Help Center

Search for an Answer

How Do I Allow Webex Meetings Traffic on My Network?

Article ID: WBX264
Last Updated: Mar 16, 2020
Product: TelePresence, Webex Events, Webex Meetings, Webex Site Administration, Webex Support, Webex Training
Activities: Video Conferencing
Operating System: Mac,Web Browser,Windows Desktop
Release: WBS33, WBS39

202802 view(s) 299 people thought this was helpful

Allow domains access through your Firewall, Web Proxy, or any other filtering device, List of IP addresses by region, Ports u Webex client for communication for both inbound and outbound traffic, Default Ports used by Video Collaboration Devices

How do I allow Webex Meetings traffic on my network?
Network Requirements
Network Requirements for Cisco Webex
How do I optimize firewall and proxy settings for use with Webex services?
What ports need to be opened to use Webex services?
What exceptions should I add to my firewall for Webex?
What IP range is assigned to Webex?
What settings does Webex recommend for proxy servers?

Note:

Special note: UDP is recommended vs. TCP when configuring your media ports. The client will perform a test to attempt connection on UDP 9000. If this closed, the connection will fail back to TCP. Please ensure that UDP 9000 is open outbound and return traffic is allowed back inbound. The connection is initiated outbound from the Webex client to the Webex Server.

Using TCP in a near congested network will cause retransmissions, which in turn can create a choppy video or low bandwidth error experience. UDP doe retransmit, and will provide a better video experience

For more info on the low bandwidth error, see: WBX84420 - Low-Bandwidth Errors in Cisco Webex Video Platform Meetings

Audio/Video packets use the standard RTP protocol. Depending on your existing firewall rules, an adjustment may be necessary to allow the standard RTP protocol.

Solution:

Ports used by Webex Meeting Clients:

Depending on the services you are using in your particular deployment of Webex, you may connect to our services over a variety of different ports.

The chart below is provided to help you identify what ports you might need to open on your firewall. Some services like video collaboration, have on-premise components that configured to use non-standard port ranges. For those devices, please see the specific deployment guide for that device or technology in order to determine the exact ports tc

If you are also leveraging Webex Teams (formerly Cisco Spark) in your environment, implement the settings from this article and the Webex Teams Network Requirements articl

Ports used by the Webex client for communication (both inbound and outbound traffic):

In order to connect to Webex, you must have a working DNS server. Most DNS queries are made over UDP; however, DNS queries may use TCP as well.

Webex website, Webex Desktop App/Productivity Tools, Webex Meetings for Android/iOS, Webex Web App		

Protocol	Port Number(s)	Direction	Access Type	Comments
TCP	80***** / 443	Outbound	Webex Client Access port and Webex Events (Audio Streaming)	The Webex Client makes the majority of its data transfers and loading using HTTPS over port 443. In some cases, port 80 will also be used before being redirected to a secure connection. Webex Events Audio Broadcast is only available on TCP port 443.
TCP/UDP	53	Outbound	DNS	In order to connect to Webex you must have a working DNS server. Most DNS queries are made over UDP; however, DNS queries may use TCP as well.
UDP	9000*****	Outbound	Webex Client Media (VoIP and Video RTP)	The Webex client will try to connect to a Multimedia server over UDP port 9000. If unable to establish a connection over UDP 9000, it will use TCP port 443 and 80. Due to the nature of TCP and how lost delayed packets are retransmitted, it is not recommended to use TCP. We recommend allowing UDP port 9000 whenever possible. (This media is sent over standard RTP. Firewalls should not manipulate the RTP being sent or received.)
TCP	5004*	Outbound	Alternate Webex Client Media (VoIP and Video RTP)	The Webex Desktop App will attempt to connect to a Multimedia server over TCP port 5004 if it cannot establish a connection over UDP port 9000. If both of those ports are closed the connection will be established via TCP port 443. Due to the nature of TCP and how lost delayed packets are retransmitted, it is not recommended to use TCP. We recommend allowing UDP port 9000 whenever possible. (This media is sent over standard RTP. Firewalls should not manipulate the RTP being sent or received.)
TCP/UDP	Operating System Specific Ephemeral Ports	Inbound	Return traffic from Webex	Webex will communicate to the destination port received when the client makes its connection. A firewall should be configured to allow these return connections through.

* See Exceptions below:

- When all three ports (UDP 9000, TCP 80, TCP 5004) are blocked, audio and video will not work for sending and receiving.
- Receiving static (Desktop/Application/Content) sharing will work if these ports (UDP 9000, TCP 80, TCP 5004) are closed: however sending static shares will not.
- With High FPS sharing, both sending and receiving content will not work.

Default Ports used by Video Collaboration Devices:

These ports are provided as a reference only. Please refer to the deployment guide/manufacturer recommendation for full details.

Protocol	Port Number(s)	Direction	Access Type	Comments
TCP	5060-5070	Outbound	SIP signaling	The Webex media edge listens on 5060 - 5070. For more information, please see the configuration guide on the specific service being used: Cisco Webex Meeting Center Video Conferencing Enterprise Deployment Guide.pdf
TCP	5060, 5061 and 5065	Inbound	SIP signaling	Inbound SIP signaling traffic from the Webex cloud
TCP / UDP	1719, 1720 and port 15000-19999	Inbound and Outbound	H.323 LS	If your endpoint requires gatekeeper communication, also open port 1719 which includes Lifesize.
TCP/UDP	Ephemeral Ports 36000-59999	Inbound and Outbound	Media ports	If you're using a Cisco Expressway, the media ranges need to be set to 36000-59999. If you are using a third party endpoint or call control, they need to be configured to use this range.

Ports used by Webex Edge Audio:

Protocol	Port Number(s)	Direction	Access Type	Comments
TCP	5061, 5062	Inbound	SIP Signaling	Inbound SIP signaling for Webex Edge Audio
TCP	5061, 5065	Outbound	SIP Signaling	Outbound SIP signaling for Webex Edge Audio
TCP/UDP	Ephemeral Ports 8000 - 59999	Inbound	Media Ports	On an enterprise firewall, pinholes need to be opened up for incoming traffic to Expressway with port range from 8000 - 59999

`

List of IP address ranges used by Cisco Webex Meeting services:

- 64.68.96.0/19 (CIDR) or 64.68.96.0 - 64.68.127.255 (net range)
- 66.114.160.0/20 (CIDR) or 66.114.160.0 - 66.114.175.255 (net range)
- 66.163.32.0/19 (CIDR) or 66.163.32.0 - 66.163.63.255 (net range)
- 170.133.128.0/18 (CIDR) or 170.133.128.0 - 170.133.191.255 (net range)
- 173.39.224.0/19 (CIDR) or 173.39.224.0 - 173.39.255.255 (net range)
- 173.243.0.0/20 (CIDR) or 173.243.0.0 - 173.243.15.255 (net range)
- 207.182.160.0/19 (CIDR) or 207.182.160.0 - 207.182.191.255 (net range)

- 209.197.192.0/19 (CIDR) or 209.197.192.0 - 209.197.223.255 (net range)
- 216.151.128.0/19 (CIDR) or 216.151.128.0 - 216.151.159.255 (net range)
- 114.29.192.0/19 (CIDR) or 114.29.192.0 - 114.29.223.255 (net range)
- 210.4.192.0/20 (CIDR) or 210.4.192.0 - 210.4.207.255 (net range)
- 69.26.176.0/20 (CIDR) or 69.26.176.0 - 69.26.191.255 (net range)
- 62.109.192.0/18 (CIDR) or 62.109.192.0 - 62.109.255.255 (net range)
- 69.26.160.0/20 (CIDR) or 69.26.160.0 - 69.26.175.255 (net range)

Webex does not support or recommend filtering IP addresses for a particular region. Filtering by region can cause serious degradation to the in meeting experience up to and i inability to join meetings entirely.

Webex leverages the Akamai content delivery network (CDN). The addresses akamaicdn.webex.com and lp.webex.com serve static content and are hosted by Akamai, which h outside of the Webex IP ranges and these are subject to change at anytime.

Domains that need to be whitelisted

Webex recommends that content should not be cached at any time. The following domain(s) will be used by meeting clients that connect to Webex Meetings:

Client Type	Domain(s)
Webex Desktop Clients (Mac/PC, including WebApp the browser based thin client) connecting to Webex Meetings	***.webex.com**
On-prem SIP/H323 devices calling into (or being called back from) a Webex Meeting	***.webex.com** (note IP dialing also available)
Webex Mobile Clients (iOS, Android) connecting to Webex Meetings	***.webex.com**
Teams Desktop Clients, Cloud Registered Devices (including Webex Boards), connecting to Webex Meetings	See Article: Network Requirements for Webex Teams Services

If leveraging the People Insights feature the domain *.accompany.com also needs to be whitelisted.

We also require certificate validation through a certificate revocation list. This Certificate Revocation List is hosted by Quovadis, and will require the following domain to be reac

- *.quovadisglobal.com

If your firewall or web filtering system does not allow wildcard filtering, you can open your firewall by IP address (this is not recommended). Due to the expanding nature of the business, we maintain the right to add IP addresses at any time without notice.

All Webex hosted services are advertised under AS13445. All traffic from AS13445 should be allowed. Services hosted by other service providers are not included here. This partner systems or our content delivery partners. If you are connecting to partner-hosted systems such as a Partner VoIP system, please contact the partner for the appropriat and ports or refer to the peering policy.

Information for China Clusters

- Network Requirements for the Cisco Webex China Cluster

Additional Resource:

- WBX000028782 - Network Requirements for Webex Teams Services