

Virtual Office Technical Requirements

Copyright © 2019, 8x8, Inc.. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

8x8® is a registered trademark of 8x8, Inc.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owner/s. All other brands and/or product names are the trademarks (or registered trademarks) and property of their respective owner/s.

Contents

Purpose	1
Network Considerations	2
Key Terms	4
Requirements	5
Network	5
Subnets	7
<i>Firewall Ports</i>	8
Virtual Office Apps and Classic Meetings Experience	10
New Meetings Experience	11

Purpose

This document provides customers with a checklist of technical requirements, functionality, and capabilities necessary to prepare their network and workstations to interoperate with 8x8 Virtual Office. These changes include shaping traffic to guarantee bandwidth as well as ensuring specific ports are opened to allow proper connection to 8x8 services.

Network Considerations

Like any Internet-based service, voice over IP (VoIP) requires bandwidth to run. If bandwidth is too low or inconsistent, users suffer from a poor VoIP connection. 8x8 system performance is dependent on the underlying network. Make sure to test your Internet connection to ensure it is VoIP-ready; problems with voice calls are most often caused by network congestion in home offices, or by issues with the Internet Service Provider.

On the other hand, hardware (such as your headset) plays a big role in the quality of your VoIP calls. On your computer, Virtual Office would be competing with your browser and other applications for resources such as your computer's CPU time. Factors that can result in downtime or quality degradation can include (but are not limited to) USB headset drivers, viruses, reboots, component failures, CPU overuse, weak Wi-Fi signal, or connecting to saturated access points.

You can improve the quality of your VoIP service by taking items such as the following into consideration:

- Ensure no conflict with any anti-virus application. Do not run virus scans during business hours, as this can tax the resources of your computer.
- Ensure sufficient CPU and memory requirements based on all applications that the end user has open simultaneously.
- Get the latest updates for hardware such as sound card and USB headset drivers.
- Provide users with high-quality headsets.
- Control the user environment to ensure that hardware resources are not overtaxed by a large number of applications open at once.
- When connecting via Wi-Fi, ensure a strong signal, and do not connect to saturated access points.
- When possible, perform proper WLAN assessments with QoS-enabled apps.
- Occasionally reboot your end points, and clear any applications that are not being used; this prevents background applications from consuming hardware resources.
- Avoid streaming video or audio while a VoIP call is in progress.
- Ensure plenty of bandwidth, especially for remote users. Take into account video streaming, multiple devices, ISP throttling speeds, and so on:
 - Make sure users are wired to the network as much as possible.
 - 8x8 recommends that you disable ALG. [Click here](#) for details on ALG and how to disable it.
 - A call on 8x8 Virtual Office requires about 90 kbps of symmetric bandwidth. 8x8 recommends that you keep about half of the available bandwidth free at all times.

- When users are more often connected on VPN from their home or a remote office, please configure split tunnels on 8x8 clients to make sure that 8x8-destined traffic does not traverse the VPN tunnel; this prevents additional latency and complexity.
- Run all tests on the 8x8 Network Utility once, and send 8x8 a report on the results to provide information on your baseline usage and needs.

Key Terms

The following terms are important in understanding your network requirements for 8x8:

- **Jitter:** A measure of the time interval between data packets as they reach their destination. A low degree of jitter indicates a relatively steady stream of data packets.
- **Packet loss:** Data, such as a VoIP transmission, is sent over the Internet in the form of packets. Packet loss occurs when some of these packets do not arrive at their destination. For each packet lost, a small amount of speech is cut out. If the degree of packet loss is high, conversation audio can sound very choppy, delayed, or unclear.
- **MOS score:** The higher your MOS score, the better your VoIP experience will be. A MOS score is measured on a scale of 1 to 5, in which 5 represents the best possible call quality, and 1 represents the worst possible call quality. The scale is subjective, and based on normative data collected from experimental trials.


Requirements

Please work with your 8x8 engineer to run the 8x8 Network Utility on all your networks where you use an 8x8 endpoint. This helps diagnose most common network issues.

If you have a use case that requires the use of the 8x8 Virtual Office desktop app or Virtual Office mobile app over Wi-Fi, you must run the utility on your wireless network as well. If your phones are on a separate VLAN and the Virtual Office apps are on a different VLAN, make sure to run the test on all applicable VLANs.

Network

Parameters	Requirements
Wiring	At least Cat 5 (preferably Cat 6) wiring to each user
PoE (recommended)	For details, please refer to PoE requirements for: <ul style="list-style-type: none">■ Polycom■ Yealink■ Cisco
Packet loss	0% packet loss
Jitter	<20 ms jitter
Network latency	<100 ms latency to 8x8 data centers. VoIP services are known to work even in higher latency conditions up to 150-200 milliseconds. However, this must be maintained consistently with no packet loss.
Bandwidth	■ G711 Codec: 90 kbps symmetric/call

Parameters	Requirements
requirement	<ul style="list-style-type: none"> ■ G722 Codec: 90 kbps symmetric/call ■ G729 Codec: 35 kbps symmetric/call <p>Please make sure you have 50% of your available bandwidth free to accommodate any spike in usage.</p> <p>Always assume that at least 35% of your users are on call at any time. However, depending on your company's use case, you may have a higher percentage.</p>
If running a converged network for voice and data	<p>Configure VLANs to separate the traffic.</p> <p>Please ensure that the Phone VLAN has the following DNS and NTP in its DHCP scope:</p> <ul style="list-style-type: none"> ■ Use 8x8 DNS (Global Traffic Managers) servers 192.84.18.11 and 8.28.0.9 ■ Use 8x8 NTP server ntp.packet8.net <div>  <p>Note: The recommended DNS and NTP do not resolve any other domain except 8x8.com and packet8.net.</p> </div>
Quality of Service (QoS) and traffic shaping	<p>Configure on premises to prioritize voice traffic specific to 8x8 IP ranges on all UDP and TCP ports.</p> <p>Please define egress QoS.</p>
QoS for Wi-Fi	<p>If the majority of your users are on Wi-Fi rather than Ethernet, please make sure you follow the best practices in Wi-Fi deployment to ensure plenty of coverage.</p>
Local DNS consideration	<p>If you use DNS situated on the LAN, please make sure that you are using local Internet service providers as your forwarders.</p>
DHCP scope	<p>Ensure that there are no rules specified to force any provisioning server or NTP server to deviate from default 8x8 values. For example:</p> <ul style="list-style-type: none"> ■ For provisioning servers, you must disable Option 66. ■ For NTP servers (other than 8x8 NTP servers), you must disable Options 4 and 42.
VPN use cases	<p>If your remote users or Internet egress use a VPN tunnel, please make sure that the 8x8 traffic does not traverse it. You need to consider a Split Tunnel to have local Internet egress for 8x8 traffic. In addition, split DNS to resolve 8x8 domain queries locally. Speak to your 8x8 engineer for more</p>

Parameters	Requirements
	information.
WAN failover	We highly recommend that you use dual WAN connections in a failover state by using WAN link redundancy. Dual WAN connections in load balancing are not supported.
Maximum Transmission Unit (MTU)	The network must support an MTU of 1500 bytes per packet. The MTU is the size of the largest protocol data unit that the layer can pass onward.
UDP protocol priority	High
Stateful Packet Inspection (SPI)	Disabled
ALG/Helper and UDP flood detection	Disabled; for details, please refer to our page on ALG and how to disable it .

Subnets

We recommend that you allow outbound traffic to the following 8x8 subnets through your firewall, and have all ports open to 8x8 subnets. Traffic from any IP port on your internal LAN to any IP port on 8x8's secure subnets is outbound only.



Note: 8x8 employs third-party security measures against cyber-attacks, which require traffic to be routed through that service's IP addresses. [Please click here for the list of the latest ranges](#), and make sure to allow outbound TCP connections to them from your network.

Zones	Subnets
US East Coast	<ul style="list-style-type: none"> ■ 8.28.0.0/22 ■ 162.221.238.0/23 ■ 3.14.30.96/27

Zones	Subnets
US West Coast	<ul style="list-style-type: none"> ■ 192.84.16.0/22 ■ 162.221.236.0/23 ■ 8.5.248.0/23 ■ 63.209.12.0/24
United Kingdom	<ul style="list-style-type: none"> ■ 217.163.57.0/24 ■ 18.220.177.235 ■ 18.222.57.56 ■ 52.14.160.43 ■ 3.9.159.0/27
Hong Kong	103.252.162.0/24
Australia	103.239.164.0/24
Brazil	168.90.173.112/28
Amsterdam	64.95.100.96/28
Singapore	117.20.40.192/28
India	124.124.82.224/28
Canada	67.225.14.144/28
TBD (for future use)	209.94.72.0/22

Firewall Ports

If you want to allow access port-by-port rather than by allowing access to subnets, please refer to the following lists of ports and the traffic they support. Note that, if you have enabled access to subnets, you do not need to enable ports individually.

To prevent premature NAT session changes that can cause de-registration, intermittent one way audio, and phones to not pick up or ring when using certain firewalls, our firewall session timers are as follows:

- UDP session timer: 600 seconds
- TCP session timer (TLS connections only, port 5443): 360 seconds

The following customer firewalls must allow both outbound TCP and UDP traffic for 8x8 services to function. Generally, traffic is allowed by default by all firewalls.

Traffic types	TCP and UDP ports
SIP signaling	UDP and TCP 5196-5199 (5199 Primary)
Registration	UDP and TCP 5060-5061 (5060 Primary)
8x8 activation service	UDP and TCP 5299 and 5399
DNS	UDP and TCP 53

The following customer firewalls must allow outbound UDP traffic for 8x8 services to function. Generally, traffic is allowed by default by all firewalls.


Traffic types	UDP ports
Polycom phones	UDP 2222-2269
Cisco Linksys SPA and ATA	UDP 16384-16538
Aastra phones	UDP 3478-3480 (3479 Primary)
Panasonic DECT	UDP 16000-20000
Obihai ATA	UDP 16600-18398
AudioCodes ATA	UDP 6000-6230
Yealink and Yealink DECT	UDP 11780-12780
Virtual Office mobile app	UDP 5199
NTP	UDP 123
8x8 applications	UDP 5401
8x8 applications	<ul style="list-style-type: none"> ■ UDP 24000 to 30999 RTP for voice/video ■ UDP 38000 to 44999 RTP for voice/video ■ UDP 52000 to 58999 RTP for voice/video ■ UDP 50000 to 65535 RTP for Virtual Office Meetings video
Virtual Office desktop app with advanced audio codec	UDP 30000-30040
8x8 Network Diagnostics and Network Monitoring Tools	UDP 3478-3480
BPA	UDP 15044

The following customer firewalls must allow outbound TCP traffic for 8x8 services to function. Generally, traffic is allowed by default by all firewalls.

Traffic types	TCP ports
Switchboard Pro	<ul style="list-style-type: none"> ■ TCP 15000 ■ TCP 20080-23080 ■ TCP 2098-2130
Virtual Office desktop app	<ul style="list-style-type: none"> ■ TCP 80 (HTTP) ■ TCP 443 (RTPM or HTTPS) ■ TCP 8443 (HTTPS Exchange/Gmail) ■ TCP 23960 (Click2Pop)
LDAPS for Corporate Directory	TCP 636
Salesforce plug-in	TCP 2097-2601
Act! integration	TCP 2099
XMPP for Virtual Office desktop app and Virtual Office online app	TCP 5222
SRTP for IP phone	TCP 5443
SRTP for Virtual Office desktop app	TCP 5401
8x8 applications	<ul style="list-style-type: none"> ■ TCP 5960 ■ TCP 9443 ■ TCP 16443 ■ TCP 8243

Virtual Office Apps and Classic Meetings Experience

Parameters	Requirements
Operating systems	<ul style="list-style-type: none"> ■ Windows 7 or newer, with: <ul style="list-style-type: none"> ○ 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor ○ 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit) ○ 16 GB of available hard disk space (32-bit) or 20 GB (64-bit)

Parameters	Requirements
	<ul style="list-style-type: none"> DirectX 9 graphics device with WDDM 1.0 or higher driver <div>  <p>Note: If you are using an international edition of Windows 7 or 10 (such as N or KN) that does not include any audio codecs in the installation package, Virtual Office also requires you to download the Microsoft Windows Media Feature Pack.</p> </div> <ul style="list-style-type: none"> Mac OS 10.10 (Yosemite) or newer
Browsers	<ul style="list-style-type: none"> Internet Explorer® 9.0 or newer Google Chrome 5.0 or newer Firefox® 2.0 or newer Safari™ 3.0 or newer
Bandwidth	Minimum 1.5 Mbps down/up (Cable modem, DSL, or better)
Other	Headset with microphone

Depending on which platform you are using, you will have to tag your SIP and RTP packets differently.

Platform	SIP	RTP
Windows (normal user)	0xA0 (DSCP 40, CS5)	0xE0 (DSCP 56, CS7)
Windows (admin user)	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Mac/iOS (pre-iOS 10/Sierra)	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Mac/iOS (iOS 10/Sierra+)	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Android	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Polycom	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)

New Meetings Experience

We recommend that you allow outbound traffic to the following 8x8 subnets through your firewall, and have all ports open to 8x8 subnets. Traffic from any IP port on your internal LAN to any IP port on 8x8's secure subnets is outbound only.



Note: 8x8 employs third-party security measures against cyber-attacks, which require traffic to be routed through that service's IP addresses. [Please click here for the list of the latest ranges](#), and make sure to allow outbound TCP connections to them from your network.

Zones	Subnets
All zones	<ul style="list-style-type: none"> ■ 13.248.132.124 ■ 76.223.3.109 ■ 13.248.142.92 ■ 76.223.9.91
Virginia	<ul style="list-style-type: none"> ■ 3.219.176.32/27 ■ 54.167.244.60
Ohio	18.220.195.182
Oregon	<ul style="list-style-type: none"> ■ 34.223.80.128/27 ■ 54.214.212.235
Mumbai	13.232.101.208
Singapore	<ul style="list-style-type: none"> ■ 18.139.118.128/27 ■ 3.0.167.49
Sydney	<ul style="list-style-type: none"> ■ 3.106.23.128/27 ■ 54.66.154.44
Canada	35.182.147.109
Frankfurt	<ul style="list-style-type: none"> ■ 3.123.12.160/27 ■ 3.122.28.43
Ireland	63.32.210.13
London	<ul style="list-style-type: none"> ■ 3.9.41.96/27 ■ 35.176.73.125
São Paulo	<ul style="list-style-type: none"> ■ 18.229.100.64/27 ■ 54.233.170.124

The following customer firewalls must allow outbound TCP traffic for 8x8 services to function. Generally, traffic is allowed by default by all firewalls.

Traffic Types	Ports
New Meetings Experience	<ul style="list-style-type: none"> ■ UDP and TCP 443 ■ UDP 10000

In order to use the New Meetings Experience, the following Internet domains must be whitelisted:

Domain Types	Domain URLs
New Meetings Experience server	<ul style="list-style-type: none"> ■ https://api.amplitude.com/ ■ https://8x8.vc/ ■ https://*.jitsi.net/ ■ https://*.8x8.com/ ■ https://www.gravatar.com/ ■ https://*.callstats.io/ ■ https://www.google-analytics.com/ ■ https://*.gstatic.com/ ■ https://*.googleapis.com/ ■ https://*.google.com/ ■ https://*.microsoft.com/ ■ https://*.dropboxapi.com/
Pop-ups from third-party services	<ul style="list-style-type: none"> ■ https://*.dropboxstatic.com ■ https://*.dropbox.com ■ https://*.dropboxusercontent.com ■ https://*.dropboxapi.com ■ https://dropboxcaptcha.com ■ https://*.googleapis.com ■ https://*.gstatic.com ■ https://*.google.com ■ https://*.googleusercontent.com ■ https://*.youtube.com

Domain Types	Domain URLs
	<ul style="list-style-type: none">■ https://*.microsoftonline.com■ https://*.msauth.net■ https://*.live.com■ https://*.microsoft.com■ https://*.microsoftonline-p.com