Genesys Softphone Deployment Guide

Genesys Softphone 8.5.4

1/1/2022

Table of Contents

Genesys Softphone Deployment Guide 3
Overview 5
Deploying the Genesys Softphone 7
Single sign on with Workspace Web Edition 12
Configuration Options Reference 16
Using the Genesys Softphone 36

Genesys Softphone Deployment Guide

Welcome to the Genesys Softphone Deployment Guide. This document describes how to deploy and use the Genesys Softphone in your environment.

Contacting Genesys Customer Care

If you have purchased support directly from Genesys, please contact Genesys Customer Care.

Before contacting Customer Care, please refer to the Genesys Care Program Guide for complete contact information and procedures.

About This Document

The following list explains different features of the Genesys Softphone:

Overview

This section introduces you to the features of the Genesys Softphone.

- Architecture
- Features and Functionality

Deployment

This section explains how to deploy the Genesys Softphone.

- Installation
- Configuration
- Configuration Options Reference
- Single sign on with Workspace Web Edition

How to Use

This section explains how to use the Genesys Softphone.

- Using the Genesys Softphone

Overview

Architecture

The Genesys Softphone sits on top of the SIP Endpoint SDK for .NET to enable it to take advantage of the SIP-based third-party call control functionality.

The following diagram illustrates the Genesys Softphone architecture:

file:Genesys_Softphone_Architecture.png

Features and Functionality

DTMF

The Genesys Softphone supports Dual-Tone Multi-Frequency (DTMF) signalling according to the RFC 2833 standard for third-party call control.

After receiving a NOTIFY with DTMF event, the Softphone Endpoint generates DTMF signals.

DTMF can be sent by using one of the three possible methods:

- InbandRTP
- RFC 2833
- SIP INFO message

Third-party Call Control

When the Genesys Softphone Endpoint has registered on the Genesys SIP Server, it will support the following third-party call control scenarios:

- Make a call
- Answer a call
- Hold and retrieve a call
- Single step and two step transfers
- Participate in a conference that is provided by the GVP
- Play DTMF signals.

SIP Voice

The Genesys Softphone supports the following codecs for SIP signaling:

- PCMU/8000 (G.711/mu-law)
- PCMA/8000 (G.711/A-law)
- G722/16000
- iLBC/8000 (iLBC — internet Low Bitrate Codec)
- iSAC/32000 ((iSAC/32kHz) — internet Speech Audio Codec)
- iSAC/16000
- G729/8000
- OPUS/48000/2

Deploying the Genesys Softphone

This topic describes how to install and configure the Genesys Softphone in your environment.

Environment Prerequisites

Ensure that your environment meets the prerequisites described in this section.

Supported Operating Systems

- Windows 10 32-bit and 64-bit
- Windows 8 32-bit and 64-bit
- Windows 7 32-bit and 64-bit

Other Prerequisites

To work with the Genesys Softphone, you must ensure that your system meets the software requirements established in the Genesys Supported Operating Environment Reference Manual, as well as meeting the following minimum software requirements:

- Visual C++ Redistributable Packages for Visual Studio 2013 (32 bits version) — The Genesys Installation Package installs this redistributable package on the workstation where it is executed.
- Windows Media Player for ringtone playback.

Installing the Genesys Softphone

To install the Genesys Softphone follow these steps:

1. Double-click the `setup.exe` file that is located in the `<Genesys Softphone Install Directory>\windows\` directory. The **Genesys Installation Wizard** displays the **Welcome to the Installation** window.
2. Click **Next**. The **Choose Destination Location** window is displayed.
3. Click **Next** to accept the default destination folder, or click **Browse** to select another destination location. The **Startup and Secure Connection options** window is displayed.
4. You may choose one or more of the following options, then click **Next**:
    - Auto Startup—Choose this option to specify that Genesys Softphone launches when Windows starts up. Selecting this option means that agents do not have to manually launch Genesys Softphone before they launch Workspace or other agent desktops.
    - Enable Dynamic Configuration Connector—Choose this option to allow Workspace Web Edition to dynamically configure the

Genesys Softphone when it is launched.

If you choose the Enable Dynamic Configuration Connector option, the **Dynamic Configuration Connector parameters** window is displayed.

a. Specify the Connector Port for the Genesys Softphone. This port must be compliant with the value specified by the `sipendpoint.uri` option.

b. You can enable HTTPS secure connections. If you choose a secure connection, you must choose the type of security certificate that you use:

   - Self-signed Certificate — In this mode, the IP creates a self-signed certificate, installs it in the Personal Certificate section of the workstation where `setup.exe` is executed and also installs it as a root certificate authority at Machine level in the workstation where `setup.exe` is executed.
   - Certificate Authorities from the Windows Certificate Store

   Click **Next**. The **Ready to Install** window is displayed.

5. Select **Install**. The wizard installs the Genesys Softphone and all associated files in the selected directory and displays the **Installation Status** window. The installation might take several minutes.
6. At the **Installation Complete** window, select **Finish**.

> Important
>
> For more information about Softphone deployment for Workspace Web Edition (WWE), see Single sign on with Workspace Web Edition.

Installing the Genesys Softphone in Silent Mode

To install the Genesys Softphone in silent mode, use the Installation Wizard silent arguments as follows:

1. Update the `genesys_silent.ini` file by making the following modifications:
   - Add the path to the Genesys Softphone installation directory—for example, `InstallPath=C:\GCTI\Genesys Softphone`.
   - Specify whether Genesys Softphone starts automatically when Windows starts up by using the `Startup=<Std or Auto>` parameter.
   - Specify whether Workspace Web Edition can dynamically modify the Genesys Softphone configuration by using the `Connector=<Disable or Enable>` parameter.
   - If you are *deploying* Softphone for Workspace Web Edition dynamic configuration:
     - Specify the Connector Port if the Connector is enabled by using the `ConnectorPort=<port number>` parameter.
     - Specify whether the connector uses HTTPS secure connection by using the `HTTPS=<NotUsed or Used>` parameter.
     - If you are using a secure connection, specify the type of certificate to be used by using the `CertificateType=<SelfSigned or WindowsStore>` parameter.

    - If you assign the value `WindowsStore` to the `CertificateType` option, specify the certificate thumbprint by using the `CertThumbPrint=<certificate thumbprint>` parameter.

- If you are *upgrading* Genesys Softphone specify:
    - `IPVersion= <current version of Genesys Softphone on this box (before upgrade)>`
    - `IPBuildNumber= <current build number of Genesys Softphone on this box (before upgrade)>`

2. Execute the following command:
   `setup.exe /s /z"-s 'FullPathToGenesysSilentConfigurationFile' -sl 'FullPathToGenesysSilentResultFile'"` where:
    - /s—Specifies that the installation is running in InstallShield Silent Mode.
    - /z—Passes the Genesys Silent Mode silent parameters to the installation.
    - -s—Specifies the full path to the silent configuration file. The `<Full path to Genesys Silent Configuration file>` is optional. If the `<Full path to Genesys Silent Configuration file>` parameter is not specified, the installation uses the `genesys_silent.ini` file in the same directory where the `setup.exe` is located.

      > **Important**
      >
      > Enclose the value of the `<Full path to Genesys Silent Configuration file>` parameter by apostrophes (') if the parameter contains white symbols.

    - -sl—Specifies the full path to the installation results file. If the `<Full path to Genesys Installation Result file>` parameter is not specified, the installation creates the `genesys_install_result.log` file in the `<System TEMP folder>` directory.

      > **Important**
      >
      > Enclose the value of the `<Full path to Genesys Installation Result file>` parameter by apostrophes (') if the parameter contains white symbols.

   The `InstallShield setup.exe` installation starter requires that:
    - there is *no* space between the `/z` argument and quotation mark. For example, `/z"-s"` is valid, while `/z "-s"` is not valid.
    - there *is* a space between the -s,-sl parameters and quotation mark. For example, `/z"-s c:\temp\genesys_silent.ini"` is valid, while `/z "-sc:\temp\genesys_silent.ini"` is not valid. For example,
      `setup.exe /s /z"-s 'C:\8.5.000.05\windows\b1\ip\genesys_silent.ini' -sl 'C:\GSP\silent_setup.log'"`.
3. After executing this command, verify that the Genesys Softphone is installed in the `C:\<Genesys Softphone Installation Directory>`, and that the `silent_setup.log` file created in the `C:\GSP\` directory.

Configuring the Genesys Softphone

The Genesys Softphone installation includes a configuration file (`<Genesys Softphone Installation Directory>/Softphone.config`) with configuration settings that are applied to the Softphone when it starts.

> **Important**
>
> You can make changes to the configuration file, but you must restart the Softphone before any of the changes take effect.

The configuration file is organized into containers. Each container is divided into domains that are broken into sections that hold the settings for a group of parameters. The following configuration file examples illustrate these settings:

For the description and valid values of each parameter, see Configuration Options Reference.

Basic Container

The Basic container sets the Genesys Softphone user's DNs and the protocol used.

```
<Container name ="Basic">
    <Connectivity user ="DN0" server="Server0:Port0" protocol="Protocol"/>
    <Connectivity user ="DN1" server="Server1:Port1" protocol=" Protocol"/>
  </Container>
```

Genesys Container

The Genesys container sets the policy, endpoint, session, device, connector, codecs, proxy, mailbox, system and security parameters.

Configuring the Agent's DN

Set the following `TServer` section option for the DNs of the Place to which the agent is logging in:

- `sip-cti-control` = `talk,hold,dtmf`

> **Important**
>
> This option is mandatory to use third-party call control on the SIP device.

For information about configuring DN objects, see the Genesys Administrator Extension Help.

Configuring SIP Server

Genesys recommends setting the following SIP Server options:

- `dual-dialog-enabled=true` (default value)
- `make-call-rfc3725-flow=1` (allows for better and/or simpler codec negotiation)
- `ring-tone-on-make-call=true` (default value)
- `use-register-for-service-state=true`

For more information about these options, see the SIP Server Deployment Guide.

Suppressing the Ringtone

The ringtone is generated for all incoming call to the Genesys Softphone. 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 Genesys Softphone in the contact center is configured with the `ringing_enabled` option set to 1, the SIP Server `make-call-alert-info` option should be set to one of the specified values.

Single sign on with Workspace Web Edition

Genesys Softphone includes an HTTP/HTTPS connector to simplify using Genesys Softphone with Workspace Web Edition (WWE):

- Single sign-on—WWE controls the SIP settings for Softphone based on explicit WWE centralized options and agent login credentials (Place and DN).
- Simplified deployment—each agent workstation runs the same application and configuration files, avoiding workstation specific configuration.
- Password authentication—WWE passes the DN password as one of the parameters through the Genesys Softphone connector to allow the Softphone to securely login to SIP Server and avoid the need for MPLS.

Configuring Softphone for Workspace Web Edition

1. Create a common **Softphone.config** configuration file for all workstations. Uncomment and configure the options in the **connector** section of the **policy** domain:

```
<Container name ="Genesys">
...
        <domain name="policy">
        ...
                <section name="connector">

                <!-- Activates HTTP or HTTPS communication.
                Requires a port defined in the port option. -->
                  <setting name="protocol" value="http"/>

                  <!-- Specifies the port used when communicating in HTTP or HTTPS -->
                  <setting name="port" value="8000"/>

                  <!-- Activates the SESSIONID in cookies -->
                <setting name="enable_sessionid" value="1"/>

                <!-- Gives a thumbprint string value Workspace
                uses to select a certificate if the 'protocol' option
                is set to HTTPS. -->
                <setting name="certificate_search_value" value="55 75 66 dd af 08 23 b6
18 80 fd 19 69 f8 4a 3d e5 c7 94 a5"/>

                <!-- Specifies if the Softphone application is auto started
                or started by the client application.-->
                <setting name="standalone" value="1"/>

                </section>
        ...
        </domain>
...
</Container>
```

   You must synchronize the values of the **protocol** (HTTP or HTTPS) and **port** settings with the SIP Endpoint connectivity option configured on WWE side, see the **sipendpoint.uri** option in the WWE SIP Endpoint configuration page.

When you specify HTTPS in the **protocol** setting you must configure the **certificate_search_value** setting so Genesys Softphone can open a secured port for WWE to send HTTPS requests. You must populate this setting with a thumbprint accessible from the Certificate Store of the agent workstation. To get the same thumbprint configured on all Softphone instances, Genesys recommends that you generate a wildcard certificate for the domain to which the agents belong and make the certificate available to all agents through regular Microsoft Windows GPO rules.

Configure additional Softphone options in your common configuration file.

2. Install Genesys Softphone and your common configuration file on each agent workstation. This is commonly done by using products like Microsoft SMS.

   Once installed, agents can now login using WWE and use Softphone as the SIP endpoint.

Overriding option values

You can override most Softphone options when you provision Workspace Web Edition options. You can override all options in the **proxies** and **system** domain and you can override the **endpoint**, **session**, and **device** sections of the **policy** domain.

Options in the **Connector** section of the **policy** domain must be specified in the configuration file; these cannot be overridden. WWE implicitly controls configuration for options in the **Basic** container to enable single sign-on with WWE.

Overriding an Option

To override a Softphone option when provisioning WWE, convert the option to the following format:

```
sipendpoint.<domain>.<section>.<setting>
```

For example, to override the **ringing_file** setting in the **session** section, configure **sipendpoint.policy.session.ringing_file** in your WWE provisioning. See the options reference for a list of Softphone settings.

Codec Priority

The **sipendpoint.codecs.<codec_name>.priority** option is superseded for assigning priority to the ordering of Codecs. Use the **enabled** section of the **codecs** domain in the **Softphone.config** configuration file to specify the order in which audio codecs are given priority.

> ### Tip
>
> For more details, refer to Working with Codec Priorities in the *SIP Endpoint SDK Developer's Guide 9.0.0NET*.

For example:

```
<domain name="codecs">
  <section name="enabled">
    <setting name="audio" value="opus,pcmu,pcma,G722,iSAC/16000,G729"/>
  </section>
  <section name="PCMU/8000"/>
```

```
    <section name="PCMA/8000"/>
    <section name="G722/16000"/>
```

> Important
>
> In the above examples, the "/<number> after the section name represents the clock rate of the codec.

> Warning
>
> Any codec that is not explicitly included in the **enabled** section will not be used, even if the section for that codec is present in the configuration file or the Genesys Configuration Layer.

To specify the priority of enabled codecs, use the **sipendpoint.codecs.enabled.audio** option in the configuration layer.

For example:

```
sipendpoint.codecs.enabled.audio, "iLBC,G722"
```

To use the Genesys SIP Endpoint SDK 9.0 **enabled** section, follow these guidelines:

- Codec names are *case-insensitive*. You can omit the clock rate portion of the section name unless needed to discriminate between two sections with the same name. The clock rate portion must be provided for **iSAC**.
- Specify codec parameters as a comma-separated list in parenthesis after an equals sign. You can use abbreviations such as "pt" for "payload_type".
- If there are codec conflicts, the value in the **enabled** section takes precedence over value in corresponding codec section, regardless of whether those values come from the configuration file or the Genesys Configuration Layer. For example:

  ```
  <setting name="audio" value="g729=(fmtp='annexb=no'),opus=(pt=125),pcmu,pcma"/>
  <setting name="video" value="h264=(pt=120,fmtp='profile-level-id=420028')"/>
  ```

- If codec parameters are specified in-line (or a particular codec does not require any parameters, such as the PCMU and PCMA codecs), then a separate codec section is not necessary. In any case, codecs specified in the "enabled" section do not require presence of corresponding section to take effect.
- If the **enabled** section is not present, or both "audio" and "video" settings have empty values, then the 8.5.400.11 and lower method of setting priorities, based on the setting order, is applied.

Signing on with WWE

Before starting WWE, agents need to have Softphone running. Administrators can specify that Softphone starts automatically when the Windows user logs in or agents can startup Softphone

User interface and call controls

When using Softphone with WWE, Softphone disables its default user interface. Instead, agents can use the WWE user interface for call controls, mute, and volume control. For information on the WWE user interface, see the WWE Help.

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 the 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:por
		server		The SIP Server or Proxy location for the first user. Included in the SIP URI—for example, <sip:DN0@**serverHostName0:p**
		protocol		The transport procotcol 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	A value of IPv4 means that the application selects an available local IPv4 address; IPv6 addresses are ignored. 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. A value of IPv6,IPv4 means that the application selects an IPv6 address if one exists. If not, an available IPv4 address is selected. Default: IPv4. NOTE: This parameter has no effect if the public_address option specifies an explicit IP address.
		public_address	String	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. **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:B3

Domain	Section	Setting	Values	Description
				`FF: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: • `$auto`—The GSP selects the first valid IP address on the first network adapter that is active (status=up) and has the default gateway configured. IP family preference is specified by the **policy.endpoint.ip_versions** setting. • `$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
				• `$fqdn`—The GSP retrieves the fully qualified DNS name of the local computer. The GSP uses the `GetComputerNameEx` function with parameter `ComputerNameDnsFullyQualified`. • An adapter name or part of an adapter name prefixed with `$`. For example, `$Local Area Connection 2` or `$Local`. The specified name must be different from the special values `$auto`, `$ipv4`, `$host`, and `$fqdn`. **Default Value:** Empty string which is fully equivalent to the `$auto` value. If the value is specified as an explicit host name, FQDN, or `$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.
		include_mac_address	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	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

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 suppresion 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	Defaul 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
				ringtone 1 = Play ringtone through system default device only. Configure media in `system.media.ringing_file`. 2 = Play ringtone through communication device (headset) only. Configure media in `policy.session.ringing_file`. 3 = Play ringtone through both devices at the same time. 4 = Play ringtone through separate ringer device, specified by policy.device.ringer_device. Default Value: 1 Specifies whether to enable the ringing tone and on which device to play the media file.
		ringing_timeout	Number	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	String	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. Default Value: `ringing.wav` Specifies the audio file that is played in the audio out device (headset) 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-

Domain	Section	Setting	Values	Description
				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.
	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 `audio_in_device` and `audio_out_device` 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 `certificate_search_value` 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
				the period specified by `regInterval`. 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.
		reg_match_received_rport	Number	DEPRECATED 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.
		reg_timeout	Number	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.
	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`	Valid Values: `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 Deafult 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.
		log_expire	`false` Number Number `file` Number day	Valid Values: `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` Deafult 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.
		log_time_convert	`local` `utc`	Valid Values: `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

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 Defaul 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 defualt 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.

Using the Genesys Softphone

[**Modified:** 8.5.4]

This topic describes how to use the Genesys Softphone.

Starting the Genesys Softphone

[**Modified:** 8.5.4]

You can start the Genesys Softphone in one of two ways:

- If your administrator has set up Genesys Softphone to automatically launch when Windows starts up, you do not have to start Genesys Softphone yourself. [**Added:** 8.5.4]
- Double-click the Genesys Softphone shortcut in your **Start** Menu.

To open the Genesys Softphone UI, right-click the Genesys Softphone (link=) icon from the Icon Tray:

center

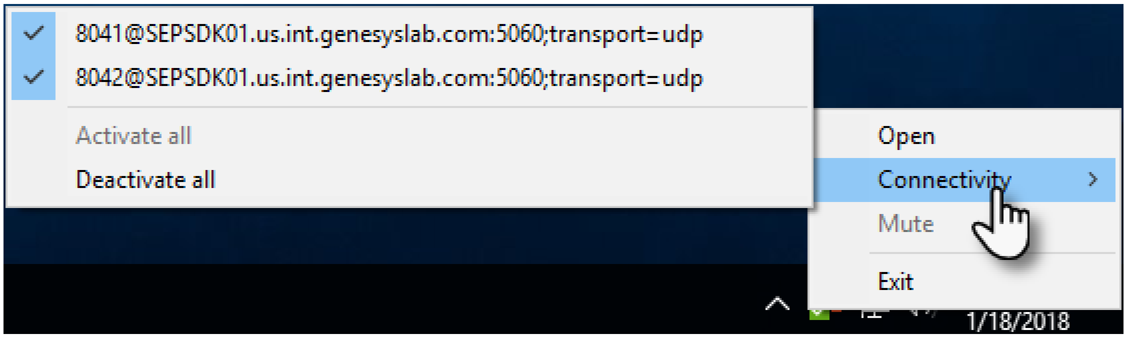
and select **Open**.

> Important
>
> The Genesys Softphone UI is not available in Connector Mode.

Activating and Registering the User

When the Genesys Softphone first starts, it reads the user's information from the `Softphone.cfg` file, and automatically registers the user.

To verify that the user is registered, after starting the Genesys Softphone, right-click the softphone icon from the Icon Tray and hover over the **Connectivity** menu. You can register or un-register a connection by clicking and toggling the check marks. The notification area shows that the Softphone is active and ready to take calls.


✓ 8041@SEPSDK01.us.int.genesyslab.com:5060;transport=udp
✓ 8042@SEPSDK01.us.int.genesyslab.com:5060;transport=udp
Activate all
Deactivate all
Open
Connectivity ›
Mute
Exit
1/18/2018

Selecting the Input and Output Devices

The Genesys Softphone configures the input and output devices during start-up when it reads the list of devices from the Softphone.config file. However, if required, the softphone user can change the brand of device used while the Genesys Softphone is running.

To select an input or output device:

1. In the application, click the **devices** tab. center
2. Select the appropriate microphone from the **Input Device** drop-down list.
3. Select the appropriate speaker from the **Output Device** drop-down list.

Viewing the Softphone Users and Status

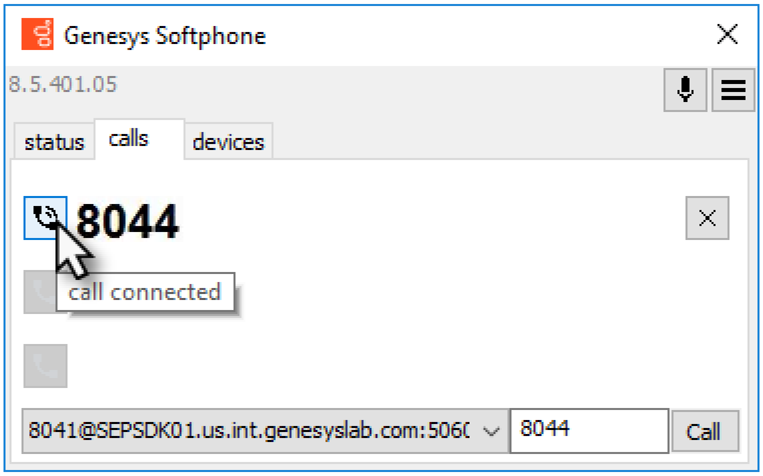
Each Genesys Softphone instance can have up to six SIP user accounts configured.

To view the number of users configured and their statuses, right-click the softphone icon, and click **Open**. The **Genesys Softphone** window displays. Click the **status** tab.

center

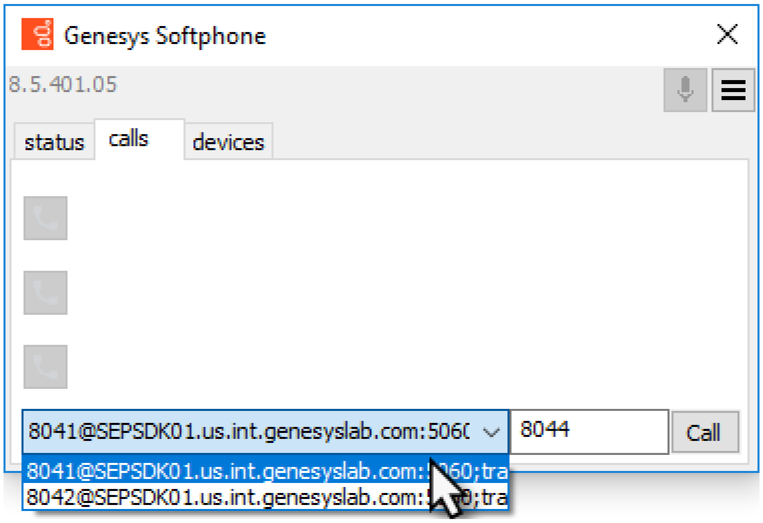
Making and Receiving Calls

You can make and receive calls from the **calls** tab.



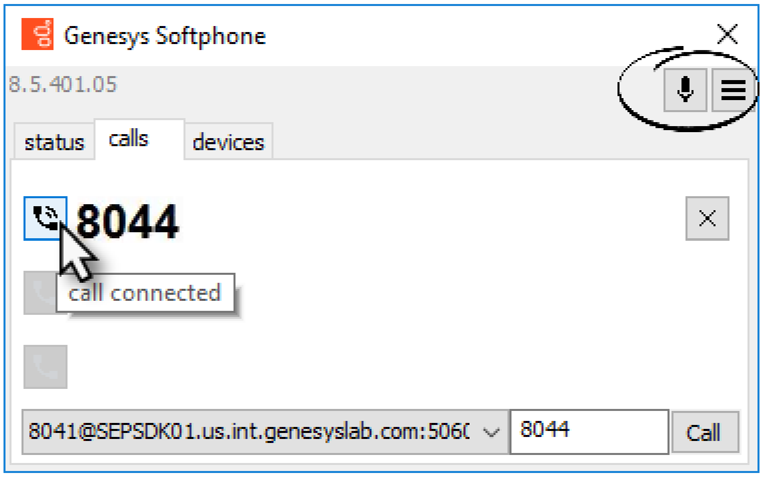
From this tab, you can perform the following operations:

- Answer an incoming call—click the button of an *alerting* call to answer. If you were on another call, that call will be placed on hold.
- Hold a call—when you switch to another call, the currently active call is placed on hold.
- Retrieve a call—click the the line button of a call on hold to retrieve that call.
- Hangup a call—click the hangup button to terminate a call. You can terminate calls that are on hold.
- Dial and make a call—you can make a call by selecting an originating account (connection) from the connections combo box, entering a destination number, and clicking **Call**. Making a new call while another call is active places the existing call on hold.


Genesys Softphone
8.5.401.05
status
calls
devices
8041@SEPSDK01.us.int.genesyslab.com:506(
8044
Call
8041@SEPSDK01.us.int.genesyslab.com:5060;tra
8042@SEPSDK01.us.int.genesyslab.com:5060;tra

Muting the Microphone

The microphone button shows the current mute status, either muted or un-muted. Clicking the microphone button changes the status.



Mute/un-mute functionality works on the application level and not the system level:

- The mute button is only available when there is an active call.
- Muting the microphone in the Softphone is done on the session level. The mute status does not depend on the selected devices nor on device presence and status. A session may be muted even if a microphone is not plugged in.

You may also mute/un-mute the microphone from the tray icon menu. To mute/un-mute the input device:

1. Right-click the Softphone icon, and click **Mute**.
2. From the same menu, click **Un-mute** un-mute the input device.

> ### Important
> The mute menu item is clickable only when the Genesys Softphone is in an active session.