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.

Contact Center Advisor and Workforce Advisor Administrator User's Guide

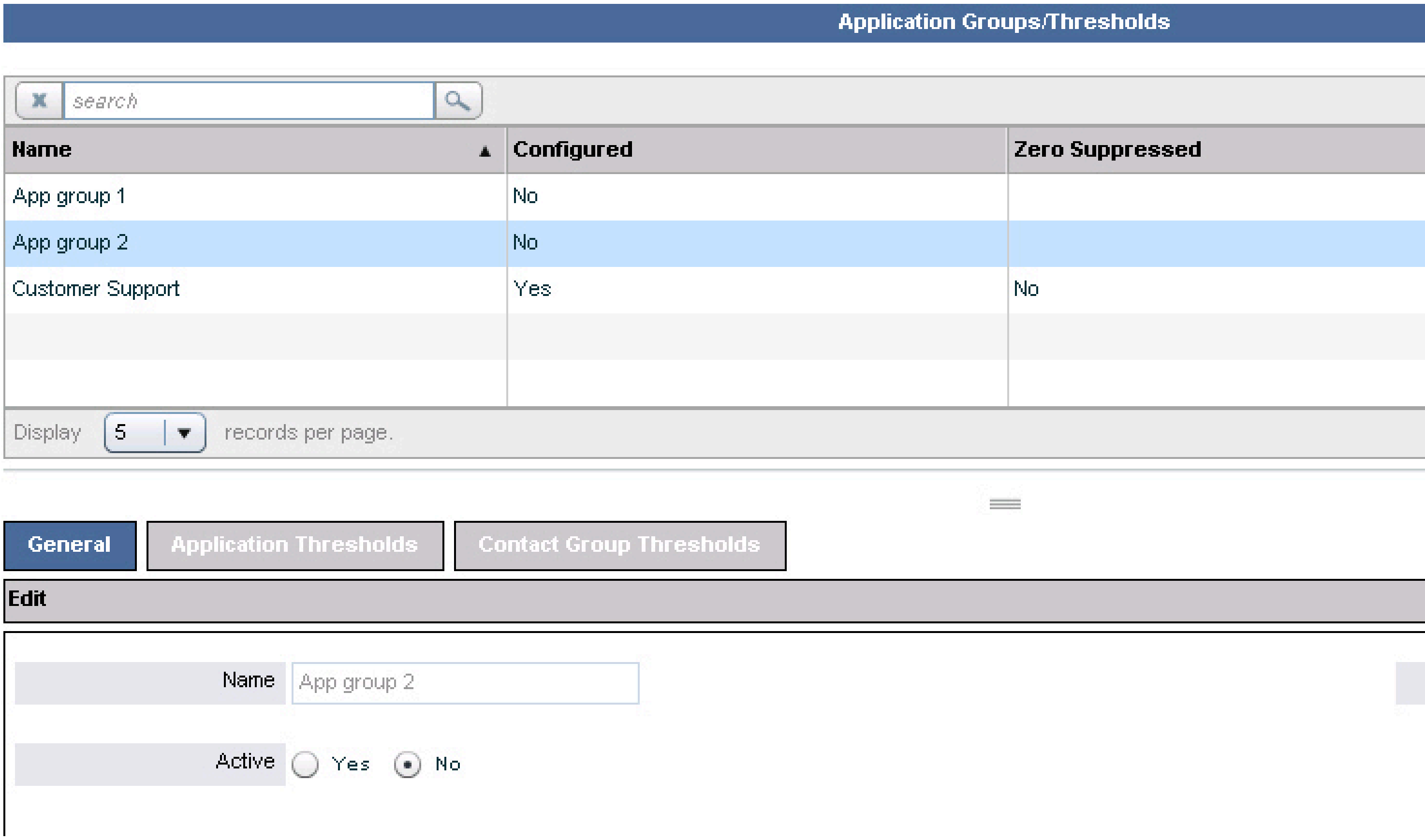
Application Groups and Thresholds

12/15/2025

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.



Name ▲	Configured	Zero Suppressed
App group 1	No	
App group 2	No	
Customer Support	Yes	No

Display 5 ▾ records per page.

Name: App group 2

Active ○ Yes ● No

Application Groups/Thresholds Page

Adding/Deleting a New Application Group in Configuration Manager

New application groups can be added only in Genesys Configuration Manager. Adding and deleting application groups cannot be performed in the Advisors Administration module. However, you can remove the application group from the Advisors configuration. To add a new application group in Configuration Manager, or to delete an application group from Configuration Manager, see Advisors Business Objects.

Configuring an Application Group's Attributes in Advisors

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 Configuration Manager.

Complete the fields in the Edit panel as follows:

- Active: Select whether the status of the application group is active or inactive.
- Zero Suppressed: Select Yes for application groups where little or no activity is expected.

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

- If the application group has been newly created in Configuration Manager, 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 Manager.

> **Important**
>
> Before removing an application group from the Advisors configuration, you must remove its assignment from contact centers and rollups.

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.

Configuring Application Groups and Thresholds

The Application Groups/Thresholds page allows you to:

- Maintain application groups, using the General tab. Application groups provide a meaningful roll up of types of contact center activity in the summary displays.
- Define critical (red), warning (yellow), and normal conditions for each metric in the context of an

application group, using the `Application Thresholds` tab. Only metrics that have the `Threshold` check box selected on the Metric Manager page display in the `Application Thresholds` list. The threshold violations display in the `Applications` pane, and alerts display on the map. A violation appearing in the `Contact Centers` pane means that an application related to that hierarchy object is reporting a threshold violation.

- Define critical (red), warning (yellow) and normal conditions for each metric and contact group, using the `Contact Group Thresholds` tab. Only metrics that have the `Threshold` check box selected on the Metric Manager page display in the `Contact Group Thresholds` list. The threshold violations display in the `Contact Groups` pane, and alerts display on the map. A violation appearing in the `Contact Centers` pane means that a contact group related to that hierarchy object is reporting a threshold violation.

You cannot reset or delete a threshold if it is currently causing an active alert. To end the alert and make it inactive, change the threshold's values so that the metric 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. The Application Thresholds page and the Contact Group Thresholds page display the threshold rule details including:

- `Application Group`: Affected application group name
- `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
- `Decimal Places`: Number of decimal places to which the metric value is defined
- `Lower-Bound Warning`, Lower-Bound Critical: The lower threshold limits for warning and critical violations
- `Upper-Bound Warning`, Upper-Bound Critical: The upper threshold limits for warning and critical violations

> **Tip**
>
> You can define lower bound thresholds, or upper bound thresholds, or both.

- `# of Exceptions`: The number of exceptions

> **Important**
>
> Only metrics that have the Threshold check box selected on the Metric Manager page display in the Thresholds list.

Exceptions

You can add time-based alternative thresholds (that is, exceptions) for the calculation of violations to vary your performance objectives. For instance, you may decide to lower the performance goals for metrics such as service level during the busiest periods of the day rather than increasing staff. Threshold exceptions override the normal (baseline) thresholds and substitute different thresholds for a defined time period. Exception rules can repeat daily, weekly, or monthly.

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 Now time period data, XML Generator examines threshold violations and alerts. For alerts caused by threshold violations, it creates new alerts, updates alerts that existed previously, and ends (expires) alerts that are no longer being caused. For alerts caused by offline peripherals, it does the same.
- 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. For alerts caused by threshold violations, it creates new alerts, updates alerts that existed previously, and ends (expires) alerts that are no longer being caused. After it 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.

Thresholds and 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 parameter settings are important for managing notifications:

- `Threshold Trigger Delay Rate`: This parameter controls how many minutes a threshold violation must exist in a state exceeding a threshold before the application triggers an alert e-mail message and displays on the map. Peripheral alerts (Cisco ICM only) and manual alerts are an exception to the threshold trigger delay rate—they display immediately.
- `Notification Refresh Rate`: This parameter determines the frequency of distributing alert messages. The delay prevents unnecessary repetition of alert messages. Every minute, Advisors 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. Advisors also send e-mail about an alert if its severity changed since the last e-mail about the alert was sent. This is independent of the refresh rate.

Typically a `Threshold Trigger Delay Rate` 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 may 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, it is important to remember that how the root thresholds are set is the most important consideration.

Threshold levels, which drive alerts, 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 may be better to remove it.

The final variable in the notification process is distribution lists. Careful understanding of the goal(s) of the notification will influence successful utilization 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 so time is of the essence.

Distribution lists can be set up to finely 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 finely targeted e-mail notifications to just the right audience.

Some organizations may prefer to distribute yellow/cautionary alerts to a small (sometimes one person) group 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 Advisor, 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 Advisor capabilities.

Genesys advises having a documented process that outlines and links the various Advisor 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 Advisor. Those queues would need to be mapped to an Application Group; thresholds would be set; notifications would be set.