Genesys Softphone Deployment Guide

Single sign-on with Workspace Web Edition

4/4/2025

Contents

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.