Frontline Advisor Administration User's Guide

FA Access Privileges

12/16/2025

FA Access Privileges

You can control access to information in the Genesys Frontline Advisor (FA) dashboard and on the FA administration page using roles, and associating permissions and privileges with each role. Controlling information using roles, and associated privileges and permissions, is called Role-Based Access Control (RBAC).

<tabber>

|-| RBAC and Advisors=

Performance Management Advisors support role-based access control (RBAC). You can use RBAC to control which users can access specific components—for example, use Genesys' RBAC to configure access to the Administration module for a specific subset of managers.

Advisors use Configuration Manager business attributes, which means Advisors can take advantage of Genesys roles for controlling access at a detailed level to Advisors' business objects and metrics.

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.

There are three important concepts associated with RBAC:

- Permissions
  Permissions protect access to a whole object; if you have access permissions, you see the entire object.
- Roles
  Roles protect properties of an object by hiding or disabling those properties to which you want to restrict access. Roles are intended to work with permissions to more finely tune what a user can access.
- Privileges
  Privileges determine what tasks or functions a user can execute on objects to which he or she has access. You assign privileges to roles to further refine access to objects and object functionality.

What are RBAC permissions?

Elementary permissions protect access to a whole object. Permissions applied to an object apply equally to all properties of the object – if you have access permissions, you see the entire object.

Object permissions determine which users have access to a certain object or to what objects a given user has access. 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)

> **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). Starting in 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.

What are RBAC roles?

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. One user can be assigned multiple roles, and one role can be assigned to multiple users. 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.

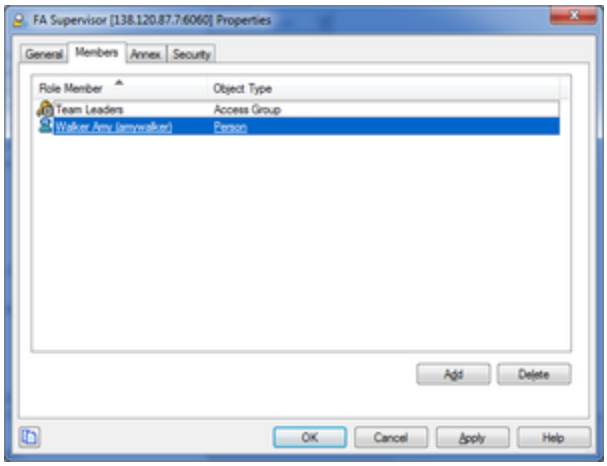
Different roles can have different access and allowed functionality for the same objects. In essence, roles resolve both problems associated with using only permissions – users can access and work with only those parts of the object to which they are allowed.

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 to an object by 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). For data that is available in the session, role privileges refine what can be done with the data.

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.

> **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 screenshot to the right, the role `FA Supervisor` has been assigned to:

- The `TeamLeaders` 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 to be able to access the role.

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

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 package 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

You can change the preceding role names 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

What are RBAC privileges?

Roles consist of a set of role privileges (Read, Change, Execute, and so on). Privileges determine what tasks or functions a user can execute on objects to which he or she has access. Role privileges 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. 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.

Functionality permissions, or privileges, determine what tasks or functions a user can execute on objects to which he or she has access. Privileges for each role are stored as key-value pairs in the **Annex** tab of that role in Genesys Configuration Manager. 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.

Where do I configure roles, permissions, and privileges?

You must have access to the Genesys Configuration Manager to complete the configuration of an Advisors installation and perform administrative functions. Roles are defined, maintained, and associated with users in the Genesys Configuration Server using the Configuration Manager.

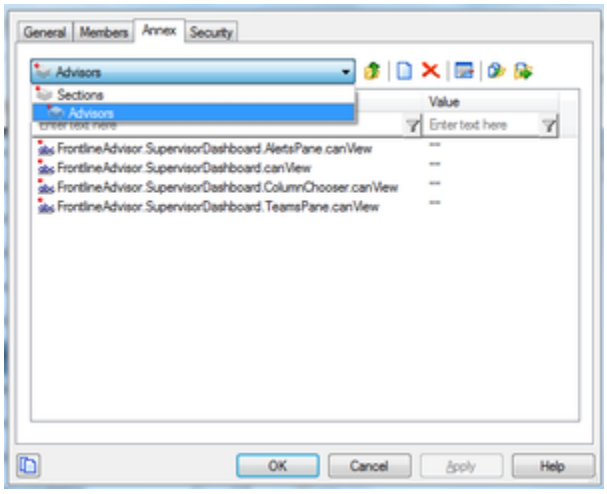
Typically, you configure RBAC in Configuration Manager in the following order:

1. Add roles.
2. Add tasks to roles.
3. Assign Access Groups to Business Attribute instances.
4. Assign users to roles.

Add users to a role on the **Members** tab of the properties dialog box for that role. Add users with one of the following methods:

- indirectly, as a member of an Access Group
- directly, as a member of a role

Assign permissions for a role on the **Security** tab of the properties dialog box for that role. A user must have Read access to the role (either directly or through an Access Group) to which he is assigned.



Annex tab for FA Supervisor role in Configuration Manager

Privileges for each role are stored as key-value pairs in the **Annex** tab of the properties dialog box for each role in Genesys Configuration Manager. The screenshot to the left shows the **Annex** tab of a new role called `FA Supervisor` – a user who can view the **Agent Alerts** pane on the FA dashboard.

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]

> **Important**
>
> Ensure you copy the exact privilege with no leading or trailing spaces. Some privileges work as single entries; some require a group of privileges to ensure full access as you expect. In the preceding example, all three privileges shown in the screenshot above are required so the user can view the Agent Alerts pane. See the list of privileges in the Privileges tab on this page for more information.

Am I limited to a specific number of users, access groups, or roles?

There is no limit on:

- the number of roles that can be present in the Configuration Manager
- the number of access groups or users that can be present in the Configuration Manager
- the number of roles supported by Advisors
- the number of access groups that are supported by Advisors

Roles, and the privileges associated with roles, are cumulative. A single user or access group can be assigned multiple roles. 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.

Each user can also 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, unless access is specifically denied for one group, which takes precedence (see the following scenarios).

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.

|-| RBAC and FA=

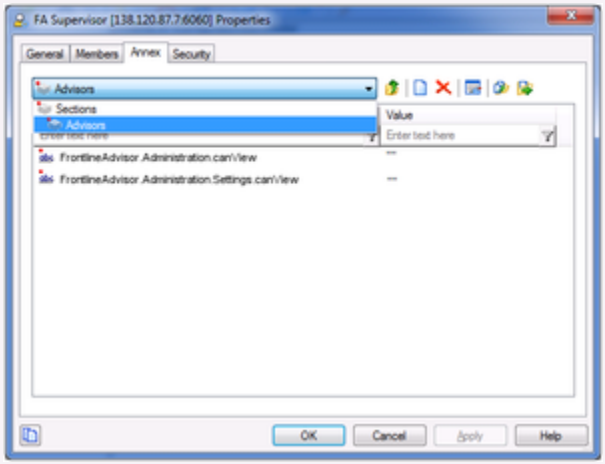
When managers log in to the Frontline Advisor dashboard or the Administration module, they are presented with a customized view of agent groups and agents relevant to them. With the introduction of role-based access control (RBAC) to Frontline Advisor, it is no longer assumed that managers can navigate to all child nodes simply because they have access to the parent. The opposite is also true; if a manager has access to child nodes, that manager does not automatically have access to the parent node. You can configure permissions in Genesys Configuration Manager such that a user can view only specific levels of the hierarchy.

For example, a group leader sees all teams and agents under them, but might see only the aggregated values at higher-level nodes in the hierarchy. To perform threshold or rule overrides at a given node, the manager must have explicit change permission for that node granted by an administrator in the Genesys Configuration Manager. In this example, the group leader is granted change access at the group level and below, but not at higher level nodes (because changes would affect other groups not even visible to this group leader).

Example of RBAC Use

RBAC can control access to areas of the FA administration page. For example, the **Settings** tab on the FA administration page is displayed only if the user has explicit role-based access to it. If such access is granted, it is granted to all settings, not just the ones that relate to the manager's team of agents. Access to the **Hierarchy Reload** section of the **Settings** tab is controlled separately. A user can have access to the **Settings** tab, but the **Hierarchy Reload** portion of the tab displays only if that user's role has that privilege granted.

In this example, our user is called FA Supervisor. To configure the scenario described above for this user, assign privileges to the FA Supervisor role using Configuration Manager to allow access to the **Settings** tab, but restrict access to the **Hierarchy Reload** section of that tab:



Assigning privileges for the FA Supervisor role in Configuration Manager

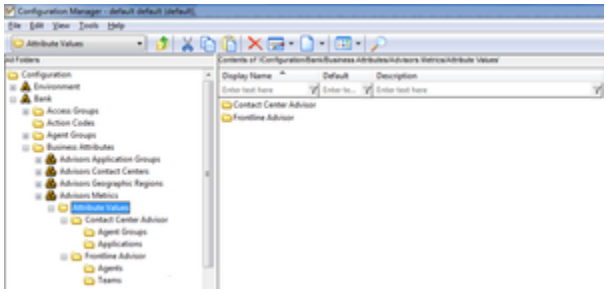
If you want the user to see the **Settings** tab, you must ensure you also assign the privilege that allows the user to access the administration module. The user's role does not include the privilege to reload the hierarchy – the **Hierarchy Reload** section of the **Settings** tab does not display for the FA Supervisor role.

When do I configure roles?

If it is important in your enterprise to control users' access to information (metrics, hierarchy levels, and business objects), you configure roles (including the assignment of permissions and privileges to each role) and users before any of those users log in to FA for the first time. Each time you have a new user in your enterprise, you assign that person to roles in Configuration Manager.

Controlling access to metrics

Metrics are handled differently than other Advisors business objects. Metrics for Contact Center Advisor, Workforce Advisor, and Frontline Advisor are stored under the Advisors Metrics business attribute; a folder structure segments the metrics for each application and for each object. The following screenshot shows an example of the folder structure for Advisors metrics in Configuration Manager. The folder structure shown below is mandatory. The business attributes must be created in the "Default Tenant" chosen during Advisors installation. Click on the image to enlarge it.



Advisors metrics in Configuration Manager

Each application's metrics are created under the appropriate folder, and are subdivided by the object types with which they are associated.

To avoid confusion over similarly named metrics, and because Configuration Manager does not allow duplicated names for attribute values, the names of the metrics use a namespace and are case-sensitive. The format of the namespace is:

[Application].[ObjectType].[Channel].[Name]

The values for each characteristic of the namespace are described in the following table:

Namespace characteristic	Definition or values
Application	FrontlineAdvisor, WorkforceAdvisor, or ContactCenterAdvisor
ObjectType	Represents the object type associated with this metric. This could be AgentGroup, Agent, Contact Group, Application, or Team
Channel	Email, WebChat, Voice, All, or AllNonVoice
Name	The name of the metric

For example, FA metrics would have names like:

- `FrontlineAdvisor.Agent.Voice.nch`
- `FrontlineAdvisor.Team.Voice.taht`

Interaction on the **Thresholds** tab of the FA administration page is also controlled by a user's access to metrics. A user can view and override only thresholds where they have access to the corresponding metric. Access to the metrics and levels in the hierarchy also determines which metrics and levels the user sees in the administration module.

|-| FA Privileges=

In Performance Management Advisors Frontline Advisor (FA), you use Role-Based Access Control (RBAC) to control users' access to:

- tabs on the FA administration page
- portions of tabs
- the entire FA dashboard

The following Table lists the privileges available in Configuration Manager for Frontline Advisor. The Table includes a description of the consequence to the user if the privilege is present or absent.

Privilege	Behavior When Present	Behavior When Absent
AdvisorsAdministration.Metrics.canView	User can access the Report Metrics page; option shown on menu.	Report Metrics option is not shown on the Administration menu.
AdvisorsAdministration.MMW.canCreate	User can create custom metrics.	The Create function and the Copy function do not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.canEdit	Grants privilege to edit any metrics.	The Edit function does not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.canDelete	Grants privilege to delete custom metrics.	The Delete function does not display in the Report Metrics Manager.

Privilege	Behavior When Present	Behavior When Absent
NEW AdvisorsAdministration.MMW.SourceMetrics.canView	Grants privilege to view the Source Metrics page.	The Source Metrics page, and the link to it in the Administration module, do not display.
NEW AdvisorsAdministration.MMW.SourceMetrics.canCreate	Grants privilege to create custom source metrics.	The `Create Source Metrics` button does not display on the Source Metrics page.
NEW AdvisorsAdministration.MMW.SourceMetrics.canEdit	Grants privilege to edit source metrics.	The Edit function does not display on the Source Metrics page.
NEW AdvisorsAdministration.MMW.SourceMetrics.canDelete	Grants privilege to delete custom source metrics.	The Delete function does not display on the Source Metrics page.
FrontlineAdvisor.SupervisorDashboard.canView	User can access the FA Supervisor Dashboard.	User cannot access the FA Supervisor dashboard, and the FA Dashboard tab is not shown to the user.
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege*	User can see the Teams pane.	The Teams pane is hidden along with both alerts panes.
FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges*	User can see the Team and Agent Alerts panes.	Neither of the alerts panes is displayed on the dashboard. If access to the Team pane is not available, the Alert pane is not shown even though user has access.
FrontlineAdvisor.SupervisorDashboard.ColumnChooser.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege*	User can access the column chooser.	The column chooser button on the dashboard is hidden.
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges*	User can sort the entries in the Team pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Team pane. The cursor does not change when hovering over a column header.
FrontlineAdvisor.SupervisorDashboard.TeamAlertsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges*	User can sort the entries in the Team Alerts pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Team Alerts pane. The cursor does not change when hovering over a column header.
FrontlineAdvisor.SupervisorDashboard.AgentAlertsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView*	User can sort the entries in the Agent Alerts pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Agent Alerts pane. The cursor does not change when hovering over a column header.

Privilege	Behavior When Present	Behavior When Absent
and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges		
FrontlineAdvisor.Administration.canView	User can access the FA Administration module.	User cannot access the FA Administration module, and the FA Administration tab is not shown to the user.
FrontlineAdvisor.Administration.Settings.canView *Requires the FrontlineAdvisor.Administration.canView privilege*	User can access the Settings tab in the FA Administration module.	Settings tab is not shown to the user.
FrontlineAdvisor.Administration.Hierarchy.canReload *Requires the FrontlineAdvisor.Administration.canView and FrontlineAdvisor.Administration.Settings.canView privileges*	User can initiate a hierarchy reload through the action on the Settings tab.	Hierarchy reload action is not accessible.
FrontlineAdvisor.AgentDashboard.canView	User can access the FA Agent Dashboard.	User cannot access the FA Agent dashboard, and the FA Agent Dashboard tab is not shown to the user.
FrontlineAdvisor.AgentDashboard.AlertsPane.canView *Requires FrontlineAdvisor.AgentDashboard.canView privilege*	User can see the Alerts pane.	The Alerts pane is not displayed.
FrontlineAdvisor.AgentDashboard.ColumnChooser.canView *Requires FrontlineAdvisor.AgentDashboard.canView privilege*	User can see the Column Chooser.	The Column Chooser is not displayed.