Grant Conversational Analytics API IAM roles and permissions

This product or feature is subject to the "Pre-GA Offerings Terms" in the General Service Terms section of the Service Specific Terms (/terms/service-terms#1). Pre-GA products and features are available "as is" and might have limited support. For more information, see the launch stage descriptions (/products#product-launch-stages).

The Conversational Analytics API uses Identity and Access Management (IAM) (/iam/docs/overview) to control access for creating, managing, and interacting with data agents. With IAM, you grant permissions to *principals* (/iam/docs/overview#principals) (such as users, groups, and service accounts) by assigning roles to the principals. Each role is a collection of one or more permissions that determines what actions a principal can perform.

This page describes the predefined IAM roles for the Conversational Analytics API. You can assign these IAM roles in the Google Cloud console for the project in which the Conversational Analytics API is enabled. For detailed instructions, see Granting roles using the Google Cloud console (/iam/docs/granting-changing-revoking-access#grant-single-role). You can also use the Google Cloud CLI (/sdk/gcloud/reference/projects/add-iam-policy-binding) to grant roles, as described in Grant IAM roles (#grant-iam-roles).

Before you begin

To get the permissions that you need to assign Conversational Analytics API IAM roles, ask your administrator to grant you the Project IAM Admin (/iam/docs/roles-permissions/resourcemanager#resourcemanager.projectIamAdmin) (`roles/resourcemanager.projectIamAdmin`) IAM role on the project in which the Conversational Analytics API is enabled. For more information about granting roles, see Manage access to projects, folders, and organizations (/iam/docs/granting-changing-revoking-access).

You might also be able to get the required permissions through custom roles (/iam/docs/creating-custom-roles) or other predefined roles (/iam/docs/roles-overview#predefined).

Note: IAM basic roles (/iam/docs/roles-overview#basic) might also contain permissions to assign Conversational Analytics API IAM roles. You shouldn't grant basic roles in a production environment, but you can grant them in a development or test environment.

Overview of Conversational Analytics API IAM roles

The Conversational Analytics API provides a set of predefined IAM roles. These roles let you grant permissions for tasks such as creating and editing agents, sharing and managing agents, viewing and chatting with agents, and using the API in a stateless chat mode.

Note: Conversational Analytics API IAM roles control access to agents and their configurations, not to the underlying data itself.

The predefined IAM roles for the Conversational Analytics API are part of the `geminidataanalytics` service. The technical names for these roles follow the pattern `roles/geminidataanalytics.`*`ROLE_NAME`*. In the Google Cloud console, you can find these roles by filtering for the **Gemini Data Analytics** service.

You can assign Conversational Analytics API IAM roles at the project level.

Required roles for common user tasks

To decide which roles to assign to a principal, consider the following common user tasks.

Create new data agents

> Assign the Gemini Data Analytics Data Agent Creator (#data-agent-creator) role to users who are responsible for creating new data agents within a project.

Manage agent permissions

> Assign the Gemini Data Analytics Data Agent Owner (#data-agent-owner) role to users who need the highest level of control over an agent, including the ability to manage permissions and share or delete agents. When a user creates an agent, the system automatically grants this role to that user for the specific agent.

Edit agent configurations

Assign the Gemini Data Analytics Data Agent Editor (#data-agent-editor) role to users who modify an agent's configuration, such as its context or data source mappings. These users don't have permissions to share or delete the agent.

Chat with agents

Assign the Gemini Data Analytics Data Agent User (#data-agent-user) role to users or applications that primarily interact with agents by asking questions and receiving responses.

View agent configurations

Assign the Gemini Data Analytics Data Agent Viewer (#data-agent-viewer) role to users who need read-only access to view agent configurations.

Chat by using inline context

Assign the Gemini Data Analytics Stateless Chat User (#data-analytics-stateless-user) role to users or applications that interact with the API in a stateless mode, where the user provides all context for the conversation within each request.

For a list of predefined roles and the permissions that they include, see Predefined roles for the Conversational Analytics API (#predefined-roles).

Predefined roles for the Conversational Analytics API

Note: Granting a user access to a data agent doesn't provide the ability to view conversations that were initiated by other users. For example, listing conversations for an agent only returns conversations that were created by the current user.

The following table describes the predefined roles for the Conversational Analytics API. If the predefined roles don't provide the set of permissions that you want, you can also create your own custom roles (/iam/docs/creating-custom-roles).

Role	Permissions
Gemini Data Analytics Data Agent Creator (`roles/geminidataanalytics.dataAgentCreator`) Grants a principal permission to create new data agent resources in a specific project. When a principal creates an agent, the system automatically grants that principal the `dataAgentOwner` role for the specific agent.	`geminidataanalytics.dataAgents.create`

Gemini Data Analytics Data Agent Owner (`roles/geminidataanalytics.dataAgentOwner`)
 	
Grants a principal full control over the lifecycle of any agent within the project, including sharing and deleting agents. This role is for trusted principals who can manage agent sharing. This role inherits all permissions from the `dataAgentEditor`, `dataAgentUser`, and `dataAgentViewer` roles.
 	
A principal with this role can share and delete agents.
	`geminidataanalytics.dataAgents.list`
	
	`geminidataanalytics.dataAgents.get`
	
	`geminidataanalytics.dataAgents.chat`
	
	`geminidataanalytics.dataAgents.update`
	
	`geminidataanalytics.dataAgents.delete`
	
	`geminidataanalytics.dataAgents.getIamPolicy`
	
	`geminidataanalytics.dataAgents.setIamPolicy`

Gemini Data Analytics Data Agent Editor (`roles/geminidataanalytics.dataAgentEditor`)
 	
Grants permission to modify and manage existing agent configurations. This role inherits all permissions from the `dataAgentUser` and `dataAgentViewer` roles.
	`geminidataanalytics.dataAgents.list`
	
	`geminidataanalytics.dataAgents.get`
	
	`geminidataanalytics.dataAgents.chat`
	
	`geminidataanalytics.dataAgents.update`

Gemini Data Analytics Data Agent User (`roles/geminidataanalytics.dataAgentUser`)
 	
Grants permission to chat with the specific agents to which the principal has been granted access. This role inherits all permissions from the `dataAgentViewer` role.
	`geminidataanalytics.dataAgents.list`
	
	`geminidataanalytics.dataAgents.get`
	
	`geminidataanalytics.dataAgents.chat`

Role	Permissions

Gemini Data Analytics Data Agent Viewer (`roles/geminidataanalytics.dataAgentViewer`)
 	
Grants a principal read-only permission to list and view agent configurations. This role doesn't allow chatting with agents.
	`geminidataanalytics.dataAgents.list`
	
	`geminidataanalytics.dataAgents.get`

Gemini Data Analytics Stateless Chat User (`roles/geminidataanalytics.dataAgentStatelessUser`) Grants a principal permission to call the Chat API in stateless mode. With stateless chat, context is provided directly in the request instead of being saved explicitly in the agent configuration during creation.	`geminidataanalytics.chat`

Grant IAM roles

You can grant Conversational Analytics API IAM roles to principals by using the Google Cloud console or the Google Cloud CLI.

consolegcloud (#gcloud)
(#console)

To grant a role to a principal in the Google Cloud console, complete the following steps:

1. In the Google Cloud console, go to the **IAM** page.

   Go to IAM (https://console.cloud.google.com/iam-admin/iam?supportedpurview=project)

2. Click **Grant access**.
3. In the **New principals** field, enter the email address of the user, group, or service account.
4. From the **Select a role** menu, filter for **Gemini Data Analytics** to see the available IAM roles for the Conversational Analytics API.

5. Select the appropriate role, such as **Gemini Data Analytics Data Agent User** (#data-agent-user).
6. Click **Save**.

Last updated 2025-09-12 UTC.