

Manage access to service accounts

This page describes how to grant, change, and revoke a principal's access to a single service account. To manage a principal's access to all service accounts in a project, folder, or organization, manage their access at the [project, folder, or organization level](https://cloud.google.com/iam/docs/granting-changing-revoking-access?authuser=5) (<https://cloud.google.com/iam/docs/granting-changing-revoking-access?authuser=5>).

In Identity and Access Management (IAM), access is managed through *allow policies*, also known as IAM policies. An allow policy is attached to a Google Cloud resource. Each allow policy contains a collection of *role bindings* that associate one or more principals, such as users or service accounts, with an IAM role. These role bindings grant the specified roles to the principals, both on the resource that the allow policy is attached to and on all of that resource's [descendants](https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy?authuser=5) (<https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy?authuser=5>). For more information about allow policies, see [Understanding allow policies](https://cloud.google.com/iam/docs/policies?authuser=5) (<https://cloud.google.com/iam/docs/policies?authuser=5>).

Service accounts are both resources that other principals can be granted access to, and principals that can be granted access to other resources. This page treats service accounts as resources and describes how to grant other principals access to them. To learn how to grant a service account access to other resources, the following guides:

- To grant a service account access to a project, folder, or organization, see [Managing access to projects, folders, and organizations](https://cloud.google.com/iam/docs/granting-changing-revoking-access?authuser=5) (<https://cloud.google.com/iam/docs/granting-changing-revoking-access?authuser=5>).
- To grant a service account access to other resources, see [Managing access to other resources](https://cloud.google.com/iam/docs/manage-access-other-resources?authuser=5) (<https://cloud.google.com/iam/docs/manage-access-other-resources?authuser=5>).

Note: Granting roles on service accounts can allow principals to impersonate service accounts. See [Roles for service account authentication](https://cloud.google.com/iam/docs/service-account-permissions?authuser=5) (<https://cloud.google.com/iam/docs/service-account-permissions?authuser=5>) for more information.

This page describes how to manage access to service accounts using the Google Cloud console, the Google Cloud CLI, and the REST API. You can also manage access using the [IAM client libraries](https://cloud.google.com/iam/docs/client-libraries?authuser=5#iam) (<https://cloud.google.com/iam/docs/client-libraries?authuser=5#iam>).

Note: You can also use deny policies to prevent principals from using specific IAM permissions. For more information, see [Deny policies](https://cloud.google.com/iam/docs/deny-overview?authuser=5) (<https://cloud.google.com/iam/docs/deny-overview?authuser=5>).

Before you begin

- Enable the IAM API.

[Enable the API](https://console.cloud.google.com/flows/enableapi?apiid=iam.googleapis.com&%3) (https://console.cloud.google.com/flows/enableapi?apiid=iam.googleapis.com&%3

- Learn about [service accounts](https://cloud.google.com/iam/docs/service-accounts?authuser=5) (https://cloud.google.com/iam/docs/service-accounts?authuser=5).

Required roles

To get the permissions that you need to manage access to a service account, ask your administrator to grant you the [Service Account Admin](https://cloud.google.com/iam/docs/understanding-roles?authuser=5#iam.serviceAccountAdmin) (roles/iam.serviceAccountAdmin) IAM role on the service account or the project that owns the service account. For more information about granting roles, see [Manage access](https://cloud.google.com/iam/docs/granting-changing-revoking-access?authuser=5) (https://cloud.google.com/iam/docs/granting-changing-revoking-access?authuser=5).

This predefined role contains the permissions required to manage access to a service account. To see the exact permissions that are required, expand the **Required permissions** section:

Required permissions

The following permissions are required to manage access to a service account:

- `iam.serviceAccounts.get`
- `iam.serviceAccounts.list`
- `iam.serviceAccounts.getIamPolicy`
- `iam.serviceAccounts.setIamPolicy`

You might also be able to get these permissions with [custom roles](https://cloud.google.com/iam/docs/creating-custom-roles?authuser=5) (https://cloud.google.com/iam/docs/creating-custom-roles?authuser=5) or other [predefined roles](https://cloud.google.com/iam/docs/understanding-roles?authuser=5) (https://cloud.google.com/iam/docs/understanding-roles?authuser=5).

View current access

The following section shows you how to use the Google Cloud console, the gcloud CLI, and the REST API to view who has access to a service account. You can also view access by using the [IAM client libraries](https://cloud.google.com/iam/docs/client-libraries?authuser=5#iam) (https://cloud.google.com/iam/docs/client-libraries?authuser=5#iam) to get the service account's allow policy.

[Console](#) (#console) [gcloud](#) [REST](#) (#rest)
(#gcloud)

To see who has access to your service account, get the allow policy for the service account. To learn how to interpret allow policies, see [Understanding allow policies](https://cloud.google.com/iam/docs/policies?authuser=5) (https://cloud.google.com/iam/docs/policies?authuser=5).

★ **Note:** A resource's allow policy does not show any roles gained through [policy inheritance](https://cloud.google.com/iam/docs/policies?authuser=5#inheritance) (https://cloud.google.com/iam/docs/policies?authuser=5#inheritance). To view inherited roles, use the Google Cloud console, or follow the instructions on [Viewing effective IAM policies](https://cloud.google.com/asset-inventory/docs/view-effective-iam-policies?authuser=5) (https://cloud.google.com/asset-inventory/docs/view-effective-iam-policies?authuser=5).

To get the allow policy for the service account, run the `get-iam-policy` (https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/get-iam-policy?authuser=5) command for the service account:

```
gcloud iam service-accounts get-iam-policy SA_ID --format=FORMAT >
```

Provide the following values:

- ***SA_ID***: The ID of your service account. This can either be the service account's email address in the form `SA_NAME@PROJECT_ID.iam.gserviceaccount.com`, or the service account's unique numeric ID.

★ **Note:** If you want to identify a service account just after it is created, use the numeric ID rather than the email address to ensure that it is reliably identified.

- ***FORMAT***: The desired format for the policy. Use `json` or `yaml`.
- ***PATH***: The path to a new output file for the policy.

For example, the following command gets the policy for the service account `my-service-account` and saves it to your home directory in JSON format:

```
gcloud iam service-accounts get-iam-policy my-service-account --format j
```

Grant or revoke a single role

You can use the Google Cloud console and the gcloud CLI to quickly grant or revoke a single role for a single principal, without editing the service account's allow policy directly.

Common types of principals include Google accounts, service accounts, Google groups, and domains. For a list of all principal types, see [Concepts related to identity](https://cloud.google.com/iam/docs/overview?authuser=5#concepts_related_identity) (https://cloud.google.com/iam/docs/overview?authuser=5#concepts_related_identity).

Note: In general, policy changes take effect within 2 minutes. However, in some cases, it can take 7 minutes or more for changes to propagate across the system.

If you need help identifying the most appropriate predefined role, see [Choose predefined roles](https://cloud.google.com/iam/docs/choose-predefined-roles?authuser=5) (<https://cloud.google.com/iam/docs/choose-predefined-roles?authuser=5>).

Grant a single role

To grant a single role to a principal, do the following:

[Console](#) (#console) [gcloud](#) (#gcloud)

To quickly grant a role to a principal, run the [add-iam-policy-binding](https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/add-iam-policy-binding?authuser=5) (<https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/add-iam-policy-binding?authuser=5>) command:

```
gcloud iam service-accounts add-iam-policy-binding SA_ID \
  --member=PRINCIPAL --role=ROLE_NAME \
  --condition=CONDITION
```

Provide the following values:

- **SA_ID:** The ID of your service account. This can either be the service account's email address in the form **SA_NAME@PROJECT_ID.iam.gserviceaccount.com**,

or the service account's unique numeric ID.

★ **Note:** If you want to identify a service account just after it is created, use the numeric ID rather than the email address to ensure that it is reliably identified.

- **PRINCIPAL:** An identifier for the principal, or member, which usually has the following form: **PRINCIPAL-TYPE: ID**. For example, **user:my-user@example.com**. For a full list of the values that **PRINCIPAL** can have, see the [Policy Binding reference](https://cloud.google.com/iam/docs/reference/rest/v1/Policy?authuser=5#Binding) (<https://cloud.google.com/iam/docs/reference/rest/v1/Policy?authuser=5#Binding>).

For the principal type **user**, the domain name in the identifier must be a Google Workspace domain or a Cloud Identity domain. To learn how to set up a Cloud Identity domain, see the [overview of Cloud Identity](https://cloud.google.com/identity/docs/overview?authuser=5).

(<https://cloud.google.com/identity/docs/overview?authuser=5>).

- **ROLE_NAME:** The name of the role that you want to grant. Use one of the following formats:
 - Predefined roles: **roles/SERVICE.IDENTIFIER**
 - Project-level custom roles: **projects/PROJECT_ID/roles/IDENTIFIER**
 - Organization-level custom roles: **organizations/ORG_ID/roles/IDENTIFIER**

For a list of predefined roles, see [Understanding roles](https://cloud.google.com/iam/docs/understanding-roles?authuser=5)

(<https://cloud.google.com/iam/docs/understanding-roles?authuser=5>).

- **CONDITION:** Optional. The condition to add to the role binding. For more information about conditions, see the [conditions overview](https://cloud.google.com/iam/docs/conditions-overview?authuser=5) (<https://cloud.google.com/iam/docs/conditions-overview?authuser=5>).

For example, to grant the Service Account User role to the user **my-user@example.com** for the service account **my-service-account@my-project.iam.gserviceaccount.com**:

```
gcloud iam service-accounts add-iam-policy-binding my-service-account@my-
--member=user:my-user@example.com --role=roles/iam.serviceAccountUser
```

Revoke a single role

To revoke a single role from a principal, do the following:

Console (#console) **gcloud** (#gcloud)

To quickly revoke a role from a user, run the `remove-iam-policy-binding` (<https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/remove-iam-policy-binding?authuser=5>) command:

```
gcloud iam service-accounts remove-iam-policy-binding SA_ID \
  --member=PRINCIPAL --role=ROLE_NAME
```

Provide the following values:

- ***SA_ID***: The ID of your service account. This can either be the service account's email address in the form `SA_NAME@PROJECT_ID.iam.gserviceaccount.com`, or the service account's unique numeric ID.

★ **Note:** If you want to identify a service account just after it is created, use the numeric ID rather than the email address to ensure that it is reliably identified.

- ***PRINCIPAL***: An identifier for the principal, or member, which usually has the following form: `PRINCIPAL - TYPE: ID`. For example, `user:my-user@example.com`. For a full list of the values that ***PRINCIPAL*** can have, see the [Policy Binding reference](https://cloud.google.com/iam/docs/reference/rest/v1/Policy?authuser=5#Binding) (<https://cloud.google.com/iam/docs/reference/rest/v1/Policy?authuser=5#Binding>).

For the principal type `user`, the domain name in the identifier must be a Google Workspace domain or a Cloud Identity domain. To learn how to set up a Cloud Identity domain, see the [overview of Cloud Identity](https://cloud.google.com/identity/docs/overview?authuser=5) (<https://cloud.google.com/identity/docs/overview?authuser=5>).

- ***ROLE_NAME***: The name of the role that you want to revoke. Use one of the following formats:
 - Predefined roles: `roles/SERVICE.IDENTIFIER`
 - Project-level custom roles: `projects/PROJECT_ID/roles/IDENTIFIER`
 - Organization-level custom roles: `organizations/ORG_ID/roles/IDENTIFIER`

For a list of predefined roles, see [Understanding roles](#)

(<https://cloud.google.com/iam/docs/understanding-roles?authuser=5>).

For example, to revoke the Service Account User role from the user `my-user@example.com` for the service account `my-service-account@my-project.iam.gserviceaccount.com`:

```
gcloud iam service-accounts remove-iam-policy-binding my-service-account
--member=user:my-user@example.com --role=roles/iam.serviceAccountUser
```


Grant or revoke multiple roles using the Google Cloud console

You can use the Google Cloud console to grant and revoke multiple roles for a single principal:

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

[Go to Service Accounts](https://console.cloud.google.com/iam-admin/serviceaccounts?authuser=5) (<https://console.cloud.google.com/iam-admin/serviceaccounts?authuser=5>)

2. Select a project.
3. Click the email address of the service account.
4. Go to the **Permissions** tab and find the section **Principals with access to this service account**.
5. Select the principal whose roles you want to modify:


- To modify roles for a principal who already has roles on the service account, find a row containing the principal, then click  **Edit principal** in that row, then click **+ Add another role**.

If you want to modify roles for a [Google-managed service account](#)


(<https://cloud.google.com/iam/docs/service-account-types?authuser=5#google-managed>), you must select the **Include Google-provided role grants** checkbox to see its email address.



Note: You cannot edit inherited roles when managing access to service accounts. To edit inherited roles, go to the resource where the role was granted.

- To grant roles to a principal who doesn't have any existing roles on the service account, click **+  Grant access**, then enter the principal's email address or other identifier.

6. Modify the principal's roles:

- To grant a role to a principal who doesn't have any existing roles on the resource, click **Select a role**, then select a role to grant from the drop-down list.
- To grant an additional role to the principal, click **Add another role**, then select a role to grant from the drop-down list.
- To replace one of the principal's roles with a different role, click the existing role, then choose a different role to grant from the drop-down list.
- To revoke one of the principal's roles, click the **Delete ** button for each role that you want to revoke.

You can also [add a condition](#)

(<https://cloud.google.com/iam/docs/managing-conditional-role-bindings?authuser=5#add>) to a role, [modify a role's condition](#)

(<https://cloud.google.com/iam/docs/managing-conditional-role-bindings?authuser=5#modify>), or [remove a role's condition](#)

(<https://cloud.google.com/iam/docs/managing-conditional-role-bindings?authuser=5#removing>).

7. Click **Save**.

Grant or revoke multiple roles programmatically

To make large-scale access changes that involve granting and revoking multiple roles for multiple principals, use the *read-modify-write* pattern to update the service account's allow policy:

1. Read the current allow policy by calling `getIamPolicy()`.
2. Edit the allow policy, either by using a text editor or programmatically, to add or remove any principals or role bindings.
3. Write the updated allow policy by calling `setIamPolicy()`.

This section shows how to use the gcloud CLI and the REST API to update the allow policy.

You can also update the allow policy using the [IAM client libraries](#)

(<https://cloud.google.com/iam/docs/client-libraries?authuser=5#iam>).

Note: In general, policy changes take effect within 2 minutes. However, in some cases, it can take 7 minutes or more for changes to propagate across the system.

Get the current allow policy

gcloudREST (#rest)
(#gcloud)

To get the allow policy for the service account, run the **get-iam-policy** (https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/get-iam-policy?authuser=5) command for the service account:

```
gcloud iam service-accounts get-iam-policy SA_ID --format=FORMAT >
```

Provide the following values:

- **SA_ID:** The ID of your service account. This can either be the service account's email address in the form **SA_NAME@PROJECT_ID.iam.gserviceaccount.com**, or the service account's unique numeric ID.

★ **Note:** If you want to identify a service account just after it is created, use the numeric ID rather than the email address to ensure that it is reliably identified.

- **FORMAT:** The desired format for the allow policy. Use **json** or **yaml**.
- **PATH:** The path to a new output file for the allow policy.

For example, the following command gets the allow policy for the service account **my-service-account** and saves it to your home directory in JSON format:

```
gcloud iam service-accounts get-iam-policy my-service-account --format j
```

Modify the allow policy

Programmatically or using a text editor, modify the local copy of your service account's allow policy to reflect the roles you want to grant or revoke to given users.

To ensure that you do not overwrite other changes, do not edit or remove the allow policy's etag field. The etag field identifies the current state of the allow policy. When you set the updated allow policy (#setting-policy), IAM compares the etag value in the request with the existing etag, and only writes the allow policy if the values match.

Important: None of your changes to the allow policy will take effect until you set the updated allow policy (#setting-policy).

To edit the roles that an allow policy grants, you need to edit the role bindings in the allow policy. Role bindings have the following format:

```
{
  "role": " ROLE_NAME ",
  "members": [
    " PRINCIPAL_1 ",
    " PRINCIPAL_2 ",
    ...
    " PRINCIPAL_N "
  ],
  "conditions": {
    CONDITIONS
  }
}
```

The placeholders have the following values:

- *ROLE_NAME*: The name of the role that you want to grant. Use one of the following formats:
 - Predefined roles: `roles/SERVICE.IDENTIFIER`
 - Project-level custom roles: `projects/PROJECT_ID/roles/IDENTIFIER`
 - Organization-level custom roles: `organizations/ORG_ID/roles/IDENTIFIER`

For a list of predefined roles, see [Understanding roles](#)

(<https://cloud.google.com/iam/docs/understanding-roles?authuser=5>).

- *PRINCIPAL_1*, *PRINCIPAL_2*, ... *PRINCIPAL_N*: Identifiers for the principals that you want to grant the role to.

Principal identifiers usually have the following form: *PRINCIPAL - TYPE: ID*. For example, `user:my-user@example.com`. For a full list of the values that *PRINCIPAL* can have, see the [Policy Binding reference](#)

(<https://cloud.google.com/iam/docs/reference/rest/v1/Policy?authuser=5#Binding>).

For the principal type `user`, the domain name in the identifier must be a Google Workspace domain or a Cloud Identity domain. To learn how to set up a Cloud Identity domain, see the [overview of Cloud Identity](#).

(<https://cloud.google.com/identity/docs/overview?authuser=5>).

- **CONDITIONS:** Optional. Any [conditions](#) (<https://cloud.google.com/iam/docs/conditions-overview?authuser=5>) that specify when access will be granted.

Grant a role

To grant roles to your principals, modify the role bindings in the allow policy. To learn what roles you can grant, see [Understanding roles](#)

(<https://cloud.google.com/iam/docs/understanding-roles?authuser=5>), or [view grantable roles](#)

(<https://cloud.google.com/iam/docs/viewing-grantable-roles?authuser=5>) for the service account. If you need help identifying the most appropriate predefined roles, see [Choose predefined roles](#) (<https://cloud.google.com/iam/docs/choose-predefined-roles?authuser=5>).

Optionally, you can use [conditions](#)

(<https://cloud.google.com/iam/docs/conditions-overview?authuser=5>) to grant roles only when certain requirements are met.

To grant a role that is already included in the allow policy, add the principal to an existing role binding:

`gcloudREST (#rest)`
(`#gcloud`)

Edit the allow policy by adding the principal to an existing role binding. Note that this change will not take effect until you [set the updated allow policy](#) (`#setting-policy`).

For example, imagine the allow policy contains the following role binding, which grants the Service Account User role (`roles/iam.serviceAccountUser`) to `kai@example.com`:

```
{
  "role": "roles/iam.serviceAccountUser",
  "members": [
```

```
"user:kai@example.com"
  ]
}
```

To grant that same role to `raha@example.com`, add `raha@example.com` to the existing role binding:

```
{
  "role": "roles/iam.serviceAccountUser",
  "members": [
    "user:kai@example.com",
    "user:raha@example.com"
  ]
}
```

To grant a role that is not yet included in the allow policy, add a new role binding:

`gcloudREST` (#rest)
(#gcloud)

Edit the allow policy by adding a new role binding that grants the role to the principal. This change will not take effect until you set the updated allow policy (#setting-policy).

For example, to grant the Service Account Token Creator role (`roles/iam.serviceAccountTokenCreator`) to `raha@example.com`, add the following role binding to the `bindings` array for the allow policy:

```
{
  "role": "roles/iam.serviceAccountTokenCreator",
  "members": [
    "user:raha@example.com"
  ]
}
```

Revoke a role

To revoke a role, remove the principal from the role binding. If there are no other principals in the role binding, remove the entire role binding from the allow policy.

Note: Role bindings with no principals are not allowed and will result in an error when setting the allow policy.

`gcloudREST (#rest)`
(#gcloud)

Edit the allow policy by removing the principal or the entire role binding. This change will not take effect until you set the updated allow policy (#setting-policy).

For example, imagine the allow policy contains the following role binding, which grants `kai@example.com` and `raha@example.com` the Service Account User role (`roles/iam.serviceAccountUser`):

```
{
  "role": "roles/iam.serviceAccountUser",
  "members": [
    "user:kai@example.com",
    "user:raha@example.com"
  ]
}
```

To revoke the role from `kai@example.com`, remove `kai@example.com` from the role binding:

```
{
  "role": "roles/iam.serviceAccountUser",
  "members": [
    "user:raha@example.com"
  ]
}
```

To revoke the role from both `kai@example.com` and `raha@example.com`, remove the role binding from the allow policy.

Set the allow policy

After you modify the allow policy to grant and revoke the desired roles, call `setIamPolicy()` to make the updates.

Warning: Setting a new allow policy permanently overwrites the existing allow policy on the service account. To avoid removing role bindings unintentionally, always follow the read-modify-write pattern when updating an allow policy: read the existing policy, modify it as needed, and then write the updated version of the allow policy.

gcloudREST (#rest)
(#gcloud)

To set the allow policy for the resource, run the `set-iam-policy` (https://cloud.google.com/sdk/gcloud/reference/iam/service-accounts/get-iam-policy?authuser=5) command for the service account:

```
gcloud iam service-accounts set-iam-policy SA_ID PATH
```

Provide the following values:

- **SA_ID:** The ID of your service account. This can either be the service account's email address in the form `SA_NAME@PROJECT_ID.iam.gserviceaccount.com`, or the service account's unique numeric ID.

★ **Note:** If you want to identify a service account just after it is created, use the numeric ID rather than the email address to ensure that it is reliably identified.

- **PATH:** The path to a file that contains the new allow policy.

The response contains the updated allow policy.

For example, the following command sets the allow policy stored in `policy.json` as the allow policy for the service account `my-service-account@my-project.iam.gserviceaccount.com`:

```
gcloud iam service-accounts set-iam-policy my-service-account@my-project  
~/policy.json
```

★ **Note:** If you treat policies as code and store them in a version-control system, you should store

the policy that is returned, not the policy that you sent in the request.

What's next

- Learn which roles to grant to allow principals to [authenticate as service accounts](https://cloud.google.com/iam/docs/service-account-permissions?authuser=5) (<https://cloud.google.com/iam/docs/service-account-permissions?authuser=5>).
- Find out how to [choose the most appropriate predefined roles](https://cloud.google.com/iam/docs/choose-predefined-roles?authuser=5) (<https://cloud.google.com/iam/docs/choose-predefined-roles?authuser=5>).
- Review [Best practices for working with service accounts](https://cloud.google.com/iam/docs/best-practices-service-accounts?authuser=5) (<https://cloud.google.com/iam/docs/best-practices-service-accounts?authuser=5>) to learn how to use service accounts securely.
- Learn how to [manage access to projects, folders, and organizations](https://cloud.google.com/iam/docs/granting-changing-revoking-access?authuser=5) (<https://cloud.google.com/iam/docs/granting-changing-revoking-access?authuser=5>).
- Learn the general steps for [managing access to other resources](https://cloud.google.com/iam/docs/manage-access-other-resources?authuser=5) (<https://cloud.google.com/iam/docs/manage-access-other-resources?authuser=5>).
- Learn how to make a principal's access conditional with [conditional role bindings](https://cloud.google.com/iam/docs/conditions-overview?authuser=5) (<https://cloud.google.com/iam/docs/conditions-overview?authuser=5>).

Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (<https://www.apache.org/licenses/LICENSE-2.0>). For details, see the [Google Developers Site Policies](https://developers.google.com/site-policies?authuser=5) (<https://developers.google.com/site-policies?authuser=5>). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2023-11-27 UTC.