Application Note

Public

Connecting Webex Calling to Lumen SIP Trunk via a Multi-tenant Registration-based Local Gateway using Virtual Cisco Unified Border Element deployed in AWS (vCUBE-on-AWS) [IOS-XE17.9.02a]

August 4, 2023

Table of Contents

Table of Figures

Introduction

This application note describes a tested virtual Cisco Unified Border Element (vCUBE) in Amazon Web Services (AWS) configuration being used as a multi-tenant registration-based Local Gateway (LGW) to connect Webex Calling to a SIP PSTN provider such as Lumen. 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 vCUBE-in-AWS. The configuration settings specifically required for Webex Calling registration-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 registration-based LGW with multi-tenancy running on vCUBE-in-AWS [IOS-XE 17.9.1a] for connectivity to Lumen SIP Trunking service.**
- Testing was performed in accordance with Webex Calling registration-based Local Gateway test methodology along with multi-tenancy and among features verified were – basic calls, DTMF transport, Music on Hold (MOH), semi-attended, attended, and blind transfers, call forward and conference.
- The vCUBE 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 Webex Calling registration-based Local Gateway with multi-tenancy. 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 registration-based Local Gateway trunk to successful interworking with the service provider network.

Network Topology

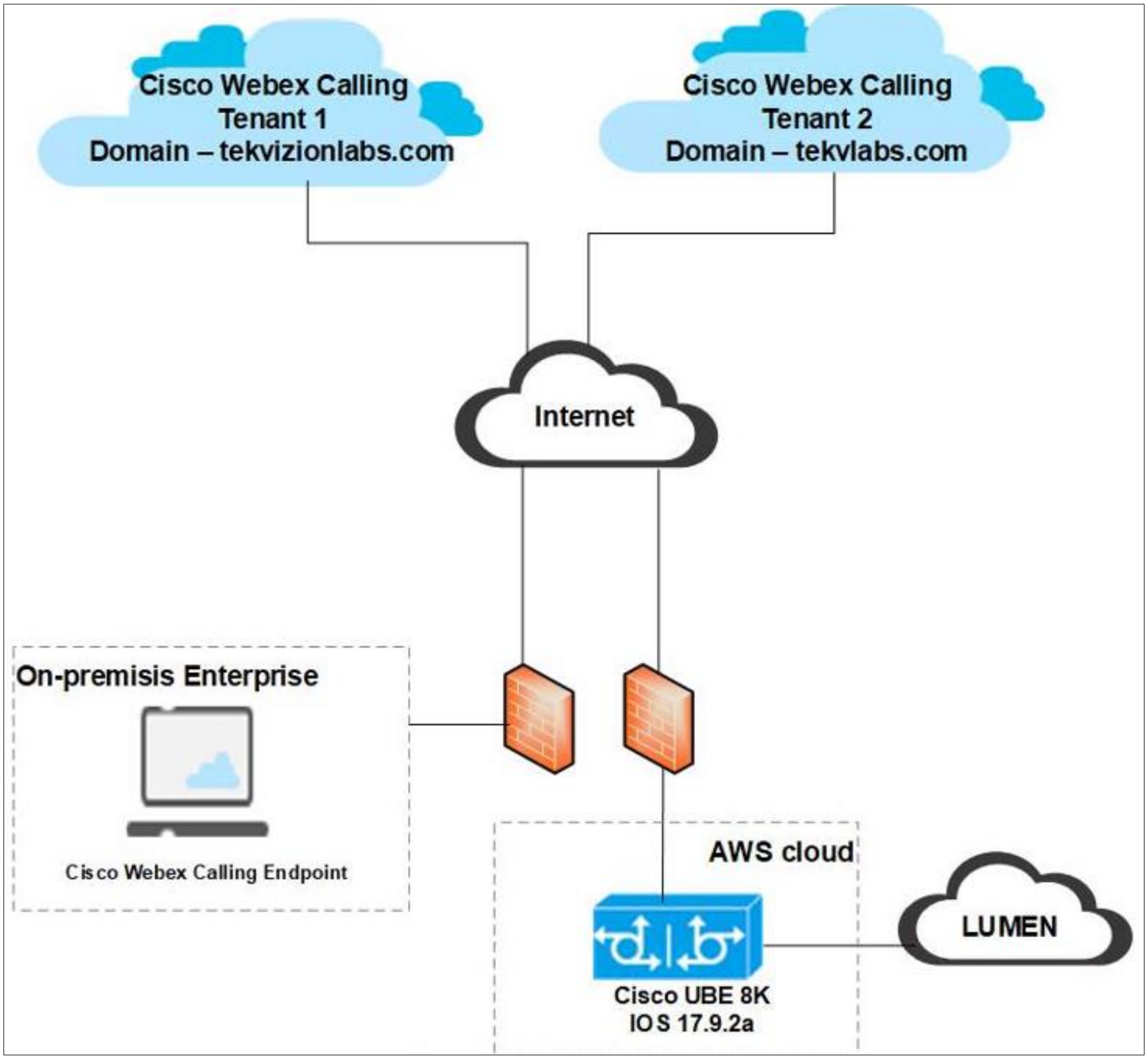


Figure 1: Network Topology

- The network topology includes vCUBE running in AWS as an EC2 instance, Lumen SIP Trunking service, and Cisco Webex Calling Endpoints that include the Webex client and Cisco ATA. vCUBE is registered to Cisco Webex Calling as a LGW for multiple Webex Calling tenants.

Cisco Webex Calling and Cisco CUBE Settings:

Setting	Value
Transport from vCUBE to Webex Calling	TLS with SRTP
Transport from vCUBE to Lumen	UDP with RTP
Voice Mail Support	YES
Session Refresh	YES
Early Media support	YES

System Components

Hardware Requirements

- vCUBE running on AWS
    - cisco C8000V (VXE) processor (revision VXE)
- Cisco ATA 19X

Software Requirements

- vCUBE:
    - 14.6 running IOS-XE 17.9.2a
    - Cisco IOS Software [Cupertino], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.9.2a, RELEASE SOFTWARE (fc4)
- Cisco ATA 19X-MPP-Version: 11-2-1MPP0001-006
- Cisco Webex Client Version: 43.3.0.25468

Features

Verified Features

- Incoming and outgoing calls using G711ulaw voice codecs
- Call Conference
- Fax
    - G711 Pass-through
    - T38 Fax
- Auto Attendant
- Voice Mail
- Call hold & Resume (MoH)
- Semi-attended and Attended Call transfer
- Blind Transfer
- Call forward (all, busy and no answer)
- DTMF (RFC2833)
- IP-PBX Calling number privacy

Features Not Supported

- Cisco Webex Calling does not support the following
    - Fax Super G3 speed
    - Tone on Hold

Features Not Verified

- No option to set G729 codec in Webex. As a result, the G729 FAX test cases are not tested.

Features Not Applicable

- The following are the sections that are not applicable for this test topology:
    - Codec mid-call re-negotiation
    - IP-PBX Telephone Number Support

Caveats

- Internet Gateway in AWS will not convert the public IP to private IP assigned to the vCUBE when it hands over the SIP request from Lumen to the vCUBE-in-AWS. SIP Profiles are used in vCUBE to convert the public IP to the private IP in the SIP messages to process the incoming call. Similarly SIP Profiles are created to convert the private IP address to the public IP address in the SDP and SIP headers for the SIP messages from vCUBE to Lumen for proper call establishment and call clearance.

- The following behavior is observed in media establishment when Webex users use the MPP phone and the Webex client.
    - In the MPP phone, the ICE candidates are not nominated, though STUN request and response are processed between MPP phone and vCUBE. Hence ICE Re-INVITE is not received from Webex. However, media connected between Webex relay server IP and call connected with bi-directional audio. The issue has been raised to cisco [CUBE-1177].
    - In Webex clients, the ICE candidates are nominated with successful STUN processing and media connected with Client User IPs. Hence Webex client is used for this testing.

- Cisco ATA registered to Webex calling uses only G711 codec for voice call. Hence, T38 fax transmission test cases were successful with G711 voice codec only.

- Webex does not negotiate ICE candidate attributes with ATA 19X.

Configuration

1 Configuring Cisco Webex Calling Tenant

1.1 Add location-Trunk

Step1:

Login to Cisco Webex Control Hub and navigate to Services.

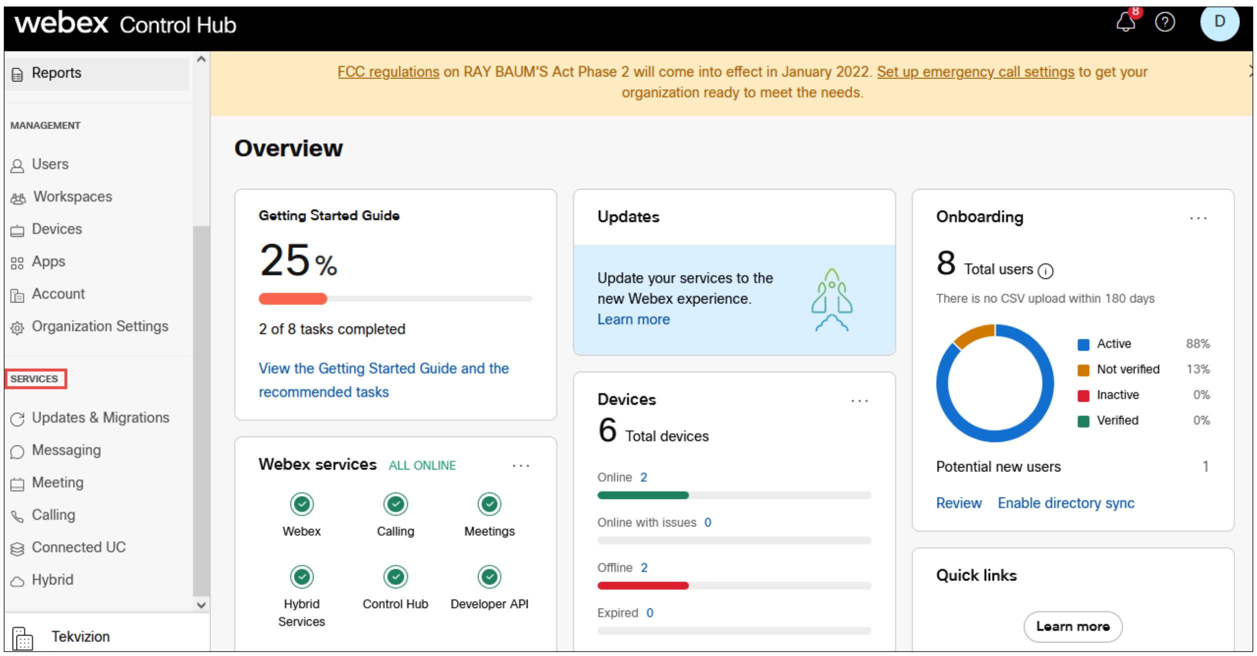


Figure 2: Control Hub Services

Step 2:

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

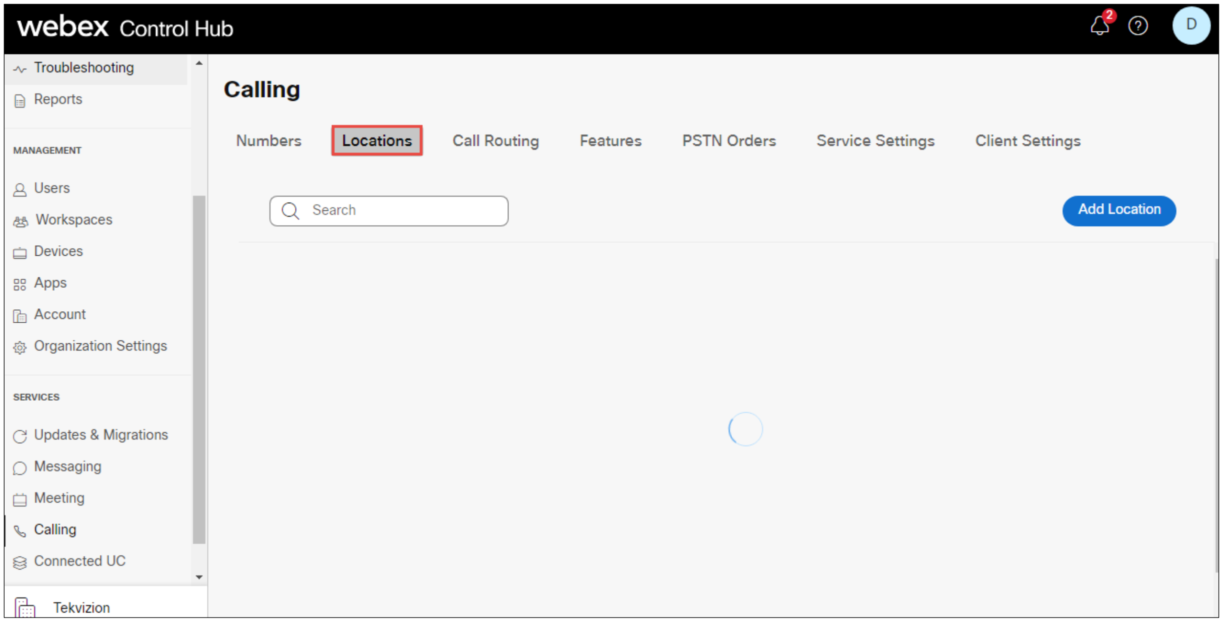


Figure 3: Locations

Step 3:

Click on Add **Location**

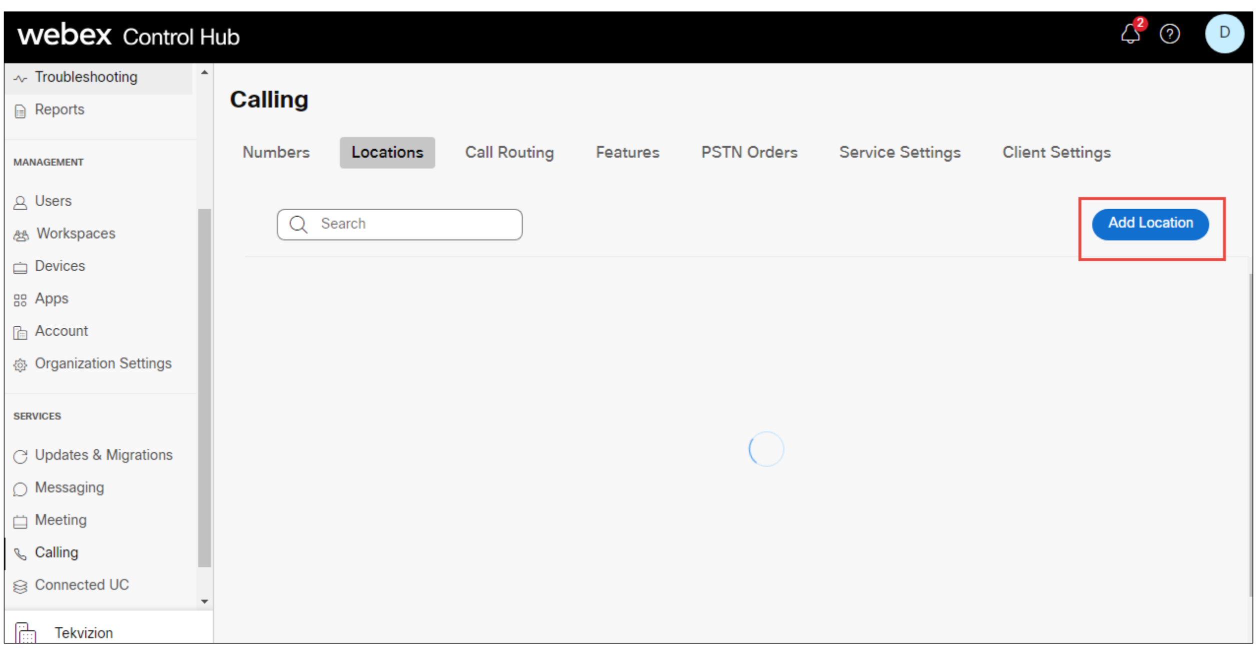


Figure 4: Location creation or selection

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.

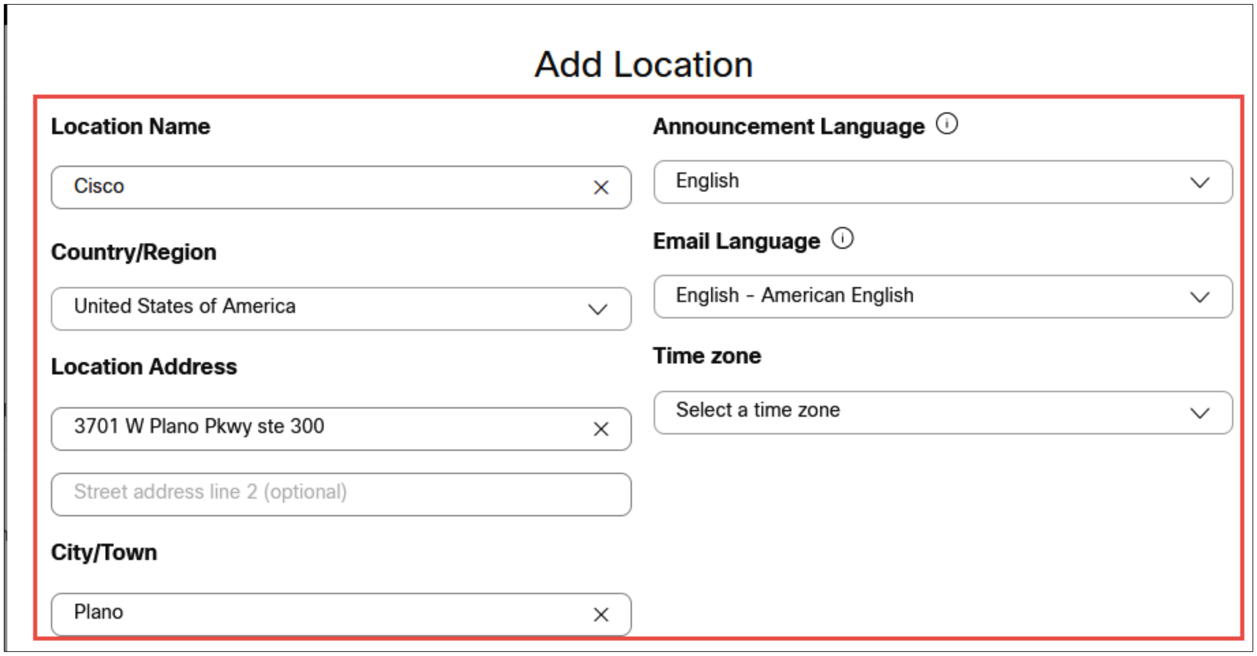


Figure 5: Add location details.

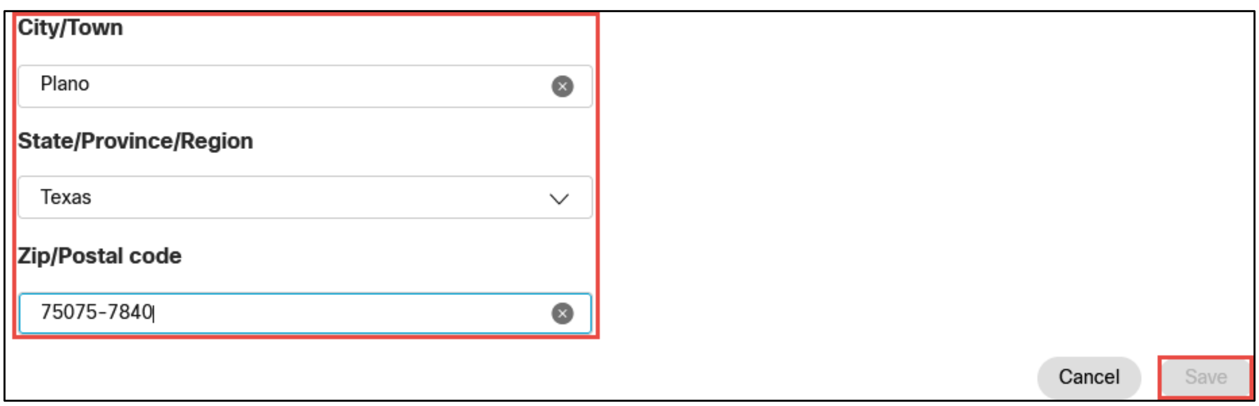


Figure 6: Add location details Contd.,

Step 5:

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

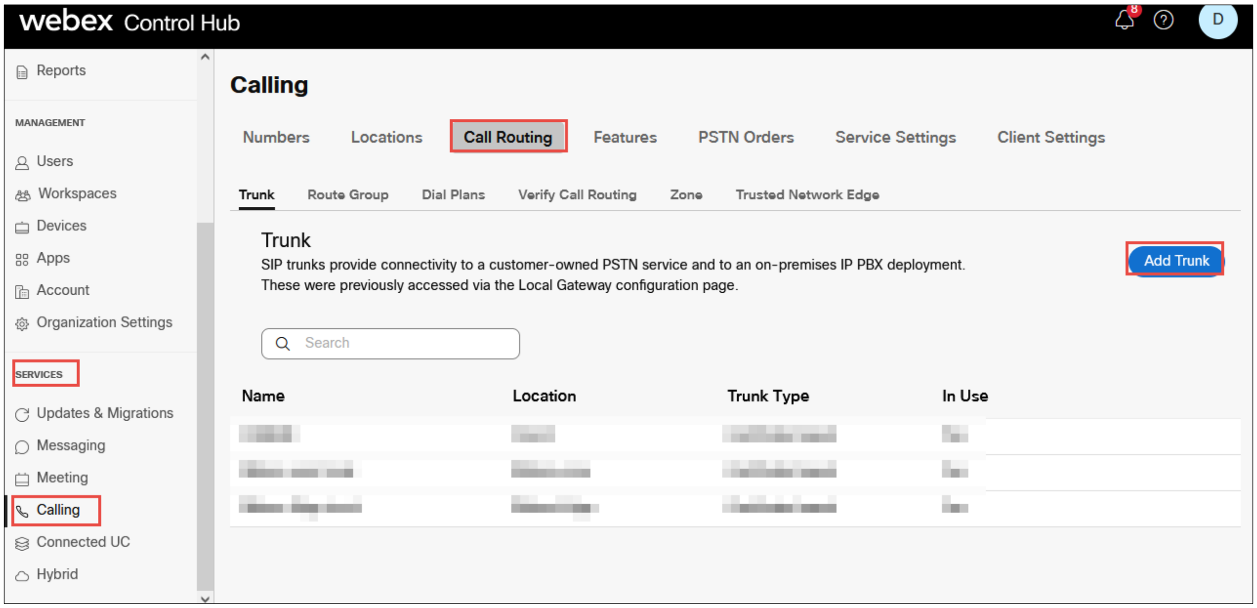
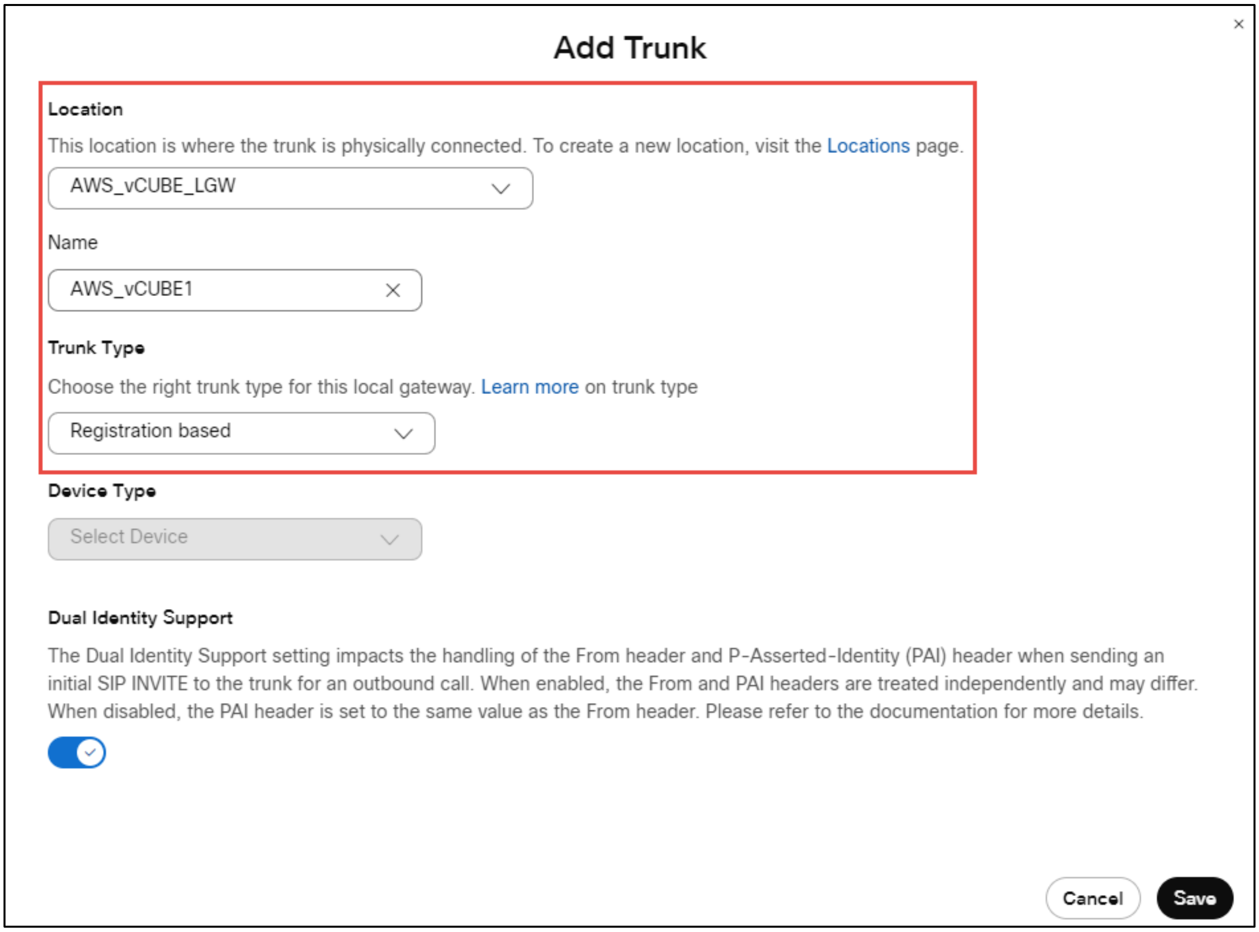


Figure 7: Add Trunk details Contd.,


Add Trunk
Location
This location is where the trunk is physically connected. To create a new location, visit the Locations page.
AWS_vCUBE_LGW
Name
AWS_vCUBE1
Trunk Type
Choose the right trunk type for this local gateway. Learn more on trunk type
Registration based
Device Type
Select Device
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

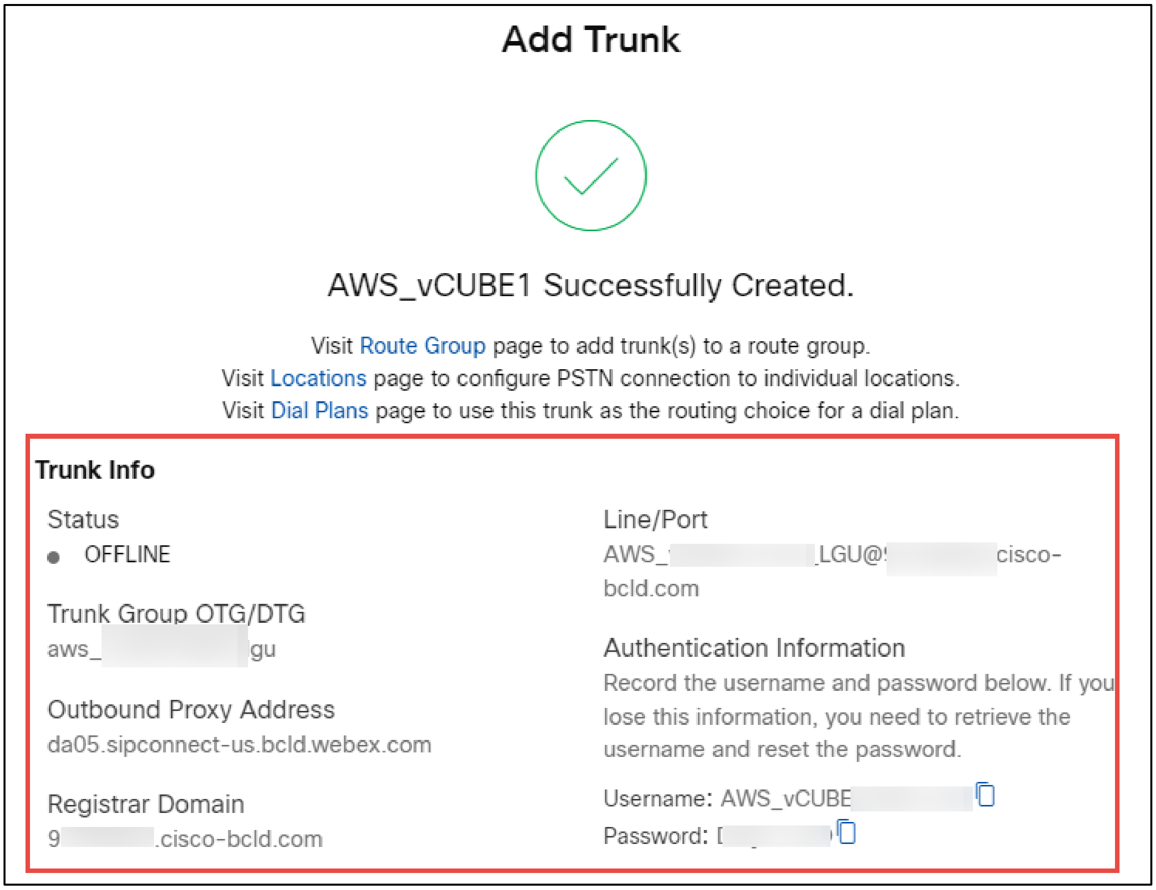


Figure 8: Add Trunk details Contd.

Step 6:
Choose the location and select Manage in PSTN Connection to add Connection type.

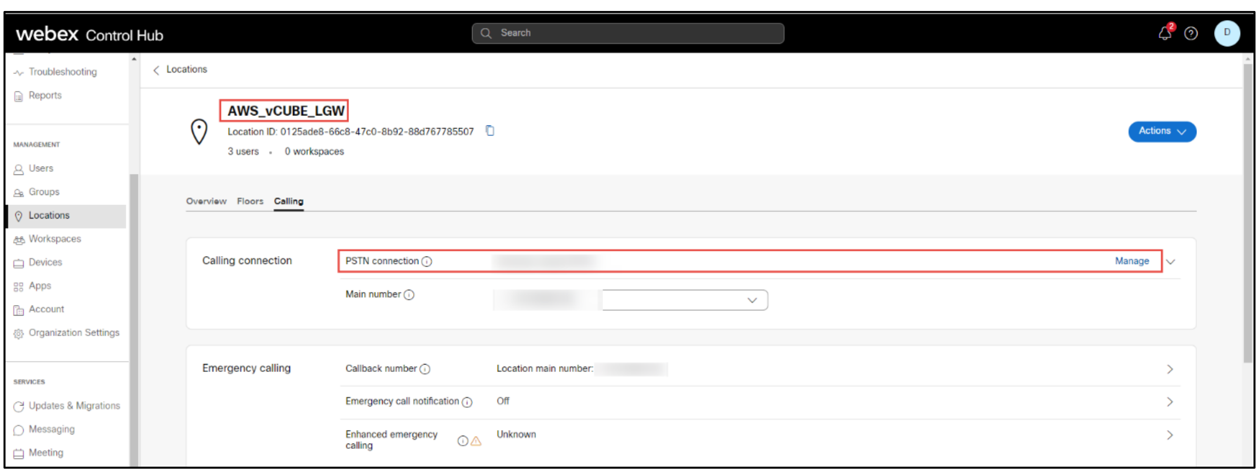


Figure 9:PSTN Connection

Step 7:

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

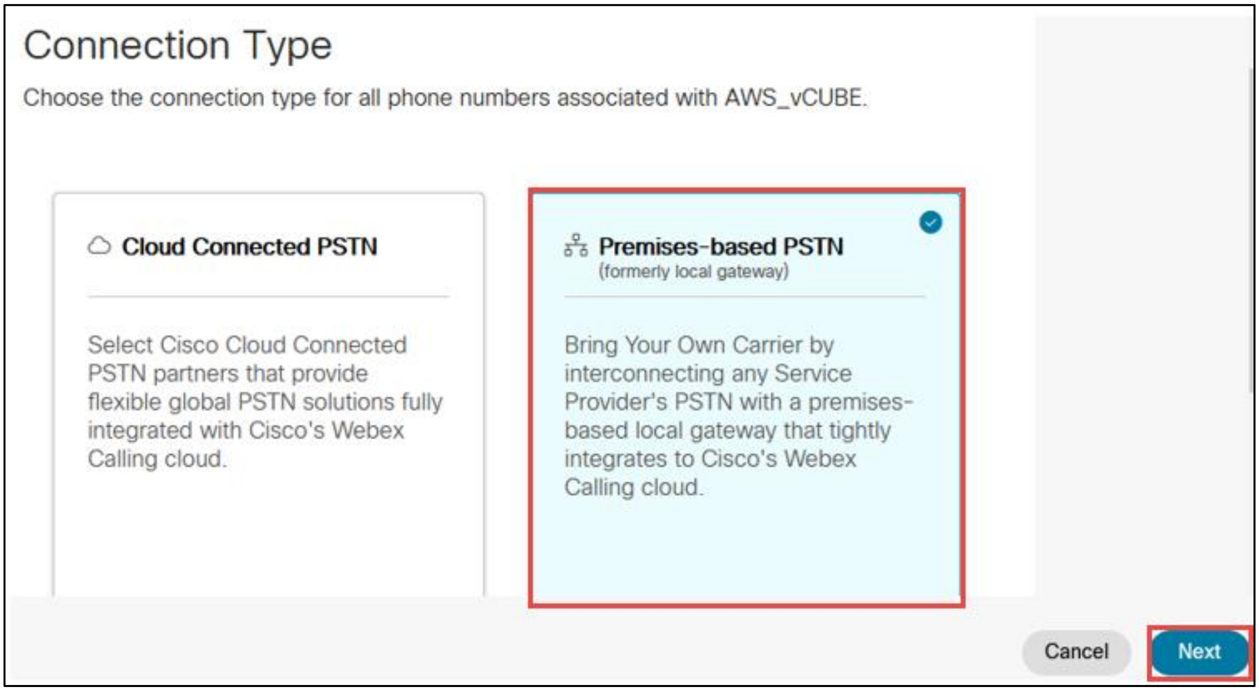


Figure 10: PSTN Connection Contd.,

Step 8:

Select the SIP trunk created earlier and click on Save

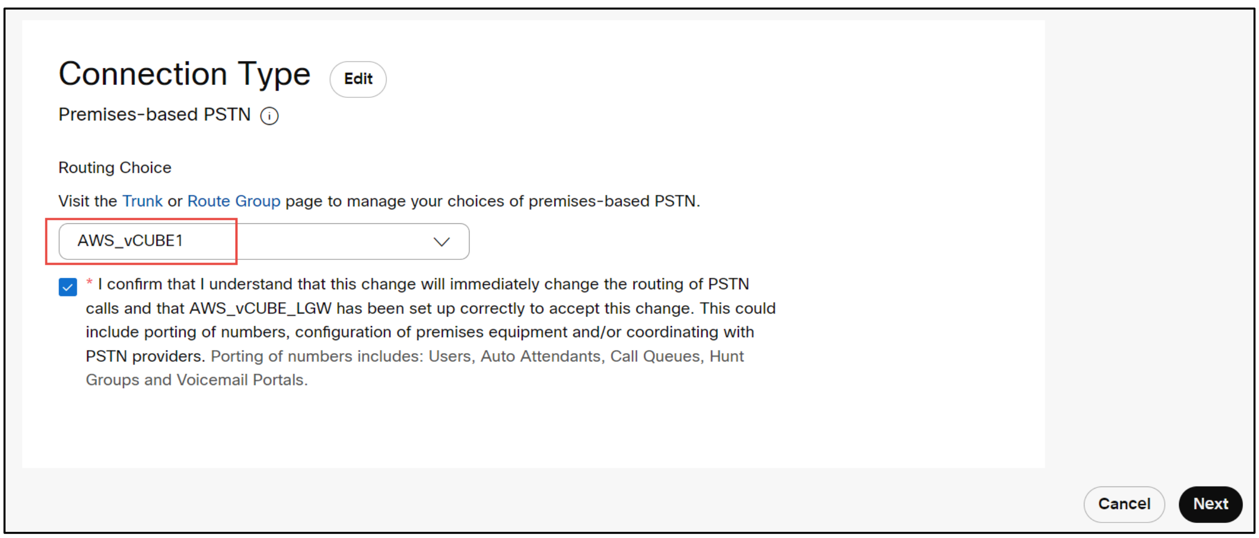


Figure 11: PSTN Connection Contd.,

Step 9:
Select the **Numbers**, Click on **Manage** and choose **Add**. Select the **Location** and **PSTN Connection**

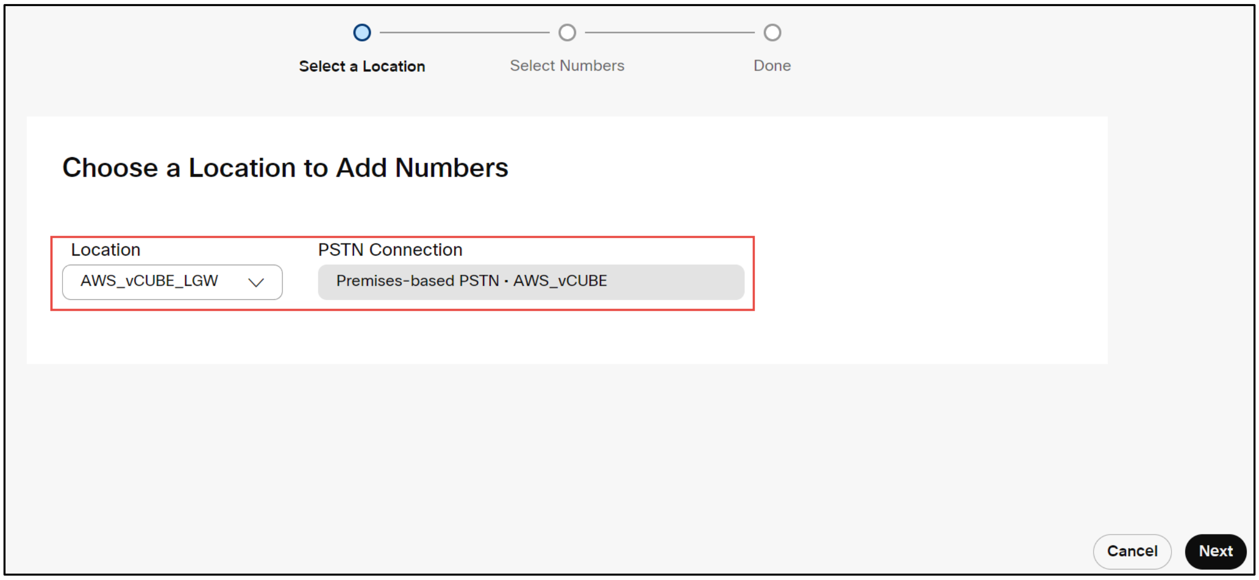


Figure 12: Add Numbers

Step 10:
Add the phone numbers provided by service provider and complete the wizard.

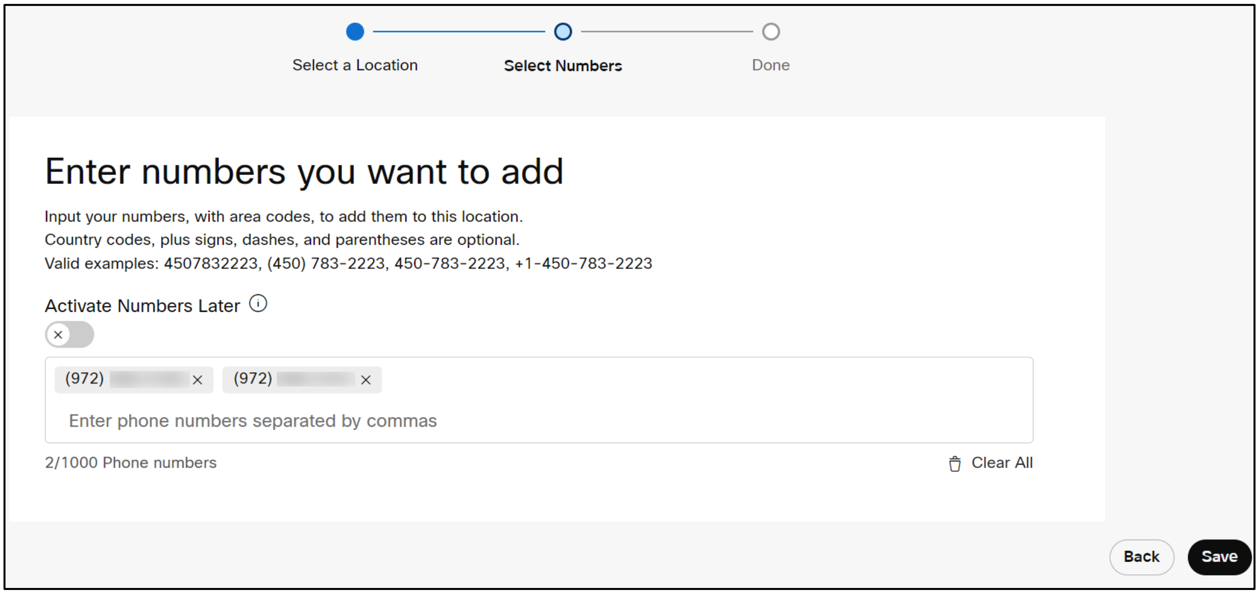


Figure 13: Add Numbers Contd.,

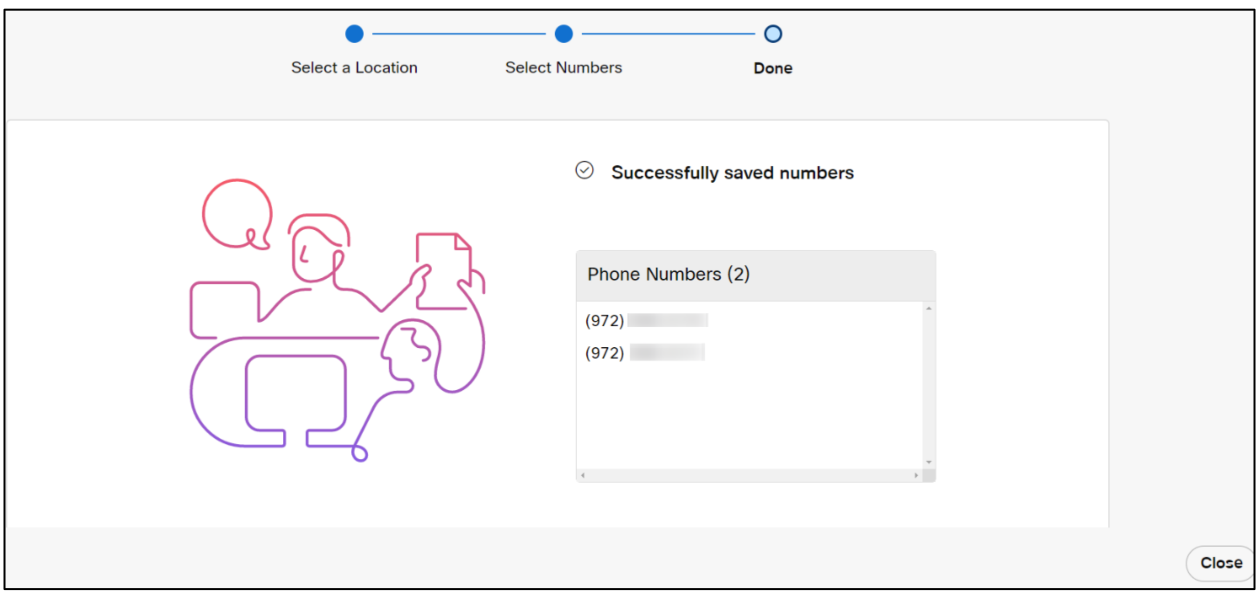


Figure 14: Add Numbers Contd.,

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.

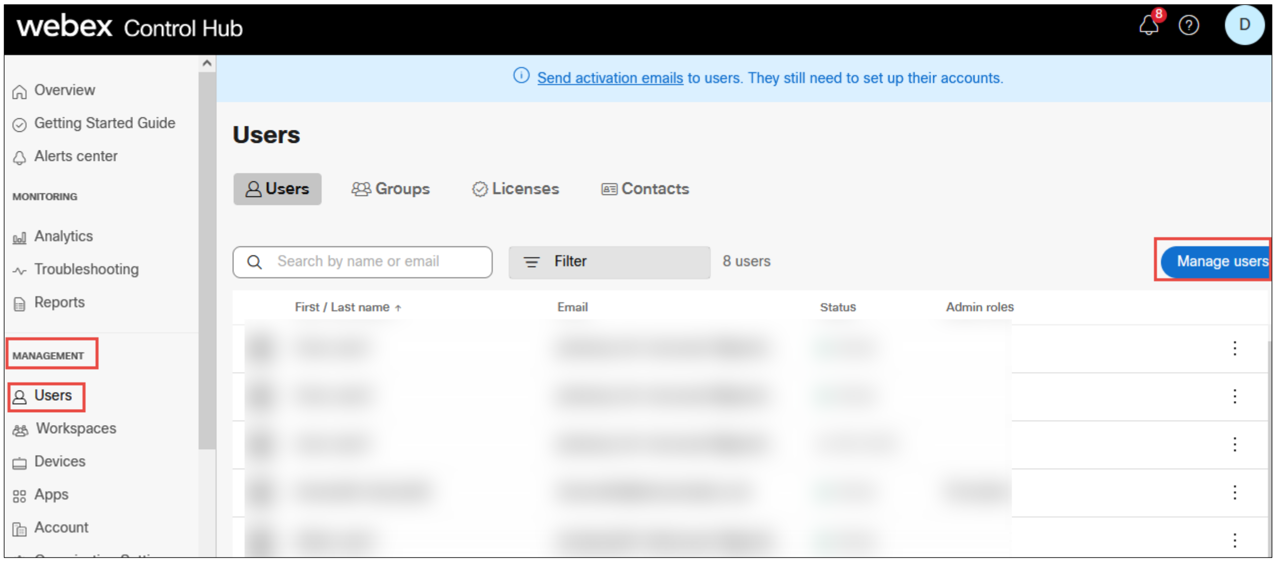


Figure 15: Adding Users

Step 2:

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

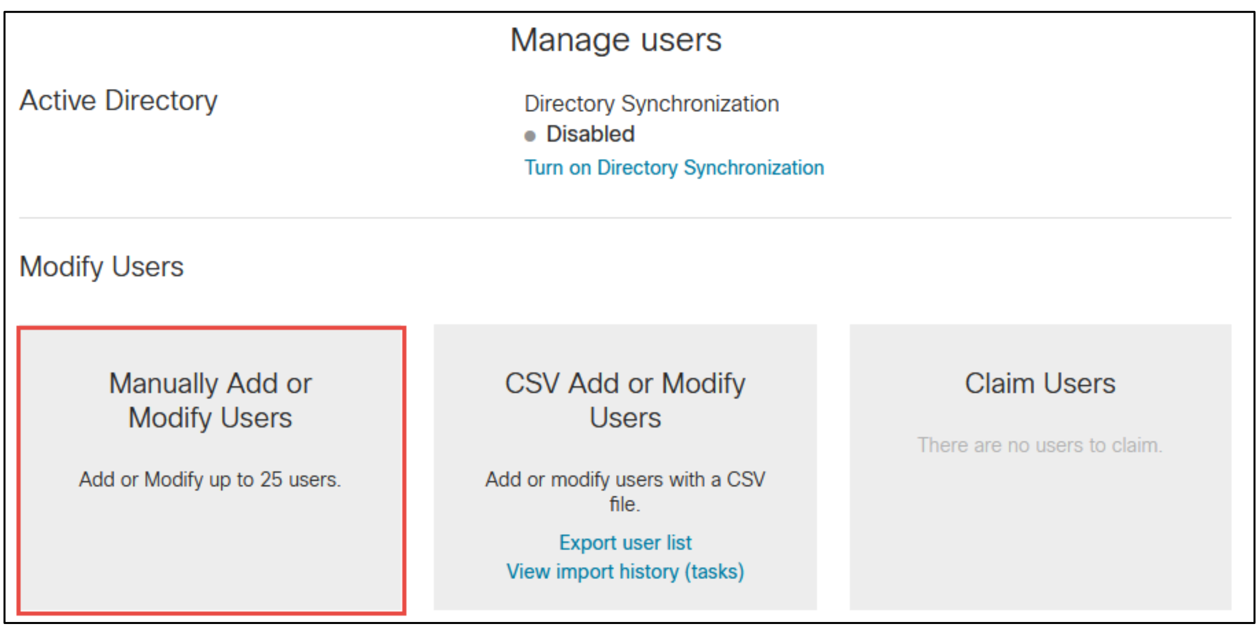


Figure 16: Manually Add or Modify Users

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.**

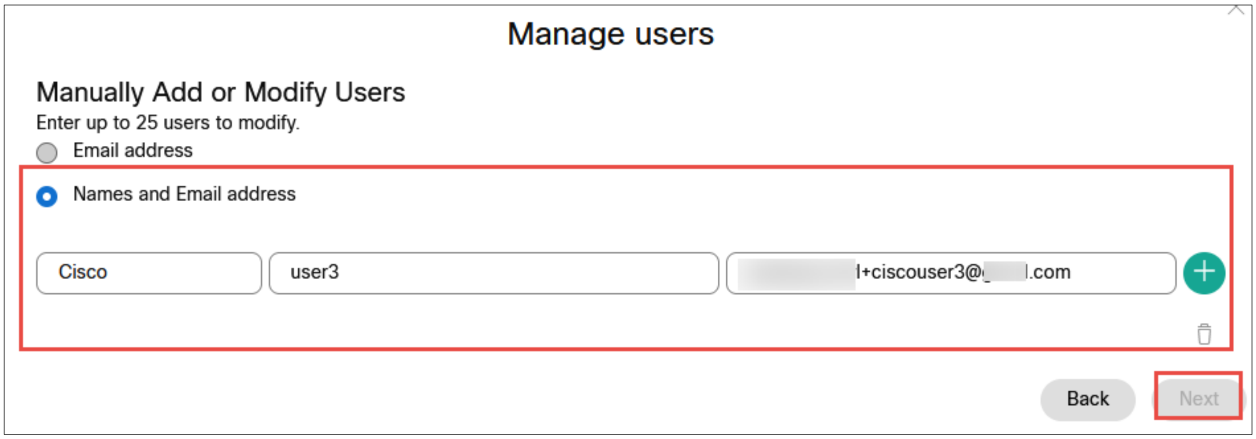


Figure 17: Adding email address and name.

Step 4:

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

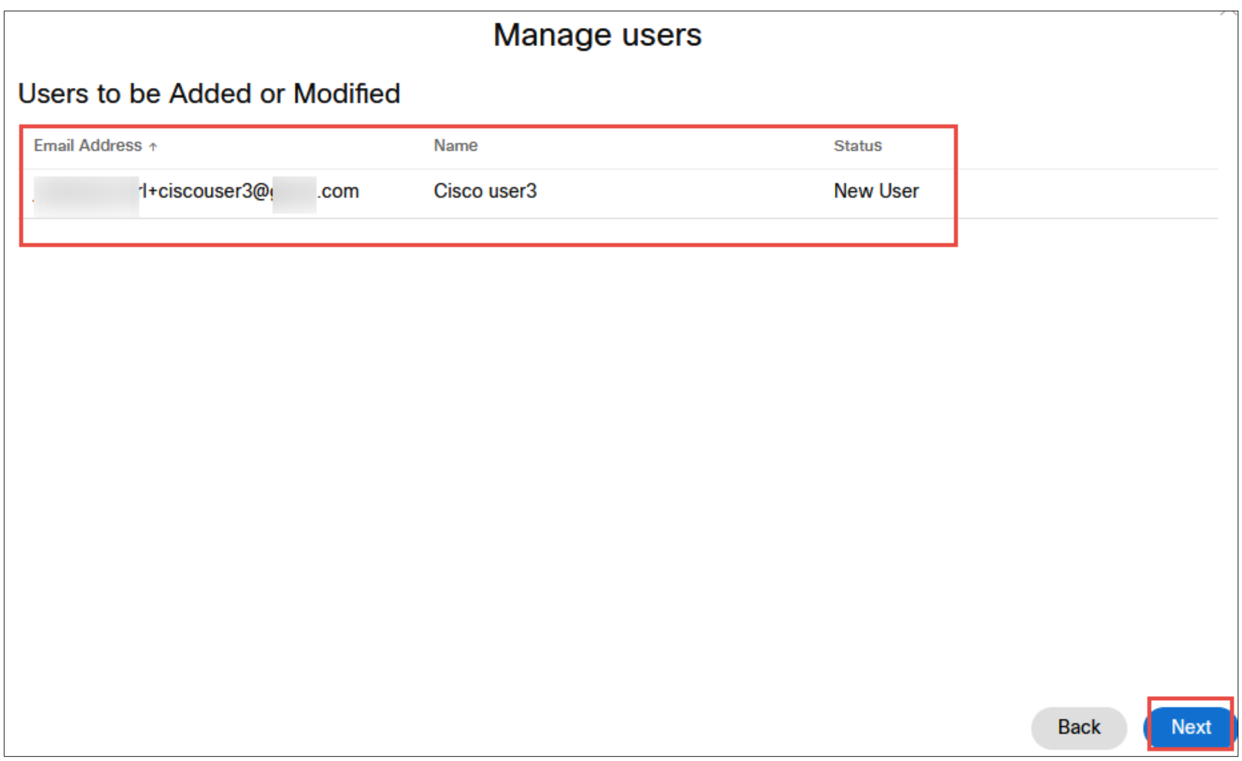


Figure 18: Confirm Adding

Step 5:

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

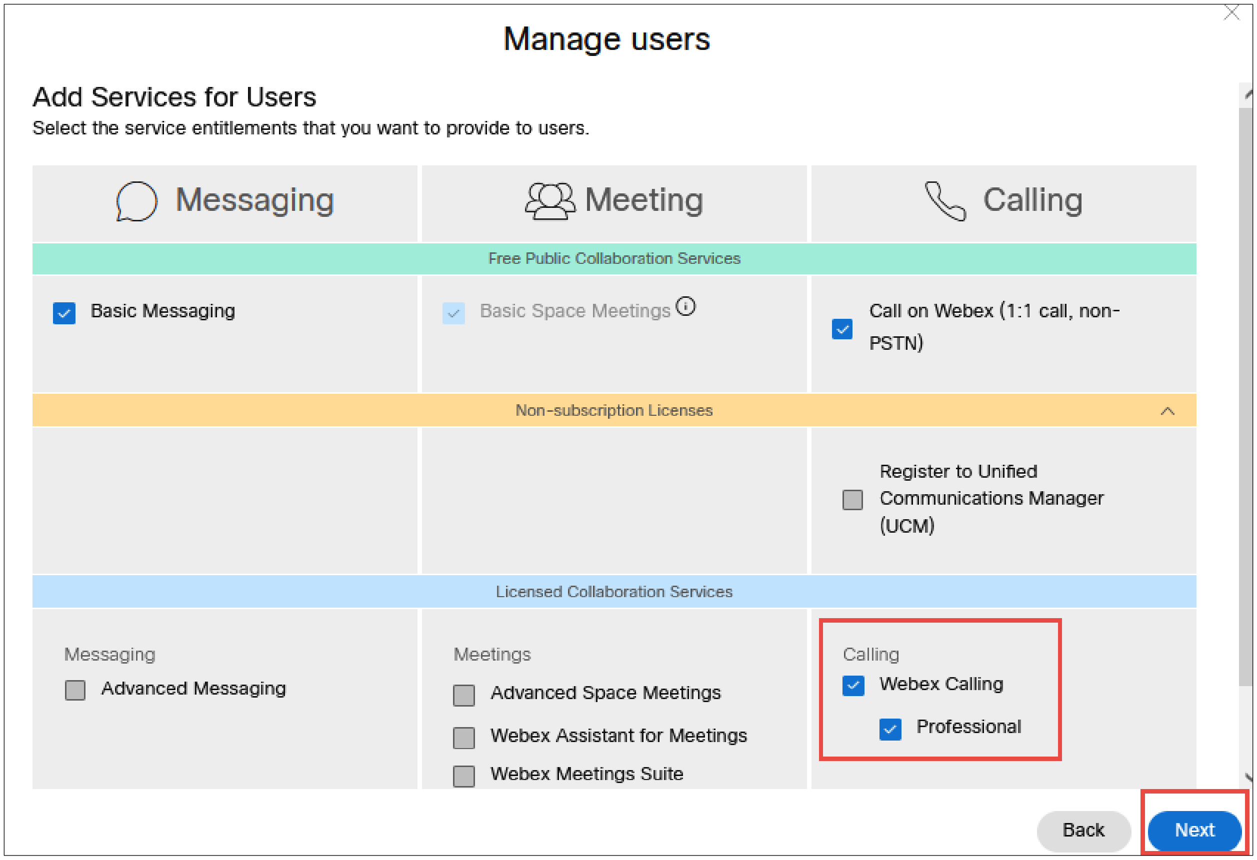


Figure 19: Add Services for Users

Step 6:

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

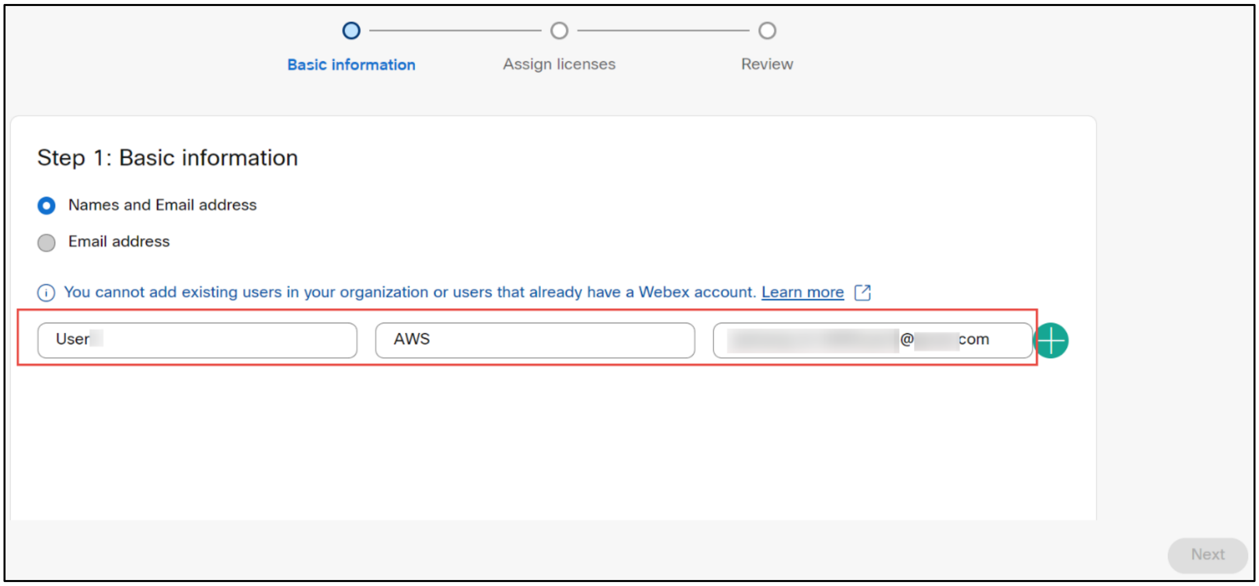


Figure 20: Assign Numbers

Step 7:

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

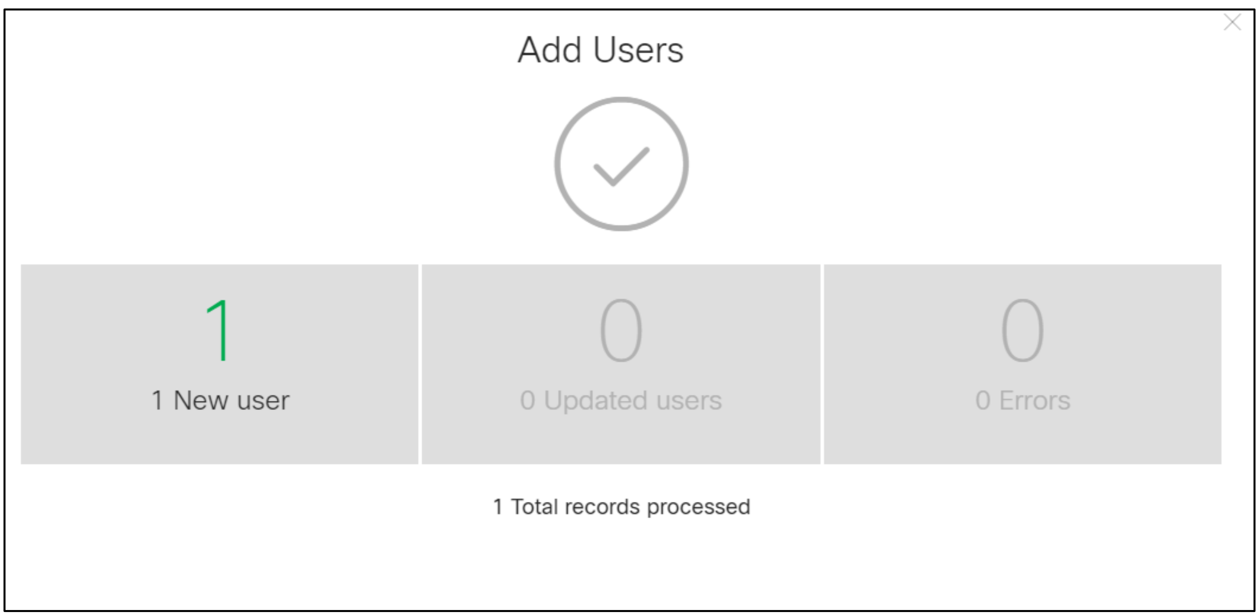


Figure 21: Add User successful.

Repeat the same steps in another Webex tenant for Multi tenancy setup.

2 Deploying vCUBE on AWS

Step 1:
Login to AWS console using the URL **https://console.aws.amazon.com/** . Expand **Instances**, click on **instances** and click on **Launch instances**

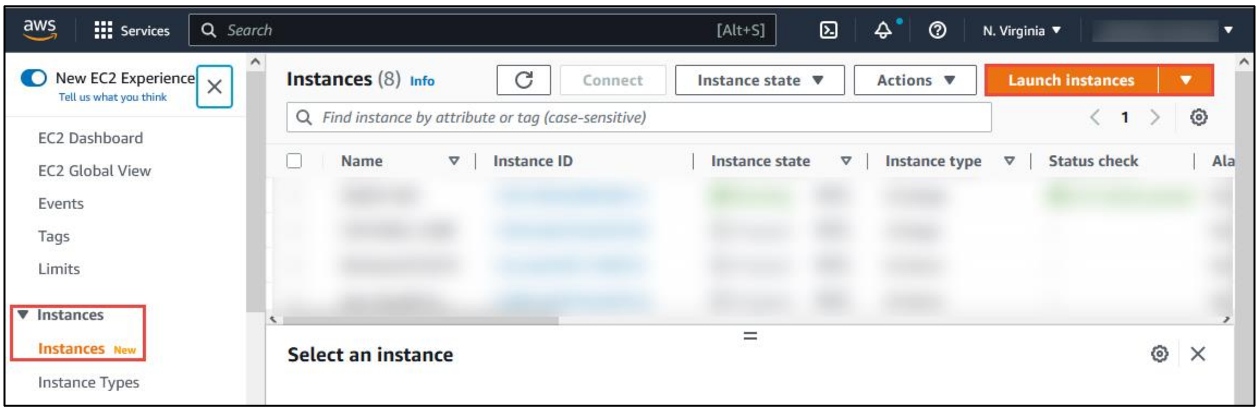


Figure 22: Launch Instance

Step 2:
Enter the **Name and Tags** for the instance

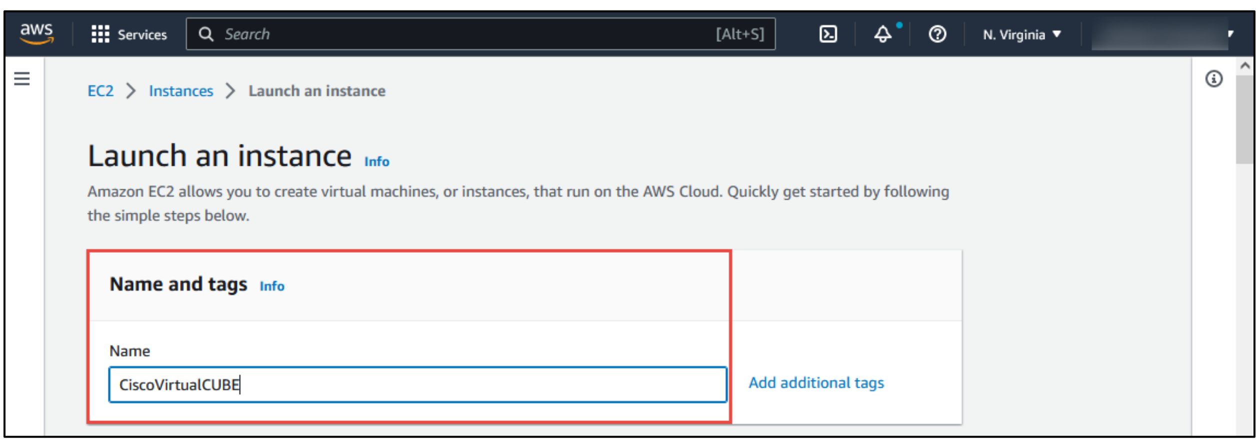


Figure 23: Name and Tags

Step 3:
In the **Application and OS Images (Amazon Machine Image)** section click on **Browse more AMIs**

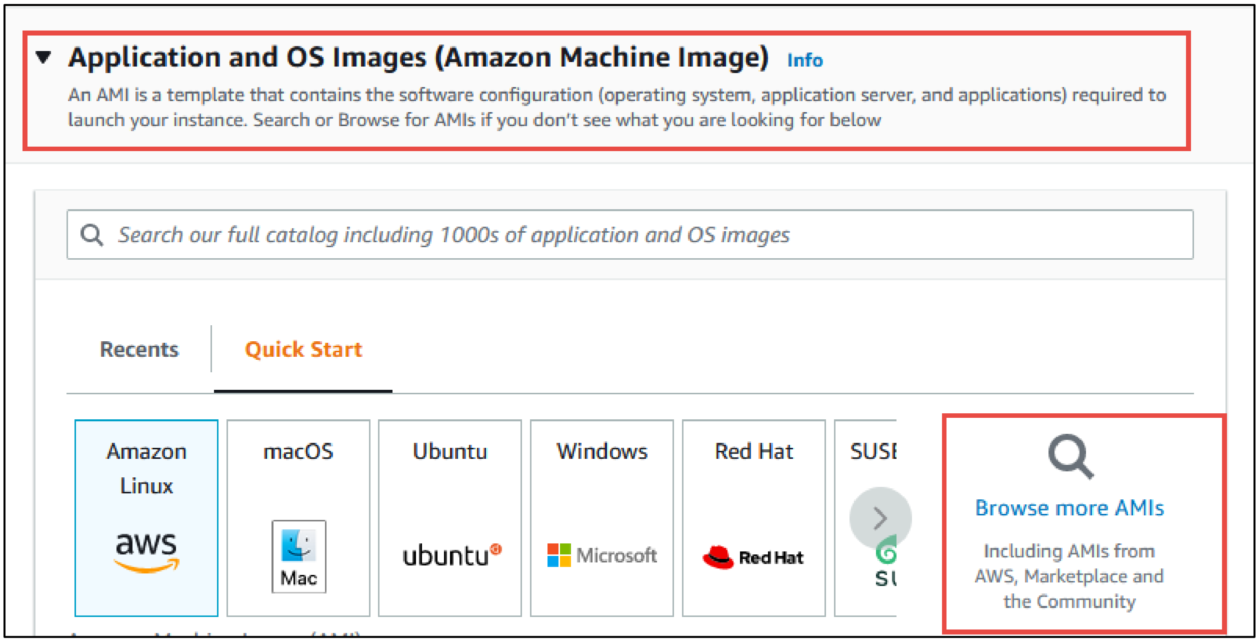


Figure 24: Browsing AMIs

Step 4:
In the search box query for **“Cisco-vCUBE”** and **select** the required image for **vCUBE** and click on **Continue**

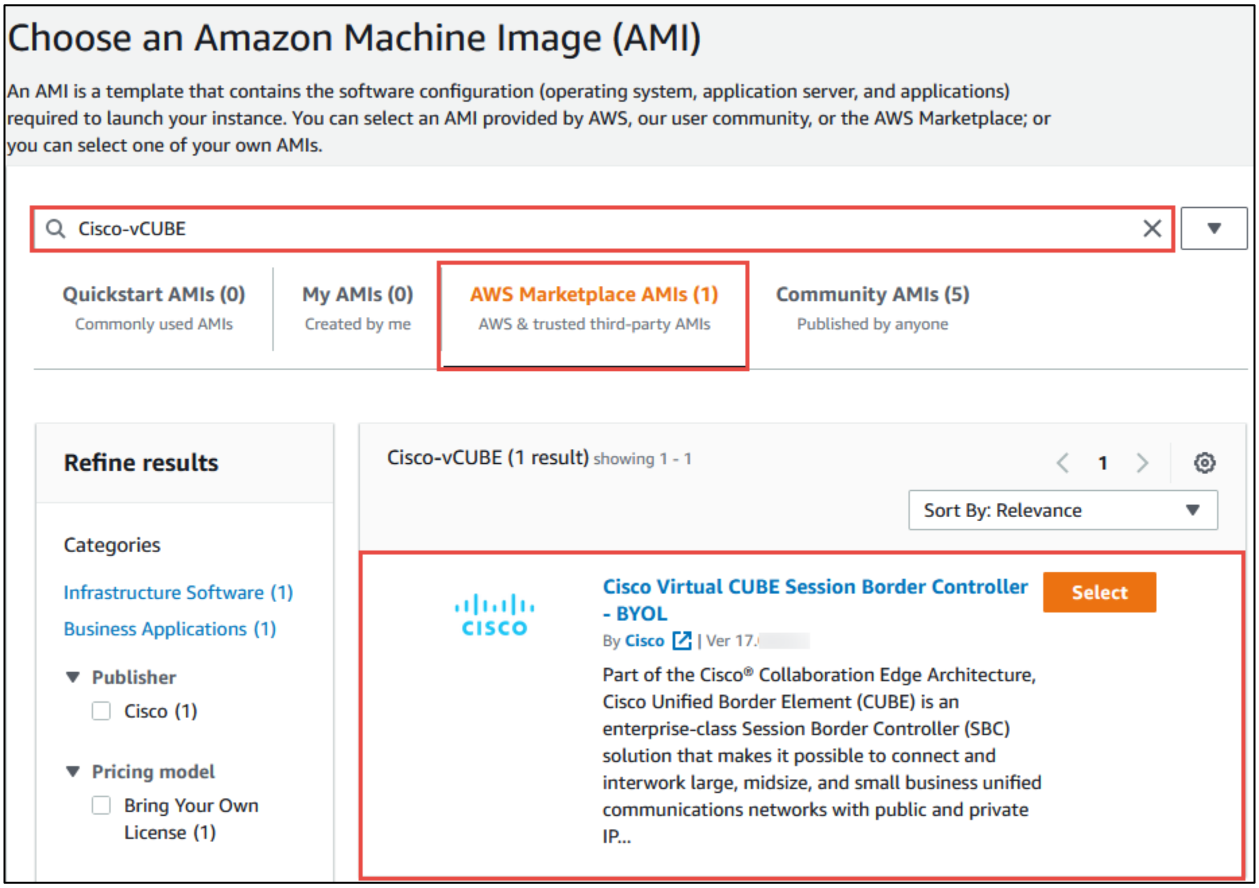


Figure 25: Selecting AMI

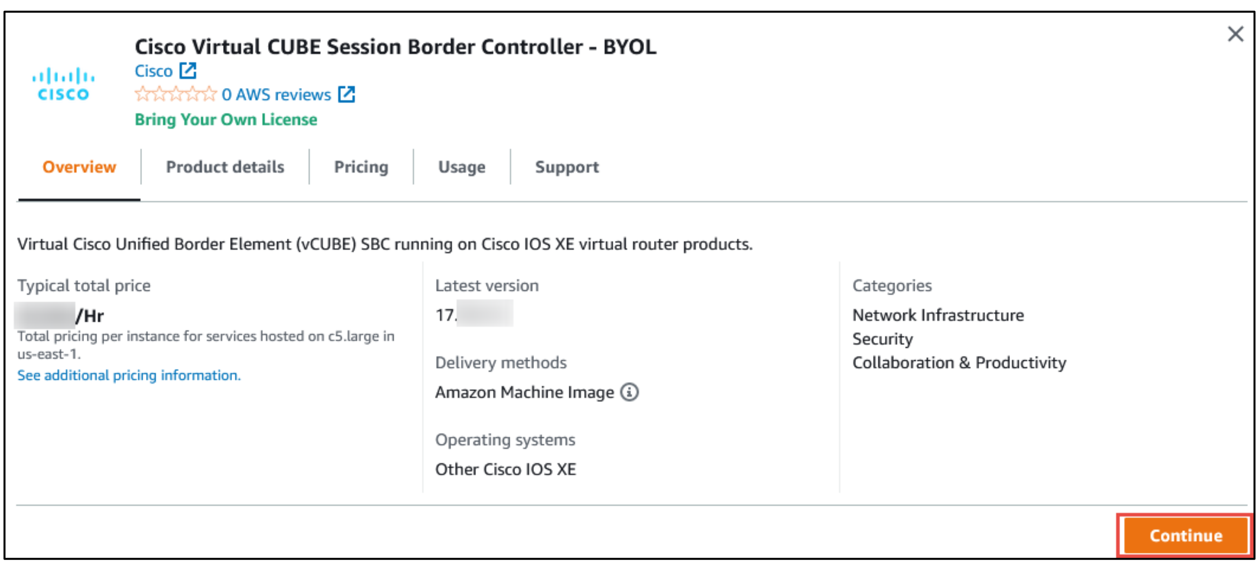


Figure 26: Selecting AMI Contd.,

Step 5:
Selected **Cisco-vCUBE** AMI will appear under the section **AMI from catalog** with the details

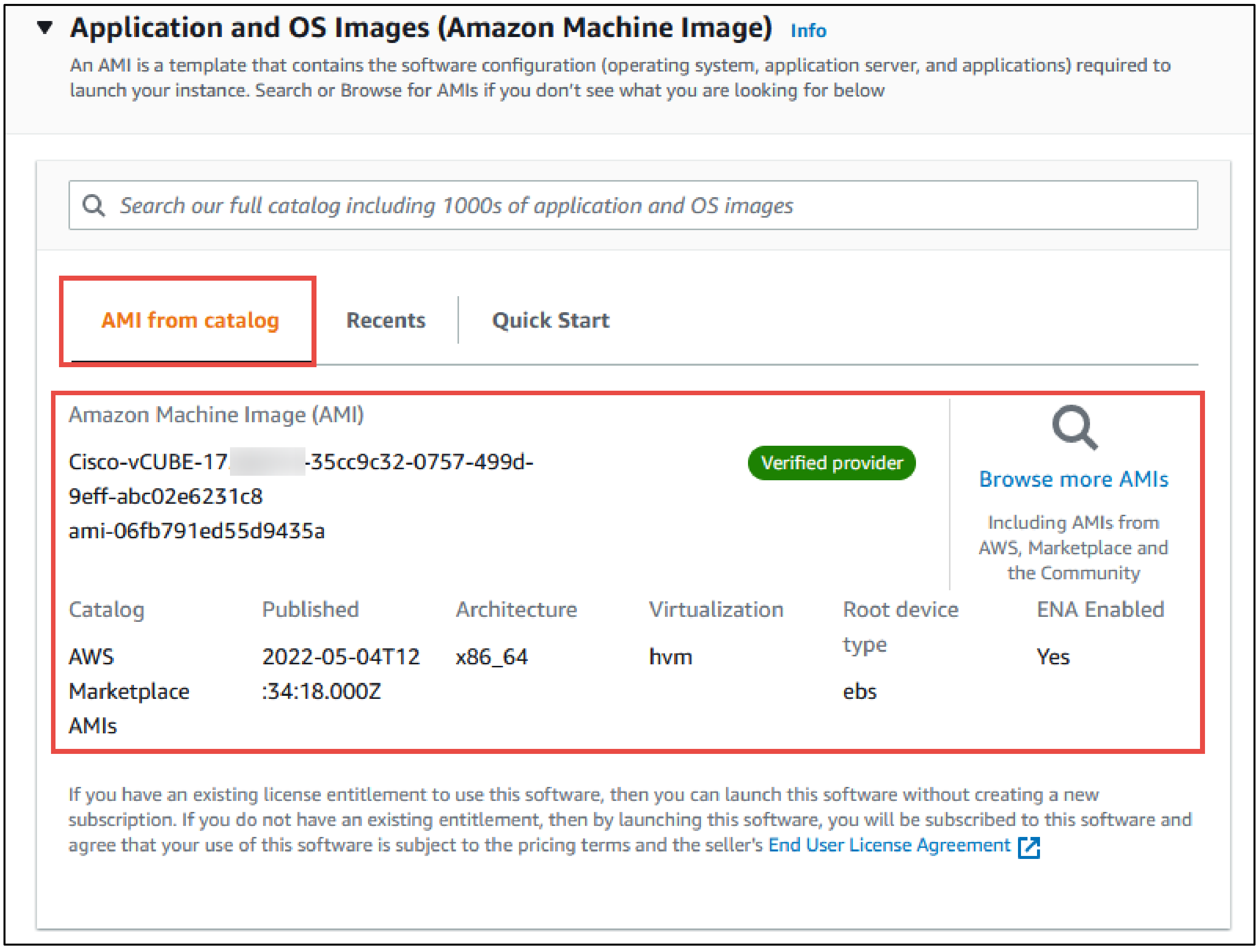


Figure 27: Verifying the selected AMI

Step 6:
Instance type will be auto populated based on the chosen AMI. Choose the existing **Key pair** or create a new key pair to access the instance

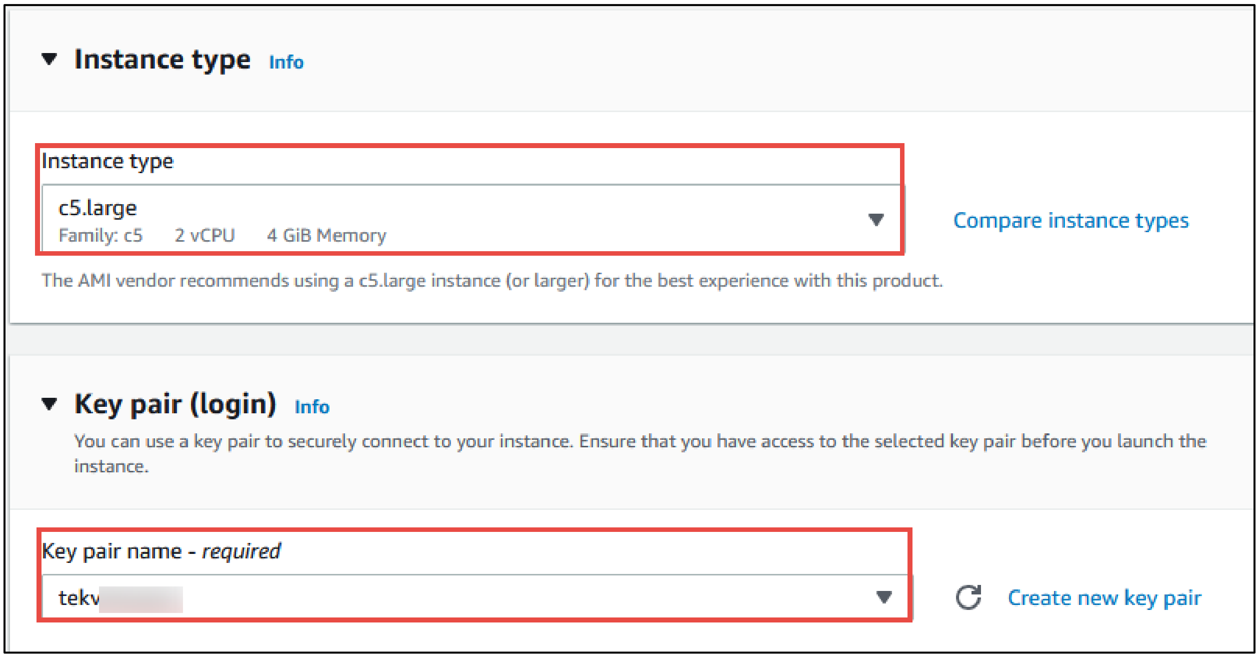


Figure 28: Instance Type and Key Pair

Step 7:
In the **Network Settings** choose **VPC** and **Subnet** as defined for the network to host vCUBE. **Security Group name** will be auto created while deploying the image

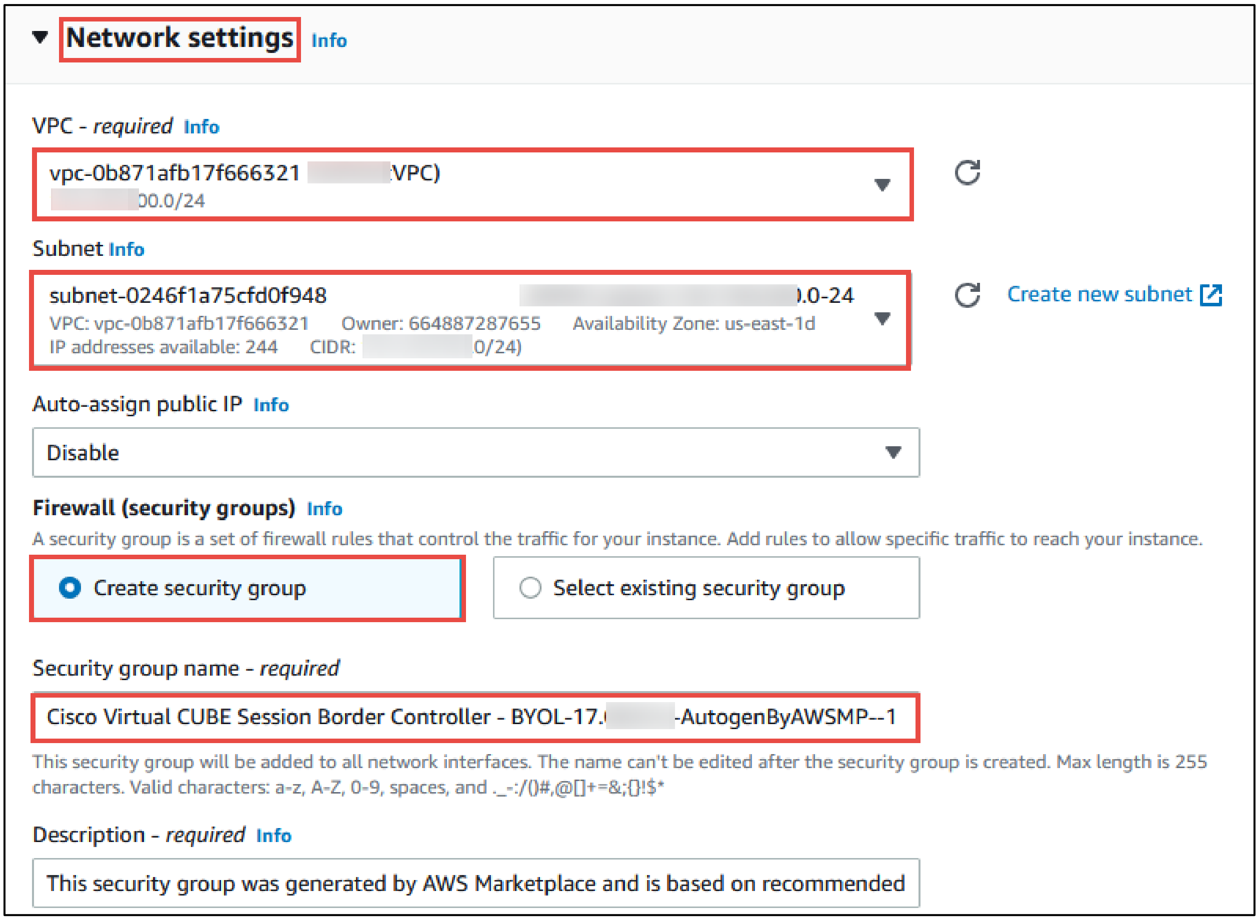


Figure 29: Network Settings

Step 8:
In the **Inbound Security Groups rules** section define the rules as per the requirement to access the instance and leave the values to default or customize the configuration in the **Advanced network configuration** based on the requirement

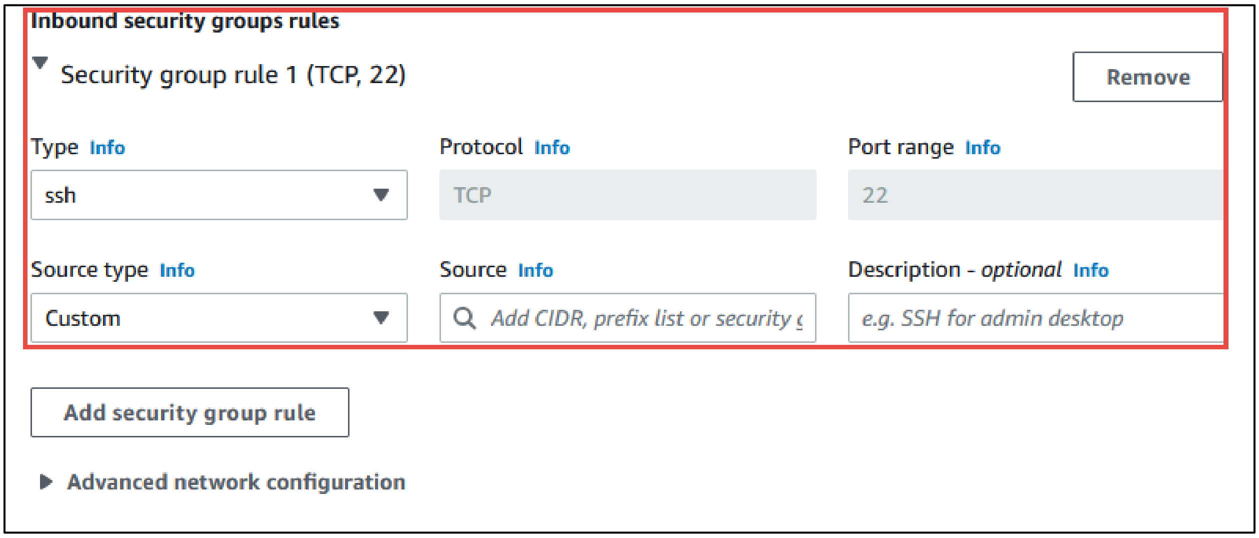


Figure 30: Inbound Security Group Rules

Step 9:
In the **Configure Storage** leave the settings to default

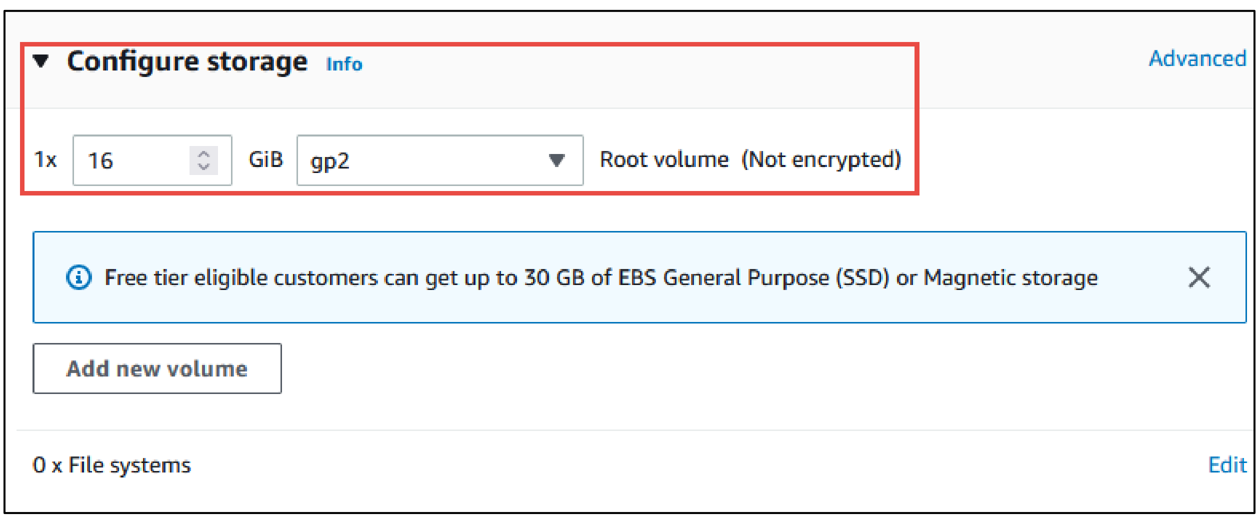


Figure 31: Storage configuration

Step 10:
In the **Summary** section review the detail and click on **Launch instance**. vCUBE will be running as an EC2 instance in AWS after a successful launch

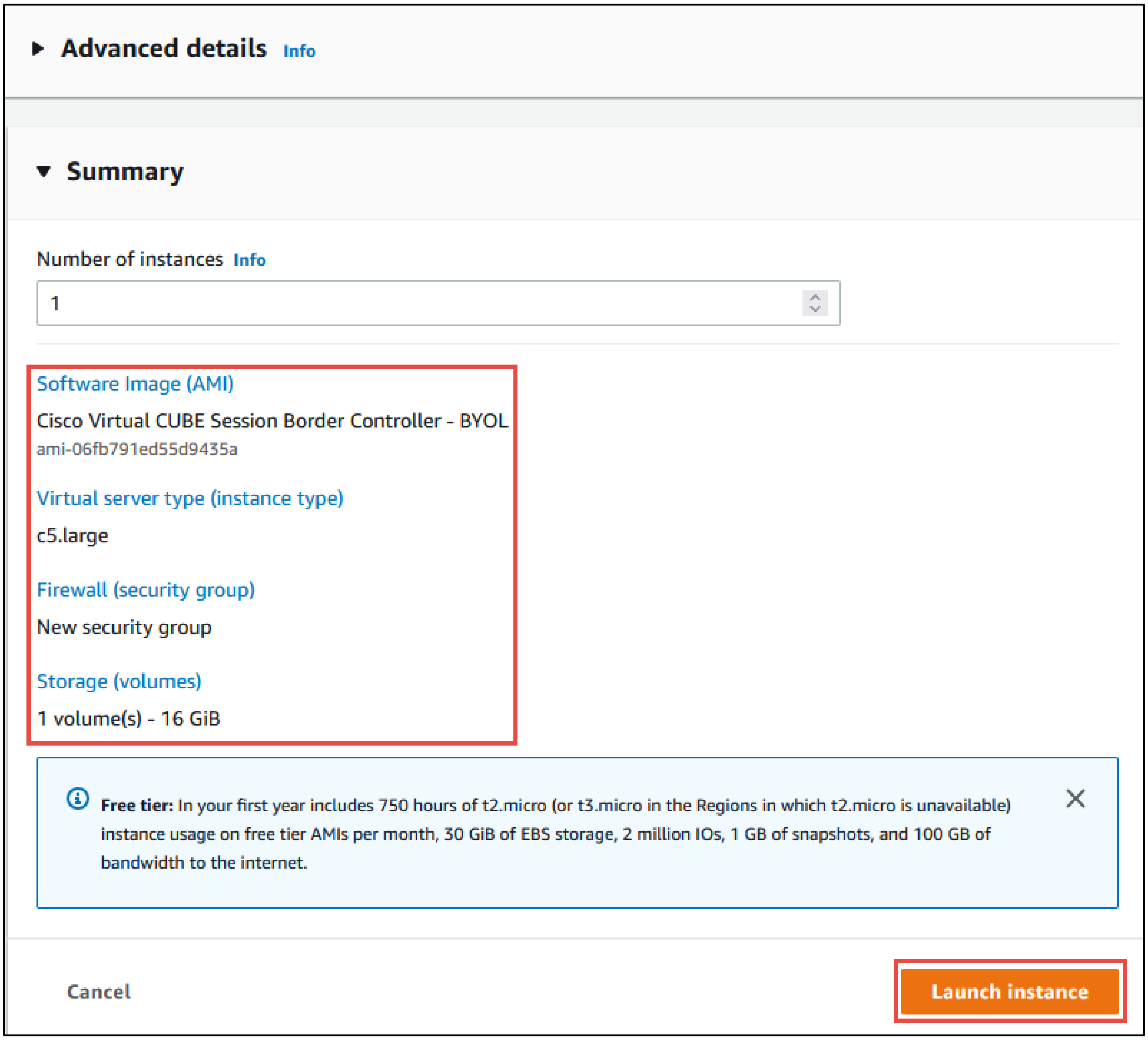


Figure 32: Summary and Launch instance

3 Configuring Cisco Unified Border Element

Global vCUBE settings

In order to enable vCUBE IP2IP SBC functionality, following command must be entered:

```
voice service voip
 ip address trusted list
  ipv4 23.89.76.128 255.255.255.128
  ipv4 128.177.14.0 255.255.255.0
  ipv4 139.177.64.0 255.255.248.0
  ipv4 170.72.242.0 255.255.255.0
  ipv4 170.72.17.128 255.255.255.128
  ipv4 199.19.196.0 255.255.254.0
  ipv4 23.89.33.0 255.255.255.0
  ipv4 23.89.154.0 255.255.255.128
  ipv4 128.177.36.0 255.255.255.0
  ipv4 139.177.72.0 255.255.254.0
  ipv4 150.253.209.128 255.255.255.128
  ipv4 170.72.82.0 255.255.255.128
  ipv4 199.19.199.0 255.255.255.0
  ipv4 23.89.40.0 255.255.255.128
  ipv4 85.119.56.0 255.255.254.0
  ipv4 135.84.168.0 255.255.248.0
  ipv4 170.72.29.0 255.255.255.0
  ipv4 185.115.196.0 255.255.252.0
  ipv4 199.59.64.0 255.255.248.0
  ipv4 170.72.0.128 255.255.255.128
  ipv4 XX.XX.79.250 255.255.255.255
  ipv4 XX.XX.235.70
 address-hiding
 mode border-element
 media bulk-stats
 allow-connections sip to sip
 no supplementary-service sip refer
 no supplementary-service sip handle-replaces
 fax protocol pass-through g711ulaw
 trace
 sip
  early-offer forced
```

```
  midcall-signaling passthru
  privacy-policy passthru
  g729 annexb-all
  sip-profiles inbound
```

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
early-offer forced	Forces LGW to send the SDP information in the initial INVITE message
g729 annexb-all	Allows all variants of G729

Codecs

G711u-Law and G729 voice codecs are configured for this testing. Codec preferences used to change according to the test plan description.

```
voice class codec 1
codec preference 2 g711ulaw
 codec preference 1 g729br8
```

IP Networking

```
interface GigabitEthernet1
 ip address dhcp
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
```

Routing

IP route is used to route calls to Webex and PSTN Lumen.

```
ip route 0.0.0.0 0.0.0.0 172.31.26.1
```

DNS Servers

DNS must be configured to resolve addresses for Webex Calling

```
ip name-server 8.8.8.8
```

Message Handling Rules

Manipulations for outbound messages to Webex calling tenant 1

```
voice class sip-profiles 200
 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 11 request ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 20 request ANY sip-header From modify ">" ";otg=aws_XXXX_lgu>"
 rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
 rule 31 request ANY sdp-header Connection-Info modify "172.31.26.74" "XX.228.235.70"
 rule 32 request ANY sdp-header Session-Owner modify "IN IP4 172.31.26.74" "IN IP4
XX.228.235.70"
 rule 33 request ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
172.31.26.74 (.*)" "a=candidate:1 1\1 XX.228.235.70 \2"
 rule 34 request ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
172.31.26.74 (.*)" "a=candidate:1 2\1 XX.228.235.70 \2"
 rule 35 response ANY sdp-header Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 36 response ANY sdp-header Session-Owner modify "IN IP4 172.31.26.74" "IN IP4
XX.228.235.70"
 rule 37 response ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
172.31.26.74 (.*)" "a=candidate:1 1\1 XX.228.235.70 \2"
 rule 38 response ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
172.31.26.74 (.*)" "a=candidate:1 2\1 XX.228.235.70 \2"
 rule 40 response ANY sdp-header Audio-Connection-Info modify "172.31.26.74"
"XX.228.235.70"
```

```
 rule 41 request ANY sdp-header Audio-Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 42 response ANY sdp-header Audio-Connection-Info modify "172.31.26.74"
"XX.228.235.70"
```

Manipulations for outbound messages to Webex calling tenant 2

```
voice class sip-profiles 500
 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 11 request ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 20 request ANY sip-header From modify ">" ";otg=aws_XXXX_lgu>"
 rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)" "sip:\1"
 rule 31 request ANY sdp-header Connection-Info modify "172.31.26.74" "XX.228.235.70"
 rule 32 request ANY sdp-header Session-Owner modify "IN IP4 172.31.26.74" "IN IP4
XX.228.235.70"
 rule 33 request ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
172.31.26.74 (.*)" "a=candidate:1 1\1 XX.228.235.70 \2"
 rule 34 request ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
172.31.26.74 (.*)" "a=candidate:1 2\1 XX.228.235.70 \2"
 rule 35 response ANY sdp-header Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 36 response ANY sdp-header Session-Owner modify "IN IP4 172.31.26.74" "IN IP4
XX.228.235.70"
 rule 37 response ANY sdp-header Audio-Attribute modify "a=candidate:1 1(.*)
172.31.26.74 (.*)" "a=candidate:1 1\1 XX.228.235.70 \2"
 rule 38 response ANY sdp-header Audio-Attribute modify "a=candidate:1 2(.*)
172.31.26.74 (.*)" "a=candidate:1 2\1 XX.228.235.70 \2"
 rule 40 response ANY sdp-header Audio-Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 41 request ANY sdp-header Audio-Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 42 response ANY sdp-header Audio-Connection-Info modify "172.31.26.74"
"XX.228.235.70"
```

Manipulations for outbound messages to Lumen

```
voice class sip-profiles 100
 rule 1 request ANY sip-header Contact modify "@.*:" "@XX.228.235.70:"
```

```
 rule 2 response ANY sip-header Contact modify "@.*:" "@XX.228.235.70:"
 rule 4 request ANY sip-header P-Asserted-Identity modify "@.*>" "@XX.228.235.70>"
 rule 5 response ANY sip-header P-Asserted-Identity modify "@.*>" "@XX.228.235.70>"
 rule 6 response ANY sdp-header Audio-Connection-Info modify "172.31.26.74" "XX.228.235.70"
 rule 7 request ANY sdp-header Audio-Connection-Info modify "172.31.26.74" "XX.228.235.70"
 rule 8 request ANY sdp-header Connection-Info modify "172.31.26.74" "XX.228.235.70"
 rule 9 response ANY sdp-header Connection-Info modify "172.31.26.74" "XX.228.235.70"
 rule 10 request ANY sdp-header Session-Owner modify "IN IP4 172.31.26.74" "IN IP4 XX.228.235.70"
 rule 11 response ANY sdp-header Session-Owner modify "IN IP4 172.31.26.74" "IN IP4 XX.228.235.70"
 rule 12 request ANY sip-header Via modify "172.31.26.74:5060" "XX.228.235.70:5060"
 rule 13 request INVITE sip-header Diversion modify "@.*>" "@XX.228.235.70>"
```

Manipulations for inbound messages from Lumen

```
voice class sip-profiles 222
 rule 200 request ANY sip-header To copy "sip:(.*)@" u01
 rule 201 request INVITE sip-header SIP-Req-URI modify "sip:(.*)@.*:(.*)" "sip:\1@172.31.26.74:\2"
 rule 202 request ACK sip-header SIP-Req-URI modify "sip:.*@(.*) (.*)" "sip:\u01@172.31.26.74:5060 \2"
 rule 203 request INVITE sip-header To modify "<sip:(.*)@.*>" "<sip:\1@172.31.26.74>"
```

SRTP crytpo

Used to set the crypto cipher for the Webex Calling

```
voice class srtp-crypto 200
 crypto 1 AES_CM_128_HMAC_SHA1_80
```

STUN ICE-lite

```
voice class stun-usage 200
 stun usage ice lite
```

Tenant

To Webex Calling tenant 1

```
voice class tenant 200
  registrar dns:XXXX.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
  credentials number AWS_XXXX_LGU username AWS_XXXX_LGU password 6 XXXXXX realm
Broadworks
  authentication username AWS_XXXX_LGU password 6 XXXXXX realm BroadWorks
  authentication username AWS_XXXX_LGU password 6 XXXXXX realm XXXX.cisco-bcld.com
  no remote-party-id
  sip-server dns:XXXX.cisco-bcld.com
  connection-reuse
  srtp-crypto 200
  session transport tcp tls
  url sips
  error-passthru
  asserted-id pai
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  no pass-thru content custom-sdp
  sip-profiles 200
  outbound-proxy dns:da05.sipconnect-us.bcld.webex.com
  privacy-policy passthru
```

To Webex Calling tenant 2

```
voice class tenant 500
  registrar dns:XXXX.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
  credentials number AWS_XXXX_LGU username AWS_XXXX_LGU password 6 XXXXXX realm
Broadworks
  authentication username AWS_XXXX_LGU password 6 XXXXXX realm BroadWorks
  authentication username AWS_XXXX_LGU password 6 XXXXXX realm XXXX.cisco-bcld.com
  no remote-party-id
  sip-server dns:XXXX.cisco-bcld.com
  connection-reuse
  srtp-crypto 200
  session transport tcp tls
  url sips
  error-passthru
```

```
  asserted-id pai
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  no pass-thru content custom-sdp
  sip-profiles 500
  outbound-proxy dns:da09.sipconnect-us.bcld.webex.com
  privacy-policy passthru
```

To Lumen

```
voice class tenant 100
  session transport udp
  url sip
  error-passthru
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  no pass-thru content custom-sdp
  sip-profiles 100
```

Number translation rules

To Lumen

```
voice translation-rule 1
 rule 1 /^0972\(.*\)/ /972\1/
 rule 2 /^\+1\(.*\)/ /\1/
 rule 3 /^\+91\(.*\)/ /01191\1/
voice translation-profile called
 translate called 1
```

Dial peer

Inbound calls from Cisco Webex Calling tenant 1

```
voice class uri 200 sip
 pattern dtg=aws_XXXX_lgu
!
dial-peer voice 200 voip
 description Incoming dial-peer from Webex Calling to vCUBE-AWS
 session protocol sipv2
```

```
 incoming uri request 200
 voice-class codec 1
 voice-class sip asserted-id pai
 voice-class stun-usage 200
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
```

Inbound calls from Cisco Webex Calling tenant 2

```
voice class uri 500 sip
 pattern dtg=aws_XXXX_lgu
!
dial-peer voice 500 voip
 description Incoming dial-peer from Webex Calling-2 to vCUBE-AWS
 session protocol sipv2
 incoming uri request 500
 voice-class codec 1
 voice-class stun-usage 200
 voice-class sip asserted-id pai
 voice-class sip tenant 500
 dtmf-relay rtp-nte
 srtp
 no vad
```

Outbound calls to Lumen

```
voice class e164-pattern-map 101
  e164 +121424259..
  e164 09725980...
  e164 +18.........
  e164 411
 !
dial-peer voice 101 voip
 description Outgoing dial-peer from vCUBE-AWS to PSTN
 translation-profile outgoing called
 session protocol sipv2
 session target ipv4:XX.XX.79.250:5060
 session transport udp
```

```
 destination e164-pattern-map 101
 voice-class codec 1
 voice-class sip asserted-id pai
 voice-class sip profiles 100
 voice-class stun-usage 200
 voice-class sip tenant 100
 voice-class sip options-keepalive
 dtmf-relay rtp-nte
 no vad
```

Inbound calls from Lumen

```
voice class uri 100 sip
 host ipv4:XX.XX.79.250
!
dial-peer voice 100 voip
 description Incoming dial-peer from PSTN to vCUBE-AWS
 session protocol sipv2
 session transport udp
 incoming uri via 100
 voice-class codec 1
 voice-class sip asserted-id pai
voice-class sip profiles 222 inbound
 voice-class stun-usage 200
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
```

Outbound calls to Cisco Webex Calling tenant 1

```
voice class e164-pattern-map 201
  e164 9725980XXX
 !
 dial-peer voice 201 voip
 description Outgoing dial-peer from vCUBE-AWS to Webex Calling
 session protocol sipv2
 session target sip-server
 session transport tcp tls
 destination e164-pattern-map 201
 voice-class codec 1
```

```
 voice-class sip asserted-id pai
 voice-class stun-usage 200
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
```

Outbound calls to Cisco Webex Calling tenant 2

```
voice class e164-pattern-map 501
  e164 9725980XXX
 !
 dial-peer voice 501 voip
 description Outgoing dial-peer from vCUBE-AWS to Webex Calling-2

 session protocol sipv2
 session target sip-server
 session transport tcp tls
 destination e164-pattern-map 501
 voice-class codec 1
 voice-class stun-usage 200
 voice-class sip asserted-id pai
 voice-class sip tenant 500
 dtmf-relay rtp-nte
 srtp
 no vad
```

Configuration example

The following configuration snippet contains a sample configuration of vCUBE with all parameters mentioned previously.

```
show running-config
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 console virtual
!
hostname vCUBE_LGW
!
boot-start-marker
boot system bootflash:c8000v-universalk9.17.09.02a.SPA.bin
boot-end-marker
!
vrf definition GS
 rd 100:100
 !
 address-family ipv4
 exit-address-family
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local none
!
aaa session-id common
!
ip name-server 8.8.8.8
ip domain lookup source-interface GigabitEthernet1
!
login on-success log
ipv6 unicast-routing
!
subscriber templating
!
Multilink bundle-name authenticated
!
password encryption aes
!
crypto pki trustpoint TP-self-signed-534146329
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-534146329
 revocation-check none
 rsakeypair TP-self-signed-534146329
```

```
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint dummyTp
 revocation-check crl
!
crypto pki certificate chain TP-self-signed-534146329
 certificate self-signed 01

crypto pki certificate chain SLA-TrustPoint
 certificate ca 01

crypto pki certificate chain dummyTp
!
crypto pki certificate pool
 cabundle nvram:ios_core.p7b
 cabundle nvram:ios.p7
voice service voip
 ip address trusted list
  ipv4 23.89.76.128 255.255.255.128
  ipv4 128.177.14.0 255.255.255.0
  ipv4 139.177.64.0 255.255.248.0
  ipv4 170.72.242.0 255.255.255.0
  ipv4 170.72.17.128 255.255.255.128
  ipv4 199.19.196.0 255.255.254.0
  ipv4 23.89.33.0 255.255.255.0
  ipv4 23.89.154.0 255.255.255.128
  ipv4 128.177.36.0 255.255.255.0
  ipv4 139.177.72.0 255.255.254.0
  ipv4 150.253.209.128 255.255.255.128
  ipv4 170.72.82.0 255.255.255.128
  ipv4 199.19.199.0 255.255.255.0
  ipv4 23.89.40.0 255.255.255.128
  ipv4 85.119.56.0 255.255.254.0
  ipv4 135.84.168.0 255.255.248.0
  ipv4 170.72.29.0 255.255.255.0
  ipv4 185.115.196.0 255.255.252.0
  ipv4 199.59.64.0 255.255.248.0
  ipv4 170.72.0.128 255.255.255.128
  ipv4 XX.XX.79.250 255.255.255.255
  ipv4 XX.XX.235.70
 address-hiding
 mode border-element
 media bulk-stats
 allow-connections sip to sip
 no supplementary-service sip refer
 no supplementary-service sip handle-replaces
 fax protocol pass-through g711ulaw
 trace
 sip
```

```
  early-offer forced
  midcall-signaling passthru
  privacy-policy passthru
  g729 annexb-all
  sip-profiles inbound
!
voice class uri 200 sip
 pattern dtg=aws_XXXX_lgu
!
voice class uri 100 sip
 host ipv4:XX.XX.79.250
!
voice class uri 500 sip
 pattern dtg=aws_XXXX_lgu
!
voice class codec 1
 codec preference 2 g711ulaw
 codec preference 1 g729br8
!
voice class stun-usage 200
 stun usage ice lite
!
voice class sip-profiles 200
 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 11 request ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>"
"<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 20 request ANY sip-header From modify ">" ";otg=aws_XXXX_lgu>"
 rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)"
"sip:\1"
 rule 31 request ANY sdp-header Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 32 request ANY sdp-header Session-Owner modify "IN IP4
172.31.26.74" "IN IP4 XX.228.235.70"
 rule 33 request ANY sdp-header Audio-Attribute modify "a=candidate:1
1(.*) 172.31.26.74 (.*)" "a=candidate:1 1\1 XX.228.235.70 \2"
 rule 34 request ANY sdp-header Audio-Attribute modify "a=candidate:1
2(.*) 172.31.26.74 (.*)" "a=candidate:1 2\1 XX.228.235.70 \2"
 rule 35 response ANY sdp-header Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 36 response ANY sdp-header Session-Owner modify "IN IP4
172.31.26.74" "IN IP4 XX.228.235.70"
 rule 37 response ANY sdp-header Audio-Attribute modify "a=candidate:1
1(.*) 172.31.26.74 (.*)" "a=candidate:1 1\1 XX.228.235.70 \2"
 rule 38 response ANY sdp-header Audio-Attribute modify "a=candidate:1
2(.*) 172.31.26.74 (.*)" "a=candidate:1 2\1 XX.228.235.70 \2"
 rule 40 response ANY sdp-header Audio-Connection-Info modify
"172.31.26.74" "XX.228.235.70"
```

```
 rule 41 request ANY sdp-header Audio-Connection-Info modify
"172.31.26.74" "XX.228.235.70"
 rule 42 response ANY sdp-header Audio-Connection-Info modify
"172.31.26.74" "XX.228.235.70"
!
voice class sip-profiles 222
 rule 200 request ANY sip-header To copy "sip:(.*)@" u01
 rule 201 request INVITE sip-header SIP-Req-URI modify
"sip:(.*)@.*:(.*)" "sip:\1@172.31.26.74:\2"
 rule 202 request ACK sip-header SIP-Req-URI modify "sip:.*@(.*) (.*)"
"sip:\u01@172.31.26.74:5060 \2"
 rule 203 request INVITE sip-header To modify "<sip:(.*)@.*>"
"<sip:\1@172.31.26.74>"
!
voice class sip-profiles 100
 rule 1 request ANY sip-header Contact modify "@.*:" "@XX.228.235.70:"
 rule 2 response ANY sip-header Contact modify "@.*:"
"@XX.228.235.70:"
 rule 4 request ANY sip-header P-Asserted-Identity modify "@.*>"
"@XX.228.235.70>"
 rule 5 response ANY sip-header P-Asserted-Identity modify "@.*>"
"@XX.228.235.70>"
 rule 6 response ANY sdp-header Audio-Connection-Info modify
"172.31.26.74" "XX.228.235.70"
 rule 7 request ANY sdp-header Audio-Connection-Info modify
"172.31.26.74" "XX.228.235.70"
 rule 8 request ANY sdp-header Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 9 response ANY sdp-header Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 10 request ANY sdp-header Session-Owner modify "IN IP4
172.31.26.74" "IN IP4 XX.228.235.70"
 rule 11 response ANY sdp-header Session-Owner modify "IN IP4
172.31.26.74" "IN IP4 XX.228.235.70"
 rule 12 request ANY sip-header Via modify "172.31.26.74:5060"
"XX.228.235.70:5060"
 rule 13 request INVITE sip-header Diversion modify "@.*>"
"@XX.228.235.70>"
!
voice class sip-profiles 500
 rule 9 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 10 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 11 request ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>"
"<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 14 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 15 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 20 request ANY sip-header From modify ">" ";otg=aws_XXXX_lgu>"
 rule 30 request ANY sip-header P-Asserted-Identity modify "sips:(.*)"
"sip:\1"
```

```
 rule 31 request ANY sdp-header Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 32 request ANY sdp-header Session-Owner modify "IN IP4
172.31.26.74" "IN IP4 XX.228.235.70"
 rule 33 request ANY sdp-header Audio-Attribute modify "a=candidate:1
1(.*) 172.31.26.74 (.*)" "a=candidate:1 1\1 XX.228.235.70 \2"
 rule 34 request ANY sdp-header Audio-Attribute modify "a=candidate:1
2(.*) 172.31.26.74 (.*)" "a=candidate:1 2\1 XX.228.235.70 \2"
 rule 35 response ANY sdp-header Connection-Info modify "172.31.26.74"
"XX.228.235.70"
 rule 36 response ANY sdp-header Session-Owner modify "IN IP4
172.31.26.74" "IN IP4 XX.228.235.70"
 rule 37 response ANY sdp-header Audio-Attribute modify "a=candidate:1
1(.*) 172.31.26.74 (.*)" "a=candidate:1 1\1 XX.228.235.70 \2"
 rule 38 response ANY sdp-header Audio-Attribute modify "a=candidate:1
2(.*) 172.31.26.74 (.*)" "a=candidate:1 2\1 XX.228.235.70 \2"
 rule 40 response ANY sdp-header Audio-Connection-Info modify
"172.31.26.74" "XX.228.235.70"
 rule 41 request ANY sdp-header Audio-Connection-Info modify
"172.31.26.74" "XX.228.235.70"
 rule 42 response ANY sdp-header Audio-Connection-Info modify
"172.31.26.74" "XX.228.235.70"
!
voice class e164-pattern-map 101
  e164 +121424259..
  e164 09725980...
  e164 +18.........
  e164 411
 !
voice class e164-pattern-map 501
  e164 9725980XXX
 !
voice class e164-pattern-map 201
  e164 9725980XXX
 !
voice class tenant 200
  registrar dns:XXXX.cisco-bcld.com scheme sips expires 240 refresh-
ratio 50 tcp tls
  credentials number AWS_XXXX_LGU username AWS_XXXX_LGU password 6
XXXXXX realm Broadworks
  authentication username AWS_XXXX_LGU password 6 XXXXXX realm
BroadWorks
  authentication username AWS_XXXX_LGU password 6 XXXXXX realm
XXXX.cisco-bcld.com
  no remote-party-id
  sip-server dns:XXXX.cisco-bcld.com
  connection-reuse
  srtp-crypto 200
  session transport tcp tls
  url sips
  error-passthru
  asserted-id pai
```

```
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  no pass-thru content custom-sdp
  sip-profiles 200
  outbound-proxy dns:da05.sipconnect-us.bcld.webex.com
  privacy-policy passthru
!
voice class tenant 100
  session transport udp
  url sip
  error-passthru
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  no pass-thru content custom-sdp
  sip-profiles 100
!
voice class tenant 500
  registrar dns:XXXX.cisco-bcld.com scheme sips expires 240 refresh-
ratio 50 tcp tls
  credentials number AWS_XXXX_LGU username AWS_XXXX_LGU password 6
XXXXXX realm Broadworks
  authentication username AWS_XXXX_LGU password 6 XXXXXX realm
BroadWorks
  authentication username AWS_XXXX_LGU password 6 XXXXXX realm
XXXX.cisco-bcld.com
  no remote-party-id
  sip-server dns:XXXX.cisco-bcld.com
  connection-reuse
  srtp-crypto 200
  session transport tcp tls
  url sips
  error-passthru
  asserted-id pai
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  no pass-thru content custom-sdp
  sip-profiles 500
  outbound-proxy dns:da09.sipconnect-us.bcld.webex.com
  privacy-policy passthru
!
voice class srtp-crypto 200
 crypto 1 AES_CM_128_HMAC_SHA1_80
!
voice translation-rule 1
 rule 1 /^0972\(.*\)/ /972\1/
 rule 2 /^\+1\(.*\)/ /\1/
 rule 3 /^\+91\(.*\)/ /01191\1/
!
voice translation-profile called
 translate called 1
!
license udi pid C8000V sn XXXXXXXX
```

```
license boot level network-essentials addon dna-essentials
diagnostic bootup level minimal
memory free low-watermark processor 64139
!
spanning-tree extend system-id
!
username ec2-user privilege 15 password 6 XXXXXX
username admin privilege 15 password 6 \XXXXXX
!
redundancy
!
interface VirtualPortGroup0
 vrf forwarding GS
 ip address 192.168.35.101 255.255.255.0
 ip nat inside
 no mop enabled
 no mop sysid
!
interface GigabitEthernet1
 ip address dhcp
 ip nat outside
negotiation auto
 no mop enabled
 no mop sysid
!
iox
ip forward-protocol nd
ip tcp window-size 8192
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet1
!
ip nat inside source list GS_NAT_ACL interface GigabitEthernet1 vrf GS
overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 172.31.26.1
ip route XX.XX.79.250 255.255.255.255 GigabitEthernet1 172.31.26.1
ip route vrf GS 0.0.0.0 0.0.0.0 GigabitEthernet1 172.31.26.1 global
ip ssh rsa keypair-name ssh-key
ip ssh version 2
ip ssh pubkey-chain
  username ec2-user
   key-hash ssh-rsa XXXXXX ec2-user
   key-hash ssh-rsa XXXXXX ec2-user
ip ssh server algorithm publickey ecdsa-sha2-nistp256 ecdsa-sha2-
nistp384 ecdsa-sha2-nistp521 ssh-rsa x509v3-ecdsa-sha2-nistp256
x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp521
ip scp server enable
!
ip access-list standard GS_NAT_ACL
 10 permit 192.168.35.0 0.0.0.255
ip access-list standard PSTN
```

```
 10 permit any
ip access-list standard Wx
 10 permit any
!
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 100 voip
 description Incoming dial-peer from PSTN to vCUBE-AWS
 session protocol sipv2
 session transport udp
 incoming uri via 100
 voice-class codec 1
 voice-class stun-usage 200
 voice-class sip asserted-id pai
 voice-class sip profiles 222 inbound
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 201 voip
 description Outgoing dial-peer from vCUBE-AWS to Webex Calling
 session protocol sipv2
 session target sip-server
 session transport tcp tls
 destination e164-pattern-map 201
 voice-class codec 1
 voice-class stun-usage 200
 voice-class sip asserted-id pai
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
!
dial-peer voice 200 voip
 description Incoming dial-peer from Webex Calling to vCUBE-AWS
 session protocol sipv2
 incoming uri request 200
 voice-class codec 1
 voice-class stun-usage 200
 voice-class sip asserted-id pai
 voice-class sip tenant 200
 dtmf-relay rtp-nte
 srtp
 no vad
!
```

```
dial-peer voice 101 voip
 description Outgoing dial-peer from vCUBE-AWS to PSTN
 translation-profile outgoing called
 session protocol sipv2
 session target ipv4:XX.XX.79.250:5060
 session transport udp
 destination e164-pattern-map 101
 voice-class codec 1
 voice-class stun-usage 200
 voice-class sip asserted-id pai
 voice-class sip profiles 100
 voice-class sip tenant 100
 voice-class sip options-keepalive
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 500 voip
 description Incoming dial-peer from Webex Calling-2 to vCUBE-AWS
 session protocol sipv2
 incoming uri request 500
 voice-class codec 1
 voice-class stun-usage 200
 voice-class sip asserted-id pai
 voice-class sip tenant 500
 dtmf-relay rtp-nte
 srtp
 no vad
!
dial-peer voice 501 voip
 description Outgoing dial-peer from vCUBE-AWS to Webex Calling-2
 session protocol sipv2
 session target sip-server
 session transport tcp tls
 destination e164-pattern-map 501
 voice-class codec 1
 voice-class stun-usage 200
 voice-class sip asserted-id pai
 voice-class sip tenant 500
 dtmf-relay rtp-nte
 srtp
 no vad
!
sip-ua
 transport tcp tls v1.2
 crypto signaling default trustpoint dummyTp cn-san-validate server
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
 transport input ssh
line vty 5 20
```

```
 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
!
app-hosting appid guestshell
 app-vnic gateway1 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.35.102 netmask 255.255.255.0
 app-default-gateway 192.168.35.101 guest-interface 0
 name-server0 8.8.8.8
end
```

Important Information

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