This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

SIP Endpoint SDK Developer's Guide

Configuration Settings

12/13/2025

Contents

- 1 Configuration Settings
  - 1.1 Using the Default Configuration File
  - 1.2 **policy** Domain
  - 1.3 **codecs** Domain
  - 1.4 **proxies** Domain
  - 1.5 system Domain
  - 1.6 Additional Configuration Options

Configuration Settings

Using the Default Configuration File

You can find the default configuration file in the following location:

```
<installation folder>/Configuration/SipEndpoint.config
```

This file contains XML configuration details that affect how your SIP Endpoint SDK application behaves. The inital settings are the same as those specified for use with the QuickStart application that is included with your SIP Endpoint SDK release.

Configuration settings are separated into two containers: the Basic Container holds the connectivity details that are required to connect to your SIP Server, while the Genesys Container holds a variety of configuration settings.

Basic Container

The first Container ("Basic") holds the basic connectivity details that are required to connect to your SIP Server. This container has at least one connection (Connectivity) element with the following attributes:

```
<Connectivity user="DN" server="SERVER:PORT" protocol="TRANSPORT"/>
```

If you are using a configuration that supports Disaster Recovery and Geo-Redundancy, there may be multiple connection elements present with each specifying a separate possible connection. Refer to the configuration settings of that feature for details. You will have to make the following changes and save the updated configuration file before using the SIP Endpoint SDK:

- `user="DN"`—Supply a valid DN for the user attribute.
- `server="SERVER:PORT"`—Replace SERVER with the host name where your SIP Server is deployed, and PORT with the SIP port of the SIP Server host. The default SIP port value is 5060. For SRV resolution, specify the SRV record without including the port number in the server's URI. Also see SRV Resolution below.
- `protocol="TRANSPORT"`—Set the protocol attribute to reflect the protocol being used to communicate with SIP Server. Possible values are UDP, TCP, or TLS.

SRV Resolution

When using an SRV record for the **server** parameter, note the following:

- SIP Endpoint SDK selects the SRV target based on the **priority** field only and does not consider the **weight** field of an SRV record.
- You can not combine IPv4 and IPv6 for a single FQDN.
- The maximum number of targets (SRV records) per service is 20.

- You can only specify SRV records in the **server** parameter of the **Connectivity** element. You can not use SRV records for the mailbox section or the **vq_report_collector** setting.

Genesys Container

The second Container ("Genesys") holds a number of configurable settings that are organized into domains and sections. These settings do not have to be changed, but can be customized to take full control over your SIP Endpoint SDK applications.

An overview of the settings in this container and the valid values for these settings is provided here:

Domain	Section	Setting
policy		
	endpoint	
		audio_qos
		include_os_version_in_user_agent_header
		include_sdk_version_in_user_agent_header
		ip_versions
		public_address
		include_mac_address
		refer_to_proxy
		rtp_inactivity_timeout
		rtp_port_binding
		rtp_port_min
		rtp_port_max
		tcp_port_min
		tcp_port_max
		signaling_qos
		sip_port_min
		sip_port_max
		sip_transaction_timeout
		video_max_bitrate
		video_qos
		vq_report_collector
		vq_report_publish
		vq_alarm_threshold
		webrtc_audio_layer

Domain	Section	Setting
		answer_sdp_priority
		sip_port_binding
		defer_device_release
	session	
		agc_mode
		auto_accept_video
		auto_answer
		auto_answer_delay
		dtmf_method
		dtmf_feedback
		echo_control
		noise_suppression
		dtx_mode
		reject_session_when_headset_na
		sip_code_when_headset_na
		vad_level
		ringback_enabled
		ringback_file
		ringing_file
		ringing_enabled
		ringing_timeout
		ringing_while_call_held
		restart_audio_if_stuck
		reject_session_when_busy
		number_sessions_for_busy

Domain	Section	Setting
		sip_code_when_busy
		rx_agc_mode
	device	
		audio_in_device For more information, see Audio Device Settings
		audio_out_device
		capture_device
		headset_name
		exclude_headset
		use_headset
		include_headset
codecs — See Working with Codec Priorities		
proxies		
	proxy''	
		display_name
		domain
		password
		reg_interval
		reg_match_received_rport
		reg_timeout
		mailbox (sub-section of proxy)
		password]]
		server

Domain	Section	Setting
		timeout
		transport
		user
		nat (sub-section of proxy)
		ice_enabled
		stun_server
		stun_server_port
		turn_password
		turn_relay_type
		turn_server
		turn_server_port
		turn_user_name
system		
	diagnostics	
		enable_logging
		log_file
		log_filter
		log_level
		log_options_provider
		log_options_endpoint
		logger_type
		log_segment
		log_expire
		log_time_convert
		log_time_format

Domain	Section	Setting
	security	
		certificate
		dylib-path
		tls_enabled
		tls-target-name-check
		use_srtp
	media	
		ringing_file

policy Domain

endpoint Section

audio_qos

Valid Values: Integer

Integer value representing the DSCP bits to set for RTP audio packets. **Note:** QoS is not supported for Windows Vista, Windows 7, or higher.

include_os_version_in_user_agent_header

Valid Values: `0`, `1`

Default Value: `1`

If set to 1, the user agent field includes the OS version the client is currently running on.

include_sdk_version_in_user_agent_header

Valid Values: `0`, `1`

Default Value: `1`

If set to 1, the user agent field includes the SDK version the client is currently running on.

ip_versions

Valid Values: `IPv4`, `IPv6`, `IPv4`, `IPv6`, `IPv6`, `IPv4`, or empty

Default Value: `IPv4`, `IPv6`

- IPv4—the application selects an available local IPv4 address; IPv6 addresses are ignored.
- IPv6—the application selects an available local IPv6 address; IPv4 addresses are ignored.

- IPv4,IPv6 or an empty—the application selects an IPv4 address if one exists. If not, an available IPv6 address is selected.
- IPv6,IPv4—the application selects an IPv6 address if one exists. If not, an available IPv4 address is selected.

Note: This parameter has no effect if the **public_address** option specifies an explicit IP address.

public_address

Valid Values: See description below

Default Value: Empty string which is fully equivalent to the `$auto` value

Local IP address or Fully Qualified Domain Name (FQDN) of the machine. This setting can be an explicit setting or a special value that the SDK uses to automatically obtain the public address.

Valid Values:

This setting may have one of the following explicit values:

- An IP address. For example, `192.168.16.123` for IPv4 or `FE80::0202:B3FF:FE1E:8329` for IPv6.
- A bare host name or fully qualified domain name (FQDN). For example, `epsipwin2` or `epsipwin2.us.example.com`.

This setting may have one of the following special values:

- $auto—The SDK selects the first valid IP address on the first network adapter that is active (status=up) and has the default gateway configured. IP family preference is specified by the policy.endpoint.ip_versions setting.
- $ipv4 or $ipv6—Same behavior as the $auto setting but the SDK restricts the address to a particular IP family.
- $host—The SDK retrieves the standard host name for the local computer using the gethostname system function.
- $fqdn—The SDK retrieves the fully qualified DNS name of the local computer. The SDK uses the GetComputerNameEx function with parameter ComputerNameDnsFullyQualified.
- An adapter name or part of an adapter name prefixed with $. For example, `$Local Area Connection 2` or `$Local`. The specified name must be different from the special values `$auto`, `$ipv4`, `$host`, and `$fqdn`.
  If the value is an explicit host name, FQDN, or $fqdn, the Contact header includes the host name or FQDN for the recipient of SIP messages (SIP Server or SIP proxy) to resolve on their own. For all other cases, including $host, the resolved IP address is used for Contact. The value in SDP is always the IP address.
- $net:subnet - The SDK will select the IP address matching the given network (from any local interface). The *subnet* is the full CIDR name as per RFC 4632. For example, `$net:192.168.0.0/16`.
- $(rule1,rule2,...) – the SDK will select the IP address from the network interface matching at least one of the given rules, where valid rules are:
    - `if='string'` – matches interface with name or description including the given string, for example:

`if='Wi-Fi'` selects the IP address from the 'Wi-Fi' adapter (if available).

- `if!='string'` – matches interface with name and description that does NOT contain the given string; intended to exclude one particular interface only, for example: `if!='Bluetooth'`.
- `net='CIDR'` – matches interface with IP address on given subnet, where CIDR is the full CIDR name as per RFC 4632, for example: net='10.0.0.0/8' selects network adapter having IP address on given local subnet.
- `net!='CIDR'` – matches interface with IP address that does NOT belong to given subnet, intended to exclude specific subnet, for example: net!='192.168.1.0/24'.
  when multiple interfaces satisfy the given rule set, local IP address selection is based on OS-defined priorities, working the same way as it does with default configuration.

include_mac_address

Valid Values: `0`, `1`

Default Value: `0`

If set to 1, the MAC address is included in the Contact header of the REGISTER message of the host's network interface in a format compatible with RFC 5626.

refer_to_proxy

Valid Values: `0`, `1`

Default Value: `0`

Specifies the destination of a referred INVITE.

- `0`—Send the INVITE to the URL specified in the Refer-To header of the REFER message.
- `1`—Send the INVITE to your configured SIP Proxy.

rtp_inactivity_timeout

Valid Values: `5-150`

Default Value: `150`

Suggested Value: `30`

Timeout interval in seconds for RTP inactivity.

rtp_port_binding

Valid Values: `0,1`

Specifies how SIP Endpoint binds the RTP port:

- 0 — opens the RTP and RTCP ports to listen on any network interface.
- 1 — the RTP and RTCP ports bind to the interface specified by the **public_address** setting and listen only on that IP address.

Important: When **rtp_port_binding** is set to `0`, the **ip_versions** option must specify a single IP version, otherwise a wrong protocol version might be selected for outgoing UDP packages. Default value: 1

rtp_port_min

Valid Values: `9000-65535`

The integer value representing the minimum value for an RTP port range. Must be within the valid port range of `9000` to `65535`. If the minimum and maximum values are not specified or are set to an invalid value, the default minimum (9000) and maximum (minimum value + 999) are used. Setting the minimum to a value that is larger than the maximum is considered an error and will result in a failure to initialize the endpoint.

rtp_port_max

Valid Values: `9000-65535`

The integer value representing the maximum value for an RTP port range. Must be within the valid port range of `9000` to `65535`. If the minimum and maximum values are not specified or are set to an invalid value, the default minimum (9000) and maximum (minimum value + 999) are used. Setting the maximum to a value that is less than the minimum is considered an error and will result in a failure to initialize the endpoint.

tcp_port_min

Valid Values: `0-65535`

The integer value representing the minimum value for a TCP client-side port range. Must be within the valid port range of `1` to `65535`. If set to `0` (default) or if the configured range is not valid, SIP connections over TCP and TLS use ephemeral ports, assigned by the operating system.

tcp_port_max

Valid Values: `0-65535`

The integer value representing the maximum value for a TCP client-side port range. Must be within the valid port range of `1` to `65535`. If set to `0` (default) or if the configured range is not valid, SIP connections over TCP and TLS use ephemeral ports, assigned by the operating system.

If the value is non-zero and greater than the *tcp_port_min* value, this value specifies the maximum value for a TCP client-side SIP port range that will be used for all outgoing SIP connections over TCP and TLS transport.

signaling_qos

Valid Values: Integer

The integer value representing the DSCP bits to set for SIP packets. **Note:** QoS is not supported for Windows Vista, Windows 7, or higher.

sip_port_min

Valid Values: `1-65535`

The integer value representing the minimum value for a SIP port range. Must be within the valid port range of 1 to 65535. If the minimum and maximum values are not specified or are set to an invalid value, the default minimum (5060) and maximum (minimum value + 6) are used. Setting the minimum to a value that is larger than the maximum is considered an error and will result in a failure to initialize the endpoint.

sip_port_max

Valid Values: `1-65535`

The integer value representing the maximum value for a SIP port range. Must be within the valid port range of 1 to 65535. If the minimum and maximum values are not specified or are set to an invalid value, the default minimum (5060) and maximum (minimum value + 6) are used. Setting the maximum to a value that is less than the minimum is considered an error and will result in a failure to initialize the endpoint.

sip_transaction_timeout

Valid Values: `1-32000`

Default Value: `4000`

SIP transaction timeout value in milliseconds. Valid values are 1 through 32000, with a default value of 4000. The recommended value is 4000.

video_max_bitrate

Valid Values: Integer

Integer value representing the maximum video bitrate.

video_qos

Valid Values: Integer

The integer value representing the DSCP bits to set for RTP Video packets. **Note:** QoS is not supported for Windows Vista, Windows 7, or higher.

vq_report_collector

See Producing RTCP Extended Reports.

vq_report_publish

See Producing RTCP Extended Reports.

vq_alarm_threshold

Valid Values: `0` or a number from `1.0` to `5.0`

Default Value: `0`

Specifies the MOS threshold for generating Voice Quality Alarms. A `0` value disables the alarms. The recommended threshold value is `3.5`. Genesys recommends that you avoid using values above `4.2` as an MOS that high might not be obtainable with some codecs, even in perfect network conditions.

webrtc_audio_layer

Valid Values: `0`, `1`, `2`, `1000`, `2000`, `3000`

Default Value: `0`

Specifies which audio layer is used for WebRTC.

- `0` — The audio layer is defined by the `GCTI_AUDIO_LAYER` environment variable — Core audio is used if this environment variable is not specified.
- `1` — Wave audio layer is used.

- 2 — Core audio layer is used.
- `1000` — Instructs the audio layer to open the microphone channel when the endpoint starts up, using the audio layer type defined by option `0`, and to keep it open until the endpoint is terminated.
- `2000` — Opens the speaker channel for the life of the endpoint, using the audio layer type defined by option `0`. Eliminates any delay in opening the audio device when an incoming or outgoing call is connected, for example in environments where audio device startup is slow due to a required restart of the Windows MMCSS service.
- `3000` — Opens the microphone and speaker channels for the life of the endpoint, using the audio layer type defined by option `0`.

> **Important**
>
> Keeping the audio channels permanently open eliminates any delay in connecting audio device to the call works around any issues with device occasionally not starting (or stopping) properly, at the cost of very small performance penalty.

answer_sdp_priority

Valid Values: `config`, `offer`

Default Value: `config`

- `config`—the endpoint selects the first codec from the codec configuration listed in both the codec configuration and the SDP offer.
- `offer`—the endpoint selects the first codec in the SDP offer listed in both the codec configuration and the SDP offer.

sip_port_binding

Valid Values: `0`, `1`

Default Value: `0`

- `0`—opens the SIP port to listen on any interface.
- `1`—the SIP port binds to the interface specified by the `public_address` setting and listens only on this IP address.

> **Important**
>
> The **sip_port_binding** must be set to `0` for automatic IP address change detection to work properly. When set to `1` for specific deployments, agents have to re-register connections manually after an IP address

> change.

defer_device_release

Valid Values: Any integer

Default Value: `200`

If set to a non-zero value, releasing of audio devices will be deferred for a given time (in milliseconds) after the audio stream has been stopped, to avoid any potential service interruptions when the audio is going to be quickly restarted, and if audio device operations are too slow on the user workstation or have other problems with restart. A zero value disables the deferred device release.

session Section

agc_mode

Valid Values: `0`, `1`

Default Value: 1

If set to 0, AGC (Automatic Gain Control) is disabled; if set to 1, it is enabled. Other values are reserved for future extensions. This configuration is applied at startup, after which time the **agc_mode** setting can be changed to 1 or 0 from the main sample application.

Note: It is not possible to apply different AGC settings for different channels in multi-channel scenarios.

auto_accept_video

Valid Values: `0`, `1`

This setting is only used in auto-answer scenarios when `auto_answer=1`.

If auto_accept_video is set to 1, both audio and video streams are accepted, otherwise incoming calls are answered as audio only, even if video is present in the offer.

auto_accept_video applies to a 3pcc answer when make-callrfc3275 is configured to 1 on the originating DN and a video codec is configured in the endpoint. auto_accept_video is not applied to a 3pcc answer when make-call-rfc3275 is configured to 2 on an originating DN, even if auto_accept_video is set to 1 and a video codec is configured in the endpoint.

auto_answer

Valid Values: `0`, `1`

If set to 1, all incoming calls should be answered automatically.

auto_answer_delay

Valid Values: Number in milliseconds

Default Value: `0`

Time in milliseconds to wait before auto-answering (only applicable when `auto_answer=1` and `auto-answer` is not blocked by missing headset).

callwait_tone_enabled

Valid Values: 0, 1

Default Value: 0

Specifies whether the call waiting tone is enabled for incoming calls, to be played when a new call arrives while user is on active call.

callwait_tone_file

Valid Values: Empty or the path to the call waiting tone sound file. The path can be a file in the current directory or the full path to the sound file.

Default Value: Empty

Specifies the audio file that is played when the call waiting tone is enabled with the `callwait_tone_enabled` option.

The call waiting tone file must be a RIFF (little-endian) WAVE file using one of the following formats:

- kWavFormatPcm = 1, PCM, each sample of size bytes_per_sample
- kWavFormatALaw = 6, 8-bit ITU-T G.711 A-law (8 KHz sampling rate)
- kWavFormatMuLaw = 7, 8-bit ITU-T G.711 mu-law (8 KHz sampling rate)

Uncompressed PCM audio must be 16-bit mono or stereo with a sampling rate of 8, 16, or 32 KHz.

dtmf_feedback

Valid Values: 0 (disable feedback), 1 (enable feedback)

Default Value: 1

Controls whether local feedback tone is played when Endpoint sends DTMF to remote party.

dtmf_method

Valid Values: `Rfc2833`, `Info`, `InbandRtp`

Method to send DTMF.

echo_control

Valid Values: `0`, `1`

If set to 1, echo control is enabled.

noise_suppression

Valid Values: `0`, `1`

If set to 1, noise suppresion is enabled.

dtx_mode

Valid Values: `0`, `1`

If set to 1, DTX is activated.

reject_session_when_headset_na

Valid Values: `0`, `1`

If the SDK is configured to use the headset setting (`policy.device.use_headset`=1) and the `reject_session_when_headset_na` option is set to 1, the SDK should reject the incoming session if a

USB headset is not available.

sip_code_when_headset_na

Valid Values: SIP Error Code

Default Value: `480`

If a valid SIP error code is supplied, the SDK rejects the incoming session with the specified SIP error code if a USB headset is not available.

vad_level

Valid Values: `0-3`

Sets the degree of bandwidth reduction, from `0` for conventional VAD to `3` for aggressive high.

ringback_enabled

Valid Values: `0`, `1`, `2`, `3`, `4`, `6`

Default Value: `2`

Specifies whether the ringback tone is enabled for outgoing calls.

- `0` — The ringback is not played when the INVITE dialog is not yet established. In scenarios where ringback is provided by Media Server, the ringback tone would be still present.
- `1` — The incoming media stream is played if provided by the Media gateway in a reliable provisional response with SDP.
- `2` — A local file is used for the ringback.
- `3` — The ringback is always played using either a local file or media provided by the gateway, if the provisional response is reliable.
- `4` — Same as `1`, but the incoming media stream is played even if the provisional response from Media gateway is not reliable.
- `6` — The ringback is always played using either a local file or media provided by the gateway (regardless of whether the provisional response is reliable or not).

ringback_file

Valid Values: Empty or the path to the ringback sound file. The path can be a file in the current directory or the full path to the sound file.

Default Value: Empty

Specifies the audio file that is played when the ringing tone is enabled with the `ringing_enabled` option.

WebRTC does not support MP3 playback. The ringtone file for built-in ringback must be a RIFF (little-endian) WAVE file using one of the following formats:

- kWavFormatPcm = 1, PCM, each sample of size bytes_per_sample
- kWavFormatALaw = 6, 8-bit ITU-T G.711 A-law (8 KHz sampling rate)
- kWavFormatMuLaw = 7, 8-bit ITU-T G.711 mu-law (8 KHz sampling rate)

Uncompressed PCM audio must be 16-bit mono or stereo with a sampling rate of 8, 16, or 32 KHz.

ringing_enabled

Valid values: An integer between 0 to 7.
Default Value: 3

- 0—event Ringing disabled
- 1—event Ringing enabled
- 2—play ringtone internally (event Ringing disabled)
- 3—play ringtone internally and enable event Ringing.
- 4—play ringtone through a separate ringer device.
- 5—play ringtone through the ringer device and enable event Ringing.
- 6—play ringtone internally once for full duration (**ringing_timeout** is not used and the ringing does not stop when call is answered).
- 7—play ringtone once for full duration and enable event Ringing.

> **Important**
>
> If the ringtone is configured to play for full duration (values *6* or *7*), then it will be played even in case of auto-answer with zero delay (configured either in SIP Endpoint SDK or desktop application), unless it is suppressed. This configuration setting assumes **ringing_file** option being configured with a short "beep" sound that would not interfere much with agent hearing the customer (as the ringtone will be played in parallel / mixed with remote audio stream).

Suppressing the Ringtone

The ringtone is generated for all incoming calls to the Genesys SIP Endpoint SDK. To suppress the ringtone for third-party call control for the originating DN, configure the following SIP Server option:

- `make-call-alert-info=<urn:alert:service:3pcc@genesys>`

or

- `make-call-alert-info=<file://null>;service=3pcc`

> **Important**
>
> If at least one application based on SIP Endpoint in the contact center is configured with the `ringing_enabled` option set to a non-zero value, the SIP Server `make-call-alert-info` option should be set to one of the specified values.

ringing_timeout

Valid Values: Empty, `0`, or a positive number

Default Value: `0`

Specifies the duration, in seconds, of the ringing tone. If set to `0` or if the value is empty, the ringing time is unlimited.

ringing_file

Valid Values: Empty or the path to the ringing sound file. The path may be a file name in the current directory or the full path to the sound file.

Default Value: ringing.wav

Specifies the audio file that is played when the ringing tone is enabled with the `ringing_enabled` option.

Note that WebRTC does not support MP3 playback. The ringtone file for built-in ringing should be a RIFF (little-endian) WAVE file using one of the following formats:

- kWavFormatPcm = 1, PCM, each sample of size bytes_per_sample
- kWavFormatALaw = 6, 8-bit ITU-T G.711 A-law
- kWavFormatMuLaw = 7, 8-bit ITU-T G.711 mu-law

Uncompressed PCM audio must 16 bit mono or stereo and have a frequency of 8, 16, or 32 KHZ.

ringing_while_call_held

Valid Values: `0` or 1

Default Value: 1
If set to `0`, when another call is held, playing ringtone is suppressed and call wait tone is played instead (if configured). If set to 1 (default value), ringtone is played whenever a new call arrives and there are no other active calls; held calls are not considered active in this case.

restart_audio_if_stuck

Valid Values: Empty, 0, 1

Default Value: 0

- 0 or Empty—disable auto restart for stuck audio
- 1—enable auto restart for stuck audio

reject_session_when_busy

Valid Values: Empty, 0, 1

Default Value: 0

- 0 or Empty—disable rejection of a session when busy
- 1—enable rejection of a session when busy

number_sessions_for_busy

Valid Values: Positive integer

Default Value: 1

Sets the number of sessions before busy. Must be a positive integer.

sip_code_when_busy

Valid Values: Empty, 4xx, 5xx, 6xx

Default value: Empty

SIP error response code to use when busy. Can be set to any valid SIP error response code in the 4xx, 5xx, or 6xx range, for example, 486.

rx_agc_mode

Valid Values: 0, 1

Default value: 0

When set to 1, the SDK enables the receiving-side AGC allowing the volume of the received RTP stream to be adjusted automatically. When set to `0` (default), the feature is disabled.

device Section

audio_in_device

Valid Values: A regex that matches the ECMAScript standard.

Microphone device name.

For more information, see Audio Device Settings

audio_out_device

Valid Values: A regex that matches the ECMAScript standard.

Speaker device name.

capture_device

Valid Values: A regex that matches the ECMAScript standard.

Capture device name.

headset_name

Valid Values: A regex that matches the ECMAScript standard.

The name of the headset model.

exclude_headset

Valid Values: A regex that matches the ECMAScript standard.

Default Value: Empty

When set, this will exclude devices whose name matches the regex pattern from being considered a valid headset for automatic device selection. Microphone and speaker parts of the excluded headset can still be selected manually (or even automatically, if no better device is found), but such a selection will not set "headset available" flag.

use_headset

Valid Values: `0`, `1`

If set to `0`, the audio devices specified in audio_in_device and audio_out_device are used by the SDK.

If set to 1, the SDK uses a headset as the preferred audio input and output device and the audio devices specified in audio_in_device and audio_out_device are ignored.

include_headset

Valid Values: Pair of device names or name parts with microphone and speaker names separated by colon, or comma-separated list of such pairs, for example: `External Mic : Headphones`

Default Value: Empty

When set, specifies the list of audio in/out devices to be considered as headset for automatic device selection, applicable to case when *use_headset = 1*. The names including delimiter character (quotes, colon or comma) must be enclosed in single or double quotes.

codecs Domain

See Working with Codec Priorities

proxies Domain

Configure a proxy section for each connectivity line. For example, for three connectivity lines, configure sections for `proxy0`, `proxy1`, and `proxy2`.

When the proxy section does not exist in the configuration file for a particular connectivity line, the framework takes the configurations settings from the `proxy0` section. You can use this feature in use cases where the proxy sections are the same for all connectivity lines.

proxy Section

display_name

Valid Values: String

Proxy display name.

domain

Valid Values:Any valid SIP domain

Default Value: Empty

A SIP domain is an application layer configuration defining the management domain of a SIP proxy. The configured value should include hostport and may include uri-parameters as defined by RFC 3261. The scheme, userinfo, and transport URI parameters are included automatically.

If set to an empty string, SIP Endpoint SDK for .NET uses the parameters from the Connectivity section to construct the SIP domain value as it did in previous versions.

password

Valid Values: String

Proxy password.

reg_interval

Valid Values: Integer

Default Value: `0`

The period, in seconds, after which the endpoint starts a new registration cycle when a SIP proxy is down. Valid values are integers greater than or equal to `0`. If the setting is empty or negative, the default value is 0, which means no new registration cycle is allowed. If the setting is greater than 0, a new registration cycle is allowed and will start after the period specified.

reg_match_received_rport

Valid Values: `0` or 1

Default Value: `0`

This setting controls whether or not SIP Endpoint SDK should re-register itself when receiving an IP address (in the `received` parameter of a REGISTER response) that is different from the address supplied in the Contact header and does not match any local network interfaces. A value of `0` (default) disables this feature and a value of 1 enables re-registration.

Starting from 9.0.003, this setting is deprecated and is not recommended for use, unless suggested by Genesys Technical Support to fix specific problems. When the `received` parameter of a REGISTER response matches a local IP address, changing the IP address and re-registering is now done automatically.

reg_timeout

Valid Values: Number in seconds

The period, in seconds, after which registration should expire. A new REGISTER request will be sent before expiration. Valid values are integers greater than or equal to 0. If the setting is `0` or empty/null, then registration is disabled, putting the endpoint in standalone mode.

mailbox Sub-section

> **Important**
> **mailbox** is a sub-section of the **proxy<n>** section.

password

Valid Values: String

Mailbox password.

server

Valid Values: String

Proxy server address and port for this mailbox.

timeout

Valid Values: Number in seconds

Default Value: `1800`

Subscription expiration timeout in seconds. If the setting is missing or set to `0`, the SDK uses a default timeout of `1800` seconds (30 minutes).

transport

Valid Values: `udp`, `tcp`, `tls`

Transport protocol to use when communicating with the server.

user

Valid Values: String

Mailbox ID for this mailbox.

nat Sub-section

> **Important**
> **nat** is a sub-section of the **proxy<n>** section.

ice_enabled

Valid Values: Boolean

Enable or disable ICE.

stun_server

Valid Values: String

STUN server address. An empty or null value indicates this feature is not used.

stun_server_port

Valid Values: Valid port number

Default Value: 3478

STUN server port value.

turn_password

Valid Values: String

Password for TURN authentication.

> **Warning**
> Starting from 9.0.012.02, this setting is deprecated and is not recommended for use, unless suggested by Genesys Technical Support to fix specific problems. Use the GCTI_TURN_PASSWORD environment variable to set the password for TURN authentication.

turn_relay_type

Valid Values: `0`, `udp`, `1`, or `tcp`

Type of TURN relay.

- `0` or `udp` for TURN over UDP.
- `1` or `tcp` for TURN over TCP.

turn_server

Valid Values: String

TURN server address. An empty or null value indicates this feature is not used.

turn_server_port

Valid Values:Valid port number

Default Value: 3478

TURN server port value.

turn_user_name

Valid Values: String

User ID for TURN authorization

> **Warning**
> Starting from 9.0.012.02, this setting is deprecated and is not recommended for use, unless suggested by Genesys Technical Support to fix specific problems. Use the GCTI_TURN_USERNAME environment variable to set the username for TURN authentication.

`system` Domain

diagnostics Section

enable_logging

Valid Values: `0` or 1

Default Value: 1

Disable or enable logging.

log_file

Valid Values: String

Log file name, for example, `SipEndpoint.log`.

log_filter

Valid Values: *Empty*, `dtmf`

Default Value: *Empty*

Specifies the list of log filters to be applied to hide sensitive data from the endpoint log. Currently the only supported filter is `dtmf`, which hides all occurrences of DTMF data from the log (by replacing entered digits with 'x').

log_level

Valid Values: `0`-4

Default Value: 3

Log levels: `0` = "Fatal"; 1 = "Error"; 2 = "Warning"; 3 = "Info"; 4 = "Debug"

log_options_provider

Valid Values: Comma-separated list of log setting for various low-level components, including:

- `gsip=N` - Genesys SIP library log level, default is 2
- `webrtc=(level)` - Log level(s) for third-party WebRTC native code component. The default is `error` to include error messages and important WebRTC diagnostic, value `api` adds low-level API printouts.

Example value: `gsip=2,webrtc=(error)`

> **Warning**
>
> This settings control low-level debug information used for troubleshooting. Please don't change the value unless instructed by Genesys Technical Support engineer.

log_options_endpoint

Valid Values: `0`-4, same as **log_level**

Default Value: 2

Log levels: `0` = "Fatal"; 1 = "Error"; 2 = "Warning"; 3 = "Info"; 4 = "Debug"

5 = Logging disabled.

This setting should not be set higher than log_level setting.

logger_type

Valid Values: file

If set to `file` the log data will be printed to the file specified by the **log_file** value.

log_segment

Valid Values: `false`, number, or number in KB,MB, or hr

Default Value: `10 MB`

- false: No segmentation is allowed
- or KB: Size in kilobytes
- MB: Size in megabytes
- hr: Number of hours for segment to stay open

Specifies the segmentation limit for a log file. If the current log segment exceeds the size set by this option, the file is closed and a new one is created. This option is ignored if log output is not configured to be sent to a logfile.

log_expire

Valid Values: `false`, number, number `file`, number day

Deafult Value: `10` (store 10 log fragments and purge the rest)

- false: No expiration; all generated segments are stored.
- or file: Sets the maximum number of log files to store. Specify a number from 1—1000.
- day: Sets the maximum number of days before log files are deleted. Specify a number from 1—100

Determines whether log files expire. If they do, sets the measurement for determining when they expire, along with the maximum number of files (segments) or days before the files are removed. This option is ignored if log output is not configured to be sent to a log file.

log_time_convert

Valid Values: `local`, `utc`

Default Value: `local`

- `local`: The time of log record generation is expressed as a local time, based on the time zone and any seasonal adjustments. Time zone information of the application's host computer is used.
- `utc`: The time of log record generation is expressed as Coordinated Universal Time (UTC).

Specifies the system in which an application calculates the log record time when generating a log file. The time is converted from the time in seconds since the Epoch (00:00:00 UTC, January 1, 1970).

log_time_format

Valid Values: `time`, `locale`, `ISO8601`

Default Value: time

- `time`: The time string is formatted according to the HH:MM:SS.sss (hours, minutes, seconds, and milliseconds) format
- `locale`: The time string is formatted according to the system's locale.
- `ISO8601`: The date in the time string is formatted according to the ISO 8601 format. Fractional seconds are given in milliseconds.

Specifies how to represent, in a log file, the time when an application generates log records. A log record's time field in the ISO 8601 format looks like this: 2001-07-24T04:58:10.123.

security Section

> **Important**
> SIP Endpoint SDK no longer uses the **tls_enabled** setting.

certificate

See Configuring certificate option for TLS.

dylib-path

Valid Values: Empty, path to dynamic library location
Default Value: Empty

Specifies the location of Genesys security module's dynamic libraries for TLS support. The name of the dynamic library in different processors are:

- `libgsecurity_openssl_64.dylib` for Intel processor
- `libgsecurity_openssl_arm64.dylib` for Apple processor

If the option is not specified or set to empty value (default), SIP Endpoint SDK requires the dynamic libraries to be located in the **Resources** folder of the application's main bundle

tls-target-name-check

See Configuring tls-target-name-check option for TLS.

use_srtp

Valid Values: `optional`, `allowed`, `disabled`, `off`, `elective`, `both`, `enabled`, `force`, `mandatory`

Indicates whether to use SRTP:

- `optional` or `allowed`—do not send secure offers, but accept them
- `disabled` or `off`—do not send secure offers and reject incoming secure offers
- `elective` or `both`—send both secure and non-secure offers and accept either
- `enabled`—send secure offers, accept both secure and non-secure offers
- `force` or `mandatory`—send secure offers, reject incoming non-secure offers

Adding either `',UNENCRYPTED_SRTCP'` (long form) or `',UEC'` (short form) to any value (for example, "*enabled,UEC*""), would result in the **UNENCRYPTED_SRTCP** parameter being added to that offer. When this parameter is negotiated, RTCP packets are not encrypted, but are still authenticated.

media Section

ringing_file

Valid Values: Empty, String file name

Default Value: `ringing.mp3`

The Ringing sound file name in the current directory or the full local path to the ringing sound file.

Additional Configuration Options

The default configuration file may not contain all settings that may be used with the SIP Endpoint SDK; additional settings can be added to change certain behaviors. Check Configuring SIP Endpoint SDK for .NET for a discussion of these additional settings.