



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.

Genesys Softphone Deployment Guide

Configuration Options Reference

12/19/2025

Configuration Options Reference

[**Modified:** 8.5.4]

This topic lists and describes, by container and then by domain, the configuration settings found in the <Genesys Softphone Installation Directory>/Genesys Softphone/GenesysSoftphone/Softphone.config file. For an example of the configuration file, see [Configuring Genesys Softphone](#).

The Softphone.config file is **installed**, along with genesys_softphone.exe, by either the **Genesys Installation Wizard** or silently by command line. The contents of the Softphone.config file is generated by the choices specified in the wizard or by modifications made to the genesys_silent.ini file.

In the Softphone.config file, the following attributes of the **Connector** section are set by setup.exe: protocol, port, and certificate_search_path, while enable_sessionid, auto_restart are not. The default value of these attributes are designed to address most business deployments. However, if you want to adjust their values, follow these steps to make a custom deployment:

1. Install Genesys Softphone on an administrator's machine.
2. Edit the Softphone.config file to change the values of the attributes in the **Connector** section.
3. Repackage Genesys Softphone with the custom Softphone.config file through an IT-controlled installation.
4. Push the custom package to the agent workstations.

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:

- Do not specify the port in the server URI.
- SIP Endpoint SDK does not take into account 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.

Important

Your environment can have up to six SIP URIs (Connectivity sections) that represent six endpoint connections with SIP Server.

Domain	Section	Setting	Default Value	Description
	Connectivity	user		The first user's DN extension as configured in the configuration database. Included in the SIP URI—for example, <sip: DN0 @serverHostName0:port>
		server		The SIP Server or Proxy location for the first user. Included in the SIP URI—for example, <sip:DN0@ serverHostName0 :port>
		protocol		The transport protocol for the first user. For example, UDP, TCP, or TLS.
		For more information, see the Basic Container description in the SIP Endpoint SDK for .NET Developer's Guide.		

Genesys Container

[**Modified:** 8.5.4]

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.

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

Domain	Section	Setting	Values	Description
policy				
	endpoint			
		include_os_version_in_user_agent_header	Number	If set to 1, the user agent field includes the OS version the client is currently running on. Default: 1.
		gui_call_lines	Number from 1 to 7	This option controls the number of phone lines in the First Party Call Control tab. Valid values: Integer between 1 and 7 Default value: 3
		gui_tabs	Comma-separated list of tab names	This option controls what tabs are shown in the GUI and their order. Valid values: Comma-separated list of tab names in any order. The tab names are status, calls, and devices. Names may be shortened to stat, call, and dev. The value is case-sensitive. This option ignores unrecognizable and duplicate tab names. If the setting is present but has an incorrect value, the value will fall back to the single tab status. Default value: status,calls,devices
		include_sdk_version_in_user_agent_header	Number	If set to 1, the user agent field includes the SDK version the client

Domain	Section	Setting	Values	Description
				is currently running on. Default: 1.
		ip_versions	IPv4 IPv6 IPv4,IPv6 IPv6,IPv4 empty	<p>A value of IPv4 means that the application selects an available local IPv4 address; IPv6 addresses are ignored.</p> <p>A value of IPv6 means that the application selects an available local IPv6 address; IPv4 addresses are ignored. A value of IPv4, IPv6 or an empty value means that the application selects an IPv4 address if one exists. If not, an available IPv6 address is selected.</p> <p>A value of IPv6, IPv4 means that the application selects an IPv6 address if one exists. If not, an available IPv4 address is selected.</p> <p>Default: IPv4.</p> <p>NOTE: This parameter has no effect if the public_address option specifies an explicit IP address.</p>
		public_address	String	<p>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 GSP uses to automatically obtain the public address.</p> <p>Valid Values: This setting may have one of the following explicit values:</p> <ul style="list-style-type: none"> An IP address. For example, 192.168.16.123 for IPv4 or FE80::0202:B3

Domain	Section	Setting	Values	Description
				<p>FF:FE1E:8329 for IPv6.</p> <ul style="list-style-type: none">• A bare host name or fully qualified domain name (FQDN). For example, epsipwin2 or epsipwin2.us. example.com. <p>This setting may have one of the following special values:</p> <ul style="list-style-type: none">• \$auto—The GSP 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 GSP restricts the address to a particular IP family.• \$host—The GSP retrieves the standard host name for the local computer using the gethostname system function.

Domain	Section	Setting	Values	Description
				<ul style="list-style-type: none">• <code>\$fqdn</code>—The GSP retrieves the fully qualified DNS name of the local computer. The GSP uses the <code>GetComputerNameEx</code> function with parameter <code>ComputerNameFullyQualified</code>.• An adapter name or part of an adapter name prefixed with <code>\$</code>. For example, <code>\$Local Area Connection 2</code> or <code>\$Local</code>. The specified name must be different from the special values <code>\$auto</code>, <code>\$ipv4</code>, <code>\$host</code>, and <code>\$fqdn</code>. <p>Default Value: Empty string which is fully equivalent to the <code>\$auto</code> value.</p> <p>If the value is specified as an explicit host name, FQDN, or <code>\$fqdn</code>, 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 <code>\$host</code>, the resolved IP address is used for Contact. The value in SDP is always the IP address.</p>
		<code>include_mac_address</code>	Number	Default Value: 0. If set to 1, the MAC address is included in the Contact header of the

Domain	Section	Setting	Values	Description
				REGISTER message of the host's network interface in a format compatible with RFC 5626.
		rtp_inactivity_timeout	Number	Timeout interval for RTP inactivity. Valid values are positive integers. A value of 0 means that this feature is not activated. A value 1 or higher indicates the inactivity timeout interval in seconds. Default: 0. Suggested values: 1 through 150.
		rtp_port_min	Number	The integer value representing the minimum value for an RTP 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 (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	Number	The integer value representing the maximum value for an RTP port range. Must be within the valid port range of 1 to

Domain	Section	Setting	Values	Description
				65535. If the minimum and maximum values are not specified or are set to an invalid value, the default minimum (9999) 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	Number	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	Number	<p>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.</p> <p>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.</p> <p>If the value is non-zero and greater than the tcp_port_min value, this value specifies the</p>

Domain	Section	Setting	Values	Description
				maximum value for a TCP client-side SIP port range that will be used for all outgoing SIP connections over TCP and TLS transport.
		sip_port_min	Number	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	Number	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

Domain	Section	Setting	Values	Description
				error and will result in a failure to initialize the endpoint.
		sip_transaction_timeout	Number	SIP transaction timeout value in milliseconds. Valid values are 1 through 32000, with a default value of 4000. The recommended value is 4000.
		vq_report_collector		See SIP Endpoint SDK for .NET—Producing RTCP Extended Reports
		vq_report_publish		See SIP Endpoint SDK for .NET—Producing RTCP Extended Reports
		webrtc_audio_layer	0 1 2	Valid values: 0—the audio layer is defined by environment variable "GCTI_AUDIO_LAYER" 1—Wave audio layer is used 2—Core audio layer is used
	session			
		agc_mode	0 1	If set to 0, AGC (Automatic Gain Control) is disabled; if set to 1, it is enabled. Default: 1. 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

Domain	Section	Setting	Values	Description
				to apply different AGC settings for different channels in multi-channel scenarios.
		auto_answer	Number	If set to 1, all incoming calls should be answered automatically.
		dtmf_method	Rfc2833 Info InbandRtp	Method to send DTMF
		echo_control	0 1	Valid values: 0 or 1. If set to 1, echo control is enabled.
		noise_suppression	0 1	Valid values: 0 or 1. If set to 1, noise suppression is enabled.
		dtx_mode	Number	Valid values: 0 or 1. If set to 1, DTX is activated.
		reject_session_when_headset_na	Number	Valid values: 0 or 1. If set to 1, the GSP should reject the incoming session if a USB headset is not available.
		sip_code_when_headset_na	Number	Default Value: 480 If a valid SIP error code is supplied, the GSP rejects the incoming session with the specified SIP error code if a USB headset is not available.
		vad_level	Number	Sets the degree of bandwidth reduction. Valid values: 0 – 3 — from 0 (conventional VAD) to 3 (aggressive high).
		ringing_enabled	Number	Valid values: 0, 1, 2, 3, or 4. 0 = None, disable

Domain	Section	Setting	Values	Description
				<p>ringtone</p> <p>1 = Play ringtone through system default device only. Configure media in <code>system.media.ringing_file</code>.</p> <p>2 = Play ringtone through communication device (headset) only. Configure media in <code>policy.session.ringing_file</code>.</p> <p>3 = Play ringtone through both devices at the same time.</p> <p>4 = Play ringtone through separate ringer device, specified by <code>policy.device.ringer_device</code>.</p> <p>Default Value: 1</p> <p>Specifies whether to enable the ringing tone and on which device to play the media file.</p>
		ringing_timeout	Number	<p>Valid Values: Empty, 0, or a positive number</p> <p>Default Value: 0</p> <p>Specifies the duration, in seconds, of the ringing tone. If set to 0 or if the value is empty, the ringing time is unlimited.</p>
		ringing_file	String	<p>Valid values: Empty or the path to the ringing sound file for the audio out device (headset). The path may be a file name in the current directory or the full path to the sound file.</p> <p>Default Value: <code>ringing.wav</code></p> <p>Specifies the audio file that is played in the audio out device (headset) when the ringing tone is enabled with the <code>ringing_enabled</code> option.</p> <p>Note that WebRTC does not support MP3 playback. The ringtone file for built-in ringing should be a RIFF (little-</p>

Domain	Section	Setting	Values	Description
				<p>endian) WAVE file using one of the following formats:</p> <p>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</p> <p>Uncompressed PCM audio must 16 bit mono or stereo and have a frequency of 8, 16, or 32 KHZ.</p>
	device			
		audio_in_device For more information, see SIP Endpoint SDK for .NET—Audio Device Settings	String	Microphone device name
		audio_out_device	String	Speaker device name
		ringer_device	String	Ringer device name. Used when ringing_enabled = 4
		headset_name	String	The name of the headset model. When the value of the use_headset option is set to 1, you can set the value of this option to *, the default value, to select the default headset. If the value of this option is empty, this option is not considered as a regular expression and will fail to find a headset.
		use_headset	Number	Valid values: 0 or 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

Domain	Section	Setting	Values	Description
				preferred audio input and output device and the audio devices specified in <code>audio_in_device</code> and <code>audio_out_device</code> are ignored.
	connector			
		protocol	String	Valid values: http or https. Specifies whether the HTTP requests sent from HTTP client (typically WWE running in a browser) are secured. If set to a non empty value the option port must be populated with a valid port number. If set to https, the option <code>certificate_search_value</code> must be populated with a valid certificate thumbprint.
		port	Number	The port that Softphone is opening at start-up time to listen to HTTP or HTTPS requests sent by the HTTP Client (typically WWE running in a browser). If sent to empty value (default) the connector is not activated and Softphone runs in regular standalone GUI mode.
		certificate_search_value	String	The thumbprint of a valid certificate that is accessible from the Certificate Store of the workstation where Softphone is

Domain	Section	Setting	Values	Description
				running.
		enable_sessionid	Number	Valid values: 0 or 1. If set to 1 (default), a SESSION_ID attribute is generated in the header of the HTTP response returned to the HTTP Client (typically WWE running in a browser). [Modified: 8.5.4]
		auto_restart	Number	Valid values: 0 or 1. If set to 1 (default) the Softphone must be restarted after every client session. [Added: 8.5.4]
codecs — For Softphone 8.5.401.03, see SIP Endpoint SDK for .NET 9.0.0NET—Working with Codec Priorities , and for Softphone 8.5.400.04 to 8.5.400.11, see SIP Endpoint SDK for .NET 8.5.2—Working with Codec Priorities				
proxies				
	proxy<n>			
		display_name	String	Proxy display name
		password	String	Proxy password
		reg_interval	Number	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

Domain	Section	Setting	Values	Description
				<p>the period specified by regInterval.</p> <div> Important The re-registration procedure uses a smaller timeout (half a second) for the first re-try only, ignoring the configured reg_interval setting; the reg_interval setting is applied to all further retries. </div>
		reg_match_received_number	Number	<p>DEPRECATED</p> <p>Valid Values: 0 or 1 Default Value: 0 This setting controls whether or not SIP Endpoint SDK should re-register itself when receiving a mismatched IP address in the received parameter of a REGISTER response. This helps resolve the case where SIP Endpoint SDK for .NET has multiple network interfaces and obtains the wrong local IP address. A value of 0 (default) disables this feature and a value of 1 enables re-registration.</p>
		reg_timeout	Number	<p>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.</p>
	nat			
		ice_enabled	Boolean	Enable or disable ICE

Domain	Section	Setting	Values	Description
		stun_server	String	STUN server address. An empty or null value indicates this feature is not being used.
		stun_server_port	String	STUN server port value
		turn_password	Number	Password for TURN authentication
		turn_relay_type	Number	Type of TURN relay
		turn_server	String	TURN server address. An empty or null value indicates this feature is not being used.
		turn_server_port	String	TURN server port value
		turn_user_name	String	User ID for TURN authorization
system				
	diagnostics			
		enable_logging	Number	Valid values: 0 or 1. Disable or enable logging.
		log_file	String	Log file name, for example, SipEndpoint.log
		log_level	Number	Valid values: 0 - 4. Log levels: 0 = "Fatal"; 1 = "Error"; 2 = "Warning"; 3 = "Info"; 4 = "Debug".
		log_options_provider	String	Valid values for webrtc = (warning, state, api, debug, info, error, critical). For example: gsip=2, webrtc=(error,critical)
		logger_type	file	If set to file, the log data will be printed to the file specified by the log_file parameter.

Domain	Section	Setting	Values	Description
		log_segment	false Number Number in KB,MB, or hr	<p>Valid Values:</p> <p>false: No segmentation is allowed <number> or <number> KB: Size in kilobytes <number> MB: Size in megabytes <number> hr: Number of hours for segment to stay open Default Value: 10 MB 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.</p>
		log_expire	false Number Number file Number day	<p>Valid Values:</p> <p>false: No expiration; all generated segments are stored. <number> or <number> file: Sets the maximum number of log files to store. Specify a number from 1–1000. <number> day: Sets the maximum number of days before log files are deleted. Specify a number from 1–100 Default Value: 10 (store 10 log fragments and purge the rest) 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.</p>
		log_time_convert	local utc	<p>Valid Values:</p> <p>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</p>

Domain	Section	Setting	Values	Description
				computer is used. utc: The time of log record generation is expressed as Coordinated Universal Time (UTC). Default Value: local 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	time locale ISO8601	Valid Values: 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. Default Value: time 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			
		cert_file	String	Thumbprint value of the Public endpoint certificate file, which is used as a client-side certificate for outgoing TLS connection and server-side certificate for incoming TLS connections. For example: 78 44 34 36 7a c2 22 48 bd 5c 76 6b

Domain	Section	Setting	Values	Description
				00 84 5d 66 83 f5 85 d5
		tls_enabled	Number	If set to 1, connection with TLS transport will be registered. Default: 0.
		use_srtp	String disabled optional mandatory	Indicates whether to use SRTP
	media			
		ringing_file	String	Valid Values: Empty or 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. Specifies the audio file that is played in the default audio device (speakers) when the default device ringing tone is enabled with the ringing_enabled option.

For more information about these options, see [SIP Endpoint SDK for .NET Developer's Guide](#).