

EMAIL SETTINGS FOR COMMON EMAIL PROVIDERS

If you are setting up email or Email Theater with Security Validation, you may be connecting to one of many email providers. This article provides information around common settings and how to work with those email providers related to the Security Validation platform.

- If two-factor authentication is enabled for your email, you need to obtain an application-specific password that allows the Director and your email provider to communicate. This section provides some guidance in setting up accounts on these popular email providers to work with the Director.
- It is important to understand that the account password used for the Director to send and receive email from your email provider is not necessarily the same as the credentials you use to log in to the account to access email.



This topic is not intended to replace any documentation or guidance from your email provider. Rather, it is intended to guide you toward the more common configurations.

Email Settings for Office 365 with Graph API

Before you set up the Email Theater for Microsoft Office 365, you must first prepare the environment for use by the Email Theater.

Allow list requirements for Office 365 with Graph API

The following domains must be added to the allow list from the Actor. This ensures the Actor can communicate with the cloud email service through the API.

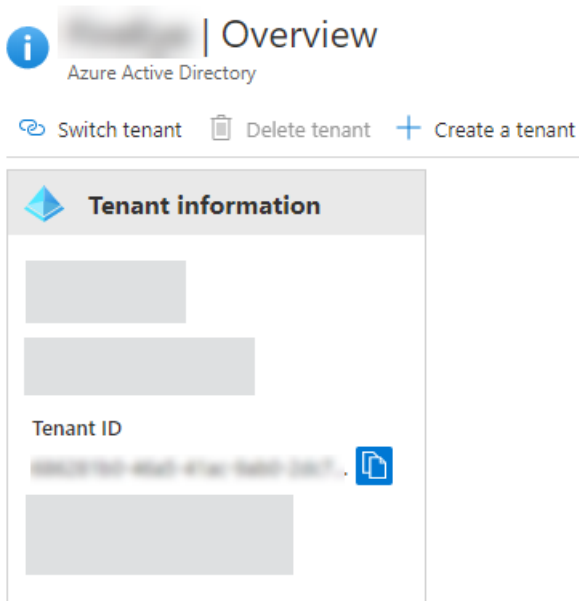
- `https://login.microsoftonline.com/*`
- `https://graph.microsoft.com/*`

For Office 365 in government tenants, use the following domains:

- `login.microsoftonline.us/*`
- `graph.microsoft.us/*`
- `dod-graph.microsoft.us/*`

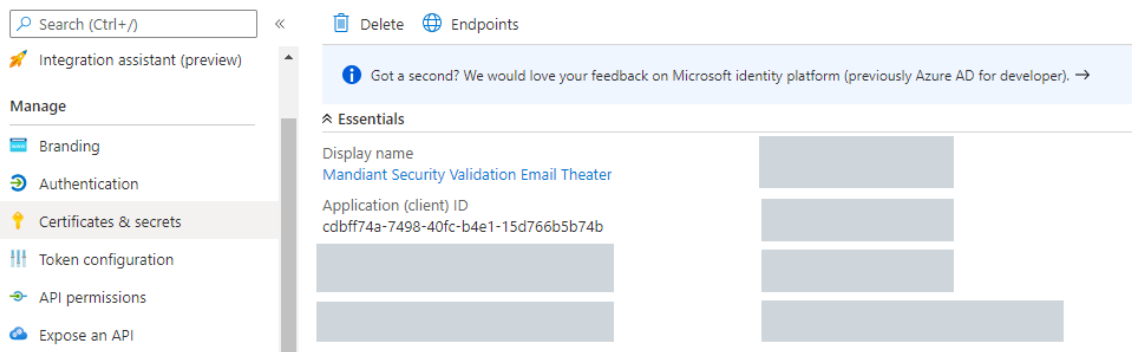
Configure email settings for Office 365 with Graph API

1. Log in to Azure (<https://portal.azure.com/#home>).
2. Open the Azure Active Directory. Make a note of the Tenant ID in Tenant Information.



3. In the search bar at the top of the portal window, search for "app registration" and open the App Registrations page.
4. Create a new registration by entering or selecting the following information:
 - **Name:** Enter a name for the application.
 - **Single Tenant:** Select this option.
 - **Redirect URL:** Set the redirect URL (for example, <http://localhost/auth>).
 - **Register:** Select this option and make a note of the Application (client) ID.

 **Mandiant Security Validation Email Theater** 



5. From the left pane of the application registration page, select **Certificates & Secrets**.
6. Create a new client secret.



Be sure to make a note of the client secret, as you need it later and it does not display in its entirety again.

7. Select **API permissions** and then **Add a permission**.
8. Select **Microsoft APIs** and then choose **Microsoft Graph**.
9. Select **Application permissions**.
10. In the Select permissions search bar, enter "mail" and check the following check boxes:
 - **Mail.ReadWrite** (Write is needed for large attachment support.)
 - **Mail.Send**



An administrator must grant consent for the selected permissions to become effective. Once consent has been granted and you have recorded the values of the Tenant/Application/Secret IDs, the application is technically ready for use.

Be aware that anyone who knows the Client Secret and knowledge of the Tenant and Application (client) IDs can read email for any account in the tenant, as well as send email as any account in the tenant. Therefore, you should create dedicated accounts/mailboxes for use with Email Theater.

11. Create a distribution group containing the email accounts created earlier by running a PowerShell cmdlet command, for example:

```
New-DistributionGroup -Name <"name of distribution group"> -Type "Security" -Members <"add email accounts added earlier">
```

After you have created one or more accounts in the tenant, which are licensed for email, you should restrict the application to those email accounts.

You can create an application access policy to limit application access to a specific group of mailboxes using the New-ApplicationAccessPolicy PowerShell cmdlet. Executing this policy restricts the Email Theater application to only those accounts that are members of specific distribution groups.



This process is specific only to Exchange Online resources and does not apply to other Microsoft Graph workloads.

To Restrict an Application to a Specific Group

1. Connect to Exchange Online PowerShell.

```
Connect-ExchangeOnline
```

2. In the [Azure app registration portal](https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade) (https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade), identify the Application (client) ID of the application, for which you want to limit access.

3. Create a new mail-enabled security group, or use an existing one, and identify the email address for the group. The following is an example of creating a new mail-enabled security group:

```
New-DistributionGroup -Name <"MSV Test Group Name"> -Type "Security" -Members <"test-group@example.com">
```

This example is the output from creating the security group:

Name	DisplayName	GroupType	PrimarySmtpAddress
MSV Test Group	MSV Test Group	Universal, SecurityEnabled	test-group@example.com

4. Create an application access policy by running the following command. Add the arguments for **AppID**, **PolicyScopeGroupID**, and **Description** that match the information for the distribution group you created.

```
New-ApplicationAccessPolicy -AppID <add AppID> -PolicyScopeGroupID <add PolicyScopeGroupID> -AccessRights RestrictAccess -Description <"Restrict this app to members of distribution group X.">
```

The following is an example of the output from this command, using `MSV Test Group` as the group ID:

```
ScopeName      : MSV Test Group
ScopelIdentity : MSV Test Group
Identity       : IDENTITY_VALUE
AppId          : "AppID"
ScopelIdentityRaw : SCOPE_IDENTITY_VALUE
Description    : Restrict this app to members of distribution group MSV Test Group.
AccessRight    : RestrictAccess
ShardType      : All
```

5. Run the following command to test the new application access policy. Add the arguments for **Identity** and **AppID**.

```
Test-ApplicationAccessPolicy -Identity <add Identity> -AppID <add AppID>
```

The following is an example of the output from this command:

```
AppId          : "AppID"
Mailbox        : MAILBOX_VALUE
MailboxId      : MAILBOX_ID_VALUE
MailboxSid     : MAILBOX_S_ID_VALUE
AccessCheckResult : Granted
```



Changes to application access policies can take up to 30 minutes to take effect in Microsoft Graph REST API calls.

Email Settings for Office 365 with IMAP/POP

An admin must enable IMAP/POP3 and generate an application-specific password in the Microsoft 365 account used by the Director. See the [Microsoft documentation \(https://docs.microsoft.com/en-us/exchange/troubleshoot/configure-mailboxes/pop3-imap-owa-activesync-office-365\)](https://docs.microsoft.com/en-us/exchange/troubleshoot/configure-mailboxes/pop3-imap-owa-activesync-office-365) for information about enabling IMAP/POP3.



The following procedure is only valid for versions of Microsoft Office 2010 or older. Two-factor authentication is not supported for Microsoft accounts using versions of Office 2010 or older. To configure settings for an Office 365 account with Office 2013 or newer, see [Configuring Email Settings for Outlook](#).

Use the following procedure to generate an application-specific password for use when setting up an Office 365 account for use by the Director.


1. Log in to the Outlook 365 account that will be used for Email and Email Actions settings in the Director.
2. Choose **Settings > Office 365**.
3. Choose **Security & Privacy > Additional security verification**.
4. Generate an application-specific password.
 - a. At the top of the page, click **App Passwords**.
 - b. Choose create to generate an app password.
 - c. Provide a nickname for the app password (such as Director), and click **Next**.
 - d. Click **copy password to clipboard**.
5. Configure the Validation Platform [Email Settings \(https://docs.mandiant.com/home/email-settings\)](https://docs.mandiant.com/home/email-settings) with the account name and the application-specific password.
See [Microsoft's Using app passwords with apps that don't support two-step verification \(https://support.microsoft.com/en-us/account-billing/using-app-passwords-with-apps-that-don-t-support-two-step-verification-5896ed9b-4263-e681-128a-a6f2979a7944\)](https://support.microsoft.com/en-us/account-billing/using-app-passwords-with-apps-that-don-t-support-two-step-verification-5896ed9b-4263-e681-128a-a6f2979a7944) for additional info.

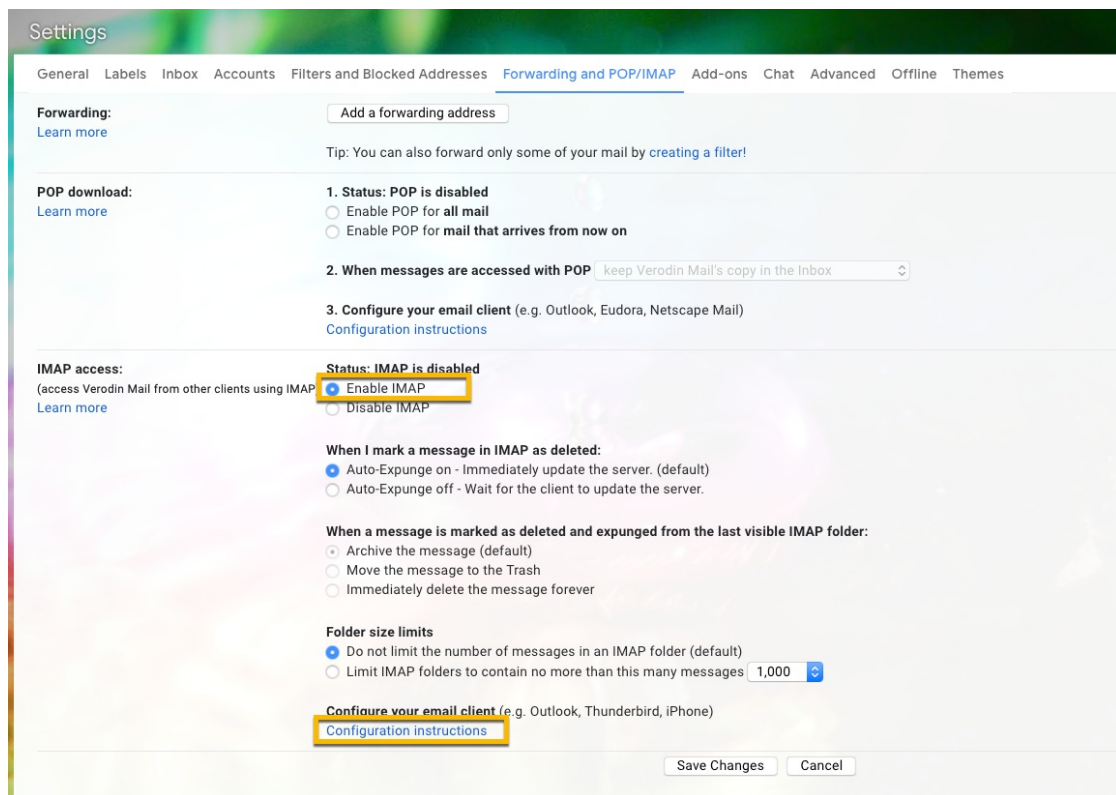
Configure Email Settings for Gmail



As of May 30, 2022, Google no longer supports the use of third-party apps or devices which ask you to sign into your Google Account using only your username and password. As a result, the procedure below will only work for Gmail accounts created prior to May 30, 2022. For more information, see [Google Account Help \(https://support.google.com/accounts/answer/6010255?hl=en&utm_source=google-account&utm_medium=profile-less-secure-apps-card\)](https://support.google.com/accounts/answer/6010255?hl=en&utm_source=google-account&utm_medium=profile-less-secure-apps-card).

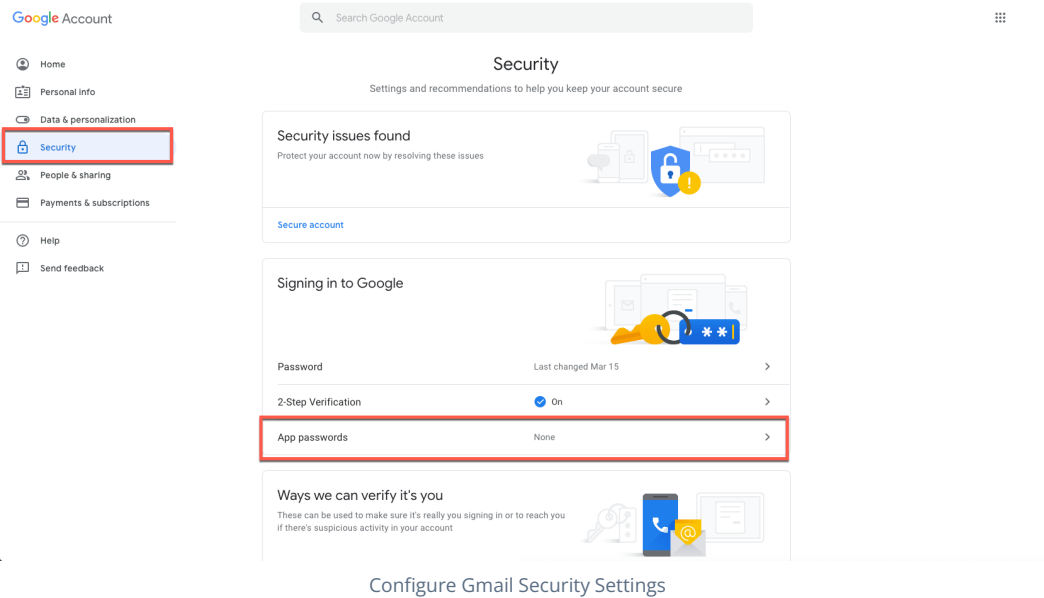
Use the following procedure to generate an application-specific password for use when setting up a Gmail account for use by the Director.

1. Log in to the Gmail account that will be used for Email and Email Actions settings in the Director.
2. Navigate to  > **Settings**.
3. Select **Forwarding and POP/IMAP**.
4. Click **Enable IMAP** in the IMAP access section.



Gmail Forwarding and POP/IMAP settings

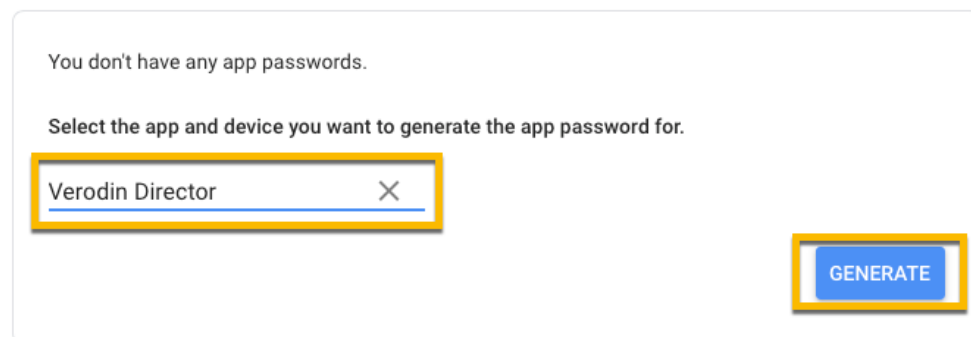
5. Click the **Configuration Instructions** link to see Gmail's recommended settings.
6. Review and make a note of the server and port settings required for Gmail. You will use these server addresses and ports when configuring Email Settings, Email Action Settings, and Email Actions.
7. Generate an application-specific password.
 - a. Go to the **Accounts** tab in your Gmail settings.
 - b. Click the **Security** menu option.



- c. Verify your account credentials when prompted.
- d. In the Select app dropdown, select **Custom**.
- e. Provide a nickname for this application (such as Security Validation Director).

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. [Learn more](#)



Generate an application-specific password

- f. Click **Generate**.
 - g. Copy the generated password. You will only need it for initial configuration of Director Email Settings.
8. Configure the Validation Platform **Email Settings** (<https://docs.mandiant.com/home/email-settings>) with the account name and the application-specific password.

Configure Email Settings for Gmail API

There are 3 steps required to establish a connection between MSV and Gmail API:

1. Establish Client ID and Client Secret
2. Grant Client ID Access to all Google Services
3. Configure Email Settings in MSV

Allow list requirements for Gmail API

The following domains must be added to the allow list from the Actor. This ensures the Actor can communicate with the cloud email service via the API.

- <https://accounts.google.com/o/oauth2>
- <https://www.googleapis.com/oauth2>
- <https://oauth2.googleapis.com/token>
- https://*.googleapis.com

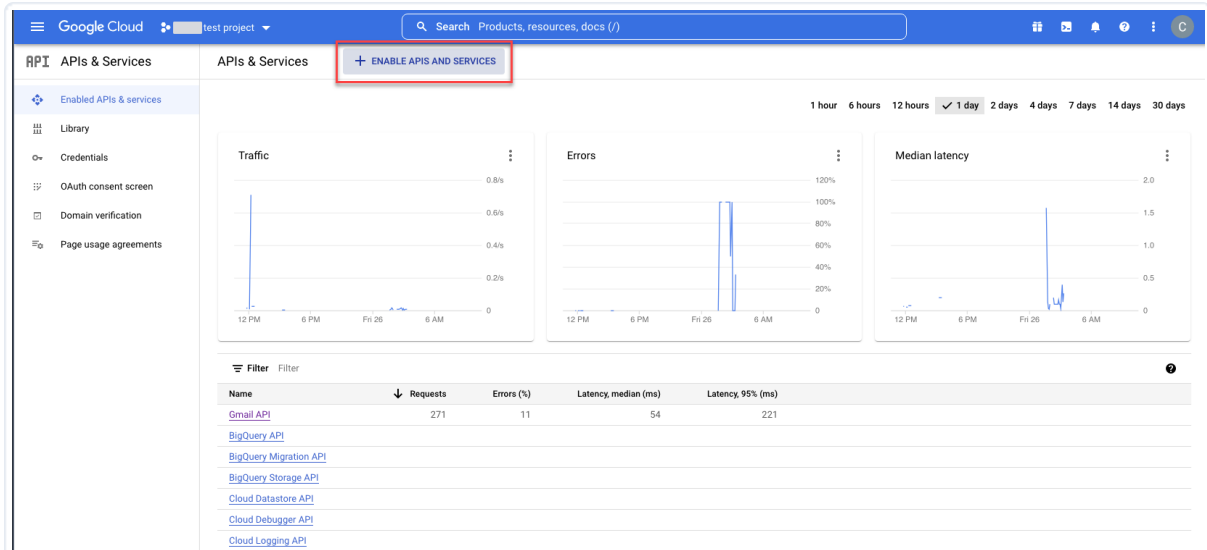
Establish Client ID and Client Secret

Use the following steps to generate a Client ID and Client Secret for use when setting up a Gmail API account for use by the Director.

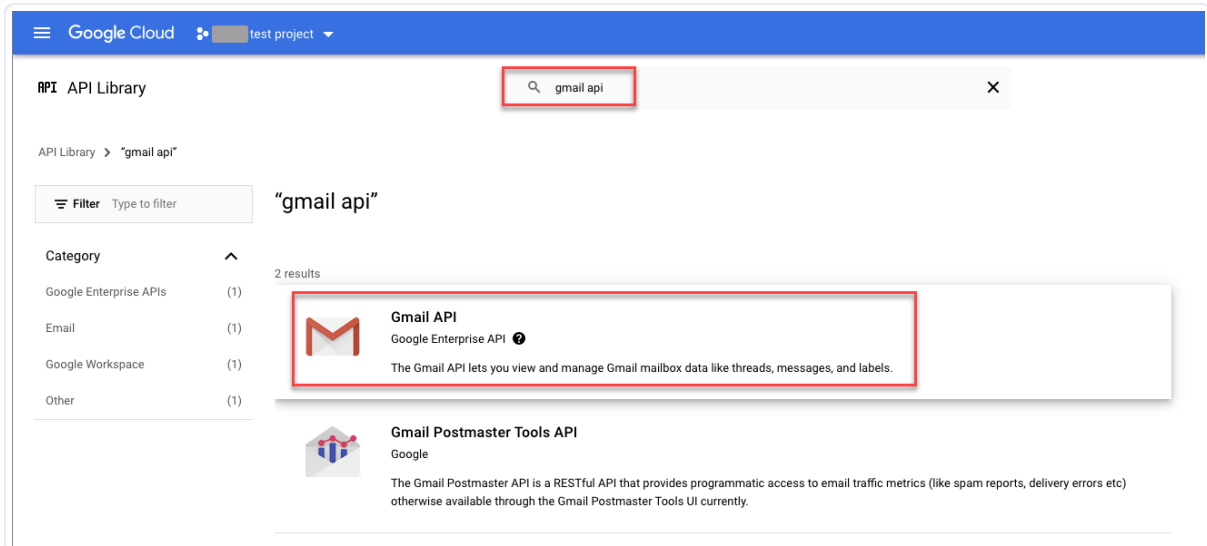


NOTE: You must be an administrator in Google Workspace to complete these steps.

1. Log in to your Google Cloud console and create a new Project dedicated to MSV Gmail API access. Each project supports only one application.
2. Within that Project, go to **APIs & Services > Enabled APIs & services**.
3. Click **+ ENABLE APPS AND SERVICES**, search for *Gmail API* in the API Library, select it, and **ENABLE**.



Name	Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
Gmail API	271	11	54	221
BigQuery API				
BigQuery Migration API				
BigQuery Storage API				
Cloud Datastore API				
Cloud Debugger API				
Cloud Logging API				



Google Cloud test project

API Library "gmail api"



API Library > "gmail api"

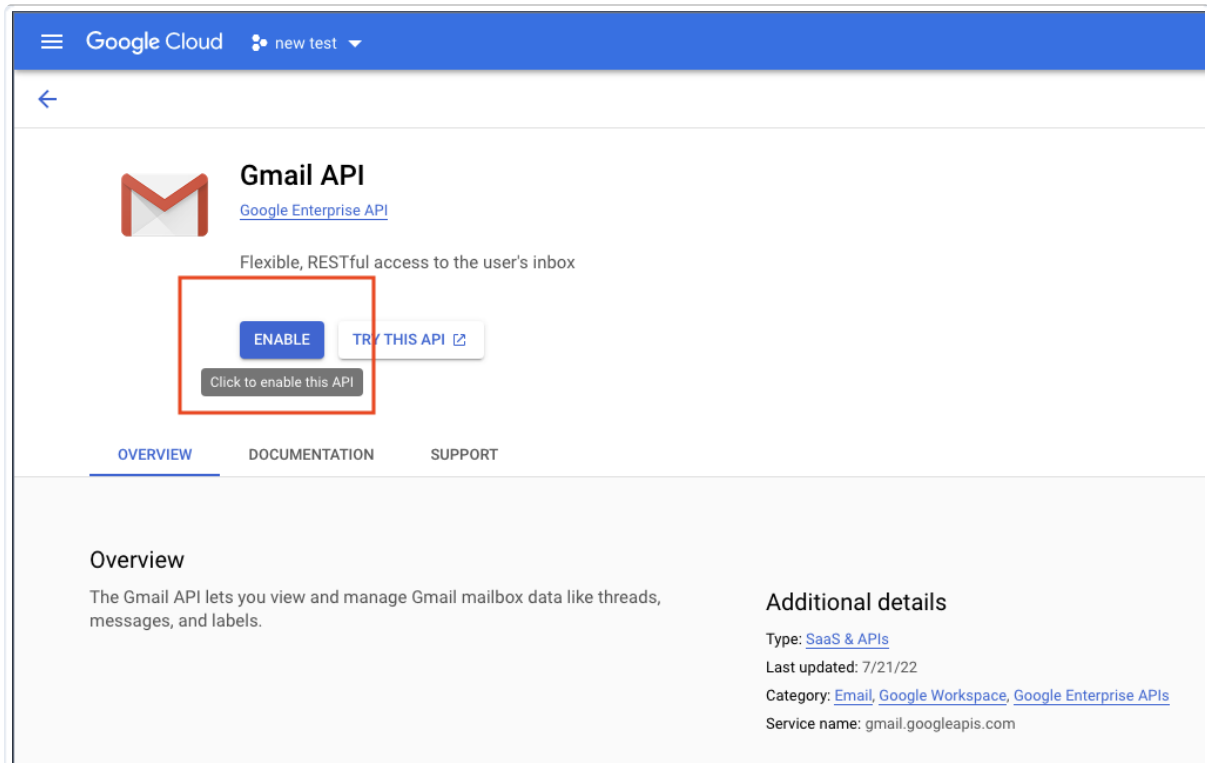
Filter Type to filter

Category

- Google Enterprise APIs (1)
- Email (1)
- Google Workspace (1)
- Other (1)

2 results

-  **Gmail API**
Google Enterprise API ⓘ
The Gmail API lets you view and manage Gmail mailbox data like threads, messages, and labels.
-  **Gmail Postmaster Tools API**
Google
The Gmail Postmaster API is a RESTful API that provides programmatic access to email traffic metrics (like spam reports, delivery errors etc) otherwise available through the Gmail Postmaster Tools UI currently.



Google Cloud new test

Gmail API
Google Enterprise API

Flexible, RESTful access to the user's inbox

[OVERVIEW](#) [DOCUMENTATION](#) [SUPPORT](#)

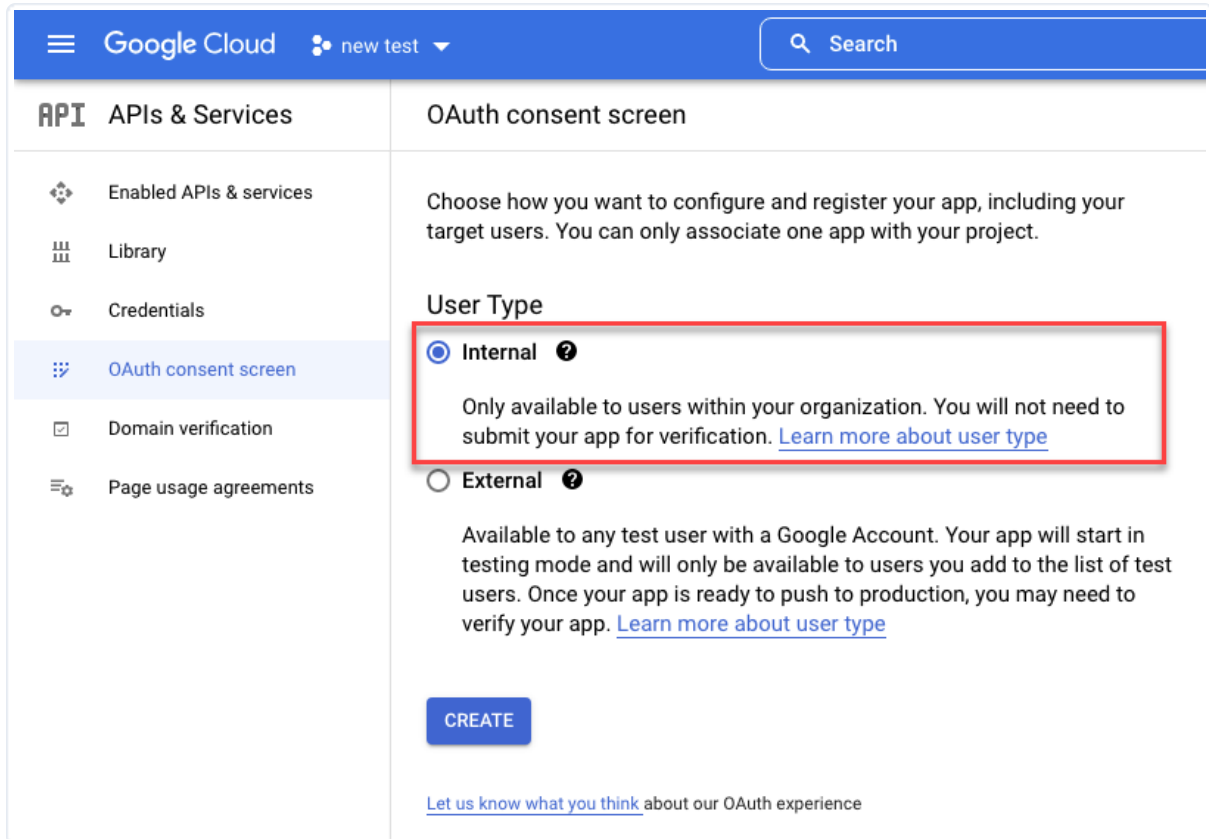
Overview

The Gmail API lets you view and manage Gmail mailbox data like threads, messages, and labels.

Additional details

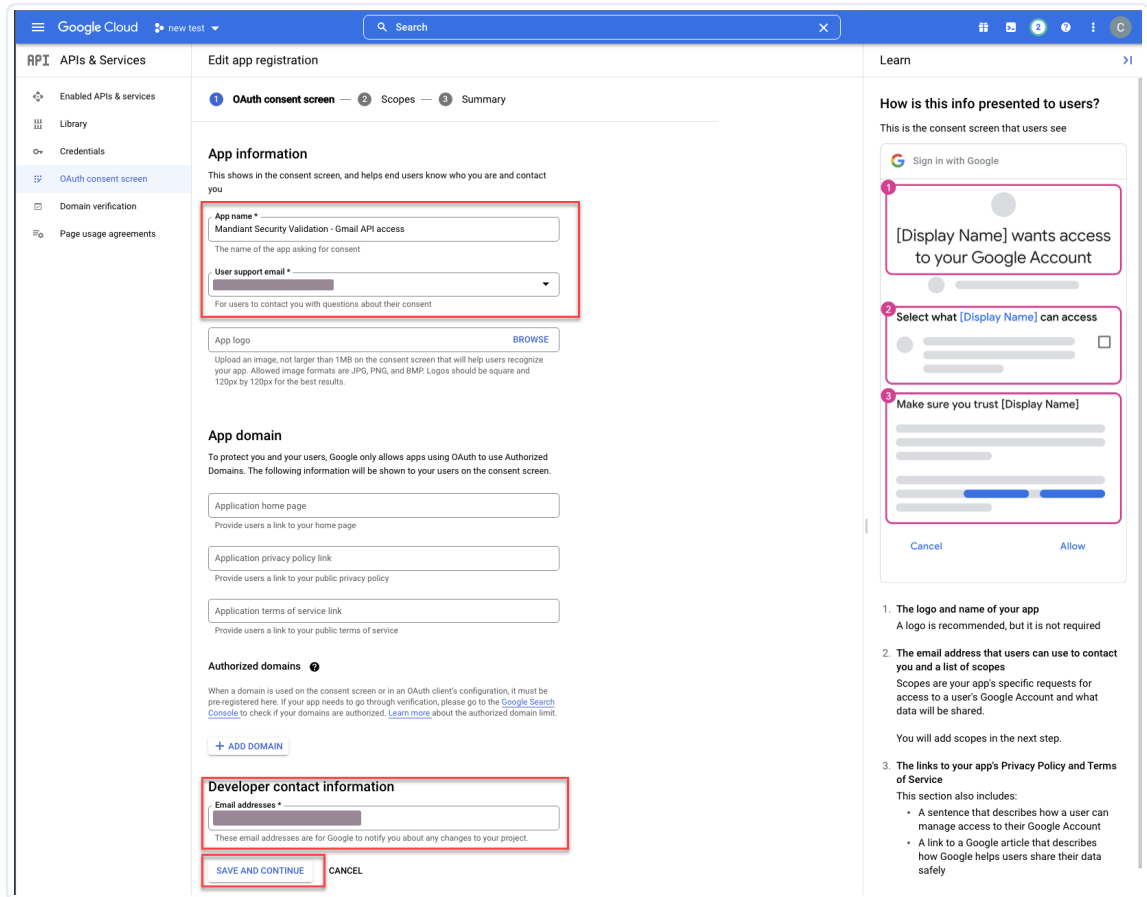
Type: [SaaS & APIs](#)
Last updated: 7/21/22
Category: [Email](#), [Google Workspace](#), [Google Enterprise APIs](#)
Service name: gmail.googleapis.com

4. Go to **APIs & Services > OAuth consent screen** . This is configuration for the enabled app.
5. Select **Internal** User Type.



The screenshot shows the Google Cloud console interface for configuring an OAuth consent screen. The left sidebar lists navigation options under 'APIs & Services', with 'OAuth consent screen' selected. The main content area is titled 'OAuth consent screen' and contains instructions: 'Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.' Below this is the 'User Type' section, which has two radio button options: 'Internal' (selected) and 'External'. The 'Internal' option is highlighted with a red rectangular box. The 'Internal' description states: 'Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)'. The 'External' option is described as: 'Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)'. At the bottom of the main area is a blue 'CREATE' button and a link: 'Let us know what you think about our OAuth experience'.

6. On the **Edit app registration** page, populate the following fields, then click **SAVE AND CONTINUE**:
- App name**
 - User support email** - This should be the person responsible for MSV in the organization
 - Developer contact information: Email addresses** - This should also be the person responsible for MSV in the organization



App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *
Mandiant Security Validation - Gmail API access
The name of the app asking for consent

User support email *
For users to contact you with questions about their consent

App logo [BROWSE](#)
Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page
Provide users a link to your home page

Application privacy policy link
Provide users a link to your public privacy policy

Application terms of service link
Provide users a link to your public terms of service

Authorized domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

[+ ADD DOMAIN](#)

Developer contact information

Email addresses *
These email addresses are for Google to notify you about any changes to your project.

[SAVE AND CONTINUE](#) [CANCEL](#)

Learn

How is this info presented to users?
This is the consent screen that users see

Sign in with Google

- The logo and name of your app**
A logo is recommended, but it is not required
- The email address that users can use to contact you and a list of scopes**
Scopes are your app's specific requests for access to a user's Google Account and what data will be shared.
You will add scopes in the next step.
- The links to your app's Privacy Policy and Terms of Service**
This section also includes:
 - A sentence that describes how a user can manage access to their Google Account
 - A link to a Google article that describes how Google helps users share their data safely

7. On the **Scopes** page, select **Gmail API** and click **Update**. This will show up under **Your restricted scopes**.

Google Cloud
new test
Search gmail api

APIs & Services

- Enabled APIs & services
- Library
- Credentials
- OAuth consent screen
- Domain verification
- Page usage agreements

Edit app registration

OAuth consent screen
 Scopes
 Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

[ADD OR REMOVE SCOPES](#)

Your non-sensitive scopes

API	Scope	User-facing description
No rows to display		

Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

API	Scope	User-facing description
No rows to display		

Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

API	Scope	User-facing description
No rows to display		

[SAVE AND CONTINUE](#)
[CANCEL](#)

Update selected scopes

Only scopes for enabled APIs are listed below. To add a missing scope to this screen, find and enable the API in the [Google API Library](#) or use the Pasted Scopes text box below. Refresh the page to see any new APIs you enable from the Library.

Filter: Gmail API Enter property name or value

API	Scope	User-facing description	
<input checked="" type="checkbox"/>	Gmail API	https://mail.google.com/	Read, compose, send, and permanently delete all your email from Gmail
<input type="checkbox"/>	Gmail API	.../auth/gmail.modify	Read, compose, and send emails from your Gmail account
<input type="checkbox"/>	Gmail API	.../auth/gmail.compose	Manage drafts and send emails
<input type="checkbox"/>	Gmail API	.../auth/gmail.addons.current.action.compose	Manage drafts and send emails when you interact with the add-on
<input type="checkbox"/>	Gmail API	.../auth/gmail.addons.current.message.action	View your email messages when you interact with the add-on
<input type="checkbox"/>	Gmail API	.../auth/gmail.readonly	View your email messages and settings
<input type="checkbox"/>	Gmail API	.../auth/gmail.metadata	View your email message metadata such as labels and headers, but not the email body
<input type="checkbox"/>	Gmail API	.../auth/gmail.insert	Add emails into your Gmail mailbox
<input type="checkbox"/>	Gmail API	.../auth/gmail.addons.current.message.metadata	View your email message metadata when the add-on is running
<input type="checkbox"/>	Gmail API	.../auth/gmail.addons.current.message.readonly	View your email messages when the add-on is running

Rows per page: 10 | 1 - 10 of 14

Manually add scopes

If the scopes you would like to add do not appear in the table above, you can enter them here. Each scope should be on a new line or separated by commas. Please provide the full scope string (beginning with 'https://'). When you are finished, click 'Add to table'.

ADD TO TABLE

[UPDATE](#)

Google Cloud new test Search

API APIs & Services

- Enabled APIs & services
- Library
- Credentials
- OAuth consent screen
- Domain verification
- Page usage agreements

Edit app registration

OAuth consent screen —
 2 **Scopes** —
 3 Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

ADD OR REMOVE SCOPES

Your non-sensitive scopes

API ↑	Scope	User-facing description
No rows to display		

🔒 Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

API ↑	Scope	User-facing description
No rows to display		

🔒 Your restricted scopes

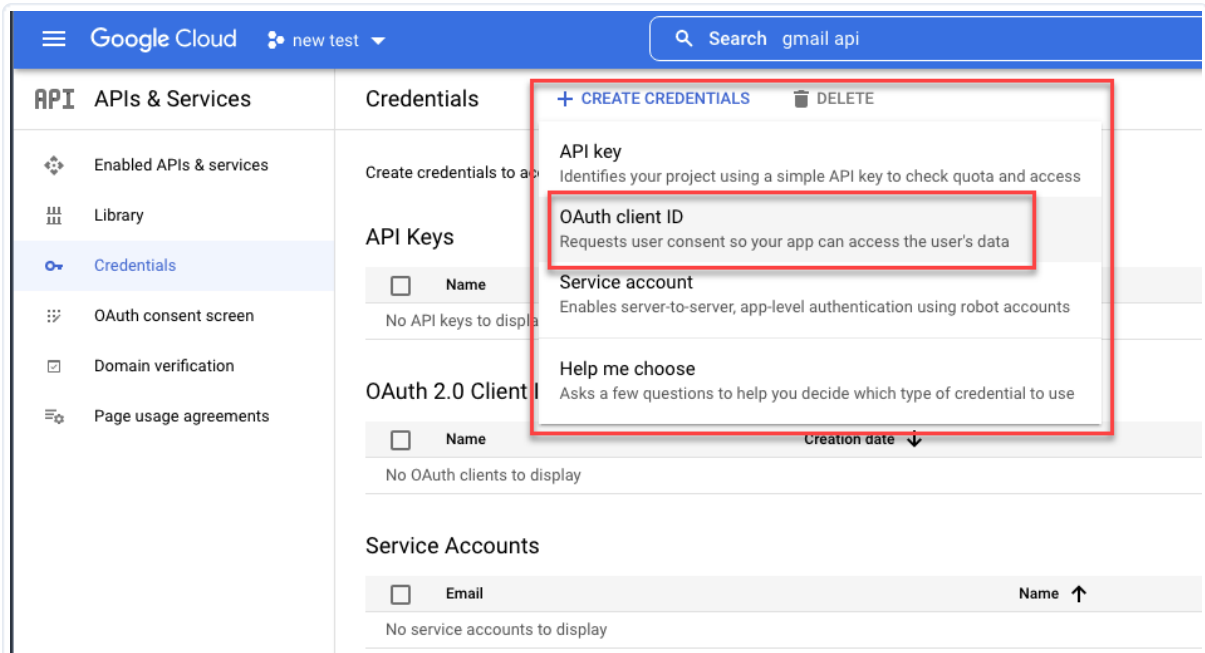
Restricted scopes are scopes that request access to highly sensitive user data.

Gmail scopes

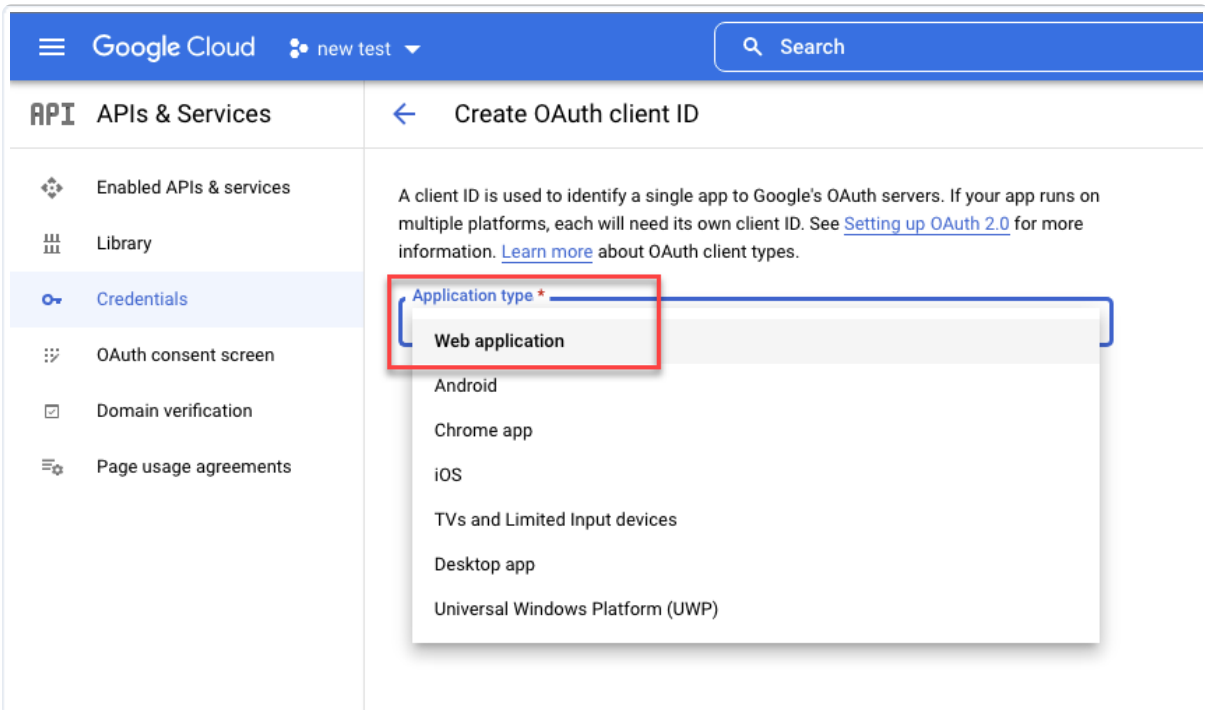
API ↑	Scope	User-facing description
Gmail API	https://mail.google.com/	Read, compose, send, and permanently delete all your email from Gmail 🗑️

SAVE AND CONTINUE
CANCEL

8. Go to **APIs & Services > Credentials**.
9. Click + **CREATE CREDENTIALS** and select **OAuth client ID**.



10. For Application type, select **Web application** and enter **Name**.



11. Enter the MSV Director address under **Authorized redirect URIs** and click **Create**.



This is the **Gmail API redirect URL** when adding a **Gmail API** email profile to MSV. For more information about adding email profiles, see **Managing Email Settings** (<https://docs.mandiant.com/home/msv-email-settings>).

Add Email Profile ✕

Profile Configuration

Server Type* Gmail API

Send verification email manually

Email Address* *Email Address*

Select Security Zone* All zones

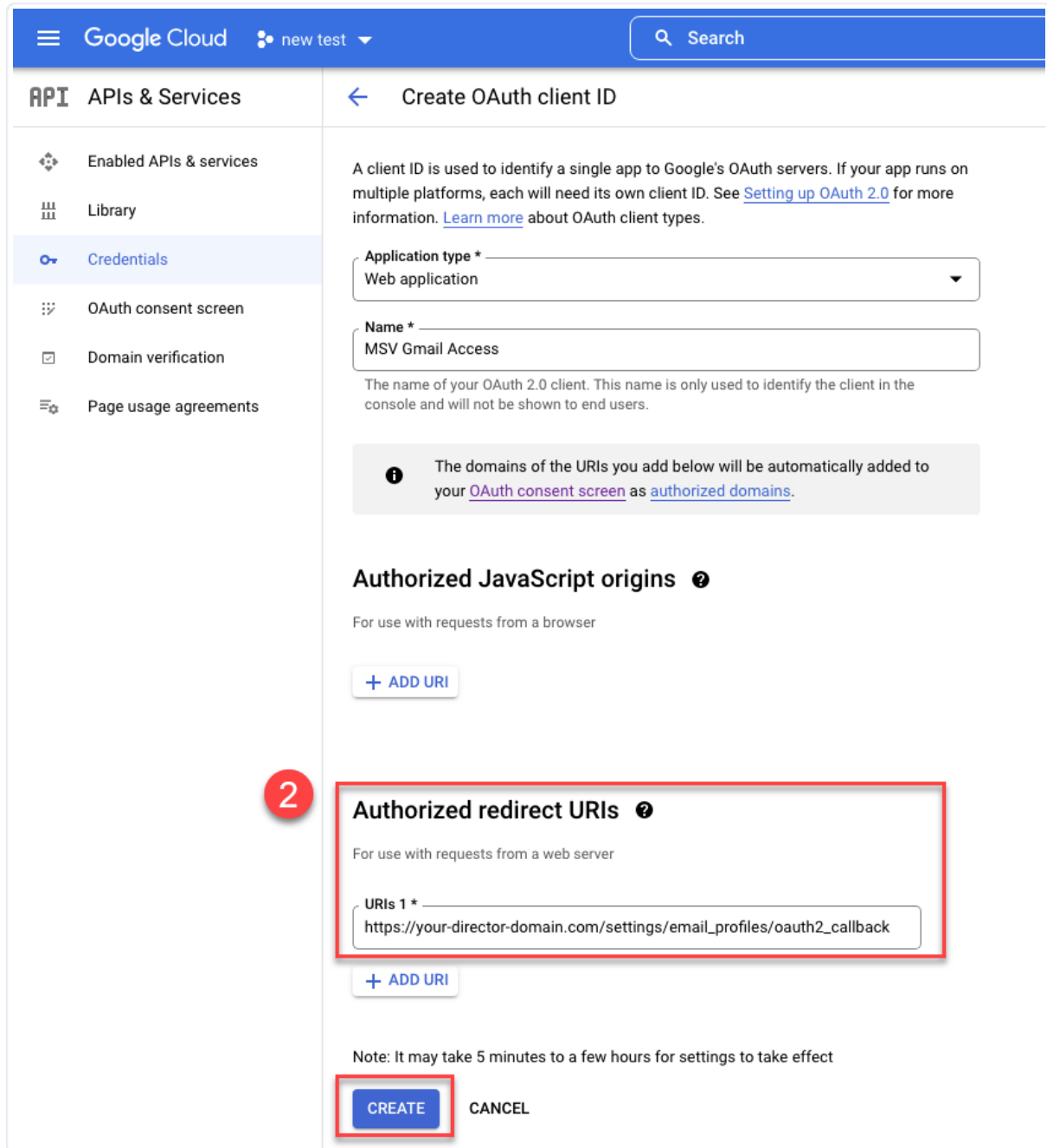
Select Actor(s)*
actor_4.9.0.0-40
actor_4.9.0.0-40_2

Client ID* *Client ID*

Client Secret* *Gmail client secret*

Gmail API redirect URL ¹ `https://[redacted].com/settings/email_profiles/oauth2_callback`

Close Submit



Google Cloud new test Search

API APIs & Services ← Create OAuth client ID

Enabled APIs & services
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

Application type *
Web application

Name *
MSV Gmail Access

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ⓘ
For use with requests from a browser
[+ ADD URI](#)

2 **Authorized redirect URIs** ⓘ
For use with requests from a web server
URIs 1 *
https://your-director-domain.com/settings/email_profiles/oauth2_callback
[+ ADD URI](#)

Note: It may take 5 minutes to a few hours for settings to take effect


[CREATE](#) CANCEL



12. Retain the resulting **Client ID** and **Client Secret** for use in the steps below.


OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth access is restricted to users within your organization unless the [OAuth consent screen](#) is published and verified

Your Client ID
575183851334-pf93i2l3pnvs38gooiobing0bi1jmg3n.apps.gc 

Your Client Secret
 

 **DOWNLOAD JSON**

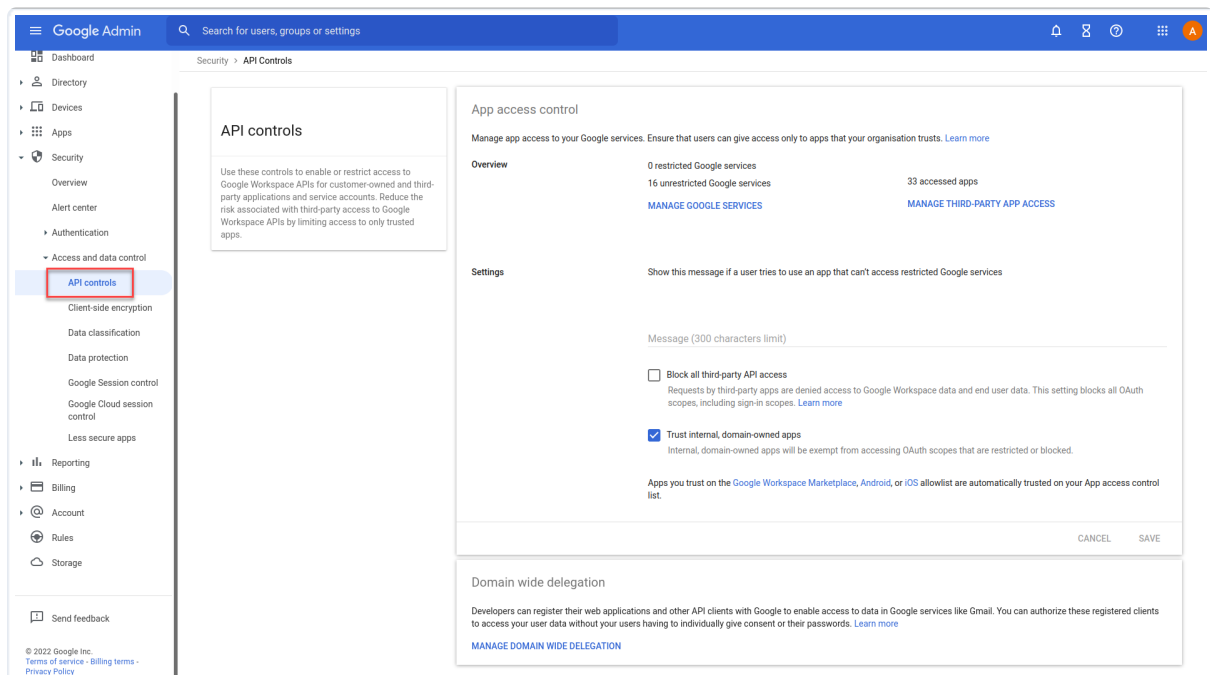
OK

Grant Client ID Access To All Google Services



You must be a superadmin to complete these steps.

1. Log in to the Google Admin console and navigate to **Security > Access and data control > API controls**.



The screenshot shows the Google Admin console interface. The left sidebar contains a navigation menu with 'API controls' highlighted in red. The main content area is titled 'API controls' and includes a description of the controls. On the right, the 'App access control' section is visible, showing '0 restricted Google services', '16 unrestricted Google services', and '33 accessed apps'. There are two buttons: 'MANAGE GOOGLE SERVICES' and 'MANAGE THIRD-PARTY APP ACCESS'. The 'Settings' section has a checkbox for 'Block all third-party API access' (unchecked) and a checked checkbox for 'Trust internal, domain-owned apps'. At the bottom, there is a 'Domain wide delegation' section with a 'MANAGE DOMAIN WIDE DELEGATION' button.

2. Click **MANAGE THIRD-PARTY APP ACCESS**.

App access control

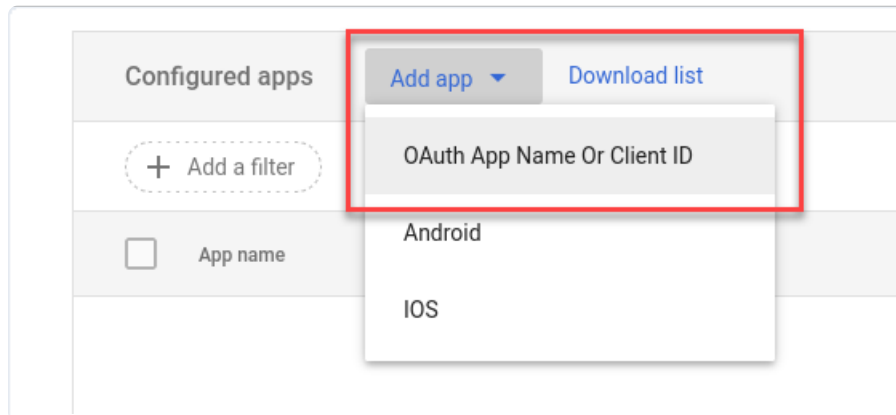
Manage app access to your Google services. Ensure that users can give access only to apps that your organisation trusts. [Learn more](#)

Overview

0 restricted Google services	33 accessed apps
16 unrestricted Google services	

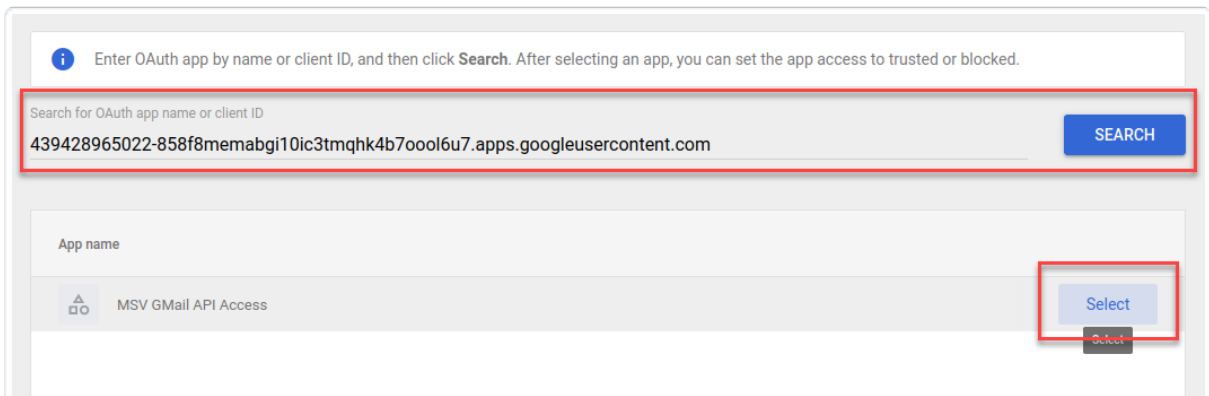
[MANAGE GOOGLE SERVICES](#) [MANAGE THIRD-PARTY APP ACCESS](#)

- Under **Configured apps**, click **Add app** and select **OAuth App Name Or Client ID**.



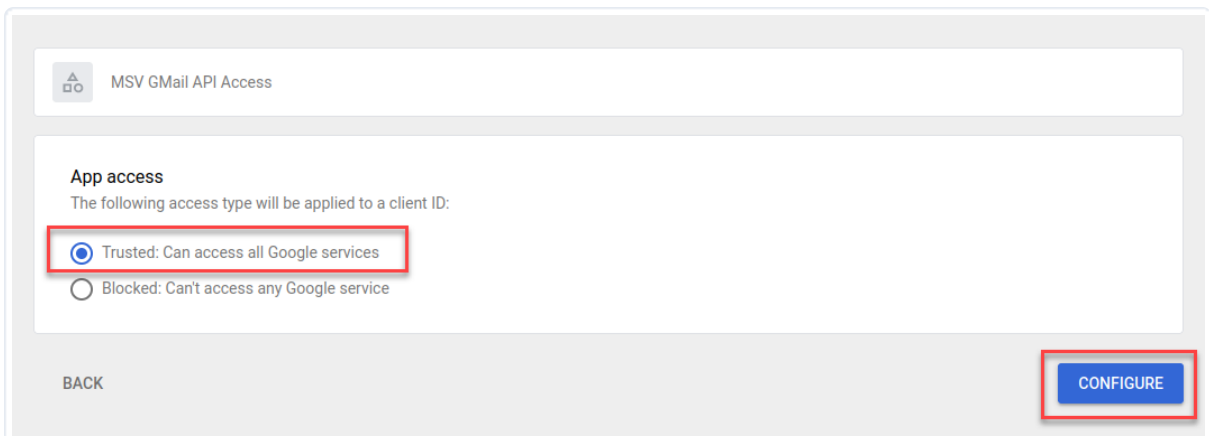
The screenshot shows the 'Configured apps' section with a red box around the 'Add app' dropdown menu. The dropdown menu is open, showing 'OAuth App Name Or Client ID' as the selected option, with 'Android' and 'IOS' as other options. A 'Download list' button is also visible.

- Search** for the **Client ID** created above and **Select**.



The screenshot shows the search interface for OAuth apps. A red box highlights the search input field containing the Client ID '439428965022-858f8memabgi10ic3tmqhk4b7ool6u7.apps.googleusercontent.com' and the 'SEARCH' button. Below the search field, the app 'MSV Gmail API Access' is listed with a 'Select' button highlighted by a red box.

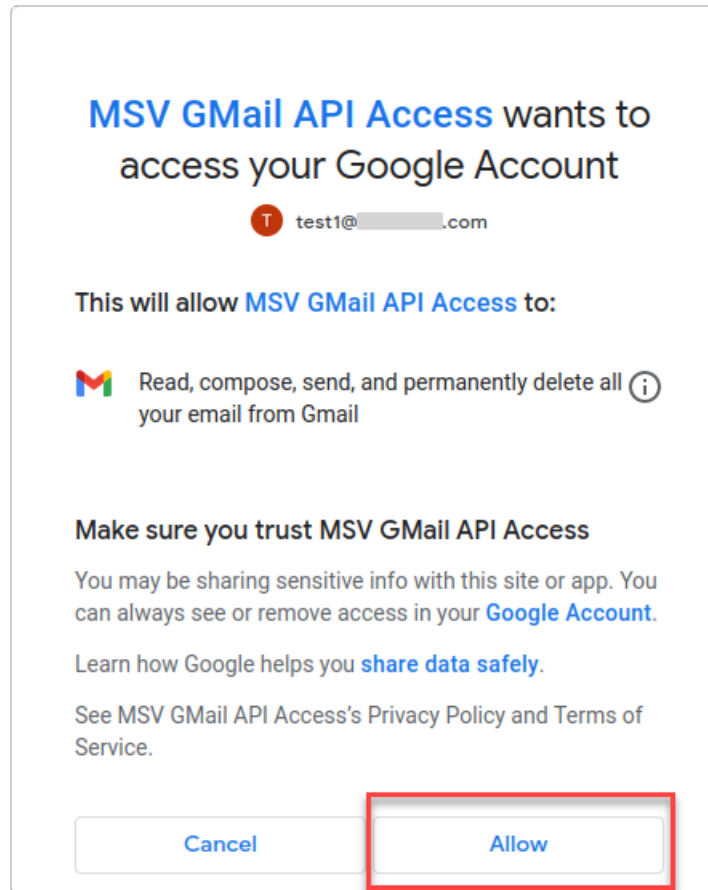
- Select **Trusted: Can access all Google services** and click **Configure**.



The screenshot shows the app access configuration screen for 'MSV Gmail API Access'. A red box highlights the 'Trusted: Can access all Google services' radio button. Another red box highlights the 'CONFIGURE' button at the bottom right.

Configure Gmail API Email Settings In MSV

- Configure the Validation Platform **Email Settings** (<https://docs.mandiant.com/home/msv-email-settings>) with the **Client ID** and **Client Secret** generated above.
- When prompted by Google, **Allow** access by MSV.



Configure Email Settings for Outlook

 This procedure is for Office 365 clients using Office 2013 or newer.

See [How to Create App Passwords for Outlook.com](https://www.lifewire.com/app-specific-passwords-outlook-1170665) (<https://www.lifewire.com/app-specific-passwords-outlook-1170665>).

Configure Email Settings for iCloud

See [How to generate app-specific passwords with iCloud on iPhone, iPad, and Mac](https://www.imore.com/how-generate-app-specific-passwords-iphone-ipad-mac) (<https://www.imore.com/how-generate-app-specific-passwords-iphone-ipad-mac>).