# 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:  
  • Source IP Address: Video Mesh Node  
  • Destination IP Address: Webex cloud media services  
  • Source UDP Ports: 35000 to 52499  
  • Destination UDP Ports: 5004  
  • Native DSCP Marking: AF41  
  • Media Type: Test STUN packets  
  • Renamed the "Bandwidth Guidelines" section to "Video Quality and Scaling", and added a link to the Preferred Architecture documentation.  
  • 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:  
  • Webex Video Mesh Analytics  
  • Available Analytics  
  • Recent Resource Usage  
  • 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  
  - Configure Unified CM TCP SIP Traffic Routing for Webex Video Mesh  
  - Configure Expressway TCP SIP Traffic Routing for Video Mesh  
  • 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 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.  
  • 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 with network configuration steps that appear on the Customize template page.  
  • Updated System and Platform Requirements for Webex Video Mesh Node Software with 72vCPUs (the equivalent of CMS 1000) for specifications-based configuration.                                                                                                                                                                                                                          |
<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
</table>
| August 29, 2019    | • Added Explicit Proxy and supported authentication types for explicit proxy configurations (No auth, Basic, Digest, NTLM).  
                     • Proxy Support for Cisco Webex Video Mesh  
                     • Requirements for Proxy Support for Webex Video Mesh  
                     • Configure Webex Video Mesh Node for Proxy Integration  
                     • Added Supported Resolutions and Framerates for Video Mesh.  
                     • Updated Clients and Devices That Use Webex Video Mesh Node to indicate that Webex Call My Video System to Webex cloud-registered video devices uses Video Mesh node. |
| July 24, 2019      | • In the Manage Webex Video Mesh Node From the Web Interface section, made the following updates:  
                     • Added new sections for Ping test, Trace Route test, NTP Server test, Reflector Tool, and Debug User Account.  
                     • Updated the Overview section—Removed cascades from the screenshot and added OS version.  
                     • Moved "Manage Video Mesh from the Console" content to the Appendix of the guide.  
                     • Renamed "Manage Webex Video Mesh" chapter to "Manage and Troubleshoot Webex Video Mesh" and moved registration troubleshooting content to that chapter. |
| July 9, 2019       | • In Call Control and Meeting Integration Requirements for Video Mesh, updated minimum supported versions for Unified CM, Expressway, and Webex sites.  
                     • In Clients and Devices That Use Webex Video Mesh Node, added supported versions of Jabber VDI and Webex VDI (they are SIP clients). Also added a testing disclaimer. |
| May 24, 2019       | • Added new sections on the troubleshooting features and updated overview screen in the Video Mesh node web interface:  
                     • Generate Webex Video Mesh Logs for Support  
                     • Generate Webex Video Mesh Packet Captures for Support  
                     • Access Overview of Webex Video Mesh Node From Web Interface |
<p>| April 25, 2019     | • Updated Manage Webex Video Mesh Node From the Console to state that Control Hub maintenance mode is required before performance any maintenance on Video Mesh nodes. |</p>
<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.</td>
</tr>
</tbody>
</table>
| February 27, 2019  | • In Guidelines for Webex Video Mesh Cluster Deployment, added a statement about the recommended number of nodes in a cluster.  
                    • In the Unified CM configuration sections, changed naming from "Hybrid Media" to "Video Mesh." |
| February 15, 2019  | Added and updated sections to cover transparent (inspecting and non-inspecting) proxy support and secure SIP trunk support for Unified CM-registered endpoints.  
                    **Transparent Proxy Updates**  
                    • Proxy Support for Cisco Webex Video Mesh  
                    • Requirements for Proxy Support for Webex Video Mesh  
                    • Configure Webex Video Mesh Node for Proxy Integration  
                    **Secure SIP Trunk Updates**  
                    • Integrate Webex Video Mesh With Unified CM or VCS Expressway Call Control Task Flow  
                    • Configure Unified CM Secure TLS SIP Traffic Routing for Webex Video Mesh  
                    • Exchange Certificate Chains Between Unified CM and Webex Video Mesh Nodes  
                    • Enable Media Encryption for the Organization and Video Mesh Clusters  
                    • Verify the Meeting Experience on the Secure Endpoint |
| February 6, 2019   | • 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.  
                    • New sections:  
                    • Set The External Network Interface of the Webex Video Mesh Node  
                    • Add Internal and External Routing Rules  
                    • Updated sections:  
                    • Set the Network Configuration of the Webex Video Mesh Node in the Console  
                    • Deployment Models Supported by Video Mesh |
<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 5, 2018</td>
<td>• In Configure Expressway TCP SIP Traffic Routing for Video Mesh, fixed the pattern string that is required for CMR-Hybrid to be exempt from routing to the Video Mesh node <code>(((\d{9})(^XX.{22,25}))@YourSite.webex.com.*)</code>).</td>
</tr>
<tr>
<td></td>
<td>• In the same section, added more context about CMR-Hybrid:</td>
</tr>
<tr>
<td></td>
<td>“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.”</td>
</tr>
</tbody>
</table>