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 Interaction Recording Solution Guide

Access Control for Recording Users

4/19/2025

Access Control for Recording Users

Contents

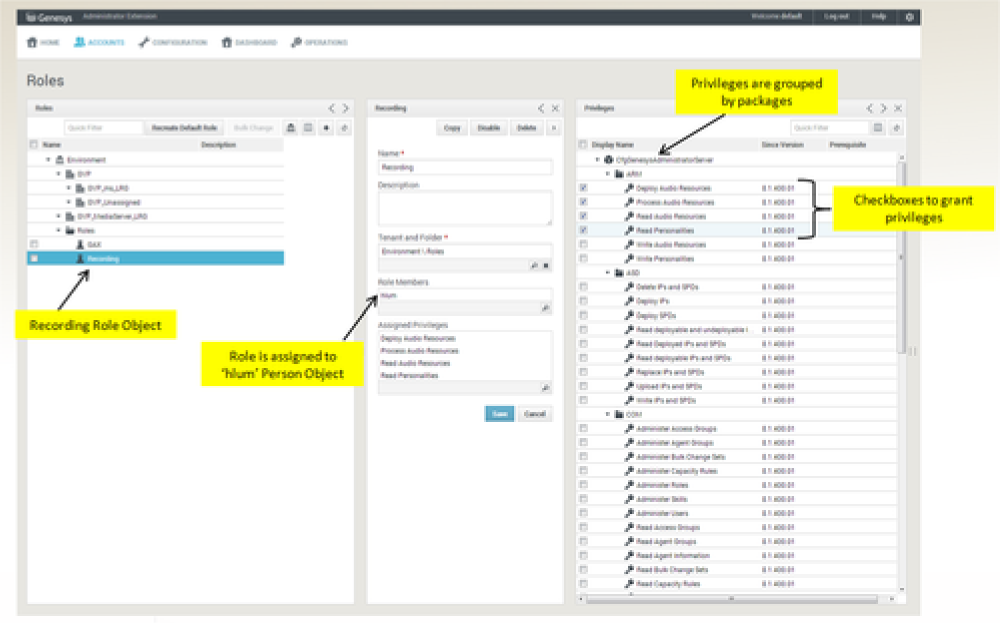
- 1 Access Control for Recording Users
    - 1.1 Recording Files

Configuration Server stores user credentials and provides authorization to those applications requesting these credentials. The Genesys Administrator Extension logs into other dependent web services by forwarding the same credentials to Interaction Recording Web Services (or Web Services if you're using version 8.5.210.02 or earlier). These credentials are required only once.

Roles and privileges use the following basic concept:

- A user (`Person` object) can belong to one or more Access Groups (`Access Group` object).
- One or more roles (`Role` object) can be assigned to an `Access Group` or a user allowing the user to inherit one or more `Roles`.
- A `Role` is a collection of privileges.
- A privilege defines whether the `Role` is enabled for a specific action or function. The specific action or function can be granular based on the application needs.
- A user inherits all privileges from all `Roles` that the user belongs to.

The following screenshot provides an example of privileged assignment using Genesys Administrator Extension:


Roles
Privileges are grouped by packages
Checkboxes to grant privileges
Recording Role Object
Role is assigned to 'hlum' Person Object
Save
Cancel

The user must have the following roles, privileges and permissions:

- `Administration of Recording Certificates and Keys` role privilege to enable uploading and deleting of recording certificates and assigning of recording certificates to IVR profiles
- `Decrypt a Recording` role privilege to view recording certificates and to access recording certificates to playback encrypted recordings
    - If the **show_cert_with_upload_privilege** option in the [**rcs**] section of the GAX application object is set to `true`, GAX will require the user to have the `Administration of Recording Certificates`

and Keys and Decrypt a Recording role privileges to view recording certificates. The default value for the **show_cert_with_upload_privilege** option is false.

- Write access to the IVR profile object to change settings on the Recording tab of the IVR Profile
- Screen Recording Certificates role privilege to view assigned screen recording certificates
- Administration of Screen Recording Certificates role privilege to assign and remove assigned screen recording certificates
- Admin permission on the Interaction Recording Web Services (Web Services) server to view and manage screen recording certificates
- Recording Scheduler role privilege to enable access of recording scheduler settings, and to view recording schedule settings
- Administration of Recording Scheduler role privilege to enable administration of recording scheduler settings
- A role selected by your Administrator that will enable users to view their own recordings. Each administrator can create and choose the required role

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

Recording Files

Each recording file is considered an object that is subject to access control at the user level. When a recording file is generated, the access control for the recording file is set based on the following criteria:

1. Access control is set based on the agent that was recorded. Agents are organized as an agent hierarchy; for example, the hierarchy can be a reporting structure in an organization.

   When there are two agents (agent 1 and agent 2), that are both configured to be recorded and are on the same SIP server, and agent 1 calls agent 2, there will only be one recording and the recording will be associated with the agent that was called (agent 2).

   In the case of an outbound call, the agent initiating the call should be configured to be recorded and not the trunk being used for the outbound call.

   Note: with IVR recording, there is no associated agent for the specific segment of the call, since IVR is not a user.

2. Access control is set based on partitions. Partitions are set as a specific attached data in a call, and the attached data is typically set by a routing strategy.

To search and playback a recording file that is subject to access control, the user accessing SpeechMiner must be assigned to the appropriate Access Groups to access the recordings. If the user accessing SpeechMiner is an agent, they are granted implicit playback access to their own recordings. However, if their agent hierarchy is changed, they will lose access to previous recordings. To enable agents to see their previous recordings, create a new recording access group in the format `/<old agent_hierarchy value>/<agent name>` and add the agent to this recording access group.

Agent Hierarchy

The agent hierarchy shows how the agents are organized in the hierarchy, and the hierarchy is represented as a field (agent_hierarchy option) in the recording section of the Annex tab in each Person (Agent Name) object.

The following example shows the agent hierarchy with four agents:

- /
    - Anthony
        - John
            - Agent1
            - Agent2
        - Paul
            - Agent3
            - Agent4

Agent1 and Agent2 are on John's team. John reports to Anthony.

To represent this structure, the following fields are stored in each of the Person object:

Person Object	agent_hierarchy Field
Agent1	/Anthony/John
Agent2	/Anthony/John
Agent3	/Anthony/Paul
Agent4	/Anthony/Paul

> **Important**
>
> When there are Person objects for items in the path, the path must contain the username for those persons. For example, for the hierarchy /Anthony/John, Anthony and John must match the usernames for Anthony and John.

If a user wants to listen to recordings handled by Agent1, the user needs to be granted access to either the Anthony, or the John Access Group. If a user is granted access to the Anthony Access Group, that user has access to recordings from all four agents, because all four agents are within Anthony’s hierarchy.

Partitions

Partitions are arbitrary names that allows a contact center to partition recordings based on business rules. For example, partitions can be business groups such as sales, support, marketing, etc. To set one or more partitions to a recording, attach data to the call with the GRECORD_PARTITIONS key with a comma-separated list of partition names.

For example, if the GRECORD_PARTITIONS key is set to /sales,/support, the recording belongs to the /sales partition as well as the /support partition.

To access any recording belonging to a partition, the user must be assigned to an Access Group with the same name. For example, if user1 is assigned to the /sales Access Group, user1 can search and playback any recordings within the /sales partition

For examples about how to work with Agent Hierarchy and partitions, see Agent Hierarchy Examples.

For more information about configuring the roles and permissions for Genesys Interaction Recording users, see Access Control for Genesys Interaction Recording Users.