Google Service Account

# Google: Service Account#

Using service accounts is more complex than OAuth2. Before you begin:

• Check if your node is compatible with Service Account.

• Make sure you need to use Service Account. For most use cases, OAuth2 is a better option.

• Read the Google documentation on Creating and managing service accounts.

## Prerequisites#

• Create a Google Cloud account.

## Set up Service Account#

There are four steps to connecting your n8n credential to a Google Service Account:

• Create a Google Cloud Console project.

• Enable APIs.

• Set up Google Cloud Service Account.

• Finish your n8n credential.

### Create a Google Cloud Console project#

First, create a Google Cloud Console project. If you already have a project, jump to the next section:

• Log in to your Google Cloud Console using your Google credentials.

• In the top menu, select the project dropdown in the top navigation and select New project or go directly to the New Project page.

• Enter a Project name and select the Location for your project.

• Select Create.

• Check the top navigation and make sure the project dropdown has your project selected. If not, select the project you just created.  
  
Check the project dropdown in the Google Cloud top navigation

Check the top navigation and make sure the project dropdown has your project selected. If not, select the project you just created.

### Enable APIs#

With your project created, enable the APIs you'll need access to:

• Access your Google Cloud Console - Library. Make sure you're in the correct project.  
Check the project dropdown in the Google Cloud top navigation

• Go to APIs & Services > Library.

• Search for and select the API(s) you want to enable. For example, for the Gmail node, search for and enable the Gmail API.

• Some integrations require other APIs or require you to request access:  
  
Google Perspective: Request API Access.  
Google Ads: Get a Developer Token.  
  
Google Drive API required  
  
The following integrations require the Google Drive API, as well as their own API:  
  
Google Docs  
Google Sheets  
Google Slides  
  
Google Vertex AI API  
  
In addition to the Vertex AI API you will also need to enable the Cloud Resource Manager API.

Some integrations require other APIs or require you to request access:

• Google Perspective: Request API Access.

• Google Ads: Get a Developer Token.

Google Drive API required

The following integrations require the Google Drive API, as well as their own API:

• Google Docs

• Google Sheets

• Google Slides

Google Vertex AI API

In addition to the Vertex AI API you will also need to enable the Cloud Resource Manager API.

• Select ENABLE.

Select ENABLE.

### Set up Google Cloud Service Account#

• Access your Google Cloud Console - Library. Make sure you're in the correct project.  
  
Check the project dropdown in the Google Cloud top navigation

Access your Google Cloud Console - Library. Make sure you're in the correct project.

• Select the hamburger menu > APIs & Services > Credentials. Google takes you to your Credentials page.

Select the hamburger menu > APIs & Services > Credentials. Google takes you to your Credentials page.

• Select + CREATE CREDENTIALS > Service account.

• Enter a name in Service account name and an ID in Service account ID. Refer to Creating a service account for more information.

• Select CREATE AND CONTINUE.

• Based on your use-case, you may want to Select a role and Grant users access to this service account using the corresponding sections.

• Select DONE.

• Select your newly created service account under the Service Accounts section. Open the KEYS tab.

• Select ADD KEY > Create new key.

• In the modal that appears, select JSON, then select CREATE. Google saves the file to your computer.

### Finish your n8n credential#

With the Google project and credentials fully configured, finish the n8n credential:

• Open the downloaded JSON file.

• Copy the client\_email and enter it in your n8n credential as the Service Account Email.

client\_email

• Copy the private\_key. Don't include the surrounding " marks. Enter this as the Private Key in your n8n credential.  
  
Older versions of n8n  
  
If you're running an n8n version older than 0.156.0, replace all instances of \n in the JSON file with new lines.

Copy the private\_key. Don't include the surrounding " marks. Enter this as the Private Key in your n8n credential.

private\_key

"

Older versions of n8n

If you're running an n8n version older than 0.156.0, replace all instances of \n in the JSON file with new lines.

\n

• Optional: Choose if you want to Impersonate a User (turned on).  
  
To use this option, you must Enable domain-wide delegation for the service account as a Google Workspace super admin.  
Enter the Email of the user you want to impersonate.

Optional: Choose if you want to Impersonate a User (turned on).

• To use this option, you must Enable domain-wide delegation for the service account as a Google Workspace super admin.

• Enter the Email of the user you want to impersonate.

• If you plan to use this credential with the HTTP Request node, turn on Set up for use in HTTP Request node.  
With this setting turned on, you'll need to add Scope(s) for the node. n8n prepopulates some scopes. Refer to OAuth 2.0 Scopes for Google APIs for more information.

• With this setting turned on, you'll need to add Scope(s) for the node. n8n prepopulates some scopes. Refer to OAuth 2.0 Scopes for Google APIs for more information.

• Save your credentials.

## Video#

The following video demonstrates the steps described above.

## Troubleshooting#

### Service Account can't access Google Drive files#

A Service Account can't access Google Drive files and folders that weren't shared with its associated user email.

• Access your Google Cloud Console and copy your Service Account email.

• Access your Google Drive and go to the designated file or folder.

• Right-click on the file or folder and select Share.

• Paste your Service Account email into Add People and groups.

• Select Editor for read-write access or Viewer for read-only access.

### Enable domain-wide delegation#

To impersonate a user with a service account, you must enable domain-wide delegation for the service account.

Not recommended

Google recommends you avoid using domain-wide delegation, as it allows impersonation of any user (including super admins) and can pose a security risk.

To delegate domain-wide authority to a service account, you must be a super administrator for the Google Workspace domain. Then:

• From your Google Workspace domain's Admin console, select the hamburger menu, then select Security > Access and data control > API Controls.

• In the Domain wide delegation pane, select Manage Domain Wide Delegation.

• Select Add new.

• In the Client ID field, enter the service account's Client ID. To get the Client ID:  
Open your Google Cloud Console project, then open the Service Accounts page.  
Copy the OAuth 2 Client ID and use this as the Client ID for the Domain Wide Delegation.

• Open your Google Cloud Console project, then open the Service Accounts page.

• Copy the OAuth 2 Client ID and use this as the Client ID for the Domain Wide Delegation.

• In the OAuth scopes field, enter a list of comma-separate scopes to grant your application access. For example, if your application needs domain-wide full access to the Google Drive API and the Google Calendar API, enter: https://www.googleapis.com/auth/drive, https://www.googleapis.com/auth/calendar.

https://www.googleapis.com/auth/drive, https://www.googleapis.com/auth/calendar

• Select Authorize.

It can take from 5 minutes up to 24 hours before you can impersonate all users in your Workspace.