CHAPTER 5

Cisco Webex Hybrid Call Service

Revised: April 29, 2020

Cisco Webex Hybrid Call Service provides seamlessly connection between Cisco Webex and Cisco Unified Communications Manager (Unified CM) as the on-premises enterprise call control.

This chapter introduces important updates to the hybrid calling architecture for users and Webex devices:

- Webex Teams application can now natively register to Cisco Unified CM and to the Webex cloud simultaneously.
- When registered to Cisco Unified CM, Webex Teams uses the same device types that Jabber uses. The Architecture, design considerations and deployment for Webex Teams with Unified CM calling are the same for as they are for Jabber, with few exceptions that are outlined in this chapter.
- If Cisco Unified CM users have already been enabled for Jabber, no additional steps are required in order to enable Webex Teams with UCM calling. However, a single user cannot use Jabber and Webex Teams at the same time.
- Webex devices (known as “Places” in Cisco Webex Control Hub) no longer require the Cisco Call Connector.
- The Cisco Call Connector is replaced by the “Cisco Webex Device Connector”, a plug-in which runs on Mac or Windows PC and used only for provisioning.

Overview

Webex Hybrid Calling enables Webex Teams users and Webex devices to make and receive calls using the same dialing procedures used by endpoints registered with Cisco Unified CM.

Webex Hybrid Calling consists of two main calling features:

- Hybrid Calling for Webex Teams (Unified CM): enable Webex Teams users to make and receive calls on their client through native registration of Webex Teams to Unified CM.
- Hybrid Calling for Webex devices: enable Webex devices to make and receive calls using the same dialing procedures used by endpoints registered with Unified CM.

Core Components

- Webex Teams with Unified CM calling provides a native integration to Cisco Unified CM

- Cisco Expressway-C and Expressway-E provide firewall traversal for SIP signaling, media, and mobile and remote access.
- Cisco Unified Communications Manager (Unified CM) provides call control.
- Cisco Webex Device Connector enables integration between Cisco Unified CM and Webex devices

Recommended Deployment

Calling in Webex Teams (Unified CM) is based on native registration of the Webex Teams application to Cisco Unified CM. As such Webex Teams application registers to Unified CM inheriting all of the benefits of Unified CM features, including Unified CM directory, corporate dial plan, user dialing habits and phone services. Registration of Webex Teams to Unified CM happens directly when the client is located on-premises, or via Mobile and Remote Access (MRA) when the client is located on the Internet.

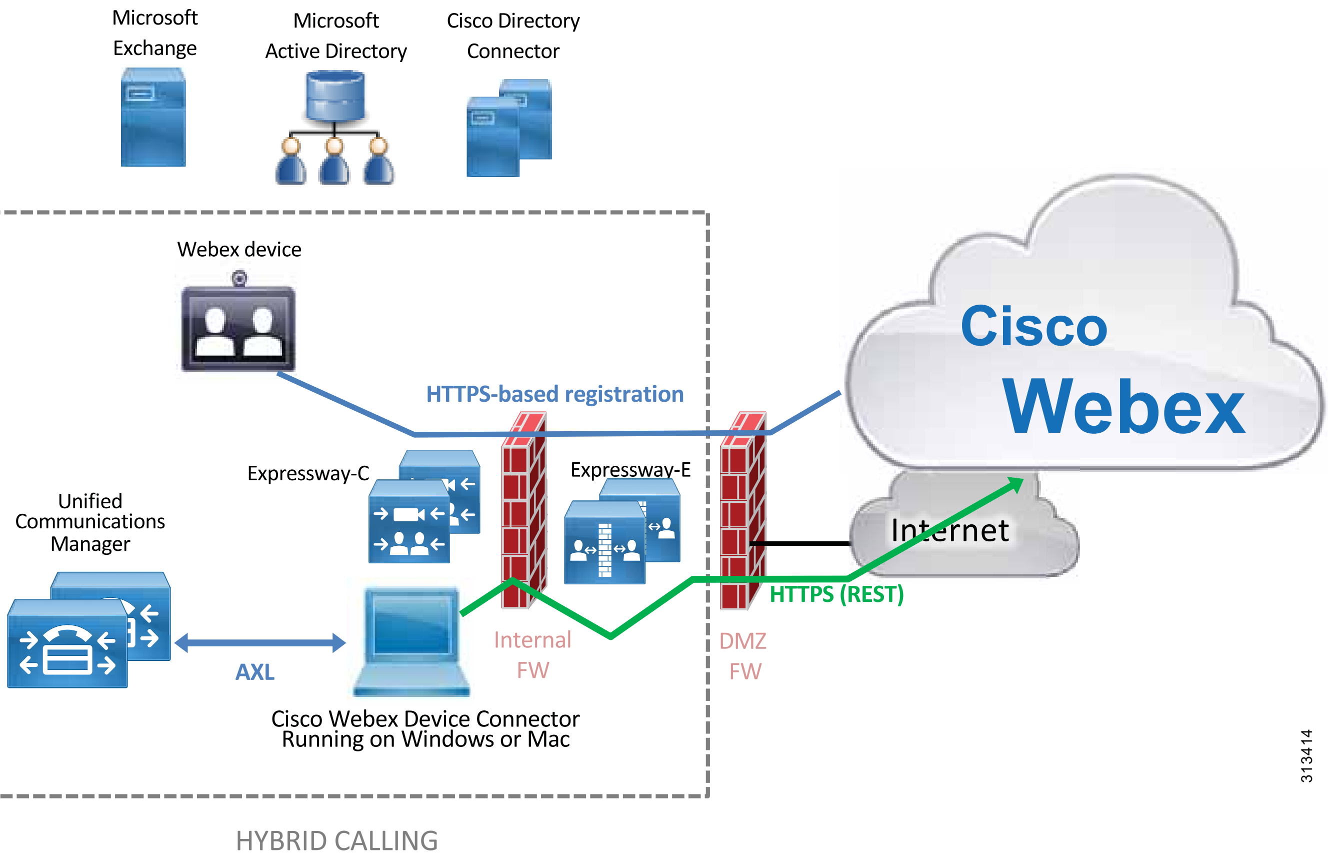
As a result of this direct registration to Unified CM a variety of native calling features become available to the Webex Teams client such as:

- Shared line: By assigning the same directory line to both the Webex Teams application and the Unified CM device, Webex Teams has access to shared line functionality.
- Direct media path: Two on-premises Webex Teams applications registered to Cisco Unified CM have a direct media path. Media is not sent to the Webex Cloud.

Webex devices are enabled for hybrid calling through the Cisco Webex Device Connector. The Webex Device Connector is a plug-in that runs on PC or Mac and connects on one side to Unified CM via Administrative XML (AXL) providing the Device Connector with access to Unified CM provisioning.

On the other side of the Device Connector HTTPS is used to communicate with Webex (See Figure 5-1.) This connection traverses the customer's Internet proxy or Internet edge and does not use the Expressway-E and Expressway-C firewall traversal setup.

Figure 5-1 Cisco Webex Device Connector Provides Communication Between Cisco Unified CM and Cisco Webex for Device Provisioning



When a Webex device is enabled for Hybrid Calling, the Cisco Webex Control Hub prompts the user to enter the email address associated with that device as a unique Cloud identifier. It is not required that the Webex device has a real mailbox. The Device Connector uses the AXL interface to find the user ID associated with that email on Cisco Unified CM, and to locate the Spark Remote Device associated to that user. Finally, it populates the associated remote destination, called the Associated Identity. Device Connector does not participate in call setup or tear-down. After provisioning is done, Device Connector can be shut down. The Webex device will be able to receive calls regardless of whether the call is initiated by a Webex Teams user, by a Unified CM registered device, or by a Unified CM connected IP or PSTN gateway. Device Connector-based provisioning allows Webex devices to place calls using enterprise dialing habits.

In order to achieve this, a SIP connection must be set up between Webex and Expressway-E using standard business-to-business technologies and Transport Layer Security (TLS) with mutual authentication. For this reason, Expressway-E must use a certificate signed by a Certification Authority trusted by Webex. For a list of trusted Certification Authorities, refer to the *Deploy Hybrid Call Service for Cisco Webex Devices* latest version of the *Deployment Guide for Cisco Webex Hybrid Call Service*, available at

https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Key Benefits

Webex Hybrid Call Service provides the following key benefits:

- Native Unified CM registration for Webex Teams applications
- Increased security with firewall traversal architecture for signaling and media
- Mobile and remote access architecture for Webex Teams applications when located on the public Internet
- Security achieved through certificates and TLS with mutual authentication for Webex devices

Architecture

The Webex Hybrid Calling architecture includes both Webex Teams applications registered natively to Cisco Unified CM and Webex devices registered to Webex. These two scenarios are quite different and each is discussed below.

Webex hybrid calling for Webex Teams users

The hybrid calling architecture has moved away from the server-side integration model based on Call Connector towards a client-side integration. In this new model Webex Teams, the client, is entirely responsible for the hybrid calling integration, and the Call Connector is no longer required.

The Webex Teams application is now able to register to both Cisco Webex and the Cisco Unified CM at the same time. While Webex spaces, whiteboarding, file sharing, and meetings are still managed by Webex, call control is managed with two different behaviors:

- Webex Teams calling. Calls are entirely managed by the Webex cloud for both signaling and media. Media is always handled by the Webex cloud.
- Webex Teams calling through Cisco Unified CM. SIP signaling is handled by Cisco Unified CM, and the Webex Teams application sends the media to the destination without involving the Webex Cloud.

When a Webex Teams user is enabled for Unified CM Calling, both calling behaviors are available, and the Webex Teams application automatically selects one of the two.

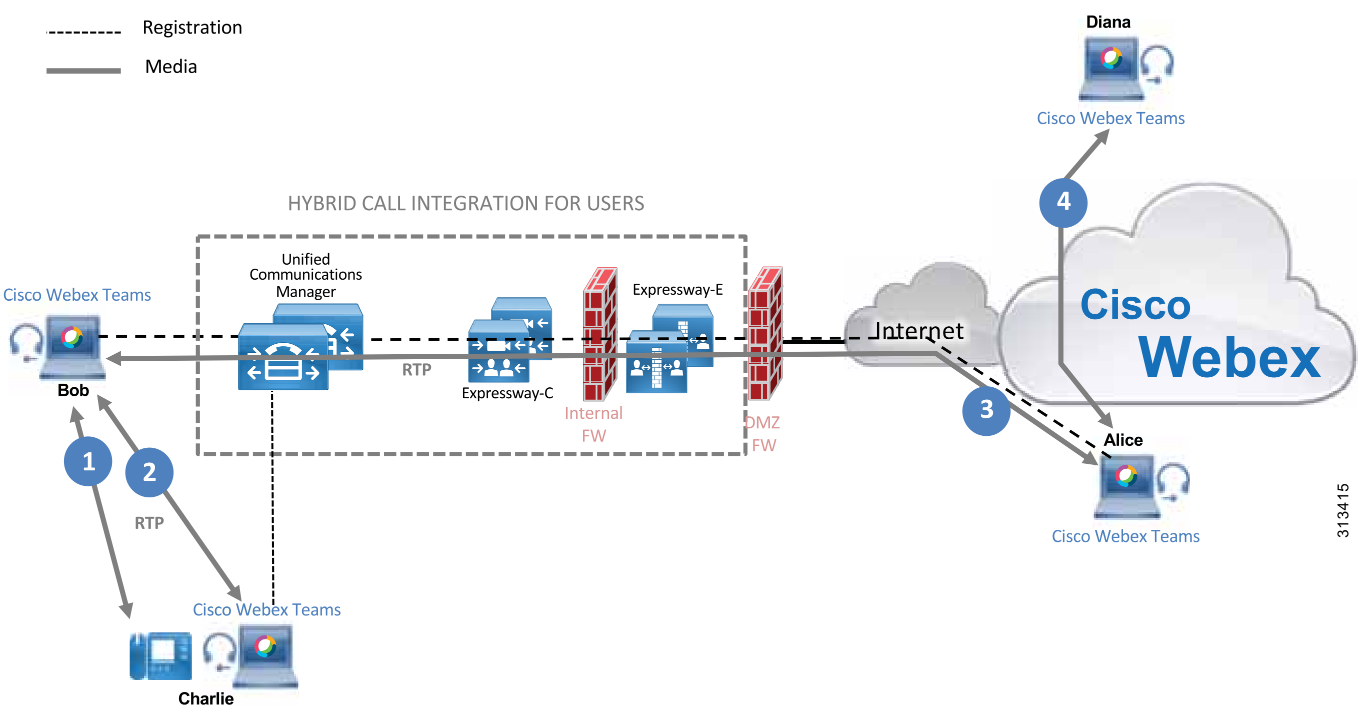
When a Webex Teams user is not enabled for Unified CM calling, only the first behavior is available, and all calls will always be sent through the Webex cloud.

Registration to Unified CM is direct when the Webex Teams application is on-premises, and through mobile and remote access when the client is connected over the Internet. An important consequence of this is that when the Webex Teams client is registered to Cisco Unified CM, it provides for peer-to-peer media path where possible (that is, when a call does not involve mobile and remote access). This is different than when a call is made using cloud calling, where the media is always hair-pinned in the Cisco

Webex Cloud. On the contrary, Webex Teams integrated with Unified CM enables media to be sent directly between two Webex Teams applications or between a Webex Teams application and a Cisco Unified CM device.

The following illustration shows some of the media paths available with Webex Teams with Cisco Unified CM registration

Figure 5-2 Media paths for Webex Teams with Unified CM registration



If a Webex Teams application is on-premises and registered to Cisco Unified CM, the media path between this and another on-premises Webex Teams application or Unified CM device is peer-to-peer (media paths #1 and #2 in Figure 5-2).

If a Webex Teams user is on the Internet, and another Webex Teams user is on-premises, the communication is peer-to-peer through Mobile and remote access (media path #3). If a Webex Teams user talks to a Webex Teams user who has not been enabled for Unified CM registration, the media path traverses the Webex cloud (media path #4) whether one or both clients are on-premises or not.

The Webex Teams application when registered with Unified CM supports CTI. This allows a Webex Teams user to:

- Select one of the desk phones associated with that user on Cisco Unified CM
- Start and answer a call on the associated desk phone by using the Webex Teams application

Note At the time this document is written, CTI is not supported through mobile and remote access. Desk phone control over MRA requires the controlled device to be registered through MRA and the controlling Webex Teams client connected via VPN.

A Webex Teams user must be enabled in Webex Control Hub for Cisco Unified CM calling. This can be done globally or for selected users. If users have already been enabled for Call Service Connect, disable Call Service Connect and Call Service Aware first before enabling Unified CM calling.

The Webex Teams application locates Unified CM by using the following DNS SRV records:

- _cisco-uds._tcp.<domain> in the internal DNS Server
- _collab-edge._tls.<domain> in a public DNS Server

Those records point to Unified CM if the user is on-premises, or to the Expressway-E if the user is on the Internet.

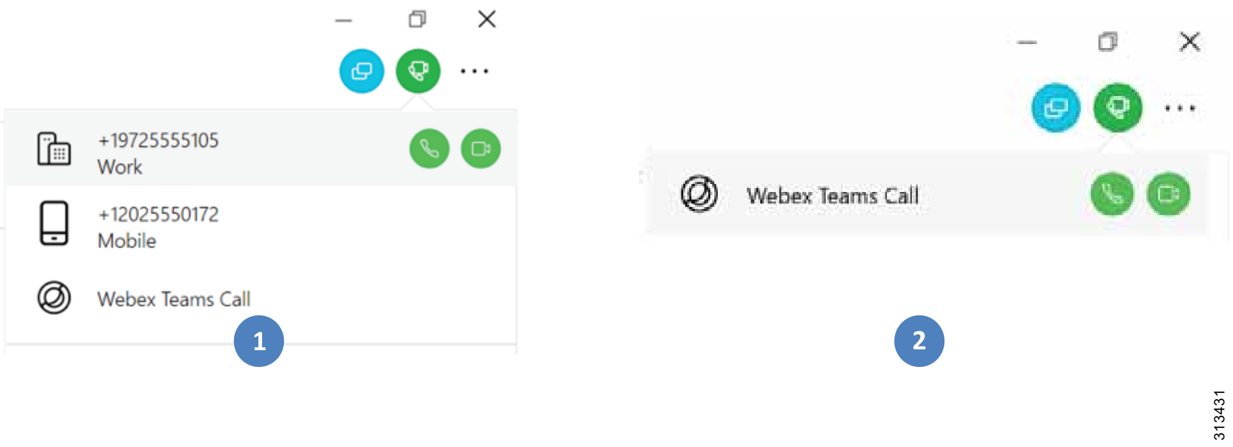
User Experience

After a Webex Teams user has been enabled for Unified CM calling, and once the user has logged into the Webex Teams application, a secondary pop-up window appears. This window requires the user to enter the username and password for Unified CM. Unless single-sign-on is enabled, a different set of credentials might be used for the Webex Teams application initial login and the Unified CM login.

When a Webex Teams user enabled for Cisco Unified CM calling wants to click-to-dial to another user, he has two options based on the called user capabilities:

- If the called user has also been enabled to Unified CM calling, the call icon shows a handset and the directory numbers configured on Active Directory and synchronized through the Directory Connector, as picture 1 shows in Figure 5.3
- If the called user is not enabled to Unified CM calling, the call icon shows a camera (picture 2 in Figure 5.3)

Figure 5-3 ***Webex Teams application calling experience***



If a Webex Teams user dials any number instead of clicking a contact, that number is routed to Cisco Unified CM, directly or through mobile and remote access. As a result, any public E.164 number, as well as enterprise significant numbers, are directed towards Cisco Unified CM, that will route those numbers internally or towards the PSTN.

When a Webex Teams user enabled for Cisco Unified CM calling wants to dial out to another user, Unified CM directory numbers will be available by clicking the contact. The calling user can select one of the numbers in the list, as illustrated in Figure 5.3 image 1. Because the call has a numeric destination, it will be sent through Cisco Unified CM.

If the called user has not been enabled for Unified CM calling, by clicking in the call icon directory numbers will not appear, as illustrated in Figure 5.3 image 2. The call will be sent through Webex and will not involve Cisco Unified CM.

It is worth noting that numbers from Unified CM are populated by Directory Connector, and they appear for all users. However, only if the calling user has been enabled for Unified CM calling they be able to see and click on the number, regardless of whether the called user is enabled in Unified CM or not. If the called user is not enabled in Unified CM the numeric call will be sent to the Unified CM desktop device.

Unlike numeric routing, SIP URIs routing behavior is configurable. A number followed by a domain is considered to be a SIP URI, and as such it follows the SIP URI configuration set by the administrator. This is discussed in the Webex Teams SIP URI dialing section.

Webex hybrid calling for Webex Room systems

Webex hybrid calling architecture allows Webex Devices to be integrated with the Unified CM dial plan, to use the same dial habits of the Enterprise, and to send and receive calls to and from the PSTN through the Unified CM. Previously this functionality has been facilitated through Call Service Connect. However, Call Connector is now replaced by Cisco Webex Device Connector, a Webex Control Hub downloadable plugin that runs on any Mac or Windows client and performs the initial provisioning of Webex devices.

Webex devices are provisioned in Webex Control Hub as "Places" and as such they do not require any user association in Webex Control Hub. However, a local user must be created on Cisco Unified CM for every Place configured on Webex Control Hub. That local user does not have to be provisioned on the LDAP directory Cisco Unified CM is synchronized with, but it must have a unique mail ID, a +E.164 telephone number, and a directory URI. Webex associates every identity to a unique email address, be it a user or a place, but the room system email address does not require an associated Exchange inbox because Webex only sends emails to Users, not to Places.

The Cisco Unified CM administrator will also configure a Cisco Spark Remote Device on Cisco Unified CM for every Webex device. The local user must be associated to a Cisco Spark Remote Device (Spark RD) on Cisco Unified CM. The Cisco Spark Remote Device is a virtual device that represents the Webex device as if it was registered on Cisco Unified CM. The Spark RD has a Directory Number and a SIP URI that are part of Cisco Unified CM dial plan. This ensures that the Webex device will be reachable using the corporate dial plan. The administrator will also specify the device pool, location, and reroute calling search space for the Spark RD. The calling search space configuration for the Spark RD will determine the dialing permissions for Webex devices based on dialed numbers or URIs.

Webex room SIP Address and Enterprise URI

Once the Cisco Spark Remote Device is configured, Device Connector will automatically configure Associated Identities (formerly Remote Destinations) on the Spark Remote Device on Cisco Unified CM in order to allow simultaneous ring functionality between Webex Teams applications and Unified CM devices.

As an example, if a Webex device is provisioned for hybrid calling, the Device Connector will add an associated identity to the Spark RD via the Unified CM AXL API. The associated identity on Cisco Unified CM matches the Webex SIP address assigned for that Webex device and shown in Cisco Webex Control Hub.

The Webex SIP address for a Place is in the form:

*<roomID>@<subdomain>****.rooms.webex.com***

Where *<roomID>* is the attribute uniquely identifying the Place in the Webex corporate directory domain, and *<subdomain>* is the unique subdomain configured for the organization in the Webex Control Hub. In this example, the corporate domain is **ent-pa.com** and the subdomain configured by the administrator is **ent-pa**. Webex asserts that the subdomain is unique or else prompts the administrator to create a new one if the subdomain is already in use.

In order to understand which **Spark RD** the Device Connector on Cisco Unified CM must populate with the Associated Identity for a specific device, the email address is used. When a device is enabled for hybrid calling, Cisco Webex Control Hub prompts for the email address associated to the device.

Next, the administrator runs the Cisco Webex Device Connector, which performs a discovery of all the Places configured for hybrid calling in Webex Control Hub. It determines the associated email, and then accesses Unified CM and retrieves the device configuration there. The pertinent aspects of this configuration include the directory number configured as line settings in the corresponding Spark RD, the SIP URI, and the telephone number configured on the device.

As an example, when a Place is created, the Webex SIP address appears in Webex Control Hub:

Cisco Webex SIP Address

conference_room01@ent-pa.rooms.webex.com

When this room is enabled for hybrid services, and after the administrator has assigned the email conf01@ent-pa.com to that room and the sync process is completed, the information specified under “Cisco Unified CM details” will appear in Cisco Webex Control Hub:

Cisco Unified CM details

Mail ID: conf01@ent-pa.com

Directory URI: meet01@ent-pa.com

Directory Number: +14085554401

Phone Number: +14085554401

Cluster Fully Qualified Domain Name (CFQDN): us-cm-pub.ent-pa.com *.ent-pa.com

Please note that while in many cases the directory URI matches the corporate email, in some other cases this does not happen, as this example shows.

Cluster Fully Qualified Domain Name (CFQDN) configured on Cisco Unified CM is used to route the call to destination via Expressway-C and Expressway-E.

Although the CFQDN enterprise parameter in Unified CM allows the use of wildcards (for example, *.ent-pa.com), the use of the first value of the CFQDN enterprise parameter as the SIP route header for hybrid calling flows prohibits the use of wildcards in the first CFQDN value. If a wildcarded value is required to maintain the existing call routing logic on Unified CM, then a non-wildcard CFQDN has to be added as the first entry, such as in the following example:

CFQDN: us-cm-pub.ent-pa.com *.ent-pa.com

Note The CFQDN must be different than the Expressway-C or Expressway-E DNS domain. As an example, if the CFQDN is set to ent-pa.com and the DNS domain of Expressway is also set to ent-pa.com, Expressway might not be able to route the call because this creates an ambiguity between regular inbound business-to-business calls and hybrid call flows.

While the directory number is taken from Cisco Unified CM device line settings, the Phone Number is retrieved from the associated end-user account configuration. The Phone Number will also show on the Webex device as the device number. If the administrator does not configure a phone number for the associated end-user, no number will be shown on the Webex device screen.

Once provisioning is done, the Webex device is ready to place and receive calls.

Call Flows

When a call is received by Cisco Unified CM matching the Directory Number or Directory URI associated to a a Webex device, as step 1 in Figure 5-4 shows, Unified CM sends the call to the corresponding Spark RD, as shown by step 2 in the same figure. The call is then extended to the Cloud using the Associated Identity conference_room01@ent-pa.rooms.webex.com through a SIP route pattern to Expressway-C. Expressway-C is configured to send any URI of the form <roomID> @ent-pa.rooms.webex.com to Expressway-E, and Expressway-E in turn sends it to the DNS zone (step 3).

In order to find the Webex cloud, Expressway-E queries the public DNS for SRV resolution for the record _sips._tcp.callservice.webex.com even if the domain portion of the SIP URI is ent-pa.rooms.webex.com, because the DNS Zone on Expressway is configured to use callservice.webex.com instead of ent-pa.rooms.webex.com. This is done through the Modify DNS Request and the Domain to search for settings in the DNS Zone, and the call is sent to Webex. The Webex room is now able to receive the call (step 4).

Figure 5-4 Call Flow for a hybrid room system

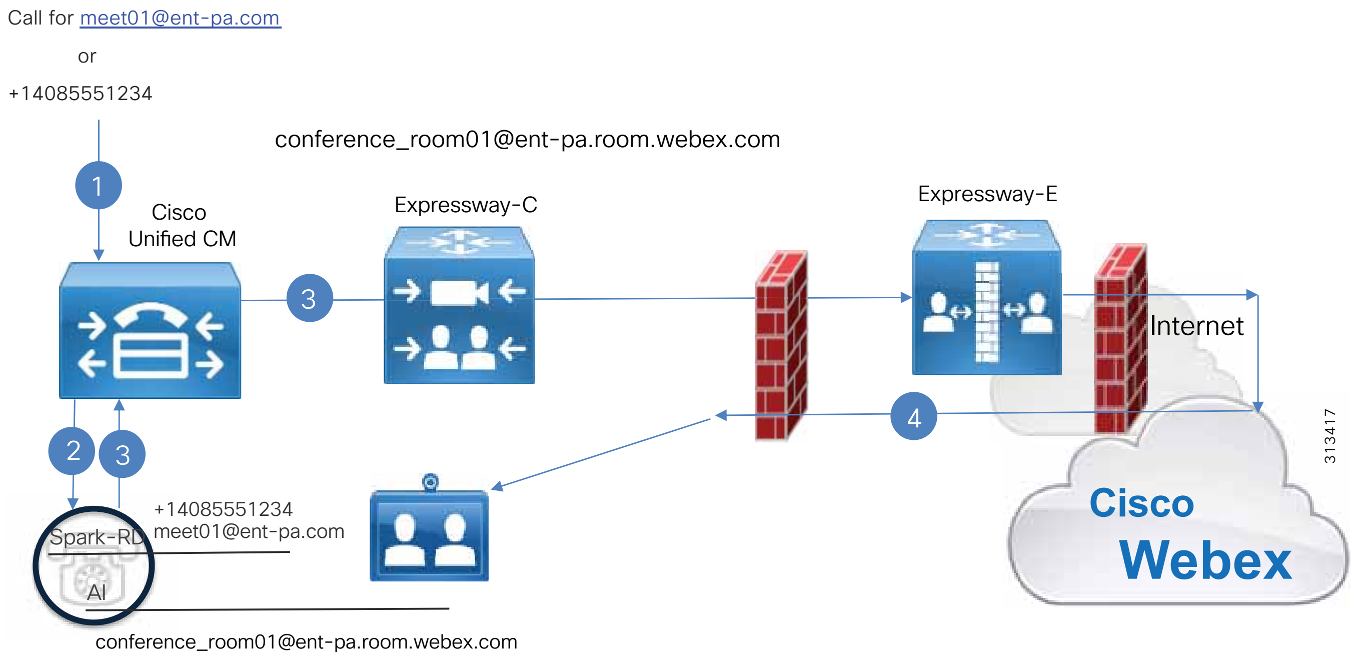


Figure 5-4 shows the following actions:

1. Cisco Unified CM receives a call for the Webex room system (telephone number +14085551234, or SIP URI meet01@ent-pa.com)
2. The call is sent to the corresponding Cisco Spark Remote Device
3. The call is extended to Webex through the associated identity included in the Cisco Spark Remote Device (conference_room01@ent-pa.rooms.webex.com), and sent to Expressway-C via a SIP Route Pattern. Then Expressway-C sends the call to Expressway-E, which uses the DNS discovery process to locate Webex
4. The call is sent to Webex and delivered to the Webex Device

When the Webex room dials a Cisco Unified CM destination or a PSTN number, Webex detects that the device is enabled for Hybrid Calling and it sends the call to the Expressway-E cluster located through the SRV record _sips._tcp.ent-pa.com.

If this record is already used for business-to-business communications, we recommend specifying a substring of the corporate domain as the SIP destination in the Webex Control Hub, and consequently a public DNS SRV record, as follows:

Service and protocol: _sips._tcp.mtls.ent-pa.com

Priority: 1 Weight: 10

Port number: 5062

Target: edge-expe1.ent-pa.com

The SIP destination configured by the corporate administrator in the Webex Control Hub determines where Webex sends hybrid call legs for this organization. By specifying mtls.ent-pa.com instead of ent-pa.com, Webex will query for the SRV record _sips._tcp.mtls.ent-pa.com instead of _sips._tcp.ent-pa.com, thus getting a different port (5062) than standard SIP port (5061).

This is necessary if the same Expressway is also used for business-to-business calls that use TLS instead of TLS with Mutual Authentication. This way, a connection to Expressway-E on destination port 5061 will trigger TLS, and a connection on destination port 5062 will trigger TLS with Mutual Authentication, and Expressway-E will check that the identity of the calling party matches the Webex cloud through certificates. This is explained in detail in the next section.

Expressway-E and Expressway-C are configured to route the call internally, as they would with any business-to-business call.

Note Webex populates the SIP request with a SIP Route Header, which takes precedence over the Request URI. In all cases, routing on Expressway-C and Expressway-E is not performed according to the Request URI but according to the Route Header instead. You must consider this when creating the search rules on Cisco Expressway. Because this is especially important in deployments of multiple Cisco Unified CM clusters, this information is covered in the section on *Deployment Considerations for Multiple Unified CM Clusters*, although it applies to a single cluster scenario as well.

When the call reaches Unified CM it is anchored on the Spark RD corresponding to the Webex device. This anchoring is based on the caller ID of the incoming SIP call leg, which matches the associated identity provisioned of the Spark RD. Call anchoring is a mobility feature that is used to preserve calling ID and apply class of service. It does this based on the calling search space (CSS) configured on the Spark RD where the call is anchored. For more details, see the section on Caller ID and Class of Service

After anchoring, the call is sent to the final destination, that is any directory number or SIP URI reachable through Unified CM, such as an extension or a PSTN number.

The following picture shows the detailed steps for a PSTN call

Figure 5-5 PSTN Call Flow

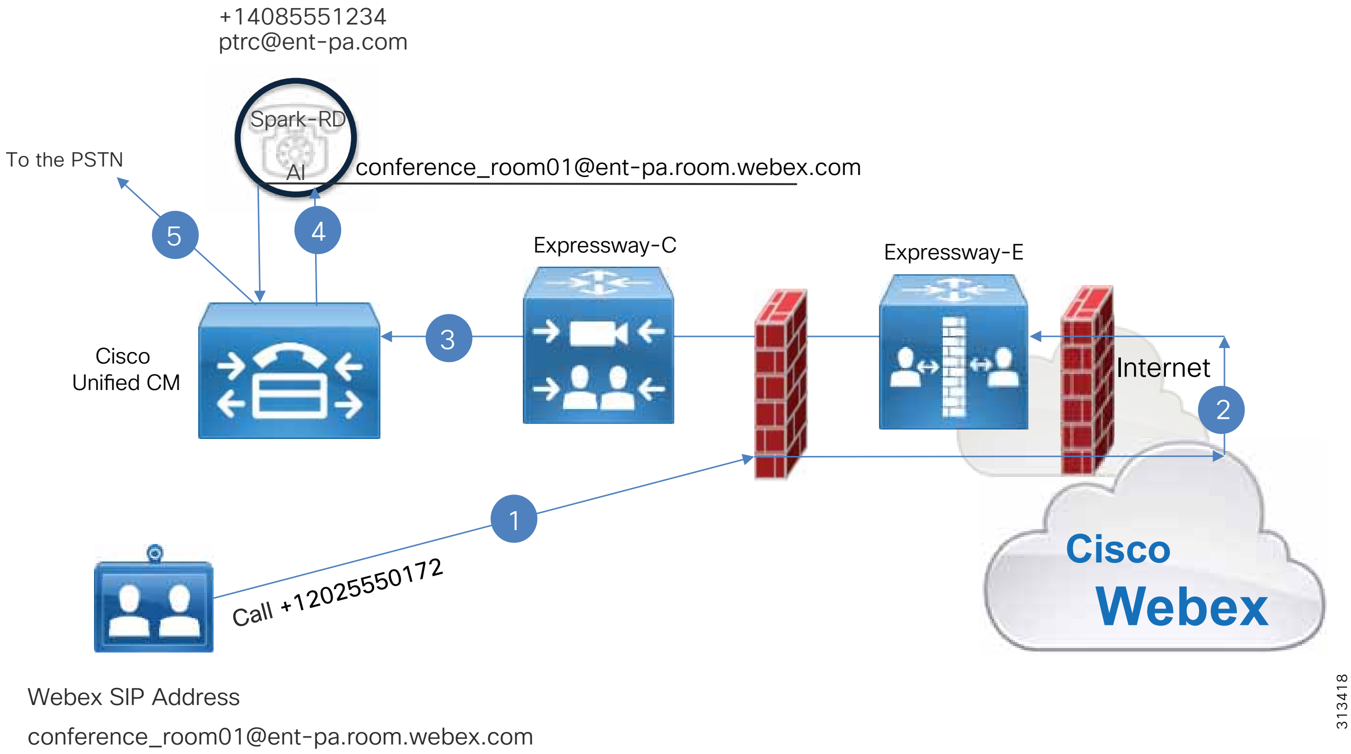


Figure 5-5 shows the following actions:

1. A users dials a destination (a PSTN number in this example) from the Webex Device. The call is sent to Webex.
2. As the Webex room is enabled for hybrid calling, Webex locates the Expressway-E based on the SIP destination set in the Control Hub
3. The call is sent to Unified CM through the Expressway
4. On Unified CM, because Calling ID (conference_room01@ent-pa.rooms.webex.com) matches the Associated Identity, the call is anchored on the Spark RD and the numeric Calling ID will be replaced with the Spark Remote Device calling ID (+14085551234 instead of conference_room01@ent-pa.rooms.webex.com)
5. The call is delivered to the PSTN using the new calling ID.

When a Webex hybrid device calls another Webex hybrid device, the media path flows through Webex.

When a Webex hybrid device calls a Webex Teams user and vice-versa, regardless from the fact that this user is enable for Unified CM calling or not, the media path flows through Webex.

Webex Teams SIP URI dialing

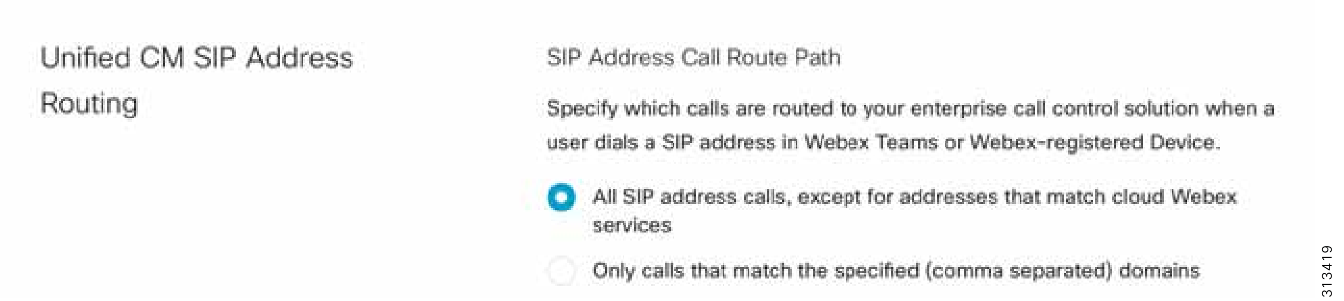
While numeric calls are always routed through Unified CM, SIP URI call routing is administratively configurable on Webex Control Hub for Webex Teams users.

Note At the time this document is written, this configuration does not affect Webex devices. Webex devices hybrid calls are always routed via Cisco Unified CM through Cisco Expressway.

Two options are available:

1. All SIP URI calls are routed via Cisco Unified CM, with the exception of Webex domains which are directly routed to Webex. This is shown in Figure 5-6.

Figure 5-6 SIP URI calls are routed through Cisco Unified CM, with the exception of Webex services



Unified CM SIP Address Routing

SIP Address Call Route Path

Specify which calls are routed to your enterprise call control solution when a user dials a SIP address in Webex Teams or Webex-registered Device.

● All SIP address calls, except for addresses that match cloud Webex services

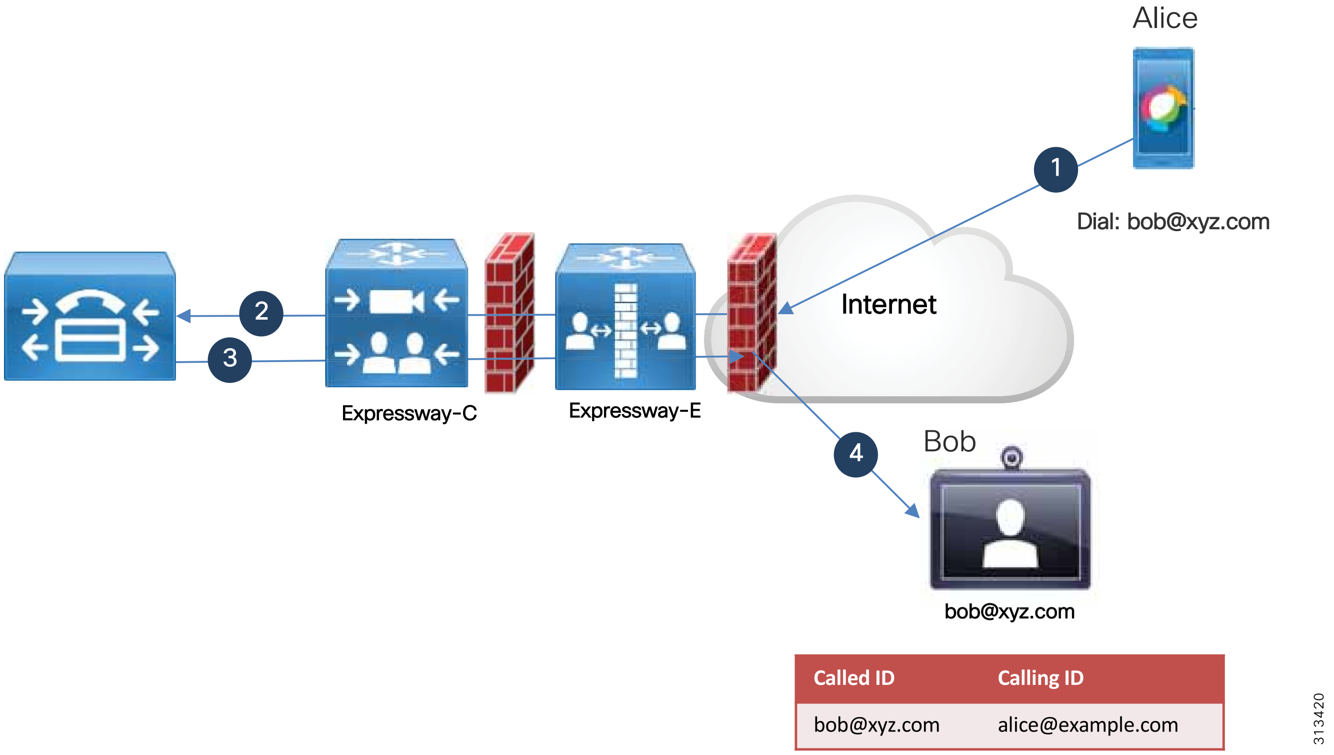
○ Only calls that match the specified (comma separated) domains

By selecting this option, all SIP URI calls will be routed through Cisco Unified CM. The major benefit is that Cisco Unified CM will be able to apply class-of-service for SIP URI calls, and a consistent calling ID. Because numbers are always routed through Cisco Unified CM, only Webex services calls (like calls to Webex meetings) are routed through Webex and do not involve Cisco Unified CM.

Figure 5-7 shows this scenario when Alice dials to Bob, who belongs to another company. As the illustration shows, this B2B call will always be hairpinned through Expressway and Cisco Unified CM.

As Figure 5-7 shows, by selecting the first option all SIP URIs will be sent to Unified CM. This way, Bob will receive a call from alice@ent-pa.com, consistent with Unified CM dial plan, instead of a call coming from the Webex SIP URI alice@ent-pa.call.webex.com.

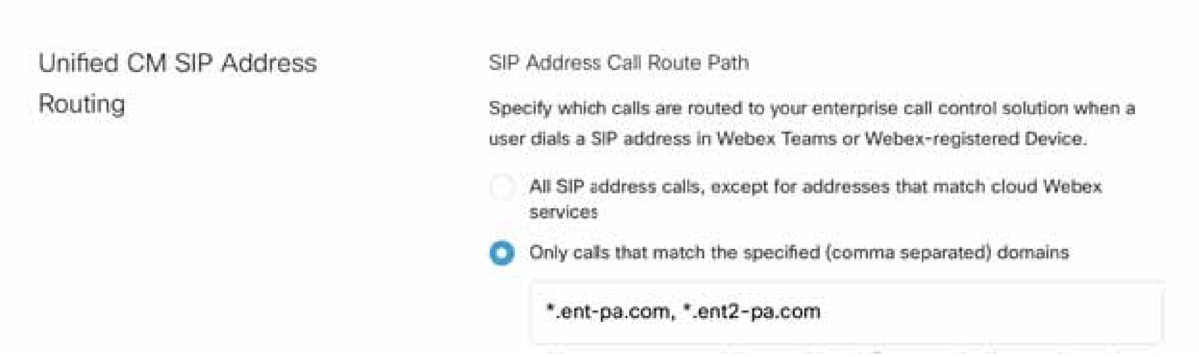
Figure 5-7 Alice making a B2B call to Bob



Called ID	Calling ID
bob@xyz.com	alice@example.com

2. Only calls that match specific domains are routed via Cisco Unified CM. All other SIP URI calls, as well as Webex domains, are routed through Webex. This is shown in Figure 5-8.

Figure 5-8 Only internal SIP URI calls are routed through Cisco Unified CM



Unified CM SIP Address Routing

SIP Address Call Route Path

Specify which calls are routed to your enterprise call control solution when a user dials a SIP address in Webex Teams or Webex-registered Device.

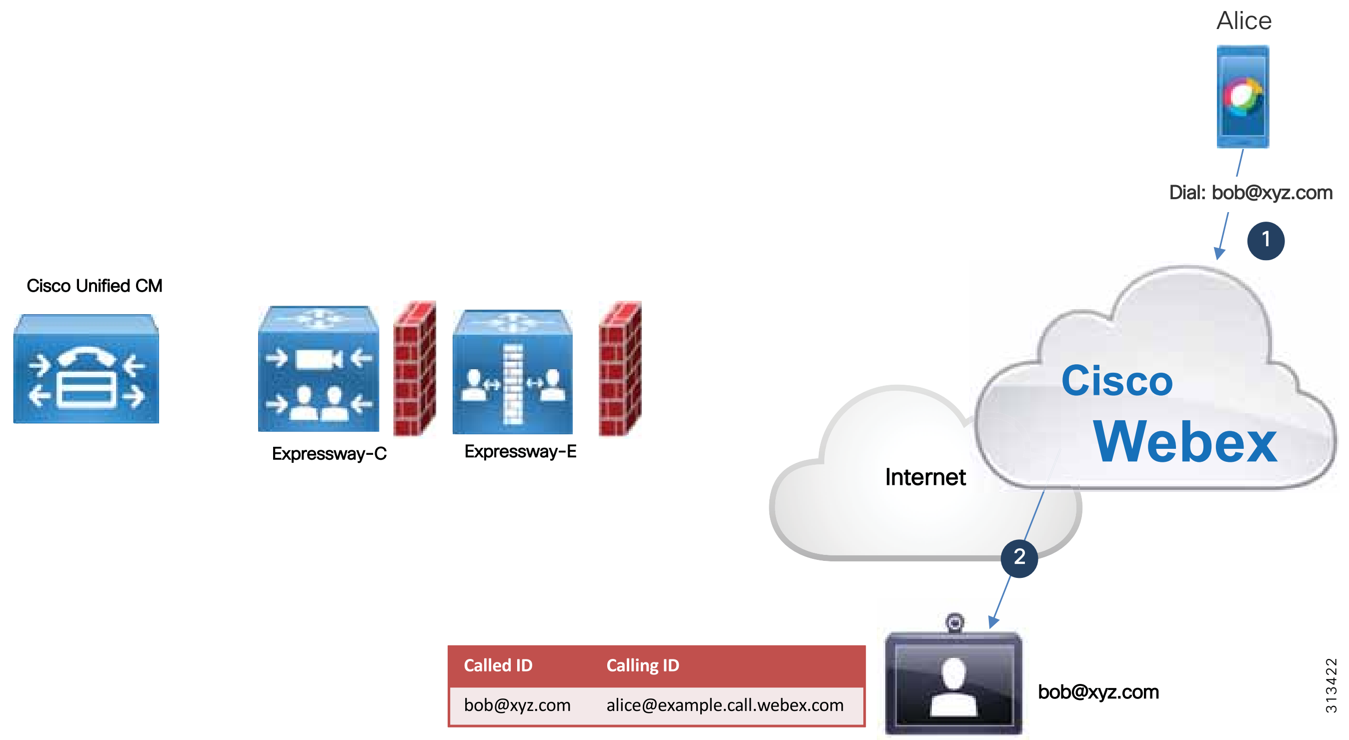
○ All SIP address calls, except for addresses that match cloud Webex services

● Only calls that match the specified (comma separated) domains

*.ent-pa.com, *.ent2-pa.com

By selecting this option, the administrator configures specific domains which will be routed via Unified CM. If the administrator configures the enterprise domains ent-pa.com and ent2-pa.com, SIP URI internal calls will be routed through Unified CM. External domains, such as B2B calls, and Webex calls will be routed through Webex. This option achieves the benefit that business-to-business calls will not consume licenses on Expressway. The downside of it is that Unified CM will not have any control on business-to-business calls, and that the calling ID will match the Webex SIP Address instead of the Directory URI configured in Unified CM. This is shown in Figure 5-9.

Figure 5-9 Selected domains are routed through Cisco Unified CM



Called ID	Calling ID
bob@xyz.com	alice@example.call.webex.com

In this scenario, the administrator wants only internal domains (ent-pa.com and ent2-pa.com in the example) to be routed through Cisco Unified CM. Because Bob's domain is xyz.com, this call is not sent through Unified CM. Instead it is routed as a B2B call by Webex. The calling ID that Bob will see is alice@ent-pa.call.webex.com instead of alice@ent-pa.com, because Webex uses the Webex SIP Address and not the directory URI.

Encryption Settings

Both architectures for users and for devices support security. Signaling is secured by means of TLS, and media is encrypted using sRTP. There are, however, differences which will be detailed in the following paragraphs.

Webex Teams users

Any Webex Teams application registering to Unified CM is subject to the encryption policies specified in the Unified CM. Webex Teams application signaling and media traffic can be authenticated and encrypted through the newer OAuth-based method with Unified CM, applying the OAuth refresh token functionality to line-side SIP. This is the only option for Webex Teams, for both authentication and encryption, available with Cisco Unified CM release 12.5 or later.

For a comprehensive overview of security on Unified CM, including SIP OAuth, please refer to the Security chapter of the latest version of the *Preferred Architecture for Cisco Collaboration Enterprise On-Premises Deployments*, available at https://www.cisco.com/go/pa.

For further information on SIP OAuth, see the SIP OAuth Mode chapter in the *Feature Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Webex Devices

While the Webex Teams application is authenticated by Cisco Unified CM during registration, Webex devices do not register to Unified CM. Consequently, when a Webex device place a call to the enterprise it must be authenticated in a different way.

For this reason, SIP signaling between Webex and the enterprise network uses TLS with mutual authentication (MTLS). MTLS is part of the TLS specification, and like any TLS architecture it is client-server based, with the client initiating the connection request. In the case of the SIP connection from the Webex cloud to the enterprise, Webex acts as the client and Expressway-E as the server. With MTLS, both Webex and Expressway-E authenticate each other based on certificates. Specifically, for the DNS zone on Expressway-E used for calls from Webex, a **TLS verify subject name** is configured, and this needs to match the Common Name (CN) or a Subject Alternative Name (SAN) of the certificate presented by Webex to Expressway-E during the TLS handshake.

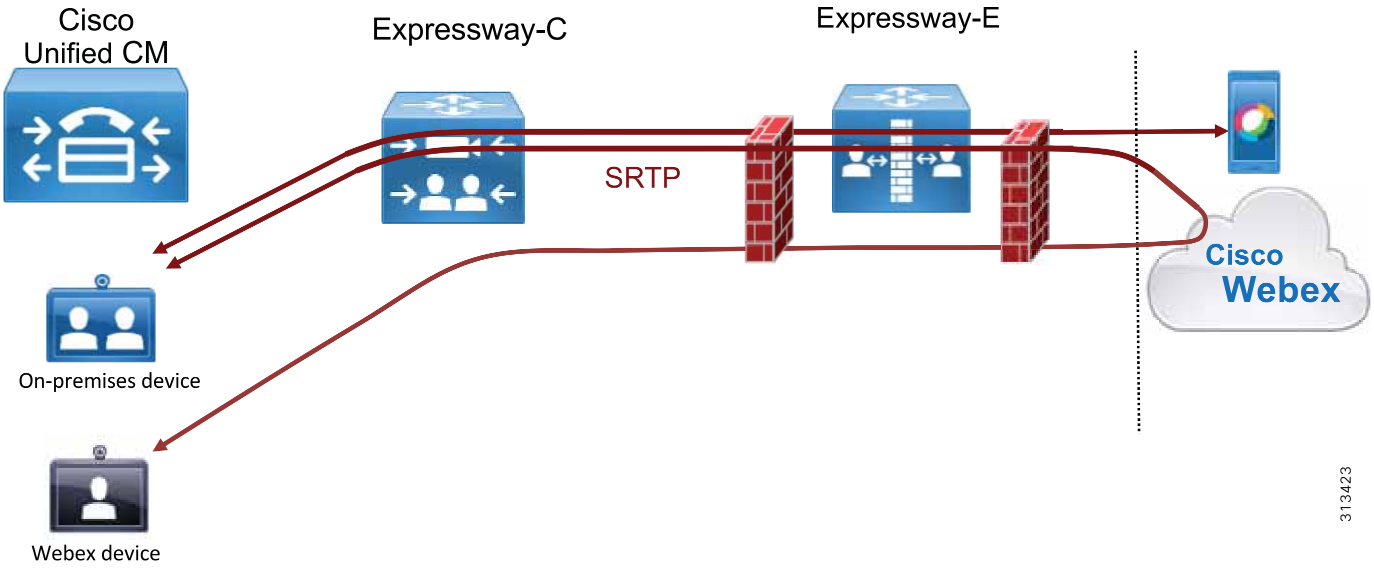
When a call is received by Expressway-E (the server side of the TLS handshake), Expressway-E requests a client certificate during the handshake which will be the Webex certificate. If the certificate is valid and the CN or one of the SANs matches what has been configured in the **TLS verify subject name** on Expressway-E, the call is treated as authenticated. Successful authentication requires that trust is established with the certificate authority (CA) that signed this certificate.

If authentication is not successful, this means that the certificate validation has failed. The call will thus enter into the Default Zone and will be routed according to the search rules provided for business-to-business scenarios, assuming business-to-business is configured on Expressway-E.

Device-terminated and Expressway-C terminated encryption

Webex Teams and Webex devices can achieve two levels of encryption: Expressway-C terminated and device-terminated encryption. With device-terminated encryption, traffic from the Webex Teams application or Webex device is encrypted all the way to the destination, as Figure 5-10 shows.

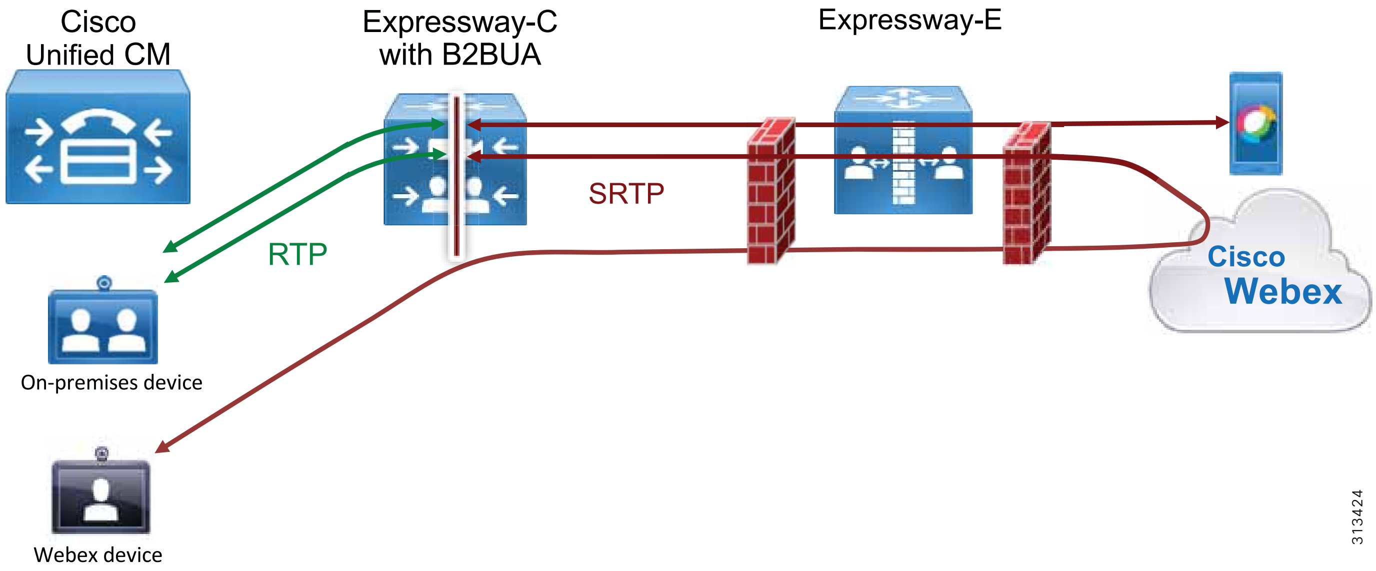
Figure 5-10 Device-terminated encryption



With Expressway-C terminated encryption, Cisco Unified CM uses non-encrypted traffic to Expressway-C, then Expressway-C terminates the RTP connection with the Unified CM endpoint and creates another call leg using SRTP to Webex. Any time Expressway performs RTP-to-SRTP conversion, it engages a back-to-back user agent (B2BUA). With Webex Teams, B2BUA is always engaged on Expressway-C. With Webex devices, B2BUA engagement is configurable. In this case we recommend enabling it on Expressway-C instead of Expressway-E so that the traffic in the DMZ will be encrypted.

Figure 5-11 shows Expressway-C terminated encryption, which involves B2BUA being engaged on Expressway-C

Figure 5-11 Expressway-C terminated encryption



Webex Teams with Expressway-C terminated encryption support the following two call flows:

- If both the parties, one of which is the Webex Teams user, are on-premises, the call will be sent in clear by Cisco Unified CM
- If the Webex Teams user is on the Internet, traffic from the Webex Teams application is encrypted between the Expressway-C and the Webex Teams application, and sent in clear between Expressway-C, Cisco Unified CM and the destination. This is shown in Figure 5-11.

Webex devices with Expressway-C terminated encryption support the following call flow:

- If one of the two parties is registered or trunked to Cisco Unified CM, such as a Unified CM room system or PSTN gateway, the Webex device traffic is sent in clear between the on-premises device and Expressway-C, and encrypted between Expressway-C and the Webex device. This is shown in Figure 5-11.

If device-terminated encryption for Webex Teams users is required, SIP OAuth feature must be turned on. SIP OAuth does not require mixed mode on Cisco Unified CM. If it is important that encryption is achieved not only between Webex Teams users, but also between Webex Teams users and Cisco Unified CM registered devices, mixed mode must be turned on, as other Cisco Unified CM devices do not support SIP OAuth.

Expressway-terminated encryption doesn’t require mixed mode on Cisco Unified CM, nor SIP OAuth.

Deployment Overview

This section describes the high-level steps required for deploying Webex Hybrid Call Service.

Few important considerations apply when Webex Teams (Unified CM) traffic is co-resident on the same Expressway pairs as hybrid Webex devices and expressway B2B traffic.

Expressway-C and Expressway-E on a Shared Deployment

If calls generated by Webex Teams applications and devices use the same Expressway that is co-resident with business-to-business calls, it is important to allow PSTN access to Webex devices and Webex Teams applications while blocking business-to-business users from unauthorized access of PSTN and other internal-only services.

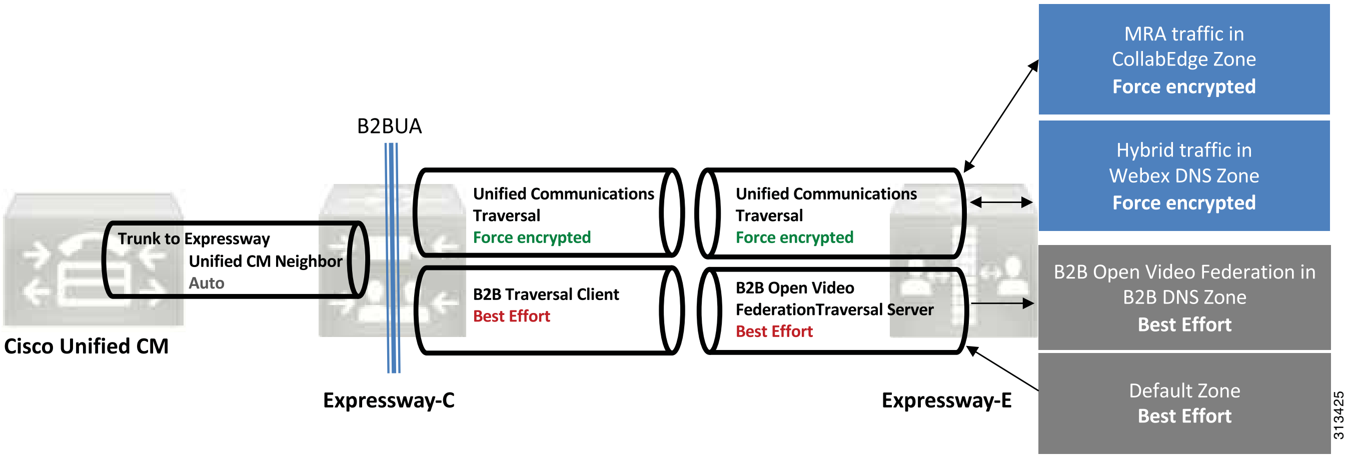
Standard business-to-business calls from other companies enter the Default Zone because these connections, even if they are configured for MTLS, will not present a certificate matching the TLS verify name configured on the Expressway-E DNS zone used for Webex. Therefore, we recommend configuring the Default Zone as non-authenticated. Call Processing Language (CPL) rules controlling access to the corporate network will thus be applied only to non-authenticated traffic, and Webex device calls will bypass the control check of non-authenticated traffic on Expressway and will be routed to the enterprise Unified CM for call anchoring.

For an explanation on how authentication works with CPL rules, refer to the CPL information in the latest version of the Cisco Collaboration 12.x Enterprise On-Premises Deployments CVD guide, available at https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/12x/120/collbcvd/edge.html#pgfId-1080298.

It is possible to use a single traversal zone between Expressway-E and Expressway-C for business-to-business calls, Webex device calls, and mobile and remote access. However, separating traversal zones by traffic type will optimize consumption of resources on Expressway. As an example, using the same traversal zone for mobile and remote access (MRA) traffic together with Webex traffic preserves resources because they share the same encryption setting (**Force encrypted**), and this optimizes the engagement of the back-to-back user agent (B2BUA). However, the business-to-business traffic encryption policy might be different. A dedicated traversal zone for business-to-business traffic would prevent multiple engagements of the B2BUA on both Expressway-C and Expressway-E.

While Webex Teams application traffic uses the MRA traversal zone by design, we recommend using the same MRA traversal zone (called **Unified Communications traversal zone** on Expressway) for Webex device traffic as well, and a separate traversal zone for business-to-business (B2B) traffic, as shown in Figure 5-12.

Figure 5-12 Separate Traversal Zone for Business-to-Business (B2B) Traffic



Traversal zones do not require any inbound port to be opened on a DMZ firewall; but if the corporate security policies block outbound access by default, then an outbound port has to be opened in the firewall for every new traversal zone. In this rare case, it is possible to use the Unified Communications traversal zone for all traffic types. Although supported, this deployment has some limitations, and it always engages the B2BUA on Expressway-E unless all business-to-business communications use encryption.

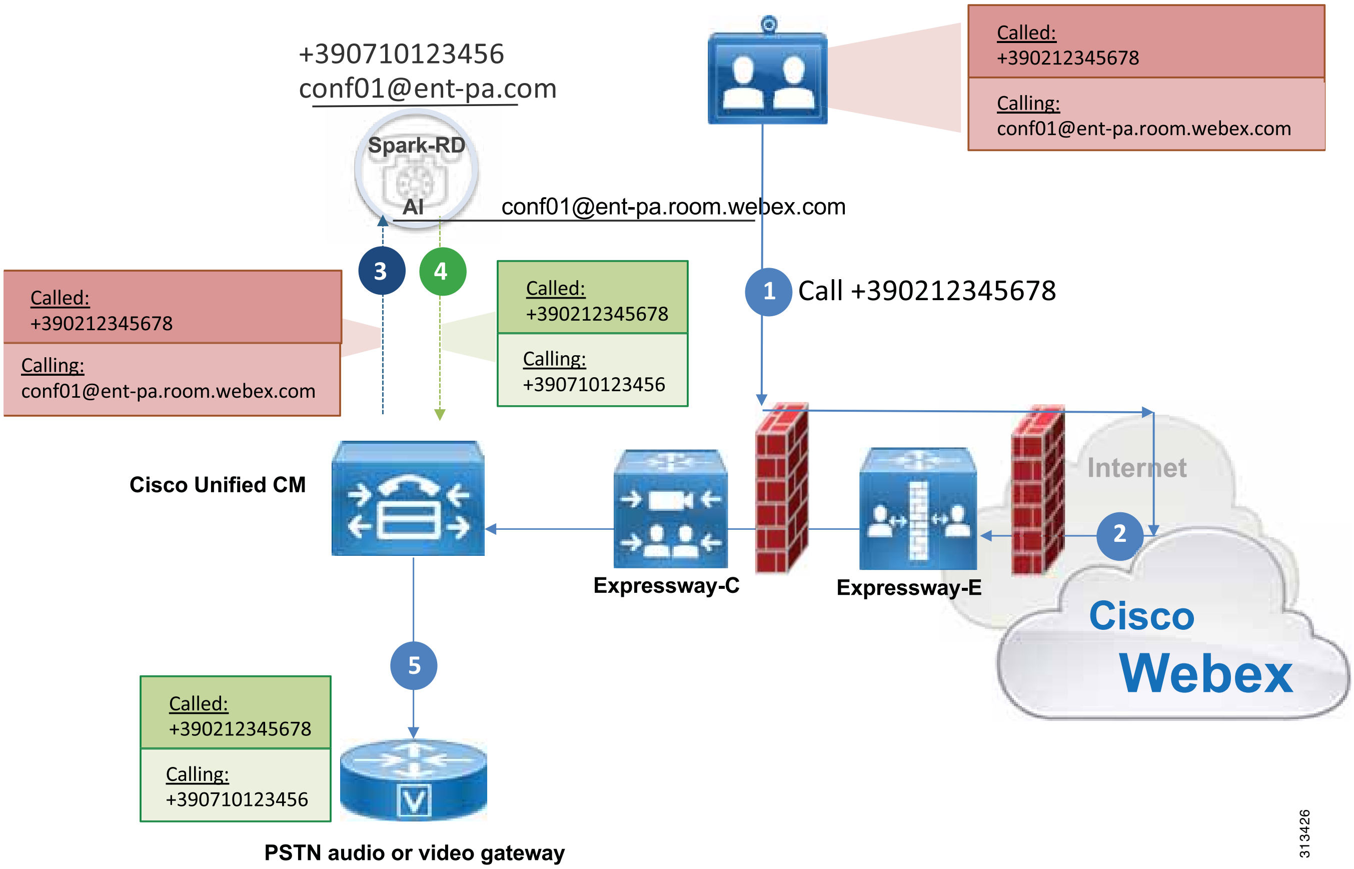
Caller ID and Class of Service

When a Webex device enabled for hybrid calling calls a Cisco Unified CM endpoint or a PSTN destination, the desired behavior is to present the calling device ID as configured in the Spark RD line.

When the call leaves Webex, the caller ID is set to the Webex SIP address of the calling Webex device, such as conf01@ent-pa.rooms.webex.com. Because this address matches the associated identity configured in the Spark RD simulating the calling Webex device, the call is anchored on the Spark RD and then routed as if it originated from this device. This also sets the caller ID for the outgoing call leg to the enterprise identity (directory number and directory URI) of the calling Webex device.

In the example in Figure 5-13, the Webex device user dials a PSTN number. In this case the Request URI of the call leg is set to <number> @ <CFQDN>, where CFQDN is the Cluster Fully Qualified Domain Name of the Cisco Unified CM cluster. This call is sent to Expressway to route the call to the Unified CM where the Spark RD for that device is configured. The CFQDN for every device enabled for hybrid calling is pushed to Webex by the Device Connector at provisioning. After the call is anchored on the calling device's Spark RD, it follows the standard routing behavior of Unified CM. The call is routed according to the numeric call routing logic of Unified CM because the host portion (right hand side) of the Request URI matches a CFQDN configured on Unified CM. On the initial call leg to the enterprise, the caller ID is set to Webex room SIP address conf01@ent-pa.rooms.webex.com. Because the Webex room SIP address matches the associated identity set in the Spark RD, this call is identified as belonging to the device on Unified CM and is forwarded to the final destination as if it originated from the Spark RD directory number. Therefore, Spark RD caller ID and the calling search space as set in Unified CM will be used instead. This is shown in Figure 5-13 where steps 3 and 4 indicate logical processes inside Unified CM and not call legs.

Figure 5-13 Call Anchoring and Caller ID

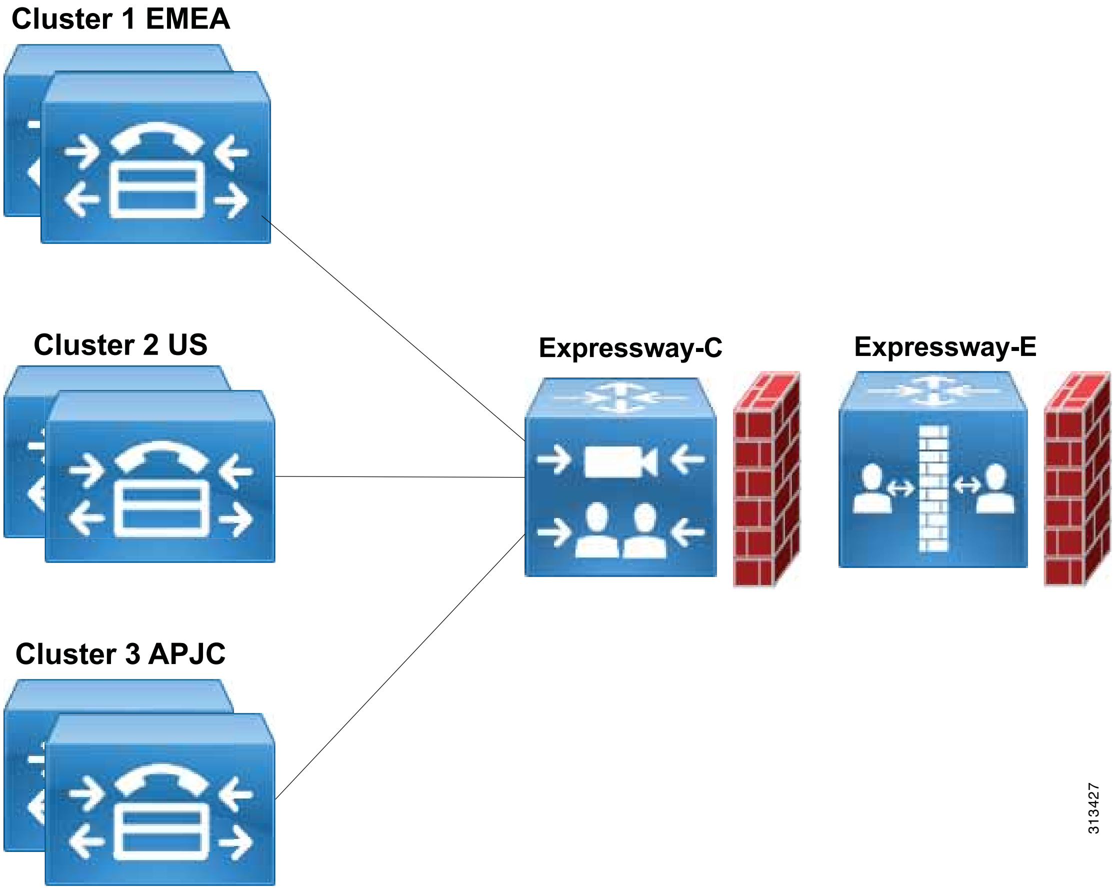


Call anchoring based on a successful match between caller ID and remote destination is a mobility feature and happens independently from the dialed destination.

Deployment Considerations for Multiple Unified CM Clusters

Webex Hybrid Calling supports multiple Cisco Unified Communications Manger clusters. In this case, Expressway-C can be associated to every cluster, as shown in Figure 5-14.

Figure 5-14 Expressway-C Supporting Multiple Unified CM Clusters



Webex Teams application with multiple Unified CM Clusters

When multiple clusters are deployed, Webex Teams application register to the correct cluster based on the user's home cluster settings. A full explanation is covered in the Preferred Architecture CVD for Cisco Collaboration, here available:

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/12x/120/collbcvd/control.html

Webex devices with multiple Unified CM Clusters

When multiple clusters are deployed, the incoming call from a Webex device has to be routed to the Unified CM cluster where the Spark RD for that Webex device resides so that call anchoring can be performed. This way it will be possible to correctly set the calling device enterprise caller ID configured in the Spark RD and apply the class of service for that Webex device. This is known as home cluster-based routing. With home cluster-based routing, the call is always anchored to the Unified CM of the calling device.

When Webex sends a call to the Expressway-E, it populates both the SIP Request URI and the Route Header. Even though the following considerations and examples apply to multiple Unified CM clusters, the use of the Route Header is a general concept and also applies to single-cluster deployments.

When both a Request URI and a Route Header are present in a SIP INVITE, the Route Header takes precedence in the routing processes. As an example, when a Webex device with Spark RD configured on the US cluster dials a device in the EMEA cluster, Expressway-E receives this INVITE, which includes *us-cm-pub.ent-pa.com* as Route Header.

```
INVITE sip:1234@us-cm-pub.ent-pa.com SIP/2.0 Via: SIP/2.0/TLS
198.51.100.22:5062;branch=z9hG4bK-393139-4880f133ef84798fb3625da14a87ad32 Call-ID:
87c778d0a17c9a3a93ef90ff530fda50@30.30.30.30 CSeq: 1 INVITE Contact: "l2sip"
<sip:l2sip@198.51.100.22:5062;transport=tls>;call-type=squared From: "conf_room01"
<sip:conf_room01@ent-pa.rooms.webex.com>;tag=1381736467 To:
<sip:1234@us-cm-pub.ent-pa.com> Max-Forwards: 70 Route:
<sip:l2sip@198.51.100.22:5062;transport=tls;lr>,<sip:us-cm-pub.ent-pa.com;lr>
```

When a Webex device has a Spark RD configured on the EMEA cluster and dials the same number, the INVITE has a different Route Header:

```
INVITE sip:1234@us-cm-pub.ent-pa.com SIP/2.0 Via: SIP/2.0/TLS
198.51.100.22:5062;branch=z9hG4bK-393139-4880f133ef84798fb3625da14a87ad32 Call-ID:
87c778d0a17c9a3a93ef90ff530fda50@30.30.30.30 CSeq: 1 INVITE Contact: "l2sip"
<sip:l2sip@198.51.100.22:5062;transport=tls>;call-type=squared From: "conf_room02"
<sip:conf_room02@ent-pa.rooms.webex.com>;tag=1401736467 To: <sip:1234@us-cm-pub.ent-pa.com
> Max-Forwards: 70 Route:
<sip:l2sip@198.51.100.22:5062;transport=tls;lr>,<sip:emea-cm-pub.ent-pa.com;lr>
```

This time Expressway routes the call based on the destination included in the Route Header *emea-cm-pub.ent-pa.com*, and thus the INVITE is sent to the EMEA Unified CM by Expressway-C.

Webex populates the Route Header based on the information received by the Device Connector and specifically taken from the Unified CM Cluster Fully Qualified Domain Name (CFQDN) enterprise parameter. Specifically, if multiple values are present in the CFQDN enterprise parameter, then the first value is considered. Using this mechanism, Webex creates associations between users and their respective CFQDNs. When a call is sent from Webex, the dialed destination (URI or numeric destination) of the call is used to populate the INVITE Request URI, and the home cluster of the calling user populates the Route Header, as illustrated in Figure 5-15.

Figure 5-15 Cluster Fully Qualified Domain Name (CFQDN)

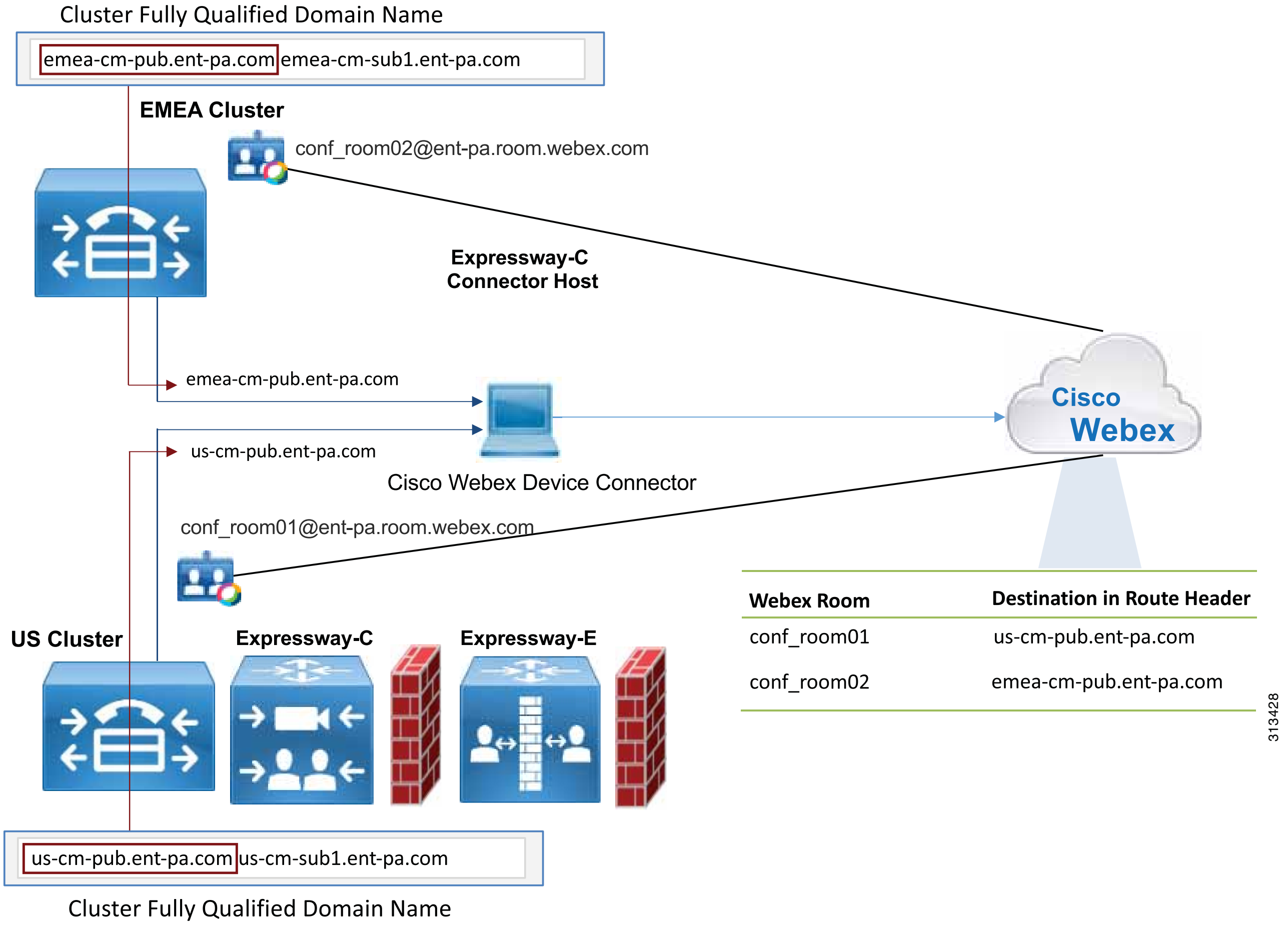


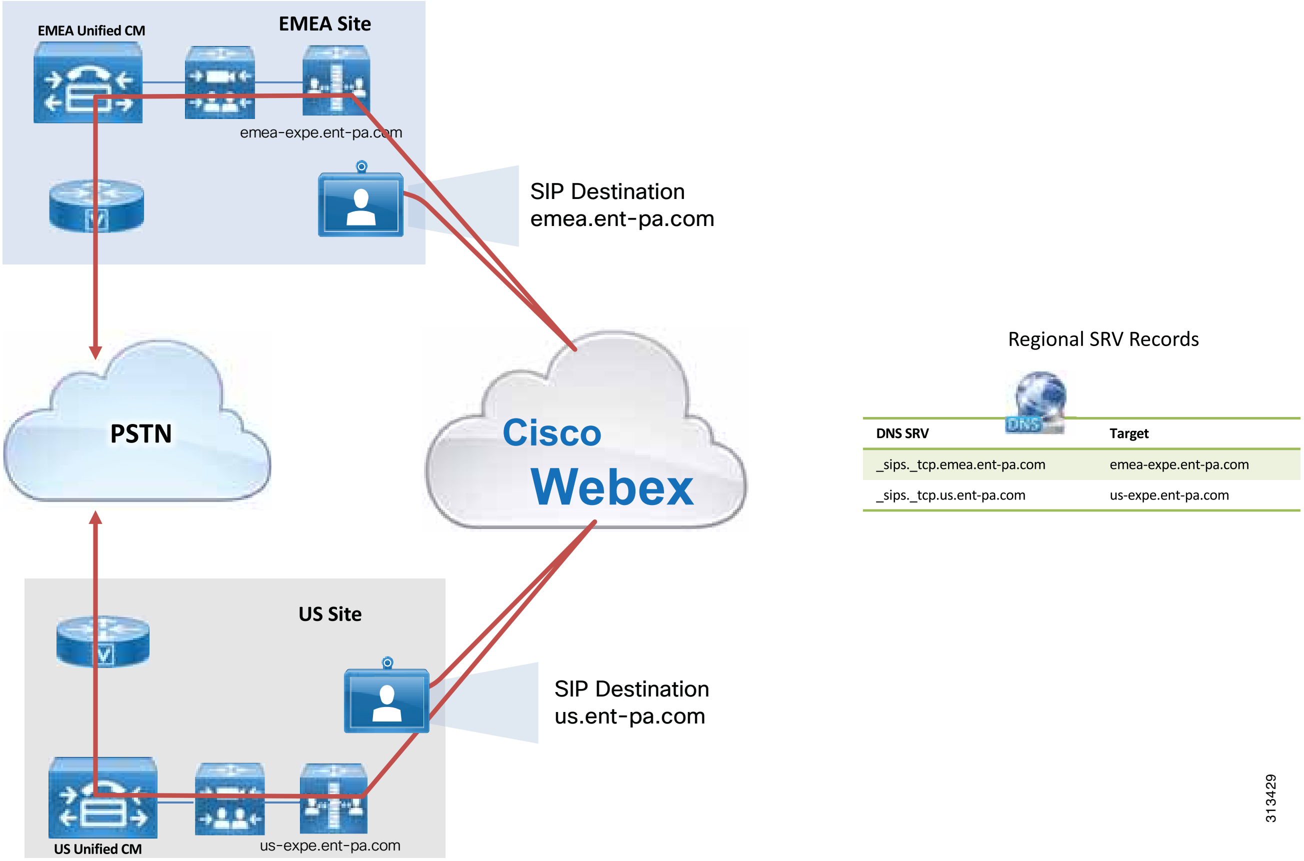
Figure 5-15 shows two Webex device with Webex SIP Addresses *conf_room01@ent-pa.rooms.webex.com* located in US, and *conf_room02@ent-pa.rooms.webex.com* located in EMEA. The Device Connector takes the CFQDN for those two devices and sends this information to Webex.

Deployment Considerations for Multiple Expressway Clusters

When multiple Expressway clusters are deployed, the administrator can granularly select the Expressway-E cluster a Webex device will use in order to minimize the distance between Webex and the Expressway, thus improving call quality. As an example, if a Webex device in US dials a PSTN number, it is desirable that the call enters the Expressway-E in US, and uses the PSTN gateway in US. In order to achieve this, a SIP destination for that room will be configured. This SIP destination will override the default SIP destination that is configured for the organization. That destination resolves through DNS SRV into the Expressway-E cluster in US. The same will be configured for other regions. The following picture illustrates this scenario.

When the Webex device in US dials a PSTN number, Webex will use the SIP destination associated to that device and configured in Cisco Webex Control Hub to perform a DNS SRV query, which will resolve to Expressway-E in US. This way, the path between Webex and the Expressway will be minimized. The following picture illustrates the paths to the PSTN for a regional installation.

Figure 5-16 Multiple Expressways: media paths to the PSTN

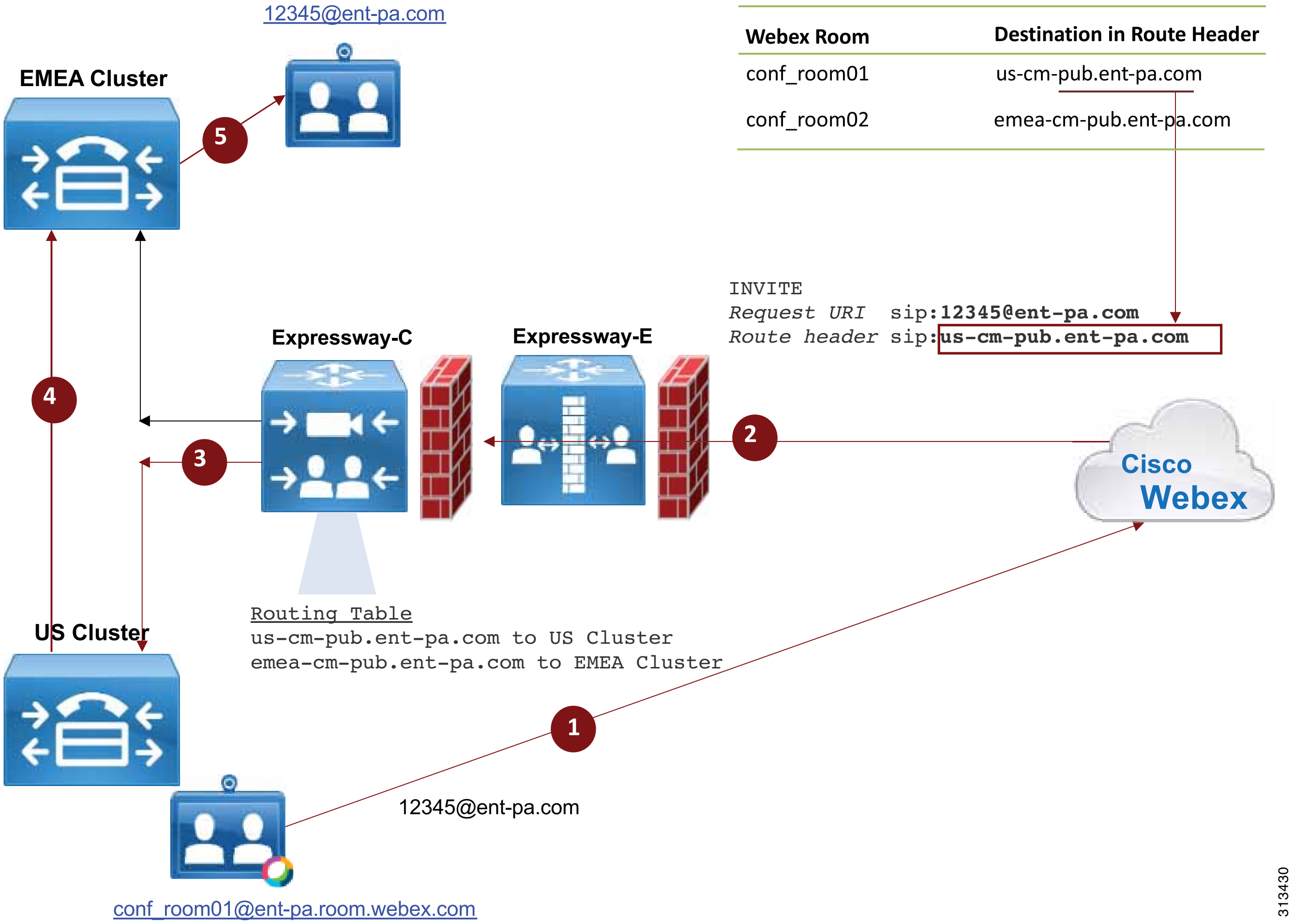


DNS SRV	Target
_sips._tcp.emea.ent-pa.com	emea-expe.ent-pa.com
_sips._tcp.us.ent-pa.com	us-expe.ent-pa.com

Expressway Routing Setup for Hybrid Webex Devices

Expressway-C therefore has to be provisioned with search rules to route the call to the correct Cisco Unified CM cluster based on the Route Header, as shown in Figure 5-14.

Figure 5-17 Call Routing Based on Route Header



Webex Room	Destination in Route Header
conf_room01	us-cm-pub.ent-pa.com
conf_room02	emea-cm-pub.ent-pa.com

```
INVITE
Request URI  sip:12345@ent-pa.com
Route header sip:us-cm-pub.ent-pa.com
```

```
Routing Table
us-cm-pub.ent-pa.com to US Cluster
emea-cm-pub.ent-pa.com to EMEA Cluster
```

First, Expressway-E receives this call on the Webex DNS Zone enabled for TLS with mutual authentication. The Webex DNS Zone, Webex traversal client, and traversal server zone must be enabled for route header support or else the call will be dropped.

In this case, the Route Header will be *us-cm-pub.ent-pa.com*.

Expressway-E considers the presence of route headers when routing the call; and since the route header takes precedence over the Request URI, the routing process will analyze *us-cm-pub.ent-pa.com* instead of *1234@us-cm-pub.ent-pa.com* in our example.

For the scenario in Figure 5-17, two search rules are built on Expressway-C: the first matches calls with destination *us-cm-pub.ent-pa.com* and sends them to Unified CM in the US cluster, and the second matches calls with destination *emea-cm-pub.ent-pa.com* and sends them to Unified CM in the EMEA cluster.

With multiple clusters, each CFQDN must be unique for home cluster-based routing to work properly, as shown in Figure 5-16 and Figure 5-17.

Figure 5-17 shows the following actions:

1. Webex device us_conf01 starts a call to a device configured in EMEA Unified CM by dialing 12345.

2. The call is extended to Expressway-E and Expressway-C.
3. Based on the route header, the call is sent to the Unified CM cluster in the US.
4. The call is first anchored on the Unified CM US cluster and then sent to the destination in the Unified CM EMEA cluster.

Starting with Unified CM release 12.0, Cisco Unified CM also can be configured to route calls based on the SIP route header. This allows support for Cisco Unified CM Session Management Edition (SME) architectures.

If Expressway-C and Expressway-E run Webex Hybrid Calling but no business-to-business traffic, it is important to reject any SIP message not generated by Webex. This is referred to as a *dedicated deployment*. A dedicated deployment uses Expressway's SIP signaling and media for Webex Hybrid Services only, and not for business-to-business traffic.

Cisco Expressway 8.9.1 and later releases permit the creation of Call Processing Language (CPL) rules to mitigate fraudulent call attempts. We highly recommend deploying Expressway 8.9.1 or a later release for toll fraud mitigation.

If business-to-business traffic is not included in the same Expressway, and because this traffic enters from the Default Zone, a CPL rule blocking any access to the Default Zone will prevent fraudulent access to Expressway-E. See the Deployment Process paragraph for further details.

Toll Fraud and Identity Theft Mitigation on a Shared Deployment

If Expressway-E allows business-to-business traffic together with hybrid call traffic, this is referred to as a *shared deployment*. For shared deployments, it is important to set up rules to minimize toll fraud attempts on Expressway-E. As a first step, the rules should determine if the calling ID is legal and should ensure that is does not contain an IP address of Expressway itself, the enterprise SIP domain, or the enterprise Webex Teams SIP address domain. Then the rules should analyze the called alias, preventing access to protected resources such as the PSTN gateway. See the *Webex room hybrid calling deployment* in Deployment Process for further details.

The administrator might want to block +E.164 aliases coming through the Default Zone, other forbidden destinations, or protected services. The PSTN can also be accessed through different escape codes. In those scenarios, the rules need to be customized.

Also, the Authentication Policy in the Default Zone has to be set to **do not check credentials**, and the SIP authentication trust mode in the Webex DNS Zone must be set to **On**, while the Authentication Policy in the traversal client and server zone must be set to **check credentials**. In this way, traffic coming from the Default Zone and containing the Webex Teams SIP domain will be marked as unauthenticated and will thus be rejected by the rules. Legal traffic from the Default Zone will be sent to Unified CM as unauthenticated (P-Asserted-Identity Header stripped off), while traffic from Webex will be delivered to Unified CM as authenticated (P-Asserted-Identity Header preserved).

Toll Fraud and Identity Theft Prevention on Cisco Unified CM

As a second line of defense, Cisco Unified CM 12.0 and later releases have the ability to distinguish between a trusted and untrusted identity. This is done through a parameter available on the SIP trunk called **Trusted Received Identity**. If this parameter is set to **Trust PAI Only**, Cisco Unified CM will not anchor any call received from that trunk if PAI is not present. Because Expressway-E trusts PAI only if the call has been previously authenticated through MTLS and the certificate clearly shows that the call is coming from Webex, the absence of PAI means that the call is coming from a different destination. In this case the call will not be anchored, and as a consequence the calling search space of the trunk will be used instead of the calling search space of the line of the anchored identity. Because calling search spaces of Expressway-C trunks should not include PSTN access, this will prevent any fraudulent attempt to access PSTN gateways and any identity theft attempt.

High Availability

Webex Hybrid Calling and Webex Teams calling through Unified CM will be highly available if Cisco Unified CM and Cisco Expressway are deployed in a cluster. High availability is covered in the Enterprise Preferred Architecture CVD, and specifically in Call Control and Collaboration Edge sections.

Deployment Process

Webex Teams (Unified CM) Deployment

For a detailed process for deploying Calling in Webex Teams (Unified CM) refer to the Deployment Guide for Calling in Webex Teams (Unified CM), available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/ucmcalling/unified-cm-wbx-teams-deployment-guide/unified-cm-wbx-teams-deployment-guide_chapter_010.html

1. Associate a Service Profile to the user. This profile is assigned to Webex Teams with Unified CM calling users, in order to enable Webex Teams users for CTI
   a. Create a Service Profile
   b. Create CTI UC Service
   c. Associate the CTI UC Service to the Service Profile
   d. Associate the Service Profile to the user so the user inherits CTI control capability.
2. Create DNS SRV records for service discovery. A detailed description is found in this document: Service Discovery chapter of the Planning Guide for Cisco Jabber, available here: https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html
   a. This involves creating a split DNS environment. For the domain ent-pa.com:
      - collab-edge._tls.ent-pa.com in the public DNS
      - cisco-uds._tcp.ent-pa.com in the internal DNS
3. In order to enable SAML Single-Sign-On, see the SAML SSO Deployment Guide for Cisco Unified Communications Applications avaliable at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

   For cloud (Webex Control Hub) configuration, see Single Sign-On Integration With Webex Control Hub at: https://help.webex.com/en-us/lfu88u/Single-Sign-On-Integration-in-Cisco-Webex-Control-Hub
4. In order to enable LDAP authentication and synchronization, see the Preferred Architecture for Cisco Collaboration Enterprise CVD, Call Control section, Architecture subsection, LDAP paragraphs: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/PAdocs.html#pgfId-92068
5. Configure users for Webex Teams applications on Unified CM:
   a. On Unified CM, check that the user’s details include the mail ID. This is an important step as the mail ID is the unique identifier in Webex.

   b. On Unified CM, associate a directory URI to the user's directory number.
   c. Check the home cluster checkbox for users who are configured on that specific Unified CM cluster
   d. Ensure that the Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile) option is not checked. Webex Teams messaging is used instead.
   e. Apply the previously configured UC Service Profile
   f. Enable CTI for the user
   g. Create a Webex Teams softphone device using the Cisco Unified Client Services Framework (CSF), Cisco Dual Mode for Android, Cisco Dual Mode for iPhone, or Cisco Jabber for Tablet device type, depending on the platform in use (PC/Mac, Android, iOS, tablets)
   h. Add a Directory Number for the device
   i. Associate the device to the user

6. On Unified CM, check that enterprise parameter Cluster Fully Qualified Domain Name is configured. Make sure that the first value in the space separated list is not a wildcard.
7. If encryption is required for on-premises call legs, enable SIP OAuth. A description is found in the Preferred Architecture CVD, Security section, available at https://www.cisco.com/go/pa. For further information on SIP OAuth, see the SIP OAuth Mode chapter in the Feature Configuration Guide for Cisco Unified Communications Manager at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
8. Set Calling Behaviour in Webex Control Hub: if Hybrid Call Service is enabled for users, disable it. Select Calling in Webex Teams (Unified CM)
9. Setup Expressway-C and Expressway-E for Mobile and remote access following the Mobile and Remote Access through Cisco Expressway Deployment Guide: https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

Webex Devices Deployment

For Webex device hybrid calling deployments follow these steps:

1. On Unified CM, configure a local user for the Webex device. You don’t need to create a user in the LDAP corporate directory.
   a. Specify the userID and Last Name
   b. Specify a Telephone Number
   c. Setup a directory URI
   d. Specify the mail ID. This attribute has to match the mail ID that will be configured in Webex Control Hub for that room
   e. Check the home cluster checkbox
2. On Unified CM, configure a Spark Remote Device (RD) for each Webex device.
   a. On Unified CM, set the Spark RD directory number. This is the extension that Unified CM will use to route the call to destination. Set up calling search space(s) and partition(s) as appropriate.
3. On Unified CM, associate the Spark RD to the local user account and specify the primary extension

4. On Expressway-E, set up a new DNS Zone for Webex Teams.
5. On Expressway-E, configure the DNS Zone for TLS with mutual authentication on a dedicated port (for example, port 5062). First enable port 5062 for MTLS globally under Configuration -> Protocols -> SIP, then set the Default Zone parameter Enable Mutual TLS on Default Zone to off. This will allow MTLS on port 5062 while continuing to support TLS with port 5061. If port 5062 must be used, make sure this port is open on the firewall.
6. On Expressway-E enable the Route Header support for this zone by setting the SIP parameter preservation to On (otherwise an INVITE containing a route header will not be processed), and set the SIP authentication trust mode to On.
   b. Make sure that the Authentication policy in the Default Zone is set to do not check credentials.
7. On Expressway-E re-use the existing MRA traversal zone (called Unified Communications Traversal) for Webex Teams users
   a. Enable Route Header support
   b. Set the Authentication policy to check credentials.
8. On Expressway-E create a search rule matching any call with a domain portion that includes *<subdomain> .rooms.webex.com* and with the destination set to the DNS Zone, such as:

   Mode: Alias pattern match Pattern

   Type: Regex

   Pattern String .*@ent-pa\.rooms\.webex\.com
9. On Expressway-E, create a search rule specifying that anything received from the Cisco Webex DNS Zone must be sent to the Cisco Webex Traversal Server Zone (or to Unified Communications Traversal):

   Source Zone:

   Named Source Name: Cisco Webex DNS Zone

   Mode: Any alias

   Target: Cisco Webex Traversal Server Zone
10. On Expressway-E, create the CPL rules as described for toll fraud and identity theft mitigation in the section on Deployment Considerations for Multiple Unified CM Clusters and as illustrated by the examples in the following tables:
    a. Dedicated Expressway

Source Type	Originating Zone	Destination Pattern	Action
Zone	Default Zone	.*	Reject

    b. Deployment shared with B2B

    The following rules block calls from the Expressway-E Default Zone that contain the Webex Teams SIP domain ent-pa.call.ciscospark.com, the corporate domain ent-pa.com, or the IP addresses of Expressway-E (198.51.100.22 and 198.51.100.23 in the example) in the calling alias.

Rule	Source Type	Rules Apply to	Source Pattern	Destination Pattern	Action
1	From Address	Unauthenticated Callers	.*@example\.rooms\.webex\.com.*	.*	Reject
2	From Address	Unauthenticated Callers	.*@example\.com.*	.*	Reject
3	From Address	Unauthenticated Callers	.*@198\.51\.100\.(22|23)	.*	Reject

The following CPL rules are used to screen the called destinations. These rules block calls with a leading 0 or 9 (calls to the PSTN), allow calls if they contain the corporate domain in the called alias, and block all other calls.

Rule	Source Type	Originating Zone	Destination Pattern	Action
1	Zone	Default Zone	[0|9]\d*(@.*)?	Reject
2	Zone	Default Zone	..*@example\.com.*	Reject
3	Zone	Default Zone	.*	Reject

Note The order of these rules is important because Expressway-E analyzes them top-down.

11. On Expressway-C:

- **a.** Re-use the existing MRA traversal zone (called Unified Communications Traversal).
- **b.** Enable Route Header support and SIP parameter preservation to preserve the Contact Header, so that Webex is able to detect the loops.
- **c.** Set the Authentication policy to check credentials.

12. On Expressway-C:

- **a.** Configure a neighbor zone to Unified CM for hybrid calling, different from the neighbor zone used for business-to-business calls.
- **b.** If mobile and remote access is configured on the same Expressway-C server, set the port to a value different than 5060 and 5061, such as 5560 or 5561.
- **c.** Enable Route Header support if the call will be sent to Unified CM SME 12.0.1 or later release. This step is not relevant for deployments where transit nodes are not used.
- **d.** The neighbor zone should be configured with a custom zone profile. In the custom zone profile, the SIP Parameter preservation should be set to On.
- **e.** For further information on how to set up the Unified CM zone, refer to the latest version of the Cisco Expressway and CUCM via SIP Trunk Deployment Guide, available at http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

13. On Expressway-C, create a search rule matching any call with a domain portion that includes <subdomain> .rooms.webex.com and with a destination set to the Webex traversal client zone or to the Unified Communications Traversal zone:

Mode: Alias pattern match Pattern Type: Regex Pattern String:.*@example\.call\.ciscospark\.com

14. On Expressway-C, create as many search rules as there are Unified CMs deployed with hybrid services users. Those search rules must match the Unified CM CFQDN, and the destination must be set to the corresponding Unified CM neighbor zone. The following two rules address two regional Unified CM clusters:

    Rule name: Calls to US UCM

    Mode: Alias pattern match

    Pattern Type: Prefix

    Pattern String: us-cm-pub.ent-pa.com

    Target: US-UCM neighbor Zone

    Rule name: Calls to EMEA UCM

    Mode: Alias pattern match Pattern

    Type: Prefix

    Pattern String: emea-cm-pub.ent-pa.com

    Target: EMEA-UCM neighbor Zone

15. On Unified CM, create a SIP Trunk Security Profile with a listening port set to match what has been configured in step 12b (for example, 5560 or 5561, in case security is turned on).

16. On Unified CM, create a SIP trunk linked to the security profile created in step 15, and point it to the Expressway-C. Include the SIP trunk in a route group and a route list.

17. On Cisco Unified CM, create a SIP route pattern (if not present) to route the domain *.webex.com to the Expressway-C, and specify the previously created route list as the target.