The bridge to possible

High-Capacity Premises-based PSTN Option for Webex Calling

Hussain Ali, Technical Marketing Engineer, CCIE# 38068 (Voice, Collaboration)
https://www.linkedin.com/in/hussaincube

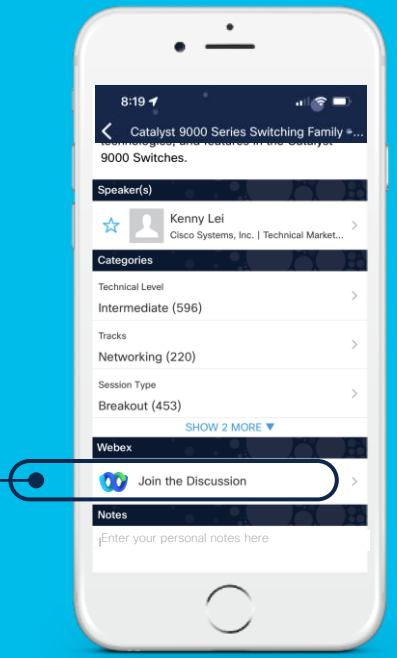
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



Webex spaces will be moderated until February 24, 2023.

Agenda

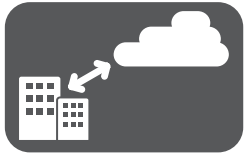
- Local Gateway (LGW) overview and sizing
- Multiple Registration-based LGWs on a single CUBE
- Managing Gateways from the Webex Control Hub
- Introducing Certificate-based Local Gateway
- Configuring a Certificate-based Local Gateway
- 3rd Party SBC as a Local Gateway
- Resources

Additional sessions on IOS-XE UC

(CUBE, Local Gateway, Survivability Gateway)

- BROCOL-2314 Introducing vCUBE on Azure and CUBE v14 Updates
- **Room D203 – Tuesday 8:30AM – 9:30AM**

- BRKCOL-2312 High-Capacity Premises-based PSTN Option for Webex Calling
- **Room D201 – Wednesday 10:30AM – 11:30AM**

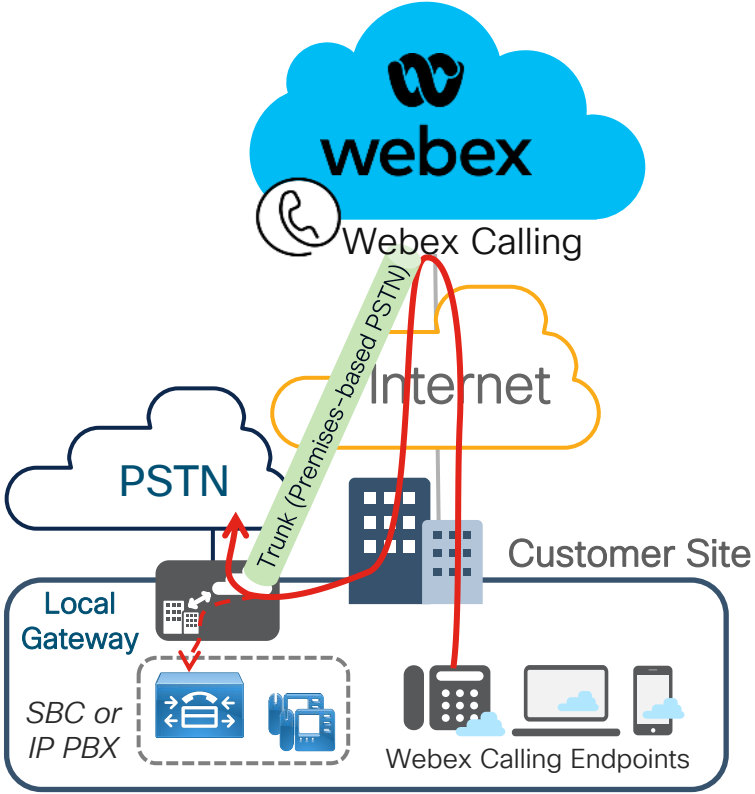


- BRKCOL-2993 Enabling Site Survivability for Webex Calling
- **Room Elicium 3 – Thursday 12:15PM – 1:15PM**

Local Gateway (LGW)
Overview and Sizing

Webex Calling Trunk - Local Gateway

(Premises-based PSTN) Deployment

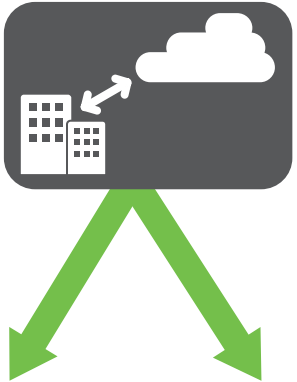


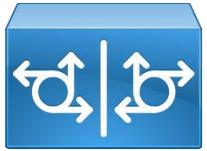
- Provides connectivity to a customer-owned premises-based PSTN service
- May also provide connectivity to an on-premises IP PBX or dedicated SBC/PSTN GW
- Enables on-prem to Webex Calling transition
- **Endpoint registration is NOT proxied through Local Gateway, unlike CUBE Lineside.** Endpoints directly register to Webex Calling over the Internet.

Local Gateway

Platform Support

Local Gateway (LGW)

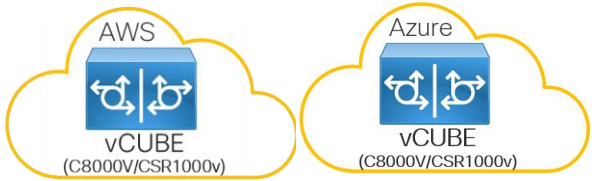




CUBE

IOS-XE GW

- **Cisco CUBE** (for IP-based connectivity) or Cisco IOS Gateway (for TDM-based connectivity)
- Hardware and software requirements:
  - ISR 4321, 4331, 4351, 4431, 4451, 4461 (IOS XE 17.6.5)
  - vCUBE in AWS, Azure



  - Catalyst 8200/8300 series (IOS XE 17.6.5/17.9.2a)

  - CSR 1000v (vCUBE) (16.12.5 or later – 17.3.5 latest) –
  - Catalyst 8000v Edge (vCUBE) (IOS XE 17.6.5)
    - C8000v/CSR 1000v licenses are not included in Webex Calling Flex and need to be purchased separately
    - Estimate 200 kbps total data throughput for every audio call
  - ISR 1100 (IOS-XE 17.6.5)

CUBE Software Release Mapping

CUBE Version	Initial IOS-XE Release for this CUBE version and Release date		Subsequent IOS-XE Release for this CUBE version
12.8.0	17.2.1r	March 2020	17.2.3
14.0	17.3.1a	July 2020	17.3.6
14.1	17.3.2*	Oct 2020	17.3.6
14.2	17.4.1a	Nov 2020	17.4.2
14.3	17.5.1	March 2021	17.5.1a
14.4	17.6.1a	July 2021	17.6.5
14.4	17.7.1a	Nov 2021	17.7.2
14.5	17.8.1a	March 2022	
14.6	17.9.1a	July 2022	17.9.2a
14.6	17.10.1a	Nov 2022	
TBD	17.11.1	March 2023	

Last release for ISR4K except ISR4461

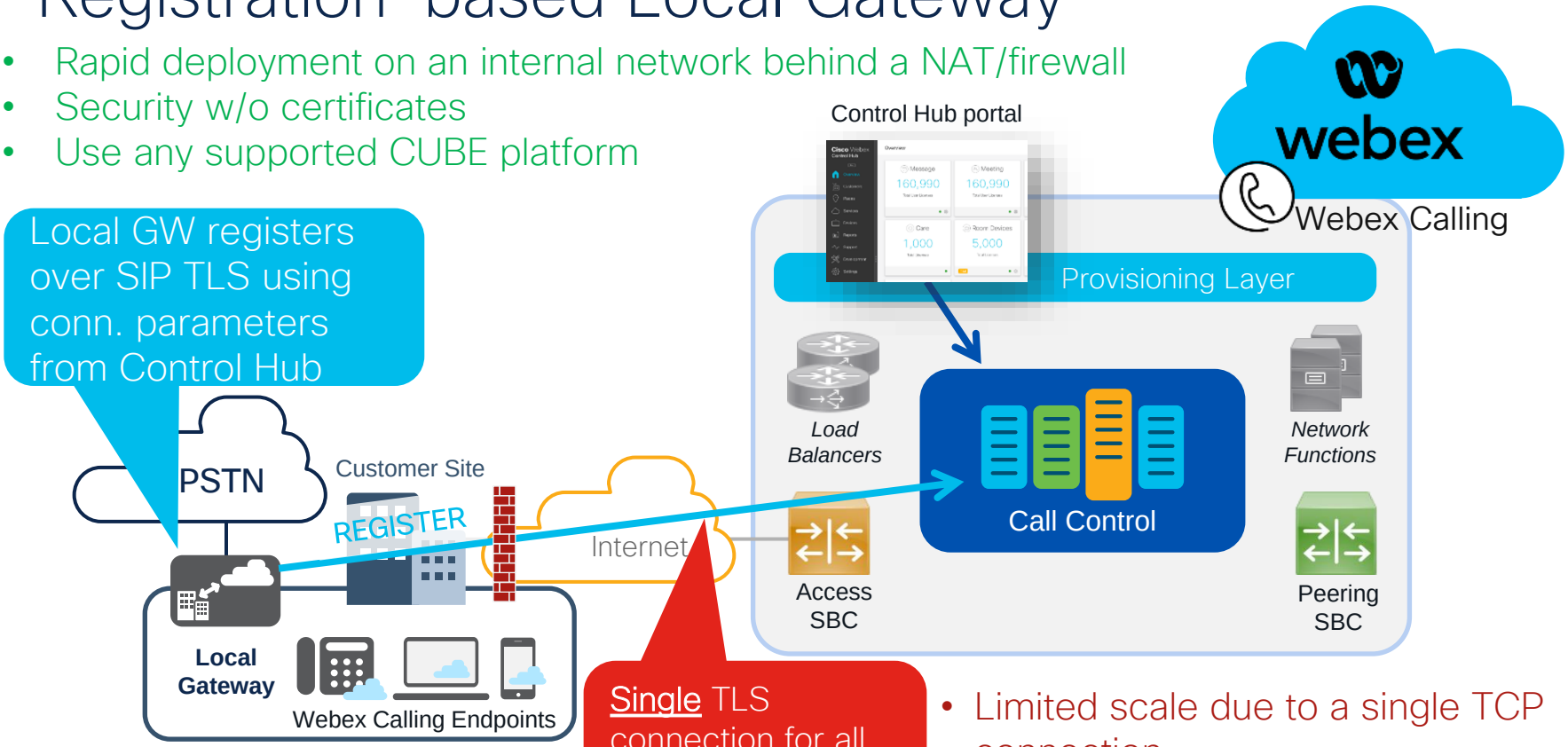
Agenda

- Local Gateway (LGW) overview and sizing
- Multiple Registration-based LGWs on a single CUBE
- Managing Gateways from the Webex Control Hub
- Introducing Certificate-based Local Gateway
- Configuring a Certificate-based Local Gateway
- 3rd Party SBC as a Local Gateway
- Resources

Multiple Registration-based LGWs on a single CUBE

Registration-based Local Gateway

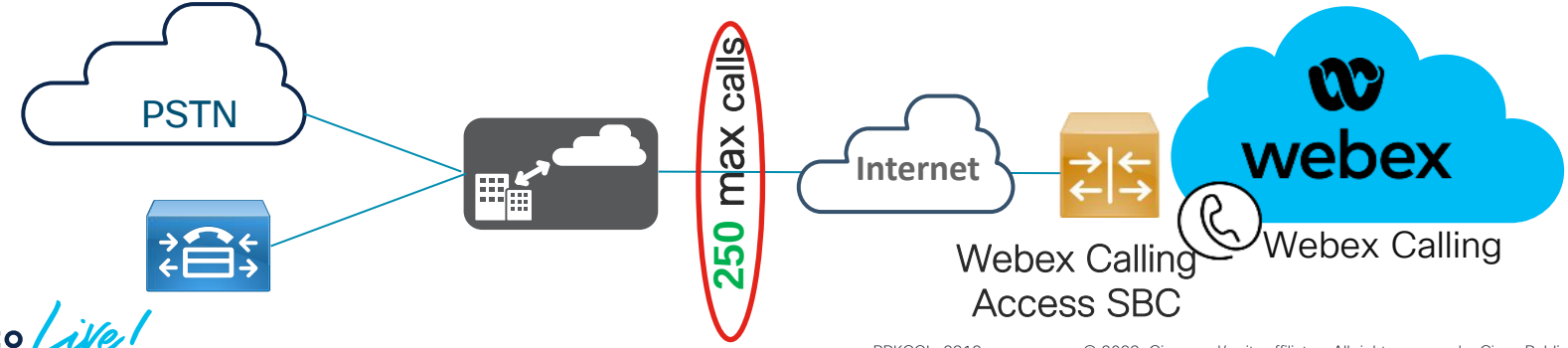
- Rapid deployment on an internal network behind a NAT/firewall
- Security w/o certificates
- Use any supported CUBE platform



- Limited scale due to a single TCP connection
- Sensitive to network impairments (TCP throughput ∝ latency/loss)

Registration-based LGW Concurrent Call Limit

- Regardless of LGW platform, premises trunks between LGW and Webex Calling cannot exceed 250 concurrent calls when connected over the Internet (OTT).
  - This assumes a maximum of 100ms one-way latency with no more than10ms jitter, less than 0.5% packet loss
  - Poor network conditions between Local Gateway and Webex Calling access SBC can limit the performance of the signaling connection leading to an even lower concurrent calls limit.
- Multiple Registration-based LGWs with Trunk and Route groups can be deployed for higher scale:
  - Premises → cloud calls: load balancing supported today *(e.g., CUCM route groups)*
  - Cloud → premises calls: Webex Calling Trunk and Route Groups



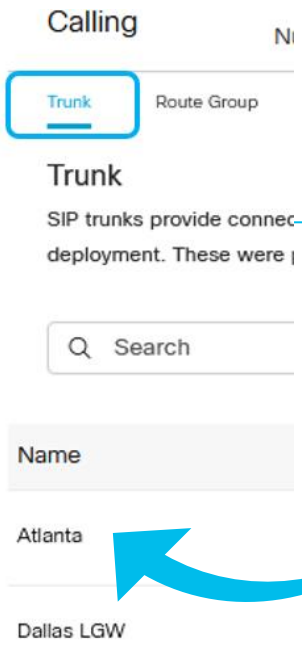
What constitutes a Registration-based LGW within a CUBE platform?

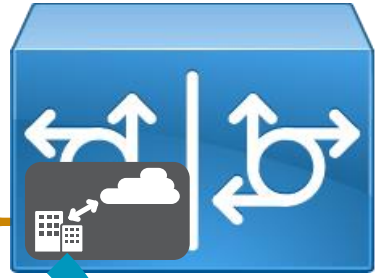
```
voice class sip-profiles 200
  rule 20 request ANY sip-header From modify ">" ";otg= hussain3847_lgu >"
```

```
voice class tenant 200
  registrar dns:XXXXXX scheme sips expires 240 refresh-ratio 50 tcp tls
  credentials number XXXXXX username XXXXXX password 0 XXXXXX realm BroadWorks
  authentication username XXXXXX password 0 XXXXXX realm BroadWorks
  authentication username XXXXXX password 0 XXXXXX realm XXXXXX
  sip-server dns:XXXXXX
  session transport tcp tls
  url sips
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  sip-profiles 200
  outbound-proxy dns:XXXXXX
```

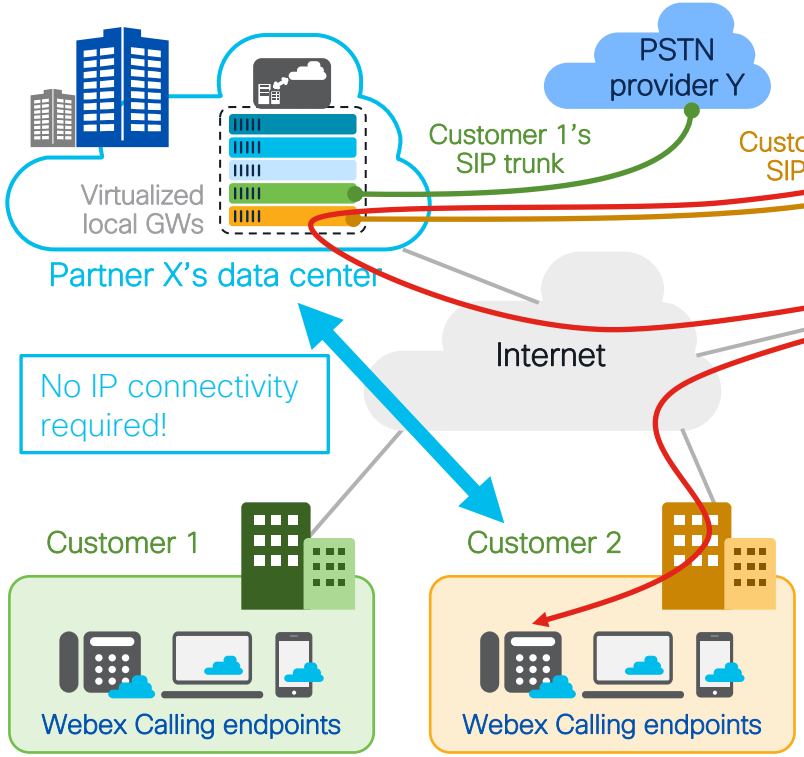
```
voice class uri 200 sip
  pattern dtg=hussain3847.lgu
```

```
dial-peer voice 200201 voip
  description In/Out WxC
  max-conn 250
  destination-pattern BAD.BAD
  session protocol sipv2
  session target sip-server
  destination dpg 100
  incoming uri request 200
  voice-class sip tenant 200
```





Partner hosted Local Gateway (Multi-tenant)



- Partner hosts and manages customer's Local Gateway (e.g., vCUBE) - connected OTT to Webex Calling
- Not recommended if on-premises PBX or SBC is present *(requires VPN between Partner DC and customer network)*

Note: Registration-based LGW Concurrent Call Limits Apply

Single CUBE instance with two LGWs – Total 500 calls

Any supported CUBE Release

Trunk1 - LGW1=250 calls

```
dial-peer voice 200201 voip
  description In/Out WxC
  max-conn 250
  destination-pattern BAD.BAD
  session protocol sipv2
  session target sip-server
  destination dpg 100
  incoming uri request 200
  voice-class sip tenant 200

voice class tenant 200
  bind control source-interface GigabitEthernet0/0/1
  bind media source-interface GigabitEthernet0/0/1
```

Trunk 2 - LGW2=250 calls

```
dial-peer voice 300301 voip
  description In/Out WxC
  max-conn 250
  destination-pattern BAD.BAD
  session protocol sipv2
  session target sip-server
  destination dpg 300
  incoming uri request 300
  voice-class sip tenant 300

voice class tenant 300
  bind control source-interface GigabitEthernet0/0/0
  bind media source-interface GigabitEthernet0/0/0
```

Single vCUBE instance with two LGWs – Total 500 calls

IOS-XE 17.8.1a or later

Trunk1 - LGW1=250 calls

```
dial-peer voice 200201 voip
  description In/Out WxC
  max-conn 250
  destination-pattern BAD.BAD
  session protocol sipv2
  session target sip-server
  destination dpg 100
  incoming uri request 200
  voice-class sip tenant 200

voice class tenant 200
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  listen-port secure 5062
  tls-profile 2

voice class tls-profile 2
  trustpoint CUBE-TLS
```

Trunk 2 - LGW2=250 calls

```
dial-peer voice 300301 voip
  description In/Out WxC
  max-conn 250
  destination-pattern BAD.BAD
  session protocol sipv2
  session target sip-server
  destination dpg 300
  incoming uri request 300
  voice-class sip tenant 300

voice class tenant 300
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  listen-port secure 5070
  tls-profile 3

voice class tls-profile 3
  trustpoint CUBE-TLS
```

BRKCOL-2314

Agenda

- Local Gateway (LGW) overview and sizing
- Multiple Registration-based LGWs on a single CUBE
- Managing Gateways from the Webex Control Hub
- Introducing Certificate-based Local Gateway
- Configuring a Certificate-based Local Gateway
- 3rd Party SBC as a Local Gateway
- Resources

Managing Gateways from the Webex Control Hub

Introducing Gateway Connectors

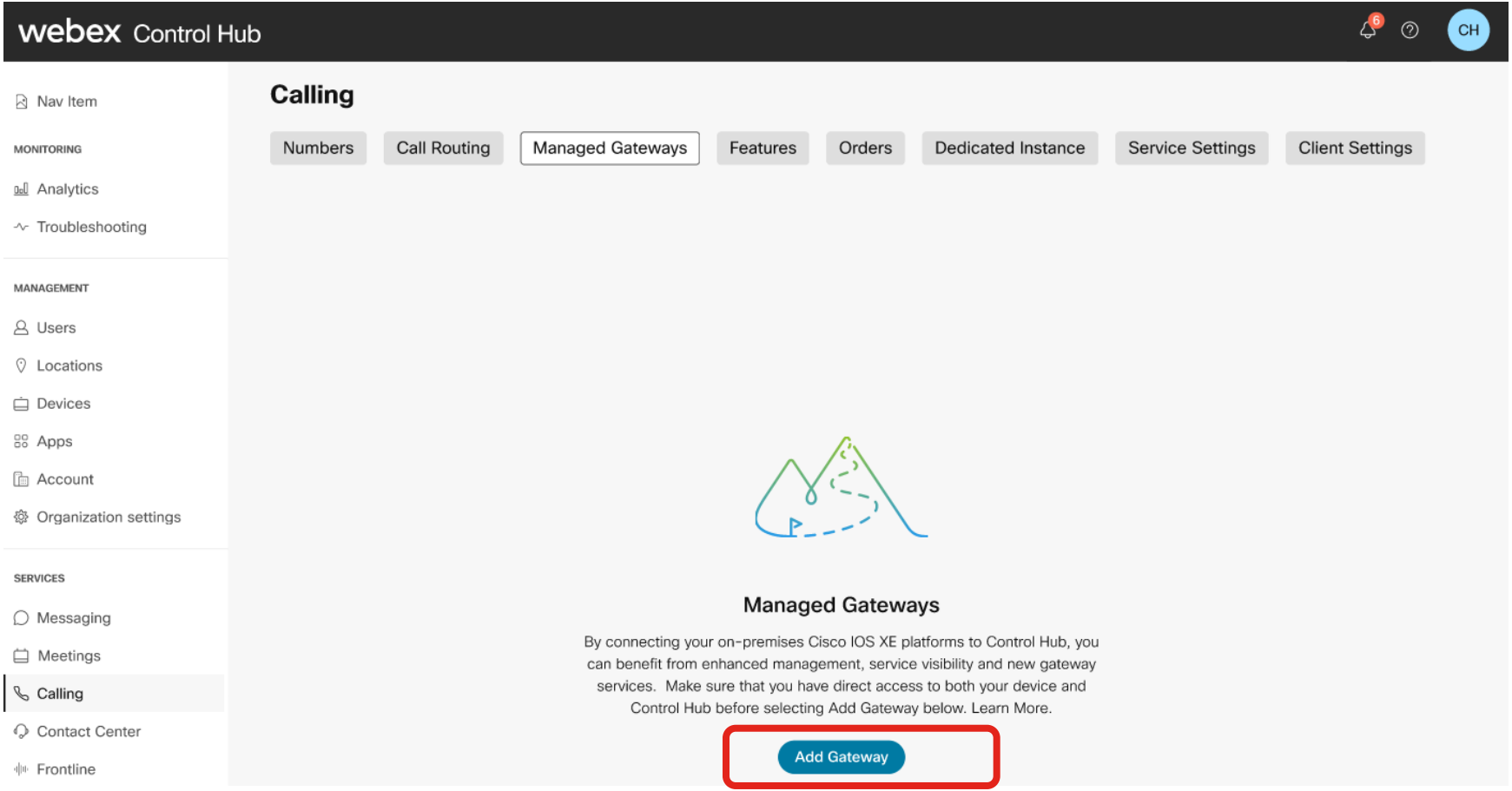
- Gateway connectors are small applications that run in the gateway Guest Shell to maintain a connection to Control Hub, co-ordinate events and collect status information.
- Guest Shell is independent of IOS-XE running on the platform
- NETCONF and YANG data models are used as opposed to the Command Line (CLI) to manage the gateways, thus, allowing APIs to manage and configure the gateways
- Two types of connectors exist
  - Management Connector - takes care of gateway enrollment to the cloud and lifecycle management of the telemetry connector
  - Telemetry Connector – used for pushing configs and getting command requests from the CH to the gateway

Connector Considerations

- ISR 1100 series are not supported
- CUBE High Availability (HA) mode is not supported
- Controller or SD-WAN mode is not supported (only IOS-XE Autonomous mode is supported)
- Currently two services are supported:
  - Registration-based Local Gateway Configuration Validation
  - Survivability Gateway Configuration template (BRKCOL-2993)
- IOS-XE version required:
  - Local Gateways—Cisco IOS XE 17.3.4a or later
  - Survivability Gateways—Cisco IOS XE 17.9.1a or later

Add a New Gateway Instance in Control Hub

Under **Services**, click **Calling** and then click the **Managed Gateways** Tab



In the **Add a Managed Gateway** window, copy the command to install the connector onto the Gateway

Add a Managed Gateway

Before you can add a gateway to Control Hub, you will need to install a connector application on your device. Access the device command line interface and paste the following command in full to start the installation. Once the connector is installed, confirm by checking the box below, then click Next. Learn more

```
tclsh https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway_onboarding.tcl
```

☐ I have installed the management connector on the gateway.

Cancel Next

Run the Management Connector deployment Script

- Run the TCL script
  - tclsh https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway_onboarding.tcl
- Follow the wizard

```
C8KV-Hussain#
C8KV-Hussain#$m/ManagedGatewayScriptProdStable/gateway_onboarding.tcl
Loading https://binaries.webex.com/ManagedGatewayScriptProdStable/gateway_onboarding.tcl !!!!!!!!!!
 Cisco IOS XE Software Version: 17.9.20221213
 Script Version: 3.0.3
 Precondition check status: Passed
 Downloading Gateway connector installer package...
```

Select the External Interface to reach Webex Cloud

```
        ==================================================================
                        Webex Gateway Connector Installation
        ==================================================================


Choose the external-interface from the below list of available interfaces:
        ==================================================================
         Number    Interface                IP-Address          Status
        ==================================================================
              1    GigabitEthernet1         10.52.12.203        up
        ==================================================================

Enter a number to choose the external interface: 1
```

Confirm or Edit DNS and Proxy settings

```
These DNS settings were detected in the gateway configuration:
144.254.71.184 173.38.200.100

Do you want to use these settings for the connector? [Y/n]: Y

These proxy settings were detected in the gateway configuration:

Proxy Server : proxy.esl.cisco.com
Proxy Port   : 80

Do you want to use these settings for the connector? [Y/n]: Y
```

Specify the Connector IP Address and Credentials

```
Enter Connector IP address: 10.52.12.216


Enter Gateway username: hussain
Enter Gateway password: ********
Confirm Gateway password: ******
```

```
Enabling guestshell...this may take upto 4 minutes, please wait for completion.
```

Connector Successfully Installed

```
==================================================================
                Webex Managed Gateway Connector
==================================================================

      *** Cloud connector is installed successfully. ***
    -------------------------------------------------------
                  *** Interface Status ***
    -------------------------------------------------------
       Interface                IP-Address          Status
    -------------------------------------------------------
       GigabitEthernet1         10.52.12.203        up
       VirtualPortGroup0        10.52.12.203        up
       Connector                10.52.12.216        up

    -------------------------------------------------------

                     *** App Status ***
    -------------------------------------------------------
            Service                    Status
    -------------------------------------------------------
            Guestshell                 RUNNING
            Management Connector       RUNNING
    -------------------------------------------------------
```

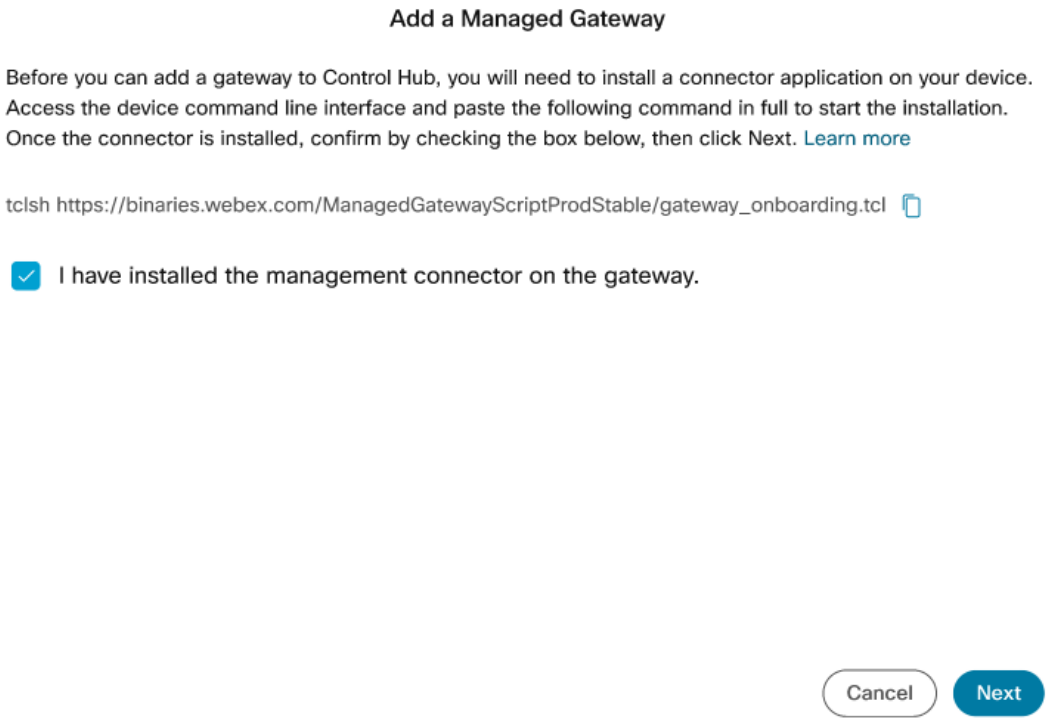
Webex Managed Gateway Connector Options

```
==================================================================
                Webex Managed Gateway Connector
==================================================================
     Options
       s :  Display Status Page
       v :  View and Modify Cloud Connector Settings
       e :  Enable Guestshell
       d :  Disable Guestshell
       l :  Collect Logs
       r :  Clear Logs
       u :  Uninstall Connector
       q :  Quit

==================================================================
               Select an option from the menu:
```

Enroll the Gateway in the Control Hub

In the **Add a Managed Gateway** window, check the **I have installed the management connector on the gateway** check box and click **Next.**



At the **Add a Managed Gateway** screen, enter the connector IP address that you entered during the connector installation procedure, and a preferred display name for the gateway

Add a Managed Gateway

Enter the following details for your installed connector. Click Next to open the connector web interface where you can complete device enrollment.

Enter the connector IP address

10.52.12.216

You will need to be able to reach this address directly from your browser.

Enter a display name for the gateway

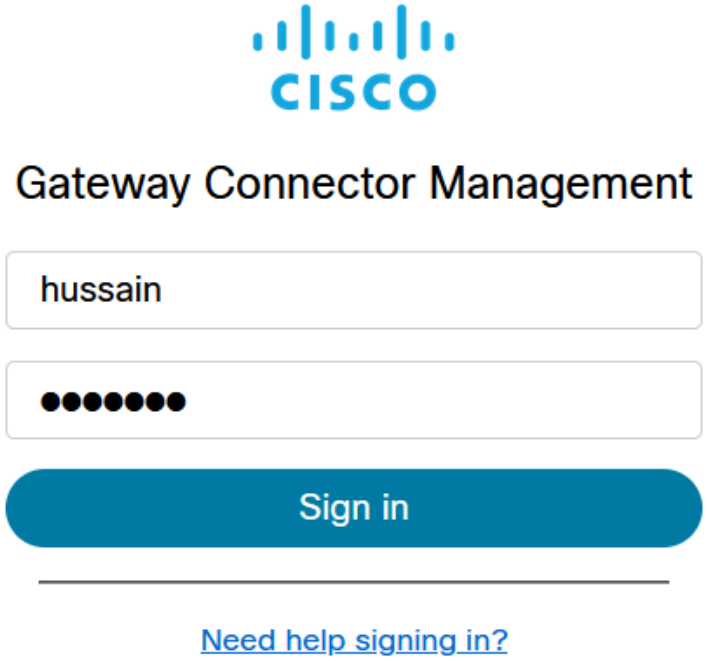
Hussain-Cat8kv

The name is for display purposes only.

Once enrollment is complete, gateways will appear in the Managed Gateway list.

Cancel Next

At the Connector Management page, enter the Gateway Admin **Username** and **Password** that you specified during the connector installation procedure



Click the **Enroll Now** button within an hour

Cisco Webex
Gateway Connector Management

Signed in as hussain

Sign out

Enroll Gateway

To complete the enrollment process, a secure connection must be established from this connector to the Cisco Webex cloud.

Use your Webex Calling administrator credentials to authenticate the connection on the next screen.

Enroll Now

Check the **Allow Access to the Gateway Management Connector** check box

Gateway Management Connector

Allow Access to Gateway Management Connector

Permissions are required to allow your Cisco Webex organization to create, read, update, and delete user accounts, as well as read and update information about your organization.

Organization

WxCSA Team Sandbox

FQDN or IP Address

10.52.12.216

☐ Allow Access to the Gateway Management Connector

Only allow access to hosts you know and trust

Continue

Enrollment Successful

Gateway Management Connector

Registration Confirmed

You will now be redirected to 10.52.12.216.

Enrollment successful.

You can close this window and proceed to Webex Control Hub to view and associate this gateway with a service.

Managed Gateways

Calling

Numbers | Locations | Call Routing | **Managed Gateways** | Features | PSTN | Service Settings | Client Settings

Search | All Gateways | 10 Gateway(s) | Events History | Add Gateway

Gateway Name	Version	Connector Sta...	Service	Assigned to	Actions
Amsterdam SGW	17.9.3	Online	Survivability Gateway	Location: Amsterdam Office	···
Hussain-Cat8kv		-	-	-	···
Lisbon SGW	17.9.3	Online	Survivability Gateway	Location: Lisbon Office	···
London SGW	17.9.3	Offline	Survivability Gateway	Location: London Branch Office	···
Madrid SGW	17.9.3	Online	Survivability Gateway	Location: Madrid Office	···
Munich SGW	17.9.3	Online	Survivability Gateway	Location: Munich Office	···
Paris SGW	17.9.3	Online	Survivability Gateway	Location: Paris Office	···
Rome SGW	17.9.3	Online	Survivability Gateway	Location: Rome Office	···
Vienna SGW	17.9.3	Online	Survivability Gateway	Location: Vienna Office	···

Validate Registration-based LGW Configuration through Control Hub

Managed Gateway now **Online**

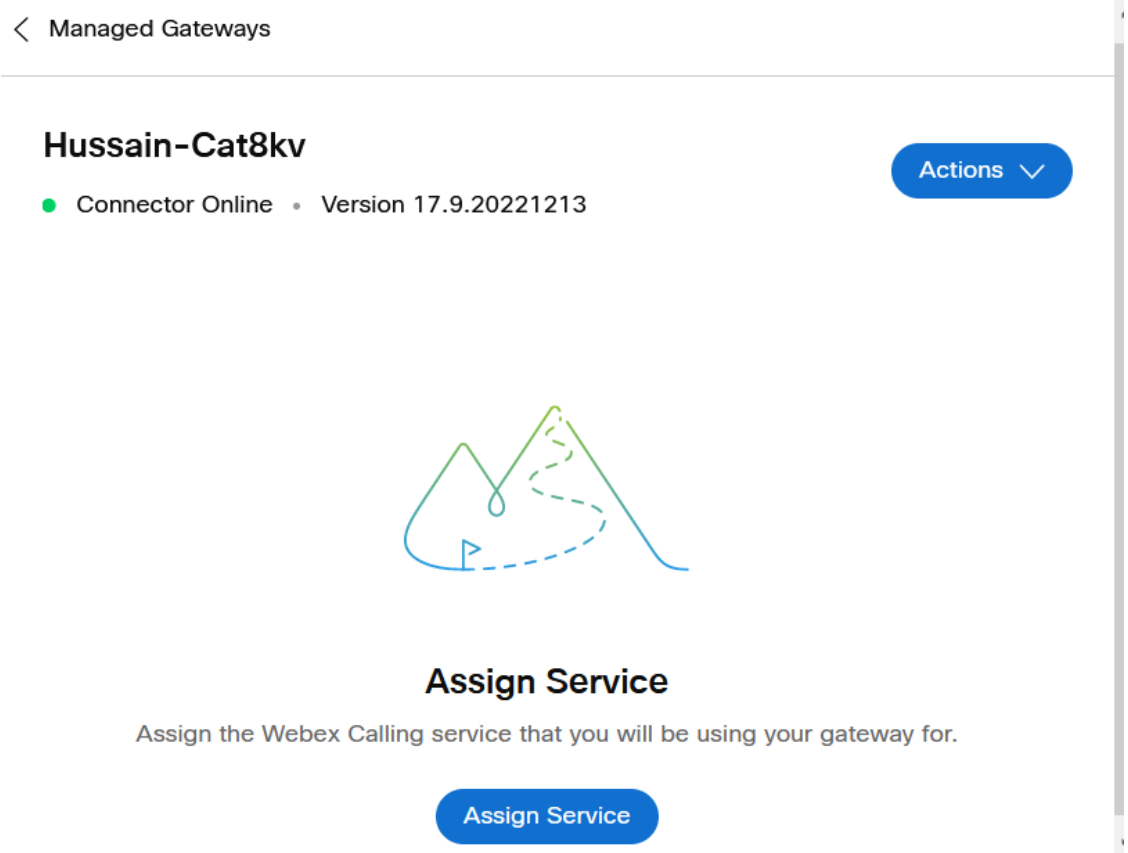
Calling

Numbers | Locations | Call Routing | **Managed Gateways** | Features | PSTN | Service Settings | Client Settings

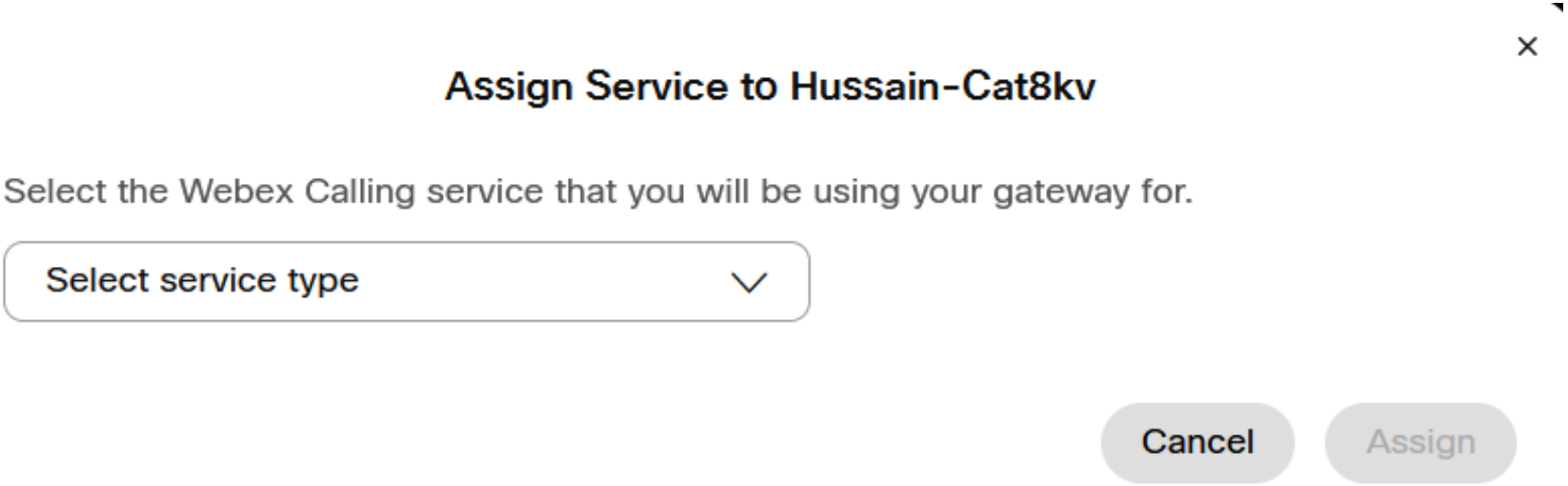
Search | All Gateways | 10 Gateway(s) | Events History | Add Gateway

Gateway Name	Version	Connector Sta...	Service	Assigned to	Actions
Amsterdam SGW	17.9.3	Online	Survivability Gateway	Location: Amsterdam Office	···
Hussain-Cat8kv	17.9.20221...	Online	-	-	···
Lisbon SGW	17.9.3	Online	Survivability Gateway	Location: Lisbon Office	···
London SGW	17.9.3	Offline	Survivability Gateway	Location: London Branch Office	···
Madrid SGW	17.9.3	Online	Survivability Gateway	Location: Madrid Office	···
Munich SGW	17.9.3	Online	Survivability Gateway	Location: Munich Office	···
Paris SGW	17.9.3	Online	Survivability Gateway	Location: Paris Office	···

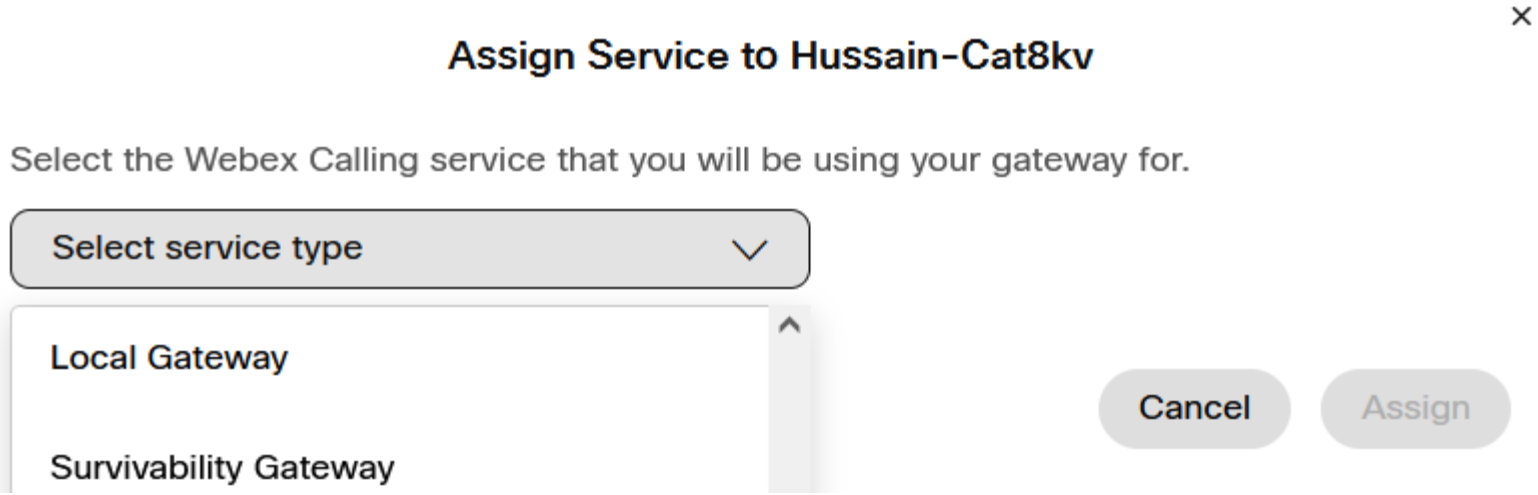
Assign a Service to the Managed Gateway



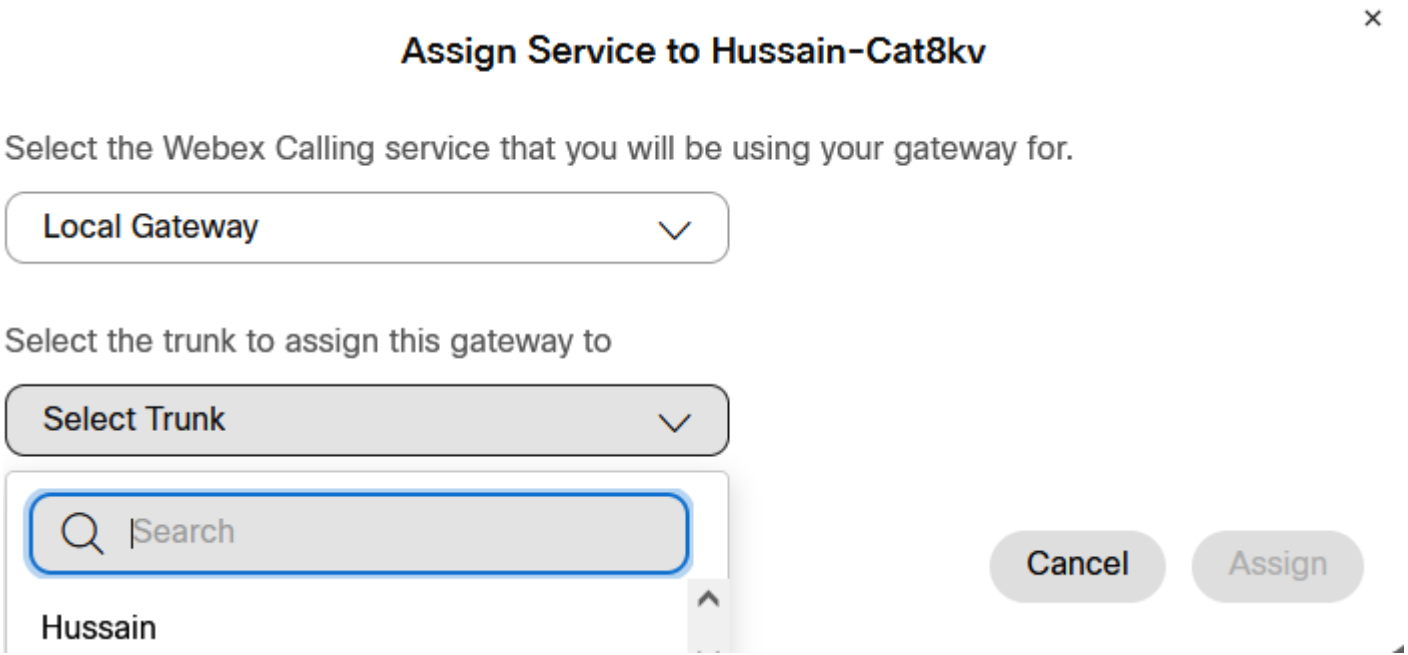
Select a Service Type



Service Type: LGW or SGW



For Service Type Local Gateway, specify the Trunk



Validate Registration-based LGW Configuration

< Managed Gateways

Hussain-Cat8kv

Actions

● Connector Online • Version 17.9.20221213

Local Gateway Service

Trunk	Hussain
Config Validation	Validate

Validation takes a few minutes

< Managed Gateways

Hussain-Cat8kv

Connector Online • Version 17.9.20221213

Actions

Local Gateway Service

Trunk	Hussain
Config Validation	Validation inititated on Feb 7, 2023, 4:46:30 PM. Results will be available shortly.

Validate

View Validation results

< Managed Gateways

Hussain-Cat8kv

● Connector Online • Version 17.9.20221213:174319

Local Gateway Service

Trunk	Hussain
Config Validation	Validation completed on Feb 7, 2023, 5:08:19 PM Validate View results

In the Validated Configuration page, verify if there are any misconfigurations

Validated Configuration

sip-ua
No issues found

voice service voip
No issues found

voice class sip-profiles 200
1 misconfigured

Misconfigured: Rule mismatches with required rule.

```
rule 11 request ANY sip-header From modify "<sips:" "<sip:\1"
```

Reference configuration

Copy

```
voice class sip-profiles 200
 rule 1 request ANY sip-header SIP-Req-URI modify "sips:(.*)" "sip:\1"
 rule 2 request ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 3 request ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 4 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
 rule 5 response ANY sip-header To modify "<sips:(.*)" "<sip:\1"
 rule 6 response ANY sip-header From modify "<sips:(.*)" "<sip:\1"
 rule 7 response ANY sip-header Contact modify "<sips:(.*)" "<sip:\1"
 rule 8 request ANY sip-header From modify ">" ";otg=hussain5773_lgu>"
```

Fix misconfigurations within the Local Gateway and run validation again

Validated Configuration

Your configuration has been checked for conformance with the recommended configuration for a Webex Calling Local Gateway. You can find more details here

Each section below details the commands that have been checked for a part of your configuration and whether any issues have been detected. Please review any issues and update your Local Gateway configuration accordingly. You can request another configuration validation after you have made your changes.

Please note that this service does not check every aspect of your configuration. As this service is not able to check encrypted passwords, you should verify that these have been entered accurately separately.

Report Date : February 7, 2023 5:14 PM
5 sections validated, 0 section(s) have issues.

sip-ua
No issues found

voice service voip
No issues found

voice class sip-profiles 200
No issues found

global
No issues found

voice class tenant 200
No issues found

Agenda

- Local Gateway (LGW) overview and sizing
- Multiple Registration-based LGWs on a single CUBE
- Managing Gateways from the Webex Control Hub
- Introducing Certificate-based Local Gateway
- Configuring a Certificate-based Local Gateway
- 3rd Party SBC as a Local Gateway
- Resources

Introducing Certificate-based Local Gateway

Why Certificate-based Trunking?

- Certificate-based Local Gateway (LGW) removes the scaling limitations of the registration-based LGW
- Allows for 3rd party SBC support

Sizing by number of concurrent calls per local gateway	Sizing by number of users behind a local gateway	Trunk type preferred	Minimum Link Quality
~ 2000-6500	65000	Certificate-based	Interconnect
250 to ~ 2000	20000	Certificate-based	OTT
up to 250	2500	Registration-based	OTT

Webex Calling Trunk - Local Gateway (Certificate-based)

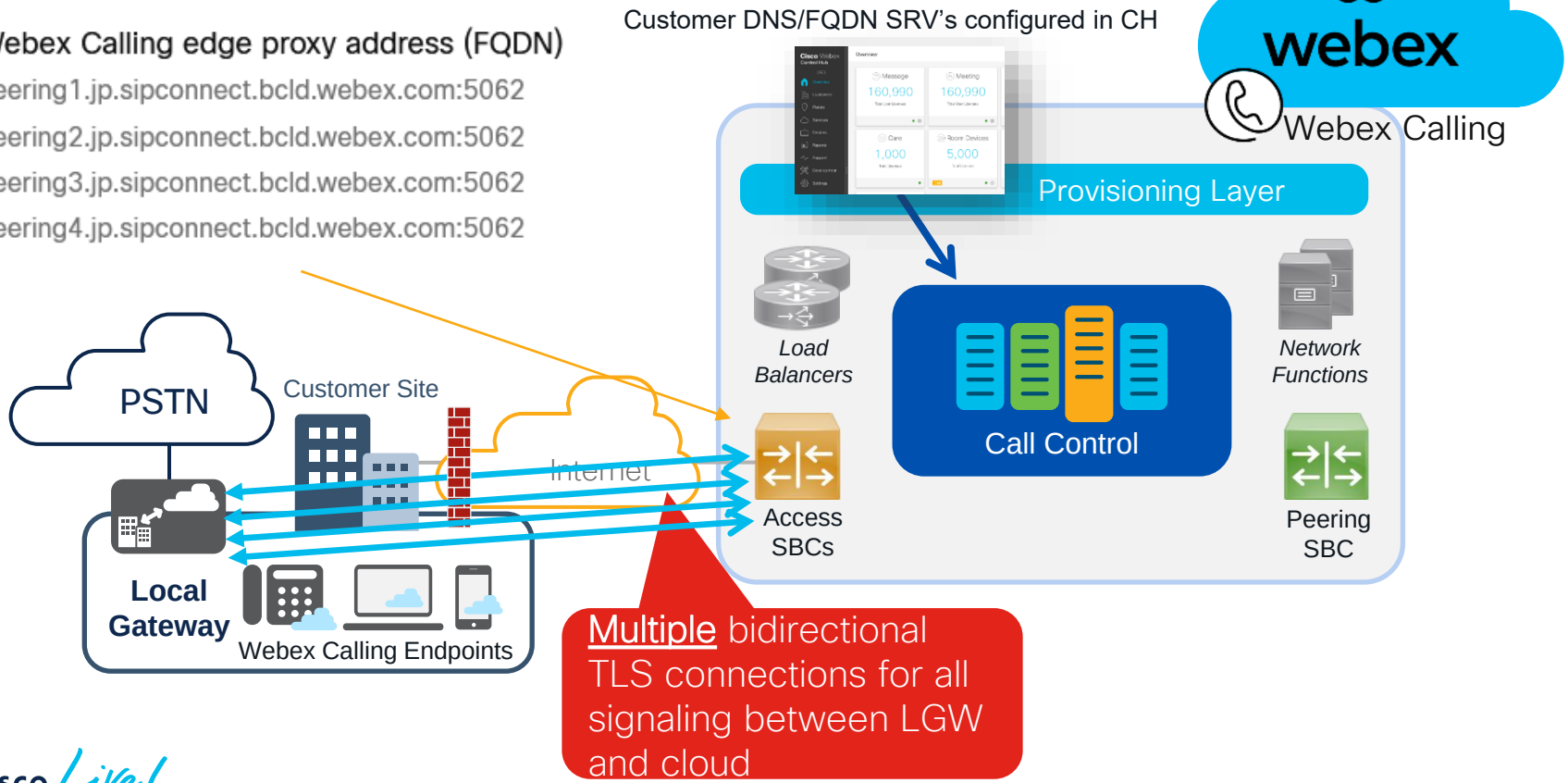
Webex Calling edge proxy address (FQDN)

peering1.jp.sipconnect.bcld.webex.com:5062

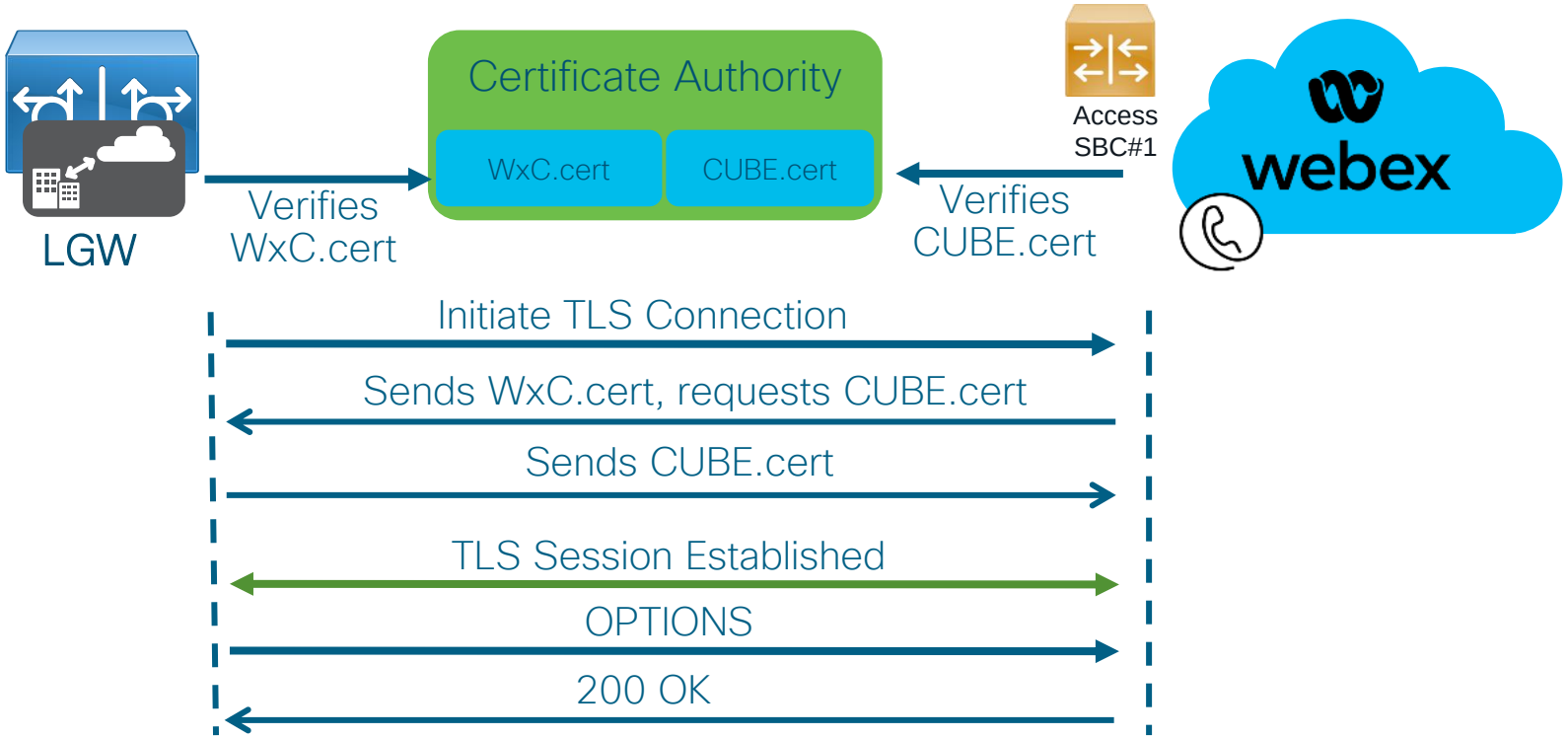
peering2.jp.sipconnect.bcld.webex.com:5062

peering3.jp.sipconnect.bcld.webex.com:5062

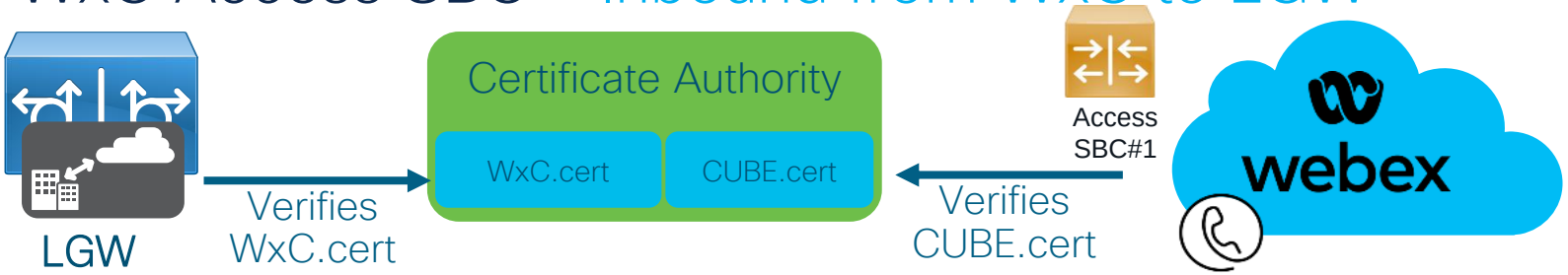
peering4.jp.sipconnect.bcld.webex.com:5062

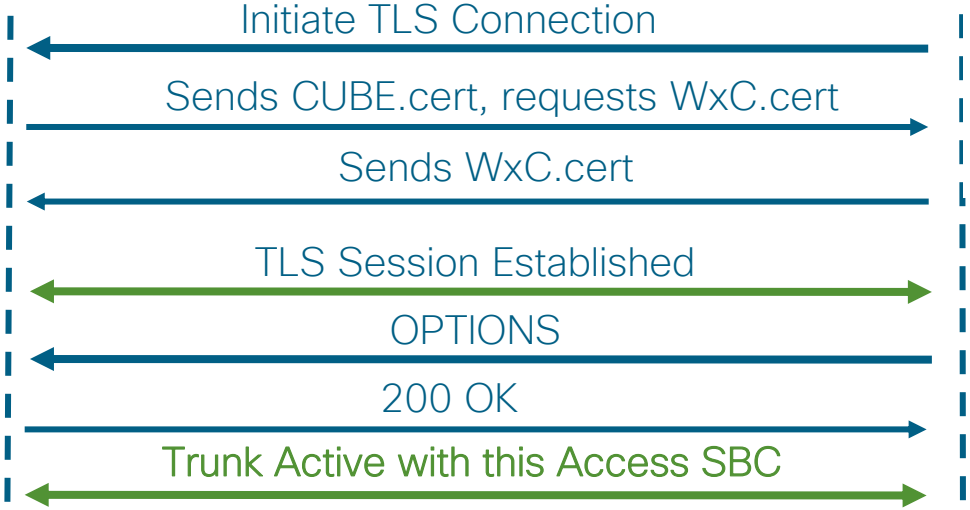


Certificate-based Local Gateway (Trunk Establishment) – 1st WxC Access SBC – Outbound from LGW to WxC



Certificate-based Local Gateway (Trunk Establishment) – 1st WxC Access SBC - Inbound from WxC to LGW





Webex Calling edge proxy address (FQDN)

1. peering1.jp.sipconnect.bcld.webex.com:5062
2. peering2.jp.sipconnect.bcld.webex.com:5062
3. peering3.jp.sipconnect.bcld.webex.com:5062
4. peering4.jp.sipconnect.bcld.webex.com:5062

Trunk > Details

Status

● Online

Trunk Type

Certificate based

Device

Cisco Unified Border Element

Now repeat the process with the 2nd, the 3rd, and the 4th WxC Access SBC

Agenda

- Local Gateway (LGW) overview and sizing
- Multiple Registration-based LGWs on a single CUBE
- Managing Gateways from the Webex Control Hub
- Introducing Certificate-based Local Gateway
- Configuring a Certificate-based Local Gateway
- 3rd Party SBC as a Local Gateway
- Resources

Configuring a Certificate-based LGW

Adding a Certificate-based Trunk in Control Hub

Add a Certificate-based Trunk to a Location

Add Trunk

Location

This location is where the trunk is physically connected. To create a new location, visit the Locations page.

Atlanta

Name

Hussain_Cert-based

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 *
sbc2	tmedemo.com	5061

Valid address

FQDN

sbc2.tmedemo.com:5061

Maximum number of concurrent calls *

1000

Cancel Save

Adding a Trunk

Add Trunk

Location

This location is where the trunk is physically connected. To create a new location, visit the Locations page.

Atlanta

Name

Hussain_Cert-based

Trunk Type

Choose the right trunk type for this local gateway. Learn more on trunk type

Certificate based

Device Type

Cisco Unified Border Element

Define the LGW hostname and select to resolve the LGW through an FQDN or an SRV

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 *
sbc2	tmedemo.com	5061

Valid address

FQDN

sbc2.tmedemo.com:5061

Maximum number of concurrent calls *

1000

Cancel Save

Save the Webex Calling Edge Addresses displayed

Add Trunk

Hussain_Cert-based 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.bcld.webex.com:5062
peering2.us.sipconnect.bcld.webex.com:5062
peering3.us.sipconnect.bcld.webex.com:5062
peering4.us.sipconnect.bcld.webex.com:5062

IOS-XE 17.6+

IOS-XE 17.9+

Webex Calling edge proxy address (SRV)

us01.sipconnect.bcld.webex.com

View your trunk

webex Control Hub

Search

- Overview
- Getting Started Guide
- Alerts center

MONITORING

- Analytics
- Troubleshooting
- Reports

MANAGEMENT

- Users
- Workspaces
- Devices
- Apps
- Account
- Organization Settings

SERVICES

- Updates & Migrations
- Messaging
- Meeting
- Calling
- Vidcast

Tekvizion

Calling

Numbers | Locations | Call Routing | Features | PSTN Orders

Trunk | Route Group | Dial Plans | Verify Call Routing | Zone | Trusted N

Trunk

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

Search

Name	Location	Trunk Typ
CUBE8	CUBE8	Certificate b
Hussain_Cert-based	Cisco1	Certificate b
Ribbon core trunk	Ribbon core	Certificate b
Ribbon Edge	Ribbon Edge	Certificate b

Hussain_Cert-based

Trunk > Details

Status
Online

Trunk Type
Certificate based

Device
Cisco Unified Border Element

FQDN
sbc2.tmedemo.com:5061

Max concurrent calls
350

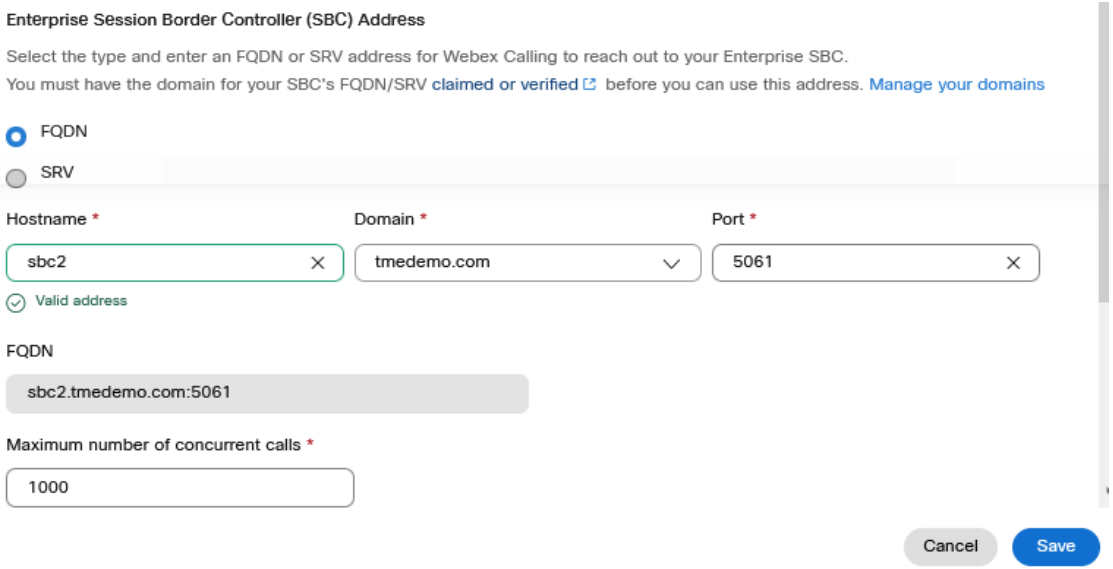
Webex Calling edge proxy address (FQDN)
peering1.us.sipconnect.bcld.webex.com:5062
peering2.us.sipconnect.bcld.webex.com:5062
peering3.us.sipconnect.bcld.webex.com:5062
peering4.us.sipconnect.bcld.webex.com:5062

Webex Calling edge proxy address (SRV)
us01.sipconnect.bcld.webex.com

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.

References in this presentation

Top level Domain	tmedemo.com
SBC/CUBE's FQDN (should be publicly reachable)	sbc2.tmedemo.com
Static Public IP associated with the CUBE FQDN	198.135.2.118



Configuring CUBE as a Certificate-based LGW

Step by Step CUBE config:
Common Global Configuration

Step 1 :
Base Platform configuration and Certificates

CUBE Reference platform configuration

- Before proceeding with CUBE configuration, ensure baseline platform configuration such as NTPs, ACLs, enable passwords, IP routing, IP Addresses, etc. are configured according to your organization's policies and procedures

- Local Gateway's cloud-facing (Webex Calling) network (interface) must not be behind a NAT service (All SIP and media ports on the external interface MUST be accessible).
-
- Public IPv4 address(es) must be reachable from the outside and should resolve through a public DNS service

- FQDN for the LGW configured within Control Hub should resolve to this interface IP
- IOS-XE 17.6+ is required.

```
interface GigabitEthernet 1
 description To Webex Calling – Public IPv4 required
 ip address 198.135.2.118 255.255.255.0
```

IOS-XE Security Configuration Requirement for CUBE

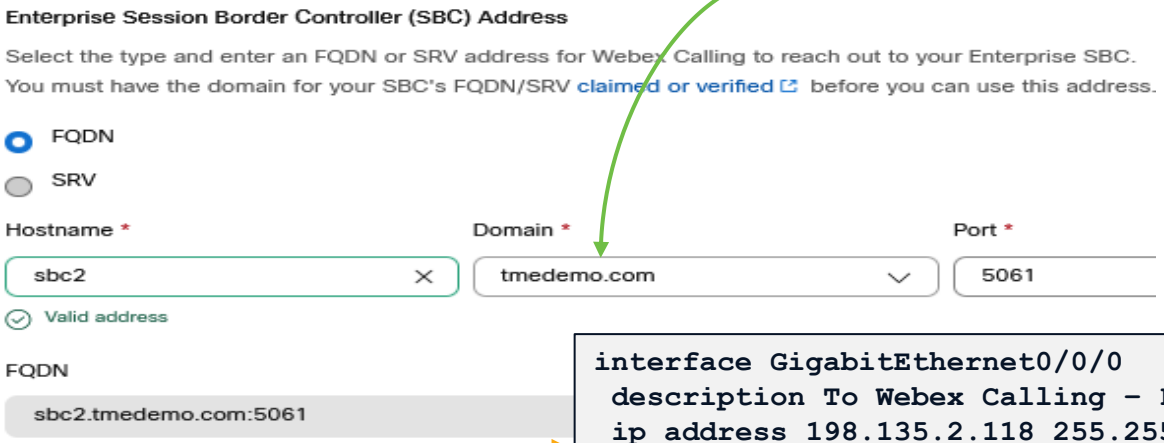
- You must preconfigure a primary key for the password with the following commands before it is used as a credential and shared secrets. Type 6 passwords are encrypted using AES cipher and user-defined primary key

```
CUBE#conf t
CUBE(config)#key config-key password-encrypt Password123
CUBE(config)#password encryption aes
```

Configure IP Name Server to enable DNS lookup, Domain-name, NTP

```
CUBE#config terminal
CUBE(config)#hostname sbc2
sbc2(config)#ip domain-name tmedemo.com
sbc2(config)#ip name-server 208.67.222.222
sbc2(config)#ntp server 0.us.pool.ntp.org
```

- DNS Servers: ensure the ip name-server is reachable by successfully pinging it. Local Gateway must resolve Webex Calling proxy addresses using this DNS
- Set the same domain name for the platform as defined in Control Hub




```
interface GigabitEthernet0/0/0
 description To Webex Calling - Public IPv4 required
 ip address 198.135.2.118 255.255.255.0
```

Certificates

Trust between Webex Calling and Local Gateway

- A signed certificate is required for a successful authorization and authentication of calls from the trunk. The certificate must meet the following requirements:
  - The certificate MUST be signed by a CA mentioned in What Root Certificate Authorities are Supported for Calls to Cisco Webex Audio and Video Platforms?
  - The trust bundle mentioned in What Root Certificate Authorities are Supported for Calls to Cisco Webex Audio and Video Platforms? should be uploaded on to the Local Gateway (CUBE).

Generate an RSA key pair – sbc2-key

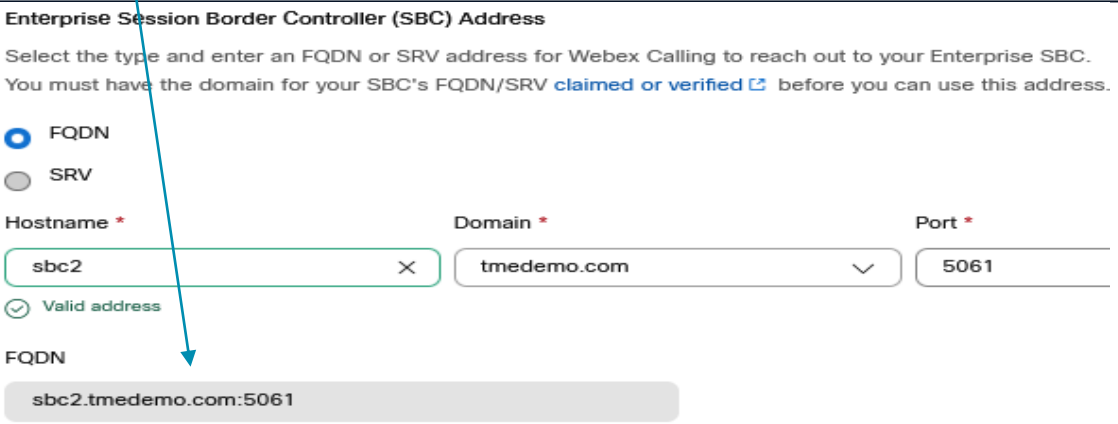
```
crypto key generate rsa general-keys label sbc2-key
modulus 4096 exportable
```

- Create an RSA key matching the certificate length of the root certificate with the above command
- Most CAs require private key size to be at least 2048 bit

Create a PKI trustpoint to hold the CA-signed CUBE certificate using the RSA key

```
crypto pki trustpoint CUBE_CA_CERT
 enrollment terminal pem
 serial-number none
 subject-name CN=sbc2.tmedemo.com ! (must match platform's DNS hostname through which it is reachable)
 subject-alt-name sbc2.tmedemo.com
 revocation-check none
 rsakeypair sbc2-key ! Created previously
```

- CUBE_CA_CERT – Trustpoint name can be anything
- Certificates MUST contain the Fully Qualified Domain Name (FQDN) as a common name or subject alternate name in the certificate with the FQDN chosen in the Control Hub



Generate a CSR on CUBE

```
crypto pki enroll CUBE_CA_CERT

% Start certificate enrollment..

% The subject name in the certificate will include: cn=sbc2.tmedemo.com
% The subject name in the certificate will include: sbc2.tmedemo.com
Display Certificate Request to terminal? [yes/no]: yes
```

- Input certificate details, make sure the LGW FQDN defined in Control Hub is present in the SAN https://www.sslshopper.com/csr-decoder.html
- Copy and save the CSR
- Send the CSR to your CA, who will send back a certificate for the host and also the root/intermediate CAs
- You may need to add the LGW FQDN (`sbc2.tmedemo.com`) record to your public DNS before your CA will issue you the cert

Paste Certificate Signing Request (CSR)


```
-----BEGIN CERTIFICATE REQUEST-----
MIICpDCCAYwCAQAwPjEaMBgGA1UEAxMRc2JjMi5jdWJlLXRtZS5jb
hkiG9w0BCQIWEXNiYzIuY3ViZS10bWUuY29tMIIBIjANBgkqhkiG9w
AQ8AMIIBCgKCAQEAjBuVXcBKtrPeAHQM1ips3MxaDYlZT6e9N1h
EtIQPvVnFDjSXS2LTMx9FHnmdpEgYkGOzxVjdd0G+aVcsrG/JqtJeS
yJT86Yre9M5uvswEWiwYy/uq3nz3CDFd5NpyUa3sHYqsdnY5/nAo
2T12i3jMpIMqjoDAnP2izd/zPqJBouRPAkx5LVVGATYm1mjfcggAW
KbuoE0Hqaot89mkJxVYKdTHFKZGt1xtQy8QXNMzyiXAe/ElqTbTi5
vCOzcA3ecOWrjrTsbd5hinLq654cyF1c2YVSTQIDAQABoCEwHwYJ
MRIwEDAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQAD
DTCNQTOpzsCjqI6f5l1z6/DGISwy2Lvm5j9SdTZZ7M7NZndEcFubq
c8az2Ss6i0fWP5+JxF1ptbWy1VaIsA4fxSgeSHNS2nvLriy9el3F7u8H
B1J5hdtqRzanCLR1IJgTKRFWqOM/NHqgTWX4LpDmePIq66XAsv+
2b3kCUGYL324Ys1+9VfuoUeSKUj4lccwNaZmRImCGF0ItgUnCUPk
JeuxjTJFdu1MZtXYMfXFCV99axLEgAuGl6Acp6LtpQfvE0rgWgKv+22
Ke9XS3t4KYM=
-----END CERTIFICATE REQUEST-----
```


CSR Information:

Common Name: sbc2.tmedemo.com

Create a PKI trustpoint to hold the Root Certificate from the Certificate Authority

```
crypto pki trustpoint Root_CA_CERT
 enrollment terminal
 revocation-check none
!
crypto pki authenticate Root_CA_CERT
<paste root CA X.64 based certificate here>
-----BEGIN CERTIFICATE-----
... ! Paste this in Root_CA_CERT
-----END CERTIFICATE-----
```

Create a PKI trustpoint to hold the Intermediate Certificate, if the root certificate has an intermediate CA

```
crypto pki trustpoint Intermediate_CA
 enrollment terminal
 chain-validation continue Root_CA_CERT
 revocation-check none
!
crypto pki authenticate Intermediate_CA
<paste Intermediate CA X.64 based certificate here>
-----BEGIN CERTIFICATE-----
... ! Paste this in Intermediate_CA
-----END CERTIFICATE-----
```

Authenticate and import the CA signed CUBE cert as shown below (Intermediate CA present)

```
! If the root certificate has an intermediate CA, then proceed as
! shown below. Paste in the top-level intermediate cert only that
! can authenticate the host (CUBE) cert
crypto pki authenticate CUBE_CA_CERT
<paste Intermediate CA X.64 based certificate here>
-----BEGIN CERTIFICATE-----
... ! Paste this in Intermediate_CA
-----END CERTIFICATE-----

! Import the host(CUBE) certificate as shown below
crypto pki import CUBE_CA_CERT certificate
<paste CUBE CA X.64 based certificate here>
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
... ! Paste this in CUBE_CA_CERT
-----END CERTIFICATE-----
```

- CUBE_CA_CERT – Trustpoint label to associate certificate

Authenticate and import the CA signed CUBE cert as shown below (Intermediate CA NOT present)

```
! If the root certificate does not have an intermediate CA, then
! proceed as shown below. Paste in the top-level root cert only
! that can authenticate the host (CUBE) cert
crypto pki authenticate CUBE_CA_CERT
<paste root CA X.64 based certificate here>
-----BEGIN CERTIFICATE-----
... ! Paste this in Root_CA_CERT
-----END CERTIFICATE-----

! Import the host(CUBE) certificate as shown below
crypto pki import CUBE_CA_CERT certificate
<paste CUBE CA X.64 based certificate here>
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
... ! Paste this in CUBE_CA_CERT
-----END CERTIFICATE-----
```

- CUBE_CA_CERT – Trustpoint label to associate certificate

Specify the default trustpoint and TLS version under SIP-UA

```
sip-ua
 transport tcp tls v1.2
 crypto signaling default trustpoint CUBE_CA_CERT
```

- `transport tcp tls v1.2` – Default TLS version to be 1.2

Import Cisco CA bundle for Webex Calling Certificate authentication

```
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.
```

Exporting RSA key and certificate from CUBE 1 for CUBE-HA

```
crypto pki export CUBE_CA_CERT pkcs12
ftp://<username>:<password>@x.x.x.x password xxxx

Address or name of remote host [x.x.x.x]?
Destination filename [CUBE_CA_CERT]?
Writing CUBE_CA_CERT Writing pkcs12 file to
ftp://<username>@x.x.x.x/CUBE_CA_CERT
!
CRYPTO_PKI: Exported PKCS12 file successfully
```

Importing RSA key and certificate in CUBE 2 for CUBE-HA

```
crypto pki import CUBE_CA_CERT pkcs12
ftp://<username>:<password>@x.x.x.x/ CUBE_CA_CERT password xxxx
% Importing pkcs12...

Address or name of remote host [x.x.x.x]?
Source filename [CUBE_CA_CERT]?
Reading file from ftp://<username>@x.x.x.x/CUBE_CA_CERT!
[OK - 4931/4096 bytes]

CRYPTO_PKI: Imported PKCS12 file successfully
```

Step by Step CUBE config:
Common Global Configuration

Step 2:
Trunk Enablement

Configure Global CUBE settings (voice service voip)

```
voice service voip
 ip address trusted list
  ipv4 X.X.X.X Y.Y.Y.Y  ! Check Webex Calling Port Reference Guide
 allow-connections sip to sip
 no supplementary-service sip refer
 no supplementary-service sip handle-replaces
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0
fallback none
 sip
  early-offer forced
```

Codec Lists

```
voice class codec 100
 codec preference 1 opus
 codec preference 2 g711ulaw
 codec preference 3 g711alaw
```

Configure STUN to enable ICE-Lite

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

- Used to enable STUN with ICE-Lite
- Will be applied to all Webex Calling facing dial-peers

Enable SRTP Crypto and SIP Profiles

```
voice class sip-profiles 100
 rule 10 request ANY sip-header Contact modify "198.135.2.118" "sbc2.tmedemo.com"
 rule 20 response ANY sip-header Contact modify "198.135.2.118" "sbc2.tmedemo.com"
!
voice class srtp-crypto 100
 crypto 1 AES_CM_128_HMAC_SHA1_80
```

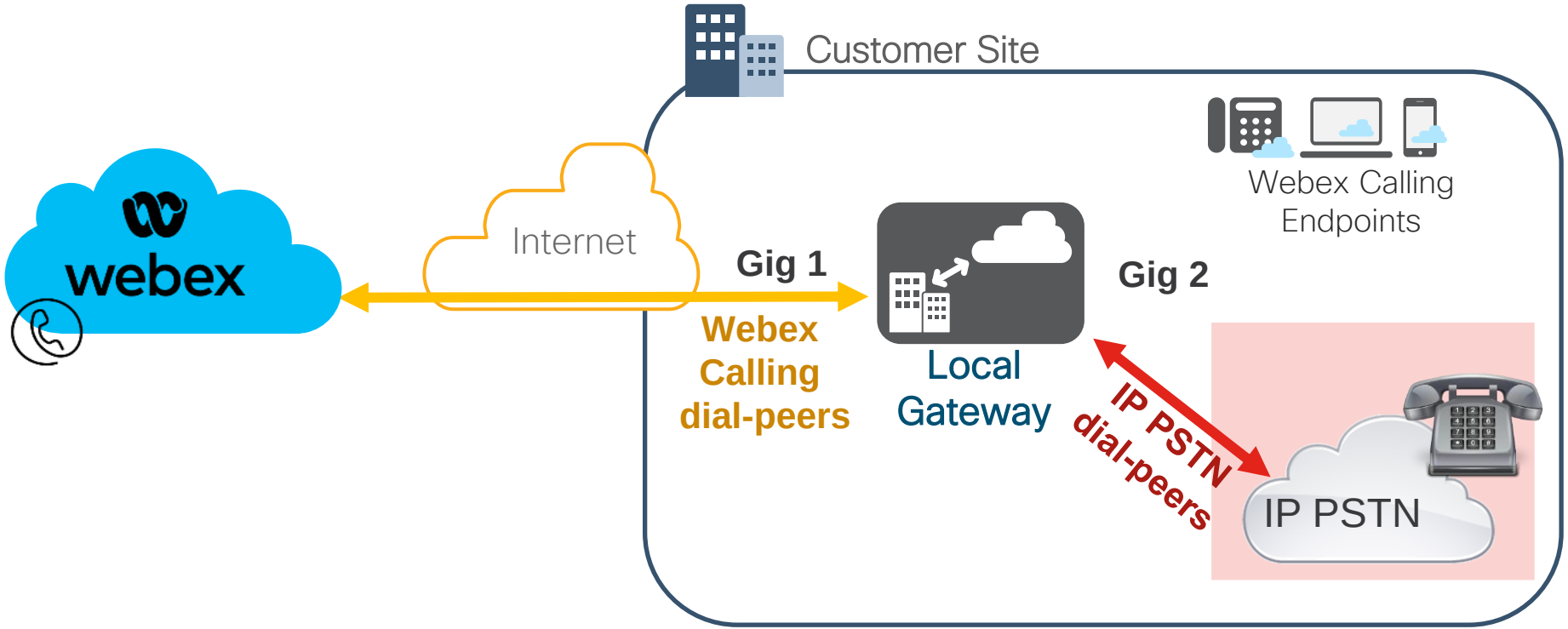
- Above SIP Profile applied to all Webex Calling facing dial-peers:
  - 198.135.2.118 is the IP address of the Local Gateway interface facing Webex Calling and sbc2.tmedemo.com is the FQDN of the enterprise SBC (Local Gateway) defined within Control Hub
  - Rules 10 and 20 ensure that the Local Gateway IP address is replaced with the FQDN in the Contact header of SIP request and response messages. This is a requirement for authentication of Certificate-based Local Gateway to be used as a trunk in Webex Calling

- **`crypto 1 AES_CM_128_HMAC_SHA1_80`** – Used to set the crypto cipher for the Webex Calling trunk.

Step by Step CUBE config:

Step 3:
Call Routing

Call Routing components



Outbound Dial-peers to Webex Calling peering proxies

- To ensure load balancing, the following 4 dial peers are used.
  1. Dial-peer voice 201 voip
  2. Dial-peer voice 202 voip
  3. Dial-peer voice 203 voip
  4. Dial-peer voice 204 voip

- IP PSTN Inbound dial-peer **100** invokes voice class dpg **200**

```
voice class dpg 200
 description Incoming IP PSTN(DP100) to WxC(DP201/202/203/204)
 dial-peer 201 preference 1
 dial-peer 202 preference 1
 dial-peer 203 preference 1
 dial-peer 204 preference 1
```

- This dial-peer structure ensures LGW is maintaining multiple active bidirectional connections with Webex Calling edge proxies

Outbound Dial-peer 201 – Towards WxC Proxy 1

```
dial-peer voice 201 voip
 description Outbound dial-peer towards Webex Calling Proxy 1
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:peering1.us.sipconnect.bcld.webex.com:5062
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

Outbound Dial-peer 202 – Towards WxC Proxy 2

```
dial-peer voice 202 voip
 description Outbound dial-peer towards Webex Calling Proxy 2
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:peering2.us.sipconnect.bcld.webex.com:5062
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

Outbound Dial-peer 203 – Towards WxC Proxy 3

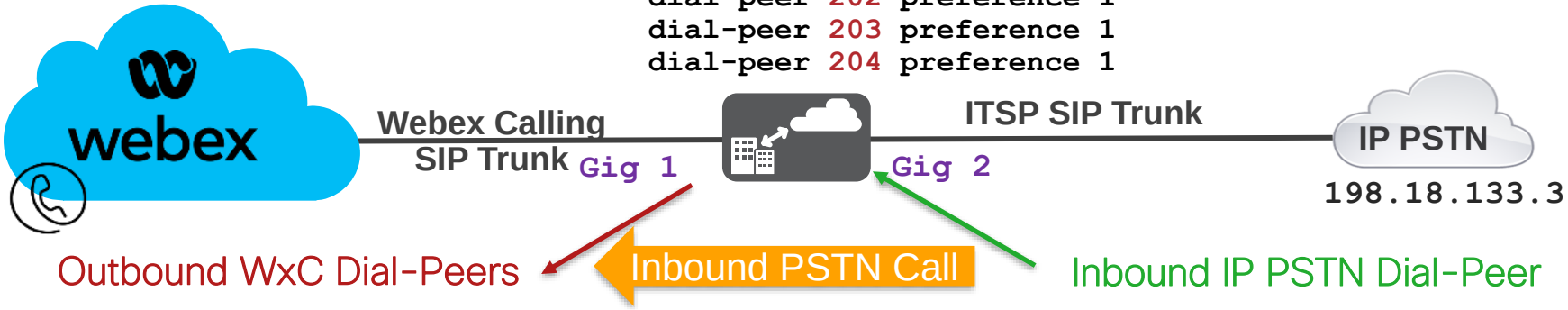
```
dial-peer voice 203 voip
 description Outbound dial-peer towards Webex Calling Proxy 3
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:peering3.us.sipconnect.bcld.webex.com:5062
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

Outbound Dial-peer 204 – Towards WxC Proxy 4

```
dial-peer voice 204 voip
 description Outbound dial-peer towards Webex Calling Proxy 4
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:peering4.us.sipconnect.bcld.webex.com:5062
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

Inbound PSTN Call

```
voice class dpg 200
 description Incoming IP PSTN(DP100) to WxC(DP201/202/203/204)
 dial-peer 201 preference 1
 dial-peer 202 preference 1
 dial-peer 203 preference 1
 dial-peer 204 preference 1
```




```
dial-peer voice 201 voip
 description Outbound dial-peer to Webex Calling Proxy 1
 session target dns:peering1.us.sipconnect.bcld.webex.com:5062

dial-peer voice 202 voip
 description Outbound dial-peer to Webex Calling Proxy 2
 session target dns:peering2.us.sipconnect.bcld.webex.com:5062

dial-peer voice 203 voip
 description Outbound dial-peer to Webex Calling Proxy 3
 session target dns:peering3.us.sipconnect.bcld.webex.com:5062

dial-peer voice 204 voip
 description Outbound dial-peer to Webex Calling Proxy 4
 session target dns:peering4.us.sipconnect.bcld.webex.com:5062
```

```
voice class uri 100 sip
  host ipv4:198.18.133.3

dial-peer voice 100 voip
  description Incoming dial-peer from IP PSTN
  incoming uri via 100
  session protocol sipv2
  destination dpg 200
  voice-class codec 100
  dtmf-relay rtp-nte
  no vad
```

Inbound Dial-peer 200 – From Webex Calling

```
voice class uri 200 sip
 pattern sbc2.tmedemo.com    ← Local Gateway's FQDN
!
dial-peer voice 200 voip
 description inbound from Webex Calling
 session protocol sipv2
 session transport tcp tls
 incoming uri request 200
 destination dpg 100
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

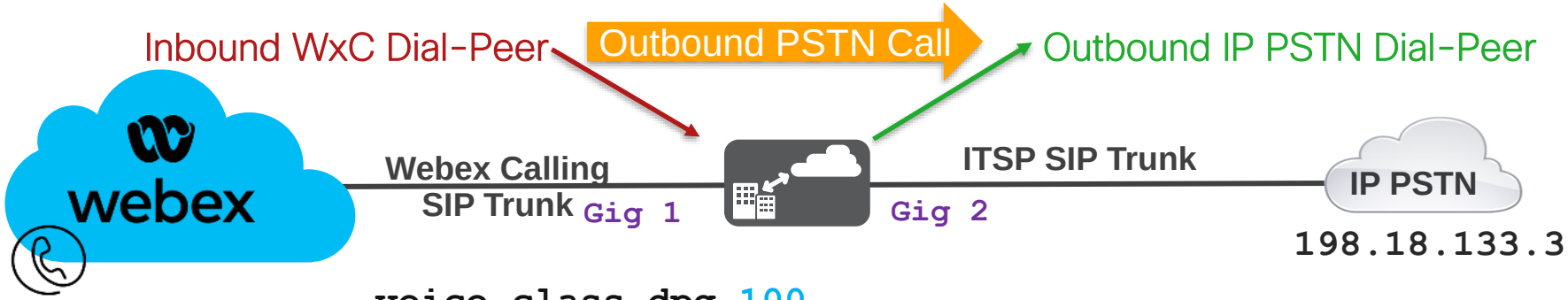
```
voice class dpg 100
 description Incoming WxC(DP200) to IP PSTN(DP101)
 dial-peer 101 preference 1
```

Outbound PSTN Call

```
voice class uri 200 sip
  pattern sbc2.tmedemo.com

dial-peer voice 200 voip
 description inbound from Webex Calling
 session protocol sipv2
 session transport tcp tls
 destination dpg 100
 incoming uri request 200
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

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




```
voice class dpg 100
 description Incoming WxC(DP200) to IP PSTN(DP101)
 dial-peer 101 preference 1
```

Registration-based Trunk

Pros and Cons

Pros:

- CUBE can sit on internal network behind a NAT/firewall
  - No need for the customer to expose CUBE's external interface
  - No need for the customer to setup a DMZ
- Easier to deploy: achieves security without a need for certificates
- Recommended method
- Config Validation from the Control Hub

Cons:

- Limited scale (single TCP connection)
  - Scales upto 250 calls (OTT), 500+ (Interconnect)
- Sensitive to network impairments (all calls affected when TCP connection is lost)

Certificate-based Trunk

Pros and Cons

Pros:

- Higher scale, up to CUBE platform limits (multiple TCP/TLS connections)
- Better resilience (each call is independent)
  - Network drop does not impact new calls as the call could land on the new connection
- Both sides (Webex Calling Access SBC and CUBE) can create connections on demand

Cons:

- CUBE must be reachable from the cloud (public IPv4 address on the external interface with inbound FW rules) [CUBE behind NAT will be supported soon]
  - Customer will need to publish an FQDN (IOS-XE 17.6+ - current help.Webex documentation) or SRV (IOS-XE 17.9+ - not yet documented) for WxC to reach the LGW
- Requires certificates signed by public CA on each CUBE and a DNS SRV
- Multitenancy is not supported today [will be supported soon]

Agenda

- Local Gateway (LGW) overview and sizing
- Multiple Registration-based LGWs on a single CUBE
- Managing Gateways from the Webex Control Hub
- Introducing Certificate-based Local Gateway
- Configuring a Certificate-based Local Gateway
- 3rd Party SBC as a Local Gateway
- Resources

3rd Party SBC as a Local Gateway

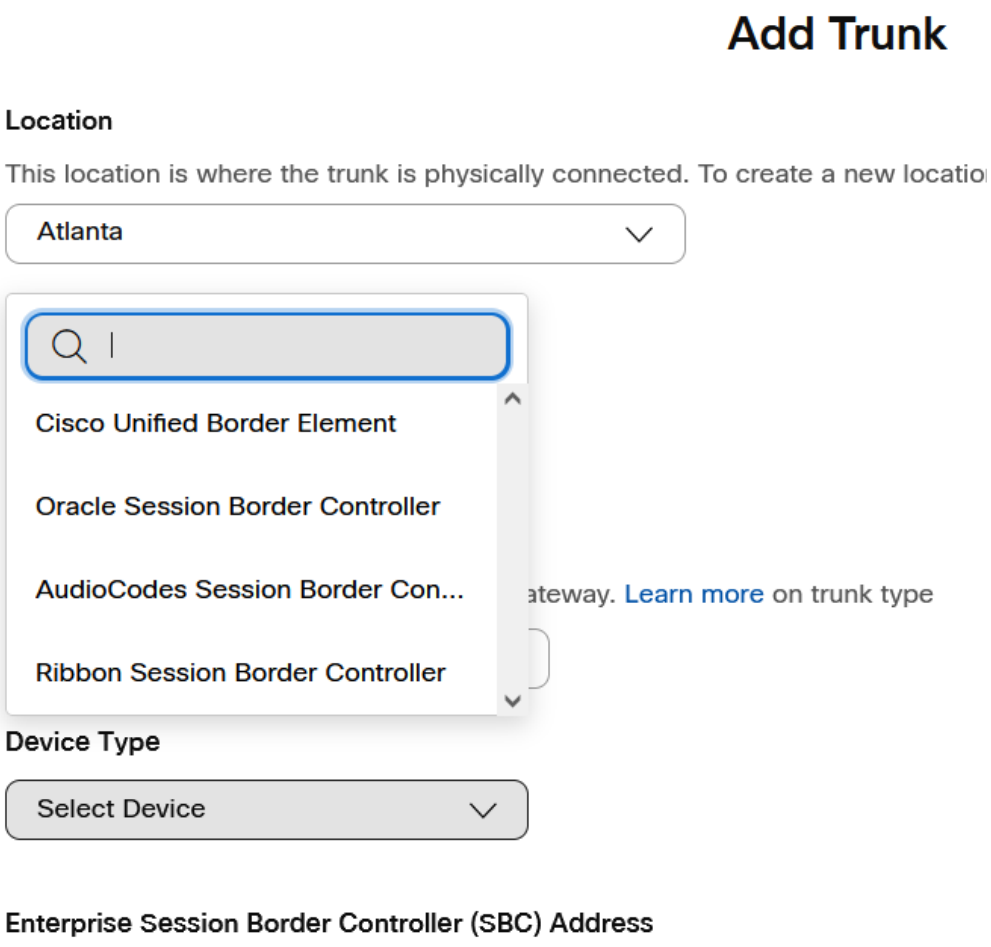
Oracle SBC support as Local Gateway

Oracle SBC is now

Certificate-based only

Oracle conducted tests with SBC 9.0 software – this on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6300
- AP 6350
- AP 3950 (Starting from SBC 9.0 version)
- AP 4900 (Starting from SBC 9.0 version)
- VME
- Oracle SBC on Public Cloud



Oracle SBC considerations

- The support is only for Certificate-based trunks not Registered trunks, this is by design and will be the case for all 3rd party SBCs.
- All Oracle SBC support and licensing is through Oracle/Oracle partners, not Cisco.
- ICE support is not immediately available, but it will be quickly supported with a SW update from Oracle on their SBCs.
- Oracle will make a Webex Calling Microsite but it's not ready yet, so we have the communities page for now.
- Configuration Guide

AudioCodes SBC support as Local Gateway

AudioCodes SBC is now supported as LGW

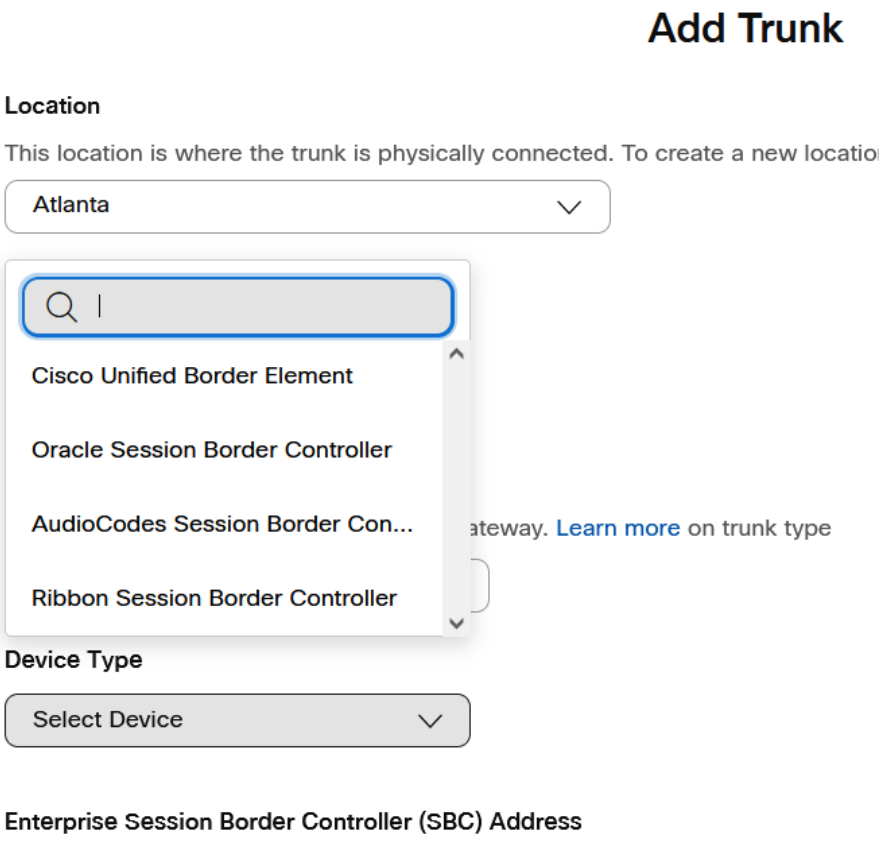
Certificate-based only

AudioCodes

- Mediant 500 Gateway & E-SBC
- Mediant 800B/C Gateway & E-SBC
- Mediant 1000B Gateway & E-SBC
- Mediant 2600 E-SBC
- Mediant 4000/B SBC
- Mediant 9000, 9030, 9080 SBC
- Mediant Software SBC (VE/SE/CE)

7.40A.250.440 or later

Configuration Guide



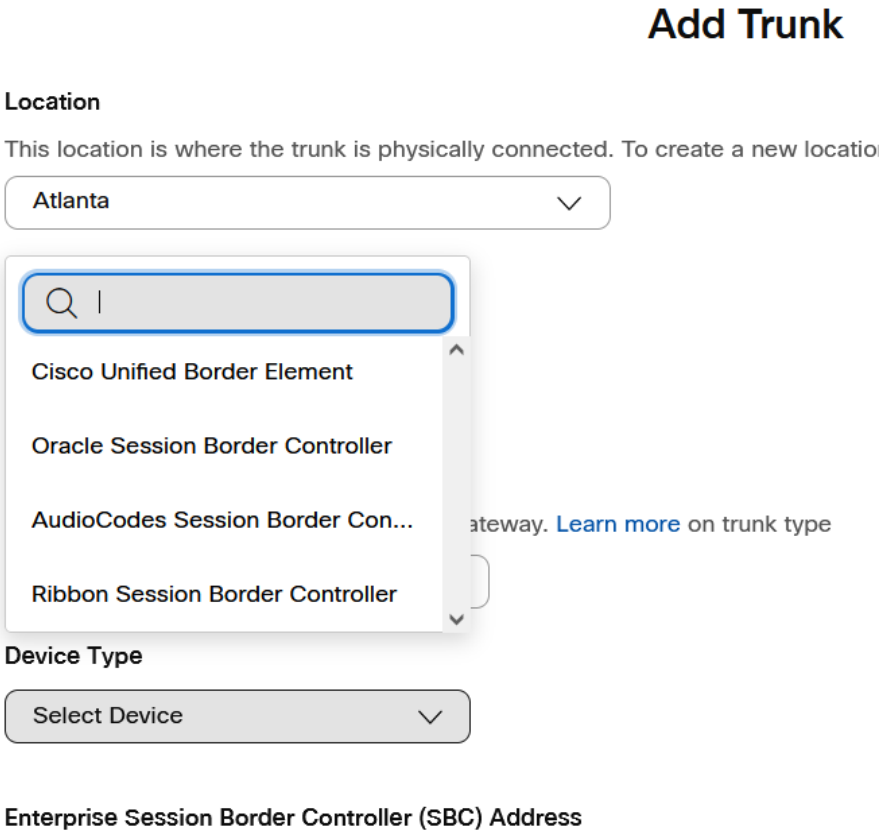
Ribbon SBC support as Local Gateway

Ribbon SBC is now supported as LGW

Certificate-based only

Ribbon Platform	Ribbon Code Version
SBC 5000	10.1.0
SBC 7000	
SBC SWe	

Configuration Guide



Agenda

- Local Gateway (LGW) overview and sizing
- Multiple Registration-based LGWs on a single CUBE
- Managing Gateways from the Webex Control Hub
- Introducing Certificate-based Local Gateway
- Configuring a Certificate-based Local Gateway
- 3rd Party SBC as a Local Gateway
- Resources

Resources

Resources

For more information take a look at the following resources:

- What's new in Webex Calling: https://help.webex.com/en-us/article/rdmb0/What's-new-in-Webex-Calling
- Trunk configuration guide: Webex Calling Trunks
- Configure Local Gateway on Cisco IOS XE for Webex Calling https://help.webex.com/en-us/article/jr1i3r/Configure-Local-Gateway-on-Cisco-IOS-XE-for-Webex-Calling
- https://help.webex.com/en-us/article/n0xb944/Configure-Trunks,-Route-Groups,-and-Dial-Plans-for-Webex-Calling

Resources

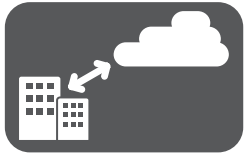
- Enroll Cisco IOS Managed Gateways to Webex Cloud
- Assign Services to Managed Gateways
- Validate Cisco Local Gateway Configuration through Control Hub
- Webex Integrations: Webex Integrations > Oracle
- Oracle SBC integration with Cisco Webex Calling as 3rd party Local Gateway (LGW) https://www.oracle.com/a/otn/docs/oracle-sbc-integration-with-cisco-webex-calling-v1.0.pdf

Additional sessions on IOS-XE UC

(CUBE, Local Gateway, Survivability Gateway)

- BROCOL-2314 Introducing vCUBE on Azure and CUBE v14 Updates
- **Room D203 – Tuesday 8:30AM – 9:30AM**

- BRKCOL-2312 High-Capacity Premises-based PSTN Option for Webex Calling
- **Room D201 – Wednesday 10:30AM – 11:30AM**



- BRKCOL-2993 Enabling Site Survivability for Webex Calling
- **Room Elicium 3 – Thursday 12:15PM – 1:15PM**

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!

CISCO Live!

ALL IN