Genesys Administrator Extension Help

Genesys Administrator 8.5.2

12/29/2021

Table of Contents

Genesys Administrator Extension Help

Welcome to the Genesys Administrator Extension Help. This document introduces you to the GUI of Genesys Administrator Extension and describes concepts and procedures relevant to using this software in your contact center.

About Genesys Administrator Extension

Genesys Administrator Extension (GAX) introduces the next-generation user interface for Genesys that reduces both the overall operating costs and the time to deployment, by providing user-friendly interfaces that perform complex operations while at the same time preventing user error. This product is focused on the user experience for both Enterprise and Hosted customers, as well as by system administrators and line-of-business users.

The following are quick links to popular chapters and topics:

The GAX Interface

- Login and Password
- Navigating the User Interface
- Setting Preferences

Configuration and Monitoring

- System Dashboard
- Using the Agents Window
- Using Configuration Manager
- Viewing Centralized Logs

Solution Deployment

- Installation Packages
- Solution Definitions
- Privileges

Operational Parameter Management

- Parameters
- Parameter Groups
- Parameter Group Templates

Audio Resource Management

Audio Resource Management

Helpful Information

Troubleshooting GAX

Interface Overview

The topics in this section describe the Genesys Administration Extension (GAX) user interface, as follows:

- Logging in to GAX
- Setting user- and system-level Preferences
- A general description of the Interface
- Adding Custom links to the main navigation bar
- Administration and other tasks, such as:
  - Managing Plug-ins
  - Using the Command Line Console
  - Using Bulk Change Sets to make changes to multiple objects at once.

Login and Password

Your user's first name is displayed in the top Header Bar of the Genesys Administrator Extension window.

You might be configured to set a new password the first time that you log in, or after a system administrator has reset your password.

Procedure: Setting a New Password

Steps

1. If you are configured to change your password the first time that you log in, or after your system administrator has reset your password, the **Change Password** dialog box is displayed.
2. Enter a new password in the **New Password** field.
3. Enter the same password in the **Confirm Password** field.
4. Click **OK**.

Inactivity Timeout

For security purposes, GAX might be configured to lock the application if you have not used the keyboard or mouse for a specified period of time. If inactivity-timeout occurs, all user input is blocked until you provide your login information to unlock the application. This feature ensures that no unauthorized user can access an unattended terminal that is running GAX.

> **Important**
> GAX employs a keep-alive strategy to prevent your session from timing out; this feature ensures that GAX maintains your session even if the inactivity-timeout feature locks the application and requires you to log in.

User Interface

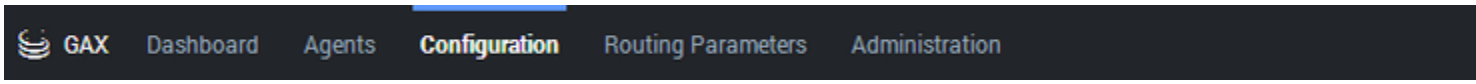
The main screen of Genesys Administrator Extension consists of two parts, as follows:

- The header, at the top of the screen, contains the main controls for the user interface.
- The workspace, under the header, is where you perform all the tasks in Genesys Administrator Extension.

> **Important**
> The workspace displays only those objects and options for which the logged-in user has role privileges and object permissions to access.

Header

The Header area is located at the top of the main screen of the interface and contains the main controls for the Genesys Administrator Extension (GAX) interface.



The Header Bar in Genesys Administrator Extension.

To the right, the Header Bar displays the name of the logged-in user and a link to this Help document. Click the user name to access the Profile menu. To the left, the Header Bar contains the menu options for navigating GAX.

When the server is in Read Only Mode or Emergency Mode, a lock icon appears on the header for the following:

- All currently logged in users
- All users logging in during Read Only Mode or Emergency Mode

For more information on the Read Only Mode and Emergency Mode, see Read Only Mode and Emergency Mode.

The following fixed headings are always displayed:

- **System Dashboard**
- **Configuration**
- **Routing Parameters**
- **Administration**

- **Centralized Logs**

Click the **Home** button from any page in GAX to return to the home page.

> **Important**
>
> The available options in the header are determined by the following:
>
> - Your access permissions.
> - The plug-ins that are installed on your system; for example, the **Routing Parameters** option does not appear if the **OPM** plug-in is not installed.
> - The options you selected in your System Preferences; for example, the **Agents** option does not appear if you have selected **Hidden** in the system preferences.

Installing plug-ins will add submenu headings to the fixed headings. For example, installing the **ASD** plug-in adds **Solution Deployment** to the **Configuration** fixed heading.

You can also add custom links to external websites. For more information, see Adding Links to the Navigation Bar.

Workspace

The workspace, located below the header, is where you perform all tasks in Genesys Administrator Extension. It displays only those objects and options for which the logged-in user has role privileges and object permissions to access.

Lists of items in the workspace are organized by Tenant in multi-tenant environments. You can choose to view all Tenants, your default Tenant, or selected multiple Tenants by clicking **Tenant Directory**  .

You can sort lists by various criteria by clicking on column heads. You can also quickly find information by using the **Quick Filter** field.

List Metrics

When working with lists of configuration objects in the Agent Management module or in Configuration Manager, metrics about the contents of the currently viewed list are displayed immediately following the breadcrumbs in the top-left corner of the view window in the following format:

```
type([x/]y)[, Selected (z)]
```

where:

- `type` is the type of objects in the list, such as Agent, Host, Application, DN, and so on.
- `x` is the total number of agents displayed after applying a filter. If no filter is applied, `x` equals `y`, and `x` is

not shown. If a series of filters are applied, x represents the number of users displayed by the most recent filter acting on the results of the previous filter.

- y is the total number of users in the current Folder.
- z is the number of agents in x selected by the user. If no users are selected, `Selected (z)` does not appear.

[+] Show examples

For these examples, assume that that are 12 Applications in the environment.

Number of Users Selected by Each Filter	Number of Users Selected Manually	Display
No filter used	0	Applications(12)
No filter used	2	Applications(12), Selected (2)
5	0	Applications(5/12)
5	2	Applications(5/12), Selected (2)
5, 3	2	Applications(3/12), Selected (2)

Auditing History

For some objects, you can view an auditing history. Select the object, such as a solution definition, to view information about the object in a new panel. In the object information panel, click the **Related** button and select **History**. The **History** panel is displayed to the right. It contains information about the change history of the object.

Availability of Menu Items

Multiple instances of Genesys Administrator Extension might be connected to the same configuration environment, to support load balancing and high availability. Each instance of Genesys Administrator Extension might be configured to use different sets of functional modules. Not all modules might be available for every instance of Genesys Administrator Extension that is installed in your Genesys environment.

Confirmation of Changes

Before saving changes, or when navigating away from a particular section in which changes were made and not saved, Genesys Administrator Extension will display a dialog box in which you indicate whether you want to save the changes. For configuration changes in more critical situations, particularly when you have deleted data or disabled objects and/or functionality, an enhanced dialog box in which the potential impact of the changes is provided, and you must first indicate that you understand the potential impact before you confirm that the changes can be saved.

Profile Menu

The Profile menu enables you to:

- View general information about GAX.
- Set or change your personal settings (preferences) when using GAX. These preferences take effect each time that you, or anyone using your login credentials, logs in to Genesys Administrator Extension from any browser.
- Launch Genesys Administrator.
- Log out of GAX.

To open the menu, click the username in the Header Bar. If configured, the menu also displays the last time that this user account was logged into Genesys Administrator Extension.

> **Important**
>
> To use the last login time feature, you must ensure:
>
> - The date and time of the local computer and the Management Framework computer are synchronized for the last login time to be accurate.
> - The following lines are included in the Configuration Server `confserv.cfg` file (located in the installation directory of the machine that hosts Configuration Server):
>   - `last-login = true`
>   - `last-login-synchronization = true`

The Profile menu contains the following options:

- **About**—Click this option to view information about your installation, including the version of GAX that you are using. If your user account has the **Read Deployable and Undeployable IPs and SPDs** privilege, you can also view information about the Configuration Server to which you are connected.

  > **Tip**
  >
  > To see the versions of plugins that are installed, see Viewing Installed Plug-ins.

- **Change Password**—Change your password. You must have the **Modify User Password** privilege to change your password.
- **User Preferences**
- **System Preferences**

- **Set Current Page As Home**—Set the currently displayed page as the home page for your User account. Once set, this page is displayed each time you log in.
- **Genesys Administrator**—Launch Genesys Administrator. This link is displayed if you are configured to log in to Genesys Administrator, when you log in to Genesys Administrator Extension.
- **Log Out**—Log out of Genesys Administrator Extension.

> ### Important
> Settings in the **User Preferences** section take precedence over settings in the **System Preferences** section. For example, if the **System Preferences** language setting is `English (US)` and the **User Preferences** language setting is different, Genesys Administrator Extension will use the **User Preferences** language setting.

User Preferences

Advanced

In the **Advanced** category, you can specify the logging level for Genesys Administrator Extension JavaScript logging. You need to set this only if instructed to do so by support personnel. Use the drop-down list to set the level to one of the following:

- **Debug**—All (error, warning, info, and debug) logs are generated.
- **Info**—Error, warning, and info logs are generated. This is the default level.
- **Warning**—Only error and warning logs are generated.
- **Error**—Only error logs are generated.
- **Off**—Logging is disabled.

These logs are viewed in the browser console.

> ### Important
> Do not confuse these logs with Tomcat logs or with logs that are generated by components and stored in the Centralized Log Database.

Configuration Manager

In the **Configuration Manager** category, you can set the following display preferences for Configuration Manager:

- **Show DBID**—Shows the database ID when viewing details about a configuration object.

- **Show Recent**—On the Configuration Manager homepage, shows a list of recently accessed configuration objects. This list displays the configuration object type and name (for example, `DNs`, `80708`), the Tenant to which the object belongs, and the last accessed date. Hover the mouse cursor over the item to see additional information, such as the specific date and time the object was accessed and its path. You can click the item to access the object.
- **Maximum number of recent items to display**—Specifies how many items to display in the **Show Recent** list.

Locale

In the **Locale** category, you can set the following preferences by selecting the appropriate radio button:

Preference (field name)	Description
Language	The language to use in the GAX user interface. The default is **Use system settings**. You can add more language options by installing language pack plug-ins. Important A browser refresh is required for the changes to take effect.
Date Format	The format in which dates are displayed in GAX. The default is **Use system settings**.
Start of Week	The day on which you consider the week to start. The default is **Use system settings**.
Number Format	The format in which numbers are displayed in GAX. The default is **Use system settings**.
Time Zone	The time zone in which times are displayed in GAX. The default is **Use system settings**.

System Preferences

Throttling

Genesys Administrator Extension enables you to throttle how many simultaneous requests are sent to Configuration Server, to minimize the risk of the server being overloaded. You can optimize these settings to help ensure consistent performance across your Genesys environment.

Bulk Update Batch Size specifies the maximum number of configuration updates that can be sent to Configuration Server simultaneously. The default value is `300`. A value of `0` indicates that there will be no throttling of changes for configuration objects (all requested operations will be sent to Configuration Server without delay). Valid values are `0` or any positive integer.

> **Important**
>
> The maximum **Bulk Update Batch Size** for users who are entering data from Genesys Administrator is 300.

Bulk Update Batch Timeout specifies how long (in seconds) Genesys Administrator Extension should wait after sending one batch before sending the next batch. The default value is 1. A value of 0 indicates that there will be no delay between bulk-update operations. Valid values are 0 to 300.

Agent Management

By default, the Agent Management dashboard is in hidden mode. If you want to manage your Agents in the Agent Management dashboard, you must enable it in premise mode.

- In **Hidden** mode, (the default), the Agents option does not appear in the GAX menu bar.
- In **Premise** mode, the Agents option is displayed. This mode simplifies the management of your Agents.

> **Important**
>
> If you were using a previous version of GAX, and were using the "Cloud" mode (no relation to the cloud-based architecture), you will be automatically moved to Hidden mode. You must manually reset the mode to Premise to continue to manage your Agents.

You can also set the following options for the **Add Agents** window, which appears only if you select the **Premise** option:

- **Enforce User Name as E-mail Address**—If checked, GAX ensures information entered in the **User Name** field is in the form of an email address.
- **Hide Employee ID**—If selected, GAX hides the **Employee ID** field when in the **Add Agent** and **Edit Agent** windows.
- **Hide External ID**—If selected, GAX hides the **External ID** field in the **Add Agent** and **Edit Agent** windows.
- **Show Folders**—If selected, GAX displays a folder-based view in the agent dashboard.
- **Default Access Group**—(Optional) The Access Group to which Agents are added when they are created in the Agents window. By default, this value is blank and Agents are not added to any Access Group.

> **Important**

- If you enter the name of an Access Group that does not exist, GAX cannot assign Agents to the group. You must create the Access Group first.
- Any value for this option does not apply when uploading Agents in bulk, since the Access Group is specified for each agent in the upload file.

- **New Virtual Agent Group's Name Suffix**—(Optional) The suffix of the name of any new Virtual Agent Group that is to be created. By default, the suffix is _VG.

Locale

In the **Locale** category, you can set the following preferences by selecting the appropriate radio button:

Preference (field name)	Description
Language	The language to use in the GAX user interface. The default is **English (US)**. You can add more language options by installing language pack plug-ins. Important A browser refresh is required for the changes to take effect.
Date Format	The format in which dates are displayed in GAX.
Start of Week	The day on which you consider the week to start, either Sunday or Monday.
Number Format	The format in which numbers are displayed in GAX.
Time Zone	The time zone in which times are displayed in GAX.

Adding Links to the Navigation Bar

Additional links can be added to the Navigation Bar by editing the configuration options of the default Application object:

Adding Custom Links

1. In Configuration Manager, click **Applications**. The **Applications** list displays.
2. Click the default client Application object in the list to edit the object.

> **Important**
> The default client Application name is defined in the options for the GAX Application object, in the **General** section. It is typically named **default**, but it might have another name in your environment.

3. Click the **Application Options** tab.
4. Click **Add**.
5. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation`
   - **Key**—You must enter the following: `categories`
   - **Value**—Enter the number of additional category items to add to the Navigation Bar. For example, to add one category item, set the value to 1.

     > **Important**
     > It is possible to enter `0` (zero), if you do not want to add additional category items to the Navigation Bar.

   - Click **OK**.
6. Click **Add**.
7. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation`
   - **Key**—You must enter the following: `items`
   - **Value**—Enter the number of additional links to add to the category item. For example, to add one link item, set the value to 1.

- Click **OK**.

Defining Category Items

For each category item, you must create an additional option that defines the parent category, an ID for the new category item, and a display name. Perform the following steps to define each category item.

1. Click **Add**.
2. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation_categories_0`
   - **Key**—You must enter the following: `category`
   - **Value**—Enter the name of the existing category items. For example, to add a menu item under the **Administration** category item, enter `administration`.

     > **Important**
     > You can add custom links only for the following categories:
     > - Administration/administration
     > - Routing Parameters/routingparam

   - Click **OK**.
3. Click **Add**.
4. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation_categories_0`
   - **Key**—You must enter the following: `name`
   - **Value**—Enter an ID for the category to add to the Navigation Bar. For example: `administration`

     > **Important**
     > You can add custom links only for the following categories:
     > - Administration/administration
     > - Routing Parameters/routingparam

   - Click **OK**.

5. Click **Add**.
6. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation_categories_0`
   - **Key**—You must enter the following: `title`
   - **Value**—Enter the name of the category to add to the Navigation Bar. For example: `Custom Links`
   - Click **OK**.

> **Important**
>
> Repeat the procedure above for additional category items. You must increment the **Section** name for each category item. For example, if you want to define three category items, the **Section** names are:
>
> - `ga_preferences.navigation_categories_0`
> - `ga_preferences.navigation_categories_1`
> - `ga_preferences.navigation_categories_2`

Defining Link Items

For each link item, you must create an additional option that defines the parent category, privilege, title, and URL. Perform the following steps to define each link item.

1. Click **Add**.
2. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation_items_0`
   - **Key**—You must enter the following: `category`
   - **Value**—Enter an ID for the category to add to the Navigation Bar. For example: `administration`

     > **Important**
     >
     > You can add custom links only for the following categories:
     >
     > - Administration/administration
     > - Routing Parameters/routingparam

   - Click **OK**.
3. Click **Add**.

4. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation_items_0`
   - **Key**—You must enter the following: `privilege`
   - **Value**—Enter the name of the privilege that dictates if the item is shown to a user. For example: `ACCESS_CUSTOM_LINKS`

   > **Important**
   > Refer to Assigned Privileges to learn more about assigning privileges.

   - Click **OK**.
5. Click **Add**.
6. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation_items_0`
   - **Key**—You must enter the following: `title`
   - **Value**—Enter the name of the link item to add to the Navigation Bar. For example: `Genesys`
   - Click **OK**.
7. Click **Add**.
8. In the pop-up window, enter the following information:
   - **Section**—You must enter the following: `ga_preferences.navigation_items_0`
   - **Key**—You must enter the following: `url`
   - **Value**—Enter the URL to which the link item points. For example: `http://www.genesys.com`
   - Click **OK**.

> **Important**
> Repeat the procedure above for additional link items. You must increment the **Section** name for each link item. For example, if you want to define three link items, the **Section** names are:
>
> - `ga_preferences.navigation_items_0`
> - `ga_preferences.navigation_items_1`
> - `ga_preferences.navigation_items_2`

Plug-In Management

This panel enables you to view information about the plug-ins that are installed in your environment. It also enables you to modify the settings of those plug-ins.

> **Important**
>
> Plug-ins can be managed on the local node only when the GAX Application object is of type:
>
> - **Generic Genesys Server** (when using Management Framework releases 8.1.0 or lower).
> - **Generic Administrator Server** (when using Management Framework releases 8.1.1 or higher).

Installing Plug-ins

Install plug-ins using the same process as for installing installation packages. For more information, see Uploading Installation Packages.

Viewing Installed Plug-ins

To see what Plug-ins are installed in your environment, select **Plug-In Management** from the **Administration** menu in the GAX Header. The **Administrator Applications** panel lists the applications that are installed in your environment and the host upon which the applications are stored. Use the **Quick Filter** field to filter the list.

In the **Administrator Applications** panel, click the name of an application to view plugins related to that application. The **Plug-in Info** panel shows the following information about each plugin:

- **Name**—The name of the plug-in
- **Version**—The version number of the plug-in
- **Language**—The language used by the user interface of the plug-in
- **Provider**—The name of the company or user that provided the plug-in
- **State**—Indicates whether the plug-in is **Enabled** or **Disabled**

To view additional information about a plug-in, click the name of a plug-in. In the <plug-in name> panel, you can also enable or disable the plug-in or modify the settings of the plug-in.

Changing the State of a Plug-in

Procedure: Enabling or Disabling a Plug-In

Steps

1. Select an application in the **Administrator Applications** panel.
2. In the Plug-in Info panel, select a plug-in in the **Plug-in Info** list.
3. In the <plug-in name> panel, click **Enable** or **Disable** (as appropriate) to enable or disable the plug-in.

Modifying the Options of a Plug-in

> **Important**
> You can modify only existing options for each plug-in from the **Plug-in Management** panels. You cannot create new options for the plug-ins.

Procedure: Modifying the Options of a Plug-In

Steps

1. Select an application in the **Administrator Applications** list.
2. In the Plug-in Info panel, select a plug-in in the **Plug-in Info** list.
3. In the <plug-in name> panel, click the gear wheel and select **Plug-in Options** to display the configuration options for this plug-in.

4. In the **Plug-in Options** panel, click a **Key** name to view details about the option, and modify its value, if necessary.
5. When you are finished making any changes, click **Save** to save any changes, or click **Cancel** to discard any changes.

Using the Command Line Console (CLC)

The Command Line Console (CLC) enables administrators to use the command line to execute certain GAX functions on solution definitions (SPDs) and installation packages (IPs). For example, you might use the CLC to silently deploy SPDs onto remote hosts.

You must be able to access the operating system's command-line interface to use the CLC. If you are not on the GAX host machine, you must have the CLC tool (**gaxclc.jar**) available on the local machine.

To access CLC's embedded Help file, execute one of the following commands:

```
java –jar gaxclc.jar help
```

```
java –jar gaxclc.jar ?
```

> **Important**
>
> As you execute commands with CLC, a log file is generated in the same location as where the tool is executed.

Structure

CLC supports commands that use the following structure:

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> <function> <operation> <args>
```

In the above example:

- `-u:user` is the user name to log in to Configuration Server.
- `-p:password` is the password to log in to Configuration Server. CLC assumes there is no password if this flag does not specify a value.
- `-s` instructs CLC to use a secure *https* connection to the GAX server. If this flag is not specified, CLC uses *http*.
- `-h:<host>:<port>` specifies the host and port of the GAX server. If this flag is not specified, CLC uses the following value: `-h:localhost:8080`.
- `<function>` can be either `ip` or `spd`.
- `<operation>` specifies the operation to be executed. The valid values for this flag are specific to the function you specified in the previous step (`ip` or `spd`).
- `<args>` specifies the operation arguments. The valid values for this flag are specific to the `<function>` and `<operation>` parameters you specified in the previous steps.

The following is an example of a CLC command:

```
java -jar gaxclc.jar -u:default -p:password -h:localhost:8080 spd execute 10054 1 "C:/GAX/
input.txt"
```

SPDs

CLC supports the following operations for SPDs:

- `add`
- `query`
- `querybyid`
- `execute`
- `delete`
- `encrypt` (see `execute` tab)

add

add

Overview

This operation adds an SPD to the GAX database. If the SPD already exists, as determined by the name and version in the SPD XML, this operation replaces the existing SPD.

If successful, the operation returns the ID of the added SPD.

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> spd add "file path"
```

- `"file path"`—The path to the XML file.

Example

```
java -jar gaxclc.jar -u:default -p:password spd add "c:\GAX\newSpd.xml"
```

query

query

Overview

This operation queries all SPDs and displays a table that lists the following for each SPD:

- ID number
- Name
- Version
- Tenant DBID

The following is an example:

```
10054 gvp 8.1.5 1
10060 genesysOne 8.1.5 1
10060 eServices 8.1.5 1
```

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> spd query
```

Example

```
java -jar gaxclc.jar -u:default -p:password -s -h:132.45.43.45:443 spd query
```

querybyid

querybyid

Overview

This operation queries an SPD by its ID. If the SPD does not exist, the operation fails.

If successful, the operation displays a table that lists the following details about the SPD:

- Profile ID
- Name

For example:

```
1 Install
```

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> spd query SPDID
```

- SPDID—The ID of the SPD that is being queried.

Example

```
java -jar gaxclc.jar -u:default -p:password -h:132.45.43.45:8080 spd query 4374
```

execute

execute

Overview

This operation executes a SPD.

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> spd execute SPDID profileName|
-profileID:profileID|-profileName:profileName -encrypted "input file"
```

- SPDID—The ID of the SPD to be executed.
- profileName|-profileID:profileID|-profileName:profileName—The SPD profile to be executed.

> **Important**
> If no flag is specified, then profileName is assumed as the SPD profile to be executed.

- -encrypted—If specified, indicates if the input file is encrypted.

[+] Show Usage

CLC provides encryption support for input files that include sensitive data such as passwords.

Format:

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> spd encrypt "input file path"
"encrypted output file path"
```

The encrypted input file is stored in the location specified by "encrypted output file path". If the file already exists at this location, it is overwritten.

Example:

```
java -jar gaxclc.jar -u:default -p:password spd -encrypted "c:\GAX\input.txt" "c:\GAX\
```

```
encrypted.txt"

java -jar gaxclc.jar -u:default -p:password spd -encrypted "input.txt" "encrypted.txt"
```

- `"input file"`—Specifies the input file that contains SPD parameters. If `-encrypted` is set, the input file is encrypted.

The input file must be in JSONObject format and include SPD parameters for a specific profile. The file must be encoded in UTF-8 format.

[+] Show usage

STRING Type

The input structure for a *string* type is described below:

```
{
        "Dialog name" : {
                "Input name" : "string"
        }
}
```

Example

SPD Profile

```
<profile name="Install">
 <dialog step="Step1">
        <input name="NAME_PARAM1" title="PERSON NAME"  default="birit" type="string"
required="true">
           <description>Please enter the person name</description>
        </input>
 </dialog>
 <dialog step="Step2">
        <input name="NAME_PARAM2" title="PERSON NAME"  default="birit" type="string"
required="true">
           <description>Please enter the person name</description>
        </input>
 </dialog>
 <execution>
        <script>
                log('string test' );
        </script>
 </execution>
</profile>
```

Input File for Install Profile

```
{
        "Step1" : {
                "NAME_PARAM1" : "Kate"
```

```
        },
        "Step2" : {
                "NAME_PARAM2" : "John"
        }
}
```

BOOLEAN Type

The input structure for a *boolean* type is described below:

```
{
        "Dialog name" : {
                "Input name" : true/false
        }
}
```

Example

SPD Profile

```
<profile name="Install">
 <dialog step="Step1">
        <input name="STATUS" title="status"  type="boolean" required="true">
           <description>status field</description>
        </input>
 </dialog>
 <execution>
        <script>
                log('boolean test');
        </script>
 </execution>
</profile>
```

Input File for Install Profile

```
{
        "Step1" : {
                "STATUS" : true
        }
}
```

INTEGER Type

The input structure for an *integer* type is described below:

```
{
        "Dialog name" : {
```

```
                "Input name" : <integer>
        }
}
```

Example

SPD Profile

```
<profile name="Install">
 <dialog step="Step1">
        <input name="NUMBER" title="number"  type="integer" required="true">
           <description>number field</description>
        </input>
 </dialog>
 <execution>
        <script>
                log('number test');
        </script>
 </execution>
</profile>
```

Input File for Install Profile

```
{
        "Step1" : {
                "NUMBER" : 132
        }
}
```

PASSWORD Type

The input structure for a *password* type is described below:

```
{
        "Dialog name" : {
                "Input name" : "password"
        }
}
```

> **Important**
>
> Input files that include sensitive data such as passwords should be encrypted using the SPD encrypt operation.

Example

SPD Profile

```
<profile name="Install">
 <dialog step="Step1">
        <input name="PASSWORD" title="password"  type="password" required="true">
           <description>password field</description>
        </input>
 </dialog>
 <execution>
        <script>
                log('password test');
        </script>
 </execution>
</profile>
```

Input File for Install Profile

```
{
        "Step1" : {
                "PASSWORD" : "xyz9846gdkjg"
        }
}
```

SELECTONE Type

The input structure for a *selectOne* type with an **<objectselect>** tag is described bellow:

```
{
        "Dialog name" : {
                "Input name" : {
                        "objectselect" : {
                                "filter" : [{
                                                "value" : "filter value",
                                                "name"  : "filter name"
                                        }
                                ]
                        }
                }
        }
}
```

> **Important**
>
> CLC intersects (*AND*) filters defined in the SPD file and input file for a *selectOne* input.

> The filter criteria should be different in an SPD input file and filter names should differ in the same filter definition.

Example

SPD Profile

```
<profile name="Install">
 <dialog step="Step1">
        <input name="APP_OBJ_SELECT_ONE" title="Application Name" hidden="false"
type="selectOne" default="">
                                <description>select application</description>
                                <objectselect>
                                        <filter value="CfgApplication" name="type"/>
                                </objectselect>
        </input>
 </dialog>
 <execution>
        <script>
                log('test select one' );
        </script>

 </execution>
```

Input File for Install Profile

```
{
        "Step1" : {
                "APP_OBJ_SELECT_ONE" : {
                        "objectselect" : {
                                "filter" : [{
                                                "value" : "SIP_lrm26",
                                                "name"  : "name"
                                        }
                                ]
                        }
                }
        }
}
```

SELECTMULTIPLE Type

The input structure for a *selectMultiple* type with **<objectselect>** tag is described below:

```
{
        "Dialog name" : {
                "Input name" : {
                        "objectselect" : {
```

```
                                "filter" : [{
                                                "value" : "filter value",
                                                "name"  : "filter name"
                                        }
                                ]
                        }
                }
        }
}
```

Filters defined in an SPD input file are joined in union (*OR*) and then intersect (*AND*) with filters defined in an SPD file for a *selectMultiple* input.

Example

SPD Profile

```
<profile name="Install">
 <dialog step="Step1">
        <input name="APP_OBJ_SELECT_MULTIPLE" title="Application Name" hidden="false"
type="selectMultiple" default="">
                                <description>select application</description>
                                <objectselect>
                                        <filter value="CfgApplication" name="type"/>
                                </objectselect>
        </input>
 </dialog>
 <execution>
        <script>
                log('test select multiple' );
        </script>

 </execution>
```

Input File for Install Profile

```
{
        "Step1" : {
                "APP_OBJ_SELECT_MULTIPLE" : {
                        "objectselect" : {
                                "filter" : [{
                                                "value" : "SIP_lrm26",
                                                "name"  : "name"
                                        },{
                                                "value" : "SIP_lrm27",
                                                "name"  : "name"
                                        }
                                ]
                        }
                }
        }
}
```

The operation returns two applications named **SIP_lrm26** and **SIP_lrm27**.

SELECTONE Type

The input structure for a *selectOne/selectMultiple/boolean* type with **<selection>** tag is described below:

```
{
        "Dialog name" : {
                "Input name" : {
                        "selection" : {
                                "option" : [{
                                                "value" : "option value assigned to the input
parameter",
                                                "name"  : "option name is displayed in UI"
                                        }
                                ]
                        }
                }
        }
}
```

CLC selects options defined in the SPD input file. Multiple options can be specified only for the *selectMultiple* input type.

Example

SPD Profile

```
<profile name="Install">
 <dialog step="Application Parameters">
        <input name="DATA_MODEL" title="Binary Version (32-bit or 64-bit)" default="64"
type="selectOne" required="true">
            <description>This parameter defines the 32-bit or the 64-bit version of the
binary to be deployed.  </description>
                <selection>
                    <option name="32" value="32"/>
                    <option name="64" value="64"/>
                </selection>
        </input>
 </dialog>
 <execution>
        <script>
                log('test selection support' );
        </script>

 </execution>
```

Input File for Install Profile

```
{
        "Application Parameters" : {
                "DATA_MODEL" : {
                        "selection" : {
                                "option" : [{
                                                "value" : "64",
                                                "name"  : "64"
                                        }
                                ]
                        }
                }
        }
}
```

Important

- If the input file does not specify a value for a SPD parameter, the value defined in the **default** attribute of the input element will be used.
- If an SPD input element has the **required** attribute set to `true`, but there is no corresponding input value that is supplied in either the SPD (as a default) or in the input file, then the SPD execution fails.
- If an SPD input element has the **readonly** attribute value set to `true`, then the value in the **default** attribute value is used for the execution, if defined. If the **readonly** attribute value is set to true, **required** is set to `false`, and the **default** attribute is not defined, then the following logic is used for input value determination:
  1. For the *boolean* input type, the input value is set to `false`.
  2. For the *string* and *password* input types, the input value is set to `""`.
  3. For the *integer* input type, the input is not propagated.
- If a dialog **cond** attribute value evaluates to false, the dialog is skipped by the CLC tool. Example:

```
<dialog step="Role input" cond="false">
  <input name="ROLE" title="Role" hidden="false" type="selectOne"
required="true">
        <description>Please indicate the role</description>
                <objectselect>
                        <filter value="CfgRole" name="type"/>
                </objectselect>
        </input>
 </dialog>
```

Example

```
java -jar gaxclc.jar -u:default -p:password -s -h:localhost:8080 spd execute 10054
-profileID:1 "C:/GAX/input.txt"
```

```
java -jar gaxclc.jar -u:default -p:password -h:localhost:8080 spd execute 10054
-profileName:"Install profile" "C:/GAX/input.txt"
```

```
java -jar gaxclc.jar -u:default -p:password -s -h:localhost:8080 spd execute 10054 1
-encrypted "C:/GAX/encryptedinput.txt"
```

delete

delete

Overview

This operation deletes an SPD. If SPD does not exist, the operation fails.

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> spd delete SPDID
```

- SPDID—The ID of the SPD to be deleted.

Example

```
java -jar gaxclc.jar -u:default -p:password spd delete 5436
```

IPs

CLC supports the following operations for the ip function:

- add
- query
- querybyid
- delete

add

add

Overview

This operation adds an IP (packaged as a .zip file) to the GAX database. If the IP already exists, it is replaced.

If successful, the operation displays the ID of the IP.

> **Important**
> The .zip file must contain the IP and the templates folder for the IP.

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> ip add "path to IP zip file"
```

Example

```
java -jar gaxclc.jar -u:default -p:password ip add "C:\GAX\TESTS\zippedIpUpload\PRODUCTION\
IP_TSrvSIP64_18100079b1_ENU_windows.zip"
```

query

query

Overview

This operation queries all IPs and displays a table that lists the following details for each IP:

- ID number
- Name
- Version
- OS
- Locale

- Status

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> ip query
```

Example

```
java -jar gaxclc.jar -u:default -p:password -s -h:132.45.43.45:443 ip query
```

querybyid

querybyid

Overview

This operation queries an IP by its ID and displays a table that lists the following details:

- ID number
- Name
- Version
- OS
- Locale
- Status

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> ip query IPID
```

- `IPID`—The ID of the IP to query.

Example

```
java -jar gaxclc.jar -u:default -p:password -h:132.45.43.45:8080 ip query 543
```

delete

delete

Overview

This operation deletes an IP.

Format

```
java –jar gaxclc.jar -u:user -p:password -s -h:<host>:<port> ip delete IPID
```

- IPID—The ID of the IP to delete.

Example

```
java -jar gaxclc.jar -u:default -p:password ip delete 547
```

System Dashboard

The System Dashboard helps you to monitor your contact center. It shows a high-level summary of the current operations of your environment, as follows:

- Active Alarms—A summary of active alarms.
- Hosts—A summary of the hosts in your environment, and their status.
- Applications—A summary of the applications in your environment, and their status.
- Solutions—a summary of the solutions in your environment, and their status.

To view detailed information about the contents of each widget in a tab, click the name of the respective tab, or open the contextual menu (three vertical dots) in the widget and select **Expand to Tab**. You can also rename the widget by selecting **Edit**.

Important

- Dashboards are not supported if you are using Internet Explorer 8 or earlier.
- GAX must have a connection to Solution Control Server (SCS) for the System Dashboard to function. See Step 5: Add SCS connection of Deploying Genesys Administrator Extension via Setup Mode in the Genesys Administrator Extension Deployment Guide for more information.

Alarms

The Alarms widget shows a list of active Critical, Major and Minor alarms in the system, sorted by priority. The widget updates automatically when a new alarm is activated.

Important

- An active alarm is visible only if you have access to the application which generated the alarm.
- For Genesys Administrator Extension to monitor the system, Management Layer components must be deployed in the system, and Genesys Administrator Extension must be deployed with connections to the Solution Control Server. For detailed instructions, see the Management Framework Deployment Guide.

Each Alarm in the list displays one of the following severity levels:

- Critical
- Major
- Minor
- Unknown

To clear an Alarm, do the following:

[+] Show steps

1. Display the Alarms tab.
2. Select the check boxes of the Alarms that you want to clear.
3. Click **More** and select **Clear**.

Troubleshooting Alarms Viewing

If an event that is configured to generate an alarm does not result in an alarm, verify that:

- The corresponding Alarm Condition is configured correctly.
- The corresponding log event was generated. To verify this, check whether the log event appears in a local text file.
- The Application that generates the event is configured to send its log to a network Message Server.
- The network log output of the given Application is set to Interaction or Trace if the event is reported at either Interaction or Trace log-output level.
- Message Server is receiving log events that the given Application generated. Check the Message Server log.
- Solution Control Server is connected to Message Server.
- Solution Control Server receives alarm messages from Message Server. Check the Solution Control Server log.
- Genesys Administrator Extension is properly connected to Solution Control Server.

Applications

The Applications widget shows a list of the Applications in the system. Applications with a status of **Unknown** are shown at the top of the list. This widget updates automatically when the status of an Application changes. Each Application in the list has one of the following status levels: **[+] Show status levels**

Status Level	Description
Initializing	Indicates that an application is performing the initialization steps, which involve:

Status Level	Description
	• Starting the application. • Reading configuration data from the Configuration Database. • Checking this data for integrity and completeness. • Establishing connections with all the resources according to the given configuration data. At this stage, the application is connected to the LCA (Local Control Agent) running on its host, but it is not ready to provide the service (for example, to accept client connections).
Started	Assigned from the moment an application is completely initialized; that is, when the application: • Has read and checked its configuration. • Has established connections with all the required resources. • Is ready to provide its service. • Is connected to the LCA running on its host. This status does not necessarily mean that the application is performing its function. To start working, some applications may require additional solution-specific control operations through their user interfaces. For information, refer to solution-specific documentation.
Service Unavailable	Indicates that, although an application is running, it cannot provide the service, for some internal reason.
Start Pending	The application is being activated. Solution Control Server (SCS) has executed the Startup command, but the application has not yet connected to the LCA on its host. This status exists only for the interval between the command to start the application and the LCA report that the application is being connected.
Stopped	Indicates that an application is installed and configured in the system, but it has not started. In other words, the application either has not been activated or has terminated unexpectedly.
Stop Pending	The application is being shut down. The application has accepted the Stop command from SCS, but it has not yet disconnected from the LCA on its host. This status exists only for the interval between the instruction to stop the application and its actual termination. Typically, the Pending stage involves some application-specific wrap-up functions, closing of all open connections, termination, and detection of the termination by LCA.

Status Level	Description
Suspended	Indicates that an application has received a request to shut down gracefully, has stopped accepting new client connections, and has finished processing all current connections and requests.
Suspending	Indicates that an application has received a request to shut down gracefully and has stopped accepting new client connections and requests. It is still processing current connections and requests.
Unknown	Indicates that the Management Layer cannot provide reliable information about the current application status. In other words, SCS is not connected to the LCA on the host where the application is configured to run. This status does not necessarily mean that the application cannot perform its function. Important All GUI desktop applications are displayed with a status of Unknown.

In the Applications tab, you can perform the following actions:

- Start the Application
- Stop the Application gracefully
- Stop the Application immediately
- Switch over a backup Application to primary mode

Hosts

The Hosts widget shows a list of Hosts in your environment. This list updates automatically when the status of a Host changes. Each Host in the list has a status, which is one of the following: **[+] Show status levels**

Status	Description
Up	Indicates that Solution Control Server (SCS) has successfully connected to Local Control Agent (LCA) running on the given host and that it, therefore, can control and monitor all applications located on this host.
Down	Indicates that SCS cannot connect to LCA running on the given host, or that it has lost a previously established connection. This status indicates one of the following: • LCA has not started on the given host, has terminated, or has stopped responding.

Status	Description
	• LCA is not configured correctly in the Configuration Database.
Unavailable	Indicates that SCS cannot connect to LCA running on the given host, or that it has lost a previously established connection because the host is not started or has failed.
Unreachable	Indicates that SCS cannot connect to LCA running on the given host, or that it has lost a previously established connection because of a network connectivity problem between SCS and the host. Specifically, there is no route to the host.
Unknown	Indicates one of two situations: • In a Distributed SCS configuration, the SCS to which Genesys Administrator is connected cannot connect to, or has lost a previously established connection with, another distributed SCS that is assigned to the given host. • Genesys Administrator Extension cannot connect to, or has lost its connection with, SCS on the given host. In this case, Genesys Administrator Extension will show all hosts with a Unknown status.

In the Hosts tab, click the graph icon in the very last column to view the following information about the Host:

- CPU and memory usage. Real-time information for each CPU is broken down as follows:
  - **User Time (%)**
  - **Kernel Time (%)**
  - **Non-Idle Time (%)**
- Basic real-time memory information, in kilobytes:
  - **Used Virtual Memory**
  - **Total Virtual Memory**

In the Host Information window, you can also select the appropriate tab to view information about the following:

- **Processes**—Displays all processes running on the host. For each process, the Processes tab displays the following:
  - **Name**
  - **PID** (process identifier)
  - **CPU Usage (%)**

  - **Mem Usage (MB)**
  - **Priority**
  - **Services**
  - **Charts**

- **Services**—Displays programs installed to run as Windows Services on the selected host. This tab only displays information about host computers running a Genesys-supported Windows operating system. For each service, the Services tab indicates:
  - **Name**—the actual name of the program installed as a Windows Service.
  - **Display Name**—the service name of the program, as it appears in the Services window.
  - **State**—the current state of the service.
  - **Win32 Exit Code**—the error code reported for an error occurring during a service startup or shutdown.
  - **Svc Exit Code**—the service-specific error code reported for an error occurring during a service startup or shutdown.
  - **Checkpoint**—the operation progress indicator that the service uses during a lengthy operation.
  - **Wait Hint**—the interval, in milliseconds, during which the current operational step should be completed.

> **Tip**
> See the documentation for your Microsoft Windows operating system for more information.

- **Charts**—Displays a graph of memory and processor usage on the host.

Solutions

The Solutions widget shows a list of Solutions in your environment. This list updates automatically when the status of a Solution changes. Each Solution in the list has a status, as follows: **[+] Show status levels**

Status Level	Description
Start Pending	Indicates that a request to start the solution was sent by SCS, but there are some applications that still need to be started in the solution.
Started	Indicates that a solution is ready to perform its major function; that is, all mandatory solution components have reported Started status. This status does not necessarily mean that the solution is actually performing its function. To start working, some solutions

Status Level	Description
	might require additional solution-specific control operations through their user interfaces. For information, refer to solution-specific documentation.
Stop Pending	Indicates that a request to stop the solution was sent by SCS, but there are some applications that still need to be stopped in the solution.
Stopped	Indicates that one or more of the solution's mandatory components do not have Started status; therefore, the solution cannot perform its function. Stopped status can indicate that a solution either has not been activated, or has failed because one of its mandatory components is unavailable.
Unknown	Indicates that the Management Layer cannot provide reliable information about the solution status. This status does not necessarily mean that the solution is unable to perform its function.

In the Solutions tab, you can perform the following actions:

- Start a Solution
- Stop a Solution gracefully
- Start a Solution immediately

Start

> **Important**
> You can start a Solution of type Default Solution Type or Framework from Genesys Administrator Extension only if the Solution was created using a Solution Wizard.

To start a Solution, do the following:

[+] Show steps

1. Select the check boxes beside the Solutions that you want to start.
2. Click **More** and select **Start**.

Genesys Administrator Extension sends the Startup command for each Solution to Solution Control Server (SCS). SCS starts Solutions in the order in which it reads their configuration from Configuration Server and processes each Startup command as it would for a Solution that was started individually.

> **Important**
>
> Complete Solution startup can take some time. The amount of time varies, depending on the number and location of Solution components and the time required to initialize each component.

SCS checks the status of all the Solution's mandatory components that are configured to be controlled by the Management Layer.

Genesys Administrator Extension reports the successful start of a Solution after all these components have reported a status of Started within the configured timeout. When the Solution starts, its status changes from Stopped to Started.

> **Important**
>
> - You can start a Solution only if you have Execute permission for the Solution configuration object in the Configuration Layer.
> - Because a number of Solutions can share the same applications, some Solution components may have a status of Started before you start the Solution.
> - In redundant configurations, both primary and backup Solution components start simultaneously; they are assigned runtime redundancy modes according to their configuration.

Stop

> **Important**
>
> You can stop a Solution of Default Solution Type or Framework from Genesys Administrator Extension only if the Solution was created using a Solution Wizard.

This action is similar to the **Graceful Stop** command in Genesys Administrator. When you stop a Solution gracefully, all of the Applications making up the Solution stop accepting new requests and finish processing those requests that each currently has in its queue.

You can stop a Solution gracefully only if you have Execute permission for the Solution object.

To stop a Solution gracefully, do the following:

[+] Click to show section

1. Select the check boxes of the Solutions that you want to stop.

2. Click **More** and select **Stop**.

Genesys Administrator sends the Stop command for each Solution to Solution Control Server (SCS). SCS uses Local Control Agents (LCA) to deactivate the Solution components in the reverse order from the component-startup order. (The component-startup order is defined in the Solution configuration object.)

Important

- Because a number of Solutions can share the same Applications, some Solution components may continue to have a status of Started after you stop the Solution, whether gracefully or ungracefully.
- In redundant configurations, both primary and backup Solution components stop simultaneously.

Force Stop

Important

You can stop a Solution of type Default Solution Type or Framework from Genesys Administrator Extension only if the Solution was created using a Solution Wizard.

When you stop a Solution ungracefully, the Solution stops abruptly, and all of its composite applications immediately stop processing, both new and current. You can stop a Solution in this way only if you have Execute permission for the Solution object.

To stop a Solution immediately, do the following:

[+] Show steps

1. Select the check boxes beside the Solutions that you want to stop.
2. Click **More** and select **Force Stop**.

Tip

You can also start and stop solutions by clicking on the status name in the Solutions tab. For example, if a solution has a status of **Started** and you click the status name, the solution attempts to stop. Likewise, if a solution has a status of **Stopped** and you click the status name, the solution attempts to start.

Genesys Administrator Extension sends the Stop command for each Solution to SCS, which uses Local Control Agents (LCA) to deactivate the Solution components in reverse order from the component startup. (The component-startup order is defined in the Solution configuration object.)

Important

- Because a number of Solutions can share the same applications, some Solution components may continue to have a status of Started after you stop the Solution, whether gracefully or ungracefully.
- In redundant configurations, both primary and backup Solution components stop simultaneously.

Agents

Agents are Users who handle customer interactions directly.

> **Important**
>
> - If the Agents option does not appear in the GAX Header, change it by selecting **Agent Management** in System Preferences and changing **Mode** to **Premise**. See System Preferences for more information.
> - If you used Cloud mode in a pre-8.5.25x version of GAX, you have automatically been converted to Hidden mode. Follow the steps in the previous point to make the Agents menu visible.

Agents View

The **Agents** view lists all Agents in your environment (or Tenant, if you are in a multi-tenant environment). You can only see those objects for which you have access.

To filter the list:

- Click **Show Quick Filter** and type a search term in the **Quick Filter** field. The list updates dynamically to show items that match the text in the **Quick Filter** field.
- Click **Show Column Filter** to show search fields for each column header. Enter a search term in one of these fields to quickly search the column for the search term.
- Click the cube icon to open the **Tenant Directory** window. In this window, click the Tenant that you want to select. Use the **Quick Filter** field to filter the Tenant list.
- Select a folder from the **Directory** drop-down list to filter based on folders (folder-based view). Folder-based view is not enabled by default. To enable folder-based view in the Agent Dashboard list view, go to **System Preferences** > **Agent Management** and then select **Show Folders**.

To sort the list, click in a column header. Clicking the header a second time reverses the sort order.

Bulk Operations on Agents

GAX provides some functionality that allows you to apply modifications to the Configuration Database in bulk, thereby speeding up the provisioning process. Currently, GAX supports the following bulk operations:

- Import/export .csv files to create new Agents and modify or delete existing Agents.

- Assign Skills to multiple Agents, including creating new Skills as required.

> **Important**
> Tenant users can update Agents for only the Tenant to which the user belongs.

Operations on Individual Agents

In the Agents view, you can:

- Add a new Agent from scratch, or create a copy of an Agent and modify it.
- Modify the properties of an existing Agent, or just toggle its State between `Enabled` or `Disabled`.
- Delete (remove) an existing Agent.

Create an Agent

> **Tip**
> If you have an existing Agent that has similar properties to the Agent that you want to add, you might want to copy the existing Agent and change its properties to create the new Agent. This will reduce your input time.

To create a new Agent, do the following:.

1. In the Agents view, click **Add**. The **Add Agent** window appears.
2. Enter the following information. For some fields, you can either enter the name or value or click **Browse** to select a value from a list:
   - Agent Information
     - **User Name**—The name that this Agent should use to log into the environment. You must specify a value for this property, and that value must be unique within the Configuration Database.
     - **First Name**—The first name of this Agent.
     - **Last Name**—The last name of this Agent.
     - **External ID**—This setting applies only if your environment is using external authentication, either LDAP or RADIUS. This may be the user name in the external authentication system. For LDAP, it might be a whole, or partial, LDAP URL corresponding to RFC 2255. For more information, refer to the *Framework External Authentication Reference Manual*.

> **Important**
>
> The **External ID** field might be hidden if the **Hide External ID** check box is checked in the System Preferences/Agent Management menu.

- **Email**—The email address of this Agent.
- **Password**—A password no longer than 64-characters that this Agent must use to log in to the environment. You cannot view the existing password.

> **Important**
>
> Passwords can be subject to format rules. Refer to the *Genesys Security Deployment Guide* for more information.

- **Organization**—The folder in which the Person object for this Agent is stored.
- **Place**—The Place assigned to this Agent. Click **Browse** to browse a list of Places in your environment. Once you select a Place, the **Number/DN** field is visible.
- **Agent Logins**—The Agent Login(s) of this Agent. Click **+** to add an Agent Login.
- **Number/DN**—The Number/DN of this Agent. This field appears once a Place is selected. Click **+** to add a DN.

- Add Agent Skills
  - You can add Skills to the Agent by:
    - Creating a Skill—Type the name of the new Skill in the **Quick Filter** field and click **+** to create the Skill.
    - Selecting an existing Skill—In the **Skills** section, select existing Skills from a list to add to the Agent. To select a Skill, click the check box beside the Skill and enter a numerical value in the **Rating** field.

> **Important**
>
> Since Agent Groups might be defined automatically based on a Skill (Virtual Agent Groups), the list of Agent Groups refreshes if you create a Skill.

3. Agent Groups
   - You can add the Agent to an Agent Group by clicking the check box beside an item in the list.
4. Click **Save**.

Copy an Agent

You might have an existing agent that has similar properties of one that you are adding. Instead of

creating that Agent from scratch, you can copy that Agent, and just modify it as required.

To copy an existing Agent, do the following:

1. In the Agents view, select the Agent that you want to copy.
2. Click **Clone**.
3. (Optional) Modify the Agent's information as required.
4. Click **Save** or **Cancel**, as appropriate.

Modify an Agent

To modify an Agent, do the following:

1. In the Agents view, select the Agent that you want to modify.
2. Click **Edit** and modify the Agent's information as required.
3. Click **Save** or **Cancel**, as appropriate.

Change the State of an Agent

To change only the State of an Agent, do the following:

1. In the Agents view, select the Agent for which you want to change its State.
2. Click **Enable** or **Disable**..
3. Click **Save** or **Cancel**, as appropriate.

Notes:

- Agents that are disabled appear grayed out in the list.
- When an Agent is disabled, GAX invalidates all sessions associated with this Agent. When the Agent next tries to use GAX, he or she will be redirected to the login page.

Delete (Remove) an Agent

To delete one or more Agents, do the following:

1. In the Agents view, select the Agents that you want to remove from your configuration.
2. Click **Delete**..
3. Click **Save** or **Cancel**, as appropriate.

Note: When deleting an Agent, GAX does not delete the DN, Place, or Agent Login objects associated with the Agent.

Bulk Import/Export of Agent Data

To create or modify or delete large numbers of agents, you upload a comma-separated value (CSV) file containing new and changed agent information. You enter or modify values in the appropriate columns for the agent. When uploaded to GAX, the agents listed in the file are created or modified or deleted, based on the action to be taken as indicated in the Action column.

The CSV file used to import/export Agent data is the same as that used to import/export Persons (Users) in Configuration Manager. Refer to CSV File for Importing and Exporting for a detailed description of the CSV file.

> **Important**
>
> Tenant users can update Agents in only the Tenant to which the user belongs.

GAX enables you to create spreadsheet templates for this purpose. You can create an empty template containing only column headers, or you can export data from existing agent records. The exported spreadsheet can be modified and then imported into GAX again to create or update or delete agent records.

> **Tip**
>
> You might want to create various templates that fit scenarios specific to your operations.

Creating an Empty Template

An empty template contains all of the mandatory columns plus column headers that you specify. It does not include any data—that is for you to fill in.

1. To create a template, click **Create Spreadsheet** in the Agents window or in the History window. This opens a column picker window in which you select the columns that you want to appear in the template.
2. In the column picker window, select the fields that you want included in the template. The selected columns appear in the columns list on the left. Drag the column names or use the arrows to put them in any order that you require. Note the following:
   - The mandatory fields are always included.
   - The Action field is always added as the first column.
   - For Skills, Agent Groups, Access Groups, and Switches, each object can be selected as a column.

The column header appears as <type>:<name>.

- Virtual Agent Group cannot be imported/exported in bulk, so are not listed in the Agent Groups table.

3. After you have selected and ordered the columns, click **Create Spreadsheet**. GAX generates and downloads the template file, called **download.csv**.

Exporting Data

GAX allows you to export data from existing data records. If you are modifying the spreadsheet to use as a template, save it as a CSV after making the appropriate changes, and upload it into GAX.

Exporting Agent Data From GAX into a CSV File

1. In the Agents list, select those Agents for whom you want to export data.
2. Click **Export**.
3. The column picker window has the associated fields pre-selected for the selected agent. For example, the associated Agent Groups, Access Groups, Skills, and Switches, will be pre-selected for those Agents that the user has selected before. Select more fields as required, or clear those fields that you do not want exported.
4. Click **Export**. GAX generates and downloads a spreadsheet called **download.csv** with the data that you selected for export.

Uploading a File

Before uploading the bulk updates, you must enter the data into a spreadsheet and save it as a CSV file. Do this in one of two ways:

- Create an empty template and fill in the appropriate values—This is probably the best way if the majority of your updates are adding new agents.
- Export existing data and make the necessary additions and changes—This is probably the best way if you are primarily making changes to existing agents. You can export the information for just those agents, saving you from filling in the mandatory information for them.

See the example of a prepared spreadsheet and CSV file here.

Now go ahead and upload the data into GAX.

1. Click **Import** in either the Agents window or in the History window.
2. Click **Select File** and, using the file browser, select your CSV file.
3. Click **Upload Spreadsheet**. GAX starts validating the file, and displays its progress. You can either click **Close** to close the window, or you can monitor the progress from here. Even if the window is closed,

processing will continue and can be monitored in the History window.

- If the **Spreadsheet is Valid**, click **Continue** to start the upload.
- If the dialog box displays one or more errors, open your file in a new window and fix the errors. Then repeat this process starting at step 2.

4. GAX starts processing the records and displays the progress. If necessary, you can do either of the following at any time:
   - Click **Close Window**. Processing will continue, and can be monitored in the History window.
   - Click **STOP Operation**, then click **Yes, STOP Operation** to confirm. When processing stops, you are returned to the Agent List view.
5. If you did not stop the upload, GAX displays **Operation Completed** when the processing of records is finished. It also displays a summary of results, namely the number of records that were successfully created and/or updated, and the number of records that were not updated or created because of an error. Click **Close Window** to go back to the main Agent list.

Script Actions

For new users:

1. Create a new Person with specified properties in the specified Folder.
2. Associate the new Person with the specified Access Groups.
3. Associated the new Person with the specified Agent Groups.
4. For Agents, add the specified Skills.
5. For Agents, do the following:
   - If the Extension field is not specified, create and associate Agent Logins on all specified Switches with the Login Code equal to the Username of the Agent. Agent Logins are created in the Switch Agent Logins folder of the same folder hierarchy specified for the Person object in the Folder property.
   - If the Extension field is specified, a new Place is created with the name equal to the Username of the Agent. Extension DNs are created with the number corresponding to the Extension field on all specified Switches. Agent Logins are created and associated with all specified Switches that have a Login Code equal to the value of the Extension field. All objects are created under their corresponding root folders using the same folder hierarchy as specified for the Person object in the Folder property.

For existing users:

1. Username and Is Agent fields must be populated in the input file identify the Person.
2. All other fields are optional.
3. If an optional field is defined, its value is compared to the existing value and, if different, updated for that Person.

Bulk Assignment of Skills to Agents

Genesys Administrator Extension enables you to assign Skills and associated ratings to multiple Agents with one click. You can even create a new Skill and assign it within the current view.

1. In the **Agents** view, select one or more Agents for whom you will be adding, modifying, or removing the same Skills. This activates the **Edit Skills** option in the **Agents** view toolbar.
2. Select **Edit Skills**. This opens the **Edit_<n>_Agents** dialog box, where **<n>** is the number of Agents selected.

> **Important**
>
> When this Edit Agents dialog box is open, you cannot perform any other operation in GAX within the current browser window. However, you can open a different browser tab or window concurrently to access the other operations in GAX. See Step 4 for information about the implications of logging out of GAX or closing your browser while this dialog box is open.

3. To modify what Skills are assigned to selected Agents, do any of the following:

> **Important**
>
> All Ratings must be a numerical value. Do not assign a Rating of `Mixed` to Agents; this term is used by GAX to indicate that selected Agents have different Ratings for the Skill.

   - To assign a Skill:

> **Tip**
>
> To create a new Skill, enter its Name in the **Quick Filter** box, press **Enter**, and then give it a numeric Rating.

     - If a Skill is not associated with any Agents (the selection box is empty), click twice in the selection box to change it to a checkmark, and enter the rating that you want to assign to the Agents.
     - If a Skill is already associated with some of the selected Agents (the selection box contains a dash (-)), clickce in the selection box to change it to a checkmark, and if required, enter or change the Rating value.
   - To remove an active skill from all selected Agents, clickce or twice in the selection box to clear it.
   - To modify a Skill Rating, click in the Rating field of the Skill and enter the new value. Note that the new value will apply only for selected Agents as indicated by the state of the selection box (checkmark–all; dash–some; empty–none).
4.

When you have finished making the changes, click **Apply** to save your changes. This opens a progress window, displaying real-time progress and results of the operation.

Updates are processed in batches of 10 Agents per batch. Do not log out of GAX or close your browser while the updates are being processing. If you do log out or close your browser before the operation is complete, the process stops, and only those batches completed up to the process stoppage are complete.

[+] Show example

For example, if you have selected 25 Agents, the changes are committed in three batches—two of ten Agents, and one of five Agents. If you log out or close the current browser session before the second batch of ten Agents has been processed or at least queued for processing at the GAX server, only the changes for the first 10 Agents (the first batch) will be saved. The changes for the second and third batches will not be made and will be discarded.

5. When the operation is complete, the progress window displays the final results of the operation. To view a detailed list of the results, click **View Details Summary**. This shows what Agents were updated successfully and what Agents were not updated. Click **Hide Details Summary** to go back to the summary of results, or click **Close Window** to close this window completely and return to the Agent's view.

Edit Agents Dialog Box

The **Edit <n> Agents** dialog box, where n is the number of Agents selected, displays a list of all Skills available for assignment to Agents.

Skills that have already been assigned to one or more or the selected Agents are listed first, and are considered *active*. In addition:

- If all selected Agents have the Skill, the Skill is marked with a checkmark in its selection box.
- If some but not all selected Agents have the Skill, the Skill is marked with a dash (`-`).

If none of the selected Agents have the Skill, the Skill is considered *inactive*, the selection box is empty, and the Skill appears greyed-out. Note that *inactive* is different from the Skill object being in a *disabled* state.

The Ratings column shows the ratings associated with corresponding Skills for all the selected Agents. If all selected Agents have different ratings for a Skill, a rating of `Mixed` is displayed; otherwise, the rating value (posessed by all of the selected agents) is given.

History Window

The **History** window displays a record of bulk (upload) operations.

Overview

To open the **History** window, click **History** in the **Agents** window. The **History** window lists recent bulk operations in descending order by time, that is, most recent first. The window contains the following columns:

- **Status**—**QUEUED**, **COMPLETE**, **IN-PROGRESS**, **STOPPED**, **FAILURE**
- **History of Operations**—The name of the .csv file that was uploaded or downloaded. If the operation is still in progress, its progress is displayed in terms of the number of records that have been processed. If the operation is finished. The total number of records processed, created, and updated is displayed, as is the number or records that were not processed because they contained an error.
- **User**—The username of the logged in user who ran the operation. This information is not displayed until the operation is finished.
- **Date**—The date and time when the operation finished.

The operations are listed by status in the following order: **FAILURE**, **IN-PROGRESS**, **QUEUED**, **STOPPED**, and **COMPLETE**. For each status, they are listed in descending order by time, that is, most recent first. The History window is refreshed every 5 seconds to keep you up to date on the state of current bulk operations.

Actions on Multiple Operations

The controls in the top left corner of the **History** window are:

- **Import**—Enables you to upload a CSV file. See Uploading a File for detailed instructions.
- **Create Spreadsheet**—Creates an empty template file containing all the mandatory columns plus any that you specify. the columns. See Generating an Empty Template File for detailed instructions.
- **Delete**—Removes the selected operations from the list. This does not remove the files themselves, just their record for purposes of this list.
- **Show Quick Filter**—Enables you to filter the list of operations to those in which you are interested.

Actions on Single Operations

In addition to the controls listed above, you can also click the gear-wheel icon next to the name of the CSV file to display a list of actions available for that particular operation. The actual actions available

depend on the status of the operation itself, but can include:

- **Stop Operation**—Stops the upload of the CSV file, if it is still in progress. GAX displays a warning that some records will not be processed, and prompts you for confirmation. Click **Yes, STOP operation**, and the operation stops. In addition to the usual record counts, the number of records not processed is displayed.
- **View Details**—Displays a list of records in the CSV file for any operation that is COMPLETED, either run to completion or stopped intentionally. An additional column **Operation**, shows the outcome for each record (`Created`, `Updated`, `Error`, or `Not Processed`). To view just those records with a specific outcome, clicke of the outcomes listed in the top right corner. To filter the record by another set of criteria, **Show Quick Filter**. To view only certain columns, click **Column Picker** and clear those columns that you do not want to see displayed. To export some or all of the records to a spreadsheet, select the records and **Export**. Then follow the steps in Exporting Data.
- **Delete**—Removes just this operation from the list of operations. This does not remove the file itself, just its record for purposes of this list. To remove more than one operation at once, select the operations and use Delete at the top of the window, as described above.

Configuration Manager

Configuration Manager is where you set up and maintain the configuration objects in your contact center. These objects, also referred to as Configuration Database objects, contain the data that Genesys applications and solutions require to operate in a particular environment.

About Configuration Objects

Configuration objects, also referred to as *Configuration Database objects*, contain the data that Genesys applications and solutions require to operate in a particular environment. You create and maintain the objects in Configuration Manager, and they are stored in the Configuration Database.

To view and manage configuration objects for a specific Tenant, click the cube icon and enter the name of the Tenant in the **Tenant Directory** field. By default, Configuration Manager lists configuration objects for the Tenant to which your user account belongs. When viewing objects by Tenant, if you choose to create a new object, that object is created in the directory for that Tenant.

Important

- The **Tenant Directory** field is not shown in a single-Tenant environment.
- Because most objects in the Configuration Database mirror physical objects in your contact center (for example, switches, agents, and installed applications), this document uses an initial capital letter for configuration objects. For example, the word switch appears in lowercase when it refers to a physical switch in your contact center, but it is capitalized when it refers to the configuration object that mirrors your physical switch. Similarly, the word application appears in lowercase when it refers to a physical installation in your contact center, but it is capitalized when it refers to the configuration object that mirrors the installed program.

Object Hierarchy

In Genesys Administrator Extension, objects are stored in folders, usually with one object type per folder.

To help you better manage your configuration environment, you can create a hierarchy by manually creating any combination of the following:

- Folders and subfolders—A folder contains objects of one type. For example, for Host objects, you might choose to create subfolders that group hosts by location.
- Business Units/Sites—Unlike folders, Business Units and Sites can contain objects of different types. For example, all configuration objects related to a specific site for your business can be grouped into a Site,

which then contains configuration objects within folders and subfolders.

In addition, the following objects include their parent objects as part of their hierarchy:

- Campaign Groups—Hierarchy includes Campaigns.
- IVR Ports—Hierarchy includes IVRs.
- Business Attribute Values—Hierarchy includes Business Attributes.
- Agent Logins—Hierarchy includes Switches.
- DNs—Hierarchy includes Switches.

Genesys Administrator Extension displays a navigation path (a set of breadcrumbs) that shows you where the displayed objects reside in your hierarchy. This path appears with all lists of objects, and is located directly above the list. You can click any element of this path to go quickly to that element.

Some object types might only exist under the root tenant or a Business Unit/Site. If you are viewing objects by Tenant, you might not see the following objects:

- Alarm Conditions
- Application Templates
- Applications
- Hosts
- Solutions
- Switching Offices

Required Permissions

The minimum permissions required to perform a task in Genesys Administrator Extension depend on the task. You must also be granted appropriate Role privileges to perform specific tasks on an object or group of objects.

Permission	Description	Prerequisites
Read	• To view a particular object, you must have Read permission for that object. • In Configuration Manager, you can view the object type. If you do not have Read permission for the object, you cannot see it in Configuration Manager. • In list views, you can view the following button: **Edit**. • You can click an object to view its details.	None

Permission	Description	Prerequisites
Create	• To create an object under a particular folder, you must have Create permission for that folder. The person who creates an object receives Full Control permissions for that object. Other accounts have the same access permissions for a newly created object as they do for the folder in which the object is created. • In list views, you can view the following buttons: **New**, **Clone**, and **Move To**. • In object detail views, you can view the following buttons: **Clone** and **Move to**. You can also view the following tabs: **Options**, **Permissions**, and **Dependencies**.	Read
Update	• To modify a particular object, you must have Update permission for that object. • In list views, you can view the following button: **Enable** or **Disable**. • In object detail views, you can view the following buttons: **Enable** or **Disable**, **Save**, and **Apply**.	Read
Delete	• To delete a particular object, you must have Delete permission for that object. • In list views, you can view the following button: **Delete**. • In object detail views, you can view the following button: **Delete**.	Read

Read Only Mode and Emergency Mode

The Read Only Mode and the Emergency Mode features enable you to restrict users from making changes to the Configuration Database during a Configuration Server maintenance. An appropriate

error message is displayed for any GAX user who attempts to update or save any configuration objects while the Configuration Server is in one of these two modes. Only Super Administrators can update the objects while the Configuration Server is in the Emergency Mode. For more information on the Read Only Mode and Emergency Mode, see Read Only Mode and Emergency Mode.

Common Object Properties

Almost all configuration objects have the following configuration properties and elements:

- **Name** property
- **State Enabled** property
- **Options** tab
- **Permissions** tab
- **Dependencies** tab

Name Property

Names uniquely identify objects within a certain range. Therefore, the name, which can be up to 255 characters, is a required parameter for most types of objects. The exceptions are:

- DNs and Agent Logins—Their unique numbers and codes identify them within a Switch.
- IVR Ports—Their unique port numbers identify them within an IVR.

The way you name objects in your environment is important. Consistent and sensible naming conventions make your configuration environment easier to understand and faster to browse, leading to a more maintainable and usable configuration.

> **Important**
>
> Although Genesys Administrator Extension supports the full character set in object names, the use of certain characters can cause problems in the behavior of other Genesys applications. Therefore, avoid spaces, dashes, periods, or special characters in object names. Consider using underscores where you might normally use spaces or dashes.

The names you set for some types of objects must match the names of the entities that those objects represent elsewhere in an environment. For example, the names of Hosts must match the names given to the computers they represent in the data network environment.

State Enabled Property

If checked, indicates that the entity represented by an object is in regular operating condition and

can be used without any restrictions. If not checked, indicates that the entity represented by an object is being used in a non-production environment. Customer interactions cannot be directed to this target, even if operating information indicates that this object is available.

Disabling a folder or an object that is a parent to other objects also disables all objects within the folder or all child objects of that parent object.

For example:

- Disabling a Switch disables all DNs and Agent Logins defined within this Switch.
- Disabling an Agent Group folder disables all Agent Groups configured within this folder.

However, if you disable a group of objects (for example, an Agent Group), the individual members of this group (in this example, Agents) remain enabled.

Options Tab

> **Important**
>
> Application and Application Template objects have an additional tab, **Application Options**, to set configuration options specific to these objects. These options are set, updated, or deleted in the same manner as regular options.

To view the options for an object, select an object and click the **Options** tab. Configuration options are listed in their sections, and you can expand or collapse a section to show or hide the options in the section. By default, all sections are collapsed when the **Options** (or **Application Options**) tab is opened, but you can click **Expand All** to expand (or collapse) all sections.

The particular section is also listed for each option in the Name column and in the Section column. This is particularly helpful in those cases where there are more options in one section than can be displayed on a single screen, in that you can never lose track of the section in which an option resides.

You can manage (add, update, remove) options for that object, either one-by-one, or in bulk, using the import/export functionality.

One-by-one:

- Add an option **[+] Show steps**
  1. Select an object, and click the **Options** tab.
  2. Click **Add**.
  3. Enter information in the **Section**, **Key**, and **Value** fields.
  4. Click **OK**.
  5. Do one of the following:
     - Click **Save** to accept the changes and return to the object list.

    - Click **Apply** to accept the changes and remain in the **Options** tab.
    - Click **Cancel** to discard the changes.

- Update an option **[+] Show steps**
  1. Select an object, and click the **Options** tab.
  2. Select an option.
  3. Edit information in the **Section**, **Key**, and **Value** fields.
  4. Click **OK**.
  5. Perform one of the following actions:
     - Click **Save** to accept the changes and return to the object list.
     - Click **Apply** to accept the changes and remain in the **Options** tab.
     - Click **Cancel** to discard the changes.
- Delete an option **[+] Show steps**
  1. Select an object, and click the **Options** tab.
  2. Select an option.
  3. Click **Delete**.
  4. Perform one of the following actions:
     - Click **Save** to accept the changes and return to the object list.
     - Click **Apply** to accept the changes and remain in the **Options** tab.
     - Click **Cancel** to discard the changes.

In bulk:

- You can click **More** to import or export options. See Bulk Provisioning of Configuration Options for more information.

You can also click **More** to **Copy** selected application options and then **Paste** them in the options of any configuration object.

> ### Important
>
> - The **Section** and **Key** fields are required, and the values for these fields must be unique in the environment.
> - You can click **More** to import or export options. See the **Importing/Exporting Data** section in the Overview tab, above, for more information.

Permissions Tab

The **Permissions** tab lists the Access Groups and Users that have been configured explicitly with permissions for this object. When you are setting permissions, it is normally performed with the User(s) or Access Group(s) for which you want to grant access. This feature improves the manner in which permissions are set, and the scope is limited to managing permissions for a single database object.

For additional instructions about granting, modifying, and removing permissions, refer to the *Genesys Security Deployment Guide*.

Important

Some configuration objects, such as Tenants and Folders, are parent objects to one or more child objects. When you access the **Permissions** tab for these parent objects, you can use the following additional options to set permissions:

- **Propagate** check box—If **Propagate** is checked, the permission is propagated to every child object under this parent object. If **Propagate** is not checked, the permission is removed from every child object under this parent object, unless the permission has been modified in the child object.
- **Replace Recursively** button—If **Replace Recursively** is clicked, the permissions of every child object are removed and replaced with permissions from the parent object.

You can perform the following actions:

Changing Members

[+] Show procedure

1. Select an object, and click the **Permissions** tab.
2. Click **Add User** or **Add Access Group**.
3. A new window appears to enable you to select a User or Access Group. You can find Users or Access Groups by using one of the following methods:
   - By Hierarchy—Click **Show Hierarchy** to see a list of all Users or Access Groups in your environment, sorted by hierarchy.
   - By List—Click **Show List** to see a list of all Users or Access Groups in your environment.
   - By Quick Filter—Enter the name or partial name of the User or Access Group in the **Quick Filter** field.
4. Perform one of the following actions:
   - Click **Save** to accept the changes and return to the object list.
   - Click **Apply** to accept the changes and remain in the **Permissions** tab.
   - Click **Cancel** to discard the changes.

Changing Access Permissions

[+] Click here to reveal procedure

1. Select an object, and click the **Permissions** tab.
2. You can change any or all of the following options:

Property	Description
Create (C)	You can create objects of this type.
Read (R)	You can view details for this object.
Update (U)	You can change, or modify, this object.
Delete (D)	You can delete this object.
Execute (X)	You can deploy, start, stop, or otherwise activate this object.
Read Object Permissions (RP)	You can view access permissions granted for this object.
Change Object Permissions (CP)	You can change access permissions granted for this object.

3. Perform one of the following actions:
   - Click **Save** to accept the changes and return to the object list.
   - Click **Apply** to accept the changes and remain in the **Permissions** tab.
   - Click **Cancel** to discard the changes.

Removing Access Permissions

[+] Click here to reveal procedure

1. Select an object, and click the **Permissions** tab.
2. Select an Access Group or User for which to remove permissions.
3. Click **Remove**.
4. A dialog box appears to confirm deletion. Perform one of the following actions:
   - Click **Save** to accept the changes and return to the object list.
   - Click **Apply** to accept the changes and remain in the **Permissions** tab.
   - Click **Cancel** to discard the changes.

Dependencies Tab

The **Dependencies** tab displays a list of all objects that are dependent on this object, and by what property they are dependent.

For example, consider a scenario in which an Application object, **AppA**, is running on a Host object, **HostA**. **AppA** is dependent on **HostA** to function, so the **Dependencies** tab for **HostA** shows **AppA**

as a dependent object, with the property being **Host**.

For all Users and Agents, the **Dependencies** tab also lists the Roles to which they are assigned.

Click any object in the list to view the properties of that dependent object. You can then modify its properties or create another object of the same type.

Common Object Property Operations

The following are operations that apply to most object properties, regardless of type. Where these operations differ for particular types, the alternate method is specified in the type-specific section later in this Help file. Additional operations are also described in the type-specific sections.

Expand/Collapse All

If available, this option allows you to **Expand** or **Collapse** all of the objects in the current view.

Add/Remove

To add an object, click **Add** to browse for an object to add to the currently selected property tab. To remove an object(s), select it and click **Remove**.

Copy/Paste

If you have the required permissions, you can click **More** to access the **Copy** and **Paste** functions. After selecting and copying an object(s), you can paste it in any location that supports an association with the copied object(s).

Security Certificates

Genesys supports the optional use of the Transport Layer Security (TLS) protocol to secure data exchange between Genesys components. The TLS protocol is implemented using security certificates, which must be configured in the Host objects and the Application objects representing these components.

> **Important**
> Before configuring secure data exchange, make sure that certificates are installed on the host computers on which the Genesys components run, and that the certificate information is available to you.

For detailed information and instructions for deploying TLS, refer to the "Secure Connections" section of the *Genesys Security Deployment Guide*.

Read Only Mode and Emergency Mode

The Read Only Mode and the Emergency Mode features enable you to restrict users from making changes to the Configuration Database during a Configuration Server maintenance.

Read Only Mode

In this mode, no users can make changes to the Configuration Database.

Emergency Mode

In this mode, only users who are members of the Super Administrators group can make changes to the Configuration Database. Emergency Mode can be helpful, for example, where the Configuration Database itself must undergo some maintenance.

Enable Read Only or Emergency modes

Only members of the Super Administrators group can enable or disable these modes.

To enable Read Only Mode or Emergency Mode, do the following:

1. On the upper-right of the Configuration Manager view, click the **More** button beside the **Environment** button.
2. Select the required check box to enable the respective mode.

When the server is in Read Only or Emergency mode, a lock icon appears in the GAX header for:

- All currently logged in users
- All users logging in while GAX is in Read Only Mode or Emergency Mode

Hovering over the lock icon shows a tooltip with the currently active mode.

When either Read Only Mode or Emergency Mode is activated, Configuration Server notifies all the users working in the Configuration Layer that Read Only Mode is now active. An appropriate error message is displayed for any GAX user who attempts to update or save any configuration objects while the Configuration Server is in one of these two modes. Only Super Administrators can update the objects while the Configuration Server is in Emergency Mode.

> **Important**

- If the GAX browser instance that has switched the Configuration Layer to be in Read Only Mode is connected to Configuration Server, then you can switch back to normal operation mode only through the same browser.
- If the GAX browser terminates abnormally, or disconnects from the network:
  1. Run another instance of GAX.
  2. Log on to an account that is a member of the Super Administrators user group.
  3. Return the system to normal operation mode.

  In addition, If the host computer on which the GAX server is running shuts down or disconnects from the network, either let GAX come back on its own if auto-restart is on, or bring up the GAX Server application manually, as follows:

  1. From any browser on another computer, connect to the GAX URL.
  2. Log on to an account that is a member of the Super Administrators user group.
  3. Return the system to normal operation mode.

Provisioning Aids

Genesys Administrator Extension provides several provisioning aids to speed up the provisioning process, as follows:

- **Bulk Provisioning of Configuration Objects:** You can create, remove, or update multiple objects of some types by importing the information from a file prepared outside of GAX. Optionally, you can also download current information, for objects that you select, into a comma separated value (CSV) format that you can edit as required and then upload back into Genesys Administrator Extension.
- **Bulk Provisioning of Configuration Options:** You can create, remove, or update configuration options of all object types by importing the information from a file prepared outside of GAX. Optionally, you can also download current information, for objects that you select, into a comma separated value (CSV) format that you can edit as required and then upload it back into Genesys Administrator Extension.
- **Managing Configuration Options for Multiple Objects:** You can add, remove, or modify options and option values for a group of objects that you select.
- **Cloning Objects:** You can create close copies of an existing object, with some properties and options set to the same values as the original object.
- **Bulk Change Sets:** You can add or remove multiple Users at once. This is an older functionality; Genesys recommends that you use the bulk import/export functionalities described above.

Bulk Provisioning of Configuration Objects

To create or modify large numbers of objects, you can upload a comma-separated value (CSV) file containing new and/or changed object information. You enter or modify values in the appropriate columns for each object. When uploaded to GAX, the objects listed in the file are created or modified, based on the action to be taken as indicated in the Action column.

You can also use GAX to download (or export) information for selected objects. If you want, you can use this download to create a "template" for the data upload.

This import/export functionality is available for the following object types:

- DNs and DN Groups
- Places and Place Groups
- Persons (Users), including Agents
- Agent Groups
- Agent Logins

You can use GAX to download (or export) information for selected objects. If you want, you can use this download to create a "template" for the data upload.

This section describes how to export and import the files. Refer to the object type for the particular information that can be included in the file, and for examples of a prepared spreadsheet and file.

Exporting Data

GAX allows you to export data from existing data records into a spreadsheet called **download.csv**. Depending on what you are doing, you can modify the spreadsheet as required, save it as a **.csv** file, and upload it back into GAX. Or, you can export the data for just one object, remove the data (but not the column headers) from it, and use this "empty" template for present and future uploads of updated data.

To export data, do the following:.

[+] Show steps

1. In Configuration Manager, select those objects for which you want to export data.
2. Click **Export** in the **More** menu. The column picker window displays the required columns for the type of objects you have selected. The set of required columns differs between object types. You can change the order in which these columns appear in the output file, but you cannot remove them from the list.
3. From the other tables in the column picker window, select more fields as required, or clear those fields that you do not want exported.
4. Click **Export**. GAX generates and downloads a spreadsheet called **download.csv** with the data that

you selected for export.

The CSV File

The content of the CSV file differs depending on the object type that you are importing or exporting, as follows:

- DNs
- DN Groups
- Places
- Place Groups
- Persons
- Agent Groups
- Agent Login

Uploading a File

Before uploading the bulk updates, you must enter the data into a spreadsheet and save it as a CSV file. Keep in mind the following recommendations:

- If most of your updates are adding new objects, create an empty template and fill in the appropriate values.
- If you are primarily making changes to existing objects, export existing data and make the necessary additions and changes You can export the information for just those objects, saving you from filling in the mandatory information for them.

To upload the data into GAX, do the following:

[+] Show steps

1. Navigate to the list of objects that you are adding to or updating.
2. In the **More** menu, click **Import**.
3. Click **Select File** and, using the file browser, select your CSV file.
4. Click **Upload Spreadsheet**. GAX starts validating the file, and displays its progress. You can either click **Close** to close the window, or you can monitor the progress from here. Even if the window is closed, processing will continue.
   - If the **Spreadsheet is Valid**, click **Continue** to start the upload.
   - If the dialog box displays one or more errors, open your file in a new window and fix the errors. Then repeat this process starting at step 2.

5. GAX starts processing the records and displays the progress. If necessary, you can do either of the following at any time:
   - Click **Close Window**. Processing will continue.
   - Click **STOP Operation**, then click **Yes, STOP Operation** to confirm. When processing stops, you are returned to the list view.
6. If you did not stop the upload, GAX displays **Operation Concluded** when the processing of records is finished. It also displays a summary of results, namely the number of records that were successfully created and/or updated, and the number of records that were not updated or created because of an error. Click **Close Window** to go back to the main object list.

Bulk Provisioning of Configuration Options

To create or modify the configuration options for an option, you can upload a comma-separated value (CSV) file containing new and/or changed options and values. You enter or modify options and values in the appropriate columns object. When uploaded to GAX, the options listed in the file are created or modified, based on the action to be taken as indicated in the Action column.

You can also use GAX to download (or export) information for selected options. If you want, you can use this download to create a "template" for the data upload.

This import/export of configuration options functionality is available for all object types.

Exporting Options

GAX allows you to export selected options into a spreadsheet. You can modify the spreadsheet as required, save it as a **.csv** or **.cfg** file, and upload it back into GAX. Or, you can remove the data (but not the column headers) from it, and use this "empty" template for present and future uploads of configuration options.

To export options, do the following:

[+] Show steps

1. In Configuration Manager, open the Options tab of the object from which you want to export options.
2. Select the sections and options to be exported.
3. Click **Export** in the **More** menu located above the option list in the right corner.
4. In the **Export Options** dialog box, select the format of the output file, either CFG or CSV, and click **Export**.
   The output file is created and downloaded to your browser, with a filename in the format
   <object type>_annex_<object DBID>.csv or cfg
   For example:
   CfgPerson_annex_6378.cfg or **CfgPerson_annex_6378.cfg**

Uploading a File

Before uploading bulk updates, you must enter the data into a spreadsheet and save it as a CSV file. Keep in mind the following recommendations:

- If most of your updates are adding new options to the object, create an empty template and fill in the appropriate values.
- If you are primarily making changes to existing options, export only the options that you are changing,

and make the changes.

To upload the data into GAX, do the following:

[+] Show steps

1. In Configuration Manager, open the **Options** tab of the object into which you want to upload the options.
2. Click **Import** in the **More** menu located above the option list in the right corner.
3. In the **Import Objects** dialog box:
   a. Click **Choose File** and select the .csv or .cfg file with your changes.
   b. Select **Overwrite existing options** if you are sure that your file contains the accurate and most up-to-date current value for any options that may already exist in the object. Otherwise, leave it blank.
   c. Click **Upload**.
4. When the records have been processed, the **Operation Concluded** dialog box is displayed, showing a summary of the results. Click **Close** to return to the **Options** tab.

Source File

GAX uses **.csv** (comma separated value) and **.cfg** files for the import and export of configuration options. Both formats support only the import and export of string options. Other types of configuration options are ignored and not imported or exported. All strings in this file must be encoded in UTF-8.

> **Important**
> The contents of the file relates to only one object.

CSV Files

In a CSV source file, each line represents a single configuration option. The same option can appear in the source file only once. If the configuration options section does not already exist in the object's configuration, it is created. The unique identifier of the option in the scope of the source file is the combination of the `Section` and Key fields. There are three columns in the file—one each for the configuration option section, the name of the option (Key), and the option value, named by the entries in the first row of the file—Section, Key, and Value. The order of the columns is not important. A comma is inserted after each column entry. The source file contains the following information for each option: **[+] Show properties**

Name	Type	Mandatory	Description
Section	String	Yes	The name of the configuration file.
Key	String	Yes	The name of the option
Value	String	No	The new value of the option.

CFG Files

In a CFG file, each section and option appears on a separate line, with section names in square brackets. Each section is followed by a list of options in that section, with the appropriate values, such as:

```
[section_name1]
option-name1=option_value2
...
option_nameN=option_valueN

[section_name2]
option-nameN+1=option_valueN+1
...
```

Example

The following data is to be uploaded to GAX to add two new options for an existing User object:

[+] Show data

Section	Key	Value
gaxproperties	datemodified	1478163902397
htcc	roles	Agent

The CSV file for this would look like this:

```
Section,Key,Value
gaxproperties,datemodified,1478163902397
htcc,roles,Agent
```

Exported from GAX as a CFG file, the same information would look like this:

```
[gaxproperties]
datemodified=1478163902397
[htcc]
roles=Agent
```

Managing Configuration Options for Multiple Objects

GAX enables you to manage configuration options for multiple configuration objects at the same time. In other words, you can add, remove, or modify option sections, names, and values for objects that you select. This functionality saves you having to individually select each object in a set of objects that require the same modifications and/or need to be added or removed. This impact is multiplied if you have to make the same option changes to a group of objects.

This functionality applies to all configuration objects.

> **Important**
>
> - You can only use this feature to manage options for Agents in Configuration Manager by selecting them as **Accounts** > **Persons** (Users).
> - Configuration options are case-sensitive.

To use this functionality, do the following:

1. Open **Configuration Manager** in GAX and select the object type for which you want to manage options.
2. Select the objects for which you want to manage objects by selecting the checkbox next to the object name, navigating to the folder where they are located, if necessary.

   > **Tip**
   >
   > To make it easier, start in the folder that contains the most objects for which you are changing objects. You can select ones from other folders later.

3. Select **Manage Options** in the **More** menu. The **Manage Options** window opens. This window is where you specify any option changes that you want to make to the objects, as described in the following steps.
4. On the **Select** tab, use the **Add** and **Remove** buttons to fine-tune the list of objects for which you will manage their options.
5. On the **Update**, **Remove**, and **Add** tabs, use the **Add**, **Edit**, and **Remove** buttons to create a list of options in each tab that you want to modify for, remove from, and add to (respectively) the objects that you have selected (they are listed in the the **Select** tab). Note the following:
   - Changes specified in the **Update** tab are applied only against existing options.
   - The **Remove** tab is not concerned with an option value, since the option will be removed regardless

of value.

6. After you have finished listing affected options in the three tabs, the **Execute** tab displays each selected object with the changes that are to be applied to its options. Review the information, and do one of the following:
   - If the information is correct, click **Execute** to apply the changes. When complete, the tab will display the status of the operation and the number of objects changed.
   - If the information is not correct, click **Back** to make any changes.

Managing Connections for Multiple Applications

GAX enables you to manage connections for multiple applications at the same time. This functionality saves you having to individually select each application that requires the same modifications to existing or bulk-added connections.

> **Important**
>
> This functionality applies to daemon (server) applications only.

To use this functionality, do the following:

- Open **Configuration Manager** in GAX and select the server application(s) for which you want to manage connections.
- Select **Manage Connections** in the **More** menu. The **Manage Connections** window opens. This window is where you specify any option changes that you want to make to the connections, as described in the following steps.
- On the **Select** tab, use the **Add** and **Remove** buttons to fine-tune the list of applications for which you will manage their connections.
- On the **Update**, **Remove**, and **Add** tabs, use the **Add**, **Edit**, and **Remove** buttons to create a list of connections in each tab that you want to modify for, remove from, and add to (respectively) the applications that you have selected (they are listed in the the **Select** tab). Note the following:
  - Changes specified in the **Update** tab are applied only against existing connections.
  - The **Remove** tab is not concerned with a value, since the connection will be removed regardless of value.
- After you have finished listing affected connections in the three tabs, the **Execute** tab displays each selected application with the changes that are to be applied to its connections. Review the information, and do one of the following:
  - If the information is correct, click **Execute** to apply the changes. When complete, the tab will display the status of the operation and the number of applications changed.
  - If the information is not correct, click **Back** to make any changes.

Cloning

When setting up configuration objects, such as DNs, users, places, and so on, that share some properties, Genesys Administrator Extension enables you to *clone* an existing object. Configuration options of the original object are also included in the clone operation. That is, you create close copies of the existing object, with some of the properties and all options set to the same value as the original object. You only need to enter or update values in the fields.

However, you might want to block some configuration options from being cloned. For example, you may not want to clone the **[provisioning_flags]** section to a new object's properties. Starting in release 8.5.240, you can specify the configuration option sections that you do not want cloned by setting the **[com].exclude_clone** option to the configuration option section name (or comma-separated list of section names, if more than one) in the **Application Options** tab of the GAX Application object. This setting applies to all objects configured in GAX that have the same section name, not just to the section of the object that you wanted to block.

Bulk Change Sets

Genesys Administrator Extension allows you to perform bulk changes to users. For example, you can create a Bulk Change Set to add or remove multiple users from your system in one action, or to add or remove multiple skills, or both.

Starting in release 8.5.250, the Bulk Change Sets feature is not available in GAX by default. Instead, Genesys recommends that you use the other Bulk Provisioning features for User (Person) objects, including Agents, and Agent Group objects. However, if you still want to use Bulk Change Sets, enable it by setting **enable_bulk_change_sets=true** in the **[general]** section of the **Options** tab of the GAX Application object. It will appear in the **Administration** menu.

Display Options

The **Bulk Change Sets** panel lists all the Bulk Change Sets in your environment that either have not been executed yet or have failed during execution. To see a list of successful Bulk Change Sets, see the **Completed Bulk Changes** panel.

Configuration Object Management respects tenancy permission settings. You can access only those objects that you have been granted permission to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the **Tenant Filter** button to open the **Tenant filter** panel. In this panel, click the check box beside each tenants that you want to select. Use the **Quick Filter** field in this panel to filter the tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

Details

The **Bulk Change Sets** list displays the following information:

- **Change Set Name**—The name of the Bulk Change Set.
- **Creator**—The name of the user that created the Bulk Change Set.
- **Creation Date**—The date on which the Bulk Change Set was created.
- **Last Modified Date**—The date on which the Bulk Change Set was last modified.
- **Change Set Status**—This can be one of the following:
  - **Empty**—No data has yet been entered in the Bulk Change Set.
  - **Incomplete**—Only partial data has been entered in the Bulk Change Set.
  - **Ready to Execute**—The Bulk Change Set is ready to be executed.

- **Execution**—This can be one of the following:
  - **Not Executed**—The Bulk Change Set has not been executed yet.
  - **Completed**—The Bulk Change Set has been executed.
  - **Failed**—The execution of the Bulk Change Set failed.
- **Progress**—During execution, this field displays a progress bar for the Bulk Change Set.
- **Executed by Tenant**—Indicates which tenant last executed the Bulk Change Set.
- **Executed by User**—Indicates which user last executed the Bulk Change Set.
- **Previously Executed Date**—Indicates the date and time at which the Bulk Change Set was last executed.

Click a Bulk Change Set in the list to view more information about the item. The following fields are displayed:

- **Change Set Name**—The name of the Bulk Change Set
- **Deletions**—The objects that will be deleted by the Bulk Change Set
- **Additions**—The objects that will be added by the Bulk Change Set
- **Updates**—The objects that will be updated by the Bulk Change Set

> **Important**
>
> A Solution Definition file is created when a Bulk Change Set is executed. See the **Completed Bulk Changes** panel for instructions on how to download the Solution Definition file.

Procedures

You can perform the following actions from the **Bulk Change Set** panels:

Creating Bulk Change Sets

To create a Bulk Change Set, do the following:

[+] Show steps

1. In the **Bulk Change Sets** panel, click **+**.
2. Enter information in the following fields:
   - **Change Set Name**—The name of the Bulk Change Set.

> **Important**
>
> The **Change Set Name** field must be unique in the environment.

- **Deletions**—Enter any Configuration Object that is to be deleted with the Bulk Change Set. If there are deletions, perform the following actions. Otherwise, move on to the next step.
  a. Click **Add**. The **New Deletion Item** panel appears to the right.
  b. Click **Browse**. A list of Configuration Objects appears to the right.
  c. Objects that appear in the list are determined by the currently selected category. Click the drop-down menu at the top of the panel to change the category type.
  d. You can use the **Quick Filter** or **Tenant Filter** field to find specific objects. Click the checkbox beside an object to add the object to the Deletions list.
  e. The name of the object appears in the **New Deletion Item** panel. Click **OK** to add it to the Deletions list.
  f. Repeat the steps in this list to add more objects to the Deletions list.
- **Additions**—Enter any Configuration Object that is to be added with the Bulk Change Set. If there are additions, perform the following actions. Otherwise, move on to the next step.
  a. Click **Add**. A new panel appears to the right.
  b. Click **Browse**. A list of Configuration Objects appears to the right.
  c. Select an object type in the **Type** drop-down menu.
  d. Click **Browse** to select an object to use as a template. A panel opens to the right. Click the checkbox beside an object to select it.

> **Important**
>
> When an object is used as a template, all aspects of the template object are used for the Addition objects, including connections and permissions.

  e. Click **Next**.
  f. In the **Number to Create** field, enter the number of objects to create with the template. The value must be an integer between 1 and 100.
  g. In the **CSV File** field, perform the following actions:
    - Click **Choose File** to select a CSV file from which to acquire the new data.
    - In the window that opens, navigate to the location in which the CSV file is stored. Select the CSV file to use.

> **Important**
>
> The following is an example of an acceptable CSV file format for creating User (Person) objects.

> Only the **employeeid** and **username** fields are mandatory. All other fields are optional and can be omitted, in which case GAX provides default values that are copied from the template object.
>
> **employeeid, folderid, tenantdbid, state, lastname, firstname, password, username, skilllevels**
>
> **bulkuser1,105,1, CFGEnabled, Tamblyn, Ericm, password, bulkuser1, "{skilldbid:102, level:10},{skilldbid:106, level:6}"**
>
> **bulkuser2,106,2, CFGEnabled, Tamblyn, Ericm, password, bulkuser1, "{skilldbid:102, level:10},{skilldbid:107, level:7}"**

- Click **Open**.

h. Click **Finish**.

- **Updates**—Enter any update that is to be performed on Configuration Objects with the Bulk Change Set. If there are updates, perform the following actions. Otherwise, move on to the next step.
  a. Click **Add**. The **New Update Item** panel appears to the right.
  b. Click **Browse**. A list of Configuration Objects appears to the right.
  c. Objects that appear in the list are determined by the currently selected category. Click the drop-down menu at the top of the panel to change the category type.
  d. You can use the **Quick Filter** or **Tenant Filter** field to find specific objects. Click the check box beside an object to add it to the Updates list.
  e. The name of the object appears in the **New Update Item** panel. Click **OK** to add it to the Update list.
  f. Repeat the steps in this list to add more objects to the Update list.

3. In the Bulk Change Set creation panel, you can reorder the objects within the **Deletions**, **Additions**, or **Updates** lists.

> **Important**
>
> Bulk Change Set actions are executed in the following order : Deletions, Additions, and then Updates.

4. Click **Save** to save the Bulk Change Set.

> **Important**
>
> This action does not execute the Bulk Change Set. To execute the Bulk Change set, follow the instructions for executing a Bulk Change Set.

Deleting Bulk Change Sets

To delete a bulk change step, do the following:

[+] Show steps

1. Click the check box beside each Bulk Change Set that is to be deleted.
2. Click **Delete**. A dialog box displays to confirm the action.
3. Click **OK** to continue, or **Cancel** to discard the action.

Executing Bulk Change Sets

To execute a buck change set, do the following:

[+] Show steps

1. Select a Bulk Change Set in the **Bulk Change Sets** list. A new panel with more information about the Bulk Change Set opens to the right.
2. You can choose to validate the Bulk Change Set before execution. Click **Validate** to ensure that the Bulk Change Set is ready to be executed.

> **Important**
>
> The **Validate** button is useful in determining whether the Bulk Change Set is ready to be executed or whether it is dependent on other Bulk Change Sets to be executed first. For example: Some Additions depend on other objects to be added. You might want to update several Agents with a new Skill. However, the Skill must be created first, before the Agents can be updated. In this scenario, clicking **Validate** will verify that the Skill has been created.

3. Click **Execute** to execute the Bulk Change Set. You can view the status of the Bulk Change Set in the Completed Bulk Changes panel.

> **Important**
>
> A Solution Definition file is created when a Bulk Change Set is executed. See the Completed Bulk Changes panel for instructions on how to download the Solution Definition file.

Completed Bulk Changes

The **Completed Bulk Changes** panel lists the successfully executed bulk changes in your environment.

The **Completed Bulk Changes** list displays the following information:

- **Change Set Name**—The name of the Bulk Change Set

- **Creation Date**—The date on which the Bulk Change Set was created
- **Executed by Tenant**—Indicates which Tenant last executed the Bulk Change Set
- **Executed by User**—Indicates which user last executed the Bulk Change Set
- **Started**—Indicates the date and time at which the execution of the Bulk Change Set was started
- **Ended**—Indicates the date and time at which the execution of the Bulk Change Set was completed

To delete records of Bulk Change Sets, click the check box beside each Bulk Change Set that is to be deleted, and then click **Delete**.

> **Important**
>
> This action does not delete the Bulk Change Set; it deletes the record of the Bulk Change Set.

Click a Bulk Change Set in the list to view more information about the item. The following fields are displayed:

- **Change Set Name**—The name of the Bulk Change Set
- **Deletions**—The objects that were deleted by the Bulk Change Set
- **Additions**—The objects that were added by the Bulk Change Set
- **Updates**—The objects that were updated by the Bulk Change Set

Click **Export** to download the solution definition file that was used during execution of the Bulk Change Set.

Click **Delete** to delete the record of the Bulk Change Set.

> **Important**
>
> This action does not delete the Bulk Change Set; it deletes the record of the Bulk Change Set.

Limitations

The Bulk Change Set functionality in GAX does not support the following scenarios:

Bulk Change Set creates new objects that also have circular dependencies

Example:

1. A user creates a Bulk Change Set and adds a new agent and a new skill to the Additions section.

2. The user saves the Bulk Change Set.
3. The user assigns the new skill to the new agent, but also gives the new agent access permissions for the new skill.

This scenario creates circular dependencies between the new objects, and the execution of the Bulk Change Set fails.

Solution:

- Execute the Bulk Change Set before assigning dependencies between objects.

Bulk Change Set references a new object before the Bulk Change Set is saved

Example:

1. A user creates a Bulk Change Set and adds a new agent and a new skill to the Additions section.
2. The user does not save the Bulk Change Set and attempts to assign the new skill to the new agent.
3. The user cannot select the new objects until the Bulk Change Set is saved.

Solution:

- Save the Bulk Change Set before referencing the new object.

Searching for Configuration Objects

You can search for one or more specific objects in Genesys Administrator Extension. Start defining the search criteria by clicking **Search** in the top right corner of the Configuration Manager home page. You can search for an object by specifying **Name**, **Type**, **State [enabled/disabled]**, and/or **Tenant**. The search can be case-sensitive or case-insensitive.

You can use Advanced Search to search for objects by specifying additional criteria. For example, you could use Advanced Search to search for a Person object by adding criteria such as **Is Agent**, **First Name**, **Last Name**, **Employee Id**, **Switch**, **Skill**, **Skill Level**, **Agent Login**, or **Agent Group**. Search results appear beneath the criteria, including the path to each object in your configuration.

> ### Warning
> The Search facility ignores any restrictions placed by Roles, meaning that a user can view any object regardless of what Roles they have been assigned. Therefore, in addition to Roles, it is imperative that you also use permissions to prevent a user seeing objects for which they have no Role privileges.

Searching for an Object

To search for an object:

1. Click **Configuration** in the GAX Header, and click **Search** in the upper-right corner.
2. Enter the search criteria in the appropriate fields, noting the following:
   - Only **Type** is required, but specifying other criteria, if known, will speed up your search and reduce the number of records in the Results.
   - By default, the search is case-insensitive.
   - In text boxes (such as **Name**), you need to enter only the first few characters of the required text. For example, to search for the Configuration Server object named **confserv**, enter `conf`. The search results will list all objects with names starting with "conf" (and "Conf", if **Case Sensitive** is not selected), including **confserv**.
   - Wildcards such as `!` and `*` are supported.
3. (Optional) Select **Case Sensitive** to make the search case-sensitive.
4. (Optional) Click **Advanced Search** to provide additional values for search criteria.
5. Click **Search**.

> **Important**
> You can perform only one search at a time. The results of one search clears the results and filter criteria of the previous search.

The **Search Results** section displays the same metrics as for other lists in the GAX. In this section, you can:

- Select any or all of the objects for further action.
- Sort the list by any column.
- Use the **Column Picker** to define what fields are displayed and not displayed.
- **Delete**, **Clone**, **Move**, **Enable**, or **Disable** selected objects.
- Further refine the list using the **Quick Filter**.

> **Tip**
> By default, the Quick Filter starts displaying results while you are typing. If you prefer to have the filtering start only when you hit **Enter**, go to the **Application Options** tab of the GAX Application object and add an option to the **general** section called **quick_filter_only_on_enter** and set its value as **true**.

Clicking on any object in the results opens the properties dialog box for that object, where you can modify or delete this object, or add new objects to your configuration.

Clearing the Search Results

To clear the results of a search, do one of the following:

- Click **Clear**. This clears the search criteria and and results.
- Perform another search. The results of one search clears the results of the previous search.

Accounts

The Accounts section of Configuration Manager enables you to configure the following objects:

- Access Groups
- Agent Groups
- Users (Persons)
- Roles
- Skills
- Capacity Rules

Video

Genesys Administrator Extension: Creating skills, agent groups, and agents

Link to video

Access Groups

Access Groups are groups of Users who need to have the same set of permissions for Configuration Database objects.

In many cases, users fall into a small number of categories with similar access needs. A team of agents all performing the same tasks often has identical access needs. Two or three people responsible for maintaining a specific site of the contact center may also have identical access needs. You can greatly simplify access control by adding individuals to Access Groups and then setting permissions for those groups.

> ### Important
>
> - The `default` user account is not related to Access Groups and, therefore, does not appear as a member of any Access Group.
> - For detailed instructions about managing Roles assigned to Access Groups, refer to the *Genesys Security Deployment Guide*.

Viewing Access Groups

The **Access Groups** list shows the Access Groups that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
>
> Access Groups that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

To select or de-select multiple objects at once, click **Select**.

Working With Access Groups

To create a new Access Group object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Important**
>
> When you delete an Access Group, only the Access Group object itself is removed from the Configuration Database. Its member objects—Access Group and User objects—are not deleted.

Otherwise, select the check box beside one or more objects and click **More** to perform the following tasks:

- **Clone**—Copy an Access Group.
- **Move To**—Move an Access Group to another hierarchical structure.
- Enable or disable Access Groups
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of an Access Group to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Access Group Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Access Group. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the `Tenant Directory` field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and

can be used without any restrictions.

3. For each User to be added to this Group:
   a. Click the **Members** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To add an existing User to the Group, select him or her from the list of Users.
      - To add a new User to the Group, click **+** to create the User in this folder and then select him or her from the list.
4. After you have finished creating the Access Group, do one of the following:
   - Click **Save** to accept the changes and return to the list of Access Groups.
   - Click **Apply** to accept the changes and return to the **General** tab of this Access Group.
   - Click **Cancel** to discard the changes.

Agent Groups

An Agent Group is a logical grouping of agents. Agent Groups are typically set up to provide particular sets of contact-center services.

Viewing Agent Groups

The **Agent Groups** list shows the Agent Groups that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
> Agent Groups that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

To select or de-select multiple objects at once, click **Select**.

Working with Agent Groups

To create a new Agent Group object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**.

To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> ### Important
> When you delete an Agent Group, only the Agent Group object itself is removed from the Configuration Database. Its member Agent objects are not deleted.

Otherwise, select the check box beside one or more objects and click **More** to perform the following tasks:

- **Clone**—Copy an Agent Group.
- **Move To**—Move an Agent Group to another hierarchical structure.
- Enable or disable Agent Groups
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Creating Agent Group Objects

To create an Agent Group object, do the following:

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Agent Group. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment). You cannot change this value as long as this Agent Group contains at least one User.
   - **Capacity Table**—This field applies only for the Enterprise Routing Solution. It is the Capacity Table associated with this Agent Group. Refer to Enterprise Routing Solution documentation for more information.
   - **Quota Table**—This field applies only for the Enterprise Routing Solution. It is the Quota Table associated with this Agent Group. Refer to Enterprise Routing Solution documentation for more information.
   - **Cost Contract**—The Cost Contract associated with this Agent Group.
   - **Site**—The Site containing this Cost Contract.
   - **Script**—Enter a valid expression on the **Script** tab to define the group as a Virtual Agent Group. The expression must be in Virtual Group Script Language (VGSL) and must define at least one skill (with optionally, a skill level) in the following format:
     `Skill("SkillName")>SkillLevel`
     Example
     `Skill("Spanish")>5`
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the `Tenant Directory` field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. To add a Supervisor to this Group:
   a. Click the **Supervisors** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To add an existing User to this Group as Supervisor, select him or her from the list of Users.
      - To add a new User to this Group as Supervisor, click **+** to create the User in this folder and then select him or her from the list.

4. For each Agent to be added to this Group:
   a. Click the **Agents** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To add an existing Agent to this Group, select him or her from the list of Agents.
      - To add a new Agent to this Group, click **+** to create the Agent in this folder and then select him or her from the list.
5. The **Origination DNs** tab lists DNs from which calls can be routed or diverted to this Agent Group.

> **Important**
>
> Only DNs of the following types can be included in this list: `Routing Point`, `External Routing Point`, `Service Number`, `Routing Queue`, `ACD Queue`, `Virtual Queue`, or `Virtual Routing Point`.

For each Origination DN to be added to the list of Origination DNs for this Group:

   a. Click the **Origination DNs** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To add an existing DN to the list of Origination DNs for this Group, select it from the list of DNs.
      - To add a new DN to the list of Origination DNs for this Group, click **+** to create the DN in this folder and then select it from the list.
6. After you have finished creating the Agent Group, do one of the following:
   - Click **Save** to accept the changes and return to the list of Agent Groups.
   - Click **Apply** to accept the changes and return to the **General** tab of this Agent Group.
   - Click **Cancel** to discard the changes.

CSV File for Importing and Exporting

You can use the Bulk Import/Export functionality to import Agent Groups from, and export Agent Groups to, a comma-separated value (CSV), file. The import file used for importing and the export file created by exporting data are fully compatible, and a single file can be used for both importing and exporting. Or, you can create the import file yourself, using the general CSV information in this Help file, and the object-specific information contained in this section.

Fields of the CSV File

The source file is a text file in a comma-separated (CSV) format, with an extension of **.csv**.

In the source file each line represents a single Agent Group. The same Agent Group can appear in the source file only once. The unique identifier of the Agent Group in the scope of the source file is the Agent Group Name field.

The columns of the file are the properties of an Agent Group. The first row in the file has column names to identify the fields. The order of the columns is not important. A comma is inserted after each column header or value, or if the column does not have a value, immediately after the previous comma. Any non-mandatory column can be omitted from the source file, depending on user preference and/or the purpose of the file.

The source file contains the following properties for each Agent Group:

Name	Type	Mandatory	Description
Action	ADD, UPDATE, DELETE	Yes	Specifies the action to be taken with this Agent Group data, either create a new Agent Group (ADD) or modify the existing Agent Group (UPDATE) or delete an Agent Group. This column is added automatically by GAX when a file is exported, with a value of UPDATE for all records in it. If you create the source file from scratch, you must add this column manually. In either case, this field is mandatory, and you must provide a value for each record.
Name	String	Yes	Name of Agent Group.
Enabled	String	No	Whether this DN is enabled (`Y`) or not (`N`).

Relational Columns

In addition to the properties and folders in the table above, each row may contain relations between this Agent Group and other configuration objects, in particular Users who are Agents (`Is Agent=Y`). Every instance of an Agent will have a separate column in the source file. For example, if there are 10 Agents, there will be 10 additional columns in the source file, each column representing each Agent configured. All relational columns are optional.

Each header for a relational column consists of the object type and the object name, which will form a unique column name. So, for example, there cannot be two Agent Groups that have the same name, but an Agent object may have the same name as an Agent Group.

Naming and value rules of relational columns are given in the following table:

Relational Columns

Type	Column Name	Valid Values	Description
Agent	Agent:<agent name>	Y – Add this Agent to this Agent Group `N` – Remove this Agent from this Agent Group <empty> - No action	The name of the Agent to be added or removed to this Agent Group.

Example

The following data is to be uploaded to GAX to modify three Agent Groups:

Action	Name	Enabled	Agent:doej	Agent:jonesj	Agent:smiths
UPDATE	Gold_Agents	Y	Y	Y	N
UPDATE	Silver_Agents	Y	N		N
UPDATE	Bronze_Agents	Y		Y	Y

The contents of the CSV file for this data looks like this:

```
Action,Name,Enabled,Agent:doej,Agent:jonesj,Agent:smiths
UPDATE,Gold_Agents,Y,Y,Y,N
UPDATE,Silver_Agents,Y,N,,N
UPDATE,Bronze_Agents,Y,,Y,Y
```

Virtual Agent Groups

A Virtual Agent Group is similar to an Agent Group except that a Virtual Agent Group has no permanent members. Instead, an Agent becomes a member of a Virtual Agent Group if that Agent meets the criteria specified by the script. Agent membership in a Virtual Agent Group can change dynamically based on changes in the Virtual Agent Group criteria or changes in the object properties of the Agent.

When you click a Virtual Agent Group in Genesys Administrator Extension, you see its current member Agents.

> ### Important
> Although you can create and configure them using Genesys Administrator Extension, Virtual Agent Groups are used primarily by Reporting applications. For more information about Virtual Agent Groups, refer to the latest version of the *Framework Stat Server User's Guide*.

> ### Warning
> If Genesys Administrator Extension finds Virtual Agent Groups (converted from an earlier installation) that contain illegal script expressions or include permanent members, Genesys Administrator Extension will display an error message. To preserve correct functionality of the Virtual Agent Groups, you must address the problem manually by either correcting the error or converting the Virtual Agent Group to a non-virtual Agent Group by removing the expression from the configuration option script.

Users (Persons)

Users are the contact-center personnel, including Agents, who need access to Genesys applications. Agents are Users who handle customer interactions directly.

Genesys Framework requires that every User who needs such access be registered in the Configuration Database with an appropriate set of permissions.

> **Important**
>
> To run a particular application, a User must have Read and Execute permissions for the object that represents this application in the Configuration Database. New Users created in Genesys Administrator Extension receive the same set of default permissions and access privileges that Configuration Server grants.

Managing Users vs. Managing Agents

You can create agents in either the Persons window (as described here) or in the Agents window. The result is the same—an agent of type Person is created and stored in the Configuration Database, and you can manage that agent in the Persons window or Agents window.

If at any time you want to work only with agents, you can select Agents in the GAX menu bar. This shows you a list of only the agents in your contact center, filtering out all non-agent users and giving you a shorter list to work with.

> **Important**
>
> If the Agents option does not appear in the GAX Header, change it in System Preferences by selecting the Agent Management category and changing the Mode from **Hidden** to **Premise**. See System Preferences for more information.

Viewing Users

The **Persons** list shows the Users that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

You can quickly distinguish between Users and Agents by looking at the icon to the left of the object name. Users that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column heading. Clicking it a second time reverses the sort order.

Click **Group By** to group objects by various criteria.

To select or de-select multiple objects at once, click **Select**.

Working with Users

To create a new User object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**.

To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a User.
- **Move To**—Move a User to another hierarchical structure.
- Enable or disable Users.

> ### Important
> When a User is either disabled or removed, Genesys Administrator Extension invalidates all sessions that are associated with this User. Upon the User's next action, he or she will be redirected to the login page.

- **Edit Skills**—Edit skills of one or more Users. When you select **Edit Skills** in the **More** menu, the **Edit_<n>_Agents** dialog box opens. This dialog box is where you can change the skills of the Users.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a User to view additional information about the object. You can also set options and permissions, and view dependencies.

Creating New Users

To create a new user, do the following:

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name that this User should use to log into the environment. You must specify a value for this property, and that value must be unique within the Configuration Database.
   - **Agent**—Indicates whether this User is an Agent. If checked, additional fields appear. Once you set this flag, you cannot change it.
   - **First Name**—The first name of this User.
   - **Last Name**—The last name of this User.
   - **E-mail Address**—The email address of this User.
   - **Employee ID**—A code of up to 64-characters that identifies this User within the contact-center staff. You must specify a value for this property and that value must be unique within the Configuration Database (in an enterprise environment), or within the Tenant (in a multi-tenant environment).
   - **Password**—A password no longer than 64-characters that this User must use to log in to the environment. You cannot view the existing password. When creating a new user, this field is always enabled. When editing an existing user, this field is enabled only if **Reset Password** is not selected.

     > **Important**
     >
     > Passwords can be subject to format rules. Refer to the *Genesys Security Deployment Guide* for more information.

   - **Confirm Password**—Confirmation of the password entered. When creating a new user, this field is always enabled. When editing an existing user, this field is enabled only if **Force Password Reset on Next Login** is not selected.

     > **Important**
     >
     > Do not copy-and-paste the value from the **Password** field. You must retype the password.

   - **Force Password Reset on Next Login**—A check-box that, if selected, prompts the user to enter a new password upon the next login.

     > **Important**
     >
     > The **Force Password Reset on Next Login** option displays only if Genesys Administrator Extension

> connects to Management Framework 8.1.1, or higher. See the *Genesys Security Deployment Guide* for more information about resetting passwords.

- **External ID**—This setting applies only if your environment is using external authentication, either LDAP or RADIUS. This may be the user name in the external authentication system. For LDAP, it might be a whole, or partial, LDAP URL corresponding to RFC 2255. For more information, refer to the *Framework External Authentication Reference Manual*.
- **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. If **Agent** is selected, enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from the following list:
   - **Default Place**—The Place assigned to this Agent, by default. This optional parameter applies to a limited number of configurations, in particular those where a real-time association between a Place and an Agent cannot be established through a telephony login procedure.
   - Capacity Rule—The name of the Script of type `Capacity Rule` that defines the ability of this Agent to handle multiple interactions. Refer to Reporting documentation for more information.
   - **Cost Contract**—The Cost Contract associated with this Agent.
   - **Site**—The Site containing this Cost Contract.
4. In the **Member Of** tab, click **Add** to add an Access Group.
5. In the **Ranks** tab, click **Add** to add a Rank.
6. Enter the following information in the pop-up window that displays on your screen:
   - **Application Type**—The type of Application to which a User needs access. Consult the manuals for a GUI application to see if this application is using Ranks to enable or block certain functions. If a manual does not contain any references to Ranks, this application does not use Ranks, and you do not need to specify the Person's Ranks with respect to this application.
   - **Application rank**—The Rank with respect to Applications of the specified type.
7. If **Agent** is selected, click **Apply** to display the following tabs:
   - In the **Skills** tab, click **Add** to add a Skill.
   - Enter the following information in the pop-up window that displays on your screen:
     - **Skill**—The Skill assigned to this Agent.
     - **Level**—The relative measure of the Agent's proficiency in this Skill.
   - In the **Agent Logins** tab, click **Add** to add an Agent Login.
   - Enter the following information in the pop-up window that displays on your screen:
     - **Agent Login**—The Agent Login code assigned to this Agent. You cannot assign an Agent Login to more than one Agent.
     - **Wrap-up Time**—Some switches do not support transfer of information about an agent's postcall work status through the CTI-link. However, when this operation is supported, consider specifying the wrapup time, in seconds, for the Agent Logins that belong to such switches. This

specification must match the corresponding switch setting.

8. Click **Save**.

> **Important**
>
> From 8.5.260.11, GAX now saves user preferences in the Person object by default. If the **[general] userpreference_in_transaction** GAX application option is set to `true`, then GAX saves user preferences in the Transaction object in the **Transactions/UserPreference** folder.
>
> In this case, GAX copies only the annex sections starting with the option **ga_preferences.**, from the Person annex to the Transaction annex.
>
> When GAX creates the Transaction object, GAX removes all access permissions (for users and access groups) to the Transaction object, except the default user and the current user.

> **Important**
>
> New Users do not automatically receive Read and Update permissions for their User object. You must manually provision these permissions to allow Users to save their user preferences in GUI-based programs, such as GAX or Workspace Desktop Edition (formerly known as Interaction Workspace).

CSV File for Importing and Exporting

You can use the Bulk Import/Export functionality to import Users from, and export Users to, a comma-separated value (CSV) file. The import file used for importing and the export file created by exporting data are fully compatible, and a single file can be used for both importing and exporting. Or, if you wish, you can create the import file yourself, using the general CSV information in this Help file, and the object-specific information contained in this section.

Fields in the CSV File

The source file is a text file in a comma-separated (CSV) format, with an extension of **.csv**.

In the source file, each line represents a single User. The same User can appear in the source file only once. The unique identifier of the User in the scope of the source file is the Employee ID field.

The columns in the file are the properties of a User and any other objects with which they might be associated. The first row in the file has column names to identify the fields. The order of the columns is not important. A comma is inserted after each column header or value, or if the column does not have a value, immediately after the previous comma. Any non-mandatory column can be omitted from the source file, depending on user preference and/or the purpose of the file.

The source file contains the following properties for each User:

> **Important**
> Field names are case-sensitive.

Name	Type	Mandatory	Description
Action	ADD, UPDATE, DELETE	Yes	Specifies the action to be taken with this User data, either create a new User (ADD) or modify the existing User (UPDATE) or delete a User (DELETE). This column is added automatically by GAX when a file is exported, with a value of UPDATE for all records in it. If you create the source file from scratch, you must add this column manually. In either case, this field is mandatory, and you must provide a value for each record.
First Name	String	Yes	User's first name.
Last Name	String	Yes	User's last name.
Username	String	Yes	Username of the User.
Employee ID	String	Yes	Unique ID assigned to this User.
Is Agent	String	Yes	Whether User is an Agent, either `Y` or `N`. Script functionality differs between an Agent and a non-Agent.
Password	String	No	Password to be used with username.
Password change	String	No	Whether this User must change their password at their next login (`Y`) or not (`N`).
External Id	String	No	A unique external ID for this User.
Email address	String	No	Email address of this User; normally it is the same as the `Username`.
Enabled	String	No	Whether this User is enabled, either `Y` or `N`.
Section | Option | Value	String	No	User options associated

Name	Type	Mandatory	Description
			with this User. **Note:** Any special characters in the key/value are escaped by using a back slash (\). For example: \,=\,\, where "," (comma) is the key and “,,” (comma,comma) is the value.
Capacity Rule	String	No	Applies only if Is Agent=Y. The default Capacity Rule with which this User is associated.
Cost Contract	String	No	Applies only if Is Agent=Y. The default Cost Contract with which this User is associated.
Site	String	No	The default Site with which this User is associated.
Default Place	String	No	Applies only if Is Agent=Y. The default Place with which this User is associated.

Relational Columns

In addition to the properties and folders in the table above, each row may contain relations between this User and other configuration objects, in particular **Access Groups**, **Agent Groups**, **Agent Logins**, **Application Ranks**, and **Skills**. Every instance of an Access Group, Agent Group, Agent Login, Application Rank, and Skill object will have a separate column in the source file. For example, if there are 10 Agent Groups, 1 Switch, 15 Skills and 4 Access Groups, there will be 30 additional columns in the source file, each column representing each configuration object. All relational columns are optional.

Each header for a relational column consists of the object type and the object name, which will form a unique column name. So, for example, there cannot be two Skills which have the same name, but a Skill object may have the same name as some Switch object.

Naming and value rules of relational columns are given in the following table:

Relational Columns

Type	Column Name	Valid Values	Description
Access Group	AccessG:<access group name>	Y – Add this User/Agent to this Access Group N – Remove this User/Agent from this Access Group	The name of the Access Group to which this User belongs. This User can belong to as many Access Groups as

		<empty> - No action	required, but only one Access Group can appear in each column. **Important** The Default Access Group specified in System Preferences does not apply when using bulk uploads, since the Access Group for the User is specified in the CSV file.
Agent Group	AgentG:<agent group name>	Y – Assign this User to this Agent Group N – Remove this User from this Agent Group <empty> - No action	Applies only if Is Agent=Y. The name of the Agent Group to which this User belongs. This User can belong to as many Agent Groups as required, but only one Agent Group can appear in each column.
Agent Login	AgentL:<switch name> / <agent login name>	<wrap-up time> – Assign this Agent Login to this User, with the stated wrap-up time. <empty> – No change. N – Remove this Agent Login from this User.	Applies only if Is Agent=Y. The Agent Login assigned to this User.
Application Rank	ApplicationR:<application name>	<rank> – Assign this Application type to this User with this Rank. Possible Ranks are Administrator, Designer, Super Administrator, Service Administrator, User, Unknown. <empty> - No action N – Remove this Rank from this User	The default Rank with respect to the given Application type.
Skill	Skill:<skill name>	<number> - Assign this Skill to this User with this Skill Level <empty> - No action N – Remove this Skill from this User	Applies only if Is Agent=Y. The proficiency of this User at the given Skill.

Example

The following data is to be uploaded to GAX to modify two new Users:

Action	FirstName	LastName	EmployeeID	Username	Is Agent	Enabled	Skill:Outgoing	Skill:Winback
UPDATE	John	Fraser	1234	JohnF	Y	Y	4	5
UPDATE	Susan	Smith	5757	SusanS	Y	Y	N	

The contents of the CSV file for this data looks like this:

```
Action,FirstName,LastName,EmployeeID,Username,Is Agent,Enabled,Skill:Outgoing,Skill:WinBack
UPDATE,John,Fraser,1234,JohnF,Y,Y,4,5
UPDATE,Susan,Smith,5757,SusanS,Y,Y,N,
```

Roles

Roles define what you can do in a given application. In Genesys Administrator Extension, roles and their privileges are controlled by the use of Role objects, which are assigned to Users (including Agents) and Access Groups. Roles are application-specific, and must be defined for each application that supports them.

In a hierarchical multi-Tenant configuration, only those Roles defined in the Environment Tenant can be used to allow Users to access all screens in Genesys Administrator Extension. Users cannot include Genesys Administrator Extension-specific privileges in Roles from other Tenants.

For more information about Roles, refer to the *Genesys Security Deployment Guide*. For a listing of Role Privileges for the Genesys Administrator Extension application, refer to Role Privileges in the *Genesys Administrator Extension Deployment Guide*.

Viewing Roles

The **Roles** list shows the Roles that are in your environment. It is sorted in a hierarchy by tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
> Roles that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

To select or de-select multiple objects at once, click **Select**.

Working with Roles

To create a new Role object, click **New**. To view or edit details of an existing object, click the name of

the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Role.
- **Move To**—Move a Role to another hierarchical structure.
- Enable or disable Roles.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Role to view additional information about the object. You can also set options and permissions.

Procedure: Creating Role Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of this Role. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Description**—A brief description of this Role.
   - **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. In the **Role Members** tab, click **Add Access Group** to add an Access Group, or **Add Person** to add a User.
4. In the **Assigned Privileges** tab, select role privileges to add to this Role object.
5. Click **Save**.

Skills

Skills are qualities or abilities that Agents possess and that affect the placement of each Agent in a contact center hierarchy. Common Skills include abilities in different languages, particular categories of product knowledge, or ability in particular types of sales.

Viewing Skills

The **Skills** list shows the Skills that are in your environment. It is sorted in a hierarchy by tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Skills that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

To select or de-select multiple objects at once, click **Select**.

Working with Skills

To create a new Skill object, click **New**.

To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. The Users listed in the **Dependencies** tab appear as link. When you click a **Username** link, the **<Person> Properties** window opens, where you can edit the properties of that particular User. In the **<Person> Properties** window, click **Back** in the **General** tab to return to the originated configuration object from where you navigated to this associated configuration object.

To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Important**
> When you delete a Skill, it is removed from the Configuration Database and from any Agent to which it is assigned. If you want to remove only the Skill from an Agent to which it is assigned, but leave it in the Configuration Database and available for assignment to another Agent, remove the Skill from the Agent.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Skill.
- **Move To**—Move a Skill to another hierarchical structure.
- Enable or disable Skills.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Skill to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Skill Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** button to select a value from a list:
   - **Name**—The name of this Skill. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Capacity Rules

The **Capacity Rules** window enables you to set Capacity Rules for various operations in your environment. For example, you may choose to set Capacity Rules for how many voice interactions or email interactions, or a combination of both, can be processed at one time.

Viewing Capacity Rules

The **Capacity Rules** list displays the Capacity Rules in your environment. The list is organized in a hierarchy, starting with Tenants, configuration units, sites, and folders.

> **Important**
> Capacity rules that are disabled will appear grayed out in the list.

This list respects tenancy permission settings. You can access only those objects that you have been granted permission to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click **Tenant Filter** to open the **Tenant Filter** window. In this window, click the check box beside each Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

Working with Capacity Rules

Click a Capacity Rule to view more details about the rule in a new panel that opens to the right. From this panel, you can also edit Access Control. You can perform the following actions:

Creating Capacity Rules

[+] Show Procedure

This short video demonstrates how to create Capacity Rules using GAX. Alternatively, you can refer to the procedure below the video.

Link to video

Procedure: Creating Capacity Rules

Steps

1. Click **New**.
2. Enter the following information:
   - **Capacity Rule Name**—The name of the Capacity Rule.

     > **Important**
     > The **Capacity Rule Name** field must be unique in the environment.

   - **Description**—A description of the function of the Capacity Rule.
   - **Tenant and Folder**—The Tenant and folder to which this Capacity Rule belongs. Click **Browse** to locate the folder in which the script is stored, or type the name of the folder in the Quick Filter field.

     > **Important**
     > The list of displayed folders is based on each Tenant's access settings.

   - **Media Types**—Click **New** to select which media types will be monitored by this Capacity Rule. For more information, see Media Types.
3. Click **Save**.

Media Types

[+] Show Procedure

You can add one or media types to Capacity Rules to specify how many instances of each media type are allowed simultaneously.

Procedure: Adding Media Types to Capacity Rules

Steps

1. Perform one of the following actions:
   - Click **New**, and create a new Capacity Rule.
   - Click an existing Capacity Rule in the **Capacity Rules** panel.
2. In the **Media Types** section, click **New** to add media types to the Capacity Rule. A new panel opens to the right.
3. In the new panel, click the **Media Type** drop-down menu to select a media type. A new section called **Conditions** displays.
4. Set the conditions for the media type.
5. Click **Save**.

Conditions

By default, the maximum value of the media type is 1. You can click the **[media type] exceeds 1** button to set a new maximum value. For example, if you select `Voice` as a media type, click **Voice exceeds 1** to open a new panel, and enter a new value in the **Maximum Capacity** field. Click **OK** to save the change.

You can also mix media types for the Capacity Rule. For example, you could set a Capacity Rule that allows one `Voice` interaction and one `Email` interaction (for a total of two simultaneous interactions). Alternately, you could set a Capacity Rule that allows one `Voice` or one `Email` interaction, but not both (for a total of one simultaneous interaction).

Procedure: Adding an **and** Condition to a Media Type

Steps

1. In the **Conditions** drop-down menu, click **and**. A new panel opens to the right that allows you to add a condition.
2. Click the **Media Type** drop-down menu, and select a media type.

3. Enter a value in the **Maximum Capacity** field.
4. Click **OK** to add the condition.

Procedure: Adding an **or** Condition to a Media Type

Steps

1. In the **Conditions** drop-down menu, click **or**. A new panel opens to the right that allows you to add a condition.
2. Click the **Media Type** drop-down menu, and select a media type.
3. Enter a value in the **Maximum Capacity** field.
4. Click **OK** to add the condition.

Validating Capacity Rules

[+] Show Procedure

When creating a new Capacity Rule or modifying an existing Capacity Rule, you can click **Validate** to verify whether the Capacity Rule is valid or not. This action ensures that the Capacity Rule is constructed properly and uses only media types that you can access.

For example, if you create a Capacity Rule that only specifies **voice** as a media type, but you use **callback** as part of a condition, GAX displays an error message after you click **Validate** that states you must add **callback** as a media type.

Otherwise, if the Capacity Rule is valid, GAX displays a confirmation message after you click **Validate**.

Procedure: Validating a Capacity Rule

Steps

1. Create a new Capacity Rule or modify an existing Capacity Rule.
2. Click **Validate**.
3. GAX displays one of the following messages:
   - A confirmation message that states the Capacity Rule is valid.
   - An error message that explains why the Capacity Rule is invalid.

Deleting Capacity Rules

[+] Show Procedure

There are multiple methods to delete a Capacity Rule. Choose a procedure below:

Procedure: Deleting a Single Capacity Rule

Steps

1. Select a Capacity Rule in the **Capacity Rules** list. More information about the Capacity Rule is displayed in a new panel to the right.
2. In the new panel, click **Delete**.
3. A dialog box displays to confirm the action:
   - Click **OK** to continue.
   - Click **Cancel** to discard the action.

Procedure: Deleting Multiple Capacity Rules

Steps

1. In the **Capacity Rules** list, click the check box of each Capacity Rule that is to be deleted.
2. Click **Bulk Change**, and select **Delete** from the pop-up list of options.
3. A dialog box displays to confirm the action:
   - Click **OK** to continue.
   - Click **Cancel** to discard the action.

Copying Capacity Rules

[+] Show Procedure

Procedure: Copying Capacity Rules

Steps

1. Select a Capacity Rule to copy. More information about the Capacity Rule is displayed in a new panel to the right.
2. In the new panel, click **Copy**. A new panel opens to the right.
3. Enter the following information:
   - **Capacity Rule Name**—The name of the Capacity Rule.

     > **Important**
     > The **Capacity Rule Name** field must be unique in the environment.

   - **Description**—A description of the Capacity Rule.
   - **Tenant and Folder**—The Tenant and folder to which this Capacity Rule belongs. Click **Browse** to locate the folder in which the script is stored, or type the name of the folder in the Quick Filter field.

> **Important**
> The list of displayed folders is based on each tenant's access settings.

- **Media Types**—Click **New** to select which media types will be monitored by this Capacity Rule. For more information, see Media Types.

4. Click **Save**.

Enabling or Disabling Capacity Rules

[+] Show Procedure

There are multiple methods to enable or disable a Capacity Rule. Choose a procedure below:

Procedure: Enabling or Disabling a Single Capacity Rule

Steps

1. Select a Capacity Rule. A new panel opens to the right.
2. In the new panel, perform one of the following actions:
   - If the Capacity Rule is currently enabled, click **Disable**.
   - If the Capacity Rule is currently disabled, click **Enable**.

Procedure: Enabling or Disabling Multiple Capacity Rules

Steps

1. In the **Capacity Rules** panel, select the check box beside each Capacity Rule that you want to enable or disable.
2. Click **Bulk Change**. A pop-up menu displays. Select **Enable** to enable the selected Capacity Rules or **Disable** to disable the selected Capacity Rules.
3. A dialog box displays to confirm the action:
   - Click **OK** to continue.
   - Click **Cancel** to discard the action.

Access Control

The **Access Control** panel lists the access groups and users that have been configured explicitly with permissions for this object. When you are setting permissions, it is normally performed with the user(s) or access group(s) for which you want to grant access. This feature improves the manner in which permissions are set, and the scope is limited to managing permissions for a single database object. For additional instructions about granting, modifying, and removing permissions, refer to the *Genesys Security Deployment Guide*. You can perform the following actions:

Creating Access Permissions

[+] Show Procedure

Procedure: Creating Access Permissions

Steps

1. Select an object.
2. Click **Related** and select **Access Control**. The **Access Control** panel opens.
3. Click **New**. A new panel opens to the right.
4. In the **Object Type** field, select the configuration object type to which this access permission applies.

5. In the **Configuration Object** field, select the configuration object to which this access permission applies.
6. In the **Access Permissions** list, select the access permissions to apply:

Property	Description
Read (R)	You can view details for this object.
Create (C)	You can create objects of this type.
Update (U)	You can change, or modify, this object.
Execute (X)	You can deploy, start, stop, or otherwise activate this object.
Delete (D)	You can delete this object.
Read Object Permissions (RP)	You can view access permissions granted for this object.
Change Object Permissions (CP)	You can change access permissions granted for this object.

7. Perform one of the following actions:
   - Click **Save** to accept the changes.
   - Click **Cancel** to discard the changes.

Changing Access Permissions

[+] Show Procedure

Procedure: Changing Access Permissions

Steps

1. Select an object.
2. Click **Related** and select **Access Control**. The **Access Control** panel opens.
3. Click an object in the **Access Control** panel to modify its access permissions. A new panel opens to the right.
4. You can change any or all of the following options:

Property	Description
Read (R)	You can view details for this object.
Create (C)	You can create objects of this type.
Update (U)	You can change, or modify, this object.
Execute (X)	You can deploy, start, stop, or otherwise activate this object.
Delete (D)	You can delete this object.
Read Object Permissions (RP)	You can view access permissions granted for this object.
Change Object Permissions (CP)	You can change access permissions granted for this object.

5. Perform one of the following actions:
    - Click **Save** to accept the changes.
    - Click **Cancel** to discard the changes.

Deleting Access Permissions

[+] Show Procedure

Procedure: Deleting Access Permissions

Steps

1. Select an object.
2. Click **Related** and select **Access Control**. The **Access Control** panel opens.
3. Click an object in the **Access Control** panel to modify its access permissions. A new panel opens to the right.
4. Click **Delete**.
5. A dialog box appears to confirm deletion. Perform one of the following actions:
    - Click **OK** to confirm deletion.
    - Click **Cancel** to cancel deletion.

Environment

The Environment section of Configuration Manager enables you to configure the following objects:

- Application Templates
- Applications
- Alarm Conditions
- Hosts
- Scripts
- Solutions
- Tenants
- Time Zones
- Detection/Reaction Scripts

Application Templates

An Application Template is the model you use for registering a new application in the Configuration Database. An Application Template describes the set of options that applies to an application of a particular type and version.

Before installing a new Genesys application, an Application Template must be available for that application. You can import the generic Application Template that is supplied with every Genesys application, or you can create a new Application Template.

> **Important**
>
> When upgrading previously installed releases of Genesys applications, you must register new Application Templates for the new releases, if the Release Notes indicate that these releases contain new configuration options that are essential for your environment.

Viewing Application Templates

The **Application Templates** list shows the Application Templates that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
>
> Application Templates that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Application Templates

To create a new Application Template object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**.

To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

Important

You cannot delete an Application Template, if it has already been used to create an Application.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy an Application Template
- **Move To**—Move an Application Template to another hierarchical structure.
- Enable or disable Application Templates
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.
- **Import Application Template**—Import an Application Template.

Click the name of an Application Template to view additional information about the object. You can also set permissions, options and application options, and view dependencies.

Important

If you change an application template for any existing application object, GAX displays a warning that the existing configuration options for the application will be replaced with options from the new template. You can choose to do one of the following:

- Click **Yes** to replace all current configuration options with the new template.
- Click **No** to open another dialog where you can choose whether to keep or replace any *matching* configuration options. (New options will automatically be appended.)
- Click **Cancel** to close the dialog without making any changes.

Procedure: Creating Application Template Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Application Template. You must specify a value for this property, and that value must be unique within the Configuration Database. Once you set the value, you cannot change it.
   - **Type**—The type of application to which the Application Template relates. Once you set the value, you cannot change it.
   - **Version**—The version of the application to which the Application Template relates. You must specify a value for this property. Once you set the value, you cannot change it. Genesys recommends that you specify the first three digits of the application version.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Procedure: Importing Application Templates

Genesys provides generic templates for all Genesys applications. You can find the .apd files for Application Templates, which come with every version of Genesys software, in the **Templates** folder on a product CD. To import an Application Template from the .apd file, perform the following procedure:

Steps

1. Click **More**, then select **Import Application Template**.
2. A new window displays. Click **Browse** to select an Application Template .apd file to import.
3. Click **OK** to upload the Application Template.

4. Refer to Creating Application Template Objects to finish creating the Application Template object.

Procedure: Importing Application Metadata

You can import an application metadata XML file into an existing or a new Application Template for Application objects. You can perform the following functions by importing application metadata:

- Define and describe Options which are available for end users to set up in an application.
- View the available Options within the Application Template object, even before an application object is created, by using the template.
- Edit or delete the user entered values of Options using the built-in editor. However, you cannot edit or delete the default template values.

Important

- The values entered by users in the Application objects are validated against the values defined in the metadata XML file.
- If the metadata for DB Server application is imported, the configuration option **[dbserver].stored_proc_result_table** may have an empty value. If the option is not filled in with a valid value, DB Server may not start correctly. The workaround is to enter a valid value for this configuration option, or delete it from the application object (recommended).

To import application metadata from an XML file, perform the following procedure:

Steps

1. Click **Import Metadata**. The **Import Metadata** window displays.
2. Click **Choose File**, then browse and select an Application Metadata XML file to import.
3. Click **Upload** to upload the Application Metadata.

4. Click **Save**. If the metadata is imported successfully, a green banner is displayed along with a confirmation message. If it is not imported, a red banner is displayed with an error message.
5. Refer to Creating Application Template Objects to finish creating the Application Template object.
6. Refresh the **Options** list to view the Options defined through the imported metadata in the Application Template object.

Applications

Applications are the various Genesys software programs that serve the contact center. There are two types of applications: graphical user interface (GUI) applications and daemon applications. Most daemon applications are servers to other applications.

You must register each instance of a daemon application separately. Configuration Server does not allow two daemon applications with the same name to be connected at the same time. By contrast, one object in the Configuration Database can represent any number of GUI applications of the same type and configuration parameters.

Viewing Applications

The **Applications** list shows the applications that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
>
> Disabled Applications are grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**. To select or de-select multiple objects at once, click **Select**.

Working with Applications

To create a new Application object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**.

To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

Otherwise, click **More** to perform the following tasks:

- **Refresh Table**—Refresh the display.
- **Clone**—Copy an Application.
- **Move To**—Move an Application to another hierarchical structure.
- **Enable** or **Disable** Applications.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.
- **Configure Logging**
- **Start** and **Stop**/**Force Stop** an Application.
- **Switch Mode**—Manually switch over a backup Application to primary mode.

Click the name of an Application to view additional information about the object. You can also set permissions, options and application options, and view dependencies.

Creating Application Objects

To create an Application, do the following:

[+] Show steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Application. You must specify a value for this property, and that value must be unique within the Configuration Database. Genesys does not recommend that you use symbols (including single and double quotation marks) in Application names; doing so may cause Applications to malfunction.
   - **Template**—The Application Template on which this Application is based. This value is set automatically when you select the Application Template.
   - **Type**—The type of the Application. This value is set automatically, based on the selected Application Template.
   - **Component Type**—Specifies the detailed purpose of this Application object within the configuration. Leave this field at its default value (Unknown) unless Application-specific documentation directs you to enter a specific value. This field is only displayed for daemon Applications.
   - **Version**—The version of the Application. This value is set automatically, based on the selected Application Template version.
   - **Is Application Server**—This field is checked for all daemon Applications and not checked for all GUI Applications. It is set automatically, based on the **Type** field.
   - **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

The following fields apply only to daemon Applications, not to GUI Applications:

- **Working Directory**—The full path to the directory where this Application is installed. This field is mandatory. When creating a new Application, Genesys recommends inserting a period (.). The path will be filled in automatically when the new Application is installed and connects to Configuration Server.
- **Command Line**—The command line that is used to start this Application, specifying the name of the Application's executable file. This field is mandatory. When creating a new Application, Genesys recommends inserting a period (.). The command line will be filled in automatically when the new Application is installed and connects to Configuration Server.
- **Command Line Arguments**—Additional command-line parameters that are used to start this Application. When creating a new Application, Genesys recommends leaving this field blank. Any arguments will be filled in automatically when the new Application is installed and connects to Configuration Server.
- **Startup Timeout**—The time interval, in seconds, during which the Management Layer expects this Application to start. If the Application has been configured with the autostart configuration option set to `true`, this is also the amount of time that Solution Control Server should wait to start this Application after initialization or after a system reboot. This field is mandatory.
- **Shutdown Timeout**—The time interval, in seconds, during which the Management Layer expects this Application to shut down. This field is mandatory.
- **Auto-Restart**—Indicates whether the Management Layer automatically restarts the Application after it shuts down unexpectedly.
- **Host**—The host computer on which the Application is running.

  > **Important**
  >
  > To support specific HA configurations, more than one server can be registered on the same port within the same host.

  Otherwise, do not assign the port number to any other server on the same host.
- **Backup Server**—The server that Client Applications contact if the connection to the primary server fails. You cannot associate one backup server with more than one primary server. You must use the same Application Template for the backup server that you use for the primary server, and you must associate the servers with the same user account.

  > **Important**
  >
  > When you designate an Application as a backup server for another server, the Application's Connections, Tenants, and Switch (for T-Server Applications) are automatically changed to match the corresponding values for the primary server. As long as this Application is associated with the primary server, its Connections are treated as read-only, and they are changed only when you apply changes to the Connections of the primary server.

- **Redundancy Type**—The type of redundancy with which this Application is running.
- **Timeout**—The amount of time, in seconds, that the client Application waits between reconnection attempts after a connection failure with the server.
- **Attempts**—The number of attempts to reconnect to this server before trying to connect to the

backup server. This value must be 1 or higher. This property is used only if you specify a Backup Server for this server.

> **Important**
>
> Setting this parameter to any value other than **1** may not take effect for some types of Applications.

- **Login as SYSTEM**—If checked, indicates that this Application logs into Configuration Server on behalf of the SYSTEM account.
- **Login As Account**—Identifies the account that applications must use to log in to Configuration Server. If **Login as SYSTEM** is checked, this field is disabled. For Configuration Server type applications, this field defaults to `Environment\default`.

> **Important**
>
> If you are configuring Configuration Server Proxy, Genesys strongly recommends that you use the default value (`Environment\default`).

- **Certificate**—The security certificate value. In Windows, select the certificate value from the list of installed certificates. In UNIX, enter the full path to the **<serial_#>_<host_name>_cert.pem** file.
- **Certificate Description**—An optional description of the Certificate.
- **Certificate Key**—The full path to the **<serial_#>_<host_name>_priv_key.pem** file of the security certificate key. This field is used only if Genesys Security is deployed on UNIX; otherwise this field is empty.
- **Trusted CA**—The full path to the **ca_cert.pem** file of the CA that issued the default security certificate. This field is used only if Genesys Security is deployed on UNIX; otherwise this field is empty.

> **Important**
>
> Refer to the *Genesys Security Deployment Guide* for more information about deploying Genesys TLS Security.

3. The **Connections** tab lists the connections that this Application has to other Applications. Click **Add** to add a connection.
4. Enter the following information in the pop-up window that displays on your screen:
   - **Server**—The server application that this application connects to as a client when it starts.
   - **Port ID**—The port of the server to which the application connects. If you want to use a secure connection, be sure to select a secure port.
   - **Connection Protocol**—The name of the connection control protocol. Select one of the following:
     - **Simple**—A simple TCP connection between Genesys components.
     - **ADDP**—Advanced Disconnect Detection Protocol (ADDP) between Genesys components. Refer to

the *Framework Deployment Guide* for more information about ADDP.

> **Important**
>
> Set the ADDP protocol between Local Control Agent and Solution Control Server in the **Options** tab of the Host object.

- **Local Timeout**—This value is required only if you specified **addp** in **Connection Protocol**. This value specifies the heartbeat polling interval, measured in seconds, on a client side. This indicates how often the client application sends polling signals to the server application. To enable this functionality, specify any integer as the value.

> **Warning**
>
> To avoid false disconnect states that might occur because of delays in the data network, Genesys recommends that you set the ADDP timeouts to values greater than 10 seconds.

- **Remote Timeout**—This value is required only if you specified **addp** in **Connection Protocol**. This value specifies the heartbeat polling interval measured, in seconds, on a server side. This indicates how often the server application sends polling signals to the client application. To enable this functionality, specify any integer as the value.

> **Warning**
>
> To avoid false disconnect states that might occur because of delays in the data network, Genesys recommends that you set the ADDP timeouts to values greater than 10 seconds.

- **Trace Mode**—The connection trace mode used between a server and its client, as follows:
  - **Trace Is Turned Off**—If you do not want either the client or the server application to print ADDP-related messages in its log.
  - **Trace On Client Side**—If you want the client application to print ADDP-related messages in its log.
  - **Trace On Server Side**—If you want the server application to print ADDP-related messages in its log.
  - **Trace On Both Sides**—If you want both the client and server applications to print ADDP-related messages in their log.
- **Connection Mode**—Specifies whether this port is secured or not by Genesys Security using the TLS protocol. This field is disabled if the client does not use Genesys Security.
- **Transport Protocol Parameters**—Any text, usually **key=value** pairs, separated by a semicolon (;). This property is application-specific. Refer to the documentation for the particular application to determine the appropriate values for this field, if any.
- **Application Parameters**—Any text, usually **key=value** pairs, separated by a semicolon (;). This property is application-specific. Refer to the documentation for the particular application to determine the appropriate values for this field, if any.

- Click **Apply** to save the information in the **Connections** tab.
- The **Ports** tab lists communication ports used by the clients of an application to connect to a server. To support specific high-availability configurations, more than one server can be registered on the same port within the same host. Otherwise, do not assign the port number to any other server on the same host. Click **Add** to add a connection.
- Enter the following information in the pop-up window that displays on your screen:
  - **Port ID**—The identifier of the port.
  - **Communication Port**—The port associated with the specified port ID.
  - **Connection Protocol**—The protocol used for the connection.
  - **HA Sync**—If selected, an HA backup server will use this port to establish a connection to the primary server.
  - **Listening Mode**—The listening mode configured for this port
  - **Certificate**—The security certificate value. In Windows, select the certificate value from the list of installed certificates. In UNIX, enter the full path to the **<serial_#>_<host_name>_cert.pem** file.
  - **Description**—An optional description of the Certificate.
  - **Certificate Key**—The full path to the **<serial_#>_<host_name>_priv_key.pem** file of the security certificate key. This field is used only if Genesys Security is deployed on UNIX; otherwise this field is empty.
  - **Trusted CA**—The full path to the **ca_cert.pem** file of the CA that issued the default security certificate. This field is used only if Genesys Security is deployed on UNIX; otherwise this field is empty.

    > **Important**
    > Refer to the *Genesys Security Deployment Guide* for more information about deploying Genesys TLS Security.

  - **Transport Parameters**—Any text, usually **key=value** pairs, separated by a semicolon (;). This property is application-specific. Refer to the documentation for the particular application to determine the appropriate values for this field, if any.
  - **Application Parameters**—Any text, usually **key=value** pairs, separated by a semicolon (;). This property is application-specific. Refer to the documentation for the particular application to determine the appropriate values for this field, if any.
- Click **Apply** to save the information in the **Ports** tab.
- The **Tenants** tab functional meaning only in a multi-Tenant environment. It specifies a list of Tenants that this application serves. The information specified in this list does not restrict the access privileges of the daemon applications with respect to the configuration data. Click **Add** to add a Tenant to this Application object.

> **Important**

> T-Server and High Availability (HA) Proxy applications do not display the Tenant property. A T-Server can serve only one Tenant, which is specified in the T-Server's **General** properties. An HA Proxy can serve only the same Tenant as the corresponding T-Server, and this Tenant is also specified in the HA Proxy's **General** properties.

- Click **Save**.

Configuring Logging

To configure logging, do the following:

[+] Show steps

1. In the **Applications** list, select one or more Applications.
2. Click **More** and select **Configure Logging**.
3. In the **Configuration of Logging** window, set the following options:
   - The Applications that you selected from the **Applications** list appears in the **Applications** section. You can select or de-select Applications to include in this procedure.
   - In the **Log Level** section, select one of the following options:
     - **All**—All events from the **Trace**, **Interaction**, and **Standard** log levels are logged.
     - **Trace**—Generates all log events from the **Trace**, **Interaction**, and **Standard** levels. This setting might adversely affect application performance. Set this level only when you are testing new interaction-processing functions or scenarios.
     - **Interaction**—Generates all log events of **Interaction** and **Standard** levels. Set this level only when you are testing events on a particular interaction.

       > **Important**
       > Interaction-level records contain the Interaction ID attribute that helps to search for log events that are generated by various applications but related to the same interaction.

       > **Warning**
       > Using the Interaction level generates a higher number of logging events on the network, which might may adversely affect the performance of the DBMS, Message Servers, and interaction-processing components.

     - **Standard**—Genesys recommends you permanently enable only a Standard level of logging during the operation of Solutions in regular production mode. This level reports events for significant problems and normal operations of in-service Solutions. An event is reported at the Standard level if it satisfies one of these criteria:

- Indicates that an attempt to perform any external operation has failed
- Indicates that the latest attempt to perform an external operation that previously failed has succeeded
- Indicates detection of a condition that has a negative impact on operations, actual or projected
- Indicates that a previously detected condition, which had a negative impact on operations, no longer exists
- Indicates a security violation of any kind
- Indicates a high-level data exchange that cannot be recognized or does not follow the expected logical sequence
- Indicates inability to process an external request
- Indicates successful completion of a logical step in an initialization process
- Indicates a transition of an Application from one operational mode to another
- Indicates that the value of a parameter associated with a configurable threshold has exceeded that threshold
- Indicates that the value of a parameter associated with a configurable threshold that earlier exceeded the threshold has returned to its normal range.

- **None**—No logging is performed.

4. In the **Log Outputs Adjustment** section, you can fine-tune the logging level for the following output types: **Network Log Server**, **Plain Text File**, and **Console**.
5. Perform one of the the following:
   - If you selected **Network Log Server** in the previous step, go to the **Message Server** section and select the Message Server to receive logs.
   - If you selected **Plain Text File** in the previous step, go to the **Log File Name** section and specify the log file name to receive logs. You can also specify the following:
     - **Create Segment**—If checked, segment the log file into chunks specified by the **Segment Size (MB)** field.
     - **Segment Size (MB)**—If **Create Segment** is checked, specify a segment size for the log file, in megabytes.
     - **Segment Expiration**—If checked, segments are deleted after a maximum number of segments is reached, as defined by **Maximum Segments**.
     - **Maximum Segments**—If **Segment Expiration** is checked, specify how many segments to retain before segments beyond this limit are removed.
6. Click **OK**.

Starting and Stopping Applications

The status of each Application object is displayed on the System Dashboard. Starting in release 8.5.240, the status is also displayed in the list of Applications in Configuration Manager. Any

Application can also be started or stopped from this list.

Starting and stopping an Application is generally the same as doing it in the System Dashboard. Basically, you:

1. Select an Application in the list.
2. Open the **More** menu.
3. Select the appropriate start, stop, or switchover action. The options available to you in the menu will depend on the current status of the Application.
4. Confirm your selection.

Genesys Administrator Extension notifies Solution Control Server, which uses Local Control Agent to remotely execute the operation on the Application.

You must have Execute permission and the appropriate Role privileges to start and stop an Application.

> **Important**
>
> - You cannot start or stop a Database Access Point Application.
> - Applications with a status of NA are container objects, such as Folders or Configuration Units, or are disabled. You cannot start or stop them.

Starting Applications

You can start an Application only if its current status is Stopped.

> **Important**
>
> - Application startup through Genesys Administrator Extension does not necessarily mean that the Application immediately starts performing its function. Applications are components of higher-level structures called Solutions, and most of them function normally only as part of the Solutions to which they belong. Genesys recommends that you activate single Applications only for maintenance purposes or during online upgrades. In normal production mode, always start a complete Solution.
> - An Application that you installed as a Service must be started only as a Service.

To start an Application from the Application list, do the following:

[+] Show steps

1. Select the Application that you want to start.
2. Open the **More** menu, and select **Start**.

Application startup might take some time, depending on:

- The amount of configuration data the Application must read from the Configuration Database.
- The amount of time it takes to check data integrity and completeness.
- The number of network connections the Application must set up to other system resources.

While an Application is being initialized, its status changes from Stopped to Pending. When the Application starts, its status changes from Pending to Running. In some scenarios, an Application might depend on internal and/or external components to perform their functions. In this case, the Application status might change as follows:

- From Stopped to Pending to Initializing and, possibly, to Service Unavailable.
- From either Initializing or Service Unavailable to Started only after all the internal and external components are ready.

Genesys Administrator reports the successful start of an Application only if the Application has reported either Started or Service Unavailable status within the configured timeout period.

> **Tip**
>
> You can also stop an Application by clicking its status. For example, if an Application has a status of **Started** and you click its status, it attempts to stop.

Stopping Applications Gracefully

> **Warning**
>
> Stopping an Application can cause the stoppage of some or all of the running Solutions to which the Application belongs.

This action is similar to the **Graceful Stop** command in Genesys Administrator. When you stop an Application, the Application stops accepting new requests and finishes processing the requests in its queue. If you are not sure if an Application supports graceful shutdown, you can use the configuration option **suspending-wait-timeout** to configure a timeout. This will ensure that the Application shuts down gracefully if it supports graceful shutdown; otherwise, it will be stopped ungracefully. Refer to the *Framework Configuration Options Reference Manual* for more information about this configuration option.

You can stop an Application only if its current status is Started, Service Unavailable, or Pending. You cannot stop an Application gracefully if its status is Suspending or Suspended.:

To gracefully stop an Application from the Application list, do the following:

[+] Show steps

1. Select the Application that you want to stop.
2. Open the **More** menu, and select **Stop**.

> **Tip**
> You can also stop an Application by clicking its status. For example, if an Application has a status of **Started** and you click its status, it attempts to stop.

Stopping Applications Immediately (Force Stop)

> **Warning**
> Stopping an Application can cause the stoppage of some or all of the running Solutions to which the Application belongs.

When you use Force Stop to stop an Application, the Application immediately stops processing all requests, both current and new. You can only stop an Application if its current status is Started, Service Unavailable, Pending, Suspending, or Suspended.

To stop an Application in the Application list using Force Stop, do the following:

[+] Show steps

1. Select the Application that you want to stop forcefully.
2. Open the **More** menu, and select **Force Stop**.

> **Tip**
> You can also start and stop applications by clicking on the status name in the Applications tab. For example, if an application has a status of **Started** and you click the status name, the application attempts to stop. Likewise, if an application has a status of **Stopped** and you click the status name, the application attempts to start.

Switch Mode (Manual Switchover)

Switch mode switches an Application configured in an HR pair, and running in backup mode, to primary mode. This forces the corresponding primary Application to run in backup mode. This option is disabled if the selected Application is not configured as the primary Application in an HA pair.

To perform a manual switchover, you must have an appropriate license for the Management Layer to perform the switchover. If no license is present, this option is disabled.

Manual switchover is not available for Applications of the following types:

- Configuration Server
- Database Access Point
- Solution Control Server

To manually switch over a backup HA Application in an HA pair to run in primary mode, do the following:

[+] Show steps

1. Select the backup Application that you want to switch to primary mode.
2. Open the **More** menu, and select **Switch Mode**.

Alarm Conditions

Alarm Conditions specify the events that you might want to know about and manage as soon as they occur, such as if a Host or Solution is unresponsive. Genesys software contains predefined Alarm Conditions, or you can create your own.

Alarm Conditions work with the following Scripts:

- Alarm Detection Scripts, which identify what system variables the Management Layer must monitor to trigger an alarm.
- Alarm Reaction Scripts, which identify what the Management Layer must do when alarms occur in, or are cleared from, the system. Alarm Reaction Scripts that identify what happens when alarms are cleared are referred to as alarm Clearance Scripts.

To create an Alarm Condition script, see Scripts. To associate Alarm Detection and Alarm Reaction Scripts with Alarm Conditions, specify them in the tabs of the Alarm Condition.

Viewing Alarm Conditions

The **Alarm Conditions** list shows the Alarm Conditions that are in your environment. It is sorted in a hierarchy by tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
> Alarm Conditions that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

To select or de-select multiple objects at once, click **Select**.

Working with Alarm Conditions

To create a new Alarm Condition object, click **New**. To view or edit details of an existing object, click

the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy an Alarm Condition.
- **Move To**—Move an Alarm Condition to another hierarchical structure.
- Enable or disable Alarm Conditions
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of an Alarm Condition to view additional information about the object. You can also set options and permissions.

Procedure: Creating Alarm Condition Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click the **Browse** button to select a value from a list:
   - **Name**—The name of the Alarm Condition. You must specify a value for this property and that value must be unique within the Configuration Database.
   - **Description**—A brief description of the Alarm Condition.
   - **Category**—The category of the Alarm Condition: **Critical**, **Major**, or **Minor**. You must specify a value for this property.
   - **Detect Script**—The Script that describes the logic applied to detect the alarm.
   - **Cancel Timeout**—The amount of time, in seconds, that the Alarm Condition is registered in the Log Database, unless another event cancels it or a user clears it. When this timeout expires, the Alarm Condition is unconditionally cleared.
   - **Detect Log Event ID**—The identifier of the event that triggers the alarm. You must specify a value for this property.
   - **Detect Selection**—The mode for event selection that the Management Layer uses for Alarm Condition analysis. The modes are as follows:
     - **Select By Any**—The specified event from any application results in an alarm.
     - **Select By Application**—The specified event from a selected application results in an alarm. Select this option to display the **Application** field. Click the **Browse** icon to select an item from a list, or type the name or partial name of the item in the **Quick Filter** field. The list is populated with Application objects that are stored in Configuration Server.

- **Select By Application Type**—The specified event from a selected application type results in an alarm. Select this option to display the **Type** field. Click the drop-down button to select an item from the list. The list is populated with Application objects that have defined subtypes.

- **Cancel Log Event ID**—The identifier of the event that triggers clearance of the alarm. For alarm clearance, the Management Layer uses the event from the same application(s) as specified for the detect event for this Alarm Condition.
- **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

Once the object has been created, you can edit the object and click the **Reaction Scripts** or **Clearance Scripts** tabs to assign scripts to the Alarm Condition. See Scripts for more information.

Procedure: Testing Alarm Conditions

Steps

1. In the **Alarm Conditions** list, click the check box beside one or more Alarm Conditions that you want to test.
2. Click **More** and select **Activate Alarm**.
3. The Alarm Condition activates. Go to the System Dashboard to view the Alarm and clear it.

Predefined Alarm Conditions

Genesys provides the predefined Alarm Conditions listed in the following table. If required, you can further configure these conditions to meet your requirements.

Alarm Type	Description
`Application Failure`	Reports that the specified application has either

Alarm Type	Description
	terminated or stopped responding.
Connection Failure	Reports that the specified connection between any two applications has been lost.
CTI Link Failure	Reports that the connection between the specified T-Server and its switch has been lost.
Host Inaccessible	Reports that the Management Layer cannot contact the Local Control Agent (LCA) on the host where Genesys daemon applications are running. LCA is not started, or it is listening on a port other than the one specified in the configuration. A condition of Host Inaccessible is also referred to as being Down.
Licensing Error	Reports that a licensing error has occurred.
Service Unavailable	Reports that a Genesys component cannot provide service for some internal reasons.
Host Unavailable	Reports that a host where Genesys daemon applications are running is unavailable (turned off).
Host Unreachable	Reports that the Management Layer cannot reach the host where Genesys daemon applications are running (no route to the host).
Unplanned Solution Status Change	Reports that the status of a Solution has changed from Started to Pending, but without any requests to stop the Solution. This may indicate a failure of one of the Solution components.
Message Server Loss of Database Connection	Reports that Message Server has lost connection to the Centralized Log Database.

For more information about predefined Alarm Conditions, see the Management Layer User's Guide.

Alarm E-mails

You can customize the Subject line and body of an Alarm Reaction email by creating a template, using plain text, and any of the following reserved variables that represent the specific information about the alarm:

Variable	Description
$REACT_NAME	The name of the Alarm Reaction.
$COND_ID	The Alarm Condition ID.
$COND_NAME	The name of the Alarm Condition.
$COND_CTGR	The category of the Alarm Condition.
$APP_ID	The Application ID.
$APP_NAME	The name of the Application.
$APP_TYPE	The Application type.

Variable	Description
$MSG_ID	The Message ID.
$MSG_DESCR	The text of the Message.
$$	The dollar sign character ($).

You can then use this Alarm Reaction script as often as appropriate. For each use, the email text is automatically customized for the specific situation.

Example

An example Alarm Reaction email uses the following template:

```
Subject:

$COND_ID detected in $APP_NAME

Message:

CPU Overload has been detected by Genesys Solution Management Layer for Host1.

Alarm Reaction: $REACT_NAME

Alarm Condition:

ID: $COND_ID

NAME: $COND_NAME

Category: $COND_CTGR

Application:

ID: $APP_ID

Name: $APP_NAME

Type: $APP_TYPE
```

In the following scenario, the system detects that a CPU overload has occurred in the Solution Control Server, an alarm is triggered, and the following email is sent in response. Note how the variable names have been replaced with actual values that are appropriate to the alarm scenario.:

```
Subject:

CPU_overload detected in Solution_Control_Server_760

Message:

CPU Overload has been detected by Genesys Solution Management Layer for Host1.

Alarm Reaction: cpu_overload_mail

Alarm Condition:

ID: 118

NAME: CPU_overload
```

Category: Major

Application:

ID: 105

Name: Solution_Control_Server_760

Type: SCS

Hosts

Hosts are the computers that run the various server applications in the environment.

Register only those hosts on which you will install and run Genesys servers or third-party servers that you configure in the Configuration Database.

Viewing Hosts

The **Hosts** list shows the hosts that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
>
> Hosts that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Hosts

To create a new Host object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Important**
> You can delete a Host only if there are no server applications currently assigned to it.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Host.
- **Move To**—Move a Host to another hierarchical structure.
- Enable or disable Hosts.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.
- Configure Logging

Click the name of a Host to view additional information about the object. You can also set options and permissions, and view dependencies.

Creating Host Objects

[+] Click to show procedure

Procedure: Creating Host Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the host. You must specify a value for this property, and that value must be unique within the Configuration Database. Because applications use this host name to establish connections with the servers running on this host, make sure that the name exactly matches the name of this host in the data network configuration.

     > **Important**
     > You cannot change this host name if any server applications are assigned to this host.

- **IP Address**—The IP address of the host. This value must be unique within the Configuration Database. Because applications may be using the specified IP address to establish connections with the servers running on this host, make sure that the value that you enter exactly matches the IP address of this host in the data network configuration.

  > **Tip**
  >
  > Click the magnifying glass in the **Name** field to have GAX automatically enter the IP address for the host.

- **OS Type**—The type of the operating system of this host. You must specify a value for this property.
- **Version**—The version of the operating system.
- **LCA Port**—The port number on which Local Control Agent (LCA) for this host is running. The LCA port must be set to a value between 2000 and 9999, inclusive. When the LCA port is specified as less than 2000, LCA starts on port number 4999 (the default value).

  > **Important**
  >
  > Do not change the value of the LCA port if any application has already connected to LCA or if Solution Control Server (SCS) has already started to control LCA.

- **Solution Control Server**—The SCS that monitors and controls this host. This property is valid only if you enable distributed SCS functionality. See the *Management Layer User's Guide* for details.
- Certificate—The security certificate value. In Windows, select the certificate value from the list of installed certificates. In UNIX, enter the full path to the **<serial_#>_<host_name>_cert.pem** file.
- **Certificate Description**—An optional description of the Certificate.
- **Certificate Key**—The full path to the **<serial_#>_<host_name>_priv_key.pem** file of the security certificate key. This field is used only if Genesys Security is deployed on UNIX; otherwise this field is empty.
- **Trusted CA**—The full path to the **ca_cert.pem** file of the CA that issued the default security certificate. This field is used only if Genesys Security is deployed on UNIX; otherwise this field is empty.

  > **Important**
  >
  > Refer to the *Genesys Security Deployment Guide* for more information about deploying Genesys

> TLS Security.

- **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

Configuring Logging

[+] Click to show procedure

Procedure: Configuring Logging

Steps

1. In the **Hosts** list, select one or more Hosts.
2. Click **More** and select **Configure Logging**.
3. In the **Configuration of Logging** window, set the following options:
   - The Hosts that you selected from the **Hosts** list appears in the **Hosts** section. You can select or de-select Hosts to include in this procedure.
   - In the **Log Level** section, select one of the following options:
     - **All**—Generates all log events from the **Trace**, **Interaction**, and **Standard** levels.
     - **Trace**—Generates all log events from the **Trace**, **Interaction**, and **Standard** levels. This setting might adversely affect application performance. Set this level only when you are testing new interaction-processing functions or scenarios.
     - **Interaction**—Generates all log events of **Interaction** and **Standard** levels. Set this level only when you are testing events on a particular interaction.

> **Important**
>
> Interaction-level records contain the Interaction ID attribute that helps to search for log events that are generated by various applications but related to the same interaction.

> **Warning**
>
> Using the Interaction level generates a higher number of logging events on the network, which might adversely affect the performance of the DBMS, Message Servers, and interaction-processing components.

- **Standard**—Genesys recommends you permanently enable only a Standard level of logging during the operation of Solutions in regular production mode. This level reports events for significant problems and normal operations of in-service Solutions. An event is reported at the Standard level if it satisfies one of these criteria:
  - Indicates that an attempt to perform any external operation has failed
  - Indicates that the latest attempt to perform an external operation that previously failed has succeeded
  - Indicates detection of a condition that has a negative impact on operations, actual or projected
  - Indicates that a previously detected condition, which had a negative impact on operations, no longer exists
  - Indicates a security violation of any kind
  - Indicates a high-level data exchange that cannot be recognized or does not follow the expected logical sequence
  - Indicates inability to process an external request
  - Indicates successful completion of a logical step in an initialization process
  - Indicates a transition of an Application from one operational mode to another
  - Indicates that the value of a parameter associated with a configurable threshold has exceeded that threshold
  - Indicates that the value of a parameter associated with a configurable threshold that earlier exceeded the threshold has returned to its normal range.
- **None**—No logging is performed.

4. In the **Log Outputs Adjustment** section, you can fine-tune the logging level for the following output types: **Network Log Server**, **Plain Text File**, and **Console**.
5. Perform one of the the following:
   - If you selected **Network Log Server** in the previous step, go to the **Message Server**

section and select the Message Server to receive logs.

- If you selected **Plain Text File** in the previous step, go to the **Log File Name** section and specify the log file name to receive logs. You can also specify the following:
  - **Create Segment**—If checked, segment the log file into chunks specified by the **Segment Size (MB)** field.
  - **Segment Size (MB)**—If **Create Segment** is checked, specify a segment size for the log file, in megabytes.
  - **Segment Expiration**—If checked, segments are deleted after a maximum number of segments is reached, as defined by **Maximum Segments**.
  - **Maximum Segments**—If **Segment Expiration** is checked, specify how many segments to retain before segments beyond this limit are removed.

6. Click **OK**.

ADDP

To configure the Advanced Disconnect Detection Protocol (ADDP) protocol between the LCA of a given host and SCS, use the **Options** tab of the Host object. If you are using the Management Layer for application failure management, set up ADDP parameters for the host as described.

Procedure: Setting up ADDP Connections

Steps

1. Open the **Options** tab of the Host.
2. Create a section called addp.
3. In the addp section, specify the following configuration options:

Option Name	Option Value	Option Description
`addp-timeout`	Any integer	Sets the ADDP timeout in seconds. If one application in the connection does not receive messages from the other application

Option Name	Option Value	Option Description
		in the connection within this interval, the first application sends a polling message. If the first application does not receive a response to the polling message within this time interval, it interprets the lack of response as a loss of connection. The recommended setting for this option is 3 seconds for a LAN connection or 10 seconds for a WAN connection.
addp-trace	local	LCA prints ADDP-related messages into its log.

> **Important**
>
> You configure ADDP between servers by using the Application's **Connections** tab.

Check Ports

You can click the name of a Host to view more information about the host's configuration, as well as check port information and identify port conflicts. Click **Check Ports** to display all applications and configured ports for the Host object, as well any port conflicts. Ports that are duplicated in multiple applications are highlighted in the list, as these ports might be in conflict. You can click an Application in the **Check Ports** list to view details about the Application object. Click **Export** to export the items in the list to a Microsoft Excel-compatible file.

Scripts

Scripts identify processing scenarios or treatments that can be applied to customer interactions. For example, an Alarm Reaction Script specifies how to react when an Alarm Condition is triggered.

> **Important**
>
> Depending on the application type, a scenario or treatment itself might be part of the Script object, in which case it is listed in the **Options** tab of the Script object.

For more information about Scripts, refer to the Management Layer User's Guide or to the documentation specific to your product.

Viewing Scripts

The **Scripts** list shows the Scripts that are in your environment. It is sorted in a hierarchy by tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
>
> Scripts that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Scripts

To create a new Script object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. When you delete a Script, it is removed from the Configuration Database and from the Alarm Condition with which it is associated. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Script.
- **Move To**—Move a Script to another hierarchical structure.
- Enable or disable Scripts.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Script to view additional information about the object. You can also set options and permissions, and view dependencies.

Creating Script Objects

Procedure: Creating Script Objects

Purpose: To create Script objects.

Prerequisites

You are in the **Scripts** window of Configuration Manager.

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Script. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Script Type**—The type of the Script. You must specify a type. Once you set the type, you cannot change it.
   - **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.

- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

Procedure: Creating Alarm Condition Script Objects

Purpose: To create Script objects for Alarm Conditions.

Prerequisites

You are in the **Detection/Reaction Scripts** window of Configuration Manager.

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Script. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Script Type**—The type of the Script. You must specify a type. Once you set the type, you cannot change it.
     - **Alarm Reaction**—See the Alarm Scripts tab, above, for more information about Alarm Reaction scripts.
       - **Alarm Reaction Types**—Select what action to take when this Script is triggered. The available text fields change to show information applicable to your selection.
     - **Alarm Detection**—See the Alarm Scripts tab, above, for more information about options you can set for Alarm Detection scripts.
       - **Detection Types**—Select what action to take when this Script is triggered. The available text fields change to show information applicable to your selection.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Alarm Scripts

Choose one of the following script types to learn more:

- Alarm Detection Scripts
- Alarm Reaction Scripts

Alarm Detection Scripts

Alarm Detection Scripts identify what system variables the Management Layer must monitor to trigger an alarm.

The system variables that the Management Layer can monitor (also called advanced alarm detection parameters) include:

- **Host System Variable Threshold**—Enables you to specify the value for an irregular change that might occur over a certain interval, in either CPU or memory use, on a given host.
- **Application System Variable Threshold**—Enables you to specify the value for an irregular change that might occur over a certain interval in either an application's CPU or memory use.
- **Local SNMP Variable Threshold**—Enables you to specify the value for an irregular change that might occur over a certain interval in any SNMP variable retrieved from the Genesys MIB file.
- **Remote SNMP Variable Threshold**—Enables you to specify the value for an irregular change that might occur over a certain interval in any SNMP variable retrieved from a non-Genesys MIB file.

> ### Warning
> The SNMP-related alarm detection capabilities require that you have a Genesys SNMP license for Solution Control Server.

> ### Important
> The Rising Threshold, which triggers an alarm when crossed only if the value is rising, must be a higher number than the Falling Threshold, which clears the alarm when crossed only if the value is falling. For example, if the Rising Threshold is `300`, the Falling Threshold must be less than `300`.

Alarm Reaction Scripts

Alarm Reaction Scripts identify what the Management Layer must do when alarms occur in, or are cleared from, the system.

The Management Layer supports the following types of Alarm Reaction Scripts:

- Shutdown of a specified application.

- Startup of a specified application.
- Restart of the application that reported the alarm.
- Startup of a specified solution.
- Sending an email message with information about the alarm to specified Internet addresses. You can customize the email with specific details about the alarm.
- Switchover of operations from the application that reported the alarm to its backup application, for applications running in primary mode, backup mode, or regardless of the mode.
- Sending an SNMP trap with detailed information about the alarm to a general-purpose network management system.
- Execution of an operating system command.

> **Important**
>
> For a description of the OS commands you can specify in an Alarm Reaction Script, refer to the Management Layer User's Guide.

- Changing a configuration option value for the specified application or for the application that reported the alarm.

Solutions

Solutions are sets of applications that accomplish particular business tasks in contact centers.

Viewing Solutions

The **Solutions** list shows the Solutions that are in your environment. It is sorted in a hierarchy by tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Solutions that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Solutions

To create a new Solution object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Solution.
- **Move To**—Move a Solution to another hierarchical structure.
- Enable or disable Solutions.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

- Configure Logging

Click the name of a Solution to view additional information about the object. You can also set options and permissions, and view dependencies.

Creating Solution Objects

To create Solution Objects, do the following:

[+] Click to show procedure

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Solution. You must specify a value for this property, and that value must be unique within the Configuration Database.
   - **Assigned to Tenant**—In a multi-tenant environment, the Tenant to which this Solution is assigned.
   - **Solution Type**—The type of the Solution. You must specify a value for this property. Once you set the value, you cannot change it. This value is automatically set, based on the type of the imported Solution.

     > **Important**
     > A Solution of type **Default Solution Type** or **Framework** cannot be started and stopped with Solution Control Interface unless they have been created using a solution wizard. See the Management Layer User's Guide for more information.

   - **Solution Control Server**—The name of the Solution Control Server that controls this Solution.
   - **Version**—The version of the Solution. You must specify a value for this property.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. In the **Application Definitions** tab, click **Add** to add an Application object to this Solution.

   > **Important**
   > The same Solution Control Server must control all Solutions that use the same Solution component.

4. Enter the following information in the pop-up window that displays on your screen:
   - **Application Type**—The type of Application used as a Solution component.

- **Version**—The version of the Application used as a Solution component.
- **Startup Priority**—The default position of the Solution component in the component startup sequence within the Solution.
- **Optional**—Specifies whether this Solution component is optional.
- Click **OK**.

5. Click **Apply** to save the information in the **Application Definitions** tab.
6. In the **Applications** tab, click **Add** to add an Application to this Solution.

> **Important**
> The same Solution Control Server must control all Solutions that use the same Solution component.

7. Enter the following information in the pop-up window that displays on your screen:
   - **Application**—The type of Application used as a Solution component.
   - **Startup Priority**—The default position of the Solution component in the component startup sequence within the Solution.
   - **Optional**—Specifies whether this Solution component is optional.
   - Click **OK**.
8. Click **Save**.

Configuring Logging

To configure logging for a Solution, do the following:

[+] Show steps

1. In the **Solutions** list, select one or more Solutions.
2. Click **More** and select **Configure Logging**.
3. In the **Configuration of Logging** window, do the following:
   - The Solutions that you selected from the **Solutions** list appear in the **Solutions** section. You can select or de-select Solutions to include in this procedure.
   - In the **Log Level** section, select one of the following options:
     - **All**—All events from the **Trace**, **Interaction**, and **Standard** log levels are logged.
     - **Trace**—Generates all log events from the **Trace**, **Interaction**, and **Standard** levels. This setting might adversely affect application performance. Set this level only when you are testing new interaction-processing functions or scenarios.
     - **Interaction**—Generates all log events of **Interaction** and **Standard** levels. Set this level only when you are testing events on a particular interaction.

> **Warning**
>
> - Using the Interaction level generates a higher number of logging events on the network, which might adversely affect the performance of the DBMS, Message Servers, and interaction-processing components.
> - Interaction-level records contain the Interaction ID attribute that helps to search for log events that are generated by various applications but related to the same interaction.

- **Standard**—Genesys recommends you permanently enable only a Standard level of logging during the operation of Solutions in regular production mode. This level reports events for significant problems and normal operations of in-service Solutions. An event is reported at the Standard level if it satisfies one of these criteria:
  - Indicates that an attempt to perform any external operation has failed
  - Indicates that the latest attempt to perform an external operation that previously failed has succeeded
  - Indicates detection of a condition that has a negative impact on operations, actual or projected
  - Indicates that a previously detected condition, which had a negative impact on operations, no longer exists
  - Indicates a security violation of any kind
  - Indicates a high-level data exchange that cannot be recognized or does not follow the expected logical sequence
  - Indicates inability to process an external request
  - Indicates successful completion of a logical step in an initialization process
  - Indicates a transition of an Application from one operational mode to another
  - Indicates that the value of a parameter associated with a configurable threshold has exceeded that threshold
  - Indicates that the value of a parameter associated with a configurable threshold that earlier exceeded the threshold has returned to its normal range.
- **None**—No logging is performed.

- In the **Log Outputs Adjustment** section, you can fine-tune the logging level for the following output types: **Network Log Server**, **Plain Text File**, and **Console**. Do one of the the following:
  - If you selected **Network Log Server** in the previous step, go to the **Message Server** section and select the Message Server to receive logs.
  - If you selected **Plain Text File** in the previous step, go to the **Log File Name** section and specify the log file name to receive logs. You can also specify the following:
    - **Create Segment**—If checked, segment the log file into chunks specified by the **Segment Size (MB)** field.
    - **Segment Size (MB)**—If **Create Segment** is checked, specify a segment size for the log file, in megabytes.

- **Segment Expiration**—If checked, segments are deleted after a maximum number of segments is reached, as defined by **Maximum Segments**.
- **Maximum Segments**—If **Segment Expiration** is checked, specify how many segments to retain before segments beyond this limit are removed.

4. Click **OK**.

Tenants

Tenants are businesses whose customer interactions are enabled or enhanced through services offered by a third party, typically a telecommunications service provider. From an architectural standpoint, however, most of the hardware and software that Tenants use to enable or enhance those interactions belong to the service provider.

From a functional standpoint, each Tenant in a hierarchical multi-tenant environment is a contact center (single or multi-site) completely equipped to process customer interactions. In a hierarchical multi-tenant environment, at any given time, Genesys Administrator Extension displays only those hardware and software resources belonging to a particular Tenant within that environment.

> **Important**
>
> To create Tenants, a user must have the appropriate permissions and role privileges to log in to Genesys Administrator Extension and create Tenants. However, the Tenant Creators Access Group must exist for the user to create a Tenant.

Allocation of Resources

Some of these hardware and software resources are allocated to each Tenant separately (for example, the telephony extensions and queues of a switching system).

Other resources are shared by the Tenants; these resources process customer interactions for some or all of the Tenants simultaneously (for example, the control and signaling devices of a switching system, and service control points of the public telephone network).

The configuration objects that describe both types of resources are allocated to Tenants accordingly.

Viewing Tenants

Normally, the Tenants that are visible depends on which Tenant is selected in the **Tenant Directory** of Configuration Manager. When set to Environment, the User is able to see all Tenants. If another Tenant is selected, the User can view only that Tenant and any existing child Tenants.

If the User is using the **Quick Filter** field, all Tenants to which the User has access are searched. If the User does not have access to the Environment (root) Tenant, it is not displayed.

Viewing Tenants

The **Tenants** list shows the Tenants that are in your environment.

> **Important**
> Tenants that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list by typing the name or partial name of an object in the **Quick Filter** field.

Working with Tenants

To create a new Tenant object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. You must click a Tenant to access functions to copy the Tenant, delete the Tenant, or to enable or disable the Tenant.

> **Important**
> When you delete a Tenant from the Configuration Database, all of its child Tenants are also deleted, and recursively, all of their child Tenants.

Click the name of a Tenant to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Tenant Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Tenant. You must specify a value for this property, and that value must be unique within the Configuration Database.
   - **Password**—A password that must be used to access this Tenant.
   - **Confirm Password**—A confirmation of the password.

- **Parent Tenant**—The parent Tenant of this Tenant. By default, the parent Tenant is the Tenant in which you are creating the new Tenant. If you change this field, the new Tenant will be created as a new child Tenant under the specified parent Tenant. To subsequently change the parent Tenant, refer to the Structure tab, above.
- **Chargeable Number**—The account number to which activities for this Tenant are charged, for cost-tracking purposes.
- **Default Capacity Rule**—The name of the Script of Capacity Rule type that defines the ability of this Tenant to handle multiple interactions. For more information, refer to Reporting documentation.
- **Default Contract**—The default cost contract applied to resources of this Tenant. For more information, refer to the Routing Solutions chapter of the *Universal Routing 8.0 Routing Application Configuration Guide*.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

Important

If you are not logged in as the default User, or are not a member of the **SuperAdministrators** Access Group, you must have special permissions and role privileges to create a Tenant. Refer to the *Genesys Security Deployment Guide* for details about the security requirements for creating a Tenant.

Tenant Structure

Hierarchical Multi-Tenant Structure

The structure of a hierarchical multi-tenant structure can contain an unlimited number of levels. This configuration environment serves the needs of every company in the hierarchy.

In any multi-tenant environment, when you run Genesys Administrator Extension for the first time after the Configuration Database initialization, you can only view the Environment Tenant. When you register a new Tenant in the Configuration Database, the Configuration Layer automatically creates all the folders necessary to support resource allocation and configuration data entry for this Tenant.

Refer to the *Genesys Security Deployment Guide* for information about how permissions are inherited in a hierarchical multi-tenant structure.

Modifying the Hierarchical Multi-Tenant Structure

To rearrange Tenants between parent Tenants in the structure, modify the Parent Tenant field for the Tenant object that you want to move.

Time Zones

Time Zones are predefined objects that provide Genesys applications with information about international time zones.

When you first open the list of Time Zone objects, you will see a list of international time zones.

Viewing Time Zones

The **Time Zones** list shows the Time Zones that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Time Zones that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Time Zones

To create a new Time Zone object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Time Zone.
- **Move To**—Move a Time Zone to another hierarchical structure.

- Enable or disable Time Zones.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Time Zone to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Time Zone Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Time Zone. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Description**—A brief description of the Time Zone.
   - **Name in Mozilla**—The name of the Time Zone used in the Mozilla Firefox browser. You must specify a value for this property.
   - **Name in Explorer**—The name of the Time Zone used in the Microsoft Internet Explorer browser. You must specify a value for this property.
   - **DST Observed**—Indicates whether Daylight Saving Time (DST) is used.

     Note: The following fields display only if the **DST Observed** check box is selected.
   - **Daylight Saving Time Type**—Select one of the following to define when DST starts and ends:
     - **Current Year or Fixed Date (local)**—DST begins and ends on a specific date and time. This setting covers only one year, and must be reset every year.
       - **Start Date**—The date at which DST begins.
       - **End Date**—The date at which DST ends.
       - **Start Time**—The time at which DST begins.
       - **End Time**—The time at which DST ends.
     - **Daylight Saving Time definition (GMT)**—DST begins and ends on a specific month/day/time. These settings are carried forward over many years, until changed or DST is no longer used.
       - **Start Year**—The year that DST started to be observed or will start to be observed. If DST is currently in use, you can also select **Not Observed**.
       - **End Year**—The year that DST is to be discontinued. If there are no plans to

discontinue DST, select **Not Observed**.

- **Start Month**—The month in which DST starts.
- **End Month**—The month in which DST ends.
- **Start Day Type**—Specifies whether the **Start Day** value is `Fixed`, in which DST starts on the same date every year, or `Variable`, in which you must define the variables to be used to determine the Start Day.
- **End Day Type**—Specifies whether the **End Day** value is `Fixed`, in which DST ends on the same date every year, or `Variable`, in which you must define the variables to be used to determine the End Day.
- (If **Start Day Type** is set to `Fixed`) **Start Day**—The date at which DST begins.
- (If **End Day Type** is set to `Fixed`) **End Day**—The date at which DST ends.
- (If **Start Day Type** is set to `Variable`) **Start Week**—The week number in which DST begins.
- (If **End Day Type** is set to `Variable`) **End Week**—The week number in which DST ends.
- (If **Start Day Type** is set to `Variable`) **Start Day of Week**—The day of the week in which DST begins.
- (If **End Day Type** is set to `Variable`) **End Day of Week**—The day of the week in which DST ends.
- **Start Time**—The time at which DST begins.
- **End Time**—The time at which DST ends.

- **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

International Time Zones

Genesys Administrator Extension includes the following international time zones:

Abbreviation	Time Zone
ACT	Australia Central Time
AET	Australia Eastern Time
AGT	Argentina Standard Time

Abbreviation	Time Zone
AtlST	Atlantic Standard Time
ART	(Arabic) Egypt Standard Time
AST	Alaska Standard Time
BET	Brazil Eastern Time
BST	Bangladesh Standard Time
CAT	Central Africa Time
CNT	Canada Newfoundland Time
CST	Central Standard Time
CTT	China Taiwan Time
EAT	Eastern Africa Time
ECT	European Central Time
EET	Eastern European Time
EST	Eastern Standard Time
GMT	Greenwich Mean Time
HST	Hawaii Standard Time
IET	Indiana Eastern Standard
IST	India Standard Time
JST	Japan Standard Time
KST	Korea Standard Time
MET	Middle East Time
MIT	Midway Islands Time
MST	Mountain Standard Time
NET	Near East Time
NST	New Zealand Standard Time
PLT	Pakistan Lahore Time
PNT	Phoenix Standard Time
PRT	Puerto Rico and US Virgin Islands Time
PST	Pacific Standard Time
SST	Solomon Standard Time
VST	Vietnam Standard Time

Switching

The Switching section of Configuration Manager enables you to configure the following objects:

- Agent Logins
- DNs
- DN Groups
- IVRs
- IVR Ports
- Places
- Place Groups
- Switches
- Switching Offices

Agent Logins

Agent Logins are unique codes defined within a Switch and assigned to agents. They identify which agent is working at which Place during a particular working session.

The configuration of Agent Logins in the Configuration Database must match exactly the configuration of those Agent Logins in the switching system. Before adding or deleting a particular Agent Login, make sure that the same change was made in the database of the switching system.

When you specify Agent Logins as objects in a Switch, they are not associated with any particular agents. For information about how to assign Agent Logins to agents, refer to Creating Agents.

Viewing Agent Logins

The **Agent Logins** list shows the Agent Logins that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

Important

- The **Switches** list displays when you select **Agent Logins** in Configuration Manager. To access the **Agent Logins** list, you must first select a Switch object and then an Agent Logins folder.
- Agent Logins that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

To select or de-select multiple objects at once, click **Select**.

Working with Agent Logins

To create a new Agent Login object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**.

To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Important**
>
> When you delete an Agent Login, the Agent Login is removed from the Configuration Database and from any Agent to which it is assigned. This might affect the configuration of a particular Agent in the contact center. Before deleting an Agent Login, consider viewing the dependencies tab to identify the Agent to which this Login is assigned. If you want to remove only the Agent Login from the Agent to which it is assigned, but leave it still existing in the Configuration Database and available for assignment to another Agent, open the User Account for the Agent, remove the Agent Login from the Agent, and click **Save**.

Otherwise, select the check box beside one or more objects and click **More** to perform the following tasks:

- **Clone**—Copy an Agent Login.
- **Move To**—Move an Agent Login to another hierarchical structure.
- Enable or disable Agent Logins
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of an Agent Login to view additional information about the object. You can also set options and permissions, and view dependencies.

Creating Agent Login Objects

To create an Agent Login, do the following:

[+] Show steps

1. Click the Switch object in which you wish to create an Agent Login.
2. Click the Agent Logins folder in which you wish to create an Agent Login.
3. Click **New**.
4. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Code**—The Agent Login code. You must specify a value for this property, and that value must be unique within the Switch. Once you set the value, you cannot change it.
   - **Switch**—The Switch to which this Agent Login belongs. This value is automatically set, based on the Switch being viewed in the **Agent Logins** list.
   - **Override**—Value to use as the override instead of the Code value for accessing this Agent Login in certain types of routing. You must specify an override value, and it must be unique within the Switch.

> **Important**
>
> To specify a value in the **Override** field, you must ensure the **Use Override** check box is checked.

- **Switch-specific Type**—An integer that corresponds to a combination of switch-specific settings for this Agent Login. It identifies the device type (for example, Extension, ACD Position, or Trunk) for each switch (PBX) that T-Server supports. It is unique for each switch/DN/T-Server configuration. In essence, it provides a cross-reference for DN Types between T-Server and PBX. You must specify a value for this property, and it must be 1 or greater. For more information, refer to the *Framework T-Server Deployment Guide* for your particular T-Server.
- **Password**—A security protection key used along with this Agent Login to authenticate a User for contact-center activity. You can associate one User with multiple password-protected Agent Logins.
- **Confirm Password**—Confirmation of the password entered in the **New Password** field.
- **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the `Tenant Directory` field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

5. Click **Save**.

You can also create a range of Agent Logins that share common properties. To create a range of Agent Logins, do the following:

<toggledisplay linkstyle font-size:larger showtext="[+] Show steps" hidetext="[-] Hide steps">
Navigate to the folder in which you wish to create the range. From the **More** menu, select **Create Range of Agent Logins**.

On the **Range of Agent Logins** tab, specify values for the following:

- **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the `Tenant Directory` field in the object list.
- **Switch**—The Switch to which this Agent Login belongs. This value is automatically set, based on the Switch being viewed in the **Agent Logins** list.
- **Start Code**—Numerical value of the starting range.
- **Number of Digits**—The number of digits that each Agent Login should have.
- **Number of Codes**—The number of codes that each Agent Login should have.

On the **General** tab, specify values for the following:

- **Use Override**—Select this option if you want to enable override.
- **Override**—Value to use as the override instead of the Code value for accessing this Agent Login in certain types of routing. You must specify an override value, and it must be unique within the Switch.

> **Important**
>
> To specify a value in the **Override** field, you must ensure the **Use Override** check box is checked.

- **Switch-specific Type**—An integer that corresponds to a combination of switch-specific settings for this Agent Login. It identifies the device type (for example, Extension, ACD Position, or Trunk) for each switch (PBX) that T-Server supports. It is unique for each switch/DN/T-Server configuration. In essence, it provides a cross-reference for DN Types between T-Server and PBX. You must specify a value for this property, and it must be 1 or greater. For more information, refer to the *Framework T-Server Deployment Guide* for your particular T-Server.
- **Password**—A security protection key used along with this Agent Login to authenticate a User for contact-center activity. You can associate one User with multiple password-protected Agent Logins.
- **Confirm Password**—Confirmation of the password entered in the **New Password** field.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

On the **Options** tab, you can add or manage any options for this range of Agent Logins.

CSV File for Importing and Exporting

You can use the Bulk Import/Export functionality to import Agent Logins from, and export Agent Logins to, a comma-separated value (CSV) file. The import file used for importing and the export file created by exporting data are fully compatible, and a single file can be used for both importing and exporting. Or, if you wish, you can create the import file yourself, using the information on this page.

Fields of the CSV File

The source file is a text file in a comma-separated (CSV) format, with an extension of **.csv**.

In the source file each line represents a single Agent Login. The same Agent Login can appear in the source file only once. The unique identifier of the Agent Login in the scope of the source file is the Code field.

The columns of the file are the properties of an Agent Login. The first row in the file has column names to identify the fields. The order of the columns is not important. A comma is inserted after each column header or value, or if the column does not have a value, immediately after the previous comma. Any non-mandatory column can be omitted from the source file, depending on user preference and/or the purpose of the file.

The source file contains the following properties for each Agent Login:

Name	Type	Mandatory	Description
Action	ADD, UPDATE, DELETE	Yes	Specifies the action to be taken with this Agent Login data, either create

Name	Type	Mandatory	Description
			a new Agent Login (ADD) or modify the existing Agent Login (UPDATE) or delete the existing Agent Login (DELETE). This column is added automatically by GAX when a file is exported, with a value of UPDATE for all records in it. If you create the source file from scratch, you must add this column manually. In either case, this field is mandatory, and you must provide a value for each record.
Code	String	Yes	Agent Login number or name.
Switch	String	Yes	Name of the Switch under which this Agent Login is created.
Switch Specific Type	Integer	Yes	An integer that corresponds to a combination of switch-specific settings for this Agent Login. It identifies the device type (for example, Extension, ACD Position, or Trunk) for each switch (PBX) that T-Server supports. It is unique for each switch/DN/T-Server configuration. In essence, it provides a cross-reference for DN Types between T-Server and PBX. You must specify a value for this property, and it must be 1 or greater.
Enabled	String	No	Whether this Agent Login is enabled (`Y`) or not (`N`).

Example

The following data is to be uploaded to GAX to create two new Agent Logins and update an existing one:

Action	Code	Switch	Switch-specific Type	Enabled
ADD	214	Switch1	3	Y
ADD	215	Switch2	5	Y
UPDATE	212	Switch1	7	Y

The contents of the CSV file for this data looks like this:

```
Action,Code,Switch,Switch-Specific Type,Enabled
ADD,214,Switch1,3,Y
ADD,215,Switch2,5,Y
ADD,212,Switch1,7,Y
```

DNs

DNs are communication devices, uniquely identified by their directory numbers (DNs), where customer interactions (for example, telephone calls or emails) reside and are handled.

Because most types of DNs represent the actual devices of the telephone system, their specification in the Configuration Database must always correspond to their Switch settings. Remember that Genesys Administrator Extension has no way of verifying this correspondence.

As a general rule, changes made to DN configurations in the Configuration Database must always follow the changes made to DNs within the telephone system, and never the other way around.

Viewing DNs

The **DNs** list shows the DNs that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

Important

- The **Switches** list displays when you select **DNs** in Configuration Manager. To access the **DNs** list, you must first select a Switch object and then a DN folder.
- DNs that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

Click **Group By** to group objects by various criteria.

To select or de-select multiple objects at once, click **Select**.

DN Types

A DN is categorized as one of the following types:

[+] Show types

DN Type	Description
Access Resource	A Switch access resource to be used in a multi-site environment for external routing.
ACD Position	An extension designated for customer interactions only.
ACD Queue	A device in a Switch, typically associated with a number of targets, where customer interactions wait while the control system is looking for an available target.
Call Processing Port	An extension connected to a call-processing equipment port.
Chat	A Chat address.
CoBrowse	A Co-Browse address.
Communication DN	A virtual device that applications use to communicate with each other through the User Event mechanism.
E-mail Address	An email address.
Extension	A regular extension line.
External Routing Point	An ISCC (Inter Server Call Control) resource dedicated to supporting the external routing and call overflow functions.
Fax	An extension connected to a fax machine.
Mixed	An extension line that can be used as both an Extension and an ACD Position.
Mobile Station	A mobile station.
Modem	An extension connected to data communication equipment.
Music Port	A music source.
Network Destination	A destination number in network routing.
Routing Point	A device in a Switch, not associated with any particular target, where customer interactions wait while a routing application is making routing decisions.
Routing Queue	A telephony device that can be used as both a Routing Point and an ACD Queue.
Service Number	A service number used as a Routing Point in network routing.
Tie Line	A direct communication channel between two Switches of a private telephone network.

DN Type	Description
Tie Line Group	A group of tie lines forming one route.
Trunk	A communication channel between the public telephone network and a private telephone network.
Trunk Group	A group of trunks forming one route.
Video over IP Port	A video channel.
Virtual Queue	A virtual device, created and maintained by the switch, with activity identical to an ACD Queue.
Virtual Routing Point	A virtual device, created and maintained by the switch, with activity identical to a Routing Point.
Voice Mail	A voice mail channel.
Voice over IP Port	A Voice over IP (VoIP) Port.
Voice over IP Service	A VoIP Service.
Voice Treatment Port	An extension connected to an electronic audio equipment port (for example, IVR).
Workflow	A Workflow resource.

Working with DNs

To create a new DN object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**.

To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> ### Important
> When you delete a DN, it is removed from the Configuration Database and from any DN Group of which it is a member. If you want to remove only the DN from a DN Group of which it is a member, but leave it still existing in the Configuration Database and available for assignment to another DN Group, you must remove it from the DNs tab of the DN Group.

Otherwise, click **More** to perform the following tasks:

- **Clone** — Copy a DN.
- **Move To** — Move a DN to another hierarchical structure.
- Enable or disable DNs.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a DN to view additional information about the object. You can also set options and

permissions, and view dependencies.

Creating DNs

To create a DN, do the following:

[+] Show steps

1. Click the Switch object in which you wish to create a DN.
2. Click the DN folder in which you wish to create a DN.
3. Click **New**.
4. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Number**—A directory number assigned to this DN within the Switch. You must specify a value for this property, and that value must be unique within the Switch for all DN types except the **Destination Label** type. Once you set the value, you cannot change it. Genesys Administrator Extension does not verify the correspondence between the numbers assigned to DNs and the switch's numbering plan defined by the **DN Range** property of the Switch. If, according to T-Server specifications, such correspondence is important in an environment, make sure that the specified **DN Range** covers all DN numbers that are defined within the Switch in question.
   - **Type**—The type of DN. Once you set the value, you cannot change it.
   - **Switch**—The Switch to which this DN belongs. You must specify a value for this property. Once you set the value, you cannot change it.
   - **Association**—An entity permanently associated with this DN (for example, an IVR port number, channel name, or access number). For DNs of **External Routing Point** type, this number may be required to substitute for the actual DN directory number and may be used when placing calls to this routing point from another Switch.
   - **Register**—Indicates whether T-Server must register this DN within the Switch. You must specify a value for this property. From the drop-down menu, select one of the following values:
     - **False**—T-Server should never register the DN in question on the Switch, but process it locally.
     - **True**—T-Server should always register the DN on the Switch during T-Server startup or reconnection.
     - **On-Demand**—T-Server should register the DN only when a T-Server client requests the registration. Consult T-Server documentation for more information.

     > **Warning**
     > The last two values force T-Server to register this DN regardless of whether it is enabled or disabled.

   - **Alias**—An alternative name for this DN. You must specify a value for this property if the DN is used as a target in routing instructions. If you specify this value, it must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Route Type**—The type of routing that applies to this DN. You must specify a value for this property.

- DN Group—The DN Group to which this DN belongs.
- **Override**—Value to use as the override instead of the number or name value for accessing this DN in certain types of routing. You must specify an override value, and it must be unique within the Switch.

> **Important**
>
> To specify a value in the **Override** field, you must ensure the **Use Override** check box is checked.

- **Login ID**—The login identifier used to activate this DN. Some types of switching systems require that the login code used to activate a particular DN be permanently associated with this DN. In that case, the Login ID may be applicable to the following types of DNs: **ACD Position**, **Extension**, **Voice Treatment Port**, **Voice Mail**, or **Mixed**.
- **Switch-specific Type**—An integer that corresponds to a combination of switch-specific settings for this DN. It identifies the device type (for example, **Extension**, **ACD Position**, or **Trunk**) for each switch (PBX) that T-Server supports. It is unique for each switch/DN/T-Server configuration. In essence, it provides a cross-reference for DN Types between T-Server and PBX. You must specify a value for this property, and it must be 1 or greater. For more information, refer to the *Framework T-Server Deployment Guide* for your particular T-Server.
- **Number of Trunks**—The number of trunks associated with this DN. It applies only if the Type property has a **Network Destination** value. The default value is `0`.
- **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

5. Click **Save**.

You can also create a range of DNs that share common properties. To create a range of DNs, do the following:

[+] Show steps

Navigate to the DN folder in which you wish to create a range of DNs. From the **More** menu, select **Create Range of DNs**.

On the **Range of DNs** tab, specify values for the following:

- **DN Prefix** (optional)—Prefix used to create the DNs.
- **DN Suffix** (optional)—Suffix used to create the DNs.
- **Start**—Numerical value of the starting range.
- **Number of Digits**—The number of digits that each DN should have.
- **DN Count**—The number of DNs to create.

On the **General** tab, specify values for the following:

- **Type**—The type of DN to use for this range of DNs. Once you set the value, you cannot change it.
- **Association**—An entity permanently associated with this range of DNs (for example, an IVR port number, channel name, or access number). For DNs of **External Routing Point** type, this number may be required to substitute for the actual DN directory number and may be used when placing calls to this routing point from another Switch.
- **Register**—Indicates whether T-Server must register these DNs within the Switch. You must specify a value for this property. From the drop-down menu, select one of the following values:
  - **False**—T-Server should never register the DNs in question on the Switch, but process it locally.
  - **True**—T-Server should always register the DNs on the Switch during T-Server startup or reconnection.
  - **On-Demand**—T-Server should register the DNs only when a T-Server client requests the registration.

> **Warning**
>
> The last two values force T-Server to register the DNs regardless of whether they are enabled or disabled. Consult T-Server documentation for more information.

- **Alias**—An alternative name for this range of DNs. You must specify a value for this property if the DNs are used as targets in routing instructions. If you specify this value, it must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
- **Route Type**—The type of routing that applies to this range of DNs. You must specify a value for this property.
- DN Group—The DN Group to which this range of DNs belong.
- **Override**—Value to use as the override instead of the number or name value for accessing these DNs in certain types of routing. You must specify an override value, and it must be unique within the Switch.

> **Important**
>
> To specify a value in the **Override** field, you must ensure the **Use Override** check box is checked.

- **Login ID**—The login identifier used to activate this range of DNs. Some types of switching systems require that the login code used to activate a particular DN be permanently associated with the DN. In that case, the Login ID may be applicable to the following types of DNs: **ACD Position**, **Extension**, **Voice Treatment Port**, **Voice Mail**, or **Mixed**.
- **Switch-specific Type**—An integer that corresponds to a combination of switch-specific settings for this range of DNs. It identifies the device type (for example, **Extension**, **ACD Position**, or **Trunk**) for each switch (PBX) that T-Server supports. It is unique for each switch/DN/T-Server configuration. In essence, it provides a cross-reference for DN Types between T-Server and PBX. You must specify a value for this property, and it must be 1 or greater. For more information, refer to the *Framework T-Server Deployment Guide* for your particular T-Server.
- **Number of Trunks**—The number of trunks associated with this range of DNs. It applies only if the Type property has a **Network Destination** value. The default value is `0`.

- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

On the **Options** tab, you can add or manage any options for this range of DNs.

CSV File for Importing and Exporting

You can use the Bulk Import/Export functionality to import DNs from, and export DNs to, a comma-separated value (CSV), file. The import file used for importing and the export file created by exporting data are fully compatible, and a single file can be used for both importing and exporting. Or, if you wish, you can create the import file yourself, using the general CSV information in this Help file, and the object-specific information contained in this section.

Fields of the CSV File

The source file is a text file in a comma-separated (CSV) format, with an extension of **.csv**.

In the source file each line represents a single DN. The same DN can appear in the source file only once. The unique identifier of the DN in the scope of the source file is the Number field.

The columns of the file are the properties of a DN. The first row in the file has column names to identify the fields. The order of the columns is not important. A comma is inserted after each column header or value, or if the column does not have a value, immediately after the previous comma. Any non-mandatory column can be omitted from the source file, depending on user preference and/or the purpose of the file.

The source file contains the following properties for each user/agent:

Name	Type	Mandatory	Description
Action	ADD, UPDATE, DELETE	Yes	Specifies the action to be taken with this DN data, either create a new DN (ADD) or modify an existing DN (UPDATE) or delete a DN (DELETE). This column is added automatically by GAX when a file is exported, with a value of UPDATE for all records in it. If you create the source file from scratch, you must add this column manually. In either case, this field is mandatory, and you must provide a value for each record.
Number	String	Yes	DN number or name.
Type	String	Yes	Type of DN.
Switch	String	Yes	Name of the Switch

Name	Type	Mandatory	Description
			under which this DN is created.
Register	String	Yes	Specifies whether the DN is registered. Valid Values: `Y`, `N`, `On-Demand`
Alias	String	No	An alternative name for this DN. You must specify a value for this property if the DN is used as a target in routing instructions.
Route Type	String	Yes	Route type of this DN.
Association	String	No	Association field value of this DN.
Switch Specific Type	String	No.	Switch-specific Type field value of this DN.
Enabled	String	No	Whether this DN is enabled (`Y`) or not (`N`).
Section | Option | Value	String	No	Options associated with this DN. **Note:** Any special characters in the key/value are escaped by using a back slash (`\`). For example: `\,=\,\,` where "," (comma) is the key and “,,” (comma,comma) is the value.

Example

The following data is to be uploaded to GAX to create two DNs:

Action	Number	Type	Switch	Register	Route Type	Enabled
ADD	2389273	Chat	Switch1	Y	Default	Y
ADD	7843920	Fax	Switch1	Y	Default	Y

The contents of the CSV file for this data looks like this:

```
Action,Number,Type,Switch,Register,Route Type,Enabled
ADD,2389273,Chat,Switch1,Y,Default,Y
ADD,7843920,Fax,Switch1,Y,Default,Y
```

DN Groups

DN Groups are logical groupings of DNs. You can use DN Groups in network-level routing algorithms and in some types of statistics. To determine if you need to set up DN Groups, refer to your solution-specific documentation.

When you are specifying a DN Group, remember that the DNs in each DN Group must have the same telephony event model.

Although a DN Group can contain DNs that belong to a number of different Switches, you can receive correct statistical information about this DN Group only if the reporting applications connect to the servers associated with those Switches.

DN Group Types

The following are DN Group types and types of DNs that you can include in a group:

[+] Show types

DN Group Type	Compatible DN Types
ACD Queues	ACD Queue, Routing Queue, and Virtual Queue
Network Ports	Network Destination
Routing Points	Routing Point, External Routing Point, Routing Queue, and Virtual Routing Point
Service Numbers	Service Number
Single Ports	Extension, ACD Position, Call Processing Port, Music Port, Communication DN, E-mail Address, Modem, Fax, Chat, CoBrowse, Voice over IP Port, Video over IP Port, Voice Treatment Port, and Voice Mail

Viewing DN Groups

The **DN Groups** list shows the DN Groups that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> DN Groups that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working With DN Groups

To create a new DN Group object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**.

To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> ### Important
> When you delete a DN Group, only the DN Group object itself is removed from the Configuration Database. Its member DN objects are not deleted.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a DN Group.
- **Move To**—Move a DN Group to another hierarchical structure.
- Enable or disable DN Groups.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Creating DN Groups

To create a DN Group, do the following:

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the DN Group. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment). You cannot change this value as long as this DN Group contains at

least one DN.

- **Type**—The type of the DN Group. Once you set the value, you cannot change it.
- **Capacity Table**—This field applies only for the Enterprise Routing Solution. It is the Capacity Table associated with this DN Group. Refer to Enterprise Routing Solution documentation for more information.
- **Quota Table**—This field applies only for the Enterprise Routing Solution. It is the Quota Table associated with this DN Group. Refer to Enterprise Routing Solution documentation for more information.
- **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. The **Origination DNs** tab lists DNs from which calls can be routed or diverted to this DN Group.

> **Important**
>
> You can include DNs of the following types into this list: **Routing Point**, **External Routing Point**, **Service Number**, **Routing Queue**, **ACD Queue**, **Virtual Queue**, or **Virtual Routing Point**.

For each DN to be added to the list of Origination DNs for this Group:

a. Click the **Origination DNs** tab and click **Add**.

b. Navigate to the appropriate folder, if necessary, and do one of the following:

- To add an existing DN to the list of Origination DN for this Group, select it from the list of DNs.
- To add a new DN to the list of Origination DN for this Group, click **+** to create the DN in this folder and then select it from the list.

4. For each DN that you want to add as a member of this DN Group:

a. Click the **DNs** tab and click **Add**.

b. Navigate to the appropriate folder, if necessary, and do one of the following:

- To add existing DNs to this Group, select a single or multiple DN(s) from the list of DNs and click **Add**.
- To add a new DN to this Group, click **+** to create the DN in this folder and then select it from the list.

> **Important**
>
> Although an Origination DN can be configured for a DN Group, it is not used by Stat Server or any of the reporting components. Therefore, this would typically only be done if required for a specific type of scenario.
>
> When an Origination DN is configured for an Agent Group or Place Group, Stat Server associates Virtual Queue activity with the linked Agent Groups, and also associates DN activity related to the Agent Group back to the mediation DNs.
>
> For more information, see DN Association with Queues in the *Stat Server User's Guide*. You can also refer to the following Stat Server Actions:

- Durable Group Actions Reflecting Origination DNs
- Retrospective Group Actions Reflecting Origination DNs
- Momentary Group Actions Reflecting Origination DNs
- Generation of Retrospective, Interaction-Related Actions Reflecting Regular DNs for Virtual Queue Mediation DN Objects

- After you have finished creating the DN Group, do one of the following:
  - Click **Save** to accept the changes and return to the list of DN Groups.
  - Click **Apply** to accept the changes and return to the **General** tab of this DN Group.
  - Click **Cancel** to discard the changes.

CSV File for Importing and Exporting

You can use the Bulk Import/Export functionality to import DN Groups from, and export DN Groups to, a comma-separated value (CSV), file. The import file used for importing and the export file created by exporting data are fully compatible, and a single file can be used for both importing and exporting. Or, if you wish, you can create the import file yourself, using the general CSV information in this Help file, and the object-specific information contained in this section.

Fields of the CSV File

The source file is a text file in a comma-separated (CSV) format, with an extension of **.csv**.

In the source file each line represents a single DN Group. The same DN Group can appear in the source file only once. The unique identifier of the DN Group in the scope of the source file is the field.

The columns of the file are the properties of a DN Group. The first row in the file has column names to identify the fields. The order of the columns is not important. A comma is inserted after each column header or value, or if the column does not have a value, immediately after the previous comma. Any non-mandatory column can be omitted from the source file, depending on user preference and/or the purpose of the file.

The source file contains the following properties for each user/agent:

Name	Type	Mandatory	Description
Action	ADD, UPDATE, DELETE	Yes	Specifies the action to be taken with this DN Group data, either create a new DN Group (ADD) or modify a DN Group (UPDATE) or delete a DN Group

Name	Type	Mandatory	Description
			(DELETE). This column is added automatically by GAX when a file is exported, with a value of UPDATE for all records in it. If you create the source file from scratch, you must add this column manually. In either case, this field is mandatory, and you must provide a value for each record.
Name	String	Yes	Name of DN Group.
Type	String	Yes	Type of DN Group.
Enabled	String	No	This DN Group is enabled (Y) or not enabled (N).
Section | Option | Value	String	No	Options associated with this DN Group. **Note:** Any special characters in the key/value are escaped by using a back slash (\). For example: `\,=\,\,` where "," (comma) is the key and “,,” (comma,comma) is the value.

Relational Columns

In addition to the properties and folders in the table above, each row may contain relations between this DN Group and DN objects. Every instance of a DN will have a separate column in the source file. For example, if there are 10 DNs, there will be 10 additional columns in the source file, each column representing each DN. All relational columns are optional.

Each header for a relational column consists of the object type and the object name, which will form a unique column name. So, for example, there cannot be two Skills which have the same name, but a Skill object may have the same name as some Switch object.

Naming and value rules of relational columns are given in the following table:

Relational Columns

Type	Column Name	Valid Values	Description
DN	DN:<switch name> / <DN number>	Y – Add this DN to this DN Group N – Remove this DN from this DN Group <empty> - No action	A DN to be added or removed to this DN Group.

Example

The following data is to be uploaded to GAX to modify two DN Groups:

[+] Show data

Action	Name	Type	DN:Switch1 / 123683	DN:Switch2 / 857463	Enabled
MODIFY	DNGroupEast	Routing Points	Y		Y
MODIFY	DNGroupWest	Routing Points	N	Y	Y

The contents of the CSV file for this data looks like this:

```
Action,Name,Type,DN:Switch1 / 123683,DN:Switch2 / 857463,Enabled
MODIFY,DNGroupEast,Routing Points,Y,,Y
MODIFY,DNGroupWest,Routing Points,N,Y,Y
```

IVRs

IVRs (Interactive Voice Responses) are telephony objects consisting of IVR Ports; they are controlled through IVR interface drivers.

When you register a new IVR in the Configuration Database, an IVR Ports folder is automatically created under this IVR.

IVR Ports are telephony objects uniquely identified by the numbers within IVRs at which telephone calls may reside and be handled.

Viewing IVRs

The **IVRs** list shows the IVRs that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
>
> IVRs that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with IVRs

To create a new IVR object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Warning**
> When you delete an IVR, this also deletes all IVR Ports specified within the IVR. Their deletion might in turn cause modifications in other objects.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy an IVR.
- **Move To**—Move an IVR to another hierarchical structure.
- Enable or disable IVRs.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of an IVR to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating IVR Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the IVR. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Description**—A brief description of the IVR.
   - **Type**—The type of this IVR. You must specify a value for this property.
   - **Version**—The version of the IVR. You must specify a value for this property.
   - **IVR Server**—The name of the Application of the IVR Interface Server type that serves this IVR.
   - **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. In the **IVR Ports** tab, click **Add** to add an IVR Port.

4. Click **Save**.

> **Important**
>
> IVR Ports are configured as separate objects. They can be created and configured only after the associated IVR has been created.

IVR Ports

IVR (Interactive Voice Response) Ports are telephony objects uniquely identified by the numbers within IVRs at which telephone calls may reside and be handled.

When you register a new IVR in the Configuration Database, an IVR Ports folder under this IVR is automatically created. An IVR Port can, therefore, be created only when the associated IVR is created.

Viewing IVR Ports

The **IVR Ports** list shows the IVR Ports that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

Important

- The **IVRs** list displays when you select **IVR Ports** in Configuration Manager. To access the **IVR Ports** list, you must first select an IVR object and then an IVR Ports folder.
- IVR Ports that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with IVR Ports

To create a new IVR Port object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Warning**
> When you delete an IVR Port, this might affect some objects in the configuration. To see associations between an IVR Port and other objects, use the **Dependencies** tab.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy an IVR Port.
- **Move To**—Move an IVR Port to another hierarchical structure.
- Enable or disable IVR Ports.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of an IVR Port to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating IVR Port Objects

Prerequisites

You have created the IVR with which these Ports are associated.

Steps

1. In the **IVRs** list, click the IVR object in which you wish to create an IVR Port.
2. Click the IVR Ports folder in which you wish to create an IVR Port.
3. Click **New**.
4. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** button to select a value from a list:
   - **Port Number**—The number associated with a channel on an IVR. You must specify a value for this property, and that value can be equal to `0` (zero) or any positive integer. It must be unique within the IVR with which it is associated.
   - **Description**—A brief description of the IVR Port.
   - IVR—The IVR to which this IVR Port belongs. This value is automatically set, and you cannot change it.
   - Associated DN—The DN associated with this IVR Port.
   - Associated Switch—The Switch associated with this IVR Port.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the

object list.

- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

5. Click **Save**.

Places

A Place is a location that has one or more DNs operated by a single agent.

You configure Places and assign individual DNs to them in order to monitor performance and availability of Agents, Agent Groups, and Place Groups, and to provide this information to call-processing applications.

A typical Agent Place consists of two DNs: one DN that an Agent uses to take customer calls, and one DN that the Agent uses to make consultation calls and transfers.

If you are using the multimedia options of the Genesys products, Places may need to be equipped with DNs of other types, such as an email address.

Viewing Places

The **Places** list shows the Places that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
> Places that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

To select or de-select multiple objects at once, click **Select**.

Working with Places

To create a new Place object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**.

To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Important**
>
> When you delete a Place, it is removed from the Configuration Database and from any Place Group of which it is a member. If you want to remove the Place from a Place Group of which it is a member, but leave it in the Configuration Database and available for membership in another Place Group, remove the Place from the Place Group.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Place.
- **Move To**—Move a Place to another hierarchical structure.
- Enable or disable Places.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Creating Place Objects

To create a place object, do the following:

[+] Show steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of this Place. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - Capacity Rule—The Capacity Rule Script associated with this Place.
   - Cost Contract—The Cost Contract associated with this Place.
   - **Site**—The Site with which the Capacity Rule and/or Cost Contract is associated. If the Capacity Rule or Cost Contract are associated with a Site, this field is set to that Site.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. In the **DNs** tab, click **Add** to add a single or multiple DN(s). Navigate to the appropriate DN folder and select the available DN(s) you want to add, and then click **Add**. In the pop-up window, you can create a new DN object by clicking **+**.
4. Perform one of the following actions after you have added a DN to the Place:
   - Click **Save** to accept the changes and return to the object list.

- Click **Apply** to accept the changes and remain in the tab.
- Click **Cancel** to discard the changes.

5. Click **Save**.

You can also create a range of Places that share common properties. To create a range of Places, do the following:

[+] Show steps

Navigate to the Places folder in which you wish to create a range of Places. From the **More** menu, select **Create Range of Places**.

On the **Range of Places** tab, specify values for the following:

- **Tenant**—This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **Place Name Base** (optional)—This value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
- **Place Prefix** (optional)—Prefix used to create the Places.
- **Place Suffix** (optional)—Suffix used to create the Places.
- **Start**—Numerical value of the starting range.
- **Number of Digits**—The number of digits that each Place should have.
- **Place Count**—The number of Places to create.

On the **General** tab, specify values for the following:

- Capacity Rule—The Capacity Rule Script associated with this Place.
- Cost Contract—The Cost Contract associated with this Place.
- **Site**—The Site with which the Capacity Rule and/or Cost Contract is associated. If the Capacity Rule or Cost Contract are associated with a Site, this field is set to that Site.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

On the **DNs** tab, click **Add** to add a single or multiple DN(s). Navigate to the appropriate DN folder and select the available DN(s) you want to add, and then click **Add**. In the pop-up window, you can create a new DN object by clicking **+**.

On the **Options** tab, you can add or manage any options for this range of Places.

CSV File for Importing and Exporting

You can use the Bulk Import/Export functionality to import Places from, and export Places to, a comma-separated value (CSV), file. The import file used for importing and the export file created by

exporting data are fully compatible, and a single file can be used for both importing and exporting. Or, if you wish, you can create the import file yourself, using the general CSV information in this Help file, and the object-specific information contained in this section.

Fields of the CSV File

The source file is a text file in a comma-separated (CSV) format, with an extension of **.csv**.

In the source file, each line represents a single Place. The same Place can appear in the source file only once. The unique identifier of the Place in the scope of the source file is the Name field.

The columns of the file are the properties of a Place, and optionally, the DNs associated with that Place. The first row in the file has column names to identify the fields. The order of the columns is not important. A comma is inserted after each column header or value, or if the column does not have a value, immediately after the previous comma. Any non-mandatory column can be omitted from the source file, depending on user preference and/or the purpose of the file.

The source file contains the following properties for each Place:

Name	Type	Mandatory	Description
Action	ADD, UPDATE, DELETE	Yes	Specifies the action to be taken with this Place data, either create a new Place (ADD) or modify the existing Place (UPDATE) or delete a Place (DELETE). This column is added automatically by GAX when a file is exported, with a value of UPDATE for all records in it. If you create the source file from scratch, you must add this column manually. In either case, this field is mandatory, and you must provide a value for each record.
Name	String	Yes	Name of the Place.
Enabled	String	No	Whether this Place is enabled (Y) or not (N).
Section | Option | Value	String	No	Options associated with this Place. **Note:** Any special characters in the key/value are escaped by using a back slash (\). For example: `\,=\,\,` where "," (comma) is the key and “,,” (comma,comma) is the value.

Relational Columns

In addition to the properties and folders in the table above, each row may contain relations between this Place and DNs. Every instance of a DN will have a separate column in the source file. For example, if there are 10 DNs, there will be 10 additional columns in the source file, each column representing a DN. All relational columns are optional.

Each header for a relational column consists of the object type and the object name, which will form a unique column name. So, for example, there cannot be two Skills which have the same name, but a Skill object may have the same name as some Switch object.

Naming and value rules of relational columns are given in the following table:

Relational Columns

Type	Column Name	Valid Values	Description
DN	DN:<switch name> / <DN number>	Y – Add this DN to this Place N – Remove this DN from this Place <empty> - No action	A DN to be added or removed from this Place.

Example

The following data is to be uploaded to GAX to modify two Places:

Action	Name	Enabled	DN:2410241	DN:4340241	DN:2140879
UPDATE	_admin	Y	Y		N
UPDATE	_support	Y	N	N	Y

The contents of the CSV file for this data looks like this:

```
Action,Name,Enabled,DN:2410241,DN:4340241,DN:2140879
UPDATE,_admin,Y,Y,,N
UPDATE,_support,Y,N,N,Y
```

Place Groups

Place Groups are logical groupings of Places. You can group Places if, according to the call-processing algorithms, the calls must be distributed among a set of Places under the control of applications instead of through the ACD mechanisms of the Switch.

As an example, consider a call-parking service: A Routing application transfers a call to a port that is assigned to a call-parking Place Group; then, while the call is parked, the application attaches information about the treatment to be applied to it.

Viewing Place Groups

The **Place Groups** list shows the Place Groups that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Place Groups that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

To select or de-select multiple objects at once, click **Select**.

Working with Place Groups

To create a new Place Group object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**.

To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Important**
> When you delete a Place Group, only the Place Group object itself is removed from the Configuration Database. Its member Place objects are not deleted.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Place Group.
- **Move To**—Move a Place Group to another hierarchical structure.
- Enable or disable Place Groups.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Creating Place Groups

To create a Place Group, do the following:

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Place Group. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment). You cannot change this value as long as this Place Group contains at least one Place.
   - **Capacity Table**—This field applies only to the Enterprise Routing Solution. It is the Capacity Table associated with this Place Group. Refer to Enterprise Routing Solution documentation for more information.
   - **Quota Table**—This field applies only to the Enterprise Routing Solution. It is the Quota Table associated with this Place Group. Refer to Enterprise Routing Solution documentation for more information.
   - Cost Contract—The Cost Contract associated with this Place Group.
   - **Site**—The Site containing this Cost Contract.
   - **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. The **Origination DNs** tab lists DNs from which calls can be routed or diverted to this Place Group. You can include DNs of the following types into this list: **Routing Point**, **External Routing Point**, **Service Number**, **Routing Queue**, **ACD Queue**, **Virtual Queue**, or **Virtual Routing Point**. For each DN to be added to the list of Origination DNs for this Group:
   a. Click the **Origination DNs** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To add an existing DN to the list of Origination DN for this Group, select it from the list of DNs.

- To add a new DN to the list of Origination DN for this Group, click **+** to create the DN in this folder and then select it from the list.

4. For each Place that you want to add as a member of this Place Group:
   a. Click the **Places** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To add an existing Place to this Group, select it from the list of Places.
      - To add a new Place to this Group, click **+** to create the Place in this folder and then select it from the list.
5. After you have finished creating the DN Group, do one of the following:
   - Click **Save** to accept the changes and return to the list of Place Groups.
   - Click **Apply** to accept the changes and return to the **General** tab of this Place Group.
   - Click **Cancel** to discard the changes.

CSV File for Importing and Exporting

You can use the Bulk Import/Export functionality to import Place Groups from, and export Place Groups to, a comma-separated value (CSV), file. The import file used for importing and the export file created by exporting data are fully compatible, and a single file can be used for both importing and exporting. Or, you can create the import file yourself, using the general CSV information in this Help file, and the object-specific information contained in this section.

Fields of the CSV File

The source file is a text file in a comma-separated (CSV) format, with an extension of **.csv**.

In the source file each line represents a single Place Group. The same Place Group can appear in the source file only once. The unique identifier of the Place Group in the scope of the source file is the Name field.

The columns of the file are the properties of a Place Group, and optionally the Places in that group. The first row in the file has column names to identify the fields. The order of the columns is not important. A comma is inserted after each column header or value, or if the column does not have a value, immediately after the previous comma. Any non-mandatory column can be omitted from the source file, depending on user preference and/or the purpose of the file.

The source file contains the following properties for each user/agent:

Name	Type	Mandatory	Description
Action	ADD, UPDATE, DELETE	Yes	Specifies the action to be taken with this Place Group data, either create a new Place Group (ADD) or modify the existing Place Group

Name	Type	Mandatory	Description
			(UPDATE) or delete a Place Group (DELETE). This column is added automatically by GAX when a file is exported, with a value of UPDATE for all records in it. If you create the source file from scratch, you must add this column manually. In either case, this field is mandatory, and you must provide a value for each record.
Name	String	Yes	Name of Place Group.
Enabled	String	No	Whether this Place Group is enabled (Y) or not (N).
Section | Option | Value	String	No	Options associated with this Place Group. **Note:** Any special characters in the key/value are escaped by using a back slash (\). For example: `\,=\,\,` where "," (comma) is the key and “,,” (comma,comma) is the value.

Relational Columns

In addition to the properties and folders in the table above, each row may contain relations between this Place Group and Places. Every instance of a Place will have a separate column in the source file. For example, if there are 10 Places, there will be 10 additional columns in the source file, each column representing each Place. All relational columns are optional.

Each header for a relational column consists of the object type and the object name, which will form a unique column name. So, for example, there cannot be two Places that have the same name, but a Place object may have the same name as a Place Group object.

Naming and value rules of relational columns are given in the following table:

Relational Columns

Type	Column Name	Valid Values	Description
Place	Place:<place name>	Y – Add this Place to this Place Group N – Remove this Place from this Place Group <empty> - No action	A Place to be added or removed to this Place Group.

Example

The following data is to be uploaded to GAX to modify two Place Groups:

Action	Name	Enabled	Place:DMS_2001	Place:DMS_2002	Place:Mobile_4001	Place:Mobile_4002
UPDATE	DMS_PlaceGroup	Y	Y	Y		
UPDATE	Mobile_PlaceGroup	Y	N	N	Y	Y

The contents of the CSV file for this data looks like this:

```
Action,Name,Enabled,Place:DMS_2001,Place:DMS_2002,Place:Mobile_4001,Place:Mobile_4002
UPDATE,DMS_PlaceGroup,Y,Y,Y,,
UPDATE,Mobile_PlaceGroup,Y,N,N,Y,Y
```

Switches

A Switch is an aggregate of telephony resources within a Switching Office.

Most enterprise-level configurations have a one-to-one match between the Switches and the Switching Offices. However, there may be instances when it is desirable to partition the office into more than one Switch or to create a more efficient and secure numbering plan. In that case, you must define a Switch within a Switching Office.

In the event of the loss of all components at a single site, a Disaster Recovery (DR) strategy is required to ensure that there is a minimal disruption in service. The central part of this strategy is the existence of synchronized switches located at separate sites, and configured with identical sets of Agent extensions and Agent Logins. An agent can log in to either switch at any time.

The Disaster Recovery strategy implemented by Genesys for Genesys components applies to Switches of type **SIP Switch**. To configure Disaster Recovery for Genesys components, at least one Switch must exist in the Configuration Database.

For additional information about Disaster Recovery, refer to the SIP Server High-Availability Deployment Guide.

Viewing Switches

The **Switches** list shows the Switches that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
> Switches that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

To select or de-select multiple objects at once, click **Select**.

Working with Switches

To create a new Switch object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Switch.
- **Move To**—Move a Switch to another hierarchical structure.
- Enable or disable Switches.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Switch to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Switch Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Switch. You must specify a value for this property, and that value must be unique within this Tenant (in a multi-tenant environment).
   - **Switching Office**—The Switching Office to which this Switch belongs. You must specify a value for this property. Once you set the value, you cannot change it.
   - **Switch Type**—The type of Switching Office to which this Switch belongs. This value is set automatically.
   - **T-Server**—The T-Server Application object through which the telephony objects of this Switch are controlled. Once you establish the association, it cannot be broken as long as the specified T-Server has at least one client application.
   - **DN Range**—The internal numbering plan of the Switch. Use a hyphen to specify a range of numbers, and use commas to specify a series of stand-alone numbers or ranges—for example, `1100-1179, 1190-1195, 1199`. Although this parameter is optional, it may be important for T-Server operation with certain types of Switches.
   - **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.

- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. The **Access Codes** tab displays a list of Access Codes that are used to place, route, or transfer calls from this Switch to other Switches in a multi-site installation. Depending on the structure of a numbering plan, you may or may not need access codes to reach DNs that belong to different Switches of a multi-site telephone network. Click **Add** to add an Access Code to this Switch.
4. Enter the following information in the pop-up window that displays on your screen:
   - **Switch**—The Switch to which you assign this Access Code.
   - **Code**—The prefix used to reach DNs of the Switch specified in the Switch property when placing or transferring calls from DNs of the Switch to the object for which you are configuring. You must specify a value for this property. You must specify an Access Code in full accordance with the numbering plan of the contact center telephone network, and you must make any changes to the Access Codes only after the corresponding changes have been made to the telephone network.
   - **Target Type**—The type of target within the Switch for which you are specifying all routing parameters.

     > **Important**
     >
     > The combination of values for the first three properties—**Switch**, **Code**, and **Target Type**—defines the uniqueness of the Switch Access Codes. You may specify multiple Access Codes with the same code to the same Switch, provided that they have different target types.

   - **Route Type**—The type of routing for the target specified in the Target Type for this Switch.
   - **DN Source**—An informational source that specifies the origination point in routing instructions.
   - **Destination Source**—An informational source that specifies the destination in routing instructions.
   - **Location Source**—An informational source that specifies the location in routing instructions.
   - **DNIS Source**—An informational source that specifies the DNIS in routing instructions.
   - **Reason Source**—An informational source that specifies the reasons in routing instructions.
   - **Extension Source**—An informational source that specifies the extensions in routing instructions.
   - Click **OK**.
5. Click **Apply** to save the information in the tab.
6. The **Default Access Codes** tab displays a list of Access Codes that can be used by default to place, route, or transfer calls to this Switch from any other Switches in a multi-site installation. Depending on the structure of a numbering plan, you may or may not need access codes to reach DNs that belong to different Switches of a multi-site telephone network. Click **Add** to add a Default Access Code to this switch.

7. Enter the following information in the pop-up window that displays on your screen:
   - **Code**—The prefix used to reach DNs of the Switch specified in the Switch property when placing or transferring calls from DNs of the Switch to the object for which you are configuring. You must specify a value for this property. You must specify an Access Code in full accordance with the numbering plan of the contact center telephone network, and you must make any changes to the Access Codes only after the corresponding changes have been made to the telephone network.
   - **Target Type**—The type of target within the Switch for which you are specifying all routing parameters.

     > **Important**
     >
     > The combination of values for the first three properties—**Switch**, **Code**, and **Target Type**—defines the uniqueness of the Switch Access Codes. You may specify multiple Access Codes with the same code to the same Switch, provided that they have different target types.

   - **Route Type**—The type of routing for the target specified in the Target Type for this Switch.
   - **DN Source**—An informational source that specifies the origination point in routing instructions.
   - **Destination Source**—An informational source that specifies the destination in routing instructions.
   - **Location Source**—An informational source that specifies the location in routing instructions.
   - **DNIS Source**—An informational source that specifies the DNIS in routing instructions.
   - **Reason Source**—An informational source that specifies the reasons in routing instructions.
   - **Extension Source**—An informational source that specifies the extensions in routing instructions.
   - Click **OK**.
8. Click **Save**.

Disaster Recovery

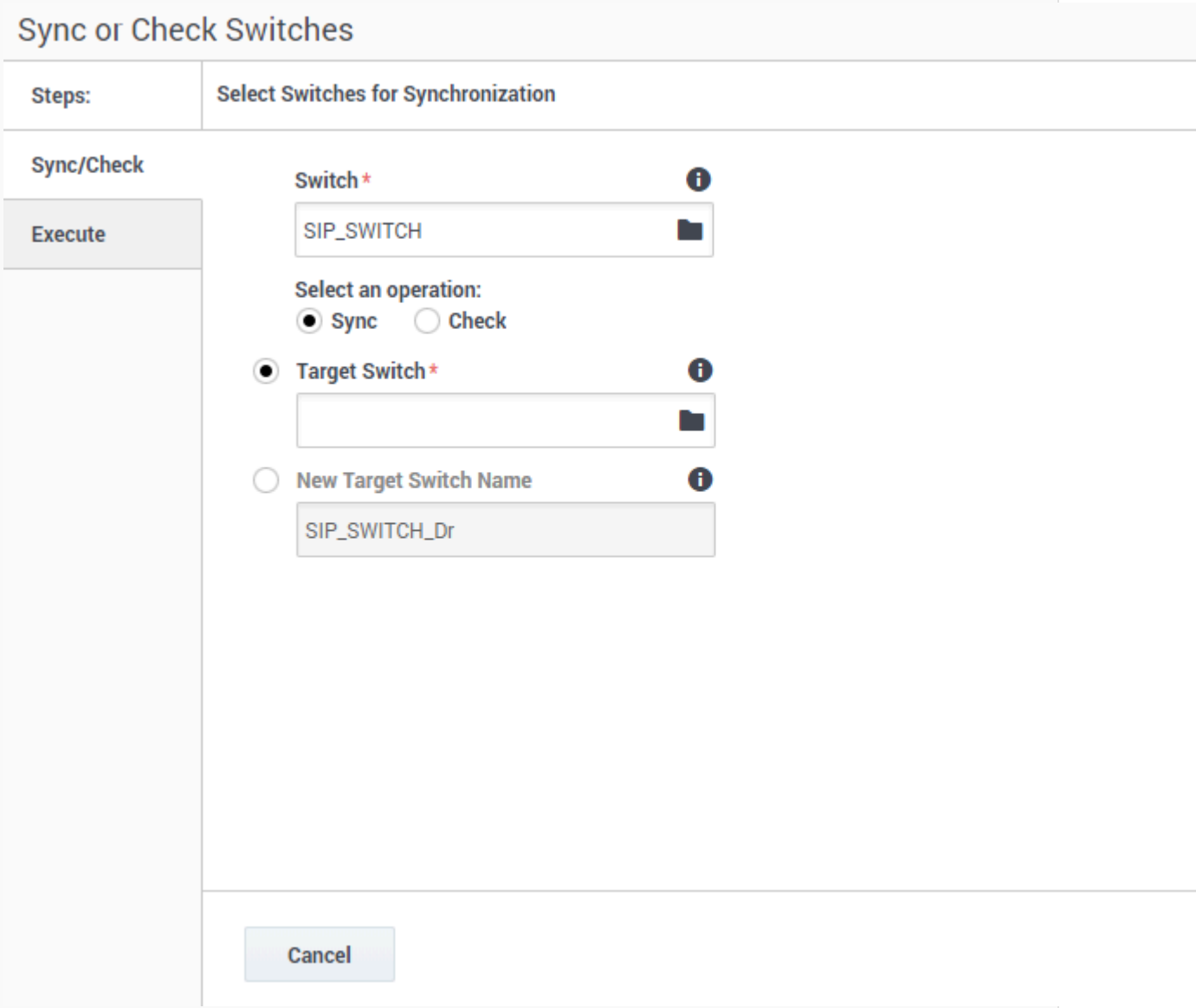
Use the Sync Switch Wizard to configure two Switches as peers, and then synchronize the two Switches so that if operations at one site are lost, the other site can take over. After the two Switches are configured as peers, synchronization will continue in real-time.

Procedure: Synchronizing Two Switches

Purpose: You can use the Sync Switch Wizard to synchronize two Switches and make them peer Switches in a Disaster Recovery configuration. The source Switch must already exist in the Configuration Database and the wizard allows you to select or create the target Switch. The sync process ensures that objects from the source Switch are copied to the target Switch and the Switches remain synchronized in real-time. You can also use the Sync Switch Wizard to check if two Switches are in sync or not.

Steps

1. Go to **Configuration** > **Switching** > **Switches**.
2. Do one of the following:
   - Select a Switch and click **More**.
   - Click **More** without selecting a Switch.
3. Click **Sync/Check Switches**. The **Sync or Check Switches** wizard is displayed. The **Switch** field displays the source Switch name if you have already selected a Switch. The **Switch** field is displayed as blank if you have not selected a Switch.



GAX Switch Sync Wizard

> **Tip**
>
> You can also click **Browse** to select another Switch regardless of whether you already selected a Switch or not.

4. Select one of the following operations:
   - **Sync** - Synchronize the two Switches and make them peer Switches
   - **Check** - Compare the objects of the two Switches and ensure that they are in sync
5. Do one of the following:
   - **Sync** or **Check** operation: Enter an existing Switch name or browse and select an existing Switch in the **Target Switch** field if the target Switch already exists.
   - **Sync** operation: Create a new Switch using the **New Target Switch Name** field and make it the target Switch. If you selected *Check* as the intended operation, the **New Target Switch Name** field is not displayed.
6. Click **Cancel** to exit the wizard or Click **Execute** to perform the operation (**Sync** or **Check**) that you selected. One of the following windows is displayed depending on the operation performed:
   - **Sync Results** - Displays the status of the synchronization of objects
   - **Check Results** - Displays the result of the comparison of objects between the two Switches

   Both windows display the folders that are synchronized, number of objects created or updated, and the sync status (IN PROGRESS, COMPLETE, or FAILURE).
7. Click **Finish** to close the wizard.

Switching Offices

Switching Offices are the actual telephone switches that provide telephone service to contact centers.

You must register a Switching Office before you configure a Switch with DNs and Agent Logins.

Viewing Switching Offices

The **Switching Offices** list shows the Switching Offices that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Switching Offices that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Switching Offices

To create a new Switching Office object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. You cannot delete a Switching Office if it has at least one Switch associated with it. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Switching Office.

- **Move To**—Move a Switching Office to another hierarchical structure.
- Enable or disable Switching Offices.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Switching Office to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Switching Office Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Switching Office. You must specify a value for this property, and that value must be unique within this Switching Office (in either an enterprise or a multi-tenant environment) or within this Tenant (in a multi-tenant environment).
   - **Switch Type**—The type of the Switching Office. You must specify a type. Once you set the type, you cannot change it.
   - **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Routing/eServices

The Routing/eServices section of Configuration Manager enables you to configure the following objects:

- Audio Resources
- Business Attributes
- Business Attribute Values
- Objective Tables
- Statistical Days
- Statistical Tables
- Transactions
- Voice Prompts

Audio Resources (Configuration Manager)

This window enables you to manage personalities and their associated audio resources (announcements and music files).

You can create Personalities to help you organize which files belong to a particular speaker. For example, you might have a personality called `John` that uses dialog spoken in English by a male speaker. Or, you might have a personality called `Marie` that uses dialog spoken in French by a female speaker.

You can upload two types of audio resources:

- Announcements—These are files that contain spoken dialog that will be played for customers. For example, you might have an announcement file that tells customers about your business hours.
- Music—These are files that play music for customers. For example, you might have a music file that plays music for customers who are about to be transferred to an Agent.

The **Audio Resources** window in Genesys Administrator Extension (GAX) is a unified list of your personalities and audio resources. For each audio resource, GAX displays the following:

- A logo to indicate whether the file has been designated as `Announcement` or `Music`.
- The name of the audio resource.
- The Audio Resource ID (ARID).
- Additional columns, one for each personality, to indicate which personality is using this audio resource.

Click **Show Quick Filter** and type the name or partial name of an object in the **Quick Filter** field. The list updates dynamically to show items that match the text in the **Quick Filter** field.

Audio Resource Management (ARM) is integrated with Operational Parameters Management (OPM) to allow users to dynamically select personalities and audio resources to be used with a parameterized strategy or orchestration application, or a parameterized routing or voice applications.

Access to ARM is based on both role privileges and Tenant access control permissions, as follows:

- User access to screens or certain ARM functionality is managed by role privileges.
- Access control permissions define which audio resources can be viewed or modified by an authenticated user. Access to audio resources is granted by Tenant. Users have access to all audio resources for each Tenant to which they have access.

Click a tab below to learn more.

Personalities

Creating a Personality

To create a new Personality, click **New**.

[+] Show Procedure

Procedure: Creating a Personality

Steps

1. Click **New** and select **Add Personality**.
2. Enter the following information:
   - **Personality Name**—The name of this personality.
   - **Language**—The language spoken by this personality.
   - **Description**—A description of this personality.
   - **Gender**—Select whether this personality is `Male`, `Female`, or `Not Specified`.
3. Click **Save**.

Other Actions

Once you create a personality, you can:

- Edit the personality—Click **Edit** beside a personality to edit personality properties.
- Delete the personality—Click **Edit** to view personality properties. In the **Edit Personality** window, click **Delete** to delete the personality.

> **Important**
> You cannot delete a Personality that is a part of one or more Audio Resource Files.

- Manipulate the audio resource—Once an audio resource is assigned to the personality, several options become available to manipulate the file.
  - Play the file—Click the play button to listen to the file.
  - **Delete**—Delete the file. This does not delete the associated personalities, but it does delete the original audio files. A file can only be removed if the audio resource to which it has been assigned has not been deployed. If the user performing this operation is a Service Provider, the file can only be removed if the file was not created by a Tenant.

- **Reprocess**—Reprocessing recreates an audio resource file from the original audio file that was uploaded (if it has not been deleted from the database and/or target storage). It also performs any necessary conversion between audio formats.
- **Download**—Download the file to your computer.
- **Encodings**—View information about how the file was encoded by GAX. When audio files are uploaded, GAX automatically encodes them to the following formats: **µ-law**, **A-law**, and **GSM**. Only **.wav** files are supported for uploading.

Audio Resources

Creating an Audio Resource

To create an Audio Resource, click **New**.

[+] Show Procedure

Procedure: Creating an Audio Resource

Steps

1. Click **New** and select **Add Message**.
2. Enter the following information:
   - **Name**—The name of this audio resource.
   - **Description**—A description of this audio resource.
   - **Type**—Select whether this audio resource is `Music` (a music file) or `Announcement` (an announcement file).
3. Click **Save**.

Uploading Audio Resources

[+] Show Procedure

Procedure: Uploading Audio Resources

Steps

1. Identify which audio resource and personality to assign to the file. Once identified, select or hover over the table cell that is shared by the target audio resource and personality.
2. Click **Upload Audio File**.
3. Your browser opens a dialog box to select an audio resource to upload. Select a file to upload.
4. The audio resource is uploaded to GAX and assigned to the personality.

Deleting Audio Resources

[+] Show Procedure

Procedure: Deleting Audio Resources

Steps

1. Click the check box beside the audio resource that you want to delete.
2. Click **Delete**.

> **Important**
>
> - If you delete an audio resource, all files that are associated with it are also deleted.
> - If you are deleting an audio resource that is being used by Operational Parameter Management, and this Audio Resource being used by one or more parameters or Parameter Groups, a message is displayed that indicates this fact. When this happens, you can either cancel the deletion or force the deletion.

Other Actions

Once you upload a file, you can select or highlight over the file and choose one of the following

actions:

- Play the file—Click the play button to listen to the file.
- **Delete**—Delete the file. This does not delete the associated personalities, but it does delete the original audio files. A file can only be removed if the audio resource to which it has been assigned has not been deployed. If the user performing this operation is a Service Provider, the file can only be removed if the file was not created by a Tenant.
- **Reprocess**—Reprocessing recreates an audio resource file from the original audio file that was uploaded (if it has not been deleted from the database and/or target storage). It also performs any necessary conversion between audio formats.
- **Download**—Download the file to your computer.
- **Encodings**—View information about how the file was encoded by GAX. When audio files are uploaded, GAX automatically encodes them to the following formats: **µ-law**, **A-law**, and **GSM**. Only **.wav** files are supported for uploading.

Sharing Audio Resources

The Environment Tenant (Service Provider) can share audio resources with other Tenants. Deployed audio resources have the following properties:

- A new audio resource is created for each Tenant.
- If the Tenant does not have matching personalities, new personalities are automatically created.
- The Personality IDs and Audio Resource IDs match the IDs of the files that are being deployed.
- File names are shared through the new audio resource. New files are not created on the file server. Audio resources provide a mechanism to make the encoded file names visible to other Tenants so that they can be used with Operational Parameter Management.
- Only the Environment Tenant can deploy an audio resource to another Tenant. It is not possible for a Tenant to re-deploy an audio resource to another Tenant.
- Changes that are made by the Environment Tenant in files of the deployed audio resources are propagated automatically. This includes adding, updating, and removal of Audio Resource Files of deployed audio resources.

Deploying Audio Resources

[+] Show Procedure

Procedure: Deploying Audio Resources

Steps

You can deploy audio resources by Tenant or by audio resource. Choose one of the methods below:

By Tenant

1. Click **Tenant Directory** and choose a Tenant to receive the audio resource.
2. Click **Edit Deployment**.
3. The **Environment Owner Messages** displays a list of audio resources in your environment. You can add or remove audio resources from the Tenant by clicking **Add** or **Remove** beside each audio resource.
4. Click **OK**.

By Audio Resource

1. Click the check box beside the audio resource that you want to deploy.
2. Click **Edit**.
3. In the Tenants list, select which Tenants to which this audio resource will be deployed. You can also click **Make this message available for all tenants** to deploy the resource to all Tenants.
4. Click **Save**.

Business Attributes

Business Attributes are objects that serve as containers of a particular type for Attribute Value objects. Instances of this object are available enumerations (classifications), such as Media Type, Service Type, and others.

> **Important**
> Business Attribute names and values may be stored using UTF-8. This enables the attributes and their values to be entered and displayed in any language, including non-ASCII languages such as Japanese. If required, two or more languages can be combined for a single Business Attribute.

For more information about Business Attributes, refer to the following documents:

- Universal Routing 8.1 Business Process User's Guide
- Universal Routing 8.1 Reference Manual
- Business Attributes topic in the eServices Interaction Properties Reference Manual.

Viewing Business Attributes

The **Business Attributes** list shows the Business Attributes that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Business Attributes that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Business Attributes

To create a new Business Attribute object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Business Attribute.
- **Move To**—Move a Business Attribute to another hierarchical structure.
- Enable or disable Business Attributes
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Business Attribute to view additional information about the object. You can also set options and permissions.

Procedure: Creating Business Attribute Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Business Attribute. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment). Once you set the value, you cannot change it.
   - **Display Name**—The localized name of the Business Attribute under which this object is to be displayed on graphical user interface elements such as dialog boxes. By default, this value is the same as for the **Name** property.
   - **Description**—A brief description of the Business Attribute.
   - **Type**—The type of the Business Attribute. You must specify a value for this property. Once you set the value, you cannot change it.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.

- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

Business Attribute Values

A Business Attribute Value is an object which represents a single value within the range of values for a given Business Attribute object.

Viewing Business Attribute Values

The **Business Attribute Values** list shows the Business Attribute Values that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

Important

- The **Business Attributes** list displays when you select **Business Attribute Values** in Configuration Manager. To access the **Business Attribute Values** list, you must first select a Business Attribute object and then a Business Attribute Value folder.
- Business Attribute Values that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Business Attribute Values

To create a new Business Attribute Value object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Business Attribute Value.
- **Move To**—Move a Business Attribute Value to another hierarchical structure.
- Enable or disable Business Attribute Values.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Business Attribute Value to view additional information about the object. You can also set options and permissions.

Procedure: Creating Business Attribute Value Objects

Steps

1. In the **Business Attributes** list, click the Business Attribute object in which you wish to create a Business Attribute Value.
2. Click the Business Attribute Value folder in which you wish to create a Business Attribute Value.
3. Click **New**.
4. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Business Attribute Value. You must specify a value for this property, and that value must be unique within the Business Attribute to which this Business Attribute Value belongs. Once you set the value, you cannot change it.
   - **Display Name**—The localized name of the Business Attribute Value under which this object is to be displayed on graphical user interface elements such as dialog boxes. By default, this value is the same as for the **Name** property.
   - Business Attribute—The Business Attribute to which this Business Attribute Value belongs. You must specify a value for this property. Once you set the value, you cannot change it.
   - **Description**—A brief description of the Business Attribute Value.
   - **Default**—If selected, indicates that this value is the default value for the Business Attribute to which it belongs. After you select this check box for one Business Attribute Value, you cannot select it for any other value that belongs to the same Business Attribute.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
5. Click **Save**.

Objective Tables

Objective Tables are collections of Objective Records that define the correspondence between interaction attributes (such as media type, service type, and customer segment) and service objectives.

If you are using Cost-Based Routing, use a Cost Contract. A Cost Contract is a special type of Objective Table, and contains the information required for calculating the cost of an interaction to be routed. Cost Contracts contain Objective Records, each of which is associated with an IT Contract. For information about working with Cost Contracts, see the Cost Contracts section in the Procedures tab, below.

Refer to the Universal Routing 8.0 Routing Application Configuration Guide for more information about Objective Tables.

Viewing Objective Tables

The **Objective Tables** list shows the Objective Tables that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
> Objective Tables that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Objective Tables

To create a new Objective Table object, click **New**. To view or edit details of an existing object, click

the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy an Objective Table.
- **Move To**—Move an Objective Table to another hierarchical structure.
- Enable or disable Objective Tables.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of an Objective Table to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Objective Table Objects

Steps

- Objective Table
- Cost Contract

Objective Table

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Objective Table. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or the Tenant (in a multi-tenant environment).
   - **Description**—A brief description of the Objective Table.
   - **Type**—Select **default** to create an Objective Table that is not a Cost Contract
   - **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Cost Contract

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Objective Table. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or the Tenant (in a multi-tenant environment).
   - **Description**—A brief description of the Objective Table.
   - **Type**—Select **Contract** to create an Objective Table that is a Cost Contract.
   - **Total Prepaid Cost**—The prepaid contract cost, for Volume Rate Contracts only.
   - **Time Zone**—The Time Zone for this Cost Contract and the Interaction Types specified in the General tab.
   - **Start**—The date on which to start the Cost Contract.
   - **End**—The date on which to end the Cost Contract.

     Refer to the Universal Routing 8.0 Routing Application Configuration Guide for more information.
3. Click **Apply** to save the Cost Contract. The **Objective Records** tab displays.
4. In the **Objective Records** tab, click **Add**.
5. Enter the following information in the pop-up window that displays on your screen:
   - **Media Type**—The type of media technology used for information exchange, for example voice, email, and fax. The range of Attribute Values for this field is defined within Media Type Business Attribute.
   - **Service Type**—The service that a customer is requesting. The range of Attribute Values for this field is defined within Service Type Business Attribute.
   - **Customer Segment**—Categorizes a customer based on their revenue potential to the enterprise relative to a business line. The range of Attribute Values for this field is defined within Customer Segment Business Attribute.
   - **Service Objective Goal**—Service Objective Goal defined for this Record. For voice interactions, this is the target time for the voice call to be answered by a live agent.
   - **Service Objective Delta**—Service Objective Delta defined for this Record. Defines the step for Service Objective Goal deviation.
   - Click **OK**.

     Refer to the Universal Routing 8.0 Routing Application Configuration Guide for more information.
6. Click **Save**.

Statistical Days

A Statistical Day is a numerically expressed workload that a particular Agent Group is expected to handle during a particular business day.

If you are using Cost-Based Routing, use a Day Contract. A Day Contract is a special type of Statistical Day. If you are using Cost-Based Routing, a Day Contract is a Statistical Day that also includes base rates, and penalties for processing a volume over or below the expected workload. Day Contracts apply only to Volume Rate IT Contracts. Day Contracts allow the base rate to vary to accommodate volume fluctuations that may occur on different days of the week, weekends, and exception days such as holidays. Refer to the Universal Routing 8.0 Routing Application Configuration Guide for more information about Day Contracts.

Statistical Days represent the definition of a point in time, and is interpreted by the Genesys server applications that are designed with these objects and coordinate them with the actual timeline that the server is running. Depending on the behavior of the server, the definition is applied to either the local time in the server's time zone, or UTC time. The Statistical Day itself does not indicate any particular time zone.

Refer to the Universal Routing 8.0 Routing Application Configuration Guide for more information about Statistical Days.

Viewing Statistical Days

The **Statistical Days** list shows the Statistical Days that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
> Statistical Days that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Statistical Days

To create a new Statistical Day object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Statistical Day.
- **Move To**—Move a Statistical Day to another hierarchical structure.
- Enable or disable Statistical Days.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Statistical Day to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Statistical Day Objects

Steps

To create a Statistical Day object, choose one of the following types:

- Statistical Day
- Day Contract

Statistical Day

To create a Statistical Day, perform the following actions:

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Statistical Day. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Type**—Select **Default** to create a Statistical Day that is not a Day Contract.
   - **Day Type**—These fields identify the calendar days to which the statistical values of the

Statistical Day apply. If **Date** is selected, you can modify the **Year**, **Month**, **Day** fields. If **Day of Week** is selected, you can modify the **Day of Week** field.

> **Important**
>
> Do not set any properties in the following section when a Statistical Day object is configured for use in a Statistical Table of the Special Day Table type.

3. **Start Time**—Start time of the Business Day. The value must be a positive number expressed in hours, minutes, and seconds from `00:00:00 AM/PM`.
4. **End Time**—End time of the Business Day. The value must be a positive number expressed in hours, minutes, and seconds from `00:00:00 AM/PM`.

> **Warning**
>
> Do not configure a Business Day that spans midnight as a single day, because it may be misinterpreted by the Routing Solution. If your Business Day starts on one day and ends on the next, you must configure it as two days, as follows:
>
> - The first Business Day starting at the overall start time and ending at `11:59 PM` of that day; and
> - The second Business Day starting at starting at `00:00 AM` of the next calendar day and ending at the overall end time.
>
> **For example**
> Assume you wish to track activity from Monday at **8:00 PM** to Tuesday at **2:00 AM**. You must explicitly create two Business Days, as follows:
>
> - The first Business Day on Monday, starting at `8:00 PM` and ending at `11:59 PM`; and
> - The second Business Day on Tuesday, starting at `00:00 AM` and ending at `2:00 AM`.

5. **Min Value**—A statistical value that represents the minimum expected workload for the whole day.
6. **Max Value**—A statistical value that represents the maximum expected workload for the whole day. This value cannot be less than the setting for **Statistical Values Minimum**.
7. **Target Value**—A statistical value that represents the target workload for the whole day. The Target Value cannot be less than the setting for the Statistical Values Minimum or greater than the setting for the Statistical Values Maximum. This property is reserved for future use.
8. **Interval Length (Min)**—The Statistical Interval in minutes. This parameter is used to break up the Statistical Day into smaller time slots that allow a model for load distribution throughout the day. This value must be a multiple of 5. Once you set the value, you cannot change it.

9. **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
10. **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
11. In the **Intervals** tab, specify the statistical intervals. Refer to the Statistical Intervals tab, above, for more information.
12. Click **Save**.

Day Contract

To create a Day Contract, perform the following actions:

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click the **Browse** button to select a value from a list:
   - **Name**—The name of the Statistical Day. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Type**—Select **Day Contract** to create a Statistical Day that is a Day Contract.
   - **Day Type**—These fields identify the calendar days to which the statistical values of the Statistical Day apply. If **Date** is selected, you can modify the following fields: **Year**, **Month**, **Day**. If **Day of Week** is selected, you can modify the **Day of Week** field.
   - **Start Time**—Start time of the Business Day. The value must be a positive number expressed in hours, minutes, and seconds from `00:00:00 AM/PM`.
   - **End Time**—End time of the Business Day. The value must be a positive number expressed in hours, minutes, and seconds from `00:00:00 AM/PM`.
   - **Interval Length (Min)**—A list of statistical intervals.
   - **Forecast Allowance (%)**—The percentage of the forecasted volume of routed interactions for this Volume Period that can be over- or underestimated without incurring a penalty. This allowance applies throughout the whole day, including intervals. The value must be a positive value.
   - **Under Forecast Allowance (%)**—The percentage of the forecasted volume of routed interactions for this Volume Period that must be exceeded to avoid a penalty for forecasting too high.
   - **Over Forecast Allowance (%)**—The percentage of the forecasted volume of routed interactions for this Volume Period that cannot be exceeded to avoid a penalty for forecasting too low.
   - **Flat Rate**—If selected, the Flat Rate to be applied during this Volume Period.
3. In the **Volume Period** tab, click **Add**. In the pop-up window, enter the following information:

- **Volume Period**—The interval number. The first interval is numbered 1 and is always counted from the start time of the Business Day.
- **Forecasted Volume**—The volume of interactions expected within the time period.
- **Base Rate**—The total cost of all interactions expected within the time period.
- **Penalty For Interaction For Over Forecast**—The additional cost, per interaction, for exceeding the forecasted interaction volume beyond that allowed by the Forecast Allowance Penalty. In effect, this is a penalty for forecasting too low.
- **Penalty For Interaction For Under Forecast**—The additional cost, per interaction, for not achieving the forecasted interaction volume beyond that allowed by the Forecast Allowance Penalty. In effect, this is a penalty for forecasting too high.

Refer to the Universal Routing 8.0 Routing Application Configuration Guide for more information.

4. Click **Save**.

Statistical Intervals

Use a Statistical Interval to associate each Statistical Interval with certain Statistical Values. For each interval, specify values representing the expected load during that interval. The value must be numeric and unique within the statistical field. When you are configuring a Statistical Day object for use in a Statistical Table of the Capacity Table type, specify:

- Statistical Value 1—A number of agents.
- Statistical Value 2—An average handling time.

When you are configuring a Statistical Day object for use in a Statistical Table of the Quota Table type, specify:

- Statistical Value 1—A statistical value that represents the minimum expected workload for the interval.
- Statistical Value 2—A statistical value that represents the target workload for the interval. This value cannot be less than the setting for the Statistical Value 1 or greater than the setting for the Statistical Value 3.
- Statistical Value 3—A statistical value that represents the maximum expected workload for the interval. This value cannot be less than the setting for the Statistical Value 1.

Statistical Tables

Statistical Tables are groups of Statistical Days that represent statistically modeled performances of Agent Groups over a calendar period of up to one year. Call-processing applications can use Statistical Tables to provide load balancing between Agent Groups when the real-time statistics for those groups are unavailable.

Viewing Statistical Tables

The **Statistical Tables** list shows the Statistical Tables that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Statistical Tables that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working With Statistical Tables

To create a new Statistical Table object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Statistical Table.
- **Move To**—Move a Statistical Table to another hierarchical structure.

- Enable or disable Statistical Tables.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Statistical Table to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Statistical Table Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Statistical Table. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Type**—The type of Statistical Table. Once you set the value, you cannot change it. The five types of Statistical Tables are:
     - Capacity Table—The call-processing applications compare the values specified in the **Intervals** list of the Statistical Days object.
     - Quota Table—The call-processing applications compare the **Minimum**, **Maximum**, and **Target** values specified in the Statistical Days object.
     - Special Day Table—The call-processing applications can identify certain days (for example, holidays).
     - Variable Rate Contract Table—The call-processing applications calculate the interaction cost based on forecasted volume, and a rate for that volume.
     - Volume Contract Table—The call-processing applications calculate the interaction cost based on a predefined call cost or agent cost.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Apply** to save the new Statistical Table.
4. If this Statistical Table is of any type other than a Variable Rate Contract Table, it will contain one or more Statistical Days. For each Statistical Day that you want to add to this Statistical Table:
   a. Click the **Statistical Days** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:

- To add an existing Statistical Day to this Table, select it from the list of Statistical Days.
- To add a new Statistical Day to this Table, click **+** to create the Statistical Day in this folder and then select it from the list.

5. After you have finished creating the Statistical Table, do one of the following:
   - Click **Save** to accept the changes and return to the list of Statistical Tables.
   - Click **Apply** to accept the changes and return to the **General** tab of this Statistical Table.
   - Click **Cancel** to discard the changes.

Transactions

Transactions define how applications calculate customer-defined statistics.

For more information about specifications and use of Transactions, consult the Universal Routing documentation.

Viewing Transactions

The **Transactions** list shows the Transactions that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
>
> Transactions that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Transactions

To create a new Transaction object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Transaction.
- **Move To**—Move a Transaction to another hierarchical structure.

- Enable or disable Transactions.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Transaction to view additional information about the object. You can also set options and permissions.

Procedure: Creating Transaction Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Transaction. You must specify a value for this property, and that value must be unique. A combination of the name and type specified in the Type property determines the uniqueness within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Alias**—An alternative name for this Transaction. If you specify this value, it must be unique within the object type specified in the **Type** property for the given contact center.
   - **Transaction Type**—The type of this Transaction. You must specify a value for this property. Once you set the value, you cannot change it.
   - **Recording Period (min.)**—A time period, in minutes, indicating how often to report the current status of the Transaction or to record it in the database.
   - **Format**—An application-specific format or script that defines how the Transaction is processed.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the `Tenant Directory` field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Important

From 8.5.260.11, GAX now saves user preferences in the Person object by default. If the **[general] userpreference_in_transaction** GAX application option is set to `true`, then GAX saves user preferences in the Transaction object in the **Transactions/UserPreference** folder.

In this case, GAX copies only the annex sections starting with the option **ga_preferences.**, from the Person annex to the Transaction annex.

When GAX creates the Transaction object, GAX removes all access permissions (for users and access groups) to the Transaction object, except the default user and the current user.

Voice Prompts

Voice Prompts are call treatment objects that may include a set of actions to be applied to a called party.

Viewing Voice Prompts

The **Voice Prompts** list shows the Voice Prompts that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Voice Prompts that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Voice Prompts

To create a new Voice Prompt object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Voice Prompt.
- **Move To**—Move a Voice Prompt to another hierarchical structure.
- Enable or disable Voice Prompts.

- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Voice Prompt to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Voice Prompt Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Voice Prompt. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment). Once you set the value, you cannot change it. If the Voice Prompt is used for a parked-call treatment, this value must correspond to the voice prompt identifier that the switch provides.
   - **Description**—A brief description of the Voice Prompt. For Text-to-Speech synthesis, a parking platform or a switch can use this property to generate the Voice Prompt.
   - **Switch**—The Switch to which this Voice Prompt belongs. Once you set the value, you cannot change it.
   - **Script**—A unique identifier of the Script for this Voice Prompt.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Desktop

The Desktop section of Configuration Manager enables you to configure the following object:

- Action Codes

Action Codes

Action Codes enable agents to report the business results of customer interactions, as well as to explain the reasons for certain operations.

After you select an appropriate code from a menu of predefined Action Codes, the code is passed along with its related request. The code then returns with the event which indicates that the request has been successfully processed. Eventually, the code is stored in the reporting database.

You can supplement each Action Code with a number of Subcodes that more precisely characterize the reasons for a certain action.

Viewing Action Codes

The **Action Codes** list shows the Action Codes that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Action Codes that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Action Codes

To create a new Action Code object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to

perform the following tasks:

- **Clone**—Copy an Action Code.
- **Move To**—Move an Action Code to another hierarchical structure.
- Enable or disable Action Codes
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of an Action Code to view additional information about the object. You can also set options and permissions.

Procedure: Creating Action Code Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The Name of this Action Code. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Type**—The Action Code Type. You must specify a value for this property. Once you set the value, you cannot change it. See the **Action Code Types** tab for more information.
   - **Code**—The Action Code. You must specify a value for this property, and that value must be unique within the Action Code type specified in the **Type** property.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. (Optional) You can also set Subcodes to more precisely characterize the reasons for a certain action. To set Subcodes, perform the following steps:
   - Click the **Subcodes** tab.
   - Click **Add**.
   - Enter the following information:
     - **Name**—The name of the Subcode. You must specify a value for this property, and that value must be unique within the Action Code. Once you set the value, you cannot change it.
     - **Code**—The Subcode value. You must specify a value for this property, and that value

must be unique within the Action Code. Once you set the value, you cannot change it.

- Perform one of the following actions:
  - Click **Save** to accept the changes and return to the object list.
  - Click **Apply** to accept the changes and remain in the tab.
  - Click **Cancel** to discard the changes.

4. Click **Save**.

Action Code Types

The following are types of Action Codes:

Type	Description
Busy Off	Selected and sent when an agent cancels the Make Busy function.
Busy On	Selected and sent when an agent activates the Make Busy function.
Conference	Selected and sent when an agent initiates a conference.
Forward Off	Selected and sent when an agent cancels the Call Forwarding function.
Forward On	Selected and sent when an agent activates the Call Forwarding function.
Inbound Call	Selected and sent when an agent releases an inbound call.
Internal Call	Selected and sent when an agent releases an internal call.
Login	Selected and sent when the agent logs in.
Logout	Selected and sent when the agent logs out.
Not Ready	Selected and sent when the agent’s status changes to Not Ready.
Outbound Call	Selected and sent when an agent releases an outbound call.
Ready	Selected and sent when the agent’s status changes to Ready.
Transfer	Selected and sent when an agent initiates a transfer.

Voice Platform

The Voice Platform section of Configuration Manager enables you to configure the following object:

- Voice Platform Profiles

Voice Platform Profiles

Voice Platform Profiles are voice (VoiceXML), call control (CCXML), announcement, or conference applications that specify the unique service information required as this application executes within the Genesys Voice Platform. Each profile contains prerequisites, parameters, and policies for each type of service.

Viewing Voice Platform Profiles

The **Voice Platform Profiles** list shows the Voice Platform Profiles that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Voice Platform Profiles that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Voice Platform Profiles

To create a new Voice Platform Profile object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Voice Platform Profile.
- **Move To**—Move a Voice Platform Profile to another hierarchical structure.

- Enable or disable Voice Platform Profiles.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Voice Platform Profile to view additional information about the object. You can also set options and permissions.

Procedure: Creating Voice Platform Profile Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Voice Platform Profile. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment). Once you set the value, you cannot change it.
   - **Display Name**—The name of the Voice Platform Profile as displayed in GVP reports and on the console.
   - **Description**—A brief description of this Voice Platform Profile.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Outbound

The Outbound section of Configuration Manager enables you to configure the following objects:

- Calling Lists
- Campaigns
- Campaign Groups
- Fields
- Filters
- Formats
- Table Accesses
- Treatments

Calling Lists

Calling Lists are database tables with records that store a collection of phone numbers and other customer and business-related data. Calling Lists are created in Genesys Administrator Extension, and inherit their structure from the assigned format. See Formats in the *Outbound Contact Deployment Guide*. See additional information about Calling Lists in the *Outbound Contact 8.1 Reference Manual*.

A Calling List must contain Genesys mandatory fields, such as **contact_info** and **contact_info_type**, and can also contain user-defined, custom fields. The campaign name, for example, is stored in a user-defined field, which is specified by the **campaign_name_field** option. A user-defined field may also serve as a customer identifier for Do Not Call requests, as an alternative to the DNC restriction on a customer's phone number.

An unlimited number of Calling Lists can be added to one Campaign, and a Calling List can be added to or deleted from a running Dialing Session for a Campaign. A Campaign can be assigned to multiple Campaign Groups.

Viewing Calling Lists

The **Calling Lists** list shows the Calling Lists that are in your environment. It is sorted in a hierarchy by tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Calling Lists that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

Click **Group By** to group objects by various criteria.

To select or de-select multiple objects at once, click **Select**.

Working with Calling Lists

To create a new Calling List object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check box beside an object and click **Edit**. To delete one or more objects, click the check box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Calling List.
- **Move To**—Move a Calling List to another hierarchical structure.
- Enable or disable Calling Lists.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Calling List to view additional information about the object. You can also set options and permissions, and view dependencies.

> **Important**
> Genesys recommends that you not modify records in a calling list while a campaign is loaded or running, because data may be lost.

Procedure: Creating Calling List Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Calling List. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Description**—A brief description of the Calling List.
   - **Table Access**—The Table Access to which the Calling List refers. You must specify a value for this property.
   - **Log Table Access**—The Table Access of the Log Table type. Genesys recommends dedicating a single Log Table Access to all Calling Lists associated with one campaign.
   - **Filter**—The Filter to be applied to this Calling List. If you specify the Filter, associate it with

the same format as the Table Access.

- **Calling Time From**—Not used at the list level at this time. The default is **8:00:00 AM**.
- **Calling Time To**—Not used at the list level at this time. The default is **6:00:00 PM**.
- **Script**—The Script Property defines the Script Object, which contains all of the attributes that are required by Agent Scripting. For more information, see the section, "Attaching Script Information to OCS User Events and Telephony Events" in the *Outbound Contact Reference Manual*.
- **Maximum Attempts**—The maximum number of attempts to call a single record in this Calling List during one campaign if a Treatment associated with this campaign results in re-dialing a particular record. You must specify a value for this property, and that value must be other than zero. The default value is 10.
- **Tenant**—In a multi-Tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Apply** to save this Calling List.
4. For each Treatment to be associated with this Calling List:
   a. Click the **Treatments** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To associate this Calling List with an existing Treatment, select it from the list of Treatments.
      - To associate this Calling List with a new Treatment, click **+** to create the Treatment in this folder and then select it from the list.
5. For each Campaign to be added to this Calling List:
   a. Click the **Campaigns** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To add an existing Campaign to this Calling List, select it from the list of Campaigns.
      - To add a new Campaign to this Calling List, click **+** to create the Campaign in this folder and then select it from the list.
6. For each Format to be associated with this Calling List:
   a. Click the **Formats** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To associate this Calling List with an existing Format, select it from the list of Formats.
      - To associate this Calling List with a new Format, click **+** to create the Format in this folder and then select it from the list.

7. After you have finished creating the Agent Group, do one of the following:
   - Click **Save** to accept the changes and return to the list of Calling Lists.
   - Click **Apply** to accept the changes and return to the **General** tab of this Calling List.
   - Click **Cancel** to discard the changes.

Campaigns

A Campaign is a flexible master plan that organizes Calling Lists and Agent Groups (or Place Groups) for dialing calls and handling call results. A Campaign can be assigned to multiple Campaign Groups. See additional information in the Outbound Contact Deployment Guide.

Viewing Campaigns

The **Campaigns** list shows the Campaigns that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Campaigns that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working With Campaigns

To create a new Campaign object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Campaign.
- **Move To**—Move a Campaign to another hierarchical structure.

- Enable or disable Campaigns.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of an Campaign to view additional information about the object. You can also set options and permissions.

Procedure: Creating Campaign Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Campaign. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Description**—A brief description of the Campaign.
   - Script—Defines the Script object that contains all of the attributes that are required by Agent Scripting.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Apply** to save the Campaign.
4. For each Calling List to be used for this Campaign:
   a. Click the **Calling List** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:
      - To add an existing Calling List to this Campaign, select it from the list of Calling Lists.
      - To add a new Calling List to this Campaign, click **+** to create the Calling List in this folder and then select it from the list.
5. After you have finished creating the Campaign, do one of the following:
   - Click **Save** to accept the changes and return to the list of Campaigns.
   - Click **Apply** to accept the changes and return to the **General** tab of this Campaign.

- Click **Cancel** to discard the changes.

Campaign Groups

Campaign Groups are structures for organizing and managing an automated process of making outbound calls to the destinations specified in Calling Lists.

Viewing Campaign Groups

The **Campaign Groups** list shows the Campaign Groups that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

Important

- The **Campaigns** list displays when you select **Campaign Groups** in Configuration Manager. To access the **Campaign Groups** list, you must first select a Campaign object and then a Campaign Groups folder.
- Campaign Groups that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the magnifying glass button to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

To select or de-select multiple objects at once, click **Select**.

Working with Campaign Groups

To create a new Campaign Group object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Campaign Group.
- **Move To**—Move a Campaign Group to another hierarchical structure.
- Enable or disable Campaign Groups.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Campaign Group to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Campaign Group Objects

Steps

1. In the **Campaigns** list, click the Campaign object in which you wish to create a Campaign Group.
2. Click the Campaign Group folder in which you wish to create a Campaign Group.
3. Click **New**.
4. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Campaign Group, in the format [Campaign@CampaignGroup]. This value is set automatically, based on the content of the fields Campaign and Group.
   - **Description**—A brief description of the Campaign Group.
   - **Group Type**—The type of Campaign Group, Agent, or Place.
   - **Group**—The name of the Agent Group or Place Group that is associated with this Campaign Group. This value is set automatically and you cannot change it.
   - **Dialing Mode**—The name of the Dialing Mode for this Campaign Group.
   - **Voice Transfer Destination**—Identifies where calls are to be delivered for handling.

     > **Important**
     > In addition to the Voice Transfer Destination DN, any ACD Queue, Virtual Queue, Routing Point, or Service Number DN that may be part of a call flow involving this group of agents or places must be specified as an Origination DN of the Agent Group or Place Group objects. Outbound Contact Server (OCS) needs to monitor these DNs to identify "r;foreign" inbound or outbound calls that are delivered to agents but were not issued by OCS on behalf of the Campaign Group, or if the ACD Queue DN is configured as an "r;overflow" DN.

   - **Operation Mode**—An operation mode: **Manual** or **Scheduled**. This property applies only to the Preview dialing mode.

- **Optimization Method**—A method to optimize direct dialing algorithms in the predictive dialing modes. These methods include: **Agent Busy Factor**, **Average Distribution Time**, **Average Waiting Time**, **Overdial Rate** and **Maximum Gain**.

  > **Important**
  > **Average Distribution Time** can be set only for the Predictive GVP Dialing Mode.

- **Optimization Target %**—The target value for the optimization method. The unit of measure depending on the optimization method selected in the preceding field. The default value is `80`.
- **Maximum Queue Size**—The number of records to keep in the dialer's queue. It is an internal counter that is used when OCS performs with Power GVP or Push Preview modes. OCS tries to always keep the dialer's buffer full with the specified Maximum Queue Size. The default value is `0` (zero).
- **IVR Profile**—The IVR Profile DBID that is specified in the GVP EMPS IVR Profile. The OCS **ivr-profile-name** option uses the value specified in this field.
- **Interaction Queue**—A configuration object that is created in the Scripts section by Interaction Routing Designer when developing a Business Process to process outbound Preview mode interactions.
- **Trunk Group DN**—Required only if you are using Outbound Contact in an Outbound VoIP environment. If specified, OCS uses this DN as the DN on behalf of which outbound and engaging calls originate.
- **Script**—The Script object that contains all of the attributes that are required by Agent Scripting.
- **Minimum Record Buffer Size**—The minimum record buffer size that acts as a multiplier, along with the optimal record buffer size, for the number of agents that are available for a campaign. The default value is 4.
- **Optimal Record Buffer Size**—The optimal record buffer size that acts as a multiplier, along with the minimum record buffer size, for the number of agents that are available for a campaign. The default value is 6.
- **Number of Channels**—Identifies the maximum number of ports that a Campaign Group can use to place calls. This max number is used in: **Progressive**, **Predictive**, **Progressive with seizing**, **Predictive with seizing**, and **Progressive GVP** dialing modes. The default value is `10`.
- **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

5. In the **Connections** tab, add all connections to all servers (except T-Server and SIP Server)

needed to run this Campaign Group. Click **Add** to add a connection. In the pop-up window, either select the connection to add, or click **+** to create a new connection and then add it.

6. Click **Save**.

Dialing Modes

Outbound Contact has many dialing modes which are listed in the table below. You can switch between Progressive and Predictive dialing modes at any time, and change the optimized parameter. Changing the dialing mode and optimized parameter in Genesys Administrator Extension is temporary. It lasts only until the Campaign is stopped or you change the setting. To change from Predictive or Progressive Dialing mode to Preview Dialing mode, the Campaign must be stopped and restarted. A Preview Only license limits the use of OCS to this one dialing mode. A full license is required in order to run Campaigns in all dialing modes.

Important

The Campaign needs to be loaded in order to change the dialing mode and optimized parameter.

The dialing mode is used in conjunction with the values in the **Optimization** parameters and **Optimization Target** value fields.

Dialing Mode	Description
Power GVP	Dial calls by issuing call requests. For more information, see the Outbound Contact Deployment Guide.
Predictive	Dials calls from a calling list and predicts agent availability. Recommended for high-volume, low-value Campaigns.
Predictive GVP	Pacing is based on optimizing agent workloads in deployments where outbound calls first arrive to GVP for self-service. A portion of these outbound calls (for customers who selected the agent-assisted service option in GVP) is then passed to an agent group. In this dialing mode, it is assumed that outbound calls passed for agent-assisted service wait in the queue for some time for the next available agent. This dialing mode requires SIP Server for placing outbound calls, rather than T-Server, and uses GVP Voice XML applications for self-serviced call processing.

Dialing Mode	Description
	Important This dialing mode is supported by OCS starting in release 8.1.2.
Predictive with seizing	Used only with the Active Switching Matrix mode. Calls are dialed automatically, similar to Predictive mode.
Preview	Dials calls from a calling list only when an agent previews a calling list record and manually requests a call to be dialed. Recommended for low-volume, high-value applications, where individual ownership of accounts is the highest priority.
Progressive	Dials calls from a calling list only when an agent is available. Recommended for low-volume, high-value Campaigns.
Progressive GVP	Dials calls from a Calling List when a GVP port is available. This dialing mode requires SIP Server for placing outbound calls, rather than T-Server, and uses Voice XML applications for call processing.
Progressive with seizing	Used only with the Active Switching Matrix mode. Calls are dialed automatically, similar to Progressive mode.
Push Preview	Dials calls that are "pushed" to the agent's desktop using Interaction Server.

Fields

A Field object defines a field in a Calling List database table. Fields are single pieces of data (for example, a phone number) within a record.

There are two types of fields in a Calling List:

- Genesys mandatory fields—These fields must exist in all Calling List tables.
- User-defined fields—These custom fields contain business-related data.

Viewing Fields

The **Fields** list shows the fields that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Fields that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the magnifying glass button to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Fields

To create a new Field object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete** button. You can also delete individual objects by clicking on the object and then clicking **Delete**.

> **Important**
> You can delete a Field only if there is no Filter associated with it.

Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Field.
- **Move To**—Move a Field to another hierarchical structure.
- Enable or disable Fields.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Field to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Field Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Field.
   - **Description**—A brief description of the Field.
   - **Data Type**—The data type for the data stored in this Field.
   - **Length**—(Required for **char** and **varchar** data types only) The length of the Field in the database.
   - **Field Type**—Outbound business-specific information for this Field.
   - **Default**—The default value for the Field. All formats that include the Field use this default value. The value should be consistent with the data type of the Field. For example, if the data type is integer, the default value should be an integer value only. When Genesys Administrator Extension imports records from an ASCII file in which a Field is missing or has no value, Genesys Administrator Extension populates the Field with this default value—if the check box **Nullable** is not checked. If the Field is nullable, Genesys Administrator Extension accepts a blank value.
   - **Primary Key**—This check box indicates whether the Field is a primary key in a database

table. In Outbound Contact, the only primary key Fields are **chain_id** and **chain_n**.

- **Unique**—This check box indicates whether the Field value is unique within the table.
- **Nullable**—The checkbox indicates whether the Field value can be set to **NULL**.
- **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

Field Types

Field Type	Description
Agent	A field containing a login ID of the last agent who handled an outbound call associated with this record.
ANI	A field containing an Automatic Number Identification.
Application	A field containing a Genesys application. An Application is: any of the executable programs that are installed and configured during a Framework installation, and which has a particular function within Framework. Examples: Configuration Server, Solution Control Server (SCS), Message Server, Local Control Agent (LCA).
Call Time	A field containing the time of the actual dialing attempt.
Campaign	A field containing the campaign with which this record is associated.
Chain	A field containing the special ID of records that should be linked in a chain. Each record that is associated with one customer account, for example, has the same chain ID.
Contact Info	A field containing a destination telephone number.
Contact Info Type	A field containing the type of telephone number, such as home or work.
Country Code	A field containing the country code.
Dialing Result	A field containing the result of a dialed call.

Field Type	Description
E-mail Subject	A field containing the text in the subject line of an email interaction.
E-mail Template ID	A field containing the template ID of an email interaction.
From	A field containing the time a record is scheduled for dialing.
Group	A field containing the name of a configuration object that groups person objects.
Info Digits	A field containing the Information Indicator-Digits, which indicate the originating line type of the caller.
LATA	A field containing the number of the Local Access and Transport Area.
Media Reference	A field containing the Configuration Server API reference to media body to be sent in case of treatment.
NPA	A field containing the number of the Numbering Plan Area.
NPA-NXX	A field containing the number of the Numbering Plan Area with an identifier of the specific telephone company central office serving that number.
Number in Chain	A field containing the priority assigned to a given record in the chain. The smallest number is processed first.
Number of Attempts	A field containing the number of attempts. (It does not include redialing attempts in the event of errors.)
Record ID	A field containing the unique ID number for the current record.
Record Status	A field containing the status of the record.
Record Type	A field containing the type of record.
Scheduled Time	A field containing the time of a scheduled personal callback or a rescheduled call (from a treatment).
State Code	A field containing State or International code, for example, a U.S. or Canadian postal code such as CA for California.
Switch ID	A field containing a configuration database object that represents a physical or virtual switch.
Time Zone	A field containing the time zone offset of the record.
To	A field containing the time the dialing attempts should conclude.
Treatments History	A field containing the record of treatments that have been applied to a customer.
User-Defined Field	A user-defined field.

Filters

A Dialing Filter restricts Calling Lists so that only certain numbers are dialed during a Campaign.

> **Important**
> Creating Dialing Filters requires using Enumeration values in place of text values for some mandatory fields. An Enumeration value is a numeric representation of a Genesys mandatory field value. For more information about Enumeration values, see "Genesys Enumeration Tables" in the Outbound Contact 8.1 Reference Manual.

Viewing Filters

The **Filters** list shows the filters that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Filters that are disabled will appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Filters

To create a new Filter object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click

the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Filter.
- **Move To**—Move a Filter to another hierarchical structure.
- Enable or disable Filters.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Filter to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Filter Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Filter.
   - **Description**—A brief description of the Filter.
   - **Format**—The format to which this filter is applied. Once it is specified, it cannot be changed. You assign a Filter object to a Calling List object with the same format.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. Click **Save**.

Formats

A Format is a user-customized template for Calling Lists. It is created in Genesys Administrator Extension and consists of Fields that form a data structure (for example, a database table); each Field has properties that describe its characteristics. A Calling List must contain Genesys mandatory fields and can also contain user-defined custom Fields. See additional information in the Outbound Contact Deployment Guide.

Mandatory Fields are necessary in order to process records properly. They identify each customer and the status of each customer record. Genesys mandatory fields are described in the Mandatory Fields tab, below. See additional information in the Outbound Contact Deployment Guide.

Custom/user-defined Fields, typically containing business-related data, can be created and added to a Format in Genesys Administrator Extension. Custom fields define customer information that is available to the agent during a call. See Fields in the Outbound Contact Deployment Guide about how to send customer data to an agent.

After custom/user-defined fields are added, the Format is finished and is ready to be used to create Calling Lists. A Calling List must be created from a Format, and inherits mandatory and custom fields from the assigned format. Each Calling List can have only one corresponding Format.

When database records are imported into a Calling List, data fills the mandatory and custom fields, conforming to properties established in the finished Format.

Viewing Formats

The **Formats** list shows the formats that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> ### Important
> Formats that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the magnifying glass button to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Formats

To create a new Format object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click the **More** button to perform the following tasks:

- **Clone**—Copy a Format.
- **Move To**—Move a Format to another hierarchical structure.
- Enable or disable Formats.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Format to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Format Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of the Format.
   - **Description**—A brief description of the Format.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
   - **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
3. For each Field to be added to this Format:
   a. Click the **Fields** tab and click **Add**.
   b. Navigate to the appropriate folder, if necessary, and do one of the following:

- To add an existing Field to this Format, select it from the list of Campaigns.
- To add a new Field to this Format, click **+** to create the Field in this folder and then select it from the list.

4. After you have finished creating the Format, do one of the following:
   - Click **Save** to accept the changes and return to the list of Format.
   - Click **Apply** to accept the changes and return to the **General** tab of this Format.
   - Click **Cancel** to discard the changes.

Mandatory Fields

The following mandatory fields are required in all Calling List Formats. This list is sorted alphabetically by field name. Default values for these fields are defined in the Fields objects during configuration.

Field Name	Data Type	Description
agent_id	varchar(32)	Login identifier of the agent who handled the record.
app_id	integer	Empty, not used at this time.
attempt	integer	Number of attempts made to reach the customer.
call_result	integer	Final outcome of the record processing. See the Call Results table in the Outbound Contact Reference Manual.
call_time	integer	Latest date and time at which the record was processed (dialed), in UTC format.
campaign_id	integer	Configuration DBID of the Outbound Dialing Campaign, as a part of which the record has been processed.
chain_id	integer	Unique identification number of the chain to which the record belongs.
chain_n	integer	Unique identification number of the record within the chain.
contact_info	varchar(128)	Customer's contact information; phone number in the voice campaign.

Field Name	Data Type	Description
contact_info_type	integer	Type of the contact information; phone type in the voice campaign. See the Contact Information Types table in the Outbound Contact Reference Manual.
daily_from	integer	Earliest time of the day at which a customer can be contacted (seconds since midnight).
daily_till	integer	Latest time of the day at which a customer can be contacted (seconds since midnight).
dial_sched_time	integer	Date and time for which the processing of the record has been scheduled or rescheduled, in UTC format (seconds since midnight 01/01/1970).
email_subject	varchar(255)	Empty, not used at this time.
email_template_id	integer	Empty, not used at this time.
group_id	integer	Empty, not used at this time.
media_ref	integer	Empty, not used at this time.
record_id	integer	Unique identification number of a calling record.
record_status	integer	Current status of the record. See the Record Types table in the Outbound Contact Reference Manual.
record_type	integer	Type of the record. See the Record Types table in the Outbound Contact Reference Manual.
switch_id	integer	DBID of the Switch where the agent who handled the record had logged in.
treatments	varchar(255)	Treatments application history. For more information, see Treatments in the Outbound Contact Deployment Guide.
tz_dbid	integer	Configuration DBID of the Time Zone object associated with the calling record.

Table Access

Table Access objects describe database tables of a specified Format and explain how to access these tables through Database Access Points (DAPs).

You cannot delete a Table Access object while it is associated with at least one Calling List.

Viewing Table Access

The **Table Access** list shows the Table Access objects that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
> Table Access objects that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the magnifying glass button to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

To select or de-select multiple objects at once, click **Select**.

Working with Table Access

To create a new Table Access object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Table Access object.
- **Move To**—Move a Table Access object to another hierarchical structure.

- Enable or disable Table Access objects.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Table Access object to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Table Access Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—The name of this Table Access object. It can contain up to 254-characters. You must specify a value for this property, and that value must be unique within the Configuration Database (in an enterprise environment) or within the Tenant (in a multi-tenant environment).
   - **Description**—A brief description of the Table Access object.
   - **Table Type**—The type of Table Access object in the database. You must specify a value for this property. Once you set the value, you cannot change it.
   - **DB Access Point**—The Database Access Point through which to access the Table. You must specify a value for this property. The Database Access Point must serve the Tenant to which this Table Access object belongs.
   - **Format**—The Format of this Table. You must specify a value for this property for all Table types except **Log Table**. Once you set the value, you cannot change it.
   - **Database Table**—The name of this table as specified in the database. You must specify a value for this property. The name length depends on the DBMS type. Genesys recommends that you do not exceed the following vendor-defined limitations:
     - 18 characters—for DB2 and Informix databases
     - 128 characters—for Microsoft SQL databases
     - 30 characters—for Oracle and Sybase databases
   - **Update Every (seconds)**—The number of seconds an application waits before updating the table data in application memory. This value is required only if the **Cacheable** check box is checked.
   - **Cacheable**—Indicates whether the Table Access data is mirrored in application memory.
   - **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.

- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

Table Access Types

Table Access Type	Description
ANI	An Automatic Number Identification table.
Calling List	A calling list table.
Country Code	A country code table.
Customer Defined Table	A user-defined table.
Do Not Call List	In Outbound, a list of customers who request not to be called is known as a Do Not Call (DNC) list. The DNC data in a Do Not Call list file includes the customer's phone number or a customer ID.
E-mail Contact List	In Outbound, a list of customers who are to be contacted.
Info Digits	An Information Indicator-Digits table.
LATA	A Local Access and Transport Area table.
Log Table	A log table.
NPA	A Numbering Plan Area table.
NPA-NXX	A table of a Numbering Plan Area with an identifier of the specific telephone company central office that serves that number.
State Code	A State or International code, for example, a U.S. or Canadian postal code, such as CA for California.

Treatments

A Treatment defines what Outbound Contact Server (OCS) should do with a call that does not reach the intended party. For example, the Treatment could instruct OCS to redial a number that returns a Busy call result.

Treatment objects are assigned to Calling List objects. If no Treatments are assigned to a call result, OCS changes the record status to Updated.

You can add or remove Treatments from a Calling List object while a Dialing Session for a Campaign is running. However, once a Treatment is in progress, it cannot be interrupted. Changes made to that Treatment are applied to the next record that receives the call result that prompts the Treatment.

Viewing Treatments

The **Treatments** list shows the Treatments that are in your environment. It is sorted in a hierarchy by Tenants, configuration units, sites, and folders. To view objects by a particular hierarchy, select the hierarchy type in the drop-down menu above the list.

> **Important**
>
> Treatments that are disabled appear grayed out in the list.

Configuration Manager respects tenancy permission settings. You can access only those objects that you have been granted permissions and privileges to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the magnifying glass button to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking **Select Columns**.

To select or de-select multiple objects at once, click **Select**.

Working with Treatments

To create a new Treatment object, click **New**. To view or edit details of an existing object, click the name of the object, or click the check-box beside an object and click **Edit**. To delete one or more objects, click the check-box beside the object(s) in the list and click **Delete**. You can also delete

individual objects by clicking on the object and then clicking **Delete**. Otherwise, click **More** to perform the following tasks:

- **Clone**—Copy a Treatment.
- **Move To**—Move a Treatment to another hierarchical structure.
- Enable or disable Treatments.
- Create a folder, configuration unit, or site. See Object Hierarchy for more information.

Click the name of a Treatment to view additional information about the object. You can also set options and permissions, and view dependencies.

Procedure: Creating Treatment Objects

Steps

1. Click **New**.
2. Enter the following information. For some fields, you can either enter the name of a value or click **Browse** to select a value from a list:
   - **Name**—(Required) The name of the Treatment.
   - **Description**—(Optional) A brief description of the Treatment.
   - **Call Result**—(Required) The call result associated with this Treatment.
   - **Apply to Record**—(Required) The action to apply to a Calling List record, based on the call result.
   - **Apply to Call**—(Optional) An alternate way to handle a call when a dialing attempt is answered or reaches an answering machine or a fax machine.
   - **Destination DN**—(Required, if **Apply to Call** is specified) The DN to which the call is connected or transferred. If **Apply to Call**is specified but **Destination DN** is not, OCS ignores the Treatment.
   - **Number in sequence**—(Required) The order in which this treatment is applied in a Treatment sequence. If it is a stand-alone treatment, specify a value of 1.
   - **Cycle Attempt**—(Required with value of greater than `0` (zero), when **Apply to Record** is set to **Next in chain**, **Next in chain after**, and **Next in chain at specified date**, or **Redial**) The maximum number of consecutive attempts to execute the Treatment on the record.
   - **Interval (Days:Hours:Minutes)**—(Required when **Apply to Record** is set to **Next in chain**, **Next in chain after**, **Redial**, or **Retry in**) A time interval, in minutes, that OCS waits between the first dialing attempt and the first Treatment attempt.

- **Increment (minutes)**—(Required when **Apply to Record** is set to **Next in chain**, **Next in chain after**, **Redial**, or **Retry in**) The number of minutes added to the previous redial time interval.
- **Date**—(Required when **Apply to Record** is set to **Next in chain at specified date**, or **Retry at specified date**) The date when another Treatment attempt is performed.
- **Time**—(Required when **Apply to Record** is set to **Next in chain at specified date**, or **Retry at specified date**) The time of day that another Treatment attempt is performed.
- **Range (Days:Hours:Minutes)**—Reserved for future use.
- **Tenant**—In a multi-tenant environment, the Tenant to which this object belongs. This value is automatically set to the Tenant that was specified in the **Tenant Directory** field in the object list.
- **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.

3. Click **Save**.

Solution Deployment

Solution Deployment enables the user to fully deploy solution definitions and installation packages (IPs) to local and remote locations. This includes installation and configuration of all necessary applications and updates to existing multi-tenant applications, where appropriate.

A solution definition consists of an XML file that dictates the steps to install, upgrade, or configure IPs and system configurations to deploy a solution successfully.

> ### Warning
> Solution Deployment requires that the Genesys Deployment Agent (GDA) be installed on all source and target hosts. Refer to the Solution Deployment Prerequisites section of the *GAX Deployment Guide* for more information.

Solution Deployment includes:

- Managing Installation Packages (IPs)
  - Installation packages
  - View Deployed IPs
- Managing Solution Definitions
  - Solution definitions
  - View a list of deployed solutions
- Managing Privileges

Installation Packages

This panel enables you to manage installation packages (IPs) by uploading IPs to a repository in GAX and deploying the IPs to hosts.

The **Installation Packages** panel on the left of the screen displays a list of IPs that you have permission to see in your environment. The list is sorted by groups. You can expand a group to see its list of IPs.

> **Important**
> Installation packages are stored in the database and not on the local file system.

Solution Deployment respects tenancy permission settings. You can access only those objects that you have been granted permission to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the cube icon to open the **Tenant Directory** filter panel. In this panel, click the Tenant that you want to select. Use the **Quick Filter** field in this panel to filter the Tenant list.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

Viewing IPs

The **Installation Packages** panel list displays the following information:

- **Name**—The name of the IP.
- **Version**—The version number of the IP.
- **Locale ID**—Indicates the language used by the plug-in.
- **Operating System**—The operating system and bit version that are required by the IP.
- **Status**—Indicates the current status of the IP. For example, a status of **Complete** indicates that the IP deployed successfully.
- **Update Time**—A timestamp that indicates when the IP was last updated.

Click an IP to reveal more details in a panel that opens to the right. This panel displays the following information about the IP:

- **Name**—The name of the IP.

- **Nickname**—The nickname for the IP.
- **Description**—An optional description of the IP; this can be modified, as required.
- **Version**—The version number of the IP.
- **Locale ID**—Indicates the language used by the plug-in.
- **Operating System**—The operating system that is required by the IP.
- **Status**—Indicates the current status of the IP For example, a status of **Complete** indicates that the IP deployed successfully.
- **Update Time**—A timestamp that indicates when the IP was last updated.
- **Group**—The group to which this IP belongs. If you change the group name, the IP is relocated to that group. If the group name you enter does not exist, it will be created. These actions take effect immediately in the **Installation Packages** list.

Working with IPs

You can perform the following actions from this panel:

- **Upload Installation Packages**—Upload an IP to the repository.
- **Copy to Tenants**—Copy the IP to tenant(s).
- **Deploy**—Deploy the IP to host(s).
- **Download**—Download a copy of the IP.
- **Delete**—Delete the IP.

Upload Installation Packages

[+] Click to show procedure

1. In the **Installation Packages** panel, click **+**. A new panel called **Software Installation Wizard** opens to the right.
2. In the **Software Installation Wizard** panel, select a method for importing the IP:

> **Important**
>
> If your installation package contains two or more templates, you must use the **Installation Package Upload (includes templates)** procedure.

- Installation Package Upload (includes templates)—Upload a file containing an installation package and its associated templates. These files are typically provided by Genesys Customer Care.
- Installation Package Upload (template uploaded separately)—Upload an installation package and its associated template.
- UNC Path to Mounted CD or Directory—Upload an IP stored on a mounted CD or network directory.

- UNC Path to an Existing Administrator Repository—Upload an IP from an existing Genesys Administrator repository.
- UNC Path to Zipped IPs through Support—Upload a .zip file provided by Genesys Customer Care that is stored on a mounted CD or network directory. This file contains an installation package and its associated templates.

3. The file(s) upload from your file system to Genesys Administrator Extension, and a progress bar displays to show the upload progress. The progress of the upload also displays in the Status column in the **Installation Packages** panel.

> **Important**
>
> When you upload a plug-in, GAX uses the template file (.tpl) to create an Application Template and extracts the default options for the plug-in. GAX stores these options in the database and merges them with the core GAX Application object upon deployment. During this merge, only new options are added—existing key value pairs are not overwritten.

Installation Package Upload (includes templates)

1. In the **Software Installation Wizard** panel, select **Installation Package Upload (includes templates)** and click **Next**.
2. The panel updates. Click **Choose File** to select the file to upload.
3. Click **Finish**.
4. The file begins uploading from your file system to Genesys Administrator Extension. When the upload is complete, the IP will be displayed in the **Installation Packages** list.

Installation Package Upload (template uploaded separately)

1. In the **Software Installation Wizard** panel, select **Installation Package Upload (template uploaded separately)** and click **Next**.
2. The panel updates and displays three boxes: **Upload a package**, **Upload an XML template**, and **Upload an APD template**. Click **Choose File**.
   - Upload a package—A file that contains the installation package.
   - Upload an XML template—The XML template file for this installation package. This is the template that is referenced by the installation package description file. This file should not be modified from the version in the template directory.
   - Upload an APD template—The APD template file for this installation package. This is the template that is referenced by the installation package description file. This file should not be modified from the version in the template directory.

   The panel updates.
3. Click **Finish**.
4. The file begins uploading from your file system to Genesys Administrator Extension. When the upload is complete, the IP will be displayed in the **Installation Packages** list.

UNC Path to Mounted CD or Directory

1. In the **Software Installation Wizard** panel, select **UNC Path to Mounted CD or Directory**.
2. In the text field, type the path for where the IP is stored.
3. Click **Next** to open the path.
4. The panel updates to display the IP(s) found at the specified location. Click the check box(es) beside the IP(s) to upload.
5. Click **Finish**.
6. The panel updates to display a progress bar for the upload process. You can click **Close** at any time to close the panel without interrupting the upload procedure. The status of the IP upload will be displayed in the **Installation Packages** list.

UNC Path to an Existing Administrator Repository

1. In the **Software Installation Wizard** panel, select **UNC Path to an Existing Administrator Repository**.
2. In the text field, type the path for the existing Genesys Administrator repository.
3. Click **Next** to open the path.
4. The panel updates to display the IP(s) found at the specified location. Click the check box(es) beside the IP(s) to upload.
5. Click **Finish**.
6. The panel updates to display a progress bar for the upload process. You can click **Close** at any time to close the panel without interrupting the upload procedure. The status of the IP upload will be displayed in the **Installation Packages** list.

UNC Path to Zipped IPs through Support

1. In the **Software Installation Wizard** panel, select **UNC Path to Zipped IPs through Support**.
2. In the text field, type the path for where the IP is stored.
3. Click **Next**.
4. The panel updates to display the IP(s) found at the specified location. Click the check box(es) beside the IP(s) to upload.
5. Click **Finish**.
6. The panel updates to display a progress bar for the upload process. You can click **Close** at any time to close the panel without interrupting the upload procedure. The status of the IP upload will be displayed in the **Installation Packages** list.

Important

- A green progress bar represents a successful upload of the installation package. A red

progress bar represents a failed upload of the installation package. You can review which step failed in the **Status** field in the **Installation Packages** list.

- You cannot upload an IP to the repository if a version of the IP already exists in the repository. You must have the **Replace IPs and SPDs** privilege enabled to overwrite an IP in the repository.

Copy Installation Packages to Tenants

[+] Click to show procedure

1. Click the name of an installation package to select it. A new panel opens to the right.
2. In the **Installation Package** details panel, click **Related** and select **Copy to Tenants**. A new panel called **Copy to Tenants** opens to the right.
3. In the **Copy to Tenants** panel, type the name of a Tenant in the **Quick Filter** field, or click **Browse** to browse a list of Tenants in your environment. A new panel called **Tenants** opens to the right.
4. Click the check box beside each Tenant that is to receive the IP. The name of the Tenant will appear in the **Copy to Tenants** panel, in the **Targeted Tenants** section.
5. Click **Next** at the bottom of the **Copy to Tenants** panel.
6. Click **Finish** to copy the IP to the Tenant(s).

Deploy Installation Packages

[+] Click to show procedure

1. Click the name of an installation package to select it. A new panel opens to the right.
2. In the Installation Package details panel, click **Related** and select **Install**. A new panel called **IP Deployment Wizard** opens to the right.
3. Follow the steps in the Deployment Wizard. Click the Deployment Wizard tab, above, for more information.

Important

- You cannot upload an IP to the repository if a version of the IP already exists in the repository. You must have the **Replace IPs and SPDs** privilege enabled to overwrite an IP in the repository.
- IP deployment does not require the use of an SPD file.
- If you install a plug-in through GAX on Windows, the deployment wizard prompts you to

specify only the plug-in installation path.

If you install a plug-in through GAX on Linux, then the deployment wizard prompts you to specify both the GAX directory path and the plug-in installation path. If the path where GAX is installed is provided incorrectly, then the deployment wizard installs the plug-in but it will not copy the plug-in files to the GAX directory. In this case, you must manually copy the plug-in files from the plug-in installed path to the GAX installed path.

Download Installation Packages

[+] Click to show procedure

1. Click the name of an installation package to select it. A new panel opens to the right.
2. Click **Download**. Genesys Administrator Extension initiates the download procedure in your browser.

Delete Installation Packages

[+] Click to show procedure

1. Click the name of an installation package to select it. A new panel opens to the right.
2. In the **Installation Package** details panel, click **Delete**.
3. A dialog box appears to confirm deletion. Perform one of the following actions:
   - Click **OK** to delete the IP permanently.
   - Click **Cancel** to cancel deletion of the IP.

Important

This action is available only if the user has the **Delete IPs and SPDs** privilege.

Important

- If the component metadata XML file contains questions that must be answered during the installation of an IP, the user is prompted to answer those questions during installation.
- IP deployment does not require the use of an SPD file.

Deployment Wizard

The **Automated Deployment Wizard** deploys an installation package (IP) or solution definition to the specified hosts and installs and configures the service as directed by the Service Package Definition.

Before You Begin

While you are using the **Automated Deployment Wizard**, take note of the following:

- Most of the fields in the Wizard are auto-complete fields. You can enter only part of the value in the field, and then you are presented with a list of all entries that contain the text that you entered; you can then select the appropriate item.
- The Wizard verifies the IPs, based on the operating system of the intended hosts. When you are selecting hosts, make sure that you select those that are running the required operating system.
- If an IP is already installed on a host, by default the Wizard will reinstall the IP. All parameters entered during the previous deployment are saved by Genesys Administrator Extension and automatically prepopulated in the Wizard.
- When upgrading an existing IP, the IP's permissions and connections are updated to the new Application object.

Items That Can Be Merged

For scenarios in which the existing IP and the new IP have conflicting values, the existing IP's values are maintained. If the existing IP does not contain a value, the value of the new IP is used. The following values are available to be merged:

- options
- annex
- connections
- ports
- timeout
- autorestart
- commandlinearguments
- commandline
- state
- shutdowntimeout
- attempts
- redundancytype
- isprimary
- startuptimeout

Plug-ins are installed using the same procedures as IPs, but take note of the following:

- The plug-in install profile automatically fetches GAX Application objects for selected Host objects.
- Plug-in options are merged into the affected GAX Application objects.
- Some input fields do not appear, such as those relating to **Application Object**, **App Port**, and **Tenant Object**.

The following are possible scenarios that you may perform by using the **Automated Deployment Wizard**:

- Installing an Installation Package
- Upgrading an Installation Package
- Rollback an Installation Package

Installing an Installation Package

[+] Click to show procedure

1. In the **Installation Packages** panel, select the IP to use for the install.
2. A new panel with additional information about the IP appears to the right. Click **Related** and select **Install**.
3. The **Automated Deployment Wizard** panel displays to the right. Click **Next**.
4. The panel updates to show the **Host set selection** list. Select the host to receive the IP. Click **Next**.
5. The panel updates to show the **Application Parameters** list. In the **GAX Application object for host** field, select the Genesys Administrator Extension Application object.
6. Click **Next**.
7. The panel updates to display the **Installation Parameters (silent.ini)** list. You can set the target installation path in the field.
8. Click **Next**.
9. The panel updates to display the **Deployment** report. Review the settings, and perform one of the following actions:
   - Click **Finish** to install the IP.
   - Click **Previous** to return to a previous panel and modify settings.
10. The panel updates to display a progress bar of the deployment. This information also displays in the **Deployed IPs** panel.

> **Important**
>
> If a deployment fails, you can review a log of the deployment by selecting the IP from the **Deployed IPs** panel. A new panel displays with additional information about the IP. Click **Deployment Action Log**.

Upgrading an Installation Package

[+] Click to show procedure

1. In the **Deployed IPs** panel, select the IP to use for the upgrade.
2. A new panel with additional information about the IP appears to the right. Click **Deploy Profile:upgrade to (version number)**.
3. The **Automated Deployment Wizard** panel displays to the right. Click **Next**.
4. The panel updates to show the **Host set selection** list. Select the host to receive the IP. By default, the host that received the previous version of the IP is already selected. Click **Next**.
5. The panel updates to show the **Application Parameters** list. Values from the previous version of the IP deployment may be displayed in the following fields:
   - **Existing Application Object**—This field is automatically generated by Genesys Administrator Extension for each host to which an IP is targeted. This is the Application object in Configuration Server for which Genesys Administrator Extension will update connections.
   - **Tenant Object**—This is the Tenant that is set on an IP Application object. Click **Browse** to select a Tenant from a list.
   - **App port**—Specify a port number for the Application object to use.
   - **Primary Configuration Server**—Click **Browse** to select the Primary Configuration Server to use. This field defaults to a Genesys Administrator Extension Application object.
   - **Backup Configuration Server**—Click **Browse** to select the Backup Configuration Server to use. This field defaults to a Genesys Administrator Extension Application object.
   - **Skip IP Re-install**—Choose one of the following options:
     - **True**—Reinstall the IP only if the Application object does not exist in Configuration Server.
     - **False**—Always reinstall the IP.
6. Click **Next**.
7. The panel updates to display the **Silent.ini Parameters** list. These values are prepopulated from the previous version of the IP, but the settings can be modified, if necessary.
8. The panel updates to display the **Deployment Summary** report. Review the settings, and perform one of the following actions:
   - Click **Finish** to upgrade the IP.
   - Click **Previous** to return to a previous panel and modify settings.
9. The panel updates to display a progress bar of the upgrade deployment. This information also displays in the **Deployed IPs** panel.

Important

If a deployment fails, you can review a log of the deployment by selecting the IP from the **Deployed IPs** panel. A new panel displays with additional information about the IP. Click **Deployment Action Log**.

Rolling Back an Installation Package

[+] Click to show procedure

1. In the **Deployed IPs** panel, select the IP to roll back.
2. A new panel with additional information about the IP appears to the right. Click **Deploy Profile:rollback to (version number)**n.
3. The **Automated Deployment Wizard** panel displays to the right. Click **Next**.
4. The panel updates to show the **Host set selection** list. Select the host to receive the IP. By default, the host that previously received the IP is already selected. Click **Next**.
5. The panel updates to show the **Application Parameters** list. Values from the previous IP deployment may be displayed in the following fields:
   - **Existing Application Object**—This field is automatically generated by Genesys Administrator Extension for each host to which an IP is targeted. This is the Application object in Configuration Server for which Genesys Administrator Extension will update connections.
   - **Tenant Object**—The Tenant that is set on an IP Application object. Click **Browse** to select a Tenant from a list.
   - **App port**—Specify a port number for the Application object to use.
   - **Primary Configuration Server**—Click **Browse** to select the Primary Configuration Server to use. This field defaults to a Genesys Administrator Extension Application object.
   - **Backup Configuration Server**—Click **Browse** to select the Backup Configuration Server to use. This field defaults to a Genesys Administrator Extension Application object.
   - **Skip IP Re-install**—Choose one of the following options:
     - **True**—Reinstall the IP only if the Application object does not exist in Configuration Server.
     - **False**—Always reinstall the IP.
6. Click **Next**.
7. The panel updates to display the **Silent.ini Parameters** list. These values are prepopulated from the previous deployment of the IP, but the settings can be modified, if necessary.
8. The panel updates to display the **Deployment Summary** report. Review the settings, and perform one of the following actions:
   - Click **Finish** to roll back the IP.
   - Click **Previous** to return to a previous panel and modify settings.
9. The panel updates to display a progress bar of the deployment. This information also displays in the **Deployed IPs** panel.

> **Important**
>
> If a deployment fails, you can review a log of the deployment by selecting the IP from the **Deployed IPs** panel. A new panel displays with additional information about the IP. Click **Deployment Action Log**.

Deployed IPs

The **Deployed IPs** panel displays a list of Installation Packages (IPs) that have been deployed and that you have the required role privileges to view. This list provides the following information about each deployed IP:

- **Name**—The name of the IP.
- **Version**—A version number that is assigned by the person who deployed the IP.
- **Current**—Indicates the IP is the latest successful deployment for the tenant.
- **Profile**—The profile type of the IP.
- **State**—Indicates whether the deployment succeeded or failed.
- **Ended**—The date and time at which the deployment of the IP finished.

Tenancy Permission Settings

Solution Deployment respects tenancy permission settings. You can access only those objects that you have been granted permission to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the **Tenant Filter** button to open the **Tenant filter** panel. In this panel, click the check box(es) beside the tenants that you want to select. Use the **Quick Filter** field in this panel to filter the tenant list.

You can sort the IPs in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

Other Actions

To view additional information, click an IP in the list. A new panel opens to the right. The following actions are available:

- To remove a deployment instance from the list, click **Delete**. This does not delete the IP from the database; it just removes the corresponding history item from the list that is displayed in this screen.
- To redeploy an already deployed IP or restart a previously run deployment, click **Redeploy**. This launches the deployment wizard and populates its fields with the values that were used to deploy the IP. You can alter these values, as required. You will have to provide your credentials for the deployment; these values are not populated.
- To export a file that contains the properties, summary, and actions of an IP for auditing purposes, select an IP and click **Export**.

- View the change history of the deployment in the **Deployment Log** panel by clicking the **Related** button and selecting **Deployment Log**.

Some IPs might have additional versions available that allow you to upgrade or roll back the currently deployed IP. If so, you will see additional buttons called **Deploy Profile:upgrade to (version number)** and/or **Deploy Profile:rollback to (version number)**. Clicking these buttons will activate the deployment wizard to complete the action.

During a deployment, the **Actions** panel is displayed to the right of the **Deployed IPs** list. During the deployment, actions are listed as they are completed. After the deployment is complete, you can view the list in its entirety by scrolling through it.

Solution Definitions

A solution definition is an XML file that describes what is being deployed, how the deployment is to be executed, as well as any necessary pre- and post-installation procedures.

> **Tip**
>
> The Hosted Provider Edition software CD includes four Service Package Definitions for use by Genesys Administrator Extension. They are for the basic deployment of four services: eServices, Inbound Voice, Outbound Voice, and Workforce Management. These files are located in the following folder: **\service\asd\spdFiles**

This screen displays a list of all solution definition files for which you have the required role privileges to view. To refresh the list at any time, click **Refresh**. Click a solution definition in the list, and the **Details** panel is displayed to the right of the list. Actions that are available for each solution definition are applied from the **Details** panel.

You can filter the contents of this list in several ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click **Tenant Filter** to open the **Tenant Filter** panel. In this panel, click the check box(es) beside the tenants that you want to select. Use the **Quick Filter** field in this panel to filter the tenant list.
- You can sort the solution definitions in the list by clicking on a column head. Clicking a column head a second time reverses the sort order.

Viewing Solution Definitions

A solution definition file defines the Genesys component installation packages (IPs) that are required to provide the service, and how they are to be deployed and configured. The IPs that are deployed as part of the solution are the actual software that provide the solution. When you select a solution definition, a new panel is displayed to the right an displays additional information:

- **Name**—The name of the solution definition.
- **Version**—The version of the solution definition
- **Description**—An optional description of the solution definition; this can be modified, as required.
- **Notes**—An optional field for notes about the solution definition; this can be modified, as required.
- **Deployable**—Indicates whether the solution definition can be deployed.

> **Important**
>
> When you are creating a solution definition file, you must give it a unique name and version number. Genesys Administrator Extension will not allow you to import a solution definition if its name or version number is the same as an existing one. Likewise, if you modify a solution definition that is already uploaded, you must increment the version number.

The **IP Availability** area is where you verify that the IPs have been uploaded into the IP repository.

Prerequisites

Before you start deploying a Solution Package by using Genesys Administrator Extension, make sure that you have performed the following tasks:

- Install the latest version of Local Control Agent (LCA) on the target hosts. This also installs and configures the Genesys Deployment Agent on each host. Refer to the *Framework Deployment Guide* for instructions.
- Install Java SDK on the target hosts to enable them to process the deployment instructions.
- Upload the necessary IPs into the IP Repository.

Refer to the *Genesys Administrator Extension Deployment Guide* for a complete list of prerequisites required for Genesys Administrator Extension and Solution Deployment.

Working with Solution Definitions

You can perform the following actions:

- Create Solution Definitions
- Modify Solution Definitions
- Copy Solution Definitions to Tenants
- Deploy Solution Definitions
- Download Solution Definitions
- Delete Solution Definitions
- View the History of Solution Definitions

Create Solution Definitions

[+] Click to show procedure

Procedure: Creating Solution Definitions

Prerequisites

Before you create a solution definition file by using Genesys Administrator Extension, you must perform the following tasks:

- Prepare the solution definition file.
- Upload all of the Genesys-component installation packages (IPs) that are required to provide the solutions into an IP repository to which Genesys Administrator Extension has access.

> **Important**
>
> When you create a solution definition file, you must give it a unique name and version number. Genesys Administrator Extension will not allow you to a import a solution definition if its name or version number is the same as the name or version number of an existing one. Likewise, if you modify a solution definition that is already uploaded, you must increment the version number.

Steps

1. In the **Solution Definitions List** screen, click **+**.
2. In the **Upload Solution Definition** area that is displayed to the right of the **Solution Definition List**, click **Browse** to browse to and select the solution definition for this solution definition file.
3. Click **Upload**. The name of the solution definition file, as defined in the solution definition, is displayed in the list.
4. To verify that the solution definition file can be deployed, perform the following steps:
   a. In the list of solution definition files, click the solution definition file that you imported in the previous steps.
   b. Verify that the solution definition file can be deployed by selecting **Check IP Availability** from the **Related** menu.
   c. The required IPs that were found in the IP repository and those that are missing are displayed in the **IP Availability** area that is displayed. Missing IPs must be uploaded to the IP repository before this solution definition file can be deployed. When all IPs are found, the solution definition file is complete and can be marked as **Deployable**.

5. If there are no missing IPs, in the **Properties** area of the **Details** panel, check the **Deployable** check box.
6. Click **Save** to save your changes or **Cancel** to leave the solution definition file unchanged.

Modify Solution Definitions

[+] Click to show procedure

Procedure: Modifying Solution Definitions

Steps

1. In the **Solution Definition List** screen, select the solution definition that you want to modify.
2. In the **Properties** area that is displayed to the right of the **Solution Definition List**, modify the following fields, as required:
   - **Description**
   - **Notes**
   - **Deployable**
3. Click **Save** to save your changes or **Cancel** to leave the solution definition unchanged.

Copy Solution Definitions to Tenants

[+] Click to show procedure

Procedure: Copying Solution Definitions to Tenants

Steps

1. Click the name of a solution definition to select it. A new panel opens to the right.
2. In the new panel, click **Related** and select **Copy to Tenants**. A new panel called **Copy to Tenants** opens to the right.
3. In the **Copy to Tenants** panel, type the name of a Tenant in the **Quick Filter** field, or click **Browse** to browse a list of tenants in your environment. A new panel called **Tenants** opens to the right.
4. Click the check box beside each tenant that is to receive the solution definition. The name of the Tenant appears in the **Copy to Tenants** panel, in the **Targeted Tenants** section.
5. Click **Next** at the bottom of the **Copy to Tenants** panel.
6. Click **Finish** to copy the solution definition to the tenant(s).

Deploy Solution Definitions

Deploying a solution installs and configures the solution at a local or remote location, as directed by the solution definition.

[+] Click to show procedure

Procedure: Deploying Solution Definitions

Steps

1. In the **Solution Definition List** screen, select the solution definition file that you want to deploy.
2. In the **Properties** area that is displayed to the right of the **Solution Definition List**, click **Related** and select **Install** or **Deploy Profile**.
3. Follow the steps in the Deployment Wizard.

> **Important**
>
> The **Deploy Profile** type varies, depending on the profile specified in the solution definition file. For example, **profile name="upgrade"** would produce a

Deploy Profile: upgrade button.

Download Solution Definitions

[+] Click to show procedure

Procedure: Downloading Solution Definitions

Steps

1. Select the solution package for which you want to export the solution definition. A new panel opens to the right.
2. Click **Download**. Genesys Administrator Extension initiates the download procedure in your browser.

Delete Solution Definitions

When you delete a solution definition file, the solution definition file is not deleted from the database, nor are the IPs deleted from the IP repository.

[+] Click to show procedure

Procedure: Deleting Solution Definitions

Steps

1. In the **Solution Definition List** screen, select the solution definition file that you want to delete.

2. In the **Properties** area that is displayed to the right of the **Solution Definition List**, click **Delete**.
3. In the Confirm Deletion dialog box, do one of the following:
   - To remove the solution definition file from the database, click **OK**.
   - To keep the solution definition file and not remove it from the database, click **Cancel**.

View the History of Solution Definitions

Solution packages might change over time. They might be upgraded (up-versioned) to include both minor and major changes in the solution definition. New solutions might be added, removed, or retired. Genesys Administrator Extension enables you to generate reports to track these changes.

[+] Click to show procedure

Procedure: View the History of Solution Definitions

Steps

1. Select a solution from the **Deployed Solution List**.
2. Click **Related** and select **History**. The **History** panel is displayed to the right of the **Deployed Solutions List**. You can filter reports by one or more of the following criteria: **Time**, **User**, **Tenant**, and **Change**.

Deployed Solutions

The **Deployed Solutions** screen displays a list of solution packages that have been deployed and that you have the required role privileges to view. The **Deployed Solution List** table provides the following information about each deployed solution:

- **Name**—The name of the solution package.
- **Version**—A version number that is assigned by the person who deployed the solution.
- **Progress**—A graphical indicator of the progress of each deployment.
- **Current**—Indicates the solution package is the latest successful deployment for the tenant.
- **Profile**—The profile type of the solution.
- **State**—Indicates whether the deployment succeeded or failed.
- **Deployed by Tenant**—The name of the tenant that deployed the solution.
- **Deployed by User**—The login name of the person who deployed the solution.
- **Started**—The date and time at which the deployment of the solution was started.
- **Ended**—The date and time at which the deployment of the solution finished.
- **Key**—The tenant that received the deployed solution.

Tenancy Permission Settings

Solution Deployment respects tenancy permission settings. You can access only those objects that you have been granted permission to access.

You can filter the contents of this list in two ways:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click the **Tenant Filter** button to open the **Tenant filter** panel. In this panel, click the check box(es) beside the tenants that you want to select. Use the **Quick Filter** field in this panel to filter the tenant list.

Sort the solutions in the list by clicking a column head. Clicking a column head a second time reverses the sort order.

Other Actions

The **Deployed Solutions** screen also features the following actions:

- To refresh the list at any time, click **Refresh**.

- To view deployment information for a deployment instance, click a solution definition file in the list. Deployment information for that deployment instance is displayed to the right of the list.
- To remove a deployment instance from the list, click **Delete**. This does not delete the solution definition file from the database; it just removes the corresponding history item from the list that is displayed in this screen.
- To redeploy an already deployed solution definition file or to restart a previously run deployment, click **Redeploy**. This launches the deployment wizard and populates its fields with the values that were used to deploy the solution definition file. You can alter these values, as required. You will have to provide your credentials for the deployment; these values are not populated.
- To export a file that contains the properties, summary, and actions of a deployed solution for auditing purposes, select a Deployed Solution and click **Export**.
- View the change history of the Deployment in the **Deployment Log** panel by clicking the **Related** button and selecting **Deployment Log**.

During a deployment, the **Actions** panel is displayed to the right of the **Deployed Solution List**. During the deployment, actions are listed as they are completed. After the deployment is complete, you can view the list in its entirety by scrolling through it.

> ### Important
> You cannot use the **Redeploy** button to redeploy a solution definition that has been deleted.

Privileges

The **Privileges** section displays a list of all privileges that are stored in Genesys Administrator Extension (GAX). It is sorted in a hierarchy by application and privilege grouping.

You can sort the items in the list by clicking a column head. Clicking a column head a second time reverses the sort order. You can add or remove columns by clicking the Select Columns button.

The **Privileges** section contains the following information:

- **Display Name**—The name of the privilege
- **Since Version**—The first version of the installation package that uses this privilege
- **Prerequisite**—Any other privilege that might be required

Roles and their privileges define what you can do in a given application. In GAX, roles and their privileges are controlled by the use of Role objects, which are assigned to Users (including Agents) and Access Groups.

For a sectioning of role privileges for GAX, refer to the *Genesys Administrator Extension Deployment Guide*. For more information about role privileges specifically, and role-based access control in general, refer to the *Genesys Security Deployment Guide*.

Privileges are imported into GAX during the upload of an installation package (IP). All privileges defined in the metadata of the IP are imported into the GAX database. Privileges are defined as "task" elements in the metadata XML of the IP.

Click **Browse** to add privileges from the **Privileges** panel. To remove a privilege from the **Assigned Privileges** list, highlight the item, and click **Remove**.

Operational Parameter Management

Operational Parameter Management (OPM) enables the creation of operational Parameters that are stored in the Configuration Database as part of Transaction objects. These Parameters can be used in parameterized Routing Strategies and other applications that are capable of reading Transaction objects, in which the values of the parameters are defined at runtime and integrated into the call flow.

In the case of Universal Routing Server type routing, Operational Parameter Management proceeds as follows—however, OPM also works in a similar way with other routing types, such as voice applications and Genesys Orchestration:

- The Service Provider defines the Parameter by specifying its type and a name by which it is referenced in a strategy, voice application, or other routing strategy.
- The Service Provider groups Parameters into a Parameter Group Template. One Parameter can be associated with one or more templates.
- The Service Provider deploys Parameter Group Templates to Tenants, at which time each Parameter Group Template becomes a Parameter Group for the Tenant. One Parameter Group Template can be deployed to more than one Tenant. Each Parameter Group in a Tenant is unique.
- The Tenant administrator, or a user with the appropriate permissions and role privileges, enters values for the Parameters in the Parameter Group, enabling control of active strategies. Genesys Administrator Extension stores those values in the Configuration Database as part of a Transaction object.
- The Universal Routing Server Application executes a Routing Strategy, which reads the values of the Parameters in the Parameter Groups with which it is associated, and integrates them into the call flow.

Operational Parameter Management respects tenancy permission settings. You can access only those objects that you have been granted permission to access.

The Operational Parameters Management module can be accessed from the **Routing Parameters** menu on the GAX header bar, and includes the following:

- Parameters
- Parameter Groups
- Group Templates

Parameters

Operational Parameters are parameters used to customize Routing Strategies. In Operational Parameter Management, the Service Provider defines Parameters and groups them into Parameter Group Templates. Tenants to whom the Parameter Group Templates are subsequently deployed customize the values of the Parameters, which are then read by a Routing Strategy and incorporated into the call flow.

Viewing Parameters

This screen displays a list of all defined Parameters for which you have the required role privileges to view. To refresh the list at any time, click **Refresh**. Click a Parameter in the list. Its properties, including its type, is displayed to the right of the list. You can filter the contents of this list in several ways:

- Type the name or partial name of the Parameter, Key, Type, or Tenant in the Quick Filter field.
- Click the **Tenant Filter** button (the icon with the circle and horizontal bar) to open the Tenant filter panel. In this panel, click the checkbox(es) beside the tenants that you want to select. Use the Quick Filter field in this panel to filter the tenant list.
- You can sort the Parameter in the list by clicking on a column head. Clicking a column head a second time reverses the sort order.

Properties

Properties of Parameters

Property	Description
Display Name	The name of the Parameter. It must be unique in the system.
Key Name	The name of the Parameter as it would be entered in the Annex/Options tab of the Transaction object in Genesys Administrator. If this field is left blank, the name that is displayed under Display Name is used.
Type	The Parameter.
Object Type	This field appears only for Parameters of Type Configuration Object, and specifies the type of configuration object. Optionally, when Configuration Object is selected, you can check the checkbox named **Multiple Types** to select multiple configuration objects to add to this Parameter. If the checkbox named **Global** is checked, a separate panel will open to allow you to select which tenants will receive the Parameter.

Property	Description
DN Type	This field appears only for Parameters of Type Configuration Object and Object Type DN, and specifies the type of DN.
Custom List Custom Value	These properties apply only to Parameters of type Custom List and specify the members of the Custom List. Define the list, as follows: • To add an item to the list, enter it in the Custom Value edit box, and click Add. • To modify an item in the list, select the value, make the change, and click OK. Important If you want the display value of an item in the Custom List to be different from the actual value stored in the transaction object, enter that information in the Key field. • To remove an item from the list, select it, and click Delete. • To reorder the items in the list, select an item in the list and use the Up and Down arrow buttons to move it up or down in the list. • For integers, dates, and times, you can define minimum and/or maximum values (limits).
Mandatory	Specifies whether the Parameter is mandatory or optional. If checked, a value must be entered for this Parameter before it is saved. If not checked, the Parameter is considered optional and can be saved without a value. This property can be modified later (for example, to change a mandatory Parameter to an optional Parameter).
Global	If checked, this Parameter is unique in the entire system and is shared across all tenants. Its actual value must be defined at the time of creation, and can be changed only by the Service Provider.
Value	If this Parameter is Global, this is the actual value of the Parameter and cannot be changed. A default value can be set that is not propagated to deployed Parameter Group instances. Providing of a default value is optional.
Help Text	Optional text describing the Parameter or providing additional information.

Types

The Parameter type appears in the Type field of the properties of a Parameter.

Type	Description
Audio Resource	The ARID of an Audio Resource.
Boolean	True or false only.
Configuration Object	The type of a configuration object, which is specified in the Object Type field of the Parameter's properties. Optionally, when Configuration Object is selected, you can check the checkbox named **Multiple Types** to select multiple configuration objects to add to this Parameter. If the checkbox named **Global** is checked, a separate panel will open to allow you to select which tenants will receive the Parameter. The following types are supported: • Agent Group • DN • Person (more often referred to as User) • Place • Place Group • Skill • Stat Server • Transaction
Custom List	Valid values are limited to the values that are specified in a user-defined list, specified in the Custom List/Custom Value field of the properties of the Parameter.
Date	A date value, in the format yyyy-mm-dd.
Integer	A 0 (zero), negative, or positive number with no decimal value.
Personality	The name of a Personality, given by the Personality Identifier value that is specified in the list of Personalities.
Schedule	Enables users to configure date and time ranges.
String	A string of characters, both alphanumeric and symbols.
Time	A time value, in the format hh:mm.

Schedule Parameter

[+] Click to show section

The Schedule Parameter enables users to specify a series of date and time ranges for Parameter Groups. For example, the Schedule Parameter can specify opening and closing hours for each Tenant.

Procedure:

Steps

1. On the **Parameter List** panel, click **+**.
2. On the **+** panel that is displayed to the right of the **Parameter List** panel, define the properties of the new Parameter.
3. In the **Type** field, select **Schedule**. A new section called **Schedule** appears below the **Type** field.
4. In the **Schedule** section, click **Add**.
5. In the **Date** panel that appears to the right, select the **Schedule** type. You can select **Date**, to select a specific date, or you can select **Day of Week**, to select a day of the week.

   If you select **Date**:

   a. You must select the **Year, Month, Day, and Time Zone** (optional) to apply the Schedule Parameter. If you do not select a **Time Zone**, the system's local time zone will be used.

   b. The **Time Ranges** field is optional. This field graphically represents the time range for the Schedule Parameter, based on a 24-hour clock. If the **Time Ranges** field is empty, the Schedule Parameter will apply to the entire day. To specify a time range:

      i. Move your mouse cursor to the time for which you want this Schedule Parameter to begin.

      ii. Click and drag the mouse cursor to the end time for this Schedule Parameter. A box will appear to visually display the times for which this Schedule Parameter will apply.

      iii. Click the **Save** button.

   If you select **Day of Week**:

   a. You must select the **Day of Week** and **Time Zone** (optional) to apply the Schedule Parameter. If you do not select a **Time Zone**, the system's local time zone will be used.

   b. The **Time Ranges** field is optional. This field graphically represents the time range for the Schedule Parameter, based on a 24-hour clock. If the **Time Ranges** field is empty, the Schedule Parameter will apply to the entire day. To specify a time range:

      i. Move your mouse cursor to the time for which you want this Schedule Parameter to begin.

      ii. Click and drag the mouse cursor to the end time for this Schedule Parameter. A box will appear to visually display the times for which this Schedule Parameter will apply.

      iii. Click **Save**.

3. In the **+** panel, do one of the following:

- To save the new Parameter, click **Save**.
- To cancel the new Parameter and not save it in the database, click **Cancel**.

Working with Parameters

You can perform the following tasks in this screen:

- Define new Parameters
- Modify Parameters
- Delete Parameters

Defining Parameters

Normally, the Service Provider defines new Parameters. Tenant administrators can also define their own, but these can be added only to Parameter Group Templates in the same tenant.

[+] Click to show procedure

Procedure: Defining Parameters

Steps

1. On the **Parameter List** panel, click **+**.
2. On the **+** panel that is displayed to the right of the **Parameter List** panel, define the properties of the new Parameter.
3. Do one of the following:
   a. To save the new Parameter, click **Save**.
   b. To cancel the new Parameter and not save it in the database, click **Cancel**.

Modifying Parameters

[+] Click to show procedure

Procedure: Modifying Parameters

Steps

> **Important**
> Follow the instructions in this topic to modify any property of a Parameter except **Value**. To set or change the actual value of a Parameter in a Parameter Group, see "Setting and Modifying Values in Parameter Groups" in the Procedures tab of the Parameter Groups page.

When you modify a Parameter, the changes are propagated to any Parameter Group Templates that contain the modified parameter. However, the changes are not propagated to any deployed Parameter Groups.

1. On the **Parameter List** panel, select the Parameter that you want to modify.
2. On the <Parameter name> panel that is displayed to the right of the **Parameter List** panel, modify the properties of the Parameter, as required.
3. Click **Save** to save your changes, or click **Cancel** to leave the Parameter unchanged.

Deleting Parameters

You can delete only Parameters that are not assigned to Parameter Group Templates.

[+] Click to show procedure

Procedure: Deleting Parameters

Steps

1. On the **Parameter List** panel, select the Parameter that you want to delete.
2. On the <Parameter name> panel that is displayed to the right of the **Parameter List** panel, click **Delete**.

3. In the Confirm Deletion dialog box, do one of the following:
   a. To remove the Parameter from the database, click **OK**.
   b. To keep the Parameter and not remove it from the database, click **Cancel**.

Parameter Groups

Parameter Groups are sets of Parameters that are associated with a Routing Strategy. They are deployed as Parameter Group Templates by the Service Provider to the Tenant. The Tenant administrator then assigns values to the Parameters in the Parameter Group. When the URS application executes a Routing Strategy, the values of the Parameters in the associated Parameter Group are incorporated into the call flow.

Access to each Parameter Group is based on the access control settings of the Configuration Transaction object. The following are general guidelines:

- If a user has **Update** permission to the Transactions folder, where the related Configuration Transaction object will be saved, the user can create a new Parameter Group.
- If a user has **Read** permission to the related Configuration Transaction object, the user can view the Parameter Group.
- If a user has **Update** permission to the related Configuration Transaction object, the user can save the Parameter Group.
- If a user has **Delete** permission to the related Configuration Transaction object, the user can delete the Parameter Group.

Viewing Parameter Groups

This screen, viewable only if you have the required role privileges, displays a list of all Parameter Groups to which the logged-in user has access. To refresh the list at any time, click **Refresh**.

If you are using GAX 8.5.220 or earlier, all Parameter Groups in the Tenant are displayed, subject to your access privileges to that Tenant. Starting in GAX 8.5.230, the list appears as a hierarchical tree of folders of Tenants, Configuration Units, and Folders to which the corresponding Parameter Group Templates were deployed, and for which you have access in Configuration Server. Therefore, you might not see all of the Parameter Groups in a Tenant, only those in Folders to which you have access.

To sort the list, click a column header. Click the header a second time to reverse the sort order.

To filter the list:

- Type the name or partial name of an object in the **Quick Filter** field.
- Click **Tenant Filter** to open the **Tenant filter** panel. In this panel, click the checkboxes beside the tenants that you want to select. Use the **Quick Filter** field in this panel to filter the tenant list.

Click the name of a Parameter Group to display more information about the Parameter Group in a new panel that opens to the right. Users can click **Access Control** to change the permissions for the Parameter Group, provided that they have **Update** permission for the object.

Working with Parameter Groups

You can perform the following tasks in this screen:

- Set or modify the values of the Parameters in the Parameter Group
- Change the template that a Parameter Group uses to another Template as its basis
- Delete a Parameter Group

Set or Modify Values

The Parameters in Parameter Groups might be assigned default values. It is the responsibility of the Tenant administrator, or someone with the appropriate role privileges, to assign values to these Parameters that are applicable to the Tenant.

[+] Show steps

1. On the **Parameter Group List** screen, select the Parameter Group that you want to modify.
2. On the **Parameters** panel that is displayed to the right of the **Parameters Group List** screen, enter or modify values for each of the Parameters, as required.
3. Click **Save** to save the changes, or click **Cancel** to cancel the changes and leave the Parameter Group unchanged.

> **Important**
>
> It is possible to modify values of Parameter Groups from applications other than GAX (for example, Genesys Administrator or the Configuration Layer). When this occurs, a message appears on the Parameter Group details panel to alert you that the Parameter Group is out of synchronization. You are asked to choose a value from one of the following options:
>
> - **Value from Database**——The value stored in the Genesys Administrator Extension database will be used.
> - **Value from Transaction Object**—The external value will be used.
>
> Click **Save** to synchronize the Parameter Group.

Change the Template

You can change the Parameters that are associated with a Parameter Group and which designated applications the group uses. This cannot be done directly in the Parameter Group, nor in the Parameter Group Template that was used to deploy the Parameter Group.

[+] Show steps

1. Create a new Parameter Group Template by copying the current Parameter Group Template of the Parameter Group that you want to change. Select the Parameter Group Template.

2. In the **<Parameter Group name>** panel that is displayed to the right, click **Change Template**.
3. In the **Change Template** panel that is displayed to the right, select the new Parameter Group Template from the **Targeted Parameter Group Template** field.
4. Click **Next**.
5. Review the Summary in the **Change Template** panel.
6. Click **Finish**.
7. Click **Close**.

If the existing Parameters and/or the designated applications are in the new Parameter Group Template that you want to change them to, then they will be reused. The following content is removed from the changed Parameter Group:

- Parameters that are not in the new Parameter Group Template to which you want to change
- Designated Applications that are not in the new Parameter Group Template to which you want to change

The transaction object that represents the Parameter Group is updated with the new parameter set.

Delete a Parameter Group

When you delete a Parameter Group from the database, the Parameter Group Template and its Parameters are not removed from the database. Likewise, the Routing Strategy with which it is associated is not deleted. The main impact of this action is that when URS executes this Routing Strategy for this Tenant, the Parameter values in the Group will not be incorporated in the call flow.

[+] Show steps

1. On the **Parameter Group List** screen, select the Parameter Group that you want to delete.
2. On the <Parameter Group name> panel that is displayed to the right of the Parameter Group List panel, click **Delete**.
3. In the Confirm Deletion dialog box, do one of the following:
   a. To remove the Parameter Group from the database, click **OK**.
   b. To keep the Parameter Group and not remove it from the database, click **Cancel**.

Parameter Group Templates

Parameter Group Templates are sets of Parameters that can be deployed to one or more Tenants, and are defined by the Service Provider. A parameter can be included in more than one Group Template. You can also group sets of parameters into sections within a Parameter Group Template to enable you to create Parameter Group Sections within your parameter groups.

Viewing Parameter Group Templates

This screen displays a list of all defined Parameter Group Templates for which you have the required role privileges to view. If you are using GAX 8.5.0 or earlier, all Parameter Group Templates in the Tenant are displayed, subject to your access privileges in the Tenant. In GAX 8.5.2, the list appears as a hierarchical tree of folders to which the corresponding Parameter Group Templates were deployed. However, you can see only those folders for which you have the appropriate role privileges. Therefore, you might not see all of the Parameter Group Templates in the Tenant, only those in the folders to which you have access.

To refresh the list at any time, click **Refresh**. Click a Parameter Group Template in the list, and its properties are displayed to the right of the list.

To sort the Templates in the list, click a column header. Clicking the header a second time reverses the sort order.

To find particular Templates in the list:

- Type the name or partial name of an object in the **Quick Filter** field. The list dynamically updates to show items that match the text in the **Quick Filter** field.
- Click **Tenant Filter** to open the **Tenant filter** panel. In this panel, click the checkboxes beside tenants that you want to select. Use the **Quick Filter** field in this panel to filter the tenant list.

Properties

The properties of Parameter Group Templates are described in the following table:

Property	Description
Name	The name of the Parameter Group Template. It must be unique in the system.
Description	Optional text describing the Parameter Group Template or providing additional information.
Parameters	A list of Parameters that have been added to the Parameter Group Template. The Section(s) to which this Parameter Group Template belongs is also displayed here.

Property	Description
	Important Sections can be deleted. Deleting a section only deletes the section grouping, and does not delete the set of Parameters previously within that section.
Used	(Read-only) Used to deploy a Parameter Group.

Working with Parameter Group Templates

You can perform the following tasks in this screen:

- Create Parameter Group Templates
- Modify Parameter Group Templates
- Delete Parameter Group Templates
- Manage the list of Parameters in a Parameter Group Template
- Distribute Parameter Group Templates
- Associate applications
- Determine where a Parameter Group Template is used and then change the Parameter Group Template that a Parameter Group uses to a different Parameter Group Template
- View the change history of the Parameter Group Template in the History panel by clicking **Related** and selecting **History**

Create Parameter Group Templates

The Service Provider creates Parameter Group Templates, and assigns Parameters to them.

[+] Show steps

1. On the **Parameter Group Template List** panel, click **+**.
2. On the **+** panel that is displayed to the right of the **Parameter Group Template List** panel, enter the properties (including adding Parameters) of the new template.
3. Optionally, you can click **Add Section** to add the Parameter Group Template to a section in the **Parameter Group Template** list. A new panel opens to the right. Perform the actions below:
   - In the new panel, type the name for the new section in the **Name** field.
   - Type the key name for the new section in the **Key Name** field.

> **Important**
> These fields must be unique in the Parameter Group Template.

4. Click **Save** to save the new Parameter Group Template, or click **Cancel** to cancel the new template and not save it in the database.

Modify Parameter Group Templates

Changes that you make to a Parameter Group Template are not propagated to Parameter Groups that use that template.

[+] Show steps

1. On the **Parameter Group Template List** panel, select the Parameter Group Template that you want to modify.
2. On the <Parameter Group Template name> panel that is displayed to the right of the **Parameter Group Template List** panel, modify the properties of the Parameter Group Template, as required.
3. When you are finished modifying the Parameter Group Template, click **Save** to save your changes, or click **Cancel** to cancel your changes and leave the Parameter Group Template unchanged.

Delete Parameter Group Templates

You cannot delete a Parameter Group Template that is currently deployed.

[+] Show steps

1. On the **Parameter Group Template List** panel, select the Parameter Group Template that you want to delete.
2. On the <Parameter Group Template name> panel that is displayed to the right of the Parameter Group Template List panel, click **Delete**.
3. In the Confirm Deletion dialog box, do one of the following:
   a. To remove the Parameter Group Template from the database, click **OK**.
   b. To keep the Parameter Group Template and not remove it from the database, click **Cancel**.

Manage the list of Parameters

In a Parameter Group Template, you can manage the list of Parameters in the following ways:

- Add Parameters to a Parameter Group Template **[+] Show steps**
  1. Select the Parameter Group Template to which the Parameter is to be added in the list of Parameter Group Templates.
  2. In the **Parameters** list, click **Add**.
  3. In the **Parameters** panel that is displayed to the right, select the Parameter(s) that you want to add. The selected Parameter(s) are now displayed in the **Parameters** list.
  4. Click **Save**.
- Change the order of the Parameters in the list of Selected Parameters **[+] Show steps**
  1. Select the Parameter Group Template in which the order of Parameters is to be changed.

2. In the **Parameters** list, select a parameter that you want to move, and click the up or down arrow to change its order in the list. You can also drag the parameter and drop it into a new position in the order.
3. Click **Save**.

- Remove Parameters from a Parameter Group Template **[+] Show steps**
  1. Select the Parameter Group Template from which the Parameter is to be removed.
  2. In the **Parameters** list, select a Parameter that you want to remove and click **Remove**.
  3. Click **Save**.

Distribute Parameter Group Templates

The Service Provider deploys Parameter Group Templates to Tenants, at which point, the Parameter Group Template becomes a Parameter Group in that Tenant.

Starting in release 8.5.230, you can deploy Parameter Group Templates to specified Folders and Configuration Units within the Tenant. This enables each Tenant to restrict access to particular Parameter Groups based on a user's permissions to that Configuration Unit or Folder. Previously, all users with access to the Tenant could access all Parameters.

You can modify a Parameter Group Template after it has been deployed. For example, you can add, remove, re-order, and/or modify the parameters in an already deployed Parameter Group Template. {{NoteFormat|If you have changed the schema of the Template, be aware that pressing the **Sync** button restores the rest of the Template (*below* the change) to default values. You will then have to set the values for that part of the Template back to the correct values.

[+] Show steps

1. On the **Parameter Group Template List** panel, select the Parameter Group Template that you want to deploy.
2. On the <Parameter Group Template name> panel that is displayed to the right of the **Parameter Group Template List panel**, click **Deploy**.
3. In the **Parameter Group Deployment** panel, do the following:
   a. In the **Parameter Group Name** field, enter the name that is assigned to this Parameter Group.
   b. In the **Tenant** field, use the folder icon to select the Tenant to which this Parameter Group belongs.
   c. (Optional) In the **Folder** field, use the folder icon to select the Transactions Folder to which this Parameter Group Template is to be deployed. You can deploy Parameter Group Templates to specified Folders and Configuration Units within the Tenant. This enables each Tenant to restrict access to particular Parameter Groups based on a user's permissions for a specified Folder or Configuration Unit. Leave this field blank if you prefer that all users with access to the Tenant have access to all Parameters and associated Templates, as has always been the case.
   d. Click **Next**.
   e. Select the applications to be associated with this Template in the Associated Applications panel.
4. Preview the deployment in the Summary. If you are satisfied with the deployment, click **Finish**. To make changes, click **Previous**.
5. Click **Close**.

Audio Resource Management

Audio Resource Management (ARM) enables you to manage personalities and their associated audio resources (announcements and music files).

You can create Personalities to help you organize which files belong to a particular speaker. For example, you might have a personality called `John` that uses dialog spoken in English by a male speaker. Or, you might have a personality called `Marie` that uses dialog spoken in French by a female speaker.

You can upload two types of audio resources:

- Announcements—These are files that contain spoken dialog that will be played for customers. For example, you might have an announcement file that tells customers about your business hours.
- Music—These are files that play music for customers. For example, you might have a music file that plays music for customers who are about to be transferred to an Agent.

ARM is integrated with Operational Parameters Management (OPM) to allow users to dynamically select personalities and audio resources to be used with a parameterized strategy or orchestration application, or a parameterized routing or voice application.

Access to ARM is based on both role privileges and Tenant access control permissions, as follows:

- User access to screens or certain ARM functionality is managed by role privileges.
- Access control permissions define which audio resources can be viewed or modified by an authenticated user. Access to audio resources is granted by Tenant. Users have access to all audio resources for each Tenant to which they have access.

For Service Providers, see Audio Resources (Configuration Manager) for information on how to share resources with Tenants.

Viewing Audio Resources

The **Audio Resources** window in Genesys Administrator Extension (GAX) is a unified list of your personalities and audio resources. To display the list, select **Audio Resources** in the **Routing Parameters** menu.

For each audio resource, GAX displays the following:

- A logo to indicate whether the file has been designated as `Announcement` or `Music`.
- The name of the audio resource.
- The Audio Resource ID (ARID). In a single-tenant environment prior to GAX 8.5.2, audio resources were assigned ARIDs in the range of 9000 to 9999 inclusive, imposing a limit of 1000 audio resources. Starting in GAX 8.5.2, the range was increased to 1000 to 9999 inclusive, increasing the number of available ARIDs to 9000.

- Additional columns, one for each personality, to indicate which personality is using this audio resource. The personalities are listed in alphabetical order. By default, all personalities to which the audio resource is assigned is listed. To hide (or unhide) personalities shown in the list for a particular tenant, click **Show Quick Filter** and select **Hide/Show Personalities** (located on the far right) to open a list of all personalities available to this Tenant. Select those personalities that you want displayed, and clear the checkbox for those that you do not want displayed.

> **Tip**
> Click or clear the checkbox for **All** first if you want a majority of the personalities displayed or not displayed, respectively, then click/clear individual personalities as needed to fine-tune the list.

To sort the list based on a column, click in the column's header. Clicking a second time reverses the sort order.

To find the name of a Audio Resource, click **Show Quick Filter** and type the name or partial name of an object in the **Quick Filter** field. The list updates dynamically to show items that match the text in the **Quick Filter** field.

Working with Personalities

Creating a Personality

To create a new Personality, do the following:

[+] Show steps

1. Click **New** and select **Add Personality**.
2. Enter the following information:
   - **Personality Name**—The name of this personality.
   - **Language**—The language spoken by this personality.
   - **Description**—A description of this personality.
   - **Gender**—Select whether this personality is `Male`, `Female`, or `Not Specified`.
3. Click **Save**.

Uploading Audio Resources

To upload an audio resource and assign it to a personality, do the following:

[+] Show steps

1. Identify which audio resource and personality to assign to the file. Once identified, select or hover over the table cell that is shared by the target audio resource and personality.

2. Click **Upload Audio File**.
3. Your browser opens a dialog box to select an audio resource to upload. Select a file to upload.
4. The audio resource is uploaded to GAX and assigned to the personality.

Other Actions

After you have created a personality, you can:

- **Edit** the personality—Click **Edit** beside a personality to edit personality properties.
- **Delete** the personality—Click **Edit** to view personality properties. In the **Edit Personality** window, click **Delete** to delete the personality.

> **Important**
> You cannot delete a Personality that is a part of one or more Audio Resource Files.

- **Manipulate** the audio resource—Once an audio resource is assigned to the personality, several options become available to manipulate the file.
  - **Play** the file—Click the play icon to listen to the file.
  - **Delete**—Delete the file. This does not delete the associated personalities, but it does delete the original audio files. A file can only be removed if the audio resource to which it has been assigned has not been deployed. If the user performing this operation is a Service Provider, the file can only be removed if the file was not created by a Tenant.
  - **Replace**—Reassign this audio resource to another personality.
  - **Download**—Download the file to your computer.
  - **Reprocess**—Reprocessing recreates an audio resource file from the original audio file that was uploaded (if it has not been deleted from the database and/or target storage). It also performs any necessary conversion between audio formats.
  - **Encodings**—View information about how the file was encoded by GAX. When audio files are uploaded, GAX automatically encodes them to the following formats: **µ-law**, **A-law**, and **GSM**. Only **.wav** files are supported for uploading.

Audio Resources

Creating an Audio Resource

To create an Audio Resource, click **New**.

[+] Show Procedure

1. Click **New** and select **Add Message**.

2. Enter the following information:
   - **Name**—The name of this audio resource.
   - **Description**—A description of this audio resource.
   - **Type**—Select whether this audio resource is `Music` (a music file) or `Announcement` (an announcement file).
3. Click **Save**.

Uploading Audio Resources

To upload an Audio Resource, do the following:

[+] Show Procedure

1. Identify which audio resource and personality to assign to the file. Once identified, select or hover over the table cell that is shared by the target audio resource and personality.
2. Click **Upload Audio File**.
3. Your browser opens a dialog box to select an audio resource to upload. Select a file to upload.
4. The audio resource is uploaded to GAX and assigned to the personality.

Deleting Audio Resources

To delete an Audio Resource:

[+] Show Procedure

1. Click the check box beside the audio resource that you want to delete.
2. Click **Delete**.

> **Important**
>
> - If you delete an audio resource, all files that are associated with it are also deleted.
> - If you are deleting an audio resource that is being used by Operational Parameter Management, and this Audio Resource being used by one or more parameters or Parameter Groups, a message is displayed that indicates this fact. When this happens, you can only cancel the deletion—you cannot force the deletion.

Other Actions

Once you upload a file, you can select or highlight it and choose one of the following actions:

- Play the file—Click the play button to listen to the file.

> **Important**
>
> Internet Explorer does not support playing the audio file directly. You have to download the file and playback the file locally. Firefox cannot play µ-law and A-law audio codecs. Only PCM Audio codecs can be played in Firefox.

- **Delete**—Delete the file. This does not delete the associated personalities, but it does delete the original audio files. A file can only be removed if the audio resource to which it has been assigned has not been deployed. If the user performing this operation is a Service Provider, the file can only be removed if the file was not created by a Tenant.
- **Replace**—Replace this personality with another one.
- **Download**—Download the file to your computer.
- **Reprocess**—Reprocessing recreates an audio resource file from the original audio file that was uploaded (if it has not been deleted from the database and/or target storage). It also performs any necessary conversion between audio formats.
- **Encodings**—View information about how the file was encoded by GAX. When audio files are uploaded, GAX automatically encodes them to the following formats: **µ-law**, **A-law**, and **GSM**. Only **.wav** files are supported for uploading.

Audit Logs

Starting in GAX 8.5.25x, additional Audit logs have been added to Audio Resource logs in the Centralized Log Database to provide an audit trail of configuration changes to Audio Resource and Personalities. You can view these logs in the Centralized Logs list, by selecting **Application** > **All Logs** or **Audit** in the side panel on the left.

The new Audit Logs log the following tasks:

- Create Personality
- Modify certain properties of a Personality, namely the Name, Language, Description, and Gender properties.
- Delete Personality
- Create Audio Resource
- Modify certain properties of an Audio Resource, namely the Name, Description, and Type properties.
- Delete Audio Resource
- Upload/Replace Audio File
- Reprocess Audio File
- Delete Audio File
- Download Audio File

Two additional columns have been added to the list of logs, but only if you are looking at a list of Audit logs generated from the **Audit** section of the side panel. They are:

- **User Name—**Specifies the name of the user who modified that particular object in GAX. If the log message contains a link to the field that was changed, this column entry is left blank.
- **Object Type—**Specifies the object type that was modified by the user. If the log message explicitly contains a link to the field that was changed, this column entry is left blank.

Centralized Logs

The Centralized Log Database contains log messages generated by Genesys applications. The Centralized Log plugin for Genesys Administrator Extension displays a summary of those logs, from which you can select and investigate any that are of special interest. As with all objects in GAX, you can only see those logs for which you have the required privileges.

> **Important**
>
> The Centralized Log Database supports only the Oracle, Microsoft, and PostgreSQL DBMS; IBM DB2 is not supported.

Log messages stored in the Centralized Log Database are of two types:

- Application logs: Generated by most Genesys applications, these logs feature the same unified log record format.
- Audit logs: Generated by only a few applications (notably Configuration Server and Solution Control Server), these logs contain additional attributes and information about configuration changes and control actions performed for processes, solutions, and alarms.

To view the Centralized Log, select **Centralized Logs** in the GAX menu bar.

Centralized Log Window

Log records are displayed in the Centralized Log window.

In the window, the menu on the left shows the views that are available for display, including any Saved Searches.

> **Important**
>
> Audit Logs are displayed only in the Audit view, and in the results of any searches where the **Type** criteria is set to `Audit`.

Above the list of logs, the following information and controls appear:

- The number of logs that have been retrieved, and the total number of logs to be retrieved. To minimize any delays caused by retrieving all records from a Log Database that contains a huge number of records, records are retrieved in batches from the Database (default batch size is 100); more records are retrieved when you have scrolled halfway through the existing list. In addition, to increase performance, the number of records that can be displayed by GAX is limited (default number of records is 5000). If these parameters are not adequate for you, you can change them using the **minlogs** and

maxlogs options (respectively). Refer to the "clog Section" of the *Genesys Administrator Extension Deployment Guide*.

- Search criteria used to select the logs in the list. By default, only logs generated on the current day (**Date Range:** Today) are selected. See Filtering Logs for more information about selecting logs using filters.
- Four control icons:
  - Opens the search window, in which you set filters to create the list of logs in which you are interested, or at least reduce the list down to a more manageable size.
  - Removes selected logs from the list. To select a log for deletion, select the check box in the first column. Select as many as required, or select the check box in the header row to select all of the displayed records.

    > **Warning**
    > If you select the check box in the header row, you will also be prompted to select all records in the database (not just the displayed records) that meet the same criteria as the displayed records. Choose this option ONLY if you are sure that you want to select for deletion all the records in your database that meet those criteria.

  - Enables you to select what columns (attributes) are displayed in the list.
  - Refreshes the display.
- Quick filter box—Enter text in this box to search for specific logs without using the full filter capability. Those logs containing that text (including numbers, such as the log ID) will be returned and listed. This filter is case-insensitive, and is cumulative—the query is evaluated and performed, and the list of results is updated as you type each character. For best results, enter as many characters as you can.

Each log record is displayed with some or all of its attributes, as follows:

- **Level**—The log level of the log, either Alarm, Standard, Interaction, or Trace.
- **ID**—The unique identifier of the log, in the format `<Application id>-<message ID>`, where <Application ID> is the Application ID of the Application that generated the log, and <message ID> is the numeric identifier of the log message, unique within the component that generated the log.
- **Description**—The text of the log message.
- **Host**—The host on which the Application that generated the log was running.
- **App**—The name of the Application that generated the log.
- **Date**—The date and time when the log was generated.
- **Interaction ID**—The identifier of the interaction for which this log was generated. This attribute appears only for Interaction-level logs.

You can also click and customize what attributes (columns) are displayed; by default, all columns are displayed.

The actual attributes displayed depends on the selection made in the menu on the left of the window, and on the attributes that you have chosen to display. For example, the **Level** attribute is not displayed if you have selected to display only Standard-level logs.

Click in the line of any log to see additional attributes.

Viewing Logs

In the Centralized Log window, you can:

- View all Application-type logs, by selecting **All Logs** under **Applications** in the left-hand menu.
- View all logs of a certain level, by selecting the appropriate level under **Applications**. For example, to view all Standard-level Application logs, select **Standard** under **Applications**.
- View all Audit-type logs, **All Logs** under **Applications** in the left-hand menu.
- View all logs meeting criteria defined in a saved search, by selecting the search name under **SAVED SEARCHES** in the left-hand menu.
- Create a new search for all logs meeting specified criteria, by filtering the logs based on specified criteria.

By default, GAX displays the logs sorted by their **Date** attribute. You can sort also them by their **Level**, **ID**, **Description**, **Host**, **App**, and **Date** (and time) when they were generated. Click in a header cell to sort the list by that attribute and/or to change the order of the list (ascending or descending).

Searching for Logs

You can search for specific logs by filtering a list of logs by one or more search criteria. Click  to open the filter window. From this window you can perform a Basic Search or an Advanced Search:

- Basic search—Enables you to view a subset of the logs using a basic set of criteria.
- Advanced search—With specified privileges, enables you to filter the list using additional criteria, save the searches, manage the list of saved searches, and remove some or all of the logs.

Click **Save As** to save up to 10 defined searches, for use at a later time. If you want to save a new search but have already saved 10, you must delete one of the existing searches (click the **x** that appears when you hover the mouse on the search name) before saving the new one. You can also drag the search names up and down to reorder them in the list.

> ### Tip

- Before starting your search, be sure that all log records have been retrieved from the database—check the record count in the top right corner of the Centralized Log window.
- If all you want to do is search for log records containing some text, or even a log record with a unique ID, you can most likely get the same results as a Basic or Advanced Search by entering the text in the Filter Table box at the top-left of the window.

Basic Search

In a basic Search, you can filter logs based on **Host**, **Application**, **Tenant**, **User**, **Date**, and/or **Description**.

Note the following when performing a basic search:

- You can enter only one filter value for each attribute.
- The **Host**, **Application**, **Tenant**, and **User** filters contain drop-down lists of the values of the corresponding attribute for each log record in the original list.
- The **Date** filter includes eight predefined filter values, as follows:
  - `Last 5 Minutes`
  - `Last 15 Minutes`
  - `Last 1 Hour`
  - `Today`
  - `Yesterday`—Current and previous days
  - `Last 5 Days`—Current and last 5 days
  - `Last 30 Days`—Current and last 30 days

  All days start at midnight (00:00:00); minute and hourly intervals are measured from the time when the filter is run.

  You can also select **Custom Date Range** and select a range of dates and times in the adjacent calendars that appear.
- The **Description** filter has no drop-down list; enter any text that might be found in the **Host name**, **Application name**, or **Description** of the log. This is somewhat different from the **Quick Filter** box located above the record list, in that this field looks only for matching text in three attributes, so cannot be used to look for a log of a given number.

To filter the logs, select a value for one or more search criteria, and click **Search**. The logs that meet the specified criteria are listed.

Advanced Search

To use the Advanced Search filter, you must have the ACCESS_CLOGS privilege. This advanced filter gives you more search criteria, and if you have the DELETE_CLOGS privilege, you can also delete

from the Centralized Log Database some or all of the log records returned by your query.

To define an Advanced filter, first enter any filter criteria for a Basic Search. Then click the arrow next to Advanced Search. The Search window expands to show the additional filters with which you can search for logs, specifically:

- **Log Type**—`Application` or `Audit`
- **Log Level**—`Alarm`, `Standard`, `Interaction`, or `Trace`
- Name of **Solution** in which the log was generated.
- Type and name of configuration objects that have been changed.
- Key name and value of attributes that have been changed.

To clear a value from a filter, click **Reset**; to clear all filters click **Reset All Filters**. To remove only some of the Key:Value pairs entered in the **Attributes** filter, click the adjacent  .

In the list of records returned by the Advanced Search, you can view and sort the log records as usual. Click  to delete selected records from the Centralized Log Database. (You must have the DELETE_CLOGS privilege to delete records.)

Log Levels

Genesys Administrator reports log events at four levels of detail: Alarm, Standard, Interaction, and Trace. Log events of these levels feature the same unified log record format and can be stored in the Centralized Log Database.

In addition, some applications also generate Audit logs. These Audit logs usually contain additional attributes and information about configuration changes and control actions performed for processes, solutions, and alarms.

Alarm Level

Alarm-level logs contain only log records of the Alarm level. Solution Control Server (SCS) generates Alarm log events on behalf of other applications when receiving from them log events configured as Detection Events in Alarm Conditions. Using this level, SCS reports the occurrence and removal of all alarms to the Centralized Log Database.

Standard Level

Standard-level logs contains high-level events that report both major problems and normal operations of in-service solutions. An event is reported at the Standard level if it satisfies one of these criteria:

[+] Show criteria

- Indicates that an attempt to perform any external operation has failed
- Indicates that the latest attempt to perform an external operation that previously failed has succeeded
- Indicates detection of a condition that has a negative impact on operations, actual or projected
- Indicates that a previously detected condition, which had a negative impact on operations, no longer exists
- Indicates a security violation of any kind
- Indicates a high-level data exchange that cannot be recognized or does not follow the expected logical sequence
- Indicates inability to process an external request
- Indicates successful completion of a logical step in an initialization process
- Indicates a transition of an application from one operational mode to another
- Indicates that the value of a parameter associated with a configurable threshold has exceeded that threshold
- Indicates that the value of a parameter associated with a configurable threshold that earlier exceeded the threshold has returned to its normal range

Interaction Level

Interaction-level logs report the details of an interaction processed by solution components that handle interactions. The log contains information about the processing steps for each interaction by each solution component. An event is reported at the Interaction level if it:

- Is a recognizable high-level data exchange with another application about an interaction.
- Indicates a change in real-time state of an interaction handled by the application (unless such a change is visible from the high-level data exchange).

The specific criteria depend on a particular component and its role in interaction processing.

Trace Level

Trace-level logs report the details of communications between the various solution components. The log contains information about the processing steps for each interaction by each solution component. An event is reported at the Trace level if it satisfies one of these criteria:

- It is a recognizable high-level data exchange with another application.
- It is a recognizable high-level data exchange with an external system.
- It indicates a change in real-time state of user-level objects that the application handles (unless such a change can be seen from the high-level data exchange).

For More Information

For more information about logging in Genesys software, refer to the *Framework 8.5 Management Layer User's Guide*. For descriptions of the logs themselves, refer to *Framework Combined Log Events Help*.

Troubleshooting GAX

Lost Connections to Database

If the Configuration Server is connected directly to the Configuration Database (**dbthread**=`true` in the Configuration Server Application object), and the connection to the Database is lost for some reason, try using the Configuration Server Application runtime option **force-offline** to restore the connections.

This option, set in the Configuration Server section of the primary Configuration Server Application object, stops and starts connections to the Configuration Database. By default, it is set to `false`, since the connections are enabled at startup and do not need to be restored. If the connections have been lost, do the following:

1. Set **force-offline**=`true`. This stops all connections to the Configuration Database, and puts Configuration Server (and therefore GAX) in read-only mode.
2. Set **force-offline**=`false`. This restores all connections to the Configuration Database, and restores Configuration Server (and therefore GAX) to read-write mode.

This action, in effect, jump-starts the connections.

> **Warning**
> When you are swapping GAX in and out of read-only mode, do not change the Configuration Server Application object in any other way.

Error Messages

This section describes error messages that you might receive when using GAX, and provides recommended actions to resolve or mitigate the error. Error messages are displayed in a red banner at the top of the page in which they occur.

Mirroring Errors

A mirroring error will read something like this:

```
Cannot mirror folder path <path name> under <folder name> folder of switch <switch name>
Please check GAX log for more detail.
```

Description

This error is generated when you are creating an agent in a specific folder structure and specifying the DNs and Agent Logins, but do not have the correct permissions to any folder in the path.

Recommended Actions

Ensure that the user creating the agent has correct permissions for the specified folder.