Workspace Desktop Edition Deployment Guide

Configuring system-access permissions

4/2/2025

Configuring system-access permissions

Contents

For Workspace to run correctly, the agent application must be granted permission to access specific system objects. When Workspace is launched, it connects to Configuration Server using the credentials of the agent who is logging in. Therefore, the required permissions to access system objects are typically much higher than those granted to an agent who uses Workspace.

To mitigate this situation you must assign three different kinds of permissions to the agent login:

- Execute permissions
- Read permissions
- Write permissions

The following subsections describe how to configure these permissions in the Permissions tab of the specified object. You can choose to configure agents individually by the Person object, or as a group by Access Group.

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

Configuring execute permissions

You must grant execute permissions for the Workspace application to each agent or groups of agents so that Workspace can connect to Configuration Server to start the application.

Configuring read permissions

Agents might require permissions to read from the Application objects that are referenced in the Connection list of the Workspace application object. They might be required to connect to one of these servers to activate its associated features. The following is a list of items to which an agent might require read access:

- The host of any application objects that are referenced in the Connection list of the Workspace application object.
- The Person object that corresponds to the agent.
- The Place object that corresponds to the voice channel to which the agent is assigned.
- The DN object that determines the capacity of the channel (Voice, IM). This information is stored in annex of the DN.
- The Switch and the T-Server object to determine the possible channel.
- The Tenant object.
- The Person objects of the Tenant to enable Team Communicator to access the firstname, lastname, and username of internal targets.
- The Skills objects of the Tenant to enable Team Communicator to access the names of Skills.
- The Agent Group objects of the Tenant to enable Team Communicator to access the names of Agent Groups.
- The Routing Point objects of the Tenant to enable Team Communicator to access the number, name, and

switch.name of Routing Points.

- The ACD Queue objects of the Tenant to enable Team Communicator to access the number, name, and switch.name of ACD Queues.
- The User Properties of the agent's Tenant, logged in application, and agent's Agent Groups, to read corporate favorites for display in Team Communicator.
- The Business Attributes of the Tenant to enable the Contact module to use Business Attributes.
- The transaction object of the Tenant that can be used for overriding options of the strategy.
- The applications used as Backup servers and configuration Server application to have HA.
- Script objects of the tenant Interaction queue and workbins.
- The Calling List, Table Access, DB Access Point Application of Table Access, Format, Field objects reflecting the data structure of the campaigns where the agent will be engaged.

Configuring write permissions

If you have configured the agent to store preferences in their Person annex instead of on their local desktop or in a shared directory, you must grant that agent write permissions on their Person object.

If you plan to store agent preferences and personal information on a shared directory, refer to Storing the agent profile on a controlled shared host.

If you have configured your system to prompt for a the agent's phone number at login time (this requires SIP Server), you must grant write access to the agent on the SIP DN in which the agent logs in, to set the `request-uri`.