



Virtual Office

Technical Requirements

Version 4.0

Revision 4.5

Copyright © 2016, 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.

Purpose

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

Requirements

Network	
Wiring	At least Cat 5 (preferably Cat 6) wiring to each user
PoE (recommended)	<p>Polycom phone PoE requirements:</p> <ul style="list-style-type: none"> VVX3xx/4xx phones (maximum consumption 6.5W) default to PoE Class 2 signature to the PoE Switch (minimum power levels at output of PoE switch 7.0W) When an expansion module is connected (max consumption 13W), the hard-wired signature reverts to PoE Class 0 (minimum power levels at output of PoE switch 15.4W)
Packet loss	0% packet loss
Jitter	< 20ms jitter
Network latency	< 100ms latency to 8x8's data centers
Bandwidth Requirement	<ul style="list-style-type: none"> G711 Codec – 90kbps symmetric/call G722 Codec – 90kbps 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.</p>
If running a converged network for voice and data	Configure VLANs to separate the traffic.

QoS (Quality of Service) and Traffic shaping	Configure on premises to prioritize voice traffic specific to 8x8 IP ranges as well as specific UDP and TCP ports.
End-to-End QoS (Recommended)	<p>If phones are on a shared network with data, please ensure a DNS is assigned to the phone that is local and has Global Traffic Management enabled. If phones are on their own subnet, then:</p> <ul style="list-style-type: none"> • Use 8x8 GTM servers 192.84.18.11 and 8.28.0.9. • Use 8x8 NTP server 192.84.16.24 and 8.28.0.60.
Local DNS Consideration	If using DNS situated on the LAN, ensure that 0.pool.ntp.org, pccfg.8x8.com , and pccfg.8x8.com can be resolved.
DHCP Scope	<p>Ensure that there are no rules specified to force any provisioning server or NTP server different than 8x8 default values. For example:</p> <ul style="list-style-type: none"> • Option 66 for Provisioning server • Option 4 and 42 for NTP server
VPN Use Cases	If your remote users/Internet egress uses VPN tunnel, please make sure that the 8x8 traffic does not traverse it. You need to consider Split Tunnel to have local Internet egress for 8x8 traffic. Speak to your 8x8 engineer for more information.
WAN Failover	Highly recommended to use dual WAN connections in a failover state by using WAN link redundancy. Dual WAN connections in load balancing are not recommended.
MTU (Maximum Transmission Unit)	Network must support a MTU of 1500 bytes per packet. MTU is the size of the largest protocol data unit that the layer can pass onwards.

Subnets	
You must allow outbound traffic to these 8x8 subnets through your firewall and have all ports open to 8x8 subnets.	
Subnets	<ul style="list-style-type: none"> • 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 • US East Coast: <ul style="list-style-type: none"> ○ 8.28.0.0/22 ○ 162.221.238.0/23 • UK: 217.163.57.0/24 • HK: 103.252.162.0/24 • AU: 103.239.164.0/24 • Brazil: 168.90.173.112/28 • Amsterdam: 64.95.100.96/27 • Singapore: 117.20.40.192/28

Customer firewall must allow outbound TCP and UDP traffic for 8x8 system to be functioning. (generally allowed by default by all firewall)	
SIP Signaling	UDP/TCP 5196-5199 (5199 Primary)
Registration	UDP/TCP 5060-5061 (5060 Primary)
8x8 Activation Service	UDP/TCP 5299
DNS	UDP/TCP 53

Customer firewall must allow outbound UDP traffic for 8x8 system to be functioning. (generally allowed by default by all firewall)	
Polycom Phones	UDP 2222-2269

Cisco Linksys SPA and ATA	UDP 16384-16404
Astra Phones	UDP 3478-3480 (3479 Primary)
VO Mobile App	UDP 5199
NTP	UDP 123
8x8 Applications	UDP 5401
8x8 Applications	<ul style="list-style-type: none"> • UDP 24,000 to 30,999 RTP for Voice/Video • UDP 38,000 to 44,999 RTP for Voice/Video • UDP 52,000 to 58,999 RTP for Voice/Video • UDP 50000 to 65535 RTP VO meeting 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
QoS for Wi-Fi	Apply the same ports and IP changes to your Wi-Fi network.

<p>Customer firewall must allow outbound TCP traffic for 8x8 system to be functioning.</p> <p>(generally allowed by default by all firewall)</p>	
Switchboard	<ul style="list-style-type: none"> • TCP 15000 • TCP 20080-23080 • TCP 2098-2130
Virtual Office Pro/Virtual Office Meetings	<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! Plug-In	TCP 2099
Virtual Office Desktop App Token Authentication	TCP 5401
Virtual Office Desktop and Online App XMPP	TCP 5222
SRTP for Polycom	TCP 5443
8x8 Application	<ul style="list-style-type: none"> • TCP 5960 • TCP 9443 • TCP 16443 • TCP 8243
UDP protocol priority	High
SPI (Stateful Packet Inspection)	Disabled
ALG/Helper and UDP flood detection	Disabled

Virtual Office Softphone / Pro / Virtual Office Meetings	
Operating Systems	<ul style="list-style-type: none"> • Windows® Vista, Windows 7 or later 4 GB of system memory • Mac OS 10.6 (Snow Leopard®) or newer 4 GB of RAM
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	Min 1.5 Mbps down/up (Cable modem, DSL or better)
Other	Headset with microphone

Packet Tagging Information		
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-iOS10/Sierra)	0x68 (DSCP 26, AF31)	0xB8 (DSCP 46, EF)
Platform	SIP	RTP
Mac/iOS (iOS10/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)