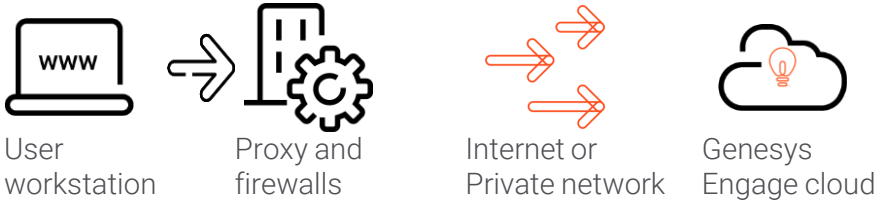
Genesys Engage™ Cloud Contact Center Availability Guide

for Customers' IT, Systems, and Network Administrators

Updated November 19, 2020

GENESYS

Connectivity is the key to availability



This guide is for IT administrators responsible for enabling communications with the Genesys Engage cloud contact center (formerly known as PureEngage Cloud [PEC]).

Good and aligned end-to-end network connectivity ensures the availability of Genesys Engage cloud services.

The topics in this guide help you 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 applications seamlessly.

A successful end-to-end journey of Genesys Engage cloud application data and voice traffic depends 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 Genesys Engage cloud contact center

GENESYS

Main topics

- User communications with Genesys Engage cloud
- User access to Genesys Engage cloud over the Internet
- User access to Genesys Engage cloud over a private network
- Business Continuity for user access to Genesys Engage cloud

GENESYS

User communications with Genesys Engage cloud

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

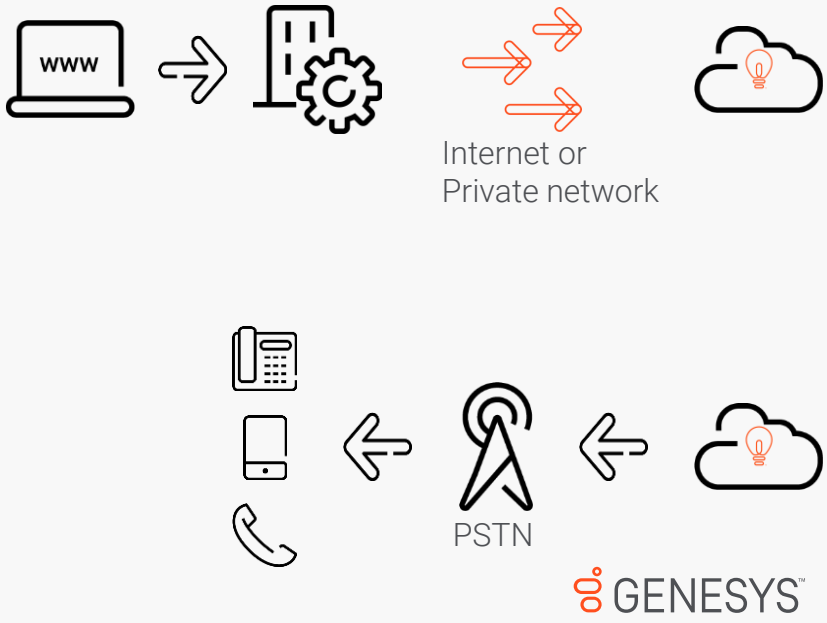
GENESYS™

Communications with Genesys Engage cloud: Transport networks

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

- You can enable your agents to communicate with Genesys Engage cloud via:
  - Internet
  - Private network (for example, MPLS)
  - Public Switched Telephone Network (PSTN)
- The majority of Genesys Engage cloud applications (see full list here) support access via both the Internet and a private network. (See Transport network limitations for exceptions that require one or the other, such as WebRTC and SIP phones.)
- Agents can use PSTN phones for voice communications.

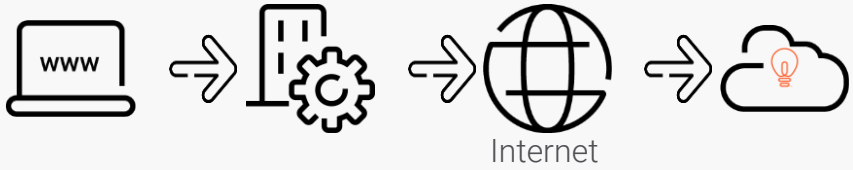
  Via PSTN, Genesys Engage cloud can invite into conversation any agent's phone that has a PSTN number (analog, digital, mobile, VoIP, home, or business phone).



Access to Genesys Engage cloud: Transport network limitations

The following Genesys Engage cloud applications support communications only via 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 Engage cloud application supports communications only via a private network:

- Genesys Softphone – SIP mode

Notes:

- Genesys Engage cloud operates using Internet Protocol version 4 (IPv4). IPv6 is not supported.
- Genesys Engage cloud uses 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.

GENESYS

Genesys Engage cloud: Agent phones

Genesys Engage cloud, which invites the phone into conversation, supports the following Agent phone types:

- PSTN phone (diagram here)

  Communications occur via PSTN.

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

  Communications occur via a SIP Trunk over a private network. The following types of phone are supported:

  - Analog or digital phone
  - VoIP phone
  - PSTN phone

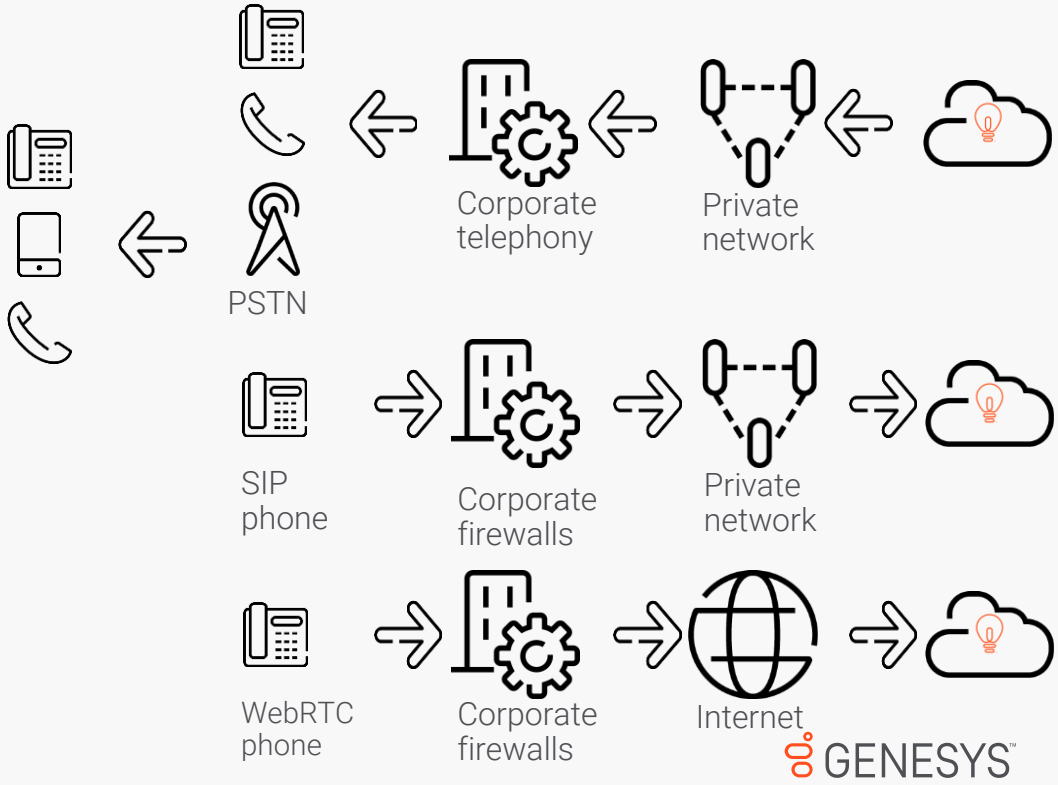
- SIP phone SIP-registering with Genesys Engage cloud (middle diagram on this page)

  Communications occur directly over a private network.

- WebRTC Phone registering with Genesys Engage cloud (bottom diagram on this page)

  Communications occur directly over the Internet.

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



Genesys Engage cloud: Bandwidth requirements for agent-originated traffic

The following table shows bandwidth requirements for typical voice and data applications.

For general information about bandwidth requirements for Genesys Engage cloud operations, see https://all.docs.genesys.com/PEC-Admin/Current/Admin/Requirements#Bandwidth_requirements.

Traffic	Bandwidth	Transport via	When
Voice (SIP/RTP)	100 kbps G.711	MPLS	Per call
WebRTC (Opus)	Variable 10 kbps to 160kbps	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

Genesys Engage cloud: 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 Engage cloud 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 Engage cloud session border controller (SBC).

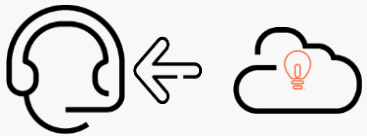
  Genesys Engage cloud can receive the PSTN call placed by your end customer via one of the following paths:
  - You can use the existing PSTN carriers of Genesys Engage cloud, which maintains connectivity with multiple PSTN carriers.
  - You can connect your own PSTN carrier to Genesys Engage cloud and 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 Engage cloud over your private network, as illustrated in the diagram below.

GENESYS

Genesys Engage cloud: End customer PSTN calls and agent calls (2)

- Genesys Engage cloud 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 Engage cloud dials the agent's phone number to invite the agent into the voice conversation.
- The agent's phone is preprovisioned in Genesys Engage cloud 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 Genesys Engage cloud 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 Engage cloud applications 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 Genesys Engage cloud applications are accessible over the Internet only from your known IP addresses.

  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 customer traffic.

- Use virtual desktop infrastructure (VDI) technologies (including on-site Windows Remote Desktop Services) for the web-based Genesys Engage cloud applications. See VDI support details here.

  Note: In an emergency situation, it is considered acceptable that a user needs to navigate to some applications directly from the user workstation and to 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 Engage cloud applications. 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. For general information about bandwidth requirements, see https://all.docs.genesys.com/PEC-Admin/Current/Admin/Requirements#Bandwidth_requirements.

GENESYS

Enabling your users to work off-site (2)

- 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.

  Important: Because Screen Recording Service (SRS) does not support use of a web proxy, SRS is not compatible with split tunneling for access to Genesys Engage cloud over the Internet. Split tunneling for access to Genesys Engage cloud over a private network is supported.
- Contact Genesys Customer Care to find out the URLs for the Genesys Engage cloud applications you currently use. For details about Genesys Engage cloud URLs, see here.
  - In an emergency situation, your off-site users may need to bypass the Genesys Portal (also known as *Genesys Hub*) and navigate directly to the Genesys Engage cloud applications using the URLs.
  - **Note:** It might be impossible to learn the URLs by clicking on the Portal widgets, because many applications have implemented an immediate redirect to the authentication page.
  - While the Portal page is accessible over the Internet only from your known IP addresses, a number of the Genesys Engage cloud applications allow access from anywhere on the Internet.
  - **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 Engage cloud.

GENESYS

Genesys Engage cloud applications for users: Browser-based vs. standalone

The majority of the Genesys Engage cloud applications used by users are web-based applications running in a browser:

- 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)
- Cloud Data Download Service (CDDS) – Administrator UI (see https://all.docs.genesys.com/PEC-CDDS)
- CX Contact – Administrator UI (see https://all.docs.genesys.com/PEC-OU/Current/CXContact/GetStarted)
- Designer (see https://all.docs.genesys.com/PEC-ROU/Current/Designer/GetStarted)
- Developer Console (see https://all.docs.genesys.com/PEC-Developer/DeveloperSandbox)
- Genesys CX Insights (see https://all.docs.genesys.com/PEC-REP/Current/Administrator/HRCXIUsrMgmt)
- Real-Time Reporting (Pulse) (see https://all.docs.genesys.com/PEC-REP/Current/RT/RealTimeReporting)
- Recording, QM 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)
- Management 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

Genesys Engage cloud applications for users: User workstation system requirements

User workstation capacity and software versions ensure successful communications with Genesys Engage cloud.

- Typically, users use a personal workstation for access to Genesys Engage cloud. Refer to the application documentation (see links here) for more information.
- Alternatively, users rely on virtual desktop infrastructure (VDI). Supported as follows:
  - Genesys Engage Agent Desktop – Workspace 9 supports Citrix XenApp, XenDesktop 7, and VMWare Horizon 7. More details here.
  - Genesys Softphone – see https://all.docs.genesys.com/PEC-GS/Current/Administrator/SPOverview

    Important: The customer assumes responsibility for WebRTC phones deployed on VDI, including WebRTC phone embedded into Workspace and Genesys Softphone in WebRTC mode.
  - Screen Recording Service – see https://all.docs.genesys.com/PEC-REC/Current/Administrator/ScreenRecordingConfig
  - All other browser-based applications support any VDI.
- Users can use their personal workstations to access one set of the Genesys Engage cloud applications and VDI for another set of the applications.

  Exception: WebRTC phone cannot be decoupled from the Workspace.

GENESYS

Genesys Engage cloud: 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 2008 R2 or Windows Server 2012 R2	Linux eLux OS	Server 2012 R2	Server 2008 R2
Workspace 9, Genesys Softphone (SIP and WebRTC) with enabled Connector and VDI adapter, 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: On January 14, 2020, Microsoft support for Windows Server 2008 R2 ended.

GENESYS

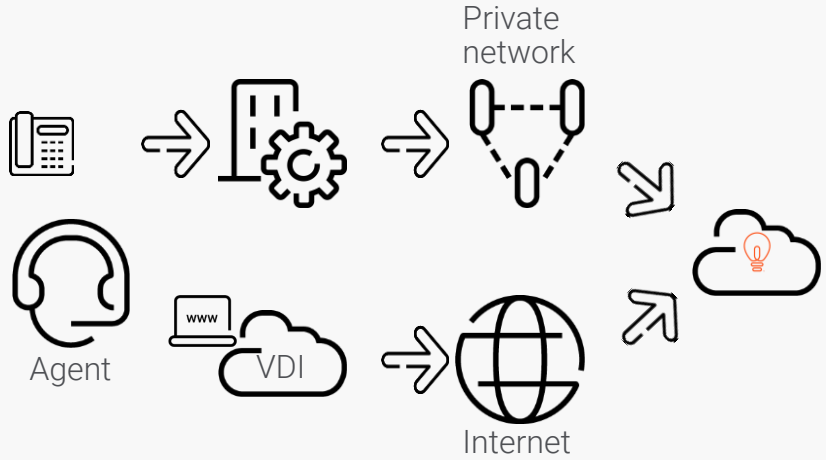
Genesys Engage cloud applications for users: Data communications and VoIP communications (1)

There is no dependency between the transport network used for agent access to the 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 Engage cloud 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.

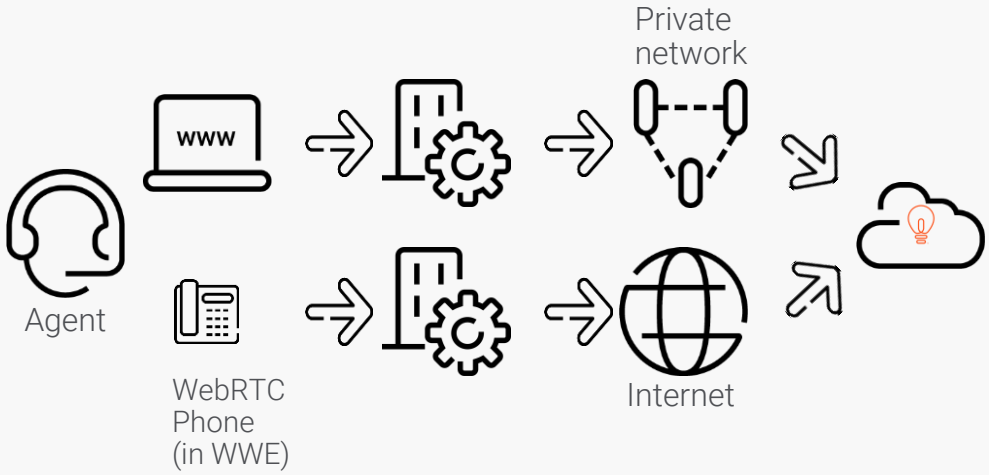


GENESYS

Genesys Engage cloud 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 application via the private network.
  - The WebRTC phone communicates with Genesys Engage cloud directly over the Internet.



GENESYS

Genesys Engage cloud 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 Engage cloud 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 Engage cloud via the corporate VPN with split tunneling enabled and over the private network. (See more information about split tunneling here.)

GENESYS

Genesys Engage cloud 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 Engage cloud over the Internet.
  - The off-site agent runs a browser with Workspace on the agent's workstation at home and accesses Genesys Engage cloud via 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 Engage cloud invites the phone into conversation via a SIP Trunk with the corporate telephony systems over a private network. The corporate systems deliver 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 Engage cloud directly over the Internet.
  - The corporate VPN with split tunneling enabled provides access to the Agent Desktop application via the private network.

GENESYS

Genesys Engage cloud applications for users: URLs and name resolution

The Genesys Engage cloud applications are addressed by means of URLs.

- The host portion of a URL (the Fully Qualified Domain Name [FQDN]) is constructed of a name within the `genesyscloud.com` domain.

  For example:

  - `best-customer.genesyscloud.com`
  - `best-customer.socialanalytics.genesyscloud.com`

  Exception: WebRTC phones embedded into Workspace and Genesys Softphones in WebRTC mode (WebRTC phones) *may* establish a media connection to the Genesys Engage cloud TURN interface addressed by an FQDN within the `amazonaws.com` domain.

- 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

Genesys Engage cloud applications for users: Protocols and ports

- Genesys Engage cloud applications 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 voice media connection to the Genesys Engage cloud TURN interface on TCP port 443 but do not use HTTPS. Instead, WebRTC phones use SRTP for the media connection.

- Genesys Engage cloud applications 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 Genesys Engage cloud port numbers for signaling and media communications are defined during the onboarding process.
  - The SIP phone port numbers for signaling and media communications are configurable.

GENESYS

Genesys Engage cloud applications for users: Web proxy support

Genesys Engage cloud applications that are accessible using a browser 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 Engage 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 Engage 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	Not supported	Not supported

GENESYS

Enabling access to Genesys Engage cloud via proxy

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

Proxy to allow navigation to https://*.genesyscloud.com

- If the proxy systems restrict web navigation, do one of the following:
  - Allow access to any URL constructed of the `genesyscloud.com` domain.

    Exception: WebRTC phone embedded into Workspace *may* establish a media connection to the Genesys Engage cloud TURN interface addressed by a Fully Qualified Domain Name (FQDN) within the `amazonaws.com` domain.
  - Allow access only to the URLs of the applications you use.

    Note that there are applications that instruct the browser to send requests to additional Genesys Engage cloud 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 embedded into Workspace, the proxy systems must be transparent for media traffic.

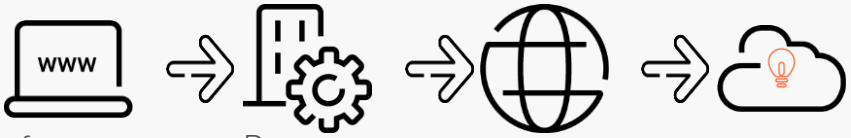
  The phone respects the browser proxy settings and establishes the media connection to the Genesys Engage cloud TURN interface (TCP port 443), but uses SRTP for this TCP connection.
- For the Genesys Softphone in WebRTC mode, the proxy systems must disable authentication processing for signaling traffic.

GENESYS

Access to Genesys Engage cloud via dedicated proxy systems: PAC file for user's browser

You can use dedicated proxy systems for access to Genesys Engage cloud.

To enforce access to Genesys Engage cloud browser-based applications via dedicated corporate proxy systems, you can use a Proxy Auto Config file (PAC file) to direct users' browsers to your dedicated corporate proxy systems.



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 Engage cloud, 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 Engage cloud applications, and other restricted 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 to Genesys Engage cloud via dedicated proxy systems: PAC file configuration example

High-level configuration steps

To enable use of a dedicated proxy for access to Genesys Engage cloud:

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: You can exclude the FQDN of the Genesys Engage cloud TURN interface from the list of destinations served by your proxy. For the voice media of WebRTC phones embedded into Workspace, you can enable direct access from user workstations to the Genesys Engage cloud TURN interface.

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-GenesysEngage.internal.example.com:8080";
            }
            else
           {
                    return "DIRECT";
            }
}
```

In this example,

- The FQDN of the proxy is To- GenesysEngage`.internal.example.com`
- The proxy listens on port 8080.
- The proxy will be used to access URLs constructed of `genesyscloud.com.`

GENESYS

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

Genesys Softphone in WebRTC mode uses HTTPS for signaling (to register with Genesys Engage cloud and to receive calls from Genesys Engage cloud).

High-level configuration steps

To enable Genesys Softphone in WebRTC mode to use dedicated proxy systems to access Genesys Engage cloud:

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-GenesysEngage.internal.example.com:8080
```

In this example:

- The FQDN of the proxy is: To-GenesysEngage.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

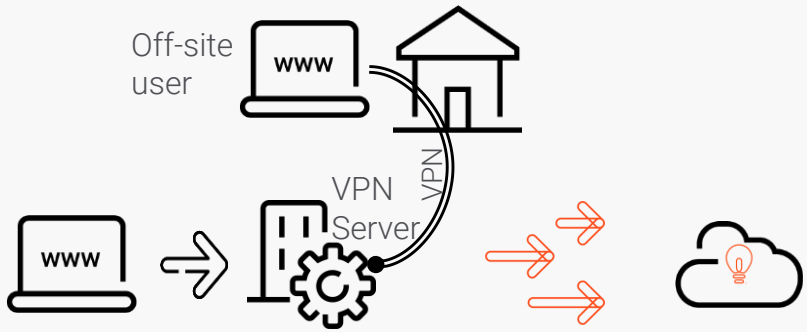
Access to Genesys Engage cloud via VPN to the corporate network

If you allow off-site users to establish a VPN connection to your corporate network, the users can connect to the Genesys Engage cloud applications 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 Engage cloud 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 Engage cloud.



GENESYS

Access to Genesys Engage cloud 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 they browse the public Internet through their local Internet connections.

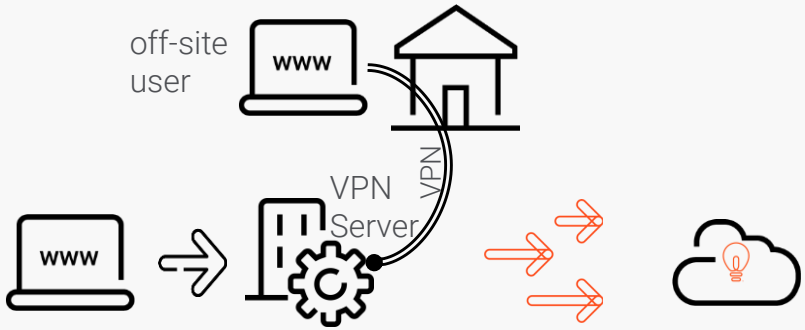
With split tunneling enabled:

- If your off-site users access the Genesys Engage cloud applications via the private network, ensure that the list of destinations accessible via the VPN includes the stable IP addresses of Genesys Engage cloud that are routable on the private network.

  For more information, see here.

- If your on-site users access Genesys Engage cloud via the Internet, allow your off-site and your on-site users to access Genesys Engage cloud applications 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 Engage cloud applications via your corporate proxy. (See here for an example of PAC file configuration.)
  - Your off-site users will connect to Genesys Engage cloud via the Internet, utilizing the known corporate public IP addresses as the source IP addresses.
  - You can exclude the TURN interface from the VPN and enable a direct WebRTC voice stream with the Genesys Engage cloud TURN interface over the Internet.

  For more information, see here.

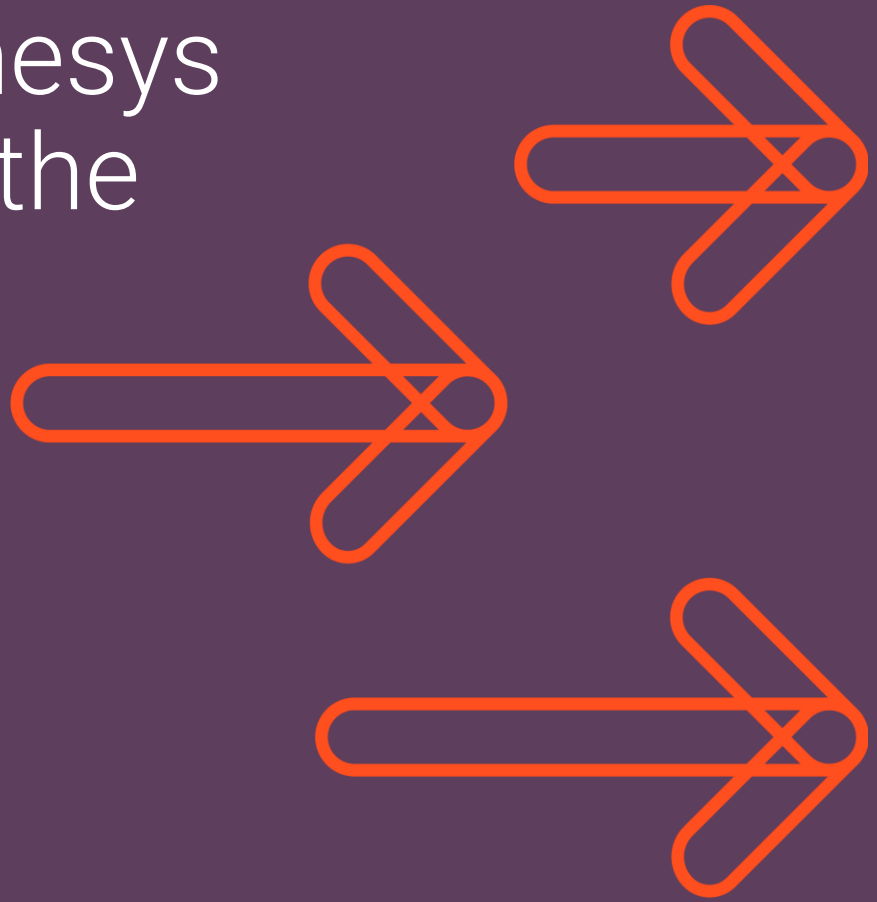


Important: Screen Recording Service (SRS) is not compatible with split tunneling for access to Genesys Engage cloud over the Internet.

GENESYS

User access to Genesys Engage cloud over the Internet

- Dynamic Genesys Engage cloud IP addresses on the Internet
- Firewall permissions
- Split tunneling for off-site users
- IP-based access restrictions and open Internet access



GENESYS™

Access to Genesys Engage cloud over the Internet

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

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

To enable user access to Genesys Engage cloud over the Internet, you must consider:

- Protocols and communication ports (more information here)
- Your proxy configuration (more information here)
- Your firewall configuration (more information here)
- Genesys Engage 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 that enables off-site work. The technique allows your off-site users to access Genesys Engage cloud via your corporate systems. As described here and here, to use split tunneling you must:
  - Use a PAC file for the browser-based Genesys Engage cloud applications accessible via the Internet to direct the browsers to the corporate web proxy.
  - Use the stable IP addresses of the Genesys Engage cloud TURN interfaces for WebRTC media traffic.

GENESYS

Accessing Genesys Engage cloud applications over the Internet: Dynamic IP addresses

- Genesys Engage cloud applications 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 Genesys Engage cloud applications.

  Exception: Genesys Engage cloud TURN interfaces for WebRTC media traffic maintain stable IP addresses for WebRTC phones.

- Do not use IP address-based permissions on your firewall to control access to Genesys Engage cloud via the Internet.

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

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

- Notes:
  - The Genesys Softphone in WebRTC mode does not support use of a proxy for media traffic. The Genesys Softphone communicates directly with the IP addresses obtained as a result of name resolution for the Genesys Engage cloud TURN interfaces.
  - If you use a PAC file to specify browser proxy settings, you can exclude the FQDN of the Genesys Engage cloud TURN interface from the list of destinations served by your proxy, thus enabling direct access from user workstations to this TURN interface for the voice media of the WebRTC phone embedded into Workspace.
  - You can exclude the TURN interface from the list of destination IP addresses handled by your VPN tunnel ("*split-include*" tunnel configuration) and enable a direct WebRTC voice stream with the Genesys Engage cloud TURN interface over the Internet.

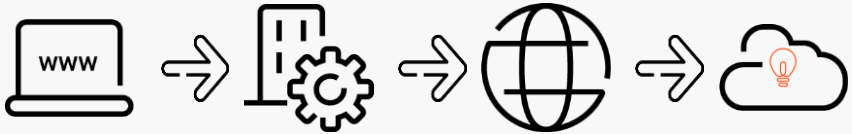
GENESYS

User access to Genesys Engage cloud over the Internet via firewall (1)

- If access to Genesys Engage cloud relies on your proxy systems, configure the firewall that controls proxy access to the Internet to allow the proxy systems to send requests to TCP port 443 (and 80) 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 Engage cloud TURN interfaces (TCP port 443). This is required because the media traffic of the WebRTC phone embedded into Workspace utilizes SRTP.

  Note: You can exclude the FQDN of the Genesys Engage cloud 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 (and 80) at any destination on the Internet.



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

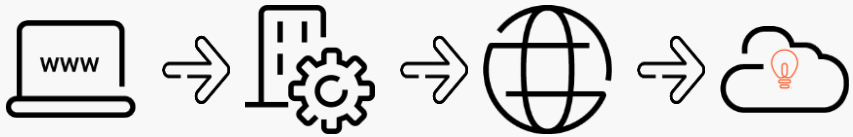
GENESYS

User access to Genesys Engage cloud over the Internet via firewall (2)

- If agents use Genesys Softphone in WebRTC mode, configure the firewall to allow outbound access on TCP port 443 for SRTP to the Genesys Engage cloud TURN interfaces. This is required for WebRTC phones to establish a voice media connection to the Genesys Engage cloud TURN interface.

  Disable HTTPS deep packet inspection for media communications with the stable IP addresses of the Genesys Engage cloud TURN interfaces (TCP port 443). This is required because the media traffic of the Genesys Softphone in WebRTC mode utilizes SRTP.
- If agents use a WebRTC phone embedded into Workspace and you exclude the FQDN of the Genesys Engage cloud 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 Engage cloud TURN interfaces. This is required for WebRTC phones to establish a voice media connection to the Genesys Engage cloud TURN interface.

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



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

GENESYS

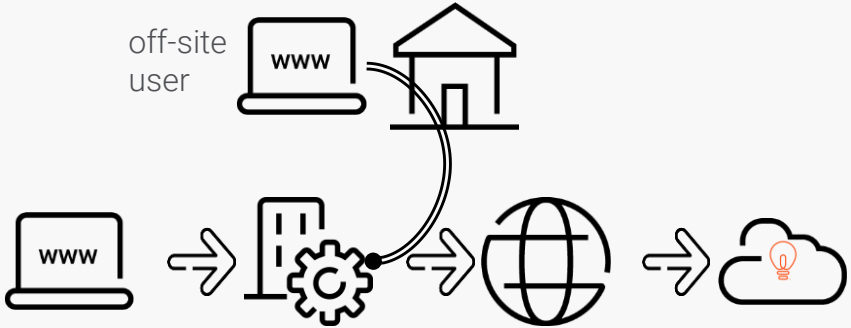
Allowing user access to Genesys Engage cloud over the Internet: VPN split tunneling

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 ("*split-include*" tunnel configuration).
2. In the list of destination IP addresses handled by your VPN tunnel, include the stable IP addresses of the Genesys Engage cloud TURN interfaces for the WebRTC media traffic of WebRTC phones.

   Note: You can exclude the TURN interface from the VPN and enable a direct WebRTC voice stream with the Genesys Engage cloud 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 Engage cloud 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.



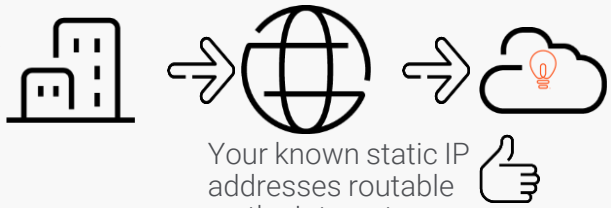
Important: Screen Recording Service (SRS) is not compatible with split tunneling for access to Genesys Engage cloud over the Internet.

GENESYS

Access to Genesys Engage cloud over the Internet: Access policy at Genesys Engage 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 Engage cloud applications 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 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).
- The Genesys Engage cloud TURN interfaces always accept connections for WebRTC media communications from the entire Internet. You cannot restrict access to the TURN interfaces on the Genesys Engage cloud side.

To request access to the Genesys Engage cloud applications 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 Engage cloud applications over the Internet).

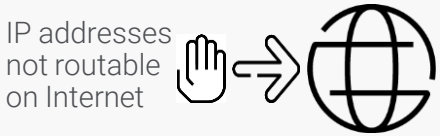
  Genesys expects that the IP addresses are allocated to your company by an IP Registry or your Internet Service Provider, or that they belong to the Vendor of your cloud-based Proxy or VDI service.
- Do not request enabling access for IP addresses that internet providers assign to your off-site workers’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

GENESYS

Access to Genesys Engage cloud 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 Engage cloud from these IP addresses will never reach the Genesys Engage cloud applications, because Internet Service Providers will reject them.

- 0.0.0.0/8 RFC 5735 RFC 6890: Current Network IP Address Block
- 10.0.0.0/8 RFC 5735, RFC 1918: Private IP Address Block
- 100.64.0.0/10 RFC 6598: Shared IP Address Block for communications between a service provider and its subscribers when using a carrier-grade NAT
- 127.0.0.0/8 RFC 5735, RFC 1122: Loopback IP Address Block
- 169.254.0.0/16 RFC 5735, RFC 3927: Link-local IP Address Block
- 172.16.0.0/12 RFC 5735, RFC 1918: Private IP Address Block
- 192.0.0.0/24 RFC 5735, RFC 5736: Private IP Address Block
- 192.0.2.0/24 RFC 5735, RFC 5737: Documentation IP Address Block
- 192.88.99.0/24 RFC 5735, RFC 3068: 6to4 relay anycast IP Address Block
- 192.168.0.0/16 RFC 5735, RFC 1918: Private IP Address Block
- 198.18.0.0/15 RFC 5735, RFC 2544: Benchmark tests IP Address Block
- 198.51.100.0/24 RFC 5735, RFC 5737: Documentation IP Address Block
- 203.0.113.0/24 RFC 5735, RFC 5737: Documentation IP Address Block
- 224.0.0.0/4 RFC 5735, RFC 3171: IPv4 Multicast Assignments IP Address Block
- 240.0.0.0/4 RFC 5735, RFC 1112: Reserved for future use IP Address Block



GENESYS

Access to Genesys Engage cloud over the Internet: Open Internet access and IP-based control

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

Note: You can apply access restrictions at the Authentication step.

Genesys Authentication Service IP-based access control allows you to govern the Genesys Engage cloud 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, Genesys Engage cloud meets access restriction requirements for some customers, while open Internet access to the applications is enabled for other customers. These other customers might require open Internet access because their off-site users require direct access to Genesys Engage cloud.

(Support pending – expected in 2020) To restrict access to the applications that have open Internet access enabled:

- Maintain a list of your known IP addresses and/or supply the IP addresses to whoever manages configuration of your organization's contact center within Genesys Engage cloud.
- Use the Agent Setup User Interface to configure the IP list and to enable the IP-based control feature.

GENESYS

Access to Genesys Engage cloud over the Internet: Dual control

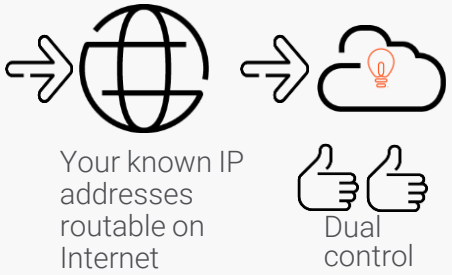
The majority of the Genesys Engage cloud applications rely on the Genesys Authentication Service. If you enable IP-based control, access to all such applications is restricted by the applied IP access-list.

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

Some of the applications 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.)
- (Support pending – expected in 2020) You restrict access to the User Interfaces by means of IP-based control in Agent Setup.

Keep the two IP address lists aligned to allow your users to access these Genesys Engage cloud applications.



User access to Genesys Engage cloud over a private network

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

GENESYS™

Access to Genesys Engage cloud 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 Engage cloud.

- Agent's browser connects to the Desktop and other Genesys Engage cloud applications.
- Agent's SIP phone registers with Genesys Engage cloud, from which it then receives calls.
- Agent's Screen Recording Service uploads screen recordings to Genesys Engage cloud.
- Administrator's browser connects to the Genesys Engage cloud applications.

To enable user access to Genesys Engage cloud 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 Engage cloud access policy and IP-based access restrictions (more information 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 Engage cloud via your corporate systems. As described here, to use split tunneling:
  - **Exception:** Use the PAC file for the browser-based applications accessible via the Internet and direct the browsers to the corporate web proxy. (As described under Transport network limitations, there are Genesys Engage cloud applications that support access only via the Internet.)
  - Use the stable IP addresses of the Genesys Engage cloud applications accessible via the private network (more information here).
  - Use the stable IP addresses of the Genesys Engage cloud SIP and media traffic.

GENESYS

Accessing Genesys Engage cloud applications over a private network: Stable IP addresses

- The Genesys Engage cloud applications are addressed by means of URLs, for example: `https://best-customer.genesyscloud.com`

  Exception: SIP Phones SIP-registering with Genesys Engage cloud over a private network use SIP for signaling traffic and RTP/RTCP for media traffic.

- IP addresses for the Genesys Engage cloud applications are stable and routable on the private network.

  Note: There are Genesys Engage cloud applications that support access only via the Internet, as described under Transport network limitations.

- **Important:** You must *not* expose to the Internet the Genesys Engage cloud interfaces accessible via the private network.

  You must not use NAT, reverse proxy, SBC, or any other techniques to enable access to the Genesys Engage cloud private interfaces over the Internet via your systems exposed to the Internet.

- You can use IP address-based permissions on your firewall to control access to Genesys Engage cloud via the private network.
  - The SIP expire timer on Genesys Engage cloud 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 Genesys Engage cloud to reach the SIP phones before the SIP registration expires.
  - The UDP session for voice media is always originated by the SIP phone. Genesys Engage cloud initiates RTP traffic towards the SIP phone after receiving RTP traffic from the phone. Genesys Engage cloud sends RTP packets to the IP address and port that the SIP phone used while initiating the voice media UDP session.

GENESYS

User access to Genesys Engage cloud over a private network via firewall (1)

- If access to Genesys Engage cloud 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 (and 80) at the Genesys Engage cloud IP ranges on the private network.

  Note: There are Genesys Engage cloud applications that support access only via the Internet, as described under Transport network limitations. For information about firewall configuration for access over the Internet, see here.

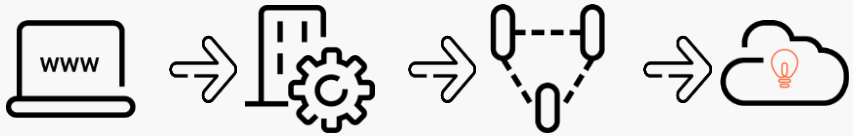
- If you do not use proxy systems, configure the on-site firewall to allow the browsers and the standalone software to send requests to TCP port 443 (and 80) at the Genesys Engage cloud IP ranges on the private network.

Firewall to allow access to the Genesys Engage cloud IP addresses

GENESYS

User access to Genesys Engage cloud over a private network via firewall (2)

- If agents use SIP Phones SIP-registering with Genesys Engage cloud, configure the on-site firewall to allow the phone to originate SIP signaling and voice media traffic (RTP/RTCP) towards Genesys Engage cloud.
  - If your firewall performs NAT/PAT, estimate the number of simultaneous UDP sessions traversing the firewall and allocate a sufficient number of the 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 Engage cloud 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 Genesys Engage cloud (140 seconds). See more information here.
    - See also the information about voice media UDP sessions and RTP streams here.



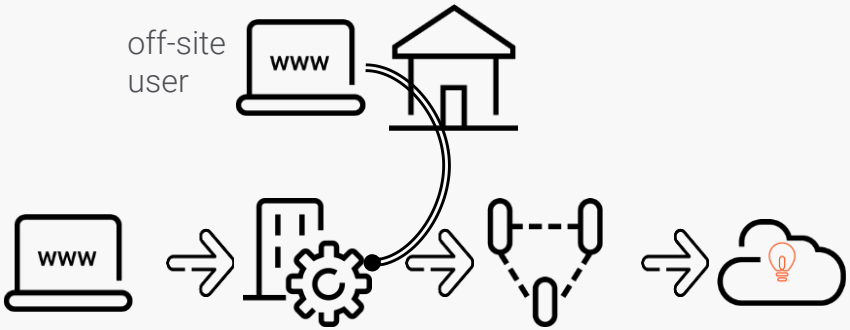
Firewall to allow access to Genesys Engage cloud IP addresses

GENESYS

Allowing user access to Genesys Engage cloud 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 Engage cloud applications routable on the private network ("*split-include*" tunnel configuration).
2. If you use a PAC file for access to Genesys Engage cloud :
    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 Engage cloud via your corporate proxy systems.
    3. Configure the off-site user's browser to use the PAC file to locate a proxy.



Note: There are Genesys Engage cloud applications that support access only via the Internet, as described under Transport network limitations. For information about split tunneling configuration for access over the Internet, see here.

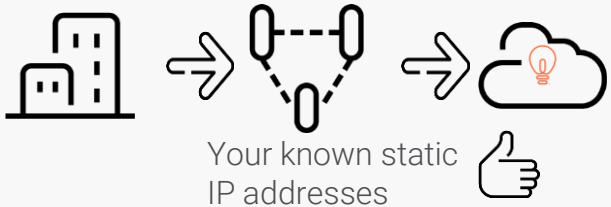
See also general information about VPN and split tunneling here and here.

GENESYS

Access to Genesys Engage cloud over a private network: Access policy at Genesys Engage 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 Engage cloud applications 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.

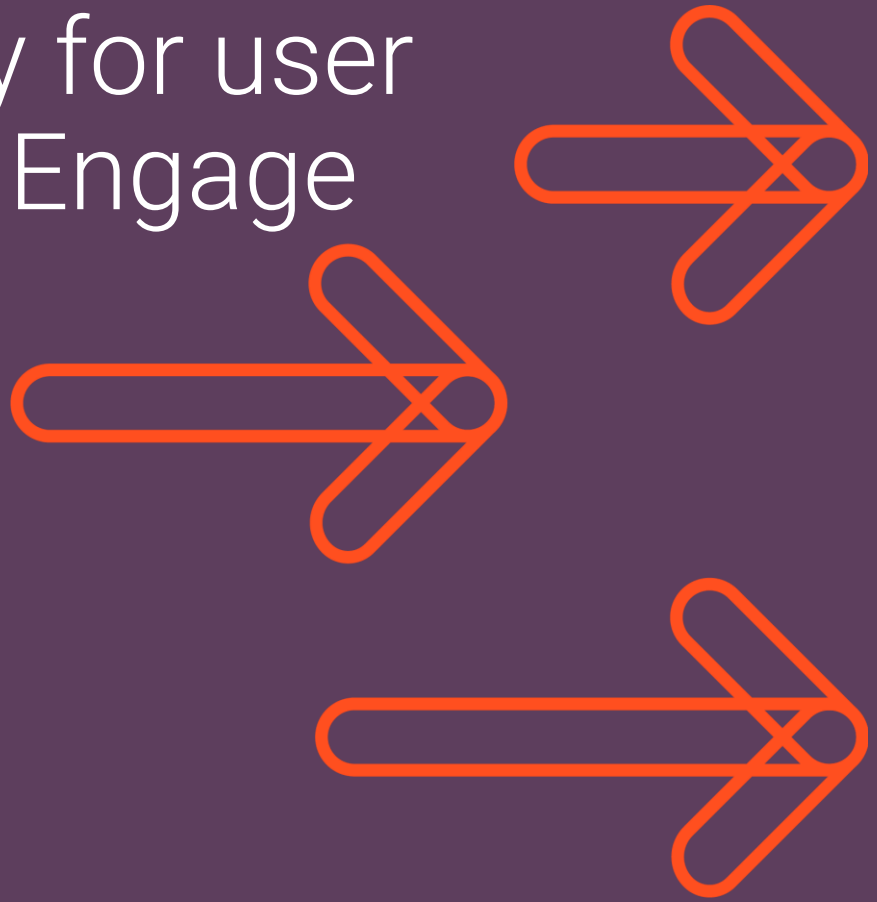
To request access to the Genesys Engage cloud applications from your new IP network, submit a request to Genesys Customer Care.

- Ensure that your corporate network team enabled IP routing between the Genesys Engage cloud 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 Engage cloud.

GENESYS

Business Continuity for user access to Genesys Engage cloud



- About Business Continuity
- Agent phones
- Genesys Engage cloud applications

GENESYS

Genesys Engage cloud and Business Continuity of your organization

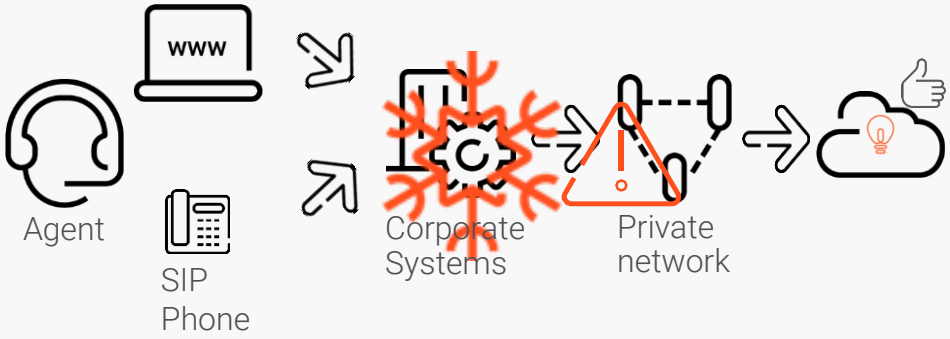
A disaster can occur at any time.

The Genesys Engage cloud 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 Engage 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 Engage 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 Engage cloud and Business Continuity of your organization (2)

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

For example, a natural disaster might:

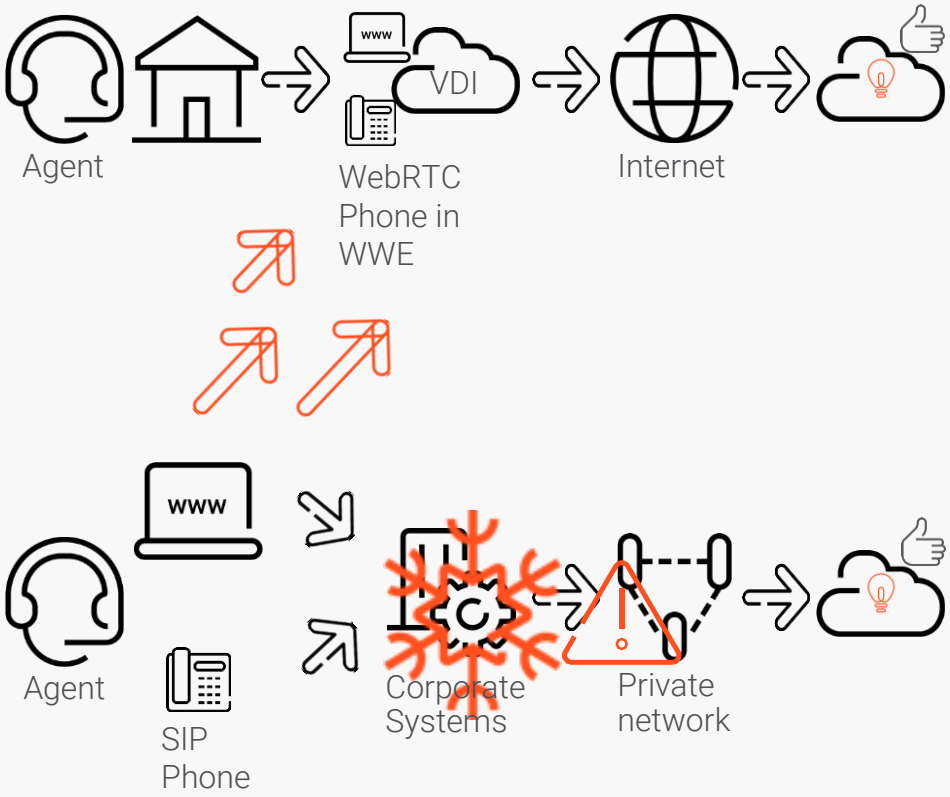
- Disrupt communications between Genesys Engage cloud and agent phones that depend on the corporate systems

  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 customer traffic.
- Impact your agents' ability to navigate to the Genesys Engage cloud web-based applications via corporate systems and networks
- Cause a power outage in the corporate data center
- Prevent your agents from working on-site

GENESYS

Genesys Engage cloud 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 Engage cloud 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 Genesys Engage cloud 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 Engage cloud setup you can preserve and what you might need to change.

GENESYS

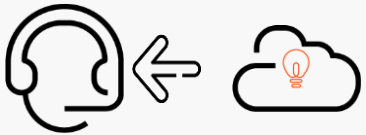
Genesys Engage cloud and Business Continuity: Agent phones

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

- If your agents can use preprovisioned PSTN phones, Genesys Engage cloud will deliver calls to the agents' phones.
- If your agents can use preprovisioned phones that depend on your corporate telephony, Genesys Engage cloud will invite the phones into conversations via SIP Trunks with the corporate systems over a private network. 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 Engage 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 Engage cloud directly over the Internet.
- If an agent cannot use a preprovisioned phone, additional considerations and provisioning within Genesys Engage 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 Engage cloud and Business Continuity: Access to applications

In an emergency situation, agents can use browser-based applications as follows:

- A number of the Genesys Engage cloud applications can be accessible from anywhere on the Internet if your contact center on Genesys Engage cloud 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 Agent Setup are examples of Genesys Engage cloud applications that are conditionally accessible to anywhere on the Internet.
- For the Genesys Engage cloud applications where IP restrictions apply, your agents must connect to Genesys Engage 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