Mandiant

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.

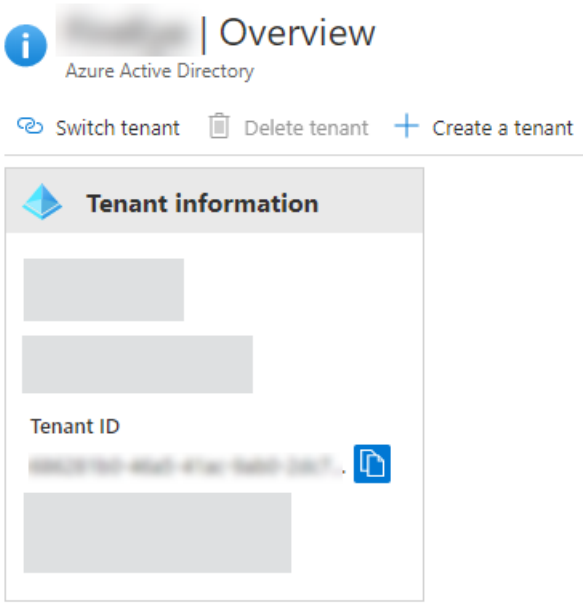
- `https://login.microsoftonline.com/*`
- `https://graph.microsoft.com/*`

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

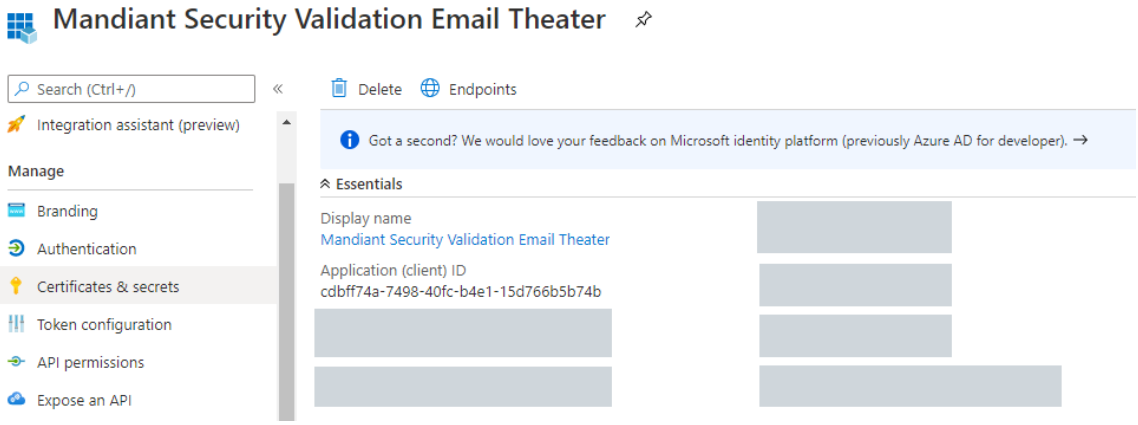
- `login.microsoftonline.us/*`
- `graph.microsoft.us/*`
- `dod-graph.microsoft.us/*`

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.



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 account
s 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)**, 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.c
om">
```

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> -AccessRig
ht 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
ScopeIdentity   : MSV Test Group
Identity        : IDENTITY_VALUE
AppId           : "AppID"
ScopeIdentityRaw : 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) 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.

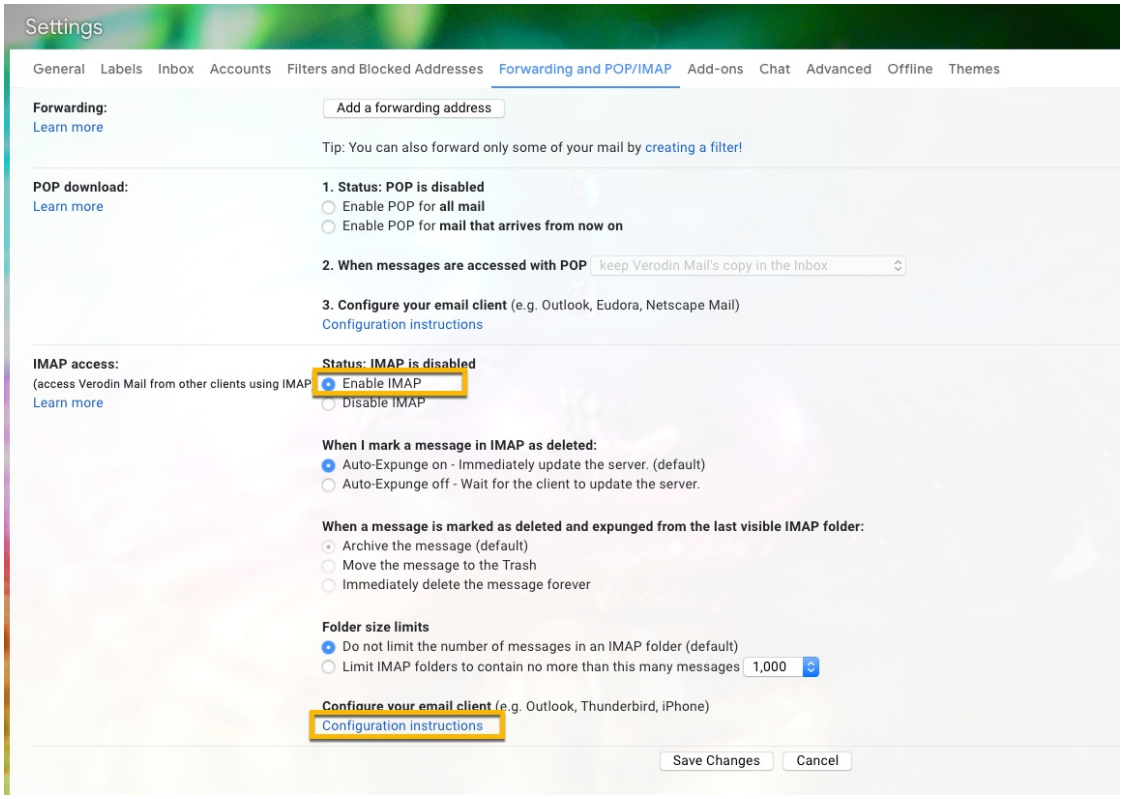
1. Log in to the Outlook 365 account that will be used for Email and Email Actions settings in the Director.
2. Choose **Settings > Office 365**.
3. Choose **Security & Privacy > Additional security verification** .
4. Generate an application-specific password.
    a. At the top of the page, click **App 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) 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) 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).

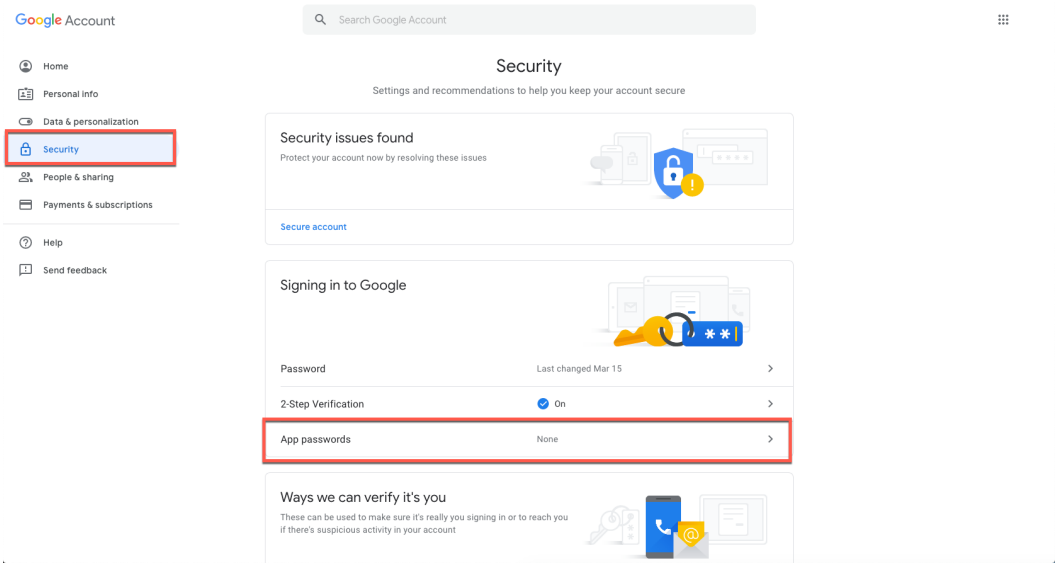
Use the following procedure to generate an application-specific password for use when setting up a Gmail account for use by the Director.

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.



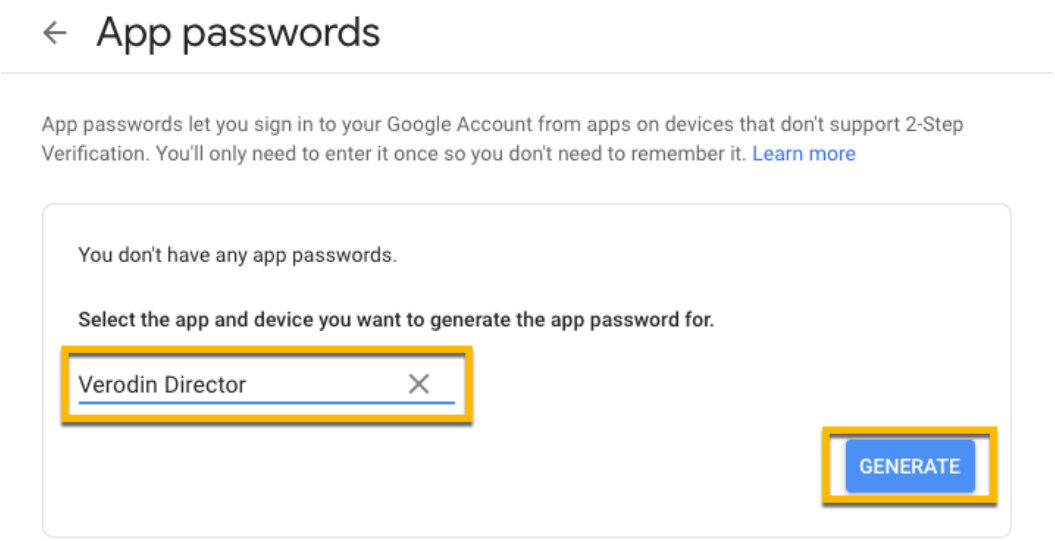
Gmail Forwarding and POP/IMAP settings

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.



Configure Gmail Security Settings

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).



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.

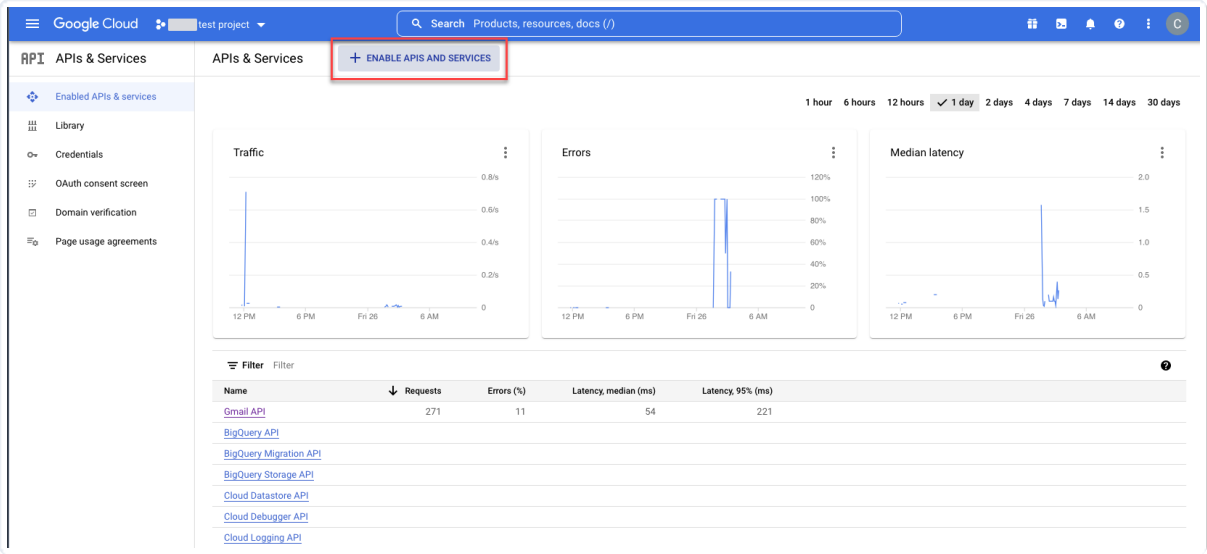
- `https://accounts.google.com/o/oauth2`
- `https://www.googleapis.com/oauth2`
- `https://oauth2.googleapis.com/token`
- `https://*.googleapis.com`

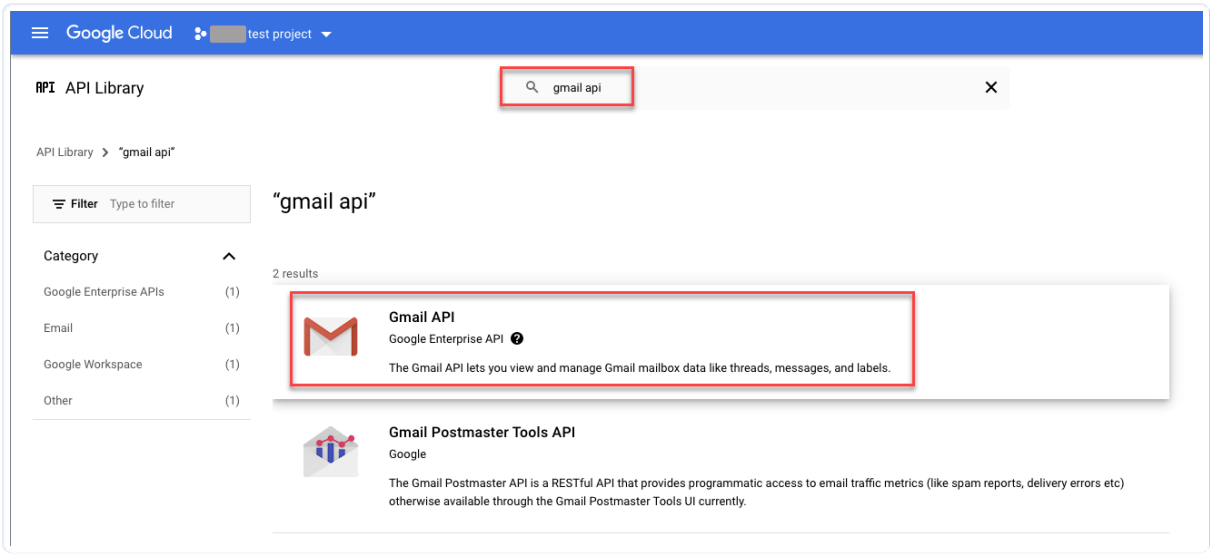
Establish Client ID and Client Secret

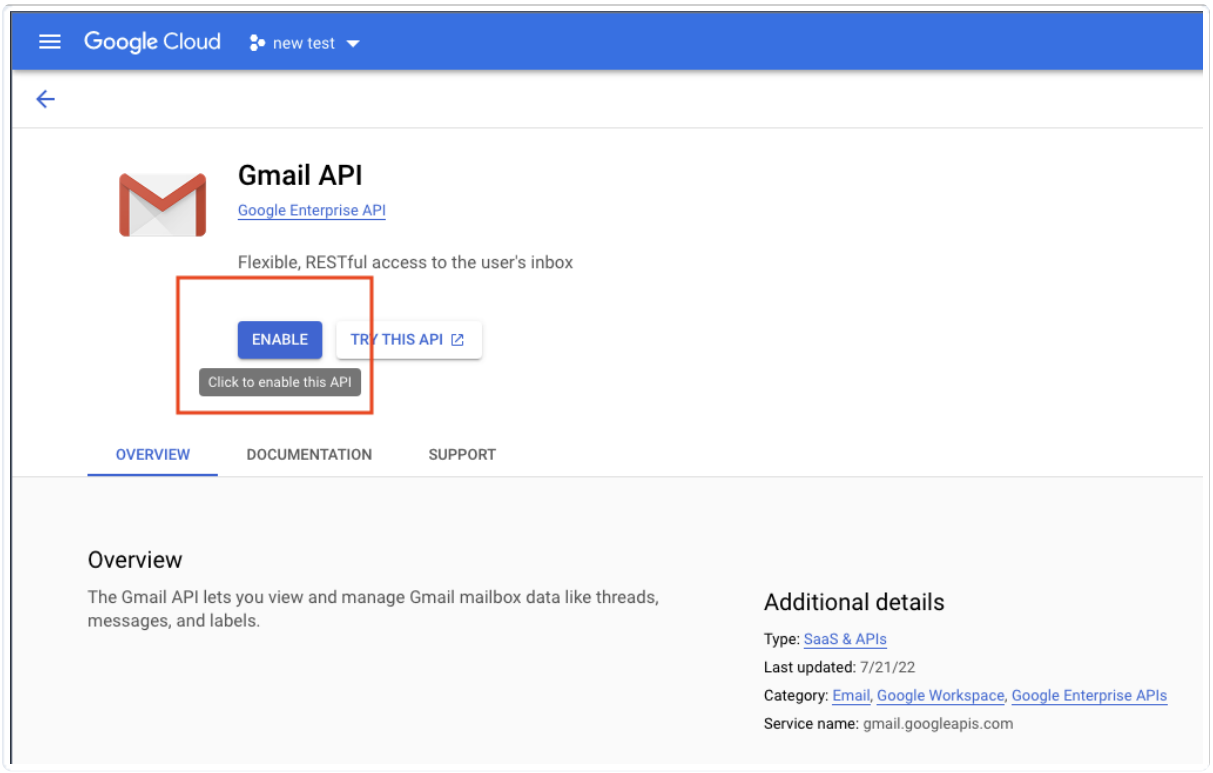
Use the following steps to generate a Client ID and Client Secret for use when setting up a Gmail API account for use by the Director.

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

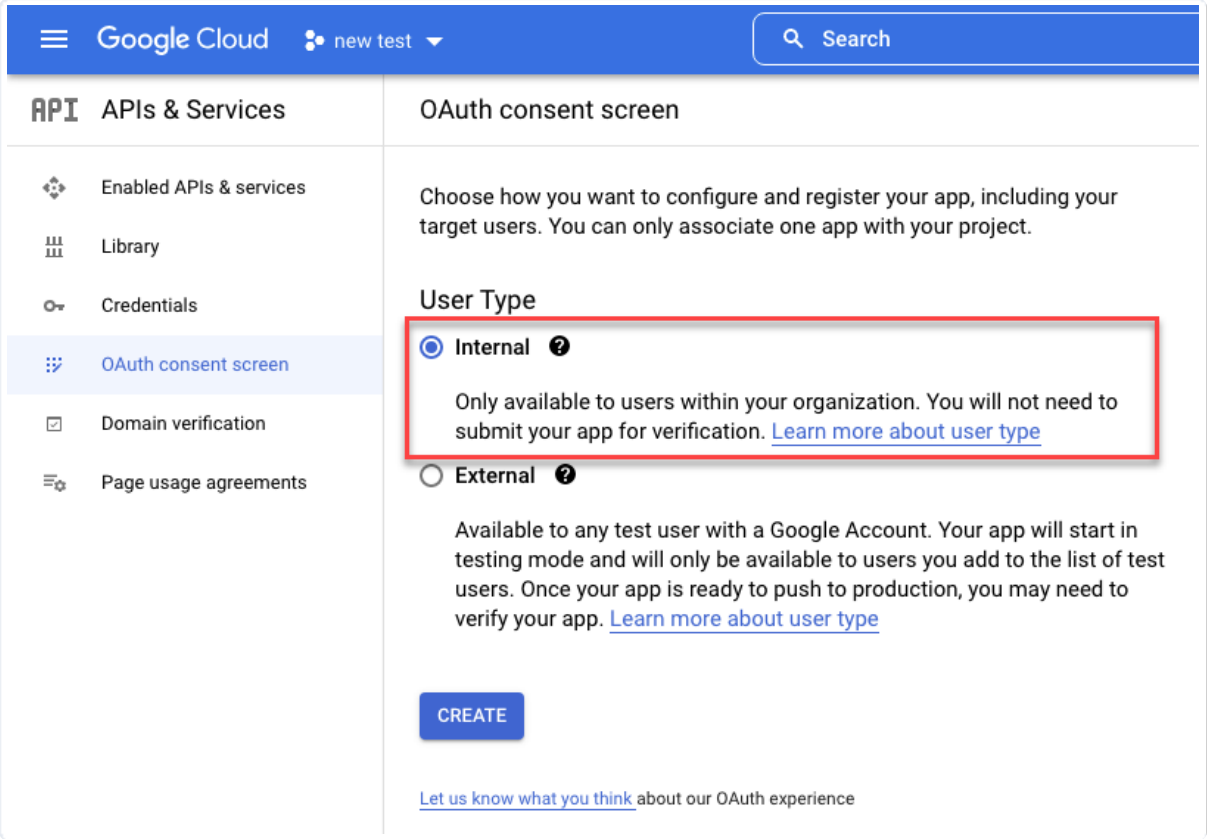
1. Log in to your Google Cloud console and create a new Project dedicated to MSV Gmail API access. Each project supports only one application.
2. Within that Project, go to **APIs & Services > Enabled APIs & services** .
3. Click **+ ENABLE APPS AND SERVICES**, search for *Gmail API* in the API Library,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



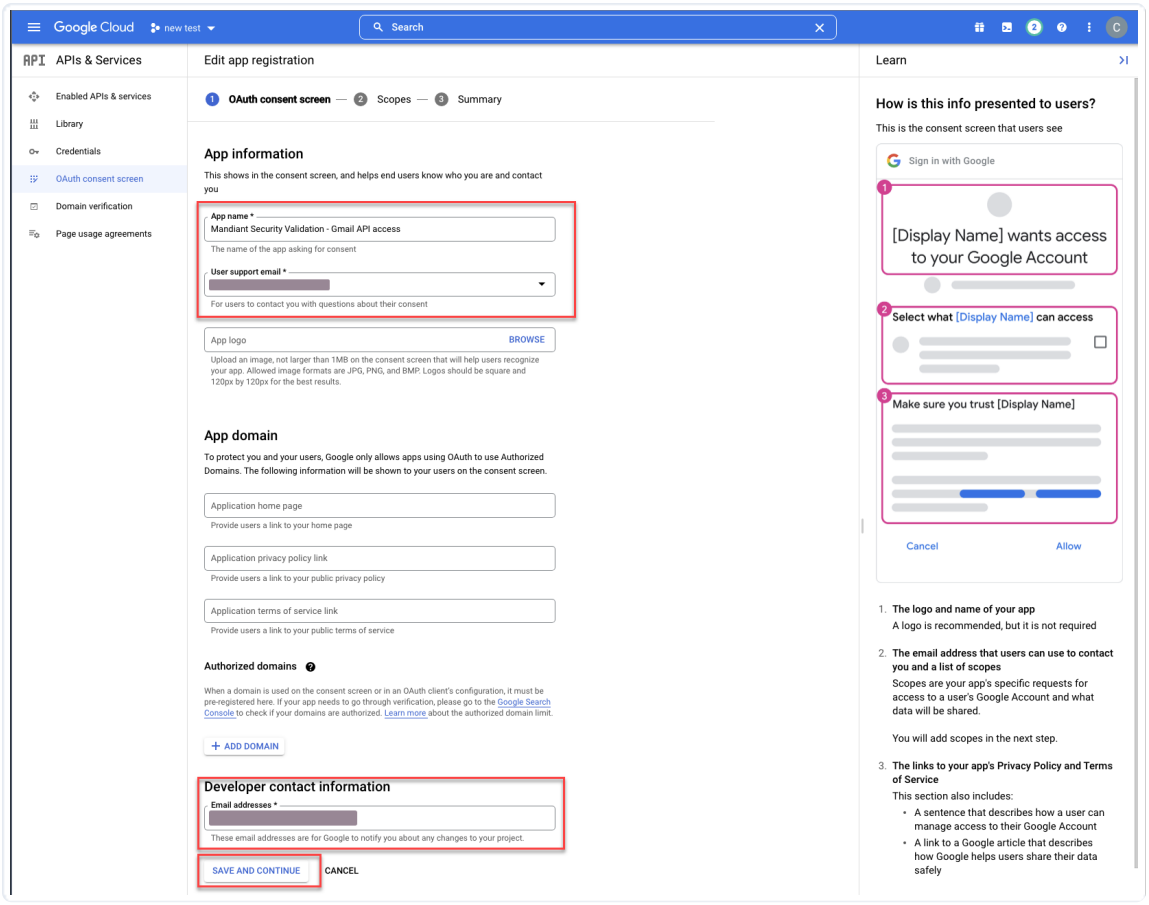




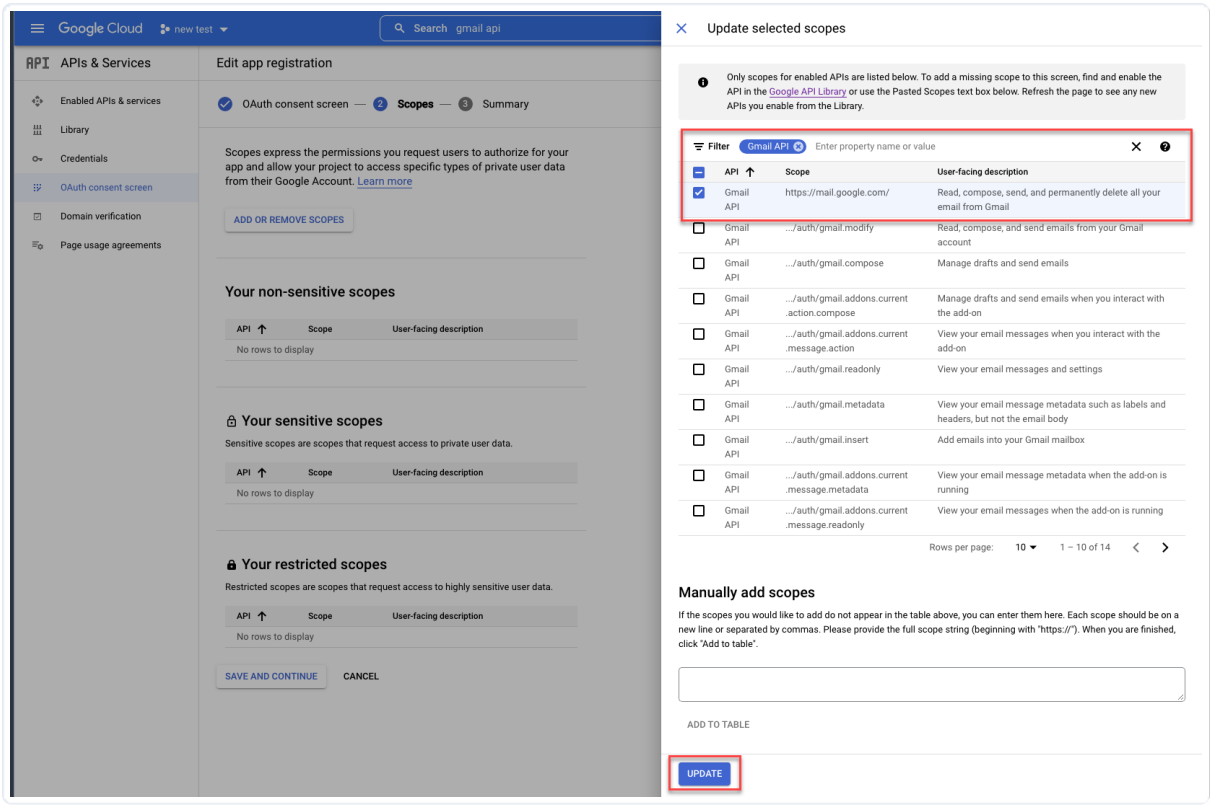
4. Go to **APIs & Services > OAuth consent screen** . This is configuration for the enabled app.
5. Select **Internal** User Type.

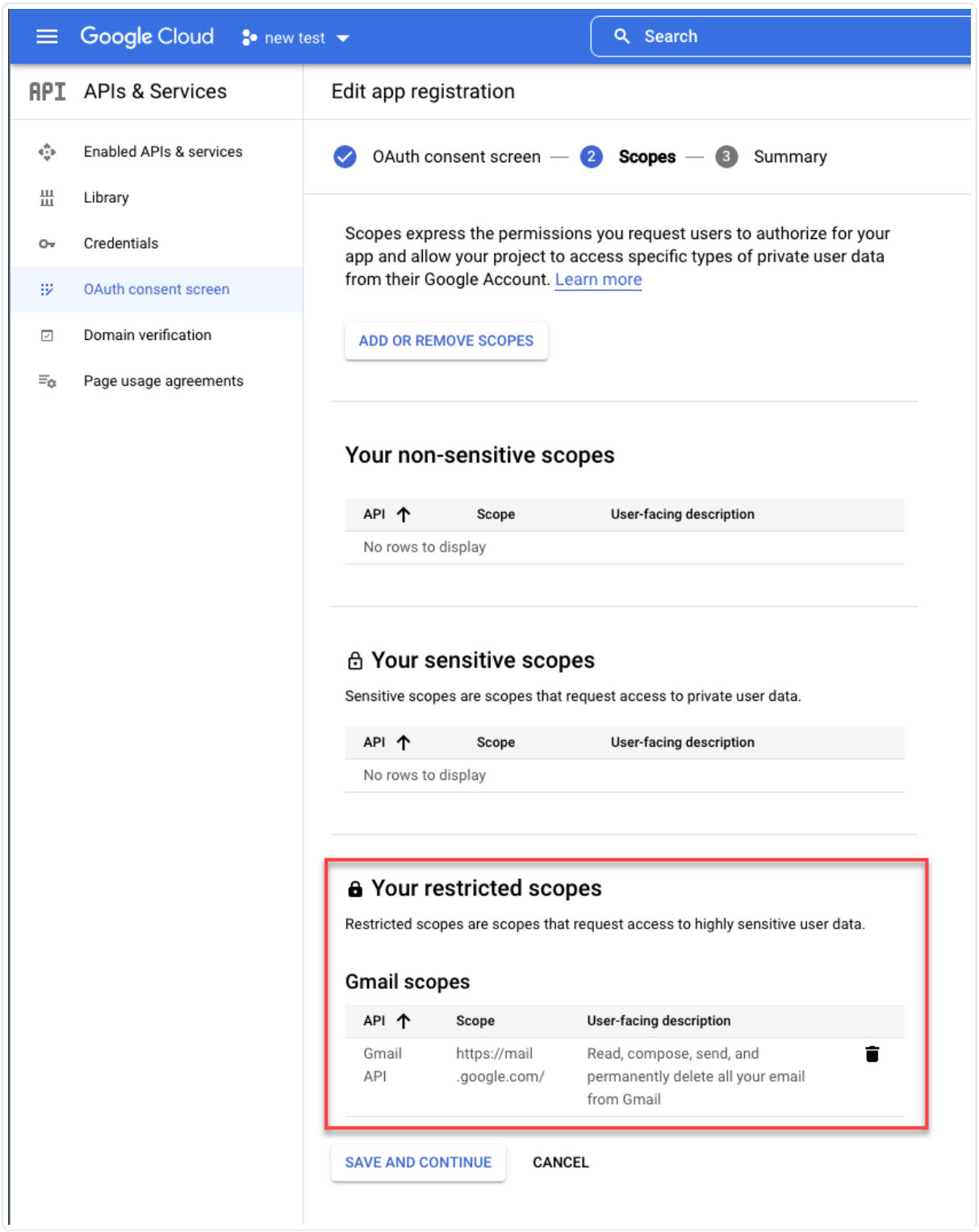


6. On the **Edit app registration** page, populate the following fields, then click **SAVE AND CONTINUE**:
    a. **App name**
    b. **User support email** - This should be the person responsible for MSV in the organization
    c. **Developer contact information: Email addresses** - This should also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

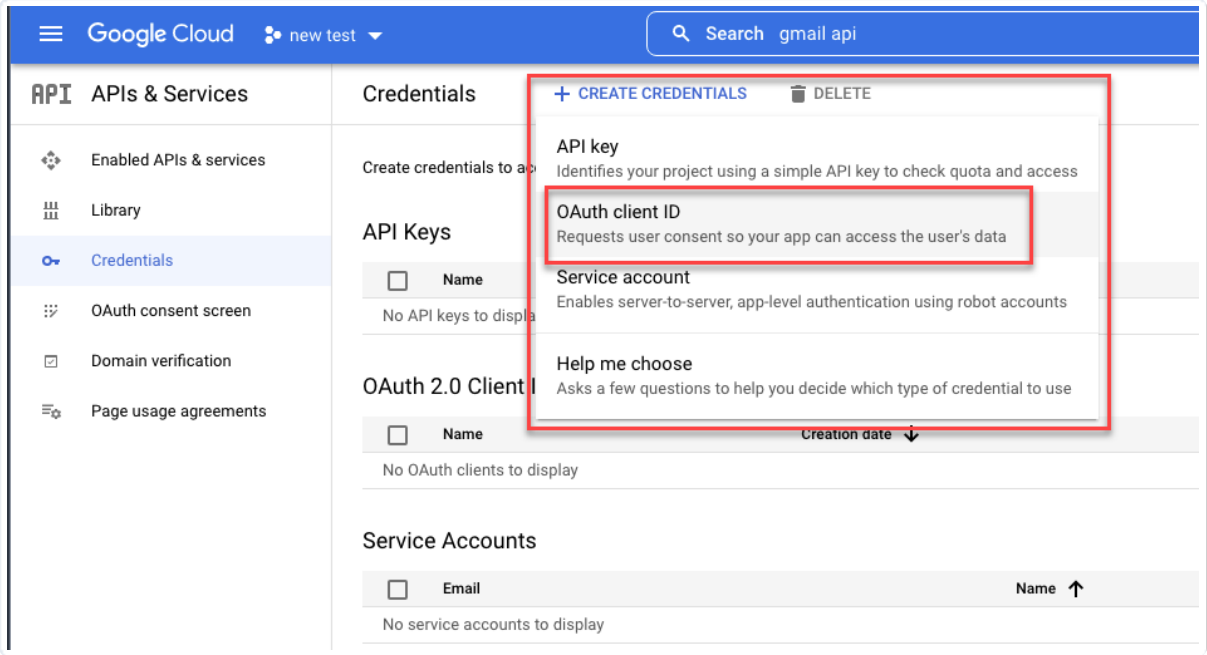


7. On the **Scopes** page, select **Gmail API** and click **Update**. This will show up under **Your restricted scopes**.

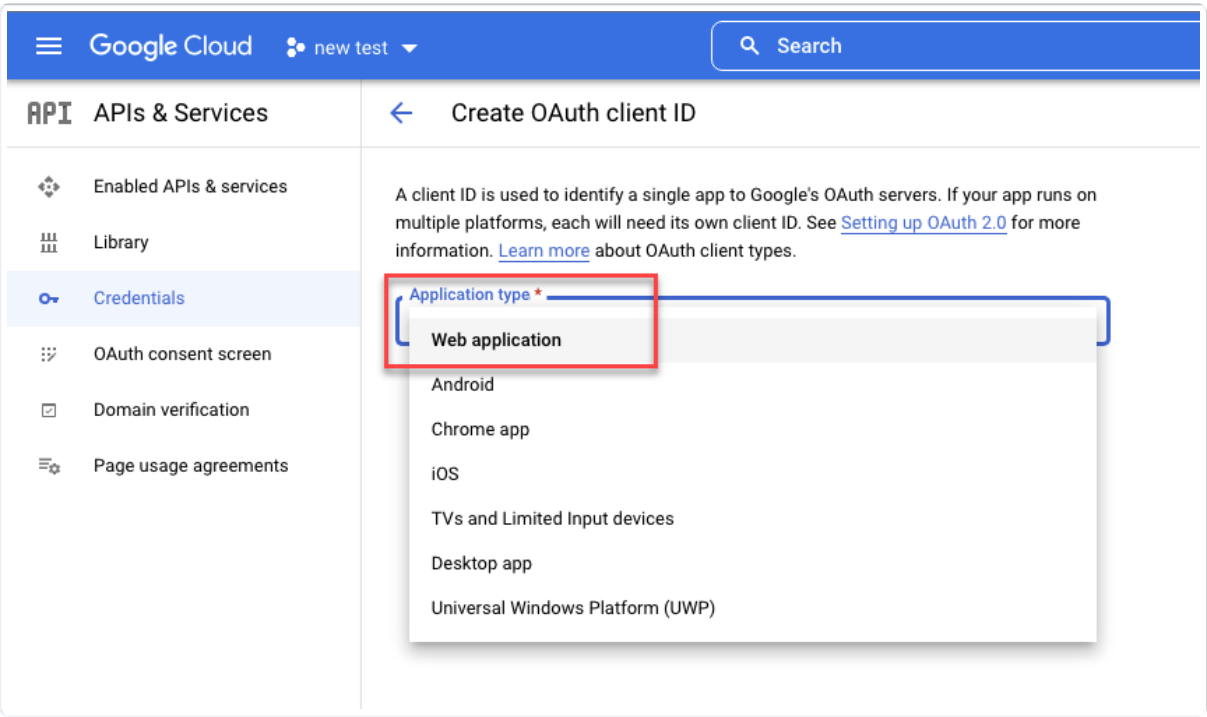




8. Go to **APIs & Services > Credentials**.
9. Click **+ CREATE CREDENTIALS** and select **OAuth client ID**.

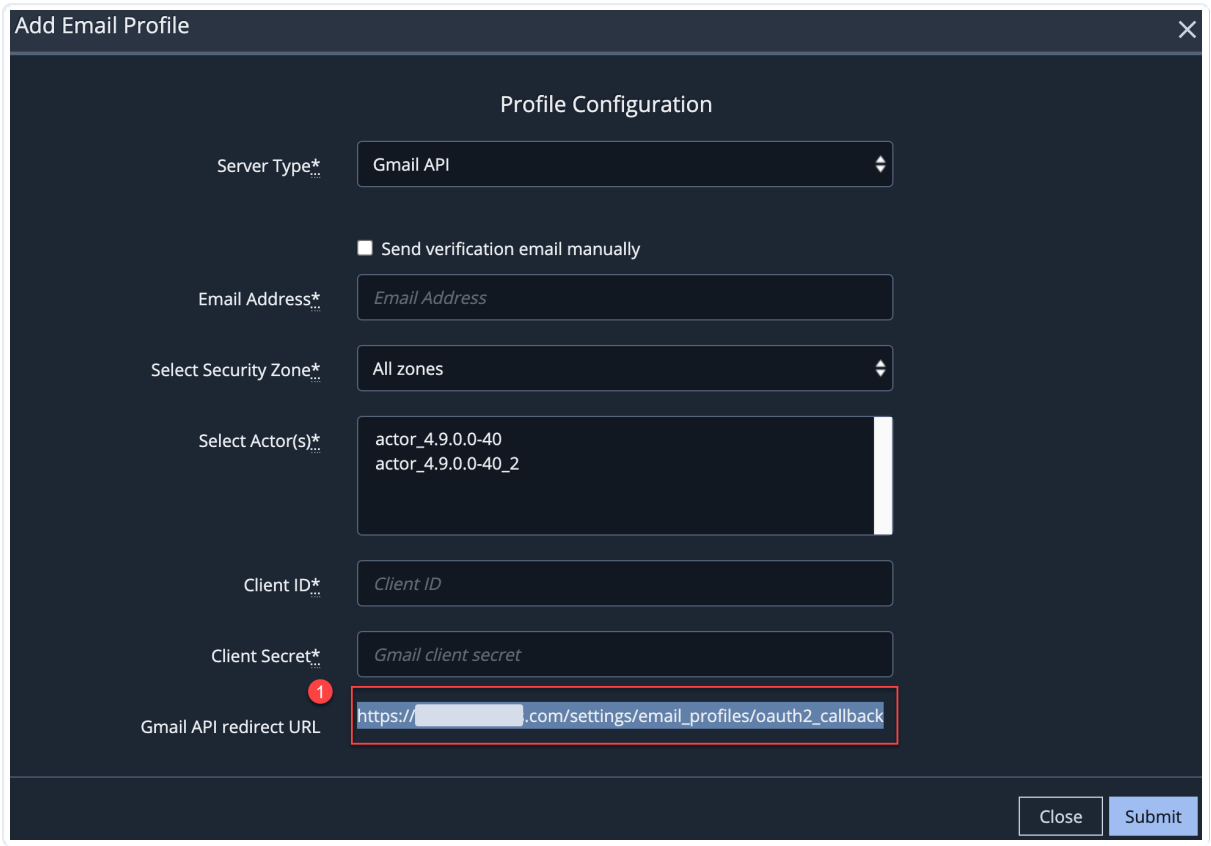


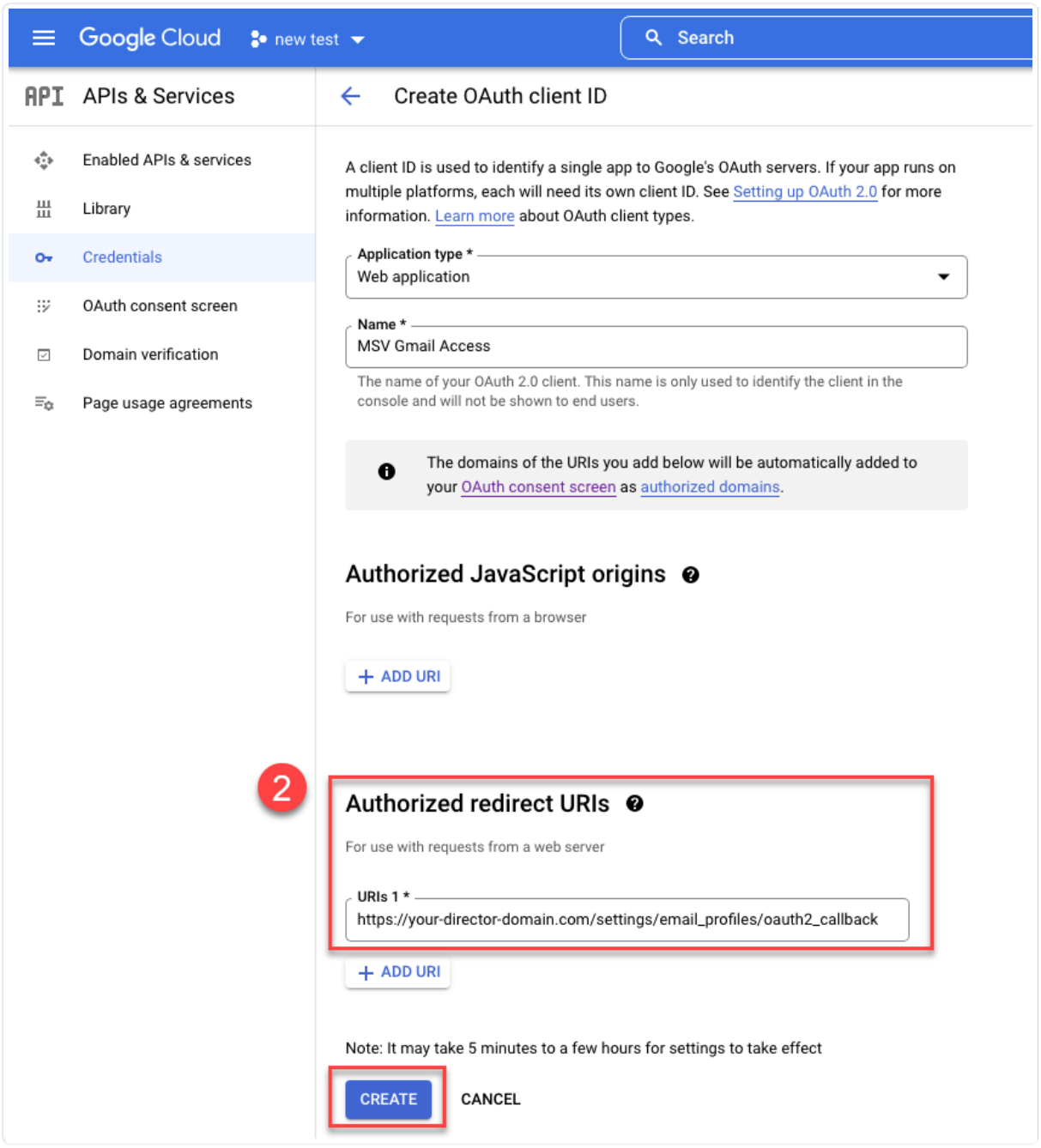
10. For Application type, select **Web application** and enter **Name**.



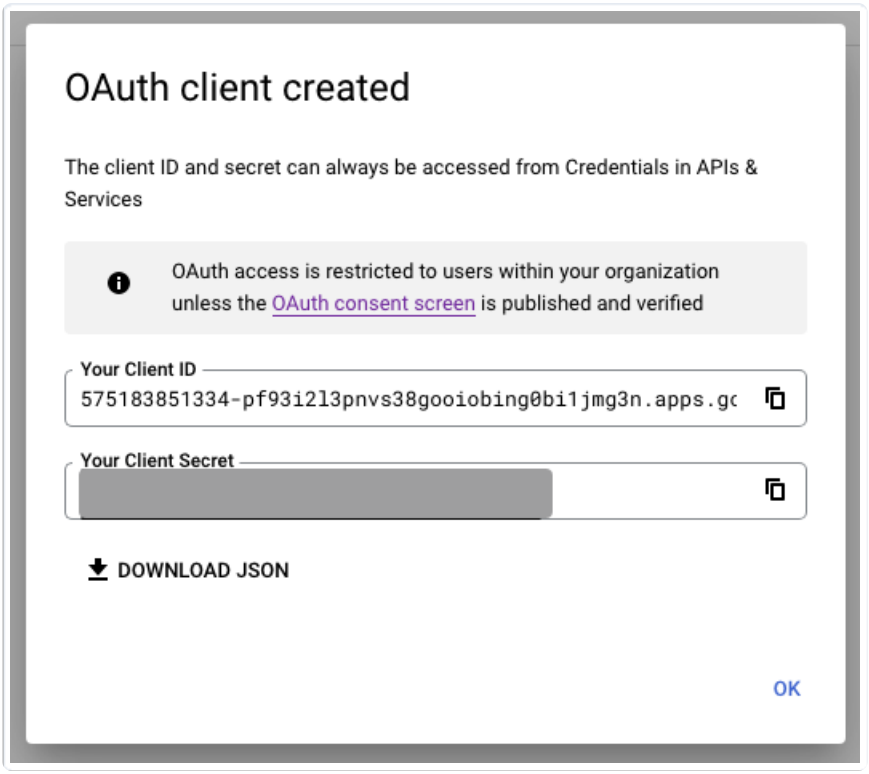
11. Enter the MSV Director address under **Authorized redirect URIs** and click **Create.**

> 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)**.





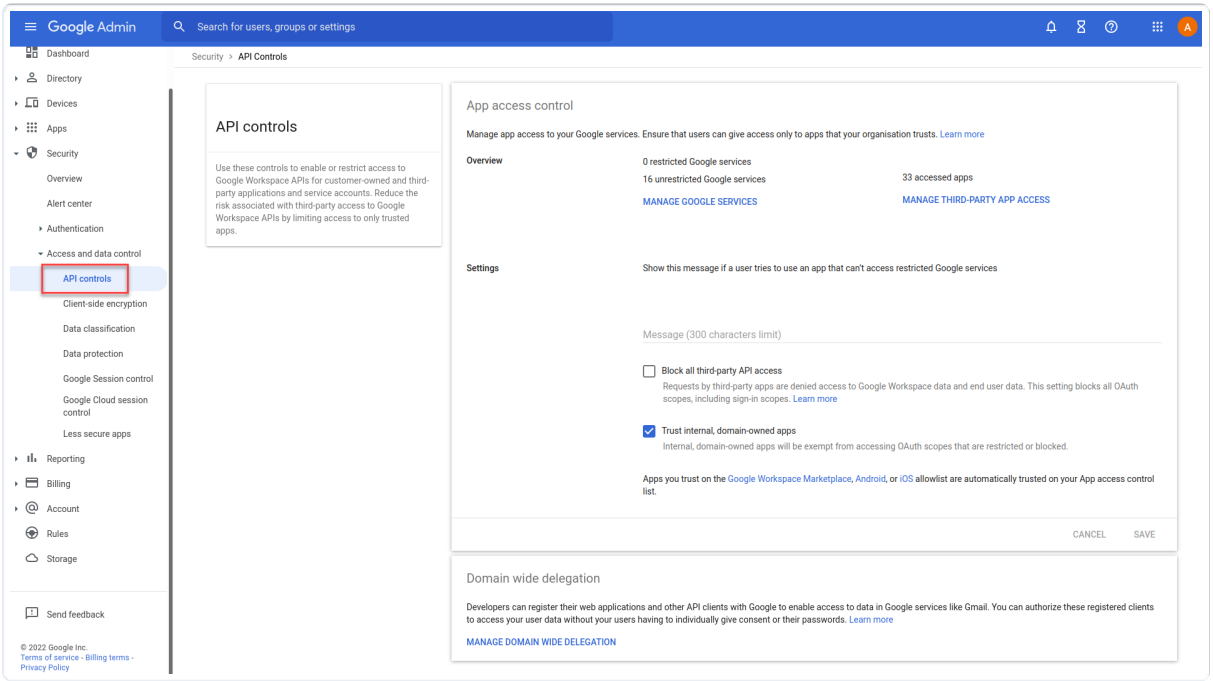
12. Retain the resulting **Client ID** and **Client Secret** for use in the steps below.



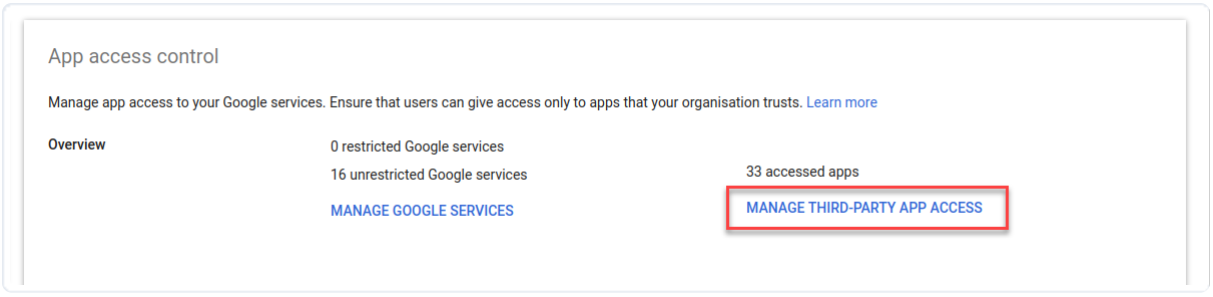
Grant Client ID Access To All Google Services

You must be a superadmin to complete these steps.

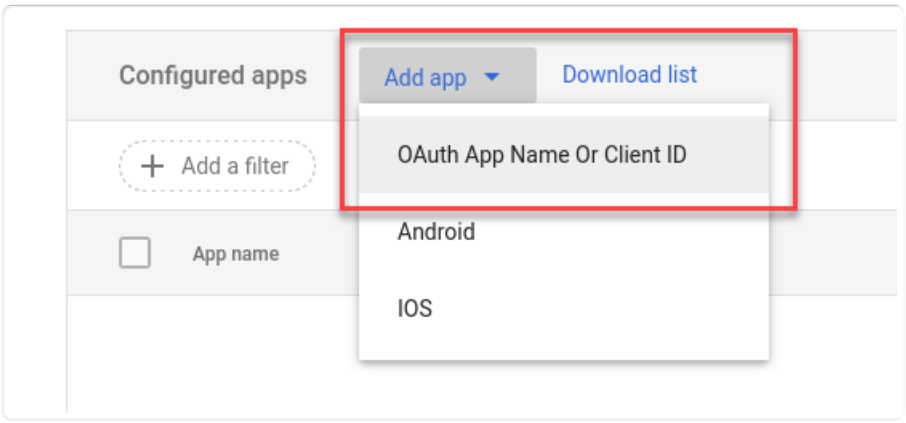
1. Log in to the Google Admin console and navigate to **Security > Access and data control > API controls** .



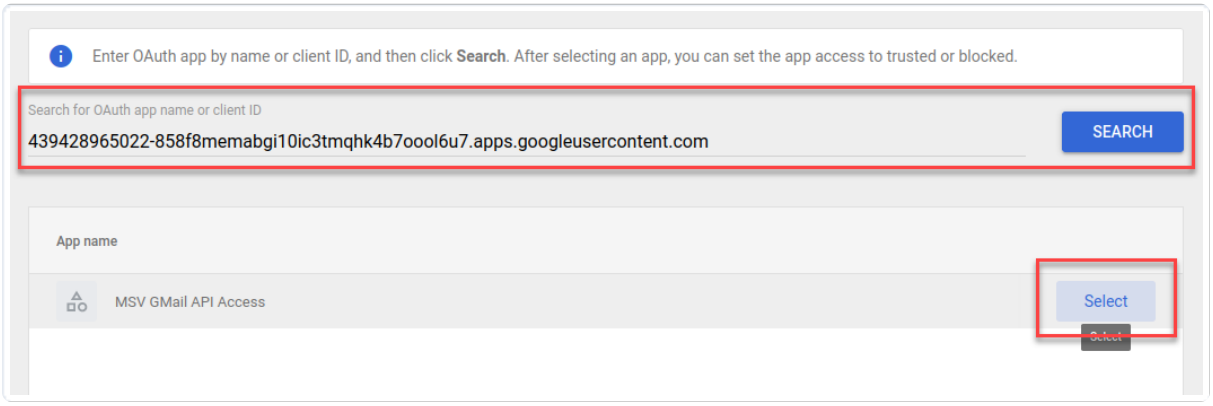
2. Click **MANAGE THIRD-PARTY APP ACCESS** .



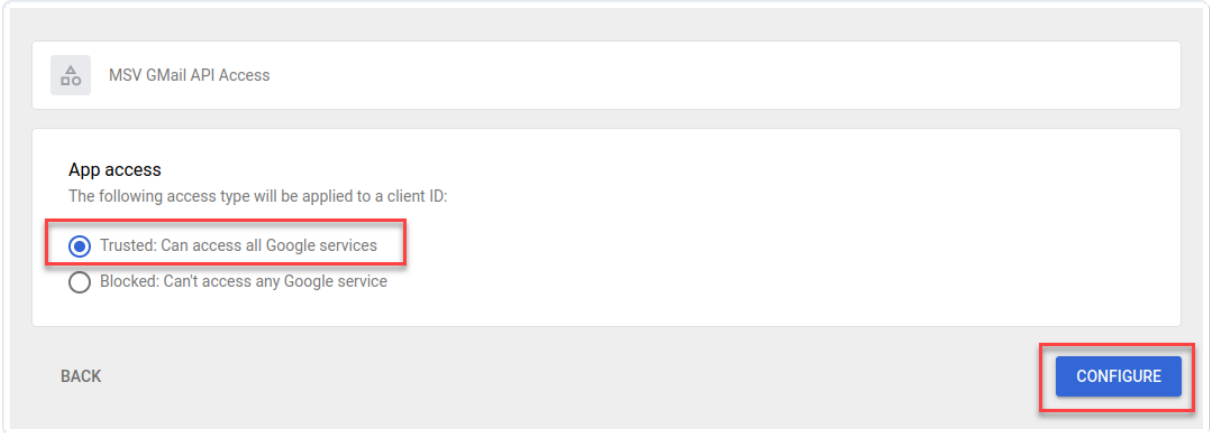
3. Under **Configured apps**, click **Add app** and select **OAuth App Name Or Client ID**.



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

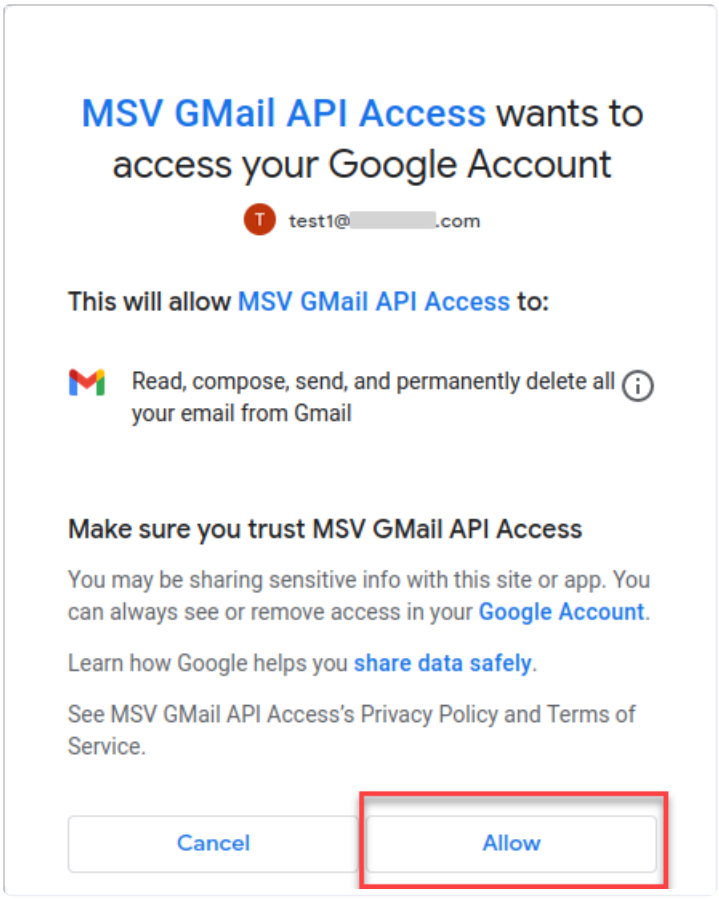


5. Select **Trusted: Can access all Google services** and click **Configure**.



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).

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).