Appendix

- Quality of Service, on page 1
- Allow Untrusted Certificates on Unified CM, on page 4

Quality of Service

Quality of Service Options

Use the following options to configure the quality of service for Webex Teams:

- Supported Codecs, on page 1
- Define a Port Range on the SIP Profile, on page 2
- Set DSCP Values, on page 2

Supported Codecs

<table>
<thead>
<tr>
<th>Type</th>
<th>Codec</th>
<th>Codec Type</th>
<th>Webex Teams for Mac</th>
<th>Webex Teams for Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>G.711</td>
<td>A-law</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>µ-law/Mu-law</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>G.722</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>G.722.1</td>
<td>24 kb/s and 32 kb/s</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>G.729</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>G.729a</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Opus</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Define a Port Range on the SIP Profile

The client uses the port range to send RTP traffic across the network. The client divides the port range equally and uses the lower half for audio calls and the upper half for video calls. As a result of splitting the port range for audio media and video media, the client creates identifiable media streams. You can then classify and prioritize those media streams by setting DSCP values in the IP packet headers.

<table>
<thead>
<tr>
<th>Type</th>
<th>Codec</th>
<th>Codec Type</th>
<th>Webex Teams for Mac</th>
<th>Webex Teams for Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video</td>
<td>H.264/AVC</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Step 1**  
Open the Cisco Unified CM Administration interface.

**Step 2**  
Select Device > Device Settings > SIP Profile.

**Step 3**  
Find the appropriate SIP profile or create a new SIP profile.

The SIP Profile Configuration window opens.

**Step 4**  
Specify whether you want common or separate port ranges for audio and video. If you are separating your audio and video port ranges, provide audio and video ports. Specify the port range in the following fields:

- **Start Media Port** — Defines the start port for media streams. This field sets the lowest port in the range.
- **Stop Media Port** — Defines the stop port for media streams. This field sets the highest port in the range.

**Step 5**  
Select Apply Config and then OK.

Set DSCP Values

Set Differentiated Services Code Point (DSCP) values in RTP media packet headers to prioritize Webex Teams traffic as it traverses the network.

Set DSCP Values on Cisco Unified Communications Manager

You can set DSCP values for audio media and video media on Cisco Unified Communications Manager. Webex Teams can then retrieve the DSCP values from the device configuration and apply them directly to the IP headers of RTP media packets.

---

**Restriction**  
Operating systems such as Microsoft Windows 7 or 10 have a security feature that prevents applications from setting DSCP values on IP packet headers. For this reason, you should use an alternate method for marking DSCP values, such as Microsoft Group Policy.

**Step 1**  
Open the Cisco Unified CM Administration interface.
Step 2  Select System > Service Parameters.

The Service Parameter Configuration window opens.

Step 3  Select the appropriate server and then select the Cisco CallManager service.

Step 4  Locate the Clusterwide Parameters (System - QOS) section.

Step 5  Specify DSCP values as appropriate and then select Save.

Set DSCP Values With Group Policy

If you deploy Webex Teams for Windows on an operating system such as Microsoft Windows 7 or later, you can use Microsoft Group Policy to apply DSCP values.

Complete the steps in the following Microsoft support article to create a group policy:


You should create separate policies for audio media and video media with the following attributes:

These directions apply to Unified CM calls that go through Webex Teams. For Webex Teams only calls, use the guidelines in Network Requirements for Webex Teams.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Audio Policy</th>
<th>Video Policy</th>
<th>Signaling Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>CiscoCollabHost.exe</td>
<td>CiscoCollabHost.exe</td>
<td>CiscoCollabHost.exe</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
<td>UDP</td>
<td>TCP</td>
</tr>
<tr>
<td>Port number or range</td>
<td>Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.</td>
<td>Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.</td>
<td>5060 for SIP</td>
</tr>
<tr>
<td>DSCP value</td>
<td>46</td>
<td>34</td>
<td>24</td>
</tr>
</tbody>
</table>

Set DSCP Values on the Network

You can configure switches and routers to mark DSCP values in the IP headers of RTP media.

To set DSCP values on the network, you must identify the different streams from the client application.

- Media Streams — Because the client uses different port ranges for audio streams and video streams, you can differentiate audio media and video media based on those port range. Using the default port ranges in the SIP profile, you should mark media packets as follows:
  - Audio media streams in ports from 16384 to 24575 as EF
  - Video media streams in ports from 24576 to 32767 as AF41

- Signaling Streams—You can identify signaling between the client and servers based on the various ports required for SIP, CTI QBE, and XMPP. For example, SIP signaling between Webex Teams and Cisco Unified Communications Manager occurs through port 5060.
You should mark signaling packets as CS3.

- For port ranges for Webex Teams only calls, use the guidelines in Network Requirements for Webex Teams.

Allow Untrusted Certificates on Unified CM

If needed, you can use Control Hub to allow untrusted certificates from your Unified CM. They may be untrusted because they're self-signed or if the certificate doesn't match the address that is being used for the connection.

⚠️ Caution

This setting downgrades your deployment's security. We strongly advise that you use a more secure method for certificate trust. Use this method as a last resort for limited deployments, such as those in a lab testing environment.

Before you begin

Before you use this option, understand certificate requirements and best practices Certificate Requirements for Calling in Webex Teams (Unified CM).

Step 1

From the customer view in https://admin.webex.com, go to Services, and then choose Client Settings from the calling card.

Step 2

In Unified CM Settings, toggle on Allow Unified CM registration without trusted certificate.

After this toggle is enabled, Webex Teams apps register to the premises, regardless of what type of certificate is being used.