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.

Workforce Management Administrator's Guide

About WFM Configuration Objects

4/25/2025

About WFM Configuration Objects

The `Configuration` modules of the WFM Configuration Utility and WFM Web enable you to configure a number of object types. The following sections briefly describe each object type and offer some considerations to assist you in planning your configuration.

Topics on this page include:

> **Important**
>
> The following sections provide only brief introductions to these objects and focus on aspects relevant to deployment planning. For a full description, refer to Workforce Management Configuration Utility Help and Workforce Management Web for Supervisors Help.

User Security

The `User Security` module enables you to configure security settings for all supervisors (that is, all non-agents who use WFM). It groups security settings into the following categories: `General`, `Configuration`, `Policies`, `Calendar`, `ForecastInsert text`, `Schedule`, `Trading`, `Performance`, `Adherence`, reports, and `Data Import/Export`. Under each category are various options.

For example, `Notifications` is an option under `Configuration`. If a user is assigned `Notifications` permission, that user can then access the `Notifications` module in WFM Web for Supervisors. Users without this permission cannot access and therefore cannot modify the configuration of email notifications.

The user security settings allow for a great deal of flexibility. You can specify which sites and business units, teams, and so on, the user can access. You can configure no calendar, forecast, and schedule access; read-only access; or full access.

In addition, you can enable users to make only pending schedule changes—that is, schedule changes that require approval from a qualified user before they are incorporated into the Master Schedule.

To configure user security settings efficiently, determine the access levels appropriate for all users. You can change settings at any time, as necessary. You can also use Security Roles to more easily configure security settings for users, by creating a Security Role, assigning permissions to it, and then assigning one or more WFM users to that Security Role.

An administrator can configure a security role as the default. All new users added to the WFM system will be assigned to this default security role—and will be limited to its access permissions. See Defining the Default Security Role

Back to Top

Organization

Use the `Organization` module to configure sites and business units (formerly called *virtual PABXs*), teams, and agents. To configure this module, determine the sites that belong to business units. Decide on the site properties, the maximum seats, the Data Aggregator and WFM Server the site uses, the switch you will use to collect statistics (if you want to use one different from the one automatically associated with the site during synchronization), and so on. Collect information about agent team and site associations, as well as agent settings, such as rotating pattern (if any), contracts, and rules for the accrual of accrued time off.

Keep in mind that there are many WFM configuration objects that are associated with a site, including Rotating Patterns, Contracts, Activities, Time Off Types, Time Off Rules, Exception Types, and more. When you move an agent from one site to another, you must reassign that agent to a new Contract, Time Off Rules, and new Rotating Patterns—if these were previously assigned. You must take this action to correctly schedule the moved agent under the new site.

Creating a New Business Unit

You might need to create a new business unit during database synchronization. To configure your new business unit, see the `Configuration` > `Organization` > `Business Units` > `Creating Business Units` topic in the Workforce Management Configuration Utility Help.

Back to Top

Activities

Activities are defined as different categories of work that comprise the total workload for a contact center. Workload and staffing forecasts are created for each activity. Each site configures its own activities, to take into account of local conditions. All agent work that is forecast and scheduled must be assigned to an activity.

Activities can take various forms. They might describe types of work, such as inbound calls or e-mail;

groups of customers served, such as preferred customer care; or work times, such as overnight. You can also use activities for non-CTI work. Each activity is then associated with one or more preconfigured skills. Because activities are a fundamental unit for forecasts and schedules, it is critical that you configure them accurately.

Maximum Simultaneous Users for Activities

The Maximum Simultaneous Users feature limits the number of agents that can be scheduled for an activity, even if the workload requires more. Maximum Simultaneous Users can be understood as a way to prevent excessive staffing for some activities so that the agents can be moved to more important activities, even if it leaves some less-important activities understaffed. This feature is best used when the contact center is understaffed as a whole. As the Maximum Simultaneous Users value is reached, agents are then assigned to other activities.

> **Important**
> Only use the Maximum Simultaneous Users feature in a multi-skilled environment.

Multi-site Activities

Multi-site activities, formerly called virtual activities, are performed at multiple physical sites. They enable you to view several local activities as a single WFM object. The performance information is split among the sites that perform the activity. You can build interaction volume forecasts, staffing forecasts, and view contact center performance for multi-site activities.

Configuring Statistics

WFM uses the WFM Data Aggregator to track four statistical categories: `Interaction Volume`, `Abandonment Percentage`, `Quality of Service`, and `Handle Time`. These statistics are written to the WFM database, providing the historical data necessary for WFM Forecasting, Scheduling, Performance monitoring, and Adherence monitoring.

Because WFM Data Aggregator receives its statistics from the Genesys Stat Server, it supports a very flexible configuration. In the WFM Configuration Utility you associate Stat Server statistics with activities. These Stat Server statistics may be ones that are provided out-of-the-box, or they can be customized statistics.

For example, you can sum up values from any set of statistics you want, such as `totalTalkTime` + `totalHoldTime` + `totalAfterCallWorkTime`. This type of flexible configuration overcomes the limitations of ACD switch reports and integration, allowing you to choose the statistics that best represent the work associated with servicing each customer interaction.

Back to Top

Adding Reason Codes

When associating agent schedule states provided by WFM with Genesys events, you can configure reason codes with Genesys events. This allows you to refine the Genesys agent-state information that WFM uses to track agent compliance with their scheduled states.

WFM Data Aggregator can process reason codes that come from hard and/or soft phones. To receive reason codes from hard phones, or in a mixed hard/soft phone environment, set the `ReasonCodeKeyName` option in the `WFM Data Aggregator Application` object to `ReasonCode`. See Configuring Data Aggregator to process Reason Codes.

Using Hot-Standby Backup for WFM Data Aggregator

You can configure a hot-standby backup WFM Data Aggregator for each primary WFM Data Aggregator server: see Step 5 in the procedure Creating a Data Aggregator Application Object. The backup reads the same information as the primary WFM Data Aggregator, so if it is necessary to switch to the backup, there is no delay or loss of data. At the transition, the backup WFM Data Aggregator simply starts writing to the database starting from where the primary WFM Data Aggregator left off.

If configured properly, WFM Data Aggregator also backs up data in the event of a disconnect from the database and the subsequent WFM Data Aggregator shutdown. It first writes all current data to a local *dump file*. You must specify a path and file name for the `DBDumpFile` option on the `Options` tab of the `WFM Data Aggregator Application` object. See Configuring Data Aggregator to Backup Data on Disconnect

Back to Top

Skills

You can configure interactions to be routed to specific agents within a contact center, based on skill definitions.

For example, you may want to have incoming interactions go first to an agent at the highest level of a certain skill. If no agent with that skill level for that activity is available, then the interaction can be routed to an agent with the next highest level of that skill. If no agent is available at that level, then the interaction can be routed to the next available agent, regardless of the agent's skill level for the activity.

The contact center manager can decide whether to staff for the higher skill levels, or whether to staff so that any agent can handle the interaction.

Skills are defined and assigned to agents in Configuration Manager. To learn how to import Configuration Manager skills into the `WFM Utility Skills` list, see the `Configuration` > `Skills` topic in the Workforce Management Configuration Utility Help.

Matching Skills and Activities

Activities often correspond to skills but may also correspond to agent skill levels. Choosing an appropriate strategy for a contact center's activities allows for improved staffing decisions.

For example, in a simple scenario, the relationship among the queue, skills, and activities is a 1-1-1 correspondence. As things get more complex, the relationships get more complex. Activities consist of multiple skills, and each site has many activities associated with it. The goal is to find the best combination of relationships to meet staffing requirements.

Back to Top

Schedule-State Groups

A *schedule-state group* is a collection of schedule states that is linked to a site. These include breaks, meals, exceptions, activities, time off, and so on. You can group these, and then associate the group with one or more Genesys states.

Additionally, you can configure adherence thresholds for this schedule state group, which define when an agent should be considered to be non-adherent to the schedule states contained in the group.

To configure schedule-state groups, determine what schedule states you are using, what are the most logical groupings, and which Genesys state(s) best corresponds to each group.

To learn how to configure Schedule State Groups and Adherence Rules for them, see the `Configuration` > `Schedule State Groups` topic in the Workforce Management Web for Supervisors Help.

Events

Events are specific instances of occurrences that affect scheduling requirements. For example, a catalog drop might increase demand for agents handling inbound interactions. By configuring an event, you can forecast and schedule to incorporate its effects, ensuring appropriate staffing levels throughout the period that the event affects.

To learn how to create and configure Events and Factors (Events are instances of Factors), see the `Forecast` > `Historical Data Views` > `New Event Page` topic in the Workforce Management Web for Supervisors Help.

Back to Top

Time Zones

Time zones are set up in Configuration Manager and imported into WFM during synchronization. You can assign time zones to sites and business units. You can also configure a default time zone, for efficiency in configuring new objects, and a user time zone, which is used as the alternative time zone in WFM Web Performance views. All newly created sites and business units use the default time zone, unless specified otherwise.

To learn how to configure and work with Time Zones, see the `Configuration` > `Time Zones` topic in the Workforce Management Configuration Utility Help.

Synchronization

Synchronization brings Configuration Database objects, such as agents, agent skills, time zones, and users into WFM. You can configure security settings to determine the users who are able to perform synchronizations.

To learn about synchronization, see the `Configuration Utility Interface` > `Synchronization` topic in the Workforce Management Configuration Utility Help.

> **Important**
> To avoid errors during synchronization and further work, your configuration must not contain duplicate names for switches, time zones, or skills—not under different tenants, and not in different Configuration Manager instances that access the same WFM database.

Back to Top

Procedures

Click the red arrow below to see a list of procedures related to the topics on this page.

<multistep>

|-| Defining the Default Security Role=

Purpose: To specify the access permissions that is assigned to all new users who are added to the WFM system.

Prerequisite: You installed WFM Configuration Utility. See the Procedure: Installing WFM Configuration Utility.

Start of Procedure

1. Open WFM Configuration Utility.
2. In the `Modules` pane, select `User Security`.
3. In the `Objects` pane, select `Security Roles/Users`.
4. (Optional): In the `Objects` pane, create a new security role.
5. In the `Data` pane, select a security role from the `Default Security Role` drop-down list.
6. Click `Apply`
   The selected role becomes the default security role.

Tip

The default security role has a special icon; its upper left corner is red.

End of Procedure

|-| Configuring Data Aggregator to Process Reason Codes=

Purpose: To enable Data Aggregator to process Reason Codes.

Prerequisite: You created a WFM Data Aggregator application object for the current installation in Configuration Manager.

Important

You can use reason codes only if your CTI environment supports them.

Start of Procedure

1. Open Configuration Manager (a Management Framework component).
2. Open the `WFM Data Aggregator Application` object.
3. On the `Options` tab, create an option named `ReasonCodeKeyName`, if it does not already exist.
4. Set the value of `ReasonCodeKeyName` to `ReasonCode`.
5. Save the changes.

End of Procedure

|-| Configuring Data Aggregator to Backup Data on Disconnect=

Purpose: To enable an emergency Data Aggregator info dump.

Prerequisite: You created a WFM Data Aggregator application object for the current installation in Configuration Manager.

Important

You can use reason codes only if your CTI environment supports them.

Start of Procedure

1. Open Configuration Manager (a Management Framework component).
2. Open the `WFM Data Aggregator Application` object.
3. On the `Options` tab, create an option named `DBDumpFile`, if it does not already exist.
4. Set the value of the `DBDumpFile` option to a path and file name—for example: `C:\DAEmergency\DBDumpFile.txt`.
5. Save the changes.
   If WFM Data Aggregator loses its connection to the database, before closing down it writes all current data to the local file (the so-called *dump file*). After restart and reconnection to the database, WFM Data Aggregator reads the dump file, writes the data to the database, and deletes the dump file.

> **Important**
> The dump file does not prevent data loss during the period that WFM Data Aggregator is shut down.

End of Procedure

</multistep>

Back to Topic