



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Frontline Advisor Administration User's Guide

Pulse Advisors 8.1.5

12/31/2021

Table of Contents

Frontline Advisor Administration User's Guide	3
Frontline Advisor Administration Basics	4
Preparing the dashboard for use	9
The FA Monitoring Hierarchy	11
Control Access to Information	18
Privileges	24
Additional Resources	26
FA Thresholds and Rules Basics	27
Metrics Thresholds	33
Working with Metric Thresholds	36
Monitor Agent Statistics	39
Working with Rules	42
Tailoring a Coaching Strategy	45

Frontline Advisor Administration User's Guide

The *Frontline Advisor Administration User's Guide* provides information to help you understand and use the Frontline Advisor administration page.

Frontline Advisor improves both agent performance and customer satisfaction by giving agents a real-time view of their activity. Customizable alerts draw immediate attention to performance-related activity, good, or otherwise. The real-time data enables agents to correct problems and reinforce progress as it happens, not after the break or during the next shift. Frontline Advisor puts everything agents need to pay attention to in a single location, so they can capture the priority issues and quickly direct their attention to areas that may require attention. Current status, performance, behavioral- or activity-based data can be presented in customized views. Sophisticated, configurable business rules monitor key performance indicators and call attention to situations requiring immediate attention. The alert activity in Frontline Advisor makes agent activity trends more obvious. Frontline Advisor is designed to help agents raise their performance, allowing them to instantly identify activities that need correction or additional training, as well as areas where agents are performing optimally.

Use the links on the left side of the page to navigate to topics.

Frontline Advisor Administration Basics

If you are new to administration for 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.

What is the Administration Module?

The administration module is separate from the FA 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 module was a standalone module dedicated to Frontline Advisor – there was a separate administration module for Contact Center Advisor and Workforce Advisor.

In release 8.1.5 and later, Performance Management Advisors has one administration module. You configure Contact Center Advisor, Workforce Advisor, and Frontline Advisor from one centralized module.

Where is the Administration Module?

The administration module is a component of Advisors, and displays as a tab in the Advisors browser, if you use any or all of the following:

- Frontline Advisor
- Contact Center Advisor
- Workforce Advisor

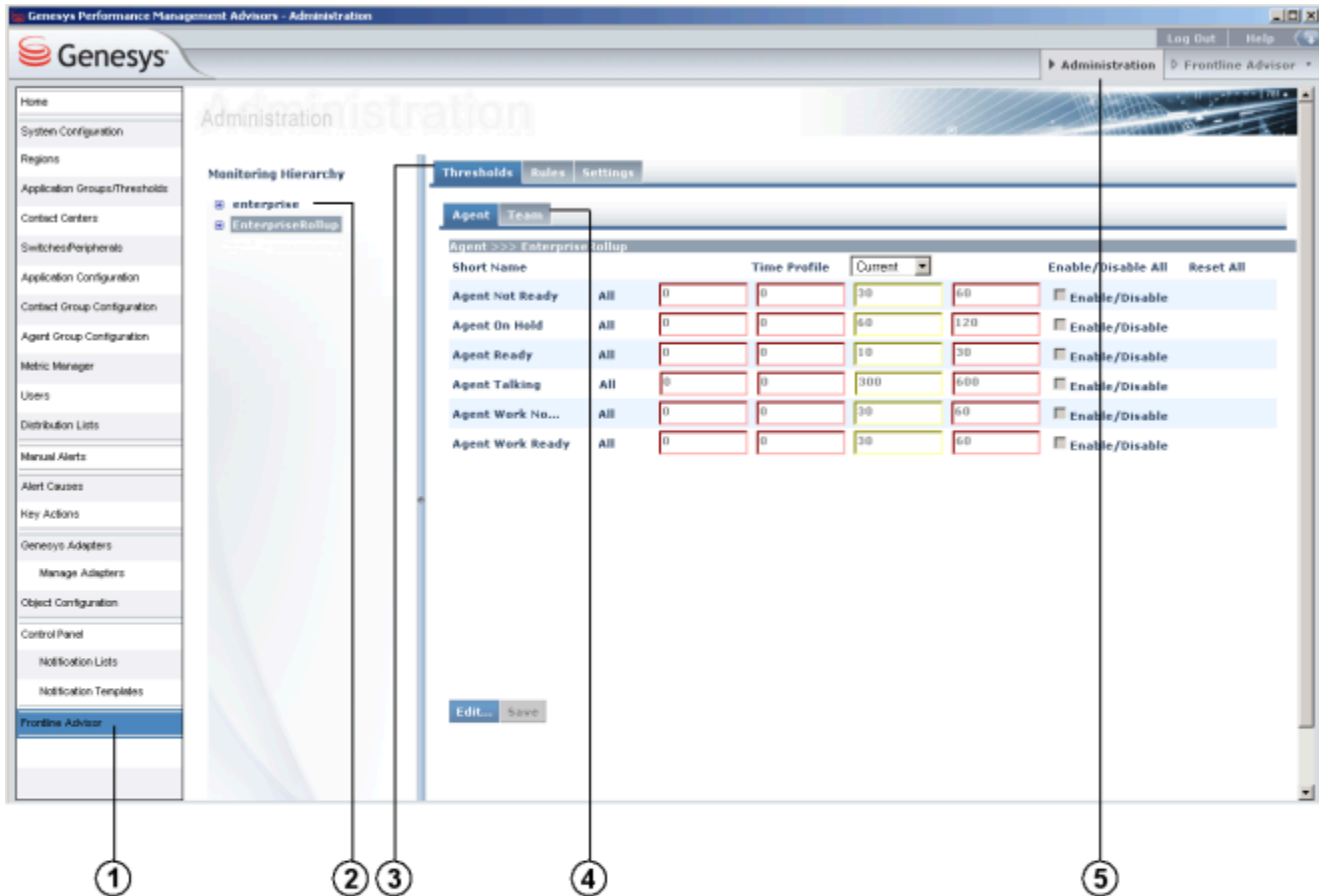
To view FA administrative options, click Frontline Advisor from the navigation menu on the left of the administration module.

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 for Frontline Advisor in release 8.1.5, the following must be true:

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

For additional information about roles, permissions, and privileges, see [Controlling Access to](#)

Information. The following screenshot shows the administration module within the Advisors browser. The FA administration section is selected and visible. Click the image to enlarge it.



1. Link to the Frontline Advisor administration page
2. Monitoring hierarchy (imported from Configuration Server)
3. Select a tab to configure thresholds, rules, or system-level settings
4. Select a tab to configure thresholds at the agent- or team-level
5. Administration module for Frontline Advisor, Contact Center Advisor, and Workforce Advisor

Frontline Advisor Administration page

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 in the Frontline Advisor and Agent Advisor dashboards.

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 pre-set 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.

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 of the overall performance for managers, directors, and vice presidents.

The following screenshot shows the alerts and thresholds in the Hierarchy pane of the FA dashboard.

HIERARCHY					
Name	Average Talk Tir ☎ 10MinSL	Longest Wrap Ti ☎ 10MinSL	Longest Talk Tir ☎ 10MinSL	Calls Handled ☎ 10MinSL	Transferred ☎ 10MinSL
▶ acd 12	0	0	0	0	0
▼ computers 78	0	0	0	0	0
▶ team1 72	0	0	0	0	0
▶ team2 6	0	0	0	0	0
▶ marketing	0	0	0	0	0
▶ sales	0	0	0	0	0
▶ Virtualgrp 36	0	0	0	0	0
▶ accounting	N/A	N/A	N/A	N/A	N/A
▶ Test-rename	N/A	N/A	N/A	N/A	N/A
▶ enterprise-aca	2015	6	2258	2	0
▶ EnterpriseRollup	0	0	0	0	0

①
②

1. Count of alerts for the team (based on rules configuration)

2. Shading indicates a threshold violation

Alerts and Violations on 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 Basics](#)
- [Metrics Thresholds](#)
- [Monitor Agent Statistics](#)

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:

- [The FA Monitoring Hierarchy](#)
- [Metrics Thresholds](#)
- [Monitor Agent Statistics](#)

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 Frontline Advisor (FA) for use is to create the monitoring hierarchy and import it to FA. The process is described in [The FA Monitoring Hierarchy](#).

After you have imported the hierarchy, there are general settings you can 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

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 performance interval is typically configured to 10 minutes (the default value). The data handling is done within FA processes (that is, there is no database interaction).

Prerequisites

- Select a hierarchy node to display data in the tab.
- 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.

Start of Procedure

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

End of Procedure

Procedure: Configuring Time Profiles

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 Genesys Adapters. 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.

Prerequisites

- Select a hierarchy node to display data in the tab.
- 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.

Start of Procedure

1. To change the settings, 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.

End of Procedure

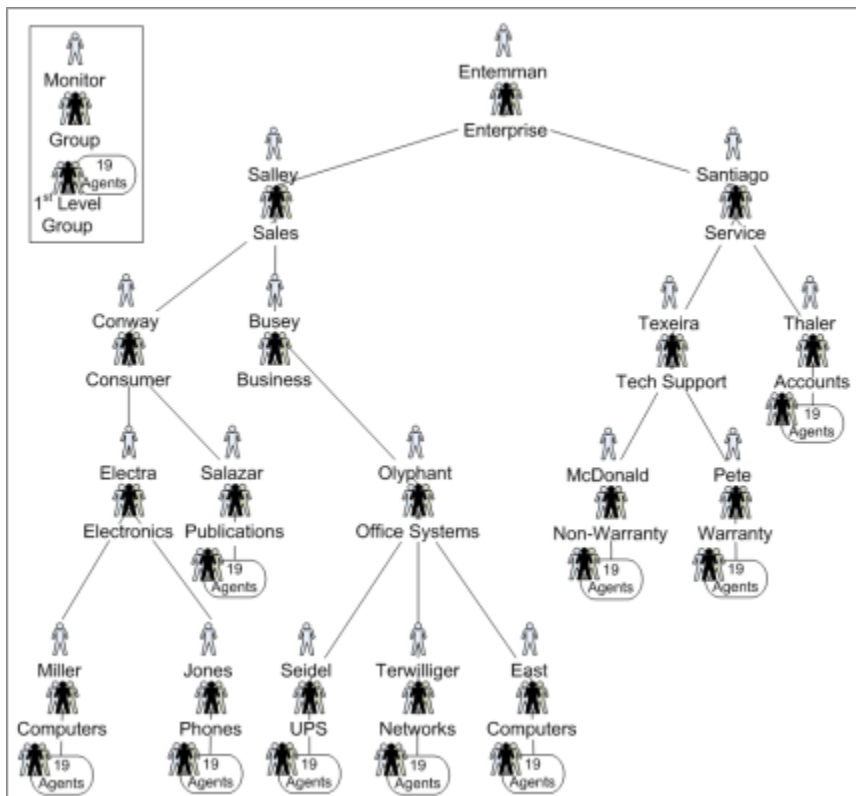
The FA Monitoring Hierarchy

The monitoring hierarchy is a representation of your enterprise and the members of that enterprise who participate in customer interactions. The hierarchy tracks groups of people. The monitoring hierarchy is the foundation of everything you do in Frontline Advisor; supervisors and other managers use the hierarchy to track and manage performance levels.

Defining a Monitoring Hierarchy

A sample monitoring hierarchy is used here to explain how to define the data representing a hierarchy. When you define your monitoring hierarchy, use this example to guide you.

The monitoring hierarchy defines how agents are grouped, how groups are grouped, and so on, until there is just one all-encompassing group at the top. The following graphic shows a sample monitoring hierarchy. Click on the image to enlarge it.



Genesys recommends that you produce a similar graphic of your hierarchy. Some hierarchies may be so large that this is not possible, but you should do it if you can. A graphic allows you to see the groups and monitors, as well as to annotate the nodes with database IDs and other details that make working with your hierarchy simpler and less prone to error.

Reading the Sample Hierarchy

The sample monitoring hierarchy has nine first-level groups, each with nineteen agents. It is common in contact centers to refer to the first-level groups as groups or nodes. On the dashboard, they are called teams.

The nine first-level groups in the sample hierarchy are:

- Computers
- Phones
- UPS
- Networks
- Computers
- Publications/Office Systems
- Non-Warranty
- Warranty
- Accounts

Note that groups are allowed to have the same name (for example, two groups named Computers), provided that they do not share the same parent.

These nine groups appear at various levels in the hierarchy. This is an important concept: groups do not all have to be at the same level of the hierarchy. For instance, the Phones group is two levels below the Accounts group.

The sample monitoring hierarchy has more groups above the first-level groups. Computers and Phones are in the Electronics group. UPS, Networks, and the second Computers group are in the Office Systems group. Groups within groups continue up the hierarchy (also called a tree), until the root node. The root node of the sample monitoring hierarchy is the Enterprise group.

The hierarchy also defines the monitors. A monitor is a person who has access to – and can monitor – a specific group in the hierarchy. For simplicity, the sample monitoring hierarchy defines only one monitor for each group. The person named Entemman monitors the Enterprise group, the person named Salley monitors the Sales group, the person named Electra monitors the Electronics group, and so on throughout the tree, with one person monitor for each group. Note that the person with the last name Conway is a monitor of the Consumer node. This implies that Conway can monitor all of the groups in the Consumer subtree, as well, which consist of the 19 agents on the Computers group, the 19 agents on the Phones group, and the 19 agents on the Publications group.

Once you understand the monitoring hierarchy in your enterprise, you must configure it in Genesys Configuration Manager for use in Frontline Advisor.

Where is the Hierarchy Stored?

Monitoring hierarchies are created and maintained in the Genesys Configuration Server by administrators with the required roles and permissions.

If you are a new Genesys customer, then hierarchies can be imported directly from a third-party system or HR system by Genesys Professional Services consultants as part of an initial deployment, and then maintained in the Genesys environment.

Who Configures the Hierarchy in Genesys Configuration Manager?

An administrator in your enterprise can configure which location or folder in the Configuration Server houses the hierarchy, and multiple folders can be chosen if the hierarchy is spread over many different folders or tenants.

When is the Hierarchy Configured?

An administrator must configure the hierarchy before FA is launched and used by managers in your enterprise. The hierarchy is the foundation of Frontline Advisor.

How do Folders in Configuration Manager become the FA Hierarchy?

During installation, you specify the root for the FA hierarchy. Hierarchy root nodes are specified by providing a tenant name and a path to the folder that is the root. This folder can be under the Agent Groups configuration unit or Persons configuration unit in Config Server

This means that the hierarchy views that are specific to a supervisor can be created; the supervisor can see only their own team's hierarchy. This also provides the opportunity to enforce uniqueness of names at the level of sibling hierarchy nodes. This in turn means that it is possible to have nodes with the same name (for example, Sales) provided they do not have the same parent.

It is possible to have multiple root nodes in the hierarchy, which can come from different tenants. A root level node is no longer automatically called Enterprise. Your enterprise can call them anything that is permitted in the Configuration Manager.

Folders and agent groups in the Genesys Configuration Server translate to groups in the FA hierarchy. Folders and agent groups created in the Configuration Server have a tree structure in which a folder can have multiple sub-folders or agent groups.

The agent groups contain agents. The agents present in agent groups in Configuration Server represent agents in the FA hierarchy. Groups and agents replace the terms supervisors, teams, and agents from previous releases.

An agent can be a member of more than one group if the hierarchy is imported from Configuration Server.

When the FA service is started, or when reload the hierarchy, the monitoring hierarchy defined in

Genesys Configuration Manager is loaded, incorporating any changes made to the hierarchy since the previous load. If multiple folders in Configuration Manager comprise the FA hierarchy, then FA creates a consolidated view of the hierarchy with a virtual enterprise node linking all the various hierarchies together.

The hierarchy is also loaded daily at 02:55 a.m., or whenever you click the Hierarchy Reload button on the Settings tab of the FA administration page. Changes made in the hierarchy using Configuration Manager are reflected in FA only when the hierarchy is reloaded at startup, at the daily refresh, or when you click the Hierarchy Reload button.

Access permissions are configured at each node of the hierarchy according to user roles defined by administrators in the Genesys Configuration Manager. These roles determine to which nodes of the hierarchy each manager has access. Supervisors and other managers no longer have automatic access to all child nodes of parent nodes to which they have access.

Supervisors can override rules and thresholds only for nodes to which they have "change" access in Configuration Manager. When a user logs in, a customized view of the hierarchy is created. This view contains only groups and agents to which the supervisor has "Read" access in Configuration Server. Managers may also be able to see nodes and their aggregations that are above those of their team(s), but require specific "change" access to those higher-level nodes before they can edit them.

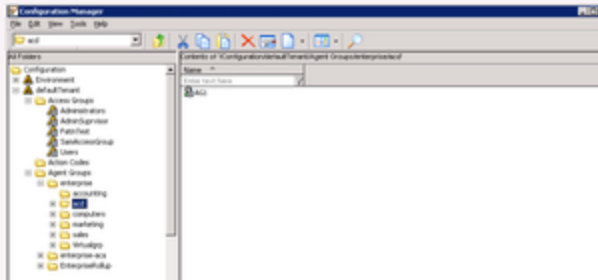
Example

The following hierarchy is used in this example to show how a graphical representation of an enterprise is used to create the monitoring hierarchy in Frontline Advisor. Note that "My Enterprise" is not in the Configuration Server. It is a virtual, unnamed root node inserted by FA. It is not visible on the dashboard by any user.



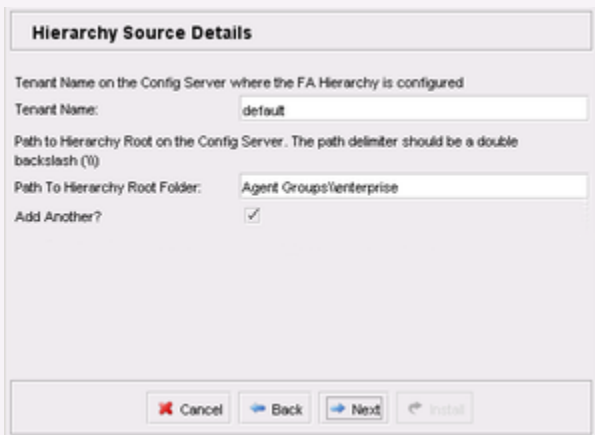
Creating a graphical representation of your enterprise

The following screenshot shows the folder structure that the system administrator configured in Configuration Manager.



The hierarchy in Genesys Configuration Manager

The person in your enterprise who installs Frontline Advisor specifies the Enterprise and Enterprise Rollup folders as hierarchy root folders when deploying Frontline Advisor. The following screenshot shows the relevant installation screen.



Specifying folders for the hierarchy during installation

The administrator grants permissions (in Genesys Configuration Manager) to a supervisor to view the groups and agents in those folders.

When the supervisor launches the FA dashboard for the first time, FA retrieves the Enterprise and EnterpriseRollup folders and subfolders from the Configuration Server. The following screenshot shows the hierarchy on the FA dashboard.

Name	Hold	Logged On	Not Ready
enterprise 62	0	12	2
acd 10	0	2	0
computers 62	0	12	2
team1 57	0	11	2
team2 5	0	1	0
marketing	0	0	0
sales	0	0	0
Virtualgrp 31	0	6	1
accounting	-	-	-
EnterpriseRollup	0	2	1

The hierarchy imported to Frontline Advisor

The following screenshot shows the hierarchy as it displays on the FA administration page.



The imported hierarchy on the FA administration page

Important

For a pure Cisco environment, the hierarchy should be configured in the Configuration Server as it is done for a Genesys or mixed environment. However, Cisco Adapter requires FA to send the Cisco AgentSkillID property to identify the agent while registering and issuing statistics. To accommodate this, the AgentSkillID must be added as an Annex property in the Advisors section of each agent in the hierarchy.

The ExternalId.CISCO attribute must be set in the agent's Annex tab under the Advisors section, and the value of the ExternalId.CISCO will be the AgentSkillID for the agent in the Cisco environment.

The hierarchy extractor will first try to extract the skill ID from the Annex section for a Cisco configuration. If the ExternalID property is undefined in the Annex section, then it will extract the EmployeeID for the Genesys configuration.

Control Access to Information

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:

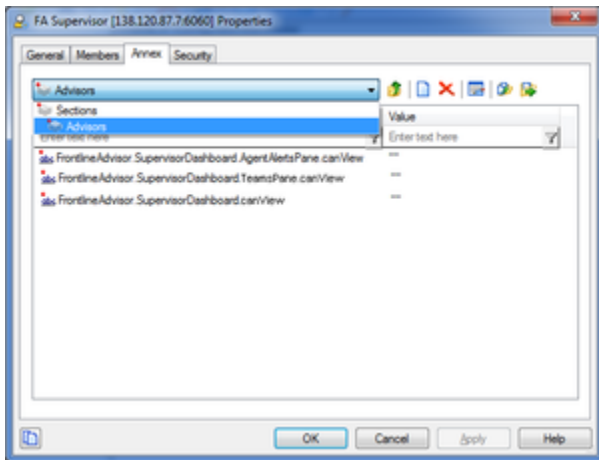
```
[application name].[module name].[task grouping].[privilege name]
```

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:

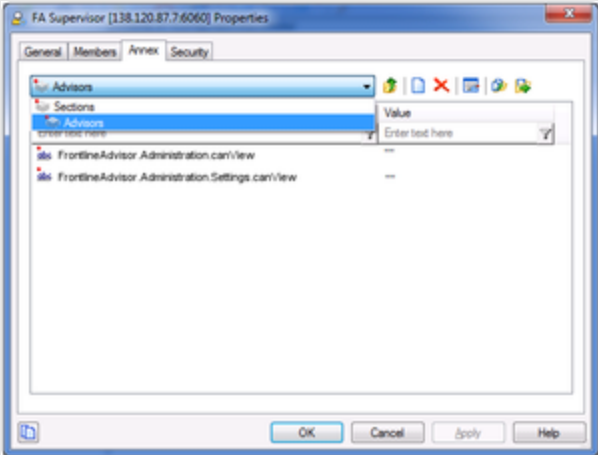


Annex tab for FA Supervisor role in Configuration Manager

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

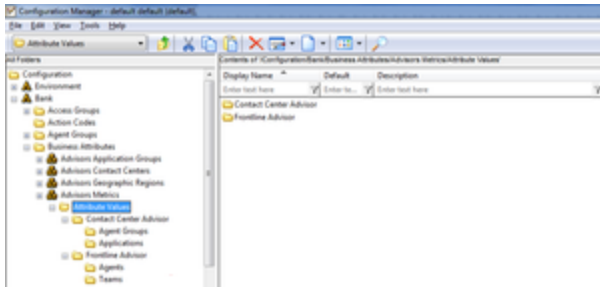
If you want the user to see the Settings tab, you must ensure you also assign the privilege that allows the user to access the Administration module. The user's role does not include the privilege to reload the hierarchy - the Hierarchy Reload section of the Settings tab does not display for the FA Supervisor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

Privileges

In Frontline Advisor (FA), you can use Role-Based Access Control (RBAC) to control users' access to tabs on the FA administration page, or to portions of tabs, or to the entire FA dashboard. The following Table lists the privileges available in Configuration Manager for Performance Management Advisors 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
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 and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges)	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
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 Admin 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. (This requires the Settings tab to be accessible via the FrontlineAdvisor.Administration.Settings.canView privilege)	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.

Additional Resources

The Performance Management Advisors 8.1 Contact Center Advisor/Workforce Advisor Administrator User's Guide contains additional information about roles, permissions, and privileges as they apply to Advisors.

Additional sources of information on role-based access 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](#)

FA Thresholds and Rules Basics

You use Frontline Advisor rules and thresholds to manage the performance levels in your enterprise. 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”).

At the top-level nodes of the hierarchy, the threshold or rule can be enabled or disabled. By default the top-level thresholds and rules are disabled. If a threshold or rule is disabled at a group level, then it is disabled for all agents of that group. The nodes underneath inherit from the closest enabled ancestor – that is, a node on the same branch, but closer to the root, or top-level, node.

If a threshold or rule is disabled at an agent level, then it is disabled for only that agent. Since there are no nodes under an agent, it affects only that agent. If a threshold or rule is overridden at an agent level, then its state applies only for that agent.

The state of a threshold or rule may be overridden at any level of the hierarchy. For example, if a threshold is enabled at the agent group level, then all agents in that group for which there are no overrides will have that threshold enabled.

With the implementation of role-based access control, managers can only enable, disable, and override thresholds and rules to which they have been granted specific change access by administrators in the Genesys Configuration Manager.

The following sections describe helpful general features of Performance Management Advisors and FA administration that help you when navigating throughout Advisors browser and the FA administration page:

- [Persistent Settings](#)
- [ToolTips](#)

The following sections describe how to work with thresholds and rules:

- [Navigating the Monitoring Hierarchy](#)
- [Understanding Inheritance in the Hierarchy](#)
- [Metrics Thresholds](#)
- [Monitor Agent Statistics](#)

Persistent Settings

When logging in to or out of any machine, or switching between tabs in the Performance Management Advisors browser, the Advisors browser retains the following settings:

- Monitoring hierarchy expansions
- Selected level in the monitoring hierarchy
- Last selected tab (module)
For example, if you were viewing the FA dashboard when you logged out, the FA dashboard displays when you next log in to the Advisors browser.

ToolTips

ToolTips can help you by providing definitions for metrics, explanations of buttons and icons, and describing impacts of your actions (for example, if you override a threshold value). To display a ToolTip for an action, move your mouse cursor over the icon or button. To see which values on the Threshold and Rules tabs are inherited or overridden, and where those values come from, place your mouse cursor over the values. This helps when navigating through the monitoring hierarchy and viewing or modifying values.

When you move your mouse cursor over a threshold or rule value, a tooltip displays one of the following types:

- Types 1 and 2—The value uses the global default because it does not inherit from any override.
- Type 3—The value is inherited from a node other than the root node (threshold or rule). Two pieces of information display:
 - The value is inherited
 - The node from which the inherited value originates
- Type 4—The value overrides an inherited value (threshold or rule). Three pieces of information display:
 - The value is an override value
 - The node whose value is being overridden
 - The inherited value that is being overridden

Type 1

Monitoring Hierarchy

- [-] Enterprise
 - [-] K. Entemman
 - [-] K. Salley
 - [-] J. Conway
 - + C. Salazar
 - [-] K. Electra

Thresholds Rules Settings

Agent >>> K. Salley

Short Name	Time Profile	Current
AAHT	120	240
AATT	110	230
AAWT	5	10

Type 1

This ToolTip displays if you move your mouse cursor over the threshold value of 540, inherited from the root node.

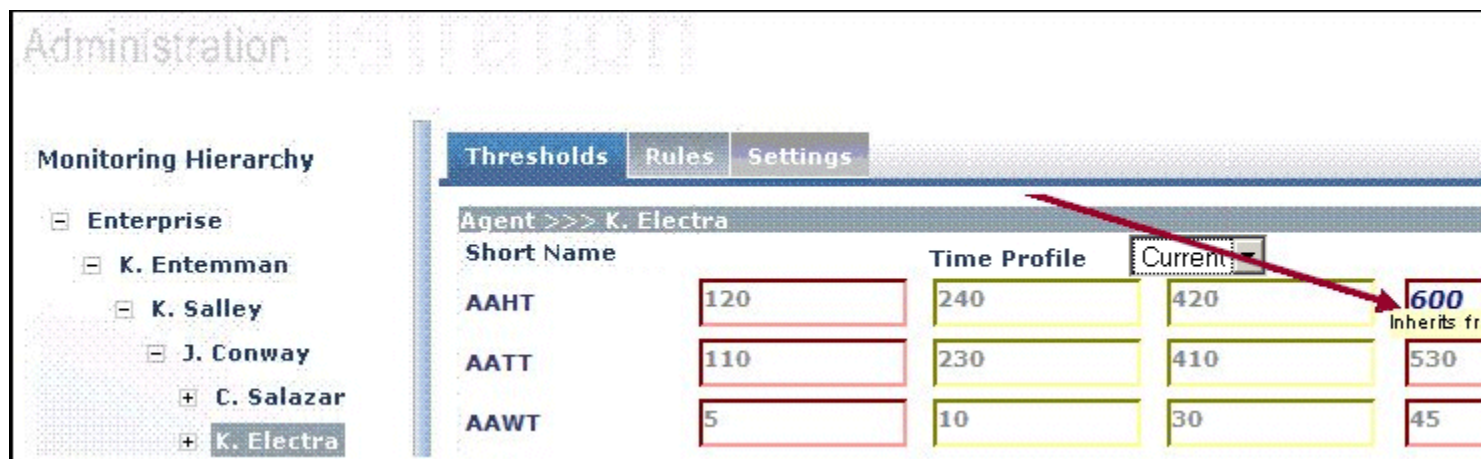
Type 2



Type 2

This ToolTip displays if you move your mouse cursor over the inherited rule value of 300, inherited from the root node.

Type 3



Type 3

This ToolTip shows that the Electra/Electronics node inherits its value of 600 from the override value stored at the Conway node.

Type 4



Type 4

This ToolTip shows that the Conway node overrides the value of 540 that would otherwise be inherited from the Enterprise node.

Navigating the Monitoring Hierarchy

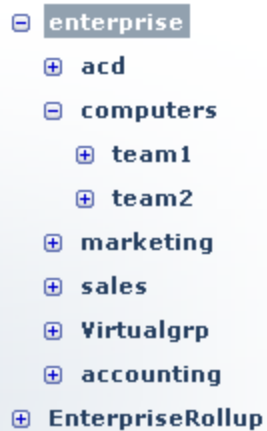
The monitoring hierarchy navigator is used to navigate to the area where thresholds and rules can be viewed or modified. The monitoring hierarchy navigator lists a hierarchy of the agents and agent groups imported from the Genesys Configuration Server. Changes made to the hierarchy in Configuration Server display in the monitoring hierarchy navigator only after Frontline Advisor imports the data. Frontline Advisor imports data from the Genesys Configuration Server at startup, once every day, and when you click the Hierarchy Reload button. The Hierarchy Reload button is available to you if your role includes privileges to view the Hierarchy Reload section of the Setting tab on the FA administration page.

Warning! Reloading the hierarchy can take up to an hour. Frontline Advisor is unavailable during the reload period.

Once your monitoring hierarchy is defined and imported, administrators control your access to Frontline Advisor and Agent Advisor users in the Genesys Configuration Server. You can expand your view of the hierarchy from groups down to agents using the Expand (+) button (subject to your access permissions), and limit the number of levels you are viewing using the Collapse (-) button. The following screenshot shows an example of the monitoring hierarchy navigator.

Administration

Monitoring Hierarchy



Monitoring hierarchy navigator

Understanding Inheritance in the Hierarchy

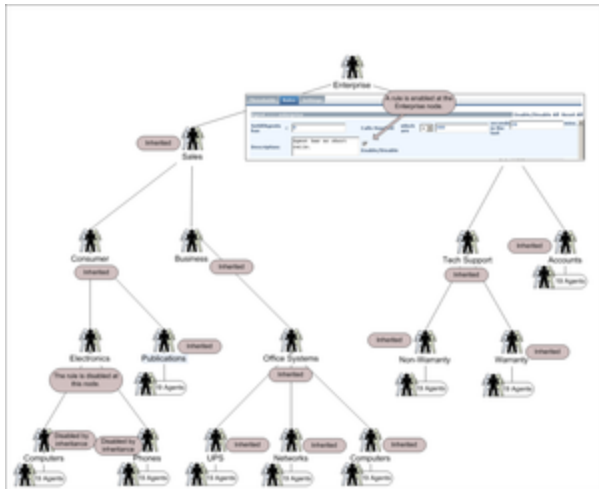
Inheritance is the mechanism by which values higher in the tree are passed down to lower levels of the tree.

The behavior of a rule or threshold at a node is defined by the nearest ancestor node (including the node itself) where an override is defined. If there are no ancestors with overrides, the behavior is inherited from the top-level ancestor node(s). An override propagates down the hierarchy tree, until another override occurs, with all descendant nodes using the values defined at the override.

Disabling a threshold or rule causes it to be disabled at all inheriting nodes (unless re-enabled at some lower-level node).

The agent's and group's values determine the status and trigger the violations for thresholds. The agent's values determine the status and trigger the alerts for rules.

The following illustration shows an example of inheritance, and an override, within the hierarchy. Click the image to enlarge it.



Example of inheritance

Metrics Thresholds

The Thresholds tab allows you to define the critical and acceptable conditions for the metrics to which you have been granted role-based access.

The standard Frontline Advisor installation provides the monitoring hierarchy with default values for all agent and group thresholds; however, you should review and change the values to meet the goals of your enterprise. Thresholds are disabled by default until enabled by an override.

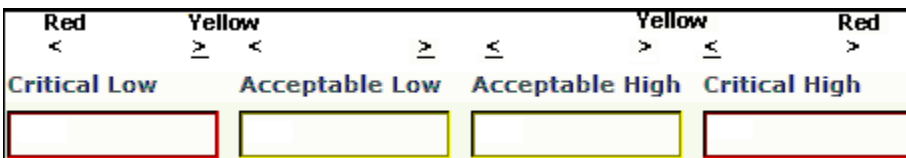
You must select a hierarchy node in the monitoring hierarchy navigator to display data in the Thresholds tab. The following screenshot shows an example of the Thresholds tab with the Team tab selected.



Thresholds tab with Team metrics displayed

Threshold Types

You can configure four types of thresholds. Depending on the metric, a value may be acceptable above or below a certain value. When thresholds are triggered, they highlight cells in Frontline Advisor or Agent Advisor. The four text boxes on the Thresholds tab are colored to provide a visual cue for the status.



Threshold ranges

The red text boxes are mandatory, while the yellow text box is optional (and may be replaced by a red text box). The text box colors change depending on the values you type. Enabled thresholds trigger a violation on the dashboard if a value is above or below defined values.

Red indicates a critical value range. Yellow indicates a warning value range. The following table describes how threshold alerts occur.

If value is ...	Value 1 ...	And ...	Value 2 ...	Result
greater than	the value in the 4th text box			then the value is critical high (red)
greater than	the value in the 3rd text box	and less than or equal to	the value in the 4th text box	then the value is warning high (yellow)
greater than or equal to	the value in the 2nd text box	and less than or equal to	the value in the 3rd text box	then the value is acceptable (no color is displayed)
greater than or equal to	the value in the 1st text box	and less than	the value in the 2nd text box	then the value is warning low (yellow)
Less than	the value in the 1st text box			then the value is critical low (red)

Example

For the purposes of these examples, the system setting for how often the metrics are calculated (that is, the performance calculation interval) is 10 minutes.

Example 1

For an average of three-minute calls, handling two or more calls but less than or equal to five calls is acceptable. Handling one call is yellow. Handling less than one call is red. Handling more than five calls but less than or equal to eight calls (that is, the calls are too short) is yellow. And handling more than eight calls (that is, short-calling) is red. The following screenshot shows how to configure this scenario on the Thresholds tab.

Example 1

Example 2

In this example, handling two or more calls but less than or equal to five calls is acceptable. Handling one call triggers a warning (yellow). Handling less than one call or more than five calls is a critical (red) violation.

Example 2

Example 3

In this example, handling one or more calls but less than or equal to five calls is acceptable. Handling more than five calls but less than or equal to eight calls triggers a warning (yellow). Handling less than one call or more than eight calls is a critical (red) violation.

NCH	1	1	5	8
-----	---	---	---	---

Example 3

Working with Metric Thresholds

Because an agent can belong to multiple agent groups, it is possible in Frontline Advisor (FA) to define a threshold in different ways, and according to different overrides, at groups of which the agent is a member. In this case, the threshold violation level can display differently, depending on the path you use to navigate to the agent in the FA dashboard. For example, the AHT metric may have a red alert when the agent is viewed as a member of the Sales group, but only yellow when the agent is viewed as a member of the Services group. Rules can also have different definitions for the same agent based on the path chosen through the hierarchy to reach that agent. Only rule violations for the selected path are shown.

Procedure: Viewing Thresholds

Purpose: To view threshold values in a level of the monitoring hierarchy.

Start of procedure

1. Select the Thresholds tab.
The thresholds are displayed based on the last selected level.
2. Select a level in the Monitoring Hierarchy navigator.
The thresholds for the selected level are displayed in the pane on the right, subject to your access permissions. The name of the selected level displays in the title bar.

End of procedure

Procedure: Disable/Override All Thresholds

Purpose: To disable or override all thresholds at the selected node at once (subject to your access permissions).

Start of procedure

1. Select the Thresholds tab.
2. Select a level in the Monitoring Hierarchy navigator.
The thresholds for the selected level are displayed in the pane on the right, subject to your access permissions.
3. Click the Edit button at the bottom of the pane.

4. Select the Enable/Disable All check box.
5. Click Save or Cancel.

End of procedure

Procedure: Defining a threshold

Purpose: To specify values for thresholds. Default values for thresholds are provided on installation; however, you can override them at any level, subject to your access permissions. To distinguish between the default values and overridden values, overridden values display in boldface and are italicized. Inherited values are in regular font. You can display the default value in a ToolTip by moving the cursor over an edited value.

For a group or agent, the state of thresholds at new nodes is inherited from the parent node. This includes whether the threshold is enabled or disabled.

Start of procedure

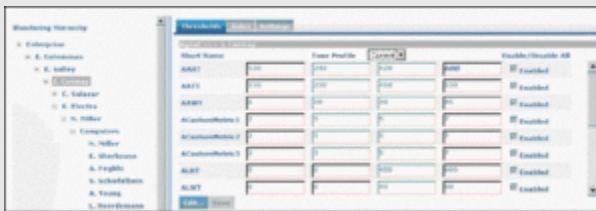
1. Select the Thresholds tab.
The thresholds for the last selected level are displayed.
2. To define thresholds, select a level in the Monitoring Hierarchy navigator.
The thresholds and the title bar for the selected level display.
If you change any text field or check box and then select a new level, all changes for the previous level are discarded.
3. Click Edit.
The fields and Save button enable. The Edit button changes to a Cancel button.
4. Type new values in one or more text boxes.
The values must increment (or remain the same) from left to right. Non-negative integer numbers are allowed. No letters or blank spaces are allowed. If an invalid value is entered, an alert message box displays when the Save button is pressed.
5. To activate the threshold, check the Enabled checkbox.
To deactivate the threshold, clear the Enabled checkbox.
6. (Optional) To reset the threshold attributes to the previously inherited values, click the Reset checkbox that displays next to the threshold row after you override one of the thresholds attributes.
The Reset checkbox disappears after you click Save.
The Reset All link performs the reset operation to all overridden thresholds.

7. Do one of the following to complete the configuration:
 1. To discard any changes made and revert the contents of the Thresholds tab to the last values saved to the database, click Cancel.
 2. To save all of the changes to the thresholds, click Save.
A confirmation message displays. If any errors are detected through validation, an alert message displays.

End of procedure

Example: Defining Thresholds

You want to store an override value of 600 at the node that Conway monitors, that is, the Computers node. To enter an override value, click the Edit button to enter the edit mode. Type a value of 600 for Critical High AHT, and click the Save button. The override value of 600 now displays at the Conway (Computers) node in italic font, and a slightly larger font than the other (inherited) values.



Configuring a threshold value

From now on, if nothing else changes, the Conway/Computers node and all nodes in that subtree (which do not have an override value) will inherit a value of 600 for critical high AHT.

Monitor Agent Statistics

The Rules tab on the Frontline Advisor administration page allows you to define the conditions that will continuously monitor the agents' statistics, such as short calling. An alert is issued if the conditions of a rule are met. The Frontline Advisor standard installation provides default values; however, you should review and change them to meet the goals of your enterprise. All rules are disabled by default.

You can modify rules values (subject to your access permissions) at the group level and agent level. To modify values for a higher level in the hierarchy, you must select the level in the hierarchy. An agent rule takes precedence over the group rule. A group rule takes precedence over the top-level rule. Rules evaluate and trigger on agent metrics, but not for group metrics.

Best Practice: Avoiding duplication of alerts triggered by rules

When a rule is set at a high level in the hierarchy, all child agent groups have the same rule, unless the rule is overridden. FA *de-duplicates* (removes duplicates of) the alert counts; if an alert is triggered, it is counted only once for the agent. However, when the rules are set at the agent-group level, there is no way to determine whether rule sets for sibling agent groups are matched. Therefore, the counts have to be totaled individually.

It is possible for rules to differ only slightly between the two such agent groups, yet they must be counted as distinct violations. If an agent violates the rule in both agent groups, he or she has two rule violations, rather than just one. To avoid this scenario, rules should be specified at the highest level possible as a best practice.

If you have access to the Rules tab, but you have only Read access permission, then you cannot modify the rules (the Edit button is disabled). If the Administrator gives you a Change or Full Control permission, the Edit button is enabled and you can modify the rules.

To distinguish between the inherited values and overridden values, overridden values display in boldface and are italicized.

You must select a node in the hierarchy to display data in the Rules tab. The following screenshot shows an example of the Rules tab.



Rules tab

Each rule may include the following:

- Rule descriptor—a fixed text that describes the rule; for example, “Set of agents has”.
- Rule operator—less than (<), greater than (>).
- Rule operator value—only non-negative integers are allowed. No letters or blank spaces are allowed.
- Filter descriptor—fixed text that describes the filter, for example, “Calls handled which are”
- Rule filter operator—less than (<), greater than (>)
- Rule filter value—only non-negative integers are allowed.
- Time Interval—the frequency in which the rule evaluates the metrics. The default value is 20.
- Description—a description of the rule that will display in the Alert Details section when an alert is triggered. The text field allows up to 256 characters.

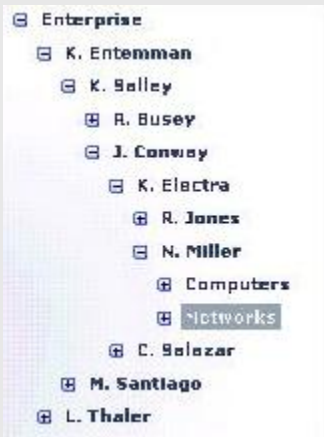
If an invalid value is entered, an alert message box displays when the Save button is pressed.

Resetting Rule Constraint Values

Once a constraint has been overridden, it is possible to “reset” the constraint to the inherited values. This effectively removes the override from the system. At any given node in the hierarchy (apart from the top-level node), the Reset option is available for all constraints that are overridden at that node. Checking this option and clicking Save results in the inherited values for this threshold being used at this node and its descendants (unless overridden elsewhere). Choosing to reset an overridden constraint takes precedence over any edits made to the other fields; these changes are lost when the constraint is reset. A value is reset to the value of the closest ancestor in the tree that has an override or the global default if there are no overrides higher in the tree.

When you make a change to the rules settings, the changes are made on the configured Genesys Adapters. If you cannot save changes to rule settings, 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, it blocks your ability to save changes in rule settings.

Example: Resetting Rule Constraints



Resetting rule constraints

If the thresholds for the AHT metric are overridden at K.Salley, J.Conway, and Networks, resetting the AHT metric at the Networks node would set it to the values specified for the J.Conway node. If the metrics are then reset at the J.Conway node, the threshold values at that node and all its children will be set to what is specified at K.Salley. This functionality works for either overridden constraint values or for the Enable/Disable checkbox.

Working with Rules

Procedure: Viewing rules

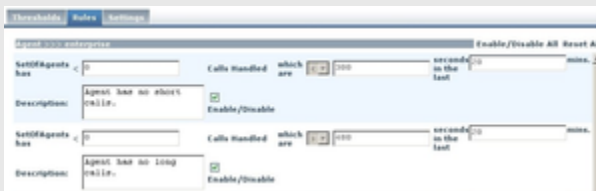
Start of procedure

1. Select the Rules tab on the Frontline Advisor administration page.
The rules are displayed based on the last selected level, and subject to your access permissions.
The edited values display in boldface and italicized.
2. Select a level in the Monitoring Hierarchy navigator.
The rules for the selected level are displayed in the pane on the right. The name of the selected level displays in the title bar.

End of procedure

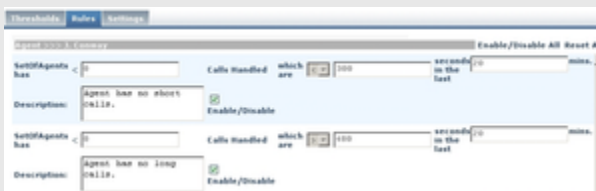
Example: Viewing Rules

The example below illustrates the default settings for rules at the top node (Enterprise in our monitoring hierarchy).



Rule configuration at the Enterprise node

When you navigate to the Conway node in the monitoring hierarchy, you see that the value of 300 for Calls Handled from the Enterprise node is inherited by the Conway node.



Inherited value

Procedure: Enable or Disable All Rules

Start of procedure

1. Select the Rules tab.
2. Select a level in the Monitoring Hierarchy navigator.
The rules for the selected level are displayed in the pane on the right, subject to your access permissions.
3. Click the Enable/Disable All button.

End of procedure

Procedure: Defining a rule

Start of procedure

1. Select the Rules tab.
The rules for the last selected level display.
2. To define rules, select a level in the Monitoring Hierarchy navigator.
The rules and the title bar for the selected level display.
3. Click Edit.
The fields and Save button are enabled. The Edit button changes to a Cancel button.
4. Type a rule operator value.
5. If available, type a rule filter operator value.
6. Enter a time interval in the text box.
If any text field or check box is changed and you select a new level without saving the changes, all changes are lost.
7. Type a comprehensive description of the rule in the Description text box.
A rule description must not exceed 128 characters. If you enter a text description that exceeds 128 characters, Frontline Advisor fails to save the rule.
8. To activate the rule, check the Enabled checkbox or to deactivate the rule, clear the Enabled checkbox.
9. To reset a rule constraint to the inherited values, select the Reset checkbox.
For more information about resetting rule constraints, see [Resetting Rule Constraint Values](#).
10. Do one of the following to complete configuration:

1. To save all of the rules, click Save.
If any errors are detected during validation, an alert message displays.
2. To discard any changes made and revert the contents of the Rules tab to the last values saved to the database, click Cancel.

End of procedure

Example: Defining Rules

Suppose you want to override the inherited Calls Handled value of 300 with an override value of 600 for the Conway node and its subtree. To modify a rule value, first click the Edit button (not displayed in the following screenshot because it is scrolled out of view). Enter the override value and click the Save button. The following screenshot shows what the values now look like.



Editing a Rule

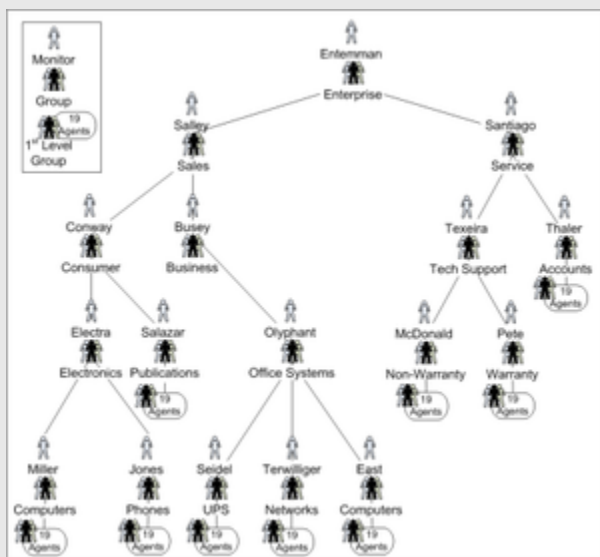
From now on, unless changes are made, the Conway node contains an override value of 600. All nodes in the subtree, if they are enabled and if they do not have their own override value, inherit the value of 600. Overridden rules are not automatically enabled, although in this example you would typically also enable it and change the definition.

Tailoring a Coaching Strategy

Example: Tailoring a Coaching Strategy

You can use the concepts explained in this section to tailor a coaching strategy. A coaching strategy can be modified at any time. In general, coaching strategies do the following:

1. Specify values for rules and thresholds based on types of groups.
2. Specify values for rules and thresholds based on types of agents.
3. Provide a framework over time for continuous improvement.



Hierarchy

Coaching Strategy Step 1

Consider our sample monitoring hierarchy, above, in which the very first level under Enterprise groups the organization into Sales and Service. In a case like this, the coaching strategy configures sales-oriented values at the Sales node and service-oriented values at the Services node. For example, agents who are selling are most likely expected to talk longer than agents who are delivering customer service.

This Step 1 approach continues throughout the monitoring hierarchy, using inheritance when situations are similar, and using overrides when situations are different. For example, under the Sales group are Consumer and Business groups. These two groups are similar in some ways because the

agents are selling, but they are also different because one group sells to consumers and the other group sells to businesses.

Agents in both groups are selling and would probably be expected to perform the same number of holds and transfers. So the two groups would be configured to inherit the hold and transfer thresholds from the Sales node. Wrap time for selling to consumers might take a shorter time than wrap time for businesses because the latter may include checking the balance in the business account. In this case, Consumer would have override values for Wrap Time different from the override values for Wrap Time in the Business group.

This Step 1 approach of specifying values according to similarities and differences of groups continues all the way down the tree to the agents.

Coaching Strategy Step 2

In any given group, some agents will be new and some will be experienced. Step 2 uses inheritance and override values at the agent level to coach differently according to agent type. For example, newer agents might be expected to talk a little longer than experienced agents, until the newer agents learn better call control, company policies, computer applications, and so on. Experienced agents know these things, so good coaching will challenge them with tighter override values to help them continue to improve.

Step 2 uses inheritance and overrides at the per-agent level, enabling coaching by agent type.

Sometimes Step 2 is required at the group level. For example, sometimes a “nest” is used to incubate new agents, while a “tiger team” is used to leverage the expertise of long-time, experienced agents. Step 2 would use inheritance and override at the group level in these cases, where groups are groups of agent types.

Coaching Strategy Step 3

Step 3 involves the improvement over time of Steps 1 and 2. Good coaching helps people get better over time by incremental improvements. In Step 3, coaches tighten or loosen values over time to challenge agents and help them continually improve their performance.