Workspace Desktop Edition Deployment Guide

Agent login, authentication, and logout

4/4/2026

Agent login, authentication, and logout

[**Modified:** 8.5.112.08, 8.5.124.08, 8.5.138.04, 8.5.140.08, 8.5.141.04]

Agent login is a two-step process:

1. User authentication and selection of Place in the primary login dialog box
2. Selection of advanced parameters in the secondary login dialog box. Workspace enhances the security of your system by limiting agent login to basic authentication. Workspace further enhances security by enabling you to limit the choices that are presented to an agent at login.

> **Important**
>
> When an agent logs in to Workspace, the application creates a list of headsets that are plugged in to the workstation. If an agent wants to use a different headset, he or she should exit Workspace, plug in the new headset, then relaunch Workspace.

User authentication

When Workspace is launched by an agent, the agent must provide a user name and password as authentication. After authentication the Configuration Layer is accessed by Workspace to obtain the list of existing places and privileges that are granted to the agent, as well as the configuration of the Workspace application for that agent.

You can specify whether the username is stored locally in the user profile so that the next time the agent logs in the username is populated automatically. [**Added:** 8.5.103.10]

> **Important**
>
> If Workspace is started from the silent command line, the username is never stored.

Changing passwords

You can require agents to automatically change their password the first time that they log in to the system. You can assign temporary passwords to new agent objects when you create them, and then specify that the password must be changed before the new agent is able to log in to Workspace for the first time.

You can also enable agents to change their passwords by selecting the `Change Password` action from the Interaction Workspace Main Menu.

Use the following `Security` privilege to enable the password change feature:

- Can Change Password

Refer to the *Genesys Security Guide* for a complete description of password policies and how to configure them.

Kerberos user authentication

[**Added:** 8.5.102.06] [**Modified:** 8.5.132.05, 8.5.135.05]

Workspace supports Kerberos single sign-on (SSO) authentication. This means that agents only have to authenticate once on their workstations to start using Workspace. If Kerberos authentication is not used, agents must still login to Workspace after authenticating on their workstations.

You must configure your Genesys Management Framework to support Kerberos (refer to Chapter 4: Kerberos External Authentication of the *Framework External Authentication Reference Manual* and the *Genesys Security Guide*).

Workspace requires that you specify the unique Service Principal Name (SPN) that is used in each Configuration Server and Configuration Server Proxy that handles SSO requests from UI applications.

To specify the Service Principal Name in the software package:

- **ClickOnce deployment:** You can specify the Service Principal Name parameter in the **Deployment Manager Wizard** if you are installing Workspace as a ClickOnce application or by using Console Mode.
- **Non-ClickOnce deployment:** Edit the `login.kerberos.service-principal-name` option in the `interactionworkspace.exe.config` property file, which is located in the Workspace Installation Package (IP), and add the following line:

```
<appSettings>
  ...
  <add key="login.kerberos.service-principal-name" value="<SPN Name>"/>
  <add key="login.url" value="tcp://<host><port>/AppName" />
  <add key="login.connections.parameters.isenable" value="false" />
  ...
</appSettings>
```

- To specify how Workspace retrieves agent identity using the Windows API set the `login.kerberos.agent-identification` option in the `interactionworkspace.exe.config` configuration file. The value should also match the way agent usernames are synchronized in the Genesys Configuration Layer. See the description of the `authentication/enable-upn` option in the the **Configuration Option** section of the *Framework External Authentication Reference Manual*. The valid values are:
  - `implicitupn`: Workspace uses the Implicit User Principal Name (iUPN), which is a combination of the **samAccountName** and the user's Domain. [**Added:** 8.5.140.08]
  - `samaccountname`: (default value) Workspace uses the SAM Account Name attribute specified by Windows Administrator in Windows Active Directory when provisioning the account of an agent (8.5.110.13 and higher).
  - `upn`: Workspace uses the User Principal Name (UPN) specified by Windows Administrator in Windows Active Directory when provisioning the account of an agent (8.5.132.05 and higher). **This mode is deprecated and should be substituted by** `implicitupn`, but is maintained for compatibility

purposes.

  - `windowsidentity`: Workspace uses the information entered by the agent when opening the Windows session. Depending on the Windows authentication mechanism, this method can return the exact case typed by the agent in the login dialog, which might not match the user name configured in Genesys Configuration Layer. This is the API used in Workspace versions up to 8.5.109.25.

- For environments using Kerberos authentication, set the value of the `login.kerberos.enable-case-insensitive-agent-identification` option to `true` to specify that the matching of the username stored in the Genesys Configuration layer and the username specified by the `login.kerberos.agent-identification` option is *not* case-sensitive (the case of the letters is ignored). [**Added:** 8.5.135.05]

If Kerberos is configured, the agent login process works as follows:

If the Workspace property file is defined to enable Kerberos authentication, Workspace tries to acquire a Kerberos ticket. If the Kerberos ticket is found, Workspace tries to open a connection to Configuration Server using this ticket.

- If the connection attempt is successful, Workspace bypasses the first Workspace Login view and displays the second Login view or immediately displays the Main Toolbar. For more information about launching and logging in to Workspace, refer to the *Workspace Desktop Edition 8.5.1 Help*.
- If connection is not successful because of an invalid Kerberos ticket, a warning message is displayed to the agent, and the application start-up is interrupted.

You can override the error message that is displayed to agents if Workspace is unable to obtain a Kerberos ticket by using the methodology to customize a dictionary to specify an alternative message string for the `Windows.login.Kerberos.Retry` key.

Place selection

[**Modified:** 8.5.114.08, 8.5.112.08, 8.5.138.04]

Genesys 8 requires that each agent connect to a unique Place. Depending on your environmental constraints, you can adjust the Place selection process to make it completely invisible to the agents or to minimize the effort required to select the correct Place where the agent logs in.

Fine-tuning Place selection

You can control or improve the way that agent Place selection is handled. This section describes optional Place selection fine-tunings that are available.

Static Place

To assign a static Place to an agent and make Place selection invisible during login, in Genesys Administrator Extension you must assign a Default Place to the Agent in the **Advanced** tab of the Agent object Properties section and set the value of the login.default-place option to `$Agent.DefaultPlace$`, and set the value of the login.prompt-place option to `false`.

Auto-complete

You can configure the agent account using the login.prompt-place option so that during authentication the agent must specify a Place in the `Place` field of the secondary login dialog box. If the value of the login.enable-place-completion is `true`, a list of Places is displayed to agents according to the text entered in the **Place** field; this feature enables agents to choose the appropriate Place without typing the entire Place name.

Last used Place

To optimize the Place selection process, you can configure Workspace to store the last used Place in the Windows User Profile by setting the value of the login.store-recent-place option to `true`. If this information is available in the Windows User Profile the next time the agent logs in, this *recent* Place is proposed to the agent for confirmation during login. If the agent confirms that the recent Place is the correct one, the agent will be able to proceed with the connection to this Place without having to select it in the second login screen.

Hot seating

The Windows User Profile can be fully or partially set up for roaming/hot seating depending on how your environment is set up and the available infrastructure.

This means that in environments where the Windows User Profile of the agent stored from Workstation A, corresponding to Place 1 where the agent sits on Day 1, can be available on Workstation B, corresponding to Place 2 where agent sits on Day 2. However, in this scenario, the Place restored from the Windows User Profile and proposed as the *recent* Place might be incorrect.

Beginning with Workspace **8.5.112.08**, you can configure the environment so that the stored Place is associated with information that corresponds to the workstation where the agent sits when an agent selects the Place. This Place is then presented to the agent as the *recent* Place during login only if it was previously stored with the current workstation as an associated identifier.

Use the login.place-location-source option to specify how Workspace stores the last selected login Place in the Windows User Profile when the value of the login.store-recent-place option is set to `true`. The following values (modes) are supported:

- `standard`: The most recently used Place is stored in the Windows User Profile without any information about the workstation. This is the legacy recent place storage mode.
- `machine-name`: The most recently used Place is stored in the Windows User Profile, along with the name of the machine where the Workspace application is running. Use this value when Workspace is installed on the physical workstation where the agent logs in.
- `vdi`: The most recently used Place is stored in the Windows User Profile, along with the name of the physical workstation from which the agent executes a virtual session (for example, in Citrix XenApp/XenDesktop, VMWare Horizon, and Windows Terminal Server environments). Use this value when Workspace is installed in a Virtual Desktop Environment. If the machine name of the VDI client is not found, for example because agents are running Workspace on a physical workstation, the `machine-name` mode is used instead. This setting is appropriate for hybrid environments where agents are running Workspace alternatively in physical workstations and in virtual sessions. [**Added:** 8.5.112.08]

SIP DN type selection

[**Added:** 8.5.138.04]

You can create multiple Places associated with different types of SIP DNs for each agent to enable them to login from different devices, such as Workspace SIP Endpoint and Genesys Softphone when they are in the office, and their mobile through SIP Server or a 3rd party SIP Endpoint when they are working at home or outside the office. Alternately, you might want a hard phone back up for your soft phone in case there are issues with an agent's endpoint.

Use the voice.device-type option in the `interaction-workspace` section of the Annex of the DN object to specify whether the DN associated with a Place is Workspace SIP Endpoint or Genesys Softphone (`auto`), or whether it is a hard phone or 3rd party SIP Endpoint (`separate`).

Genesys recommends that you name your Places in a way that it will make it easy for agents to figure out which one to choose. For example, in the office you might have a desk associated with a soft phone labeled with "SIP-abc123". When the agent sits at the desk associated with the "SIP-abc123" Place, the agent specifies "SIP-abc123" in the Place field of the login screen. For an agent calling in from their mobile or home phone, you might name the Place that the agent should enter when they log in as "Agent XYZ Mobile". It is up to you to train your agents on which Place to enter when they log in.

Automatic Place selection using Place Groups

[**Added:** 8.5.114.08]

In traditional voice contact centers, a Place contains a DN that represents a hard or a soft phone and agents select it (manually or automatically) according to the location where they work. As contact centers evolve, some individuals that handle calls might be back office workers who login intermittently, while others are workers answering from home or on a mobile device. In each of these situations, the phone that is used is not directly monitored by the Contact Center infrastructure. Creating a static Place/DN pair for each one of these worker/phone combinations is a management issue because of the large number of Places that might be unused at any given time.

To solve this issue, you can enable agents to automatically select a Place using Place Groups. A Place Group makes a small number of Places available to any agent that selects the Place Group when they log in.

Depending on which approach you choose, during login, either your agents either select a Place or a Place Group, or you can assign them a specific default Place Group.

Warning

The *Automatic place selection using Place Groups* feature currently works only with SIP Server for DNs that are provisioned to support the remote login capability, which is enabled by the login.voice.prompt-dn-less-phone-number option.

The feature is *not* supported for:

- DNs that are used with Workspace SIP Endpoint

- Places that also support eServices channels

A Place Group is a preconfigured collection of Places, each containing a preconfigured Extension DN. When an agent logs in, Workspace selects a free Place from the group based on information provided by Statistic Server and assigns it to the agent.

The physical phone number typed by the agent, according to the capability enabled by the login.voice.prompt-dn-less-phone-number option in the `PlaceGroup` option, is stored in the settings of the DN contained in the selected Place.

To use this capability, complete the following steps:

1. Create one or more Place Group objects and add to it all the Places that you want to include in the group.
2. At the Agent, Agent Group, Application, or Tenant level, use the login.place-selection-type option to specify whether agents can select within a list of Places and/or a Place Groups when they log in.
3. At the Agent, Agent Group, Application, or Tenant level, use the login.available-place-groups option to specify the list of Place Groups that is presented to the agent. You can specify a list of Place Group names, or use the `$All$` keyword to enable agents to select from all the Place Groups to which they have read access.
4. Check that the login.voice.prompt-dn-less-phone-number option is enabled, to ensure that the Login on Place Group capability has access to the agent's phone number. You can either specify the option in the traditional Application, Tenant, AgentGroup, Agent hierarchy, or specify it in the PlaceGroup object so that it is taken into account only when this Place Group is selected.

You can also use the login.default-place option at the Agent, Agent Group, Application, or Tenant level to specify a default Place Group for an Agent or a group of Agents.

Important

The following options treat Place Groups as Places:

- login.enable-place-completion
- login.prompt-place
- login.store-recent-place

Optimizing the use of eServices Interaction Server licenses

[**Added:** 8.5.108.11]

To enable the operational engagement of Agents in an eServices workflow, the eServices system relies on the following technical license scheme:

- **Seat licenses:** Agents or supervisors require one seat license to:
  - handle interactions of one or more eServices media type
  - access the content of workins or interaction queues.
- **Media Channel licenses:** One media license of the corresponding type is required for each media type that is enabled for an agent to handle interactions.

Refer to Genesys Licensing Guide for details about the different types of eServices licenses.

Workspace does not directly manage eServices licenses; however, the way that it interacts with Interaction Server or Interaction Server Proxy has a direct influence on the way that licenses are checked out or checked in by Interaction Server.

Workspace enables you to manage (optimize) the checkout of eServices licenses by your agents and supervisors by using the eservices.disconnect-on-logoff. You can choose either the legacy behavior (pre-8.5.108.11) or the optimized behavior (8.5.108.11 and higher).

Legacy seat license and media checkout

The legacy behavior of license checkout when the value of the eservices.disconnect-on-logoff option is set to `false` is as follows:

1. A seat license is checked out when:
   - an agent logs in Workspace and this agent is granted the privilege to use at least one eServices channel (email, chat, social, and so on), or,
   - an agent logs in Workspace and this agent is granted the privilege to use Team Workbin or Interaction Management privilege, or,
   - an agent is notified that he or she is part of a push preview campaign and this agent is granted the privilege to use Outbound.

     In all these cases, the seat license is checked-in when the agent exits the application. Agents can access the content of their Personal or Shared Workbins at any time during the session, independently from media channel status.
2. One media license of a specific type (email, chat, custom, and so on) is checked-out as soon as the agent logs on the corresponding media channel. This can be done automatically at application start-up by implicit or explicit selection of media, or manually during an application session by global or selective media Log On. The media license is checked-in when the corresponding media is logged off manually, or when the agent exists the application.
   The custom media license that corresponds with the ‘outboundpreview’ media login is checked out the first time the agent is notified that he or she is assigned to a push preview campaign, and is checked in when the agent logs off voice channel or exists the application.

Optimized seat and media license checkout

The optimized seat and media license checkout feature is particularly applicable to environments where the license distribution between Voice and eServices seats is asymmetric, for example in systems where the number of Chat seats represent 20% of the total number of Voice seats, and all

the agents are granted the privilege to handle voice and chat interactions.

To configure the optimized license and media checkout behavior, set the value of the eservices.disconnect-on-logoff option to `true`. The license checkout behavior is as follows:

1. A seat license is checked out when:
   - an agent logs on at least one eServices channel in Workspace, either at login time by implicit or explicit selection of media, or manually during an application session by global or selective media Log On. The seat license is checked-in when the last eServices media is logged off manually, or when the agent exists the application (**Warning:** The Agent cannot access the content of his or her Personal or Shared Workbins when no eServices media is logged on), or,
   - when an agent logs in Workspace while this agent is granted the privilege to use Team Workbin or Interaction Management. In this case the seat license is checked in when the agent exits Workspace, or,
   - when an agent is notified that he or she is part of a push preview campaign and this agent is granted the privilege to use Outbound. In this case the seat license is checked in when the agent logs off the voice channel (it will be checked out again when voice channel is logged on again) or when he or she exits Workspace.
2. The media license checkout/checkin life cycle in the optimized license model is the same as in legacy license model.

> **Important**
>
> For both the legacy and optimized licensing model, the opening of the connection to Interaction Server or Interaction Server Proxy is synchronous with the seat license check-out and its closing is synchronous with the seat license is check-in.

Specification of advanced login parameters

Advanced login parameters are defined by the privileges, such as channel privileges, that are assigned to a particular agent. The privileges assigned to a particular agent, therefore, determine which advanced parameters, if any, are displayed in the secondary login dialog box.

The Place that is specified by an agent also determines the advanced login parameters that is available to be specified by the agent. For example, if the Place is associated with a voice channel, the agent must also provide login and queue information for each assigned DN. Other advanced parameters that might be required include SIP phone numbers.

Advanced parameters can be preset for agents—making it unnecessary for the agent to specify advanced parameters.

Application options that control login

The following are the most commonly used application options in the `interaction-workspace` section to control agent login (more options can be found here):

- login.default-place—Specifies the default Place that is proposed to the authenticated agent at login.
- login.enable-place-completion—Enables the name of the Place to be completed as the agent types.
- login.im.can-unactivate-channel—Specifies whether the agent can select and deselect (activate and deactivate) IM channels.
- login.im.prompt-agent-login-id—Specifies whether the agent can select a login id from the configured ones for the IM channel in the login window.
- login.im.prompt-dn-password—If applicable, prompts for the IM channel password in the secondary login dialog box.
- login.im.prompt-queue—If applicable, prompts for the ACD Queue in the secondary login dialog box.
- login.place-location-source—Specifies how Workspace stores the last selected login Place in the Windows User Profile when the value of the login.store-recent-place option is set to `true`. [**Added:** 8.5.112.08]
- login.prompt-place—Specifies whether the agent must enter a place in the login window.
- login.store-recent-place—Specifies whether the most recently used Place on the workstation is stored and displayed for the agent at the next login.
- login.store-username—Specifies whether the most recently used Username is stored locally in the user profile. If the value is `false`, the previous value is cleared. [**Added:** 8.5.103.10]
- login.voice.can-unactivate-channel—Specifies whether the agent can select and deselect (activate and deactivate) voice channels.
- login.voice.prompt-agent-login-id—Specifies whether the agent can select a login id from those configured for the voice channel in the login window.
- login.voice.prompt-dn-password—If applicable, prompts for the DN password in the secondary login dialog box.
- login.voice.prompt-queue—If applicable, prompts for the ACD Queue in the secondary login dialog box.
- login.workmode—Specifies the work mode that is applied when the user of the voice DN logs in. If set to `auto-in`, the agent is automatically in Ready state. If set to `manual-in`, the agent must manually activate the Ready state. To determine whether your switch supports the work mode, refer to the Deployment Guide of the relevant T-Server.
- login.<media-type>.can-unactivate-channel—Specifies whether the agent can select and deselect (activate and deactivate) particular channels.
- login.<media-type>.is-auto-ready—Specifies whether the indicated workitem channel is automatically set to the Ready state at login.

DN-less login configuration options

- login.voice.prompt-dn-less-phone-number—Specifies whether a DN-less phone number is prompted for in the login window. This option is specific to the SIP Server environment.
- login.voice.use-dn-less-login-extension—Specifies how the DN-less phone number specified by an agent during login is propagated to the Genesys back-end. Passing as an extension to SIP Server limits the impact of multiple simultaneous login or logout events in the case of a Disaster Recovery/Business Continuity event. SIP Server 8.1.102.93 or higher is required for this feature. Refer to Remote Agents with Non-provisioned DNs for more information. [**Added: 8.5.141.04**]

Using the command line to start Workspace

You can pass certain Workspace login information through the command line when you start the Workspace application:

```
interactionworkspace.exe -url tcp://<host>:<port>/<appli> -u <user> -p <password> -place
<place>
where:
<host>: host name or IP Address of Configuration Server
<port>: port of Configuration Server
<appli>: Interaction Worksapce application name in Management Framework
<user> Username of the agent
<password> Password of the agent (optional)
<place> Place where the agent log to (optional)
```

Important

You must pass all of the parameters on the command line. For example, you cannot pass only the `host`, `port`, `appli` and `place`, and then prompt for the username and password, for example.

If parameters are typed manually in the first login window, they are stored in the local user profile and restored to the login window at the next login session. If the parameters of the first login window are passed by the command line, thereby bypassing the first login window, then the parameters are not saved in the local user profile.

Warning

When the command-line is used to run Workspace Desktop Edition there is no way to prompt any login parameter, neither in the first nor in the second login screen. The purpose of running from the command-line is to by-pass the login screens and to immediately display the Workspace toolbar. As a consequence the following `login.*` options are by-passed by the command-line start:

- login.<media-type>.can-unactivate-channel = false
- `login.<media-type>.available-queues` = `ACDQueue`
- `login.<media-type>.prompt-queue` = `true`
- `login.<media-type>.prompt-agent-login-id` = `false`
- `login.<media-type>.prompt-dn-password` = `false`
- login.voice.prompt-dn-less-phone-number = `false`
- login.voice.use-dn-less-login-extension = `false`
- login.store-username = `true`
- login.place-location-source = `standard`

- login.store-recent-place = `true`
- login.default-place = <any value>
- login.prompt-place = `false`
- login.enable-place-completion = `true`

Kerberos Single Sign-on

(Optional) To use Kerberos Single Sign-on (SSO) you must omit the user name and password. The URL is mandatory. Place is optional when the agent is configured with a “default place” in Management Framework:

```
interactionworkspace.exe -url tcp://<host>:<port>/<appli> -place <place>
where:
<host>: host name or IP Address of Configuration Server
<port>: port of Configuration Server
<appli>: Interaction Workspace application name in Management Framework
<place> Place where the agent log to (optional)
```

Logout

[**Added:** 8.5.124.08]

Agents log out by selecting **Exit** from the **Main Menu** in the Workspace Window. Agents cannot log out if they have active interactions on their desktop.

You can modify logout behavior by using the following two options:

- logout.enable-exit-on-logoff-error
- login.voice.restore-dn-less-phone-number-on-logout [**Added:** 8.5.140.08]
- logout.voice.use-login-queue-on-logout