Contact Center Advisor and Workforce Advisor Administrator User's Guide

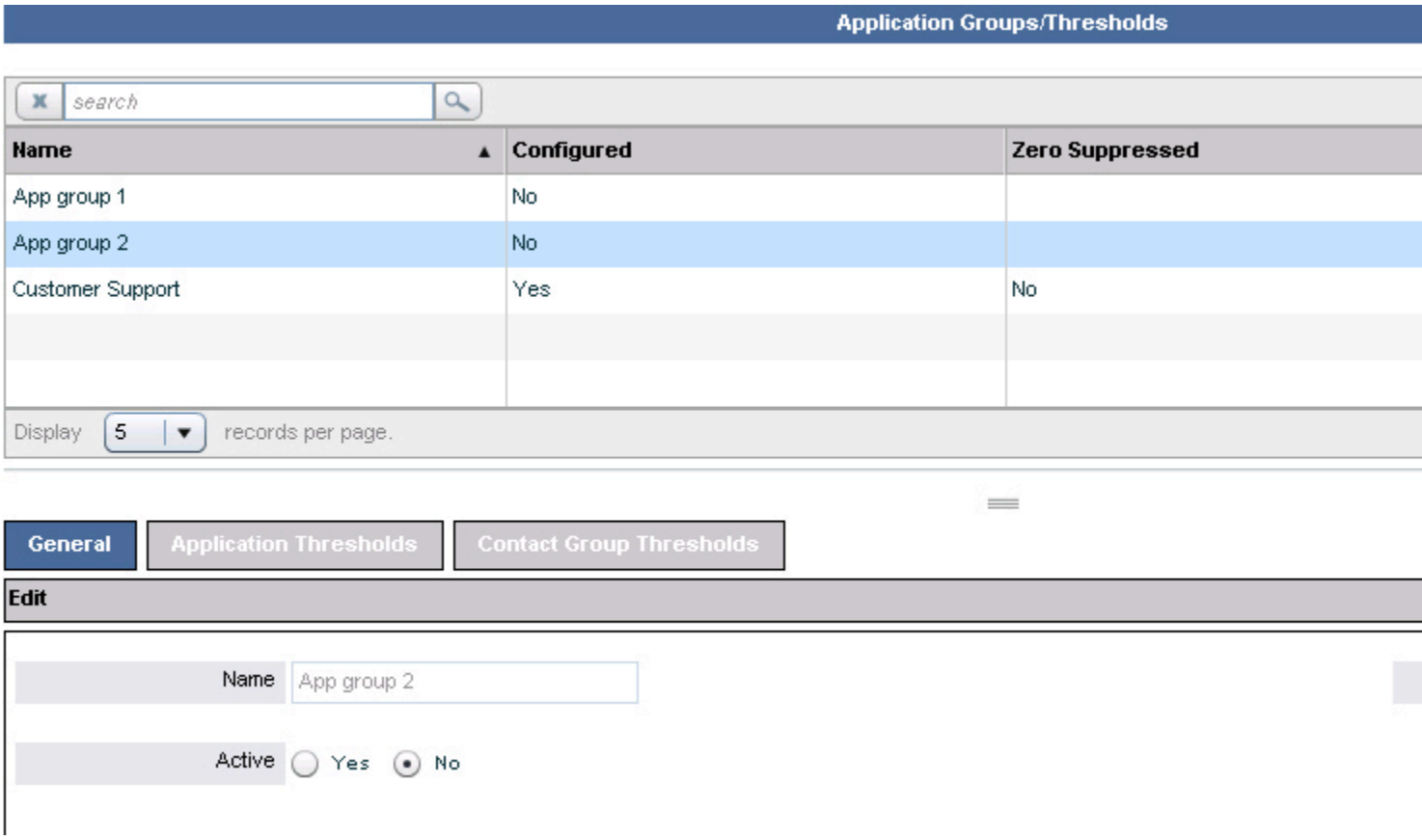
Application Groups and Thresholds

12/16/2025

Contents

Application Groups and Thresholds

This section describes how to configure application groups and thresholds. The following screenshot shows the **Application Groups/Thresholds** page in the Administration module.



Application Groups/Thresholds Page

Adding or Deleting an Application Group

New application groups must be added in Genesys Administrator. Adding and deleting application groups cannot be performed in the Advisors administration module. However, you can make an application group inactive or remove it from the Advisors configuration. To add a new application group in Genesys Administrator, or to delete an application group, see Advisors Business Objects.

Configuring an Application Group's Attributes in Advisors

Use the **General** tab to maintain application groups.

To edit an application group's configuration attributes, select it in the upper panel and edit these details in the **Edit** panel. Alternatively, type the first few letters of its name in the **Search** field, click the icon beside the **Search** field , and then select from the list. When your edits are complete, click **Save**. The **Name** field cannot be edited. This value is configured in Genesys Administrator.

Complete the fields in the **Edit** panel as follows:

- **Active**: Select whether the status of the application group is active or inactive.
  The first time you make an application group active, it becomes part of the Advisors configuration. After this, you can use it to configure applications and contact groups.
  When you change such an application group to inactive, it remains available to use in configuration, and the configurations in which it is used do not change. However, CCAdv and WA do not use the application group when calculating data for the dashboards.
- **Zero Suppressed**: Select Yes for application groups where little or no activity is expected. See Zero Suppression for details.

When you have made the **Edit** panel selections and saved them, the following happens:

- If the application group has been newly created in Genesys Administrator, the **Configured** field changes to Yes to indicate that the configuration is now complete on the Advisors side.
- An `Updated Successfully` message displays at the top of the page.
- The **Remove from Advisors configuration** button is activated.

Removing an Application Group from Advisors Configuration

To remove the application group from the Advisors configuration, click on the **Remove from Advisors Configuration** button. This removal is not synchronized back to Configuration Server.

> ### Important
> Before removing an application group from the Advisors configuration, you must remove its assignment from configured applications, configured contact groups, and distribution lists.

You cannot remove an application group if:

- A metric threshold is defined in the context of the application group.
- An active alert exists created by such a threshold.

Thresholds, Threshold Violations, and Alerts

Thresholds

You can create thresholds on a metric's value to alert users to unacceptable values of that metric.

The thresholds exist in the context of an application group. That is, for base objects related to one application group, the thresholds can be different than for another base object related to a different application group.

A threshold can have two or four values. The complete four values are low critical, low warning, high warning, and high critical. Either the two low thresholds can be empty, or the two high thresholds can be empty.

Threshold Violations

When a metric's value violates a threshold, the background to the metric's cell in the dashboard changes color. When a warning threshold is violated, the color is yellow. Violation of a critical threshold changes the color to red.

These threshold violations appear in the Applications pane of the CCAdv dashboard, and the Contact Groups pane of the WA dashboard.

They also appear in the Contact Centers pane in each dashboard. A violation appearing in the row for a business object in the Contact Centers pane means that an object related to that business object is reporting a threshold violation.

Alerts

A threshold violation escalates to an official *alert* when the metric's value remains above or below a threshold for a specific period of time. The duration to wait before creating an alert is set in the **System Configuration** page.

Alerts appear in the **Alerts** map and the **Alerts** pane in either dashboard, and in the **Alert Management** module.

Thresholds therefore drive alerts. Thresholds should be set carefully and periodically reviewed for tuning requirements. If a threshold is constantly in a violated state, then it is probably set too tight for the current capabilities of the operating environment. If, when an alert is triggered, no action will be taken or, at the least, no immediate value is delivered in knowing about that alert, it might be better to change the threshold or delete its values.

You cannot delete or reset a threshold's values if the threshold is currently causing an active alert. To end the alert and make it inactive, change the threshold's values so that the metric will no longer causes a violation. When the alert ends, and CCAdv or WA has deleted it from the Advisors database, you can reset the threshold or delete its values.

Configuring Thresholds

The **Application Groups/Thresholds** page allows you to:

- Define critical (red) thresholds, warning (yellow) thresholds, and normal conditions for each metric in the context of an application group, using the **Application Thresholds** tab.
- Define critical (red) thresholds, warning (yellow) thresholds, and normal conditions for each metric in the context of an application group, using the **Contact Group Thresholds** tab.

> ### Important
> Only metrics that have the **Threshold** checkbox selected on the **Report Metrics** page display in the **Thresholds** list.

The **Application Thresholds** page and the **Contact Group Thresholds** page display the threshold rule details including:

- **Metric**: Display name of the metric to which the threshold will be applied, when the metric belongs to an object related to the application group
- **Min** and **Max**: Minimum and maximum permissible values for the threshold. Change these in the Report Metrics page.
- **Decimal Places**: The number of decimal places that the metric's value will display. Set this in the Report Metrics page. This does not affect that values you enter for the threshold.
- **Lower-Bound Warning**, **Lower-Bound Critical**, **Upper-Bound Warning**, **Upper-Bound Critical**: The threshold limits for warning and critical violations. See Adding or Updating Thresholds for details.

  > ### Important
  > You cannot delete or reset a threshold's values if the threshold is causing an active alert, or caused an alert that is now expired but has not been deleted from the Advisors database. To end the alert and make it inactive, change the threshold's values so that the metric will no longer causes a violation. When the alert ends, and CCAdv or WA has deleted it from the Advisors database, you can reset the threshold or delete its values.

- **# of Exceptions**: The number of exceptions.

Exceptions

You can add time-based alternative thresholds (that is, exceptions) for the calculation of violations to vary your performance objectives. To do this, see Threshold Exceptions.

System Maintenance of Expired Alerts

Contact Center Advisor XML Generator uses the following process to remove expired alerts from storage for currently active alerts:

- During every processing cycle for the Short time profile group, XML Generator examines threshold violations and alerts. It creates new alerts, updates alerts that existed previously, and ends (expires) alerts that are no longer being caused.
- Every hour on the hour, XML Generator deletes from the storage for current alerts in the Advisors database the alerts that it has set to expired, and also the manual alerts whose end time indicates they are expired.
- The alerts about threshold violations and offline peripherals are retained in storage for historical alerts for display in **Alert Management**.

Workforce Advisor uses the following process to remove expired alerts from the storage for currently active alerts:

- During every processing cycle, WA examines threshold violations and alerts. It creates new alerts, updates alerts that existed previously, and ends (expires) alerts that are no longer being caused.
- After WA has processed all the alerts in this way, it deletes from the storage for current alerts in the Advisors database the alerts that it has set to expired.
- The alerts are retained in storage for historical alerts for display in **Alert Management**.

Alerts and E-Mail Notifications

A threshold violation escalates to an official alert based on persistently remaining above or below the threshold target for a specific period of time. This is set on the **System Configuration** page. Two parameters are important for managing notifications:

- **Alert Creation Delay Interval**: Controls how many minutes a metric's value must exist in a state exceeding a threshold before Advisors creates an alert. Alerts about offline peripherals in Cisco ICM, and manual alerts, are an exception to this rate: they appear immediately.
- **Notification Refresh Rate**: Determines the frequency of sending e-mail messages about alerts. The delay prevents unnecessary repetition of alert messages. Every minute, Contact Center Advisor and Workforce Advisor checks for notifiable alerts and the time an e-mail about the alert was last sent. For each alert, if the time that the e-mail was last sent is older than the notification refresh rate, an e-mail is sent. E-mail about the alert is also sent if the priority of the alert has changed since the last e-mail message about the alert, independent of the refresh rate.

Typically an **Alert Creation Delay Interval** would be in the 10–30 minute range and is entirely dependent upon the urgency and severity of issues.

The **Notification Refresh Rate** may or may not be relevant. Many organizations send an e-mail notification only once. Others with critical performance targets might want to know if an alert is still active and prefer an updated e-mail. While these two configuration settings are very important to the notification function, *how* the root thresholds are set is the most important consideration.

The final variable in the notification process is distribution lists. Careful understanding of the goal(s) of the notification will influence successful use of alert notifications. E-mail notifications should be targeted to users that really need to know about a situation regardless of their location. The users are often responsible for taking the appropriate action to address the situation when time is of the essence.

Distribution lists can be set up to very accurately target the desired audience. The list can be based on the type of alert (business or technical), the severity of the alert (warning or critical), and the contact center and/or the application group related to the application or contact group whose metric value caused the alert. All of these variables allow for targeted e-mail notifications to just the right audience.

Some organizations might prefer to distribute yellow/cautionary alerts to a small group (sometimes one person) that is responsible for the individual business unit or location affected. If the alert hits a red/critical state, the distribution widens to all potentially affected sites, as well as up the management chain.

Distribution lists, like many other aspects of Advisors, will rarely perform well if kept static. The business environment changes; performance targets change; personnel change. Regular and periodic tuning is required to ensure optimal utilization of these and many other Advisors capabilities.

Genesys advises having a documented process that outlines and links the various Advisors capabilities and settings to the broader customer care operating model. A simple example of this would be to document the process flow and impact that the addition of a group of call queues would have on Advisors. Those queues would need to be mapped to an Application Group, and thresholds and notifications would be set.