Genesys Interaction Recording Solution Guide

Configuring permissions, access control, and privacy

12/19/2025

Configuring permissions, access control, and privacy

Contents

The following sections describe, and provide examples of how to configure access control for Genesys Interaction Recording Users.

For more information about controlling the access for voice recording users, see Access Control for Voice Recording Users.

Configuring SpeechMiner roles and permissions

Configuring SpeechMiner users

All SpeechMiner users must be assigned to the `Users` Access Group. If agent hierarchy and partition features are not used, assign all the SpeechMiner users to the / (slash) Access Group. If agent hierarchy or partition features are used, the users must be granted to the specific Access Groups in order to be able to access recordings for the various agent hierarchy and partitions.

Important

- To restrict log-in to the SpeechMiner UI, a new Configuration Manager application object must be created. Backup the default Configuration Manager object, since this object is accessible by all users from all tenants. The new Configuration Manager application object should be configured to allow Environment administrators, Environment users and Super administrators access to it.
- To see members in the User Access Group (by default, SpeechMiner Users) in the Speechminer UI, Log On As the account of Speechminer_WEB application should have Read rights to User Access Group.

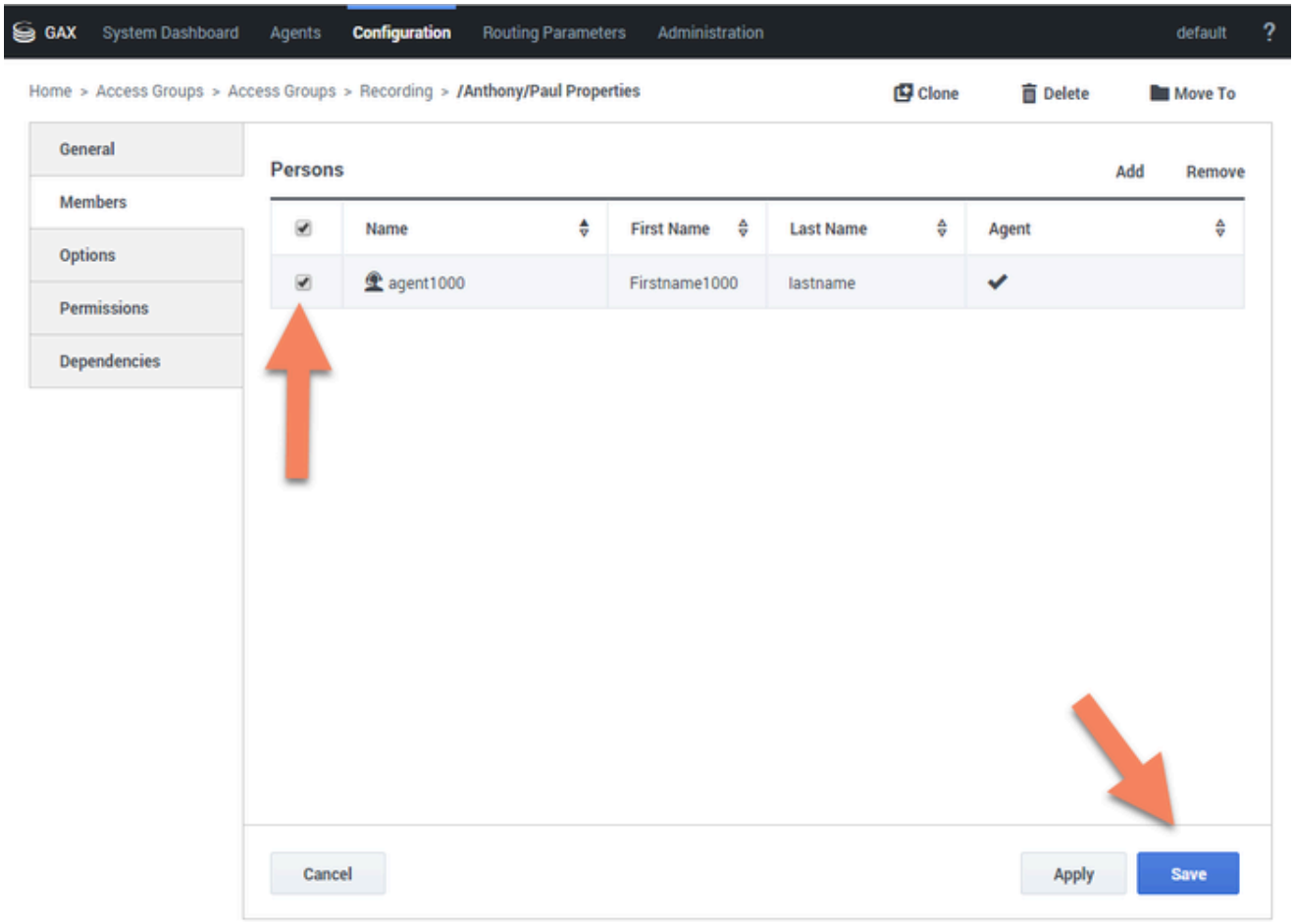
You must configure Genesys Interaction Recording to enable the SpeechMiner UI search option to display a list of agent names:

1. In the Agent's **Person** object, create a **[recording]** section in the **Annex** (if it doesn't already exist).
2. Add the **agent_hierarchy** option in the **[recording]** section, and set the value to slash: "/" or what is appropriate for access control.
3. Repeat these steps for any additional agents that might be searched for in the SpeechMiner UI.
4. This configuration will not take effect until the SpeechMiner cache is updated:
   - In the **SMConfig > Recording** tab, update the **`Update Agents Every`** parameter to the number of hours between the SpeechMiner person object updates. SpeechMiner will check the Configuration Server according to this option to retrieve the list of person objects under the **Recording folder** access group. The names of these agents are then available when searching for call recordings or screen recordings.
   - To force the list of agents to update sooner, update the **`NextAgentsUpdate`** column in the **`configServer`** table of the SpeechMiner database to a date in the near future.

Important

- The Access Group / (forward slash) grants access to all recordings.

The following is a screen shot showing the assignment of Access Group members to `/Anthony/Paul` in Genesys Administrator Extension:



The Recording Plug-in for GAX includes a Solution Definition (SPD) file that can be used to configure roles and access groups.

Configuring roles

For information about configuring roles for Genesys Interaction Recording users, see Role Privileges in the Genesys Administrator Extension Deployment Guide.

Configuring permissions for recording labels

A label definition defines a label, which can then be applied to a recording. For example, a label definition could be created to mark a recording for further review.

Permissions are required to perform these operations. You can configure the label permissions using Genesys Administrator Extension (GAX), in the IRWS_Cluster (or WS_Cluster, where applicable) application object or the Person object.

To configure label permissions, do this:

1. If you're configuring this at the application level: add a new recording settings group to the Annex/ Application options group for the IRWS_Cluster (or WS_Cluster where applicable) application object, or update the existing recording group. For details, refer to Genesys Administrator Extension Help: Configuration Manager and Installing Interaction Recording Web Services.

   > **Important**
   >
   > You are not required to do it this way; you can also set this at the Person object level.

2. Configure one or all of the following options in the recording settings as follows:

```
[recording]
RECORDING_PERMISSION_ADD_LABEL_DEFINITION = true
RECORDING_PERMISSION_DELETE_LABEL_DEFINITION = true
RECORDING_PERMISSION_ADD_LABEL = true
RECORDING_PERMISSION_DELETE_LABEL = true
```

The system applies permissions in the following order:

1. Default settings that are defined in the application code, which are overridden by:
2. Settings that are specified in the Application, which are overridden by:
3. Settings that are specified in the Person object that corresponds to the agent.

The following permissions are required to allow users with the role supervisor or agent to be able to access and use the different label operations.

Permission	Description	Applies to	Checks against
RECORDING_PERMISSION_ADD_LABEL_DEFINITION	Permission to create a label definition	• Creating a label definition • Updating a label definition	• Supervisor • Agent

Permission	Description	Applies to	Checks against
RECORDING_PERMISSION_DELETE_LABEL_DEFINITION	Permission to delete a label definition	• Deleting a label definition	• Supervisor • Agent
RECORDING_PERMISSION_ADD_LABEL	Permission to add/update label(s) on a recording	• Adding a label to a recording • Updating a label on a recording • Adding a label to multiple recordings	• Supervisor • Agent
RECORDING_PERMISSION_DELETE_LABEL	Permission to delete label(s) from a recording	• Deleting a label from a recording	• Supervisor • Agent

Configuring Permissions for Recording Non-Deletion

You can protect recordings from deletion using SpeechMiner, or using the Recording Non-Deletion API, if you have the appropriate permissions that are required.

You can configure the non-deletion permissions using Genesys Administrator Extension (GAX), in the Configuration Manager view, the IRWS_Cluster (or WS_Cluster where applicable) application object or the Person object. Contact center administrators have full access by default.

To configure non-deletion permissions, do this:

1. If you're configuring this at the application level: add a new recording settings group to the Annex/Application options group for the IRWS_Cluster (or WS_Cluster, where applicable) application object, or update the existing recording group. For details, refer to Genesys Administrator Extension Help: Configuration Manager and Installing Interaction Recording Web Services.

   > **Important**
   >
   > You are not required to do it this way; you can also set this at the Person object level.

2. Configure one or both of the following options in the recording settings as follows:

```
[recording]
RECORDING_PERMISSION_APPLY_NON_DELETE = true
RECORDING_PERMISSION_UNAPPLY_NON_DELETE = true
```

The system applies permissions in the following order:

1. Default settings that are defined in the application code, which are overridden by:
2. Settings that are specified in the Application, which are overridden by:
3. Settings that are specified in the Person object that corresponds to the agent.

The following permissions are required to allow users with the role of supervisor or agent to be able to access and use the different non-deletion operations.

Permission	Description	Applies to	Checks against
RECORDING_PERMISSION_APPLY_NON_DELETE	Permission to protect a recording from being deleted	Apply Non-Deletion to a Recording	• Supervisor • Agent
RECORDING_PERMISSION_UNAPPLY_NON_DELETE	Permission to remove deletion protection from a recording	Remove Non-Deletion from a Recording	• Supervisor • Agent

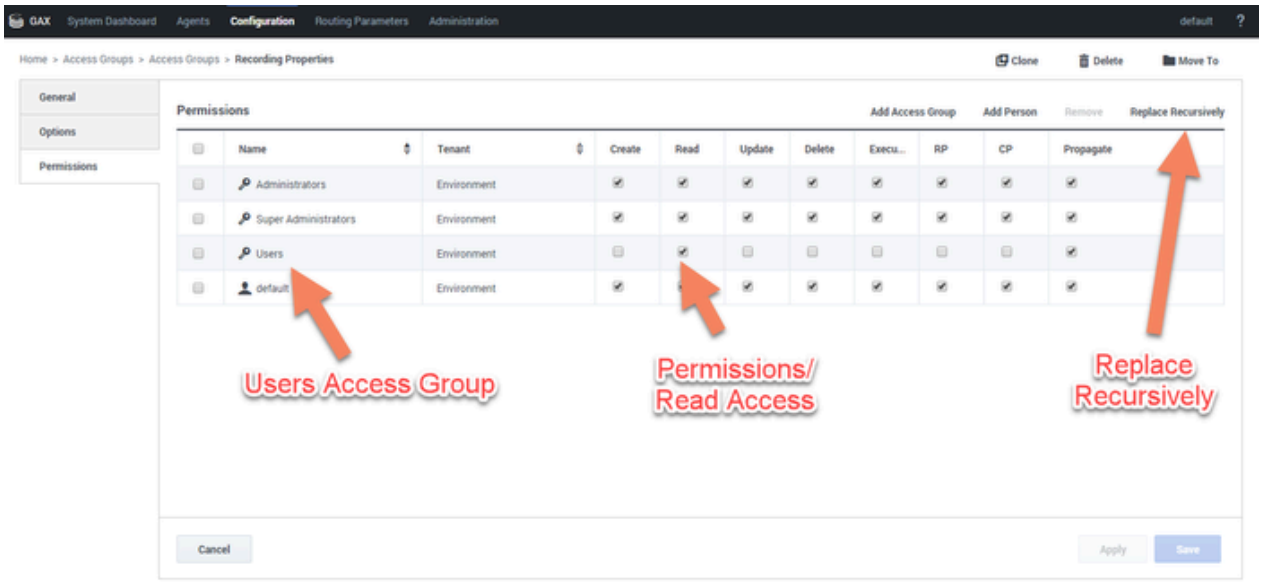
Configuring access control and agent hierarchy

Configuring access groups

By default, the Configuration Server has an **Access Group** called `Users` stored in the configuration database.

Install the Solution Deployment SPD file "Creation of base access groups" option to perform the following steps:

1. Create an **Access Group**, and set the permission to grant the users in the Access Group with Read access.
2. Add a new folder within Access Groups, called **Recording**, and set the permission to add the `Users` Access Group with Read access. Make sure the `Replace Permissions Recursively` action is set as shown in the following diagram:



3. Create the / (forward slash) Access Group within the **Recording** folder.

> ### Important
> If this **User Access Group** exists in more than one tenant, use unique naming conventions; otherwise, the users will not appear in the SpeechMiner UI.

Configuring partitions

For each partition used in the contact, create an **Access Group** object with the name of the partition within the **Recording** folder. For example, if there are three partitions— `/sales`, `/support`, and `/marketing`, create three **Access Group** objects named `/sales`, `/support`, and `/marketing`, respectively.

> ### Important
> Access Group names for partitions and agent hierarchy must be unique for each tenant.

Configuring agent hierarchy

Agent hierarchy and partitions are not required to record calls or access recordings; however, all agents must be assigned to the `Users` Access Group.

If agent hierarchy is required, assign the agent's hierarchy by configuring the `agent_hierarchy` option in the `recording` section of the `Person` object's Annex tab. For each hierarchy name, create a corresponding **Access Group** object within the **Recording** folder.

For the example above, create the following **Access Groups**:

- `/`
- `/Anthony`
- `/Anthony/John`
- `/Anthony/Paul`

> **Important**
>
> The `agent_hierarchy` field for a user should not include that user's name. For example, David's `agent_hierarchy` can be:
>
> - `/Genesys/Tel Aviv/`
>   Not:
> - `/Genesys/Tel Aviv/David`
>
> Every user can only be part of one hierarchy (a single path) in the entire hierarchy tree. For example:
>
> - If the hierarchy for David is `/Genesys/Toronto`, then John's hierarchy cannot be `/Genesys/Tel Aviv/David`. That is, David cannot be a part of two different hierarchies.
> - `/Genesys/Tel Aviv/BE` and `/Genesys/Toronto/BE` should not exist in the same hierarchy tree. But, `/Genesys/BE/Tel Aviv` and `/Genesys/BE/Toronto` can exist in the same hierarchy tree.

Configuring user access control

Agents and users can be seen by a logged in user based on the logged in user's read permissions to the agents and users Person objects in the Configuration Server. Additionally, access to items within SpeechMiner (for example, Forms, Evaluations, Reports and so on), is also limited based on read permissions to the creator of those items.

To limit which agents and users can be seen by a logged in user you must set **`AccessControlEnabled`** to **`1`** (true) in the **`ConfigServer`** table in the SpeechMiner Database (that is, the database selected during the SpeechMiner installation).

> **Important**
>
> If **`AccessControlEnabled`** is not set to true, all users can see and access all agents and users items within SpeechMiner.

Configuring sensitive data privileges

Sensitive information (for example, credit card numbers, telephone numbers, home addresses and so on) can be hidden from agents when stored in the system.

To configure sensitive data privileges:

1. Add a new Recording settings group to the Annex/Application options group for the GIR cluster application object. For details, refer to '''Genesys Administrator Extension User Guide > Configuration Manager'''
2. Configure one or both of the following options in the Recording settings group created in step #1:
   - **`metadata.privacy.agent_fields`**: Add a comma-separated value of all the metadata fields that must be hidden if the user does not have permission to view the agent metadata fields. For example, `callerPhoneNumber`, `dialedPhoneNumber`, `dnis`, `ani`, `agentIid`, `username`, `phoneNumber`, `username`, `firstName`, `lastName`, `GSIP_RECORD`, and so on.
   - **`metadata.privacy.customer_fields`**: Add a comma-separated value of all the metadata fields that must be hidden if the user does not have permission to view the customer metadata fields. For example, `firstName`, `lastName`, and so on.

> **Important**
>
> Metadata fields with angle brackets or backslashes are not supported.

With the following privileges you can view recording metadata fields that are usually masked from unauthorized users:

- **Customer Sensitive Data:** This privilege enables the user to display customer-sensitive data in the SpeechMiner GUI. When this privilege is enabled, the data is visible.
- **Agent Sensitive Data:** This privilege enables the user to display agent-sensitive data in the SpeechMiner GUI. When this privilege is enabled, the data is visible.

For more information on how to configure the above privileges, refer to Configuring Roles and Privileges in GAX.

> **Important**
>
> - Both the Customer Sensitive Data privilege and the Agent Sensitive Data privilege will not affect report results. That is, sensitive data will be included in reports. If you do not want sensitive data to be included in reports you must disable the relevant report.

For more information about configuring Access Controls in Genesys Administrator Extension, see the Genesys Administrator Extension User Guide.