Cube and Advanced Dial Plan

Lab Guide

October 4, 2023

Presented by: Cisco's Solutions Readiness Engineering Team

Lab Objectives

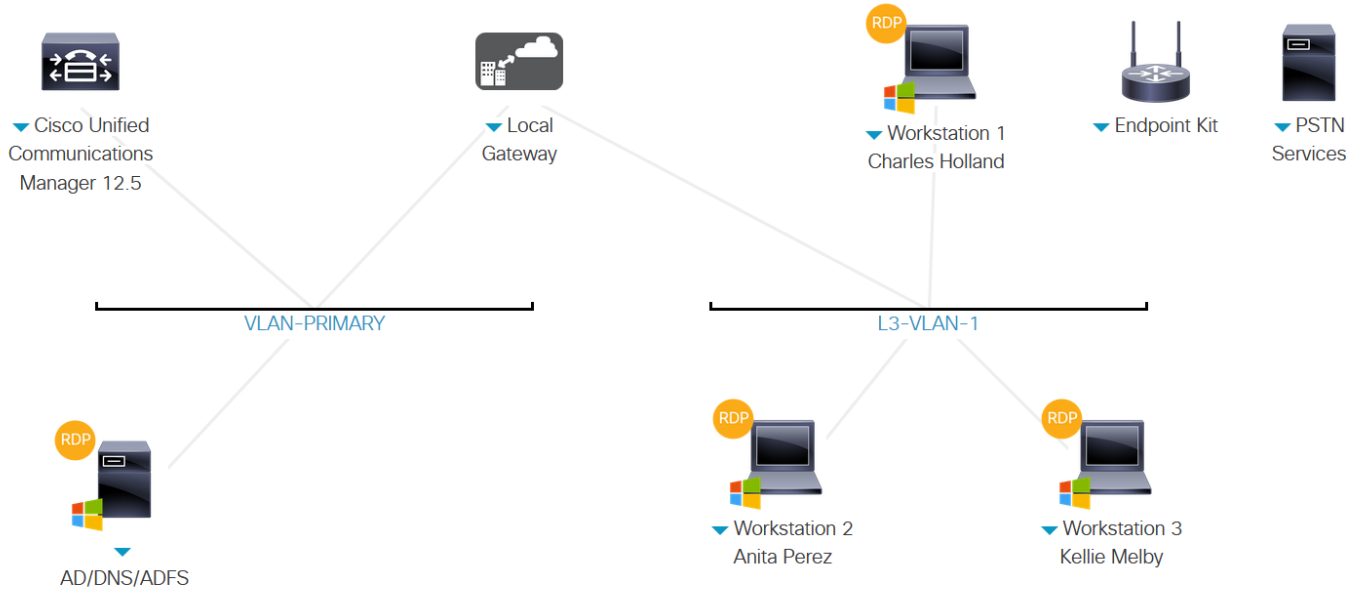
Upon completion of this lab, you will be able to: • Configure the Local Gateway for migration scenarios where you have CUCM as the access to the PSTN. • Fully understand all the configuration required to configure a Local Gateway in a customer deployment integrated with an existing on-prem CUCM. • Configure the Webex Calling solution to route internal calls to the CUCM using the Local Gateway keeping the on-prem dial plan..

About this Lab

This hands-on lab will help you understand the overall architecture of the Webex Calling solution, including Local Gateway configuration in a migration scenario where the deployment has an on-prem CUCM. You will start by enabling a user for Webex Calling in the Control Hub portal. Then you will configure the premises-based PSTN option available for Webex Calling that is connected to an on-prem CUCM using the dial plan options to keep the on-prem dial plan while the users are migrated to Webex Calling.

Lab Topology

This lab includes several server virtual machines including LGW based upon CSR1000v to simulate PSTN access. The Local Gateway are fully configurable using the administrative level account. Administrative account details are included in the lab guide steps where relevant and in the Equipment Details.


Cisco Unified Communications Manager 12.5
Local Gateway
RDP
Workstation 1 Charles Holland
Endpoint Kit
PSTN Services
VLAN-PRIMARY
L3-VLAN-1
RDP
AD/DNS/ADFS
RDP
Workstation 2 Anita Perez
RDP
Workstation 3 Kellie Melby

Equipment Details

Name	Description	Host Name (FQDN)	IP Address	Username	Password
Local Gateway	CSR 1000V	N/A	198.18.133.226	Admin	dCloud123!
Webex Control Hub	Webex Management	N/A	N/A	cholland@cbxxx.dc-yy.com	dCloudzzzz!
Workstation 1	Windows 10	wkst1.dcloud.cisco.com	198.18.1.36	dcloud\cholland	dCloud123!
Workstation 2	Windows 10	wkst1.dcloud.cisco.com	198.18.1.37	dcloud\aperez	dCloud123!

Session Users

This table details the preconfigured users available for your session.

User Name	User ID	Password*	Endpoint Devices	Internal Extension
Charles Holland	cholland@cbxxx.dc-yy.com	dCloudzzzz!	Webex App	N/A
Rebekah Barretta	rbarretta@cbxxx.dc-yy.com	dCloudzzzz!	Webex App	6022
Anita Perez	aperez@cbxxx.dc-yy.com	dCloudzzzz!	Jabber	6017

* The passwords for the session users in this lab have been added to a text file located on Charles Holland's remote desktop (Workstation 1). The name of the text file is **WEBEX_PASSWORD.txt**.

Scenario 1: Webex Calling – Local Gateway

Imagine being able to leverage enterprise-grade cloud calling, mobility, and PBX features, along with Webex App for messaging and meetings and calling from a Webex Calling soft client or Cisco device. That's exactly what Webex Calling has to offer you. Webex Calling provides the following benefits:

- Calling subscriptions for telephony users and common areas
- Webex App access for every user
- Public Switch Telephony Network (PSTN) access to let your users dial numbers outside the organization. The service is provided through an existing enterprise infrastructure (local gateway without on-premises IP PBX or with existing Unified CM call environment)

The local gateway is an enterprise or partner-managed edge device for Public Switch Telephony Network (PSTN) interworking and legacy public branch exchange (PBX) interworking (including Unified CM).

You can use Control Hub to assign a local gateway to a location, after which Control Hub provides parameters that you can configure on the CUBE. These steps register the local gateway with the cloud, and then PSTN service is provided through the gateway to Webex Calling users in a specific location.

The local gateway can be deployed standalone or in deployments where integration into Cisco Unified Communications Manager is required. For this specific lab the Local Gateway is deployed integrating Cisco Unified Communications Manager in a customer migration scenario.

- Task 1: Getting Started
- Task 2: Adding a Location in Webex Control Hub
- Task 3: Enable User with Webex Calling, Assign User to New Location
- Task 4: Add a Trunk
- Task 5: Add a Route Group
- Task 6: Assign Route Group to a Location
- Task 7: Assign a Phone Number to a Location and User
- Task 8: Dial Plan to Route Internal Calls from CUCM to Webex Calling

Task 1: Getting Started

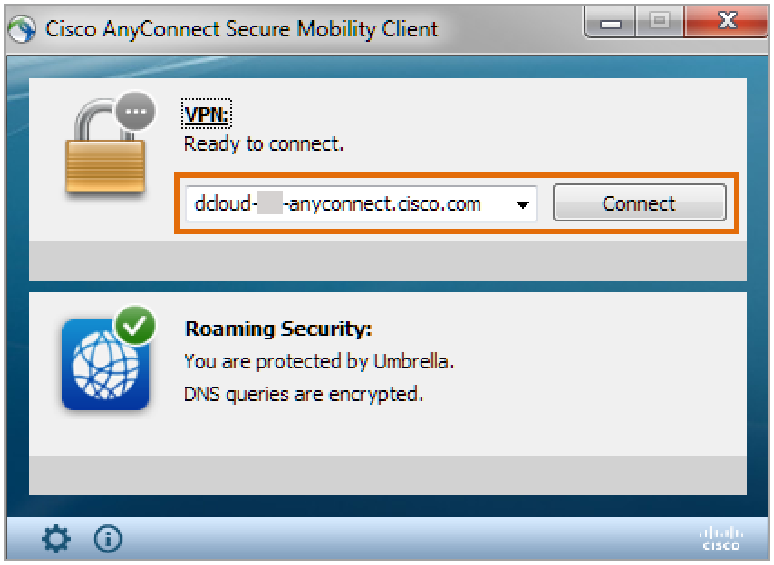
To access your Hands-on lab, you will need to log into dCloud with the AnyConnect VPN. Use the information provided by your lab proctor to complete the following steps:

Activity Procedure

Complete these steps:

Step 1 Open the Cisco AnyConnect client on your laptop.

Step 2 Enter the Host URL provided by your proctor in the URL Connection textbox in the AnyConnect login window, and then click **Connect.**



VPN:
Ready to connect.

dcloud-[redacted]-anyconnect.cisco.com

Roaming Security:
You are protected by Umbrella.
DNS queries are encrypted.

Note If you get a connection error, remove the “https://” part of the URL and try the connection again.

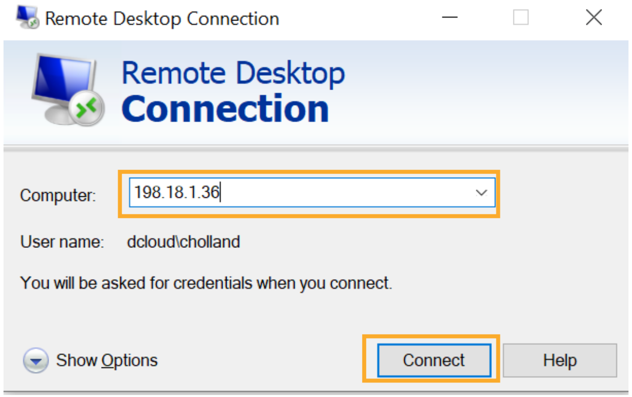
Step 3 On the popup window, enter the **User ID** and the **password** provided by your proctor.

Step 4 Click **OK**

Step 5 Click **Accept** on the window confirming your connection.

Note When connected to your AnyConnect VPN session, the AnyConnect VPN icon is displayed in the system tray (windows) or task bar (mac).

Step 6 Once AnyConnect has established a VPN connection to your assigned pod, **open Remote Desktop** on your computer.



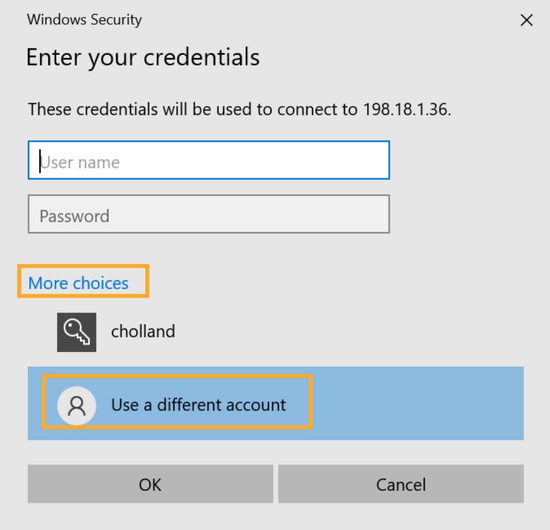
Computer: 198.18.1.36

User name: dcloud\cholland

You will be asked for credentials when you connect.

Step 7 Enter the IP address **198.18.1.36** for **Workstation 1** in the textbox labeled **Computer**, and then click on the **Connect.**

Step 8 Next, you will be given a Windows Security logon. First, click **More choices**, then click **Use a different account.**



Windows Security

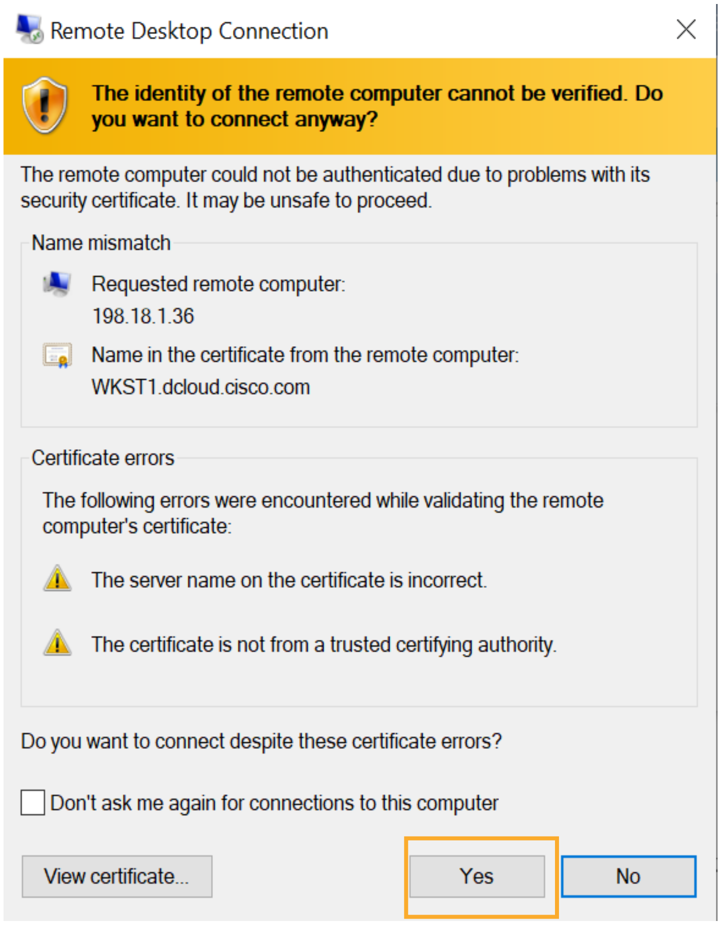
Enter your credentials

These credentials will be used to connect to 198.18.1.36.

Step 9 In the Username field, enter **dcloud\cholland**.

Step 10 In the **Windows Security** window that displays, enter the password **dCloud123!** And click **OK.**

Step 11 Click **Yes** on the certificate window when it displays. You should be logged into Workstation 1 at this time.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Name mismatch

Requested remote computer:
198.18.1.36

Name in the certificate from the remote computer:
WKST1.dcloud.cisco.com

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The server name on the certificate is incorrect.

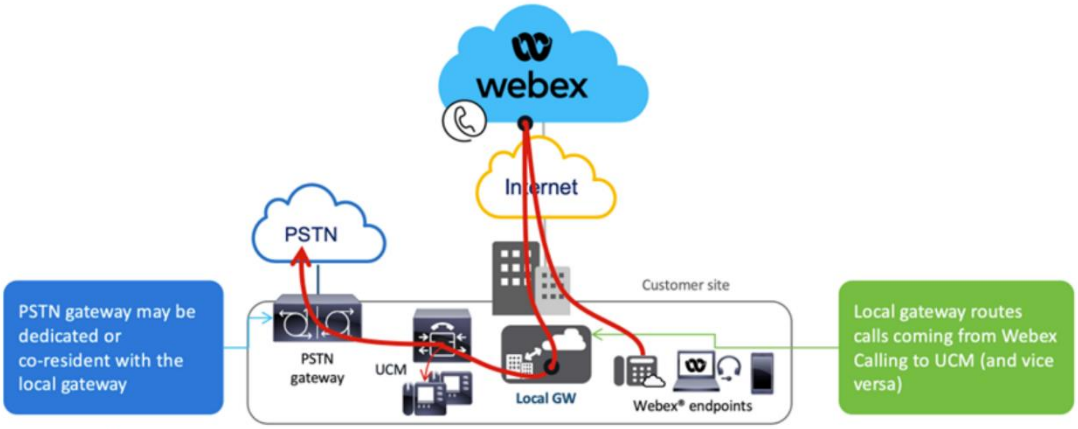
The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

☐ Don't ask me again for connections to this computer

Task 2: Adding a Location in Webex Control Hub

Location is a concept in Webex Calling to group users in the calling service perspective to have the same access to the PSTN and to have specific policies and configurations for all. A location in Webex Calling is an office, geographic location, specific building, or even a physical location. In this scenario, you configure a “WxC-Mig-Bootcamp-HQ” location where you have users assign and where you configure the access to the PSTN using a Local Gateway.


webex
Internet
PSTN
Customer site
PSTN gateway may be dedicated or co-resident with the local gateway
PSTN gateway
UCM
Local GW
Webex® endpoints
Local gateway routes calls coming from Webex Calling to UCM (and vice versa)

Activity Procedure

Complete these steps:

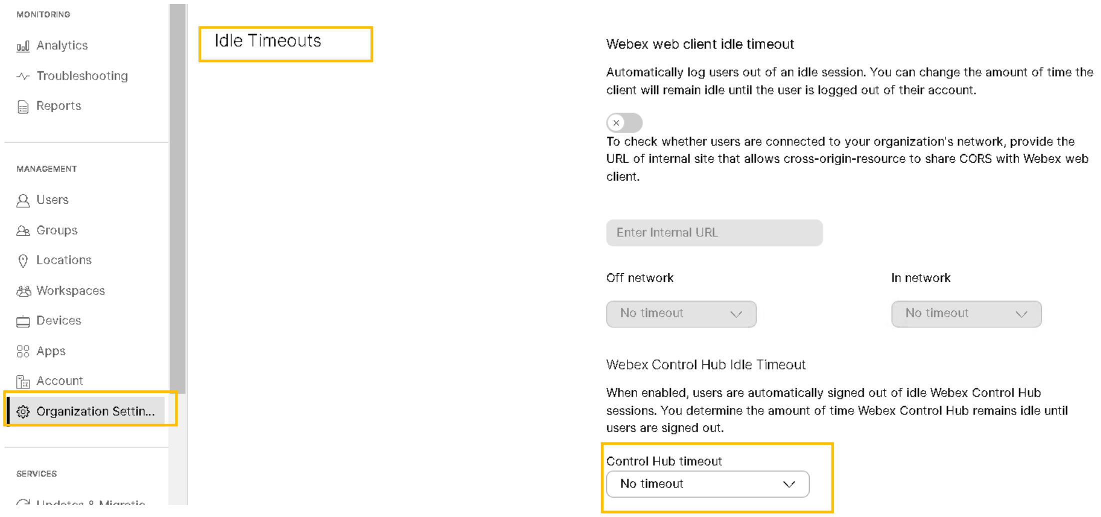
Step 1 Open Chrome web browser. Navigate to https://admin.webex.com and enter cholland@cbXXX.dc-YY.com where XXX and YY are specific to your lab session. You can find this information in your lab Resource tab. Click **Sign In.**

Step 2 Enter dCloudZZZZ! as the password and click **Sign In** again. Replace ZZZZ with the last four digits of your dCloud Session ID.

Note The password is also located on cholland’s desktop in a text file named, WEBEX_PASSWORD.txt.

Step 3 Click **Accept** on the Terms of Service pop-up window.

Step 4 In order to improve your experience in this lab, you can configure the Control Hub idle time-out to **No timeout**. This will allow you to avoid periodically signing in the Control Hub. In order to extend the idle timeout, navigate to **Management > Organization Settings** in the left panel. Configure the Control Hub timeout to **No timeout** under the Idle Timeouts.



Idle Timeouts

Webex web client idle timeout

Automatically log users out of an idle session. You can change the amount of time the client will remain idle until the user is logged out of their account.

To check whether users are connected to your organization's network, provide the URL of internal site that allows cross-origin-resource to share CORS with Webex web client.

Enter Internal URL

Off network: No timeout

In network: No timeout

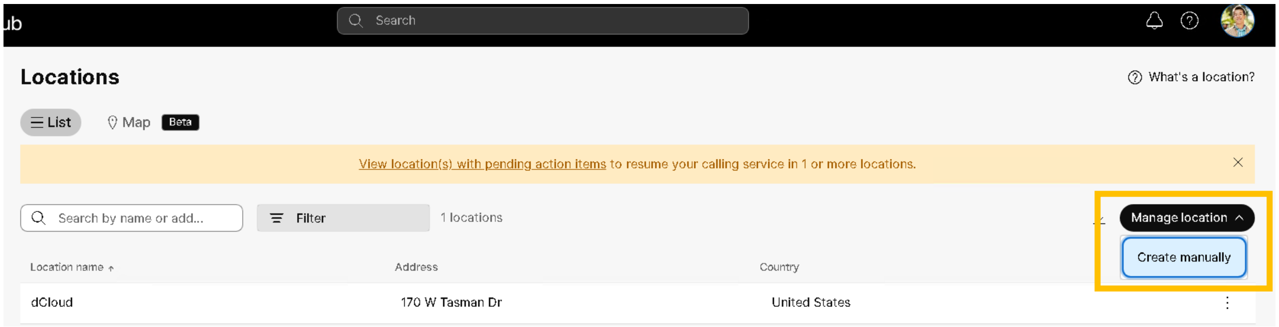
Webex Control Hub Idle Timeout

When enabled, users are automatically signed out of idle Webex Control Hub sessions. You determine the amount of time Webex Control Hub remains idle until users are signed out.

Control Hub timeout: No timeout

Step 5 Now you will configure a new Location for this organization. On the left panel, select **Management** > **Locations.**

Step 6 In the top, right-hand corner, click **Manage Location**. Then select **Create manually**.



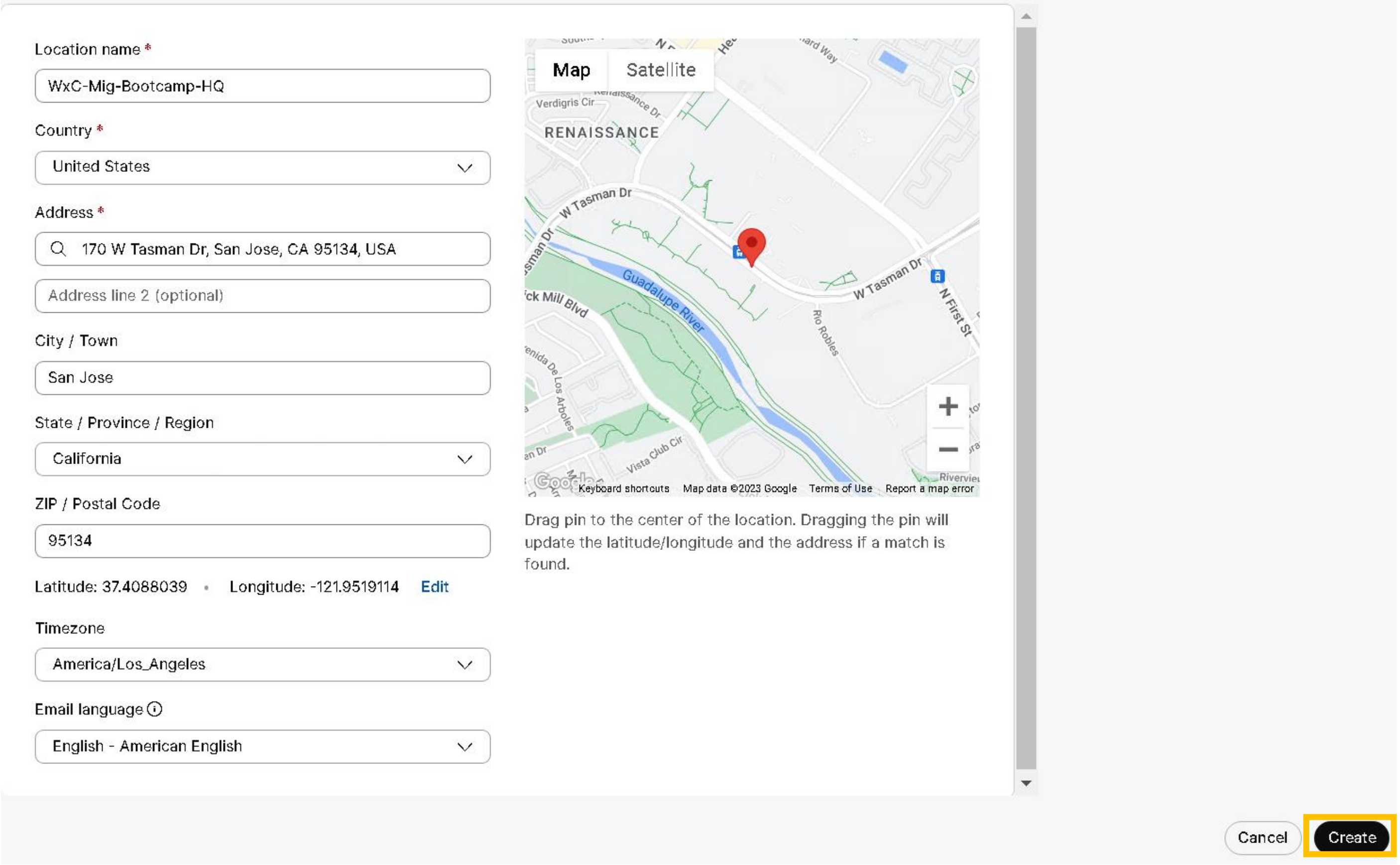
Locations

What's a location?

View location(s) with pending action items to resume your calling service in 1 or more locations.

Location name	Address	Country
dCloud	170 W Tasman Dr	United States

Step 7 Fill in the fields with the following information.



Location name *
WxC-Mig-Bootcamp-HQ

Country *
United States

Address *
170 W Tasman Dr, San Jose, CA 95134, USA

Address line 2 (optional)

City / Town
San Jose

State / Province / Region
California

ZIP / Postal Code
95134

Latitude: 37.4088039 • Longitude: -121.9519114 Edit

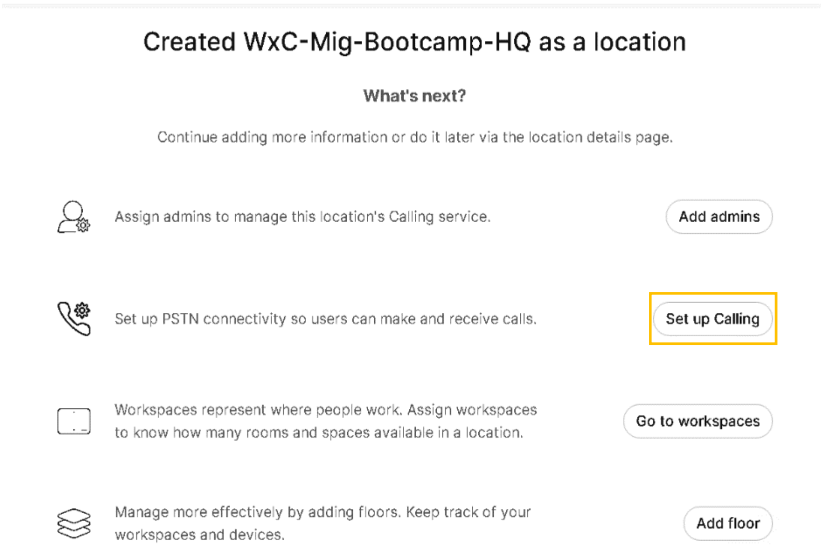
Timezone
America/Los_Angeles

Email language
English - American English

Drag pin to the center of the location. Dragging the pin will update the latitude/longitude and the address if a match is found.

Step 8 Click **Create.**

Step 9 On the next screen, click **Set up Calling.**



Created WxC-Mig-Bootcamp-HQ as a location

What's next?

Continue adding more information or do it later via the location details page.

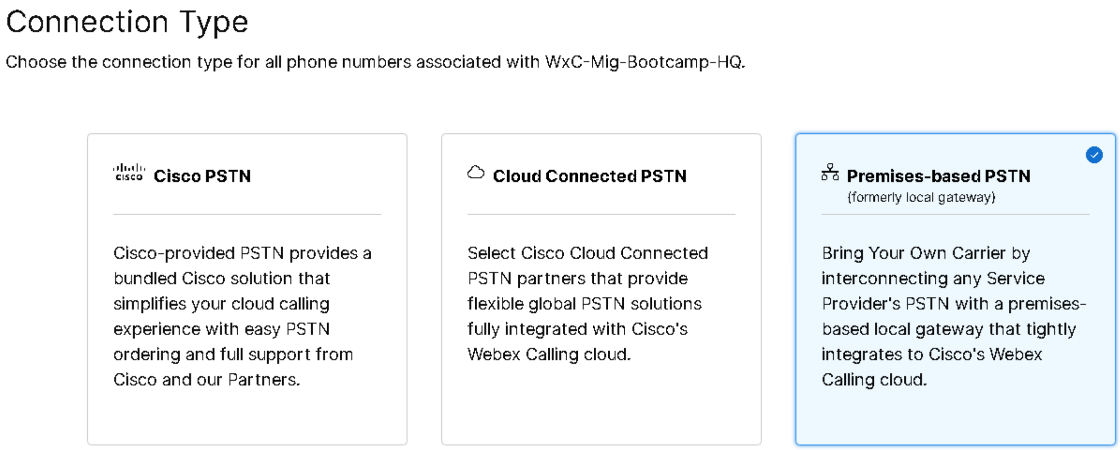
Assign admins to manage this location's Calling service.

Set up PSTN connectivity so users can make and receive calls.

Workspaces represent where people work. Assign workspaces to know how many rooms and spaces available in a location.

Manage more effectively by adding floors. Keep track of your workspaces and devices.

Step 10 On the **Connection Type** page, select **Premises-based PSTN**. Click **Next**.



Connection Type

Choose the connection type for all phone numbers associated with WxC-Mig-Bootcamp-HQ.

Cisco PSTN

Cisco-provided PSTN provides a bundled Cisco solution that simplifies your cloud calling experience with easy PSTN ordering and full support from Cisco and our Partners.

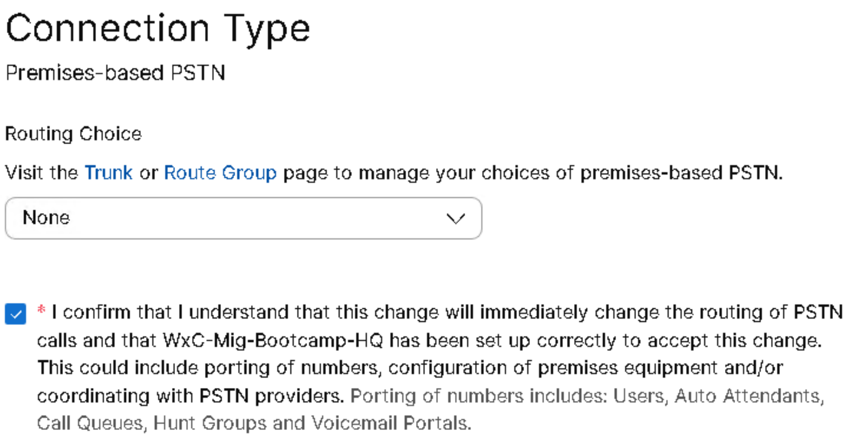
Cloud Connected PSTN

Select Cisco Cloud Connected PSTN partners that provide flexible global PSTN solutions fully integrated with Cisco's Webex Calling cloud.

Premises-based PSTN (formerly local gateway)

Bring Your Own Carrier by interconnecting any Service Provider's PSTN with a premises-based local gateway that tightly integrates to Cisco's Webex Calling cloud.

Step 11 For the **Routing Choice**, choose **None** from the drop-down menu, then check the checkbox to confirm that this change will immediately change the routing of PSTN calls. Click **Next.**



Connection Type

Premises-based PSTN

Routing Choice

Visit the Trunk or Route Group page to manage your choices of premises-based PSTN.

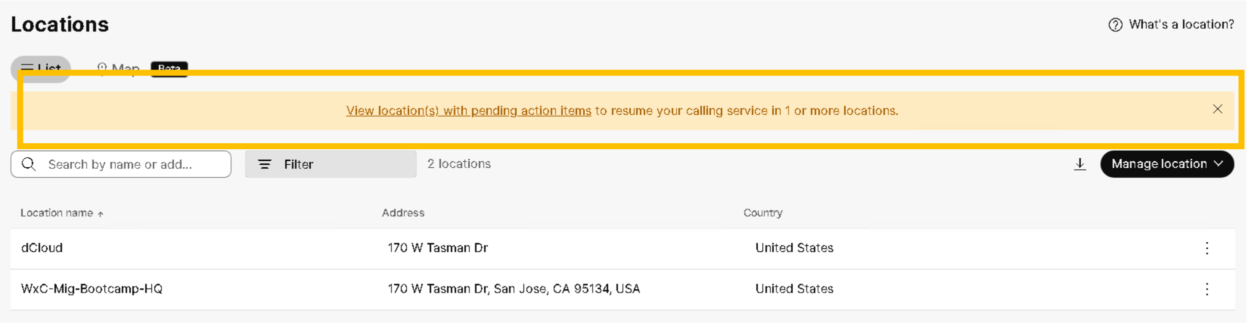
None

☑ * I confirm that I understand that this change will immediately change the routing of PSTN calls and that WxC-Mig-Bootcamp-HQ has been set up correctly to accept this change. This could include porting of numbers, configuration of premises equipment and/or coordinating with PSTN providers. Porting of numbers includes: Users, Auto Attendants, Call Queues, Hunt Groups and Voicemail Portals.

Step 12 Click **Done (Add Numbers Later)**

Step 13 Click **Locations** on the left-hand side of the screen.

Step 14 There are two Locations now in your lab organization: **dCloud** and **WxC-Mig-Bootcamp-HQ**. You will see a "pending action item" warning at the top of the screen for these locations because there is currently no main number assigned to them. Do not worry about this warning; you will configure the numbers later in this lab.



View location(s) with pending action items to resume your calling service in 1 or more locations.

2 locations

Location name	Address	Country
dCloud	170 W Tasman Dr	United States
WxC-Mig-Bootcamp-HQ	170 W Tasman Dr, San Jose, CA 95134, USA	United States

Task 3: Enable a User with Webex Calling and Assign the User to the New Location

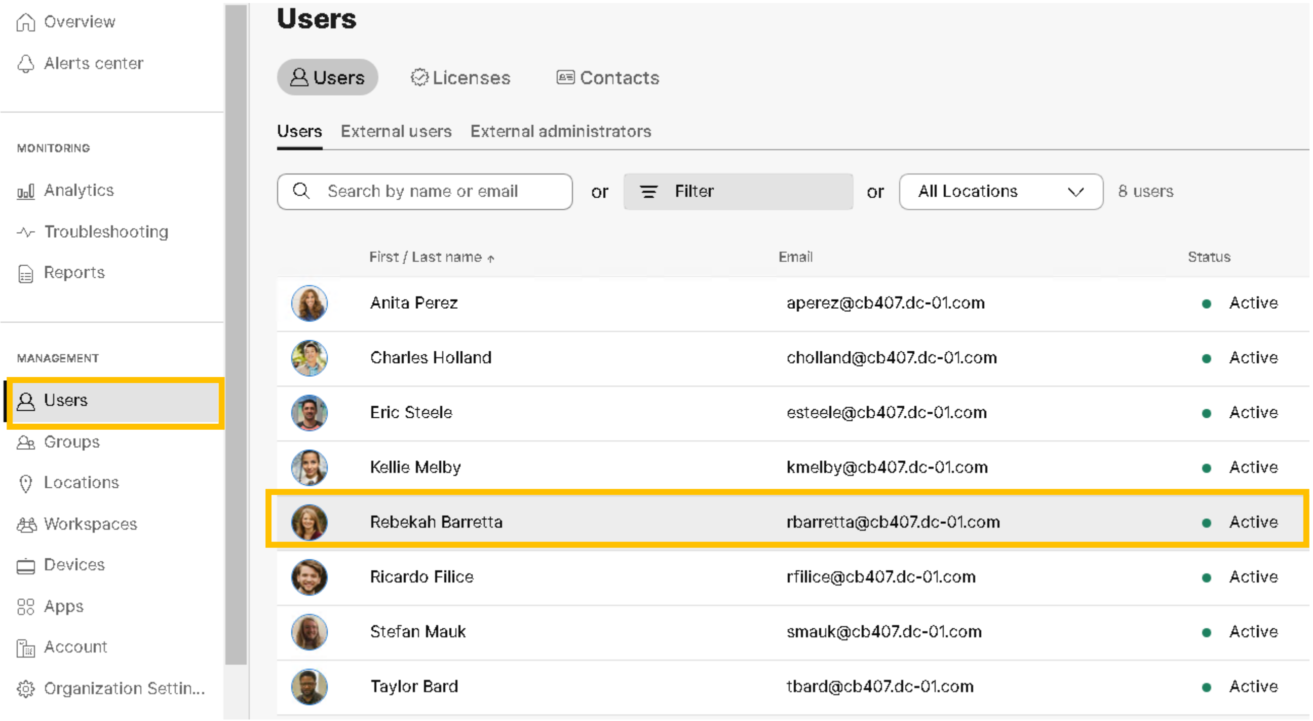
Now that you have a new location called WxC-Mig-Bootcamp-HQ, you will enable a user with Webex Calling and assign the user to this location.

Activity Procedure

Complete these steps:

Step 1 In Control Hub, navigate to **Management > Users** in the left panel.

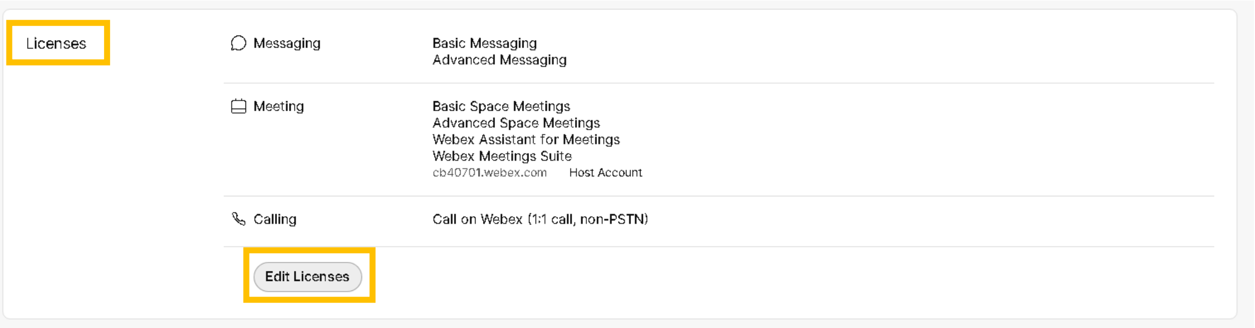
Step 2 Select user **Rebekah Barretta**.



First / Last name ↑	Email	Status
Anita Perez	aperez@cb407.dc-01.com	● Active
Charles Holland	cholland@cb407.dc-01.com	● Active
Eric Steele	esteele@cb407.dc-01.com	● Active
Kellie Melby	kmelby@cb407.dc-01.com	● Active
Rebekah Barretta	rbarretta@cb407.dc-01.com	● Active
Ricardo Filice	rfilice@cb407.dc-01.com	● Active
Stefan Mauk	smauk@cb407.dc-01.com	● Active
Taylor Bard	tbard@cb407.dc-01.com	● Active

Step 3 Scroll down the page to where it says, **Licenses.**

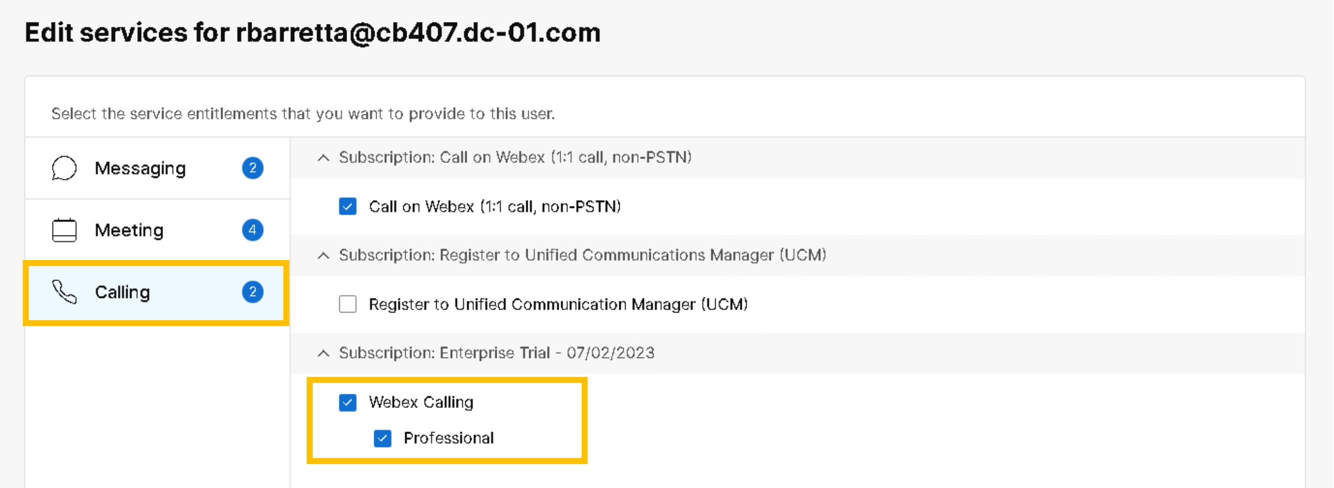
Step 4 Click **Edit Licenses.**



Messaging	Basic Messaging Advanced Messaging
Meeting	Basic Space Meetings Advanced Space Meetings Webex Assistant for Meetings Webex Meetings Suite cb40701.webex.com Host Account
Calling	Call on Webex (1:1 call, non-PSTN)

Step 5 On the next screen, you'll need to click **Edit Licenses** again.

Step 6 In the **Services enabled for Rebekah Barretta** window select the **Calling** tab.



Edit services for rbarretta@cb407.dc-01.com

Select the service entitlements that you want to provide to this user.

Subscription: Call on Webex (1:1 call, non-PSTN)

☑ Call on Webex (1:1 call, non-PSTN)

Subscription: Register to Unified Communications Manager (UCM)

□ Register to Unified Communication Manager (UCM)

Subscription: Enterprise Trial - 07/02/2023

☑ Webex Calling

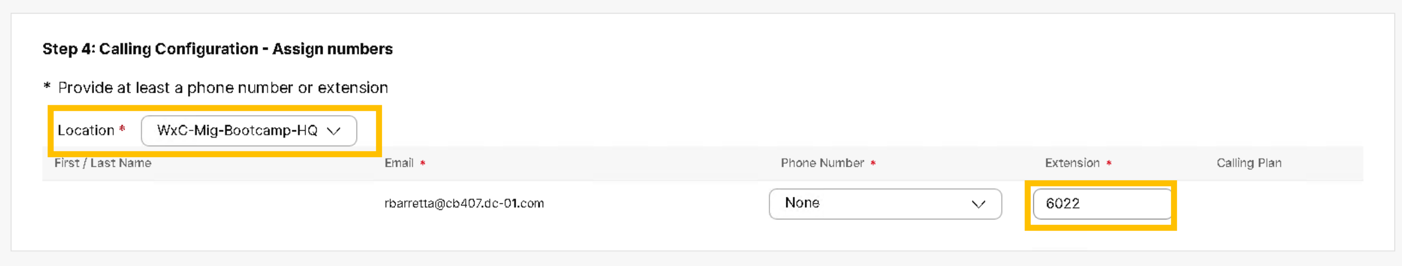
☑ Professional

Step 7 Check **Webex Calling and Professional** (Selecting one will automatically select both).

Step 8 Click **Save.**

Step 9 Under the **Location** dropdown menu, select **WxC-Mig-Bootcamp-HQ**.

Step 10 Assign the extension number **6022** under Extension.



Step 4: Calling Configuration - Assign numbers

* Provide at least a phone number or extension

Location * WxC-Mig-Bootcamp-HQ

First / Last Name	Email *	Phone Number *	Extension *	Calling Plan
	rbarretta@cb407.dc-01.com	None	6022	

Step 11 Click **Save.**

Step 12 Click **Close.**

Task 4: Add a Trunk

Now that you have a user enabled for Webex Calling in the WxC-Mig-Bootcamp-HQ location, you can add a SIP trunk to connect to the CUCM.

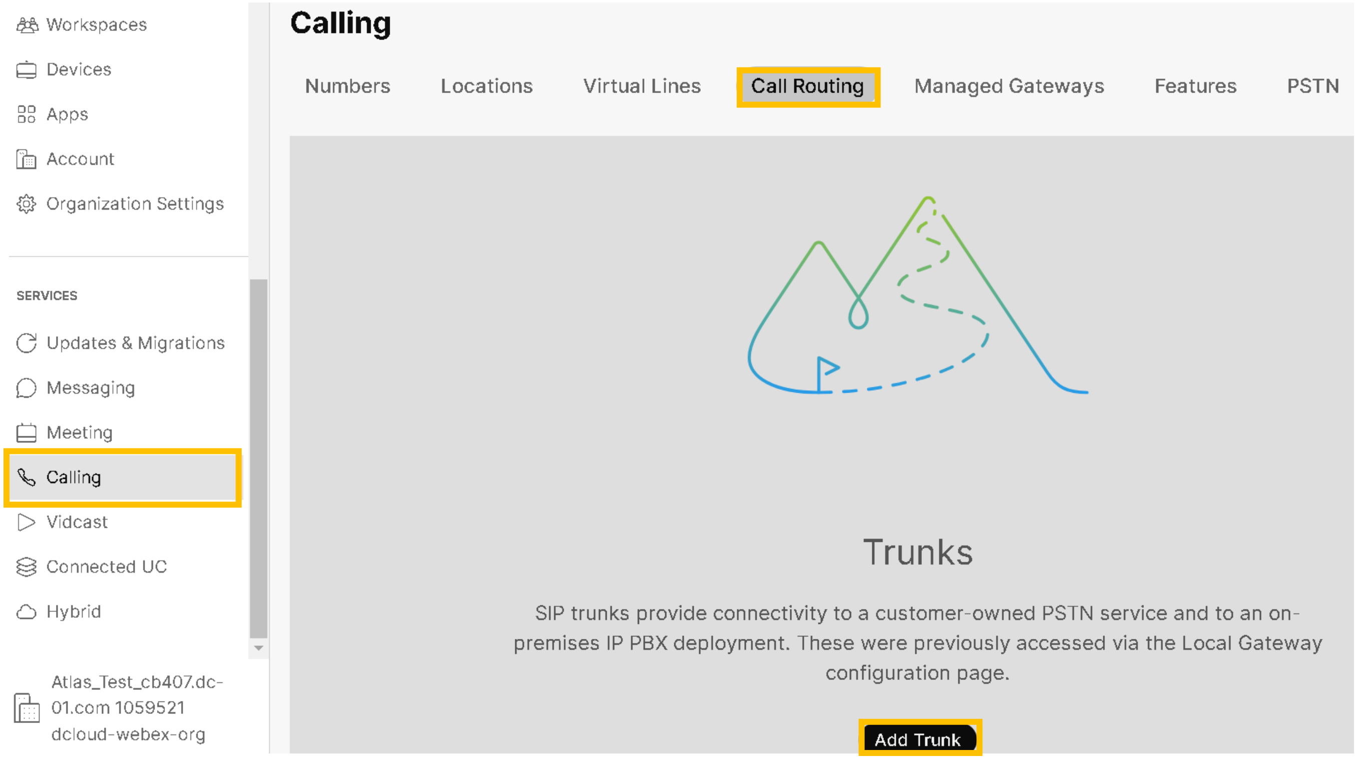
Activity Procedure

Complete these steps:

Step 1 On the left panel, click **Services > Calling.**

Step 2 Click the **Call Routing** tab.

Step 3 Click **Add Trunk**.



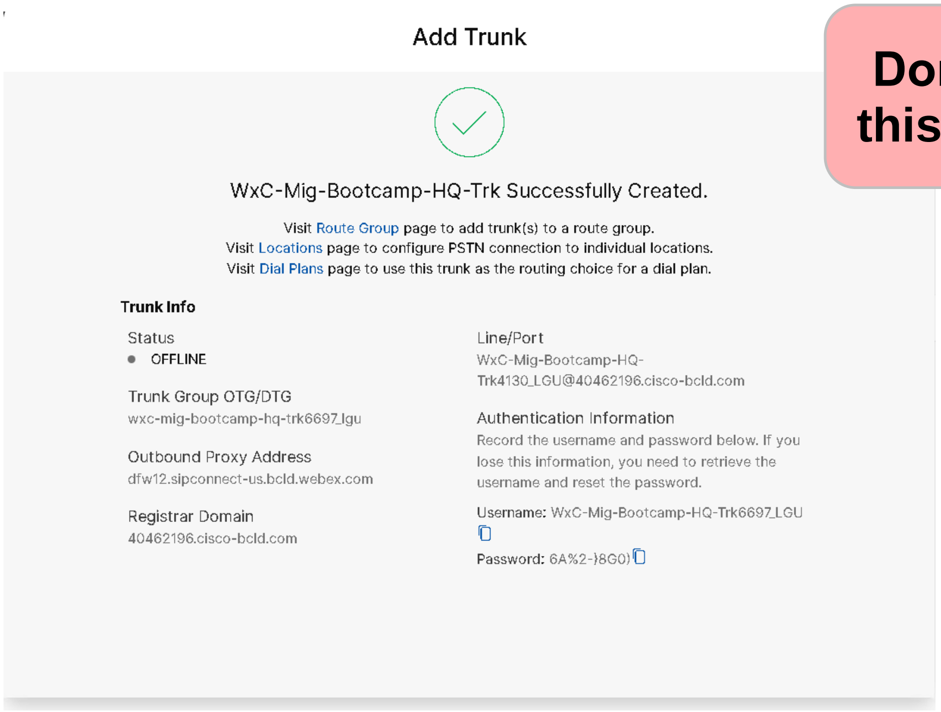
SIP trunks provide connectivity to a customer-owned PSTN service and to an on-premises IP PBX deployment. These were previously accessed via the Local Gateway configuration page.

Step 4 Under the Location menu, select **WxC-Mig-Bootcamp-HQ**. Define the name of the trunk as **WxC-Mig-Bootcamp-HQ-Trk**. Leave all other fields as default, as described in the table below. (See the next step before clicking Save.)

Location	**Select**: WxC-Mig-Bootcamp-HQ
Name	**Define**: WxC-Mig-Bootcamp-HQ-Trk
Trunk Type	**Leave Default**: Registration based
Device Type	**Leave Default**: Do not select anything from the drop-down menu
Dual Identity Support	**Leave Default**: Enabled

Step 5 Click **Save** and do **not** close the Add Trunk window.

Note **The next step is the MOST IMPORTANT step in this lab. PLEASE READ CAREFULLY.**



Add Trunk

WxC-Mig-Bootcamp-HQ-Trk Successfully Created.

Visit Route Group page to add trunk(s) to a route group.
Visit Locations page to configure PSTN connection to individual locations.
Visit Dial Plans page to use this trunk as the routing choice for a dial plan.

Trunk Info

Status
● OFFLINE

Trunk Group OTG/DTG
wxc-mig-bootcamp-hq-trk6697_lgu

Outbound Proxy Address
dfw12.sipconnect-us.bcld.webex.com

Registrar Domain
40462196.cisco-bcld.com

Line/Port
WxC-Mig-Bootcamp-HQ-Trk4130_LGU@40462196.cisco-bcld.com

Authentication Information
Record the username and password below. If you lose this information, you need to retrieve the username and reset the password.

Username: WxC-Mig-Bootcamp-HQ-Trk6697_LGU

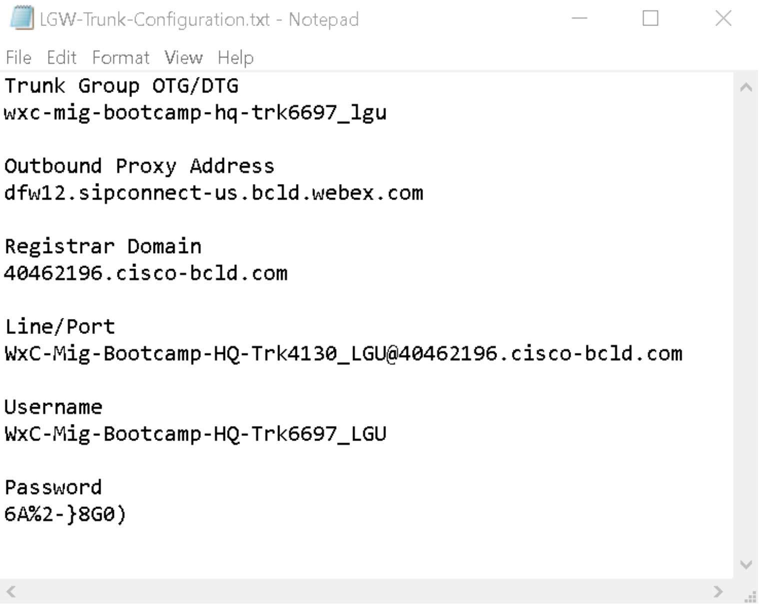
Password: 6A%2-}8G0)

Don't Close this Window!

Step 6 You need to copy parameters from the **Add Trunk** configuration and paste them into a text file. First, open the Notepad app and save an empty file entitled **LGW-Trunk-Configuration** on the Workstation 1 desktop.

Step 7 Copy the parameters from your **Add Trunk** configuration into your newly created **LGW-Trunk-Configuration** Notepad file. The image below is just an example. The information in your own lab is different. Ensure you get all the following information.

- Trunk Group OTG/DTG
- Outbound Proxy Address
- Registrar Domain
- Line/Port
- Username
- Password



LGW-Trunk-Configuration.txt - Notepad
File Edit Format View Help

```
Trunk Group OTG/DTG
wxc-mig-bootcamp-hq-trk6697_lgu

Outbound Proxy Address
dfw12.sipconnect-us.bcld.webex.com

Registrar Domain
40462196.cisco-bcld.com

Line/Port
WxC-Mig-Bootcamp-HQ-Trk4130_LGU@40462196.cisco-bcld.com

Username
WxC-Mig-Bootcamp-HQ-Trk6697_LGU

Password
6A%2-}8G0)
```

Step 8 After you copy all the information to the Notepad file, click **File** and click **Save.**

Note You can review all the parameters except the username and password after you close the Add Trunk window. To review the trunk configuration parameters, click Manage. Also, you can retrieve the Username and Password, but the process will change the Password, that is why it is so important to copy the information now.

Step 9 Close the **Add Trunk** window. Now you have one SIP trunk configured in your Webex Control Hub organization, as seen on the Call Routing tab.

Task 5: Add a Route Group

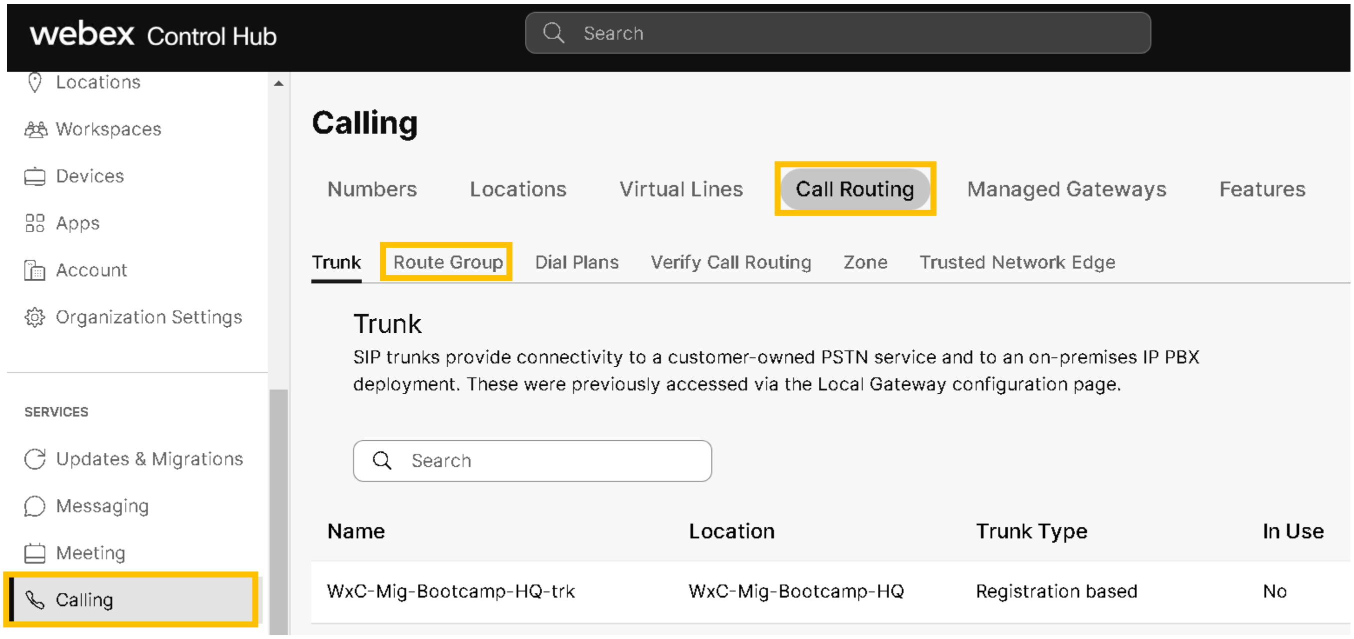
A Route Group is a group of trunks that allows Webex Calling to distribute calls over multiple trunks or provide redundancy. We recommend always assigning a Route Group to a Location instead of assigning a trunk because when you assign a Route Group to a Location, and you need to add more trunks, there will be no impact on the service.

Activity Procedure

Complete these steps:

Step 1 If not already on the Call Routing tab, click **Services > Calling** in the left panel.

Step 2 Click the **Call Routing** tab.



Calling

Trunk

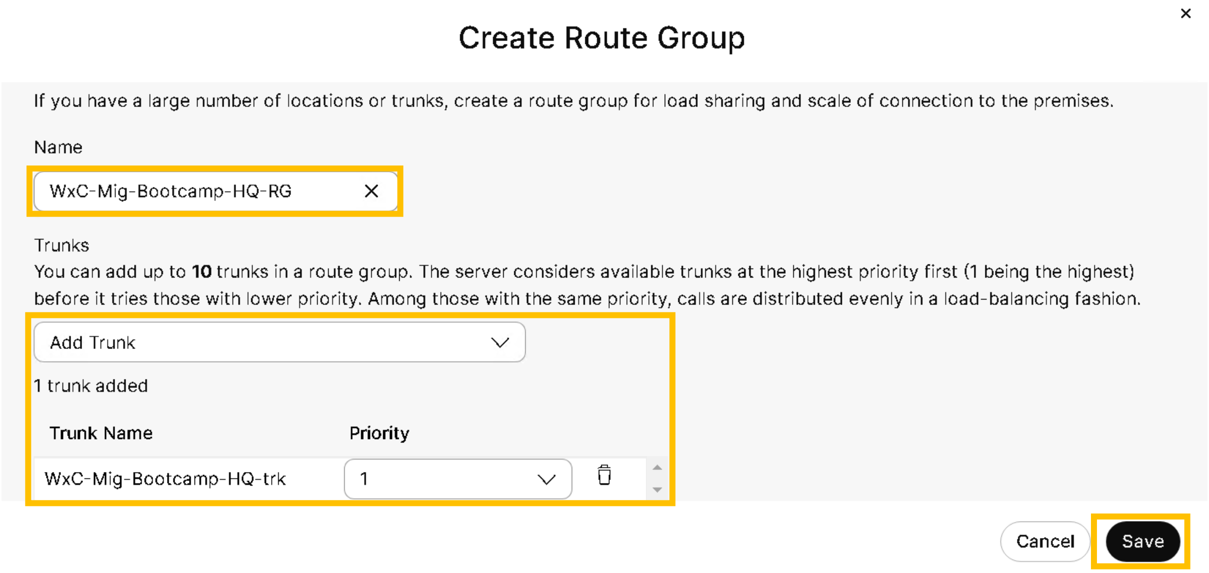
SIP trunks provide connectivity to a customer-owned PSTN service and to an on-premises IP PBX deployment. These were previously accessed via the Local Gateway configuration page.

Name	Location	Trunk Type	In Use
WxC-Mig-Bootcamp-HQ-trk	WxC-Mig-Bootcamp-HQ	Registration based	No

Step 3 Under the Route Group tab, click **Create Route Group**.

Step 4 In the Create Route Group window, define the Name for the Route Group as **WxC-Mig-Bootcamp-HQ-RG**. Select the Trunk you created before. Assign Priority 1.

Name	**Define:** WxC-Mig-Bootcamp-HQ-RG
Trunks	**Select:** WxC-Mig-Bootcamp-HQ-Trk
Trunk Name	**Set Priority to**: 1



Create Route Group

If you have a large number of locations or trunks, create a route group for load sharing and scale of connection to the premises.

Name: WxC-Mig-Bootcamp-HQ-RG

Trunks

You can add up to **10** trunks in a route group. The server considers available trunks at the highest priority first (1 being the highest) before it tries those with lower priority. Among those with the same priority, calls are distributed evenly in a load-balancing fashion.

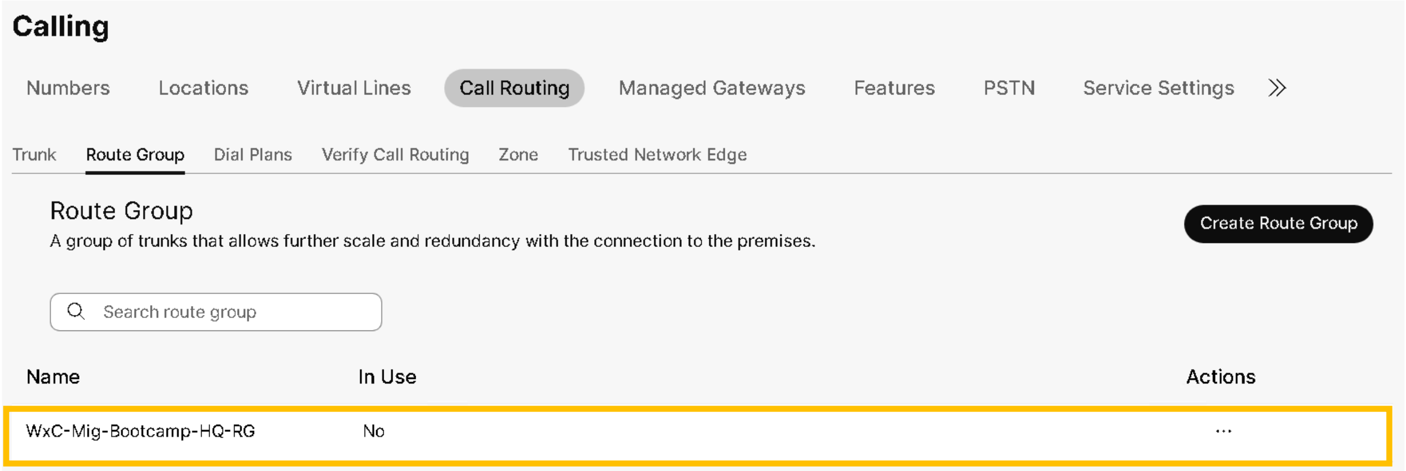
Add Trunk

1 trunk added

Trunk Name	Priority
WxC-Mig-Bootcamp-HQ-trk	1

Step 5 Click **Save.** Close the **Create Route Group** window.

Step 6 You have now a Route Group in this organization, as seen on the **Route Group** tab.



Route Group

A group of trunks that allows further scale and redundancy with the connection to the premises.

Name	In Use	Actions
WxC-Mig-Bootcamp-HQ-RG	No	···

Task 6: Assign the Route Group to a Location

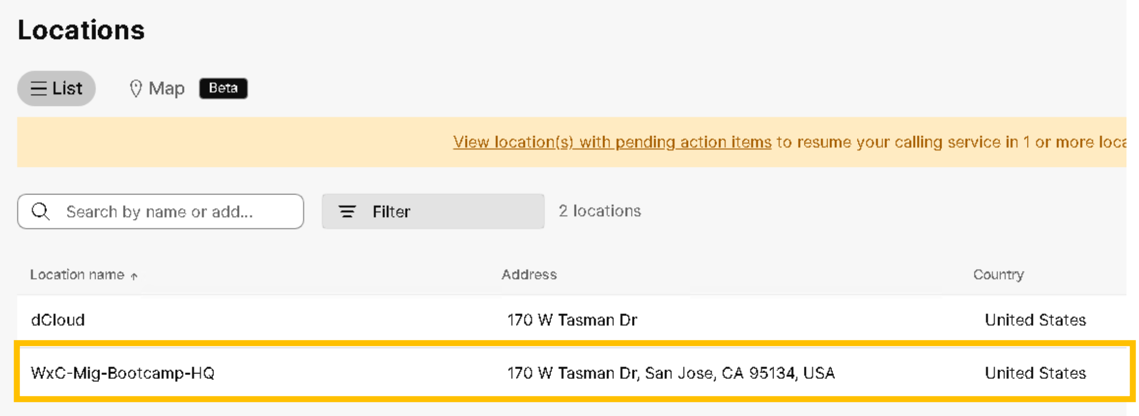
To have the PSTN service for this organization, you must assign a Route Group or Trunk to the location. For this lab, you will assign the Route Group that you just created to the WxC-Mig-Bootcamp-HQ location.

Activity Procedure

Complete these steps:

Step 1 Click **Management > Locations** in the left panel.

Step 2 Click the **WxC-Mig-Bootcamp-HQ** location.



Locations

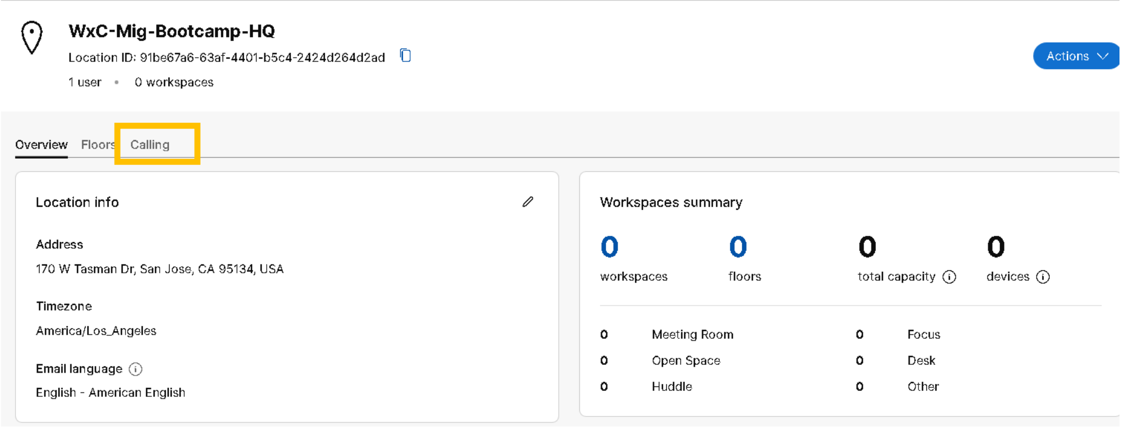
List   Map Beta

View location(s) with pending action items to resume your calling service in 1 or more loca

Search by name or add...   Filter   2 locations

Location name	Address	Country
dCloud	170 W Tasman Dr	United States
WxC-Mig-Bootcamp-HQ	170 W Tasman Dr, San Jose, CA 95134, USA	United States

Step 3 Click the **Calling** tab near the top of the screen.



WxC-Mig-Bootcamp-HQ

Location ID: 91be67a6-63af-4401-b5c4-2424d264d2ad

1 user • 0 workspaces

Actions

Overview   Floors   Calling

Location info

Address

170 W Tasman Dr, San Jose, CA 95134, USA

Timezone

America/Los_Angeles

Email language

English - American English

Workspaces summary

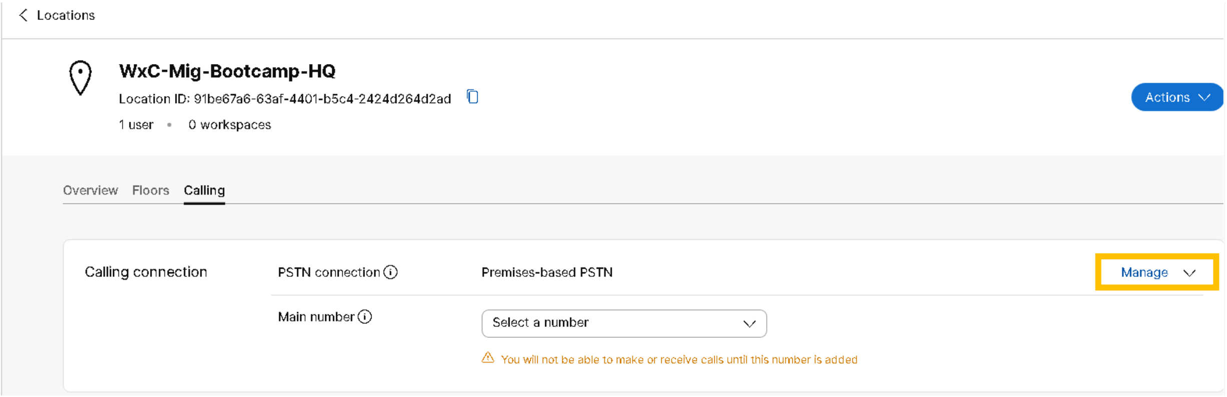
0 workspaces   0 floors   0 total capacity   0 devices

0 Meeting Room   0 Focus

0 Open Space   0 Desk

0 Huddle   0 Other

Step 4 In the **Calling Connection** section, click **Manage** on the right-hand side of the screen.



Locations

WxC-Mig-Bootcamp-HQ

Location ID: 91be67a6-63af-4401-b5c4-2424d264d2ad

1 user • 0 workspaces

Actions

Overview   Floors   Calling

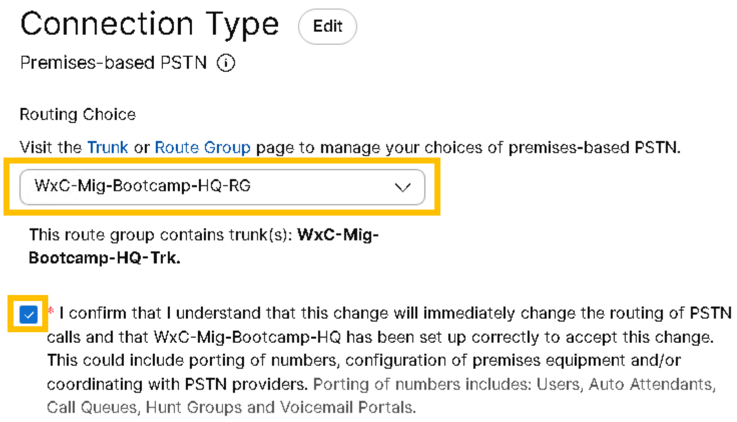
Calling connection

PSTN connection: Premises-based PSTN   Manage

Main number: Select a number

⚠ You will not be able to make or receive calls until this number is added

Step 5 Under Routing Choice, choose the **WxC-Mig-Bootcamp-RG Route Group**. Add a check to the confirmation warning at the bottom.



Connection Type

Premises-based PSTN ⓘ

Routing Choice

Visit the Trunk or Route Group page to manage your choices of premises-based PSTN.

WxC-Mig-Bootcamp-HQ-RG

This route group contains trunk(s): **WxC-Mig-Bootcamp-HQ-Trk.**

☑ * I confirm that I understand that this change will immediately change the routing of PSTN calls and that WxC-Mig-Bootcamp-HQ has been set up correctly to accept this change. This could include porting of numbers, configuration of premises equipment and/or coordinating with PSTN providers. Porting of numbers includes: Users, Auto Attendants, Call Queues, Hunt Groups and Voicemail Portals.

Step 6 Click **Next.**

Step 7 Click **Done (Add Numbers Later).** You will add the numbers in the next scenario.

Task 7: Add Phone Numbers to a Location

As an administrator, you can manage phone numbers in Control Hub. You can view, activate, remove, and add phone numbers to your organization, and move phone numbers from one location to another.

Remember that numbers must follow the E.164 format for all countries, except for the United States, which can also follow the National format.

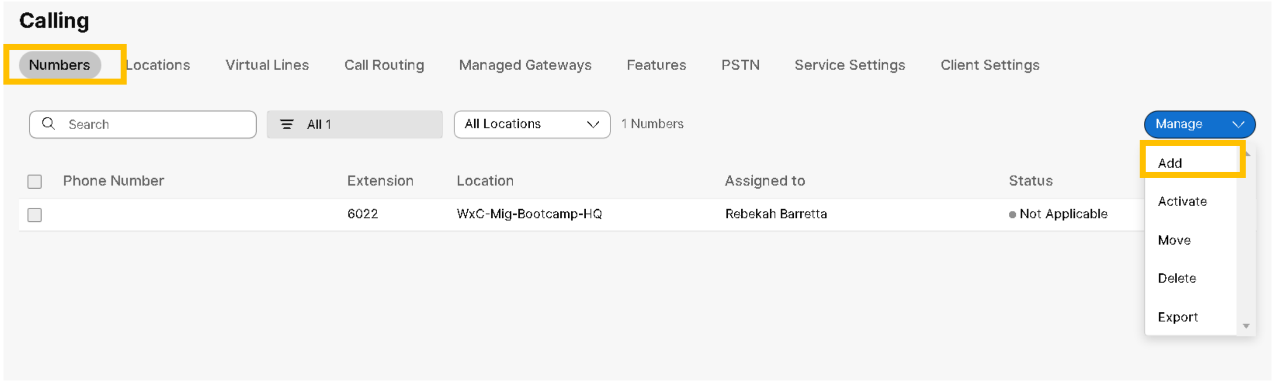
Activity Procedure

Complete these steps:

Step 1 Click **Services > Calling** in the left panel.

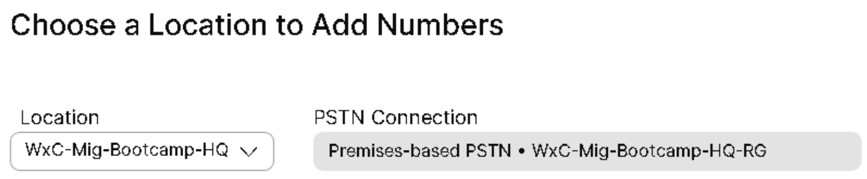
Step 2 Click the **Numbers** tab.

Step 3 Click the **Manage** drop-down and choose **Add.**



□ Phone Number	Extension	Location	Assigned to	Status
□	6022	WxC-Mig-Bootcamp-HQ	Rebekah Barretta	● Not Applicable

Step 4 Under the **Location** drop-down list, select **WxC-Mig-Bootcamp-HQ**. The wizard displays the PSTN option that this location must connect with to access the PSTN. Click **Next**.

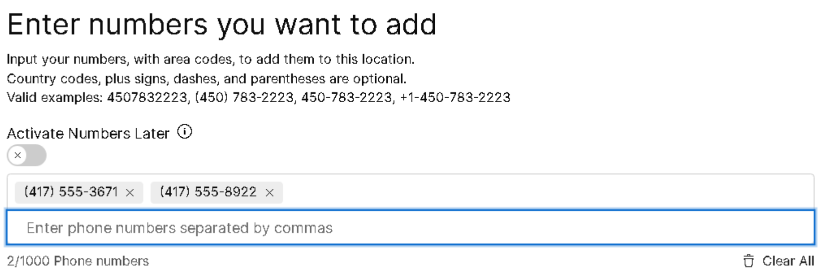


Choose a Location to Add Numbers

Location: WxC-Mig-Bootcamp-HQ

PSTN Connection: Premises-based PSTN • WxC-Mig-Bootcamp-HQ-RG

Step 5 In the **Enter numbers you want to add** box, add **two** unique numbers that start with **417555** and then a random string of four numbers at the end (for example, 4175557698). Press **Enter/Return** on your keyboard after entering the number. Click **Save** followed by **Close.**



Enter numbers you want to add

Input your numbers, with area codes, to add them to this location.
Country codes, plus signs, dashes, and parentheses are optional.
Valid examples: 4507832223, (450) 783-2223, 450-783-2223, +1-450-783-2223

Note Use any four random numbers. The numbers in the image are just an example. If you click **Save** and you get an error, try a different four-digit random number.

Step 6 Click **Save.**

Step 7 Click **Close.**

Task 8: Assign a Phone Number to a Location and a User

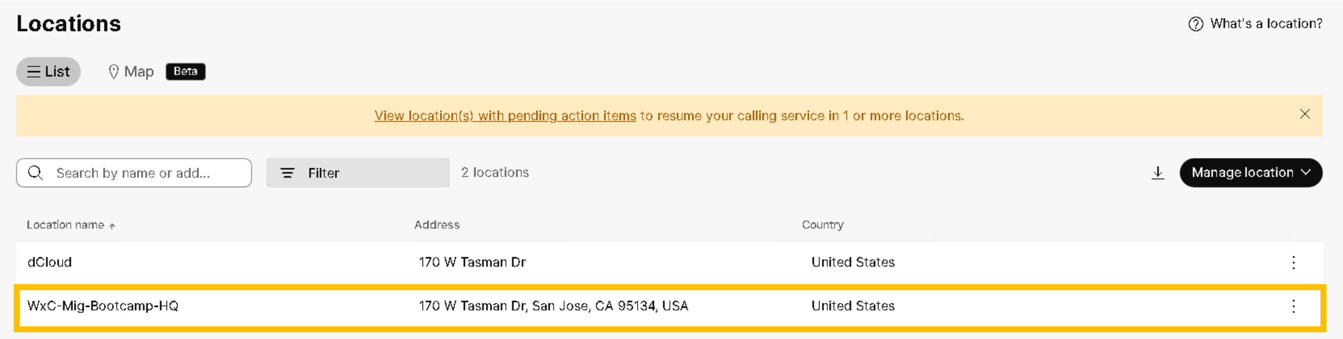
Now, you have your numbers added to your organization. These numbers are ready to be used as a main number for the **WxC-Mig-Bootcamp-HQ** Location and an E.164 number for the user **Rebekah Barretta**.

Activity Procedure

Complete these steps:

Step 1 Go to **Management>Locations** on the left-hand panel.

Step 2 Click the **WxC-Mig-Bootcamp-HQ location**.



Locations

What's a location?

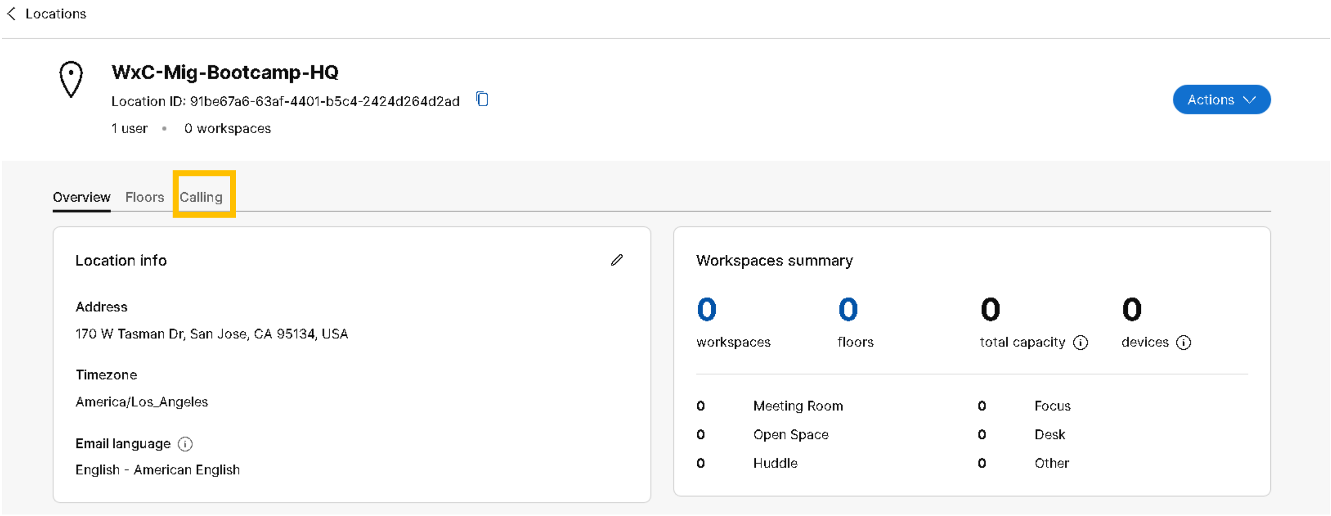
List · Map Beta

View location(s) with pending action items to resume your calling service in 1 or more locations.

Search by name or add... · Filter · 2 locations · Manage location

Location name	Address	Country
dCloud	170 W Tasman Dr	United States
WxC-Mig-Bootcamp-HQ	170 W Tasman Dr, San Jose, CA 95134, USA	United States

Step 3 Click the **Calling** tab.



Locations

WxC-Mig-Bootcamp-HQ

Location ID: 91be67a6-63af-4401-b5c4-2424d264d2ad

1 user • 0 workspaces

Actions

Overview · Floors · Calling

Location info

Address
170 W Tasman Dr, San Jose, CA 95134, USA

Timezone
America/Los_Angeles

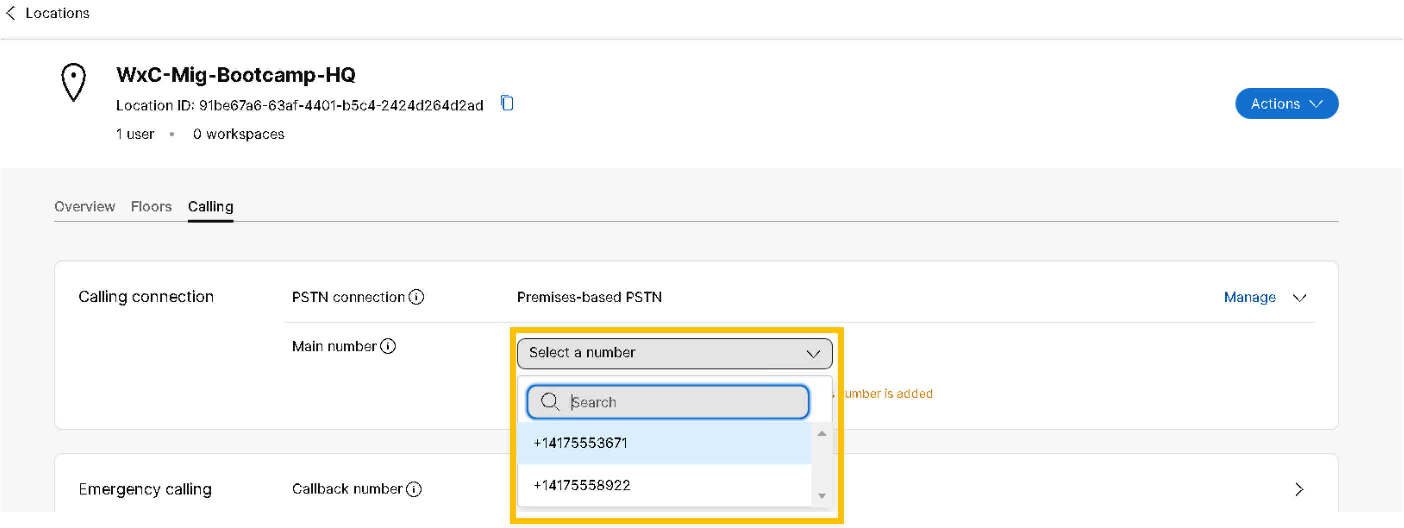
Email language
English - American English

Workspaces summary

0 workspaces · 0 floors · 0 total capacity · 0 devices

0	Meeting Room	0	Focus
0	Open Space	0	Desk
0	Huddle	0	Other

Step 4 Click the **Main Number** drop-down list and select either of the two numbers you created in the previous scenario.



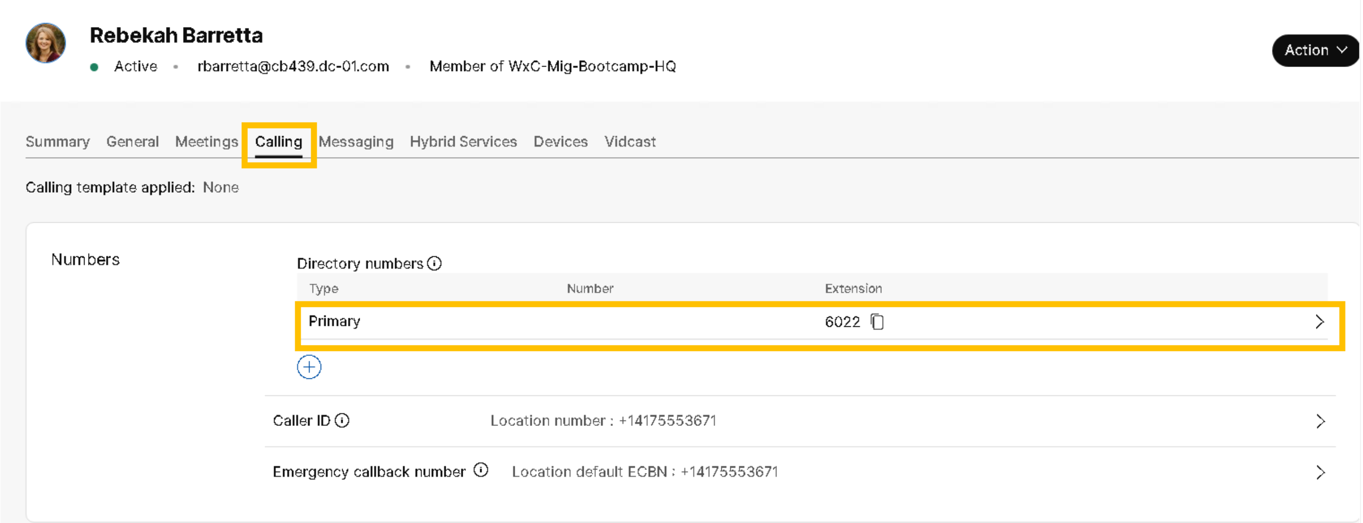
Step 5 Click **Save.**

Next, you will assign a number to the user, Rebekah Barretta.

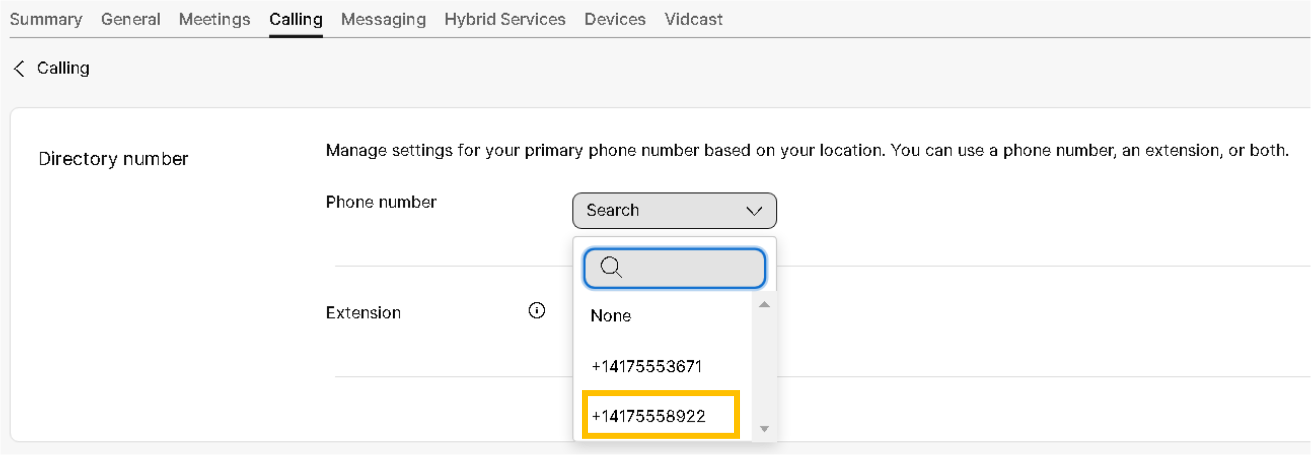
Step 6 Go to **Users** under the **Management** menu in the left panel.

Step 7 Select the user, **Rebekah Barretta.**

Step 8 Click the **Calling** tab, and then click the Primary number where you already configured the extension number 6022.


Rebekah Barretta
Active • rbarretta@cb439.dc-01.com • Member of WxC-Mig-Bootcamp-HQ
Action
Summary
General
Meetings
Calling
Messaging
Hybrid Services
Devices
Vidcast
Calling template applied: None
Numbers
Directory numbers
Type
Number
Extension
Primary
6022
Caller ID
Location number : +14175553671
Emergency callback number
Location default ECBN : +14175553671

Step 9 Under the **Phone Number** drop-down menu, select the number you configured that is different from the one you already assigned to the main number of the location.



Manage settings for your primary phone number based on your location. You can use a phone number, an extension, or both.

Phone number: Search

Step 10 Click **Save.**

Step 11 The user **Rebekah Barretta** is now configured with a E.164 number for the PSTN service.

Task 9: Dial Plan to Route Internal Calls to CUCM from Webex Calling

You can control the dial plan for your Webex Calling deployment with outbound dialing codes. Customize extension lengths, routing prefixes, and dialing preferences (internal and external) to be compatible with the dialing habits of your users. For this specific lab you are going to configure how to route internal calls from a user in Webex Calling using Webex app to a user in CUCM using Jabber emulating a real customer scenario.

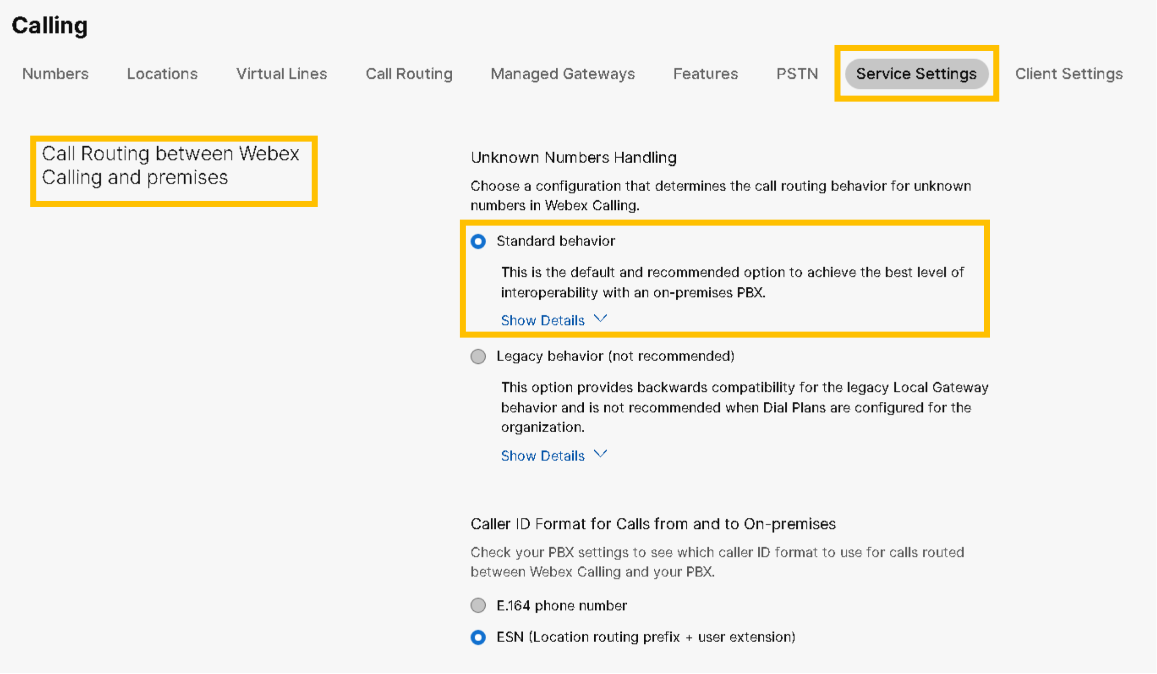
Activity Procedure

Complete these steps:

Step 1 On the left panel under Services, click **Calling.**

Step 2 Click **Service Settings** near the top of the screen.

Step 3 Under **Call Routing between Webex Calling and Premises**, verify that the **Standard behavior** is checked. With this configuration, all the dialed number length of 2 to 6 digits is routed to the selected SIP trunk only if the caller's Location has the "**Calls to On-Premises Extensions**" setting enabled. You can click, **Show Details** to see how the calls are routed in Webex Calling.



Unknown Numbers Handling

Choose a configuration that determines the call routing behavior for unknown numbers in Webex Calling.

● Standard behavior

This is the default and recommended option to achieve the best level of interoperability with an on-premises PBX.

○ Legacy behavior (not recommended)

This option provides backwards compatibility for the legacy Local Gateway behavior and is not recommended when Dial Plans are configured for the organization.

Caller ID Format for Calls from and to On-premises

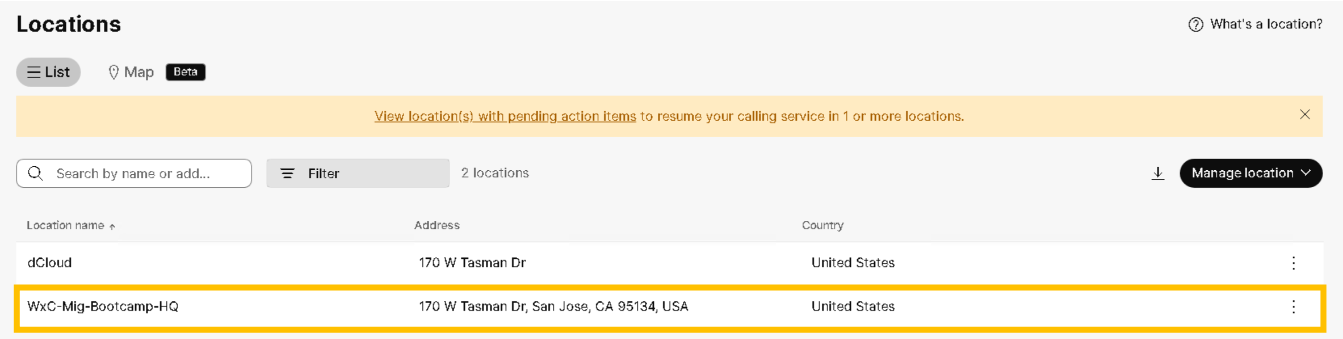
Check your PBX settings to see which caller ID format to use for calls routed between Webex Calling and your PBX.

○ E.164 phone number

● ESN (Location routing prefix + user extension)

Step 4 Click **Management>Locations** on the left-hand side.

Step 5 Click the **WxC-Mig-Bootcamp-HQ location**.

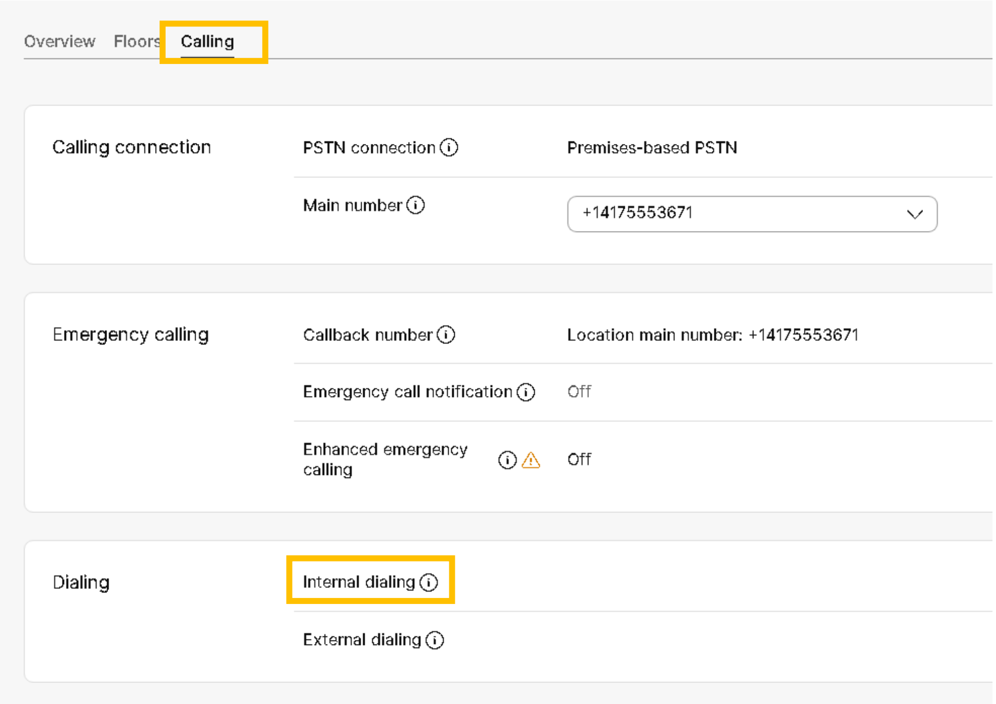


View location(s) with pending action items to resume your calling service in 1 or more locations.

2 locations

Location name	Address	Country
dCloud	170 W Tasman Dr	United States
WxC-Mig-Bootcamp-HQ	170 W Tasman Dr, San Jose, CA 95134, USA	United States

Step 6 Click the **Calling** tab, then scroll down to the section labeled, **Dialing> Internal Dialing**.



Calling connection

PSTN connection ⓘ Premises-based PSTN

Main number ⓘ +14175553671

Emergency calling

Callback number ⓘ Location main number: +14175553671

Emergency call notification ⓘ Off

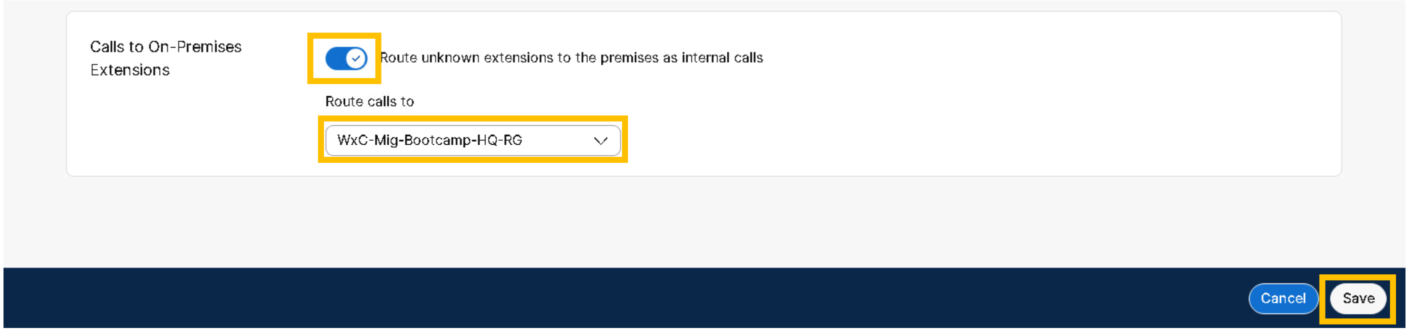
Enhanced emergency calling ⓘ ⚠ Off

Dialing

Internal dialing ⓘ

External dialing ⓘ

Step 7 Click **Internal Dialing**. Enable the toggle button for **Route unknown extensions to the premises as internal calls**, and then select the **WxC-Mig-Bootcamp-HQ-RG** route group.



Calls to On-Premises Extensions

☑ Route unknown extensions to the premises as internal calls

Route calls to

WxC-Mig-Bootcamp-HQ-RG

Step 8 Click **Save.**

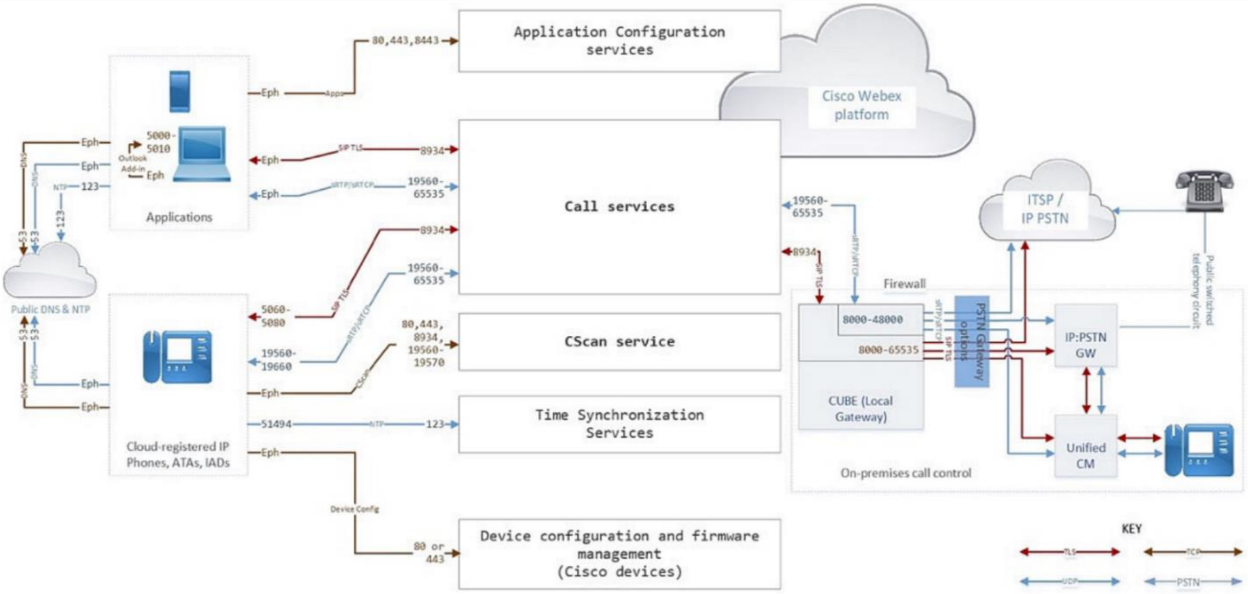
Scenario 2: Local Gateway Configuration

Objective

Use this task flow to configure local gateways for your Webex Calling deployment. The steps that follow are performed on the CLI interface itself. The trunk between the local gateway and Webex Calling is always secured using SIP TLS transport and SRTP for media between Local Gateway and the Webex Calling Access SBC. In your real deployment there are some networks requirements that you need to keep in mind:

https://help.webex.com/en-us/article/b2exve/Port-Reference-Information-for-Cisco-Webex-Calling

Webex Calling Network Requirements.



Supported platforms with Local Gateway:

https://help.webex.com/en-us/article/n4cprps/Prepare-Your-Environment-for-Webex-Calling

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/supported-platforms.html

Now you will configure your local gateway with the information you have configured and copied in a Notepad file in the previous scenario.

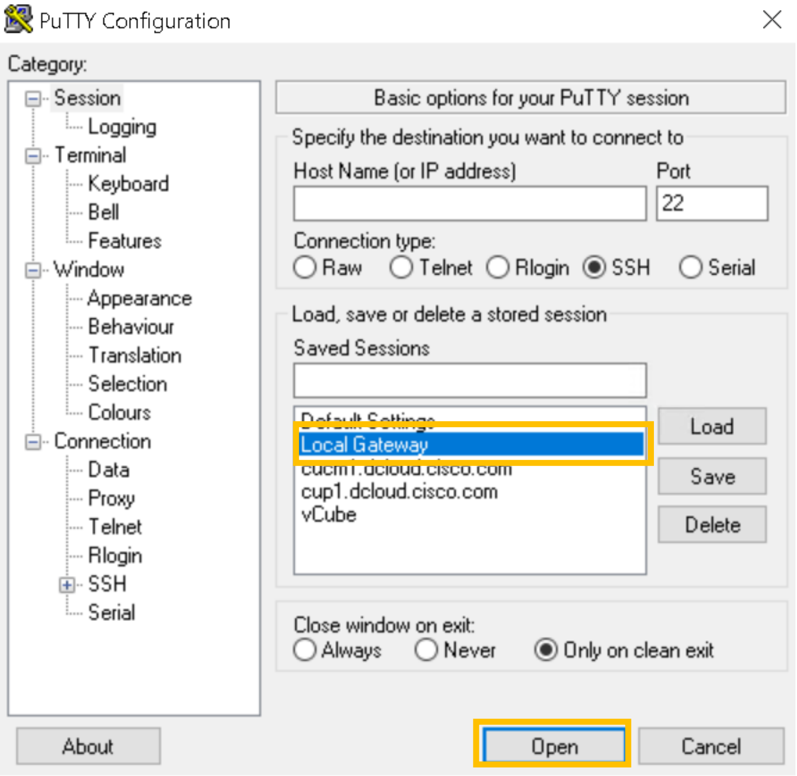
- Task 1: Configure Local Gateway for Webex Calling Deployment
- Task 2: PSTN Calls and Inbound Calls to Webex Calling

Task 1: Configure Local Gateway for Webex Calling Deployment

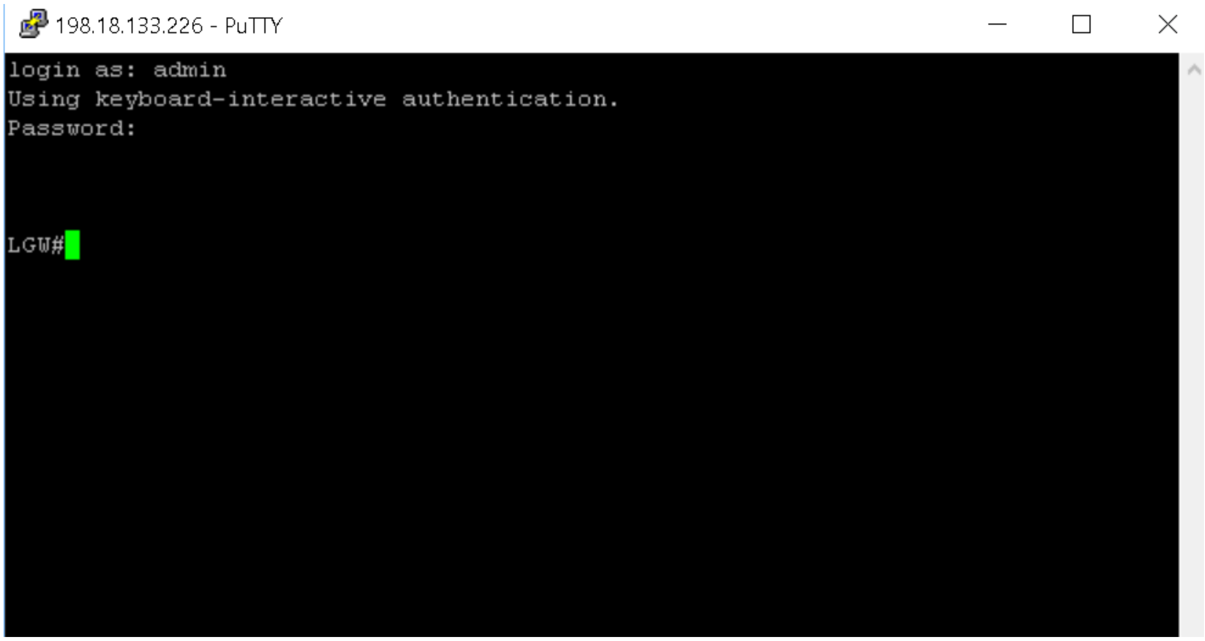
Activity Procedure

Complete these steps:

Step 1 On Workstation 1, open the **PuTTY** application [ ], then select **Local Gateway** and click **Open** to access the **CSR1000v** that is the Local Gateway for this lab.



Step 2 Log in with **admin / dCloud123!**



```
login as: admin
Using keyboard-interactive authentication.
Password:



LGW#
```

Step 3 Before you proceed with the Local Gateway configuration, we need to ensure that a master key must be pre-configured for the password with the commands shown below before it can be used in the credentials and/or shared-secrets. Type 6 passwords are encrypted using AES cipher and user-defined master key. We will use Password123 as our master key.

```
configure terminal
key config-key password-encrypt Password123
password encryption aes
end
```

Step 4 Create a dummyPKI Trustpoint and call itdummyTp. Assign the trustpoint asthe defaultsignaling trustpoint under sip-ua. The cn-san-validate server is needed to ensure LGW establishes the connection only if the outbound proxy configured on the tenant you will configure later and that matches with CN-SAN list received from the server.

The crypto trustpoint is needed for TLS to work even though a local client certificate (i.e. mTLS) is not required for the connection to be set up. Finally, disable TLS v1.0 and v1.1 by enabling v1.2 exclusivity and set tcp-retry count to 1000 (5 seconds)..

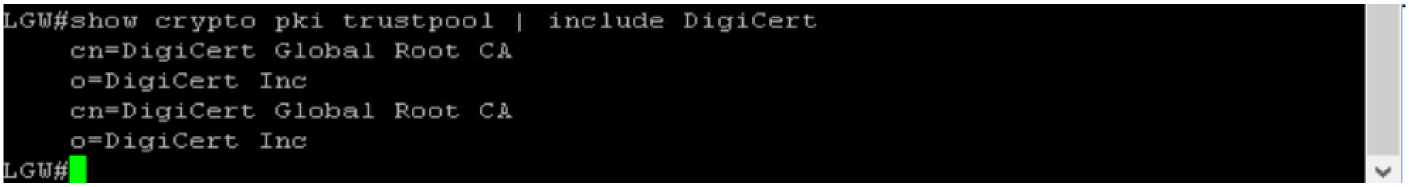
```
configure terminal
crypto pki trustpoint dummyTp
revocation-check crl
exit
sip-ua
crypto signaling default trustpoint dummyTp cn-san-validate server
transport tcp tls v1.2
tcp-retry 1000
end
```

Step 5 The default trustpool bundle does not include the DigiCert Root CA certificate needed for validating the server-side certificate during TLS connection establishment to Webex. The trustpool bundle must be updated by downloading the latest Cisco Trusted Core Root Bundle from http://www.cisco.com/security/pki.

```
configure terminal
crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_core.p7b
end
```

Step 6 Check if the DigiCert Root CA certificate is in the trustpool.

```
show crypto pki trustpool | include DigiCert
```



```
LGW#show crypto pki trustpool | include DigiCert
    cn=DigiCert Global Root CA
    o=DigiCert Inc
    cn=DigiCert Global Root CA
    o=DigiCert Inc
LGW#
```

Step 7 Configure the IP address trusted list. This is to explicitly enable the source IP addresses of entities from which Local Gateway expects legitimate VoIP calls, for example, Webex peers, Unified CM nodes, IP PSTN. By default, LGW blocks all incoming VoIP call setups from IP addresses not in its trusted list. IP addresses from dial-peers with session target ip or Server Group are trusted by default and need not be populated here.

```
configure terminal
voice service voip
ip address trusted list
ipv4 23.89.0.0 255.255.0.0
ipv4 85.119.56.128 255.255.255.192
ipv4 85.119.57.128 255.255.255.192
ipv4 185.115.196.0 255.255.255.128
ipv4 185.115.197.0 255.255.255.128
ipv4 128.177.14.0 255.255.255.128
ipv4 128.177.36.0 255.255.255.192
ipv4 135.84.169.0 255.255.255.128
ipv4 135.84.170.0 255.255.255.128
ipv4 135.84.171.0 255.255.255.128
ipv4 135.84.172.0 255.255.255.192
ipv4 199.59.64.0 255.255.255.128
ipv4 199.59.65.0 255.255.255.128
ipv4 199.59.66.0 255.255.255.128
ipv4 199.59.67.0 255.255.255.128
ipv4 199.59.70.0 255.255.255.128
ipv4 199.59.71.0 255.255.255.128
ipv4 135.84.172.0 255.255.255.128
ipv4 135.84.173.0 255.255.255.128
ipv4 135.84.174.0 255.255.255.128
ipv4 199.19.197.0 255.255.255.0
ipv4 199.19.199.0 255.255.255.0
ipv4 139.177.64.0 255.255.255.0
ipv4 139.177.65.0 255.255.255.0
ipv4 139.177.66.0 255.255.255.0
ipv4 139.177.67.0 255.255.255.0
ipv4 139.177.68.0 255.255.255.0
ipv4 139.177.69.0 255.255.255.0
ipv4 139.177.70.0 255.255.255.0
ipv4 139.177.71.0 255.255.255.0
ipv4 139.177.72.0 255.255.255.0
ipv4 139.177.73.0 255.255.255.0
end
```

Step 8 In this step you are going to configure the CUBE specific configuration.

```
configure terminal
voice service voip
allow-connections sip to sip
media statistics
media bulk-stats
no supplementary-service sip refer
no supplementary-service sip handle-replaces
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
stun
stun flowdata agent-id 1 boot-count 4
stun flowdata shared-secret 0 Password123$
sip
g729 annexb-all
early-offer forced
end
```

- **media statistics** - Enables media monitoring on the LGW.
- **media bulk-stats** - Enables the control plane to poll the data plane for bulk call statistics.
- **allow-connections sip to sip** - Allows this platform to bridge two VoIP SIP call legs. It is disabled by default.
- **no supplementary-service sip refer and no supplementary-service sip handle-replaces** - Disables REFER and replaces the Dialog ID in the Replaces header with the peer dialog ID.
- **fax protocol pass-through g711ulaw** - Enables audio codec for fax transport.
- **stun**
- **stun flowdata agent-id 1 boot-count 4**
- **stunflowdata shared-secret 0 Password123$** - Enables STUN globally. When a call is forwarded back to a Webex user (such as when both the called and calling parties are Webex subscribers and have the media anchored at the Webex SBC), the media cannot flow to the local gateway as the pin hole is not opened. The STUN bindings feature on the local gateway allows locally generated STUN requests to be sent over the negotiated media path.
- The shared secret is arbitrary as STUN is only used to open the pinhole in the firewall and allow media latching to take place in the Webex Access SBC. STUN password is a pre-requisite for LGW/CUBE to send STUN message out. IOS/IOS-XE-based firewalls can be configured to check for this password and open pin-holes dynamically (i.e. without explicit in-out rules).
- But for the LGW deployment case, the firewall is statically configured to open pin-holes in the outbound direction based on Webex SBC subnets, so the firewall should just treat this as any inbound UDP packet, which will trigger the pin-hole opening without explicitly looking at the packet contents.
- **sip**
- **g729 annexb-all** - Allows all variants of G729.
- **sip**
- **early-offer forced** - This command forces the LGW/CUBE to send the SDP information in the initial INVITE message itself instead of waiting to send the information till it gets an acknowledgement from the neighboring peer.

Step 9 Configure Codec Profile, STUN definition, and SRTP Crypto suite as shown.

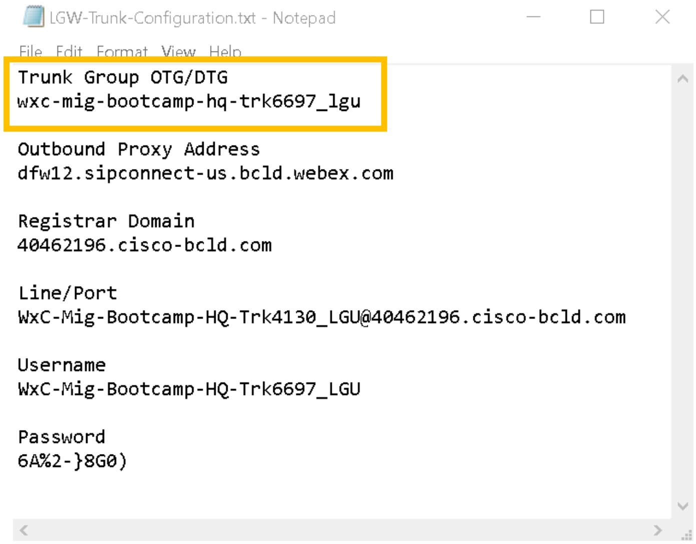
```
configure terminal
voice class codec 99
codec preference 1 g711ulaw
codec preference 2 g711alaw
exit
voice class srtp-crypto 200
crypto 1 AES_CM_128_HMAC_SHA1_80
exit
voice class stun-usage 200
stun usage firewall-traversal flowdata
stun usage ice lite
end
```

- **voice class codec 99 -** Allows G711 (mu and a-law) codec for sessions. Will be applied to all the dial-peers.
- **voice class srtp-crypto 200** - Specifies SHA1_80 as the only SRTP cipher-suite that will be offered by LGW/CUBE in the SDP in offer and answer. Webex only supports SHA1_80. This command will be applied to voice class tenant 200 (discussed later) facing Webex.
- **voice class stun-usage 200** - Defines STUN usage. Will be applied to all Webex facing (200201 tag) dial-peers to avoid no-way audio when a Unified CM Phone forwards the call to another Webex phone.

Step 10 Configure the following SIP profile required to convert SIPS URIs back to SIP as Webex does not support SIPS URI in the request/response messages (but needs them for SRV query, for example, _sips._tcp.). Rule 20 modifies the From header to include the Trunk Group OTG/DTG parameter from Control Hub to uniquely identify a LGW site within an enterprise. In the example below, wxc-mig-bootcamp-hq-trk3638_lgu is used and you can see it in the trunk configuration and highlighted in the configuration.

Important: Make sure you replace the example with your respective Trunk Group OTG/DTG information that you copied from notepad in the previous scenario.

```
configure terminal
voice class sip-profiles 200
rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
rule 11 request ANY sip-header From modify "<sips:(.*)" "<sip:\1"
rule 12 request ANY sip-header Contact modify "sips:(.*)" "sip:\1;transport=tls"
rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
rule 20 request ANY sip-header From modify ">" ";otg=wxc-mig-bootcamp-hq-trk6697_lgu>"
rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
end
```



LGW-Trunk-Configuration.txt - Notepad
File Edit Format View Help

```
Trunk Group OTG/DTG
wxc-mig-bootcamp-hq-trk6697_lgu

Outbound Proxy Address
dfw12.sipconnect-us.bcld.webex.com

Registrar Domain
40462196.cisco-bcld.com

Line/Port
WxC-Mig-Bootcamp-HQ-Trk4130_LGU@40462196.cisco-bcld.com

Username
WxC-Mig-Bootcamp-HQ-Trk6697_LGU

Password
6A%2-}8G0)
```

Step 11 Configure the voice class tenants specifically related to the connection to the CUCM. First you will configure the Voice Class Tenant 100 that will be applied on all OUTBOUND dial peers facing the CUCM.

```
configure terminal
voice class tenant 100
session transport udp
url sip
error-passthru
bind control source-interface GigabitEthernet2
bind media source-interface GigabitEthernet2
no pass-thru content custom-sdp
end
```

Step 12 Configure now the Voice Class Tenant 300 that will be applied on all INBOUND dial peers from the CUCM.

```
configure terminal
voice class tenant 300
bind control source-interface GigabitEthernet2
bind media source-interface GigabitEthernet2
no pass-thru content custom-sdp
end
```

Step 13 This is the **MOST IMPORTANT** step to configure the Local Gateway. You will need all the configuration you copied in the “LGW-Trunk-Configuration” notepad file to create the Voice Class Tenant 200 that allows the Local Gateway to register to Webex Calling. Be sure to use the parameters obtained from the Control Hub to your own POD and that are explain in detailed bellow.

IMPORTANT: DO NOT COPY THE NEXT COMMANDS IN THE LOCAL GATEWAY CLI UNTIL YOU HAVE REPLACED ALL THE PARAMETERS WITH THE CORRECT ONES.

```
configure terminal
voice class tenant 200
registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
credentials number WxC-Mig-Bootcamp-HQ-Trk9975_LGU username WxC-Mig-Bootcamp-HQ-Trk3638_LGU password 0 kAG^V5^ZaZ realm BroadWorks
authentication username WxC-Mig-Bootcamp-HQ-Trk3638_LGU password 0 kAG^V5^ZaZ realm BroadWorks
authentication username WxC-Mig-Bootcamp-HQ-Trk3638_LGU password 0 kAG^V5^ZaZ realm 40462196.cisco-bcld.com
no remote-party-id
sip-server dns:40462196.cisco-bcld.com
connection-reuse
srtp-crypto 200
session transport tcp tls
url sips
error-passthru
asserted-id pai
bind control source-interface GigabitEthernet1
bind media source-interface GigabitEthernet1
no pass-thru content custom-sdp
sip-profiles 200
outbound-proxy dns:da09.sipconnect-us.bcld.webex.com
privacy-policy passthru
end
```

- The text in Yellow needs to be replaced by **The Register Domain** parameter.
- The text in Green needs to be replaced by the **Line/Port** parameter. **IMPORTANT**: Do not copy the entire parameter. Copy only the portion *before* the @ sign.
- The text in Turquoise needs to be replaced by the **Username** parameter.
- The text in Pink needs to be replaced by the **Password** parameter.
- The text in Blue needs to be replaced by **Outbound Proxy Address** parameter.

Explanation of the Voice Class Tenant 200 commands:

- **voice class tenant 200** - This CUBE multi-tenant feature enables specific global configurations for multiple tenants on SIP trunks that allow differentiated services for tenants.
- **registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls** - Registrar server for the Local Gateway with the registration set to refresh every two minutes(50% of 240 seconds). \
- **credentials number WxC-Mig-Bootcamp-HQ-Trk9975_LGU username WxC-Mig-Bootcamp-HQ-Trk3638_LGU password0kAG^V5^ZaZrealm BroadWorks** -Credentials for Trunk Registration challenge.
- **authentication username WxC-Mig-Bootcamp-HQ-Trk3638_LGU password 0 kAG^V5^ZaZ realm BroadWorks** - Authentication challenge for calls.
- **authentication username WxC-Mig-Bootcamp-HQ-Trk3638_LGU password 0 kAG^V5^ZaZ realm 40462196.cisco-bcld.com** - Authentication challenge for calls.

- **no remote-party-id** - Disable SIP Remote-Party-ID (RPID) header as Webex supports PAI, which is enabled using CLI asserted-id pai (see below).
- **sip-server dns:40462196.cisco-bcld.com** - Webex servers.
- **connection-reuse** - To use the same persistent connection for registration and call processing.
- **srtp-crypto 200** - Specifying SHA1_80 defined in voice class srtp-crypto 200.
- **session transport tcp tls** - Setting transport to TLS.
- **url sips** - SRV query has to be SIPS as supported by the access SBC; all other messages will be changed to SIP by sip-profile 200.
- **error-passthru** - SIP error response pass-thru functionality.
- **asserted-id pai** - Turn on PAI processing in LGW/CUBE.
- **bind control source-interface GigabitEthernet1** - Signaling source interface facing Webex.
- **bind media source-interface GigabitEthernet1** - Media source interface facing Webex.
- **no pass-thru content custom-sdp** - Default command under tenant.
- **sip-profiles 200** - To change SIPS to SIP and modify Line/Port for INVITE and REGISTER messages as defined in: voice class sip-profiles 200.
- **outbound-proxy dns:da09.sipconnect-us.bcld.webex.com** - Webex Access SBC.
- **privacy-policypassthru** - Transparently pass across privacy header valuesfrom incoming to the outgoing leg.

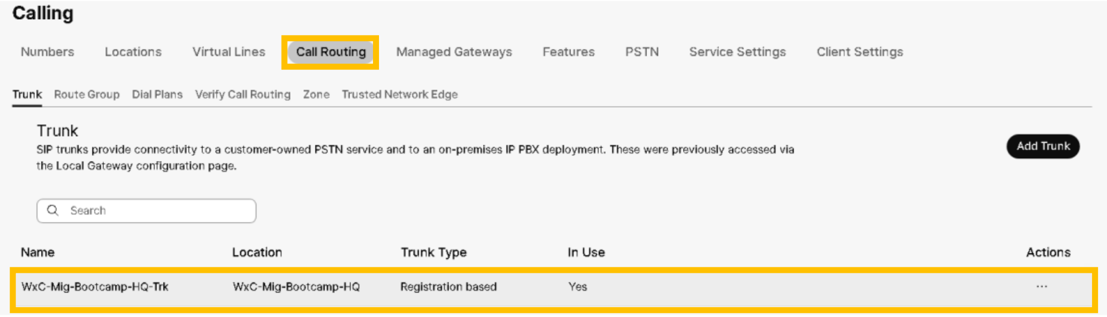
Step 14 At this point, after you have configured the Voice Class Tenant 200, the LGW is registered to Webex Calling. You will see the trunk in LGW and in Webex Calling up/online. In the LGW use the next command:

```
show sip-ua register status
```

You will see the registration status on yes **after about 2 to 3 minutes.**

```
Tenant: 200
--------------------- Registrar-Index 1 ---------------------
Line                             peer      expires(sec) reg survival P-Associ-URI
================================ ========= ============ === ======== ============
WxC-Mig-Bootcamp-HQ-Trk9975_LGU  -1        47           yes normal
```

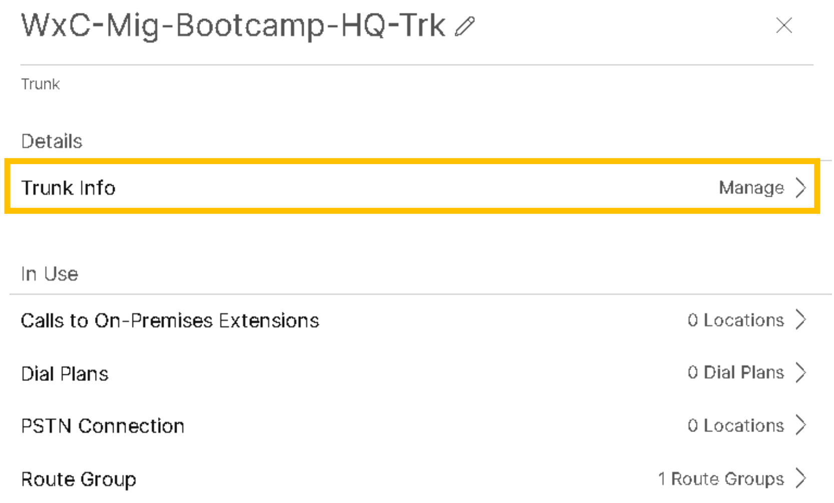
Step 15 In Webex Control Hub check the status of the Trunk you configured in the previous scenario. In order to do that, go to **Services>Calling** on the left panel, then click **Call Routing** near the top of the page, then select **WxC-Mig-Bootcamp-HQ-Trk**, and under the **Details** menu click **Trunk Info/Manage**.



Trunk

SIP trunks provide connectivity to a customer-owned PSTN service and to an on-premises IP PBX deployment. These were previously accessed via the Local Gateway configuration page.

Name	Location	Trunk Type	In Use	Actions
WxC-Mig-Bootcamp-HQ-Trk	WxC-Mig-Bootcamp-HQ	Registration based	Yes	···



WxC-Mig-Bootcamp-HQ-Trk

Trunk

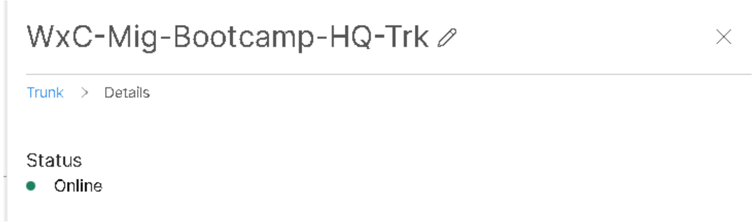
Details

Trunk Info	Manage

In Use

Calls to On-Premises Extensions	0 Locations
Dial Plans	0 Dial Plans
PSTN Connection	0 Locations
Route Group	1 Route Groups

Step 16 You can see that the trunk Status is Online. If the output of the command shows you that the registration status is now on the Local Gateway and you see the trunk Status Offline in the Webex Control Hub, check the configuration of the SIP Profile 200 and the configuration of the Voice Class Tenant 200. Review the parameters you got from the Control Hub when you created the Trunk.



WxC-Mig-Bootcamp-HQ-Trk

Trunk > Details

Status

● Online

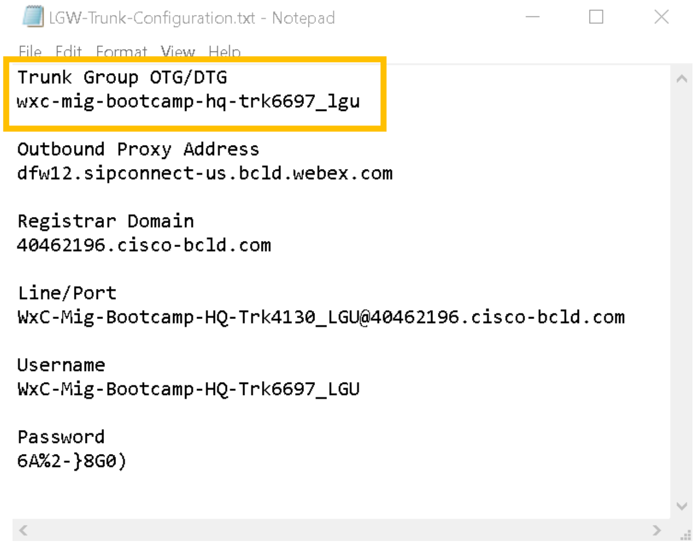
Remember that the parameters are unique to your trunk; they need to be replaced in the Voice Class Tenant configuration as it was explained in step 13.

Step 17 Now that you have the LGW registered to Webex Calling, we need to configure the dial peers required to route the calls from Webex Calling to the CUCM, and from CUCM to Webex Calling. In order to do that you need to define the pattern to uniquely identify the specific organization to be matched by the incoming dial peer in the Local Gateway from Webex Calling. This voice class URL will be used in the dial peer you configure in the next steps to receive and send calls from and to Webex Calling.

Important: In this command, you need to replace the value of the Trunk Group OTG/DTG (below in red) OTG/DTG value that you pasted in notepad. **BEFORE YOU PASTE THIS PARAMETER**, note that Local Gateway does not support the underscore "_" in the match pattern. As a workaround we are using the dot "." Wildcard (match any) to match the underscore within the Trunk Group OTG/DTG "wxc-mig-bootcamp-hq-trk3638_lgu".

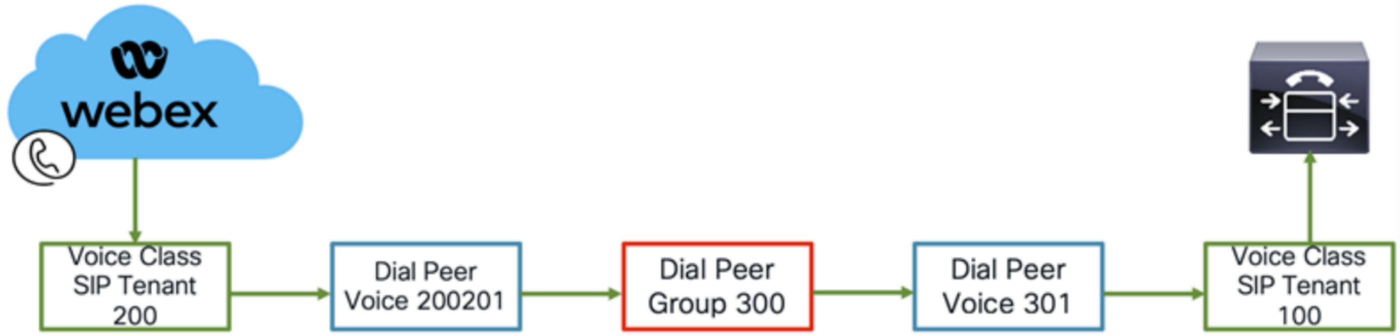
```
configure terminal
voice class uri WxCMigBootcamp sip
pattern dtg=wxc-mig-bootcamp-hq-trk6697.lgu
end
```

BE SURE TO replace the last underscore in the dtg parameter with a dot ".", as shown above.


LGW-Trunk-Configuration.txt - Notepad
File Edit Format View Help

```
Trunk Group OTG/DTG
wxc-mig-bootcamp-hq-trk6697_lgu

Outbound Proxy Address
dfw12.sipconnect-us.bcld.webex.com

Registrar Domain
40462196.cisco-bcld.com

Line/Port
WxC-Mig-Bootcamp-HQ-Trk4130_LGU@40462196.cisco-bcld.com

Username
WxC-Mig-Bootcamp-HQ-Trk6697_LGU

Password
6A%2-}8G0)
```

Before you configure the dial peers, this is the diagram for this specific lab in order to understand how the calls are routed from Webex Calling to CUCM to have internal calls for users that are on both platform sharing the same dial plan and also for calls going to the PSTN.



For the calls coming from Webex Calling to CUCM, the call uses the dial peer 200201 because there is a match using the Voice Class URI you just configured. Then the call is routed to the dial peer group 300 that points to dial peer 301. And finally, the call will be using the Voice Class Tenant 100 that is the outbound trunk to the CUCM in this lab.

Step 18 All the calls coming from Webex Calling will be routed to the CUCM, regardless if it is an internal call from users in Webex Calling to users in CUCM, or if it is a PSTN call. We need to define the CUCM as the target for the dial peer 301. In order to do that, you need to create voice class server group with all the IP addresses of the CUCM nodes with the call manager service enabled. CUCM is configured to receive these calls using the port 5065.

```
configure terminal
voice class server-group 301
ipv4 198.18.133.33 port 5065
end
```

Step 19 This is the configuration of the dial peer used to route the calls to the CUCM. The destination pattern is a wild card BAD.BAD due to all calls routed based on the dial peer group that is defined, and that is routed from the dial peer you will be using to route calls from and to Webex Calling. All the calls will be routed to the Voice Class Tenant 100 that was configured to be the trunk to the CUCM for outbound calls.

```
configure terminal
dial-peer voice 301 voip
description Outgoing dial-peer to Unified CM Webex Calling Trunk for inbound from Webex
destination-pattern BAD.BAD
session protocol sipv2
session server-group 301
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 100
no vad
end
```

Step 20 Configure the dial peer group used by the dial peer 200201 to route the calls to the CUCM according to the diagram in Step 17. As you can see in the commands below, the voice class DPG has the dial peer 301 with preference 1 to route the call.

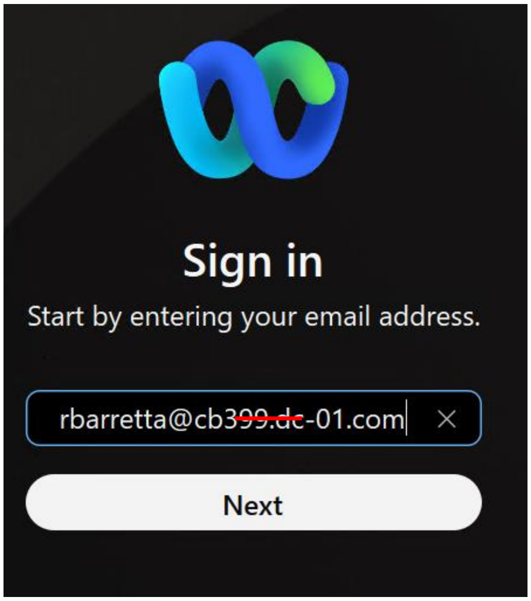
```
configure terminal
voice class dpg 300
description Incoming WxC (DP200201) to CUCM(DP301)
dial-peer 301 preference 1
end
```

Step 21 Configure the dial peer that is the one that will match the traffic coming from Webex Calling to route calls to the PSTN. There is a maximum connection limit of 250, which is the number of simultaneous calls a single Local Gateway can have with Webex Calling. You can see here that the destination is the dial peer group 300. Now you can route calls from your Webex Calling organization to the CUCM. Also this dial peer has the Voice Class Tenant 200 as the trunk to Webex Calling.

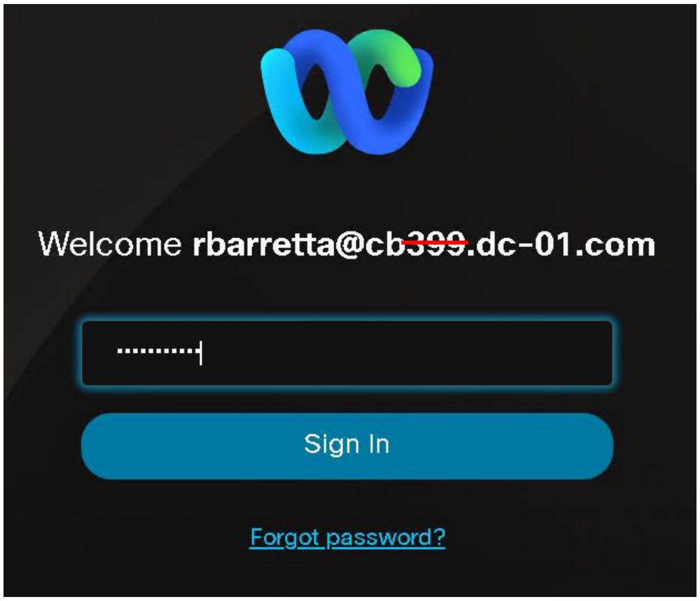
```
configure terminal
dial-peer voice 200201 voip
description Inbound/Outbound Webex Calling
max-conn 250
destination-pattern BAD.BAD
session protocol sipv2
session target sip-server
destination dpg 300
incoming uri request WxCMigBootcamp
voice-class codec 99
voice-class stun-usage 200
no voice-class sip localhost
voice-class sip tenant 200
dtmf-relay rtp-nte
srtp
no vad
end
```

Step 22 At this point you can test an internal outbound call to the CUCM from Webex Calling. On Workstation 1, open the Webex app. Sign in using the credentials for Rebekah Barretta, rbarretta@cbXXX.dc-YY.com and password dCloud**ZZZZ**!.

Important! Remember, you need to replace the XXX, YY, and ZZZZ (last four digits of your Session ID) with the information that is specific for your session.



rbarretta@cb3~~99.dc~~-01.com



Welcome rbarretta@cb~~399~~.dc-01.com

··········

Step 23 In this lab, the user Anita Perez has configured Jabber in the CUCM in order to place and receive calls to and from Webex Calling. In order to log in this user in Jabber. RDP to the **Workstation 2 (198.18.1.37)** using the Remote Desktop client with the following credentials:

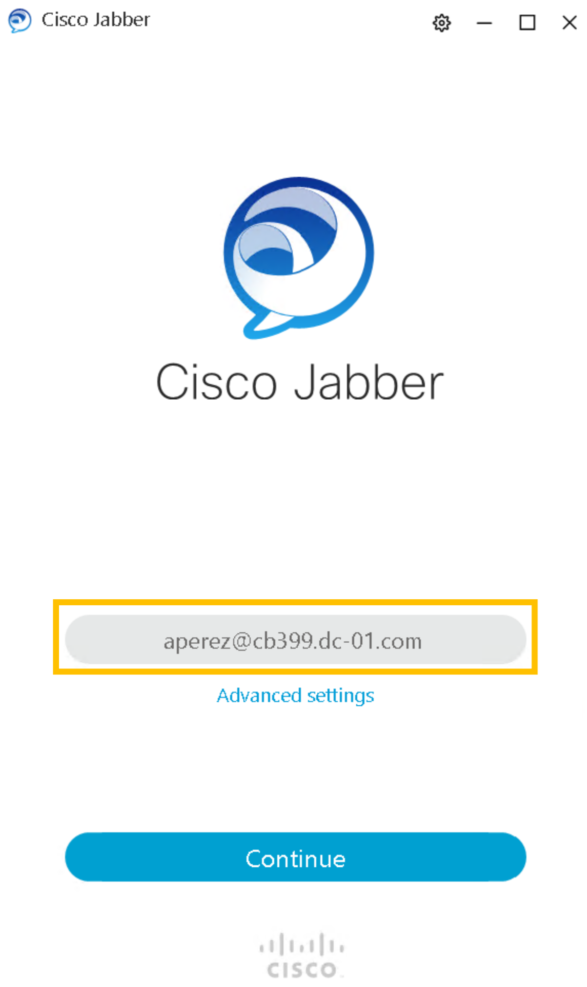
- Username: **dcloud\aperez**
- Password: **dCloud123!**

Step 24 Open the **Jabber** app and use the credentials for **Anita Perez**: **aperez@cbXXX.dc-YY.com.**

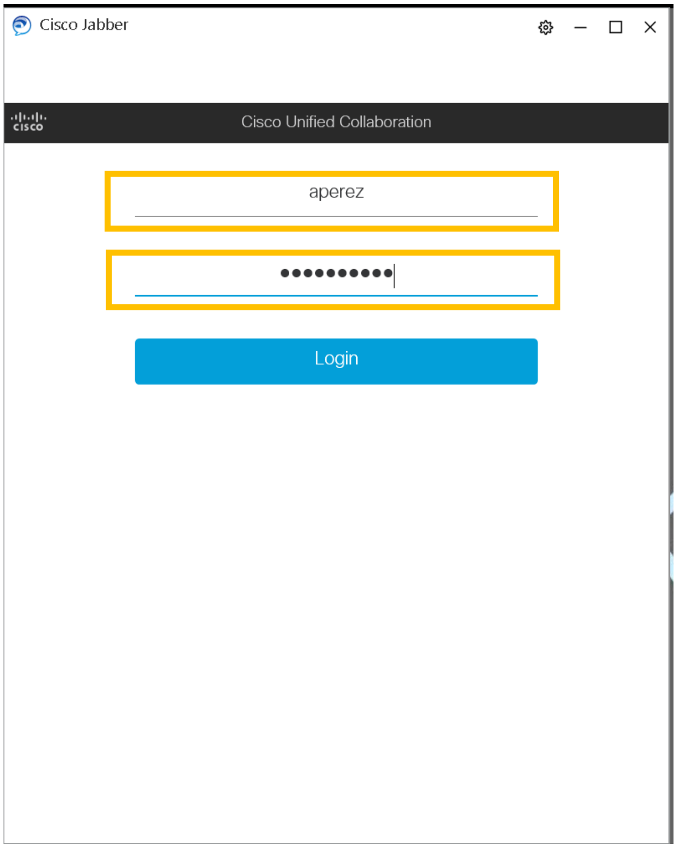
Note Remember, you need to replace the XXX and YY with the information that is specific for your POD.

Step 25 Click **Continue.**

Step 26 Use **aperez** as username and **dCloud123!** as password to login in Jabber app.



aperez@cb399.dc-01.com

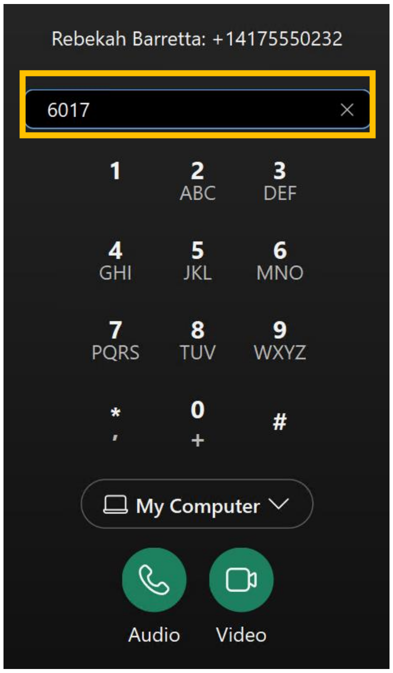


aperez

●●●●●●●●●●

Step 27 Click **Login.**

Step 28 From the **Workstation 1** using the Webex app of the **Rebekah Barretta** user, dial **6017**. You can see now that the call is made from this user in Webex Calling using the Webex app to the user in the CUCM using the Jabber app, this is an specific use case in real live scenarios.



Rebekah Barretta: +14175550232

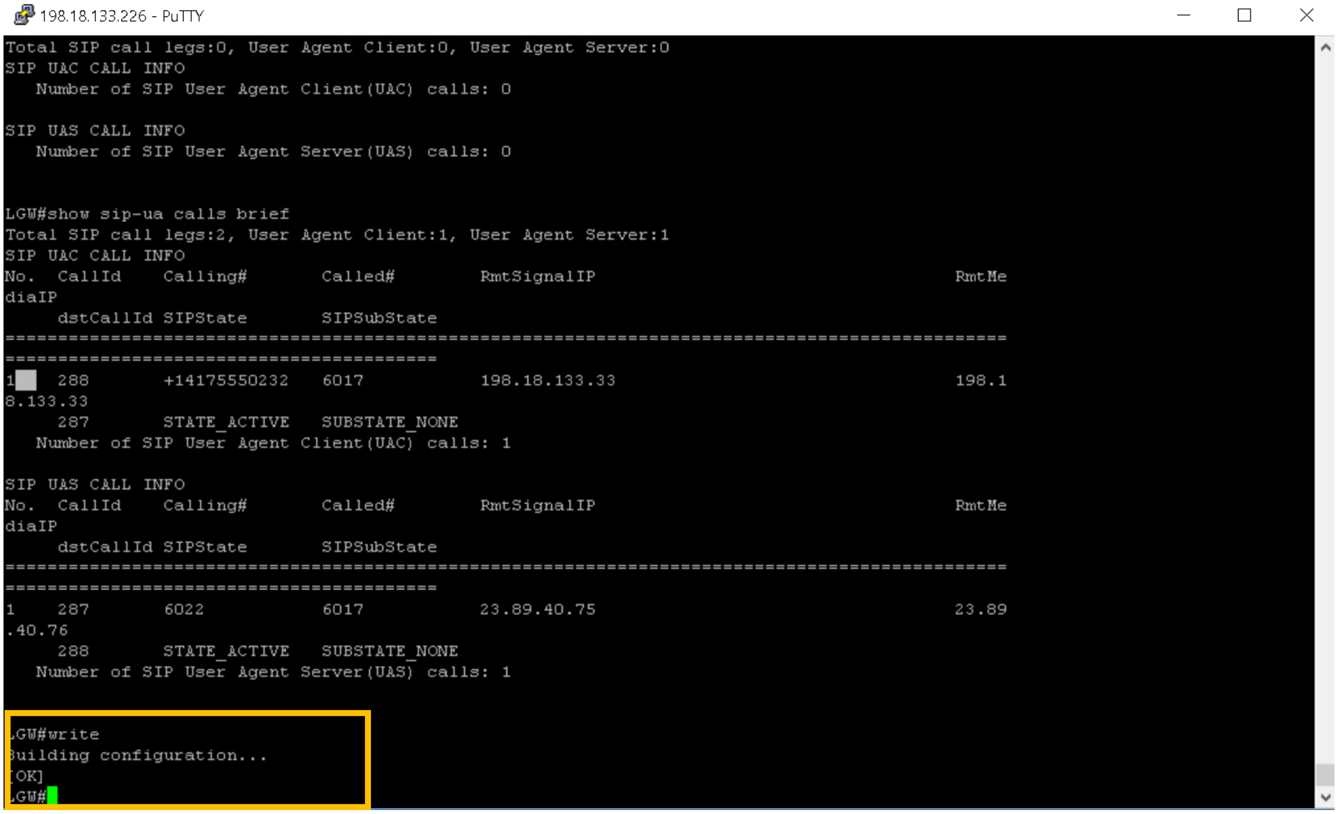
6017

Step 29 You can verify this test call flow in the Local Gateway. You can see how the call made to the 6017 number of the user Anita Perez is routed to the LGW and then to the CUCM.

```
LGW#show sip-ua calls brief
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
No.  CallId    Calling#        Called#        RmtSignalIP
RmtMediaIP
     dstCallId SIPState        SIPSubState
=========================================================================================
1    27        +14175550232    6017           198.18.133.33
198.18.133.33
     25        STATE_ACTIVE    SUBSTATE_NONE
   Number of SIP User Agent Client(UAC) calls: 1


SIP UAS CALL INFO
No.  CallId    Calling#        Called#        RmtSignalIP
RmtMediaIP
     dstCallId SIPState        SIPSubState
=========================================================================================
1    25        6022            6017           23.89.1.204
23.89.1.223
     27        STATE_ACTIVE    SUBSTATE_NONE
   Number of SIP User Agent Server(UAS) calls: 1
```

Step 30 Save the Local Gateway configuration.

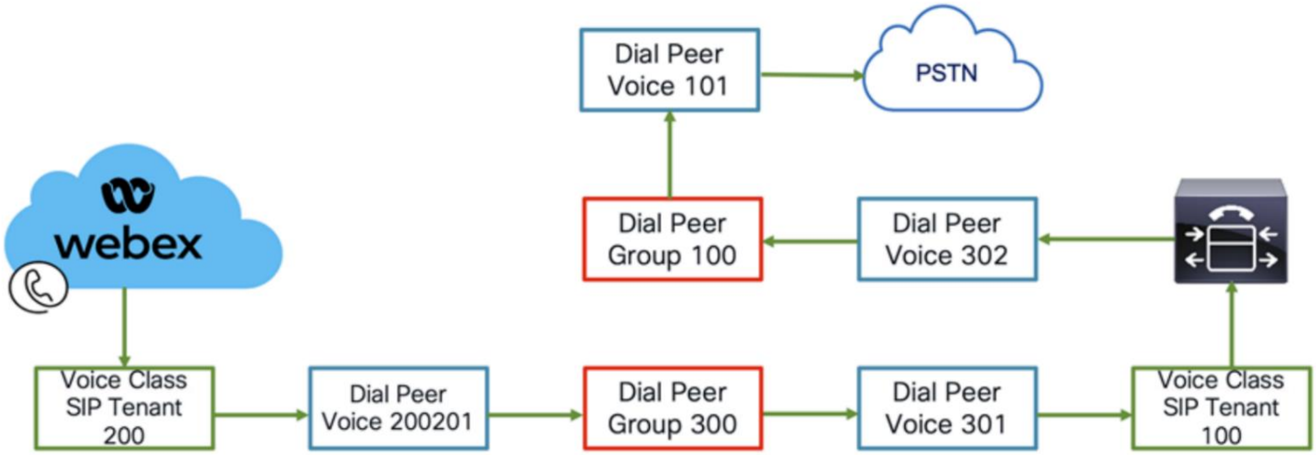
```
write
```



```
Total SIP call legs:0, User Agent Client:0, User Agent Server:0
SIP UAC CALL INFO
   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO
   Number of SIP User Agent Server(UAS) calls: 0


LGW#show sip-ua calls brief
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
No.  CallId    Calling#       Called#        RmtSignalIP                                  RmtMe
diaIP
     dstCallId SIPState       SIPSubState
===============================================================================================
=========================================
1    288       +14175550232   6017           198.18.133.33                                198.1
8.133.33
     287       STATE_ACTIVE   SUBSTATE_NONE
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
No.  CallId    Calling#       Called#        RmtSignalIP                                  RmtMe
diaIP
     dstCallId SIPState       SIPSubState
===============================================================================================
=========================================
1    287       6022           6017           23.89.40.75                                  23.89
.40.76
     288       STATE_ACTIVE   SUBSTATE_NONE
   Number of SIP User Agent Server(UAS) calls: 1


LGW#write
Building configuration...
[OK]
LGW#
```

Task 2: PSTN Calls and Inbound Calls to Webex Calling

Now that internal calls are working, you will configure the solution to have PSTN calls. To do that, remember that all the calls are routed to the CUCM, and for this lab, the calls are routed back to the LGW and then to the PSTN. This is the diagram that shows how the calls are routed from Webex Calling to CUCM and then to the PSTN.



For the calls coming from Webex Calling to PSTN, the call uses the dial peer 200201 because there is a match using the Voice Class URI configured in Scenario 9. Then the call is routed to the dial peer group 300 that points to dial peer 301 and the call will be using the Voice Class Tenant 100 that is the outbound trunk to the CUCM in this lab. The CUCM now manages the call, and it will send back the call to the LGW using the Voice Class Tenant 300. The call uses the dial peer 302 because, if it matches a voice class URI with the CUCM IP address, then the call uses the dial peer group 100 that points to dial peer 101 that has as a session target the PSTN IP Address.

Activity Procedure

Complete these steps:

Step 1 This is the configuration of the dial peer used to route the calls to the PSTN. The destination pattern is a wild card BAD.BAD due to all calls are routed based on the dial peer group that is defined and that is routed from the dial peer you will be using to route calls from and to Webex Calling. All the calls will be routed to the Voice Class Tenant 100 that was configured to be the trunk to the CUCM and to the PSTN.

```
configure terminal
dial-peer voice 101 voip
description Outgoing dial-peer to IP PSTN
destination-pattern BAD.BAD
session protocol sipv2
session target ipv4:198.18.133.3
voice-class codec 99
voice-class sip tenant 100
dtmf-relay rtp-nte
no vad
end
```

Step 2 Configure the dial peer group used by the dial peer 302 to route the calls to the PSTN. As you can see in the commands bellow, the voice class DPG has the dial peer 101 with preference 1 to route the call.

```
configure terminal
voice class dpg 100
description Incoming CUCM (DP302) to PSTN(DP101)
dial-peer 101 preference 1
end
```

Step 3 Configure the voice class uri 302 to have a match on the CUCM IP address and the port 5060 that is used by the CUCM to send calls from CUCM to the LGW. This voice class will be used by the dial peer 302 in order to match all the calls coming from the CUCM to the PSTN.

```
configure terminal
voice class uri 302 sip
pattern 198.18.133.33:5060
end
```

Step 4 Configure the dial peer 302 that is the dial peer matching the calls from CUCM to the PSTN.

```
configure terminal
dial-peer voice 302 voip
description Incoming dial-peer from CUCM for PSTN
session protocol sipv2
destination dpg 100
incoming uri via 302
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 300
no vad
end
```

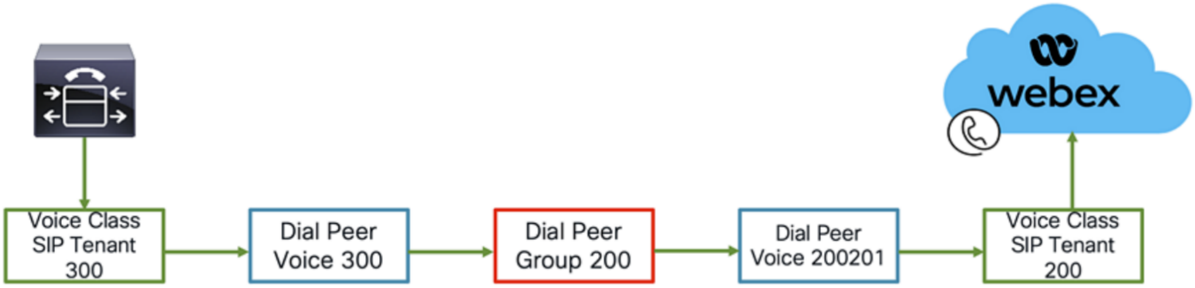
Step 5 At this point you can test an outbound call to the PSTN. In the Workstation 1 from the Webex app, you can make now a call. Let´s use the Cisco´s San Jose number in California “4085264000” if your POD is in RTP or in SJC. If your POD is on Singapore or if it is in London go to Annex A, because you have to do some configuration for this PSTN call to work. Take a look at the note below.

Note If you are doing this lab during the scheduled SRE Hands-on Labs, your POD will be in RTP. If you are doing this lab any other time, you can verify where your POD is located by looking at the Any Connect VPN host in the lab credentials:

- RTP: Anyconnect VPN host is dcloud-rtp-anyconnect.cisco.com
- SJC: Anyconnect VPN host is dcloud-sjc-anyconnect.cisco.com
- Singapore: Anyconnect VPN host is dcloud-sng-anyconnect.cisco.com
- London: Annyconnect VPN host is dcloud-lon-anyconnect.cisco.com

Now that outbound calls are working, let´s configure the dial peers and dial peer groups needed to have inbound calls.

Inbound calls from CUCM to Webex Calling:



The calls will come in from CUCM to Voice Class Tenant 300. For this part of the lab, the dial peer 300 matches based upon the voice class URL of the CUCM port 5065, then the call is routed to the dial peer group 200, and finally to the dial peer 200201 that you have already configured.

Step 6 Configure now the dial peer group 200, you can see here how this dial peer group is routing the calls to dial peer 200201.

```
configure terminal
voice class dpg 200
description Incoming CUCM (DP300) to WxC(DP200201)
dial-peer 200201 preference 1
end
```

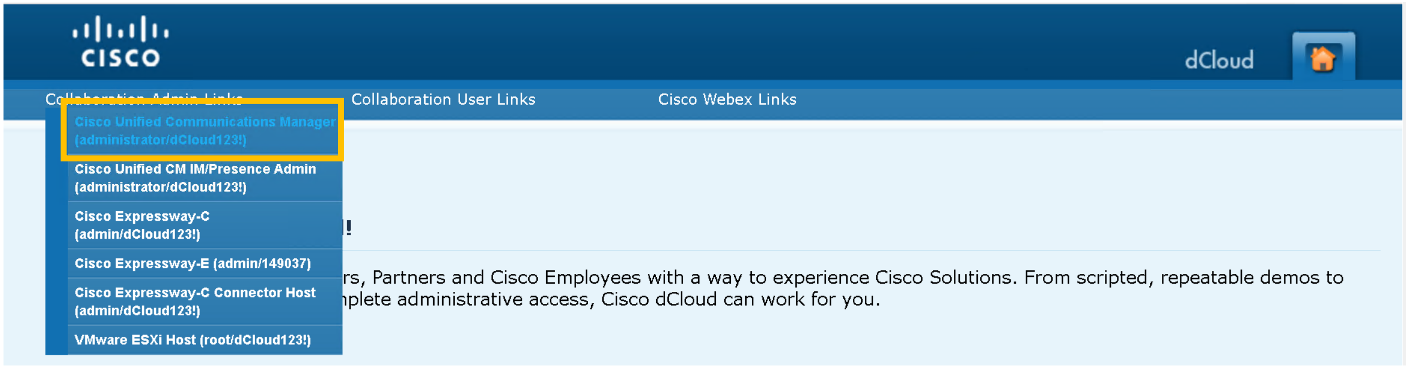
Step 7 Configure the voice class URI to match the CUCM IP address.

```
configure terminal
voice class uri 300 sip
host ipv4:198.18.133.33
end
```

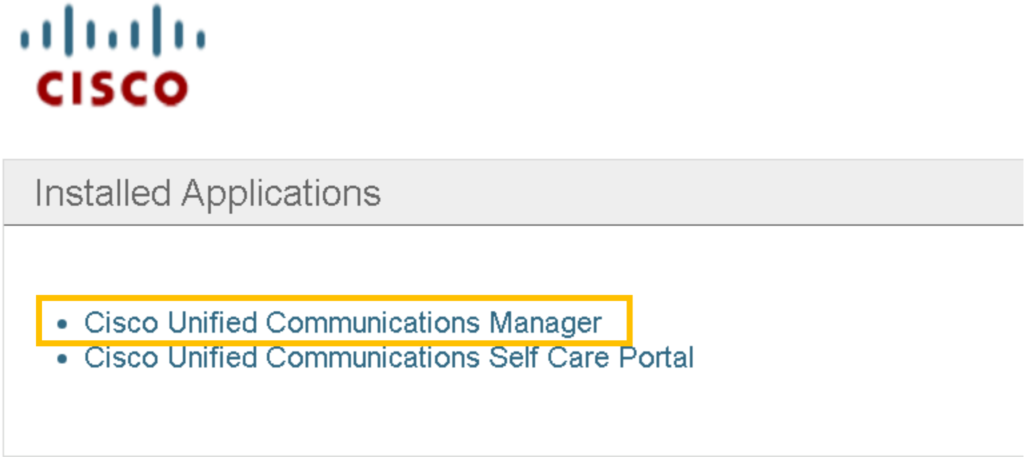
Step 8 Now configure the dial peer that matches all incoming calls from CUCM to Webex Calling, you can see here that the call is routed to the dial peer group 200 that you have already configured. In the configuration you can also see that the match for this dial peer is the voice class URI 300.

```
configure terminal
dial-peer voice 300 voip
description Incoming dial-peer from Unified CM for Webex
session protocol sipv2
destination dpg 200
incoming uri via 300
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 300
no vad
end
```

Step 9 You have now to configure CUCM to route internal calls to Webex Calling, for this specific case we have one user in Webex Calling configured with the extension 6022, you are going to configure a route pattern in CUCM for this extension number. In order to do that open Chrome browser in Workstation1 and under Collab Admin Links click on Cisco Unified Communications Manager.

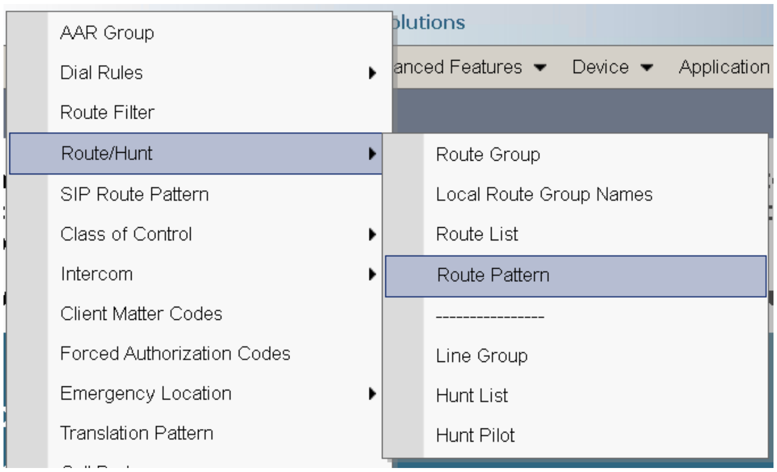

cisco
dCloud
Collaboration Admin Links
Collaboration User Links
Cisco Webex Links
Cisco Unified Communications Manager (administrator/dCloud123!)
Cisco Unified CM IM/Presence Admin (administrator/dCloud123!)
Cisco Expressway-C (admin/dCloud123!)
Cisco Expressway-E (admin/149037)
Cisco Expressway-C Connector Host (admin/dCloud123!)
VMware ESXi Host (root/dCloud123!)
!

rs, Partners and Cisco Employees with a way to experience Cisco Solutions. From scripted, repeatable demos to nplete administrative access, Cisco dCloud can work for you.


cisco
Installed Applications
Cisco Unified Communications Manager
Cisco Unified Communications Self Care Portal

Step 11 Log in to CUCM with USERNAME: **administrator** PASSWORD: **dCloud123!**

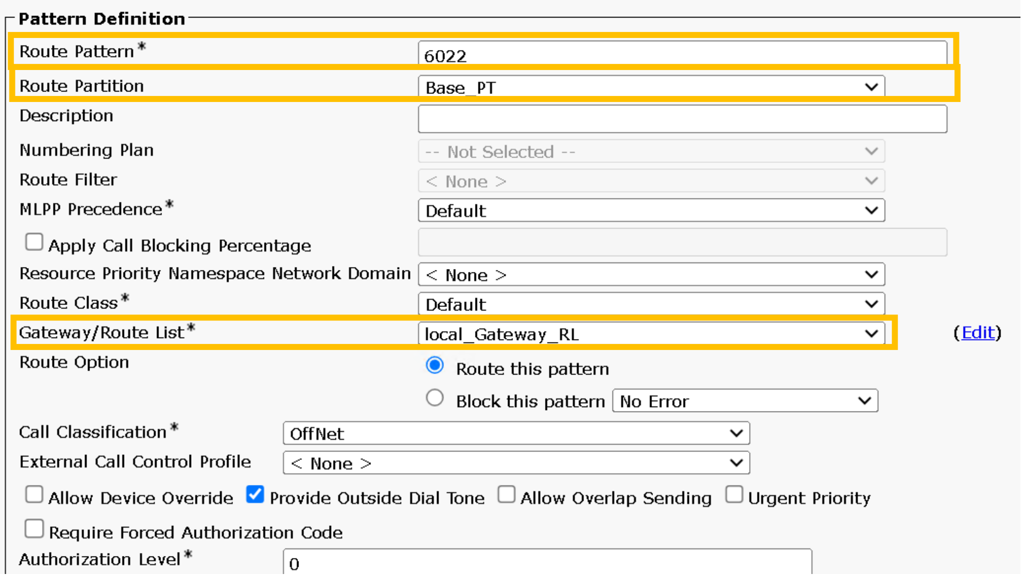
Step 12 Go to **Call Routing**, **Route Hunt**, and **Route Pattern**.



Step 13 Click **Add New.**

Step 14 Configure the Route Pattern with the following parameters.

Field Name	Value
Route Pattern	6022
Route Partition	Base_PT
Gateway/Route List	Local_Gateway_RL



Pattern Definition

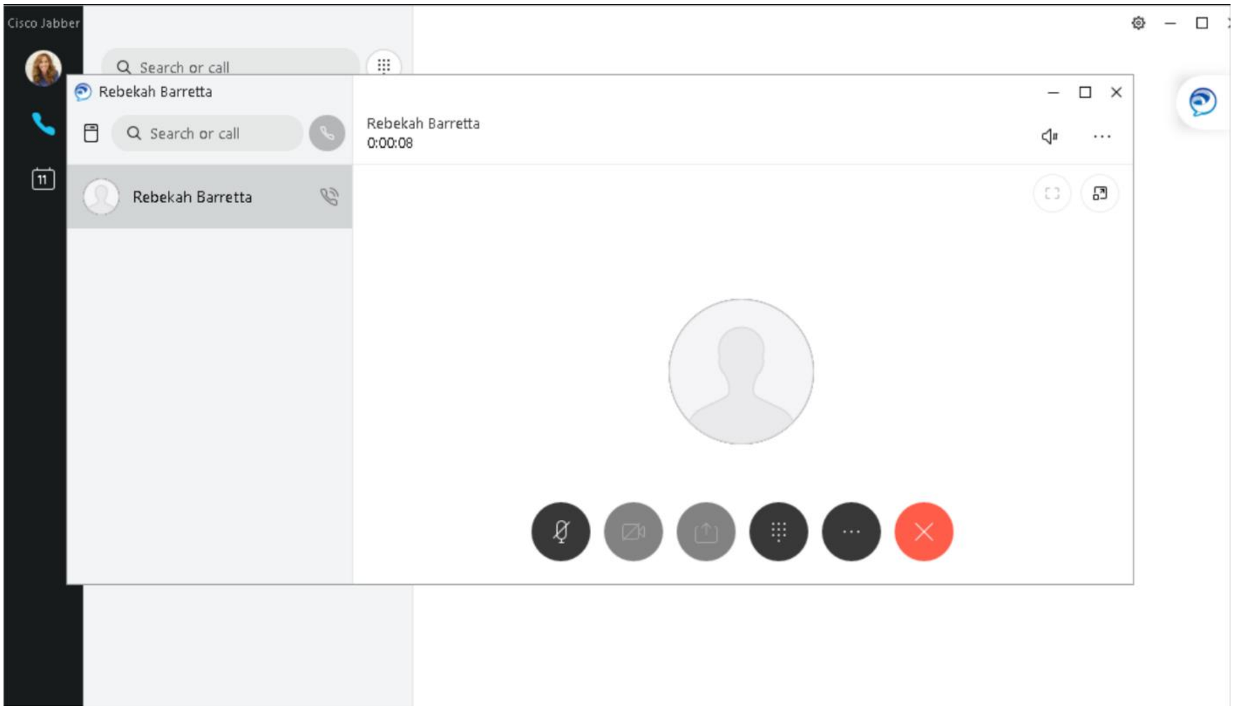
Route Pattern*	6022
Route Partition	Base_PT
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	local_Gateway_RL (Edit)
Route Option	● Route this pattern ○ Block this pattern No Error
Call Classification*	OffNet
External Call Control Profile	< None >
Authorization Level*	0

□ Allow Device Override ☑ Provide Outside Dial Tone □ Allow Overlap Sending □ Urgent Priority

□ Require Forced Authorization Code

Step 15 Click **Save**, then click **OK**, and **OK** again.

Step 16 You can now test a call from the user using Jabber registered to CUCM to the user in Webex Calling. In the Workstation 2 from the Jabber app you can dial Rebekah Barretta's extension –6022.



There is one configuration remaining. You are going to configure the Local Gateway to have inbound calls from the PSTN. For this lab, all the calls coming from the PSTN are going to be routed to the CUCM and with the configuration you just did this calls will be routed to Webex Calling.

Step 17 Configure the server group in order to match all the IP addresses of CUCM with the callmanager service on.

```
configure terminal
voice class server-group 305
ipv4 198.18.133.33
end
```

Step 18 Configure the dial peer 305 that matches the CUCM server group.

```
configure terminal
dial-peer voice 305 voip
description Outgoing dial-peer to Unified CM PSTN SIP trunk
destination-pattern BAD.BAD
session protocol sipv2
session server-group 305
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 100
no vad
end
```

Step 19 Configure the dial peer group 302 that has dial peer 305 with priority 1 to route the calls.

```
configure terminal
voice class dpg 302
description Incoming PSTN (DP100) to CUCM(DP305)
dial-peer 305 preference 1
end
```

Step 20 Configure the voice class uri 100 that will match the IP address of the PSTN and that is used by the dial peer 100 to route all the PSTN inbound calls.

```
configure terminal
voice class uri 100 sip
host ipv4:198.18.133.3
end
```

Step 21 Configure the dial peer 100 that is the dial peer matching the IP Address of the PSTN, the calls are going to be routed to dial peer group 302 and the dial peer 305 as it is shown in step 16 above.

```
configure terminal
dial-peer voice 100 voip
description Incoming dial-peer from PSTN
session protocol sipv2
destination dpg 302
incoming uri via 100
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 300
no vad
end
```

Step 22 At this point you are able to test incoming calls. In order to do that and because this is a lab with no direct access to the PSTN, we need to add some rules in order to have the incoming calls working. In the Workstation 1 open the Notepad file DN_to_DID. Look for the 86022 number and see what the E.164 PSTN number is. That E.164 number will be the number you dial from the PSTN. Because we are receiving (due to the lab environment) we need to add a translation rule to transform this 6022 number to the E.164 number you configured earlier in this lab for the user Rebekah Barretta. Important Replace the XXXX for the number in your own lab.

```
configure terminal
voice translation-rule 1000
rule 1 /6022/ /+1417555XXXX/
end
```

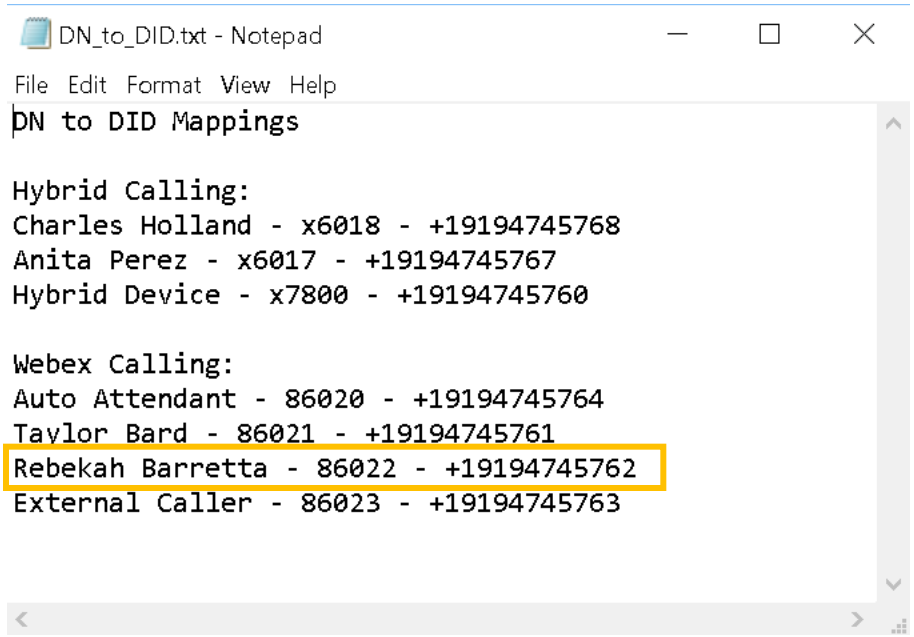
Step 23 Create the translation profile to apply the rule you just have configured.

```
configure terminal
voice translation-profile Inbound_Call
translate called 1000
end
```

Step 24 Now you can apply the voice translation profile to the outgoing dial peer 200 to route the call to Webex Calling to the E.164 number that you have configured for the user “Rebekah Barretta”. Also do not forget to write your configuration in both Local Gateway.

```
configure terminal
dial-peer voice 200201 voip
translation-profile outgoing Inbound_Call
end
write
```

Step 25 Test the incoming call dialing the E.164 that you have in the Workstation1 in the Notepad file named DN_to_DID that matches the 86022 number. You will have a call ringing on the Webex app for the user Rebekah Barretta. The image bellow is just an example, you have your own Notepad file in your lab.



```
DN to DID Mappings

Hybrid Calling:
Charles Holland - x6018 - +19194745768
Anita Perez - x6017 - +19194745767
Hybrid Device - x7800 - +19194745760

Webex Calling:
Auto Attendant - 86020 - +19194745764
Taylor Bard - 86021 - +19194745761
Rebekah Barretta - 86022 - +19194745762
External Caller - 86023 - +19194745763
```

Congratulations! You have finished the lab!

Appendix A: Complete Configurations for CUBE and Advanced Dial Plan

```
****TASK 1, STEP 3
configure terminal
key config-key password-encrypt Password123
password encryption aes
end

****TASK 1, STEP 4
configure terminal
crypto pki trustpoint dummyTp
revocation-check crl
exit
sip-ua
crypto signaling default trustpoint dummyTp cn-san-validate server
transport tcp tls v1.2
tcp-retry 1000
end

****TASK 1, STEP 5
configure terminal
crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_core.p7b
end


****TASK 1, STEP 6
show crypto pki trustpool | include DigiCert
```

```
****TASK 1, STEP 7
configure terminal
voice service voip
ip address trusted list
ipv4 23.89.0.0 255.255.0.0
ipv4 85.119.56.128 255.255.255.192
ipv4 85.119.57.128 255.255.255.192
ipv4 185.115.196.0 255.255.255.128
ipv4 185.115.197.0 255.255.255.128
ipv4 128.177.14.0 255.255.255.128
ipv4 128.177.36.0 255.255.255.192
ipv4 135.84.169.0 255.255.255.128
ipv4 135.84.170.0 255.255.255.128
ipv4 135.84.171.0 255.255.255.128
ipv4 135.84.172.0 255.255.255.192
ipv4 199.59.64.0 255.255.255.128
ipv4 199.59.65.0 255.255.255.128
ipv4 199.59.66.0 255.255.255.128
ipv4 199.59.67.0 255.255.255.128
ipv4 199.59.70.0 255.255.255.128
ipv4 199.59.71.0 255.255.255.128
ipv4 135.84.172.0 255.255.255.128
ipv4 135.84.173.0 255.255.255.128
ipv4 135.84.174.0 255.255.255.128
ipv4 199.19.197.0 255.255.255.0
ipv4 199.19.199.0 255.255.255.0
ipv4 139.177.64.0 255.255.255.0
ipv4 139.177.65.0 255.255.255.0
ipv4 139.177.66.0 255.255.255.0
ipv4 139.177.67.0 255.255.255.0
ipv4 139.177.68.0 255.255.255.0
ipv4 139.177.69.0 255.255.255.0
ipv4 139.177.70.0 255.255.255.0
ipv4 139.177.71.0 255.255.255.0
ipv4 139.177.72.0 255.255.255.0
ipv4 139.177.73.0 255.255.255.0
end
```

```
****TASK 1, STEP 8
configure terminal
voice service voip
allow-connections sip to sip
media statistics
media bulk-stats
no supplementary-service sip refer
no supplementary-service sip handle-replaces
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
stun
stun flowdata agent-id 1 boot-count 4
stun flowdata shared-secret 0 Password123$
sip
g729 annexb-all
early-offer forced
end

****TASK 1, STEP 9
configure terminal
voice class codec 99
codec preference 1 g711ulaw
codec preference 2 g711alaw
exit
voice class srtp-crypto 200
crypto 1 AES_CM_128_HMAC_SHA1_80
exit
voice class stun-usage 200
stun usage firewall-traversal flowdata
stun usage ice lite
end



****TASK 1, STEP 10 ********************* BE SURE TO REPACE XXXXXXXX WITH OTG PARAMETER
configure terminal
voice class sip-profiles 200
rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
rule 11 request ANY sip-header From modify "<sips:(.*)" "<sip:\1"
rule 12 request ANY sip-header Contact modify "sips:(.*)" "sip:\1;transport=tls"
rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
rule 20 request ANY sip-header From modify ">" ";otg=XXXXXXXXXXXXX>"
rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
end
```

```
****TASK 1, STEP 11
configure terminal
voice class tenant 100
session transport udp
url sip
error-passthru
bind control source-interface GigabitEthernet2
bind media source-interface GigabitEthernet2
no pass-thru content custom-sdp
end

****TASK 1, STEP 12
configure terminal
voice class tenant 300
bind control source-interface GigabitEthernet2
bind media source-interface GigabitEthernet2
no pass-thru content custom-sdp
end


****TASK 1, STEP 13********************* BE SURE TO REPACE ****** WITH COLOR-CODED PARAMETER IN THE LAB GUIDE
configure terminal
voice class tenant 200
registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
credentials number ***LINE/PORT username ***USERNAME password 0 ***PASSWORD realm BroadWorks
authentication username ***USERNAME password 0 ***PASSWORD realm BroadWorks
authentication username ***USERNAME password 0 ***PASSWORD realm 40462196.cisco-bcld.com
no remote-party-id
sip-server dns:40462196.cisco-bcld.com
connection-reuse
srtp-crypto 200
session transport tcp tls
url sips
error-passthru
asserted-id pai
bind control source-interface GigabitEthernet1
bind media source-interface GigabitEthernet1
no pass-thru content custom-sdp
sip-profiles 200
outbound-proxy dns:***OUTBOUND_PROXY_DNS
privacy-policy passthru
end


****TASK 1, STEP 14
show sip-ua register status
```

```
****TASK 1, STEP 17 ********************* BE SURE TO REPACE XXXXXXXX WITH OTG PARAMETER..... DO NOT USE AN UNDERSCORE!!!!
configure terminal
voice class uri WxCMigBootcamp sip
pattern dtg=XXXXXXXXXXXXXXXXXXX.lgu
end

****TASK 1, STEP 18
configure terminal
voice class server-group 301
ipv4 198.18.133.33 port 5065
end

****TASK 1, STEP 19
configure terminal
dial-peer voice 301 voip
description Outgoing dial-peer to Unified CM Webex Calling Trunk for inbound from Webex
destination-pattern BAD.BAD
session protocol sipv2
session server-group 301
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 100
no vad
end

****TASK 1, STEP 20
configure terminal
voice class dpg 300
description Incoming WxC (DP200201) to CUCM(DP301)
dial-peer 301 preference 1
end

****TASK 1, STEP 21
configure terminal
dial-peer voice 200201 voip
description Inbound/Outbound Webex Calling
max-conn 250
destination-pattern BAD.BAD
session protocol sipv2
session target sip-server
destination dpg 300
incoming uri request WxCMigBootcamp
voice-class codec 99
voice-class stun-usage 200
no voice-class sip localhost
voice-class sip tenant 200
dtmf-relay rtp-nte
srtp
no vad
end
```

```
****TASK 1, STEP 29
show sip-ua calls brief

****TASK 1, STEP 30
write



*******************************************************
****TASK 2, STEP 1
configure terminal
dial-peer voice 101 voip
description Outgoing dial-peer to IP PSTN
destination-pattern BAD.BAD
session protocol sipv2
session target ipv4:198.18.133.3
voice-class codec 99
voice-class sip tenant 100
dtmf-relay rtp-nte
no vad
end

****TASK 2, STEP 2
configure terminal
voice class dpg 100
description Incoming CUCM (DP302) to PSTN(DP101)
dial-peer 101 preference 1
end

****TASK 2, STEP 3
configure terminal
voice class uri 302 sip
pattern 198.18.133.33:5060
end



****TASK 2, STEP 4
configure terminal
dial-peer voice 302 voip
description Incoming dial-peer from CUCM for PSTN
session protocol sipv2
destination dpg 100
incoming uri via 302
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 300
no vad
end
```

```
****TASK 2, STEP 6
configure terminal
voice class dpg 200
description Incoming CUCM (DP300) to WxC(DP200201)
dial-peer 200201 preference 1
end



****TASK 2, STEP 7
configure terminal
voice class uri 300 sip
host ipv4:198.18.133.33
end


****TASK 2, STEP 8
configure terminal
dial-peer voice 300 voip
description Incoming dial-peer from Unified CM for Webex
session protocol sipv2
destination dpg 200
incoming uri via 300
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 300
no vad
end


****TASK 2, STEP 17
configure terminal
voice class server-group 305
ipv4 198.18.133.33
end


****TASK 2, STEP 18
configure terminal
dial-peer voice 305 voip
description Outgoing dial-peer to Unified CM PSTN SIP trunk
destination-pattern BAD.BAD
session protocol sipv2
session server-group 305
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 100
no vad
end
```

```
****TASK 2, STEP 19
configure terminal
voice class dpg 302
description Incoming PSTN (DP100) to CUCM(DP305)
dial-peer 305 preference 1
end


****TASK 2, STEP 20
configure terminal
voice class uri 100 sip
host ipv4:198.18.133.3
end



****TASK 2, STEP 21
configure terminal
dial-peer voice 100 voip
description Incoming dial-peer from PSTN
session protocol sipv2
destination dpg 302
incoming uri via 100
voice-class codec 99
dtmf-relay rtp-nte
voice-class sip tenant 300
no vad
end

****TASK 2, STEP 22
configure terminal
voice translation-rule 1000
rule 1 /6022/ /+1417555XXXX/
end


****TASK 2, STEP 23
configure terminal
voice translation-profile Inbound_Call
translate called 1000
end


****TASK 2, STEP 24
configure terminal
dial-peer voice 200201 voip
translation-profile outgoing Inbound_Call
end
write
```