Frontline Advisor Administration User's Guide

FA Administration Overview

12/17/2025

Contents

FA Administration Overview

If you are new to administration for Genesys Frontline Advisor (FA), read the information on this page first to understand what is available in the Frontline Advisor section of the administration module, and how configuration of the administrative options affects the FA dashboard.

<tabber>

Overview=

What is the Genesys Advisors Administration Module?

The administration module is separate from the Genesys Frontline Advisor supervisor dashboard, but you use the module to configure benchmarks (thresholds and rules) that improve the effectiveness of the FA dashboard. The thresholds and rules help you and your team to quickly identify issues, which means you can provide coaching to agents where it is most needed. You can define thresholds and rules at the agent and team level.

In earlier releases, the Frontline Advisor administration module was separate from Genesys Contact Center Advisor and Workforce Advisor. All Genesys Advisors components use the same administration module. You configure Contact Center Advisor, Workforce Advisor, and Frontline Advisor using one centralized module.

What Languages are Supported in the Administration Module?

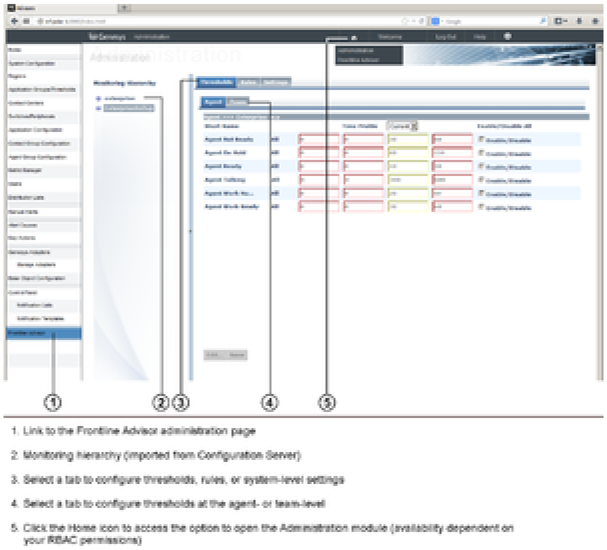
The administration module is available in English only.

Where is the Administration Module?

The administration module is a component of Advisors. On the Frontline Advisor supervisor dashboard, click the icon to open the list of modules available to you; if you have permissions to view the administration module, the option is available in the list.

Display of the administration module is controlled by permissions and privileges, based on roles (role-based access control). The definition of roles, and the permissions associated with each, can be unique to your enterprise. In summary, to view the administration module options for Frontline Advisor, the following must be true:

- You have privileges to access the Advisors administration module.
- You have privileges to access the Frontline Advisor administration page.



Frontline Advisor Administration page

To view FA administrative options, click **Frontline Advisor** in the navigation menu on the left of the administration module.

For additional information about roles, permissions, and privileges, see FA Access Privileges.

The Figure, "Frontline Advisor Administration page", shows the administration module. The FA administration section is selected and visible. Click the image to enlarge it.

Who uses the administration module?

Supervisors and managers typically use the FA page of the administration module. System administrators can also use the administration area for FA to configure system-level values such as time profiles and the frequency at which the system is to update the groups' or agents' data.

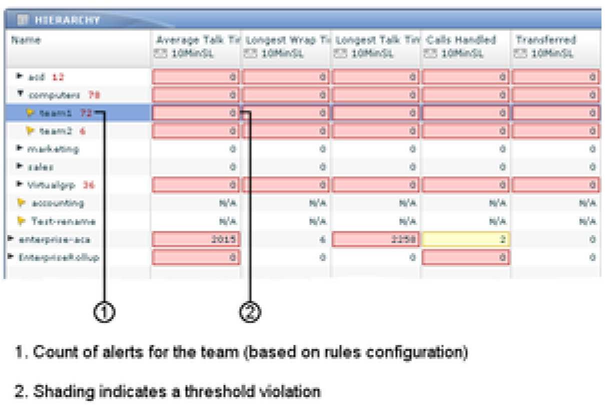
Why use the FA administration page?

The FA administration page is used primarily to enter threshold and rule values. Administrators or supervisors choose what rules and thresholds apply to each agent, team, or group (also called nodes) in the monitoring hierarchy, and enable or disable the threshold or rules for each. Based on the configured rules and thresholds, appropriate alerts display on the Frontline Advisor dashboard.

Thresholds and rules continuously evaluate metrics, issue alerts, and help to focus the attention of supervisors on the most important issues affecting their agents' performance and behavior. Each threshold checks one measured value at a point in time and triggers when the value falls within a preset range. Rules add another layer of sophistication by calling trigger functions that do more than simple range checking at points in time. Rules can count events throughout an interval of time, which allows them to trigger on the frequency of events.

When a threshold is exceeded, the triggered threshold changes the color of the appropriate table cell on the dashboard. When a rule is triggered, the rule creates an alert and posts it to the FA dashboard. The status is visually represented: red indicates an active rule alert.

Threshold violations are visible at all levels of the hierarchy, not just at the agent levels. The actual violation at the agent level is highlighted in a solid color, and the rolled-up violation at the group level is highlighted in a shaded color. Rule alerts roll up through all levels of the hierarchy; the value that rolls up is the count of active alerts.



Alerts and Violations on the FA Dashboard

Active alerts are those alerts for which the agent is still in violation of the rule. Inactive alerts are those alerts for which the agent has corrected his or her behavior and is not in violation of the rule any more. Inactive alerts are cleared when the agent keeps his behavior corrected and does not violate the rule for a time governed by the rule’s time period. This visibility provides a view for managers, directors, and vice presidents of the overall performance.

The Figure, "Alerts and Violations on the FA Dashboard", shows the alerts and thresholds in the Hierarchy pane of the FA dashboard.

When do I use the administration module?

System administrators use the FA administration page to perform initial FA system-level configuration such as specifying general settings for the FA dashboard.

If you use thresholds and rules effectively in your enterprise, then supervisors continue to use the administration module for FA on a regular and ongoing basis. For information about how to use thresholds and rules effectively, see the following:

- FA Thresholds and Rules Overview
- Working with FA Metrics Thresholds
- Working with FA Rules

How do I make best use of the administration module for FA?

The following topics provide information about using the monitoring hierarchy and give examples of defining thresholds and rules:

- FA Monitoring Hierarchy
- Working with FA Metrics Thresholds
- Working with FA Rules

It is important to keep rules and thresholds focused on specific goals and aimed at highlighting significant situations. Too many configured rules or thresholds can be difficult to manage and can create too much information – in the form of alerts – to monitor on the dashboard. Ideally, the number of alerts should be low: one or two for each agent each day would lead to very effective coaching. For example, use rules to monitor only one or two types of situations a week. The rules can be changed to tighten the triggering numbers in a future week (to "raise the bar"). Tailoring a Coaching Strategy provides an example of using thresholds and rules to create successful coaching strategies.

|-| Preparing the dashboard for use=

The first step in preparing Genesys Frontline Advisor (FA) for use is to create the monitoring hierarchy and import it to FA. The process is described in FA Monitoring Hierarchy.

After you have imported the hierarchy, there are general settings you configure on the **Settings** tab of the FA administration page. You can change the values on the **Settings** tab at any time after the hierarchy is imported. If you are an administrator in your enterprise, you will typically configure the dashboard settings before supervisors or managers log in and use FA.

The following procedures provide additional information about the FA dashboard settings.

Procedure: Defining Refresh Rates for your FA Dashboard

Purpose: You can change the rate at which data is refreshed on your FA dashboard. The **Agent State Interval** specifies how frequently state metrics are rolled up. The agent state interval is typically configured to 10 seconds (the default value).

The **Agent Performance Interval** controls how frequently performance metrics are rolled up and rule violations checked. The data handling is done within FA processes (that is, there is no database interaction).

Important

NEW Genesys recommends changing the **Agent Performance Interval** to 300 seconds for best performance.

Prerequisites

- You require access permissions to the **Settings** tab (a system administrator configures permissions). The tab is unavailable if you do not have permissions to view it.

Steps

1. To change the settings, click the `Edit` button, and then type values in the text boxes.
2. Click Save or, to discard changes and revert to the last saved values, click `Cancel`.

Procedure: Configuring Time Profiles

Purpose: You can specify up to three system-wide time profiles for performance metrics, each with its own definable name, interval (minutes), and type (either Sliding or Growing).

Genesys recommends that the time profile values be divisible by either 60 minutes or 10 minutes, otherwise the last interval is cut short when the midnight reset occurs.

The time profile name defined here is the name that displays in the FA dashboard. The time profile name must not exceed 18 characters.

When changes are made to the time profile setting, the changes are made on the configured Advisors Genesys Adapters or Advisors Cisco Adapters, whichever you use. If you cannot save your changes, check the adapter deployments for any potential issues. If the configured adapters are not live, or if there is some other issue on the adapters blocking the change in time profile, the changes to the time profile setting cannot be saved.

You do not need to request information for all metrics for all time profiles. You can enable only those metrics for which you require data and, for each enabled metric, you can enable and disable time profiles so you are collecting data only for relevant time profiles for each metric. Careful configuration at this level can improve your FA performance. See Report Metrics for details about the `Time Profile` options available with the **Report Metrics** page in the administration module.

Prerequisites

- You require access permissions to the **Settings** tab (a system administrator configures permissions). The tab is unavailable if you do not have permissions to view it.

Steps

1. To change the settings, click the `Edit` button, and then type values in the text boxes.
2. Click Save or, to discard changes and revert to the last saved values, click `Cancel`.
   When you change the time profile setting, the system propagates the changes to the configured Advisors Genesys Adapters. If a change to the time profile setting fails to save, check the adapter deployments for issues; a problem with the adapters can block the change in time profile.

Procedure: Enabling and Disabling the Time in Reason Code Information

Purpose: You can show or hide the *time in reason code* information associated with the Reason Code metric on the FA dashboard. If you make changes to the setting, you must restart the FA presentation instance(s) on which you want the changes to take effect. Changes take effect only after a restart.

Steps

1. To show agent time spent in the `Reason Code` state, select the `Show Time in Reason Code` checkbox. The default setting for the `Show Time in Reason Code` checkbox is enabled: the time in reason code information displays on the dashboard until the checkbox is cleared.
2. To hide agent time spent in the `Reason Code` state, clear the checkmark from the `Show Time in Reason Code` checkbox. The Reason Code state metric displays on the dashboard, but does not include information about how long agents spend in a reason code state.