Performance Management Advisors Deployment Guide

Advisors Roles

12/20/2025

Advisors Roles

You can control access to information in the Contact Center Advisor (CCAdv), Workforce Advisor (WA), and Frontline Advisor (FA) dashboards and in the administration module 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).

It is typical to require access to various Advisors components early in the deployment and configuration process. The following sections describe Role-Based Access Control (RBAC) in terms of Genesys Performance Management Advisors, and include the list of privileges available with Advisors release 8.5.1.

> **Important**
> You must use Genesys Configuration Manager to add or edit privileges associated with roles.

[+] RBAC and Advisors

Performance Management 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?

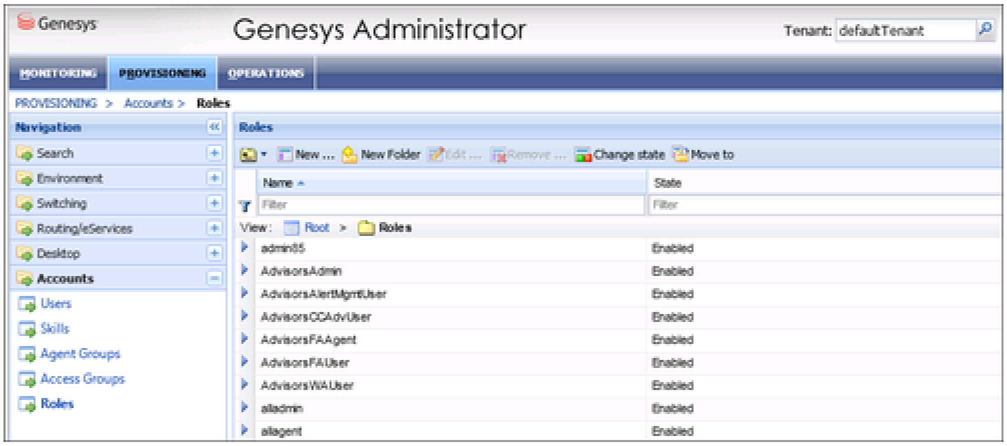
The major component of RBAC is a Role. If it is important in your enterprise to control users' access to information (metrics, hierarchy levels, and business objects), you configure Users and Roles – including the assignment of permissions and privileges to each Role – before any of those users log in 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.

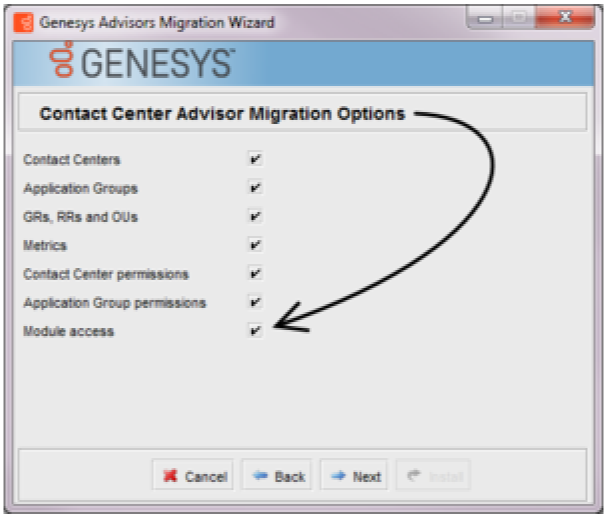
The figure shows an example of Advisors Role configuration.

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 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 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.

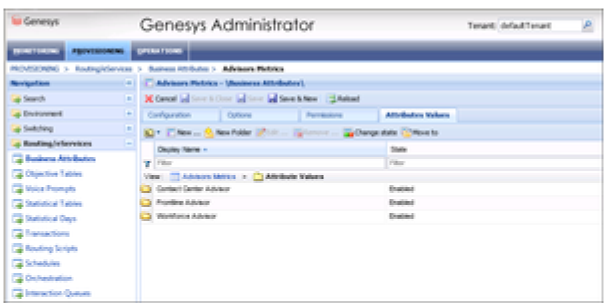
  In this case, user A will be denied access to the metric.
- User A is part of Access Groups X and Y.
  Neither group has defined access to the metric.

  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`

[+] Show CCAdv/WA Privileges

The following Tables list all Contact Center Advisor/Workforce Advisor privileges. The Tables include a description of the consequence to the user if the privilege is present or absent.

The Administration module **Users** page is not controlled by an option; all users who can access the Administration module have access to the **Users** page. However, the Users page no longer displays any information about the user accounts, so there is no need to control access to this page. Please refer to the following documents for more information about configuring user profiles:

- Framework Configuration Manager Help
- Genesys Administrator Extension Help

Advisors Interface

Privilege	Behavior When Present	Behavior When Absent
Advisors.ChangePassword.canView	User sees the Change Password button located at the top of the Advisors interface.	Change Password button is hidden.
		User does not see options to launch the

Privilege	Behavior When Present	Behavior When Absent
NEW Advisors.RMC.canView **NOTE:** Replaces AdvisorsAdministration.RMC.canView starting with Advisors release 8.5.101. For detailed information about configuring users to access RMC in Advisors release 8.5.101 and later, including which permissions to assign, see Configuring RMC Users in the Genesys Configuration Layer.	can access the Resource Management Console (RMC) from the CCAdv dashboard and the WA dashboard.	RMC in either the CCAdv dashboard or the WA dashboard.
NEW Advisors.RMC.ManageAgentSkills.canView Introduced in release 8.5.101. For detailed information about configuring users to access RMC in Advisors release 8.5.101 and later, including which permissions to assign, see Configuring RMC Users in the Genesys Configuration Layer.	When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, the **Manage Skills** pane displays in the RMC window and is active.	When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, there is no **Manage Skills** pane in the RMC window.
NEW Advisors.RMC.ManageAgentStatus.canView Introduced in release 8.5.101. For detailed information about configuring users to access RMC in Advisors release 8.5.101 and later, including which permissions to assign, see Configuring RMC Users in the Genesys Configuration Layer.	When the user opens the RMC window from either the	When the user opens the RMC window from either the CCAdv dashboard or the WA dashboard, there is no **Manage Status** pane in the RMC window.

Privilege	Behavior When Present	Behavior When Absent
	CCAdv dashboard or the WA dashboard, the **Manage Status** pane displays in the RMC window and is active.	

Contact Center Advisor

Privilege	Behavior When Present	Behavior When Absent
ContactCenterAdvisor.ActionManagementReport.canView Introduced in release 8.1.3. **NOTE:** The privilege to grant access to the Action Management Report in Contact Center Advisor or Workforce Advisor is related to the Alert Management privilege. That is, if a user has the ContactCenterAdvisor.ActionManagementReport.canView privilege, then that user should also have the privilege to view Alert Management (AlertManagement.canView).	User can access an Action Management Report by double-clicking on an Alert tile in the Map pane, or by clicking on the arrow for each alert in the	Clicking on the tiles in the Map pane does not launch an Action Management Report, and the Action Management Report arrow for alerts in the Alerts pane is not shown.

Privilege	Behavior When Present	Behavior When Absent
	Alerts pane.	
ContactCenterAdvisor.Dashboard.canView	User can access the CCAdv dashboard. This is a replacement for the module access that was previously assigned on a user-by-user basis.	User cannot access CCAdv dashboard, and the Contact Center Advisor tab is not shown to the user.
ContactCenterAdvisor.Dashboard.AgentGroupsPane.canView	User can see data in the Agent Groups pane.	User sees an empty Agent Groups pane at all times.
ContactCenterAdvisor.Dashboard.ColumnChooser.canView	User has access to the column chooser button on the dashboard.	Column chooser button is not displayed on dashboard.
ContactCenterAdvisor.Dashboard.EnterpriseStats.canView	User can see the Enterprise row	The Enterprise row is not sent from the server to the dashboard, which means the user does not see it.

Privilege	Behavior When Present	Behavior When Absent
	and statistics on the dashboard.	
ContactCenterAdvisor.PerformanceMonitor.canView	User can access Performance Monitor.	User does not see the Performance Monitor button on the dashboard.
ContactCenterAdvisor.PerformanceMonitor.CallFlowPane.canView **NOTE:** If both ContactCenterAdvisor.PerformanceMonitor.CallFlowPane.canView and ContactCenterAdvisor.PerformanceMonitor.CurrentCapacity.canView are excluded from a user's role, then the left side of the Performance Monitor window is not displayed to the user.	User can see the Call Flow pane and metrics in the Performance Monitor window.	The Call Flow pane is shown, but no metrics or values are displayed.
ContactCenterAdvisor.PerformanceMonitor.CurrentCapacity.canView **NOTE:** If both ContactCenterAdvisor.PerformanceMonitor.CallFlowPane.canView and ContactCenterAdvisor.PerformanceMonitor.CurrentCapacity.canView are excluded from a user's role, then the left side of the Performance Monitor window is not displayed to the user.	User can see the Current Capacity pane and metrics in the Performance Monitor window.	The Current Capacity pane is shown, but no metrics or values are displayed.
ContactCenterAdvisor.Dashboard.PivotSelect.canView	User has access to the pivot drop-down list that allows them to switch	Pivot drop-down list is not shown in the top left pane.

Privilege	Behavior When Present	Behavior When Absent
	views of the pivot table.	
ContactCenterAdvisor.AlertManagement.canView **NOTE:** In release 8.1.3, this privilege was replaced with Alert Management–specific privileges.	User has access to the Alert Management tab and the Action Management Report page. User can access the Action Management Report either by clicking on the Alert Management tab, by double-clicking on the alert tiles in the map, or by clicking on the arrow for each alert	The Alert Management tab is not shown; clicking on the tiles in the map does not launch the Action Management Report; and the Action Management Report arrow for alerts in the Alerts pane is not shown.

Privilege	Behavior When Present	Behavior When Absent
	in the Alerts pane.	

Workforce Advisor

Privilege	Behavior When Present	Behavior When Absent
WorkforceAdvisor.ActionManagementReport.canView This privilege is applicable to Release 8.1.3 and later. In a migration scenario, this privilege is not defined in any existing Advisors role in the Configuration Server settings. An administrative user must update existing roles, or create new roles, and add the privilege to allow the described access or activity.	User can access an Action Management Report page by double-clicking on an Alert tile in the Map pane, or by clicking on the arrow for each alert in the Alerts pane.	Clicking on the tiles in the Map pane does not launch an Action Management Report page, and the Action Management Report arrow for alerts does not display in the Alerts pane.
WorkforceAdvisor.Dashboard.AgentGroupsPane.canView Introduced in release 8.1.3.	User can see data in the Agent Groups pane.	User always sees an empty Agent Groups pane with a message stating the lack of access to the Agent Groups pane.
WorkforceAdvisor.Dashboard.canView	User	User cannot access WA dashboard, and

Privilege	Behavior When Present	Behavior When Absent
	can access the WA dashboard.	The Workforce Advisor tab is not shown to the user.
WorkforceAdvisor.Dashboard.ColumnChooser.canView Introduced in release 8.1.3.	User has access to the Column Chooser button on the dashboard.	The Column Chooser button is not displayed on the dashboard.
WorkforceAdvisor.Dashboard.EnterpriseStats.canView Introduced in release 8.1.3.	User can see the Enterprise row in the pivot table (Contact Centers pane).	The Enterprise row does not display in the pivot table (Contact Centers pane).
WorkforceAdvisor.Dashboard.PivotSelect.canView **NOTE:** Because there are additional hierarchies in WA specifically to display agent group contact centers, users must have permission to access the hierarchy grouping (WorkforceAdvisor.Dashboard.PivotSelect.canView) if agent group contact centers are configured. Introduced in release 8.1.3.	User has access to the hierarchy drop-down list on the Contact Centers pane.	The hierarchy drop-down list does not display on the Contact Centers pane.

Alert Management

Privilege	Behavior When Present	Behavior When Absent
AlertManagement.canView	User has	The Alert Management tab does not display for the user.

Privilege	Behavior When Present	Behavior When Absent
Introduced in release 8.1.3.	access to the Alert Management tab.	
AlertManagement.ActionManagementReport.canView Introduced in release 8.1.3.	User can create a new Action Management Report, and update or delete an existing report.	The New and Delete buttons are not displayed in the Action Management Report pane, and the Edit/Delete column is not shown.

Administration Module

Privilege	Behavior When Present	Behavior When Absent
AdvisorsAdministration.canView	User has access to the Administration module.	User cannot access the Administration module, and the module tab is not shown to the user.
AdvisorsAdministration.SystemConfiguration.canView	User can access System Configuration page; option is shown on menu.	System Configuration option is not shown on the Administration menu.
AdvisorsAdministration.Regions.canView	User can access the Regions page;	Regions option is not shown on the Administration menu.

Privilege	Behavior When Present	Behavior When Absent
	option is shown on the Administration menu.	
AdvisorsAdministration.ApplicationGroups.canView	User can access the Application Groups/Thresholds page; option shown on menu.	Application Groups/Thresholds option is not shown on the Administration menu.
AdvisorsAdministration.ContactCenters.canView	User can access the Contact Centers page; option shown on menu.	Contact Centers option is not shown on the Administration menu.
AdvisorsAdministration.ApplicationConfiguration.canView	User can access the Application Configuration page; option shown on menu.	Application Configuration option is not shown on the Administration menu.
AdvisorsAdministration.AgentGroupConfiguration.canView	User can access the Agent Group Configuration page; option shown on	Agent Group Configuration option is not shown on the Administration menu.

Privilege	Behavior When Present	Behavior When Absent
	menu.	
AdvisorsAdministration.ContactGroupConfiguration.canView	User can access the Contact Group Configuration page; option shown on menu.	Contact Group Configuration option is not shown on the Administration menu.
AdvisorsAdministration.Metrics.canView	User can access the Report Metrics page; option shown on menu.	Metrics option is not shown on the Administration menu.
AdvisorsAdministration.MMW.canCreate Introduced in release 8.1.3.	User can create custom metrics.	The Create function and the Copy function do not display in the Metric Manager.
AdvisorsAdministration.MMW.canEdit Introduced in release 8.1.3.	Grants privilege to edit any metrics.	The Edit function does not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.canDelete Introduced in release 8.1.3.	Grants privilege to delete custom metrics.	The Delete function does not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.SourceMetrics.canView	Grants privilege to view the Source Metrics page.	The Source Metrics page, and the link to it in the Administration module, do not display.
AdvisorsAdministration.MMW.SourceMetrics.canCreate	Grants	The `Create Source Metrics` button

Privilege	Behavior When Present	Behavior When Absent
	privilege to create custom source metrics.	does not display on the Source Metrics page.
AdvisorsAdministration.MMW.SourceMetrics.canEdit	Grants privilege to edit source metrics.	The Edit function does not display on the Source Metrics page.
AdvisorsAdministration.MMW.SourceMetrics.canDelete	Grants privilege to delete custom source metrics.	The Delete function does not display on the Source Metrics page.
AdvisorsAdministration.DistributionLists.canView	User can access the Distribution Lists page; option shown on menu.	Distribution Lists option is not shown on the Administration menu.
AdvisorsAdministration.ManualAlerts.canView	User can access the Manual Alerts page; option shown on menu.	Manual Alerts option is not shown on the Administration menu.
AdvisorsAdministration.AlertManagement.AlertCauses.canView	User can access the Alert Causes page; option shown on	Alert Causes option is not shown on the Administration menu.

Privilege	Behavior When Present	Behavior When Absent
	menu.	
AdvisorsAdministration.AlertManagement.KeyActions.canView	User can access the Key Actions page; option shown on menu.	Key Actions option is not shown on the Administration menu.
AdvisorsAdministration.GenesysAdapter.Configuration.canView	User can access the Genesys Adapter Objects Configuration page; option shown on menu.	The Genesys Adapter section (which includes the Object Configuration and Manage Adapters options) is not shown on the Administration menu.
AdvisorsAdministration.RMC.canView **NOTE:** The AdvisorsAdministration.RMC.canView privilege is discontinued starting with Advisors release 8.5.101; Advisors.RMC.canView and AdvisorsAdministration.RMC.Notifications.canView replace it. If your existing Advisors installation includes AdvisorsAdministration.RMC.canView, and you migrate to Advisors release 8.5.101 or higher, the AdvisorsAdministration.RMC.canView privilege remains in your installation, but Advisors ignores it. You must add the Advisors.RMC.canView privilege to provide user access to the RMC and the AdvisorsAdministration.RMC.Notifications.canView privilege to maintain the role-based access control of RMC notification lists and templates in the Administration module.	User can access the Resource Management-related pages in the Administration module which are **Notification Lists** and **Notification Templates**; both options are shown on the Administration module	**Control Panel** section (which includes the **Notification Lists** and **Notification Templates** options) is not shown on the Administration module menu.

Privilege	Behavior When Present	Behavior When Absent
	menu.	
NEW AdvisorsAdministration.RMC.Notifications.canView **NOTE:** Replaces AdvisorsAdministration.RMC.canView starting with Advisors release 8.5.101.	User has access to the following pages in the Administration module: • Notification Templates • Notification Lists User can create a new notification template in the **Resource Management** window and use it once, or save the template to use it again.	The **Control Panel** section does not appear in the Administration module's navigation pane and there are no links to the following pages: • Notification Templates • Notification Lists User can create a template in the **Resource Management** window and use it once; there is no option to save a new template for reuse.
AdvisorsAdministration.PeripheralGateways.canView	User can access the Switches/Peripherals page.	Switches/Peripherals option is not shown on the Administration menu.
AdvisorsAdministration.DeletedObjects.canView	User can see the deleted objects in	Deleted objects in Genesys Administrator are not shown in the corresponding Administration page.

Privilege	Behavior When Present	Behavior When Absent
	Genesys Administrator server in the corresponding Administration pages.	

[+] Show FA Privileges

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 Table lists the privileges available in Configuration Manager for Frontline Advisor. The Table includes a description of the consequence to the user if the privilege is present or absent.

Privilege	Behavior When Present	Behavior When Absent
AdvisorsAdministration.Metrics.canView	User can access the Report Metrics page; option shown on menu.	Report Metrics option is not shown on the Administration menu.
AdvisorsAdministration.MMW.canCreate	User can create custom metrics.	The Create function and the Copy function do not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.canEdit	Grants privilege to edit any metrics.	The Edit function does not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.canDelete	Grants privilege to delete custom metrics.	The Delete function does not display in the Report Metrics Manager.
AdvisorsAdministration.MMW.SourceMetrics.canView	Grants privilege to view the Source Metrics page.	The Source Metrics page, and the link to it in the Administration module, do not display.
AdvisorsAdministration.MMW.SourceMetrics.canCreate	Grants privilege to create custom source metrics.	The `Create Source Metrics` button does not display on the Source Metrics page.
AdvisorsAdministration.MMW.SourceMetrics.canEdit	Grants privilege to edit source metrics.	The Edit function does not display on the Source Metrics page.
AdvisorsAdministration.MMW.SourceMetrics.canDelete	Grants privilege to delete custom source metrics.	The Delete function does not display on the Source Metrics page.
FrontlineAdvisor.SupervisorDashboard.canView	User can access the FA	User cannot access the FA

Privilege	Behavior When Present	Behavior When Absent
	Supervisor Dashboard.	Supervisor dashboard, and the FA Dashboard tab is not shown to the user.
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege*	User can see the Teams pane.	The Teams pane is hidden along with both alerts panes.
FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges*	User can see the Team and Agent Alerts panes.	Neither of the alerts panes is displayed on the dashboard. If access to the Team pane is not available, the Alert pane is not shown even though user has access.
FrontlineAdvisor.SupervisorDashboard.ColumnChooser.canView *Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege*	User can access the column chooser.	The column chooser button on the dashboard is hidden.
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges*	User can sort the entries in the Team pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Team pane. The cursor does not change when hovering over a column header.
FrontlineAdvisor.SupervisorDashboard.TeamAlertsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges*	User can sort the entries in the Team Alerts pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Team Alerts pane. The cursor does not change when hovering over a column header.
FrontlineAdvisor.SupervisorDashboard.AgentAlertsPane.canSort *Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges*	User can sort the entries in the Agent Alerts pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Agent Alerts pane. The cursor does not change when hovering over a column header.
NEW FrontlineAdvisor.SupervisorDashboard.Export.canView	User can see the Print button on the Frontline Advisor dashboard.	The Print button is not displayed on the Frontline Advisor dashboard.
FrontlineAdvisor.Administration.canView	User can access the FA Administration module.	User cannot access the FA Administration module, and the FA Administration tab is not shown to the user.
FrontlineAdvisor.Administration.Settings.canView *Requires the FrontlineAdvisor.Administration.canView*	User can access the Settings tab in the FA Administration module.	Settings tab is not shown to the user.

Privilege	Behavior When Present	Behavior When Absent
privilege		
FrontlineAdvisor.Administration.Hierarchy.canReload *Requires the FrontlineAdvisor.Administration.canView and FrontlineAdvisor.Administration.Settings.canView privileges*	User can initiate a hierarchy reload through the action on the Settings tab.	Hierarchy reload action is not accessible.
FrontlineAdvisor.AgentDashboard.canView	User can access the FA Agent Dashboard.	User cannot access the FA Agent dashboard, and the FA Agent Dashboard tab is not shown to the user.
FrontlineAdvisor.AgentDashboard.AlertsPane.canView *Requires FrontlineAdvisor.AgentDashboard.canView privilege*	User can see the Alerts pane.	The Alerts pane is not displayed.
FrontlineAdvisor.AgentDashboard.ColumnChooser.canView *Requires FrontlineAdvisor.AgentDashboard.canView privilege*	User can see the Column Chooser.	The Column Chooser is not displayed.
NEW FrontlineAdvisor.AgentDashboard.Export.canView	User can see the Print button on the Agent Advisor dashboard.	The Print button is not displayed on the Agent Advisor dashboard.