Genesys Multicloud CX™ Contact Center Availability Guide

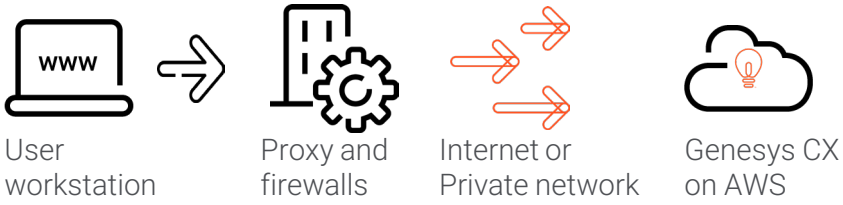
for Customers' IT, Systems, and Network Administrators

Genesys CX on AWS

Updated June 29, 2022

GENESYS™

Connectivity is the key to availability



Genesys Multicloud CX™ (formerly known as Genesys Engage cloud or PureEngage Cloud [PEC]) is the cloud-native Contact Center as a Service (CCaaS) solution available on several public cloud platforms.

This guide is for IT administrators responsible for enabling communications with Genesys CX on AWS, which is the Genesys Multicloud CX contact center deployed on the Amazon Web Services (AWS) public cloud platform.

Good and aligned end-to-end network connectivity ensures the availability of your 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 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, MPLS)

  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
  - The cloud contact center's intermediate security gateways, such as Akamai
- Settings and characteristics of the contact center

GENESYS

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

GENESYS

User communications with Genesys Multicloud CX cloud

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

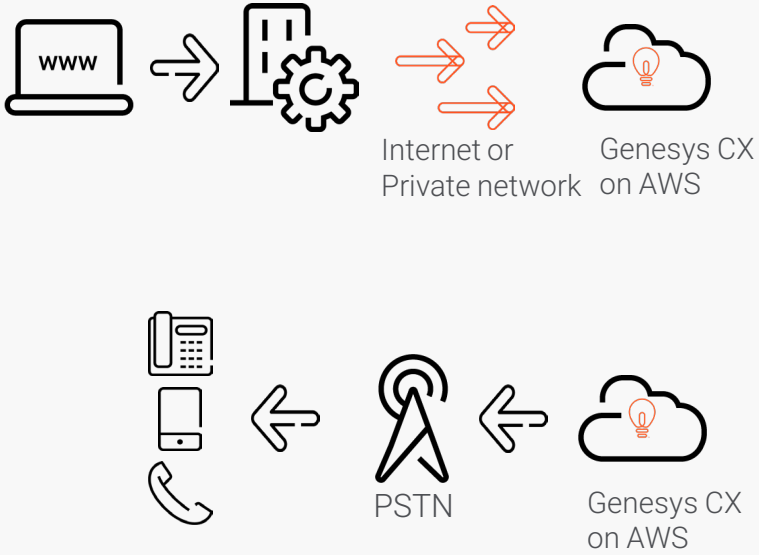
GENESYS™

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
  - Private network (for example, MPLS)
  - Public Switched Telephone Network (PSTN)
- The majority of Genesys Multicloud CX services and applications (see full list here) support access over both the Internet and a private network. (See here for exceptions that require one or the other, such as WebRTC and SIP phones.)
- Agents can use PSTN phones for voice communications.

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



GENESYS

Transport network limitations

The following Genesys Multicloud CX services and applications support communications only over the Internet:

- Genesys Softphone – WebRTC mode
- WebRTC phone embedded into Workspace
- Recording, QM and Speech Analytics – Administrator UI
- Genesys Predictive Routing – Administrator UI

The following Genesys Multicloud CX application supports communications only over a private network:

- Genesys Softphone – SIP mode

Notes:

- Genesys Multicloud CX services operate using Internet Protocol version 4 (IPv4). IPv6 is not supported.
- 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 workstations.

GENESYS

Agent phones (1)

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

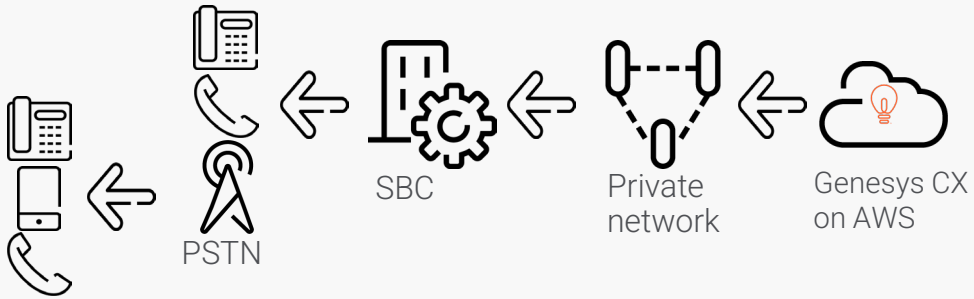
- PSTN phone (bottom diagram here)

  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 (diagram on this page)

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

  - Analog or digital phone
  - VoIP phone
  - PSTN phone



GENESYS

Agent phones (2)

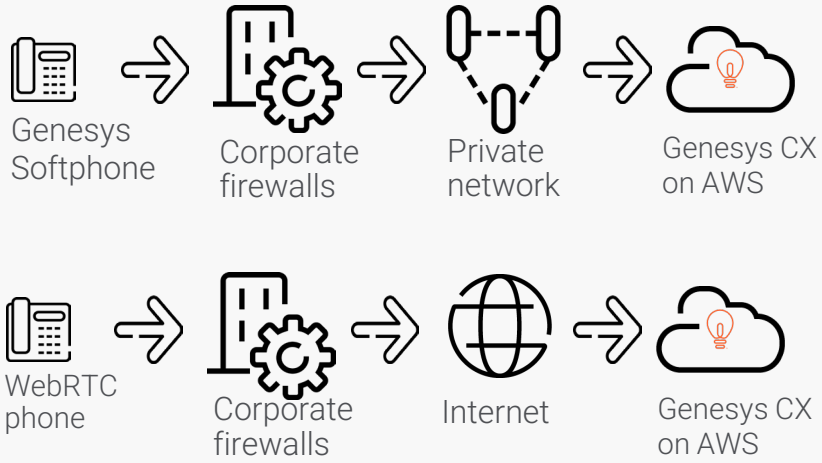
- SIP phone (for example, Genesys Softphone) SIP-registering with Genesys Multicloud CX voice service (diagram on the right)

  Communications occur directly over a private network.

- WebRTC Phone registering with Genesys Multicloud CX voice service (bottom diagram on this page)

  Communications occur directly over the Internet.

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



GENESYS

Bandwidth requirements for agent-originated traffic

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

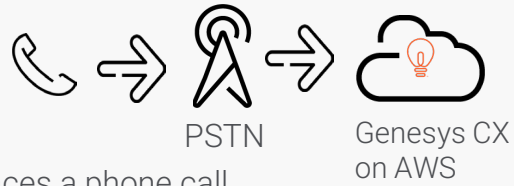
See Bandwidth Requirements for general information about bandwidth requirements for your contact center operations.

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

GENESYS

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 use the existing PSTN carriers of Genesys Multicloud CX cloud, which maintains connectivity with multiple PSTN carriers.
  - You can connect your own PSTN carrier to Genesys Multicloud CX cloud and use their dedicated circuits.
  - 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.

GENESYS

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.
  - The voice service dials the agent's phone number to engage the agent into the voice conversation.
- The agent's phone is preprovisioned in your 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.

    The set of configuration options enables your 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.

GENESYS

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: A number of services are accessible over the Internet 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 PSTN phones as additional off-site agents' phones 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 workstation to the corporate proxy for access to Genesys Multicloud CX services. See details here.
- 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. See Bandwidth Requirements for general information about bandwidth requirements.

GENESYS

Enabling your users to work off-site (2)

- Improve the capacity of the corporate VPN service.
- Use VPN with enabled split tunneling, together with PAC files and a corporate proxy, if the capacity of your corporate system is insufficient when you use VPN with disabled split tunneling. For more information, see here and here.

  Important: Because Screen Recording Service (SRS) versions prior to 8.5.370.78 do not support use of a web proxy, the SRS versions prior to 8.5.370.78 are not compatible with split tunneling for access to Genesys Multicloud CX services over the Internet. SRS of any version supports VPN with enabled split tunneling for access to the services over a private network.
- Contact Genesys Customer Care to find out the URLs for the Genesys Multicloud CX services you currently use. For details about the URLs, see here.
  - In an emergency situation, your off-site users may need to bypass the Genesys Multicloud CX Portal and navigate directly to the services using the URLs.
  - **Note:** It might be impossible to learn the URLs by clicking on the Portal widgets, because many Genesys Multicloud CX services have implemented an immediate redirect to the Authentication service prompt.
  - While the Genesys CX Portal is accessible over the Internet only from your known IP addresses, a number of the Genesys Multicloud CX services allow access from anywhere on the Internet. See here for more details about open Internet access and IP-based controls.
  - **Note:** If your off-site users have been accessing applications directly during an emergency, they must return to using the Portal when normal operations resume. This is required because the URLs on the Portal are updated periodically.
- See also Business Continuity for user access to Genesys Multicloud CX services.

GENESYS

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)
- Platform Administration (GAX) (see https://all.docs.genesys.com/PEC-PA)
- 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 – WebRTC mode (https://all.docs.genesys.com/PEC-GS/Current/Administrator/SPOverview)
- Genesys Softphone – SIP mode (https://all.docs.genesys.com/PEC-GS/Current/Administrator/SPOverview)

GENESYS

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 for access to 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:
  - 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 Agent Desktop application.

GENESYS

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 and WebRTC) with enabled Connector and VDI adapter, Screen Recording Service (SRS)	Supported	Not supported	Not supported	Not supported
Workspace 9, Genesys Softphone (SIP and WebRTC) 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. Windows Server 2012 R2 Extended Support will end in October, 2023.

GENESYS

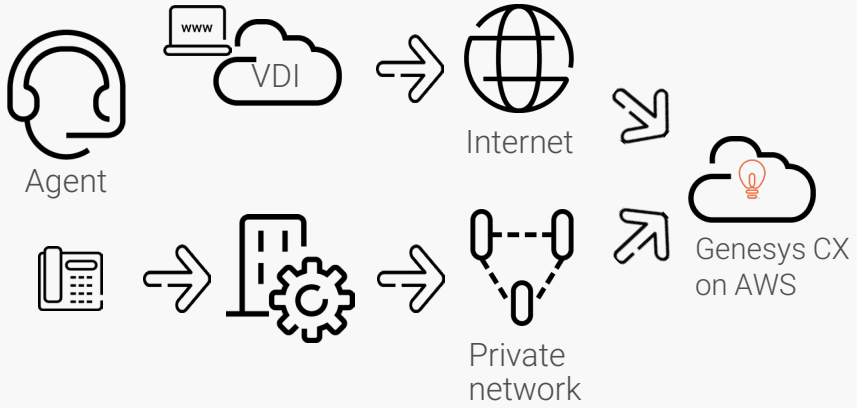
Applications for users: Data communications and VoIP communications (1)

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.

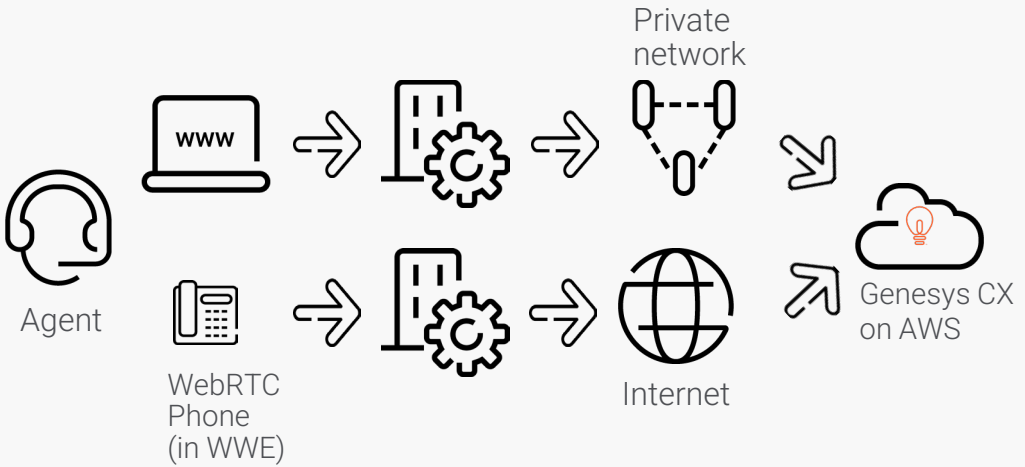


GENESYS

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 over the private network.
  - The WebRTC phone communicates with Genesys Multicloud CX services directly over the Internet.



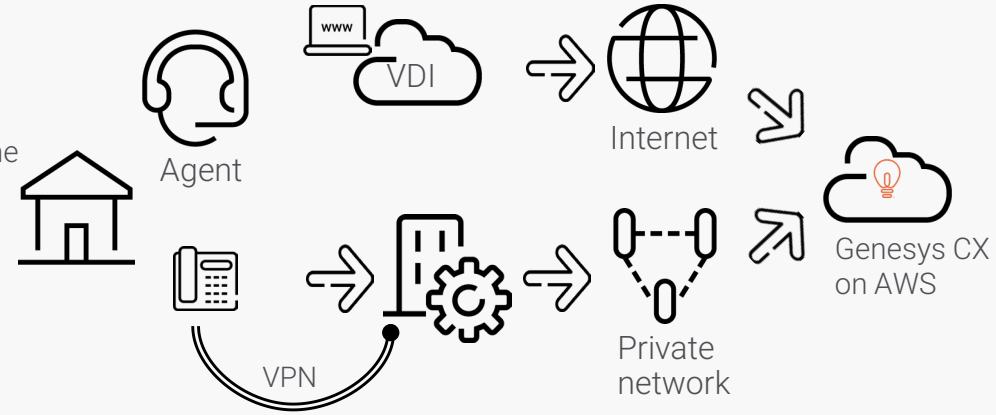
GENESYS

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.
  - The browser running on 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 Genesys Multicloud CX voice service via the corporate VPN with enabled split tunneling and over the private network. (See more information about split tunneling here.)



GENESYS

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 the 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 agent's phone into conversation with the end customer 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 enabled split tunneling provides access to the Agent Desktop service over the respective transport network.

GENESYS

Applications for users: URLs and name resolution

The Genesys Multicloud CX cloud 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 `genesyscloud.com` domain.

  For example:

  - `best-customer.genesyscloud.com`
  - `best-customer.digital.genesyscloud.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://*.genesyscloud.com

GENESYS

Applications for users: Protocols and ports

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

Exception: For better user experience, the Portal web page (for example, `best-customer.genesyscloud.com`) supports plain text HTTP (TCP port 80) with immediate redirection to HTTPS.

Exception: WebRTC phones establish the media stream 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 stream 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).
  - You can define and configure the signaling and media port numbers that the phone will occupy on the user workstation while originating connections towards Genesys Multicloud CX voice service.
  - The Genesys Multicloud CX cloud SBC port numbers for signaling and media communications are defined during the onboarding process.

GENESYS

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 cloud applications that are deployed as standalone software support web proxy as follows:

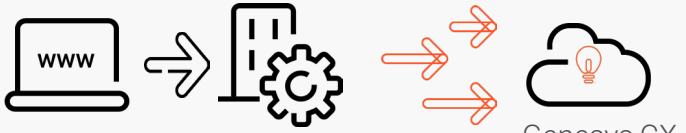
Software installed on user workstation	Proxy settings in the configuration file	Proxy settings in Genesys Multicloud CX cloud (Person level, Agent Group level, etc.)
Signaling traffic of Genesys Softphone in WebRTC mode	Supported (except for authentication)	Supported (except for authentication)
Media traffic of Genesys Softphone in WebRTC mode	Not supported	Not supported
Control and upload traffic of Screen Recording Service, 8.5.370.78 and higher	Supported	Not supported

Note: Screen Recording Service (SRS) versions prior to 8.5.370.78 do not support use of a web proxy.

GENESYS

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.



- If the proxy systems restrict web navigation, do one of the following:
  - Allow access to any URL constructed of the `genesyscloud.com` domain.
  - 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:
    - The majority of web-based applications utilize additional URLs for authentication; Agent Desktop utilizes the Telemetry service URL.
    - Recording, QM and Speech Analytics utilizes additional URLs for the Recording Crypto Service and Recording Playback.

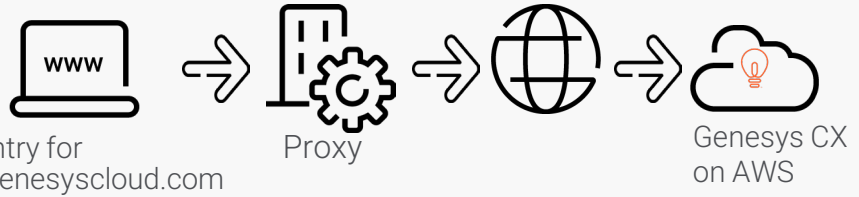
    To find out the host portion of all URLs your users use, contact Genesys Customer Care.
- If your agents use Genesys Softphone in WebRTC mode, to enable signaling (HTTPS):
  - Disable Proxy authentication for the URL of the WebRTC service handling the signaling traffic.
- If your agents use WebRTC phones embedded into Workspace, to enable the media stream (SRTP protocol, TCP port 443):
  - Exclude the URL of the TURN interface from the list of destinations served by your proxy (see here for more details).
  - If you cannot exclude the URL, disable HTTPS deep packet inspection for the SRTP traffic to the TURN interface.

GENESYS

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 the 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 enabled split tunneling. The VPN enables access to corporate systems; to the Genesys Multicloud CX services; and to 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

GENESYS

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 workstations. 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.
3. If you use a PAC file for WebRTC phones embedded into Workspace, exclude the FQDN of the TURN interface from the list of destinations served by your proxy. In this way, you enable a direct media stream connection from WebRTC phones to the TURN interface over the Internet.

Example of PAC file content

```
function FindProxyForURL(url, host) {
           // URLs from the domains under genesyscloud.com must use the proxy:
           if (shExpMatch(host, "*.genesyscloud.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 `genesyscloud.com`.

GENESYS

Access via dedicated proxy systems: Signaling traffic of Genesys Softphone in WebRTC mode

Genesys Softphone in WebRTC mode uses HTTPS for signaling (to register with and receive calls from the Genesys Multicloud CX voice service through the WebRTC service).

High-level configuration steps

To enable Genesys Softphone in WebRTC mode to use dedicated proxy systems to access the voice service through the WebRTC service:

1. The Workspace Connector must be enabled.
2. Use the Agent Setup User Interface to configure the **sipendpoint.proxies.proxy0.http_proxy** option, to specify the proxy name (or IP address) and the port. You can configure the option at different levels – for example, at the level of the Person, Agent Group, Virtual Agent Group (VAG), and so on.

Configuration option example

```
[interaction-workspace]
sipendpoint.proxies.proxy0.http_proxy = To-GenesysMulticloudCX.internal.example.com:8080
```

In this example:

- The FQDN of the proxy is: `To-GenesysMulticloudCX.internal.example.com`
- The Proxy listens on port 8080.

Note: The proxy can be configured in the local configuration file if the Workspace Connector is disabled. For more information, see https://all.docs.genesys.com/PEC-GS/Current/Administrator/SPDeploy

GENESYS

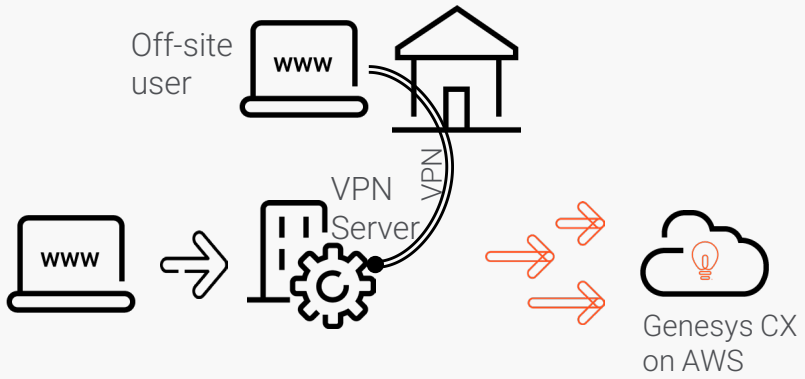
Access via VPN to the corporate network

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:

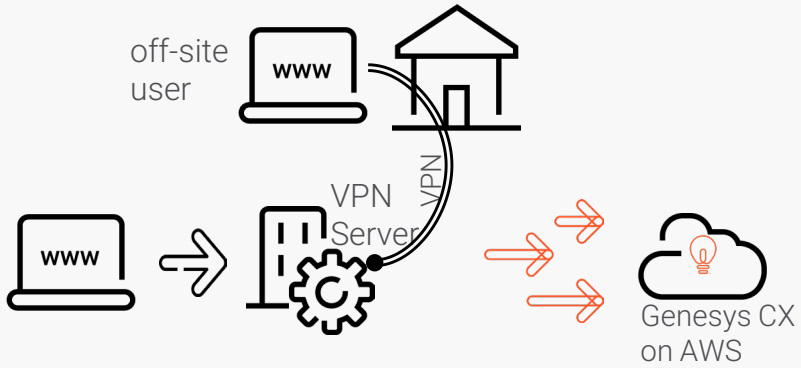
- The same proxy systems and firewalls usually control the Internet traffic originated by internal users and by VPN-connected users.
- If additional intermediate systems control Internet access from the VPN-connected workstation, configure the additional systems to enable access to Genesys Multicloud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



GENESYS

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.



- If your off-site users access the Genesys Multicloud CX services over a private network, ensure that the list of destinations accessible via the VPN includes the stable IP addresses of these services on the private network.

  For more information, see here.

- If your on-site users access Genesys Multicloud CX services over the Internet, allow your off-site and your on-site users to access the 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 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 stable IP addresses from the list of destination IP addresses handled by your VPN tunnel. In this way, you enable a direct voice stream connection from WebRTC phones to the TURN interface over the Internet.

  For more information, see here.

GENESYS

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

GENESYS™

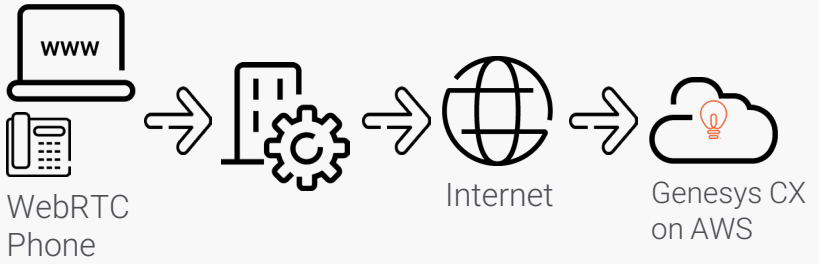
Access over the Internet

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

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

- The diagram on the right shows this type of connectivity for access to Genesys Multicloud CX services and WebRTC phone communications.

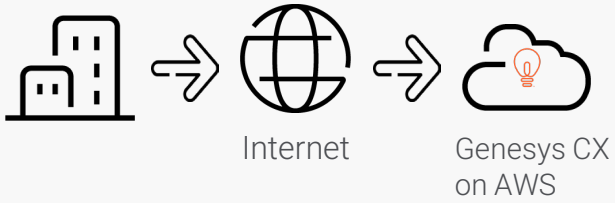


GENESYS

Access over the Internet: Considerations

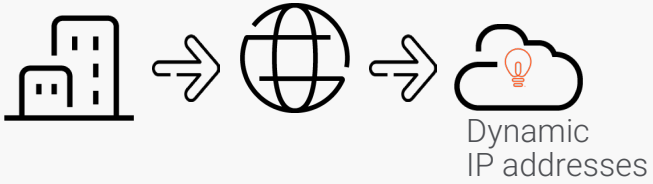
To enable user access to Genesys Multicloud CX cloud services reachable over the Internet by a public IP address, you must consider:

- 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)
- 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 the services via the proxy.
  - Use the stable IP addresses of the TURN interfaces to exclude WebRTC media traffic from the VPN tunnel.



GENESYS

User access over the Internet: Dynamic IP addresses



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

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

- There are no stable Internet-routable IP addresses for the services.

  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 Genesys Multicloud CX services over the Internet.

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

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

- To enable a direct media stream connection from WebRTC phones to the TURN interface over the Internet:
  - If you use a PAC file for browsers running WebRTC phones embedded into Workspace, exclude the FQDN of the TURN interface from the list of destinations served by your proxy.

    Note: The Genesys Softphone in WebRTC mode does not support use of a proxy for media traffic. The Genesys Softphone originates a media connection directly to the IP addresses obtained as a result of name resolution for the TURN interfaces.
  - If your users use VPN, exclude the TURN interface IP addresses from the list of destination IP addresses handled by your VPN tunnel.

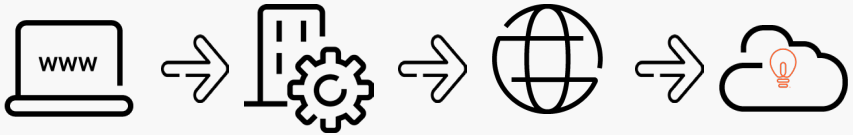
GENESYS

User access over the Internet via firewall

- To enable access to Genesys Multicloud CX services, configure the firewall that controls access to the Internet to allow connections to TCP port 443 at any destination on the Internet.

  Ensure you configure all firewalls under your control on the traffic path.

  - If access to the services relies on your proxy systems, allow the proxy systems to connect to any destination.
  - If you do not use proxy systems, configure the on-site firewall to allow the browsers and the standalone software to connect to any destination.
  - If you use a software firewall on user workstations, allow the browsers and the standalone software to connect to any destination.
- If your agents use WebRTC phones:
  - To enable the media stream (SRTP protocol, TCP port 443), disable HTTPS deep packet inspection for connections to the TURN Interface IP addresses.



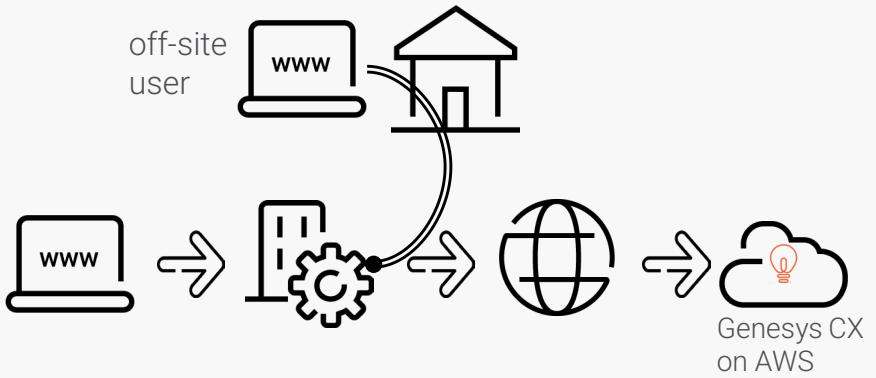
GENESYS

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 TURN Interface IP addresses (so, you enable a direct media stream connection from WebRTC phones to the TURN interface over the Internet).
3. Configure a PAC file on the off-site user workstations 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.

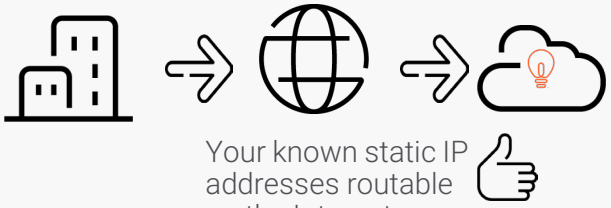
See additional details here and here.



GENESYS

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

Genesys deploys each new contact center according to the Least Privilege policy: “Deny everything that is not explicitly permitted."



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 cloud side.

Genesys implements network access control, configuring explicit permissions that allow access to the Genesys Multicloud CX services over the Internet only from the known IP addresses of the customer.

- For each customer, Genesys maintains a list of the customer’s 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).

To request access to the Genesys Multicloud CX services from your network, submit a request to Genesys Customer Care.

- 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).

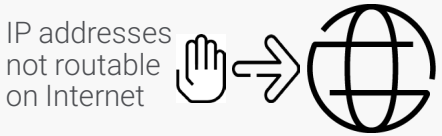
  Genesys expects that the IP addresses are allocated to your company by an IP Registry or your Internet Service Provider, or that they belong to the Vendor of your cloud-based Proxy or VDI service.
- Do not request enabling access for IP addresses that Internet Service Providers assign to your off-site workers’ network equipment. Such addresses are dynamic and temporary.

GENESYS

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



GENESYS

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

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

Authentication 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.

A number of the Genesys Multicloud CX services, such as Agent Desktop and WebRTC, are approved to be accessible from anywhere on the Internet.

If your contact center on Genesys Multicloud CX cloud utilizes Single Sign On (SSO) authentication with enabled Multi Factor Authentication, you can request enabling open Internet access to the approved services.

Relying on Authentication IP-based control, Genesys Multicloud CX cloud meets access restriction requirements for some customers, while open Internet access to the approved services is enabled for other customers whose off-site users require direct access to their Genesys Multicloud CX contact center.

The MACD process to manage access restrictions requires you to open a case with Genesys Customer Care:

- To enable open Internet access to the approved services
- To re-apply restricted access by re-enabling Genesys Authentication Service IP-based access control

GENESYS

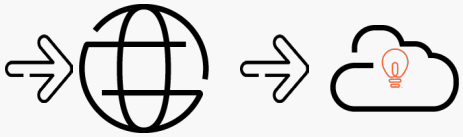
Access over the Internet: Dual control

The majority of the Genesys Multicloud CX services rely on the Genesys Authentication Service. If you enable Authentication Service IP-based control, access to all such services is restricted by the applied IP access-list.

- For a list of applications that support Authentication Service, see https://all.docs.genesys.com/PEC-Admin/Current/Admin/SSO

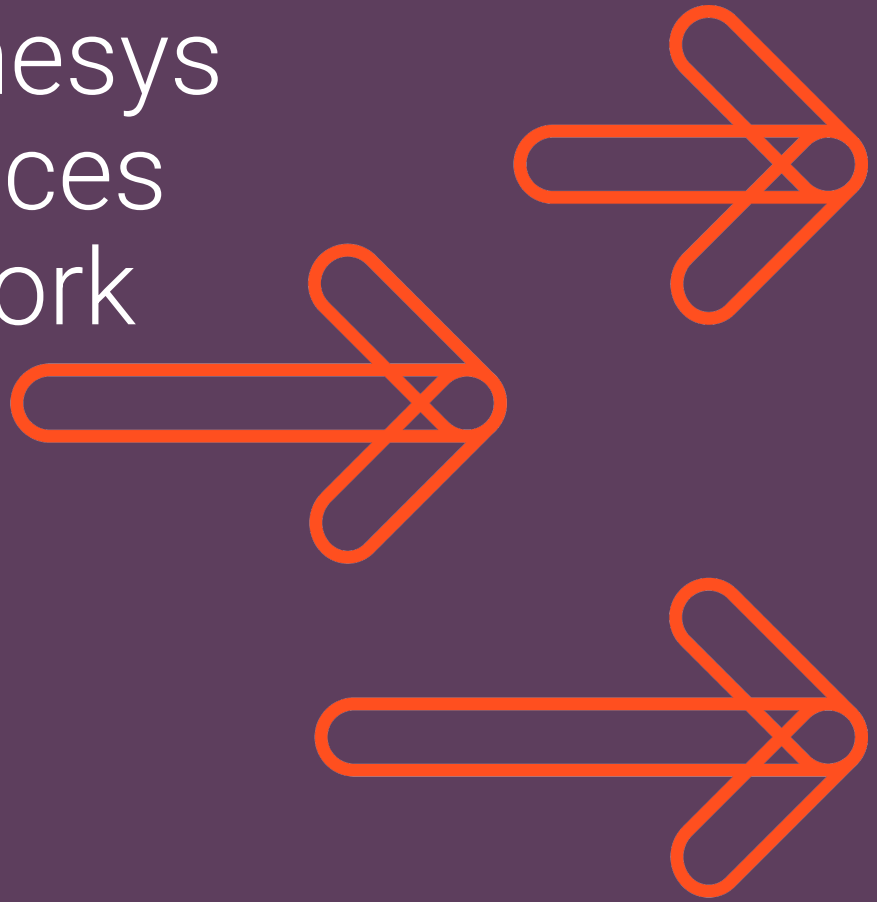
Some of the applications and services that utilize Authentication Service do not support open Internet access. Access to such applications is restricted at two control points:

- Genesys implements network access control and allows access to the applications only from your known IP addresses. (You provide the up-to-date list of your known IP addresses to Genesys Customer Care.)
- Authentication Service restricts access at the authentication step.



User access to Genesys Multicloud CX services over a private network

- Stable Genesys Multicloud CX IP addresses on the private network
- Firewall permissions
- Split tunneling for off-site users
- IP-based access restrictions

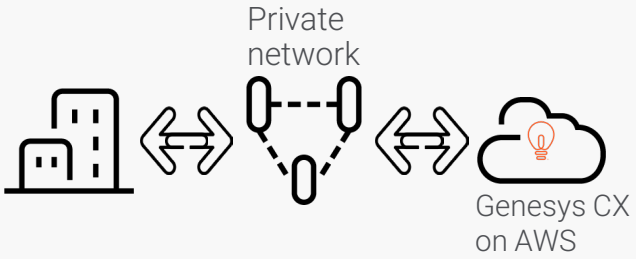


GENESYS™

Access over private networks

A private network, such as MPLS, 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 Agent Desktop and other services.
- Agent's SIP phone registers with the voice service through the cloud SBC, from which it then receives calls.
- Agent's Screen Recording Service uploads screen recordings.
- Administrator's browser connects to your contact center services.



To enable user access over a private network, 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 cloud access policy and IP-based access restrictions (more information starts here)
- There are additional configuration considerations if you want to use VPN split tunneling as the technique to enable 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 for the web-based services accessible over the Internet and direct the browsers to the corporate web proxy. (As described under Transport network limitations, there are services that support access only over the Internet.)
  - Use the stable IP addresses of the services accessible over the private network (more information here).
  - Use the stable IP addresses of the cloud SBC SIP and media interfaces.

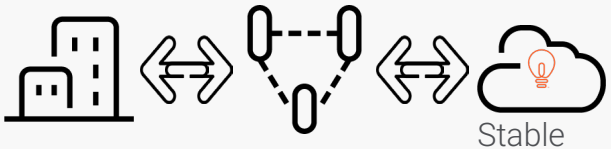
GENESYS

Access over a private network: Stable IP addresses

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

  Exception: SIP Phones SIP-registering with the voice service through the cloud SBC use SIP for signaling traffic and RTP/RTCP for media traffic.
- IP addresses for the services are stable and routable on the private network.

  Note: As described under Transport network limitations, there are service that support access only over the Internet.



- **Important:** You must *not* expose to the Internet the Genesys Multicloud CX interfaces accessible over the private network.

  Do not use NAT, reverse proxy, SBC, or any other techniques to enable access over the Internet to the Genesys Multicloud CX private interfaces via your systems exposed to the Internet.
- You can use IP address-based permissions on your firewall to control access to your contact center services over the private network.
  - The SIP expire timer in the voice service is set to 140 seconds. The firewall idle timeout for UDP sessions 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 your contact center voice service to reach the SIP phones before the SIP registration expires.
  - The UDP session for the media stream is always originated by the SIP phone. The cloud SBC initiates RTP traffic towards the SIP phone after receiving RTP traffic from the phone. The cloud SBC sends RTP packets to the IP address and port that the SIP phone used while initiating the UDP session for the media stream.

GENESYS

Access over a private network via firewall (1)

- If access to Genesys Multicloud CX services relies on your proxy systems, configure the firewall that controls the proxy access to the private network to allow the proxy systems to send requests to TCP port 443 at the Genesys Multicloud CX IP ranges on the private network.

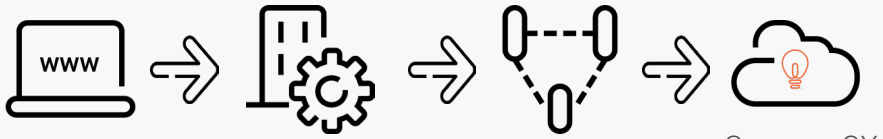
  Note: As described under Transport network limitations, there are services that support access only over the Internet. For information about firewall configuration for access over the Internet, see here.

- 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 the Genesys Multicloud CX IP ranges on the private network.

GENESYS

Access over a private network via firewall (2)

- If agents use SIP Phones SIP-registering with Genesys Multicloud CX voice service, configure the on-site firewall to allow the phone to originate SIP signaling and media stream traffic (RTP/RTCP) towards Genesys Multicloud CX cloud.
  - If your firewall performs NAT/PAT, estimate the number of simultaneous UDP sessions traversing the firewall and allocate a sufficient number of IP:port pairs to avoid port collision across the UDP sessions.
  - Determine the port numbers for signaling and media (RTP/RTCP) configured on the Genesys Softphone in SIP mode.
  - The Genesys Multicloud CX port numbers for signaling and media communications are defined during the onboarding process.
  - Configure firewall permissions for signaling and media traffic originated by SIP phones.
  - Additional considerations for the firewall configuration:
    - Configure the firewall UDP session idle timeout to allow for the SIP expire timer controlled by the voice service (140 seconds). See more information here.
    - See also the information about voice media UDP sessions and RTP streams here.



GENESYS

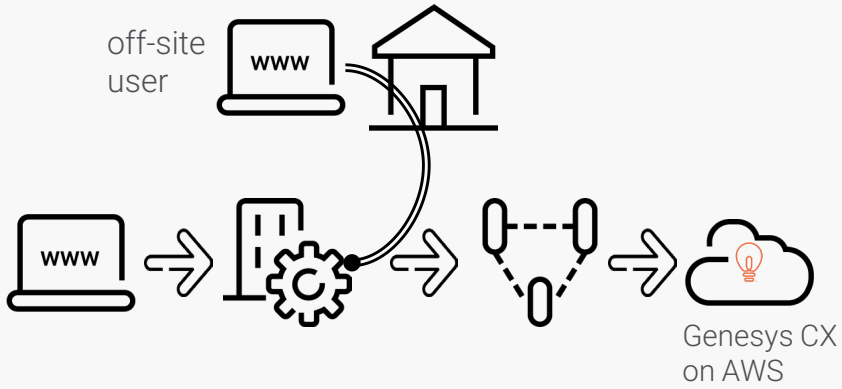
Access over a private network: VPN split tunneling

High-level configuration steps

1. In the list of destination IP addresses handled by your VPN tunnel, include the stable IP addresses of the Genesys Multicloud CX services routable on the private network (“*split-include*“ tunnel configuration).
2. If you use a PAC file to access the services:
    1. In the list of destination IP addresses handled by your VPN tunnel, include the internal IP addresses of your corporate proxy systems.
    2. 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.
    3. Configure the off-site user’s browser to use the PAC file to locate a proxy.

Note: As described under Transport network limitations, there are services that support access only over the Internet. Forinformation about split tunneling configuration for access over the Internet, see here.

See also general information about VPN and split tunneling here and here.

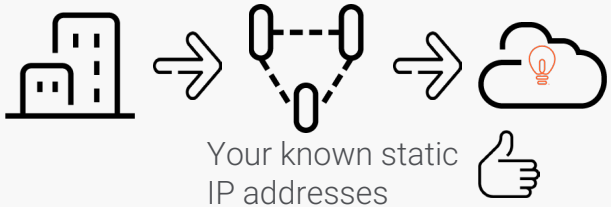


GENESYS

Access over a private network: Access policy at Genesys Multicloud CX cloud

Genesys deploys each new contact center according to the Least Privilege policy: “Deny everything that is not explicitly permitted"

Genesys implements network access control, configuring explicit permissions that allow access to the Genesys Multicloud CX services over the private network only from the known IP addresses of the customer.



- For each customer, Genesys maintains a list of the customer’s known IP addresses routable on the customer’s private network.
- The list includes only the IP addresses routable on the private network, such as MPLS.

To request access to Genesys Multicloud CX services from your new IP network, submit a request to Genesys Customer Care.

- Ensure that your corporate network team enabled IP routing between the Genesys Multicloud CX networks and your new IP network.

  If your MPLS carrier controls the routing for your networks, ensure that the carrier enabled the IP routing for your new network.
- Provide the IP addresses of your new IP network.
  - Genesys will verify the existence of the IP route to your network in the routing table on the private network.
  - Genesys will add the IP addresses to the list of known IP addresses and thus enable access to the Web-based, SIP, and media interfaces of Genesys Multicloud CX cloud.

GENESYS

Business Continuity for user access to Genesys Multicloud CX services

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

GENESYS™

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

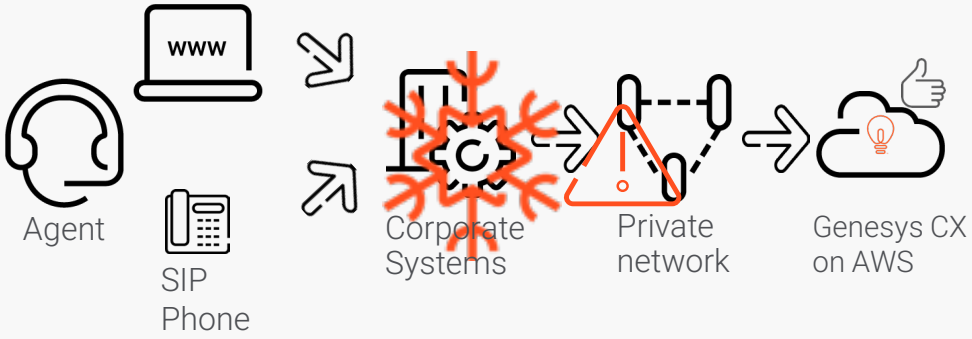
A disaster can occur at any time.

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

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:

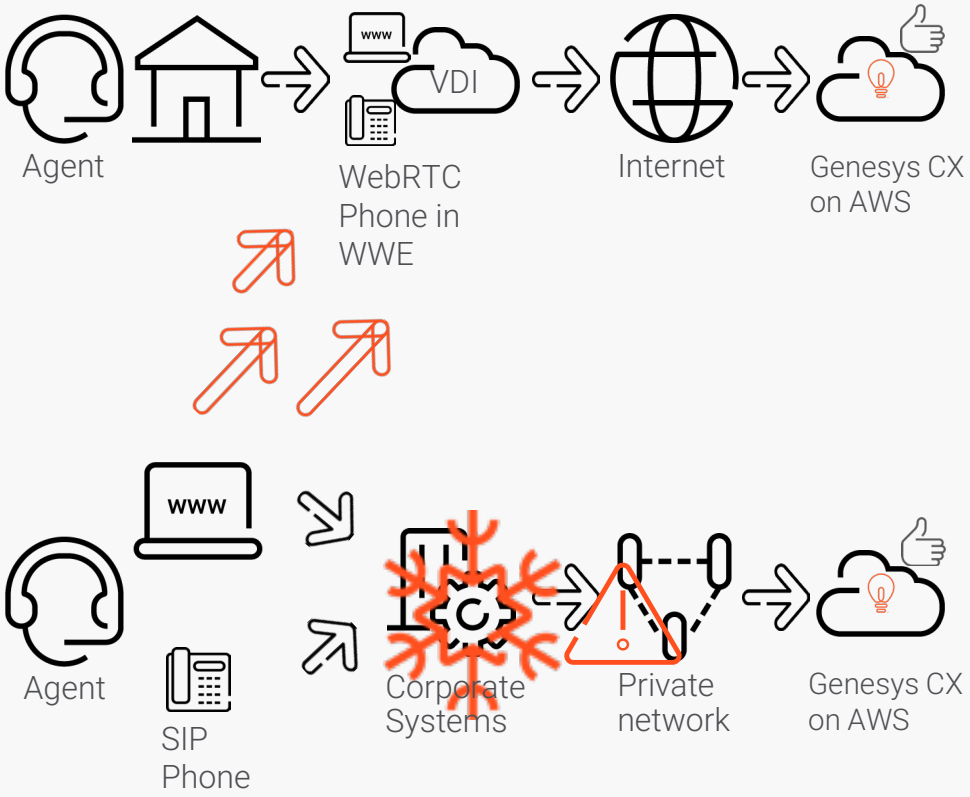
- Disrupt communications between Genesys Multicloud CX cloud and agent phones that depend on the corporate systems

  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

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

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.

  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

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

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

- A number of the services can be accessible from anywhere on the Internet if your contact center utilizes Single Sign On (SSO) authentication with enabled Multi Factor Authentication. For a list of the applications that support SSO, see https://all.docs.genesys.com/PEC-Admin/Current/Admin/SSO.

  Agent Desktop and WebRTC are examples of the services that are conditionally accessible from anywhere on the Internet.

  If you maintain access restrictions at the Authentication step for access to your contact center services, you might need to consider and make the services accessible from anywhere on the Internet.
- For your contact center 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

GENESYS