Prepare Your Environment

- Requirements for Hybrid Calling, on page 1
- High Availability, on page 4
- Custom Certificates for Mutual TLS Authentication between Expressway-E and the Cloud, on page 4
- Complete the Prerequisites for Hybrid Calling, on page 5
- Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services, on page 9
- Cisco Spark Remote Device Overview and License Requirements, on page 13

Requirements for Hybrid Calling

Cisco Webex Teams License Requirements

To deploy Hybrid Call Service and provide its features to your users:

- You must have a Cisco Webex organization with a paid subscription.
- Cisco Webex Teams hybrid call users must be assigned a paid license that provides access to core Cisco Webex messaging and meeting services.
- The paid user licenses must not provide Cisco Webex hybrid call users access to a non-Unified CM-based calling service, such as Cisco Webex Calling (Formerly Spark Call).

Unified CM Device Requirements

Hybrid Call Service is supported only with Cisco SIP phones and Cisco Jabber clients that are registered to Unified CM.

SCCP phones may encounter problems due to the 48-character limitation on the destination address. Third-party IP phones and clients registered to Unified CM are not supported, neither are IP phones and clients registered to other call control servers (such as Cisco VCS/Expressway, Cisco Meraki, Microsoft Lync/Skype for Business, BroadSoft/BroadWorks).
Cisco Call Control Solution Requirements

To enable Hybrid Calling, you must use one of the supported Unified CM-based Cisco call control solutions, and ensure that you’re on the minimum supported version or later.

Table 1: Cisco Call Control Requirements

<table>
<thead>
<tr>
<th>Unified-CM Based Call Control Solution</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager</td>
<td></td>
</tr>
<tr>
<td>Supported Cisco Spark Remote Device (Cisco Spark-RD) releases are required for Hybrid Calling deployments.</td>
<td></td>
</tr>
<tr>
<td><strong>Releases with Cisco Spark Remote Device Support</strong></td>
<td></td>
</tr>
<tr>
<td>• 11.5(1)SU3 and later; we recommend the latest SU release.</td>
<td></td>
</tr>
<tr>
<td><strong>Releases with Session Management Edition (SME) support</strong></td>
<td></td>
</tr>
<tr>
<td>• 12.0(1) and later; we recommend the latest release.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The leaf clusters that are connected to the SME cluster do not have to be on release 12.0(1)</td>
<td></td>
</tr>
<tr>
<td>Cisco Business Edition</td>
<td></td>
</tr>
<tr>
<td>Check the software load summary documentation for BE6K and BE7K to ensure the solution is running a supported version of Unified CM.</td>
<td></td>
</tr>
<tr>
<td>Cisco Hosted Collaboration Solution (check to see if your provider is offering Cisco Webex Hybrid Services)</td>
<td>11.5 and later</td>
</tr>
</tbody>
</table>

Cisco Expressway Requirements

You must deploy Expressway to host the connectors. Organizations using Cisco Hosted Collaboration Solution do not need Cisco Expressway on their premises. Instead, their Hosted Collaboration Solution partner will deploy it in the cloud as part of their Cisco Webex Hybrid Services offering.

Table 2: Cisco Expressway Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Cisco Webex Teams App Requirements

Cisco Webex hybrid call users must download the Cisco Webex Teams app for a supported platform from [https://www.webex.com/downloads.html](https://www.webex.com/downloads.html).

Hybrid Calling is supported on Cisco Webex Teams for Windows, Mac, and mobile (Android and iOS). The web client is not supported.

### Network Requirements

- Port access for HTTPS or secure web sockets outbound from Expressway to *.rackcdn.com, *.wbx2.com, *.webex.com, *.ciscospark.com, and *.clouddrive.com: TCP port 443 (secure)
- For AXL queries from Call Connector to Unified CM, TCP port 8443.
- Open the following ports for media traversal between phones, Expressways in the traversal pair, and the Cisco Webex cloud:

### Cisco Expressway E and C Traversal Pair (for hybrid call traffic)

| | X8.11.4 or later is required for Hybrid Calling. See the “Important Information” section in the Expressway Release Notes for more information. This release provides added security and toll fraud mitigation. Hybrid Calling calls are classified the same as Mobile Remote Access (MRA), Business-To-Business (B2B) calls, and the calls traverse existing Expressway C and E pairs.  
|---|---|
| - Calls that include *.webex.com in the route path do not count towards the traversal license cost.  
- Any B2B calls for a Cisco Webex Teams app after anchoring on the Cisco Spark-RD and then routing back out through the Expressways will consume traversal licenses.  
Hybrid Calling follows existing MRA and B2B preferred architecture planning recommendations.  
- Determine the total number of concurrent MRA, B2B, and Call Service Connect calls  
- Deploy the appropriate number of Expressway E/C pairs  
- There is no dedicated Expressway C or E required for Hybrid Calling traversal. |  
| | You can download the software image from [software.cisco.com](http://software.cisco.com) at no charge.  
We recommend the latest released version of Expressway for connector host purposes. See [Expressway Connector Host Support for Hybrid Services](https://www.webex.com/downloads.html) for more information about which versions are supported for new and existing registrations to the cloud.  

### Cisco Expressway Connector Host (for hosting software connectors)
Table 3: Media Traversal Port Requirements for Hybrid Calling

<table>
<thead>
<tr>
<th>Client</th>
<th>Destination</th>
<th>Ports</th>
<th>Protocol</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expressway traversal pair</td>
<td>Any</td>
<td>36000–59999</td>
<td>UDP</td>
<td>SIP media between phones and Expressways. Open these ports on the Expressways themselves.</td>
</tr>
<tr>
<td>Cisco Webex Teams app</td>
<td>Any*</td>
<td>33434–33598</td>
<td>TCP/UDP</td>
<td>Cisco Webex Hybrid Services media.</td>
</tr>
</tbody>
</table>

* If you want to restrict by IP addresses, see the IP address ranges that are documented in Webex Teams IP subnets for media.

Other Network Requirements

We recommend that you implement network requirements that are covered in the following documents:

- Network Requirements for Cisco Webex
- Network Requirements for Webex Teams Services

High Availability

For Hybrid Call, if each cluster contains at least two nodes, the cluster has high availability by default. The total number of onboarded users is affected by high availability. On each connector host in a cluster, a different user number is shown. Take the sum total and divide it by two to get an accurate total of your users. You can also verify this total in Cisco Webex Control Hub (https://admin.webex.com) by choosing the applicable cluster under Services > All Resources > View all.

For more information about how each Expressway-based Hybrid Service ensures continuous service to users, see User Capacity Limits for Expressway-Based Hybrid Services.

Custom Certificates for Mutual TLS Authentication between Expressway-E and the Cloud

For extra security, you might want your Expressway to communicate with the cloud through certificates that were signed by a certificate authority (CA).

If your Expressway-E SIP TLS certificate was signed by a private certificate authority (or a certificate authority that is not trusted by the Cisco Webex default trust list—see the links below), then you can upload the certificate authority's root certificate to your organization's custom trust list on the Services > Hybrid Call > Settings page.

- To use a custom certificate, you must verify any domain that is used in your organization. Any verified domains must be present on the Expressway-E certificate as a subject alternate name (SAN).
- When a SIP-TLS transaction takes place between the Cisco Webex cloud and your Expressway-E, the cloud analyzes the domains that are listed in your Expressway-E SAN list. The cloud then checks if the domain in the SAN has been verified by the organization. If the check fails, the TLS connection will terminate.
• If the Expressway-E certificate does not contain your domain as a SAN, or if you did not verify the domain, the cloud cannot identify which certificate store to use. The result is that TLS negotiations fail, even if you have supplied the correct certificates on the Services > Hybrid Call > Settings page.

**Certificate Revocation Lists**

If your private certificate authority inserts a certificate revocation list (CRL), ensure that the CRL locations are reachable from the public internet. If a CRL is present but not reachable, the Cisco Webex cloud cannot verify whether the certificate was revoked.

In this case, the certificate must not try to access a CRL.

**Related Topics**

Add, Verify, and Claim Domains  
Supported Certificate Authorities for Cisco Webex

---

**Complete the Prerequisites for Hybrid Calling**

Use this checklist to prepare your call control environment for Hybrid Calling. Address these items in advance to ensure a smooth deployment of Hybrid Calling and activation of your Cisco Webex Teams users.

**Procedure**

**Step 1**  
Allow extra time to prepare these items:

• Determine your certificate trust method. You can use manual or automatic upload; see Supported Certificate Authorities for Cisco Webex for more information.

• Verify your identity by registering all the domains that are used to form your users' directory URIs and email addresses. Ensure that the subject alternative names (SANs) belong to the domains that are registered on your Cisco Webex organization.

See Why the Cloud Checks Domain Ownership to understand why domain checks are an important security measure.

• Install or upgrade to a supported version of Cisco Unified Communications Manager, as described in Requirements for Hybrid Calling, on page 1

• Prepare your Expressway-Es (default SIP Destination and cluster-specific SIP destinations for each location) for the secure mutual TLS connection between Cisco Webex and your call control environment:

  • An SRV record (multiple Expressway-Es for redundancy) is recommended for large deployments:
    
    • You cannot reuse an existing SRV; allow the time to request a dedicated SRV for Hybrid Calling and use port 5062. The SRV record resolves into Expressway-E A-records; the hostname is the A-record for Expressway-E.

    • Request that port 5062 be open on the enterprise firewall. This port is required to establish a mutual TLS connection between the premises and cloud.

    • Make sure that the port is open to and from the Internet.

    • Verify that the mutual TLS port is reachable by using a ping utility—for example, `telnet [domainname or ip] [port]` in a command prompt.
In a global Hybrid Calling scenario, you'll need one SRV record for each location (see Recommendations for Global Hybrid Calling Deployments, on page 8 for deployment options and accompanying diagrams). Note these guidelines for the SIP destinations.

- If you don't have time to request a dedicated SRV domain or have a small deployment, you can use FQDN:port or IP address:port to avoid blocking the rest of setup. Later, you can change to an SRV-based SIP destination if you prefer.

See TCP Port 5062 on the Internet Firewall for more information.

- Follow these Expressway pair requirements:
  - If you don't have an existing Expressway pair that is deployed, read the following documents (Release X8.11.4 and later) 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
  - Install or upgrade your Expressway pair that handles SIP traffic to a supported version, as described in Requirements for Hybrid Calling, on page 1. Use the recommended version for all Expressways that are handling SIP calls to take full advantage of Hybrid Calling.
  - For a global Hybrid Calling deployment, you must deploy one Expressway pair per location. See Recommendations for Global Hybrid Calling Deployments, on page 8 for deployment options and accompanying diagrams.

The Call Connector can run on a standalone or shared Expressway-C connector host, not the C or E in the Expressway pair. See Expressway Connector Host Support for Hybrid Services for the minimum supported version and User Capacity Limits for Expressway-based Hybrid Services for capacity planning guidelines.

You can use an Expressway pair that's already configured for B2B or MRA deployments. You cannot use a Jabber Guest Expressway pair to handle Hybrid Calling calls.

**Step 2**

Follow these Cisco Unified Communications Manager requirements:

- Install or upgrade your Cisco Unified Communications Manager to the minimum version that supports Cisco Spark-RD, as described in Requirements for Hybrid Calling, on page 1.
- Prepare your licensing. (See Cisco Spark Remote Device Overview and License Requirements, on page 13)
- On the Unified CM, configure Directory URIs in one or both of the following ways, depending on your deployment:
  - Intracluster routing for intracluster routing in single cluster and multicluster deployments.
  - Intercluster lookup service (ILS) routing for multicluster and business-to-business deployments.
- Check your codec configuration.

Cisco Webex supports the following codecs:

- Audio—G.711, G.722, AAC-LD
• Video—H.264

Note We support G.729 when users join a Webex meeting, Personal Room meeting, or Cisco Webex meeting from a SIP device. We do not support G.729 when a user dials 1:1 from Cisco Webex to a SIP device or bridge.

• Configure the following settings to be used for Cisco Spark-RD creation:
  • Device pools
  • Locations
  • Calling search spaces

Note The calling search space must be able to route to partition of the PSTN gateway or trunk, and any other destinations that you want Cisco Webex Teams users to be able to reach (conference bridges, enterprise-to-enterprise trunks, and so on).

• Note these values. You will use them when you create each Cisco Spark-RD.

Step 3 Provide port access (for media traversal between phones, Expressways, and the Cisco Webex cloud), as covered in the Network Requirements, on page 3.

Step 4 For all existing SIP trunks between Cisco Unified Communications Manager clusters, go to Device > Trunk, open the trunk settings, and set the Calling and Connected Party Info Format to Deliver URI and DN in connected party.

Step 5 Enable the AXL Web Service on at least one node in the cluster (the bootstrap server, which can be the publisher or subscriber node of a cluster).

We recommend that you enable AXL Web Service on at least two nodes in the cluster.

Step 6 Ensure that Cisco CallManager Serviceability is enabled on at least one node in the cluster. This service is enabled by default and is used to discover nodes where the AXL Web Service is enabled.

Step 7 (Optional) Download the latest Cisco Directory Connector software from Cisco Webex Control Hub (https://admin.webex.com) and use it to import user attributes from your Active Directory:
  • Enterprise work phone numbers
  • Email addresses—These values must match the user's Cisco Webex Teams user email address.

For more information about how to use Cisco Directory Connector, see the Deployment Guide for Cisco Directory Connector.

Things to Keep in Mind

To support user-friendly mobile and web dial plans, Cisco Webex performs digit manipulation for US and Canadian locales before sending the dialed digit to enterprise call control. Cisco Webex transforms a national PSTN number (for example, convert (214) 555-2121 into +12145552121), but does not transform a private extension number. A valid national number is converted to E.164 format for Cisco Webex Teams users that are based in the US or Canada. For other locales, a minimal conversion takes place that removes everything but digits and the symbols +, *, and #. See the Dial Plans chapter in the Cisco Collaboration System Solution Reference Network Designs (SRND) guide for information about the role of dial plans and digit manipulation.
Recommendations for Global Hybrid Calling Deployments

**Distributed Unified CM Call Control**

See the following diagram for an example of a global deployment with SIP destinations associated with each Call Connector cluster and geographically distributed Unified CM clusters.

**Recommended Deployment for Distributed Unified CM**

- An Expressway-C/E cluster is required for each location (US, EMEA, and so on). Create a SIP mutual TLS SRV pointing at each cluster.
- The local Call Connector pulls in users from local Unified CM and searches for a user for calls outbound from the cloud across all connectors.

*Figure 1: Cloud, On-Premises, and Connector Components for Multiple SIP Destinations and Distributed Unified CM Call Control for a Hybrid Calling Deployment*

---

**Centralized Unified CM Call Control**

See the following diagram for an example of a global deployment with SIP destinations associated with each Call Connector cluster and a centralized Unified CM call control solution. If you are designing this architecture, we recommend that you deploy dedicated Hybrid Connector Expressways with Call Connector for each geography or site.

---

**Note**

Deploy all Expressway connector hosts at the same site as the centralized Unified CM cluster to minimize AXL latency.

**Recommended Deployment for Centralized Unified CM**
Complete the Expressway-C Connector Host Prerequisites for Cisco Webex Hybrid Services

Use this checklist to prepare an Expressway-C for Cisco Webex Hybrid Services, before you register it to the Cisco Webex cloud to host hybrid services connector software.

Before you begin

We recommend that the Expressway-C be dedicated to hosting connectors for Cisco Webex Hybrid Services. You can use the Expressway-C connector host for other purposes, but that can change the supported number of users.

See User Capacity Limits for Expressway-based Hybrid Services so that you can plan your deployment accordingly.

As an administrator of hybrid services, you retain control over the software running on your on-premises equipment. You are responsible for all necessary security measures to protect your servers from physical and electronic attacks.
Procedure

Step 1  Obtain full organization administrator rights before you register any Expressways, and use these credentials when you access the customer view in Cisco Webex Control Hub (https://admin.webex.com).

Step 2  Plan your connector capacity by referring to User Capacity Limits for Expressway-based Hybrid Services.

Step 3  Deploy the Expressway-C connector host in a cluster to account for redundancy. Follow the supported Expressway scalability recommendations:

- For Hybrid Call Service on a dedicated Expressway-C:
  - Call Connector supports multiple Expressway-C clusters with no specific upper limit.
  - Each cluster supports up to 6 Expressway-C nodes for active/active redundancy.

Hybrid Calling is highly available if Unified CM and Cisco Expressways are deployed in a cluster. The same guidelines apply for the Expressway-C connector host clustering. For more information, see User Capacity Limits for Expressway-Based Hybrid Services.

Step 4  Follow these requirements for the Expressway-C connector host.

- Install the minimum supported Expressway software version. See the version support statement for more information.
- Install the virtual Expressway OVA file according to the Cisco Expressway Virtual Machine Installation Guide, after which you can access the user interface by browsing to its IP address. You can find the document in the list of Cisco Expressway Install and Upgrade Guides on cisco.com.

Note  The serial number of a virtual Expressway is based on the virtual machine's MAC address. The serial number is used to validate Expressway licenses and to identify Expressways that are registered to the Cisco Webex cloud. Do not change the MAC address of the Expressway virtual machine when using VMware tools, or you risk losing service.

- You do not require a release key, or an Expressway series key, to use the virtual Expressway-C for Cisco Webex Hybrid Services. You may see an alarm about the release key. You can acknowledge it to remove it from the interface.
- Use the Expressway web interface in a supported browser. (See the Cisco Expressway Administrator Guide.) The interface may or may not work in unsupported browsers. You must enable JavaScript and cookies to use the Expressway web interface.

Step 5  If this is your first time running Expressway, you get a first-time setup wizard to help you configure it for Cisco Webex Hybrid Services.

Select Cisco Webex Hybrid Services. This ensures that you will not require a release key.

Step 6  Check that the following requirements are met for the Expressway-C connector host. You would normally do this during installation. See the Cisco Expressway Basic Configuration Deployment Guide, in the list of Cisco Expressway Configuration Guides on cisco.com, for details.

- Basic IP configuration (System > Network interfaces > IP)
- System name (System > Administration settings)
- DNS settings (System > DNS)
- NTP settings (System > Time)
• New password for admin account (Users > Administrator accounts, click Admin user then Change password link)
• New password for root account (Log on to CLI as root and run the passwd command)

**Note** Expressway-C connector hosts do not support dual NIC deployments.

**Step 7** Configure the Expressway-C as a "cluster of one":

• We recommend that you configure the Expressway as a primary peer before you register it, even if you do not currently intend to install an extra peer.

  **Caution** When you change clustering settings on X8.11 and later, be aware that removing all peer addresses from the System > Clustering page signals to the Expressway that you want to remove it from the cluster. This causes the Expressway to factory reset itself on its next restart. If you want to remove all peers but keep configuration on the remaining Expressway, leave its address on the clustering page and make it the primary in a "cluster of one".

• Here are the minimum clustering settings required, but the Cisco Expressway Cluster Creation and Maintenance Deployment Guide has more detail:


    **Note** You may not see the H.323 menu item if you used the Service Select wizard to configure the Expressway for Hybrid Services. You can work around this problem by signing in to the Expressway console and issuing the command `xconfig H323 Mode: "On"`.

  - **System > Clustering > Cluster name** should be an FQDN. Typically this FQDN is mapped by an SRV record in DNS that resolves to A/AAAA records for the cluster peers.

  - **System > Clustering > Configuration primary** should be 1.

  - **System > Clustering > TLS verification mode** should be Permissive, at least until you add a second peer.

    Select Enforce if you want cluster peers to validate each others' certificates before allowing intercluster communications.

  - **System > Clustering > Cluster IP version** should match the type of IP address of this Expressway-C.

  - **System > Clustering > Peer 1 address** should be the IP address or FQDN of this Expressway

    Each peer FQDN must match that Expressway's certificate if you are enforcing TLS verification.

  **Caution** To ensure a successful registration to the cloud, use only lowercase characters in the hostname that you set for the Expressway-C. Capitalization is not supported at this time.

**Step 8** If you have not already done so, open required ports on your firewall.

• All traffic between Expressway-C and the Cisco Webex cloud is HTTPS or secure web sockets.
• TCP port 443 must be open outbound from the Expressway-C. See https://collaborationhelp.cisco.com/article/WBX000028782 for details of the cloud domains that are requested by the Expressway-C.
**Step 9**

Get the details of your HTTP proxy (address, port) if your organization uses one to access the internet. You'll also need a username and password for the proxy if it requires basic authentication. The Expressway cannot use other methods to authenticate with the proxy.

- We tested and verified Squid 3.1.19 on Ubuntu 12.04.5.
- We have not tested auth-based proxies.

**Note**

If your organization uses a TLS proxy, the Expressway-C must trust the TLS proxy. The proxy's CA root certificate must be in the trust store of the Expressway. You can check if you need to add it at Maintenance > Security > Trusted CA certificate.

**Note**

The details of the proxy, as configured on the primary Expressway in the connector host cluster, are shared throughout the Expressway cluster. You cannot configure different proxies for different nodes in the cluster.

**Step 10**

Review these points about certificate trust. You can choose the type of secure connection when you begin the main setup steps.

- Cisco Webex Hybrid Services requires a secure connection between Expressway-C and Cisco Webex. You can let Cisco Webex manage the root CA certificates for you. However, if you choose to manage them yourself, be aware of certificate authorities and trust chains; you must also be authorized to make changes to the Expressway-C trust list.

---

**Management Connector**

The Management Connector is included in the Expressway-C base. You use it to register an Expressway to the cloud and link the Expressway interface with Cisco Webex Control Hub. The Management Connector plays an important role as the coordinator of all connectors running on the Expressway server or cluster: It provides you with a single point of control for connector activities. The Management Connector enables cloud-based management of the on-premises connectors, handles initial registration with the cloud, manages the connector software lifecycle, and provides status and alarms.

For an HTTPS connection to be established between the Management Connector and the cloud, you must update the trust list on the Expressway-C connector host with certificates that were signed by certificate authorities in use by the Cisco Webex cloud. You can allow the Cisco Webex cloud to upload CA certificates to the Expressway-C trust store. Or, in the case where security policies prevent the Cisco Webex cloud from uploading trusted certificate authority certificates on Expressway-C, you may upload them manually.

**Call Connector**

The Call Connector is the on-premises component Hybrid Call Service. The connector runs on a dedicated or shared Expressway-C connector host that you register to the Cisco Webex cloud.

Hybrid Call Service use the Call Connector software that runs as a module within Cisco Expressway. Call Connector uses AXL APIs to discover user devices configured in Cisco call control.

Call Connector also creates or updates a virtual remote device that represents Cisco Webex within Cisco call control. Hybrid Call Service uses this remote device to extend calls to Webex Teams, and to allow calls from Webex Teams to be identified with the calling user. In addition, Hybrid Call Service requires a Cisco
Expressway firewall traversal solution to enable these calls between Webex Teams and your existing call control.

Note

SIP traffic to and from the cloud is not routed to the same Expressway-C on which Call Connector runs. The Call Connector provisions aspects of users and their devices, but does not handle the calls themselves.

The Call Connector acts like a broker between the cloud and your on-premises call control environment (Cisco Unified Communications Manager, Business Edition 6000/7000, or Hosted Collaboration Solution). The connector establishes a secure connection and, in addition to securely connecting your on-premises environment to the cloud, the connector is used to:

- Discover users’ telephony devices and associated settings.
- Provide active/active redundancy if you configure the connector on a second Expressway-C.
- Provide automatic load balancing of users across different Expressway-C connector clusters (1 cluster with 2 nodes)—no manual administration is required.
- Retrieve users’ Directory URIs from Cisco Unified Communications Manager and makes them available to Cisco Webex for reaching users.
- Automatically create Cisco Spark Remote Device (Cisco Spark-RD) with a basic configuration for each user enabled for Hybrid Calling.
- Configure a user's Cisco Spark-RD with a Webex SIP address automatically created as the remote destination (for Hybrid Calling).
- Builds a table that the user directory URIs to cluster fully qualified domain names (FQDN) in a multi-cluster scenario.
- Does a lookup to add the correct route header information to the SIP message.

Cisco Spark Remote Device Overview and License Requirements

To activate Cisco Webex Hybrid Calling for a user, you must create a virtual device for that user in Unified CM. The device ties in with the user's remote destination so that incoming calls are forked to both Webex Teams and the user's main device. Outgoing calls can be made from the app as if from the user's desk phone, too.

The Cisco Spark Remote Device (Cisco Spark-RD) is a dedicated and fully compatible virtual device for Hybrid Calling’s functional requirements and behaviors. Cisco Spark-RD provides the following features:

- Remote Destination (Cisco Webex SIP address) length can be greater than 48 characters
- Does not require an MTP for calls
- Does not require IOS-MTP passthrough for video or screen share capability

A standalone Cisco Spark-RD uses one Enhanced UCL. If a user has any other UC device that requires an Enhanced UCL, then Cisco Spark-RD does not count towards the license total.
Use this table to understand the license requirements for Cisco Spark-RD for Unified CM or HCS.

**Table 4: License Requirements for Cisco Spark-RD**

<table>
<thead>
<tr>
<th>Device</th>
<th>License Requirement for Unified CM or HCS</th>
</tr>
</thead>
</table>
| Cisco Spark-RD alone | • Enhanced UCL for Unified CM  
• HCS Foundation |
| Cisco Spark-RD plus desk phone | • Enhanced UCL for Unified CM—A Basic UCL must be upgraded to Enhanced UCL.  
• HCS Foundation |
| Cisco Spark-RD plus 2 desk phones | • Enhanced Plus UCL for Unified CM  
• HCS Standard |
| Cisco Spark-RD plus Hybrid Call for Cisco Webex (Room, Desk, and Board) Devices in a Place | Enhanced UCL—For a newly deployed system, this license must be provided.  
For a Webex device that is converted from Unified CM-registered to Cisco Webex-registered, its existing Unified CM license is sufficient. |