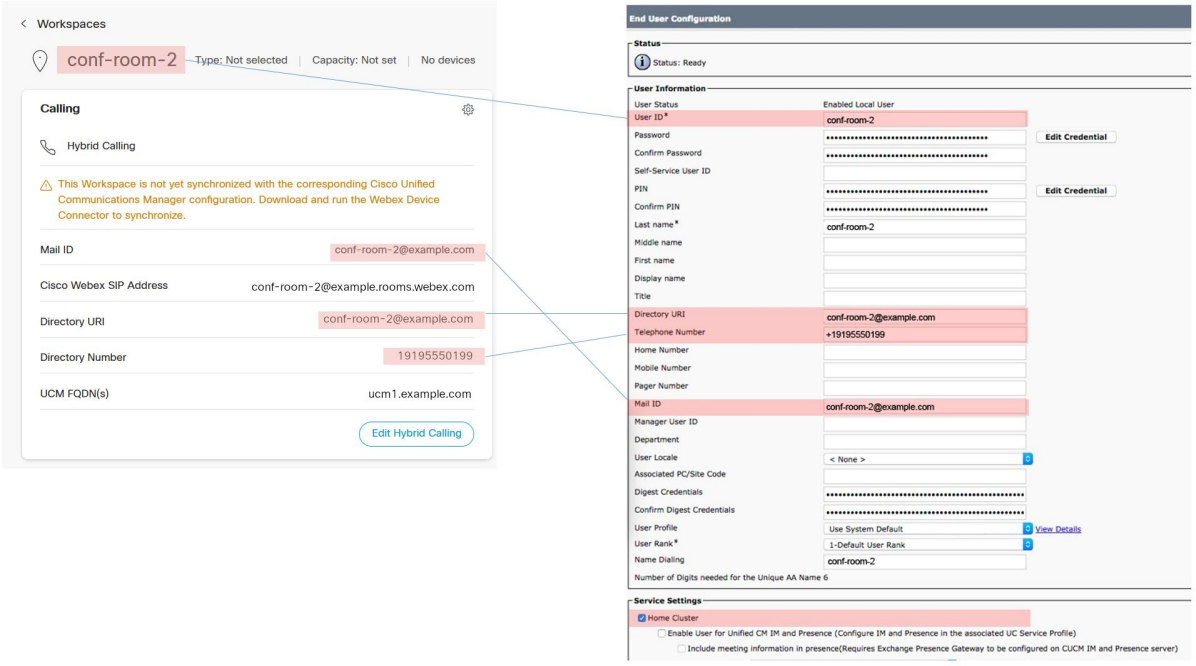
Deploy Hybrid Calling for Webex Devices

Hybrid Calling for Webex Devices deployment task flow

This task flow walks you through how to first configure Unified CM settings for Webex devices, configure Expressway settings, activate Hybrid Calling for your organization, and then add Hybrid Calling to either a newly created Workspace or an existing Workspace with Webex cloud-registered video devices. A Workspace is configured in Control Hub. After you complete all the required configuration on-premises and in the cloud, you can install and run the Webex Device Connector to synchronize the configuration between both.

Figure 1: Field mapping between Control Hub and Unified CM

As you configure Hybrid Calling for Webex Devices, refer to this screenshot which shows the mapping of fields between Control Hub (on the left) and Unified CM (on the right).



The following points provide a functional overview of the feature:

- This feature uses a Cisco Spark Remote Device (Cisco Spark-RD) in on-premises Unified CM to route calls on the device to enterprise extensions, users, and PSTN.
- Features that are initiated from on-premises phones (such as hold, transfer, and conference) can include Webex devices with Hybrid Calling.
- Any calls from Webex devices to PSTN or on-premises extensions are anchored to the Cisco Spark-RD in Unified CM.

Before you begin

- Read the overview: Hybrid Calling for Webex Devices
- Complete the requirements: Requirements for Hybrid Calling for Webex Devices

Procedure

	Command or Action	Purpose
Step 1	Manage domains (external article)	Domain verification is essential to the security and integrity of your organization. Verification proves to us that you own a particular domain and is required for this service to work. If your company has multiple domains, add each domain one at a time. For example, if you have Webex devices and administrators of the devices in `sales.example.com` and in `support.example.com`, you must add both domains.

	Command or Action	Purpose
		If your organization enforces email addresses, you are presented with warnings about possible lockout. You are forced to verify and remove domains in a particular order to prevent administrator lockout. When adding domains, for example, you must add the administrator domain first, followed by all other domains.
Step 2	Configure Unified Communications Manager settings for Hybrid Calling, on page 4	Configure Unified Communications Manager to receive calls directly from Expressway-E. This configuration enables URI routing between the cloud and the on-premises enterprise. You'll create a cluster FQDN, which is the enterprise parameter that is used in SIP routing decisions and that helps identify multiple clusters so calls can occur between them.

Step 3	Configure the Expressway-E for Hybrid Calling, on page 8 by following these tasks:
	• Update the Expressway-E trust list with Webex cloud certificates, on page 9
	• Choose one depending on your deployment:
	  • Configure services and mutual TLS authentication between a new Expressway-E and the Webex Cloud, on page 10
	  • Configure services and mutual TLS authentication between an existing Expressway-E and the Webex Cloud, on page 13
	• Create an automatic Webex DNS zone (Expressway-E to the Webex Cloud), on page 14
	• Configure a secure traversal server zone from Expressway-E to Expressway-C, on page 14
	• Create inbound and outbound search rules on Expressway-E, on page 16
		Enterprise calls are securely routed over the Expressway pair. If you want to reuse an existing pair, some of the required traversal configuration for Hybrid Calling may already be in place. However, read the procedures that follow to ensure that Expressway-E and Expressway-C are correctly configured.

Step 4	Configure the Expressway-C for Hybrid Calling, on page 18 by following these tasks: • Configure a secure traversal client zone from Expressway-C to Expressway-E, on page 19 • Create an Expressway-C neighbor zone for each Unified CM cluster, on page 20 • Configure search rules on Expressway-C (to Unified CM), on page 23	Enterprise calls are securely routed over the Expressway pair. If you want to reuse an existing pair, some of the required traversal configuration for Hybrid Calling may already be in place. However, read the procedures that follow to ensure that Expressway-E and Expressway-C are correctly configured.
Step 5	Activate Hybrid Calling for your organization, on page 25	Use this procedure to begin the initial setup for Hybrid Calling in Control Hub. These settings ensure that Hybrid Calling is first enabled for your organization before you do further configuration. You specify the desired subdomain for your company, and that setting creates Webex App SIP

	Command or Action	Purpose
		addresses as unique identifiers. Then, you toggle on hybrid call connect for your organization. Last, you enter the SIP destination address which resolves to your Expressway-E in the call traversal pair. This entry is typically a DNS-SRV record which can resolve to multiple Expressway-Es.
Step 6	Configure Workspace settings, on page 27 by following these tasks: • Create a directory number and directory URI for Webex devices with Hybrid Calling, on page 27 • Create a Unified CM account for Webex devices with Hybrid Calling, on page 28 • Create a Cisco Spark-RD for Webex devices with Hybrid Calling, on page 29 • Enable Hybrid Calling for Webex devices, on page 30	Follow these tasks to configure the necessary Unified CM settings that are required for enabling Workspaces or Personal Mode devices for Hybrid Calling.
Step 7	Install Webex Device Connector, on page 33	You can get the Webex Device Connector software from Control Hub. After you install the software, you can use it to synchronize Unified CM configuration (dial plan, directory number, extension, and so on) to Webex devices that are in Workspaces enabled for Hybrid Calling. The tool also synchronizes cloud configuration such as the Webex SIP address down to Unified CM.
Step 8	Synchronize device configuration changes with Webex Device Connector, on page 34	Webex Device Connector keeps your on-premises and cloud configuration for Webex devices in sync. The software also identifies any mismatch issues that you can resolve before you resync the changes.

Configure Unified Communications Manager settings for Hybrid Calling

Configure Unified Communications Manager to receive calls directly from Expressway-E. This configuration enables URI routing between the cloud and the on-premises enterprise. You'll create a cluster FQDN, which is the enterprise parameter that is used in SIP routing decisions and that helps identify multiple clusters so calls can occur between them.

Before you begin

Follow the Unified CM prerequisites that are covered in Complete the prerequisites for Hybrid Calling.

Step 1 From Cisco Unified CM Administration on your publisher node, go to **System > Enterprise Parameters**, scroll to **Clusterwide Domain Configuration**, and then check the value for the **Cluster Fully Qualified Domain Name** field.

Step 2 If the field is empty or the field contains domain entries with wildcards, enter a new value for Hybrid Calling and follow these guidelines:

FQDN Guideline	Description and Example
Multiple clusters	The entry must be unique for each cluster with Hybrid Calling—For example, `cluster1.example.com`, `cluster2.example.com`, and so on.
No wildcards	Do not use entries with wildcards, such as *.example.com or example*.com.
First FQDN entry for Hybrid Calling	In a list of multiple entries, the Webex cloud uses the first entry on the left for Hybrid Calling, and that first entry must not contain a wildcard. See this example of three FQDN entries from left to right (the first one being for Hybrid Calling): ***`cluster1.example.com`*** `*.example.com example*.com`
Different from Expressway-E	Must be different from the Expressway-E system, DNS, and domain name. Otherwise, Expressway-E strips the route header.
New entry for Hybrid Calling	If your current FQDN entry in Unified CM doesn't meet the requirements listed above, you can add a new element to the beginning of the cluster FQDN setting for Hybrid Calling. For example, if your existing FQDN setting in Cisco Unified Communications Manager is ***.example.com *.example.org**, add a unique, non-wildcard entry at the beginning of the field: *"**cluster1.example.com** *.example.com *.example.org"*

You are not required to restart Unified Communications Manager or services for a cluster FQDN change to take effect.

Step 3 Record or write down the name of the FQDN value that you want to use for Hybrid Calling. You need it for this procedure: Configure search rules on Expressway-C (to Unified CM), on page 23.

Step 4 Go to **Device > Device Settings > SIP Profile** to create a new SIP profile that is based on the **Standard SIP Profile For Cisco VCS** template.

a) Click **Find**, choose **Standard SIP Profile For Cisco VCS**, and then click **Copy**.
b) Enter a name for the new profile—for example, **`Standard SIP Profile for Webex Hybrid Calling`**.
c) Scroll to **Trunk Specific Configuration**, and then set **Early Offer support for voice and video calls** to **Best Effort (no MTP inserted)**.

   You can apply this setting to a new SIP trunk to the Webex cloud (routed by external domain **webex.com**). The setting does not affect any existing SIP trunking or call routing.

d) Leave all other fields with their default values and save your changes.

Step 5 (Optional) If your Expressway pair runs MRA or B2B, go to **System** > **Security** > **SIP Trunk Security Profile** and create a new SIP trunk security profile for Hybrid Services.

a) Enter a name for the new profile that is related to Webex or Hybrid Calling—for example, **`SIP Trunk Security Profile for Webex Hybrid Calling`**.
b) Set **Device Security Mode** to **Encrypted**.

   This is required because Expressway supports only encrypted TLS. This setting avoids an encryption mismatch between Expressway-C and Unified CM.

c) Leave the **Enable Digest Authentication** check box unchecked.
d) Do not set the incoming port value to 5061. Instead, change to an appropriate alternative—We recommend 5561.

We recommend that you use TLS. This setting doesn't require Unified CM to be in mixed mode. In this case, you must specify the following:

- **Transport type**—TLS instead of TCP/UDP
- **X.509 Subject Name**—Must match one of the Subject Alternative Names (SANs) of the Expressway-C.

e) Leave all other fields with their default values and save your changes.

Step 6 Go to **Device > Trunk** to create a new SIP trunk to the Expressway-C, and then link the Webex SIP profile to this trunk.

a) Choose **SIP Trunk** as the trunk type; leave the other settings, and click **Next**.

b) Configure these settings and leave the defaults for any settings not mentioned:

Field name	Value
Name	**Hybrid_Calling_SIP_Trunk** (for example)
Device Pool	Choose a device pool that contains the device-specific settings that you want the SIP trunk to inherit.
Calling and Connected Party Info Format	**Deliver URI and DN in connected party, if available** This setting enables blended identity. It allows the SIP trunk to transmit the enterprise-side party's directory URI to Webex. The directory URI is what allows the cloud to match the enterprise end user account to the Webex-registered device in a Workspace or Personal Mode. This match enables the Webex device to be provided with a Unified CM directory number. **Note** You must also apply this setting on any intercluster trunks within your organization and SIP trunks to any organizations that you want to work with Hybrid Calling.
Destination Address	Enter the Expressway-C node addresses in the fields.
Destination Port	Enter **5060/5061**.
SIP Profile	**Standard SIP Profile for Webex Hybrid Calling** (for example)

c) Save your changes.

Step 7 Go to **Call Routing > SIP Route Pattern** to create the following new route patterns that match the required subdomains for Hybrid Calling.

Table 1: SIP route pattern for Webex domain For Hybrid Calling for devices

Field Name	Value
IPv4 Pattern	***.rooms.webex.com**
Pattern Usage	**Domain Routing**
Description	**`Routing for` Webex hybrid calling devices**

Field Name	Value
Route Partition	Choose a route partition to contain this SIP route pattern. You must also include the same partition in the rerouting calling search space (CSS) of the Cisco Spark-RD. (We do not recommend using the **<None>** partition.)
SIP Trunk/Route List	Choose the trunk you created—**Hybrid_Calling_SIP_Trunk** (for example)
SIP Profile	**Standard SIP Profile for Webex Hybrid Calling** (for example)

Note We include this route pattern so that your deployment remains backwards compatible. If you're not sure if your Webex Devices have a webex.com SIP address, we recommend that you follow the directions in the *Migrate Cisco Spark Hybrid Call Service organization to the Cisco Webex domain* documentation to convert ciscospark.com domains over to webex.com.

Table 2: SIP route pattern for Cisco Spark domain (backwards compatibility)

Field name	Value
IPv4 Pattern	***.ciscospark.com**
Pattern Usage	**Domain Routing**
Description	**`Routing for` Cisco Spark hybrid calling**
Route Partition	Choose a route partition to contain this SIP route pattern. You must also include the same partition in the rerouting calling search space (CSS) of the Cisco Spark-RD. (We do not recommend using the **<None>** partition.)
SIP Trunk/Route List	Choose the trunk you created—**Hybrid_Calling_SIP_Trunk** (for example)
SIP Profile	**Standard SIP Profile for Webex Hybrid Calling** (for example)

Example

Combine Hybrid Calling with other solutions, such as B2B and MRA

- You can run Webex hybrid calls, B2B calls, and MRA calls across the same Expressway.
- If MRA is set up on your Expressway: For the trunk that you create for Webex, use a port other than 5060/5061 on Unified Communications Manager. This setup avoid conflicts with MRA calls and device registrations. On Unified Communications Manager, set up the Device Security Profile for your Webex trunk to use a port other than 5060 or 5061.
- If B2B is set up on your Expressway: You can reuse your existing B2B trunks between Unified Communications Manager and Expressway for Webex hybrid calls. If you want to run B2B calls and Webex hybrid calls on separate trunks between the Expressway-C and Unified

Communications Manager, you cannot run TLS on both trunks at the same time. See this bug overview for more information.

- If any of your Webex Hybrid Calling traffic goes over B2B, you must preserve the SIP parameters on all zones for all Expressways that are involved in call routing to and from the enterprise.

Configure the Expressway-E for Hybrid Calling

Enterprise calls are securely routed over the Expressway pair. If you want to reuse an existing pair, some of the required traversal configuration for Hybrid Calling may already be in place. However, read the procedures that follow to ensure that Expressway-E and Expressway-C are correctly configured.

Procedure

	Command or Action	Purpose
Step 1	Update the Expressway-E trust list with Webex cloud certificates, on page 9	Your Expressway-E must trust the certificate issuer of the server certificates that are passed by the server during the client/server SSL handshake with the Webex cloud. To establish this trust, you must add these certificates to the trusted CA list on your Expressway-E.
Step 2	Perform one of the following tasks, depending on your configuration: • Configure services and mutual TLS authentication between a new Expressway-E and the Webex Cloud, on page 10 • Configure services and mutual TLS authentication between an existing Expressway-E and the Webex Cloud, on page 13	Set up a mutual TLS port as part of establishing a trusted connection between your on-premises and the cloud. From a technical standpoint, Hybrid Calling SIP uses mutual TLS between the Expressway-E and Webex, so each side authenticates the other. This behavior requires valid and verifiable certificate and trust configuration on both sides.
Step 3	Create an automatic Webex DNS zone (Expressway-E to the Webex Cloud), on page 14	The DNS zone allows your Expressway-E to identify and route calls between Unified Communications Manager and the Webex cloud. The DNS zone is used because a secure mutual TLS connection between the cloud and Expressway-E is required to map the appropriate domains. The Webex Zone pre-configures the zone with the correct settings for Hybrid Calling.
Step 4	Configure a secure traversal server zone from Expressway-E to Expressway-C, on page 14	If you already have a traversal zone pair (typically for business-to-business (B2B) calling) or Unified Communications traversal zone pair (typically for Mobile and Remote Access (MRA)), or both, then we recommend that you create a separate traversal zone pair for Hybrid Calling.
Step 5	Create inbound and outbound search rules on Expressway-E, on page 16	Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified

	Command or Action	Purpose
		according to the conditions defined in the search rule. Create search rules on Expressway-E to: • Identify calls from the Webex cloud and route down the traversal zone to Expressway-C. • Identify calls from Unified Communications Manager and route through the DNS zone to Webex.

Update the Expressway-E trust list with Webex cloud certificates

Your Expressway-E must trust the certificate issuer of the server certificates that are passed by the server during the client/server SSL handshake with the Webex cloud. To establish this trust, you must add these certificates to the trusted CA list on your Expressway-E.

Before you begin

If you don't have an existing Expressway pair deployed, read the following documents to design your new Expressway pair to work together:

- Cisco Expressway Installation Guides
- Cisco Expressway Basic Configuration Deployment Guide
- Cisco Expressway and CUCM via SIP Trunk Deployment Guide
- Cisco Expressway IP Port Usage for Firewall Traversal Deployment Guide

Step 1 From Expressway-E, go to **Applications > Cloud Certificate management**.

Step 2 Click **Get certificates** for the cloud to automatically add and manage the certificates.

Step 3 To verify the added certificates, go to **Maintenance > Security certs > Trusted CA certificate** to view the entries that were added.

Configure call processing language (CPL) rules on Expressway-E

If Expressway-C and Expressway-E run both hybrid call and mobile and remote access (MRA) traffic, but no business-to-business traffic, the system must reject any SIP message not generated by MRA endpoints or Hybrid Services.

You can create call processing language (CPL) rules to mitigate fraudulent call attempts. We recommend doing this 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, the following CPL rule will prevent any fraudulent access to Expressway-E.

Step 1 From Expressway-E, go to **Configuration > Call Policy > Configuration**, set **Call Policy mode** to **Local CPL**, and then click **Save**.

Step 2 Go to **Configuration > Call Policy > Rules**, click **New**.

This opens the **Add Call Policy rule** page.

Step 3 Configure the following settings:

Field	Setting
Source type	**From address**
Rule applies to	**Unauthenticated callers**
Source pattern	**.*@example\.calls\.webex\.com.***, where **example** is your company's subdomain.
Destination pattern	**.***
Action	**Reject**

Step 4 Click **Add** to save this new rule.

Step 5 (Optional) In case TLS must be set to **On**, or B2BUA must be engaged on Expressway-E for some unknown reason, create the following CPL rule to block any TLS call from the Default Zone.

This step is not needed if TLS is switched off.

a) From Expressway-E, go to **Configuration > Call Policy > Configuration**, set **Call Policy mode** to **Local CPL**, and then click **Save**.
b) From related tasks, go to **Edit Call Policy rules**.
c) Click **New**.
d) Configure the following settings:

Field	Setting
Source type	**Zone**
Originating Zone	**DefaultZone**
Destination pattern	**.***
Action	**Reject**

e) Click **Add** to save this new rule.

Configure services and mutual TLS authentication between a new Expressway-E and the Webex Cloud

If Expressway-C and Expressway-E are dedicated to Hybrid Calling, or more generally to Cloud services using Mutual TLS only (such as Hybrid Services and CMR Hybrid), you don't require H.323, SIP UDP, SIP TCP and SIP TLS on Expressway-E.

Before you begin

- Update the Expressway-E trust list with Webex cloud certificates, on page 9
- If you configured a DNS SRV as the SIP destination in Control Hub (Activate Hybrid Calling for your organization, on page 25), ensure that that value specifies the MTLS port.

Step 1 From Expressway-E, go to **Configuration > Protocols > H.323**, and then set **H.323 mode** to **Off**, unless this setting is critical for your organization, and then save your changes.

Note If you Expressway-E is clustered, you can't disable H.323 box-wide because clustering relies on H.323. For this reason, we recommend setting up firewall rules on Expressway or the Internet firewall to block H.323 inbound.

Step 2 Go to **Configuration > Protocols > SIP**, and then configure these settings:

Field Name	Value
Configuration	
SIP mode	**On**
UDP mode	**Off**
UDP port	**5060**
TCP mode	**Off**
TCP port	**5060**
TLS mode	**On**
TLS port	**5061**
Mutual TLS mode	**On**
Mutual TLS port	**5062**
TCP outbound port start	**25000**
TCP outbound port end	**29999**
Session refresh interval (seconds)	**1800**
Minimum session refresh interval (seconds)	**500**
TLS handshake timeout (seconds)	**5**
Certificate revocation checking	
Certificate revocation checking mode	**Off**
Registration controls	

Field Name	Value
Standard registration refresh strategy	**Maximum**
Standard registration refresh minimum (seconds)	**45**
Standard registration refresh maximum (seconds)	**60**
Outbound registration refresh strategy	**Variable**
Outbound registration refresh minimum (seconds)	**300**
Outbound registration refresh maximum (seconds)	**3600**
SIP registration proxy mode	**Off**
Authentication	
Delegated credential checking	**Off**
Advanced	
SDP max size	**32768**
SIP TCP connect timeout	**10**

Step 3 Click **Save**.

Step 4 Go to **Configuration** > **Zones** > **Zones**, and then click **DefaultZone**.

Step 5 Configure the following fields:

Field Name	Value
Policy	
Authentication mode	**Do not check credentials**
SIP	
Media encryption mode	**Auto**
ICE support	**Off**
Multistream mode	**On**
Enable Mutual TLS on Default Zone	**On** This setting enables mutual TLS (Mutual Transport Layer Security) on the dedicated mutual TLS port 5062 on incoming connections through the Default Zone.

Step 6 Click **Save**.

Configure services and mutual TLS authentication between an existing Expressway-E and the Webex Cloud

Expressway-E can be shared between mobile and remote access (MRA), business-to-business (B2B), and Webex Hybrid Calling media traffic. If Expressway is used for B2B traffic, turn off those services that are not needed. H.323 is a signaling protocol that doesn't allow for encryption and should be switched off if it's not critical for the company. SIP UDP must be switched off for security reasons. This change won't affect the calling scenarios, because only SIP endpoints with IP dialing use SIP UDP. Endpoints that are involved with IP dialing are typically H.323-based. SIP TCP should be switched off if it's not critical for the company.

Before you begin

- Update the Expressway-E trust list with Webex cloud certificates, on page 9
- If using a dedicated MTLS port, ensure that the DNS SRV in Control Hub specifies this MTLS port. (See Activate Hybrid Calling for your organization, on page 25.)
- You cannot use Hybrid Calling on an Expressway firewall traversal pair that is used for Jabber Guest. In this case, set up a dedicated Expressway pair for Hybrid Calling.

Step 1 From Expressway-E, go to **Configuration > Protocols > H.323**, and then set **H.323 mode** to **Off**, unless this setting is critical for your organization, and then save your changes.

Note If you Expressway-E is clustered, you can't disable H.323 box-wide because clustering relies on H.323. For this reason, we recommend setting up firewall rules on Expressway or the Internet firewall to block H.323 inbound.

Step 2 Go to **Configuration > Protocols > SIP**, and then configure these settings:

Field Name	Value
SIP mode	**On**
UDP mode	**Off**
TCP mode	**Off**, if possible. If this breaks services such as B2B, set it back to **On**.
TLS mode	**On**
Mutual TLS mode	**On**
Mutual TLS port	**5062**

Step 3 Click **Save**.

Step 4 Go to **Configuration > Zones**, and then click **Default zone**.

Step 5 Set **Enable Mutual TLS on Default Zone** to **Off**.

Step 6 Click **Save**.

Create an automatic Webex DNS zone (Expressway-E to the Webex Cloud)

The DNS zone allows your Expressway-E to identify and route calls between Unified Communications Manager and the Webex cloud. The DNS zone is used because a secure mutual TLS connection between the cloud and Expressway-E is required to map the appropriate domains.

On Expressway, you can choose the Webex DNS zone which automatically creates a pre-configured zone for Hybrid Services. The system applies the correct settings and you cannot modify the zone. You can only have one zone of this type.

Step 1 From Expressway-E, navigate to **Configuration** > **Zones** > **Zones** and click **New**.

Step 2 For **Type**, choose **Webex**, and then save your changes.

This step creates the Hybrid DNS zone, identified by the automatically populated name **Webex Zone**.

Step 3 (Optional) Next to the hybrid domain, click **Check Connectivity**.

The connectivity test tool queries DNS for the supplied SRV domain and displays the results of the query if the lookup was successful. It then attempts a TCP connection followed by a TLS connection if applicable according to the DNS SRV protocol.

Configure a secure traversal server zone from Expressway-E to Expressway-C

If you already have a traversal zone pair (typically for business-to-business (B2B) calling) or Unified Communications traversal zone pair (typically for Mobile and Remote Access (MRA)), or both, then we recommend that you create a separate traversal zone pair for Hybrid Calling.

However, if you need to share the zones between the different services:

- You can share the Unified Communications traversal pair between MRA and Hybrid Calling (you can only have one Unified Communications traversal zone pair between Expressway-C and Expressway-E).
- Do not share a B2B traversal pair with Hybrid Calling. Create a separate traversal pair between Expressway-C and Expressway-E if they are used for B2B and Hybrid Calling.

Step 1 From Expressway-E, go to **Configuration** > **Zones** > **Zones**, and then click **New**.

Step 2 Configure these settings:

Field	Value
Configuration	
Name	**Webex hybrid traversal server**
Type	**Traversal server**

Field	Value
Hop count	**15** (Default)
Connection credentials	
Username	Enter **traversal**, for example.
Password	Go to **Add/Edit Local authentication database**, click **New**, enter **traversal** as the username, and then set a password. Click **Create Credentials**, and then close the window.
H.323	
Mode	**Off**
Protocol	**Assent** (Default)
Port	**6006** (Default)
H.460.19 demultiplexing mode	**Off** (Default)
SIP	
Mode	**On**
Port	**7004** or any value in 7XXX range. (This value must match the port number that is configured on Expressway-C.)
Transport	**TLS**
TLS verify mode	**On**
TLS verify subject name	Enter one of the Subject Alternative Names (SANs) of an Expressway-C certificate. For a cluster, enter at least a common SAN that is shared between all Expressway-C cluster peers.
Media encryption mode	**Force encrypted**
ICE support	**Off** (Default)
Multistream mode	**On** (Default)
SIP poison mode	**Off** (Default)
Preloaded SIP routes support	**On**
SIP parameter preservation	**On** **Note** This parameter must be set to **On** for all zones on all Expressways that are involved in call routing to and from the enterprise.

Step 3 Do not change settings under **Authentication** or **UDP/TCP Probes**.

Step 4 Click **Create zone**.

Create inbound and outbound search rules on Expressway-E

Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule. Create search rules on Expressway-E to:

- Identify calls from the Webex cloud and route down the traversal zone to Expressway-C.
- Identify calls from Unified Communications Manager and route through the DNS zone to Webex.

Before you begin

Configure a secure traversal server zone from Expressway-E to Expressway-C, on page 14

Step 1 From Expressway-E, go to **Configuration > Dial Plan > Search rules**, and then click **New**.

Step 2 Click **New**.

We're creating a rule to identify calls coming from Webex (through the DNS zone) and route them inwards (through the traversal zone) to Expressway-C.

Step 3 Configure the following settings:

Field	Value
Rule Name	Enter **Webex Hybrid inbound calls**, for example.
Description	Enter **Route traffic from Webex Hybrid Cloud to UCM via Expressway-C**, for example.
Priority	**100** (Default)
Protocol	**SIP**
Source	**Named**
Source name	**Webex hybrid DNS zone**, for example. Choose the Webex DNS zone from the drop-down list.
Request must be authenticated	**No** (Default)
On successful match	**Stop**
Target	**Webex hybrid traversal server**, for example. Choose the traversal server zone (or Unified Communications traversal zone) that you modified in the previous section.
State	**Enabled** (Default)

Step 4 Click **Create search rule**.

Step 5 Click **New**.

We're creating a rule to identify calls coming from Unified Communications Manager (through the traversal zone) and route them outwards (through the DNS zone) to Webex.

Step 6 Configure the following settings:

Field	Value
Name	Enter **Webex Hybrid outbound calls**, for example.
Description	Enter **Route traffic from Expressway-E to Webex Hybrid Cloud**, for example.
Priority	**100** (Default)
Protocol	**SIP**
Source	**Named**
Source name	**Webex hybrid traversal server**, for example. Choose the traversal server zone (or Unified Communications traversal zone) that you modified in the previous section.
Request must be authenticated	**No** (Default)
Mode	**Alias pattern match**
Pattern Type	**Regex**
Pattern string	`.*@.*\.webex\.com`
Pattern behavior	**Leave**
On successful match	**Stop** (Default)
Target	**Webex hybrid DNS zone**, for example. Choose the Webex DNS zone from the drop-down list.
State	**Enabled** (Default)

Step 7 Click **Create search rule**.

What to do next

Configure a secure traversal client zone from Expressway-C to Expressway-E, on page 19

Configure the Expressway-C for Hybrid Calling

Procedure

	Command or Action	Purpose
Step 1	Configure a secure traversal client zone from Expressway-C to Expressway-E, on page 19	Create a dedicated traversal client zone on Expressway-C. Though Webex traffic can coexist on the same traversal zone with MRA or B2B, we recommend that you create a dedicated traversal client zone on Expressway-C, specifically for handling Hybrid Calling signaling and media. That way, any settings for B2B or MRA won't affect Webex traffic, and the other direction won't be affected either.
Step 2	Create an Expressway-C neighbor zone for each Unified CM cluster, on page 20	Configure neighbor zones for each Unified Communications Manager cluster to which you want to route: • Each zone can accommodate 6 peer addresses, which supports a Unified Communications Manager cluster with 6 nodes. If you need to connect to a Unified Communications Manager cluster with more nodes, you can configure an SRV record for that cluster and use Expressway-C to discover neighbor nodes by SRV lookup. • This neighbor zone must route to a Unified Communications Manager home cluster—the zone can route to an SME if the SME is Unified CM 12.0(1). • The exact port to use for each zone depends on the SIP trunk security profile that you configured on Unified Communications Manager. If you have B2B or MRA configured, we recommend that you use 5561 for SIP TLS and 5560 for SIP TCP so that the new configuration doesn't interfere with your existing setup. • Do not reuse any existing neighbor zones to Unified Communications Manager for MRA.
Step 3	Configure search rules on Expressway-C (to Unified CM), on page 23	Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule. Configure search rules on Expressway-C to route calls to the correct Unified Communications Manager cluster based on the route header.

Configure a secure traversal client zone from Expressway-C to Expressway-E

Create a dedicated traversal client zone on Expressway-C. Though Webex traffic can coexist on the same traversal zone with MRA or B2B, we recommend that you create a dedicated traversal client zone on Expressway-C, specifically for handling Hybrid Calling signaling and media. That way, any settings for B2B or MRA won't affect Webex traffic, and the other direction won't be affected either.

Step 1 From Expressway-C, go to **Configuration** > **Zones** > **Zones**, and then click **New**.

Step 2 Configure these settings:

Field	Value
Configuration	
Name	**Webex Hybrid traversal client** (for example)
Type	**Traversal client**
Hop Count	**15**
Connection credentials	
Username	**traversal**
Password	Enter the password that you created on the Expressway-E for the **traversal** account.
H.323	
Mode	**Off**
SIP	
Mode	**On**
Port	**7004** or any value in 7XXX range. (This value must match the port number that is configured on Expressway-E.)
Transport	**TLS**
TLS verify mode	**On**
Accept proxied registrations	**Deny**
Media encryption mode	**Force encrypted**
ICE support	**Off**
Multistream mode	**On**
SIP poison mode	**Off**
Preloaded SIP routes support	**On** (Enables this zone to process SIP INVITE requests that contain the route header.)

Field	Value
SIP parameter preservation	**On** **Note** This parameter needs to be set to **On** for all zones on all Expressways that are involved in call routing to and from the enterprise.
Authentication	
Authentication policy	**Check credentials**
Accept delegated credential checks	**Off**
Client settings	
Retry Interval	**120**
Location	
Peer 1-6 address	Enter the Fully Qualified Domain Name (FQDN) of the traversal server. If you are using secure traversal, then this value must be either the Common Name or one of the Subject Alternate Names on the traversal server's certificate. IP addresses or hostnames are not recommended. If the traversal server is a cluster of VCS Expressways, enter the FQDN of each of the peers in that cluster.

Step 3 Click **Create Zone**.

Create an Expressway-C neighbor zone for each Unified CM cluster

Configure neighbor zones for each Unified Communications Manager cluster to which you want to route:

- Each zone can accommodate 6 peer addresses, which supports a Unified Communications Manager cluster with 6 nodes.

  If you need to connect to a Unified Communications Manager cluster with more nodes, you can configure an SRV record for that cluster and use Expressway-C to discover neighbor nodes by SRV lookup.
- This neighbor zone must route to a Unified Communications Manager home cluster—the zone can route to an SME if the SME is Unified CM 12.0(1).
- The exact port to use for each zone depends on the SIP trunk security profile that you configured on Unified Communications Manager. If you have B2B or MRA configured, we recommend that you use 5561 for SIP TLS and 5560 for SIP TCP so that the new configuration doesn't interfere with your existing setup.
- Do not reuse any existing neighbor zones to Unified Communications Manager for MRA.

Step 1 From Expressway-C, go to **Configuration** > **Zones** > **Zones**, and then click **New**. Create a zone for each cluster.

Step 2 Configure these settings:

Field	Value
Configuration	
Name	**UCM Neighbor for Webex** (for example)
Type	**Neighbor**
Hop Count	**15**
H.323	
Mode	**Off**
SIP	
Mode	**On**
Port	Enter the Unified Communications Manager listening port number, such as **5561**. If MRA is deployed, standard 5060 and 5061 ports are used as line-side registration. The configured port (5561) must match the listening port configured in the Communications Manager SIP Trunk Security Profile. Ports 5060 and 5061 can be used if MRA is not enabled.
Transport	**TCP** is the default, but we recommend **TLS** for connecting Expressway-C to Unified CM. For a trunk that is enabled for SIP TLS, Unified CM does not need to be in mixed mode. If you want to use TLS, see "Connecting Expressway to Unified CM Using TLS" in the Cisco Expressway and CUCM via SIP Trunk Deployment Guide for your Expressway and Unified CM version.
TLS Verify Mode	**On** to verify the CallManager certificate for subsequent SIP communications.
Accept proxied registrations	**Allow**
Media encryption mode	**Auto**
ICE support	**Off**
Multistream mode	**On**
Preloaded SIP routes support	**On**
AES GCM support	**On**
Authentication	
Authentication policy	**Do not check credentials**
SIP authentication trust mode	**Off**
Location	

Field	Value
Look up peers by	**Address** or **Service record** Choose **Address** if you want to enter up to 6 IP addresses, hostnames, or FQDNs of individual Unified CM nodes in the neighbor cluster. Choose **Service record** if you want Expressway to query DNS for an SRV record that resolves to the addresses of the nodes in the neighbor cluster.
Peer 1-6 addresses	If you chose to Lookup peers by Address, enter IP addresses or hostnames for each server in the 6 peer address fields. For TLS negotation, the peer address must match the CN name that is used in the Unified CM certificates; otherwise, TLS negotiation fails.
Service Domain	If you chose to Lookup peers by Service Record, enter the domain to search for. Expressway will prepend the protocol and transport, then do the DNS query based on the other parameters in your neighbor zone configuration. For example, if SIP mode is On and TLS verify mode is on, then when you enter `example.com`, Expressway queries DNS for `_sips._tcp.example.com`..

Step 3 Configure these fields for the zone profile:

Field	Value
Advanced	
Zone profile	**Custom**, the zone profile to use for the supported version of Unified CM for Hybrid Call Service.
Monitor peer status	**Yes**
Call signaling routed mode	**Always**
Automatically respond to H.323 searches	**Off**
Automatically respond to SIP searches	**Off**
Send empty INVITE for interworked calls	**On**
SIP Parameter Preservation	**On** **Note** This parameter needs to be set to **On** for all zones on all Expressways that are involved in call routing to and from the enterprise.
SIP poison mode	**Off**
SIP encryption mode	**Auto**
SIP REFER mode	**Forward**

Field	Value
SIP multipart MIME strip mode	**Off**
SIP UPDATE strip mode	**Off**
Internetworking SIP search strategy	**Options**
SIP UDP/BFCP filter mode	**Off**
SIP UDP/IX filter mode	**Off**
SIP record route address type	**IP**
SIP Proxy-Require header strip list	Leave this field blank.

Step 4 Click **Create Zone**.

Configure search rules on Expressway-C (to Unified CM)

Search rules define how the Expressway routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule. Configure search rules on Expressway-C to route calls to the correct Unified Communications Manager cluster based on the route header.

Before you begin

For the Expressway-E to Unified CM search rule, you need the cluster fully qualified domain name (FQDN) value that you configured in this procedure: Configure Unified Communications Manager settings for Hybrid Calling, on page 4.

Step 1 Go to **Configuration > Dial plan > Search rules** .

Step 2 Click **New**.

We're going to create a rule to identify calls coming from the Expressway-E (through the traversal zone) and route them inwards (through the neighbor zone) to Unified Communications Manager.

You'll need a rule for each Unified CM cluster that is trunked to the Expressway-C.

Step 3 Configure the following settings:

Field	Value
Rule Name	**From Webex Hybrid Cloud to Unified CM via Expressway-E**, for example.
Description	**Route traffic from Expressway-C to Unified CM**, for example.
Priority	**60**
Protocol	**SIP**

Field	Value
Source	**Named**
Source name	Choose **Webex Hybrid Traversal client**.
Request must be authenticated	**No**
Mode	**Alias pattern match**
Pattern type	**Prefix**
Pattern string	**`cluster1.example.com`**, for example. This is the **Cluster Fully Qualified Domain Name** enterprise parameter value for the Unified Communications Manager cluster. Add the other cluster FQDNs (`cluster2.example.com`, `cluster3.example.com`, and so on) for the corresponding Unified Communications Manager neighbor zones that you need to create on the Expressway-C.
Pattern behavior	**Leave** (The alias is not modified.)
On successful match	**Stop**
Target	Choose the Unified Communications Manager neighbor zone—for example, **UCM Neighbor for Webex**. This setting will be different for each cluster; each cluster should have its own neighbor zone.

Step 4 Click **Create search rule**.

Step 5 Click **New**.

We're going to create one rule to identify any calls (by Webex devices) arriving at Expressway-C that are destined for Webex, and route them outwards (through the traversal client zone) to the Expressway-E.

Step 6 Configure the following settings:

Field	Value
Rule Name	**From Unified CM to Webex Hybrid Cloud via Expressway-E**, for example.
Description	Enter **Route traffic from Unified CM to Expressway-E**, for example.
Priority	**70**
Protocol	**SIP**
Source	**Named**
Source name	**UCM Neighbor for Webex**, for example.
Request must be authenticated	**No**
Mode	**Alias pattern match**

Field	Value
Pattern type	**Regex** (The string is treated as a regular expression.)
Pattern string	`.+@.*\.((ciscospark)|((rooms|calls)\.webex)\.com).*` **Note** We include this pattern string so that your deployment remains backwards compatible. If you're not sure if your Webex App users and Webex Devices have a webex.com SIP address, we recommend that you follow the directions in the *Migrate Cisco Spark Hybrid Call Service Organization to the Cisco Webex Domain* documentation to convert ciscospark.com domains over to webex.com.
Pattern behavior	**Leave** (The alias is not modified.)
On successful match	**Stop**
Target	**Webex Hybrid traversal client**
State	**Enabled**

Step 7 Click **Create search rule**.

Activate Hybrid Calling for your organization

Use this procedure to begin the initial setup for hybrid call connect in Control Hub. These settings ensure that hybrid call connect is first enabled for your organization before you do further configuration. You specify the desired subdomain for your company, and that setting creates Webex App SIP addresses to identify users in the Webex cloud. Then, you toggle on hybrid call connect for your organization. Last, you enter the SIP destination address which resolves to your Expressway-E in the call traversal pair. This entry is typically a DNS-SRV record which can resolve to multiple Expressway-Es.

Before you begin

- You must complete all prerequisites in the “Prepare your environment” chapter and all the required deployment steps in this chapter before you can activate Hybrid Calling. Otherwise, the **Call Service Connect** activation button is greyed out.
- If you have multiple Expressway-Es for redundancy, we recommend that you create a dedicated DNS-SRV record with a subdomain specifically for the mutual TLS port on Expressway-E. For Hybrid Calling, the secure mutual TLS connection is a requirement for the Expressway-E and cloud to trust each other.

Step 1 From the customer view in https://admin.webex.com, perform one of the follow steps:

- From the first-time setup wizard for a new organization, choose **Enterprise Settings**
- For an existing Webex organization, go to **Management** > **Organization Settings**, and then scroll to Webex SIP Address.

Step 2 Follow the on-screen instructions to configure a custom SIP subdomain for your organization.

This subdomain value creates individual Webex SIP addresses for each Webex device in the form *workspacename@example.rooms.webex.com*. The addresses are used to receive calls from any standards-based SIP calling service. See Webex SIP addresses for more information.

Step 3 Go to **Services** > **Hybrid**, and then click **Settings** on the Hybrid Call card.

Step 4 Scroll to **Call Service Connect**, and then click **Activate** to enable the service for your organization.

Tip At this point, you can view the prerequisites in Control Hub before activation to make sure your environment is ready.

Caution If the Connect activation button is not available, you missed necessary configuration. Make sure you start over and follow all the prerequisites in the Prepare Your Environment chapter and every deployment step in this chapter.

Step 5 Scroll to the **Default SIP Destination** field on the same page, and then enter a network value that resolves to your Expressway-E and the SIP mutual TLS port.

Enter a network value using one of these formats:

Address Format	Example Of Value to Enter (In Bold)
SRV domain	_sips._tcp.**sipmtls.example.com**
Hostname/FQDN:port	**example.com:5062**
IP address:port	**203.0.113.0:5062**

For multiple IP address entries, you must use the DNS SRV record method.

Tip The SRV record can take time to request. If you want to start a trial or pilot, you can use *hostname:port* for a single Expressway-E so that you can proceed with the setup steps. You can modify this setting later and use the SRV record when that becomes available.

Step 6 Click **Test** to run a tool that checks that it can connect to the Expressway-E SIP destination you entered.

The tool initiates a TLS connection to that address. The results indicate whether the Expressway-E is reachable and secure.

Note If you're a partner sales administrator, you can run this test on behalf of your customer.

Step 7 After the test shows the results, click **View test results** to get more details on what the test ran and the outcomes.

The results show the type of lookup (such as DNS SRV), FQDN, IP address, and the specific connection tests such as a socket connection, SSL handshake with the Expressway-E, and a SIP OPTIONS ping. If any tests fail, the tool shows suggested steps to troubleshoot the issue. See Hybrid connectivity test tool (Control Hub) for more information.

Step 8 Save your changes.

Step 9 (Optional) If you have your own certificates, check **Upload your own certificate**, and then browse to and upload self-signed custom certificates that you want to use instead of the Webex default trust list.

For more information about manual certificate management, see Custom certificates for mutual TLS authentication between Expressway-E and the cloud.

Configure Workspace settings

Follow these tasks to configure the necessary Unified CM settings that are required for enabling Workspaces for Hybrid Calling.

Procedure

	Command or Action	Purpose
Step 1	Create a directory number and directory URI for Webex devices with Hybrid Calling, on page 27	Use Cisco Unified CM Administration to configure directory numbers that you want to later associate (through an end user account) with Webex devices. You'll also assign directory URIs to the directory numbers.
Step 2	Create a Unified CM account for Webex devices with Hybrid Calling, on page 28	Even though the Webex devices are registered to the cloud, you can associate a number to them from an on-premises Cisco Unified Communications Manager (Unified CM). You can use a Unified CM end user account to represent the Webex devices. The Workspace contains Webex-registered devices in a physical location.
Step 3	Create a Cisco Spark-RD for Webex devices with Hybrid Calling, on page 29	The Cisco Spark-RD is a virtual device that is attached to a Unified CM end user work number. The device links the Webex device to the enterprise SIP identity so that calls anchor on the Unified CM side.
Step 4	Enable Hybrid Calling for Webex devices, on page 30 by following either or both these steps: • Enable Hybrid Calling for a New or Existing Workspace With Webex Devices, on page 31 • Enable Hybrid Calling for Personal Mode Devices, on page 32	You can use Conttrol Hub to enable Hybrid Calling for Webex cloud-registered devices—both shared devices in workspaces and personal devices assigned to users.

Create a directory number and directory URI for Webex devices with Hybrid Calling

Use Cisco Unified CM Administration to configure directory numbers and directory URIs that you want to later associate (through an end user account) with Webex devices in a Workspace or in Personal Mode.

Before you begin

Workaround for directory URI dialing—If your users want to call a Hybrid Calling-enabled Webex device by using a directory URI from their Webex App or another device, we recommend that you create the directory URI to match the name of the Workspace in Control Hub. Then, the caller can enter the user portion of the directory URI and call the device based on directory name lookup.

Note This configuration works with devices that are in the same organization as the caller. The directory name lookup only matches devices and callers that are in the same organization.

Step 1 From Cisco Unified CM Administration, go to **Call Routing > Directory Number**, and then click **Add New**.

Step 2 For the Workspace, enter a dialable **Directory Number** and choose the **Route Partition** the number belongs to.

Step 3 In **Description**, **Alerting Name**, and **ASCII Alerting Name**, enter the name of the Workspace.

The Directory Number Alerting Name and ACSII Alerting Name can be no more than 30 characters in length. The names can only contain letters, numbers, spaces, and the following special characters: **!#$'()*+,./:;=?@^_**

Step 4 Choose a **Calling Search Space**.

A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that are using this directory number.

Step 5 Click **Save**, enter an address in **Directory URI**, and click **Save** again.

Note Make sure the Directory URI matches the Directory URI on your end user. See the Before You Begin section for a recommendation.

Create a Unified CM account for Webex devices with Hybrid Calling

Even though the Webex devices are registered to the cloud, you can associate a number to them that comes from your Cisco Unified Communications Manager (Unified CM) environment. To tie the number to the device, you can use a Unified CM end user account to represent the Webex devices in a Workspace or in Personal Mode.

This account is not tied to a real user. Instead, the account stands in for the devices and provides a PSTN number or extension from the Unified CM dial pool to the devices in the Workspace or in Personal Mode.

When you manually run the Webex Device Connector, the configuration within the end user account is associated with the Webex device in a Workspace or in Personal Mode. The device obtains a directory number, directory URI, and Webex SIP address (the remote destination of the Cisco Spark-RD). Behind the scenes, the Cisco Spark-RD creates the link between the Webex device and the premises configuration.

Note You only need to run Webex Device Connector as and when you need to take an action, such as completing all required config on Unified CM and in the cloud, then needing to synchronize the two together.

Before you begin

- The email address domain must be one of your verified domain entries in Control Hub (https://admin.webex.com). See Manage Domains.

Step 1 From Cisco Unified CM Administration, go to **User Management > End Users**, and then choose one:

- Specify any search criteria, click **Find**, and then open the existing account that you want to represent a Workspace.
- Click **Add New** to create a new account to represent a Workspace.

Step 2 If creating a new account, enter a **User ID** and **Last name**.

Because the account doesn't correspond to an actual user, you can enter values that identify the Workspace, such as a conference room location.

Step 3 Verify that the account has a valid **Directory URI** that contains the same domain as your organization.

The Directory URI for the user must match the Directory URI for the directory number that you created for the Workspace. The Directory URI is a linkage into more details from the Unified CM.

Step 4 (Optional) If you want your users to see the external number of the Workspace on the devices, enter the **Telephone Number** as the full E.164 number.

This number will show up on your hybrid-enabled Workspace. You could also use an internal number or extension. If you have multiple Webex devices in the Workspace, the same directory number is assigned to all of them, like shared lines. From a technical standpoint, a call to this number is sent to the assigned Webex SIP address, which Webex forks to all the Webex devices in the Workspace.

Step 5 Verify that **Mail ID** contains a unique email address that you'll use for the Workspace.

The email address must be an exact match between both Webex and on-premises. Use unique email accounts for each Workspace.

Step 6 Under the service settings, check the **Home Cluster** checkbox.

Configure this setting on the Cisco Unified Communications Manager where the account is homed.

Step 7 (Optional) If the user account has a device in the controlled list, set the primary extension to a directory number. Choose one that you want to provide to the devices in the Workspace, and then save your changes.

Note For Cisco Spark-RD, do this step after you create the devices.

Create a Cisco Spark-RD for Webex devices with Hybrid Calling

The Cisco Spark-RD is a virtual device that is attached to a Unified CM end user work number. The device links the Webex device to the enterprise SIP identity so that calls anchor on the Unified CM side.

Note A Cisco Spark-RD must be 15 characters or less.

Step 1 From Cisco Unified CM Administration, go to **Device > Phone**, click **Add New**, and then choose **Cisco Spark Remote Device**.

Step 2 For **Owner User ID**, specify the user account for the Workspace that you are configuring.

The **Device Name** is automatically created after you choose the user account. If you see an error, you may have to manually shorten the device name.

Step 3 For line association, specify the primary extension (the shared line).

Step 4 Ensure that the partition used by the SIP route pattern is listed in the remote device's rerouting calling search space (CSS). The route from the remote device to the SIP trunk happens through the rerouting CSS.

Use these documents to understand the settings that the remote device uses:

- Device pools
- Locations
- Calling search spaces

The calling search space must be able to route to the partition of the PSTN gateway or trunk, as well as any other destinations that you want devices in the Workspace to be able to reach (conference bridges, enterprise-to-enterprise trunks, and so on).

Step 5 Save your changes.

Step 6 From Cisco Unified CM Administration, go to **User Management > End User**, and then reopen the user account for the Workspace.

Step 7 Under Device Information, click **Device Association**.

Step 8 Specify any search criteria and click **Find**.

Step 9 Check the remote device that you created, and then save your changes.

The remote device is associated with the Workspace end user account and is added to the controlled devices list. The remote destination is added later when you run a sync from the Webex Device Connector tool. The tool synchronizes the Webex SIP address from the cloud and links it to the Cisco Spark-RD as the remote destination under **Associated Remote Destinations**.

Step 10 If the user account has a device in the control list, set the primary extension to a directory number. Choose one that you want to provide to the devices in the Workspace, and then save your changes.

Enable Hybrid Calling for Webex devices

You can use Control Hub to enable Hybrid Calling for Webex cloud-registered devices—both shared devices in workspaces and personal devices assigned to users.

Procedure

	Command or Action	Purpose
Step 1	Enable Hybrid Calling for a New or Existing Workspace With Webex Devices, on page 31	You can set up shared Webex devices and add them to a Workspace, add services, and then watch the collaboration happen. Whatever device you choose to add to that Workspace, the device is assigned to the Workspace, not a user. The key advantage is shared usage.
Step 2	Enable Hybrid Calling for Personal Mode Devices, on page 32	Personal mode devices are Webex Room, Desk, or Board devices that are registered to the cloud but also assigned to

	Command or Action	Purpose
		a user in Control Hub. You can add Unified CM calling functionality by enabling Hybrid Calling for these devices.

Enable Hybrid Calling for a New or Existing Workspace With Webex Devices

When people are at work, they get together in lots of Workspaces like lunch rooms, lobbies, and conference rooms. You can set up shared Webex devices and add them to a Workspace, add services, and then watch the collaboration happen. Whatever device you choose to add to that Workspace, the device is assigned to the Workspace, not a user. The key advantage is shared usage.

Procedure

- To create a new Workspace, add a device, and enable Hybrid Calling:
  a) From the customer view in https://admin.webex.com, go to **Management** > **Workspaces**, and then click **Add Workspace**.
  b) Enter a name for the Workspace (such as the name of the physical room), specify other attributes (**Type**, **Capacity**, and **Avatar**), and then click **Next**.
  c) Choose **Other Cisco device** (this option supports Webex cloud-registered devices and Hybrid Calling), and then click **Next**.

     You can have a combination of devices in a single Workspace (for example, a single Webex Room Device or a Webex Board). You cannot have multiple instances of the same type of device in a Workspace (for example, 2 Webex Boards).

  d) Choose **Hybrid Calling** to use call service (PSTN access or internal extension access) through your on-premises Unified CM call control environment. Unified CM provides the phone number or extension for the devices in the Workspace. Then click **Next**.
  e) Enter the Unified CM mail ID for the account that you created in Cisco Unified CM Administration.

     The service discovers where the email address is located on a Unified CM cluster.

  f) Click **Download** to get the Webex Device Connector software and choose the platform your system is running (Windows or Mac).
  g) After you download and install the software, return to Control Hub and click **Done**.
  h) Click **Next**, and then activate the device with the code provided.
- To enable Hybrid Calling for devices in an existing Workspace:
  a) From the customer view in https://admin.webex.com, go to **Workspaces**, and then choose the Workspace that you want to update.
  b) Next to **Calling**, click  , and then choose **Hybrid Calling** to use call service (PSTN access or internal extension access) through your on-premises Unified CM call control environment. Unified CM provides the phone number or extension for the Webex devices in the Workspace. Then click **Next**.
  c) Enter the Unified CM mail ID for the account that you created in Cisco Unified CM Administration.

     The service discovers where the email address is located on a Unified CM cluster.

  d) Click **Download** to get the Webex Device Connector software and choose the platform your system is running (Windows or Mac).
  e) After you download and install the software, return to Control Hub and click **Done**.

Enable Hybrid Calling for Personal Mode Devices

Personal mode devices are Webex Room, Desk, or Board devices that are registered to the cloud but also assigned to a user in Control Hub. These devices share the same line that is assigned to the end user account in Unified CM. Once the required Unified CM configuration is in place, you can add Unified CM calling functionality by enabling Hybrid Calling for these devices.

Note Users can answer incoming calls on the device or desktop. If they answer on their desktop, there's no option to escalate to the device.

Before you begin

- Hybrid Calling must be enabled for your organization. Review the steps in "Retain Configuration for Hybrid Calling for Webex Devices" in the Prepare Your Environment chapter of this guide..
- The followed Unified CM configuration must be in place:
  - For each user that requires PSTN for their Personal Mode device, you must create an end user account (this can be a local Unified CM account) that is specific to the device and contains a mailID (this does not need to be an active email address) and directoryID that matches. If the device owner also uses Unified CM Calling in Webex App, that ID must be unique and separate from the end user account that is tied to the Webex App user.

    Note the following example to understand the difference between the two accounts:
    - *username@example.com* for the end user account associated with Webex App.
    - *username.pstn@example.com* for the end user account associated with the personal mode device.
  - A Cisco Spark-RD device that is associated with the end user's account for the personal mode device the directory number that the user uses in Webex App. Both accounts in Unified CM must be associated with the same directory number.
- Assign a Personal Room or Desk Device to a User

Note Users can also Set Up a Webex Board, Room or Desk Device as a Personal Device.

Step 1 From the customer view in https://admin.webex.com, go to **Management** > **Devices**, and then choose a Webex device that you want to enable for Hybrid Calling.

Note The Webex device must have a **Type** of **Rooms & Desks** and have a user assigned to it in the **Belongs to** column.

Step 2 Scroll to **Calling**, and then click **Calling** to open the Hybrid Calling configuration screen.

Step 3 Enter the Unified CM mail ID for the account that you created in Cisco Unified CM Administration.

The service discovers where the email address is located on a Unified CM cluster.

Step 4 Click **Download** to get the Webex Device Connector software and choose the platform your system is running (Windows or Mac).

Step 5 After you download and install the software, return to Control Hub and click **Done**.

Step 6 From Webex Device Connector, connect to the Unified CM using the AXL account.

Step 7 Sync the new personal mode device.

Note You do not have to wait for all the devices to populate. You can synchronize the personal mode device as soon as you see it.

Install Webex Device Connector

You can get the Webex Device Connector software from Control Hub. After you install the software, you can use it to onboard devices in bulk or synchronize Unified CM configuration (dial plan, directory number, extension, and so on) to Webex devices that are in Workspaces enabled for Hybrid Calling.

Step 1 From the customer view in https://admin.webex.com, go to **Management** > **Devices**, and then click **Resources**.

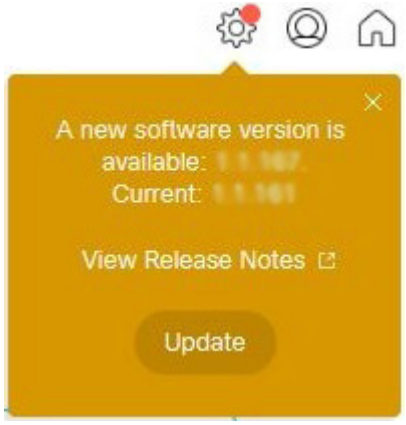
Step 2 Scroll to **Tools**, click **Download**, and then choose **Download for Mac** or **Download for Windows**, depending on your platform.

Step 3 Open the installer file and then choose one, depending on your platform:

- For Windows:
  1. **a.** Click **Next**, check the box to accept the terms in the License Agreement, and then click **Next**.
  2. **b.** Optionally, change the destination folder or leave the default, and then click **Next**.
  3. **c.** Click **Install**, and then the setup wizard installs the software.
- For Mac:
  1. **a.** Read the introduction and then click **Continue**.
  2. **b.** Click **Continue** and then click **Agree** to accept the software license.
  3. **c.** Choose the disk where you want the software to be installed, and then click **Continue**.
  4. **d.** Optionally, click **Change Install Location** if you want to install the software somewhere else; otherwise, click **Install**.
  5. **e.** After the screen appears that says the software installed successfully, click **Close**.

What to do next

- You're ready to sign into the connector with your full or device admin credentials. You can then run the software manually to synchronize your devices. This step is only required once to sync the configuration changes.
- You're notified in the software whenever an upgrade is available. We recommend that you click **Update** to remain on the latest version of the software for bug fixes and security enhancements:



Synchronize device configuration changes with Webex Device Connector

Whenever you make changes to configuration on Unified CM (premises) or to Workspaces and Personal Mode devices in Control Hub (the cloud), you can run the Webex Device Connector to make sure the changes on both sides are synchronized and Webex devices continue to function properly with Hybrid Calling. The software synchronizes the SIP address, Workspace name, and device information into the cloud.

Note You only need to run Webex Device Connector as and when you need to take an action, such as completing all required config on Unified CM and in the cloud, then needing to synchronize the two together.

Before you begin

Make sure you download the software from Control Hub and install it on a supported Mac or Windows system.

Step 1 Open the Webex Device Connector.

Step 2 (Optional) Check **Remember Me** if you want the software to save your credentials so that you don't have to reenter them.

After you check this box, we securely store the refresh token for the account locally on the machine. You can remove this token any time by signing out of the application or uninstalling the application.

Step 3 Sign in with your full admin credentials (the same ones that you use for Control Hub).

Step 4 Click **Hybrid Calling**, and then enter the following information to connect to the Unified CM:

- **Host**—Enter the IP address or FQDN of the Unified CM.
- **Username** and **Password**—Enter credentials for a Unified CM application account that is enabled for AXL.

Step 5 Click **Connect**.

The connector loads all of the Workspaces that are enabled for Hybrid Calling. For each Workspace, the connector finds a matching end user account (mail ID), directory number, and Cisco Spark-RD on Unified CM.

Step 6 Enter terms in the **Search for devices** field or use a filter (for example, **Ready to sync**) to limit the number of devices that appear in the results.

If you chose one filter but want to change to a different one, click X next to the filter name and then choose the new filter that you want to use.

Step 7 If the tool flags any mismatches in the premises and cloud configuration, resolve the configuration issue (typically in Cisco Unified CM Administration), return to the tool and click **Refresh List**. When you verify that the configuration issue is resolved, run a synchronization (click **Sync** next to one device or click **Sync All** for multiple devices) to match configuration on both sides.

- From cloud to Unified CM, the remote destination of the Cisco Spark-RD in Unified CM is automatically updated with any cloud Webex SIP address change.
- From Unified CM to cloud, relevant configuration (directory number, extension, home cluster, and so on) is associated with Webex devices in a Workspace.

Note For any configuration issues (for example, a matched user account but missing directory number), use the error messages in the tool to help you resolve configuration on Unified CM and then rerun a sync afterwards.

What to do next

If you need to synchronize changes on other Unified CM clusters, you can click **Connect to different Unified CM** and enter the host, username, and password for that Unified CM.

Known issues and limitations with Hybrid Calling for Webex devices

Workspaces

- When you configure Webex devices with Hybrid Call Service, you first configure a URI while creating your directory number. Then, when the Workspace is activated, a second URI is created and assigned to the directory number. The new URI is the same as the original, but in a different partition. The end result is that the directory number has two (almost identical) URIs configured in Unified CM.
- The Webex SIP address for Webex devices is generated from the Workspace name. If this name is changed after you enable the devices with Hybrid Call Service, the remote destination (the Webex SIP address) in the Cisco Spark-RD on Unified CM is not updated. You must rerun the Webex Device Connector to synchronize this cloud configuration change down to the Unified CM.
- Calling another Webex App device (with Hybrid Calling) by extension is not supported.

- Calling another Webex App device (with Hybrid Calling) by directory URI is not supported. Use the suggestion in Create a directory number and directory URI for Webex devices with Hybrid Calling, on page 27 as a workaround.

  For more information, see the Loop Detection and Avoidance section in the *Preferred Architecture for Cisco Webex Hybrid Services*.

- Whether the device has Hybrid Calling or not, calling a Webex App device by name or directory lookup is only supported within the same organization.

Personal Mode devices

- Enterprise directory URIs cannot be dialed from a Personal Mode device.

Mobile and Remote Access (MRA)

If you also have MRA deployed, see "Unsupported Expressway Features and Limitations" in the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* for your release at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.