CHAPTER 5

Cisco Webex Hybrid Call Service

Revised: May 31, 2019

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 or Cisco Hosted Collaboration Solution (HCS) as the hosted enterprise call control.

Note Please be aware that the Webex Hybrid Call Service architecture discussed in this document is currently going through a transitional phase. To better understand the future changes and how they will impact your deployment of the Webex Hybrid Services architecture, we recommend that you contact your Cisco account team before deploying the architecture described in this document.

Overview

Webex Hybrid Call Service is based on Call Connector. This service enables Webex Teams users to make and receive calls on their Webex Room Device or Webex Teams application using the same dialing procedures as with endpoints registered with Cisco Unified CM or Hosted Collaboration Solution (HCS).

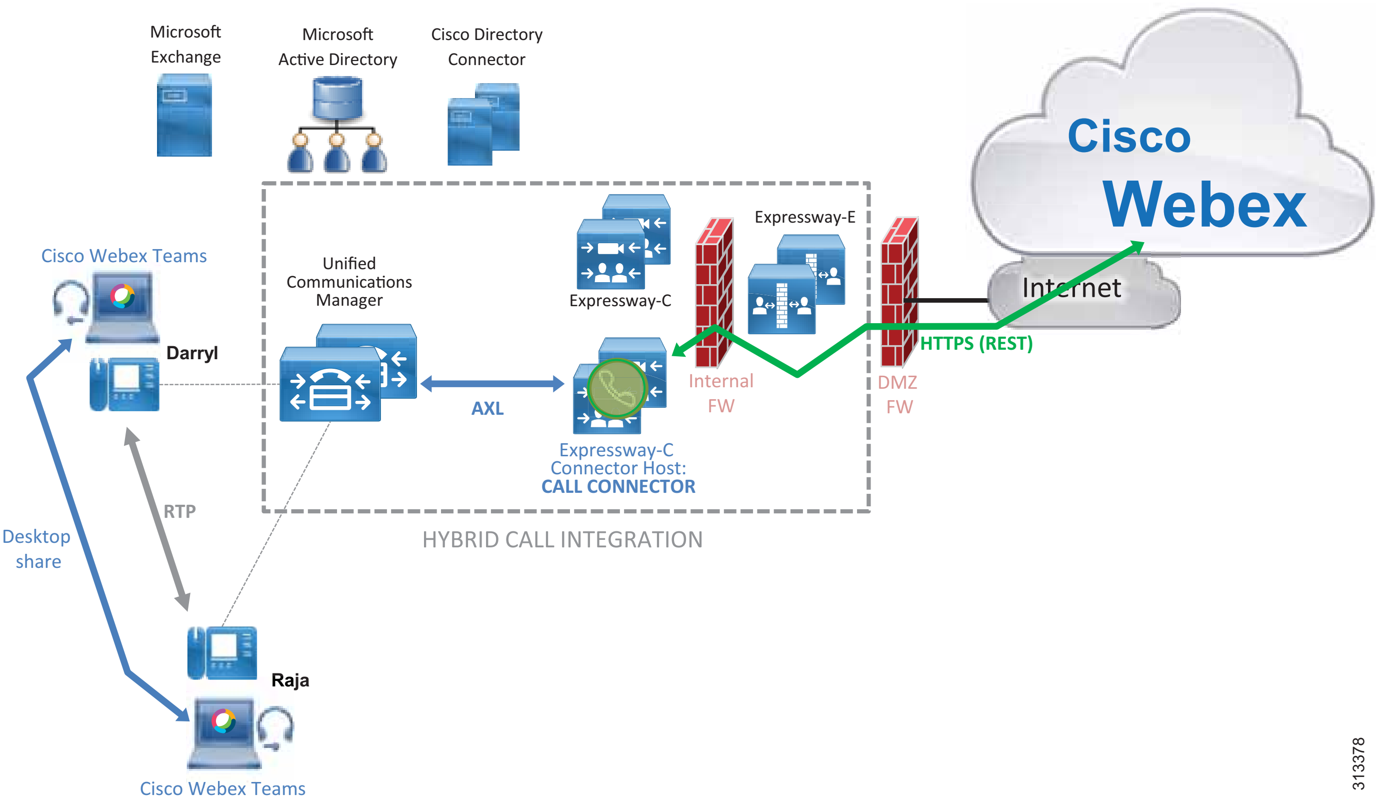
Core Components

- Cisco Expressway-C runs the Call Connector.
- Cisco Expressway-C and Expressway-E provide firewall traversal for SIP signaling and media.
- Cisco Unified Communications Manager (Unified CM) or Hosted Collaboration Solution (HCS) provides call control.

Recommended Deployment

The Hybrid Call Connector runs on the Cisco Expressway-C host and connects on one side to Unified CM via Administrative XML (AXL). This provides Call Connector with access to Unified CM provisioning. On the other side, the Call Connector uses HTTPS to communicate with Webex. (See Figure 5-1.) This connection traverses through the customer's Internet edge firewall and does not use the Expressway-E and Expressway-C firewall traversal setup.

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



When a user in Webex is enabled for Hybrid Call Service, the Call Connector uses the AXL interface to find devices associated with that user on Unified CM and adds specific configuration, such as a Spark Remote Device (if configured for automatic Spark Remote Device provisioning) and the associated remote destination, called the *Associated Identity*. Call Connector does not participate in call setup or tear-down.

If a user has an endpoint registered to Cisco Unified CM and also has a Webex Teams application, both the endpoint and the Webex Teams application will receive calls regardless of whether the call is initiated by another Webex Teams application, by a Unified CM registered device, or by a Unified CM associated IP or PSTN gateway. Call Service Connect not only enables dual ringing on Webex Teams applications, including Webex Room Devices and Cisco Unified CM endpoints, but also allows Webex Teams users to place calls using enterprise dialing habits from their Webex Teams applications.

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 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:

- Automatic provisioning of meetings
- Firewall traversal architecture for signaling and media, which increases security by minimizing the need to open outbound ports in the internal firewall
- Secure signaling and media encryption based on public certificates with mutual authentication

Architecture

Call Service Connect enables dual ringing for Webex Teams and Cisco Unified CM devices associated with the same user. In addition, it keeps the user experience consistent so that the user of Webex Teams has the same dialing habits, calling ID, and unified call history as any other user on Cisco Unified CM.

In order to achieve all of this, the Cisco Unified CM administrator must configure a Cisco Spark Remote Device for every user's primary extension. The administrator can configure the Call Connector to create the Spark Remote Device automatically, with the limitation that parameters such as device pool, calling search space, location, and reroute calling search space will be shared between all the Spark Remote Devices.

Webex Teams SIP Address and Enterprise URI

Once the Cisco Spark Remote Device is configured, Call Connector will automatically configure associated identities (formerly called remote destinations) associated with the Spark Remote Device on Cisco Unified Communications Manager in order to allow simultaneous ring functionality between Webex Teams applications and Unified CM devices.

As an example, if the user bob@ent-pa.com is provisioned for Call Service Connect, the Call Connector will add an associated identity to the Spark Remote Device of this user via the Unified CM AXL API. The associated identity will be in the form:

*<userID>***@***<subdomain>***.call.webex.com**

For example: bob@ent-pa.call.webex.com (see Figure 5-2)

Where *<userID>* is the attribute uniquely identifying the user in the 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.

When a user is provisioned for Call Service Connect, Webex via the Call Connector learns the user's enterprise URI from the Directory URI defined for the user in Unified CM. This information is pushed to Webex.

Each user has two addresses:

- Enterprise URI — It matches the Directory URI on Cisco Unified CM (bob@ent-pa.com in our example). This address uniquely identifies the user in Unified CM.
- Webex Teams SIP address — This address (set to bob@ent-pa.call.webex.com in our example) identifies the user on Webex. The subdomain ent-pa.call.webex.com is a publicly reachable subdomain of the domain call.webex.com managed by Webex.

When Alice calls Bob using her Cisco Unified CM device (step 1 in Figure 5-2), Unified CM forks the call to the Spark Remote Device that shares Bob's directory number with Bob's device, as shown by step 2 in Figure 5-2. The associated identity is triggered, and the call is sent to bob@ent-pa.call.webex.com through a SIP route pattern to Expressway-C. Expressway-C is configured to send any URI of the form <*user*>@ent-pa.call.webex.com to Expressway-E, and Expressway-E in turn sends it to the DNS zone (step 3 in Figure 5-2).

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.call.webex.com, because the DNS Zone on Expressway is configured to use callservice.webex.com instead of ent-pa.call.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. As a consequence, both Bob's Unified CM endpoint and his Webex Teams application receive the call, and Bob can decide which of the two clients he will use.

Figure 5-2 shows the call signaling flow for this example.

Figure 5-2 Call Signaling Flow for Call Service Connect

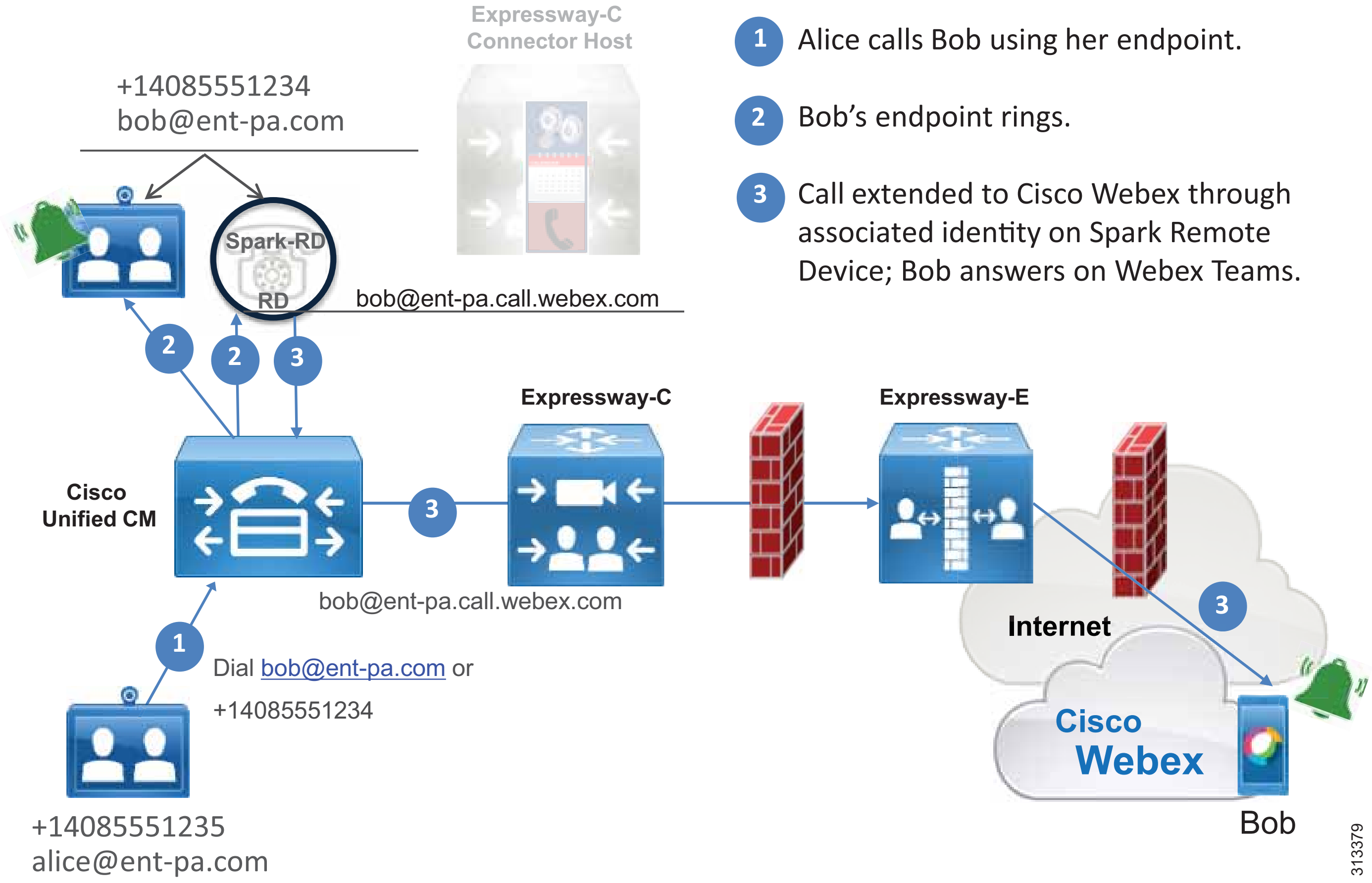


Figure 5-2 shows the following actions:

1. Alice calls Bob using her Unified CM registered device.
2. The call is sent to Bob's directory number, shared between Bob's Unified CM registered device and his Cisco Spark Remote Device. Bob's Unified CM device starts ringing.
3. The call is extended to Webex through the associated identity included in the Cisco Spark Remote Device.
4. Bob's Webex Teams application starts ringing. Bob can answer the call using the Webex Teams application or his Unified CM device.

When Alice on her Webex Teams application calls Bob, Webex detects that Bob is enabled for Call Service Connect with an enterprise URI set to bob@ent-pa.com, and it sends the call to both Bob's Webex Teams application and 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 subdomain 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: us-expe1.ent-pa.com
```

The SIP destination configured by the corporate administrator in the Webex Control Hub determines where Webex sends Call Service Connect call legs for this organization.

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 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 (bob@ent-pa.com) 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.

The call reaches Cisco Unified CM and is anchored on Alice's Cisco Spark Remote Device based on the caller ID of the incoming SIP call leg, which matches the associated identity provisioned on Alice's Cisco Spark Remote Device. Call anchoring is a mobility feature that is used to preserve the calling ID and also to apply a user-based class of service based on the calling search space (CSS) configured on the Cisco Spark Remote Device 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 Bob's DN on which Bob's directory URI is configured as an alias. This is shared between Bob's Unified CM devices and his Cisco Spark Remote Device. As a consequence, the incoming call is presented on Bob's Unified CM devices and at the same time a forked call leg is created to Bob's cloud SIP URI, which is configured as an associated identity on Bob's Cisco Spark Remote Device, as shown in step 4 of Figure 5-3.

Figure 5-3 Call Flow to Bob's Cisco Spark Remote Device

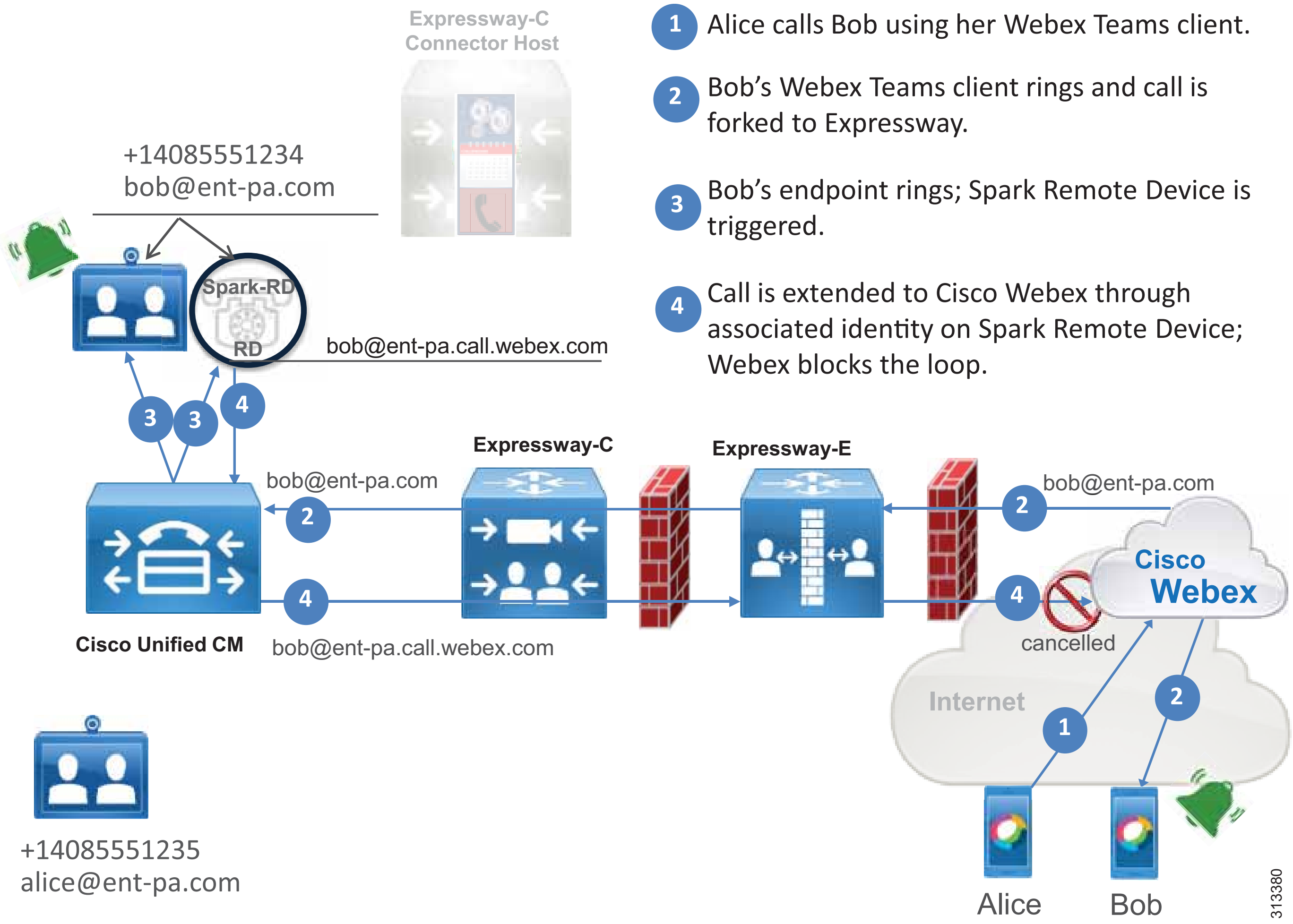

Expressway-C
Connector Host
1 Alice calls Bob using her Webex Teams client.
2 Bob's Webex Teams client rings and call is forked to Expressway.
3 Bob's endpoint rings; Spark Remote Device is triggered.
4 Call is extended to Cisco Webex through associated identity on Spark Remote Device; Webex blocks the loop.
+14085551234
bob@ent-pa.com
Spark-RD
RD
bob@ent-pa.call.webex.com
3
3
4
Expressway-C
Expressway-E
bob@ent-pa.com
2
2
bob@ent-pa.com
Cisco Webex
4
4
cancelled
Cisco Unified CM
bob@ent-pa.call.webex.com
Internet
1
2
+14085551235
alice@ent-pa.com
Alice
Bob
313380

Figure 5-3 shows the following actions:

1. Alice calls Bob using her Webex Teams application.
2. Bob is notified of an incoming call from Alice on his Webex Teams application. The call is extended to Expressway-E, Expressway-C, and Unified CM.
3. The call is sent to Bob's shared line, appearing on both his Unified CM registered device and his Cisco Spark Remote Device. Bob has the option to answer the call from either his Unified CM device or his Webex Teams application.
4. The associated identity on the Cisco Spark Remote Device extends the call to Webex through Expressway-C and Expressway-E. Webex detects that it is a looped call and disconnects it through the mechanism explained in the section on Loop Detection and Avoidance.

Loop Detection and Avoidance

Before forking the call to the calling user's enterprise (step 2 in Figure 5-3), Webex populates the SIP request with a Contact Header parameter **call-type=squared**. When Webex receives a call from the corporate network (step 4 in Figure 5-3) that contains the Contact Header set to **call-type=squared**, Webex detects that this is a looped call and does not send it back to the Webex Teams application. Therefore, Cisco Expressway must be configured to allow Contact Header pass-through on Expressway-C and Expressway-E.

TLS with Mutual Authentication

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 as the initiator of the request. In the case of the SIP connection from Webex to the enterprise, Webex acts as the client for this connection and Expressway-E is the server side. With MTLS, both Webex and Expressway-E authenticate each other based on certificates. Specifically, on the DNS zone on Expressway-E to be used for calls from Webex, a **TLS verify subject name** is configured, and this needs to match the Common Name (CN) or one Subject Alternative Names (SANs) of the certificate presented by Webex to Expressway-E during TLS handshake.

When a Webex Teams call is received by Expressway-E (server-side in TLS handshake), Expressway-E requests the TLS client certificate that is the Webex certificate. If the certificate is valid and one of its SANs matches what has been configured in the **TLS verify subject name**, the call is treated as authenticated. Successful authentication also 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, if business-to-business is configured on Expressway-E.

Media Encryption

Media is encrypted with Secure Real-time Transport Protocol (SRTP) between Cisco Webex and Cisco Expressway. Depending on the configuration, different scenarios can be achieved:

- End-to-end encryption

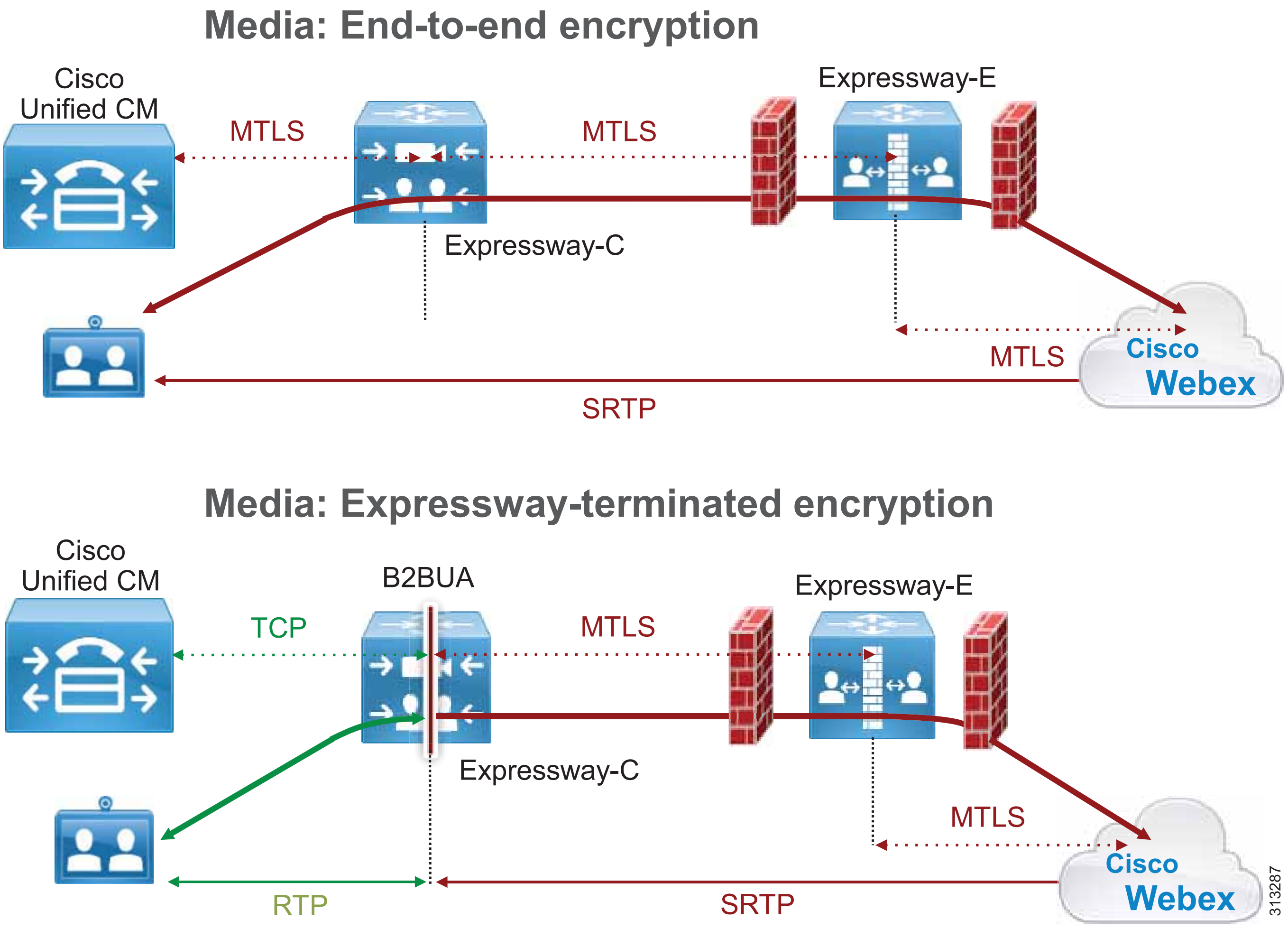
  This requires Cisco Unified CM to be in mixed mode and the endpoints to be provisioned for encryption.

- Expressway-terminated encryption

  If Cisco Unified CM is not in mixed mode and uses non-encrypted RTP media 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). If Expressway performs RTP-to-SRTP conversion, we recommend enabling it on Expressway-C instead of Expressway-E so that the traffic in the DMZ will be encrypted.

Figure 5-4 illustrates these two encryption options.

Figure 5-4 Media Encryption Options



Call Service Connect for Webex Room Devices

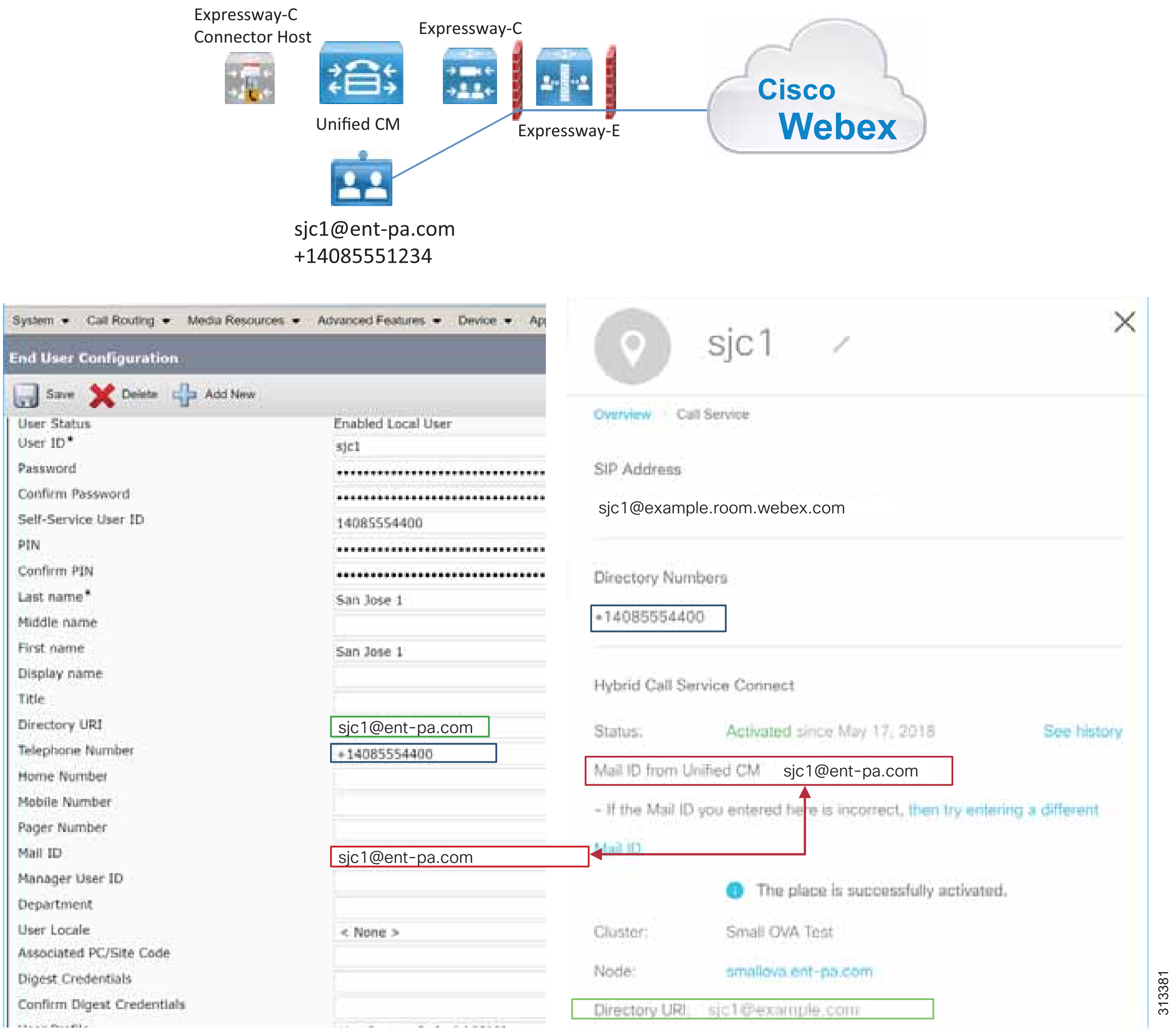
Cisco Webex Room Devices can be enabled for Call Service Connect. The result is similar to Webex Teams users enabled for Call Service Connect. The room device will have a directory number on Cisco Unified CM and a +E.164 number associated with the PSTN, and it will be able to dial out to the PSTN and to receive calls from the PSTN. In addition it will have all associated benefits of Call Service Connect, including the same dialing habits and same calling restrictions that are configured on Cisco Unified CM.

The room 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 email address is not required to have an associated Exchange inbox because Webex sends emails (if configured) to Users, not to Places.

The associated Spark Remote Device will be configured by Expressway-C Connector Host if it has been configured for automatic provisioning, or it must be configured manually if automatic provisioning is disabled. In this case, only the associated identity will be configured by the Connector Host.

Figure 5-5 shows the fields that must be configured on Cisco Unified CM and on the Webex Control Hub.

Figure 5-5 Required Configuration Fields for Webex Room Devices



End User Configuration

User Status	Enabled Local User
User ID*	sjc1
Password	••••••••••••••••••••••••••••••••
Confirm Password	••••••••••••••••••••••••••••••••
Self-Service User ID	14085554400
PIN	••••••••••••••••••••••••••••••••
Confirm PIN	••••••••••••••••••••••••••••••••
Last name*	San Jose 1
Middle name	
First name	San Jose 1
Display name	
Title	
Directory URI	sjc1@ent-pa.com
Telephone Number	+14085554400
Home Number	
Mobile Number	
Pager Number	
Mail ID	sjc1@ent-pa.com
Manager User ID	
Department	
User Locale	< None >
Associated PC/Site Code	
Digest Credentials	
Confirm Digest Credentials	

sjc1

SIP Address

sjc1@example.room.webex.com

Directory Numbers

+14085554400

Hybrid Call Service Connect

Status: Activated since May 17, 2018

Mail ID from Unified CM sjc1@ent-pa.com

- If the Mail ID you entered here is incorrect, then try entering a different Mail ID

The place is successfully activated.

Cluster: Small OVA Test

Node: smallova.ent-pa.com

Directory URI: sjc1@example.com

Deployment Overview

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

Expressway-C and Expressway-E on a Shared Deployment

If calls generated by Call Service Connect are co-resident with business-to-business calls, it is important to allow PSTN access to Webex Teams users while blocking business-to-business users from unauthorized access of PSTN and other internal-only services.

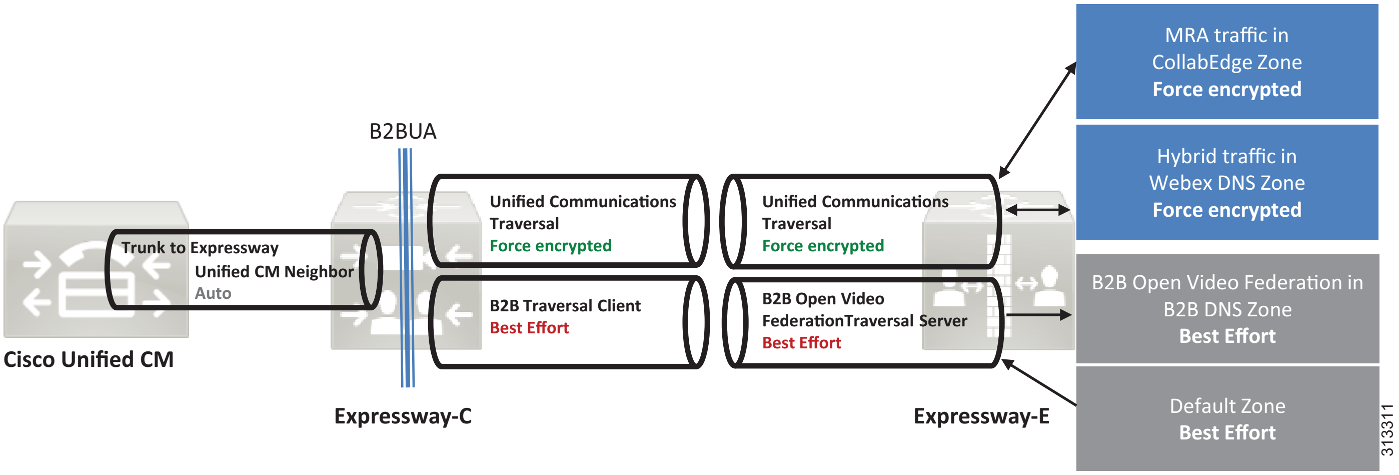
Standard business-to-business calls from other companies enter the Default Zone because these connections, even if they are configured for MTLS, will not present a certificate matching the TLS verify name configured on the Webex DNS zone. Therefore, we recommend configuring the Default Zone as non-authenticated. Call Processing Language (CPL) rules controlling access to the corporate network will thus be applied only to non-authenticated traffic, and Call Service Connect 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 System Solution Reference Network Designs (SRND)* guide, available at http://www.cisco.com/go/srnd.

It is possible to use a single traversal zone between Expressway-E and Expressway-C for business-to-business calls, Webex Hybrid Call Service 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.

We recommend using the MRA traversal zone (called **Unified Communications** traversal zone on Expressway) for Webex Hybrid Services traffic as well, while using a separate traversal zone for business-to-business (B2B) traffic, as shown in Figure 5-6.

Figure 5-6 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.

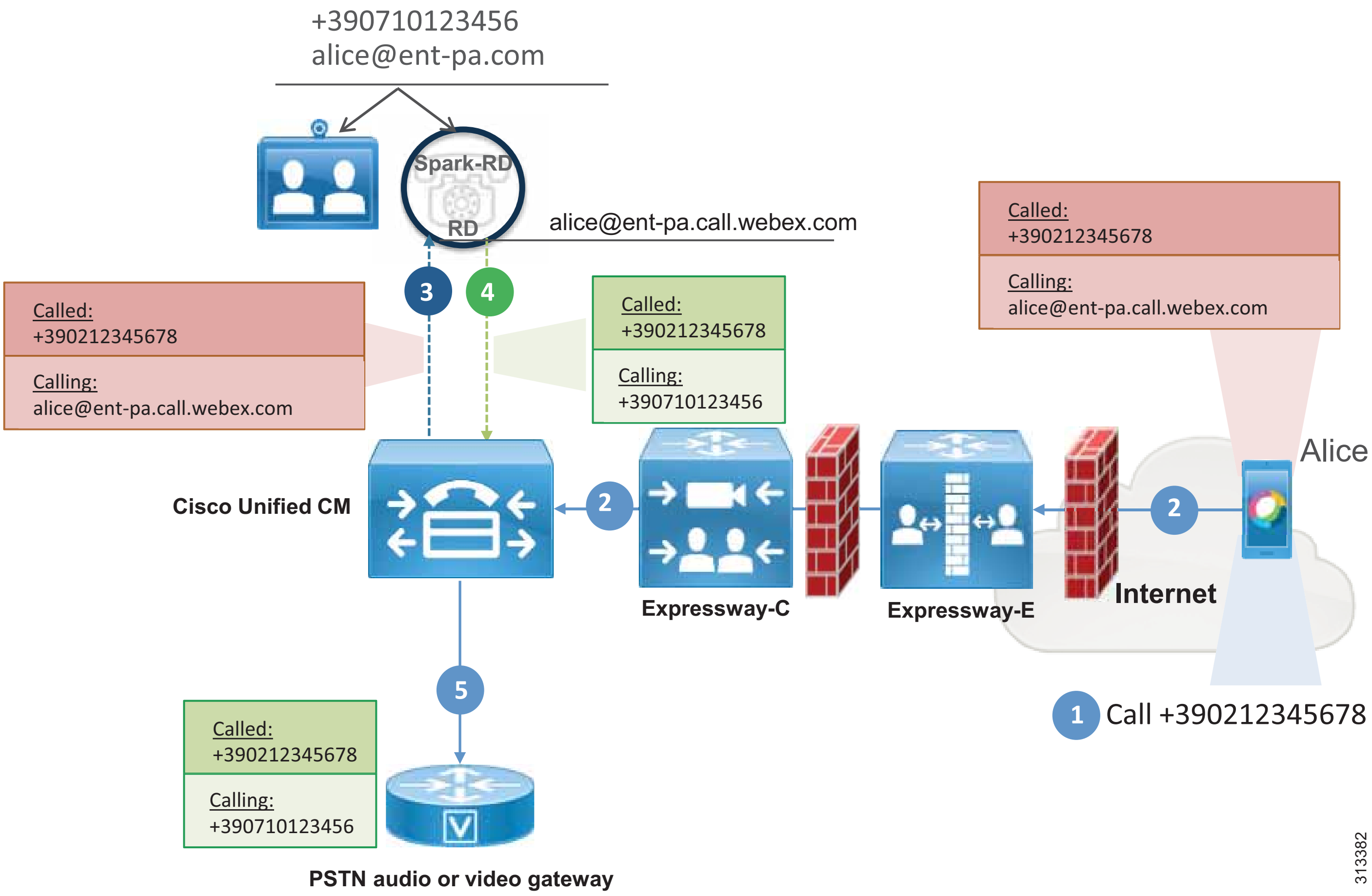
Caller ID and Class of Service

When a Webex Teams user calls a Cisco Unified CM endpoint or service, or when the user dials out to the PSTN, the desired behavior is to present the calling user's Unified CM directory URI or +E.164 number as the caller ID.

When the call leaves Webex, the caller ID is set to the Webex Teams SIP address of the calling user, such as alice@ent-pa.call.webex.com. Because this address matches the associated identity configured in the Cisco Spark Remote Device associated with the calling user, the call is anchored on the calling user's Cisco Spark Remote Device 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 user.

In the example in Figure 5-7, Alice dials a PSTN number using Webex Teams. When a call is placed from the Webex Teams application using the Calls tab, any number (such as a +E.164 number) can be entered. In this case the Request URI of the call leg forked to Expressway to route the call to the calling user's Unified CM is set to *<number>***@***<CFQDN>*, where CFQDN is the Cluster Fully Qualified Domain Name of the Cisco Unified CM cluster. The CFQDN of every user enabled for Call Service Connect is pushed to Webex by the Call Connector during the initial provisioning phase and is derived from the CFQDN enterprise parameter of the Unified CM cluster where the user is provisioned. Because the CFQDN enterprise parameter allows for provisioning multiple values in a space-separated list, the Call Connector always picks the first value and pushes that value to Webex. After the call is anchored on the calling users's Spark Remote Device, it follows the standard routing behavior of Unified CM and 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 Alice's Webex Teams SIP address alice@ent-pa.call.webex.com. Because the Webex Teams SIP address matches the associated identity set in the Cisco Spark Remote Device, this call is identified as belonging to Alice on Cisco Unified CM and is forwarded to the final destination as if it originated from Alice's directory number. Therefore, Alice's caller ID and Alice's calling search space as set in Unified CM will be used instead. This is shown in Figure 5-7, where steps 3 and 4 indicate logical processes inside Cisco Unified CM and not call flows.

Figure 5-7 Call Anchoring and Caller ID



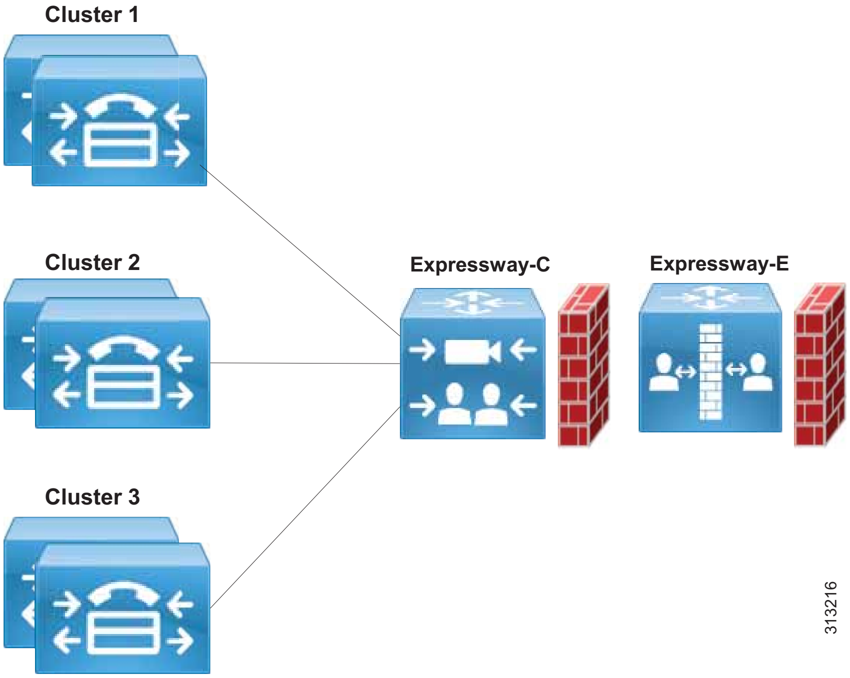
Call anchoring based on a successful match between caller ID and remote destination is a mobility feature and happens independently from the dialed destination.

Note Webex has no knowledge of the enterprise dial plan. For this reason, if Alice cannot call Bob using her endpoint on the enterprise network due to a restricted class of service, Alice may still call Bob if both use Webex Teams. If Alice uses Webex Teams, Cisco Unified CM will prevent the call from reaching Bob's endpoint, but Bob's Webex Teams application will ring.

Deployment Considerations for Multiple Unified CM Clusters

Webex Hybrid Call Service supports multiple Cisco Unified Communications Manger clusters. In this case, Expressway-C can be associated to every cluster, as shown in Figure 5-8.

Figure 5-8 Expressway-C Supporting Multiple Unified CM Clusters



When multiple clusters are deployed, the incoming call from Webex has to be routed to the calling user's Cisco Unified CM cluster for call anchoring and not to the Unified CM of the called user, in order to associate the call with the calling user's Spark Remote Device and correctly set the calling user’s enterprise caller ID and apply the calling user’s class of service. This is known as home cluster-based routing. With home cluster-based routing, the call is always anchored to the Cisco Unified CM of the calling user.

With home cluster-based routing, 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 Cisco Unified CM clusters, the use of the Route Header is a general concept and applies also to single-cluster deployments. Thus, Expressway search rules always have to match on Route Header and not Request URI values.

When both a Request URI and a Route Header are present in a SIP INVITE, the Route Header takes precedence in the routing processes if routing based on the route header is enabled on the zone that the call ingresses through on Expressway. As an example, when Alice on the US cluster dials Bob in the EMEA cluster using her Webex Teams application, Expressway-E receives this INVITE:

```
INVITE sip:bob@ent-pa.com SIP/2.0
Via: SIP/2.0/TLS 10.10.10.10:5062;branch=z9hG4bK-393139-4880f133ef84798fb3625da14a87ad32
Call-ID: 87c778d0a17c9a3a93ef90ff530fda50@30.30.30.30
CSeq: 1 INVITE
Contact: "l2sip" <sip:l2sip@10.10.10.10:5062;transport=tls>;call-type=squared
From: "Alice" <sip:alice@ent-pa.call.webex.com>;tag=1381736467
To: <sip:bob@ent-pa.com>
Max-Forwards: 70
Route: <sip:l2sip@20.20.20.20:5062;transport=tls;lr>,<sip:us-cm-pub.ent-pa.com;lr>
```

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.

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 alice@ent-pa.com in our example. Search rules on Expressway-E will thus match us-cm-pub.ent-pa.com and route the call to the next hop, Expressway-C first and Cisco Unified CM after.

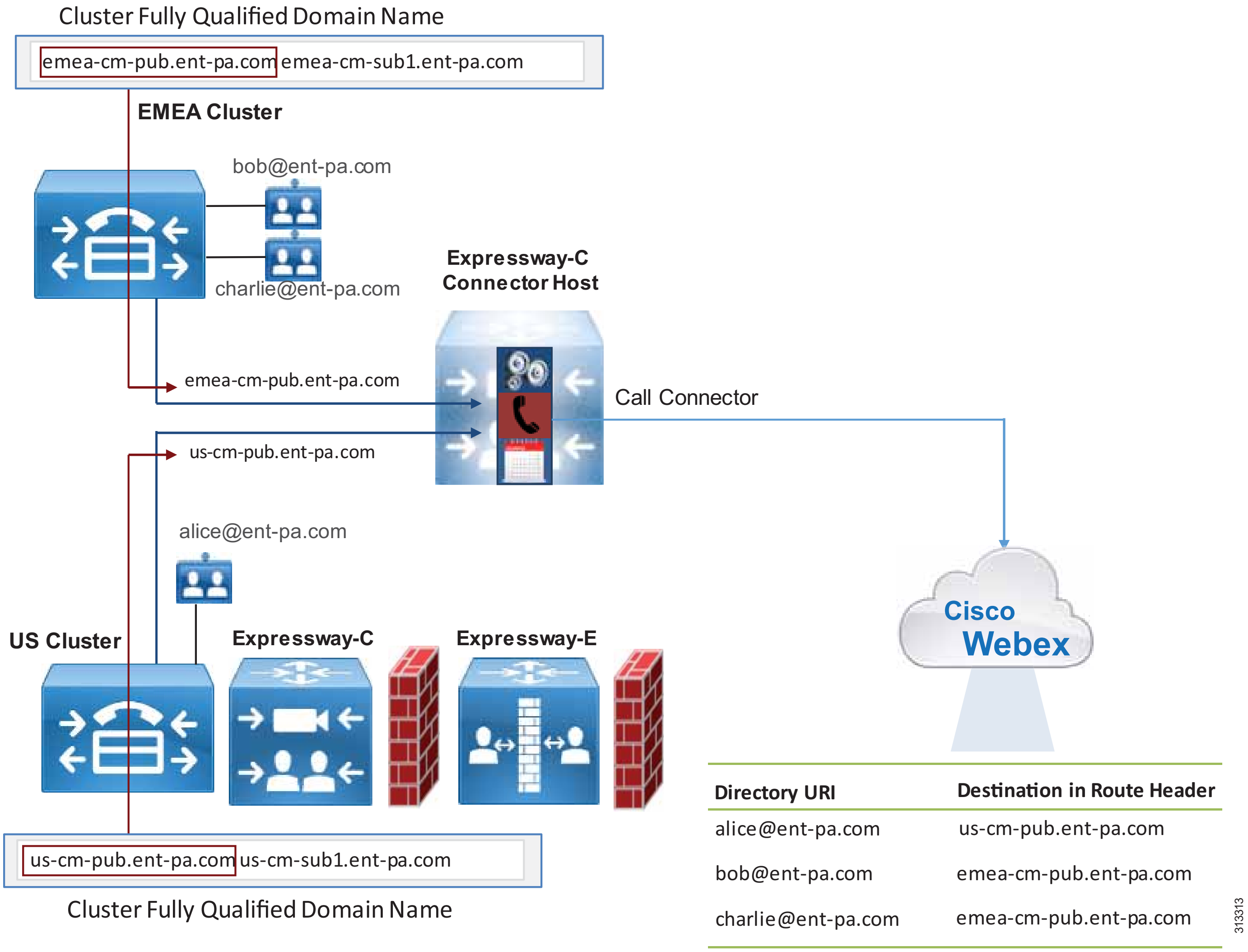
When Charlie on the EMEA cluster calls Bob, the INVITE looks different:

```
INVITE sip:bob@ent-pa.com SIP/2.0
Via: SIP/2.0/TLS 10.10.10.10:5062;branch=z9hG4bK-393139-4880f133ef84798fb3625da14a87ad32
Call-ID: 87c778d0a17c9a3a93ef90ff530fda50@30.30.30.30
CSeq: 1 INVITE
Contact: "l2sip" <sip:l2sip@10.10.10.10:5062;transport=tls>;call-type=squared
From: "Charlie" <sip:charlie@ent-pa.call.webex.com>;tag=1381736467
To: <sip:bob@ent-pa.com>
Max-Forwards: 70
Route: <sip:l2sip@20.20.20.20:5062;transport=tls;lr>,<sip:emea-cm-pub.ent-pa.com;lr>
```

This time Expressway routes the call based on the destination emea-cm-pub.ent-pa.com, and thus the INVITE is sent to the EMEA Unified CM through the Route Header, where Charlie's devices are registered.

Webex populates the Route Header based on the information received by the Call Connector and specifically taken from the Cisco 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 5-9.

Figure 5-9 Cluster Fully Qualified Domain Name (CFQDN)


Cluster Fully Qualified Domain Name
emea-cm-pub.ent-pa.com emea-cm-sub1.ent-pa.com
EMEA Cluster
bob@ent-pa.com
charlie@ent-pa.com
Expressway-C Connector Host
emea-cm-pub.ent-pa.com
Call Connector
us-cm-pub.ent-pa.com
alice@ent-pa.com
Cisco Webex
US Cluster
Expressway-C
Expressway-E
us-cm-pub.ent-pa.com us-cm-sub1.ent-pa.com
Cluster Fully Qualified Domain Name
313313

Directory URI	Destination in Route Header
alice@ent-pa.com	us-cm-pub.ent-pa.com
bob@ent-pa.com	emea-cm-pub.ent-pa.com
charlie@ent-pa.com	emea-cm-pub.ent-pa.com

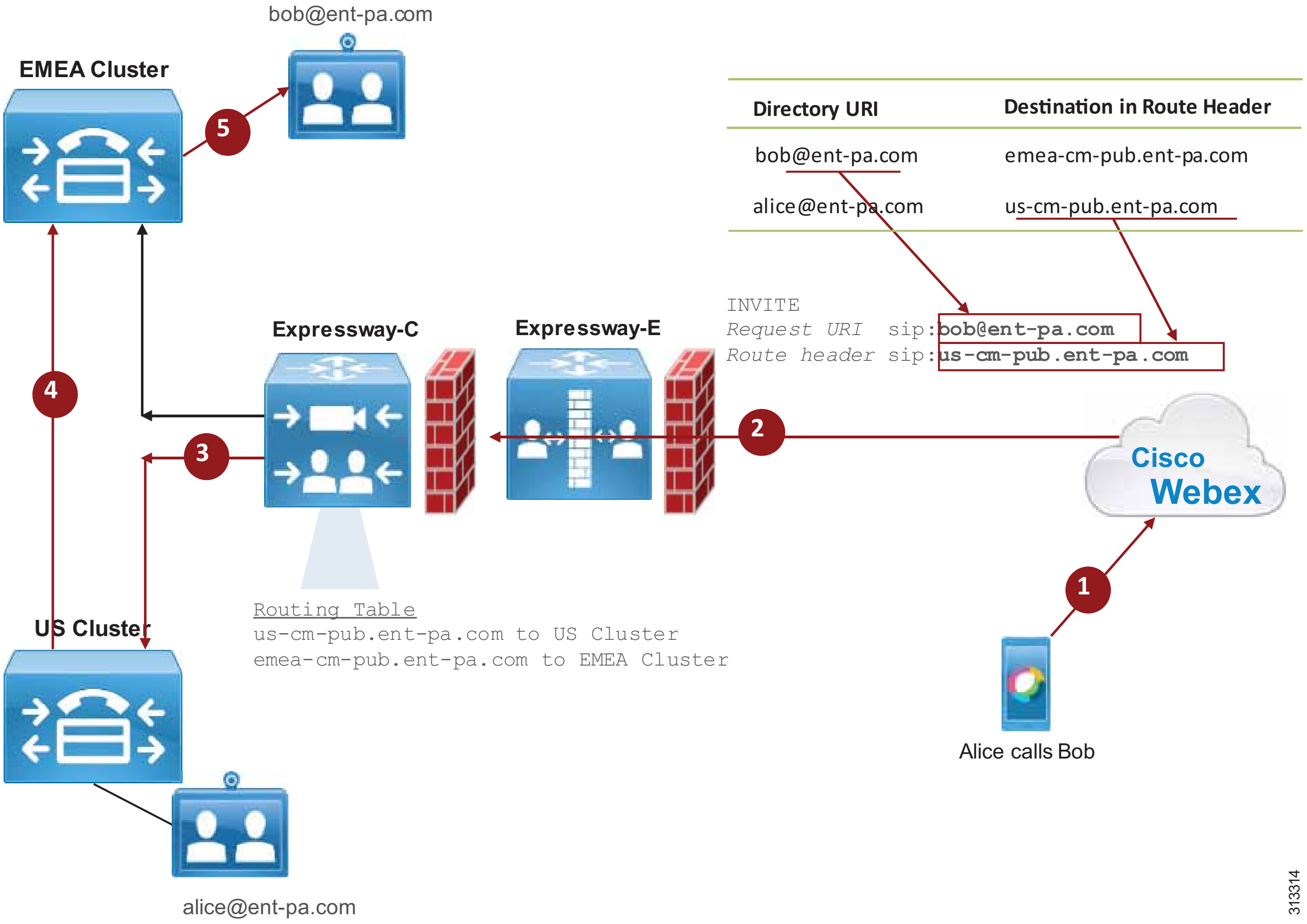
Although the CFQDN enterprise parameter in Unified CM allows the use of wildcards (for example, *.ent-pa.com), the use of the first value of the CFQDN enterprise parameter as the SIP route header for Call Service Connect call flows prohibits the use of wildcards in the first CFQDN value. If a wildcarded 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 Cisco 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 Call Service Connect call flows.

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 5-10.

Figure 5-10 ***Call Routing Based on Route Header***



Directory URI	Destination in Route Header
bob@ent-pa.com	emea-cm-pub.ent-pa.com
alice@ent-pa.com	us-cm-pub.ent-pa.com

```
INVITE
Request URI  sip:bob@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
```

For the scenario in Figure 5-10, two search rules are built on Expressway-C: the first matches calls with destination us-cm-pub.ent-pa.com and sends them to Cisco Unified CM in the US cluster, and the second matches calls with destination emea-cm-pub.ent-pa.com and sends them to Cisco 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 5-9 and Figure 5-10.

Figure 5-10 shows the following actions:

1. Alice starts a call to Bob using her Webex Teams application.
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 release 12.0, Cisco Unified CM also can be configured to route calls based on the SIP route header. This allows support of Cisco Unified CM Session Management Edition (SME) architectures.

If Expressway-C and Expressway-E run Webex Hybrid Services but no business-to-business traffic, it is important to reject any SIP message not generated by Webex Hybrid Services. 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 permits the creation of Call Processing Language (CPL) rules to mitigate fraudulent call attempts. We highly recommend deploying CPL rules for toll fraud mitigation.

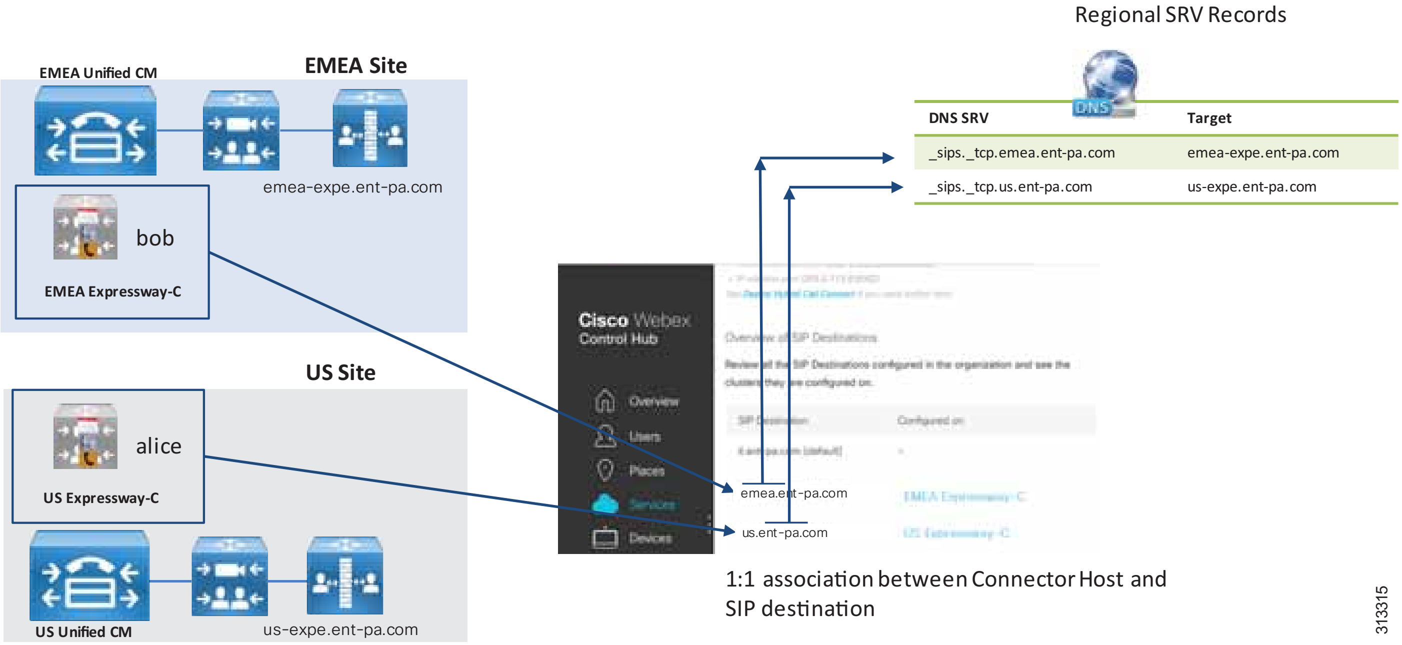
If business-to-business traffic is not included in the same Expressway, and because this traffic enters from the Default Zone, a CPL rule blocking any access to the Default Zone will prevent fraudulent access to Expressway-E. See the Call Connector Deployment Process for further details.

Multiple Cisco Unified CM and Expressway Clusters

When Cisco Unified CM is deployed in regional installations, every Cisco Unified CM cluster serves a specific region. That region might also have a dedicated Internet connection. In this case, the Expressway-C and Expressway-E cluster might also be dedicated to that region. In this scenario, Webex is able to route the call to the Expressway cluster connected to the Unified CM cluster where the calling user is configured.

In order for this routing architecture to work, it is important that an Expressway-C Connector cluster is dedicated to each Cisco Unified CM cluster. That way, it is possible to associate a specific SIP destination to each Connector Host, as shown in Figure 5-11.

Figure 5-11 Multiple Unified CM and Expressway Clusters



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

With the configuration in Figure 5-11, if Alice calls Bob, because Alice is provisioned by the US Expressway-C Connector Host, the SIP destination associated to the US Connector Host is chosen, and Webex performs the DNS SRV query to _sips._tcp.emea.ent-pa.com, which resolves into the Expressway-E in the US. The call is sent to the US Unified CM and is anchored before being routed to the destination Unified CM in EMEA.

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 Call Connector 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).

For more details on CPL rules, refer to the information on dial plan protection and Call Processing Language (CPL) in the *Cisco Collaboration System Solution Reference Network Designs (SRND)* guide, available at http://www.cisco.com/go/srnd.

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 Services will be highly available if Cisco Unified CM and Cisco Expressway are deployed in a cluster. Specifically, Expressway-C Connector Host can be deployed in a cluster to provide redundancy. The same guidelines that apply to Cisco Expressway also apply for Expressway-C Connector Host clustering. However, note that Call Service Connect takes an active role during the provisioning phase only, and if no Call Connector is available due to outages, calls will still work. With a non-redundant Call Connector, any user provisioning will be blocked during a Call Connector outage, planned or unplanned.

Call Connector Deployment Process

For detailed instructions on how to install and configure Call Connector, refer to the 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

Call Service Prerequisites

1. On Cisco Unified CM, set the mail ID of the user or import it from the LDAP directory.
2. On Cisco Unified CM, associate a directory URI to the user's directory number.
3. On Cisco Unified CM, set the telephone number attribute and associate it to the user's primary directory number.
4. On Cisco Unified CM, configure the enterprise parameter **Cluster Fully Qualified Domain Name**.
5. On Cisco Unified CM, associate users with devices.
6. On Cisco Unified CM, set the home cluster on the user configuration page.
7. Deploy Cisco Expressway-C and Expressway-E for firewall traversal capabilities.

Deploying Call Service Connect

1. On Cisco Unified CM, enable users for Cisco Unified Mobility.
2. On Cisco Unified CM, configure a Cisco Spark Remote Device for each user's primary extension. Alternatively, the administrator can configure automatic creation of the Cisco Spark Remote Devices, with the limitation that settings such as Device Calling Search Space, Rerouting Calling Search Space, Location, and Device Pool will be shared among all Cisco Spark Remote Devices. Note also that Line Calling Search Space is copied from the user's primary extension, and as such is user-specific
3. On Cisco Unified CM, set the Cisco Spark Remote Device to the user's primary extension and partition.
4. On Cisco Unified CM, associate the Cisco Spark Remote Device to the user's account.
5. On Expressway-E, set up a new DNS Zone for Webex Teams.
6. 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.
7. On Expressway-E:
   a. 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**.

8. On Expressway-E:
   a. Configure a Webex traversal server zone (standard traversal server zone enabled for SIP only) or re-use the existing MRA traversal zone (called Unified Communications Traversal).
   b. If you are setting up a new zone, set the media encryption mode to **force encrypted** in order to have encrypted communications between Webex and Expressway-C.
   c. Enable Route Header support (see step 7a).
   d. Set the Authentication policy to **check credentials**.
9. On Expressway-E, create a search rule matching any call with a domain portion that includes <*subdomain*>**.call.webex.com** and with the destination set to the DNS Zone, such as:

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

10. 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
```

11. 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. Call Service Connect Dedicated Expressway

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

    b. Call Service Connect Shared Deployment

    The following rules block calls from the Expressway-E Default Zone that contain the Webex Teams SIP domain ent-pa.call.webex.com, the corporate domain ent-pa.com, or the IP addresses of Expressway-E (10.10.10.10 and 10.10.10.11 in the example) in the calling alias.

Rule	Source Type	Rules Applies to	Source Pattern	Destination Pattern	Action
1	From address	Unauthenticated callers	.*@example\.call\.webex\.com.*	.*	Reject
2	From address	Unauthenticated callers	.*@example\.com.*	.*	Reject
3	From address	Unauthenticated callers	.*@10\.10\.10\.(10|11)	.*	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
4	Zone	Default Zone	[0|9]\d*(@.*)?	Reject
5	Zone	Default Zone	.*@example\.com.*	Allow
6	Zone	Default Zone	.*	Reject

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

12. On Expressway-C:

    a. Configure a Webex traversal client zone (standard traversal client zone enabled for SIP only) or re-use the existing MRA traversal zone (called Unified Communications Traversal).

    b. If you are setting up a new zone, set the encryption type to **force encrypted** in order to have encrypted communications between Webex and Expressway-C.

    c. Enable Route Header support and SIP parameter preservation to preserve the Contact Header, so that Webex is able to detect the loops.

    d. Set the Authentication policy to **check credentials**.

13. On Expressway-C:
    a. Configure a neighbor zone to Cisco Unified CM for Hybrid Call Services, different from the neighbor zone used for business-to-business calls.
    b. If mobile and remote access is configured in 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 Cisco 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 Cisco 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.
14. On Expressway-C, create a search rule matching any call with a domain portion that includes <*subdomain*>**.call.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\.webex\.com
```

15. On Expressway-C, create as many search rules as there are Cisco Unified Communications Managers deployed with hybrid services users. Those search rules must match the Cisco Unified CM CFQDN, and the destination must be set to the corresponding Unified CM neighbor zone:

```
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
```

16. On Cisco Unified CM, create a SIP Trunk Security Profile with a listening port set to match what has been configured in step 13b (for example, 5560 or 5561, in case security is turned on).
17. On Cisco Unified CM, create a SIP trunk linked to the security profile created in step 16, and point it to the Expressway-C. Include the SIP trunk in a route group and a route list.
18. 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.