Frontline Advisor Administration User's Guide

Control Access to Information

5/13/2025

Control Access to Information

Contents

You can control access to information in the 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).

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. FA objects are metrics and the levels of the hierarchy.
- Privileges
  Privileges determine what tasks or functions a user can execute on objects to which he or she has access. For the list of objects and functionality controlled by privileges, see Privileges.
- Roles
  Roles protect properties of an object by hiding or disabling those properties to which you want to restrict access. You assign privileges to roles to further refine access to objects and object functionality.

A role may be assigned to an access group, and users in that access group are then able to do what the role permits. A role can also be assigned to a user, and that user is then able to do only what that role permits. Roles consist of a set of role 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.

When managers log in to the dashboard or the Administration module, they are presented with a customized view of agent groups and agents relevant to them. Using RBAC, 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 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).

Can a user belong to more than one role?

Roles are cumulative. There is no limit on the number of roles supported by Advisors. A single user can belong to multiple access groups, with different permissions coming from each group. The privileges (Read, Change, Execute, and so on) associated with these roles are cumulative and are a union of the permissions of all the access groups to which he or she is assigned, unless No Access is specified, which takes precedence.

Who assigns privileges to roles and roles to users?

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.

Where do I configure roles, permissions, and privileges?

To complete the configuration of an Advisors installation and perform administrative functions, you must have access to the Genesys Configuration Manager. Roles are defined, maintained, and associated to 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 either 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.

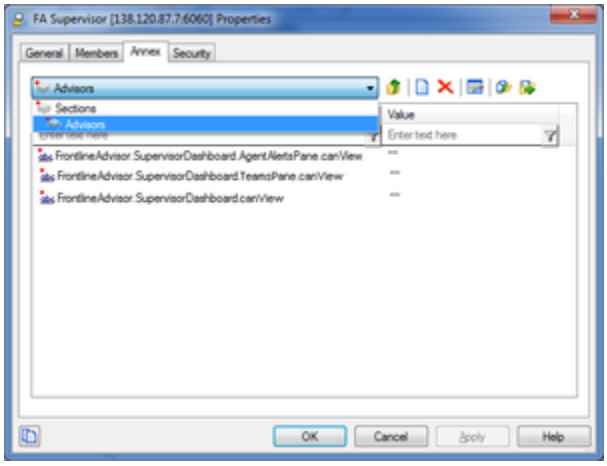
Privileges determine what tasks or functions a user can execute on objects to which he or she has access.

Privileges for each role are stored as key-value pairs in the Annex tab of the properties dialog box for each role in Genesys Configuration Manager. 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.

If a privilege is present in a role, then any user assigned that role has access to the functionality controlled by that privilege.

The following screenshot shows the Annex tab of a new role called FA Supervisor – a user who can view the Agent Alerts pane on the FA dashboard:

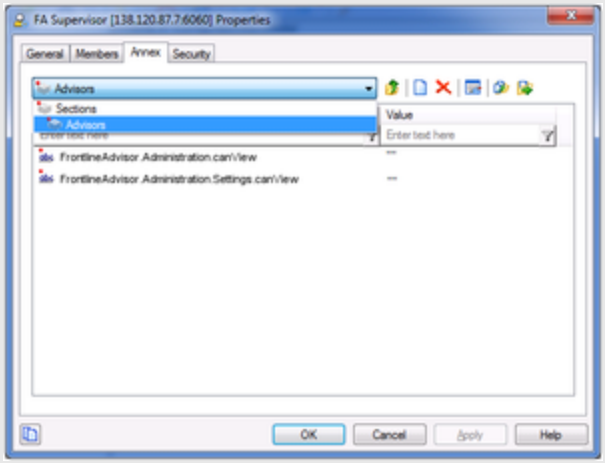


Annex tab for FA Supervisor role in Configuration Manager

Example

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

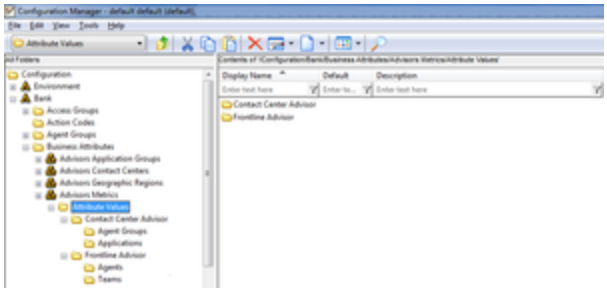
If you want the user to see the Settings tab, you must ensure you also assign the privilege that allows the user to access the Administration module. The user's role does not include the privilege to reload the hierarchy – the Hierarchy Reload section of the Settings tab does not display for the FA Supervisor 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 from other Advisors business objects. Because 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 they are associated with.

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_1 FrontlineAdvisor.Team.Voice.taht_2

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.

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

- 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.