Workspace Desktop Edition Deployment Guide

Setting up agents on the system

4/9/2026

Setting up agents on the system

[**Modified:** 8.5.112.08, 8.5.117.18, 8.5.143.08]

Refer to *Genesys Administrator Extension Help* and *Genesys Administrator Extension Deployment Guide* for detailed information on how to use Genesys Administrator Extension and Management Framework to configure access permissions.

1. Creating a Role and allowing a Workspace privilege and assigning a Role to an agent or agent group

Purpose:

To restrict the privileges that are assigned to an agent or agent group.

The security.disable-rbac configuration option in the `interaction-workspace` section determines whether agents have all privileges granted or whether the Role-Based Access Control (RBAC) control system is used.

> ### Important
> RBAC requires Configuration Server 8.0.2 or higher. RBAC requires Genesys Administrator 8.0.2 or higher, or Genesys Administrator Extension (9.0.100.56 or higher is recommended).

If security.disable-rbac is set to `true`, RBAC is disabled and all privileges are assigned to all agents and Agent Groups. If security.disable-rbac is set to `false`, RBAC is enabled and you must assign roles to agents and Access Groups.

> ### Important
> Beginning with Workspace 8.5.143.08, Workspace supports both the Genesys Administrator Role storage model and the Genesys Administrator Extension Role storage model. Before you create a Role, refer to Role-Based Approach of Genesys 8 for more information about using these different storage models.

Prerequisites

- Genesys Administrator 8.0.200.29 or higher or Genesys Administrator Extension (9.0.100.56 or higher is recommended), configured to show Advanced View.

- Configuration Server 8.0.2 or higher.
- A working knowledge of Genesys Administrator Extension.
- Workspace Application Template in the Configuration Layer.

Start

1. Create the Workspace `Application` object from the Workspace Application Template.
2. From the `Tenant` drop-down list, select the Tenant for which you want to create the role.
3. In the Genesys Administrator Extension `Provisioning` view, select `Accounts` in the `Navigation` column.
4. Select the `Roles` view.
5. In the `Roles` view, click `New`.
6. In the `Configuration` tab, specify the following `General` parameters:
   - A name for the role.
   - A description of the role (optional).
   - Whether or not the role is enabled.
7. In the `Configuration` tab, specify a list of users or access groups in the `Members` view.
8. In the `Role Privileges` tab, click `Workspace privileges`.
9. Initially, all privileges are unassigned. To assign a privilege, click the drop-down list in the `Value` column that is associated with the privilege and select `Allowed`. Refer to Role Privileges for a list of all the privileges.
10. To save the new role, click `Save and Close`. The new role is now applied to the specified agents and Agent Groups. For information on privilege conflicts, refer to Conflict Resolution for Configuration Options.

    To discard the new role without saving your changes, click `Cancel`.

End

2. Optimizing the Login window

[**Modified:** 8.5.114.08]

> **Important**
>
> Refer to Agent login, authentication, and logout for detailed information about configuring agent accounts and Places for login and authentication.

Purpose:

To control the behavior of the Workspace Agent Login Window.

> **Tip**
>
> - Agent login can be configured as either a one-step or a two-step process depending on whether you want to prompt the agent for connection parameters in the secondary login window or specify the parameters for the agent.
> - For a list of configuration options that are related to login, refer to Login.
> - You can specify whether agents login to a Place or Place Group.

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

Start

1. Configure the agent for two-step login by setting the options that control Password, Queue, Switch, and Place.
   a. If the agent must enter a phone-set Password, set the login.voice.prompt-dn-password option to `true`. The second login window is displayed after the agent is authenticated. A phone-set Password prompt will be displayed in the secondary login window.
   b. If the agent must enter a Queue at login, set the login.voice.prompt-queue option to `true`. A Queue prompt will be displayed in the secondary login window.

      If the switch has multiple logins for the agent, the agent will be prompted to enter the particular login that they want to use.

   c. For details about setting up Places or Place Groups, refer to Place Selection. Several options control Place login:
      i. If the agent must enter a Place at each login, set the login.prompt-place option to `true`.
      ii. If the agent always logs in to a default Place at each login, do the following:
         - Assign a default Place in the Agent Advanced tab.
         - Set the login.prompt-place option to `false`.
         - Set the login.default-place option to `true`.
      iii. If the agent must specify a Place only the first time that the agent logs in (**Note:** The Place is stored in the local settings of the agent):
         - Set the login.default-place option to `false`.
         - Set the login.prompt-place option to `false`.
4. Configure the agent for one-step login by using the following configuration-option settings:

- Set the login.voice.prompt-dn-password option to `false`.
- Set the login.voice.prompt-queue option to `false`.
- Set the login.prompt-place option to `false`.

Note: If the default Place in the Agent Advanced tab is blank, the agent will have to perform a two-step login the first time that the agent logs in to a particular workstation.

End

3. Provisioning Workspace for the Voice channel

Purpose:

To enable an agent to log in to the Voice channel.

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.
- T-Server with associated switch and switching office.
- A Switch that is configured with DNs that correspond to agent devices in the switch.
- Agent logins that are configured in the Switch that can be referred by agents.
- A Place that contains one or more DNs from the Switch.

Start

For each agent that you want to configure to use the Voice channel, do the following:

1. Reference at least one `AgentLogin` from the Switch.
2. Check the `isAgent` flag.
3. Set a default Place. (Optional)
4. Allow the voice media privilege (see Voice Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role, allowing an Interaction Workspace privilege, and assigning a Role to an agent or agent group).
5. Allow the voice media privileges that you want the agent to use (see Voice Privileges).
6. Configure the voice options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Voice configuration option reference for a list of Voice options and a description of how to configure them).

End

> **Tip**
>
> Agents sometimes click **Hang up** by accident while handling a call. Use the voice.prompt-for-end option to ensure that a confirmation dialog box is displayed so that the call is not ended accidentally.

4. Provisioning a hybrid voice agent

Example: Provisioning a hybrid Skype for Business and Workspace SIP Endpoint agent

[**Added:** 8.5.117.18]

In the past, Workspace has supported a single Voice channel represented by a softphone (Workspace SIP Endpoint, Skype for Business, and so on) or a hard phone during an agent session. Beginning with 8.5.117.18, you can set up agents to have multiple voice devices on the same Place so that they can be hybrid agents with typically at least one voice device, being a softphone, and the second one a hard phone or another softphone. Typical device combinations include:

- Skype for Business DN + SIP Server Voice DN (embedded SIP Endpoint or hard/soft SIP Phone)
- Skype for Business DN + Voice DN of a non-SIP Server system
- Voice DNs from any two voice systems (such as a third party vendor and SIP Server)

> **Important**
>
> In hybrid mode, two voice channels are supported, but only one IM channel can be supported. If hybrid mode agents are set up to use IM, all IM interactions should be handled by the same T-Server (SIP Server or T-Server for Skype for Business) to avoid functional issues. Furthermore, it is not possible to send IMs between SIP Server and Skype for Business Server.

With this configuration, agents can make calls and Workspace selects the best device to use according to configuration and internal rules to select the best way.

During login, the agent chooses a Place that is set up to support multiple devices.

While logged in, the agent can independently control and view the status of the two devices in the **My Channels** tab.

Supervisors can monitor any device for silent monitoring, coaching, and barge-in of hybrid agents as soon as Workspace supports the supervision capability of the corresponding voice channel.

> **Important**
>
> - If both voice channels are software devices running on an agent workstation, this solution supports a single headset for both devices.
> - The two devices cannot be used simultaneously. One call must be on hold while the other is active. If an agent accepts a call on another device, the first device is automatically put on hold.

Purpose:

To enable an agent to log in to two separate Voice channels, one for Skype for Business and one for Workspace SIP Endpoint.

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- A Workspace `Application` object exists in the Configuration Database.
- T-Server with associated switch and switching office.
- A Switch that is configured with DNs that correspond to agent devices on the switch.
- Agent logins that are configured on the Switch that can be referred by agents.
- An environment that contains one T-Server for Skype for Business and one SIP Server and associated Switches.
- (optional) ISCC connection between SIP Server and T-Server for Skype for Business, using **cast-type**= `route`.
- A Trunk between SIP Server and Skype for Business Server.
- A Place that contains one voice DN from SIP Server and one DN from the Skype for Business Switch.

Start For each agent that you want to configure to be a hybrid Voice agent, do the following:

1. Reference at least one `AgentLogin` from the Switch.
2. Check the `isAgent` flag.
3. Set a default Place. (Optional)
4. Allow the voice media privilege (see Voice Privileges) for the role to which the agent is assigned (refer to the Procedure: Creating a Role, allowing an Interaction Workspace privilege, and assigning a Role to an agent or agent group).
5. Allow the voice media privileges that you want the agent to use (see Voice Privileges).
6. Configure the voice options in the `interaction-workspace` section of the Workspace `Application` object (refer to the Voice configuration option reference for a list of Voice options and a description of how to configure them).

7. In the `interaction-workspace` section, set the value of the `spl.switch-policy-label` on the Skype for Business Switch annex to `SIPSwitch::Lync`.
8. In the `interaction-workspace` section, set the value of the `display-name` or `display-name.<language-code>-<country-code>` option on the Switch annex to the display name of the switch object as you want it to appear in Team Communicator and the **My Channels** tab. The value of this option overrides the `name` property of the switch.
9. In the `interaction-workspace` section, set the value of the expression.callable-phone-number on the Switch or DN annex to the pattern of phone numbers that can be dialed from this switch or DN. You can use this option to limit the numbers that can be called from each switch or DN in a hybrid environment.

   Examples:

   a. You could configure the SIP Server to dial only outgoing calls and Skype for Business only for internal calls.

   b. If you have Skype for Business urls like these:

      - `sip:lync-user13_qa95@lyncdco13.lab`
      - `sip:lyncuser13_qa95@lyncdco13.lab`

      You could set the regular expression value of the `expression.callable-phone-number` option to `sip:\w+-?\w+@\w+\.\w+`.

10. Set the value of the voice.hybrid-switch-preference option to a comma-separated list of switch names in your hybrid environment. The order of the names specifies the preferred switch when the call policy does not favor either switch.

End

5. Enabling Workspace to play ring tones

Purpose: To enable Workspace to play ring tones for inbound interactions on one or more devices.

In Interaction Workspace 8.0 and 8.1, tones were played through the embedded Windows Media Player application on a single audio device that was configured as the default console sound device in the Windows Sound configuration panel. Starting from 8.5.0, the sounds are played through the Direct Sound API, which enables more flexibility on the device(s) that are used to play the sound.

The following procedure enables you to specify whether tones are played on the default audio device, a secondary audio device, or both.

A secondary audio device can be defined as either a specific audio device or all of the non-default audio devices. You can individually each configure sound (ringing bells, state changes, and so on).

All file formats that are playable by Windows DirectShow are usable (*.wav; *.mpa; *.mp2; *.mp3; *.au; *.aif; *.aiff; *.snd).

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

Start

1. Enable the secondary audio device(s) by specifying the value of the new application.secondary-audio-out-device configuration option to the name of the secondary audio device or by specifying the value `$AllNonDefault$` to enable all non-default audio divices.
2. The following existing configuration options have been modified in Workspace 8.5, and higher, to enable a tone to be played on the default audio device, a secondary audio device, or both.
   - webcallback.ringing-bell
   - chat.ringing-bell
   - chat.new-message-bell
   - email.ringing-bell
   - im.new-message-bell
   - im.ringing-bell
   - outbound-callback.ringing-bell
   - outbound.sound.campaign-updated
   - sms.ringing-bell
   - voice.ringing-bell
   - <media-type>.ringing-bell
   - accessibility.agent-state-change-bell
   - accessibility.interaction-state-change-bell
   - accessibility.warning-message-bell
   - broadcast.sound.minimal-priority
   - broadcast.sound.low-priority
   - broadcast.sound.normal-priority
   - broadcast.sound.high-priority
   - broadcast.sound.important-priority

   For each of these options, you can add an additional parameter to the end of the ringing sound configuration string:

   - `|primary`—Play the sound on the default audio output device
   - `|secondary`—Play the sound on the secondary audio device, as defined by the application.secondary-audio-out-device configuration option
   - `|both`—Play the sound on the default and secondary (application.secondary-audio-out-device configuration option) audio devices
3. You can restrict which sound files are pre-loaded when an agent logs in by using the sounds.preloadfiles option. Pre-loading only selected sound files at login can improve bandwidth performance at the start of

a shift when many agents log in simultaneously.

End

6. Declaring and using new Not-Ready Reason codes

Purpose:

To enable an agent to use custom Not-Ready Reason codes and to support the `aux work` mode.

The only Not-Ready Reasons that Workspace supports by default are `Unknown` and `After Call Work`. Custom Not-Ready Reason codes are defined in the `Action Codes` folder of the `Desktop` folder in the `Provisioning` view of Genesys Administrator Extension.

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

Start

1. Create a new Action Code in the following Genesys Administrator Extension view: `Provisioning > Desktop > Action Code`.
2. Enable the new Action Code so that it can be used in the Configuration Layer.
3. To enable the Action Code to display in the Agent Interface, configure the agent-status.enabled-actions-global option in the `interaction-workspace` section of the Workspace `Application` object (refer to the Agent status configuration option reference for a list of agent status options and a description of how to configure them).
4. Configure the Workspace agent-status.not-ready-reasons option to include the value that is specified in the Action Code (refer to the Agent status configuration option reference). Not-Ready Reasons are displayed in the order that is defined by the value of the agent-status.not-ready-reasons option. If no value is specified for the agent-status.not-ready-reasons option, the default behavior is to display all Not-Ready Reasons that are defined and enabled in the Action Code folder.

End

7. Storing the agent profile on a controlled shared host

[**Added:** 8.5.112.08]

Purpose:

To enable agents to store preferences and configuration information on a common directory instead of in the Configuration Database or their local workstation.

Genesys recommends using this feature in contact centers that have a large number of agents. The goal of this feature is to reduce the amount of information being sent back and forth between Workspace and Configuration Server. Workspace stores many agents specific preferences and other information both locally (on the agent's workstation) and in the Configuration Database. In some environments, this means that a large amount of configuration data is sent from Configuration Server to Configuration Server Proxy (CSP) and then from CSP to Workspace.

This feature also supports contact center where agents are not required to log in to Workspace from the same workstation each time. This feature supports agent roaming to different workstations. In environments where agents do not always use the same workstation, locally stored configuration data and personalized information is available only on the workstation where the agent first logged in. Use the following procedure to set up your environment to enable agents to roam by storing agent configuration, preferences, and personalized information in a common shared directory.

To set up your environment to support this feature, administrators should work with IT to set up a host where agent information is stored so that it does not have to be stored on Configuration Server or locally on the agent workstation.

Genesys recommends the following best practices that you can discuss with IT.

Security

When you create a directory on the host, the agent windows user must have write access. Workspace will write encrypted files that only Workspace running on the agent account can read. You do not have to create explicit permissions for the files. The files should inherit their permissions from the user's folder on the host. You can choose to set up a personal or a global shared directory.

When you implement the procedure below, agent information on Config Server will be merged with the new file location. Once that is complete, it will no longer be necessary for agents to have write access to the agent annex in the Configuration Layer; however, if you remove write access, you must grant it each time that that you need to change record location.

Recommendations about external storage selection

When you create the user profile storage on a network share, follow the Microsoft Windows Group Policy Object Management practices for the redirection of User Profile Folder, following the principles of the definition of the Network Share.

Genesys recommends one of two approaches; however, your IT might have other approaches that they might want to employ.

1. Personal Network Space

   Configure the agent workstations with a login script that assigns a Drive letter to a personal network space for the agent. In this scenario, the profile configuration can explicitly refer to this area. Security is ensured by the design of the Personal network share.

   For example: `G:\WDE\Profile`

2. Dedicated User Profile storage

   Microsoft recommends this approach to administrate the sharing of Roaming Profiles.

In this scenario, the IT administrator must define the first level of security when the share is configured. For example, refer to How to enable Roaming Profiles on Windows Server 2012 R2

A second level of security is implemented at run time by the capability for Workspace to restrict access permissions to the created folder and files. In Microsoft Windows, use the following optional setting for Folder Redirection configuration: **Grant the user exclusive rights**. This setting is enabled by default. This setting specifies that the administrator and other users do not have permissions to access this folder.

Share sizing suggestions

Use the following guidelines for *minimum* sizing requirements for each agent when setting up the storage folders.

- `externalUserSettings.conf`: Contains about 100 options and requires at least 10 KB
- Peronsal Favorites: 10 favorites is about 7 KB; 100 favorites is about 70 KB
- List of pushed-url: 10 items is about 3 KB; 100 items is about 30 KB
- List of Recents (recent contacts): 10 contacts is about 8 KB; 100 contacts is about 80 KB

Migration considerations

When Workspace starts, it checks to determine whether a value is specified for the options.record-location option. If no value is specified, Workspace does nothing. If a directory is specified, Workspace checks to determine if the directory exists a the location. If it does not exist, Workspace tries to create it; therefore, Workspace must have permission (*read/write access) to create directories and file on the specified location.

Workspace then compares the location specified by the `options.record-location` option with the last location where personal information was stored. If these locations are different, Workspace attempts to migrate the data from the previous location to the specified location.

If the migration fails, Workspace will attempt to complete the migration again the next time that the application is started; and, if the value of the options.clean-up-former-record-location option is set to `true`, Workspace will not remove data from the former location.

If the migration is successful and the value of the `options.clean-up-former-record-location` option is set to `true`, Workspace will remove data from the former location.

Migration use case 1

The User Profile was previously configured to be stored in Person's annex and is then configured to be stored in a shared directory. The content of the annex in the configuration layer is copied to the shared directory. Workspace will no longer access the Configuration Layer to store personal information.

Migration use case 2

The User Profile was previously configured to be stored in a shared directory and is then configured to be stored in Person's annex in the Configuration Layer. The content of the shared directory is copied to the Person's annex in the configuration layer. Workspace will no longer access the personal directory to store personal information.

Migration use case 3

The User Profile storage location is modified from one shared directory to another shared directory. The content of the first shared directory is copied to the second shared directory. Workspace will no longer access the first shared directory to store personal information.

> **Warning**
>
> Profile data that is stored on a workstation cannot be migrated.

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.
- Agent objects created in the Configuration Database.

Start

1. Create a shared directory on a host for your agents.
2. If you you have previously configured the value of the options.record-option-locally-only option to `true` to store the agent profile information locally instead of in the Configuration Database, set the value to `false`.
3. Use the options.record-location option to specify the path to the shared directory on the host that you created. The full path can also contain the following field codes: `$Agent.UserName$`, `$Agent.LastName$`,`$Agent.FirstName$`,`$Agent.EmployeeId$`,`$Env.X$` (where X is the name of the environment variable). Genesys recommends that you append the agent's `Username` to the specified path as shown above.

End

8. Enabling accessibility features

[**Modified:** 8.5.102.06, 8.5.109.16, 8.5.143.08]

Purpose:

To enable agents to use the accessibility and navigation features of Workspace.

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator

Extension.

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

Start

1. In Genesys Administrator Extension, open the Workspace Application.
2. Select the Application Options tab.
3. In the `interaction-workspace` section, configure the following option value:
   - accessibility.visual-impairment-profile: Specify `true` to optimize Workspace for keyboard navigation and screen reader applications.
   - In the `interaction-workspace` section, configure the following option values to specify whether or not the Interaction Preview should receive the focus when it is displayed on the desktop:
     - accessibility.focus-on-interaction-toast: Specifies whether all Interaction Notification views receive the focus when they are displayed. This option does not rely on accessibility.visual-impairment-profile; therefore, it applies to all configured agents, not just visually impaired agents. By default, the Interaction Notification views do not receive then focus automatically; agents must click the view to make it active.
     - accessibility.<media-type>.focus-on-interaction-toast: Specifies that all Interaction Notification views for the <media-type> receives the focus when they are displayed. When specified, this option overrides the value specified for `accessibility.focus-on-interaction-toast`. This option does not rely on accessibility.visual-impairment-profile; therefore, it applies to all configured agents, not just visually impaired agents.
4. In the `interaction-workspace` section, configure the following option values to add sounds to specific interface events:
   - accessibility.agent-state-change-bell: Specify the name of the sound file that you want to play to the agent when the agent changes state.
   - accessibility.interaction-state-change-bell: Specify the name of the sound file that you want to play when an interaction changes state.
   - accessibility.warning-message-bell: Specify the name of the sound file that you want to play when a warning message is displayed to the agent.
   - <media-type>.ringing-bell: Specify the name of the sound file that you want to play to the agent when an interaction of <media-type> is received.
   - chat.new-message-bell: Specify the name of the sound file that you want to play to the agent when a new chat message is received.
   - im.new-message-bell: Specify the name of the sound file that you want to play to the agent when a new IM message is received.
5. To enable the high contrast theme for visually impaired agents, in the `interaction-workspace` section, configure the following option value:
   - gui.themes : Specify only the value `HighContrast`.
6. To change the default display size of interface elements in Workspace views, use the gui.magnification-factor.

> **Important**
>
> This feature functions only with the default Workspace 8.5 GUI themes, and to custom themes that are developed according to the documentation and samples of the *Workspace Developer's Guide*. If the blue, royale, and fancy legacy themes are used, the magnification is forced to normal.

7. To enable agents to set the zoom of text editing fields, such as email, chat, and SMS, and transcript areas, use the gui.editor-zoom-range option to specify minimum and maximum text zoom. This feature applies to the following views:
   - IM (text entry, transcript, and interaction data tooltip)
   - Chat (text entry, transcript, and interaction data tooltip)
   - Email (text entry and inbound email view)
   - SMS (text entry, transcript, and interaction data tooltip)
   - Interaction history
     - IM
     - Chat
     - Email
     - SMS
   - Standard responses
   - Social media (text entry only)
8. To specify how long contextual warning messages are displayed to agents, set the number of seconds by using the alert.timeout option. You can specify that message notifications must be manually closed by setting the value to `0`.

End

9. Enabling security features

Purpose:

To enable the security features of Workspace.

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

Start

1. In Genesys Administrator Extension, open the Workspace Application.
2. Select the Application Options tab.
3. Configure any of the following options in the `Security` section:
   - security.disable-rbac: Specify whether Role Based Access is applied to agents to control access to Workspace features and functionality.
   - security.inactivity-timeout: Specify whether the agent workstation locks after a certain period of inactivity.
   - security.inactivity-set-agent-not-ready: Specify whether the agent is automatically set to `Not Ready` when agent inactivity is detected.
   - security.inactivity-not-ready-reason: Specify the default Not Ready Reason if the agent's workstation times out.
4. Configure any of the following options to control appearance of sensitive data in logs:
   - log.default-filter-type: Specify the default filter type for logging.
   - log.filter-data.<keyName>: Specify the treatment of log data. Enables you to filter for specific attached data keys, by specifying the key name in the option name.
   - sipendpoint.system.diagnostics.log_filter: Specifies the list of keys of SIP Messages for which the value should be hidden in the log files.

End

10. Creating Corporate Favorites

Purpose:

To enable the use of corporate favorites in the Team Communicator.

Prerequisites

- Genesys Administrator 8.0.2 or higher, configured to show Advanced View, or Genesys Administrator Extension.
- A working knowledge of Genesys Administrator Extension.
- An Workspace `Application` object exists in the Configuration Database.

Start

1. In Genesys Administrator Extension, open the Workspace Application.
2. Select the Application Options tab.
3. Create a new section and name it with the name of the Corporate Favorite that you want to create.
4. Configure the new Corporate Favorite section to be one of the following types:
   - `Agent`
   - `Agent Group`

- `Skill`
- `Queue`
- `Interaction Queue`
- `Routing Point`
- `Custom Contact`

The Table **Corporate Favorite Options by Type** defines the Corporate Favorite types and the mandatory options.

Corporate Favorite Options by Type

Type	Options	Mandatory	Valid values	Example
Agent	type	Yes	Agent	Agent
	id	Yes	<user name of the agent>	User123
	category	Yes	<a semicolon-separated list of category names>	CorporateCategory1;FavoriteAgen
Agent Group	type	Yes	AgentGroup	AgentGroup
	id	Yes	<name of the agent group>	Agent Group Meridian
	category	Yes	<a semicolon-separated list of category names>	CorporateCategory1;FavoriteAgen
Skill	type	Yes	Skill	Skill
	id	Yes	<name of the skill>	French
	category	Yes	<a semicolon-separated list of category names>	French Speaking Agents; Mandarin Speaking Agents
Queue	type	Yes	Queue	Queue
	id	Yes	DN number in the following format <DN>@<SwitchName>	123@MySwitch
	category	Yes	<a semicolon-separated list of category names>	CorporateCategory1;FavoriteAgen
Interaction Queue	type	Yes	InteractionQueue	InteractionQueue
	id	Yes	<script name of the interaction queue>	queue_email_inbound
	category	Yes	<a semicolon-separated list of category names>	CorporateCategory1;FavoriteAgen
Routing Point	type	Yes	RoutingPoint	RoutingPoint
	id	Yes	DN number in the following format	123@MySwitch

Type	Options	Mandatory	Valid values	Example
			<DN>@<SwitchName>	
	category	Yes	<a semicolon-separated list of category names>	CorpRoutingPoint
Custom Contact	type	Yes	CustomContact	CustomContact
	category	Yes	<a semicolon-separated list of category names>	External Resources
	firstname	No	<any string>	First
	lastname	No	<any string>	External
	phonenumber	Yes (one or both)	<a semicolon-separated list of phone numbers>	+1555234567890;+5551234543
	emailaddress		<a semicolon-separated list of email addresses>	external1@mail.dom; external2@mail.dom

5. The list of corporate favorites can be defined by the teamcommunicator.corporate-favorites options or by using the `teamcommunicator.corporate-favorites` field in an XML file.

   Configure one or both of the following options in the `interaction-workspace` section of agent, agent group, tenant, and/or application annexes:

   - teamcommunicator.corporate-favorites: The list of corporate favorites (quick dial favorites) that are configured in the Configuration Layer in GAX or in a XML file containing corporate favorites for an Agent, Agent Group, Skill, Routing Point, Queue, Interaction Queue, or Custom Contact in the same tenant as the agent. Favorites that are configured at the agent level take precedence over those that are configured at the agent group level, which take precedence over the tenant level, which takes precedence over the application level.
   - teamcommunicator.corporate-favorites-file: The name and the path to an XML file that contains a list and definition of each corporate favorite. The path can be relative to the Workspace working directory (for example: `Favorites\CorporateFavorites.xml`) or an absolute path (for example: `C:\PathToFavorites\CorporateFavorites.xml`).

   The corporate favorites functionality works in one of **three** ways, depending on how you choose to configure the two options and whether corporate favorites are specified in the Configuration Layer or in an XML file:

   - If teamcommunicator.corporate-favorites-file is *not* configured and corporate favorites are specified in the Configuration Layer.
     - Workspace selects corporate favorites only from the list of favorites specified by the teamcommunicator.corporate-favorites option for the Main Window Team Communicator and the Interaction Window Team Communicator.
     - Corporate Favorites in the Interaction Window Team Communicator, for operations such as transfer and conference, can be overridden by favorites specified by a transaction object override.
   - If teamcommunicator.corporate-favorites-file *is* configured, an XML file is present, the XML file *does not* include the **<teamcommunicator.corporate-favorites>** parameter, and the teamcommunicator.corporate-favorites option *is* configured in the Configuration Layer.
     - Workspace searches for corporate favorites from the list of favorites in the XML file that are specified by the teamcommunicator.corporate-favorites option.

- Corporate Favorites in the Interaction Window Team Communicator, for operations such as transfer and conference, can be overridden by favorites specified by a transaction object override *only if* those favorites are included in the XML file.

- If teamcommunicator.corporate-favorites-file *is* configured, an XML file is present, and the XML file *includes* the **<teamcommunicator.corporate-favorites>** parameter, for example:

```
<interaction-workspace>
 <teamcommunicator.corporate-favorites>fav2;fav3</teamcommunicator.corporate-
favorites>
 </interaction-workspace>
```

  - Workspace selects only corporate favorites from the XML file specified by the **<teamcommunicator.corporate-favorites>** parameter for the Main Window Team Communicator and the Interaction Window Team Communicator.
  - Workspace ignores the teamcommunicator.corporate-favorites option in the Configuration Layer.
  - For operations such as transfer and conference, corporate favorites *cannot* be overridden by a transaction object.

6. To enable each interaction to have an independent list of corporate favorites that are dynamically loaded into the corporate favorites in the team communicator view of the current interaction, configure the following options:

   a. Configure a Transaction object of type `list`. For example, you could configure a Transaction object that is named: `IW_CorporateFavoritesOverrideOptions`.

   b. In the `interaction-workspace` section configure the `teamcommunicator.corporate-favorites` option to a value such as `fav1` as described in the previous steps.

   c. To the `interaction.override-option-key` option in the `interaction-workspace` section, set a valid key name, for example `IW_OverrideOptions`.

   d. Add the Transaction object name to the `AttachedData` in your strategy. In this example, set the value of `IW_OverrideOptions` to `IW_CorporateFavoritesOverrideOptions`.

   Refer to the Modifying a Routing Strategy to Override Workspace Options, Based on Attached Data section for a general description of this mechanism.

End

Corporate Favorites sample XML

The following is an example of an XML file that is used to define corporate favorites:

```
<?xml version="1.0" encoding="utf-8"?>
<options>
<interaction-workspace>
<teamcommunicator.corporate-favorites>fav2;fav3</teamcommunicator.corporate-favorites>
</interaction-workspace>
<fav3>
<category>Partners</category>
<type>Agent</type>
<id>Jim</id>
</fav3>
<fav2>
<category>CorporatePartners;Partners2</category>
<type>Agent</type>
<id>John</id>
```

```
</fav2>
<fav4CustomContact>
<category>CorporatePartners</category>
<type>CustomContact</type>
<firstname>Bob</firstname>
<lastname>Davis</lastname>
<phonenumber>+12121231234;+18001231234</phonenumber>
<emailaddress>bob@genesys.com;sales@genesys.ca</emailaddress>
</fav4CustomContact>
<fav5RoutingPt>
<type>RoutingPoint</type>
<category>RoutingPoint</category>
<id>122@LucentG3</id>
</fav5RoutingPt>
<fav6AgentGroup>
<category>CorpAgentGroup</category>
<type>AgentGroup</type>
<id>Agent Group Meridian</id>
</fav6AgentGroup>
<fav7Skill>
<category>CorpSkill</category>
<type>Skill</type>
<id>Email-QualityConfidencePercentageSkill</id>
</fav7Skill>
<fav8ACDQueue>
<category>CorpACDQueue</category>
<type>Queue</type>
<id>8000@1LucentG3</id>
</fav8ACDQueue>
<fav9IxnQueue>
<category>CorpIxnQueues</category>
<type>InteractionQueue</type>
<id>route-to-agent-group-8002</id>
</fav9IxnQueue>
</options>
```