

Bring Your Own PSTN Solution for Webex for Cisco BroadWorks

Modified: 08 April 2024



Change History

Version	Date	Change
1-36	08-Apr 2024	<ul style="list-style-type: none"> Added note that DNS-SRV is dynamic in nature and added wildcard to the IP Addresses.
1-35	10-Jan 2024	<ul style="list-style-type: none"> Rule 4 was added in Translation Profiles section.
1-34	22-Dec 2023	<ul style="list-style-type: none"> Updated Meeting Join using Callback (Optional), RoutingNE, Enable Webex Meeting Callback, Translation Profiles, and Cube Call Flows sections were updated.
1-33	04-Jul 2023	<ul style="list-style-type: none"> Updated Meeting Join using Callback (Optional) section.
1-32	02-Feb 2023	<ul style="list-style-type: none"> Added New domain for UK, and North Africa added under Webex Call Routing Domains. Added Meeting Host Session and Application Delivery Platform under Step 9: Provision Partner BroadWorks Configuration.
1-31	02-Feb 2023	<ul style="list-style-type: none"> Updated Apply updates to an in-service Phone Number Group/Callback DNS SRV Group section.
1-30	31-Jan 2023	<ul style="list-style-type: none"> Added Application Delivery Platform section under Application Server.
1-29	29-Nov 2022	<ul style="list-style-type: none"> Added Enable Webex Meeting Callback in Network Server section. Added Create a VoiceXML Meeting Callback Subscriber in Application Server section. Updated DNS SRV records under Webex Call Routing Domains.
1-28	27 July 2022	<ul style="list-style-type: none"> Minor updates to <i>Ports Used by Webex</i> to clarify port requirements. Updated SIP signaling port for traffic from CUBE to Webex Edge Audio to use port 5065 specifically.
1-27	18 July 2022	<ul style="list-style-type: none"> Updated certificate requirements to reflect IdenTrust certificate requirement for SBCs. QuoVadis is no longer supported.
1-26	08 March 2022	<ul style="list-style-type: none"> Updated <i>Step 6: Select the Primary Seed Solution Organization</i> with additional conditions when removing a seed organization
1.25	29 Oct 2021	<ul style="list-style-type: none"> Added Note for alternative method of loading certificates when you are using your own SBC and the prescribed method does not work Updated Webex Call Routing Domains to 'eccspx'
1.24	15 Oct 2021	<ul style="list-style-type: none"> Edited Edge audio port range in <i>Ports used by Webex</i> Minor edits throughout to clarify the following: <ul style="list-style-type: none"> Updated Seed organization overview Updated Provisioning task flow to clarify optional use cases such as when not deploying Callback, and when deploying your own SBC Updated step 10 to clarify requirements when deploying your own SBC Added section on Wildcard Certificates Edited text to clarify TLS and mTLS as requirements

Version	Date	Change
1.22	30 Sep 2021	<ul style="list-style-type: none"> Added Webex Call Routing domain for Australia and New Zealand.
1.21	13 Aug 2021	<ul style="list-style-type: none"> Edited NOTE in CUBE IP address range configuration. Removed redundant link.
1.20	10 Aug 2021	<ul style="list-style-type: none"> Updated IP address ranges for CUBE configuration. Directed readers to external Webex article for up to date IP address range.
1.19	14 July 2021	<ul style="list-style-type: none"> Minor correction to citation for <i>Bring Your Own PSTN Acceptance Procedure</i>
1.18	13 July 2021	<ul style="list-style-type: none"> Updated logo for Webex rebranding
1.17	02 July 2021	<ul style="list-style-type: none"> Added Webex Meetings Call Type configuration for controlling the charge indicator in the billing CDRs and Session Admission Control call processing behavior.
1.16	22 June 2021	<ul style="list-style-type: none"> Updated document to highlight that the Callback method of joining meetings with Callback DNS SRV Groups is optional. Retitled and updated for Webex rebranding Added IdenTrust root certificates to Trustpool certificates
1.14	18 June 2021	<ul style="list-style-type: none"> Added configuration for setting Maximum Segment Size (MSS) on CUBE Added section on G.722 Interoperability when leveraging your own SBC
1.13	09 June 2021	<ul style="list-style-type: none"> Added details on how to disable callback when creating or updating a Customer Template.
1.12	28 May 2021	<ul style="list-style-type: none"> Updated <i>Webex Call Routing Domains</i> to use DNS SRV for <code>_sips._tcp.<domain></code> Updated step 1 of <i>Provisioning</i> to include option to leverage your own SBC Updated <i>Network Server</i> topic with missing step for PreCallTyping instance
1.11	05 May 2021	<ul style="list-style-type: none"> Updated the limit for Callback SRV Group to 200
1.10	22 April 2021	<ul style="list-style-type: none"> Updated Webex Call Routing Domains with DNS SRV example. Updated Before You Begin in Step 9 to account for UDP support
1.9	14 April 2021	<ul style="list-style-type: none"> In <i>mTLS Configuration</i> section, added reference to the QuoVadis root certificate that is used for Webex Edge Audio
1.8	30 March 2021	<ul style="list-style-type: none"> Added locale tag to Contact sip header
1.7	16 March 2021	<ul style="list-style-type: none"> Added <i>Solution Configuration Overview</i> along with information on creating Seed Organizations.
1.6	02 March 2021	<ul style="list-style-type: none"> Added Before You Begin with TCP requirements for BroadWorks. Moved Call Processing heading up to capture call processing tasks that were included in Network Configuration. Added requirement to create a new template to Step 5. Edited CUBE port requirements Added NOTE to Step 2 Minor corrections to CUBE configs based on feedback
1.5	21 February 2021	<ul style="list-style-type: none"> Added SIP Profile Requirements. Updated CUBE requirements.

Version	Date	Change
1.4	10 February 2021	<ul style="list-style-type: none"> ▪ Added link to BYoPSTN Certification Procedure
1.3	05 February 2021	<ul style="list-style-type: none"> ▪ Added BYoPSTN Certification step
1.2	04 February 2021	<ul style="list-style-type: none"> ▪ Updated Webex link in Trustpoint section
1.1	02 February 2021	<ul style="list-style-type: none"> ▪ Additional edits and clarifications to CUBE configuration.
1.0	20 January, 2020	<ul style="list-style-type: none"> ▪ Initial draft

Contents

CHANGE HISTORY	2
CONTENTS	5
DEFINITIONS	7
OVERVIEW	8
ARCHITECTURE	9
MEETING JOIN USING CALL-IN	10
MEETING JOIN USING CALLBACK (OPTIONAL)	11
SOLUTION CONFIGURATION OVERVIEW	12
Seed Organizations	12
BYOPSTN CONFIGURATION ELEMENTS	14
PHONE NUMBER GROUP (PNG)	14
CALLBACK DNS SRV GROUP (CDSG)	15
CUSTOMER TEMPLATE	16
BROADWORKS CALLING CLUSTER	16
BYOPSTN CONFIGURATION ELEMENTS EXAMPLE	17
PORTS USED BY WEBEX	20
TLS AND SRTP CIPHER SUITES	20
AUDIO CODECS SUPPORTED	21
SIP AND RTP PROFILE REQUIREMENTS	21
WEBEX CALL ROUTING DOMAINS	22
NOTE: THE DNS-SRV IS DYNAMIC IN NATURE, THE IP ADDRESSES ARE PRONE TO CHANGE; THEREFORE, AVOID HARD-CODING OR BOOKMARKING THE IP ADDRESSES. REFER TO THE 'DOCUMENT REVISION HISTORY' SECTION FOR ANY CHANGES OR UPDATES MADE TO THE PORT REFERENCE INFORMATION FOR WEBEX CALLING DOCUMENT.	23
CUBE REDUNDANCY	23
DUPLEX CUBE DEPLOYMENT FOR BROADWORKS DEPLOYED IN SINGLE SITE	24
SIMPLEX CUBE DEPLOYMENT FOR BROADWORKS DEPLOYED IN MULTI-SITE	24
PROVISIONING	25
STEP 1: PARTNER PREREQUISITES	26

STEP 2: PROVISION PHONE NUMBER GROUPS (PNG) IN PARTNER HUB.....	26
STEP 3: PROVISION CALLBACK DNS SRV GROUPS (CDSG) IN PARTNER HUB (OPTIONAL).....	28
STEP 4: ASSOCIATE PNG AND CDSG TO CUSTOMER TEMPLATES IN PARTNER HUB	30
STEP 5: PROVISION SEED SOLUTION ORGANIZATIONS.....	32
STEP 6: SELECT THE PRIMARY SEED SOLUTION ORGANIZATION	33
STEP 7: DOWNLOAD BROADWORKS CONFIGURATION (BYoPSTN)	35
STEP 8: DETERMINE THE WEBEX EDGE AUDIO DNS SRV DOMAIN.....	38
STEP 9: PROVISION PARTNER BROADWORKS CONFIGURATION	39
Before you Begin.....	41
Application Server	41
VoiceXML Meeting Callback Virtual Subscriber	46
Meeting Host Session	47
Application Delivery Platform	47
Network Server	49
STEP 10: PROVISION PARTNER CUBE (OR YOUR OWN SBC)	55
Initial Configuration	55
Networking Configuration.....	56
Call Processing Configuration.....	57
mTLS Configuration	63
CUBE Logs	67
Other useful commands.....	68
STEP 11: BYoPSTN CERTIFICATION.....	68
APPLY UPDATES TO AN IN-SERVICE PHONE NUMBER GROUP/CALLBACK DNS SRV GROUP	69
G722 MEDIA INTEROPERABILITY WHEN USING YOUR OWN SBC.....	71
KNOWN LIMITATIONS.....	71

Definitions

Definitions	Description
Cisco Partner	An entity (generally a Service Provider) who sells Cisco Products and Services to their customers.
End Customer	Users who use the Cisco Products and Services sold to them by a Cisco Partner.
CUBE	Cisco Unified Border Element
Partner Organization	Webex Identity and Service Management repository that maintains information about Cisco Partners and their Customers.
Partner Hub	Web portal to provision Identity and Services for Cisco Partners and the customers they manage.
Customer Organization	Webex Identity and Service Management repository that maintains information about End Customer.
BroadWorks Enterprise or Service Provider / Group	Representation of the end customer in BroadWorks.

Overview

The Bring Your Own PSTN (BYoPSTN) solution lets Webex for Cisco BroadWorks Service Providers provision phone numbers that they own for users to use when joining Webex Meetings. The solution lets Partners leverage their own PSTN networks and make use of existing relationships with PSTN providers, rather than using Cisco-provided numbers.

The reference architecture in this document provides an end-to-end design for the BYoPSTN option. This architecture is validated by Cisco and uses Cisco Unified Border Element (CUBE) as the Session Border Controller (SBC) for call traffic between BroadWorks and Webex Meetings.

Choosing the Meeting Join Option

Currently, Webex for Cisco BroadWorks supports two options for provisioning meeting phone numbers. Service Providers must choose one of these two options—a mix is not supported:

- Cisco call-in numbers (Cisco PSTN)--Cisco provides the phone numbers that meeting participants can use to join meetings
- Partner provided call-in numbers (BYoPSTN)--Service Providers provide their own phone numbers to be used by meeting participants when joining meetings

BYoPSTN Solution

Partners who choose the Partner provided call-in numbers (BYoPSTN) option must provide their own PSTN phone numbers and must provision the network infrastructure that is required to route calls to and from Webex. The BYoPSTN solution facilitates routing calls Over the Top (OTT) via the public internet from BroadWorks to Webex.

The following conditions apply when selecting the BYoPSTN option:

- Cisco Partners may use the same phone numbers for more than one End Customer. These phone numbers can be in any country that the Partner operates.
- The BYoPSTN option requires no changes to the general onboarding process for Webex for Cisco BroadWorks customers.
- BYoPSTN requires provisioning at the Cisco Partner level and any End Customers that Partners activate after BYoPSTN is operational, are enabled automatically.
- All of the provisioning required for customer Meeting sites is automatic, as with the current generally available solution.
- Partners activating both Standard and Premium packages have two Meeting sites: one site for Standard users and another for Premium users. Both sites are enabled for BYoPSTN.
- Meeting participants who call in to meetings may choose to use Video and Content share via the internet.
- Applies to meeting joins for both Space meetings and PMR meetings. Note that for Space meetings, the space must have been created by a Standard or Premium user with Webex Meeting host capabilities in order to receive a PSTN access number—spaces created by Basic users do not receive PSTN access numbers.

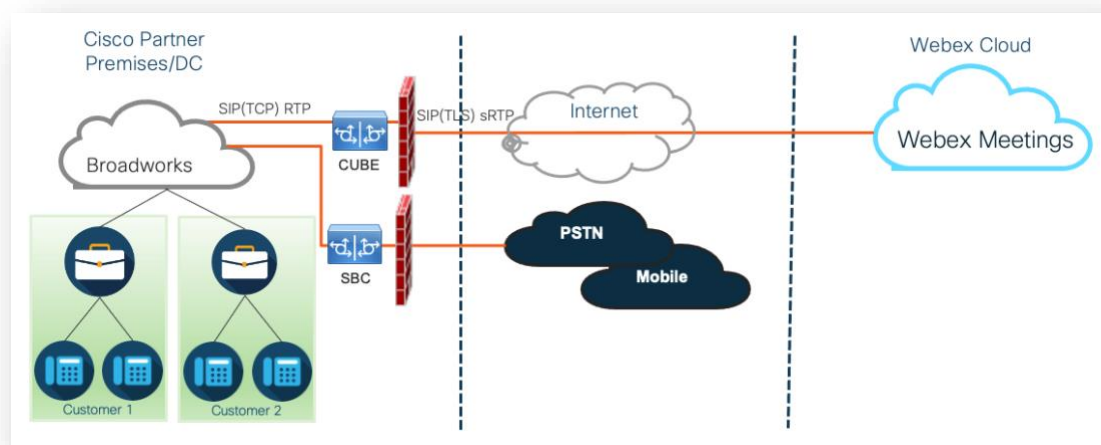
- This document provides a validated configuration that uses CUBE as your SBC. However, if you don't want to use CUBE, you can deploy your own SBC.

Architecture

The Webex for Cisco BroadWorks BYoPSTN solution builds on the Webex Edge set of services, more specifically, the Webex Edge Audio service available to Enterprise Customers. The architecture is adapted to integrate the Cisco Partners BroadWorks infrastructure with Webex Edge Audio, thereby enabling the Cisco Partner to centrally configure sets of phone numbers for use by their End Customers.

The main elements of the architecture are as follows:

- BroadWorks—Cisco Partners BroadWorks infrastructure
- Cisco Unified Border Element (CUBE)—Reference Session Border Controller (SBC) for the solution deployed in the Cisco Partners data center. The CUBE must be inside a DMZ. Note that if you don't want to use CUBE, you can deploy your own SBC.
- Webex Edge Audio—Webex service, which decouples the PSTN from Webex by changing the call routing to make use of the Cisco Partner provided infrastructure.



Calls by participants to join a meeting traverse through BroadWorks to CUBE and from CUBE to the Webex infrastructure in the cloud via the internet. This model is applicable for both of the following meeting join scenarios:

- **Call-in**—a participant dials the phone number in the meeting invite on either their BroadWorks registered handset, mobile device or on the Webex App. The call is initiated by BroadWorks.
- **Callback (optional)**—a participant requests that Webex call a phone number that the participant provides. The call is initiated by Webex.

Calls routed from BroadWorks to CUBE within the Partner infrastructure will use SIP TCP for call signaling and RTP for media. From CUBE to Webex, calls use SIP TLS for signaling and sRTP for media. Call routing from CUBE to WebEx is via the Internet and does not use a SIP Trunk.

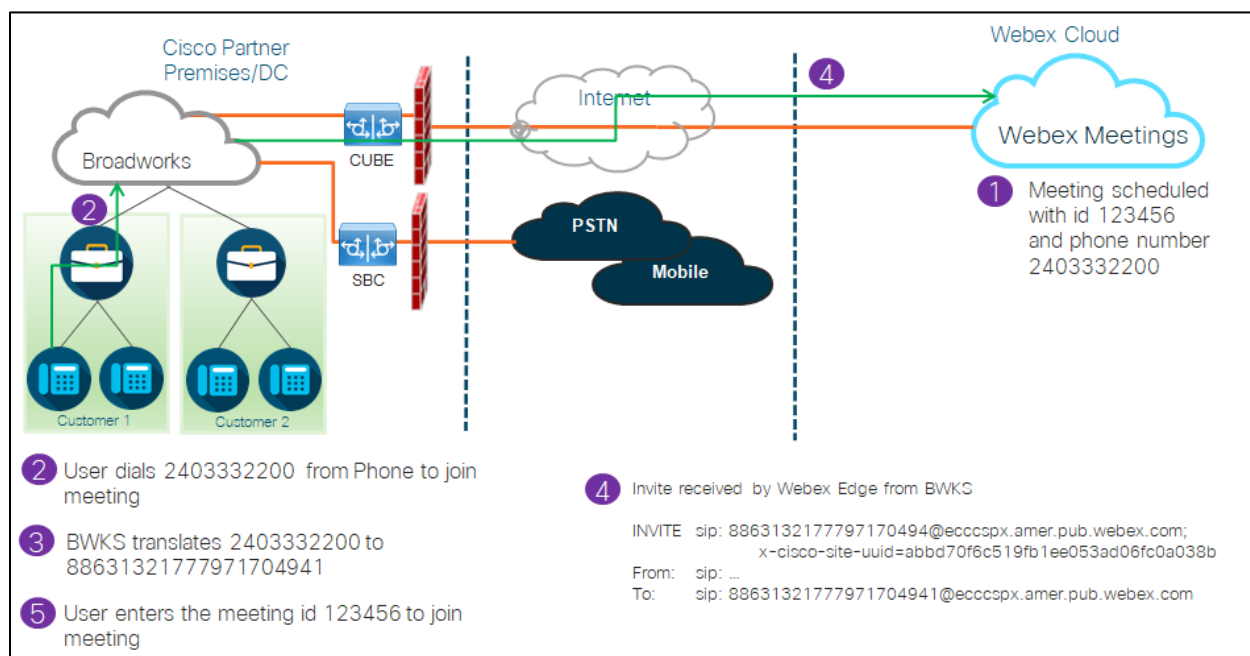
The typical setup for call-in/callback scenarios is as follows:

- Cisco Partner has a PSTN phone number (for example, 2403332200) and an associated Webex access code (for example, 88631321777971704941).
- Cisco Partner provisions a Virtual Subscriber on BroadWorks that corresponds to the CUBE device. The Partner maps the phone number to the access code and vice-versa.
- The access code, which is sent to Webex in the SIP messages, identifies the meeting sites associated with the Cisco Partner.
- The above phone number to access code mapping is configured once and is common to all End Customer meeting sites.
- Participants joining the meeting must enter the corresponding meeting id (for example, 123456), which identifies the specific meeting to join.

It is recommended that Partners follow the redundancy model outlined below.

Meeting Join using Call-in

The following picture depicts the process of a user who joins the meeting by call-in.



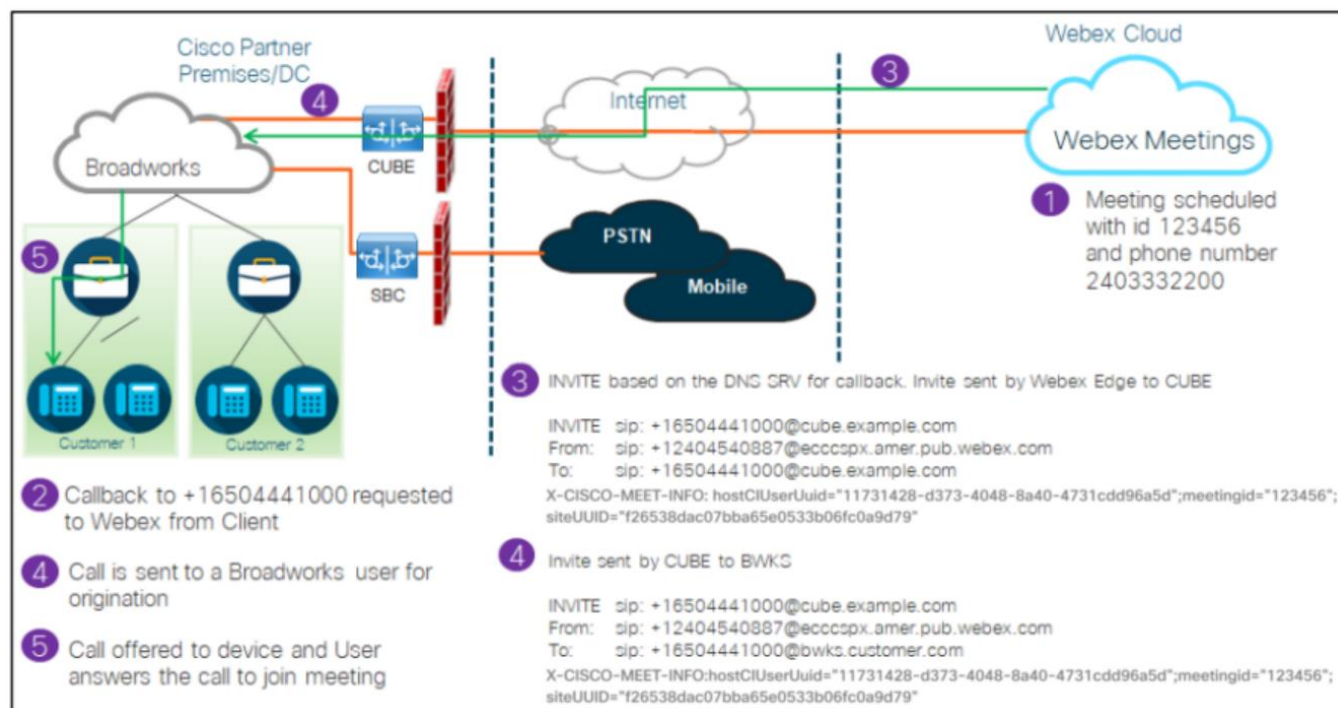
Here are the steps involved for the participant to join a meeting by call-in.

1. User schedules a meeting in Webex. Webex assigns a meeting id (for example, 123456).
2. User dials the Phone Number that is associated with the meeting (for example, 2403332200). The SIP INVITE carries the Request URI as the phone number associated to the meeting.
3. BroadWorks translates the Phone Number to an access code (for example, 88631321777971704941) associated to the Meeting site and routes the call to CUBE with the Request URI as the access code.

- Webex receives the SIP INVITE and answers the call. The language of the announcements is determined by the language specified for the Phone Number when it is provisioned in Cisco Partner Hub and BroadWorks
- User enters the meeting id (for example, 123456) using DTMF. Webex verifies the user and then lets the user join the meeting.

Meeting Join using Callback (Optional)

The following picture shows the process of a user who joins the meeting by call-back, the user requests a call from Webex to join a meeting.



Here are the steps involved for the participant to join a meeting by callback:

- User schedules a meeting in Webex. Webex assigns a meeting id (for example, 123456).
- User requests a call from Webex to their desired number (for example, +16504441000) to join the meeting using the Webex app or Meetings client.
- Webex initiates a SIP INVITE to CUBE based on the Callback DNS SRV group, provisioned in Cisco Partner Hub and BroadWorks. The SIP INVITE Request URI contains the phone number that must receive the call, (for example, +16504441000@cube.example.com).
- The CUBE SBC sends SIP INVITE request to the Broadworks NS. The NS redirects the call to Broadworks AS hosting the meeting host. The Broadworks AS receives the SIP INVITE from the CUBE SBC. The Broadworks AS identifies the meeting host using the CI UUID in the X-CISCO-MEET-INFO header. Additionally, Broadworks checks if VoiceXML Webex Meeting Callback subscriber is configured on the system.

5. Call is offered to the user requested Phone Number and user answers the call to join the meeting. This phone number can be a BroadWorks subscriber or a PSTN number. If the requested number is a PSTN number, BroadWorks uses the provisioned path to route the call to the PSTN.

For the Callback option, it is mandatory to activate the following two features:

- 102746 – BroadWorks Support for CI UUID
- 102074 – BYO PSTN Billing support for CallBack and CallIn

This can be confirmed from CLI as below:

```
AS_CLI/System/ActivatableFeature> get
```

Id Timestamp	Description	Activated	Last Modified
102746	BroadWorks Support for CI UUID	true	
102074	BYO PSTN Billing support for CallBack and CallIn	true	

For a detailed description of these features and activation can be found in the Section 'VoiceXML Meeting Callback Virtual Subscriber' in this document.

NOTE: If you choose not to configure the Meeting Join using Callback option, users can still use either the Call-in option to join meetings or they can join with computer audio. In this case, then you are not required to configure DNS SRV Callback Groups.

Solution Configuration Overview

The solution has several different components, each of which must be configured correctly for the solution to operate successfully. The components are as follows:

- BroadWorks
- CUBE (or an alternative SP Certified Session Border Controller (SBC))
- Webex Edge Audio

There are inter-dependencies between the configuration of these different components and as such one or more solution seed organizations are required to complete the required solution configuration and verification.

Seed Organizations

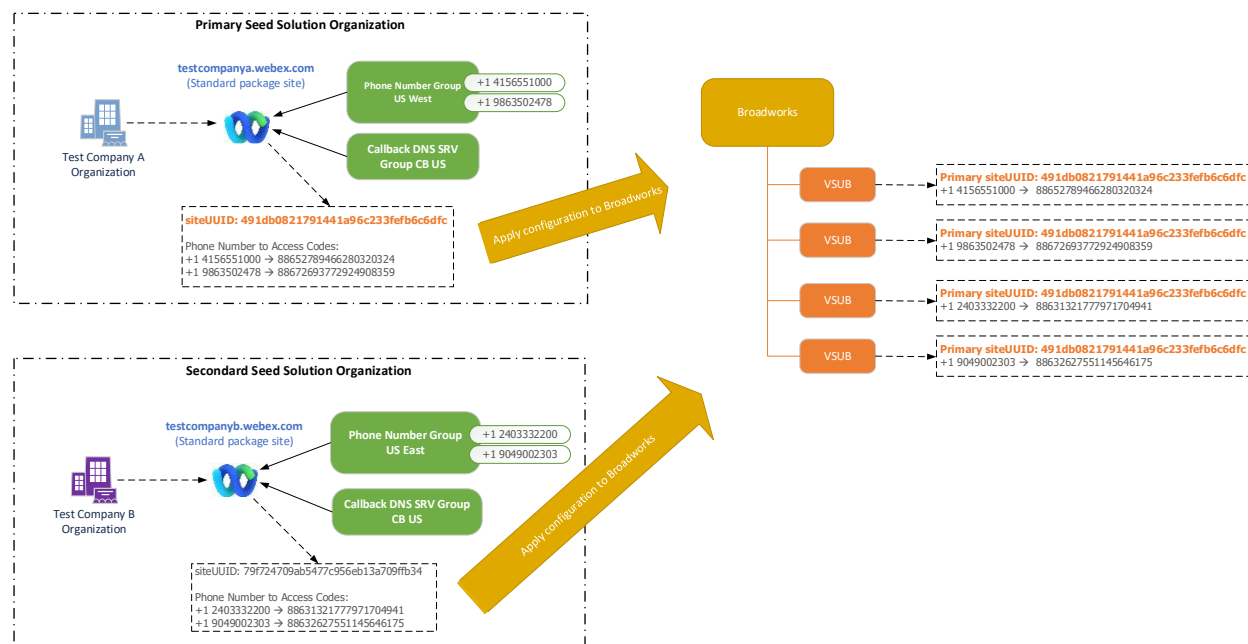
A seed organization is a Webex Organization that you configure to generate and validate settings for the BYoPSTN solution. The seed organization must have at least one user assigned a **Standard package**, and that Standard package must use the **Partner provided call-in numbers (BYoPSTN)** meeting join option. It is recommended that you associate the seed organization with a test BroadWorks Service Provider or Enterprise.

The solution seed organizations serve two purposes:

- 1) **Seed configuration:** the provisioning of the seed organization(s) generates phone number to meeting access codes mappings and a meeting site universally unique identifier (site UUID) that are required for

the on-going operation of the solution. This information is required to configure BroadWorks Virtual Subscribers (VSUB).

2) **Configuration validation:** use the seed organization to determine if your BYoPSTN solution is configured in accordance with your requirements. Use the seed organization and test users to validate meeting call-in and callback use cases using the Partner provided call-in numbers and DNS SRV Callback records (if callback is enabled).



The administrator must generate a seed solution organization for each unique set of phone numbers and DNS SRV callback records. The generation of the seed solution organization in each case, generates the required phone number to meeting access code mappings and the capability to verify the associated meeting call-in and callback use cases for those phone numbers and callback DNS SRV records.

The administrator, using Cisco Partner Hub must select one seed solution organization as the **primary seed solution organization**. The meeting site UUID of the Standard package meeting of this primary seed solution organization must be configured on BroadWorks. It is critical that this meeting site remains provisioned as this site UUID is sent in each call-in meeting join request as an authentication token. This single site UUID is shared by all sets of phone numbers and callback DNS SRV records. Multiple site UUID values are not required.

The primary and any secondary seed solution organizations can be deleted, if desired prior to the set of phone numbers and callback DNS SRV records being assigned to non-test customers. When the set of phone numbers and callback DNS SRV records are assigned to any non-test customers, those phone numbers and callback records are associated with meeting sites for those customers and are in use for meeting join using call-in and callback. Any changes should be considered as service impacting.

The subsequent sections provide more details on the different configuration elements.

BYoPSTN Configuration Elements

A key element of the solution is the configuration of Cisco Partner phone numbers and DNS SRV callback records. BYoPSTN uses Phone Number Groups and Callback DNS SRV Groups as a way of assigning geographically based phone numbers and redundant call routing for Webex meetings. These elements are assigned to End customers by the Customer Template.



Phone Number Group (PNG)

Cisco Partners provision the Phone Numbers used by participants to join Meetings in Cisco Partner Hub. These Phone Numbers are arranged together into a Phone Number Group. The list of Phone numbers is associated to a Meeting site. All Personal Meeting Rooms (PMR) and scheduled meetings in that Meeting site use the associated Phone Numbers. The following is an example of a Phone Number Group:

Phone Number Group: US East

Phone Number Name	Country	Country Code	Phone Number	Announcement	Toll Type	Call-in Priority
US Maryland	US	+1	2403332200	English	Toll	Primary
US Florida	US	+1	9049002303	English	Toll	Secondary
US New York	US	+1	8056504578	English	Toll Free	None

Phone Numbers have the following attributes:

- Phone Number Name—Name to describe the phone number
- Country—Country to which the phone is assigned
- Country Code—Country calling code or country dial-in code
- Phone Number—The phone number to use to join a meeting without the country code
- Announcement—Language of the announcement to be played when a participant is joining a meeting
- Toll Type—The type of number: Toll or Toll free

- **Call-in priority**—The priority assigned to the meeting numbers. The participants view of the meeting join numbers is ordered based on this priority.

Default Phone Numbers: Administrators can assign a Call-in Priority of Primary, Secondary or None to a phone number in the Phone Number Group. The phone numbers with a priority of Primary or Secondary are default phone numbers. The default phone numbers are sent in the meeting invite emails and are listed in the priority order that participants should use to join meetings. The default phone numbers are not required to be in the same country. A primary phone number must be selected, a secondary phone number is optional. At least one of the default phone numbers must of type Toll.

End Customer users can choose to specify their own default phone numbers using the meeting site web interface. These numbers appear for that user and their participants when they are the meeting host. If the user joins a meeting as an attendee, they'll appear only for them.

As per the example above, the Cisco Partner administrator provisions **US Maryland** as the primary and **US Florida** as secondary, these are the default phone numbers. A user may choose to override this in their meetings by changing the primary to **US New York** and secondary as **US Maryland**.

The maximum number of phone numbers for a given Phone Number Group is 98.

NOTE: It is not supported to configure a dedicated number for a single enterprise.

Callback DNS SRV Group (CDSG)

To allow meeting participants to choose the callback option, a Callback DNS SRV Group is required that points to the CUBE instance(s) within the Cisco Partner's network. Webex uses these records to route the callback via CUBE to BroadWorks, which can then place the meeting callback to the meeting participant's phone number.

Following is an example of a Callback DNS SRV Group.

Callback DNS SRV Group Name: Global CB

Country/Region	Country Code	DNS SRV Record
United States	+1	cube.us.example.com
Mexico	+52	cube.mx.example.com
All other countries	N/A	cube.global.example.com

Callback DNS SRV records have the following attributes:

- **Country/Region:** The country or region for which this DNS SRV Record should be used to send call requests.
- **Country Code:** The country code associated with the Country/Region. You can only have one DNS SRV record per country code.
- **DNS SRV Record:** The DNS SRV record for the Cisco Partner CUBE instance(s).

When the participant requests a call on their specified phone number, Webex uses the Callback DNS SRV associated with the country code for the specified phone number to route the call to the appropriate elements in the Cisco Partners network.

Using a DNS SRV record in this way provides support for redundant CUBE instances to service the call requests from Webex. In the example above, when meeting participants in the US request a callback from Webex to their US phone number, Webex uses the DNS SRV `cube.us.example.com` to route that call to the Cisco Partner's network. When Meeting participants in Mexico request a callback from Webex to their Mexico phone number, Webex will use the DNS SRV `cube.mx.example.com` to route that call to the Cisco Partner's network.

For any Country/Regions that do not have a specific Callback DNS SRV record, those call requests route to the '**All other countries**' DNS SRV record. The administrator must configure an 'All other countries' DNS SRV record.

The maximum number of records for a given Callback DNS SRV Group is 200.

Customer Template

The Customer Template is an existing concept for the Webex for BroadWorks solution. The template provides the default configuration that is used to provision an End Customer. BYoPSTN provides additional attributes to the Customer Template:

- Meeting Join Type—Can be either Cisco call-in numbers or Partner provided call-in numbers. This attribute indicates the phone numbers that are configured for meeting sites associated with the Standard and Premium packages. Partner provided call-in numbers should be selected by the administrator.
- Phone Number Group—Associated with Partner provided call-in numbers option only, this attribute indicates the phone numbers that are used by End Customers that are provisioned for Standard and Premium packages when joining meetings.

Callback DNS SRV Group—Associated with Partner provided call-in numbers option only, this attribute indicates the DNS SRV records that are used by Webex when calling back to End Customers that are provisioned for Standard and Premium packages when joining meetings. If you do not want to enable callback, you can choose "Disable Callback" when creating or updating a customer template. When the first subscriber for either Standard or Premium is provisioned for an End Customer, the associated package meeting site is provisioned. The package meeting site is provisioned as per the above Customer Template. Any subsequently provisioned subscriber for either Standard or Premium is added to the already provisioned meeting site—the meeting site configuration is not changed.

Any changes to the Customer Template with respect to the above attributes apply only to newly provisioned package meeting sites. Existing meeting sites, already provisioned, are unaffected by changes to the Customer Template.

The one notable exception is that if an End Customer already has a package meeting site, any new package meeting site is provisioned using the same Meeting Join Type as the existing package meeting site. For example, if an End Customer has a Standard package meeting site using Cisco call-in numbers and the Customer Template is updated to use Partner provided call-in numbers, a new Premium package meeting site is provisioned using Cisco call-in numbers, the Customer Template setting does not apply. The Standard and Premium meeting sites for a given End Customer shall always be provisioned consistently.

BroadWorks Calling Cluster

Cisco Partner Hub - BroadWorks Calling Cluster screen provides access to view and/or download the

BroadWorks configuration (BYoPSTN) information. The BYoPSTN configuration information for a given cluster includes the following data:

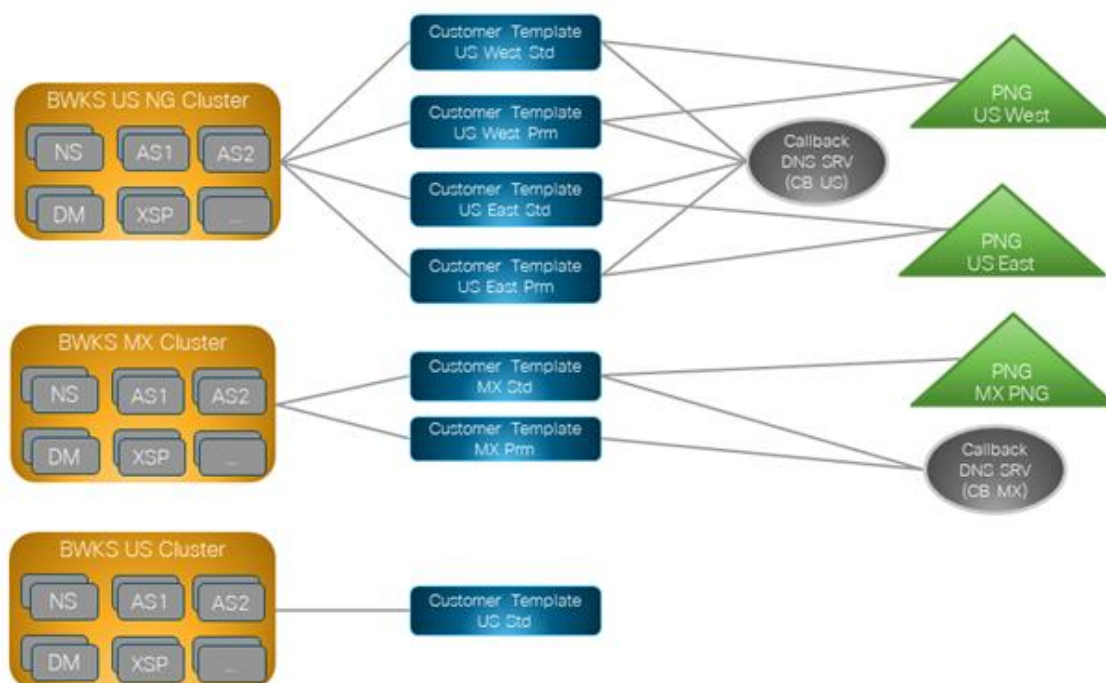
- Primary Seed Solution Organization details including the Standard package meeting site UUID and site URL
- Phone Number Group details for all groups configured for this cluster. This includes the phone number to meeting access code mappings for each group. Note the details should include groups that are associated with all secondary seed solution organizations.
- Callback DNS SRV Group details for all groups configured for this cluster. Note the details should include groups that are associated with all secondary seed solution organizations.
- Customer Template details for those templates using any of the Phone Number Groups and Callback DNS SRV Groups

Each BroadWorks Calling Cluster has its own *BroadWorks configuration (BYoPSTN)* information specifically its assigned Phone Number Groups and Callback DNS SRV Group. However, please note that all BroadWorks Calling Cluster share the same Primary Seed Solution Organization and as such all include the same the Standard package meeting site UUID and site URL.

The *BroadWorks configuration (BYoPSTN)* information is only available for view/download when the administrator configures and selects the Primary Seed Solution Organization. The primary seed solution organization must have at least one user assigned to the Standard package and that Standard package must use the Partner provided call-in numbers (BYoPSTN) meeting join option.

BYoPSTN Configuration Elements Example

The following image shows an example of a multi-cluster BroadWorks deployment with geographically based customer templates, phone numbers and routing.



The first table shows a multi-cluster BroadWorks deployment with regionally based Customer Templates, Phone Number Groups and Callback DNS SRV groups. The subsequent tables expand on the Phone Number Group and Callback DNS SRV Groups

BroadWorks Cluster	Template Name	Package	Meeting Join Type	Phone Number Group	Callback DNS SRV Group
BWKS US NG	US West Std	Standard	Partner provided call-in numbers	US West	CB US
	US West Prm	Premium			
	US East Std	Standard		US East	
	US East Prm	Premium			
BWKS MX	MX Std	Standard	Partner provided call-in numbers	MX PNG	CB MX
	MX Prm	Premium			
BWKS UK	UK Std	Standard	Partner provided call-in numbers	UK PNG	Callback Disabled
	UK Prm	Premium			
BWKS US	US Std	Standard	Cisco call-in numbers	None	None

- Subscribers provisioned using the US West Std or US West Prm template use the US West Phone number when joining meetings. Those subscribers meeting join callback requests are sent to the CB US DNS SRV records.
- Subscribers provisioned using the US East Std or US East Prm template use the US East Phone number when joining meetings. Those subscribers meeting join callback requests are sent to the CB US DNS SRV records.
- Subscribers provisioned using the MX Std or MX Prm template use the MX PNG Phone number when joining meetings. Those subscribers meeting join callback requests are sent to the CB MX DNS SRV records.
- Subscribers provisioned using the UK Std or UK Prm template use the UK PNG Phone numbers when joining meetings. Those subscribers will not be offered meeting join via callback as callback is disabled.
- Subscribers provisioned using the US Std are using Cisco call-in numbers and therefore have no Phone Number Group or Callback DNS SRV Group assigned. These subscribers use Cisco provided phone numbers for meeting joins and Cisco DNS SRV records for meeting joins using callback.

Details of the example Phone Number Groups are as follows:

Phone Number Group	Phone Number Name	Country	Country Code	Phone Number	Announcement	Toll Type	Call-in Priority
US West	US San Francisco	US	+1	4156551000	English	Toll	Primary
	US Palo Alto	US	+1	9863502478	English	Toll Free	None
US East	US Maryland	US	+1	2403332200	English	Toll	Primary
	US Florida	US	+1	9049002303	English	Toll	Secondary
	US New York	US	+1	8056504578	English	Toll Free	None
MX PNG	Mexico	MX	+52	2065304086	European Spanish	Toll	Primary
UK PNG	UK	UK	+44	4527789651	English	Toll	Primary

Details of the example Callback DNS SRV Groups are as follows:

Callback DNS SRV Group	Country	DNS SRV
CB US	US	cube.us.example.com
	All Other Countries	cube.row.example.com
CB MX	MX	cube.mx.example.com
	All Other Countries	cube.row.example.com

The configuration for the US DNS SRV record, `cube.us.example.com` may be as in the example:

<code>_sips._tcp.cube.us.example.com</code>	86400	IN	SRV	10	10	5061	<code>cube01.us.example.com</code>
<code>_sips._tcp.cube.us.example.com</code>	86400	IN	SRV	10	10	5061	<code>cube02.us.example.com</code>

This DNS SRV record may resolve to the following DNS A record:

<code>cube01.us.example.com</code>	86400	IN	A	45.84.168.81
<code>cube02.us.example.com</code>	86400	IN	A	45.84.168.82

NOTE: The DNS SRV records resolve to secure SIP calls from Webex to CUBE.

Ports used by Webex

The ports in the table below must be opened on the firewall of the DMZ where the CUBE resides, and other ports can be closed. For additional information on ports and network requirements, refer to the following article:

<https://collaborationhelp.cisco.com/article/WBX264>

Source	Source Ports	Destination	Destination Ports	Protocol	Description
Webex Edge Audio Services	Ephemeral	CUBE	5061	TCP	(mTLS 1.2) Inbound SIP signaling from Webex Edge Audio to CUBE SBC. NOTE: CUBE SBC requires specifically the use of port 5061. The use of other ports in the range from 5060-5070 may be supported by other SBCs.
Webex Edge Audio Services	4000-4010	CUBE	5061	TCP	(mTLS 1.2) Options Ping for Webex Edge Audio.
CUBE	Ephemeral	EdgeAudio	5065	TCP	(mTLS 1.2) Outbound SIP signaling for Webex Edge Audio.
Webex Edge Audio Services	Ephemeral	CUBE	Ephemeral ports 8000-59999	UDP	(SRTP) Firewall pinholes need to be opened up for incoming media traffic to Edge audio.
CUBE	Ephemeral ports 10200 - 28000	Edge Audio	Ephemeral	UDP	(SRTP) Firewall pinholes need to be opened up for outgoing media traffic to CUBE.

TLS and sRTP Cipher Suites

TLS v1.2 or higher is used for mTLS handshake, and the following ciphers are supported by Webex Edge Audio (during Call-Back, Webex Edge Audio offers these in the TLS Handshake's Client Hello):

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

The following ciphers are used for sRTP:

- AEAD_AES_256_GCM.
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Audio Codecs Supported

- G722
- G711 μ
- G711a

SIP and RTP Profile Requirements

The Solution requires that between CUBE (or your SBC) and Webex, you deploy SIP TLS for signaling and sRTP for media.

The SIP and RTP profiles as part of this communication should conform to the following requirements:

SIP Profile Requirements	Details
Session Expiry Timer	2220 sec (accept SIP 422) * is adjusted per business need and 422 is expected.
Media Offer for ingress	Early Offer
Media Offer for egress	Late Offer
Options ping interval	30s (Minimum)
DTMF	RFC2833 Payload 101 (No Acoustic DTMF!)
SIP – UDP ports	4000-4010,5061,5065

RTP Profile	Details
Voice payload profile	G.722/ G.711μ /G.711a
Packet size	20ms
VAD (Voice Activity Detection)	No
Media inactivity timer	1200 ms
Mid dialog codec change	Not accepted
RTP	8000-48198
sRTP Ciphers	AEAD_AES_256_GCM AEAD_AES_128_GCM AES_CM_128_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_32

Note: G.729 codec is not supported. If you want to use G.729, you must use transcoders.

Webex Call Routing Domains

The DNS SRV `_sips._tcp.<domain>` is used to reach Webex Edge Audio. There are four domains depending on the region:

Region	Domain
Americas	ecccspx.amer.pub.webex.com
UK, North Africa	ecccspx.emea.pub.webex.com
Asia Pacific	ecccspx.apac.pub.webex.com
Australia / New Zealand	ecccspx.anz.pub.webex.com
Europe	ecccspx.euro.pub.webex.com

The DNS SRV resolves to several A records pointing to the primary and secondary site. The following table provides an example for the AMER region and is subject to change in the future.

Record Type	Record	Target	Purpose
SRV	<code>_sips._tcp.ecccspx.amer.pub.webex.com</code>	<code>ecccspxpr1.amer.pub.webex.com</code>	Discovery of Webex Edge Audio
SRV	<code>_sips._tcp.ecccspx.amer.pub.webex.com</code>	<code>ecccspxpr2.amer.pub.webex.com</code>	Discovery of Webex Edge Audio
SRV	<code>_sips._tcp.ecccspx.amer.pub.webex.com</code>	<code>ecccspxsc1.amer.pub.webex.com</code>	Discovery of Webex Edge Audio

Record Type	Record	Target	Purpose
SRV	_sips._tcp.ecccspx.amer.pub.webex.com	ecccspxsc2.amer.pub.webex.com	Discovery of Webex Edge Audio
A	ecccspxpr1.amer.pub.webex.com	207.182.174.101*	Points to Webex Edge Audio AMER Primary 1
A	ecccspxpr2.amer.pub.webex.com	207.182.174.102*	Points to Webex Edge Audio AMER Primary 2
A	ecccspxsc1.amer.pub.webex.com	207.182.174.229*	Points to Webex Edge Audio AMER Secondary 1
A	ecccspxsc2.amer.pub.webex.com	207.182.174.230*	Points to Webex Edge Audio AMER Secondary 2

Note: The DNS-SRV is dynamic in nature, the IP addresses are prone to change; therefore, avoid hard-coding or bookmarking the IP addresses. Refer to the 'Document Revision History' section for any changes or updates made to the [Port Reference Information for Webex Calling](#) document.

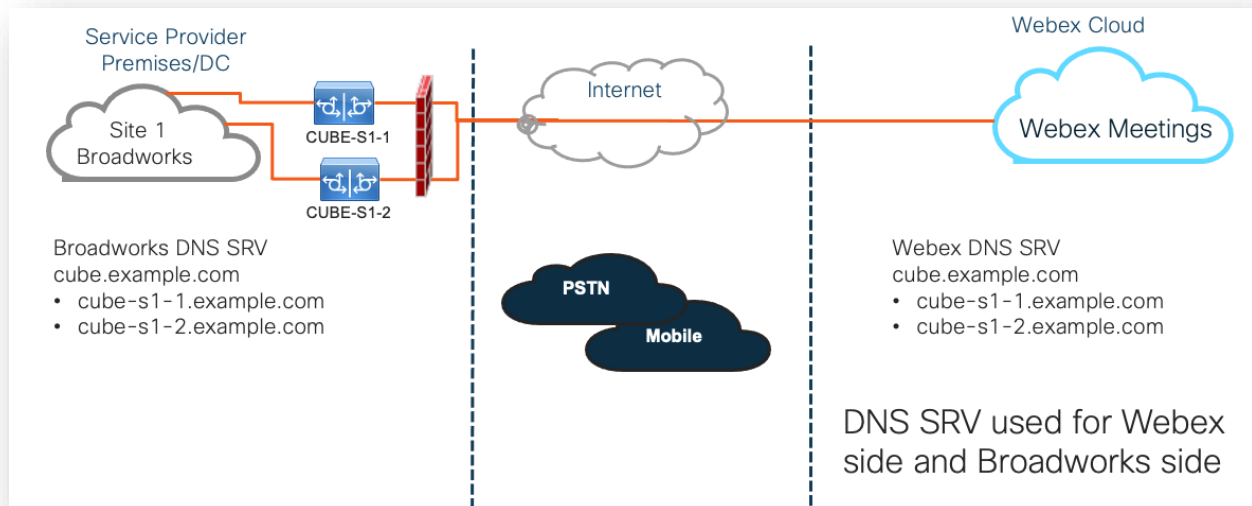
CUBE Redundancy

Cisco Unified Border Element (CUBE) enables the Session Border Control capability in a network managing SIP connections between external entities and internal network. More information about CUBE is available in Prerequisites section below.

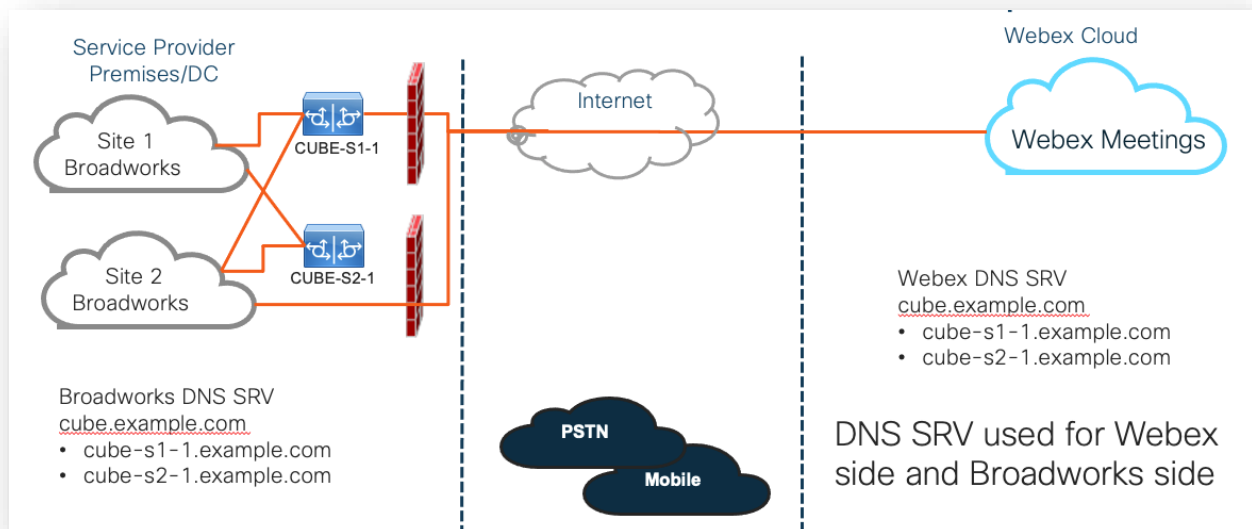
The redundancy models supported are defined with the purpose of providing High Availability and eliminating single-point-of-failure for the Cisco Partner. Three different models are outlined below. Cisco Partners should adopt whichever model is applicable to their environment.

During onboarding process partner should disable ICMP filters.

Duplex CUBE Deployment for BroadWorks deployed in Single Site



Simplex CUBE Deployment for BroadWorks deployed in Multi-Site



One more redundancy model is possible where CUBE is deployed in duplex mode in every site. This model is not necessary considering that BroadWorks is deployed with geo-redundancy.

Provisioning

Cisco Partners are required to deploy and manage the required infrastructure mentioned above for enabling BYoPSTN in their network. The following steps are required to provision and enable BYoPSTN for a Cisco Partner.

1.Partner Prerequisites	<ul style="list-style-type: none">•Deploy BroadWorks System•Deploy CUBE for Webex Edge Audio or leverage your own SBC
2. Provision Phone Numbers in Cisco Partner Hub	<ul style="list-style-type: none">• Provision Phone Number Groups to be associated with Customer templates
3. Provision Callback DNS SRV Groups in Cisco Partner Hub (Optional)	<ul style="list-style-type: none">•If you want to deploy Meeting Join via Callback, provision Callback DNS SRV groups and update your DNS settings. Otherwise, you can skip this step.
4. Associate PNG (and CDSG) to Customer Templates	<ul style="list-style-type: none">•Associate Phone Number Groups and Callback DNS SRV Groups (only if Meeting Callback is deployed) to your Customer Templates.
5. Provision Seed Solution Organizations	<ul style="list-style-type: none">•Provision a test Service Provider or Enterprise for Webex For BroadWorks using each of the Customer Templates• Provision a subscriber with a Standard package that uses Partner Provided call-in numbers meeting join option
6. Select the Primary Seed Solution Organization	<ul style="list-style-type: none">•Select a single primary seed solution organization for BYoPSTN
7. Download the BroadWorks configuraion (BYoPSTN)	<ul style="list-style-type: none">•Download the JSON file from Cisco Partner Hub which contains the information needed to configure BroadWorks
8. Determine the Webex Edge Audio DNS SRV domain	<ul style="list-style-type: none">•Identify the Webex Edge Audio DNS SRV domain
9. Provision Partner BroadWorks Configuration	<ul style="list-style-type: none">•CUBE Virtual Subscriber Configuration•Apply the Phone Number to access code mapping, from downloaded JSON file, in Virtual Subscribers•Network Server Configuration
10. Provision Partner CUBE (or your own SBC)	<ul style="list-style-type: none">•Follow validated configuration to provision CUBE as your SBC•Alternative. If you don't want to use CUBE, provision your own SBC using the CUBE configuration as a high-level guide
11. BYoPSTN Certification	<ul style="list-style-type: none">•Complete acceptance tests for certification.

Step 1: Partner Prerequisites

The following prerequisites must be completed for the provisioning of BYoPSTN. The prerequisites given below assume that the Partner has a working Webex for Cisco BroadWorks deployment that includes:

- Functioning BroadWorks System – as documented in the *Webex for Cisco BroadWorks Solution Guide*
- BroadWorks AS license with “VoiceXML” service in sufficient quantity (1 per PSTN number)
- BroadWorks patches required:
 - For R22:
 - AP.xsp.22.0.1123.ap376935
 - AP.as.22.0.1123.ap376935
 - For R23:
 - AP.xsp.23.0.1075.ap376935
 - AP.as.23.0.1075.ap376935
 - For R24:
 - AP.as.24.0.944.ap376935
- Cisco CUBE System deployed (IOS Version 16.12.2 or higher):
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book.html>

Both hardware-based and virtual CUBE is supported. Hardware based CUBE is recommended for scalability and handling larger numbers of calls.

- Webex Partner organization – as outlined in the *Webex for Cisco BroadWorks Solution Guide*

If the Partner is performing a brand-new deployment, all the prerequisites in the Webex for Cisco BroadWorks Solution guide must be completed before starting on the following.

Step 2: Provision Phone Number Groups (PNG) in Partner Hub

The procedure the Cisco Partner uses to add their Webex meeting call-in phone numbers is as follows:

1. Login to Cisco Partner Hub.
2. Go to **Settings**.
3. Scroll to **BroadWorks Calling**.
4. Under **Meeting Join configuration (BYoPSTN)**, select **Create Call-in Phone Number Group**.
5. Enter the **Phone Number Group** name and select **Next**.
6. Enter the **Phone Number** details and select **Next**.
7. Review the Phone Number Group details summary and select **Save**.
8. Repeat this procedure for each Phone Number Group to be added

The screenshots below illustrate the procedure.

BroadWorks Calling

Clusters

2 active clusters

View Clusters

Add Cluster

Templates

7 active templates

View Templates

Add Template

Meeting join configuration (BYoPSTN)

When providing Webex meeting call-in numbers, phone number and callback DNS SRV groups must be created. A group will become active when assigned to a template.

Call-in phone number groups

3 active groups

View groups

Create group

Callback DNS SRV groups

3 active groups

View groups

Create group

Partner Configuration Resources

Download Webex CA certificate 1

Create a call-in phone number group

Group name

Phone numbers

Summary

Call-in phone number group name

Enter a new, unique name for the group.

US East

Next

Create a call-in phone number group

Group name

Phone numbers

Summary

Call-in phone numbers

Add your own call-in phone numbers for users joining Webex meetings. Add at least one primary default call-in number.

Phone number name	Country / region	Country Code	Phone number	Announcement	Toll type	Call-in priority
US Maryland	United States of America	+1	2403332200	English (United States)	Toll	Primary
US Florida	United States of America	+1	9049002303	English (United States)	Toll	Secondary
US New York	United States of America	+1	8056504578	English (United States)	TollFree	None

Add another call-in phone number

Back

Next

Group name

Phone numbers

Summary

Summary

Please review the call-in phone numbers group settings to make sure they are correct. Click "Save" to confirm or "Back" to make changes.

Call-in phone number group name

US East

Call-in phone numbers

Phone number name	Country / region	Country code	Phone number	Announcement	Toll type	Call-in priority
US Maryland	United States of America	+1	2403332200	English (United States)	Toll	PRIMARY
US Florida	United States of America	+1	9049002303	English (United States)	Toll	SECONDARY
US New York	United States of America	+1	8056554578	English (United States)	TollFree	NONE

Back

Save

Step 3: Provision Callback DNS SRV Groups (CDSG) in Partner Hub (Optional)

NOTE: This step is to be completed only if you want to deploy the Meeting Join via Callback option. Otherwise, you can skip this step.

NOTE: If you do not configure this option, users can use the Call-in option to join meetings, or can join with computer audio.

When you use the Meeting Callback option, a Callback DNS SRV Group is required to route calls from Webex to CUBE. The procedure the Cisco Partner uses to add their CUBE DNS SRV records to Webex is as follows:

1. Login to Cisco Partner Hub.
2. Go to **Settings**.
3. Scroll to **BroadWorks Calling**.
4. Under **Meeting Join configuration (BYoPSTN)**, select **Create callback DNS SRV Group**.
5. Enter the Callback DNS SRV **Group name**.
6. Select **Next**
7. Enter the Callback DNS SRV details.
8. Select **Next**.
9. Review the Callback DNS SRV details summary.
10. Select **Save**.
11. Provision any updates to DNS to reflect the new records in the DNS SRV group
12. Repeat this procedure for each Callback DNS SRV Group to be added

The screenshots below illustrate the procedure.

Create a callback DNS SRV group

Group name

DNS SRV records

Summary

Callback DNS SRV group name

Enter a new, unique name for the callback DNS SRV group.

Global CB

Next

Create a callback DNS SRV group

Group name

DNS SRV records

Summary

Add callback DNS SRV records to the group

DNS SRV name	Country / region	Country code	DNS SRV record	
US record	United States of America / ...	+1	cube.us.example.cr	
MX record	Mexico	+52	ube.mx.example.com	
RoW record	All other countries		lbe.row.example.com	

+ Add another callback server

Back

Next

Create a callback DNS SRV group

● Group name
● DNS SRV records
○ Summary

Summary
Please review the callback DNS SRV group settings to make sure they are correct. Click 'Save' to confirm or 'Back' to make changes.

Callback DNS SRV group name
Global CB

Callback DNS SRV records

DNS SRV name	Country / region	Country code	DNS SRV record
US record	United States of America / C...	+1	cube.us.example.com
MX record	Mexico	+52	cube.mx.example.com
RoW record	All other countries		cube.row.example.com

Back
Save

Step 4: Associate PNG and CDSG to Customer Templates in Partner Hub

Initial configuration and verification of the BYoPSTN solution requires a seed organization for each unique combination of **Phone Number Group** and **Callback DNS SRV Group (if callback is required)**. Therefore, it is recommended that Cisco Partners similarly create a new **Customer Template** for each unique combination of Phone Number Group and Callback DNS SRV Group. Each customer template should be used to generate a corresponding seed organization.

Once the BYoPSTN configuration is seeded and verified using the seed organizations, the Phone Number Groups and Callback DNS SRV Groups can be applied to existing Customer Templates as required.

Please note that newly created Customer Templates are not in use by existing non-test customers and therefore can safely be used for manual verification of the BYoPSTN configuration.

NOTE: If you are not deploying Meeting Join via Callback, you do not need to associate Callback DNS SRV Groups to the Customer Template. However, you do need to select **Disable Callback**.

To add a new Customer Template, do the following:

1. Login to Cisco Partner Hub.
2. Go to **Settings**.
3. Scroll to **BroadWorks Calling**.
4. Under **Templates**, select **Add Template**.
5. Enter the Template details. At the **Package Type** stage:
 - Select **Package Type** as **Standard**.

- Select **Meeting join configuration** as **Partner provided call-in numbers (BYoPSTN)**.
- Select a provisioned **Phone Number group**.
- For **Callback DNS SRV group**, if you want to enable the Meeting Callback option then select a provisioned Callback DNS SRV group. Otherwise, select **Disable Callback**.

6. Select **Next**.
7. Enter the remaining Template details.
8. Review the Template details summary.
9. Select **Save**.
10. Repeat this procedure for each Customer Template that must be added

The screenshot below illustrates the procedure.

Add a new template

Progress bar steps: Template Name, Provisioning, Package Type, Authentication Mode, User Verification, Preferences, Summary.

☐ Basic

☒ Standard

☐ Premium

☐ Softphone

Meeting join configuration
Select the default call-in option for users joining Webex meetings.

☐ Cisco call-in numbers (PSTN)
Use call-in numbers provided by Cisco.

☒ Partner provided call-in numbers (BYoPSTN)
Use call-in numbers provided by the Partner.

Phone number group
Assign a call-in phone number group to this template.

US East

Callback DNS SRV group
Assign a callback DNS SRV group to this template.

Global CB

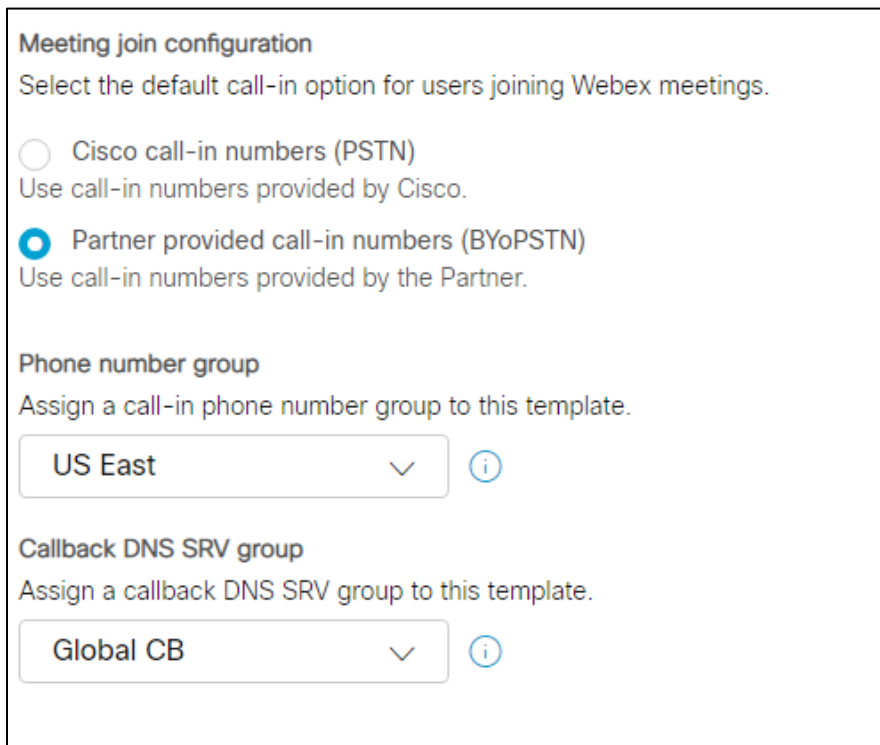
Cancel Back **Next**

To update an existing Customer Template, do the following:

1. Login to Cisco Partner Hub.
2. Go to **Settings**.
3. Scroll to **BroadWorks Calling** section.

4. Under **Templates**, select **View Template**.
5. Select the Template to be updated.
6. Scroll to the **Meeting join configuration** section:
 - Select **Partner provided call-in numbers (BYoPSTN)**
 - Select a previously configured **Phone Number group**
 - For **Callback DNS SRV group**, if you want to enable the Meeting Callback option, select a provisioned Callback DNS SRV group. Otherwise, select **Disable Callback**.
7. Select **Save**.

The screenshot below illustrates the procedure.



Meeting join configuration
Select the default call-in option for users joining Webex meetings.

☐ Cisco call-in numbers (PSTN)
Use call-in numbers provided by Cisco.

☒ **Partner provided call-in numbers (BYoPSTN)**
Use call-in numbers provided by the Partner.

Phone number group
Assign a call-in phone number group to this template.

US East ⓘ

Callback DNS SRV group
Assign a callback DNS SRV group to this template.

Global CB ⓘ

Step 5: Provision Seed Solution Organizations

The BYoPSTN solution has several different components, each of which must be configured correctly for the solution to operate successfully. One of the two purposes of the seed solution organizations is to generate phone number to meeting access codes mappings and a meeting site universally unique identifier (site UUID) that are required for the on-going operation of the solution. The other purpose being configuration verification.

For each unique combination of Phone Number Group and Callback DNS SRV Group to be used, a corresponding Customer Template should be created previously. For each of these Customer Templates, a seed solution organization must be provisioned. The provisioning of these seed organizations generates the phone number to meeting access codes mappings and a meeting site UUID that are required to configure BroadWorks.

Using each of the previously configured Customer Templates, provision a subscriber for a new test BroadWorks Service Provider or new BroadWorks Enterprise with a **Standard package** user. The resulting **Standard package** meeting site should be using Partner Provider call-in numbers meeting join option. Either of the following methods can be used to provision the subscriber:

1. Provision the test subscriber using BroadWorks Subscribers APIs as documented on developer.webex.com.
2. Enable the test subscriber for the IM&P Service on a BroadWorks configured to use the Customer Template. Please ensure the Customer Template is using the Standard package as the default to ensure the test subscriber is assigned a Standard package. Alternatively, the test subscriber must be subsequently updated to have the Standard package.

Please note it is recommended that the seed solution organizations are associated with a test BroadWorks Service Provider or test BroadWorks Enterprise.

Step 6: Select the Primary Seed Solution Organization

One of the seed solution organizations must be selected as the **primary seed solution organization**. The meeting site UUID of the Standard package meeting of this primary seed solution organization must be configured on BroadWorks. This single site UUID is shared by all sets of phone numbers and callback DNS SRV records. Multiple site UUID values are not required to be configured in BroadWorks.

It is critical that this meeting site remains provisioned as this site UUID is sent in each call-in meeting join request as an authentication token. You should not delete the seed organization as the associated meeting site will also be deleted. If the seed organization is removed, you will need to provision a new one and reconfigure Broadworks with the new site UUID.

The primary and any secondary seed solution organizations can be deleted, if desired prior to the set of phone numbers and callback DNS SRV records being assigned to non-test customers. When the set of phone numbers and callback DNS SRV records are assigned to any non-test customers, those phone numbers and callback records are associated with meeting sites for those customers and are in use for meeting join using call-in and callback. Any changes should be considered as service impacting.

To select the Primary Seed Solution Organization, do the following:

1. Login to Cisco Partner Hub.
2. Go to **Settings**.
3. Scroll to **BroadWorks Calling** section.
4. Under **Configuration Validation (BYoPSTN)** section, select **Assign**
5. In the **Assign organization** screen, search for and select one of the seed organizations previously configured
6. Select **Assign**

The selected seed organization is the primary seed organization.

The screenshots below illustrate the procedure.

Templates

7 active templates

View Templates

Add Template

Meeting join configuration (BYoPSTN)

When the Partner is providing Webex meeting call-in numbers, both call-in phone number groups and callback DNS SRV groups must be created. The groups become active when associated with calling templates.

Call-in phone number groups

4 active groups

View groups

Create group

Callback DNS SRV groups

4 active groups

View groups

Create group

Configuration Validation (BYoPSTN)

Configuration validation is used to determine if your BYoPSTN solution is configured in accordance with your requirements. It is based on an organization that has been configured for BYoPSTN. The organization has to be configured with at least one standard package user, one phone number group, and one callback group for validation to pass. We recommend that you use the assigned validation organization for testing purposes only.

[Learn More](#)

Assign an organization that meets the basic BYoPSTN configuration requirements.

Assign

Assign organisation

×

Validate your BYoPSTN solution by assigning an organization that meets the basic BYoPSTN configuration requirements.

Search

▼

Only organisation configured for BYoPSTN will be searchable

Cancel

Assign

Assign organisation

×

Validate your BYoPSTN solution by assigning an organization that meets the basic BYoPSTN configuration requirements.

Seed Test Enterprise ABC

▼

Only organisation configured for BYoPSTN will be searchable

Cancel

Assign

Configuration Validation (BYoPSTN)

Configuration validation is used to determine if your BYoPSTN solution is configured in accordance with your requirements. It is based on an organization that has been configured for BYoPSTN. The organization has to be configured with at least one standard package user, one phone number group, and one callback group for validation to pass. We recommend that you use the assigned validation organization for testing purposes only.

[Learn More](#)

Organization name

Seed Test Enterprise ABC ⓘ

Organization ID

d927ac4d-3d73-4d7f-8506-a1bc0a221934 ⓘ

Step 7: Download BroadWorks configuration (BYoPSTN)

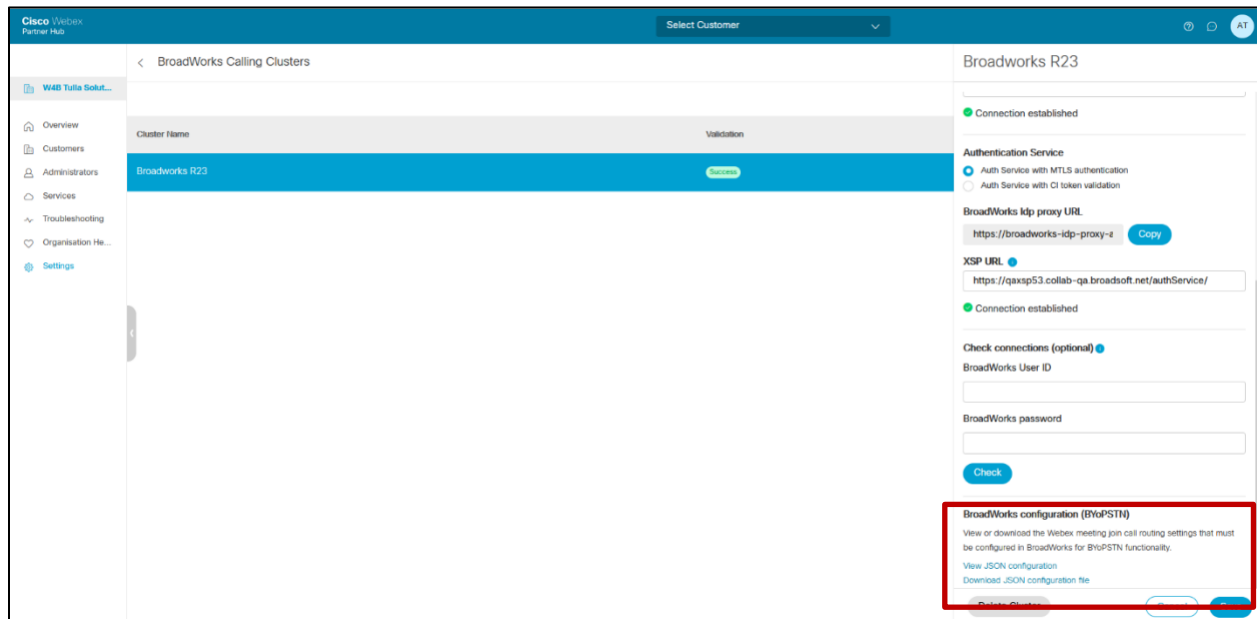
The Primary Seed Solution Organization, Phone Number Groups and Callback DNS SRV Group details for a given BroadWorks Cluster are available in a single location, the BroadWorks configuration (BYoPSTN) JSON file. This information is needed to configure BroadWorks for BYoPSTN.

Please note the JSON configuration file is only available for view/download after the primary seed solution organization is selected.

The procedure to view/download the JSON configuration file is as follows:

1. Login to Cisco Partner Hub
2. Go to **Settings**
3. Scroll to **BroadWorks Calling**.
4. Under **Clusters**, select **View Cluster**.
5. Select the Cluster that is associated with the Customer Templates that are configured for BYoPSTN.
6. Scroll to the **BroadWorks configuration for BYoPSTN** section
7. Click **Download JSON configuration file**.
8. Repeat this procedure for any other BroadWorks Clusters.

The screenshots below illustrate the procedure.



Please see the sample JSON configuration file below. The file contains supplementary information on each Phone Number Group, Callback DNS SRV Group, the following key configuration items which must be entered on BroadWorks are marked in bold.

- **siteUUID**: BroadWorks must send this value in the SIP messages, it is a token which Webex Edge Audio uses to confirm the identity of the Cisco Partner's BroadWorks and its access to meeting sites managed by this Cisco Partner.
- **Phone number -to- access code mapping**: The phone numbers and their associated Webex access codes must be configured on BroadWorks.
 - **phoneNumber**
 - **accessCode**
- **localeTag**: The desired announcement language associated with phone number must be configured on BroadWorks.
- **dnsSrv**: The Callback DNS SRV must be configured in the DNS and refer to the desired CUBE instances.

```
{
  "siteUUID": "491db0821791441a96c233fefb6c6d6c",
  "siteURL": " seedtestenterpriseabc.webex.com ",
  "partnerOrgId": "1da175de-3651-4467-b26b-b0d85a2cb3ad",
  "solutionValidationOrgId": "d927ac4d-3d73-4d7f-8506-a1bc0a221934",
  "customerTemplates": [
    {
      "name": "US West Std",
      "id": "27fe1337-ab1d-44b0-8b5e-ff1d32f6e3f8",
      "phoneNumberGroupId": "1bcb05bd-b919-45fd-b30e-71d2abb59e26",
      "callbackDnsSrvGroupId": "25392686-a390-49b9-bad5-cb47159c3e992"
    },
    {
      "name": "US East Std",
```

```

        "id": "070d6682-b64f-46ea-bc4b-b2e1218ba4bb",
        "phoneNumberGroupId": "12bc0b8f-ea1d-457f-8fe2-069ccf78907e",
        "callbackDnsSrvGroupId": "25392686-a390-49b9-bad5-cb47159c3e992"
    },
    ],
    "phoneNumberGroups": [
        {
            "name": "US West",
            "id": "1bcb05bd-b919-45fd-b30e-71d2abb59e26",
            "phonenumbers": [
                {
                    "id": "617c5faa-1721-45c7-bc70-e6d7c20ccc29",
                    "name": "US Palo Alto",
                    "countryCode": "US",
                    "localeTag": "en_US",
                    "tollType": "TollFree",
                    "defaultPhoneNumberType": "NONE",
                    "phoneNumber": "9863502478",
                    "accessCode": "88672693772924908359"
                },
                {
                    "id": "48fa7c50-9da0-4c8b-9b2f-307ff435c7c7",
                    "name": "US Toll San Francisco",
                    "countryCode": "US",
                    "localeTag": "en_US",
                    "tollType": "Toll",
                    "defaultPhoneNumberType": "PRIMARY",
                    "phoneNumber": "4156551000",
                    "accessCode": "88652789466280320324"
                }
            ]
        },
        {
            "name": "US East",
            "id": "12bc0b8f-ea1d-457f-8fe2-069ccf78907e",
            "phonenumbers": [
                {
                    "id": "ca0c622a-8621-4477-91e0-b3e214833568",
                    "name": "US Maryland",
                    "countryCode": "US",
                    "localeTag": "en_US",
                    "tollType": "Toll",
                    "defaultPhoneNumberType": "PRIMARY",
                    "phoneNumber": "2403332200",
                    "accessCode": "88631321777971704941"
                },
                {
                    "id": "00875574-9a46-4447-a967-350b6176755a",
                    "name": "US Florida",
                    "countryCode": "US",
                    "localeTag": "en_US",
                    "tollType": "Toll",
                    "defaultPhoneNumberType": "SECONDARY",
                    "phoneNumber": "9049002303",
                    "accessCode": "88632627551145646175"
                },
                {
                    "id": "a2c10316-9266-4423-a669-d67949f99d33",
                    "name": "US New York",
                    "countryCode": "US",

```

```

        "localeTag": "en_US",
        "tollType": "TollFree",
        "defaultPhoneNumberType": "NONE",
        "phoneNumber": "8056504578",
        "accessCode": "88649679020033567943"
      }
    ]
  },
  "callbackDnsSrvGroups": [
    {
      "name": "CB US",
      "callbackDnsSrvs": [
        {
          "name": "Callback US",
          "countryCode": "US",
          "dnsSrv": "cube.us.example.com",
          "id": "c5209d17-7c2f-45b3-95a6-65d7f5f53c7e"
        }
      ],
      "id": "25392686-a390-49b9-bad5-cb47159c3e992"
    },
    {
      "name": "CB MX",
      "callbackDnsSrvs": [
        {
          "name": "Callback MX",
          "countryCode": "MX",
          "dnsSrv": "cube.mx.example.com",
          "id": "cca0e4c3-5cff-412c-a854-bfb719f603a2"
        }
      ],
      "id": "36403797-b401-50c0-cbe5-dc58260d4f003"
    }
  ]
}

```

Step 8: Determine the Webex Edge Audio DNS SRV domain

The Webex Edge Audio DNS SRV domain must be configured on BroadWorks. Use the following procedure to determine the value.

1. Login to Cisco Partner Hub.
2. Go to **Customers**.
3. Select the BYoPSTN Validation Enterprise.
4. Select **View Customer**.
5. Go to **Services/Meetings**.
6. Select the Standard package meeting site.
7. Scroll to the bottom of the side-out panel, select **Configure Site**.
8. Select **Common Settings / Audio Settings**.
9. Under the **Edge Audio Custom Global Call-in Numbers** section, select **Generate Lua Script**.
10. In the pop-up window search for value "-- Update To header with CCAX URL"

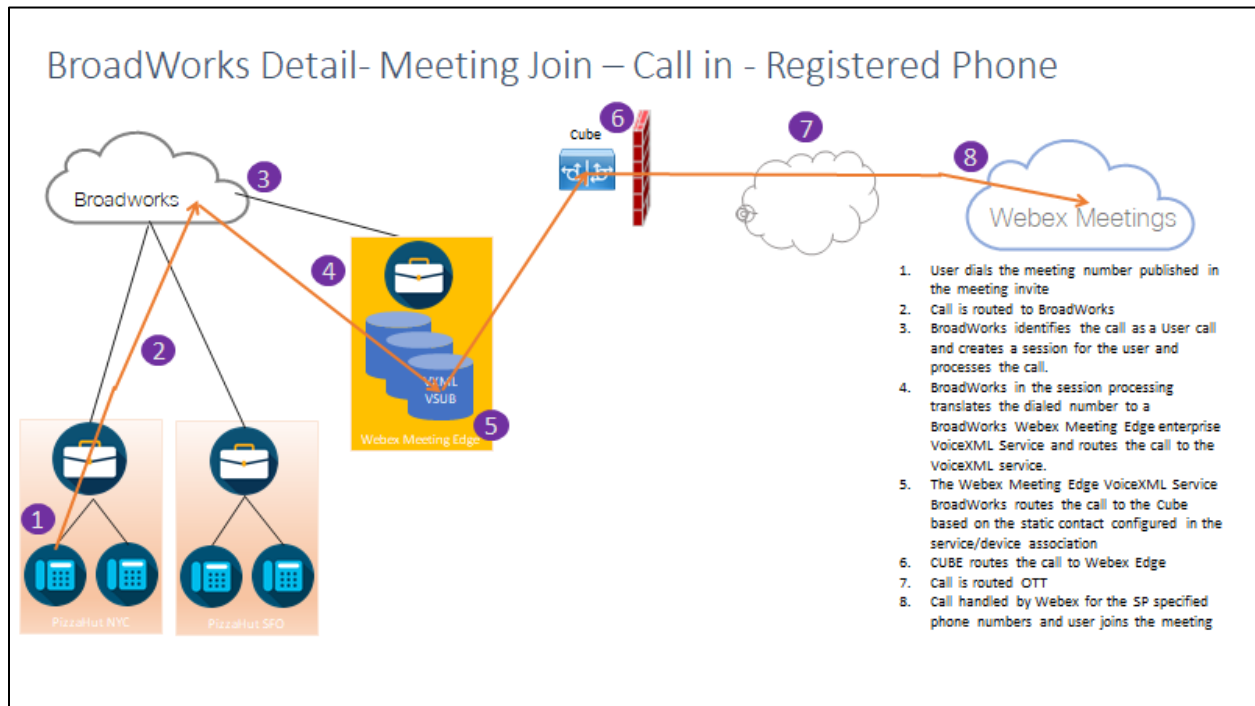
```
-- Update To header with CCAX URL
local oldTo1 = msg:getHeader("To")
local newTo1 = string.gsub(oldTo1, "<sip:(.+)@(.*)>",
"<sip:%1@ecccspx.amer.webex.com>")
msg:modifyHeader("To", newTo1)
```

11. Extract out the value in bold, for example, `ecccspx.amer.webex.com`.

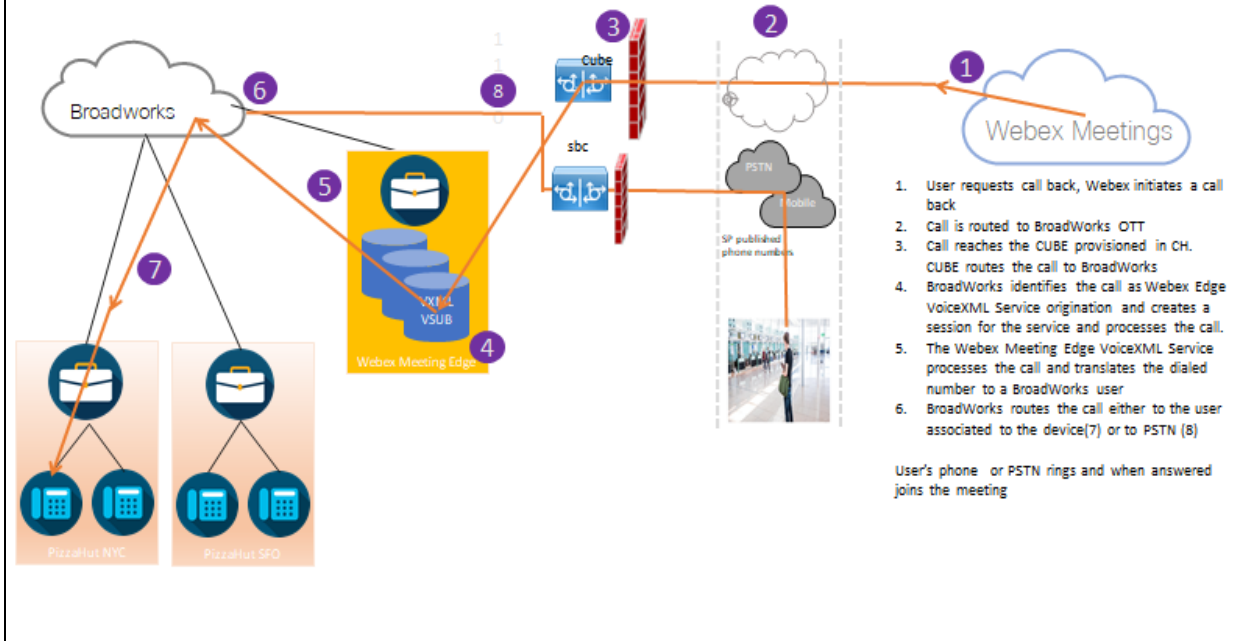
This is the Webex Edge Audio DNS SRV domain that must be configured on BroadWorks.

Step 9: Provision Partner BroadWorks Configuration

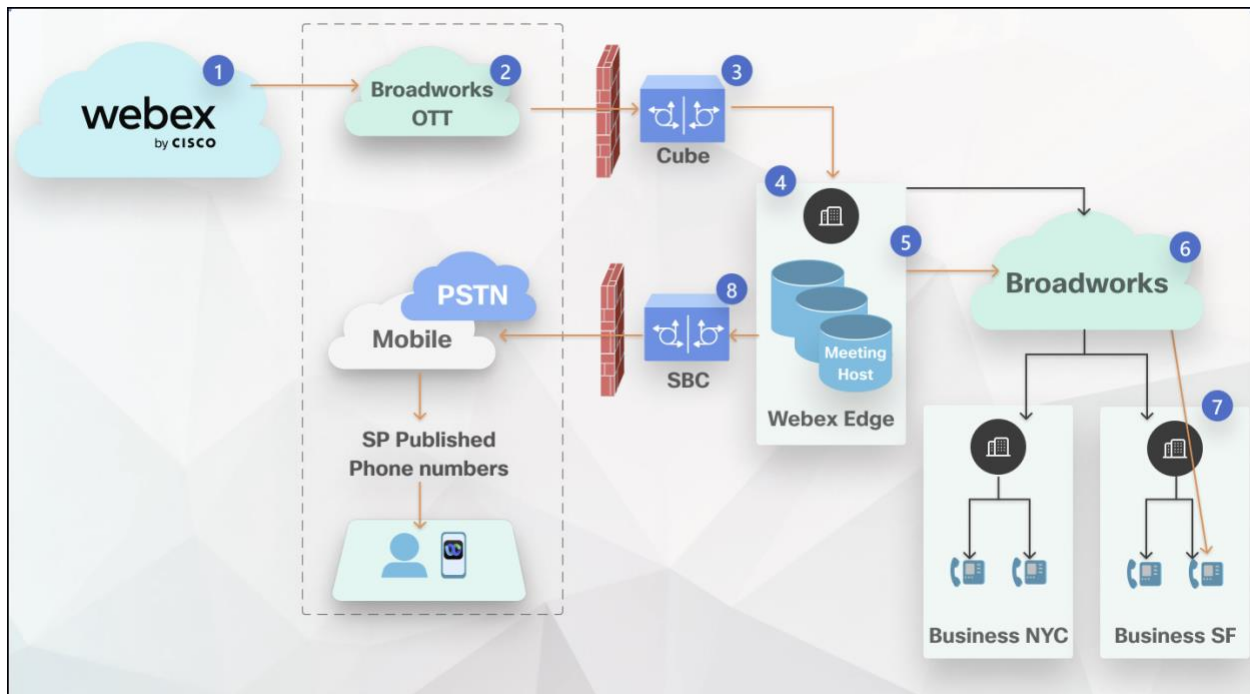
This section describes the BroadWorks configuration necessary to implement the Meeting Call-in and Callback scenarios shown in the diagrams below. The configuration examples are based on the data in the JSON file shown in the previous section. Numbers, domains, naming of enterprise/groups, type of devices, policies, profiles, etc. are expected to vary by partner.



BroadWorks Detail- Call me (Callback) - to Registered Phone / PSTN



BroadWorks Detail— Call me (Callback using SIP X-Cisco-Meet-Info header) – to Registered Phone / PSTN



Call flow:

1. User requests call back, Webex initiates a call back.
2. Call is routed to BroadWorks OTT.
3. Call reaches the CUBE provisioned in CH. CUBE routes the call to BroadWorks.

4. BroadWorks identifies the call as Meeting Host origination and creates a session for the meeting host user and processes the call.
5. The meeting host user session processes the call and translates the dialed number. Additionally, a billing record is generated on behalf of the meeting host user.
6. BroadWorks routes the call either to the user associated to the device (7) or to PSTN (8).
User's phone or PSTN rings and when answered joins the meeting.

Before you Begin

SIP communication between BroadWorks and the CUBE can be over UDP or TCP depending on your network requirements. For example, if some network or access devices (for example, gateways or endpoints) in the BYoPSTN call-in or callback flows do not support TCP, then UDP should be used instead.

The configuration and examples shown in this guide use TCP as the transport protocol. To use TCP, make sure that your BroadWorks Application Server and Network Server are both configured for TCP:

```
_CLI/Interface/SIP> get
networkProxyTransport = unspecified
accessProxyTransport = unspecified
supportDnsSrv = true
supportTcp = true
```

Application Server

Identify/Device Profile Type

A new Identity/Device Profile Type should be created to represent the CUBE. Make sure to set the following properties below, while others can be left at default values:

- **Signaling Address Type**—Set to **Intelligent Proxy Addressing**
- **Authentication**—Set to **Enabled**
- **Support Identity in UPDATE and Re-INVITE**—Checked

- **Static Registration Capable** – Set to **Enabled**
- **Video Capable** – Set to **Disabled**

In the example below, the new Identity/Device Profile Type “VXML_profile” is created to represent the CUBE.

Options:

Identity/Device Profile Type

Identity/Device Profile Type Modify

Modify an existing identity/device profile type.

Identity/Device Profile Type: VXML_profile
 Signaling Address Type: Intelligent Proxy Addressing
☐ Obsolete

Standard Options

Number of Ports: ☒ Unlimited ☐ Limited To
 Ringback Tone/Early Media Support: ☐ RTP - Session
☐ RTP - Early Session
☒ Local Ringback - No Early Media
 Authentication: ☒ Enabled
☐ Disabled
 Hold Normalization: ☐ Unspecified Address
☐ Inactive
☒ RFC3264
☐ Registration Capable ☐ Authenticate REFER
☒ Static Registration Capable ☐ Video Capable
☒ E164 Capable ☐ Use History Info Header
☐ Trusted

Advanced Options

☐ Route Advance ☐ Forwarding Override
☐ Wireless Integration ☐ Conference Device
☐ PBX Integration ☐ Mobility Manager Device
☐ Add P-Called-Party-ID ☐ Music On Hold Device
☐ Auto Configuration Soft Client ☐ Requires BroadWorks Digit Collection
☐ Requires BroadWorks Call Waiting Tone ☐ Requires MWI Subscription
☐ Advice of Charge Capable ☐ Support Call Center MIME Type
☐ Support Emergency Disconnect Control ☒ Support Identity In UPDATE and Re-INVITE
☐ Enable Monitoring ☐ Support RFC 3398
☐ Static Line/Port Ordering ☐ Support Client Session Info
☐ Support Call Info Conference Subscription URI ☐ Support Remote Party Info
☐ Support Visual Device Management Redirect Link ☐ Bypass Media Treatment
☐ Support Cause Parameter ☐ Verstat In From Header
☐ Verstat In PAI Header
 Reset Event: ☐ reSync ☐ checkSync ☐ resetString ☒ Not Supported
 Reset String:
 Trunk Mode: ☒ User ☐ Pilot ☐ Proxy
 Hold Announcement Method: ☒ Inactive ☐ Bandwidth Attributes
 Device Category: ☒ Generic ☐ Hosted ☐ Client App ☐ Trunking ☐ Local Gateway
 Unscreened Presentation Identity Policy: ☒ Profile Presentation Identity
☐ Unscreened Presentation Identity
☐ Unscreened Presentation Identity With Profile Domain
 Web Based Configuration URL Extension:

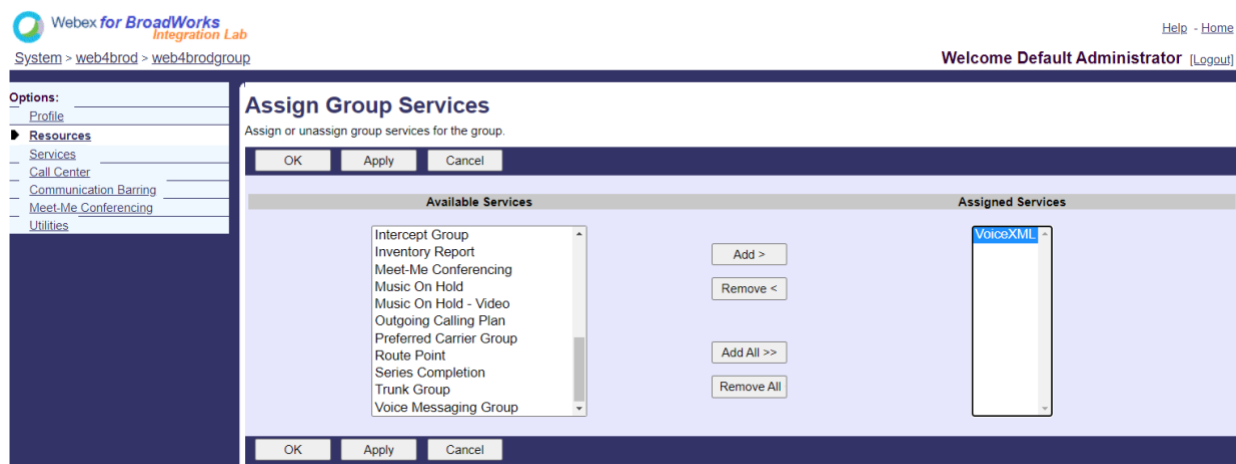
 Device Configuration Options: ☒ Not Supported ☐ Device Management ☐ Legacy

VoiceXML Virtual Subscriber

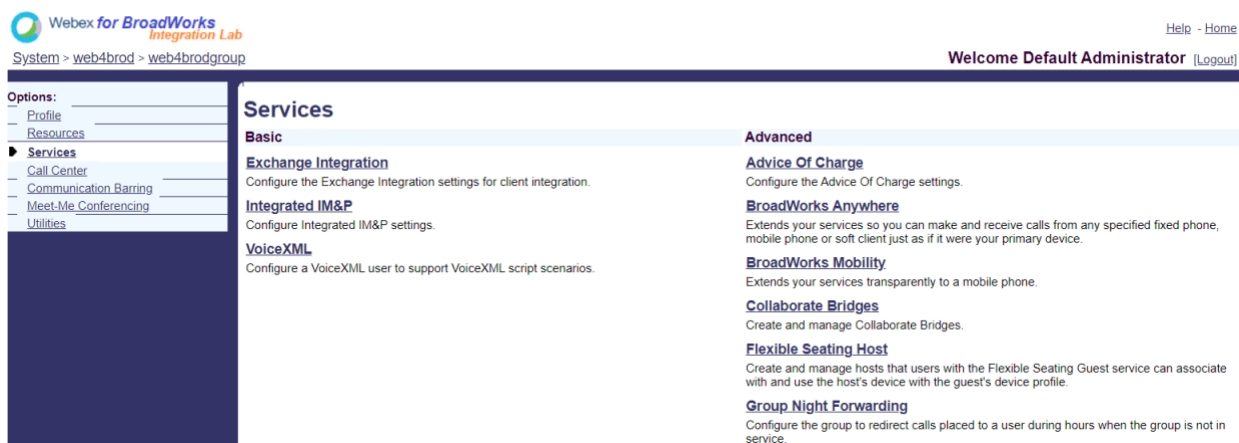
Create a VoiceXML Instance

Each Webex Meetings PSTN number is represented by a virtual subscriber in BroadWorks, and the VoiceXML virtual subscriber functionality can be used. It is recommended that a dedicated enterprise and group are used for all VoiceXML virtual subscribers. Note that we are not actually exploiting any VoiceXML capabilities, but this type of virtual user is suitable for interacting with the CUBE.

In order to use the VoiceXML service, ensure that the license has sufficient “VoiceXML” quantities and that the service is authorized on the enterprise and group levels, and the VoiceXML service is assigned to the group as shown in the example picture below.



Under **Group -> Services**, select **VoiceXML** and create an instance for each PSTN number.



Configure VoiceXML Addresses

For each VoiceXML instance, provision the following under the VoiceXML Addresses:

- **Phone Number**—Enter the dial-in number for the Webex Meetings site (for example, 2403332200).
- **Extension**
- **Identity/Device Profile**—Create one instance (for example, VXML_deviceProf) based on the device type created in the previous section (VXML_profile in the example) and enter the following configuration:
- **Line/port**—Enter in the <access number>@<domain> format, where
 - <access number> is the Access Code number for the Webex Meetings site (available from the JSON file) (for example, 88631321777971704941)

- <domain> is the domain of the Webex Edge Audio for this meeting site (for example, ecccspx.amer.pub.webex.com)
- **Contact sip**—For Meeting Call-In calls to the access number, the INVITE will be sent with a Request URI set to the value of this field. Enter the SIP contact in this format <sip contact>;<Locale>;<Meetings Site UUID>;<SIP transport>, where:
 - <sip contact> is the <number> from the line/port field but with the domain as the SRV that resolves to the CUBE's address (for example, 88631321777971704941@cube.internal.local)
 - <Locale> represents the language setting according to the user locale (for example, locale=en_US)
 - <Meetings Site UUID> is site UUID from the JSON file (for example, x-cisco-site-uuid=abbd70f6c519fb1ee053ad06fc0a038b)
 - <SIP transport> should be transport=tcp to have the AS use TCP to send messages to the CUBE.

Below is an example of VoiceXML Addresses settings.

The screenshot displays the 'VoiceXML Addresses' configuration window. It includes a sidebar with 'Options' (Profile, Communication Bar, Utilities) and a main configuration area. The 'Profile' option is selected. The configuration area contains the following fields and values:

- Phone Number: 2403332200 (Activated)
- Extension: 1000
- Identity/Device Profile: Identity/Device Profile (selected), None (radio button)
- Identity/Device Profile Name: VXML_deviceProf (System)
- * Line/Port: 88631321777971704941
- Contact sip: 88631321777971704941@cube.internal.local
- Path: (empty field)
- Aliases: Three entries, each with 'sip:' and 'atlasprodbyopstnc1u2.webex.com'

NOTE: For each additional Meeting access number to be used, an additional VoiceXML virtual subscriber should be created analogous to the one above. The same device profile can be used, but the Line Port and Contact fields must be constructed from the access number information as shown above.

NOTE: Make sure to verify that the Call Processing Policy limits that you configure on the BroadWorks virtual subscriber are sufficient to handle the extra BYoPSTN calls in your Phone Number Groups.

Assign SIP Authentication to VoiceXML Instance

Assign the Authentication service to the VoiceXML virtual subscriber. This will be used to authenticate SIP INVITE messages from the CUBE in the Callback scenario. It also prevents the VoiceXML virtual subscriber from accepting calls from parties other than the CUBE.

Go to the virtual subscriber Authentication page under Utilities and enter the SIP username and password as shown below:

NOTE: the CUBE must be configured with the same username and password in order to properly authenticate the INVITE messages that are sent to the AS.

An example of the command to configure SIP authentication on the CUBE is as follows:

```

sip-ua authentication username VSUB password 0 <unencrypted password>
(See the CUBE onfiguration/datafill for more details)

```

Namedefs file

The VoiceXML virtual subscriber SIP contact field contains the URL where the domain part resolves to the CUBE address. This is an internal SRV, and the namedefs file on the AS can be used to resolve the internal SRV to the CUBE IP.

In our example, the SIP contact SRV is cube.internal.local and resolves to address 10.165.196.30 port 5060 to reach the CUBE. On the AS, the `/usr/local/broadworks/bw_base/conf/namedefs` file is updated as follows:

```

_sip.tcp.cube.internal.local SRV 1 99 5060 10.165.196.30

```

Webex Meetings Call Type

Webex Meetings call processing configuration options are available to control how Meeting Call-In calls are handled. By default, Meeting Call-In calls are processed as external calls as Call-In numbers are

hosted in a dedicated enterprise or service provider. External calls are normally included in the Session Admission Control session counts and flagged for charging in the CDR field *chargeIndicator*.

The following example adds the recommended configuration to process Meeting Call-Ins as internal calls such that they are excluded from charging and excluded from the Session Admission Control counts.

By setting *Enforce NS Charge Field* to true, the population of CDR field *chargeIndicator* is based on the configured Charge attribute of the Network Server call type.

```
AS_CLI/System/CallP/WebexMeetings/WebexCallTypes> add "Webex Meetings" WXM true true

AS_CLI/System/CallP/WebexMeetings/WebexCallTypes> get
      Name      NS Call Type      Enforce NS Charge Field      Process As Internal For SAC-Subscriber
=====
Webex Meetings      WXM                        true                        true
```

VoiceXML Meeting Callback Virtual Subscriber

Create a VoiceXML Meeting Callback Subscriber

A dedicated VoiceXML virtual subscriber with a special Webex Meeting Callback option (hereafter called VoiceXML meeting callback subscriber) needs to be configured on the BroadWorks Application Server (AS) to handle the Webex Meetings callback calls. Only a single instance of this subscriber can be configured on the AS.

To enable the feature, set the Activatable Feature 102074 to true via CLI.

```
AS_CLI/System/ActivatableFeature> activate 102074
***** Warning *****
This activity should only be done during a maintenance window because
this may cause large amounts of data to be added/modified/deleted and
it may take some time to execute. Features that have web page impacts
require that users and administrators log out and log back in.
Are you sure you want to continue?

Please confirm (Yes, Y, No, N): y
...Done

AS_CLI/System/ActivatableFeature> get

      Id      Description      Activated      Last Modified
      Timestamp
=====
102746      BroadWorks Support for CI UUID      true
102074      BYO PSTN Billing support for CallBack and CallIn      true
104256      Weak Password Validation Service      false
104073      Add FAC Support for Call Center Agent Join-Unjoin in CDR      false
103542      Configurable Endpoint For Auto-Answer And Forced Answer      false
104255      Control password usage and behavior to ensure security      false
```

NOTE: Since "BYO PSTN Billing support for CallBack and CallIn" feature depends on "BroadWorks Support for CI UUID" feature, before activating (102074) feature you also need to activate (102746) feature. For more details refer "CI User UUID Sync (Broadworks Support for CI UUID)" section.

The VoiceXML meeting callback subscriber is similar to the existing BYOPSTN VXML virtual subscriber but tagged it with a new "Webex Meeting Callback" flag. This VoiceXML meeting callback subscriber is

configured with the same device profile as the existing BYOPSTN VXML virtual subscriber, as well as the Authentication service with the same credentials.

An example is shown below:

The VoiceXML meeting callback subscriber must exist on the AS hosting the meeting host user. When the AS receives the meeting callback INVITE request, it attempts to locate both the VoiceXML meeting callback user and the meeting host user on the AS during call setup. If neither of these users are found, the call is rejected.

Meeting Host Session

In the callback scenario with the X-Cisco-Meet-Info header, the Cisco BroadWorks Application Server receives a SIP INVITE request and identifies the meeting host user using the host CI User UUID parameter of the SIP X-Cisco-Meet-Info header. A call session is created on behalf of the meeting host user is created to process the call and execute the service profile of the user. Additionally, a billing record is generated on behalf of the meeting host user. The meeting ID and the site UUID information from the SIP X-Cisco-Meet-Info header are captured in the billing record.

An example of the SIP X-Cisco-Meet-Info header is shown below:

```
X-Cisco-Meet-Info:hostCIUserUuid="52f4c6cb-c6a3-4283-a1ab-04cc8828b7c1";meetingid="26551128462";siteUUID="ec6659987f473332e0531b04fc0acae
c"
```

Application Delivery Platform

CI User UUID Sync (Broadworks Support for CI UUID)

The user CI UUID is a unique identifier to identify users within the Webex environment.

This Webex Provisioning Sync application on the Cisco BroadWorks Application Delivery Platform (ADP) is used to synchronize, map, and store the user CI UUID into the BroadWorks infrastructure such that it can be used in various interactions with Webex and Webex for BroadWorks service.

Refer to the “Enable Webex Meeting Callback” on how the CI User UUID association is used by the Cisco BroadWorks Network Server and Cisco BroadWorks Application Server.

The following steps set up the Webex Provisioning Sync application to periodically poll and update the BroadWork Users with the CI UUID.

The Webex Provisioning Sync Application requires OAuth credentials with the spark-admin:broadworks_subscribers_read scope for the Cisco Identity Provider and can be obtained by raising a service request with your onboarding agent.

Check 'Obtaining OAuth credentials for your Webex for Cisco BroadWorks' section for more details to raise the service request at:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wx4bwks/Solution_Guide/wbx/bw_b_solution-guide/wbxbw_b_SolutionGuide-PDF_chapter_01.html?bookSearch=true#Cisco_Generic_Topic.dita_0e1beabc-80ae-4e8d-b177-17108ec5daed

Add the token with an appropriate partner name as follows:

```
ADP_CLI/System/CommunicationUtility/DefaultSettings/ExternalAuthentication/CiscoIdentityProvider/Partners> add custBYO refreshToken
New Password:
Re-type New Password:

ADP_CLI/System/CommunicationUtility/DefaultSettings/ExternalAuthentication/CiscoIdentityProvider/Partners> get
Partner Name Refresh Token
=====
FederationPartner *****
custPart *****
custBYO *****
```

Add the partner name associated with the OAuth token to the list of partners to be monitored by the Webex Provisioning Sync application with the 'enabled' flag set to 'true'.

By this Webex Provisioning Sync application will start doing CI user UUID syncing on defined polling interval.

```
ADP_CLI/Applications/WebexProvisioningSync/GeneralSettings/MonitoredPartners> add custBYO true
```

Once the partner is included, the Webex Provisioning Sync application can now perform the association of the CI UUID to the BroadWorks users.

Change the connection timeout using the following commands:

```
ADP_CLI/Applications/WebexProvisioningSync/GeneralSettings/Controller> set requestTimeout 30000
...Done

ADP_CLI/Applications/WebexProvisioningSync/GeneralSettings/Controller> get requestTimeout = 30000

ADP_CLI/Applications/WebexProvisioningSync/GeneralSettings/Controller> cd http

ADP_CLI/Applications/WebexProvisioningSync/GeneralSettings/Controller/Http> set connectionTimeout 300
*** Warning: BroadWorks needs to be restarted for the changes to take effect ***

ADP_CLI/Application/WebexProvisioningSync/GeneralSetting/Controller/HTTP > get
```



```

connectionPoolSize = 5
connectionTimeout = 300
connectionIdleTimeOut = 300
maxConcurrentRequests = 10
maxCookieAgeInHours = 24

```

This association can be done automatically or manually. The CLI manualSync command can instantly trigger the association to take place.

```

ADP_CLI/Applications/WebexProvisioningSync/GeneralSettings/MonitoredPartners>
manualSync custBYO

```

Partners with 'Enabled' set to 'true' perform the associated on the polling interval. During the initial association, the Webex Provisioning Sync application queries the Webex Subscriber API to retrieve the data containing the CI UUID for all users hosted by the partner. The BroadWorks user's External ID is updated with the associated CI UUID. Subsequent associations affect users added to the partner. The status command can be used to see if the synchronization is complete.

```

ADP_CLI/Applications/WebexProvisioningSync/GeneralSettings/MonitoredPartners>
status

```

Partner Name	Status	Last Sync Time
custBYO	synchronizing	
custPart	monitoring	2023-01-29T15:36:43.873-05:00

2 entries found.

Once the synchronization is complete, the status changes back to monitoring. Subsequent synchronization is performed on users added to the partner after the "Last Sync time".

The following figure shows the CI UUID set within the External ID:

System > MtiASDev > North_as77 > Users : north00

Options:

- Profile
- Incoming Calls
- Outgoing Calls
- Call Control
- Calling Plans
- Messaging
- Communication Barring
- Utilities

Profile

Profile allows you to view and maintain your profile information. The information filled in specifies your primary phone number, extension, and device that are used for section allows your mobile phone, pager, and other information to be visible to other group members in the group phone list. Some of this information can only be r

OK Apply Delete Cancel

Enterprise ID: MtiASDev
Group: North_as77
User ID: north00
External ID: 6970e6bb-7439-4ffb-ad34-d3ff0167ddad
Person ID: Y2tzY29zcGFyazovL3VzL1BFT1BMRs82OTcwZTZiY03NDM5L
* Last Name: north
* First Name: john0
* Calling Line ID Last Name: north
* Calling Line ID First Name: john0
Name Dialing Last Name:
Name Dialing First Name:
Department: None
Language: English
Time Zone: (GMT-05:00) (US) Eastern Time
Network Class of Service: None

[Move User to Another Group \(Also saves current screen data\)](#)
[Change User ID \(Also saves current screen data\)](#)
[Change External ID \(Also saves current screen data\)](#)
[Change Person ID \(Also saves current screen data\)](#)

Network Server

Call Type

For billing and reporting purposes, it may be desirable to mark CDRs for Meetings Call-In calls. This can be accomplished using the Network Server PreCallTyping policy.

First, on the NS CLI under /System/CallP/CallType, add a new call type. The following example adds the new "WXM" call type:

```

NS_CLI/System/CallP/CallTypes> add WXM LOCAL true false "Webex Meetings"
NS_CLI/System/CallP/CallTypes> get calltype WXM
  CallType      Description  Category      Scope  SupportE164  Charge
=====
WXM            Webex Meetings  LOCAL        User Defined      true    false

```

The call type can then be used in a PreCallTyping instance that is part of the BroadWorks user's routing profile. In this example, a new PreCallTyping instance "wxm" was added under /Policy/PreCallTyping CLI context, but it could be an existing PreCallTyping instance already being used:

```

NS_CLI/Policy/PreCallTyping> add wxm true CallTypes ALL

NS_CLI/Policy/PreCallTyping> get wxm
Policy: PreCallTyping  Instance: wxm
  CallTypes:
    Selection = {ALL}
    From = {PCS, ALL, TRMT, LO, GNT, DP, WXM, LPS, OA, TPS, EA, FGB, POA, SV, SVCD,
    IN, MS, CSV, EM, SVCO, SMC, ZD, NIL, CT, TF, GAN, TO, DA, OAP}
    supportLCABasedNormalization = false
    Enable = true

```

The next step is to add entries to the PreCallTyping instance for all the dial in numbers under the /Policy/PreCallTyping/DialPlan CLI context. For example:

```

NS_CLI/Policy/PreCallTyping/DialPlan> add wxm 1 dflt 12403332200 12403332200 exact
  11 11 WXM 0 0 Webex Meetings
NS_CLI/Policy/PreCallTyping/DialPlan> add wxm 1 dflt_e164 12403332200 12403332200
  exact 11 11 WXM 0 0 Webex Meetings

NS_CLI/Policy/PreCallTyping/DialPlan> get wxm 1
Policy: PreCallTyping  Instance: wxm  Table: DialPlan
CC Dial Plan  From      To      Match Min Max Call Type Prefix Action  Call Ind
Description
=====
=====
1 dflt      12403332200 12403332200 {exact} 11 11 {WXM}      0
  Webex Meetings
1 dflt_e164 12403332200 12403332200 {exact} 11 11 {WXM}      0
  Webex Meetings

```

The PreCallTyping instance is then added (provided it doesn't already exist) to the applicable routing profile of the originating user as shown in the example below:

```

NS_CLI/Policy/Profile> add Profall PreCallTyping wxm
NS_CLI/Policy/Profile> get profile Profall
Profile:  Profall
          Policy      Instance
=====
          CallTyping  DefaultInst

```

CallScreening	DefaultInst
SubLocation	DefaultInst
FarEndRtg	DefaultInst
NearEndRtg	DefaultInst
UrlDialing	DefaultInst
MediaSrvSel	DefaultInst
SIMPLE	DefaultInst
DstSvcRtg	DefaultInst
NumberPortability	DefaultInst
RCBasedRtg	DefaultInst
NetVoicePortalRtg	DefaultInst
PreCallTyping	wxm

NOTE: BroadWorks originating CDR's are only generated by calls originated from BW subscribers. PSTN originated calls from the "network" side of the AS will not generate originating CDR's. There will be a terminating CDR for the VoiceXML virtual subscriber in either case.

RoutingNE

A RoutingNE is required on the NS under /System/Device/RoutingNE CLI context to represent the CUBE. This way, when the NS receives the INVITE from the CUBE, it will match the via header to the RoutingNE entry that is provisioned on the NS. Refer to the [Cisco BroadWorks Network Server Command Line Interface Administration Guide](#) for details on how to add a RoutingNE.

Below is an example of the commands to add the RoutingNE "WebexMeetings", where the CUBE IP address = 10.165.196.30. The example also shows commands to create a new OrigRedirect and Profile instances to associate with the RoutingNE, but existing instances can also be used.

```
NS_CLI/Policy/OrigRedirect> add wxm_Inst true CallTypes ALL
supportTrunkGroupLookups disable applyAccessSideRules enableRestrictive

NS_CLI/Policy/OrigRedirect> get wxm_Inst
Policy: OrigRedirect Instance: wxm_Inst
Enable = true
CallTypes:
  Selection = {ALL}
  From = {PCS, ALL, TRMT, LO, GNT, DP, WXM, LPS, OA, TPS, EA, FGB, POA, SV, SVCD,
IN, MS, CSV, EM, SVCO, SMC, ZD, NIL, CT, TF, GAN, TO, DA, OAP}
supportTrunkGroupLookups:
  Selection = {disable}
  From = {disable, enablePermissive, enableRestrictive}
applyAccessSideRules:
  Selection = {enableRestrictive}
  From = {disable, enablePermissive, enableRestrictive}

NS_CLI/Policy/Profile> add wxm_routing

NS_CLI/Policy/Profile> add wxm_routing OrigRedirect wxm_Inst

NS_CLI/Policy/Profile> add wxm_routing SubLocation DefaultInst
```

```

NS_CLI/Policy/Profile> get profile wxm_routing
Profile:  wxm_routing
          Policy              Instance
          =====
          OrigRedirect         wxm_Inst
          SubLocation          DefaultInst

NS_CLI/System/Device/RoutingNE> add  WebexMeetings 1240364 1 99 wxm_routing false
OnLine AccessRoutingNE

NS_CLI/System/Device/RoutingNE/Address> add WebexMeetings 10.165.196.30 1 99 tcp

NS_CLI/System/Device/RoutingNE> get
Network Element  WebexMeetings
  Location       = 1240364
  Static Cost    = 1
  Static Weight  = 99
  Poll           = false
  OpState        = enabled
  State          = OnLine
  Profile        = wxm_routing
  Signaling Attributes= AccessRoutingNE

NS_CLI/System/Device/RoutingNE/Address> get
Routing NE  Address      Cost    Weight    Port    Transport Route
WebexMeetings  10.165.196.30    1      99      -      tcp

```

With the example configuration, the CUBE sends to the NS an INVITE that is similar to the following (important fields highlighted in red):

```

INVITE sip:+19991111111@domain.com:5060 SIP/2.0
Via:SIP/2.0/TCP 10.10.10.10:5060;branch=z9hG4bK7C7B9EB
Remote-Party-ID:" BroadWorks
"<sip:88622222222@domain.com>;screen=no;party=calling;privacy=off
From:" BroadWorks "<sip:+12403333333@10.20.20.20>;tag=958BDDF4-1AB
To:<sip:+19991111111@domain.com>
Date:Thu, 03 Nov 2022 12:39:58 GMT
Call-ID:75D3B642-5AAB11ED-AC82BA3C-276254A1@10.20.20.30
Supported:100rel,timer,resource-priority,replaces,sdp-anat
Min-SE:14400
Cisco-Guid: 1976459008-1521160685-2893855292-0660755617
X-Cisco-Meet-Info:hostCIUserUuid="52f4c6cb-c6a3-4283-
a1ab04cc8828b7c1";meetingid="26551128462";siteUUID="ec6659987f473332e0531b04fc0
acaec"
X-Cisco-Org-Id:82e2eb35-1610-44e7-9b20-ab607e026270
User-Agent: Cisco-SIPGateway/IOS-16.12.2s
Timestamp: 1667479198
Session-ID:
e13cc71f24ae400669d5247d8306ac23;remote=00000000000000000000000000000000
Allow:INVITE,OPTIONS,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY,INFO,REGSTE
R
CSeq:101 INVITE
Contact:<sip:+12403333333@10.20.20.20:5060;transport=tcp>

```

```
Expires:180
Allow-Events:telephone-event
Max-Forwards:68
```

Where:

- INVITE Request URI contains the callback number
- Via header: contains the IP address of the CUBE which will be used to select the RoutingNE profile.
- X-Cisco-Info-Meet header: used to identify hostCIUserUuid, meetingid & siteUUID.

Upon receiving the INVITE, the NS uses the Via header to match with the RoutingNE “WebexMeetings”. This will in turn select the “wxm_routing” routing profile which contains the “wxm_Inst” instance of the OrigRedirect.

The NS OrigRedirect policy will then match the X-CISCO-MEET-INFO header

```
X-Cisco-Meet-Info:hostCIUserUuid="52f4c6cb-c6a3-4283-
a1ab04cc8828b7c1";meetingid="26551128462";siteUUID="ec6659987f473332e0531b04fc0
acaec
```

with the Line Port configured on the VoiceXML virtual subscriber and send a 302 redirect to the AS pair hosting that subscriber. The 302 message is similar to the following:

```
SIP/2.0 302 Moved temporarily
Via:SIP/2.0/TCP 10.165.196.30:5060;branch=z9hG4bK5452684
From:" Webex "<sip:+12403332200@10.165.196.30>;tag=8EEAA586-1675
To:<sip:+14519615001@10.155.6.172>;tag=394411970-1602687588994
Call-ID:ABC5CCA2-D6411EB-8AD6D92D-EE20F768@10.165.196.30
CSeq:101 INVITE
Contact:<sip:+14519615001@hs2-bwks-v-as01-alpha.bwlab.org:5060;user=phone> ;q=0.5,
<sip:+14519615001@hs2-bwks-v-as02-alpha.bwlab.org:5060;user=phone>;q=0.25
Content-Length:0
```

Alias

The domain in the INVITE URI (in the example, it's bw.myenterprise.com) sent by the CUBE to the NS has to be recognized by the NS. This can be done by adding the domain on the NS_CLI/System/Alias context, for example:

```
NS_CLI/System/Alias> add bw.myenterprise.com
```

The command to configure the INVITE URI domain on the CUBE can be found in the in the next section, under dial-peer/session target, for example:

```
dial-peer voice 23401 voip
  session target dns:bw.myenterprise.com
```

HostingNE

To support Webex Meetings call processing configuration options for billing and Session Admission Control, the Application Server's Hosting NE signaling attributes *CallTypeInfoRequired* and *RequiresChargeIndication* must be enabled on the NS_CLI/System/Device/HostingNE context. For example:

```
NS_CLI/System/Device/HostingNE> set broadworksASHostNe signaling E164Compliant,  
    CallTypeInfoRequired, SourceId, RequiresNetworkIndication  
    RequiresChargeIndication;
```

Enable Webex Meeting Callback

In the callback scenario with the SIP X-Cisco-Meet-Info header, the CUBE sends the call to Network Server for originator redirect to the AS pair. The AS pair is determined based on the ***enableWebexMeetingHostLookup*** system parameter.

```
NS_CLI/System/CallP/Options> get  
    accessSideRoutingNeDeterminedViaSignaling = false  
    disableNdcValidationForCalledNumbers = true  
    forceRoutingNEProfile = false  
    skipPrivatePoliciesOnEmergency = true  
    maxReturnedContacts = 10  
    enableWebexMeetingHostLookup = true
```

When ***enableWebexMeetingHostLookup*** system parameter is set to true, the meeting host user CI UUID in the X-Cisco-Meet-Info header is used to identify the AS pair hosting the meeting host user.

```
INVITE sip:+19991111111@domain.com:5060 SIP/2.0  
Via:SIP/2.0/TCP 10.10.10.10:5060;branch=z9hG4bK7C7B9EB  
Remote-Party-ID:" BroadWorks  
    "<sip:88622222222@domain.com>;screen=no;party=calling;privacy=off  
From:" BroadWorks "<sip:+12403333333@10.20.20.20>;tag=958BDDF4-1AB  
To:<sip:+19991111111@domain.com>  
Date:Thu, 03 Nov 2022 12:39:58 GMT  
Call-ID:75D3B642-5AAB11ED-AC82BA3C-276254A1@10.20.20.30  
Supported:100rel,timer,resource-priority,replaces,sdp-anat  
Min-SE:14400  
Cisco-Guid: 1976459008-1521160685-2893855292-0660755617  
X-Cisco-Meet-Info:hostCIUserUuid="52f4c6cb-c6a3-4283-alab-  
    04cc8828b7c1";meetingid="26551128462";siteUUID="ec6659987f473332e0531b04fc0acae  
    c"  
X-Cisco-Org-Id:82e2eb35-1610-44e7-9b20-ab607e026270  
User-Agent: Cisco-SIPGateway/IOS-16.12.2s  
Timestamp: 1667479198  
Session-ID:  
    e13cc71f24ae400669d5247d8306ac23;remote=00000000000000000000000000000000  
Allow:INVITE,OPTIONS,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY,INFO,REGIST  
    ER  
CSeq:101 INVITE  
Contact:<sip:+12403333333@10.20.20.20:5060;transport=tcp>  
Expires:180  
Allow-Events:telephone-event  
Max-Forwards:68
```

Step 10: Provision Partner CUBE (or your own SBC)

This section provides a validated configuration for how to deploy Cisco Unified Border Element (CUBE) as the Session Border Controller (SBC) for the Bring Your Own PSTN Solution.

This section focuses on the CUBE configurations that are necessary to interwork with the example Webex for Cisco BroadWorks configuration shown in the previous section. For a more general discussion of initial CUBE deployment and configuration, refer to the following guides:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/configuration/cube-book/voi-cube-overview.html>

<https://help.webex.com/en-us/b6vrdc/Cisco-Webex-Edge-Audio-for-CUBE-Customer-Configuration-Guide>

Deploy Your Own SBC Option

If you don't want to deploy CUBE, you have the option to deploy your own SBC. However, note that this document does not provide a validated configuration for SBCs other than CUBE.

If you deploy your own SBC, you can follow the high-level CUBE configuration requirements (for example, assignments such as the domain, public and private interfaces, and gateways) to guide your configuration. However, refer to your SBC documentation for detailed command line help as the actual commands for your own SBC will likely differ from CUBE.

NOTE: Unless specified otherwise, the remaining configuration requirements in Step 10 apply no matter which SBC you deploy. However, the command line examples are for CUBE only, unless specified that the example applies for other SBCs. For other SBCs, refer to your SBC documentation for configuration commands.

Initial Configuration

To configure CUBE, the privileged EXEC mode must be enabled. If prompted, enter the password.

```
enable
```

To enter global configuration mode:

```
configure terminal
```

Set the domain:

```
ip domain name myenterprise.com
```

Set the Maximum Segment Size (MSS):

```
ip tcp mss 1360
```

Networking Configuration

Define the public and private interfaces. In our CUBE example:

```
----- Private side -----
interface GigabitEthernet1
  description Interface facing BC
  ip address <CUBE PRIV IP> <SUBNET MASK>
  negotiation auto
  no mop enabled
  no mop sysid
!
----- Public side -----
interface GigabitEthernet2
  description Interface facing WEBEX
  ip address <CUBE PUB IP> <SUBNET MASK>
  negotiation auto
  no mop enabled
  no mop sysid
!
```

Configure the gateways for IP Routing for the public and private sides:

```
ip route 0.0.0.0 <PUB SUBNET MASK> <CUBE PUB GW IP>
ip route 10.0.0.0 <PRIV SUBNET MASK> <CUBE PRIV GW IP>
```

Enable SSH:

```
ip ssh logging events
ip ssh version 2
!
username admin privilege 15 password <password>
```

Note that CUBE (or your own SBC) must be inside a DMZ with properly configured firewall rules. See section *Ports used by Webex* for the list of ports to open on the external firewall.

Configure SRV records for callback calls sent from CUBE (or your SBC) to the BroadWorks Network Servers. For example, the SRV for bw.myenterprise.com:

```
ip host _sip._tcp.bw.myenterprise.com srv 1 50 5060 ns01.myenterprise.com
ip host _sip._tcp.bw.myenterprise.com srv 1 50 5060 ns02.myenterprise.com
ip host ns01.myenterprise.com <NS01 IP>
ip host ns02.myenterprise.com <NS02 IP>
```

Configure the DNS server:

```
ip name-server <DNS_IP_address>
```

NOTE: An alternative DNS option is to configure internal DNS where the internal DNS reaches out to a parent DNS server if the internal lookup fails.

Call Processing Configuration

General

Configure the CUBE (or your SBC) with all IP addresses that need to access the VoIP service. This includes:

- Private side SIP signaling addresses for the BroadWorks AS, NS and MS servers.
- Public side addresses for Webex Edge for Audio infrastructure.

See below for an example CUBE configuration:

```
voice service voip
ip address trusted list
  ----- IPs on private side (needs to include all BroadWorks AS, NS and MS
    signaling addresses) -----
  ipv4 <NS01 IP>
  ipv4 <NS02 IP>
  ipv4 <AS01 IP>
  ipv4 <AS02 IP>
  ipv4 <MS01 IP>
  ----- IPs on public side (These are the public addresses for the Webex audio
    infrastructure. The below range is an example only.) -----
  ipv4 64.68.96.0 255.255.224.0
  ipv4 66.114.160.0 255.255.240.0
  ipv4 66.163.32.0 255.255.224.0
```

NOTE: The above IP address range is an example. For the current list of public IP addresses for the Webex audio infrastructure, go to:

- [How Do I Allow Webex Meetings Traffic on My Network?](#)—The IP Address range for most clusters appears under **List of IP address ranges used by Cisco Webex Meeting Services**. One exception is for China clusters, for which the range appears at the below link:
- [Network Requirements for Cisco Webex China Cluster](#)

The default timer for the CUBE to establish a TCP connection before it route advances is 20 seconds. To change it:

```
ip tcp synwait-time <5-300 (seconds)>
```

On BroadWorks side, the default timer for the Application Server to time out on an unresponsive access device is 6 seconds. To change it:

```
AS_CLI/System/CallP/AccessRouting> set terminationAttemptTimeoutSeconds <1-15
(seconds)>
```

The public and private side interfaces for RTP traffic on CUBE (or your own SBC) need to be opened. See below for the CUBE example:

```
voice service voip
rtcp all-pass-through
media disable-detailed-stats
  ----- CUBE public IP + port range -----
media-address range <CUBE PUB IP> <CUBE PUB IP> port-range 10200-28000
  ----- CUBE private IP + port range -----
```

```
media-address range <CUBE PRIV IP> <CUBE PRIV IP> port-range 10200-28000
```

Where:

- <CUBE PUB IP> is the public IP address of the CUBE
- <CUBE PRIV IP> is the private IP address of the CUBE
- Port-range: in the example, port range from 10200 to 28000

The CUBE supports the following TLS cipher suites (during call-in, CUBE offers these in the TLS Handshake's Client Hello):

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV

Other general settings to configure (see below for sample CUBE configurations):

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
!
ip scp server enable
!
voice service voip
address-hiding
allow-connections sip to sip
no supplementary-service sip moved-temporarily
call-quality
max-dropout 2
max-reorder 2
sip
contact-passing
```

Uri's for inbound and outbound dialing must be defined for later use in dial-peers:

```
voice class uri INEdgeAudio sip
pattern x-cisco-webex-service=audio
!
voice class uri OUTEdgeAudio sip
host cube.internal.local
```

Webex Edge Audio supports G722, G711ulaw, and G711alaw codecs. The following voice class code must be defined for later use in dial peers:

```
voice class codec 3
```

```
codec preference 1 g722-64
codec preference 2 g711ulaw
codec preference 3 g711alaw
```

Webex Edge Audio uses SRTP. The voice class SRTP-crypto assigns the preferred SRTP crypto suite to use for Edge Audio. Configure the following crypto suites in order. The voice class srtp-crypto configuration must be applied to the dial-peers used for the connection with Edge Audio.

```
voice class srtp-crypto 234
  crypto 1 AEAD_AES_256_GCM
  crypto 2 AEAD_AES_128_GCM
  crypto 3 AES_CM_128_HMAC_SHA1_80
  crypto 4 AES_CM_128_HMAC_SHA1_32
```

Preconfigure a primary key to be able to set a password for authentication

```
key config-key password-encrypt Password123 authentication username <username>
password encryption aes
```

Enter the SIP authentication credentials that was provisioned for the VoiceXML virtual subscriber on the AS using the following command. For callback scenarios, these credentials will be used when AS challenges the INVITE that the CUBE (or your own SBC) sends to the AS.

```
sip-ua
----- to enable authentication -----
authentication username <username> password 0 <password>
```

Once the authentication is configured, the password will be obfuscated when viewing with the “show running-config” command

```
sip-ua
----- to enable authentication -----
authentication username <username> password 6 [GF]XXXXX[YYYYYY\ZZZZZ]\
```

The following global SIP configuration must also be done:

```
----- Max INVITE retries -----
retry invite 3
----- By default, use TLS -----
transport tcp tls v1.2
connection-reuse
----- What trustpoint to use when mTLS is challenged -----
crypto signaling default trustpoint <trustpoint>
```

Translation Profiles

The SIP message translation profile 2340 is used for Meeting call-in calls. It should have an entry to modify the SIP messages incoming from BroadWorks before sending out to Edge Audio, as shown in the example rule 11 below in red.

```
----- BroadWorks to Webex -----
voice class sip-profiles 2340
rule 1 request INVITE sip-header SIP-Req-URI modify "sips:" "sip:"
rule 2 request INVITE sip-header To modify "sips:" "sip:"
rule 3 request INVITE sip-header From modify "sips:" sip:
rule 4 request INVITE sip-header Remote-Party-ID modify "sips:" "sip:"
rule 5 request INVITE sip-header P-Asserted-Identity modify "sips:" "sip:"
rule 6 request ACK sip-header From modify "sips:" "sip:"
rule 7 request REINVITE sip-header P-Asserted-Identity modify "sips:" "sip:"
rule 8 request REINVITE sip-header From modify "sips:" "sip:"
rule 9 request REINVITE sip-header Contact modify "sips:(.*)>"
"sip:\1;transport=tls>"
rule 10 request INVITE sip-header Contact modify "sips:" "sip:"
rule 11 request INVITE sip-header SIP-Req-URI modify "cube.internal.local"
"ecccspx.amer.pub.webex.com"
```

The above rule 11 maps the incoming Request Uri from BroadWorks, which has the Contact value of the CUBE virtual subscriber device profile (value of the Contact field in the VXML_deviceProf Device Profile in our example):

```
88631321777971704941@cube.internal.local;x-cisco-site-
  uuid=abbd70f6c519fb1ee053ad06fc0a038b;transport=tcp
```

To the appropriate Webex Edge Audio Call Routing Domain:

```
88631321777971704941@ecccspx.amer.pub.webex.com;x-cisco-site-
  uuid=abbd70f6c519fb1ee053ad06fc0a038b;transport=tcp
```

Note that when CUBE (or your own SBC) is behind a static NAT, additional configuration to the sip-profile 2340 is required. Refer to the following link for more information:

<https://help.webex.com/en-us/b6vrdc/Cisco-Webex-Edge-Audio-for-CUBE-Customer-Configuration-Guide>

NOTE: If you deploy your own SBC, you will need to configure similar rules on your own SBC.

In order to forward 486 messages sent by the AS back to the Webex Edge Audio, the following configuration is required on CUBE (for your own SBC, refer to your SBC documentation for help)

```
voice service voip
  no notify redirect ip2ip
  sip
    sip-profiles inbound
!
voice class sip-profiles 1
  response 486 sip-header Reason modify "7" ""
  response 486 sip-header SIP-StatusLine modify "486.*" "600 Busy Everywhere"
```

If other 4xx messages need to be forwarded back to the Webex Edge Audio, follow the same example above.

Dial Peers

A voice class tenant must be defined on CUBE (or your own SBC) for use in the dial peers later on, which satisfies the following criteria:

- There is no payload interworking that is needed for RTP-NTE DTMF packets, so configure asymmetric payload full.
- Edge audio doesn't support caller ID updates, so the "no update-callerid" value must be configured.
- Webex Edge Audio call routing is based on URIs. The call-route URI must be enabled to match dial-peers based on URIs.

```
voice class tenant 234
  asymmetric payload full
  no update-callerid
  Header-passing
  no pass-thru content custom-sdp
  call-route url
```

The following dial peers are configured to allow the CUBE to process calls between BroadWorks and Webex Edge Audio. Configure the following on CUBE (a similar configuration would need to be configured on your own SBC):

```
dial-peer voice 23411 voip
  description External Webex edge audio entry or exit dial-peer
  session protocol sipv2
  session target dns:ecccspx.amer.pub.webex.com
  session transport tcp tls
  destination uri OUTEdgeAudio
  incoming uri request INEdgeAudio
  voice-class codec 3 offer-all
  voice-class sip url sips
  voice-class sip profiles 2340
  voice-class sip tenant 234
  voice-class sip srtp-crypto 234
  voice-class sip bind control source-interface GigabitEthernet2
  voice-class sip bind media source-interface GigabitEthernet2
  voice-class sip requi-passing
  voice-class sip audio forced
  dtmf-relay rtp-nte
  srtp
!
dial-peer voice 23401 voip
  description Internal mix mode Webex edge audio entry or exit dial-peer
  session protocol sipv2
  ---- using DNS SRV (preferred) - must match srv record configured above
    (_sip._tcp.bw.myenterprise.com) ----
  session target dns:bw.myenterprise.com
```

```

session transport tcp
destination uri INEdgeAudio
incoming uri request OUTEdgeAudio
voice-class codec 3
voice-class sip url sip
voice-class sip profiles 2341
voice-class sip profiles 1 inbound
voice-class sip tenant 234
voice-class sip bind control source-interface GigabitEthernet1
voice-class sip bind media source-interface GigabitEthernet1 dtmf-relay rtp-nte
!

```

CUBE Call flows

With the configuration done above, examples of the incoming/outgoing call flow scenarios on the CUBE are described below. The color coding on a specific step relates it to the same color entries in the dial peers above.

NOTE: If you are deploying your own SBC, refer to your SBC documentation for details on call flows with your SBC.

For a Meeting Call-In scenario from BroadWorks to Webex:

- An incoming INVITE is received from BroadWorks on the internal interface with:

```

INVITE sip: 88631321777971704941@cube.internal.local;transport=tcp;x-cisco-
site-uuid=abbd70f6c519fb1ee053ad06fc0a038b SIP/2.0
To:"VXML Virtual"<sip: 88631321777971704941@ecccspx.amer.pub.webex.com;x-cisco-
site-uuid=abbd70f6c519fb1ee053ad06fc0a038b>

```

- The incoming dial peer profile 23401 is selected based on the host in the incoming request URI ("cube.internal.local") matching the "incoming uri request OUTEdgeAudio" configuration.
- The outgoing dial peer 23411 is selected based on the host in the request URI ("cube.internal.local") matching the "destination uri OUTEdgeAudio" configuration.
- An outgoing INVITE is sent on the external interface with the host in the request URI changed from "cube.internal.local" to "ecccspx.amer.pub.webex.com" using the "voice-class sip profiles 2340" message translation profile specified in the dial peer:

```

INVITE sip: 88631321777971704941@ecccspx.amer.pub.webex.com;transport=tcp;x-
cisco-site-uuid=abbd70f6c519fb1ee053ad06fc0a038b SIP/2.0
To: " VXML Virtual" <sip: 88631321777971704941@ecccspx.amer.pub.webex.com;x-
cisco-site-uuid=abbd70f6c519fb1ee053ad06fc0a038b>

```

For a Meeting Callback scenario from Webex to BroadWorks

- An incoming INVITE is received from Webex on the CUBE external interface with:

```

INVITE sip:+14519615001@cube.us.example.com;transport=tls;x-cisco-site-
uuid=abbd70f6c519fb1ee053ad06fc0a038b;x-cisco-webex-service=audio SIP/2.0
To: sip:+14519615001@cube.us.example.com;type=carrier_sbc
X-Cisco-Meet-Info:hostCIUserUid="52f4c6cb-c6a3-4283-
alab04cc8828b7c1";meetingid="26551128462";siteUUID="ec6659987f473332e0531b04fc0
acaec

```

- The incoming dial peer 23411 is selected based on the pattern “x-cisco-webex-service=audio” being present in the incoming request URI based on the “incoming uri request INEdgeAudio” configuration.
- Two outgoing dial peers are chosen based on the pattern “x-cisco-webex-service=audio” being present in the request URI based on the “destination uri INEdgeAudio” configuration.
 - Dial Peer 302
 - Dial Peer 23401
- An outgoing INVITE is sent to the Network Servers (SRV lookup based on “session target dns:bw.myenterprise.com entry” in the dial peer) on the internal interface

```
INVITE sip:+14519615001@10.155.6.172:5060 SIP/2.0
X-Cisco-Meet-Info:hostCIUserUuid="52f4c6cb-c6a3-4283-
alab04cc8828b7c1";meetingid="26551128462";siteUUID="ec6659987f473332e0531b04fc0
acaec"
From: " Webex " ;tag=B91821B7-561
```

- The Network Server returns contacts for the AS pair hosting the CUBE virtual subscriber:

```
SIP/2.0 302 Moved temporarily
Via:SIP/2.0/TCP 10.165.196.30:5060;branch=z9hG4bK880BD
From:" Webex "<sip:+12404540887@10.165.196.30>;tag=B91821B7-561
To:<sip:+14519615001@10.155.6.172>;tag=1829261807-1603395221529
Call-ID:3C88DF6A-13D411EB-8EE3D92D-EE20F768@10.165.196.30
CSeq:101 INVITE
Contact:<sip:+14519615001@hs2-bwks-v-as01-
alpha.bwlab.org:5060;user=phone;transport=tcp>;q=0.5,<sip:+14519615001@hs2-
bwks-v-as02-alpha.bwlab.org:5060;user=phone;transport=tcp>;q=0.25
Content-Length:0
```

- The CUBE routes the call to the active AS based on the returned contact in the 302 message:

```
INVITE sip:+14519615001@hs2-bwks-v-as01-
alpha.bwlab.org:5060;user=phone;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 10.165.196.30:5060;branch=z9hG4bK8812341
X-Cisco-Meet-Info:hostCIUserUuid="52f4c6cb-c6a3-4283-
alab04cc8828b7c1";meetingid="26551128462";siteUUID="ec6659987f473332e0531b04fc0
acaec"
From: " Webex " <sip:+12404540887@10.165.196.30>;tag=B91821C8-1AF5
To: <sip:+14519615001@10.155.6.172>
```

mTLS Configuration

The following configuration steps must be done to allow mTLS connections between CUBE (or your own SBC) and Webex Edge Audio.

NOTE: It's mandatory that you configure mTLS between CUBE (or your own SBC) and Webex Edge Audio.

Wildcard Certificate Support

Wildcard signed certificates use a generic subject-name (e.g., *.us.example.com) that corresponds to the domain for CUBE or your own SBC.

Wildcard certificates are supported for multi-cluster CUBE or SBC deployments but are not supported for single node CUBE or SBC deployments.

Trustpool

During the TLS handshake, when the Webex Edge Audio sends its certificate, the CUBE will validate it against the list of certificates accepted in the trustpool.

The trustpool bundle has to be updated with the Cisco Root CA by downloading the latest “Cisco Trusted Core Root Bundle” from <http://www.cisco.com/security/pki/> using the command:

```
crypto pki trustpool import clean url <url>
```

The certificates sent by Webex Edge Audio are signed by IdenTrust. Make sure that the “IdenTrust Commercial Root CA” certificate is installed. See this link for more details:

<https://help.webex.com/en-us/WBX9000008850/What-Root-Certificate-Authorities-are-Supported-for-Calls-to-Cisco-Webex-Audio-and-Video-Platforms>

NOTE: If you are using your own SBC, and are unable to complete the import, you can convert the bundle to .pem format using open-source tools, such as OpenSSL. For example, you could use hydrantID certificates with the following command: `openssl x509 -inform der -in certificate.cer -out certificate.pem`

Trustpoint

Edge Audio requires your CUBE to offer signed certificates from trusted CA certificate authorities for Mutual TLS (mTLS) connections. Use the following link to get to a list of certificate authorities that Cisco trusts. Certificates that are signed by authorities in this list are considered valid and the connection will be allowed: <https://help.webex.com/en-us/WBX9000008850/What-Root-Certificate-Authorities-are-Supported-for-Calls-to-Cisco-Webex-Audio-and-Video-Platforms>

Single Node CUBE

Single node means that the CUBE (or your own SBC) will import a certificate with the subject-name unique to its FQDN, which means that no other CUBE would be able to import it (in other words, NOT a wildcard certificate).

- To create the CSR (Certificate Signing Request) for CUBE:
 - create keypair (this keypair will be linked to the trustpoint)

```
CUBE(config)# crypto key generate rsa general-keys label <key label> exportable
```

- general-keys - Specifies that the general-purpose key pair should be generated.
- label <key-label> - (Optional) Name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used.
- exportable - (Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router.

- create trustpoint (A trustpoint contains the certificate that you want to bind on the CUBE. When the CUBE receives a certificate request, it will respond with the trustpoint's certificate attached)

```
CUBE(config)#crypto pki trustpoint <trustpoint>
CUBE(ca-trustpoint)#
    crl optional
    enrollment terminal pem
    fqdn <fqdn>
    subject-name CN=<fqdn>
    rsakeypair <key label>
```

crl - A certificate revocation list (CRL) is a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when each certificate was issued and when it expires.

enrollment terminal pem - Adds privacy-enhanced mail (PEM) boundaries to the certificate request (manual copy-paste from BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST)

fqdn – Fully qualified domain name of the CUBE

subject-name CN=<fqdn> - the subject name to sign

rsakeypair <key label> - the keypair generated from previous step

(reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/15-mt/sec-pki-15-mt-book/sec-cert-enroll-pki.html)

- generate CSR:

```
CUBE(config)#crypto pki enroll <trustpoint>
% Start certificate enrollment ..
...
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes

Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
...
-----END CERTIFICATE REQUEST-----

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
```

- Send the CSR (from BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST) to CA (Certificate Authority)
- CA will generate a signed certificate

- Depending on the CA, they will provide the root certificate (e.g. DigiCertCA.crt) and the requested certificate (e.g. cube.crt)

- Load the CA certificate

- First, authenticate the trustpoint with the root's certificate

```
CUBE(config)#crypto pki authenticate <trustpoint>
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
<ENTER THE ROOT CERT>
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint: 40065311 FDB33E88 0A6F7DD1 4E229187
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

- Then, import the CUBE's certificate on the trustpoint

```
CUBE(config)# crypto ca import <trustpoint> certificate
% The fully-qualified domain name in the certificate will be: ...

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

-----BEGIN CERTIFICATE-----
<ENTER THE FQDN CERT>
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

NOTE: If you are deploying your own SBC, refer to your SBC documentation for details on how to create the CSR.

Multi Node CUBE Cluster (Using Alternate Names in Certificate) - NOT Supported

Multi node means that the CUBE will be able to import the same certificate for more than one CUBE deployment. Using the subject alternate name to generate the CSR is currently not supported:

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCud90920/?rfs=iqvred>

Multi Node CUBE Cluster (Using wildcard signed certificate as pkcs12 format)

Multi node using a wildcard signed certificate means that the subject-name is generic (e.g., *.us.example.com) and it corresponds to the CUBE's domain (or your SBC domain).

- Assuming you have a wildcard certificate ready, get the public (.crt) and private key (.key) files ready
- Using OpenSSL, create a bundled PKCS12 format (.pfx) file including the .crt and .key file: (use cygwin on Windows) - reference: <https://www.ssl.com/how-to/create-a-pfx-p12-certificate-file-using-openssl/>

```
openssl pkcs12 -export -out <pfxfilename>.pfx -inkey <privatekeyfile>.key -in
<certfile>.crt
```

- Transfer the .pfx file in the CUBE:bootflash: (scp from Linux server to CUBE)

```
scp <pfxfilename>.pfx <user>@<CUBEIP>:bootflash:<pfxfilename>.pfx
```

- Create a trustpoint and import the pkcs12 file:

```
CUBE# conf t
CUBE(config)#
CUBE(config)# crypto pki trustpoint <trustpoint>
CUBE(ca-trustpoint)# revocation-check crl
CUBE(ca-trustpoint)# exit
CUBE(config)# crypto pki import <trustpoint> pkcs12 bootflash:<pfxfilename>.pfx
password <password>
```

Validate the CUBE Certificate Configuration

Verify that the entire chain is included in the certificate. The following example shows validation commands for CUBE. If you are deploying your own SBC, use the commands that apply to your SBC.

```
CUBE(config)#crypto pki certificate validate <trustpoint>
Chain has 2 certificates
Certificate chain for <trustpoint> is valid

CUBE#show crypto pki trustpoints status
...
Trustpoint <trustpoint>:
  Issuing CA certificate configured:
  Subject Name:
    cn=HydrantID SSL ICA G2,o=HydrantID (Avalanche Cloud Corporation),c=US
  Fingerprint MD5: 1135E326 56E5AADF 53A4DD32 C8D5590F
  Fingerprint SHA1: AC4A728B 4DFC3560 1FA34B92 2422A42C 253F756C
  Router General Purpose certificate configured:
  Subject Name:
    cn=*.us.example.com,ou=Webex,o=Cisco Systems, Inc.,l=San
    Jose,st=California,c=US
  Fingerprint MD5: 756E4C83 CF36311A 7839FA51 7FA7ABA0
  Fingerprint SHA1: 8268817F 79EF91E0 3BA976A1 5C9D97F3 E834EB54
  State:
    Keys generated ..... Yes (General Purpose, non-exportable)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

Set SIP signaling to use trustpoint

Use the following command to provision the SIP UA with the CUBE trustpoint. Following is an example for CUBE. If you are deploying your own SBC, refer to your SBC documentation for command help.

```
CUBE(config)#sip-ua
CUBE(config-sip-ua)#crypto signaling default trustpoint <trustpoint>
```

CUBE Logs

To see enabled debug filters

```
CUBE# show debug
```

To set debug filters (examples)

```
CUBE# debug ccsip messages
CUBE# debug ccsip transport
CUBE# debug ccsip error
CUBE# debug ccsip info
CUBE# debug voip dialpeer inout
CUBE# debug voip ccapi inout
CUBE# debug voip application
CUBE# debug ip tcp transaction
```

To unset debug filters (example)

```
CUBE# no debug ccsip messages
```

To clear and check log buffer

```
CUBE# clear log
>>> make test call <<<
CUBE# show log
```

NOTE: If you are not deploying CUBE, refer to the documentation for your own SBC for details on how to use logs.

Other useful commands

To check current config

```
CUBE# show running-config (or just CUBE# show run)
```

To save config to ROM which will be used when booted

```
CUBE# write
```

Step 11: BYoPSTN Certification

After the configuration and provisioning of the BYoPSTN solution is completed, the Partner is required to run through a set of acceptance test cases in order to certify their solution. This is a required step for the Partner BYoPSTN to be approved and enabled.

The acceptance test cases are outlined in the document *Bring Your Own PSTN Acceptance Procedure Webex For Cisco BroadWorks at*

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/wx4bwks/BYoPSTN/BYoPSTN_Acceptance.pdf.

The partner should provide the results of the successfully executed acceptance tests to the onboarding and certification teams.

Questions, issues and results from the execution of the acceptance test cases should be reported and shared in the Webex space assigned for onboarding the Partner.

Apply updates to an in-service Phone Number Group/Callback DNS SRV Group

Once non-test customers are assigned to a Customer Template using Partner provided call-in numbers, the following meeting join options are available to those users:

- Meeting invites include one or more default phone numbers from the assign Phone Number Group
- Webex App displays one or more default phone numbers from the assign Phone Number Group as a meeting join option
- Webex Meeting site UI displays one or more default phone numbers from the assign Phone Number Group as a meeting join option
- If callback has been enabled on the Customer Template, Webex Meeting provides the 'Call me at' option where the callback request is routed to one of the records specified in the assigned DNS SRV Callback Group

A change to meeting join options for a Customer Template or a change to an assigned Phone Number Group or a change to a Callback DNS SRV Group can affect the above meeting join options. These changes do not apply to existing customers, but newly provisioned customers will see these changes reflected immediately for their Standard and Premium package meeting sites. Therefore, it is highly recommended that any such change is verified using a seed solution organization before being applied to existing Customer Templates, Phone Number Groups or Callback DNS SRV Groups (if Callback DNS SRV Groups are deployed).

The following steps should be followed when making an update to the meeting join options for a customer template and/or applying updates to Phone Number Groups or Callback DNS SRV Groups.

Please note if the Customer Templates, Phone Number Groups or Callback DNS SRV Groups are in use by test BroadWorks Service Providers and/or test BroadWorks Enterprises, this procedure is optional. It may be more appropriate to simply delete the test BroadWorks Service Providers and/or test BroadWorks Enterprises organizations and re-provision them using the updated Customer Templates, Phone Number Groups or Callback DNS SRV Groups.

Update Phone Number Group only:

1. Create a new temporary Phone Number Group with the required updates.
2. Create a new temporary Customer Template that uses the new Phone Number Group. If an existing Phone Number Group is being used along with the group, assign that to the template.
3. Create a seed solution organization by provisioning a subscriber from a test BroadWorks Service Provider or test BroadWorks Enterprise with a Standard package using the new Customer Template. Please note that this is a secondary seed solution organization, no update to the meeting siteUUID configured on BroadWorks is required.
4. Download the BroadWorks Configuration (BYoPSTN) JSON file, it contains the phone number to access code mapping for the new phone numbers in the Phone Number Group.
5. Determine the Webex Edge Audio DNS SRV domain for the seed solution organization Standard package meeting site. It should be unchanged from the value previously determined for the original Phone Number Group.
6. Apply the configuration updates to BroadWorks using the BroadWorks Configuration (BYoPSTN) JSON file.
7. Verify the configuration by scheduling meetings using the seed organization Standard package site and joining the meeting using the call-in phone numbers.

8. Apply the update to the original Phone Number Group. The change is now in-service for non-test customers.
9. The seed solution organization, the temporary Phone Number Group, and Customer Template can be deleted. These elements are no longer required once the original Phone Number Group has been updated.

Update Callback DNS SRV Group Only:

1. Create a new temporary DNS SRV Callback Group with the required updates.
2. Create a new temporary Customer Template that uses the new Callback DNS SRV Group and existing Phone Number Group. If an existing DNS SRV Callback Group is being used along with the group, assign that to the template.
3. Create a seed solution organization by provisioning a subscriber from a test BroadWorks Service Provider or test BroadWorks Enterprise with a Standard package using the new Customer Template. Please note that this is a secondary seed solution organization, no update to the meeting siteUUID configured on BroadWorks is required.
4. Verify the configuration by scheduling meetings using the seed organization Standard package site, joining the meeting using the call-in phone numbers, and using the 'Call me at' option.
5. Apply the update to the original DNS SRV Callback Group. The change is now in-service for non-test customers.
6. The seed solution organization, DNS SRV Callback Group and Customer Template can be deleted. These elements are no longer required once the original Callback DNS SRV Group has been updated.

Update both Phone Number and Callback DNS SRV Group:

1. Create a new temporary Phone Number and DNS SRV Callback Group with the required updates.
2. Create a new temporary Customer Template that uses the new Phone Number Group and new Callback DNS SRV Group. If an existing Phone Number Group and/or DNS SRV Callback Group is being used along with the group, assign that to the template.
3. Create a seed solution organization by provisioning a subscriber from a test BroadWorks Service Provider or test BroadWorks Enterprise with a Standard package using the new Customer Template. Please note that this is a secondary seed solution organization, no update to the meeting siteUUID configured on BroadWorks is required.
4. Download the BroadWorks Configuration (BYoPSTN) JSON file, it contains the phone number to access code mapping for the new phone numbers in the Phone Number Group.
5. Determine the Webex Edge Audio DNS SRV domain for the seed solution organization Standard package meeting site. It should be unchanged from the value previously determined for the original Phone Number Group.
6. Apply the configuration updates to BroadWorks using the BroadWorks Configuration (BYoPSTN) JSON file.
7. Verify the configuration by scheduling meetings using the seed organization Standard package site, joining the meeting using the call-in phone numbers, and using the 'Call me at' option.
8. Apply the update to the original Phone Number and DNS SRV Callback Group. The change is now in-service for non-test customers.
9. The seed solution organization, the temporary Phone Number Group, DNS SRV Callback Group, and Customer Template can be deleted. These elements are no longer required once the original Phone Number Group and Callback DNS SRV Group has been updated.

Please note that the primary seed solution organization should not be deleted unless a new primary seed solution organization has been selected and configured on BroadWorks. Deleting the primary seed solution organization removes the siteUUID on which the BYoPSTN solution depends for SIP message authentication to Webex Edge Audio. If deleted, meeting joins using call-in for sites using Partner provided call-in number will fail.

G722 Media Interoperability when using your own SBC

When leveraging your own SBC, interoperability issues that are normally taken care of by CUBE need to be considered between the Cisco Partners BroadWorks Infrastructure and Webex Cloud. One example is a call-in or callback using G722 codec that involves the BroadWorks Media Server (for example, when using the BroadWorks Call Recording service). In this scenario, the Webex Edge Audio may send an SDP with "a=fmtp:9" line. Your SBC would need to update this line to add the bitrate parameter to have "a=fmtp:9 bitrate=64" before sending it to the BroadWorks backend.

Known Limitations

- Any changes to the Customer Template Meeting Join Option, Cisco call-in numbers, or Partner Provided call-in numbers are applied only to newly provisioned customers. Existing customers using the template remain unchanged.
- Any changes to the Customer Template Phone Number Group or Callback DNS SRV Group settings are applied only to newly provisioned customers or existing customers being provisioned for their first Standard or Premium package user. Existing customers that already have Standard or Premium package users remain unchanged.
- Any changes to the Phone Number Groups or Callback DNS SRV Groups that are assigned to Customer Templates are applied only to newly provisioned customers or existing customers being provisioned for their first Standard or Premium package user. Existing customers assigned to associated templates that already have Standard or Premium package users remain unchanged.
- A given Customer Template supports Cisco call-in numbers or Partner provided call-number meeting join option, a combination of the two options for the same template is not supported.
- The SIP messaging for 'Call me at' or callback meeting join use case does not include information on the customer and/or user that is hosting the meeting to be joined.
- The phone numbers and associated meeting access codes for a given Phone Number Group, only support a single Webex Edge Audio DNS SRV domain (for example, `ecccspx.amer.webex.com`). Using these phone numbers to call-in to meetings in a different Webex Edge Audio DNS SRV domain is not supported.
- Webex Edge Audio does not support renegotiating codecs mid call. As such, services that are invoked after a call is answered may not work properly.
- Webex App, Webex Meeting site UI and the Webex Meeting invite email provides a link to a "Toll-free calling restrictions" document. This document is specific to Cisco-provided phone numbers and should be ignored by users when using Partner provided phone numbers for meeting joins.