Contact Center Advisor and Workforce Advisor Help

Role-Based Access and Permissions

5/7/2025

Role-Based Access and Permissions

Access to business objects (regions, contact centers, application groups) and metrics is controlled by roles defined by the administrator (role-based access). When you do not have access to these objects, you cannot see them or work with them in their respective panes on the dashboard. Access to base objects (applications, contact groups, and agent groups) depends on your access to the associated business objects. Therefore, on the dashboard, you can only see objects and metrics (and alerts that contain such metrics) to which the administrator specifically grants access.

Accessing Metrics

When you have access to a metric, you can see it in the following places:

- On the dashboard
- On the Column Chooser
- On the Performance Monitor

You can also graph the metric, see alerts for the metric, and receive alert notifications. (To see alerts and receive notifications, you must have access to the metric, geographic region, contact center, and application group of the alert.)

Accessing Other Objects

Role-based access also controls your ability to see and use the following objects and views in the interface:

- Enterprise row in the Contact Centers pane
- Column Chooser button
- Data in the Agent Group pane
- Grouping drop-down list
- Change Password menu
- Administration module
- Resource Management console (particularly the Access to Notification Lists and Templates section)
- Alert Management module and the data within the module
- Action Management Report page and the data in the page

Accessing the Alert Management Module and Action Management Report Page

Access to the Alert Management module and Action Management Report page is controlled by user roles defined by your administrator (role-based access). If your role does not include permissions to view the Alert Management module or the Action Management Report page, it is not displayed on your dashboard. Functionality within the Alert Management module and Action Management Report page is also controlled by the permissions associated with your role.

On the dashboard, on the Alert Management module, and in the Action Management Report page, access to alerts is controlled by role-based access to metrics and to the entities related to the base objects (geographic region, contact center, and application group) that generate the alerts. You see only those alerts that are based on metrics or related to business objects to which you have role-based access. To see an alert, you must have role-based access to the application group, contact center, and geographic region to which it relates.

Look for the following buttons and columns on your Alert Management module—they are indicators of the permissions associated with your role:

- New button: If present, you can create key action reports.
- Edit/Delete column: If present, you can edit and delete existing key action reports.
- Only the owner of the report can edit or delete a column.

You can see all key action reports with associated alerts to which you have role-based access. If a key action report has three alerts associated with it, you must have access to all of those alerts to access that report. All users can view key action reports which have no associated alerts.

When you assign a key action report, the assignee's permission to the report is checked when you attempt to save it. If the assignee does not have permission to view the report, you receive an error and it does not save until you assign it to someone who has permission to view it.

If the assignee of a key action report is later denied access to view the report because his/her permissions have changed, the following occurs:

- The report is not displayed in the list of key action reports.
- A warning is logged in the log file.
- The Advisors server reassigns the report to the person who created it.