8x8 Global Cloud Communications

Virtual Contact Center

Technical Requirements Guide

Version 9.4

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.

Preface

Use this document to learn how to prepare your network and agent workstations to interoperate with your Virtual Contact Center tenant.

About 8x8, Inc

Virtual Contact Center from 8x8 is the fastest and easiest way to deploy a world-class contact center.

Virtual Contact Center makes it easy to manage all of your customer interactions – phone, email and chat – via a single system. Our award-winning solution is 100% web-based and was developed by industry-leading designers to be extremely easy to use, thus speeding the adoption process for both agents and supervisors. Virtual Contact Center includes all of the functionality you need to provide an exceptional customer experience: skills based routing, multi-media interaction management, IVR, CTI, case & contact management, call recording, real-time monitoring, desktop sharing, reporting, and much more.

8x8, Inc
SALES: 1.877.725.2621
SUPPORT: 1.866.975.2273
vccsales@8x8.com
www.8x8.com

Contents

Overview of Configuration Requirements

The primary requirements to use Virtual Contact Center are:

- a personal computer with a web browser.
- a high-speed connection to the Internet.
- a telephone device.

In typical small business and home setups, you can open your browser, log in to the Virtual Contact Center services site, and gain full access to the service.

In larger business environments, you may be required to configure various browser and network permissions and security policies to allow full access to Virtual Contact Center features.

This document discusses the technical details of the system and network capabilities required to support all features of the Virtual Contact Center application.

You must configure both your network and agent workstations to interoperate with Virtual Contact Center.

On most networks, the only required configuration tasks are to allow Virtual Contact Center to:

- retrieve email messages from your organization’s email server.
- allow Agent Console to access the Virtual Contact Center platform assigned to them.

In networks with aggressive security policies, you may also need to selectively enable access for specific IP addresses and associated firewall ports used by Virtual Contact Center.

For each agent workstation supported by the Virtual Contact Center, you must provide the agent with appropriately-configured network, computer, and telephony equipment.

Network Configuration Requirements

This section describes how to configure the following network components to interoperate with Virtual Contact Center:

- Your email server
- Your firewall or other network address translation (NAT) equipment
- The Collaborate feature

Enabling Virtual Contact Center to Retrieve Email

Virtual Contact Center supports the POP3/POP3 SSL and IMAP/IMAP SSL email protocols.

The only inbound network access required by the Virtual Contact Center are the ports used to retrieve email from your organization's email server. If your network uses only a third-party email host such as AOL, Yahoo, or Gmail, you do not need to open firewall ports to support email access.

When retrieving email from your existing email server, Virtual Contact Center submits the username and password for a mailbox.

The following table is a list of the default access requirements for the ports the Virtual Contact Center uses to retrieve POP3 and IMAP email messages.

Email protocol	Default email port access requirements
POP3	▪ For POP3 email support, enable port 110. ▪ For POP3 SSL, enable port 995.
IMAP	▪ For IMAP email support, enable port 143. ▪ For IMAP SSL, enable port 993.

If your network uses non-default email ports, in the Configuration Manager, use the **Properties** tab of the **Email Channels** page to specify the non-default port numbers.

Alternatively, you can set your firewall to allow all traffic from the IP that Virtual Contact Center uses to contact clients.

The following are the Source IPs required to pull emails from customers' mail systems.

Site	IPs
US West Coast (NA1-NA6, NA11-NA12)	8.21.164.0/24 , 216.136.148.199
US East Coast (NA7-NA10, NA17)	8.28.3.0/24
United Kingdom (EU2-EU3)	217.163.57.0/24
Asia Pacific (AP1)	103.252.162.0/24
Canada (CA1)	142.165.219.0/24
Canada Ontario (BC1)	50.100.15.0/24
Australia (AU1)	103.239.164.0/24

You can set up both ports and firewall settings for added security.

Enabling Outbound HTTP/HTTPS Communications

The only outbound network access required by the Virtual Contact Center are TCP ports 80 and 443, used for HTTPS communications with each Agent Console.

Selectively Enabling IP Addresses and TCP Ports

In networks that block unknown IP addresses and ports by default, you may need to selectively enable the IP addresses and TCP ports used to access your Configuration Manager and Agent Console.

Your Virtual Contact Center representative will provide you with the URL you need to access your Configuration Manager. You can then use that URL information to enable the associated IP traffic to pass through your network’s firewall.

Enabling Call Recording FTP Requirements

To enable downloading of call recordings from your Virtual Contact Center tenant, you must use a FTPS client. 8x8 validates the use of the following FTPS client:

- Core FTP LE, available from http://www.coreftp.com/

Note: Other commercially-available FTPS clients may work, but are not tested and certified by 8x8.

For host name settings in the FTP client, enter a value based on the platform your tenant is hosted on:

- In the United States East (NA1 to NA6, NA11-NA12), type *vcc-ftps-us1.8x8.com*
- In the United States East (NA7 to NA10, NA17), type *vcc-ftps-us2.8x8.com*
- In Canada (CA1-P1/P2), type *vcc-ftps-ca1.8x8.com*
- In Canada Ontario(BC1), type *ftps.on.odcc.bell.ca*
- In the United Kingdom (EU2-P3/P4), type *vcc-ftps-uk2.8x8.com*
- In the United Kingdom (EU3-P5/P6), type *vcc-ftps-uk3.8x8.com*
- In Asia Pacific (AP1-P1/P2), type *vcc-ftps-hk1.8x8.com*
- In Australia (AU1), type *vcc-ftps-sy1.8x8.com*

For a complete list of platform URLs, refer to the Platform URL Guide.

You must also open the following outbound ports on the firewall with the IP address of the specific FTP server (e.g. vcc-ftps-us1.com for United States):

- TCP: 21(FTP)
- TCP: 30000 - 30999

Collaborate Technical Requirements

The optional Collaborate feature in Virtual Contact Center enables agents to connect to a customer computer for the purpose of providing hands-on assistance.

To allow an agent to use the Collaborate feature, and a customer computer to run the Collaborate feature:

- Configure both the agent's and customer's computer to allow traffic to pass through TCP port 5907.
  If an agent's or customer's computer is behind a corporate firewall, the firewall must also permit the Collaborate feature to use TCP Port 5907.
- Verify that the customer computer includes a Java Runtime Environment (JRE).
- Configure the anti-virus software and operating system security features on the customer computer to permit the download and running of the Collaborate program.
  Some anti-virus programs or operating system security features may incorrectly identify the program downloaded to the customer's computer by the Collaborate feature as a security threat.

Configuring Your Network to Support VoIP Telephony

If you plan to use Voice over IP (*VoIP*) for your phone calls, you need to ensure that your network has sufficient capacity to carry the VoIP traffic.

To begin estimating how much network bandwidth your VoIP traffic requires, see Estimating VoIP Network Bandwidth Requirements.

Next, contact Virtual Contact Center Support for assistance determining whether your network contains sufficient bandwidth to support that VoIP traffic.

Finally, use the information in Enabling VoIP Calls to Pass Through Your Network's Firewall to configure your network firewall to permit the VoIP traffic to be transmitted and received.

For information about your agent's use of VoIP, see Agent Voice over IP Telephone Requirements.

Estimating VoIP Network Bandwidth Requirements

If you plan to use VoIP for your Virtual Contact Center voice channels, you must determine whether your network has sufficient capacity to carry the VoIP traffic.

VoIP equipment used in conjunction with Virtual Contact Center must comply with either of the G.729 or G.711a law or G.711µ law CODEC standards.

The following table is a summary of the voice quality and bandwidth usage for the two supported CODECs by Virtual Contact Center.

CODEC	Voice quality and bandwidth usage
G.729	■ Transmits compressed voice (2nd choice recommendation for temporary use until Internet capacity can be increased to support G.711a/µ uncompressed voice encoding) ■ Good voice quality ■ Requires approximately 30 Kbps per VoIP call
G.711a/µ	■ Transmits uncompressed voice (1st choice recommendation; provision Internet capacity accordingly) ■ High voice quality ■ Requires approximately 90-Kbps per VoIP call center **Note:** When setting up devices to use uncompressed

CODEC	Voice quality and bandwidth usage
	voice CODEC, enable both G.711a law and G.711µ law capabilities available on the device. This prevents call quality loss by eliminating transcoding of international VoIP calls. This has no impact on bandwidth requirements. Either choice uses 80 Kbps per call.

You can estimate the amount of network bandwidth required to support your agents' VoIP telephones.

To estimate the network bandwidth required to support a VoIP station:

1. Choose the CODECs you plan to deploy in your network.
2. Multiply each CODEC's bandwidth requirements by the number of simultaneous calls the network must support.
   For example, if you are using a G.711a/µ CODEC, and you need to support 100 simultaneous calls, then multiply 90 Kbits per second by 100 calls to calculate that you need 8.79 Mbps of symmetrical transmit-and-receive bandwidth to support the estimated call volume.
3. Add the bandwidth required to support VoIP traffic to the bandwidth required to support your existing network traffic.
   When calculating total network load, be sure to include all applications that use the network, especially applications with high bandwidth requirements such as video conferencing.

Contacting Virtual Contact Center for a VoIP Simulation

For assistance estimating how well your network carries VoIP traffic, contact your Virtual Contact Center support representative to arrange for a VoIP simulation.

Enabling VoIP Calls to Pass through Your Network's Firewall

If you plan to use VoIP for your agent telephones, you may need to configure your network firewall to permit outbound VoIP traffic.

The following table is a list of the network devices you must configure to support your implementation of Virtual Contact Center.

VoIP Protocol	Associated ports usage
8x8 Virtual Contact Center VoIP Server	Port 5060
Real-Time Transfer Protocol (RTP)	UDP ports 35000-65000. Blocking any of the UDP ports in that range interferes with audio delivery.
SIP Application Layer Gateway (ALG)	If you are using 8x8 Virtual Contact Center SIP registrar, you must disable your router's ALG services. Disabling your router's ALG services enables Virtual Contact Center to manage all SIP processes. The following lists some common network devices and the ALG services that must be disabled to ensure interoperation with Virtual Contact Center: ■ Cisco routers: `sip-fixup` ■ Cisco PIX, versions 6 and below: `sip-fixup` ■ Cisco PIX, versions 7 and above: `sip-inspection` ■ Cisco ASA: `sip-inspection` ■ Netscreen, Juniper: `SIP ALG` ■ Sonicwall: `SIP Transformations` For more information about SIP ALG settings, contact your network equipment supplier.

If you need help configuring your firewall, contact Virtual Contact Center Support.

Overview of Agent Technical Requirements

Each Virtual Contact Center agent requires:

- A properly equipped and configured computer.
- A high-speed network connection.
- A telephone device.

Depending on the types of transactions being managed by Virtual Contact Center, an agent workstation may also require additional equipment or configuration steps.

Agent Network Connectivity Requirements

All Virtual Contact Center agents, supervisors, and administrators must have high-speed Internet access. Examples of high-speed Internet include DSL, Cable, or most corporate LANs.

Although Virtual Contact Center can interoperate with high-speed satellite connections, the round-trip transmission delay inherent in all satellite connections is likely to result in an undesirable degradation in performance.

Dial-up Internet connections are not supported.

Agent Computer Hardware and Software Requirements

The following table is a list of the computer hardware and software required to run Agent Console.

Computer component	Description
Computer hardware	Agents require a personal computer and a high-speed Internet connection capable of running Microsoft Internet Explorer (version 9 or higher), Firefox, or Chrome quickly when accessing popular search sites such as Google and Yahoo. If an agent uses a Voice over IP (VoIP) soft phone provided by 8x8, then the agent's computer and Internet connection must consistently perform well while processing all other desktop applications required by an agent. Agent screens must support a resolution of no less than 1200x900 pixels. Higher screen resolution is recommended.
Java	If the Agent Collaborate feature is enabled, then the computer running the Virtual Contact Center must include a Java Runtime Environment (JRE).
Firewall and Network Address	Virtual Contact Center works with typical default stateful inspection firewall set-

Computer component	Description
Translation (NAT) Requirements	tings. Virtual Contact Center requires standard NAT with any VoIP Application Layer Gateway (ALG) address fix up features disabled. The Virtual Contact Center browser and VoIP phone sessions periodically generate activity to keep stateful inspection ports open. For organizations with restrictive firewall settings, Virtual Contact Center recommends stateful inspection to open the following ports automatically when needed: ■ Agent browser session uses ports 80 and 443. ■ VoIP softphones use ports 5060, 8000 & 8001, plus ports in range 35000-65000. ■ The Collaborate feature uses port 5907. ■ Downloading call recordings through FTPS clients uses port 21 and ports in range 30000-30999. Agents using Counterpath software-based softphones (eyeBeam and Bria) may need to configure any firewall products (for example, Windows firewall, Symantec, or Trend Micro) to allow the softphones to receive calls.

Agent Browser Configuration Requirements

Supported Browsers

- Chrome^{TM}
- Firefox®
- Internet Explorer® 9 to 11
- Microsoft Edge browser

Known Issue: If you use Internet Explorer to run Virtual Contact Center applications, you may encounter high memory usage. To resolve this issue, clear cookies and cache, activate the setting to clear history, clear history on exit, and reboot.

Important: Compatibility View must be disabled in Internet Explorer 9 or older.

Note: Virtual Contact Center is partially compatible with Safari, offering support for the Agent Console Control Panel functionality.

Note: Firefox requires the QuickTime plug-in for audio features.

Managing Agent Browser Security Zones

You may need to configure Internet Explorer to allow you to work with all Agent Console features.

Internet Explorer places Web sites in one of four security zones:

- Internet (most trusted, least strict security settings)
- Local intranet
- Trusted sites
- Restricted sites (least trusted, strictest security settings)

When you assign a site's URL to an Internet Explorer security zone, you are specifying the security settings that Internet Explorer uses when you visit that site. Depending on your call center's security policies, if you are an Agent Supervisor, in Internet Explorer you add the URL of your Agent Supervisor Console to either the **Internet** or **Trusted sites** zone.

If Virtual Contact Center updates the URL of your agent or agent supervisor desktop, you then need to update your Internet Explorer settings in response to that change. More specifically, you must:

1. Remove the old URL from its security zone.
2. Add the new URL to the zone.
3. Configure the new URL's security settings as described in the table for Internet Explorer configuration requirements for Agent and Agent Supervisor accounts, which lists the Internet Explorer tasks you must perform to configure your Agent Console or Agent Supervisor Console to interoperate with your Virtual Contact Center tenant.

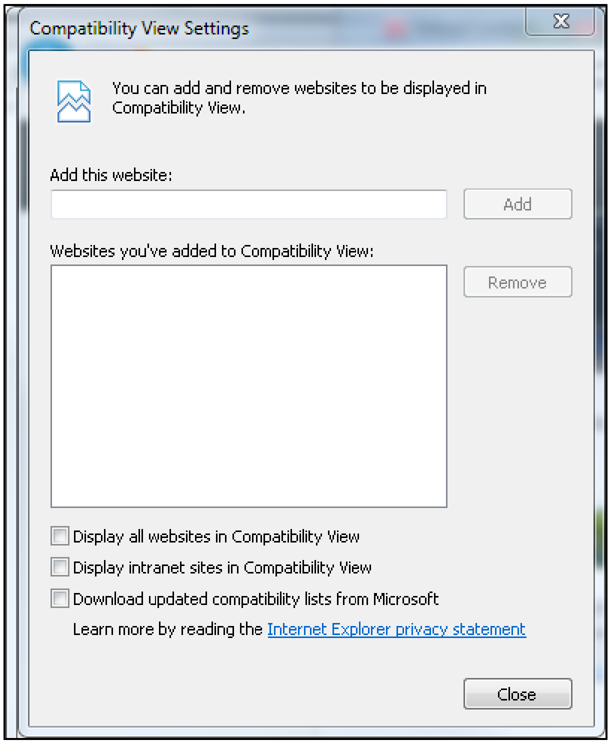
Configuring Internet Explorer

The configuration requirements for Internet Explorer differ slightly, depending on:

- Whether the agent account type is Agent or Agent Supervisor.
- Which version of Internet Explorer the Agent or Agent Supervisor account uses.

The following table is a list of Internet Explorer configuration requirements for Agent and Agent Supervisor accounts.

Agent	Agent Supervisor	IE9-11	Configuration task
X	X	X	For both Agent and Agent Supervisor accounts, in Internet Explorer, you must disable Internet Explorer's SmartScreen Filter feature. **To disable Internet Explorer SmartScreen Filter for both Agent and Agent Supervisor accounts:** 1. In **Tools**, choose **Internet Options**, then click the **Advanced** tab. 2. In the **Security** area of the **Advanced** tab, clear the **Enable SmartScreen Filter** check box to disable the feature.
	X	X	For Agent Supervisor accounts, in all supported versions of Internet Explorer, you must disable file download prompting. **To disable Internet Explorer download prompting for Agent Supervisor accounts:** 1. In **Tools**, choose **Internet Options**, then click the **Security** tab. 2. In the **Security** tab, choose the **Internet** or **Trusted site** zone. For information about security zones, see Managing Agent Browser Security Zones. 3. In the **Security** tab, click **Custom Level**, then in the **Download** section enable **Automatic Prompting for File Downloads**.

Agent	Agent Supervisor	IE9-11	Configuration task
X	X	X	For Agent and Agent Supervisor accounts that use CRM integration, including Salesforce and NetSuite, in all supported versions of Internet Explorer, you must disable pop-up blocking and all Internet accelerators. **To disable Internet Explorer pop-up blocking and accelerators for Agent and Agent Supervisor accounts that use CRM integration:** 1. In **Tools**, choose **Pop-up Blocker**, then choose **Turn Off Pop-up Blocker**. 2. In **Tools**, choose **Manage Add-ons**, then in **Accelerators** right-click each accelerator and choose **Disable**.
X	X	X	If you use IE11, you must turn off compatibility view. In your browser session: 1. Tap or click **Tools**, and then tap or click **Compatibility View Settings**.  Compatibility View Settings You can add and remove websites to be displayed in Compatibility View. Add this website: Websites you've added to Compatibility View: □ Display all websites in Compatibility View □ Display intranet sites in Compatibility View □ Download updated compatibility lists from Microsoft Learn more by reading the Internet Explorer privacy statement 2. Disable all compatibility view settings.

Agent Telephone Connection and Equipment Requirements

To receive telephone calls from the Virtual Contact Center application, agents must have access to one of the following types of telephone connection:

- Public switched telephone network (PSTN) connection
- Voice over IP (VoIP) connection

For both VoIP or PSTN telephones, the telephone assigned to the Virtual Contact Center must:

- Always be available to receive incoming calls.
- Not forward calls to a non-Virtual Contact Center voicemail box before Virtual Contact Center can offer an incoming call to an agent, and forward that call to an agent's Virtual Contact Center voicemail box if no agent accepts the call.

Agent PSTN Equipment Requirements

Public Switched Telephone Network (PSTN) telephone connections:

- Can be directly accessed by dialing a Direct Inward Dialing (DID) phone number.
- Must not prompt or otherwise require a caller to dial a separate extension number.

Virtual Contact Center supports the following types of PSTN equipment:

- A telephone connected to a conventional telephone wire (landline)
- A cell phone
- A direct-access IP phone

Agent Voice over IP Telephone Requirements

Voice over IP (VoIP) telephone connections use a data connection to originate and transport telephone calls.

The Virtual Contact Center supports the following types of VoIP telephone equipment:

- Software-based VoIP phones, such as the CounterPath eyeBeam Basic softphone
- Hardware-based VoIP phones, such as the Cisco 7940/7960 series IP phone

For more information about using eyeBeam softphones, see firewall and NAT requirements in the table listing computer hardware and software required to run Agent Console.

For more information about VoIP equipment and configuration, contact Virtual Contact Center Support.

Agent VoIP Headset Selection Guidelines

To help you select agent headsets, 8x8 recommends professional-quality equipment manufactured by leading companies such as Plantronics or Jabra (aka GN Netcom).

Consider the following criteria when selecting an agent headset:

Headset component	Description
Connection interface	Manufacturers of high-quality telephone headsets offer products that can be connected to either: ■ Different models and brands of desktop telephones ■ Computer-based soft phones via a computer's USB connector Avoid PC sound card analog headsets that require the use of separate headphone and microphone plugs. These headsets generally do not deliver high-quality sound, and tend to have poor-quality microphones.
Microphone sensitivity	■ Select a headset that is suitable for the agent's work environment (e.g. quiet or noisy surroundings). ■ Avoid headsets that use omnidirectional microphones, as they can pick up too much background noise. ■ Conversely, be sure the headset microphone is sensitive enough to transmit the full spectrum of the human voice. Test with external callers.

Note: Consumer-grade headsets are generally not suitable for contact center agents due to inferior audio performance, lack of all-day comfort, and limited durability. Agent productivity and customer frustration losses quickly negate any benefits of low-cost and ill-suited headsets.

8x8-Suggested Headsets

8x8 recommends using any of the professional Plantronics models listed on the 8x8 web store. You may also use alternative brands such as Jabra. Professional headsets are sometimes sold in two parts. In this case, the TOP PART is the headset itself, and the BOTTOM PART is the interface adapter (which is either USB for softphones, or an adapter designed for a particular brand and model of desk phone).

8x8 suggests the following professional headsets with USB connectors for soft phones:

- Plantronics
  TOP PART = headset
  HW261N binaural noise-canceling microphone

HW251N monaural noise-canceling microphone

BOTTOM PART = USB adapter

DA55 USB-to-Headset Adapter

- GN Netcom or JABRA

  TOP PART = headset

  GN2125 binaural noise-canceling microphone

  GN2120 monaural noise-canceling microphone

  BOTTOM PART = USB adapter = Jabra Link 220

Important: The headset components listed above are suitable for a USB softphone connection. For a desk phone, substitute the headset BOTTOM PART with a desk phone adapter. Refer to the headset manufacturer's web site for the BOTTOM PART adapter that is designed for your brand and model of desk phone.

Tips for Choosing Headsets

- Many alternate TOP PART headset styles are available from Plantronics and Jabra (GN Netcom), and can be respectively substituted for the TOP PART models listed above.
- For environments with high ambient noise, select models with noise-canceling microphones and binaural ear speakers.
- Select TOP and BOTTOM parts from the same manufacturer. TOP and BOTTOM parts from different manufacturers do not interoperate.
- Avoid using units with built-in line volume controls. Adjusting the volume between the headset and PC/softphone can be confusing in these units.
- An agent's preferences for in-ear vs. over-ear headset designs should be respected.
- Select hardwired or wireless models based on need. If you choose a wireless model, be sure that local radio frequency congestion is not excessive (check the manufacturer's recommendations).
- Select a headset interface based on need for use with a softphone or desk phone, or both.

For more information, visit support.8x8.com.