



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 8.1.5

Table of Contents

Contact Center Advisor and Workforce Advisor Administrator User's Guide	3
Genesys Advisors Browser	4
Advisors Business Objects	8
Role Based Access Control	14
Advisors Privileges	20
Objects in the Administration Module	27
Notes about the Interface	29
Zero Suppression	30
System Configuration	32
Regions	35
Application Groups and Thresholds	38
Adding or Updating Thresholds	43
Adding Threshold Exceptions	44
Contact Centers	47
Configuring Contact Centers	49
Switches and Peripherals	52
Application Configuration	54
Contact Group Configuration	64
Agent Group Configuration	74
Metric Manager	80
Users	91
Distribution Lists	92
Working with Distribution Lists	94
Manual Alerts	96
Alert Causes	99
Key Actions	101
Base Object Configuration	104
Notification Lists	107
Notification Templates	109

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 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.

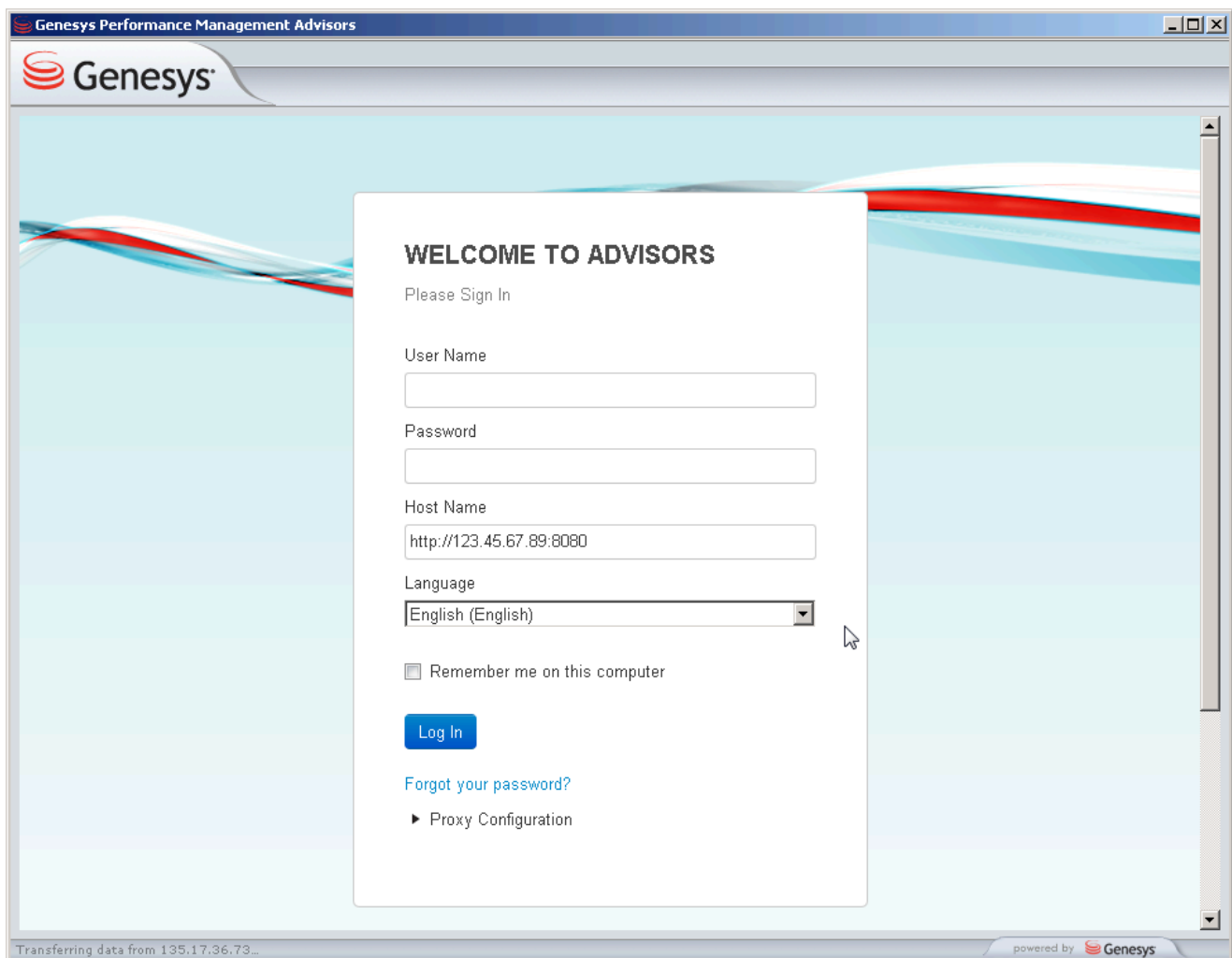
Alert Management provides the ability to record the action taken to resolve one or more alert violations, as well as the results of that action. Each action is recorded in a separate key action report. The key action reports create a knowledge base that helps identify repetitive patterns and resolve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

Genesys Advisors Browser

The Genesys Advisors Browser is installed in your Start folder or on your desktop when your Advisors suite is deployed. Only users with the admin role can access the Administration Console. Starting in Release 8.1.5, permissions for your user account are loaded when you log in. If a user is logged in to the Advisors browser, and a new object is added to Genesys Configuration Server, it is not added to the user's view until that user logs out and logs in again (if the user has the necessary security permission to view the object). Similarly, to see objects that were activated in Advisors after the user logged on, that user must log out and log in again. The following screenshot shows the login page.



The screenshot shows the Genesys Performance Management Advisors login interface. The window title is "Genesys Performance Management Advisors". The Genesys logo is in the top left. The background features a blue and red wavy design. A central white box contains the login form with the following elements:

- WELCOME TO ADVISORS**
- Please Sign In
- User Name:
- Password:
- Host Name:
- Language: (dropdown menu)
- ☐ Remember me on this computer
- [Log In](#) (blue button)
- [Forgot your password?](#)
- [Proxy Configuration](#)

At the bottom of the window, a status bar shows "Transferring data from 135.17.36.73..." on the left and "powered by Genesys" on the right.

Logging in to the Genesys Advisors browser

Start Procedure

1. Double click on the Genesys Advisors browser icon. The Login page is displayed.
2. Type a user name and password.
3. The host name is <http://home.genesysadvisors.local> by default. However, if the home.genesysadvisors.local server is not found while the Login page loads, you must type your server name in the Host Name field. The host name is configured by the installer. If it is incorrect, see your system administrator. The new host name will become the default server for subsequent logins.
4. To save the user name and password on your local machine, check the Remember Me on this Computer check box. If selected, the user name and password will pre-populate when you start the Genesys Advisors browser.
5. Click the Log In button. The Genesys Advisors browser displays with the module tabs to which you have access. Once logged in, you can display other modules to which you have access in other windows by clicking the New Window button.
The Genesys Advisors browser also accepts login via proxy servers. You need to specify the IP address and port number during login. See [Proxy Login](#).

Proxy Login

The Genesys Advisors browser also accepts login via proxy servers. To log in using a proxy, click the Proxy Configuration menu below the Login button. The following screenshot shows the proxy login configuration.



▼ Proxy Configuration

☐ Direct Connection to the Internet

☐ Auto Detect Proxy settings for this network

☒ Manual Proxy Configuration

HTTP Proxy

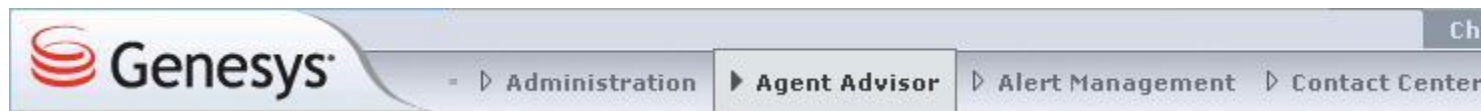
Port

Proxy Login

Select one of the proxy configuration options. For manual proxy configuration, specify the IP address and port number in the HTTP Proxy and Port fields during login, in the format 123.456.78.90 and 8080, for example.

Navigation

Only the modules to which you have access are displayed. The tab labels are configurable in the Contact Center Advisor Administration module on the System Configuration page. The following screenshot shows an example of the Advisors browser tabs.



Advisors Browser Tabs

Requesting a New Password

The ability to request a new password is determined by an installation parameter, and so might not be available.

Requesting a new password

Start Procedure

1. On the Login page, click Forgot Your Password?
A Forgot Password? page is displayed.
LDAP is handled within the Configuration Management environment.
2. Enter your user name and e-mail address.
3. Click Submit.
A new password is sent to your e-mail address.

Changing a Password

The ability to change your password is determined by an installation parameter, and so might not be available.

Changing a password

Prerequisite

You must be logged in to change your password.

Start Procedure

1. Click the Change Password button. A Change Password page displays.
If your company uses LDAP, you must use your corporate tools to change your LDAP password.
2. Enter your old password, then your new password.
3. To confirm, re-enter your new password.
4. 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.

Accessing Help

You can display this document by clicking the Help button in the Advisors Browser Administration tab.

Logging Out

Log out of the Advisors Browser by clicking the Log Out button. This closes all instances of the application you are logged into.

Important

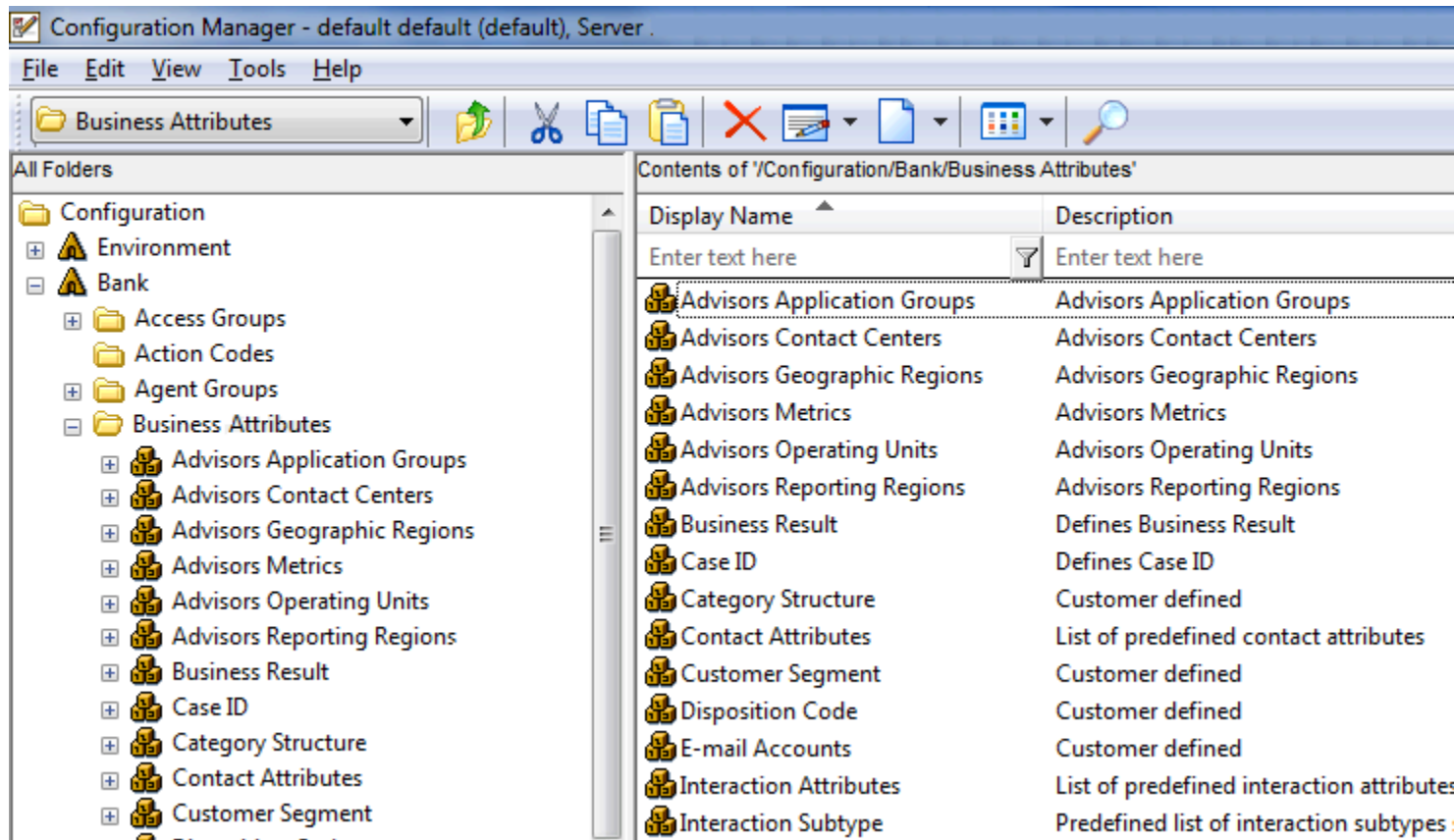
Using the browser Close button only closes the current instance of your application. Always log out before closing the browser.

Advisors Business Objects

All user profile functions and role-based access are handled in Configuration Server. To be able to fully complete the configuration of an Advisors installation and perform administrative functions, you must have access to the Genesys Configuration Manager. 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. Subsequently configured to completion in the Advisors Administration module.
3. Deleted only in the Configuration Manager (although it can also be removed from Advisors).

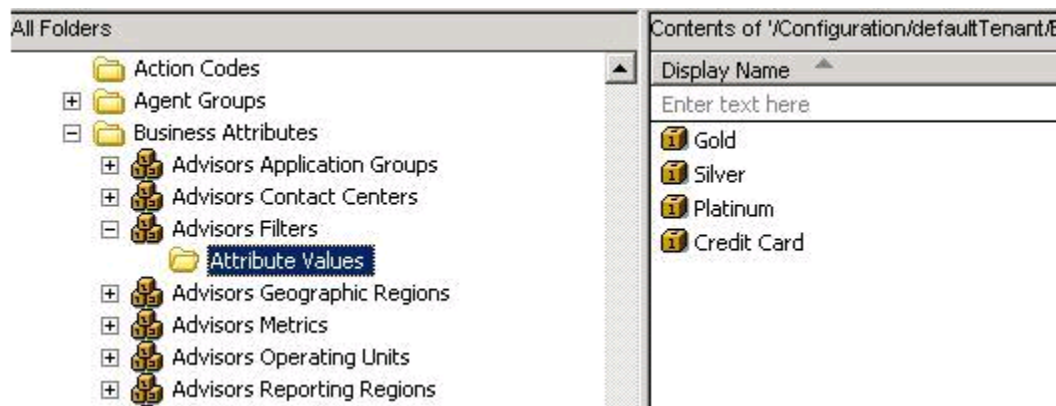
The Genesys Configuration Manager database is the master record holder for these Advisors business objects. Consequently, all create and delete functions are performed in the Genesys Configuration Manager. Metrics are created by the Platform database, and configured in the Advisors Administration module. 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. Objects (other than metrics) can be made active or inactive in the Advisors environment. The following screenshot shows the Advisors business attributes in Configuration Manager.



Configuration Manager Business Attributes

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

Starting in Release 8.1.5, the master list of filters for Advisors (for CCAAdv, WA, or FA) no longer comes from the Stat Server configuration, but from the Configuration Server. Advisors Filters is added to the Advisors Business Attributes section of the Configuration Manager (see the following screenshot).



Advisors Filters business attribute in Configuration Manager

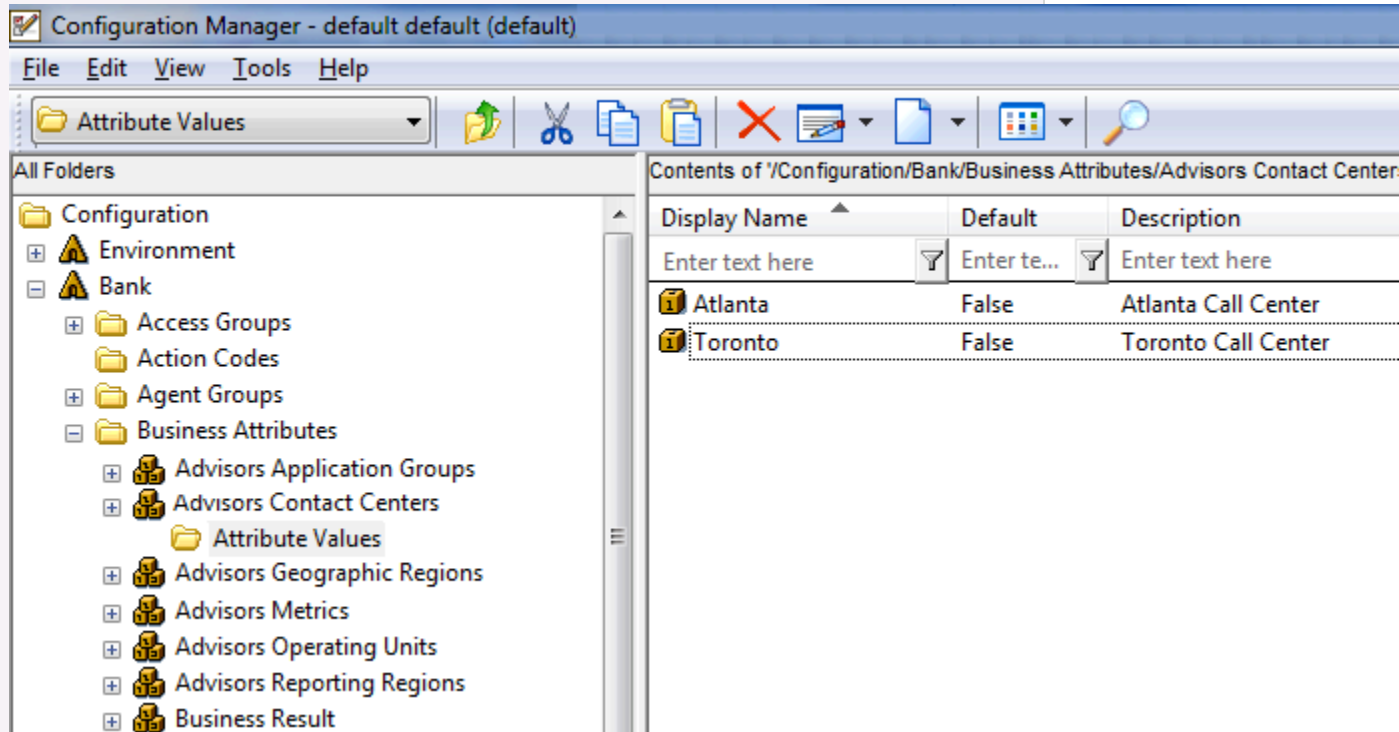
The Advisors Filters business attribute must exist on one – and only one – tenant. Genesys recommends you configure the Advisors Filters business attribute on a tenant that is the default tenant for the Advisors suite installation, on which you configure all Advisors metadata. If there are Advisors Filters 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. Advisors metadata elements (business objects and metrics) are not represented as standard objects in Configuration Manager. The business attribute values contain just the ID and name of the metadata 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. 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.

Example: 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

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, Type and Tenant are mandatory for completing the new object in Configuration Manager.

- **Name:** For metrics, this field is a concatenation of [Application].[ObjectType].[Channel].[Name]. For more information, see [Configuring Metrics](#). This name does not represent the name displayed for this metric on the dashboard, which can be configured on the Advisors Administration Metric Manager page. For CCAdv hierarchy objects, this field represents the name of the object, and is the display name.

Warning

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

- **Tenant:** The tenant to which this Advisors object belongs. This value is set when the Advisors Platform is installed, and cannot be changed.
- **Type:** This is always Custom . Once set, the value cannot be changed.
- **Description:** A simple description of this object. For a filter, enter the filter expression in the Description field. This description is used only in Configuration Manager. This is not the description used for the object in the Advisors application.

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-side configuration have been correctly processed.

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.

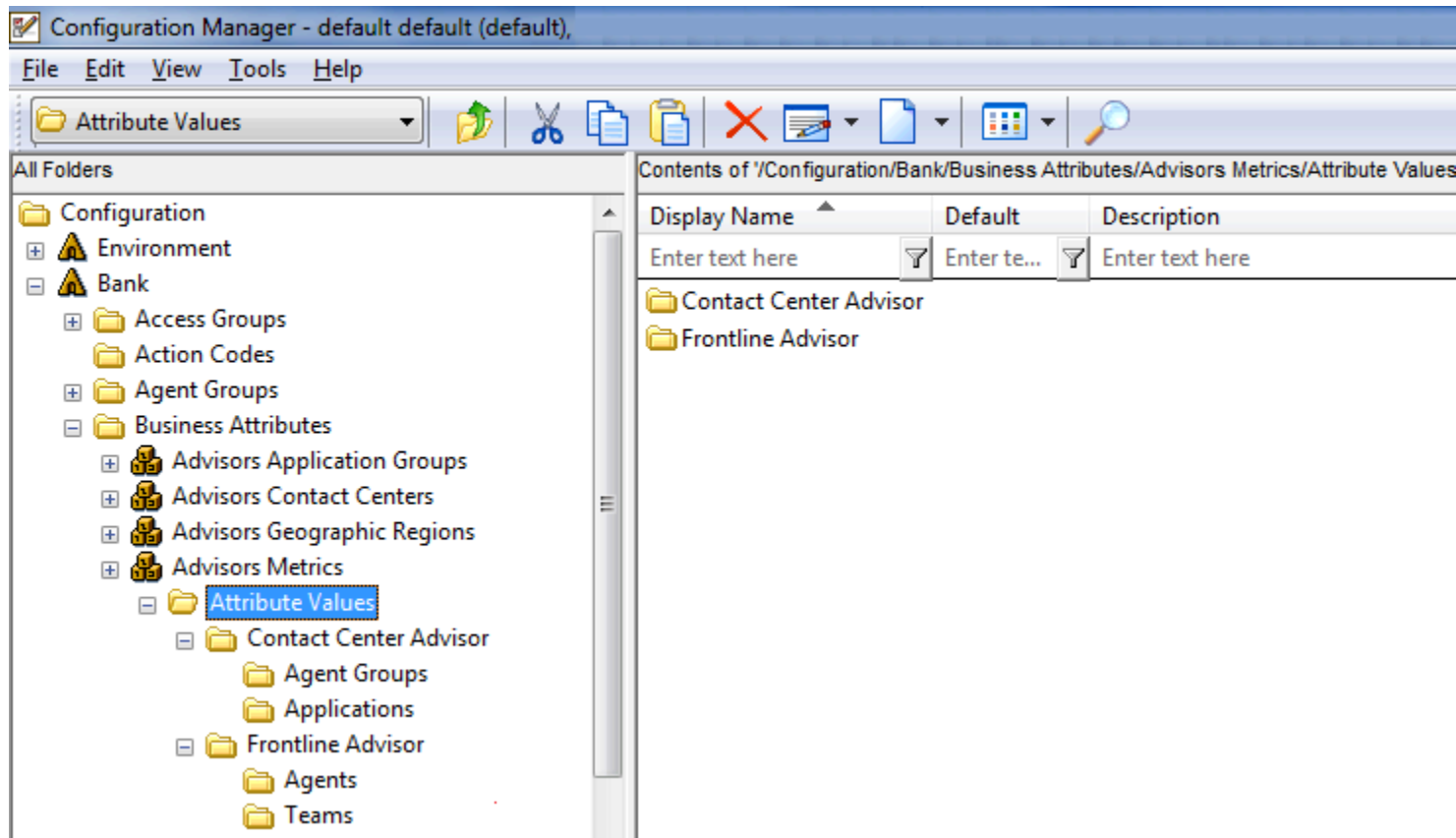
Synchronization

When a new object is created in the Configuration Manager and saved, it is automatically propagated to the Advisors environment and appears in the Administration module marked as not configured and inactive. Its remaining attributes must be configured in the Advisors Administration module. Once this configuration is complete, the object is available and can be used for rollups. Changes made on the Advisors side are not stored in the Configuration Manager.

Configuring 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

The `Display Name` field of the metric business attribute has only a copy of the business attribute's name.

Role Based Access Control

Because Advisors uses Configuration Manager business attributes, Advisors can take advantage of Genesys roles for controlling access at a very detailed level to Advisors business objects and metrics. This is referred to as role-based access control (RBAC).

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.

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. Roles consist of a set of role privileges. Role privileges are tasks that can be performed on a given type of data. They 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—see [Advisors Privileges](#). 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.

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.

Roles and Permissions

Elementary permissions protect access to a whole object. Roles are intended to work with permissions to more finely tune what a user can access.

So, the permissions applied to the object apply equally to all properties of the object—if you have access permissions, you see the entire object.

Roles, on the other hand, serve to protect properties of an object by hiding or disabling those properties to which you want to restrict access.

Different roles can have different access and allowed functionality for the same objects. In essence, roles resolve both problems with using 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 of an object to 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). Then, for that data that is available in the session, role privileges refine what can be done with the data.

One user can be assigned multiple roles, and one role can be assigned to multiple users. There is no

limit to the number of roles that can be present in the Configuration Manager.

Object Permissions in Advisors

Object permissions determine which users have access to a certain object or what objects a given user has access to. 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)

There is no limit on the number of access groups that are supported by the Advisors.

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). From 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.

Multiple Access Groups

A single user can 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.

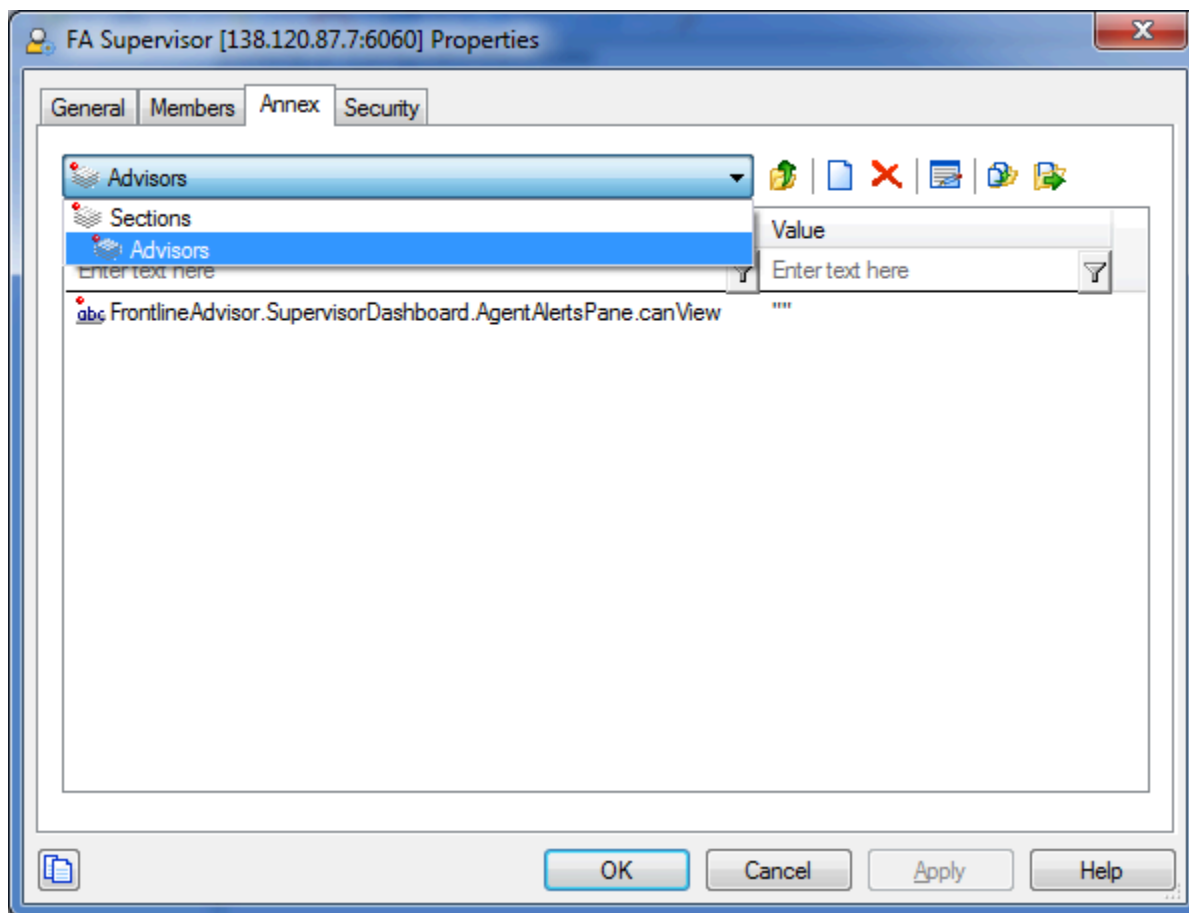
Advisors follow the principle of least privilege. The following scenarios show how this union should work:

- 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.

Privileges in Advisors

Functionality permissions, or privileges, determine what tasks or functions a user can execute on objects he/she has access to. Privileges are configured via roles. Privileges for each role are stored as key-value pairs in the Annex tab of that role in Genesys Configuration Manager. For example, below shows the Annex tab of a new role called FA Supervisor who can view the Agent Alerts pane on the Supervisor dashboard:



Assigning Privileges to a Role

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]

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 anything, or can be left blank.

Accumulation of Privileges

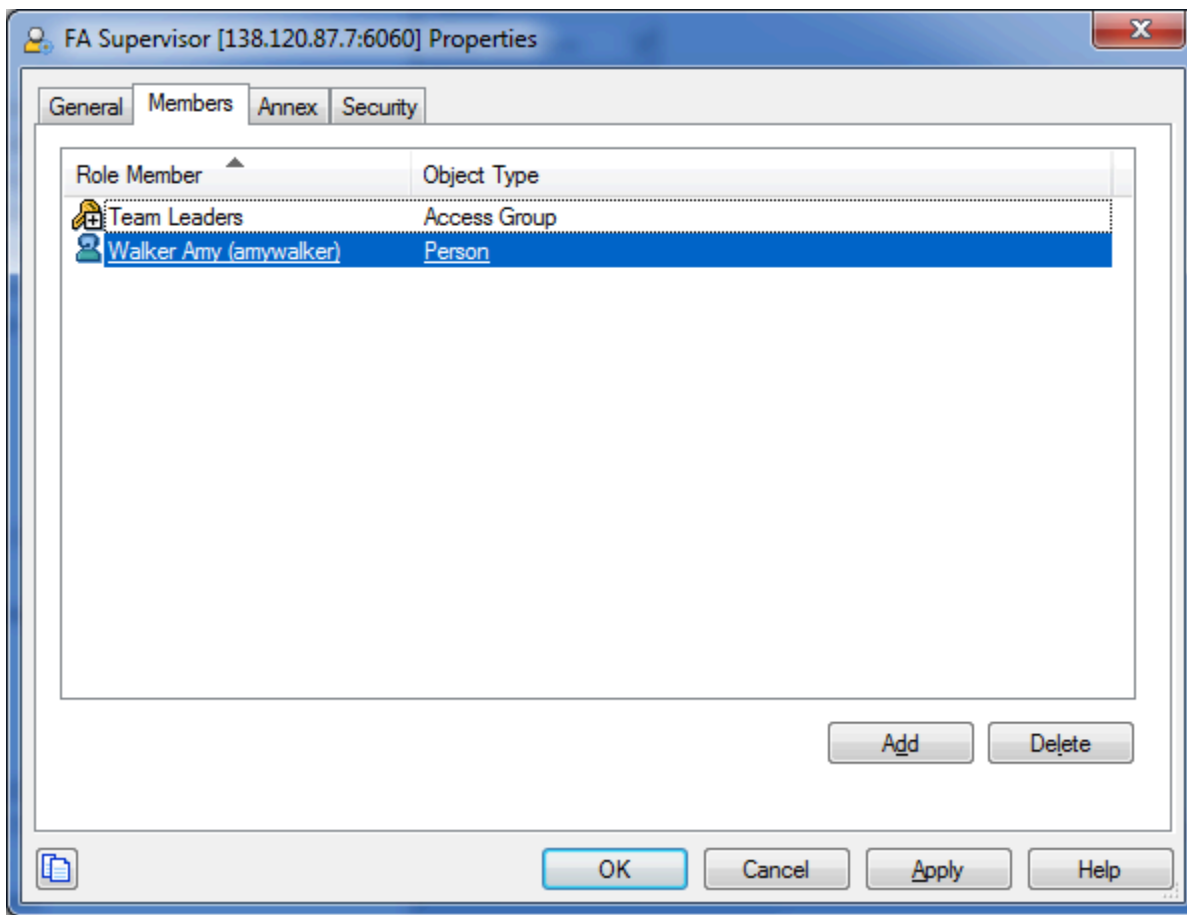
Roles are cumulative. A single user or access group can have multiple roles associated with them. The privileges in these roles are cumulative.

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 as shown in the following screenshot.

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 preceding screenshot, the role FA Supervisor has been assigned to:

- The Team Leaders 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 in order to be able to access the role.

Important

Names of access groups must not contain spaces.

Multiple Roles

You can assign more than one role to a user. 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.

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 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`

These role names can be changed 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](#)

Advisors Privileges

The following tables list all Advisor privileges. 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 Browser

Privilege	Behavior When Present	Behavior When Absent
Advisors.ChangePassword.canView	User sees the Change Password button located at the top of the Advisors Browser.	Change Password button is hidden.

Contact Center Advisor

Privilege	Behavior When Present	Behavior When Absent
ContactCenterAdvisor.ActionManagementReport.canView 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). Also, 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 by double-clicking on an Alert tile in the Map pane, or by clicking on the arrow for each alert in the Alerts pane.	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.
ContactCenterAdvisor.Dashboard.canView	User can access the CCAAdv dashboard. This is a replacement for the module access that was previously assigned on a user-by-user basis.	User cannot access CCAAdv 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 on the dashboard.	Column chooser button is not displayed on dashboard.
ContactCenterAdvisor.Dashboard.EnterpriseState.canView	User can see the Enterprise row	The Enterprise row is not sent

Privilege	Behavior When Present	Behavior When Absent
	and statistics on the dashboard.	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.PivotTableListView	User has access to the pivot table drop-down list that allows them to switch views of the pivot table.	Pivot drop-down list is not shown in the 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 tiles in the map, or by clicking on the arrow for each alert in the Alerts pane.	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.

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 Alerts pane.	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.
WorkforceAdvisor.Dashboard.AgentGroupsPane.canView This privilege is applicable to Release	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.

Privilege	Behavior When Present	Behavior When Absent
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.		
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 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 has access to the Column Chooser button on the dashboard.	The Column Chooser button is not displayed on the dashboard.
WorkforceAdvisor.Dashboard.EnterpriseStats.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 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. Also, 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 has access to the hierarchy drop-down list on the Contact Centers pane.	The hierarchy drop-down list does not display on the Contact Centers pane.

Alert Management

Privilege	Behavior When Present	Behavior When Absent
AlertManagement.canView This privilege is applicable to Release 8.1.3 and later. In a migration scenario,	User has access to the Alert Management tab.	The Alert Management tab does not display for the user.

Privilege	Behavior When Present	Behavior When Absent
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.		
AlertManagement.ActionManagementReport.canView	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.

Frontline Advisor

Privilege	Behavior When Present	Behavior When Absent
FrontlineAdvisor.SupervisorDashboard.canView	User can access the FA Supervisor Dashboard.	User cannot access the FA Supervisor dashboard, and the FA Dashboard tab is not shown to the user.
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canView (Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege)	User can see the Teams pane.	The Teams pane is hidden along with both alerts panes.
FrontlineAdvisor.SupervisorDashboard.AlertsPane.canView	User can see the Team and Agent Alerts panes.	Neither of the alerts panes is displayed on the dashboard. If access to the Team pane is not available, the Alert pane is not shown even though user has access.
FrontlineAdvisor.SupervisorDashboard.ColumnChooser.canView (Requires the FrontlineAdvisor.SupervisorDashboard.canView privilege)	User can access the column chooser.	The column chooser button on the dashboard is hidden.
FrontlineAdvisor.SupervisorDashboard.TeamsPane.canSort	User can sort the entries in the Team pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Team pane. The cursor does not change when hovering over a column header.
FrontlineAdvisor.SupervisorDashboard.TeamAlertsPane.canSort This privilege is applicable to Release 8.1.3 and later. In a migration scenario,	User can sort the entries in the Team Alerts pane. The cursor changes when hovering over the header of a column that can be	User cannot sort entries in the Team Alerts pane. The cursor does not change when hovering over a column header.

Privilege	Behavior When Present	Behavior When Absent
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.	sorted.	
FrontlineAdvisor.SupervisorDashboard.AgentAlertsPane.canSort 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 sort the entries in the Agent Alerts pane. The cursor changes when hovering over the header of a column that can be sorted.	User cannot sort entries in the Agent Alerts pane. The cursor does not change when hovering over a column header.
FrontlineAdvisor.Administration.canView	User can access the FA Administration module.	User cannot access the FA Administration module, and the FA Administration tab is not shown to the user.
FrontlineAdvisor.Administration.Settings.canView (Requires the FrontlineAdvisor.Administration.canView privilege)	User can access the Settings tab in the FA Admin module.	Settings tab is not shown to the user.
FrontlineAdvisor.Administration.Hierarchy.canReload (This requires the Settings tab to be accessible via the FrontlineAdvisor.Administration.Settings.canView privilege)	User can initiate a hierarchy reload through the action on the Settings tab.	Hierarchy reload action is not accessible.
FrontlineAdvisor.AgentDashboard.canView	User can access the FA Agent Dashboard.	User cannot access the FA Agent dashboard, and the FA Agent Dashboard tab is not shown to the user.
FrontlineAdvisor.AgentDashboard.AlertsPane.canView (Requires FrontlineAdvisor.AgentDashboard.canView privilege)	User can see the Alerts pane.	The Alerts pane is not displayed.
FrontlineAdvisor.AgentDashboard.ColumnChooser.canView (Requires FrontlineAdvisor.AgentDashboard.canView privilege)	User can see the Column Chooser.	The Column Chooser is not displayed.

Administration Module

Privilege	Behavior When Present	Behavior When Absent
AdvisorsAdministration.canView	User has access to the	User cannot access the

Privilege	Behavior When Present	Behavior When Absent
	Administration module.	Administration Module, and the module tab is not shown to the user.
AdvisorsAdministration.SystemConfiguration.canView	User can access System Configuration page; option is shown on menu.	System Configuration option is not shown on the Administration 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.Thresholds.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 menu.	Application Configuration option is not shown on the Administration 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 Metrics page; option shown on menu.	Metrics option is not shown on the Administration menu.
AdvisorsAdministration.MMW.canCreate	User can create custom metrics.	The Create function and the Copy function do not display in the Metric Manager.
<p>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.</p>		
AdvisorsAdministration.MMW.canEdit	Grants privilege to edit any metrics.	The Edit function does not display in the Metric Manager.
<p>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.</p>		
AdvisorsAdministration.MMW.canDelete	Grants privilege to delete custom metrics.	The Delete function does not display in the Metric Manager.
<p>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</p>		

Privilege	Behavior When Present	Behavior When Absent
must update existing roles, or create new roles, and add the privilege to allow the described access or activity.		
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 menu.	Manual Alerts option is not shown on the Administration 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.ObjectConfiguration	User can access the Genesys Adapter Object 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 options shown on menu.	Control Panel section (which includes the Notification Lists and Notification Templates options) is not shown on the Administration 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 Manager are not shown in the corresponding Administration page.

Objects in the Administration Module

Before you configure the relationships, it is important to note that there are some dependencies that affect the sequence of the software maintenance:

- After you first install Contact Center Advisor or Workforce Advisor, you must define your external data source systems manually in the database if you did not create them when you installed the XML Generator of Contact Center Advisor.
- After the external data source systems are defined, you must run the 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.
- The relationships between applications and agent groups support certain functionality in the dashboards. First, they support highlighting agent groups when applications are selected, and vice versa. Second, they support displaying the set of agent groups related to both a contact center and an application group. The XML Generator updates these relationships when it starts, and after that once per day, overnight. For the configuration to take effect immediately, stop and restart XMLGen.

Configuring Organizational Hierarchies for the Dashboard

Menu options for the Administration module are controlled by individual privileges, so Administrators will only see menu items for which they have privileges assigned.

To display contact centers on the dashboard, multiple procedures must be completed and rollups 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 alert behavior, as well as the application-and-agent group relationship setting.
 - Data Source: To set the update-delay threshold rule and notification distribution list.
 - 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. Specify whether they are reporting regions, or operating unit regions, or geographic regions. See [Regions](#).
- Application Groups /Thresholds: To provide a meaningful rollup of types of contact center activity in the summary displays, complete the configuration of application groups (see [Application Groups and Thresholds](#)). Threshold rules define the critical (red) and warning (yellow) conditions that trigger alerts 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 a contact center for a data source that supplies services, another kind of real-time call data, or agent groups, and select a geographic region; see [Configuring Contact Centers](#).

-
- **Switches/Peripherals:** To deactivate a Genesys switch or Cisco peripheral. A peripheral is a communications interface between a call distributor and call router. To make a peripheral active, see [Switches and Peripherals](#).
 - **Application Configuration:**
 - **Rollups:** To configure the hierarchy displayed on the dashboard and control how it is rolled up, 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 other properties, such as Zero Suppress.
 - **Contact Group Configuration: (WA only)**
 - **Rollups:** To configure the hierarchy displayed on the dashboard and control how it is rolled up, 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 contacts, contact centers, and application groups you want to include in 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:** In Release 8.1.5, 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.

Zero Suppression

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

The CCAAdv dashboard can simultaneously display metrics from more than one time period. 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 period that is now zero-suppressed, or was zero-suppressed. In time, the row will either not display at all, or completely display.

Zero Suppression Rules

The following sections provide guidelines for using zero suppression.

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 = 0 and calls handled = 0

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 = 0 and e-mails processed = 0 and Web-chats entered = 0 and Web-chats processed = 0

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 = 0 and calls handled = 0 and logged on = 0

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

- e-mails offered = 0 and e-mails handled = 0 and Web-chats offered = 0 and Web interactions handled = 0

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

The Logged On criterion is included by default.

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 = 0 and calls handled = 0

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

- e-mails entered = 0 and e-mails processed = 0 and Web-chats entered = 0 and Web-chats processed = 0

Application Group

For WA, if zero suppress = Yes and forecast calls offered, calls offered, and calls handled are null or 0, 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 = 0 and calls handled = 0

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

- e-mails entered = 0 and e-mails processed = 0 and Web-chats entered = 0 and Web-chats processed = 0

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.

The screenshot displays the 'System Configuration' page with the 'Contact Center/Workforce Advisor' tab selected. The page has a dark blue header with the title 'System Configuration'. Below the header, there are three tabs: 'Contact Center/Workforce Advisor' (active), 'Data Source', and 'Modules'. The main content area contains several configuration fields:

- Notification Refresh Rate (minutes):** A text input field containing the value '5'.
- Application-To-Agent Group Relationships:** A dropdown menu showing 'Auto Override'.
- Show Totals and Averages row for Agent Groups:** A dropdown menu showing 'Yes'.
- Default Grouping:** A section containing a dropdown menu for 'Contact Center Advisor' showing 'Reporting-Contact Centers'.

At the bottom right of the configuration area, there are 'Save' and 'Cancel' buttons. On the right side of the page, partially visible, are labels for 'Threshold Trigg', 'Display Agent Group', and 'Integrated C'.

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.

- **Threshold Trigger Delay Rate (minutes):** Controls how many minutes a metric's value must exist in a state exceeding a threshold before the application or contact group triggers an alert e-mail message and displays on the map. Peripheral offline alerts (Cisco ICM only) and manual alerts are an exception to the threshold trigger delay rate: they display 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 Advisor 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, or dependent, configuration between Contact Center Advisor and WorkforceAdvisor. If you select independent configuration mode, WA operates independently from the CCAdv configuration structure. For detailed information, see *Performance Management Advisors 8.1 Deployment Guide*.

- **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 rollups to include that region type. If users are unable to change the grouping on the dashboard, ensure that the region type in the default grouping is also specified in the rollups for those users.

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 a data source has exceeded 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. 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 amount of time (in 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. This field 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, Deployment URL, and Version: You can modify the application name that displays on the Genesys Advisor tabs that are used to switch between the applications.

Regions

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

Regions

search

Name	Configured	Type	Zero Suppressed
ABCD	No	Reporting	
ABCD	No	Operating Unit	
abcd	No	Operating Unit	
abcd1	No	Operating Unit	
ABCD1	No	Reporting	
ABCD1	No	Operating Unit	

Display 15 records per page.

Edit

Name

Active

☐ Yes

Type

Select

* Zero Suppressed

☐ Yes

Save

Reset

Regions Page in the 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.

In the pane, alerts are shown in relation to a geographic region. CCAAdv 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 remove the region 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.
- Zero Suppressed: Select Yes for contact centers where little or no activity is expected.

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 rollups.

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

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

Display records per page.

General Application Thresholds Contact Group Thresholds

Edit

Name

Active ☐ Yes ☒ No

Application Groups/Thresholds Page

Adding/Deleting a New Application Group in Configuration Manager

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

Configuring an Application Group's Attributes in Advisors

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

Complete the fields in the Edit panel as follows:

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

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

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

Removing an Application Group from Advisors Configuration

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

Important

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

You cannot remove an application group if:

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

Configuring Application Groups and Thresholds

The Application Groups/Thresholds page allows you to:

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

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

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

You cannot reset or delete a threshold if it is currently causing an active alert. To end the alert and make it inactive, change the threshold's values so that the metric no longer causes a violation. When the alert ends, and CCAAdv or WA has deleted it from the Advisors database, you can reset the threshold. The Application Thresholds page and the Contact Group Thresholds page display the threshold rule details including:

- **Application Group:** Affected application group name
- **Metric:** Display name of the metric to which the threshold will be applied, when the metric belongs to an object related to the application group
- **Min and Max:** Minimum and maximum permissible values
- **Decimal Places:** Number of decimal places to which the metric value is defined
- **Lower-Bound Warning, Lower-Bound Critical:** The lower threshold limits for warning and critical violations
- **Upper-Bound Warning, Upper-Bound Critical:** The upper threshold limits for warning and critical violations

Tip

You can define lower bound thresholds, or upper bound thresholds, or both.

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

Important

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

Exceptions

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

a defined time period. Exception rules can repeat daily, weekly, or monthly.

System Maintenance of Expired Alerts

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

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

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

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

Thresholds and Notifications

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

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

Typically a Threshold Trigger Delay Rate would be in the 10-30 minute range and is entirely dependent upon the urgency and severity of issues. The Notification Refresh Rate may or may not be relevant. Many organizations send an e-mail notification only once. Others with critical performance targets may want to know if an alert is still active and prefer an updated e-mail. While

these two configuration settings are very important to the notification function, it is important to remember that how the root thresholds are set is the most important consideration.

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

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

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

Some organizations may prefer to distribute yellow/cautionary alerts to a small (sometimes one person) group that is responsible for the individual business unit or location affected. If the alert hits a red/critical state, the distribution widens to all potentially affected sites as well as up the management chain. Distribution lists, like many other aspects of Advisor, will rarely perform well if kept static. The business environment changes; performance targets change; personnel change. Regular and periodic tuning is required to ensure optimal utilization of these and many other Advisor capabilities.

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

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 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 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.

Updating 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 Edit panel, select a metric to work with.
4. Type the values for the upper-bound and/or lower-bound limits for the selected metric.
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](#).

Adding 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 that the organization does not try and 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 color-coded violations on the dashboard, alerts triggering to the map and the Action Management console as well as e-mail distributions going out. 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, then 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 in all calculations and display of alerts. Multiple thresholds may affect the same moment in time. In general, 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, but not before. For instance, from 07:55-08:50, assume a metric value is not a 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 a threshold rule if it is causing an active alert. You cannot delete an exception if it is causing an active alert, or an inactive alert that has not yet been deleted from the Advisors database.

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. For example, you might have different expectations on holidays or Friday afternoon than you do on Wednesday afternoon.
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

search

Name	Configured	Geographic Regions	Data Source	Type
Alexandria	Yes	Geo ABC	Other	Network
Denver	No			
El Paso	No			
Miami	No			
Orlando	No			

Display 5 records per page.

Edit

Name

Alexandria

* Open Time

00:00

* Close Time

23:00

Type

Network

* Effective Date

04/24/2012

* Time Zone

Pacific Time (US , Canada), Tijuana (GMT-07:00)

Map Location

40.43

(Latitude)

-75.75

(Longitude)

* Data Source

Other

Expiration Date

Agent Groups

Contact Centers

+

search

Name

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 remove the contact center from the Advisors configuration. To add a new contact center in Configuration Manager, see [Advisors Business Objects](#). In addition to the Name and Type fields, add the data source for the contact center. This cannot be changed subsequently. In the Data Source field, valid values are:

- **Service:** for site contact centers
- **Other:** for site and network contact centers
The value Other represents voice queues, interaction queues, and call types.

To delete a contact center from Configuration Manager, see [Advisors Business Objects](#).

Configuring the Attributes for a Contact Center in Advisors

To edit a contact center's configuration attributes, select it in the upper panel of the Contact Centers page and edit the 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, Type, and Data Source fields cannot be edited. Complete the fields in the Edit panel. When you have made the Edit panel selections and saved them, the following happens:

- If the contact center 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 screen.
- The Remove from Advisors configuration button is activated.

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.

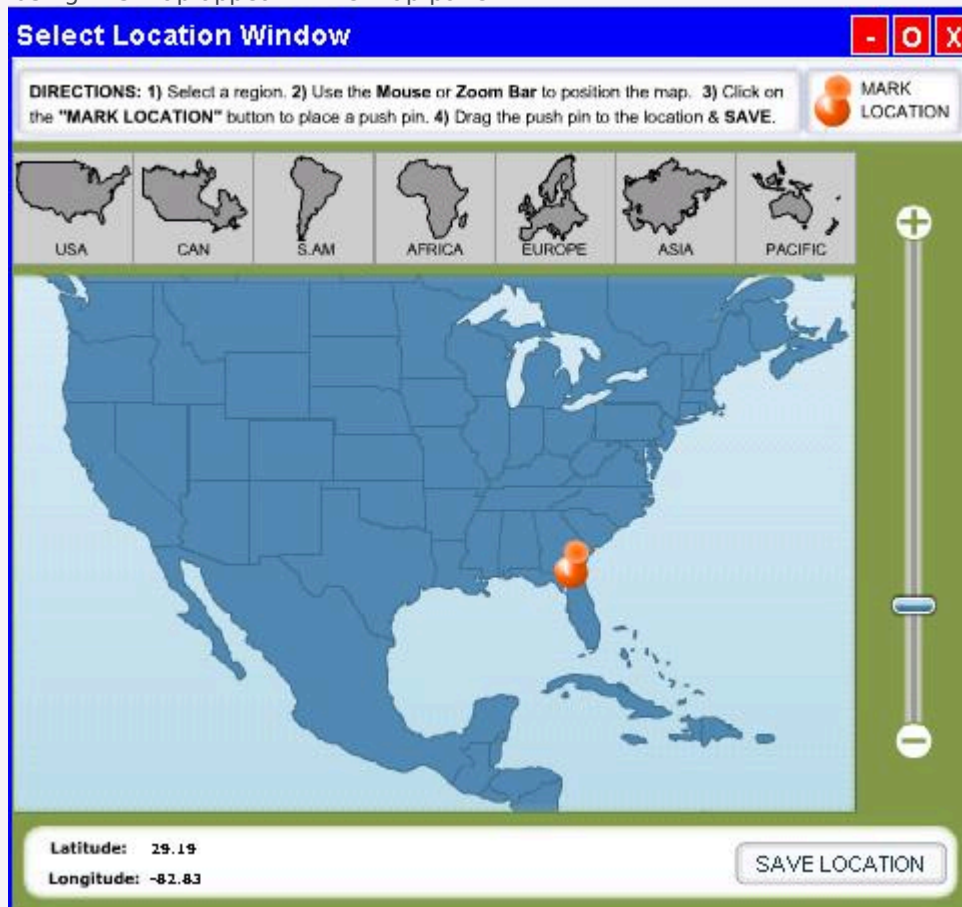
A network contact center does not require map coordinates (that is, latitude and longitude). However, it will not display on the map without them. If you add or remove the latitude and longitude later, wait for at least five minutes for the change to propagate to the applications. Then log out of the dashboard and log back in for the change to be reflected in the dashboard. 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.

Configuring 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 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.
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. If you change this setting, you must log out of the dashboard and back in for this change to take effect. There may be a delay of a few minutes as the change propagates through the applications.
7. To set the location of the contact center on the map, type the decimal latitude and longitude or click the map icon. The mapping window opens (see the following screenshot). Instructions for using this map appear in the map pane.



Select Location Window

8. Click the pushpin tool. The pushpin displays on the map.

9. Drag the pushpin to the correct location.
10. Click the Save Location button. The mapping window closes.
11. Enter the type of the contact center: Site or Network.
12. Select the geographic region for the contact center from the drop-down list.
13. 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.
14. 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 Switches/Peripherals page allows you make a switch or peripheral active or inactive and shows their assignments to contact centers as defined in the Application Configuration module. The following screenshot shows the Switches/Peripherals page in the Administration module.

Switches/Peripherals

Name ▲	Assigned Contact Centers	Active
lxnSwitch		Yes
K-Worker		Yes
K-Worker Generic		Yes
LucentG3		Yes
Meridian		Yes

Display **5** records per page.

Details

Assigned Contact Centers

Active ☐ Yes

Save

Reset

Switches/Peripherals Page

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

Switches and peripherals are added automatically. For each switch/peripheral, a user with access to the Switches/Peripherals page may update the status (active or inactive). Applications that belong to inactive switches/peripherals will be excluded from the dashboard. An administrator assigns a switch/peripheral to a contact center indirectly. The assignment happens when a user that has access to the Application Configuration page 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.

Activating Switches and Peripherals

Start Procedure

1. To activate a switch or peripheral:
 - 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.
2. Click the Save button.
A confirmation message displays and the assignment and active status displays in the list.

Application Configuration

Access to applications, contact groups, 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. To configure the hierarchy displayed on the CCAdv dashboard and control how it is rolled up, you must create the associations between applications, agent groups, and the levels in the hierarchy (for example, regions, contact centers, and application groups). Access to objects that form levels in the hierarchy must be configured by an administrator in Configuration Manager. Objects to which users have no permissions will not be displayed. The Application Configuration page is used for configuration of:

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

Application Configuration

Contact Center All

Application Group All

Reporting Region All

Operating Unit

SL Threshold Time All

Include in Rollup All

Zero Suppress All

Display on Dashboard

Rollups

Applications - Agent Groups

Application Details

Object Type
☒ Voice Queues
 ☒ Interaction Queues
 ☒ Call Types
 ☒ Services

x search
🔍

Assigned Applications								
<input type="checkbox"/>	Name ▲	Descriptive Na...	Contact Center	Application Gr...	Reporting Regi...	Operating Unit	SL Threshold ...	Inclu
<input type="checkbox"/>	238		Atwater	[ABC]	CAT	3G	20 sec	Yes
<input type="checkbox"/>	[defaultTenant] 7...		Austin	NewABC	CATexpansion	3Gexpansion	20 sec	Yes
<input type="checkbox"/>	[defaultTenant] 7...		Austin	NewABC	CATexpansion	3Gexpansion	20 sec	Yes
<input type="checkbox"/>	[defaultTenant] 7...		Austin	NewABC	CATexpansion	3Gexpansion	20 sec	Yes
<input type="checkbox"/>	Cafe		Atwater	[ABC]	CAT	3G	20 sec	Yes
<input type="checkbox"/>	Cafe2		Atwater	[ABC]	CAT	3G	20 sec	Yes
<input type="checkbox"/>			Atwater	[ABC]	CAT	3G	20 sec	Yes

Display 20 records per page.

Assign
Unassign

x search
🔍

<input type="checkbox"/>	Name ▲	Object Type	Data Source Name	Genesys Switch	Genesys Ter
<input type="checkbox"/>	12345	Call Type	felix_awddb	N/A	N/A
<input type="checkbox"/>	238_Double_Dip	Call Type	felix_awddb	N/A	N/A
<input type="checkbox"/>	399_Double	Call Type	felix_awddb	N/A	N/A
<input type="checkbox"/>	8005552628	Call Type	felix_awddb	N/A	N/A
<input type="checkbox"/>	8005552356	Call Type	felix_awddb	N/A	N/A
<input type="checkbox"/>	8005557289	Call Type	felix_awddb	N/A	N/A

Display 30 records per page.

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. For CCAdv, you assign agent groups, an application group, reporting region, and operating unit to an application for a contact center. 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. For agent groups to display on the dashboard, the Application-to-Agent Group relationship must be created. The rollups for network contact centers must be configured first to make agent groups available for the agent-group contact centers. For Cisco TDM, 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. 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.

Tip

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

First, they support displaying the set of agent groups related to both a contact center and an application group, as well as highlighting agent groups when applications are selected, and vice versa. 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.

Second, the relationships are used for deriving some agent group metrics that need to be displayed on the related applications and related hierarchy levels (aggregated objects) such as regions, contact centers, application groups, and enterprise.

Filtering the Display of Rollups

You can filter the list of objects by the 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.

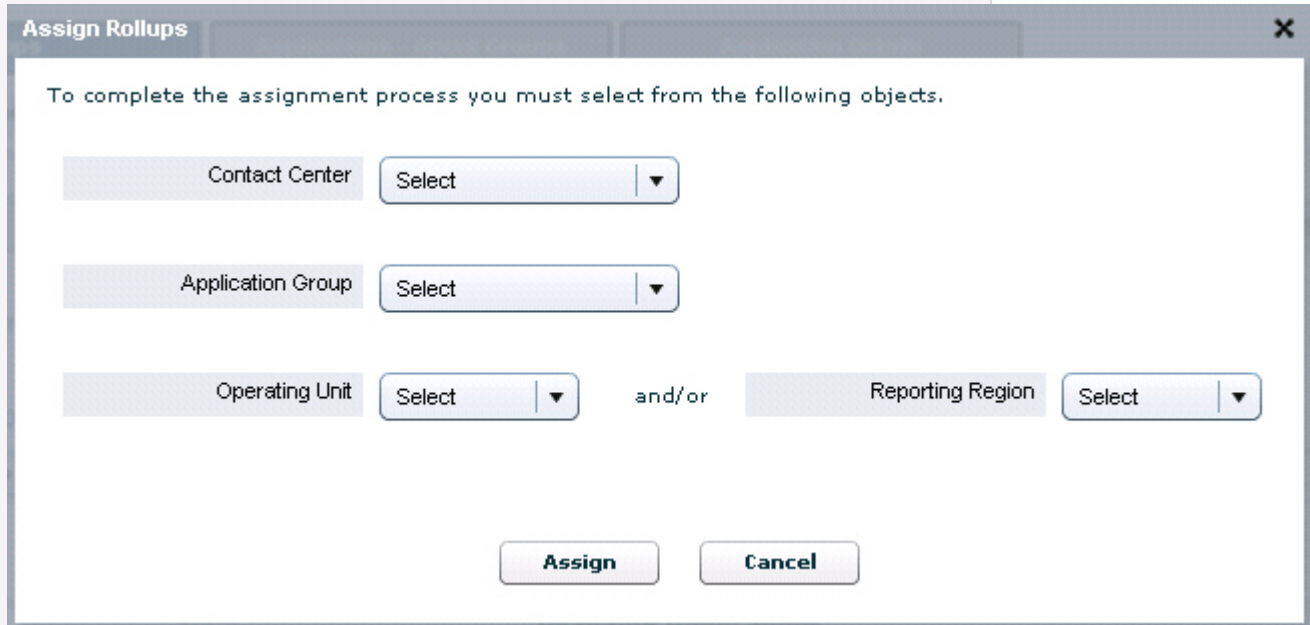
Assigning and Unassigning Applications for

Rollup

Start Procedure

1. Select Rollups.
2. Use the filter buttons at the top of the page to filter the displayed list of records.
If you do not select a filter when assigning an application to a rollup, the following defaults are applied:
 - SL Threshold Time: 20 sec
 - Zero Suppress: No
 - Display on Dashboard: Yes
 - Include in Rollup: Yes

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 | Rollups tab.
3. Select one or more applications from the list by checking their check box(es).
4. To assign an application for rollup, select it from the Available Applications table and click the Assign button.



The image shows a dialog box titled "Assign Rollups" with a close button (X) in the top right corner. Inside the dialog, there is a message: "To complete the assignment process you must select from the following objects." Below this message are four selection fields, each consisting of a label and a dropdown menu. The first field is "Contact Center" with a dropdown showing "Select". The second field is "Application Group" with a dropdown showing "Select". The third field is "Operating Unit" with a dropdown showing "Select". The fourth field is "Reporting Region" with a dropdown showing "Select". Between the "Operating Unit" and "Reporting Region" fields is the text "and/or". At the bottom of the dialog are two buttons: "Assign" and "Cancel".

Assign Rollups page

5. Define the rollup by select the Contact Center, Application Groups, Operating

Unit and/or Reporting Region for this application from the drop-down lists of options.

Assigning the application group, reporting region, and/or operating unit is required for the application to display on the dashboard and to be included in the metric rollup for the specific grouping. In order for an application to be rolled up to any grouping, you must select a contact center and an application group for it.

6. Click Assign to save the changes.
When you click Assign, the Assign prompt pop-up does not appear if the mandatory options are already specified in the filter options. If only some of the mandatory options are specified, then only the remaining missing options need to be specified.
7. To unassign an application, check its check box in the Assigned table, and click Unassign. No confirmation message is displayed.

Tip

An alternative method to selecting the attributes for applications is to select them from the filter area. To do this, click Filter, select from the Available list then click Assign.

Editing 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 in the Application | Rollups tab.
3. Select an application from the list by checking its check box. You can select multiple applications in the same way. To navigate to the next or previous page use the page controls.
You can select multiple applications for edit, but the changes you make will apply to all selected applications.
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

Contact Center	No Change ▼	Reporting Region	No Change ▼
Application Group	No Change ▼	Operating Unit	No Change ▼
SL Threshold Time	No Change ▼	Include in Rollup	No Change ▼
Zero Suppress	No Change ▼	Display on Dashboard	No Change ▼

Save **Cancel**

Edit Rollups page

Assigning the application group, reporting region, and/or operating unit is required for the application to display on the dashboard and to be included in the metric rollup for the specific grouping. In order for an application to be rolled up to any grouping, you must select a contact center and application group for it.

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

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.

The screenshot displays the 'Applications - Agent Groups' configuration interface. It features three main tabs: 'Rollups', 'Applications - Agent Groups' (which is the active tab), and 'Application Details'. Within the active tab, there are two radio buttons: 'View Applications - Agent Groups' (selected) and 'View Agent Groups - Applications'. To the right of these buttons are two links: 'Display Descriptive Names' and 'Display Technical Names'. The central part of the interface contains two search bars, each with a search icon. Below the first search bar is a list of applications with a scroll bar. The list includes: 12345 (Call Type, felix_awddb), 238_Double_Dip (Call Type, felix_awddb), 399 (Call Type, felix_awddb), 8005552628 (Call Type, felix_awddb), 8005552356 (Call Type, felix_awddb), 8005557289 (Call Type, felix_awddb), 8003700538 (Call Type, fedex_awddb), and 8004685754_Spanish_Ground (Call Type, fedex_awddb). Below the list is a pagination bar showing 'Display 20 records per page. Page 1 of 334'. To the right of the application list is a section for 'Assigned Agent Groups' and 'Available Agent Groups', each with a search bar and a list. Below these sections are 'Save' and 'Reset' buttons.

Configuration Manager Business Attributes—Individual Objects

Maintaining 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. Starting in Release 8.1.5, 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 8.1 Deployment Guide. Only the agent groups from the same external data source display for the selected application.

Start Procedure

1. Select the Applications-Agent Groups tab.
You can opt to display either descriptive or technical names by clicking the Display Descriptive/Technical Name link.
You can reverse the order of display by selecting the relevant radio button.
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.

Rollups

Applications - Agent Groups

Application Details

×

search

Q

Assigned Applications

Name ▲	Descriptive Name	SL Threshold Time	Include in Rollup	Zero Suppress	Di
238		20 sec ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
[defaultTenant] 7...		20 sec ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
[defaultTenant] 7...		20 sec ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
[defaultTenant] 7...		20 sec ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Cafe		20 sec ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Cafe2		20 sec ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Display 20 ▼ records per page.

⏮

⏪

Page 1

Save

Reset

×

Search

Q

Available Applications

Name ▲	Object Type	Data Source Name	Genesys Switch	Genesys Tenant	CISCO Per
[defaultTenant] 20001...	Voice Queue	Genesys	Meridian	defaultTenant	N/A
[defaultTenant] 20002...	Voice Queue	Genesys	Meridian	defaultTenant	N/A

Display 5 ▼ records per page.

⏮

⏪

Page 1

of

Application Details tab

Maintaining application details

The master list of available SL threshold times is predefined. To add additional entries to this list, new entries can be added to the default list that is stored in the platform database table SL_THRESHOLD.

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 generated name.
 - SL Threshold Time: (Applicable only to Genesys voice queues (ACD &

Virtual queues)) Select a value from the drop-down list.

- Include in Rollup: Check the box to include the application in rollups.
- 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.
Assigning the application group, reporting region, and/or operating unit is required for the application to display on the dashboard and to be included in the metric rollup for the specific grouping. In order for an application to be rolled up to any grouping, you must select a contact center and application group for it.

3. Click Save.

Contact Group Configuration

Access in Advisors to contact 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. 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 8.1 Deployment Guide. Access to objects that form levels in the hierarchy 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. To configure the hierarchy displayed on the WA dashboard and control how it is rolled up, you must create the associations between contact groups, agent groups, and the levels in the hierarchy (for example, regions, contact centers, and application groups). In Genesys Advisors, the term contact group is synonymous with the terms activities, forecast group, staff group, and contact type. The Contact Group Configuration page is used for configuration of:

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

With the introduction of the independent configuration mode, and if that mode is enabled, you can manually assign any contact group to applications and agent groups, unless the contact group is mapped to an agent group contact center (AGCC). If such a contact group is selected on the Contact Groups - Agent Groups tab, all published agent groups that are not mapped to this contact group display in the Available Agent Groups pane and can be mapped. When you map a contact group to an AGCC, all agent groups with the following characteristics display in the Available Agent Groups pane and can be mapped to the selected contact group:

- mapped to the same AGCC as the contact group
- Include in WA rollup property is set to Yes
- not already mapped to the selected contact group

AGCC names display with the names of the parent network contact center (NCC) and use the format NCC Name: AGCC Name. Setting the Include in WA agent group rollup property to No on the Rollups tab 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. There is no restriction on the number of contact groups to which an agent group can be mapped.

Rollups Tab

The Rollups tab allows you to assign hierarchy objects to a workforce management system's forecasting entities (activities in Genesys WFM, forecast groups and staff group in Aspect eWorkforce Management, and contact types in IEX TotalView). You must import contact groups from your WFM system before configuring rollups on the Contact Group Configuration/Rollups page. For information about importing contact groups from a WFM system, see that section in the *Performance*

*Management Advisors 8.1 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.

The IEX data source names, the eWFM, and Genesys WFM data source names must be unique. To display a contact group on the WA dashboard, in the Rollups tab, assign a contact center and application group to it. You must also assign either a reporting region or an operating unit to it. If you have selected the integrated configuration mode, in the Contact Groups - Applications page, you must assign one or more applications to the contact group. Chat and e-mail are not available in WA; consequently, you cannot assign an application that is an interaction queue. In integrated configuration mode, agent groups assigned to the applications are, in effect, thus assigned to the contact group. Finally, in the Contact Groups - Agent Groups page, you can directly assign agent groups to contact groups that are assigned to agent-group contact centers. If there are no agents logged on to the agent group where the zero-suppress property is Yes and calls handled are zero and calls offered are zero, the agent group will be hidden. Depending on your WA system configuration, logged-on could be excluded from this criterion. The logged-on criterion is included by default, but can be excluded by changing the value of a property in the conf/WorkforceUtilization.properties file. For each contact group, you provide a Descriptive Name. Descriptive names display on the dashboard. Hovering over the descriptive name displays the generated name.

Assigning contact groups for rollup

Start Procedure

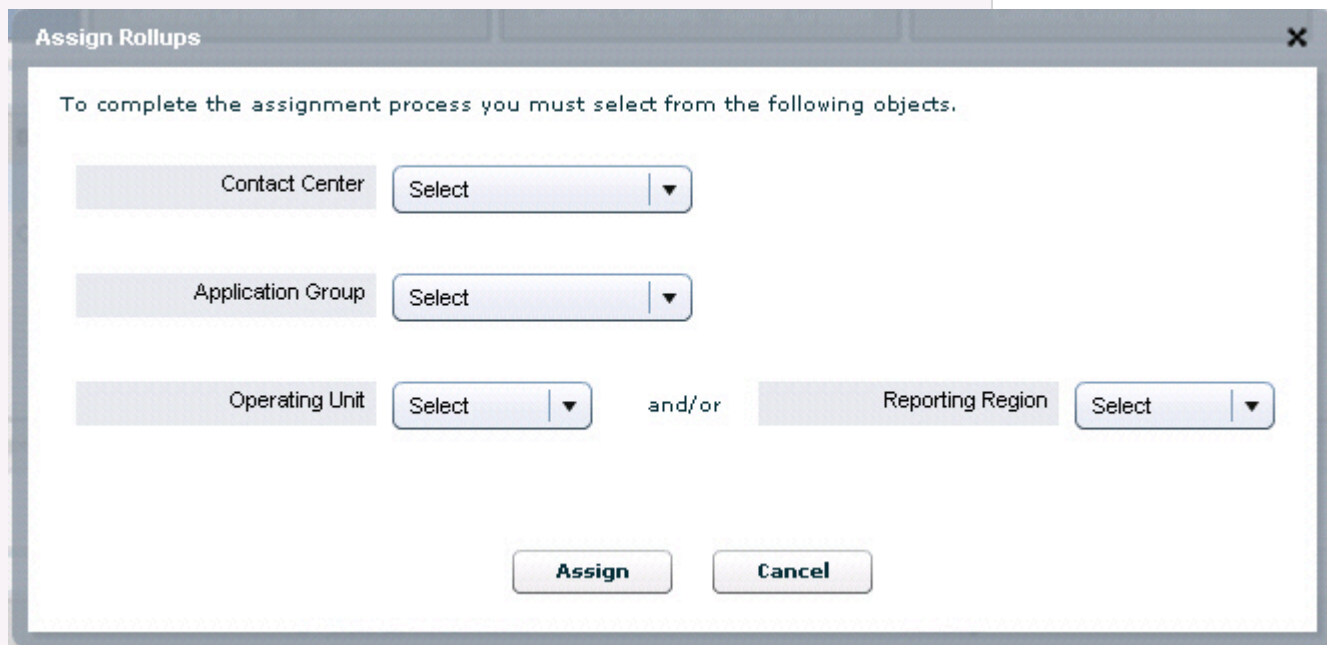
1. Select the Rollups tab.

The following screenshot shows the Rollups tab in the Contact Group Configuration page.

Name	Descriptive Name	Contact Center	Application Group	Reporting Region	Operating Unit	Include in Rollup
<input type="checkbox"/> BSE	BilingSilverEmail	Network Other Contact Center	APPLICATION GROUP 1	Reporting Region 1	Operating Unit 1	Yes
<input type="checkbox"/> DOI_XD		Network Other Contact Center	Application Group 2	Reporting Region 2	Operating Unit 2	Yes

Name	Data Source Name	Group
<input type="checkbox"/> A	charlotte	Staff
<input type="checkbox"/> B	charlotte	Staff
<input type="checkbox"/> Biling_Global	buly_airlines	Staff
<input type="checkbox"/> BilingGoldChatGlobal	buly_airlines	Staff

2. Select a contact group from the Available Contact Groups pane.
3. To associate the contact group for rollup, click Assign. The Assign Rollups pane displays.



The image shows a dialog box titled "Assign Rollups" with a close button (X) in the top right corner. Inside the dialog, there is a text instruction: "To complete the assignment process you must select from the following objects." Below this instruction are four selection fields, each with a "Select" button and a dropdown arrow. The first field is labeled "Contact Center", the second is "Application Group", the third is "Operating Unit", and the fourth is "Reporting Region". The "Operating Unit" and "Reporting Region" fields are separated by the text "and/or". At the bottom of the dialog are two buttons: "Assign" and "Cancel".

Assign Rollups page

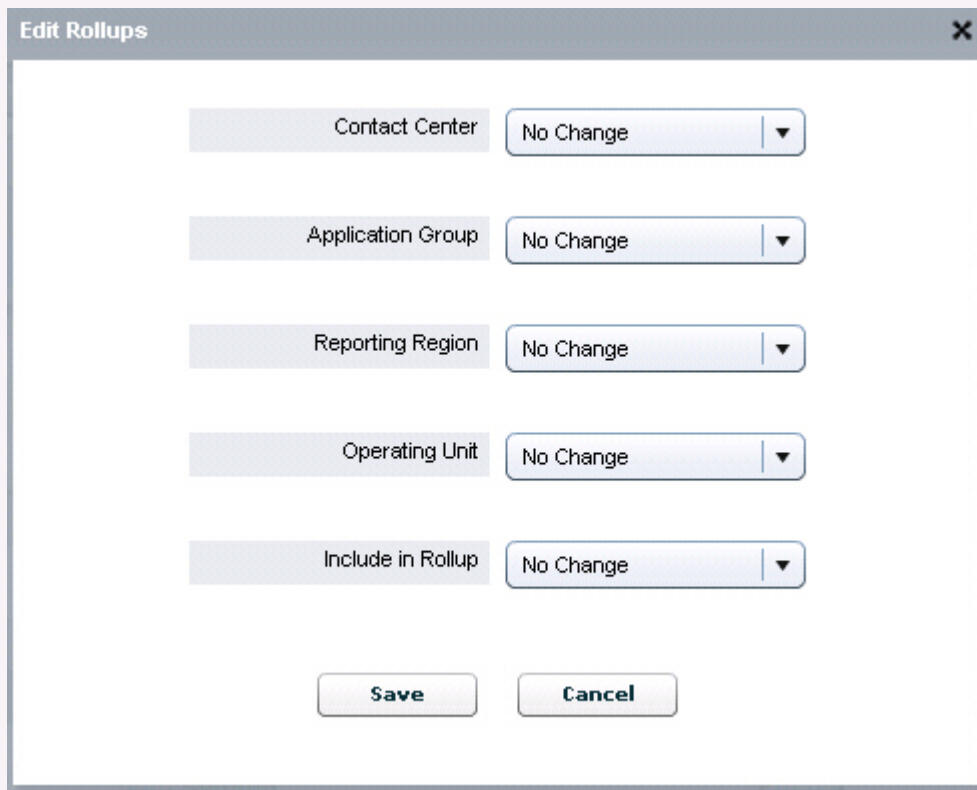
4. Define the rollup by selecting a contact center, application group, reporting region, and/or operating unit for the contract group.
Assigning an application group and contact center is required for the contact group to be used in rollups and to display on the dashboard. Assigning a reporting region or operating unit is required for the contact group to be used in the rollup for that grouping, and to display on the dashboard when that grouping is selected.
5. Click Assign. The Assign Rollups dialog box closes.
6. In the main Rollups tab, click Save.
A confirmation message displays and the details display in the table.
7. 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.

Editing a contact group rollup

For each contact group in a contact center, you select the application group, reporting region, and/or operating unit in which you want the contact group to belong, then you assign agent groups.

Start Procedure

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



Field	Value
Contact Center	No Change
Application Group	No Change
Reporting Region	No Change
Operating Unit	No Change
Include in Rollup	No Change

Buttons: Save, Cancel

Contact Groups Edit page

4. Edit the rollup by selecting a contact center, application group, reporting region, and/or operating unit and whether to include it in rollups or not. Assigning a contact center and application group is required for the contact group to be used in rollups and to display on the dashboard. Assigning a reporting region or operating unit is required for the contact group to be used in the rollup for that grouping, and to display on the dashboard when

that grouping is selected.

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. Starting in 8.1.5, the content of this page depends on the selected CCAdv/WA configuration mode:

- If integrated configuration mode is enabled, the list of available applications represents a set of configured applications not mapped to this, or any other, contact group in the system and is mapped to the same aggregated objects to which the selected contact group is mapped for use in CCAdv. If such an application is mapped to the contact group, and then later removed from CCAdv configuration or modified in a such way that the aggregated objects no longer match, this application disappears from the list of assigned applications, the list of available applications, and from the dashboard views.
- 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 in the system.

Tip

In the independent configuration mode, contact group-to-application mappings are completely independent from CCAdv configurations. Applications inherit rollup properties of the contact groups mapped to them and contribute to the real-time metrics of the contact centers, application groups, and regions that are related to the contact group.

Tip

In any configuration mode, if there are no applications mapped to a configured contact group, the contact group displays on the dashboard showing only forecast metrics.

The following screenshot shows the Contact Groups – Applications tab.

Chat and e-mail are not available in WA. Consequently, you cannot assign an application that is an interaction queue.

Maintaining 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 or application from the left panel.
This displays the already assigned contact groups or applications, if any, in the Assigned panel on the right. Applications or contact groups that are available for assignment appear in the Available panel.
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 Groups - Agent Groups

In releases prior to 8.1.5, you use the Contact Groups - Agent Groups page to assign agent groups to contact groups that are assigned to agent group contact centers (AGCC). Only AGCC are available for selection in the Contact Group drop-down list and only contact groups mapped to AGCC are shown on the Contact Groups pane.

In release 8.1.5, all types of contact centers are available for selection in the Contact Group drop-down. The contact groups mapped to any type of contact center display on the Contact Groups pane. The content of other panes on this page depends on the selected CCAdv/WA Configuration mode.

In integrated 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
 - mapped to an application that is mapped to the parent network contact center of the AGCC and the same application group and regions to which the selected contact group is mapped
- 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 list is derived from the applications mapped to the contact group and to the same aggregated 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.

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 agent group. Any such contact group can be mapped directly to any agent group present in the available agent group list.

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

The screenshot displays the 'Contact Group Configuration' interface. At the top, there are four filter dropdowns: 'Contact Center' (All), 'Application Group' (All), 'Reporting Region' (All), and 'Operating Unit' (All). Below these are four tabs: 'Rollups', 'Contact Groups - Applications', 'Contact Groups - Agent Groups' (which is selected and highlighted in blue), and 'Contact Group De...'. Under the selected tab, there are two links: 'Display Descriptive Names' and 'Display Technical Names'. The main area is divided into two panels. The left panel, titled 'Contact Groups', has a search bar and a table with 10 empty rows. Below the table is a pagination control showing 'Display 25 records per page.' and 'Page 1 of 1'. The right panel contains two sections: 'Assigned Agent Groups' and 'Available Agent Groups', each with a search bar and a table. The 'Assigned Agent Groups' section also includes a pagination control showing 'Display 5 records per page.' and up/down arrow buttons. At the bottom right of the interface are 'Save' and 'Reset' buttons.

Agent Groups Assignments tab

In Release 8.1.5, 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

Maintaining 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. You can opt to display the descriptive or technical names by clicking on the Display Descriptive/Technical Names link. You can reverse the order of display by selecting the relevant radio button.
3. Select a contact group or agent group from the left panel. This displays the already assigned contact group or agent group, if any, in the Assigned panel on the right. Agent groups or contact groups that are available for assignment appear in the Available panel. Note that though agent groups associated only with interaction queues will appear here, you should not assign these agent groups to a contact group. This is because you cannot assign the interaction queue 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.

Updating 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. Click Save.
A confirmation message displays and the details display in the table.

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.
- **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.

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. Starting in Release 8.1.5, two new options are added to the Agent Group Configuration page:

- Include in CCAAdv
- Include in WA

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

For more information about the CCAAdv/WA configuration modes, see *Performance Management Advisors 8.1 Deployment Guide*.

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:

- Maintain agent group details
- Assign agent groups to agent-group contact centers, and review the agent groups assigned to a contact center, application group, reporting region, or operating unit

For agent-group contact centers, you assign the agent groups that are already assigned 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.

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 Configuration

Contact Center All ▼

Application Group All ▼

Reporting Region All ▼

Operating Unit All ▼

Zero Suppress All ▼

Display on Dashboard All ▼

Include in CCAdv All ▼

Include in WA All ▼

Agent Group - Agent Group Contact Center

Agent Group Details

Search

Assigned Agent Groups

Name ▲	Descriptive Name	Zero Suppress	Display on Dashboard
[defaultTenant] AG-700 051	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
[defaultTenant] AG-700 Gold	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
[defaultTenant] AG_305 01	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
[defaultTenant] AG_4300_LT	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
[defaultTenant] AG2test	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Display 5 ▼ records per page. Page 1 of 1

Save

Reset

Search

Available Agent Groups

Name ▲	Tenant Name	Data Source Name
[defaultTenant] AGtest	defaultTenant	Genesys
[defaultTenant] team1	defaultTenant	Genesys

Display 5 ▼ records per page. Page 1 of 11

Agent Group Details tab

Maintaining 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.
6. To make the agent group display on the dashboard, select Display on Dashboard.
7. Click Save.
A confirmation message displays.

Assigning Agent Groups to Agent Group Contact Centers

In Advisors releases prior to release 8.1.5, if no contact centers are selected in the contact center drop-down list, the Assigned Agent Group pane shows all agent groups that are associated with an agent group contact center (AGCC). If a contact center is selected in the contact center drop-down list, the Assigned Agent Group pane shows all agent groups that are associated with this particular contact center.

Starting in release 8.1.5, an agent group can be assigned to more than one AGCC. In release 8.1.5 and later, 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.

The following screenshot shows the Agent Group Contact Center tab.

Agent Group Configuration

Agent Group Contact Center All ▼
 Zero Suppress All ▼

Application Group All ▼
 Display on Dashboard All ▼

Reporting Region All ▼
 Include in CCAdv All ▼

Operating Unit All ▼
 Include in WA All ▼

Agent Group - Agent Group Contact Center

Agent Group Details

☐	Name ▲	Agent Group Contact Center	Include in CCAdv	Include in WA
<input type="checkbox"/>	MANITOBA C_A580	AGCC_1 _Atwater	Yes	Yes
<input type="checkbox"/>	MANITOBA	AGCC_1	Yes	Yes
<input type="checkbox"/>	WINNIPEG MS	AGCC_1 _Atwater	Yes	Yes
<input type="checkbox"/>	WINNIPEG	AGCC_1	Yes	Yes
<input type="checkbox"/>	WINNIPEG	AGCC_1	Yes	Yes

Display 5 ▼ records per page.
⏪ ⏩ ⏴ ⏵

Assign Unassign

☐	Name ▲	Tenant Name	Data Source Name
<input type="checkbox"/>	[defaultTenant] AG-700 051_3100	defaultTenant	Genesys
<input type="checkbox"/>	[defaultTenant] AG-700 Gold	defaultTenant	Genesys
<input type="checkbox"/>	[defaultTenant] AG_305 3100	defaultTenant	Genesys

Display 5 ▼ records per page.
⏪ ⏩ ⏴ ⏵ Pa

Agent Group Contact Center tab

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.

Maintaining 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.

Editing 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 CCAAdv and Include in WA options are grayed out if you use integrated configuration mode.

5. Click Save.

Metric Manager

Use the Metric Manager link on the Administration module navigation pane to access the metrics management and configuration page. 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.

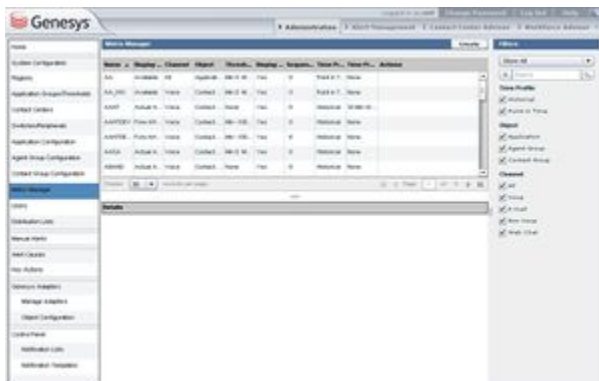
Metric Manager Overview

You can view and edit all Contact Center Advisor and Workforce Advisor metrics in the Metric Manager. You can customize the set of standard metrics that ship with Performance Management Advisors to address your specific Contact Center performance and service quality measurements. You can also use the Metric Manager to create custom metrics for the dashboard.

Important

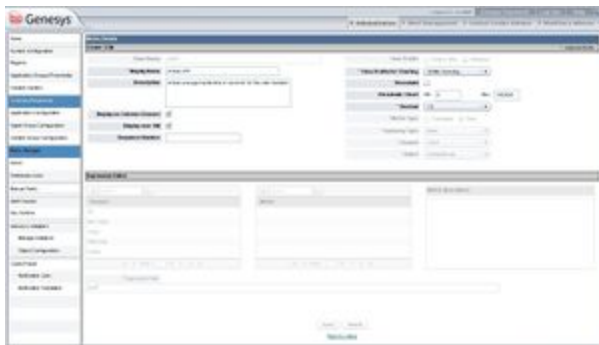
You can create only custom application metrics. You cannot create agent group or contact group metrics.

The elements of formulas for custom application metrics are limited to existing standard or custom source metrics provided by the Genesys Adapter, source metrics imported from the CISCO environment, and existing CCA application dashboard metrics. The Metric Manager page displays only the metrics to which you have Read permission in the Configuration Server. The following screenshot shows the Metric Manager page in the Administration module.



Metric Manager page

The following screenshot shows the Metric Details page. Use the Metric Details page to edit or customize a selected metric.



Metric Details page

The display attributes of all metrics, including standard metrics (metrics that ship with Advisors), can be edited in the Metric Manager. There are limitations on what you can edit for a standard metric. For more information, see [Descriptions of Metric Properties on the Metric Details Page](#). Any changes that you make using the Metric Manager are logged in the audit log file, similar to all other logged administrative actions.

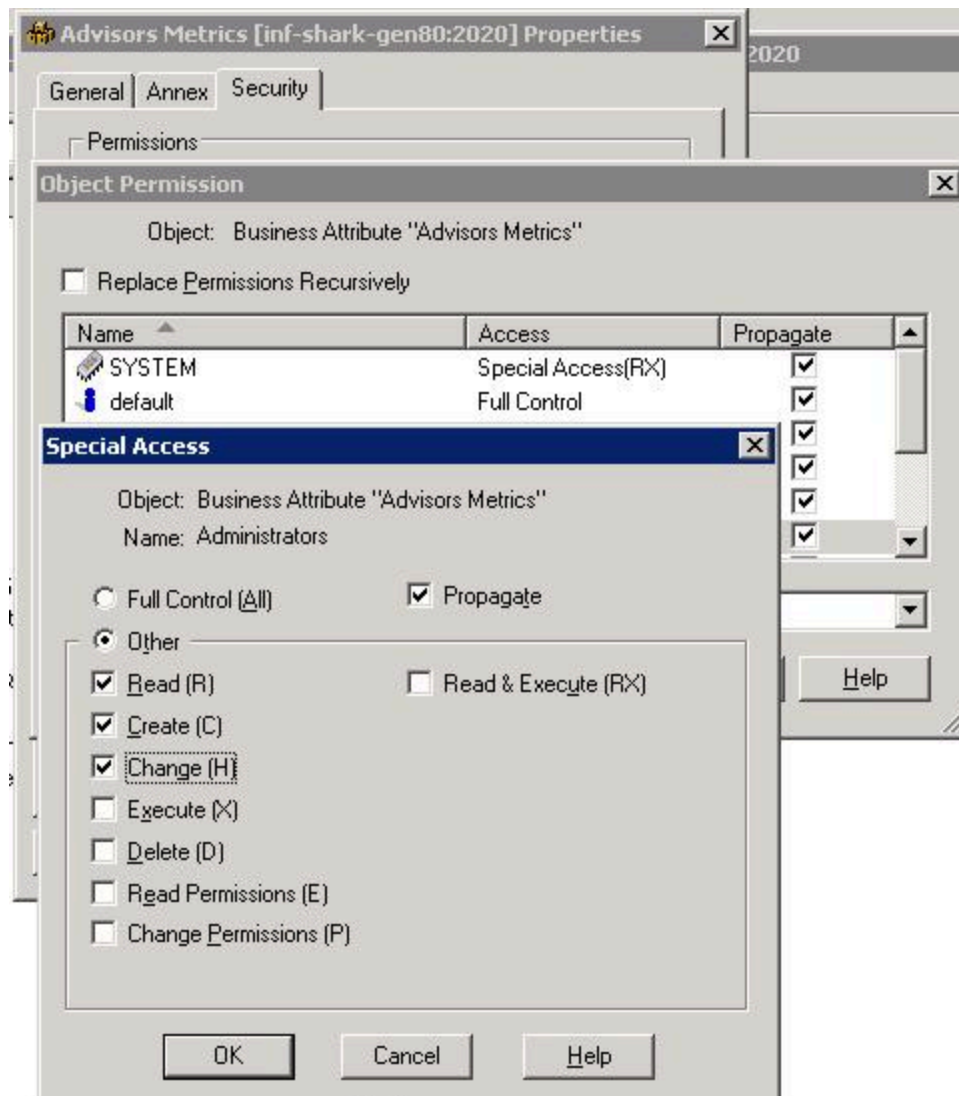
Important

Frontline Advisor metrics do not display in the Metric Manager.

Role Based Access Control and the Metric Manager

The Metric 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 Metric Manager, the view, create, copy, edit, and delete actions are individually controlled by privileges. For information about the Metric Manager-specific privileges, see [Advisors 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 following screenshot..



Security Settings in Configuration Manager for Metric Manager Users

Using Metric Manager

You can create custom application metrics using the Metric Manager. To create a custom metric, 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.

Metric Type	Acceptable Operands
Raw custom point-in-time and calculated dashboard custom metrics	Arithmetic operators: <ul style="list-style-type: none"> + (addition)

Metric Type	Acceptable Operands
	<ul style="list-style-type: none">• - (subtraction)• * (multiplication)• / (division) Brackets (to ensure the required operation sequence)
Calculated dashboard custom metrics	In addition to the above, the >, <, and = operators can be used.

Viewing 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 Metric Manager page displays only the metrics to which you have Read permission in the Configuration Server.

Start Procedure

1. From the Administration Module, navigate to the Metric Manager.
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 the metric on the Metric Manager page to select the metric.
Details about the metric display at the bottom of the Metric Manager page.

Creating 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 (see [Role Based Access Control and the Metric Manager](#)) 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. From the Administration Module, navigate to the Metric Manager.
2. Click Create.
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 [Descriptions of Metric Properties on the Metric Details 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 Metric Manager page. The new metric displays in the list of metrics.

Copying 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 (see [Role Based Access Control and the Metric Manager](#)) 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. From the Administration Module, navigate to the Metric Manager.
2. Select the custom or standard metric that you want to use as a template for a new custom metric.
You can use only application metrics as templates for new custom metrics. If you select a standard dashboard metric as a template for a new custom metric, the expression of the original standard metric may 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 [Descriptions of Metric Properties on the Metric Details Page](#).
5. Click Save to save the metric.
If you entered all information correctly, the page returns to the Metric Manager page. The new metric displays in the list of metrics.

Editing 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. From the Administration Module, navigate to the Metric Manager.
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 Metric Manager page. The metric displays in the list of metrics.

Deleting 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 the metric that you want to delete.

- You require a Change permission in the Configuration Server (see [Role Based Access Control and the Metric Manager](#)) 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. From the Administration Module, navigate to the Metric Manager.
2. Select a metric to delete.
3. Click Delete.
If a raw dashboard metric is used in a calculation for a calculated dashboard metric, you cannot delete that raw dashboard metric. If you attempt to delete a metric that is used in another metric calculation, Advisors displays a message that indicates which dashboard metric or metrics use that metric.

Descriptions of Metric Properties on the Metric Details Page

The following Table provides descriptions of the metric properties you define on the Metric Details page.

Property	Description
Short Name	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.
Display Name	The name used for display in the column chooser and dashboard. The name must be unique for a given channel.
Description	The metric description.
Display on Column Chooser	Enable/disable option. Determines if the metric displays in the Column Chooser.

Property	Description
Display over 100%	A format option. Yes indicates that values over 100 display actual values. No indicates that values over 100 display as 100+.
Sequence Number	The default order of the metrics in the Column Chooser. Clicking Reset in the Column Chooser (accessed from the dashboard) displays the metrics with a sequence number.
Time Profile	<p>Determines if the time profile is Point in Time or Historical (5 Min, 30 Min, or Today).</p> <p>You cannot edit this property for a standard metric.</p> <p>The following rule applies to the time profile of the metric itself and time profiles of the operands participating in its calculation:</p> <ul style="list-style-type: none"> If the metric belongs to the historical time profile, the operands can be either historical or point-in-time. If the metric belongs to the point-in-time time profile, only point-in-time operands are allowed. <p>This rule governs the operand selection list in the custom metric expression editor. Only compatible operands are available for selection. If an incompatible operand is entered using the keyboard, the calculation is rejected with a corresponding error message.</p>
Time Profile for Charting	Determines if the metric is available for graphing (charting). To enable a metric for graphing, you must select a specific graphing period for the time profile. If None is selected, the metric is not displayed in the Metric Graphing window.
Threshold	Determines if a threshold rule can be created.
Threshold/Chart	The threshold range (minimum and maximum) values for the threshold, as well as y-axis values in the chart.
Decimal	A format option. Determines the number of decimal places to display for values.
Metric Type	<p>Custom metrics are either raw metrics or calculated metrics.</p> <p>You cannot edit this property for a standard metric.</p>
Summary Type	<p>Determines how aggregation is performed on rolling up the metric to the various aggregating levels:</p> <ul style="list-style-type: none"> When the metric type is Raw, the options are: <ul style="list-style-type: none"> SUM MIN MAX

Property	Description
	<ul style="list-style-type: none"> When the metric type is Calculated, Summary Type is not defined (None). <p>A raw metric is a metric associated with an aggregation function and its single operand in the form of a source metric pulled directly from the source.</p> <p>A calculated metric is defined as a calculation expression involving one or more existing raw or other calculated metrics as operands and arithmetical operations applied to the set of these operands. Aggregation functions cannot be applied to the operands of a calculated metric expression.</p> <p>You cannot edit this property for a standard metric.</p>
Channel	<p>Determines the media channel type under which the custom metric is shown in the Column Chooser and on the dashboard.</p> <p>You cannot edit this property for a standard metric.</p>
Object	<p>Type of the target object. For example, Application.</p> <p>You can create custom application metrics only (you cannot create agent group or contact group metrics) You cannot edit this property for a standard metric.</p>
Expression Editor	<p>Use the Expression Editor to build the formula that produces a metric value.</p> <p>Use the Channel and Metric boxes to find existing metric expressions that you can use in the calculation of your new custom metric. In the Metric box, the Expression Editor lists only the metrics you can use in the calculation of the custom metric. The list of metrics that displays is based on the custom metric type (Raw or Calculated) and the base time profile (Historical or Point in Time). When you select a metric in the Metric box, a description of that metric displays in the Metric Description box. You cannot edit this property for a standard metric.</p>

Using Metric Manager to Enable Metrics for Graphing

The Metric Graphing window is accessible from both Contact Center Advisor and Workforce Advisor. You specify which metrics users can graph using the Metric Manager. Use the Edit option associated with each metric on the Metric Manager page, or the Create button, to open the Metric Details page. On the Metric Details page, you can specify a time profile. That is, you specify whether the selected metric displays point-in-time (Now) or historical (5 Min, 30 Min, or Today) values. To enable a metric for graphing, you must select a time profile. Each metric 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.

Enabling Metrics for Graphing

Start Procedure

1. Open the Administration module.
2. Click Metric Manager in the navigation pane.
3. Use the filters on the Metric Manager page (on the right) to show as many or as few metrics as required.
4. Do one of the following:
 - Select a 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 custom metric.
5. On the Metric Details page, select the Time Profile checkbox, if applicable. The Time Profile radio buttons are grayed out (that is, you cannot change the Time Profile) for Standard metrics.
6. To enable the metric for graphing, select time profiles from the Time Profile for Charting list. If you select None, the metric is not displayed in the list of metrics in the Metric Graphing window (that is, it cannot be graphed). The Time Profile for Charting list is applicable only for Application and Contact Group metric types; it is disabled for Agent Group metric types (users cannot graph Agent Group metrics).

Users

The functionality of the Users page has moved to Genesys Configuration Manager starting in release 8.1.2. A message displays if you select the Users option in the Administration module, and indicates that user profiles are maintained in the Configuration Server.

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. Please refer to:

- [Advisors Business Objects](#)
- [Role Based Access Control](#)

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

Access to contact centers and application groups must be configured by an administrator in Genesys Configuration Manager. Data relating to or depending on objects to which users have no permissions will not be displayed. CCAdv and WA have the ability to generate and distribute e-mail notifications to specified distribution lists. The following screenshot shows the Distribution Lists page.

Distribution Lists

<input type="checkbox"/>	Name ▲	Effective Date	Active
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

Display records per page.

Create / Edit

* Name

* Effective Date

* Distribution Alert

☐ Technical - 1
☐ Technical - 2
☐ Business - 1
☐ Business - 2

* Contact Centers

Members

Distribution Lists Page

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

- B1 and B2 for business alerts
- T1 and T2 for technical alerts

The message notification is delivered to all users contained in the list who have permission to see the business objects associated with the alert.

Working with Distribution Lists

Contact centers and application groups must be assigned to distribution lists in order for contacts to receive e-mail notifications about threshold violation alerts or peripheral offline alerts that are created for applications or contact groups related to the application groups or contact centers.

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.

E-mail alerts are not sent to users who have no object permissions configured in Genesys Configuration Manager to the contact centers, application groups, and geographic regions related to the alert. See [Role Based Access Control](#). Each distribution list must always have at least one contact center and one application group associated with it. If you select individual distribution list members, you must assign any members added in the future manually. When assigning a network contact center, you may also add its related agent group contact centers.

Maintaining distribution lists

If you select individual distribution list members, you must assign any members added in the future manually. When assigning a network contact center, you may also add its related agent group contact centers.

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.

Deleting 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

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. 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 carousel and the Alerts pane in the Map pane of CCAdv and WA. The following screenshot shows the Alerts page.

Manual Alerts

<input type="checkbox"/>	Alert Time ▲	Expiration Date	Alert Type	Alert Priority	Alert Message

Display **5** records per page.

Create / Edit

* Alert Message

* Alert Type

☒ Business ☐ Technical

Effective Date

* Expiration Date

* Expiration Time

* Alert Priority

☐ 1-Re

* Contact Centers

Save

Reset

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.

Adding 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.

Updating 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.

Deleting 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			
Name	Author	Approved	Display Order

Row 1 to 0 of 0

Create / Edit

* Alert Cause

Display Order

Approved ☒

Save Reset

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.

Approving or Rejecting 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					
Search					New
Name	Author	Metric	Metric Type	Approved	Display Order

Row 1 to 0 of 0

Page 1

Create / Edit

* Key Action

Metric

Display Order

Approved ☒

Save Reset

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.

Approving or Rejecting 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.

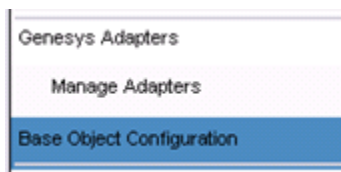
- c. Click Save.
The approved key action displays in the table with a check mark.
- 2. To leave a key action off the list on the Action Management page:
 - a. Highlight a row for an approved key action in the Key Actions table.
The details display in the details section.
 - b. Clear the Approved check box.
 - c. Click Save.
The unapproved key action displays in the table with the symbol.

Base Object Configuration

In earlier releases, you managed Advisors Genesys Adapters and configured object on pages in a Genesys Adapters section of the Administration module. In Release 8.1.5, the Manage Adapters page in the Administration module is read-only. You no longer manage adapters from this page, although you can view information about the adapters. Because CCAdv interacts with Data Manager starting in Release 8.1.5, component roles have changed. Information that was previously stored in Advisors Genesys Adapters has moved to the Platform database or to Genesys Configuration Server. In Release 8.1.5, you manage the adapters from the Platform database. For more information, see Performance Management Advisors 8.1 Deployment Guide. You configure objects on the Base Object Configuration page in the Administration module.

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

In earlier releases, you selected an adapter instance before you edited any object details. In Release 8.1.5, this is unnecessary. 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 8.1 Deployment Guide*.

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 8.1 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.

Mapping 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.

Mapping 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.

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.

Adding 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.

Editing 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.

Deleting 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
			<p>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></p>
Skill Change	Users on Notification List	Notification of Skill Change	<p>The skills of the included agents have been changed. <Insert statement about how skills have been changed—see description after table>.</p> <p>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></p>
General Notification	Agent	<title of template that is used>	<p>Message From the Operator:</p> <p><Insert any comments entered by the user—this is what is displayed in the message text box></p>