



Deploying a Multi-tenant Webex Calling Certificate- based Local Gateway with Cisco Unified Border Element (CUBE-HA) [IOS- XE 17.9.1a]

August 5, 2023

Table of Contents

Introduction	5
Network Topology.....	6
System Components	7
Hardware Requirements.....	7
Software Requirements	7
Features	8
Features Supported	8
Features Not Supported.....	8
Caveats.....	9
Configuration	10
1 Configuring Cisco Webex Calling in Tenant 1.....	10
1.1 Add location-Trunk	10
1.2 Adding user.....	20
1.3 Adding Devices	24
1.4 Assign main number to a location.....	28
2 Configuring Cisco Webex Calling in Tenant 2.....	29
2.1 Add location-Trunk	29
3 Cisco CUBE Configuration.....	39
3.1 IP Networking	39
3.2 IP Routing	41
3.3 DNS Servers	41
3.4 Certificates.....	41
3.5 Global Cisco CUBE settings.....	47
3.6 Configure Redundancy group.....	49
3.7 SRTP crypto.....	50
3.8 STUN ICE-lite.....	50
3.9 Codecs	50
3.10 Options keepalive to Webex Calling	50
3.11 Message Handling Rules.....	53
3.12 Specify the trust point in TLS profile.....	57
3.13 Tenant	58
3.14 Number translation rules	60

3.15	Dial peers.....	60
3.16	Running Configuration	65
3.17	Show commands	87
	Important Information.....	101

Table of Figures

Figure 1: Network Topology.....	6
Figure 2: Control Hub Services.....	10
Figure 3: Locations	11
Figure 4: Location creation or selection	11
Figure 5: Add location details.	12
Figure 6: Add location details Contd.,.....	12
Figure 7: Add Trunk details Contd.,	13
Figure 8: Add Trunk details Contd.	14
Figure 9: Add Trunk details Contd.,	15
Figure 10: PSTN Connection.....	16
Figure 11: PSTN Connection Contd.,	17
Figure 12: PSTN Connection Contd.,	17
Figure 13: Add Numbers	18
Figure 14: Add Numbers Contd.,.....	19
Figure 15: Add Numbers Contd.,.....	19
Figure 16: Adding Users	20
Figure 17: Manually Add or Modify Users	20
Figure 18: Adding email address and name.....	21
Figure 19: Confirm Adding	21
Figure 20: Add Services for Users	22
Figure 21: Assign Numbers	22
Figure 22: Add User successful.	23
Figure 23: Add Devices Window	24
Figure 24: Assign to a user or a place	25
Figure 25: User Association with Device.....	26
Figure 26: Select Device and add MAC address.....	27
Figure 27: Assign Main number in location.	28
Figure 28: Control Hub Services.....	29
Figure 29: Add location.	30
Figure 30: Add location details.	31
Figure 31: Add location details Contd.,.....	31
Figure 32: Add Trunk details Contd.,	32
Figure 33: Add Trunk details Contd.	33
Figure 34: Add Trunk details Contd.,	34
Figure 35: PSTN Connection.....	35
Figure 36: PSTN Connection Contd.,	36
Figure 37: PSTN Connection Contd.,	36
Figure 38: Add Numbers	37
Figure 39: Add Numbers Contd.,.....	38
Figure 40: Add Numbers Contd.,.....	38

Introduction

This application note describes a tested Cisco Unified Border Element High Availability (CUBE-HA) configuration for connecting a Webex Calling Multi-tenant certificate-based Local Gateway to the IP PSTN. Please refer to provider documentation and content provided at www.cisco.com/go/interoperability for guidance on how to adjust this tested configuration to meet the specific requirements of your trunking service.

This document assumes the reader is knowledgeable with the terminology and configuration of CUBE. The configuration settings specifically required for Webex Calling certificate-based LGW along with multi-tenancy are presented. Feature configuration and most importantly the dial plan is customer specific and need individual approach.

- **This application note describes how to configure a Webex Calling certificate-based LGW running on a Catalyst C8300 CUBE platform [IOS-XE 17.9.1a] with a public IP address and behind a NAT for connectivity to a PSTN SIP Trunking service.**
- Testing was performed in accordance with Webex Calling certificate-based Local Gateway test methodology and among features verified were – basic calls, DTMF transport, Music on Hold (MOH), semi-attended, attended, and blind transfers, call forward and conference.
- The CUBE configuration presented in this document is based on a lab environment with a simple dial-plan used to ensure proper interoperability between PSTN network and Cisco Webex Calling Certificate-based Local Gateway. The configuration described in this document details the important configuration settings to enable interoperability to be successful and care must be taken by the network administrator deploying Cisco Webex Calling Certificate-based Local Gateway trunk to successful interworking with the service provider network.

Network Topology

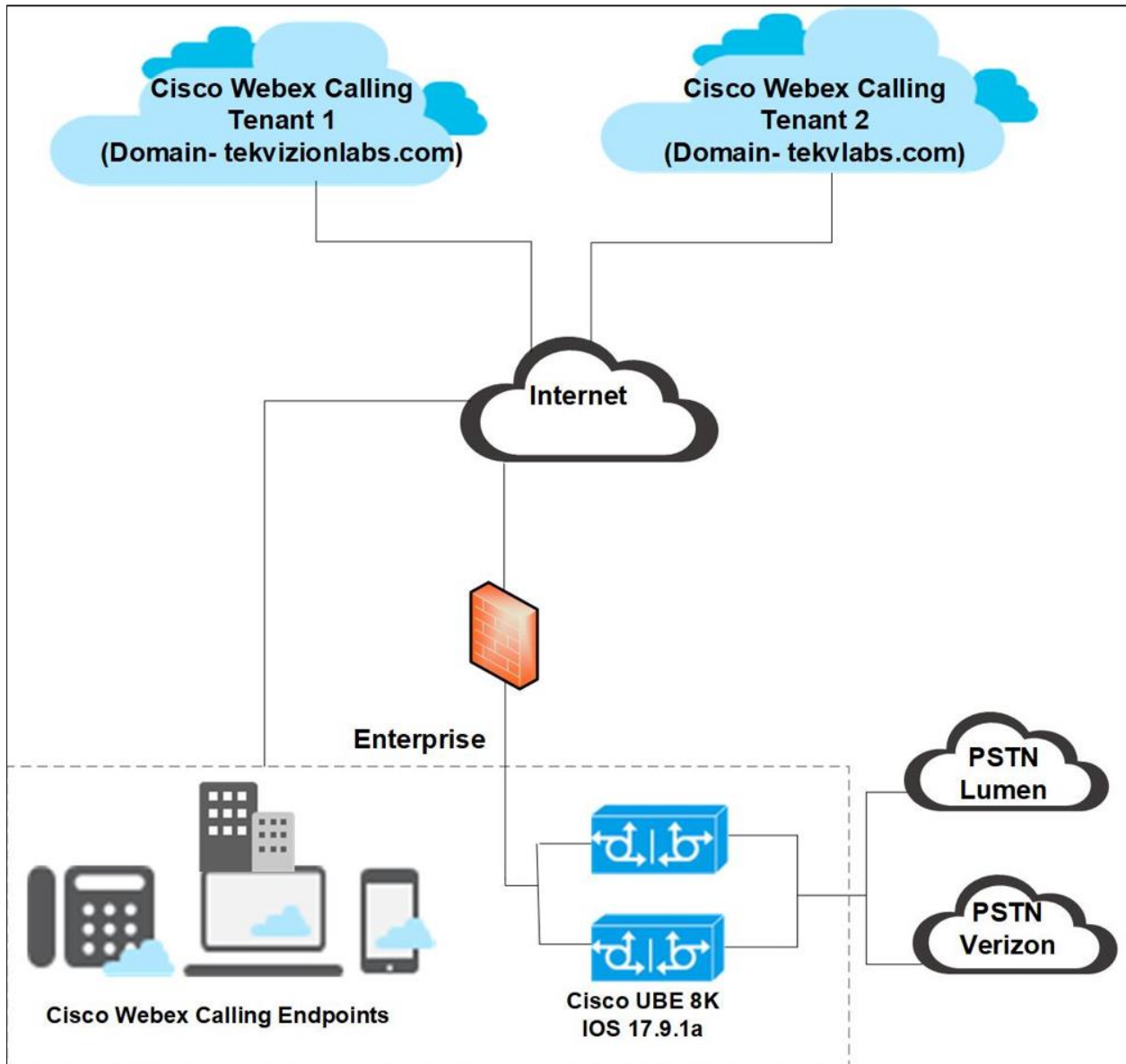


Figure 1: Network Topology

Cisco Webex Calling and Cisco CUBE Settings:

Setting	Value
Transport from Cisco CUBE to Cisco Webex Calling	TLS with SRTP
Transport from Cisco CUBE to PSTN Lumen	TCP with RTP
Transport from Cisco CUBE to PSTN Verizon	UDP with RTP

System Components

Hardware Requirements

- Cisco CUBE platform 8300-1N1S-6T
- Cisco IP Phones with Multiplatform Firmware connected with Webex users to make calls.
- Cisco ATA 19X to connect FAX in Webex control hub.

Software Requirements

- Cisco CUBE:
 - 14.6 running IOS-XE 17.9.1a
 - Cisco IOS Software [Cupertino], c8000be Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.9.1a, RELEASE SOFTWARE (fc2)
- Cisco MPP-Version: sip68xx.11-3-7MPP0001-272.loads
- Cisco MPP-Version: sip8845_65.11-3-7MPP0001-272.loads
- Cisco ATA 19X-MPP-Version: 11-2-2MPP0101-013

Features

Features Supported

- Incoming and outgoing calls using G711ulaw voice codecs
- Call Conference
- Fax
 - G711 Pass-through
- Auto Attendant
- Call hold & Resume (MoH)
- Semi-attended and Attended Call transfer
- Blind Transfer
- Call forward all
- DTMF (RFC2833)
- IP-PBX Calling number privacy

Features Not Supported

- Webex does not currently support GCM crypto encryption suite.

Caveats

The following are the observations from Cisco CUBE.

- During Webex call hold scenarios, two Re-INVITE messages are sent by Webex. One is sent with the "send-only" attribute, while the other includes "send-recv." It is important to note that this behavior does not impact user experience, as call hold and resume functions seamlessly function with Music on Hold (MOH) during this process.
- In video call redundancy, audio is preserved on failover, but video is not preserved.
- Webex does not negotiate ICE candidate attributes with ATA 19X FAX or with video in MPP phones.

The following are the observations when Cisco CUBE is behind NAT.

- The media establishment behavior is as follows when a Webex user is connected both inside and outside of a NAT firewall:
 - When the Webex user is connected to the internal network, ICE candidates are not nominated. However, STUN request and response occurs between the Webex user and CUBE. As a result, ICE Re-INVITE is not received from Webex and media connection is established between the Webex relay server IP in the call, ensuring bi-directional audio functionality.
 - On the other hand, when the Webex user is connected to an external NAT (public network), ICE Re-INVITE is received, containing the nominated candidate of the Webex user's public IP. This leads to the establishment of media between the Webex user's public IP and CUBE.
 - In summary, the behavior varies based on the user's network configuration, with ICE candidates behaving differently in each scenario to facilitate media establishment.
- Call Park and retrieve functionality test: During this test, Webex user 1, located in the internal network, initiates a call park against Webex user 2, who is in an external public network. Webex user 2 successfully receives the notification of the call park. However, when attempting to retrieve the parked call using the unpark button, the call retrieval fails. As a result, this behavior is considered a failure for the test scenario.

Configuration

1 Configuring Cisco Webex Calling in Tenant 1

1.1 Add location-Trunk

Step1:

Login to Cisco Webex Control Hub and navigate to Services.

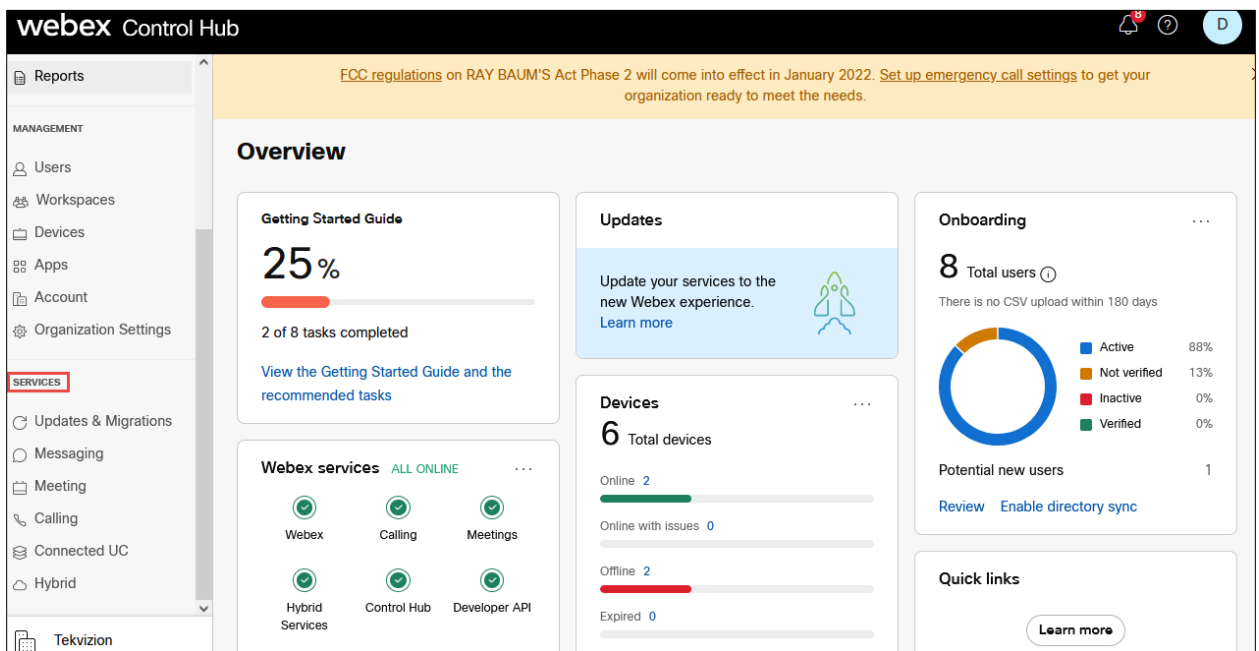


Figure 2: Control Hub Services

Step 2:

Navigate to **Calling** and click on **Locations**.

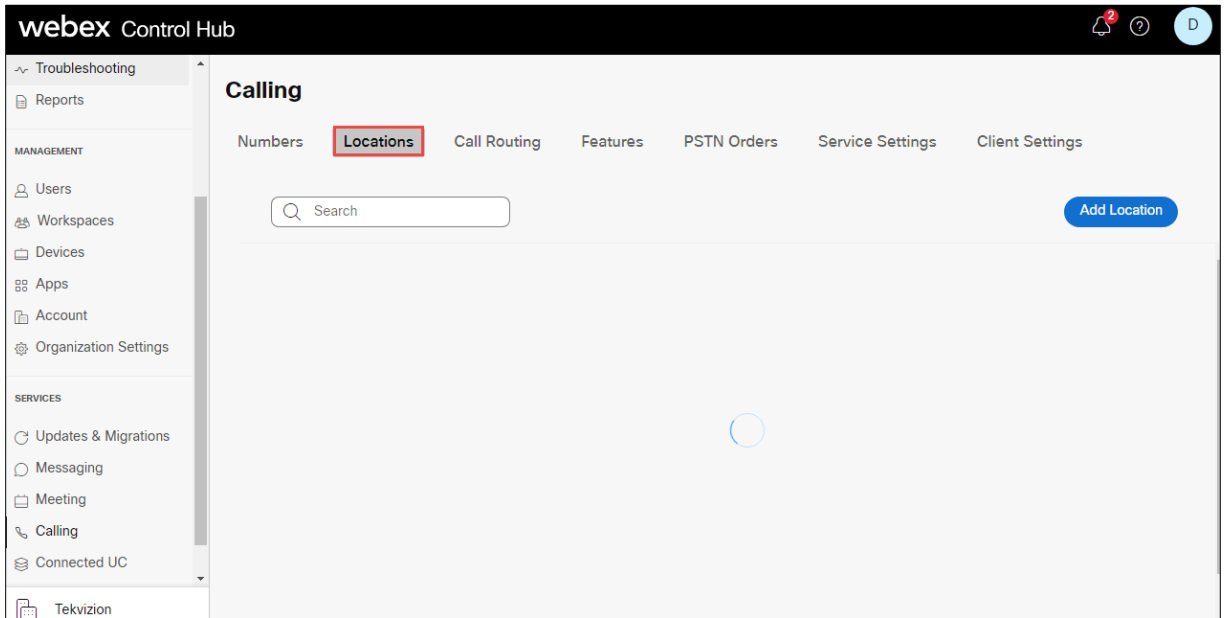


Figure 3: Locations

Step 3:

Click on **Add Location**

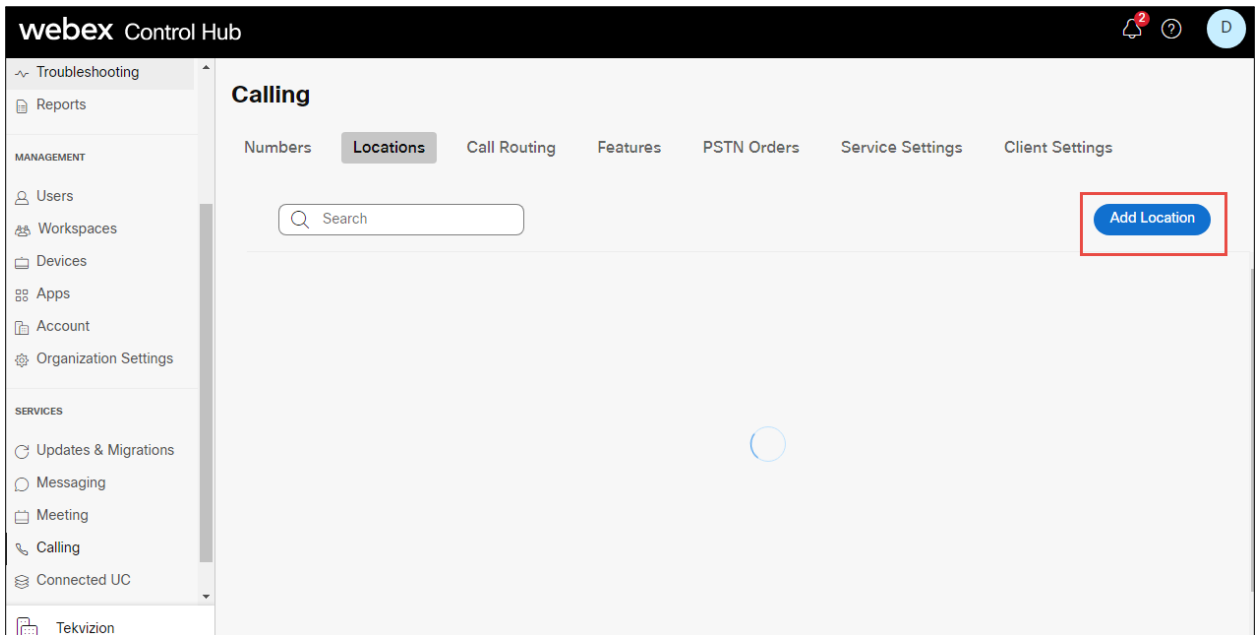


Figure 4: Location creation or selection

Step 4:

Enter **Location** details and click **save**. After adding the location, you will be prompted to add connection type, select No for the connection type. It can be added later.

The screenshot shows a form titled "Add Location" with a red border. The form is divided into two columns. The left column contains: "Location Name" with a text input field containing "Cisco"; "Country/Region" with a dropdown menu showing "United States of America"; "Location Address" with a text input field containing "3701 W Plano Pkwy ste 300" and a secondary field for "Street address line 2 (optional)"; and "City/Town" with a text input field containing "Plano". The right column contains: "Announcement Language" with a dropdown menu showing "English"; "Email Language" with a dropdown menu showing "English - American English"; and "Time zone" with a dropdown menu showing "Select a time zone". Each input field has a small 'x' icon for clearing the text.

Figure 5: Add location details.

This screenshot shows the continuation of the "Add Location" form. The left column contains: "City/Town" with a text input field containing "Plano"; "State/Province/Region" with a dropdown menu showing "Texas"; and "Zip/Postal code" with a text input field containing "75075-7840". At the bottom right of the form, there are two buttons: "Cancel" and "Save". The "Save" button is highlighted with a red border.

Figure 6: Add location details Contd.,

Step 5:

Navigate to **Calling** → **Call Routing** → **Add Trunk** and provide the details of Location and name for the SIP Trunk

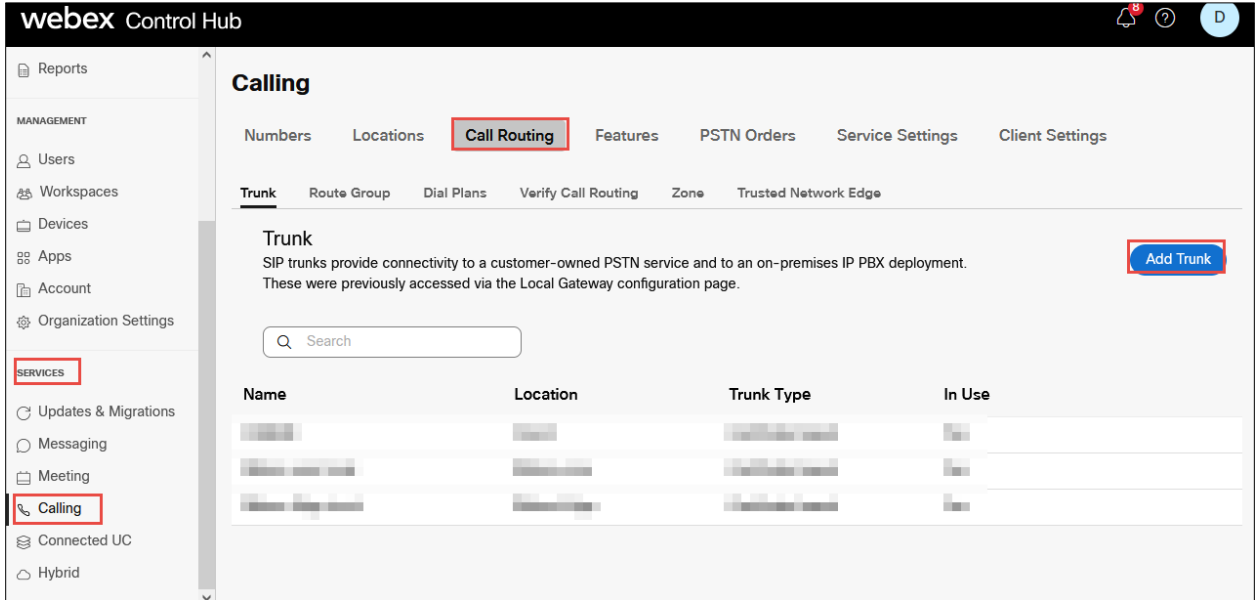


Figure 7: Add Trunk details Contd.,

Add Trunk

Location
This location is where the trunk is physically connected. To create a new location, visit the [Locations](#) page.

Cisco1

Name

CUBE8K|

Trunk Type
Choose the right trunk type for this local gateway. [Learn more](#) on trunk type

Certificate based

Device Type

Cisco Unified Border Element

Enterprise Session Border Controller (SBC) Address

Select the type and enter an FQDN or SRV address for Webex Calling to reach out to your Enterprise SBC. You must also [add and verify](#) your domains before you can use this address. [Manage your domains](#)

FQDN
 SRV

Hostname *	Domain *	Port *
<input type="text" value="sbc6"/>	<input type="text" value="tekvizionlabs.com"/>	<input type="text" value="5061"/>

FQDN

Maximum number of concurrent calls *

Dual Identity Support

The Dual Identity Support setting impacts the handling of the From header and P-Asserted-Identity (PAI) header when sending an initial SIP INVITE to the trunk for an outbound call. When enabled, the From and PAI headers are treated independently and may differ. When disabled, the PAI header is set to the same value as the From header. Please refer to the documentation for more details.

Figure 8: Add Trunk details Contd.

Add Trunk



CUBE8K 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 ⓘ

● Unknown

Webex Calling edge proxy address (FQDN)

peering1.us.sipconnect.bclid.webex.com:5062
peering2.us.sipconnect.bclid.webex.com:5062
peering3.us.sipconnect.bclid.webex.com:5062
peering4.us.sipconnect.bclid.webex.com:5062

Webex Calling edge proxy address (SRV)

us01.sipconnect.bclid.webex.com

Figure 9: Add Trunk details Contd.,

Step 6:

Choose the location and select Manage in PSTN Connection to add Connection type.

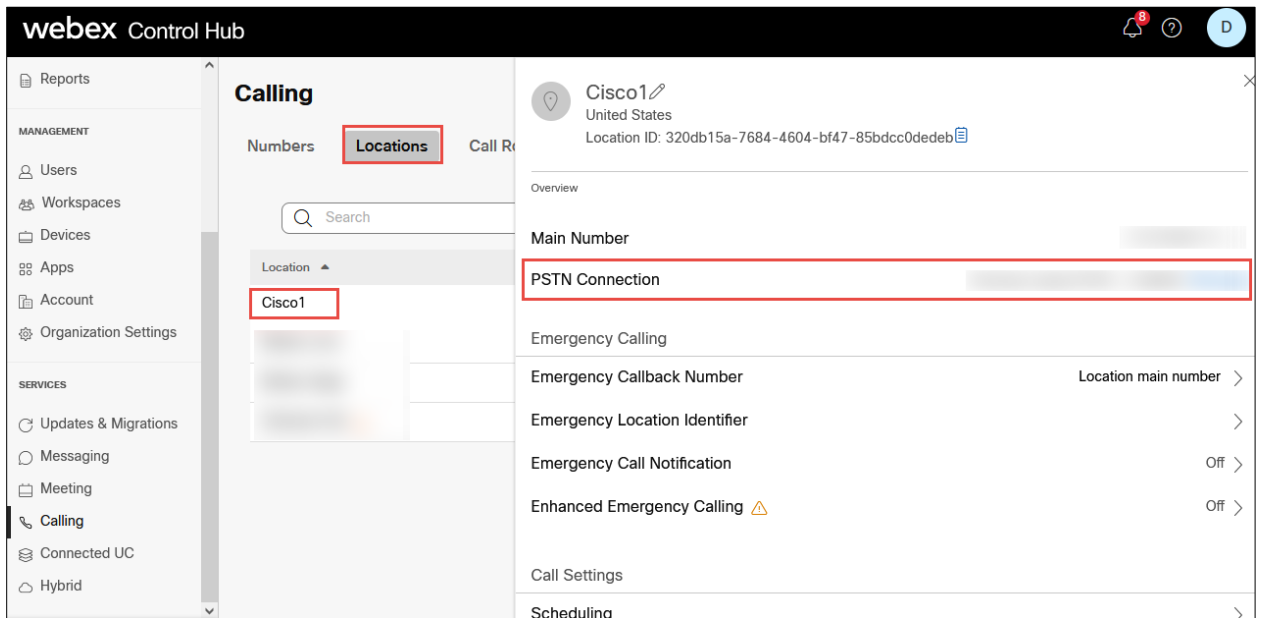


Figure 10: PSTN Connection

Step 7:

Select the **Connection Type** as **Premises-based PSTN** and click on Next.

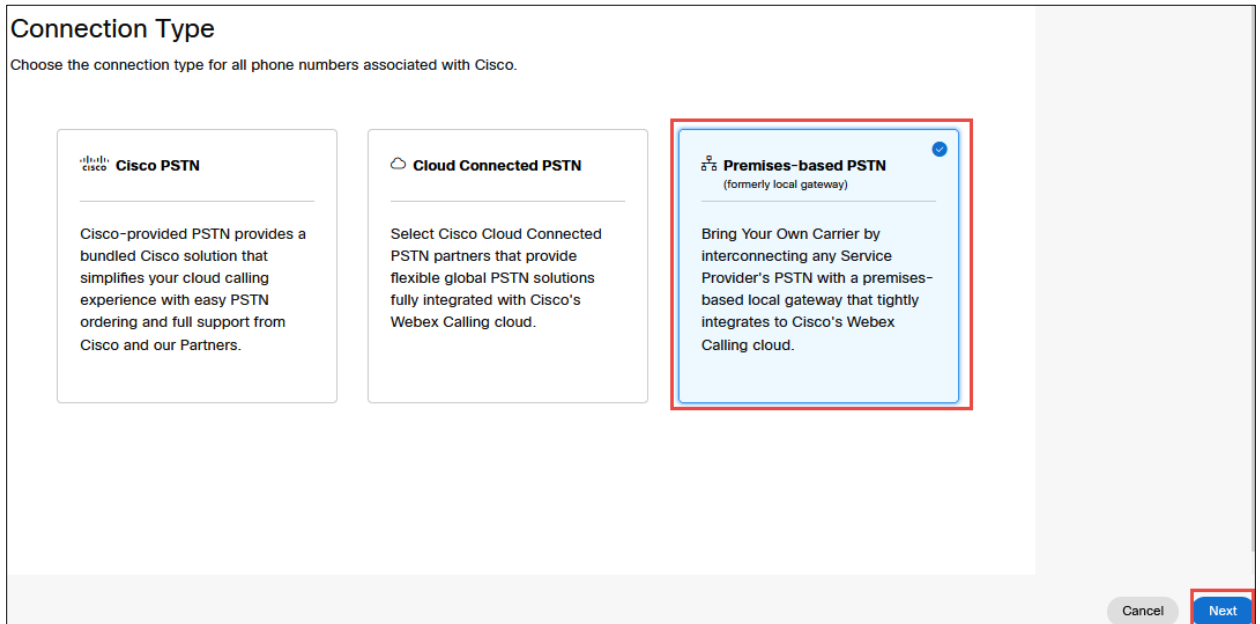


Figure 11: PSTN Connection Contd.,

Step 8:

Select the SIP trunk created earlier and click on Save.

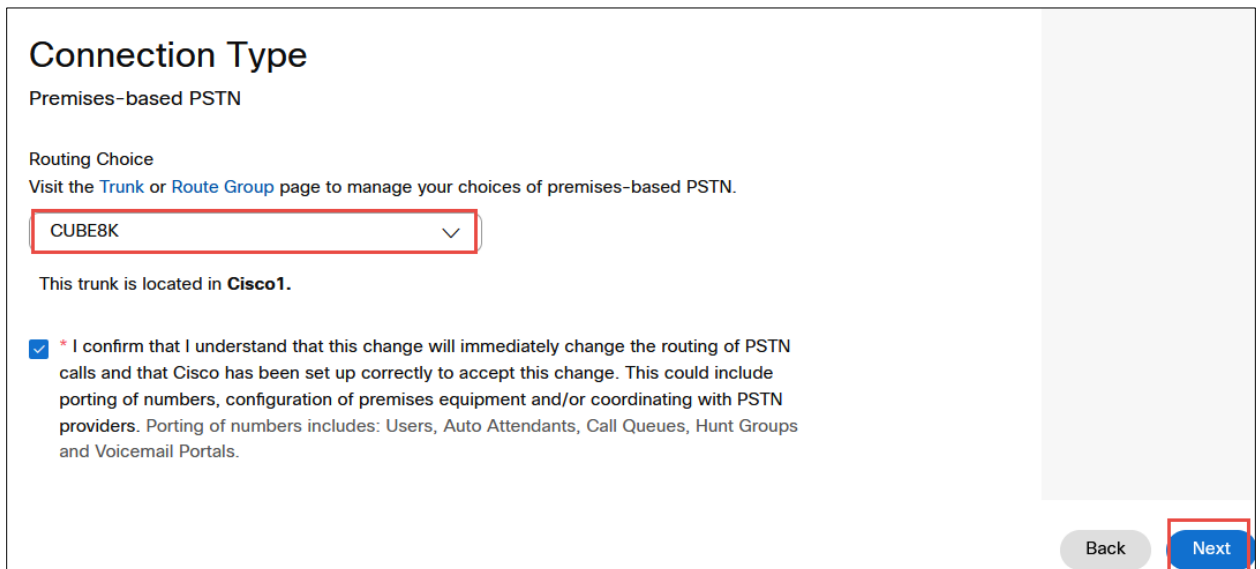


Figure 12: PSTN Connection Contd.,

Step 9:

Select the **Numbers**, Click on **Manage** and choose **Add**. Select the **Location** and **PSTN Connection**

The screenshot displays a two-part interface. The top part, titled "PSTN connection saved", shows a summary for a "Premises-based PSTN" connection. It includes a 3x3 grid of icons representing people and animals. To the right of the grid, the following details are listed: "Routing Choice: CUBE8K", "Type: Trunk", and "Location: Cisco1". At the bottom right of this section are two buttons: "Done (add numbers later)" and "Add Numbers Now" (highlighted with a red box).

The bottom part of the screenshot is a modal window titled "Add Numbers". It features a progress indicator with three steps: "Select a Location" (active), "Select Numbers", and "Done". Below the progress indicator is a section titled "Choose a Location to Add Numbers". This section contains two dropdown menus: "Location" (set to "Cisco1") and "PSTN Connection" (set to "Premises-based PSTN · CUBE8K"). A red box highlights these two dropdowns. At the bottom right of the modal are "Cancel" and "Next" (highlighted with a red box) buttons.

Figure 13: Add Numbers

Step 10:

Add the phone numbers provided by the service provider and complete the wizard.

Select a Location Select Numbers Done

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

Activate Numbers Later ⓘ

(97 17 x (97 18 x

Enter phone numbers separated by commas

2/1000 Phone numbers Clear All

Back **Save**

Figure 14: Add Numbers Contd.,

Add Numbers

Select a Location Select Numbers Done

Successfully saved numbers

Phone Numbers (1)

(97: 18

Close

Figure 15: Add Numbers Contd.,

1.2 Adding user

Step 1:

In the Cisco Webex Control Hub, select **Users** in the left pane. To add a user, click on **Manage Users** button.

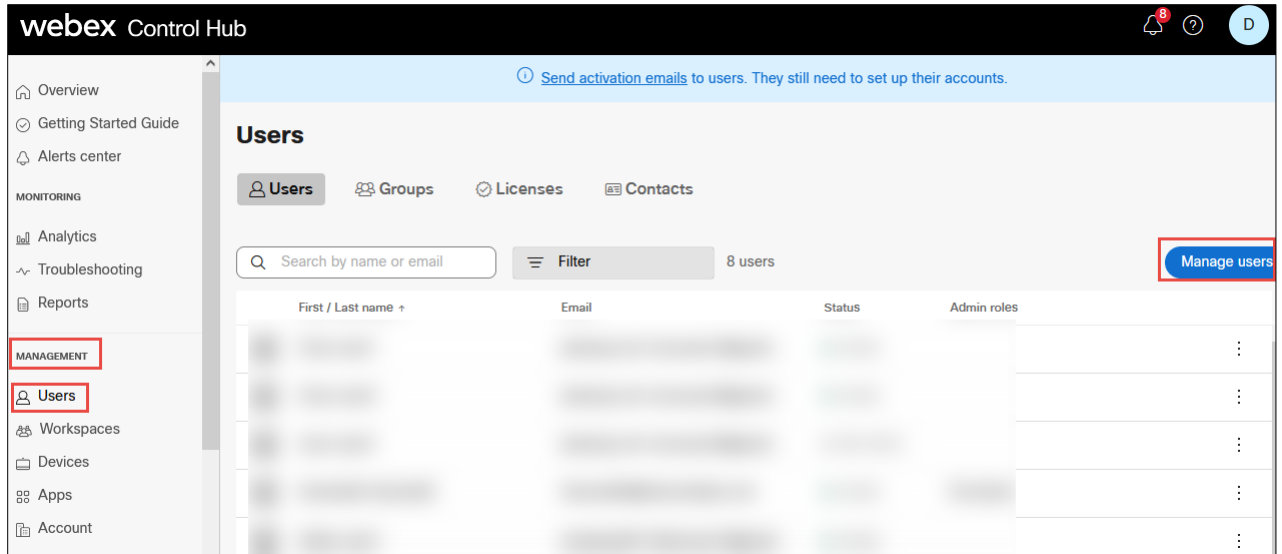


Figure 16: Adding Users

Step 2:

In the Manage Users window, click on **Manually Add or Modify Users** option.

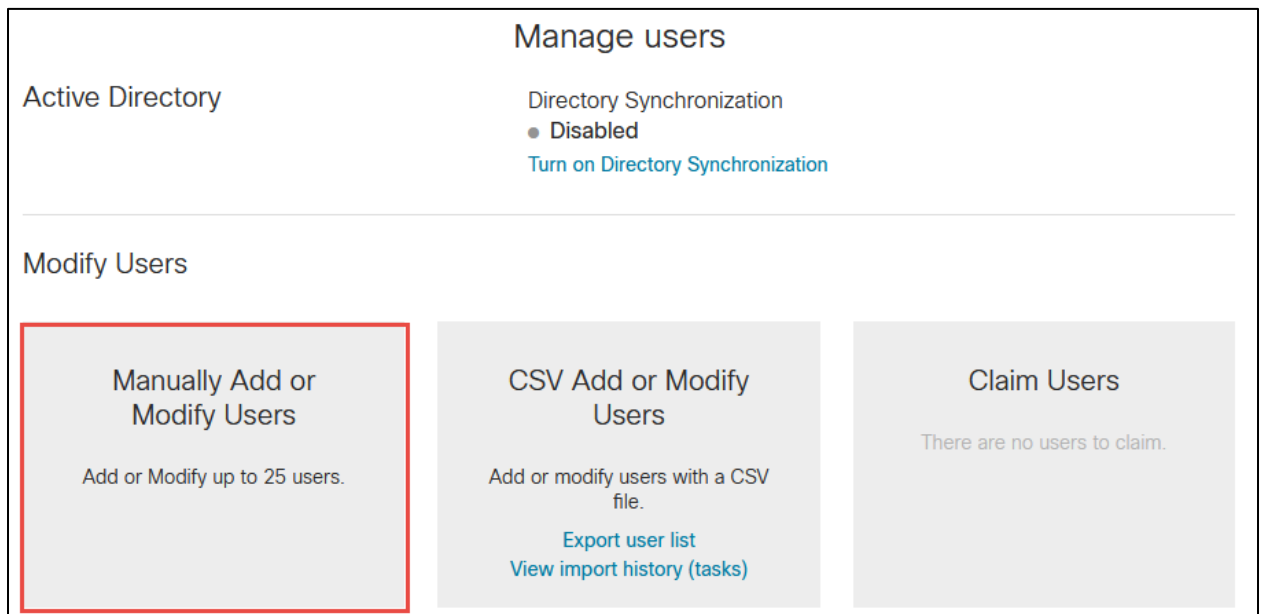


Figure 17: Manually Add or Modify Users

Step 3:

Select either **Email address** or **Names and Email address** and provide the necessary email address. Sample Name and email address provided here is below. Click on **+** symbol to add the user and click on **Next**.

Manage users

Manually Add or Modify Users
Enter up to 25 users to modify.

Email address

Names and Email address

Cisco user3 l+ciscouser3@...l.com +

Back Next

Figure 18: Adding email address and name.

Step 4:

Click on **the Confirm Adding** button to add the new user and click on **Next**.

Manage users

Users to be Added or Modified

Email Address ↑	Name	Status
l+ciscouser3@...l.com	Cisco user3	New User

Back Next

Figure 19: Confirm Adding

Step 5:

Add Services for the Users. Here select **Webex Calling** under **the Calling** section and click **Next**.

The screenshot shows the 'Manage users' interface with the following sections and options:

- Messaging:** Basic Messaging
- Meeting:** Basic Space Meetings
- Calling:** Call on Webex (1:1 call, non-PSTN)
- Non-subscription Licenses:** Register to Unified Communications Manager (UCM)
- Licensed Collaboration Services:**
 - Messaging:** Advanced Messaging
 - Meetings:** Advanced Space Meetings, Webex Assistant for Meetings, Webex Meetings Suite
 - Calling:** Webex Calling, Professional

Buttons: Back, Next

Figure 20: Add Services for Users

Step 6:

Assign the user to an appropriate location and select the phone number and extension. Click on **the Finish** button.

The screenshot shows the 'Assign Numbers' interface with the following details:

User	Location	Phone Number	Extension	Calling Plan
Cisco user3 1+ciscouser3@...l.c...	Cisco1	+197 18	18	

Buttons: Back, Finish

Figure 21: Assign Numbers

Step 7:

Successful creation of user will be displayed in the Add Users window. Click on the Finish button.

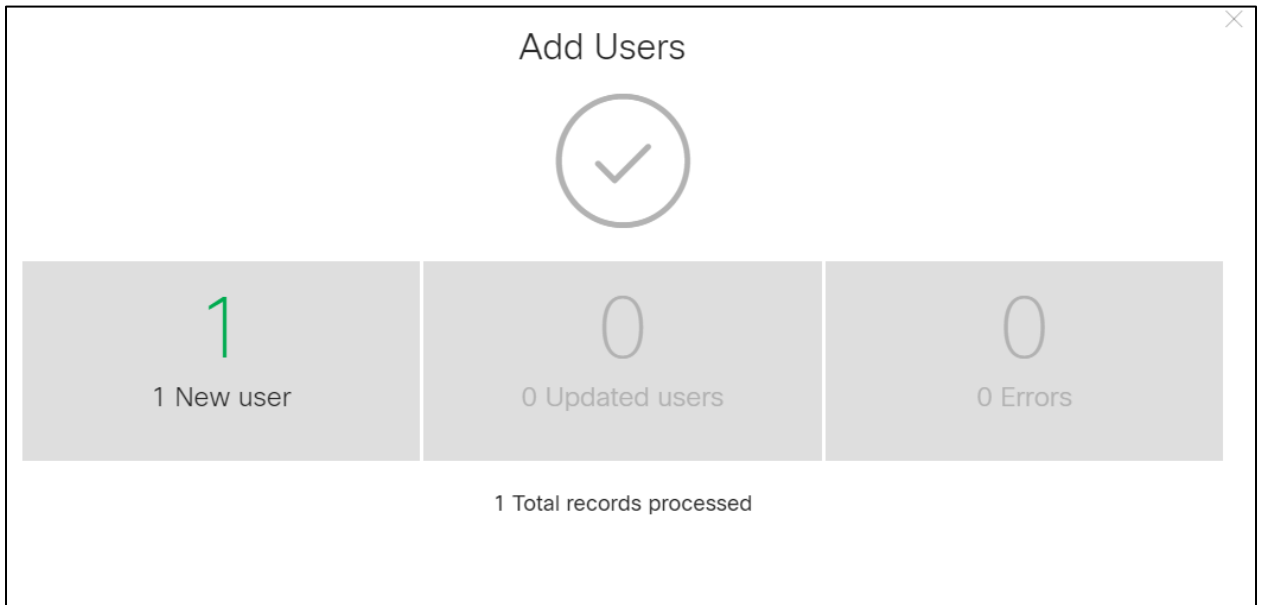


Figure 22: Add User successful.

1.3 Adding Devices

Step 1:

To add a device, navigate to **Devices** in Cisco Webex Control Hub. The existing devices will be listed out. Click the **Add Device** button.

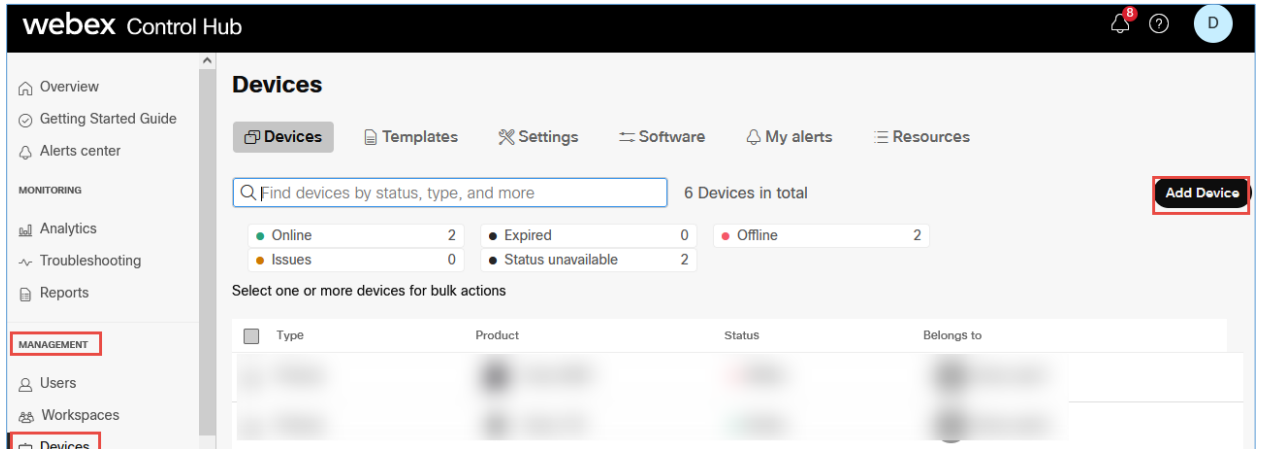
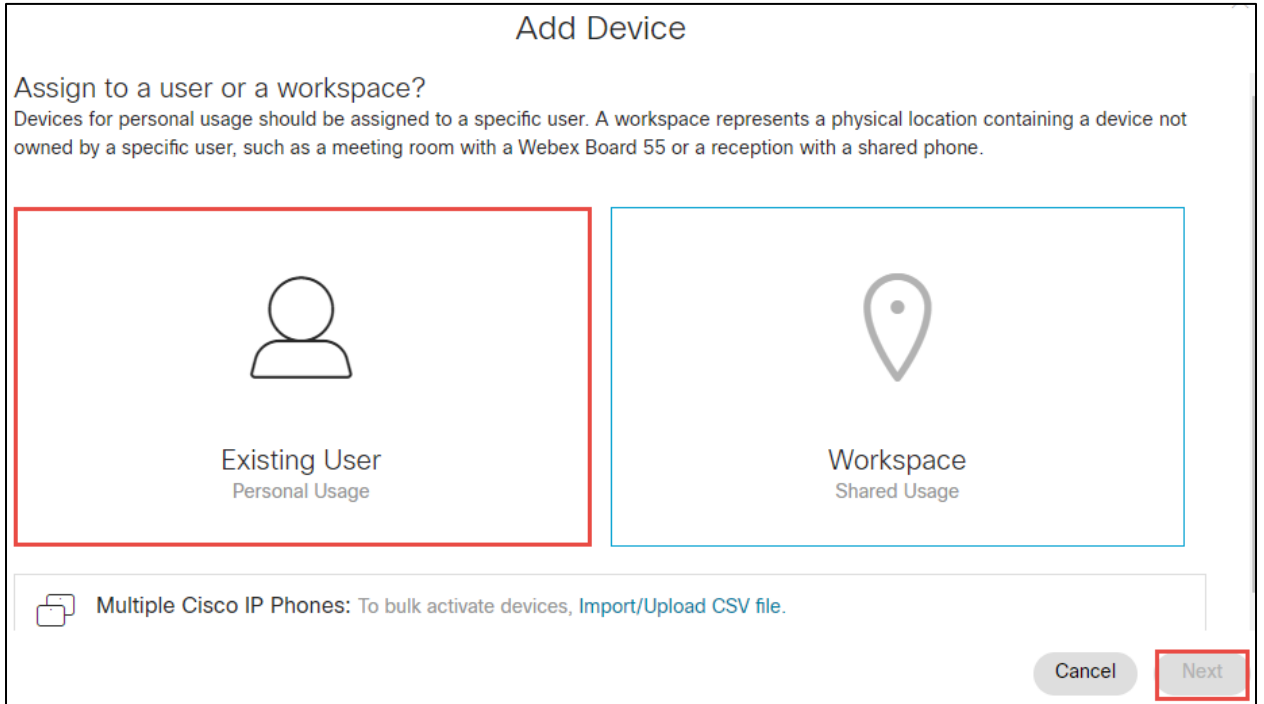


Figure 23: Add Devices Window

Step 2:

In the Add Device window, assign the device to a user or a place. Select **Existing User** and Click on Next.




The screenshot shows a window titled "Add Device". Below the title is the question "Assign to a user or a workspace?". A paragraph explains that devices for personal usage should be assigned to a specific user, while a workspace represents a physical location containing a device not owned by a specific user, such as a meeting room with a Webex Board 55 or a reception with a shared phone. There are two main options: "Existing User" (Personal Usage) and "Workspace" (Shared Usage). The "Existing User" option is highlighted with a red border. At the bottom, there is a section for "Multiple Cisco IP Phones" with a link to "Import/Upload CSV file". There are "Cancel" and "Next" buttons at the bottom right, with the "Next" button highlighted by a red border.

Add Device

Assign to a user or a workspace?
Devices for personal usage should be assigned to a specific user. A workspace represents a physical location containing a device not owned by a specific user, such as a meeting room with a Webex Board 55 or a reception with a shared phone.

Existing User
Personal Usage

Workspace
Shared Usage

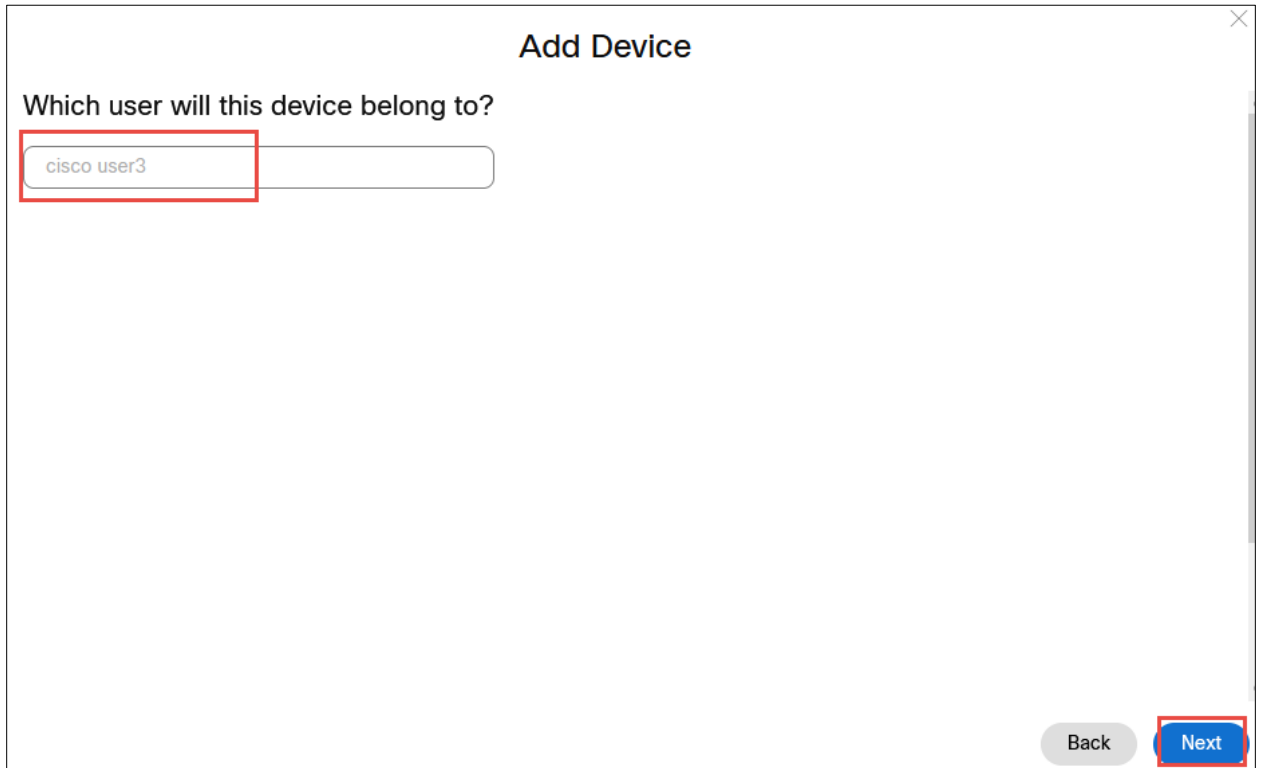
 **Multiple Cisco IP Phones:** To bulk activate devices, [Import/Upload CSV file](#).

Cancel Next

Figure 24: Assign to a user or a place

Step 3:

Select appropriate user from the **search for a user list** and click **Next**.



The screenshot shows a dialog box titled "Add Device" with a close button (X) in the top right corner. Below the title is the question "Which user will this device belong to?". A search input field contains the text "cisco user3" and is highlighted with a red border. At the bottom right of the dialog, there are two buttons: a grey "Back" button and a blue "Next" button, which is also highlighted with a red border.

Figure 25: User Association with Device

Step 4:

In the Select Device drop down box, select the appropriate **device** and enter the **MAC address**. Click on **the Save** button. The device will be added successfully.

Add Device

What kind of device do you want to set up for this user?

Room, Board or Desk series
e.g. Cisco Webex Board, Room, and Desk series, and Webex Share.

Cisco IP Phone
e.g. Cisco 8845, 8865, 8800 and Analog Telephone Adapter ports

Select Device
Cisco 6851

How would you like to setup this device?

By Activation Code

By Mac Address

Enter MAC Address
Enter the MAC address of the IP phone you want to add.

47 |

Back Save

Figure 26: Select Device and add MAC address.

1.4 Assign main number to a location

Step 1:

Assign number in location as the Main number.

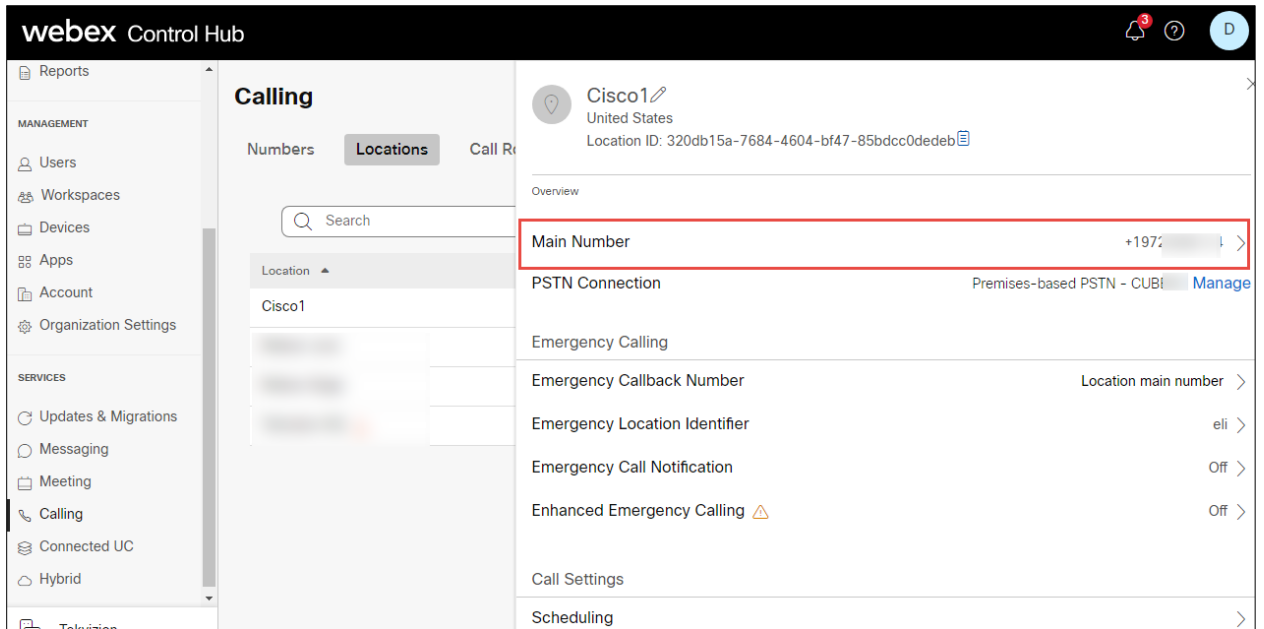


Figure 27: Assign Main number in location.

2 Configuring Cisco Webex Calling in Tenant 2

2.1 Add location-Trunk

Step1:

Login to Cisco Webex Control Hub and navigate to Services.

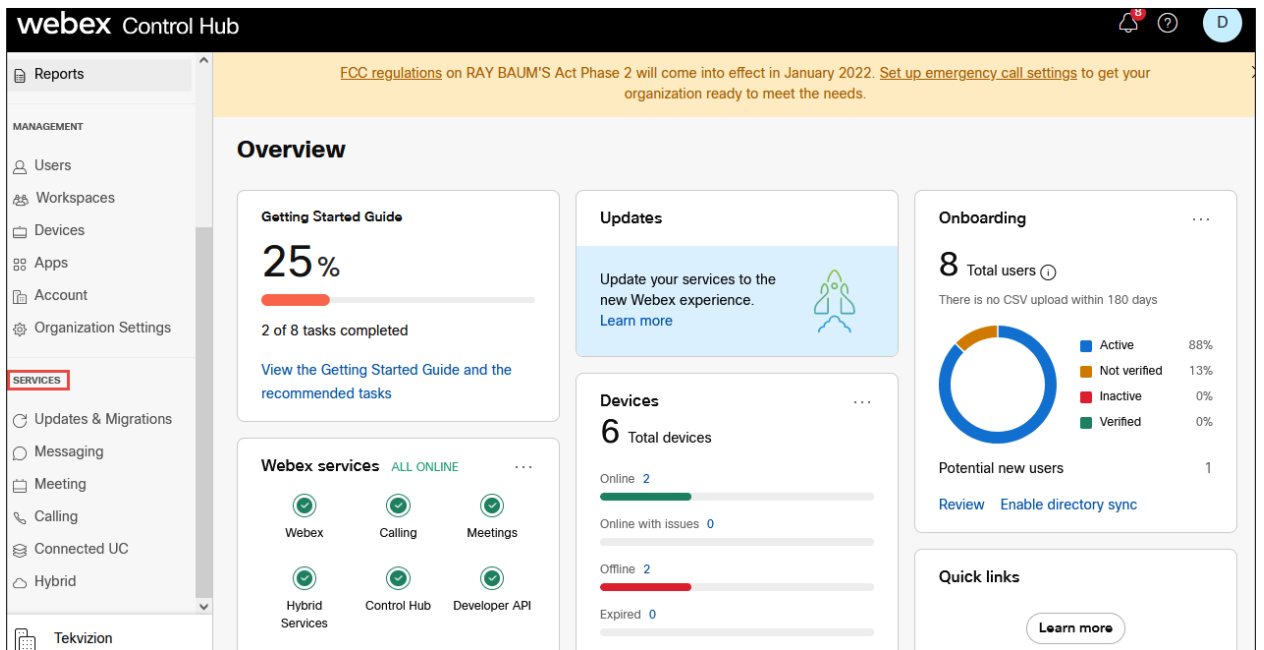


Figure 28: Control Hub Services

Step 2:

Navigate to **Calling** and click on **Locations** and Click **Add location**.

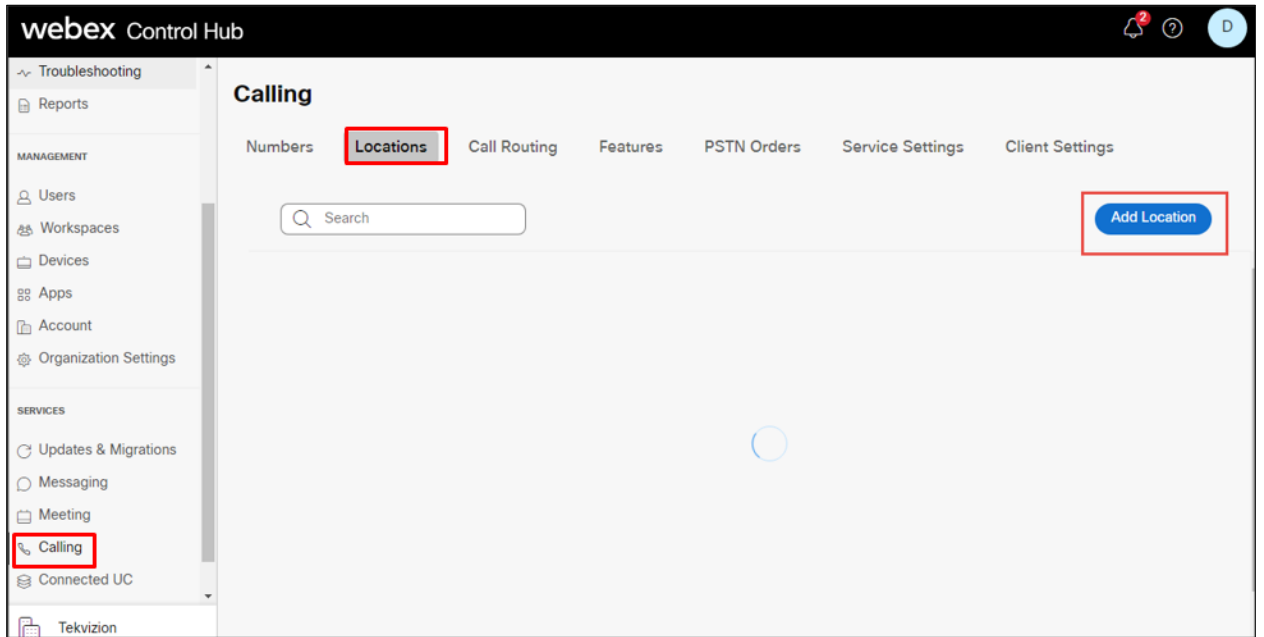


Figure 29: Add location.

Step 3:

Enter **Location** details and click **save**. After adding the location, you will be prompted to add connection type, select No for the connection type. It can be added later.

The screenshot shows a form titled "Add Location" with a red border. The form is organized into two columns. The left column contains: "Location Name" with a text input field containing "Cisco"; "Country/Region" with a dropdown menu showing "United States of America"; "Location Address" with a text input field containing "3701 W Plano Pkwy ste 300" and a secondary field for "Street address line 2 (optional)"; and "City/Town" with a text input field containing "Plano". The right column contains: "Announcement Language" with a dropdown menu showing "English"; "Email Language" with a dropdown menu showing "English - American English"; and "Time zone" with a dropdown menu showing "Select a time zone". Each input field has a small 'x' icon for clearing the text.

Figure 30: Add location details.

This screenshot shows the continuation of the "Add Location" form. The left column contains: "City/Town" with a text input field containing "Plano"; "State/Province/Region" with a dropdown menu showing "Texas"; and "Zip/Postal code" with a text input field containing "75075-7840". At the bottom right of the form, there are two buttons: "Cancel" and "Save". The "Save" button is highlighted with a red border.

Figure 31: Add location details Contd.,

Step 4:

Navigate to **Calling** → **Call Routing** → **Add Trunk** and provide the details of Location and name for the SIP Trunk

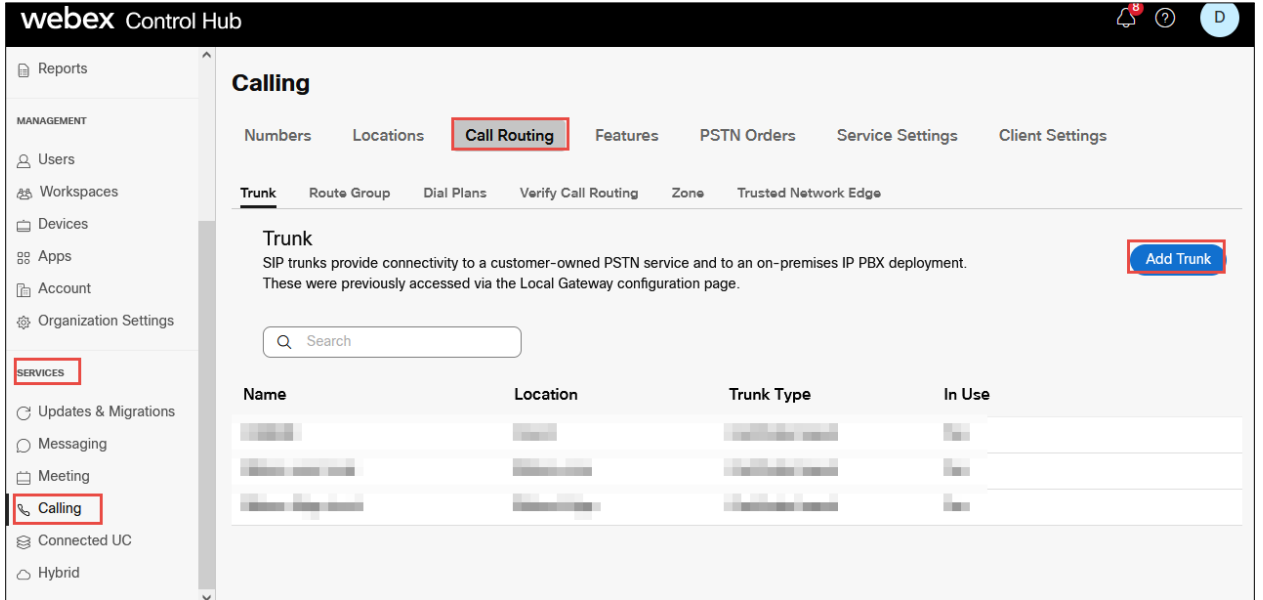


Figure 32: Add Trunk details Contd.,

Add Trunk

Location
This location is where the trunk is physically connected. To create a new location, visit the [Locations](#) page.

Cisco1

Name

CUBE8K|

Trunk Type
Choose the right trunk type for this local gateway. [Learn more](#) on trunk type

Certificate based

Device Type

Cisco Unified Border Element

Enterprise Session Border Controller (SBC) Address

Select the type and enter an FQDN or SRV address for Webex Calling to reach out to your Enterprise SBC.
You must have the domain for your SBC's FQDN/SRV claimed or verified [before you can use this address. Manage your domains](#)

FQDN
 SRV

Hostname * Domain * Port *

sbc5 tekvlabs.com 5062

Valid address

FQDN

sbc5.tekvlabs.com:5062

Maximum number of concurrent calls *

400

Cancel Save

Dual Identity Support

The Dual Identity Support setting impacts the handling of the From header and P-Asserted-Identity (PAI) header when sending an initial SIP INVITE to the trunk for an outbound call. When enabled, the From and PAI headers are treated independently and may differ. When disabled, the PAI header is set to the same value as the From header. Please refer to the documentation for more details.

Cancel Save

Figure 33: Add Trunk details Contd.

Add Trunk



CUBE8K 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 ⓘ

● Unknown

Webex Calling edge proxy address (FQDN)

peering1.us.sipconnect.bclid.webex.com:5062
peering2.us.sipconnect.bclid.webex.com:5062
peering3.us.sipconnect.bclid.webex.com:5062
peering4.us.sipconnect.bclid.webex.com:5062

Webex Calling edge proxy address (SRV)

us01.sipconnect.bclid.webex.com

Figure 34: Add Trunk details Contd.,

Step 5:

Choose the location and select Manage in PSTN Connection to add Connection type.

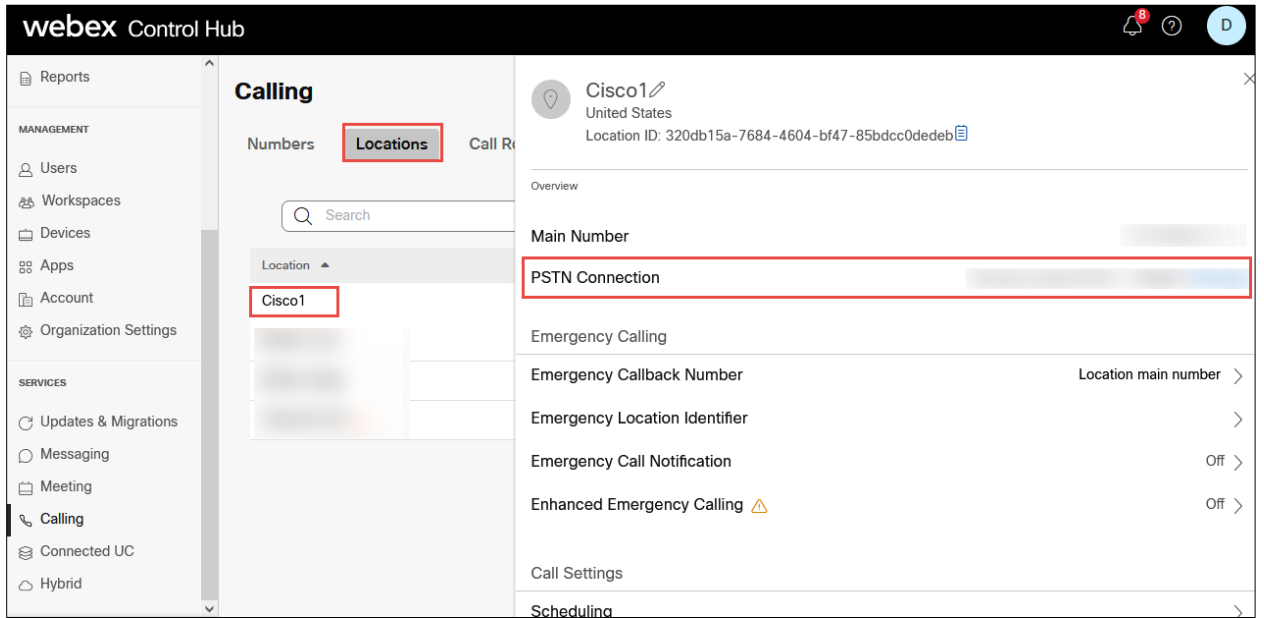


Figure 35: PSTN Connection

Step 6:

Select the **Connection Type** as **Premises-based PSTN** and click on Next.

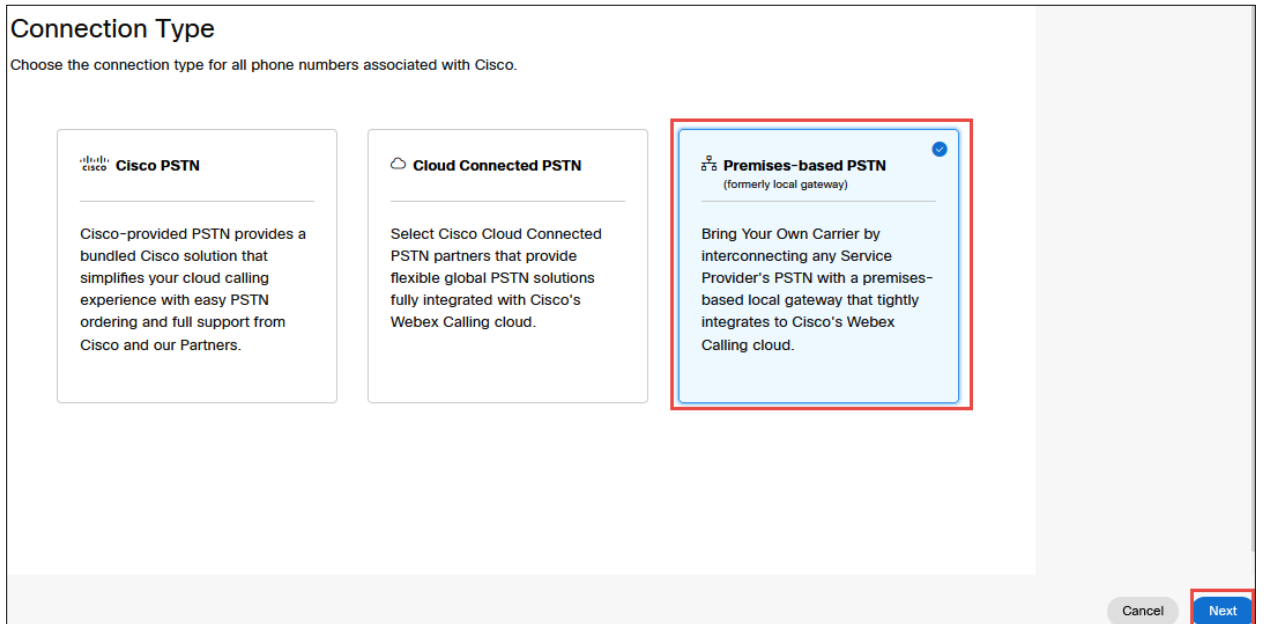


Figure 36: PSTN Connection Contd.,

Step 7:

Select the SIP trunk created earlier and click on Save.

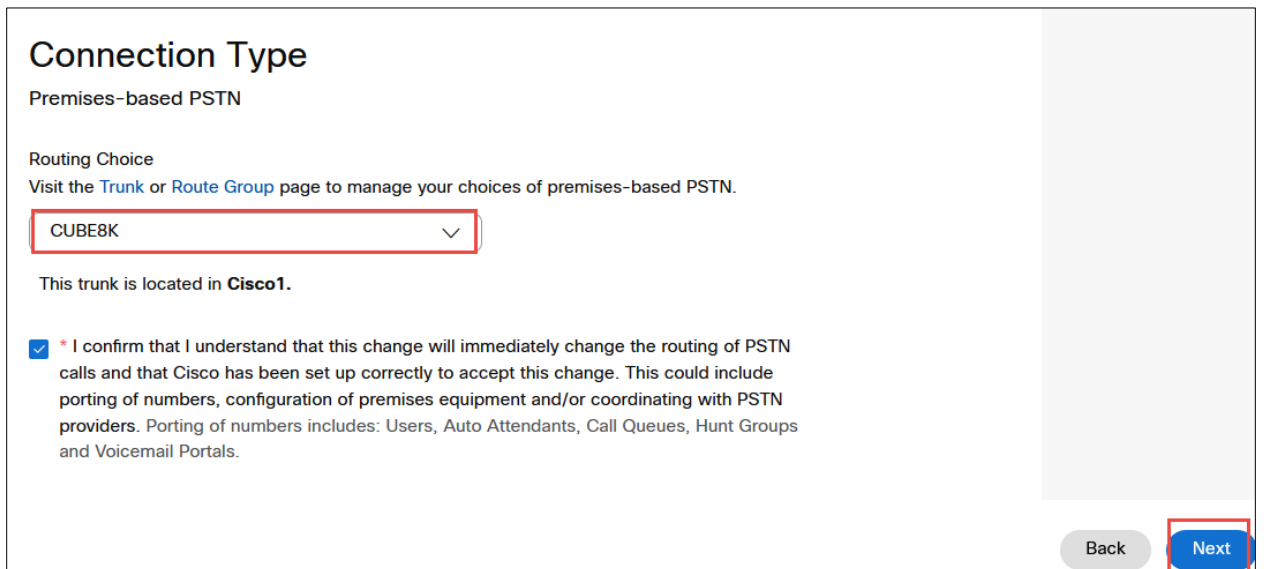


Figure 37: PSTN Connection Contd.,

Step 8:

Select the **Numbers**, Click on **Manage** and choose **Add**. Select the **Location** and **PSTN Connection**

The screenshot displays the 'Add Numbers' configuration interface. At the top, a confirmation message states 'PSTN connection saved'. Below this, a summary card for a 'Premises-based PSTN' connection is shown, including a grid of icons representing people and animals, and the following details:

- Routing Choice:** CUBE8K
- Type:** Trunk
- Location:** Cisco1

At the bottom right of this card are two buttons: 'Done (add numbers later)' and 'Add Numbers Now' (highlighted with a red box).

The main 'Add Numbers' window features a progress bar with three steps: 'Select a Location' (active), 'Select Numbers', and 'Done'. Below the progress bar, the title 'Choose a Location to Add Numbers' is displayed. A form contains two fields:

- Location:** A dropdown menu with 'Cisco1' selected.
- PSTN Connection:** A dropdown menu with 'Premises-based PSTN · CUBE8K' selected.

At the bottom right of the window are 'Cancel' and 'Next' buttons (the 'Next' button is highlighted with a red box).

Figure 38: Add Numbers

Step 9:

Add the phone numbers provided by the service provider and complete the wizard.

Select a Location Select Numbers Done

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

Activate Numbers Later ⓘ

(97 17 x (97 18 x

Enter phone numbers separated by commas

2/1000 Phone numbers Clear All

Back Save

Figure 39: Add Numbers Contd.,

Add Numbers

Select a Location Select Numbers Done

Successfully saved numbers

Phone Numbers (1)

(97: 18

Close

Figure 40: Add Numbers Contd.,

Repeat step 1.2 to 1.4 (Adding user, adding devices, Assign main number to a location) in this Webex tenant.

3 Cisco CUBE Configuration

The following configuration is for CUBE HA (active/standby for stateful failover of active calls).

In a multi-tenancy setup on this CUBE, two customers with FQDN “sbc6.tekvizionlabs.com” (tenant 1) and sbc5.tekvlabs.com (tenant 2) are being pointed to same interface IP address but each has its own unique SIP listening port on the Cisco CUBE.

For example, sbc6.tekvizionlabs.com will listen on port 5061 and sbc5.tekvlabs.com on port 5062.

3.1 IP Networking

```
interface GigabitEthernet0/0/0
  description To HA interface
  ip address 10.64.5.234 255.255.0.0
  negotiation auto
!
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/1.1
  description To PSTN Lumen
  encapsulation dot1Q 3811
  ip address 10.80.11.138 255.255.255.0
  redundancy rii 16
  redundancy group 1 ip 10.80.11.136 exclusive
!
interface GigabitEthernet0/0/1.2
  description To PSTN Verizon
  encapsulation dot1Q 1506
  ip address 199.182.124.25x 255.255.255.192
  redundancy rii 18
  redundancy group 1 ip 199.182.124.2xx exclusive
!
interface GigabitEthernet0/0/2
  description To Webex tenant
  ip address 192.65.79.11x 255.255.255.224
  negotiation auto
  redundancy rii 17
  redundancy group 1 ip 192.65.79.1xx exclusive
```

Explanation

Command	Description
redundancy rii id	Redundant interface identifier to generate virtual MAC. Same rii id must be used on CUBEs that have the same virtual IP on their respective interfaces
redundancy group 1 ip x.x.x.x exclusive	Enable Redundancy group on physical interface with virtual IP towards PSTN and Webex calling
Interface GigabitEthernet0/0/1.x	Physical interface divided into multiple sub-interfaces, each for a different PSTN provider
encapsulation dot1Q xxxx	to configure VLAN tagging on each sub-interface to forward traffic.

3.2 IP Routing

3.2.1 To Webex Calling Tenants

```
ip route 0.0.0.0 0.0.0.0 192.65.79.x
```

3.2.2 To PSTN Lumen

```
ip route 10.64.0.0 255.255.0.0 10.80.11.1
```

3.2.3 To PSTN Verizon

```
ip route 152.188.28.0 255.255.255.0 199.182.124.x
```

3.3 DNS Servers

DNS must be configured to resolve addresses for Webex Calling

```
ip name-server 8.8.8.8
```

3.4 Certificates

The following steps describe how to create and install a certificate.

3.4.1 For Webex Tenant 1

3.4.1.1 Generate RSA key

```
crypto key generate rsa general-keys label sbc6 exportable redundancy modulus 4096
The name for the keys will be: sbc6

% The key modulus size is 4096 bits
% Generating 4096 bit RSA keys, keys will be exportable with redundancy...
[OK] (elapsed time was 1 seconds)
```

3.4.1.2 Create SBC Trustpoint

Hostname based certificate is used in Cisco CUBE for Multi-tenant.

```
crypto pki trustpoint sbc6
  enrollment terminal
  subject-name cn=sbc6.tekvizionlabs.com
  revocation-check crl
  rsakeypair sbc6
```

3.4.1.3 Generate Certificate Signing Request (CSR)

Use this CSR to request a certificate from one of the supported Certificate authorities.

```
crypto pki enroll sbc6
% Start certificate enrollment ..

% The subject name in the certificate will include: cn=sbc6.tekvizionlabs.com
% The subject name in the certificate will include: sbc6.tekvizionlabs.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
```

3.4.1.4 Authenticate CA Certificate

Enter the following command, then paste the CA certificate that verifies the host certificate into the trust point (usually the intermediate certificate). Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted.

```
crypto pki authenticate sbc6

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

3.4.1.5 Import signed host certificate

Enter the following command then paste the host certificate into the trust point. Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted.

```
crypto pki import sbc6 certificate
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

3.4.1.6 Specify the TLS version to use

```
sip-ua
```

```
transport tcp tls v1.2
```

3.4.1.7 Import Cisco CA bundle for Webex calling certificate authentication

Create the CA certificate trust point used to validate Webex Calling SIP Link TLS messages:

```
crypto pki trustpool import clean url
```

```
http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
Reading file from http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
Loading http://www.cisco.com/security/pki/trs/ios_core.p7b
```

```
% PEM files import succeeded.
```

3.4.1.8 Exporting RSA key and certificate from Cisco CUBE 1 for High Availability

```
crypto pki export sbc6 pkcs12 ftp://<username>:<password>@x.x.x.x/ password xxxxx
```

```
Address or name of remote host [x.x.x.x]?
```

```
Destination filename [sbc6]?
```

```
Writing sbc6 Writing pkcs12 file to ftp://<username>@x.x.x.x/sbc6
```

```
!
```

```
CRYPTO_PKI: Exported PKCS12 file successfully.
```

3.4.1.9 Import RSA key and certificate in Cisco CUBE 2 for High Availability

Using the below command, import the certificate to Cisco CUBE 2. This will automatically create the trustpoint "sbc6"

```
crypto pki import sbc6 pkcs12 ftp://<username>:<password>@x.x.x.x/sbc6 password xxxx
% Importing pkcs12...
Address or name of remote host [x.x.x.x]?
Source filename [sbc6]?
Reading file from ftp://<username>@x.x.x.x/sbc6!
[OK - 4931/4096 bytes]

CRYPTO_PKI: Imported PKCS12 file successfully.
```

3.4.2 Webex Tenant 2

The following steps describe how to create and install a certificate for Webex Tenant 2

3.4.2.1 Generate RSA key

```
crypto key generate rsa general-keys label sbc5 exportable redundancy modulus 4096
The name for the keys will be: sbc5

% The key modulus size is 4096 bits
% Generating 4096 bit RSA keys, keys will be exportable with redundancy...
[OK] (elapsed time was 1 seconds)
```

3.4.2.2 Create SBC Trustpoint

Hostname based certificate is used in Cisco CUBE for Multi-tenant.

```
crypto pki trustpoint sbc5
  enrollment terminal
  subject-name cn=sbc5.tekvlabs.com
  revocation-check crl
  rsakeypair sbc5
```

3.4.2.3 Generate Certificate Signing Request (CSR)

Use this CSR to request a certificate from one of the supported Certificate authorities.

```
crypto pki enroll sbc5
% Start certificate enrollment ..

% The subject name in the certificate will include: cn=sbc5.tekvlabs.com
% The subject name in the certificate will include: sbc5.tekvlabs.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
```

3.4.2.4 Authenticate CA Certificate

Enter the following command, then paste the CA certificate that verifies the host certificate into the trust point (usually the intermediate certificate). Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted.

```
crypto pki authenticate sbc5

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

3.4.2.5 Import signed host certificate

Enter the following command then paste the host certificate into the trust point. Open the base 64 CER/PEM file with notepad, copy the text, and paste it into the terminal when prompted.

```
crypto pki import sbc5 certificate

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

3.4.2.6 Import Cisco CA bundle for Webex calling certificate authentication

Create the CA certificate trust point used to validate Webex Calling SIP Link TLS messages:

```
crypto pki trustpool import clean url
http://www.cisco.com/security/pki/trs/ios_core.p7b
Reading file from http://www.cisco.com/security/pki/trs/ios_core.p7b
Loading http://www.cisco.com/security/pki/trs/ios_core.p7b
% PEM files import succeeded.
```

3.4.2.7 Exporting RSA key and certificate from Cisco CUBE 1 for High Availability

```
crypto pki export sbc5 pkcs12 ftp://<username>:<password>@x.x.x.x/ password xxxxx
Address or name of remote host [x.x.x.x]?
Destination filename [sbc5]?
Writing SAN Writing pkcs12 file to ftp://<username>@x.x.x.x/sbc5
!
CRYPTO_PKI: Exported PKCS12 file successfully.
```

3.4.2.8 Import RSA key and certificate in Cisco CUBE 2 for High Availability

Using the below command, import the certificate to Cisco CUBE 2. This will automatically create the trustpoint "sbc5".

```
crypto pki import sbc5 pkcs12 ftp://<username>:<password>@x.x.x.x/sbc5 password xxxxx
% Importing pkcs12...
Address or name of remote host [x.x.x.x]?
Source filename [sbc5]?
Reading file from ftp://<username>@x.x.x.x/sbc5
[OK - 4931/4096 bytes]

CRYPTO_PKI: Imported PKCS12 file successfully.
```

3.5 Global Cisco CUBE settings

In order to enable Cisco CUBE with settings required to interwork with Webex calling Voice, the following commands must be entered:

```
voice service voip
ip address trusted list
  ipv4 139.177.65.53 255.255.255.255
  ipv4 85.119.56.128 255.255.255.192
  ipv4 85.119.57.128 255.255.255.192
  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 135.84.172.0 255.255.255.128
  ipv4 135.84.173.0 255.255.255.128
  ipv4 135.84.174.0 255.255.255.128
  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
  ipv4 185.115.196.0 255.255.255.128
  ipv4 185.115.197.0 255.255.255.128
  ipv4 199.19.197.0 255.255.255.0
  ipv4 199.19.199.0 255.255.255.0
  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 128.177.14.0 255.255.255.128
  ipv4 128.177.36.0 255.255.255.192
  ipv4 10.64.1.0
  ipv4 152.188.28.0
```

```

address-hiding
mode border-element
allow-connections sip to sip
redundancy-group 1
no supplementary-service sip refer
no supplementary-service sip handle-replaces
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
trace
sip
  listen-port secure 5067
  early-offer forced
  g729 annexb-all
  no call service stop

```

Explanation

Command	Description
allow-connections sip to sip	Allow IP2IP connections between two SIP call legs
fax protocol	Specifies the fax protocol
no supplementary-service sip refer no supplementary-service sip handle-replaces	Disable forwarding SIP REFER message for call transfers and replace the Dialog-ID in the Replaces header with the peer Dialog-ID
Redundancy group 1	Enable redundancy group
listen-port secure 5067	To set 5061 as a secure listening port in Cisco CUBE tenant configuration, the global secure listen port needs to be changed other than the ports mentioned in tenants. Example: In a multi-tenant setup, sbc6.tekvizionlabs.com is listening on 5061 and sbc5.tekvlabs.com is listening on port 5062, hence, the global listen port is set to 5067.

3.6 Configure Redundancy group

```

redundancy
mode none
application redundancy
group 1
  priority 150 failover threshold 75
  timers delay 30 reload 60
  control GigabitEthernet0/0/0 protocol 1
  data GigabitEthernet0/0/0
  track 1 shutdown
  track 2 shutdown
  track 3 shutdown
!
track 1 interface GigabitEthernet0/0/1.1 line-protocol
!
track 2 interface GigabitEthernet0/0/1.2 line-protocol
!
track 3 interface GigabitEthernet0/0/2 line-protocol

```

Explanation

Command	Description
priority 150 failover threshold 75	Set priority weightage for Cisco CUBE 1 and Cisco CUBE 2. High priority Cisco CUBE turns Active and other StandBy
timers delay 30 reload 60	the amount of time to delay RG group's initialization and role negotiation after the interface comes up and reload
control GigabitEthernet0/0/0 protocol 1	interface used to exchange keepalive
data GigabitEthernet0/0/0	interface used for checkpointing of data traffic
Track x interface GigabitEthernet x/x/x line-protocol	The track command is used in RG to track the voice traffic interface state so that the active router initiates switchover after the traffic interface is down.
Track x shutdown	Enable RG group tracking

3.7 SRTP crypto

Used to set the crypto cipher for the Webex Calling

```
voice class srtp-crypto 1
crypto 1 AES_CM_128_HMAC_SHA1_80
```

3.8 STUN ICE-lite

```
voice class stun-usage 100
stun usage ice lite
```

3.9 Codecs

3.9.1.1 To Webex calling/PSTN

```
voice class codec 100
codec preference 2 g711ulaw
codec preference 3 g711alaw
codec preference 4 opus
```

3.10 Options keepalive to Webex Calling

Enable SIP Options towards Webex certificate-based trunk configured and to track the trunk status frequently set the interval and transport protocol. This keepalive profile is triggered from dial-peer configured towards Webex.

3.10.1.1 To Webex calling Tenant 1

The following sip profile is required to:

1. [Rule 10] - To ensure that the Contact header includes the SBC's fully qualified domain name.
2. [Rule 30] – Replace embedded private IP address in the VIA with the external NAT address.
3. [Rules 40 and 50] – Replace embedded private IP addresses in SDP with the external NAT address.

CUBE configured with a public IP address

```
voice class sip-profiles 100
  rule 10 request OPTIONS sip-header Contact modify "<sip.*:"
"<sip:sb66.tekvizionlabs.com:"
!
voice class sip-options-keepalive 100
  description Keepalive Webex calling
  up-interval 5
  transport tcp tls
  sip-profiles 100
```

CUBE behind NAT

```
voice class sip-profiles 100
  rule 10 request OPTIONS sip-header Contact modify "<sip.*:"
"<sip:sb66.tekvizionlabs.com:"
  rule 30 request ANY sip-header Via modify "SIP(.*) 10.80.13.12(.*)" "SIP\1
192.65.79.x\2"
  rule 40 response ANY sdp-header Connection-Info modify "IN IP4 10.80.13.12" "IN IP4
192.65.79.x"
  rule 50 response ANY sdp-header Audio-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
!
voice class sip-options-keepalive 100
  description Keepalive Webex calling
  up-interval 5
  transport tcp tls
  sip-profiles 100
```

3.10.1.2 To Webex calling Tenant 2

The following sip profile is required to:

1. [Rule 10] - To ensure that the Contact header includes the SBC's fully qualified domain name.
2. [Rule 30] – Replace embedded private IP address in the VIA with the external NAT address.
3. [Rules 40 and 50] – Replace embedded private IP addresses in SDP with the external NAT address.

CUBE configured with a Public IP address

```
voice class sip-profiles 601
  rule 10 request OPTIONS sip-header Contact modify "<sip.*:"
"<sip:svc5.tekvlabs.com:"
!
voice class sip-options-keepalive 600
  description Keepalive Webex calling
  up-interval 5
  transport tcp tls
  sip-profiles 601
```

CUBE behind NAT

```
voice class sip-profiles 601
  rule 10 request OPTIONS sip-header Contact modify "<sip.*:"
"<sip:svc5.tekvlabs.com:"
  rule 30 request ANY sip-header Via modify "SIP(.*) 10.80.13.12(.*)" "SIP\1
192.65.79.x\2"
  rule 40 response ANY sdp-header Connection-Info modify "IN IP4 10.80.13.12" "IN IP4
192.65.79.x"
  rule 50 response ANY sdp-header Audio-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
!
voice class sip-options-keepalive 600
  description Keepalive Webex calling
  up-interval 5
  transport tcp tls
  sip-profiles 601
```

3.11 Message Handling Rules

3.11.1.1 SIP Profiles: Manipulations for outbound messages to Webex Calling

The following sip profile is required to:

1. [Rules 10 and 20] – Replace CUBE IP address with Fully qualified domain names (FQDN) in the 'Contact' header of INVITE messages.
2. [Rules 21 – 96] – Replace embedded private IP addresses in SDP with the external NAT address.

3.11.1.2 To Tenant 1

CUBE configured with a Public IP address

```
voice class sip-profiles 200
rule 10 request ANY sip-header Contact modify "@.*:" "@sbc6.tekvizionlabs.com:"
rule 20 response ANY sip-header Contact modify "@.*:" "@sbc6.tekvizionlabs.com:"
```

CUBE behind NAT

```
voice class sip-profiles 200
rule 10 request ANY sip-header Contact modify "@.*:" "@sbc6.tekvizionlabs.com:"
rule 20 response ANY sip-header Contact modify "@.*:" "@sbc6.tekvizionlabs.com:"
rule 21 response ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
10.80.13.12 (.*)" "a=candidate:1 1\1 192.65.79.x \2"
rule 22 response ANY sdp-header Video-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
rule 30 response ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
10.80.13.12 (.*)" "a=candidate:1 2\1 192.65.79.x \2"
rule 40 response ANY sdp-header Audio-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
rule 41 request ANY sdp-header Audio-Connection-Info modify "IN IP4 10.80.13.12" "IN
IP4 192.65.79.x"
rule 50 request ANY sdp-header Connection-Info modify "IN IP4 10.80.13.12" "IN IP4
192.65.79.x"
rule 51 response ANY sdp-header Connection-Info modify "IN IP4 10.80.13.12" "IN IP4
192.65.79.x"
rule 60 response ANY sdp-header Session-Owner modify "(.*) IN IP4 10.80.13.12" "\1
IN IP4 192.65.79.x"
rule 61 request ANY sdp-header Session-Owner modify "(.*) IN IP4 10.80.13.12" "\1 IN
IP4 192.65.79.x"
rule 80 request ANY sdp-header Audio-Attribute modify "a=rtcp:(.*) IN IP4
10.80.13.12" "a=rtcp:\1 IN IP4 192.65.79.x"
```

```

rule 81 response ANY sdp-header Audio-Attribute modify "a=rtcp:(.*) IN IP4
10.80.13.12" "a=rtcp:\1 IN IP4 192.65.79.x"

rule 91 request ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
10.80.13.12 (.*)" "a=candidate:1 1\1 192.65.79.x \2"

rule 93 request ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
10.80.13.12 (.*)" "a=candidate:1 2\1 192.65.79.x \2"

```

3.11.1.3 To Tenant 2

CUBE configured with a Public IP address

```

voice class sip-profiles 600
rule 10 request ANY sip-header Contact modify "@.*:" "@sbc5.tekvlabs.com:"
rule 20 response ANY sip-header Contact modify "@.*:" "@sbc5.tekvlabs.com:"

```

CUBE behind NAT

```

voice class sip-profiles 600
rule 10 request ANY sip-header Contact modify "@.*:" "@sbc5.tekvlabs.com:"
rule 20 response ANY sip-header Contact modify "@.*:" "@sbc5.tekvlabs.com:"
rule 22 response ANY sdp-header Video-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
rule 41 request ANY sdp-header Audio-Connection-Info modify "IN IP4 10.80.13.12" "IN
IP4 192.65.79.x"
rule 42 response ANY sdp-header Audio-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
rule 50 request ANY sdp-header Connection-Info modify "IN IP4 10.80.13.12" "IN IP4
192.65.79.x"
rule 51 response ANY sdp-header Connection-Info modify "IN IP4 10.80.13.12." "IN IP4
192.65.79.x"
rule 61 request ANY sdp-header Session-Owner modify "(.*) IN IP4 10.80.13.12" "\1 IN
IP4 192.65.79.x"
rule 62 response ANY sdp-header Session-Owner modify "(.*) IN IP4 10.80.13.12" "\1
IN IP4 192.65.79.x"
rule 80 request ANY sdp-header Audio-Attribute modify "a=rtcp:(.*) IN IP4
10.80.13.12" "a=rtcp:\1 IN IP4 192.65.79.x"
rule 91 request ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
10.80.13.12 (.*)" "a=candidate:1 1\1 192.65.79.x \2"
rule 92 response ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
10.80.13.12 (.*)" "a=candidate:1 1\1 192.65.79.x \2"
rule 93 request ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
10.80.13.12 (.*)" "a=candidate:1 2\1 192.65.79.x \2"
rule 94 request ANY sip-header Via modify "10.80.13.12:5062;" "192.65.79.x:5062;"

```

```
rule 95 response ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
10.80.13.12 (.*)" "a=candidate:1 2\1 192.65.79.x \2"
rule 96 response ANY sdp-header Audio-Attribute modify "a=rtcp:(.*) IN IP4
10.80.13.12" "a=rtcp:\1 IN IP4 192.65.79.x"
```

3.11.1.4 SIP Profiles: Manipulations for inbound messages from Webex Calling

The following sip profile is required to:

1. [Rule 20] - Modify the Contact header to replace the CUBE IP with the FQDN in SIP requests and responses.
2. Rule [30 – 90] – Replace embedded private IP addresses in SDP with the external NAT address.

3.11.1.5 To Tenant 1

CUBE configured with a Public IP address

```
voice class sip-profiles 201
rule 20 response ANY sip-header Contact modify "@.*:" "@sbc6.tekvizionlabs.com:"
```

CUBE behind NAT

```
voice class sip-profiles 201
rule 20 response ANY sip-header Contact modify "@.*:" "@sbc6.tekvizionlabs.com:"
rule 30 response ANY sdp-header Connection-Info modify "IN IP4 10.80.13.12." "IN IP4
192.65.79.x"
rule 31 response ANY sdp-header Video-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
rule 40 response ANY sdp-header Audio-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
rule 60 response ANY sdp-header Session-Owner modify "(.*) IN IP4 10.80.13.12" "\1
IN IP4 192.65.79.x"
rule 70 response ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
10.80.13.12 (.*)" "a=candidate:1 1\1 192.65.79.x \2"
rule 80 response ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
10.80.13.12 (.*)" "a=candidate:1 2\1 192.65.79.x \2"
rule 90 response ANY sdp-header Audio-Attribute modify "a=rtcp:(.*) IN IP4
10.80.13.12" "a=rtcp:\1 IN IP4 192.65.79.x"
```

3.11.1.6 To Tenant 2

1. [Rule 20] - Modify the Contact header to replace the CUBE IP with the FQDN in SIP requests and responses.
2. Rule [30 – 90] – Replace embedded private IP addresses in SDP with the external NAT address.

CUBE configured with a Public IP address

```
voice class sip-profiles 602
rule 20 response ANY sip-header Contact modify "@.*:" "@sbc5.tekvlabs.com:"
```

CUBE behind NAT

```
voice class sip-profiles 602
rule 20 response ANY sip-header Contact modify "@.*:" "@sbc5.tekvlabs.com:"
rule 30 response ANY sdp-header Video-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
rule 31 response ANY sdp-header Connection-Info modify "IN IP4 10.80.13.12." "IN IP4
192.65.79.x"
rule 40 response ANY sdp-header Audio-Connection-Info modify "IN IP4 10.80.13.12"
"IN IP4 192.65.79.x"
rule 60 response ANY sdp-header Session-Owner modify "(.*) IN IP4 10.80.13.12" "\1
IN IP4 192.65.79.x"
rule 70 response ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
10.80.13.12 (.*)" "a=candidate:1 1\1 192.65.79.x \2"
rule 80 response ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
10.80.13.12 (.*)" "a=candidate:1 2\1 192.65.79.x \2"
rule 90 response ANY sdp-header Audio-Attribute modify "a=rtcp:(.*) IN IP4
10.80.13.12" "a=rtcp:\1 IN IP4 192.65.79.x"
```


3.12 Specify the trust point in TLS profile

3.12.1.1 To Webex calling Tenant 1

```
voice class tls-profile 100
description Webexcalling_tenant1
trustpoint sbc6
cn-san validate bidirectional
cn-san 1 us01.sipconnect.bclld.webex.com
```

3.12.1.2 To Webex calling Tenant 2

```
voice class tls-profile 600
description Webexcalling_tenant2
trustpoint sbc5
cn-san validate bidirectional
cn-san 1 us01.sipconnect.bclld.webex.com
```

Explanation

Command	Description
cn-san validate bidirectional	Enable CN SAN FQDN validation for bidirectional handshake in certificates from Webex
cn-san 1 us01.sipconnect.bclld.webex.com	Mention the CN SAN FQDN to validate in Webex certificate
trustpoint sbcx	Associate the trunk FQDN trustpoint to Webex calling tenants

3.13 Tenant

Mention secure listen-port in each tenant towards Webex calling tenant.

3.13.1.1 To Webex Calling tenant 1

```
voice class tenant 200
  tls-profile 100
  listen-port secure 5061
  no remote-party-id
  srtp-crypto 200
  localhost dns:sbc6.tekvizionlabs.com
  session transport tcp tls
  no session refresh
  error-passthru
  bind control source-interface GigabitEthernet0/0/2
  bind media source-interface GigabitEthernet0/0/2
  no pass-thru content custom-sdp
  sip-profiles 200
  sip-profiles 201 inbound
  privacy-policy passthru
```

3.13.1.2 To Webex Calling tenant 2

```
voice class tenant 600
  tls-profile 600
  listen-port secure 5062
  no remote-party-id
  srtp-crypto 200
  localhost dns:sbc5.tekvlabs.com
  session transport tcp tls
  no session refresh
  error-passthru
  bind control source-interface GigabitEthernet0/0/2
  bind media source-interface GigabitEthernet0/0/2
  no pass-thru content custom-sdp
  sip-profiles 600
  sip-profiles 602 inbound
  privacy-policy passthru
```

3.13.1.3 *Tenant to PSTN Lumen*

```
voice class tenant 100
  session transport tcp
  error-passthru
  bind control source-interface GigabitEthernet0/0/1.1
  bind media source-interface GigabitEthernet0/0/1.1
  no pass-thru content custom-sdp
  privacy-policy passthru
```

3.13.1.4 *Tenant to PSTN Verizon*

```
voice class tenant 400
  session transport udp
  error-passthru
  bind control source-interface GigabitEthernet0/0/1.2
  bind media source-interface GigabitEthernet0/0/1.2
  no pass-thru content custom-sdp
  privacy-policy passthru
```

3.14 Number translation rules

The following translation rule applies for non +E164 from PSTN to Webex calling in E164.

3.14.1.1 To Webex Calling

```
voice translation-rule 100
  rule 1 /^\[2-9].....\)/ /+1\1/
!
voice translation-profile 100
  translate calling 100
  translate called 100
```

3.14.1.2 To PSTN

```
voice translation-rule 200
  rule 1 /^+1\(.*\)/ /\1/
  rule 2 /^+91\(.*\)/ /01191\1/
!
voice translation-profile 200
  translate calling 200
  translate called 200
```

3.15 Dial peers

3.15.1.1 Inbound calls from Cisco Webex Calling tenant 1

```
voice class uri 200 sip
  host sbc6.tekvizionlabs.com
!
voice class dpg 200
  description Wxtenant1 to Lumen
  dial-peer 101 preference 1
!
dial-peer voice 200101 voip
  description Inbound from Webex Calling
  session protocol sipv2
```

```
session transport tcp tls
destination dpg 200
incoming uri request 200
voice-class codec 100
voice-class stun-usage 100
voice-class sip profiles 200
voice-class sip tenant 200
dtmf-relay rtp-nte
srtp
no vad
```

3.15.1.2 Outbound calls to Cisco Webex Calling tenant 1

```
dial-peer voice 200201 voip
description Outbound Webex Calling tenant1
destination-pattern BAD.BAD
session protocol sipv2
session target dns:us01.sipconnect.bcld.webex.com
session transport tcp tls
voice-class codec 100
voice-class stun-usage 100
voice-class sip rel1xx disable
voice-class sip asserted-id pai
voice-class sip profiles 200
voice-class sip tenant 200
voice-class sip options-keepalive profile 100
dtmf-relay rtp-nte
srtp
no vad
```

3.15.1.3 Inbound calls from Cisco Webex Calling tenant 2

```
voice class uri 600 sip
  host sbc5.tekvlabs.com
!
voice class dpg 600
  description wxtenant2 to Verizon
  dial-peer 401 preference 1
!
dial-peer voice 600101 voip
  description Inbound from Webex Calling tenant 2
  session protocol sipv2
  session transport tcp tls
  destination dpg 600
  incoming uri request 600
  voice-class codec 100
  voice-class stun-usage 100
  voice-class sip profiles 600
  voice-class sip tenant 600
  dtmf-relay rtp-nte
  srtp
  no vad
```

3.15.1.4 Outbound calls to Cisco Webex Calling tenant 2

```
dial-peer voice 600201 voip
  description Outbound Webex Calling tenant2
  destination-pattern BAD.BAD
  session protocol sipv2
  session target dns:us01.sipconnect.bcld.webex.com
  session transport tcp tls
  voice-class codec 100
  voice-class stun-usage 100
  voice-class sip rel1xx disable
  voice-class sip asserted-id pai
  voice-class sip profiles 600
  voice-class sip tenant 600
  voice-class sip options-keepalive profile 600
```

```
dtmf-relay rtp-nte
srtp
no vad
```

3.15.1.5 Inbound calls from PSTN Lumen

```
voice class uri 100 sip
  host 10.64.1.x
!
voice class dpg 100
  description Lumen to Wxtenant1
  dial-peer 200201
!
dial-peer voice 100 voip
  description Incoming dial-peer from PSTN
  translation-profile incoming 100
  session protocol sipv2
  destination dpg 100
  incoming uri from 100
  voice-class codec 100
  voice-class sip tenant 100
  dtmf-relay rtp-nte
  no vad
```

3.15.1.6 Outbound calls to PSTN Lumen

```
dial-peer voice 101 voip
  description outgoing dial-peer to IP PSTN
  translation-profile outgoing 200
  destination-pattern BAD.BAD
  session protocol sipv2
  session target ipv4:10.64.1.x:5060
  session transport tcp
  voice-class codec 100
  voice-class sip options-ping 60
  voice-class sip tenant 100
  dtmf-relay rtp-nte
  no vad
```

3.15.1.7 Inbound calls from PSTN Verizon

```
voice class uri 400 sip
  host ipv4:152.188.28.14x
  host ipv4:152.188.28.19x
!
voice class dpg 201
  description verizon to Wxtenant2
  dial-peer 600201
!
dial-peer voice 400 voip
  description Incoming dial-peer from PSTN Verizon
  translation-profile incoming 100
  session protocol sipv2
  session transport udp
  destination dpg 201
  incoming uri via 400
  voice-class codec 100
  voice-class sip tenant 300
  voice-class sip bind control source-interface GigabitEthernet0/0/1.2
  voice-class sip bind media source-interface GigabitEthernet0/0/1.2
  dtmf-relay rtp-nte
  no vad
```

3.15.1.8 Outbound calls to PSTN Verizon

```
dial-peer voice 401 voip
  description outgoing dial-peer to PSTN Verizon
  translation-profile outgoing 200
  destination-pattern BAD.BAD
  session protocol sipv2
  session target ipv4:152.188.28.14x:5232
  session transport udp
  voice-class codec 100
  voice-class sip tenant 400
  voice-class sip options-keepalive
  dtmf-relay rtp-nte
  no vad
```


3.16 Running Configuration

The following configuration snippet contains a sample configuration of Cisco CUBE (non-NAT) with all parameters detailed above.

3.16.1.1 Cisco CUBE 1

Building configuration...

```
Current configuration: 11165 bytes
!
version 17.9
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
!
hostname 8K_MTLS_webex
!
boot-start-marker
boot system bootflash:c8000be-universalk9.17.09.01a.SPA.bin
boot-end-marker
!
logging buffered 21474836
no aaa new-model
clock timezone UTC -5 0
clock calendar-valid
!
ip name-server 8.8.8.8
ip domain name example.com
!
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-995020091
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-995020091
  revocation-check none
  rsakeypair TP-self-signed-995020091
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
```

```
    revocation-check crl
!
crypto pki trustpoint sbc6
  enrollment pkcs12
  revocation-check crl
  rsakeypair sbc6
!
crypto pki trustpoint sbc5
  enrollment pkcs12
  revocation-check crl
  rsakeypair sbc5
!
crypto pki certificate chain TP-self-signed-995020091
  certificate self-signed 01
crypto pki certificate chain SLA-TrustPoint
  certificate ca 01
crypto pki certificate chain sbc6
  certificate 00BAB7A09A134933DF
  certificate ca 07
crypto pki certificate chain sbc5
  certificate 00AA64B57D9D3ACFCD
  certificate ca 07
!
crypto pki certificate pool
  cabundle nvram:ios_core.p7b
!
voice service voip
  ip address trusted list
    ipv4 139.177.65.53 255.255.255.255
    ipv4 85.119.56.128 255.255.255.192
    ipv4 85.119.57.128 255.255.255.192
    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 135.84.172.0 255.255.255.128
    ipv4 135.84.173.0 255.255.255.128
    ipv4 135.84.174.0 255.255.255.128
    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
    ipv4 185.115.196.0 255.255.255.128
    ipv4 185.115.197.0 255.255.255.128
    ipv4 199.19.197.0 255.255.255.0
    ipv4 199.19.199.0 255.255.255.0
    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 128.177.14.0 255.255.255.128
ipv4 128.177.36.0 255.255.255.192
ipv4 10.64.1.x
ipv4 152.188.28.0
address-hiding
mode border-element
allow-connections sip to sip
redundancy-group 1
no supplementary-service sip refer
no supplementary-service sip handle-replaces
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback
none
trace
sip
listen-port secure 5067
early-offer forced
g729 annexb-all
no call service stop
!
!
voice class uri 100 sip
host 10.64.1.x
!
voice class uri 200 sip
host sbc6.tekvizionlabs.com
!
voice class uri 600 sip
pattern sbc5.tekvlabs.com
!
voice class uri 300 sip
pattern 10.71.12.11
!
voice class uri 400 sip
host ipv4:152.188.28.xxx
host ipv4:152.188.28.xx
!
voice class codec 100
codec preference 2 g711ulaw
codec preference 3 g711alaw
codec preference 4 opus
!
voice class codec 200
codec preference 1 opus
!
voice class stun-usage 100
stun usage ice lite
!

```

```

voice class sip-profiles 100
  rule 10 request OPTIONS sip-header Contact modify "<sip:.*:"
"<sip:sbc6.tekvizionlabs.com:"
!
voice class sip-profiles 200
  rule 10 request ANY sip-header Contact modify "@.*:"
"@sbc6.tekvizionlabs.com:"
  rule 20 response ANY sip-header Contact modify "@.*:"
"@sbc6.tekvizionlabs.com:"

!
voice class sip-profiles 601
  rule 10 request OPTIONS sip-header Contact modify "<sip:.*:"
"<sip:sbc5.tekvlabs.com:"
!
voice class sip-profiles 600
  rule 10 request ANY sip-header Contact modify "@.*:"
"@sbc5.tekvlabs.com:"
  rule 20 response ANY sip-header Contact modify "@.*:"
"@sbc5.tekvlabs.com:"
!
voice class dpg 600
  description wxtenant2 to Verizon
  dial-peer 401 preference 1
!
voice class dpg 200
  description Wxtenant1 to Lumen
  dial-peer 101 preference 1
!
voice class dpg 201
  description verizon to Wxtenant2
  dial-peer 600201
!
voice class dpg 100
  description Lumen to Wxtenant1
  dial-peer 200201
!
voice class sip-options-keepalive 100
  description Keepalive Webex Calling
  up-interval 5
  transport tcp tls
  sip-profiles 100
!
voice class sip-options-keepalive 600
  description Keepalive Webex calling
  up-interval 5
  transport tcp tls
  sip-profiles 601
!
voice class tenant 200
  tls-profile 100
  listen-port secure 5061

```

```

no remote-party-id
srtp-crypto 200
localhost dns:sbc6.tekvizionlabs.com
session transport tcp tls
no session refresh
error-passthru
sip-profiles 200
sip-profiles 201 inbound
bind control source-interface GigabitEthernet0/0/2
bind media source-interface GigabitEthernet0/0/2
no pass-thru content custom-sdp
privacy-policy passthru
!
voice class tenant 100
  session transport tcp
  error-passthru
  bind media source-interface GigabitEthernet0/0/1.1
  bind control source-interface GigabitEthernet0/0/1.1
  no pass-thru content custom-sdp
  privacy-policy passthru
!
!
voice class tenant 400
  session transport udp
  error-passthru
  bind control source-interface GigabitEthernet0/0/1.2
  bind media source-interface GigabitEthernet0/0/1.2
  no pass-thru content custom-sdp
  privacy-policy passthru
!
voice class tenant 600
  tls-profile 600
  listen-port secure 5062
  no remote-party-id
  srtp-crypto 200
  localhost dns:sbc5.tekvlabs.com
  session transport tcp tls
  no session refresh
  error-passthru
  bind control source-interface GigabitEthernet0/0/2
  bind media source-interface GigabitEthernet0/0/2
  no pass-thru content custom-sdp
  sip-profiles 600
  sip-profiles 602 inbound
  privacy-policy passthru
!
voice class srtp-crypto 200
  crypto 1 AES_CM_128_HMAC_SHA1_80
!
voice class tls-profile 100
  description Webexcalling_tenant1
  trustpoint sbc6

```

```

cn-san validate bidirectional
cn-san 1 us01.sipconnect.bclld.webex.com
!
voice class tls-profile 600
description Webexcalling_tenant2
trustpoint sbc5
cn-san validate bidirectional
cn-san 1 us01.sipconnect.bclld.webex.com
!
voice translation-rule 100
rule 1 /^\[2-9].....\)/ /+1\1/
!
voice translation-rule 200
rule 1 /^+1\(.*\)/ /\1/
rule 4 /^+91\(.*\)/ /01191\1/
!
voice translation-profile 100
translate calling 100
translate called 100
!
voice translation-profile 200
translate calling 200
translate called 200
!
voice-card 0/1
dsp services dspfarm
no watchdog
!
no license feature hseck9
license udi pid C8300-1N1S-6T sn xxxx
license boot level network-essentials addon dna-essentials
memory free low-watermark processor 69096
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
enable secret 9 xxxx
!
redundancy
mode none
application redundancy
group 1
name cube-ha
priority 100 failover threshold 75
timers delay 30 reload 60
control GigabitEthernet0/0/0 protocol 1
data GigabitEthernet0/0/0
track1 shutdown
track 2 shutdown
track 3 shutdown
!

```

```

track 1 interface GigabitEthernet0/0/1.1 line-protocol
!
track 2 interface GigabitEthernet0/0/1.2 line-protocol
!
track 3 interface GigabitEthernet0/0/2 line-protocol
!
interface GigabitEthernet0/0/0
  description To HA interface
  ip address 10.64.5.234 255.255.0.0
  negotiation auto
!
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/1.1
  description To PSTN Lumen
  encapsulation dot1Q 3811
  ip address 10.80.11.138 255.255.255.0
  redundancy rii 16
  redundancy group 1 ip 10.80.11.136 exclusive
!
interface GigabitEthernet0/0/1.2
  description To PSTN Verizon
  encapsulation dot1Q 1506
  ip address 199.182.124.25x 255.255.255.192
  redundancy rii 18
  redundancy group 1 ip 199.182.124.2xx exclusive
!
interface GigabitEthernet0/0/2
  description To Webex tenant
  ip address 192.65.79.11x 255.255.255.224
  negotiation auto
  redundancy rii 17
  redundancy group 1 ip 192.65.79.1xx exclusive
!
interface GigabitEthernet0/0/3
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/0/4
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/0/5
  no ip address
  shutdown
  negotiation auto
!
interface Service-Engine0/1/0

```

```

!
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/2
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.65.79.129
ip route 10.64.0.0 255.255.0.0 10.80.11.1
ip route 10.70.0.0 255.255.0.0 10.80.11.1
ip route 152.188.28.0 255.255.255.0 199.182.124.1xx
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
dial-peer voice 200101 voip
  description Inbound from Webex Calling
  session protocol sipv2
  session transport tcp tls
  destination dpg 200
  incoming uri request 200
  voice-class codec 100
  voice-class stun-usage 100
  voice-class sip profiles 200
  voice-class sip tenant 200
  dtmf-relay rtp-nte
  srtp
  no vad
!
dial-peer voice 200201 voip
  description Outbound Webex Calling tenant1
  destination-pattern BAD.BAD
  session protocol sipv2
  session target dns:us01.sipconnect.bclld.webex.com
  session transport tcp tls
  voice-class codec 100
  voice-class stun-usage 100
  voice-class sip rellxx disable
  voice-class sip asserted-id pai
  voice-class sip profiles 200
  voice-class sip tenant 200
  voice-class sip options-keepalive profile 100
  dtmf-relay rtp-nte
  srtp
  no vad
!
dial-peer voice 600101 voip

```



```

description Inbound from Webex Calling tenant 2
session protocol sipv2
destination dpg 600
session transport tcp tls
incoming uri request 600
voice-class codec 100
voice-class stun-usage 100
voice-class sip profiles 600
voice-class sip tenant 600
dtmf-relay rtp-nte
srtp
no vad

!
dial-peer voice 600201 voip
description Outbound Webex Calling tenant2
destination-pattern BAD.BAD
session protocol sipv2
session target dns:us01.sipconnect.bcl.d.webex.com
session transport tcp tls
voice-class codec 100
voice-class stun-usage 100
voice-class sip rel1xx disable
voice-class sip asserted-id pai
voice-class sip profiles 600
voice-class sip tenant 600
voice-class sip options-keepalive profile 600
dtmf-relay rtp-nte
srtp
no vad

!
dial-peer voice 100 voip
description Incoming dial-peer from PSTN
translation-profile incoming 100
session protocol sipv2
destination dpg 100
incoming uri from 100
voice-class codec 100
voice-class sip tenant 100
dtmf-relay rtp-nte
no vad

!
dial-peer voice 101 voip
description outgoing dial-peer to IP PSTN
translation-profile outgoing 200
destination-pattern BAD.BAD
session protocol sipv2
session target ipv4:10.64.1.x:5060

voice-class codec 100
voice-class sip options-ping 60
voice-class sip tenant 100

```

```

dtmf-relay rtp-nte
no vad
!
dial-peer voice 400 voip
description Incoming dial-peer from PSTN Verizon
translation-profile incoming 100
session protocol sipv2
destination dpg 201
session transport udp
incoming uri via 400
voice-class codec 100
voice-class sip tenant 400
dtmf-relay rtp-nte
no vad
!

dial-peer voice 401 voip
description outgoing dial-peer to PSTN Verizon
translation-profile outgoing 200
destination-pattern BAD.BAD
session protocol sipv2
session target ipv4:152.188.28.14x:5232
session transport udp
voice-class codec 100
voice-class sip tenant 400
voice-class sip options-keepalive
dtmf-relay rtp-nte
no vad
!
gateway
timer receive-rtp 1200
!
sip-ua
no remote-party-id
transport tcp tls v1.2
!
line con 0
exec-timeout 5 0
password 7 xxxxxx
logging synchronous
login
stopbits 1
line aux 0
line vty 0 4
exec-timeout 60 0
password 7 xxxxxx
logging synchronous
login
transport input telnet
line vty 5 14
login
transport input ssh

```

```
!  
call-home  
  ! If contact email address in call-home is configured as sch-smart-  
  licensing@cisco.com  
  ! the email address configured in Cisco Smart License Portal will be  
  used as contact email address to send SCH notifications.  
  contact-email-addr sch-smart-licensing@cisco.com  
  profile "CiscoTAC-1"  
  active  
  destination transport-method http  
ntp server 10.10.10.5  
!  
end
```

3.16.1.2 Cisco CUBE2

Building configuration...

```
Current configuration : 12534 bytes
!
version 17.9
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform hardware throughput crypto 25M
!
hostname CUBE8K
!
boot-start-marker
boot system bootflash:c8000be-universalk9.17.09.01a.SPA.bin
boot-end-marker
!
logging buffered 214748364
no aaa new-model
clock timezone UTC -5 0
clock calendar-valid
!
ip name-server 8.8.8.8
ip domain name example.com
!
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint TP-self-signed-2307055185
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2307055185
  revocation-check none
  rsakeypair TP-self-signed-2307055185
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
crypto pki trustpoint sbc6
  enrollment pkcs12
  revocation-check crl
  rsakeypair sbc6
!
```

```

crypto pki trustpoint sbc5
  enrollment pkcs12
  revocation-check crl
  rsakeypair sbc5
!
crypto pki certificate chain TP-self-signed-2307055185
  certificate self-signed 01
crypto pki certificate chain SLA-TrustPoint
  certificate ca 01
crypto pki certificate chain sbc6
  certificate 00BAB7A09A134933DF
  certificate ca 07
crypto pki certificate chain sbc5
  certificate 00AA64B57D9D3ACFCD
  certificate ca 07
!
crypto pki certificate pool
  cabundle nvram:ios.p7bcrypto pki certificate chain SAN
  certificate 00A76F21D0D0E2906D
  certificate ca 07
!
crypto pki certificate pool
  cabundle nvram:ios_core.p7b
!
voice service voip
  ip address trusted list
    ipv4 139.177.65.53 255.255.255.255
    ipv4 85.119.56.128 255.255.255.192
    ipv4 85.119.57.128 255.255.255.192
    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 135.84.172.0 255.255.255.128
    ipv4 135.84.173.0 255.255.255.128
    ipv4 135.84.174.0 255.255.255.128
    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
    ipv4 185.115.196.0 255.255.255.128
    ipv4 185.115.197.0 255.255.255.128
    ipv4 199.19.197.0 255.255.255.0
    ipv4 199.19.199.0 255.255.255.0
    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 128.177.14.0 255.255.255.128
    ipv4 128.177.36.0 255.255.255.192
    ipv4 10.64.1.x
    ipv4 152.188.28.0
address-hiding
mode border-element
allow-connections sip to sip
redundancy-group 1
no supplementary-service sip refer
no supplementary-service sip handle-replaces
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback
none
trace
sip
    listen-port secure 5067
    early-offer forced
    g729 annexb-all
no call service stop
!
voice class uri 100 sip
    host 10.64.1.x
!
voice class uri 200 sip
    host sbc6.tekvizionlabs.com
!
voice class uri 600 sip
    pattern sbc5.tekvlabs.com
!
voice class uri 300 sip
    pattern 10.71.12.11
!
voice class uri 400 sip
    host ipv4:152.188.28.xxx
    host ipv4:152.188.28.xx
!
voice class codec 100
    codec preference 2 g711ulaw
    codec preference 3 g711alaw
    codec preference 4 opus
!
voice class codec 200
    codec preference 1 opus
!
voice class stun-usage 100
    stun usage ice lite
!
voice class sip-profiles 100
    rule 10 request OPTIONS sip-header Contact modify "<sip:.*:"
"<sip:sbc6.tekvizionlabs.com:"

```

```

!
voice class sip-profiles 200
  rule 10 request ANY sip-header Contact modify "@.*:"
"@sbc6.tekvizionlabs.com:"
  rule 20 response ANY sip-header Contact modify "@.*:"
"@sbc6.tekvizionlabs.com:"

!
voice class sip-profiles 601
  rule 10 request OPTIONS sip-header Contact modify "<sip:.*:"
"<sip:sbc5.tekvlabs.com:"

!
voice class sip-profiles 600
  rule 10 request ANY sip-header Contact modify "@.*:"
"@sbc5.tekvlabs.com:"
  rule 20 response ANY sip-header Contact modify "@.*:"
"@sbc5.tekvlabs.com:"
!
voice class dpg 600
  description wxtenant2 to Verizon
  dial-peer 401 preference 1
!
voice class dpg 200
  description Wxtenant1 to Lumen
  dial-peer 101 preference 1
!
voice class dpg 201
  description verizon to Wxtenant2
  dial-peer 600201
!
voice class dpg 100
  description Lumen to Wxtenant1
  dial-peer 200201

!
voice class sip-options-keepalive 100
  description Keepalive Webex Calling
  up-interval 5
  transport tcp tls
  sip-profiles 100
!
voice class sip-options-keepalive 600
  description Keepalive Webex calling
  up-interval 5
  transport tcp tls
  sip-profiles 601
!
voice class tenant 200

```

```

tls-profile 100
listen-port secure 5061
  no remote-party-id
  srtp-crypto 200
  localhost dns:sbc6.tekvizionlabs.com
  session transport tcp tls
  no session refresh
  error-passthru
  bind control source-interface GigabitEthernet0/0/2
  bind media source-interface GigabitEthernet0/0/2
  no pass-thru content custom-sdp
  sip-profiles 200
  sip-profiles 201 inbound
  privacy-policy passthru
!
voice class tenant 100
  session transport tcp
  error-passthru
  bind media source-interface GigabitEthernet0/0/1.1
  bind control source-interface GigabitEthernet0/0/1.1
  no pass-thru content custom-sdp
  privacy-policy passthru
!
voice class tenant 400
  session transport udp
  error-passthru
  bind control source-interface GigabitEthernet0/0/1.2
  bind media source-interface GigabitEthernet0/0/1.2
  no pass-thru content custom-sdp
  privacy-policy passthru
!
voice class tenant 600
  tls-profile 600
  listen-port secure 5062
  no remote-party-id
  srtp-crypto 200
  localhost dns:sbc5.tekvlabs.com
  session transport tcp tls
  no session refresh
  error-passthru
  bind control source-interface GigabitEthernet0/0/2
  bind media source-interface GigabitEthernet0/0/2
  no pass-thru content custom-sdp
  sip-profiles 600
  sip-profiles 602 inbound
  privacy-policy passthru
!
voice class srtp-crypto 200
  crypto 1 AES_CM_128_HMAC_SHA1_80
!
voice class tls-profile 100
  description Webexcalling_tenant1

```



```

track 1 interface GigabitEthernet0/0/1.1 line-protocol
!
track 2 interface GigabitEthernet0/0/1.2 line-protocol
!
track 3 interface GigabitEthernet0/0/2 line-protocol
!
interface GigabitEthernet0/0/0
  description To HA interface
  ip address 10.64.5.235 255.255.0.0
  negotiation auto
!
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
!
interface GigabitEthernet0/0/1.1
  description To PSTN Lumen
  encapsulation dot1Q 3811
  ip address 10.80.11.138 255.255.255.0
  redundancy rii 16
  redundancy group 1 ip 10.80.11.136 exclusive
!
interface GigabitEthernet0/0/1.2
  description To PSTN Verizon
  encapsulation dot1Q 1506
  ip address 199.182.124.2xx 255.255.255.192
  redundancy rii 18
  redundancy group 1 ip 199.182.124.2xx exclusive
!
interface GigabitEthernet0/0/2
  description To Webex tenant
  ip address 192.65.79.1xx 255.255.255.224
  negotiation auto
  redundancy rii 17
  redundancy group 1 ip 192.65.79.1xx exclusive
!
interface GigabitEthernet0/0/3
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/0/4
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet0/0/5
  no ip address
  shutdown
  negotiation auto
!
interface Service-Engine0/1/0

```

```

!
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/2
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.65.79.129
ip route 10.64.0.0 255.255.0.0 10.80.11.1
ip route 10.70.0.0 255.255.0.0 10.80.11.1
ip route 152.188.28.0 255.255.255.0 199.182.124.1xx

!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
dial-peer voice 200101 voip
  description Inbound from Webex Calling
  session protocol sipv2
  destination dpg 200
  session transport tcp tls
  incoming uri request 200
  voice-class codec 100
  voice-class stun-usage 100
  voice-class sip profiles 200
  voice-class sip tenant 200
  dtmf-relay rtp-nte
  srtp
  no vad
!
dial-peer voice 200201 voip
  description Outbound Webex Calling tenant1
  destination-pattern BAD.BAD
  session protocol sipv2
  session target dns:us01.sipconnect.bclld.webex.com
  session transport tcp tls
  voice-class codec 100
  voice-class stun-usage 100
  voice-class sip rel1xx disable
  voice-class sip asserted-id pai
  voice-class sip profiles 200
  voice-class sip tenant 200
  voice-class sip options-keepalive profile 100
  dtmf-relay rtp-nte
  srtp
  no vad
!

```

```
dial-peer voice 600101 voip
  description Inbound from Webex Calling tenant 2
  session protocol sipv2
  destination dpg 600
  session transport tcp tls
  incoming uri request 600
  voice-class codec 100
  voice-class stun-usage 100
  voice-class sip profiles 600
  voice-class sip tenant 600
  dtmf-relay rtp-nte
  srtp
  no vad
```

!

```
dial-peer voice 600201 voip
  description Outbound Webex Calling tenant2
  destination-pattern BAD.BAD
  session protocol sipv2
  session target dns:us01.sipconnect.bclid.webex.com
  session transport tcp tls
  voice-class codec 100
  voice-class stun-usage 100
  voice-class sip rel1xx disable
  voice-class sip asserted-id pai
  voice-class sip profiles 600
  voice-class sip tenant 600
  voice-class sip options-keepalive profile 600
  dtmf-relay rtp-nte
  srtp
  no vad
```

!

```
dial-peer voice 100 voip
  description Incoming dial-peer from PSTN
  translation-profile incoming 100
  session protocol sipv2
  destination dpg 100
  incoming uri from 100
  voice-class codec 100
  voice-class sip tenant 100
  dtmf-relay rtp-nte
  no vad
```

!

```
dial-peer voice 101 voip
  description outgoing dial-peer to IP PSTN
  translation-profile outgoing 200
  destination-pattern BAD.BAD
  session protocol sipv2
  session target ipv4:10.64.1.x:5060
  voice-class codec 100
  voice-class sip options-ping 60
  voice-class sip tenant 100
```

```

dtmf-relay rtp-nte
no vad
!
dial-peer voice 400 voip
description Incoming dial-peer from PSTN Verizon
translation-profile incoming 100
session protocol sipv2
destination dpg 201
session transport udp
incoming uri via 400
voice-class codec 100
voice-class sip tenant 400
dtmf-relay rtp-nte
no vad
!
!
dial-peer voice 401 voip
description outgoing dial-peer to PSTN Verizon
translation-profile outgoing 200
destination-pattern BAD.BAD
session protocol sipv2
session target ipv4:152.188.28.14x:5232
session transport udp
voice-class codec 100
voice-class sip tenant 400
voice-class sip options-keepalive
dtmf-relay rtp-nte
no vad
!
!
gateway
timer receive-rtp 1200
!
sip-ua
no remote-party-id
transport tcp tls v1.2
!
line con 0
exec-timeout 5 0
password 7 xxxx
logging synchronous
login
stopbits 1
line aux 0
line vty 0 4
exec-timeout 60 0
password 7 xxxxx
logging synchronous
login
transport input telnet
line vty 5 14
login

```

```
transport input ssh
!
call-home
! If contact email address in call-home is configured as sch-smart-
licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be
used as contact email address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
ntp server 10.10.10.5
!
End
```

3.17 Show commands

The following show command output for Cisco CUBE (non-NAT) with public IP address.

3.17.1.1 Dial-peer status to Webex calling

```
8K_MTLS_webex# show dial-peer voip keepalive status
```

TAG	TENANT	DESTINATION	OOD-SessID	PRI	WT	STATUS
200201	200	dns:us01.sipconnect.bcld.webex				active
		sipconnect01ah-us.bcld.webex.	1613	5	25	active
		ipv4:139.177.64.53:5062				
		sipconnect01ai-us.bcld.webex.	1614	5	25	active
		ipv4:139.177.64.54:5062				
		sipconnect02ai-us.bcld.webex.	1615	10	25	active
		ipv4:139.177.65.54:5062				
		sipconnect02ah-us.bcld.webex.	1616	10	25	active
		ipv4:139.177.65.53:5062				
600201	600	dns:us01.sipconnect.bcld.webex				active
		sipconnect01ah-us.bcld.webex.	1617	5	25	active
		ipv4:139.177.64.53:5062				
		sipconnect01ai-us.bcld.webex.	1618	5	25	active
		ipv4:139.177.64.54:5062				
		sipconnect02ai-us.bcld.webex.	1619	10	25	active
		ipv4:139.177.65.54:5062				
		sipconnect02ah-us.bcld.webex.	1620	10	25	active
		ipv4:139.177.65.53:5062				

Note: Command introduced from 17.9.1a IOS

3.17.1.2 Dial-peer Summary

```
8K_MTLS_webex#show dial-peer voice summary
dial-peer hunt 0

          AD                                PRE PASS SESS-SER-GRP\ OUT
TAG      TYPE MIN OPER PREFIX DEST-PATTERN FER THRU SESS-TARGET  STAT PORT  KEEPALIVE
VRF
100      voip up up                                0 syst
101      voip up up          map:100      0 syst ipv4:10.64.1.x:5060      active  NA
200101   voip up up                                0 syst
200201   voip up up          map:2002    0 syst dns:us01.sipconnect.    active  NA
401      voip up up          map:200      0 syst ipv4:152.188.x.x          active  NA
400      voip up up                                0 syst
600201   voip up up          map:6002    0 syst dns:us01.sipconnect.    active  NA
600101   voip up up                                0 syst
```

For server-grp details please execute command: `show voice class server-group <tag_id>`
 To see complete session target for ipv6 use `'sh running-config | section dial-peer <tag>`

3.17.1.3 Voice class Keepalive sip Options

```
8K_MTLS_webex# show voice class sip-options-keepalive
Voice class sip-options-keepalive: 100          AdminStat: Up
Description: Keepalive webex_mTLS
Transport: tcp tls          Sip Profiles: 100
Interval(seconds) Up: 5          Down: 30
Retry: 5

Peer Tag      Server Group    OOD SessID      OOD Stat        IfIndex
-----
200201              Active          13

OOD SessID: 1629          OOD Stat: Active
Target: ipv4:139.177.64.53:5062
Transport: tcp tls          Sip Profiles: 100

OOD SessID: 1630          OOD Stat: Active
Target: ipv4:139.177.64.54:5062
```


Transport: tcp tls Sip Profiles: 100

00D SessID: 1631 OOD Stat: Active

Target: ipv4:139.177.65.54:5062

Transport: tcp tls Sip Profiles: 100

00D SessID: 1632 OOD Stat: Active

Target: ipv4:139.177.65.53:5062

Transport: tcp tls Sip Profiles: 100

Voice class sip-options-keepalive: 600 AdminStat: Up
Description: Keepalive webex_mTLS
Transport: tcp tls Sip Profiles: 601
Interval(seconds) Up: 5 Down: 30
Retry: 5

Peer Tag	Server Group	00D SessID	00D Stat	IfIndex
600201			Active	16

00D SessID: 1633 OOD Stat: Active

Target: ipv4:139.177.64.53:5062

Transport: tcp tls Sip Profiles: 601

00D SessID: 1634 OOD Stat: Active

Target: ipv4:139.177.64.54:5062

Transport: tcp tls Sip Profiles: 601

00D SessID: 1635 OOD Stat: Active

Target: ipv4:139.177.65.54:5062

Transport: tcp tls Sip Profiles: 601

00D SessID: 1636 OOD Stat: Active

Target: ipv4:139.177.65.53:5062

Transport: tcp tls Sip Profiles: 601

For destination configured as DNS - please execute: show dial-peer voip keepalive status

3.17.1.4 SIP-ua connection details

```
8K_MTLS_webex# show sip-ua connections tcp tls detail
Total active connections      : 16
No. of send failures         : 20
No. of remote closures       : 51
No. of conn. failures        : 123
No. of inactive conn. ageouts : 0
TLS client handshake failures : 34
TLS server handshake failures : 4

-----Printing Detailed Connection Report-----
Note:
** Tuples with no matching socket entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
    to overcome this error condition
++ Tuples with mismatched address/port entry
  - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
    to overcome this error condition
* Connections with SIP OAuth ports

Remote-Agent:139.177.64.53, Connections-Count:4
  Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
  TLS-Version Cipher Curve Tenant
  =====
  =====
      5062      77 Established           0 192.65.79.1xx:33971
  TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-256  200
      5062     138 Established           0 192.65.79.1xx:37202
  TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-256  600
      8934     180 Established           0 192.65.79.1xx:5062
  TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-256  600
      8934     221 Established           0 192.65.79.1xx:5061
  TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-256  200

Remote-Agent:139.177.65.54, Connections-Count:4
```

```

Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
TLS-Version Cipher Curve Tenant
=====
=====
5062 63 Established 0 192.65.79.1xx:57535
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 600
5062 99 Established 0 192.65.79.1xx:39149
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 200
8934 224 Established 0 192.65.79.1xx:5061
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 200
8934 227 Established 0 192.65.79.1xx:5062
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 600

```

Remote-Agent:139.177.64.54, Connections-Count:4

```

Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
TLS-Version Cipher Curve Tenant
=====
=====
5062 217 Established 0 192.65.79.1xx:41829
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 200
5062 218 Established 0 192.65.79.1xx:19070
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 600
8934 191 Established 0 192.65.79.1xx:5061
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 200
8934 226 Established 0 192.65.79.1xx:5062
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 600

```

Remote-Agent:139.177.65.53, Connections-Count:4

```

Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
TLS-Version Cipher Curve Tenant
=====
=====
5062 34 Established 0 192.65.79.1xx:26708
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 600
5062 61 Established 0 192.65.79.1xx:22740
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 200
8934 181 Established 0 192.65.79.1xx:5062
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 600
8934 223 Established 0 192.65.79.1xx:5061
TLsv1.2 ECDHE-RSA-AES256-GCM-SHA384 P-256 200

```

----- SIP Transport Layer Listen Sockets -----

Conn-Id	Local-Address	Tenant
=====	=====	=====
0	[0.0.0.0]:5067:	0
6	[10.80.11.136]:5067:	0
7	[199.182.124.2xx]:5067:	0
8	[192.65.79.1xx]:5061:	200
9	[192.65.79.1xx]:5062:	600

3.17.1.5 Show voip trace tenant

INVITE from SBC to Webex – Tenant 1

```
8K_MTLS_webex#Show voip trace tenant 200
----- Cover Buffer -----
Search-key      = +12142425947:+19725980xxx:38486
  Timestamp     = *Mar 29 09:36:16.176
  Buffer-Id     = 6
  CallID       = 38486
  Peer-CallID  = 38485
  Correlator   = 3
  Called-Number = +19725980xxx
  Calling-Number = +12142425947
  SIP CallID   = FC8E292F-CD4B11ED-91928507-E8464F66@sbc6.tekvizionlabs.com
  SIP Session ID = d9f608f394f85a3f85a363d4e5126dc0
  GUID        = 042BF9F18E34
  Tenant      = 200
-----

Sent: SIP TLS message from 192.65.79.1xx:5061 to 139.177.64.53:5062
INVITE sip:+19725980xxx@us01.sipconnect.bcld.webex.com:5062 SIP/2.0

Via: SIP/2.0/TLS 192.65.79.1xx:5061;branch=z9hG4bK8BE31C4F
From: "Joshua Alphin" <sip:+12142425947@sbc6.tekvizionlabs.com>;tag=154F6F3-2102
To: <sip:+19725980xxx@us01.sipconnect.bcld.webex.com>
Date: Wed, 29 Mar 2023 09:36:16 GMT
Call-ID: FC8E292F-CD4B11ED-91928507-E8464F66@sbc6.tekvizionlabs.com
Supported: timer,resource-priority,replaces
Min-SE: 1800
Cisco-Guid: 0069990897-3444314605-2385798166-2368317232
User-Agent: Cisco-SIPGateway/IOS-17.9.1a
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY,
INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1680082576
Contact: <sip:+12142425947@sbc6.tekvizionlabs.com:5061;transport=tls>
Expires: 180
```

```
Allow-Events: telephone-event
Max-Forwards: 69
P-Asserted-Identity: "Joshua Alphin" <sip:+12142425947@sbc6.tekvizionlabs.com>
Session-ID: d9f608f394f85a3f85a363d4e5126dc0;remote=00000000000000000000000000000000
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 580

v=0
o=CiscoSystemsSIP-GW-UserAgent 1220 4872 IN IP4 192.65.79.1xx
s=SIP Call
c=IN IP4 192.65.79.1xx
t=0 0
a=ice-lite
m=audio 8010 RTP/SAVP 0 8 101
c=IN IP4 192.65.79.1xx
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=candidate:1 1 UDP 2130706431 192.65.79.1xx 8010 typ host
a=candidate:1 2 UDP 2130706430 192.65.79.1xx 8011 typ host
a=rtcp:8011 IN IP4 192.65.79.1xx
a=ice-ufrag:MeRy
a=ice-pwd:zS1EH899d0jMFXynSfTWtV
```

INVITE from SBC to Webex – Tenant 2

```
8K_MTLS_webex#Show voip trace tenant 600
```

```
----- Cover Buffer -----
Search-key      = +12142425947:+14698384xxx:38574
Timestamp       = *Mar 29 09:37:06.335
Buffer-Id       = 8
CallID          = 38574
Peer-CallID     = 38573
```

Correlator = 4
Called-Number = +14698384xxx
Calling-Number = +12142425947
SIP CallID = 1A73D143-CD4C11ED-91EF8507-E8464F66@sbc5.tekvlabs.com
SIP Session ID = a972c8f7d7d8521796f93362ceb22b35
GUID = 1A73832F91E9
Tenant = 600

Sent: SIP TLS message from 192.65.79.1xx:5062 to 139.177.64.53:5062
INVITE sip:+14698384xxx@us01.sipconnect.bcld.webex.com:5062 SIP/2.0
Via: SIP/2.0/TLS 192.65.79.1xx:5062;branch=z9hG4bK8C3A2700
From: "214 2425947" <sip:+12142425947@sbc5.tekvlabs.com>;tag=155BAF5-DA9
To: <sip:+14698384xxx@us01.sipconnect.bcld.webex.com>
Date: Wed, 29 Mar 2023 09:37:06 GMT
Call-ID: 1A73D143-CD4C11ED-91EF8507-E8464F66@sbc5.tekvlabs.com
Supported: timer,resource-priority,replaces
Min-SE: 1800
Cisco-Guid: 0443777839-3444314605-2448000263-3896921958
User-Agent: Cisco-SIPGateway/IOS-17.9.1a
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY,
INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 1680082626
Contact: <sip:+12142425947@sbc5.tekvlabs.com:5062;transport=tls>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 68
P-Asserted-Identity: "214 2425947" <sip:+12142425947@sbc5.tekvlabs.com>
Session-ID: a972c8f7d7d8521796f93362ceb22b35;remote=00000000000000000000000000000000
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 580

v=0
o=CiscoSystemsSIP-GW-UserAgent 1435 9731 IN IP4 192.65.79.1xx
s=SIP Call

```
c=IN IP4 192.65.79.1xx
t=0 0
a=ice-lite
m=audio 8014 RTP/SAVP 0 8 101
c=IN IP4 192.65.79.1xx
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=candidate:1 1 UDP 2130706431 192.65.79.1xx 8014 typ host
a=candidate:1 2 UDP 2130706430 192.65.79.1xx 8015 typ host
a=ice-ufrag:uUDK
a=ice-pwd:AemDR17C5z78gg9kcX50DW
a=rtcp:8015 IN IP4 192.65.79.1xx
```

INVITE from Webex to SBC - Tenant 1

```
8K_MTLS_webex#Show voip trace tenant 600
```

```
----- Cover Buffer -----
Search-key      = +19725980xxx:+12142425982:38003
Timestamp       = *Mar 29 09:31:36.593
Buffer-Id       = 1
CallID          = 38003
Peer-CallID     = 38004
Correlator      = 1
Called-Number   = +12142425982
Calling-Number  = +19725980xxx
SIP CallID      = SSE093151853290323-842692971@139.177.65.53
SIP Session ID  = f640087e4d4156d6a7ccd26a58857a68
GUID            = 55E92DB28FA3
Tenant          = 200
-----
```

```
Received: SIP TLS message from 139.177.65.53:8934 to 192.65.79.1xx:5061
```


INVITE
sip:+12142425982@sbc6.tekvizionlabs.com:5061;transport=tls;dtg=sbc6.tekvizionlabs.com
SIP/2.0
Via:SIP/2.0/TLS 139.177.65.53:5062;branch=z9hG4bKBroadworksSSE.-192.65.79.1xxV5061-0-
100-229559215-1680082311853-
From:"Cisco user2"<sip:+19725980xxx@139.177.65.53;user=phone>;tag=229559215-
1680082311853-
To:<sip:+12142425982@91366808.cisco-bcld.com;user=phone>
Call-ID:SSE093151853290323-842692971@139.177.65.53
CSeq:100 INVITE
Contact:<sip:139.177.65.53:5062;transport=tls>
P-Asserted-Identity:"Cisco user2"<sip:+19725980xxx@10.21.0.213;user=phone>
Privacy:none
Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Recv-Info:x-broadworks-client-session-info
X-BroadWorks-Correlation-Info:73896655-e0fb-46f8-a627-f43944f9a17e
Accept:application/media_control+xml,application/sdp,multipart/mixed
Supported:
Max-Forwards:69
Session-ID:be13595c00105000a0004c710c4dfec3;remote=00000000000000000000000000000000
Content-Type:application/sdp
Content-Length:1115

v=0
o=BroadWorks 5488600 1680082311850 IN IP4 135.84.172.117
s=-
c=IN IP4 135.84.172.117
t=0 0
m=audio 22464 RTP/SAVP 99 9 0 8 18 101 108
a=rtpmap:99 opus/48000/2
a=fmtp:99 maxplaybackrate=16000;sprop-
maxcapture=16000;maxaveragebitrate=64000;stereo=0;sprop-
stereo=0;usedtx=0;useinbandfec=0
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:108 telephone-event/48000

```
a=fmtp:108 0-15
a=ptime:20
a=sendrecv
a=ice-ufrag:PP31
a=ice-pwd:YWRD5LI1Ljez/os3HzfuS2
a=candidate:1 1 udp 2130706431 172.16.31.241 19652 typ host
a=candidate:1 2 udp 2130706430 172.16.31.241 19653 typ host
a=candidate:3 1 udp 1694494975 14.142.185.162 19652 typ srflx raddr 172.16.31.241
rport 19652
a=candidate:3 2 udp 1694494974 14.142.185.162 19653 typ srflx raddr 172.16.31.241
rport 19653
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=candidate:mse 1 UDP 16777215 135.84.172.117 22464 typ relay
a=candidate:mse 2 UDP 16777214 135.84.172.117 22465 typ relay
```

INVITE from Webex to SBC - Tenant 2

```
8K_MTLS_webex#Show voip trace tenant 600
----- Cover Buffer -----
Search-key      = +14698384xxx:+12142425947:38168
  Timestamp     = *Mar 29 09:33:10.473
  Buffer-Id      = 3
  CallID        = 38168
  Peer-CallID   = 38169
  Correlator    = 2
  Called-Number = +12142425947
  Calling-Number = +14698384xxx
  SIP CallID    = SSE093325723290323-571795958@139.177.65.54
  SIP Session ID = ea22fc907844537cb529b6ecca898746
  GUID          = 8DDDF4A904B
  Tenant        = 600
-----
289: *Mar 29 09:33:10.473: //38168/8DDDF4A904B/CUBE_VT/SIP/Msg/ccsipDisplayMsg:
Received: SIP TLS message from 139.177.65.54:8934 to 192.65.79.1xx:5062
INVITE sip:+12142425947@sbc5.tekvlabs.com:5062;transport=tls;dtg=sbc5.tekvlabs.com
SIP/2.0
Via:SIP/2.0/TLS 139.177.65.54:5062;branch=z9hG4bKBroadworksSSE.-192.65.79.1xxV5062-0-
100-140154880-1680082405723-
```

From:"CUBE user1"<sip:+14698384xxx@139.177.65.54;user=phone>;tag=140154880-1680082405723-
To:<sip:+12142425947@91366808.cisco-bcld.com;user=phone>
Call-ID:SSE093325723290323-571795958@139.177.65.54
CSeq:100 INVITE
Contact:<sip:139.177.65.54:5062;transport=tls>
P-Asserted-Identity:"CUBE user1"<sip:+14698384xxx@10.71.100.214;user=phone>
Privacy:none
Allow:ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Recv-Info:x-broadworks-client-session-info
X-BroadWorks-Correlation-Info:a1c2be6d-484a-4067-94ff-efeec6b0d999
Accept:application/dtmf-relay,application/media_control+xml,application/sdp,multipart/mixed
Supported:
Max-Forwards:69
Session-ID:7ffeaef100105000a0004c710c4dff2b;remote=00000000000000000000000000000000
Content-Type:application/sdp
Content-Length:1149

v=0
o=BroadWorks 2354893 1680082405717 IN IP4 135.84.172.105
s=-
c=IN IP4 135.84.172.105
t=0 0
m=audio 29704 RTP/SAVP 99 9 0 8 18 101 108
a=rtpmap:99 opus/48000/2
a=fmtp:99 maxplaybackrate=16000;prop-maxcapture=16000;maxaveragebitrate=64000;stereo=0;prop-stereo=0;usedtx=0;useinbandfec=0

a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:108 telephone-event/48000
a=fmtp:108 0-15
a=ptime:20

```
a=sendrecv
a=altc:1 IP4 172.16.25.138 19594
a=ice-ufrag:HUWS
a=ice-pwd:tA0k1z/B7XoPuzl/AotKmZ
a=candidate:1 1 udp 2130706431 172.16.25.138 19594 typ host
a=candidate:1 2 udp 2130706430 172.16.25.138 19595 typ host
a=candidate:3 1 udp 1694494975 14.142.185.162 19594 typ srflx raddr 172.16.25.138
rport 19594
a=candidate:3 2 udp 1694494974 14.142.185.162 19595 typ srflx raddr 172.16.25.138
rport 19595
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=candidate:mse 1 UDP 16777215 135.84.172.105 29704 typ relay
a=candidate:mse 2 UDP 16777214 135.84.172.105 29705 typ relay
```

Important Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES

Corporate

Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European

Headquarters

CiscoSystems
International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas

Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

AsiaPacific

Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at <http://www.cisco.com/go/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

© 2023 Cisco Systems, Inc. All rights reserved.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Printed in the USA