Frontline Advisor Administration User's Guide

Pulse Advisors Current

12/30/2021

Table of Contents

Genesys Frontline Advisor Administration User's Guide

The *Genesys 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 supervisors a real-time view of agent activity. Customizable alerts draw immediate attention to performance-related activity, good, or otherwise.

The real-time data enables supervisors to correct problems and reinforce progress as it happens, not after the break or during the next shift. Frontline Advisor puts everything supervisors 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 supervisors 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.

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?

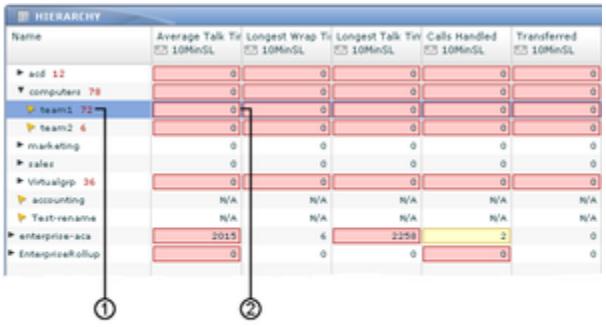
The FA administration page is used primarily to enter threshold and rule values. Administrators or supervisors choose what rules and thresholds apply to each agent, team, or group (also called nodes) in the monitoring hierarchy, and enable or disable the threshold or rules for each. Based on the configured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



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

2. Shading indicates a threshold violation

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.

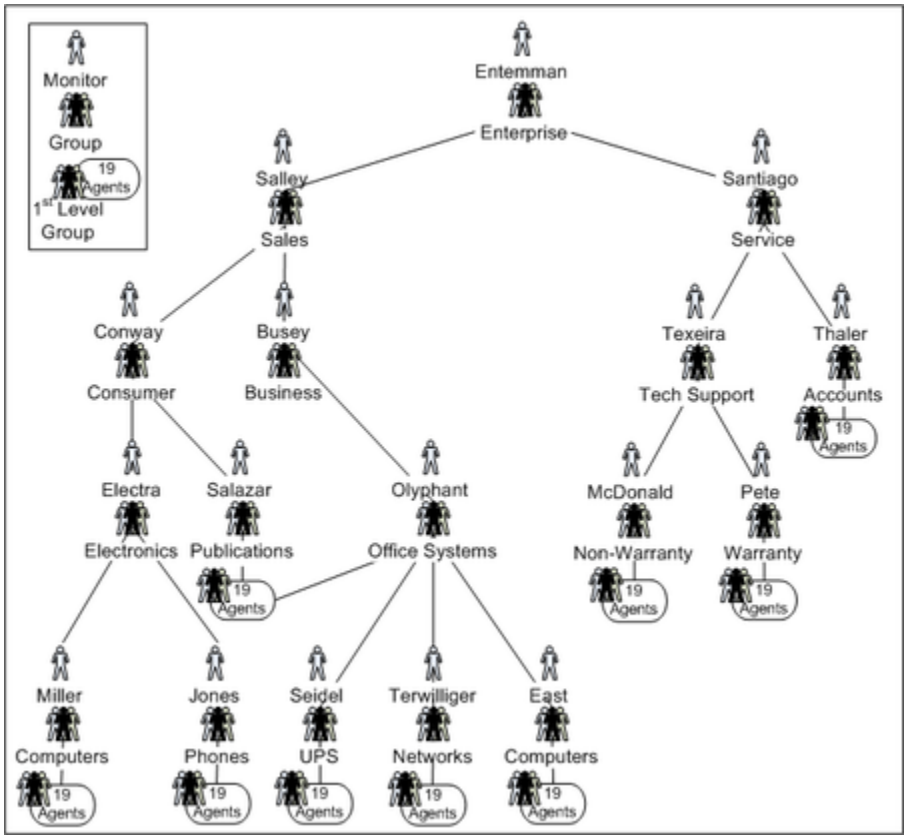
FA Monitoring Hierarchy

The monitoring hierarchy, used in Genesys Frontline Advisor supervisor dashboard, 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.



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 Administrator 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?

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 Server 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 Genesys Configuration 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 Genesys Administrator.

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, the monitoring hierarchy defined in Genesys Configuration Server is loaded. If multiple folders in Configuration Server comprise the FA hierarchy, then FA creates a consolidated view of the hierarchy with a virtual enterprise node linking all the various hierarchies together.

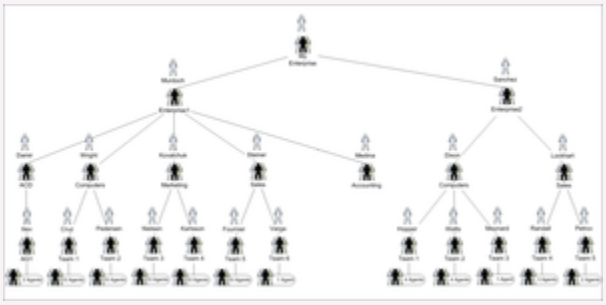
The hierarchy is also loaded daily at 02:55 a.m., or whenever you click the **Hierarchy Reload** button on the **Settings** tab of the FA administration page. Any subsequent changes to the hierarchy are reflected after the next rollup cycle, without waiting for the overnight reset or reloading the hierarchy manually.

Access permissions are configured at each node of the hierarchy according to user roles defined by administrators. 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 Server. 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.

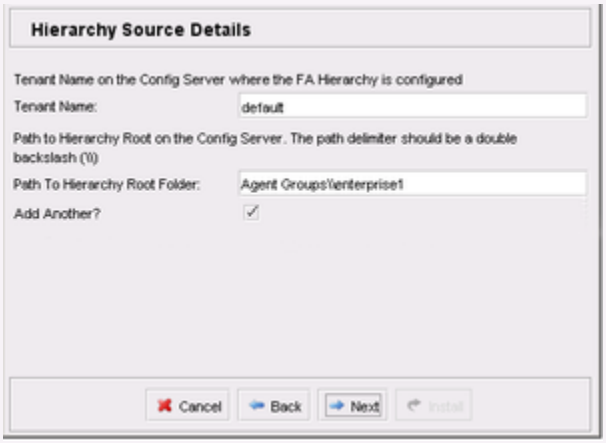


Creating a graphical representation of your enterprise

You configure the hierarchy, shown in the preceding figure, using a Genesys configuration interface, such as Genesys Administrator. The hierarchy must be configured and stored in the Genesys Configuration Server in order for it

to display on the FA dashboard. For example, under **Agent Groups** in the Genesys configuration interface, you would have an `enterprise1` folder, and within it you would have folders for the `accounting`, `acd`, `computers`, `marketing`, and `sales` teams. You would configure the appropriate agent groups within each of those folders.

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 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 Enterprise rollup folders and subfolders from the Configuration Server. The following screenshot shows the hierarchy on the FA dashboard.

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.

Can I View Agent Skills in the Monitoring Hierarchy?

You can view agent skills and skill levels on the Frontline Advisor dashboard. The Frontline Advisor server retrieves the list of skills and skill levels for each agent from the Configuration Server. The names of skills display in the Frontline Advisor dashboard exactly as an administrator entered them in the Genesys configuration interface (for example, Genesys Administrator).

On the FA dashboard, **Agent Skills** is a default column in the **Team** pane. You can hide the metric from display by removing the Agent Skills metric from the **Selected Metrics** pane in the Column Chooser.

Related Information

See the following for more information:

- *Genesys Frontline Advisor Help* for information about using Column Chooser to hide or display metrics on the FA dashboard.
- State Metrics Displayed for Agents for information about the Agent Skills metric.

Role-Based Access Control for Advisors

Pulse Advisors support role-based access control (RBAC). You can use RBAC to control which users can access specific components—for example, you can use RBAC to configure access to the Advisors administration module for a specific subset of managers.

Advisors applications use Configuration Server business attributes, which means that the Advisors applications can take advantage of Genesys Roles for controlling access at a detailed level to Advisors' business objects and metrics.

RBAC is enforced primarily by visibility in the interface. What a user sees is determined by the Roles which have been assigned. If the user is not assigned a Role that grants him or her access to a piece of functionality, that functionality is not displayed to that user.

There are three important concepts associated with RBAC:

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

What are RBAC permissions?

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

Object permissions determine which users have access to a certain object or to what objects a given user has access. This is done through the use of access groups or on an individual user basis. Objects include the following:

- Contact Center Advisor and Workforce Advisor
  - Metrics
  - Operating Units
  - Reporting Regions
  - Geographic Regions
  - Contact Centers

  - Application Groups
- Frontline Advisor
  - Metrics
  - Levels of the Frontline Advisor hierarchy (that is, the folders and agent groups)

What are RBAC roles?

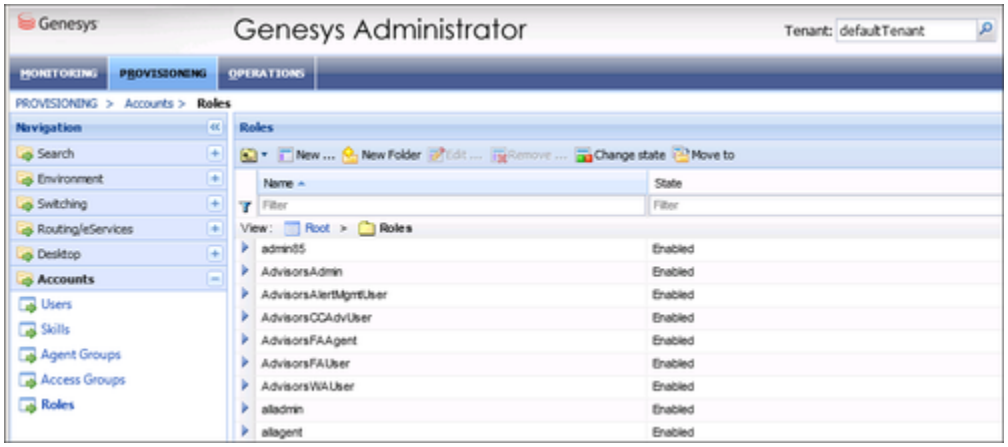
The major component of RBAC is a Role. If it is important in your enterprise to control users' access to information (metrics, hierarchy levels, and business objects), you configure Users and Roles – including the assignment of permissions and privileges to each Role – before any of those users log in for the first time. Each time you have a new user in your enterprise, you assign that person to Roles in a Genesys configuration interface, such as Genesys Administrator.

Roles define what facilities are provided to users to review and manipulate various types of data. These include which property controls are available for items permitted by object permissions, what modules are visible, and access control for entities not represented by configuration objects. A Role is assigned to a User, and that User is then able to do only what that Role permits. One User can be assigned multiple Roles, and one Role can be assigned to multiple Users. A Role may also be assigned to an Access Group, and Users in that Access Group are then able to do what the Role permits.

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

Roles can also be used to protect access to entities that are not configured as configuration objects, such as logs. In general, when determining the accessibility to an object by a user, the user session cannot retrieve objects if they are not among those objects to which the user has access (as defined by object-access permissions). For data that is available in the session, Role privileges refine what can be done with the data.

Assigning Roles to Users and Access Groups



Roles can be assigned to either Users or Access Groups.

> **Important**
> To inherit permissions, Access Groups and Users must belong to the tenant specified during the Advisors Platform installation.

Once a Role is assigned to an Access Group, all Users in the Access Group are assigned that Role. The Access Groups and/or Users must have Read access to the Role to be able to access the Role.

> **Important**
> Names of Access Groups must not contain spaces.

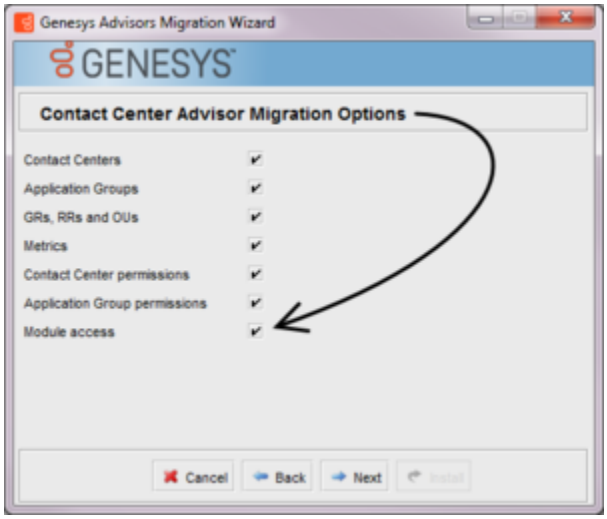
The figure shows an example of Advisors Role configuration.

New Users

By default, new users are not assigned any default Roles. They must be assigned Roles by a system administrator or by an existing user with appropriate permissions.

Default Roles Created by Migration

Module access is determined by the Roles associated with a user's profile. An optional check box on the Advisors migration utility, which is provided in the software distribution package, creates the module access schema. The figure, Migration Wizard, shows the optional **Module access** check box.



Migration Wizard

The utility creates default Roles in the Configuration Server, with each one representing access to a

particular module. Each Role has a limited set of privileges associated with it. The default Roles are:

1. AdvisorsAdmin – allows access to the Advisors administration module for Frontline Advisor, Contact Center Advisor, and Workforce Advisor users, to whom you have assigned that Role.
2. AdvisorsFAUser
3. AdvisorsFAAgent
4. AdvisorsCCAdvUser
5. AdvisorsWAUser
6. AdvisorsAlertMgmtUser

You can change the preceding Role names post-migration.

Further Reading on Roles

Additional sources of information on Role-based access, privileges and permissions are:

- Genesys Security Deployment Guide
- Genesys Administrator Extension Deployment Guide
- Framework Configuration Manager Help
- Genesys Administrator Extension Help

What are RBAC privileges?

Roles consist of a set of role privileges (Read, Change, Execute, and so on). Privileges determine what tasks or functions a user can execute on objects to which he or she has access. You must define Advisors Role privileges in a Genesys configuration interface, such as Genesys Administrator or GAX.

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

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, typically a system administrator, bundles these tasks into Roles. The Roles are then assigned to Users. As a result, each User can perform only those tasks for which they have privileges.

Functionality permissions, or privileges, determine what tasks or functions a user can execute on objects to which he or she has access. If a privilege is present in a Role, then any user who is assigned that Role has access to the functionality controlled by that privilege.

Where do I configure roles, permissions, and privileges?

Roles, and related configuration, are stored in the Genesys Configuration Server.

Typically, you configure RBAC 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.

Use a Genesys configuration interface, such as Genesys Administrator, to add Users to a Role. Add users with one of the following methods:

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

You also use a Genesys configuration interface to import Advisors privileges into a Role, or to assign Role-based permissions to Persons or Access Groups.

> **Tip**
> A user must have Read access to the Role (either directly or through an Access Group) to which he or she is assigned.

Each Advisors privilege name uses the following general structure:
[application name].[module name].[task grouping].[privilege name]

Ensure you copy the exact privilege with no leading or trailing spaces. Some privileges work as single entries; some require a group of privileges to ensure full access as you expect. For the list of privileges for each Advisors component, see the CCAdv/WA Access Privileges and FA Access Privileges pages.

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

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

roles?

There is no limit on:

- the number of Roles that can be present in the Configuration Server
- the number of Access Groups or Users that can be present in the Configuration Server
- the number of Roles supported by Advisors
- the number of Access Groups that are supported by Advisors

Roles, and the privileges associated with Roles, are cumulative. A single User or Access Group can be assigned multiple Roles. In such cases, the user will have the combined set of privileges granted by each Role. In other words, the user is granted any privilege that is granted by at least one of the assigned Roles. This ensures that the user is able to perform the tasks of all Roles in which they participate.

Each user can also belong to multiple Access Groups, with different permissions coming from each group. In such scenarios, the user's permissions are a union of the permissions of all the Access Groups to which he or she belongs, unless access is specifically denied for one group, which takes precedence (see the following scenarios).

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

- User A is part of Access Groups X and Y.
  Group X does not have any defined access to a metric.

  Group Y has explicit access granted to the metric.

  In this case, user A is granted access to the metric.
- User A is part of Access Groups X and Y.
  Group X is explicitly denied access to a metric.

  Group Y is explicitly given access to the same metric.

  In this case, user A is denied access to the metric.
- User A is part of Access Groups X and Y.
  Group X is explicitly denied access to a metric.

  Group Y does not have any defined access to the same metric.

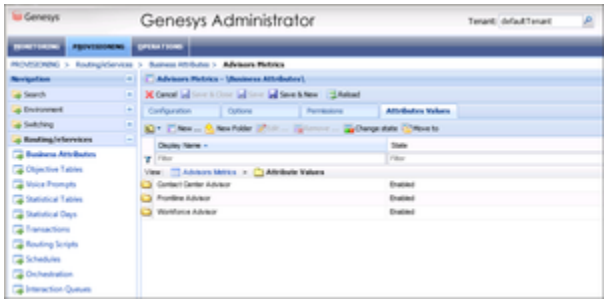
  In this case, user A will be denied access to the metric.
- User A is part of Access Groups X and Y.
  Neither group has defined access to the metric.

  In this case, user A will be denied access to the metric.

Can I control access to metrics?

Metrics are handled differently than other Advisors business objects. You must add the Advisors metrics in Genesys Configuration Server before you can assign the necessary permissions to Users or Access Groups (you use permissions to control access to metrics (see What are RBAC permissions?, above)).

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 figure shows an example of the folder structure for Advisors metrics. The folder structure shown below is mandatory. The business attributes must be created in the "Default Tenant" chosen during Advisors installation. Click the figure to enlarge it.



Advisors metrics in Genesys Administrator

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

To avoid confusion over similarly-named metrics, and because Configuration Server 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, ContactGroup, Application, or Team
Channel	Email, WebChat, Voice, All, or AllNonVoice
Name	The name of the metric

For example, FA metrics would have names like:

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

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.

FA Access Privileges

You can control access to information in the Genesys Pulse Advisors 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).

In FA, you use RBAC to control users' access to:

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

The following tables list the RBAC privileges that are available for Frontline Advisor users.

See the following documents for more information about configuring user profiles:

- Framework Configuration Manager Help
- Genesys Administrator Extension Help

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

Administration Module

Privilege	Controls Access To:
AdvisorsAdministration.canView	Administration module

Advisors Dashboards

Privilege	Controls Access To:
Advisors.ChangePassword.canView	Change Password function

Frontline Advisor Dashboard

Privilege	Controls Access To:
AdvisorsAdministration.Metrics.canView	**Report Metrics** page
AdvisorsAdministration.MMW.canCreate	The Create and Copy functions in the Report Metrics Manager. Users require this privilege to create custom metrics.
AdvisorsAdministration.MMW.canEdit	The Edit function in the Report Metrics Manager. Users require this privilege to edit metrics.
AdvisorsAdministration.MMW.canDelete	The Delete function in the Report Metrics Manager. Users require this privilege to delete custom metrics.
AdvisorsAdministration.MMW.SourceMetrics.canView	**Source Metrics** page
AdvisorsAdministration.MMW.SourceMetrics.canCreate	The **Create Source Metrics** button on the **Source Metrics** page. Users require this privilege to create custom source metrics.
AdvisorsAdministration.MMW.SourceMetrics.canEdit	The Edit function on the **Source Metrics** page. Users require this privilege to edit source metrics.
AdvisorsAdministration.MMW.SourceMetrics.canDelete	The Delete function does not display on the Source Metrics page. Users require this privilege to delete custom source metrics.
FrontlineAdvisor.SupervisorDashboard.canView	Frontline Advisor supervisor dashboard
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView *The FrontlineAdvisor.SupervisorDashboard.canView privilege must also be present*	**Teams** pane in the FA supervisor dashboard. In addition to the **Teams** pane, the **Alerts** pane is not displayed to users to whom you have not assigned this privilege.
FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges*	**Alerts** pane. If you have not assigned the FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privilege to a user, the user will not have access to the **Alerts** pane even though the FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privilege is assigned.
FrontlineAdvisor.SupervisorDashboard.ColumnChooser.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege*	Column Chooser
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges*	The data sorting functionality in the **Teams** pane
FrontlineAdvisor.SupervisorDashboard.TeamAlertsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges*	The data sorting functionality in the **Alerts** pane
FrontlineAdvisor.Administration.canView	Frontline Advisor page in the administration module

FrontlineAdvisor.Administration.Settings.canView *Requires the FrontlineAdvisor.Administration.canView privilege*	The **Settings** tab on the FA administration page in the Administration module.
FrontlineAdvisor.Administration.Hierarchy.canReload *Requires the FrontlineAdvisor.Administration.canView and FrontlineAdvisor.Administration.Settings.canView privileges*	The hierarchy reload action on the **Settings** tab of the FA administration page in the Administration module.

FA Thresholds and Rules Overview

You use Pulse Advisors 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 in the Genesys Configuration Server by administrators.

The following sections describe helpful general features of Pulse Advisors and FA administration that help you when navigating throughout the Advisors interface 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
- Working with FA Metrics Thresholds
- Working with FA Rules

Persistent Settings

When logging in to or out of any machine, or switching between modules in the Pulse Advisors interface, the Advisors interface retains the following settings:

- Monitoring hierarchy expansions
- Selected level in the monitoring hierarchy
- Last selected 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

Type 1

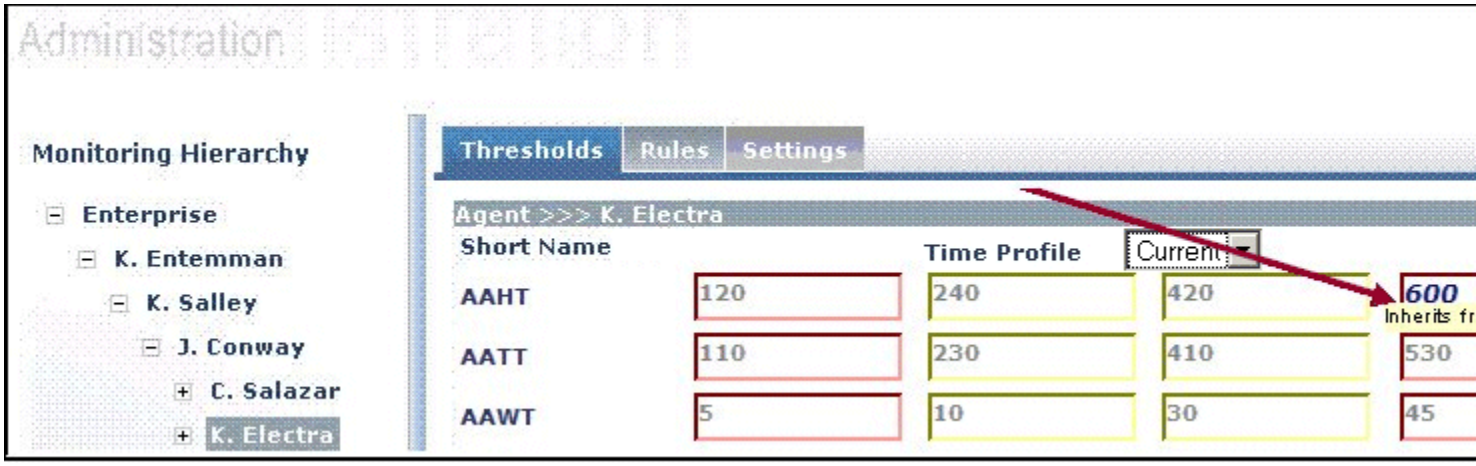
This ToolTip displays if you move your mouse cursor over the threshold value of 540, inherited from the root node.

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

Monitoring Hierarchy Navigator

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, after each rollup cycle, 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 **Settings** tab on the FA administration page.

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

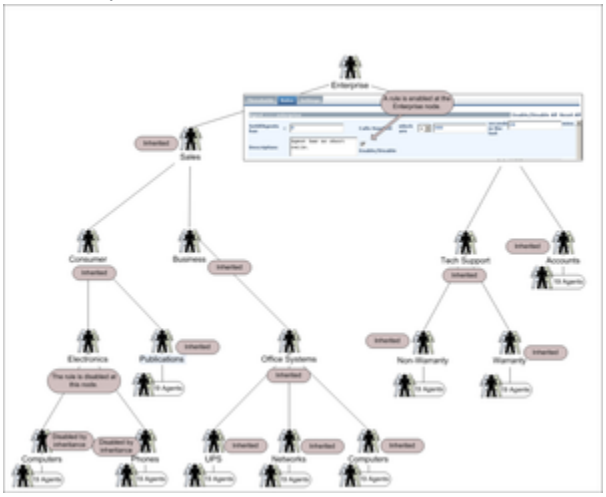
Once the monitoring hierarchy is defined and imported, you, or another administrator in your organization, can control each FA dashboard user's access to agents and other users (see Role-Based Access Control for FA).

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 figure, "Monitoring Hierarchy Navigator", is an example of the 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.



Example of inheritance

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 figure, "Example of inheritance", shows an example of inheritance, and an override, within the hierarchy. Click the image to enlarge it.

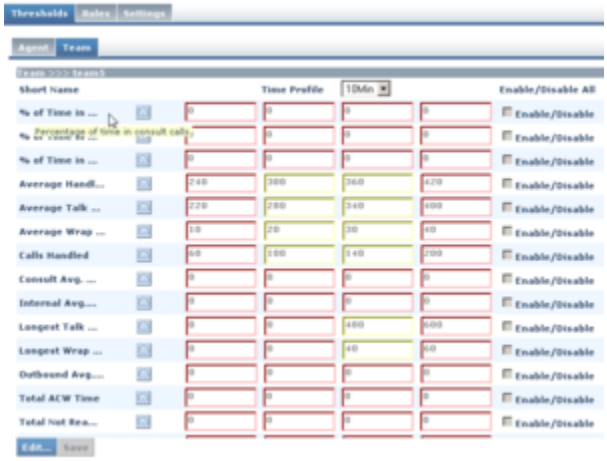
Working with FA Metrics Thresholds

The **Thresholds** tab on the Genesys Frontline Advisor (FA) administration page enables you to define the critical and acceptable conditions for the metrics to which you have been granted role-based access.

Because an agent can belong to multiple agent groups, it is possible in Frontline Advisor to define a threshold in different ways, and according to different overrides, for 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.

<tabber>

About=



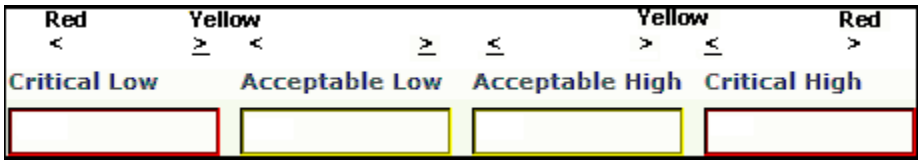
Thresholds tab with Team metrics displayed

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 Figure, "Thresholds tab with Team metrics displayed", shows an example of the **Thresholds** tab with the **Team** tab selected. Click the image to enlarge it.

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 the Frontline Advisor dashboard. 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.

Example 3

|-| How To ...=

Procedure: View Thresholds

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

Steps

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.

Procedure: Disable/Override All Thresholds

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

Steps

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**.

Procedure: Define 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 mouse 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.

Steps

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:
   a. To discard any changes made and revert the contents of the **Thresholds** tab to the last values saved to the database, click **Cancel**.
   b. 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.

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.

Working with FA Rules

The **Rules** tab on the Genesys Frontline Advisor (FA) administration page enables 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.

<tabber>

About=

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 totalled 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 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 figure, "Rules tab", shows an example of the **Rules** tab. Click the image to enlarge it.

Rules tab

Each rule can 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.

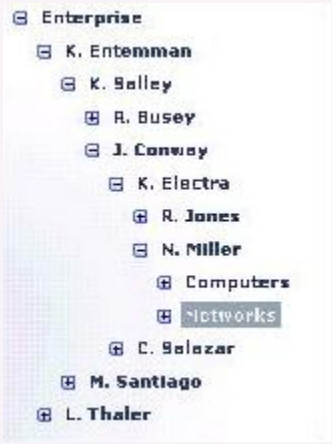
If an invalid value is entered, an alert message box displays when you press the **Save** button.

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 Advisors 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.

|-| How To ...=

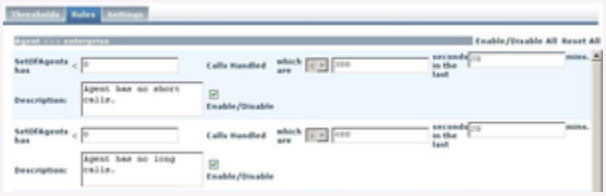
Procedure: View rules

Steps

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.

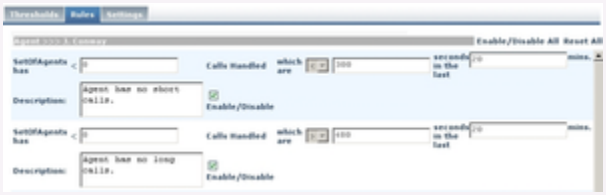
Example: Viewing Rules

The figure, "Rule configuration at the Enterprise node", 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

Steps

1. Select the **Rules** tab on the Frontline Advisor administration page.
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.

Procedure: Define a rule

Steps

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.
10. Do one of the following to complete configuration:
    a. To save all of the rules, click **Save**.
       If any errors are detected during validation, an alert message displays.
    b. To discard any changes made and revert the contents of the **Rules** tab to the last values saved to the database, click **Cancel**.

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 figure, "Editing a Rule", shows what the values now look like.

Editing a Rule

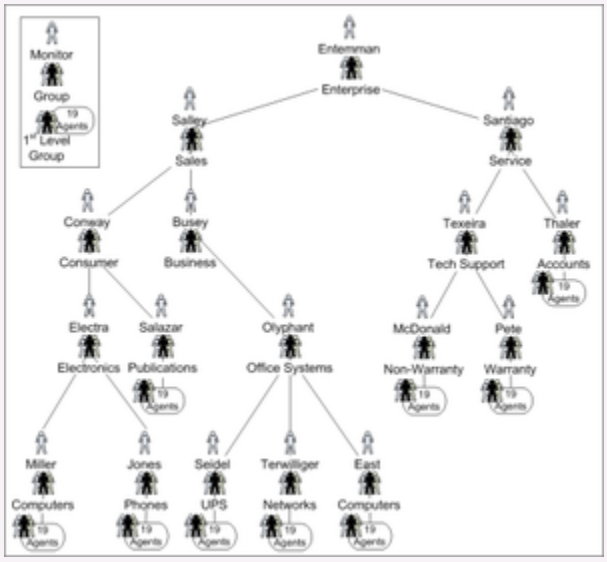
From now on, unless changes are made, the Conway node contains an override value of 600. All nodes in the subtree, if they are enabled and if they do not have their own override value, inherit the value of 600. Overridden rules are not automatically enabled, although in this example you would typically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

Metric Manager

The Advisors "Metric Manager" label in the administration module is a section heading, and is not a link to a page.

The Metric Manager section of the Advisors Administration module contains two pages:

- Source Metrics
- Report Metrics

What are Source Metrics and Report Metrics?

A report metric is a metric used in the dashboard of one of the reporting applications. It refers to a metric used in the dashboard of either Contact Center Advisor/Workforce Advisor or Frontline Advisor.

A source metric is the definition of the metric in the source system, such as Genesys Stat Server.

See *Terminology* below for detailed definitions.

Custom Metrics Support

You can create and update custom metrics for application and agent group objects for Contact Center Advisor and for agent objects for Frontline Advisor.

Restrictions

Genesys does not support the creation of new custom metrics for the WA application.

Access to metrics must be configured by an administrator in Genesys Configuration Server. Data relating to or dependent on metrics to which a user does not have access permissions does not display for that user. For information about role-based access control (RBAC) privileges related to metric management actions, see CCAdv/WA Access Privileges and FA Access Privileges.

Terminology

The following terminology is used in the descriptions of the **Source Metrics** and **Report Metrics** pages of the Administration module.

- The *Application* object type means the base object types of queue, interaction queue, calling list, call type, or service, for CCAdv.
- A *Raw Report Metric* is a report metric that is created from a source metric. When creating a raw report

metric, you must select a source metric. The source metrics available for selection are the Genesys source metrics that are created and maintained using the Source Metric Manager. Only the source metrics that correspond to the object type you selected are available when creating a raw report metric.

- A *Calculated Report Metric* is a report metric expressed as a formula involving one or more raw report metrics as operands. The format options specified for the calculated report metric override any format options specified for the individual raw report metric used to build the calculated report metric. A source metric cannot be directly associated with a calculated report metric.

Source Metrics

In the Source Metric Manager, you manage source metric definitions that come from the Genesys Stat Server data source, also called Statistic definitions.

You can perform the following actions in the Source Metric Manager:

- View the source metrics.
- Create and edit new custom source metrics.
- Delete custom source metrics.

Fields and options on the **Source Metric Details** page are dependent on one another. For example, the `Subjects` drop-down list is populated based on your selection in the `Objects` list. As you make selections, other lists, options, and fields update to offer only applicable properties.

Use `Queue` object–type source metrics with both ACD queues and virtual queues.

For information about source metrics and source metric attributes, see documentation for the Real-Time Metrics Engine (Stat Server), particularly the Stat Server User's Guide and the Reporting Technical Reference.

Supported Media Types

The Source Metric manager supports the following media types for custom source metrics:

- Voice
- E-mail
- Chat
- Workitem
- NEW SMS (starting with release 8.5.2)

Stat Server Current State Source Metrics

New custom source metrics cannot be created for the Stat Server categories of `Current State` and `Current State Reasons`. There are source metrics that ship with Advisors for these categories, and the customization available on these metrics is limited. For example, the Reason Code Key is configurable, but it is not possible to extract agent readiness based on capacity rules for a non-voice channel. See also Customizing the Stat Server Current Target State Source Metrics.

The AgentState source metric – derived from the Stat Server `Current State` category – includes a filtered source metric definition called `AgentDN`. Frontline Advisor uses the related AgentDN report metric to provide information about the DN extension, ACD position, or multimedia channel into

which each agent is logged.

Related Information

- See Team View for more information about the display of DN information on the Frontline Advisor supervisor dashboard.
- See Source Metrics Retrieved for Each Agent and State Metrics Displayed for Agents for information about the metrics associated with the display of agent DN information on the FA supervisor dashboard.
- See Filtered Source Metrics for more general information about filtered source metrics.

Relationships between Source and Report Metrics

The following table lists the relationship between the source metrics and the report metrics on the **Report Metrics** page.

If you select this object type in the Source Metric Objects field	Then the Source Metric will be available for this Report Metric object type
Agent	Agent
GroupAgents	Agent Group
Queue*	Application (queue-based)
NEW GroupQueues*	Application (DN Group-based)
StagingArea	Application
CallingList	Application
* When you create a new custom source metric using the `Mediation DN` object group, you can select either the `Queue` or `GroupQueues` object, or you can select both. Selecting the `Queue` object means the source metric will be applicable only to queues. Selecting the `GroupQueues` object means the source metric will be applicable only to DN groups. If your custom source metric should be applicable to both DN groups and queues, then select both `Queues` and `GroupQueues` in the **Objects** field for the `Mediation DN` object group.	

Source Metrics and RBAC

If you have sufficient privileges to see the **Source Metrics** page, then you can view all existing statistics definitions. There is no role-based access control on the individual statistic definitions.

RBAC privileges also manage the following:

- A user's ability to create custom source metrics
- A user's ability to edit source metrics
- A user's ability to delete source metrics

See CCAdv/WA Access Privileges and FA Access Privileges for the list of privileges associated with the Source Metric Manager.

Working with Source Metrics

A custom source metric that you create is immediately available for use in the creation of a report metric.

The source metrics that ship with Advisors (default metrics) cannot be edited, with the exception of the Reason Code source metric, for which you can edit the following attributes:

- Reason code Key
- Reason Start Overrides Status Start

For users with `Edit` privileges:

- The `Edit` button is present and enabled if a selected metric is a custom metric (not a default source metric).
- The `Edit` button is absent or disabled if a selected metric is a default source metric.
- When editing a source metric with dependent report metrics, a warning message indicates that the edit will affect the dependent metric(s).
- You cannot change the category for an existing source metric from `Current` to `Historical`, nor the reverse.

The source metrics that ship with Advisors (default metrics) cannot be deleted. You can delete a custom source metric provided no report metric is derived from it.

For users with `Delete` privileges:

- The `Delete` button is present and enabled if the selected metric is a custom metric (not a default source metric).
- When attempting to delete a custom source metric that has dependent report metrics, an error message indicates that you cannot delete the metric because of the dependent report metric(s).

Category Options

A statistic category is either a `Current` category or a `Historical` category. The `Current` category is the current value of the evaluated measurement in the Stat Server. The `Historical` category means the metric is evaluated over a specific time interval (the time profile).

JavaCategory source metrics can be either Current or Historical; you can specify which to use based on your requirements.

Main Mask/Relative Mask Wild Cards

Wild cards such as * to select all options or ~ to exclude a mask are implicitly supported in the Main Mask and Relative Mask editing windows. Use the Select All feature at the bottom of the editing window to select all options and then selectively deselect one or more options with the radio buttons.

For example, if MainMask = *, ~LoggedOut, do the following in the Main Mask editing window:

1. Use Select All: Selected to select all the options in the window.
2. Click the LoggedOut radio button to deselect it.

Filtered Source Metrics

When you select a source metric on the **Source Metrics** page, the attributes for that metric are displayed in the lower half of the page, including the Filtered Source Metrics table in which you can create a filter for the metric.

To apply a filter to a selected metric, specify the following in the Filtered Source Metrics table:

- Name of the filter
- A description for the filter
- The filter: A filter must be one that is available in the Configuration Server **Business Attributes** > **Advisors Filters** section.

You can add as many filters to an unfiltered source metric as you require; each filtered version becomes a new source metric.

You can edit filtered source metric properties. You can also delete a filtered source metric if no report metric is using a filtered variation. This includes filtered source metrics defined on default metrics; they can be edited or deleted.

Each filtered variation is stored on a database table separate from the source metric table.

Finding Filtered Source Metrics in the Source Metrics Manager

Filtered source metrics are variations of other parent source metrics; you can find the filtered source metrics only under the respective parent source metric. For example, to find the filtered variations of a source metric called Retrieved Calls, navigate to the Retrieved Calls source metric and select it. The filtered variations are displayed in the details in the lower half of the page.

Configuring the Media_Workitem Filter as the Business Attribute Value for the

Default iWD Source Metrics

Advisors applications include some intelligent Workload Distribution (iWD) source metrics (not including iWD Datamart metrics). These iWD source metrics include a `Media_Workitem` filter. Before you enable the iWD metrics, you must configure an attribute value in the **Advisors Filters** business attribute to correspond to the `Media_Workitem` filter. Genesys recommends that you configure the **Advisors Filters** business attribute on a tenant that is the default tenant for the Advisors suite installation (on which you configure all Advisors metadata).

Use the following properties when you configure the `Media_Workitem` filter attribute value in Configuration Server:

- Name = `Media_Workitem`
  The name of the filter (`Media_Workitem`) is case-sensitive; ensure you enter it correctly.
- The Annex of the `Media_Workitem` filter attribute value must contain a mandatory section called `Filter`. In this `Filter` section, you must enter an option value that defines the filter. For the `Media_Workitem` filter attribute value, enter the following option value:
  `PairExists("MediaType","workitem")`

  For more information about Advisors filter attribute configuration, see Using Advisors Filters Configuration to Segment Objects and Metrics.

Customizing the Stat Server Current Target State Source Metrics

Starting in release 8.5.001, you can create custom source metrics for the Stat Server category of `CurrentTargetState`.

In release 8.5.0, the following default metrics were available in the Metric Manager, and were evaluated from the Current Target State source metric. In release 8.5.001, these metrics based on Genesys Stat Server data are no longer shipped with Advisors because you can create your own custom metrics based on the Current Target State metric.

Object Type	Report Metric	Reporting Application
Application	Avail Voice	CCAdv
Agent Group	Avail Voice	CCAdv
Agent	Voice Ready	CCAdv
Agent	Voice Ready	FA

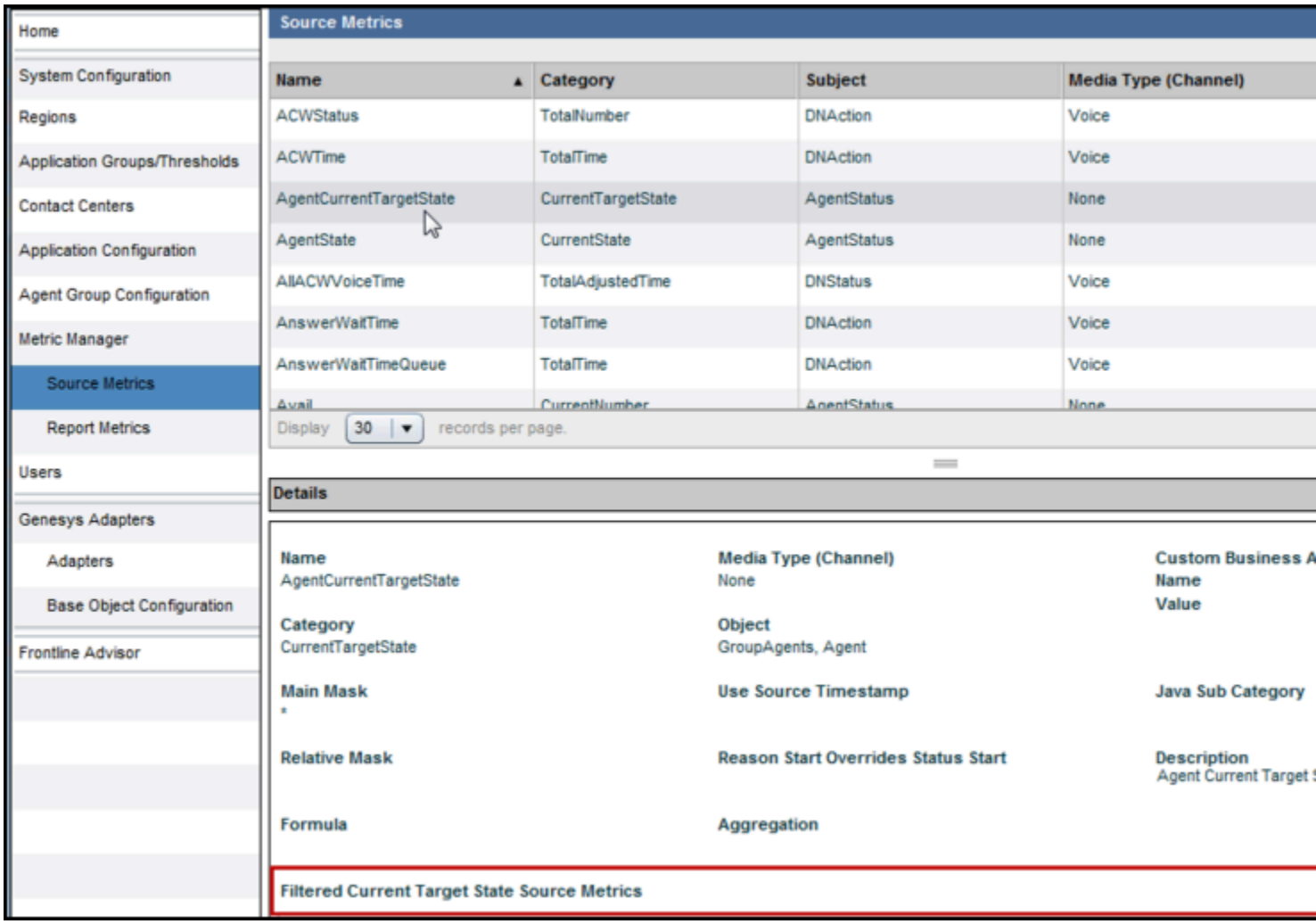
Creating a Custom Source Metric for the CurrentTargetState Category

In release 8.5.001, Advisors Genesys Adapter can extract agent media-capacity information from the default Current Target State source metric. An example of media-capacity is the maximum number of chat interactions that an agent can handle simultaneously.

You use the default Current Target State source metric that is supplied with Advisors and the **Filtered Current Target State Source Metrics** section of the Source Metrics Manager to configure your specific Current Target State attributes. The default Current Target State source metric supports both

agent and agent group object types.

Click the **Edit** button in the **Filtered Current Target State Source Metrics** section of the Source Metrics Manager for the Current Target State source metric. The following figure shows the **Edit** button at the bottom of the **Source Metrics** window.



The **Create** dialog box – instead of presenting filters – offers the following attributes:

- Type (that is, the Current Target State attribute type; only Media Capacity is available in release 8.5.001)
- Capacity Media Type
- Capacity Attribute

All media types registered in the Genesys Configuration Server under **Business Attributes > Media Types** are listed under the **Capacity Media Type** option.

The following options are available for **Capacity Attribute**:

- Routable Interactions Count (also known as Current Margin Count)
- Maximum Interactions Count
- Current Interactions Count

Create an enabled raw report metric for either CCAdv or FA based on each of the source metrics with the filtered media capacity attribute. You can create a raw report metric to display on the dashboard, or you can use the raw report metric to create other calculated report metrics.

Current Target State Metrics and Agent Groups

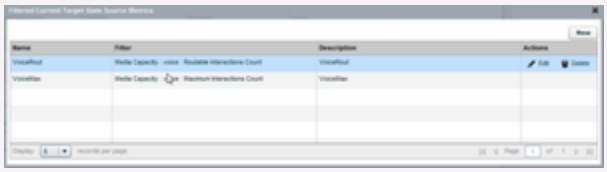
When the Current Target State metric is reported, AGA extracts the configured media capacity attributes for each agent in an agent group. The corresponding metric at the agent group level is evaluated based on the media capacity attribute at the agent level. Therefore, for all the media capacity attributes that Genesys supports in release 8.5.001, a formula of **SUM** is used to evaluate the agent group level metric value from the agent level attribute value.

Current Target State Metrics and Metric Applicability

You can configure metric applicability for the custom Current Target State report metrics in the same way that you configure applicability for any other raw report metric.

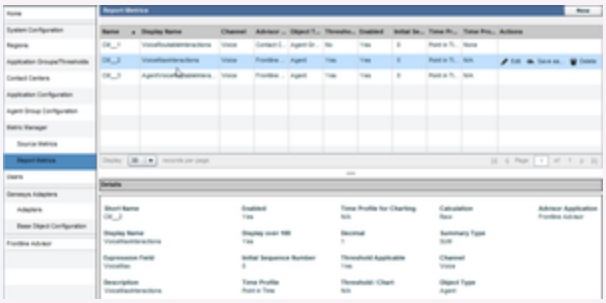
Example: Using Metrics Based on Current Target State

While an agent might manage many chat or email interactions simultaneously, that same agent can typically manage only one voice interaction at a time. To track an agent's availability for routable voice interactions using metrics on the dashboard, you could create report metrics based on the Current Target State metric that ships with Advisors. For example, the following screenshot shows two custom source metrics – VoiceMax tracks the maximum number of voice interactions for an agent and VoiceRout tracks the availability of the agent to handle a voice interaction.



Custom source metrics based on the default Current Target State source metric

You would then create custom raw report metrics that use those custom source metrics as the foundation. The following screenshot shows an example of custom report metrics.



Custom report metrics that use the previously-created Current Target State–based source metrics

After you create and save the enabled custom report metrics, they are available in the Advisors column chooser so you can display the metrics on the dashboard. In this example, which uses the Frontline Advisor dashboard, the custom report metric that tracks an agent's availability to take calls is the AgentVoiceRoutableInteractions metric. The VoiceMaxInteractions metric tracks the maximum number of voice interactions (calls) an agent can handle simultaneously.

The following screenshot shows one ready agent (J. Davis) and two logged-off agents. Note that the AgentVoiceRoutableInteractions metric indicates that only the agent in the Ready state is available for a voice interaction.

An agent in the Ready state is available to take a call. The AgentVoiceRoutableInteractions metric has a value of 1 for the agent who is ready. The VoiceMaxInteractions metric indicates that the agent can handle a maximum of 1 call at any time.

If that agent should take a break, or be on the phone, the AgentVoiceRoutableInteractions metric indicates that the agent is no longer available for any further calls.

An agent in the Not Ready state is unavailable to take a call. The AgentVoiceRoutableInteractions metric has a value of 0 for the agent in the Not Ready state.

An agent in the Talking state is unavailable to take a call. The AgentVoiceRoutableInteractions metric has a value of 0 for the agent in the Talking state.

Report Metrics

With the correct role-based access control (RBAC) permissions, you can view and edit all Contact Center Advisor, Workforce Advisor, and Frontline Advisor metrics on the **Report Metrics** page. Only certain attributes are editable.

You can customize the default metrics that ship with Pulse Advisors to address your specific Contact Center performance and service quality measurements. You can also use the **Report Metrics** page to create custom metrics for the dashboard.

You can search by metric name or description in all supported languages, regardless of the language you selected at login.

Any changes that you make using the **Report Metrics** page are logged in the audit log file, similar to all other logged administrative actions.

Custom Agent Group Metrics and the CCAdv Totals & Averages Row

Genesys does not provide an equivalent agent-level metric for a custom CCAdv agent group metric; therefore, de-duplication on the `Totals & Averages` line is not supported for custom agent group metrics.

Role Based Access Control and the Metric Manager

The Report Metrics Manager functionality is controlled by privileges and permissions (Role-Based Access Control), which you assign to Users and Access Groups in a Genesys configuration interface, such as Genesys Administrator. A privilege determines the actions a user can perform. A permission grants or denies viewing of individual metrics for a user.

In the Report Metrics Manager, the view, create, copy, edit, and delete actions are individually controlled by privileges. For information about Metric Manager–specific privileges, see CCAdv/WA Access Privileges and FA Access Privileges.

Use the following information if you are granting or denying Metrics Manager–related permissions and privileges to users:

- A user can view all the metrics to which he or she has a Read object permission.
- A user who can create a custom metric can also view and delete that metric, unless the `View` permission or the Change permission to the metric was explicitly denied in the Configuration Server after the user created the metric.
- To create custom metrics, a user must have a `Create` security permission granted on the `Advisors Metrics Business Attributes` section in Configuration Server. Without this permission, the user cannot create custom metrics. Similarly, a Change permission must be granted at the root attribute level or at the individual metric attribute value level to ensure the user can delete an existing custom metric.

Editing Default Metrics

You cannot delete Advisors' default metrics, but you can edit some of the properties. The display name, description, and the reporting application–specific formatting properties can be edited. You can also edit the following properties for metrics that have them:

- Time Range upper bound/lower bound (if applicable to the corresponding source metric)
- Notification mode and frequency
- Insensitivity
- Exclude Base Object filter
- Enabled

Creating Custom Metrics

You can create custom metrics using the **Report Metrics** page. Custom report metrics are created from Genesys Stat Server source metrics.

> ### Important
> You can create only custom application and agent group metrics for CCAdv, and custom agent metrics for FA. You cannot create custom metrics for any other types of objects. For example, you cannot create custom metrics for contact groups.

There are two key selections you must make when you create a custom report metric:

- Select an Advisors application
- Select the object type

The **Report Metrics** page then shows the relevant custom metric configuration properties based on the Advisors application and object type you select.

You must provide an expression for the metric (that is, a formula that produces a metric value). Expressions can contain other metrics and constants (numbers) as operands, as well as the operators, functions, constructs, and symbols described in the following Table. Supported operands are included as buttons in the `Expression Editor` on the **Report Metric Details** page.

The elements of expressions are limited to existing standard or custom source metrics provided by the Genesys Adapter, source metrics imported from the CISCO environment, and existing CCAdv application, CCAdv agent group, and FA agent dashboard metrics. Metrics that are used in expressions for calculated metrics must have time profile definitions that are compatible with the calculated metric. To state it differently, time profiles for all non-point-in-time reporting metrics that are used in the expression of another metric must use a time profile definition that is the same as the time profile definition of the calculated metric. For example, if you want to create a custom report

metric that has a 30 minute sliding time profile, then metrics in the expression for that custom metric must also have a 30 minute sliding time profile.

Metric Type	Acceptable Operands
Calculated custom report metrics	Arithmetic operators: • + (addition) • – (subtraction) • * (multiplication) • / (division) Brackets (to ensure the required operation sequence) You can also include the >, < , and = operators in expressions.

Example: Expression Field Entries

The following examples demonstrate valid formulas you can enter into the Expression Field. If you have multiple operands in the expression, it is important to use parentheses to group the calculations.

- Custom metric is a sum: Enter (<Metric1>+<Metric2>). For example, (CallsAnsweredTo5+RouterCallsAbandQTo5).
- Custom metric is a percentage-based metric: Enter 100*(<Metric1>/<Metric2>). For example, 100*(RouterCallsQNow/STF). For this type of expression, you must start the expression with the 100* component followed by the metric calculation, as shown in the example.
- Custom metric measures the longest value for an activity or state: Enter (DateTime - <AgentGroupMetric>). For example, (DateTime - RouterLongestCallQ)

Propagating custom metric changes to the Stat Server

If you create a new custom metric, or make changes to an existing metric that must be propagated to the Stat Server, these changes are applied during the overnight refresh. The dashboard shows values for any newly-added custom metrics only after the changes have been applied. This is applicable to both CCAdv/WA and FA metrics.

Enabling a disabled metric or disabling an enabled metric is applied to the Stat Server during the overnight refresh.

Metric Groups

Every raw custom report metric must be assigned to a Metric Group. This is not applicable to calculated report metrics; you do not assign them to metric groups.

A metric grouping indicates applicability of metrics to configured objects, which determines if metric statistic(s) must be requested for a certain object. See the *Working with Metric Groups* page for an example.

The default selection for a new metric is the `Default` metric group. When creating a custom metric, you can assign the metric to another available metric group. You also have the option to create a new metric group and assign the report metric to that new group.

After you create a metric group, it is available for selection for subsequent metric grouping. The metric group information for a report metric is not stored in the Genesys Configuration Server.

See the *Working with Metric Groups* page for more information about the metric groups and how to manage them.

Working With Metrics

<tabber>

Metric Properties Descriptions=

The following Table provides descriptions of the metric properties.

Property	Advisors Application	Object Types	Editable For	Description
Short Name	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	None	The name of the metric that uniquely identifies it for internal purposes. This field is system generated. You can only view this property; you cannot edit it.
Language	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	A drop-down list that includes supported languages for your release. English is the default value. Your selection for this parameter controls the language property for the metric

Property	Advisors Application	Object Types	Editable For	Description
				display name and description.
Display Name	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	The name used for display in the column chooser and dashboard. The name must be unique for a given channel and language. The display name property accepts 128 characters or less. The default language of the display name is English, but you can specify the name in another supported language using the Language parameter in the Report Metrics manager. NEW Manually Adding a Display Name If there is no display name provided for a metric that you want to enable, or if the display name field contains `Not Displayed`, then you can provide a meaningful display name manually. When adding a display name manually, you must use the following two rules: • The display name must be something other than `Not Displayed`. • Display names must be unique within each language and

Property	Advisors Application	Object Types	Editable For	Description
				channel. The administration module will reject a display name if it is already used by another enabled metric within a given language and channel. While each metric display name must be unique for enabled metrics within each language group, you can use identical display names (and descriptions) amongst the three available languages. That is, you can enter a display name for a metric in English, copy and paste that display name to the German-language and French-language versions of that same metric, and then successfully enable the metric in all three languages. See also Manually Adding a Description for information about manually adding a description to a metric.
Description	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	The metric description. The default language of the description is English, but you can specify the description in another supported language using the Language parameter in the Report Metrics manager.

Property	Advisors Application	Object Types	Editable For	Description
				NEW Manually Adding a Description If there is no description provided for a metric that you want to enable, then you can provide a description manually. You can use identical descriptions (and display names) amongst the three available languages. That is, you can enter a description for a metric in English, copy and paste that description to the German-language and French-language versions of that same metric, and then successfully enable the metric in all three languages. Be sure to read Manually Adding a Display Name for additional information about entering a display name manually.
Advisor Application	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	A drop-down list with values representing each supported reporting application. The default value is Contact Center Advisor. Your choice of reporting application is reflected in the values available for the `Object` Type parameter.
Object Type	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	A drop-down list containing the options available for the Advisor Application you selected. For example, if you selected Contact Center Advisor as

Property	Advisors Application	Object Types	Editable For	Description
				the Advisor Application, `Application` is one of the options in the `Object Type` list.
Calculation	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	Formerly `Metric Type`. Select a radio button to indicate if the custom metric is `Raw` or `Calculated`.

Summary Type	FA, CCAdv, WA	FA: Agent
		CCAdv: Agent Group or Application
		WA: Contact Group
			Custom Metric	A drop-down list containing options that determine how aggregation is to be performed when rolling up the metric to the higher level of the hierarchy:
				• When the metric type is `Raw`, the options are:
				  • SUM
				  • MIN
				  • MAX
				• When the metric type is `Calculated`, `Summary Type` is not applicable (`None`).

Metric Group	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	For a custom metric, a drop-down list with values for all available metric groups. There is one metric group that ships with Advisors – `Default`. To create your own metric group, click `Create New`

Property	Advisors Application	Object Types	Editable For	Description
				`Metric Group`. On confirmation, the new metric group name is appended to the list of metric groups, and is automatically selected in the drop-down. The new metric group value is saved as part of the custom metric creation process, and is subsequently available for selection for other metrics. The metric group name is case-sensitive. A metric group labelled `MG` is a different metric group from one labelled `mg`.
Enabled	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	Formerly `Display on Column Chooser`. Select a radio button to specify whether the metric displays in the Column Chooser (Enable) or not (Disable). Disabling a raw report metric means that the corresponding source metrics are not collected at the data source for the respective reporting application. In the case of Genesys Stat Server, you can reduce the load on the Stat Server by disabling unused metrics for a reporting application. However, note that each raw report metric is evaluated in two cases: 1. when directly enabled 2. when indirectly

Property	Advisors Application	Object Types	Editable For	Description
				enabled by its participation in the calculation of another enabled metric Therefore, to completely disable a raw report metric so it is not collected at the data source, you must both disable the metric and ensure it is not used in the calculation of another metric that is enabled. You can re-enable any disabled metric by updating the `Enabled` checkbox. Disabling or enabling raw report metrics takes effect on overnight refresh or on restart. Disabling a metric for Contact Center Advisor means that CCAdv does not calculate the metric or send values for it to the dashboard. The effect of disabling takes place at the start of the next Short processing cycle in CCAdv XML Generator.
Channel	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	A drop-down list containing options to specify the media channel type for which the custom metric is shown in the Column Chooser and on the dashboard.
Decimal	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	A drop-down list containing options you can use to specify the number of decimal places to display for metric values.
Initial Sequence Number	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	Formerly Sequence `Number`. Use this parameter to specify the initial column order

Property	Advisors Application	Object Types	Editable For	Description
				sequence in which to place the metrics on the dashboard. Clicking Reset in the dashboard's Column Chooser displays the metrics with a sequence number, in the order specified by the number.
Reorder Columns	FA	Agent	Custom metric	By default, the checkbox is cleared. Select the check box to allow users to re-order the column positions on the dashboard.
Threshold Applicable	CCAdv, WA	CCAdv: Application WA: Contact Group	All	Formerly Threshold. When creating a custom metric, the checkbox is cleared by default. If this box is checked, you can define thresholds for the metric on the **Application Groups/ Thresholds** page. If this box is cleared, then you will not be able to define thresholds on that page.
Threshold/Chart	CCAdv, WA	CCAdv: Application WA: Contact Group	All	Enter values for the threshold range (minimum and maximum). These values also determine the y-axis values in a graph.
Display over 100%	CCAdv, WA	CCAdv: Application WA: Contact Group	All	A format option. When creating a custom metric, the checkbox is selected by default. A checkmark in the box

Property	Advisors Application	Object Types	Editable For	Description
				indicates that values over 100 display actual values. If the checkbox is cleared, values over 100 display as 100+.
Format Pattern	FA	Agent	All	A drop-down list containing options to specify the general structure of the metric. The default selection is `Number`.
Time Profile	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All, but with qualifications: • CCAdv/WA: Fully editable for custom metrics. For default metrics, you can enable or disable charting only. • FA: You can enable or disable the time profile only.	Select a radio button to indicate if the time profile is `Point in Time` or `Historical`. `Point in Time` on the **Metric Details** page is the `Current` time profile with a duration of 0. You can assign a time profile group (Short, Medium, or Long) to a point-in-time custom report metric for an application or agent group in the Time Profile section. The time profile interval and time profile type are not shown for the point-in-time metric. XML Generator creates alerts only for metrics that are mapped to the Short time profile group. If you select the `Historical` time profile, available additional options are dependent on the Advisors component with which the metric is associated: • CCAdv: When you select the `Historical` radio button, you can configure up to three time profiles in the `Time Profile` table. You must specify at least one. Use the `Enabled` checkbox to enable and

Property	Advisors Application	Object Types	Editable For	Description
				disable CCAdv metrics by time profile. The allowed time interval for an enabled profile is from 1 minute to 24 hours. The default time intervals are: • 5 minutes for a Short group • 30 minutes for a Medium group • 24 hours for a Long group **Tip** NEW Custom historical chat and email agent group metrics that use the Short, Medium, or Long time profile group, and which you enable, are available in the Column Chooser for display on the dashboard. Previously, Contact Center Advisor could display only Short email and chat agent group report metrics on the dashboard. For each enabled time profile, you must also indicate the time profile type (`Sliding` or `Growing`). The default type for each time profile group is: • Sliding for a Short group

Property	Advisors Application	Object Types	Editable For	Description
				• Growing for a Medium group • Growing for a Long group The `Chart` checkbox is available for CCAdv application-type metrics. The checkbox is cleared, by default. Metrics that are used in formulas for calculated metrics must have time profile definitions that are consistent with the calculated metric. For example, to create a custom metric that has a 30 minute sliding time profile, all metrics used in the expression for the custom metric must also have a 30 minute sliding time profile. • WA: The `Chart` checkbox is available for WA contact group–type metrics. The checkbox is cleared, by default. • FA: You can enable and disable metrics for FA by time profile in the `Time Profile` table; you can specify which metrics are enabled for a given time profile and disable metrics that are not required for that time profile. The time profile durations displayed in the

Property	Advisors Application	Object Types	Editable For	Description
				`Time Profile` table are those that are configured in the FA administration page. You cannot edit the time profiles in the Report Metrics manager; you continue to configure and edit the FA time profiles in the FA administration page. To enable a time profile for a specific metric, both of the following conditions must be true: • the time profile is enabled at the application level (that is, on the `Settings` tab of the FA administration page) • the time profile is enabled for that metric in the Report Metrics manager To disable a time profile, you need to disable the time profile in only one of the preceding locations. The results of enabling a time profile for a particular metric are the following: • The metric is available in the column chooser and dashboard for display for its enabled time profiles. • The aggregation engine

Property	Advisors Application	Object Types	Editable For	Description
				calculates the metric for the enabled time profiles. **Important** You can enable or disable time profiles for calculated metrics irrespective of their associated operand-level metrics. The disabled time profile for the operand-level metric impacts only the visibility of that metric on the dashboard. FA time profile durations cannot be configured on a per-metric basis; therefore, calculated metrics are limited to the time profiles configured in the FA administration page. Default settings are: • all of the time profiles for the default metrics are enabled in the Report Metrics manager • only the first time

Property	Advisors Application	Object Types	Editable For	Description
				profile in the Settings tab of the FA administration page is enabled (consistent with previous releases). Changes to time profile settings in the FA administration page are automatically updated in the Report Metrics manager. However, enabling or disabling time profiles for FA metrics in the Report Metrics manager require you to reload the FA hierarchy before the changes are propagated to the FA application; you can reload the hierarchy manually, or wait for the overnight refresh.

Expression Editor

Use the Expression Editor to build the formula that produces a value for your custom metric.

Property	Description
Channel and Metric tables	Use the Channel and Metric tables to find existing metric expressions that you can use in the calculation of your new custom metric. The entries from the list of metrics serve as operands for building the expression. When creating a raw report metric, the operands available are source metrics. And when creating a calculated report metric, the operands available are other raw report metrics and other calculated report metrics.
Metric Description	When you select a metric in the Metric table, a description of that metric displays in the Metric Description box.
Expression Field	You build the expression, or formula, for your custom metric

Property	Description
	in the Expression Field. Use the buttons above the field to add operands to the expression of a calculated metric. You might see two expression fields for some agent group metrics. This happens when the calculation for individual agent groups is different from the totals and averages calculation. If you are creating a custom agent group metric, you can specify only one calculation expression to be applied in both individual agent groups and totals and averages calculations. You might see two expression fields for some agent group metrics. This happens when the calculation for individual agent groups is different from the totals and averages calculation. If you are creating a custom agent group metric, you can specify only one calculation expression to be applied in both individual agent groups and totals and averages calculations.
Notification Mode	Available for raw metrics and only when the selected source metric belongs to a Genesys Stat Server data source. See the *Stat Server User's Guide* for more information. Select a value from the drop-down list. The default value is Time Based. This means that Stat Server will notify the adapter periodically based on the notification frequency. Changed Based means that the Stat Server will notify the adapter as soon as the values change in Stat Server.
Notification Frequency	Available for raw metrics and only when the selected source metric belongs to a Genesys Stat Server data source. See the *Stat Server User's Guide* for more information. Specify a non-negative integer. The default value is 0. This field is enabled only when the notification mode is Time Based.
Insensitivity	Available for raw metrics and only when the selected source metric belongs to a Genesys Stat Server data source. See the *Stat Server User's Guide* for more information. Specify a non-negative integer. The default value is 0, which indicates that insensitivity is not applied.
Exclude Base Object Filter	Available for raw metrics and only when the selected source metric belongs to a Genesys Stat Server data source. `Exclude base object filter` is a property of the statistic template. See the `Stat Server User's Guide` for more information. The checkbox is available for Contact Center Advisor application and agent group metrics. Select the checkbox to exclude the base object configuration filter when statistics are requested for the metric. The checkbox is cleared, by default. **[+] Additional information about Exclude Base Object Filter** When a Genesys Stat Server filter is combined with an agent group or a queue, and the combination is published on the CCAdv administration module's Base Object configuration page, the statistic for any metric for which you opted to exclude the base object filter is requested, but without the object configuration filter. The same base object configuration filter is applied on all the statistics that are requested for a given source object. All default CCAdv application metrics are configured to include this object configuration filter.

Property	Description
	However, because the configured filter is applied to all the statistics, there will be circumstances when you must exclude some of the metrics from being subjected to this "blanket" filter. For example, on the agent state–based agent group metrics, you should not apply an interaction-based filter; it could result in incorrect results. In such cases, you use this property to specify which metrics to exclude from the filter. For example, the default interaction queue metrics and the calling list metrics are configured to exclude the base object filter. On the CCAdv dashboard, each filtered combination displays on a separate line. Any metric that is excluded from the base object configuration filter is shown on a separate line as an unfiltered metric for the selected agent group or queue. The Exclude Base Object Filter property does not influence the Stat Server filter that is specified at the source metric level. The property in Metric Manager is called the *base object filter* to help you distinguish between the Stat Server filter that is applied on the filtered source metric, and the Stat Server filter that is applied at the base object level. It is possible that both filters (the metric filter and the object configuration filter) must be applied to a certain metric. In such cases, the filters are combined; both filtering conditions must be met for a statistic value to be reported for that metric.
Time Range Lower Bound and Time Range Upper Bound	The Time Range Lower Bound and Time Range Upper Bound fields are enabled for raw metrics, and only when the selected source metric is based on a category that requires a time range. For example, TotalNumberInTimeRange. Available for CCAdv raw report metrics only. Specify a non-negative integer. The upper bound must be greater than the lower bound. The default value is 0.

|-| How To...=

Use the following procedures to help you work with the Metric Manager.

For information about changing the default Service Level threshold setting, see Change the Default Service Level Threshold Setting.

Procedure: View Information about a Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.
- You require permission to view at least one metric.

  The **Report Metrics** page displays only the metrics to which you have Read permission in the Configuration Server.

Steps

1. In the Administration module, click **Report Metrics** in the navigation pane.
2. Locate the metric for which you want to view detailed information.

   To assist you when searching for a specific metric, use the filters on the right side of the page to reduce the number of metrics that display. By default, all filters are selected.

   Use the page navigation arrows under the list of metrics to move between pages of metrics. By default, the metrics are displayed in alphabetical order.
3. Click a metric to select it. Details about the metric display at the bottom of the **Report Metrics** page.

Procedure: Create a Custom Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.
- You require the `Create` permission in the Configuration Server for the Advisors Metrics Business Attribute on the default tenant.
- You require the privilege that grants you access to the **Create** button.
- Read the notes in the section called Creating a Custom Metric for important information about correctly building a custom metric, including how to build the expression for a custom metric.

Steps

1. In the Administration module, click **Report Metrics** in the navigation pane.
2. Click **New**.

   The **Metric Details** page opens.
3. Enter information to define the new metric. Ensure you enter information into all required fields.

   For descriptions of the metric properties, see the **Metric Properties Descriptions** tab on this page.
4. If you want to return the **Metric Details** page to the default settings, click **Reset**.
5. Click **Save** to save the metric.

   If you entered all information correctly, the page returns to the **Report Metrics** page. The new metric displays in the list of metrics.

Procedure: Copy a Metric to Create a Custom Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.
- You require the `Create` permission in the Configuration Server for the Advisors Metrics Business Attribute on the default tenant.
- You require permission to view the metric that you want to copy.
- You require the privilege that grants you access to the **Save as** option.
- Read the notes in the section called Creating a Custom Metric for important information about correctly building a custom metric, including how to build the expression for a custom metric.

Steps

1. In the Administration module, click **Report Metrics** in the navigation pane.
2. Select the custom or standard metric that you want to use as a template for a new custom metric.

   You can use application or agent group metrics as templates for new CCAdv custom metrics, and agent-level metrics for new FA custom metrics.

   If you select a standard dashboard metric as a template for a new custom metric, the expression of the original standard metric might not be supported in the new custom metric. You must edit the calculation to limit operands to those supported by the custom dashboard metric creation process. See Creating a Custom Metric for important information about correctly building a custom metric.
3. Click the **Save as...** option. The **Metric Details** page opens.
4. Edit information to define the new metric. Ensure you enter a new display name for the new custom metric. Ensure you enter information into all required fields.

   For descriptions of the metric properties, see the **Metric Properties Descriptions** tab on this page.
5. Click **Save** to save the metric.

   If you entered all information correctly, the page returns to the **Report Metrics** page. The new metric displays in the list of metrics.

Procedure: Edit a Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.

- You require permission to view the metric that you want to edit.
- You require the privilege that grants you access to the **Edit** option.

> **Important**
>
> You require the `AdvisorsAdministration.MMW.canEdit` privilege to edit metrics, but a Change permission is not required in the Configuration Server for the metric business attribute value because none of the edited information is updated on the Configuration Server after the initial creation of the business attribute value.

Steps

1. In the Administration Module, click **Report Metrics** in the navigation pane.
2. Select an existing metric to edit.
3. Click **Edit**. The **Metric Details** page opens.
4. Edit the metric properties.

   The metric properties you can edit are dependent on the type of metric you selected to edit. Your ability to edit standard (default) metrics is limited. For example, the expression editor is always disabled for standard metrics. If you want to edit a standard metric, you must copy the metric and save it as a new custom metric.

   If you change the display name or description of a metric, the information is updated in Advisors only and is not propagated to the Configuration Server.
5. Click **Save** to save the metric.

   If you entered all information correctly, the page returns to the **Report Metrics** page. The metric displays in the list of metrics.

Procedure: Delete a Custom Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.
- You require permission to view the metric that you want to delete.
- You require a Change permission in the Configuration Server for the business attribute that represents the metric that you are deleting.

- You require the privilege that grants you access to the **Delete** option.

> **Important**
>
> Deleting a custom metric deletes the record in Advisors and also deletes the business attribute value under the Advisors Metrics Business Attributes section in the Configuration Server.

Steps

1. In the Administration module, click **Report Metrics** in the navigation pane.
2. Select a custom metric to delete.
3. Click **Delete**.

   If a raw report metric is used in a calculation for a calculated report metric, you cannot delete that raw report metric. If you attempt to delete a metric that is used in another metric calculation, Advisors displays an error message.

Procedure: Enable Graphing of Metrics (CCAdv/WA)

Purpose:

A Metric Graphing window is accessible from both Contact Center Advisor and Workforce Advisor. You specify which combination of metrics and time profiles to graph using the **Chart** checkboxes in the **Time Profile** table.

You can choose to graph Application-type metrics in CCAdv, and Contact Group-type metrics in WA.

If you attempt to enable more metrics for graphing than the limit configured in the database, a warning message displays stating that the maximum number of metrics that can be graphed has been exceeded. You cannot save updates in the Metric Manager until you reduce the number of metrics enabled for graphing.

Steps

1. Open the Administration module.
2. Click **Report Metrics** in the navigation pane.

3. Use the filters on the **Report Metrics** page (on the right) to show as many or as few metrics as required.
4. Do one of the following:
   - Select an Application-type metric or a Contact Group-type metric and click **Edit** in the **Actions** column to open the **Metric Details** page.
   - Click **Create** to open the **Metric Details** page and create a new Application-type custom metric.
5. On the **Metric Details** page, select the applicable time profile.

   The **Time Profile** radio buttons are grayed out (that is, you cannot change the time profile) for default metrics.
6. To enable the metric for graphing, select at least one time profile from the **Time Profile** table, and select the **Chart** checkbox.

   The **Time Profile** table offers only one time profile group if the **Point in Time** radio button is selected, and three possible time profile options if the **Historical** radio button is selected.

   Each historical metric that can be graphed can have more than one time profile for graphing. For example, you can enable both AHT 30 Min Growing and 5 Min Sliding for graphing.

Procedure: Propagate Changes to Column Chooser in CCAdv and WA

Purpose:

A change you make in the **Report Metrics** page does not appear immediately in the Column Choosers in the dashboards. This applies to any kind of change, whether to a default metric, or to a custom metric, including creation or deletion of the latter.

Steps

1. Save or apply the change on the **Report Metrics** page.
2. Log out of Advisors.
3. Wait at least five minutes for the changes to be read from the Advisors database into cached data.
4. Log in to Advisors.
5. In the appropriate dashboard, open the Column Chooser. You should see your changes reflected there.

Procedure: Propagate Changes to Column Chooser in FA

Purpose:

A change you make in the **Report Metrics** page does not appear immediately in the Column Choosers in the dashboards. This applies to any kind of change, whether to a default metric, or to a custom metric, including creation or deletion of the latter.

Steps

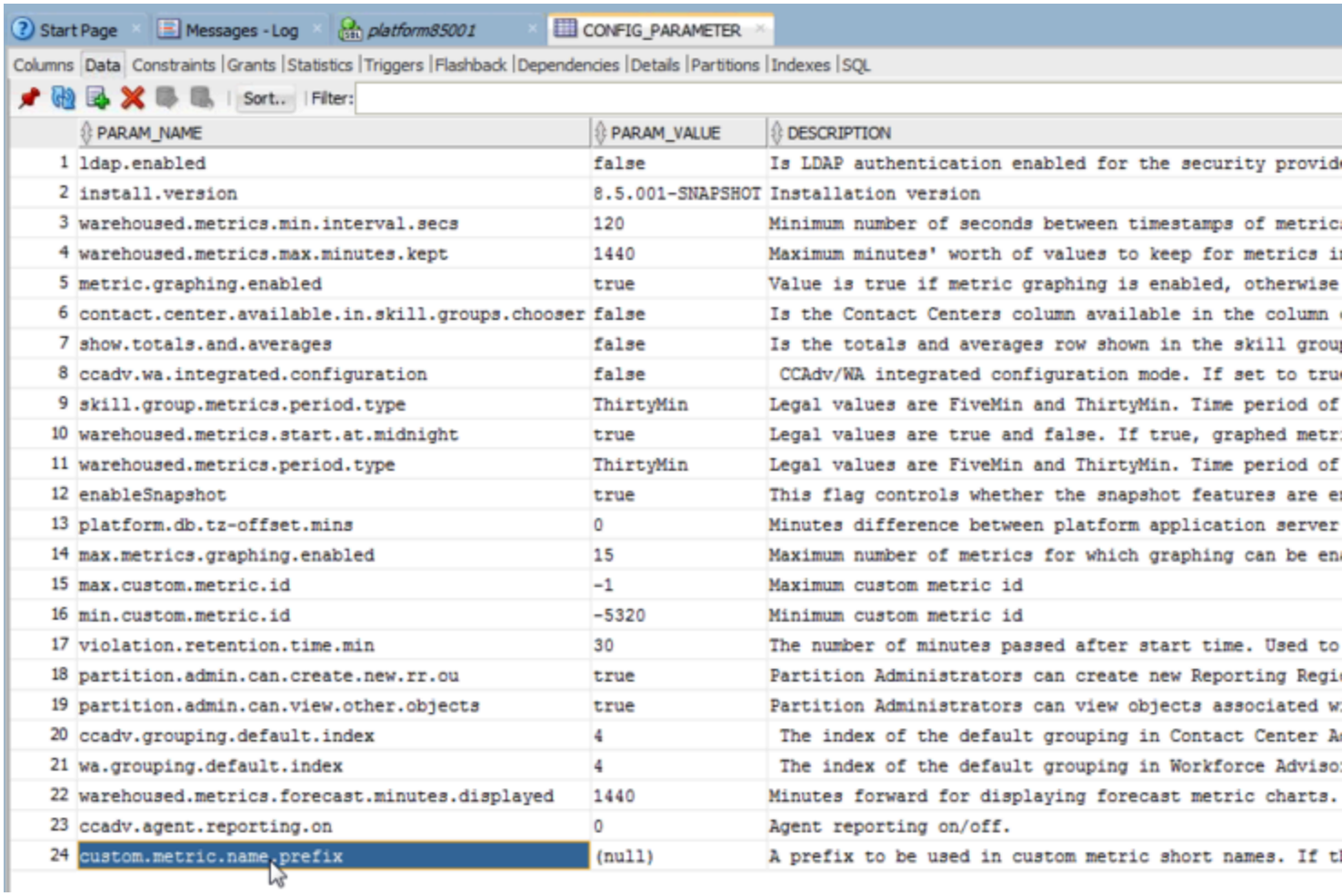
1. Save or apply the change on the **Report Metrics** page.
2. In the FA Administration page, **Settings** tab, click the **Hierarchy Reload** button. Alternatively, wait until the nightly reset procedure has executed.

   Note that new report metrics will not be displayed in the accessible dashboard until the application server is restarted.

|-| Changing the Custom Metric Internal Name Prefix=

Custom metrics for Advisors have a standard, auto-generated `CM__metric id` internal name. You might have several Advisors installations that use the same Genesys Configuration Server, and if an administrator creates a custom report metric in each of two different installations, but uses the same metric ID (and, therefore, the same name), one metric overwrites the other in the Configuration Server. Overlapping metrics loaded into the Configuration Server impact permission settings for different installations. These metrics can also be deleted with a negative impact on other installations.

To resolve these types of issues, the `Config_Parameter` table of the Advisors Platform database includes a parameter, `custom.metric.name.prefix`, that governs the custom metric naming space within the installation. The figure shows the parameter.



The custom.metric.name.prefix parameter in the Config_Parameter table of the Platform database. A value of "null" means the Met will use the default prefix (CM) for the internal name of new custom report metrics.

The value you enter for this parameter becomes the prefix for custom report metric names and replaces the standard CM prefix in the internal system name. This lets you differentiate and isolate the metrics created in different installations and therefore avoid any conflicts at the Configuration Server level.

When you change the value for the `custom.metric.name.prefix` parameter, it immediately triggers the replacement of all custom metric names with a name that uses the specified prefix. The names of custom metrics used as operands in calculation expressions are also replaced.

You must run the Advisors Object Migration Wizard to import the metrics for which you specified a new prefix into the Configuration Server. Users of the Advisors interface who were logged in when you configured the prefix must log out and log in again to gain access to the metrics with the new names. All new custom metrics are created with the new prefix.

The Advisors administrator must ensure the prefixes are unique within the existing set of Advisors installations. There is no restriction on the number of metric prefix changes, but Genesys recommends that you carefully manage the number of obsolete metrics in Configuration Server and that you remove metrics that no longer exist in any Advisors installation.

Working with Metric Groups

You can collect raw reporting metrics into groups under each supported reporting application on the **Report Metrics** page in the administration module. Reporting applications supported by the **Report Metrics** page are Contact Center Advisor and Frontline Advisor. A metric can participate in only one metric group. You can decide how you want to group the reporting metrics used in your enterprise based on your business needs.

One consideration when grouping report metrics is the relationship between a metric and the source objects. Previously, by default, all enabled metrics were applied on all configured base objects for a given object type. For example, all the enabled queue metrics were applicable to all the CCAdv queues published in a deployment. Also previously, you could distinguish between voice and non-voice virtual queues based on the Advisors queue type configuration. Voice and non-voice metrics could be based on the queue. However, this did not allow further sub-classification within the queue type, or allow classification of other object-type metrics.

Using the metric grouping functionality, you can specify exactly which metrics are applicable to each source object. On the **Report Metrics** page, group raw report metrics, and then map the metric groups to configured source objects using Genesys Administrator. This mapping of metric groups to configured source objects specifies the applicability of a metric to configured source objects. The configured metric applicability works on all of the enabled time profiles of a given metric.

Metric applicability configured on a given object is applied to all of the CCAdv object-filter segments. You cannot specify the metric applicability on individual CCAdv base object-filter combinations because each filter combination is not a separate object in Genesys Configuration Server.

You can configure metric applicability for the following CCAdv and FA source objects:

- CCAdv:
  - Agent Groups
  - Applications (Genesys source objects: queues, calling lists, and interaction queues)
- FA:
  - Agents

Metric Grouping

The **Report Metrics** page allows grouping of metrics at the level of the raw report metric. Each raw report metric configured for a reporting application can be classified under one of the metric groups.

You can group related raw report metrics that are involved in evaluations of calculated report metrics for a source object in the same group, but it is not strictly necessary. If the various raw metrics involved in the calculation of a metric for a specific base object are in different metric groups, you must ensure that all metric groups that contain the contributing raw metrics for the calculation are mapped to the source object. If a group containing a raw metric required to successfully evaluate a calculated metric is not mapped to the corresponding source object, that raw metric cannot contribute to the metric’s calculated value. See the example below on this page.

Metric groups created using the **Report Metrics** page are not saved in the Configuration Server, but only in the Advisors Platform database. See additional information on the *Report Metrics* page in this document.

Restrictions

A metric can participate in only one metric group.

Metric grouping is allowed only on raw report metrics. You cannot group calculated report metrics.

Example

You have a calculated report metric – Total Handle time – that is evaluated as the sum of two raw report metrics. The formula is Total HandleTime = Total Talk time + Total AfterCallWork Time.

Scenario 1:

- You place Total Tallk Time in metric group 1.
- You place Total AfterCallWork Time also in metric group 1.

Assumption: On a given source object, the Total Handle Time metric must be evaluated.
Configuration: Configure the metric applicability such that metric group 1 is applicable on the given source object.

Scenario 2:

- You place Total Tallk Time in metric group 1.
- You place Total AfterCallWork Time in metric group 2.

Assumption: On a given base object, the Total Handle Time metric must be evaluated.
Configuration: You must configure the metric applicability such that metric group 1 and metric group 2 are applicable on the given source object.

Scenario 3:

- You place Total Tallk Time in metric group 1.
- You place Total AfterCallWork Time in metric group 2.

Assumptions:

- On a given base object, the Total Handle Time metric must be evaluated.
- You configured metric group 1 to be applicable on the given source object.
- You configured metric group 2 to be applicable on a source object that is not the given source object.

In this scenario, only Total Talk Time is available for evaluation of the calculated metric; Total AfterCallWork time is not considered in that evaluation. Depending on the evaluation of the formula, this can result in Total Talk time = Total Handle Time in the case of CCAdv, but in FA, the result of the evaluation might be N/A.

Configuring Metrics Applicability in Configuration Server

To configure metric applicability using Genesys Administrator, specify the metric groups as **Annex** options on the source objects.

You can configure metric applicability to individual source objects, or you can select more than one source object and configure identical metric applicability on all that you have selected.

For CCAdv, you can select agent groups, queues, interaction queues, and calling lists to configure metric applicability.

For FA, you can select agents to configure metric applicability.

The following procedures show you how to use Genesys Administrator to configure metric applicability for agent groups. The same procedure can be used for configuring all other source objects.

Tip

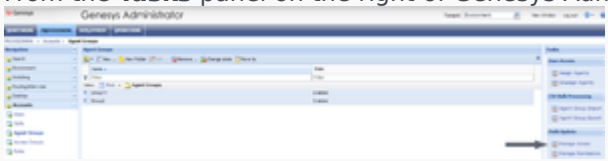
When you add new applications and agent groups to your configuration, any configured metric groups that exist in Genesys Configuration Server are used to determine the metric applicability of the new objects. If you want a new object to belong to a specific metric group, then you must add the metric group to the new object in Configuration Server before you refresh the **Application Configuration** page. Refreshing the **Application Configuration** page pulls the new applications and agent groups into the administration module as objects available for rollup configuration.

Procedure: Configure metric applicability for selected objects

Purpose: Use this procedure to add new metric groups as options to selected objects in Genesys Administrator.

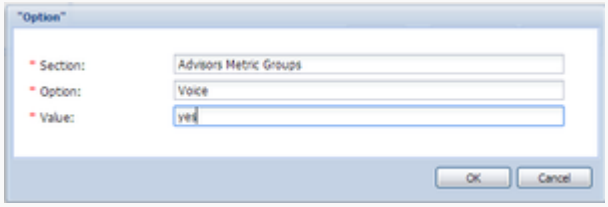
Steps

1. Select the objects for which you want to configure identical metric applicability. For example, if the same metric applicability should be configured for a given set of agent groups, identify those agent groups and multi-select them.
2. From the **Tasks** panel on the right of Genesys Administrator, select **Manage Annex**.



Select Manage Annex

3. On the **Add** section, click the **Add** button and add a new annex section called `Advisors Metric Groups`, as well as an option called the name of the metric group. The name of the metric group entered here must match the name of the metric group created and selected for the raw report metric on the Advisors **Report Metrics** page. The metric group name must also match in case; that is, it is case-sensitive.

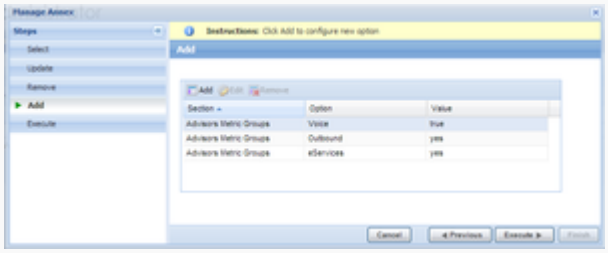


Add the Advisors Metric Groups Section

Genesys Administrator requires that you specify a value for each option. Anything can be entered, such as `true` or `yes`. The value for the option is not used.

If you have more than one metric group to add as an applicable metric group for the selected objects, click the **Add** button and repeat the process.

For example, the figure, "Advisors Metric Groups options" shows three metric groups added: Voice, Outbound, and eServices. Those three metric groups contain metrics that must be associated with the selected agent groups.



Advisors Metric Groups options

4. Click **Execute** and **Finish** to save your changes.

Procedure: Remove a metric group from selected objects

Purpose: Use this procedure to remove a configured metric group from selected objects.

Steps

1. Select the objects for which identical metric applicability must be configured. For example, if you must configure identical metric applicability for a given set of agent groups, identify those agent groups and multi-select them.

2. From the **Tasks** panel on the right of Genesys Administrator, select **Manage Annex**.
3. On the **Remove** section, click the **Add** button to add the metric group option that must be removed.
4. Click **Execute** and **Finish** to save your changes.

Default Metric Group

The Advisors default raw report metrics are all grouped under the `Default` metric group. Adding report metrics to this default metric group means that these metric groups are implicitly applicable to all source objects.

There is no need to explicitly configure a default metric group in the Configuration Server. See also *When the statistic template metric group is the Default metric group* below.

What Happens if I do not Assign Metric Groups to a Source Object?

If, for a given source object, you do not add any metric groups as Options, then none of the metrics from metric groups are applicable for that source object. However, if there are any other metrics of that object type that are still grouped under the `Default` metric group, they are still considered to be applicable. Therefore, there is no need to configure metric applicability on metrics that must be applied to all the source objects; it needs to be configured when some metrics must be excluded from some objects.

When are Configuration Server Changes Applied for CCAdv?

On startup, the configured source objects are fetched from the Configuration Server and stored in memory; this includes the metric groups configured on the CCAdv source objects. CCAdv subscribes to changes to the source objects in the Configuration Server, and this includes updates to the metric group configuration.

For both new and already-published objects, changes in the metric applicability are applied during the overnight refresh.

When are Configuration Server Changes Applied for FA?

On startup, when the FA hierarchy is loaded from the Configuration Server, the metric groups configured on the FA agent source objects are also loaded. On overnight refresh, or on the forced reload of the hierarchy from the Configuration Server, any changes to the metric group configuration on the FA agent objects are also reloaded.

How Metric Applicability works with Include/Exclude in Statistic Requests

CCAdv and FA use the metrics applicability configuration to decide which statistics to request on a specific object.

CCAdv and the FA application send the configured statistics to the data manager, which then routes those statistics to one or more adapter instances. When statistic requests are sent to the data manager, the applications (FA and CCAdv) also look up the metrics applicability configuration. Based on the results, the application (CCAdv or FA) determines which statistics to include in the statistics request.

When the statistic template metric group is the Default metric group

There is no default metric group in the Configuration Server to correspond to the `Default` metric group (the default metric group) in Advisors. It is unnecessary to fetch the objects applicable to this default metric group; any statistic that belongs to the `Default` metric group is automatically included for any object of that object type. For example, if there is an agent group metric that is included in the `Default` metric group, then it is applicable to all the published agent groups. In this example, "agent group" is the object type that links the agent group metric with the agent group source object.

When the statistic template metric group is a custom metric group

For a metric group that you create, CCAdv and FA look up the applicable objects. For a specific statistic request, if the corresponding metric group is applicable for the object (identified by the object ID and the object type), then that specific statistic is included in the statistic requests to Stat Server. If the metric group is not applicable for the object that corresponds to the statistic, then the statistic is excluded from the statistic requests to the Stat Server.

How Metric Applicability works with Voice and Non-Voice Stats Requests on Queues

In release 8.1.5, you used queue-type configuration of the virtual queues to specify if non-voice statistics should be requested on the virtual queues. If the option of "queueType = NonvoiceOnly" was set on a virtual queue in Configuration Server, then only non-voice statistics were requested.

Starting in release 8.5.0, metric grouping and the mapping of metric groups to configured source

objects replaces the usage of queue-type configuration. You can no longer use queue-type configuration in Configuration Server to indicate if non-voice statistics are requested on specific virtual queues. Instead, using metric applicability, the system determines if non-voice statistics can be requested on a virtual queue.

On every voice-only queue, the metric applicability must be configured to point to voice metric groups. On non-voice queues, the metric applicability must be configured to point to non-voice metric groups.

If there are queue metrics assigned to the `Default` metric group, those metrics are requested on both voice and non-voice queues.

If you currently use queue-type configuration, there is no migration path to convert to the metric applicability configuration. You must reconfigure based on metric applicability.

Metric Applicability in FA

FA gets its metric applicability mapping from Configuration Server. The FA tasks that issue statistics for state and performance metrics and rules do the following:

1. Resolve IDs of the agents to whom metric applicability applies
2. Resolve IDs of the metrics that apply to the above agents, and
3. Before issuing statistics, filter out metrics that do not apply to certain agents.

The result of the preceding actions is the following:

1. The connector returns statistics for certain metrics for certain agents.
2. When a metric does not apply to an agent:
    a. users see `N/A` on the dashboard, and
    b. a metric that does not apply to an agent is excluded from rollups that include this agent. That is, metrics contribute to rollups based on applicability.
3. Assigned and unassigned metrics are mutually exclusive:
    a. If no metric groups are assigned, all metrics apply to all agents.
    b. If metric group MG1 is associated with agent A1, then only metrics in MG1 apply to A1.
    c. If agent A2 has no metric groups applied, then all metrics apply to A2 except the metrics from MG1, which was assigned to agent A1.

If there are a number of metric groups configured in Metric Manager, but those metric groups are not configured on any of the agents in the FA hierarchy, then this is considered an incomplete configuration for FA metric applicability; the metrics on such metric groups are considered as applicable for all agents. Therefore, whenever metrics are in specific metric groups, make sure those metric groups are also configured on agents, as needed.

If a configured metric group is removed from all agents in the hierarchy, make sure to either unassign such metrics from that metric group by placing the metric back in the `Default` metric group, or disable those metrics if the intention is to not make those metrics applicable to any of the agents.

Genesys recommends that you avoid disabling metrics by placing them in an unused metric group.

Tracing the Metric Applicability in CCAdv

To trace how metrics have been applied to source objects for CCAdv, in the XML Generator `log4j.xml` file, change the priority value for the `com.genesyslab.advisors.eacore.adapterclient` category to `DEBUG`:
`log4j.category.com.genesyslab.advisors.eacore.adapterclient=DEBUG`

Whenever an object is published, the log indicates the number of statistics that are applicable on an object. For example:

```
2014-02-22 13:31:17,775 DefaultThreadPool 6 DEBUG [IssueStatistics] Found 28
applicable metrics for object: ObjectIdentifier [id=8354, name=7007@LucentG3,
tenantName=defaultTenant, filterName=null, objectSubType=ACD]
```