Contact Center Advisor and Workforce Advisor Administrator User's Guide

Role Based Access Control

12/14/2025

Contents

- 1 Role Based Access Control
  - 1.1 Roles and Permissions
  - 1.2 Object Permissions in Advisors
  - 1.3 Privileges in Advisors
  - 1.4 Assigning Roles to Users and Access Groups
  - 1.5 Multiple Roles
  - 1.6 New Users
  - 1.7 Default Roles Created by Migration
  - 1.8 Further Reading on Roles

Role Based Access Control

Because Advisors uses Configuration Manager business attributes, Advisors can take advantage of Genesys roles for controlling access at a very detailed level to Advisors business objects and metrics. This is referred to as role-based access control (RBAC).

The major component of RBAC is a role. Roles define what facilities are provided to users to review and manipulate various types of data. These include which property controls are available for items permitted by object permissions, what modules are visible, and access control for entities not represented by configuration objects. A role is assigned to a user, and that user is then able to do only what that role permits.

A role may also be assigned to an access group, and users in that access group are then able to do what the role permits. Roles consist of a set of role privileges. Role privileges are tasks that can be performed on a given type of data. They are defined in Genesys Configuration Manager.

By default, role privileges are not assigned to any role, so you must explicitly assign privileges to roles. Role privileges range from general to very specific tasks—see Advisors Privileges. An authorized user, normally a System Administrator, bundles these tasks into roles. These roles are then assigned to users. As a result, each user can perform only those tasks for which they have privileges.

RBAC is enforced primarily by visibility in the interface. What a user sees is determined by the roles which have been assigned. If the user is not assigned a role that grants them access to a piece of functionality, that functionality is not displayed to the user.

Roles and Permissions

Elementary permissions protect access to a whole object. Roles are intended to work with permissions to more finely tune what a user can access.

So, the permissions applied to the object apply equally to all properties of the object—if you have access permissions, you see the entire object.

Roles, on the other hand, serve to protect properties of an object by hiding or disabling those properties to which you want to restrict access.

Different roles can have different access and allowed functionality for the same objects. In essence, roles resolve both problems with using permissions—users can access and work with only those parts of the object to which they are allowed.

Roles can also be used to protect access to entities that are not configured as configuration objects, such as logs. In general, when determining the accessibility of an object to a user, the user session cannot retrieve objects if they are not among those objects to which the user has access (as defined by object-access permissions). Then, for that data that is available in the session, role privileges refine what can be done with the data.

One user can be assigned multiple roles, and one role can be assigned to multiple users. There is no

limit to the number of roles that can be present in the Configuration Manager.

Object Permissions in Advisors

Object permissions determine which users have access to a certain object or what objects a given user has access to. This is done through the use of access groups or on an individual user basis. Objects include the following:

- Contact Center Advisor and Workforce Advisor
  - Metrics
  - Operating Units
  - Reporting Regions
  - Geographic Regions
  - Contact Centers
  - Application Groups
- Frontline Advisor
  - Metrics
  - Levels of the Frontline Advisor hierarchy (that is, the folders and agent groups)

There is no limit on the number of access groups that are supported by the Advisors.

> **Tip**
> In Advisors release 8.1.1, three special access groups were introduced to represent the three different types of users in Advisors (Super Administrator, Partition Administrator and Dashboard User). From release 8.1.2, these access groups are no longer required. Unless they are used to actively manage object permissions, they can be removed from the Configuration Manager.

Multiple Access Groups

A single user can belong to multiple access groups, with different permissions coming from each group. In such scenarios, the user’s permissions are a union of the permissions of all the access groups to which he or she belongs.

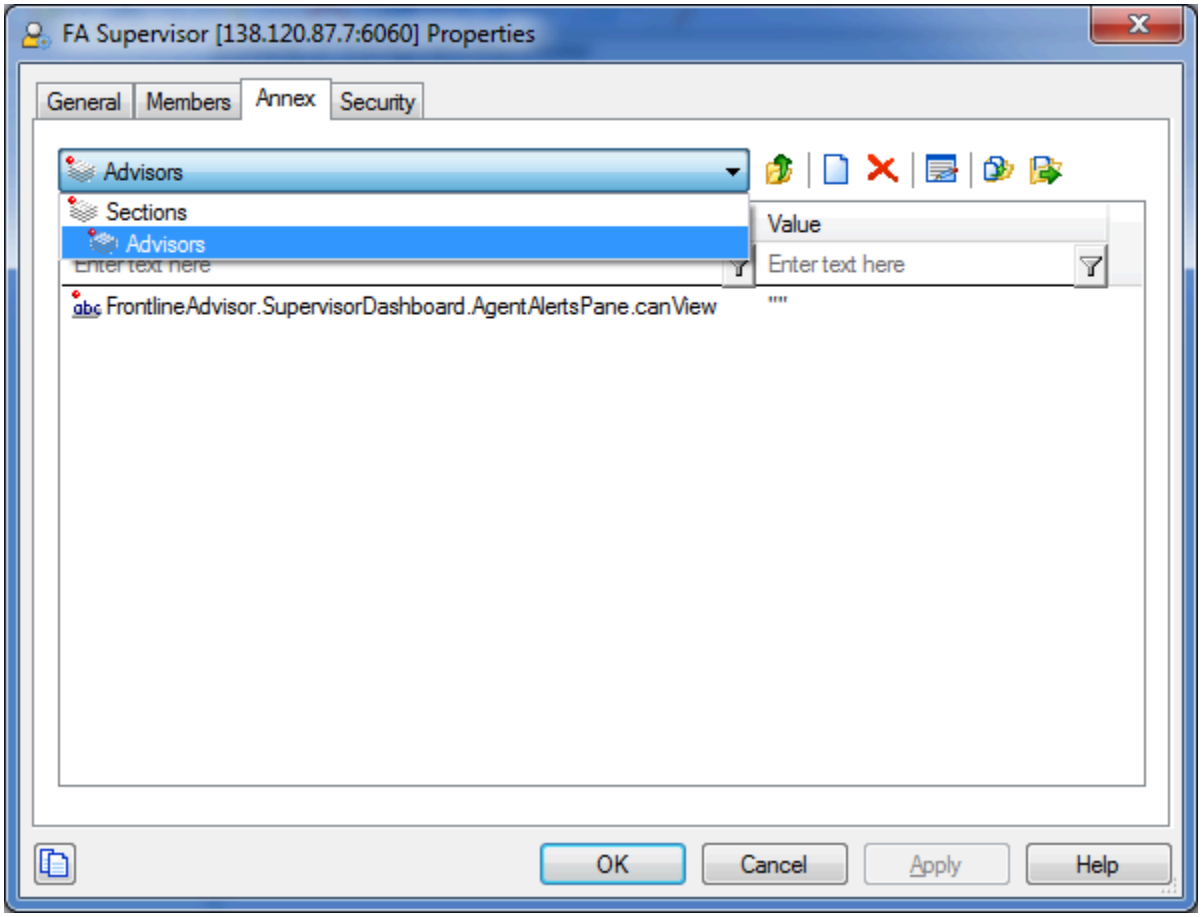
Advisors follow the principle of least privilege. The following scenarios show how this union should work:

- User A is part of access groups X and Y. Group X does not have any defined access to a metric. Group Y has explicit access granted to the metric. In this case, user A is granted access to the metric.
- User A is part of access groups X and Y. Group X is explicitly denied access to a metric. Group Y is explicitly given access to the same metric. In this case, user A is denied access to the metric.

- User A is part of access groups X and Y. Group X is explicitly denied access to a metric. Group Y does not have any defined access to the same metric. In this case, user A will be denied access to the metric.
- User A is part of access groups X and Y. Neither group has defined access to the metric. In this case, user A will be denied access to the metric.

Privileges in Advisors

Functionality permissions, or privileges, determine what tasks or functions a user can execute on objects he/she has access to. Privileges are configured via roles. Privileges for each role are stored as key-value pairs in the Annex tab of that role in Genesys Configuration Manager. For example, below shows the Annex tab of a new role called `FA Supervisor` who can view the `Agent Alerts` pane on the Supervisor dashboard:



Assigning Privileges to a Role

The privileges for Advisors are bundled under a single section in the `Annex` tab with the title `Advisors`. Each privilege name uses the following general structure:

[application name].[module name].[task grouping].[privilege name]

If a privilege is present in a role, then any users assigned that role have access to the functionality

controlled by that privilege. The value for the privilege key can be anything, or can be left blank.

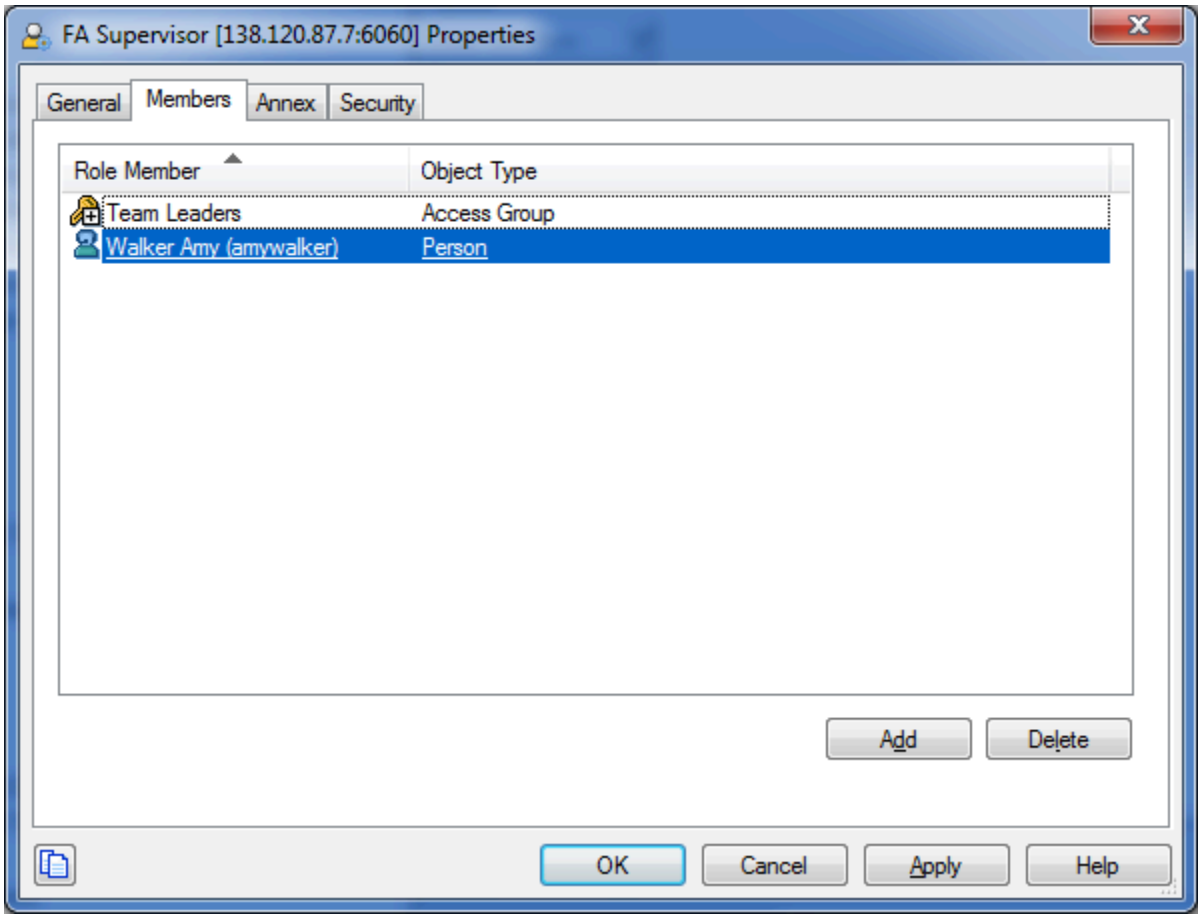
Accumulation of Privileges

Roles are cumulative. A single user or access group can have multiple roles associated with them. The privileges in these roles are cumulative.

Assigning Roles to Users and Access Groups

Roles can be assigned to either users or access groups. This assignment is done on the `Members` tab of the role as shown in the following screenshot.

> **Important**
>
> To inherit permissions, access groups and users must belong to the tenant specified in the Advisors Platform installer.



Assigning Roles to Users and Access Groups

In the preceding screenshot, the role `FA Supervisor` has been assigned to:

- The `Team Leaders` access group
- User `Amy Walker`

Once a role is assigned to an access group, all users in the access group are assigned that role. The access groups and/or users must have Read access to the role in the `Security` tab in order to be able to access the role.

> **Important**
> Names of access groups must not contain spaces.

Multiple Roles

You can assign more than one role to a user. In such cases, the user will have the combined set of privileges granted by each role. In other words, the user is granted any privilege that is granted by at least one of the assigned roles. This ensures that the user is able to perform the tasks of all roles in which they participate.

New Users

By default, new users are not assigned any default roles. They must be assigned roles by a System Administrator or by an existing user with appropriate privileges.

Default Roles Created by Migration

Module access is no longer determined by entries in a user's `Annex` tab. Instead, module access is determined by the roles associated with the user's profile. An optional section of the migration utility provided in the software distribution creates this new module access schema.

Seven default roles are created by the utility in the Configuration Manager, with each one representing access to a particular module. Each role has a limited set of privileges associated with it. The default roles are:

- AdvisorsAdmin
- AdvisorsFAUser
- AdvisorsFAAdmin
- AdvisorsFAAgent

- AdvisorsCCAdvUser
- AdvisorsWAUser
- AdvisorsAlertMgmtUser

These role names can be changed post-migration.

Further Reading on Roles

Additional sources of information on role-based access, privileges and permissions are:

- Genesys 8.1 Security Deployment Guide
- Framework 8.1 Genesys Administrator Deployment Guide
- Framework 8.1 Configuration Manager Help
- Genesys Administrator 8.1 Help