




Manage and troubleshoot Hybrid Calling for Webex Devices

- [Rename a Workspace enabled for Hybrid Calling, on page 1](#)
- [Override the default SIP destination for a Workspace, on page 2](#)
- [Remove Hybrid Calling from Webex device, on page 3](#)
- [Deactivate Hybrid Calling for Webex Devices, on page 4](#)
- [Troubleshooting sources for Hybrid Calling, on page 4](#)
- [Webex status page, on page 6](#)
- [Mutual TLS and SIP destination, on page 6](#)
- [Expressway pair configuration, on page 7](#)
- [Unified CM configuration, on page 7](#)

Rename a Workspace enabled for Hybrid Calling

You can change the name of a Workspace that you configured with Hybrid Calling. This action updates the Webex SIP address, and further steps are required to synchronize the change on the premises. Use this procedure to change the name and verify the changes.

-
- Step 1** From the customer view in <https://admin.webex.com>, go to **Management > Workspaces**, and then choose a Workspace from the list to open the overview panel.
- Step 2** To the right of the Workspace name, click  **Edit**, enter the new name for the Workspace, and then click **Save**.
- Step 3** Under **Calling**, verify that the Webex SIP address is updated.

Override the default SIP destination for a Workspace

Next, you must run the Webex Device Connector manually, so that these changes are replicated to Unified CM as the updated remote destination for each Cisco Spark-RD.

- Step 4** Open the Webex Device Connector, choose **Hybrid Calling**, and then sign into the Unified CM with an administration account with AXL permissions.
- Step 5** From the list, click **Sync** next to the devices to run the synchronization step and match the premises configuration to the cloud configuration.
- Step 6** Verify that the remote destinations were synchronized correctly from the cloud to the premises: From Cisco Unified CM Administration, go to **Device > Remote Destination**, choose **CTI Remote Device/Cisco Spark Remote Device** from the **Find destination where** drop down, and then click **Find**.

The results show each Cisco Spark-RD in your deployment and the remote destination (under **Destination Number**. If the name was updated correctly, the Cisco Spark-RD for the Workspace has a remote destination that starts with the new Workspace name that you saved in Control Hub.

| Remote Destination (1 - 18 of 18) | | | | | | |
|--|------------------------------------|----------------------------|-----------------|-----------------------|---|--|
| Find Remote Destination where CTI Remote Device/Cisco Spark Remote Device contains | | | | | | |
| Name | Destination Number | Remote Destination Profile | Dual-Mode Phone | DNS-Integrated Mobile | CTI Remote Device/Cisco Spark Remote Device | |
| <input type="checkbox"/> Cisco_Spark_Client | place1@example.room.ciscospark.com | | | | SparkRDplace1 | |

Override the default SIP destination for a Workspace

After you add a default SIP destination for Hybrid Calling, you can add more SIP destinations to Workspaces in Control Hub. A single default SIP destination means that all of the hybrid call traffic goes through a single Expressway-E or DNS SRV entry. You may want to add more SIP destinations to override the default entry that you configure in Hybrid Call settings, so that you have more control over where the hybrid call traffic for Workspaces is routed.

Before you begin

[Recommendations for global Hybrid Calling deployments](#)

Step 1 From the customer view in <https://admin.webex.com>, go to **Management > Workspaces**, and then search for and open the Workspace that you want to configure.

Step 2 Click **Edit Hybrid Calling**, choose **Configure a SIP Destination for the workspace**, 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 3 Click **Test** to run a tool in Control Hub that checks the connection to the Expressway-E SIP destination you entered.

The tool initiates a TLS connection to the SIP destination 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 4 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 \(Control Hub\)](#), on page 5 for more information.

Step 5 Save your changes.

Remove Hybrid Calling from Webex device

Use this procedure to remove Hybrid Calling from a single workspace that contains a Webex device. This step converts a device in a Workspace to free calling (SIP calling) and disables Unified CM-based calling functionality.

Before you begin



Note This step affects individual Workspaces. If you want to remove Hybrid Calling from all enabled Workspaces in your organization, use the steps in [Deactivate Hybrid Calling for Webex Devices](#), on page 4

Step 1 From the customer view in <https://admin.webex.com>, go to **Management > Workspaces**, search for the Workspace enabled for Hybrid Calling, and then open it.

Step 2 Next to **Calling**, click , choose **Call on Webex (1:1 Call, Non-PSTN)** (default), and then click **Save**.

This step does not delete the Workspace in Control Hub or the Cisco Spark-RD in Unified CM. This step removes Hybrid Calling functionality from the Webex devices in the Workspace. Any devices in the remaining Workspace can still support the features that come with free calling, specifically SIP dialing and pairing to the Webex App. The Cisco Spark-RD remains on Unified CM; you must manually remove that device if you want to clean up that configuration.

Deactivate Hybrid Calling for Webex Devices

Use these steps to remove Hybrid Calling from all Webex devices in Workspaces in your Control Hub-managed organization. Deactivating the service does not remove the cloud-registered devices, but the step downgrades all devices to free calling (SIP calling) and disables Unified CM-based calling functionality.

Before you begin



Note This step affects all devices in a Workspace. If you only want to remove Hybrid Calling from individual devices, use the steps in [Remove Hybrid Calling from Webex device, on page 3](#).

Step 1 From the customer view in <https://admin.webex.com>, go to **Services > Hybrid**, and then click **Edit settings** from the Hybrid Call card.

Step 2 Scroll to **Deactivate Hybrid Call Service**, and then click **Deactivate**.

Step 3 Read the prompt that appears, and click **Deactivate** when you understand that the service is removed after this step.

Step 4 Go to **Workspaces**, open a few Workspace entries, and confirm that Hybrid Calling was removed.

Troubleshooting sources for Hybrid Calling

This section covers the various information sources and tools that you can use to troubleshoot your Hybrid Calling for Webex devices deployment.

If you go through the troubleshooting information in this chapter and are still having trouble, you can access more advanced troubleshooting steps in the [Troubleshooting Guide for Cisco Webex Hybrid Call Service](#). You can also access the known issues and limitation lists in this guide.

Hybrid connectivity test tool (Control Hub)

You can access the Hybrid connectivity test tool from Control Hub: from the customer view in <https://admin.webex.com>, go to **Services > Hybrid**, click **Edit settings** in the Hybrid Call card, scroll to **Default SIP Destination**, and then click **Test** next to the SIP destination that you entered.

This table lists common errors that may appear after you test a SIP destination address for Hybrid Calling. The table also provides some next steps for troubleshooting, including links to relevant details in the [Troubleshooting Guide for Hybrid Call Service](#).

Table 1: Common errors and troubleshooting steps for testing a SIP destination address for Hybrid Calling

| Error | Keyword | More Information and Troubleshooting Steps |
|------------------------|-------------------------------|---|
| No DNS addresses found | DNS SRV | DNS Lookup failed. Check that a DNS or SRV record exists for your SIP Destination and that it resolves to one or more valid IP addresses. See Unable to resolve the Expressway-E DNS SRV/hostname in the troubleshooting guide for more information. |
| Connection timed out | Socket failure | Network and/or Mutual TLS connection timed out. Check network connectivity, connection speed, firewall configuration, and Mutual TLS configuration. See these sections of the troubleshooting guide for more information: <ul style="list-style-type: none"> • Socket Failure: Port 5062 is Blocked Inbound to Expressway • Socket Failure: Expressway-E is not Listening on Port 5062 |
| TLS failure | Mutual TLS handshake failures | Mutual TLS Error: Check Mutual TLS configuration in both Expressway and https://admin.webex.com , and that Mutual TLS certificates are present and valid in both locations. See Mutual TLS Handshake Failures in the troubleshooting guide for more information. |
| Connect failure | Socket failure | TCP Connection failure: Check network connectivity, connection speed, and/or firewall configuration. See these sections of the troubleshooting guide for more information: <ul style="list-style-type: none"> • Socket Failure: Port 5062 is Blocked Inbound to Expressway • Socket Failure: Expressway-E is not Listening on Port 5062 |

| Error | Keyword | More Information and Troubleshooting Steps |
|------------------------|----------------|--|
| TCP read/write failure | Socket failure | <p>TCP read/write failure: Please try again. If the error persists, check network connectivity, firewall configuration, and Mutual TLS configuration.</p> <p>See these sections of the troubleshooting guide for more information:</p> <ul style="list-style-type: none"> • Socket Failure: Port 5062 is Blocked Inbound to Expressway • Socket Failure: Expressway-E is not Listening on Port 5062 |
| TCP Failure | Socket failure | <p>TCP failure: TCP read/write failure: Please try again. If the error persists, check network connectivity, firewall configuration, and Mutual TLS configuration.</p> <p>See these sections of the troubleshooting guide for more information:</p> <ul style="list-style-type: none"> • Socket Failure: Port 5062 is Blocked Inbound to Expressway • Socket Failure: Expressway-E is not Listening on Port 5062 |

Webex status page

If calls from Webex to your enterprise are not ringing on the enterprise side, walk through the points in this checklist to double-check your configuration.

Before you walk through these troubleshooting suggestions, see <https://status.webex.com> for the latest information on any cloud outages. From that status page, you can also subscribe to notifications.

Mutual TLS and SIP destination

Check these troubleshooting points related to the mutual TLS connection and certificates:

- Install the Webex cloud root certificate bundle on the Expressway-E.
- Configure a dedicated mutual TLS port on the Expressway-E.
- Configure a DNS zone for the cloud on the Expressway-E.
- Open the mutual TLS port number in your firewall—5062, which may not be open by default.
- Determine which root certificate option you are using in the Webex cloud—The option is used to verify your Expressway-E's SIP TLS certificate.
 - Default store—Is your Expressway-E certificate signed by one of the public authorities? If you are unsure, use the custom store option.

- Custom store—Is your Expressway-E certificate or its signer installed in the cloud? Does the certificate contain verified Expressway-E hostnames?

From the customer view in <https://admin.webex.com>, go to **Services > Hybrid > Hybrid Call > Settings**. Check these points that are related to your SIP destination that you set during the deployment process:

- The value points at your Expressway-E dedicated mutual TLS port.
- Try to connect to the *IP address:port*. (Multiple addresses if you configured an SRV.)
- If you configured an IP address or hostname, specify the mutual TLS port.
- If you used an SRV, ensure it is in the format *_sips._tcp.<domain you put in as SIP Destination>*.
- If you do not want to set up an SRV, you can enter *IP address:port* or *hostname:port* as your organization's SIP destination.

Expressway pair configuration

- If calls from Expressway-E to the cloud are failing and you're using the manual certificate management method, make sure you follow the steps in [Webex Root CA Certificate Update](#) and upload the IdenTrust certificate to your Expressway devices as soon as possible.
- For calls that route from Webex toward the enterprise, check the search history and network logs on the Expressway-E. This step helps you isolate the problem to either the cloud or the enterprise.
- If you reuse an existing B2B zone and search rules, consider creating dedicated zones and search rules instead. This setup avoids interference with existing zone settings for B2B/MRA, avoids routing loops, and makes troubleshooting easier.
- Check the search history and network logs on the Expressway-E. Verify that the SIP INVITE from the cloud arrives at the Expressway-E and matches the DNS zone that you configured for the cloud.
 - If the SIP INVITE does not arrive or match the configured DNS zone, then follow the route of the call toward the Unified Communications Manager. This step helps you find where the call is failing or lost.
 - See the mutual TLS troubleshooting checklist.
- Check the route header. Verify that it contains the cluster fully qualified domain name (FQDN) value that is configured under Unified Communications Manager enterprise settings and in the Expressway search rules. See this example route header and highlighted cluster FQDN:
 - Route: <sip:[Obfuscated];transport=tls;lr>, <sip:myucmcluster.example.com;lr>
 - In this example, the home cluster FQDN is **myucmcluster.example.com**.

Unified CM configuration

- Emails in Unified Communications Manager must exactly match the email (synchronized from Active Directory or from any other source) in the Webex cloud.

- Directory URIs must match any domains that you verified in your organization.
- [Check your codec configuration.](#)

Webex services support the following codecs:

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



Note We support G.729 for joining a Webex meeting, Personal Room meeting, or Webex App meeting from a SIP device. We do not support G.729 for dialing 1:1 from Webex App to a SIP device or bridge.

- On the home Unified Communications Manager cluster of the affected users, choose **System > Enterprise Parameters**; under **Clusterwide Domain Configuration**, check the cluster fully qualified domain name (FQDN) setting. The FQDN value that you used must follow these guidelines:

| FQDN Guideline | Description and Example |
|-------------------------------------|--|
| Multiple clusters | The entry must be unique for each cluster with Hybrid Calling—For example, <code>cluster1.example.com</code> , <code>cluster2.example.com</code> , and so on. |
| No wildcards | Do not use entries with wildcards, such as <code>*.example.com</code> or <code>example*.com</code> . |
| 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): <code>cluster1.example.com</code> <code>*.example.com</code> <code>example*.com</code> |
| 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 <code>*.example.com *.example.org</code> , add a unique, non-wildcard entry at the beginning of the field: <code>"cluster1.example.com *.example.com *.example.org"</code> |