Frontline Advisor Administration User's Guide

Role-Based Access Control for FA

3/3/2025

Role-Based Access Control for 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 Configuration Server 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 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).

Interaction on the **Thresholds** tab of the FA administration page is 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 determines which metrics and levels the user sees in the administration module.

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 might have access to the **Settings** tab, but not to the **Hierarchy Reload** portion of the tab.

In this example, our user is called FA Supervisor. To configure the scenario described above for this user (allow access to the **Settings** tab, but restrict access to the **Hierarchy Reload** section), you assign privileges to the FA Supervisor Role using a Genesys configuration interface, such as Genesys Administrator or GAX.

Some privileges are dependent on others in order to work as expected. For example, 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. If the user's Role does not include the privilege to reload the hierarchy, then the **Hierarchy Reload** section of the **Settings** tab does not display for the FA Supervisor role.

See FA Access Privileges for the list of Frontline Advisor privileges, including notes about privilege dependencies.

> **Tip**
>
> While you can use any Genesys configuration interface to import Advisors privileges into a Role, or to assign Role-based permissions to Persons or Access Groups for

> access to the Advisors business attributes, you can view the Advisors privileges associated with a Role only in Genesys Configuration Manager. For more information about RBAC and Advisors, see Role-Based Access Control for Advisors.