

Genesys Multicloud CX™ Contact Center Availability Guide for Azure

for Customers' IT, Systems, and Network Administrators

Updated October 20, 2021



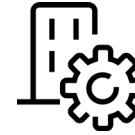
The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Cloud Services, Inc. Copyright © 2021 Genesys Cloud Services, Inc. All rights reserved.



Connectivity is the key to availability



User
workstation



Proxy and
firewalls



Internet or
ExpressRoute



Genesys
Multicloud CX cloud

This guide is for IT administrators responsible for enabling communications with the Genesys Multicloud CX™ contact center (formerly known as Genesys Engage cloud) on Azure.

Good and aligned end-to-end network connectivity ensures the availability of your Genesys Multicloud CX contact center operations.

The topics in this guide help you, the customer, to understand communications with the cloud contact center, to configure your on-site systems, to manage cloud contact center settings, and to allow your on-site and off-site users to access the cloud services seamlessly.

The user experience and successful engagement into your Genesys Multicloud CX contact center operations depend on:

- The settings and characteristics of user workstations and/or virtual desktops
- The status and capacity of:
 - The on-site network
 - The transport network between your network and the cloud – Internet or private network (for example, ExpressRoute)Contact your Technical Account Manager or Customer Success Manager to find out how to perform capacity evaluation.
- Configuration of intermediate systems:
 - On-site VPN Servers
 - On-site or cloud-based proxy systems and firewalls
- Settings and characteristics of the Genesys Multicloud CX contact center

Main topics

- ☆ User communications with Genesys Multicloud CX cloud
- ☆ User access to Genesys Multicloud CX services over the Internet
- ☆ User access to Genesys Multicloud CX services over a private network
- ☆ Business Continuity for user access to Genesys Multicloud CX services

User communications with Genesys Multicloud CX cloud

- Supported transport networks
- Agent phones and calls in Genesys Multicloud CX cloud
- Enabling off-site work
- Services and applications
- User workstations and VDI
- Voice and data communications
- Proxy support
- Proxy configuration
- Access via corporate VPN



Transport networks

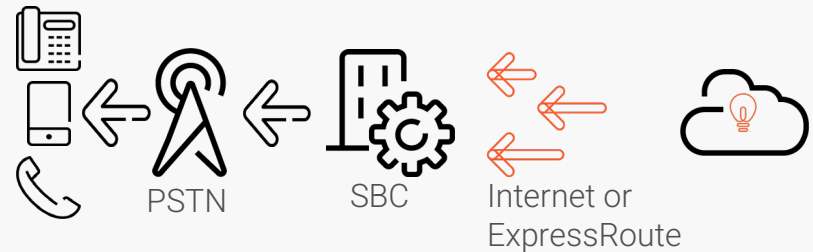
Transport networks provide transparent transmission of data and voice traffic between connected devices.

- You can enable your agents to communicate with Genesys Multicloud CX services over:
 - Internet (see [here](#)), Internet using Azure Peering Service (see [here](#)), Azure ExpressRoute with Microsoft Peering (see [here](#))
 - Azure ExpressRoute with Private Peering (see [here](#) and below)
- Genesys Multicloud CX services and applications (see full list [here](#)) support access over both the Internet and ExpressRoute. (See [Transport network limitations](#) for SIP phones that must communicate with the customer's session border controller [SBC] over a private network of the customer.)

Note: Only the customer's SBC and the Genesys Multicloud CX cloud SBC can communicate over Azure ExpressRoute with Private Peering.

- Agents can use PSTN phones for voice communications.

Via carrier's SBC or customer's SBC and PSTN, Genesys Multicloud CX services can invite into conversation any agent's phone that has a PSTN number (analog, digital, mobile, VoIP, home, or business phone).



Transport network limitations

Genesys Multicloud CX web-based services and applications support communications only over the Internet (see [here](#)), Internet using Azure Peering Service (see [here](#)), and Azure ExpressRoute with Microsoft Peering (see [here](#)).

The following Genesys Multicloud CX application supports communications only over the customer's private network:

- Genesys Softphone – SIP mode



Genesys Softphone in SIP mode must communicate with the customer's SBC over the customer's private network (see [here](#)).

The SBC communicates with the Genesys Multicloud CX cloud SBC over the Internet (see [here](#)), Internet using Azure Peering Service (see [here](#)), Azure ExpressRoute with Microsoft Peering (see [here](#)) or Azure ExpressRoute with Private Peering (see [here](#)).

Notes:

- Genesys Multicloud CX services operate using Internet Protocol version 4 (IPv4). IPv6 is not supported.
- Genesys Multicloud CX services use the already established connection or active session to provide data to the user or to deliver VoIP calls to the agent; TCP connections and UDP sessions are always originated by the user's workstation.



Agent phones (1)

The Genesys Multicloud CX contact center supports the following Agent phone types:

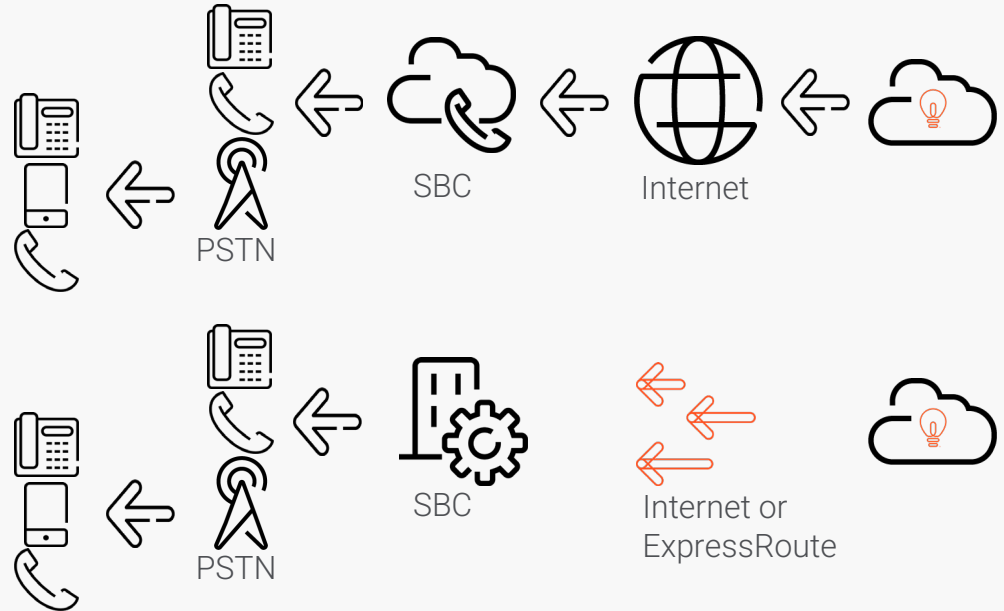
- PSTN phone (bottom diagram [here](#))

Genesys Multicloud CX voice service engages the phone via the carrier's SBC or the customer's SBC. Communications occur via [PSTN](#).

- Phone behind the corporate telephony systems (diagrams on this page)

Genesys Multicloud CX voice service engages the phone via the customer's SBC. Communications between the customer's SBC and the Genesys Multicloud CX cloud SBC occur via a SIP Trunk over the Internet or over Azure ExpressRoute. The following types of phone are supported:

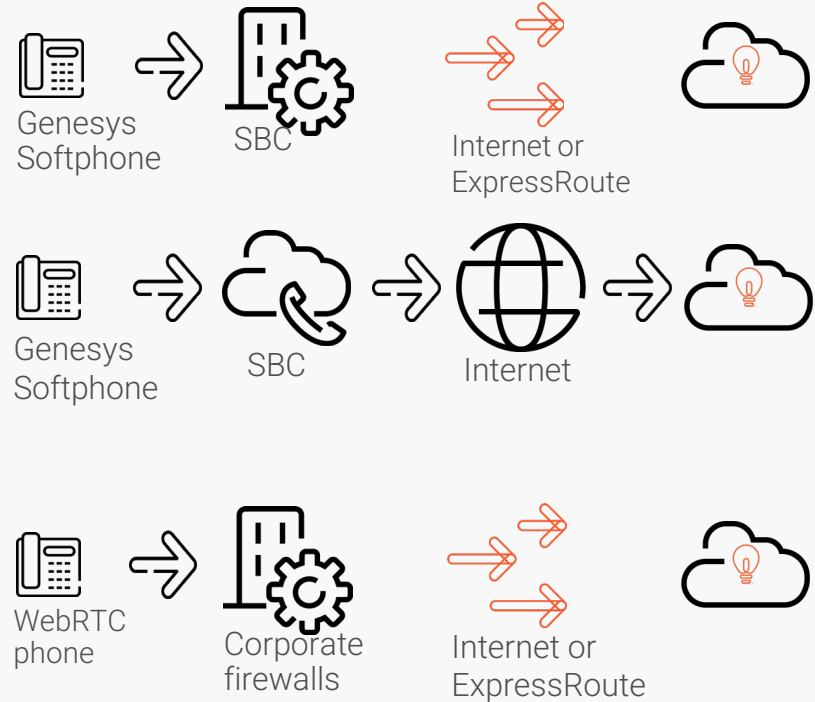
- Analog or digital phone
- VoIP phone
- PSTN phone



Agent phones (2)

- Genesys Softphone as the SIP phone SIP-registering with Genesys Multicloud CX voice service (diagrams on the right)
The phone communicates with the customer's SBC over a private network.
The customer's SBC communicates with the Genesys Multicloud CX voice service SBC over the Internet or over Azure ExpressRoute. Genesys Multicloud CX cloud engages the agent's phone via the customer's SBC.
- WebRTC Phone registering with Genesys Multicloud CX voice service (bottom diagram on this page)
Communications occur directly over the Internet or Azure ExpressRoute.

Note: Communications between Genesys Multicloud CX cloud and the corporate telephony systems, the SIP phones, and the WebRTC phones are Voice over IP communications.



Bandwidth requirements for agent-originated traffic

The following table shows bandwidth requirements for communications with typical voice and data services.

See [Bandwidth Requirements](#) for general information about bandwidth requirements for Genesys Multicloud CX contact center operations.

Traffic	Bandwidth	Transport via	When
Voice (SIP/RTP)	100 kbps G.711	Internet or ExpressRoute	Per call
WebRTC (Opus)	Variable 10 kbps to 160kbps	Internet or ExpressRoute (HTTPS for signaling + SRTP for media)	Per call
Desktop/CTI	16 kbps	Internet or ExpressRoute (HTTPS)	Per call
Screen Recording	350 kbps two screens	Internet or ExpressRoute (HTTPS)	Per recorded call/screen. Can be scheduled

End-customer PSTN calls and agent calls (1)

"The public switched telephone network (PSTN) is the aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication."

- Wikipedia

- The usual Genesys Multicloud CX contact center call flow starts when an end customer places a phone call.
- The call arrives at the national or global PSTN through the end customer's local carrier, then goes through an unpredictable chain of PSTN carriers.
- The call eventually arrives at a carrier that delivers the call to the Genesys Multicloud CX cloud SBC.

Genesys Multicloud CX cloud can receive the PSTN call placed by your end customer via one of the following paths:

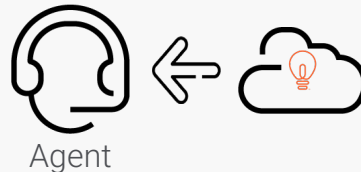
- You can connect your own PSTN carrier to the Genesys Multicloud CX cloud SBC over the Internet.
- You can keep your existing PSTN carriers, which deliver calls to your corporate telephony systems, and enable delivery of those calls to Genesys Multicloud CX cloud over the respective network, as illustrated in the diagram below.




End-customer PSTN calls and agent calls (2)

- Genesys Multicloud CX contact center starts processing the call from the end customer when the call arrives.
 - The end customer proceeds with the IVR self-service, navigates the IVR menu, and starts enjoying the music in queue.
 - The relevant end-customer data is ready to be presented to an agent in the Agent Desktop application.
 - The call routing service applies the relevant logic and selects the agent with the most relevant skills.
 - Genesys Multicloud CX voice service dials the agent's phone number to invite the agent into the voice conversation.
- The agent's phone is preprovisioned in the Genesys Multicloud CX contact center as an Extension DN object.
 - Each agent phone has a unique number within your contact center.
 - The Extension DN is appropriately configured so as to represent an agent phone of the desired type. (For additional information about SIP Phone provisioning, see [SIP Phone Types](#).)

The set of configuration options enables Genesys Multicloud CX contact center to use the appropriate transport network to engage the phone and to handle the call in the manner supported by the particular agent phone type (see [Agent phones](#)).
- There is no dependency between the network path taken by the end-customer call and the network path taken by the agent call.



Enabling your users to work off-site (1)

- Allow your off-site users and your on-site users to access Genesys Multicloud CX services over the same transport networks and via the same on-site systems. For information about the supported transport networks, see [here](#).
-  **Note:** If your company policies require, you can maintain IP-based control over access to Genesys Multicloud CX services, and permit access only from your known IP addresses. (See more about IP-based control [here](#).) There is no IP-based control over the TURN interface, which relies on other firewall techniques.
- Important:** During an emergency, the PSTN carriers might experience congestion in their infrastructure and decline PSTN calls, including end-customer inbound calls; outbound calls to end customers, external professional resources, partners, and vendors; and calls to the agents' PSTN phones. This issue is a concern if you want to support off-site phones over PSTN or you have an increase in end-customer calls.
- Use virtual desktop infrastructure (VDI) technologies (including on-site Windows Remote Desktop Services) for the web-based Genesys Multicloud CX applications. See VDI support details [here](#).
- Note:** During an emergency, it is considered acceptable that a user needs to launch some applications directly on the user workstation and work with other applications using a browser running on another system.
- Enable use of a corporate proxy for the off-site users. Use a Proxy Auto Config file (PAC file) to direct the browser launched on an off-site user's workstation to the corporate proxy for access to Genesys Multicloud CX services. See details [here](#).

Enabling your users to work off-site (2)

- Upgrade the bandwidth of your Internet connections to account for the traffic generated by your off-site users. See details about requirements for typical agent applications [here](#). For general information about bandwidth requirements, see [Bandwidth Requirements](#).
- Improve the capacity of the corporate VPN service.
- Use VPN with split tunneling enabled, together with PAC files and a corporate proxy, if the capacity of your corporate system is insufficient when you use VPN with split tunneling disabled. For more information, see [here](#) and [here](#).
- Genesys deploys each new contact center with services accessible from anywhere on the Internet. (See more about Genesys Multicloud CX access policy [here](#).)
 - If you maintain access restrictions at the Authentication step for access to Genesys Multicloud CX services that support SSO, consider that in an emergency situation you might need to make the services accessible from anywhere on the Internet.
 - **Note:** If your off-site users have been accessing services directly during an emergency, you may re-enable IP-based control when normal operations resume.
- See also [Business Continuity for user access to Genesys Multicloud CX services](#).

Applications for users: Web-based vs. standalone

Your users operate in your Genesys Multicloud CX contact center using a browser and web-based (browser-based) applications:

- Agent Desktop — Workspace Web Edition (see <https://all.docs.genesys.com/PEC-Agent>)
- WebRTC phone embedded into Workspace (not the Genesys Softphone) (see <https://all.docs.genesys.com/PEC-Agent>)
- Agent Desktop — Gplus Adapter Salesforce (see <https://all.docs.genesys.com/PEC-GPA/Current/Agent/GPASFLGettingStarted> and <https://all.docs.genesys.com/PEC-GPA/Current/Administrator>)
- Agent Setup (see <https://all.docs.genesys.com/PEC-AS>)
- Callback — Administrator UI (see <https://all.docs.genesys.com/PEC-CAB/Current/Administrator/GES>)
- CX Contact — Administrator UI (see <https://all.docs.genesys.com/PEC-OU/Current/CXContact/GetStarted>)
- Designer (see <https://all.docs.genesys.com/DES/Current/Designer/GetStarted>)
- GCXI Reporting (Genesys CX Insights — see <https://all.docs.genesys.com/PEC-REP/Current/Administrator/HRCXIUsrMgmt>)
- Pulse Reporting (Real-Time Reporting — see <https://all.docs.genesys.com/PEC-REP/Current/RT/RealTimeReporting>)
- Recording, Quality Management and Speech Analytics — Administrator UI (see <https://all.docs.genesys.com/PEC-REC/HIW>)
- Workforce Management (see <https://all.docs.genesys.com/PEC-WFM/Current/Agent>, <https://all.docs.genesys.com/PEC-WFM/HIW>, and <https://all.docs.genesys.com/PEC-WFM/ProductAlerts>)
- Genesys Predictive Routing — Administrator UI (see https://all.docs.genesys.com/PEC-ROU/HIW#Predictive_Routing)

Only a few applications are installed as standalone software on user workstations:

- Screen Recording Service (<https://all.docs.genesys.com/PEC-REC/Current/Administrator/ScreenRecordingConfig>)
- Genesys Softphone — SIP mode (<https://all.docs.genesys.com/PEC-GS/Current/Administrator/SPOverview>)

Applications for users: User workstation system requirements

User workstation capacity and software versions ensure successful operations of your Genesys Multicloud CX contact center.

- Typically, users use a personal workstation to access Genesys Multicloud CX services. Refer to the application documentation (see [links here](#)) and [System Requirements](#) for more information.
- Alternatively, users rely on virtual desktop infrastructure (VDI). Supported as follows:
 - Genesys Multicloud CX Agent Desktop — Workspace 9 supports Citrix XenApp, XenDesktop 7, and VMWare Horizon 7. Details [here](#).
- **Important:** The customer assumes responsibility for WebRTC phones deployed on VDI.
- Genesys Softphone – see <https://all.docs.genesys.com/PEC-GS/Current/Administrator/SPOverview>.
- Screen Recording Service – see <https://all.docs.genesys.com/PEC-REC/Current/Administrator/ScreenRecordingConfig>.
- All other web-based applications support any VDI.
- Users can use their personal workstations to launch one set of the Genesys Multicloud CX applications and VDI for another set of the applications.

Exception: WebRTC phone cannot be decoupled from the Workspace (in other words, from the Agent Desktop application).



VDI support for typical agent applications

Refer to the application documentation (see [links here](#)) for full information.

Agent Application on User Workstation	Citrix XenApp 7 or Citrix XenDesktop 7 on		VMware Horizon 7 on	
	Windows Server 2012 R2 or Windows Server 2008 R2	Linux eLux OS	Server 2012 R2	Server 2008 R2
Workspace 9, Genesys Softphone – SIP mode with enabled Connector and VDI adapter, Screen Recording Service (SRS)	Supported	Not supported	Not supported	Not supported
Workspace 9, Genesys Softphone – SIP mode with enabled Connector and VDI adapter	Supported	Supported	Not supported	Not supported
Workspace 9, SRS	Supported	Not supported	Supported	Not supported
Workspace 9	Supported	Supported	Supported	Supported

Note: Microsoft support for Windows Server 2008 R2 ended in 2020.

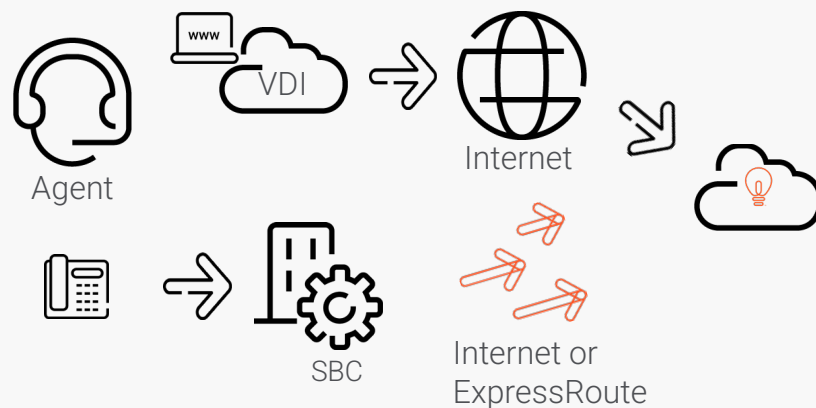
Applications for users: Data communications and VoIP communications (1)

There is no dependency between the transport network used by the data traffic of the user's web-based applications and the transport network used by the VoIP traffic of the agent's voice calls.

Example 1

- An on-site agent connects to VDI over the Internet and runs a browser with the Agent Desktop in the VDI, which accesses Genesys Multicloud CX services over the Internet.
- The agent uses Genesys Softphone in SIP mode installed on the agent's workstation.

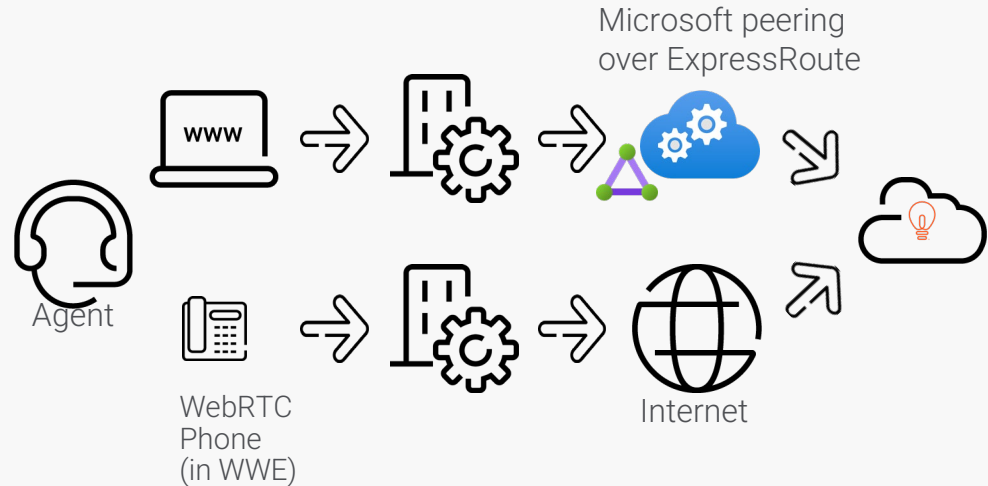
Workspace Connector for the phone is disabled. The phone obtains configuration from a local configuration file.



Applications for Users: Data communications and VoIP communications (2)

Example 2

- An agent runs a browser with Workspace and the WebRTC phone embedded into WWE on the agent's workstation.
 - The browser connects to the Agent Desktop service via the customer's corporate proxy and over the Azure ExpressRoute.
 - The WebRTC phone communicates with Genesys Multicloud CX services directly over the Internet.

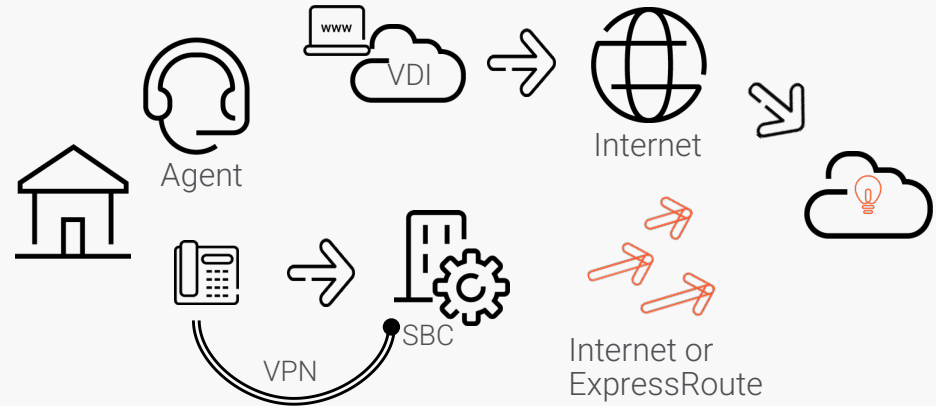


Applications for users: Data communications and VoIP communications (3)

Examples for off-site agents (1)

- An off-site agent connects to VDI over the Internet and runs a browser with the Agent Desktop in the VDI.
 - VDI ensures that the agent is unable to collect sensitive information and save such information on the agent's home workstation.
 - VDI accesses Genesys Multicloud CX services over the Internet.
 - The off-site agent uses Genesys Softphone in SIP mode installed on the agent's workstation at home.

Workspace Connector for the phone is disabled. The phone obtains configuration from a local configuration file.
 - The SIP phone communicates with the on-premises SBC via the corporate VPN with split tunneling enabled and over the private network. (See more information about split tunneling [here](#).)



Applications for users: Data communications and VoIP communications (4)

Examples for off-site agents (2)

- An off-site agent connects to VDI over the Internet and runs a browser with the Workforce Management and Recording, QM and Speech Analytics applications in the VDI. The VDI accesses Genesys Multicloud CX services over the Internet.
 - The off-site agent runs a browser with Workspace on the agent's workstation at home and accesses Genesys Multicloud CX services over the Internet.
 - The off-site agent uses a software phone integrated into the corporate telephony infrastructure or PSTN phone (see [Phone behind the corporate telephony systems](#)).
 - Genesys Multicloud CX voice service engages the phone into conversation via a SIP Trunk with the customer's SBC. The customer's SBC delivers the call to the agent's phone.
- An off-site agent runs a browser with Workspace and the WebRTC phone embedded into WWE on the agent's home workstation.
 - The WebRTC phone communicates with Genesys Multicloud CX services directly over the Internet.
 - The corporate VPN with split tunneling enabled provides access to the Agent Desktop service over the respective transport network.

Applications for users: URLs and name resolution

The Genesys Multicloud CX services are addressed by means of URLs.

- The host portion of the URLs (the Fully Qualified Domain Name [FQDN]) is constructed of a name within the `prodNNN.genesysengage.com` domain, where `NNN` is the numeric ID of your Genesys Multicloud CX contact center.

For example:

- `best-customer.prod009.genesysengage.com`
 - `best-service.api01-eastus2.prod009.genesysengage.com`
 - `best-service.api01-westus2.prod009.genesysengage.com`
- Name resolution for the FQDNs is provided by the global internet DNS service.
- To find out the host portion of the URLs, contact [Genesys Customer Care](#).



`https://*.prodNNN.genesysengage.com`

Applications for users: Protocols and ports

- Genesys Multicloud CX services are accessible using HTTPS (TCP port 443).



Exception: WebRTC phones establish the voice media connection to the Genesys Multicloud CX TURN interface on TCP port 443 but do not use HTTPS. Instead, WebRTC phones use SRTP for the media connection.

- Genesys Multicloud CX services support TLS 1.2 and rely on SSL certificates issued by Trusted 3rd Party Certificate Authorities.
 - While validating the SSL certificates during TLS negotiation, the browser may connect to the Certificate Revocation List (CRL) systems of the Trusted 3rd Party Certificate Authorities.



Exception: WebRTC phones do not use TLS for the media connection. SRTP uses other techniques for authenticating the identity of the systems and encrypting media connection data.

- Genesys Softphone in SIP mode uses SIP for signaling traffic and RTP for media traffic.
 - If encryption is enabled for communications of the Genesys Softphone in SIP mode, the user workstation may connect to the CRL systems of the Certificate Authorities that issued the SSL certificates for the SIP User Agents (SIP UAs).
 - The phone communicates with the customer's SBC over a private network.
 - The customer's SBC port numbers for signaling and media communications are defined by the customer.
 - The SIP phone port numbers for signaling and media communications are configurable.
 - The customer's SBC communicates with the Genesys Multicloud CX cloud SBC.
 - The Genesys Multicloud CX cloud SBC port numbers for signaling and media communications are defined during the onboarding process.

Applications for users: Web proxy support

Genesys Multicloud CX browser-based applications respect the proxy settings of the browser. (See [here](#) for a list of the applications.)

Applications in browser	Browser Proxy settings (including PAC file)
All applications running in browser	Supported

Genesys Multicloud CX applications that are deployed as standalone software support web proxy as follows:

Software installed on user workstation	Proxy settings in the configuration file
Screen Recording Service, 8.5.370.78 and higher	Supported

Note: Screen Recording Service (SRS) communicates with Genesys Multicloud CX services to control the screen recording activities at the user's workstation and upload the recordings. SRS versions prior to 8.5.370.78 do not support use of a web proxy.

Enabling access via proxy

If your users use on-site proxy systems or cloud-based proxy providers, access to Genesys Multicloud CX services depends on the availability and configuration of the proxy systems.



Proxy to allow navigation to
`https://*.prodNNN.genesysengage.com`

- If the proxy systems restrict web navigation, do one of the following:
 - Allow access to any URL constructed of the `prodNNN.genesysengage.com` domain, including any URL constructed of the regional API sub-domains, such as `api01-eastus2.prodNNN.genesysengage.com` or `api01-westus2.prodNNN.genesysengage.com`.
 - Allow access to the URLs of the services you use.

Note that there are applications that instruct the browser to send requests to additional Genesys Multicloud CX URLs. For example:

- Agent Desktop utilizes additional URLs for authentication and telemetry.
- Recording, QM and Speech Analytics utilizes additional URLs for the Recording Crypto Service and Recording Playback.

To find out the host portion of all URLs your users use, contact [Genesys Customer Care](#).

- For WebRTC Phones, which are embedded into Workspace, the proxy systems must be transparent for media traffic.



Note: Genesys recommends that you exclude the WebRTC media traffic URLs from the list processed by proxy.

The phone respects the browser proxy settings and establishes the media connection to the Genesys Multicloud CX TURN interface (TCP port 443), but uses SRTP for this TCP connection.

Access via dedicated proxy systems: PAC file for user's browser

You can use dedicated proxy systems for access to Genesys Multicloud CX services.

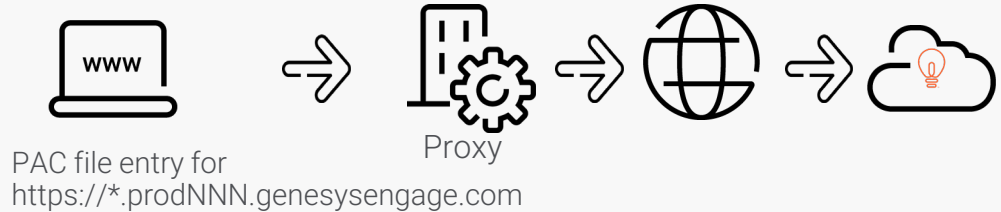
You can use a Proxy Auto Config file (PAC file) to direct users' browsers to your dedicated corporate proxy systems for access to Genesys Multicloud CX services.

Benefits of using a PAC file include, but are not limited to, the following:

- Group Policy management provides centralized control you can utilize to enable traffic engineering and optimization for web browsing in your corporate network.
- You can maintain dedicated system capacity and network bandwidth for communications with Genesys Multicloud CX services, thus ensuring the Quality of Service for WebRTC voice media traffic and improving both the agent and the end-customer experience.
- You establish control over the web access originated by your off-site users who utilize a corporate VPN with split tunneling enabled. The VPN enables access to corporate resources; the Genesys Multicloud CX services; and other restricted, third-party resources on the Internet.

For more information, see:

- <https://blogs.msdn.microsoft.com/askie/2015/07/17/how-can-i-configure-proxy-autoconfigurl-setting-using-group-policy-preference-gpp/>
- https://en.wikipedia.org/wiki/Proxy_auto-config



Access via dedicated proxy systems: PAC file configuration example

High-level configuration steps

To enable use of a dedicated proxy for access to Genesys Multicloud CX services:

1. Configure a Proxy Auto Config file (PAC file) on the user's workstation. Include a directive for the browser to send requests via the dedicated proxy systems.
2. Configure the browser to use the PAC file to locate a proxy.

Note: Exclude the FQDN of the Genesys Multicloud CX TURN interface from the list of destinations served by your proxy, thus enabling direct access from user workstations to the TURN interface for the WebRTC media traffic of the WebRTC phone.

Example of PAC file content

```
function FindProxyForURL(url, host) {  
    // URLs from the domains under prod009.genesysengage.com must use the proxy:  
    if (shExpMatch(host, "*.prod009.genesysengage.com"))  
    {  
        return "PROXY To-GenesysMulticloudCX.internal.example.com:8080";  
    }  
    else  
    {  
        return "DIRECT";  
    }  
}
```

In this example,

- The FQDN of the proxy is To-GenesysMulticloudCX.internal.example.com
- The proxy listens on port 8080.
- The proxy will be used to access URLs constructed of prod009.genesysengage.com.

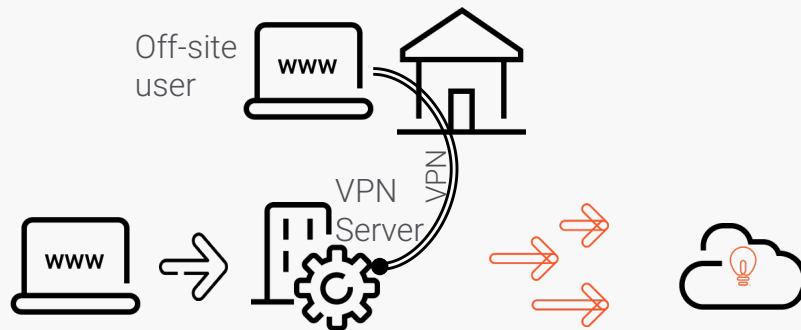
Access via VPN to the corporate network

If you allow off-site users to establish a VPN connection to your corporate network, the users can connect to the Genesys Multicloud CX services via the VPN and your corporate systems.

Note: VPN may affect voice quality by increasing jitter and latency. Contact your VPN Server Vendor for best practices related to VPN configuration.

If your setup allows off-site users to use the VPN to access both internal corporate resources and Internet resources, enabling access to Genesys Multicloud CX services from a VPN-connected workstation is similar to enabling access from an internal workstation:

- The same proxy systems and firewalls usually control the Internet traffic originated by internal users and by VPN-connected users.
- If additional intermediate systems control Internet access from the VPN-connected workstation, configure the additional systems to enable access to Genesys Multicloud CX services.

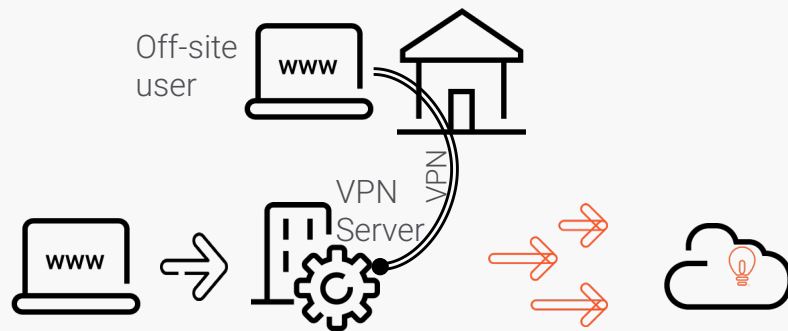


Access via VPN to the corporate network: Split tunneling

You can use VPN split tunneling to allow off-site users to connect to your corporate resources at the same time that the users browse the public Internet through their local Internet connections.

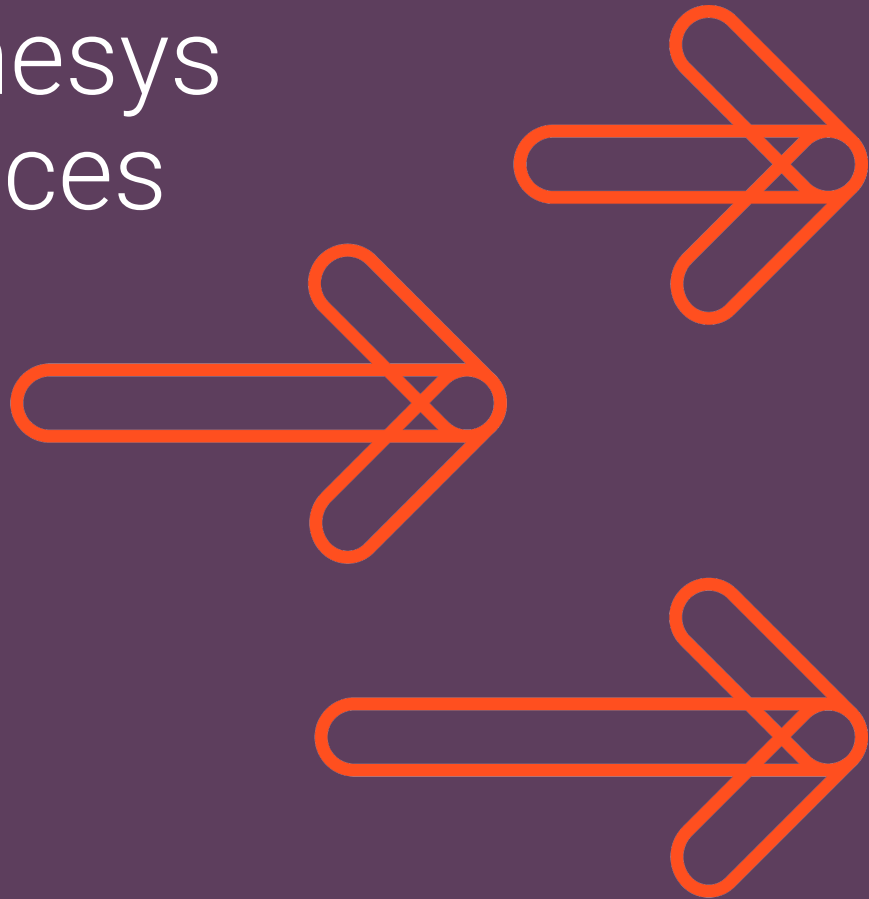
- Allow your off-site and your on-site users to access Genesys Multicloud CX services over the same transport network and via the same on-site systems. Deploy a PAC file on the off-site workstations and direct the browsers to communicate with the Genesys Multicloud CX services via your corporate proxy. (See [here](#) for an example of PAC file configuration.)
 - Your off-site users will connect to Genesys Multicloud CX services over the Internet, utilizing the known corporate public IP addresses as the source IP addresses.
 - Exclude the TURN interface from the VPN and enable a direct WebRTC voice stream with the Genesys Multicloud CX TURN interface over the Internet.

For more information, see [here](#).



User access to Genesys Multicloud CX services over the Internet

- Connectivity options
- Dynamic Genesys Multicloud CX IP addresses on the Internet
- Firewall permissions
- Split tunneling for off-site users
- IP-based access restrictions and open Internet access



Access over the Internet

The Internet is one of the transport networks you can use for your agents and administrators to communicate with Genesys Multicloud CX services.

- Agent's browser connects to the Desktop and other Genesys Multicloud CX services.
- Agent's WebRTC phone registers with Genesys Multicloud CX voice service, from which it then receives calls.
- Agent's Screen Recording Service uploads screen recordings to Genesys Multicloud CX cloud.
- Administrator's browser connects to the Genesys Multicloud CX services.

Genesys Multicloud CX services are reachable over the Internet by public IP addresses. You can enable your agents to communicate with Genesys Multicloud CX services over:

- Internet (see [here](#))
- Internet using Azure Peering Service (see [here](#))
- Azure ExpressRoute with Microsoft Peering (see [here](#))



Connectivity over the Internet

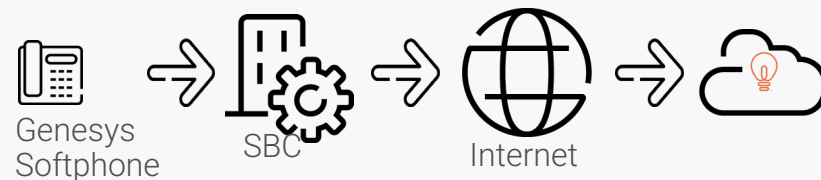
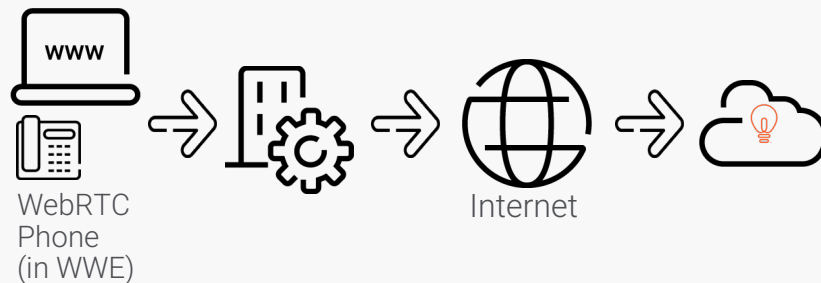
Your Internet connectivity with Genesys Multicloud CX cloud can rely on the regular (undefined, unpredictable in general) chain of the Internet Service Providers.

Examples of user access to Genesys Multicloud CX services over the Internet:

- Upper diagram on the right shows this type of connectivity for access to Genesys Multicloud CX services and WebRTC phone communications.
- Lower diagram on the right shows this type of connectivity for the Genesys Softphone – SIP mode communications.

The phone communicates with the customer's SBC over a private network.

The customer's SBC communicates with the Genesys Multicloud CX cloud SBC.



Connectivity over the Internet using Azure Peering Service

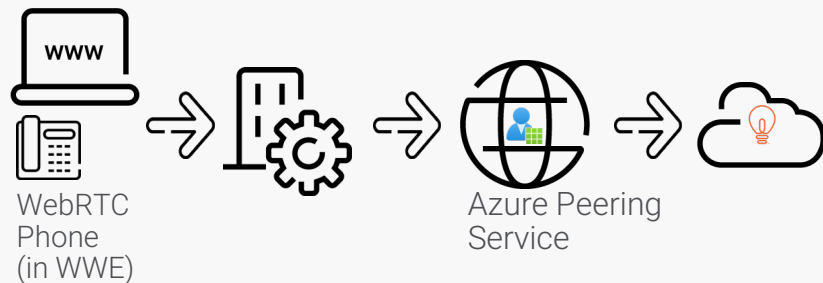
Your Internet connectivity with Genesys Multicloud CX cloud can use Azure Peering Service. (For general information, see [Azure Peering Service Overview](#).) Microsoft and service providers have partnered to deliver reliable and performance-centric public connectivity to the Microsoft cloud.

Note: Even though your selected service provider provides you with a dedicated network path to Microsoft cloud, you connect to the same public IP addresses of the Genesys Multicloud CX services as when you connect over the Internet. From the perspective of Genesys Multicloud CX cloud, you connect over the Internet.

Examples of user access to Genesys Multicloud CX services over the Internet using Azure Peering Service:

- Upper diagram on the right shows this type of connectivity for access to Genesys Multicloud CX services and WebRTC phone communications.
- Lower diagram on the right shows this type of connectivity for the Genesys Softphone – SIP mode communications.

The phone communicates with the customer's SBC over a private network. The customer's SBC communicates with the Genesys Multicloud CX cloud SBC.



Connectivity over Azure ExpressRoute with Microsoft Peering (1)

Your connectivity with Genesys Multicloud CX cloud can use Microsoft peering over ExpressRoute.

- Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection. (See [What is Azure ExpressRoute?](#))
 - ExpressRoute circuits can include two independent peerings: Microsoft peering and Private peering (see [here](#)).
- To utilize your dedicated Ethernet fiber-optic cables for connection to Genesys Multicloud CX services normally reachable over the Internet by public IP addresses, use Microsoft peering over ExpressRoute.
 - **Exception:** You cannot use this type of connectivity for access to Portal and static pages of Agent Desktop because Azure CDN delivers to your users the content of Genesys Multicloud CX Portal and the static pages of Agent Desktop. (For information about Azure CDN, see [What is a content delivery network on Azure?](#)) You must connect to Azure CDN over the Internet (see [here](#)) or Internet using Azure Peering Service (see [here](#)).
- **Note:** Even though the ExpressRoute is in use, you connect to the same public IP addresses of the services as when you connect over the Internet. From the perspective of Genesys Multicloud CX cloud, you connect over the Internet.
- **Note:** ExpressRoute with Microsoft Peering enables connectivity with Microsoft cloud. Over this ExpressRoute, your users might access third-party services that are also deployed on the Microsoft cloud.

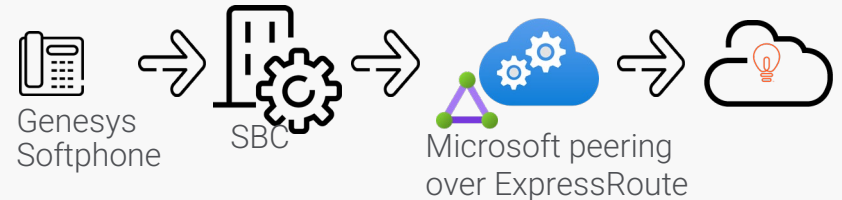
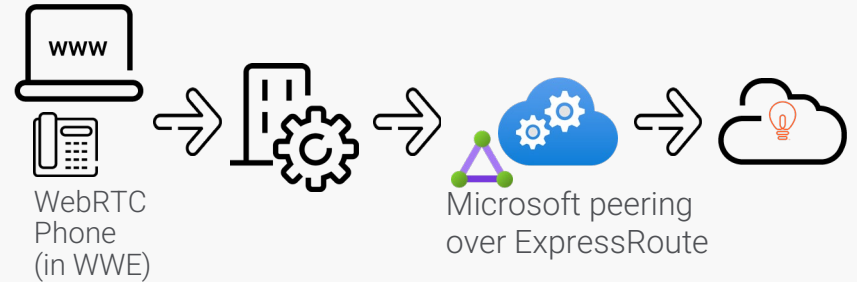
Connectivity over Azure ExpressRoute with Microsoft Peering (2)

Examples of user access to Genesys Multicloud CX services over Azure ExpressRoute with Microsoft Peering:

- Upper diagram on the right shows this type of connectivity for access to Genesys Multicloud CX services and WebRTC phone communications.
- Lower diagram on the right shows this type of connectivity for the Genesys Softphone – SIP mode communications.

The phone communicates with the customer's SBC over a private network.

The customer's SBC communicates with the Genesys Multicloud CX cloud SBC.



Connectivity between customer's SBC and Genesys SBC over the Internet

- SIP Phones SIP-registering with Genesys Multicloud CX voice service via customer's SBC use SIP for signaling traffic and RTP/RTCP for media traffic.
- IP addresses for the Genesys Multicloud CX cloud SBC are stable and routable on the Internet.



- **Important:** You must *not* expose to the Internet the Genesys Multicloud CX cloud SBC.
You must not use NAT, reverse proxy, SBC, or any other techniques to enable access over the Internet to the Genesys Multicloud CX cloud SBC via your systems exposed to the Internet.
- You can use IP address-based permissions on your firewall to control access to Genesys Multicloud CX cloud SBC.
 - The SIP expire timer in Genesys Multicloud CX voice service is set to 140 seconds. The firewall idle timeout for SIP signaling must make allowance for the timer. Ensure that the permissions injected dynamically because of SIP REGISTER requests from SIP phones are intact for at least 140 seconds, so that your firewall allows SIP INVITE requests originated by Genesys Multicloud CX cloud to reach the SIP phones before the SIP registration expires.
 - The voice media session is always originated by the SIP phone. Genesys Multicloud CX cloud initiates RTP traffic towards the SIP phone after receiving RTP traffic from the customer's SBC. The Genesys Multicloud CX cloud SBC sends RTP packets to the IP address and port that the customer's SBC used while initiating the voice media session.

Access over the Internet: Considerations

To enable user access to Genesys Multicloud CX services reachable over the Internet by a public IP address, you must consider:

- Protocols and communication ports (more information [here](#))
- Your proxy configuration (more information [here](#))
- Your firewall configuration (more information [here](#))
- Genesys Multicloud CX access policy and IP-based access restrictions (more information starts [here](#))
 - **Note:** If your company policies require, you can maintain IP-based control over access to Genesys Multicloud CX services, and permit access only from your known IP addresses. There is no IP-based control over the TURN interface, which relies on other firewall techniques.
- There are additional configuration considerations if you want to use VPN split tunneling as the technique that enables off-site work. The technique allows your off-site users to access Genesys Multicloud CX services via your corporate systems. As described [here](#) and [here](#), to use split tunneling you must:
 - Use a PAC file to direct users' browsers to the corporate proxy and enforce access to Genesys Multicloud CX services via the proxy.
 - Use the stable IP addresses of the Genesys Multicloud CX TURN interfaces to exclude WebRTC media traffic from the VPN tunnel.



User access over the Internet: Dynamic IP addresses

- Genesys Multicloud CX services are addressed by means of URLs, for example:
`https://best-customer.genesysengage.com`

Exception: Media traffic of WebRTC phones uses TCP port 443 and SRTP.

- There are no stable Internet-routable IP addresses for Agent Desktop and Portal services. Other Genesys Multicloud CX services tend to preserve stable IP addresses.

Exception: Genesys Multicloud CX TURN interfaces maintain stable IP addresses for WebRTC media traffic.

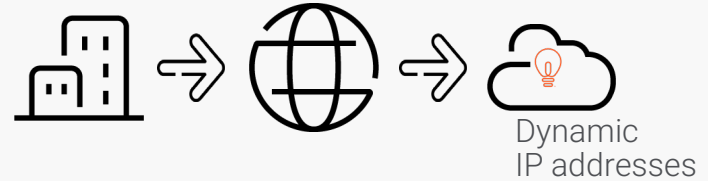
- Do not use IP address-based permissions on your firewall to control access to the Genesys Multicloud CX Portal and Agent Desktop over the Internet.

Configuring firewall permissions based on the current name resolution will prevent users from accessing Genesys Multicloud CX services. Outages will occur because the Genesys Multicloud CX IP addresses change periodically and unpredictably.

Exception: IP-based firewall permissions can be configured for the WebRTC media traffic of WebRTC phones.

- **Notes:**

- If you use a PAC file, exclude the FQDN of the Genesys Multicloud CX TURN interface from the list of destinations served by your proxy, thus enabling direct access from user workstations to the TURN interface for the WebRTC media traffic of the WebRTC phone.
- Exclude the TURN interface from the list of destination IP addresses handled by your VPN tunnel, and enable a direct WebRTC voice stream with the TURN interface over the Internet.



User access over the Internet via firewall (1)

- If access to Genesys Multicloud CX services relies on your proxy systems, configure the firewall that controls access to the Internet to allow the proxy systems to send requests to TCP port 443 at any destination on the Internet.
If agents use WebRTC phones embedded into Workspace, disable HTTPS deep packet inspection for media communications with the stable IP addresses of the Genesys Multicloud CX TURN interfaces (TCP port 443). This is required because the media traffic of the WebRTC phone embedded into Workspace utilizes SRTP.
Note: Genesys recommends that you exclude the FQDN of the Genesys Multicloud CX TURN interface from the list of destinations served by your proxy.
- If you do not use proxy systems, configure the on-site firewall to allow the browsers and the standalone software to send requests to TCP port 443 at any destination on the Internet.



User access over the Internet via firewall (2)

- If agents use a WebRTC phone, which is embedded into Workspace, and you exclude the FQDN of the Genesys Multicloud CX TURN interface from the list of destinations served by your proxy, configure the firewall to allow outbound access on TCP port 443 for SRTP to the Genesys Multicloud CX TURN interfaces. This is required for WebRTC phones to establish a voice media connection to the Genesys Multicloud CX TURN interface.

Disable HTTPS deep packet inspection for media communications with the stable IP addresses of the Genesys Multicloud CX TURN interfaces (TCP port 443). This is required because the media traffic of the WebRTC phone embedded into Workspace utilizes SRTP.

Ensure you configure all firewalls under your control on the media path, including the software firewall on the user's workstation if such is in use.



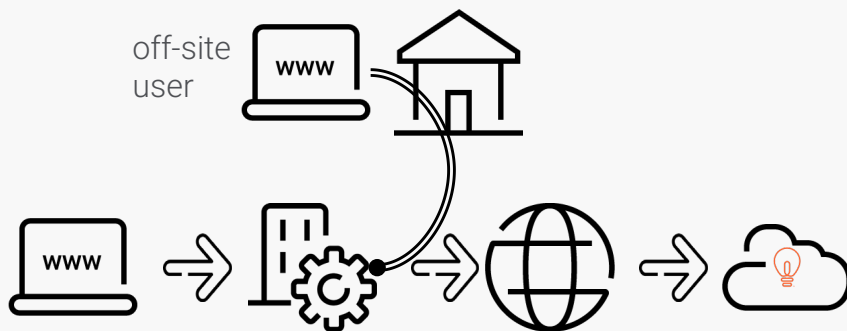
Firewall to allow
access to TURN IP
address, TCP port 443

Allowing user access over the Internet: “split-include” VPN split tunneling

High-level configuration steps

1. In the list of destination IP addresses handled by your VPN tunnel, include the internal IP addresses of your corporate proxy systems.
2. In the list of destination IP addresses handled by your VPN tunnel, verify that you do not include the stable IP addresses of the Genesys Multicloud CX TURN interfaces (so, you enable a direct WebRTC voice stream with the Genesys Multicloud CX TURN interface over the Internet).
3. Configure a PAC file on the off-site user's workstation and include a directive for the browser to send requests to Genesys Multicloud CX services via your corporate proxy systems.
4. Configure the off-site user's browser to use the PAC file to locate a proxy.

See additional details [here](#) and [here](#).



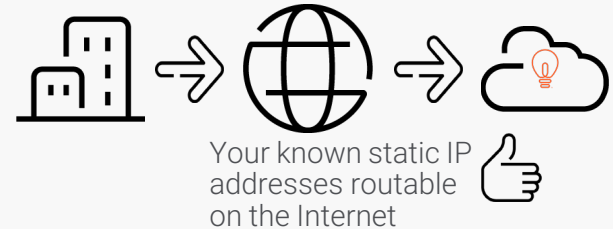
Access over the Internet: Access policy at Genesys Multicloud CX cloud

Genesys deploys each new contact center with services accessible from anywhere on the Internet.

Note: The Genesys Multicloud CX TURN interfaces always accept legitimate connections for WebRTC media communications from the entire Internet. You cannot restrict access to the TURN interfaces on the Genesys Multicloud CX cloud side.

If your company policies require, you can maintain IP-based control over access to Genesys Multicloud CX services and permit access only from your known IP addresses.

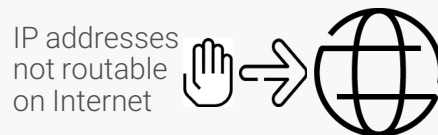
- The IP list includes only IP addresses that are routable on the Internet.
Genesys does not include in the list any IP addresses that are not routable on the Internet (see [here](#)).
- Provide the static IP addresses that are used when your users browse the Internet (specifically, when your users connect to Genesys Multicloud CX services over the Internet).
Genesys expects that the IP addresses are allocated to your company by an IP Registry or your Internet Service Provider, or that they belong to the Vendor of your cloud-based Proxy or VDI service.
- Do not request enabling access for IP addresses that Internet Service Providers assign to your off-site workers' network equipment. Such addresses are dynamic and temporary.



Access over the Internet: Not-routable IP addresses

IP addresses that are **not routable on the Internet** will not be included in your list of known IP addresses. The reason is that attempts to connect to Genesys Multicloud CX cloud from these IP addresses will never reach the Genesys Multicloud CX services, because Internet Service Providers will reject them.

- 0.0.0.0/8 (0.0.0.0 - 0.255.255.255): RFC 5735, RFC 6890
- 10.0.0.0/8 (10.0.0.0 - 10.255.255.255): RFC 5735, RFC 1918
- 100.64.0.0/10 (100.64.0.0 - 100.127.255.255): RFC 6598
- 127.0.0.0/8 (127.0.0.0 - 127.255.255.255): RFC 5735, RFC 1122
- 169.254.0.0/16 (169.254.0.0 - 169.254.255.255): RFC 5735, RFC 3927
- 172.16.0.0/12 (172.16.0.0 - 172.31.255.255): RFC 5735, RFC 1918
- 192.0.0.0/24 (192.0.0.0 - 192.0.0.255): RFC 5735, RFC 5736
- 192.0.2.0/24 (192.0.2.0 - 192.0.2.255): RFC 5735, RFC 5737
- 192.88.99.0/24 (192.88.99.0 - 192.88.99.255): RFC 5735, RFC 3068
- 192.168.0.0/16 (192.168.0.0 - 192.168.255.255): RFC 5735, RFC 1918
- 198.18.0.0/15 (198.18.0.0 - 198.19.255.255): RFC 5735, RFC 2544
- 198.51.100.0/24 (198.51.100.0 - 198.51.100.255): RFC 5735, RFC 5737
- 203.0.113.0/24 (203.0.113.0 - 203.0.113.255): RFC 5735, RFC 5737
- 224.0.0.0/4 (224.0.0.0 - 239.255.255.255): RFC 5735, RFC 3171
- 240.0.0.0/4 (240.0.0.0 - 255.255.255.255): RFC 5735, RFC 1112



Access over the Internet: Open Internet access and IP-based control

Genesys Multicloud CX services are accessible from anywhere on the Internet.

Note: You can apply access restrictions at the Authentication step for access to Genesys Multicloud CX services with enabled Single Sign On (SSO) authentication. See <https://all.docs.genesys.com/PEC-Admin/Current/Admin/SSO> for a list of the services that support SSO.

Genesys Authentication Service IP-based access control allows you to govern the Genesys Multicloud CX authentication process for your users. You can permit login requests from your known Internet-routable IP addresses and reject login requests from unknown IP addresses.

IP-based control is essential for customers that must meet regulatory requirements. For example, if sensitive information must not be exposed to off-site users or collected on home workstations.

Relying on IP-based control, the Genesys Multicloud CX solution meets access restriction requirements for some customers, while open Internet access to the services is enabled for other customers. These other customers might require open Internet access because their off-site users require direct access to Genesys Multicloud CX services.

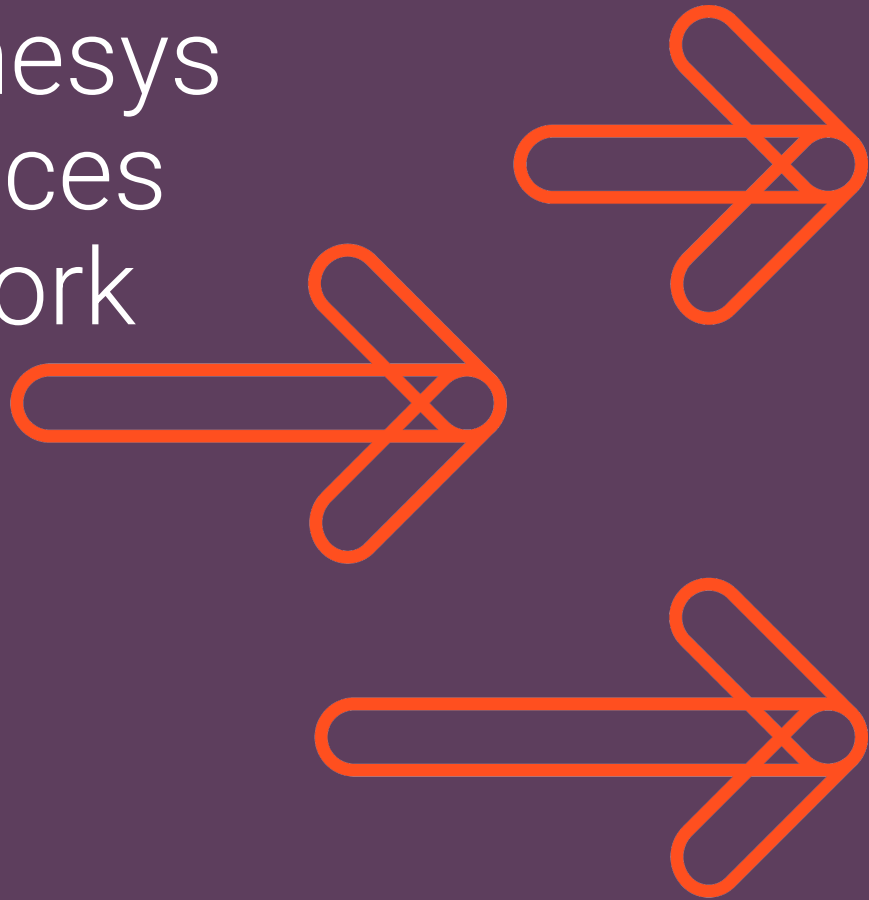
Use the following MACD process to manage access restrictions:

- To apply restricted access:
 1. Maintain a list of your known IP addresses.
 2. Open a case with [Genesys Customer Care](#) to request enabling Genesys Authentication Service IP-based access control. Provide your known IP addresses.
- To re-enable open Internet access to the Agent Desktop service, open a case with [Genesys Customer Care](#).



User access to Genesys Multicloud CX services over a private network

- Connectivity over Azure ExpressRoute with Private Peering



Agent phones: Genesys Softphone SIP phones and connectivity over Azure ExpressRoute with Private Peering

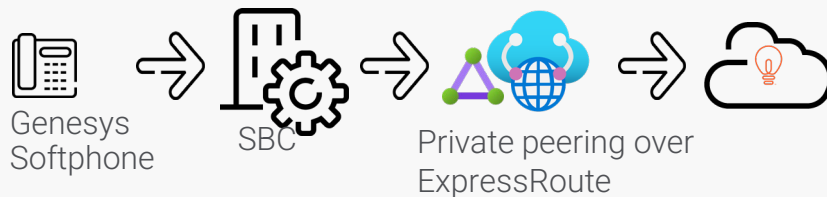
Your private network connectivity with Genesys Multicloud CX cloud can use Private peering over ExpressRoute.

- Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection. (See [What is Azure ExpressRoute?](#))
 - ExpressRoute circuits can include two independent peerings: Microsoft peering (see [here](#)) and Private peering.
- To allow your on-premises SBC to communicate with the Genesys Multicloud CX cloud SBC over a dedicated private connection, use Private peering over ExpressRoute.
- **Note:** ExpressRoute with Private Peering enables connectivity only with Genesys Multicloud CX cloud SBC.
- **Note:** Even though the ExpressRoute is in use, you connect to the same SBC public IP addresses as when you connect over the Internet.

The diagram below shows this type of connectivity for the Genesys Softphone SIP and media communications.

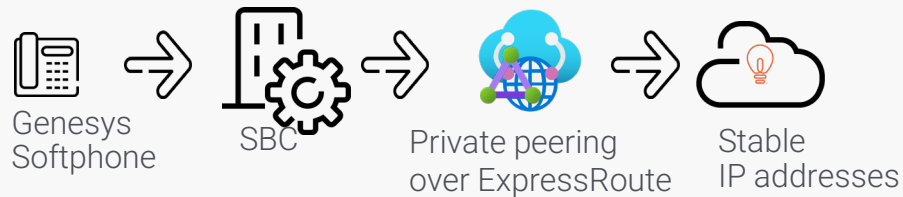
The phone communicates with customer's SBC over a private network.

The customer's SBC communicates with the Genesys Multicloud CX cloud SBC.



Connectivity between customer's SBC and Genesys SBC over Azure ExpressRoute with Private Peering

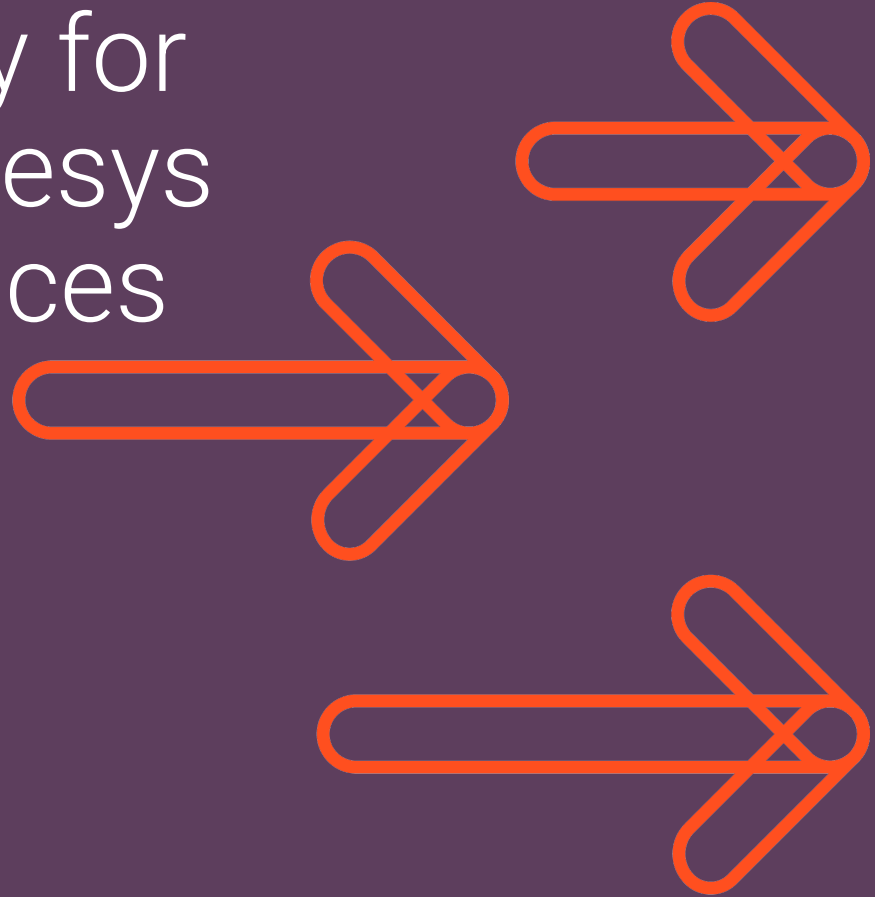
- SIP Phones SIP-registering with Genesys Multicloud CX voice service via the customer's SBC use SIP for signaling traffic and RTP/RTCP for media traffic.
- IP addresses for the Genesys Multicloud CX cloud SBC are stable and routable on the private network.



- **Important:** You must *not* expose to the Internet the Genesys Multicloud CX cloud SBC.
You must not use NAT, reverse proxy, SBC, or any other techniques to enable access over the Internet to the Genesys Multicloud CX cloud SBC via your systems exposed to the Internet.
- You can use IP address-based permissions on your firewall to control access to the Genesys Multicloud CX cloud SBC.
 - The SIP expire timer on Genesys Multicloud CX voice service is set to 140 seconds. The firewall idle timeout for SIP signaling must make allowance for the timer. Ensure that the permissions injected dynamically because of SIP REGISTER requests from SIP Phones are intact for at least 140 seconds, so that your firewall allows SIP INVITE requests originated by Genesys Multicloud CX voice services to reach the SIP phones before the SIP registration expires.
 - The voice media session is always originated by the SIP phone. Genesys Multicloud CX cloud initiates RTP traffic towards the SIP phone after receiving RTP traffic from the customer's SBC. Genesys Multicloud CX cloud SBC sends RTP packets to the IP address and port that the customer's SBC used while initiating the voice media session.

Business Continuity for user access to Genesys Multicloud CX services

- About Business Continuity
- Agent phones
- Genesys Multicloud CX services and applications



Genesys Multicloud CX services and Business Continuity of your organization (1)

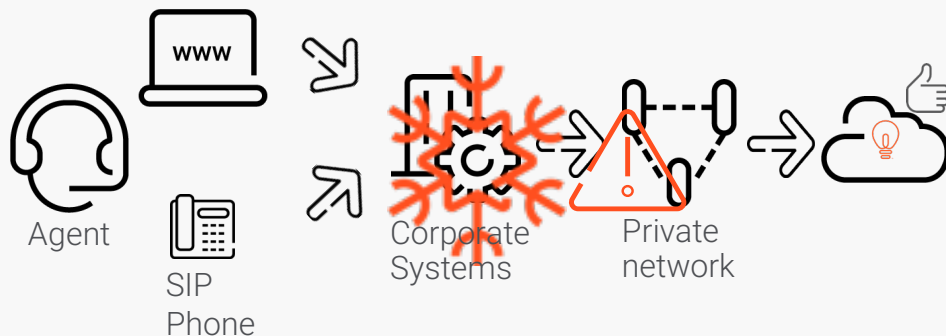
A disaster can occur at any time.

The Genesys Multicloud CX architecture is intrinsically resilient. Relying on high availability features, it leverages the distributed nature of the environment to facilitate prompt restoration of contact center service if a catastrophic event affects Genesys Multicloud CX cloud. Consult the materials about your contact center architecture for specific details.

A catastrophic event might take down some of the corporate systems and networks used during normal operations for access to Genesys Multicloud CX cloud, or the event might simply restrict their usability.

A traditional Disaster Recovery Plan, which focuses on restoring the company data center, might not be sufficient.

A more comprehensive and rigorous Business Continuity Plan is needed to achieve a state of business continuity where the critical services of your organization are continuously available.



Example: Catastrophic failure of corporate systems and network

(The example might not apply to your setup, but it illustrates the risk of a catastrophic event.)

Genesys Multicloud CX services and Business Continuity of your organization (2)

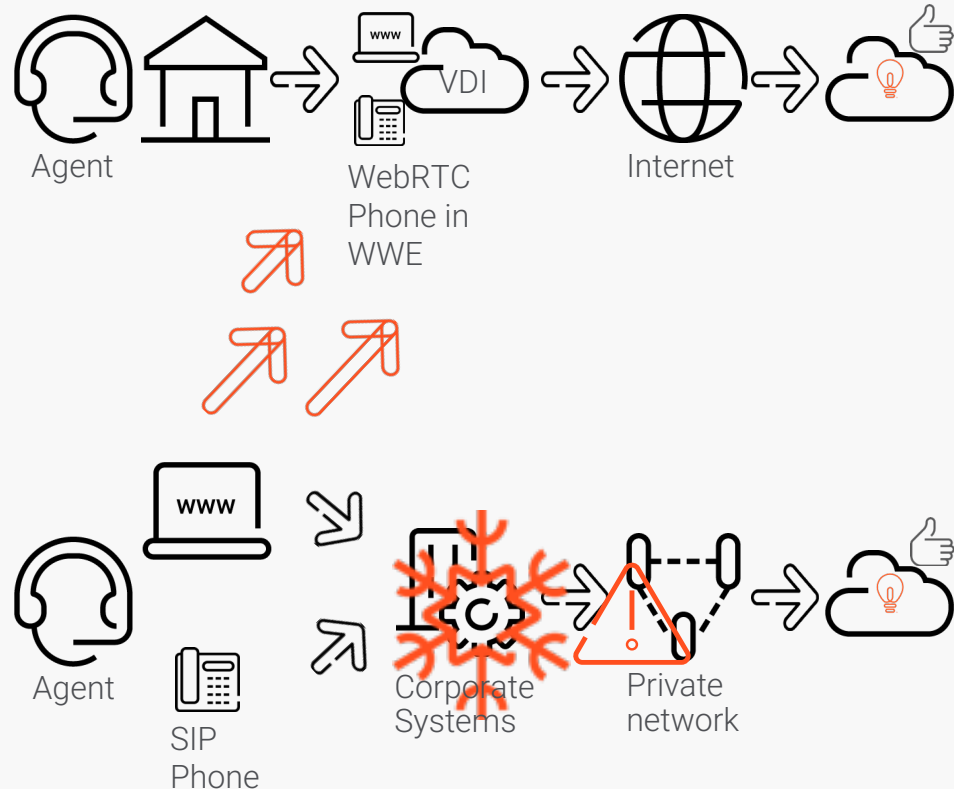
The impact of a catastrophic event is unique for each organization.

For example, a natural disaster might:

- Disrupt communications between Genesys Multicloud CX cloud and agent phones that depend on the corporate systems
Important: In an emergency situation, the PSTN carriers might start experiencing congestion in their infrastructure and decline PSTN calls, including end-customer inbound calls; outbound calls to end customers, external professional resources, partners, and vendors; and calls to the agents' PSTN phones. This issue is a concern if you want to support off-site phones over PSTN or you have an increase in end-customer calls.
- Impact your agents' ability to navigate to the Genesys Multicloud CX services via corporate systems and networks
- Cause a power outage in the corporate data center
- Prevent your agents from working on-site

Genesys Multicloud CX services and Business Continuity of your organization (3)

Example: Recovery from catastrophic failure of corporate systems and network



There are different options for you to restore access to your Genesys Multicloud CX contact center.

(Again, the example shown might not apply to your setup or might represent an unsuitable option for service restoration in your contact center.)

The wide range of supported transport networks, agent phone types, VDI technologies, proxy and VPN configurations, and so on described in this guide is an indication that the Genesys Multicloud CX solution supports many alternative ways for you to minimize the disruption and to maintain contact center operations.

Information starting [here](#) describes how you can enable your users to work off-site.

The following pages describe what elements of your Genesys Multicloud CX setup you can preserve and what you might need to change.

Genesys Multicloud CX services and Business Continuity: Agent phones

In an emergency situation, Genesys Multicloud CX cloud can deliver calls to agents as follows:

- If your agents can use preprovisioned PSTN phones, Genesys Multicloud CX cloud will deliver calls to the agents' phones.
- If your agents can use preprovisioned phones that depend on your corporate telephony, Genesys Multicloud CX cloud will engage the phones into conversations via SIP Trunks with the corporate systems. The corporate systems will deliver the calls to the agents' phones. For information about agent phones behind corporate telephony systems, see [here](#).
- If your agents can use preprovisioned SIP phones and connect to your corporate network via VPN, Genesys Multicloud CX cloud will deliver calls to the agents' phones via your SBC.

Note: VPN may affect voice quality by increasing jitter and latency.

- If your agents can use preprovisioned WebRTC phones, their phones can communicate with Genesys Multicloud CX cloud directly over the Internet.
- If an agent cannot use a preprovisioned phone, additional considerations and provisioning within Genesys Multicloud CX cloud apply. Contact your Technical Account Manager or Customer Success Manager for more information.

Amongst other requirements, you might need to define a new type of phone for the agent and/or create a new Extension DN and Place. A typical agent phone type in an emergency situation is PSTN or WebRTC.



Genesys Multicloud CX services and Business Continuity: IP-based control

In an emergency situation, agents can access Genesys Multicloud CX services as follows:

- Genesys deploys each new contact center with services accessible from anywhere on the Internet. If you maintain access restrictions at the Authentication step for access to Genesys Multicloud CX services, you might need to consider and make the services accessible from anywhere on the Internet.
- For the Genesys Multicloud CX services where IP restrictions apply, your agents must connect to Genesys Multicloud CX cloud via corporate VPN, on-premises proxy or your cloud-based proxy, or VDI. For more information about:
 - VPN, see [here](#)
 - Proxy usage, see [here](#)
 - Proxy support, see [here](#)
 - VDI support, see [here](#)

