Genesys Softphone Deployment Guide

Genesys Softphone Current

12/19/2024

Table of Contents

Genesys Softphone Deployment and User Guide

Version 9.0.020.10

9.x **Billing Data Server** is part of 9.x, which can include component releases from both 9.1.x, 9.0.x, and 8.5.x code streams. See Billing Data Server to check which component releases are part of 9.x. **Genesys Decisions** is part of 9.x, which can include component releases from both 9.1.x, 9.0.x, and 8.5.x code streams. See Genesys Decisions to check which component releases are part of 9.x. **Genesys Softphone** is part of 9.x, which can include component releases from both 9.1.x, 9.0.x, and 8.5.x code streams. See Genesys Softphone to check which component releases are part of 9.x. **Genesys Widgets** is part of 9.x, which can include component releases from both 9.1.x, 9.0.x, and 8.5.x code streams. See Genesys Widgets to check which component releases are part of 9.x. **Interaction Server** is part of 9.x, which can include component releases from both 9.1.x, 9.0.x, and 8.5.x code streams. See Interaction Server to check which component releases are part of 9.x.

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

About this document

The following topics are covered in this document:

Overview

This section introduces you to the features of Genesys Softphone.

Architecture

Features and functionality

Deployment

This section explains how to deploy Genesys Softphone.

Installation

Configuration

How to use

This section explains how to use Genesys Softphone.

Using the Genesys Softphone

Configuration Options Reference

Configuring Workspace Desktop Edition to use Genesys Softphone

Single sign on with Workspace Web Edition

Audio device settings

What's new in Genesys Softphone?

Here is a list of major changes for each specified release of Genesys Softphone:

Genesys Softphone 9.0.020.10

The following content has been added to the Genesys Softphone Deployment Guide for 9.0.020.10:

- To support the call waiting tone, the following options have been added to the Genesys Softphone options:
  - `callwait_tone_enabled`
  - `callwait_tone_file`
- To support improved automatic headset selection, the following option is added to the Genesys Softphone options:
  - `policy.device.include_headset`
- Support for VMWare Horizon 8 support on HP Thinclient with ThinPro OS deployment.
- Support for 64-bit deployment of Genesys Softphone.
- Refer to the *Supported Operating Environment Reference Guide* for information about discontinued support Microsoft Windows 7 and 8, and Windows Server 2012 and 2016.

Genesys Softphone 9.0.007.09

The following content has been added to the Genesys Softphone Deployment Guide for 9.0.007.09:

- Support for the Genesys Softphone VDI Adapter in an eLux environment.

Genesys Softphone 9.0.006.02

The following content has been added to the Genesys Softphone Deployment Guide for 9.0.006.02:

- policy.endpoint.defer_device_release to control the delay period for releasing audio devices after the audio stream has stopped.

Genesys Softphone 9.0.002.06

The following content has been added to the Genesys Softphone Deployment Guide for 9.0.002.06:

- policy.endpoint.public_address:$net:<subnet> to support dynamic VPN connections.
- policy.session.rx_agc_mode to enable and disable Receiving-side Automatic Gain Control (Rx AGC)
- policy.security.use_srtp has been extended with new valid values.

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.

Overview

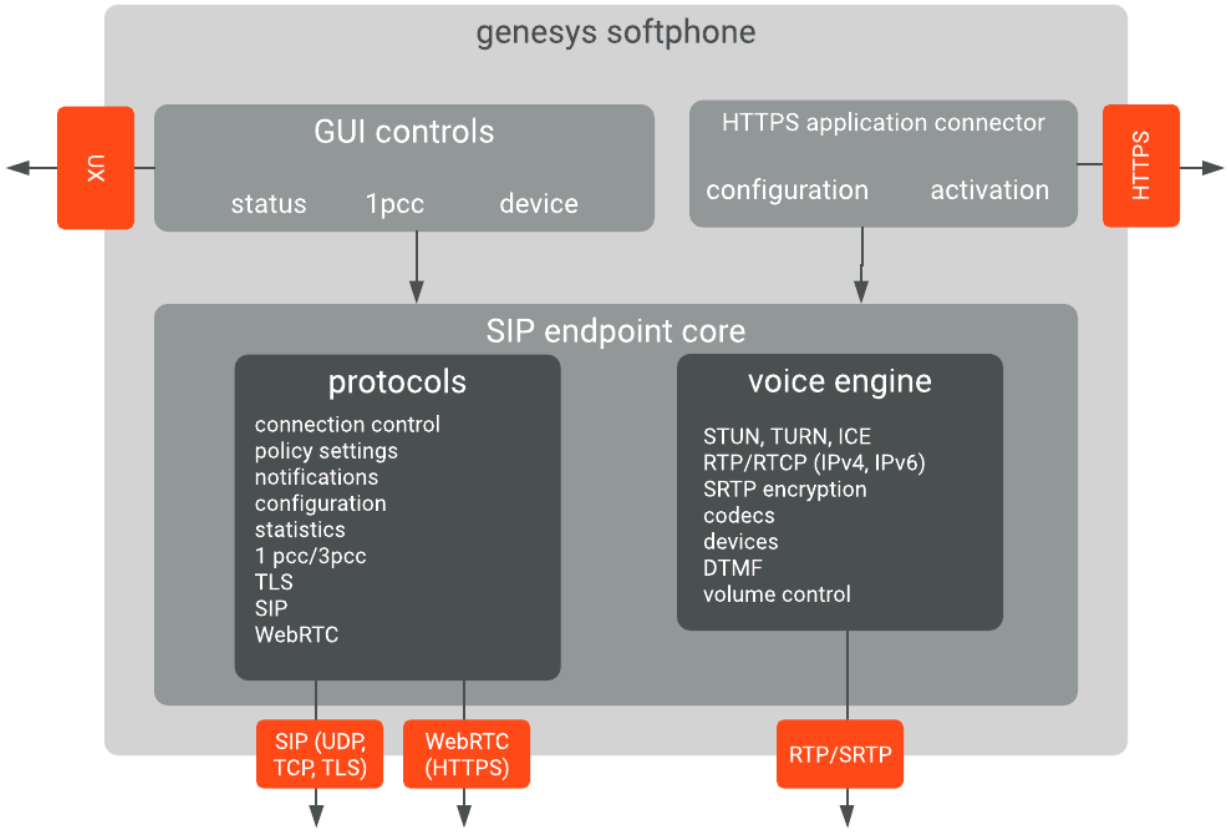
This article describes the Genesys Softphone architecture in your environment. It covers both standard and Virtual Desktop Infrastructure (VDI) installations.

Architecture

The Genesys Softphone embeds the Genesys SIP Endpoint Core Library to enable the use of the SIP-based third-party call control functionality.

Standard Architecture

The following diagram illustrates the Genesys Softphone architecture when it is installed on a physical workstation as a standard executable, summarizing all product functionalities (as opposed to being installed in a virtualized environment):



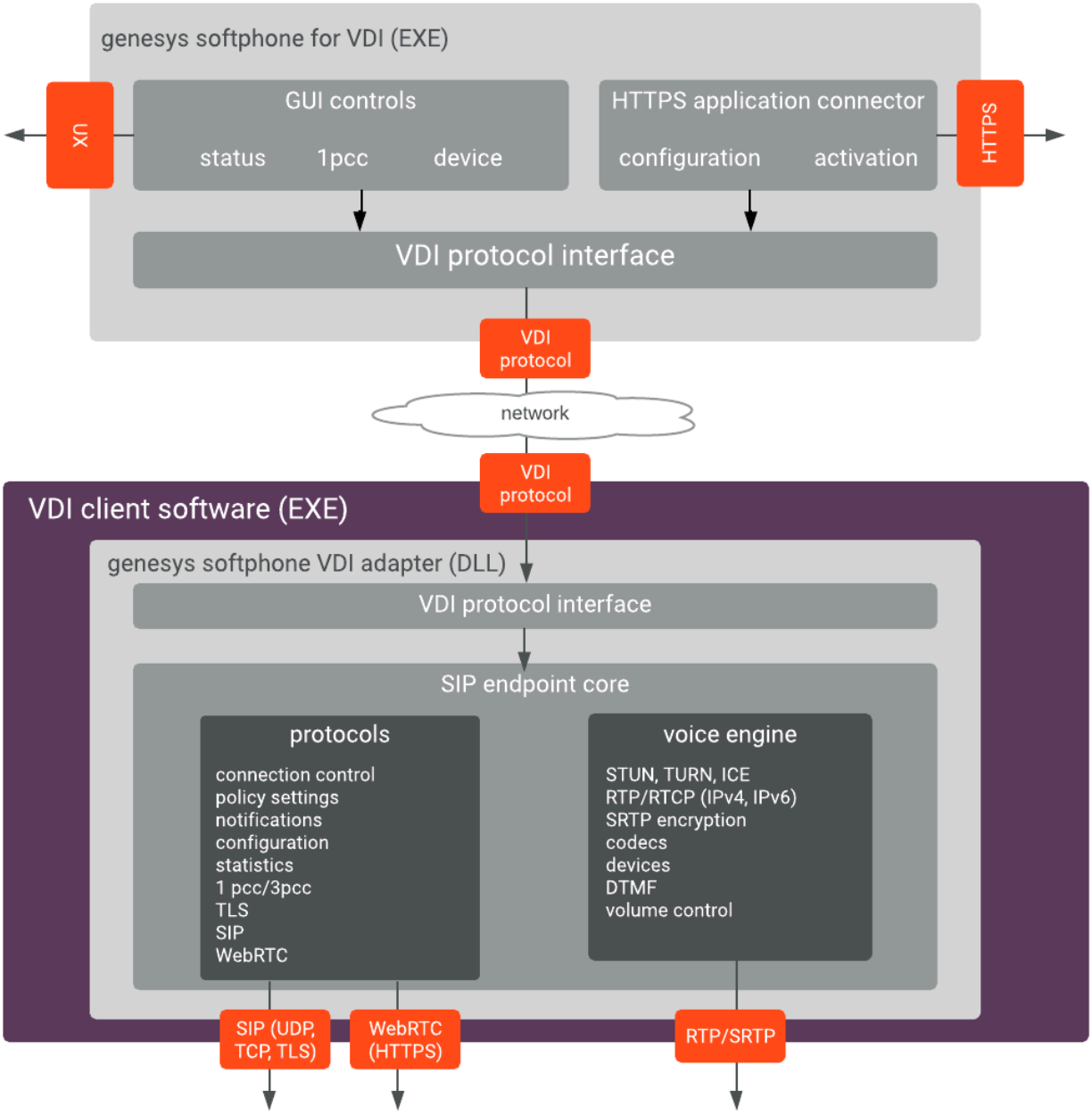
Architecture in VDI Environments

Genesys Softphone supports the Citrix Virtual Desktop Infrastructure (VDI). When deployed in a virtualized environment, the Genesys Softphone software is deployed in two parts:

- The application layer, running in the virtualized system. This is the Genesys Softphone executable. The user interface and connectivity with other applications, such as Workspace Desktop Edition and Workspace Web Edition, run in the application layer. You install this part through the Genesys Softphone installation package by selecting the **Citrix** installation option.
- The signaling protocols, media protocols, and audio device management. These functionalities are off-loaded to the physical workstation to optimize call quality and ensure network and data center scalability. These functionalities are delivered as a plug-in (DLL) to the VDI Client runtime (Citrix Workspace app, previously known as Citrix Receiver). The plugin is deployed by the Genesys Softphone VDI Adapter installation package.

The two Software parts communicate over the Citrix ICA proprietary protocol already established for standard Citrix operations; therefore, there is no need for you to configure any extra connectivity settings.

The following diagram illustrates the Genesys Softphone architecture in the Citrix VDI environment:



Features and functionality

Genesys Softphone media stack is based on Google's open source WebRTC Native Code package. Softphone includes an adaptive jitter buffer, Packet Loss Concealment (PLC), echo cancellation, and noise reduction. For more information refer to SDK for .NET.

The following are the standard features and functions of Genesys Softphone.

DTMF signaling

Genesys Softphone supports Dual-Tone Multi-Frequency (DTMF) signaling according to the RFC 2833 standard for third-party call control. DTMF is a method used to dial telephone numbers or to issue commands to switching systems. DTMF is widely used for telecommunication signaling between telephone handsets and switching centers over analog telephone lines in voice-frequency bands.

After receiving a NOTIFY with DTMF event, the Softphone endpoint generates DTMF signals using one of the three possible methods you can specify through configuration:

- InbandRTP
- RFC 2833
- SIP INFO message

Third-party call control

The following third-party call control scenarios are supported after Genesys Softphone endpoint has registered on Genesys SIP Server:

- 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

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

Security

Genesys Softphone supports the following security protocol:

- TLS v1.2
- TLS v1.3 (starting from 9.0.100.06)

For more information about security, refer to the *Genesys Security Guide*

Virtual Desktop Infrastructure (VDI)

Genesys Softphone supports Virtual Desktop Infrastructure (VDI) to enable agents to use Softphone in a VDI environment.

Softphone can be deployed in a Citrix virtual environment.

- Prerequisites for installing Softphone in a Citrix VDI environment
- Installing the Genesys Softphone VDI Adapter

Localization

Starting from release 9.0.012.04, Genesys Softphone can be presented in various languages.

In Connector Mode, some agent applications like Workspace Web Edition can automatically align the language with the one selected in the controlling application. In other cases, the agent can select the language using the appropriate menu.

Deploying Genesys Softphone

This article describes how to install and configure Genesys Softphone in both standard and Virtual Desktop Infrastructure (VDI) environments.

Environment prerequisites

Ensure that your environment meets the prerequisites described in the following sections. This section covers the prerequisites for Genesys Softphone 9.0.1 and lower versions as well.

There is a prominent difference in using **Visual C++ Redistributable Packages for Visual Studio 2019** (required for Genesys Softphone 9.0.1) and **Visual C++ Redistributable Packages for Visual Studio 2013** (required for Genesys Softphone 9.0.0). These differences are noted in the respective procedures for user's convenience. Unless explicitly noted, all other prerequisites are required for installing Genesys Softphone in the environment you chose to deploy the software.

Supported operating systems

Refer to the Genesys Softphone and the Virtualization Platform Support topics in the *Genesys Supported Operating Environment Reference Manual* for a list of the latest supported operating systems.

Prerequisites for a full deployment of Genesys Softphone on a physical workstation

To work with Genesys Softphone, ensure that your system meets the software requirements established in the *Genesys Supported Operating Environment Reference Manual*, and meets the following minimum software requirements:

- Visual C++ Redistributable Packages for Visual Studio 2019 (or above) is required for Genesys Softphone VDI Adapter 9.0.1:
  - The 64-bit version of the redistributable is installed by the Genesys Softphone 64-bit installer.
- Visual C++ Redistributable Packages for Visual Studio 2013 is required for Genesys Softphone VDI Adapter 9.0.0:
  - The 32-bit version of the redistributable is installed by the Genesys Softphone 32-bit installer.
  - The 64-bit version of the redistributable is not installed by the Genesys Softphone 64-bit installer, so you must install `vcredist64.exe` from the above link when the 64-bit version of Genesys Softphone is installed.
- .NET Framework 4.0 or higher: This framework is used only when the administrator installs Genesys Softphone with an HTTPS connector based on a *self-signed certificate*.
- Quality of service (QoS) for voice, either one-to-one or on a conference connection capability, requires the following:

- ≤ 150 ms of one-way latency from mouth to ear (per the ITU G.114 standard)
- ≤ 30 ms jitter
- ≤ 1 percent packet loss
- 17 to 106 kbps of guaranteed priority bandwidth per call (depending on the sampling rate, codec, and Layer 2 overhead)
- 150 bps (plus Layer 2 overhead) per phone of guaranteed bandwidth for voice control traffic

> **Important**
>
> QoS policies are managed by the operating system. To configure a QoS policy in Windows, refer to Quality of Service (QoS) Policy in the Microsoft documentation.

- A headset or other microphone and speaker audio device that is supported by Windows OS installed on the workstation.

Prerequisites for deployment in a VDI environment

To work with Genesys Softphone in a VDI environment, ensure that your system meets the software requirements established in the *Genesys Supported Operating Environment Reference Manual*, and meets the following minimum software requirements:

1. On the workstation running the VDI client:
   - For Citrix Workspace (formerly Citrix Receiver) for Windows (applicable to Genesys Softphone VDI Adapter 9.0.0 and 9.0.1):
     - Visual C++ Redistributable Packages for Visual Studio 2013 (32-bit version). The Genesys installation package 32-bit installs this redistributable package on the workstation where it is executed.
   - For VMWare Horizon on Windows,
     - Visual C++ Redistributable Packages for Visual Studio 2019 (or above) is required for Genesys Softphone VDI Adapter 9.0.1. The 64-bit package of the Genesys Softphone VDI Adapter installs this redistributable package on the workstation where it is executed.
     - Visual C++ Redistributable Packages for Visual Studio 2013 is required for Genesys Softphone version 9.0.0. You must install the `vcredist64.exe` from the link location before running the Genesys Softphone VDI Adapter for VMWare Horizon.
   - Quality of service (QoS) for voice, either one-to-one or on a conference connection capability, requires the following:
     - ≤ 150 ms of one-way latency from mouth to ear (per the ITU G.114 standard)
     - ≤ 30 ms jitter
     - ≤ 1 percent packet loss
     - 17 to 106 kbps of guaranteed priority bandwidth per call (depending on the sampling rate, codec, and Layer 2 overhead)
     - 150 bps (plus Layer 2 overhead) per phone of guaranteed bandwidth for voice control traffic

> **Important**
>
> QoS policies are managed by the operating system. To configure a QoS policy, refer to the documentation for your platform.

- A headset or other microphone and speaker audio device that is supported by the OS installed on either the client or the host.

2. On the workstation used to build deployments for running eLux systems:
   - Virtual Driver for Citrix shared object.
   - **libgsecurity** module.
   - Scout Enterprise ELIAS tool.
   - Windows workstation from which to run the Genesys Softphone VDI Adapter executable.
3. On the workstation used to build deployments for HP ThinPro systems:
   - The packaging tool recommended by your HP vendor.
4. On the VDI environment (Citrix Virtual Application/Desktop or VMWare Horizon server) that runs the application layer of the Genesys Softphone runtime:
   - Visual C++ Redistributable Packages for Visual Studio 2019 (or above) is required for Genesys Softphone version 9.0.1.
     - The 64-bit version of the redistributable is installed by the Genesys Softphone 64-bit installer.
   - Visual C++ Redistributable Packages for Visual Studio 2013 is required for Genesys Softphone version 9.0.0.
     - The 32-bit version of the redistributable is installed by the Genesys Softphone 32-bit installer.
     - The 64-bit version of the redistributable is not installed by the Genesys Softphone 64-bit installer. You must install `vcredist64.exe` from the link location when the 64-bit version of Genesys Softphone is installed.
   - .NET Framework 4.0 or higher: This framework is used only when the administrator installs Genesys Softphone with an HTTPS connector based on a *self-signed certificate*.
5. In the Citrix Virtual Application/Desktop settings:
   - In Citrix Virtual Apps and Desktop LSTR 2203, the **virtual channel allow list** feature is enabled by default. This means that in this Citrix release, and any older deployment where administrator explicitly enables this feature, only the Virtual Channels shipped by Citrix are authorized by default.

     In this deployment, the administrator must explicitly authorize the Genesys Softphone Virtual Channel to make Genesys Softphone for VDI operate successfully. This can be done using the instructions on the Citrix Virtual Channel Security page. As a Citrix Administrator, you need to add a Virtual channel allow list policy and configure it with the value:

```
GENESYS, <Genesys_Softphone_Installation_Path>\GenesysSoftphone_Citrix.exe
```

> **Important**
>
> To use Workspace Desktop Edition and Genesys Screen Recording Service with Genesys Softphone in a VDI environment such as Citrix Xenapp, you must configure the screen-recording.client.address option to point to the SRS Loopback address.

Installing Genesys Softphone for Windows

(For information on installing Genesys Softphone in a VDI environment see Installing the Genesys Softphone VDI Adapter)

> **Tip**
>
> Beginning with Genesys Softphone 9.0.020.08, multiple installation packages are available from the download center, 32-bit and 64-bit. Ensure that you download the correct package for your environment.

To install Genesys Softphone, follow these steps:

1. Download the Genesys Softphone installation package.
2. Double-click the **setup.exe** file located in the **<Genesys Softphone Install Package Directory>\windows** directory to open the **Genesys Installation Wizard**.
3. In the **Welcome to the Installation** window, click **Next**.
4. In the **Choose Destination Location** window, click **Next** to accept the default destination folder, or click **Browse** to select another destination location.
5. In the **Deployment Type** window, click **Standard** or **VDI: Citrix or VMware Horizon** (for virtualization deployments only), and then click **Next**.
6. In the **Startup and Secure Connection options** window, choose one or more of the following options, and then click **Next**:
   - Auto Startup: Specifies that Genesys Softphone launches when Windows starts. Agents do not have to manually launch Genesys Softphone before they launch Workspace or other agent desktops.
   - Enable Dynamic Configuration Connector: Specifies that Workspace Web Edition (Agent Desktop) is allowed to dynamically configure Genesys Softphone when it is launched.

     If you select this option, the **Dynamic Configuration Connector Parameters** window is displayed.

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

     b. Enable HTTPS secure connections (optional). If you select this option, 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 the machine level in the workstation where **setup.exe** is executed.

- Certificate Authorities from the Windows Certificate Store.

> **Important**
>
> To properly install the self-signed certificate, .NET Framework 4.0 or higher is mandatory.

7. If you do not select the **Enable Dynamic Configuration Connector** option and are upgrading Genesys Softphone, you can select **Configuration Option** to preserve the existing configuration file. Otherwise, the installation process overwrites the existing configuration file with the new upgrade version. Click **Next**.
8. In the **Ready to Install** window, select **Install**. The wizard installs Genesys Softphone and all associated files in the selected directory and displays the **Installation Status** window. The installation might take several minutes.
9. In the **Installation Complete** window, select **Finish**.

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

> **Important**
>
> For information about Genesys Softphone deployment and configuration for Workspace Desktop Edition (WDE), see Configuring Workspace Desktop Edition to use Genesys Softphone

Installing Genesys Softphone in Silent mode for Windows

To install 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 directory. For example, **InstallPath=C:\GCTI\Genesys Softphone**.
   - Specify if Genesys Softphone is a physical workstation ("Std") or on a desktop/application virtualization environment (Citrix or VMWare Horizon) ("Citrix") by using the **DeploymentType=<Std or Citrix>** parameter.
   - Specify whether Genesys Softphone starts automatically when Windows starts 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:
  - If the Connector is enabled, specify the Connector Port 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 certificate type 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 the version, build number, and if the existing configuration file is to be preserved ("preserve") or replaced ("nopreserve") before the upgrade:
  - **IPVersion= <current (before upgrade) version of Genesys Softphone on this box>**
  - **IPBuildNumber= <current (before upgrade) build number of Genesys Softphone on this box>**
  - **OldCfgFile= <preserve or nopreserve the existing configuration file for this upgrade>** (this parameter is ignored if the Connector is enabled)

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** file 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 in apostrophes (') if the parameter contains white space characters.

- Replace `-sl` flag by `-t` for verbose logs of the silent installation process.

The **InstallShield setup.exe** installer 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 Genesys Softphone is installed in the **C:\<Genesys Softphone Directory>**, and that the **silent_setup.log** file has been created in the **C:\GSP** directory.

Installing the Genesys Softphone VDI Adapter (Windows)

If you installed Genesys Softphone in a VDI environment, you must install the Genesys Softphone VDI Adapter on each Windows workstation by following these steps:

1. From the Genesys Download Center, download the Genesys Softphone VDI Adapter package corresponding to your environment:
   - For Citrix, use the Genesys Softphone VDI Adapter 32-bit package.
   - For VMWare Horizon, use the Genesys Softphone VDI Adapter 64-bit package.
2. Double-click the **setup.exe** file located in the **<Genesys Softphone VDI Adapter Install Package Directory>\windows** directory to open the **Genesys Installation Wizard**.
3. In the **Welcome to the Installation** window, click **Next**.
4. In the **Select Operating System** window, select the option that is appropriate for your environment. For Citrix environments, select **Citrix support on Windows**. For VMware Horizon environments, select **VMware Horizon support on Windows**. Click **Next**.
5. If the **Choose Destination Location** window is presented (if installing on VMware Horizon), click **Next** to accept the default destination folder, or click **Browse** to select another destination location.
6. In the **Ready to Install** window, select **Install**. The wizard installs Genesys Softphone VDI Adapter and displays the **Installation Status** window.
7. In the **Installation Complete** window, select **Finish**.

Installing the Genesys Softphone VDI Adapter (eLux)

If you installed Genesys Softphone in a VDI environment, you must install the Genesys Softphone VDI Adapter on each eLux workstation by following these steps:

1. From the Genesys Download Center, download the Genesys Softphone VDI Adapter package 32-bit or 64-bit.
2. Double-click the **setup.exe** file located in the **<Genesys Softphone VDI Adapter Install Package Directory>\windows** directory to open the **Genesys Installation Wizard**.
3. In the **Welcome to the Installation** window, click **Next**.
4. In the **Select Operating System** window, select **eLux**, specify the destination to install the installation package, and click **Next**.
5. In the **Ready to Install** window, select **Install**. The wizard installs Genesys Softphone VDI Adapter and displays the **Installation Status** window.
6. In the **Installation Complete** window, select **Finish**.
   The installation package installs the following items:
   - a Virtual Driver for Citrix shared object
   - a **libgsecurity** module
   - a startup script to update the Citrix **module.ini** config file.

   These files are packaged into an EPM/FPM pair, each with a separate signature file with four files for the VD package and three files with certificates used for signing:
   - **genesysvd-<ip-version>-1.UC_RP6_X64-1.0.fpm**
   - **genesysvd-<ip-version>-1.UC_RP6_X64-1.0.fpm.sig**
   - **genesysvd-<ip-version>-1.UC_RP6_X64-1.0.epm**
   - **genesysvd-<ip-version>-1.UC_RP6_X64-1.0.epm.sig**
   - **certificates_chain_01.pem**: Genesys certificate used for signing packages
   - **certificates_chain_02.pem**: DigiCert Trusted G4 Code Signing CA
   - **certificates_chain_03.pem**: DigiCert Trusted Root G4
7. Import the package files to the existing container and add them to the client image using the Unicon Scout Enterprise ELIAS tool:
   1. Using the **Security / Manage certificates** menu option, import the certificates as trusted.
   2. If the client is configured with **signature check**, the VeriSign Root CA certificate must be installed on each client in the **/setup/cacerts** folder.
   3. To add packages to the container, in ELIAS select the **Container / Import Package** menu option, then select the files with .the **epm** extension.
   4. To update the image definition file (IDF), open it in ELIAS, then add the new package by selecting **Genesys VD for Citrix, <ip-version>** in the right pane and press the **<==** button.
   5. Update the client workstation using the Scout Enterprise Console and perform these steps:
      - Check the firmware configuration of the relevant Thin Clients by selecting **Device**

configuration and then choosing **Firmware**.

- Update the device by selecting the **Commands / Update** option to initiate the update and force a device restart.

Installing the Genesys Softphone VDI Adapter (HP ThinPro)

> **Important**
>
> Beginning with version 9.0.1, Genesys Softphone VDI Adapter for HP ThinPro supports both Citrix and VMWare Horizon environments. Note that the 9.0.0 version supports only VMWare Horizon.

If you installed Genesys Softphone in a VDI environment, you must install the Genesys Softphone plugin for VMWare Horizon and Citrix Client on each HP ThinPro workstation by following these steps:

1. From the Genesys Download Center, download the Genesys Softphone VDI Adapter 32-bit or 64-bit package.
2. To open the **Genesys Installation Wizard**, double-click the **setup.exe** file located in the **<Genesys Softphone VDI Adapter Install Package Directory>\windows** directory.
3. In the **Welcome to the Installation** window, click **Next**.
4. In the **Select Operating System** window, select **HP ThinPro**, specify the destination to install the installation package, and click **Next**.
5. In the **Ready to Install** window, select **Install**. The wizard installs Genesys Softphone VDI Adapter and displays the **Installation Status** window.
6. In the **Installation Complete** window, select **Finish**.
   The installation package installs the following file for the Genesys Softphone plugin for VMWare Horizon and Citrix Client.

   This file is packaged into a DEB file:

   - **vdhgenesys_<ip-version>_amd64.deb**
7. Deploy the Genesys Softphone plugin for VMWare Horizon and Citrix Client on ThinPro host:
   - Manual deployment:
     1. Copy the client-side package to any convenient location accessible by wget or scp.
     2. From the main menu, switch to **Administrator** on the ThinPro host.
     3. To copy the client-side package on ThinPro host, start **Xterm**.
     4. To install the client-side package, run the following commands:

```
fsunlock

dpkg -i vdhgenesys_<ip-version>_amd64.deb

fslock
```

- Bulk deployment:
  Use the packaging tools and procedures provided by HP to build a new ThinPro OS package that contains the Genesys Softphone VDI Adapter Debian package, then distribute it to the HP ThinPro hardware boxes.

Installing Genesys Softphone VDI Adapter in Silent mode

To install Genesys Softphone VDI Adapter in Silent mode, use the Installation Wizard **Silent** arguments as follows:

1. Update the **genesys_silent.ini** file by making the following modifications:
   - Specify if Genesys Softphone VDI Adapter should be installed for Windows (Citrix) ("citrix_windows", only on the 32-bit version), Windows (VMware Horizon) ("vmware_horizon", only on the 64-bit version), eLux ("citrix_elux_5"), or HP ThinPro OS (Citrix and VMware Horizon) ("vmware_pro") by using the **DeploymentType** parameter. For example, **DeploymentType=citrix_windows**.

     > **Important**
     > Beginning with version 9.0.1, the Genesys Softphone VDI Adapter for HP ThinPro supports both Citrix and VMWare Horizon environments. The 9.0.0 version supports only VMWare Horizon.

   - If installing on VMware Horizon, you can choose to install to a specific location by specifying the path with the **InstallPath** parameter. For example, **InstallPath=C:\GCTI\Genesys SoftphoneVDIAdapter**.
   - If installing on eLux5, add the path to the Genesys Softphone VDI Adapter directory using the **InstallPath** parameter. For example, **InstallPath=C:\GCTI\Genesys SoftphoneVDIAdapter**.
2. If you are *upgrading* Genesys Softphone VDI Adpater specify:
   - **IPVersion= <current version of Genesys Softphone VDI Adapter on this box (before upgrade)>**
   - **IPBuildNumber= <current build number of Genesys Softphone VDI Adapter on this box (before upgrade)>**
3. 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 in apostrophes (') if the parameter contains white space characters.

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:\9.0.007.03\windows\b1\ip\genesys_silent.ini' -sl 'C:\GSP\silent_setup.log'"`.

4. After executing this command, verify that Genesys Softphone VDI Adapter is installed in the expected directory, and that the **silent_setup.log** file has been created in the **C:\GSP** directory.

Installing Genesys Softphone for macOS

To install the Genesys Softphone for macOS:

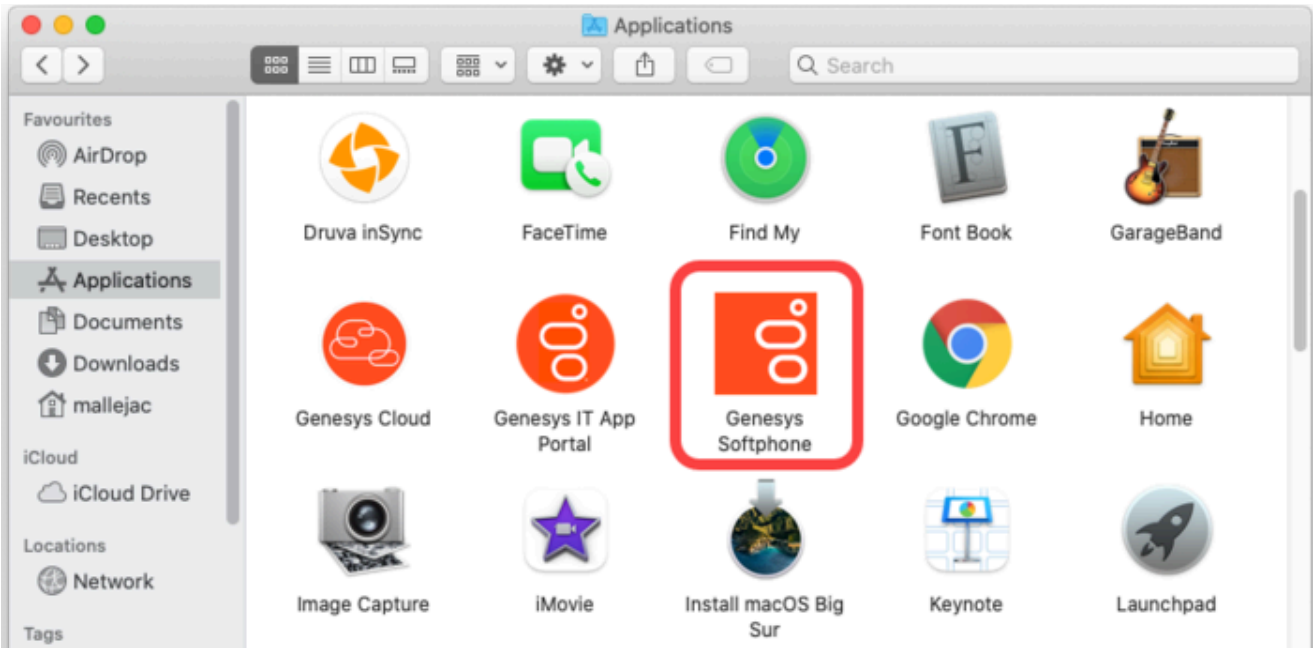
1. Download the Genesys Softphone installation package.
2. Open a Terminal session. From the **<IPversion>/mac/bX/ip** directory path, run the **install.sh** script using administrator privileges:
   ```
   sudo ./install.sh
   ```

> **Important**
>
> If the installation fails due to insufficient macOS user privileges (for example, you receive an error message due to "unidentified developers"), you can perform the following workaround:
>
> - Open a Terminal session and run the following command: `sudo spctl --master-disable`. This allows applications from unidentified developers to be opened.

- Execute the Genesys Softphone installation script.
- When the installation is complete, run the command `sudo spctl --master-enable` to revert the system back to the default privilege settings.

3. At the **Launch Genesys Softphone on MacOS startup** prompt, enter **y** to enable Softphone to run automatically when the agent is opening the OS session or **n** for Softphone to be started manually by agent.
4. At the **Enable connector to allow dynamic configuration by Workspace Web Edition** prompt, enter **n** to select standalone mode or **y** to enable the connector.
   - If you are upgrading Genesys Softphone in standalone mode, you can then enter **n** to overwrite the existing configuration file (**Softphone.config**) or **y** to continue using the existing configuration file.
   - If you choose to enable the connector, confirm the default connector port number (`8000`), or enter the port number you want to use. You can then enter **y** to enable a secure connection (HTTPS) or **n** to use a non-secure connection (HTTP).
5. Enter **y** to accept the destination directory for the installation and continue.
6. After the installation process completes, the script displays messages to confirm the following:
   - The **Tuning** file attributes are automatically tuned.
   - If you enabled the connector with a secure connection (HTTPS), the RSA private key certificate is automatically created and installed.

You can launch Genesys Softphone from the **Applications** folder:



Installing Genesys Softphone in Silent mode for macOS

To install the Genesys Softphone in Silent mode:

1. Update the **genesys_silent.ini** file by making the following modifications:
   - Add the absolute path to the Genesys Softphone directory. For example, **InstallPath= /Applications/Genesys Softphone.app**.
   - Specify whether Genesys Softphone starts automatically when MacOS starts by setting the **AutoStart=<yes or no>** parameter.
   - Specify whether Workspace Web Edition can dynamically modify the Genesys Softphone configuration by setting the **EnableConnector=<yes or no>** parameter.
   - If you are *deploying* Genesys Softphone for Workspace Web Edition dynamic configuration:
     - If the Connector is enabled, specify the Connector Port by setting the **ConnectorPort=<port number>** parameter.
     - Specify whether the connector uses HTTPS secure connection by setting the **SecuredCommunication=<yes or no>** parameter.
   - Specify whether to keep the existing configuration file during upgrades by setting the **PreserveConfigFile=<yes or no>** parameter. If you enter no for this value, the configuration file is overwritten during the upgrade. (This parameter is ignored if the Connector is enabled.)
2. Enter the following command using administrator privileges: `sudo ./install.sh -s -fr /<IPpath>/<IPversion>/mac/bX/ip/genesys_silent.ini -fl /<IPpath>/<IPversion>/mac/bX/ip/genesys_install_result.log` where
   - `<IPpath>` is the path to the installation package.
   - `<IPversion>` is the version of the installation package version you are installing. For example, `9.0.014.12`.

Pre-configuring Genesys Softphone

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

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

The configuration file is organized into *containers*. Each container is divided into *domains* that are further divided into *sections* that hold the *settings* for a group of parameters. The following configuration file examples describe the settings in each container:

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>
```

> **Important**
>
> If Single sign-on is used with Workspace Web Edition or Workspace Desktop Edition, these parameters in configuration file are not taken in account.

Genesys container

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

> **Important**
>
> If single sign-on is used with Workspace Web Edition or Workspace Desktop Edition, these parameters can be overridden. See Overriding option values with options in WWE.

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 application 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

A ringtone is generated for all incoming calls to Genesys Softphone. To suppress the ringtone for third-party call control for the originating DN, configure the following SIP Server option with one of the following values:

- `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, set the SIP Server `make-call-alert-info` option to one of the values specified above.

Conditional auto-answer

Starting from version 9.0.024.06, Genesys Softphone supports conditional auto-answer, based on the value of Alert-Info SIP header in the incoming INVITE. This header can be added by URS when routing call to the agent, using SIP_HEADERS extension in the RouteCall request. For more information, see the SIP Server Deployment Guide. Include the following value to force auto-answer for the call:

```
Alert-Info: <file://null>;info=alert-autoanswer
```

where the header value in single angle brackets is currently ignored by Softphone and only required to comply with SIP standard. The `info` parameter after the semicolon triggers the auto-answer.

Mass deployment on multiple workstations

Genesys Softphone can be distributed to end user workstations through Desktop Configuration Management solutions, such as Microsoft Endpoint Manager (formerly Microsoft SCCM), that enable mass deployments of desktop software.

Although Genesys Softphone is not shipped with a Microsoft Software Installer (MSI), you can repackage **Genesys Softphone setup** into an MSI using the silent installation mode. Next, use a repackaging tool, such as https://www.exemsi.com/ to repackage the MSI. Finally, deploy the resulting MSI package using your Desktop Configuration Manager.

Post-installation procedures

Enabling FIPS

Beginning with the version 9.0.101.xx, Genesys Softphone is Federal Information Processing Standards (FIPS) compliant. This means that Genesys Softphone requires configuring OpenSSL 3.x through the FIPS (**fips.dll**) module.

To enable FIPS,

1. Locate the **fipsinstall.bat** script in the Genesys Softphone installation path.
2. In the Administrator Console, run the **fipsinstall.bat** script.
3. Running the script automatically configures OpenSSL. You can verify the configuration from the following sample output:

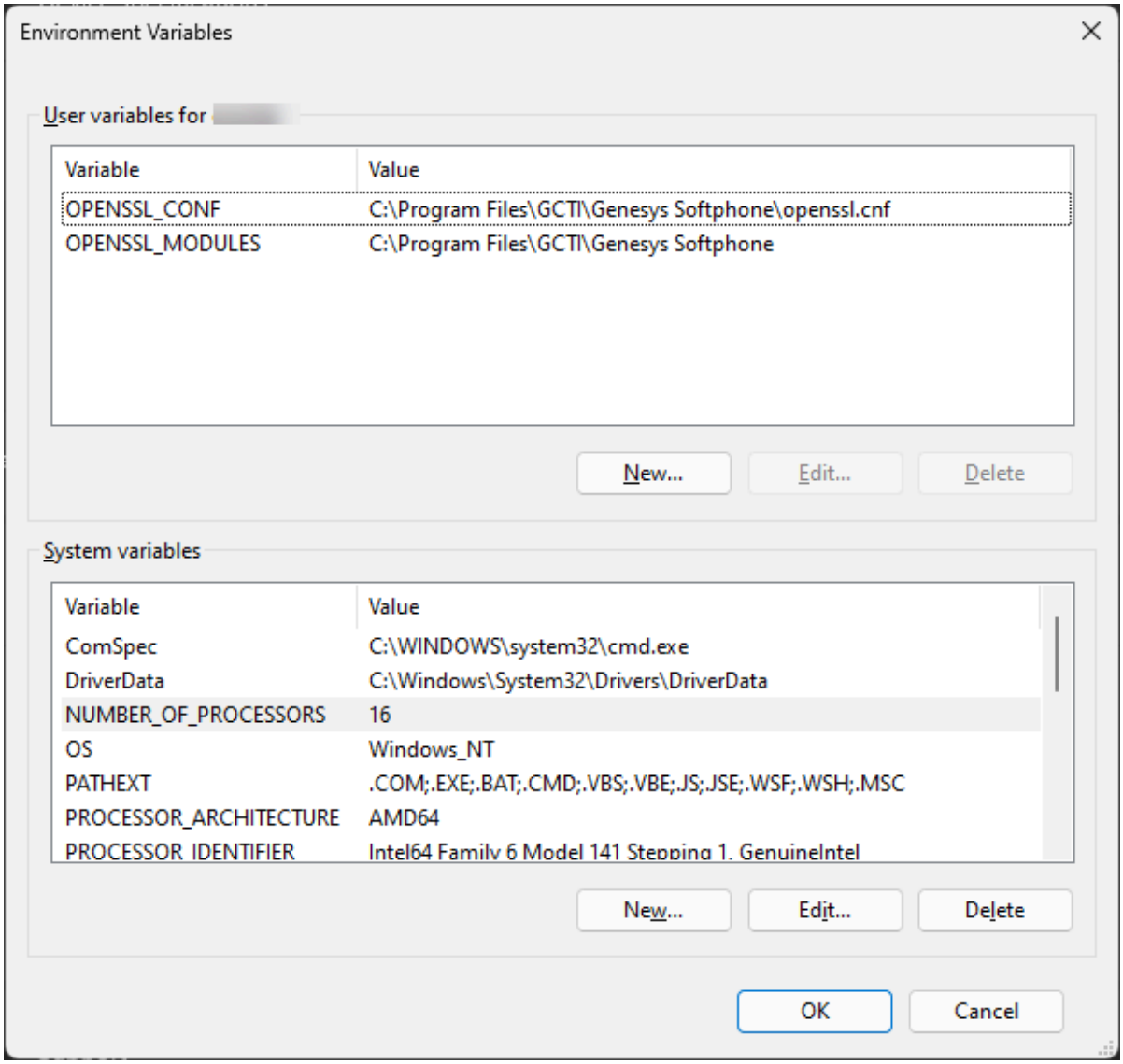
```
C:\Program Files\GCTI\Genesys Softphone>fipsinstall.bat

C:\Program Files\GCTI\Genesys Softphone>echo off
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
```

```
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
For using FIPS security module set the following environment variables:
  set OPENSSL_MODULES=C:\Program Files\GCTI\Genesys Softphone
  set OPENSSL_CONF=C:\Program Files\GCTI\Genesys Softphone\openssl.cnf
```

4. After executing the script, set the following environment variables in the Windows system (see screenshot) to activate the full FIPS compliance.

   - `OPENSSL_MODULES`
   - `OPENSSL_CONF`

   An example setting is shown in the following screenshot.


Environment Variables
User variables for
Variable
Value
OPENSSL_CONF
C:\Program Files\GCTI\Genesys Softphone\openssl.cnf
OPENSSL_MODULES
C:\Program Files\GCTI\Genesys Softphone
New...
Edit...
Delete
System variables
Variable
Value
ComSpec
C:\WINDOWS\system32\cmd.exe
DriverData
C:\Windows\System32\Drivers\DriverData
NUMBER_OF_PROCESSORS
16
OS
Windows_NT
PATHEXT
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE
AMD64
PROCESSOR_IDENTIFIER
Intel64 Family 6 Model 141 Stepping 1, GenuineIntel
New...
Edit...
Delete
OK
Cancel

Single sign-on with Workspace Web Edition

Genesys Softphone includes an HTTP/HTTPS connector to simplify using Genesys Softphone with Workspace Web Edition (WWE). It includes the following features:

- Single sign-on: WWE controls the SIP settings for Genesys Softphone based on explicit WWE centralized options and agent login credentials (Place and DN). Single sign-on (SSO) allows a user to use one set of login credentials (e.g., name and password) to access multiple applications.
- Simplified deployment: each agent workstation runs the same application and configuration files so that you don't have to configure each workstation separately.
- Password authentication: WWE passes the DN password as a parameter through the Genesys Softphone connector to allow Genesys Softphone to securely log into SIP Server so that you do not need Multi-protocol Label Switching (MPLS).

Signing on with WWE

Before starting WWE, agents must have Genesys Softphone running on their workstation. Administrators can specify that Genesys Softphone starts automatically when the Windows user logs in or agents can start Genesys Softphone manually.

User interface and call controls

When using Genesys Softphone with WWE, Genesys 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 *Workspace Web Edition Help*.

> **Important**
>
> In this mode, Genesys Softphone does not prevent the WWE application from claiming WCAG 2.1 levels A and AA when it supports this standard for its own UI.

Configuring Genesys Softphone for Workspace Web Edition

1. The **Softphone.config** configuration file contains a **connector** section in 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 in WWE, see the **sipendpoint.uri** option in the WWE SIP Endpoint configuration page.

When you specify HTTPS in the **protocol** setting, configure the **certificate_search_value** setting so Genesys Softphone can open a secured port for WWE to send HTTPS requests. Populate this setting with a thumbprint accessible from the Certificate Store of the agent workstation. To configure the same thumbprint on all Genesys 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. You can use products like Microsoft SMS to complete this step.

   After the installation is complete, agents can log in using WWE and use Genesys Softphone as the SIP endpoint.

Running WWE and Genesys Softphone in a VDI Environment

If the goal is to run WWE and Genesys Softphone in a VDI environment, and the plan is to have agents use Windows sessions on the same Windows Server, the Virtual IP Loopback feature must be activated to allow successful communication between WWE and Genesys Softphone when multiple users are assigned to the same Windows Server. For more information, see the Virtual IP and virtual loopback page in the Citrix documentation.

In the IP Loopback configuration, register the **genesyssoftphone.exe** executable, as well as the executable name of the browser that is loading WWE (for example, **chrome.exe**, **firefox.exe**, **internetexplorer.exe**, or **microsoftedge.exe**).

Overriding option values with options in WWE

You can override the following Genesys Softphone options when you provision Workspace Web Edition options:

- In the **proxies** and **system** domains, you can override all options.
- In the **policy** domain, you can override **endpoint**, **session**, and **device** sections.

> **Important**
>
> 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.

How to override a Genesys Softphone option

To override a Genesys 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 Genesys Softphone settings.

Codec priority

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"/>
```

> **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 internet Speech Audio Codec (iSAC).
- Specify codec parameters as a comma-separated list in parentheses 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 the corresponding codec section, 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 the presence of a corresponding section to take effect.

Configuring Workspace Desktop Edition to use Genesys Softphone

This article describes how to set up Workspace Desktop Edition (WDE) to work with Genesys Softphone instead of the Workspace SIP Endpoint to handle SIP Voice-over-IP calls. Genesys Softphone provides agents with interface elements in the WDE Voice Interaction window, including muting and volume control for both the microphone channel and the speaker channel of the selected audio device(s) on the agent workstation.

> **Tip**
>
> Any USB headset that is supported by the Windows Operating System works normally with Genesys Softphone.

Other SIP VoIP features included with Genesys Softphone: automatic gain control, beep tone, auto-answer, unavailable headset detection, log-level support, Real-time Transport Protocol (RTP) support, and speaking detection.

Workspace Desktop Edition deployment template

Workspace Desktop Edition provides three templates from which you can choose when you deploy WDE, one for the application, and two optional ones for the Workspace SIP Endpoint. Use the **Workspace_Desktop_Edition_SEP85_851.apd** template when you deploy WDE to use Genesys Softphone. After deploying WDE with this template, install Genesys Softphone and configure WDE as described in this topic.

USB headset configuration

You can use the following options to configure Workspace Desktop Edition to use a headset:

- sipendpoint.policy.device.use_headset: Specifies whether a USB head set is used for voice calls.
- sipendpoint.policy.device.headset_name: Specifies what type of USB headsets that you support in your environment. Use the "|" character to separate the names of different headsets if more than one type is supported. For example: 'Plantro|Jabra'.

If these options are set, and the corresponding USB headset is connected to the agent workstation at start-up time, the headset is selected automatically.

If the configured USB headset is not connected to the agent workstation, then the behavior depends on the following configuration option in the **interaction-workspace** section of the Workspace

Application object:

- sipendpoint.headset-enforce-configured-usage: This option specifies whether the agent must plug in the specified USB headset to complete logging in. When it is set to **false**, and if the headset is not plugged in at start-up time, the default audio devices that are available on the workstation, if any, are selected. When the option is set to **true**, and if the headset is not plugged in when the agent logs in, Workspace Desktop Edition waits for the headset to be plugged in before finalizing the login of the voice channel.

Genesys Softphone enables agents to switch to a preconfigured Not Ready state if the USB headset becomes unplugged after the agent has logged in to the SIP Voice Media. The agent will remain logged in to other eServices media such as email and chat.

Use the following configuration options in the **interaction-workspace** section of the Workspace Application object to control the behavior of this feature:

- sipendpoint.headset-unplugged.not-ready-reason: Specifies the Not Ready reason to be set to the SIP DN if the USB headset that is used by the agent becomes unplugged.
- sipendpoint.headset-unplugged-set-not-ready: Specifies whether the SIP DN of the agent is set automatically to **Not Ready** if the USB Headset that is used by the agent becomes unplugged.
- sipendpoint.headset-replugged-set-ready: Specifies whether the SIP DN of the agent is set automatically to **Ready** if the USB Headset that is used by the agent is plugged back in.

Genesys Softphone can be configured to retain volume setting of the USB headset between agent sessions.

Use the following configuration options in the `interaction-workspace` section of the Workspace Application object to control the behavior of this feature:

- sipendpoint.retain-volume-settings-between-sessions: Specifies whether the volume settings are saved for both microphone and speaker, when the agent logs out.

> **Important**
>
> When an agent logs in to Workspace Desktop Edition, the application creates a list of headsets that are plugged into the workstation. If an agent wants to use a different headset, they must exit Workspace, plug in the new headset, and then relaunch Workspace.

Session Border Controller configuration

Genesys Softphone supports connecting to SIP Server through a Session Border Controller (SBC) (refer to *Server 8.1 Deployment Guide*).

You must configure Workspace Desktop Edition to connect to SIP Server through an SBC instead of directly to SIP Server. If you do not configure Workspace Desktop Edition to connect to SIP Server by using an SBC, Genesys Softphone connects directly to SIP Server to register the agent SIP Endpoint by using the **TServer/sip-address** and **TServer/sip-port** options of the corresponding SIP Server application. However, when you configure Workspace Desktop Edition to connect by using an SBC

you decouple the address and port information that is sent to the SIP REGISTER from SIP Server and Workspace Desktop Edition obtains the host address and port from the configuration.

Configure the following two options in the **interaction-workspace** section of the Application, Tenant, Agent Group, or User object:

- sipendpoint.sbc-register-address: Specifies the address of your SBC to which Genesys Softphone connects.
- sipendpoint.sbc-register-port: Specifies the port on your SBC to which Genesys Softphone connects.

To set the Domain/Realm of your contact center instead of an IP when Genesys Softphone tries to register through a session border controller (SBC) device, set the value of the following two options to represent valid SIP domain names to specify a 'request-uri' in the SIP REGISTER request that is decoupled from the SIP Proxy address that is contacted:

- sipendpoint.proxies.proxy0.domain
- sipendpoint.proxies.proxy1.domain

Genesys SIP Proxy configuration

Genesys Softphone supports Genesys SIP Proxy. This feature enables SIP high availability (HA) without requiring a virtual IP address. Refer to the SIP Proxy 8.1 Deployment Guide for information about deploying and using SIP Proxy.

DNS SRV

You can configure the Genesys Softphone with one of the following:

- A standard DNS A-Record. The final URI form is: **sip:user@<host_fqdn>:<port>** where **<host_fqdn>** can be virtual and can represent multiple physical addresses behind the scenes, but the **:<port>** is mandatory, or
- A DNS SRV (Service record) as specified in the Genesys SIP Proxy Architecture. The final URI form is: **sip:user@<host_fqdn>**

Limitations

- Genesys SIP Proxy currently does not support scenarios with switchover mid-transaction; therefore, call ANSWER and CANCEL probably will not work; however, BYE is fully supported.

Provisioning

Configure the connection to the SIP Proxy by using the following Workspace Desktop Edition configuration options:

- sipendpoint.sbc-register-address: Specifies the IP Address, Host Name of the SIP Proxy or the FQDN of the SIP Proxy farm.

- sipendpoint.sbc-register-port: Specifies the port of the SIP Proxy. For a SIP Proxy farm, all SIP Proxy instances must have the same SIP Port. For a DNS SRV, set this option to **0**.
- sipendpoint.sbc-register-address.peer: Specifies the IP Address, Host Name of the DR peer SIP Proxy or the FQDN of the DR peer SIP Proxy farm.
- sipendpoint.sbc-register-port.peer: Specifies the port of the DR peer SIP Proxy. In case of DNS SRV, set this option to **0**.

These options were introduced in Workspace Desktop Edition to support Session Border Controller; therefore, they are not specific to SIP Proxy.

Genesys recommends that you set the value of the sipendpoint.policy.endpoint.rtp_inactivity_timeout option to the default value of **30**.

Enabling an agent to use Genesys Softphone

Prerequisites

- A working knowledge of Genesys Administrator Extension.
- A Workspace **Application** object exists in the Configuration Database.

Procedure

To enable an agent to use the Genesys Softphone to send and receive SIP-based interactions, perform the following steps:

1. Install Genesys Softphone on the agent workstation in connector mode.
2. During installation, specify the **Connector port** and configure the port for either **http** or **https**.
3. In the **GenesysSoftphone.config** file, in the **connector** section, set the value of the **enable_sessionid** option to **0**.
4. Configure the options sipendpoint.standalone.port and sipendpoint.standalone.protocol according to the values specified for the Connector at Genesys Softphone installation time.
5. If required, configure the other SIP Endpoint options in the **interaction-workspace** section of the Workspace **Application** object (refer to the Genesys Softphone configuration option reference for a list of SIP Endpoint options and a description of how to configure them).
6. If required, configure SIP Endpoint for SIP Proxy support.
7. Set the following **TServer** section options for the DNs of the Place to which the agent is logging in:
   - **sip-cti-control = talk,hold**
   - voice **= true**

Running Workspace and Genesys Softphone in a VDI

Environment

If the goal is to run Workspace and Genesys Softphone in a VDI environment, the sipendpoint.standalone.vdi-detection-model option must be set to **localhost** and Genesys Softphone must be installed using the appropriate VDI type.

In a Citrix environment where agents are using Windows sessions on the same Windows Server, the Virtual IP Loopback feature must be activated to allow successful communication between WDE and Genesys Softphone when multiple users are assigned to the same Windows Server. For more information, see the Virtual IP and virtual loopback page in the Citrix documentation.

In the IP Loopback configuration, register the following executables:

- **interactionworkspace.exe**
- **genesyssoftphone.exe**

Overriding Genesys Softphone option values

You can override the following Genesys Softphone options when you provision Workspace Desktop Edition options:

- In the **proxies** and **system** domains, you can override all options.
- In the **policy** domain, you can override **endpoint**, **session**, and **device** sections.

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

Overriding an option

To override a Genesys Softphone option when provisioning WDE, 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 WDE provisioning. See the options reference for a list of Genesys Softphone settings.

Codec priority

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"
```

Or 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.

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"/>
```

> ## 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 use the **enabled** section of the "codecs" domain, 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.

Genesys Softphone configuration options

This article lists and describes, by container and then by domain, the configuration settings in the **<Genesys Softphone Installation Directory>\Softphone.config** file. For an example of the configuration file, see Configuring Genesys Softphone. It also describes how to configure Genesys Softphone to work with the audio devices that you use in your environment.

When you install Genesys Softphone, either by using the **Genesys Installation Wizard** or silently by command line, the **Softphone.config** and **genesys_softphone.exe** files are both installed. The contents of the **Softphone.config** file is generated by the choices you specify in the wizard or by modifications you make to the **genesys_silent.ini** file.

In the **Softphone.config** file, the **setup.exe** executable sets the values of the following attributes of the **Connector** section: **protocol**, **port**, and **certificate_search_value**. The **enable_sessionid** and **auto_restart** are not set by the executable; you must set these yourself. The default values 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.

> **Tip**
>
> If you use Workspace Web Edition with Genesys Softphone, use the Workspace SIP Endpoint options to set up your environment.

Basic container

The Basic container holds the connectivity details that are required to connect to your SIP Server, optionally through a Session Border Controller (SBC). 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 can be multiple connection elements present, with each element specifying a separate possible connection. Refer to the configuration settings of that feature for details.

You must make the following changes and save the updated configuration file before using Genesys Softphone:

- **user="DN"**: Supply a valid DN for the user attribute.
- **server="SERVER:PORT"**: Replace SERVER with the host name where your SIP Server or SBC is deployed, and PORT with the SIP port of the SIP Server or SBC 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 or SBC. 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.
- Genesys Softphone does not take into account the **weight** field of an SRV record.
- You cannot 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 cannot 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 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* and *SIP*		

Domain	Section	Setting	Default value	Description
		Endpoint SDK for OSX Developer's Guide.		

Genesys container

The Genesys container holds configurable settings that are organized into domains and sections. You don't have to change these settings but you can customize them.

The following table describes the settings in this container and their valid values:

Domain	Section	Setting	Values	Description
policy				
	endpoint			
		defer_device_release	Integer	Specifies a time in milliseconds before releasing audio devices after the audio stream has been stopped. Deferring device release avoids potential service interruptions if the audio will be restarted quickly and if audio device operations are too slow on the user workstation or has other problems with restart. The value 0 disables deferred device release. Default Value: 200
		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

Domain	Section	Setting	Values	Description
				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 can 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_mac_address	Number	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. Default value: 0
		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 value: 1
		include_sdk_version_in_user_agent_header	Number	If set to 1, the User Agent field includes the SDK version the client is currently running on. Default value: 1

Domain	Section	Setting	Values	Description
		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 value: 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

Domain	Section	Setting	Values	Description
				the GSP uses to automatically obtain the public address. Valid values: This setting can 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 can 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 specifies the default gateway. 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.

Domain	Section	Setting	Values	Description
				• $host: The GSP retrieves the standard host name for the local computer using the gethostname system function. • $fqdn: The GSP retrieves the fully qualified DNS name of the local computer. The GSP uses the GetComputerNameEx function with parameter ComputerNameDnsFullyQualifi • $net:<subnet> Where 'subnet' is a full CIDR name, as per RFC 4632. For example, '$net:192.168.0.0/16'. The first valid IP address that belongs to the specified subnet is selected. To support a dynamic VPN connection, Genesys Softphone does not start registration attempts until the interface (configured by adapter name or subnet) is available. • An adapter name or part of an adapter name prefixed with $. For example,

Domain	Section	Setting	Values	Description

				$Local Area Connection 2 or $Local. The specified name must be different from the special values $auto, $ipv4, $host, and $fqdn.
				• $(rule1,rule2,...) – Genesys Softphone will select the IP address from the network interface that matches with at least one of the given rules. The valid rules are:
				  • `if='string'` – matches interface with name or description given in the string. For example, `if='Wi-Fi'` selects IP address from **Wi-Fi** adapter (if present).
				  • `if!='string'` – excludes the interface name that matches with the interface name and description given in the string; intended to exclude

Domain	Section	Setting	Values	Description
				only one particular interface. For example, **if!= 'Bluetooth'** • `net='CIDR'` – matches the 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'` – excludes the interface with IP address on given subnet that matches with the given IP address on a specific subnet, where CIDR is the full CIDR name as per RFC 4632; intended to exclude specific

Domain	Section	Setting	Values	Description
				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 the default configuration. 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.
		rtp_inactivity_timeout	Number	Timeout interval in seconds for RTP inactivity. Valid values: Integers from 5 to 150.

Domain	Section	Setting	Values	Description
				Default value: 150 Suggested value: 30
		rtp_port_binding	Number	Specifies how Genesys Softphone binds the RTP port: • `0` — opens the RTP and RTCP ports to listen on any network interface. • 1 — opens the RTP and RTCP ports to listen only on the interface specified by the **public_address** setting. **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. Valid values: `0,1` Default value: 1
		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

Domain	Section	Setting	Values	Description
				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 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	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

Domain	Section	Setting	Values	Description
				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.
		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

Domain	Section	Setting	Values	Description
				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	Number	SIP transaction timeout value in milliseconds. Valid values: 1 through 32000. Default value: 32000 (starting from release 9.0.018.06; for previous releases: 4000) Recommended value: 32000
		vq_alarm_threshold	0 (default) or number from 1.0 to 5.0	Specifies Mean Opinion Score (MOS — a measure of reported network quality ratings) threshold for generating Voice Quality Alarms. The value 0 disables the alarms. The recommended threshold value is 3.5. Using values above 4.2 are not recommended as an MOS that high might not be obtainable with some codecs, even under perfect network conditions.
		vq_report_collector		See SIP Endpoint SDK for .NET 9.0.0NET—Producing_RTCP_Extend and SIP Endpoint

Domain	Section	Setting	Values	Description
				SDK for OSX—Producing RTCP Extended Reports.
		vq_report_publish		See SIP Endpoint SDK for .NET 9.0.0NET—Producing_RTCP_Extend and SIP Endpoint SDK for OSX—Producing RTCP Extended Reports.
		webrtc_audio_layer	0 1 2 500 501 502 1000 1001 1002 2000 2001 2002 3000 3001 3002	Valid values: • 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. • 500: The audio layer ensures that Microsoft Windows MultiMedia Class Scheduler Service (MMCSS) is kept alive by the system independent of the actual audio activity on input and output devices. It can be combined with the values 0, 1, or 2 (500, 501, or 502) to specify the type of audio

Domain	Section	Setting	Values	Description
				layer. • 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. It can be combined with the values 0, 1, or 2 (1000, 1001, or 1002) to specify the type of audio layer. • 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. It can be combined with the values 0, 1, or 2 (2000, 2001, or 2002) to

Domain	Section	Setting	Values	Description
				specify the type of audio layer. • 3000: Opens the microphone and speaker channels for the life of the endpoint, using the audio layer type defined by option 0. It can be combined with the values 0, 1, or 2 (3000, 3001, or 3002) to specify the type of audio layer.
	session			
		agc_mode	0 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 that the agc_mode setting can be changed to 1 or 0 from the main sample application. Default value: 1 NOTE: It is not possible to apply different AGC settings for different channels in multi-channel scenarios.
		rx_agc_mode	0 1	Enables and disables Receiving-side Automatic Gain Control (Rx AGC).

Domain	Section	Setting	Values	Description
				• 0: Disables the feature (default). • 1: Enables Receiving-side AGC, resulting in automatic adjustment of the volume of the received RTP stream. This ensures that the volume of all calls is adequate for agents to hear the contact.
		auto_answer	Number	If set to 1, all incoming calls are answered automatically.
		callwait_tone_enabled	0 1	Valid Values: 0, 1 Default Value: 1 Specifies whether the call waiting tone is enabled (1) or disabled (0). This configuration is applied at startup.
		callwait_tone_file	String	Valid Values: Empty, or the path to the call waiting sound file. The path may be a file name in the current directory or the full path to the sound file. Default Value: callwait.wav Specifies the audio file that is played when the call waiting tone is enabled by the callwait_tone_enabled option. **Note**: WebRTC does not support MP3 playback. The callwait 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

Domain	Section	Setting	Values	Description
				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.
		dtmf_feedback	0 1	Valid values: 0 or 1 (default). If set to 1, DTMF feedback (audio tones played locally when sending DTMF signals to the remote side of the conversation) is enabled. See also: dtmf_method. (**Added:** 9.0.018.04)
		dtmf_method	Rfc2833 Info InbandRtp	Method to send DTMF when dtmf_feedback is enabled.
		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 rejects the incoming session if a USB headset is not available.
		sip_code_when_headset_na	Number	If a valid SIP error code is supplied, the GSP rejects the

Domain	Section	Setting	Values	Description
				incoming session with the specified SIP error code if a USB headset is not available. Default value: 480
		vad_level	Number	Sets the degree of bandwidth reduction. Valid values: 0 – 3 — from 0 (conventional VAD) to 3 (aggressive high).
		ringing_enabled	0, 1, 2, 3, 4, 5, 6, or 7	Specifies whether to enable the ringtone and on which device to play the media file. Valid values: • 0: None, disable ringtone. • 1: (default) 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 (the combination of values 1 and 2).

Domain	Section	Setting	Values	Description
				• 4: Play ringtone through a separate ringer device, specified by policy.device.ringer_device. • 5: Play ringtone through system default device and lay ringtone through a separate ringer device (the combination of values 1 and 4). • 6: Play ringtone through the communication device (headset) once only for the full duration (policy.session.ringing_timeout is ignored, and ringing does not stop when the call is answered). Configure media in policy.session.ringing_file. • 7: Play ringtone once for the full duration through both system default device and communication device (headset) (policy.session.ringing_timeout is ignored, and ringing does not stop when call is answered). Configure media in system.media.ringing_file and

Domain	Section	Setting	Values	Description
				policy.session.ringing_file. Default value: 1
		ringing_timeout	Number	Specifies the duration, in seconds, of the ringtone. If set to 0 or if the value is empty, the ringing time is unlimited. Valid values: Empty, 0, or a positive number Default value: 0
		ringing_file	String	Specifies the audio file that is played in the audio out device (headset) when the ringtone is enabled with the ringing_enabled option. Note that WebRTC does not support MP3 playback. The ringtone files for built-in ringing are RIFF (little-endian) WAVE files 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 be 16 bit mono or stereo and have a frequency of 8, 16, or 32 KHZ. Sample ringing sound files are provided. Each file is adjusted to have a higher or lower level of volume than the default ringing sound file, as follows: • ringing.wav (default) • ringing_+10dB.wav • ringing_-10dB.wav

Domain	Section	Setting	Values	Description
				• ringing_-20dB.wav You can adjust the volume level of the default ringer sound by specifying the file that has the preferred level of volume. Valid values: Empty or the path to the ringing sound file for the audio out device (headset). The path can be a filename in the current directory or the full path to the sound file. Default value: ringing.wav
		ringback_enabled	0, 1, 2, 3, 4, or 6	Specifies how the ringback feature is enabled. • 0: (default) do not play a ringback when the INVITE dialog is not yet established. • 1: play the incoming media stream, if provided by the media gateway in a reliable provisional response with SDP. • 2: play ringback from a local file only. • 3: always play ringback using media provided by gateway or a local file if not provided. • 4: same as 1, but the incoming media stream

Domain	Section	Setting	Values	Description
				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).
		ringing_while_call_held	0, 1	Valid values: 0 or 1 Default value: 1 Specifies whether to play ringtone or not when a call is held and a new call arrives. • 0: call wait tone (if configured) is played instead of ringtone. • 1 (default): ringtone is played whenever a new call arrives and there are no other active calls; held calls are not considered active in this case.
		ringback_file	Empty or a valid path to a 16-bit 8-, 16-, or 32-Khz **.wav** sound file.	Specifies the audio file that is played when the ringback_enabled option is configured to play a local file as the ringback tone.

Domain	Section	Setting	Values	Description
	device			
		audio_in_device	String	Microphone device name: can be either the device proper name or a regular expression.
		audio_out_device	String	Speaker device name: can be either the device proper name or a regular expression.
		ringer_device	String	Ringer device name: can be either the device proper name or a regular expression. Used when ringing_enabled = 4
		headset_name	String	The name of the headset model: can be either the device proper name or a regular expression. 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.
		include_headset	String	Valid values: A pair of device names or name parts, with microphone and speaker names separated by a colon, or a comma-separated list of name pairs. For example: `External Mic:Headphones` If the names include delimiter characters such as quotes, colons, or comma, they must be enclosed in single or double quotes. Specifies the list of audio in / out devices to be considered as a

Domain	Section	Setting	Values	Description
				headset for automatic device selection. This option is applicable to the case when use_headset = "1"
		use_headset	Number	If set to 0, the audio devices specified in audio_in_device and audio_out_device are used by the Genesys Softphone. If set to 1, the Genesys Softphone 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. Valid values: 0 or 1
		exclude_headset	String	The name of a headset model or built-in audio device (example: `Realtek`). The specified device is excluded from being recognized or automatically selected as a valid headset. Note that components of an excluded device, such as a microphone or speaker, can still be selected manually (or automatically, if Softphone does not find a better device). However, even if a component of an excluded device is selected, Softphone does not recognize the excluded device as an available headset. Valid values: Any valid

Domain	Section	Setting	Values	Description
				regular expression. Default value: Empty **Note:** This option is only available for Genesys Softphone installed on Windows.
	connector			
		auto_restart	Number	Valid values: 0 or 1. If set to 1 (default) the Softphone must be restarted after every client session.
		certificate_search_value	String	The thumbprint of a valid certificate that is accessible from the Certificate Store of the workstation where Softphone is 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 Workspace Web Editon (WWE) running in a browser). This option must always be set to 0 when connecting Workspace Desktop Edition (WDE) to Genesys Softphone.
		partitioned_cookies	Number	Valid values: 0, 1, or 2. This option controls the capability of Genesys Softphone to leverage the support by Chrome and Edge

Domain	Section	Setting	Values	Description
				(Chromium) of the cookies attribute partitioned which allows limited cookie sharing across domains. Once this cookie flag is in place, the versions of Chrome and Edge (Chromium) that implement the Phase Out of Third Party Cookie continue to accept the session cookie generated by Genesys Softphone. Valid from release 9.0.126.05. • 0: disabled, never add the cookie attribute • 1: enabled, always add the cookie attribute • 2 (default): auto, enable the cookie attribute conditionally for Chrome and Edge (Chromium) version greater or equal to v 118.
		port	Number	The port that Softphone opens 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

Domain	Section	Setting	Values	Description
				activated and Softphone runs in regular stand-alone GUI mode.
		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.
		allowed_origin_headers	a comma separated list of domains using star notation and FQDNs	For Softphone connector clients establishing a CORS connection, specify the list of authorized origins, separated by commas, in the form of domains using star notation (for example, *.genesyscloud.com) and FQDNs (for example, gwa-use1.genesyscloud.com). If empty, any origin is accepted.
sec_protocol	String	Valid values: • strict mode: SSLv3, TLSv1, TLSv11, and TLSv12 are the strict protocol version modes. These settings can be used to enforce a specific protocol		

Domain	Section	Setting	Values	Description
		version. The connection will not be established if the remote server does not accept the enforced protocol version. • compatibility mode: SSLv23, the default mode, is compatible with all modes from SSLv2 up to and including TLSv12; it will connect with the highest mode offered by the other server. If SSLv2 ciphers are explicitly specified, the SSLv2 client can connect only to servers running in SSLv23 mode. Otherwise, the SSLv2 mode is deprecated; but it is highly vulnerable and is not recommended.		
codecs — See SIP Endpoint SDK for .NET 9.0.0NET—Working with Codec Priorities and SIP Endpoint SDK for OSX —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

Domain	Section	Setting	Values	Description
				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 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_port	Number	DEPRECATED: This setting controls whether or not Genesys Softphone re-registers itself when receiving a mismatched IP address in the received parameter of a REGISTER response. This helps resolve the case where the Genesys Softphone has multiple network interfaces and obtains the wrong local IP address. A value of 0 (default)

Domain	Section	Setting	Values	Description
				disables this feature and a value of 1 enables re-registration. Valid values: 0 or 1 Default value: 0
		reg_timeout	Number	The period, in seconds, after which registration expires. 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 stand-alone mode.
	nat			
		ice_enabled	Boolean	Enable or disable ICE.
		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			

Domain	Section	Setting	Values	Description
		enable_logging	Number	Disable or enable logging. Valid values: 0 or 1
		log_file	String	Log filename, 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.
		log_segment	false Number Number in KB,MB, or hr	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 log file. 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 Default value: 10 MB

Domain	Section	Setting	Values	Description
		log_expire	false Number Number file Number day	Determines whether the 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. 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 to 1000. <number> day: Sets the maximum number of days before log files are deleted. Specify a number from 1 to 100 Default value: 10 (store 10 log fragments and purge the rest)
		log_time_convert	local 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). 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 computer is used. utc: The time of log record generation is expressed as Coordinated Universal Time (UTC). Default value: local

Domain	Section	Setting	Values	Description
		log_time_format	time locale ISO8601	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. 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
	security			
		certificate	String	For more information, see the **certificate** option for .NET and macOS.
		use_srtp	optional allowed disabled off elective both enabled force mandatory	Indicates whether to use SRTP (Secure Real-Time Transport Protocol) [**Modified:** 9.0.005.06] • 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

Domain	Section	Setting	Values	Description
				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'), adds the UNENCRYPTED_SRTCP parameter to that offer. When this parameter is negotiated, RTCP packets are not encrypted but are still authenticated.
		tls-target-name-check	no host	For more information, see the **tls-target-name-check** option for .NET and macOS.
	media			
		ringing_file	String	The Ringing sound filename 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 ringtone is enabled with the ringing_enabled

Domain	Section	Setting	Values	Description
				option. Sample ringing sound files are provided. Each file is adjusted to have a higher or lower level of volume than the default ringing sound file, as follows: • ringing.wav (default) • ringing_+10dB.wav • ringing_-10dB.wav • ringing_-20dB.wav You can adjust the volume level of the default ringer sound by specifying the file that has the preferred level of volume. Valid values: Empty or String filename Default value: ringing.wav

For more information about these options, see *SIP Endpoint SDK for .NET Developer's Guide* and *SIP Endpoint SDK for OSX Developer's Guide*.

Audio device settings

This section describes how to set up Genesys Softphone to work with your audio devices, such as headsets.

Genesys Softphone uses the following criteria to select its audio input and output devices:

- Basic settings for audio input and output devices.
- Selection rules used to choose an audio device, auto-answer a call, and reject a call.
- Combinations of settings that affect audio device selection, auto-answer, and call rejection.

Basic settings

Use the following parameters to configure headsets and other audio input devices:

- **headset_name**

- **audio_in_device**
- **audio_out_device**

If none of the audio devices that are accessible to the endpoint, match the device names in the configuration file; Genesys Softphone picks up the first available devices from the WebRTC list for audio devices.

> **Tip**
>
> The **headset_name**, **audio_in_device**, and **audio_out_device** options support both device proper names and regular expressions.

Audio device selection rules

The following rules are used to select an audio device, auto-answer a call, and reject a call.

The following audio device selection procedure is applied on startup and every time any changes are made to device presence (such as when a new device is plugged in or an existing device is removed):

1. The first device in the applicable list that is present in the system is selected when possible. This device (or devices) will either be specified by the **headset_name** parameter or by the **audio_in_device** and **audio_out_device** parameters, depending on whether the **use_headset** parameter has been enabled.
2. If none of the configured devices are present (or if the configuration list is empty), then Genesys Softphone selects the audio devices using the priority provided by WebRTC, based on the order of the available devices in its device list.

Auto-answer

When either of the following conditions is met, Softphone blocks the auto-answer functionality (a manual answer is still possible):

- the **use_headset** parameter is set to **1**, and none of the devices listed in the **headset_name** settings are present (but session rejection is not applicable, that is, the **reject_session_when_headset_na** parameter has been set to **0**).
- Genesys Softphone was unable to find any usable microphone or speaker device (applicable to cases where the **use_headset** parameter is set to **0**).

If the **auto_answer** parameter is set to 1 and the auto-answer functionality is not blocked (and the call was not already rejected), Genesys Softphone answers the incoming call automatically (the **should answer** policy returns the value **true**).

In addition, auto-answer will be triggered by the Alert-Info SIP header in the incoming INVITE, as described in the Deploying Genesys Softphone page.

Rejecting a call

For backward compatibility with previous releases, a call can only be rejected when both of the following conditions are met (a policy of **should answer** returns the value **false**):

- Both the **use_headset** and **reject_session_when_headset_na** parameters are set to 1.
- None of the devices listed in the **headset_name** settings is present on the workstation.

When these conditions are both met, an incoming call is rejected with the SIP response code that is configured in the **sip_code_when_headset_na** setting. If the setting is missing or the value is not in the valid range of **400** to **699**, then the default value of **480** (**Temporarily Unavailable**) is used.

In addition, when these conditions are met, Genesys Softphone refuses to initiate any new calls; it rejects all outgoing call attempts.

The availability of a fallback device (selected by Step 2 in the Audio device selection section) does not affect call rejection.

Audio setting combinations

Sometimes combinations of settings that you make can have unexpected results. Before adjusting your settings, review this section. The following combinations of settings affect audio device selection, auto-answer, and call rejection in the ways described below:

use_headset=1

<table>
<tr><td rowspan="2">Headset is available

Genesys Softphone considers a headset to be available if a headset is found by name in the list of headset names stored in the headset_name parameter. (The highest priority device in the list is selected).

Outgoing calls can be initiated.</td><td>auto_answer=1</td><td>Incoming calls are answered automatically.</td></tr>
<tr><td>auto_answer=0</td><td>Incoming calls are answered manually.</td></tr>
<tr><td rowspan="2">Headset is not available

Genesys Softphone determines that no headset is available if a headset is not found by name in the list of headset names stored in the headset_name parameter.

An audio device is still assigned if any supported devices are present in the system, using the first available audio input and output devices from the list compiled by WebRTC.</td><td rowspan="2">No auto-answer is possible in this subcase, so the auto_answer setting is not used.</td><td>reject_session_when_headset_na=1
Incoming calls are automatically rejected.
Outgoing calls are blocked.</td></tr>
<tr><td>reject_session_when_headset_na=0
Incoming calls can be answered manually. It is assumed that the agent will plug in the headset (or use an available non-headset device, if applicable) before answering the call.</td></tr>
</table>

		• Outgoing calls can be initiated. It is the agent's responsibility to ensure that the appropriate audio devices are available before the call is answered by the remote side.

use_headset=0

Audio devices are configured using the names from the **audio_in_device** and **audio_out_device** settings. Genesys Softphone selects the highest-priority input and output devices from that list or, if no valid devices are found in that list, from the first available devices in the list compiled by WebRTC. Outgoing calls can be initiated.

Both microphone and speaker are available	**auto_answer=1**	Incoming calls are answered automatically.
	auto_answer=0	Incoming calls are answered manually.
Either microphone or speaker is not available • Incoming calls can be answered manually. It is assumed that the agent will plug in the headset (or use an available non-headset device, if applicable) before answering the call. • Outgoing calls can be initiated. It is the agent's responsibility to ensure that the appropriate audio devices are available before the call is answered by the remote side.	No auto-answer is possible in this subcase, so the **auto_answer** setting is not used.	Auto-rejection is not applicable, so the **reject_session_when_headset_na** setting is not used.

Using Genesys Softphone

Genesys Softphone is an application that enables your computer and phone or headset to connect to the public phone system. This section describes how to use the Genesys Softphone.

This article tells you how to use Genesys Softphone on your workstation, including how to start Genesys Softphone, activate and register users, view device and user status, and make and receive calls.

Genesys Softphone in Connector Mode

For most Genesys Engage cloud users, Genesys Softphone is in Connector Mode and starts automatically when Windows starts up, you do not have to start Genesys Softphone yourself.

If you right-click the Genesys Softphone system tray icon, you are given one menu option, **Exit**. Selecting this option stops Genesys Softphone. You must restart Genesys Softphone to enable you to log in to Workspace.

> **Important**
>
> The Genesys Softphone UI described in the Standalone mode section is not available in Connector Mode.

Genesys Softphone status indicators

Genesys Softphone displays different icons in the system tray to let you know its status and if there are any warnings or errors.

If you see a warning icon, hover your mouse pointer over the icon to read a tooltip summary of the problem. This tooltip will include the type of protocol your Genesys Softphone is configured to implement: "SIP" or "WebRTC." Specify which type is displayed when reporting an incident to your Administrator.

System tray Genesys Softphone status icons

Icon	Condition
	Waiting for agent login
	Agent logged in and Softphone registered
	Activation or registration error
	Headset issue

Icon	Condition
	Voice quality is currently degraded
	Microphone is muted

Genesys Softphone language selection

Genesys Softphone can be presented in various languages.

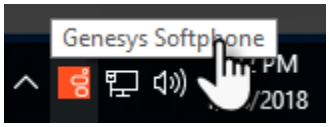
The default language can be aligned with the language selected in your application that is controlling your Genesys Softphone (for example Workspace Web or Desktop Edition).

You can also personalize the language through the menu accessible from the system tray Genesys Softphone status icons.

Genesys Softphone in Standalone Mode

If your system does not use Connector Mode, you can start the Genesys Softphone by double-clicking the Genesys Softphone shortcut on your desktop or by selecting it in your **Start** Menu.

To open the Genesys Softphone UI, right-click the Genesys Softphone ( ) icon from the Icon Tray and select **Open**.



Genesys Softphone status indicators

Genesys Softphone displays different icons in the system tray to let you know its status and if there are any warnings or errors.

If you see a warning icon, hover your mouse pointer over the icon to read a tooltip summary of the problem. This tooltip will include the type of protocol your Genesys Softphone is configured to implement: "SIP" or "WebRTC." Specify which type is displayed when reporting an incident to your Administrator.

System tray Genesys Softphone status and warning icons

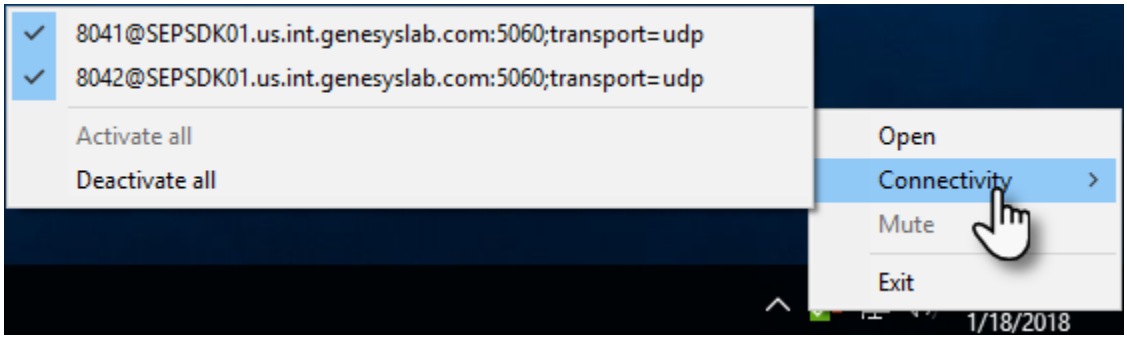
Icon	Condition
	Registered
	Registration error
	Headset issue

Icon	Condition
	Voice quality is currently degraded
	Microphone is muted

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 Genesys Softphone is active and ready to take calls.



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

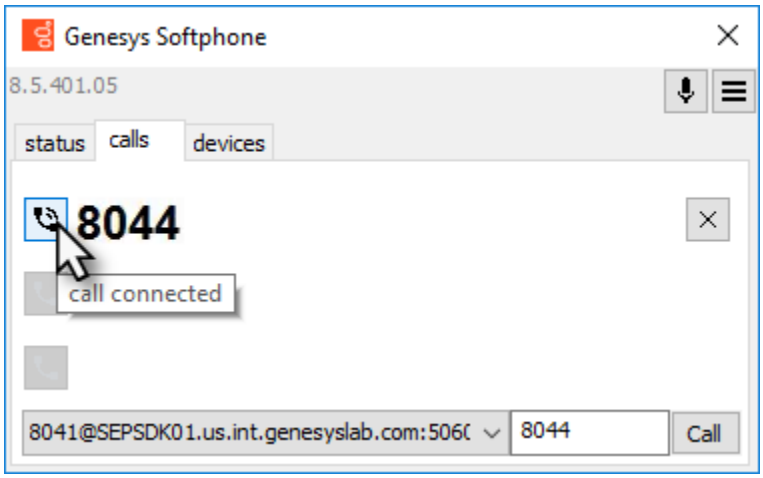
Each Genesys Softphone instance can have up to six SIP user accounts configured.

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

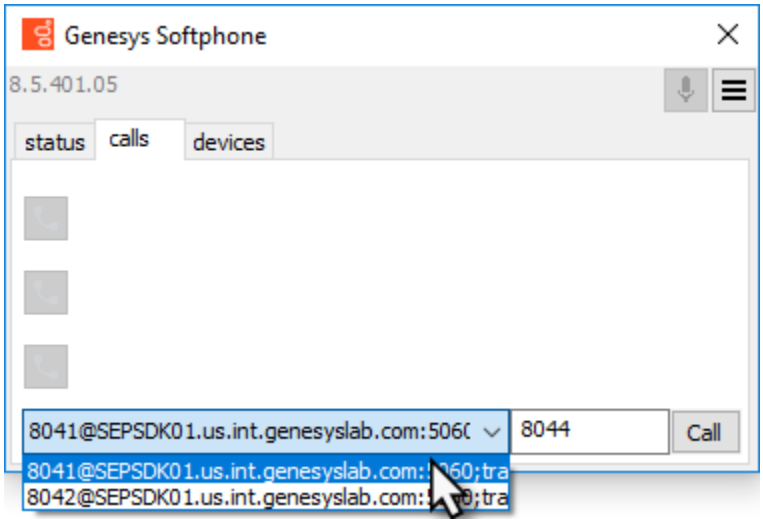
Making and receiving calls

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



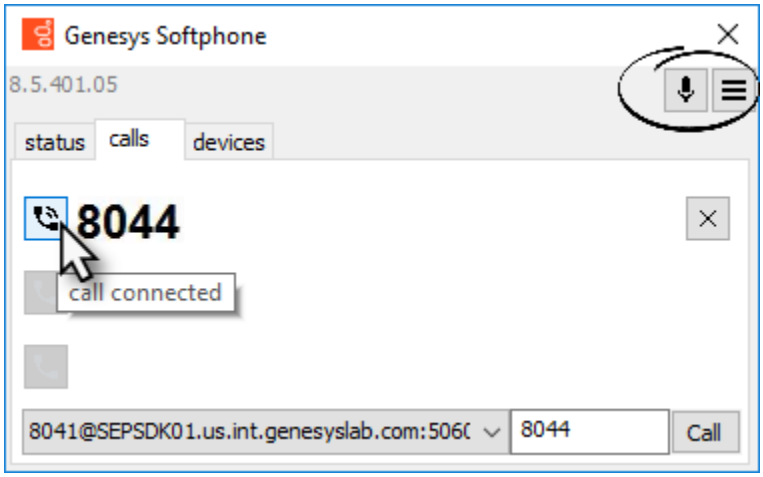
In the Genesys Softphone window, click the Calls tab and perform any of the following operations:

- 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.



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 at the application level and not the system level:

- The mute button is only available when there is an active call.
- Muting the microphone in Genesys Softphone is done at the session level. The mute status does not depend on the selected devices or on device presence and status. A session may be muted even if a microphone is not plugged in.

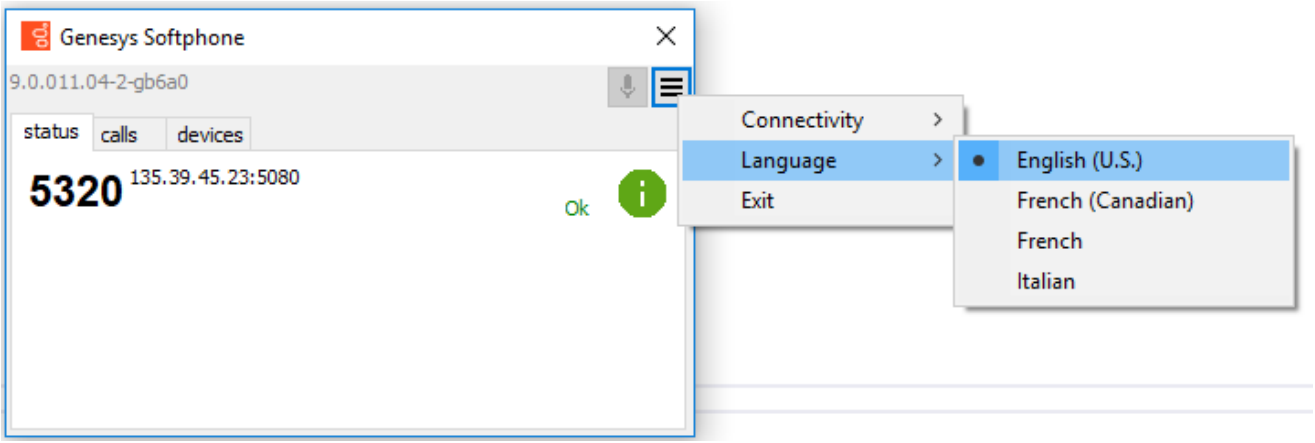
You may also mute/un-mute the microphone from the tray icon menu. To mute/un-mute the input device:

1. Right-click the Genesys 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.

Selecting the display language

You can personalize the language used to display text in Genesys Softphone through the main menu.



Important

For the new language to take effect, you will need to restart Genesys Softphone.