



Creating a service account in Google Workspace

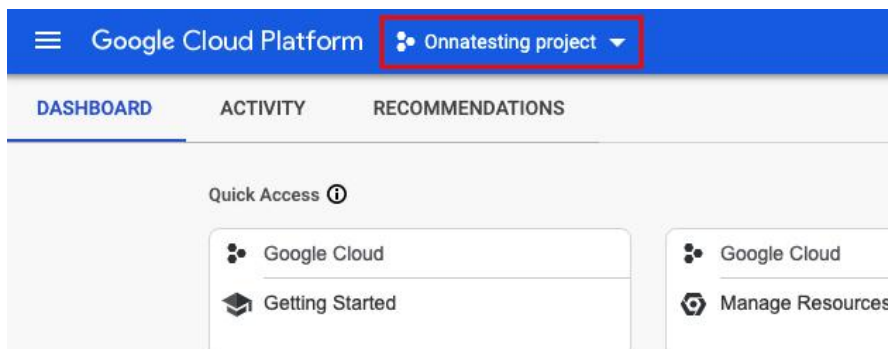
Google Workspace encompasses Google's set of collaboration and productivity tools such as: Gmail, Google Drive, Audits, Vault and more. Currently, Onna connects directly to Google Workspace's API to integrate with an organization's Gmail, Drive, Shared Drives and Vault files.

Onna recommends creating a separate Google Workspace account with needed permissions in order to perform collections. The account will need the **User Management Admin**, **Services Admin**, **Groups Reader** and **Reports** (see page 8) Admin roles assigned.

A Google Workspace Super Admin is needed for creating the project and service account steps below. Alternatively, a Super Admin account can also be used to perform collections.

1) Create a Project

You will need access to your Google Cloud Console. Navigate to the [Google Cloud Console](#). Next to the "Google Cloud Platform" name at the top, click the Down arrow for a dialog box to appear.



In the dialog box Click New Project in the upper right corner.

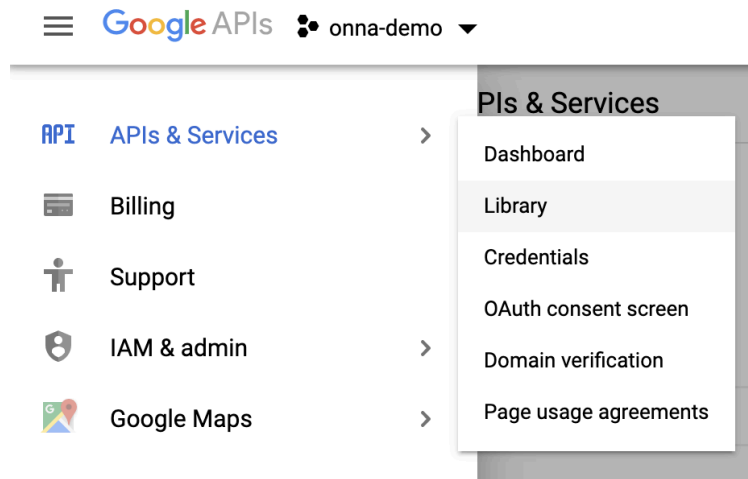




Enter the Project name and select the Organization and Location and then "Create". Once created, you will need to use the drop-down navigation again to ensure you are within the newly created project or select from the notifications' menu.

2) Enable API's for the project:

Once inside the project, select the Menu (3 lines) → APIs & Services → Library. Search for and enable the needed APIs.



API's to enable:

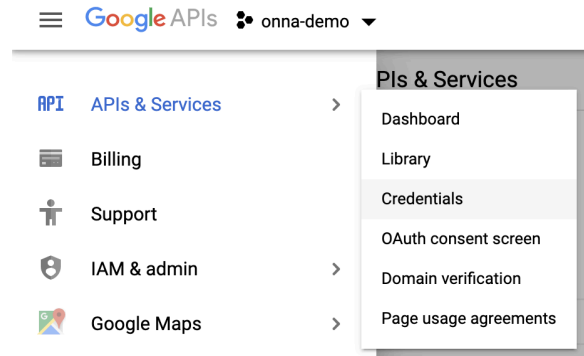
- Gmail API
- Google Drive API
- Admin SDK
- Google Vault API*

It is important to enable the correct APIs for the sync to work properly.

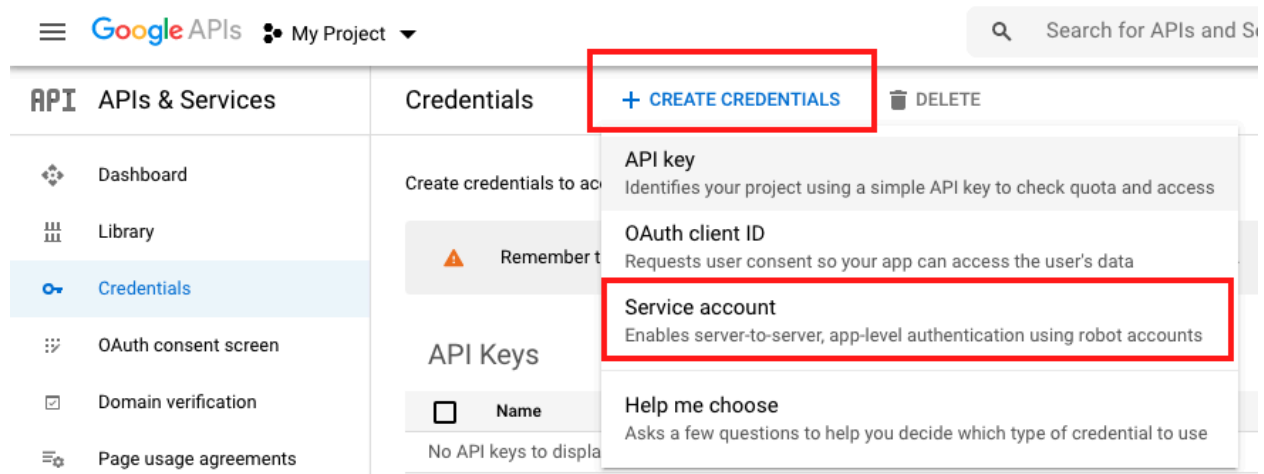
* Vault API not necessary for Gmail and Drive collections. Only needed if planning to collect from Vault OR use [Onna's Integrated Legal Holds source hold](#) feature with Google Vault.

3) Create the Service Account

Go to the Menu → APIs & Services → Credentials:



Select "Create credentials" and choose "Service account"



Enter the Service account name, Service account ID and click Create and Continue. *You can also choose to enter an optional description.*

1 Service account details

Service account name

Onna Demo Service

Display name for this service account

Service account ID

onna-demo-service @onnapsoproject.iam.gserviceaccount.com X ↺

Service account description

Describe what this service account will do

CREATE AND CONTINUE

Step 2 → in the Role section scroll and select "Project" → "Viewer"

Create service account

✓ Service account details

2 Grant this service account access to project (optional)

Grant this service account access to My Project1021 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role

Condition

Type to filter

Project

Access Approval

Access Context Ma...

Actions

AI Notebooks

Android Manageme...

API Gateway

App...

Browser

Editor

Owner

Viewer

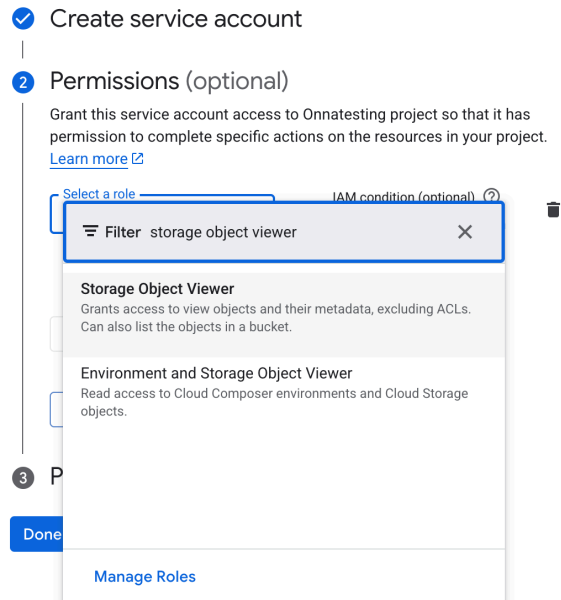
Viewer

Read access to all resources.

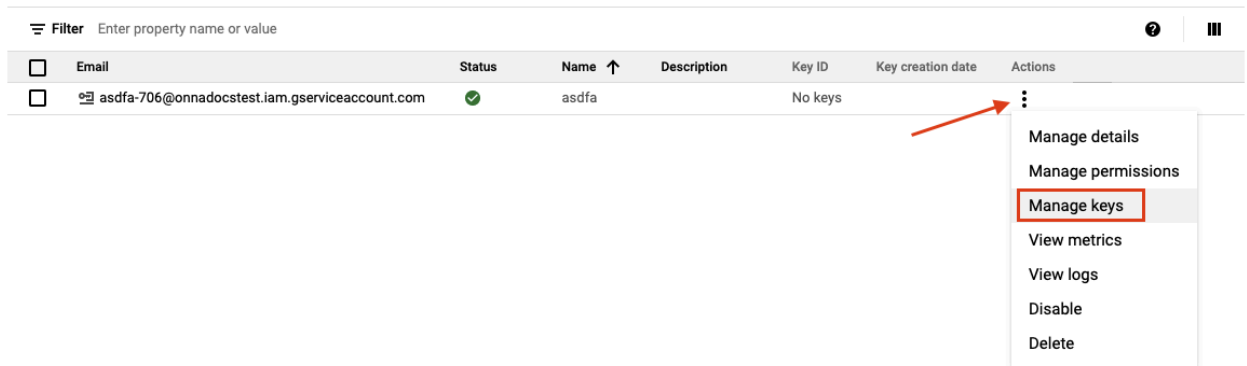
MANAGE ROLES



Step 3 → in the Role section search for “Storage Object Viewer” and select → click Continue → then Done



Once the service account is created click “[Manage service accounts](#)” → then click on the ellipsis → from the menu select 'Manage Keys'



Next click Add Key → Select Create new key → JSON → Create. The JSON key will be automatically downloaded to your computer. Be sure to store it securely and take note of location, we will need this file at a later step.



Create private key for "test"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

☒ JSON
Recommended

☐ P12
For backward compatibility with code using the P12 format

CANCEL CREATE

Once the JSON key is stored securely click Close.

4) Copy Client ID

After clicking Close click on the Details tab. Copy the "Unique ID" which will be used for the next step.

Service account details

Name
asdfa SAVE

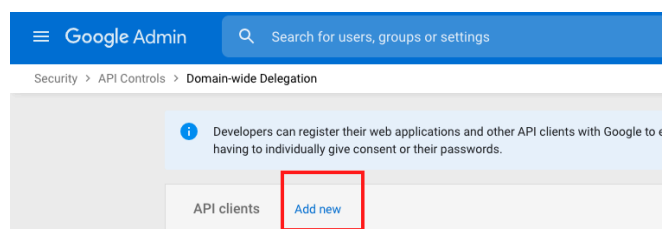
Description SAVE

Email
[REDACTED]

Unique ID
[REDACTED] ←

5) Delegate domain-wide authority to your service account from Google Admin console

Navigate to the Google Admin console (<http://admin.google.com/>). From the left menu select → Security → Access and data control API Controls → then Manage Domain Wide Delegation at the bottom of the page→ then select Add New





Paste the Client ID (Unique ID) into the Client ID section. Then paste the URLs below into the OAuth Scopes (comma separated) field:

https://www.googleapis.com/auth/admin.directory.group,
https://www.googleapis.com/auth/admin.directory.user,
https://www.googleapis.com/auth/admin.reports.audit.readonly,
https://www.googleapis.com/auth/admin.reports.usage.readonly,
https://www.googleapis.com/auth/drive.readonly,
https://www.googleapis.com/auth/gmail.readonly,
https://www.googleapis.com/auth/userinfo.email,
https://www.googleapis.com/auth/userinfo.profile,
https://www.googleapis.com/auth/ediscovery,
https://www.googleapis.com/auth/devstorage.read_only

A screenshot of the 'Add a new client ID' dialog box in the Google Cloud Console. The dialog has a blue header with the title 'Add a new client ID'. Below the header, there is a text input field labeled 'Client ID'. Underneath this field is a checkbox labeled 'Overwrite existing client ID' with a help icon. Below the checkbox is another text input field labeled 'OAuth scopes (comma-delimited)'. At the bottom right of the dialog are two buttons: 'CANCEL' and 'AUTHORIZE'. The background of the screenshot shows a list of OAuth scopes, including 'https://www.googleapis.com/auth/admin.directory.group' and 'https://www.googleapis.com/auth/admin.directory.user', with a '+7 More' link at the bottom.

Once the values have been entered click on **Authorize**.

Note: the new configuration you just created may take time for the changes to propagate. If the initial Google Workspace connection fails in Onna, give it a few minutes and try again.



Granting Permissions to non Super Admin Account (Must be performed by Google Workspace Super Admin)

Note: The below steps can be skipped if you are performing a collection as a Google Workspace Super Admin since all privileges are already available.

1. Navigate Google Admin console at <https://admin.google.com>
2. Under Directory -> Users, select 'Add new user' to add a new user. Ex. onna-service@domain.com
3. Once created, navigate to the Google Admin console Roles section: <https://admin.google.com/u/1/ac/roles>
4. Select 'Create a new role'
5. Name the Role (*Example: Onna Connector, or a similar title*)
6. Under 'Admin console privileges' search for 'Google Vault' and provide the following privileges
 - a. Manage Matters
 - b. Manage Holds
 - c. Manage Exports
 - d. Manage Searches

Admin console privileges ?

Google Vault

Privilege Name

▼ Services

▼ Google Vault

▼ ☐ Access All Logs

☐ Manage Audits

☐ View All Matters

☒ Manage Matters

☐ Approve Deletion

☒ Manage Exports

▼ ☐ Manage Retention Policies

☐ View Retention Policies

☒ Manage Searches

☒ Manage Holds

7. Under the 'Admin API privileges' , search and select 'Reports' → then save the changes

Admin API privileges ?

Reports

Privilege Name


☒ Reports

8. Once the new role has been created → select "Assign users" and assign the user account or service account that will be used for the authorized connection
9. Next assign the account the following System Roles built into Google Workspace
 - "User Management Admin"
 - "Services Admin"
 - "Groups Reader"

Admin roles

Roles

[Create new role](#)

Role	Role description	Type 
Super Admin	Google Apps Administrator Seed Role	System role
Groups Admin	Groups Administrator	System role
User Management Admin	User Management Administrator	System role
Help Desk Admin	Help Desk Administrator	System role
Services Admin	Services Administrator	System role