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

Pulse Advisors 8.5.0

1/23/2022

Table of Contents

Genesys Contact Center Advisor and Workforce Advisor Administrator User's Guide

Contact Center Advisor (CCAdv) and Workforce Advisor (WA) provide your company with the capability to view and analyze contact center and workforce management operations using real-time information from a central point of reference. Information business technology and operations personnel can proactively manage both business and technical aspects of the contact center operations and take action to correct problems before they affect business operations.

Contact Center Advisor and Workforce Advisor provide a real-time display of contact center activity and workforce management for contact centers throughout the enterprise. Predefined alerting conditions on applications and contact groups are established to display alerts on the dashboard, as well as notify designated contacts. In Genesys Advisors, applications are queues, calling lists, or interaction queues from Genesys Stat Server, or services or call types from CISCO ICM. Contact groups are activities from Genesys WFM, contact types from IEX TotalView, and forecast groups or staff groups from Aspect eWFM. In addition, Cisco ICM peripherals are monitored and can activate an alert when they go offline.

Alert Management provides the ability to record the action taken to resolve one or more alert violations, as well as the results of that action. Each action is recorded in a separate key action report. The key action reports create a knowledge base that helps identify repetitive patterns and resolve future violations more rapidly.

With Resource Management you can change the skills, skill levels, status and call-routing behavior of agents, as well as notify the affected parties of the actions by e-mail. Changes are published to Genesys operational systems so that they have immediate impact on contact center operations.

The *Contact Center Advisor and Workforce Advisor Administrator User's Guide* is primarily intended for system administration-level users of the Contact Center Advisor and Workforce Advisor modules. This document focuses on using the features and functions of the System Administration module. In particular, it is a reference for system administrators responsible for configuring Contact Center Advisor and Workforce Advisor, including configuring applications and contact groups.

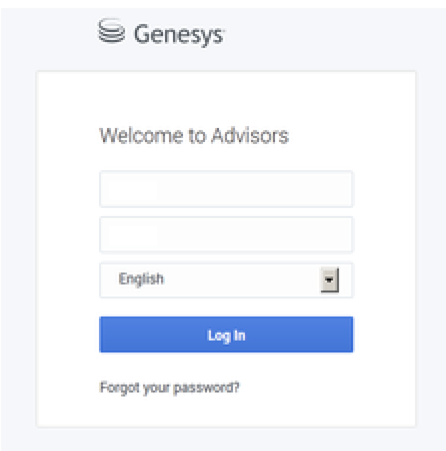
Accessing Genesys Performance Management Advisors

NEW Prior to Genesys Performance Management Advisors release 8.5.0, you accessed Advisors modules using the Genesys Advisors browser. Starting in release 8.5.0, there is no longer a standalone Advisors browser. Advisors modules run in a standard, commercially-available browser. See the Genesys Supported Operating Environment Reference Guide for information about supported browsers in which you can use the Advisors modules.

NEW Contact Center Advisor and Workforce Advisor must be connected to the Genesys environment to function; it is not strictly necessary for the Advisors servers to have Internet access.

<tabber>

About=



You open the Advisors login page in a supported browser. If you do not have the correct URL to open the Advisors login page, see your system administrator.

The Advisors login page is shown at left; click the image to view it full-size.

Permissions for your user account are loaded when you log in. If you log in to Advisors, and a new object is added to Genesys Configuration Server, it is not added to your view until you log out and log in again (that is, if you have the necessary security permissions to view the object). Similarly, to see objects that were activated in Advisors after you logged on, you must log out and log in again.

|-| How To ...=

Log in to and out of the Advisors interface

1. Open a supported browser.
   See the Genesys Supported Operating Environment Reference Guide for information about supported browsers in which you can run the Advisors modules.
2. Enter the Advisors URL provided by your system administrator in the browser address bar.
   If you do not have the correct URL to open the Advisors login page, see your system administrator.
3. Type a user name and password.
4. Select the language of your choice from the dropdown menu.
   The available language options are dependent on your release of Advisors. For information about which languages are supported in your release of Advisors, see the Advisors Read Me or the Advisors Release Notes.
5. Click the **Log In** button.
   The Advisors interface displays.
6. To exit the Advisors interface:
   a. Click the **Log Out** button. If you have more than one Advisors module open in your browser, clicking the Log out button on any one module ends the session for all open modules. Genesys recommends that you log out of the Advisors modules before closing the browser.
   b. Click the browser **Close** button.

Navigate to Advisors modules

1. Log in to the Advisors interface.
2. To select an Advisors module, click the icon and select a module from the dropdown list.
   Only modules to which you have access permissions are available for selection in the dropdown list.
3. To open another Advisors module without closing the module you are using, right-click a module name in the drop-down list under the icon and select

an option to open the module (open in a new tab or open in a new window).

Navigate to an accessible dashboard

1. Log in to the Advisors interface.
2. To open the accessible dashboard, click the icon and select the accessible dashboard option from the drop-down list.

Get Help information for a dashboard

1. Log in to the Advisors interface.
2. Open this document by clicking the ? icon while the Advisors Administration module is the active (selected) module.
3. Open Help information for a specific dashboard by clicking the ? icon while the dashboard is selected. For example, to get Help information specific to the Contact Center Advisor (CCAdv) dashboard, ensure the CCAdv dashboard is selected and in view, and then click the ? icon on the Advisors interface.

Request a new password

1. On the Advisors login page, click **Forgot your password?**
   The ability to request a new password is determined by an installation parameter– this option might be unavailable in your Advisors interface.
2. Enter your user name and e-mail address in the **Forgot password?** window.
3. Click **Submit**.
   A new password is sent to your e-mail address.

Change a password

1. Log in to the Advisors interface.
2. Click the icon on the Advisors interface.
3. Select **Change Password** from the dropdown menu.
   The ability to change your password is determined by an installation parameter – this option might be unavailable in your Advisors interface.
   If your enterprise uses LDAP, you must use your corporate tools to change your LDAP password.
4. Enter your old password, then your new password.
5. To confirm, re-enter your new password.
6. To save, click **Submit**.
   If Advisors rejects your new password, you receive an error message. The error message is generic; it does not indicate the cause of the failure. If Advisors rejects your new password request, update the password and submit the request again. You cannot reuse a password. A space character at the end of a password is not allowed.

Configuration Modes

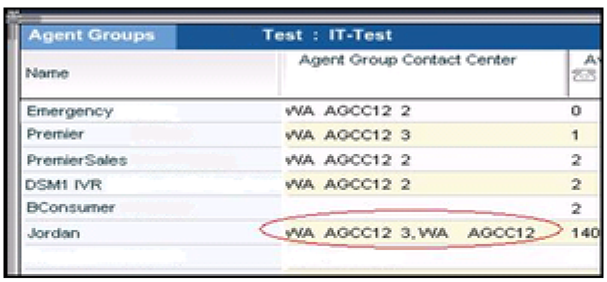
You can choose between two Contact Center Advisor/Workforce Advisor configuration modes:

- Integrated CCAdv/WA configuration mode
- Independent CCAdv/WA configuration mode

The default mode is integrated configuration mode.

The choice of the mode determines all further configuration processes, what data is stored, and how the configuration data is interpreted and used inside the application.

You can select the mode at any time on the System Configuration page (`Integrated CCAdv/WA configuration = Yes` or `No`). A change to the parameter has an immediate impact on the application. Both manual and bulk configuration options consider the configuration mode. For more information on bulk configuration, see *Genesys Performance Management Advisors Deployment Guide*.



Multiple AGCC to AG mapping

With the introduction of the configuration modes, you can map an agent group to multiple agent group contact centers (AGCC) that are under the same network contact center (NCC).

In this topic, the following terminology is used:

- *Configured application* is an application mapped to a contact center, an application group, a region, and/or an operating unit.
- *Configured contact group* is a contact group mapped to a contact center, an application group, a region, and/or an operating unit.

<tabber>

Integrated CCAdv/WA Configuration Mode=

Earlier releases of the Advisors application included integrated, or dependent, configuration between Contact Center Advisor and Workforce Advisor. Starting in release 8.1.5, to select integrated mode for CCAdv/WA, set the `Integrated CCAdv/WA configuration` parameter to `Yes`. The integrated configuration mode makes WA dependent on the CCAdv configuration structure.

After switching to integrated mode, the application applies the following rules automatically:

1.

CCAdv applications mapped to WA contact groups contribute to contact group metrics only if they are included in the CCAdv rollup and these applications are mapped to the same aggregation objects as the associated contact groups (that is, contact centers, application groups, reporting regions, and operating units).

2. An agent group assigned to an application is automatically included (enabled) in the CCAdv rollup when you assign this agent group to an application mapped to a contact center and an application group.
3. Agent group-to-application relationships are automatically propagated to contact groups associated with these applications if the applications have properties described in 1 above.
4. An agent group assigned to an agent group contact center (AGCC) is automatically included (enabled) in the CCAdv rollup – under the network contact center (NCC) associated with that AGCC – when you assign this agent group to an application mapped to the NCC and the `Include in CCAdv Rollup` property for this agent group is set to `Yes`. If mapped to a contact group, such an agent group contributes to the related contact group metrics and becomes visible on the dashboard only when it is mapped to an application that has properties described in 1 above.

If you map at least one contact group to a contact center, application group, and region (or operating unit), the dashboard view is generated and the forecast metrics display.

In the integrated mode, only configured applications mapped to the same contact center, application group, and regions appear as available for mapping to a contact group.

There are two new agent group properties:

- `Include in CCAdv`
- `Include in WA`

Both `Include in CCAdv` and `Include in WA` properties have a default setting of `Yes` in integrated mode. In the integrated mode, setting `Include in WA` to `Yes` makes an agent group – agent group G, for example – available for mapping to a contact group – contact group C, for example – when:

- C is mapped to the same AGCC as G.
- There is a parent contact group – P – mapped to a configured application where the application is associated with the agent group G and where P is mapped to the parent NCC and the same application group and regions as C.

|-| Independent CCAdv/WA Configuration Mode=

To select the independent CCAdv/WA configuration mode, set the `Integrated CCAdv/WA configuration` parameter to `No`. In this configuration mode, WA operates independently from the CCAdv configuration structure.

After switching to independent mode, the application applies the following rules automatically:

1. All applications that are published, and not yet mapped to other contact groups, can be mapped to configured WA contact groups. Once mapped to configured contact groups, the applications contribute to real-time metrics for the contact groups. Contact groups that are not mapped to applications do not have real-time metric data; for example, Actual AHT, Actual SL%, and so on.
2. You can manually assign any agent group to a configured WA contact group mapped to a network contact center (NCC).
3. Any agent group that is assigned to an agent group contact center (AGCC), and that has the `Include in WA Rollup` property set to `Yes`, can be mapped to configured WA contact groups that are also

assigned to that AGCC.

4. An agent group can be mapped to multiple configured WA contact groups.
5. You can edit the `Include in CCAdv` and `Include in WA` agent group rollup properties. Agent groups appear on the CCAdv and WA dashboard views only if the corresponding `Include in Rollup` parameter is set to `Yes`.

The `Include in CCAdv` and `Include in WA` agent group rollup properties control AGCC visibility in the independent CCAdv/WA configuration mode. The properties are applicable only to agent groups mapped to an AGCC.

When you set the `Include in CCAdv` rollup property to `Y` for an agent group, and that agent group is mapped to an AGCC, then the agent group and the AGCC are automatically enabled for CCAdv when you map the agent group to a configured application(s) that belongs to the associated NCC parent.

Changing the `Include in CCAdv` rollup value from `N` to `Y` automatically enables all AGCCs – and agent groups under this AGCC – if the agent groups are already mapped to a configured application(s) that belongs to the associated NCC parent.

If the `Include in CCAdv` rollup property is set to `N` for an agent group, that agent group does not appear in CCAdv configuration. An AGCC does not appear in CCAdv configuration if none of the agent groups mapped to it have the `Include in CCAdv` rollup property set to `Y`. If you do not want an AGCC used for WA to be visible on the CCAdv dashboard, then ensure you set the `Include in CCAdv` rollup property to `N` for all agent groups assigned to the AGCC.

Advisors Business Objects

Role-based access to business objects and metrics is configured in the Genesys Configuration Manager. To be able to fully complete the configuration of an Advisors installation and perform administrative functions, you must have access to the Configuration Manager.

Advisors business objects are created and related to access groups or persons in the Configuration Manager.

These objects are then synchronized with the Advisors database, and the administrator can then configure the remaining information for each object along with the necessary relationships by using the Advisors Administration module.

Advisors metrics are related to access groups or persons in the Configuration Manager.

Business objects and metrics can be made active or inactive in the Administration module.

These items are not represented as standard objects in Configuration Manager. The business attribute values contain just the ID and name of the object. You can enter a description for a business attribute in the Configuration Manager, but Advisors does not import it into the Advisors database, or use the description in any other way.

Business Objects

Business objects (reporting regions, geographic regions, operating units, contact centers and application groups) are:

1. Created initially in the Genesys Configuration Manager under a single tenant as business attributes.
2. Related to access groups or persons to assign permissions to see them.
3. Synchronized with the Platform database.
4. Subsequently configured to completion in the Advisors Administration module.
5. Deleted only in the Configuration Manager (although they can be removed from Advisors without deleting them from the Configuration Manager).

The Genesys Configuration Manager database is the master record holder for these Advisors business objects. Consequently, all create and delete functions are performed in the Genesys Configuration Manager.

Agent-group contact centers are not configured in the Configuration Manager. They are added as children of network contact centers during network contact center configuration on the Advisors side. All users that have permissions to see network contact centers are allowed to see the whole set of the related agent-group contact center.

Metrics

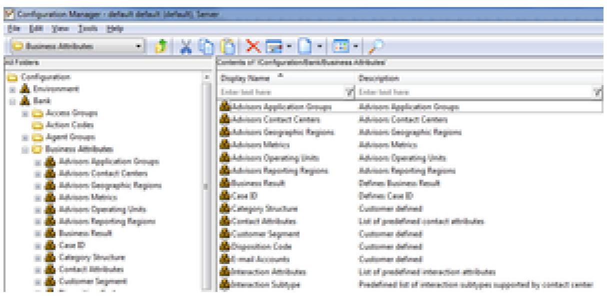
Metrics are created in the Platform database when you install Advisors. Then they are configured in the Advisors Administration module.

You use Configuration Manager to assign permissions to access groups and to persons to determine whether the users can see the metrics in the Administration module and in the dashboards.

Deleting a metric from the Configuration Manager does not delete it from Advisors, but does hide it in any functionality that would otherwise show it.

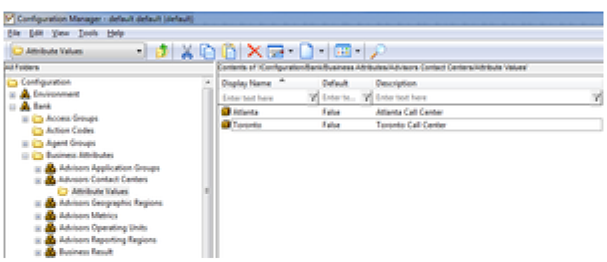
Examples

The following screenshot shows the Advisors business attributes in Configuration Manager.



Configuration Manager Business Attributes

Under each Configuration Manager business attribute, there is a folder that contains the list of attribute values. These attribute values represent the individual objects for this object type. For example, if there are two contact centers (Atlanta and Toronto) being configured in CCAdv, the Configuration Manager metadata would look as follows:



Configuration Manager Business Attributes—Individual Objects

Users

Users are configured entirely in the Configuration Manager. There is no user configuration functionality in the Advisors Administration module.

Region Types

A region represents a subdivision of the business operations of your company within each of the following views:

- Geographic is based on the physical location of the contact center. The applications and contact groups within a contact center fall under only one geographic region.
- Reporting Region is management-based. Applications and contact groups within a contact center may fall within multiple reporting regions.
- Operating Unit is based on the defined groupings of your company that are summarized and displayed on the Operating Unit view. Applications and contact groups within a contact center may fall within multiple operating units.

Filters

The master list of filters for Advisors (for CCAdv, WA, or FA) comes from the Configuration Server. `Advisors Filters` are part of the Advisors `Business Attributes` section of the Configuration Manager (see the following screenshot).

Advisors Filters business attribute in Configuration Manager

The Advisors Filters business attribute must exist on one – and only one – tenant. Genesys recommends you configure the Advisors Filters business attribute on a tenant that is the default tenant for the Advisors suite installation, on which you configure all Advisors metadata. If there are Advisors Filters business attributes configured on multiple tenants, you receive an error message on the Genesys Adapter installation and the filters are not loaded.

If filters are associated with configured objects on the `Base Object Configuration` page in the Administration module, the filter and object combination is stored on the `Annex` tab of the object's `Properties` window.

Creating an Advisors Object as a Business Attribute in Configuration Manager

When creating an Advisors object as a business attribute value in Configuration Manager, the following fields are required. `Name` and `Tenant` are mandatory for completing the new object in Configuration Manager.

- `Name`: For business objects, the `Name` is the name of the object. It becomes the name of the object in Advisors.
  For metrics, this field is a concatenation of [Application].[ObjectType].[Channel].[Name]. For more information, see Creating Metrics. This name is not the metric's display name in Advisors. Enter a metric's display names in the Advisors Administration Metric Manager page.

> **Warning**
> Once an object/business attribute value is created, the `Name` field cannot be changed.

- `Tenant`: The tenant to which this Advisors object belongs. You choose the Tenant when installing Advisors Platform, and cannot change it in Configuration Manager.
- `Display Name`: The name of the object to display in the Configuration Manager. Advisors does not use this display name.
- `Description`: A simple description of this object. For a filter, enter the filter expression in the `Description` field. For any other object other than a filter, Advisors does not use this description.

Required Permissions

To create a business attribute, you must have `Create` permission with respect to the business attribute folder or sub-folder in which the object will reside. `Create` permissions are configured for you by a super administrator.

Deleting an Advisors Object from Configuration Manager

Genesys recommends that you do not delete Advisors objects from Configuration Manager until all their interdependencies and relationships in the Advisors configuration have been correctly processed. That is, do not delete Advisors objects before removing the rollup associations to regions, application groups, contact centers, contact groups and agent groups.

Required Permissions

To delete a business attribute, you must have `Delete` permission with respect to the business attribute folder or sub-folder in which the object resides.

Synchronization of Business Objects

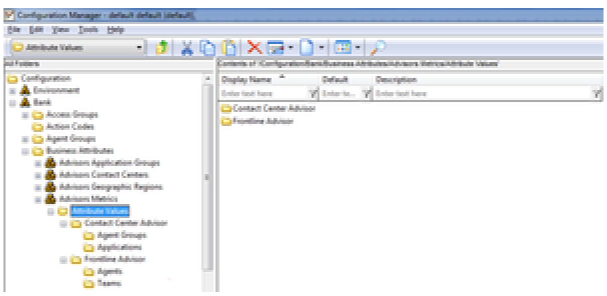
When a new business object is created in the Configuration Manager and saved, Advisors automatically propagates it to the Advisors Platform database. It appears in the Administration module marked as not configured and inactive. Its remaining attributes must be configured in the Advisors Administration module.

Once this is complete, the object is available and can be used in Advisors.

Changes made in the Administration module are not stored in the Configuration Manager.

Creating Metrics

Metrics are handled differently from other Advisors business objects. Because metrics for CCAdv, WA and FA are stored under the `Advisors Metrics` business attribute, a folder structure has been created to segment the metrics for each application and for each object. See the following screenshot.



Configuration Manager Metrics Attributes

Each application’s metrics are created under the appropriate folder, and are subdivided by the object types they are associated with. For example, there could be an AHT for applications and an AHT for agent groups in CCAdv. There would then be an AHT business attribute value under Contact Center Advisor/Applications and another one under Contact Center Advisor/Agent Groups. This allows the control over which users have access to specific metrics at a very granular level; a user could be given access to the AHT metric for applications but not for agent groups.

To avoid confusion over similarly named metrics, and because Configuration Manager does not allow duplicated names for attribute values, the names of the metrics are name-spaced and case sensitive. The format of the name-space is: [Application].[ObjectType].[Channel].[Name] where:

- [Application] —Can be FrontlineAdvisor, WorkforceAdvisor, or ContactCenterAdvisor.
- [ObjectType] —Represents the object type associated with this metric. This could be AgentGroup, Agent, Contact Group, Application, or Team.
- [Channel] —Can be Email, WebChat, Voice, All or AllNonVoice.
- [Name] —The name of the metric.

For example, the AHT for agent groups in CCAdv would have the following name: ContactCenterAdvisor.AgentGroup.Voice.AHT An FA metric could have the following name:

FrontlineAdvisor.Agent.Voice.nch_1 FrontlineAdvisor.Team.Voice.taht_2

An anomaly are the metrics in the folder Contact Center Advisor/Agent Groups. The [Application] component of the names of these metrics is ContactCenterAdvisor. These metrics are displayed in Contact Center Advisor, and some of them are also displayed in Workforce Advisor. WA chooses the subset of them it displays; you cannot control this. Thus, changes you make to these metrics affect CCAdv and may also affect WA.

CCAdv/WA Access Privileges

You can control access to information in the Genesys Contact Center Advisor/Workforce Advisor (CCAdv/WA) dashboards and on the CCAdv/WA administration page 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).

<tabber>

|-| 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, use Genesys' RBAC to configure access to the Administration module for a specific subset of managers.

Advisors use Configuration Manager business attributes, which means Advisors 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 them access to a piece of functionality, that functionality is not displayed to the 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 tune 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)

> **Tip**
> In Advisors release 8.1.1, three special access groups were introduced to represent the three different types of users in Advisors (Super Administrator, Partition Administrator and Dashboard User). Starting in release 8.1.2, these access groups are no longer required. Unless they are used to actively manage object permissions, they can be removed from the Configuration Manager.

What are RBAC roles?

The major component of RBAC is a role. 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.

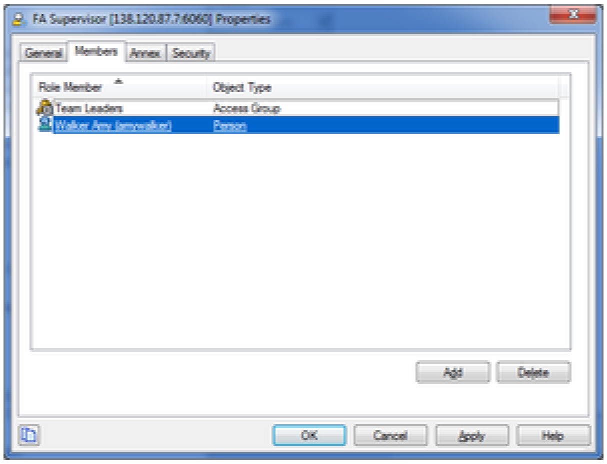
Roles can also be used to protect access to entities that are not configured as configuration objects, such as logs. In general, when determining the accessibility to an object by a user, the user session cannot retrieve objects if they are not among those objects to which the user has access (as defined 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. This assignment is done on the **Members** tab of the role.

Important

To inherit permissions, access groups and users must belong to the tenant specified in the Advisors Platform installer.



Assigning Roles to Users and Access Groups

In the screenshot to the right, the role `FA Supervisor` has been assigned to:

- The `TeamLeaders` access group
- User `Amy Walker`

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 in the **Security** tab to be able to access the role.

Important

Names of access groups must not contain spaces.

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 privileges.

Default Roles Created by Migration

Module access is no longer determined by entries in a user's **Annex** tab. Instead, module access is determined by the roles associated with the user's profile. An optional section of the migration utility provided in the software distribution package creates this new module access schema.

Seven default roles are created by the utility in the Configuration Manager, with each one representing access to a particular module. Each role has a limited set of privileges associated with it. The default roles are:

- AdvisorsAdmin
- AdvisorsFAUser
- AdvisorsFAAdmin
- AdvisorsFAAgent
- AdvisorsCCAdvUser
- AdvisorsWAUser
- 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 8.1 Security Deployment Guide
- Framework 8.1 Genesys Administrator Deployment Guide
- Framework 8.1 Configuration Manager Help
- Genesys Administrator 8.1 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. Role privileges are defined 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, normally a System Administrator, bundles these tasks into roles. These 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. Privileges for each role are stored as key-value pairs in the **Annex** tab of that role in Genesys Configuration Manager. If a privilege is present in a role, then any users assigned that role have access to the functionality controlled by that privilege. The value for the privilege key can be left blank.

Where do I configure roles, permissions, and privileges?

You must have access to the Genesys Configuration Manager to complete the configuration of an Advisors installation and perform administrative functions. Roles are defined, maintained, and associated with users in the Genesys Configuration Server using the Configuration Manager.

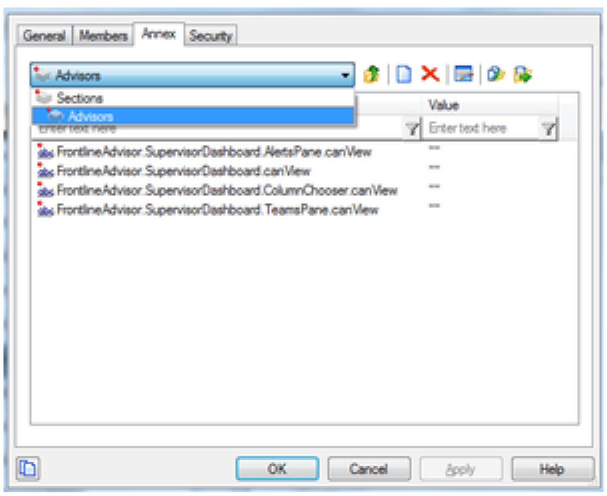
Typically, you configure RBAC in Configuration Manager in the following order:

1. Add roles.
2. Add tasks to roles.
3. Assign Access Groups to Business Attribute instances.
4. Assign users to roles.

Add users to a role on the **Members** tab of the properties dialog box for that role. Add users with one of the following methods:

- indirectly, as a member of an Access Group
- directly, as a member of a role

Assign permissions for a role on the **Security** tab of the properties dialog box for that role. A user must have Read access to the role (either directly or through an Access Group) to which he is assigned.



Annex tab for FA Supervisor role in Configuration Manager

Privileges for each role are stored as key-value pairs in the **Annex** tab of the properties dialog box for each role in Genesys Configuration Manager. The screenshot to the left shows the **Annex** tab of a new role called `FA Supervisor` – a user who can view the **Agent Alerts** pane on the FA dashboard.

The privileges for Advisors are bundled under a single section in the **Annex** tab with the title `Advisors`. Each privilege name uses the following general structure:

[application name].[module name].[task grouping].[privilege name]

> **Important**
> 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. In the preceding example, all three privileges shown in the screenshot above are required so the user can view the Agent Alerts pane. See the list of privileges in the Privileges tab on this page for more information.

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 Manager
- the number of access groups or users that can be present in the Configuration Manager
- 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 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.

|-| CCAdv/WA Privileges=

The following Tables list all Contact Center Advisor/Workforce Advisor privileges available in Configuration Manager. 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 8.1 Configuration Manager Help
- Genesys Administrator 8.1 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.

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	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
	pane, or by clicking on the arrow for each alert in the 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 is not displayed on dashboard.

Privilege	Behavior When Present	Behavior When Absent
	column chooser button on the dashboard.	
ContactCenterAdvisor.Dashboard.EnterpriseStats.canView	User can see the Enterprise row and statistics on the dashboard.	The Enterprise row is not sent from the server to the dashboard, which means the user does not see it.
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	Pivot drop-down list is not shown in the

Privilege	Behavior When Present	Behavior When Absent
	has access to the pivot drop-down list that allows them to switch views of the pivot table.	top left pane.
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	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
	tiles in the map, or by clicking on the arrow for each alert 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	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.

Privilege	Behavior When Present	Behavior When Absent
	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 can access the WA dashboard.	User cannot access WA dashboard, and 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 hierarchy drop-down list does not display on the Contact Centers pane.

Privilege	Behavior When Present	Behavior When Absent
	the Contact Centers pane.	

Alert Management

Privilege	Behavior When Present	Behavior When Absent
AlertManagement.canView Introduced in release 8.1.3.	User has access to the Alert Management tab.	The Alert Management tab does not display for the user.
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	System Configuration option is not shown on the Administration menu.

Privilege	Behavior When Present	Behavior When Absent
	page; option is shown on menu.	
AdvisorsAdministration.Regions.canView	User can access the Regions page; option is shown on the Administration menu.	Regions option is not 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	Application Configuration option is not shown on the Administration menu.

Privilege	Behavior When Present	Behavior When Absent
	menu.	
AdvisorsAdministration.AgentGroupConfiguration.canView	User can access the Agent Group Configuration page; option shown on menu.	Agent Group Configuration option is not shown on the Administration 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	The Delete function does not display in the Report Metrics Manager.

Privilege	Behavior When Present	Behavior When Absent
	custom metrics.	
NEW 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.
NEW AdvisorsAdministration.MMW.SourceMetrics.canCreate	Grants privilege to create custom source metrics.	The `Create Source Metrics` button does not display on the Source Metrics page.
NEW AdvisorsAdministration.MMW.SourceMetrics.canEdit	Grants privilege to edit source metrics.	The Edit function does not display on the Source Metrics page.
NEW 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	Manual Alerts option is not shown on the Administration menu.

Privilege	Behavior When Present	Behavior When Absent
	menu.	
AdvisorsAdministration.AlertManagement.AlertCauses.canView	User can access the Alert Causes page; option shown on menu.	Alert Causes option is not shown on the Administration 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	User can access the Resource Management-related pages, which are Notification Lists and Notification Templates; both	Control Panel section (which includes the Notification Lists and Notification Templates options) is not shown on the Administration menu.

Privilege	Behavior When Present	Behavior When Absent
	options shown on menu.	
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 Configuration Manager server in the corresponding Administration pages.	Deleted objects in Configuration Server are not shown in the corresponding Administration page.

Objects in the Administration Module

Before you configure relationships, it is important to note that there are some dependencies that affect your ability to configure data in the Administration module:

- Review the *Performance Management Advisors 8.5.0 Deployment Guide* to ensure you have completed all deployment requirements. Also review the Post Installation Configuration topics in that book.
- Run Contact Center Advisor XML Generator to pull from the external data source systems the base objects you will configure in the Administration module. Until you do this, no switches/peripherals, applications, or agent groups will appear in the user interface.
- Run Workforce Advisor server to pull from the external WFM systems the contact groups you will configure in the Administration module. If you are using IEX TotalView, then use FTP as detailed elsewhere to push its contact groups into the Advisors Platform database. Until you do this, no contact groups will appear in the user interface.

Overview of Administration Module

Menu options for the Administration module are controlled by role-based access set up in the Configuration Manager. Administrators will see only menu items for which they have privileges assigned.

To display metrics' values on dashboards, multiple procedures must be completed and base objects must be configured. You use the following Administration module pages to configure objects and relationships for display on the Contact Center Advisor and Workforce Advisor dashboards:

- System Configuration:
  - Contact Center Advisor/Workforce Advisor: To configure:
    - Notification refresh rate: how often Advisors sends e-mail about alerts.
    - Application to agent group relationships
    - Show Totals and Averages row for agent groups: Whether or not the Totals and Averages row appears in the Agent Groups pane in Contact Center Advisor and Workforce Advisor.
    - Threshold trigger delay rate: How long a metric's value must exceed a threshold before Advisors creates an alert about it.
    - Display agent group contact center column: Whether this column appears in the Agent Groups pane in Contact Center Advisor.
    - Integrated CCAdv/WA configuration: See Configuration Modes.
    - Default grouping: in the Contact Centers pane in the dashboards.
  - Data Source: To set how long an external source of real-time data can be quiescent before Advisors notifies users about it, and the distribution list to use to send the e-mail.
  - Modules: To modify the application name that displays on the dashboard tabs.

  See System Configuration.

- Regions: Complete the configuration of regions to represent the subdivisions of your company's business operations. See Regions.
- Application Groups/Thresholds: To provide a meaningful configuration of types of contact center activity in the dashboards, complete the configuration of application groups (see Application Groups and Thresholds). Threshold rules define the critical (red) and warning (yellow) conditions that trigger threshold violations, at the application group level. To define the critical and warning conditions for each metric in the context of an application group, see Adding or Updating Thresholds.
- Contact Centers: Complete the configuration of contact centers for a data source that supplies applications and agent groups, and select a geographic region for each; see Configuring Contact Centers.
- Switches/Peripherals: To enable or disable a Genesys switch or Cisco peripheral as far as Advisors is concerned. (A peripheral is a communications interface between a call distributor and call router.) To change this status, see Switches and Peripherals.
- Application Configuration:
    - Rollups: To configure the hierarchy displayed on the dashboard, create the associations between applications, agent groups, and the levels in the hierarchy (for example, regions, contact centers, and application groups).
    - Applications – Agent Groups: Assign agent groups to applications.
    - Application Details: Define descriptive names for applications and change their settings for zero suppression, being displayed on the dashboard, and SL Threshold.
- Contact Group Configuration: (WA only)
    - Rollups: To configure the hierarchy displayed on the dashboard, create the associations between contact groups and the levels in the hierarchy (for example, regions, contact centers, and application groups).
    - Contact Groups–Applications: Assign applications to contact groups.
    - Contact Groups–Agent Groups: Assign agent groups to contact groups.
    - Contact Group Details: Define descriptive names for contact groups and change their other properties.
- Agent Group Configuration: Map agent groups to an agent-group contact center. Configure agent groups to display on the dashboard. See Agent Group Configuration.
- Metric Manager: Define the many properties of a metric, such as its descriptive name. See Metric Manager.
- Users: All creation and configuration of users is now carried out in the Genesys Configuration Manager. See Advisors Business Objects.
- Distribution Lists: To group users who are sent e-mail about alerts based on a specific alert type, add distribution lists and select the users, contact centers, and application groups you want to relate to the distribution list. See Working with Distribution Lists.
- Manual Alerts: Add manual alerts and specify the alert type and affected contact centers. See Manual Alerts.
- Alert Causes: Add and approve alert causes used in Action Management reports. See Alert Causes.
- Key Actions: Add and approve key actions used in Action Management reports. See Key Actions.
- Manage Adapters: The Manage Adapters page is read-only; you can view information about adapters on this page. You no longer select an adapter before performing object configuration.

- Base Object Configuration: You can view and maintain the list of agent group, queue, and filter combinations. See Base Object Configuration
- Notification Lists: If Resource Management is installed, notifications lists are used to inform groups of users within an organization about changes being made to the agents or resources. To view and maintain notification lists, see Notification Lists.
- Notification Templates: If Resource Management is installed, provide standard content for e-mails describing the directives and actions taken from Resource Management. To view and maintain notification templates, see Notification Templates.

Notes about the Interface

Asterisks (*) indicate required fields.

- The date format is MM/DD/YYYY.
- The time format is HH:MM using the 24-hour clock.
- The e-mail address format is username@company.com.
- To search a list of items in a table, type any valid character string from the item’s name in the `Search` field, then click the icon beside the field. The items that match the entered string display. For example, typing `nv` will display Denver. To display the whole list again, click the x beside the Search field.

The search functionality is not available on the `Alerts` pages.

Where paging is implemented, to navigate to the next or previous page in the returned list, click the arrows in the paging control at the bottom right of the table; to navigate to the first or last page in the returned list, click the double arrows in the paging control.

NEW The Administration module is available in English only.

Zero Suppression

Zero suppression is used to prevent objects from displaying on dashboards when there is no activity for them. Certain combinations of metrics' values are used as criteria for the objects to become suppressed. The rules are different for different objects.

Multiple Time Profiles in CCAdv

The CCAdv dashboard can simultaneously display metrics from more than one time profile. When a row in this dashboard becomes suppressed, or leaves suppression, the row can display with certain cells empty. The empty cells are from the time profile that is now zero-suppressed, or was zero-suppressed. In time, the row will either not display at all, or completely display.

Disabled Metrics

In the Administration module, you can disable an application group metric or agent group metric. Advisors does not collect real-time values for a disabled metric. If a metric that CCAdv uses to evaluate zero suppression is disabled, values for it are not collected and CCAdv sees its value as zero. That will influence zero-suppression.

For example, if the calls offered metric and calls handled metrics are disabled, then CCAdv will see their values as zero for every application. A voice queue for which zero suppress = Yes will be zero-suppressed and will not appear on the dashboard even if it actually has currently offered calls, or calls being handled.

Disabling such a metric also affects zero-suppression in WA. If you disabled CCAdv's calls offered metric, this means that Advisors does not collect data for it for either CCAdv or for WA. Zero-suppression in WA will also see its value as zero.

Zero Suppression Rules

The following sections provide guidelines for using zero suppression. The metrics that are used in the rules must be enabled for zero suppression to work.

Contact Group

Contact Groups can never be suppressed.

Application

For applications that reflect voice activity (CISCO services, call types and Genesys queues), if zero suppress = Yes, the following criteria must be met for the application to be hidden on the dashboard:

- calls offered is 0 or N/A *and* calls handled is 0 or N/A

For applications that reflect multi-channel activity (Genesys interaction queues), if zero suppress = Yes, the following criteria must be met for the application to be hidden on the dashboard:

- e-mails entered is 0 or N/A *and* e-mails processed is 0 or N/A *and* Web-chats entered is 0 or N/A *and* Web-chats processed is 0 or N/A

Agent Group

If zero suppress = Yes, and if only CISCO external systems are present, then an agent group is hidden on the dashboard when:

- calls offered is 0 or N/A *and* calls handled is 0 or N/A *and* logged on is 0 or N/A

If at least one Genesys external system is present, then in addition to the above criteria:

- e-mails offered is 0 or N/A *and* e-mails handled is 0 or N/A *and* Web-chats offered is 0 or N/A *and* Web interactions handled is 0 or N/A

Depending on your WA system configuration, logged on could be excluded from this criteria.

The Logged On criterion is included by default. To exclude it, in conf/WorkforceUtilizationZeroSuppression.properties, change the value zero_supress.check_loggedin_for_skill_group and restart WA server and web services.

Region

For WA, if zero suppress = Yes and forecast calls offered, calls offered, and calls handled are N/A or 0, then a Region is hidden on the dashboard.

For CCAdv, if zero suppress = Yes and if only CISCO external systems are present, then a Region is hidden on the dashboard when:

- calls offered is 0 or N/A *and* calls handled is 0 or N/A

If at least one Genesys external system is present, then in addition to the above criteria:

- e-mails entered is 0 or N/A *and* e-mails processed is 0 or N/A *and* Web-chats entered is 0 or N/A *and* Web-chats processed is 0 or N/A

Application Group

For WA, if zero suppress = Yes and forecast calls offered, calls offered, and calls handled are 0 or N/A, then an application group is hidden on the dashboard. For CCAdv, if zero suppress = Yes and if only CISCO external systems are present, then an application group is hidden on the dashboard when:

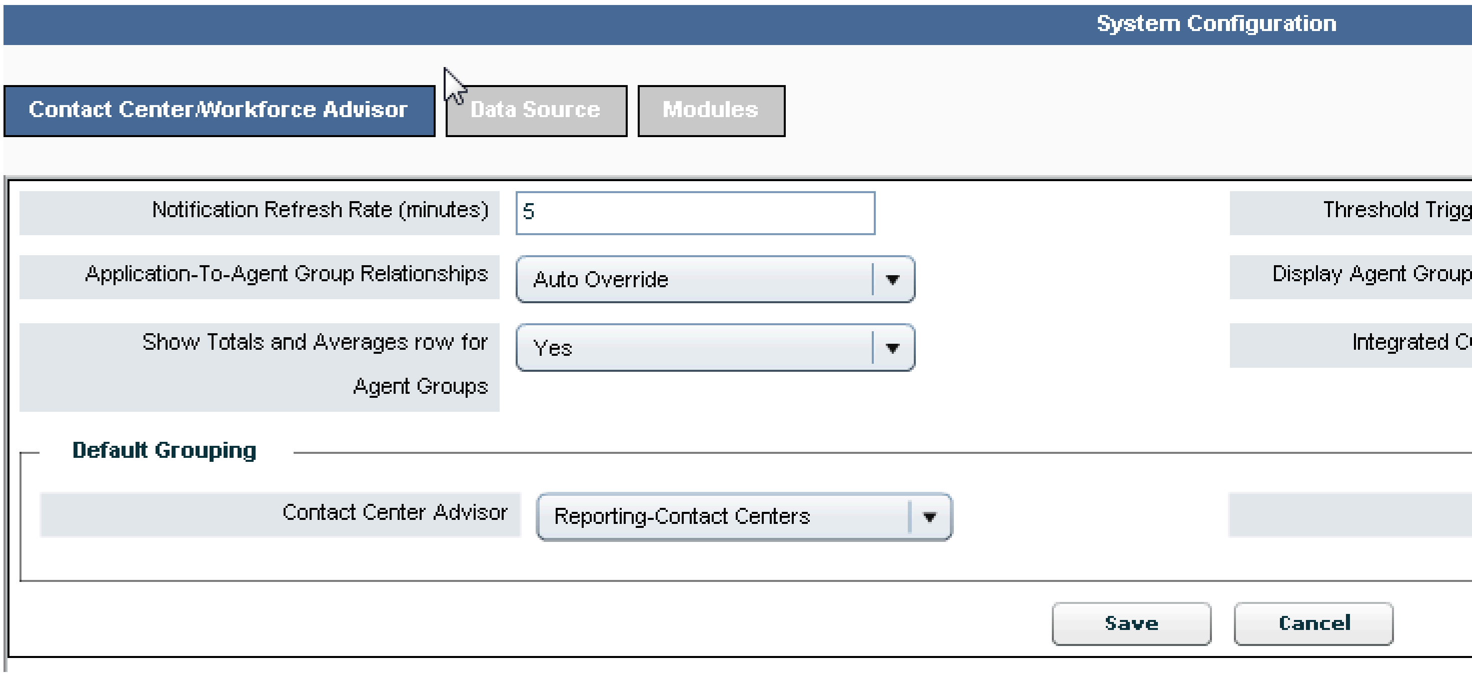
- calls offered is 0 or N/A *and* calls handled is 0 or N/A

If at least one Genesys external system is present, then in addition to the above criteria:

- e-mails entered is 0 or N/A *and* e-mails processed is 0 or N/A *and* Web-chats entered is 0 or N/A *and* Web-chats processed is 0 or N/A

System Configuration

The System Configuration page allows you to control various global capabilities in CCAdv and WA. To make changes, edit the relevant fields and click Save. Changes take effect immediately. Access to this menu option must be configured by an administrator in Genesys Configuration Manager. The following screenshot shows the System Configuration page.



System Configuration Page

System Configuration Tabs

The System Configuration section consists of the following three subsections presented as tabs:

- Contact Center/Workforce Advisor (displayed by default)
- Data Source
- Modules

Contact Center / Workforce Advisor Tab

The Contact Center/Workforce Advisor tab displays the following fields:

- `Notification Refresh Rate (minutes)`: 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. For more information about alerts, see Application Groups and Thresholds.

- `Threshold Trigger Delay Rate (minutes)`: Controls how many minutes a metric's value must exist in a state exceeding a threshold before Advisors creates an alert that appears in the Alerts Map, Alerts Pane, and Alert Management. Alerts about offline peripherals in Cisco ICM, and manual alerts, are an exception to this rate: they appear immediately.
- `Application-to-Agent Group Relationships` :
  - `Manual`: You manually assign agent group(s) to an application or application(s) to an agent group. For CISCO ICM the relationships between Services and Skill Groups that are pre-determined at the source will not be imported if manual mode is selected.
  - `Auto Override`: You manually assign agent group(s) to an application or application(s) to an agent group. For CISCO ICM the relationships between Services and Skill Groups that are pre-determined at the source will be imported automatically.

  The consequences of changing the Application-to-Agent Group Relationships option are:

  - Changing from `Manual` to `Auto Override` will trigger the automatic import of the relationships that exist at the source.
  - Changing from `Manual` to `Auto Override` honors manual entries. Only the relationships that you exclude are removed. Changing from `Auto Override` to `Manual` honors manual entries.
  - Changing `Auto Override` to `Manual` prevents relationships from being imported from the source and erases all automatically imported relationships. After the change, all relationships must be created manually from the administration module.
- `Display Agent Group Contact Center` column: Determines whether the `Contact Center` column is displayed in the `Agent Groups` pane in Contact Center Advisor, thereby controlling whether dashboard users can see the name of the agent group contact center for an agent group related to a network contact center.
  The interval at which the Contact Center Advisor and Workforce Advisor read data from external data sources is not displayed on the page. It is in XML configuration files (CCAdv) or a properties file (WA) in the Advisors deployment directory, and can be changed, but is separately maintained so that it is not arbitrarily changed.
- `Show Totals and Averages Row for Agent Groups`: `Yes/No`. Determines whether the `Totals and Averages` row appears in the `Agent Groups` pane in a dashboard (Contact Center Advisor and Workforce Advisor). This row aggregates the values of metrics of the agent groups related to the applications or contact groups related to the aggregating object currently selected in the `Contact Centers` pane. The default setting is to display the `Totals and Averages` row. You must restart the XML Generator for your changes to appear on the dashboard.
- `Integrated CCAdv/WA Configuration`: `Yes/No`. Starting in Release 8.1.5, you can choose between two Contact Center Advisor/Workforce Advsior configuration modes:
  - Integrated CCAdv/WA configuration mode
  - Independent CCAdv/WA configuration mode

  The default is integrated configuration mode. The choice of the mode determines all further configuration processes, what data is stored, and how the configuration data is interpreted and used inside the application. You can change the mode at any time. A change to the parameter has an immediate impact on the application.

  Earlier releases of the Advisors application used integrated, configuration mode, in which the configuration of Workforce Advisor depends on that of Contact Center Advisor. If you select independent configuration mode, WA operates independently from the CCAdv configuration structure.

  For detailed information, see Configuration Modes.

- `Default Grouping`: Use the drop-down lists to change the default grouping selection for the CCAdv and WA Contact Centers panes. The default grouping selection for business objects in CCAdv and WA is Reporting Region - Contact Centers. You may have users who cannot change the grouping (that is, they do not have the necessary permissions); therefore, you may prefer to have a different default grouping.

  For users who have permission to change the grouping, the default grouping applies only to initial login to Contact Center Advisor or Workforce Advisor. If the user changes the grouping, the grouping that the user selected is cached and maintained. The selected grouping displays after the user logs out and logs in again.

  The selected default grouping does not force the configuration to include that region type. For example, if the default grouping is Reporting Region - Contact Centers, you can still configure an application or a contact group so that it is not related to a reporting region. Then, it will not appear in the dashboards when that grouping is selected, and it will not contribute values to the rollup for that grouping.

  If users are unable to change the grouping on the dashboard, ensure that the region type in the default grouping is also used in the configuration of the objects you want those users to see.

Data Sources Tab

The `Data Source` tab displays a list of the real-time data sources connected to the Advisors suite. The fields represent the following:

- `Status`: Shows the current status of this data source. If the data source's controller time has not been updated for the duration specified by the update delay threshold, then a red icon is displayed in this column next to that data source.
- `Name`: The name of the data source that was registered when installing XML Generator. This field represents the name of a SQL Server database, Oracle schema, or a database link associated with the data source. This is a noneditable field.
- `Descriptive Name`: Descriptive name of the data source. Can be edited by an administrator and is a required field. Appears in the ToolTip of the red stop sign icon displayed in the Contact Center Advisor dashboard when the data source has exceeded the update delay threshold.
- `Type`: Underlying platform for the data source, as specified when installing CCAdv. Current supported values are `GENESYS` and `CISCO`. This value cannot be changed by the administrator through the user interface.
- `Update Delay Threshold (minutes)`: The maximum number of minutes allowed between the last update time of the data source and the current time. Exceeding this threshold causes the red stop sign icon to display in the top right of Contact Center Advisor's dashboard, and in the Status field in this page. This value can be edited and is required. The minimum value that can be entered in this field is 1 and the maximum value is 30.
- `Last Update`: The time of the last update from this data source in the time zone of the server on which the administration user interface is running. This is the controller time in the external data source system and is a noneditable field.
- `Distribution List`: Distribution list to which e-mail is sent if the data source's controller time is not updated and the delay violates the delay threshold. If no distribution list has been previously selected for a data source, the drop-down shows the `Select` option. Otherwise it shows the distribution list associated with the data source. Note that in the use of this distribution list, Contact Center Advisor ignores the settings of an alert's priority and severity, and it also does not use any contact centers or application groups associated with the distribution list.

Modules Tab

The `Modules` tab displays the names and URLs of individual modules of your installation.

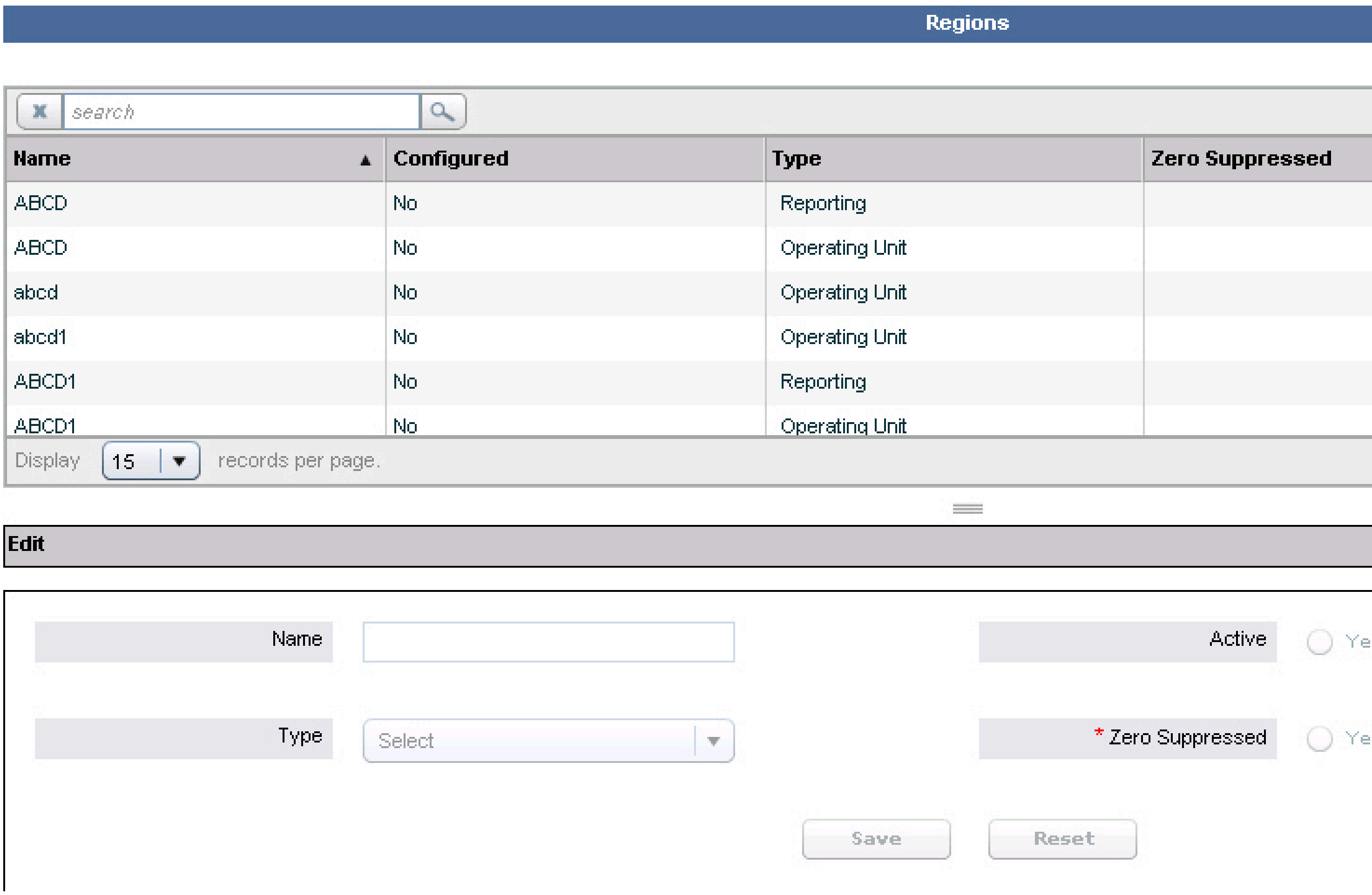
`Application Name`: You can modify the name that displays for the module in the menu you use to switch between modules.

`Deployment URL`: You can modify the URL that Advisors uses to load each module. We suggest you just never do this.

`Version`: Shows the module's version so you can check what you have deployed.

Regions

This section describes how to configure regions in Performance Advisors. The following screenshot shows the Regions page.



Regions Page in the Administration Module

Region Types

In the pane, alerts are shown in relation to a geographic region. CCAdv and WA filter alerts by the user’s permission to see the geographic region associated with the alerts. So, to see alerts in the alerts pane, you must have permission to the alert’s corresponding geographic region, as well as the contact center and application group related to the application or contact group that displays the violation.

Adding/Deleting a New Region in Configuration Manager

New regions can be added only in Genesys Configuration Manager. Adding and deleting regions cannot be performed in the Advisors Administration module. However, you can make a region inactive, or remove it from the Advisors configuration. To add a new region in Configuration Manager, or to delete a region from Configuration Manager, see Advisors Business Objects.

Configuring a Region's Attributes in Advisors

To edit a region's active status and zero suppression status, select the region in the upper panel and edit these details in the `Edit` panel. Alternatively, locate the region in the list by typing the first few letters of its name in the `Search` field, click `Search`, and then select from the list. When your edits are complete, click `Save`. The `Name` and the `Type` fields cannot be edited. These values are configured in Configuration Manager. Complete the fields in the `Edit` panel as follows:

- `Active`: Select whether the status of the region is active or inactive.
  The first time you make a region Active, it becomes part of the Advisors configuration. After this, you can use it to configure applications and contact groups.
  When you change such a region to Inactive, it remains available to use in configuration and the configurations in which it is used do not change. But CCAdv and WA do not use the region when calculating data for the dashboards.
- `Zero Suppressed`: You can select `Yes` for regions 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 region 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.

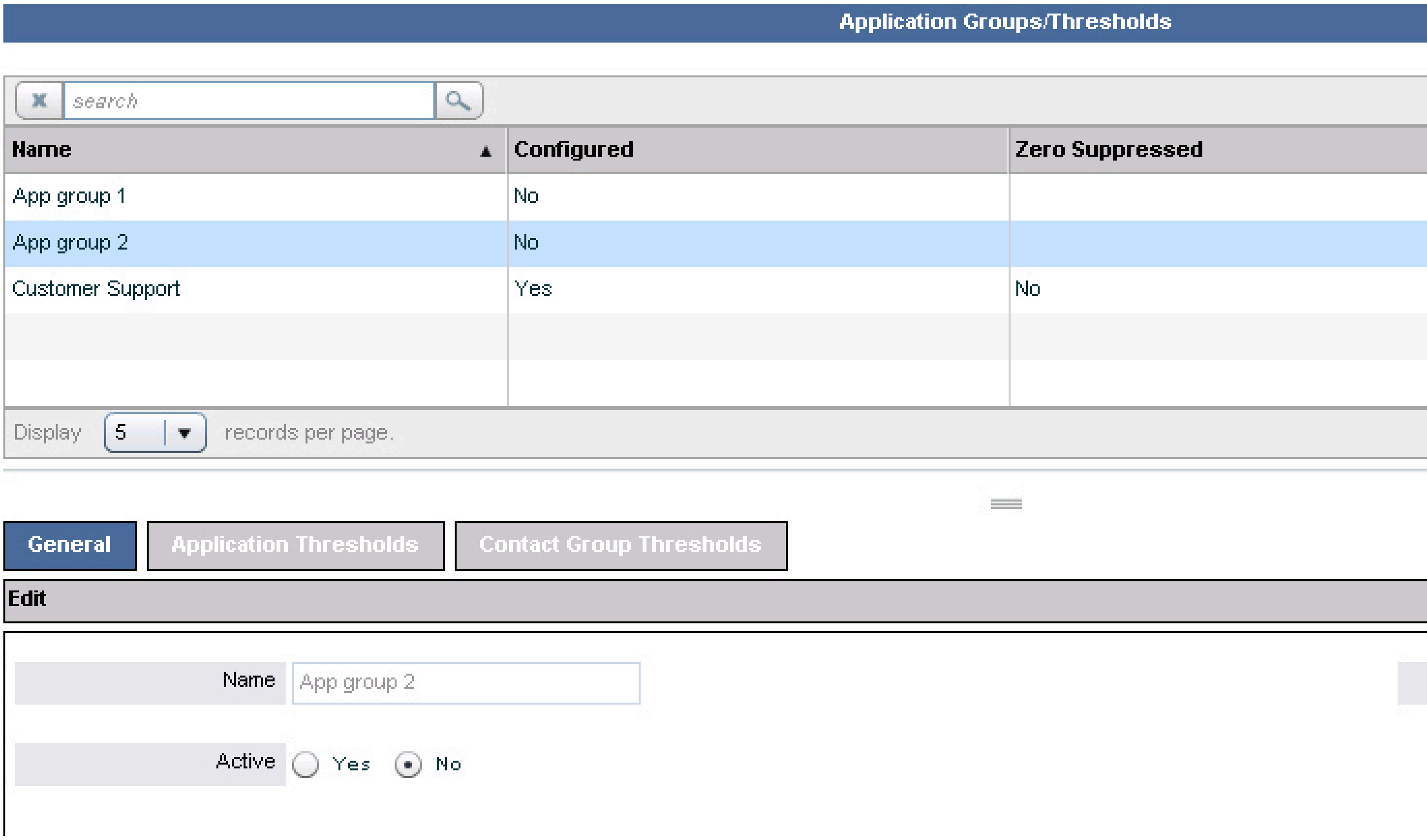
Removing a Region from Advisors Configuration

To remove the region from the Advisors configuration, click on the `Remove from Advisors Configuration` button. This removal is not synchronized back to Configuration Manager. The region continues to be present in the regions list, but displays as not configured and not active. The region completely disappears from the list only after if it is deleted from the Configuration Manager.

> **Important**
> Before removing a region from the Advisors configuration, you must remove its assignment from contact centers and configured applications and contact groups.

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/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 make an application group inactive or remove it 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

Maintain application groups, using the `General` tab.

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.
  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. But 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 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 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 may 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 check box 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 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.

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:

- `Threshold Trigger Delay Rate`: 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 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.

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 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; thresholds would be set; notifications would be set.

Adding or Updating Thresholds

You can update the values for a threshold in Advisors. You can enter values for `Lower-Bound Critical` and `Lower-Bound Warning`, or `Upper-Bound Warning` and `Upper-Bound Critical`, or all four values.

Depending on the metric, the value may be acceptable above or below a certain value.

If for example, the threshold is defined with only Upper-Bound Warning of 50 and Upper-Bound Critical of 75 then a value between 50 and 75 triggers a warning. If the value is above 75, a critical violation is triggered.

If the threshold is defined with a only Lower-Bound Warning of 75 and Lower-Bound Critical of 70 then a value between 70 and 75 triggers a warning. If the value is below 70, a critical violation is triggered.

For a case in which all four values are set, the threshold values are defined to trigger if the value is below or above defined values. For example, values below 10 or above 90 may trigger a critical violation, values between 80 and 90 or between 10 and 20 trigger a warning violation, and values between 20 and 80 are acceptable.

Update application or contact group thresholds

Start Procedure

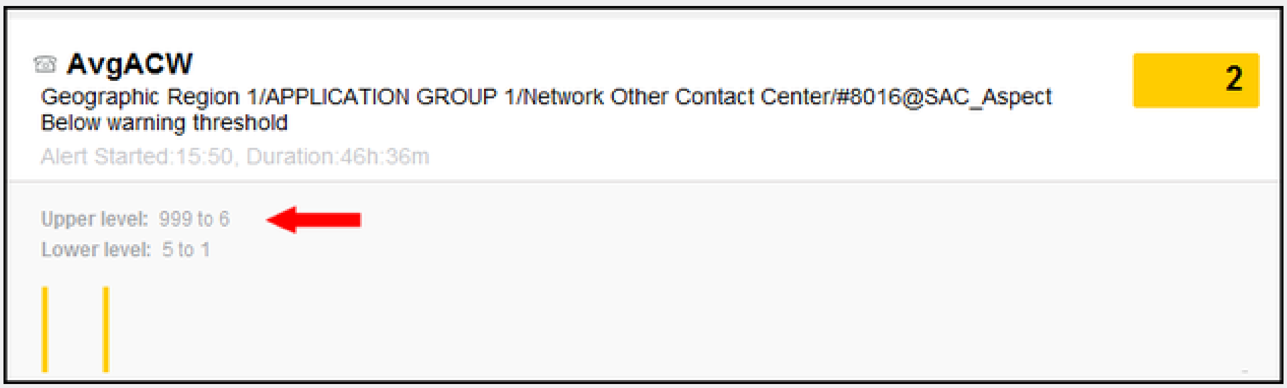
1. For CCAdv, click the `Application Thresholds` tab. For WA, click the `Contact Group Thresholds` tab.
2. Select an application group.
3. In the `Thresholds` panel, select a metric to work with. If you do not see the metric you want, then its `Threshold Applicable` setting is not set to `Yes`. To set it, go to the go to the Report Metrics page and change it there.
4. Type the values for the upper-bound and/or lower-bound limits for the selected metric. Your values are restricted by those in the Min and Max columns of the metric. To set new Min and Max values, go to the Report Metrics page and change them there.
5. To save the changes, click Save.
   A confirmation message displays. The values display on the **Thresholds** page.
6. Add any exceptions required. See Adding Threshold Exceptions.

Important

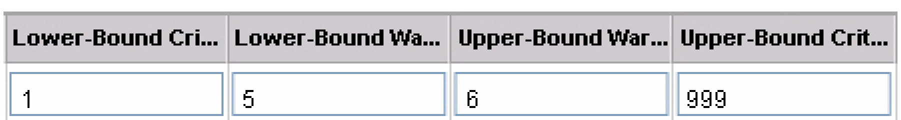
You cannot delete or reset a threshold's values if the threshold is causing an active alert, or caused an alert that is now expired but has not been deleted from the Advisors database. To end the alert and make it inactive, change the threshold's values so that the metric will no longer causes a violation. When the alert ends, and CCAdv or WA has deleted it from the Advisors database, you can reset the threshold or delete its values. See Application Groups and Thresholds for details. A section in that page describes how Advisors ends and then deletes active alerts.

Example: Working with thresholds

You can find the values for configured thresholds in the **Alerts** panel on the dashboard. The following Figure shows the location of threshold values on the panel.

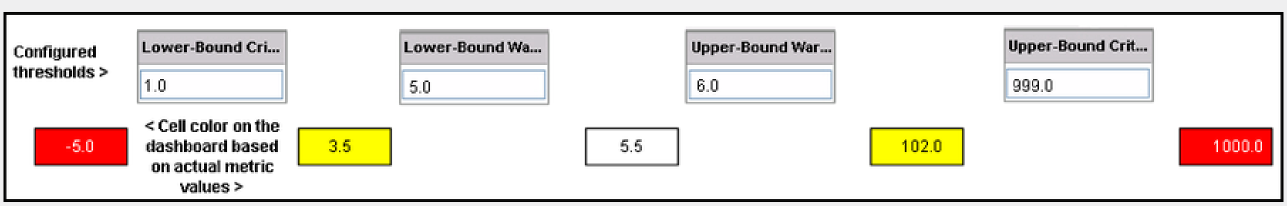


The lower level values shown on the **Alerts** panel correspond to the **Lower-Bound Critical** and **Lower-Bound Warning** values. The upper level values shown on the **Alerts** panel correspond to the **Upper-Bound Warning** and **Upper-Bound Critical** values. See the following Figure.



Threshold values entered on the **Application** tab

Based on the threshold values for the AvgACW metric, shown in the **Alerts** panel, cell color in the dashboard behaves as shown in the following Figure:



You can enter values for only the **Lower-Bound Critical** and **Lower-Bound Warning** thresholds:

Example: Working with thresholds

Lower-Bound Cri...	Lower-Bound Wa...	Upper-Bound War...	Upper-Bound Crit...
400	500		

Configured lower thresholds only

You can also enter values for only the **Upper-Bound Warning** and **Upper-Bound Critical** thresholds:

Lower-Bound Cri...	Lower-Bound Wa...	Upper-Bound War...	Upper-Bound Crit...
		-10.00	-5.50

Configured upper thresholds only

You cannot, however, enter values for only the **Lower-Bound Warning** and **Upper-Bound Warning** thresholds.

You can enter negative numbers for threshold values, however, they must be entered in increasing order from the lowest-level threshold you use to the uppermost-level you use. That is, if you enter values for all four thresholds (**Lower-Bound Critical**, **Lower-Bound Warning**, **Upper-Bound Warning**, and **Upper-Bound Critical**), then you would enter them as shown in the following example:

Lower-Bound Cri...	Lower-Bound Wa...	Upper-Bound War...	Upper-Bound Crit...
-1000	-900	-400	-300

Negative values configured for thresholds

Threshold Exceptions

As part of the Advisor threshold and alert management capabilities, you can configure threshold exceptions. Exceptions are useful when certain periods of time perform differently than others. These differences are specific to the impact on threshold violations. For example, even though call volume fluctuates significantly throughout the day, expected performance should be maintained throughout the day.

Typically a metric target used for alerting (SL% for example) does not change just because other conditions change. However, certain conditions warrant exception usage as they are expected, understood and managed.

Many Advisor users have certain peak periods for which the organization does not try to staff. For example, every Monday from 09:00 to 11:00 a call spike occurs following the weekend. Since that spike is not staffed to deliver typical SL% performance, there is a weekly expected period where normal thresholds are consistently violated. An Advisor threshold exception is useful in this case to lower the targets for SL% and thus avoid threshold violations on the dashboard, alerts on the map, and e-mail notifications being sent.

Used correctly, threshold exceptions can avoid false alarms notifying people of a problem that does not really exist. If the situation is expected, known and accepted, than there should be no reason to alert on it. Alerting should be isolated to the intended purpose of bringing attention to an issue that requires action.

Operation

You can add exceptions to override baseline threshold rules. When the exception is in effect, the values for the thresholds specified in the exception are used to detect violations and create alerts.

Multiple thresholds may affect the same moment in time. Thresholds and exceptions behave as follows when multiple thresholds affect the same moment in time:

- The threshold that started later and ended earlier is the one in effect.
- Non-repeating exceptions override repeating ones.

Specifically, when multiple thresholds affect the same moment in time, thresholds and exceptions behave as follows:

- If more than one threshold affects the same moment in time, the threshold that started later applies.
- If more than one threshold starts at the same time, then the one that ends the earliest applies.
- If more than one exception starts and ends at the same time, then the single instance exception supersedes the repeating exception.
- If more than one single instance exception starts and ends at the same time, then the exception created most recently applies.
- If more than one repeating exception applies, then the repeating exception created most recently

applies.

The example in the following table describes which of the multiple thresholds apply at a given period of time.

Baseline Rule and Exceptions	Time Period	Threshold Applied
Baseline (00:00 - 24:00)	00:00–07:59	Baseline
A: 1/11/2006 08:00 - 10:00; created 1/10/2006 09:00:02 AM EST	08:00–08:44	Exception C
B: 1/11/2006 09:00 - 11:00; created 1/10/2006 10:00:02 AM EST	08:45–08:59	Exception A
C: 1/11/2006 08:00 - 08:45; created 1/10/2006 11:00:02 AM EST	09:00–10:59	Exception B
D: Repeat Weekly 09:00 - 13:00; created 1/8/2006 11:00:02 AM EST	11:00–12:59	Exception E
E: Repeat Monthly 09:00 - 13:00; created 1/9/2006 09:22:13 AM EST	13:00–23:59	Baseline

Threshold violations are raised as soon as they exist. For instance, from 07:55–08:50, assume a metric value is not in violation of the baseline threshold; however, it is a warning (yellow) violation according to Exception C. Therefore, the warning violation will occur at 08:00 and persist until 08:44 (assuming that Exception A is not a violation).

To determine when alerts are generated and displayed on the map and when e-mails are sent, the threshold trigger delay begins counting when the violation is raised. If the violation disappears before the threshold trigger delay because either the actual metric came back into compliance or the threshold changed, then an alert is not raised. If the violation changes (from yellow to red or red to yellow), either because the actual metric moved or the threshold changed, the trigger delay is calculated from when the metric first passed out of compliance (into yellow or red) and the alert, if generated, reflects the current state of the violation.

For exceptions, the start and stop time fields are relative to the contact center. The time zone is used to determine the times. For example:

- For contact centers in PST, typing the start time 6:00 AM and stop time 8:00 AM is 6:00 AM to 8:00 AM PST (that is, 14:00 -16:00 GMT).
- For contact centers in EST, typing the start time 6:00 AM and stop time 8:00 AM is 6:00 AM to 8:00 AM EST (that is, 11:00–13:00 GMT).

> **Important**
> You cannot delete an exception, or delete or reset its values, if the exception 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

exception'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.

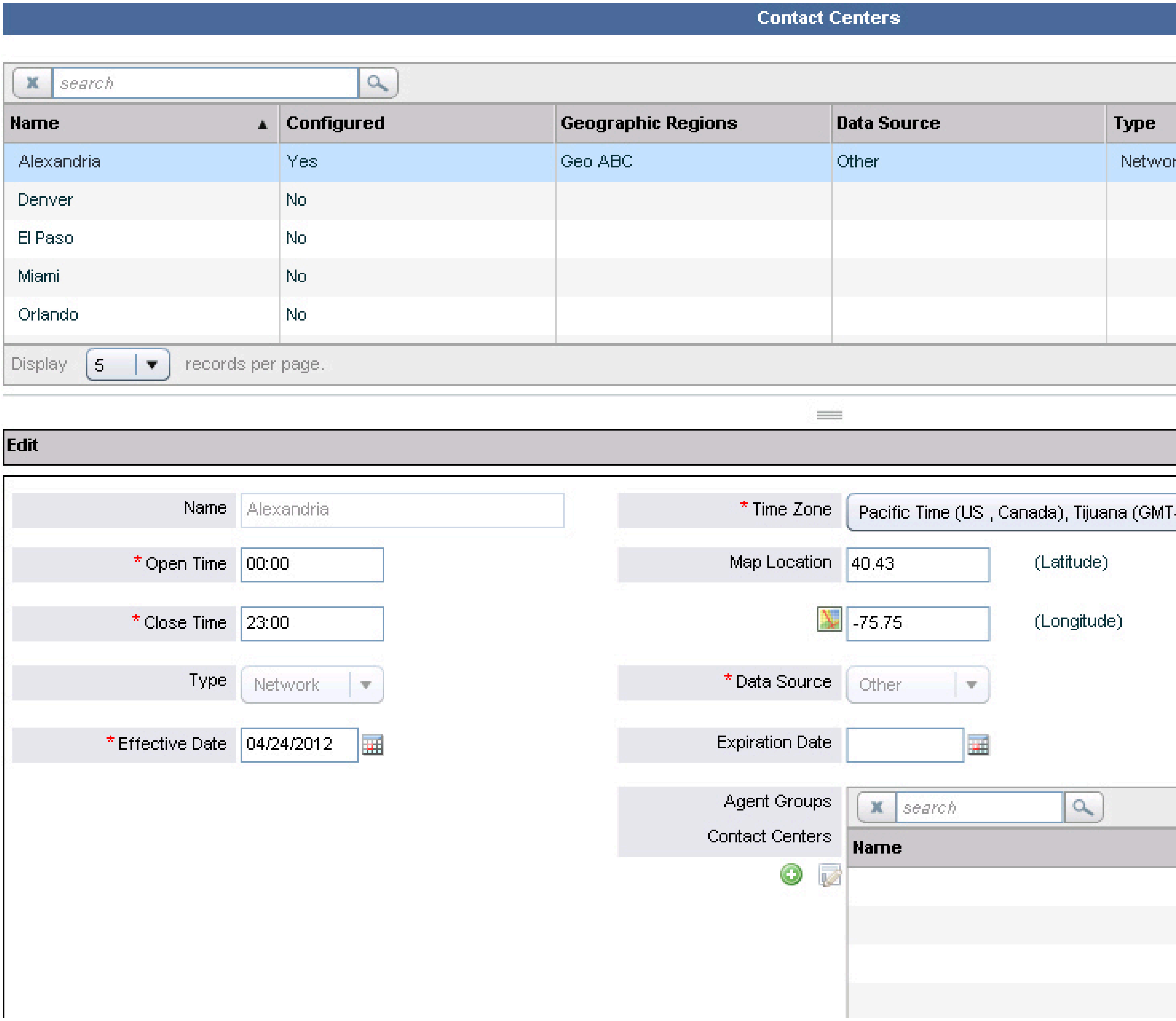
Adding/editing an exception

Start Procedure

1. From the Application Thresholds or Contact Groups Threshold tabs, click on a live (blue underlined) link in the # of Exceptions column.
   Note that there must be a threshold rule before an application or contact group can have an exception to the rule.
2. To add an exception, click New and go to Step 3.
   To edit an existing exception, select it, or search for and then select it in the upper pane.
3. Type or edit the name for the exception in the Name field.
4. Select the time zone from the drop-down field.
   The values are converted to UTC prior to being saved in the database.
5. Enter the start time of the exception.
   The start time must be less than the end time and range from 00:00–23:59.
6. Enter the end time of the exception.
   The end time must be greater than the start time and range from 00:00–23:59.
7. Specify the date the exception applies from the Effective Date calendar.
8. Select the frequency that the exception repeats from the Frequency drop-down list. The default is None.
9. If the exception repeats weekly, select which day of the week the exception repeats.
10. If the exception repeats monthly, select which day of the month the exception repeats.
11. Add the lower-bound and upper-bound warning and critical threshold limits.
12. To save the exception, click Save.
    A confirmation message displays. The exception displays in the table.

Contact Centers

This section describes how to configure contact centers. The following screenshot shows the Contact Centers page in the Administration module.



Contact Centers Page

Adding or Deleting a Contact Center in Configuration Manager

New contact centers can be added only in Genesys Configuration Manager. Adding and deleting contact centers cannot be performed in the Advisors Administration module. However, you can make a contact center inactive, or remove the contact center from the Advisors configuration.

To add a new contact center or delete a contact center in Configuration Manager, see Advisors Business Objects.

Configuring the Attributes for a Contact Center in Advisors

See Configuring Contact Centers.

Removing a Contact Center from Advisors Configuration

To remove the contact center from the Advisors configuration, click on the `Remove from Advisors Configuration` button. This removal is not synchronized back to Configuration Manager. The contact center continues to be present in the contact center list, but displays as not configured and not active. The contact center completely disappears from the list only after it is deleted from the Configuration Manager.

Important

Before removing a contact center from the Advisors configuration, you must remove all other objects that are dependent on it.

Configuring Contact Centers

The Contact Centers page allows you to update contact centers. Multiple steps are required for contact centers to display on the dashboard.

There are three types of contact centers:

- Site: A location-based contact center.
- Network: A contact center for which an exact physical location cannot be specified. A network contact center can be divided into smaller units that represent one or more agent groups from the set of all agent groups belonging to the network contact center. Each such subset of agent groups is called an agent group contact center. In this case, the network contact center becomes a parent of one or more agent group contact centers.
- Agent group: A subset of agent groups from the set of all agent groups belonging to a network contact center.

Genesys recommends adding only one network contact center, and then adding agent-group contact centers to see a more granular view of your data. Because an agent group contact center can only be assigned to one network contact center, if more than one network contact center is created, you must add a second agent group contact center for each physical location.

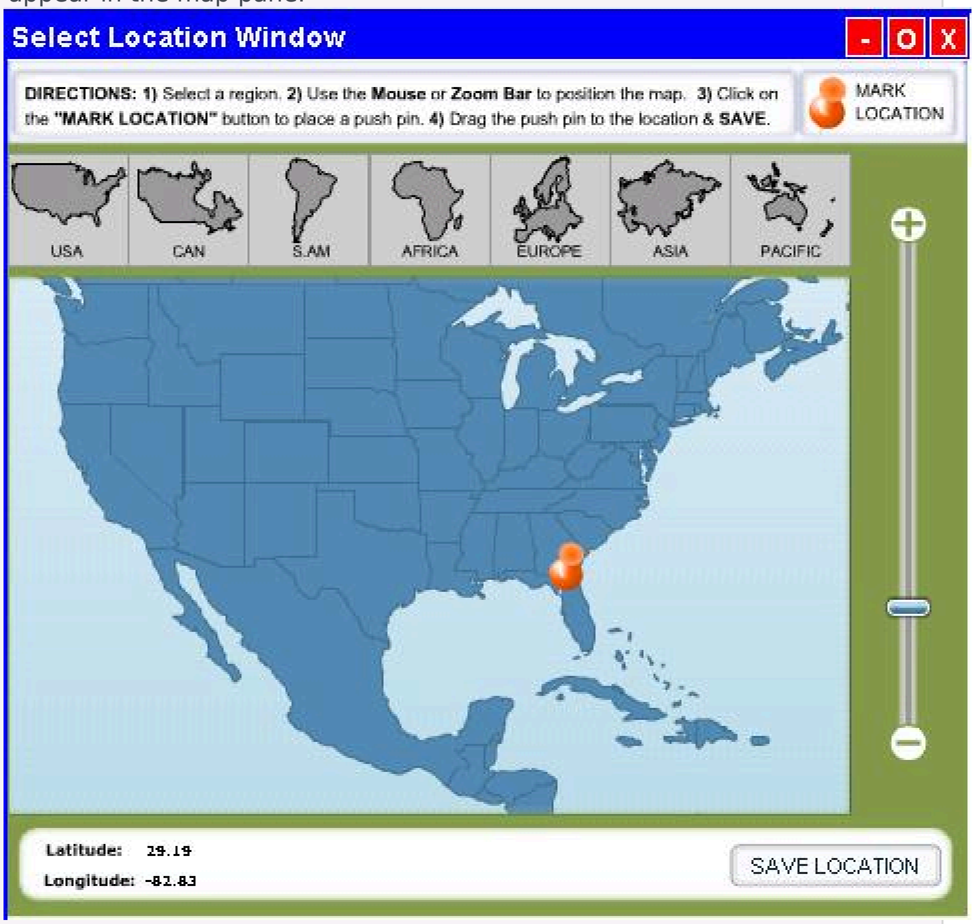
To receive e-mail about alerts concerning a contact center, the contact center must be assigned to distribution lists on the `Distribution Lists` page for users in that distribution list, and who have access to that contact center.

Configure a Contact Center

Start Procedure

1. On the navigation bar, select the Contact Centers page.
   The Contact Centers page displays.
2. Select the contact center that you want to configure.
3. Select the time zone from the drop-down list.
4. To specify the hours of business operation, type the open and close times within the selected time zone.
   The format is hh:mm.
   The open and closed times represent the official time for active data analysis.
   During non-operational hours, summaries that draw data from the contact centers (such as regional or application summaries) are calculated without that data. During non-operational hours, the contact center is hidden from the CCAdv contact centers pane and from the WA contact centers pane.

5. To set the location of the contact center on the map, type the decimal latitude and longitude or click the map icon. A network contact center does not require map coordinates, but it will not display on the map without them.
    a. The mapping window opens as below. Instructions for using this map appear in the map pane.



Select Location Window

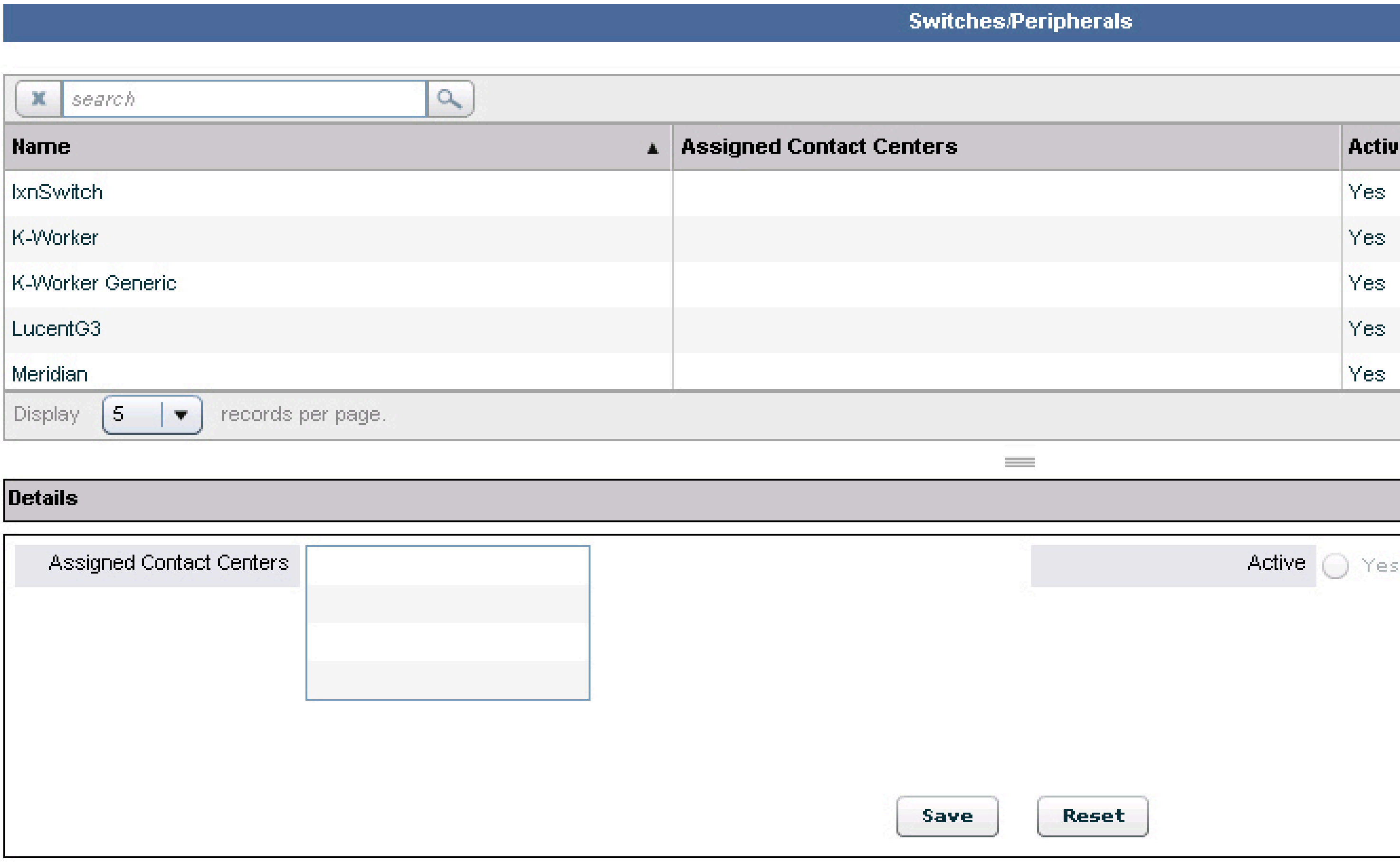
    b. Drag the map with the hand cursor to show more of it in the window.
    c. Click the pushpin tool.
    The pushpin displays on the map.
    d. Drag the pushpin to the correct location.
    e. Click the Save Location button. The mapping window closes.
6. To activate the contact center, click Yes for the Active button.
Selecting No deactivates the contact center and prevents it from displaying on the dashboard allowing you to set it up in advance.

7. Select the geographic region for the contact center from the drop-down list.
8. Enter the type of the contact center: Site or Network. This cannot be changed subsequently.
9. Choose the data source for the contact center. This cannot be changed subsequently. In the `Data Source` field, values are:
   - `Service`: for site contact centers
   - `Other`: for network contact centers
     The value `Other` represents voice queues, interaction queues, calling lists, and call types.
10. To specify when a contact center displays and ceases to display, click the Calendar icons and select the Effective Date and the Expiration Date. The expiration date is optional.
11. For a network-type contact center, enter the agent-group contact centers with which it will be associated by clicking the plus icon beside the list of agent group contact centers.
12. To save the contact center, click Save.
    A confirmation message displays and the contact center displays in the list.

Switches and Peripherals

A switch/peripheral is a communications interface between a call distributor and call router.

The following screenshot shows the Switches/Peripherals page in the Administration module.



Switches/Peripherals Page

The Switches/Peripherals page displays both Cisco TDM logical interface controllers and Genesys switches.

Switches and peripherals are added automatically to Advisors when you run Contact Center Advisor XML Generator.

The Switches/Peripherals page allows you to make a switch or peripheral active or inactive as far as Advisors is concerned. This setting doesn't have any effect on the switch or peripheral.

Applications and agent groups related inactive switches/peripherals will not be used by Contact Center Advisor or Workforce Advisor.

The page also shows the contact centers related to the switch. An administrator assigns a switch/

peripheral to a contact center indirectly. The assignment happens when a user assigns an application to a contact center. If the application belongs to a switch/peripheral, the contact center appears on the Switches/Peripherals page as related to the corresponding switch/peripheral.

Activate Switches and Peripherals

Start Procedure

1. To make a switch or peripheral active or inactive:
    a. Select from the list, or search and select, to display the details of a switch/peripheral.
    b. Select Yes to activate the switch or peripheral, or no to make it inactive.
2. Click the Save button.
   A confirmation message displays and the assignment and active status displays in the list.

Application Configuration

To configure the hierarchy displayed on the CCAdv dashboard and control how applications' metrics are rolled up, create associations between:

- Applications and the business objects that become the levels of the hierarchy in the Contact Centers pane
- Applications and agent groups

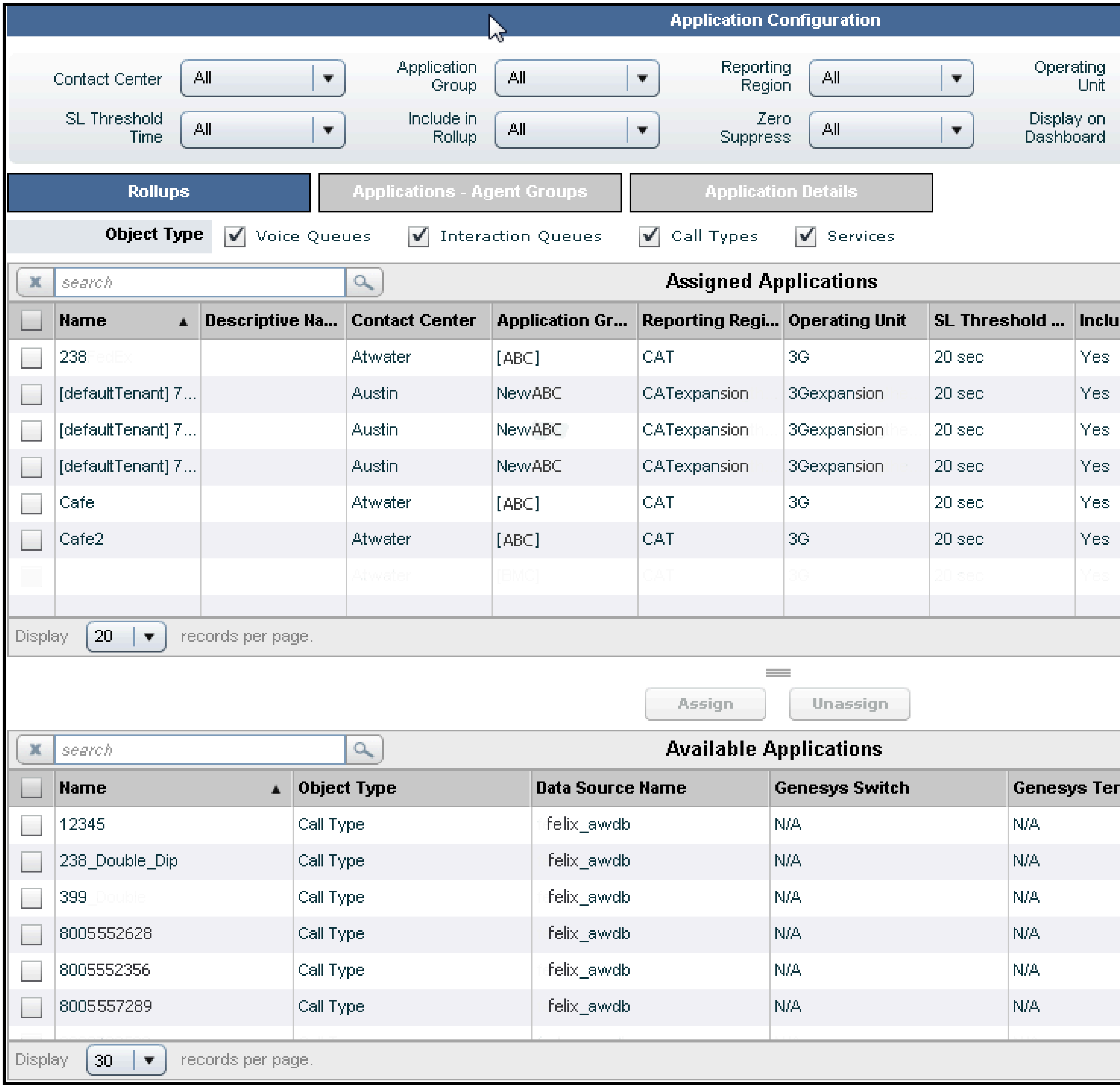
Access to applications and agent groups is not configured in Configuration Manager. Advisors users only have access or not to these objects indirectly, via access to business objects related to them. Data relating to or depending on objects to which users have no permissions will not be displayed.

Access to business objects must be configured by an administrator in Configuration Manager. Objects to which users have no permissions will not be displayed, either in this page or in the dashboard.

Applications are added to Advisors by being imported from external data sources, and cannot be deleted.

The Application Configuration page is used for configuration of:

- Rollups (or aggregations)
- Associations between applications and agent groups
- Details of applications



Application Configuration Page

Rollups

The Rollups tab allows you to define how information displays, summarizes, expands, and contracts in the Contact Centers pane on the dashboard.

You assign a contact center, an application group, and a reporting region or operating unit to an application. These assignments are required for the application to display on the dashboard and to be included in the metric rollup for the specific grouping.

You have the option to do bulk configuration of rollup relationships for CCAdv and WA. For information about bulk configuration, see that chapter in *Performance Management Advisors 8.5.0 Deployment Guide*.

Filtering the Display of Rollups

You can filter the list of objects in the Rollups display.

Filter by business object and other properties using the menus and the Filter button at the top of the page.

Filter object type for a contact center using the check boxes that appear at the top of the Rollups tab.

- `Voice Queues`: For a Genesys data source, select the `Voice Queues` check box to display the voice queues.
- `Interaction Queues`: For a Genesys data source, select the `Interaction Queues` check box to display the interaction queues for chat and e-mail.
- `Call Types`: For a CISCO data source, select the `Call Types` check box to display the call types.
- `Services`: For a CISCO data source, select the `Services` check box to display the services.

Sorting the Display of Rollups

To sort the data in the Rollup table, click on a column heading. The arrow in the down or up position indicates which column is sorted.

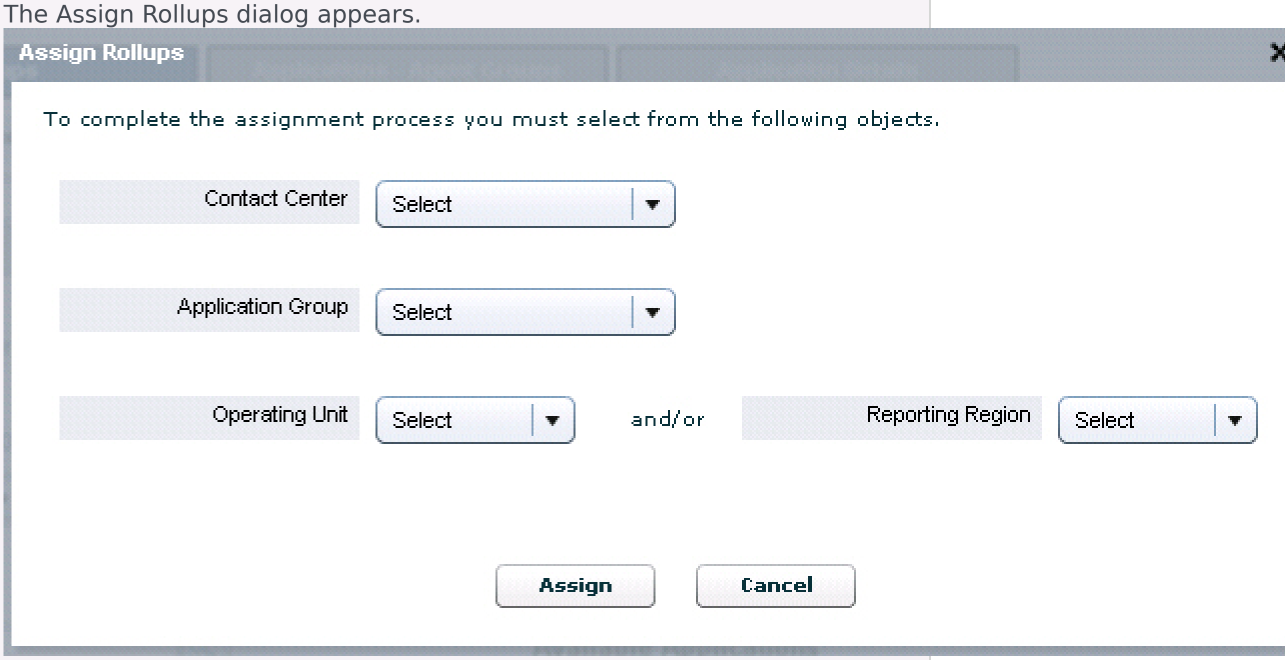
Assigning and Unassigning Applications for Rollup

Assign and Unassign Applications for Rollup

Start Procedure

1. Select Rollups.

2. Use the filter buttons at the top of the page to filter the displayed list of records.
   You cannot select an agent group contact center because you cannot assign an application to an agent-group contact center in the Application | Rollups tab. Agent group rollups are configured on the Agent Group Configuration page.
3. Select one or more applications from the Available Applications table by checking their check box(es).
4. Click the Assign button.
   a. The Assign Rollups dialog appears.



Assign Rollups page

The Assign Rollups dialog does not appear if the required related business objects were already specified in the filter options. If only some of the mandatory objects are specified, then only the remaining missing ones need to be specified.

   b. Define the rollup by selecting the Contact Center, Application Groups, Operating Unit and/or Reporting Region for this application from the drop-down lists of options.
      If you did not select a filter to display the data in the tables, the following defaults are applied:
      - SL Threshold Time: 20 sec
      - Zero Suppress: No
      - Display on Dashboard: Yes

- Include in Rollup: Yes

If you did select a filter, then the values in the filter are applied.

c. Click Assign to save the changes.

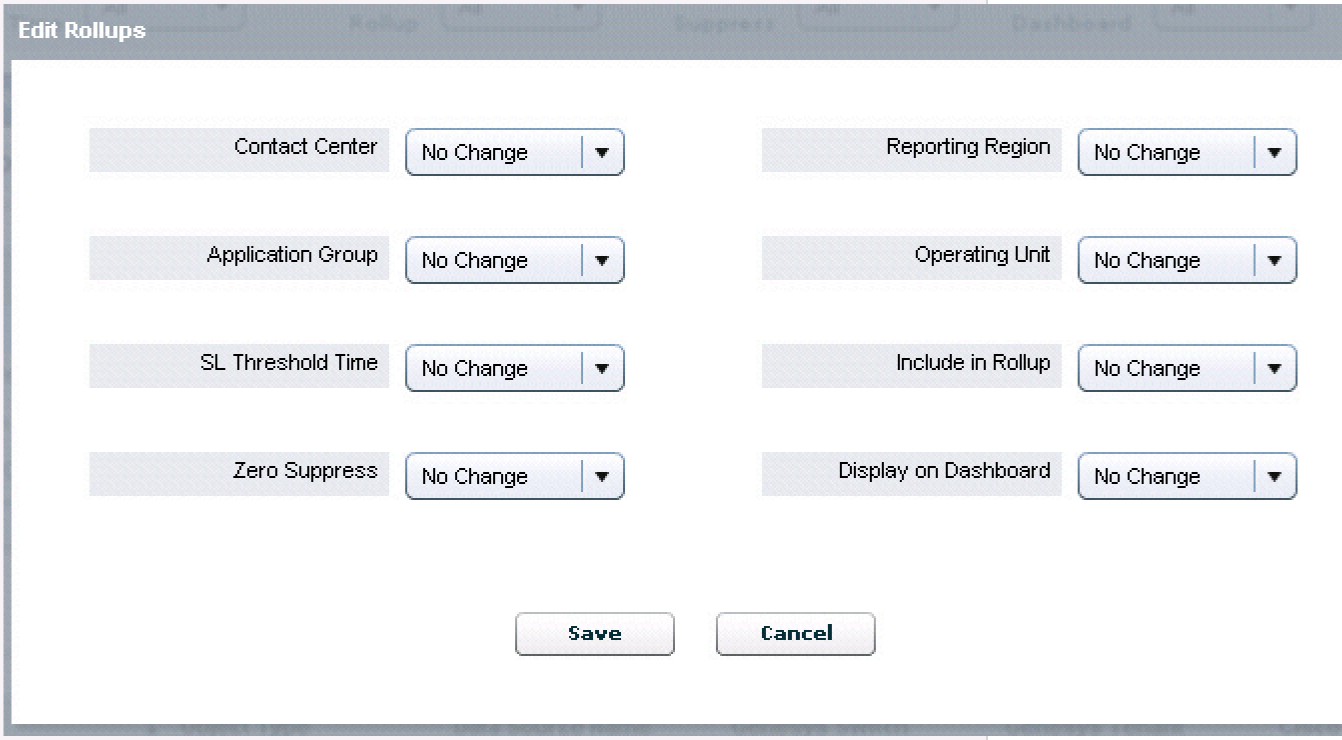
4. To unassign an application, check its check box in the Assigned table, and click Unassign. No confirmation message is displayed.

Editing an Application Rollup

Edit an application rollup

Start Procedure

1. Select Rollups.
2. Use the filter buttons at the top of the page to filter the displayed list of records.
You cannot select an agent group contact center because you cannot assign an application to an agent-group contact center here. To do this, go to the Agent Group Configuration page.
3. Select an application from Available Applications by checking its check box. You can select multiple applications in the same way. The changes you make will apply to all the applications you select. To navigate to the next or previous page use the page controls.
4. Click Edit.
5. Select a value for each of Contact Center, Application Group, SL Threshold Time, Zero Suppress, Reporting Region, Operating Unit, SL Threshold Time, Include in Rollup , Zero Suppress and Display on Dashboard, using the drop-down lists.



Edit Rollups page

With `Include in Rollup` set to No and `Display on Dashboard` set to Yes, the application's metrics values will not contribute to rolled up values, but the application will still appear in the Applications pane when you select the appropriate grouping.

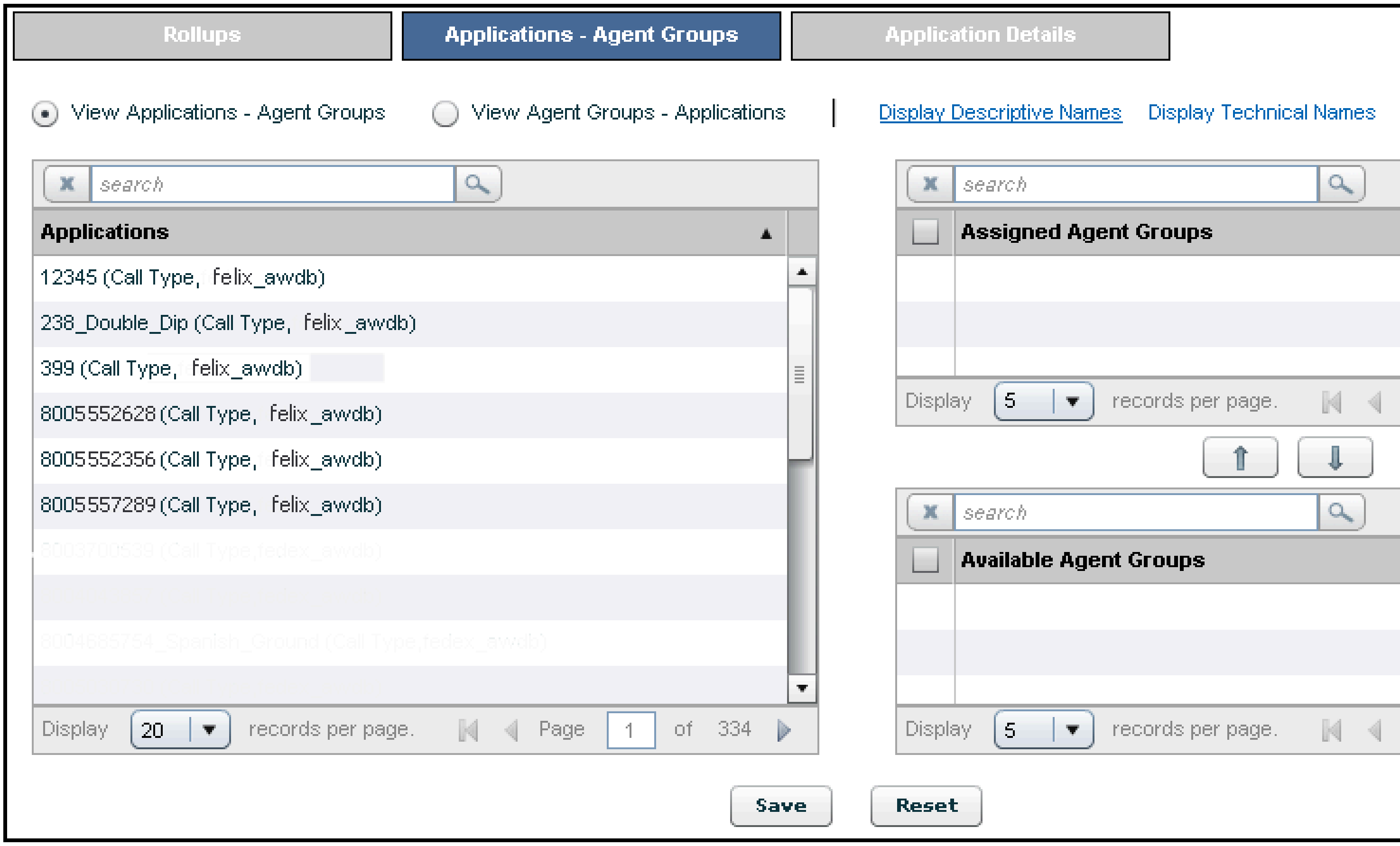
Only consider selecting No for `Include in Rollup` and Yes for `Display on Dashboard` for IVR/VRU-related applications in which you want to display IVR performance in the Applications pane but not in the contact centers pane. The IVR should handle 100% of the calls and the performance could indicate whether or not this is happening or if there may be a problem. In this case including these numbers in the rollup would inflate the performance of call handling by the agents.

For the violations triggered by threshold rules on an application's metrics to display on the Dashboard, you must select Yes for Include in Rollup.

Applications – Agent Groups tab

For agent groups to display on the dashboard, the Application-to-Agent Group relationship must be created.

The Applications-Agent Groups tab allows you to maintain the associations between application and agent groups. The following screenshot shows the Applications – Agent Groups tab.



Configuration Manager Business Attributes—Individual Objects

You can opt to display either descriptive or technical names of objects by clicking the Display Descriptive/Technical Name link.

To see the agent groups available to assign to an application, and those already assigned to it, select the application.

Only the agent groups from the same external data source display for the selected application.

From Cisco ICM, both base and non-base agent groups are imported. The enterprise name is used to distinguish agent groups with the same name but from different peripherals.

You can reverse the order of display by selecting the relevant radio button. When the agent groups display in the left-most pane, then to see the applications available to assign to an agent group, and those already assigned to it, select the agent group.

Depending on how the application-to-agent groups relationship is defined in system configuration, you may map agent groups to applications manually or, if Auto Override mode is selected, automatically with Cisco ICM.

Tip

The relationships between applications and agent groups support certain functionality in the dashboards.

1. They support displaying the set of agent groups related to both a contact center and an application group.
2. They support highlighting agent groups when applications are selected, and vice versa.
3. They are used for deriving some metrics of business objects related to applications, where the metrics are based on agent group metrics.

The XML Generator updates these relationships when it starts, and then once per day (overnight). If a relationship changes in the System Administration module, and you do not want to wait overnight to obtain the effects of this, then the administrator must restart the XML Generator.

Maintain Applications-Agent Groups Assignments

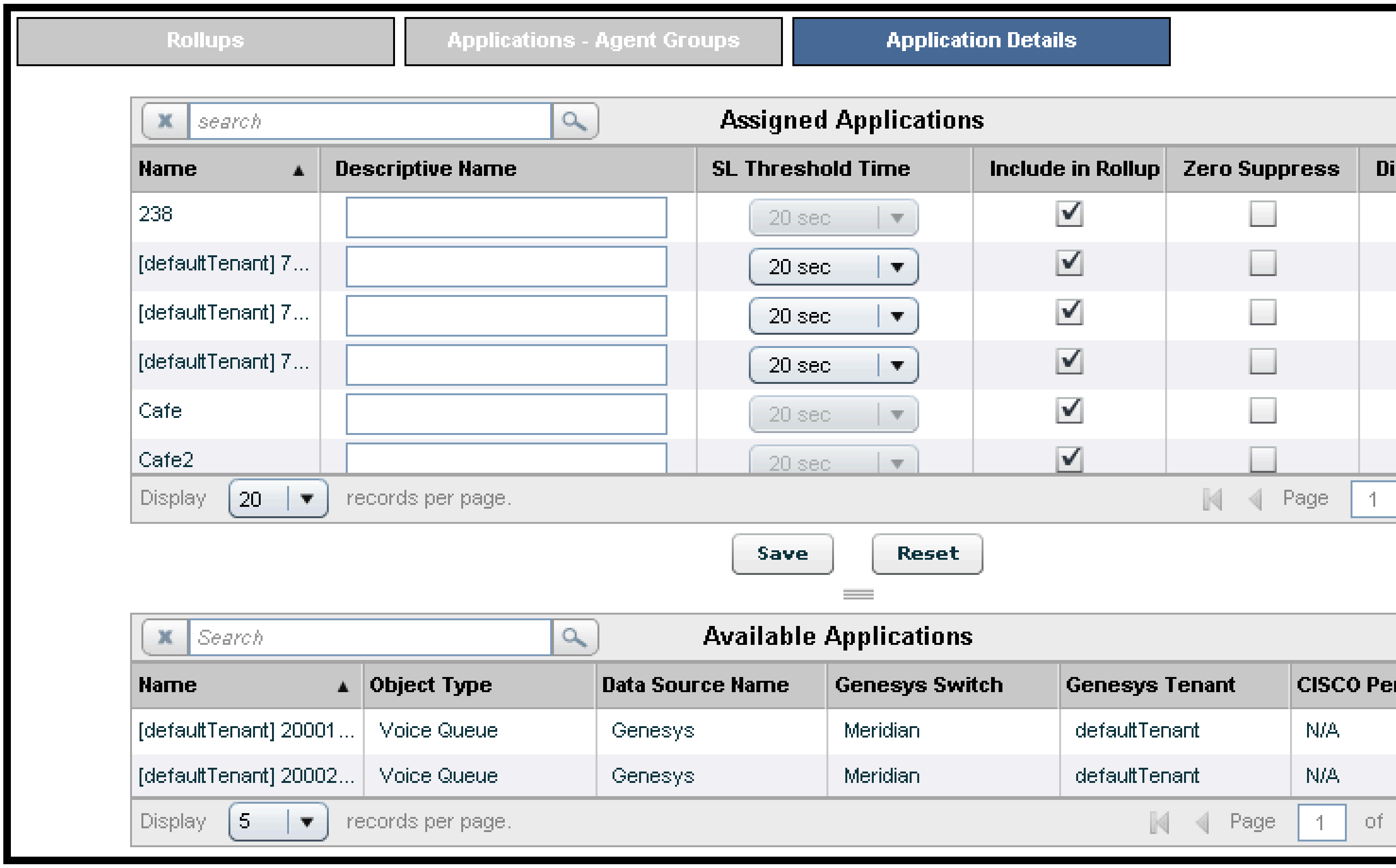
Multiple edits are not available for assigning agent groups to applications in the Administration. You must edit individual applications to associate agent groups after creating the rollups.

Start Procedure

1. Select the Applications-Agent Groups tab.
2. Select an application or agent group from the left panel. This displays the already assigned applications or agent groups in the Assigned panel on the right. Applications or agent groups that are available for assignment appear in the Available panel.
3. To move an object between the Available and Assigned panels, check its check box and click on either the up or down arrow between the two panels.
4. Click Save.

Application Details

You can use Application Details tab to maintain all the details of an application other than its technical name. The following procedure shows the Application Details tab.



Application Details tab

Maintain application details

Start Procedure

1. Click on the Application Details tab to display.
2. Edit the details as follows:
   - Descriptive Name: Descriptive names display on the dashboard. Hovering over the descriptive name displays the technical name.
   - SL Threshold Time: Applicable only to ACD & Virtual queues from Genesys Stats Server. Select a value from the drop-down list. The list of available SL threshold times is predefined. To add additional entries to this list, new entries can be added to the platform database table SL_THRESHOLD.

- Include in Rollup: Check the box to include the application in rollups.
  In addition to this setting, the application must be configured, that is, related to a contact center, application group, reporting region, and/or operating unit.
  See *Editing an Application Rollup*, earlier on this page, for further information on this option.
- Zero Suppress: Check the box to zero-suppress the application. (See Zero Suppression.)
- Display on Dashboard: Check the check box to display the application on the user dashboard.
  In addition to this setting, the application must be configured, that is, related to a contact center, application group, reporting region, and/or operating unit.
  See *Editing an Application Rollup*, earlier on this page, for further information on this option.

3. Click Save.

Contact Group Configuration

In Advisors, the term *contact group* means an forecasting entity from a workforce management system. These are activities in Genesys WFM, forecast groups and staff groups in Aspect eWorkforce Management, and contact types in IEX TotalView.

To configure the hierarchy displayed on the WA dashboard and control how contact groups' metrics are rolled up, create associations between:

- Contact groups and the business objects that become the levels of the hierarchy in the Contact Centers pane
- Contact groups and applications
- Contact groups and agent groups

Access in Advisors to contact groups is not configured in Configuration Manager. Advisors users only have access or not to them indirectly, via access to business objects related to them.

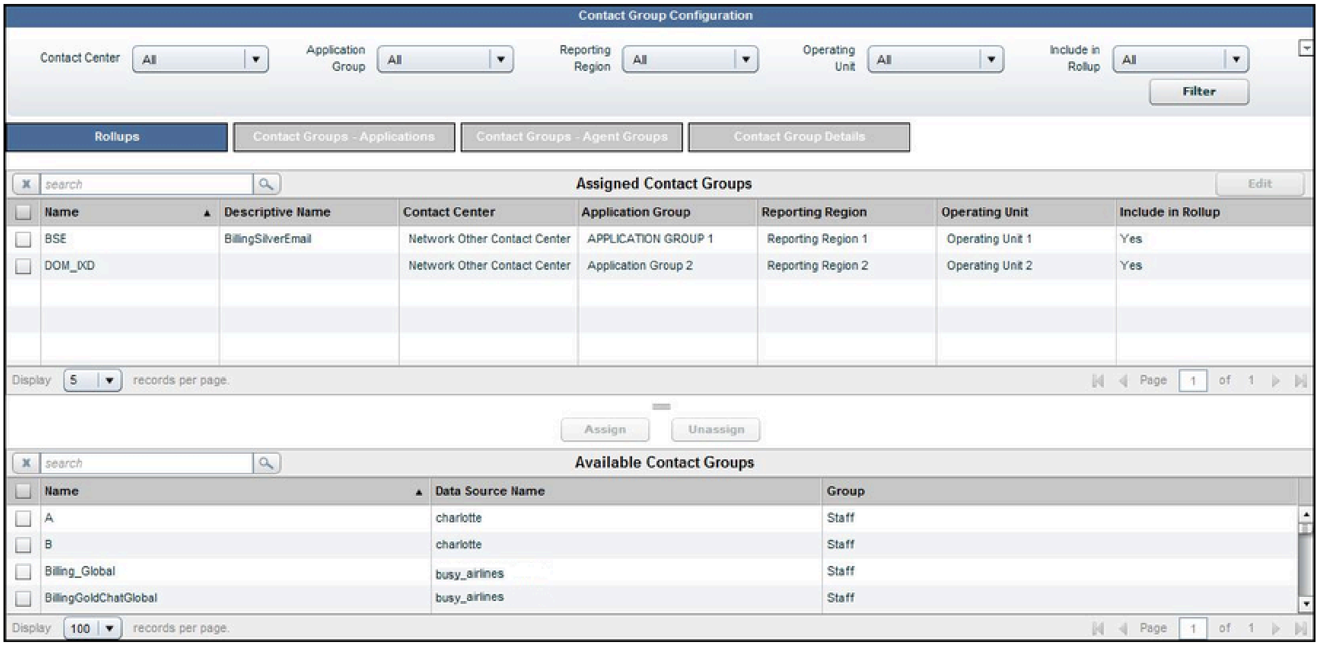
Access to business objects that form levels in the hierarchy on the WA dashboard must be configured by an administrator in Configuration Manager. Objects and data relating to or depending on objects to which users have no permissions will not be displayed, either in the dashboard or on this page.

If contact groups do not load or do not update on the Contact Group Configuration page in the Administration module, see information about how to import contact groups in the Performance Management Advisors 8.5 Deployment Guide.

Contact Group Configuration Page

To configure contact groups, use the Contact Groups Configuration page. It has four tabs:

- Rollups (aggregations: create associations between contact groups and business objects -- contact centers, application groups, and reporting regions or operating units)
- Contact Groups - Applications: create associations between contact groups and applications from Genesys Stats Server or CISCO ICM.
- Contact Groups - Agent Groups: create associations between contact groups and agent groups from Genesys Stats Server or CISCO ICM.
- Details of contact groups



Rollups Tab

The Rollups tab allows you to define how information displays, summarizes, expands, and contracts in the Contact Centers pane on the dashboard.

To configure a contact group, assign a contact center, an application group, and a reporting region or operating unit toit. These assignments are required for the contact group to display on the dashboard and to be included in the metric rollup for the specific grouping.

You have the option to do bulk configuration of rollup relationships for CCAdv and WA. For information about bulk configuration, see information about bulk configuration in the *Performance Management Advisors 8.5.0 Deployment Guide*.

> **Important**
>
> WA does not control the data source names; if data source names are the same, but one is in lower case and the other is in upper case, then WA interprets them as two different data source names. For more information on data source names, see the section on importing contact groups in the Deployment Guide.

Filtering the Display of Rollups

You can filter the list of objects in the Rollups display.

Filter by business object and other properties using the menus and the Filter button at the top of the page.

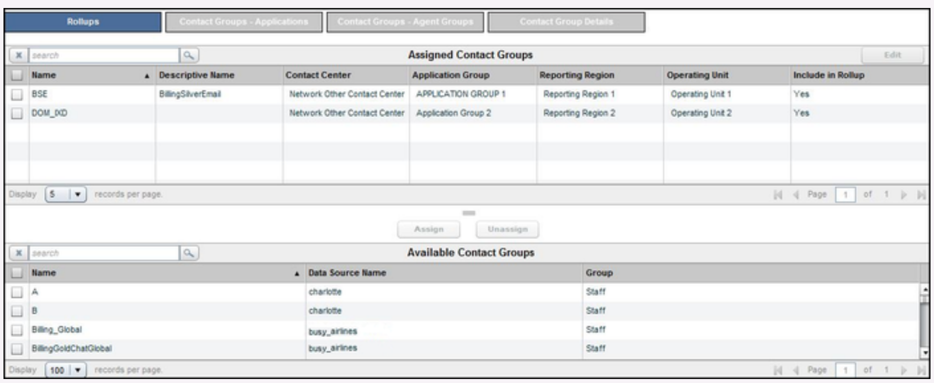
Sorting the Display of Rollups

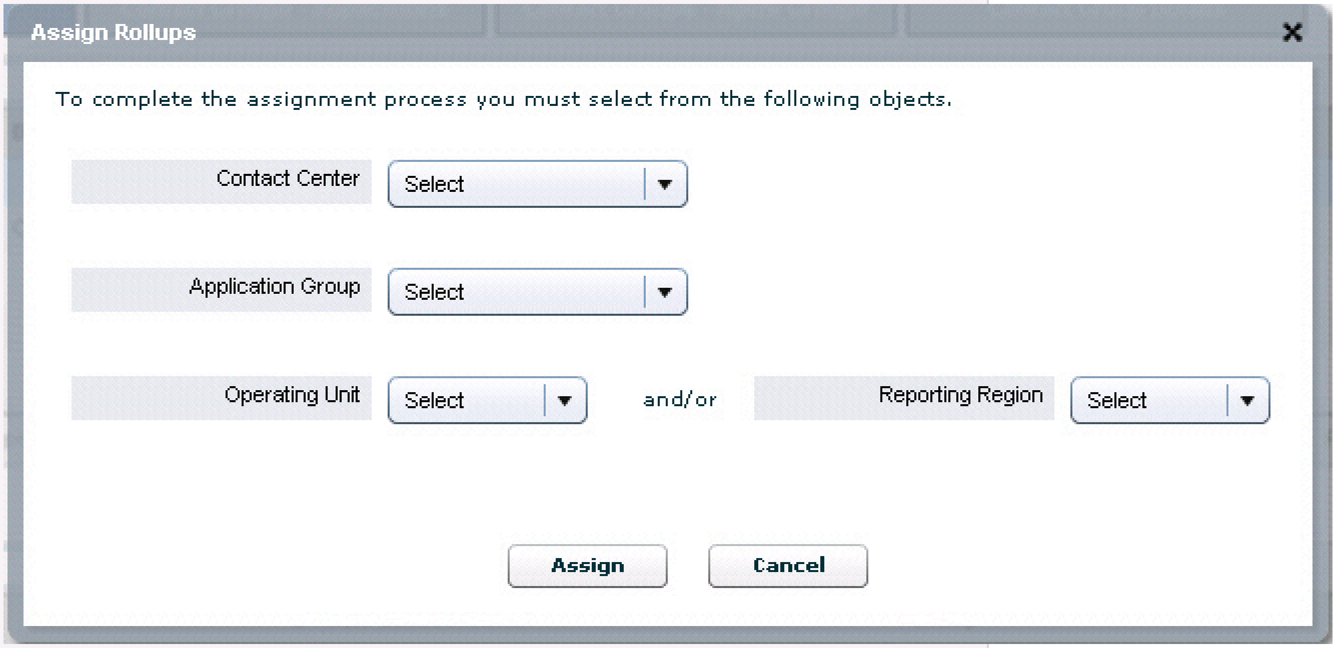
To sort the data in the Rollup table, click on a column heading. The arrow in the down or up position indicates which column is sorted.

Assigning Contact Groups for Rollup

Assign contact groups for rollup

Start Procedure

1. Select the Rollups tab.
   The following screenshot shows the Rollups tab in the Contact Group Configuration page.
   
2. Select a contact group from the Available Contact Groups pane by checking its check box. You can select multiple contact groups in the same way. The changes you make will apply to all those you select. To navigate to the next or previous page use the page controls
3. To associate the contact group for rollup, click Assign. The Assign Rollups pane displays.



Assign Rollups page

The Assign Rollups dialog does not appear if the required related business objects were already specified in the filter options. If only some of the mandatory objects are specified, then only the remaining missing ones need to be specified.

4. Define the rollup by selecting a contact center, application group, reporting region, and/or operating unit for the contract group.
   If you did not select a filter to display the data in the tables, the following defaults are applied:
   - Include in Rollup: Yes

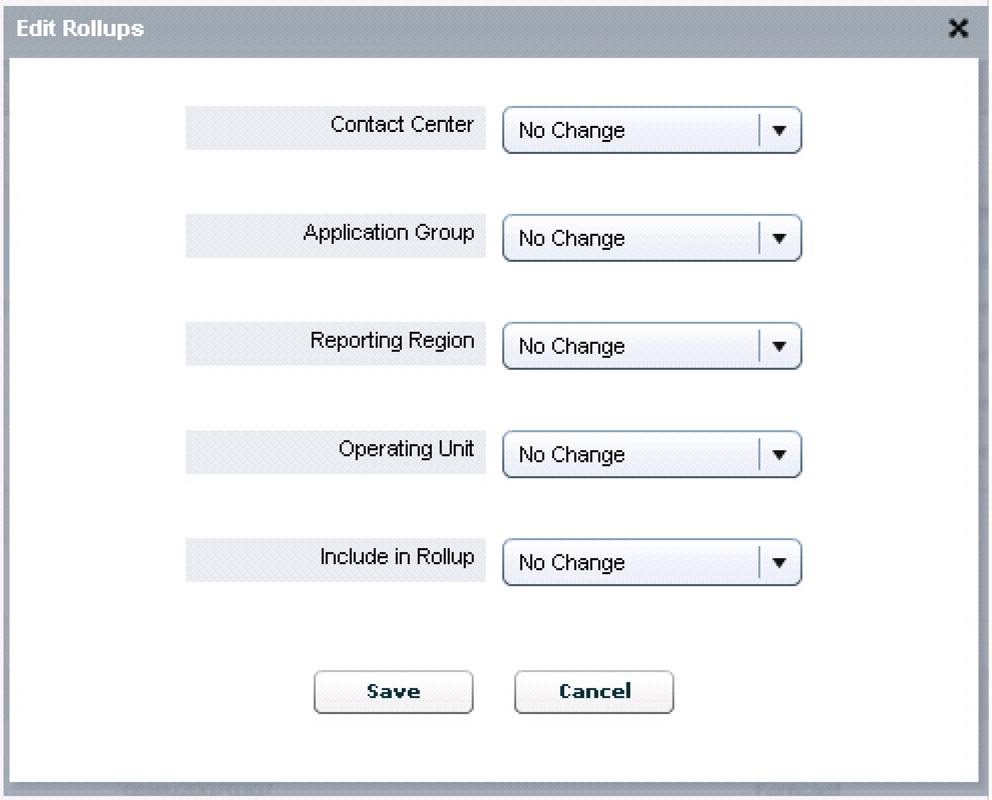
   If you did select a filter, then the values in the filter are applied.
5. Click Assign. The Assign Rollups dialog box closes.
6. In the main Rollups tab, a confirmation message displays and the details display in the table.

Editing a Contact Group Rollup

Edit a contact group rollup

Start Procedure

1. Select Rollups.
2. Select one or more contact centers from the list.
3. Click Edit.



Contact Groups Edit page

4. Edit the rollup by selecting a contact center, application group, reporting region, and/or operating unit.
5. To roll up the metric values of a contact group to an application group, contact center, regional level, or enterprise level, select Yes for the Include in Rollup. Selecting No for Include in Rollup excludes the values from the WA rollup.
   For the violations triggered by threshold rules on a contact group's metrics

to display on the dashboard, you must select Yes for Include in Rollup.

6. Click Save.

Contact Groups – Applications

Use the Contact Groups - Applications tab to assign applications to contact groups. The content of this page depends on the selected CCAdv/WA configuration mode.

> **Tip**
> In either configuration mode, if there are no applications mapped to a configured contact group, the contact group displays on the dashboard showing only forecast metrics from the WFM systems.

Integrated Configuration Mode

If integrated configuration mode is enabled, the list of available applications presents applications that meet *all* of the following criteria:

- Configured applications
- Applications mapped to the same business objects to which the selected contact group is mapped
- Applications not mapped to this, or any other, contact group

If such an application is mapped to the contact group, and then later removed from CCAdv configuration, this application disappears from the applications assigned to the contact group and the list of available applications. It no longer contributes metric values to the WA dashboard.

The same thing happens if the configuration of the application or the contact group is modified in a such way that their business objects no longer match.

In integrated configuration mode, you must assign one or more applications to the contact group.

In integrated configuration mode, agent groups assigned to the applications are automatically assigned to the contact group

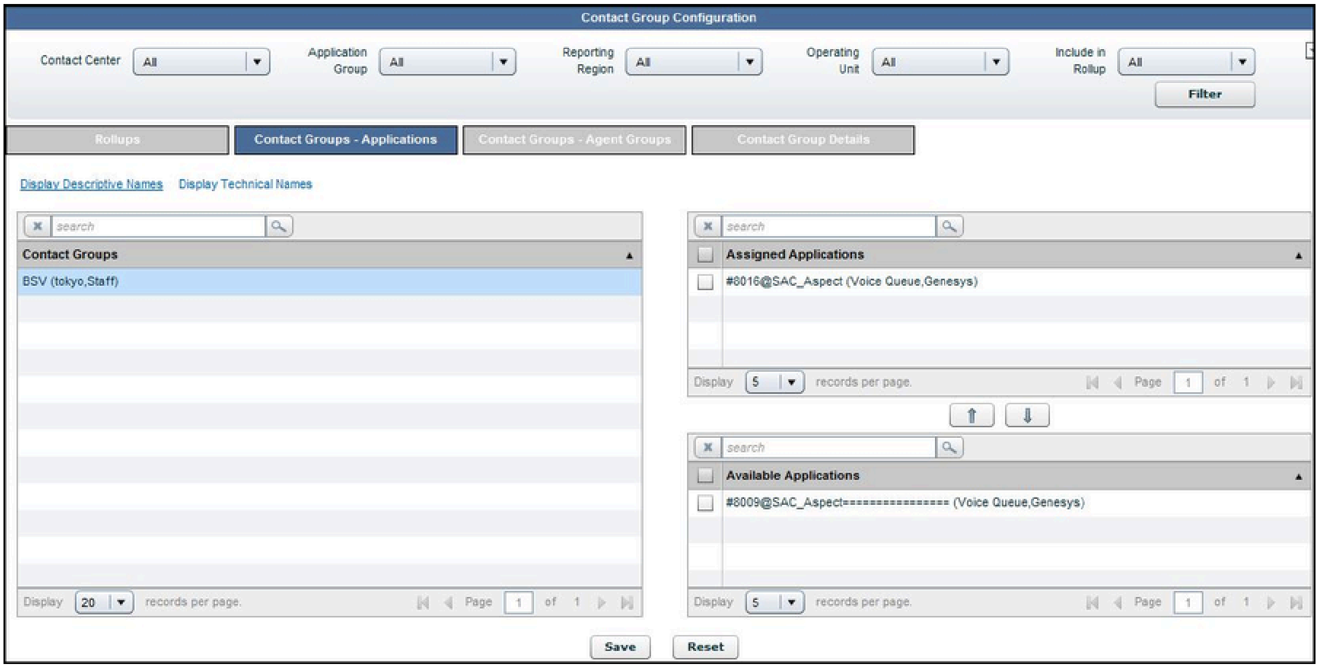
Independent Configuration Mode

If independent configuration mode is enabled, the list of available applications represents a set of all applications that are not mapped to this, or any other, contact group. Contact group-to-application mappings are independent of the CCAdv configurations. You can assign any application to a contact group that is not associated with an agent group contact center.

In independent configuration mode, agent groups assigned to the applications are not automatically assigned to the contact group

Contact Group - Applications

The following screenshot shows the Contact Groups – Applications tab.



You can opt to display either descriptive or technical names of objects by clicking the Display Descriptive/Technical Name link.

Maintain contact groups-to-applications assignments

Start Procedure

1. Select the Contact Groups - Applications tab.
2. Use the filters in the uppermost panel to filter the display of contact groups in the Contact Groups panel.
   The display shows contact groups, assigned applications and available

applications.

3. Select a contact group in the left panel.
 This displays the already assigned applications, if any, in the Assigned panel on the right. Applications that are available for assignment appear in the Available panel. Chat, e-mail, and outbound metrics are not available in WA. Consequently, applications that are interaction queues or calling lists are never available here.
4. To move an application between the Available and Assigned panels, check its check box and click on either the up or down arrow between the two panels.
5. Click Save.

Contact Groups - Agent Groups

All types of contact centers are available for selection in the Contact Center drop-down menu. The menu contains both agent group contact centers, and other types of contact center. The names of AGCCs display with the names of the related network contact center (NCC), formatted as NCC Name: AGCC Name.

The contact groups mapped to any type of contact center display in the Contact Groups pane. The content of other panes on this page depends on the selected CCAdv/WA configuration mode.

There is no restriction on the number of contact groups to which an agent group can be mapped.

Available Agent Groups in Integrated Configuration Mode

In integrated configuration mode:

- If the selected contact group is mapped to an AGCC, then here are the steps to make an agent group appear in Available Agent Groups for assignment to a contact group:
  - In Application Configuration:
    - Configure an application, assigning it to a network contact center.
    - Assign the agent group to the application.
  - In Agent Group Configuration:
    - Assign the agent group to the agent group contact center.
  - Now in Contact Group Configuration:
    - Configure contact group 1, assigning it to the same business objects as the application.
    - Now the agent group will appear in the Available Agent Groups in the Contact Group - Agent Groups tab, and you can assign the agent group to contact group 2.

- If the selected contact group is mapped to any other type of contact center, no available agent groups display in integrated configuration mode. The list of assigned agent groups is shown, but you cannot edit it. The agent groups are those mapped to the applications that are mapped to the contact group and also to the same business objects to which the contact group is mapped. The page, in this case, can be used only for viewing the lists of agent groups expected on the dashboard view.

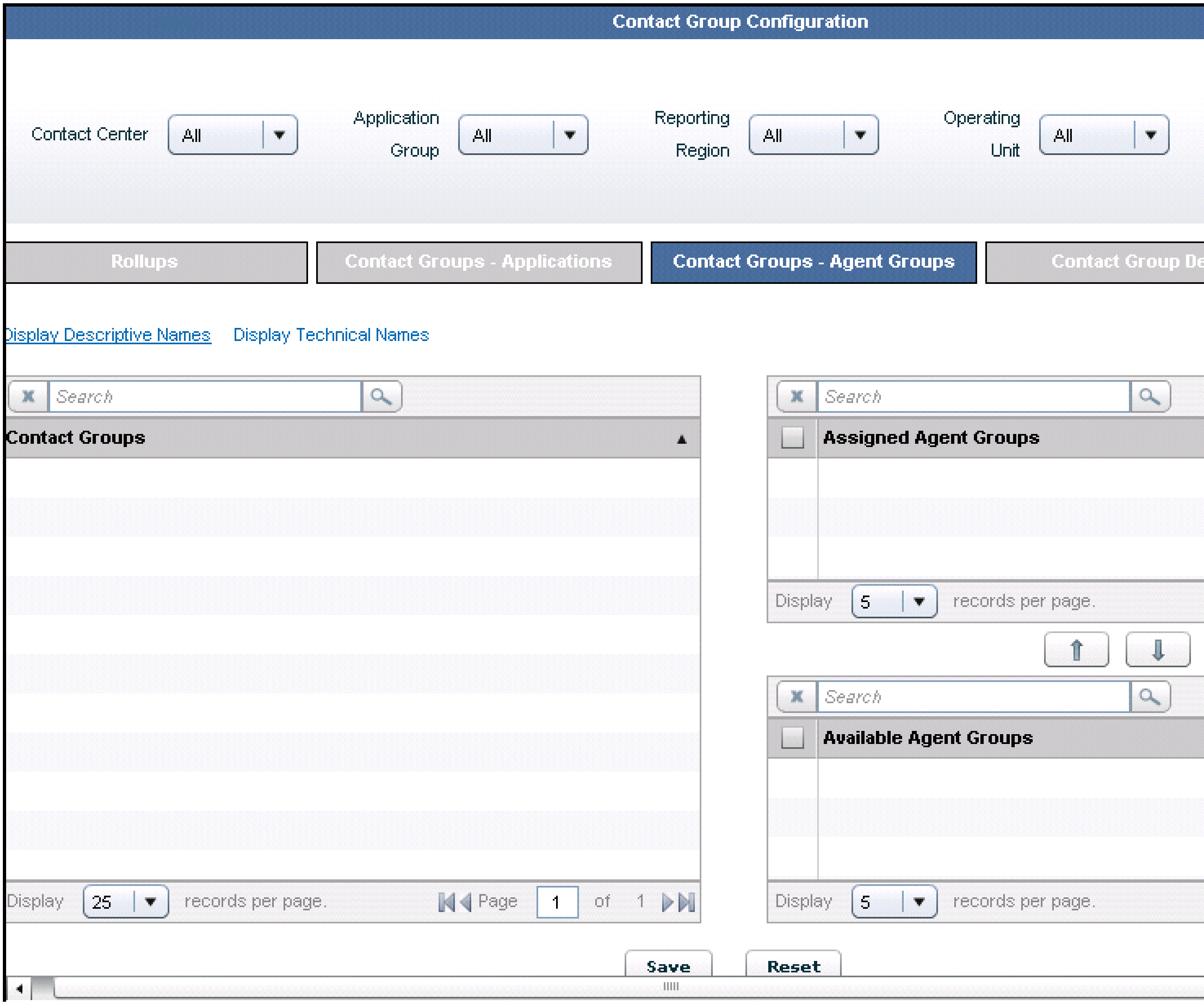
Available Agent Groups in Independent Configuration Mode

In independent configuration mode:

- If the selected contact group is mapped to an AGCC, the list of available agent groups includes all agent groups that have the following characteristics:
    - assigned to the same AGCC to which the selected contact group is mapped
    - `Include in WA` property set to `Yes`
    - not already mapped to the selected contact group
- If the selected contact group is mapped to any other type of contact center, the list of available agent groups includes all agent groups that are not mapped to the selected contact group. Any such contact group can be mapped directly to any agent group present in the available agent group list.

Contact Groups - Agent Groups

The following screenshot shows the Contact Groups – Agent Groups page.



Agent Groups Assignments tab

The Contact Groups - Agent Groups tab allows selection of contact centers of any type. Each AGCC name is shown together with its parent NCC name. The names display in the following format: `NCC Name: AGCC Name`

You can opt to display the descriptive or technical of contact groups and agent groups, by clicking on the Display Descriptive/Technical Names link.

Maintain agent groups-to-contact groups assignments

Start Procedure

1. Select the Contact Groups - Agent Groups tab.
2. Use the filters in the uppermost panel to filter the display of contact groups in the Contact Groups panel. The display shows configured contact groups, the agent groups assigned to them, and the available agent groups.
3. Select a contact groupfrom the left panel. This displays the already assigned agent groups, if any, in the Assigned panel on the right.
   Agent groups that are available for assignment appear in the Available panel. Note that though agent groups associated only with interaction queues or calling lists will appear here, you should not assign these agent groups to a contact group. This is because you cannot assign the interaction queue or calling list to a contact group, and so these agent groups will never appear in the WA dashboard.
4. To move an object between the Available and Assigned panels, check its check box and click on either the up or down arrow between the two panels.
5. Click Save.

Contact Group Details

The Contact Group Details table displays the details of each contact group, including:

- `Name`: The name of the contact group provided by the workforce management system.
- `Source`: The workforce management system that provided the contact groups (for example, Genesys Workforce Management, Aspect eWFM, IEX TotalView) or the Site ID (or the contact center ID) of the contact group from the Genesys Workforce Management. For more information on where this name comes from, see the section on importing contact groups in the Deployment Guide.
- `Group`: The type of contact group (for example, forecast or staff).
- `Active`: Indicates whether the contact group is active or not. The status will be Yes if the last time WA imported that system’s data, the contact group was present in the imported data. The status will be No if the last time WA imported that system’s data, the contact group was not present in the imported data.
- `Include in Rollup`: Indicates whether or not WA should use this contact group when calculating metrics of related business objects, and display this contact group on the dashboard.

Update a contact group

Start Procedure

1. To display the details of a contact group either select from the list or search and select.
2. Type a meaningful name in the Descriptive Name field.
3. Include in Rollup: Check the box to include the contact group in rollups.
In addition to this setting, the contact group must be configured, that is, related to a contact center, application group, reporting region, and/or operating unit.
4. Click Save.
A confirmation message displays and the details display in the table.

Agent Group Configuration

Access in Advisors to agent groups is not configured in Configuration Manager. Advisors dashboard users only have access or not to these objects indirectly, via access to business objects related to them.

Adding/Deleting a New Agent Group in Configuration Manager

Agent groups are added to Advisors by being imported from external data sources, and cannot be deleted.

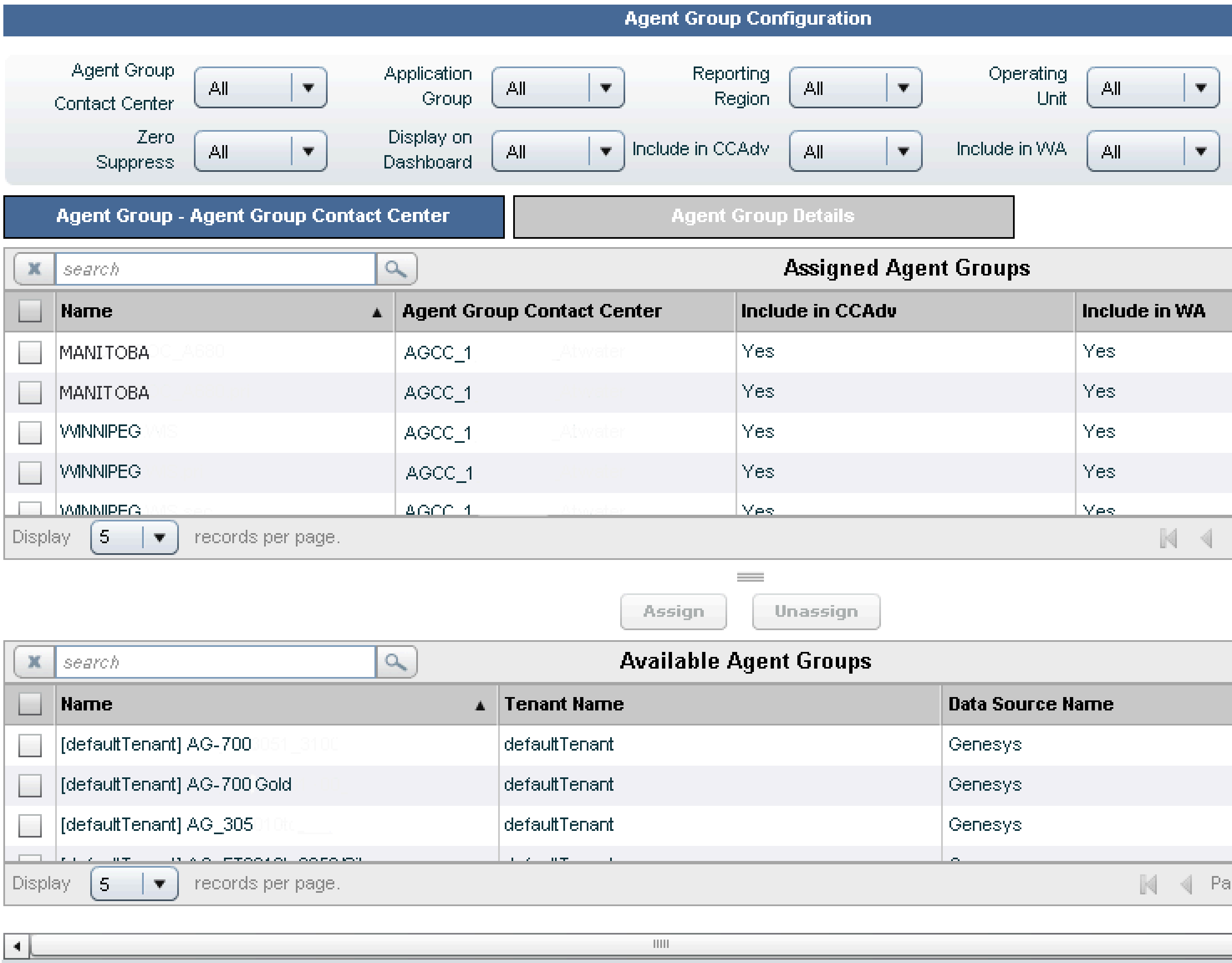
Configuring Agent Group Attributes in Advisors

The Agent Group Configuration page allows you to:

- Assign agent groups to agent group contact centers
- Maintain agent group details

Assigning Agent Groups to Agent Group Contact Centers

The following screenshot shows the Agent Group Contact Center tab.



Agent Group Contact Center tab

To make agent groups available to assign to agent-group contact centers (AGCCs) on this page, the rollups for network contact centers must be configured first. To agent-group contact centers, you assign agent groups that are already related to a network contact center.

An agent group can be assigned to a network contact center through its association to applications on the Applications Configuration page. If an agent group is later removed from the association to the application, the association to the agent-group contact center is removed automatically.

An agent group can be assigned to more than one AGCC. If no contact centers are selected in the contact center drop-down list, the Available Agent Group pane shows all agent groups that are not associated with any AGCC. If a contact center is selected in the contact center drop-down list, the Available Agent Group pane shows all agent groups that are not associated with this particular contact center.

When you are using independent configuration mode, two options are available when assigning:

- Include in CCAdv
- Include in WA

You use these options to specify whether an agent group assigned to an agent group contact center (AGCC) participates in the CCAdv and WA rollups. If you use CCAdv and WA in integrated configuration mode, the default value for both options is Yes, and you cannot edit the options. If, however, you use CCAdv and WA in independent configuration mode, you can specify to the configuration of which application (CCAdv or WA) to add the agent group and its associated AGCC.

Setting the Include in WA agent group rollup property to No automatically removes all mappings of contact groups to this agent group within the associated AGCC. Reverting the Include in WA rollup property to Yes restores previously-added mappings.

For more information about the CCAdv/WA configuration modes, see Configuration Modes.

The names of agent group contact centers display on the page with the corresponding network contact center name and use the format NCC Name: AGCC Name.

Maintain agent groups-to-agent group contact center assignments

Start Procedure

1. Select the Agent Group - Agent Group Contact Center tab.
2. Use the filters in the uppermost panel to filter the display of assigned agent groups in the Assigned Agent Groups panel. To display all assigned agent groups, select All.
   The display shows assigned agent groups and available agent groups.
3. Select an agent group from the Available Agent Groups pane, and click Assign.
   The Assign Rollups window opens.
4. Select the agent group contact center from the drop-down list.
   If you use CCAdv and WA in integrated configuration mode, the Include in CCAdv and Include in WA rollup options are grayed out. If you use CCAdv and WA in independent configuration mode, specify whether the agent group should be included in the CCAdv and/or WA rollups. Select Yes to include it in the rollup, and No to exclude it from contributing to rollup information in the relevant application.
5. Click Assign.

Tip

If you want to map an agent group to an AGCC, and this agent group is already mapped to an AGCC, select the contact center in the uppermost contact center drop-down list and click the `Filter` button to place the agent group onto the Available pane; then you can map it to the selected AGCC.

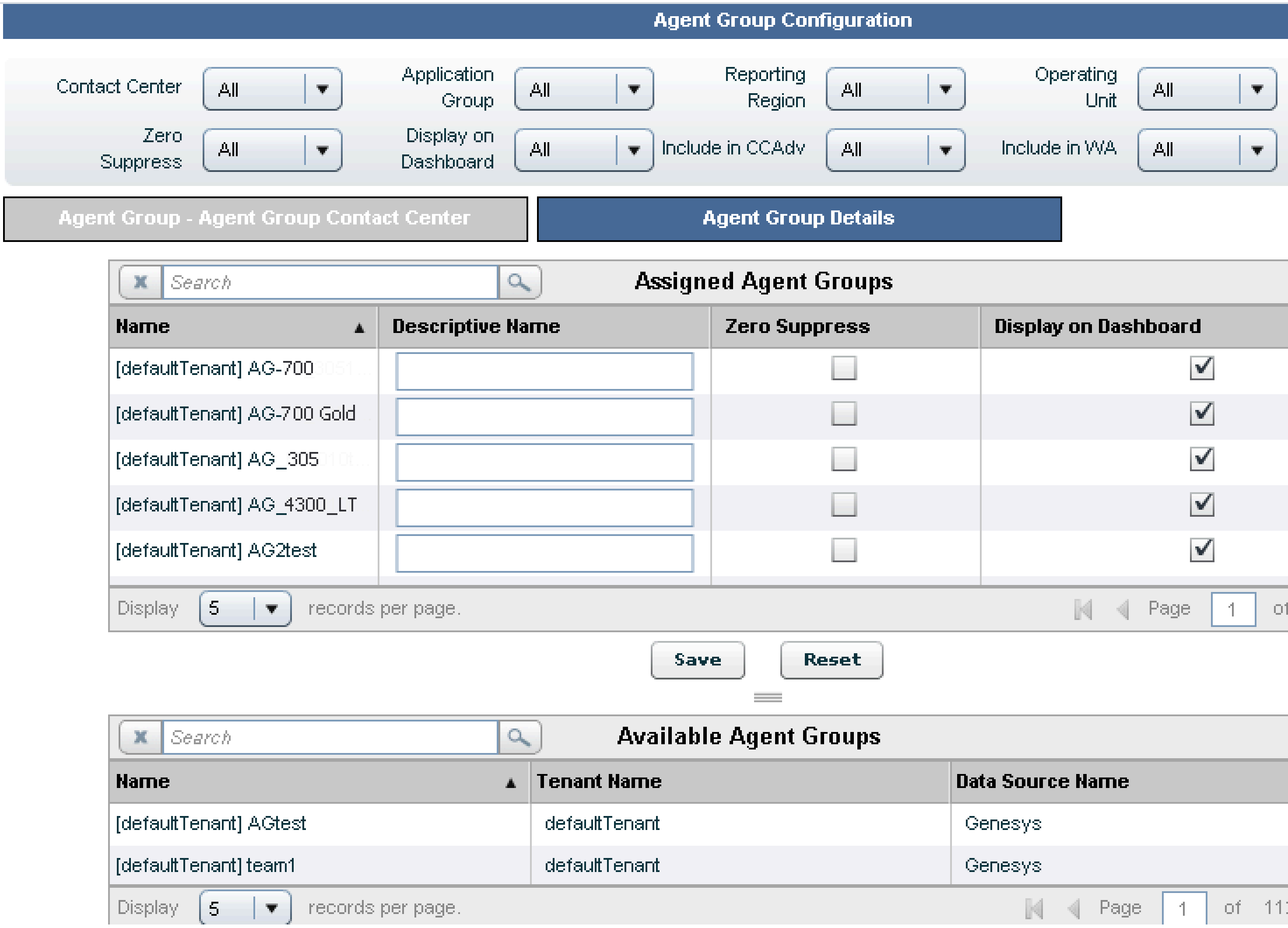
Edit an Agent Group Assignment

Start Procedure

1. Select the Agent Group - Agent Group Contact Center tab.
2. Select an assigned agent group from the list by checking the checkbox.
   You can select multiple agent groups for edit, but the changes you make will apply to all selected applications.
3. Click Edit.
4. Select a new Agent Group Contact Center from the drop-down list, or change your selection to include or exclude the agent group from CCAdv or WA rollups.
   The Include in CCAdv and Include in WA options are grayed out if you use integrated configuration mode.
5. Click Save.

Maintaining Agent Group Details

The Agent Group Details tab allows you to maintain details of agent groups, apart from their primary name. The following screenshot shows the Agent Groups Details tab.



Agent Group Details tab

Maintain agent group details

To maintain details of agent groups, including determining which agent groups can display in the Agent Groups pane on the dashboard.

Start Procedure

1. Select the Agent Group Details tab.

2. Use the filters in the uppermost panel to filter the display of agent groups.
   Filters on the Agent Group Details tab are used exclusively to narrow down the list of agent groups; the filters do not restrict the range of updates or changes you make on the tab. All changes you make to agent group properties on this tab are Advisors-wide; for example, an agent group displays the same descriptive name throughout WA and CCAdv even if it is mapped to multiple aggregated objects. The same applies to Zero Suppress and Display on Dashboard properties: either an agent group is suppressed/hidden or it is not suppressed/not hidden in any view.
3. Select an agent group from the list.
4. Type a descriptive name in the Descriptive Name field.
   The descriptive name will display on the dashboard. If a descriptive name is not provided, the generated name displays on the dashboard.
5. To prevent an agent group from displaying on the dashboard when no current call activity exists, select Yes for Zero Suppress. See Zero Suppression for details.
6. To make the agent group display on the dashboard, select Display on Dashboard.
7. Click Save.
   A confirmation message displays.

Metric Manager

NEW Starting in release 8.5.0, the Metric Manager label in the Administration Module is a section heading, and is not a link to a page. The **Report Metrics** page replaces the Metric Manager of earlier releases.

The Metric Manager section of the Advisors Administration module contains two pages:

- Source Metrics
- Report Metrics

What are Source Metrics and Report Metrics?

A report metric is a metric used in the dashboard of one of the reporting applications. In Advisor release 8.5.0, this refers to a metric used in the dashboard of either Contact Center Advisor/ Workforce Advisor or Frontline Advisor.

A source metric is the definition of the metric in the source system, such as Genesys Stat Server.

See *Terminology* below for detailed definitions.

Custom Metrics Support

Starting in release 8.5.0, you can create and update custom metrics for application, agent group, and agent objects for the Contact Center Advisor and Frontline Advisor.

Restrictions

Creation of new custom metrics for the WA application is not supported.

Access to metrics must be configured by an administrator in Genesys Configuration Manager. Data relating to or dependent on metrics to which a user does not have access permissions does not display for that user. For information about role-based access control (RBAC) privileges related to metric management actions, see CCAdv/WA Access Privileges and FA Access Privileges.

Terminology

The following terminology is used in the descriptions of the **Source Metrics** and **Report Metrics** pages of the Administration module.

- The `Application` object type means the base object types of queue, interaction queue, calling list, call type, or service, for CCAdv.
- A `Raw Report Metric` is a report metric that is created from a source metric. When creating a raw report metric, you must select a source metric. The source metrics available for selection are the Genesys source metrics that are created and maintained using the Source Metric Manager. Only the source metrics that correspond to the object type you selected are available when creating a raw report metric.
- A `Calculated Report Metric` is a report metric expressed as a formula involving one or more raw report metrics as operands. The format options specified for the calculated report metric override any format options specified for the individual raw report metric used to build the calculated report metric. A source metric cannot be directly associated with a calculated report metric.

Source Metrics

NEW You manage source metric definitions from the Genesys Stat Server data source, also called Statistic definitions, in the Source Metric Manager.

You can perform the following actions in the Source Metric Manager:

- View the source metrics.
- Create and edit new custom source metrics.
- Delete custom source metrics.

Fields and options on the **Source Metric Details** page, on which you can create custom source metrics, are dependent on one another. For example, the `Subjects` drop-down list is populated based on your selection in the `Objects` list. As you make selections, other lists, options, and fields update to offer only applicable properties.

Use `Queue` object type source metrics with both ACD queues and virtual queues.

For information about source metrics and source metric attributes, see documentation for the Real-Time Metrics Engine (Stat Server), particularly the Framework 8.1 Stat Server User's Guide and the Reporting Technical Reference.

Customizing the Stat Server CurrentState Source Metrics

New custom source metrics cannot be created for the Stat Server categories of `Current State`, `Current Target State`, and `Current State Reasons`. There are source metrics supplied out-of-box for these categories, and the customization available on these metrics is limited. For example, the Reason Code Key is configurable, but it is not possible to extract agent readiness based on capacity rules for a non-voice channel.

Relationships between Source and Report Metrics

The following Table lists the relationship between the source metrics and the report metrics on the **Report Metrics** page.

If the Genesys Source Metric `Object` field belongs to one of the below object types	Then the Source Metric is Available for this Report Metric Object Type
Agent	Agent
GroupAgents	Agent Group
Queue	Application
StagingArea	Application

If the Genesys Source Metric Object field belongs to one of the below object types	Then the Source Metric is Available for this Report Metric Object Type
CallingList	Application

If you select Queue, StagingArea, or CallingList in the Genesys source metric Object field, then that source metric will be available for selection for application object type report metrics. GroupAgents object type source metrics will be available for selection for agent group report metrics. Agent object type source metrics will be available for selection for agent metrics in Report Metrics manager.

Source Metrics and RBAC

If you have sufficient privileges to see the **Source Metrics** page, then you can view all existing statistics definitions. There is no role-based access control on the individual statistic definitions.

RBAC privileges also manage the following:

- A user’s ability to create custom source metrics
- A user’s ability to edit source metrics
- A user’s ability to delete source metrics

See CCAdv/WA Access Privileges and FA Access Privileges for the list of privileges associated with the Source Metric Manager.

Working with Source Metrics

A custom source metric that you create is immediately available for use in the creation of a report metric.

The source metrics that ship with Advisors (out-of-box metrics) cannot be edited, with the exception of the Reason Code source metric, for which you can edit the following attributes:

- Reason code Key
- Reason Start Overrides Status Start

For users with Edit privileges:

- The Edit button is present and enabled if a selected metric is a custom metric (not an out-of-box source metric).
- The Edit button is absent or disabled if a selected metric is an out-of-box source metric.
- When editing a source metric with dependent report metrics, a warning message indicates that the edit will affect the dependent metric(s).
- You cannot change the category for an existing source metric from Current to Historical, nor the reverse.

The source metrics that ship with Advisors (out-of-box metrics) cannot be deleted. You can delete a custom source metric provided no report metric is derived from it.

For users with `Delete` privileges:

- The `Delete` button is present and enabled if the selected metric is a custom metric (not an out-of-box source metric).
- When attempting to delete a custom source metric that has dependent report metrics, an error message indicates that you cannot delete the metric because of the dependent report metric(s).

Category Options

A statistic category is either a `Current` category or a `Historical` category. The `Current` category is the current value of the evaluated measurement in the Stat Server. The `Historical` category means the metric is evaluated over a specific time interval (the time profile).

JavaCategory source metrics can be either `Current` or `Historical`; you can specify which to use based on your requirements.

Main Mask/Relative Mask Wild Cards

Wild cards such as * to select all options or ~ to exclude a mask are implicitly supported in the `Main Mask` and `Relative Mask` editing windows. Use the `Select All` feature at the bottom of the editing window to select all options and then selectively deselect one or more options with the radio buttons.

For example, if `MainMask = *, ~LoggedOut`, do the following in the `Main Mask` editing window:

1. Use `Select All: Selected` to select all the options in the window.
2. Click the `LoggedOut` radio button to deselect it.

Filtered Source Metrics

When you select a source metric on the **Source Metrics** page, the attributes for that metric are displayed in the lower half of the page, including the `Filtered Source Metrics` table in which you can create a filter for the metric.

To apply a filter to a selected metric, specify the following in the `Filtered Source Metrics` table:

- Name of the filter
- A description for the filter
- The filter: A filter must be one that is available in the Configuration Server **Business Attributes** > **Advisors Filters** section.

You can add as many filters to an unfiltered source metric as you require; each filtered version becomes a new source metric.

You can edit filtered source metric properties. You can also delete a filtered source metric if no report metric is using a filtered variation. This includes filtered source metrics defined on out-of-box metrics;

they can be edited or deleted.

Each filtered variation is stored on a database table separate from the source metric table.

Finding Filtered Source Metrics in the Source Metrics Manager

Filtered source metrics are variations of other parent source metrics; you can find the filtered source metrics only under the respective parent source metric. For example, to find the filtered variations of a source metric called `Retrieved Calls`, navigate to the `Retrieved Calls` source metric and select it. The filtered variations are displayed in the details in the lower half of the page.

Customizing the Stat Server Current Target State Source Metrics

Starting in release 8.5.001, you can create custom source metrics for the Stat Server category of `CurrentTargetState`.

In release 8.5.0, the following out-of-box metrics were available in the Metric Manager, and were evaluated from the Current Target State source metric. In release 8.5.001, these metrics based on Genesys Stat Server data are no longer shipped with Advisors because you can create your own custom metrics based on the Current Target State metric.

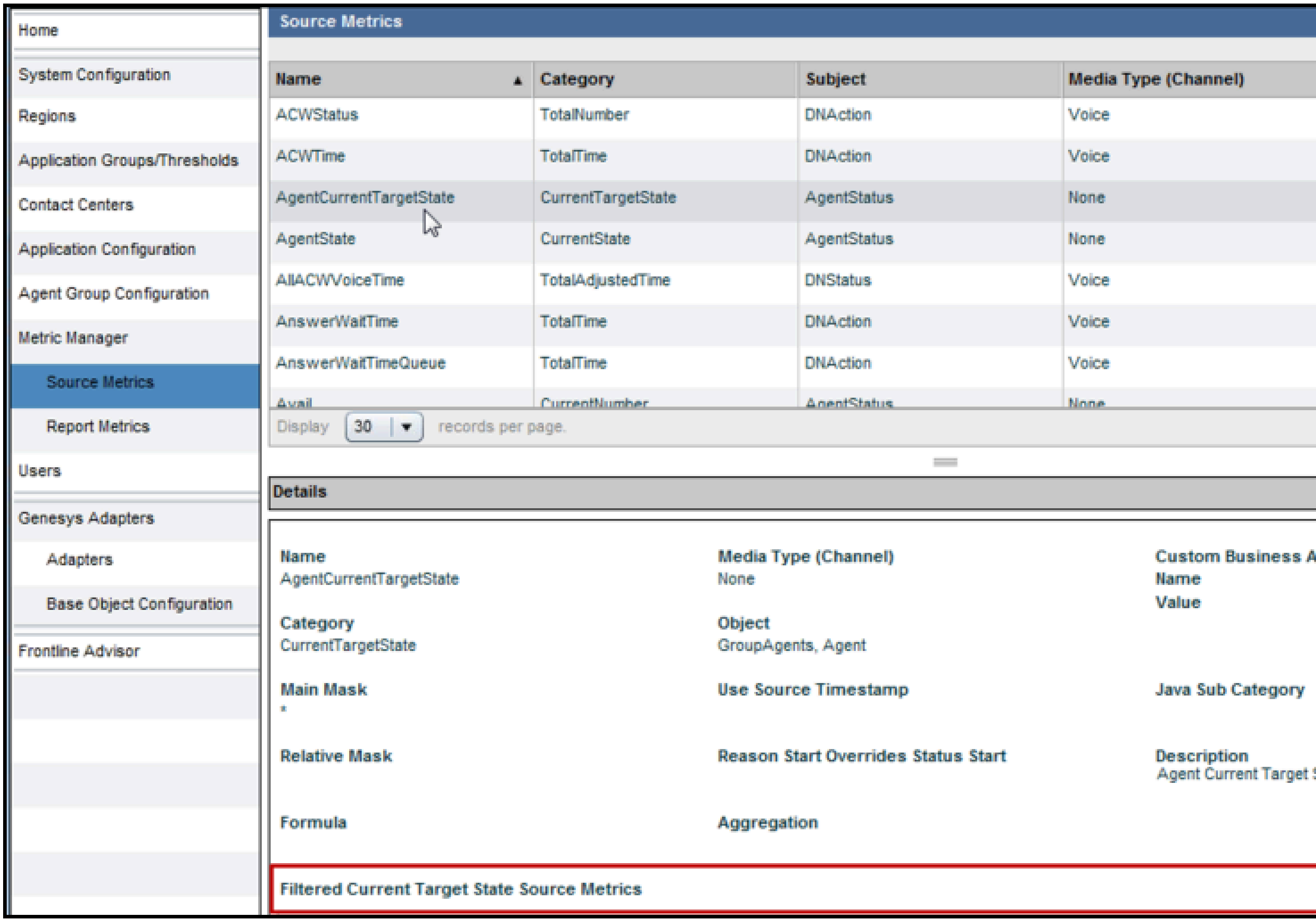
Object Type	Report Metric	Reporting Application
Application	Avail Voice	CCAdv
Agent Group	Avail Voice	CCAdv
Agent	Voice Ready	CCAdv
Agent	Voice Ready	FA

Creating a Custom Source Metric for the CurrentTargetState Category

In release 8.5.001, Advisors Genesys Adapter can extract agent media-capacity information from the default (out-of-box) Current Target State source metric. An example of media-capacity is the maximum number of chat interactions that an agent can handle simultaneously.

You use the default Current Target State source metric that is supplied with Advisors and the **Filtered Current Target State Source Metrics** section of the Source Metrics Manager to configure your specific Current Target State attributes. The default (out-of-box) Current Target State source metric supports both agent and agent group object types.

Click the **Edit** button in the **Filtered Current Target State Source Metrics** section of the Source Metrics Manager for the Current Target State source metric.



The **Create** dialog box – instead of presenting filters – offers the following attributes:

- Type (that is, the Current Target State attribute type; only Media Capacity is available in release 8.5.001)
- Capacity Media Type
- Capacity Attribute

All media types registered in the Genesys Configuration Server under **Business Attributes > Media Types** are listed under the **Capacity Media Type** option.

The following options are available for **Capacity Attribute**:

- Routable Interactions Count (also known as Current Margin Count)
- Maximum Interactions Count
- Current Interactions Count

Create an enabled raw report metric for either CCAdv or FA based on each of the source metrics with the filtered media capacity attribute. You can create a raw report metric to display on the dashboard, or you can use the raw report metric to create other calculated report metrics.

Current Target State Metrics and Agent Groups

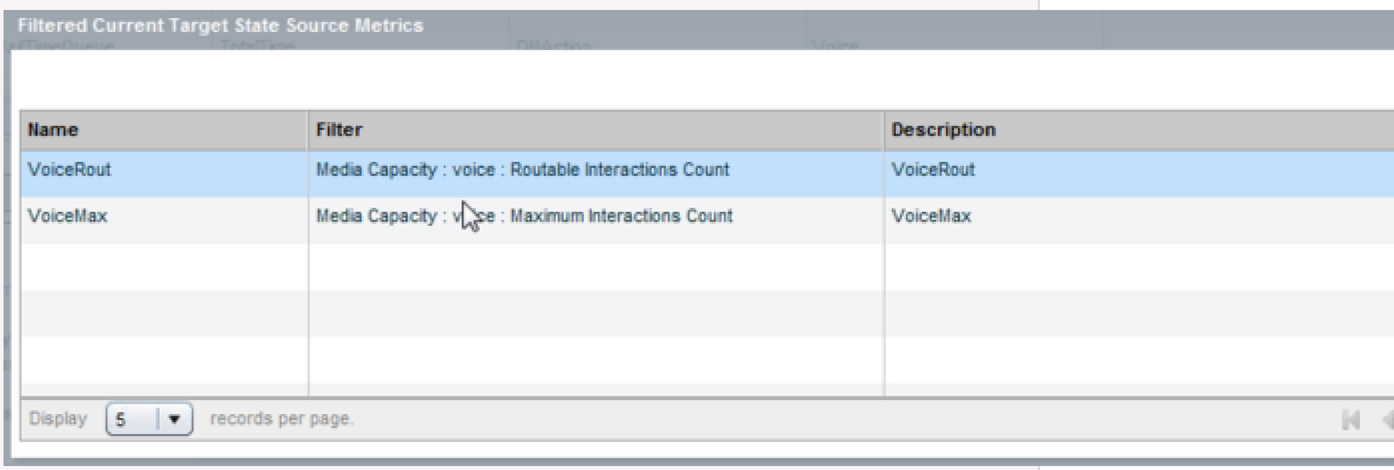
When the Current Target State metric is reported, AGA extracts the configured media capacity attributes for each agent in an agent group. The corresponding metric at the agent group level is evaluated based on the media capacity attribute at the agent level. Therefore, for all the media capacity attributes that Genesys supports in release 8.5.001, a formula of **SUM** is used to evaluate the agent group level metric value from the agent level attribute value.

Current Target State Metrics and Metric Applicability

You can configure metric applicability for the custom Current Target State report metrics in the same way that you configure applicability for any other raw report metric.

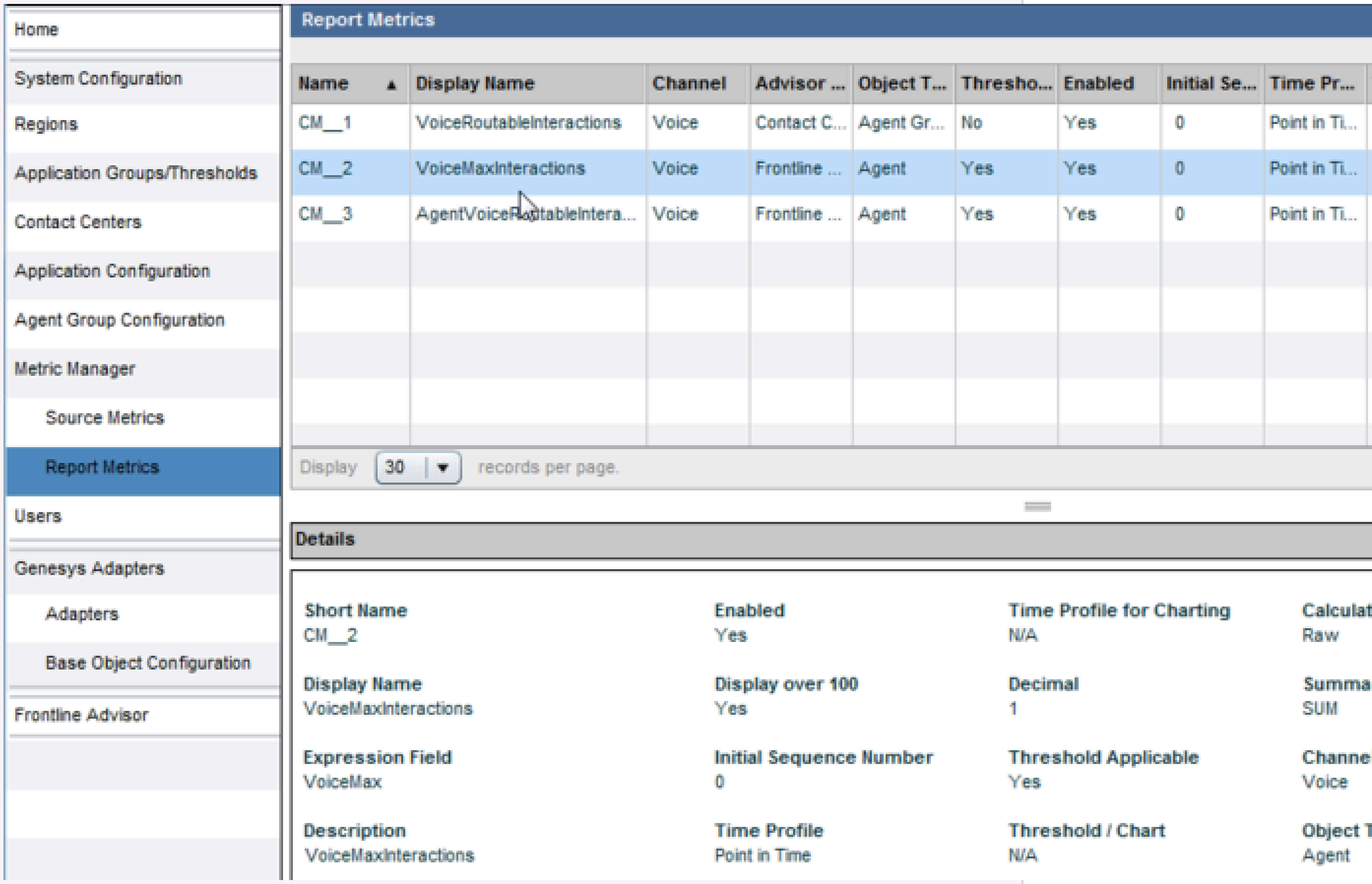
Example: Using Metrics Based on Current Target State

While an agent might manage many chat or email interactions simultaneously, that same agent can typically manage only one voice interaction at a time. To track an agent's availability for routable voice interactions using metrics on the dashboard, you could create report metrics based on the Current Target State metric that ships with Advisors. For example, the following screenshot shows two custom source metrics – VoiceMax tracks the maximum number of voice interactions for an agent and VoiceRout tracks the availability of the agent to handle a voice interaction.



Custom source metrics based on the out-of-box Current Target State source metric

You would then create custom raw report metrics that use those custom source metrics as the foundation. The following screenshot shows an example of custom report metrics.



Custom report metrics that use the previously-created Current Target State–based source metrics

After you create and save the enabled custom report metrics, they are available in the Advisors column chooser so you can display the metrics on the dashboard. In this example, which uses the Frontline Advisor dashboard, the custom report metric that tracks an agent's availability to take calls is the AgentVoiceRoutableInteractions metric. The VoiceMaxInteractions metric tracks the maximum number of voice interactions (calls) an agent can handle simultaneously.

The following screenshot shows one ready agent (J. Davis) and two logged-off agents. Note that the AgentVoiceRoutableInteractions metric indicates that only the agent in the Ready state is available for a voice interaction.

TEAM

AG100

Agent Name	Average Handle 10Min	Alert State	Login Time	Calls Handled 10Min	Reason Code	Call Type	Current Skill	State	Time In Curren
J. Davis	0		09:18:02 AM 0...	0	N/A	-	-	Ready	34:07
F. Craig	0		07:00:00 PM 1...	0	N/A	-	-	Logged Off	5523:28
J. Miller	0		07:00:00 PM 1...	0	N/A	-	-	Logged Off	5523:28

An agent in the Ready state is available to take a call. The AgentVoiceRoutableInteractions metric has a value of 1 for the a VoiceMaxInteractions metric indicates that the agent can handle a maximum of 1 call at any ~~one~~ time.

If that agent should take a break, or be on the phone, the AgentVoiceRoutableInteractions metric indicates that the agent is no longer available for any further calls.

TEAM

AG100

Agent Name	Average Handle 10Min	Alert State	Login Time	Calls Handled 10Min	Reason Code	Call Type	Current Skill	State	Time In Curren
J. Davis	0		09:18:02 AM 0...	0	Break : 1012 (...	-	-	Not Ready	00:01
F. Craig	0		07:00:00 PM 1...	0	N/A	-	-	Logged Off	5524:28
J. Miller	0		07:00:00 PM 1...	0	N/A	-	-	Logged Off	5524:28

An agent in the Not Ready state is unavailable to take a call. The AgentVoiceRoutableInteractions metric has a value of 0 fo

TEAM

AG100

Agent Name	Average Handle 10Min	Alert State	Login Time	Calls Handled 10Min	Reason Code	Call Type	Current Skill	State	Time In Current
J. Davis	0		09:18:02 AM 0...	0	N/A	-	-	Talking	00:00
F. Craig	0		07:00:00 PM 1...	0	N/A	-	-	Logged Off	5525:38
J. Miller	0		07:00:00 PM 1...	0	N/A	-	-	Logged Off	5525:38

An agent in the Talking state is unavailable to take a call. The AgentVoiceRoutableInteractions metric has a value of 0 for th

Report Metrics

Report Metrics Overview

NEW With the correct role-based access control (RBAC) permissions, you can view and edit all Contact Center Advisor, Workforce Advisor, and Frontline Advisor metrics on the Report Metrics page. Only certain attributes are editable.

You can customize the out-of-box metrics that ship with Performance Management Advisors to address your specific Contact Center performance and service quality measurements. You can also use the Report Metrics page to create custom metrics for the dashboard.

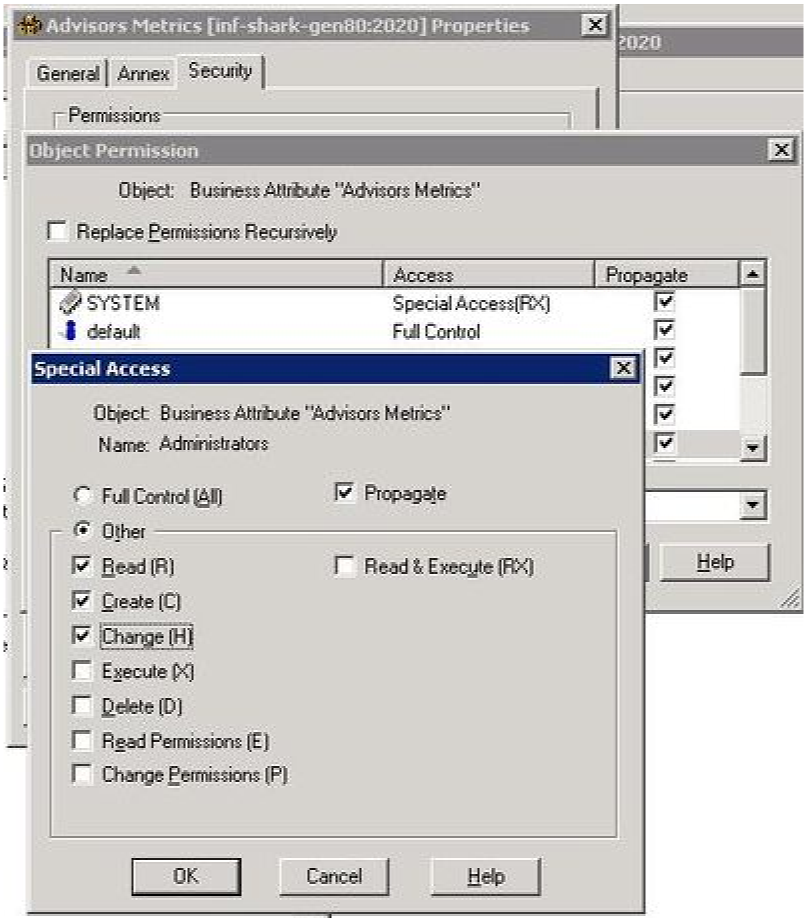
You can search by metric name or description in all supported languages, regardless of the language you selected at login.

Any changes that you make using the Report Metrics page are logged in the audit log file, similar to all other logged administrative actions.

Custom Agent Group Metrics and the CCAdv Totals & Averages Row

Genesys does not provide an equivalent agent-level metric for a custom CCAdv agent group metric; therefore, de-duplication on the `Totals & Averages` line is not supported for custom agent group metrics.

Role Based Access Control and the Metric Manager



The Report Metrics manager functionality is controlled by privileges and permissions (Role-Based Access Control). A privilege determines the actions a user can perform. A permission grants or denies viewing of individual metrics for a user. In the Report Metrics Manager, the view, create, copy, edit, and delete actions are individually controlled by privileges. For information about Metric Manager–specific privileges, see CCAdv/WA Access Privileges and FA Access Privileges.

Use the following information if you are granting or denying Metric Manager–related permissions and privileges to users:

- A user can view all the metrics to which he or she has a "read" object permission.
- A user who can create a custom metric can also view and delete that metric, unless View permission or the Change permission to the metric was explicitly denied in the Configuration Server after the user created the metric.
- To create custom metrics, a user must have a Create security permission granted on the Advisors Metrics Business Attributes section in Configuration Manager. Without this permission, the user cannot create custom metrics. Similarly, a Change permission must be granted at the root attribute level or at the individual metric attribute value level to ensure the user can delete an existing custom metric. For an example of this configuration, see the Figure on the right.

Editing Out-Of-Box Metrics

You cannot delete Advisors' out-of-box metrics, but you can edit some of the properties. The display name, description, and the reporting application–specific formatting properties can be edited. You can also edit the following properties of metrics that have them:

- Time Range upper bound/lower bound (if applicable to the corresponding source metric)
- Notification mode and frequency
- Insensitivity
- Exclude Base Object filter
- Enabled

Creating Custom Metrics

You can create custom metrics using the **Report Metrics** page. Custom report metrics are created from Genesys Stat Server source metrics. The **Report Metrics** page is based on the Metric Manager of earlier releases, but, starting in release 8.5.0, includes additional functionality.

> **Important**
> You can create only custom application and agent group metrics for CCAdv, and custom agent metrics for FA. You cannot create custom metrics for any other types of objects. For example, you cannot create custom metrics for contact groups.

There are two some key selections you must make when you create a custom report metric:

- Select an Advisors application
- Select the object type

The **Report Metrics** page then shows the relevant custom metric configuration properties based on the Advisors application and object type you select.

You must provide an expression for the metric (that is, a formula that produces a metric value). Expressions can contain other metrics and constants (numbers) as operands, as well as the operators, functions, constructs, and symbols described in the following Table. Supported operands are included as buttons in the `Expression Editor` on the **Report Metric Details** page.

The elements of expressions are limited to existing standard or custom source metrics provided by the Genesys Adapter, source metrics imported from the CISCO environment, and existing CCAdv application, CCAdv agent group, and FA agent dashboard metrics.

Metric Type	Acceptable Operands
Calculated custom report metrics	Arithmetic operators:

Metric Type	Acceptable Operands
	• + (addition) • – (subtraction) • * (multiplication) • / (division) Brackets (to ensure the required operation sequence) You can also include the >, < , and = operators in expressions.

Example: Expression Field Entries

The following examples demonstrate valid formulas you can enter into the Expression Field. If you have multiple operands in the expression, it is important to use parentheses to group the calculations.

- Custom metric is a sum: Enter (<Metric1>+<Metric2>). For example, (CallsAnsweredTo5+RouterCallsAbandQTo5).
- Custom metric is a percentage-based metric: Enter 100*(<Metric1>/<Metric2>). For example, 100*(RouterCallsQNow/STF). For this type of expression, you must start the expression with the `100*` component followed by the metric calculation, as shown in the example.
- Custom metric measures the longest value for an activity or state: Enter (DateTime - <AgentGroupMetric>). For example, (DateTime - RouterLongestCallQ)

Propagating custom metric changes to the Stat Server

If you create a new custom metric, or make changes to an existing metric that must be propagated to the Stat Server, these changes are applied during the overnight refresh. The dashboard shows values for any newly-added custom metrics only after the changes have been applied. This is applicable to both CCAdv/WA and FA metrics.

Enabling a disabled metric or disabling an enabled metric is applied to the Stat Server during the overnight refresh.

Metric Groups

Every raw custom report metric must be assigned to a Metric Group. This is not applicable to calculated report metrics; you do not assign them to metric groups.

A metric grouping indicates applicability of metrics to configured objects, which determines if metric statistic(s) must be requested for a certain object. See the *Working with Metric Groups* page for an example.

The default selection for a new metric is the `Default` metric group. When creating a custom metric, you can assign the metric to another available metric group. You also have the option to create a new metric group and assign the report metric to that new group.

After you create a metric group, it is available for selection for subsequent metric grouping. The metric group information for a report metric is not stored in the Genesys Configuration Server.

See the *Working with Metric Groups* page for more information about the metric groups and how to manage them.

Working With Metrics

<tabber>

Metric Properties Descriptions=

The following Table provides descriptions of the metric properties.

Property	Advisors Application	Object Types	Editable For	Description
Short Name	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	None	The name of the metric that uniquely identifies it for internal purposes. This field is system generated. You can only view this property; you cannot edit it.
Language	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	A drop-down list that includes supported languages for your release. English is the default value. Your selection for this parameter controls the language property for the metric display name and

Property	Advisors Application	Object Types	Editable For	Description
				description.
Display Name	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	The name used for display in the column chooser and dashboard. The name must be unique for a given channel. The display name property accepts 128 characters or less. The default language of the display name is English, but you can specify the name in another supported language using the Language parameter in the Metric Manager.
Description	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	The metric description. The default language of the description is English, but you can specify the description in another supported language using the Language parameter in the Metric Manager.
NEW Advisor Application	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	A drop-down list with values representing each supported reporting application. The default value is Contact Center Advisor. Your choice of reporting application is reflected in the values available for the `Object` Type parameter.
Object Type	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application	Custom Metric	A drop-down list containing the options available for the Advisor

Property	Advisors Application	Object Types	Editable For	Description
		WA: Contact Group		Application you selected. For example, if you selected Contact Center Advisor as the Advisor Application, `Application` is one of the options in the `Object` Type list.
Calculation	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	Formerly `Metric` Type. Select a radio button to indicate if the custom metric is Raw or `Calculated`.

Summary Type	FA, CCAdv, WA	FA: Agent
		CCAdv: Agent Group or Application
		WA: Contact Group
			Custom Metric	A drop-down list containing options that determine how aggregation is to be performed when rolling up the metric to the higher level of the hierarchy:
				• When the metric type is Raw, the options are:
				  • SUM
				  • MIN
				  • MAX
				• When the metric type is `Calculated`, `Summary Type` is not applicable (None).

NEW Metric Group	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	For a custom metric, a drop-down list with values for all available metric groups. There is one available value "out-of-box"

Property	Advisors Application	Object Types	Editable For	Description
				– `Default`. To create your own metric group, click `Create New Metric Group`. On confirmation, the new metric group name is appended to the list of metric groups, and is automatically selected in the drop-down. The new metric group value is saved as part of the custom metric creation process, and is subsequently available for selection for other metrics. The metric group name is case-sensitive. A metric group labelled `MG` is a different metric group from one labelled `mg`.
Enabled	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	Formerly `Display on Column Chooser`. Select a radio button to specify whether the metric displays in the Column Chooser (Enable) or not (Disable). Disabling a raw report metric means that the corresponding source metrics are not collected at the data source for the respective reporting application. In the case of Genesys Stat Server, you can reduce the load on the Stat Server by disabling unused metrics for a reporting application. However, note that each raw report metric is evaluated in two cases:

Property	Advisors Application	Object Types	Editable For	Description
				1. when directly enabled 2. when indirectly enabled by its participation in the calculation of another enabled metric Therefore, to completely disable a raw report metric so it is not collected at the data source, you must both disable the metric and ensure it is not used in the calculation of another metric that is enabled. You can re-enable any disabled metric by updating the `Enabled` checkbox. Disabling or enabling raw report metrics takes effect on overnight refresh or on restart. Disabling a metric for Contact Center Advisor means that CCAdv does not calculate the metric or send values for it to the dashboard. The effect of disabling takes place at the start of the next Short processing cycle in CCAdv XML Generator.
Channel	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	Custom Metric	A drop-down list containing options to specify the media channel type for which the custom metric is shown in the Column Chooser and on the dashboard.
Decimal	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All	A drop-down list containing options you can use to specify the number of decimal places to display for metric values.
Initial Sequence	FA, CCAdv, WA	FA: Agent	All	Formerly Sequence

Property	Advisors Application	Object Types	Editable For	Description
Number		CCAdv: Agent Group or Application WA: Contact Group		`Number`. Use this parameter to specify the initial column order sequence in which to place the metrics on the dashboard. Clicking `Reset` in the dashboard's Column Chooser displays the metrics with a sequence number, in the order specified by the number.
NEW Reorder Columns	FA	Agent	Custom metric	By default, the checkbox is cleared. Select the check box to allow users to re-order the column positions on the dashboard.
Threshold Applicable	CCAdv, WA	CCAdv: Application WA: Contact Group	All	Formerly `Threshold`. When creating a custom metric, the checkbox is cleared by default. If this box is checked, you can define thresholds for the metric on the **Application Groups/ Thresholds** page. If this box is cleared, then you will not be able to define thresholds on that page.
Threshold/Chart	CCAdv, WA	CCAdv: Application WA: Contact Group	All	Enter values for the threshold range (minimum and maximum). These values also determine the y-axis values in a graph.
Display over 100%	CCAdv, WA	CCAdv: Application WA: Contact Group	All	A format option. When creating a custom metric, the checkbox is

Property	Advisors Application	Object Types	Editable For	Description
				selected by default. A checkmark in the box indicates that values over 100 display actual values. If the checkbox is cleared, values over 100 display as 100+.
NEW Format Pattern	FA	Agent	All	A drop-down list containing options to specify the general structure of the metric. The default selection is `Number`.
Time Profile	FA, CCAdv, WA	FA: Agent CCAdv: Agent Group or Application WA: Contact Group	All, but with qualifications: • CCAdv/WA: Fully editable for custom metrics. For out-of-box metrics, you can enable or disable charting only. • FA: You can enable or disable the time profile only.	Select a radio button to indicate if the time profile is `Point in Time` or `Historical`. `Point in Time` on the **Metric Details** page is the same as `Now` elsewhere in the products: it is the `Current` time profile with a duration of 0. NEW Starting in release 8.5.001, you can assign a time profile group (Short, Medium, or Long) to a point-in-time custom report metric for an application or agent group in the Time Profile section. The time profile interval and time profile type are not shown for the point-in-time metric. XML Generator creates alerts only for metrics that are mapped to the Short time profile group. If you select the `Historical` time profile, available additional options are dependent on the Advisors component with which the metric is associated:

Property	Advisors Application	Object Types	Editable For	Description
				• CCAdv: When you select the `Historical` radio button, you can configure up to three time profiles in the `Time Profile` table. You must specify at least one. Use the `Enabled` checkbox to enable and disable CCAdv metrics by time profile. The allowed time interval for an enabled profile is from 1 minute to 24 hours. The default time intervals are: • 5 minutes for a Short group • 30 minutes for a Medium group • 24 hours for a Long group Metrics that are used in formulas for calculated metrics must have time profiles that are compatible with the calculated metric. For each enabled time profile,

Property	Advisors Application	Object Types	Editable For	Description
				you must also indicate the time profile type (`Sliding` or `Growing`). The default type for each time profile group is: • Sliding for a Short group • Growing for a Medium group • Growing for a Long group The `Chart` checkbox is available for CCAdv application-type metrics. The checkbox is cleared, by default. • WA: The `Chart` checkbox is available for WA contact group–type metrics. The checkbox is cleared, by default. • NEW FA: Starting in Advisors 8.5.001, you can enable and disable metrics for FA by time profile in the `Time Profile` table; you can specify which metrics are

Property	Advisors Application	Object Types	Editable For	Description
				enabled for a given time profile and disable metrics that are not required for that time profile. The time profile durations displayed in the `Time Profile` table are those that are configured in the FA administration page. You cannot edit the time profiles in the Report Metrics manager; you continue to configure and edit the FA time profiles in the FA administration page. To enable a time profile for a specific metric, both of the following conditions must be true: • the time profile is enabled at the application level (that is, on the `Settings` tab of the FA administration page)

Property	Advisors Application	Object Types	Editable For	Description
				• the time profile is enabled for that metric in the Report Metrics manager To disable a time profile, you need to disable the time profile in only one of the preceding locations. The results of enabling a time profile for a particular metric are the following: • The metric is available in the column chooser and dashboard for display for its enabled time profiles. • The aggregation engine calculates the metric for the enabled time profiles. **Important** You can enable or disable time profiles for calculated metrics irrespective

Property	Advisors Application	Object Types	Editable For	Description
				of their associated operand-level metrics. The disabled time profile for the operand-level metric impacts only the visibility of that metric on the dashboard. FA time profile durations cannot be configured on a per-metric basis, therefore, calculated metrics are limited to the time profiles configured in the FA administration page. Default settings are: • all of the time profiles for the out-of-box metrics are enabled in the Report Metrics manager • only the first time profile in the `Settings` tab of the FA administration page is enabled (consistent with previous

Property	Advisors Application	Object Types	Editable For	Description
				releases). Changes to time profile settings in the FA administration page are automatically updated in the Report Metrics manager. However, enabling or disabling time profiles for FA metrics in the Report Metrics manager require you to reload the FA hierarchy before the changes are propagated to the FA application; you can reload the hierarchy manually, or wait for the overnight refresh.

Expression Editor

Use the Expression Editor to build the formula that produces a value for your custom metric.

Property	Description
Channel and Metric tables	Use the Channel and Metric tables to find existing metric expressions that you can use in the calculation of your new custom metric. The entries from the list of metrics serve as operands for building the expression. When creating a raw report metric, the operands available are source metrics. And when creating a calculated report metric, the operands available are other raw report metrics and other calculated report metrics.
Metric Description	When you select a metric in the Metric table, a description of that metric displays in the Metric Description box.
Expression Field	You build the expression, or formula, for your custom metric in the Expression Field. Use the buttons above the field to add operands to the expression of a calculated metric. You might see two expression fields for some agent group metrics. This happens when the calculation for individual agent groups is different from the totals and averages calculation. If you are creating a custom agent group metric, you can specify only one calculation expression to be applied in both individual agent groups and totals and averages calculations. You might see two expression fields for some agent group metrics. This happens when the calculation for individual agent groups is different from the totals and averages calculation. If you are creating a custom agent group

Property	Description
	metric, you can specify only one calculation expression to be applied in both individual agent groups and totals and averages calculations.
NEW Notification Mode	Available for raw metrics and only when the selected source metric belongs to a Genesys Stat Server data source. See the Stat Server User Guide for more information. Select a value from the drop-down list. The default value is Time Based. This means that Stat Server will notify the adapter periodically based on the notification frequency. Changed Based means that the Stat Server will notify the adapter as soon as the values change in Stat Server.
NEW Notification Frequency	Available for raw metrics and only when the selected source metric belongs to a Genesys Stat Server data source. See the Stat Server User Guide for more information. Specify a non-negative integer. The default value is 0. This field is enabled only when the notification mode is Time Based.
NEW Insensitivity	Available for raw metrics and only when the selected source metric belongs to a Genesys Stat Server data source. See the Stat Server User Guide for more information. Specify a non-negative integer. The default value is 0, which indicates that insensitivity is not applied.
NEW Exclude Base Object Filter	Available for raw metrics and only when the selected source metric belongs to a Genesys Stat Server data source. `Exclude base object filter` is a property of the statistic template. See the Stat Server User Guide for more information. The checkbox is available for Contact Center Advisor application and agent group metrics. Select the checkbox to exclude the base object configuration filter when statistics are requested for the metric. The checkbox is cleared, by default. **[+] Additional information about Exclude Base Object Filter** When a Genesys Stat Server filter is combined with an agent group or a queue, and the combination is published on the CCAdv administration module's Base Object configuration page, the statistic for any metric for which you opted to exclude the base object filter is requested, but without the object configuration filter. The same base object configuration filter is applied on all the statistics that are requested for a given source object. All *out-of-box* CCAdv application metrics are configured to include this object configuration filter. However, because the configured filter is applied to all the statistics, there will be circumstances when you must exclude some of the metrics from being subjected to this "blanket" filter. For example, on the agent state –based agent group metrics, you should not apply an interaction-based filter; it could result in incorrect results. In such cases, you use this property to specify which metrics to exclude from the filter. For example, the out-of-box interaction queue metrics and the calling list metrics are configured to exclude the base object filter. On the CCAdv dashboard, each filtered combination displays on a separate line. Any metric that is excluded from the base object configuration filter is

Property	Description
	shown on a separate line as an unfiltered metric for the selected agent group or queue. The Exclude Base Object Filter property does not influence the Stat Server filter that is specified at the source metric level. The property in Metric Manager is called the base object filter to help you distinguish between the Stat Server filter that is applied on the filtered source metric, and the Stat Server filter that is applied at the base object level. It is possible that both of the above filters (the metric filter and the object configuration filter) must be applied to a certain metric. In such cases, the filters are combined; both filtering conditions must be met for a statistic value to be reported for that metric.
Time Range Lower Bound and Time Range Upper Bound	The Time Range Lower Bound and Time Range Upper Bound fields are enabled for raw metrics, and only when the selected source metric is based on a category that requires a time range. For example, TotalNumberInTimeRange. Available for CCAdv raw report metrics only. Specify a non-negative integer. The upper bound must be greater than the lower bound. The default value is 0.

|-| How To...=

View Information about a Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.
- You require permission to view at least one metric.
  The **Report Metrics** page displays only the metrics to which you have Read permission in the Configuration Server.

Start Procedure

1. In the Administration module, click **Report Metrics** in the navigation pane.
2. Locate the metric for which you want to view detailed information.
   To assist you when searching for a specific metric, use the filters on the right side of the page to reduce the number of metrics that display. By default, all filters are selected.
   Use the page navigation arrows under the list of metrics to move between pages of metrics. By default, the metrics are displayed in alphabetical order.
3. Click a metric to select it.
   Details about the metric display at the bottom of the **Report Metrics** page.

Create a Custom Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.
- You require the `Create` permission in the Configuration Server for the Advisors Metrics Business Attribute on the default tenant.
- You require the privilege that grants you access to the `Create` button.

Start Procedure

1. In the Administration module, click **Report Metrics** in the navigation pane.
2. Click New.
   The **Metric Details** page opens.
3. Enter information to define the new metric. Ensure you enter information into all required fields.
   For descriptions of the metric properties, see the **Metric Properties Descriptions** tab on this page.
4. If you want to return the **Metric Details** page to the default settings, click `Reset`.
5. Click Save to save the metric.
   If you entered all information correctly, the page returns to the **Report Metrics** page. The new metric displays in the list of metrics.

Copy a Metric to Create a Custom Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.
- You require the `Create` permission in the Configuration Server for the Advisors Metrics Business Attribute on the default tenant.

- You require permission to view the metric that you want to copy.
- You require the privilege that grants you access to the Save as option.

Start Procedure

1. In the Administration module, click **Report Metrics** in the navigation pane.
2. Select the custom or standard metric that you want to use as a template for a new custom metric.
   You can use application or agent group metrics as templates for new CCAdv custom metrics, and agent-level metrics for new FA custom metrics.
   If you select a standard dashboard metric as a template for a new custom metric, the expression of the original standard metric might not be supported in the new custom metric. You must edit the calculation to limit operands to those supported by the custom dashboard metric creation process.
3. Click the Save as... option.
   The **Metric Details** page opens.
4. Edit information to define the new metric. Ensure you enter a new display name for the new custom metric. Ensure you enter information into all required fields.
   For descriptions of the metric properties, see the **Metric Properties Descriptions** tab on this page.
5. Click Save to save the metric.
   If you entered all information correctly, the page returns to the **Report Metrics** page. The new metric displays in the list of metrics.

Edit a Metric

You cannot edit the short name for a metric (this includes custom metrics).

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.
- You require permission to view the metric that you want to edit.

- You require the privilege that grants you access to the `Edit` option.

> **Important**
> You require the `AdvisorsAdministration.MMW.canEdit` privilege to edit metrics, but a Change permission is not required in the Configuration Server for the metric business attribute value because none of the edited information is updated on the Configuration Server after the initial creation of the business attribute value.

Start Procedure

1. In the Administration Module, click **Report Metrics** in the navigation pane.
2. Select an existing metric to edit.
3. Click `Edit`.
   The Metric Details page opens.
4. Edit the metric properties.
   The metric properties you can edit are dependent on the type of metric you selected to edit. Your ability to edit standard (out-of-the-box) metrics is limited. For example, the expression editor is always disabled for standard metrics. If you want to edit a standard metric, you must copy the metric and save it as a new custom metric.
   If you change the display name or description of a metric, the information is updated in Advisors only and is not propagated to the Configuration Server.
5. Click Save to save the metric.
   If you entered all information correctly, the page returns to the **Report Metrics** page. The metric displays in the list of metrics.

Delete a Custom Metric

Prerequisites

- You require the privilege that grants you access to the Administration module and the privilege that grants you access to the Metric Manager to perform this procedure.

- You require permission to view the metric that you want to delete.
- You require a Change permission in the Configuration Server for the business attribute that represents the metric that you are deleting.
- You require the privilege that grants you access to the `Delete` option.

> **Important**
> Deleting a custom metric deletes the record in Advisors and also deletes the business attribute value under the Advisors Metrics Business Attributes section in the Configuration Server.

Start Procedure

1. In the Administration module, click **Report Metrics** in the navigation pane.
2. Select a custom metric to delete.
3. Click `Delete`.
   If a raw report metric is used in a calculation for a calculated report metric, you cannot delete that raw report metric. If you attempt to delete a metric that is used in another metric calculation, Advisors displays an error message.

Enable Graphing of Metrics

The Metric Graphing window is accessible from both Contact Center Advisor and Workforce Advisor. You specify which combination of metrics and time profiles to graph using the `Chart` checkboxes in the `Time Profile` table.

You can choose to graph Application-type metrics in CCAdv, and Contact Group-type metrics in WA.

Use the `Edit` option associated with the metric on the **Report Metrics** page, or the `Create` button, to open the **Metric Details** page. On the Metric Details page, navigate to the Time Profile.

To enable a metric and time profile for graphing, choose the time profile and select the `Chart` checkbox beside it. Each metric that can be graphed can have more than one time profile for graphing. For example, you can enable both AHT 30 Min Growing and 5 Min Sliding for graphing.

The number of metric/time profile combinations that can be graphed is controlled by the configurable property `max.metrics.graphing.enabled` in the `CONFIG_PARAMETER` database table in the Contact

Center Advisor database. While this property can theoretically be set to any value, Genesys recommends you configure the limit to be 5 or less for performance reasons.

Note this parameter is shared by all Advisors modules, including CCAdv and WA. The parameter governs the total number of graphable combinations in both CCAdv and WA. Each metric/time profile combination is counted as 1. For example, if you select AHT 30 Min Growing and AHT 5 Min Sliding, that is counted as 2 graph-enabled metrics.

If you attempt to enable more metrics for graphing than the limit configured in the database, a warning message displays stating that the maximum number of metrics that can be graphed has been exceeded. You cannot save updates in the Metric Manager until you reduce the number of metrics enabled for graphing.

Enable Metrics for Graphing

Start Procedure

1. Open the Administration module.
2. Click **Report Metrics** in the navigation pane.
3. Use the filters on the **Report Metrics** page (on the right) to show as many or as few metrics as required.
4. Do one of the following:
    - Select an Application-type metric or a Contact Group-type metric and click `Edit` in the `Actions` column to open the **Metric Details** page.
    - Click `Create` to open the **Metric Details** page and create a new Application-type custom metric.
5. On the **Metric Details** page, select the applicable time profile.
   The `Time Profile` radio buttons are grayed out (that is, you cannot change the time profile) for out-of-box metrics.
6. To enable the metric for graphing, select at least one time profile from the `Time Profile` table, and select the `Chart` checkbox.
   The `Time Profile` table offers only one time profile type (Current) if the `Point in Time` radio button is selected, and three possible time profile options if the `Historical` radio button is selected.

Propagate Changes to Column Choosers

A change you make in the **Report Metrics** page does not appear immediately in the Column Choosers in the dashboards. This applies to any kind of change, whether to an out-of-box metric, or to a custom metric, including creation or deletion of the latter.

Propagate Changes to Column Choosers in CCAdv and WA

Start Procedure

1. Save or apply the change on the **Report Metrics** page.
2. Log out of Advisors.
3. Wait at least five minutes for the changes to be read from the Advisors database into cached data.
4. Log in to Advisors.
5. In the appropriate dashboard, open the Column Chooser.
6. You should see your changes reflected there.

Propagate Changes to Column Choosers in FA

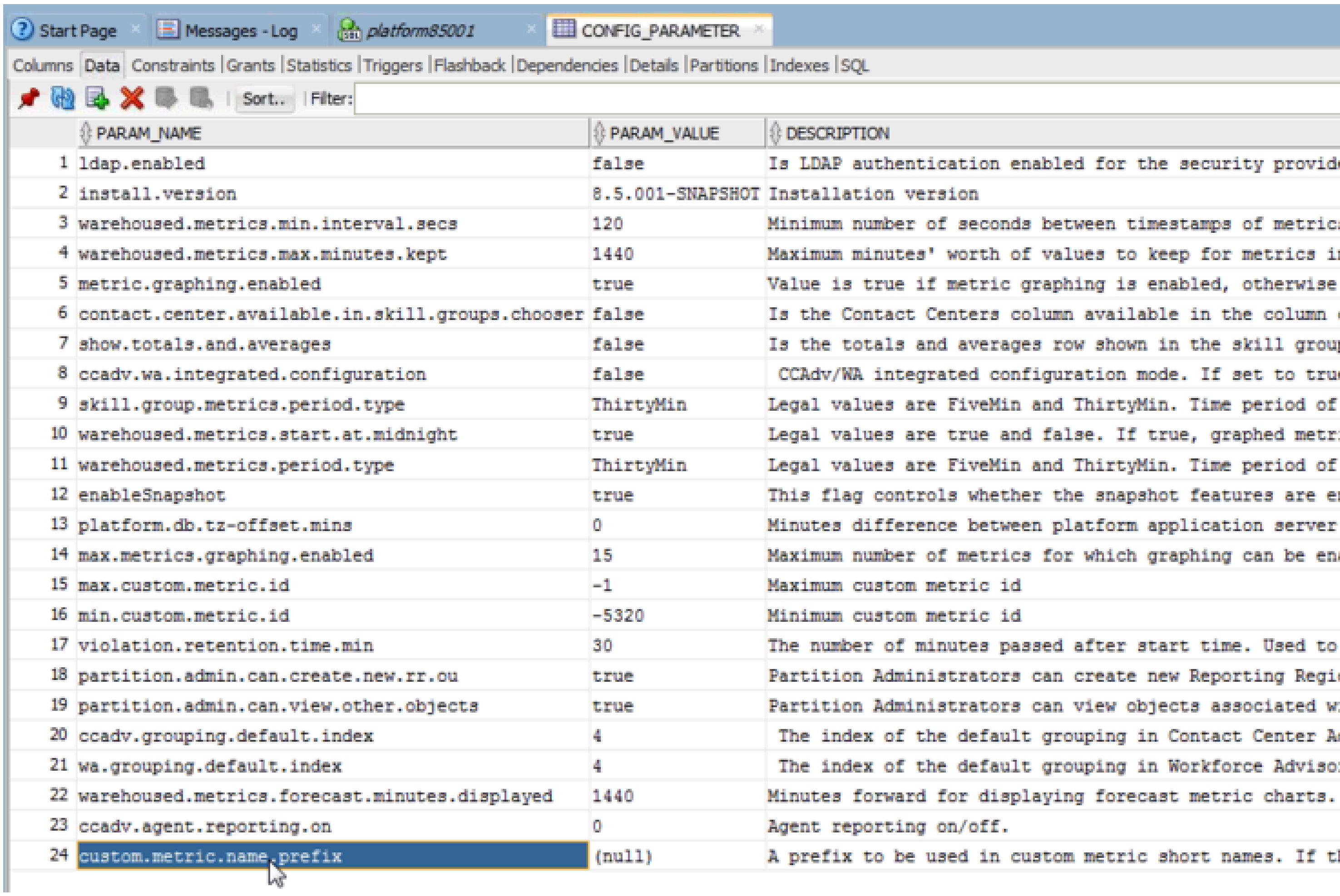
Start Procedure

1. Save or apply the change on the **Report Metrics** page.
2. In the FA Administration page `Settings` tab, click the `Hierarchy Reload` button. Alternatively, wait until the nightly reset procedure has executed.
3. Note that new report metrics will not be displayed in the accessible dashboard until the application server is restarted.

|-| Changing the Custom Metric Internal Name Prefix=

Custom metrics for Advisors have a standard, auto-generated `CM__metric id` internal name. You might have several Advisors installations that use the same Genesys Configuration Server, and if an administrator creates a custom report metric in each of two different installations, but uses the same metric ID (and, therefore, the same name), one metric overwrites the other in the Configuration Server. Overlapping metrics loaded into the Configuration Server impact permission settings for different installations. These metrics can also be deleted with a negative impact on other installations.

To resolve these types of issues, release 8.5.001 includes a parameter, `custom.metric.name.prefix`, that governs the custom metric naming space within the installation. The parameter is in the `Config_Parameter` table of the Advisors Platform database. The following screenshot shows the parameter.



	PARAM_NAME	PARAM_VALUE	DESCRIPTION
1	ldap.enabled	false	Is LDAP authentication enabled for the security provid
2	install.version	8.5.001-SNAPSHOT	Installation version
3	warehoused.metrics.min.interval.secs	120	Minimum number of seconds between timestamps of metric
4	warehoused.metrics.max.minutes.kept	1440	Maximum minutes' worth of values to keep for metrics i
5	metric.graphing.enabled	true	Value is true if metric graphing is enabled, otherwise
6	contact.center.available.in.skill.groups.chooser	false	Is the Contact Centers column available in the column
7	show.totals.and.averages	false	Is the totals and averages row shown in the skill grou
8	ccadv.wa.integrated.configuration	false	CCAdv/WA integrated configuration mode. If set to tru
9	skill.group.metrics.period.type	ThirtyMin	Legal values are FiveMin and ThirtyMin. Time period of
10	warehoused.metrics.start.at.midnight	true	Legal values are true and false. If true, graphed metr
11	warehoused.metrics.period.type	ThirtyMin	Legal values are FiveMin and ThirtyMin. Time period of
12	enableSnapshot	true	This flag controls whether the snapshot features are e
13	platform.db.tz-offset.mins	0	Minutes difference between platform application server
14	max.metrics.graphing.enabled	15	Maximum number of metrics for which graphing can be en
15	max.custom.metric.id	-1	Maximum custom metric id
16	min.custom.metric.id	-5320	Minimum custom metric id
17	violation.retention.time.min	30	The number of minutes passed after start time. Used to
18	partition.admin.can.create.new.rr.ou	true	Partition Administrators can create new Reporting Regi
19	partition.admin.can.view.other.objects	true	Partition Administrators can view objects associated w
20	ccadv.grouping.default.index	4	The index of the default grouping in Contact Center A
21	wa.grouping.default.index	4	The index of the default grouping in Workforce Adviso
22	warehoused.metrics.forecast.minutes.displayed	1440	Minutes forward for displaying forecast metric charts.
23	ccadv.agent.reporting.on	0	Agent reporting on/off.
24	custom.metric.name.prefix	(null)	A prefix to be used in custom metric short names. If t

The custom.metric.name.prefix parameter in the Config_Parameter table of the Platform database. A value of "null" means the Met will use the default prefix (CM) for the internal name of new custom report metrics.

The value you enter for this parameter becomes the prefix for custom report metric names and replaces the standard `CM` prefix in the internal system name. This lets you differentiate and isolate the metrics created in different installations and therefore avoid any conflicts at the Configuration Server level.

When you change the value for the `custom.metric.name.prefix` parameter, it immediately triggers the replacement of all custom metric names with a name that uses the specified prefix. The names of custom metrics used as operands in calculation expressions are also replaced.

You must run the Advisors Object Migration Wizard to import the metrics for which you specified a new prefix into the Configuration Server. Users of the Advisors interface who were logged in when you configured the prefix must log out and log in again to gain access to the metrics with the new names. All new custom metrics are created with the new prefix.

The Advisors administrator must ensure the prefixes are unique within the existing set of Advisors installations. There is no restriction on the number of metric prefix changes, but Genesys recommends that you carefully manage the number of obsolete metrics in Configuration Server and that you remove metrics that no longer exist in any Advisors installation.

Working with Metric Groups

Starting in release 8.5.0, you can collect raw reporting metrics into groups under each supported reporting application on the **Report Metrics** page in the administration module. Reporting applications supported by the **Report Metrics** page in release 8.5.0 are Contact Center Advisor and Frontline Advisor. A metric can participate in only one metric group. You can decide how you want to group the reporting metrics used in your enterprise based on your business needs.

One consideration when grouping report metrics is the relationship between a metric and the source objects. Previously, by default, all enabled metrics were applied on all configured base objects for a given object type. For example, all the enabled queue metrics were applicable to all the CCAdv queues published in a deployment.

Previously, you could distinguish between voice and non-voice virtual queues based on the Advisors queue type configuration. Voice and non-voice metrics could be based on the queue. However, this did not allow further sub-classification within the queue type, or allow classification of other object-type metrics.

Starting in release 8.5.0, and using the metric grouping functionality, you can specify exactly which metrics are applicable to each source object. On the **Report Metrics** page, group raw report metrics, and then map the metric groups to configured source objects using Genesys Administrator or Configuration Manager. This mapping of metric groups to configured source objects specifies the applicability of a metric to configured source objects. The configured metric applicability works on all of the enabled time profiles of a given metric.

Metric applicability configured on a given object is applied to all of the CCAdv object-filter segments. You cannot specify the metric applicability on individual CCAdv base object-filter combinations because each filter combination is not a separate object in Genesys Configuration server.

You can configure metric applicability for the following CCAdv and FA source objects:

- CCAdv:
  - Agent Groups
  - Applications (Genesys source objects: queues, calling lists, and interaction queues)
- FA:
  - Agents

Metric Grouping

The **Report Metrics** page allows grouping of metrics at the level of the raw report metric. Each raw report metric configured for a reporting application can be classified under one of the metric groups.

You can group related raw report metrics that are involved in evaluations of calculated report metrics for a source object in the same group, but it is not strictly necessary. If the various raw metrics involved in the calculation of a metric for a specific base object are in different metric groups, you must ensure that all metric groups that contain the contributing raw metrics for the calculation are mapped to the source object. If a group containing a raw metric required to successfully evaluate a calculated metric is not mapped to the corresponding source object, that raw metric cannot contribute to the metric’s calculated value. See an example below on this page.

Metric groups created using the Report Metrics page are not saved in the Configuration Server, but only in the Advisors platform database. See additional information on the *Report Metrics* page in this document.

Restrictions

A metric can participate in only one metric group.

Metric grouping is allowed only on raw report metrics. You cannot group calculated report metrics.

Example

You have a calculated report metric – Total Handle time – that is evaluated as the sum of two raw report metrics. The formula is Total HandleTime = Total Talk time + Total AfterCallWork Time.

Scenario 1:

- You place Total Tallk Time in metric group 1.
- You place Total AfterCallWork Time also in metric group 1.

Assumption: On a given source object, the Total Handle Time metric must be evaluated. Configuration: Configure the metric applicability such that metric group 1 is applicable on the given source object.

Scenario 2:

- You place Total Tallk Time in metric group 1.
- You place Total AfterCallWork Time in metric group 2.

Assumption: On a given base object, the Total Handle Time metric must be evaluated. Configuration: You must configure the metric applicability such that metric group 1 and metric group 2 are applicable on the given source object.

Scenario 3:

- You place Total Tallk Time in metric group 1.
- You place Total AfterCallWork Time in metric group 2.

Assumptions:

- On a given base object, the Total Handle Time metric must be evaluated.
- You configured metric group 1 to be applicable on the given source object.
- You configured metric group 2 to be applicable on a source object that is not the given source object.

In this scenario, only Total Talk Time is available for evaluation of the calculated metric; Total AfterCallWork time is not considered in that evaluation. Depending on the evaluation of the formula, this can result in Total Talk time = Total Handle Time in the case of CCAdv, but in FA, the result of the evaluation might be N/A.

Configuring Metrics Applicability in Configuration Server

To configure metric applicability using Genesys Administrator or Configuration Manager, specify the metric groups as Annex options on the source objects.

You can configure metric applicability to individual source objects, or you can select more than one source object and configure identical metric applicability on all that you have selected.

For CCAdv, you can select agent groups, queues, interaction queues, and calling lists to configure metric applicability.

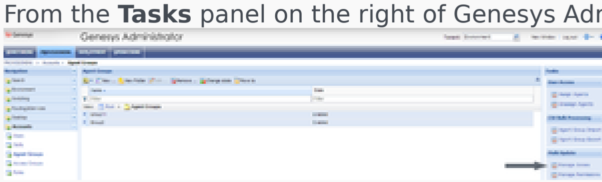
For FA, you can select agents to configure metric applicability.

The following procedures show you how to use Genesys Administrator to configure metric applicability for agent groups. The same procedure can be used for configuring all other source objects.

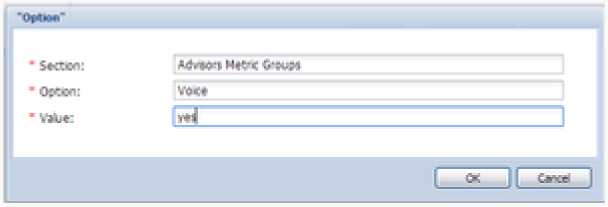
Procedure: Configure metric applicability for selected objects

Purpose: Use this procedure to add new metric groups as options to selected objects in Genesys Administrator.

Steps

1. Select the objects for which you want to configure identical metric applicability. For example, if the same metric applicability should be configured for a given set of agent groups, identify those agent groups and multi-select them.
2. From the **Tasks** panel on the right of Genesys Administrator, select **Manage Annex**.


Select Manage Annex
3. On the **Add** section, click the **Add** button and add a new annex section called `Advisors Metric Groups`, as well as an option called the name of the metric group. The name of the metric group entered here must match the name of the metric group created and selected for the raw report metric on the Advisors **Report Metrics** page. The metric group name must also match in case; that is, it is case-sensitive.

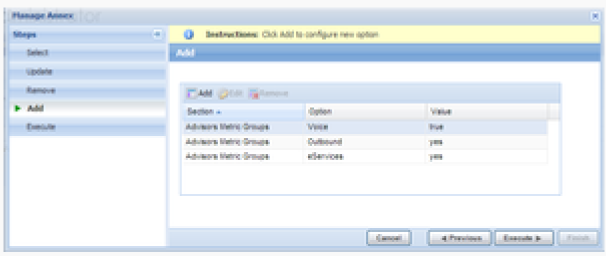


Add the Advisors Metric Groups Section

Genesys Administrator requires that you specify a value for each option. Anything can be entered, such as `true` or `yes`. The value for the option is not used. If you use Genesys Configuration Manager, the value is optional and you can leave it blank.

If you have more than one metric group to add as an applicable metric group for the selected objects, click the **Add** button and repeat the process.

For example, the Figure, "Advisors Metric Groups options" shows three metric groups added: Voice, Outbound, and eServices. Those three metric groups contain metrics that must be associated with the selected agent groups.



Advisors Metric Groups options

4. Click **Execute** and **Finish** to save your changes.

Procedure: Remove a metric group from selected objects

Purpose: Use this procedure to remove a configured metric group from selected objects.

Steps

1. Select the objects for which identical metric applicability must be configured. For example, if you must configure identical metric applicability for a given set of agent groups, identify those agent groups and multi-select them.
2. From the **Tasks** panel on the right of Genesys Administrator, select **Manage Annex**.
3. On the **Remove** section, click the **Add** button to add the metric group option that must be removed.

4. Click **Execute** and **Finish** to save your changes.

Default Metric Group

The Advisors out-of-box raw report metrics are all grouped under the `Default` metric group. Adding report metrics to this default metric group means that these metric groups are implicitly applicable to all source objects.

There is no need to explicitly configure a default metric group in the Configuration Server. See also *When the statistic template metric group is the Default metric group* below.

What Happens if I do not Assign Metric Groups to a Source Object?

If, for a given source object, you do not add any metric groups as Options, then none of the metrics from metric groups are applicable for that source object. However, if there are any other metrics of that object type that are still grouped under the `Default` metric group, they are still considered to be applicable. Therefore, there is no need to configure metric applicability on metrics that must be applied to all the source objects; it needs to be configured when some metrics must excluded from some objects.

When are Configuration Server Changes Applied for CCAdv?

On startup, the configured source objects are fetched from the Configuration Server and stored in memory; this includes the metric groups configured on the CCAdv source objects. CCAdv subscribes to changes to the source objects in the Configuration Server, and, in release 8.5.0, this includes updates to the metric group configuration.

For both new and already-published objects, changes in the metric applicability are applied during the overnight refresh.

When are Configuration Server Changes Applied for FA?

On startup, when the FA hierarchy is loaded from the Configuration Server, the metric groups configured on the FA agent source objects are also loaded. On overnight refresh, or on the forced reload of the hierarchy from the Configuration Server, any changes to the metric group configuration on the FA agent objects are also reloaded.

How Metric Applicability works with Include/Exclude in Statistic Requests

CCAdv administration and FA use the metrics applicability configuration to decide which statistics to request on a specific object.

CCAdv administration and the FA application send the configured statistics to the data manager, which then routes those statistics to one or more adapter instances. When statistic requests are sent to the data manager, the applications (FA and the CCAdv administration) also look up the metrics applicability configuration. Based on the results, the application (CCAdv or FA) determines which statistics to include in the statistics request.

When the statistic template metric group is the Default metric group

There is no default metric group in the Configuration Server to correspond to the `Default` metric group (the out-of-box metric group) in Advisors. It is unnecessary to fetch the objects applicable to this default metric group; any statistic that belongs to the `Default` metric group is automatically included for any object of that object type. For example, if there is an agent group metric that is included in the `Default` metric group, then it is applicable to all the agent groups published. In this example, "agent group" is the object type that links the agent group metric with the agent group source object.

When the statistic template metric group is a custom metric group

For a metric group that you create, CCAdv administration and FA look up the applicable objects. For a specific statistic request, if the corresponding metric group is applicable for the object (identified by the object ID and the object type), then that specific statistic is included in the statistic requests to Stat Server. If the metric group is not applicable for the object that corresponds to the statistic, then the statistic is excluded from the statistic requests to the Stat Server.

How Metric Applicability works with Voice and Non-Voice Stats Requests on Queues

In release 8.1.5, you used queue-type configuration of the virtual queues to specify if non-voice statistics should be requested on the virtual queues. If the option of "queueType = NonvoiceOnly" was set on a virtual queue in Configuration Server, then only non voice statistics were requested.

Starting in release 8.5.0, metric grouping and the mapping of metric groups to configured source objects replaces the usage of queue-type configuration. You can no longer use queue-type configuration in Configuration Server to indicate if non-voice statistics are requested on specific virtual queues. Instead, using metric applicability, the system determines if non-voice statistics can be requested on a virtual queue.

On every voice-only queue, the metric applicability must be configured to point to voice metric groups. On non-voice queues, the metric applicability must be configured to point to non-voice metric groups.

If there are queue metrics assigned to the `Default` metric group, those metrics are requested on both voice and non-voice queues.

If you currently use queue-type configuration, there is no migration path to convert to the metric applicability configuration. You must reconfigure based on metric applicability.

Metric Applicability in FA

FA gets its metric applicability mapping from Configuration Server. The FA tasks that issue statistics for state and performance metrics and rules do the following:

1. Resolve IDs of the agents to whom metric applicability applies
2. Resolve IDs of the metrics that apply to the above agents, and
3. Before issuing statistics, filter out metrics that do not apply to certain agents.

The result of the preceding actions is the following:

1. The connector returns statistics for certain metrics for certain agents.
2. When a metric does not apply to an agent:
    a. users see `N/A` on the dashboard, and
    b. a metric that does not apply to an agent is excluded from rollups that include this agent; that is, metrics contribute to rollups based on applicability.
3. Assigned and unassigned metrics are mutually exclusive:
    a. If no metric groups are assigned, all metrics apply to all agents.
    b. If metric group MG1 is associated with agent A1, then only metrics in MG1 apply to A1.
    c. If agent A2 has no metric groups applied, then all metrics apply to A2 except the metrics from MG1, which was assigned to agent A1.

If there are a number of metric groups configured in Metric Manager, but those metric groups are not configured on any of the agents in the FA hierarchy, then this is considered an incomplete configuration for FA metric applicability; the metrics on such metric groups are considered as applicable for all agents. Therefore, whenever metrics are in specific metric groups, make sure those metric groups are also configured on agents, as needed.

If a configured metric group is removed from all agents in the hierarchy, make sure to either unassign such metrics from that metric group by placing the metric back in the `Default` metric group, or disable those metrics if the intention is to not make those metrics applicable to any of the agents. Genesys recommends that you avoid disabling metrics by placing them in an unused metric group.

Tracing the Metric Applicability in CCAdv

To trace how metrics have been applied to source objects for CCAdv, turn on the Debug log mode for the Platform Geronimo application logs:
`log4j.category.com.genesyslab.advisors.eacore.adapterclient=DEBUG`

Whenever an object is published, the log indicates the number of statistics that are applicable on an object. For example:

```
2014-02-22 13:31:17,775 DefaultThreadPool 6 DEBUG [IssueStatistics] Found 28
applicable metrics for object: ObjectIdentifier [id=8354, name=7007@LucentG3,
tenantName=defaultTenant, filterName=null, objectSubType=ACD]
```

Users

User profiles are maintained in the Configuration Server. To access these profiles, please use the Genesys Administrator or Configuration Manager.

Users Page

In the Genesys Configuration Manager and Genesys Administrator, users correspond to the `Person` object. Users (persons) and roles must be assigned access to modules, as well as to contact centers, application groups, regions, and metrics.

See also:

- Advisors Business Objects
- CCAdv/WA Access Privileges

The `Effective Date` and `Expiration Date` fields have been removed from the user profiles in Configuration Manager because they are not supported by the Configuration Manager for `Person` accounts. Further information about creating and maintaining `Persons` in the Genesys configuration environment can be found in:

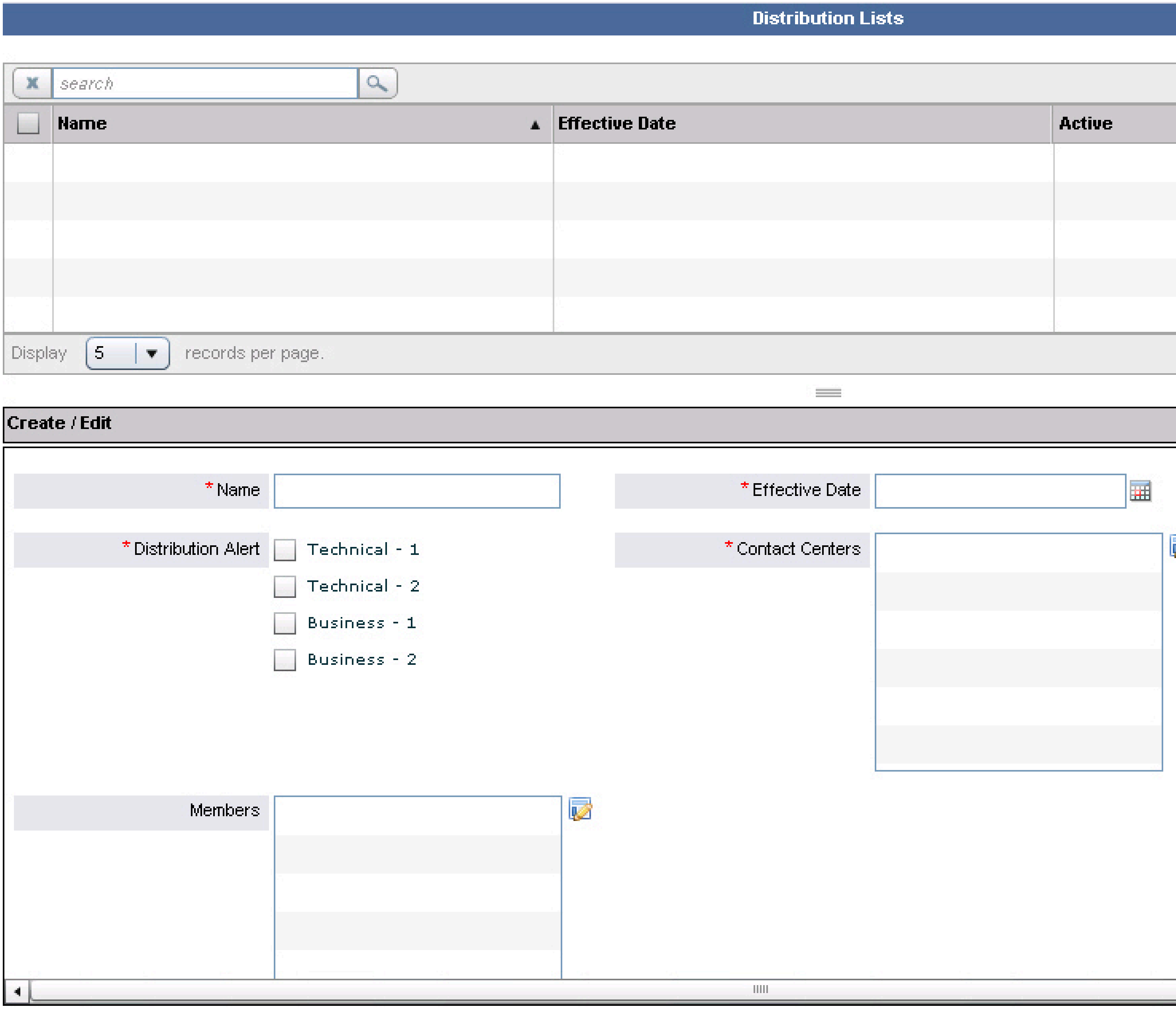
- Framework 8.1 Genesys Administrator Deployment Guide
- Framework 8.1 Configuration Manager Help
- Genesys Administrator 8.1 Help

Distribution Lists

CCAdv and WA can send e-mail notifications to specified distribution lists. The notifications are about:

- Alerts caused by metrics' violations of thresholds. See Application Groups and Thresholds for a lot of detail on how CCAdv and WA use these lists to notify users about alerts.
- Alerts about offline peripherals.
- An external source system has not provided updated real-time data within a configurable interval. See System Configuration.

The following screenshot shows the Distribution Lists page.



Distribution Lists Page

Threshold Violations Alerts and Offline Peripheral Alerts

Assign contact centers and application groups to distribution lists in order for users to receive e-mail notifications about threshold violation alerts or peripheral offline alerts. The users will receive e-mail about alerts that are created for applications or contact groups related to the application groups or contact centers.

Access to contact centers and application groups must be configured by an administrator in Genesys Configuration Manager. In this page, data relating to or depending on objects to which you have no permission will not be displayed. See CCAdv/WA Access Privileges.

E-mail about threshold violation alerts, and alerts about offline peripherals, are not sent to users who have no permissions configured in Genesys Configuration Manager to the contact centers, application groups, and geographic regions related to the alert.

Distribution lists are associated with a specific type of alert. The types are:

- B1 and B2 for business alerts. (*1* means critical severity, and *2* means severity.)
- T1 and T2 for technical alerts

The distribution list only sends e-mail about alerts whose type and severity matches the typs and severities for which the list is configured.

Each distribution list must always have at least one contact center and one application group associated with it. When assigning a network contact center, you may also add its related agent group contact centers.

Alert Email Notification About Source System Not Updating Data

Contact Center Advisor sends e-mail to a distribution list if an external source system has not provided updated real-time data within a configurable interval. See System Configuration. When sending this e-mail, Contact Center Advisor ignores the `Distribution Alert` settings of the distribution list, even though at least one checkbox must be selected. Contact Center Advisor also ignores the application groups and contact centers assigned to such a list when sending e-mail about these failures.

Selecting Individual Distribution List Members

If you select individual distribution list members, you must assign any members added in the future manually.

Maintaining Distribution Lists

Maintain distribution lists

Start Procedure

1. On the navigation bar, select Distribution Lists.
   The Distribution Lists page displays.
2. To add a new distribution list, do one of the following:
   - Click New and begin adding details in the Create/Edit panel.
   - Click in the Name field and begin adding details in the Create/Edit panel.

3. To edit a distribution list, do one of the following:
   - Check its check box in the upper panel and edit the details in the Create/Edit panel.
   - Search for it using the Search feature above the upper panel, then check its check box and edit the details in the Create/Edit panel.
4. Click the Save button.
   A confirmation message displays.

Delete a distribution list

Delete a distribution list to stop subsequent alert notifications. Note that you can deactivate a distribution list instead of deleting it to avoid the need to reenter it in the future.

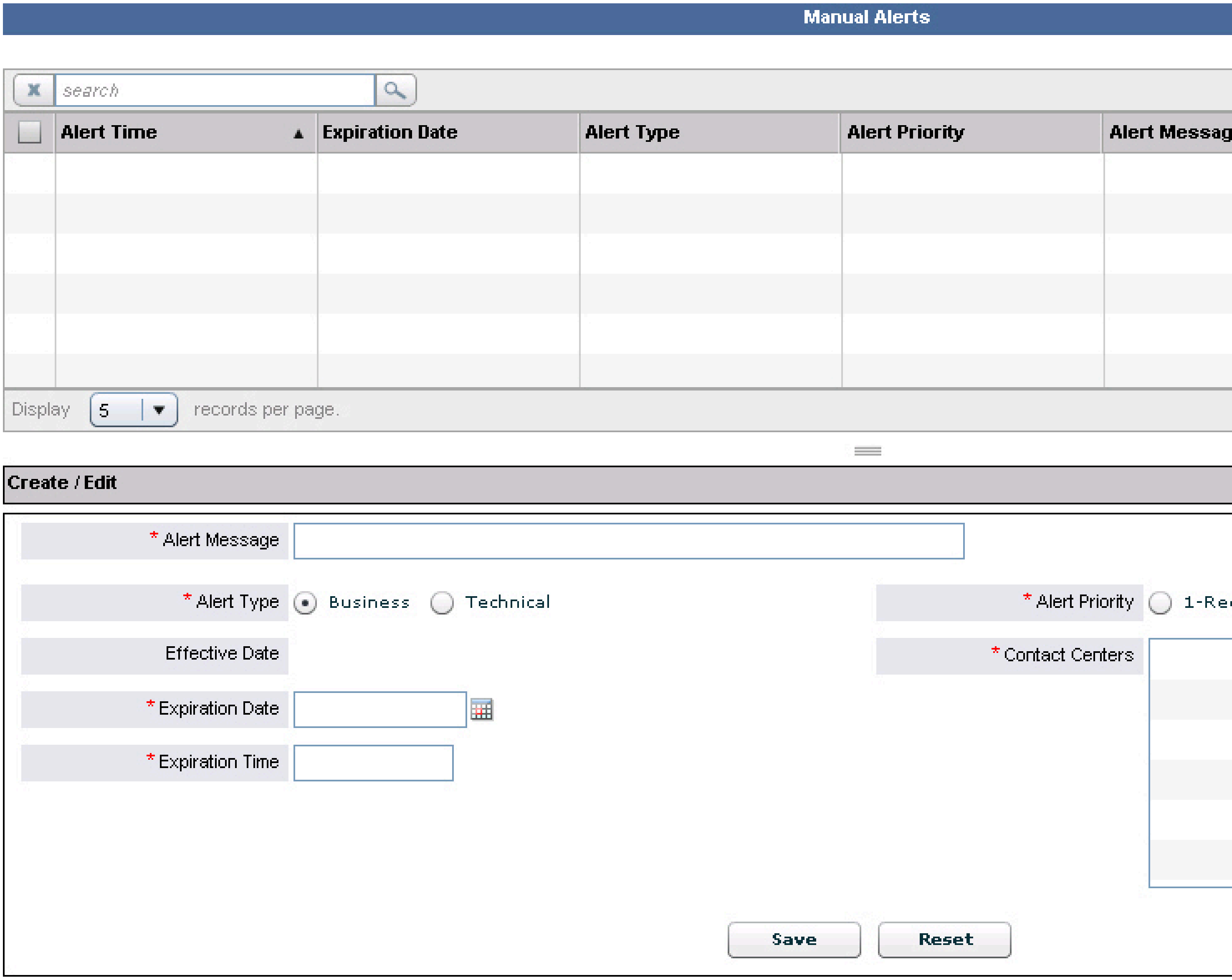
Start Procedure

1. On the navigation bar, select Distribution Lists.
   The Distribution Lists page displays.
2. To display the details of a user, either select the check box for a user from the list in the upper panel, or search for a specific user and then select the checkbox associated with that user.
3. Click the Delete button.
   A confirmation window displays.
4. To confirm the deletion, click OK.
   A message confirms the deletion.

Manual Alerts

Manual alerts allow for the distribution of information to Advisor users. These manual alerts are useful for quickly disseminating information to the field through the dashboard.

The Alerts page allows you to add an alert message manually. The alerts display, based on the users' viewing rights, in the Alerts Map and the Alerts Pane in CCAdv and WA. The following screenshot shows the Alerts page.



Alerts Page

There are two types of manual alerts:

- Business alerts (B)
- Technical alerts (T)

There are two alert severities:

- 1 (critical - red)
- 2 (warning - yellow)

If both an agent group contact center and a network contact center are selected for the manual alert, two alerts display on the map; that is, if the network contact center has latitude and longitude coordinates.

If both an agent group contact center and a network contact center are selected for the manual alert, the network contact center alert and the agent group contact center alert display in the Alerts panel.

If only an agent group contact center is selected, the agent group contact center alert displays in the Alerts panel.

Access to contact centers must be configured by an administrator in Genesys Configuration Manager. Data relating to or depending on contact centers to which users have no permissions will not be displayed.

Add a Manual Alert

Start Procedure

1. Click New.
2. Enter the text of the alert message. The text should be no longer than 24 characters.
   The text displays in the carousel and the Alerts panel on the dashboard.
3. Type the alert message.
4. Choose the alert type.
5. Choose the alert priority and severity.
6. To determine the duration of the displayed message, type the expiration date and the expiration time.
7. To choose the affected contact centers, select the associated check boxes.
8. To add the alert, click Save.
   A confirmation message displays. The alert displays in the Alerts panel.

Update a Manual Alert

Start Procedure

1. Type the updated message.
   You can only update the message.
2. Click the Save button when complete.
   A message confirms the update.

Delete a Manual Alert

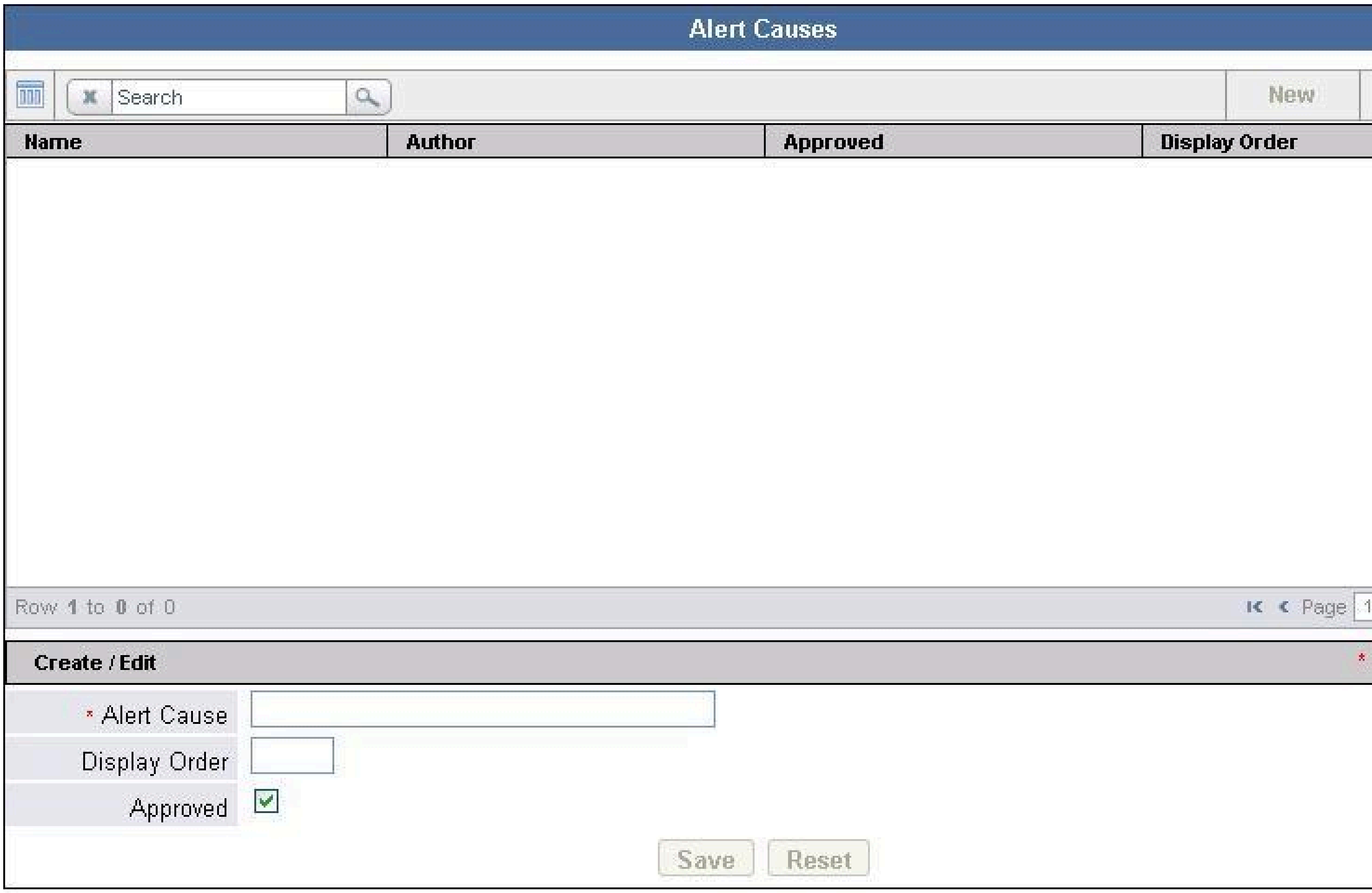
Deleting a manual alert removes it from the Alerts list and from the dashboard.

Start Procedure

1. Click the Delete button beside the alert to be deleted.
   A confirmation window displays.
2. To confirm the deletion, click OK.
   A message confirms the deletion.

Alert Causes

Users record the alert cause when creating a key action report. They may select the cause from the Alert Cause drop-down list or enter a new cause. In addition, users can suggest that the entered cause be added to the drop-down list for future use. The alert causes are maintained on the Alert Causes page in the Administration component. The following screenshot shows the Alert Causes page.



Alert Causes Page

The details of an alert cause include:

- `Name`: The name of the alert cause. The name must be unique and is not case sensitive. If the name is modified, it will change on existing key action reports.
- `Author` (display only): Properties that identify the person who created the cause on the Alert Causes page or on a key action report. These are the person's first and last name, or e-mail address, or username, depending on what is available in the Configuration Manager.

- `Display Order` (optional): The location of the cause in the `Causes` drop-down list on the Action Management page. Causes without a sequence number display in alphabetical order. The range of the display order is 30.
- `Approved`: The status of the cause is either approved or unapproved. When added from the Alert Causes page, the `Approved` check box is automatically selected. When suggested from the Action Management page, the `Approved` check box is unselected (unapproved).

From the Alert Causes page, you can:

- Add a new alert cause to be available in the `Alert Cause` drop-down list on the Action Management page. Open the Alert Causes page and use the `Search` field.
- Approve an alert cause.
- Edit an alert cause.
- Delete one or more alert causes that are not used and not included in a key action report.

Approve or Reject an Alert Cause

On the Action Management page, users may enter new alert causes and suggest that they are added to the drop-down list. The suggested causes display in the Alert Causes table on the Alert Causes page. The causes suggested by a user are initially unapproved.

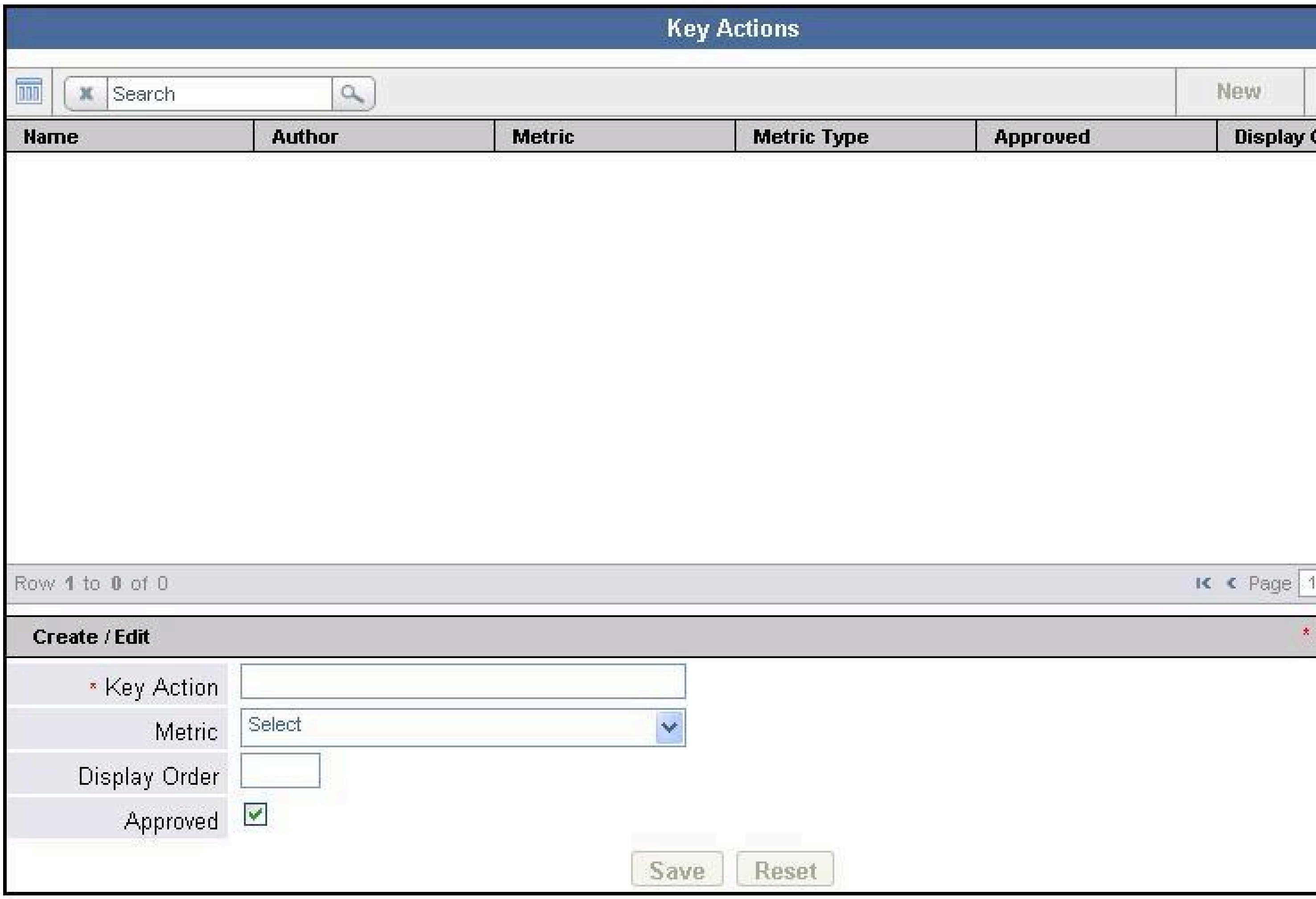
Start Procedure

1. To add an unapproved cause to the drop-down list on the Action Management page:
   a. Highlight a row for an unapproved cause in the Alert Causes table. The details display in the details section.
   b. Select the Approved check box.
   c. Click Save. The approved cause displays in the table with a check mark.
2. To leave a cause off the drop-down list on the Action Management page:
   a. Highlight a row for an approved cause in the Alert Causes table. The details display in the details section.
   b. Clear the Approved check box.
   c. Click Save. The unapproved cause displays in the table with symbol to indicate that is it unapproved.

Key Actions

Access to metrics must be configured by an administrator in Genesys Configuration Manager. Data relating to or depending on metrics to which users have no permissions will not be displayed.

Users record the key action taken to resolve the violations when creating a key action report. They may select the key action from the Key Action drop-down list or enter a new key action. In addition, users can suggest that the entered key action be added to the drop-down list for future use. The table of key actions is maintained on the Key Actions page in the Administration module. The following screenshot shows the Key Actions page.



Key Actions Page

The details of a key action include:

- `Name`: The name of the key action. The name must be unique and is not case sensitive. If the name is modified, it will change on existing key action reports.

- `Author`: Properties that identify the person who created the key action on the Key Actions page or on a key action report. These are the person's first and last name, or e-mail address, or username, depending on what is available in the Configuration Server. The author is display only.
- `Metric` (optional): The metric to which the key action applies. A key action associated to a metric is available on the Action Management page only if the metric matches one of the alerts for the key action report. Key actions without a defined metric are available on the Action Management page for all alerts.
  The metric cannot be changed if it is included in a key action report but it can always be removed. Only the metrics that can have a threshold rule display in the drop-down list. The drop-down lists the display names of the metrics within metric type.
  If the key action is suggested from the Action Management page, the metric defaults to unselected.
- `Display Order`: The location of the key action in the `Key Actions` drop-down list on the Action Management page. Key actions without a sequence number display in alphabetical order. The range of the display order is 30.
- `Approved`: The status of the key action is either approved or unapproved. When added from the Key Actions page, the `Approved` check box is automatically selected. When suggested from the Action Management page, the `Approved` check box is unselected (unapproved).

From the Key Actions page, you can:

- Add a new key action to be available in the `Key Action` drop-down list on the Action Management page.
- Approve key actions.
- Edit a key action.
- Delete one or more key actions that are not used and not included in a key action report.

Approve or Reject a Key Action

On the Action Management page, users may enter new key actions and suggest that they are added to the drop-down list. The suggested key actions display in the Key Actions table on the Key Actions page. The key actions suggested by a user are initially unapproved.

Start Procedure

1. To add an unapproved key action to the drop-down list on the Action Management page:
   a. Highlight a row for an unapproved key action in the Key Actions table. The details display in the details section.
   b. Select the Approved check box.

c. Click Save.
   The approved key action displays in the table with a check mark.

2. To leave a key action off the list on the Action Management page:

   a. Highlight a row for an approved key action in the Key Actions table.
      The details display in the details section.

   b. Clear the Approved check box.

   c. Click Save.
      The unapproved key action displays in the table with the symbol.

Manage Adapters

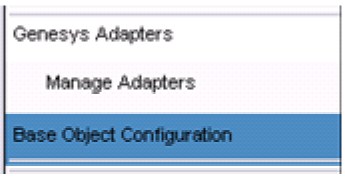
The **Manage Adapters** page in the Administration module is read-only. You can view information about the adapters on this page. Information about adapters is stored in the Platform database. You manage the adapters from the Platform database.

For more information, see *Performance Management Advisors 8.5.0 Deployment Guide*.

Base Object Configuration

Administration Module Navigation

The following screenshot shows the link to the Base Object Configuration page on the Administration module navigation pane.



Base Object Configuration link in the Administration Module Navigation Pane

Access Permissions

Visibility of the agent groups and queues on the Base Object Configuration page is determined by the tenants to which the administrator has access. Note that the access permission is determined only at the tenant level. If the administrator has access to a given tenant, all the objects under that tenant are displayed in the Base Object Configuration page, irrespective of whether the administrator has access to individual objects in it. Therefore, in order for an administrator to be able to view objects to publish in the Base Object Configuration page, either the user, or the user’s access group, must be granted at least Read access permission to the tenants under which the administrator will be publishing the objects.

Configuring Genesys Objects

Statistics distribution is handled automatically by the Data Manager. The associations that display on the Base Object Configuration page are no longer tied to a selected adapter, but instead represent a global configuration for CCAdv/WA. For more information, see *Performance Management Advisors 8.5.0 Deployment Guide*.

NEW Starting in release 8.5.0, you must deploy the Contact Center Advisor application (including XML Generator) and configure the Genesys metric sources before you can use the **Base Object Configuration** page in the Administration module. Data manager requests no statistics for pre-configured objects until the CCAdv module, XML Generator, and Genesys metric data sources are deployed and working.

Base Object Configuration

On the Base Object Configuration page, you can:

- configure objects (queues and agent groups):
    - assign objects to filters on the Base Object to Filter Mapping tab
    - assign filters to an object on the Mapping to Base Object tab
- identify and filter objects by object type
- view the count of configured objects
- search each listbox

You require Read access to one or more tenants to use the Base Object Configuration page. You see only agent groups and queues in the Base Object Configuration page for the tenant(s) to which you have Read access permission. The Base Object Configuration page prevents contradictory configuration. For example, if you select No Filter for an object, and later attempt to assign a filter, you receive an error message. You must de-select No Filter before a filter can be assigned to that object. Filter categorization is not applicable for interaction queue statistics. No Filter is the only option you can successfully apply to interaction queues. If you attempt to combine filters with an interaction queue, the filters are discarded and the No Filter option is automatically selected again. For detailed information about the filters and objects that display on the Base Object Configuration page, see Data Manager content in the *Performance Management Advisors 8.5.0 Deployment Guide*.

Base Object Configuration Page Filters

Both tabs on the Base Object Configuration page include a Filters panel. You use these filters to refine the list of filters and objects you view on the page. For example, if you want to view only filters that are assigned to objects, select the box beside Selected under Filter and ensure the box beside Unselected is not checked. The list of object filters now shows only filters that have been assigned to objects. Unassigned filters are hidden. The Filters panel also includes a Search field. Use the Search field to quickly find a filter or object by typing its name in the field and clicking the icon beside the field.

Map objects to a filter

On the Base Object to Filter Mapping tab, you select a filter and map objects to it. Use this procedure to quickly assign multiple objects to one filter. If you select No Filter for an object, and later attempt to assign a filter, the system prevents you from proceeding. You must de-select No Filter before a filter can be assigned to that object.

Start Procedure

1. Open the Base Object to Filter Mapping tab.

2. Select a filter.
   The list of available agent groups and queues displays in the pane to the right.
   The list of filters and available objects is configured in the Genesys Configuration Server. If you do not see a filter or object that you require, contact your system administrator. Object visibility is controlled by permissions.
3. Click the checkbox beside an object to select it and assign it to the filter.
4. After you have selected the objects to assign to the filter, click Save to save the assignments or click Cancel to discard the assignments.

Map filters to an object

On the Mapping to Base Object tab, you can select an object and map filters to it. Use this procedure to quickly assign multiple filters to an object, and to discover what filters are assigned to an object.

Start Procedure

1. Open the Mapping to Base Object tab.
2. Select an object from the list of available agent groups or queues.
   The list of relevant filters displays in the pane to the right. Filters that are already assigned to the selected object have a checkmark beside the filter name.
   The list of filters and available objects is configured in the Genesys Configuration Server. If you do not see a filter or object that you require, contact your system administrator. Object visibility is controlled by permissions.
3. Click the checkbox beside a filter to select it and assign it to the object.
4. After you have selected the filters to assign to the object, click Save to save the assignments or click Cancel to discard the assignments.

Resource Management

A good routing and resource plan based on historical data should represent a typical day. However, for unplanned events that happen during a day, **Resource Management** is available to address temporary changes to skills and skill levels, such as increased volume.

Warning

Resource Management is not intended for bulk changes and may disrupt mission critical system requests.

Launching **Resource Management** from the hierarchy is not recommended because the number of agents and agent data pulled might be very large and impact performance. Genesys recommends launching **Resource Management** from the **Agent Groups** pane, the **Applications** pane in CCAdv, or **Contact Group** pane in WA, in order to pull less than 150 agents.

The **Notification Lists** and **Notification Templates** pages in the Administration module are applicable to the **Resource Management** console.

Notification Lists

Notification lists are used to inform groups of users within an organization about changes being made to the agents or resources. The notification lists are simply a collection of e-mail addresses. Administrators maintain the e-mail addresses from the Notification Lists page on the Administration module. These addresses are linked to the actions of Resource Management.

From the Notification Lists page, you can:

- View the e-mail addresses on a notification list by selecting a single row in the table. The row expands to show the e-mail addresses.
- Delete an e-mail address.
- Search for an e-mail address.
- Add a notification list.
- Delete a notification list that is no longer used. Note that multiselection (for deletion) is not available for Notification lists (including e-mail addresses within a notification list) or Notification templates.
- Update an existing notification list.
- Reset the updates to a notification list before it is saved.

Add a Notification List

Start Procedure

1. On the navigation bar, click Notification Lists.
   The Notification Lists page displays.
2. Click New.
   The Add/Edit Notification List page displays.
3. Type a name for the notification list.
4. To add an e-mail address, type one in the Add E-mail field and click Add.
5. Click Save.
   The Notification Lists page displays.

Edit a Notification List

Start Procedure

1. On the navigation bar, click Notification Lists.
2. Click the Edit icon next to the notification list that you want to edit.
3. The Add/Edit Notification List page displays. The details display in the User’s E-mail section.
4. Update the name of the notification list.
5. To add a new e-mail address, type one in the Add E-mail field and click Add.
6. Click Save. The Notification Lists page displays.

Delete an E-mail Address from the List

Start Procedure

1. On the navigation bar, click Notification Lists.
2. Click the Delete button next to the e-mail address you want to delete.
   The following message displays: “Do you want to delete the selected item?” with Yes/No buttons.
3. Click Yes. The item is removed from the table.
   Click No to cancel the deletion. The confirmation dialog closes and the item remains in the table.

Notification Templates

Notification templates provide standard content for e-mails that describe the directives and actions taken from Resource Management. Notification templates are preconfigured messages that users can send to affected agents (and users) who are on notification lists. Administrators maintain notification templates from the Notification Templates page. Templates can also be created dynamically (while using Resource Management); however, they must be managed from the Notification Templates page.

Notification Templates Page

From the Notification Templates page, you can:

- Add a notification template. If you have permission, you can create up to 50 distinct templates.
- Delete a notification template that is no longer used. Note that multiselection (for deletion) is not available for Notification lists (including e-mail addresses within a notification list) or Notification templates.
- Update an existing notification template.
- Reset the updates to a notification template before it is saved.

Notification templates are composed of the name of the template and its contents.

Skills Change Statement

The skills change statement is one of the following:

- The following skills have been added: <list skill name and level>
- The levels of the following skills have been changed: <list skill name and new level>
- The following skills have been removed: <list skill name>

Default E-mail Notification Templates

The following table shows the default e-mail formats of the notification templates.

Action	Target Object	E-mail Subject	E-mail Body
Status Change	Agent	Notification of Status Change	Your status has been changed to <new status inserted here>

Action	Target Object	E-mail Subject	E-mail Body
			Additional Comments: <Insert any comments entered by the user – this is what is displayed in the message textbox>
Status Change	Supervisor	Notification of Status Change	The status of the listed agents in agent group <Insert agent group name here> has been changed to <Insert new status here>. Additional Comments <Insert any comments entered by the user— this is what is displayed in the message text box> Agents Affected <Insert list of agents from this agent group here>
Status Change	Users on Notification List	Notification of Status Change	The status of the listed agents in agent group <Insert agent group name here> has been changed to <Insert new status here>. Additional Comments <Insert any comments entered by the user— this is what is displayed in the message text box> Agents Affected <Insert list of agents from this agent group here>
Skill Change	Agent	Notification of Skill Change	Your skills have been changed. <Insert statement about how skills have been changed—see description after table>. Additional Comments <Insert any comments entered by the user— this is what is displayed in the message text box>
Skill Change	Supervisor	Notification of Skill Change	The skills of the listed agents in agent group <Insert agent group name here> have been changed. <Insert statement about how skills have been changed—see description after table>.

Action	Target Object	E-mail Subject	E-mail Body
			Additional Comments: <Insert any comments entered by the user—this is what is displayed in the message text box> Agents Affected <Insert list of agents from this agent group here>
Skill Change	Users on Notification List	Notification of Skill Change	The skills of the included agents have been changed. <Insert statement about how skills have been changed—see description after table>. Additional Comments sent to Agent <Insert any comments entered by the user—this is what is displayed in the message text box> Additional Comments <Insert the additional comments entered for the notification lists here> Agents Affected: <Insert list of agents here>
General Notification	Agent	<title of template that is used>	Message From the Operator: <Insert any comments entered by the user—this is what is displayed in the message text box>

Logs

For information about logs, including which actions are logged and how to configure audit logs, see logging information in the *Performance Management Advisors Deployment Guide*.