SIP Interoperability Specification

Genesys Cloud

Version 2.4

GENESYS

Name	Modification	Document Version	Date
Ben Newlin	Document Creation	1.0	8/9/2017
Ben Newlin	Added Record-Route information	1.1	2/9/2018
Ben Newlin	Added Response Codes for Unsupported and Unrecognized Methods	1.2	2/23/2018
Ben Newlin	Added statement of RFC 3261 compliance. Added 4XX Client response section.	1.3	1/8/2019
Ben Newlin	Clarified IP addressing sections for media and signaling	1.4	3/19/2019
Ben Newlin	Added TCP documentation	1.5	4/16/2019
Ben Newlin	Removed incorrect section 3.8.4 Replaces and Referred-By Headers	1.6	11/11/2020
Ben Newlin	Rebranding to Genesys Cloud	2.0	11/11/2020

Name	Modification	Document Version	Date
Ben Newlin	Adding media CIDR ranges	2.1	05/04/2022
Ben Newlin	Clarify INFO support	2.2	11/15/2023
Ben Newlin	Fix incorrect section reference	2.3	06/05/2024
Ben Newlin	Clarify 408 response behavior. Add TCP/TLS fragmentation limits	2.4	09/30/2025

Table of contents

1 Summary

This document describes the requirements for Carrier SIP trunk connections to Genesys Cloud. This includes the Genesys Cloud Voice and Genesys Cloud Bring Your Own Carrier – Cloud (BYOC-C) products. It does not include Genesys Cloud Bring Your Own Carrier - Premises (BYOC-P). Requirements for BYOC-P as well as phones or any other external devices are detailed on the Genesys Cloud Resource Center. All further references to Genesys Cloud in this document refer to both the Genesys Cloud Voice and BYOC-C product offerings, except where one offering is named explicitly.

2 SIP Signaling

This section describes the requirements for SIP signaling on the external trunk.

2.1 Protocol

Genesys Cloud supports SIP as defined in RFC 3261. All interconnected Carriers must be SIP-compliant to this specification. Genesys Cloud is not responsible for any changes in our system which cause non-compliant devices to lose interoperability.

2.2 Connectivity

Genesys Cloud is a public internet service that is deployed in the Amazon Web Services (AWS) cloud. At this time, Genesys Cloud cannot support any physical connections into the Genesys Cloud environment. This includes, but is not limited to, MPLS circuits, VPLS circuits, point-to-point layer 2 circuits, and IP VPN circuits. All communication to and from Genesys Cloud must traverse the public internet.

Genesys Cloud is compatible with an AWS offering called Direct Connect. Direct Connect is a physical connection between the Carrier location and an AWS region. This will provide dedicated bandwidth from the Carrier to Genesys Cloud if the Carrier has concerns about transmitting over the internet. Genesys Cloud is only compatible with public virtual interfaces within Direct Connect. Please review the information on Direct Connect in the Genesys Cloud Resource Center here.

2.3 Transport

UDP/TCP/TLS over IPv4 are supported. IPv6 is not supported.

Please review the documentation on TLS in the Genesys Cloud Resource Center here for further information and requirements for using TLS with Genesys Cloud.

2.3.1 Fragmentation

Packet fragmentation is sometimes necessary for larger SIP messages. Genesys Cloud supports receiving fragmented packets, however the Carrier must ensure fragmentation is only performed when necessary to ensure delivery of the SIP payload.

For TCP/TLS, Genesys Cloud enforces a strict limit of 4 fragments per SIP message. Upon receipt of the fourth fragment for a message, if the message is still not complete Genesys Cloud will drop the message and reset the TCP/TLS connection.

2.4 Addressing

2.4.1 IP Addresses

The Carrier must provide only publicly addressable IP endpoints when communicating with Genesys Cloud. Any required Network Address Translation (NAT) must be handled within the Carrier's network.

All Carrier IP addresses that will be used to send traffic to Genesys Cloud must be provided and configured in Genesys Cloud when the trunk is provisioned. Genesys Cloud public IP addresses can be provided to the Carrier and are also available in the Genesys Cloud Resource Center here.

2.4.2 DNS

2.4.2.1 Inbound to Genesys Cloud

Genesys Cloud maintains DNS SRV and DNS A records for all public endpoints. DNS SRV is the preferred way for the Carrier to locate Genesys Cloud services. The Carrier must honor the weights and priorities provided by the SRV query. If DNS SRV is not supported, the published individual endpoint DNS records should be used. If no DNS is supported, calls should be sent directly to the Genesys Cloud public endpoint IP addresses. If DNS SRV is not used, it is the Carrier's responsibility to distribute traffic evenly across the Genesys Cloud endpoints. Either random or round-robin distribution is acceptable. Carriers failing to properly distribute traffic to all endpoints may be rate limited to protect the endpoints, Genesys Cloud, and other customers.

2.4.2.2 Outbound from Genesys Cloud

Genesys Cloud supports DNS lookups for outgoing traffic to the Carrier. If DNS SRV is supported it will be used and Genesys Cloud will honor the weights and priorities provided by the SRV query. If DNS SRV is not available, Genesys Cloud will route directly to the Carrier's provided DNS or public IP addresses and will distribute traffic evenly across all provided endpoints using a random distribution.

2.5 SIP Methods

2.5.1 Supported Methods

- INVITE
- ACK
- BYE
- CANCEL
- REFER
- NOTIFY
- OPTIONS
- INFO (out of dialog)

2.5.2 Unsupported Methods

- SUBSCRIBE
- MESSAGE
- UPDATE
- PRACK
- PUBLISH
- REGISTER
- INFO (in-dialog)

Unsupported methods will receive a “405 Method Not Allowed” response.

2.5.3 Unrecognized Methods

Any method that is not listed in either of the preceding sections will receive a “501 Not Implemented” response.

2.5.4 INFO Method

Genesys Cloud does not support the exchange of in-call application information, such as dialed digits or other information, via SIP INFO requests. Therefore, SIP INFO requests sent within a dialog will receive a “405 Method Not Allowed” response, as they serve no purpose without application level support.

SIP INFO requests are only supported when sent outside the context of a dialog/call. This is typically done to verify connectivity/availability, similar to the common use of OPTIONS requests.

2.6 SIP Responses

2.6.1 18X Provisional Responses

Genesys Cloud responds to INVITE requests with '183 Session Progress' messages with SDP for early media establishment or '180 Ringing' without SDP to initiate Carrier-provided ringback.

Carriers may respond to INVITE requests with any 18X message with SDP for early media establishment or any 18X message without SDP to initiate Genesys Cloud-provided ringback.

2.6.2 302 Moved Temporarily

Genesys Cloud will not send a 302 response to the Carrier.

Genesys Cloud will not redirect on a 302 response from the Carrier. Such responses will be treated as call rejection.

2.6.3 4XX Client Responses

Genesys Cloud will send 4XX Client-level responses only when the disposition of the Called Party is known. Carriers must not perform failover or retry a call that receives a 4XX Client response.

Genesys Cloud will not perform automatic failover or retry calls that receive any 4XX Client responses from the Carrier, except for a 408 Timeout response. The Carrier must not send a 4XX Client response unless the disposition of the Called Party is known. In the event Carrier does not establish contact with the Called Party, whether due to error or routing decision, a 4XX response must not be sent as the disposition of the Called Party is not known. Carriers must instead send a “503 Service Unavailable” response in this situation to allow Genesys Cloud to attempt the call via another Carrier if available.

2.6.4 503 Service Unavailable

The Carrier must perform failover to the next available Genesys Cloud endpoint on receipt of any 503 response.

2.7 SIP URI

Note: Please review the documentation in Genesys Cloud Resource Center here for SIP URI requirements specific to BYOC-C trunks.

2.7.1 User

Genesys Cloud Voice utilizes SIP URIs with the destination telephone number as the User portion in the left of the URI. The telephone number must be in E.164 format and include a "+" before the number. At least one of the Request-URI or the To header URI must contain a valid telephone number in this format or the call will be rejected with a "484 Address Incomplete" response.

BYOC-C will accept any value in the user portion of a SIP URI and will pass the value unmodified, except in the case where DNIS Replacement is in use, as described in the Resource Center here.

2.7.2 Host

Genesys Cloud will accept host values that are:

- The IP address of the Genesys Cloud endpoint
- The DNS entry of the Genesys Cloud endpoint
- The DNS SRV entry for Genesys Cloud
- A custom FQDN provided by the Carrier and provisioned in Genesys Cloud

When sending to the Carrier, Genesys Cloud will use one of the following as the host portion of URIs, in this order as available:

- A custom domain provided by the Carrier and provisioned in Genesys Cloud (BYOC-C only)
- Carrier DNS SRV entry
- DNS A entry for the Carrier endpoint
- The IP address of the Carrier endpoint

2.8 SIP Headers

2.8.1 Compact Headers

Genesys Cloud can receive both full and compact headers.

The Carrier must be able to receive both full and compact headers.

2.8.2 Unrecognized Headers

Genesys Cloud silently ignores any SIP headers it does not understand or recognize.

The Carrier must silently ignore any proprietary/non-standard headers in messages received from Genesys Cloud, as required for SIP compliance by RFC 3261.

2.8.3 Record-Route and Route Headers

Genesys Cloud utilizes the Record-Route mechanism defined in RFC 3261 to ensure proper routing of sequential SIP requests. Carriers must fully support Record-Routing as required for SIP compliance by the RFC.

2.9 Registration

Registration is not supported on Genesys Cloud trunks. Genesys Cloud will not register with the Carrier and will not accept registration from the Carrier under any circumstances. SIP REGISTER requests will receive a “405 Method Not Allowed” response from Genesys Cloud.

2.10 Authentication

Genesys Cloud does not require or support authentication on calls from the Carrier trunk. Any authentication information present in received SIP messaging will be ignored.

Genesys Cloud can optionally authenticate calls to the Carrier trunk, using standard SIP Digest Authentication.

2.11 Identity & Privacy

2.11.1 P-Asserted-Identity

Genesys Cloud supports the P-Asserted-Identity header as defined in RFC 3325, and this is the preferred method to transmit the Calling Party name and number. Requirements for the formatting of SIP URIs as described in Section 2.7 apply.

If using the P-Asserted-Identity header and privacy is requested from the caller the Carrier must include the Privacy header defined in RFC 3323. The Carrier must also set the display-name and user in any From and Contact headers to “anonymous”.

2.11.2 Remote-Party-ID

Genesys Cloud also supports the Remote-Party-ID header as defined in draft-ietf-sip-privacy-04. Requirements for the formatting of SIP URIs as described in Section 2.7 apply.

If using the Remote-Party-ID header and privacy is requested from the caller, the Carrier must set rpi-screen to “yes” and the rpi-priv-element to “full”. The Carrier must also set the display-name and user in any From and Contact headers to “anonymous”.

2.11.3 From

If neither P-Asserted-Identity nor Remote-Party-ID is supported, Genesys Cloud will use the From header as the source for Calling Party information. When privacy is requested from the caller, the Carrier must set the display-name and user in any From and Contact headers to “anonymous”.

3 Media

3.1 Supported Codecs

The following codecs are supported by Genesys Cloud:

- Opus (preferred)
- G.711 a-law
- G.711 u-law
- G.722
- G.729

3.2 Fax

Fax transmissions must use G.711 passthrough mode. T.38 fax is not supported by Genesys Cloud.

3.3 DTMF

Genesys Cloud supports in-band DTMF when using G.711 codec and Named Telephony Events (NTE) (RFC 2833) with any codec. Only events 0-15 are supported. The use of NTE is preferred and strongly encouraged.

Use of the SIP INFO method for passing DTMF is not supported in Genesys Cloud.

3.4 IP Addressing

Genesys Cloud media servers are allocated dynamically in AWS so that we can scale with demand. Information about the IP Addresses used for media can be found on our Resource Center here.

Genesys Cloud does not support automatic NAT resolution for RTP, also known as media latching. Any IP Address advertised in SDP from the Carrier must be public and must be the actual IP address used to send and receive RTP. Genesys Cloud will accept RTP from any public IP address.

3.5 Port Assignment

Genesys Cloud considers UDP ports 0-1023 "Well Known Ports" (as defined by the IANA) and as such disallows their use. Genesys Cloud can send and receive RTP media on any other port.

Genesys Cloud requires symmetric RTP transmission. Symmetric RTP means that the Carrier must use a single port for sending and receiving the RTP stream on each call. The Carrier cannot send RTP from a different source port than the one on which it expects to receive.

Appendix A - Glossary

AWS	Amazon Web Services
DNS	Domain Name System
DTMF	Dual Tone Multi Frequency
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NTE	Named Telephony Events
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
RTP	Real-time Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network