



GENESYS CLOUD REQUIREMENTS SUMMARY

CVT (Global) Pty Ltd
July 2025

1 CONTENTS

2	Genesys Cloud Requirements	2
2.1	Supported PC and Mac Operating Systems	2
2.2	Supported web browsers	2
2.2.1	Disable your browser's sleep mode setting	2
2.3	Network bandwidth.....	2
3	Telephony – User Settings	4
3.1	Call Waiting and Call Forwarding.....	4
3.2	Handsets and Headset.....	4
3.3	About WebRTC	4
4	Ports and services for WebRTC	5
4.1	Detailed WebRTC diagram.....	6
5	Ports and Services for Genesys Cloud.....	7
5.1	Ports.....	7
5.2	IP addresses for the firewall allow list.....	8
5.3	Domains.....	9
5.4	Force TURN Configuration (Optional).....	10
5.5	Test Tools.....	11
6	Screen Recording Requirements (Optional)	12
6.1	Requires WebRTC	12
6.2	Supported PC and Mac Desktop Client.....	12
6.3	Desktop Client Deployment.....	12
6.4	Record the agent's monitors	13
6.5	Network bandwidth.....	13

2 GENESYS CLOUD REQUIREMENTS

The system requirements detail the browsers, operating systems, hardware, and other components supported by Genesys Cloud.

<https://help.mypurecloud.com/articles/genesys-cloud-requirements/>

2.1 SUPPORTED PC AND MAC OPERATING SYSTEMS

- Mac OS — two versions previous to the current release
- Windows 11

2.2 SUPPORTED WEB BROWSERS

Full support: <https://help.mypurecloud.com/articles/browser-check/>

- Microsoft Edge Chromium — Requires current release.
- Chrome — Requires current major release or one version previous.
 - Chrome major releases occur monthly.
- Firefox — Requires current release, one version previous, current ESR release, or transitional ESR release
 - Firefox scripts may not load unless AdBlocker or AdBlockPlus are disabled.
- JavaScript must be enabled.

2.2.1 Disable your browser's sleep mode setting

When using Genesys Cloud in a browser with multiple tabs open, you may experience connection issues when Genesys Cloud isn't the active tab. To prevent this from happening, you might want to consider disabling your browser's sleep mode setting. For more information, see [Disable your browser's sleep mode setting](#).

2.3 NETWORK BANDWIDTH

It is recommended the Local Area Network is at least 100 Mbit/s switched to the Agent desktop. We recommend the following bandwidth for each quality setting:

- High Definition (HD): 1mbps – 2mbps per connected user in the video chat
- Medium Definition: 500kbps – 1mbps per connected user in the video chat
- Low Definition: 100kbps – 500kbps per connected user in the video chat
- Voice only (camera off): 32kbps – 150kbps per connected user in the video chat

If current internet connection is often saturated by other applications, customer should consider bandwidth requirements.

If you plan to use WebRTC, it is recommended that you have sufficient network bandwidth to support your maximum concurrent calls and implement QoS.

The bi-directional bandwidth required per call is **40 to 132kbps** based on an adaptive voice codec.

For contact centre calls, it is recommended to allocate bandwidth at the higher end of the spectrum to ensure best possible audio quality.

Notes:

- Genesys recommends against multiple simultaneous logins to the same Genesys Cloud account. For example, the same account logged in to multiple tabs or browsers, the same account logged in to the desktop app and in a browser, or the same account logged in to different computers at the same time. For more information, see the FAQ [Why do multiple concurrent Genesys Cloud logins cause problems?](#)
- Genesys recommends that PCs exceed the minimum system requirements when WebRTC voice, video, or third-party resource-intensive software is used. For example, third-party applications can be more resource-intensive than Genesys Cloud. Since the type and number of additional applications in any machine is different, Genesys cannot provide specific guidance. The best approach is experimentation with the desired agent configuration to ensure that the machine has enough CPU, memory, and networking to support all applications comfortably.
- Genesys recommends that each Genesys Cloud-enabled device or computer includes antimalware protection. For more information, see [Malware and antispyware protection best practices](#).
- Some antivirus software runs real-time inspection on HTTPS and audio packets, and may lower the audio quality of WebRTC.
- For Genesys Cloud embedded clients, the minimum system requirements are based on the host or browser running the client, and vary based on the implementation. For more information, see [Browser requirements for the Genesys Cloud embedded clients](#).
- Genesys recommends that PCs exceed the minimum system requirements when screen recording is enabled for a desktop with multiple monitors, to successfully handle recording multiple concurrent digital interactions. For more information, see [Multi-monitor screen recording](#).

3 TELEPHONY – USER SETTINGS

3.1 CALL WAITING AND CALL FORWARDING

Call Waiting and all call forwarding should be deactivated on phones used by Genesys Cloud users as these features can interfere with call delivery.

3.2 HANDSETS AND HEADSET

The following are highly recommended for all Genesys Cloud users who will use the system to receive or make calls. The telephony endpoints they use when connecting to the Genesys Cloud system should have:

- An industry standard and approved headset,
- No third-party voicemail active,
- No call-diversion features active,
- No multi-line configuration

While Genesys Cloud will work with most handsets and wireless headsets, it is a requirement that you perform suitable testing of your telephony infrastructure and Genesys Cloud.

3.3 ABOUT WEBRTC

Genesys Cloud supports WebRTC technology with the Genesys Cloud WebRTC phone. The Genesys Cloud WebRTC phone runs right from your browser so once you enable the Genesys Cloud WebRTC phone, you can immediately use it to make and receive calls.

<https://help.mypurecloud.com/articles/about-genesys-cloud-webrtc-phones/>

If you are planning on utilising the WebRTC (softphone) option, it is important to note the specific requirements as outlined in <https://help.mypurecloud.com/articles/genesys-cloud-ports-services/>

4 PORTS AND SERVICES FOR WEBRTC

Please refer to the following site for current and full details:

<https://help.mypurecloud.com/articles/ports-and-services-for-webrtc/>

Genesys Cloud WebRTC has specific ports and services configurations to consider before you configure a firewall in various network scenarios. The diagrams presented here show how to configure the ports and services for asymmetric NAT scenario:

Client inside firewall - Asymmetric NAT

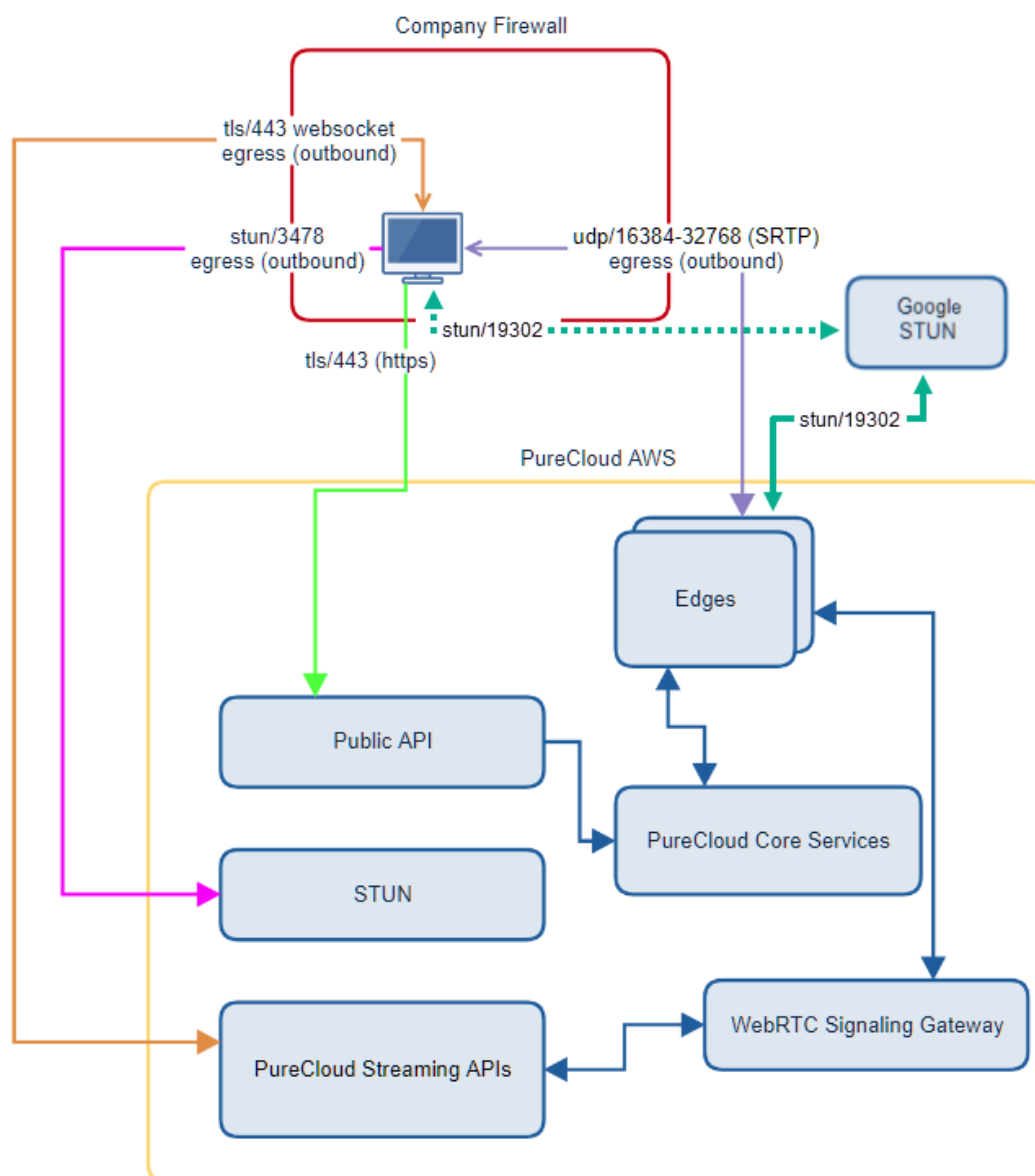
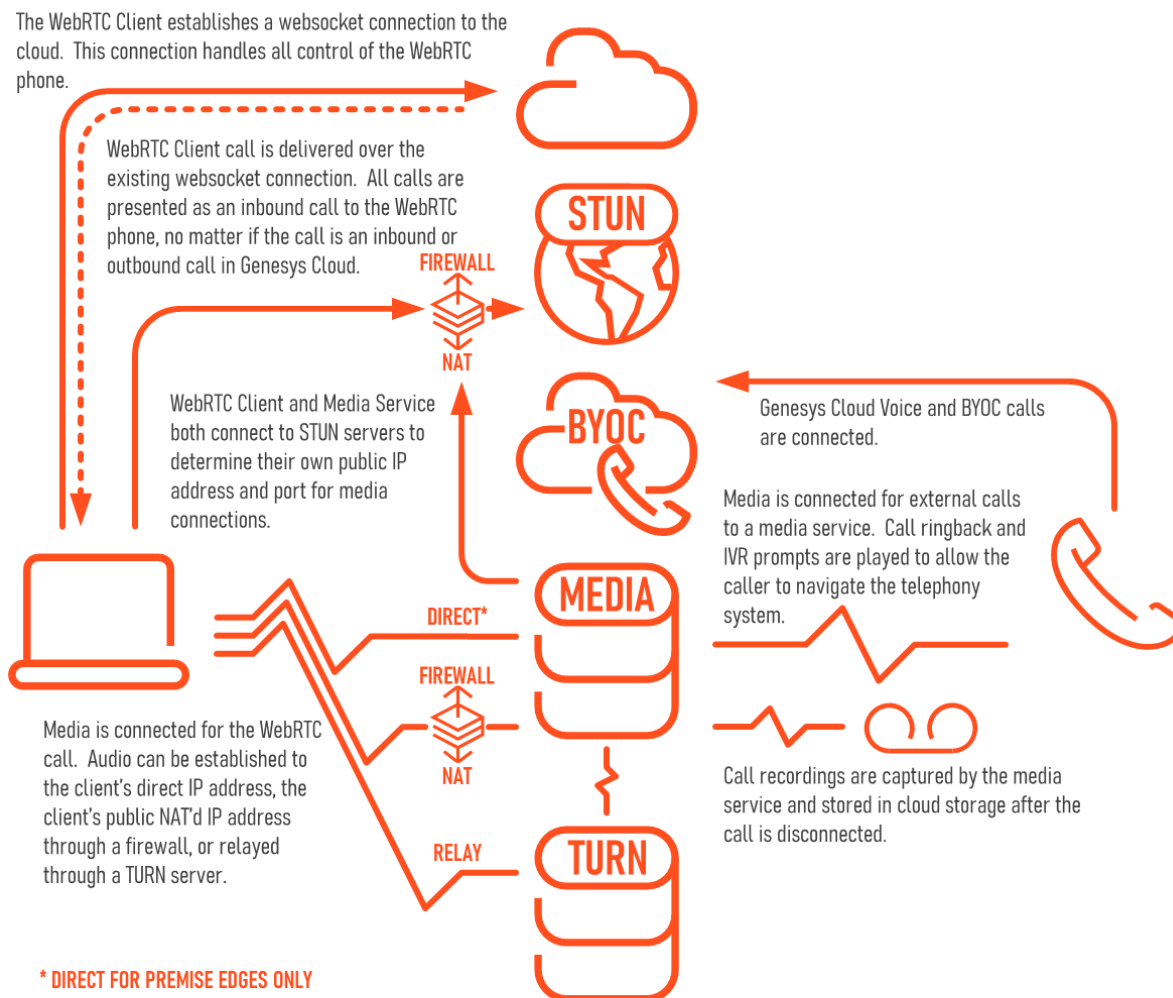


Figure 1 Client inside firewall - Asymmetric NAT

When an agent using a WebRTC phone handles a call from a Genesys Cloud Voice or BYOC trunk, the client discovers all available media paths and then determines the best path between the client and

the media service (or Edge for BYOC premises deployments). The following diagram illustrates this process. <https://help.mypurecloud.com/articles/webrtc-call-flow/>



WebRTC Call Flow
 Figure 2 WebRTC call flow

GENESYS

4.1 DETAILED WEBRTC DIAGRAM

Please refer to following site for a detailed diagram of WebRTC network flow.

<https://help.mypurecloud.com/articles/detailed-webrtc-diagram/>

5 PORTS AND SERVICES FOR GENESYS CLOUD

Please refer to the following site for current and full details:

<https://help.mypurecloud.com/articles/ip-addresses-for-the-firewall-allowlist/>

Within the below tables, you will find detailed information on the ports and services that you will need to configure on your company firewall based on your product/source(client).

For WebRTC connections, you can access the Genesys Cloud WebRTC Diagnostics app and run the automated tests found on the Network Test tab here: <https://help.mypurecloud.com/articles/run-the-standalone-genesys-cloud-webrtc-diagnostics-app/>

5.1 PORTS

Source	Destination	Port	Type	Remarks
Agent PC	Genesys Cloud Amazon AWS (CloudFront, S3, and others)	80, 443	TCP (HTTP/S)	The secure connection from your client (desktop, web, mobile) to the Genesys Cloud Services on the public Internet.
Agent PC	52.129.96.0/20 169.150.104.0/21 167.234.48.0/20 136.245.64.0/18	443	TCP	Controls plane signalling between the WebRTC Client and cloud-based XMPP Gateway. Used in both cloud media and premises Edge deployments.
Agent PC	52.129.96.0/20 169.150.104.0/21 167.234.48.0/20 136.245.64.0/18	16384 - 65535	UDP (SRTP)	The transmission of secured streaming media (audio).
Agent PC	52.129.96.0/20 169.150.104.0/21 167.234.48.0/20 136.245.64.0/18	3478, 19302	UDP/TCP (STUN)	Identifies the public IP address of the WebRTC Client.

<https://help.mypurecloud.com/articles/cidr-ip-address-range-expansion-for-cloud-media-services-in-new-regions/>

5.2 IP ADDRESSES FOR THE FIREWALL ALLOW LIST

Genesys Cloud is deployed in a public cloud environment where IP addresses are expected to change. The IP addresses used by Genesys Cloud are provided by our vendor from their public IP pool, which contains many IP addresses used by many other organizations. All client connections (including BYOC Premises Edges, WebRTC Clients, and hard phones for BYOC Cloud and PCV customers) to Genesys Cloud are initiated as outbound connections to Genesys Cloud services. When network access restrictions are used, such as a firewall, Genesys Cloud recommends allowing client outbound access on the specified ports to any IP destination.

Owner	Services	IP addresses	Description
Amazon AWS	Genesys Cloud Amazon AWS (CloudFront, S3, and others)	See the Amazon AWS IP address JSON file.	Amazon AWS utilizes a large set of IP address ranges.
Genesys Cloud Media	- WebRTC stations - Polycom stations with Genesys Cloud Voice or BYOC Cloud. - ACD screen recording - Video chat	52.129.96.0/20 169.150.104.0/21 167.234.48.0/20 136.245.64.0/18	Genesys-owned /20 CIDR IP address range for public facing media services. Genesys Cloud uses the CIDR IP address range in the majority supported regions. For more information, see Cloud media services CIDR IP address range.

Genesys Cloud's cloud media services CIDR block provides a smaller range of IP addresses for outbound connections to and from telephony endpoints.

Please also refer the link below for updates –

<https://help.mypurecloud.com/articles/cidr-ip-address-range-for-cloud-media-services/>

Owner	Domain	CIDR IP range
Genesys Cloud	netdiag.apse2.pure.cloud	52.129.96.0/20 169.150.104.0/21 167.234.48.0/20 136.245.64.0/18

5.3 DOMAINS

Owner	Domain	Region	Description
Genesys Cloud	*.mypurecloud.com.au	Australia & New Zealand	Provides the Genesys Cloud interface for users and admins; domains are region-specific and each Genesys Cloud organization exists within only one region. Entities with multiple organizations may be deployed in various regions.
	*.apse2.pure.cloud		
Amazon AWS[†]	*.cloudfront.net	All	Provides static content for Genesys Cloud user interface.
	*.s3.amazonaws.com	All	Provides S3 download links.
	*.s3-ap-southeast-2.amazonaws.com		
	*.s3.ap-southeast-2.amazonaws.com		
Google (optional)[†]	*.googleapis.com	All	Provides cascading style sheet (CSS) and font information.
	*.gstatic.com	All	Provides static content, mainly images.
	*.google-analytics.com	All	Provides Google analytics.
	stun.l.google.com stun1.l.google.com stun2.l.google.com stun3.l.google.com stun4.l.google.com	All	Provides STUN services for Edge devices, VoIP phones, WebRTC softphones, and Collaborate multimedia.

5.4 FORCE TURN CONFIGURATION (OPTIONAL)

The Force TURN feature is designed to reduce the number of IP addresses you have to allow on the open outbound ports needed for Genesys Cloud's WebRTC client implementation.

<https://help.mypurecloud.com/articles/use-the-force-turn-feature/>

Note: You still need to have the full supported port range (udp/16384 - 65535) open on your firewall. You limit access by adding the dedicated IP addresses for your region or satellite region to your firewall's allowlist. In addition, you'll need to add Genesys Cloud's cloud media services /20 CIDR block of IP addresses to your existing firewall allowlist.

After you enable the Force TURN feature, you must add the dedicated IP addresses in the Asia Pacific (Sydney) / ap-southeast-2 region, listed here: <https://help.mypurecloud.com/articles/use-the-force-turn-feature/>

In summary, the required ports and services are:

Source	Destination	Port	Type	Remarks
Agent PC	Genesys Cloud Amazon AWS (CloudFront, S3, and others)	80, 443	TCP (HTTP/S)	The secure connection from your client (desktop, web, mobile) to the Genesys Cloud Services on the public Internet.
Agent PC	52.129.96.0/20 169.150.104.0/21 167.234.48.0/20 136.245.64.0/18	443	TCP	Controls plane signaling between the WebRTC Client and cloud-based XMPP Gateway. Used in both cloud media and premises Edge deployments.
Agent PC	52.129.96.0/20 169.150.104.0/21 167.234.48.0/20 136.245.64.0/18	16384 - 65535	UDP (SRTP)	The transmission of secured streaming media (audio).
Agent PC	52.129.96.0/20 169.150.104.0/21 167.234.48.0/20 136.245.64.0/18	3478, 19302	UDP/TCP (STUN)	Identifies the public IP address of the WebRTC Client.

5.5 TEST TOOLS

- Network Readiness Assessment: <https://help.mypurecloud.com/articles/run-the-genesys-cloud-network-readiness-assessment/>
<https://help.mypurecloud.com/articles/cidr-ip-address-range-for-cloud-media-services/>
- Network Assessment download:
http://australia.pna.inindca.com:8080/myspeed/purecloud_presales_version_1.html
- Generic WebRTC test: <https://test.webrtc.org/>
- Genesys Cloud WebRTC test: <https://apps.mypurecloud.com.au/webrtc-troubleshooter/>
 - WebRTC with Audio
 - Network Test

6 SCREEN RECORDING REQUIREMENTS (OPTIONAL)

The screen recording requirements detail the operating systems, hardware, and other components supported by Genesys Cloud.

<https://help.mypurecloud.com/articles/screen-recording-overview/>

6.1 REQUIRES WEBRTC

Screen recording uses WebRTC so associated setup outlined in this document required.

6.2 SUPPORTED PC AND MAC DESKTOP CLIENT

- Latest version of Genesys Cloud Desktop app should be in use
- For screen recording with Mac we recommend MacOS 10.13: High Sierra or later. If you use Catalina, then you need to set the OS permission for the desktop app to allow screen recording. For more information about setting this permission, see <https://support.apple.com/guide/mac-help/control-access-to-screen-recording-on-mac-mchld6aa7d23/mac>
- Genesys Cloud does not support screen recording while an agent is logged in to the same Genesys Cloud account on more than one desktop app. Genesys Cloud records both screens but only retains one of the recordings. You cannot select which recording to retain.
- Screen recording is only available for the Genesys Cloud desktop apps during ACD interactions. If agents use the web app or take a non-ACD interaction, Genesys Cloud does not record their screens.

6.3 DESKTOP CLIENT DEPLOYMENT

Genesys Cloud Desktop Client is required for screen recording.

<https://help.mypurecloud.com/articles/desktop-app/>

If the organization's security policies require it, the administrator can prevent users from installing and updating the desktop app. Instead, the administrator can push out the desktop app install and updates to users on specified days and times using a third-party software deployment tool.

<https://help.mypurecloud.com/articles/deploy-the-desktop-app-admin/>

Note: it is important to keep the desktop client up to date for any new features and functions.

6.4 RECORD THE AGENT'S MONITORS

Genesys Cloud records the entire desktop of the agent's monitor or monitors. For more information, see <https://help.mypurecloud.com/articles/multi-monitor-screen-recording/>

- Genesys Cloud can record up to 4 monitors during an ACD interaction.
- Genesys Cloud records each monitor as an individual recording and preserves the monitor orientation.
- Recording of more than a single monitor counts as only one session toward the concurrent session limit. There is a maximum of 2000 sessions.
- Frame rate: 3 frames per second.
- Screen recordings have a maximum length of 9 hours.
- Genesys Cloud pauses screen recording during secure pause but resumes recording the screen when the secure pause ends. Train agents to hide sensitive information on their screens before they end a secure pause.
- Screen recordings can be kept for a maximum of 365 days.

6.5 NETWORK BANDWIDTH

A single screen recording typically requires 150-250 kbps. Screen resolution and the amount of on-screen movement affect the amount of bandwidth required.

Each additional monitor may multiply the amount of bandwidth required. For example, 4 monitors could require 4 times as much bandwidth.

Maximum number of screen recording sessions should be configured to limit max bandwidth
<https://help.mypurecloud.com/articles/recording-management/>