enables a switchport to carry 2 VLANS, even when in mode access (not trunk), but only if there is a Cisco Phone connected on this port.

But how will the Cisco Switch know if there is a phone connected to this port or not? The answer is: Cisco Discovery Protocol (CDP). The phone will attempt to communicate with the Switch using CDP, and if the Switch recognizes a Cisco Phone, it will use CDP to provide the Phone VLAN.

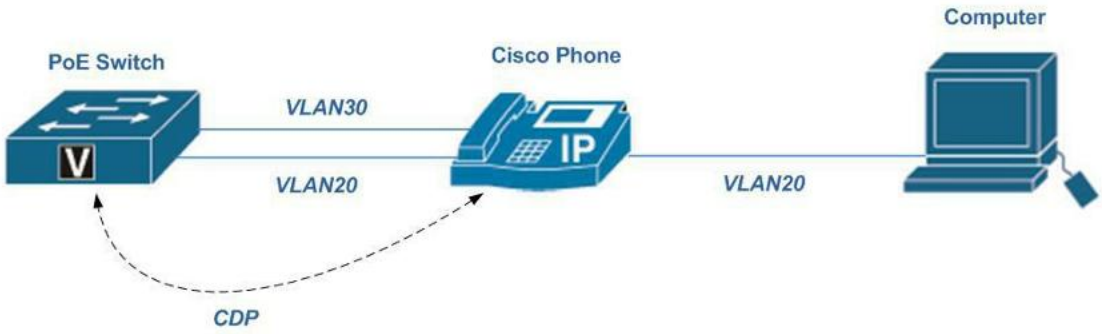


Figure 165: Voice VLAN via CDP

If the network switch is not Cisco and it has Voice VLAN support, usually there is another method to place the phone in the correct VLAN; the newest is Link Layer Discovery Protocol (LLDP), which is the IEEE version of CDP, which is also available on new Cisco hardware.
Another way to achieve this is using the Organization Unique Identifier (OUI); this method uses the vendor MAC Address to recognize that a Cisco Phone is connected to a port and place this port on dual-VLAN mode. For example, on old 3COM switches (1910, 2928, 4210, etc.), this is the way to

set it up. Some of these 3COM switches are still available on the market, but now they are known as HP Switches (as HP bought 3COM in 2010).

IP Helper Address

The next phase on the boot process of a Cisco Phone is to send a broadcast on the network asking for its IP Address. If your phone is directly connected to the same subnet of your DHCP server, you can skip this step. However, the most common situation is to have your phone on a different subnet/VLAN from your DHCP Server. On this situation, you will need a way to forward these DHCP Broadcasts to your DHCP server as a unicast packet, so it can travel all necessary hops to reach the correct DHCP server.

This process is done using the IP Helper Address on a Cisco Switch/Router:

```
interface vlan 1510
ip helper-address 10.100.55.99
```

You need to apply this command on every layer 3 interfaces where you have Cisco phones. This layer 3 interface needs to be on the same subnet as the DHCP Scope that you'll create on your DHCP server, as the server use this to identify which scope the DHCP request must match.

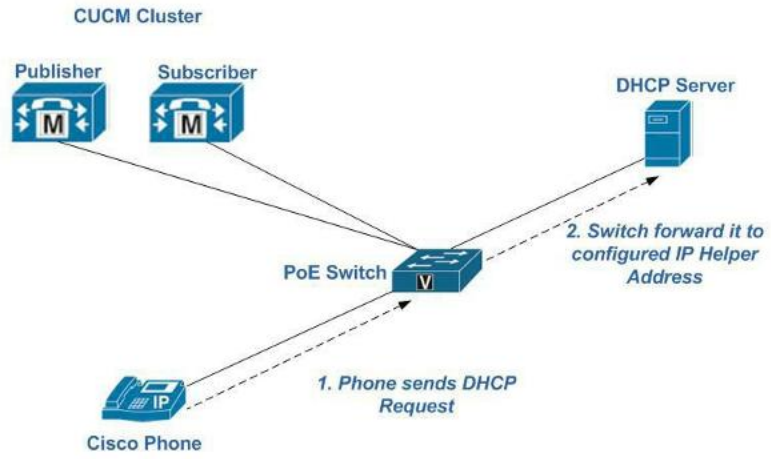


Figure 166: DHCP Request from Phone

When completed, you need to create the DHCP scope on your DHCP server. Let's see how to do it on a Windows Server and on a Cisco Router/Layer 3 Switch as well.

DHCP Server

At this stage, your phone's power is on and is sending a broadcast that reached your DHCP server. The DHCP Server needs to be ready to receive this DHCP Request and offer the Phone all configurations it needs to continue the registration process. These configurations are:

IP Address	Mandatory
Network Mask	Mandatory
Default Gateway	Mandatory
DNS Server 1	Optional
DNS Server 2	Optional
TFTP Server 1	Mandatory
TFTP Server 2	Optional

Table 17: DHCP Server information

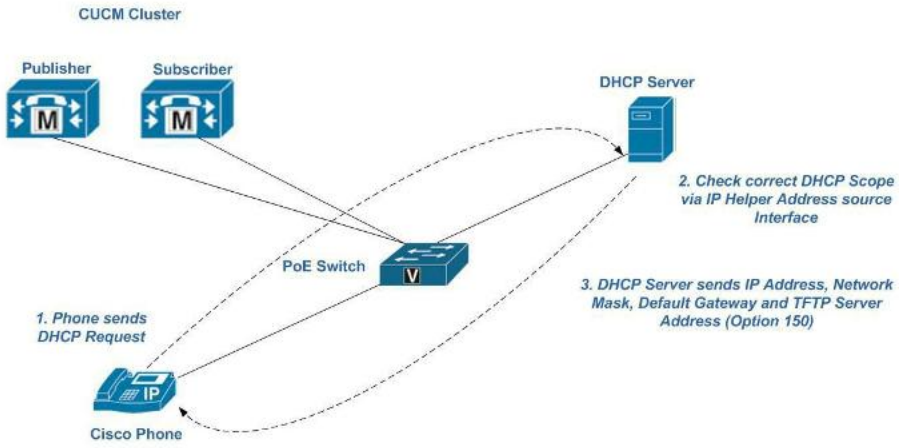


Figure 167: DHCP Request forwarded to a Windows Server

You can have your Phones network dependent or independent of DNS. Usually, it's better to have it independent of DNS resolution, to avoid an additional point of failure. The decision revolves around some network factors of your company, but it is possible to have a perfectly functioning global IP Telephony network with thousands of devices without any DNS resolution dependency for years.

DHCP Server on Windows Server

To create this scope on Windows Server, create a regular DHCP Scope on Windows and enable the DHCP Option 150 on this scope. The procedure is almost the same on Windows Server 2003, 2008, 2012 and 2016.

To do it, right-click in “IPv4” and then “Set Predefined Options”:

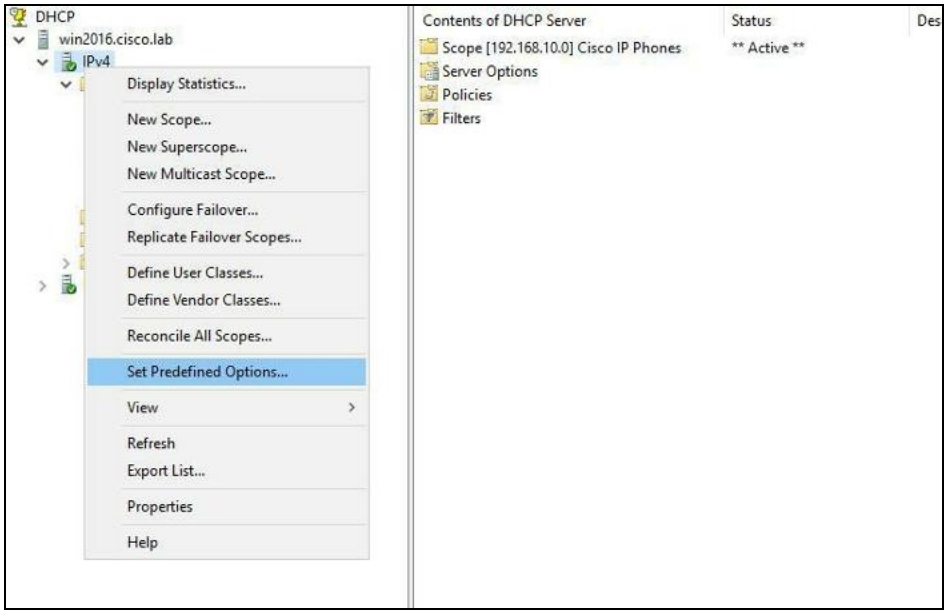


Figure 168: Configure TFTP Option 150 on Windows Server

In the next window, click “Add…”

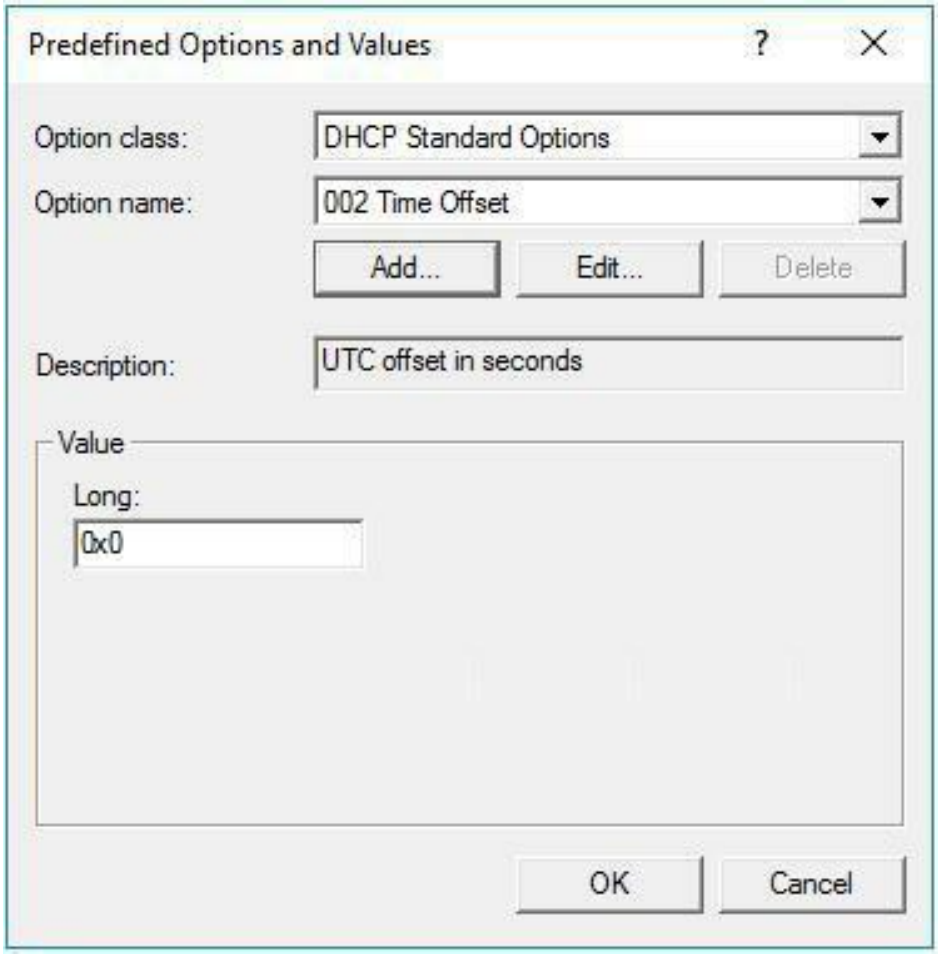


Figure 169: Configure TFTP Option 150 on Windows Server

Now, fill the Option Type with the following and click OK.

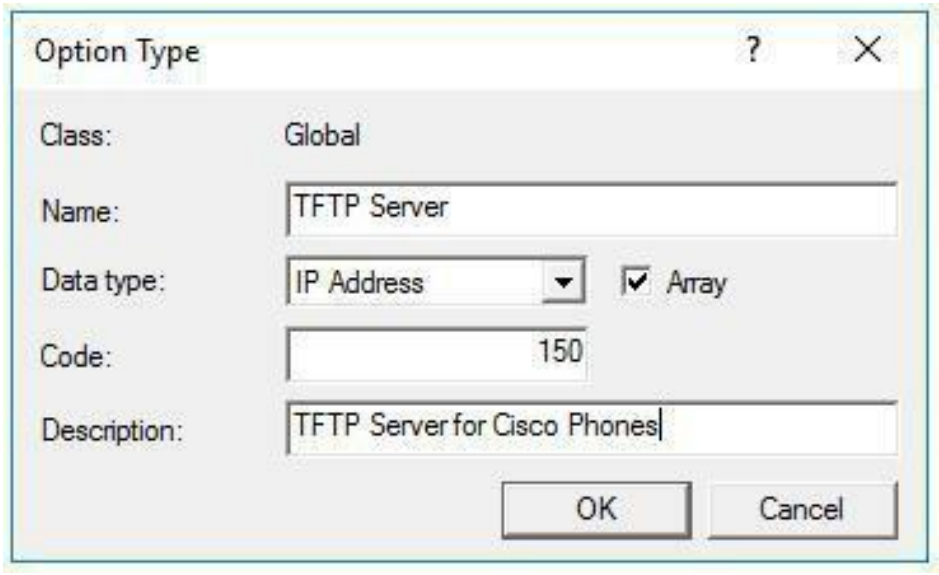


Figure 170: Configure TFTP Option 150 on Windows Server

Now that you have created the DHCP Option 150 on your DHCP Server, you need to apply it to your Cisco IP Phones DHCP Scope. To do it, right-click on your scope window, and click “Configure Options”.

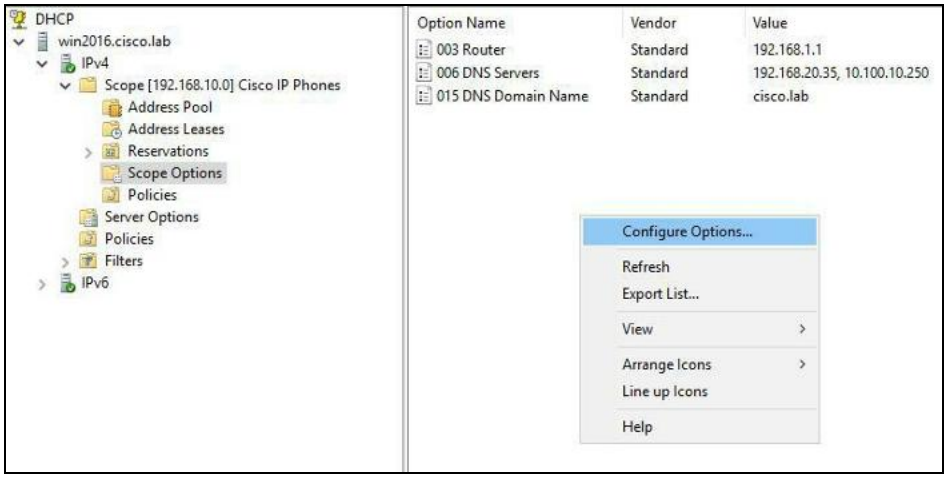


Figure 171: Configure TFTP Option 150 on Windows Server

Scroll down until you find the option 150 and select it. Then, type the IP Address of your CUCM servers running the TFTP service, and click “Add”. You can add up to 2 IP address on this list. While you can type 3 or more addresses here, the Cisco Phone won’t accept more than 2 entries.

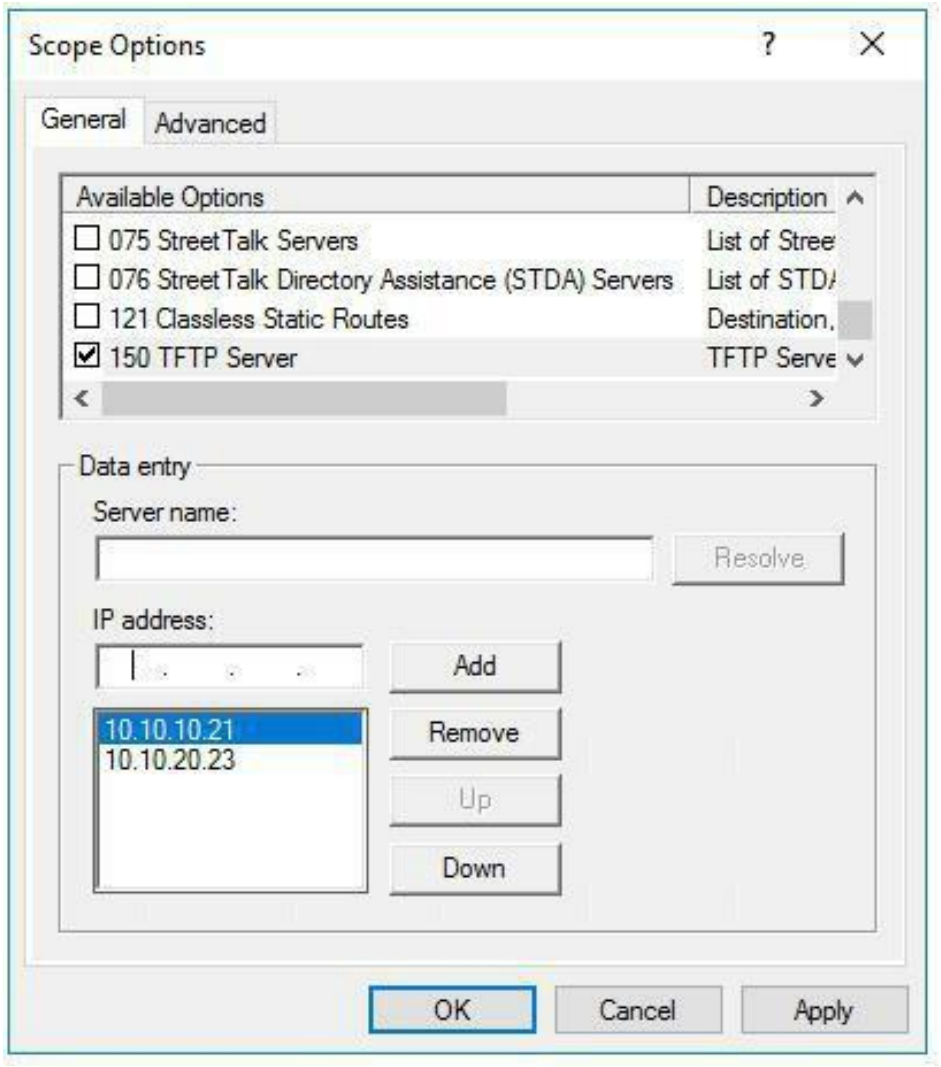


Figure 172: Configure TFTP Option 150 on Windows Server

Click OK to finish.

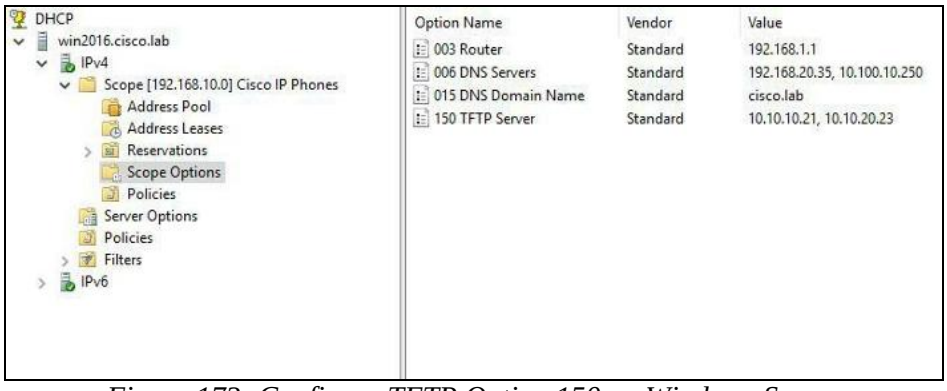


Figure 173: Configure TFTP Option 150 on Windows Server

Now your DHCP is ready to provide the TFTP Servers to your Cisco Phone.

Restart your DHCP Service to apply these configurations (Right-click on your server name, “All Tasks”, “Restart”).

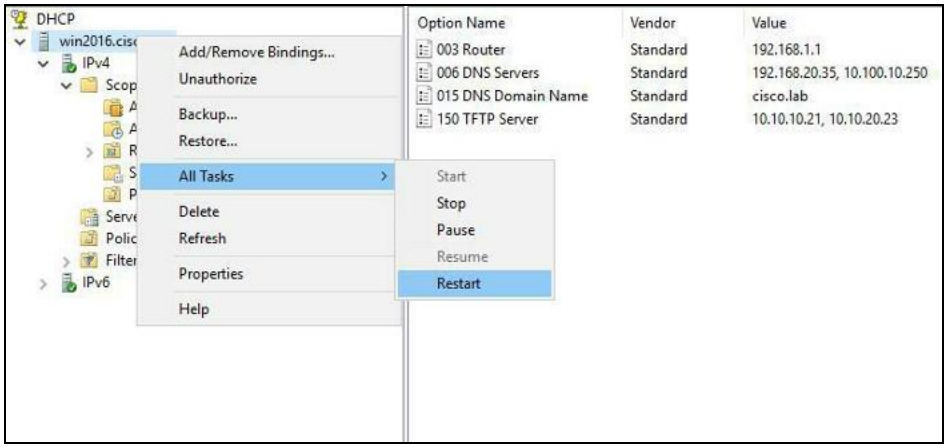


Figure 174: Restart the DHCP Service on Windows Server

DHCP Server on Cisco Router/Switch

If you decide to use your Cisco Router or Switch as the DHCP server to your Phones, the configuration is straightforward. Just enable the DHCP Option 150 as enabled on the Windows Server.

```
ip dhcp excluded-address 10.102.66.1 10.102.66.29
ip dhcp excluded-address 10.102.66.230 10.102.66.254

ip dhcp pool VOICE
network 10.102.66.0 255.255.255.0
default-router 10.102.66.254
option 150 ip 10.102.66.254 10.102.66.253
```

The configuration below will:

- Exclude the IPs 10.102.66.1 to 10.102.66.29 from the DHCP scope
- Exclude the IPs 10.102.66.230 to 10.102.66.254 from the scope
- Then, provide IP Addresses starting at 10.102.66.30 to 10.102.66.229
- Provide the IP Gateway 10.102.66.254
- Provide the DHCP Option 150 10.102.66.254 and 10.102.66.253 as TFTP servers

These configurations are enough for phones to be able to connect to your network and look for their TFTP Server, which are, in reality, their Cisco Call Manager servers. There, the phones need to be created to register them.

You can create the phones manually or enable the feature on CUCM called "Phones Auto-Registration", which allows Call Manager to accept and register all phones which attempt to register. It is important to know both methods.

Creating the Phone on CUCM

There are three ways to insert phones on CUCM:

- Manually
- Auto-Registration
- Bulk Administration Tool

Depending on your environment, you may need to use one process or another, but usually, the best uses are:

Manually	If you need to insert or edit few phones.
Auto-Registration	Useful during a massive deployment process. Can be disabled after the large-scale deployment or not, as it can always be used to implement new phones.
Bulk Administration Tool	Useful to migration environment or to initiate massive deployment where you have control of what phone goes to each user.

Table 18: Insert Phones options

It is good to know all three options, so you can decide which is better for your environment. Let's go through them one by one.

Create a Phone Manually

To create a phone manually, you will need to have the Phone MAC Address. Go to CUCM Administration, menu "Device > Phone > , then click on "Add New":

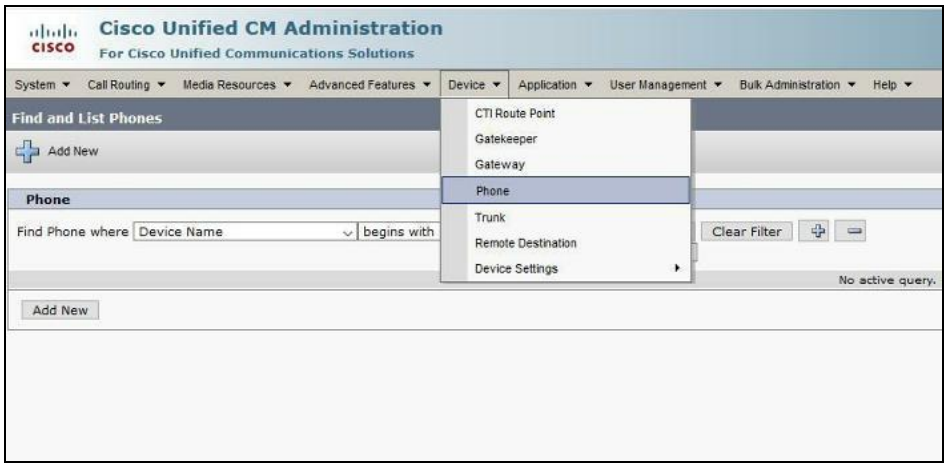


Figure 175: Add a New Phone Manually on CUCM

Next, select your phone model. Depending on the Phone model, in the next window, you may need to choose the device protocol, SCCP or SIP.

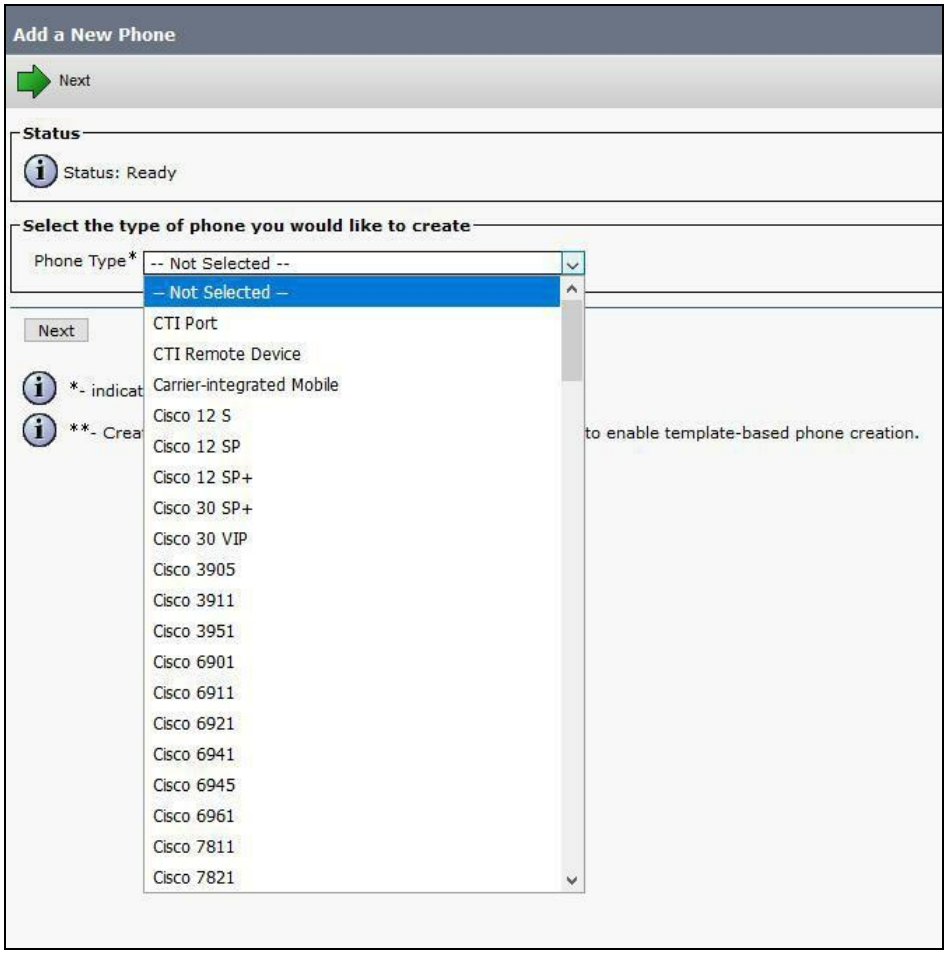


Figure 176: Select the Phone Model

If, for example, the phone selected is Cisco 8851, the page to choose SCCP

or SIP will not be shown, as this phone model only has SIP support. After selecting the phone, the following window will ask the phone information, such as MAC Address, Description, Device Pool, etc.

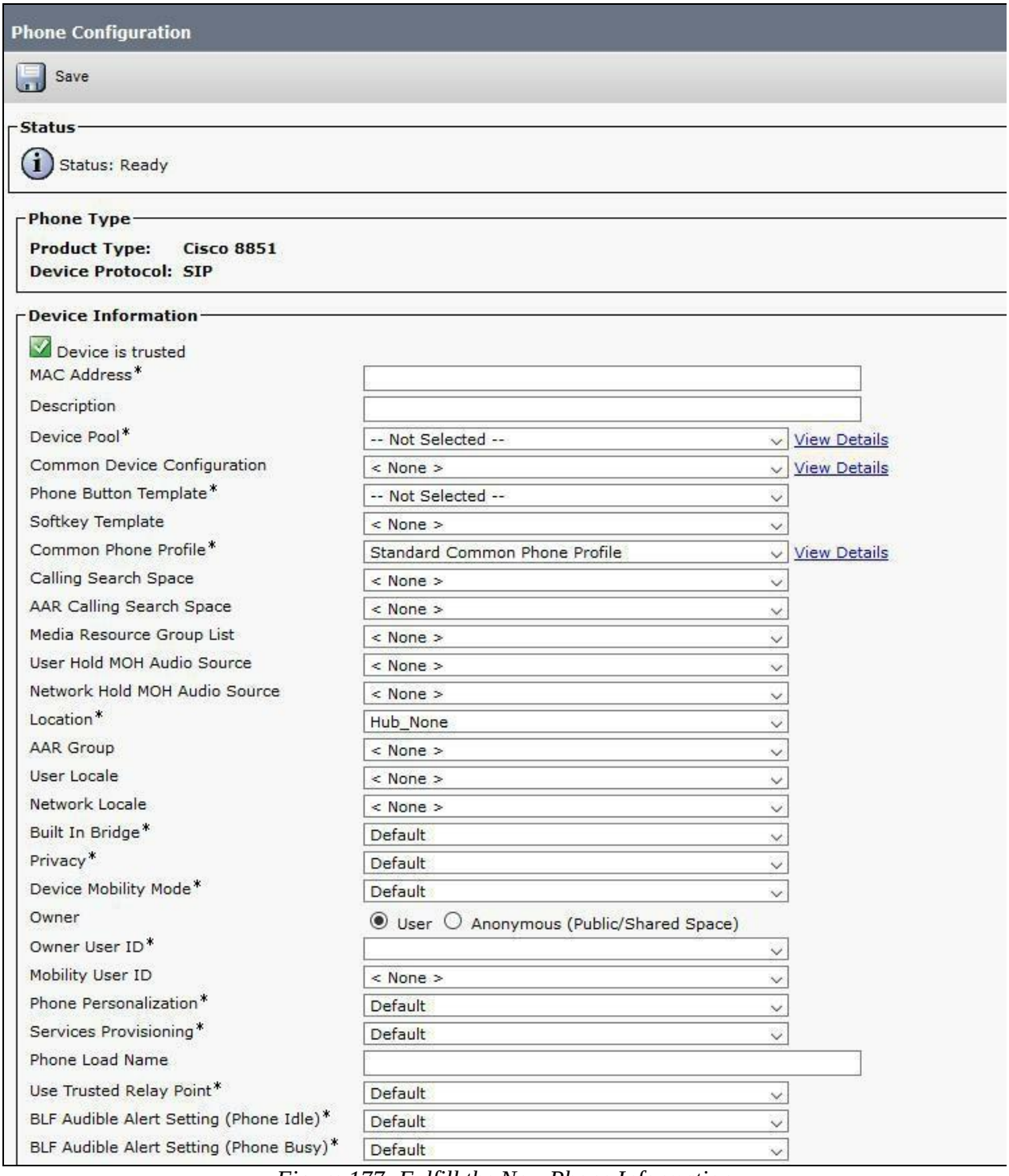


Figure 177: Fulfill the New Phone Information

There are a lot of required fields, but some of them are already filled with the

default options. What you usually need to type/select is:

MAC Address	Type in the MAC Address of the phone; 12 characters, no space or symbols.
Device Pool	If there is no specific Device Pool for this phone, select the "Default" Device Pool.
Phone Button Template	If there is no specific Phone Button Template created, select the basic for your phone, e.g. "Standard 8851 SIP".
Owner/Owner User ID	If there is no specific user to this phone, select Anonymous (Public/Shared Space).
Device Security Profile	If there is no specific configuration, select the basic for this phone model, e.g.: "Cisco 8851 - Standard SIP Non-Secure Profile".
SIP Profile	If there is no specific SIP Profile created for this phone, select the basic "Standard SIP Profile".

Table 19: Information required to create a New Phone

After this information is included, click "Save" to create your Phone. The next step is to create a new extension or associate an existing extension to this phone.

Extension Creation / Association

To create a new line or associate an existing line with your phone, on the top-left corner of the Phone Configuration Window, click “Add a new DN”.

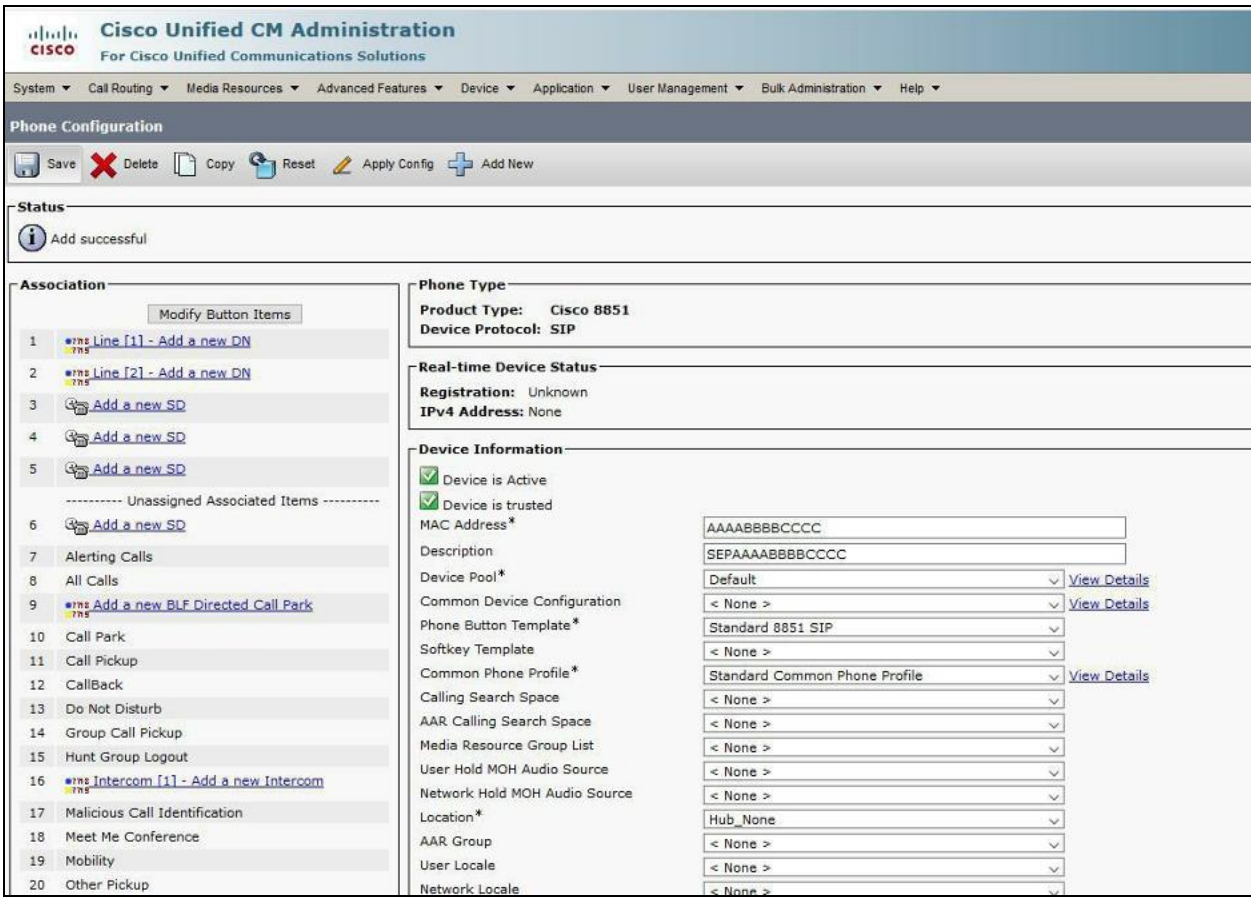


Figure 178: Phone Configuration Windows

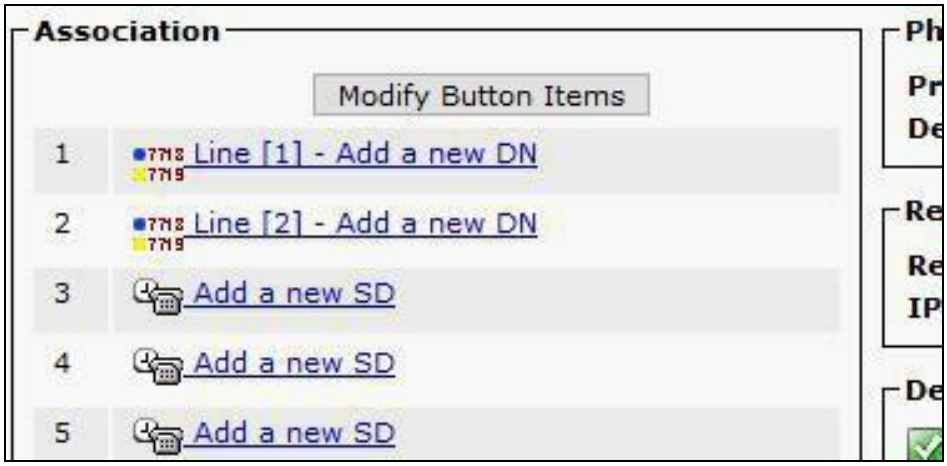


Figure 179: Add a New DN link

The Directory Number Configuration window will open. The most important fields to fulfill here are:

Directory Number	Type the extension number you want to assign to this phone.
Route Partition	Select the Route Partition you want to assign to this extension.
Calling Search Space	Select the Calling Search Space you want to assign to this extension. This configuration will define to where this directory number will be able to call (internal extension, external, mobiles, long distance, international, etc.).

Table 20: Directory Number Information

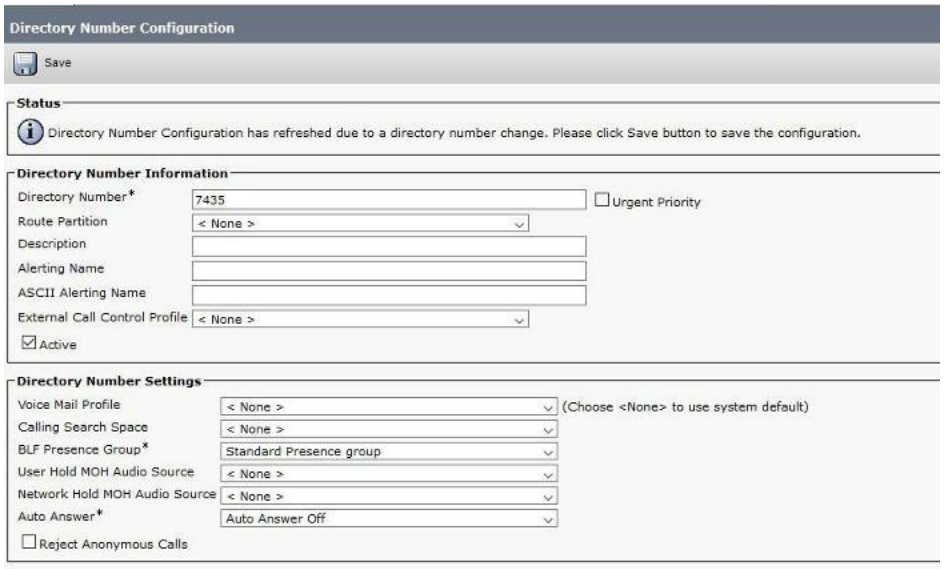


Figure 180: Add a New Directory Number page

On this page, you can also select other relevant information about this extension, like:

Description	A description, usually the name and last name of the owner of this extension.
Alerting Name	This is how a call from this extension will appear on another phone screen when the call is made.
ASCII Alerting Name	Same as above, but for phones that only accept ASCII characters (old models).
Active (checkbox)	If this line will be activated or not.
Voice Mail Profile	If there is a voicemail available on this CUCM (usually Cisco Unity Connection), select the voicemail profile here.
BLF Presence Group	If there is a Cisco Presence available on the CUCM, select the Busy Lamp Field Presence Group here. This field will indicate who can see the phone status of this line.
User Hold MOH Audio Source	Choose the audio caller will hear when this user initiates a hold action.
Network Hold MOH Audio Source	Choose the audio caller will hear when the network initiates a hold action (like during a transfer).
Auto Answer	Select if you want to activate the Auto Answer feature on this line. The options are: Auto Answer Off <Default> Auto Answer with Headset Auto Answer with Speakerphone
Forward All (Destination)	If you want to forward all calls sent to this extension, type the number on this form box.
Forward All (Calling Search Space)	Used to select which CSS will be used on the option above (Forward All Destination box).
No Answer Ring Duration (seconds)	Duration of ringing for this line before taking another action. Usually, one ring takes 3 seconds. As an example, if you want this extension to ring five times before the calling gets a busy tone, select 15 seconds.
Call Pickup Group	If there are Call Pickup Groups available on your CUCM, select the Group this line belongs.
Display (Caller ID)	Used to display information of this phone user when the call is connected.
	Same as below, but to phones which only accept

Technet24

ASCII Display (Caller ID)	ASCII characters (old models).
Line Text Label	The message on the phone screen, right on the side of the line button. If blank, this will show the extension number.
External Phone Number Mask	The message on the top phone screen, right on the side of the line button. If blank, this will show the extension number. You can use the format with XXXX in the end, example: +1408555XXXX, and this will fulfill the last 4 digits with the extension number.
Maximum Number of Calls	The number of simultaneous calls this extension can have active, including placed and received.
Busy Trigger	The number of calls this phone can receive before it starts to reject with a busy cause.

Table 21: Some important options on Directory Number Configuration page

There are two options very similar, “Alerting name” and “Display (Caller ID)”. The main difference is:

Alerting name	Used for Ring in state.
Display (Caller ID)	Used for Connected state

Table 22: Alerting name x Display (Caller ID) difference

To simplify, set the same values to both fields.

There are more options to select on this page. To understand all available options, remember you can always use the CUCM Help Web Page, under menu “Help > This Page”.

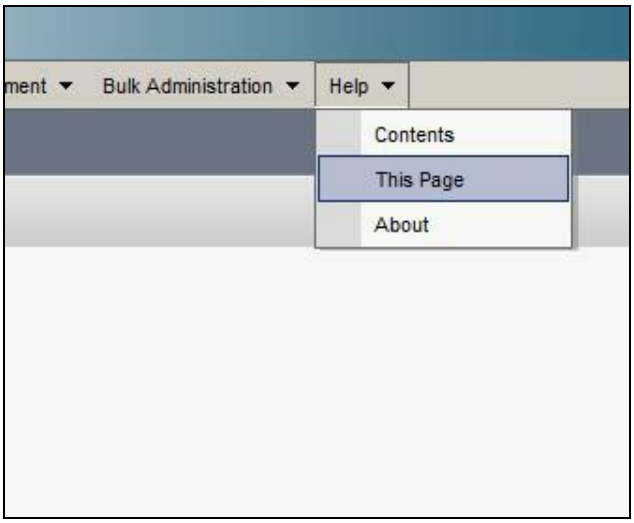


Figure 181: Help > This Page Menu

Phones Auto-registration

The “Phones Auto-registration” feature enables your CUCM server to automatically accept all Cisco Phones that are attempting to register to the CUCM Cluster. It also provides an automatic extension to these phones. It’s like a DHCP Server, but instead of delivering IP Address, it provides extension numbers to all phones that request it.

This function is frequently used in large CUCM environment with thousands of phones, where you want to provide at least the essential internal call ability to all phones easier.

You need to create an extension numbers range (like from 1000 to 1999), and phones will get these extensions during the registration process. The steps are:

1. IP Phone goes to the TFTP Server looking for configuration files
2. The TFTP Server sends an XML file to phones with Registration information
3. Phones Attempt to register with configured CUCM
4. Auto-registration that automatically provides extension 1001 to Phone

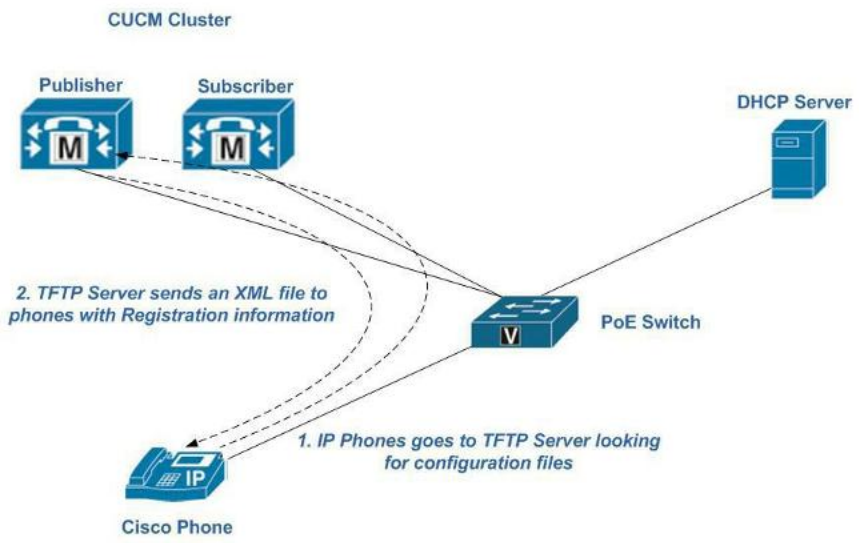


Figure 182: Cisco Phone connecting to TFTP Server

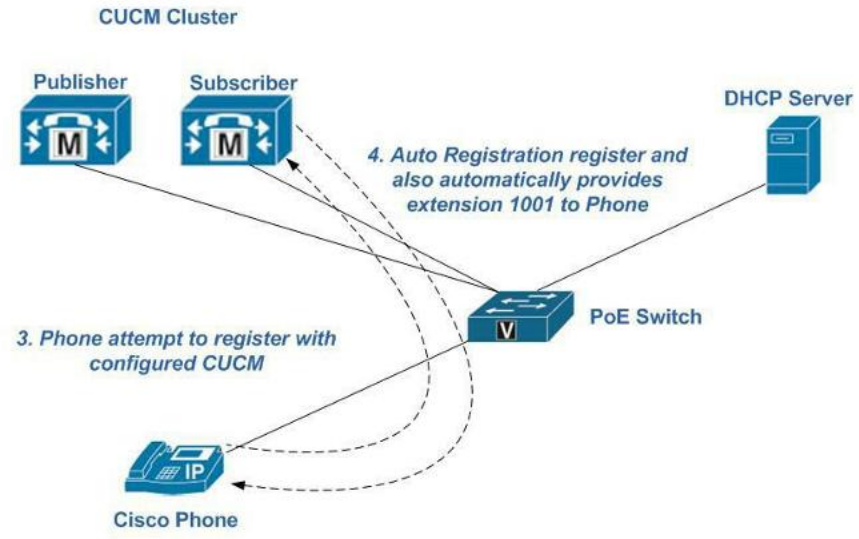


Figure 183: Cisco Phone auto registering

CUCM disables Auto-registration by default. To enable it, configure it in the menu “System > Cisco Unified CM” and selecting the server where you want to enable the Auto-registration feature.

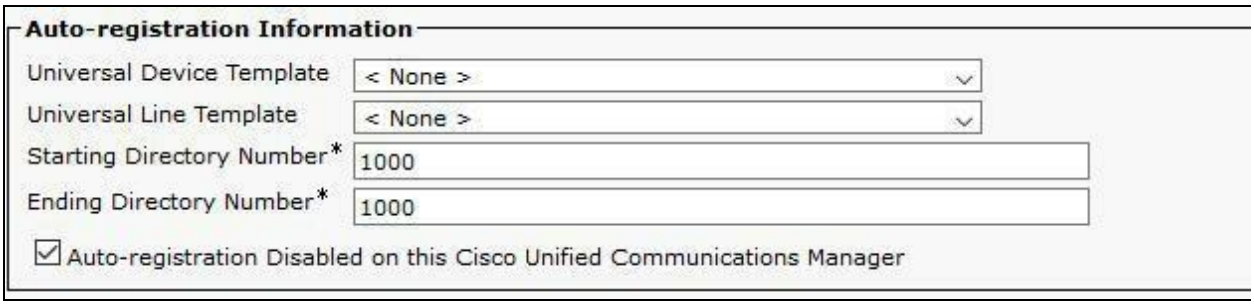


Figure 184: Auto-Registration Information

When you click on “Auto-registration Disabled on this Cisco Unified Communications Manager”, the following pop-up will appear:



Figure 185: Auto-Registration pop-up

You also need to select the "Universal Device Template" and "Universal Line Template" fields.

To edit the "Universal Device Template" field, go to “User Management > User/Phone Add > Universal Device Template; and to edit the "Universal Line Template", go to “User Management > User/Phone Add > Universal Line Template.

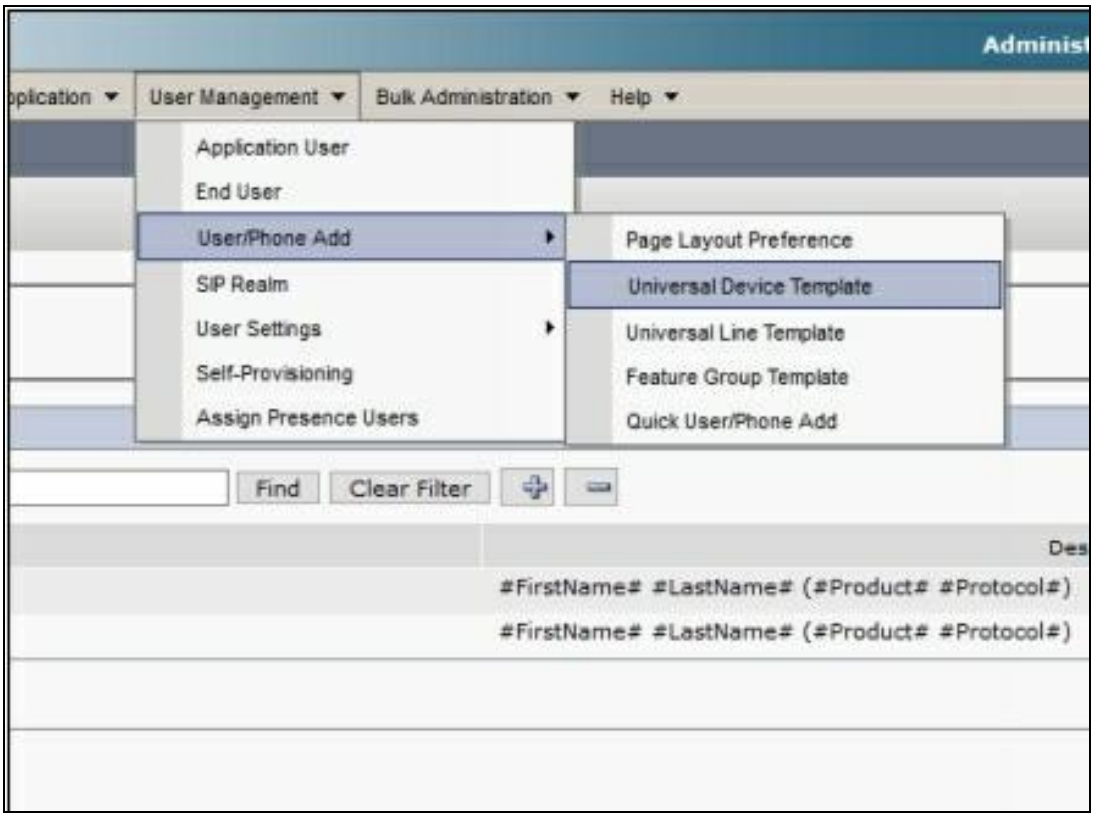


Figure 186: Universal Device Template menu

If editing of these fields is not wanted, select the defaults values, then type the extension range you want to use on “Starting Directory Number” and “Ending Directory Number”.

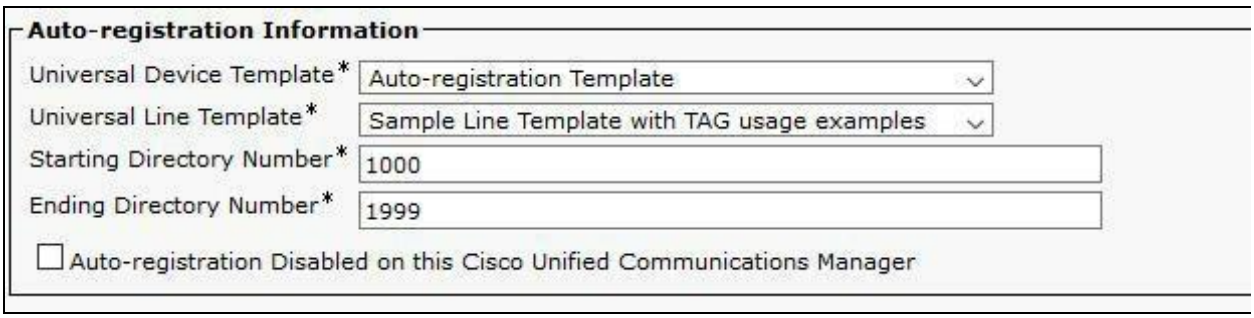


Figure 187: Auto-Registration Information

With this configuration, the next unknown phone trying to register on CUCM for the first time will receive the extension 1000. The second, extension 1001. This will go until the CUCM provides the extension 1999 to a phone.

If these auto-registration numbers get exhausted, the next phones will not get an automatic extension, and the phone will not register; you may need to increase the ending directory number to have the auto-registration working

again.

Of course, the auto registration does not apply to phones which are already configured on CUCM. To all know phones, the CUCM will provide the correct extension this phone has set.

Usually, I like to have extension mobility enabled on the CUCM. As soon as I have the user phone registered, I can ask him which extension his phone got, and replace it with the correct extension number if necessary. This makes the registration process more manageable, as I don't have to ask the end user which MAC Address his phone has.

Bulk Administration Tool

The Bulk Administration Tool is a menu available only at CUCM Publisher where you can perform bulk transactions to the CUCM database. You can use it to add, update, or delete many similar phones, users, or ports at the same time.

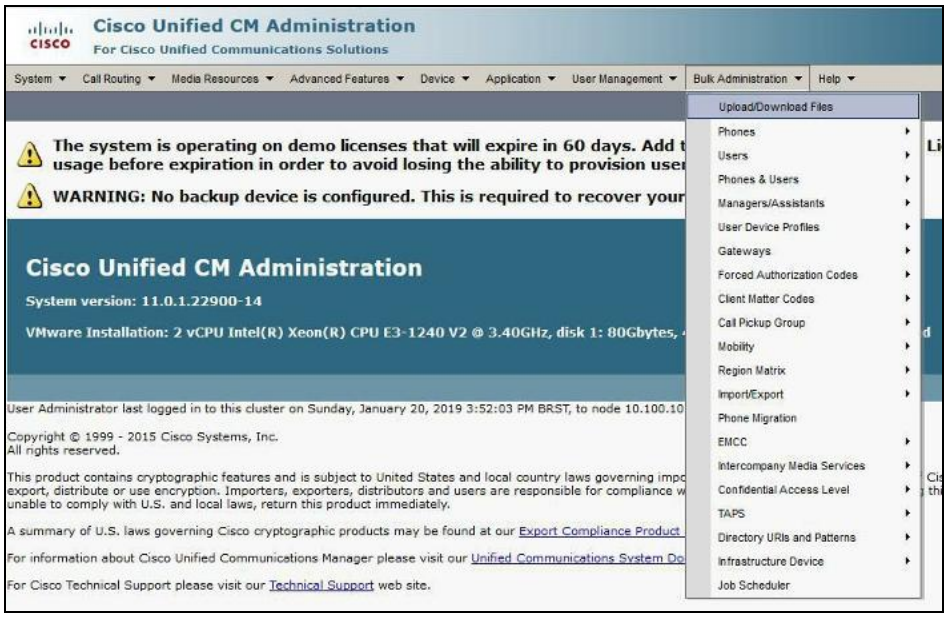


Figure 188: Upload/Download Files menu

As you can see, there is plenty of options available on the Bulk Administration menu. Here, we will cover only the Insert Phone option.

To insert a phone via Bulk, go to "Bulk Administration > Phones > Insert a Phone";

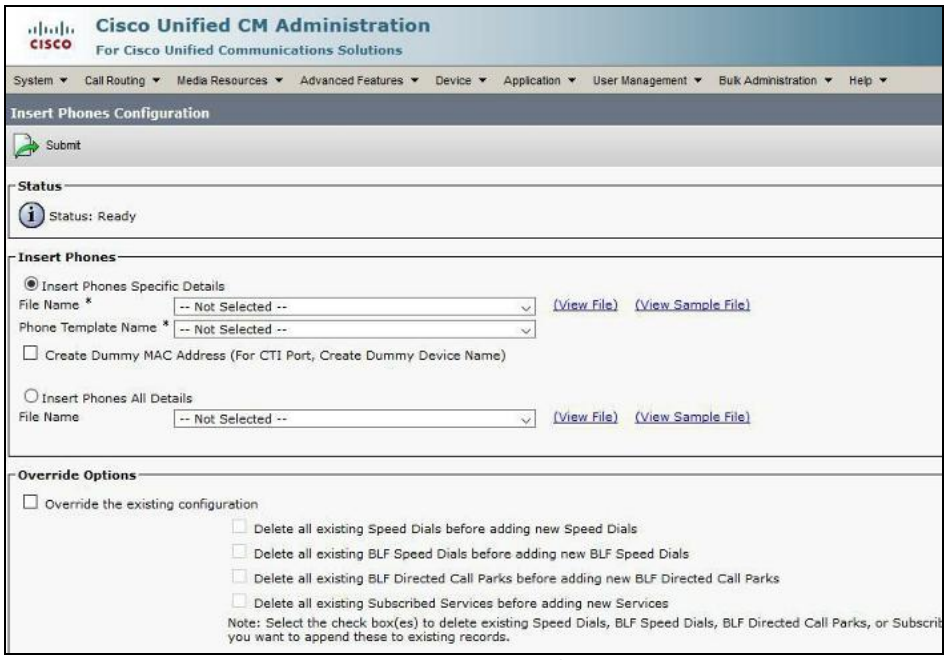


Figure 189: Insert Phones Configuration window

In the “Insert Phones Configuration” window, you have two main options:

Insert Phones Specific Details	Easier option. Better when you will prepare your script from scratch, and you only need to insert the phones on CUCM with basic configs.
Insert Phones All Details	Useful if you have a file exported from another CUCM server, but it can be hard to use as some field names can change from one CUCM version to another, so you may need to “clean up” or correct a file exported on another CUCM before insert it here.

Table 23: Insert Phone options

To see a file sample, click on (View Sample File):

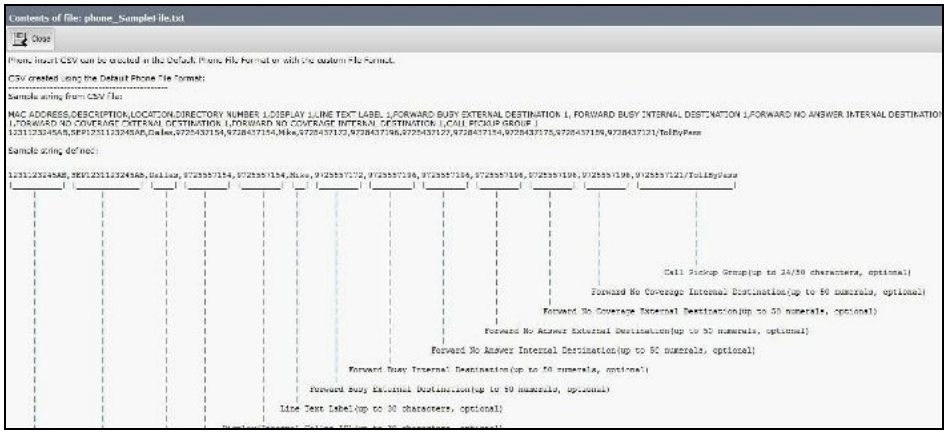


Figure 190: Insert Phone sample file

Here is the file format. It must be a .CSV (comma-separated values) file with these fields:

MAC ADDRESS,DESCRIPTION,LOCATION,DIRECTORY NUMBER 1,DISPLAY 1,LINE TEXT LABEL 1,FORWARD BUSY EXTERNAL DESTINATION 1, FORWARD BUSY INTERNAL DESTINATION 1,FORWARD NO ANSWER INTERNAL DESTINATION 1,FORWARD NO ANSWER EXTERNAL DESTINATION 1,FORWARD NO COVERAGE EXTERNAL DESTINATION 1,FORWARD NO COVERAGE INTERNAL DESTINATION 1,CALL PICKUP GROUP 1

The only mandatory field is the MAC Address.

Scroll down to see a more straightforward sample file:

MAC ADDRESS,DESCRIPTION,DIRECTORY NUMBER 1
2234900AEF01,SEP2234900AEF01,9725098827

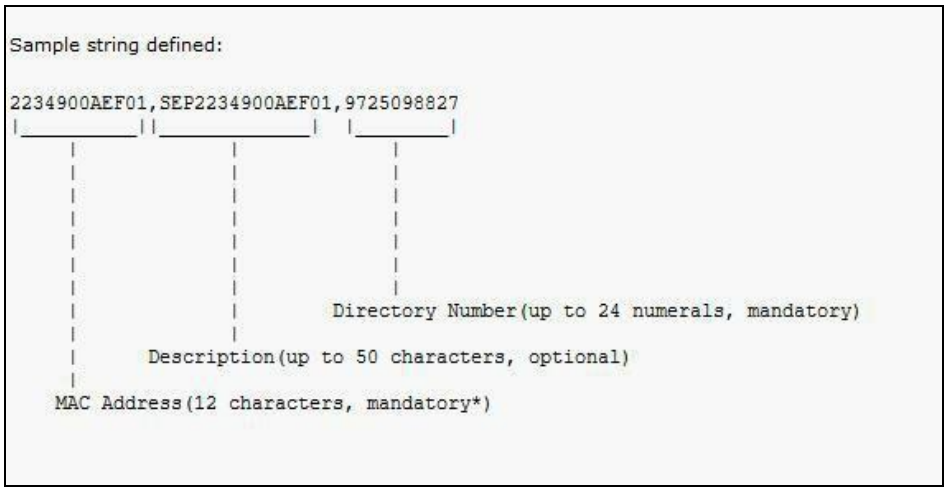


Figure 191: Insert Phone sample file

You need to prepare this file in a basic text editor like Microsoft Notepad. You can also use Microsoft Excel to adjust all your phones data, but before upload the CSV file on CUCM, try to open it on Notepad to make sure all the data is formatted correctly. Some Excel versions can change the comma to a semicolon in the final CSV file. If this happens to you, use Notepad "Replace" function to correct the file.

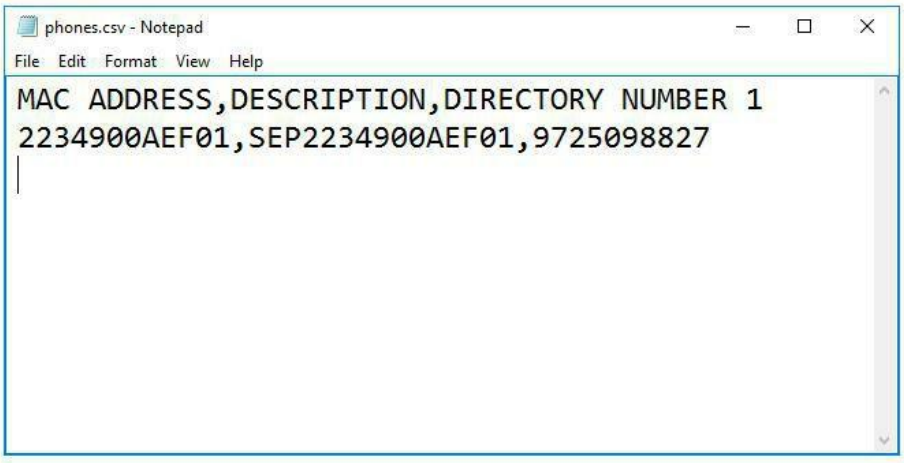


Figure 192: phones.csv file example

With the file ready, upload it to “Bulk Administration > Upload/Download Files > Add New”.

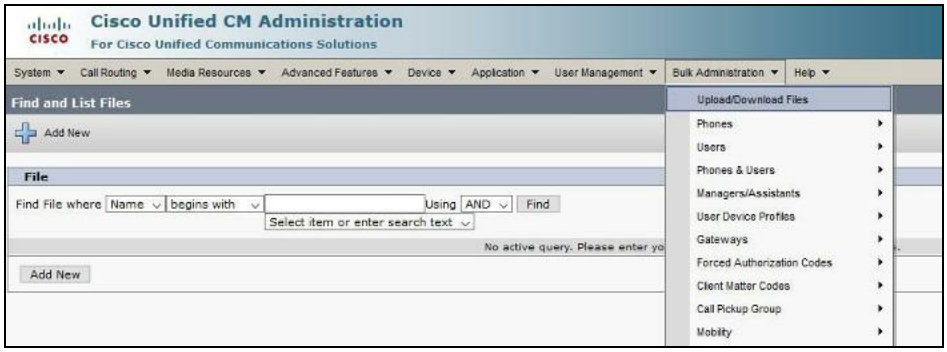


Figure 193: Upload/Download Files menu

Select the newly created file, then select the target “Phones” and the Transaction type as “Insert Phones - Specific Details” and click “Save”.

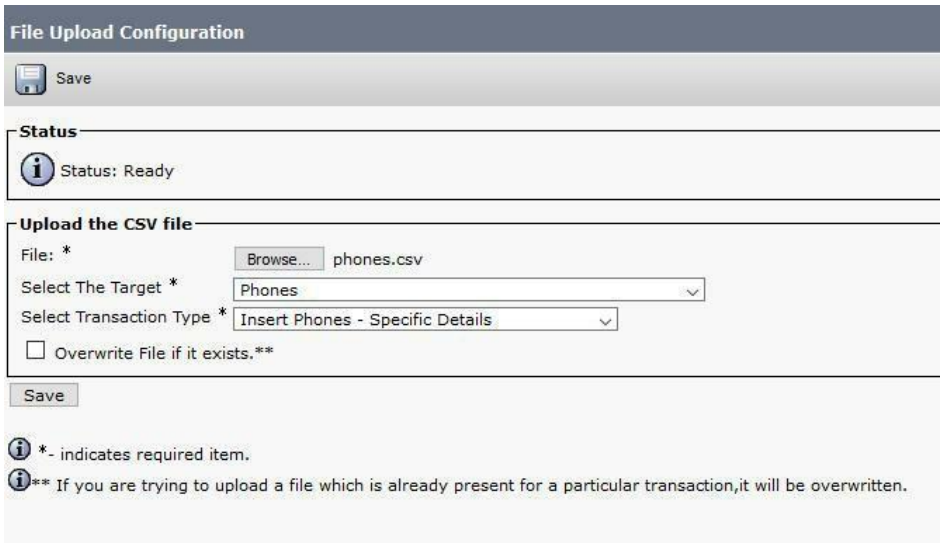


Figure 194: File Upload Configuration window

When you receive the "Upload successful" message, go to the next step: to prepare the phone template. Go to "Bulk Administration > Phones > Phone Template > Add New".

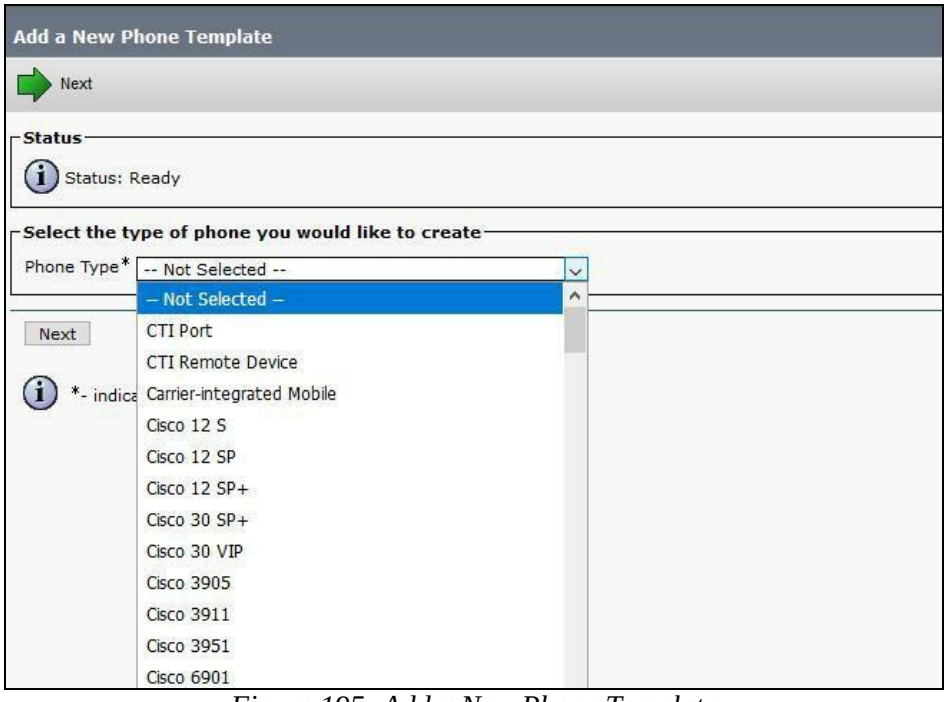


Figure 195: Add a New Phone Template

Now, select the phone type you would like to create a template for. In my case, I'll choose Cisco 8851. Create a name for this template and fill in all the information you want, including the main configurations for your phone model, like Device Pool, Phone Button Template, Device Security Profile,

SIP Profile, etc., and save it.
Now you also need to configure a line template associated with this Phone Template. To do it, on the Phone Template Configuration window, on the top-left corner, click in “Line [1] - Add a new DN”:



Figure 196: Phone Template Configuration window

Select the same configurations you would select if you were creating a regular directory number, except the first option that is "Line Template Name" instead of "Directory Number".



Figure 197: Phone Template Configuration window

Finally, go back to "Bulk Administration > Phones > Insert a Phone" and select the file and the created template.

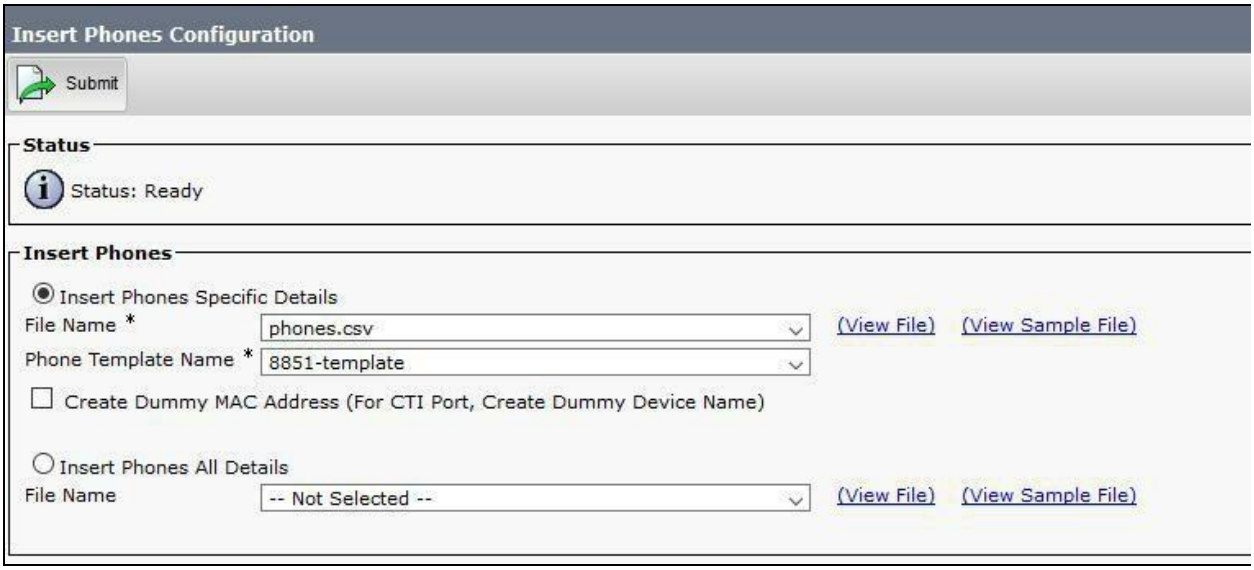


Figure 198: Insert Phones Configuration window

Then, at the bottom of the page, select "Run Immediately" and click "Submit".



Figure 199: Insert Phones Configuration window

If the configuration is successful, you will see this screen:



Figure 200: Insert Phones Configuration window

Finally, go to "Bulk Administration > Job Scheduler" to check if there was an error on the job.

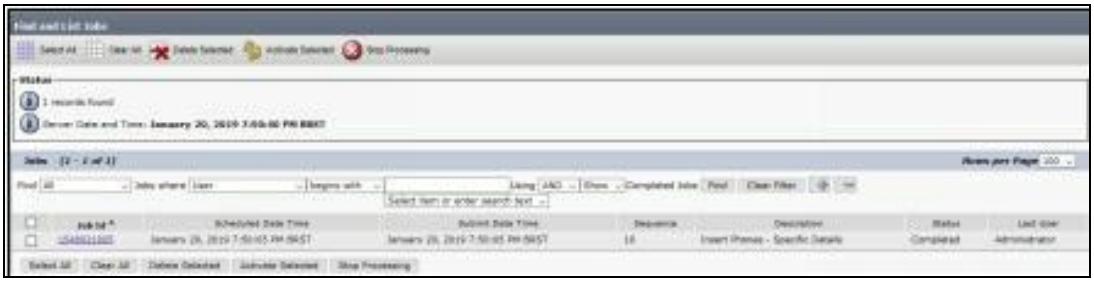


Figure 201: Find and List Jobs window

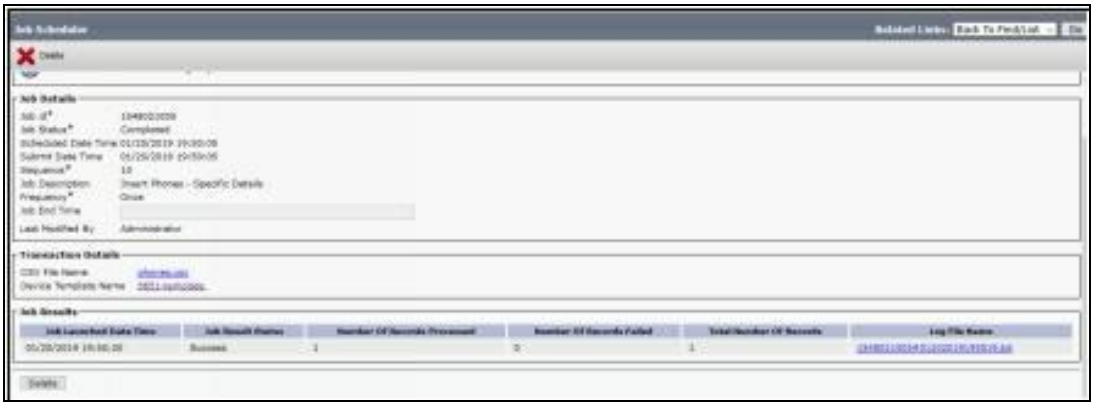


Figure 202: Job Scheduler configuration window

As seen here, there are several steps to insert a phone via Bulk. This process is only attractive if you have a vast quantity of phones to add.

Registration Troubleshooting

Some basic steps to check the phone registration is:

- **Check if the phone has received an IP Address**

You can check this on the Phone Screen. If you don't have physical access on the phone, try to check on your DHCP Server if there is any log of this phone DHCP Request.

- **Check the phone Web Page**

By default, Cisco Phones have an HTTP web page. If the phone IP Address is known, type it in the Google Chrome, Firefox or Internet Explorer, and try to find message logs about a registration problem.

- **Check if the phone MAC Address is correct**

Confirm if the phone MAC Address is the same as configured on CUCM.

- **Check if the phone model is correct**

Confirm if the phone model is the same as configured on CUCM.

- **Check if is there any firewall blocking the registration traffic**

If there is a firewall on the network path between your CUCM and your phones, you may need to create rules allowing this phone/CUCM connectivity.

- **Set the TFTP Address manually**

If your DHCP server is not providing the DHCP option 150 (TFTP Server), you can try setting the TFTP Address manually on the phones. This configuration is a little different on each phone model, but usually, it is on "Configuration > Network > IPv4 > TFTP Server".

- **Delete the CTL File**

If the phone is registered on a CUCM Cluster and is moved to a different CUCM Cluster, it is necessary to delete the Certificate Trust List (CTL) file. It is a list of CUCM Servers that this phone can register to in a Certificate file.

The configuration necessary to delete it depends on the phone model, but usually, you can find it navigating on the phone menu. If you cannot see this option there, check the phone manual to delete this file.

- **Perform a phone factory reset**

This option must be used as a last resort. It will clean all your phone configuration, including network configuration, CTL file, and all other configurations. The factory reset depends on the phone model, but usually is one of these procedures:

1. Remove power from the phone (Unplug the power adapter or Unplug the LAN cable); Press the pound (#) key and plug the phone in; When the Headset and Speaker buttons are lit, enter the following key sequence: 123456789*0#

2. On the phone menu, go to Applications > Administrator Settings > Reset Settings > All.

CHAPTER 7 - VOICE GATEWAYS

Voice Gateways enable the interoperability between the VOIP environment and the old telephony phone systems.

There are four main protocols to connect Voice Gateways on CUCM:

- H.323
- SIP
- MGCP
- SCCP

H.323 and SIP devices are different from MGCP and SCCP devices, because they can process the calls without a CUCM involved.

Protocol	Need CUCM available to process calls?
H.323	No
SIP	No
MGCP	Yes
SCCP	Yes

Table 24: H.323, SIP, MGCP and SCCP - CUCM comparison

In this chapter, we will check how to configure H.323, MGCP and SCCP Gateways, and also, some cards and interfaces normally used in Cisco Voice Gateways.

> **Note:** SIP Protocol will be discussed in chapter 9, “Trunks”.

H.323 Gateway

H.323 was one of the first widely-deployed VoIP Protocols. It was also the first VoIP standard to adopt standard Real-time Transport Protocol (RTP) to transport audio and video over IP networks. In an H.323 Network we can

have voice, video, and presentations.

H.323 is the default voice codec in a Cisco Voice router. Until nowadays, when you create a dial-peer, unless you specify that you would like to make it a SIP dial-peer, this will be an H.323 dial-peer by default.

H.323 Gateways are devices able to process the calls completely. When CUCM sends a call setup to an H.323 Gateway, it needs to have dial-peers to receive this call (inbound) and dial-peers to send out this call (outbound). If you do not create an inbound dial-peer to receive calls, the router will use the default dial-peer 0, which accept any codec (G.729, G.711, etc.) and has VAD (Voice Activity Detection) enabled. You cannot change the configuration on this dial-peer 0, so it's highly recommended that you create your default inbound dial-peer to receive calls (VoIP and/or POTS).

H.323 Configuration on Cisco Router

There are many configuration possibilities to create an H.323 Gateway. We will check some of the main configurations available:

voice service voip

The "voice service voip" configuration is a global configuration on a Cisco Voice Router. Here you can configure a lot of parameters, but we will focus on these 3: "ip address trusted authenticate", "allow-connections" and "h323" submenu. Follow a basic example configuration:

```
voice service voip
ip address trusted list
  ipv4 10.10.10.0 255.255.255.0
  ipv4 192.168.0.0 255.255.0.0
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
h323
  no h225 timeout keepalive
  call preserve limit-media-detection
```

ip address trusted list

When you type "voice service voip" and press enter, you will enter a new

command sublevel on the voice gateway. There, the first thing we can configure is the IP Address Trusted List:

```
voice service voip
ip address trusted list
  ipv4 10.10.10.0 255.255.255.0
  ipv4 192.168.0.0 255.255.0.0
```

This command is part of a Toll-Fraud Prevention Feature implemented by Cisco in 2010, IOS Release 15.1(2)T. This is like an access-list specifically to VoIP calls. Before this command, Cisco Voice Gateways accepted calls from all IP sources, which can be considered a security risk.

To configure this parameter, type all the subnets you would like to allow VoIP calls on your gateway. This includes your CUCM IP Addresses, the subnet of all your phones. This command accepts up to 100 subnets; if you have more than this, you can try to summarize the network mask to reach all your networks.

To Identify if Toll-Fraud Prevention Feature is Blocking Your Call, run the commands "debug voip ccapi inout" and "terminal monitor" and search for the "_ManagedAppProcess_TOLLFRAUD_APP" and "Cause Value=21", which represents ‘Call Rejected’.

```
ROUTER# debug voip ccapi inout
ROUTER# terminal monitor
ROUTER#
%VOICE_IEC-3-GW: Application Framework Core: Internal Error (Toll fraud call rejected):
IEC=1.1.228.3.31.0 on callID 3 GUID=F146D6B0539C11DF800CA596C4C2D7EF
000183: *Apr 30 14:38:57.251: //3/F146D6B0800C/CCAPI/ccCallSetContext:
   Context=0x49EC9978
000184: *Apr 30 14:38:57.251: //3/F146D6B0800C/CCAPI/cc_process_call_setup_ind:
   >>>>CCAPI handed cid 3 with tag 1002 to app "_ManagedAppProcess_TOLLFRAUD_APP"
000185: *Apr 30 14:38:57.251: //3/F146D6B0800C/CCAPI/ccCallDisconnect:
     Cause Value=21, Tag=0x0, Call Entry(Previous Disconnect Cause=0, Disconnect Cause=0)
```

The Toll Fraud is blocking this call above, as the IP address or subnet of the device placing the call was not added to the “ip address trusted list”.

To disable these debugs, type:

```
ROUTER# undebug all
ROUTER# terminal no monitor
```

As this is a security feature, it is not recommended that you disable Toll-Fraud Prevention Feature. But if you decided to, there are two ways to disable it:

- Add the subnet 0.0.0.0 0.0.0.0 (all subnets) to the ip address trusted list:

```
voice service voip
ip address trusted list
  ipv4 0.0.0.0 0.0.0.0
```

- Disable the toll-fraud prevention application:

```
voice service voip
no ip address trusted authenticate
```

I have worked with some routers where both commands were available, but the configuration only worked with the first one (probably a software bug).

Allow-connections

By default, Cisco Voice Gateways does not allow VoIP to VoIP calls, as usually they are used to connect VoIP Networks to the plain old telephone system (POTS), which is the telephony world we usually know (PSTN, Mobile Phones, Fax Machines, etc.).

To allow VoIP to VoIP calls, you need to enable these commands:

```
voice service voip
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
```

Follow what these commands do:

Command	Explanation
allow-connections h323 to h323	Allow a incoming H.323 call to go outside via another H.323 dial-peer
	Allow a incoming H.323 call to go outside via another SIP

allow-connections h323 to sip	dial-peer
allow-connections sip to h323	Allow a incoming SIP call to go outside via another H.323 dial-peer
allow-connections sip to sip	Allow a incoming SIP call to go outside via another SIP dial-peer

Table 25: allow voip to voip calls commands

Please note that you don't need to enable all of these four commands. You need to verify which one you need on your VoIP network; if necessary, enable them all, if not, enable what you need.

H323 submenu

Inside "voice service voip", we have a dedicated menu to H.323 parameters, but usually, it's not necessary to configure none of these parameters, as the default H.323 values works very well.

```
voice service voip
h323
  no h225 timeout keepalive
  call preserve limit-media-detection
```

These two commands above are related to H.323 Call Preservation for H.323 VoIP Calls when we are running SRST Mode on our gateway.

Voice class codec

By default, when a Cisco device places a call, it will negotiate the codec to be used with the remote end of the call. Voice class codec is an ordered list of codecs that a router can use to select the codec of a call. The routers negotiate with the remote end, and they will decide the best codec based on this list.
Let's see an example. Router01 and Router02 negotiate a call:

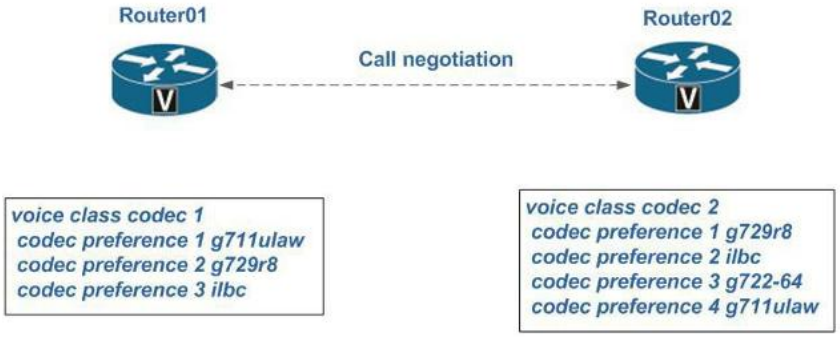


Figure 203: voice call codec negotiation

Preference order	Router A Codec List	Router B Codec List
preference 1	g711ulaw	g729r8
preference 2	g729r8	ilbc
preference 3	ilbc	g722-64
preference 4	-	g711ulaw

Table 26: codec preference list

As a result, this call will be placed using G.729, which is the first codec that matches between these two routers.

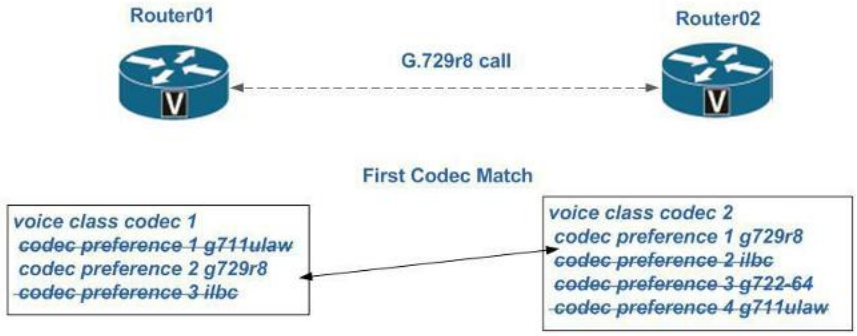


Figure 204: voice call codec negotiation

A codec voice class must be applied to a dial peer, which then follows the preference order defined in the codec voice class.

```
dial-peer voice 1 voip
destination-pattern 4...
session target ipv4:10.53.32.11
```

```
voice-class codec 1
```

The configuration above will apply the voice-class codec 1 to dial-peer voice 1 voip.

> **Note:** To create the voice-class, the command is “voice class codec <number>”, but to apply it to a dial-peer, the command is “voice-class codec <number>”.

Voice Translation-Profile

Voice translation-profiles are used to manipulate the calling and/or called digits in a call. It is useful when to remove an access-code (like 9 in from of a PSTN call), edit the dialing format (to include any special code), mask the source or change the destination of a call.

We will check the translations-profile in depth in Chapter 10, “Digits Manipulation.”

Dial-peers

Dial-peers are the most important thing related to call routing on a Cisco Voice Gateway. It’s where we allow and configure the router to place and receive all calls to the correct destinations. Making a comparison, it’s like the static routes in the IP Routing environment. But differently from the IP routing, there is no automatic routing protocol for the VoIP networks (I mean, there was at least one from Cisco, Service Advertisement Framework (SAF), but it’s not widely used, even on Cisco environments).

So, dial-peers are one of the main concepts to be fully understood.

```
dial-peer voice 4 voip
description TO CUCM PUB
destination-pattern 3...$
session protocol sipv2
session target ipv4:10.10.20.30
dtmf-relay sip-kpml rtp-nte
no vad
```

As this is a critical topic, we will check the dial-peers in more depth in Chapter 10, “Digits Manipulation.”

H.323 Configuration on CUCM

To create a H.323 Gateway on CUCM, you need to:

- Menu "Device > Gateway";
- Click "Add New";
- Select the Gateway type as “H.323 Gateway” and click “Next”;

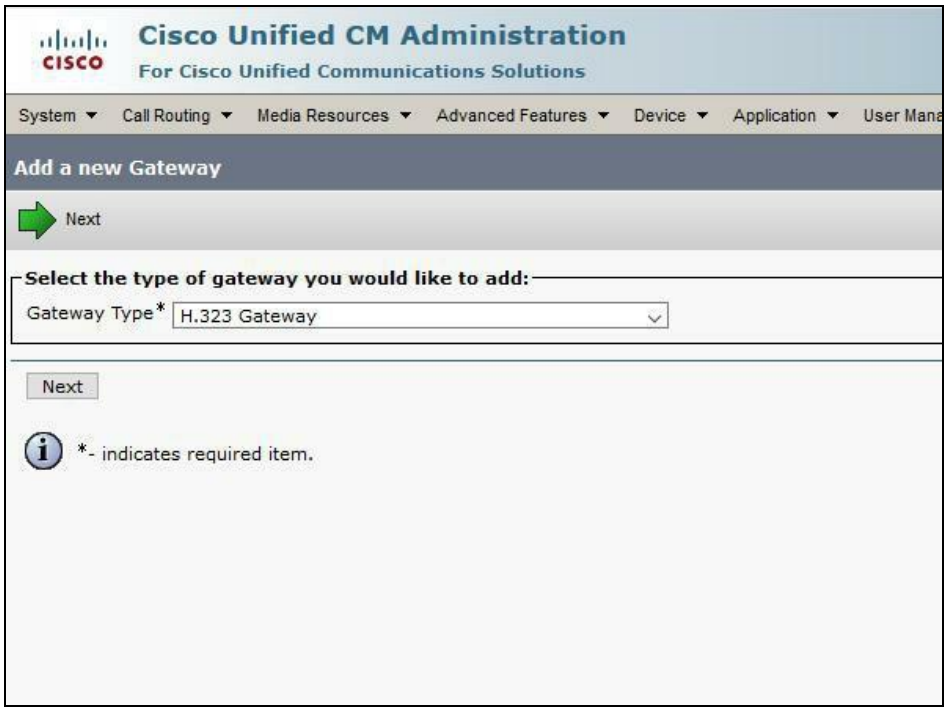


Figure 205: Add new H.323 Gateway

- Fill the device name field with the H.323 Gateway IP Address;
- Select the Device Pool;
- Save it;
- Click in “Reset” - pop-up will open - click again in “Reset”.

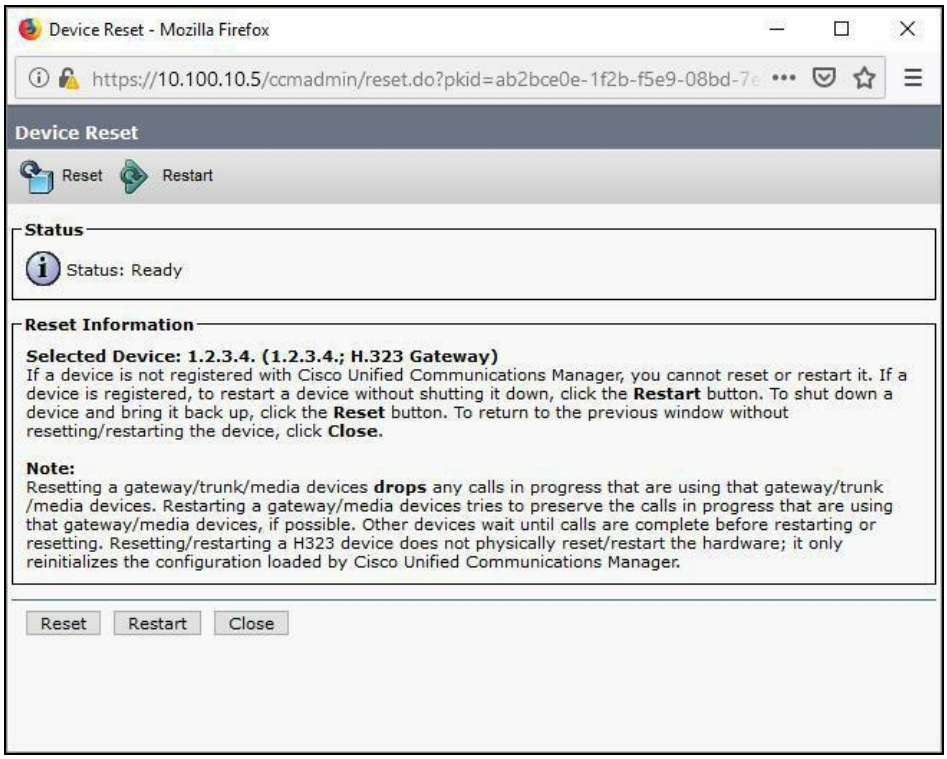


Figure 206: H.323 Gateway Reset

This configuration is enough to have your H.323 created. To have it working on your environment, you will probably to change more settings. Do not forget to edit the "Call Routing Information - Inbound calls - Calling Search Space" configuration, as it will define the CSS to all your incoming calls from this H.323 Gateway. If this field is incorrect, you will not receive calls from this gateway. In the example below, I changed my inbound CSS to "INTERNAL_CSS", so I can reach all my internal extensions.

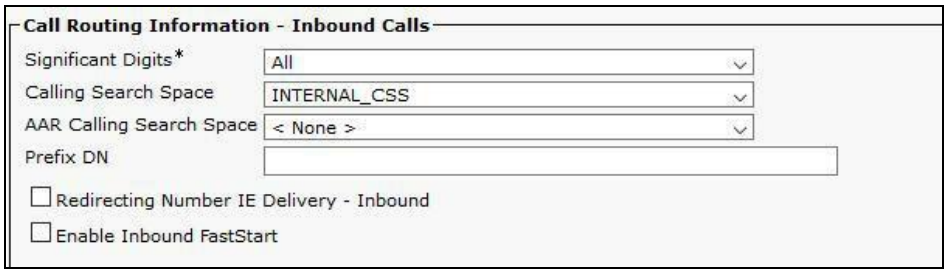


Figure 207: H.323 Gateway Inbound Call configuration

At this point, besides there's a lot of other H.323 configuration available, this gateway is configured on CUCM. However, it is not ready to receive calls from this gateway, as there is no dial-peer on this router to send calls to CUCM, and also it's not prepared to forward calls to the PSTN, as there are no Route Patterns configured on CUCM. We will complete this gateway

configuration on Chapter 9, “Call Routing”.

MGCP Gateway

MGCP is a master/slave protocol that allows CUCM to control all ports on a gateway. Differently of what happens on an H.323 and SIP Gateway, with MGCP the gateways do not have the call "intelligence", and all decisions are made in CUCM, which inform to the Gateway what action it should take at any time. Cisco CallManager knows and controls the state of each configured MGCP port on the gateway.

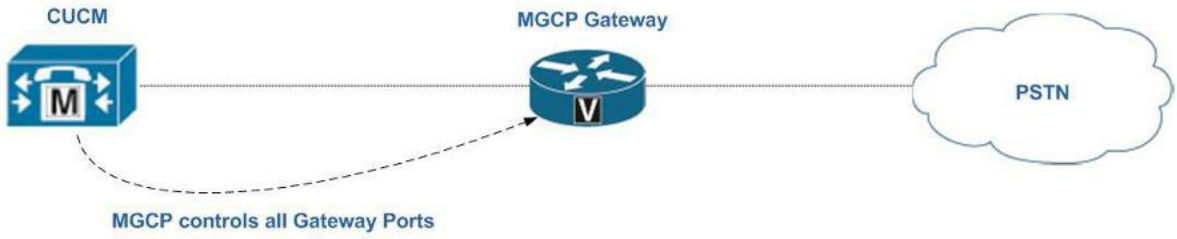


Figure 208: CUCM MGCP Gateway

The MGCP Gateway must register on CUCM. After it is registered, the CUCM becomes his "Master", and the MGCP Gateway, its "Slave"; this provides the advantage of centralized gateway administration, used in largely scalable IP Telephony solutions.

CUCM can control all configured ports, even if these ports are connected to the public switched telephone network (PSTN), legacy PBX, voice mail systems, plain old telephone service (POTS) phones, etc.

Configuring a MGCP Gateway on CUCM

To configure your MGCP Gateway on the CUCM, the steps are:

- Menu "Device > Gateway"
- Click "Add New"
- Select your router type on the list of models available, then, click "Next"

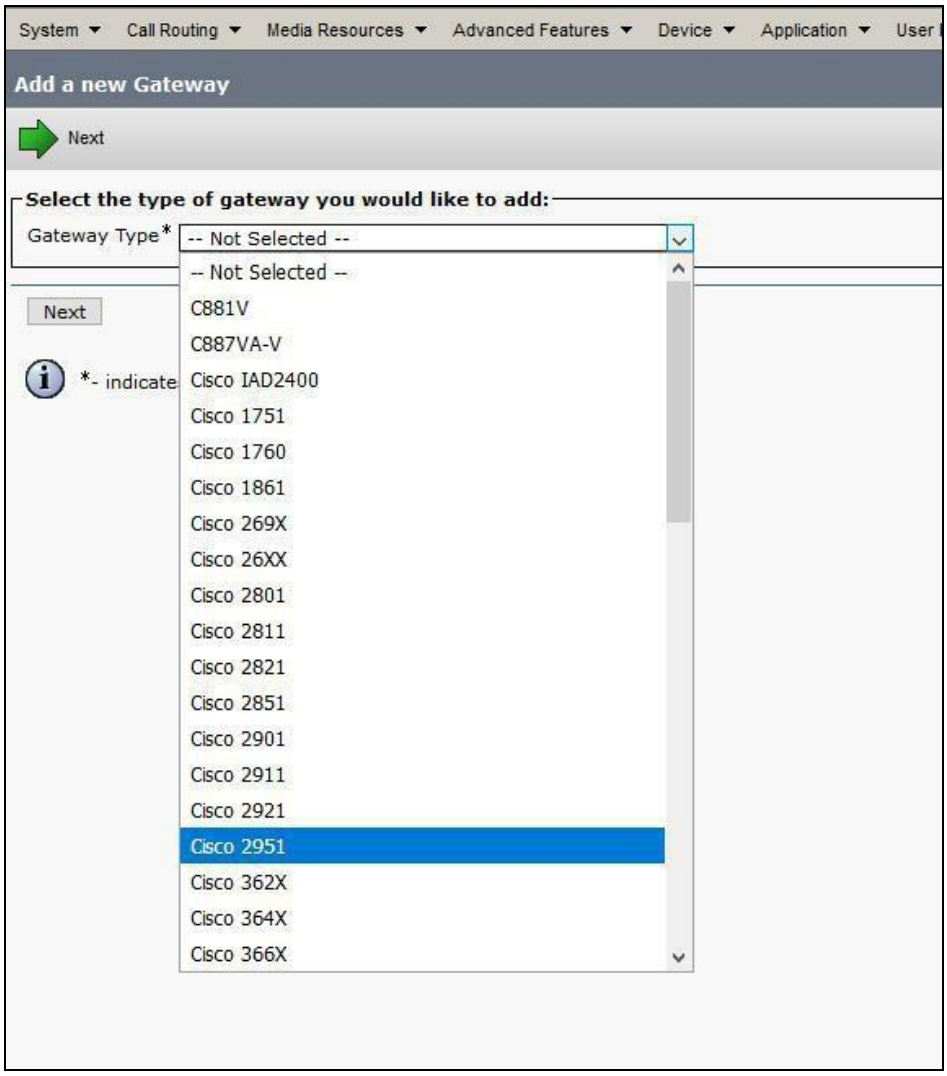


Figure 209: Add new MGCP Gateway

- If asked, select the protocol as MGCP, then, click "Next"
- In "Domain Name" field, type the correct FQDN of your router.
- Select the "Cisco Unified Communications Manager Group" of your Gateway (if you don't know, select the default);
- Click "Save" and then, "Reset".

To check the FQDN of your router, check the hostname of your router plus the ip domain name configured. Examples:

```
ROUTER01#sh run | in domain
no ip domain-lookup
ip domain-name cisco.lab
```

In this example, the FQDN of this router is "ROUTER01.cisco.lab".

```
ROUTER02#sh run | in domain
no ip domain-lookup
```

In this second example, the FQDN of this router is only "ROUTER02" (as the command ip domain-name is not present).

Configuring a MGCP Gateway on the router

The configuration on the router is straightforward. As soon as you have your MGCP Gateway created on CUCM, type these commands on your voice gateway (changing 1.2.3.4 to your CUCM IP Address):

```
ccm-manager config
ccm-manager config server 1.2.3.4
```

This configuration should be enough, as it will go to CUCM and download all necessary commands to complete your MGCP Gateway configuration.

Q.931 Backhaul

If you have an ISDN circuit and would like to implement an MGCP Gateway to control it, you will need to implement a feature called “Q.931 Backhaul”. This executes a TCP connection between the MGCP Gateway to forward all Q.931 signaling in the D channel of the ISDN interface to CUCM. Only the Q.931 (layer 3) will be sent to CUCM, and the gateway will still handle the Q.921 traffic (layer 2).

To configure this, manually insert the command “isdn bind-l3 ccm-manager” to the interface Serial created by the ISDN configuration.

```
interface Serial0/0/0:23
no ip address
encapsulation hdlc
isdn switch-type primary-ni
isdn incoming-voice voice
 isdn bind-l3 ccm-manager
 no cdp enable
```

If you are connecting the CUCM to a legacy PBX, the MGCP Gateway with ISDN and Q.931 Backhaul is by far the best option to do it. It will allow you

more interoperability functions, like passing calling number and name, call back, conference and others.

SCCP Gateways

The Skinny Client Control Protocol (SCCP) is a proprietary network terminal control protocol developed initially by Selsius Systems, before Cisco Systems acquired it in 1998. Like MGCP, it takes full control of the remote end ports. It is used in devices like:

- Cisco Phones Series (69xx, 79xx, IP Communicator and others)
- Cisco Unity voicemail server ports
- Voice Gateways like VG224, VG248, VG320, VG350, and others

Newer phone models such as the Cisco 88xx series no longer support the SCCP protocol, which shows that Cisco is slowly abandoning the SCCP and preferring the SIP Protocol instead.

SCCP can be used to control SCCP Gateways like VG248, which is a 48 ports Analog Gateway.



Figure 210: Cisco VG224

To create a SCCP Gateway, go do menu:

- Menu "Device > Gateway";
- Click "Add New";
- Select your Gateway model on the list, then, click "Next";
- Type the device MAC Address, then, click "Save";

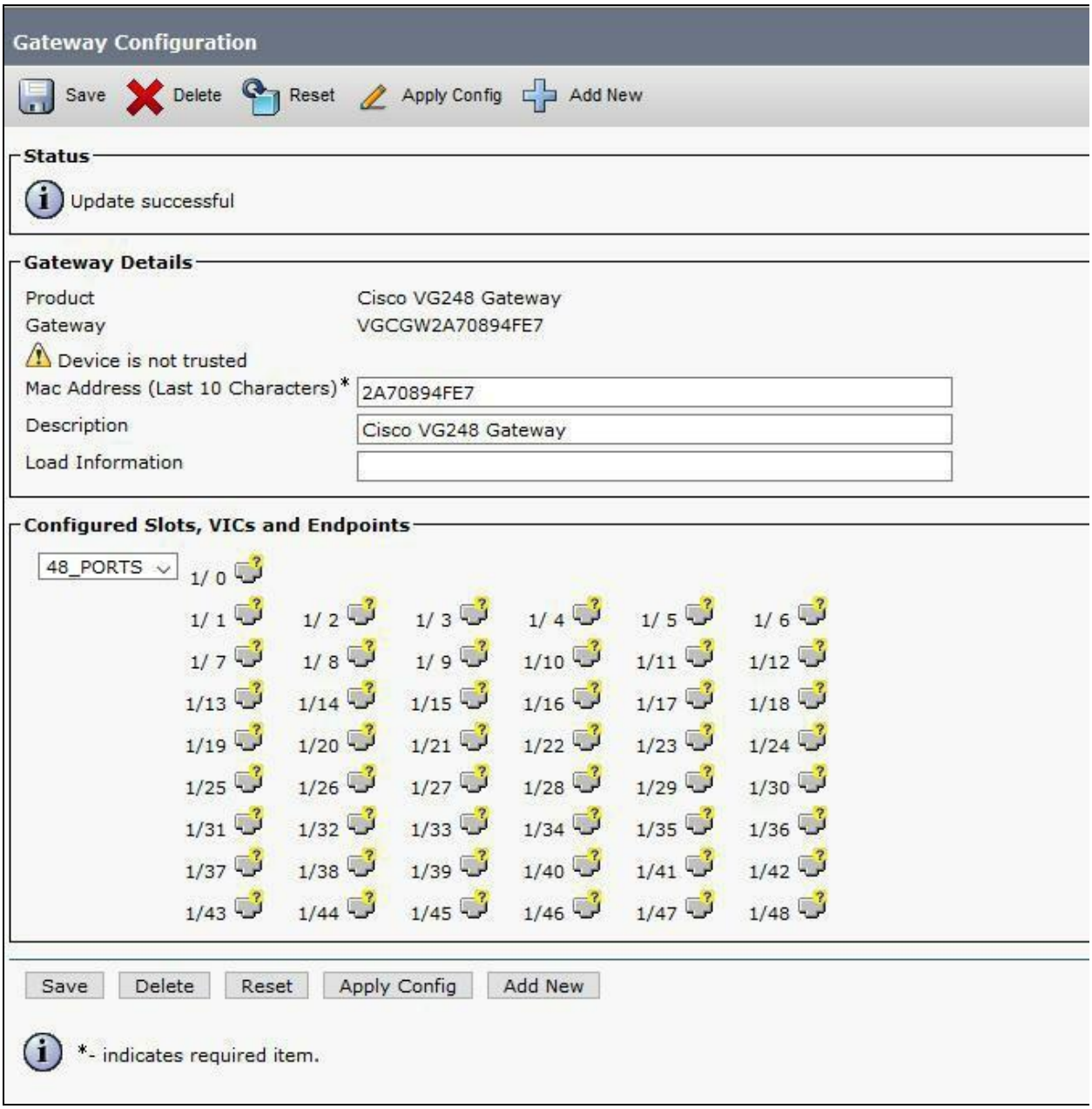


Figure 211: Cisco VG248 Gateway Configuration window

Now you can configure each port individually. These ports are connected to analog phones or faxes, not directly, but via a “Leaded Panel", which is a patch panel with RJ21 ports.



Figure 212: Lead Panel to VG Analog Gateways

Voice Cards and ATAs

Voice Cards like T1, E1, FXO, and FXS can be configured on various types of VoIP protocols, like H.323, MGCP, SCCP or SIP. Each of these cards has specific functions:

T1/E1 Card



Figure 213: Cisco VWIC2-2MFT-T1/E1 card

T1/E1 cards are an essential way to connect the VoIP environment to the PSTN world.

T1 and E1 are equivalent digital data transmission formats you can get from a Telephone company (Telco) to connect your company to the PSTN. It can also be used to connect CUCM to a legacy PBX.

T1 is a digital data transmission medium capable of handling 24 simultaneous connections (channels/timeslots) running at a combined 1.544 Mbps, while E1 is the European format for DS1 digital transmission. E1 links are similar to T1 links except that they carry signals at 2.048 Mbps, each signal has 32 channels/timeslots.

Depending on the country, you can find T1 or E1 circuits. United States, Canada, and Japan use T1, while Europe and Latin America use E1.

Cisco VWIC3-2MFT-T1/E1 or VWIC2-2MFT-T1/E1 cards can be used for this type of connection. It can be used in T1 circuits or E1 circuits, just needing to change the configuration.

A basic configuration to a T1 circuit includes:

```
card type t1 0 0
```

This command is used to configure the card inserted at slot 0, subslot 0 of the router motherboard as a T1 card; to configure the same card as E1, the command is "card type e1 0 0".

```
network-clock-participate wic 0
```

This command allows the port to use the network clock for timing.

```
controller T1 0/0/0
pri-group timeslots 1-3,24
```

This command configures the T1 controller as a PRI circuit (ISDN) with 23 channels for voice.

```
voice-port 0/0/0:23
```

Technet24

This voice-port is automatically created when you configure the controller port as an ISDN circuit. On this port, we can apply some configurations like country-specific call tones and translation-profiles.

FXO Card



Figure 214: Cisco VWIC2-4FXO card

The Cisco Foreign Exchange Office (FXO) interface is an RJ-11 connector that allows an analog connection to be directed at the public switched telephone network (PSTN). It does not provide dial-tone, so it should not be connected to an analog phone; instead it pretends to be an analog phone to receive this connection from Telco.

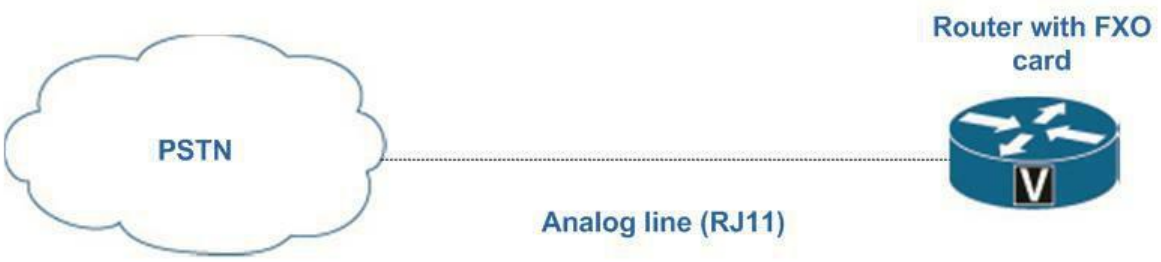


Figure 215: FXO Card topology

FXS Card



Figure 216: Cisco VWIC3-4FXS/DID card

A Foreign Exchange Station (FXS) interface connects directly to a standard telephone, fax machine, or similar device and supplies ring, voltage, and dial tone.



Figure 217: FXS Card topology

Cisco ATA



Figure 218: Cisco ATA 190 Analog Telephone Adaptor

Cisco ATA is like an FXS port, but instead of being connected to a router port, it is a standalone device. Usually, it provides 2 or more FXS ports to connect to analog devices.

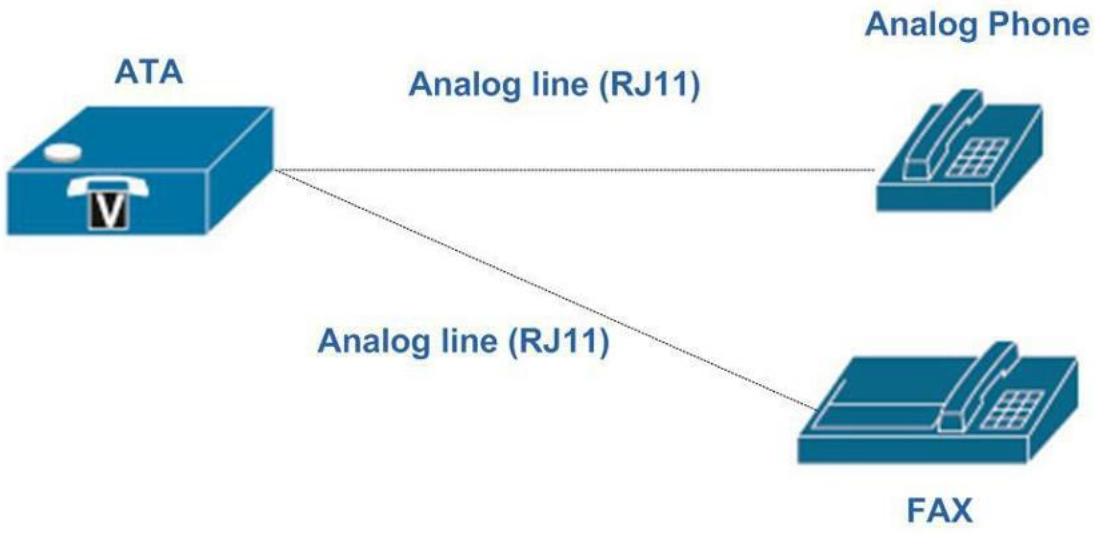


Figure 219: Cisco ATA topology

ISDN Circuit

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched

telephone network. It can be used with T1 or E1 circuits.

A basic ISDN configuration to an E1 circuit includes:

```
isdn switch-type primary-net5
```

This command sets the global ISDN switch type to “primary-net5”, commonly used in Europe and Latin America. To see all options available, type “isdn switch-type ?”.

```
controller E1 0/0/0
framing NO-CRC4
pri-group timeslots 1-31
```

These commands below configure the E1 card 0/0/0 as a primary E1 with all 30 slots available for voice. Also, the command “framing NO-CRC4” configures the framing mode, which can be “NO-CRC4” or “CRC4” (ask your telco PSTN provider for this information).

```
interface Serial0/0/0:15
no ip address
encapsulation hdlc
isdn switch-type primary-net5
isdn incoming-voice voice
no cdp enable
```

This serial interface 0/0/0:15 is automatically created when you configure your ISDN circuit on card 0/0/0. Obviously, this number can be different, depending on which slot your VWIC is inserted.

On this serial interface, we can configure some parameters like ISDN IE parameters, change the ISDN switch-type of the individual port, configure Q.931 Backhaul to MGCP Gateways, and others.

```
voice-port 0/0/0:15
```

As we saw earlier in this chapter, this voice-port is automatically created when you configure the controller port as an ISDN circuit. On this port, we can apply some configurations like country-specific call tones and translation-profiles.

R2 Digital Circuit

R2 Digital Circuits are used with E1 circuits and is widely used in Europe, Asia and Central/South America. The configuration to a basic E1 circuit usually includes:

```
card type e1 0 0
```

Sets the card type to E1.

```
controller E1 0/0/0
framing NO-CRC4
ds0-group 0 timeslots 1-10 type r2-digital r2-compelled ani
cas-custom 0
  country brazil
```

Configure the controller e1 0/0/0 to “framing NO-CRC4” (check with Telco it should be NO-CRC4 or CRC4); create a DS0-Group 0 with 10 channels/timeslots (check with your Telco how many channels you have available to use), and select the type as R2-Digital.

Also, inside, you can select the specific configurations available under cas-custom country command. In this example, we are setting it to use default parameters for Brazil. You can type “country?” to check all countries configurations available.

```
voice-port 0/0/0:0
cptone BR
```

This voice-port 0/0/0 was automatically created when we inserted the command “ds0-group 0 timeslots 1-10 type r2-digital r2-compelled ani”. Inside this port, you can for example configure the CP Tone to your country. The example below is setting the tones for Brazil, and you can type “cptone?” to check all countries configurations available.

CHAPTER 8 - TRUNKS

Forget legacy telephony, let's connect VoIP with VoIP directly

Trunks are used to connect distinct VoIP domains in large VoIP environments. In CUCM, we have 3 types of trunks available:

- SIP Trunks
- H.225 Trunks
- Intercluster Trunks

The main question here is which trunk to use in each situation. However, if you want a good tip, here it is: always when possible, go with SIP Trunks!

SIP Trunks

SIP Trunk is the most critical Trunk Type to be configured on CUCM because SIP is "de facto" the standard protocol to allow interoperability between different VoIP vendors:

- Trunks to PSTN SIP Providers;
- Trunks to GSM Gateways;
- Trunks to vendors like Microsoft, Avaya, Alcatel, Asterisk, AudioCodes, etc.

Even Cisco is migrating all its VoIP network to SIP Protocol:

- Communication between CUCM and other Cisco Server (Voicemail, Presence, etc.);
- Newer Cisco Phones;
- Cisco Jabber;
- Video Conferences;
- All other Cisco Voice and Video Devices.

Everything now is becoming SIP. SIP is the way to go.

Components of a SIP Trunk

To create a SIP Trunk in CUCM, we need to have the following components:

- SIP Trunk Security Profile
- SIP Profile
- SIP Trunk

CUCM comes with pre-defined default values to "SIP Trunk Security Profile" and to "SIP Profile", and we can use these default values. However, it is essential to understand what they do, so we can edit these values if necessary.

SIP Trunk Security Profile

SIP Trunk Security Profiles are located under menu “System > Security > SIP Trunk Security Profile”.

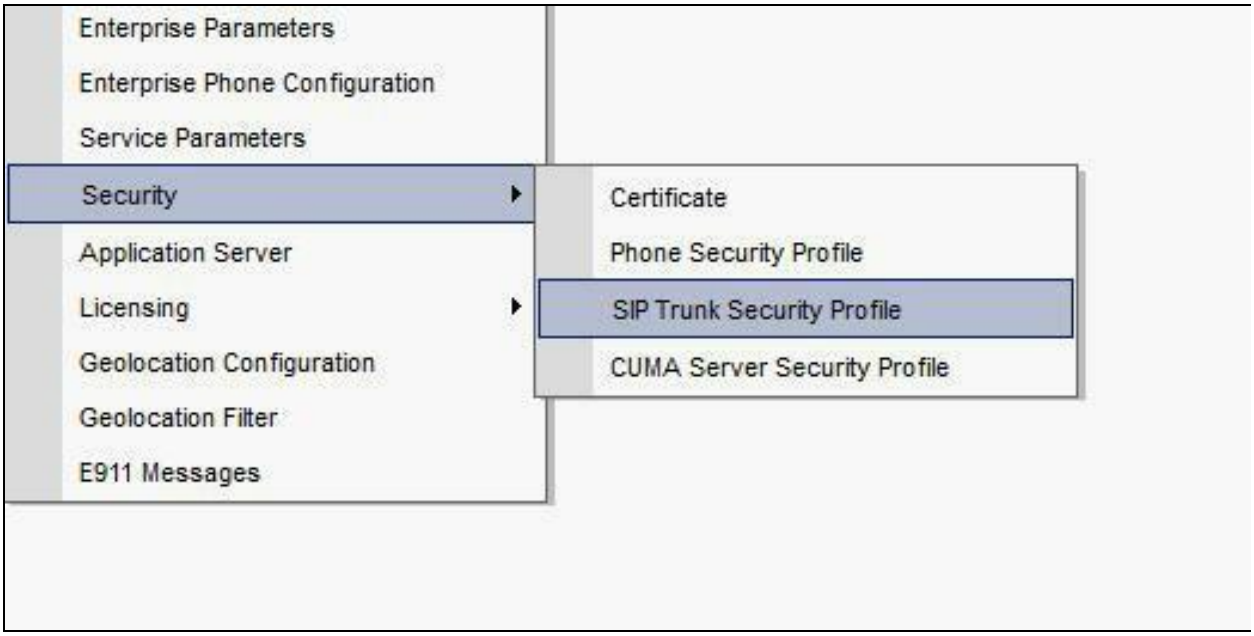


Figure 220: SIP Trunk Security Profile menu

We can use the default profile “Non Secure SIP Trunk Profile” to almost all our SIP Trunks. Alternatively, we can copy this default to a new profile and work on this copy; example: we can copy this Profile and rename it to “Cisco Unity SIP Trunk Profile” and use this only to Cisco Unity Connection Voicemail. The main reason to do it is to be able to edit the parameters only to a specific SIP Trunk and not change other trunks.

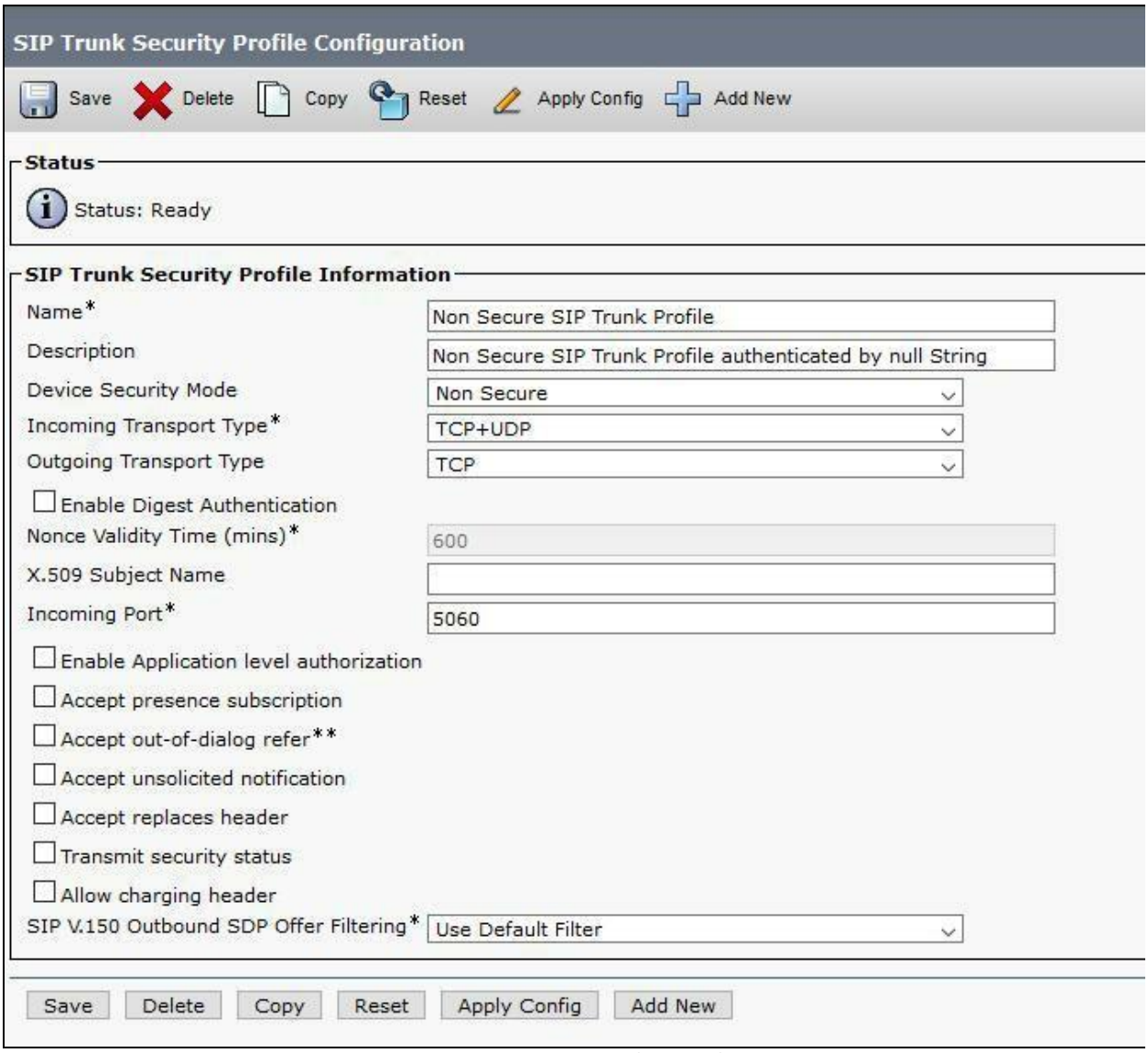


Figure 221: SIP Trunk Security Profile configuration window

As you can see, there are many options to configure in a SIP Security Trunk Profile, and some examples are:

Incoming Transport Type: If the incoming calls can use TCP+UDP or only TLS (for SIP Trunks with TLS encryption enabled);

Outgoing Transport Type: If the outgoing calls must use TCP, UDP or TLS.

Incoming Port: on which TCP/UDP port CUCM is waiting to receive calls. The default is 5060.

Tip: If you are planning a SIP Trunk to an Asterisk PBX, you will

probably need to create a SIP Trunk Security Profile with the Outgoing Transport Type set as UDP, as this is the default in most Asterisk systems.

SIP Profile

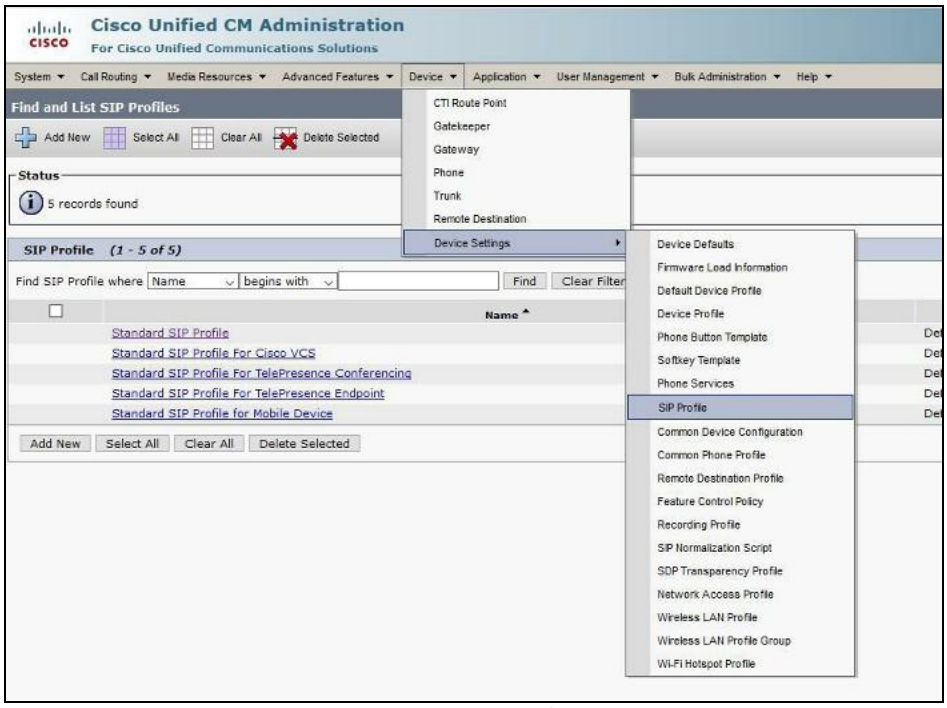


Figure 222: SIP Profile menu

SIP Profiles are located under the menu “Device > Device Settings > SIP Profile. Again, we can use the default “Standard SIP Profile” or we can copy it and work with this copy.

Under SIP profile, there are a lot of options available, and some of the most important are:

Option	Description
Retry INVITE	Specifies the maximum number of times that an INVITE request gets retransmitted.
Media Port Ranges	Specifies if CUCM should use the same UDP Port Range for Audio and Video or not.
Start Media Port	Specifies the initial UDP Port for RTP.
Stop Media Port	Specifies the final UDP Port for RTP.

DSCP for Audio Calls	QoS Marking for Audio Calls.
DSCP for Video Calls	QoS Marking for Video Calls.
Enable VAD	If VAD should be enabled or not.
SIP OPTIONS Ping	If the SIP OPTIONS Ping should be enable to monitor the status of a Trunk.
Allow Presentation Sharing using BFCP	BFCP is a protocol used for example to allow computer presentation sharing when placing a Jabber Video Call.

Table 27: SIP Profile options

If you don't have any specific needs, you can use the default "Standard SIP Profile" with no problem.

SIP Trunk

Finally, let's see how to create a new SIP Trunk. Go to menu "Device > Trunk > Add New".

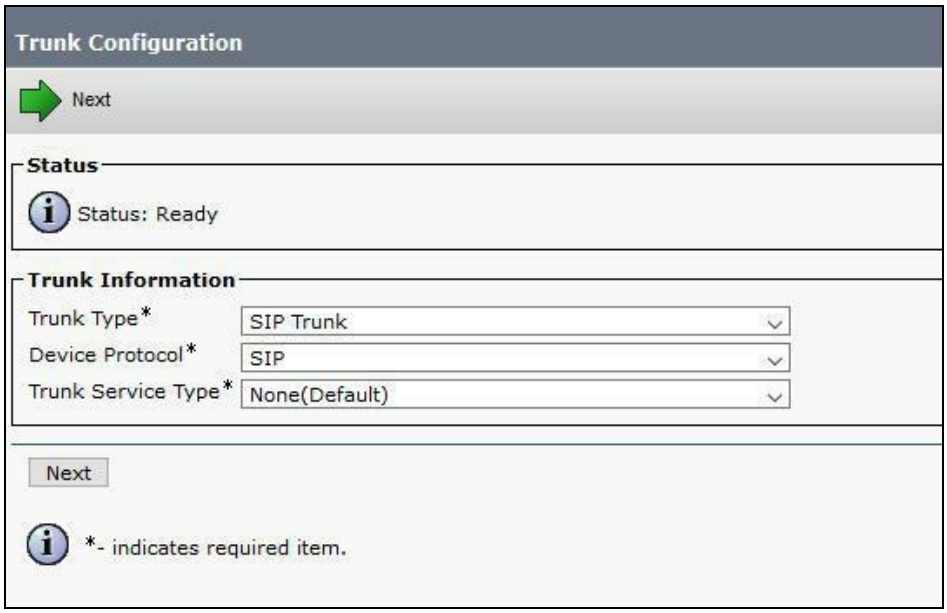


Figure 223: SIP Trunk configuration wizard

Select the trunk type "SIP Trunk", the Device Protocol "SIP" and Trunk Service Type "None(Default)" and click "Next".

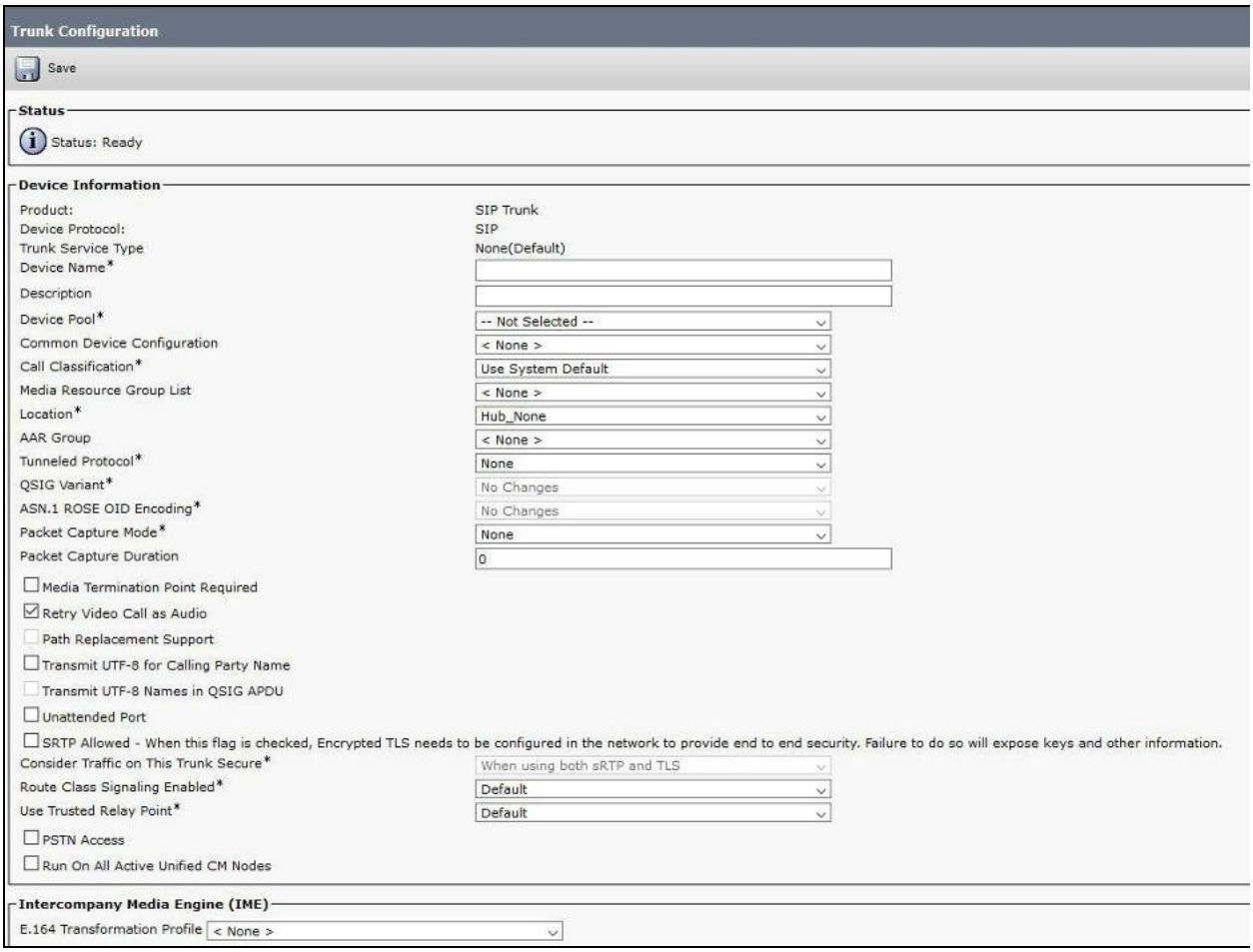


Figure 224: SIP Trunk configuration window

In the Trunk Configuration page, the main options to edit are:

Configuration	Description
Device Name	The SIP Trunk name.
Description	A short description of this trunk.
Device Pool	The Device Pool where this trunk should register. If you are not sure, select “Default”.
Run On All Active Unified CM Nodes	Enable it if you want this SIP Trunk active on all your CUCM Nodes (recommended).
Inbound Calls / Significant Digits	Provides a basic digit manipulation method. Check Chapter 10, “Digit Manipulation” for more details.
Inbound Calls / Calling Search Space	Which CSS should be used to search for incoming calls from this trunk.
	Also provides a basic digit manipulation method.

Prefix DN	Check Chapter 10, “Digit Manipulation” for more details.
SIP Information / Destination Address	The IP Address of the Remote Destination of this Trunk.
SIP Trunk Security Profile	This is where we apply the SIP Trunk Security Profile.
SIP Profile	This is where we apply the SIP Profile.

Table 28: SIP Trunk options

These are the necessary steps to create a SIP Trunk on CUCM. Please note that this is a profound topic, with many books dedicated only to SIP Trunking. So if you need more information, I put some links of sites and books in the References Section.

H.225 Trunks

H.225 Trunks are used in H.323 network that uses gatekeepers. The H.225 Trunk connects to a gatekeeper, and this gatekeeper allows and controls the access to other Cisco CallManager clusters and H.323 devices.

Please note that you do not need to create an H.225 Trunk to connect to an H.323 Gateway, as H.323 Gateways are created directly on CUCM as we saw in Chapter 7, "Voice Gateways".

H.225 Trunks are only necessary if you have H.323 Gatekeepers on your VoIP Network, which is very rare nowadays.

If you need to create an H.225 Trunk, go to menu “Device > Trunks > Add New > H.225 Trunk (Gatekeeper Controlled) > Next”. The information necessary here is very similar to the necessary to create an H.323 Gateway, except by the fact that you need to create a Gatekeeper first (Menu “Device > Gatekeeper > Add New”).

Intercluster Trunk

Intercluster Trunks are divided into 2 types: Gatekeeper controlled, and Non-gatekeeper controlled. The main difference is:

- If your network has a Gatekeeper, you need to create one Intercluster Trunk to your Gatekeeper, and it will allow your

system to place calls to all remote Clusters connected to this Gatekeeper.

- If your network does not have a Gatekeeper, you need to create one Intercluster Trunk to each remote Cluster you need to connect.

> **Note:** the configuration of a Gatekeeper is out of the scope of this book.

For example, you can create an Intercluster Trunk between 2 CUCM Clusters and route calls using this trunk to reach one another. However, if you don't have any reason for using Intercluster Trunks, I recommend instead to use SIP Trunks for this.

CHAPTER 9 - CALL ROUTING

How to forward calls on CUCM and Cisco Voice Routers

Designing and implementing a good dial plan has always been one of the most difficult and important aspects of the voice system. The Call Routing process is done on CUCM, with Route Patterns, and also on the Voice Gateways with dial-peers, if they are using H.323 or SIP.

Call Routing on CUCM

The call routing on CUCM is done via “Route Patterns”. However, to have the complete call, routing scheme on CUCM includes four configurations:

- Route Patterns
- Route List
- Route Groups
- Gateways/Trunks

You need to:

- Create a Gateway or Trunk;
- Create a Route Group and include a Gateway or a Trunk;
- Create a Route List and include one or more Route Lists;
- Create a Route Pattern and associate it with the Route List.

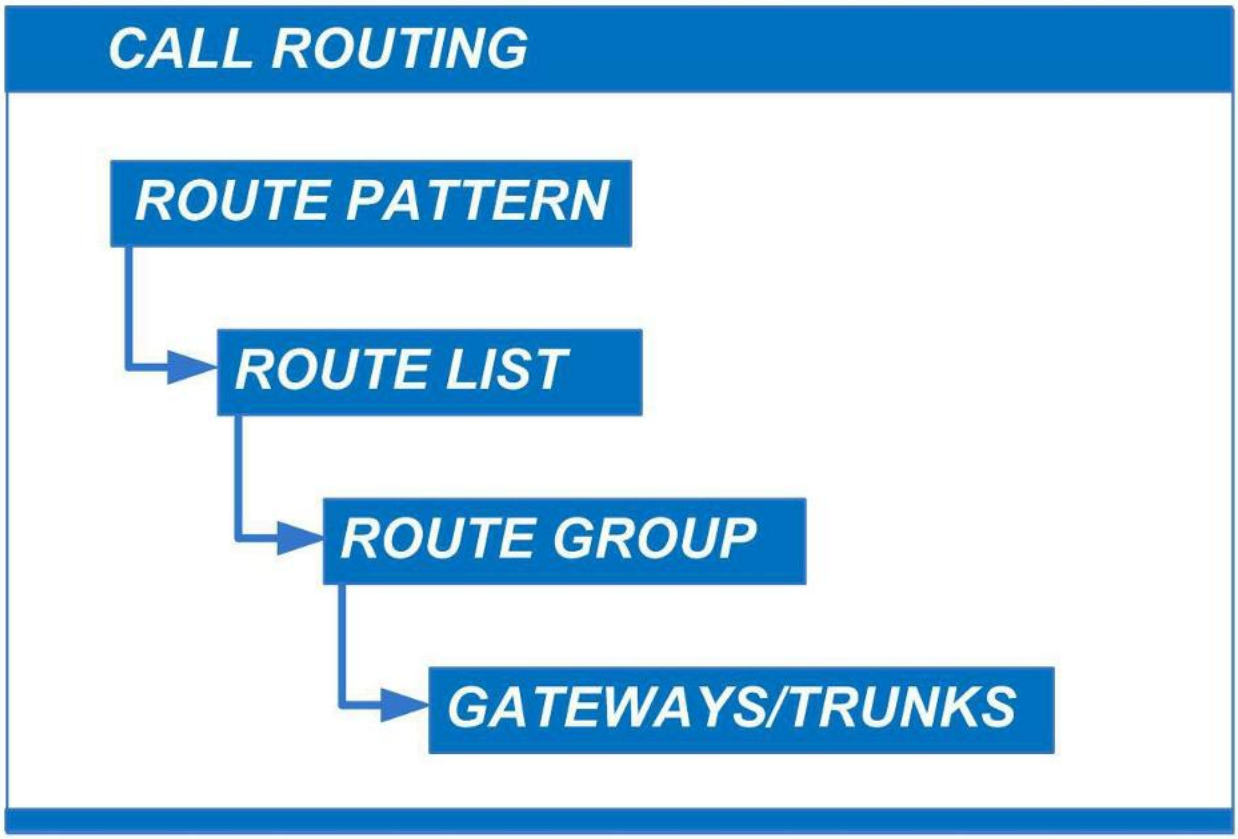


Figure 225: Call Routing scheme

With this configuration, you can have a fully redundant routing scheme. When a call is placed, the steps are as follows:

- When a Route Pattern is matched, it sends the call to the created Route List;
- The Route List sends the calls to the created Route Group;
- The Route Group sends the calls to the created Gateway or Trunk;
- The Gateway/Trunk completes the call.

You can route your calls on CUCM using another configuration by pointing the Route Pattern directly to the Gateway/Trunk. This configuration works very good as well. However, it is not recommended, because:

- You will lose the ability to have redundancy
- CUCM will duplicate the Gateway/Trunk in the configuration window for each Route Pattern you have created and pointed to a Gateway/Trunk

Thus, it is highly recommended to create the Route List/Route Group configuration even if you do not plan to implement redundancy to a Route Pattern.

Let's check how to create it.

Step 1:Create a Gateway or SIP Trunk;

You need to have a Gateway (H.323, MGCP or SCCP) or SIP Trunk available on CUCM. If you have not created it yet, this topic is covered in details in Chapter 7 (H.323, MGCP or SCCP) or Chapter 8 (SIP Trunk).

Step 2:Create a Route Group;

To create your Route Group, go to menu "Call Routing > Route/Hunt > Route Group > Add New":

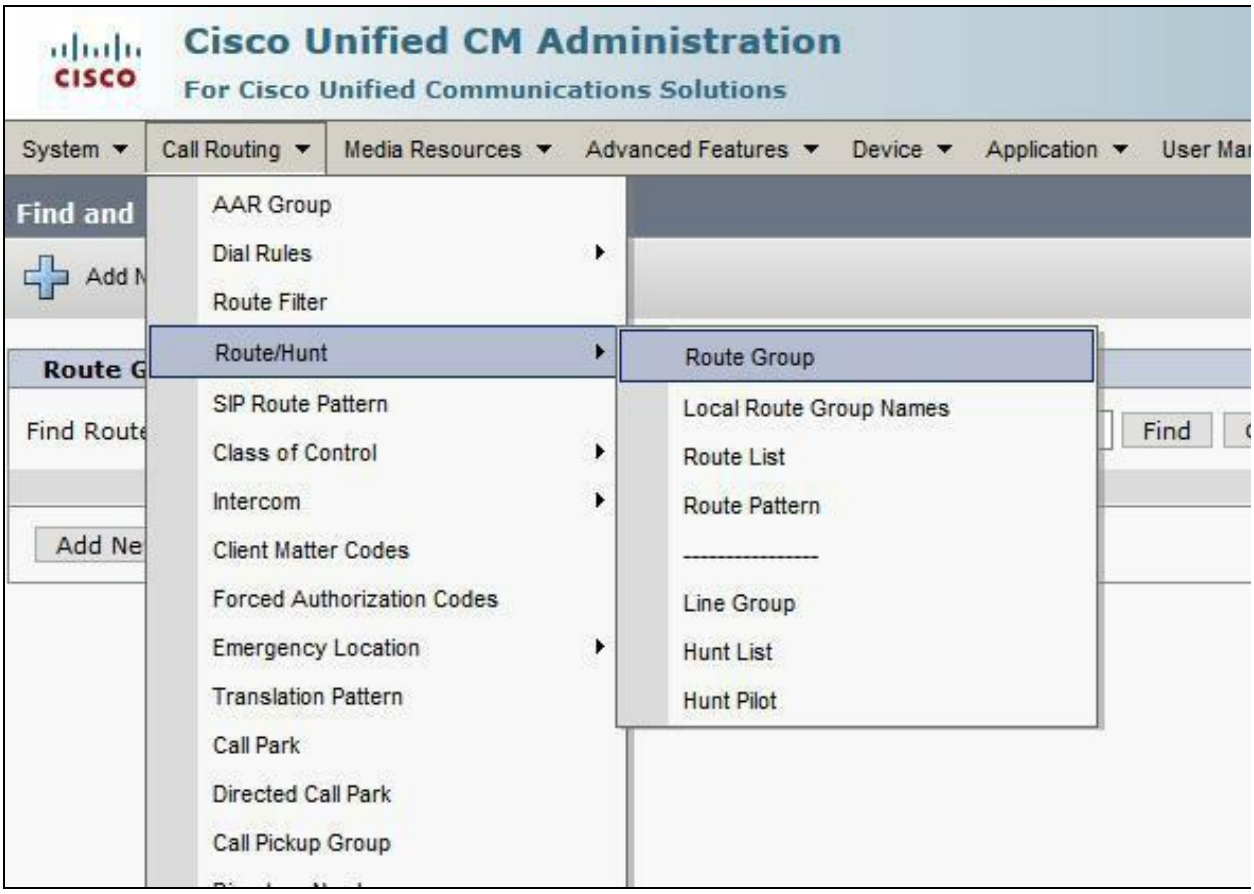


Figure 226: Route Group menu

Note: In the same menu, you can see the “Route List” and “Route Pattern” options.

Type the Route Group Name and select the Distribution Algorithm:

- Top-down: CUCM sends the calls to the first member of a Route Group until it is unable to accept any more calls, then it will start sending them to the second member;
- Circular: CUCM sends the calls using round-robin load balancing).

The Distribution Algorithm will only take effect if you add more than one device to this Route Group.
Select the device on the available devices box, click “Add to Route Group” and then “Save”.

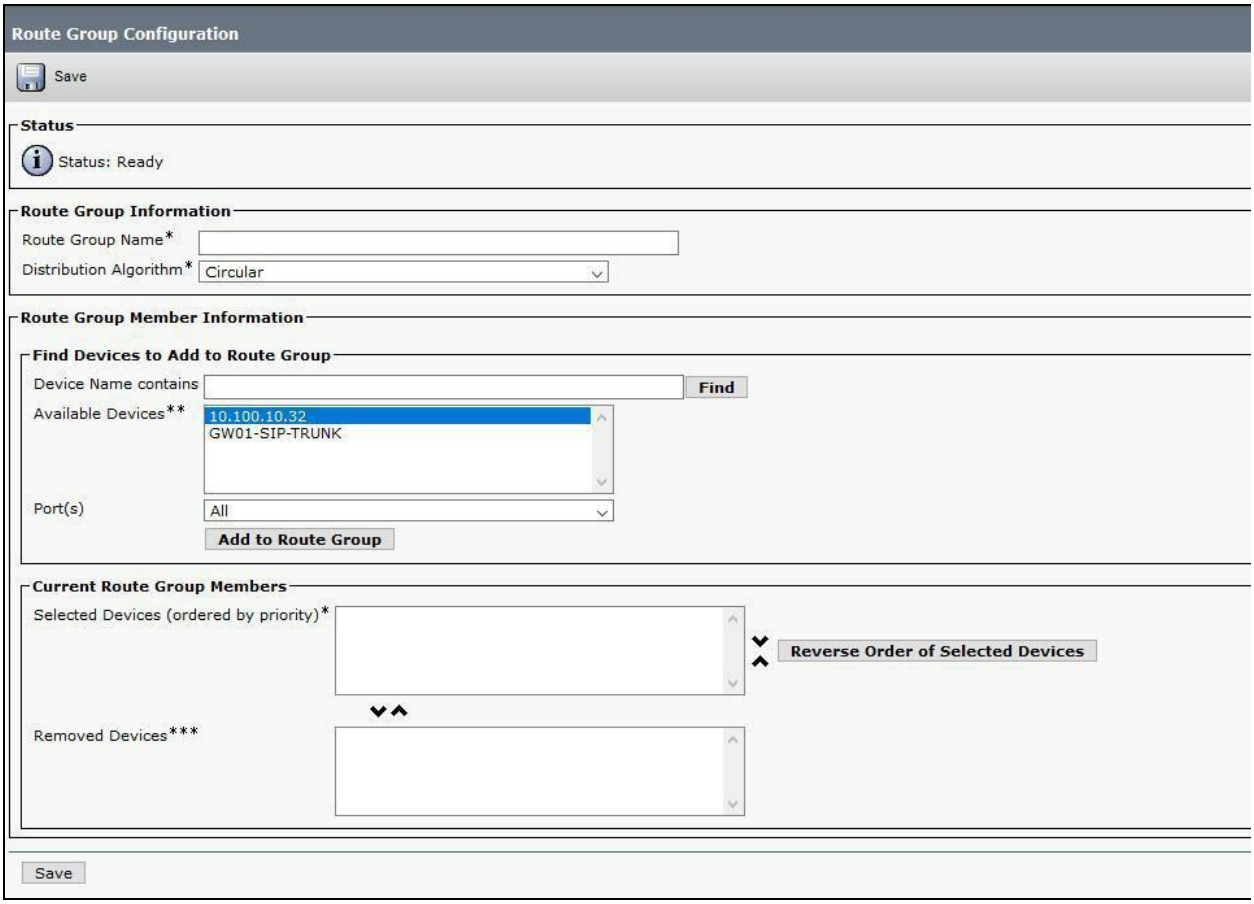


Figure 227: Route Group Configuration

Step 3:Create a Route List;

After you configured the Route Group, let's create the Route List. In order to do so, go to menu "Call Routing > Route/Hunt > Route List > Add New":

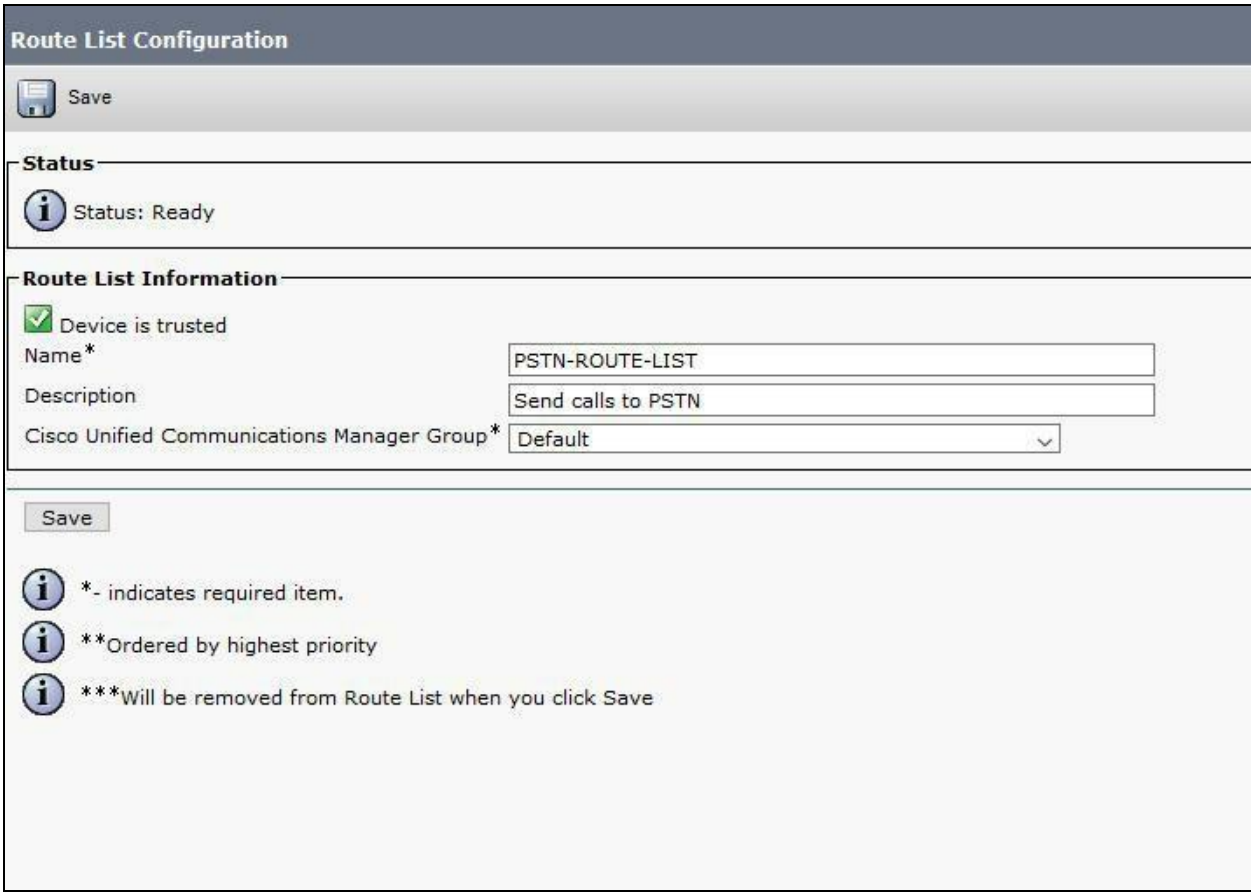


Figure 228: Route List Configuration

Create a name (mandatory) and a description (optional). Select the Cisco Unified Communications Manager Group it will be associated with (mandatory) and click "Save". The configuration page will change and a new box will open where you can add the Route Group(s) associated with this Route List.

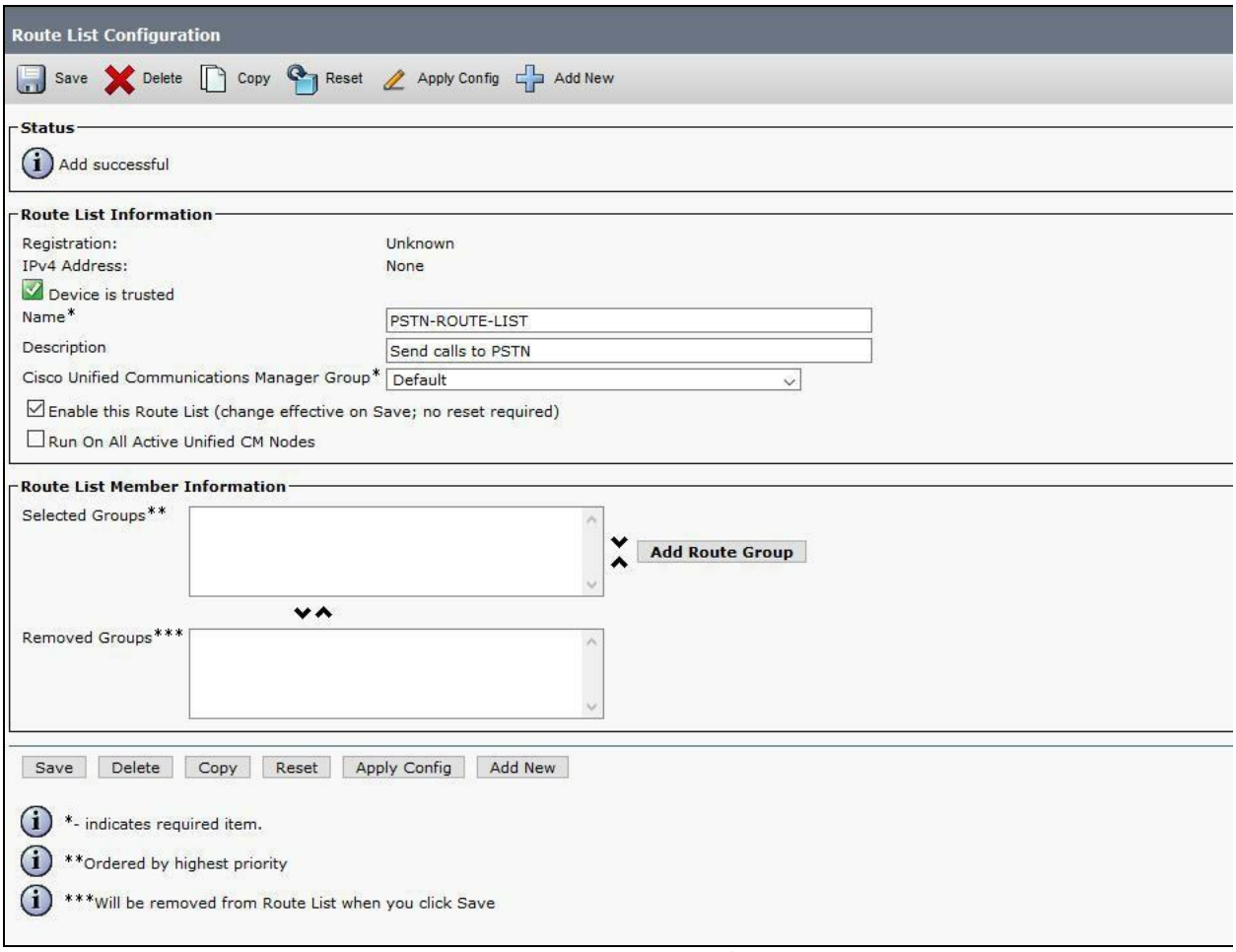


Figure 229: Route List Configuration

Click “Add Route Group”, select the Route Group you want to associate it with and click “Save”. It’s not necessary to enable the option “Run On All Active Unified CM Nodes”, however, it is strongly recommended. Save it and click “Reset”.

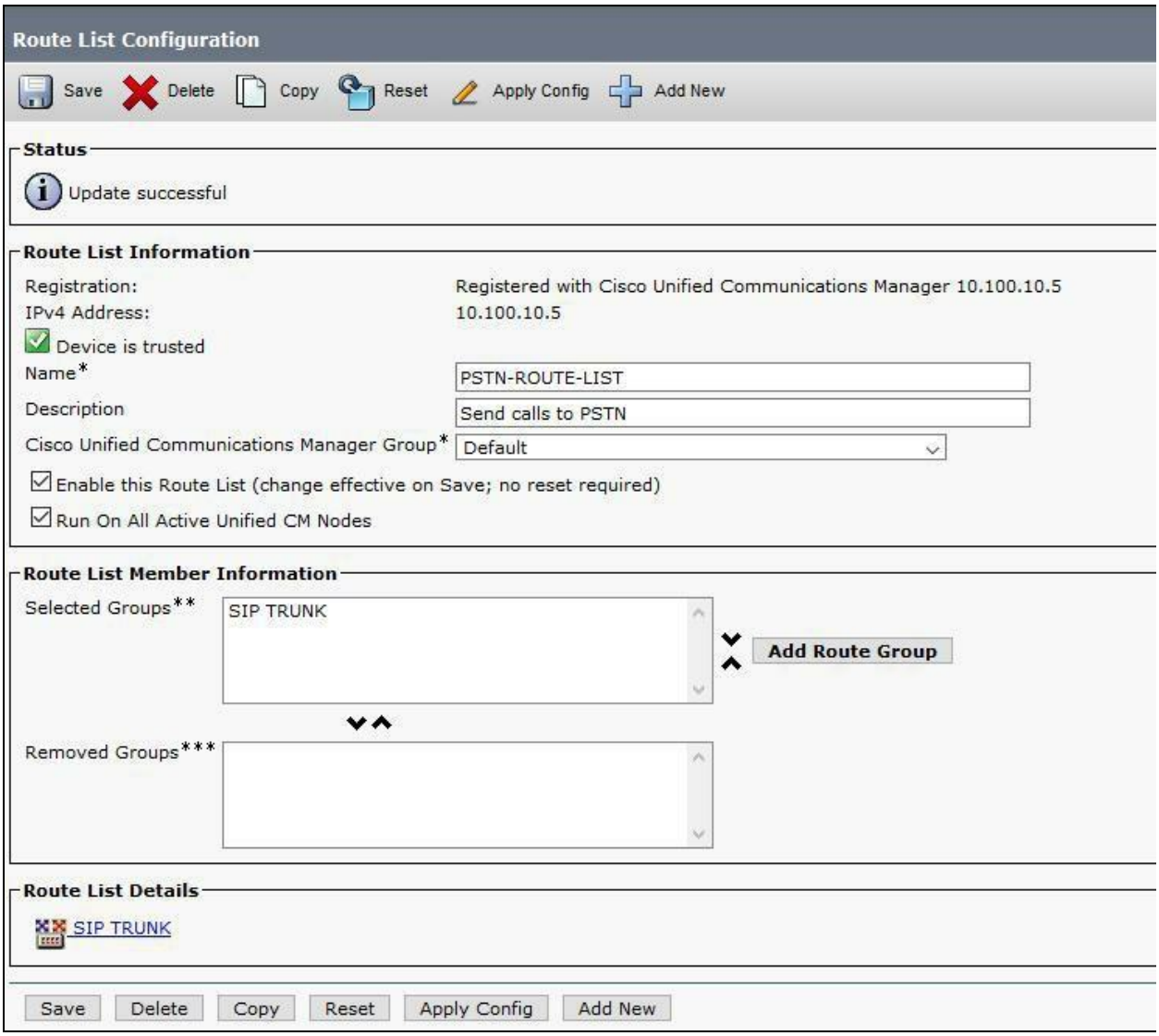


Figure 230: Route List Configuration

Step 4:Create a Route Pattern;

To create your Route Pattern, go to menu “Call Routing > Route/Hunt > Route Pattern > Add New”. As an example, follow the basic Route Pattern to send calls starting with digit “9” to our Route List “PSTN-ROUTE-LIST”:

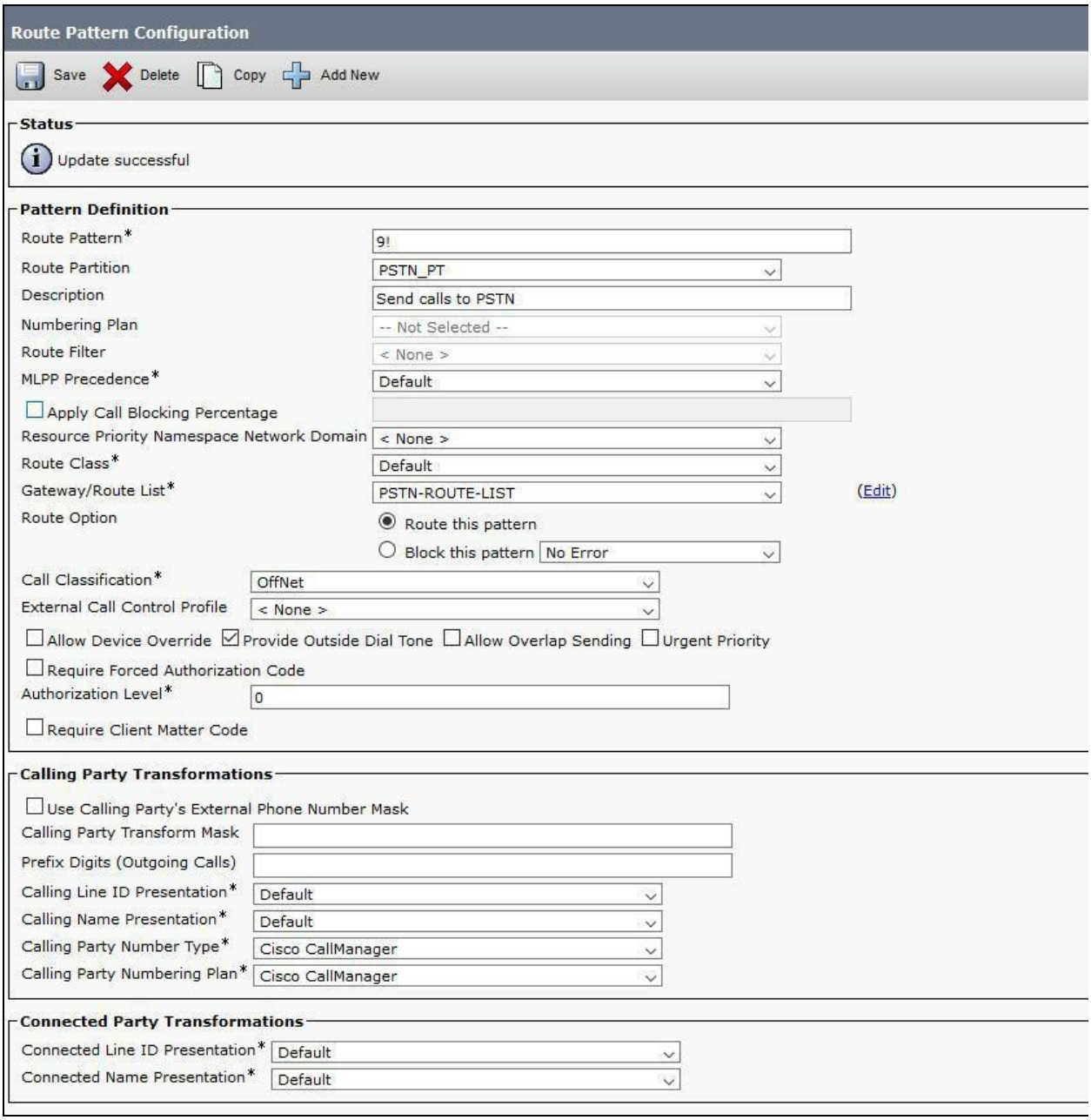


Figure 231: Route Pattern Configuration

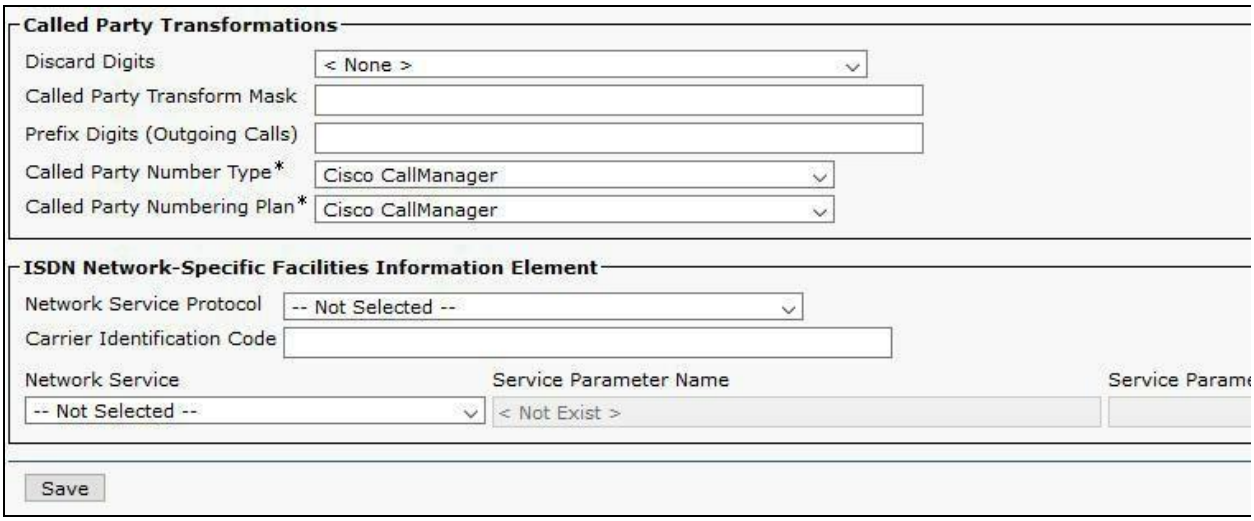


Figure 232: Route Pattern Configuration

Field	Description	Configuration example
Route Pattern	The pattern you want to forward.	9! (digit “9” + any digits dialed after it)
Route Partition	The Partition to which the Route Pattern should belong.	PSTN_PT
Description	A description of what this Route Pattern is used for.	“Send calls to PSTN”
Gateway/Route List	A place where this Route Pattern will send the call.	“PSTN-ROUTE-LIST”
Provide Outside Dial Tone	Showed if the user hears a secondary dial-tone when dialing the Route Pattern.	Checked
Urgent Priority	Showed if the Route Pattern should be routed as soon as the result is matched. It can be used only with the Route Pattern which does not overlap with others.	Unchecked

Table 29: Route Pattern options

These are the most common configurations that need to be filled. There are other important ones, like “Discard Digits” and “Prefix Digits (Outgoing Calls)”, but those will be explained later in details in Chapter 10, “Digit Manipulation”.

Save the Route Pattern. At this moment, the Route Pattern is active and ready to forward the call to our SIP Trunk. Let's check how to implement redundancy to our Route Patterns.

Call Routing Redundancy on CUCM

If you have more than one network device that routes your call to the same destination, you can implement a call redundancy. It can be done in two ways:

- Add a secondary Gateway/Trunk to the existing Route Group;
- Add a secondary Route Group to the existing Route List.

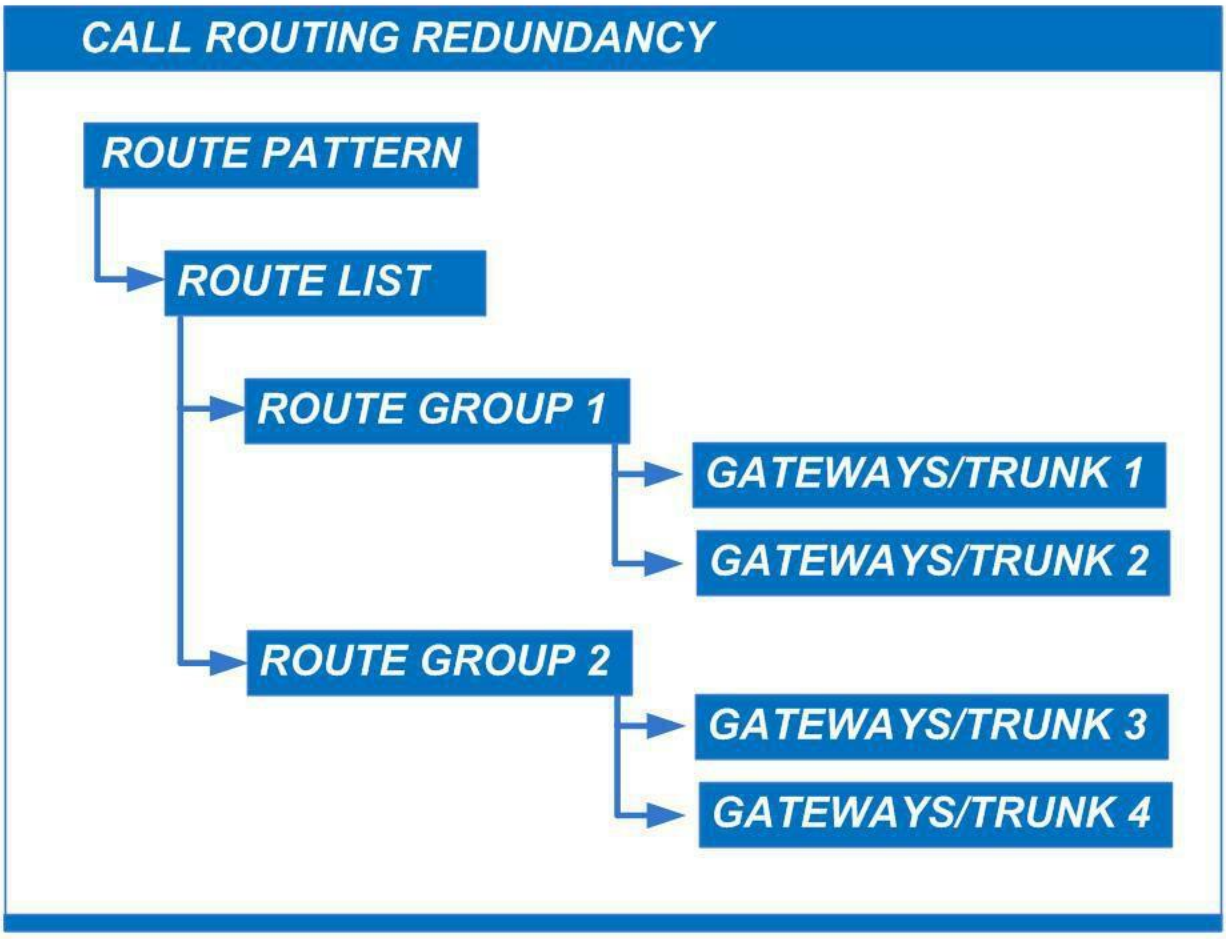


Figure 233: Call Routing Redundancy

Both configurations are very simple and work almost in the same way. If you have an MGCP Gateway and H.323 or SIP, CUCM will only allow you to use the second method which is adding a new Route Group to the existing

Route List. However, apart from this, there is nothing special about this configuration.

Call Routing on Cisco Gateways

Dial-peers on Cisco Gateways is an equivalent of the Route Patterns on CUCM. They are similar to static IP routes, and you need to create one for each destination you want to reach. The main difference is that you also need to create an Inbound Dial-peer to receive the calls; if you do not create it, the Router will use a default "Dial-peer 0" with its default settings, and you will not be able to edit them. Thus, it is recommended to create an inbound dial-peer to receive the calls and be able to change their parameters if needed.

Calls from CUCM to the PSTN

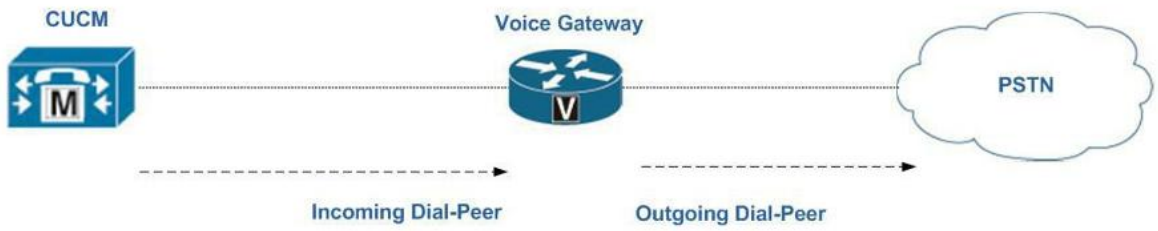


Figure 234: Calls from CUCM to the PSTN

In the example above, the call came from CUCM to the Voice Gateway, and it has an incoming dial-peer to receive the call. The Voice Gateway has another dial-peer to send the call to the PSTN.

Calls from PSTN to the CUCM

On the other hand, calls that come from PSTN to the CUCM extensions need an incoming dial-peer to be received by the PSTN and an outgoing dial-peer which will send them to the CUCM:

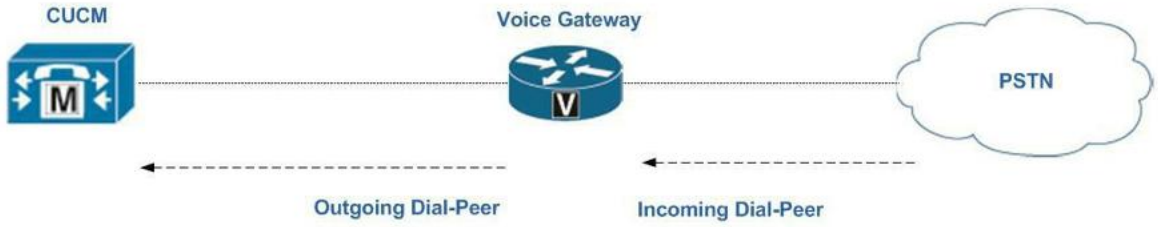


Figure 235: Calls from PSTN to the CUCM

Dial-Peer Configuration

With that in mind, our basic dial-peer topology will look like this:

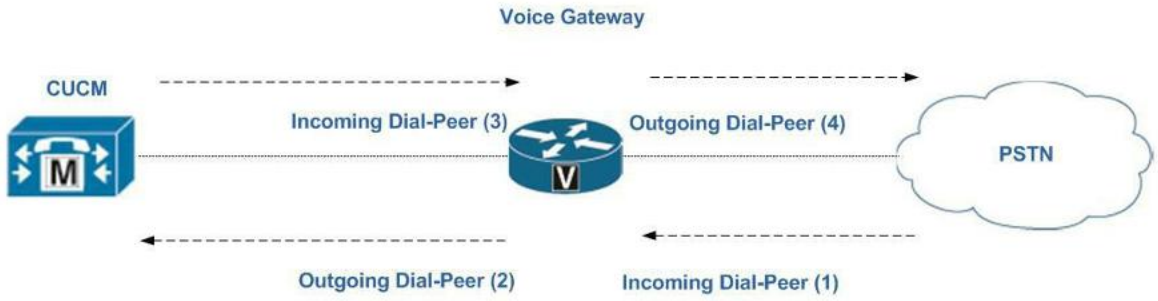


Figure 236: Calls from PSTN to the CUCM

The dial-peers that will be created are identified with the numbers from 1 to 4. Let's see how to create them:

Step 1:Incoming Dial-Peer from PSTN to the Voice Gateway:

```
dial-peer voice 1 voip
tone ringback alert-no-PI
description INCOMING FROM SIP PROVIDER
rtp payload-type nte 102
session protocol sipv2
incoming called-number 5…$
voice-class sip early-offer forced
dtmf-relay rtp-nte
codec g711alaw
no vad
```

The dial-peer 300 will receive our call from the PSTN provider. In this example, our PSTN provider uses SIP Trunk to deliver our calls, and this is why a VoIP dial-peer is used, instead of a POTS dial-peer (used for T1/E1/FXO ports).

The most important command in this dial-peer is: “incoming called-number 5…”. It is where you specify what will be used to identify the incoming calls which should be received by this dial-peer which, in this case, are calls coming with 4 digits starting with the number “5”. The “$” symbol means that it will be matched if the call has 4 digits only. For example, calls to number 54321 will not match this dial-peer, as they have five digits.

In this dial-peer, you also use SIP (session protocol sipv2), select the G.711 codec (codec g711alaw), select the DTMF-Relay to RTP-NTE (dtmf-relay rtp-nte), disable VAD (no vad) and force the use of the SIP mode “early-offer” (voice-class sip early-offer forced).

The other three dial-peers will be very similar to this one, with only minor changes.

Step 2:Outgoing Dial-Peer from Voice Gateway to CUCM

```
dial-peer voice 2 voip
tone ringback alert-no-PI
description OUTGOING TO CUCM PUBLISHER
rtp payload-type nte 102
session target ipv4:10.100.10.10
session protocol sipv2
destination-pattern 5…$
voice-class sip early-offer forced
dtmf-relay rtp-nte
codec g711alaw
no vad
```

Now, we are configuring the dial-peer to send the call received on dial-peer 1 to CUCM Publisher. The configuration is almost the same with the main differences being:

- The session target IP Address is different (CUCM Publisher IP Address);
- The command “destination-pattern 5…$” is used to identify

where this router should send the call, instead of the command "incoming called-number 5…$", which is used in dial-peer 1 to identify the incoming calls to this router.

Step 3:Incoming Dial-Peer from CUCM to the Voice Gateway:

```
dial-peer voice 3 voip
tone ringback alert-no-PI
description INCOMING FROM CUCM
rtp payload-type nte 102
session protocol sipv2
incoming called-number .T
voice-class sip early-offer forced
dtmf-relay rtp-nte
codec g711alaw
no vad
```

Here, as we are again configuring an inbound dial-peer, we need to configure the command "incoming called-number" again, but now pointing to destination ".T", which means "all calls". With that, we can match both, the calls that our routers receive from CUCM, but also from all other sources.

Note: Please be aware that it is highly recommended to configure the "Toll-Fraud Prevention Feature" feature when configuring this kind of SIP Trunking to the PSTN. Refer to Chapter 7 on how to configure it.

Step 4:Outgoing Dial-Peer from Voice Gateway to PSTN

Now, the last dial-peer, sending our calls to the PSTN:

```
dial-peer voice 4 voip
tone ringback alert-no-PI
description OUTGOING TO PSTN
rtp payload-type nte 102
session target ipv4:152.6.8.40
session protocol sipv2
destination-pattern 9T
```

```
voice-class sip early-offer forced
dtmf-relay rtp-nte
codec g711alaw
no vad
```

The main changes in this dial-peer are:

- session target ipv4:152.6.8.40 - this session target is the Public IP Address of our SIP PSTN Provider (ask your PSTN SIP Trunk Provider which IP Address to use).
- destination-pattern 9T - this dial-peer match all routes that start with the digit 9 and have any number of digits after that.

In this part, it is better to configure multiple dial-peers to each PSTN destination such as local calls, mobile phones, long distance calls, international calls, Toll-Free services, etc. It provides better control and helps the calls to be sent faster to the destination.

Note: I used dial-peer number 1, 2, 3 and 4 to easier to identify each one on the topology. Depending on your Cisco IOS version, it will not allow you to use these numbers. If so, create them with higher numbers, as required by your IOS.

Call Routing Redundancy on Cisco Gateways

To implement a redundancy on Cisco Gateways, we need to configure it globally on the router and also on the dial-peer level.

Redundancy to SIP dial-peers

To configure redundancy to SIP dial-peers, we need to:

Step 1:Configure the SIP User-Agent timers:

```
sip-ua
```

```
retry invite 3
timers trying 200
```

In the example above, the router will send the SIP INVITE message 3 times and wait 200 milliseconds between each message. After that, the router will consider a dial-peer to be out of reach and will try the next one, if available.

Step 2:Configure a secondary dial-peer to the same destination:

Duplicate the dial-peer for which you want to enable the redundancy and change the following commands:

- Dial-peer tag - it cannot use the same number, so use the next number available;
- Description - create a different description for this redundancy; it is optional, however, highly recommended;
- Session target - configure the secondary destination for the call;
- Preference - this is where we enable the redundancy. We have not inserted this command to our first dial-peer, but it uses the "preference 0" as default. What we do now is to create this dial-peer with "preference 1", which has less preference than "preference 0".

```
dial-peer voice 5 voip
tone ringback alert-no-PI
description OUTGOING TO CUCM SUBSCRIBER
preference 1
rtp payload-type nte 102
session target ipv4:10.100.10.11
session protocol sipv2
destination-pattern 5…$
voice-class sip early-offer forced
dtmf-relay rtp-nte
codec g711alaw
no vad
```

In the example above, we have configured an Outgoing secondary Dial-Peer from Voice Gateway to CUCM, so it will be a redundant dial-peer from dial-peer voice 2 voip that we have created earlier.

Redundancy to H.323 dial-peers

To configure the redundancy to H.323 dial-peers, the configuration is a little different, as there is no global configuration like the SIP UA.

What we do is creating a voice-class that should be applied to all H.323 dial-peers for which we want to enable the redundancy.

Step 1:Create the voice-class:

The voice-class configuration is:

```
voice class h323 1
h225 timeout tcp establish 2
```

With that, we have configured a timeout of 2 seconds, which is more than enough for a router to discover that the remote destination is not available.

Step 2:Apply the voice-class created to all dial-peers we want to enable redundancy:

```
dial-peer voice 100 voip
description OUTGOING TO CUCM PUBLISHER
destination-pattern 5..$
session target ipv4:10.100.10.10
voice-class h323 1
dtmf-relay h245-alphanumeric
codec g722-64
no vad
!
dial-peer voice 101 voip
description OUTGOING TO CUCM SUBSCRIBER
preference 1
destination-pattern 5..$
session target ipv4:10.100.10.11
voice-class h323 1
dtmf-relay h245-alphanumeric
codec g722-64
no vad
```

This configuration will:

- Use the “dial-peer voice 100 voip” to send the calls to CUCM Publisher;
- If the “dial-peer voice 100 voip” fails, it will send the calls to the

CUCM Subscriber using the “dial-peer voice 101 voip”

This process will repeat for each call that reaches this gateway searching for the destination, so as soon as the primary destination target is back online, it will return to receive calls normally. Remember to apply the voice-class h.323 to all your H.323 dial-peers for which you want to enable redundancy.

CHAPTER 10 - DIGITS MANIPULATION

Digits Manipulation is one of the most important functionalities of a telephony system, to enable correct routing on incoming and outgoing calls.

You will need to manipulate digits on CUCM. Inbound PSTN calls, outgoing PSTN calls, calls from other SIP systems, translate internal calls... there are a lot of reasons to edit the calling, or called number.

Fortunately, there are a lot of options on how to edit the digits. You can use CUCM or the Voice Gateway (H.323 or SIP). It's important to understand all the tools, so you can decide which one to use in each case.

Digits Manipulation on CUCM

Translation Patterns

Translation Patterns are the most basic and useful digit manipulation method on CUCM, because it applies globally to all the system, based on the Partition/CSS used - if you want to create a Translation Pattern to be used from everyone, just create it in a Partition that all your users can access.

To create it, go to menu "Call Routing > Translation Pattern > Add New":

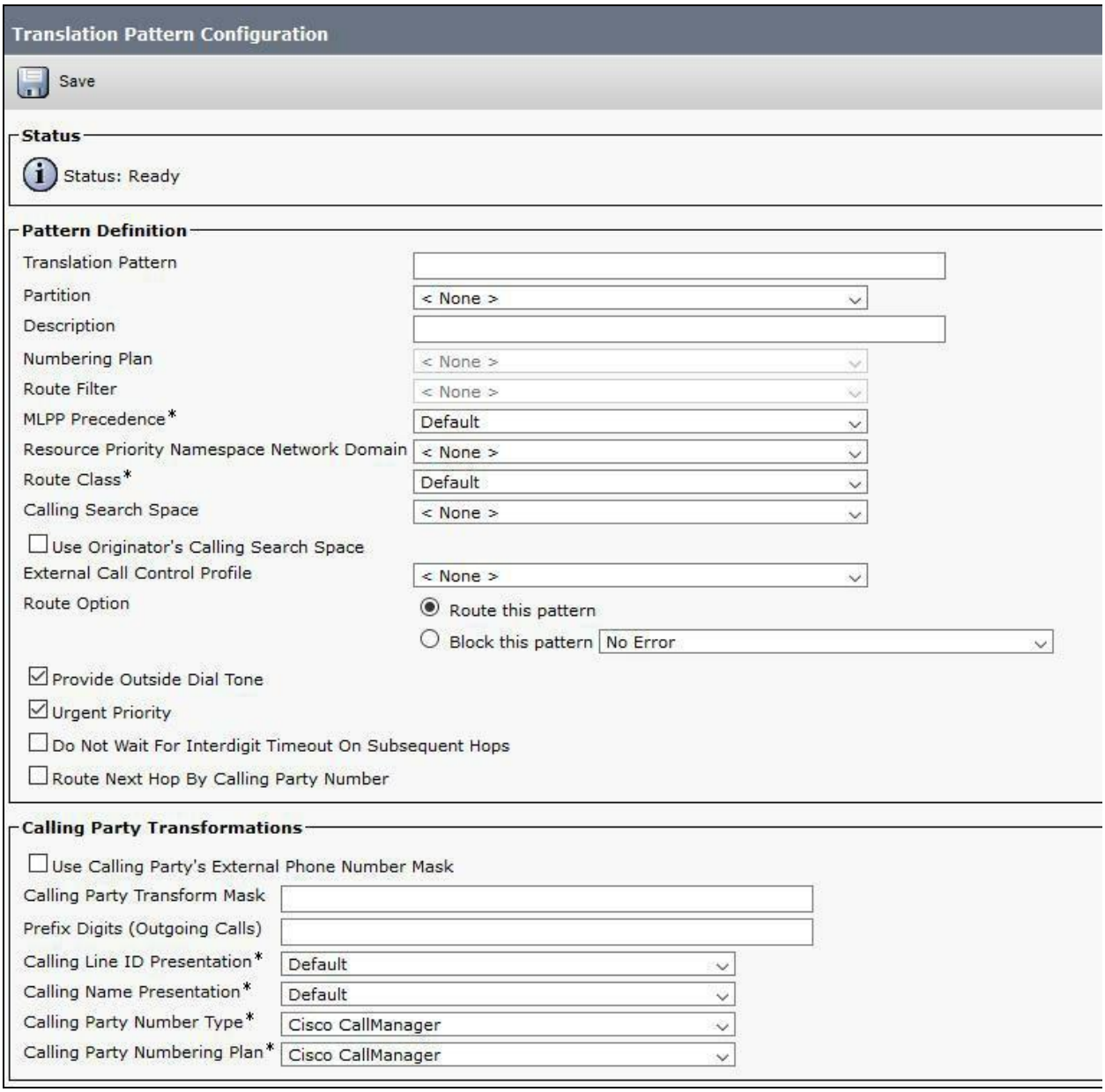


Figure 237: Translation Pattern configuration window

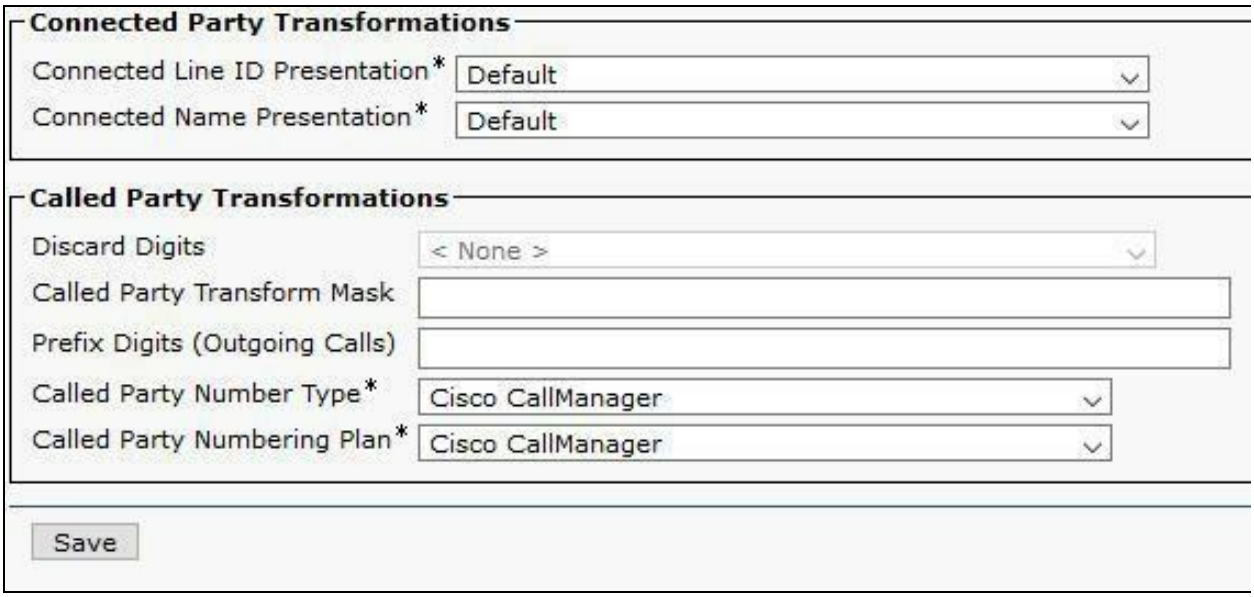


Figure 238: Translation Pattern configuration window

Here, the more important fields are:

Field	Description	Example
Translation Pattern	The called number you want to translate.	1500
Partition	The Partition where this Translation belongs.	INTERNAL_PT
Description	A description of the translation pattern.	Translate 1500 to 1003
Calling Search Space	A CSS that can reach the destination,	INTERNAL_CSS
Route Option / Route this pattern	Select if you want to enable it (default).	Checked
Route Option / Block this pattern	Select if you want to disable it temporarily.	Unchecked
Provide Outside Dial Tone	Select if you want the users to hear a secondary dial-tone when reached this translation (not recommended).	By default, always uncheck it.
Urgent Priority	If you want to route this translation as soon as it matches the numbers dialed Recommended, but can cause problems with other overlapping numbers, route patterns or	Checked

Technet24

	translations.	
Calling Party Transformations / Use Calling Party's External Phone Number Mask	Select if you want to edit the calling number.	-
Calling Party Transformations / Calling Party Transform Mask	Edit the calling number.	-
Calling Party Transformations / Prefix Digits (Outgoing Calls)	Prefix some digits to the calling number.	-
Called Party Transformations / Discard Digits	If you have typed any digit on your translation pattern, you can use this to edit the number.	-
Called Party Transformations / Called Party Transform Mask	Edit the called number.	-
Called Party Transformations / Prefix Digits (Outgoing Calls)	Prefix some digits to the called number.	-

Table 30: Translation Pattern main options

Some of the most commons uses are:

Completely edit the called number

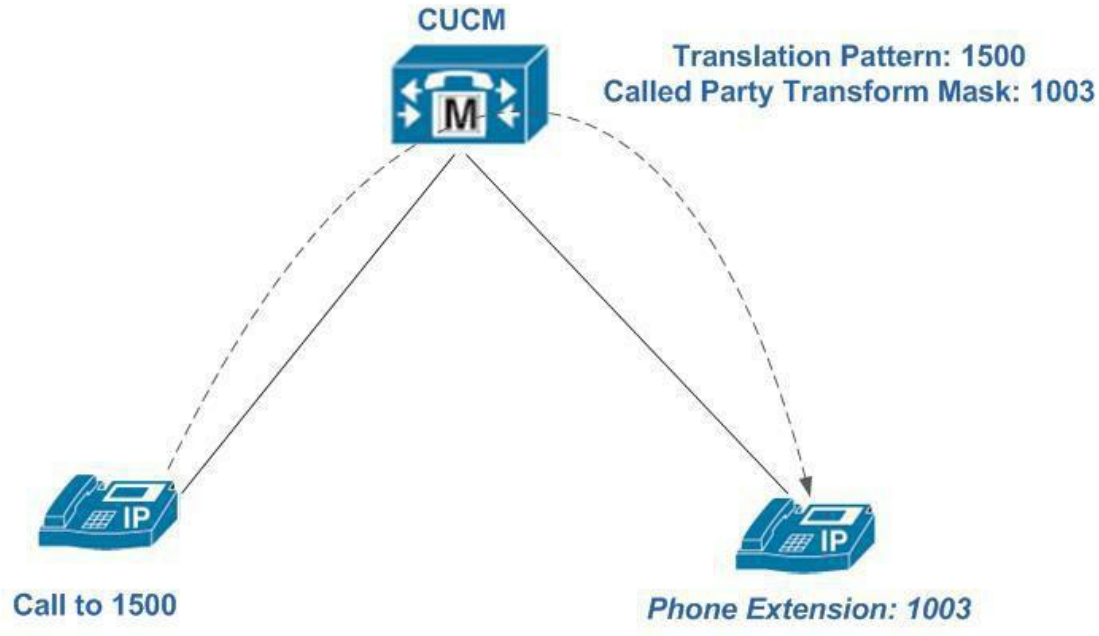


Figure 239: Translation Pattern editing called number

To do this configuration, edit the fields:

- Translation Pattern
- Partition
- Calling Search Space
- Provide Outside Dial Tone
- Called Party Transform Mask

Follow the example below:

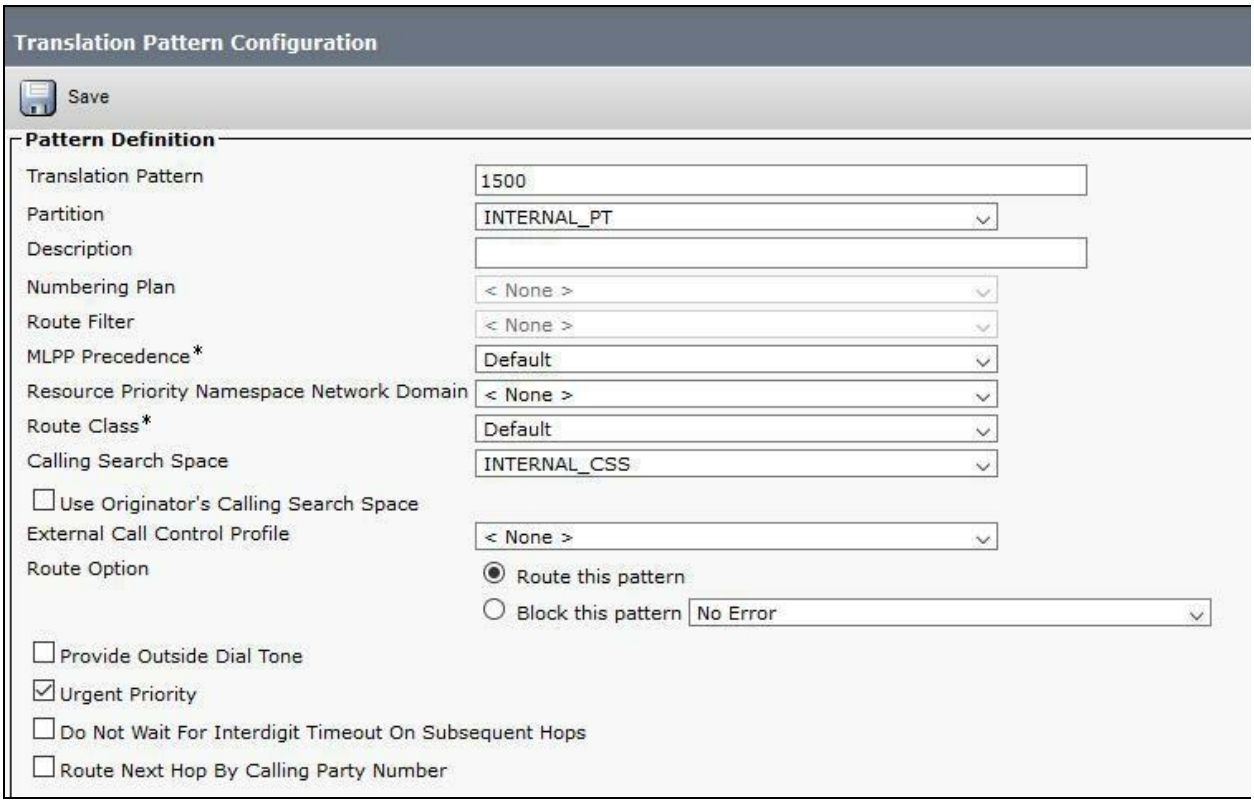


Figure 240: Translation Pattern editing called number

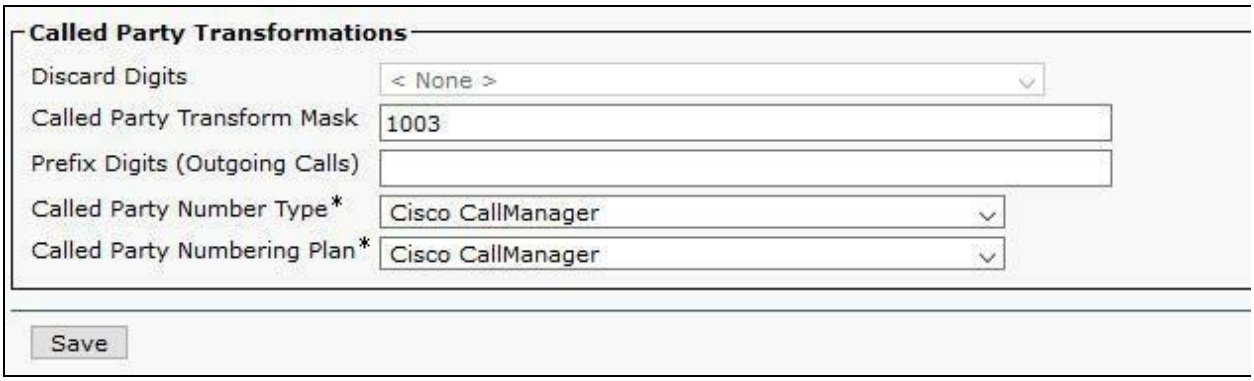


Figure 241: Translation Pattern editing called number

Remove the beginning of a number

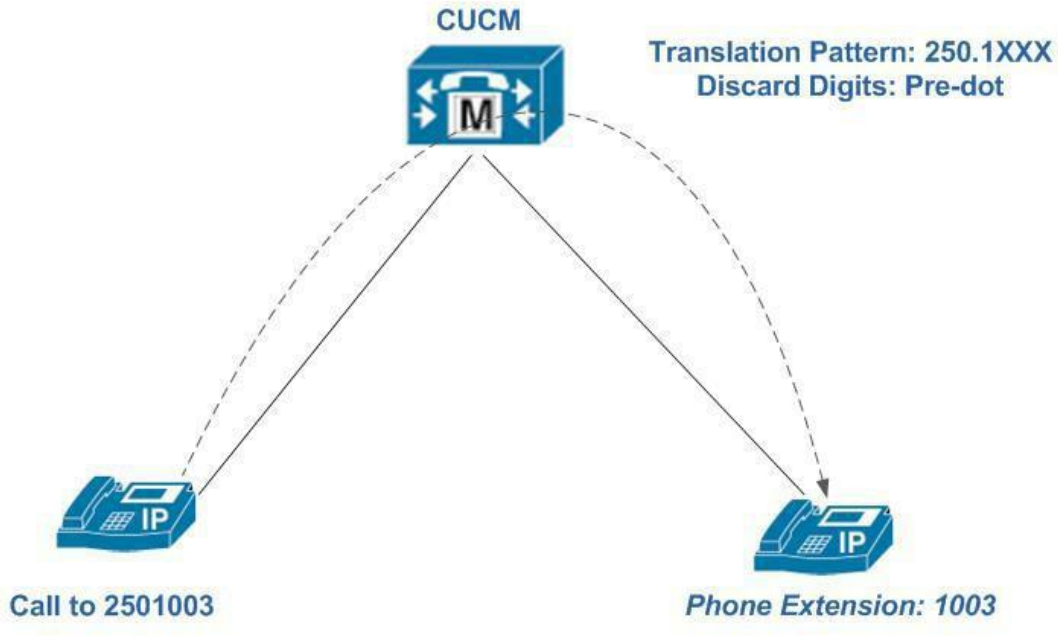


Figure 242: Translation Pattern editing the beginning of a number

To do this configuration, edit the fields:

- Translation Pattern
- Partition
- Calling Search Space
- Provide Outside Dial Tone
- Discard Digits

Follow the example below:

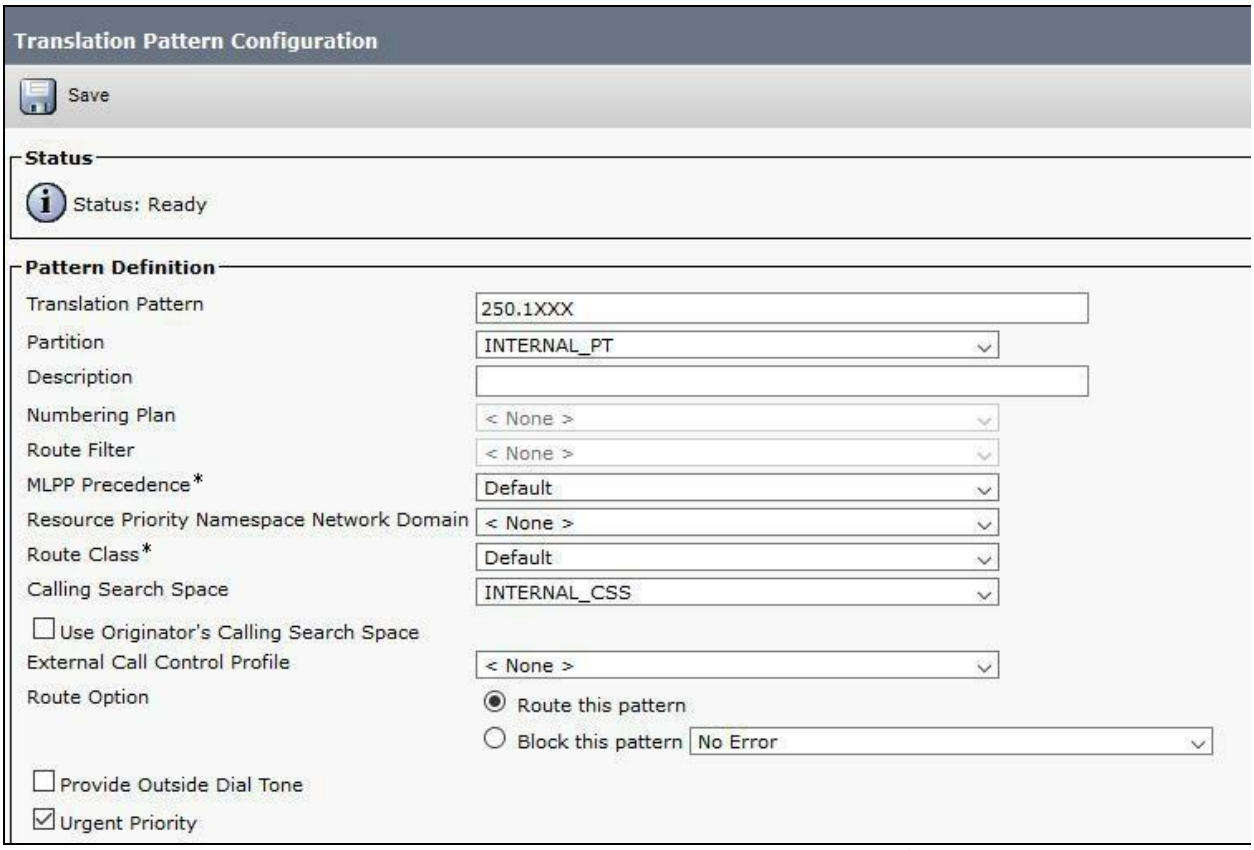


Figure 243: Translation Pattern editing the beginning of a number

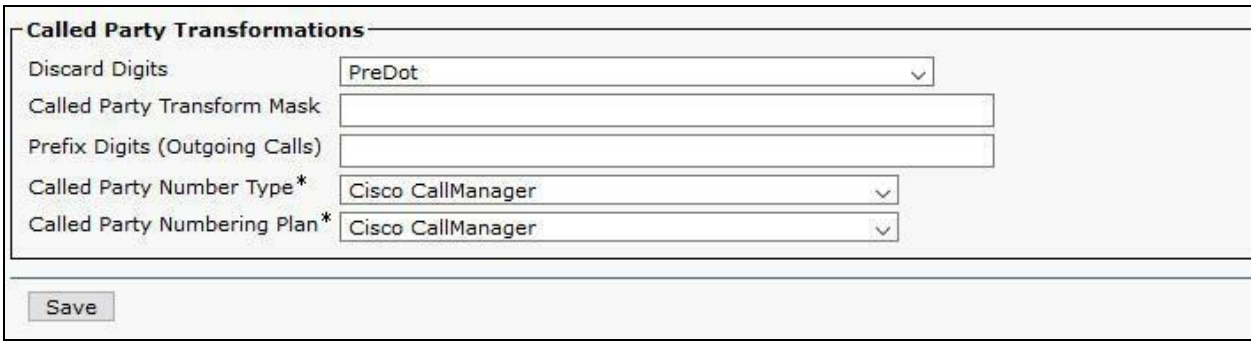


Figure 244: Translation Pattern editing the beginning of a number

Add a prefix in the beginning of a number

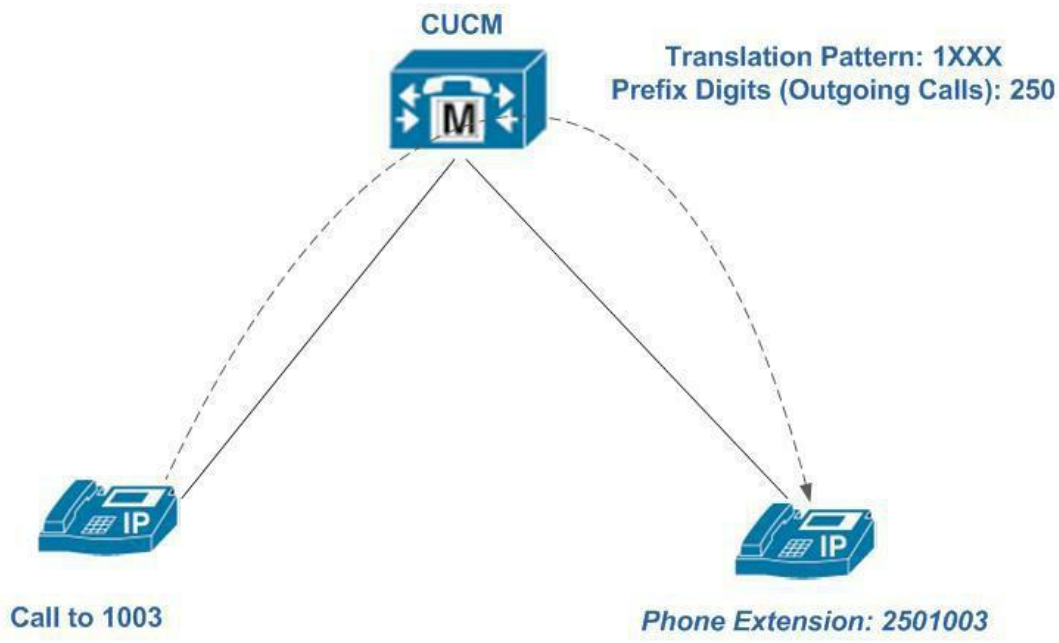


Figure 245: Translation Pattern add a prefix to a number

To do this configuration, edit the fields:

- Translation Pattern
- Partition
- Calling Search Space
- Provide Outside Dial Tone
- Prefix Digits (Outgoing Calls)

Follow the example below:

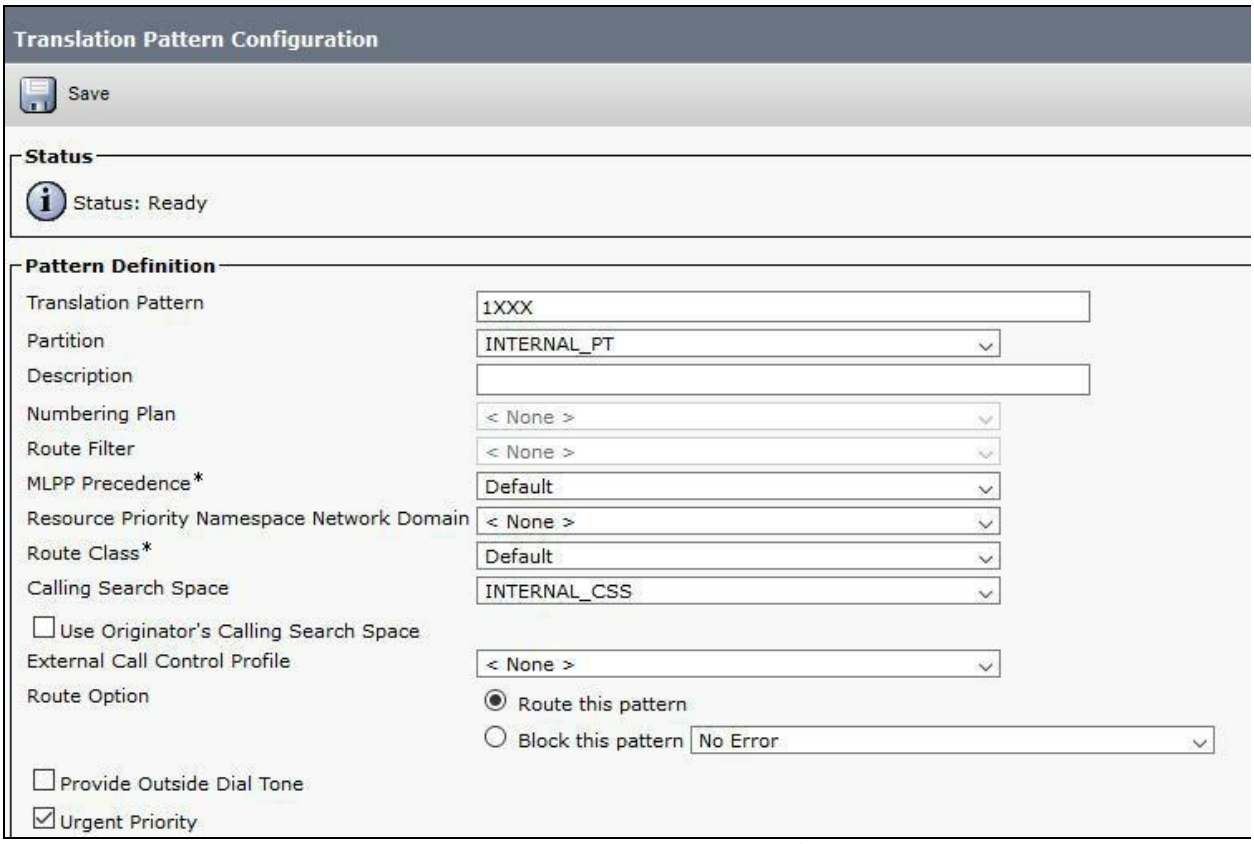


Figure 246: Translation Pattern add a prefix to a number

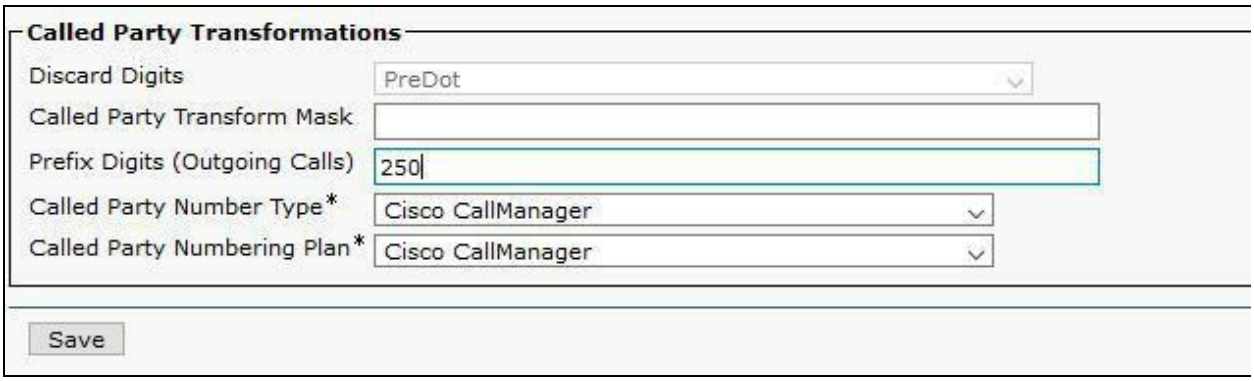


Figure 247: Translation Pattern add a prefix to a number

These 3 examples are very common, and you can mix then to get the result you want.

Route Pattern

Under CUCM Route Pattern (Call Routing > Route/Hunt > Route Pattern), there is some basic digit manipulation you can do like:

- Discard Digits (Pre-Dot)
- Calling Party Transform Mask
- Prefix Digits (Outgoing Calls)
- Called Party Transform Mask
- Prefix Digits (Outgoing Calls)

These are the same options we have under Translation Pattern configuration, so you can use the same examples we saw before in this chapter.

Incoming call under Gateway or Trunk

Under CUCM Gateway windows (menu Device > Gateway or Trunk), there are also a basic incoming call edit. You can:

- Significant Digits
- Prefix DN

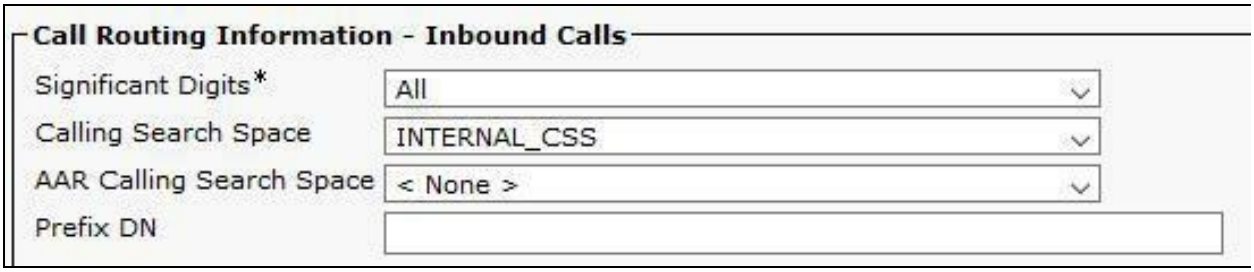


Figure 248: Inbound calls configuration under Gateway/Trunk

Field	Description	Example
Significant Digits	How many digits you want to collect from the incoming calls from this Gateway/Trunk to route in the CUCM.	Your PSTN provider is sending a call to number 333-1000, and your internal extensions are in the 1XXX range - you can select “4” as the significant digits, so you only will consider the 1XXX range. These digits are viewed from right to left.
Prefix DN	If you want to prefix some numbers/code.	Your PSTN provider is sending a call to number 1000, and your internal extensions are in the 2501XXX range - you can prefix the

		code 250 here.

Table 31: Incoming calls configuration options

You can use these 2 options together. Example: your PSTN is sending you a call with 7 digits, and your internal extension use as the user extension the 4 digits from the PSTN range plus an internal site code:

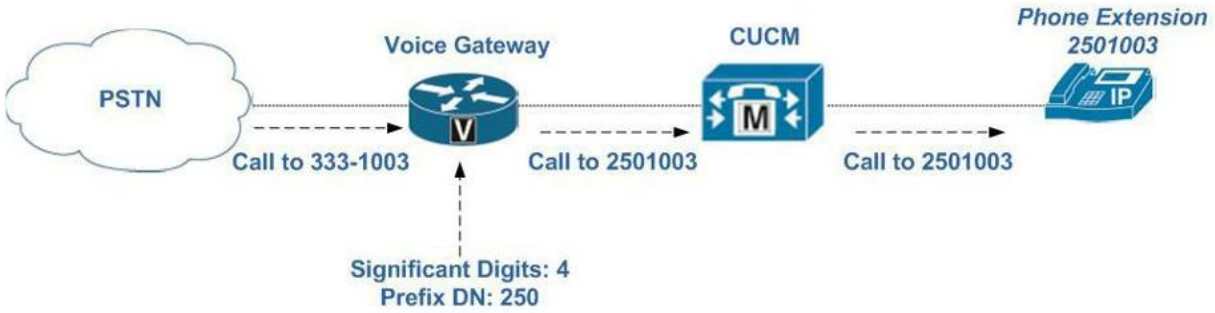


Figure 249: editing the significant digits and prefix

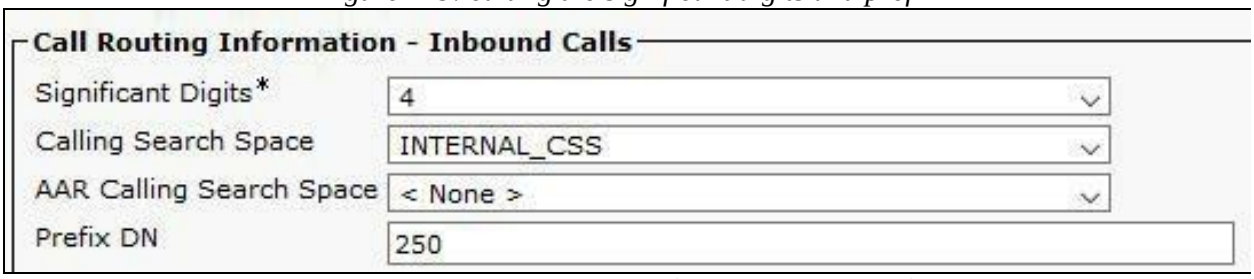


Figure 250: editing the signifcant digits and prefix

In this example, we are using the CUCM Gateway Configuration window to do all the number editing, but we can also do it within the Voice Gateway.

Wildcards available under CUCM

To have more flexibility on CUCM Translations and Route Patterns, it is good to use Wildcards, which are special characters that allow a single route pattern/translation to match a range of numbers.

Follow this list of frequent characters:

Character	Description	Example
X	Matches any single digit in the range 0 through 9.	1XXX - from 1000 to 1999
!	Matches one or more digits	9! - all numbers starting with 9

	in the range 0 through 9.	
[ ]	The square bracket ([ ]) characters enclose a range of values.	100[12345] - matches numbers 1001, 1002, 1003, 1004 and 1005
-	The hyphen (-) character, used with the square brackets, denotes a range of values.	100[1-5] - matches numbers 1001, 1002, 1003, 1004 and 1005
^	The circumflex (^) character, used with the square brackets, negates a range of values. It must be the first first character following the opening bracket ([). Each route pattern can have only one ^ character.	100[^1-5] - matches numbers 1000, 1006, 1007, 1008 and 1009.
.	Mark where you want to delete part of the number. To be used with the "Discard Digits" option.	250.100[1-5] - used with the "Discard Digits", remove the "250" and allow/send 100[1-5].
*	Provide an extra digit for special dialed numbers.	*1005 is different from extension 1005. You can use these numbers with * to special numbers, receptionist, security, etc.
#	Identifies the end of the dialing sequence.	You can create the following Route Pattern: 9.!# and remove the Pre-Dot and Trailing #. As soon as the user dials the #, the call will be routed without these 2 characters and do not wait for the interdigit timeout

		(which is 15 seconds by default).
$	Indicates that additional digits are not allowed.	1003$ - will match only number 1003, and not 10031.

Table 32: Wildcards available under CUCM

On the Cisco Website you can find the complete list, but these examples above are more than enough for almost all situations.

Digits Manipulation on Voice Gateways

Dial-Peers

Under POTS dial-peers, we have the following basic digit manipulation commands:

- digit stripping
- prefix
- forward digits

These 3 options are not available under VoIP dial-peers.

Digit Stripping

Digit stripping is automatically done on POTS dial-peers. The best way to understand it is an example:

```
dial-peer voice 9 pots
destination-pattern 9T
port 0/0/0:23
```

The dial-peer above will send this call to the voice-port 0/0/0:23 (probably a PSTN) and will automatically strip the first digit “9”. If you want to disable the digit-strip, you must do it on the dial-peer level with the command “no digit-strip”.

```
dial-peer voice 9 pots
destination-pattern 9T
no digit-strip
port 0/0/0:23
```

Prefix

The “prefix” command is used to prefix digits to a POTS dial-peer.

```
dial-peer voice 57 pots
destination-pattern 57....
prefix 250
port 0/0/0:23
```

In this example, as the dial-peer has the destination-pattern as “57….”, it will send as called only the last 4 digits; but as we added the command “prefix 250”, this call will be sent to the destination “250….”

Forward Digits

You can also edit how many digits you want to send on a POTS dial-peer with the command “forward-digits”. You can use it as a “forward-digits all”, which gives you the same result as the “no digit-strip” command;

```
dial-peer voice 9 pots
destination-pattern 9T
forward-digits all
prefix 250
```

or you can use it by choosing how many digits you want to forward:

```
dial-peer voice 9 pots
destination-pattern 9T
forward-digits 7
prefix 250
```

Voice Translation Rules

Voice Translation Rule is by far the most complete and advanced method to edit the calling and called information on a Cisco Voice Gateway. You can edit not only the digits, but also the calling/called type (unknown, subscriber, national, international) and even the plan (unknown, isdn).

Voice Translation rules can be used in POTS and VoIP dial-peers.

Topology

Voice Translation Rules can be applied to voice ports and dial-peers, as

inbound or outbound direction.

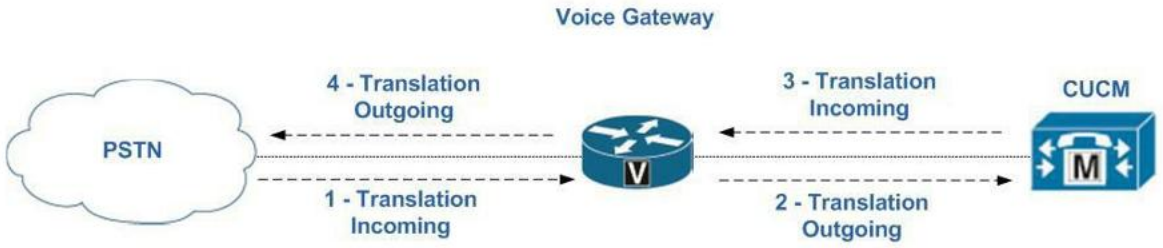


Figure 251: Voice Translation rules directions

In this image above, we have:

1. Inbound call leg from PSTN to Voice Gateway
2. Outgoing call leg from Voice Gateway to CUCM
3. Inbound call leg from CUCM to Voice Gateway
4. Outgoing call leg from Voice Gateway to PSTN

On each of these call legs, we can apply different translations. So it is very flexible and can solve problems in any environment you find. You need to pay attention to where you need to use the translation rule to get the results you want, as follows:

- If you apply a translation rule to an inbound call from the PSTN, the route pattern that sends the calls to the CUCM must use as the destination already traduced;

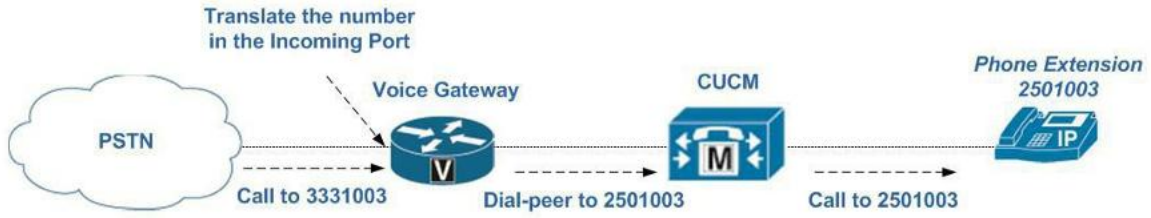


Figure 252: Voice Translation rule at incoming port

- If you do not apply the translation to the inbound call, you can

use the same number that the PSTN provider sent you to forward this to CUCM and translate it on the outgoing to PSTN dial-peer.

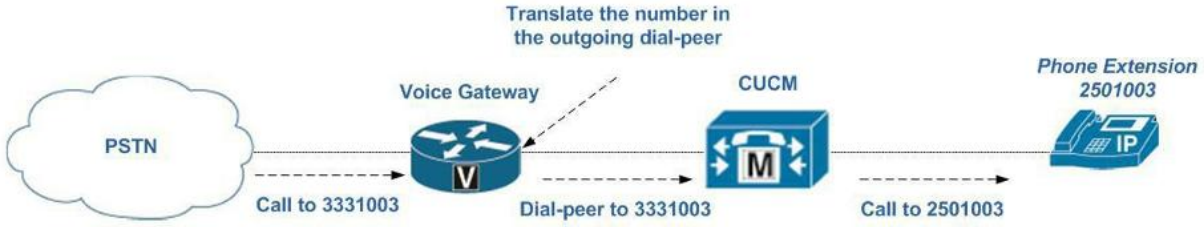


Figure 253: Voice Translation rule at outgoing dial-peer

In both scenarios above, the CUCM will receive the call correctly to extension 2501003. The CUCM doesn't know if the Voice Gateway has translated the call in the incoming port or in the outgoing dial-peer. The CUCM doesn't even know that the call has been translated at all.

Basic Translation Rule

Voice Translation Rules have the following format:

```
voice translation-rule 1
rule 1 /123/ /456/
rule 2 /789/ /159/
```

On the first line, we have the command "voice translation-rule" and a number associated with it (from 1 up to 1073741823).

Then, on the second line, we have the command "rule", rule number (from 1 up to 100) and the translation itself. The translation is divided in:

/before/ /after/

The objective is to replace the occurrence of the number. So, if we have 1234 and would like to change it to 5678, we will have:

/1234/ /5678/

```
voice translation-rule 1
rule 1 /1234/ /5678/
```

To test if our translation-rule is correct, we have a “test” command available, with the syntax “test voice translation-rule <rule_number> <test>

```
Router#test voice translation-rule 1 1234
Matched with rule 1
Original number: 1234   Translated number: 5678
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

As we can see below, our test was successful in translation-rule 1 using the number 1234. We can see the translation-rule output under the column “Translated number: 5678”.

The same test will not have any results if we test the number 123:

```
Router#test voice translation-rule 1 123
Router#
```

However, if we check the number 12345, the result is:

```
Router#test voice translation-rule 1 12345
Matched with rule 1
Original number: 12345  Translated number: 56785
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

As we can see, the number 12345 matches with our rule 1, because our rule does not specify that we want to edit only the number 1234, but any sequence of the digits in any part of our calls.

```
Router#test voice translation-rule 1 0001234000
Matched with rule 1
Original number: 0001234000     Translated number: 0005678000
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

If this is not our objective, we need to use more tools to be more specific.

The first thing we can do is limit the beginning of the number by using the character “^”:

```
voice translation-rule 1
rule 1 /^1234/ /5678/
```

With this configuration, we are specifying that the beginning of the number must start with 1234.

```
Router#test voice translation-rule 1 0001234
0001234 Didn't match with any of rules
```

This solves part of our problem. Now, to specify the end of the number, we can use the character “$”:

```
voice translation-rule 1
rule 1 /1234$/ /5678/
```

```
Router#test voice translation-rule 1 1234000
1234000 Didn't match with any of rules
```

If you want to specify the beginning and the end of the number, we just need to use both characters:

```
voice translation-rule 1
rule 1 /^1234$/ /5678/
```

Advanced Translation Rules

We can create advanced translation-rules by using wildcards. Follow some examples:

- Example 1:

```
voice translation-rule 1
rule 1 /^777....$/ /5000/
```

Replace any number with 7 digits that starts with 777 with “5000”.

- Example 2:

```
voice translation-rule 2
rule 1 /.*/ /5000/
```

Replace any number possible with “5000”.

- Example 3:

```
voice translation-rule 3
rule 1 /.+/ /5000/
```

Replace any number possible except null with “5000”.

- Example 4:

```
voice translation-rule 4
rule 1 /^0+/ /9011/
```

Replace any number that starts with a combination of zeros (0, 00, 000, etc) with “9011”.

```
Router#test voice translation-rule 4 0012223334444
Matched with rule 1
Original number: 0012223334444  Translated number: 901112223334444
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

Number Slice

Now our configuration will become more complex.

You can use number slice when you need to copy parts of a matched number and paste it to the replacement number. You slice the matched number into sets that you can keep or ignore.

To see a very common situation for this, let’s imagine this scenario:

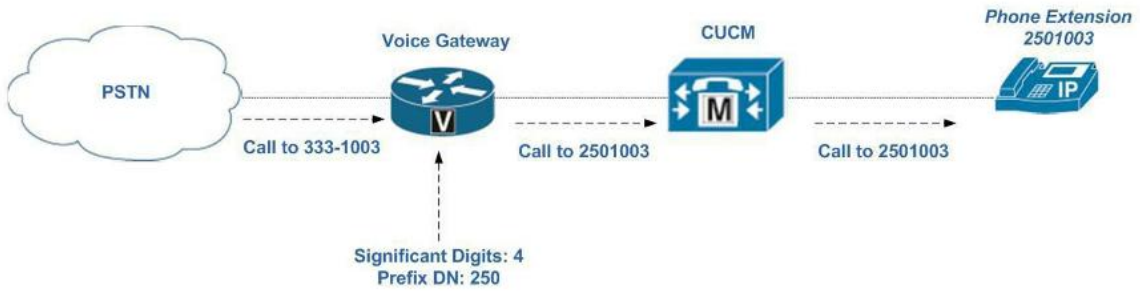


Figure 254: Voice Gateway topology

We saw this same topology in this chapter, but there we did the digit

manipulation under CUCM. Our problem is:

- The PSTN is sending the call to number 3331003;
- The CUCM has the extension 2501003;
- So we need to remove this “333” and prefix “250” before sending this call to CUCM.

We need to:

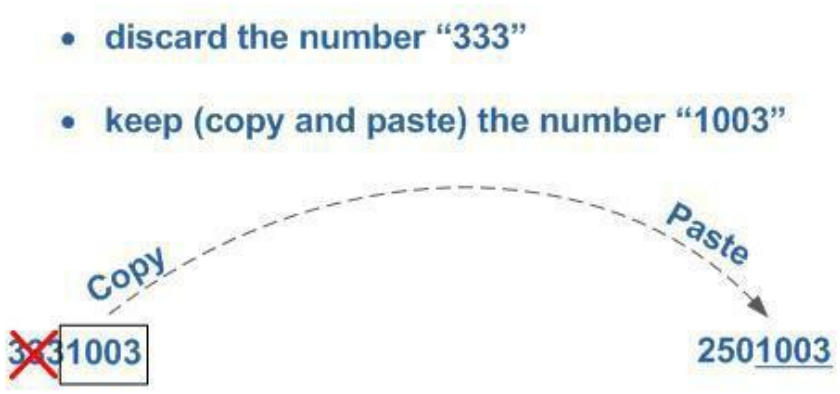


Figure 255: copy and past via number slice

The voice translation-rule to achieve this is:

```
voice translation-rule 4
rule 1 /^333\(....\)/ /250\1/
```

Explaining this mess:

Character	Explanation
/	Begin the first part of our translation.
^	The “^” character specifies that the number must start with the following digits.
333	The digits 333 (beginning of the number).
\(	Where our selection starts; our selection will be inside the brackets (); however, we need to add the special character \ to mark the beginning and the end of the brackets.

....	How many digits we want to “copy” - any 4 digits in this case.
\)	Where our selection ends. The closing bracket) plust the special character \
/	End of the first part of our translation.
/	Begin of the second part of our translation.
250	Add the digits 250 to the beginning of the second selection
\1	This is where the magic happens. This command “\1” paste the first selection we have copied to this point.
/	End of the second part of our translation.

Table 33: voice translation-rule 4 explained

The number slice is very flexible. You can do many things with this tool. Another example:

```
voice translation-rule 4
rule 1 /^\(333\)444\(....\)/ /\1555\2/
```

In this example, we are selecting the digits 333 as our first selection, skipping the number 444 and selecting the last 4 digits as our second selection. Then, we are copying these 2 selections to the second part of our translation. The final result is the number 333 555 ....

```
R1#test voice translation-rule 4 3334445678
Matched with rule 1
Original number: 3334445678     Translated number: 3335555678
Original number type: none      Translated number type: none
Original number plan: none      Translated number plan: none
```

Applying the translation-rules

To apply the translation rule you need to:

Step 1:Create the Translation-rule;

Create the translation rule as we have done above.

Remember that we can have up to 100 rules under each voice translation-rule.

Step 2:Create a Translation-Profile and associate the translation-rule created as called or calling;

```
voice translation-profile INCOMING-FROM-PSTN
translate called 1
```

Note that a translation-profile can translate called and calling at the same time:

```
voice translation-profile INCOMING-FROM-PSTN
translate called 1
translate calling 2
```

Also, it's not common, but sometimes you can use the same translation-rule as called and calling on a translation-profile if you want to.

```
voice translation-profile INCOMING-FROM-PSTN
translate called 1
translate calling 1
```

Step 3:Apply the translation-profile created:

You can apply the translation-profile as incoming, outgoing, or both:

```
voice-port 0/0/0:15
translation-profile incoming INCOMING-FROM-PSTN
```

```
voice-port 0/0/0:15
translation-profile outgoing OUTGOING-TO-PSTN
```

```
voice-port 0/0/0:15
translation-profile incoming INCOMING-FROM-PSTN
translation-profile outgoing OUTGOING-TO-PSTN
```

Wildcards available under Voice Gateways

Unfortunately, the wildcards available under voice gateways are not precisely the same as we have under CUCM, so this can cause some mistakes. Follow

below the list of more used wildcards under voice gateways (H.323 and SIP):

Character	Description	Example
.	Matches any single digit in the range 0 through 9.	1… - from 1000 to 1999
[ ]	The square bracket ([ ]) characters enclose a range of values.	100[12345] - matches numbers 1001, 1002, 1003, 1004 and 1005
-	The hyphen (-) character, used with the square brackets, denotes a range of values.	100[1-5] - matches numbers 1001, 1002, 1003, 1004 and 1005
^	The circumflex (^) character, used with the square brackets, negates a range of values. It must be the first first character following the opening bracket ([). Each route pattern can have only one ^ character.	100[^1-5] - matches numbers 1000, 1006, 1007, 1008 and 1009
T	Matches any number of dialed digits.	9T - all numbers starting with 9 9.T - all numbers starting with 9 with at least 1 character after the first “9” (more common to use this way);

Table 34: Wildcards available under Voice Gateways

CHAPTER 11 - SRST

How to configure and test the SRST functionality

What is SRST Mode?

Cisco Unified Survivable Remote Site Telephony (SRST) is used when you have a remote site without a CUCM on the local network. In this case, these phones register on the remote CUCM using any kind of WAN link (MPLS, VPN, etc.). If this link goes down, your phones will lose connectivity to the CUCM Cluster, and they won't have a server to register themselves. SRST provides a primary telephony system to these phones while the WAN link is down. Without the SRST, these phones will not work until the WAN link is restored.

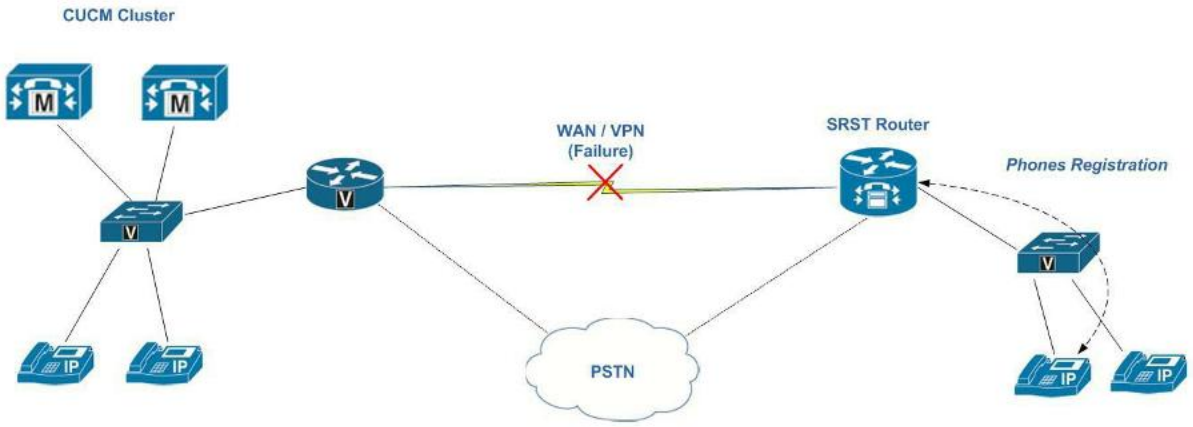


Figure 256: Cisco Phones registered remotely via WAN link

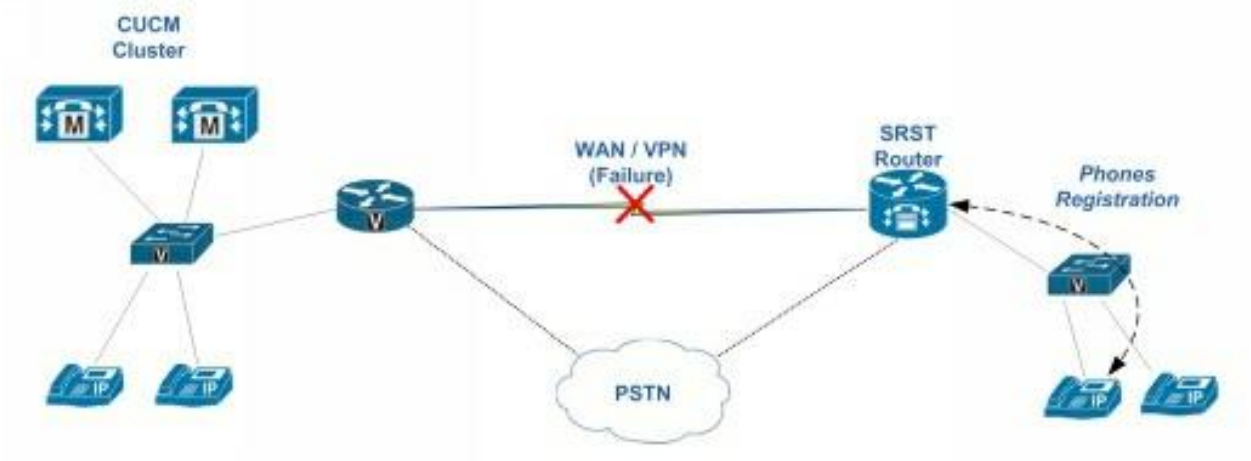


Figure 257: Cisco Phones local SRST registration during WAN failure

The SRST functionality is entirely automatic. When the WAN connectivity is lost, all phones on the remote site will be registered on the SRST Gateway and will be able to:

- Place and Receive internal calls from phones registered on the same SRST Gateway
- Place and Receive external calls, if any kind of PSTN connectivity is available on the SRST Gateway (FXO, T1, E1, SIP Trunking, etc.).

As soon as the WAN link is restored, the phones will automatically register back to the configured CUCM server as it was before the link outage.

Hardware requirements

The numbers of phones being supported on Cisco SRST depends on the hardware model:

Platform	Number of Phones Supported
Cisco 800 Integrated Services Router	Up to 5 phones
Cisco 2901 Integrated Services Router	Up to 35 phones
Cisco 2911 Integrated Services Router	Up to 50 phones
Cisco 2921 Integrated Services Router	Up to 100 phones
Cisco 2951 Integrated Services Router	Up to 250 phones

Cisco 3925 Integrated Services Router	Up to 700 phones
Cisco 3945 Integrated Services Router	Up to 1200 phones
Cisco 3925E Integrated Services Router	Up to 1350 phones
Cisco 3945E Integrated Services Router	Up to 1500 phones
Cisco 4321 Integrated Services Router	Up to 50 phones
Cisco 4331 Integrated Services Router	Up to 100 phones
Cisco 4351 Integrated Services Router	Up to 750 phones
Cisco 4431 Integrated Services Router	Up to 1200 phones
Cisco 4451-X Integrated Services Router	Up to 2000 phones

Figure 35: Cisco Unified SRST ISR Platform Density

Configuring SRST Mode

The steps to configure the SRST to a remote site are:

Step 1:Create the SRST Reference on CUCM.

- Go to menu “System > SRST”;
- Add New;
- Configure Name, Port (leave the default, 2000), IP Address, SIP Network/IP Address (same as IP Address) and SIP Port (leave the default, 5060);

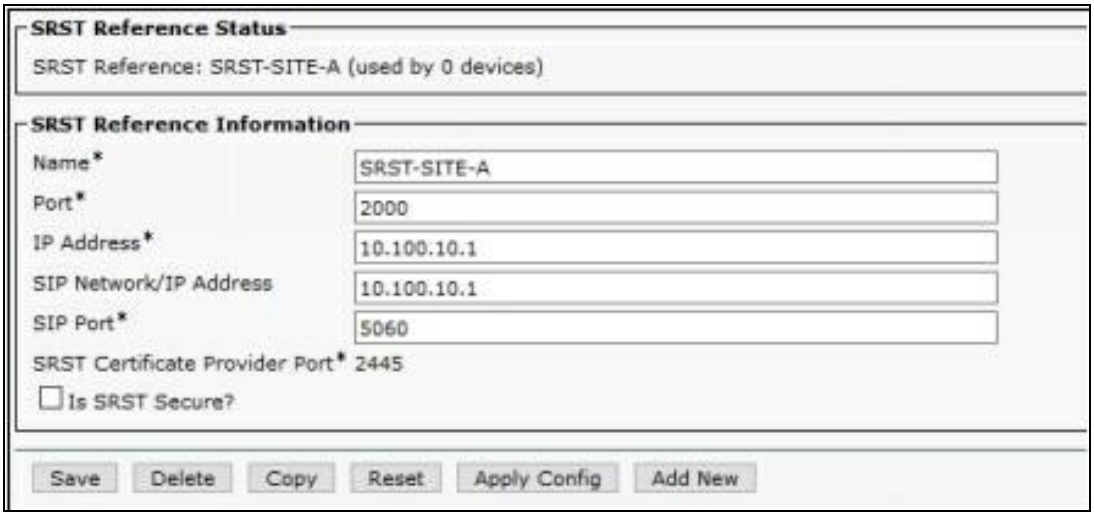


Figure 258: Cisco Phones local SRST registration during WAN failure

- Save it.

Step 2: Associate the SRST Reference to a Device Pool.

- Go to menu “System > Device Pool”;
- Click “Find”;
- Select the Device Pool you want to configure the SRST Reference;
- On “SRST Reference”, select the SRST Reference you created;
- Save it;
- Click “Reset” (all phones on this Device Pool will reset);

After the reboot, these phones will receive the SRST as the 2nd or 3rd registration option, depending on your environment.

Step 3: Configure the SRST Reference on the Voice Gateway for SCCP Phones.

The SRST Configuration is straightforward. Follow an example configuration:

```
call-manager-fallback
secondary-dialtone 9
max-conferences 8 gain -6
transfer-system full-consult
timeouts interdigit 3
ip source-address 10.100.10.1 port 2000
max-ephones 30
max-dn 144
system message primary SRST Fallback Active
system message secondary SRST Fallback
transfer-pattern .T
date-format dd-mm-yy
```

Follow the commands detailed:

Command	Description
call-manager-fallback	Enter the SCCP SRST Configuration mode.
secondary-dialtone 9	Provides secondary when the users dials 9.
	Limit the number of conferences and set the volume

max-conferences 8 gain -6	conference.
transfer-system full-consult	Defines the call-transfer method for all lines served by the Cisco Unified SRST router.
timeouts interdigit 3	Defines how many seconds the phone will wait until forward a call.
ip source-address 10.100.10.1 port 2000	Define the source IP Address for the SCCP SRST process. Should be the same as configured in CUCM.
max-ephones 30	Defines the maximum of phones able to register on SCCP SRST.
max-dn 144	Defines the maximum of lines able to register on SCCP SRST.
system message primary SRST Fallback Active	Defines the message to be displayed on phones when in SCCP SRST Mode.
system message secondary SRST Fallback	Message to be displayed in old Cisco Phones ike 7910.
transfer-pattern .T	Allows call transfer to other phone numbers.
date-format dd-mm-yy	Format how the date will be displayed on the Phone screen.

Table 36: SCCP SRST commands explanation

If you are using this router as an H.323 Gateway or SIP Trunk, you will already have dial-peers to the PSTN, so the phones probably will be able to place and receive PSTN normally. If not, check your dial-plan and if is there any translation-pattern missing.

If you are using this router as an MGCP Gateway, you will need to create dial-peers to be used by the router when it is in SRST Mode.

Step 4: Configure the SRST Reference on the Voice Gateway for SIP Phones.

Follow the commands necessary:

```
voice service voip
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
```

```
!
sip
   registrar server expires max 600 min 60
!
voice register global
max-dn 300
max-pool 58
!
voice register pool  11
id network 10.100.11.0 mask 255.255.255.0
dtmf-relay rtp-nte cisco-rtp sip-notify
 codec g711ulaw
no vad
!
sip-ua
registrar ipv4:10.100.10.1 expires 600
```

And the commands explanation:

Command	Description
voice service voip	Enter the voip configuration mode.
allow-connections h323 to h323	Allow calls from H.323 to H.323.
allow-connections h323 to sip	Allow calls from H.323 to SIP.
allow-connections sip to h323	Allow calls from SIP to H.323.
allow-connections sip to sip	Allow calls from SIP to SIP.
sip	Enter the SIP configuration mode
registrar server expires max 600 min 60	Enables SIP registrar functionality and set expiration timers in seconds.
voice register global	Enter the voice register global SRST mode.
max-dn 300	
max-pool 58	Defines the maximum of phones able to register on SCCP SRST.Defines the maximum of lines able to register on SCCP SRST.
voice register pool 10	Create a pool to control which registrations are accepted by a Cisco SIP SRST device.
codec g711ulaw	Set the default codec for SIP SRST mode.
id network 10.100.10.0 mask	

255.255.255.0	Set the phone subnet allowed to register in this router.
dtmf-relay rtp-nte cisco-rtp sip-notify	Set the DTMF-Relay type.
codec g711ulaw	Set the default codec for SIP SRST mode.
no vad	Disable calls with VAD (Voice Activity Detection) while in SIP SRST Mode.
sip-ua	Enter the SIP User-Agent configuration mode.
registrar ipv4:10.100.10.1 expires 600	SIP SRST IP Address, same as configured in CUCM SRST Reference
voice register global	Enter the Voice Register Global mode.
mode srst	Set the mode to SRST (default).
system message "SRST Fallback Active”	Defines the message to be displayed on phones when in SIP SRST Mode.
max-dn 200	Defines the maximum of phones able to register on SIP SRST.
max-pool 100	Defines the maximum of lines able to register on SIP SRST.

Table 37: SIP SRST commands explanation

Testing SRST

To test SRST and simulate a WAN failure, the two best options are:

- remove the WAN network cable;
- create a route pointing the CUCM IP Addresses to the “Null 0” interface.

Of course, the problem with the first option is that it will impact all your network traffic for this location. Also, sometimes if you are talking on the phone with someone who is not precisely a technician, and this person can remove the wrong cable, or even won’t be able to restore the correct wire to the correct network port.

The second option is better if you only have remote access to a location, and you want to test the telephony without interrupting the other network traffic from this location. To do it, the command is:

```
ip route network mask Null0
```

For example:

```
ip route 10.10.20.32 255.255.255.255 Null 0
```

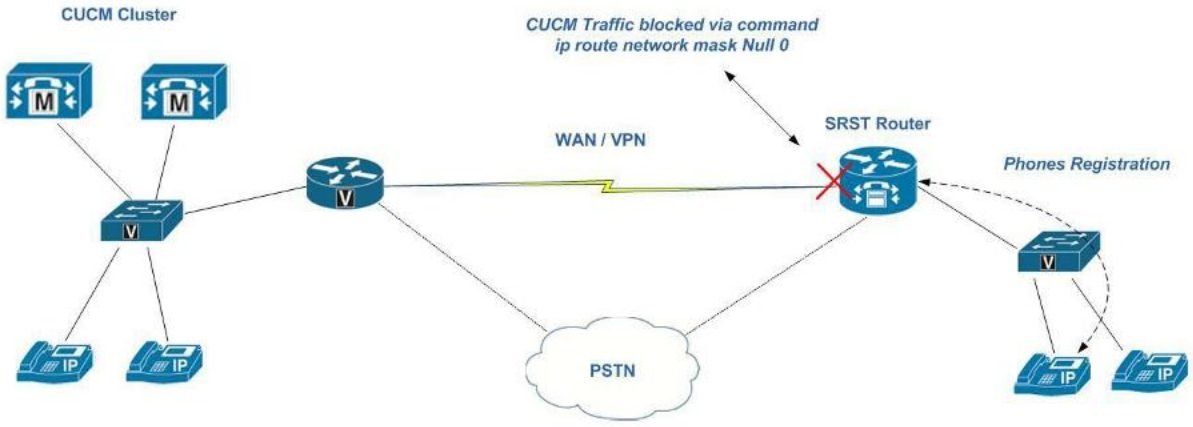


Figure 259: Cisco Phones local SRST registration during WAN failure

The command above will route the CUCM IP Address (10.10.20.32) to this Null 0 interface, which is a kind of “trash can” of the Cisco router/switch. As we are using the /32 IP Address, we need to type this command to each CUCM server.

After you type this command, ask someone on the remote site to test the internal calls in this location. They should also be able to place and receive PSTN calls if this site has an independent PSTN connection, like T1, E1, FXO or a SIP Trunk to a PSTN provider.

When your tests are finished, to remove this configuration and return to normal operation, the command is:

```
no ip route network mask Null0
```

For example:

```
no ip route 10.10.20.32 255.255.255.255 Null 0
```

Verify SRST

To verify the SRST during your test, first you need to check if the phones are

registered locally with these commands:

Command	Purpose
show call-manager-fallback all	Displays the detailed configuration of all the Cisco Unified IP phones, voice ports, and dial peers of the Cisco Unified SRST Router.
show call-manager-fallback dial-peer	Displays the output of the dial peers of the Cisco Unified SRST Router.
show call-manager-fallback ephone-dn	Displays Cisco Unified IP Phone destination numbers when in call manager fallback mode.
show call-manager-fallback voice-port	Displays output for the voice ports.
show dial-peer voice summary	Displays a summary of all voice dial peers.
show ephone phone	Displays Cisco Unified IP Phone status.
show ephone offhook	Displays Cisco Unified IP Phone status for all phones that are off hook.
show ephone registered	Displays Cisco Unified IP Phone status for all phones that are currently registered.
show ephone remote	Displays Cisco Unified IP Phone status for all nonlocal phones (phones that have no Address Resolution Protocol [ARP] entry).
show ephone ringing	Displays Cisco Unified IP Phone status for all phones that are ringing.
show ephone summary	Displays a summary of all Cisco Unified IP Phones.
show ephone telephone-number phone-number	Displays Unified IP Phone status for a specific phone number.
show ephone unregistered	Displays Unified IP Phone status for all unregistered phones.
show ephone-dn tag	Displays Unified IP Phone destination numbers.
show ephone-dn summary	Displays a summary of all Cisco Unified IP Phone destination numbers.
show sip-ua status registrar	Display SIP registrar clients.
show voice port summary	Displays a summary of all voice ports.
show voice register all	Displays all SIP SRST configurations, SIP phone registrations and dial peer info.

Technet24

show voice register global	Displays voice register global config.
show voice register pool all	Displays all config SIP phone voice register pool detail info.
show voice register pool <tag>	Displays specific SIP phone voice register pool detail info.
show voice register dial-peers	Displays SIP-SRST created dial peer.
show voice register dn all	Displays all config voice register dn detail info.
show voice register dn <tag>	Displays specific voice register dn detail info

Table 38: SRST troubleshooting commands

You can also use debugs like:

```
debug voice ccapi inout
debug isdn q931
terminal monitor
```

To cancel all these debugs, run:

```
undebug all
```

CHAPTER 12 - CUCM USERS

There are 3 types of users in CUCM: Local Users, LDAP Synchronized Users and Application Users

Local User

Local users are users created directly on CUCM. On old CUCM versions, you cannot have Local Users and LDAP Synchronized users in the same CUCM Cluster, but this is not a problem anymore.

If you have enabled the LDAP Synchronized users, you can still create some users manually as local users. It is useful if you are not the administrator of your Microsoft Active Directory Domain.

The creation process is straightforward, just go to “User Management > End User > Add New”. Fill the form with the information necessary, and you are done. Use the field “Telephone Number” to add the user extension, so other users will be able to find this user under the Corporate Directory.

LDAP Synchronized User

LDAP Synchronized User is users synchronized from an external LDAP user database, usually from Microsoft Active Directory. This configuration is divided into 4 parts:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Custom Filter

All these options are available under the menu “System > LDAP”.

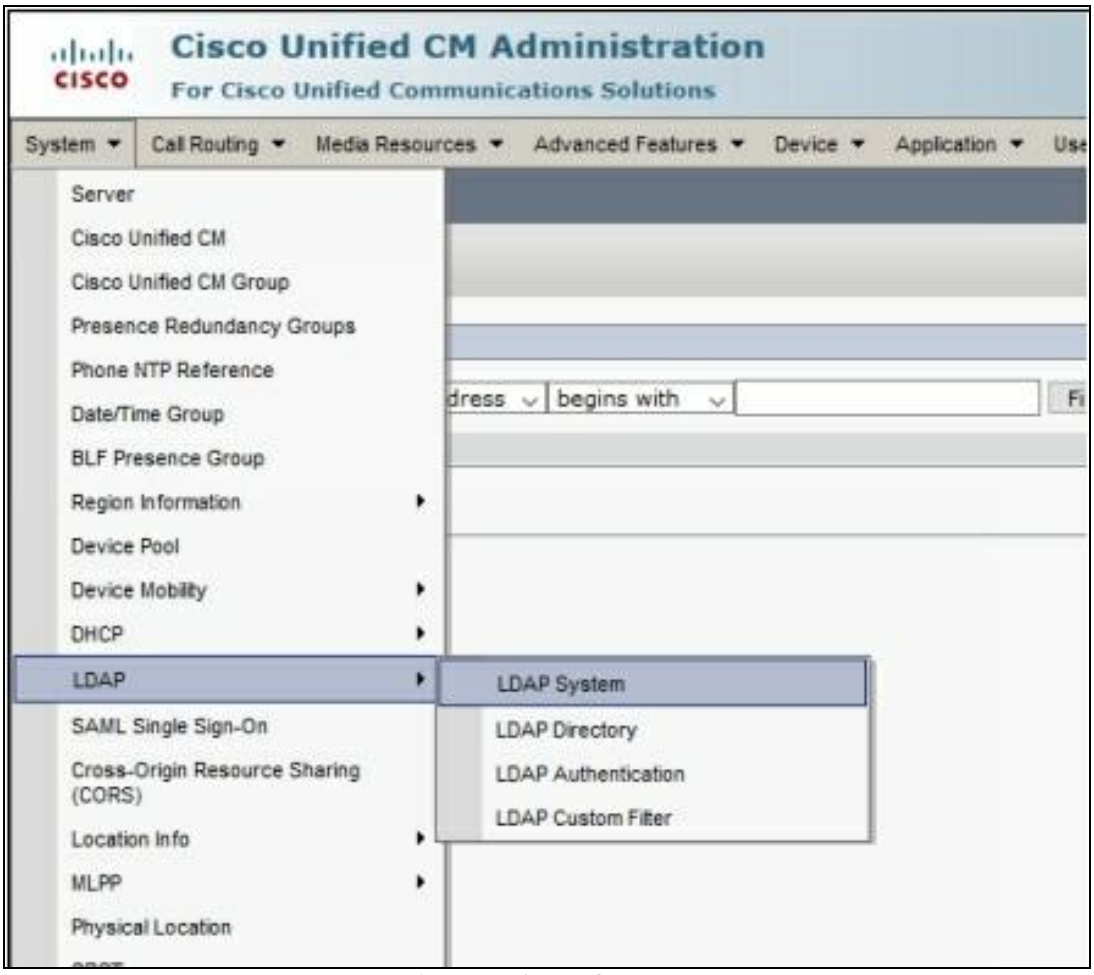


Figure 260: LDAP menu

LDAP System Configuration

This is the initial configuration, where you enable the LDAP System Configuration. Here, you will check the field “Enable Synchronizing from LDAP Server”, choose the “LDAP Server Type” (usually, Microsoft Active Directory) and select which LDAP Attribute you want to use as the User ID in CUCM (usually, sAMAccountName).

LDAP Directory

Now you will really configure your LDAP Directory. You need to have an Active Directory Account with at least Read Permissions under your Active Directory structure. You need to fill the following information:

Field	Description	Example
LDAP Configuration Name	A short description to CUCM	Company Domain.com

	configuration	
LDAP Manager Distinguished Name	The AD Account with at least Read Permissions on this domain	Domain\Administrator
LDAP Password	The password for the AD Account	-
LDAP User Search Base	Where CUCM should search for users	DC=domain,DC=com
Synchronize	Users Only or Users and Groups	-
LDAP Custom Filter for Groups	If you have a LDAP Custom Filter, apply it here	-
Perform Sync Just Once	Select if you only want to synchronize 1 time	-
Perform a Re-sync Every	Select if you want to synchronize with some regularity	1 DAY
Next Re-sync Time (YYYY-MM-DD hh:mm)	When will be the next sync date	2019-02-19 20:59
Phone Number	Which field of Active Directory should be used to find the user extension	telephoneNumber (or ipPhone)
Directory URI	The field in AD where is located the Directory URI of the user	msRTCSIP-primaryuseraddress (or "mail")
LDAP Server Information - Host Name or IP Address for Server	IP Address of the AD Server	10.10.10.10
LDAP Port	TCP Port in AD Server	389

Table 39: LDAP Directory configuration options

LDAP Authentication

While LDAP Directory will allow the users database to synchronized from Microsoft Active Directory to CUCM, LDAP Authentication will allow these users to authenticate using these credentials.

Usually, you will insert the same information here as you have entered in the LDAP Directory if you want to enable LDAP Authentication for your users in CUCM.

LDAP Custom Filter

LDAP Custom Filter is used when you need to find your users in Active Directory; when you don’t want to import all users from a specific location, but only part of these users with particular attributes. You can create this LDAP Custom Filter and apply it to an LDAP Directory.

Some examples:

```
(&(objectclass=user)(!(objectclass=Computer))(!(UserAccountControl:1.2.840.113556.1.4.803:=2 ))
(telephonenumber=919*))
```

This filter selects only users that have a prefix of 919 in their telephone number field.

```
(&(objectClass=group)(CN=Sales*)(!(groupType:1.2.840.113556.1.4.803:=2147483648)))
```

This filter selects only groups that begin with the name Sales.

You can check on the internet for "Microsoft Active Directory LDAP Syntax Filters" to create your own filter, as this filter is not a Cisco CUCM filter, but an LDAP filter.

Application User

Application Users are users created in CUCM to some specific tasks like AXL and IPMA Access. Regular daily tasks do not require the creation of Application Users. These users are located under “User Management > Application User”.

If an application requires the creation of an Application User to access CUCM, check this Application documentation, as it will probably inform you which level of permission is necessary for this application.

Create an Admin user on CUCM

An Admin User in CUCM is a regular user, local or LDAP Synchronized,

which has received Admin Permissions on CUCM. There are some permissions levels, but in this example, we will allow the user full admin permission. You can test the permissions level if you need to have a more granular access permissions, like “able to create phones but not able to reboot CUCM”.

To allow a regular user to become a CUCM Administration, open the user you want, scroll down until “Permissions Information”, click “Add to User Group”, and select the group “Standard CCM Admin Users” and save it.

As you can see, on this screen you can see other groups like “Standard CCM Phone Administration” or “Standard CCM Server Maintenance”. If you want to know what each of these groups is allowed to do, go to the menu “User Management > User Settings > Role”.
Click on the Role you want to check, and a window will open explaining all “Resource Access Information”, which are the permissions to this group.

You can use one of these default Roles or create your own personalized. To make this process easier, use the function “Copy” to create your own Role based on one of these default Roles.

CHAPTER 13 - MEDIA RESOURCES

How to provide advanced resources to your devices

Conference Bridge

Conference Bridge allows the devices to make audio and video conferences. There are 2 types of conference bridge: Software and Hardware:

Software Conference Bridge

Software Conferences Bridges automatically get created when the CUCM is installed, so you cannot add or remove it. Each CUCM node hosts one Software Conferences Bridge.

It supports G.711 codecs by default, and it can handle 128 streams; it means that you can run a software conference bridge with 128 users in a single conference, or up to 42 conferencing resources with three users per conference.

To check your Software Conferences Bridges, go to menu “Media Resources > Conference Bridge”:

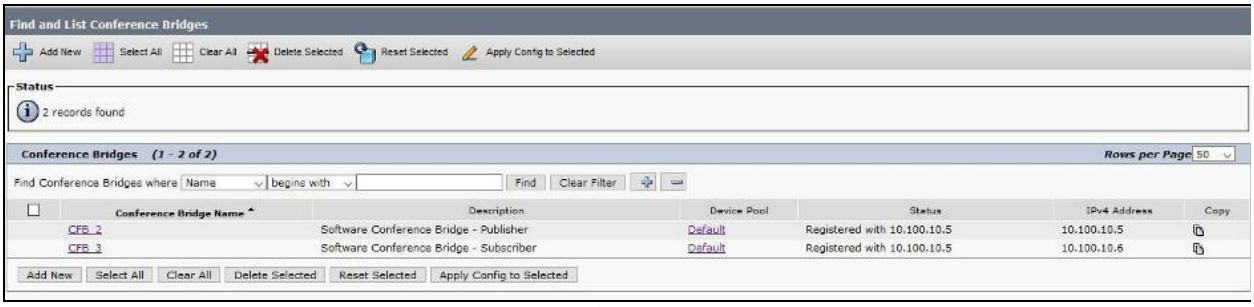


Figure 261: Conference Bridge window

Hardware Conference Bridge

Hardware Conferences Bridges requires dedicated hardware to provide and host this conference. Usually, it is a Cisco Router with a dedicated memory

called Voice Digital Signal Processor (DSP) like Cisco PVDM2 or PVDM3.

The hardware conference bridge allows the use of different codecs at the same time, like G.711, G.729, G.722, and iLBC.

Router configuration

To create a Hardware Conferences Bridge, we need to configure it on the router and also on CUCM. Follow a router configuration sample:

```
voice-card 0
dsp services dspfarm
!
sccp local GigabitEthernet0/0.10
sccp ccm 10.100.10.5 identifier 1 priority 1 version 7.0
sccp ccm 10.100.10.6 identifier 2 priority 2 version 7.0
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
associate ccm 2 priority 2
associate profile 1 register R1-CONFERENCE
!
dspfarm profile 1 conference
codec ilbc
codec g722-64
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec g729r8
codec g729br8
maximum conference-participants 8
maximum sessions 2
associate application SCCP
no shutdown
```

As you can see, to configure the Hardware Conferences Bridge we need to enable the SCCP protocol and configure it. Follow these commands explained:

Command	Usage
voice-card 0	enter the configuration mode for your DSP module
dsp services dspfarm	enable the dsp modules to be used with the

	dspfarm
sccp local GigabitEthernet0/0.10	select which router interface will be used in the SCCP process as a source IP Address
sccp ccm 10.100.10.5 identifier 1 priority 1 version 7.0	identifies the CUCM IP Address, his priority and the CUCM version 7 or superior
sccp ccm 10.100.10.6 identifier 2 priority 2 version 7.0	identifies the CUCM secondary server, priority and version
sccp	enables the sccp process
sccp ccm group 1	creates a sccp group
associate ccm 1 priority 1	associates the CUCM with identifier 1 with this group, and give its priority 1 (will be the first used to register the hardware conference)
associate ccm 2 priority 2	associates the CUCM with identifier 2 with this group, and give its priority 2 (will be the secondary used to register the hardware conference)
associate profile 1 register R1-CONFERENCE	associates the profile 1 (not created yet) with this group and name it as “R1-CONFERENCE”
dspfarm profile 1 conference	creates the profile 1 as a conference resource
codec (codec-name)	these various “codec” commands enable these codecs under this profile
maximum conference-participants 8	defines the maximum number of conference participants
maximum sessions 2	how many conference will be available
associate application SCCP	associate this profile with the SCCP process
no shutdown	enable this conference profile

Figure 40: Hardware Conferences Bridge commands explained

The number of conference participants and sessions depends on your PVDM model. If you try to create it and receive an error, maybe you need to decrease the number of sessions or participants.

These commands are used to create an audio conference bridge. If you want to create a video conference bridge, the commands are very similar, only changing the profile configuration:

```
dspfarm profile 1 conference video homogeneous
codec ilbc
codec g722-64
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec g729r8
codec g729br8
codec h264 cif frame-rate 30 bitrate 320kbps
maximum conference-participants 8
maximum sessions 2
associate application SCCP
no shutdown
```

CUCM configuration

Now we need to configure the CUCM part. Go to menu “Media Resources > Conference Bridge > Add New; select “Cisco IOS Enhanced Conference Bridge”.

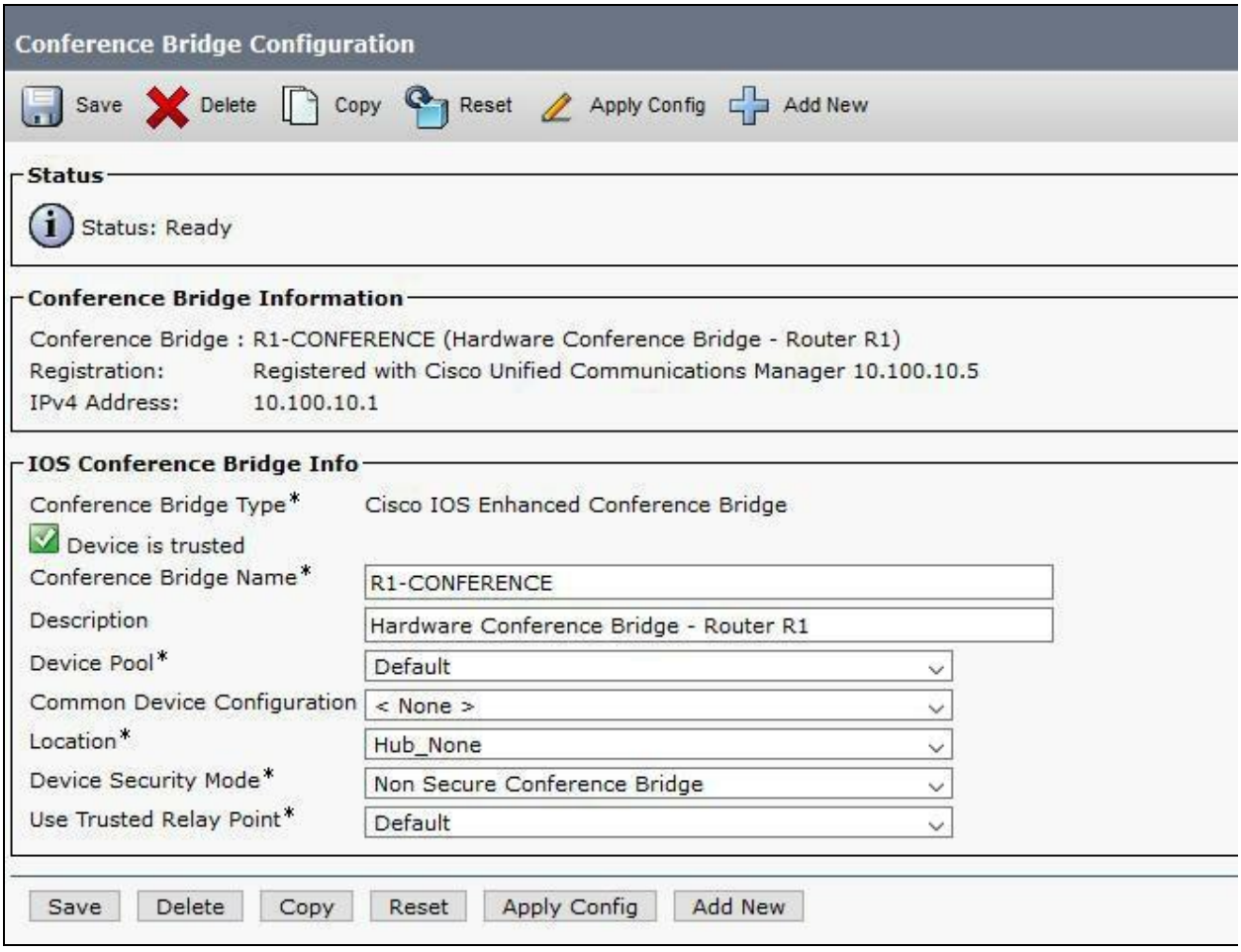


Figure 262: Conference Bridge configuration window

The most important step here is to match the name under “Conference Bridge Name” with the command “associate profile 1 register”; in this example, I used “R1-CONFERENCE” but you can use anything you want, just make sure that both names are the same.

If the status of the conference is “Rejected”, try to Reset it on CUCM by clicking “Reset” and/or go to the router and reset the SCCP process with the commands:

```
no sccp
sccp
```

Now you can see you Hardware and Software Conference Bridges on the same screen. As you can see, you can delete your Hardware Conference Bridges, but not the Software Conference Bridge.

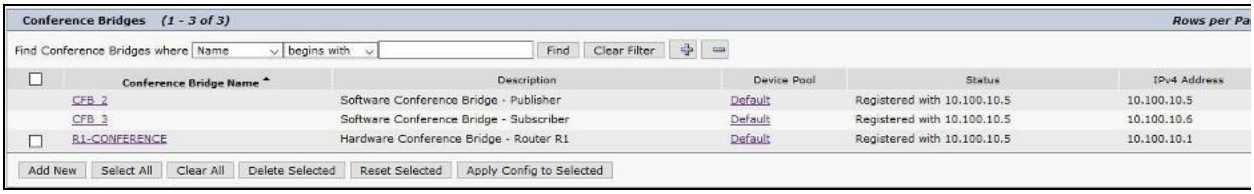


Figure 263: Conference Bridges window

Transcoder

A transcoder is a process to connect calls with different codecs. You need dedicated hardware (router) to do it, as there is no Software Transcoder on CUCM.

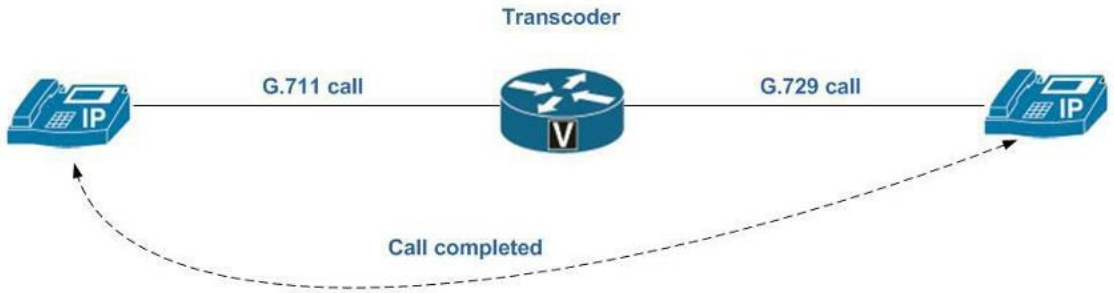


Figure 264: Transcoder

Router configuration

The configuration is very similar to the configuration we did to create the Hardware Conference Bridge above, and we will complement it. On the router, you type the following commands:

```
sccp ccm group 1
associate profile 2 register R1-TRANSCODER
!
dspfarm profile 2 transcode universal
codec g729r8
 codec g722-64
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
maximum sessions 5
associate application SCCP
no shutdown
```

We are using the same SCCP CCM Group to associate the secondary profile "R1-TRANSCODER". Then, we create this profile with the command dspfarm profile 2 transcode universal, selected the codecs, maximum sessions, associate it to CUCM and did a "no shutdown". As you can see, the commands are the same as we used to create our Hardware Conference Bridge.

CUCM configuration

Now, in CUCM, go to menu "Media Resources > Transcoder > Add New", select "Cisco IOS Enhanced Media Termination Point" and fill the information necessary:

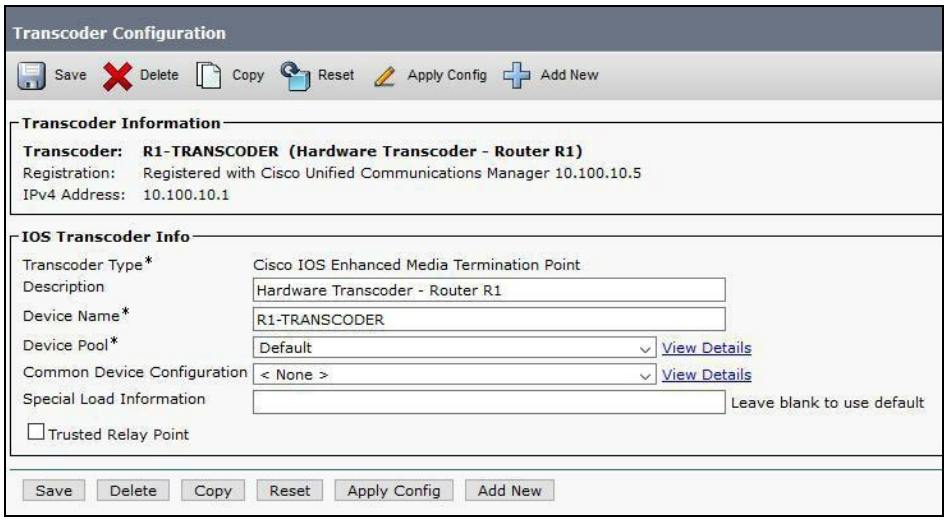


Figure 265: Transcoder

Again, the most important aspect here is to match exactly the "Device Name" with the "associate profile 2 register" command on the router. Click "Reset" and do a "no sccp / sccp" in the router if necessary to register it.

Music on Hold

Music on Hold is a service that allows the CUCM to send audio streams to the user when a call is on hold. Usually is something like a corporate announcement. There are two situations for music on hold:

Hold	When is used
User Hold	Activated when the user receives a call and press the "Hold" button.
Network Hold	Activated via transfer hold, conference hold, and call park hold.

Table 41: User Hold x Network Hold differences

So you can configure both cases with the same MoH or with different MoH audios.

If you want to test and use the default MoH audio that comes with CUCM, go to "Device > Phone" and look for "User Hold MOH Audio Source" and "Network Hold MOH Audio Source", select the available "1-SampleAudioSource", save and reset the phone.

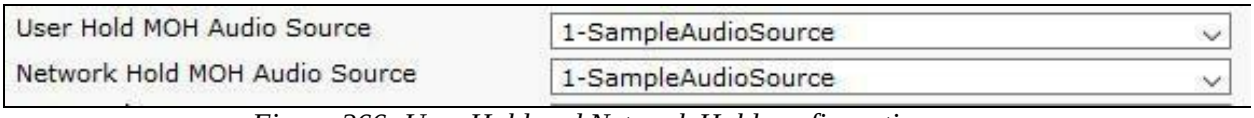


Figure 266: User Hold and Network Hold configuration menu

It is enough to have the phone using this default music on hold stream. You can also apply this via BULK to a group of phones, or to all your phones at the same (check Chapter 15, Bulk Administration).

To create your personalized audio, the process is not hard, but it requires some steps. The most complicated is to prepare the audio in the correct format for CUCM to use it. CUCM does not accept MP3 files, only WAV files; but even the WAV file requires some adjusts:

- Format: WAV
- Encoding: 8-bit CCITT u-Law or a-Law (stereo/mono)
- Average Data Rate: 8 kbps
- Sample Rates: 8 kHz, 16 kHz, 32 kHz, 48 kHz
- Audio Sample Size: 16-bit PCM (stereo/mono)
- Channels: 1 (Mono)

You can prepare this file with any audio editing software you have. If you want some examples, in this book Appendix I show you three different ways to do it: using the free software “Audacity”, the command “ffmpeg” available to Mac OS or Linux and with some websites online.

Media Resource Group

Now that you have some Media Resources created, you need to create a Media Resource Group (MRG). MRG is the location where you will aggregate all your media resources like Conference Bridge, Transcoder and Music on Hold.
Go to menu “Media Resources > Media Resources Group > Add New”; add here all Media Resources you want to provide to the users.

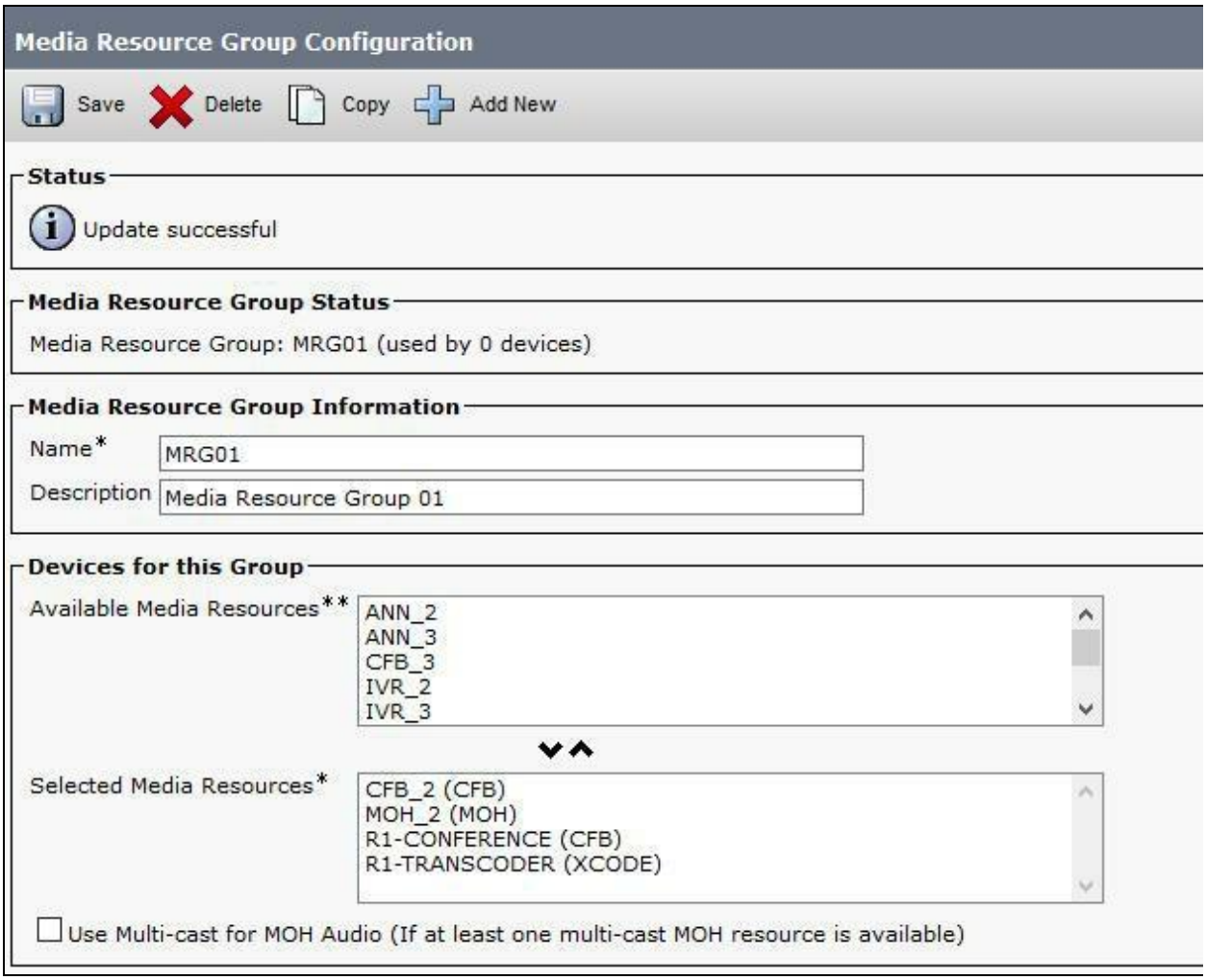


Figure 267: Media Resource Group configuration window

Save it. The next part is to create the Media Resource Group List (MRGL).

Media Resource Group List

Media Resource Group List is the location where you will configure your Media Resource Groups. Media Resource Group List is also the final configuration that you will apply to your devices, like Phones, Gateways, Trunks, and others.
For example, a typical configuration is:

- The Cisco Phones have a Media Resource Group List;
- This Media Resource Group List has 1 or more Media Resource Groups;
- This Media Resource Groups have a Conference Bridge, a Transcoder and a Music on Hold.

So you will not associate a Conference Bridge directly to the user phone; you will associate a Media Resource Group List.

To create it, go to menu “Media Resources > Media Resources Group List > Add New”, then, add the MRG you have created.

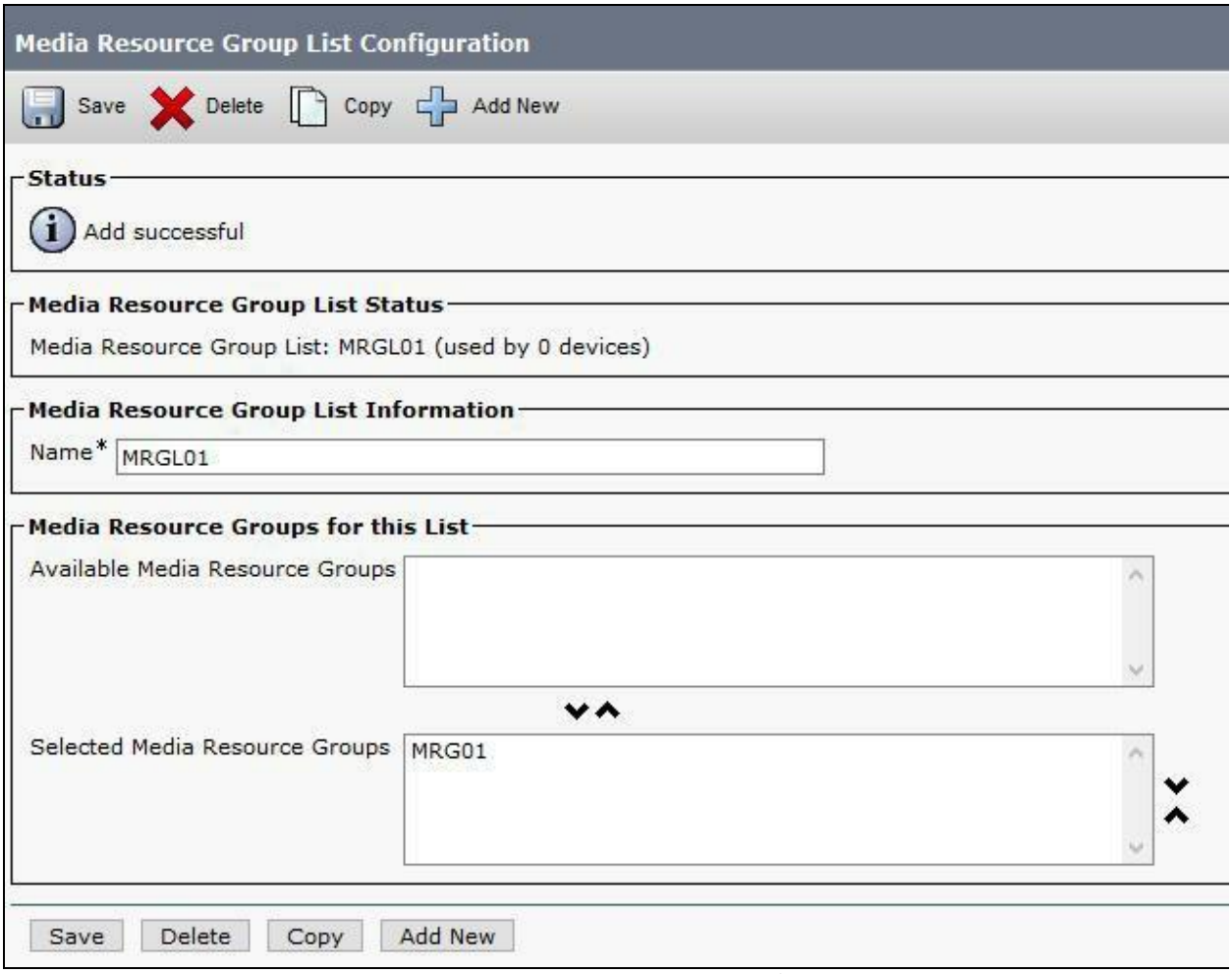


Figure 268: Media Resource Group List configuration window

Finally, you need to add the MRGL to the phones, gateways and other devices you want to enable to access these media resources:



Figure 269: Media Resource Group List configuration

Save and reset the Phones or devices to apply it.

CHAPTER 14 - FEATURES

How to implement advanced features in CUCM

Pickup group

Pickup groups are a group of phones that can pick up calls from other phones. Usually, this feature is configured in a group of devices that are physically near each other, so the user can hear that a college phone is ringing and pick up that call on his phone.

To configure it, go to: “Call Routing > Call Pickup Group > Add New”.

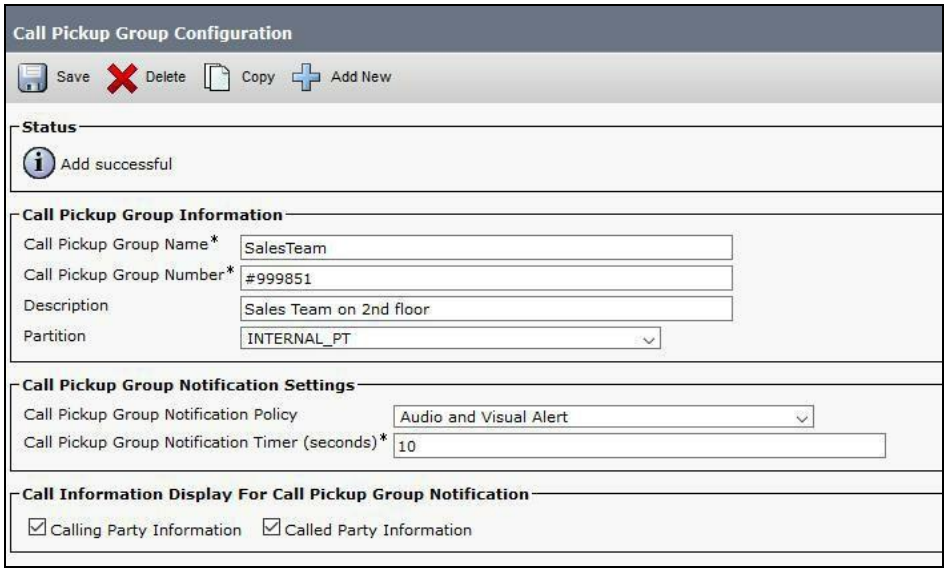


Figure 270: Call Pickup Group configuration window

The information you need to fill:

Field	Description	Example
Call Pickup Group Name	A name for the Group	SalesTeam
Call Pickup Group Number	An internal identifier on CUCM	#999851
Description	A short description for the group	Sales Team on 2nd floor
Partition	The partition where this group belongs	INTERNAL_PT
Call Pickup Group Notification Policy	How will the users be notified that there is a call available to pick up from this group	Audio and Visual Alert (some users prefer only Visual Alert)
Call Pickup Group Notification Timer (seconds)	How many seconds the call will ring to the original called user before being available to the Pick Up Group	10 seconds (at about 3 rings)
Calling Party Information	Select if you want to display the Calling Party Information	-
Called Party Information	Select if you want to display the Called Party Information	-

Table 42: Call Pickup Group options

Create these configs and test it with your users to find the best option for them. After you create it, go to the user line “Device > Phone > Find your user > open his Directory Number and select it under Call Pickup Group” and apply this Pickup Group to the user line.

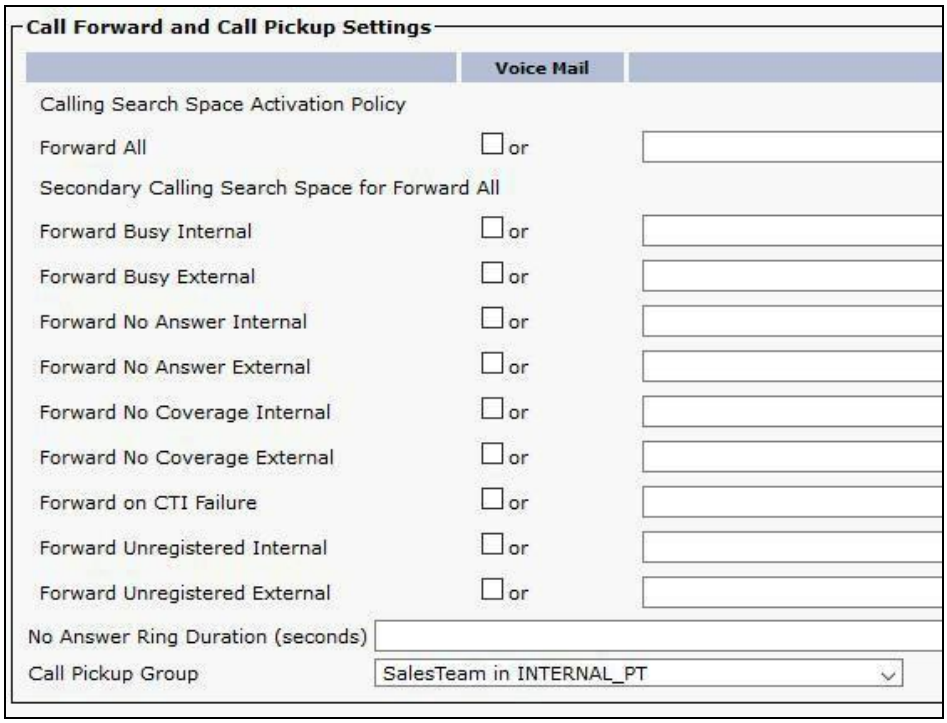


Figure 271: Call Pickup Group selection under Directory Number

Hunt Group

Hunt Group is configured when you want to have a main number to reach a group of users, like a department in your company. When a call is placed to this number, this call can be distributed in the following ways:

Distribution Algorithm	Description
Top Down	The call will be routed to the first user, then to the second, third, etc. If the first and the second users are in a call, and the first user finish his call, the next incoming call go to him, not to the third users. It is useful to implement a escalation calling process.
Circular	The call goes circulating to all users (First, Second, Third, Fourth, until the end, then First, etc.).
Longest Time Idle	The CUCM will send the call the starting from the longest idle member to the least idle member of a line group.
Broadcast	CUCM will send the call to all idle or available members of a line group at the same time; all phones will ring together. Useful for emergency teams.

Table 43: Hunt Group configuration options

Very similar with what we have with the Route Pattern configuration, we

need to create a Line Group, a Hunt List and a Hunt Pilot to complete our configuration.

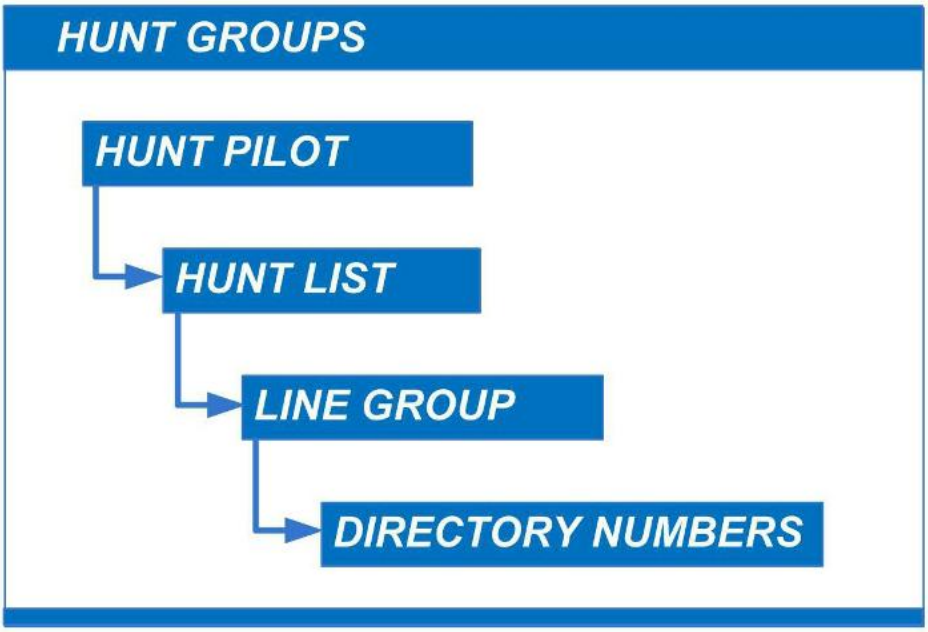


Figure 272: Hunt Group, Hunt List and Line Group

Creating a Line Group

Go to menu “Call Routing > Route/Hunt > Line Group > Add New” and fill the following information:

Information	Description
Line Group Name	The name for this Line Group.
RNA Reversion Timeout	How many seconds will a call ring on one phone before going to other or taking the next action.
Distribution Algorithm	What should be the distribution algorithm for this group.
Hunt Options	What should be the action in No Answer, Busy or Not Available scenarios.
Line Group Member Information	Where you will select the extensions belonging to this Line Group.

Table 44: Line Group configuration options

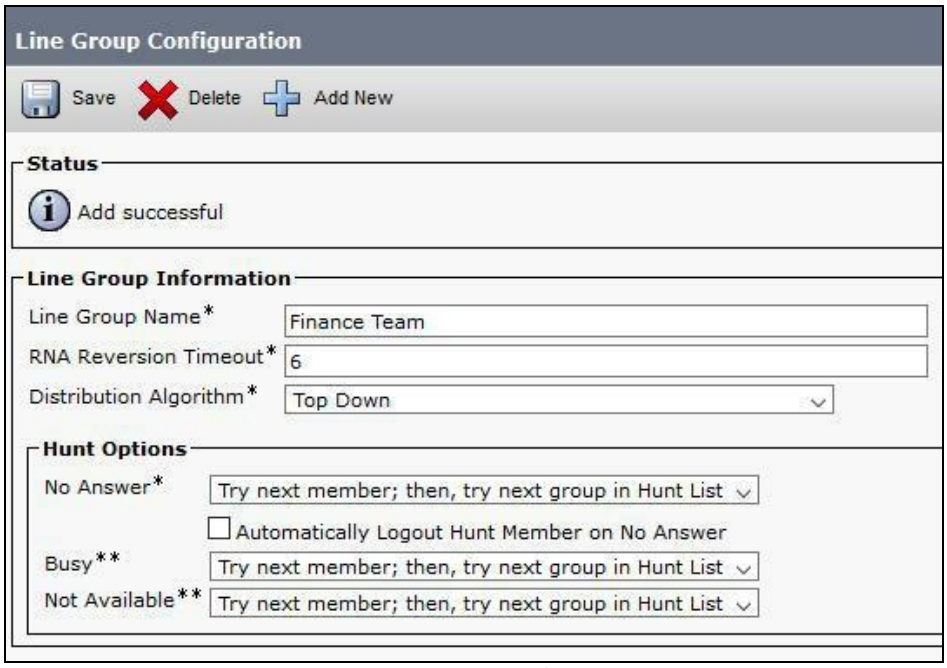


Figure 273: Line Group configuration options

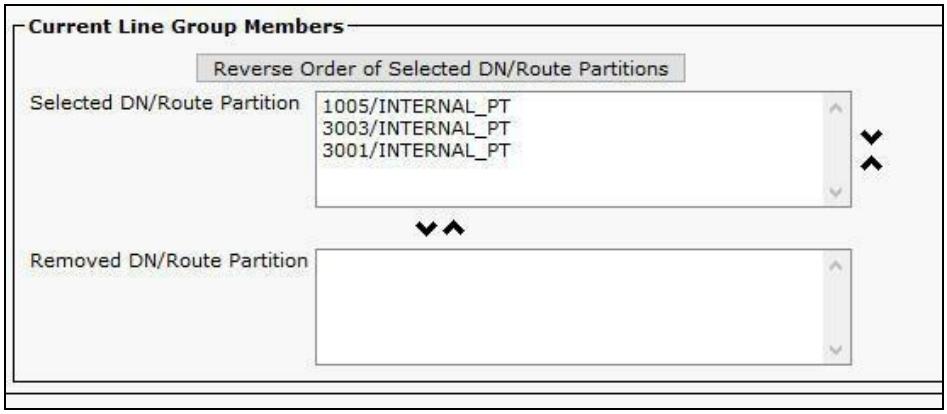


Figure 274: Line Group configuration options

In this example, as I have created this Line Group “Finance Team” with the Distribution Algorithm “Top Down”, the call will ring the following order:

- 1005
- 3003 (if 1005 is busy)
- 3001 (if 1005 and 3003 are busy)

Also, the RNA Reversion Timeout is set to 6 seconds. As a regular ring can take at about 3 seconds, this is close to 2 rings between each call transfer.

Creating a Hunt List

Now, to create a Hunt List, go to menu “Call Routing > Route/Hunt > Hunt List > Add New”. Give it a name, a description (optional) and associate it with the Line Group you had created.

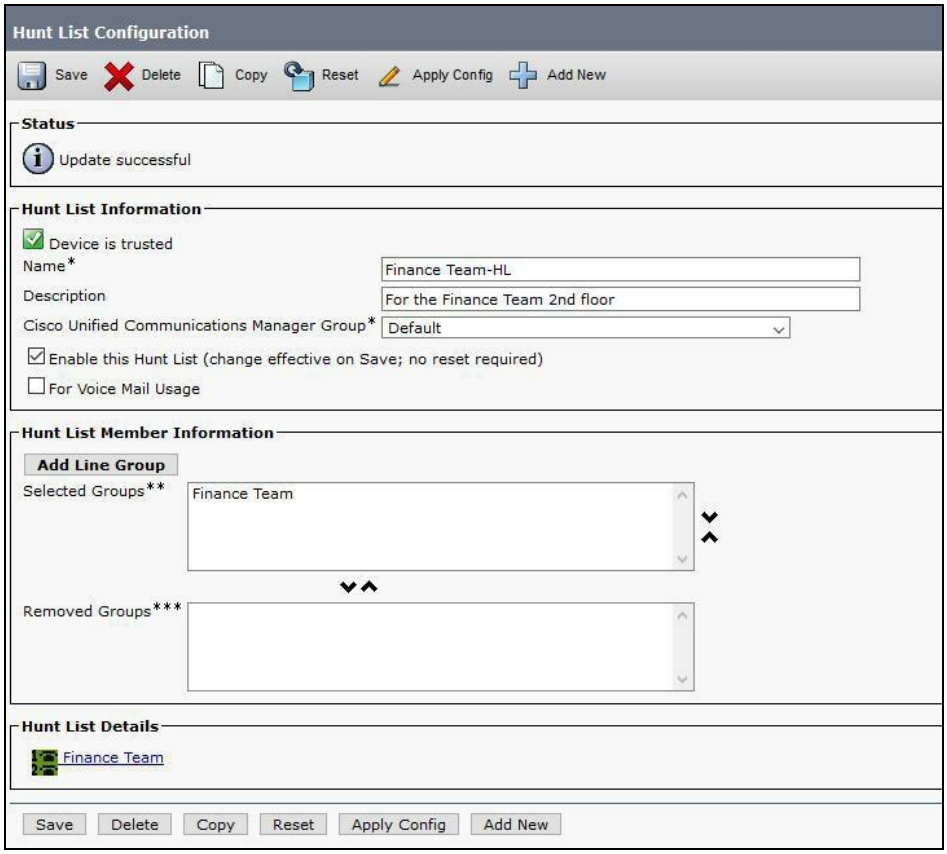


Figure 275: Hunt List configuration window

Save it and Reset it.

Creating a Hunt Pilot

The last part is to create the pilot for this Hunt Group. The pilot is the number users will call to reach this group. Go to menu “Call Routing > Route/Hunt > Hunt Pilot > Add New”. Let’s see the main options to configure here:

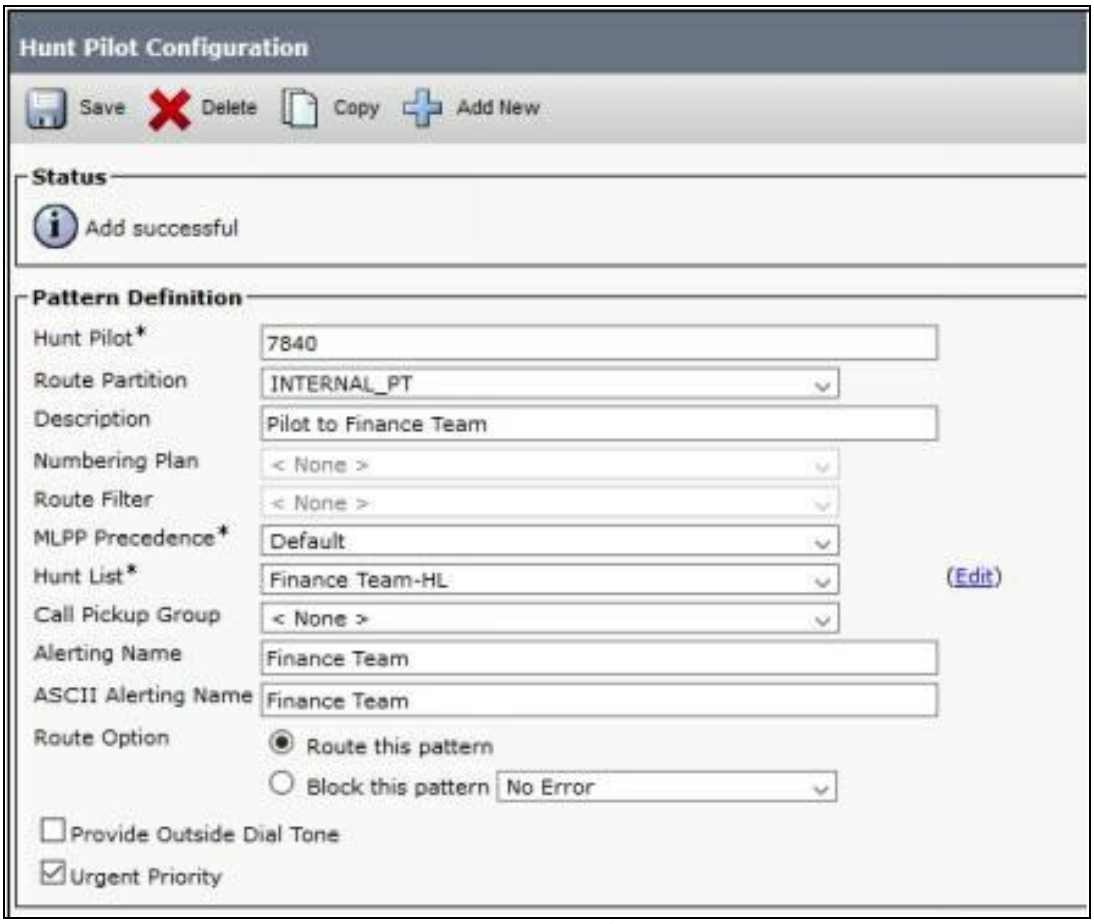


Figure 276: Hunt Pilot configuration window

Option	Description
Hunt Pilot	The Hunt Pilot Number.
Route Partition	The Partition where this number should belong.
Description	A description for this Hunt Pilot (Optional).
Hunt List	The Hunt List associated with this Hunt Pilot. Select the List you have created.
Call Pickup Group	Choose the number that can be dialed to answer calls to this directory number (in the specified partition). This allows users that do not belong to this Hunt Pilot to Pickup these calls.
Alerting Name	The name to be displayed when calling this name.
ASCII Alerting Name	Same as Alerting Name, but to old phone models (ASCII characters only).

Route Option: Route this pattern	The default option is to enable this Hunt Pilot and route these calls.
Route Option: Block this pattern	You can temporarily block this Hunt Pilot by selecting this. Also, choose what error will users dialing this Hunt Pilot hear while it is blocked.
Provide Outside Dial Tone	Select if users dialing this numbers should hear an Outside Dial Tone (not recommended, disable it).
Urgent Priority	If this call should be routed as soon as the numbers are matched. If there are no overlapping numbers or patterns, enable it so that calls can be routed faster.
Forward Hunt No Answer	Select what to do with these calls in “No Answer” situations.
Forward Hunt Busy	Select what to do with these calls in “Busy” situations.
Queue Calls	You can queue the calls from this Hunt Pilot. This is an interesting option, as we can use it as a very basic call center, but with no advanced reports or controls. We can keep our callers on hold listening to a music/audio until we have an user available to transfer their call.
Network Hold MOH Source & Announcements	What audio should our callers hear while in the queue waiting for their transfer.
Maximum Number of Callers Allowed in Queue	How many users to be allowed in this queue.

Table 45: Hunt Pilot configuration options

There are more options available under “Queue Calls”, but they are very intuitive:

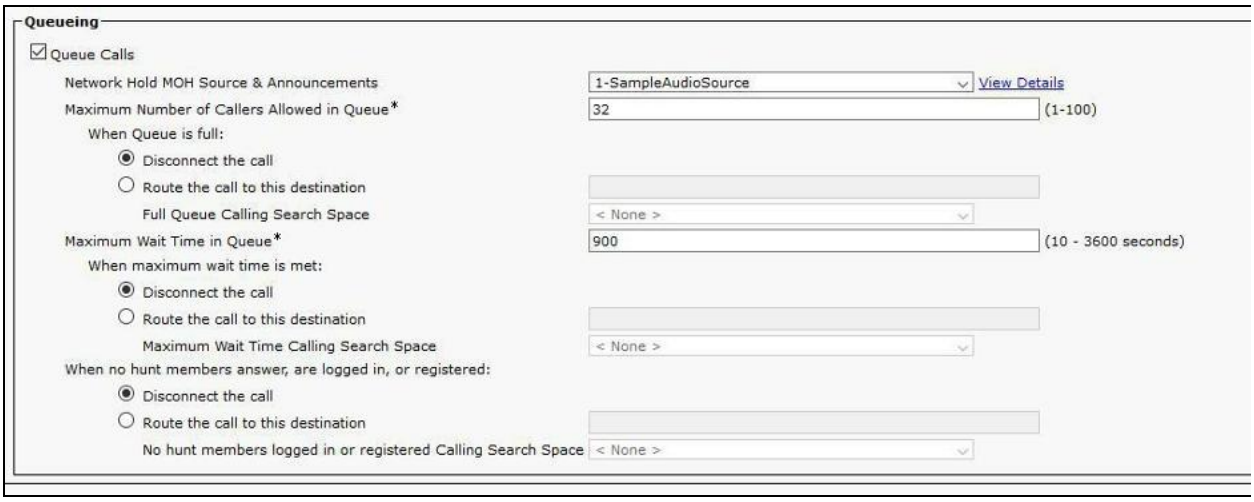


Figure 277: Hunt Pilot queue calls options

This queueing option is very good. It is available since CUCM 10.x, and it can help us to implement very basic, but functional Hunt Pilots to internal teams like IT Support Team, Finance Team, Sales Team, and others. Besides it is not an entirely Call Center, it works very well to a team that only need basic call routing and queueing.

Meet-me number

Meet-me numbers are a very basic conference available under CUCM. It is an Audio Conference Room that should be opened by the user. When opened, users can dial this number and participate in this conference.
The main problem with Meet-me is that it does not allow the conference to have a password. So anyone who knows the conference number can call in and participate in this conference if his Calling Search Space can reach the Meet-me Number Partition.

To create a Meet-me conference, go to menu “Call Routing > Meet-me Number/Pattern > Add New”. You can create multiple conference numbers by using brackets and dash; example: 500[0-9] will create 10 Meet-me Conference Rooms, from 5000 to 5009.

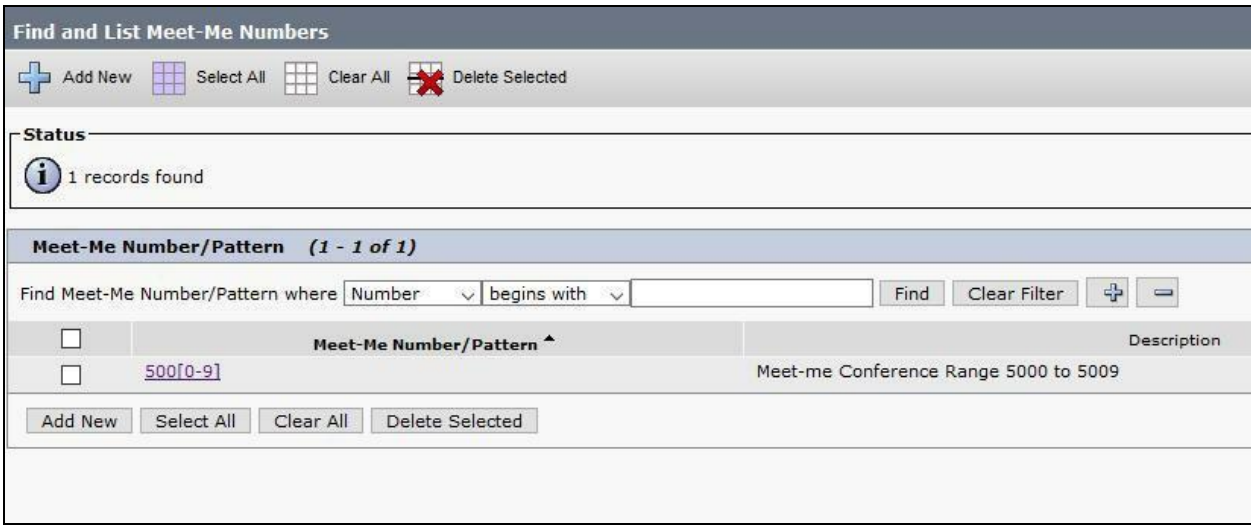


Figure 278: Meet-me number

To access these Meet-me Conferences, the first participant needs to need to press “MeetMe” softkey on the Phone and dial the Meet-me room number. Then, the room is “opened”, and the following participants only need to dial the Meet-me Number to join it.

As soon as the last participant disconnect, the Meet-me room is closed, and this process should be repeated to open it again.

Conference Now

The Conference Now is a very cool feature available starting on CUCM 11. It solves the main problem with Meet-me Conference, as it has a password. The process to create it is:

Creating a Conference Now

Step 1:Configure the Conference Now;

Go to menu “Call Routing > Conference Now” and edit the Conference Now IVR Directory Number, Route Partition, Description, and other options:

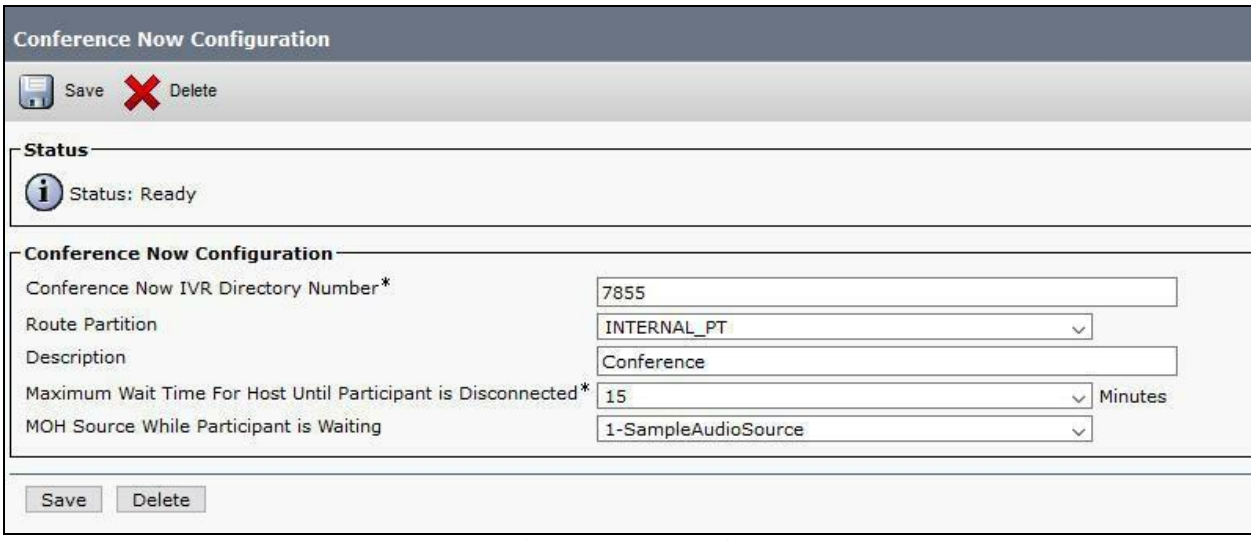


Figure 279: Conference Now configuration window

The "Conference Now IVR Directory Number" is the main number where all users should dial to reach the Conference Now. Calling this number, users will be prompted to select which Conference Now room they want to access, and prompted for the room password.
Type the number and information you want to use and save it.

Step 2:Create a user;

Go to User Management > Add New; fill the information necessary to create a user. Create a PIN (number), as it will be used to open the Conference Now as the host of the conference. As an example, set the PIN to 1234.

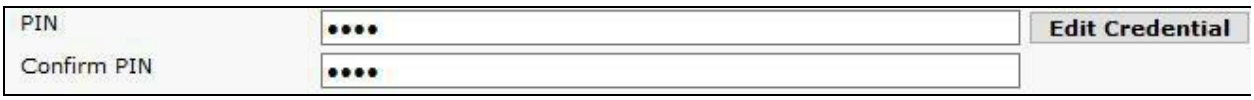


Figure 280: PIN number under End User page

Step 3:Associate a Phone and a Number to this user;

Under the End User page, search for "Device Information / Controlled Devices". We need to associate the End User with his Phone, where we can find his Extension Number.

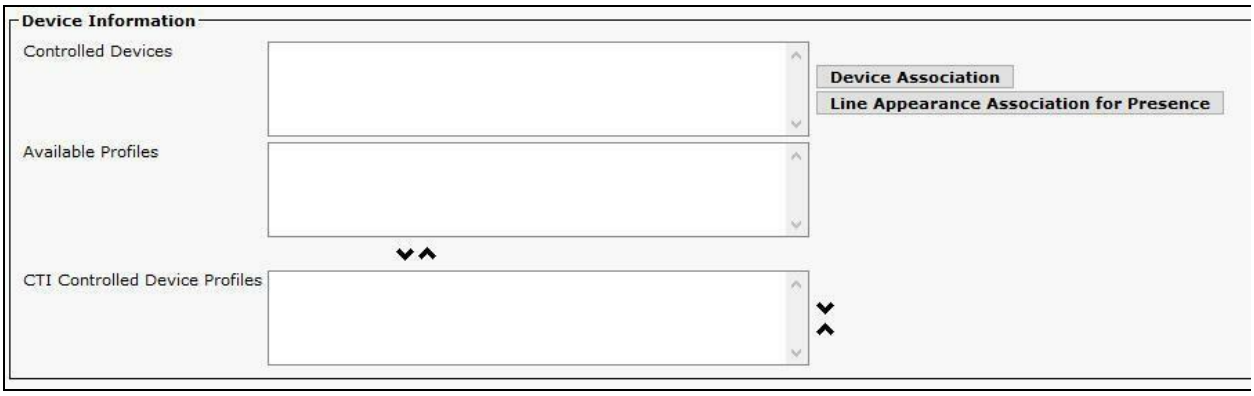


Figure 281: Controlled Device under End User page

Click “Device Association”. Then, search for the user phone. Select it, then press “Save Selected/Changes”.

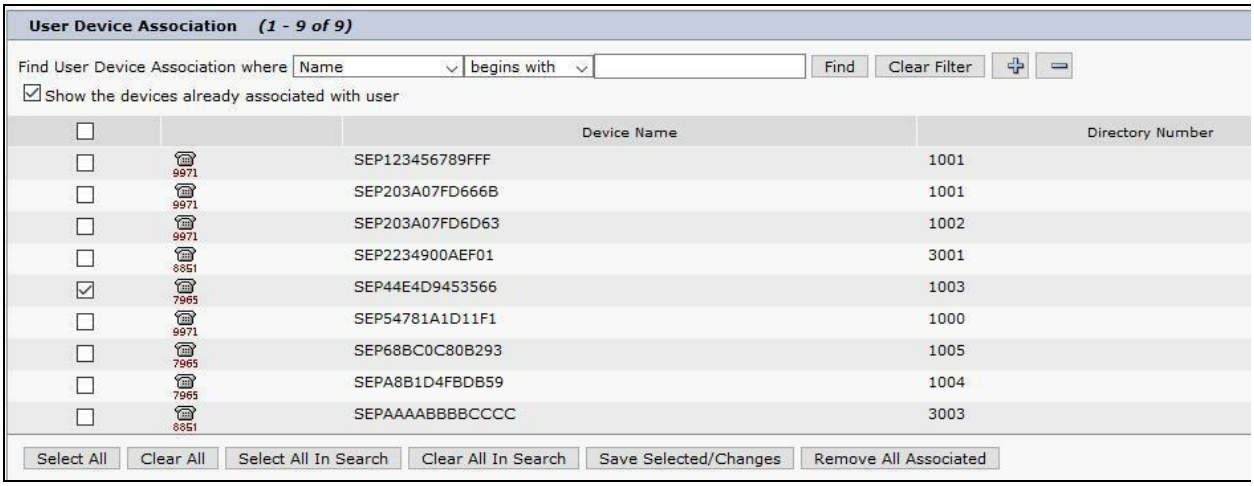


Figure 282: Controlled Device under End User page

On the right-top corner, select “Related Links: Back to User / Go” to return to the End User Page.

Now, search for “Directory Number Associations / Primary Extension”, select the End User Primary Extention associated with Conference Now and Save it.

Step 4: Enable “Conference Now” for the user

Scroll down until the end of the End User page and enable “Enable End User to Host Conference Now”. Create an “Attendees Access Code”, which will be the password to access his Conference.

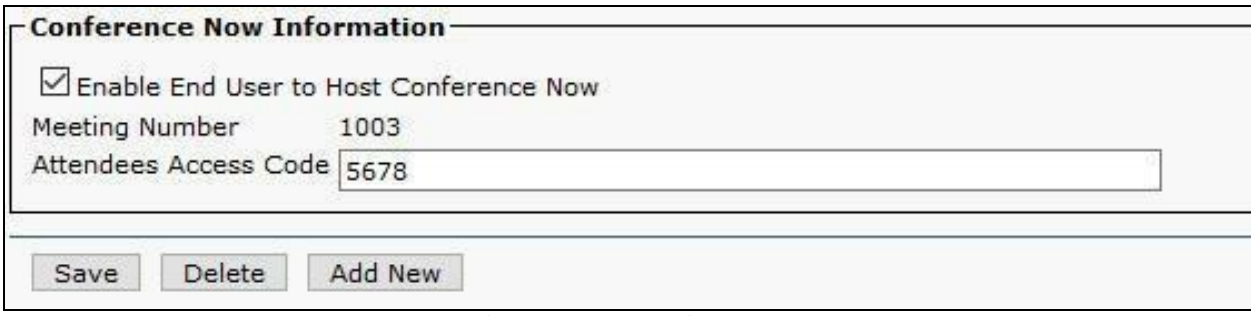


Figure 283: Conference Now config under End User page

The “Conference Now” configuration is completed.
Only the Conference Host has the password to open it. He can provide this password to other users if he wants, but someone needs to open the conference with this password.

In this example we have created, the steps are:

To open the Conference Now (as Host)

- Dial the Conference Now main number 7855;
- When asked for Meeting Number, type 1003 and press #;
- When asked “If you are Meeting Host”, press the user PIN number (1234 as our example) and press #.

To access the Conference Now (as regular user)

- Dial the Conference Now main number 7855;
- When asked for Meeting Number, type 1003 and press #;
- When asked for the “Attendees Access Code”, press the code (5678 as our example) and press #.

When all participants leave the Conference Now, it will be closed and should be opened again.

Extension Mobility

Extension Mobility is a feature that allows a user to login to a Phone and has his Device Profile loaded in this Phone.

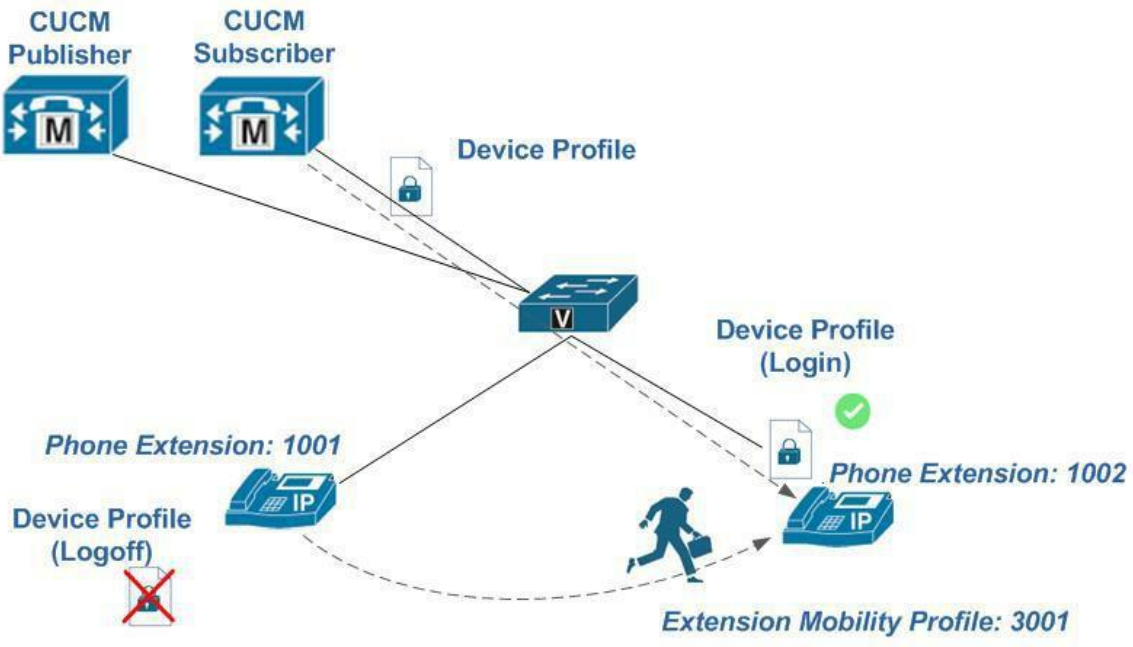


Figure 284: Extension Mobility topology

With this, the user can log in to each phone available and have his extension wherever he is going, like a conference room or even another company location/site. In the picture above, the user has his Extension 3001 enabled in his Device Profile so he can log in on Phone with extension 1002, and this process will override configuration, automatically configuring this phone with extension 3001.

To configure this, the steps are:

Step 1:Verify if the Extension Mobility Service is enabled;

Go to the Cisco Unified Serviceability page (https://CUCM-IP-ADDRESS/ccmservice/ or via right-top menu “Navigation > Cisco Unified Serviceability > Go”). Open the menu “Tools > Service Activation” and select your CUCM Publisher node; check if the service “Cisco Extension Mobility” is activated; if not, enable and save it.

Step 2:Create the IP Phone Service (URL);

Go back to CUCM Administration Page, go to menu “Device > Device Settings > Phone Services > Add New”. Here, type the service name as you want to users to see it in the Phone Display and the Service URL.

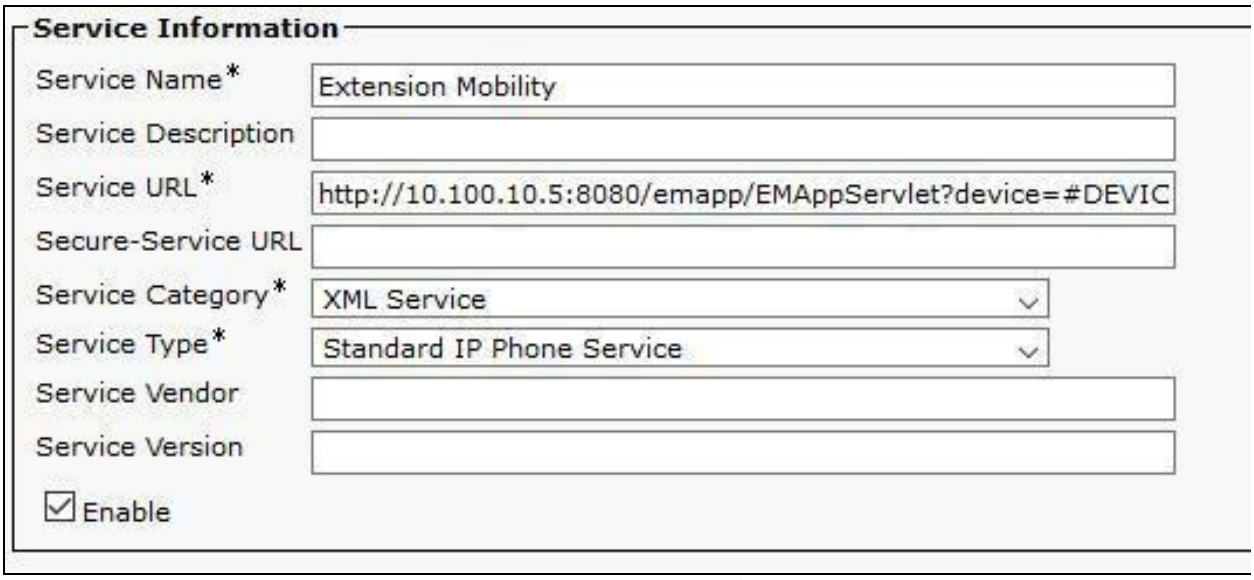


Figure 285: Extension Mobility configuration window

In our example the URL was:

http://10.100.10.5:8080/emapp/EMAppServlet?device=#DEVICENAME#

Enable it and Save it.

Step 3:Phone Services Subscribe;

To subscribe a phone to the Extension Mobility Service, go to menu “Device > Phone”, open the Phone you want to add it and in the top-right corner of the page, search for “Related Links”; select “Subscribe/Unsubscribe Services” and press “Go”.

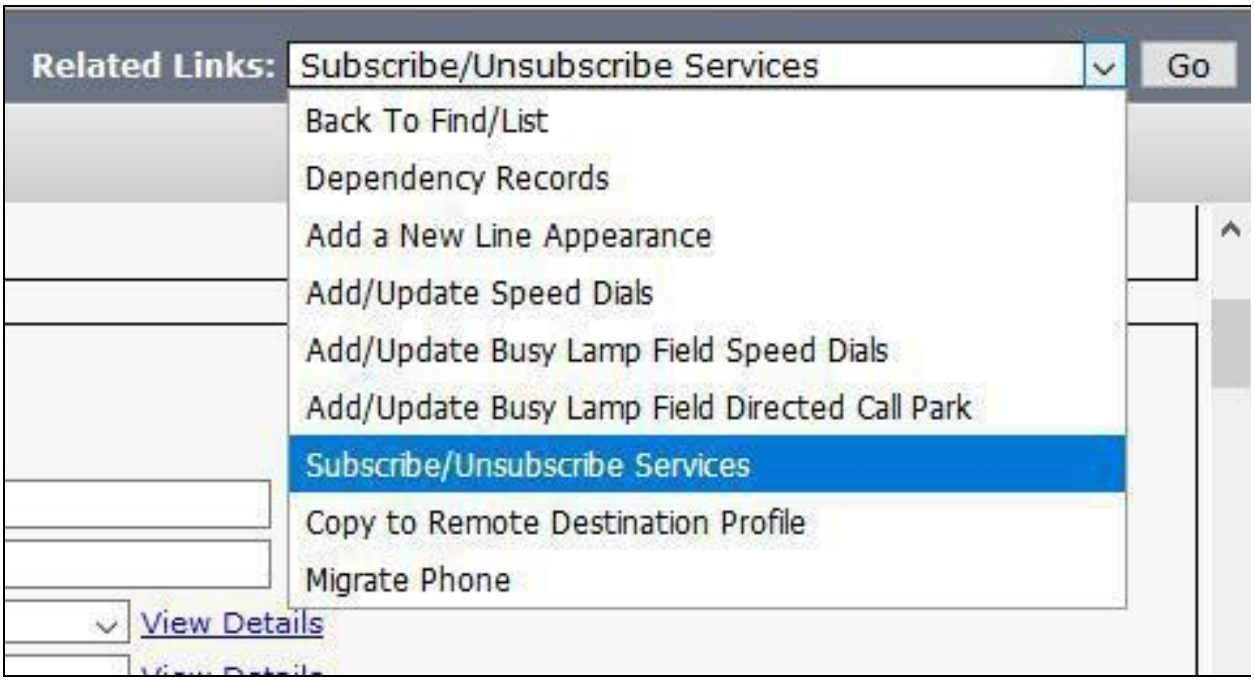


Figure 286: Extension Mobility subscription

A pop-up window will open, where you should select the service you have created; click “Next” and then “Subscribe”.

Step 4:Select "Enable Extension Mobility" on the phone; save and apply it.

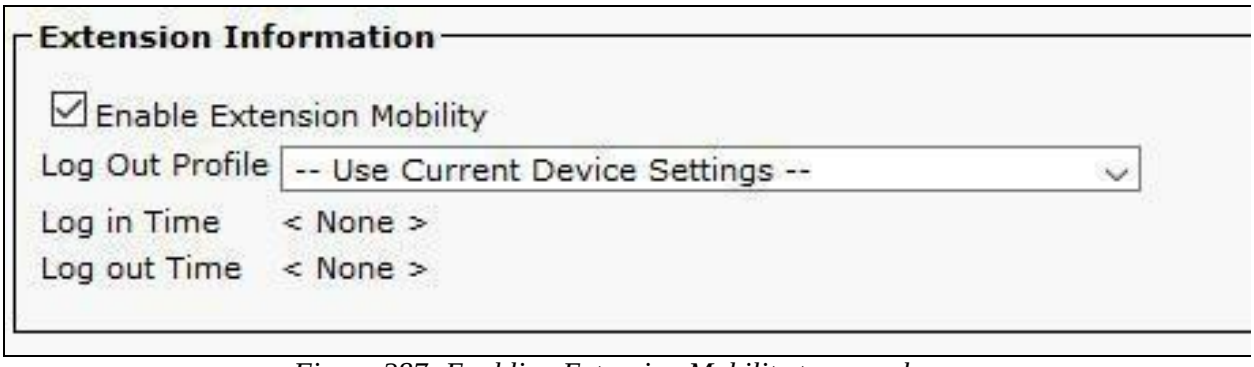


Figure 287: Enabling Extension Mobility to user phone

> **Note:** You can do steps 3 and 4 via BULK to all your phones - check Chapter 15 how to use BULK Administration Tool (BAT).

Step 5:Create the Device Profile for the Extension;

Go to menu “Device > Device Settings > Device Profile > Add New”; select the phone Model and the Device Protocol (if necessary); choose a Device Profile Name and Phone Button Template and save it;

After the save, you will be able to insert a Directory Number to this Profile on the top-left corner as you do on a regular phone. Apply the extension you want to use and save it.

You also need to Subscribe this Profile to Extension Mobility Service under “Related Links > Subscribe/Unsubscribe Services” as we did with our Phones. This is necessary because if the profile doesn’t have access to Extension Mobility Service, the user will be able to log in but not able to log out. Yes, this is strange, I agree.

Step 6:Associate a user with this profile;

With the Device Profile ready, select the user you want to associate with this profile. Go to “User Management > End User” and open the user; under “Extension Mobility”, you will see the profile you created in “Available Profiles”; select it and move it down to “Controlled Profiles” and save it.

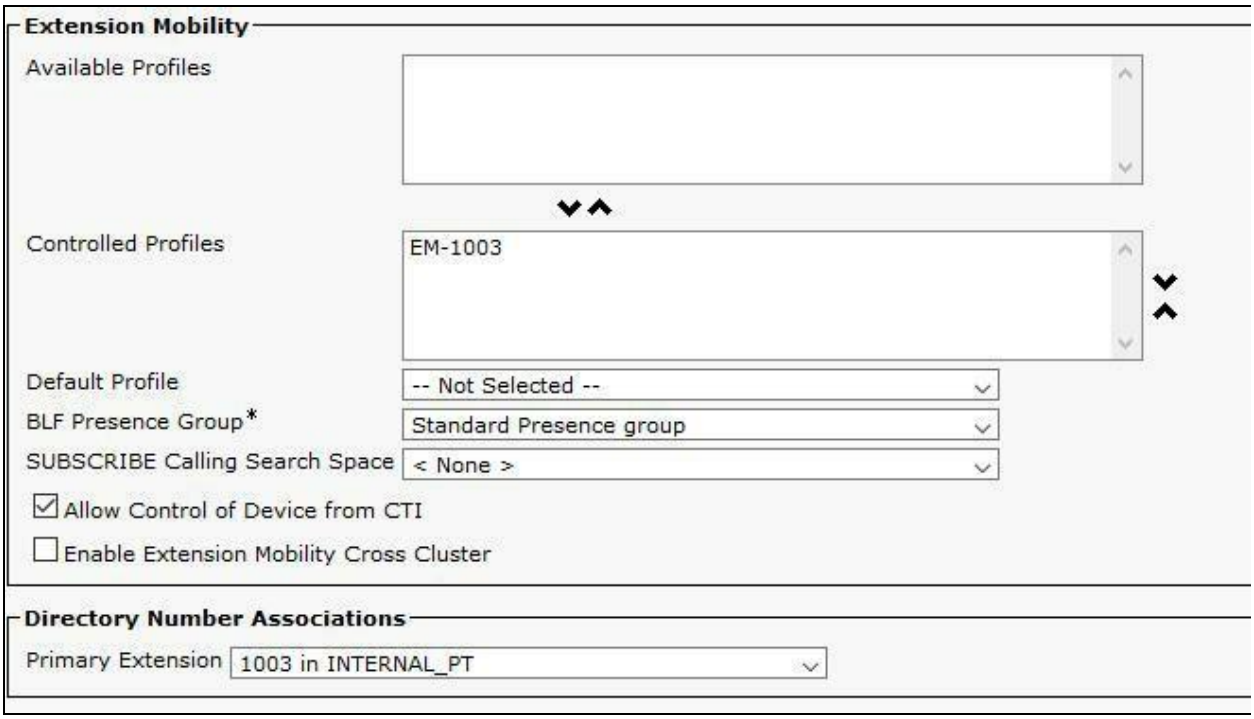


Figure 288: Extension Mobility configuration window

Also, check if under “Directory Number Associations” the correct Primary

Extension is selected.

Step 7:Change the user pin (optional);

If you don't know what's the user PIN, you can use this user page to reset it. If you know it, skip this step.

Step 8:Extension Mobility Login and Logout from the phones;

To log in and log out from the phones, they need to have the Extension Mobility enabled and subscribed (steps 3 and 4).

The process can be a little different from one phone to another. In Cisco Phones 79xx, you need to press the button "Services"  while in Cisco 88xx series, the button is .

Remote Destination

Remote Destination is used to forward calls to remote phones in certain situations. When a phone desk receives a call, it rings for some time, then it starts ringing in a second device at the same time, but keep ringing at first. So multiples phones keep ringing until the call is answered in one of these devices.

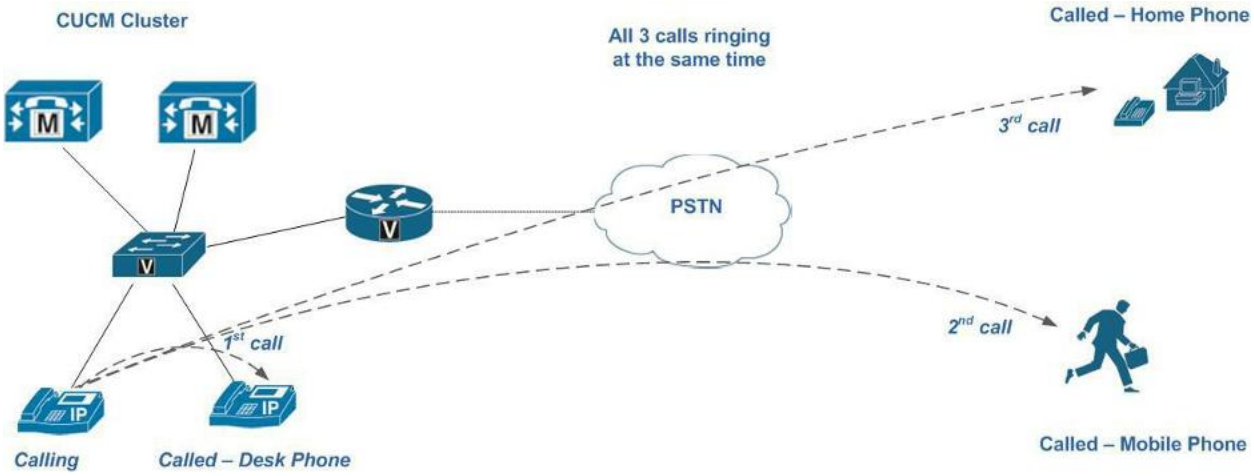


Figure 289: Remote Destination topology

As soon as the user answers the call at one of these devices, the others stop

ringing. This feature is useful also to be used in an escalation team because you can have a call ringing until someone answers it. Just need to verify if any voicemail system will answer it because you can configure the system to stop ringing in a specific device before this device forwards the call to the voicemail.

The Remote Destination must be a remote phone, like a user mobile phone or his home phone. It cannot be used to transfer to another internal extension.

Step 1:Enable Mobility to the user;

Go to User Management > End User > open the user > scroll down until you find “Mobility Information”, where you must select “Enable Mobility”.



Figure 290: Enabling Mobility under End User page

Step 2:Add New Remote Destination Profile;

Menu “Device > Device Settings > Remote Destination Profile > Add New”

Create the profile Name, select the user ID, Device Pool, Calling Search Space and Rerouting Calling Search Space - these CSS’s needs to have access to the PSTN.

Save it, and the option to associate a line will be available. Click on “Add a new DN”, associate the user extension and save it.

Then, on the right-top corner, click "Related Links: Configure Device" to return to the Remote Destination Profile Configuration. Now, click "Add a New Remote Destination" do add a remote destination, like a mobile phone for this user. Add the Destination Number and select the checkbox under “Line Association”.

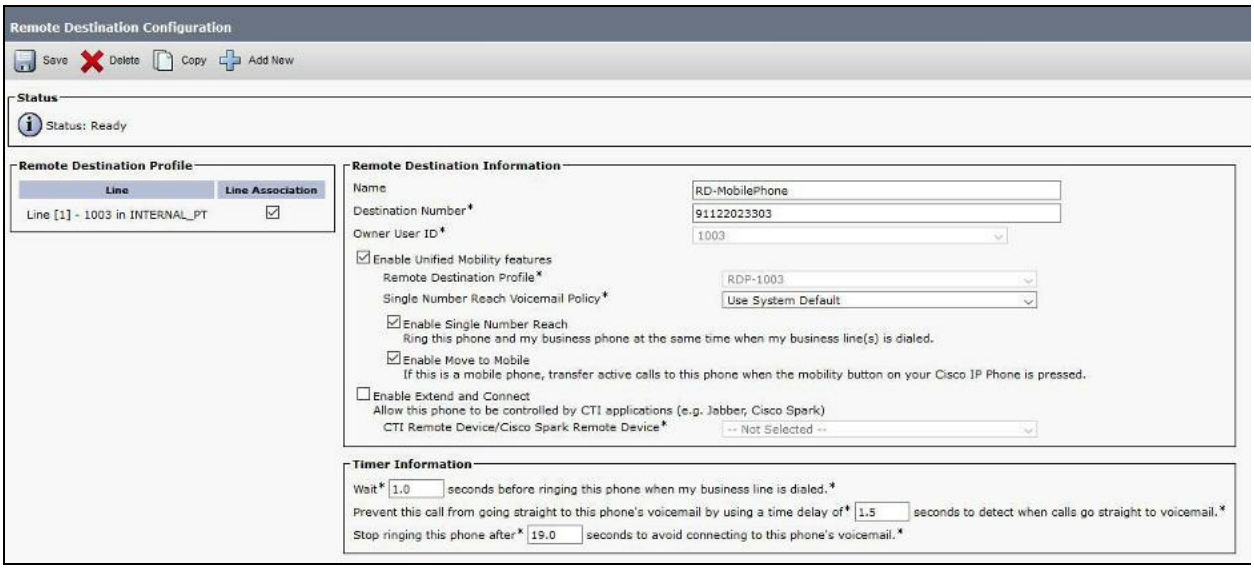


Figure 291: Remote Destination configuration window

Under "Timer Information", you can change how many time before this mobile phone is dialed, under "Wait ___ seconds before ringing this phone when my business line is dialed."

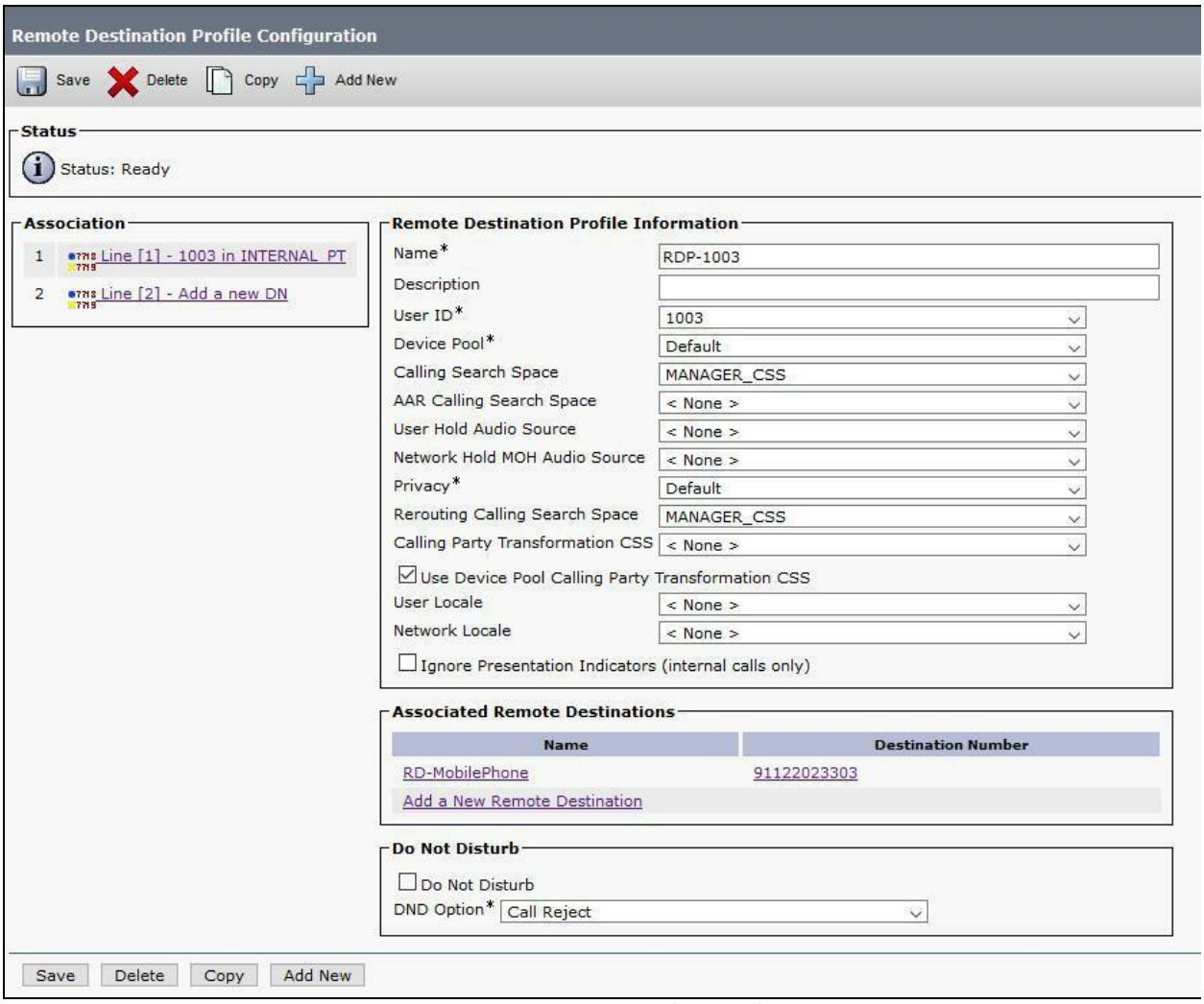


Figure 292: Remote Destination Profile configuration window

The final configuration will look like this. In my example, when I dial the extension 1003, after 1 second the call starts to be also sent to the remote extension 91122023303 (9 is the PSTN access code).

CHAPTER 15 - BULK ADMINISTRATION

How to edit phones and configurations massively

The change of a simple configuration like Device Pool to one Phone is very easy. However, to change it manually to hundreds of phones is definitively a more difficult task.

Bulk Administration Tool (BAT) is an application available at CUCM Publisher that performs bulk transactions. It lets you add, delete and modify a large number of similar devices and configurations like phones and their users. It automates the process and achieves faster massive operations.

In this Chapter, we will see some of the most commons tasks we can do using BULK. Please note that I will not cover all the possibilities available, but if you know how to do these basic tasks, you can go forward and try the advanced options available.

Update Phones using BULK

Updating a group of phones with similar configurations is the easiest and fastest operation available on BULK. You can search for the phones with similar characteristics such as Device Pool or Phone Model, and apply the same settings to all the phones at the same time.

To do so, go to menu Bulk Administration > Phones > Update Phones > Query:

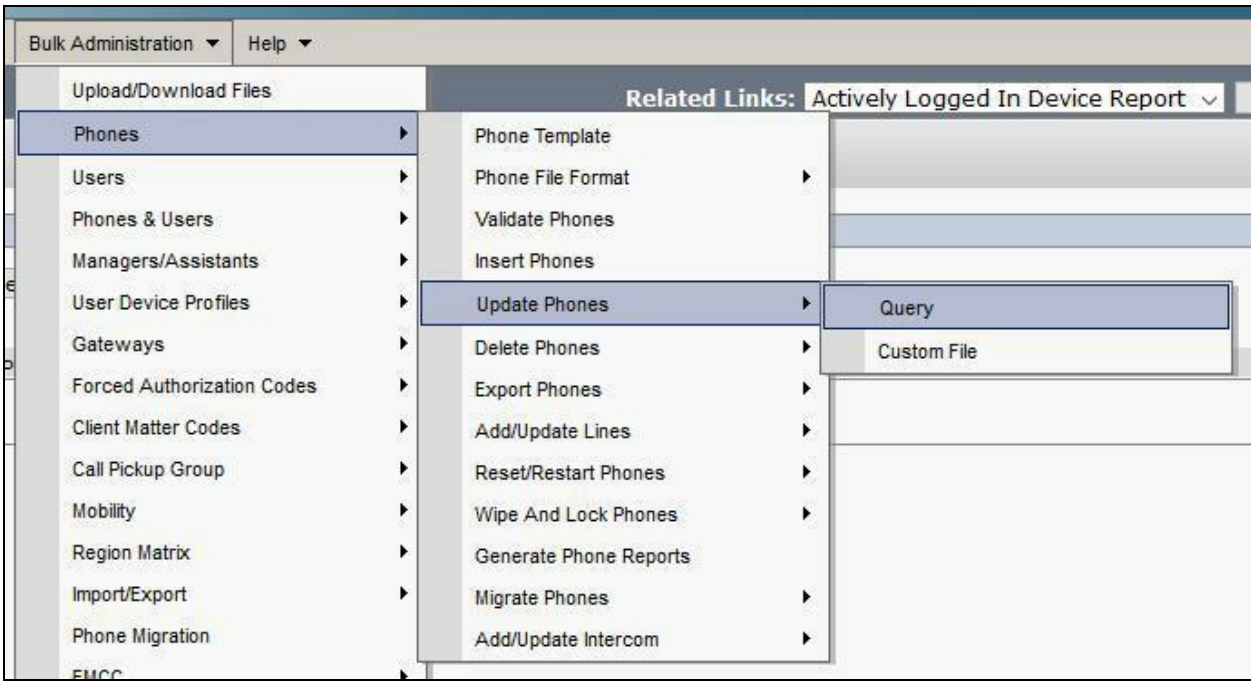


Figure 293: BULK Update Phones menu

> **Note:** Remember that BULK Administration is only available at the Publisher, so you will not see the Bulk Menu on any Subscriber server.

Here we can search for any characteristics we want, for example, "Find Phones where Device Pool begins with Default":

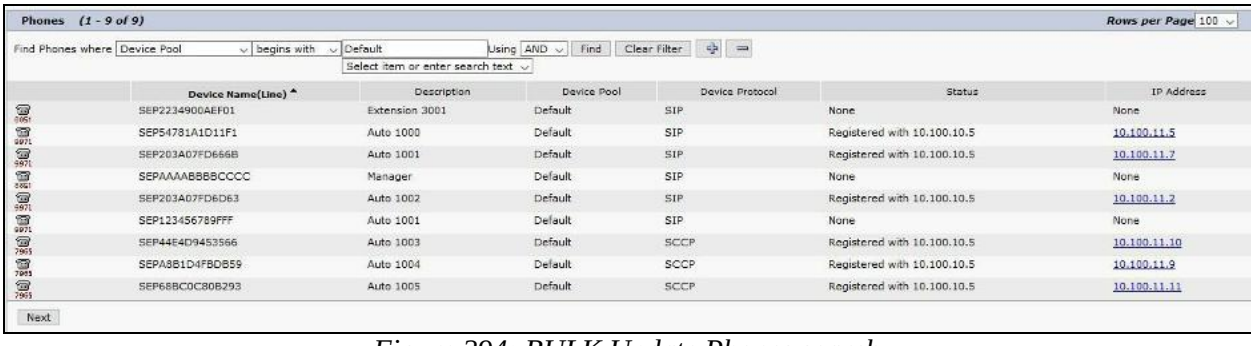


Figure 294: BULK Update Phones search

Now, in the Next window, we can edit any configuration which is available and similar to the group of devices we have selected. For example, if you have chosen a group of phones containing SIP and SCCP Phones, you will not be able to edit any SIP parameter, as these parameters are not available for SCCP Phones. After making all the changes to the selected Phones, there are two actions to choose from. On the top of the screen, we can select the

option to reset/restart/apply the config to our devices:



Figure 295: BULK Update Phones options

And at the bottom of the screen, we can choose to run this configuration immediately or later:

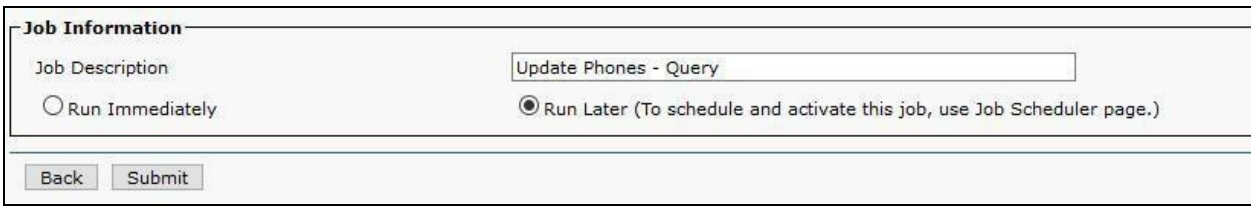


Figure 296: BULK Update Phones options

After we have selected one of the options, we can check the status of our changes on the "Job Scheduler" page by going to menu "Bulk Administration > Job Scheduler". Here, we can check all our tasks, verify the status and check if they were successful or if they failed. Click on "Job Id" to open it and verify the task logs.

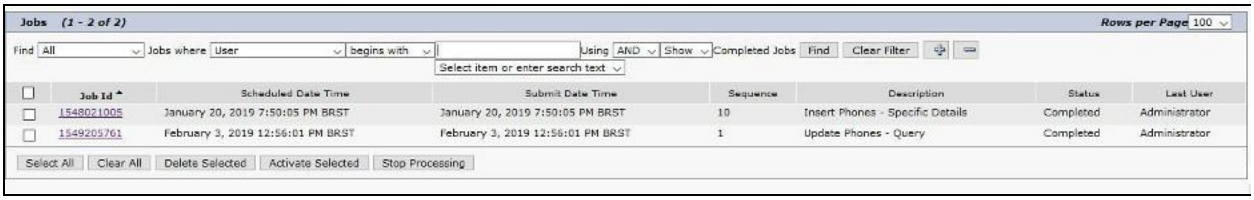


Figure 297: Jobs list

If the task fails to run, the reason will show on the screen. In the example below, the Number Of Records Processed is 5, so it means that the script has reached 5 devices, and the Number Of Records Failed is 0, so there are no errors.

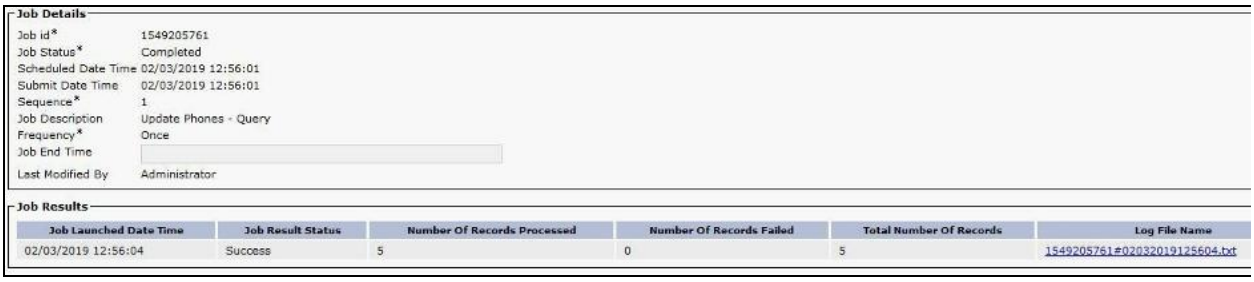


Figure 298: Jobs details

By clicking on the "Log File Name" a pop-up opens showing you more details. For example, in my case, I can see that the field "restart phones" is set to true, so after this task was executed, all these 5 phones rebooted in order to apply these changes.

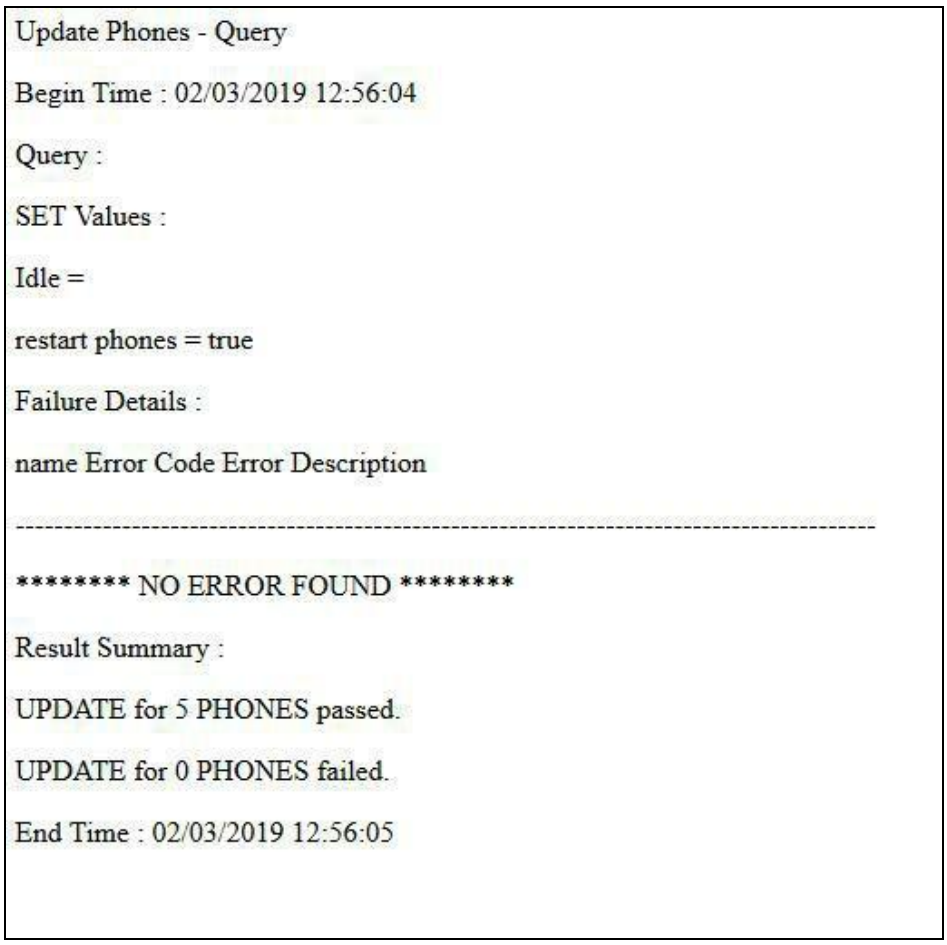


Figure 299: Log File example

Export all phones details using BULK

You can export all your phones details via BULK to have a list of all your devices. You can use it as a simple reference spreadsheet or even import it

again to CUCM. You can export all your phones or select a list to export, for example, only with the devices from a specific Device Pool.

To do so, go to Bulk Administration > Export Phones and select “Specific Details” or “All Details”:

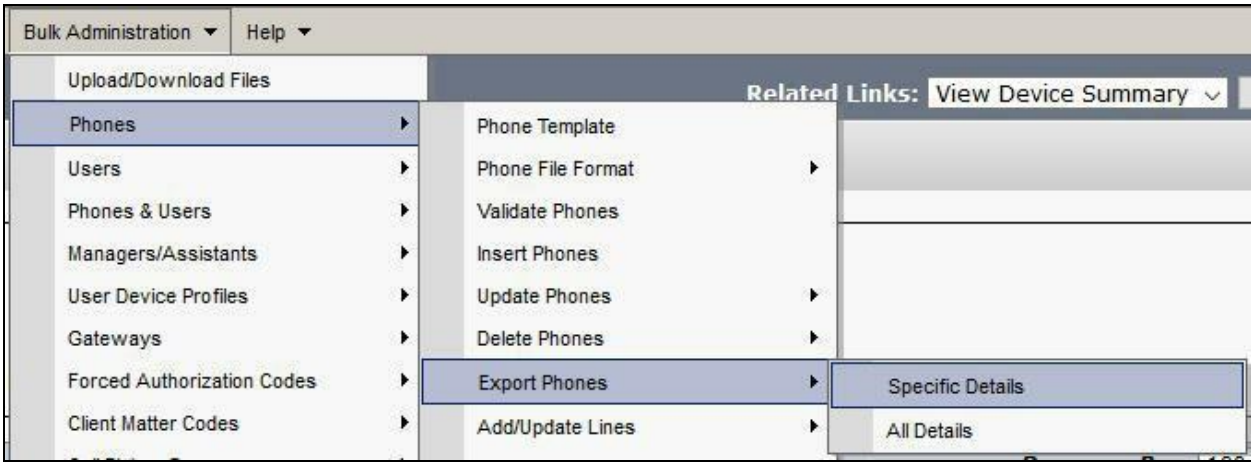


Figure 300: BULK Export Phones

Depending on your CUCM version, these options can be a little different. On CUCM 11.0, when I open “Export Phones > All Details”, I can select which phone models I want to export or select “All Phone Types”:

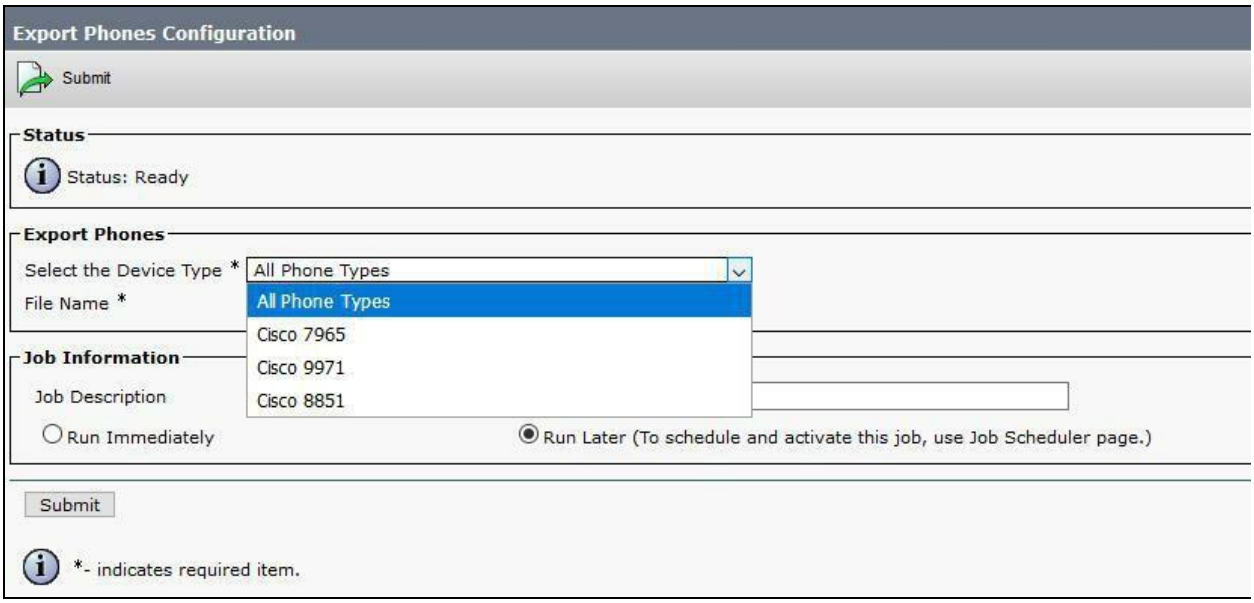


Figure 301: BULK Export Phones Configuration window

Select it, create a File Name (required) and a Job Description (optional), and then select “Run Immediately” or “Run Later (To schedule and activate this job, use Job Scheduler page.)”.

If you have selected “Export Phones > Specific Details”, the process is almost the same. The differences are that you can choose phones from a specific Device Pool, Device Type, Description, Calling Search Space, Device Protocol and other options available.

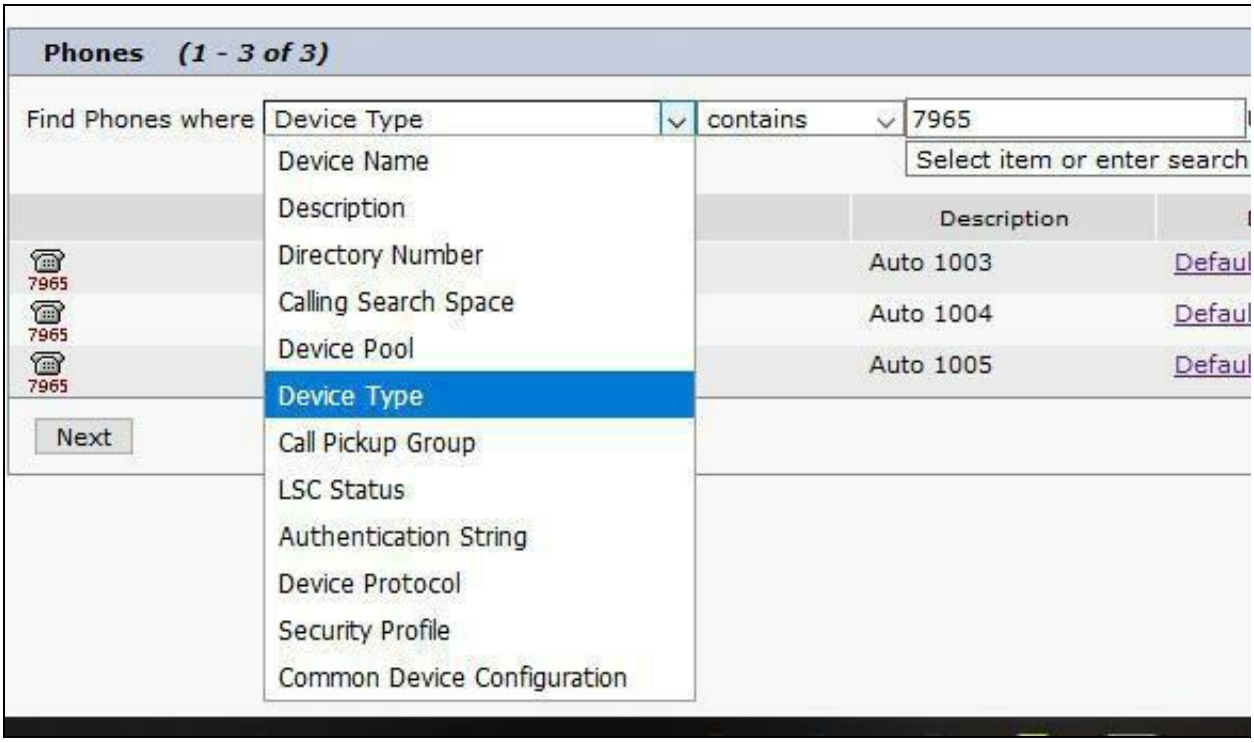


Figure 302: BULK Export Phone options

After you have created your query, in the next window you can select the format you want to use for this export; it can be the “Default Phone Format”, which includes more phone information, or the “Simple Phone Format”, which includes only the fields with MAC Address, Description, and first Directory Number. Make your choices and run it.

Then, go to “Bulk Administration > Job Scheduler” and search for your task. Depending on how many devices you have, you can go to this party while the task is still in the “Processing” state. Wait some time until it goes to status “Completed” and open it by clicking on the Job Id.

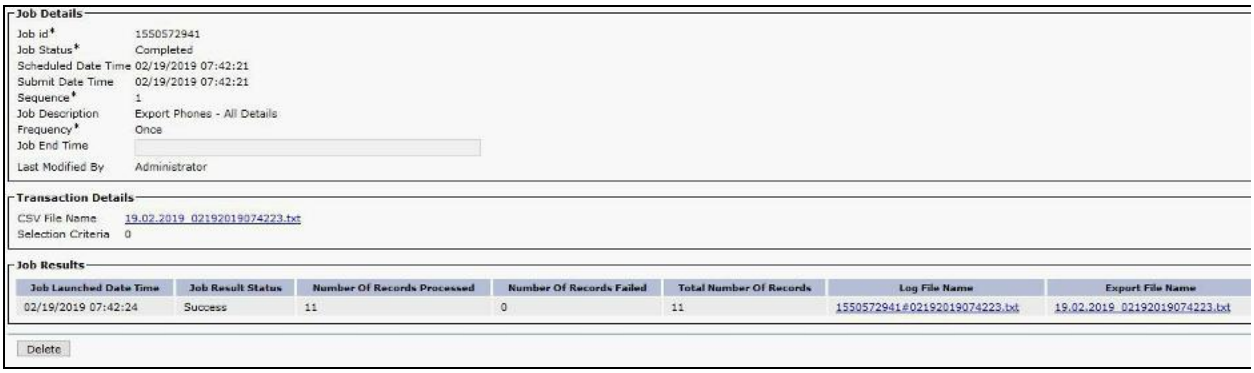


Figure 303: Job details

Now, if you click on “CSV File Name” or on “Export File Name”, a pop-up will open, and there you can select all the fields, copy and paste it to a notepad file and save it as a CSV file. But the best way is to download it by going to menu “Bulk Administration> Upload/Download Files”, search the file name, select it and click “Download Selected”.

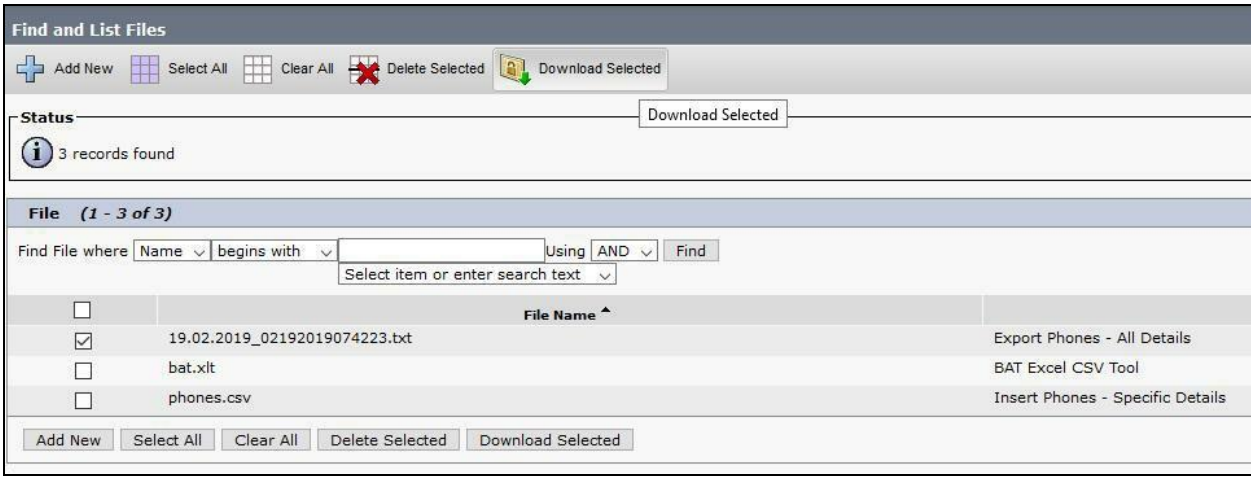


Figure 304: Find and List Files

Insert phones using BULK

You can import these files back to CUCM via BULK. As you saw, you can export two types of files, “Export Phones > All Details” and “Export Phones > Specific Details”, so the options to import them back match: “Insert Phone Specific Details” and “Insert Phone All Details”.

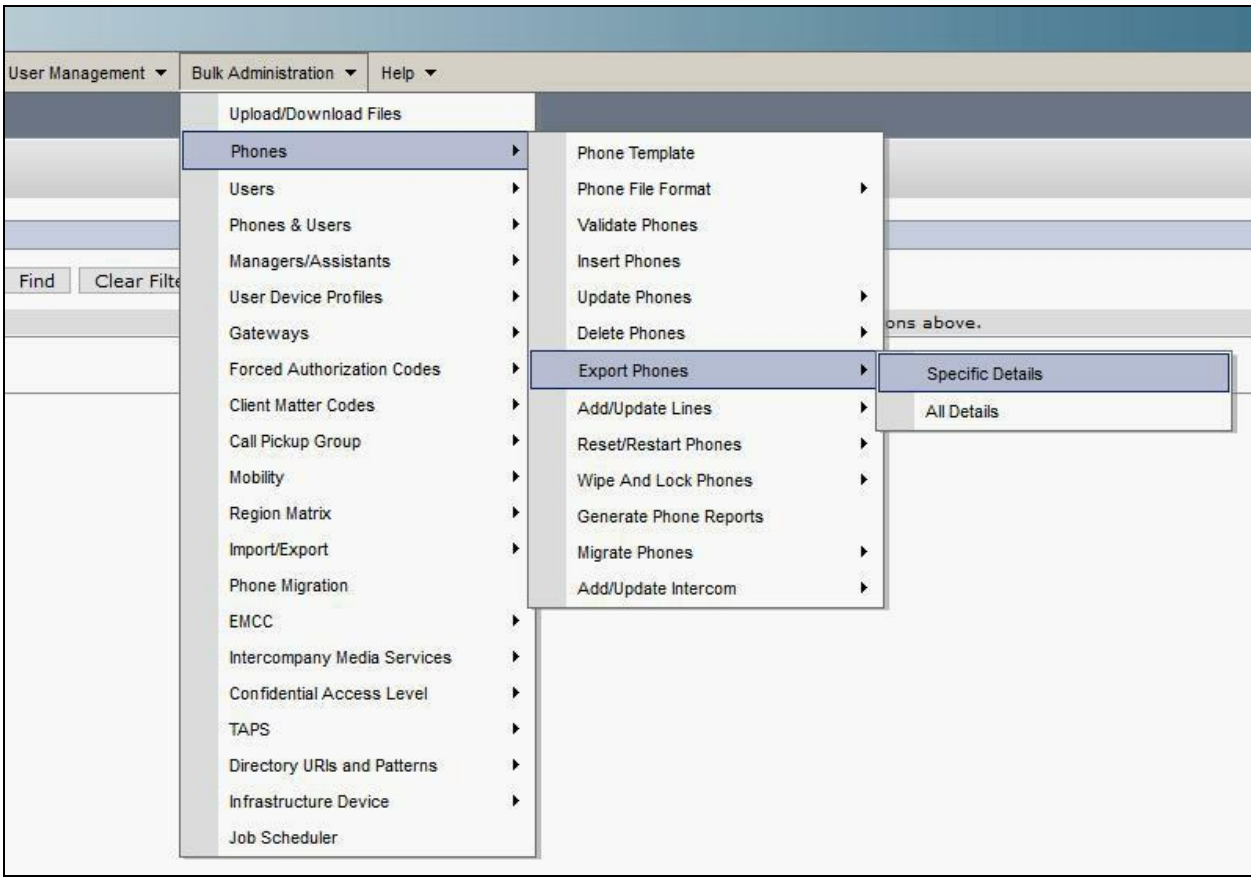


Figure 305: BULK Export Phones

File Upload

The first thing to do in this part, is to upload your file, regardless you want to “Insert Phone Specific Details” or “Insert Phone All Details”. To do so, go to menu “Bulk Administration > Upload/Download Files > Add New”.

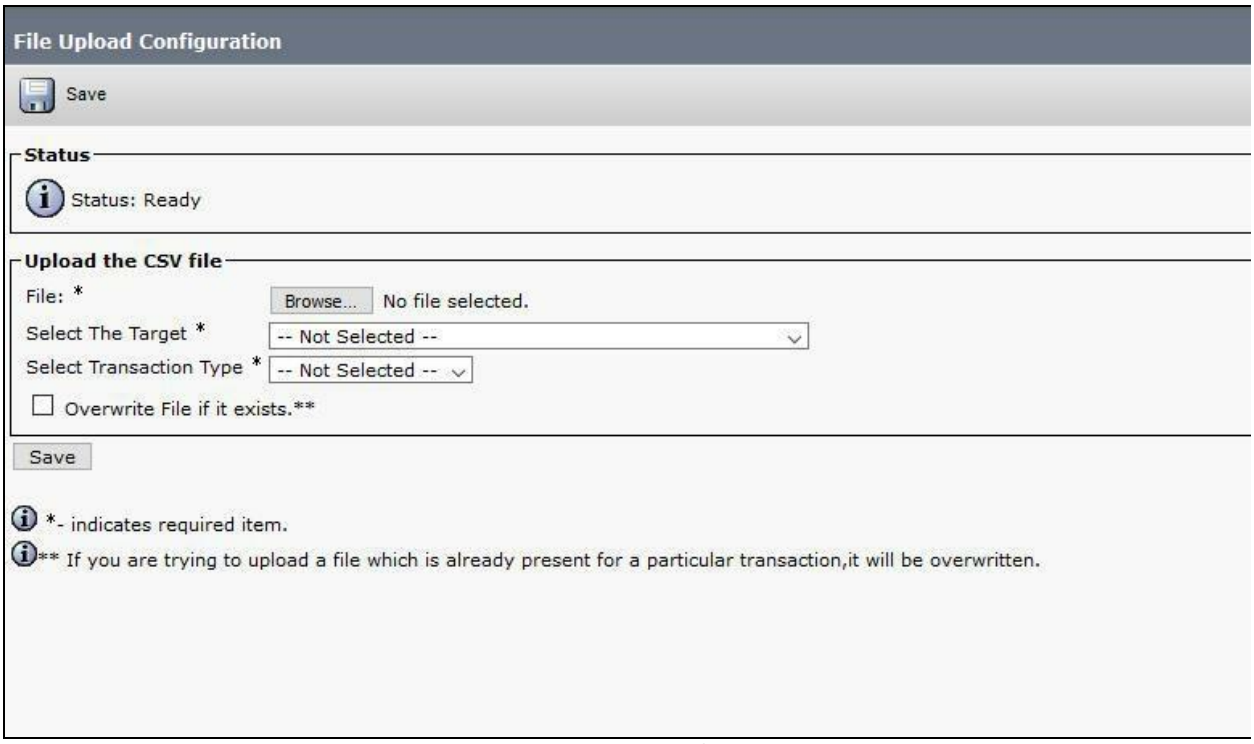


Figure 306: File Upload Configuration window

Here you need to select the target (Phones) and the transaction type (Insert Phones - All Details or Insert Phones - Specific Details). Upload your file and click “Save”.

Insert Phone Specific Details

If you are going to choose “Insert Phone Specific Details”, you will need to create a Phone Template first. Go to menu “Bulk Administration > Phones > Phone Template”. Click “Add New” and follow the wizard. The template will ask you about the phone model; you can use the same template for the phones with similar characteristics, like the series 79xx – for example: if you create a template for the phone 7942, it will work with phones 7945, but it will only allow you to configure the first 2 directory numbers (as the 7942 only has 2 buttons for directory numbers).

After you have created your Template, go back to “Bulk Administration > Phones > Insert Phones”. Select “Insert Phones Specific Details”, the File Name you have uploaded and the Phone Template Name you have created. Then, in “Override Options”, if you wish, you can update existing phones within this process.

The last part is to select one of two options - “Run Immediately” or “Run Later”. Again, use the Job Scheduler page to see the job status.

Insert Phone All Details

If you select to “Insert Phones with All Details”, the process is easier as you do not need to create a Phone Template. Select “Insert Phones All Details”, choose your file, and you are ready to proceed.

If you are inserting a file from a different CUCM version, you may have problems with this process, as sometimes Cisco changes the field names with the CSV files. I do not quite understand why it happens. Possibly you need to open your CSV file in Excel to edit some field names (or even remove some non-critical fields) and then try to import it again.

I had some situations where I repeated this process many times until I had a fully functional file to be imported in a different CUCM version. But in the end, it worked.

CHAPTER 16 - CALL DETAIL RECORDS

How to check call logs

To check for your call logs on CUCM, first, you need to confirm if the Call Detail Records is correctly configured. To check this, go to the menu:

- System;
- Service Parameter;
- Select your CUCM Publisher;
- Select the service “Cisco Call Manager”;
- Look for option "CDR Enabled Flag Required"; change it to True (necessary);
- Look for option "CDR Log Calls with Zero Duration Flag"; change it to True (recommended).

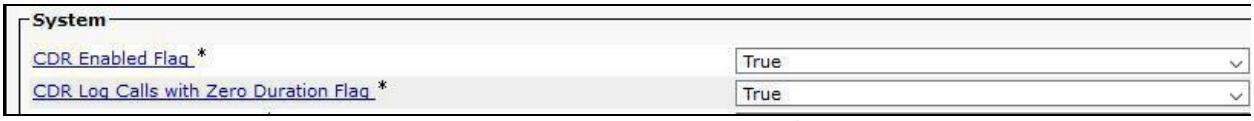


Figure 307 - CDR Enabled Flag configuration

The option "CDR Log Calls with Zero Duration Flag" will log not answered calls. It’s not necessary on environments working correctly, but can help on troubleshooting if needed.

Repeat these steps to all your Subscribers servers.

Search for call logs

Now that we have calls being logged, we can look at Cisco Unified CM CDR Analysis and Reporting (CAR). Go to https://CUCM-PUB-IP-ADDRESS/car/ to open it.

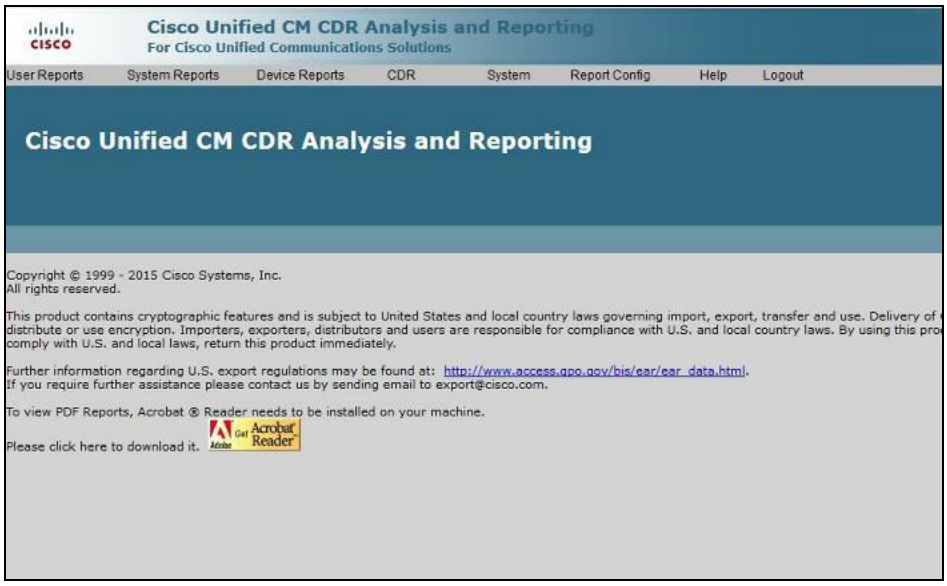


Figure 308 - Cisco CAR Web Page

Now, go to menu CDR > Search; as you can see, there are a lot of options available, and you can try them all. I strongly recommend that you try them. But let's check the most basic option, "By User/Phone Number/SIP URL":

Click on "CDR > Search > By User/Phone Number/SIP URL":

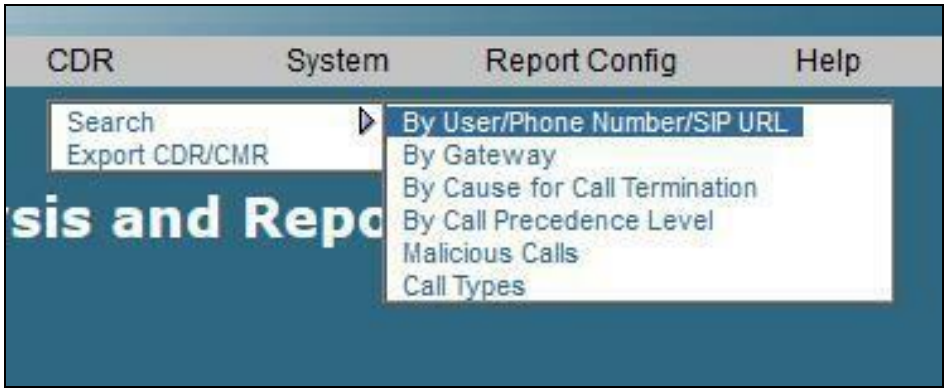


Figure 309 - Cisco CDR Search menu

In this window, you can type the extension number you want to search logs. Or you can leave it blank and press "OK" to see all call logs from the last hour.

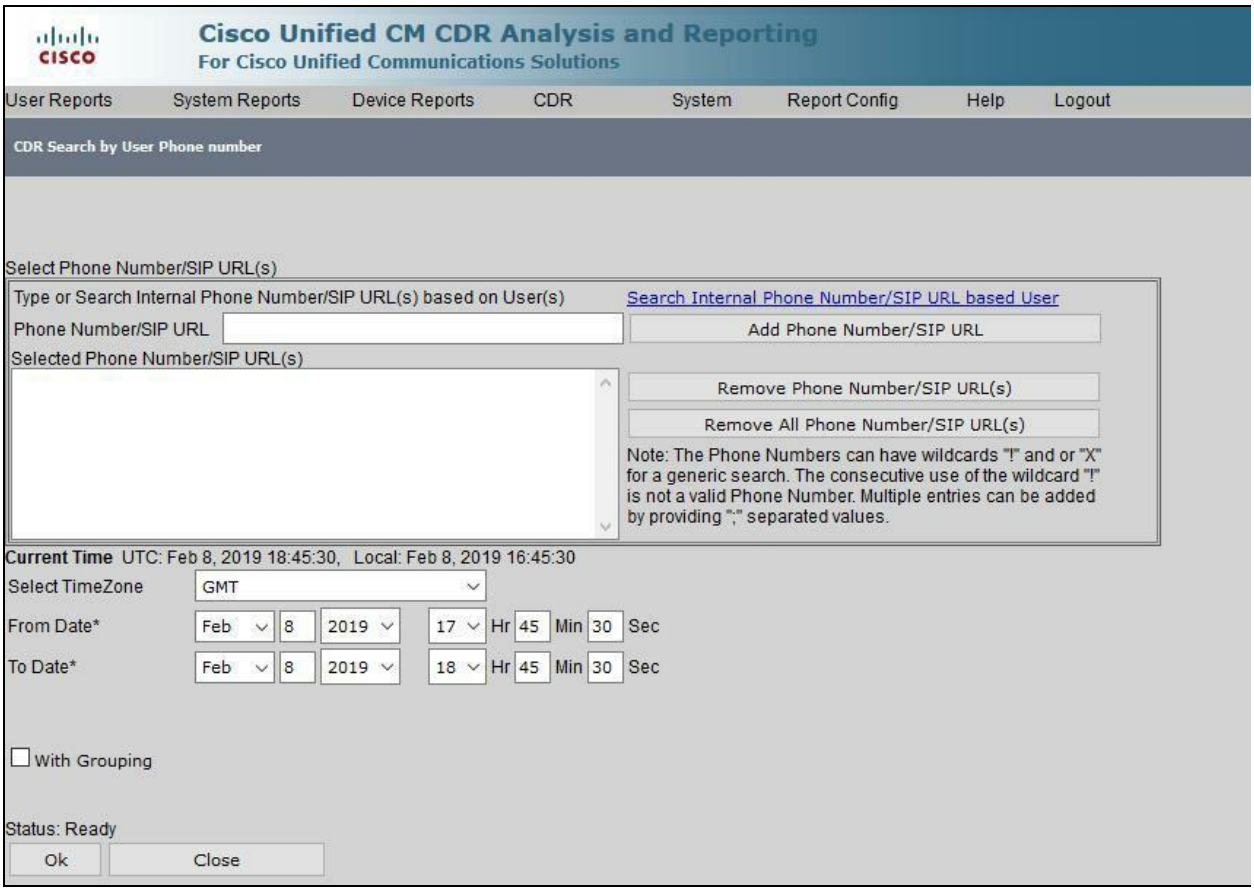


Figure 310 - Cisco CDR Search page

In my example, I was able to find 2 calls:

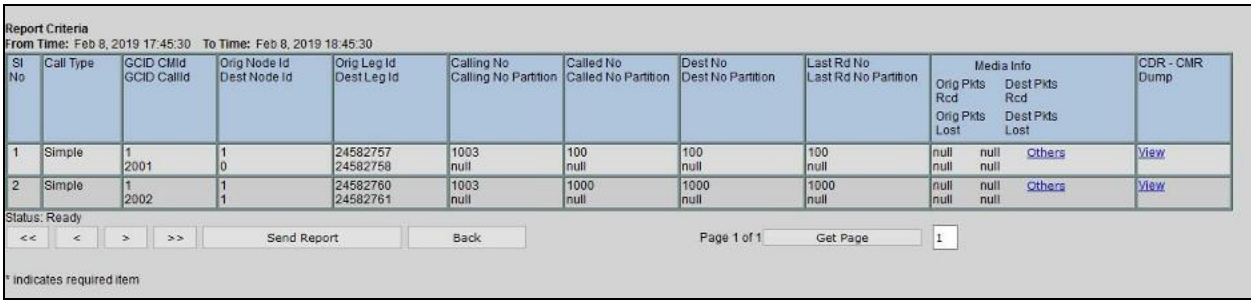
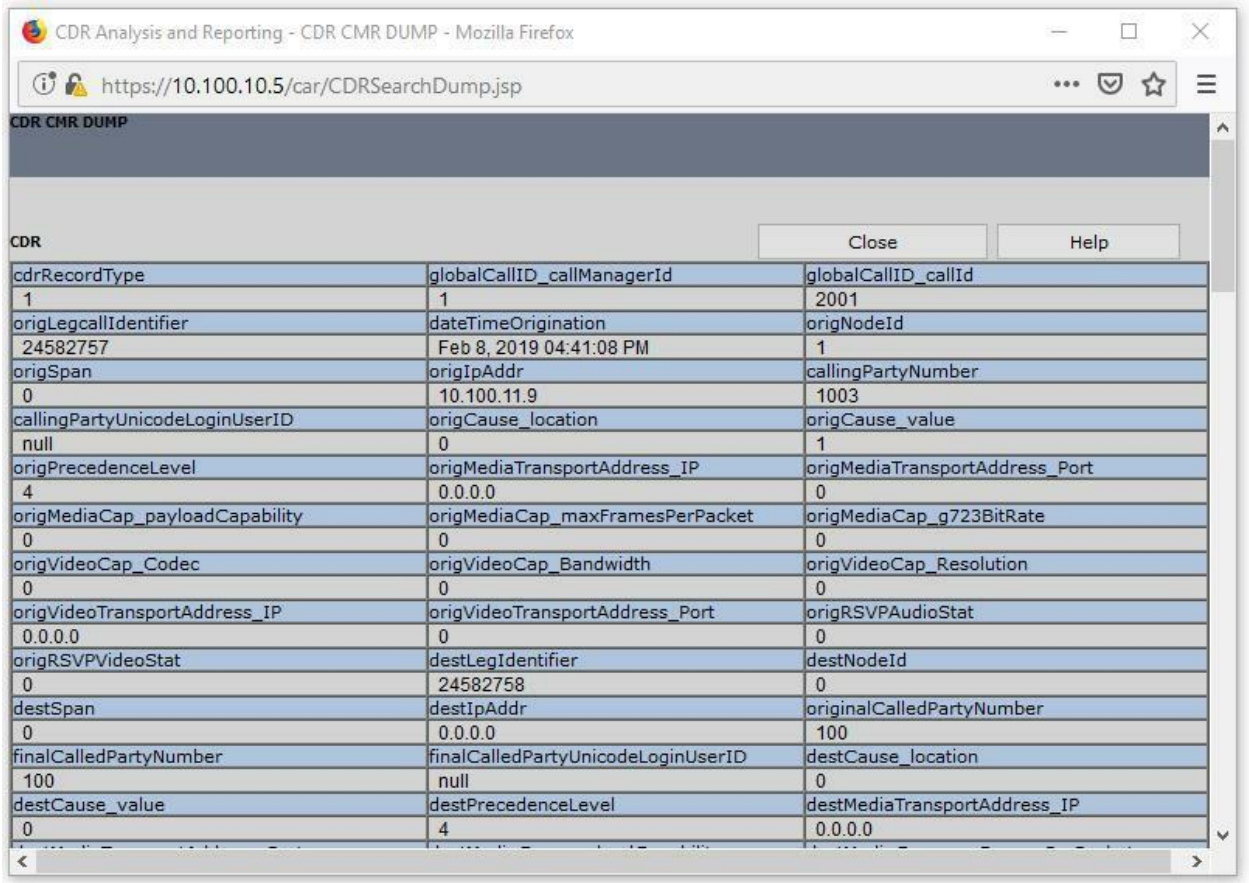


Figure 311 - Cisco CDR Search results

To check the call details, click on the “View”, in the last column, “CDR - CMR Dump”.

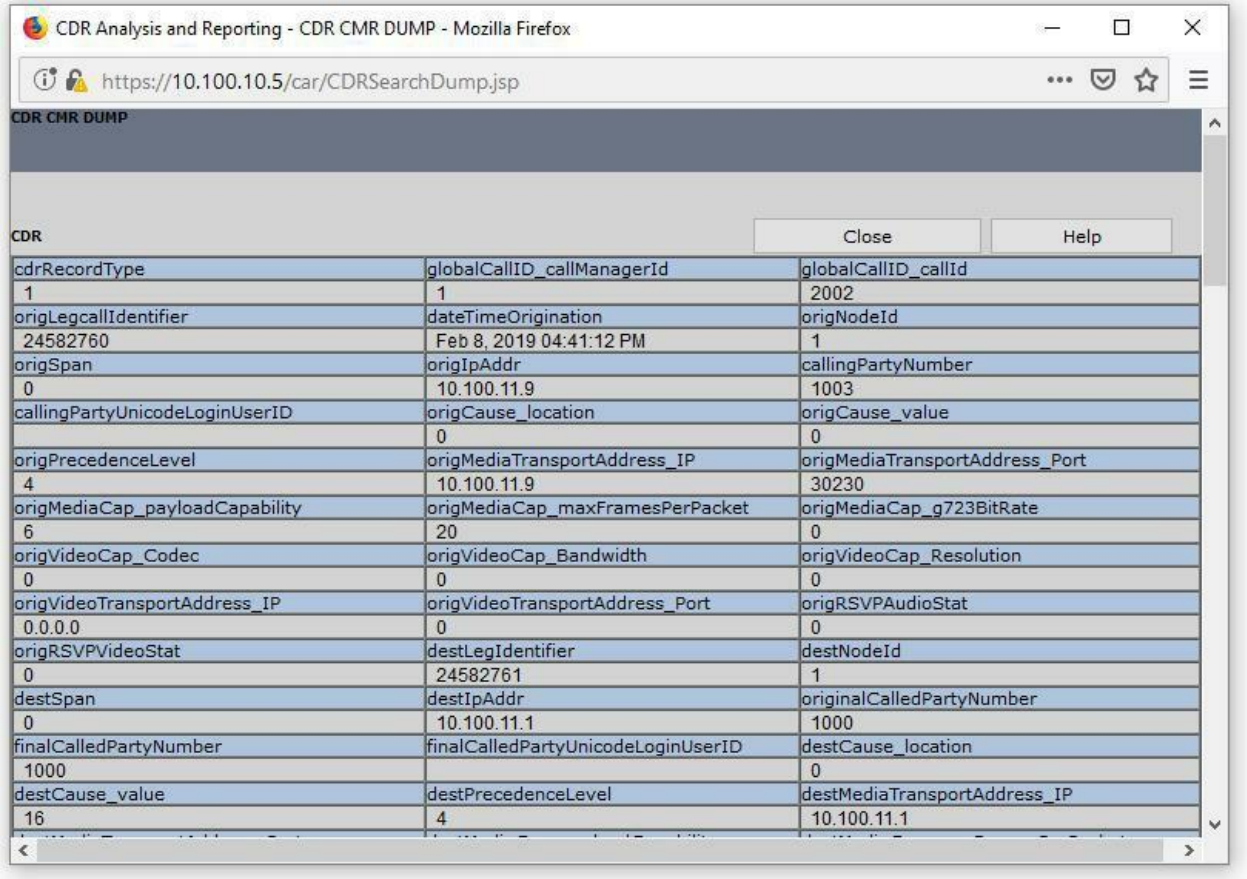


cdrRecordType	globalCallID_callManagerId	globalCallID_callId
1	1	2001
origLegcallIdentifier	dateTimeOrigination	origNodeId
24582757	Feb 8, 2019 04:41:08 PM	1
origSpan	origIpAddr	callingPartyNumber
0	10.100.11.9	1003
callingPartyUnicodeLoginUserID	origCause_location	origCause_value
null	0	1
origPrecedenceLevel	origMediaTransportAddress_IP	origMediaTransportAddress_Port
4	0.0.0.0	0
origMediaCap_payloadCapability	origMediaCap_maxFramesPerPacket	origMediaCap_g723BitRate
0	0	0
origVideoCap_Codec	origVideoCap_Bandwidth	origVideoCap_Resolution
0	0	0
origVideoTransportAddress_IP	origVideoTransportAddress_Port	origRSVPAudioStat
0.0.0.0	0	0
origRSVPVideoStat	destLegIdentifier	destNodeId
0	24582758	0
destSpan	destIpAddr	originalCalledPartyNumber
0	0.0.0.0	100
finalCalledPartyNumber	finalCalledPartyUnicodeLoginUserID	destCause_location
100	null	0
destCause_value	destPrecedenceLevel	destMediaTransportAddress_IP
0	4	0.0.0.0

Figure 312 - Cisco CDR call details

This call was finished with error 1 - which means “Unallocated (unassigned) number”. You can see this error on column “origCause_Value”. This happened because the user dialed “100” when he probably was trying to dial to extension “1000”, as extension “100” does not exist.

The second call worked properly, but it was not answered (cause code 0) and the calling user has canceled the call:



cdrRecordType	globalCallID_callManagerId	globalCallID_callId
1	1	2002
origLegcallIdentifier	dateTimeOrigination	origNodeId
24582760	Feb 8, 2019 04:41:12 PM	1
origSpan	origIpAddr	callingPartyNumber
0	10.100.11.9	1003
callingPartyUnicodeLoginUserID	origCause_location	origCause_value
	0	0
origPrecedenceLevel	origMediaTransportAddress_IP	origMediaTransportAddress_Port
4	10.100.11.9	30230
origMediaCap_payloadCapability	origMediaCap_maxFramesPerPacket	origMediaCap_g723BitRate
6	20	0
origVideoCap_Codec	origVideoCap_Bandwidth	origVideoCap_Resolution
0	0	0
origVideoTransportAddress_IP	origVideoTransportAddress_Port	origRSVPAudioStat
0.0.0.0	0	0
origRSVPVideoStat	destLegIdentifier	destNodeId
0	24582761	1
destSpan	destIpAddr	originalCalledPartyNumber
0	10.100.11.1	1000
finalCalledPartyNumber	finalCalledPartyUnicodeLoginUserID	destCause_location
1000		0
destCause_value	destPrecedenceLevel	destMediaTransportAddress_IP
16	4	10.100.11.1

Figure 313 - Cisco CDR call details

Follow all possible call termination cause codes (in bold, the most commons):

Code	Description
0	**No error**
1	**Unallocated (unassigned) number - usually, the extension does not exist or CSS wrong**
2	No route to specified transit network (national use)
3	**No route to destination (missing dial-peer/route pattern)**
4	Send special information tone
5	Misdialed trunk prefix (national use)
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
8	Preemption

9	Preemption—circuit reserved for reuse
16	**Normal call clearing - this is the default to a correct and completed call.**
17	**User busy**
18	No user responding
19	No answer from user (user alerted)
20	Subscriber absent
21	**Call rejected - call is being denied by some device - if it's your router denying it, check Chapter 7, "ip address trusted list"**
22	Number changed
26	Non-selected user clearing
27	**Destination out of order - google "Route List Exhausted" bug, check if T1/E1 channels are available, CSS problems or others**
28	Invalid number format (address incomplete)
29	Facility rejected
30	Response to STATUS ENQUIRY
31	Normal, unspecified
34	No circuit/channel available
38	**Network out of order - check same as code 27**
39	Permanent frame mode connection out of service
40	Permanent frame mode connection operational
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded
44	Requested circuit/channel not available
46	Precedence call blocked
47	Resource unavailable, unspecified
49	Quality of Service not available

50	Requested facility not subscribed
53	Service operation violated
54	Incoming calls barred
55	Incoming calls barred within Closed User Group (CUG)
57	Bearer capability not authorized
58	Bearer capability not presently available
62	Inconsistency in designated outgoing access information and subscriber class
63	Service or option not available, unspecified
65	Bearer capability not implemented
66	Channel type not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available (national use)
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
87	User not member of CUG (Closed User Group)
88	Incompatible destination
90	Destination number missing and DC not subscribed
91	Invalid transit network selection (national use)
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type nonexistent or not implemented
98	Message is not compatible with the call state, or the message type is nonexistent or

Technet24

	not implemented
99	An information element or parameter does not exist or is not implemented
100	Invalid information element contents
101	The message is not compatible with the call state
102	Call terminated when timer expired; a recovery routine executed to recover from the error
103	Parameter nonexistent or not implemented - passed on (national use)
110	Message with unrecognized parameter discarded
111	Protocol error, unspecified
122	Precedence Level Exceeded
123	Device not Preemptable
125	Out of bandwidth (Cisco specific)
126	Call split (Cisco specific)
127	Interworking, unspecified
129	Precedence out of bandwidth
131	Call Control Discovery PSTN Failover (Cisco specific)

Table 46 - Call Termination cause codes

Export CDR automatically to external Billing Server

You can also export all your call logs to an external billing server, which will receive these logs via FTP/SFTP and process it. To do it, on the right-top corner of CUCM page, go to “Cisco Unified Serviceability > Tools > CDR Management:



Figure 314 - Cisco Unified Serviceability menu

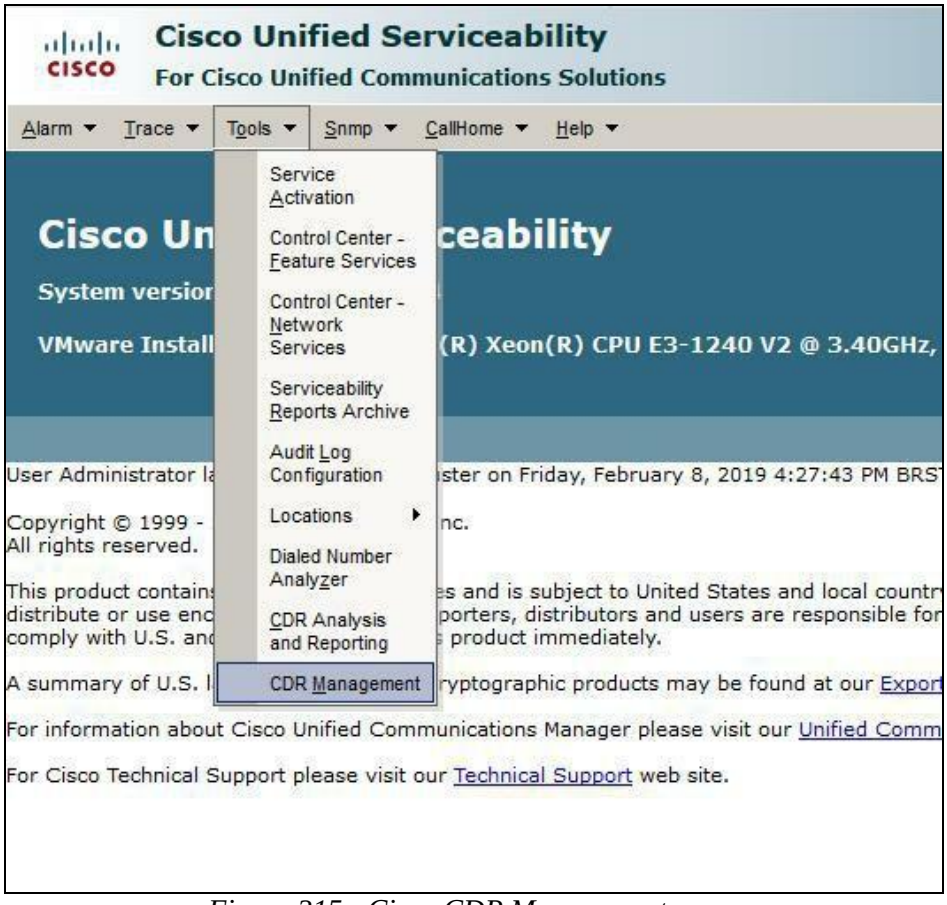


Figure 315 - Cisco CDR Management menu

On “Billing Application Server Parameters”, click “Add New”:

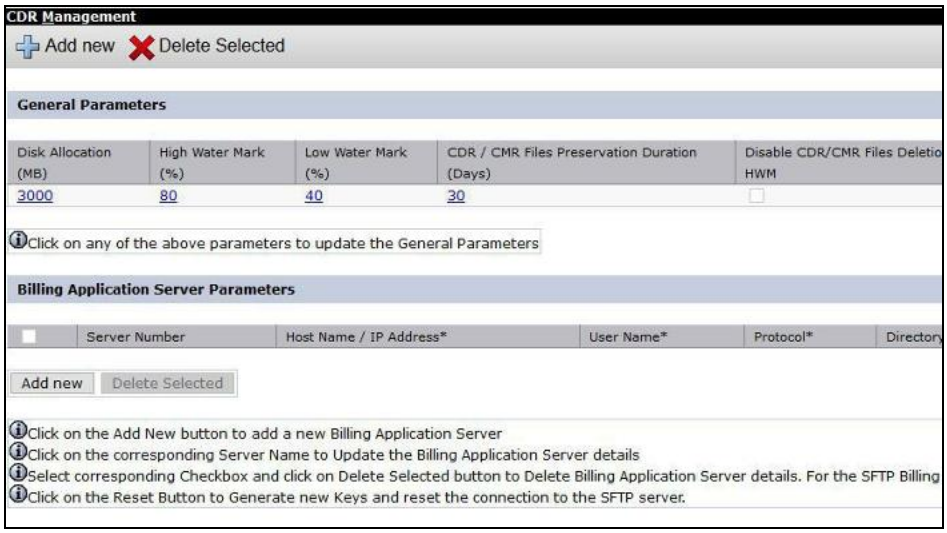


Figure 316 - Cisco CDR Management page

Now, you need to add your server information. You can send these CDR files to the external server via FTP or SFTP.

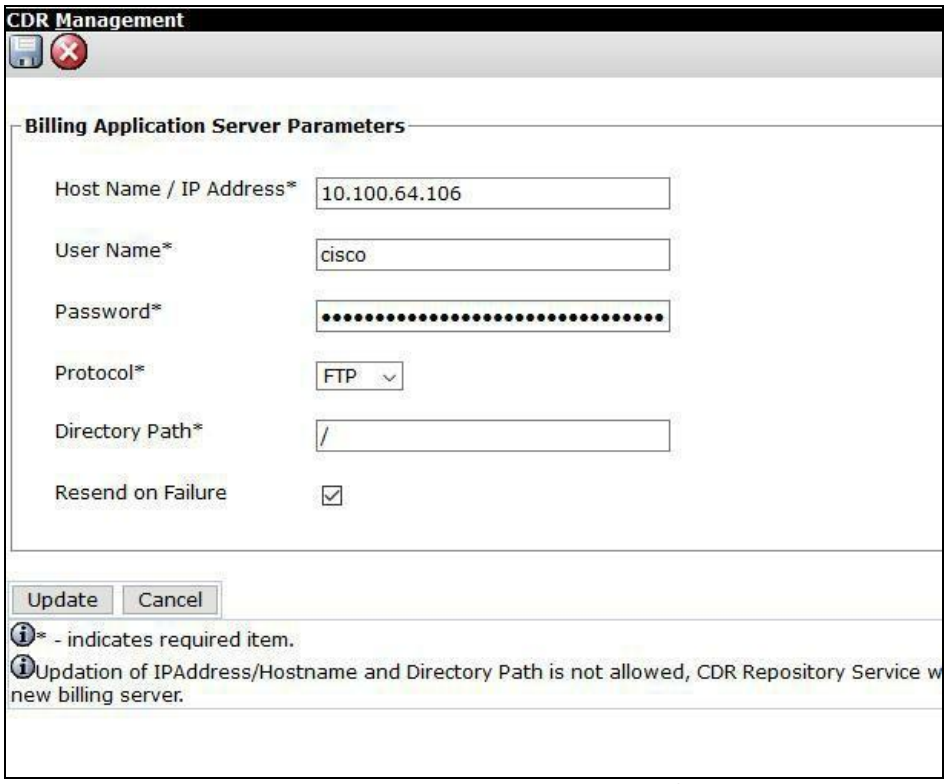


Figure 317 - Cisco CDR Management configuration

Then, on your FTP/SFTP server, you will start to see the files being transfered:



Figure 318 - CDR file being sent to FTP server

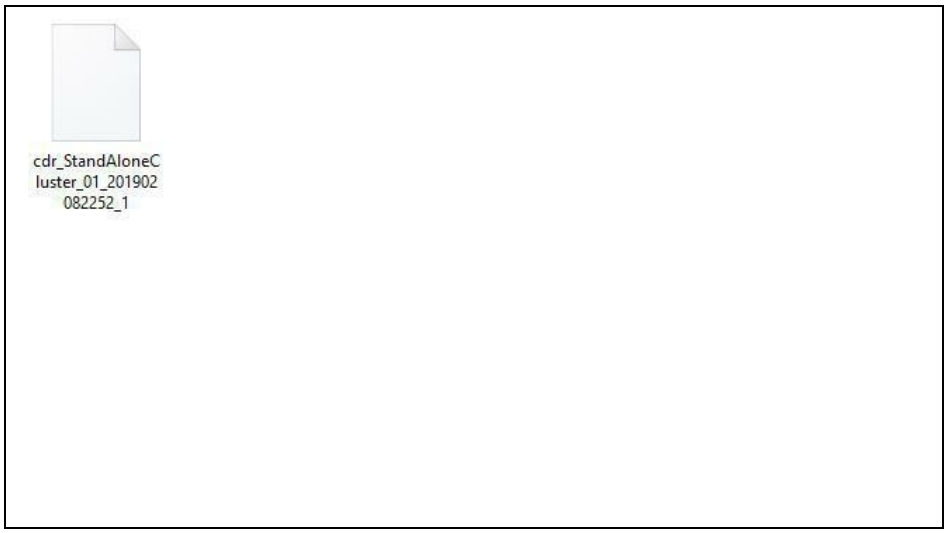


Figure 319 - CDR file received on FTP server

Each file sends from CUCM will contain 1 minute of CDR data. If you want to change this parameter (not recommended), you can go back to the Cisco Unified CM Administration window, then “System > Enterprise Parameters > CDR File Time Interval” and change it.

The last step is to configure your billing application to read these files in the correct folder of your server. Contact your Billing vendor to check how to do this.

CHAPTER 17 - REAL TIME MONITORING TOOL

How to monitor the CUCM environment

Cisco Real-Time Monitoring Tool (RTMT) is a software included in CUCM that allows for monitoring of the CUCM server. We can:

- check the number of active (registered) phones;
- check the number of calls in progress;
- check system logs;
- collect traces of calls;
- collect more details about the CUCM Cluster status.

To use it, we need to download it from the CUCM server and install it. Let's check the process.

Install and access RTMT

To install RTMT, download it directly from your CUCM server. Go to menu "Applications > Plugins > Find". Look for "Cisco Unified Real-Time Monitoring Tool - Windows" (or Linux, if you are using a Linux Desktop).

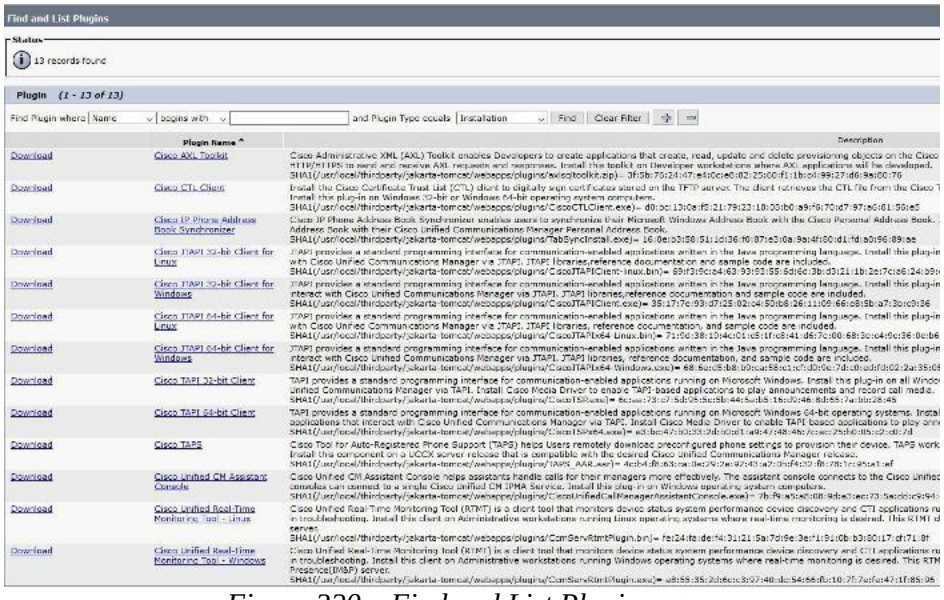


Figure 320 – Find and List Plugins page

Download it and proceed to the installation. The file size is at about 75MB. The installation process is very straightforward; basically, it will ask you for information such as installation folder, etc.; You will also need to have JAVA installed on your PC.



Figure 321 – Cisco RTMT installation

After the installation is completed, open it. It will ask for the server IP address (Publisher), login and password. This is the same password that you use to access the CUCM Web page (not the SSH login/password).

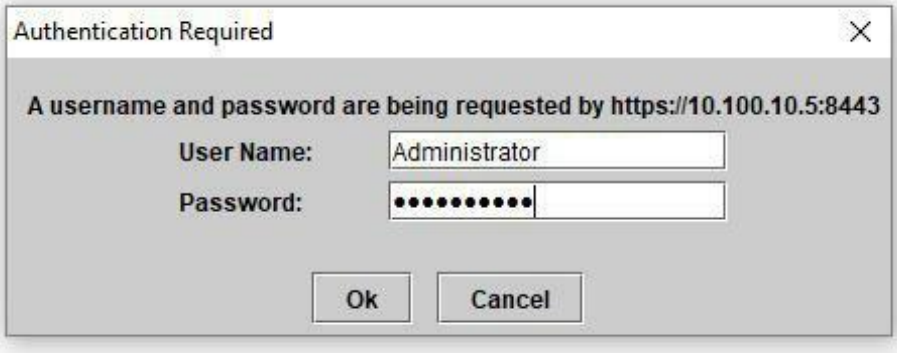


Figure 322 – Cisco RTMT Authentication

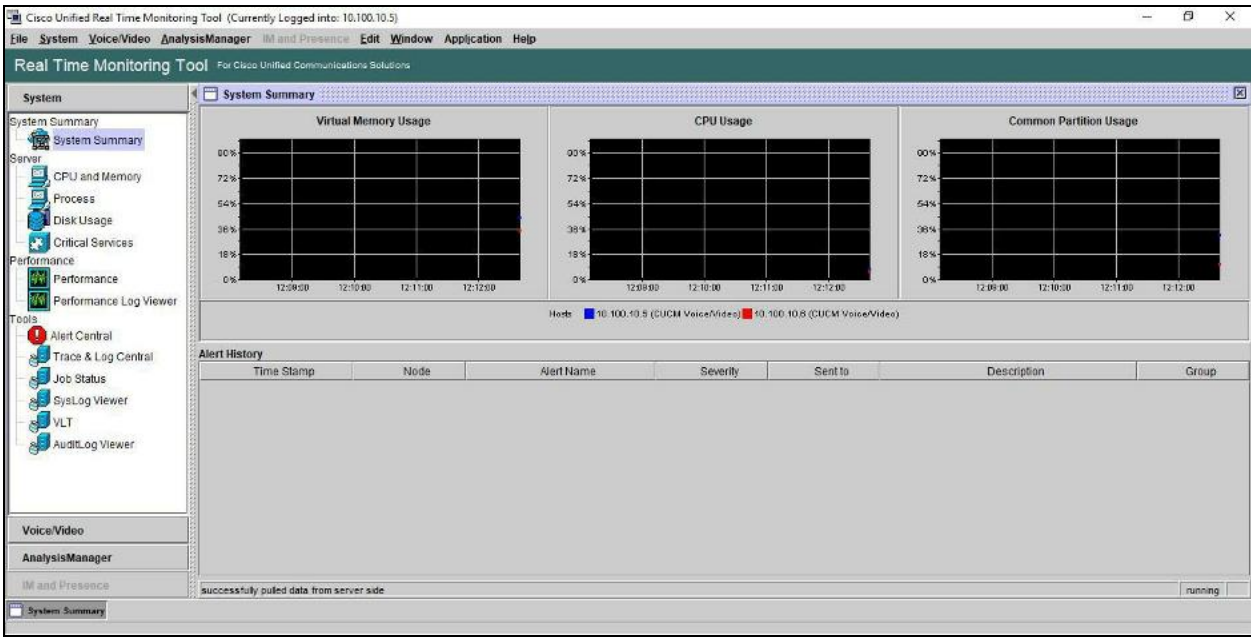


Figure 323 – Cisco RTMT main page

Basic checks with RTMT

To check how many phones are registered on your cluster, go to tab Voice/Video Summary > Voice and Video Summary. You will see a screen with the number of registered phones in your cluster as well as the number of calls in progress. You can also go to the tab Voice/Video Summary > Device Summary to check the same information.

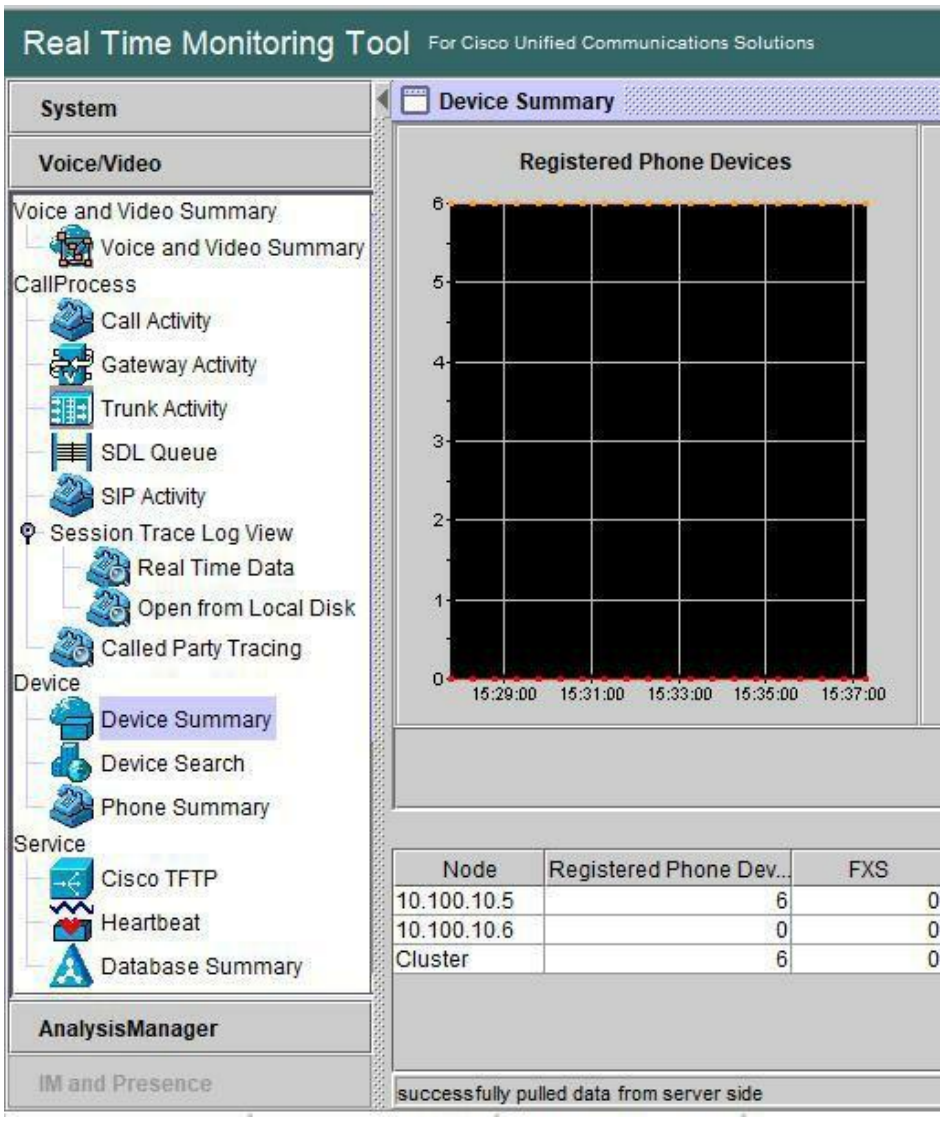


Figure 324 – Cisco RTMT Device Summary page

I recommend you to navigate and explore all the information you can get on RTMT. You can also open it and let running for your monitoring support team if you wish.

Collecting Traces with RTMT

- Collecting Traces with RTMT is very useful for troubleshooting complex problems. Usually, the Cisco TAC Support Team ask us to collect and send these logs when issues in CUCM appear. There are a lot of traces possible, so you need to know what you are looking for.
- In CUCM 9.x and later, detailed tracing is enabled by default for

the CallManager service. But if you want to confirm it, or if you're going to remove the default trace and allow only what you need (useful to trace just SIP calls, an example), the procedure is as follows:

- On the top right corner of CUCM, go to Cisco Unified Serviceability page;
- Choose Trace > Configuration.
- From the Server drop-down list, choose the CUCM Publisher and click Go.
- From the Service Group drop-down list, choose CM Services and click Go.
- From the Service drop-down list, choose Cisco CallManager and click Go.
- Remove/Select what you need, select the option "Apply to All Nodes" (recommended) and press Save.

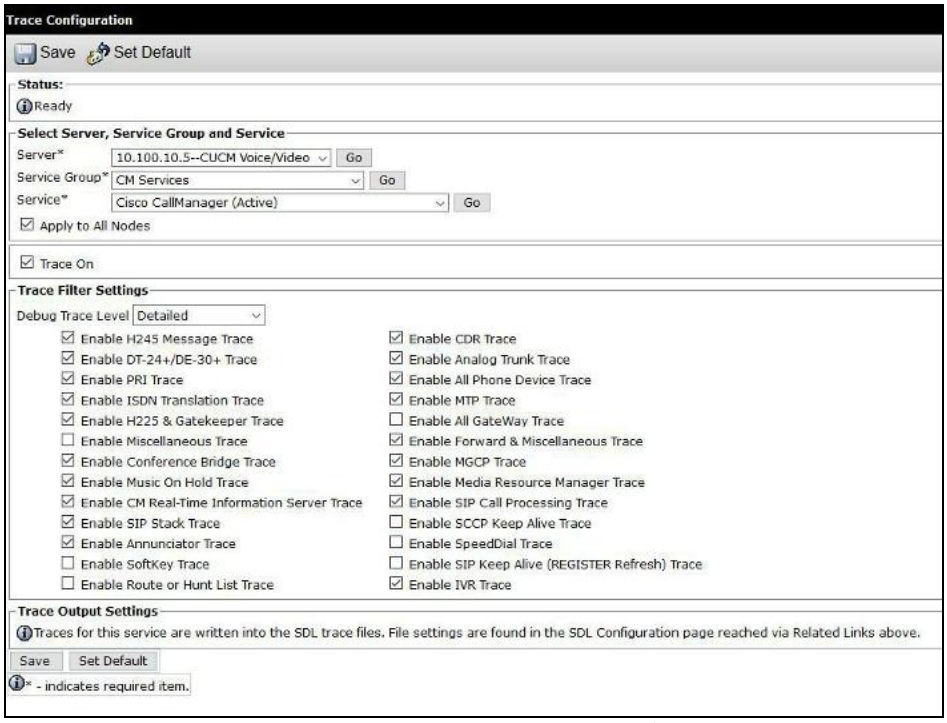


Figure 325 – Cisco CUCM Trace Configuration

Now, to download these log files, go to System > Tools > Trace & Log Central > Collect Files:

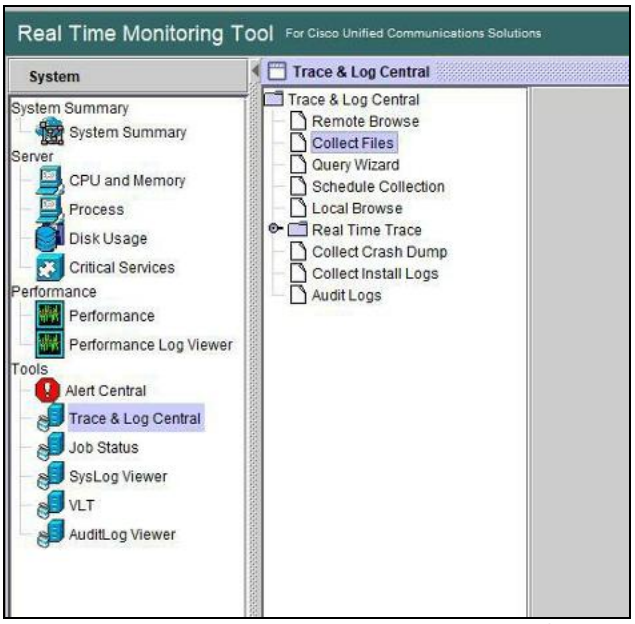


Figure 326 – Cisco RTMT Collect Trace files

Now, select the Service you want to use to collect trace files. For example, Cisco Call Manager:

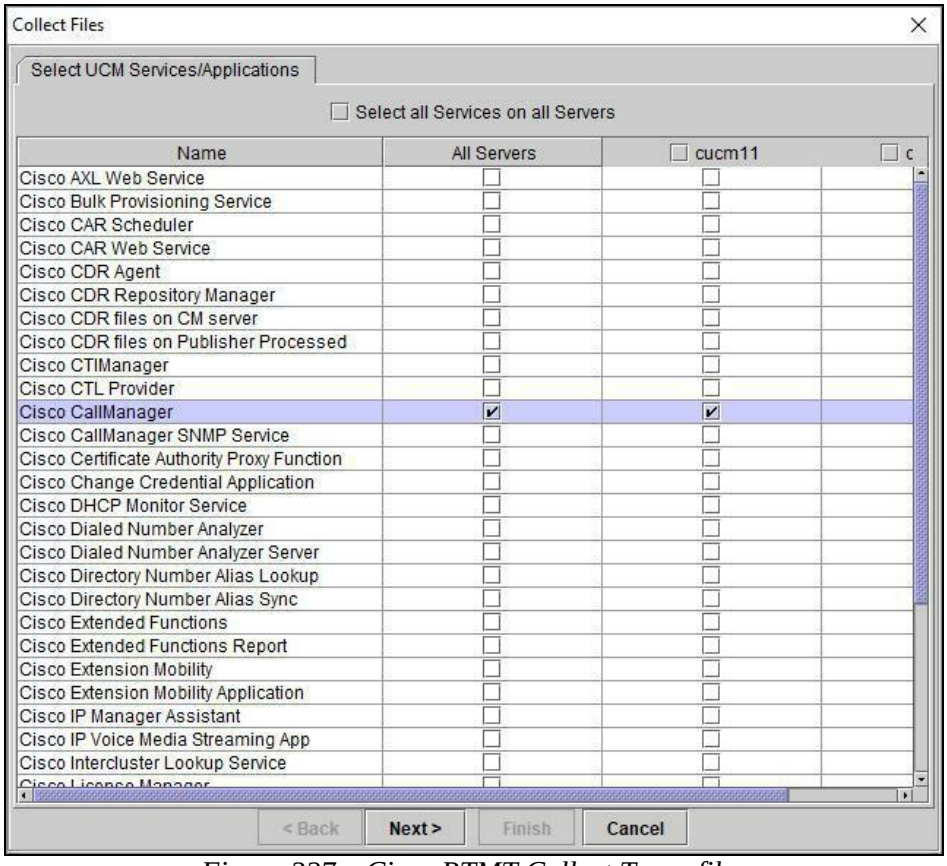


Figure 327 – Cisco RTMT Collect Trace files

In the "Select UCM Services/Applications", click the checkbox in the All Servers column for "Cisco CallManager" and then click “Next”.

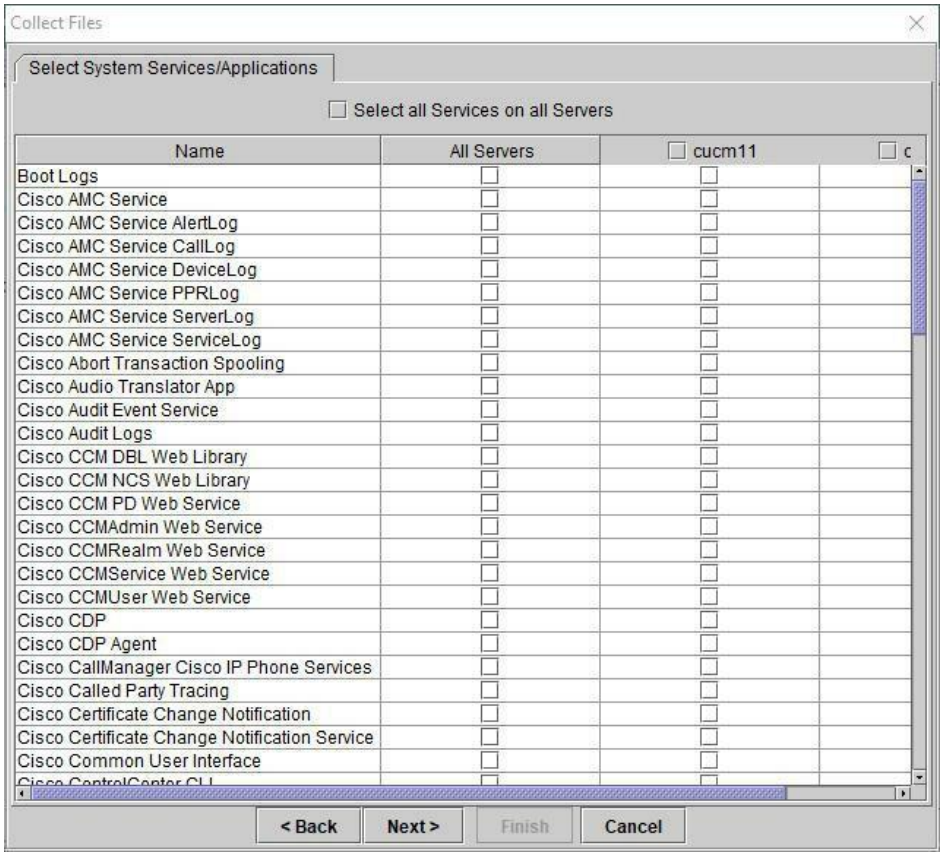


Figure 328 – Cisco RTMT Collect Trace files

Now, if you want to select any additional “System Service/Application”, select it here. If not, just select “Next” to proceed.

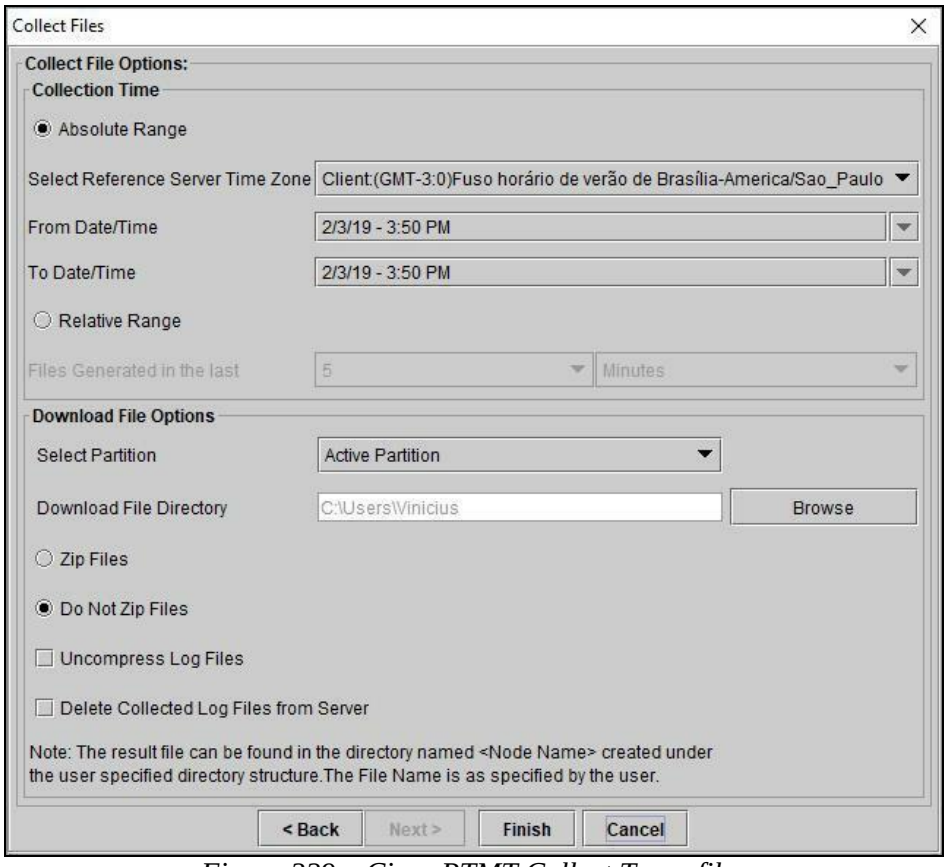


Figure 329 – Cisco RTMT Collect Trace files

Finally, select the time range from the logs you want to connect with. You can choose a from/to date, or select a relative range, for example, “last 60 minutes”.

Select the download file directory, and if you want to, zip the files (useful for slow connections).

You can open these files on your computer to check it, or send it to Cisco TAC Support Team if you have an open ticket with them.

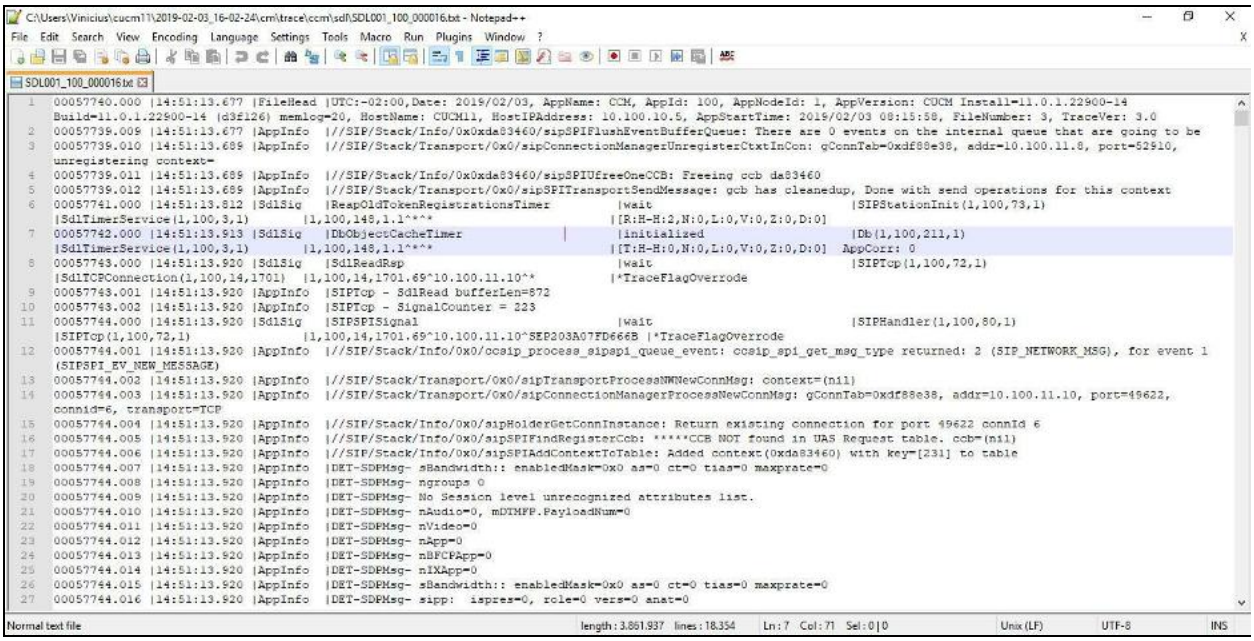


Figure 330 – Cisco Trace file

SIP Call traces on RTMT

SIP Call Trace is necessary to troubleshoot SIP calls on CUCM. Traces provide detailed information about the call and generate SIP messages when enabled on CUCM.

This traces are also enabled by default in the new CUCM versions, but you can check it yourself. Go to Cisco Unified CM Administration > System > Enterprise Parameter > Call Trace Log Configuration for Session Trace > make sure “Enable Call Trace Log” is enabled.

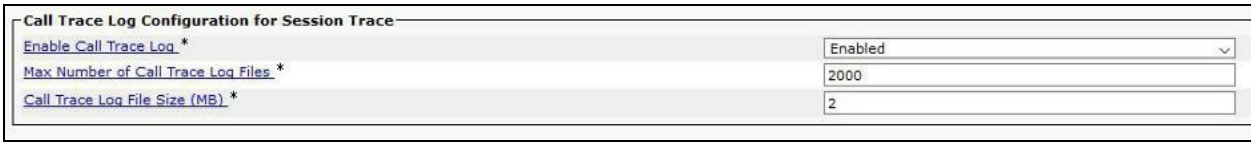


Figure 331 – Call Trace Log configuration

Then, on RTMT, go to Voice/Video Menu > Session Trace Log View > Real-Time Data and press “Run”:

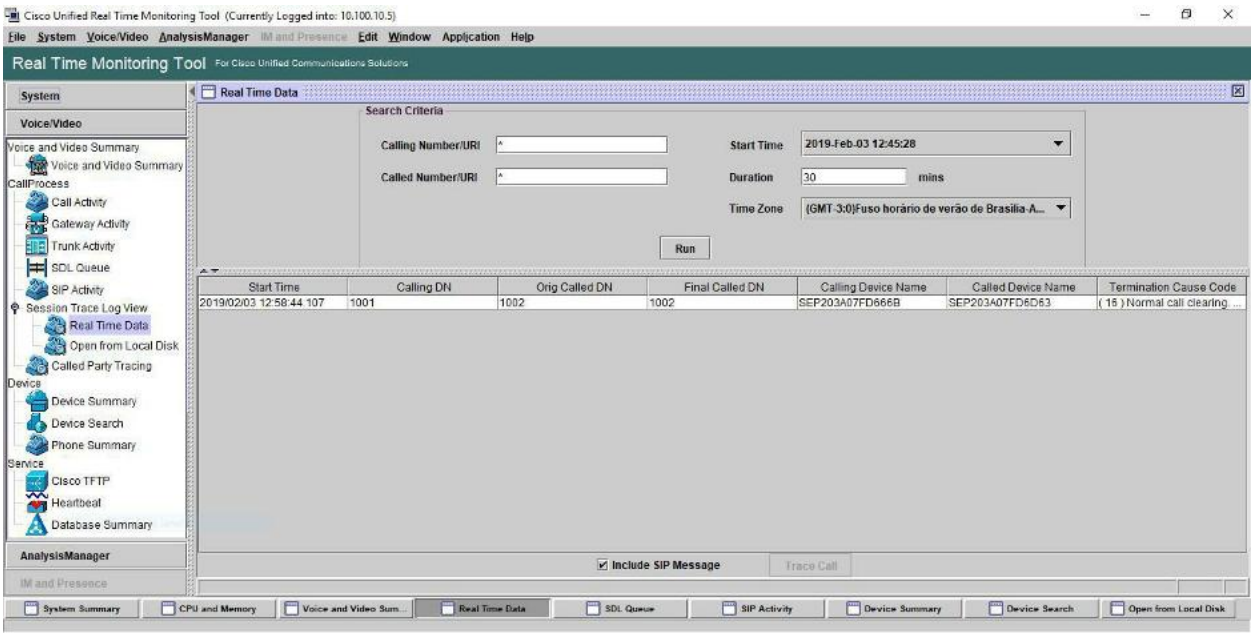


Figure 332 – Call Trace Log search

By default, you will see all your SIP Call logs from the last 30 minutes, and you can change these search criteria if you want.

To check the trace for a specific call, double-click on it and a pop-up window will open:

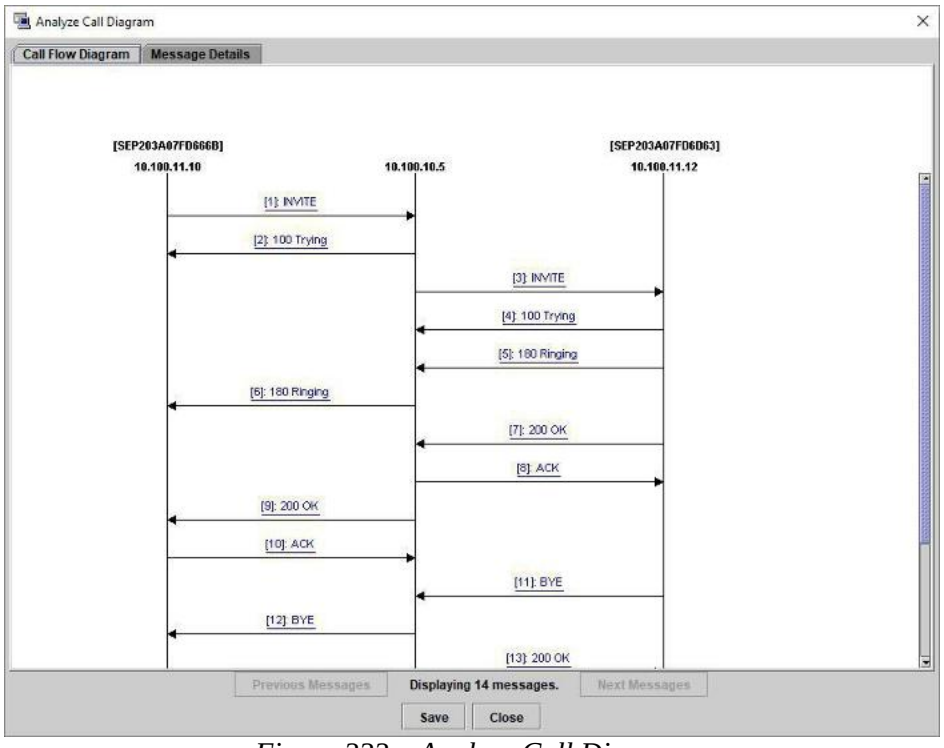


Figure 333 – Analyse Call Diagram

You can check every call step individually by clicking on it:

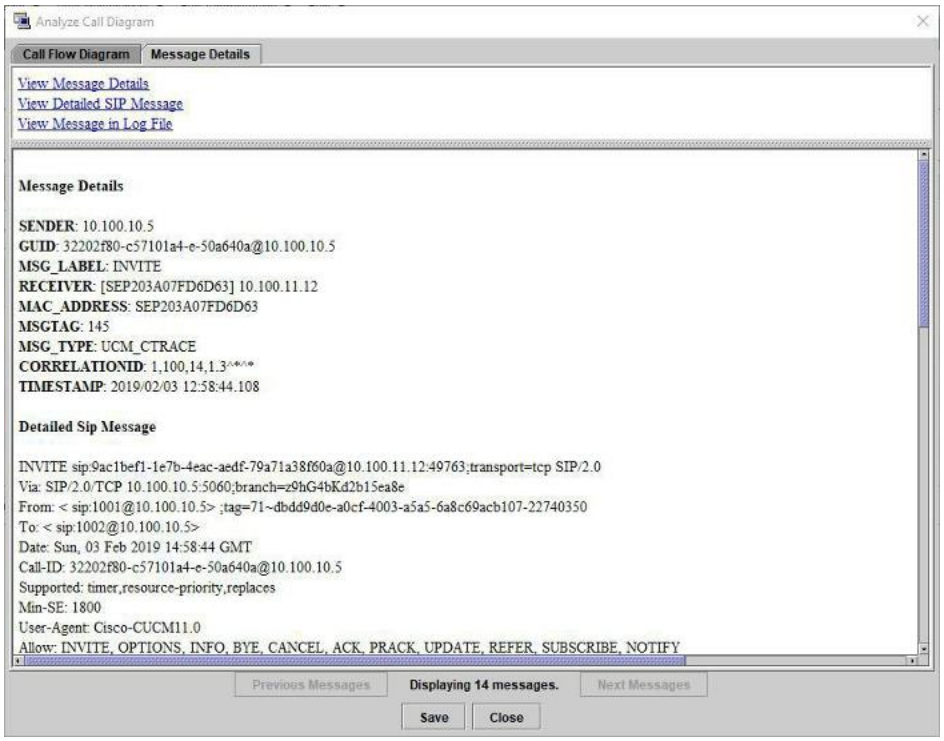


Figure 334 – Analyse Call Diagram

CHAPTER 18 - BACKUP AND RESTORE

How to backup and restore the CUCM Server

The backup of the CUCM system is critical. We always need to have an updated backup because we never know when something bad is going to happen.

There are different backup alternatives available, but I strongly recommend using the official backup tool that comes with CUCM: Disaster Recovery Tool (DRS), as it works very well, is very simple (just being necessary an SFTP server to transfer your files) and it is the only officially supported by Cisco TAC Support Team.

Backup

SFTP Server

First, let's prepare our SFTP server. You can use any server you want, just check if your server can transfer large files.

If you do not have any SFTP server in your environment, I recommend the SolarWinds SFTP/SCP Server, available for free at https://www.solarwinds.com/free-tools/free-sftp-server. Just download it, install it on your server and configure a username, password and Root Directory.

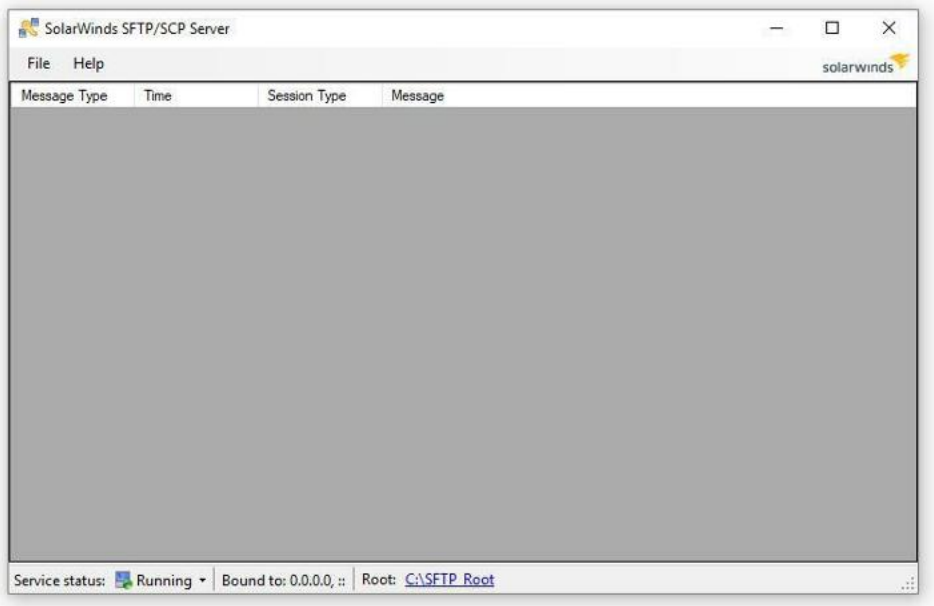


Figure 335 - Solarwinds SFTP/SCP Server screen

Since a single CUCM backup can take at about 1.5 GB, you will need at least 15 GB to store the last ten backups.

Now that our SFTP server is online, let's go back to CUCM. On the top right corner of the CUCM, select "Disaster Recovery System" and click "Go".

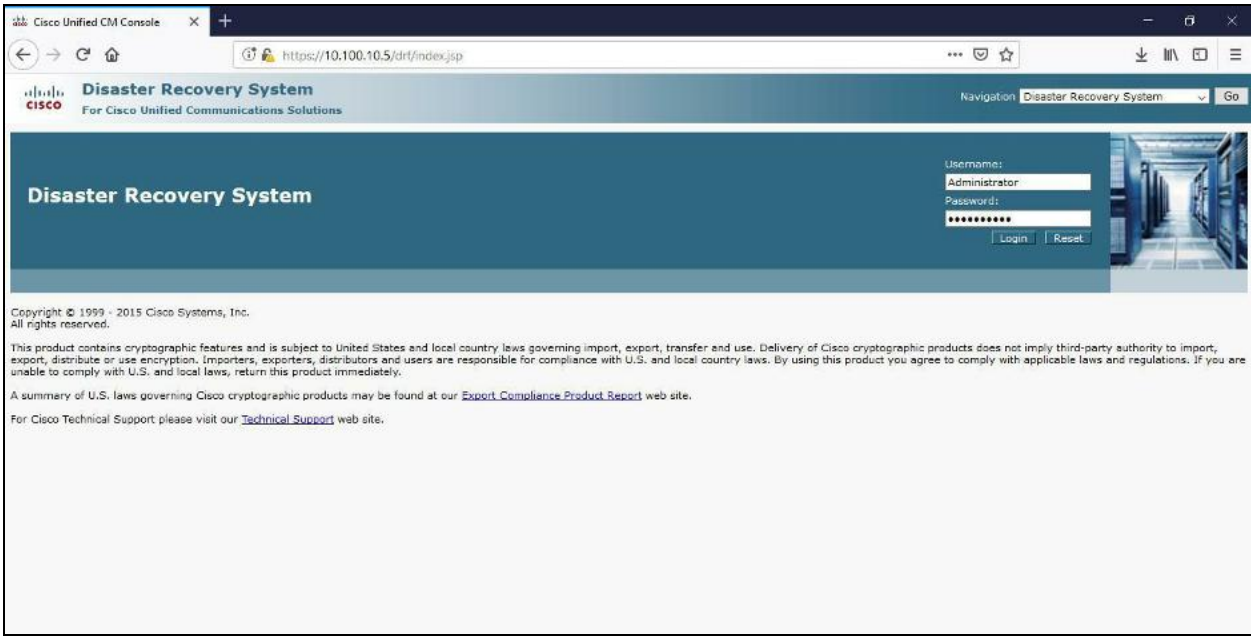


Figure 336 - CUCM Disaster Recovery System page

Now, open the menu "Backup" and select "Backup Device":

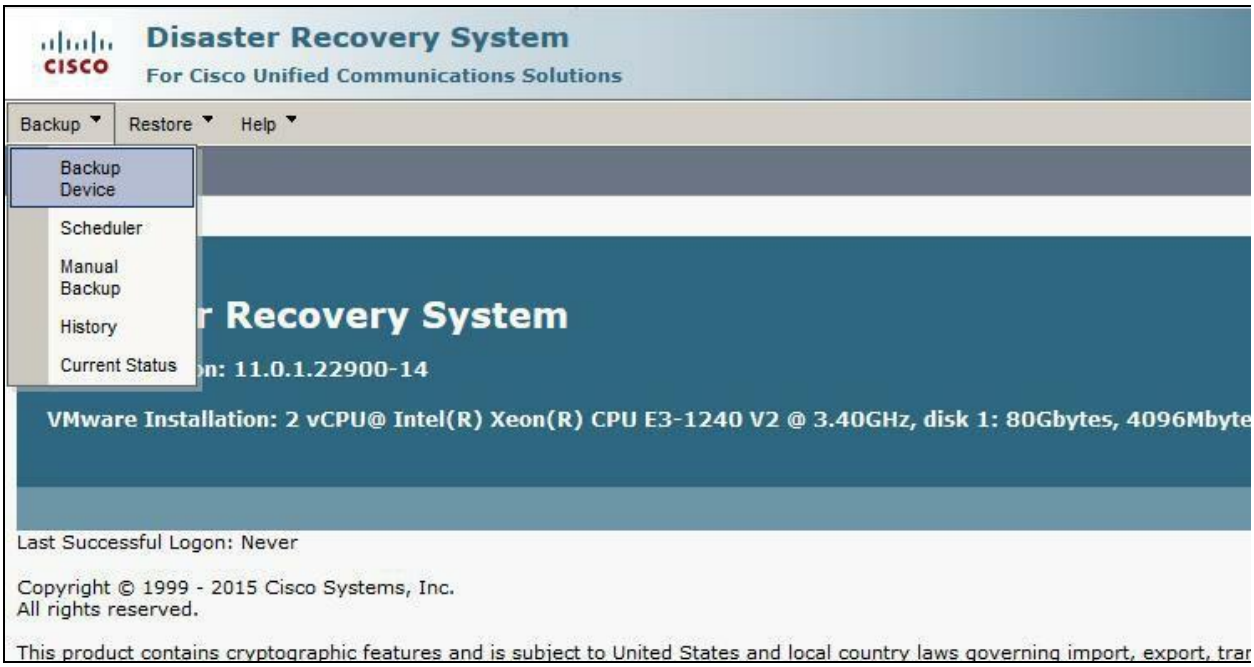


Figure 337 - CUCM DRS Backup Device menu

Insert the name, IP address, and credentials of your SFTP server.

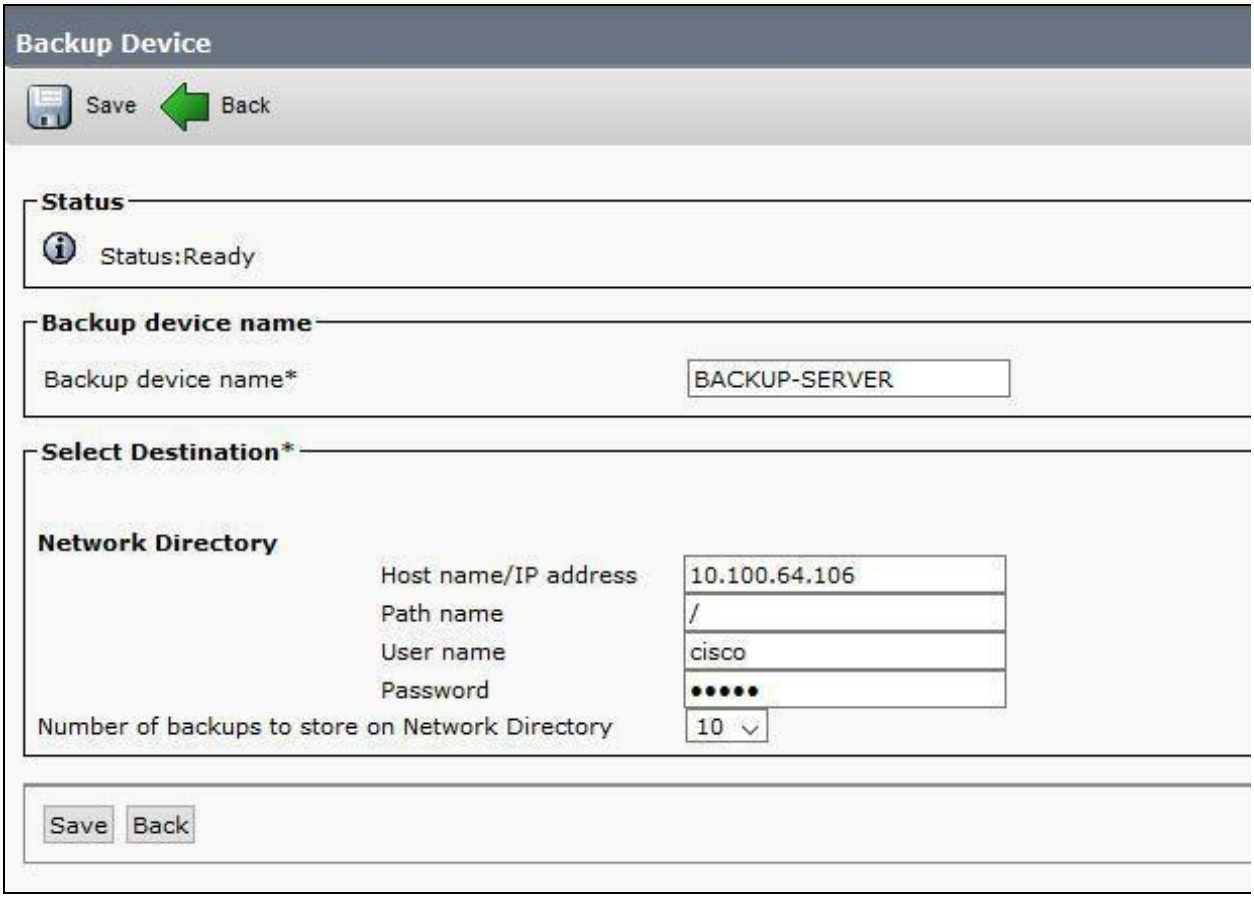


Figure 338 - CUCM DRS Backup Device configuration

Click “Save”. The DRS will try to connect to your SFTP server, and if there is any configuration error, it will not allow for the backup device to be added.

After completing this step, we can proceed to a Manual backup or a Scheduled Backup.

Manual Backup

The Manual Backup is recommended if you want to have an emergency or additional backup apart from your scheduled one. To add it, go to Menu “Backup > Manual”:



Figure 339 - CUCM DRS Manual Backup menu

Select your backup device and choose the features you want to backup (I recommend choosing all of them) and click start. A pop-up window will open with the following message:

> The DRS Backup archive encryption depends on the current security password. During a restore, you could be prompted to enter this security password if this password has been changed.

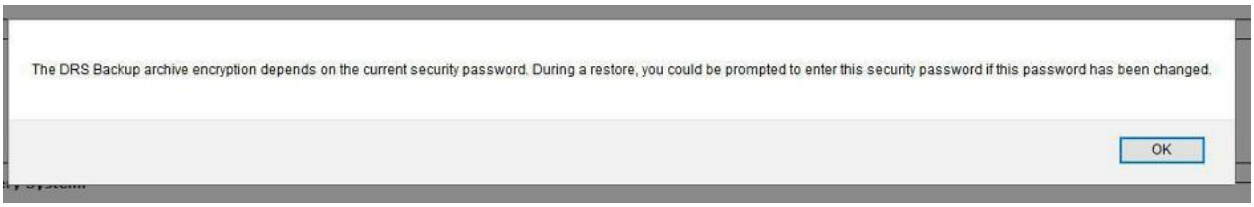


Figure 340 - CUCM DRS Backup alert

Click OK to proceed. You can check your SFTP server logs if the file transfer has started.



Figure 341 - SolarWinds SFTP/SCP Server screen logs

On the Backup Status page, you can check the backup status and process.

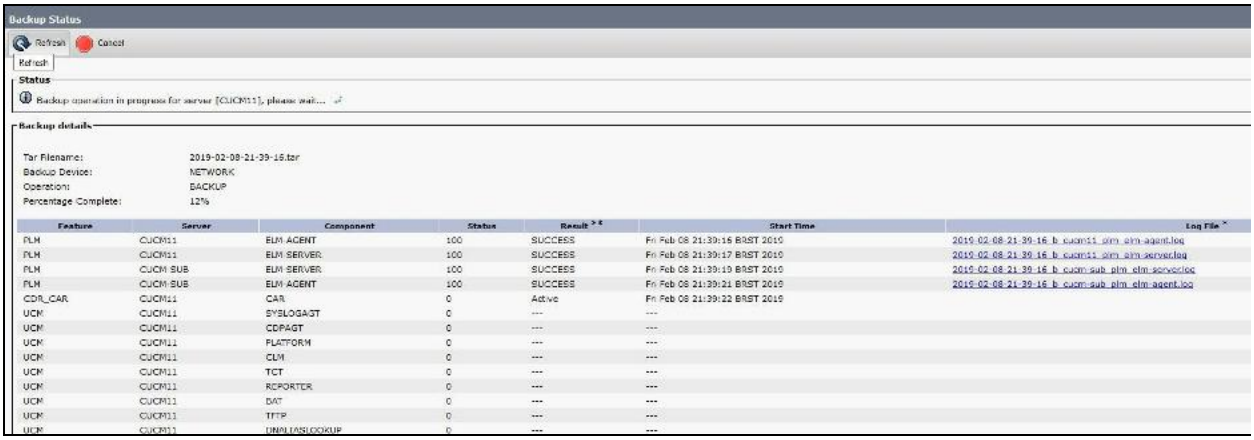


Figure 342 - CUCM DRS Backup Status page

In the end, if no errors happened, you should see a screen like this:

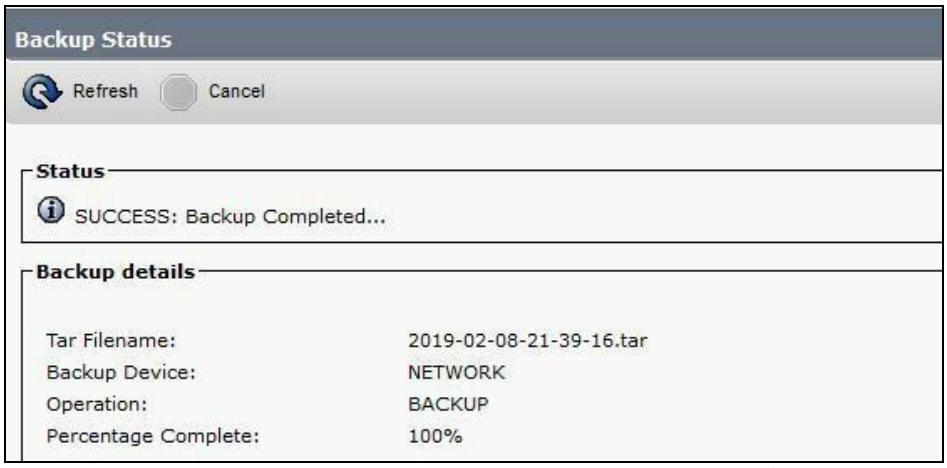


Figure 343 - CUCM DRS Backup completed successfully

You can also open the menu “Backup > History” to check the history of all your backups.



Figure 344 - CUCM DRS Backup History page

Scheduler

To schedule your CUCM Backups, open the menu “Backup > Scheduler”:

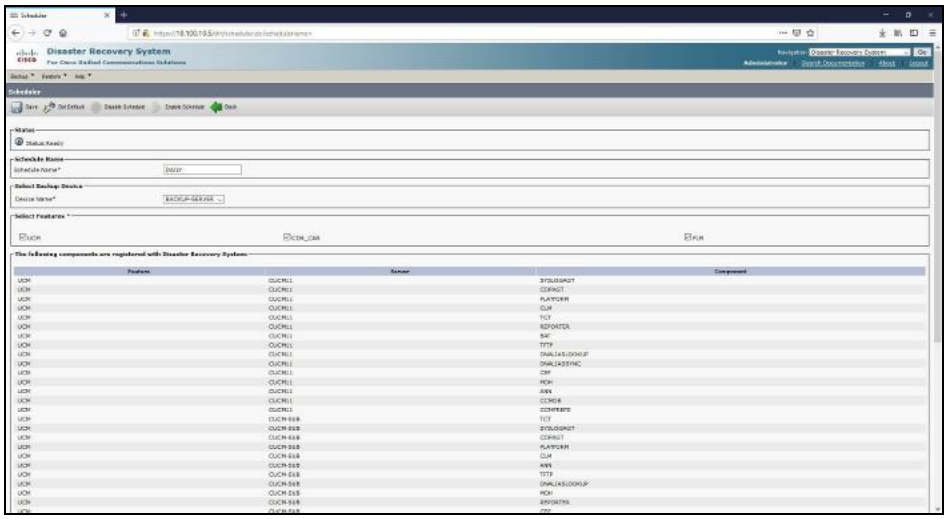


Figure 345 - CUCM DRS Scheduler page

Select the backup device, the features you want to backup (I recommend all the features), the start date and the frequency.



Figure 346 - CUCM DRS Scheduler options

Save it and activate it. Then, click “Back” to return to the Schedule List. The schedule status has to show “Enabled”; if it does not, select it and click “Enable Selected Schedules”.

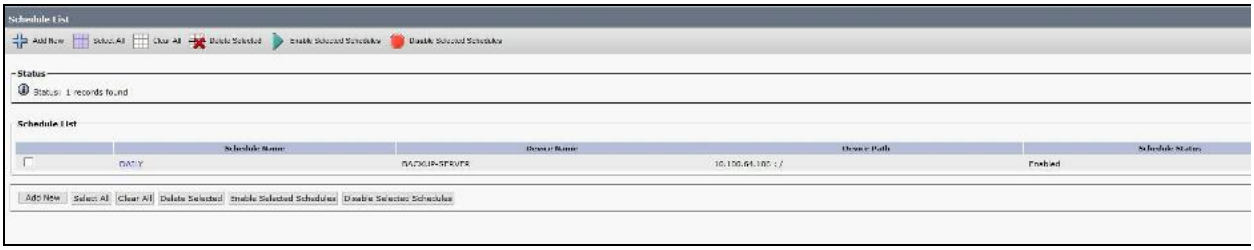


Figure 347 - CUCM DRS Scheduler list

Backup strategy

The backup strategy will depend on how much your telephone system is changed during the weeks. I like to have a daily backup at least during the implementation period. After that, you can change it to weekly backup, as

usually there are not too many system changes. However, if you wish, you can stick with the daily one.

Restore

To restore your CUCM system, the steps are as follows:

Step 1: Go to menu “Restore > Restore Wizard”;

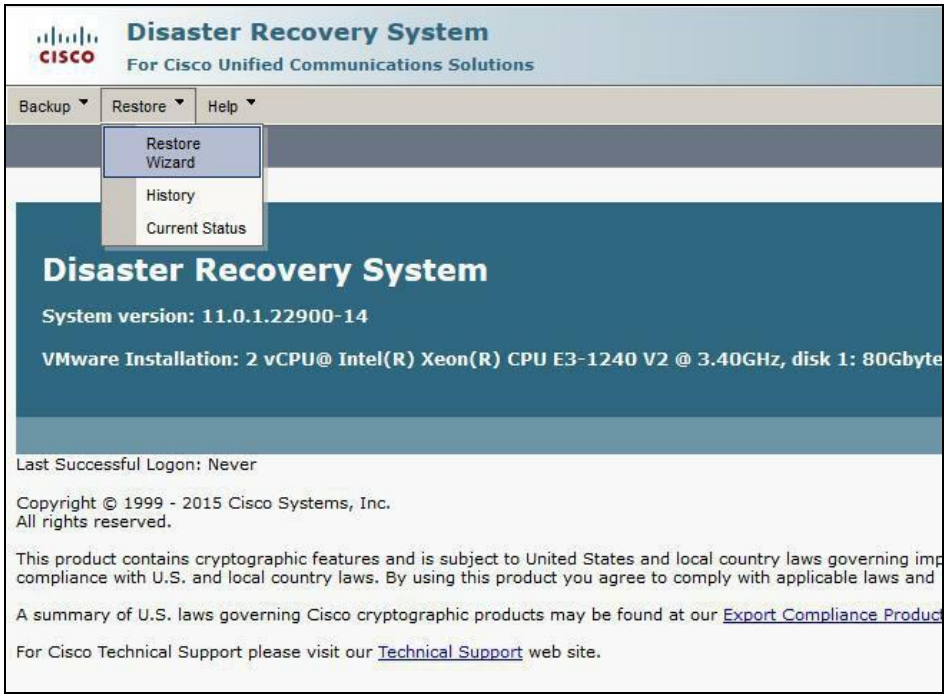


Figure 348 - CUCM DRS Restore Wizard

Step 2:Choose your Backup device;



Figure 349 - CUCM DRS Restore Wizard step 1

Step 3:Select the file you want to restore. You can check the file date and look for the updated file.

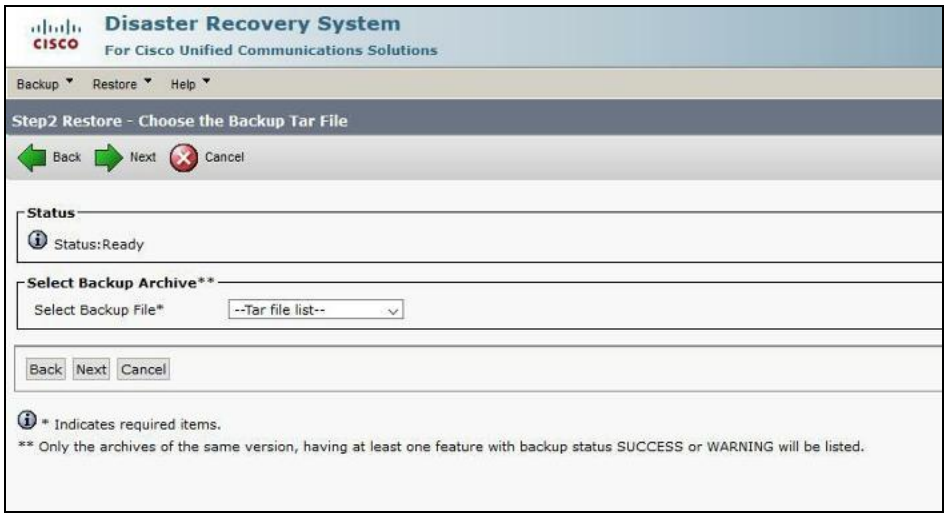


Figure 350 - CUCM DRS Restore Wizard step 2

Step 4:Select the type of the restore;

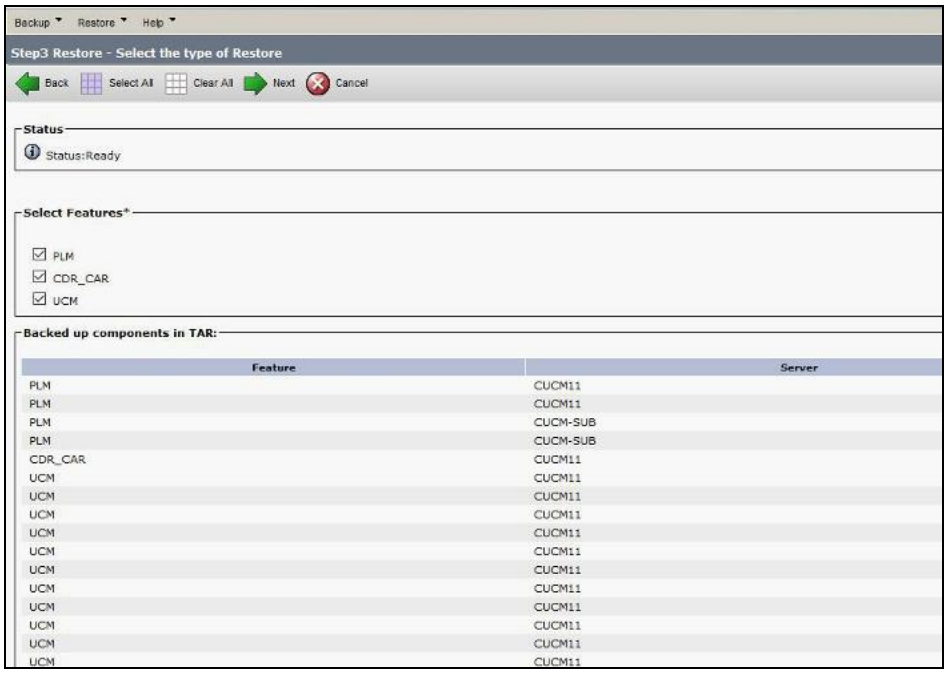


Figure 351 - CUCM DRS Restore Wizard step 3

Step 5: Select the servers you want to use for these restores and finish.

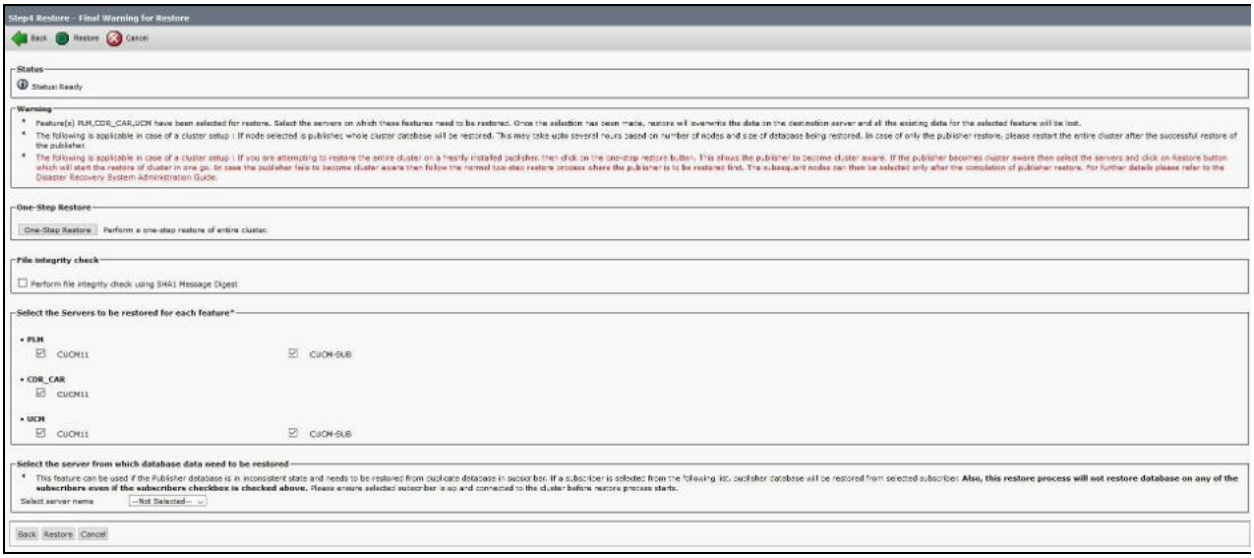


Figure 352 - CUCM DRS Restore Wizard final step

After your restore is completed, you will see a screen like this:

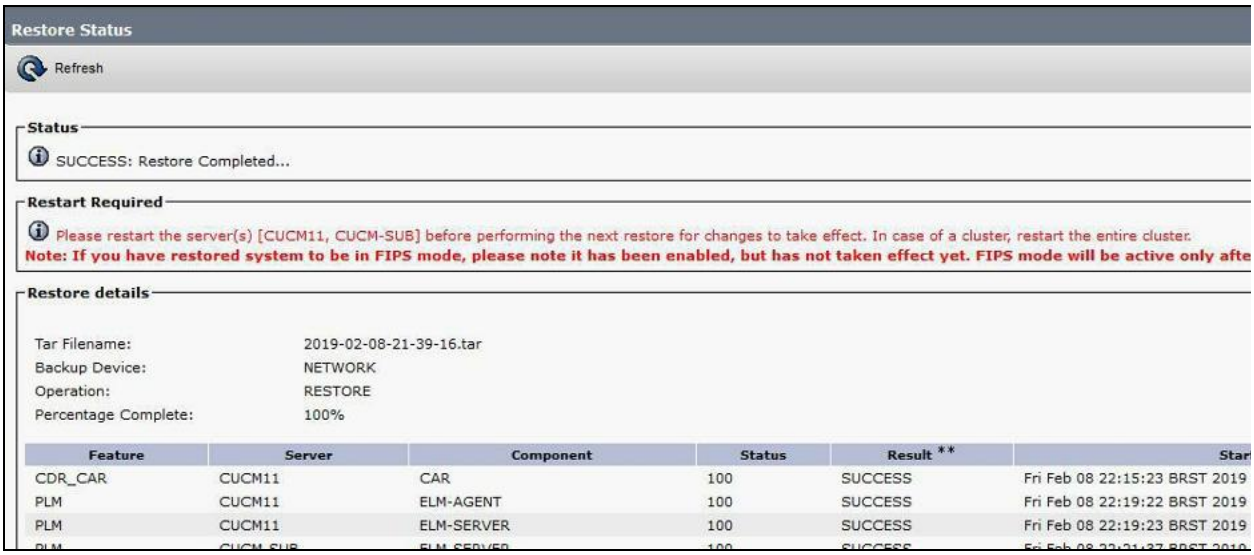


Figure 353 - CUCM DRS Restore completed

Manually copy VM on VMware

If it is an official backup, you can manually copy your VMware CUCM Virtual Machine. It is useful, and I have to admit that this has saved my skin more than once. As I said, try to always use the Cisco DRS as your primary backup system. In case of any problems, these methods can help you as a last resort. Please note that this method requires you to shut down your CUCM server, so you probably need to do it when the maintenance window is open.

Copy via vSphere

To copy the virtual machine, open your vSphere Client, go to “Configuration > Storage” and find the storage where your CUCM VM is located. Right-click on it, and select “Browse Datastore...”.

> **Note:** Please remember that the CUCM Virtual Machine **must be in shutdown state** to proceed.

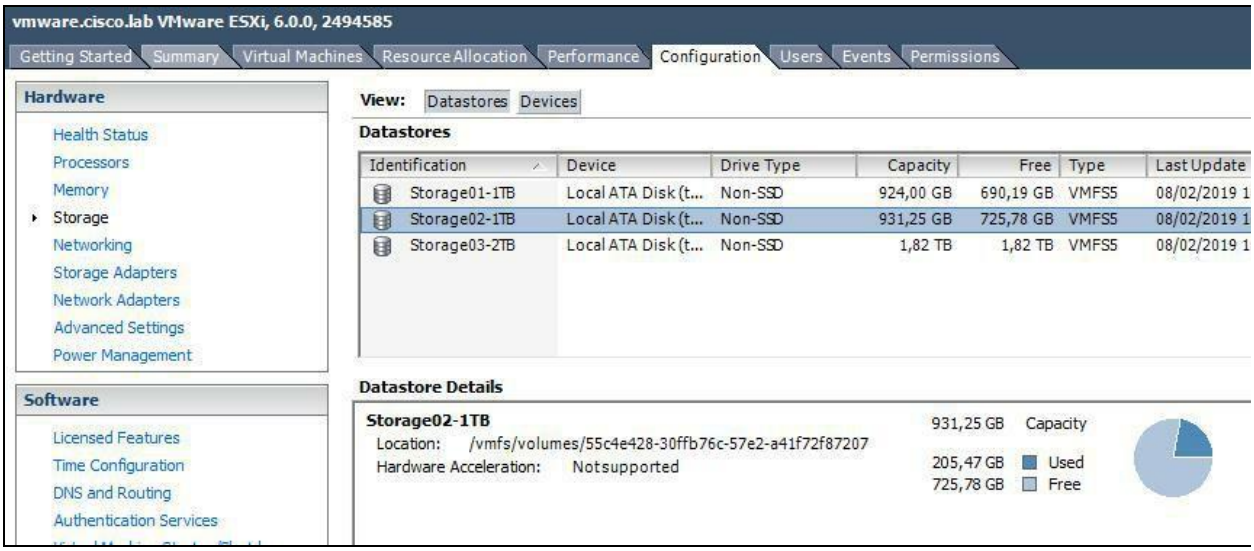


Figure 354 – Vmware Datastore window

Now, select your CUCM installation folder, right-click and select “Copy”.

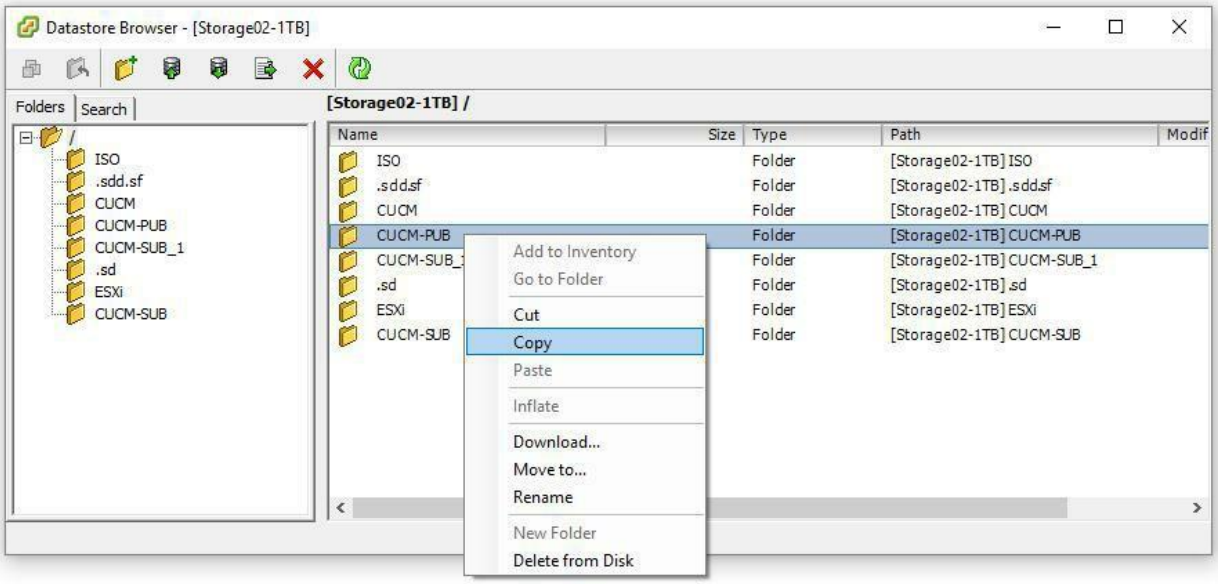


Figure 355 – Vmware Datastore window

Select where you want to copy this VM. For example, you can create a folder with the date of this copy, like I did - “CUCM-copy-08.feb.2019”.

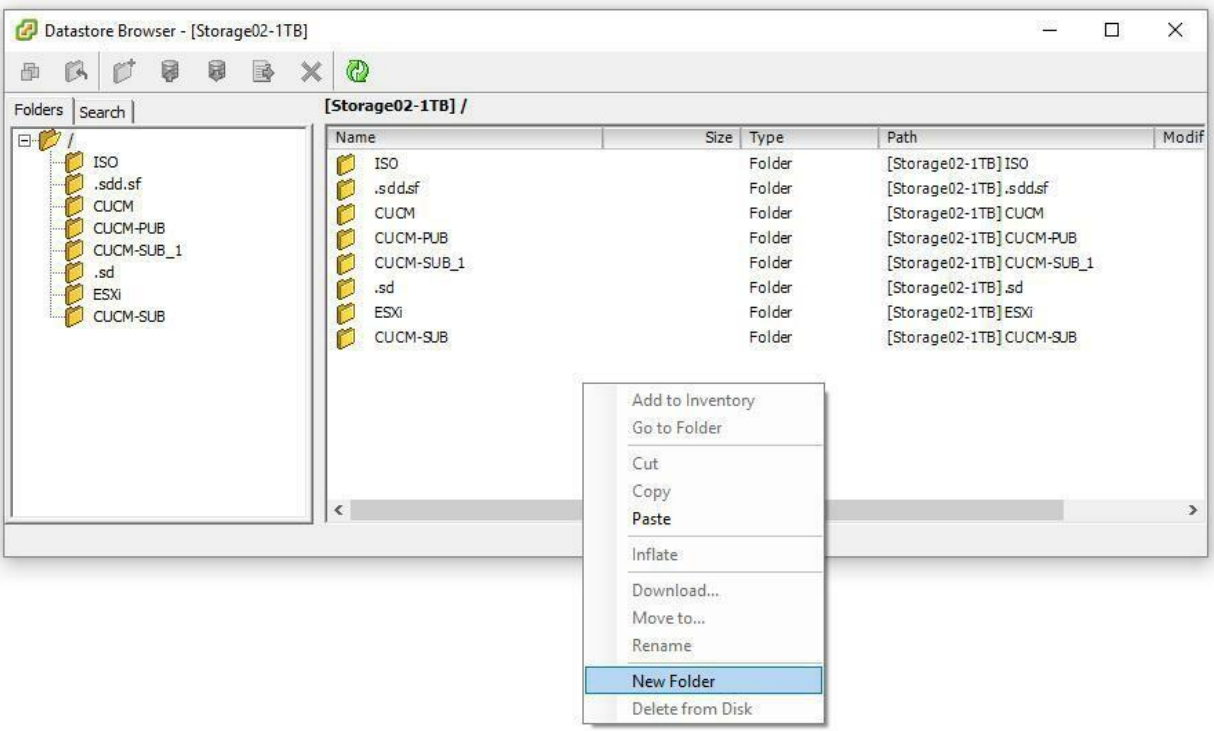


Figure 356 – Vmware Datastore window

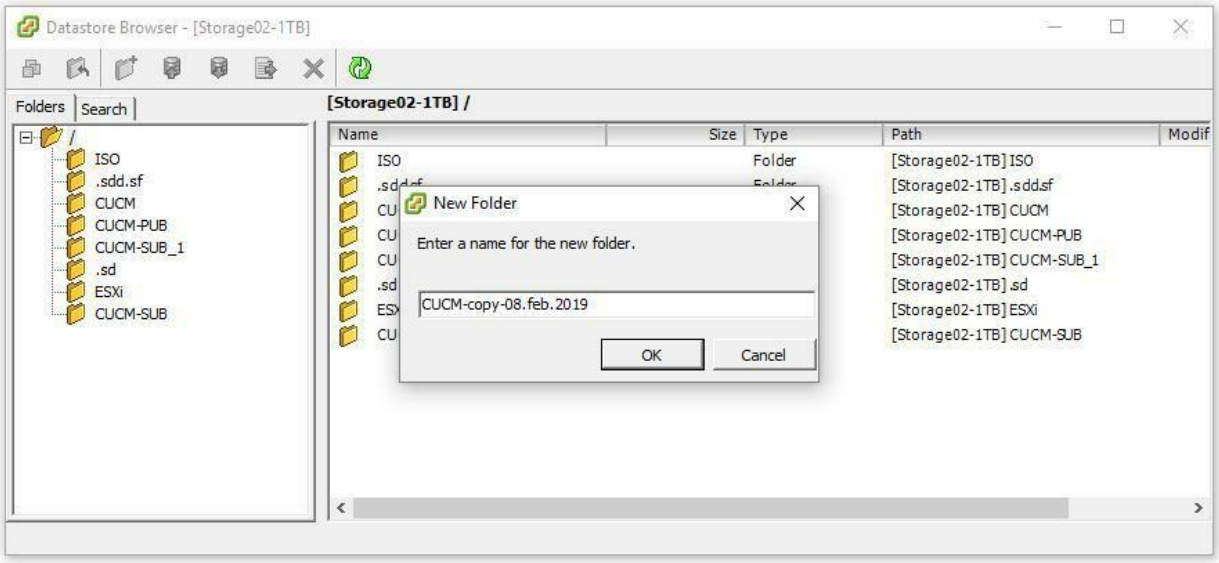


Figure 357 – Vmware Datastore creating folder

Now, enter the folder you have created and paste your CUCM installation.

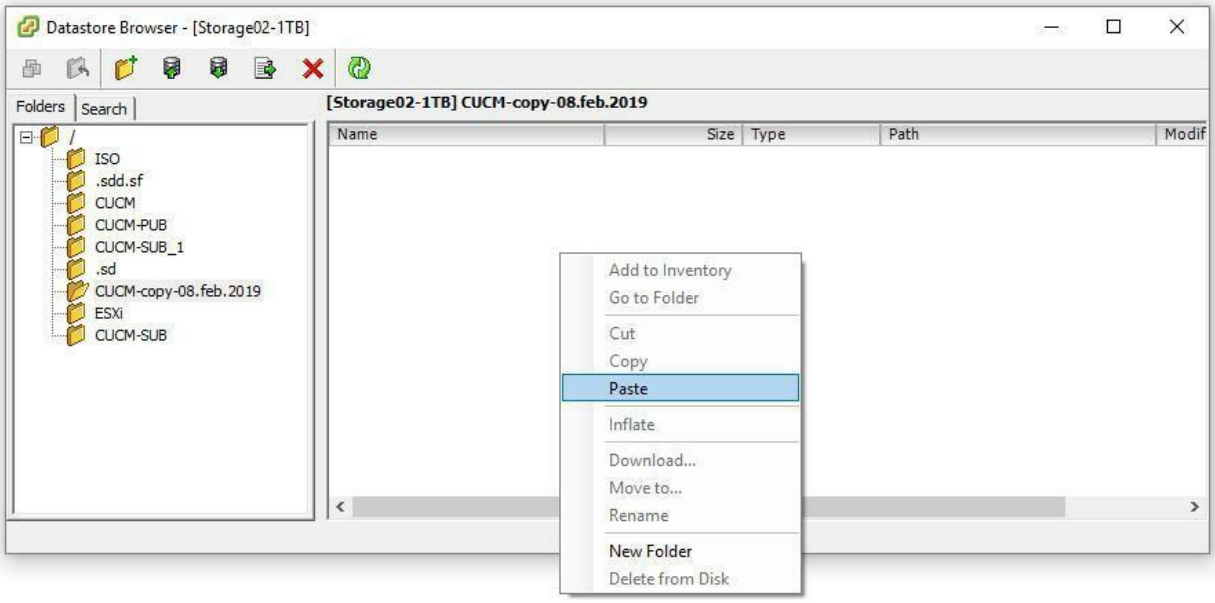


Figure 358 – Vmware Datastore copying folder

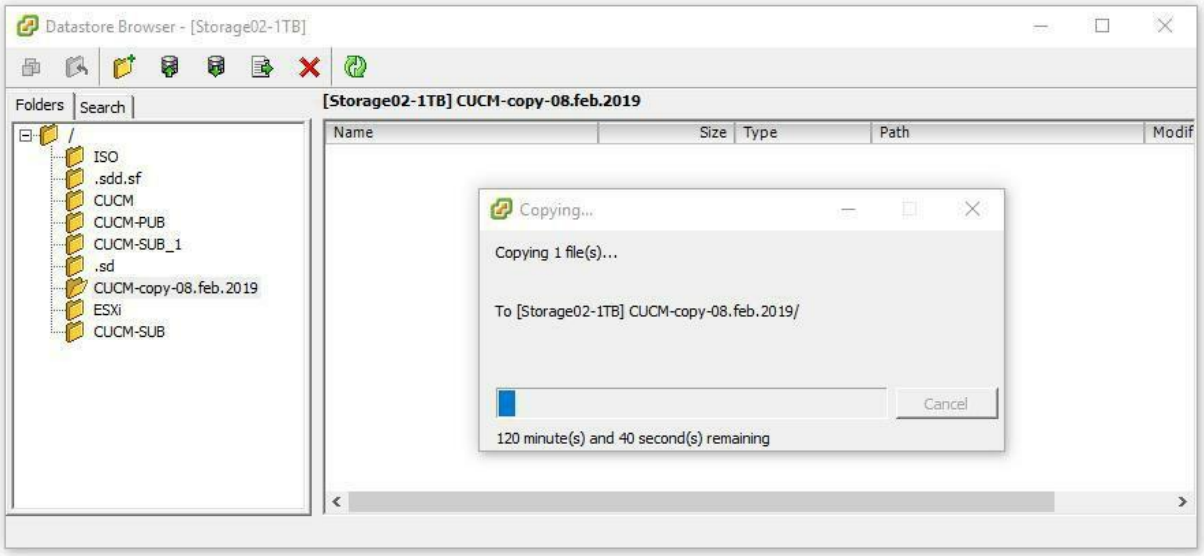


Figure 359 – Vmware Datastore copying folder

After the copying is completed, you can turn on your CUCM server.

You can also copy the CUCM installation folder directly to your computer via the network. It can take more time depending on your network and computer configuration. To save time, maybe you can copy it first to another folder on vSphere Data Storage, turn on your CUCM Virtual Machine and then use the copied VM Folder to download it to your computer. Remember, do not copy a running VM using this method, as it will not work correctly

when you try to restore it.

To download it to your computer, right-click on the installation folder and select “Download”:

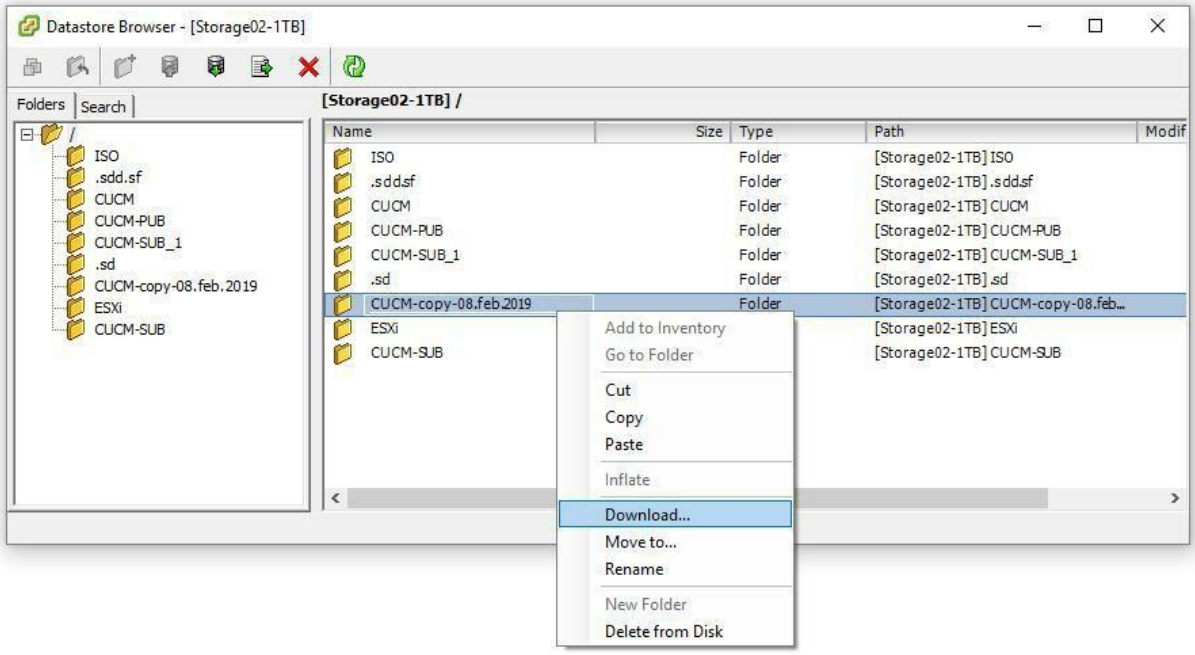


Figure 360 – Vmware Datastore download folder

Select the folder on your Desktop you want to use and click “OK”. The download to your computer will start.

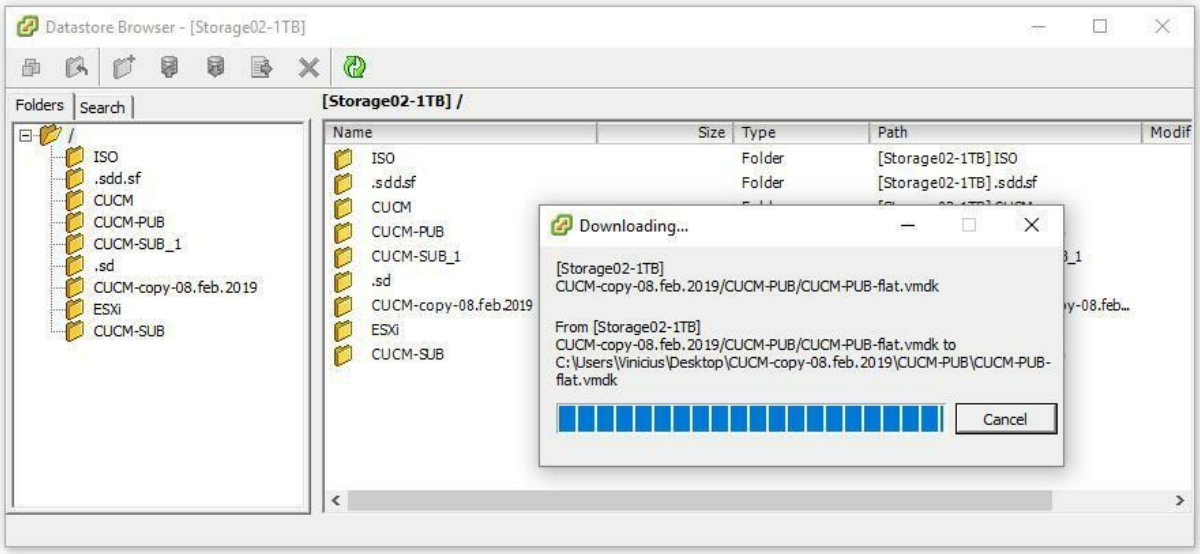


Figure 361 – Vmware Datastore download folder

Copy via SSH

You can copy a VM directly from VMware host to another one using the Linux command SCP. SCP stands for “Secure Copy Protocol”, and it allows for a secure transferring of files between a local host and a remote host or between the two remote hosts. It uses the same authentication and security as the Secure Shell (SSH) protocol it is based on.

To do so, first you need to enable the SSH Protocol on your VMware servers. Access them via vSphere and go to “Configurations > Security Profile > Properties” > Select SSH service and press the Options button > Start the service and press OK to Finish. Now, go back to the Security Profile and in the Firewall section select "Properties" and enable both "SSH Client" and "SSH Server". Click OK to finish.

Repeat this process on both VMware Hosts. Then, go to the server where your CUCM server is installed and run the command:

```
scp -rv  remote_folder user@server_IP:/remote_folder
```

Example:

```
scp -rv /vmfs/volumes/DataStore01/CUCM root@10.101.64.16:/vmfs/volumes/DataStore02/
```

This command will copy the VM “CUCM” located at the DataStore01 of the local VMware server to the remote server 10.101.64.16, on the remote folder “/vmfs/volumes/DataStore02/”.

Restore a manually copied VM

To restore a manually copied VM:

- Open the vSphere Client;
- Click "Configuration”;
- Choose “Storage”;
- Right-click on the appropriate datastore and click Browse Datastore;
- Navigate to the folder named after the virtual machine, and locate

the <virtual machine>.vmx file;

- Right-click the .vmx file and click "Add to inventory"; Add to Inventory wizard opens.

> **Note:** If the wizard asks you if you have "Copied" or "Moved" the virtual machine, always select "I Moved it" to CUCM/CUC/Cisco servers. If you select "I copied it", the VMware will automatically create a new random MAC Address to this virtual machine, and it can impact your Cisco license for this software.

Now, your VM should be visible from the Inventory List, and you can start it.

External Tools

There are other tools from third-party vendors that manage backups from the VMware Virtual Machines. I think one of the most famous ones is Veeam Backup & Replication, from Veeam (https://www.veeam.com). It automatically backups a virtual machine even when it is running and active, but it also has other features such as backup compression, automatic restore to another VMware ESXi Host, backup scheduling, etc.

As I mentioned, at this moment, these tools are not homologated by Cisco. So if we use them and some problems appear, we cannot ask for support from Cisco TAC for these tools.

If you have them in your environment and you would like to use them, you use it on your own risk. I still prefer to use Cisco DRS as this is the only tool officially supported by Cisco TAC Support Team.

CHAPTER 19 – APPENDIX

Here, we will check some other useful information and configurations.

Making a non-bootable ISO image bootable

Original source: http://htluo.blogspot.com/2010/04/how-to-make-non-bootable-iso-image.html

If you are looking for a CUCM image to install on a Lab, you need a bootable ISO file. However, on the Cisco website there are no bootable ISO files to download. Cisco only provides bootable ISO files within Cisco UCS Servers or via “Product Upgrade Tool (PUT)”.

If you need a bootable ISO file, you can make it by “editing” a non-bootable file. Please note that this procedure is not supported by Cisco and should be used ONLY FOR LAB PURPOSES.

To use this procedure, I’m using the software “UltraISO” (http://www.ezbsystems.com/ultraiso/), but you can use other software with similar ISO editing functions.

First, you need to open your CUCM non-bootable ISO file on UltraISO. Then, open the folder "isolinux, select and click “Extract to” and choose the file "isolinux.bin"; extract this file to your desktop.

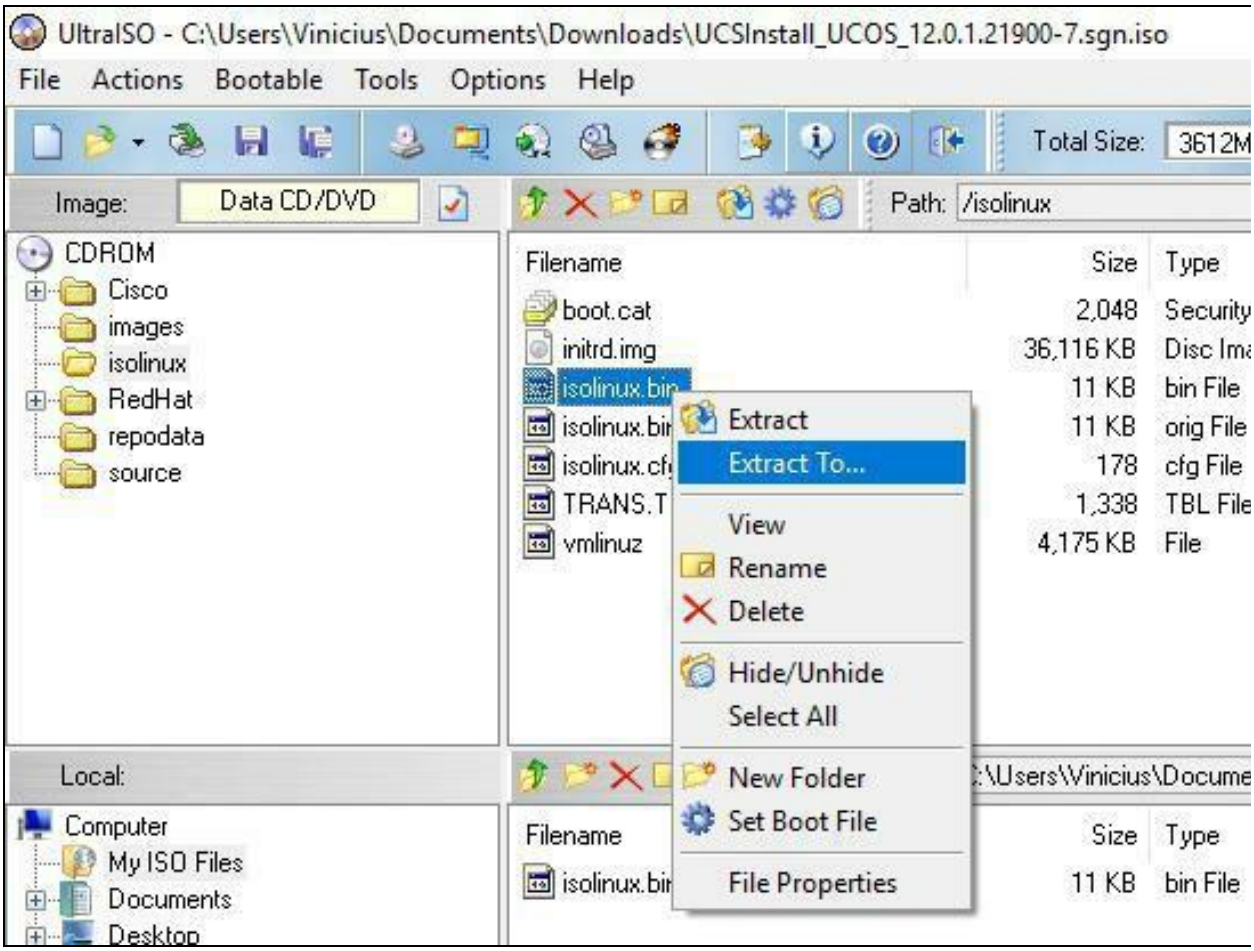


Figure 362 – UltraISO extract "isolinux.bin" file

Now, go to the menu "Bootable" and click "Generate Bootinfotable" to enable it. Then click "Load Boot File..." and select the file "isolinux.bin" you saved on your desktop.
Check, if the image has changed to "Bootable CD/DVD":

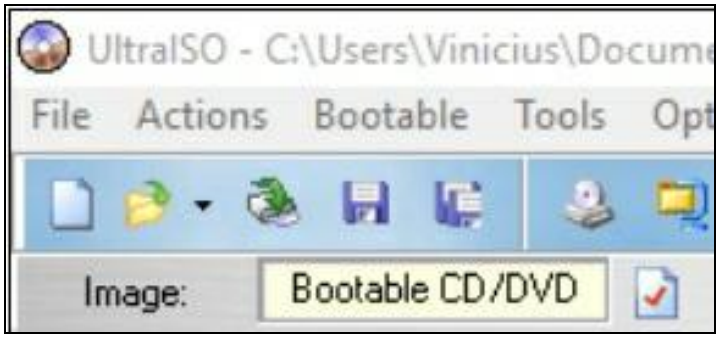


Figure 363 – UltraISO Bootable message

If yes, then the last step is to save it. Go to menu "File > Save As…" and create a name for this file.

CUCM Database Synchronization Check

If the CUCM is acting strangely, like phones that are showing Registered in one CUCM node but Unregistered in another one, you might be facing a Database Synchronization problem.

The best way to check it is to:

- Access your CUCM Publisher server via SSH
- Run the command:

```
utils dbreplication runtimestate
```

```
admin:utils dbreplication runtimestate

Server Time: Sat Feb 16 10:36:32 BRST 2019

Cluster Replication State: BROADCAST SYNC ended at: 2019-02-09-22-38
     Sync Result: SYNC COMPLETED on 692 tables out of 692
     Sync Status: All Tables are in sync
     Use CLI to see detail: 'file view activelog cm/trace/dbl/20190209_223512_dbl_repl_output_Broadcast.log'

DB Version: ccm11_0_1_22900_14
Repltimeout set to: 300s
PROCESS option set to: 1

Cluster Detailed View from CUCM11 (2 Servers):

                                  PING      DB/RPC/   REPL.    Replication    REPLICATION SETUP
SERVER-NAME         IP ADDRESS    (msec)    DbMon?    QUEUE    Group ID       (RTMT) & Details
-----------         ----------    ------    -------   -----    -----------    ------------------
CUCM11              10.100.10.5   0.019     Y/Y/Y     0        (g_2)          (2) Setup Completed
CUCM-SUB            10.100.10.6   0.092     Y/Y/Y     0        (g_3)          (2) Setup Completed
```

Figure 364 – "utils dbreplication runtimestate" command output

The correct scenario is to have “Status 2” in the column “REPLICATION SETUP” applied to all nodes. The replication queue needs to be zero, but it’s not a problem if this number is not zero during a short period, as the servers are always doing some small synchronizations. But after a few minutes, it should always reach “0”.

If It is not your scenario, maybe you need to make a Database Synchronization Recovery. Check below how to do it.

CUCM Database Synchronization Recovery

If you have an active Cisco Smartnet contract, you have access to Cisco TAC Support Team, so you do not need to do this procedure without them. The best way is to call/contact them at http://www.cisco.com/techsupport to help you with this issue.

If you do not have this support, you are on your own. Be careful! Try to make a backup before doing this procedure, at least shut down your CUCM server and copy the virtual machine so you are able to restore it, if necessary. Check Chapter 18, “Backup and Restore”.

First, try to validate if the Database Synchronization Recovery is really necessary. Run the command “utils dbreplication runtimestate”, wait a few minutes, then rerun it, to check if CUCM is automatically solving your database problem or not. For example, if one of your CUCM Subscriber servers was offline for an extended period of time, it can be doing a database recover from CUCM Publisher, and you do not need to do anything, just wait for the recovery process.

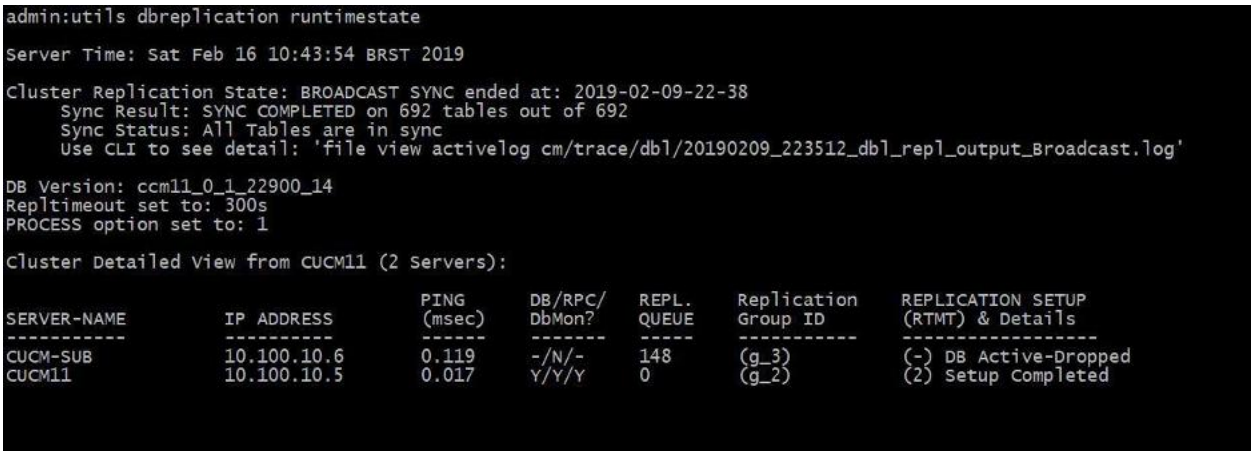


Figure 365 – "utils dbreplication runtimestate" command output

You need to be sure that something is wrong with the recovery process. A symptom of this is a number of the column “REPL. QUEUE” always increasing instead of decreasing.

The database status codes are:

Replication Setup status code	Description
0	Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service has not been running since the subscriber was installed.
1	Replicas have been created, but their count is incorrect.
2	Replication is good. This is what we want.
3	Replication is bad in the cluster.

Technet24

4	Replication setup did not succeed.

Table 47 – Replication Setup status codes

To recover it, the steps are:

Step 1:Only on the CUCM Publisher, run the command:

```
utils dbreplication stop all
```

Step 2:The next command, do it first for all the Subscribers one by one and then on the Publisher:

```
utils dbreplication dropadmindb
```

Step 3:The final command, run it only on the Publisher:

```
utils dbreplication reset all
```

```
admin:utils dbreplication runtimestate

Server Time: Sat Feb 16 17:47:08 BRST 2019

Cluster Replication State: PUB SETUP Started at 2019-02-16-17-45
     Setup Progress: 1 node(s) added to the replication network
     Setup Errors: No errors


DB Version: ccm11_0_1_22900_14
Repltimeout set to: 300s
PROCESS option set to: 1

Cluster Detailed View from CUCM11 (2 Servers):

                                  PING      DB/RPC/   REPL.    Replication    REPLICATION SETUP
SERVER-NAME         IP ADDRESS    (msec)    DbMon?    QUEUE    Group ID       (RTMT) & Details
-----------         ----------    ------    -------   -----    -----------    ------------------
CUCM11              10.100.10.5   0.023     Y/Y/Y     0        (g_2)          (0) Realizing...
CUCM-SUB            10.100.10.6   0.118     Y/Y/Y     --       (-)            (-) Not Requested
```

Figure 366 – "utils dbreplication runtimestate" command output

Type this command and wait. This process will take a few hours. I highly recommend to run it during non-business hours, or even during the weekend, if you can. But I already faced some situations where the system was entirely or partially down, and I ran this command to have the telephone system back online as soon as possible. This command will consider the CUCM Publisher database to be the most updated database, and will rebuild all CUCM Subscribers database by copying it from the Publisher.

Keep typing the command “utils dbreplication runtimestate” to check the status of the field “REPL. QUEUE” and to check the replication queue.

When the replication queue is zero and the status is “2”, your system is back to normal again.

Verify all Extensions created on CUCM

To check all Extensions created on CUC, go to:

- Menu Call Routing > Directory Numbers > Find

Verify all Extensions created on CUCM but not associated with Phones

To check all extensions created on CUCM but not associated with any phone, go to:

- Menu Call Routing > Route Plan Report > Unassigned DN > Find

Verify if a number exist at any place on CUCM

To check if a number exists on CUCM at any place (extension, unassigned extension, route pattern, translation), go to:

- Menu Call Routing > Route Plan Report > Find

Insert Phones via BULK with Handheld Barcode Scanner

If you have a lot of phones to insert on CUCM, you can use a Handheld Barcode Scan to read the MAC Address of all your phones directly from the Phone Boxes.



Figure 367 – Handheld Barcode Scan

With the handheld connect to a PC, open Microsoft Excel and read the MAC Address from the phone. The Microsoft Excel will automatically jump to the next line, and then you can proceed to the next phone.

At the end of the process, you will have a spreadsheet with all your MAC Address, all in the same column, one below the other. Then, you can prepare a script to insert them as a BULK on the CUCM. To do it, check Chapter 15, “BULK Administration”.

You can also use a color pen to write on the phone box the extension, department or username you want to send the phones to, and make it easier to an onsite team to distribute these phones to the correct end users.

Verify an T1 or E1 status on the Voice Gateway

The command to verify a T1 or E1 status on a Voice Gateway is:

```
show controller t1
```

or

```
show controller e1
```

The correct status should be “UP”: If the status is “down”, check internal

cabling and/or contact your PSTN Provider (Telco).

Check ISDN Status on a Voice Gateway

The command to check the ISDN status on a Voice Gateway is:

```
show isdn status
```

The correct scenario should be the Layer 1 Status “ACTIVE” and Layer 2 “MULTIPLE_FRAME_ESTABLISHED”:

```
Router01#show isdn status
Global ISDN Switchtype = primary-qsig
ISDN Serial0:23 interface
        dsl 0, interface ISDN Switchtype = primary-qsig
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
            TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
```

Troubleshoot ISDN Status on a Voice Gateway

To Troubleshoot ISDN Status on a Voice Gateway, the main commands are:

```
debug isdn q921
```

and

```
debug isdn q931
```

To Troubleshoot ISDN Status on a Voice Gateway, the main commands are: The first command will check the Layer 2 connectivity on an ISDN link, and the second will check the Layer 3 connectivity.

Display active calls on a Voice Gateway

Here are some commands to display the active calls on a Voice Gateway:

```
show voice call status
show voice call summary
show call active voice
show call active voice summary
```

Troubleshoot calls on a ISDN Gateway

The main command to troubleshoot calls on an ISDN Gateway is:

```
debug isdn q931
```

If you want to see these calls on real time, do not forget to enable the "terminal monitor"; otherwise, you will only be able to see these logs with the command "show logging".

Troubleshoot calls on a R2 Digital Gateway

The main command to troubleshoot calls on a R2 Digital Gateway is:

```
debug voice ccapi inout
```

This command is not as "clean" as the "debug isdn q931" to do the troubleshoot ISDN call. However, it can be used to verify any kind of call, including R2 Digital, ISDN, H.323, SIP, etc.

Troubleshoot calls on a SIP Trunk

The main command to troubleshoot calls on a SIP Trunk is:

```
debug ccsip calls
```

You can also try some other useful like:

```
debug ccsip messages
debug ccsip errors
debug ccsip events
debug ccsip info
debug ccsip media
```

If none of these were helpful, you have this last command, but take care, as it generates a lot of log messages:

```
debug ccsip all
```

Troubleshoot calls on a H.323 Gateway

The main command to troubleshoot calls on an H.323 Digital Gateway is the same used in the R2 Digital Gateway:

```
debug voice ccapi inout
```

Troubleshoot calls CUCM

Check “Chapter 16 - Call Detail Records”, section “Search for call logs”.

Troubleshoot SIP calls on CUCM

Check “Chapter 17 - Real Time Monitoring Tool”, section “SIP Call traces on RTMT”.

Preparing CUCM MoH File with Audacity

You can use the audio editing software “Audacity” to prepare the CUCM Music On Hold audio files. It is free and can be downloaded from:

https://www.audacityteam.org/download/

I am using Audacity version 2.2.2, so these options can be a little bit different. It goes as follows:

1. Open Audacity;
2. Open the audio file you are going to use (Menu File > Open...);
3. On the top left corner, open this menu:

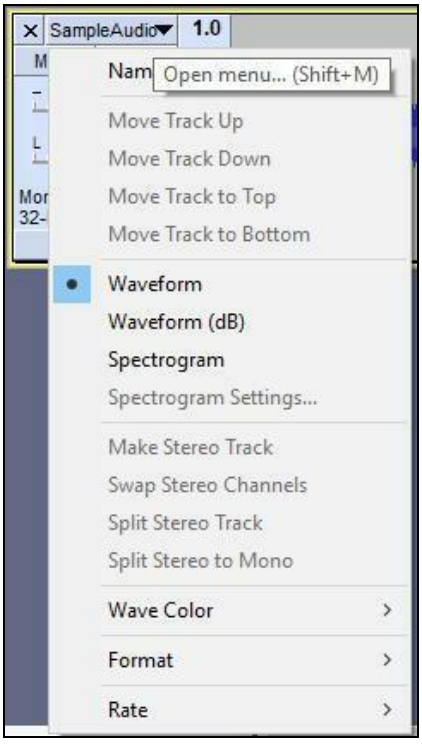


Figure 368 – Audacity menu

4. Here, go to option “Rate” and select “8000”;
5. In the same menu, select the option “Split Stereo to Mono”; delete one of the 2 tracks;
6. Again, in this menu, change the "Format" to "16-bit PCM";
7. You should see “Mono, 8000Hz 16-bit PCM” in your file description

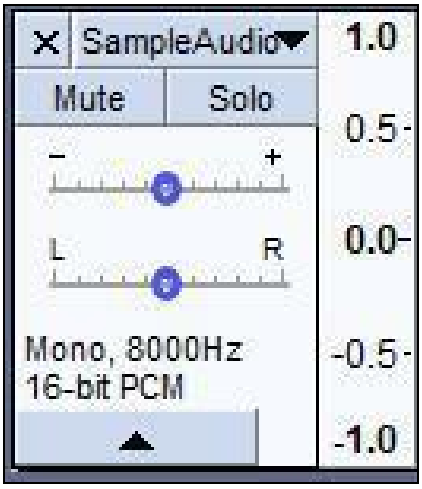


Figure 369 – Audacity menu

8. Now select from the menu "File> Export > as WAV";
9. Choose the name of the file without using spaces in the file name;
10. From this screen select:
11. File type: "Other uncompressed files"
12. Header: "WAV (Microsoft)"
13. Encoding: "U-Law"
14. Save it.

Preparing CUCM MoH File with ffmpeg command

If you use Mac OS or Linux, there is also a command line tool for this: ffmpeg (you may need to download it).

The syntax of the command is:

ffmpeg -i file.mp3 -ar 8000 -ac 1 -ab 64 file.wav -ar 8000 -ac 1 -ab 64 -f

mulaw

This command transforms the file "file.mp3" into "file.wav". You can use it also to transform a WAV file into the WAV file in the correct format.

(maybe you need to execute it as ./ffmpeg if running it in the same folder where the ffmpeg file is located)

Preparing CUCM MoH File with online sites

You can google it and find some websites which can be used to convert the Cisco Music on hold file, such as:

http://kernelmanic.com/call-manager-and-asterisk-audio-converter/

Please note that I am not the responsible for this site and it can go offline in the future.