



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Genesys Administrator Extension Help

Configuration Manager

5/5/2025

Configuration Manager

Configuration Manager enables you to create and manage system-level configuration objects such as Alarm Conditions, Business Attributes, Hosts, and more.

Overview

Configuration Manager Overview

The **Configuration Manager** page is a central location for viewing and managing the configuration objects used by your system. Genesys Administrator Extension can manage objects in single-Tenant and multi-Tenant configurations.

Configuration objects, also known as Configuration Database objects, contain the data that Genesys applications and solutions require to operate in a particular environment. These objects are all contained in the Configuration Database.

Configuration Manager lists these objects by type. For example, configuration objects related to outbound campaigns are listed under the **Outbound** heading.

Click on a configuration object type to view a list of the related configuration objects on your system. From this list, you can edit or delete the existing configuration objects, or you can create a new configuration object.

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.

Click on a topic below to learn more about Configuration Manager.

Object Hierarchy

[+] Click here to reveal section

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

Importing/Exporting Data

[+] [Click here to reveal section](#)

Most configuration objects allow you to import and export data, such as configuration options, by clicking **More** and selecting **Import** or **Export**. Genesys Administrator Extension uses the CFG/CONF file formats.

Refer to the File Formats tab, above, for more information on acceptable file formats for import.

Required Permissions

[+] [Click here to reveal section](#)

The minimum permissions required to perform a task in Genesys Administrator Extension depend on

the task. For more information about permissions, see the Permissions tab, above.

You must also be granted appropriate **Role privileges** to perform specific tasks on an object or group of objects.

| Permission | Description | Prerequisites |
|------------|---|---------------|
| Read | <ul style="list-style-type: none">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 on an object to view its details. | None |
| Create | <ul style="list-style-type: none">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 | <ul style="list-style-type: none">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. | Read |

| Permission | Description | Prerequisites |
|------------|--|---------------|
| | <ul style="list-style-type: none">In object detail views, you can view the following buttons: Enable or Disable, Save, and Apply. | |
| Delete | <ul style="list-style-type: none">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 |

Manipulating Multiple Objects

[+] Click here to reveal section

Genesys Administrator Extension uses **Bulk Change Sets** to manipulate several objects at once. For example, you can use Bulk Change Sets to add and/or remove multiple users at once. You can use Bulk Change Sets to replicate the wizard functionality in Genesys Administrator.

Naming Conventions

[+] Click here to reveal section

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 Database 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.

Common Properties

Common Object Properties

All objects have the following configuration properties and elements:

- Name**—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**—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.

Permissions

Permissions

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 8.1 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

[+] Click here to reveal procedure

Procedure: Changing Members

Steps

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

Procedure:

Steps

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

Procedure:

Steps

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.

Configuration Options

Configuration Options

Important

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

The **Options** tab enables you to set configuration options for the object. You can perform the following actions:

Creating an Option

[+] Click here to reveal procedure

Procedure: Creating an Option

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. 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.

Updating an Option

[+] Click here to reveal procedure

Procedure: Updating an Option

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.

Deleting an Option

[+] Click here to reveal procedure

Procedure: Deleting an Option

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.

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.

Dependencies

Dependencies

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 have been 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.

Security

Assigning 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.

Security certificates are assigned at the **Host** level, and optionally at the **Application and Port** levels. The Host certificate is used by Applications and Ports by default, unless the Applications and Ports specify their own certificates. In this case, those specific certificates override the default Host certificate.

For more information about deploying TLS, refer to the [Genesys 8.1 Security Deployment Guide](#).

File Formats

Supported File Formats

The CFG/CONF file format is a plain-text format. The CFG format is for use on Microsoft Windows systems, and the CONF format on UNIX systems.

Both formats support only the import and export of string options. Other types of configuration options are ignored and not imported or exported.

Syntax

The syntax of the .cfg and .conf files is identical. 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:

```
[section_name1]
option_name1=option_value2
...
option_nameN=option_valueN

[section_name2]
option_nameN+1=option_valueN+1
...
```

Example

The following excerpt from a configuration file illustrates the correct syntax in a .cfg or .conf file:

```
[confserv]
port=2520
management-port=2521
server=dbserver
encryption=false
encoding=utf-8

[log]
verbose=standard
all=stderr

[hca]
schema=none
```