Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)
CONTENTS

Full Cisco Trademarks with Software License  ii

PREFACE

New and Changed Information  ix

CHAPTER 1

Overview of Webex Video Mesh  1
  Cisco Webex Video Mesh Overview  1
  Clients and Devices That Use Webex Video Mesh Node  2
  Quality of Service on Webex Video Mesh Node  3
  Proxy Support for Cisco Webex Video Mesh  3
  Supported Resolutions and Framerates for Video Mesh  5

CHAPTER 2

Prepare Your Environment  7
  Requirements for Webex Video Mesh  7
    Call Control and Meeting Integration Requirements for Video Mesh  7
    Endpoint and Cisco Webex Teams App Requirements  8
    System and Platform Requirements for Webex Video Mesh Node Software  10
    Requirements for Proxy Support for Webex Video Mesh  11
  Call Capacity on Webex Video Mesh Node Platforms  12
  Webex Video Mesh Clusters  13
    Guidelines for Webex Video Mesh Cluster Deployment  14
    Cisco Webex Device Registers with Cisco Webex  15
    Round-trip Delay Tests—Cloud Device Fails to Reach On-Premises Cluster  16
    Round-trip Delay Tests—Cloud Device Successfully Reaches On-Premises Cluster  16
    On-Premises and Cloud Call  17
    On-Premises Call with Different Cluster Affinities  18
    Cisco Webex Cloud Device Connects to Cloud  18
New and Changed Information

This table covers new features or functionality, changes to existing content, and any major errors that were fixed in the Deployment Guide.

For information about Webex Video Mesh node software updates, see the Webex Video Mesh Release Notes.

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 22, 2020</td>
<td>• Added new section: “Factory Reset a Webex Video Mesh Node From The Web Interface”.</td>
</tr>
<tr>
<td></td>
<td>• Added more details on connectivity checks in the “Manage Webex Video Mesh Node from the Web Interface” section.</td>
</tr>
<tr>
<td></td>
<td>• Added in-room wireless share to the “Clients and Devices That Use Webex Video Mesh Node” section.</td>
</tr>
<tr>
<td>December 12, 2019</td>
<td>• Added change passphrase and passphrase expiry procedures to the “Manage Webex Video Mesh Node From the Web Interface” section in the Manage and Troubleshoot chapter.</td>
</tr>
<tr>
<td>Date</td>
<td>Change</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| December 10, 2019  | • Added the following information and port ranges to the traffic signature tables (for QoS enabled and disabled:<br>  
  • Source IP Address: Video Mesh Node<br>  
  • Destination IP Address: Webex cloud media services<br>  
  • Source UDP Ports: 35000 to 52499<br>  
  • Destination UDP Ports: 5004<br>  
  • Native DSCP Marking: AF41<br>  
  • Media Type: Test STUN packets<br>  
  • Renamed the "Bandwidth Guidelines" section to "Video Quality and Scaling", and added a link to the Preferred Architecture documentation.<br>  
  • In the Unified CM TLS configuration, our guide erroneously stated to configure a non-secure SIP trunk for Webex cloud failover. Corrected the statement to say to create a SIP trunk (you can configure it as either secure or non-secure). |
| November 4, 2019   | • Retired old analytics content and added new section that covers analytics and troubleshooting:<br>  
  • Webex Video Mesh Analytics, on page 75<br>  
  • Available Analytics, on page 81<br>  
  • Recent Resource Usage, on page 85<br>  
  • In the “Exchange Certificates” section, added information about the Subject Alternative Name(s) field and added the following note in the Before You Begin section: “For security reasons, we recommend that you use a CA signed certificate on your Video Mesh nodes instead of the node's default self-signed certificate.” |
<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
</table>
| October 18, 2019 | • Added short video address routing configuration to the following sections:  
  • Configure Unified CM Secure TLS SIP Traffic Routing for Webex Video Mesh, on page 59  
  • Configure Unified CM TCP SIP Traffic Routing for Webex Video Mesh, on page 62  
  • Configure Expressway TCP SIP Traffic Routing for Video Mesh, on page 65  
  • Updated the description of the 1080p Control Hub setting to clarify that this setting affects call capacity and only applies to on-premises SIP registered devices. See Enable 1080p High-Definition Video for On-Premises SIP Devices in Webex Video Mesh Node Meetings, on page 88 for more information.  
  • Updated the supported device and endpoints table to list only the tested cloud-registered devices.                                                                                                                                                                                                 |
| September 26, 2019 | • Added new section Configure Network Settings From Webex Video Mesh Node Web Interface, on page 94.  
  • Fixed the description if the Resource Utilization report. It now states: “Average resource utilization for the media microservices used in the Video Mesh clusters.”  
  • Added a note to the capacity section: “Overflows on low call volume (especially SIP calls that originate on-premises) are not a true reflection of scale. Video Mesh analytics (under Control Hub > Resources > Call Activity) indicate the call legs that originate on-premises; they do no specify the call streams that came in through the cascade to the Video Mesh node for media processing. As remote participant numbers increase in a meeting, the resulting cascade increases and consumes on-premises media resources on the Video Mesh node.”                                                                                                                                                                                                 |
| September 13, 2019 | • Updated Install and Configure Webex Video Mesh Node Software, on page 42 with network configuration steps that appear on the Customize template page.  
  • Updated System and Platform Requirements for Webex Video Mesh Node Software, on page 10 with 72vCPUs (the equivalent of CMS 1000) for specifications-based configuration.                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 29, 2019</td>
<td>• Added Explicit Proxy and supported authentication types for explicit proxy configurations (No auth, Basic, Digest, NTLM).</td>
</tr>
<tr>
<td></td>
<td>• Proxy Support for Cisco Webex Video Mesh, on page 3</td>
</tr>
<tr>
<td></td>
<td>• Requirements for Proxy Support for Webex Video Mesh, on page 11</td>
</tr>
<tr>
<td></td>
<td>• Configure Webex Video Mesh Node for Proxy Integration, on page 55</td>
</tr>
<tr>
<td></td>
<td>• Added Supported Resolutions and Framerates for Video Mesh, on page 5.</td>
</tr>
<tr>
<td></td>
<td>• Updated Clients and Devices That Use Webex Video Mesh Node, on page 2 to indicate that Webex Call My Video System to Webex cloud-registered video devices uses Video Mesh node.</td>
</tr>
<tr>
<td>July 24, 2019</td>
<td>• In the Manage Webex Video Mesh Node From the Web Interface, on page 92 section, made the following updates:</td>
</tr>
<tr>
<td></td>
<td>• Added new sections for Ping test, Trace Route test, NTP Server test, Reflector Tool, and Debug User Account.</td>
</tr>
<tr>
<td></td>
<td>• Updated the Overview section—Removed cascades from the screenshot and added OS version.</td>
</tr>
<tr>
<td></td>
<td>• Moved &quot;Manage Video Mesh from the Console&quot; content to the Appendix of the guide.</td>
</tr>
<tr>
<td></td>
<td>• Renamed &quot;Manage Webex Video Mesh&quot; chapter to &quot;Manage and Troubleshoot Webex Video Mesh&quot; and moved registration troubleshooting content to that chapter.</td>
</tr>
<tr>
<td>July 9, 2019</td>
<td>• In Call Control and Meeting Integration Requirements for Video Mesh, on page 7, updated minimum supported versions for Unified CM, Expressway, and Webex sites.</td>
</tr>
<tr>
<td></td>
<td>• In Clients and Devices That Use Webex Video Mesh Node, on page 2, added supported versions of Jabber VDI and Webex VDI (they are SIP clients). Also added a testing disclaimer.</td>
</tr>
<tr>
<td>May 24, 2019</td>
<td>• Added new sections on the troubleshooting features and updated overview screen in the Video Mesh node web interface:</td>
</tr>
<tr>
<td></td>
<td>• Generate Webex Video Mesh Logs for Support, on page 95</td>
</tr>
<tr>
<td></td>
<td>• Generate Webex Video Mesh Packet Captures for Support, on page 96</td>
</tr>
<tr>
<td></td>
<td>• Access Overview of Webex Video Mesh Node From Web Interface, on page 92</td>
</tr>
<tr>
<td>April 25, 2019</td>
<td>• Updated Manage Webex Video Mesh Node From the Console, on page 104 to state that Control Hub maintenance mode is required before performance any maintenance on Video Mesh nodes.</td>
</tr>
</tbody>
</table>
### New and Changed Information

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 11, 2019</td>
<td>• Removed outdated information from Bandwidth Requirements. Updated the content and diagrams, and changed the section name to Video Quality and Scaling for Video Mesh, on page 31.</td>
</tr>
<tr>
<td>February 27, 2019</td>
<td>• In Guidelines for Webex Video Mesh Cluster Deployment, on page 14, added a statement about the recommended number of nodes in a cluster.</td>
</tr>
<tr>
<td></td>
<td>• In the Unified CM configuration sections, changed naming from &quot;Hybrid Media&quot; to &quot;Video Mesh.&quot;</td>
</tr>
<tr>
<td>February 15, 2019</td>
<td>Added and updated sections to cover transparent (inspecting and non-inspecting) proxy support and secure SIP trunk support for Unified CM-registered endpoints.</td>
</tr>
<tr>
<td></td>
<td><strong>Transparent Proxy Updates</strong></td>
</tr>
<tr>
<td></td>
<td>• Proxy Support for Cisco Webex Video Mesh, on page 3</td>
</tr>
<tr>
<td></td>
<td>• Requirements for Proxy Support for Webex Video Mesh, on page 11</td>
</tr>
<tr>
<td></td>
<td>• Configure Webex Video Mesh Node for Proxy Integration, on page 55</td>
</tr>
<tr>
<td></td>
<td><strong>Secure SIP Trunk Updates</strong></td>
</tr>
<tr>
<td></td>
<td>• Integrate Webex Video Mesh With Unified CM or VCS Expressway Call Control Task Flow, on page 57</td>
</tr>
<tr>
<td></td>
<td>• Configure Unified CM Secure TLS SIP Traffic Routing for Webex Video Mesh, on page 59</td>
</tr>
<tr>
<td></td>
<td>• Exchange Certificate Chains Between Unified CM and Webex Video Mesh Nodes, on page 68</td>
</tr>
<tr>
<td></td>
<td>• Enable Media Encryption for the Organization and Video Mesh Clusters, on page 70</td>
</tr>
<tr>
<td></td>
<td>• Verify the Meeting Experience on the Secure Endpoint, on page 72</td>
</tr>
<tr>
<td>February 6, 2019</td>
<td>• Added and updated sections to cover the dual NIC feature which separates enterprise network traffic from cloud network traffic on Video Mesh nodes for deployments in the DMZ.</td>
</tr>
<tr>
<td></td>
<td>• New sections:</td>
</tr>
<tr>
<td></td>
<td>• Set The External Network Interface of the Webex Video Mesh Node, on page 47</td>
</tr>
<tr>
<td></td>
<td>• Add Internal and External Routing Rules, on page 48</td>
</tr>
<tr>
<td></td>
<td>• Updated sections:</td>
</tr>
<tr>
<td></td>
<td>• Set the Network Configuration of the Webex Video Mesh Node in the Console, on page 45</td>
</tr>
<tr>
<td></td>
<td>• Deployment Models Supported by Video Mesh, on page 20</td>
</tr>
<tr>
<td>Date</td>
<td>Change</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| December 5, 2018  | • In *Configure Expressway TCP SIP Traffic Routing for Video Mesh*, on page 65, fixed the pattern string that is required for CMR-Hybrid to be exempt from routing to the Video Mesh node `(((\d{9})(^XX.{22,25}))@YourSite\.webex\.com.*)`).  
  • In the same section, added more context about CMR-Hybrid:  
    “CMR-Hybrid uses a cascade between the on-premises TelePresence Server/MCU to Webex. The URI of the cascade represents the telephony domain site and the meeting that the cascade is for. The first two digits identify which telephony domain the call routes to, and the rest is the unique identifier for the meeting. These URIs are always 22-25 characters.” |
Overview of Webex Video Mesh

Cisco Webex Video Mesh dynamically finds the optimal mix of on-premises and cloud conferencing resources. On-premises conferences stay on premises when there are enough local resources. When local resources are exhausted, conferences then expand to the cloud.

Webex Video Mesh Node is software that is installed on an on-premises Cisco UCS server, registered to the cloud, and managed in Cisco Webex Control Hub. Cisco Webex Teams meetings, Cisco Webex-powered meetings, and Cisco Webex Teams calls (between two people) can be routed to the local, on-net Webex Video Mesh nodes. Webex Video Mesh selects the most efficient way to use the available resources.

Webex Video Mesh provides these benefits:

- Improves quality and reduces latency by allowing you to keep your calls on premises.
- Extends your calls transparently to the cloud when on-premises resources have reached their limit or are unavailable.
- Manages your Webex Video Mesh clusters from the cloud with a single administrative interface: Cisco Webex Control Hub (https://admin.webex.com).
- Optimizes resources and scale capacity, as needed.
- Combines the features of cloud and on-premises conferencing in one seamless user experience.
- Reduces capacity concerns, because the cloud is always available when additional conferencing resources are needed. No need to do capacity planning for the worst case scenario.
- Uses local media processing when users dial in to a Cisco Webex meeting or Cisco Webex Teams meeting from on-premises standards-based SIP endpoints and clients.
• SIP based endpoints and clients (Cisco endpoints, Jabber, 3rd party SIP), registered to on-premises call control (Cisco Unified Communications Manager or Expressway), that call into a Cisco Webex meeting or Cisco Webex Teams meeting.

• Cisco Webex Teams app (including paired with room devices) that join a Cisco Webex meeting.

• Cisco Webex room and desk devices (including Cisco Webex Board) that directly join a Webex meeting.

• Provides optimized audio and video interactive voice response (IVR) to on-net SIP based endpoints and clients.

• Cisco Webex clients (internal and external) continue to join meetings from the cloud.

• H.323, IP dial-in, and Skype for Business (S4B) endpoints continue to join meetings from the cloud.

• Supports 1080p 30fps high definition video as an option for meetings, if meeting participants that can support 1080p are hosted through the local on-premises Webex Video Mesh nodes. (If a participant joins an in-progress meeting from the cloud, on-premises users continue to experience 1080p 30fps on supported endpoints.)

• Enhanced and differentiated Quality of Service (QoS) marking: separate audio (EF) and video (AF41).

### Clients and Devices That Use Webex Video Mesh Node

We endeavor to make Webex Video Mesh interoperable with relevant clients and device types. Although it is not possible to test all scenarios, the testing on which this data is based covers most common functions of the listed endpoints and infrastructure. The absence of a device or client implies a lack of testing and a lack of official support from Cisco.

*Table 1: Clients and Devices That Use Webex Video Mesh Node*

<table>
<thead>
<tr>
<th>Client or Device Type</th>
<th>Uses Webex Video Mesh Node on Point to Point Call</th>
<th>Uses Webex Video Mesh Node on Multiparty Meeting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Webex Teams app (desktop and mobile)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Webex devices, including room devices and Webex Board. (See the Requirements section for a full list.)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>In-room wireless share between Cisco Webex Teams app and supported Room, Desk, and Board devices.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Unified CM-registered devices (including IX endpoints) and clients (including Jabber VDI 12.6 and later, and Webex VDI 39.3 and later), calling into a Webex scheduled or Webex Personal Room meeting.*</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VCS/Expressway-registered devices, calling into a Webex scheduled or Webex Personal Room meeting.*</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Quality of Service on Webex Video Mesh Node

Webex Video Mesh nodes conforms to recommended quality of service (QoS) best practices by enabling port ranges that allow you to differentiate audio and video streams in all flows to and from the Video Mesh nodes. This change will let you create QoS policies and effectively remark traffic to and from the Video Mesh Nodes.

Accompanying these port changes are QoS changes. Webex Video Mesh nodes automatically mark media traffic from SIP registered endpoints (on-premises Unified CM or VCS Expressway registered) for both audio (EF) and video (AF41) separately with appropriate class of service and use well-known port ranges for specific media types.

The source traffic from the on-premises registered endpoints is always determined by the configuration on the call control (Unified CM or VCS Expressway).

For more information, see the QoS table at Ports and Protocols Used by Webex Video Mesh, on page 24 and the steps to enable or disable QoS in the Video Mesh Deployment Task Flow, on page 39

Cisco Webex Teams apps continue to connect to Webex Video Mesh nodes over shared port 5004. These ports are also used by Cisco Webex Teams apps and endpoints for STUN reachability tests to Webex Video Mesh nodes. Webex Video Mesh node to Webex Video Mesh node for cascades use a destination shared port of 5004.

Proxy Support for Cisco Webex Video Mesh

Cisco Webex Video Mesh supports explicit, transparent inspecting, and non-inspecting proxies. You can tie these proxies to your Webex Video Mesh deployment so that you can secure and monitor traffic from the enterprise out to the cloud. This feature sends signaling and management https-based traffic to the proxy. For transparent proxies, network requests from Video Mesh nodes are forwarded to a specific proxy through
enterprise network routing rules. You can use the Webex Video Mesh admin interface for certificate management and the overall connectivity status after you implement the proxy with the nodes.

**Note**

Media does not travel through the proxy. You must still open the required ports for media streams to reach the cloud directly.

The following proxy types are supported by Video Mesh:

- **Explicit Proxy (inspecting or non-inspecting)**—With explicit proxy, you tell the client (Video Mesh nodes) which proxy server to use. This option supports one of the following authentication types:
  - None—No further authentication is required. (For HTTP or HTTPS explicit proxy.)
  - Basic—Used for an HTTP user agent to provide a username and password when making a request, and uses Base64 encoding. (For HTTP or HTTPS explicit proxy.)
  - Digest—Used to confirm the identity of the account before sending sensitive information, and applies a hash function on the username and password before sending over the network. (For HTTPS explicit proxy.)
  - NTLM—Like Digest, NTLM is used to confirm the identity of the account before sending sensitive information. Uses Windows credentials instead of the username and password. This authentication scheme requires multiple exchanges to complete. (For HTTP explicit proxy.)

- **Transparent Proxy (non-inspecting)**—Video Mesh nodes are not configured to use a specific proxy server address and should not require any changes to work with a non-inspecting proxy.

- **Transparent Proxy (inspecting)**—Video Mesh nodes are not configured to use a specific proxy server address. No http(s) configuration changes are necessary on Video Mesh, however, the Video Mesh nodes need a root certificate so that they trust the proxy. Inspecting proxies are typically used by IT to enforce policies regarding which websites can be visited and types of content that are not permitted. This type of proxy decrypts all your traffic (even https).

*Figure 1: Example of Webex Video Mesh Nodes and Proxy*

This diagram shows an example connection between the Webex Video Mesh, network and a proxy. For the transparent inspecting and explicit inspecting proxy options, the same root certificate must be installed on the proxy and on the Video Mesh nodes.
Supported Resolutions and Framerates for Video Mesh

This table covers the supported resolutions and framerates from a sender-receiver perspective in a meeting that is hosted on a Video Mesh node. The sender client (app or device) is across the top row of the table, whereas the receiver client is on the left side column of the table. The corresponding cell between the two participants captures the negotiated content resolution, frames per section, and audio source.

Resolution affects the call capacity on any Video Mesh node. For more information, see Call Capacity on Webex Video Mesh Node Platforms, on page 12

The resolution and framerate value is combined as XXXpYY—for example, 720p10 means 720p at 10 frames per second.

The definition abbreviations (SD, HD, and FHD) in the sender row and receiver column refer to the upper resolution of the client or device:

- SD—Standard Definition (576p)
- HD—High Definition (720p)
• FHD—Full High Definition (1080p)

**Table 2: Supported Resolutions and Framerates for Video Mesh**

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Sender</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Webex Teams Desktop</td>
</tr>
<tr>
<td>Webex Teams Mobile</td>
<td>Webex Mobile</td>
</tr>
<tr>
<td></td>
<td>SIP Registered Devices (HD)</td>
</tr>
<tr>
<td></td>
<td>SIP Registered Devices (FHD)</td>
</tr>
<tr>
<td></td>
<td>Webex Registered Devices (HD)</td>
</tr>
<tr>
<td></td>
<td>Webex Registered Devices (FHD)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Webex Teams Desktop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webex Teams Mobile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Registered Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(HD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Registered Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(FHD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webex Registered Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(SD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webex Registered Devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(FHD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Content Audio refers to the audio that is played from the specific content being shared, such as a streaming video. This audio stream is separate from the regular meeting audio.

** Mixed Audio refers to a mix of the meeting participant audio and audio from the content share.
CHAPTER 2

Prepare Your Environment

• Requirements for Webex Video Mesh, on page 7
• Call Capacity on Webex Video Mesh Node Platforms, on page 12
• Webex Video Mesh Clusters, on page 13
• Deployment Models Supported by Video Mesh, on page 20
• Deployment Models For Webex Video Mesh and Cisco Unified Communications Manager, on page 21
• Ports and Protocols Used by Webex Video Mesh, on page 24
• Video Quality and Scaling for Video Mesh, on page 31
• Requirements for Cisco Webex Services, on page 35
• Complete the Prerequisites for Webex Video Mesh, on page 36

Requirements for Webex Video Mesh

Webex Video Mesh is available with the offers documented in License Requirements for Hybrid Services.

Call Control and Meeting Integration Requirements for Video Mesh

Call control and existing meetings infrastructure are not required to use Video Mesh, but you can integrate the two. If you're integrating Video Mesh with your call control and meeting infrastructure, make sure your environment meets the minimum criteria that are documented in the following table.

Table 3: Call Control and Meeting Requirements for Video Mesh

<table>
<thead>
<tr>
<th>Component Purpose</th>
<th>Minimum Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Premises call control</td>
<td>Cisco Unified Communications Manager, Release 11.5(1) SU3 or later. (We recommend the latest SU release.)</td>
</tr>
<tr>
<td></td>
<td>Cisco Expressway-C or E, Release X8.11.4 or later. (See the &quot;Important Information&quot; section in the Expressway Release Notes for more information.)</td>
</tr>
</tbody>
</table>
## Endpoint and Cisco Webex Teams App Requirements

### Table 4: Endpoint and App Requirements for Video Mesh

<table>
<thead>
<tr>
<th>Component Purpose</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Endpoints</td>
<td>See Webex Meeting Center Video Compatibility and Support.</td>
</tr>
<tr>
<td>Supported versions of the Cisco Webex Teams app</td>
<td>Video Mesh supports Cisco Webex Teams for desktop (Windows, Mac) and mobile (Android, iPhone, and iPad). To download the app for a supported platform, go to <a href="https://www.webex.com/downloads.html">https://www.webex.com/downloads.html</a>.</td>
</tr>
<tr>
<td>Component Purpose</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Supported codecs</td>
<td>See the Cisco Webex Meetings Data Sheet for a list of supported audio and video codecs. Note these caveats for Video Mesh:</td>
</tr>
<tr>
<td></td>
<td>• For video quality, Video Mesh supports up to 1080p in certain scenarios. You can configure this setting in <a href="https://admin.webex.com">https://admin.webex.com</a>.</td>
</tr>
<tr>
<td></td>
<td>• For SIP video systems, Video Mesh supports SIP clients that do dual tone multi frequency (DTMF) audio tones. The service also supports keypad markup language (KPML).</td>
</tr>
<tr>
<td></td>
<td>• Webex Teams for Windows and Mac and Room, Desk, and Board devices registered to the cloud support up to 1080p 30fps with content audio.</td>
</tr>
<tr>
<td></td>
<td>• H.323 clients are mentioned in the data sheet, but they only go to the cloud.</td>
</tr>
<tr>
<td>Supported Webex-registered Room, Desk, and Board devices</td>
<td>The following devices are tested and confirmed to work with Video Mesh nodes:</td>
</tr>
<tr>
<td></td>
<td>• Cisco DX70</td>
</tr>
<tr>
<td></td>
<td>• Cisco Webex DX80</td>
</tr>
<tr>
<td></td>
<td>• Cisco Webex Board 55</td>
</tr>
<tr>
<td></td>
<td>• Cisco Webex Room Kit</td>
</tr>
<tr>
<td></td>
<td>• Cisco Webex Room Kit Mini</td>
</tr>
<tr>
<td></td>
<td>• Cisco Webex Room Kit Plus</td>
</tr>
<tr>
<td></td>
<td>• Cisco Webex Room Kit Plus Precision 60</td>
</tr>
<tr>
<td></td>
<td>• Cisco Webex Room Kit Pro</td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence SX10 Quick Set</td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence SX20 Quick Set</td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence SX80 Codec</td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence MX200 G2</td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence MX300 G2</td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence MX700</td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence MX800</td>
</tr>
</tbody>
</table>
## System and Platform Requirements for Webex Video Mesh Node Software

For any platform that runs Webex Video Mesh Node software, coresidency with other services is not permitted.

### Table 5: System and Platform Requirements for Webex Video Mesh Node Software

<table>
<thead>
<tr>
<th>Hardware Configuration</th>
<th>Specifications for Production Software Image</th>
<th>Specifications for Demo Software Image</th>
<th>Notes</th>
<th>Common Requirements</th>
</tr>
</thead>
</table>
| **Cisco Meeting Server 1000 (CMS 1000)** | • 72vCPUs (70 for Webex Video Mesh Node, 2 for ESXi)  
• 60 GB main memory  
• 250 GB local hard disk space | —                                         | We recommend this platform for Webex Video Mesh Node.            | • VMware ESXi 6 or vSphere 6 or later  
• Hyperthreading enabled |
| **Specific Hardware Configuration** | • 48vCPUs (46 for Webex Video Mesh Node, 2 for ESXi) or 72vCPUs (70 for Webex Video Mesh Node, 2 for ESXi)  
• 60 GB main memory  
• 250 GB local hard disk space  
• 2.6 GHz Intel Xeon E5-2600v3 or later processor | • 14vCPUs (12 for Webex Video Mesh Node, 2 for ESXi)  
• 8 GB main memory  
• 20 GB local hard disk space  
• 2.6 GHz Intel Xeon E5-2600v3 or later processor | For more information about the demo software, see Webex Video Mesh Node Demo Software, on page 103. | |
| **Cisco Multiparty Media 410v server**       | —                                             | —                                         | While this platform is supported for Webex Video Mesh Node, note that it is an End of Sale/End of Life product. See the End-of-Sale and End-of-Life Announcement for the Cisco Multiparty Media 410V for more information. | |
Hardware Configuration | Specifications for Production Software Image | Specifications for Demo Software Image | Notes | Common Requirements
--- | --- | --- | --- | ---
 | • 48vCPUs (46 for Webex Video Mesh Node, 2 for ESXi) | | | |
 | • 60 GB main memory | | | |
 | • 250 GB local hard disk space | | | |

**Note** We do not support the first generation MM400v server.

---

**Requirements for Proxy Support for Webex Video Mesh**

- We officially support the following proxy solutions that can integrate with your Webex Video Mesh nodes.
  - Cisco Web Security Appliance (WSA) for transparent proxy
  - Squid for explicit proxy

- For an explicit proxy or transparent inspecting proxy that inspects (decrypts traffic), you must have a copy of the proxy's root certificate that you'll need to upload to the Webex Video Mesh node trust store on the web interface.

- We support the following explicit proxy and authentication type combinations:
  - No authentication with http and https
  - Basic authentication with http and https
  - Digest authentication with https only
  - NTLM authentication with http only

- For transparent proxies, you must use the router/switch to force HTTPS/443 traffic to go to the proxy. You can also force Web Socket/444 to go to proxy. (Web Socket uses https.) Port 444 depends on your network setup. If port 444 is not routed through the proxy, it must be open directly from the node to the cloud.
Webex Video Mesh requires web socket connections to cloud services, so that the nodes function correctly. On explicit inspecting and transparent inspecting proxies, http headers that are required for a proper websocket connection are altered and websocket connections fail.

The symptom when this occurs on port 443 (with transparent inspecting proxy enabled) is a post-registration warning in Control Hub: “Webex Video Mesh SIP calling is not working correctly.” The same alarm can occur for other reasons when proxy is not enabled. When websocket headers are blocked on port 443, media does not flow between apps and SIP clients.

If media is not flowing, this often occurs when https traffic from the node over port 444 is failing:

• Proxy is not inspecting, but port 444 traffic is not allowed by the proxy.
• Port 444 traffic is allowed by the proxy, but it is an inspecting proxy and is breaking the websocket.

To correct these problems, you may have to “bypass” or “splice” (disable inspection) on ports 444 and 443 to: *.wbx2.com and *.ciscospark.com.

Call Capacity on Webex Video Mesh Node Platforms

When considering capacity, keep in mind that Webex Video Mesh is a software-based media product which works along with other Webex cloud-based services. The capacity of a Webex Video Mesh node in a cluster can vary. Factors that influence the capacity are the type of devices and clients in a meeting, resolution, quality of network, peak load, deployment, and so on.

Because of these variables, the capacity numbers that follow are a general guideline that are based on 2 scenarios. We have used a combination of real and simulated clients for testing; these tests inherently can produce some variation. In all the scenarios, the load was placed at 1 call per second.

In general, adding more nodes to the cluster does not double the capacity, mainly because of overhead associated with setting up cascades. Use these numbers as general guidance. However, we strongly recommend the following:

• Test out common meeting scenarios for your deployment
• Use the analytics in Control Hub to see how your deployment is evolving and add capacity as needed

This document lists some example scenarios under which the capacity of system was tested:

• **Scenario 1**—2 Cisco Webex Teams participants are in a meeting. Both the participants are within the enterprise network, using the same Webex Video Mesh node.

• **Scenario 2**—Multiple SIP participants are in a meeting. All the participants are placed on the same Video Mesh node.
Overflows on low call volume (especially SIP calls that originate on-premises) are not a true reflection of scale. Video Mesh analytics (under Control Hub > Resources > Call Activity) indicate the call legs that originate on-premises; they do no specify the call streams that came in through the cascade to the Video Mesh node for media processing. As remote participant numbers increase in a meeting, the resulting cascade increases and consumes on-premises media resources on the Video Mesh node.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Scenario 1</th>
<th>Scenario 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Meeting Server 1000 (CMS 1000) (Full Version)</td>
<td>100 (up to 720p)</td>
<td>75 (up to 720p)</td>
</tr>
<tr>
<td></td>
<td>35 (up to 1080p)</td>
<td>38 (up to 1080p)</td>
</tr>
<tr>
<td>MM410v (Full Version)</td>
<td>100 (up to 720p)</td>
<td>65 (720p)</td>
</tr>
<tr>
<td></td>
<td>35 (up to 1080p)</td>
<td>28 (1080p)</td>
</tr>
</tbody>
</table>

Webex Video Mesh node capacity does not increase the size of the Webex meeting from a video participant perspective. (For example, MC200 does not affect the number of participants that can use the Webex Video Mesh node.)

**Webex Video Mesh Clusters**

Webex Video Mesh nodes are deployed in clusters. A cluster defines Webex Video Mesh nodes with similar attributes, such as network proximity. Cisco Webex participants are directed to use a particular cluster or the cloud, depending on the following conditions:

- A client on a corporate network that can reach an on-premises cluster will connect to it—the primary preference for clients that are on the corporate network.
- A client that cannot reach an on-premises cluster will connect to the cloud—the case for a mobile device that is not connected to the corporate network.
- Which cluster is used also depends on latency rather than just location. For example, a cloud cluster with lower STUN round-trip (SRT) delay than a Webex Video Mesh cluster may be a better candidate for the meeting. This logic prevents a user from landing on a geographically far cluster with a high SRT delay.

Each cluster contains logic that cascades meetings across other cloud meeting clusters, as needed. Cascading provides a data path for media between clients in their meetings. Meetings are distributed across nodes and the clients land on the most efficient node nearest to them, depending on factors such as network topology, WAN link, and resource utilization.

Reachability is determined by the client's ability to "ping" media nodes. A variety of potential connection mechanisms such as UDP and TCP are used during an actual call. Before the call, the Cisco Webex device (Room, Desk, Board, and Webex Teams app) registers with the Cisco Webex cloud, which provides a list of cluster candidates for the call.
Guidelines for Webex Video Mesh Cluster Deployment

- In typical enterprise deployments, we recommend that customers use up to 10 nodes per cluster. There are no hard limits set in the system to block a cluster size with greater than 10 nodes. However, if you need to create larger clusters, we strongly recommend that you review this option with Cisco engineering through your Cisco Account Team.

- Create fewer clusters when resources have similar network proximity (affinity).

- When creating clusters, only add nodes that are in the same geographical region and the same data center. Clustering across the wide area network (WAN) is not supported.

- Typically, deploy clusters in enterprises that host frequent localized meetings. Plan where you place clusters on the bandwidth available at various WAN locations inside the enterprise. Over time, you can deploy and grow cluster-by-cluster based on observed user patterns.

- Clusters located in different time zones can effectively serve multiple geographies by taking advantage of different peak/busy hour calling patterns.

- If you have two Webex Video Mesh nodes in two separate data centers (EU and NA, for example), and you have endpoints join through each data center, the nodes in each data center would cascade to a single Webex Video Mesh node in the cloud. These cascades would go over the Internet. If there is a cloud participant (that joins before one of the HMN participants), the nodes would be cascaded through the cloud participant’s media node.

Time Zone Diversity

Time zone diversity can allow clusters to be shared during off-peak times. For example: A company with a Northern California cluster and a New York cluster might find that overall network latency is not that high between the two locations that serve a geographically diverse user population. When resources are at peak usage in the Northern California cluster, the New York cluster is likely to be off peak and have additional capacity. The same applies for the Northern California cluster, during peak times in the New York cluster. These aren't the only mechanisms used for effective deployment of resources, but they are the two main ones.

Overflow to the Cloud

When the capacity of all on-premises clusters are reached, an on-premises participant overflows to the Cisco Webex. This does not mean that all calls will be hosted in the cloud. Only those participants that are either remote or can't connect to an on-premises cluster will be directed to the cloud. In a call with both on-premises and cloud participants, the on-premises cluster is bridged (cascaded) to the cloud to combine all participants into a single call.
In addition to determining reachability, the clients also perform periodic round-trip delay tests using Simple Traversal of UDP through NAT (STUN). STUN round-trip (SRT) delay is an important factor when selecting potential resources during an actual call. When multiple clusters are deployed, the primary selection criteria are based on the learned SRT delay. Reachability tests are performed in the background, initiated by a number of factors including network changes, and do not introduce delays that affect call setup times. The following two examples show possible reachability test outcomes.
Round-trip Delay Tests—Cloud Device Fails to Reach On-Premises Cluster

Determine cluster reachability and affinity by performing STUN round-trip (SRT) delay

Round-trip Delay Tests—Cloud Device Successfully Reaches On-Premises Cluster

Determine cluster reachability and affinity by performing STUN round-trip (SRT) delay

Learned reachability information is provided to the Cisco Webex cloud every time a call is set up. This information allows the cloud to select the best resource (cluster or cloud), depending on the relative location.
of the client to available clusters and the type of call. If no resources are available in the preferred cluster, additional clusters are tested for availability based on SRT delay. A preferred cluster is chosen with the lowest SRT delay. Calls are served on premises from a secondary cluster when the primary cluster is busy. Local reachable Webex Video Mesh resources are tried first, in order of lowest SRT delay. When all local resources are exhausted, the participant connects to the cloud.

Cluster definition and location is critical for a deployment that provides the best overall experience for participants. Ideally, a deployment should provide resources where the clients are located. If not enough resources are allocated where the clients make the majority of calls, more internal network bandwidth is consumed to connect users to distant clusters.

**On-Premises and Cloud Call**

![Diagram of On-Premises and Cloud Call](image)

On-premises Cisco Webex devices that have the same cluster affinity (preference, based on proximity to the cluster) connect to the same cluster for a call. On-premises Cisco Webex devices with different on-premises cluster affinities, connect to different clusters and the clusters then bridged to the cloud to combine the two environments into a single call.
On-Premises Call with Different Cluster Affinities

The Cisco Webex device connects to either on-premises cluster or cloud based upon its reachability. The following show examples of the most-common scenarios.

Cisco Webex Cloud Device Connects to Cloud
Cisco Webex On-Premises Device Connects to On-Premises Cluster

Cloud Cluster Selection for Overflow Based on 250 ms or Higher STUN Round-Trip Delay

While the preference for node selection is your locally deployed Video Mesh nodes, we support a scenario where, if the STUN round-trip (SRT) delay to an on-premises Video Mesh cluster exceeds the tolerable round-trip delay of 250 ms (which usually happens if the on-premises cluster is configured in a different
continent), then the system selects the closest cloud media node in that geography instead of a Video Mesh node.

### Video Mesh Clusters

<table>
<thead>
<tr>
<th>Location</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Jose</td>
<td>10 ms</td>
</tr>
<tr>
<td>Amsterdam</td>
<td>150 ms</td>
</tr>
<tr>
<td>Shanghai</td>
<td>750 ms</td>
</tr>
</tbody>
</table>

### Cisco Webex Cloud Media Clusters

<table>
<thead>
<tr>
<th>Location</th>
<th>Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Francisco</td>
<td>20 ms</td>
</tr>
<tr>
<td>France</td>
<td>120 ms</td>
</tr>
<tr>
<td>Australia</td>
<td>450 ms</td>
</tr>
</tbody>
</table>

- The Cisco Webex Teams app or device is on the enterprise network in San Jose.
- San Jose and Amsterdam clusters are at capacity or unavailable.
- SRT delay to the Shanghai cluster is greater than 250 ms and will likely introduce media quality issues.
- The San Francisco cloud cluster has an optimal SRT delay.
- The Shanghai Video Mesh cluster is excluded from consideration.
- As a result, the Cisco Webex Teams client overflows to the San Francisco cloud cluster.

---

**Note**

Intercluster cascades always go to the cloud.

### Deployment Models Supported by Video Mesh

#### Supported in a Video Mesh Deployment

- You can deploy a Webex Video Mesh Node in either a data center (preferred) or demilitarized zone (DMZ). For guidance, see *Ports and Protocols Used by Webex Video Mesh*, on page 24.
- For a DMZ deployment, you can set up the Video Mesh nodes in a cluster with the dual network interface (NIC). This deployment lets you separate the internal enterprise network traffic (used for interbox communication, cascades between node clusters, and to access the node's management interface) from the external cloud network traffic (used for connectivity to the outside world and cascades to the cloud).
Dual NIC works on both the full version and demo version of Video Mesh node software. You can also deploy the Video Mesh behind a 1:1 NAT setup.

- You can integrate Video Mesh nodes with your call control environment. For example deployments with Video Mesh integrated with Unified CM, see Deployment Models For Webex Video Mesh and Cisco Unified Communications Manager, on page 21.

- The following types of address translation are supported:
  - Dynamic Network Address Translation (NAT) using an IP pool
  - Dynamic Port Address Translation (PAT)
  - 1:1 NAT
  - Other forms of NAT should work as long as the correct ports and protocols are used, but we do not officially support them because they have not been tested.

- IPv4
- Static IP address for the Webex Video Mesh Node

Not Supported in a Video Mesh Deployment

- IPv6
- DHCP for the Webex Video Mesh Node
- A cluster with a mixture of single NIC and dual NIC
- Clustering Video Mesh nodes over the wide area network (WAN)
- Audio, video, or media that does not pass through a Webex Video Mesh Node:
  - Audio from phones
  - Peer-to-peer call between Cisco Webex Teams app and standards-based endpoint
  - Audio termination on Webex Video Mesh Node
  - Media sent through Expressway C/E pair
  - Video call back

Deployment Models For Webex Video Mesh and Cisco Unified Communications Manager

These examples show common Webex Video Mesh deployments and help you understand where Webex Video Mesh clusters can fit in to your network. Keep in mind that Webex Video Mesh deployment depends on factors in your network topology:

- Data center locations
- Office locations and size
- Internet access location and capacity
In general, try to tie the Webex Video Mesh nodes to the Unified CM or Session Management Edition (SME) clusters. As a best practice, keep the nodes as centralized as possible to the local branches.

Video Mesh supports Session Management Edition (SME). Unified CM clusters can be connected through an SME, and then you must create a SME trunk that connects to the Webex Video Mesh nodes.

Hub and Spoke Architecture

This deployment model involves centralized networking and internet access. Typically, the central location has a high employee concentration. In this case, a Webex Video Mesh cluster can be located at central location for optimized media handling.

Locating clusters in branch locations may not yield benefits in the short term and may lead to suboptimal routing. We recommend that you deploy clusters in a branch only if there is frequent communication between branches.
The geographically distributed deployment is interconnected, but can exhibit noticeable latency between regions. Lack of resources can cause suboptimal cascades to be setup in the short term when there are meetings between users in each geographical location. In this model, we recommend that you allocate Webex Video Mesh nodes near regional internet access.
Geographic Distribution with SIP Dialing

This deployment model contains regional Unified CM clusters. Each cluster can contain a SIP trunk to select resources in the local Webex Video Mesh cluster. A second trunk can provide a failover path to an Expressway pair if resources become limited.

Ports and Protocols Used by Webex Video Mesh

To ensure a successful deployment of Video Mesh and for trouble-free operation of the Video Mesh nodes, open the following ports on your firewall for use with the protocols.

- See Network Requirements for Webex Teams Service to understand the overall network requirements for Webex Teams.

- See the Firewall Traversal Whitepaper for more information about firewall and network practices for Cisco Webex services.

- To mitigate potential DNS query issues, follow the DNS Best Practices, Network Protections, and Attack Identification documentation when you configure your enterprise firewall.

- For more design information, see the Preferred Architecture for Hybrid Services, CVD.
The Webex Video Mesh nodes in a cluster must be in the same VLAN or subnet mask.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Source Description</th>
<th>Destination Description</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Transport Protocol</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Management computer</td>
<td>Webex Video Mesh node</td>
<td>As required</td>
<td>TCP, HTTPS</td>
<td>Webex Video Mesh node</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td>SSH for access to Webex Video Mesh admin console</td>
<td>Management computer</td>
<td>Webex Video Mesh node</td>
<td>As required</td>
<td>TCP</td>
<td>Webex Video Mesh node</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Transcoding and Playback</td>
<td>Gateway service on Webex Video Mesh node(s)</td>
<td>Webex Video Mesh node</td>
<td>As required</td>
<td>TCP, HTTPS (WebSocket)</td>
<td>Any</td>
<td>33432-33433</td>
<td></td>
</tr>
<tr>
<td>Intracluster Communication</td>
<td>Webex Video Mesh node</td>
<td>Webex Video Mesh node</td>
<td>IP address of other Webex Video Mesh nodes in the cluster</td>
<td>TCP</td>
<td>Webex Video Mesh nodes</td>
<td>8443</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: Ports and Protocols for Management
<table>
<thead>
<tr>
<th>Purpose</th>
<th>Source</th>
<th>Destination</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Transport Protocol</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Webex Video Mesh node</td>
<td>Cisco Webex cloud</td>
<td>As required</td>
<td>Any</td>
<td>UDP, NTP</td>
<td>Any</td>
<td>123*</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>53*</td>
</tr>
<tr>
<td>Cascade Signaling</td>
<td>Webex Video Mesh node</td>
<td>Cisco Webex cloud</td>
<td>Any</td>
<td>Any</td>
<td>TCP</td>
<td>Any</td>
<td>444</td>
</tr>
<tr>
<td>Management</td>
<td>Webex Video Mesh node</td>
<td>Cisco Webex cloud</td>
<td>As required</td>
<td>Any</td>
<td>TCP, HTTPS</td>
<td>Any**</td>
<td>443</td>
</tr>
<tr>
<td>Management</td>
<td>Webex Video Mesh node (1)</td>
<td>Webex Video Mesh node (2)</td>
<td>Webex Video Mesh node (1)</td>
<td>Any</td>
<td>TCP, HTTPS (WebSockets)</td>
<td>Webex Video Mesh node (2)</td>
<td>5000–5001</td>
</tr>
</tbody>
</table>

* The default configuration in the OVA is configured for NTP and DNS. The OVA requires that you open those ports outbound to the internet. If you configure a local NTP and DNS server, then ports 53 and 123 are not required to be opened through the firewall.

** Because some cloud service URLs are subject to change without warning, ANY is the recommended destination for trouble-free operation of the Webex Video Mesh nodes. If you prefer to filter traffic based on URLs, see the “Webex Teams URLs for Hybrid Services” section of the Network Requirements for Webex Teams Services for more information.

**Traffic Signatures for Video Mesh (Quality of Service Enabled)**

For deployments where the Video Mesh node sits in the enterprise side of the DMZ or inside the firewall, there is a Video Mesh Node configuration setting in the Webex Control Hub that allows the administrator to optimize the port ranges used by the Video Mesh Node for QoS network marking. This Quality of Service setting, when enabled (enabled by default), changes the source ports that are used for audio, video, and content sharing to the values in this table. This setting allows you to configure QoS marking policies based on UDP port ranges to differentiate audio from video or content sharing and mark all Audio with recommended value of EF and Video and Content sharing with a recommended value of AF41.
The table and diagram show UDP ports that are used for audio and video streams, which are the main focus of QoS network configurations. While network QoS marking policies for media over UDP are the focus of the following table, Webex Video Mesh nodes also terminate TCP traffic for presentation and content sharing for Cisco Webex Teams apps using ephemeral ports 52500–65500. If a firewall sits between the Video Mesh nodes and the Cisco Webex Teams apps, those TCP ports also must be allowed for proper functioning.

**Note** Video Mesh Node marks traffic natively. This native marking is asymmetric in some flows and depends on whether the source ports are shared ports (single port like 5004 for multiple flows to various destinations and destination ports) or whether they are not (where the port falls in a range but is unique to that specific bidirectional session).

To understand the native marking by a Video Mesh Node, note that the Video Mesh node marks audio EF when it is not using the 5004 port as a source port. Some bidirectional flows like Video Mesh to Video Mesh cascades or Video Mesh to Webex Teams App will be asymmetrically marked, a reason to use the network to remark traffic based on the UDP port ranges provided.

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Source UDP Ports</th>
<th>Destination UDP Ports</th>
<th>Native DSCP Marking</th>
<th>Media Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Mesh Node</td>
<td>Webex cloud media services</td>
<td>35000 to 52499</td>
<td>5004</td>
<td>AF41</td>
<td>Test STUN packets</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Webex cloud media services</td>
<td>52500 to 62999</td>
<td>5004</td>
<td>EF</td>
<td>Audio</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Webex cloud media services</td>
<td>63000 to 65500</td>
<td>5004</td>
<td>AF41</td>
<td>Video</td>
</tr>
<tr>
<td>Video Mesh Node*</td>
<td>Video Mesh Node*</td>
<td>52500 to 62999</td>
<td>5004</td>
<td>EF / AF41*</td>
<td>Audio</td>
</tr>
</tbody>
</table>
**Video Mesh to Video Mesh cascades have asymmetrically marked media for the audio. When the Video Mesh Nodes initiates the cascade the source ports for audio 52500 to 62999 are used and the VMN can mark EF for that audio, however the return audio from the Video Mesh node answering the cascade will use the shared ports (5004) and thus mark that return audio traffic AF41.**

**The direction of media traffic determines the DSCP markings. If the source ports are from the Video Mesh node (from the Video Mesh node to Webex Teams app), the traffic is marked as AF41 only. Media traffic that originates from the Webex Teams app or Webex endpoints has the separate DSCP markings, but the return traffic from the Video Mesh node shared ports does not.**

### Traffic Signatures for Video Mesh (Quality of Service Disabled)

For deployments where the Video Mesh node sits in the DMZ, there is a Video Mesh Node configuration setting in the Webex Control Hub that allows you to optimize the port ranges used by the Video Mesh node. This Quality of Service setting, when disabled (enabled by default), changes the source ports that are used for audio, video, and content sharing from the Video Mesh node to the range 34000 to 34999. The Video Mesh node then natively marks all audio, video, and content sharing to a single DSCP of AF41.

<table>
<thead>
<tr>
<th>Video Mesh Node</th>
<th>Video Mesh Node*</th>
<th>5004</th>
<th>AF41</th>
<th>Video</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM SIP endpoints</td>
<td>63000 to 65500</td>
<td>5004</td>
<td>AF41</td>
<td>Video</td>
</tr>
<tr>
<td>Unified CM SIP endpoints</td>
<td>52500 to 62999</td>
<td>Unified CM SIP Profile</td>
<td>EF</td>
<td>Audio</td>
</tr>
<tr>
<td>Webex Teams application or endpoint**</td>
<td>63000 to 65500</td>
<td>Unified CM SIP Profile</td>
<td>AF41</td>
<td>Video</td>
</tr>
<tr>
<td>Webex Teams application or endpoint**</td>
<td>5004</td>
<td>52000 to 52099</td>
<td>AF41</td>
<td>Audio</td>
</tr>
<tr>
<td>Webex Teams application or endpoint**</td>
<td>5004</td>
<td>52100 to 52299</td>
<td>AF41</td>
<td>Video</td>
</tr>
</tbody>
</table>

* Video Mesh to Video Mesh cascades have asymmetrically marked media for the audio. When the Video Mesh Nodes initiates the cascade the source ports for audio 52500 to 62999 are used and the VMN can mark EF for that audio, however the return audio from the Video Mesh node answering the cascade will use the shared ports (5004) and thus mark that return audio traffic AF41.

** The direction of media traffic determines the DSCP markings. If the source ports are from the Video Mesh node (from the Video Mesh node to Webex Teams app), the traffic is marked as AF41 only. Media traffic that originates from the Webex Teams app or Webex endpoints has the separate DSCP markings, but the return traffic from the Video Mesh node shared ports does not.**

---

**Note**

Because the source ports are the same for all media regardless of destination, you cannot differentiate the audio from video or content sharing based on port range with this setting disabled. This configuration does let you configure firewall pin holes for media more easily that with Quality of Service enabled.
The table and diagram show UDP ports that are used for audio and video streams when QoS is disabled.

**Table 6: Traffic Signatures for Video Mesh (Quality of Service Disabled)**

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Source UDP Ports</th>
<th>Destination UDP Ports</th>
<th>Native DSCP Marking</th>
<th>Media Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Mesh Node</td>
<td>Webex cloud media services</td>
<td>34000 to 34999</td>
<td>5004</td>
<td>AF41</td>
<td>Audio</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Webex cloud media services</td>
<td>34000 to 34999</td>
<td>5004</td>
<td>AF41</td>
<td>Video</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Video Mesh Node</td>
<td>34000 to 34999</td>
<td>5004</td>
<td>AF41</td>
<td>Audio</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Video Mesh Node</td>
<td>34000 to 34999</td>
<td>5004</td>
<td>AF41</td>
<td>Video</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Unified CM SIP endpoints</td>
<td>34000 to 34999</td>
<td>Unified CM SIP Profile</td>
<td>AF41</td>
<td>Audio</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Unified CM SIP endpoints</td>
<td>34000 to 34999</td>
<td>Unified CM SIP Profile</td>
<td>AF41</td>
<td>Video</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Webex cloud media services</td>
<td>35000 to 52499</td>
<td>5004</td>
<td>AF41</td>
<td>Test STUN packets</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Webex Teams application or endpoint</td>
<td>5004</td>
<td>52000 to 52099</td>
<td>AF41</td>
<td>Audio</td>
</tr>
<tr>
<td>Video Mesh Node</td>
<td>Webex Teams application or endpoint</td>
<td>5004</td>
<td>52100 to 52299</td>
<td>AF41</td>
<td>Video</td>
</tr>
</tbody>
</table>
## Ports and Protocols for Webex Meetings Traffic

*Figure 4: Ports and Protocols for Cisco Webex Meetings*

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Source</th>
<th>Destination</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Transport Protocol</th>
<th>Destination IP</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling to meeting</td>
<td>Apps (Cisco Webex Teams desktop and mobile apps)</td>
<td>Webex Video Mesh node</td>
<td>As required</td>
<td>Any</td>
<td>UDP and TCP (Used by the Cisco Webex Teams app) SRTP (Any)</td>
<td>Any****</td>
<td>5004</td>
</tr>
<tr>
<td></td>
<td>Cisco Webex room, desk, or board device</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cascade</td>
<td>Webex Video Mesh node</td>
<td>Cisco Webex cloud</td>
<td>34000-34999</td>
<td>34000-34999</td>
<td>UDP, SRTP (Any)**</td>
<td>Any****</td>
<td>5004</td>
</tr>
<tr>
<td>Cascade</td>
<td>Webex Video Mesh node</td>
<td>Webex Video Mesh node</td>
<td>As required</td>
<td>34000-34999</td>
<td>UDP, SRTP (Any)**</td>
<td>Any****</td>
<td>5004</td>
</tr>
</tbody>
</table>

---

**Note**

Port 5004 is used for all cloud media and on-premises Webex Video Mesh nodes.

Cisco Webex Teams apps continue to connect to Webex Video Mesh nodes over shared ports 5004. These ports are also used by Cisco Webex Teams apps and endpoints for STUN tests to Webex Video Mesh nodes. Webex Video Mesh node to Webex Video Mesh node for cascades use a destination shared port of 5004.

*** TCP is also supported, but not preferred because it may affect media quality.

**** If you want to restrict by IP addresses, see the IP address ranges that are documented in Webex Teams IP subnets for media.
For the best experience using Cisco Webex in your organization, configure your firewall to allow all outbound TCP and UDP traffic that is destined toward ports 5004 as well as any inbound replies to that traffic. The port requirements that are listed above assume that Webex Video Mesh nodes are deployed either in the LAN (preferred) or in a DMZ and that Cisco Webex Teams apps are in the LAN.

## Video Quality and Scaling for Video Mesh

Below are some common meeting scenarios when a cascade is created. Webex Video Mesh is adaptive depending on the available bandwidth and distributes resources accordingly. For devices in the meeting that use the Webex Video Mesh node, the cascade link provides the benefit of reducing average bandwidth and improving the meeting experience for the user.

---

**Note**

For bandwidth provisioning and capacity planning guidelines, see the [Preferred Architecture documentation](#).

---

Based on the active speakers in the meeting, the cascade links are established. Each cascade can contain up to 6 streams and the cascade is limited to 6 participants (6 in the direction of Webex Teams/SIP to Webex cloud and 5 in the opposite direction). Each media resource (cloud and Video Mesh) ask the remote side for the standard definition streams that are needed to fulfil the local endpoint requirements of all remote participants across the cascade.

To provide a flexible user experience, the Webex platform can do multistream video to meeting participants. This same ability applies to the cascade link between Video Mesh nodes and the cloud. In this architecture, the bandwidth requirements vary depending on a number of factors, such as the endpoint layouts.
Architecture

Cloud Registered

SIP Endpoints

Signaling

Switching

Transcoding

Mesh Node

In this architecture, Cisco Webex-registered endpoints send signaling to the cloud and media to the switching services. On-premises SIP endpoints send signaling to the call control environment (Unified CM or Expressway), which then sends it to the Video Mesh node. Media is sent to the transcoding service.

Cloud and Premises Participants

Local on-premises participants on the Video Mesh node request the desired streams based on their layout requirements. Those streams are forwarded from the Video Mesh node to the endpoint for local device rendering.

Each cloud and Video Mesh node requests HD and SD resolutions from all participants that are cloud registered-devices or Webex Teams apps. Depending on the endpoint, it will send up to 4 resolutions, typically 1080p, 720p, 360p, and 180p.

Cascades

Most Cisco endpoints can send 3 or 4 streams from a single source in a range of resolutions (from 1080p to 180p). The layout of the endpoint dictates the requirement for the streams needed on the far end of the cascade. For active presence, the main video stream is 1080p or 720p, the video panes (PiPS) are 180p. For equal view, the resolution is 480p or 360p for all participants in most cases. The cascade created between Video Mesh nodes and the cloud also sends 720p, 360p and 180p in both directions. Content is sent as single stream, and audio is sent as multiple streams.

Cascade bandwidth graphs that provide a per-cluster measurement are available in the Analytics menu in Webex Control Hub. You cannot configure cascade bandwidth per meeting in Control Hub.
The maximum negotiated cascade bandwidth per meeting is 20Mbps for main video for all sources and the multiple main video streams that they could send. This maximum value does not include the content channel or audio.

**Main Video With Multiple Layout Example**

The following diagrams illustrate an example meeting scenario and how the bandwidth is influenced when multiple factors are at play. In the example, all Webex Teams apps and Webex-registered devices are transmitting 1x720p, 1x360p and 1x180p streams. On the cascade, streams of 2x720p, 2x360p, and 2x180p are transmitted in both directions. The reason is because there are Webex Teams apps and Webex-registered devices that are receiving 720p, 360p and 180p on both sides of the cascade.

In the diagrams, the bandwidth numbers for transmitted and received data are for example purposes only. They are not an exhaustive coverage of all possible meetings and accompanying bandwidth requirements. Different meeting scenarios (joined participants, device capabilities, content sharing within the meeting, activity at any given point in time during the meeting) will yield different bandwidth levels.

**Figure 5: Main Video With Multiple Layout at Time of Meeting**

This diagram shows a meeting with cloud and premises registered endpoints and an active speaker.

**Figure 6: Cascade From Video Mesh Node to Cloud**

In the same meeting, this diagram shows an example of a cascade created between the Video Mesh nodes and the cloud in both directions.
In the same meeting, this diagram shows an example of a cascade from the cloud.

This diagram shows a meeting with the same devices above, along with a Webex Meetings client. The system sends the active speaker and last active speaker in high definition, along with an extra HD stream of the active
Requirements for Cisco Webex Services

Work with your partner, customer success manager (CSM), or trials representative to correctly provision the Cisco Webex site and Cisco Webex services for Video Mesh:

1. You must have a Cisco Webex organization with a paid subscription to Cisco Webex services.

2. To take full advantage of Webex Video Mesh, make sure your Webex site is on video platform version 2.0. (You can verify that your site is on video platform version 2.0 if it has the Media Resource Type list available in the Cloud Collaboration Meeting Room site options.)

3. You must enable CMR for your Webex site under user profiles. (You can do this in a bulk update CSV with the SupportCMR attribute).
Complete the Prerequisites for Webex Video Mesh

Use this checklist to ensure you are ready to install and configure Webex Video Mesh nodes and integrate a Webex site with Video Mesh.

Procedure

Step 1
Ensure the following is in place:

- Meet the minimum system requirements that are described in Requirements for Webex Video Mesh, on page 7 and License Requirements for Hybrid Services.
- Understand the call capacity examples that are described in Call Capacity on Webex Video Mesh Node Platforms, on page 12.
- Understand the supported deployment models described in Deployment Models Supported by Video Mesh, on page 20.
- Ensure that your network allows connectivity on the ports and using the protocols described in Ports and Protocols Used by Webex Video Mesh, on page 24.
- Ensure that your network supports the bandwidth requirements described in Video Quality and Scaling for Video Mesh, on page 31.

Step 2
Work with your partner, customer success manager, or trials representative to understand and prepare your Webex environment so that it's ready to connect to Video Mesh. For more information, see Requirements for Cisco Webex Services, on page 35.

Step 3
Note the following network information to assign to your Webex Video Mesh nodes:

- IP address (Recommended)
- Network mask
- Gateway IP address
- DNS servers
- NTP servers
- A hostname and optionally domain name for the Webex Video Mesh node. (Optional)

Note
We recommend that you use IP addresses for Webex Video Mesh. If you plan to configure the nodes with FQDN, the FQDN value should be resolvable using all the entries in the DNS servers list configured on the node. You must also create both forward- and reverse-DNS (A- and PTR-records) in the DNS configuration.
Prepare Your Environment

Step 4  Before starting installation, make sure your Cisco Webex organization is enabled for Video Mesh. This service is available for organizations with certain paid Cisco Webex service subscriptions as documented in License Requirements for Cisco Webex Hybrid Services. Contact your Cisco partner or account manager for assistance.

Step 5  Choose a supported hardware or specifications-based configuration for your Webex Video Mesh node, as described in System and Platform Requirements for Webex Video Mesh Node Software, on page 10.

Step 6  Make sure your server is running VMware ESXi 6 (or later) and vSphere 6 (or later) with a VM host operational.

Step 7  If you're integrating Webex Video Mesh with your Unified CM call control environment and you want the participant lists to be consistent across meeting platforms, make sure your Unified CM cluster security mode is set to mixed mode so that it supports TLS-encrypted traffic. End-to-end encrypted traffic is required for this functionality to work.

See the TLS setup chapter in the Security Guide for Cisco Unified Communications Manager for more information about switching your Unified CM environment to mixed mode. See the Active Control solution guide for more information about the features and about how to set up end-to-end encryption.

Step 8  If you're integrating a proxy (explicit, transparent inspecting, or transparent non-inspecting) with Webex Video Mesh, make sure you following the requirements as documented in Requirements for Proxy Support for Webex Video Mesh, on page 11.

What to do next

Install and Configure Webex Video Mesh Node Software, on page 42
Deploy Webex Video Mesh

- Video Mesh Deployment Task Flow, on page 39
- Install and Configure Webex Video Mesh Node Software, on page 42
- Log in to the Webex Video Mesh Node Console, on page 45
- Set the Network Configuration of the Webex Video Mesh Node in the Console, on page 45
- Set The External Network Interface of the Webex Video Mesh Node, on page 47
- Add Internal and External Routing Rules, on page 48
- Register the Webex Video Mesh Node to the Cisco Webex Cloud, on page 49
- Enable Quality of Service (QoS) for Webex Video Mesh Node, on page 52
- Verify Webex Video Mesh Node Port Ranges With Reflector Tool in the Web Interface, on page 53
- Configure Webex Video Mesh Node for Proxy Integration, on page 55
- Integrate Webex Video Mesh With Unified CM or VCS Expressway Call Control Task Flow, on page 57
- Exchange Certificate Chains Between Unified CM and Webex Video Mesh Nodes, on page 68
- Enable Media Encryption for the Organization and Video Mesh Clusters, on page 70
- Enable Webex Video Mesh for the Webex Site, on page 71
- Assign Collaboration Meeting Rooms to Cisco Webex Teams Users, on page 72
- Verify the Meeting Experience on the Secure Endpoint, on page 72

Video Mesh Deployment Task Flow

Before you begin
Prepare Your Environment, on page 7

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Log in to the Webex Video Mesh Node Console, on page 45</td>
<td>Sign in to the console for the first time. The Webex Video Mesh Node software has a default password. You need to change this value before you configure the node.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Set the Network Configuration of the Webex Video Mesh Node in the Console, on page 45</td>
<td>Use this procedure to configure the network settings for the Webex Video Mesh Node if you didn't configure them when you set up the node on a virtual machine. You'll set a static IP address and change the FQDN/hostname and NTP servers, if needed. DHCP is not currently supported.</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 4** Use these steps to configure the external interface for a dual network interface (dual NIC) deployment:  
  • Set The External Network Interface of the Webex Video Mesh Node, on page 47  
  • Add Internal and External Routing Rules, on page 48 | After the node is back online and you verified the internal network configuration, you can configure the external network interface if you're deploying the Webex Video Mesh Node in your network's DMZ so that you can isolate the enterprise (internal) traffic from the outside (external) traffic.  
You can also make exceptions or overrides to the default routing rules. |
| **Step 5** Register the Webex Video Mesh Node to the Cisco Webex Cloud, on page 49 | Use this procedure to register Webex Video Mesh nodes to the Cisco Webex cloud and complete additional configuration. When you use Cisco Webex Control Hub to register your node, you create a cluster to which the node is assigned. A cluster contains one or more media nodes that serve users in a specific geographic region. The registration steps also configure SIP call settings, set an upgrade schedule, and subscribe to email notifications. |
| **Step 6** Enable and verify Quality of Service (QoS) with the following tasks:  
  • Enable Quality of Service (QoS) for Webex Video Mesh Node, on page 52  
  • Verify Webex Video Mesh Node Port Ranges With Reflector Tool in the Web Interface, on page 53 | Enable QoS if you want Webex Video Mesh nodes to automatically mark SIP traffic (on-premises SIP registered endpoints) for both audio (EF) and video (AF41) separately with appropriate class of service and use well-known port ranges for specific media types. This change will let you create QoS policies and effectively remark return traffic from the cloud if desired.  
Use the Reflector Tool steps to verify the correct ports are opened on your firewall. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> Configure Webex Video Mesh Node for Proxy Integration, on page 55</td>
<td>Use this procedure to specify the type of proxy that you want to integrate with a Webex Video Mesh. If you choose a transparent inspecting proxy, you can use the node’s interface to upload and install the root certificate, check the proxy, and troubleshoot any potential issues.</td>
</tr>
<tr>
<td><strong>Step 8</strong> Follow Integrate Webex Video Mesh With Unified CM or VCS Expressway Call Control Task Flow, on page 57 and choose one of the following, depending on your call control, security requirements, and whether you want to integrate Webex Video Mesh with your call control environment:</td>
<td>SIP devices don't support direct reachability, so you must use Unified CM or VCS Expressway configuration to establish a relationship between on-premises registered SIP devices and your Video Mesh clusters. You only need to trunk your Unified CM or VCS Expressway to Webex Video Mesh Node, depending on your call control environment.</td>
</tr>
<tr>
<td>- Configure Unified CM Secure TLS SIP Traffic Routing for Webex Video Mesh, on page 59 (TLS)</td>
<td></td>
</tr>
<tr>
<td>- Configure Unified CM TCP SIP Traffic Routing for Webex Video Mesh, on page 62 (TCP)</td>
<td></td>
</tr>
<tr>
<td>- Configure Expressway TCP SIP Traffic Routing for Video Mesh, on page 65 (TCP)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> Exchange Certificate Chains Between Unified CM and Webex Video Mesh Nodes, on page 68</td>
<td>In this task, you download certificates from the Unified CM and Webex Video Mesh interfaces and upload one to the other. This step establishes secure trust between the two products and, in conjunction with the secure trunk configuration, allows encrypted SIP traffic and SRTP media in your organization to land on Webex Video Mesh nodes.</td>
</tr>
<tr>
<td><strong>Step 10</strong> Enable Media Encryption for the Organization and Video Mesh Clusters, on page 70</td>
<td>Use this procedure to turn on media encryption for your organization and individual Video Mesh clusters. This setting forces end-to-end TLS setup and you must have a secure TLS SIP trunk in place on your Unified CM that points to your Video Mesh nodes.</td>
</tr>
<tr>
<td><strong>Step 11</strong> Enable Webex Video Mesh for the Webex Site, on page 71</td>
<td>To use optimized media to the Webex Video Mesh Node for a Webex meeting, Personal Room meeting, or Cisco Webex Teams app meeting that allows you to join from a video device, this configuration needs to be turned on for the Webex site. Enabling this setting links Webex Video Mesh and meeting instances in the cloud together and allows</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>cascades to occur from Webex Video Mesh nodes.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>Assign Collaboration Meeting Rooms to Cisco Webex Teams Users, on page 72</strong></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>Verify the Meeting Experience on the Secure Endpoint, on page 72</strong></td>
</tr>
<tr>
<td></td>
<td>If you are using media encryption through the end-to-end TLS setup, use these steps to verify that the endpoints are securely registered and the correct meeting experience appears.</td>
</tr>
</tbody>
</table>

**Install and Configure Webex Video Mesh Node Software**

Use this procedure to deploy a Webex Video Mesh Node to your host server running VMware ESXi or vCenter. You install the software on-premises which creates a node and then perform initial configuration, such as network settings. You'll register it to the cloud later.

You must download the software package (OVA) from Cisco Webex Control Hub (https://admin.webex.com), rather than using a previously downloaded version. This OVA is signed by Cisco certificates and can be downloaded after you sign in to Control Hub with your customer administrator credentials.

**Before you begin**

- See **System and Platform Requirements for Webex Video Mesh Node Software, on page 10** for supported hardware platforms and specifications requirements for the Webex Video Mesh Node.
- Make sure you have these required items:
  - A computer with:
    - VMware vSphere client 6.0 or later
      For a list of supported operating systems, refer to VMware documentation.
    - Video Mesh software OVA file downloaded.
      Download the latest Video Mesh software from Cisco Webex Control Hub, rather than using a previously downloaded version. You can also access the software from this link. (The file is approximately 1.5 gb.)
  - A supported server with VMware ESXi or vCenter 6.0 or later installed and running
  - Disable virtual machine backups and live migration. Webex Video Mesh Node clusters are realtime systems; any virtual machine pauses can make these systems unstable. (For maintenance activities on a Webex Video Mesh Node, use maintenance mode from Cisco Webex Control Hub.)

**Procedure**

**Step 1**  
Using your computer, open the VMware vSphere client and sign in to the vCenter or ESXi system on the server.
Step 2  Go to Actions > Deploy OVF Template.
Step 3  On the Select an OVF template page, click Local File, then Choose Files. Navigate to where the videomesh.ova file is located, choose the file, and then click Next.
  
  Caution Each time you do a Webex Video Mesh Node installation, we recommend that you redownload the OVA rather than using a previously downloaded version. If you try to deploy an old OVA, your Webex Video Mesh Node may not work properly nor register to the cloud.
  
  Make sure you download a new copy of the OVA from this link.
  
Step 4  On the Select a name and folder page, enter a Virtual machine name for the Webex Video Mesh Node (for example, "Video.Mesh.Node_1"), choose a location where the virtual machine node deployment can reside, and then click Next.
  
  A validation check runs. After it finishes, the template details appear.
Step 5  Verify the template details and then click Next.
Step 6  On the Configuration page, choose the type of deployment configuration, and then click Next.
  
  • MM410v (default)
  • CMS 1000 (recommended)
  
  The options are listed in the order of increasing resource requirements.
Step 7  On the Select storage page, ensure that the default disk format of Thick Provision Lazy Zeroed and VM storage policy of Datastore Default are selected and then click Next.
Step 8  On the Select networks page, choose the network option from the list of entries to provide the desired connectivity to the VM.
  
  • For Internal Interface Network, choose the node's internal IP address.
  • For External Interface Network, choose the external IP address that faces the public network. Ignore this option if you don't have a dual NIC deployment.
  
  Note The inside interface (the default interface for traffic) is used for CLI, SIP trunks, SIP traffic and node management. The outside (external) interface is for HTTPS and websockets communication to the Webex cloud, along with the cascades traffic from the nodes to a meeting.
  
  For a DMZ deployment, you can set up the Video Mesh node with the dual network interface (NIC). This deployment lets you separate the internal enterprise network traffic (used for interbox communication, cascades between node clusters, and to access the node's management interface) from the external cloud network traffic (used for connectivity to the outside world and cascades to the cloud). All nodes in a cluster must be in dual NIC mode; a mixture of single and dual NIC is not supported.
  
  Note For an existing installation of Webex Video Mesh Node software, you cannot upgrade from a single NIC to a dual NIC configuration. You must do a fresh install of Webex Video Mesh Node in this case.
Step 9  On the Customize template page, configure the following network settings:
  
  • Hostname (Optional)—Enter the FQDN (hostname and domain) or a single word hostname for the node.
Note

- To ensure a successful registration to the cloud, use only lowercase characters in the FQDN or hostname that you set for the Webex Video Mesh Node. Capitalization is not supported at this time.

- When using or configuring FQDN or hostname, you must also enter a valid and resolvable domain. The total length of the FQDN must not exceed 64 characters.

- **IP Address**—Enter the IP address for the internal interface of the node.
- **Mask**—Enter the subnet mask address in dot-decimal notation. For example, 255.255.255.0.
- **Gateway**—Enter the gateway IP address. A gateway is a network node that serves as an access point to another network.
- **DNS Servers**—Enter a comma-separated list of DNS servers, which handle translating domain names to numeric IP addresses. (Up to 4 DNS entries are allowed.)
- **NTP Servers**—Enter your organization's NTP server or another external NTP server that can be used in your organization. The default NTP servers may not work for all enterprises. You can also use a comma-separated list to enter multiple NTP servers.

The Webex Video Mesh Node must have an internal IP address and resolvable DNS name. The node IP address must not belong to the IP address range reserved for Webex Video Mesh Node internal use. The default reserved IP address range is 172.17.0.0–172.17.255.255, which can be configured later in the Diagnostic menu. This IP address range is for communication within the Webex Video Mesh Node and between the software containers which hold the different components of the node—for example, SIP interface and media transcoding.

- Deploy all the nodes on the same subnet or VLAN, so that all nodes in a cluster are reachable from wherever the clients reside in your network.

- For a dual NIC DMZ deployment, you can set the external IP address in the node console, after you've saved the internal network configuration and rebooted the node later.

If preferred, you can skip the network setting configuration and follow the steps in Set the Network Configuration of the Webex Video Mesh Node in the Console, on page 45 after you sign into the node.

**Step 10**

On the Ready to Complete page, verify that all the settings that you entered match the guidelines in this procedure, and then click Finish.

After deployment of the OVA is complete, your Webex Video Mesh Node appears in the list of VMs.

**Step 11**

Right-click the Webex Video Mesh Node VM, and then choose Power > Power On.

The Webex Video Mesh Node software is installed as a guest on the VM Host. You are now ready to sign in to the console and configure the Webex Video Mesh Node.

**Troubleshooting Tips**

You may experience a delay of a few minutes before the node containers come up. A bridge firewall message appears on the console during first boot, during which you can't sign in.

**What to do next**

Log in to the Webex Video Mesh Node Console, on page 45
Log in to the Webex Video Mesh Node Console

Sign in to the console for the first time. The Webex Video Mesh Node software has a default password. You need to change this value before you configure the node.

Procedure

Step 1  From the VMware vSphere client, go to the Webex Video Mesh Node VM, and then choose Console.

The Webex Video Mesh Node VM boots up and a login prompt appears. If the login prompt does not appear, press Enter. You may briefly see a message that indicates the system is being initialized.

Step 2  Use the following default username and password to log in:

a) Login: admin
b) Password: cisco

Because you are logging in to the Webex Video Mesh Node for the first time, you must change the administrator passphrase (password).

Step 3  For (current) password, enter the default password (from above), and then press Enter.

Step 4  For new password, enter a new passphrase, and then press Enter.

Step 5  For retype new password, retype the new passphrase, and then press Enter.

A "Password successfully changed" message appears, and then the initial Webex Video Mesh Node screen appears with a message about unauthorized access being prohibited.

Step 6  Press Enter to load the main menu.

What to do next

Set the Network Configuration of the Webex Video Mesh Node in the Console, on page 45

Set the Network Configuration of the Webex Video Mesh Node in the Console

Use this procedure to configure the network settings for the Webex Video Mesh Node if you didn't configure them when you set up the node on a virtual machine. You'll set a static IP address and change the FQDN/hostname and NTP servers, if needed. DHCP is not currently supported.

These steps are required if you didn't configure network settings at the time of OVA deployment.

Note

The inside interface (the default interface for traffic) is used for CLI, SIP trunks, SIP traffic and node management. The outside (external) interface is for HTTPS and websockets communication to the Webex cloud, along with the cascades traffic from the nodes to a meeting.
Procedure

Step 1
Open the node console interface through the VMware vSphere client and then sign in using the admin credentials.

After first time setup of the network settings and if the Video Mesh is reachable, you can access the node interface through secure shell (SSH).

Step 2
From the main menu of the Webex Video Mesh Node console, choose option 2 Edit Configuration and then click Select.

Step 3
Read the prompt that the calls will end on the Webex Video Mesh Node, and then click Yes.

Step 4
Click Static, enter the IP address for the internal interface, Mask, Gateway, and DNS values for your network.

- The Webex Video Mesh Node must have an internal IP address and resolvable DNS name. The node IP address must not belong to the IP address range reserved for Webex Video Mesh Node internal use. The default reserved IP address range is 172.17.0.0–172.17.255.255, which can be configured in the Diagnostic menu. This IP address range is for communication within the Webex Video Mesh Node and between the software containers which hold the different components of the node—for example, SIP interface and media transcoding.

- Deploy all the nodes on the same subnet or VLAN, so that all nodes in a cluster are reachable from wherever the clients reside in your network.

- For a dual NIC DMZ deployment, you can set the external IP address in the next procedure, after you've saved the internal network configuration and rebooted the node.

Step 5
Change the default NTP servers to your organization's NTP server or another external NTP server that can be used in your organization.

Caution The default NTP servers may not work for all enterprises.

After you configure the NTP server and save network settings, you can follow the steps in Check Health of Webex Video Mesh Node From Console, on page 108 to verify that the time is synchronizing correctly through the specified NTP servers.

Step 6
(Optional) Change the hostname or domain, if required.

Note
- To ensure a successful registration to the cloud, use only lowercase characters in the hostname that you set for the Webex Video Mesh Node. Capitalization is not supported at this time.

- When using or configuring FQDN or hostname, you must also enter a valid and resolvable domain. The total length of the FQDN must not exceed 64 characters.

Step 7
Click Save, and then click Save Changes & Reboot.

During the save, DNS validation is performed if you provided a domain. A warning is displayed if the FQDN (hostname and domain) is not resolvable using the DNS server addresses provided. You may choose to save by ignoring the warning but calls will not work until the FQDN can resolve to the DNS configured on the node. After the Webex Video Mesh Node reboots, the network configuration changes take effect.
What to do next

Once the software image is installed and configured with the network settings (IP Address, DNS, NTP, and so on) and accessible on the enterprise network, you can move to the next step of securely registering it to the cloud. The IP address that is configured on the Webex Video Mesh Node is accessible only from the enterprise network. From a security perspective, the node is hardened whereby only customer administrators can access the node interface to perform configuration.

Set The External Network Interface of the Webex Video Mesh Node, on page 47

Set The External Network Interface of the Webex Video Mesh Node

After the node is back online and you verified the internal network configuration, you can configure the external network interface if you're deploying the Webex Video Mesh Node in your network's DMZ so that you can isolate the enterprise (internal) traffic from the outside (external) traffic.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the main menu of the Webex Video Mesh Node console, choose option 5 External IP Configuration and then click Select.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click 1 Enable/Disable, then Select, and then Yes to enable the external IP address options on the node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>As you did with the initial network configuration, enter the IP Address (external), Mask, and Gateway values.</td>
</tr>
<tr>
<td>Note</td>
<td>The Interface field shows the name of the external interface for the node.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Save and Restart. The node once again reboots to enable the dual IP address, and then automatically configures the basic static routing rules. These rules determine that traffic to and from a private class IP address uses an internal interface; traffic to and from a public class IP address uses an external interface. Later, you can create your own routing rules—For example, if you need to configure an override and allow access to an external domain from the internal interface.</td>
</tr>
<tr>
<td>Note</td>
<td>Under certain circumstances, the existing SSH connection may terminate. For organizations that use IP addresses from the public range, you must reestablish an SSH connection to the public IP address of the Webex Video Mesh Node.</td>
</tr>
<tr>
<td>Step 5</td>
<td>To validate the internal and external IP address configuration, from the main menu of the console, go to 4 Diagnostics, and then choose Ping.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the ping field, enter a destination address that you want to test, such as an external destination or an internal IP address, and then click OK.</td>
</tr>
<tr>
<td>•</td>
<td>Test an external destination (example, cisco.com); if successful, the results show that the destination was accessed from the external interface.</td>
</tr>
</tbody>
</table>
• Test an internal IP address; if successful, the results show that the address was accessed from the internal interface.

What to do next
Register the Webex Video Mesh Node to the Cisco Webex Cloud, on page 49

Add Internal and External Routing Rules

In a dual network interface (NIC) deployment, you can fine tune the routing for Video Mesh nodes by adding user-defined route rules for external and internal interfaces. The default routes are added to the nodes, but you can make exceptions—for example, external subnets or host addresses that need to be accessed through the internal interface, or internal subnets or host addresses that need to be accessed from the external interface. Perform the following steps as needed.

Procedure

| Step 1 | From the Video Mesh node interface, choose 5 External IP Configuration and then click Select. |
| Step 2 | Choose 3 Manage Routing Rules, and then click Select. |

The first time you open this page, the default system routing rules appear in the list. By default, all internal traffic goes through the internal interface and external traffic through the external interface.

You can add manual overrides to these rules in the next steps.

| Step 3 | Follow these steps as needed: |
|        | • Click Add external route, and then enter the internal subnet or host IP address to use for the external route. |
|        | • Click Add internal route, and then enter the external subnet or host IP address to use for the internal route. |

As you add each rule, they appear in the routing rule list, categorized as user defined rules.
The default routes cannot be deleted, but you can delete any user-defined overrides that you configured.

Note

Custom routing rules may create potential for conflicts with other routing. For example, you may define a rule that freezes your SSH connection to the Webex Video Mesh Node interface. If this happens, do one of the following and then remove or modify the routing rule:

- Open an SSH connection to the public IP address of the Webex Video Mesh Node.
- Access the Webex Video Mesh Node through the ESXi console

![Caution]

Register the Webex Video Mesh Node to the Cisco Webex Cloud

Use this procedure to register Webex Video Mesh nodes to the Cisco Webex cloud and complete additional configuration. When you use Cisco Webex Control Hub to register your node, you create a cluster to which the node is assigned. A cluster contains one or more media nodes that serve users in a specific geographic region. The registration steps also configure SIP call settings, set an upgrade schedule, and subscribe to email notifications.

Before you begin

- Once you begin registration of a node, you must complete it within 60 minutes or you have to start over.
- Ensure that any popup blockers in your browser are disabled or that you allow an exception for https://admin.webex.com.
- For best results, deploy all nodes of a cluster in the same data center. See Webex Video Mesh Clusters, on page 13 for how they work and best practices.
- From the host or machine where you're registering Webex Video Mesh nodes to the cloud, you must have connectivity to the Webex cloud and the Webex Video Mesh IP addresses that are being registered (in a dual NIC environment, specifically the internal IP addresses of the Webex Video Mesh nodes).

Procedure

Step 1

From the customer view in https://admin.webex.com, go to Services, and then choose one:

- If this is the first Webex Video Mesh Node you're registering, click Set up on the Video Mesh card, and then click Next. Note On this page, you can review the prerequisites. See Complete the Prerequisites for Webex Video Mesh, on page 36 for more information.
- If you've already registered one or more Webex Video Mesh Nodes, click View all on the Video Mesh card, and then click Add Resource.
You sign in to Control Hub using the customer admin credentials. The Control Hub admin functionality is available only to users who are defined as admins. See Customer Account Roles for more information.

Step 2  Make sure you have installed and configured your Webex Video Mesh Node, click Yes, I'm ready to register... and then click Next.

Step 3  In Create a new or select a cluster, choose one:
- For a new cluster, enter a name for the cluster to which you want to assign your Webex Video Mesh Node.
- For an existing cluster, Click the field and then choose an existing cluster to add the new node to.

Tip  We recommend that you name a cluster based on where the nodes of the cluster are located geographically. Examples: “San Francisco” or “New York” or “Dallas.”

Step 4  In Enter the FQDN or IP address, enter the fully qualified domain name (FQDN) or internal IP address of your Webex Video Mesh Node and then click Next.
- If you use FQDN, enter a domain that can be resolved by DNS.
- If you use an IP address, enter the same internal IP address that you used to configure the node from the console.

An FQDN must resolve directly to the IP address. Otherwise it is not useable. We perform the validation on FQDN to rule out any typo or configuration mismatch.

Note  The dual network interface does not support specifying an FQDN for the external IP address. The FQDN can be added only on the screen where internal IP address is entered. That is what the FQDN must resolve to using the DNS servers that are specified on the same screen.

Step 5  Under Upgrade Schedule, choose a time, frequency, and time zone.

When an upgrade is available, the Webex Video Mesh Node software automatically upgrades during the time that you select.

Step 6  Under Email Notifications, add any administrator email addresses to subscribe to notifications about service alarms and software upgrades.

Your administrator email address is automatically added, but you may remove it if you prefer.

Step 7  Toggle the Video Quality setting on to enable 1080p 30fps video.

With this setting, participants that join a meeting that is hosted in a Webex Video Mesh Node can use 1080p 30fps video if they are all inside the corporate network and they're using a high definition-capable device. The setting applies to all clusters of nodes.

Note  • If this setting is off, the default is 720p.
- For video resolutions that the Cisco Webex Teams app supports, see Video Specifications for Calls and Meetings.

Step 8  Read the information under Complete Registration and then click Go to Node to register the node to the Cisco Webex cloud.

A new browser tab opens to check the node. This step white lists the Webex Video Mesh Node using the IP address of node. During the registration process, Control Hub redirects you to the Webex Video Mesh Node. The IP address must be whitelisted, otherwise registration will fail. The registration process must be completed from the enterprise network where the node is installed.
**Step 9** Check **Allow Access to the Webex Video Mesh Node**, and then click **Continue**.

**Step 10** Click **Allow**.

Your account is validated, your Webex Video Mesh Node is registered and the message "Registration Complete" appears indicating your Webex Video Mesh Node is now registered to Cisco Webex.

The Webex Video Mesh Node gets machine credentials based on your organization's entitlements. The generated machine credentials expire periodically and are refreshed.

**Step 11** Click the portal link or close the tab to go back to the Video Mesh page.

On the **Video Mesh** page, you now see the new cluster that contains the Webex Video Mesh Node that you registered.

- If you go to the cluster, you'll see the new Webex Video Mesh Node, which initially shows a status of Registering. The node changes to Running when it is ready for use in your Cisco Webex organization.

- Because the software is a container that contains a couple of services from the cloud infrastructure, it gets updates from the cloud to remain in sync with the cloud services. Required updates may install shortly after you register the node to the cloud. You can also change your automatic upgrade schedule. See **Configure Automatic Upgrades for Cisco Webex Hybrid Services Resources** for more information.

- If you installed the demo image on the node that you registered, you'll see a “demo mode” yellow-status alarm. This alarm is normal, but you should install the full software image before the 90-day grace period expires for the demo image.

At this point, the Webex Video Mesh node is ready to communicate with Cisco cloud services over the secured channels using a token issued for authentication. The Webex Video Mesh node also communicates with Docker Hub (docker.com, docker.io). Docker is used by Webex Video Mesh node to store containers for distribution to different Webex Video Mesh nodes all over the world. Only Cisco has credentials to write to Docker Hub. The Webex Video Mesh nodes can reach out to Docker Hub using read-only credentials to download the containers for upgrades.

**Note** Images are downloaded based on checksum, which is transmitted to the node as part of the provisioning data. See this document for more details on how docker pull works: https://docs.docker.com/v17.09/engine/userguide/storagedriver/imagesandcontainers/#sharing-promotes-smaller-images

---

**Things to Keep in Mind**

Keep the following information in mind about Webex Video Mesh Node and how it works once registered to your Webex organization:

- When you deploy a new Webex Video Mesh Node, Cisco Webex Teams app and Webex-registered won't recognize the new node for up to 2 hours. The clients check for node reachability during startup, a network change, or cache expiration. You can wait for 2 hours or, as a workaround, restart your Cisco Webex Teams app or reboot the Cisco Webex room or desk device. Afterwards, call activity is captured in the Webex Video Mesh reports in Cisco Webex Control Hub.

- A Webex Video Mesh Node registers to a single Webex organization; it is not a multitenant device.

- To understand what uses Webex Video Mesh Node and what doesn't, see the table in **Clients and Devices That Use Webex Video Mesh Node**, on page 2.
• Webex Video Mesh Node is used locally for all cloud registered devices and SIP video endpoints dialing into a Webex Meeting to handle the media resources if the following conditions are met:
  • The Webex site is on video platform 2.0.
  • The Video Mesh capabilities are enabled under the CMR settings in Control Hub. (You do this step in Enable Webex Video Mesh for the Webex Site, on page 71.) This setting enables cascade links from the Webex Video Mesh Node to the cloud. If this setting is not enabled, then the devices do not use the Webex Video Mesh Node and connect directly to the cloud (just like a scenario where the meeting overflows to the cloud).

• The Webex Video Mesh Node can connect to your Webex site or to another customer or partner's Webex site. For example, Site A deployed a Webex Video Mesh Node cluster and registered it with the example1.webex.com domain. If users in Site A dial in to mymeeting@example1.webex.com, they use the Webex Video Mesh Node and a cascade can be created. If the users in site A dial yourmeeting@example2.webex.com, the Site A users will use their local Webex Video Mesh Node and connect to the meeting on Site B's Webex organization (assuming that Site B also has video platform 2.0 and has the preceding Video Mesh CMR setting enabled).

**What to do next**

• To register additional nodes, repeat these steps.

• If an upgrade is available, we recommend that you apply it as soon as possible. The upgrade process uses these steps:
  1. The provisioning data is pushed to the Cisco Webex cloud by the Cisco development team over secured channels. The provisioning data is signed. For the containers, the provisioning data contains name, checksum, version, and so on. Webex Video Mesh Node also gets its provisioning data from the Cisco Webex cloud over secured channels.
  2. Once Webex Video Mesh Node gets its provisioning data, the node authenticates with read-only credentials and downloads the container with specific checksum and name and upgrades the system. Each container running on Webex Video Mesh Node has an image name and checksum. These attributes are uploaded to the Cisco Webex cloud using secured channels.
  3. The service uses cloudfront.net for distribution of container images.

### Enable Quality of Service (QoS) for Webex Video Mesh Node

**Before you begin**

• Make the necessary firewall port changes that are covered in the diagram and table. See Ports and Protocols Used by Webex Video Mesh, on page 24.

• For Video Mesh nodes to be enabled for QoS, the nodes must be online. Nodes in maintenance mode or offline states are excluded when you enable this setting.
### Procedure

**Step 1**

From the customer view in https://admin.webex.com, go to **Services**, click **Edit settings** on the Video Mesh card, scroll to **Quality of Service**, and then click **Enable**.

When enabled, you get the large, discrete port range (determined by on-premises call control configuration) that's used for audio and video for on-premises SIP clients/endpoints and intracluster cascades with unique DSCP markings:

- Audio: 52500–59499, DSCP EF (Expedited Forwarding)
- Video/Content: 63000–64667, DSCP AF41

All SIP and cascade traffic from Video Mesh nodes is marked with EF for audio and AF41 for video. The discrete port ranges are used as source ports for cascade media to other Video Mesh nodes and cloud media nodes as well as source and destination ports for SIP client media. Webex Teams apps and cascade media continue to use the destination shared port of 5004.

**Note**

All Video Mesh return traffic (audio, video, content) from the shared ports is marked with AF41. The audio traffic needs to be remarked to EF in your network, based on the source port numbers.

A status message appears that shows which nodes are being enabled one-by-one for the QoS port range. You can click **review pending nodes** to see a list of nodes that are pending for QoS. Enabling this setting can take up to 2 hours, depending on call traffic on the nodes.

**Step 2**

If QoS is not fully enabled in 2 hours, **open a case with support** for further investigation.

The nodes reboot and are updated with the new port range.

If you decide to disable the setting, you get the small, consolidate port range that's used for both audio and video (34000–34999). All traffic from Video Mesh nodes (SIP, cascades, cloud traffic, and so on) gets a single marking of AF41.

---

### Verify Webex Video Mesh Node Port Ranges With Reflector Tool in the Web Interface

The reflector tool (a combination of a server on the Webex Video Mesh node and client through a Python script) is used to verify whether the required TCP/UDP ports are open from Webex Video Mesh nodes.

**Before you begin**

- Download a copy of the [Reflector Tool Client (Python script)](resources) and then unzip the file to a location that's easy to find. The zip file contains the script and a readme file.
- For the script to work properly, ensure that you're running Python 2.7.10 or later in your environment.
- Currently, this tool supports SIP endpoints to Webex Video Mesh nodes and intracluster verification.
**Procedure**

**Step 1**  
From the customer view in [https://admin.webex.com](https://admin.webex.com), enable maintenance node for the Video Mesh Node by following these instructions.

**Step 2**  
Wait for the node to show a 'Ready for maintenance' status in Control Hub.

**Step 3**  
In a browser tab, open the Webex Video Mesh node interface ([IP address/setup](https://192.0.2.0/setup)) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 4**  
Scroll to **Reflector Tool**, and then start either the **TCP Reflector Server** or **UDP Reflector Server**, depending on what protocol you want to use.

**Step 5**  
Click **Start Reflector Server**, and then wait for the server to start successfully. You'll see a notice when the server starts.

**Step 6**  
From a system (such as a PC) on a network that you want Video Mesh nodes to reach, run the script with the following command:

```
$ python <local_path_to_client_script>/reflectorClient.py --ip <ip address of the server> --protocol <tcp or udp>
```

At the end of the run, the client shows a success message if all the required ports are open:

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
[--------------------------] 100.00%  Success/Failed/Total: 3/0/3

No ports are blocked for tcp in ['5004', '5060-5061']

Exiting Reflector Client tool...
```

The client shows a failed message if any required ports are not open:

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp --start-port 5060 --end-port 5062 ...
[--------------------------] 100.00%  Success/Failed/Total: 2/1/3

Failed ports in the first try: ['5062']
Retrying (4 times) the above failed ports:
Retry number 1:
  Verifying port -> 5062
Retry number 2:
  Verifying port -> 5062
Retry number 3:
  Verifying port -> 5062
Retry number 4:
  Verifying port -> 5062

Ports which are not open for tcp are: ['5062']

Exiting Reflector Client tool...
```

**Step 7**  
Resolve any port issues on the firewall and then rerun the above steps.

**Step 8**  
Run the client with **--help** to get more details.
Configure Webex Video Mesh Node for Proxy Integration

Use this procedure to specify the type of proxy that you want to integrate with a Webex Video Mesh. If you choose a transparent inspecting proxy or an explicit proxy, you can use the node's interface to upload and install the root certificate, check the proxy connection, and troubleshoot any potential issues.

Before you begin

• See Proxy Support for Cisco Webex Video Mesh, on page 3 for an overview of the supported proxy options.

• Requirements for Proxy Support for Webex Video Mesh, on page 11

Procedure

Step 1 Enter the Webex Video Mesh setup URL https://[IP or FQDN/setup] in a web browser, enter the admin credentials you set up for the node, and then click Sign In.

Step 2 Go to Trust Store & Proxy, and then choose an option:

• **No Proxy** — The default option before you integrate a proxy. No certificate update is required.

• **Transparent Non-Inspecting Proxy** — Video Mesh nodes are not configured to use a specific proxy server address and should not require any changes to work with a non-inspecting proxy. No certificate update is required.

• **Transparent Inspecting Proxy** — Video Mesh nodes are not configured to use a specific proxy server address. No http(s) configuration changes are necessary on Video Mesh; however, the Video Mesh nodes need a root certificate so that they trust the proxy. Inspecting proxies are typically used by IT to enforce policies regarding which websites can be visited and types of content that are not permitted. This type of proxy decrypts all your traffic (even https).

• **Explicit Proxy** — With explicit proxy, you tell the client (Video Mesh nodes) which proxy server to use, and this option supports several authentication types. After you choose this option, you must enter the following information:
  
  a. **Proxy IP/FQDN** — Address that can be used to reach the proxy machine.
  
  b. **Proxy Port** — A port number that the proxy uses to listen for proxied traffic.
  
  c. **Proxy Protocol** — Choose http (Video Mesh tunnels its https traffic through the http proxy) or https (traffic from the Video Mesh node to the proxy uses the https protocol). Choose an option based on what your proxy server supports.
d. Choose from among the following authentication types, depending on your proxy environment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Choose for HTTP or HTTPS explicit proxies where there's no authentication method.</td>
</tr>
<tr>
<td>Basic</td>
<td>Available for HTTP or HTTPS explicit proxies. Used for an HTTP user agent to provide a username and password when making a request, and uses Base64 encoding.</td>
</tr>
<tr>
<td>Digest</td>
<td>Available for HTTPS explicit proxies only. Used to confirm the account before sending sensitive information, and applies a hash function on the user name and password before sending over the network.</td>
</tr>
<tr>
<td>NTLM</td>
<td>Available for HTTP explicit proxies only. Like Digest, used to confirm the account before sending sensitive information. Uses Windows credentials instead of the username and password. If you choose this option, enter the Active Directory domain that the proxy uses for authentication in the <strong>NTLM Domain</strong> field. Enter the name of the proxy workstation (also referred to as a workstation account or machine account) within the specified NTLM domain in the <strong>NTLM Workstation</strong> field.</td>
</tr>
</tbody>
</table>

Follow the next steps for a transparent inspecting or explicit proxy.

**Step 3**  Click **Upload a Root Certificate or End Entity Certificate**, and then locate and choose the root certificate for the explicit or transparent inspecting proxy.

The certificate is uploaded but not yet installed because the node needs to be rebooted to install the certificate. Click the arrow by the certificate issuer name to get more details or click **Delete** if you made a mistake and want to reupload the file.

**Step 4**  For transparent inspecting or explicit proxies, click **Check Proxy Connection** to test the network connectivity between the Video Mesh node and the proxy.

If the connection test fails, you'll see an error message that shows the reason and how you can correct the issue.

**Step 5**  After the connection test passes, for explicit proxy, turn the toggle on to **Route all port 443/444 https requests from this node through the explicit proxy**. This setting requires 15 seconds to take effect.

**Step 6**  Click **Install All Certificates Into the Trust Store** (appears whenever a root certificate was added during proxy setup) or **Reboot** (appears if no root certificate was added), read the prompt, and then click **Install** if you're ready.
The node reboots within a few minutes.

**Step 7**

After the node reboots, sign in again if needed, and then open the **Overview** page to check the connectivity checks to make sure they are all in green status.

The proxy connection check only tests a subdomain of webex.com. If there are connectivity problems, a common issue is that some of the cloud domains listed in the install instructions are being blocked at the proxy.

---

**Integrate Webex Video Mesh With Unified CM or VCS Expressway Call Control Task Flow**

Configure SIP trunks to route SIP dial-in and dial-out for Cisco Webex meetings to Video Mesh. SIP devices don't support direct reachability, so you must use Unified CM or VCS Expressway configuration to establish a relationship between on-premises SIP devices and your Video Mesh clusters.

**Before you begin**

- See [Deployment Models For Webex Video Mesh and Cisco Unified Communications Manager, on page 21](#) to understand common deployment examples.

- Video Mesh supports either TCP or TLS between Unified CM and SIP signaling. SIP TLS is not currently supported for VCS Expressway.

- In Unified CM, each SIP trunk can support up to 16 Video Mesh destinations (IP addresses).

- In Unified CM, incoming ports on SIP trunk security profile can be default (Non Secure SIP Trunk Profile).

- Video Mesh supports 2 route patterns: `sitename.webex.com` and `meet.ciscospark.com`. Other route patterns are unsupported.
### Procedure

<table>
<thead>
<tr>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose one of these options, depending on your call control environment and security requirements:</td>
</tr>
<tr>
<td></td>
<td>- Configure Unified CM Secure TLS SIP Traffic Routing for Webex Video Mesh, on page 59</td>
</tr>
<tr>
<td></td>
<td>- Configure Unified CM TCP SIP Traffic Routing for Webex Video Mesh, on page 62</td>
</tr>
<tr>
<td></td>
<td>- Configure Expressway TCP SIP Traffic Routing for Video Mesh, on page 65 (TCP only)</td>
</tr>
</tbody>
</table>
| **SIP Devices Registered to Unified CM (TLS or TCP)** | Configure Unified CM with Video Mesh, using either TLS encrypted or TCP SIP traffic. You can create a trunk routing policy that reflects cluster preferences, and is highly available and resilient to device failures. If you use Unified CM Session Management Edition (SME), configure trunks on the Unified CM SME and leaf systems so that inbound and outbound calls are evenly distributed across the Unified CM servers within the Session Management cluster. Typically, each site will have a dedicated Unified CM cluster associated with it. These clusters will be connected through intercluster SIP trunks. Each cluster will have call-in trunks to the local site for the Webex Video Mesh nodes. You can also configure your deployment to handle failure or overflow conditions. This configuration helps if there's an outage or if the Video Mesh clusters reached capacity. If the SIP meeting or call cannot
**Purpose**

Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>be established with a cluster, the meeting or call will overflow to the cloud.</td>
</tr>
</tbody>
</table>

**SIP Devices Registered to VCS Expressway (TCP Only)**

Configure neighbor zones and search rules to route SIP dial-in and dial-out for Cisco Webex meetings to Video Mesh clusters. SIP devices registered to a VCS Control or Expressway-C don't support direct reachability, so you must use a TCP-based Expressway configuration to establish a relationship between on-premises SIP devices and your Video Mesh clusters.

You can also configure your deployment to handle failure or overflow conditions. This configuration helps if there's an outage or if the Video Mesh clusters reached capacity. If the SIP meeting or call cannot be established with a cluster, the meeting or call will overflow to the cloud through the VCS Control/Expressway-C or an Expressway C/E pair.

---

**Configure Unified CM Secure TLS SIP Traffic Routing for Webex Video Mesh**

**Procedure**

**Step 1** Create a SIP profile for Video Mesh clusters:

a) From Cisco Unified CM Administration, go to Device > Device Settings > SIP Profile, and then click Find.

b) Choose Standard SIP Profile For Cisco VCS, and then click Copy.

c) Enter a name for the new profile—for example, “Video Mesh SIP Profile”.

d) Under Trunk Specific Configuration, 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 Cisco Webex cloud (routed by the external domain for the Webex site). The setting does not affect any existing SIP trunking or call routing.

   e) Make sure that Enable OPTIONS Ping to monitor destination status for Trunks with Service Type is checked.

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

**Step 2** Add a new SIP trunk security profile for Video Mesh clusters:

a) From Cisco Unified CM Administration, choose System > Security > SIP Trunk Security Profile, and then click Add New.
b) Enter a meaningful name, such as “Video Mesh Secure SIP Trunk Security Profile”

c) Confirm these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Security Mode</td>
<td>Encrypted</td>
</tr>
<tr>
<td>Incoming Transport Type</td>
<td>TLS</td>
</tr>
<tr>
<td>Outgoing Transport Type</td>
<td>TLS</td>
</tr>
<tr>
<td>X.509 Subject Name</td>
<td>Enter the common name of the Video Mesh node certificate.</td>
</tr>
<tr>
<td>Secure Certificate Subject or</td>
<td></td>
</tr>
<tr>
<td>Subject Alternate Name</td>
<td></td>
</tr>
<tr>
<td>Incoming Port</td>
<td>5061</td>
</tr>
<tr>
<td>SIP V.150 Outbound SDP Offer</td>
<td>Use Default Filter</td>
</tr>
</tbody>
</table>

Step 3 Add a new SIP trunk to point to your Video Mesh clusters:

- In a Unified CM-only deployment, add a single trunk.
- In an SME deployment, a trunk typically exists between Unified CM and SME. Add another trunk between SME and Webex Video Mesh nodes. Both trunks must have the same settings specified below.

a) From Cisco Unified CM Administration, choose Device > Trunk, and then click Add New.

b) Choose SIP Trunk for the trunk type; leave the other values and click Next.

c) Enter a meaningful name, such as “Video_Mesh_SIP_Trunk_UCMtoVMN”.

d) Check the SRTP Allowed check box.

e) For Calling and Connecting Party Info Format, check 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 Cisco Webex.

f) Check Run On All Active Unified CM Nodes.

g) Under SIP Information - Destination, enter an IP address or fully qualified domain name (FQDN) for each of your Webex Video Mesh nodes.

h) Enter 5061 for the Destination Port.

i) For the SIP Trunk Security Profile, choose the Video Mesh Trunk Security Profile that you created earlier. (For example, “Video Mesh Secure SIP Trunk Security Profile”.)

j) For the SIP Profile, choose the Video Mesh SIP Profile that you created earlier. (For example, “Video Mesh SIP Profile”.)

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

Note A Webex Video Mesh call or meeting might assign media to any node in a cluster, not just the node that terminates the SIP call.

Step 4 Create a SIP trunk to point to an Expressway for Webex cloud failover.
You can use a SIP trunk already in place for an existing Unified CM and Expressway deployment. If you create another one, and you also run Mobile Remote Access (MRA) with those Expressways, you can break MRA.

Caution a) From Cisco Unified CM Administration, choose Device > Trunk, and then click Add New.
b) Choose SIP Trunk for the trunk type; leave the other values and click Next.
c) Enter a meaningful name, such as “Video_Mesh_VCS_Trunk”.
d) For Calling and Connecting Party Info Format, check 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 Cisco Webex.
e) Under SIP Information - Destination, enter an IP address or fully qualified domain name (FQDN) for each of your Expressways. For the Port, enter 5060.
f) For SIP Profile, choose Standard SIP Profile For Cisco VCS.

Step 5 Create a new route group for calls to Video Mesh clusters:

a) From Cisco Unified CM Administration, choose Call Routing > Route/Hunt > Route Group, and then click Add New.
b) Enter a meaningful name, such as “Video Mesh Node Route Group”.
c) Change the Distribution Algorithm to Top Down.
d) In the Route Group Member Information section, Find the Devices with name Video Mesh.
e) Add “Video_Mesh_SIP_Trunk_UCMtoVMN” by clicking Add to Route Group.
f) Save your changes.

Step 6 For overflow to the cloud, create a new route group for calls to Expressway:

a) From Cisco Unified CM Administration, choose Call Routing > Route/Hunt > Route Group, and then click Add New.
b) Enter a meaningful name, such as “Video Mesh Expressway Route Group”.
c) Change the Distribution Algorithm to Top Down.
d) In the Route Group Member Information section, Find the Devices with name Video Mesh.
e) Add “Video_Mesh_VCS_Trunk” by clicking Add to Route Group.
f) Save your changes.

Step 7 Create a new route list for calls to Video Mesh clusters and Expressway:

a) From Cisco Unified CM Administration, choose Call Routing > Route/Hunt > Route List, and then click Add New.
b) Enter a meaningful name, such as “Video Mesh Node Route List”.
c) Set the Cisco Unified Communications Manager Group to Default, or another value depending on your configuration.
d) Save your changes.
e) In the Route List Member Information section, click Add Route Group, and then choose Video Mesh Route Group.
f) Leave the defaults for the other settings, and then save your changes.
g) In the Route List Member Information section, click Add Route Group, and then choose Video Mesh Expressway Route Group.
h) Leave the defaults for the other settings, and then save your changes.

Step 8 Create a SIP route pattern for the Webex site:

a) From Call Routing > SIP Route Pattern, click Add New and enter the name “Video Mesh Route Pattern for Webex Sites”.
b) In the IPv4 pattern, enter the Webex site for which you want optimized media—For example, “examplesitename.webex.com”.

c) For SIP Trunk/Route List, choose the Route List created for Webex Video Mesh—For example, “Video Mesh Route List”.

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

**Step 9**
Create a SIP route pattern for Cisco Webex Teams app meetings (backwards compatibility):

a) From Call Routing > SIP Route Pattern, click Add New, and then enter the name “Video Mesh Route Pattern for Teams Meetings”.

b) In the IPv4 pattern, enter the meet.ciscospark.com.

c) For SIP Trunk/Route List, choose the Route List created for Webex Video Mesh—For example, “Video Mesh Route List”.

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

---

**Configure Unified CM TCP SIP Traffic Routing for Webex Video Mesh**

**Procedure**

**Step 1**
Create a SIP profile for Video Mesh clusters:

a) From Cisco Unified CM Administration, go to Device > Device Settings > SIP Profile, and then click Find.

b) Choose Standard SIP Profile For Cisco VCS, and then click Copy.

c) Enter a name for the new profile—for example, “Video Mesh SIP Profile”.

d) Under Trunk Specific Configuration, 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 Cisco Webex (routed by the external domain for the Webex site). The setting does not affect any existing SIP trunking or call routing.

e) Make sure that Enable OPTIONS Ping to monitor destination status for Trunks with Service Type is checked.

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

**Step 2**
Add a new SIP trunk security profile for Video Mesh clusters:

a) From Cisco Unified CM Administration, choose System > Security > SIP Trunk Security Profile, and then click Add New.

b) Enter a meaningful name, such as “Video Mesh Trunk Security Profile”

c) Confirm these settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Security Mode</td>
<td>Non Secure</td>
</tr>
<tr>
<td>Incoming Transport Type</td>
<td>TCP+UDP</td>
</tr>
<tr>
<td>Outgoing Transport Type</td>
<td>TCP</td>
</tr>
<tr>
<td>Incoming Port</td>
<td>5060</td>
</tr>
</tbody>
</table>
### Field | Value
---|---
SIP V.150 Outbound SDP Offer Filtering | Use Default Filter

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

#### Step 3

Add a new SIP trunk to point to your Video Mesh clusters:

- In a Unified CM-only deployment, add a single trunk.
- In an SME deployment, a trunk typically exists between Unified CM and SME. Add another trunk between SME and Webex Video Mesh nodes. Both trunks must have the same settings specified below.

a) From Cisco Unified CM Administration, choose Device > Trunk, and then click Add New.
b) Choose SIP Trunk for the trunk type; leave the other values and click Next.
c) Enter a meaningful name, such as “Video_Mesh_SIP_Trunk_UCMtoVMN”.
d) For Calling and Connecting Party Info Format, check 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 Cisco Webex.
e) Check Run On All Active Unified CM Nodes.
f) Under SIP Information - Destination, enter an IP address or fully qualified domain name (FQDN) for each of your Webex Video Mesh nodes.
g) Enter 5060 for the Destination Port.
h) For the SIP Trunk Security Profile, choose the Video MeshTrunk Security Profile that you created earlier. (For example, “Video Mesh Trunk Security Profile”).
i) For the SIP Profile, choose the Video Mesh SIP Profile that you created earlier. (For example, “Video Mesh SIP Profile”).
j) Leave all other fields with their default values and save your changes.

#### Note

A Webex Video Mesh call or meeting might assign media to any node in a cluster, not just the node that terminates the SIP call.

#### Step 4

Create a new SIP trunk to point to an Expressway.

**Caution** You can use a SIP trunk already in place for an existing Unified CM and Expressway deployment. If you create another one, and you also run Mobile Remote Access (MRA) with those Expressways, you can break MRA.

a) From Cisco Unified CM Administration, choose Device > Trunk, and then click Add New.
b) Choose SIP Trunk for the trunk type; leave the other values and click Next.
c) Enter a meaningful name, such as “Video_Mesh_VCS_Trunk”.
d) For Calling and Connecting Party Info Format, check 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 Cisco Webex.
e) Under SIP Information - Destination, enter an IP address or fully qualified domain name (FQDN) for each of your Expressways. For the Port, enter 5060.
f) For SIP Profile, choose Standard SIP Profile For Cisco VCS.

#### Step 5

Create a new route group for calls to Video Mesh clusters:

a) From Cisco Unified CM Administration, choose Call Routing > Route/Hunt > Route Group, and then click Add New.
b) Enter a meaningful name, such as “Video Mesh Node Route Group”.

c) Change the Distribution Algorithm to Top Down.

d) In the Route Group Member Information section, Find the Devices with name Video Mesh.

e) Add the “Video_Mesh_SIP_Trunk_UCMtoVMN” by clicking Add to Route Group.

f) Save your changes.

**Step 6** For overflow to the cloud, create a new route group for calls to Expressway:

a) From Cisco Unified CM Administration, choose Call Routing > Route/Hunt > Route Group, and then click Add New.

b) Enter a meaningful name, such as “Video Mesh Expressway Route Group”.

c) Change the Distribution Algorithm to Top Down.

d) In the Route Group Member Information section, Find the Devices with name Video Mesh.

e) Add the “Video_Mesh_VCS_Trunk” by clicking Add to Route Group.

f) Save your changes.

**Step 7** Create a new route list for calls to Video Mesh clusters and Expressway:

a) From Cisco Unified CM Administration, choose Call Routing > Route/Hunt > Route List, and then click Add New.

b) Enter a meaningful name, such as “Video Mesh Node Route List”.

c) Set the Cisco Unified Communications Manager Group to Default, or another value depending on your configuration.

d) Save your changes.

e) In the Route List Member Information section, click Add Route Group, and then choose Video Mesh Route Group.

f) Leave the defaults for the other settings, and then save your changes.

g) In the Route List Member Information section, click Add Route Group, and then choose Video Mesh Expressway Route Group.

h) Leave the defaults for the other settings, and then save your changes.

**Step 8** Create a SIP route pattern for the Webex site:

a) From Call Routing > SIP Route Pattern, click Add New and enter the name “Video Mesh Route Pattern for Webex Sites”.

b) In the IPv4 pattern, enter the Webex site for which you want optimized media—For example, “examplesitename.webex.com”, where examplesitename is the name of your actual Webex site.

c) For SIP Trunk/Route List, choose the Route List created for Webex Video Mesh—For example, “Video Mesh Route List”.

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

**Step 9** Create a SIP route pattern for Cisco Webex Teams app meetings:

a) From Call Routing > SIP Route Pattern, click Add New, and then enter the name “Video Mesh Route Pattern for Teams Meetings”.

b) In the IPv4 pattern, enter the meet.ciscospark.com.

c) For SIP Trunk/Route List, choose the Route List created for Webex Video Mesh—For example, “Video Mesh Route List”.

d) Leave all other fields with their default values and save your changes.
Configure Expressway TCP SIP Traffic Routing for Video Mesh

**Procedure**

**Step 1** Create a zone that points to Video Mesh clusters:

a) From VCS Control or Expressway-C, go to **Configuration > Zones > Zones**, and then click **New**.

b) Configure the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name that easily identifies the zone—for example, <strong>WebexVideoMeshZone</strong></td>
</tr>
<tr>
<td>Type</td>
<td><strong>Neighbor</strong></td>
</tr>
<tr>
<td><strong>H.323</strong></td>
<td><strong>Off</strong></td>
</tr>
<tr>
<td>Mode</td>
<td><strong>SIP</strong></td>
</tr>
<tr>
<td><strong>5060</strong></td>
<td><strong>TCP</strong></td>
</tr>
<tr>
<td>Location</td>
<td><strong>Address</strong></td>
</tr>
<tr>
<td>Peers</td>
<td>Enter the IP addresses for each Webex Video Mesh node.</td>
</tr>
</tbody>
</table>


c) Leave the other fields with their default settings, and then save your changes.

**Step 2** Create dial patterns for Video Mesh clusters for Webex sites:

a) From Expressway-C, go to **Configuration > Dial Plan > Search Rules**, and then click **New**.

b) Configure the following fields for the Webex site search rule:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Enter a rule name that easily identifies the search rule—for example, <strong>WebexVideoMesh-YourSite</strong></td>
</tr>
<tr>
<td><strong>100</strong></td>
<td>Ensure that this number is lower than the cloud fallback and B2B rules.</td>
</tr>
<tr>
<td><strong>SIP</strong></td>
<td><strong>Alias Pattern Match</strong></td>
</tr>
<tr>
<td><strong>Regexp</strong></td>
<td><strong>Deployment Guide for Cisco Webex Video Mesh</strong> <strong>65</strong></td>
</tr>
</tbody>
</table>
CMR-Hybrid uses a cascade between the on-premises TelePresence Server/MCU to Webex. The URI of the cascade represents the telephony domain site and the meeting that the cascade is for. The first two digits identify which telephony domain the call routes to, and the rest is the unique identifier for the meeting. These URIs are always 22-25 characters.

**Pattern String**

- \1@\2

**Replace String**

\1@\2

**On Successful Match**

Stop

**Target**

Choose the Webex Video Mesh zone that you created—for example, WebexVideoMeshZone.

c) Leave the other fields with their default settings, and then save your changes.
d) From Expressway-C, go to **Configuration > Dial Plan > Search Rules**, and then click **New**.
e) Leave the other fields with their default settings, and then save your changes.

**Step 3**

Create a traversal client and zone pair that points to the cloud Expressway for failover:

a) See the Expressway Basic Configuration Guide for your release for steps to create the traversal client and zone pair.

**Step 4**

Create a fallback search rule to the Traversal Client Zone that leads to the Expressway-E:

a) From Expressway-C, go to **Configuration > Dial Plan > Search Rules**, and then click **New**.
b) Configure the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Enter a rule name that easily identifies the search rule—for example, WebexVideoMesh-Fallover</td>
</tr>
<tr>
<td>Priority</td>
<td>100 is the default. Ensure that the priority is lower by entering a number that is higher than the Video Mesh dial pattern, short address, and B2B rules. (For example, if the short address priority is 110, enter 120.)</td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP</td>
</tr>
</tbody>
</table>
c) Leave the other fields with their default settings, and then save your changes.

**Step 5**

Create a DNS zone for the cloud Expressway:

a) From Expressway-E, go to Configuration > Zones > Zones, and then click New.
b) Configure the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name that easily identifies the zone—for example, WebexVideoMeshZoneCloud</td>
</tr>
<tr>
<td>Type</td>
<td>DNS</td>
</tr>
<tr>
<td>H.323</td>
<td>Off</td>
</tr>
<tr>
<td>Mode</td>
<td>On</td>
</tr>
<tr>
<td>SIP</td>
<td>On</td>
</tr>
<tr>
<td>Mode</td>
<td>On</td>
</tr>
<tr>
<td>TLS verify mode</td>
<td>On</td>
</tr>
<tr>
<td>TLS verify subject name</td>
<td>sip.webex.com</td>
</tr>
<tr>
<td>TLS verify inbound mapping</td>
<td>On</td>
</tr>
<tr>
<td>Fallback transport protocol</td>
<td>TLS</td>
</tr>
<tr>
<td>Media encryption mode</td>
<td>Force encrypted</td>
</tr>
</tbody>
</table>

c) Leave the other fields with their default settings, and then save your changes.

**Step 6**

Create a dial pattern for the cloud Expressway:

a) From Expressway-E, go to Configuration > Dial Plan > Search Rules, and then click New.

b) Configure the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Enter a rule name that easily identifies the search rule—for example, WebexVideoMesh-toCloud</td>
</tr>
<tr>
<td>Priority</td>
<td>Enter a higher value than the rule for the local Webex Video Mesh nodes. If the nodes are set to 100, set this value to 101. You must also ensure that the value is lower than all B2B rules on your Expressway.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Value</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Protocol</td>
<td>SIP</td>
</tr>
<tr>
<td>Source</td>
<td>Named</td>
</tr>
<tr>
<td>Source Name</td>
<td>Choose the secure traversal server zone from Expressway-C—for example, WebexVideoMeshZone</td>
</tr>
<tr>
<td>Mode</td>
<td>Alias Pattern Match</td>
</tr>
<tr>
<td>Pattern Type</td>
<td>Regex</td>
</tr>
<tr>
<td>Pattern String</td>
<td>(.<em>)(webex.(com)).</em></td>
</tr>
<tr>
<td>Pattern Behavior</td>
<td>Replace</td>
</tr>
<tr>
<td>Replace String</td>
<td>\1@\2</td>
</tr>
<tr>
<td>On Successful Match</td>
<td>Stop</td>
</tr>
<tr>
<td>Target</td>
<td>Choose the failover DNS zone that you created—for example, WebexVideoMeshCloud</td>
</tr>
</tbody>
</table>

**Step 7**  
For SIP devices registered to the Expressway-C, open the device IP address in a browser, go to Setup, scroll to SIP, and choose Standards from the Type drop-down.

---

**Exchange Certificate Chains Between Unified CM and Webex Video Mesh Nodes**

In this task, you do a certificate exchange to establish two-way trust between the Unified CM and Webex Video Mesh interfaces. In combination with the secure trunk configuration, allows encrypted SIP traffic and SRTP media in your organization from trusted Unified CMs to land on trusted Webex Video Mesh nodes.

**Note**  
In a clustered environment, you must install CA and server certificates on each node individually.

**Before you begin**  
For security reasons, we recommend that you use a CA signed certificate on your Video Mesh nodes instead of the node's default self-signed certificate.
**Procedure**

**Step 1**  
In one browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 2**  
Go to **Server Certificates**, and follow these steps to request and upload a certificate and key pair as needed:

- **a)** (Optional) If you need a certificate issued from a certified provider, click **Create a Certificate Signing Request**, fill out the required information on the screen (including the Subject Alternative Name(s), which are FQDNs that must contain the common name, and then generate the request. Download the CSR to submit the request to the provider (you can request multiple ones). They return the certificate authority (CA) signed certificate (the private key was already generated during the CSR creation step).

  **Note**  
  The common name is not a URL. It doesn’t include any protocol (e.g. http:// or https://), port number, or pathname. The common name is technically represented by the commonName field in the X.509 certificate specification. For https://www.example.com, the correct value is example.com.

- **b)** If you received or already have the certificate and key, click **Upload a Server Certificate (.crt or .pem file)**, choose the certificate file, then click **Upload a Private Key (.key file)** and enter a passphrase if you have one.

- **c)** After you get the certificate, go to the first Video Mesh node in a cluster, click **Install Server Certificate**, read the prompt, click **Install**, then click **OK**.

  A Video Mesh node that's registered to the cloud waits up to 2 hours for any calls to end and puts itself into a temporary inactive state (quiesces). Once either the existing calls finish or 2 hours pass (whichever comes first), this node will complete the certificate installation. A prompt appears when the server certificate is installed, and you can then reload the page to view the new certificate and key entry.

- **d)** Click **Download** next to the certificate and key files to save a local copy.

  Save the files somewhere that's easy to remember and leave the Webex Video Mesh instance open in the browser tab.

- **e)** Go to the second Video Mesh node in the cluster, fill in the passphrase, and then upload the private key file. Then click **Upload a Server Certificate** and then choose **Install Server Certificate**, read the prompt, click **Install**, then click **OK**.

- **f)** Repeat these steps for any Video Mesh nodes in the same cluster.

**Step 3**  
In another browser tab, from Cisco Unified OS Administration, go to **Security > Certificate Management**, specify search criteria and click **Find**, then choose the file name of the certificate or certificate trust list (CTL) and click **Download**.

As with the Video Mesh node certificate, save the Unified CM file somewhere that's easy to remember and leave Unified CM instance open in the browser tab.

**Step 4**  
Go back to the Webex Video Mesh node interface tab, click **Trust Store & Proxy**, and then choose an option:

- If the Callmanager's CA certificate is signed by a generally recognized organization, such as DigiCert, GeoTrust, or GlobalSign, then the Video Mesh node will trust it without any additional action required (based on the list of root certificates from the VMN node's host OS, which are updated periodically).
Enable Media Encryption for the Organization and Video Mesh Clusters

Use this procedure to turn on media encryption for your organization and individual Video Mesh clusters. This setting forces an end-to-end TLS setup and you must have a secure TLS SIP trunk in place on your Unified CM that points to your Video Mesh nodes.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified CM is configured with a secure trunk and this Video Mesh Control Hub setting is not enabled.</td>
<td>Calls fail.</td>
</tr>
<tr>
<td>Unified CM is not configured with a secure trunk and this Video Mesh Control Hub setting is enabled.</td>
<td>Calls won't fail but they fall back to non-secure mode.</td>
</tr>
</tbody>
</table>

**Caution**
Cisco endpoints must also be configured with a security profile and TLS negotiation for end-to-end encryption to work. Otherwise, calls overflow to the cloud from endpoints that are not configured with TLS. We recommend that you enable this feature only if all endpoints can be configured to use TLS.
Before you begin

- Configure Unified CM Secure TLS SIP Traffic Routing for Webex Video Mesh, on page 59
- Exchange Certificate Chains Between Unified CM and Webex Video Mesh Nodes, on page 68

Procedure

Step 1
From the customer view in https://admin.webex.com, go to Services, and then click Edit settings from the Video Mesh card.

Step 2
Scroll to Media Encryption, and then toggle on the setting.

This setting makes encryption mandatory on all media channels that pass through Video Mesh nodes in your organization. Note the preceding table and caution note for situations where calls may fail and what's required for end-to-end encryption to work.

Repeat the following steps on each Video Mesh cluster that you want to enable for secure SIP traffic.

Step 3
Click Resources, click a Video Mesh cluster entry in the list, and then click Edit cluster settings.

Step 4
Scroll to SIP Calls, check the checkbox, and then under Trusted SIP sources, enter the Common Name (CN) or any FQDNs that are present in the Subject Alternative Name on the Callmanager certificate (typically the FQDN of the Unified CM).

These entries are identified as trusted SIP sources and are allowed to send secure SIP calls to Webex Video Mesh.

---

Enable Webex Video Mesh for the Webex Site

To use optimized media to the Webex Video Mesh Node for a Webex meeting, Personal Room meeting, or Cisco Webex Teams app meeting that allows you to join from a video device, this configuration needs to be turned on for the Webex site. Enabling this setting links Webex Video Mesh and meeting instances in the cloud together and allows cascades to occur from Webex Video Mesh nodes.

Before you begin

This setting is available if your Webex site is on video platform version 2.0, a mandatory requirement for Webex Video Mesh. This setting is not available if you're on a TSP site. If you don't see this setting and you believe it's an error, you must contact your customer success manager (CSM) or partner.

Procedure

Step 1
Choose one, depending on how you manage your Webex site:

- For Control Hub-managed, from the customer view in https://admin.webex.com, go to Services, click the Webex site from the Meetings card, and then click Configure to access the the Webex site configuration options.
• For Site Admin-managed, proceed directly to Site Administration (https://SITENAME.webex.com/admin, where “SITENAME” is your Webex site name), and then follow the steps below.

**Step 2** From **Common Settings**, click **Cloud Collaboration Meeting Rooms (CMR)**, choose **Video Mesh** for **Media Resource Type**, and then click **Update** at the bottom.

This setting links Webex Video Mesh and meeting instances in the cloud together and allows cascades to occur from Webex Video Mesh nodes. The setting should populate across your environment after 15 minutes. If you leave this field set to Cloud (the default option), all meetings are hosted in the cloud and the Webex Video Mesh node is not used.

---

**Assign Collaboration Meeting Rooms to Cisco Webex Teams Users**

**Procedure**

• If you manage your site through Cisco Webex Control Hub:
  a) From the customer view in https://admin.webex.com, go to Users > Manage Users.
     To assign to users in bulk, see this document.
  b) Assign **Webex Collaboration Meeting Rooms** to users in your organization.

• If you manage your site through Site Admin:
  a) From Site Admin, go to **User Management**.
  b) Edit the user account and check Collaboration Meeting Room.
     To assign to users in bulk, see this document.

**Verify the Meeting Experience on the Secure Endpoint**

Use these steps to verify that the endpoints are securely registered and the correct meeting experience appears.
## Procedure

**Step 1** Join a meeting from the secured endpoint.

**Step 2** Verify that the meeting roster list appears on the device.

This example shows how the meeting list looks on an endpoint with a touch panel:

<table>
<thead>
<tr>
<th>Webex Conference</th>
<th>4:25</th>
<th>3:38 PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 participants</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marc Brown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marla Ross</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONF-ROOM-1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3** During the meeting, access the Webex Conference information from **Call Details**.

**Step 4** Verify that Encryption section shows the **Type** as **AES-128** and the **Status** as **On**.
## Verify the Meeting Experience on the Secure Endpoint

### Webex Conference

**Participant(s)**
- URL
- Call rate: 6000 kbps

**Video**
- Protocol: H264
- Resolution: 1280x720
- Frame rate: 30 fps
- Channel rate: 2484 kbps
- Total packet loss (%): 0.0%
- Current packet loss (%): 0.0%
- Jitter: 1 ms

**Audio**
- Protocol: AACLD
- Channel rate: 63 kbps
- Total packet loss (%): 0.0%
- Current packet loss (%): 0.0%
- Jitter: 1.00 ms

**Encryption**
- Type: AES-128
- Status: On

---

**Deployment Guide for Cisco Webex Video Mesh**

---
CHAPTER 4

Manage and Troubleshoot Webex Video Mesh

- Webex Video Mesh Analytics, on page 75
- Enable 1080p High-Definition Video for On-Premises SIP Devices in Webex Video Mesh Node Meetings, on page 88
- Deregister Webex Video Mesh Node, on page 89
- Move Webex Video Mesh Node, on page 89
- Set Webex Video Mesh Cluster Upgrade Schedule, on page 90
- Delete Webex Video Mesh Cluster, on page 91
- Deactivate Webex Video Mesh, on page 91
- Troubleshoot Webex Video Mesh Node Registration, on page 92
- Manage Webex Video Mesh Node From the Web Interface, on page 92

Webex Video Mesh Analytics

Analytics provide information about how you use your on-premises Webex Video Mesh nodes and clusters in your Cisco Webex organization. With the historical data in the metrics view, you can more effectively manage your Webex Video Mesh resources by monitoring the capacity, utilization, and availability of your on-premises resources. You can use this information to make decisions about adding more Webex Video Mesh nodes to a cluster or creating new clusters, for example. Webex Video Mesh analytics can be found in Cisco Webex Control Hub under Analytics > Video Mesh and Troubleshooting > Recent Resource Usage.

To help with analyzing the data in your organization, you can zoom in on data that appears on the graph and isolate a specific time period. For Analytics, you can also slice and dice reports to show more granular details.
Video Mesh analytics and troubleshooting reports show data in the time zone that is set for the local browser.

Analytics

Webex Video Mesh analytics provide a long-term trend (up to 3 months of data) in the categories of engagement, resource usage, and bandwidth usage.

Recent Resource Usage

The recent resource usage view under troubleshooting provides a near-realtime view of activity in your organization: up to 1 minute aggregation and the ability to view the last 4 hours or 24 hours on all clusters or specific clusters. The page in Cisco Webex Control Hub is automatically refreshed—every 1 minute for the last 4 hours and every 10 minutes for the last 24 hours.
Access, Filter, and Save Webex Video Mesh Analytics

Webex Video Mesh metric reports are available on the Analytics page of Cisco Webex Control Hub (https://admin.webex.com), once Webex Video Mesh is active and has a cluster with at least one registered Webex Video Mesh node.

Procedure

**Step 1**
From the customer view in https://admin.webex.com, choose Analytics, and then click Video Mesh on the upper-right side of the screen.

**Step 2**
Click a category, depending on the type of data you're looking for:

- Engagement
- Resources
- Bandwidth Usage

**Tip**
Click info to get a short description of the donut graph or chart. When done reading, click info again to flip back to the graph view.

**Step 3**
From the drop-down on the right, choose an option to filter on how far back in time you want to show data.

- **Last 7 Days** (Default)—Changes the horizontal axis to every 10 minutes.
- **Last 24 Hours**—Changes the horizontal axis to every 1 hour.
- **Last 30 Days**—Changes the horizontal axis to every 3 hours.
**Last 90 Days**—Changes the horizontal axis to every 8 hours.

**Step 4**  
Interact with the charts or donut graphs by using the following options as needed:

- Click one or more segments on the donut graph or chart view and then click to update the donut view and the corresponding chart view.

- On a specific graph or overview, click maximize if you want to increase the view. The other graphs and overviews won't appear. Click minimize to zoom back out to the default analytics view.

- Choose legend items on the graph or overview to update the view on that specific legend item and then click. For example, after you select the legend item Cloud and On-Premises, the line graph updates with that data highlighted.

- Choose the lasso tool and use it to draw a freehand selection across the data that you want to filter on and then click.  
- On a graph that shows data in a time range, narrow down to a specific time range by clicking on the left and dragging your mouse to the right and then clicking. (This action affects all the related data that appears on the analytics page.)
After you've filtered data in the reports, click more, and then choose a file format option, which saves a local copy of the report so you can use it offline (for example, in an internally created report):

- PDF
- PNG
- CSV

Click Clear all if you'd like to reset the analytics view.

Access, Filter, and Save Webex Video Mesh Troubleshooting Reports

Webex Video Mesh troubleshooting reports are available on the Troubleshooting page of Cisco Webex Control Hub (https://admin.webex.com), once Webex Video Mesh is active and has a cluster with at least one registered Webex Video Mesh node.

Procedure

Step 1 From the customer view in https://admin.webex.com, choose Troubleshooting, then Status, then click View Details on the Video Mesh card.

Tip Click info to get a short description of the donut graph or chart. When done reading, click info again to flip back to the graph view.
Step 2
From the drop-down on the right, choose an option to filter on how far back in time you want to show data.

- **Last 4 Hours** (Default)—When you choose this option, the graph data refreshes every 1 minute.
- **Last 24 Hours**—When you choose this option, the graph data refreshes every 10 minutes.

**Note** You can also choose **All Clusters** or a specific cluster to change the filtered view.

Step 3
Interact with the charts or donut graphs by using the following options as needed:

- Hover over segments on the donut graph or chart view to view information about that specific data point.

- Click legend items on the graph or overview to update the view on the other legend items. For example, after you select the legend item On-Premises, the line graph updates to exclude On-Premises and only include the data for the other legend items.

- On a graph that shows data in a time range, narrow down to a specific time range by clicking on the left and dragging your mouse to the right. (This action affects all the related data that appears on the analytics page.)
Hover over sections of a donut, lines on a graph, or insight points on a graph to view more information on the specific point in time of the data.

After you've filtered data in the reports, click more... and then choose a file format option, which saves a local copy of the report so you can use it offline (for example, in an internally created report):

- PNG
- JPG
- PDF
- CSV
- XLSX

Available Analytics

Engagement

Call Join Activity and Overview

This chart provides a summary and historical trend of call join activity based on where the organization's calls were hosted. The chart gives an overall perspective of the number of calls hosted on the cloud compared to the number of calls that were hosted on on-premises clusters in an organization.

- **Cloud Calls** — Number of call joins that could not use the Video Mesh Nodes, because of no connection to the enterprise network or the calls being subject to enforced policy.

- **Overflowed to Cloud** — Number of call joins made within an enterprise network but overflowed to a cloud node.

- **On-Premises** — Number of calls hosted on any of the enterprise nodes.
Client Type Usage and Overview

This report provides a summary and historical trend of common categories of meeting clients that are used in the organization. This data helps you have access to the most popular categories of client types and assess utilization in the organization.

Common meeting type clients include the following:

- Webex Teams for mobile (iPad, iPhone, Android)
- Webex Teams for desktop (Windows, Mac, web)
- Webex Devices (Room/Desk/Board, Video Endpoints)
- Webex Meetings for desktop (Windows, Mac, Web)
- Webex Meetings for Mobile (iPad, iPhone, Android)
- Webex Meetings Center (Windows, Mac)
- Jabber for desktop (Windows, Mac)
- Jabber for mobile (iOS, Android)
- PSTN Dial In
- SIP Devices
- Desk Phones

Meeting Details and Resources

This report provides a summary and historical trend of the number meetings events at a specific point in time and based on where the organization's calls were hosted:

- **On-Premises**—Meeting and participants were hosted on the enterprise clusters
- **Cloud**—Meeting and participants were hosted on cloud clusters
- **Cloud and On-Premises**—Meeting and participants cascaded between enterprise and cloud clusters

![Meeting Details](image1)

**Resources**

**Node Availability Per Cluster, Total Node Availability, and Overflow to Cloud**

This report shows a percentage of node availability for each cluster that can host calls, an overview of the percentage of clusters that can host calls, and an overview of the calls that overflowed to a cloud cluster. This data helps you gain an overall perspective of offending clusters at the organization level. Click on any of these clusters to filter all the associated graphs to show details that are related to the selected cluster.

![Percentage of Node Availability Per Cluster](image2)

- 100.00% Total Node Availability
- 2.61% Overflow to Cloud

**Node Availability Across On-Premises Clusters and Nodes in Service**

The chart (below on the left) provides a historical trend of node availability for each cluster that can host calls in the organization. After you choose at least one cluster in the left chart, the Nodes in Service chart on the right updates and provides a view of the number of nodes that are in service to host calls over the selected time period.

![Node Availability Across On-Premises Clusters](image3)

**Overflow to Cloud**

This chart shows a trend of calls that overflowed to the cloud. This can happen for a number of reasons—for example, a node exceeds its capacity, is being upgraded, has network connectivity issue, or the Webex site is not properly enabled for Video Mesh. This metric helps you pinpoint potential reasons for overflow and do the capacity planning at the organization level.
The Reason for Overflow column shows error states and provides suggestions for how to troubleshoot the issue.

Call Redirects and Call Redirect Details

This report provides details about the redirected calls and a trend of the number of calls that were not hosted on clusters—typically because of high CPU usage or network capacity being full. These calls redirected to another Video Mesh cluster that was able to host the call. This data helps you gain an overall perspective of the utilization of the clusters in the organization, so that you can better do capacity planning.

For example, after trying a maximum number of nodes in a cluster and all attempts getting rejected, the cloud tries to place the call in another cluster, if available, in the same organization based on the configuration. 16 calls were rejected from San Jose cluster.

The Reason for Redirect column shows error states and provides suggestions for how to troubleshoot the issue.

Call Distribution Across On-Premises Clusters

The chart shows a trend and the donut graph shows a summary of how calls are distributed across the different on-premises clusters in your organization. This report lets you compare the data about calls that are hosted across the various clusters in the organization over time.

Resource Utilization

The chart provides a trend and the donut graph provides a summary of the average resource utilization for the media services used in the Video Mesh clusters (organization view) or a selected cluster compared to other clusters (cluster view).
The CPU utilization is directly proportional to the number of participants that land on an on-premises cluster and how many cloud participants are in the meeting.

**Bandwidth Usage**

This chart shows the trend of total bandwidth used across all Webex Video Mesh clusters when cascades are established between on-premises and the cloud. The value appears in Mbps.

When you choose a cluster on the graph, you see a breakdown of the **cascade bandwidth usage for transmitted and received data** and the **cascade bandwidth usage across streams** (audio, video, and content share).

**Recent Resource Usage**

**Total Calls, Overflow to Cloud, and Clusters in Service**

The overview cards provide an at-a-glance view of your Video Mesh deployment.
**Total Calls**

The sum total of participants that were on a meeting hosted on-premises and participants that were hosted on the Cisco Webex cloud (including overflowed to the cloud) for the Cisco Webex organization

- **Cloud Calls**—Number of calls that could not utilize enterprise Video Mesh Nodes, because of no connection to the enterprise network or being subject to enforced policy.

- **Overflowed to Cloud**—Number of calls made within an enterprise but overflowed to a cloud cluster.

- **On-Premises**—Number of calls hosted on any of the enterprise clusters.

**Overflow to Cloud**

The number of calls that were made within an enterprise but overflowed to a cloud cloud, and a percentage calculation of the increased or decreased overflow trend in the time period that you select.

The overflow to cloud percentage is calculated by this formula: \( \frac{\text{Number of overflow calls}}{\text{Total number of on-premises and overflow calls}} \times 100 \)

**Clusters in Service**

Percentage of clusters that can host calls in the organization.

**Resource Utilization**

A recent view of average CPU utilization trend for all clusters in an organization (organization view) or a selected cluster compared to other clusters (cluster view).

**Call Activity**

Provides a recent view of the call activity trend across the organization, showing the calls that were hosted on-premises and calls hosted on the cloud. The calls that overflowed to the cloud are represented as dots (insight points) on the cloud call graph. Hover over a dot to show the number of calls that overflowed to the cloud at that instance.
Call Distribution Across On-Premises Clusters

Provides a recent view of call activity. This information helps you plan your organization's cluster capacity. Calls that cannot be hosted on this specific cluster are redirected to another on-premise cluster. These redirects are represented as dots on the graph. Hover over a dot to show the number of calls redirected from this specific cluster at that instance.

Cluster Cascade Bandwidth Usage

Shows a recent view of the total bandwidth used across all Webex Video Mesh clusters when cascades are established between on-premises and the cloud. Regardless of the time period that you select on the Analytics page, this data updates every 10 minutes.

The bandwidth value appears in Mbps. The graph shows a breakdown of either or both the transmitted (Tx) and received (Rx) bandwidth.

When you choose a cluster on the graph, you see a breakdown of the cascade bandwidth usage (received and transmitted bandwidth) and the streams bandwidth usage (audio, video, and content share).
Clusters in Service

A recent view of the number of clusters that were in service to host calls over the selected time period.

- **Green**—Clusters that have all nodes in service.
- **Amber**—Clusters that have 1 or more nodes that are not in service.
- **Red**—Clusters that have no available nodes in service.
- **Grey**—Data not available.

Click a cluster name to navigate to the Nodes in Service graph.

Enable 1080p High-Definition Video for On-Premises SIP Devices in Webex Video Mesh Node Meetings

This setting allows your organization to favor 1080p high-definition video for on-premises registered SIP endpoints, with a trade off being a lower meeting capacity. Participants that join a meeting that is hosted in a Webex Video Mesh Node can use 1080p 30fps video if they are all inside the corporate network and they're using an on-premises registered high definition-capable SIP device. The setting applies to all clusters that contain Webex Video Mesh nodes.

**Note**
Cloud-registered devices continue to send and receive 1080p streams, regardless of this setting being turned on or off.

**Procedure**

**Step 1**
From the customer view in [https://admin.webex.com](https://admin.webex.com), go to **Services**, and then click **Settings** on the Video Mesh card.

**Step 2**
Toggle the **Video Quality** setting on.
If this setting is off, the default is 720p.
For video resolutions that the Cisco Webex Teams app supports, see Video Specifications for Calls and Meetings.

**Deregister Webex Video Mesh Node**

Use this procedure to remove a Webex Video Mesh from the Cisco Webex cloud. After completing this procedure, your node is removed from its cluster and is unavailable for use. After deregistering a node, the only way to make it available again is to reregister it.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the customer view in <a href="https://admin.webex.com">https://admin.webex.com</a>, go to Services, and then click Resources under Video Mesh.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the list of resources, go to the cluster that contains the node you want to deregister, choose the node, and then click <strong>Action &gt; Deregister Node</strong>. A message appears asking you to confirm that you want to delete the node.</td>
</tr>
<tr>
<td>Step 3</td>
<td>After you read and understand the message, click <strong>Deregister Node</strong>.</td>
</tr>
</tbody>
</table>

**Move Webex Video Mesh Node**

You may want to move a node from one cluster to another. For example, you may have a new cluster that you want to redistribute nodes to. Use this procedure to move a Webex Video Mesh node. After completing this procedure, your node will only be available to the new resource.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the customer view in <a href="https://admin.webex.com">https://admin.webex.com</a>, go to Services, and then choose Resources under Video Mesh.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the list of clusters, go to the cluster that contains the node that you want to move, click the node and then click <strong>Perform actions on this Node</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the Actions drop-down, click <strong>Move Node</strong>.</td>
</tr>
</tbody>
</table>
| Step 4 | Choose one:  
  - Create a new cluster by entering a name.  
  - Choose an existing cluster. |
| Step 5 | Click **Move Node**. Your node is moved to the new cluster. |

**Related Topics**

Move a Node in to Maintenance Mode
Set Webex Video Mesh Cluster Upgrade Schedule

You can set a specific upgrade schedule or use the default schedule of 3 a.m. Daily United States: America/Los Angeles. You can also choose to postpone an upcoming upgrade, if necessary.

Software upgrades for Webex Video Mesh are done automatically at the cluster level, which ensures that all nodes are always running the same software version. Upgrades are done according to the upgrade schedule for the cluster. When a software upgrade becomes available, you have can manually upgrade the cluster before the scheduled upgrade time.

Before you begin

Note

Urgent upgrades are applied as soon as they are available.

Procedure

Step 1

From the customer view in https://admin.webex.com, go to Services, and then click Resources > View all under Video Mesh.

Step 2

Click a media resource and then click Edit cluster settings.

Step 3

On the Settings page, scroll to Upgrade, and then choose the time and time zone for the upgrade schedule.

Note

Upgrades may take longer than a few minutes if the Webex Video Mesh node is waiting for active calls to end before the upgrade begins. For a more immediate upgrade process, we recommend that you schedule the automatic upgrade window outside of your regular business hours.

Step 4

(Optional) If needed, click Postpone to postpone the upgrade to the following day.

Under the time zone, the next available upgrade date and time are displayed.

Upgrade Behavior

1. The node makes periodic requests to the cloud to see if an update is available.

2. The cloud does not make the upgrade available until the cluster's upgrade window arrives. Once the upgrade window arrives, the update information is given to the node during its next periodic update request to the cloud.

3. The node pulls updates over a secure channel.

4. Existing services are gracefully shut down so that no new calls are routed to the node, and existing calls have time to complete (up to 2 hours).

5. The upgrade is installed.

6. The cloud only triggers the upgrade for a percentage of nodes at a time in a cluster.
Delete Webex Video Mesh Cluster

You can permanently delete a Webex Video Mesh cluster from the Cisco Webex cloud. To complete this procedure, you must either move each node to a different cluster or deregister all the nodes. Deregistering all nodes in a cluster permanently removes them and makes them unavailable for use. The only way to make deregistered nodes available again is to reregister them.

Procedure

Step 1 From the customer view in https://admin.webex.com, go to Services, and then click All Resources.

Step 2 From the list of resources, scroll to the Webex Video Mesh resource that you want to delete, and then click Edit Cluster Settings.

Tip You can click Video Mesh to filter on just Webex Video Mesh resources.

Step 3 Click Delete Cluster, and then choose one:

• Click Move All Nodes. For each node, either create a new resource by entering a name or choose an existing resource from the drop-down list, and then click Continue.
• Click Deregister All Nodes, check the check box, and then click Delete Cluster.

Deactivate Webex Video Mesh

Deactivating Webex Video Mesh removes the ability to have media remain on-premises for your meetings. Also, all in-progress meetings using Webex Video Mesh nodes end and future meetings are hosted in the cloud. Once deactivated, the only way to use Webex Video Mesh is to deploy it from the beginning.

Before you begin

Before you deactivate Webex Video Mesh, you will deregister all Webex Video Mesh nodes.

Procedure

Step 1 From the customer view in https://admin.webex.com, go to Services, choose Settings under Video Mesh, and then click Deactivate.

Step 2 Review the list of clusters, read the disclaimer, check the check box to confirm that you understand this action, and then click Deactivate.

Step 3 When you are ready to deactivate your Webex Video Mesh, click Deactivate Service.

All the Webex Video Mesh nodes and clusters are removed and Webex Video Mesh is no longer configured.
Troubleshoot Webex Video Mesh Node Registration

This section contains possible errors you may encounter during registration of your Webex Video Mesh node to the Cisco Webex cloud and suggested steps to correct them.

The domain could not be resolved

**Possible Cause** This message appears if the DNS settings configured on your Webex Video Mesh node are not correct.

**Solution** Sign in to the console of your Webex Video Mesh node and make sure the DNS settings are correct.

Could not connect to site using port 443 via SSL

**Possible Cause** This message appears if your Webex Video Mesh node cannot connect to the Cisco Webex cloud.

**Solution** Make sure your network allows connectivity on the ports required for Webex Video Mesh. For details, see Ports and Protocols Used by Webex Video Mesh, on page 24.

Manage Webex Video Mesh Node From the Web Interface

Before you can make any network changes to Webex Video Mesh nodes that are registered to the cloud, you must use Control Hub to put them in maintenance mode. For more information and a procedure to follow, see Move a Node Into Maintenance Mode.

**Caution**

Maintence mode is intended solely to prepare a node for shutdown or reboot so that you can make certain networking setting changes (DNS, IP, FQDN) or prepare for hardware maintenance such as replace RAM, hard drive, and so on.

When you place a node into maintenance mode, it does a graceful shutdown of calling services (stops accepting new calls and waits up to 2 hours for existing calls to complete). The purpose of the graceful shutdown of calling services is to allow reboot or shutdown of the node without causing dropped calls.

Access Overview of Webex Video Mesh Node From Web Interface

Within the Webex Video Mesh node web interface, you can access a high-level summary of the node that includes calls status, node health, network settings, cloud connectivity, and so on.

**Procedure**

**Step 1** In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 2** Go to **Overview** (the default page).
The following cards appear:

- **Call Status**—Provides the number of ongoing calls through the node.
- **Node Details**—Provides the node type, software image, software version, OS version, QoS status, and maintenance mode status.
- **Node Health**—Provides usage data (CPU, memory, disk), and service status (Management Service, Messaging Service, NTP Sync).
- **Network Settings**—Provides network information: hostname, interface, IP, gateway, DNS, NTP, and whether dual IP is enabled.
- **Registration Details**—Provides registration status, organization name, org ID, cluster the node is a part of, and cluster ID.
- **Cloud Connectivity**—Runs a series of tests from the node to the Webex cloud and third party destinations that the node needs to access to run properly.
  - Three types of tests are run: DNS resolution, server response time, and bandwidth.

  **Note**

  - DNS tests validate that the node can resolve a particular domain. These tests report as failed if the server does not respond within 10 seconds. They show as "Passed" with an orange "warning color" if the response time is between 1.5 and 10 seconds. The periodic DNS checks on the node generate alarms if the DNS response time is longer than 1.5 seconds.
  - Connect tests validate that the node can connect to a particular HTTPS URL and receive a response (responses other than proxy or gateway errors are accepted as evidence of connection).
  - The list of tests run from the overview page are not exhaustive and do not include port 444 or websocket tests.
  - The node sends alarms if calling processes cannot complete websocket connections to the cloud or connect to call-related services.

  - A Pass or Fail result appears next to each test; you can hover over this text to see more information about what was checked when the test ran.

As shown in the screenshot that follows, alarm notifications can also appear in the side panel, if any alarms were generated by the node. These notifications identify potential issues on the node and make suggestions for how you can troubleshoot or resolve these issues. If no alarms were generated, the notification panel does not appear.
Configure Network Settings From Webex Video Mesh Node Web Interface

If your network topology changes, you can use the web interface for each Webex Video Mesh node and change the network settings there. You may see a caution about changing the network settings, but you can still save the changes in case you’re making changes to your network after changing Webex Video Mesh node settings.

Before you begin

These settings only affect the internal network of the Video Mesh node. If you want to configure the external network, you must use the node console. See the Appendix for more information.

Procedure

Step 1

In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click Sign In.

Step 2

Go to Network.

The current network settings for the node appear.

Step 3

Change the following settings for Host and Network Configuration as needed:

- Under Edit Hostname and Domain, change the Hostname and Domain values.
  An error is displayed if the FQDN (hostname and domain) does not have the correct format.

- Under Network Mode, Enable DHCP is listed, but DHCP is not supported. You must set a static IP address, subnet mask, and gateway.
• Under **Edit Network Configuration**, change the **IP Address** (for the internal interface), **Subnet Mask**, and **Gateway** (a network node that serves as an access point to another network) values.

**Note** The Webex Video Mesh Node must have an internal IP address and resolvable DNS name. The node IP address must not belong to the IP address range reserved for Webex Video Mesh Node internal use. The default reserved IP address range is 172.17.0.0–172.17.255.255, which can be configured later in the Diagnostic menu in the node console. This IP address range is for communication within the Webex Video Mesh Node and between the software containers which hold the different components of the node—for example, SIP interface and media transcoding.

• Under **Edit DNS Servers**, change the DNS server entries, which handle translating domain names to numeric IP addresses. You can enter up to 4 DNS servers.

**Step 4** Click **Save Host and Network Configuration**, and after the popup appears that says the node needs to reboot, click **Save and Reboot**.

During the save, all fields are validated on the server side. Warnings that appear generally indicate that the server isn't reachable or a valid response wasn't returned when queried—for example, if the FQDN is not resolvable using the DNS server addresses provided. You may choose to save by ignoring the warning but calls will not work until the FQDN can resolve to the DNS configured on the node. Another possible error state is if the gateway address is not in the same subnet as the IP address. After the Webex Video Mesh Node reboots, the network configuration changes take effect.

**Step 5** Change the following settings for **NTP Servers** as needed:

• Under **Edit NTP Servers**, change the values for the NTP server entries, which are used in your organization to synchronize time to the node.

**Step 6** Click **Save NTP Servers**.

If the NTP server is an FQDN and that isn’t resolvable, a warning is returned. If the NTP server FQDN is resolved but the resolved IP can't be queried for NTP time, a warning is returned.

---

**Generate Webex Video Mesh Logs for Support**

You may be instructed to send logs directly to Cisco, or you can download them yourself to attach to a case. Use this procedure from the web interface to generate logs and send them to Cisco or download them from any Webex Video Mesh nodes. The generated log package contains media logs, system logs, and container logs. The bundle provides useful information for connectivity to Webex, platform issues, and call setup or media, so that Cisco can troubleshoot your Video Mesh node deployment for you.

**Procedure**

**Step 1** In a browser tab, open the Webex Video Mesh node interface (**IP address/setup**, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 2** Go to **Troubleshooting**, and then choose an option next to **Send Logs**.
• Click **Send Logs to Cisco** to generate a log bundle from the node and send the bundle directly to Cisco in one step. You'll see a status indicator that changes as the logs are compressed, zipped, and uploaded.
• Click **Download** to generate a long bundle from the node that you can save locally or attach to a case later.

Generated logs are historically stored on the node and remain on the node even after reboots. An upload identifier shows on the page. Support uses this value to identify your uploaded logs.

**Step 3**

When you **open a case or interact with the Cisco TAC**, include the upload identifier value so that your support engineer can access the logs.

If you submitted the log to Cisco directly, you don't need to upload the log bundle to the TAC case.

---

**What to do next**

While logs are uploading to Cisco or being downloaded, you can run a packet capture from the same screen.

---

**Generate Webex Video Mesh Packet Captures for Support**

You can run a packet capture (PCAP) and submit it to Cisco for further analysis. A packet capture takes a snapshot of data packets from all the active interfaces that are crossing or moving over a specific network. After packets are captured and submitted, Cisco can analyze the submitted capture and help with troubleshooting your Video Mesh node deployment.

**Before you begin**

⚠️ **Caution**

The packet capture functionality is intended for debugging purposes only. If you run a packet capture on a live Video Mesh node that is hosting active calls, the packet capture may affect the performance of the node and the generated file might be overwritten. This causes a loss of captured data. We recommend that you run the packet capture only during off peak hours or when the call count is less than 3 on the node.

**Procedure**

**Step 1**

In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 2**

Go to **Troubleshooting**, and then next to **Packet Capture**, toggle the **Start Packet Capture** setting to on to begin the process.

You can start the packet capture and upload logs at the same time.

**Step 3**

Choose one:

• Click **Send PCAP to Cisco** to send the packet capture from the node directly to Cisco. You'll see a status indicator that changes as the packet capture is uploaded.
• Click **Download** to save a local copy of the packet capture from the node. You can attach it to a case later.
After a package capture is built, an upload identifier shows on the page. Support uses this value to identify your uploaded packet capture. The maximum size for packet captures is 2 GB.

**Step 4**
When you *open a case or interact with the Cisco TAC*, include the upload identifier value so that your support engineer can access the packet capture.

---

### Run a Ping from Webex Video Mesh Node Web Interface

You can run a ping from the Webex Video Mesh node web interface. This step tests a destination you enter and sees if the Webex Video Mesh node can reach it.

**Procedure**

**Step 1**
In a browser tab, open the Webex Video Mesh node interface ([IP address/setup](https://192.0.2.0/setup)) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 2**
Go to **Troubleshooting**, scroll to **Ping**, and then enter a destination address that you want to test in the **FQDN or IP Address** field under **Test Connectivity Using Ping**.

**Step 3**
Click **Ping**.

The test runs and you'll see a ping success or failure message. The test does not have a timeout limit. If you receive a failure or the test runs indefinitely, check the destination value that you entered and your network settings.

---

### Run a Trace Route from Webex Video Mesh Web Interface

You can run a traceroute from the Webex Video Mesh node web interface. This step shows the route taken by packets from the node towards the destination that you enter. Viewing the traceroute information helps you determine why a particular connection might be poor and can help you identify problems.

**Procedure**

**Step 1**
In a browser tab, open the Webex Video Mesh node interface ([IP address/setup](https://192.0.2.0/setup)) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 2**
Go to **Troubleshooting**, scroll to **Traceroute**, and then enter a destination address that you want to test in the **FQDN or IP Address** field under **Trace Route to Host**.

The test runs and you'll see trace route success or failure message. The test times out at 16 seconds. If you receive a failure or the test times out, check the destination value that you entered and your network settings.
Check NTP Server from Webex Video Mesh Node Web Interface

You can enter a FQDN or IP address of a network time protocol (NTP) server to confirm that the Webex Video Mesh node can access the server. This test is helpful if you notice time synchronization issues and want to rule out the reachability of the NTP server.

**Procedure**

**Step 1**  
In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 2**  
Go to **Troubleshooting**, scroll to **Check NTP Server**, and then enter a destination address that you want to test in the **FQDN or IP Address** field under **View SNTP Query Response**.

The test runs and you'll see a query success or failure message. The test does not have a timeout limit. If you receive a failure or the test runs indefinitely, check the destination value that you entered and your network settings.

Identify Port Issues With Reflector Tool in the Web Interface

The reflector tool (a combination of a server on the Webex Video Mesh node and client through a Python script) is used to verify whether the required TCP/UDP ports are open from Webex Video Mesh nodes.

**Before you begin**

- Download a copy of the **Reflector Tool Client (Python script)** and then unzip the file to a location that's easy to find. The zip file contains the script and a readme file.
- For the script to work properly, ensure that you're running Python 2.7.10 or later in your environment.
- Currently, this tool supports SIP endpoints to Webex Video Mesh nodes and intracluster verification.

**Procedure**

**Step 1**  
From the customer view in https://admin.webex.com, enable maintenance node for the Video Mesh Node by following **these instructions**.

**Step 2**  
Wait for the node to show a 'Ready for maintenance' status in Control Hub.

**Step 3**  
In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click **Sign In**.

**Step 4**  
Scroll to **Reflector Tool**, and then start either the **TCP Reflector Server** or **UDP Reflector Server**, depending on what protocol you want to use.

**Step 5**  
Click **Start Reflector Server**, and then wait for the server to start successfully.

You'll see a notice when the server starts.
Step 6
From a system (such as a PC) on a network that you want Video Mesh nodes to reach, run the script with the following command:

```
$ python <local_path_to_client_script>/reflectorClient.py --ip <ip address of the server> --protocol <tcp or udp>
```

At the end of the run, the client shows a success message if all the required ports are open:

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
[--------------------------] 100.00% Success/Failed/Total: 3/0/3
##########################
No ports are blocked for tcp in ['5004', '5060-5061']
##########################
Exiting Reflector Client tool...
```

The client shows a failed message if any required ports are not open:

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp --start-port 5060 --end-port 5062
Please wait while verifying tcp for port range: 5060 - 5062 ...
[--------------------------] 100.00% Success/Failed/Total: 2/1/3
Failed in the first try: ['5062']
Retrying(4 times) the above failed ports:
Retry number 1:
  Verifying port -> 5062
Retry number 2:
  Verifying port -> 5062
Retry number 3:
  Verifying port -> 5062
Retry number 4:
  Verifying port -> 5062
##########################
Ports which are not open for tcp are: ['5062']
##########################
Exiting Reflector Client tool...
```

Step 7
Resolve any port issues on the firewall and then rerun the above steps.

Step 8
Run the client with `--help` to get more details.

Enable Debug User Account From Webex Video Mesh Node Web Interface

If support requires access to the Webex Video Mesh node, you can temporarily enable a debug user account so that support can run further troubleshooting.
Procedure

Step 1  In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click Sign In.

Step 2  Go to Troubleshooting, and then toggle on the Enable Debug User setting.

An encrypted passphrase appears that you can provide to Cisco support.

Step 3  Copy the passphrase, paste it in the support ticket or directly to the support engineer, and then click OK when you have it saved.

The debug user account is valid for 3 days, after which it expires.

What to do next

You can disable the account before it expires if you return to the Troubleshooting page and then toggle off the Enable Debug User setting.

Factory Reset a Webex Video Mesh Node From The Web Interface

As part of deregistration cleanup, you can factory reset the Webex Video Mesh node from the web interface. This step removes any configuration you put in place while the node was active, but does not remove the virtual machine entry. Later, you may want to reregister this node as part of another cluster that you build from scratch.

Before you begin

You must use Control Hub to deregister the Webex Video Mesh node from the cluster that's registered in Cisco Webex Control Hub.

Procedure

Step 1  In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click Sign In.

Step 2  Go to Troubleshooting, scroll to Factory Reset, and then click Reset Node.

Step 3  Ensure that you understand the information in the warning prompt that appears, and then click Reset and Reboot.

The node reboots automatically after the factory reset.

Change Admin Passphrase From Web Interface

Use this procedure to change the administrator passphrase (password) for your Webex Video Mesh node by using the web interface.
Procedure

Step 1  In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click Sign In.
Step 2  Go to Account, and next to Change Passphrase, click Change.
Step 3  Enter the Current Passphrase, and then enter a new passphrase value in both New Passphrase and Confirm New Passphrase.
Step 4  Click Save Passphrase.
A "password changed" message appears and then you go back to the sign in screen.
Step 5  Sign in using your new admin login and passphrase (password).

Change Passphrase Expiry Interval From the Web Interface

Use this procedure to change the default passphrase expiry interval of 90 days by using the web interface. When the interval is up, you are prompted to enter a new passphrase when you sign into the Video Mesh node.

Procedure

Step 1  In a browser tab, open the Webex Video Mesh node interface (IP address/setup, for example, https://192.0.2.0/setup) in a web browser, enter the admin credentials you set up for the node, and then click Sign In.
Step 2  Go to Account, and next to Change Passphrase Expiry, enter a new value for Expiry Interval (Days) (up to 365 days), and then click Save Passphrase Expiry Interval.
A success screen appears, and you can then click OK to finish.

The Account page also shows dates for the last passphrase change and the next time the password expires.
Change Passphrase Expiry Interval From the Web Interface
Appendix

- Webex Video Mesh Node Demo Software, on page 103
- Manage Webex Video Mesh Node From the Console, on page 104
- Migrate an Existing Hardware Platform to Webex Video Mesh Node, on page 111
- Feature Comparison and Migration Path from Collaboration Meeting Room Hybrid to Webex Video Mesh, on page 112
- TelePresence Interoperability Protocol and Segment Switching, on page 114

Webex Video Mesh Node Demo Software

Use the Webex Video Mesh Node demo software only for basic demo purposes. Do not add a demo node to an existing production cluster. The demo cluster accepts fewer calls than production and expires 90 days after it is registered to the cloud.

**Note**

- The Webex Video Mesh Node demo software is not supported by the Cisco TAC.
- You cannot upgrade the Webex Video Mesh Node demo software to the full production software version.

Download the demo software image from [this link](#).

**Specifications**

See [System and Platform Requirements for Webex Video Mesh Node Software, on page 10](#) for the specs-based configuration for Webex Video Mesh Node software.

The demo software supports either a single network interface or a dual network interface.

**Capacity**

We do not test the demo image for capacity. You should only use it to test out basic meeting scenarios. See the use cases that follow for guidance.
Use Cases for the Webex Video Mesh Node Demo Software

Media Anchored to On-Premises

- Deploy and configure the node with the demo software.
- Run a meeting that includes the following participants: a Cisco Webex Teams app participant, Cisco Webex endpoint participant, and a Cisco Webex Board.
- After the meeting is over, from the customer view in https://admin.webex.com, go to Analytics to access the Video Mesh reports. In the reports, you can see that the media stayed on-premises.

Meeting with Cloud and On-Premises Participants

- Run another meeting with a couple of Cisco Webex participants on-premises and one in the cloud.
- Observe that all participants can seamlessly join and participate in the meeting.

Manage Webex Video Mesh Node From the Console

Before you can make any network changes to Webex Video Mesh nodes that are registered to the cloud, you must use Control Hub to put them in maintenance mode. For more information and a procedure to follow, see Move a Node Into Maintenance Mode.

⚠️ Caution

Maintence mode is intended solely to prepare a node for shutdown or reboot so that you can make certain networking setting changes (DNS, IP, FQDN) or prepare for hardware maintenance such as replace RAM, hard drive, and so on.

When you place a node into maintenance mode, it does a graceful shutdown of calling services (stops accepting new calls and waits up to 2 hours for existing calls to complete). The purpose of the graceful shutdown of calling services is to allow reboot or shutdown of the node without causing dropped calls.

Change Webex Video Mesh Node Network Settings in the Console

If your network topology changes, you have to open the console interface for each Webex Video Mesh node and change the network settings there. You may see a caution about changing the network settings, but you can still save the changes in case you're making changes to your network after changing Webex Video Mesh node settings.

Procedure

Step 1
Open the node console interface through the VMware vSphere client and then sign in using the admin credentials.

After first time setup of the network settings and if the Video Mesh is reachable, you can access the node interface through secure shell (SSH).

Step 2
From the main menu of the Webex Video Mesh Node console, choose option 2 Edit Configuration and then click Select.
Step 3 Read the prompt that the calls will end on the Webex Video Mesh Node, and then click Yes.

Step 4 Click Static, enter the IP address for the internal interface, Mask, Gateway, and DNS values for your network.

- The Webex Video Mesh Node must have an internal IP address and resolvable DNS name. The node IP address must not belong to the IP address range reserved for Webex Video Mesh Node internal use. The default reserved IP address range is 172.17.0.0–172.17.255.255, which can be configured in the Diagnostic menu. This IP address range is for communication within the Webex Video Mesh Node and between the software containers which hold the different components of the node—for example, SIP interface and media transcoding.

- Deploy all the nodes on the same subnet or VLAN, so that all nodes in a cluster are reachable from wherever the clients reside in your network.

- For a dual NIC DMZ deployment, you can set the external IP address in the next procedure, after you’ve saved the internal network configuration and rebooted the node.

Step 5 Change the default NTP servers to your organization's NTP server or another external NTP server that can be used in your organization.

**Caution** The default NTP servers may not work for all enterprises.

After you configure the NTP server and save network settings, you can follow the steps in Check Health of Webex Video Mesh Node From Console, on page 108 to verify that the time is synchronizing correctly through the specified NTP servers.

Step 6 (Optional) Change the hostname or domain, if required.

**Note**
- To ensure a successful registration to the cloud, use only lowercase characters in the hostname that you set for the Webex Video Mesh Node. Capitalization is not supported at this time.

- When using or configuring FQDN or hostname, you must also enter a valid and resolvable domain. The total length of the FQDN must not exceed 64 characters.

Step 7 Click Save, and then click Save Changes & Reboot.

During the save, DNS validation is performed if you provided a domain. A warning is displayed if the FQDN (hostname and domain) is not resolvable using the DNS server addresses provided. You may choose to save by ignoring the warning but calls will not work until the FQDN can resolve to the DNS configured on the node. After the Webex Video Mesh Node reboots, the network configuration changes take effect.

---

**Change the Administrator Passphrase of the Webex Video Mesh Node**

Use this procedure to change the administrator passphrase (password) for your Webex Video Mesh node in the node's console.

**Procedure**

**Step 1** Open the node console interface through the VMware vSphere client or SSH into a reachable IP address, and then sign in using the admin credentials.
**Step 2**  Open and log in to the VMware ESXi console of the VM for your Webex Video Mesh node.

**Step 3**  In the main menu, choose option 3 Manage Administrator Passphrase, then 1 Change Administrator Passphrase, and then click Enter.

**Step 4**  Read the information on the password expired page, click Enter, and then click it again after the password expiry message.

**Step 5**  Press Enter.

**Step 6**  After you're signed out of the console, go back to the sign in screen, and then sign in using the admin login and passphrase (password) that you expired.

**Step 7**  You are prompted to change your password.

**Step 8**  For Old password, enter the current passphrase, and then press Enter.

**Step 9**  For New password, enter a new passphrase, and then press Enter.

**Step 10**  For Re-enter new password, retype the new passphrase, and then press Enter.

**Step 11**  A "password changed" message appears and then you go back to the sign in screen.

**Run a Ping from Webex Video Mesh Node Console**

You can run a ping from the Webex Video Mesh node console interface. This step tests a destination you enter and sees if the Webex Video Mesh node can reach it.

**Procedure**

**Step 1**  Open the node console interface through the VMware vSphere client or SSH into a reachable IP address, and then sign in using the admin credentials.

**Step 2**  From the Webex Video Mesh node console, go to 4 Diagnostics, and then choose Ping.

**Step 3**  In the ping field, enter a destination address that you want to test, such as an IP address or hostname, and then click OK.

The test runs and you'll see a ping success or failure message. If you receive a failure, check the destination value that you entered and your network settings.

**Enable Debug User Account Through Console**

If support requires access to the Webex Video Mesh node, you can use the console interface to temporarily enable a debug user account so that support can run further troubleshooting on your node.

**Procedure**

**Step 1**  Open the node console interface through the VMware vSphere client or SSH into a reachable IP address, and then sign in using the admin credentials.
Step 2  From the Webex Video Mesh node console, go to 4 Diagnostics, choose 2 Enable Debug User Account, and after the prompt, click Yes.

Step 3  After a message appears that the debug user account was created successfully, click OK to show the encrypted passphrase.

You'll send the encrypted passphrase to support. They use this temporary account and decrypted passphrase to securely access your Webex Video Mesh node for troubleshooting. This account expires after 3 days, or you can disable it when support is finished.

Step 4  Select the start and end of the encrypted data, and copy-paste it into the support ticket or email that you're sending to support.

Step 5  After you send this information to support, return to the Webex Video Mesh node console and press any key to go back to the main menu.

What to do next

The account expires in 3 days, but when support indicates that they finished troubleshooting on the node, you can return the Webex Video Mesh node console, go to 4 Diagnostics, and then choose 3 Disable Debug User Account to disable the account before it expires.

Send Logs from Webex Video Mesh Node Console

You may be instructed to send logs directly to Cisco or through secure copy (SCP). Use this procedure to send logs directly from any Webex Video Mesh nodes that you registered to the cloud.

Procedure

Step 1  Open the node console interface through the VMware vSphere client or SSH into a reachable IP address, and then sign in using the admin credentials.

Step 2  In the main menu, click option 4 Diagnostics and then press Enter.

Step 3  Click 4 Export Log Files, provide feedback if you want, and then click Next.

Step 4  Choose an option:

- Send Logs using SCP, confirm the export of the logs, enter the SCP details (Host, Username, and Dest_Folder), and then click OK.
- Send Logs to Cisco, and then confirm the export of the logs.

Step 5  Choose OK to return to the Webex Video Mesh node main menu.

Step 6  (Optional) Choose 5 Check Status of Log Files Sent to Cisco if you sent the logs to Cisco.

What to do next

Tip  After you send logs, we recommend that you send feedback directly from the Cisco Webex Teams app so that your support contacts have all the information that they need to help you.
Check Health of Webex Video Mesh Node From Console

You can view the node health directly from the Webex Video Mesh node itself. The results are informational, but could aid in troubleshooting steps—for example, if NTP synchronization is not working, you can check the NTP server value in the network settings.

Procedure

**Step 1**
Open the node console interface through the VMware vSphere client or SSH into a reachable IP address, and then sign in using the admin credentials.

**Step 2**
From the Webex Video Mesh node console, go to 4 Diagnostics, and then choose 6 Check Node Health to view the following information about the node:

- Management Service Container
- ETCD (key value store that reliably stores data across a cluster)
- NTP Synchronized
- Disk Space (Free/Used%)
- Memory (Free/Used%)

Configure Container Network on Webex Video Mesh Node

Webex Video Mesh node reserves a subnet range for internal use within the node. The default range is 172.17.0.0–172.17.255.25. The nodes do not respond to any external-to-Webex Video Mesh node traffic originating from this range. You may want to use the node console to change the container bridge IP address to avoid conflicts with other devices in your network.

Procedure

**Step 1**
Open the node console interface through the VMware vSphere client or SSH into a reachable IP address, and then sign in using the admin credentials.

**Step 2**
From the main menu of the Webex Video Mesh node console, go to 4 Diagnostics, and then choose 7 Configure Container Network. After the caution that states that active calls will end on the node, click Yes.

**Step 3**
Change the values for Container Bridge IP and Network Mask, as needed, and then click Save.

You'll see a screen that shows the container network information, including the IP address range reserved for internal operations on the Webex Video Mesh node.

**Step 4**
Click OK.
Identify Port Issues With Reflector Tool in Console

The reflector tool (a combination of a server on the Webex Video Mesh node and client through a Python script) is used to verify whether the required TCP/UDP ports are open from Webex Video Mesh nodes.

Before you begin

- Download a copy of the Reflector Tool Client (Python script) and then unzip the file to a location that's easy to find. The zip file contains the script and a readme file.
- For the script to work properly, ensure that you're running Python 2.7.10 or later in your environment.
- Currently, this tool supports SIP endpoints to Webex Video Mesh nodes and intracluster verification.

Procedure

Step 1 From the customer view in https://admin.webex.com, enable maintenance node for the Video Mesh Node by following these instructions.

Step 2 Wait for the node to show a 'Ready for maintenance' status in Control Hub.

Step 3 Open the node console interface through the VMware vSphere client or SSH into a reachable IP address, and then sign in using the admin credentials.

Step 4 From the Video Mesh Node interface, go to Diagnostics > Reflector Server > Reflector Server for TCP or (UDP). Start the server either for TCP or for UDP.

Step 5 Scroll to Reflector Tool, and then start either the TCP Reflector Server or UDP Reflector Server, depending on what protocol you want to use.

Step 6 Click Start Reflector Server, and then wait for the server to start successfully.

You'll see a notice when the server starts.

Step 7 From a system (such as a PC) on a network that you want Video Mesh nodes to reach, run the script with the following command:

```
$ python <local_path_to_client_script>/reflectorClient.py --ip <ip address of the server> --protocol <tcp or udp>
```

At the end of the run, the client shows a success message if all the required ports are open:

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
[------------------------------------------] 100.00% Success/Failed/Total: 3/0/3

No ports are blocked for tcp in ['5004', '5060-5061']

Exiting Reflector Client tool...
```

The client shows a failed message if any required ports are not open:
Step 8 Resolve any port issues on the firewall and then rerun the above steps.

Step 9 Run the client with `--help` to get more details.

---

### Factory Reset a Webex Video Mesh Node From Console

As part of deregistration cleanup, you can factory reset the Webex Video Mesh node. This step removes any configuration you put in place while the node was active, but does not remove the virtual machine entry. Later, you may want to reregister this node as part of another cluster that you build from scratch.

**Before you begin**

You must use Control Hub to deregister the Webex Video Mesh node from the cluster that’s registered in Cisco Webex Control Hub.

**Procedure**

**Step 1** Open the node console interface through the VMware vSphere client or SSH into a reachable IP address, and then sign in using the admin credentials.

**Step 2** From the Webex Video Mesh node console, go to 4 Diagnostics, and then choose 8 Factory Reset.

**Step 3** Ensure that you understand the information in the note that appears, and then click Reset.

The node reboots automatically after the factory reset.
Migrate an Existing Hardware Platform to Webex Video Mesh Node

You can migrate an existing supported platform (for example, an MM410v or CMS1000 that runs Cisco Meeting Server) to Webex Video Mesh. Use this procedure to guide you through the migration process.

Note
The steps vary, depending on the bundled version of ESXi on the hardware platform.

Before you begin
Download a new copy of the latest Video Mesh Node software image (OVA). Do not deploy a new Webex Video Mesh node with a previously downloaded OVA.

Procedure

Step 1
Sign into the virtual machine interface and then shut down the software that is running on the platform.

Step 2
Delete the software application that was running on the platform.
There must be no software images remaining on the platform. Also, you cannot run Webex Video Mesh node software alongside other software on the same platform.

Step 3
Deploy a new virtual machine from a new OVF or OVA file.

Step 4
Enter a name for the virtual machine and choose the Webex Video Mesh node OVA file.

Step 5
Change disk provisioning to Thick.

Step 6
Upload the mfusion.ova software image that you downloaded.
Step 7 When the virtual machine is running, return to Log in to the Webex Video Mesh Node Console, on page 45 and continue initial configuration of the Webex Video Mesh node.

Feature Comparison and Migration Path from Collaboration Meeting Room Hybrid to Webex Video Mesh

Feature Comparison

To help you understand the benefits of migrating from CMR Hybrid to Webex Video Mesh, this table shows a side-by-side comparison of the key features in each offer. Along with new features detailed below for Webex Video Mesh, the existing Webex functionality will remain the same when combined with Webex Video Mesh. In addition to meeting enhancements, Webex Video Mesh lets you benefit from the agility of cloud-based management and continue to protect your existing investment.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Webex Video Mesh and Cisco Webex Meeting Center Video</th>
<th>CMR Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting Types</td>
<td>Scheduled</td>
<td>Scheduled only</td>
</tr>
<tr>
<td></td>
<td>One Click (Instant)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Personal Meeting (PMR)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consistent experience for premises and cloud-based meetings</td>
<td></td>
</tr>
<tr>
<td>Scheduling</td>
<td>Webex Productivity Tool (Windows and Mac)</td>
<td>Webex-enabled TelePresence Windows and Mac Productivity Tools</td>
</tr>
<tr>
<td></td>
<td>Hybrid Calendar scheduling with @webex Webex Portal</td>
<td>TMS Scheduling</td>
</tr>
<tr>
<td>Meeting Join Options</td>
<td>Dial-in and Dial-out</td>
<td>Dial-in only</td>
</tr>
<tr>
<td></td>
<td>PIN Protected (Host)</td>
<td>OBTP</td>
</tr>
<tr>
<td></td>
<td>One Button To Push (OBTP)</td>
<td></td>
</tr>
</tbody>
</table>
### Migration Path Checklist

Below is a high-level overview of how to migrate an existing site to video platform version 2.0 and prepare the site to integrate with Webex Video Mesh. The steps may vary, depending on your existing environment. Work with your partner or customer success manager to ensure a smooth migration.

1. Make sure that the Meeting Center Video conferencing feature is provisioned on the Webex site.
2. The site admin receives their management portal account. The admin then deploys Webex Video Mesh nodes for the Cisco Webex organization.
3. The site admin assigns the CMR privilege to enable all or some CMR Hybrid users with Cisco Webex Meeting Center Video.
4. (Optional) Disable the CMR Hybrid session type for this subset, and then enable Cisco Webex Meeting Center Video in their user profile.
5. The site admin sets up Webex Video Mesh, and then selects **Hybrid** as the media resource type under Cloud Collaboration Meeting Room Options.
6. The site admin sets up on-premises TelePresence Management Suite (TMS) and One Button to Push (OBTP) to work with Cisco Webex Meeting Center Video. See the Cisco Webex Meeting Center Video Conferencing Enterprise Deployment Guide for guidance.
7. When the CMR privilege is enabled for a user, the Webex Productivity Tools default to the Cisco Webex Meeting Center Video version. All new meetings scheduled by the users are Cisco Webex Meeting Center Video meetings.
8. If conference rooms are included in the invite, OBTP information is pushed to the conference room through TMS (for CMR Hybrid meetings only).
9. Existing meetings that were set up by CMR Hybrid users before they were switched to Cisco Webex Meeting Center Video should continue to work as long as the customer preserves the on-premises MCU and TMS settings.
10. Existing CMR Hybrid meetings cannot be modified or updated to reflect the Cisco Webex Meeting Center Video meeting information. If users want to use new invitation, they must delete the old meetings and create new meetings.
11. If the customer wishes to retire the on-premises MCU, TMS, old CMR Hybrid meetings will not work. New meetings with Cisco Webex Meeting Center Video information must be created.

### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Webex Video Mesh and Cisco Webex Meeting Center Video</th>
<th>CMR Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-Meeting Experience</td>
<td>Unified Roster (Webex Client)</td>
<td>No Unified Roster (Webex Client and TelePresence Server)</td>
</tr>
<tr>
<td></td>
<td>Unified Controls (Webex Client)</td>
<td>Separate Controls (Webex Client and TelePresence Server)</td>
</tr>
<tr>
<td></td>
<td>Lock/Unlock meeting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mute/Unmute TelePresence participants</td>
<td></td>
</tr>
<tr>
<td>Capacity and Deployment Model</td>
<td>Unlimited capacity</td>
<td>Transcoding capacity limited to the TelePresence Server</td>
</tr>
<tr>
<td></td>
<td>On-premises and automatic overflow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switching and transcoding</td>
<td></td>
</tr>
</tbody>
</table>
TelePresence Interoperability Protocol and Segment Switching

Webex Video Mesh supports negotiating TelePresence Interoperability Protocol (TIP) and multiplex (MUX) for both 1-screen and 3-screen IX and TX endpoints.

For three-screen endpoints, all three screens should show video, if there are enough participants in the conference. Another three-screen system in the conference results in segment switching instead of room switching. This means that rather than all three screens becoming large when someone in another three-screen system speaks, only the active pane becomes large. The other two panes are populated by video from other systems. When shown small, all three panes are rendered together (for all devices, one or three screens) with a single bounding box and name label.

Depending on the hosting resources in the cloud, some endpoints will show all three screens of a three-screen room in the film strip, while others will only show one pane. The Cisco Webex Teams app shows just 1 pane, even if the media is on-premises.

For large meetings that overflow from one node and cascade to a second, the same is seen by any endpoints hosted on a different node to the one hosting the three-screen system (only one pane visible in the layout). Presentation sharing requires BFCP to be negotiated through the call path.