Workspace Desktop Edition Deployment Guide

Role-based approach of Genesys 8

5/8/2025

Role-based approach of Genesys 8

[**Modified:** 8.5.143.08]

> **Tip**
> You no longer have to use Genesys Administrator to create agent Roles for Workspace Desktop Edition. Workspace also supports the Role storage model of Genesys Administrator Extension 9.0.100.56 or higher. [**Added:** 8.5.143.08]

Contents

Genesys Administrator Extension is used to create Roles that contain a list of privileges. Roles are defined as the set of privileges that are either Allowed or Not Assigned. Each agent receives only what is needed to complete the privileges that relate to the Role of that agent; everything else is inaccessible. Genesys Administrator Extension enables the assignment of a Role to an Access Group or a Person.

> **Tip**
> Users have no default assigned Role. Roles have no default granted privileges.

Depending on the privileges that are granted to an agent, Workspace enables the following:

- Module activation — Triggering of module download from the ClickOnce server; this modifies the footprint of the agent desktop application.
- User Interface rendering — Includes the display of menu items, toolbar buttons, and views.

Refer to the Procedure: Creating a Role, allowing a Workspace privilege, and assigning a Role to an agent or agent group to create or modify a role and assign privileges to an agent or Agent Group.

Role- and Privilege-Based Models

Workspace implements Role-Based Access Control (RBAC). RBAC enables administrators to limit agents to specific channels, interactions, and so on, based on their permissions.

> **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.

Workspace supports both the Genesys Administrator Role data storage model, introduced by Management Framework 8, and the Genesys Administrator Extension Role data storage model (as implemented in Genesys Engage cloud). The following are the general rules for Roles defined for Workspace:

- In one environment, you can define both Genesys Administrator and Genesys Administrator Extension Roles.
- Each Role is defined and stored either in a Genesys Administrator storage model or a Genesys Administrator Extension storage model.
- The Person (agent) object can be assigned to Roles defined by both Genesys Administrator and Genesys Administrator Extension.

The system administrator defines a Role for each agent. The Role has a series of privileges that are

associated with it; in this way, agents do not have access to privileges or functionality that are outside their assigned Roles.

RBAC enhances system security by limiting agent access to the system. This is critical for protecting the system against accidental or intentional damage. Accidental damage can occur if an agent is accessing a part of the system that is outside of the area of responsibility of that agent.

RBAC enables you to update your system easily. If agents change responsibilities or new agents are added, you do not have to assign permissions to those agents based on their username. When you create or modify an agent, all that you have to do is set the Role of that agent; system access is determined automatically. As soon as the agent logs into the system, the identity of that agent determines access. Individual permissions do not have to be set for new or modified users.

To facilitate RBAC, Workspace is constructed as a collection of modules that encompass privileges or related privileges. RBAC selects only those modules that pertain to the Role of the agent and are necessary for the context of the functions that are accessible to the agent.

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. You can set this option to `true` when you deploy the application in your testing lab to evaluate and test the application. Refer to Role Privileges for a list of all the privileges.

Views (Modules and Groups of Privileges)

Modules are assembled into views. Each module, set of modules, or view is related to a privilege or set of privileges. Privileges are implemented by modules. In a ClickOnce environment; when an agent logs in to Workspace, modules are transferred to the client desktop. The modules that are transferred are dependent upon the Role that is assigned to the user with that login.

Privileges implemented by Workspace

This section introduces the privileges that are implemented by Workspace. The privileges are grouped logically by action and access type:

- Voice actions
- Instant Messaging actions
- Statistics access
- Contact actions
- Team Communicator actions
- eServices actions
- Standard Response Favorites actions

Voice actions

Voice action privileges enable a variety of capabilities, including the use of the Voice media, transfer, conference, disposition, answering, rejecting, and making calls.

Instant Messaging actions

Instant Messaging (IM) actions enable agents to use the IM media for internal communication, and to make and release IM sessions.

Statistics access

Statistics access privileges enable the viewing of Key Performance Indicators (KPIs) and contact center statistics by agents.

Contact actions

Contact action privileges can be used to enable a wide variety of contact related privileges including marking done interactions, merging contacts and interactions, creating contacts, deleting contacts, and saving changes to contacts. Contact action privileges also enable access to Interaction Workspace features such as Contact history, information, directory, details, notepad, and case data.

Team Communicator actions

Team Communicator privileges enable contacts to use the Team Communicator feature to contact internal targets, create and use favorites, and view recent contacts.

eServices actions

eServices privileges for E-Mail, Chat, Video, Web Callback, Workitems, and Workbins. For more information on the privileges implemented by Workspace, refer to Workspace Functionality Overview.

Standard Response Favorites actions

Standard Response Favorites privileges enable the agents to save a list of favorite responses from the SRL.