



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

Performance Management Advisors Deployment Guide

Advisors Roles

12/16/2025

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 8.5.2.

Important

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.

[+] 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?

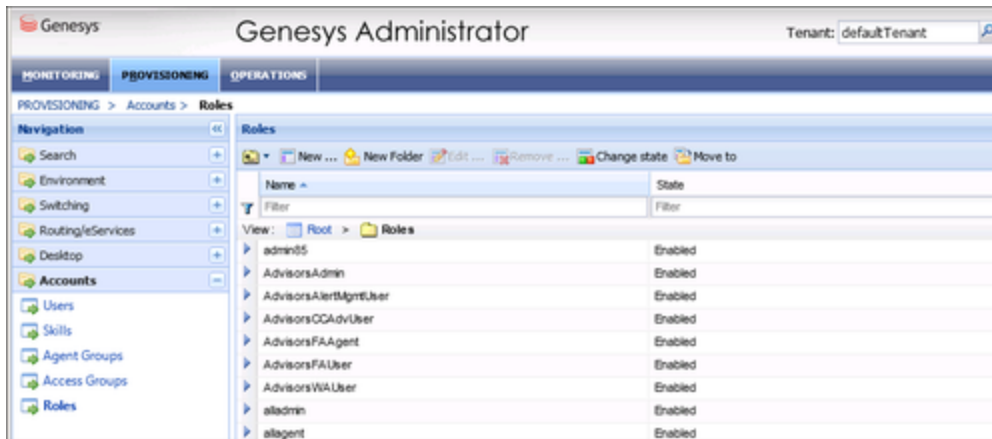
The major component of RBAC is a Role. If it is important in your enterprise to control users' access to information (metrics, hierarchy levels, and business objects), you configure Users and Roles – including the assignment of permissions and privileges to each Role – before any of those users log in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

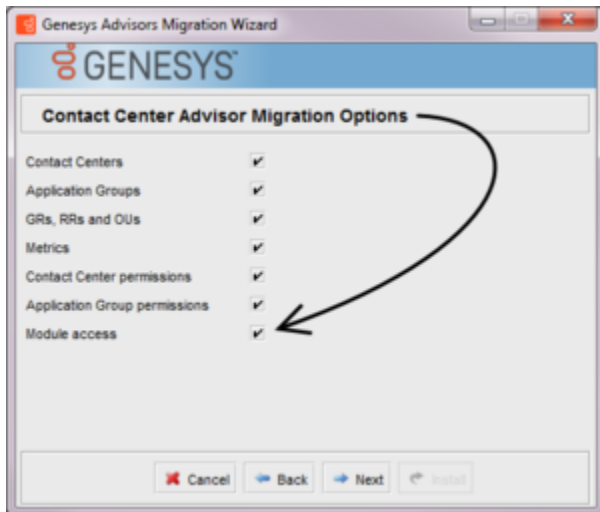
The figure shows an example of Advisors Role configuration.

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 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.

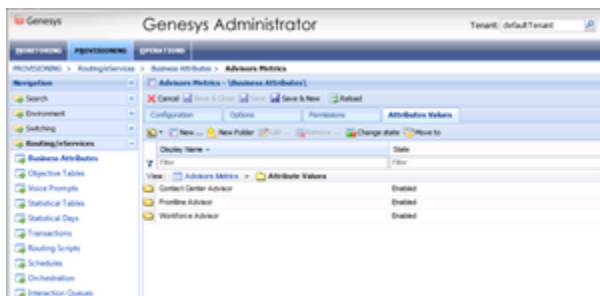
In this case, user A will be denied access to the metric.
- User A is part of Access Groups X and Y.
Neither group has defined access to the metric.

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

[+] Show CCAdv/WA Privileges

You can control access to objects in the Genesys Pulse Advisors Contact Center Advisor (CCAdv) and Workforce Advisor (WA) dashboards and on the Advisors administration module pages using Roles, and associating privileges with each Role. Controlling users' access to data and objects using Roles and associated privileges is called Role-Based Access Control (RBAC).

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

- [Authentication and Authorization](#) — This chapter in the *Genesys Security Deployment Guide* provides information about securing access to systems (in whole or in part) with user authentication and authorization. In particular, see [User Authentication and User Authorization](#), [Object-Based Access Control](#), and [Role-Based Access Control](#).
- [Framework Configuration Manager Help](#) — How to use Genesys Configuration Manager (this is a .zip file)
- [Genesys Administrator Extension Help: Users \(Persons\)](#) — Configuring Users (Persons) in the GAX interface
- [Genesys Administrator Extension Help: Access Groups](#) — Configuring Access Groups in the GAX interface
- [Genesys Administrator Extension Help: Roles](#) — Configuring Roles in the GAX interface
- [Genesys Administrator Extension Help: Configuration Manager](#) — Working with (GAX) Configuration Manager

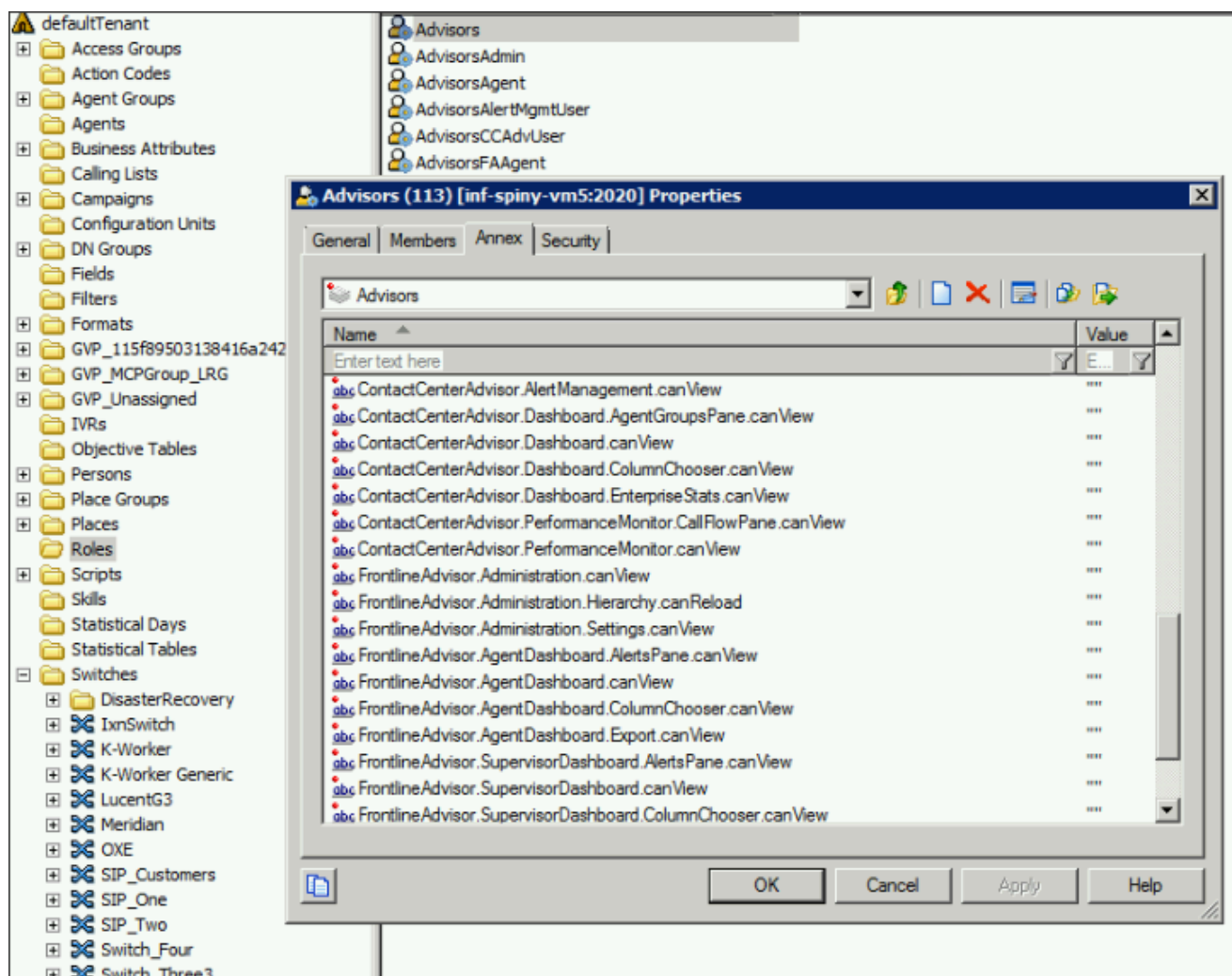
Tip

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.

The following sections provide the lists of available Advisors privileges with which you can secure access to CCAdv, WA, and Advisors administration interface objects:

- Privileges associated with the Advisors Administration module
- Privileges associated with user dashboards
- Privileges associated with Contact Center Advisor
- Privileges associated with Workforce Advisor

The following figure shows a sample of Advisors privileges configuration in Genesys Configuration Manager.



Administration Module

Privilege	Controls Access To:
<p>AdvisorsAdministration.canView</p> <p>* Not specific to Contact Center Advisor/Workforce Advisor. When the privilege is assigned, a Frontline Advisor user has access to the Administration module, as well.</p>	Administration module
AdvisorsAdministration.DeletedObjects.canView	Objects in the Administration module pages that were deleted from the Genesys Administrator server
AdvisorsAdministration.SystemConfiguration.canView	System Configuration page in the Administration module

AdvisorsAdministration.Regions.canView	Regions page in the Administration menu
AdvisorsAdministration.ApplicationGroups.canView	Application Groups/Thresholds page in the Administration module
AdvisorsAdministration.ContactCenters.canView	Contact Centers page in the Administration module
AdvisorsAdministration.ApplicationConfiguration.canView	Application Configuration page in the Administration module
AdvisorsAdministration.AgentGroupConfiguration.canView	Agent Group Configuration page in the Administration module
AdvisorsAdministration.ContactGroupConfiguration.canView	Contact Group Configuration page in the Administration module
AdvisorsAdministration.Metrics.canView	Metric Manager Report Metrics page in the Administration module
AdvisorsAdministration.MMW.canCreate	Create and Copy functions in the Metric Manager, which are used to create custom metrics
AdvisorsAdministration.MMW.canEdit	Edit function in the Report Metrics Manager, which is used to edit all metrics
AdvisorsAdministration.MMW.canDelete	Delete function in the Report Metrics Manager, which is used to delete custom metrics
AdvisorsAdministration.MMW.SourceMetrics.canView	Metric Manager Source Metrics page in the Administration module
AdvisorsAdministration.MMW.SourceMetrics.canCreate	Create Source Metrics button on the Source Metrics page
AdvisorsAdministration.MMW.SourceMetrics.canEdit	Edit function on the Source Metrics page, which is used to edit source metrics
AdvisorsAdministration.MMW.SourceMetrics.canDelete	Delete function on the Source Metrics page, which is used to delete custom source metrics
AdvisorsAdministration.DistributionLists.canView	Distribution Lists page in the Administration module
AdvisorsAdministration.ManualAlerts.canView	Manual Alerts page in the Administration module
AdvisorsAdministration.RMC.Notifications.canView	<p>User has access to the following pages in the Administration module:</p> <ul style="list-style-type: none"> • Notification Templates • Notification Lists <p>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:</p> <ul style="list-style-type: none"> • Notification Templates • Notification Lists <p>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.</p>

Advisors Dashboards

Privilege	Controls Access To:
Advisors.ChangePassword.canView	Change Password function
Advisors.RMC.canView	Resource Management Console (RMC)
Advisors.RMC.ManageAgentSkills.canView	Manage Skills pane in the RMC window
Advisors.RMC.ManageAgentStatus.canView	Manage Status pane in the RMC window

Contact Center Advisor

Privilege	Controls Access To:
ContactCenterAdvisor.Dashboard.canView	Contact Center Advisor dashboard
ContactCenterAdvisor.Dashboard.AgentGroupsPane.canView	Data in the Agent Groups pane
ContactCenterAdvisor.Dashboard.ColumnChooser.canView	Column chooser
ContactCenterAdvisor.Dashboard.EnterpriseStats.canView	The Enterprise row and statistics on the dashboard
ContactCenterAdvisor.Dashboard.PivotSelect.canView	The hierarchy grouping drop-down list on the Contact Centers pane.

Workforce Advisor

Privilege	Controls Access To:
WorkforceAdvisor.Dashboard.AgentGroupsPane.canView	Data in the Agent Groups pane
WorkforceAdvisor.Dashboard.canView	The WA dashboard
WorkforceAdvisor.Dashboard.ColumnChooser.canView	Column Chooser
WorkforceAdvisor.Dashboard.EnterpriseStats.canView	The Enterprise row in the pivot table (Contact Centers pane).
WorkforceAdvisor.Dashboard.PivotSelect.canView	The hierarchy grouping drop-down list on the Contact Centers pane.

NOTE: Because there are additional hierarchies in WA specifically to display agent group contact centers, users must have permission to use the hierarchy grouping drop-down list if agent group contact centers are configured.

[+] 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 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 <i>The FrontlineAdvisor.SupervisorDashboard.canView privilege must also be present</i>	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 <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges</i>	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 <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege</i>	Column Chooser
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canSort <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView and FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView privileges</i>	The data sorting functionality in the Teams pane
FrontlineAdvisor.SupervisorDashboard.TeamAlertsPane.canSort <i>Requires the FrontlineAdvisor.SupervisorDashboard.canView, FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView and FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView privileges</i>	The data sorting functionality in the Alerts pane
FrontlineAdvisor.Administration.canView	Frontline Advisor page in the administration module
FrontlineAdvisor.Administration.Settings.canView <i>Requires the FrontlineAdvisor.Administration.canView privilege</i>	The Settings tab on the FA administration page in the Administration module.
FrontlineAdvisor.Administration.Hierarchy.canReload <i>Requires the FrontlineAdvisor.Administration.canView and FrontlineAdvisor.Administration.Settings.canView privileges</i>	The hierarchy reload action on the Settings tab of the FA administration page in the Administration module.