Cisco Preferred Architecture for Cisco Webex Calling

Design Overview

May 2021
Contents

What’s New in This Guide ................................................................. 4
Preface ................................................................................................. 6
  Documentation for Cisco Preferred Architectures ........................................6
  Use Case ............................................................................................. 6
  About This Guide ................................................................................ 6

Introduction ......................................................................................... 7
  Cisco Webex Calling Solution Overview ................................................ 7
  Supported Devices .............................................................................. 7
  Video Support .................................................................................... 8

Architectural Overview ....................................................................... 9
  Webex Calling Datacenters ............................................................... 10
  Over-the-top TLS Connections ......................................................... 10
  PSTN Access and On-Premises Interconnect ....................................... 11
    Multiple PSTN Providers ................................................................ 12
    Trunks and Route Groups ................................................................ 12
    Local Gateway Registration ......................................................... 14
    Dedicated or Co-Resident Local Gateway ...................................... 15
    Partner Hosted Local Gateway ...................................................... 16
    Local Gateway Call Setup ............................................................. 17

Dial Plans ............................................................................................. 18
  Patterns and pattern matching ......................................................... 18
  Interconnect with On-Premises Call Control .................................... 19
  Combining Premises Trunk and Cloud PSTN for PSTN Access .......... 19
  Multiple On-Premises Call Control ................................................. 20
  Unknown Number Handling ........................................................... 21
  Trunk calls to Webex Calling ........................................................... 22
  Allowed transit calls and caller ID selection ...................................... 23
  Outbound caller ID on trunks for calls from Webex Calling users ... 23
  Service interactions ......................................................................... 24

Media Flows ........................................................................................ 25
  Media Flows for Co-located and PSTN Calls ..................................... 25
  Media Flows for Calls between Different Webex Calling Customers ... 26
  Webex Calling Regions .................................................................... 27

Deployment Aspects .......................................................................... 30
  Location Definitions .......................................................................... 30
  Local Gateway Deployment Options ............................................... 31
    CUBE High Availability as Local Gateway .................................. 31
  Firewall Requirements ..................................................................... 33
    Intrusion Protection System Requirements .................................. 36
  Codec Selection .............................................................................. 36
  Bandwidth Considerations .............................................................. 37
  Directory Integration ...................................................................... 39
    Directory Connector Architecture .............................................. 39
  Dial Plan ........................................................................................... 40
    PSTN Destinations ........................................................................ 40
    PSTN Access Code ........................................................................ 40
    Abbreviated On-net Dialing .......................................................... 40
What's New in This Guide

Service Assurance.................................................................42
CScan ................................................................................42
Analytics............................................................................42

Case Study: Unified CM with Centralized Call Processing and multiple Webex Calling Locations .......... 46

Call Routing Considerations ..................................................49
Calls from Webex Calling to Unified CM ................................49
Calls from Unified CM to Webex Calling .................................52
Class of Service (CoS)............................................................53
Unified CM Dial Plan Integration ...........................................56
Local Gateway deployment ....................................................58
Webex Calling dial plan configuration .....................................59
## What’s New in This Guide

Table 1 provides a historical list of updated and new topics added to this guide.

<table>
<thead>
<tr>
<th>Date</th>
<th>Updated or New Topic</th>
<th>Update Details and Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2020</td>
<td>Initial document publication</td>
<td>Initial release</td>
</tr>
<tr>
<td>April 2021</td>
<td>Throughout document</td>
<td>Rebranding “Webex app”. Minor edits to text and illustrations to correct spelling, grammar, etc. based on feedback.</td>
</tr>
<tr>
<td></td>
<td>Premises-based PSTN</td>
<td>New term used throughout document to refer to PSTN access via on-premises Local Gateway</td>
</tr>
<tr>
<td></td>
<td>Webex Calling Regional Datacenters</td>
<td>New Webex Calling datacenters in Canada (<a href="#">Architectural Overview, Architectural Overview &gt; Webex Calling Regions</a>).</td>
</tr>
<tr>
<td></td>
<td>Cisco Calling Plans</td>
<td>Cisco Calling plans added as additional PSTN access option (<a href="#">Architectural Overview &gt; PSTN Access and On-Premises Interconnect</a>).</td>
</tr>
<tr>
<td></td>
<td>Trunks and Route Groups</td>
<td>New section (<a href="#">Architectural Overview &gt; PSTN Access and On-Premises Interconnect &gt; Trunks and Route Groups</a>). Local Gateway deployment design guidance (<a href="#">Case Study &gt; Local Gateway deployment</a>).</td>
</tr>
<tr>
<td></td>
<td>Dial Plans</td>
<td>New section (<a href="#">Architectural Overview &gt; Dial Plans</a>). Updated description of routing behavior for interconnect with on-premises call control (<a href="#">Architectural Overview &gt; Dial Plans &gt; Interconnect with On-Premises Call Control</a>). Combining premises trunks and Cloud PSTN as new deployment option (<a href="#">Architectural Overview &gt; Dial Plans &gt; Combining Premises Trunk and Cloud PSTN for PSTN Access</a>). Use Webex Calling dial plans to establish routing to on-premises call control (<a href="#">Deployment Aspects &gt; Dial Plan &gt; Abbreviated On-net Dialing</a>). Call routing between Webex Calling and Unified CM based on Webex Calling dial plans (<a href="#">Case Study &gt; Call Routing Considerations &gt; Calls from Webex Calling to Unified CM</a>). Best practices for Webex Calling dial plan configuration (<a href="#">Case Study &gt; Webex Calling dial plan configuration</a>).</td>
</tr>
<tr>
<td></td>
<td>Local Gateway concurrent calls</td>
<td>Design Guidance on Local Gateway concurrent calls scalability and network requirements (<a href="#">Deployment Aspects &gt; Local Gateway Deployment Options</a>).</td>
</tr>
</tbody>
</table>
## What's New in This Guide

<table>
<thead>
<tr>
<th>Date</th>
<th>Updated or New Topic</th>
<th>Update Details and Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Call Detail Records in Analytics</td>
<td>CDR availability in Analytics (<a href="#">Deployment Aspects &gt; Service Assurance &gt; Analytics</a>)</td>
</tr>
<tr>
<td></td>
<td>Combining Cloud Connected PSTN and Premises Based PSTN</td>
<td>Combining Cloud Connected PSTN and Premises Based PSTN is now an option (<a href="#">Case Study: Unified CM with Centralized Call Processing and multiple Webex Calling Locations</a>)</td>
</tr>
<tr>
<td></td>
<td>Called party number format for calls from Unified CM to Webex Calling</td>
<td>Clarification of called party number format options for calls from Unified CM to Webex Calling (<a href="#">Case Study &gt; Call Routing Considerations &gt; Calls from Unified CM to Webex Calling</a>)</td>
</tr>
</tbody>
</table>
Preface

Cisco Preferred Architectures provide recommended deployment models for specific market segments based on common use cases. They incorporate a subset of products from the Cisco Collaboration portfolio that is best suited for the targeted market segment and defined use cases. These deployment models are prescriptive, out-of-the-box, and built to scale with an organization as its business needs change. This prescriptive approach simplifies the integration of multiple system-level components and enables an organization to select the deployment model that best addresses its business needs.

Documentation for Cisco Preferred Architectures

- **Cisco Preferred Architecture** (PA) design overview guides help customers and sales teams select the appropriate architecture based on an organization’s business requirements; understand the products that are used within the architecture; and obtain general design best practices. These guides support sales processes.
- **Cisco Validated Design** (CVD) guides provide details for deploying components within the Cisco Preferred Architectures. These guides support planning, deployment, and implementation (PDI).
- **Cisco Collaboration Solution Reference Network Design** (SRND) guide provides detailed design options for Cisco Collaboration. This guide should be referenced when design requirements are outside the scope of Cisco Preferred Architectures.

Use Case

This Cisco Preferred Architecture (PA) for Cisco Webex Calling document describes how organizations can embrace growth without necessarily replacing their entire calling infrastructure. Additionally, the use case details call routing considerations for:

- **Calls from Webex Calling to Unified CM**
- **Calls from Unified CM to Webex Calling**
- **Class of Service (CoS)**
- **Dial Plan Integration**

Information about Cisco Collaboration Technologies and additional use cases is available on [Cisco.com](https://www.cisco.com).

About This Guide

This *Cisco Preferred Architecture for Cisco Webex Calling* provides architectural guidance on Cisco Webex Calling sold through a value-added reseller (VAR). Specifically covered, are deployments using Webex Calling as cloud-based call control in an isolated deployment or combined with an on-premises collaboration deployment as described in the enterprise PA documents.

Unless explicitly mentioned otherwise, the term “Webex Calling” in the context of this document always refers to Webex Calling (VAR).

Readers of this guide should have a general knowledge of Cisco Voice, Video, and Collaboration products and a basic understanding of how to deploy these products.

This guide simplifies the design and sales process by:

- Recommending products in the Cisco Collaboration portfolio that are built for the enterprise and that provide appropriate feature sets for this market
- Detailing a collaboration architecture and identifying general best practices for deploying in enterprise organizations

For detailed information about configuring, deploying, and implementing this architecture, consult the related CVD documents on the [Design Zone for Collaboration](https://www.cisco.com).
Introduction

Cisco Webex Calling Solution Overview

Enterprise-level decision makers recognize that installing, securing, and maintaining an on-premises private branch exchange (PBX) is both complex and expensive. As vendors develop additional features and functionality privately deployed PBX systems tend to become outdated and less secure.

Prior to the introduction of Webex Calling, cloud-based PBX solutions lacked features, functionality, performance, and security, and were not able to replace an enterprise PBX or PBX network.

Webex Calling is part of an integrated, intelligent, and modular team collaboration suite. It provides enterprise-grade PBX features, functionality, and performance previously only possible with an on-premises PBX network. Licensing is subscription-based and managed with the Cisco Collaboration Flex Plan. The solution integrates with Webex, specifically Webex devices, and optionally with Webex Meetings.

Webex Calling is deployed as a cloud-only solution, or if you require a mixed network of both cloud and on-premises PBXs, it is deployed as part of a hybrid cloud.

Webex Calling data centers are globally distributed and geo-redundant. Cisco Value-Added Reseller (VAR) channel partners distribute Cisco Webex Calling.

In addition to enterprise-grade PBX features, Webex Calling also provides:

- Webex Calling group features, including unlimited subscriptions of auto-attendants, hunt groups, and call queues
- Integrated calling from within the Webex app
- Webex app with messaging, screen sharing, and audio and video conferencing
- The option to add Webex Meetings for advanced meeting experiences including meeting room recording, meeting room locking, remote dial-in access over PSTN, and supporting up to 1000 meeting participants
- The ability to deploy all models of Cisco Multiplatform Phones (MPP)

The Cisco Webex Calling data sheet details all supported endpoints:

- Access to public switched telephone networks (PSTN)

Supported Devices

Webex Calling provides a variety of user interfaces that may be selected based on the organization’s or end users’ requirements. These include both physical phone sets from Cisco’s Multiplatform Platform Phone (MPP) line, as well as a variety of software interfaces. The administrator selects the default calling application for the organization, however individual users may be configured by the administrator to use other applications as needed. These software options include the Webex app with its integrated messaging, calling, and meeting functions; or it may be the Webex Calling application which is a dedicated telephony only application with advanced calling features. Within the Webex app, mid-call options are the most common and it supports a single line for each user. The Webex app also allows limited control of the user’s Cisco MPP phone. Cisco’s line of headsets for end users are supported both when connected to the MPP devices or to the user’s workstation or mobile phone.

In addition to these software options from Cisco, Webex Calling users may also be configured to use Webex Calling services from within Microsoft Teams. More information on this integration is available at https://help.webex.com/en-us/ngmx08cb/Cisco-Webex-Teams-Calling-for-Microsoft-Teams
Video Support

Webex Calling supports video calls between the following endpoints:

- Video capable phones (8845, 8865)
- The Webex app (both desktop and mobile) when configured with Webex Calling for the users
- The Webex Calling application (both mobile and desktop)

In addition to these point-to-point calls, users may also dial Webex Room devices that have been provisioned with PSTN numbers through the organization’s Webex Calling deployment. With a properly configured soft key on the video capable phone, users may use a speed dial to call into Webex meetings (e.g., user’s Personal Meeting Room).

When video devices are registered to the Webex Cloud as a “Workspace” and assigned a PSTN number and an extension within the organization’s Webex Calling deployment, they can dial and receive calls from other devices per the Webex Calling dial plan configured for the organization.
Architectural Overview

Cisco Webex Calling is a cloud-based enterprise calling solution hosted in Cisco Webex datacenters in multiple geographically distributed locations.

Figure 1  Globally Distributed Datacenters

Webex Calling is available globally and is delivered from redundant data centers in five regions: the US, Canada, Europe, Australia, and Japan. The datacenters are interconnected by a multi-gigabit and fully redundant backbone.

Webex Calling uses SIP for signaling and SRTP for media. Dynamic NAT can be used for IP Phone and Local Gateway IP addresses. Phones initiate a TLS connection to the Webex Cloud and are authenticated by the Webex Cloud. The Webex Cloud continues to use the same connection to send traffic back to the phone or Local Gateway, thus providing firewall traversal.
Webex Calling Datacenters
Each Webex Calling datacenter hosts call routing functions and also provides provisioning interface access to Webex Calling.

**Figure 2  Webex Calling’s Functional Elements**

The datacenters also host the access and peering Session Border Controllers (SBCs). The access SBCs terminate all customer-facing SIP connections from Local Gateways, endpoints, and soft clients and the peering SBCs terminate the SIP peering connections to SIP service providers. Load balancers and other network functions required to build a scalable, redundant datacenter architecture are also part of each Webex Calling datacenter.

**Over-the-top TLS Connections**
Webex Calling endpoints on the customer’s network use the public Internet as the access network to connect to the Webex Calling datacenters and establish over-the-top TLS connections.

**Figure 3  Over-the-top Connections between Webex Calling Endpoints and Datacenters**
PSTN Access and On-Premises Interconnect

Webex Calling can access the PSTN in three ways: Cisco Calling Plans, Cloud Connected PSTN, and Premises-based PSTN:

- **Cisco Calling Plans (Cisco PSTN)**
  
  Cisco PSTN enables partners to sell Cisco provided PSTN options to their customers, simplifying the overall purchasing experience of a complete collaboration solution. With Cisco PSTN number ordering and initiating a port ordering is available from within Control Hub.

- **Cloud Connected PSTN (CCP)**
  
  Cisco has set up shared SIP integration with a number of Cloud Connected PSTN providers. Webex Calling customers contract directly with a Cloud Connected PSTN provider of their choice and then in Webex Control Hub, select their Cloud Connected PSTN provider to route calls to the PSTN.

- **Premises-based PSTN**
  
  The Local Gateway function running on a Cisco voice gateway or Cisco Unified Border Element (CUBE) enterprise routes calls to the PSTN. The Local Gateway function is commonly deployed on the customer’s premises but can also be hosted by a partner. The Local Gateway registers with Webex Calling and routes all calls between the PSTN and Webex Calling. Premises-based PSTN requires that a trunk or a route group with multiple trunks is selected as the PSTN choice in Webex Control Hub. Each trunk represents a connection to a Local Gateway.

Figure 4  CCP and Local Gateway PSTN Access

Figure 4 shows that the selection of PSTN type (Cisco PSTN, Cloud Connected PSTN, or Premises-based PSTN) can be configured per location. While devices in location A use the selected CCP provider for PSTN access, the devices in location B use a trunk to a Local Gateway.

In addition to providing PSTN access, a Local Gateway can also connect Webex Calling with an on-premises call control. To accomplish this, the Local Gateway must be connected to the on-premises call control.
Calls between different Webex Calling customers are always routed through the PSTN via the configured PSTN choice (Cisco PSTN, Cloud Connected PSTN, or Premises-based PSTN) in order to meet legal requirements.

**Multiple PSTN Providers**

A Webex Calling customer is not limited to using only a single CCP provider or Cisco PSTN for PSTN access. Unique CCP providers can be selected for different Webex Calling locations in order to include geographical presence of the provider in case of multi-national deployments and tariff structure, for example.

![Image showing multiple PSTN providers](Figure 5 Multiple PSTN Providers)

Figure 5 shows an example where each location uses a different PSTN choice. While PSTN services for location B are provided using Cisco PSTN, two different Cloud Connected PSTN providers are used for locations A and C. The PSTN choice used for a given call depends on the source (location) of the Webex Calling call. No other attributes related to the call affect the PSTN selection, not even the called address.

**Trunks and Route Groups**

Trunks connect Webex Calling with Local Gateways. Each trunk in Control Hub represents a trunk to one Local Gateway instance configured on a CUBE (or a Cisco voice gateway). Each CUBE can be located either within the customer’s premises or in a partner datacenter. Each trunk must be assigned to a location. Multiple trunks can be grouped together in a route group for redundancy or to provide more capacity. Each trunk can belong to multiple route groups. Route groups and trunks can be used as destination for PSTN calls or premises calls.

Using route groups as a routing choice is preferred to using individual trunks even if a route group at the start only contains a single trunk. Using route groups everywhere allows to add capacity or redundancy later simply by adding additional trunks to the route group without having to update all places where that specific route is used.

The dial plan section provides more details about the Webex Calling routing choices.
Figure 6 shows an example where trunks to two Local Gateways in the same location are combined into one route group configured as premises-based PSTN choice for that location.

A priority is assigned for each trunk within a route group. When calls are sent to route groups these calls are randomly distributed among all trunks with the highest priority (1 = highest priority). If a call cannot be sent to a trunk then rerouting occurs and a different trunk is randomly selected from the group of trunks with the highest priority. If rerouting occurs for all trunks with the highest priority, then trunk selection continues with the trunks of the next lower priority level until either the call is routed successfully or all trunks within the route group have been tried without success.

Rerouting is triggered by:

- SIP responses 401, 470, 480, and 606 if there has been no prior 18x response
- All other 4xx SIP responses except for 403, 404, 410, 413, 484 and 486
- All 5xx SIP responses
- A SIP timeout (12 seconds)

A maximum of 100 trunks is allowed per location, a route group can have a maximum of 10 trunks, and a maximum of 10,000 route groups can be configured for a Webex Calling customer.
Local Gateway Registration

Local gateways use authenticated and registered SIP trunks for the connection to Webex Calling.

**Figure 7** Local Gateway Registration

The Webex Control Hub, as part of the provisioning process of a trunk, provides connection parameters and digest credentials for SIP authentication. These SIP/TLS (SIPS) connections are only initiated from the customer's network (from endpoints and Local Gateways) to Webex Calling. No inbound connections need to be configured on the enterprise firewall because SIPS connectivity between the enterprise and Webex Calling is only outbound.
Dedicated or Co-Resident Local Gateway

A Local Gateway connects to the PSTN either directly by terminating a PSTN trunk (TDM or IP) on the same box or by connecting to an existing PSTN gateway via a SIP trunk.

Figure 8  Local Gateway Deployment Options

Figure 8 shows both options. While combining PSTN access and the connection to Webex Calling requires less hardware to be installed and maintained on the customer’s network, implementing both functions on separate devices can be a preferred option in cases where an existing PSTN gateway continues to be used after migration of a site to Webex Calling.
Partner Hosted Local Gateway

Instead of deploying individual Local Gateways on each customer’s network a partner can also host a customer’s Local Gateway in their own datacenter.

Figure 9  Hosted Local Gateways

Figure 9 shows that the partner in this example does not need to deploy separate Local Gateways in the partner data center. The dial peer-based call routing configurations of each individual customer can be combined on a single CUBE. Separation of traffic between customers is achieved by proper dial-peer routing and voice class tenant configurations. The Local Gateway configuration guide available at https://help.webex.com/en-us/jr1i3r/ describes how to configure dial-peer matching. This allows you to deterministically on the Local Gateway, map calls received from Webex Calling to customer specific PSTN trunks, and vice versa. There is no need to deploy multiple virtual routing functions (VRFs): there is no need for direct IP connectivity between the partner’s data center and customers’ networks because both signaling, and media are anchored on the access SBCs of Webex Calling in the cloud. This deployment model enables the partner to more efficiently deploy, maintain, and operate Local Gateways for various customers.

No data connectivity is needed between the partner’s datacenter and the customer networks for this deployment model. Individual per-customer registrations with Webex Calling ensure that different customers’ calls can easily be identified on the combined Local Gateway to avoid calls leaking between customers.

**IP Connectivity between Local Gateway and Customer’s Network**

Voice and video media streams need IP connectivity between the Local Gateway and the on-premises call control and related endpoints.

A Local Gateway connecting Webex Calling with an existing on-premises call control (see next section) requires IP connectivity between the Local Gateway and the customer network to enable voice and video media streams between the Local Gateway and the on-premises call control and/or endpoints controlled by the on-premises call control.

When a Local Gateway is deployed in a partner’s datacenter, the customer’s network must be extended to the partner’s datacenter. If the Local Gateway functionality is implemented on a shared platform, network separation is achieved with network virtualization mechanisms, for example, VRF configuration. The additional overhead and maintenance of this complex Local Gateway configuration combined with network security reservations may negate any benefit of sharing a single Local Gateway platform between multiple Webex Calling customers. Deploying a dedicated on-premises Local Gateway may be a more efficient deployment option if connectivity to an on-premises call control is needed.
Local Gateway Call Setup

Figure 10  SIP/TLS Connection Setup Flow

Figure 10 shows the detailed flow of the SIPS connection setup. As part of the provisioning process of the Local Gateway, the Cisco Trusted Core Root Bundle is installed. The bundle contains a set of public CA trust anchors. The digest credentials obtained from Control Hub are also provisioned on the Local Gateway.

During TLS connection setup, the Local Gateway verifies the authenticity of the Webex Calling Access SBC by validating the presented certificate with the root CA bundle.

During SIP registration, the Local Gateway is authenticated and authorized based on the presented digest credentials.

The Local Gateway’s connection and secure registration is in compliance with RFC3261. Once a persistent TLS connection is established as transport layer for SIP, the Local Gateway tries to REGISTER with the Access SBC. The first REGISTER message is sent without SIP digest credentials, the access SBC then denies registration with a SIP response 401 indicating that authentication is required. On receiving the 401 response, the Local Gateway sends another REGISTER message which contains the required authentication information based on the Local Gateway’s SIP digest credentials.
Dial Plans

Dial plans add the ability to route calls to premises-based call control or between multiple premises-based call control based on matches against dial patterns within a dial plan. Each dial plan can have up to 10,000 patterns and a maximum of 10,000 dial plans can be configured for each customer. The routing choice for each dial plan can be a trunk or a route group. Whenever a destination matches a pattern in each dial plan the respective call is sent to the trunk or route group selected as routing choice on the dial plan. As mentioned earlier always using a route group as the routing choice instead of an individual trunk simplifies adding capacity or redundancy later.

Dial plans are defined globally for an enterprise and apply to all users regardless of location. The route selection defined by dial plans is the same for all users.

Patterns and pattern matching

Numeric patterns can either represent E.164 numbers or enterprise numbers. Patterns for E.164 numbers start with a leading “+” followed by a sequence of digits “1” to “9” and finally optional wildcard characters. An enterprise number pattern is represented by a sequence of digits “1” to “9” followed by optional wildcard characters. The only valid wildcard characters are “!” and “X” where “!” matches any sequence of digits and “X” matches a single digit “0” to “9”. The “!” wildcard can only occur once at the end and only in an E.164 pattern. For example, “+496100773!” matches all national numbers in Germany (country code 49) starting with “6100773” and “84969XXX” matches all dial strings starting with “84969” followed by exactly 3 arbitrary digits.

In addition to numeric patterns, a dial plan can also contain domain patterns to enable routing of alphanumeric SIP URIs. The main use case for this is to enable URI routing between premises-based call control interconnected using Webex Calling trunks. Domain patterns are used to match the host portion of SIP URIs. A domain pattern can be a fully qualified domain for an exact match or a domain with a “*.” For a domain suffix match. All domain patterns have at least one dot (”.“).

Dial plan patterns (numeric and URI) are unique within the enterprise; the same pattern cannot exist in two different dial plans. This is enforced to guarantee deterministic routing behavior.

If the host portion (right-hand side) of a URI does not refer to Webex Calling, then Webex Calling for route selection only considers the domain patterns by matching the host portion of the URI against the provisioned domain patterns. If the host portion of the URI refers to Webex Calling (any numeric call originating from a Webex Calling phone or received from a trunk falls into this category) then for URIs with a numeric user portion (left-hand side of the URI) Webex Calling will try to find a match on +E.164 patterns first and then on enterprise patterns. No dialing normalization is applied before trying to match +E.164 patterns. If no numeric match is found, then Webex Calling uses the host portion to check for a match on one of the domain dial patterns.

If multiple dial plan matches are found, then best match routing logic is applied and the most specific pattern is selected. Range patterns using the “X” wildcard are preferred over prefix patterns using “!” to determine the best match.
Interconnect with On-Premises Call Control

Local gateways provide PSTN access for Webex Calling and can also connect Webex Calling to existing on-premises call control services. This allows customers to keep existing on-premises call control while they transition to Webex Calling. If needed, the on-premises call control can remain in permanent use, co-existing with Webex Calling.

**Figure 11**  Local Gateway providing connections for both PSTN and On-premises Call Control

![Figure 11](image)

Figure 11 shows a high-level overview of the coexistence of Webex Calling with an on-premises call control. A dial plan configured in Webex Calling ensures that enterprise destinations on Unified CM when called from Webex Calling are sent to the trunk or route group terminating to the on-premises call control as enterprise calls while all other calls, calls not matching any of the patterns of the dial plan, are sent to the trunk or route group as PSTN calls. In this example, calls sent from Webex Calling first go to the on-premises call control where the enterprise dial plan is used to differentiate between on-net and off-net calls. Off-net calls are sent to the PSTN via the regular PSTN gateways of the on-premises call control and on-net calls are routed to endpoints registered to the on-premises call control or to services provided by the on-premises call control.

Combining Premises Trunk and Cloud PSTN for PSTN Access

**Figure 12**  Combining Premises Trunk and Cloud PSTN for PSTN access

![Figure 12](image)
For each Webex Calling location, a PSTN choice (Cisco Calling Plan, Cloud Connected PSTN, or Premises-based PSTN) has to be configured. Only one PSTN choice can be selected for each location. Using a Webex Calling dial plan allows to use a choice of cloud-based PSTN (Cisco Calling Plan or Cloud Connected PSTN) for a location while still connecting to an on-premises Unified CM via a trunk or route group. In this case, all destinations matching patterns in the dial plan configured for this location are sent to the on-premises Unified CM via the trunk or route group as an enterprise call while the configured PSTN choice is used for PSTN calls.

Multiple On-Premises Call Control

Dial plans combined with trunks or route groups can also be used to establish interworking with multiple on-premises call control.

Figure 13  Interconnecting multiple on-premises call control

Figure 13 shows an example where two on-premises call control are connected to Webex Calling at the same time two sets of Local Gateways establish the connection to Webex Calling. Each set of Local Gateways is represented by a route group in Webex Calling where each route group contains the trunks connecting to the individual Local Gateways. This is shown in the following illustration

Figure 14  Dial Plan Setup for two On-Premises Call Control

For calls originating from a Webex Calling user, the dialed destination is matched against all patterns and if a match is found, the call is routed to the route group configured as the routing choice on the dial plan which contains the pattern. No dialing normalization is applied prior to executing the match. Using the example above both, “81212345” and “+12125552300”, are routed to the NYC on-premises location but “912125552300” isn’t.
The numeric routing schema established by Webex Calling dial plans cannot only be used to steer calls originating from Webex Calling users to a specific call control, but it also applies to calls originating from on-premises users and which are sent to Webex Calling by the on-premises call control via one of the trunks. If the called address of a call received by Webex Calling on a trunk does not match any Webex Calling address (user or any service) then similar to calls originating from Webex Calling users, the dial plan patterns are matched to determine which trunk or route group to send the call to. Webex Calling in this case acts as a tandem between all on-premises call control.

**Unknown Number Handling**

The routing behavior for unknown numbers is controlled by two settings. The enterprise wide “Unknown Number Handling” setting and the “Calls to On-Premises Extension” setting at the location level. The enterprise level “Unknown Number Handling” setting can be set to “Standard behavior” or “Legacy”. For new deployments “Standard behavior” should be selected and call routing to on-premises should be established by configuring Webex Calling dial plans. The other option exists mainly to provide backward compatibility for deployments that existed prior to the introduction of Webex Calling dial plans.

For calls originating from a Webex Calling user, the dialed number is first checked against emergency numbers, Webex Calling numbers defined for that customer, virtual on-net extensions, dial plan patterns, and finally national numbering plan patterns. If no match is found, and the dial string has between two and six digits, and “Calls to On-Premises Extensions” are enabled for the location the call is originating from, then the call is routed as an “unknown extension” call to the trunk or route group configured for calls to on-premises extensions for that location. If the PSTN choice of the location is set to anything other than premises-based PSTN, then the call to the unknown destination is rejected. Only if the PSTN choice of the location is premises-based PSTN, then the last step of unknown number handling is to check the enterprise level “Unknown Number Handling” setting. If this is set to “Legacy”, then the call is sent to the trunk or route group configured as the location’s PSTN choice. Else the call is blocked. Sending all unknown numbers to the premises-based PSTN is backward compatible with the routing behavior of Webex Calling prior to the introduction of Webex Calling dial plans.

Table 2 summarizes the routing behavior for an unknown number.
Table 2  Routing Logic for Unknown Numbers

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>“Calls to On-Premises Extensions”</th>
<th>Global “Unknown Number Handling”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webex Calling</td>
<td>Unknown extension (e.g., 4099)</td>
<td>Enabled</td>
<td>Route to premises PSTN choice configured on location level “Calls to On-Premises Extensions” option</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled</td>
<td>Route to PSTN (if premises-based PSTN is selected)</td>
</tr>
<tr>
<td></td>
<td>Other unknown number</td>
<td>any</td>
<td>Route to PSTN (if premises-based PSTN is selected)</td>
</tr>
<tr>
<td>Premises</td>
<td>Unknown extension (e.g., 4099)</td>
<td>Enabled</td>
<td>Route to premises PSTN choice configured on location level “Calls to On-Premises Extensions” option</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled</td>
<td>rejected</td>
</tr>
<tr>
<td></td>
<td>Other unknown number</td>
<td>any</td>
<td>rejected</td>
</tr>
<tr>
<td>External</td>
<td>Any unknown number</td>
<td>any</td>
<td>rejected</td>
</tr>
</tbody>
</table>

Trunk calls to Webex Calling

Inbound to Webex Calling, the originating trunk is identified by the otg tag inserted into the “From” header by the Local Gateway. Then the unscreened caller identity of the call is used to determine the type of the call.

When the inbound call from local gateway requests privacy, the asserted identity carried in the P-Asserted-Identity header is selected as the unscreened calling line identity if the header is present. If no privacy is requested, or privacy is requested but no P-Asserted-Identity header is present, the presentation identity carried in the “From” header is selected as the unscreened calling line identity.

For an inbound call, the unscreened caller ID is matched against dial plan patterns configured for the customer. The user portion is used for matches against numeric dial plan patterns and the host portion is used for domain pattern matches. If a match is found, then the call is classified as premises call.

If no dial plan match is found and the global “Unknown Number Handling” setting is set to “Standard”, then the “Calls to On-Premises Extension” setting of the inbound trunks is checked. If “Calls to On-Premises Extension” is enabled and the numeric caller id length is between two and six digits, then the call is considered to originate from an enterprise extension and classified as premises call.

Finally, if the global “Unknown Number Handling” setting is set to “Legacy” then the call is also classified as premises call.

If none of these checks succeed, the call is classified as a network (PSTN) call.

Table 3 summarizes this behavior.
### Table 3  Call classification for inbound calls on trunks.

<table>
<thead>
<tr>
<th></th>
<th>Global “Unknown Number Handling”</th>
<th>“Calls to On-Premises Extensions”</th>
<th>“Legacy”</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming caller id (number)</strong></td>
<td><strong>Enabled</strong></td>
<td><strong>Disabled</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Dial plan match</strong></td>
<td>Premises</td>
<td>Premises</td>
<td></td>
</tr>
<tr>
<td><strong>Unknown extension (e.g., 4200)</strong></td>
<td>Premises</td>
<td>External</td>
<td>Premises</td>
</tr>
<tr>
<td><strong>Other unknown number</strong></td>
<td>External</td>
<td>Premises</td>
<td></td>
</tr>
</tbody>
</table>

The call classification impacts how services work which takes into account whether a call is originating from an on-net source or from the PSTN. Additionally, the call classification determines which destinations can be reached (see next section for details).

#### Allowed transit calls and caller ID selection

Webex Calling dial plans enable deterministic routing between on-premises call control and from Webex Calling users to on-premises call control. Webex Calling dial plans do not aim at providing cloud PSTN for on-premises users. Transit calls from on-premises call control to Cloud Connected PSTN or Cisco PSTN are not allowed. Table 4 summarizes which transit calls are allowed and what is sent as caller ID.

<table>
<thead>
<tr>
<th></th>
<th>To Webex Calling User</th>
<th>To Trunk (DP match)</th>
<th>To Cloud Connected PSTN or Cisco PSTN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From</strong></td>
<td>Webex Calling User</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allowed,</td>
<td>See next section,</td>
<td>Allowed, external caller identity of</td>
</tr>
<tr>
<td></td>
<td>internal caller identity of the user</td>
<td>Table 5</td>
<td>the user</td>
</tr>
<tr>
<td>Trunk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allowed, incoming “From”</td>
<td>Allowed,</td>
<td>rejected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>incoming “From”</td>
<td></td>
</tr>
<tr>
<td>Cloud Connected PSTN or Cisco PSTN</td>
<td>Allowed, incoming “From”</td>
<td>rejected</td>
<td>rejected</td>
</tr>
</tbody>
</table>

*Trunk to trunk calls are only allowed if the incoming call is classified as a premises call.

#### Outbound caller ID on trunks for calls from Webex Calling users

When premises-based PSTN is used as the PSTN choice for a location, then for PSTN calls sent to a trunk the presentation identity is always determined by the user’s caller ID configuration.

For calls from Webex Calling users to premises destinations, Webex Calling checks the “Caller ID Format for Calls from and to On-premises” parameter to determine the presentation identity to send to the premises-based local gateway.

When “Caller ID Format for Calls from and to On-premises” is set to “ESN (Location routing prefix + user extension)”, then the desired presentation identity format can only be satisfied if the calling user has an extension and the caller’s location has a site prefix configured. If either the user has no extension or the site prefix is missing on the calling user’s location, then instead the presentation identity value is determined according to the user’s caller ID configuration (direct line, location number, or assigned number from user’s location) and the presentation identity is sent as +E.164.
When “Caller ID Format for Calls from and to On-premises” is set to “+E.164 phone number”, then Webex Calling ignores the user’s caller ID configuration and tries to use the user’s direct line as presentation identity. If the user doesn’t have a phone number, then the presentation identity value is determined according to the user’s caller ID configuration.

Webex Calling supports separate presentation and asserted identities. On the outgoing side, the presentation identity is included in the “From” header, and the asserted identity is included in the P-Asserted-Identity header. The asserted identity for users with a direct line is always the direct line and only for users without a direct line the location’s main number is used.

The following table summarizes what is sent as presentation identity in the “From” header and as asserted identity in the PAI header assuming that the location prefix is set.

<table>
<thead>
<tr>
<th>Does the user have phone number and/or extension configured?</th>
<th>“Caller ID Format for Calls from and to On-premises” setting</th>
<th>“+E.164 phone number”</th>
<th>“ESN (Location routing prefix + user extension)”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Number</td>
<td>Extension</td>
<td>PAI</td>
<td>From</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Phone number, +E.164</td>
<td>DN, +E.164</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Phone number, +E.164</td>
<td>DN, +E.164</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Location main number, +E.164</td>
<td>According to user’s caller ID configuration, +E.164</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td></td>
<td>No calls allowed without either DN or extension configured</td>
</tr>
</tbody>
</table>

Note: For certain regions (for example Japan) and environments delivery of separate presentation and asserted identities is disabled. In this case, the P-Asserted-Identity header contains the same value as the “From” header.

For the cases marked in red, no correct presentation ID can be sent, and thus, a callback from the called user on the terminating side, for example, on-premises Unified CM, is not possible. Assuming that all Webex Calling users at least have an extension provisioned using ESN presentation ID ensures that a callback is possible. The same can only be achieved with +E.164 presentation ID if all Webex Calling users have a phone number, which is less likely.

If ESN presentation ID is configured, then when a call from Webex Calling to an on-premises user is forwarded to the PSTN, no valid caller ID is available for the PSTN call leg (ESN is not a valid PSTN caller ID). In that case, the caller ID has to be masked to some fixed value (main number). Mapping the caller ID from ESN to +E.164 can be achieved if the next-hop call control has all ESN to +E.164 mappings of all Webex Calling locations but there is a risk that the originating user doesn’t have a phone number and that the naïve ESN to +E.164 mapping results in a number which does not belong to this customer.

Service interactions

Many Webex Calling services use routing lookups involving dial plan matching. For example, for call forward always and auto-attendant (transfer call to operator) services, Webex Calling performs a dial plan lookup to route the call to on-premises PBX in the same way as a regular user origination. The administrator can provision an ESN number as the forward-to/transfer-to numbers in the same way as a user extension.
However, other services, like Office Anywhere, do not invoke dial plan lookups when forking calls to their network locations. In these cases, this feature does not apply.

The screening services use a set of selective criteria to perform differently depending on the result of the screening. The screening service requires the calling number to be in E.164 format. The screening services should not specify premises ESN/unknown number as a calling party criterion.

**Media Flows**

Media flows are always anchored on the Webex Calling Access SBCs.

**Media Flows for Co-located and PSTN Calls**

Figure 16 shows two media flow examples. The example on the left shows a call between two co-located Webex Calling endpoints. The media flow is anchored on the Webex Calling Access SBC causing media to flow from the originating phone via the customer’s Internet edge to the Webex Calling Access SBC and then back to the destination phone. Media in the opposite direction follows the same path.

The example on the right shows that media for a PSTN call is sent from the originating phone via the customer’s Internet edge to the access SBC and from there back again via the customer’s Internet edge to the local gateway.

Anchoring media flows on the Webex Calling Access SBC occurs for all calls between any two Webex Calling phones and also for a Webex Calling phone and a local gateway.
In both cases, two full-duplex audio and/or video streams traverse through the customer’s Internet edge. When deploying Webex Calling, the Internet access for each location needs to be sized accordingly to be able to handle these two full-duplex audio and/or video streams for each intra-location, inter-location, and PSTN call in the busy hour.

**Media Flows for Calls between Different Webex Calling Customers**

Calls between two Webex Calling customers must be routed through the PSTN to meet legal requirements, for example lawful intercept.

![Webex Calling Media Flows between Two Webex Calling Customers](image)

*Figure 17* Webex Calling Media Flows between Two Webex Calling Customers

Figure 17 shows that the media flow is anchored twice in the Webex Calling access layer and also traverses through the local gateways of both the Webex Calling customers.
Webex Calling Regions
Cisco Webex Calling operates five regional platforms: US (Los Angeles, Dallas, Chicago, New York), Canada (Vancouver, Toronto), EMEAR (London, Amsterdam), APJC (Japan: Tokyo, Osaka) and APJC (Australia: Melbourne, Sydney). Each Webex Calling instance provides redundant datacenters within that region.

Each Webex Calling customer is provisioned on one of the five Webex Calling instances. All provisioning information of that customer is stored in that Webex Calling instance and the SIP signaling of all endpoints and Local Gateways provisioned for that customer is tied to the Webex Calling instance the customer is provisioned on. Because the initial Webex Calling region selection cannot be changed later it is important to consider all relevant factors as part of the decision process leading to the Webex Calling region selection. To avoid excessive signaling round-trip delay it is important to decide early in the transition process which Webex Calling instance should be used. Cisco recommends selecting the Webex Calling instance which provides the lowest signaling round-trip times for the largest number of users within the deployment.

Another factor to consider in the Webex Calling region selection is the country availability of PSTN services provided by Cloud Connected PSTN (CCP) providers available within that region. While during the transition period PSTN access for Webex Calling devices must be facilitated via a Local Gateway to enable interworking with Unified CM registered devices, after successful completion of the transition, PSTN access for Webex Calling may be switched to CCP. At that point, the country availability of the CCP providers available within the Webex Calling region becomes an important factor.

The region selection for a Webex Calling customer determines the location of the authoritative call control entity for all calls of that customer. To avoid excessive media RTT for calls that are anchored on the Webex Calling access layer, all Webex Calling call control entities can use access resources in each region.

Figure 19 shows the call flow between two phones in Australia. For simplicity, the figure shows only the US and Australia regions, but this concept applies to all regions. Even though the customer is assigned to the US region, the media path is kept on the access SBCs in the Australia region controlled by the US Webex Calling instance. The SIP signaling for this call goes back to the Webex Calling call control entity hosted in the US region because this is the Webex Calling instance on which the customer is provisioned.
Figure 20 shows how the Access SBCs in both regions anchor the media for inter-region calls. The traffic between the Access SBCs traverses the global Cisco Webex backbone and only part of the media flow between the endpoints and the Access SBCs traverses the Internet as the access network.

Media flows involving Local Gateways follow the same schema as described above: media flows involving Local Gateways are also always anchored on the access SBCs of the region in which the Local Gateway is deployed.
Deployment Aspects

This section includes details on various aspects of a Webex Calling deployment including the concept of a Location, Local Gateways, and Directory integration.

Location Definitions

For Webex Calling deployments, the division of the organization into “Locations” will require consideration of many factors. In addition to the PSTN configurations and dial plan considerations, factors like how emergency services are notified and internal telephony services for Hunt Groups, Call Queues, and the like are distributed are significant.

Each location must have a PSTN connection defined and may share that connection with other locations. The details of PSTN connectivity will be addressed later in the document, however, there is a default scale limit of 250 concurrent calls that does impact the definition of locations using a Local Gateway. Cloud Connected PSTN is not impacted by this limit. The use of site dialing prefixes also needs to be considered as will be discussed later.

When adding a location in Control Hub, a physical address and contact name and information are required. For Webex Calling VAR, these are not utilized in emergency contact functionality either to the PSAP or within the organization and are defined separately.

Emergency Calling

One aspect of location definition relates to emergency calling. United States government regulations require notification when any user within an organization calls 911. This notification, sent as an email, can either be organization-wide or selected by location. Depending upon how your organization needs to respond to emergency responders provides some indication of how granular your definition of a location may need to be.

Webex Calling VAR requires the PSTN provider to provide the mapping of numbers to phones to physical addresses to allow for the correct connection to the appropriate Public Safety Answering Point (PSAP) and present the correct ELIN (Emergency Location Identification Number).

Telephony services

Auto Attendants, Call Park Groups, Call Pickup Groups, Call Queues, Hunt Groups, and Paging groups only include users within the same location. Any groups of users that would share these calling features must be located within the same defined location.

PSTN DID numbers are also added by Location, and there is no validation of numbers (For example, is the 302-area code available in San Jose, California?). This will allow the organization to have locations that may cross geographic boundaries but make logical use of user allocation (with the correct number allocation for emergency calling).

Network Connectivity

Consider existing provider data connections (MPLS, SD-WAN, and so on) and generally plan for direct Internet access at each location within the customer deployment. Because cloud-based services will be consumed, reliable Internet connectivity with sufficient bandwidth is a base requirement.

Provided reliable network connectivity is available, Webex Calling offers global reach from all the customer locations thus, eliminating the need for endpoint survivability.
Local Gateway Deployment Options

Each trunk in Control Hub represents a connection to a single Local Gateway instance. Multiple trunks can be grouped together in a route group to provide more capacity or redundancy. All calls originating from a location that are destined for premises-based PSTN are sent to the trunk or a route group containing this trunk based on call routing configuration. A Webex Calling customer can utilize the same Local Gateway instance for multiple locations.

Currently, Webex Calling allows no more than 250 concurrent sessions from a single Local Gateway instance, which by default becomes the session count limit for Local Gateway based calls, that is, premises-based PSTN or Inter-site calls between Unified CM and Webex Calling endpoints. Multiple Local Gateways can be combined using the trunk and route groups for increased capacity. However, if a single Local Gateway deployment requires more than 250 concurrent calls, please contact your Cisco account team to explore other deployment options.

Poor network conditions between the Local Gateway and Webex Calling access SBC can limit the performance of the signaling connection leading to an even lower concurrent calls limit. One-way latency between the Local Gateway and the Webex Calling data center should not exceed 100 ms, jitter should be less than 10 ms, and packet loss should be no more than 0.5%.

Any calls exceeding this capacity limit are rejected with a “403 Forbidden”. The “show call active voice” command can be run on the Local Gateway at any instance to determine the total number of active calls.

```
LocalGateway# show call active total-calls
Total Number of Active Calls : 153
```

If the output of the above command on the Local Gateway shows more than 250 calls (153 in the above example), and troubleshooting reveals some calls getting rejected by the Webex Calling Access SBC with a “403 Forbidden” SIP response code, Cisco Technical Assistance Center (TAC) may be contacted for further assistance.

CUBE High Availability as Local Gateway

For all IP-based environments, customers have the option to deploy CUBE high availability (HA) as Local Gateway (LGW) for call preservation. CUBE high availability Layer 2 box-to-box redundancy uses the Redundancy Group (RG) Infrastructure protocol to form an active/standby pair of routers. The active/standby pair share the same virtual IP address (VIP) across the respective interfaces and continually exchange status messages. CUBE session information is checkpointed across the active/standby pair of routers enabling the standby router to immediately take over all CUBE call processing responsibilities if the active router should go out of service, resulting in stateful preservation of signaling and media.

**Note:** Checkpointing is limited to connected calls with media packets. Calls in transit are not checkpointed, for example, Trying or Ringing state.

Refer to Figure 21 below which depicts a typical CUBE high availability as Local Gateway setup.
The following requirements exist for using CUBE High Availability as Local Gateway for stateful failover of calls:

- CUBE HA as LGW deployment option is available on supported ISR 4000 and CSR1000 series platforms
- CUBE HA cannot have TDM or analog interfaces co-located
- Gig1 and Gig2 are referred to as traffic (SIP/RTP) interfaces and Gig3 is Redundancy Group (RG) Control/data interface
- No more than 2 CUBE HA pairs can be placed in the same layer 2 domain, one with group id 1 and the other with group id 2. If configuring 2 HA pairs with the same group id, RG Control/Data interfaces needs to belong to different layer 2 domains (VLAN, separate switch)
- Port channel is supported for both RG Control/data and traffic interfaces
- All signaling/media is sourced from/to the Virtual IP Address
- Anytime a platform is reloaded in a CUBE-HA relationship, it always boots up as Standby
- Lower address for all the interfaces (Gig1, Gig2, Gig3) should be on the same platform
- Redundancy Interface Identifier (RII) should be unique to a pair/interface combination on the same Layer 2
- Configuration on both the CUBEs must be identical including physical configuration and must be running on the same type of platform and IOS-XE version
- Loopback interfaces cannot be used as bind as they are always up
- Multiple traffic (SIP/RTP) interfaces (Gig1, Gig2) require interface tracking to be configured
- CUBE-HA is not supported over a crossover cable connection for the RG-control/data link (Gig3)
- Both platforms must be identical and be connected via a physical Switch across all likewise interfaces for CUBE HA to work, i.e., GE0/0/0 of CUBE-1 and CUBE-2 must terminate on the same switch and so on.
- Cannot have WAN terminated on CUBEs directly or Data HA on either side
- Both Active/Standby must be in the same Data Center
- It is mandatory to use separate L3 interface for redundancy (RG Control/data, Gig3). i.e. interface used for traffic cannot be used for HA keepalives and checkpointing
- **Upon failover, the previously ACTIVE CUBE goes through a reload by design, preserving signaling/media**

Deployment Aspects

Firewall Requirements
From an enterprise firewall’s perspective, both provisioning and registration are set up using an outbound TLS connection, so that return traffic doesn’t require opening inbound ports on the firewall.

Figure 22  Firewall Traversal Mechanism for TCP Connections

Figure 22 shows this process for an IP phone establishing a TCP/TLS connection for SIP. The firewall translates the private IP address of the phone into a public IP address and changes the source port as shown in step 1 and step 2. The Webex Cloud re-uses this same connection and sends the traffic back to the firewall. The firewall allows the return traffic, translates the public IP address into the private IP address of the phone, and the destination port (source port from the phone’s perspective) back to the original private IP Address (step 3 and step 4).

Once the TLS connection is established, the phone can send and receive SIP signaling messages to and from the Webex Calling cloud. SIP signaling from the Webex Calling cloud to the phone reuses the same SIP/TLS connection created by the phone registration. Local Gateways use registering SIP trunks to the Webex Calling cloud so that the same mechanism of creating the SIP/TLS transport connection from the inside of the corporate firewall also applies to Local Gateways. The SIP/TLS connections require outbound (egress) TCP port 8934 to be open on the corporate firewalls.
In environments where NAT is applied the transport addresses advertised by Local Gateways and IP phones within the SIP signaling messages are always internal (private) IP addresses. Those private addresses are not reachable by an external entity such as the Webex Calling access SBC. However, the SBC is able to detect NAT by checking the layer 3 transport addresses of received SIP signaling messages against the addresses contained within the SIP messages. Differing addresses point to the presence of NAT between the Webex Calling access SBC and the endpoint or Local Gateway. When NAT is detected, the SBC always reuses the existing TCP connection and does not send replies to the IP addresses contained in the Via header, or new SIP requests using the addresses contained in the Contact Header.

IP addresses to be used to send and receive media are advertised by endpoints and Local Gateways as part of the SDP based media negotiation within the SIP signaling messages. However, in most of cases those are private addresses, and the Webex Calling access SBC cannot use those addresses to stream media to. Because media runs on top of UDP, they will be translated by NAT differently from the signaling, which conversely runs on top of TCP. The Webex Calling access SBC does not know in advance how the firewall will translate the media packets until the first media packet is received on the negotiated UDP port by the Webex Calling access SBC. As soon as the first packet arrives, the SBC learns the public IP and ports corresponding to the stream that is associated with the UDP port on which the packet was received on. The access SBC then uses the public IP address and port extracted from the first received media packet (and not the address and port information from SDP) for its return media packets which will be allowed back through the corporate firewall as return traffic of an existing connection.

Using the same logic, the Webex Calling access SBC is also able to detect if a NAT change has happened on a Local Gateway or IP phone, for example following a resume after a call hold, and accordingly update IP address and port information for the return traffic.

The mechanism to extrapolate return media address and port from received media packets instead of relying on SDP is called “Media Latching”. Media Latching requires that the endpoints (Local Gateway and IP phones) inside the corporate firewall always send media packets to the Webex Calling access SBC before any media packets can be returned in the opposite direction. The media packets sent from within the corporate network create a NAT binding in and open a connection through the firewall. As a consequence, the firewall allows UDP packets inbound as return traffic of the same connection as long as source and destination IP address and port and protocol (5-tuple) match. As the Webex Calling access SBC for the return traffic uses IP address and port extracted from the received packets these return packets fulfil that condition and are recognized as return traffic by the firewall.

By always reusing the same UDP flow and TCP connection both, signaling and media from the Webex Calling access SBC to the IP phone or Local Gateway are able to traverse the firewall.

Based on Media Latching, firewall traversal for RTP media on top of UDP doesn’t differ from what is shown in Figure 22 about SIP signaling using TCP connections as transport.

This is explained in Figure 23.
Figure 23  Firewall Traversal Mechanism for Webex Calling

This picture shows an example of the firewall traversal for Webex Calling signaling and media.

1. The endpoint or Local Gateway use private IP 10.10.10.7 and port 51000 to initiate a TLS connection. The destination address is the Webex Calling SBC’s IP and port, that is 203.0.113.144 and 8934.

2. SIP uses this TLS connection as transport. The endpoint or Local Gateway sends out an INVITE to the SBC, containing the media IP and ports (i.e., 10.10.10.7 and 17482 for audio) it will use to send and receive media.

3. The SBC replies with 200 OK on the same TLS connection. SDP information in that 200 OK message contains the SBC media IP address and port (i.e., 203.0.113.144 and 19920 for audio).

4. The endpoint or Local Gateway starts sending the media to the IP address and port obtained from the SDP received with the 200 OK. The source port of these media packets is the UDP port advertised in the SDP sent with the initial INVITE, in this case, UDP port 17482. The Webex Calling access SBC for now cannot send return packets because IP address and port obtained from the SDP in the initial INVITE by the access will both be translated to still unknown values by the firewall. Once the first media packet hits the access SBC on the port advertised for this call by the access SBC, the SBC learns the firewall’s public IP address from the source IP address of the received media packet and also the source port of the media packet is the port translated by the
firewall; 23001 in above example. The access SBC now updates its connection state accordingly and starts streaming the return media to this public IP address and the translated UDP port.

In some scenarios with Local Gateways, there can be situations where both call legs are inbound from a firewall’s perspective, such as in the case where an IP phone connected to Webex Calling calls a PSTN number through the Local Gateway, and the called PSTN device transfers the call to another IP Phone belonging to the same network. These two call legs are inbound from the firewall’s perspective, and the firewall will block them because no RTP media packets are sent from the inside which would otherwise open a connection on the firewall. To solve this deadlock STUN needs to be configured on the Local Gateway. With STUN configured the Local Gateway will send STUN packets to the media IP address and port negotiated via SDP. Although no actual media packets are sent the UDP STUN packets from the firewall perspective still constitute outbound UDP packets so that the firewall creates a connection and allows inbound media to flow on the same connection. Failure to configure STUN can prevent bidirectional media in some scenarios.

As a summary, Webex Calling architecture does not require to open inbound ports on the firewall. Only outbound UDP and TCP traffic to specific IP addresses and ports have to be allowed. The required destinations, including a full list of ports, IP addresses, and DNS domains are included in the Port Reference for Cisco Webex Calling document available at https://help.webex.com/en-us/b2exve/Port-Reference-for-Cisco-Webex-Calling-Value-Added-Resellers#id_112963.

Intrusion Protection System Requirements

Because both signaling and media are encrypted, Cisco recommends that both SIP signaling, and media are allowed to flow transparently and uninspected to Local Gateways and IP phones.

IPS inspection can be performed after the traffic reaches the Local Gateway and before it is sent without any manipulation to the Unified CM or endpoint. IPS should be positioned between the Local Gateway and the UCM. For inspection to work, it is required that traffic between Local Gateway and Cisco Unified CM or endpoint is sent in the clear. In this case, the Local Gateway will decrypt the traffic from Webex Calling before sending SIP signaling to Unified CM and RTP media to the destination endpoint or gateway.

If the IPS performs actions that prevent normal operation of the whole system, for example, it identifies legitimate traffic as malicious, the IPS inspection for traffic between the Local Gateway and Unified CM or endpoints should be disabled.

Codec Selection

Webex Calling optimizes audio call quality using the Opus codec, which is supported by most clients on the platform. Opus is supported by the Webex app as well as the MPP phones. It is also supported by the Local Gateway as an end-to-end codec without the ability to do audio codec transcoding, that is, Opus to other codecs such as G.711 is not possible. However, it is currently not supported by analog telephone adapters (ATAs) and DECT phones. It is also not supported by most PSTN providers, and hence, G711 is the recommended option for PSTN and UCM interconnect calls.

To ensure a consistent call quality experience and codec negotiation, it is recommended to configure only G.711 codec on the Local Gateway to ensure all UCM and PSTN interconnect calls with Webex Calling select G.711 as the codec. If the IP PSTN provider only supports G.729 and Local Gateway is being used to provide PSTN interconnect for a Webex Calling deployment, then it is recommended to add G.729 as well along with G.711 in the Local Gateway’s voice class codec configuration.
For all other call flows, the Opus codec is supported as shown below:

- Webex app (desktop) ↔ Webex app (desktop)
- Multiplatform Phone ↔ Multiplatform Phone
- Multiplatform Phone ↔ Webex app (desktop)
- Multiplatform Phone ↔ Auto Attendant
- Multiplatform Phone ↔ Voicemail
- Webex app (desktop) ↔ Auto Attendant
- Webex app (desktop) ↔ Voicemail

### Bandwidth Considerations

To determine the bandwidth required on the internet access for Webex Calling, the number of concurrent call legs and the codec used for each call leg needs to be considered.

Table 6 shows the call types available with a Webex Calling deployment along with the codec and maximum bandwidth required for each call type. The required audio call bandwidth for each call type can be calculated using the following general formula:

\[
\text{Number of expected concurrent calls} \times \text{Bandwidth per call based on codec} = \text{Total bandwidth.}
\]

<table>
<thead>
<tr>
<th>Call Types</th>
<th>Codec - Bandwidth</th>
<th>Total bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webex app / MPP Phone → Webex app</td>
<td>OPUS - 70 kbps</td>
<td>Number of concurrent calls * 70 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → MPP Phone</td>
<td>OPUS – 70 kbps</td>
<td>Number of concurrent calls * 70 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → PSTN via LGW</td>
<td>G.711 – 80 kbps</td>
<td>Number of concurrent calls * 80 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → PSTN via CCP</td>
<td>G.711 – 80 kbps</td>
<td>Number of concurrent calls * 80 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → Enterprise via LGW</td>
<td>G.722 – 80 kbps</td>
<td>Number of concurrent calls * 80 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → Webex Calling Voicemail</td>
<td>OPUS – 70 kbps</td>
<td>Number of concurrent calls * 70 kbps</td>
</tr>
</tbody>
</table>

By summing the concurrent required network throughput per call type, the total potential bandwidth requirement for a specific site can be determined.

All call legs are always anchored on the Webex Calling access SBCs. To determine the required internet bandwidth for any given Webex Calling location not only the inter-location calls need to be considered, but also intra-location calls and calls to and from a Local Gateway at that location. For example, an intra-site call between two MPPs would need 2 x 70 kbps full duplex on the location’s internet access.
By summing the concurrent required network throughput per call type, the total potential bandwidth requirement for a specific site can be determined.

Table 7 shows an example of a complete bandwidth calculation exercise assuming that all devices are located in the same location.

<table>
<thead>
<tr>
<th>Call Types</th>
<th>Number of Concurrent Calls</th>
<th>Total Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webex app / MPP Phone → Webex app</td>
<td>15</td>
<td>2 * 15 * 70 kbps = 2,100 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → MPP Phone</td>
<td>15</td>
<td>2 * 15 * 70 kbps = 2,100 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → PSTN via Local Gateway</td>
<td>50</td>
<td>2 * 50 * 80 kbps = 8,000 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → PSTN via Cloud Connected PSTN</td>
<td>0</td>
<td>0 * 80 Kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → Enterprise via Local Gateway</td>
<td>15</td>
<td>2 * 15 * 80 kbps = 2,400 kbps</td>
</tr>
<tr>
<td>Webex app / MPP Phone → Webex Calling Voicemail</td>
<td>5</td>
<td>5 * 70 kbps = 350 kbps</td>
</tr>
<tr>
<td>TOTAL CALLS / BANDWIDTH</td>
<td>100 calls</td>
<td>14,950 kbps / 14.95 Mbps</td>
</tr>
</tbody>
</table>

**Note:** The bandwidth calculations above are based on net codec bitrate. When sizing the internet access signaling and L3 overhead need to be considered.

**Note:** The bandwidth in Table 6 and Table 7 is for audio calls. For video call bandwidth, the Webex app and the MPP 8845/65 phones support H.264 video with maximum resolution of 720p at a maximum bandwidth of 1,500 kbps per call. However, the amount of bandwidth consumed at any point during the call will fluctuate based on variable bit rate inherent in video communications.
Directory Integration

The Cisco Directory Connector synchronizes directories with the Webex cloud. This allows administrators to maintain user accounts and data in the Active Directory and on-premises changes are automatically replicated to the cloud.

Users can also be manually provisioned by importing a CSV file via the Control Hub interface.


Directory Connector Architecture

The Cisco Directory Connectors are deployed on two Microsoft Windows Servers for redundancy and high availability. They are co-located in the central site with Microsoft’s Active Directory.

Figure 24 Directory Integration

Figure 24 shows the Cisco Directory Service integration with an enterprise directory.

Cisco Directory Connector relies on Microsoft Active Directory application programming interfaces (APIs) to extract user information from the Microsoft Active Directory. The APIs are based on the Microsoft NET framework. Directory Connector uses HTTPS to push user information to the organization's Cisco Webex Common Identity Store.

Users can add contacts and search the user directory from the end-user portal at the https://settings.webex.com page.
**Dial Plan**

When a user is enabled for Webex Calling, they are assigned to a location and receive an extension within the location. The user can optionally also be assigned a phone number (DID) from a previously defined pool of available phone numbers. The phone number pool is defined in Webex Control Hub. All phone numbers must be allocated via the PSTN provider and routed to the correct customer PSTN trunk or allocated via cloud PSTN provider (Cisco or Cloud Connected PSTN provider) to establish reachability for these phone numbers.

**PSTN Destinations**

To dial PSTN destinations, a Webex Calling user can use the common PSTN dialing practice of the country the location is assigned to. For example, from a US location, national PSTN destinations can be dialed as 10 digits, “1” followed by 10 digits, or by dialing 7 digits. When dialing 7 digits Webex Calling automatically prepends the dialed digits with the NPA of the location’s main number. Similarly, international destinations can be dialed as “011” followed by the full E.164 number. Additionally, +E.164 dialing (“+” followed by an E.164 number) can be used by Webex Calling users.

Note: Because 7-digit dialing from US locations is always normalized to +E.164 based on the location’s main number, no 7-digit abbreviated on-net dialing can be used with US locations. Dialing a 7-digit abbreviated on-net dialing string would be normalized to +E.164 and not matched against any configured location prefix.

**PSTN Access Code**

An optional PSTN outbound dial digit can be defined for each location. This is called a “PSTN access code”. A PSTN access code is typically used in enterprise environments to avoid overlaps with other on-net dialing habits. In the US, “9” is commonly used as the PSTN access code.

For example, if “9” is defined as a PSTN access code for a US location, then to dial a national US destination, the user dials “9” followed by 10 digits, “91” followed by 10 digits, or 7 digits (for numbers within the same NPA). An international destination is dialed with “9011” followed by a full E.164 number.

**Abbreviated On-net Dialing**

For abbreviated on-net dialing, a routing prefix length, an internal routing prefix, and the internal extension length must be configured for each Webex Calling customer.

- Routing prefix length — defines the length for all routing prefixes to be configured for each location
- Internal routing prefix — is the common first digit for all location routing prefixes
- Internal extension length — defines the extension length to be used in each location

With these three settings, a universal abbreviated inter-site on-net dialing habit is defined in the form: `<internal routing prefix>-<site code>-extension`.

If for example, an internal routing prefix of “8”, a routing prefix length of four and an extension length of four are configured then all on-net destinations can be dialed in the form “8-XXX-XXXX”. Here the leading “8” followed by three digits is the location’s prefix and the last four digits are the extension defined within the location.

Note that the configured internal routing prefix length includes the leading routing prefix. To use three-digit site codes, the routing prefix length must be set to four.

If the routing prefix is set to “8” and the routing prefix length is set to four, always include the leading “8” in the routing prefix when defining location routing prefixes.

When configuring the location routing prefix, a warning, “Enter and save a routing prefix that aligns with global Call Settings steering digit 8 to reduce delays in dialing,” displays to remind the administrator of this requirement.
### Table 8  Abbreviated on-net, inter-site dialing with a steering digit of 8 and routing prefix length and extension length both set to four

<table>
<thead>
<tr>
<th>Site</th>
<th>Site Code</th>
<th>Location Prefix</th>
<th>Extension Range</th>
<th>Abbreviated On-Net Dialing</th>
</tr>
</thead>
<tbody>
<tr>
<td>SJC</td>
<td>140</td>
<td>8140</td>
<td>4000-4999</td>
<td>81404XXX</td>
</tr>
<tr>
<td>NYC</td>
<td>121</td>
<td>8121</td>
<td>4000-4999</td>
<td>81214XXX</td>
</tr>
<tr>
<td>RTP</td>
<td>191</td>
<td>8191</td>
<td>1000-1999</td>
<td>81911XXX</td>
</tr>
</tbody>
</table>

Table 8 shows three example sites configured with a site code, an internal routing prefix of “8”, a routing prefix length of four and an extension length of four. It also shows the resulting, abbreviated on-net, inter-site dialing to reach each site’s destinations.

Even though SJC and NYC use the same extension range, the abbreviated on-net, inter-site dialing habit to reach destinations in these sites is still unique. The site codes are all three digits long and together with the steering digit “8”, result in four-digit location prefixes.

Defining the above fixed-length structure for abbreviated on-net, inter-site dialing enables Webex Calling to push a dial plan to the Webex Calling devices. When off-hook, the phone recognizes this abbreviated on-net, inter-site dialing habit and immediately stop collecting digits and sends the dialed digits to Webex Calling for analysis and call routing.

This fixed-length number structure for abbreviated on-net, inter-site dialing helps avoid inter-digit timeout and improves the overall user experience.

To enable calling from Unified CM to on-premises Unified CM and correct call type classification at least one dial plan needs to be configured in Webex Calling and for all enterprise and +E.164 number ranges homed on Unified CM the respective +E.164 and ESN patterns need to be configured in that dial plan. This not only guarantees correct routing of Unified CM destinations to Unified CM but also makes sure that for a call received by Webex Calling from a trunk that call is correctly classified as premises or PSTN call based on a caller ID match.
Service Assurance

Service Assurance refers to the suite of tools that help customers, partners and Cisco to successfully deploy and manage Webex Calling deployments.

CScan can be used for troubleshooting initial setups or for monitoring the health of Webex Calling calls.

CScan

CScan is the network readiness tool designed for Webex Calling. Customers or partners can use CScan to test their network connection via Internet.

To test the connection, just go to cscan.webex.com and select the location (one of the Webex Calling data centers) that the user resides in (closest to the user). Users can do a basic test which would test the internet connectivity (provide information on latency, download and upload speeds, and the ports that are needed for the Webex Calling). The advanced diagnostic option provides additional details on the QoS parameters such as Jitter, packet loss and latency.

For more information on using CScan, refer to the Webex help page at https://help.webex.com/en-us/y27bej/Use-CScan-to-Test-Webex-Calling-Network-Quality

Analytics

Analytics in Calling Admin Portal

Administrators can view call activity for the numbers in Calling Admin Portal (CAP) by choosing the Analytics tab and by selecting the date range.

Call Detail Records (CDRs) of up to 12 months from the current date is available for administrators to determine the calling behavior patterns for users. With the analytics tool, administrators can view the number of minutes in a call at a detailed user level or at a macro trending level.

The call details are also available for all the users and can be exported in the form of a CSV file.
Analytics in Webex Control Hub

Administrators can login to Webex Control Hub to get details on Quality Metrics and Engagement Analytics for Webex Calling calls. They can view historical data of call usage and engagement including media quality records. The Webex Calling analytics are available in Control Hub under “Analytics à Calling”.

Figure 26  Exporting call details in CSV format
Engagement Analytics

The Engagement Analytics provides graphical information on Calls and Call Minutes, detailing all the point-to-point calls made within the organization.

Figure 27  Webex Calling Engagement Analytics
Quality Analytics

The Quality Analytics tab allows the administrator to view records for each call and use sliders to filter calls based on quality statistics.

Figure 28   Webex Calling Quality Analytics

All statistics are directly collected from the devices/endpoints so that the QoS parameters (packet loss, jitter, latency) reflect the experience of the call from the end user's perspective.
Case Study: Unified CM with Centralized Call Processing and multiple Webex Calling Locations

Adding Webex Calling to existing Unified CM installations provides a solution for when centralized call processing is not possible due to insufficient available WAN bandwidth or other logistical challenges.

This case study examines scenarios where Webex Calling locations are combined with a multi-site Unified CM deployment. This type of deployment is useful in transition scenarios such as moving smaller sites from Unified CM to Webex Calling locations.

Local Gateway is a required component to establish connectivity between Webex Calling and on-premises Unified CM. Using the Webex Calling dial plan routing logic this can be complemented by Cisco PSTN or Cloud Connected PSTN to provide PSTN services for Webex Calling users. If no cloud PSTN is present, then the Local Gateway is used both for premises and PSTN calls.

Although Local Gateway can be deployed stand-alone, this case study focuses on Cisco Unified CM deployment integration.

Figure 29 shows a single-location Webex Calling deployment with Local Gateway. PSTN calls originating from Webex Calling endpoints in this case are sent to the Local Gateway which provides access to the PSTN.
If phones registered to Unified CM deployed as on-premises call control require direct dialing to Webex Calling locations, a Local Gateway integration is required.

**Figure 30**  Local Gateway combined with a dedicated PSTN Gateway

Figure 30 shows that calls originating from Webex Calling endpoints are sent to the Local Gateway based on Webex Calling dial plan routing logic. The Local Gateway then sends the calls on to Unified CM. The enterprise dial plan provisioned on Unified CM determines whether the call needs to be extended to an endpoint registered to Unified CM or to the PSTN via the existing PSTN GW infrastructure. Routing to the PSTN is only an option if the Webex Calling location is configured for premises-based PSTN. If instead cloud PSTN is used, then PSTN calls from Webex Calling users are sent to the cloud PSTN choice configured for the calling user's location.
Figure 31 shows a variation of this deployment mode where the Local Gateway and the PSTN access function reside on the same device. The difference in this scenario is the configuration on the combined Local Gateway and PSTN Gateway device. Neither from the perspective of the Webex Calling nor the Unified CM configuration, there is any major difference to the previous scenario. Note that with this scenario, Unified CM receives two types of calls from the CUBE hosting PSTN access and Local Gateway functionality: calls from the PSTN and calls from Webex Calling. To allow for differentiated class of service to be applied to these call types, two SIP trunks should be configured between CUBE and Unified CM: one for each call type. To achieve this, different SIP listening ports must be configured for each SIP trunk on Unified CM in the SIP trunk’s security profile.

Differentiation between PSTN calls and Webex Calling calls received from the Local Gateway is also required if the Webex Calling location is configured for cloud PSTN. While no PSTN calls would need to be forwarded back Unified CM from Webex Calling via the Local Gateway and back to the PSTN, Unified CM would still need to be able to apply differentiated class of service: calls originating from Webex calling would need access to remote on-net locations in multi-cluster deployments (for example via a connected Unified CM SME) while calls from the PSTN typically don’t need this access.

Combining both functions on the same device allows for more cost-effective deployments.
Call Routing Considerations

Calls from Webex Calling to Unified CM
As described earlier in the architectural overview calls from Webex Calling users are routed to premises trunks based on Webex Calling dial plans. If premises-based PSTN is used then PSTN calls are also sent to the premises trunks. The distinction between the two call types is up to Unified CM and depends on the enterprise dial plan provisioned on Unified CM.

Figure 32  Dialing from Webex Calling to Unified CM

Figure 32 shows an example of a multi-site Unified CM deployment with centralized call processing. A Webex Calling user is dialing a +E.164 number and the dialed number does not match any number provisioned for the customer in Webex Calling but the number matches a +E.164 dial plan pattern configured in a dial plan. The call is therefore sent to the trunk or route group selected as the routing choice for that dial plan. The Local Gateway sends the call on to Unified CM. Call routing on the Local Gateway does not take the called address into consideration; routing is solely based on trunk attributes so that any call received from Unified CM is forwarded to Webex Calling and any call received from Webex Calling is forwarded to Unified CM. The called party number seen in the call leg from Webex Calling to Unified CM via the Local Gateway is the original dialed destination in +E.164 format. Unified CM references the configured dial plan and routes the call to a locally registered endpoint on which the called destination is provisioned as a directory number.

To also enable enterprise abbreviated on-net inter-site dialing from Webex Calling to Unified CM, the respective enterprise patterns need to be added to the Webex Calling dial plan.
Case Study: Unified CM with Centralized Call Processing and multiple Webex Calling

Figure 33 Enterprise abbreviated dialing from Webex Calling

Figure 33 shows an enterprise with an enterprise-specific numbering plan using steering digit “8”, four-digit routing prefixes, and four-digit extensions.

This enterprise-specific numbering plan can be used when dialing on a Webex Calling registered device. The dialed digit string, when evaluated in Webex Calling matches an enterprise pattern defined in a dial plan and as before the call is sent to the trunk or route group defined as the routing choice of the Webex Calling dial plan. The call is then sent on to Unified CM by the Local Gateway.

Unified CM implements abbreviated on-net inter-site dialing using the above enterprise specific numbering plan, the dial string “80121164” is mapped to the DID of an endpoint registered to Unified CM and the call is connected. To allow for enterprise-abbreviated dialing from Webex Calling to Unified CM, the appropriate settings (extension length, prefix length, and steering digit) must be configured and Unified CM must be configured to support this dialing habit when routing calls received from Webex Calling.
Figure 34 shows a PSTN destination dialed from a Webex Calling device in a location with premises based PSTN configured as the PSTN choice for that location. The call is considered off-net from Webex Calling’s perspective and sent to the Local Gateway and then on to Unified CM. Unified CM does not locate an on-net match for the +E.164 address received from Webex Calling so it sends it on to the PSTN via the existing PSTN gateway controlled by Unified CM.
Calls from Unified CM to Webex Calling

To enable call routing from Unified CM to Webex Calling, a set of routes must be provisioned on Unified CM. This defines the set of +E.164 and enterprise numbering plan addresses in Webex Calling.

Figure 35  Calling from Unified CM to Webex Calling

Figure 35 shows that with these routes in place, both depicted call scenarios are possible. If a PSTN caller calls a DID assigned to a Webex Calling device, the call is handed off to the enterprise via the enterprise’s PSTN gateway, and sent to Unified CM. The called address of the call matches one of the Webex Calling routes provisioned in Unified CM and the call is sent to the Local Gateway. The called address must be in +E.164 format when sent to the Local Gateway. The Webex Calling routing logic routes the call to the intended Webex Calling device based on DID assignment. Calls from the PSTN should only be forwarded to Webex Calling by Unified CM if the Webex location uses premises-based PSTN or during a transition to cloud-based PSTN while the numbers haven’t been ported to the new provider yet.

Calls originating from Unified CM registered endpoints destined for Webex Calling are subjected to the Unified CM provisioned dial plan. This dial plan usually allows users to use typical enterprise dialing habits for calling.

Called addresses for calls to Webex Calling can be in +E.164 format, enterprise format or extension format. If the called address is an extension (two to six digits) then Webex Calling uses the location of the trunk the call is received on as routing context to allow for disambiguation if the extensions in Webex Calling are not globally unique.

Allowing enterprise numbers or extensions as called addresses from Unified CM to Webex Calling enabled calls from Unified CM to Webex Calling users without a phone number.
Figure 36 shows how using appropriate dialing normalization in Unified CM enables abbreviated on-net, inter-site dialing from devices registered to Unified CM to a Webex Calling location. The called address can either be normalized to +E.164 or sent without transformation. To normalize the called address to +E.164, Unified CM needs to know the ESN to +E.164 mapping for every Webex Calling location. When sending the called address unmodified then the enterprise numbering plan on Unified CM needs to be compatible with the enterprise numbering plan configured in Webex Calling. Not normalizing enterprise dialing to +E.164 for calls from Unified CM to Webex Calling enabled calls to Webex Calling users without a phone number.

Class of Service (CoS)
Strict CoS restrictions provide multiple benefits, including call loop avoidance and toll fraud prevention. When integrating Webex Calling Local Gateway with Unified CM’s CoS, consider a CoS for each of a following:

- Unified CM registered devices
- Unified CM receiving calls from the PSTN
- Unified CM receiving calls from Webex Calling
**CoS for Unified CM registered devices**

Webex Calling destinations are added as new class of destinations to an existing CoS. Permission to call Webex Calling destinations is equivalent to permission to call on-premises (including inter-site) destinations.

If an enterprise dial-plan already implements an “(abbreviated) on-net inter-site” permission, then a partition is already provisioned on Unified CM and can be used to configure all the known on-net Webex Calling destinations in the same partition. If the “(abbreviated) on-net inter-site” permission does not yet exist yet then a new partition, for example “onNetRemote”, must be provisioned. The Webex Calling destinations are added to this partition and it must be added to the appropriate calling search spaces.

**CoS for calls coming from the PSTN or Webex Calling**

Calls from the PSTN require access to all Webex Calling destinations only if premises based PSTN is used by Webex Calling locations or during the transition to cloud PSTN. This requires adding the above partition that holds all Webex Calling destinations to the calling search space used for incoming calls on the PSTN trunk. The access to Webex Calling destinations is in addition to any existing access.

Calls from the PSTN require access to Unified CM DIDs and Webex Calling DIDs. Calls from Webex Calling need access to Unified CM DIDs and PSTN destinations. The latter is only required if Webex Calling locations use premises based PSTN.
Figure 37 shows the two classes of service for calls from PSTN and Webex Calling. If the PSTN gateway functionality is co-located with the Local Gateway, then two trunks are required from the combined PSTN GW and Local Gateway to Unified CM: one for calls originating in the PSTN and one for calls originating in Webex Calling. This is driven by the requirement to apply differentiated calling search spaces per traffic type. Only with two incoming trunks on Unified CM this can easily be achieved by configuring the required calling search space for incoming calls on each trunk. Multiple trunks...
between Local Gateway and Unified CM can be configured by using different SIP listening ports for the two SIP trunks on Unified CM. The SIP listening ports are configured in the SIP trunk’s security profile.

The dial plan in Unified CM is configured to use both trunks depending on the type of call: to PSTN or to Webex Calling. On the Local Gateway the trunk a call is received on is identified by matching on the port number in the topmost VIA header in the INVITE. This is achieved by combining incoming uri via <some voice class> on the incoming dial peer with pattern :<UCM listening port> in the voice class uri <some voice class> in the Local Gateway configuration.

Unified CM Dial Plan Integration


The recommended dial plan design follows the design approach documented in the Dial Plan chapter of the latest version of the Cisco Collaboration System SRND available at the https://www.cisco.com/go/ucsrnd page.

The following information shows the configuration on Cisco Unified CM for Class of Service.

**Figure 38**   Dial Plan Recommendation
The previous figure shows an overview of the recommended dial plan design. Key characteristics of this dial plan design include:

- All directory numbers configured on Unified CM are in +E.164 format
- All directory numbers reside the same partition (DN) and are marked urgent
- Core routing is based on +E.164
- All non-+E.164 dialing habits. For example, abbreviated intra-site dialing and PSTN dialing using common dialing habits, are normalized (globalized) to +E.164 using dialing normalization translation patterns
- Dialing normalization translation patterns use translation pattern calling search space inheritance; they have the “Use Originator's Calling Search Space” option set.
- Class of service is implemented using site and class of service specific calling search spaces
- PSTN access capabilities (for example access to international PSTN destinations) are implemented by adding partitions with the respective +E.164 route patterns to the calling search space defining class of service

Figure 39 shows how to add reachability for Webex Calling destinations to this dial plan. A partition representing all Webex Calling destinations must be created, “WebexC”, and a +E.164 route pattern for each DID range in Webex Calling is added to this partition. This route pattern references a route list with only one member: the route group with the SIP trunk to the Local Gateway for calls to Webex Calling. If multiple Local Gateways exist then a Unified CM route group can be used for load balancing and redundancy. Because all dialed destinations are normalized to +E.164 either using dialing normalization translation patterns for calls originating from Unified CM registered endpoints or inbound called party transformations for calls originating from the PSTN this single set of +E.164 route patterns is enough to achieve reachability for destinations in Webex Calling independent of the dialing habit used.

If for example a user dials "914085553165" then the dialing normalization translation pattern in partition “UStoE164” normalizes this dial string to “+14085553165” which will then match the route pattern for a Webex Calling destination in partition “WebexC” so that Unified CM will ultimately send the call to the Local Gateway.
Adding Abbreviated Inter-site Dialing

Figure 40 shows the recommended way to add abbreviated inter-site dialing to the reference dial plan by adding dialing normalization translation patterns for all sites under the enterprise numbering plan to a dedicated partition ("ESN", Enterprise Significant Numbers). These translation patterns intercept dial strings in the format of the enterprise numbering plan and normalize the dialed strings to +E.164.

Adding enterprise abbreviated dialing to Webex Calling destinations is achieved by adding the respective route pattern for the Webex Calling location to the “WebexC” partition (for example “80133XXX”). The called party is not transformed and instead sent to Webex Calling as is. This allows to use enterprise abbreviated dialing from Unified CM to extension only Webex Calling users.

Local Gateway deployment

At least one Local Gateway needs to be provisioned for the connection between Webex Calling and Unified CM. Multiple Local Gateways can be configured for scale and redundancy. The location the Local Gateway is assigned to is only relevant if the dialing context needs to be established for extension dialed calls from Unified CM to Webex Calling. As long as no partial migration occurs where some of the users of the same location are on Unified CM and some are on Webex Calling, extension dialing from Unified CM to Webex Calling is not a valid use case so that in that case the location association of the Local Gateways does not matter. The decision about the number of Local Gateways to deploy and where to deploy the Local Gateways is mainly driven by scale and reliability requirements.

In the simplest case, all Local Gateways are added to a single route group.
Webex Calling dial plan configuration

The global “Unknown Numbers Handling” parameter is set to “Standard behavior” so that routing to Unified CM and call classification is based on the dial plan patterns in an enterprise dial plan. The single route group with all Local Gateways is used as routing choice for that dial plan.

The global “Caller ID Format for Calls from and to On-premises” setting should be set to “ESN” to make sure that callback is possible from Unified CM for calls originating from Webex Calling

For each enterprise and +E.164 number range on Unified CM, the respective pattern is added to the dial plan.

On each Webex Calling location, the internal dialing routing prefix is configured in line with the end-to-end enterprise dial plan. It is essential to select a unique site prefix for each location. The same site prefix cannot exist on Webex Calling and on Unified CM at the same time. The “Enable routing unknown extensions to the Premises as internal calls” option is disabled.