



Using OAuth2 Authentication with SmtplibClient

Bruce Armstrong, Integrated Data Services
October 2026

DISCLAIMER

This presentation was authored by volunteer(s) in the Appeon community. This is not a work for hire by Appeon. The views and opinions expressed in this presentation are those of the author(s).

Its contents are protected by US copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of Appeon. All rights belong to their respective owners.

Any reference to third-party materials, including but not limited to Websites, content, services, or software, has not been reviewed or endorsed by Appeon. YOUR USE OF THIRD-PARTY MATERIALS SHALL BE AT YOUR OWN RISK.

Appeon makes no warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Appeon assumes no responsibility for errors or omissions.

Session Agenda

- Authentication vs Authorization
- Why use OAuth2 for SMTP Authentication
- OAuth2 Flows
 - Authorization Flow
 - Device Authorization Flow
- Configuring Azure
- Configuring Gmail
- Sample Code

Presenter Profile



Bruce Armstrong



<https://www.linkedin.com/in/brucearmstrong/>

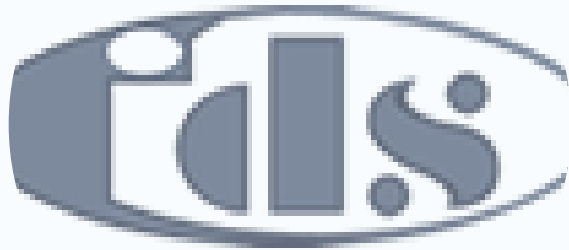
Key Skills

- PowerBuilder
- Oracle PL/SQL
- Java
- SonarQube
- C#
- C++
- AI
 - Claude Code
 - Codex
- Qlik Sense
- HTML5/JavaScript/TypeScript/Angular

Recent Projects

- [OpenSourcePFCLibraries](#) - The open-source PowerBuilder Foundation Class libraries

Company Profile



Integrated Data Services

- IDS has delivered innovative program and financial management information system solutions to the Federal Government for nearly three decades. Our flagship Enterprise Requirements Management product, CCaR™ is used by the DoD and Federal Agencies including the Air Force, Space Force, Army, Navy, USSOCOM, DSCA, DHA, JSF and DOE.

Authentication vs Authorization

- OAuth2 is an Authorization rather than an Authentication framework.
- OAuth2 relies on the identity server to perform authentication before it issues an Auth Token
- Open ID Connect (OIDC) is a protocol built on top of OAuth2 that does provide for both Authentication and Authorization

Why use OAuth2 for SMTP authentication?

- Secures your credentials
- Allows you to limit the privileges granted
- Multifactor Authentication (MFA) is often built in

OAuth 2.0 Flows

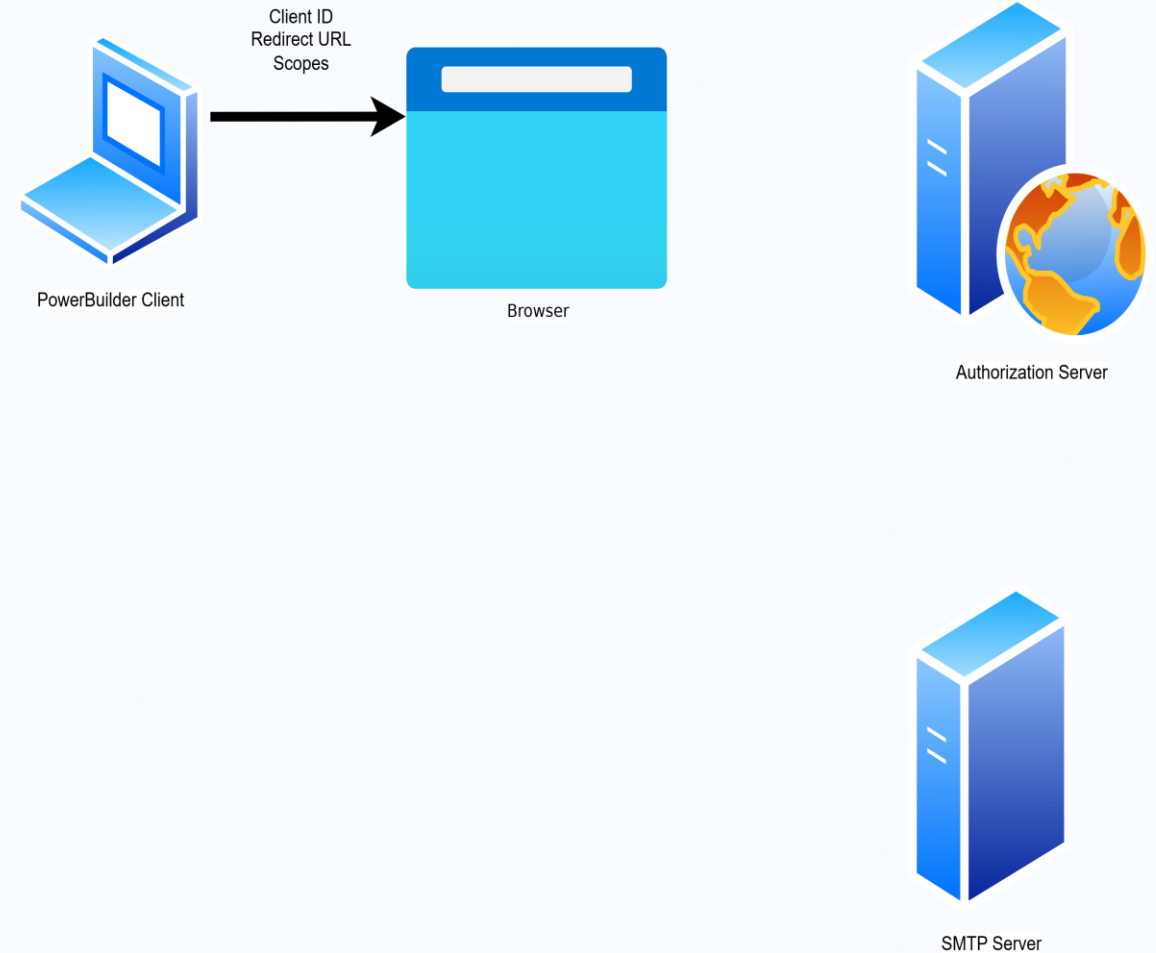
- Authorization Flow
 - The authorization server returns a single use authorization code to the client, which is then exchanged for an access token.
 - Optionally use Proof Key for Client Exchange (PKCE) for increased security
- Implicit Grant (deprecated in OAuth 2.1)
 - The access token is returned directly to the client
- Resource Owner Credentials Grant Type (deprecated in OAuth 2.1)
 - The client first obtains the resource owners credentials and then passes them to the authorization server.
 - Only applicable for highly trusted clients
- Client Credentials Grant Type
 - Used for non-interactive clients
- Device Authorization Flow
 - Used for client that have limited input options (e.g., Smart TVs)
- Refresh Token Grant
 - Used to refresh an access token that is about to expire

OAuth 2.0 Flows

- Authorization Flow
 - Used primarily by web applications as it is natural for them to be able to listen for a redirect URI
- Device Authorization Flow
 - Can be more useful for desktop apps because it doesn't require listening for a redirect URI
- Client Credential Flow
 - Used for service accounts, but requires a redirect URI like Authorization Flow
- Refresh Token Flow
 - Regardless of how the Auth Token was originally obtained the Refresh Token Flow is how the application can refresh an existing token
 - If the Auth Token can be refreshed, the user isn't forced to reauthorize a new Auth Token when the original Auth Token would have expired

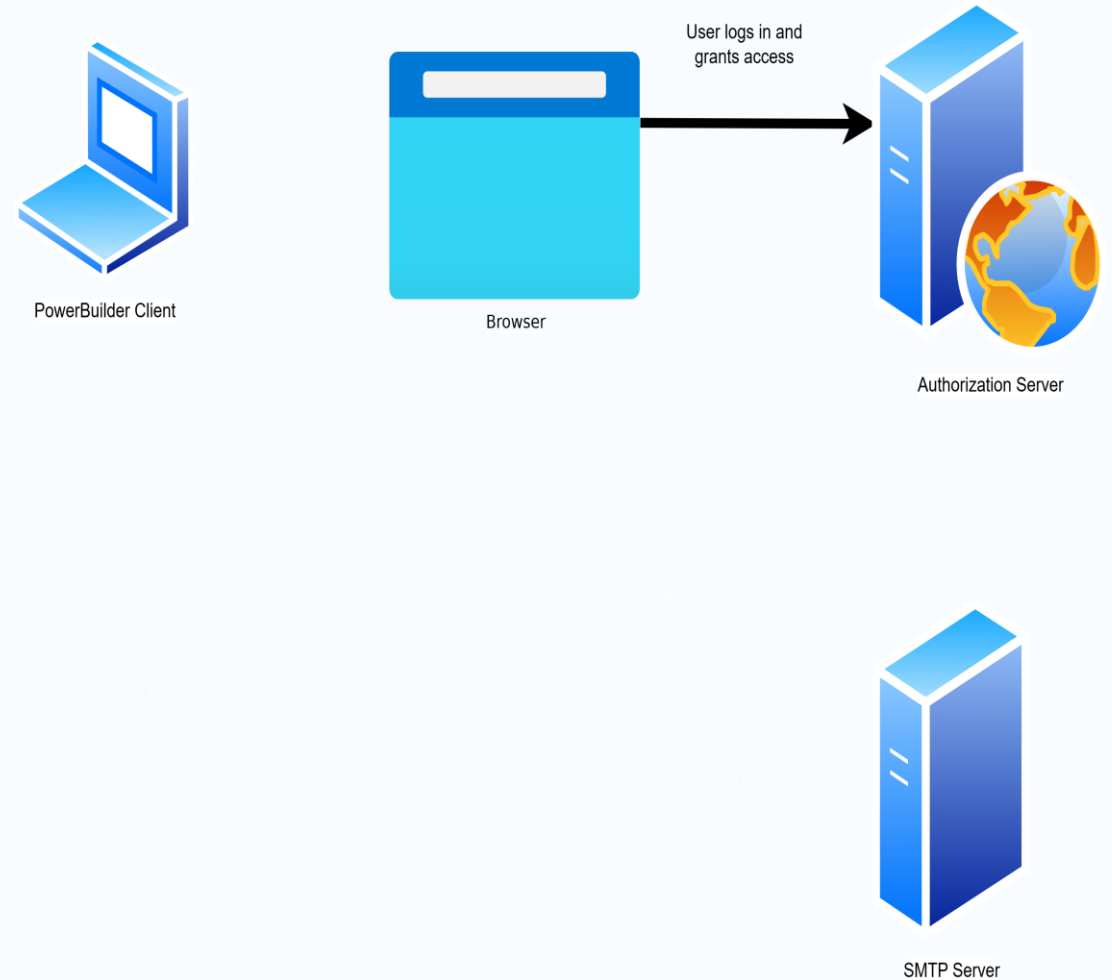
Authorization Flow

- Client composes URL to access the Authentication server that includes:
 - Client ID (and Tennant ID for Azure)
 - Requested Scopes
 - Redirect URI
- Client launches default web browser to the URL
 - Normally this would be done with system browser
 - In the demo, we're going to use a browser control in a PowerBuilder window so we can capture the Redirect URL call



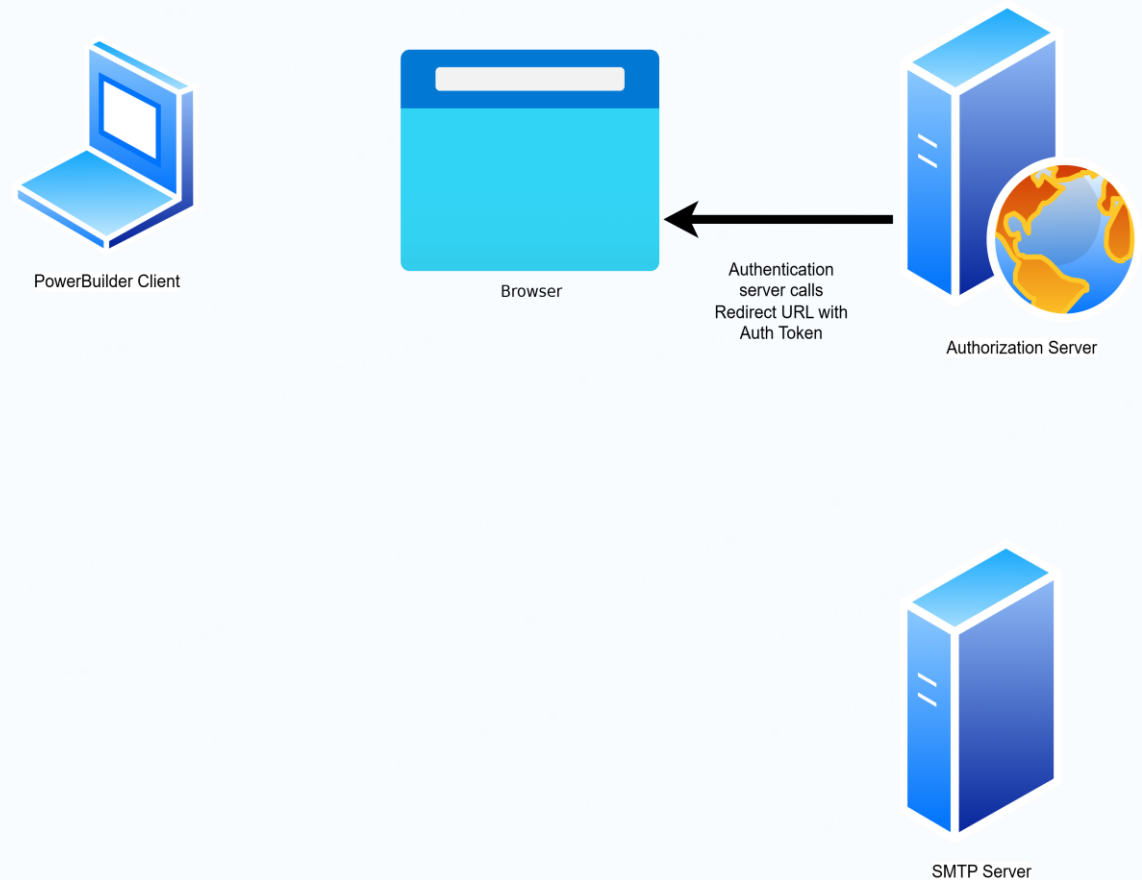
Authorization Flow

- User logs in via web browser and grants access



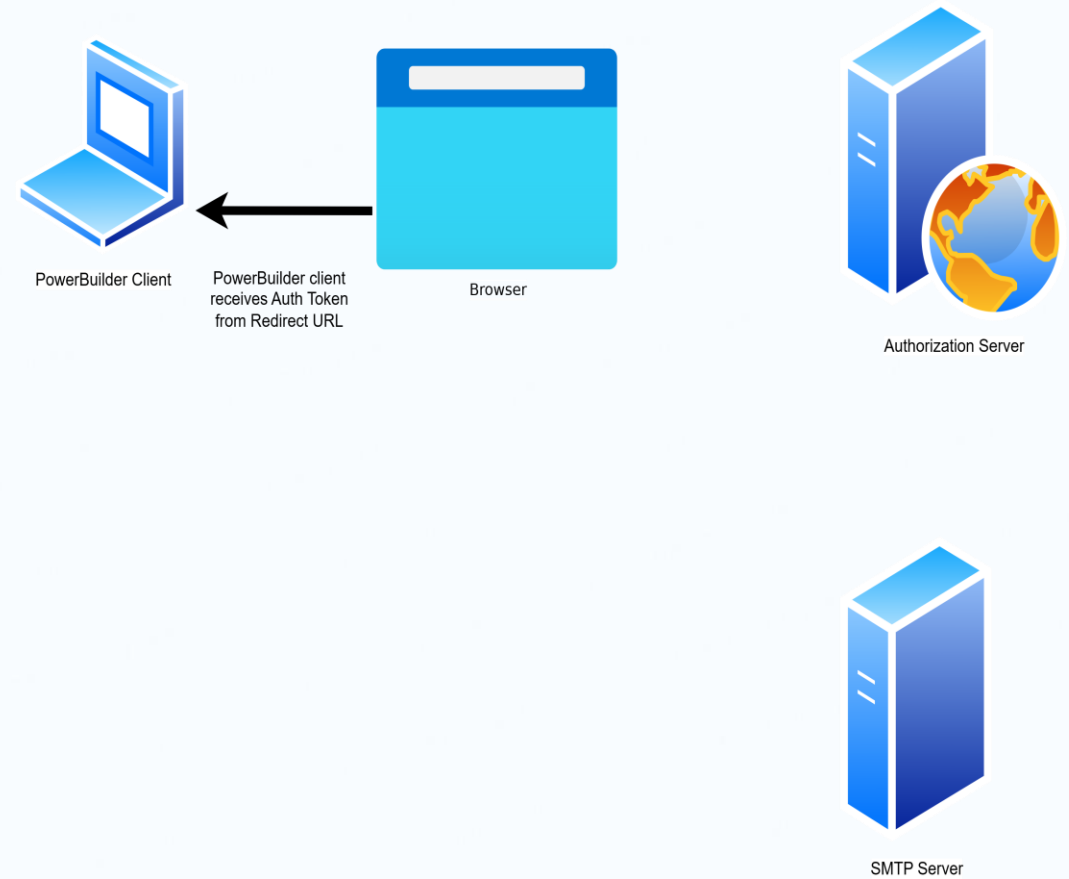
Authorization Flow

- Authentication Server adds Auth Token to Redirect URL and passes it back to browser as Redirect URL
- The best way to capture this would be to have the PowerBuilder client listen on a port using something like [WinsockPBNl](#) or [Winsock](#)
- For the demo, we're capturing the redirect sent back to the browser control in a PowerBuilder window



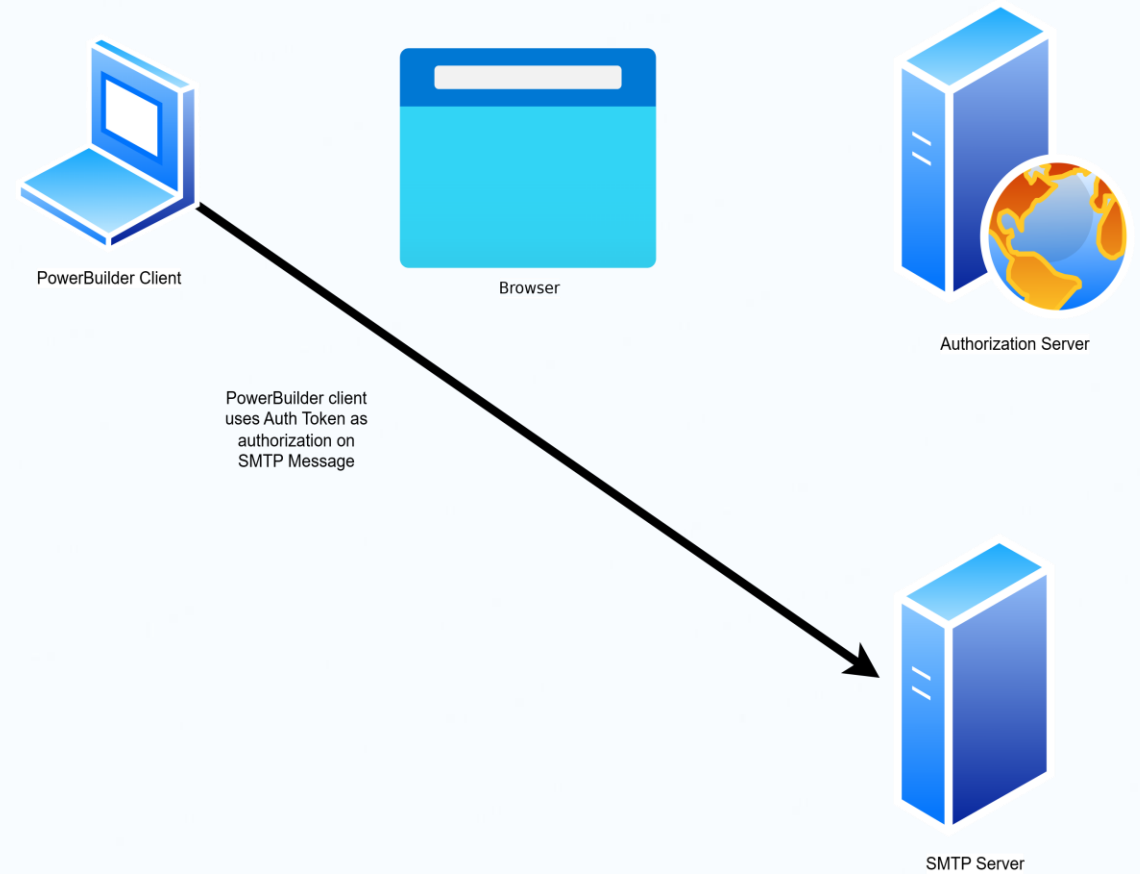
Authorization Flow

- PowerBuilder client extracts the Auth Token from the Redirect URL



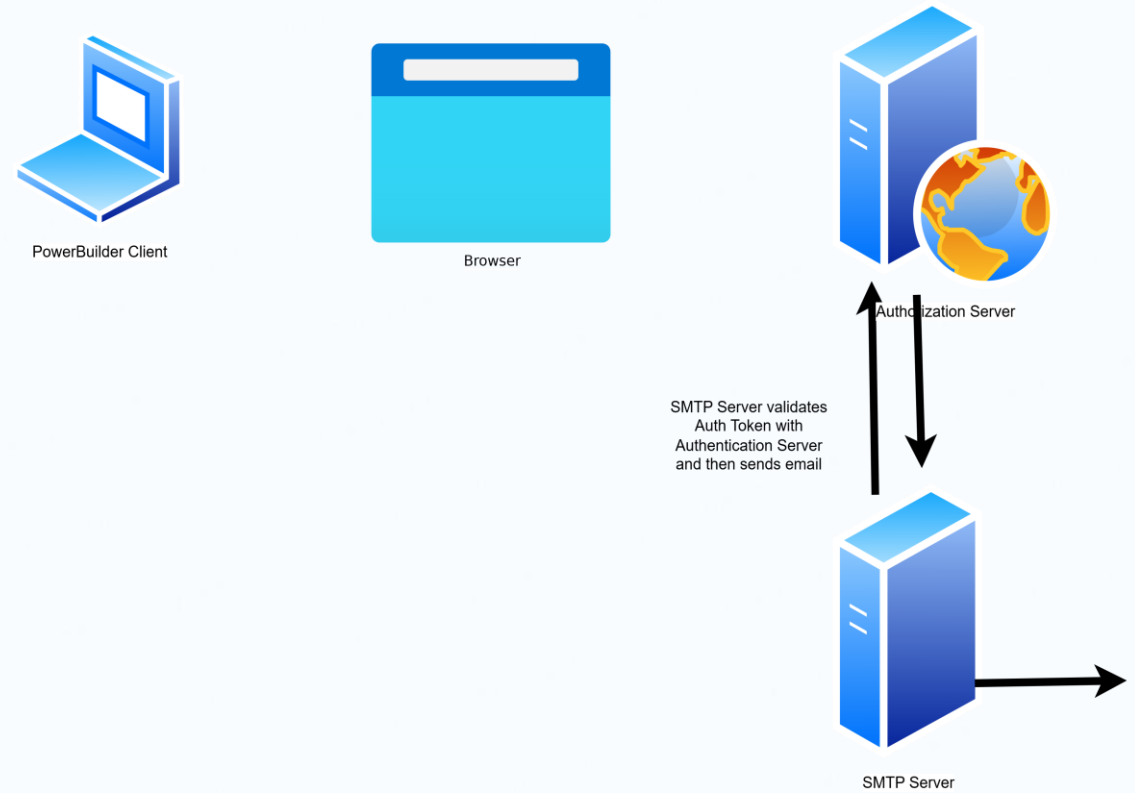
Authorization Flow

- PowerBuilder adds Auth Token to SMTP Message for Authentication



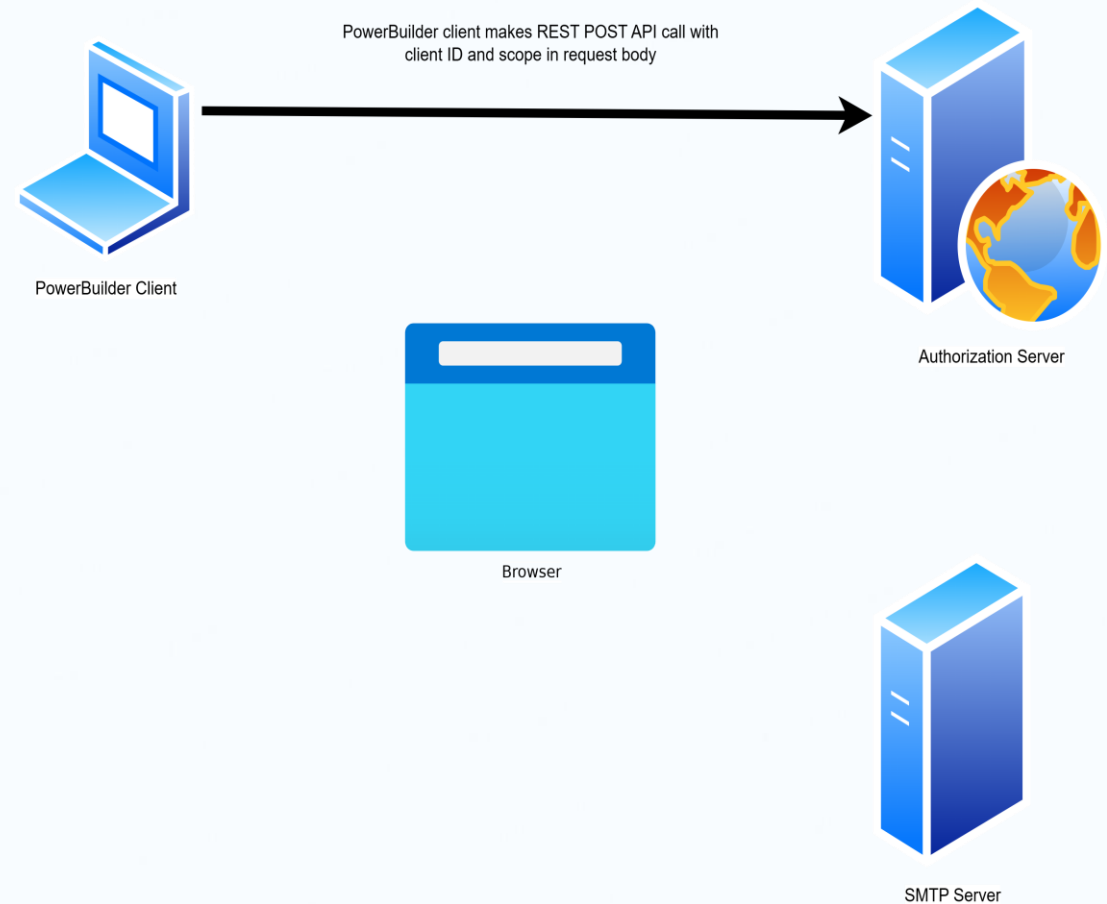
Authorization Flow

- SMTP Server verifies Auth Token and, if valid, sends email



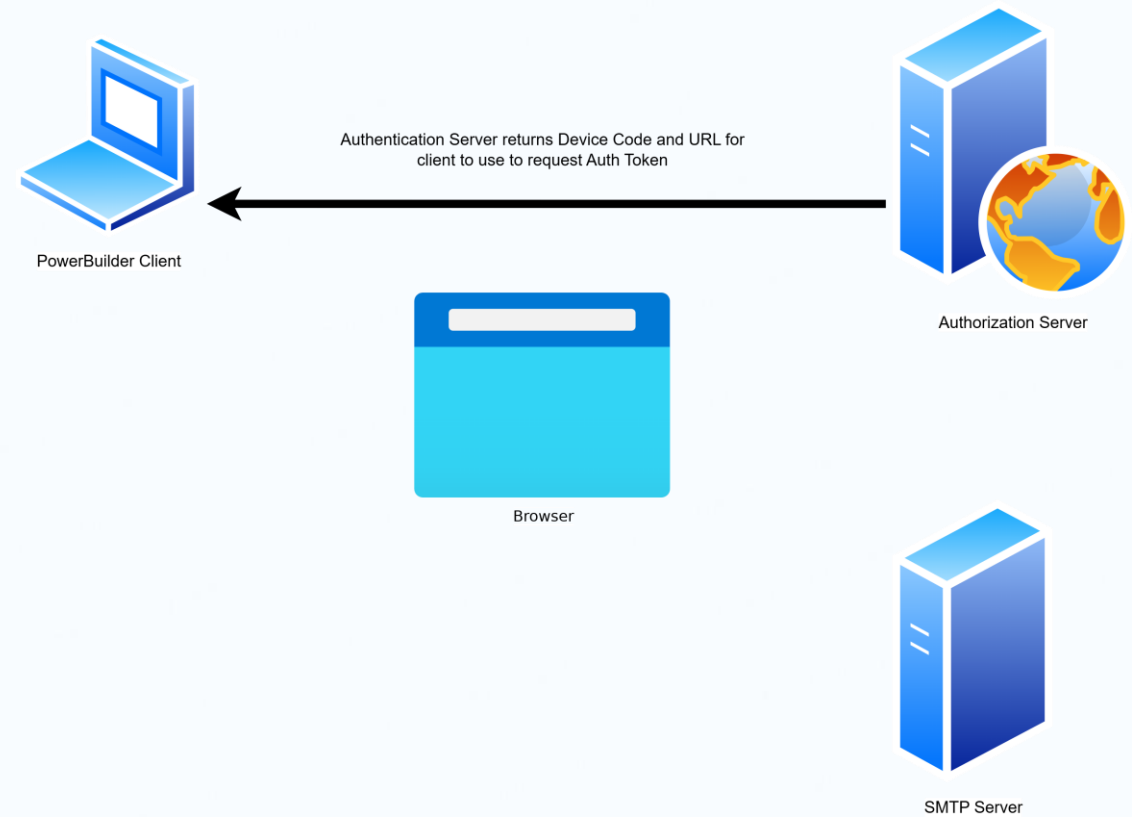
Device Authorization Flow

- PowerBuilder client makes REST POST API call to Authorization Server
- For Azure, Tenant ID is part of API URL
- Client ID and requested scopes are passed in request body



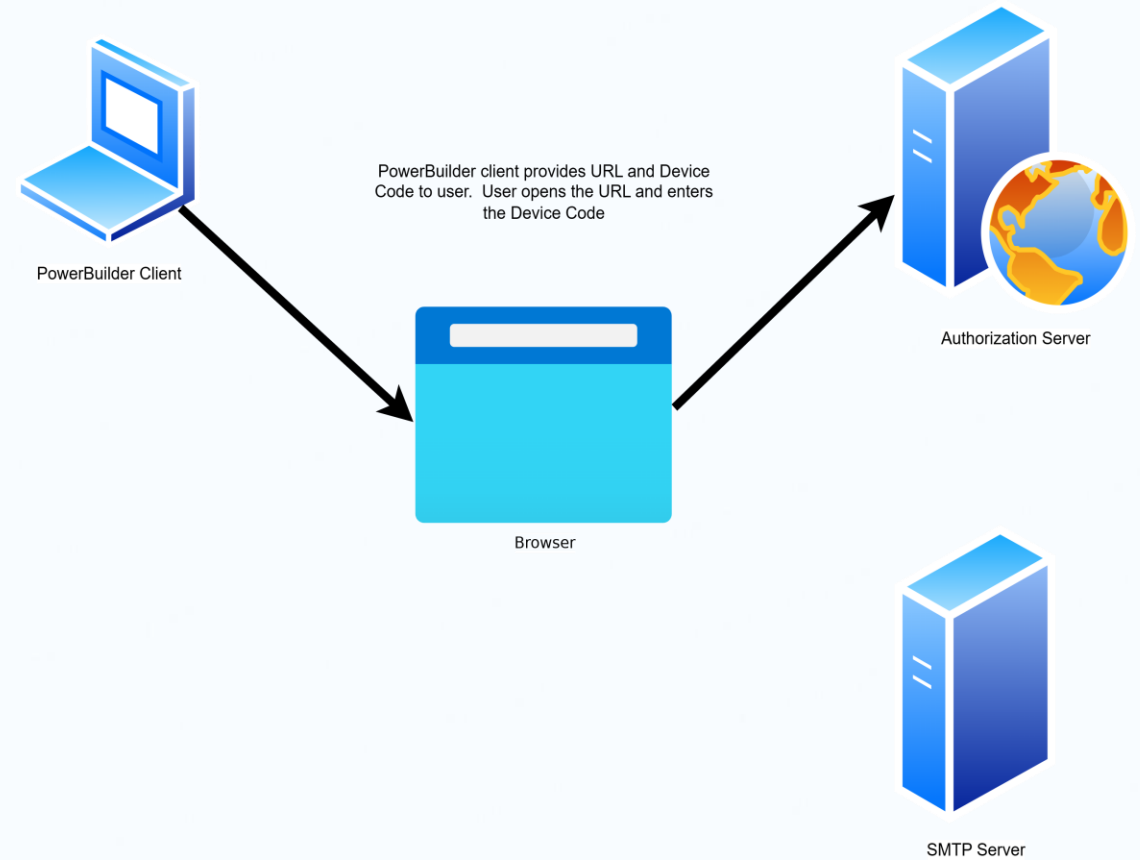
Device Authorization Flow

- Authorization Server returns:
 - Device Code
 - A URL to be used to exchange Device Code for Auth Token
- Typically, the client would generate a QR code for the URL and display that and the Device Code to the user
- The user would use the QR code to open the URL on their personal device and enter the Device Code
- For the demo, we will be opening the system browser to the URL and copying the Device Code into the clipboard



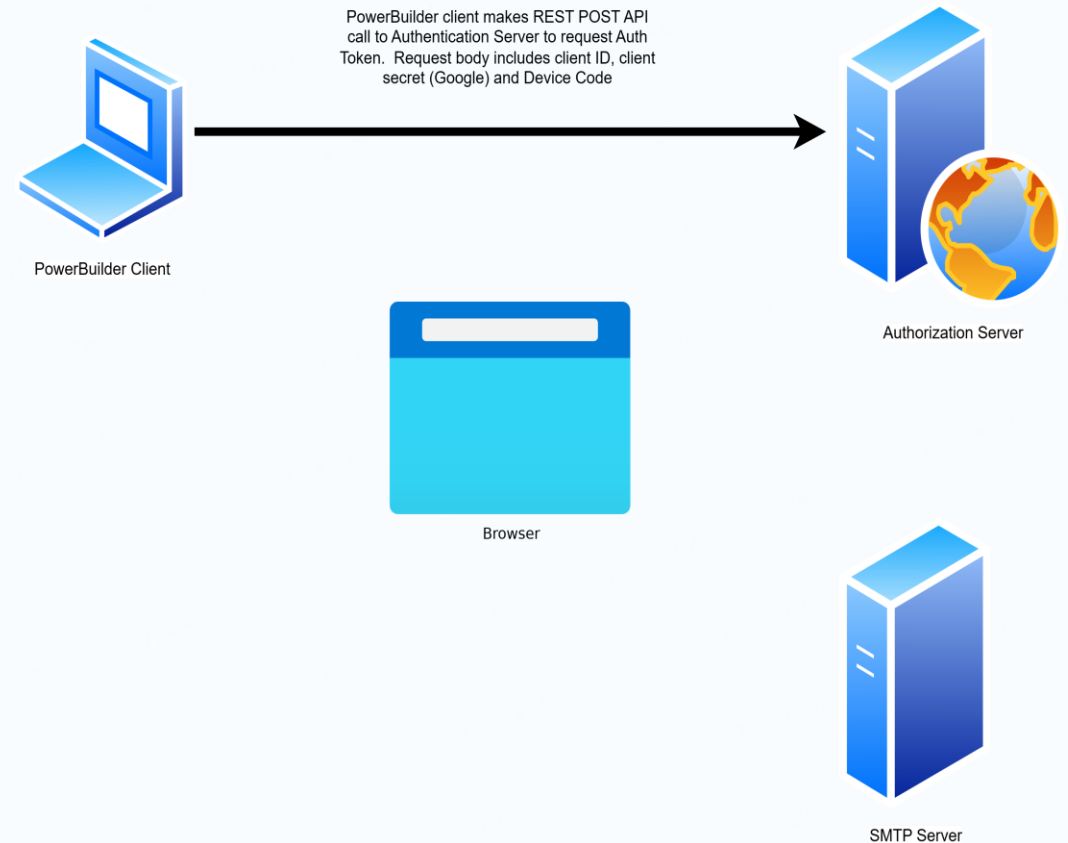
Device Authorization Flow

- User enters the Device Code into the web page and grants access
- Device code is received by the Authentication Server, which then makes the Auth Token available on a known URL



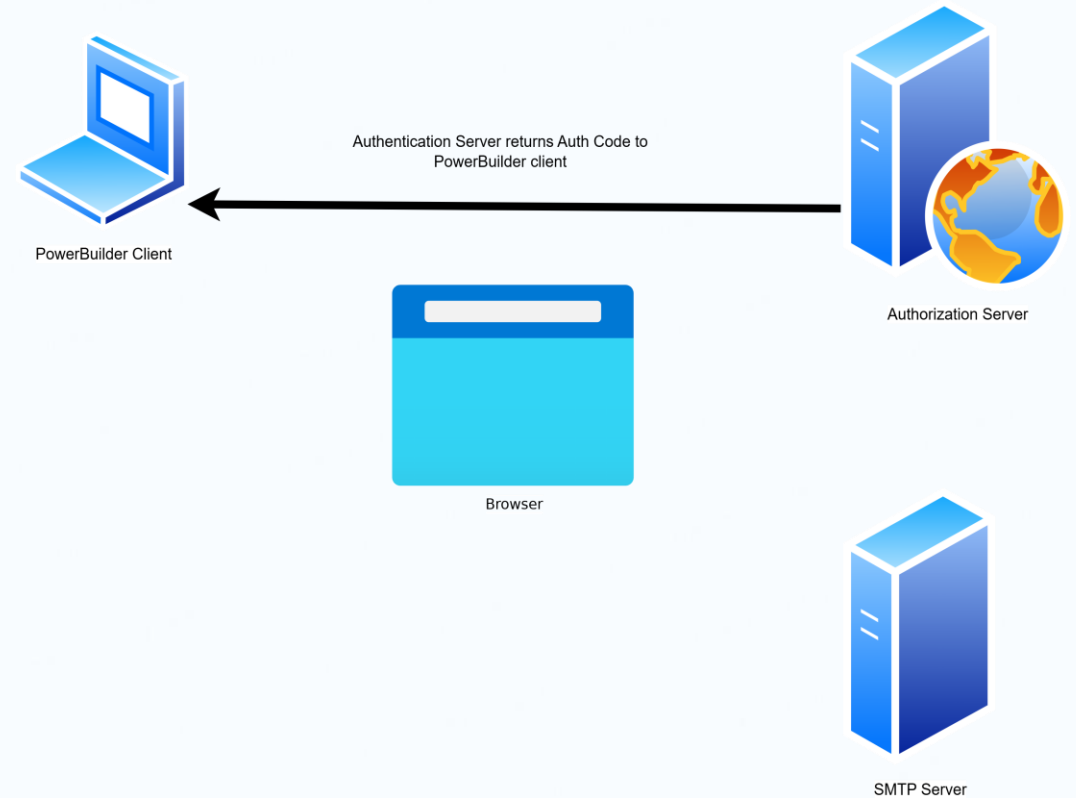
Device Authorization Flow

- PowerBuilder client makes REST POST API call to Authorization Server
- For Azure, Tenant ID is part of API URL
- Client ID and Device Code are passed in request body
- For Google, Client Secret is also pass in request body



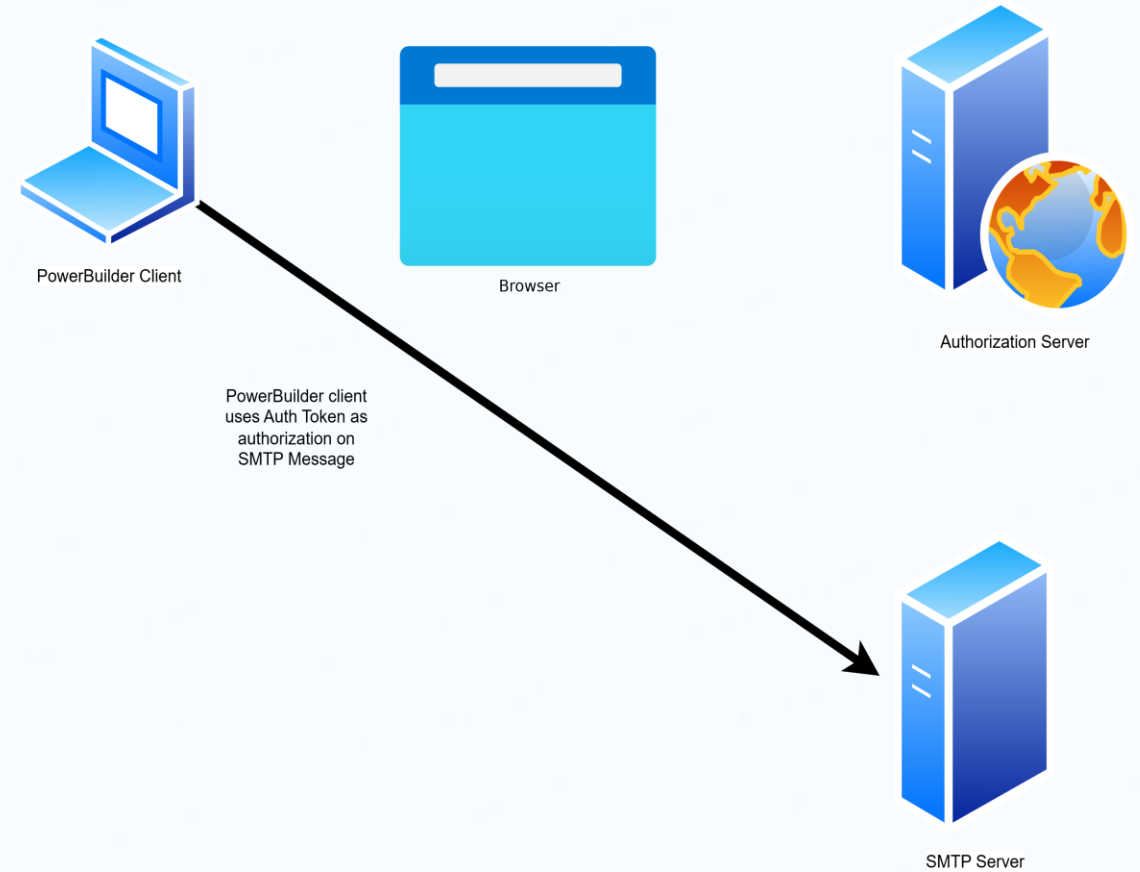
Device Authorization Flow

- Authentication Server returns Auth Token to PowerBuilder client in response to API call



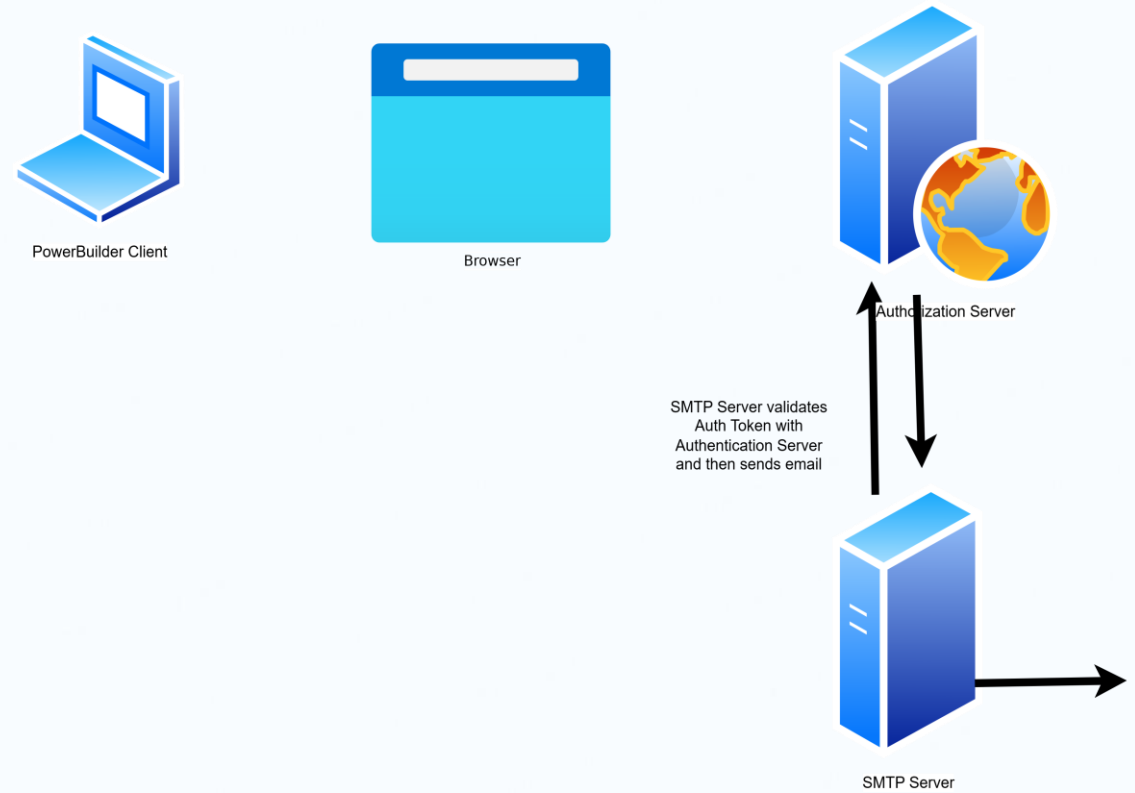
Device Authorization Flow

- PowerBuilder adds Auth Token to SMTP Message for Authentication



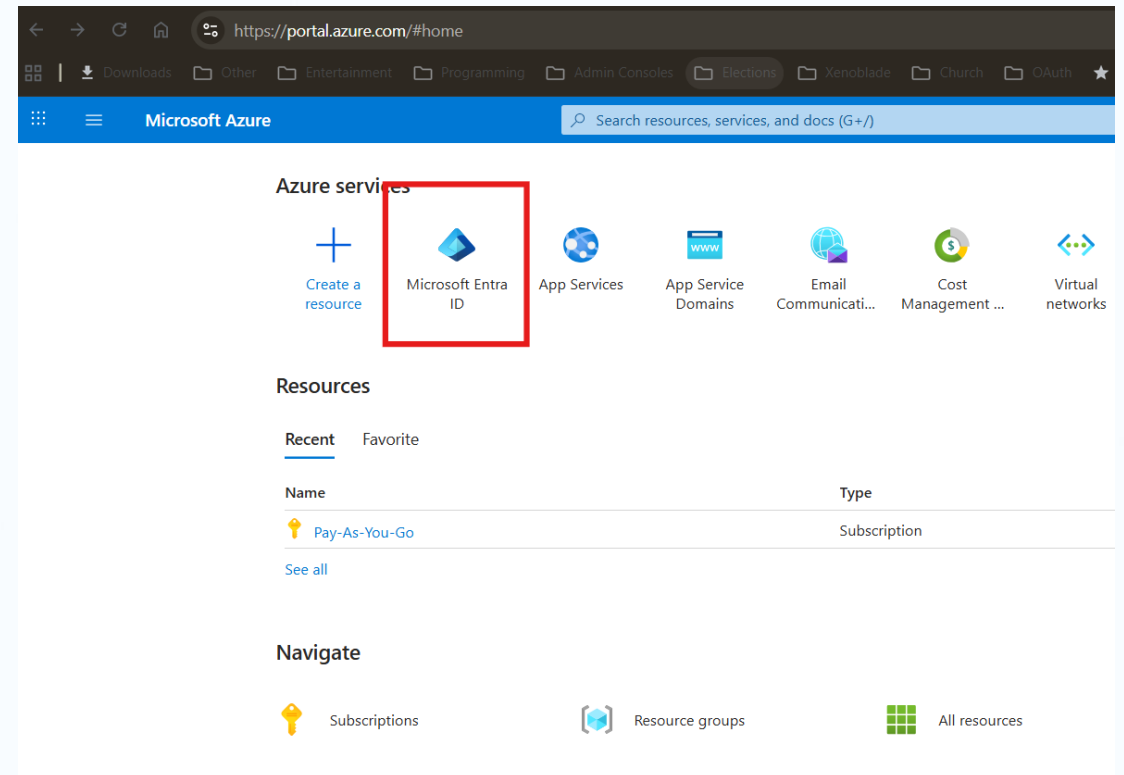
Device Authorization Flow

- SMTP Server verifies Auth Token and, if valid, sends email



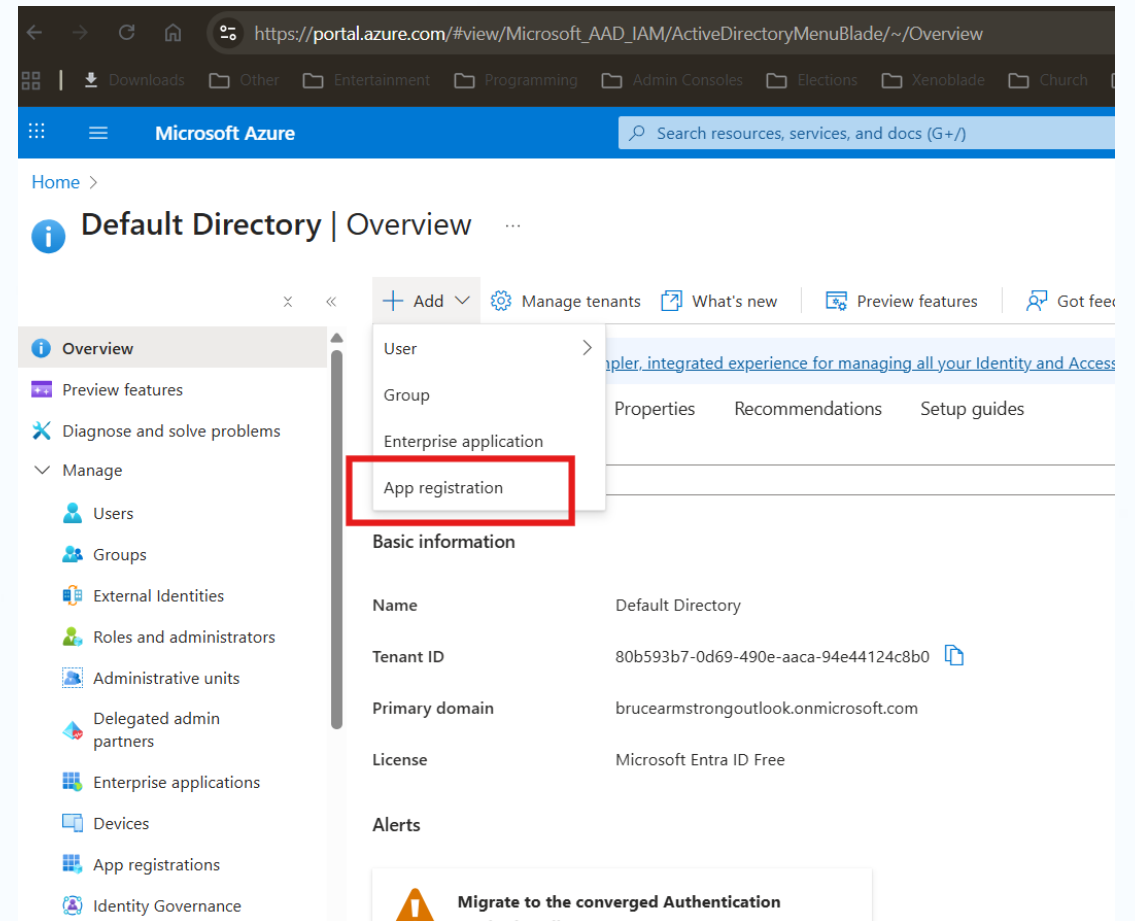
Azure

- In the Azure Portal, open Microsoft Entra ID



Azure

- Create a new App registration



Azure

- In the app registration, define which accounts can use the app and define the Redirect URL
- For Azure, we can use the same app registration for both flows

https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/CreateApplicationBlade/IsMSAApp~/false

Microsoft Azure

Home > Default Directory | Overview >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SMTP Demo ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web http://localhost:8090 ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

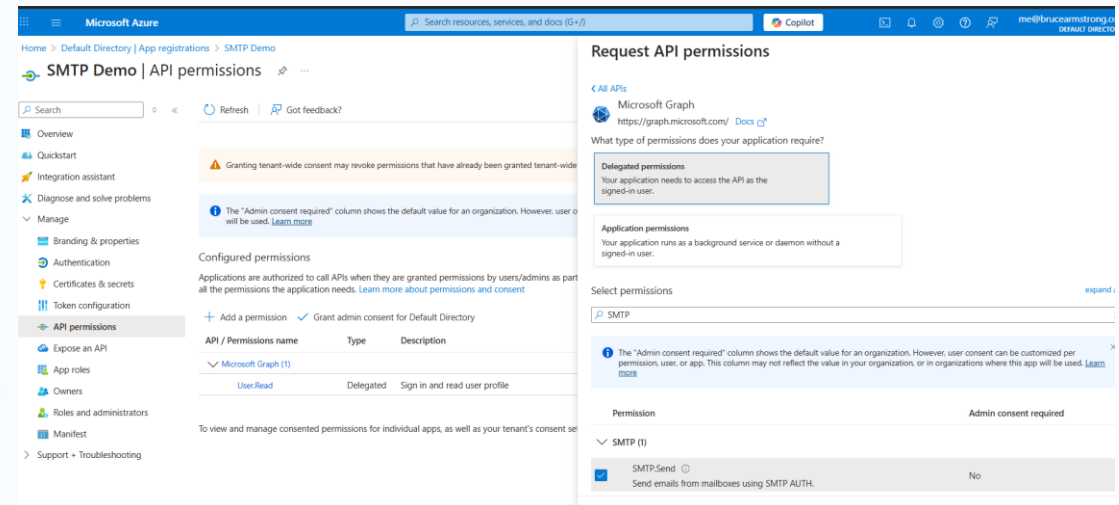
Azure

- Record the Tennant ID and Client ID for the app

The screenshot displays the Microsoft Azure portal interface for an application named 'SMTP Demo'. The left-hand navigation pane includes sections for 'Overview', 'Quickstart', 'Integration assistant', 'Diagnose and solve problems', and 'Manage'. The 'Manage' section is expanded, showing options like 'Branding & properties', 'Authentication', 'Certificates & secrets', 'Token configuration', 'API permissions', 'Expose an API', 'App roles', 'Owners', and 'Roles and administrators'. The main content area, under the 'Essentials' tab, shows the 'Application (client) ID' and 'Directory (tenant) ID' fields, both of which are redacted with '[redacted]'. To the right of these fields, there are links for 'Add a certificate or secret', '1 web, 0 spa, 0 public client', 'Add an Application ID URI', and 'SMTP Demo'. A notification banner at the bottom of the main content area states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)'. At the bottom right of the page, there is a call to action: 'Build your application with the Microsoft identity platform'.

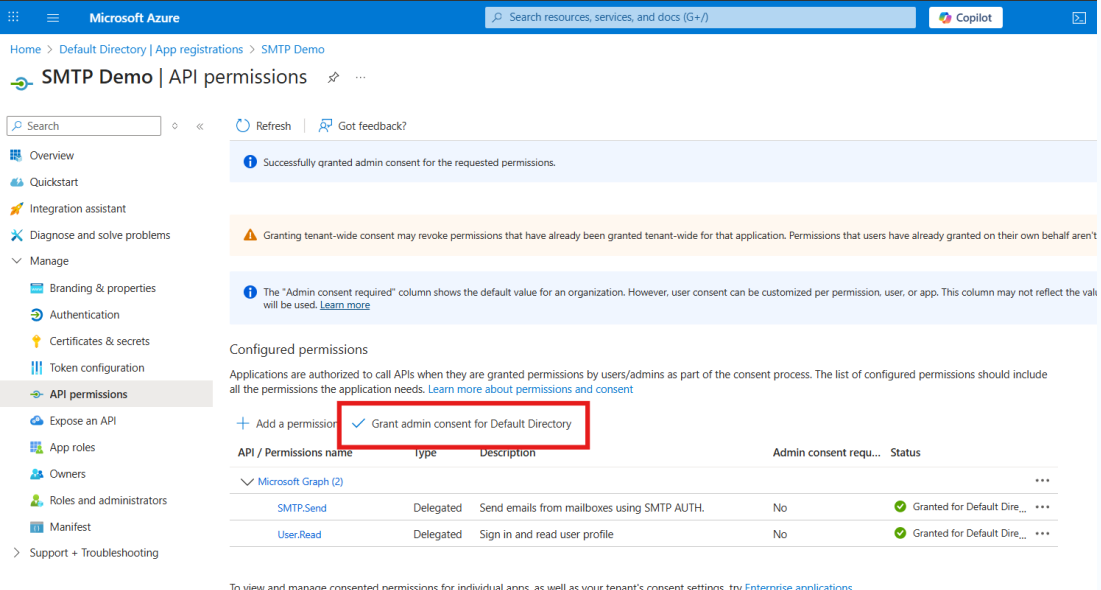
Azure

- Under Manage, select API Permissions
- Select Microsoft.Graph
- Select Delegated Permissions
- Search on “SMTP” and select the SMTP.Send scope



Azure

- Use the “Grant admin consent for Default Directory” option



Microsoft Azure

Home > Default Directory | App registrations > SMTP Demo

SMTP Demo | API permissions

Search resources, services, and docs (G+/)

Copilot

Search

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Successfully granted admin consent for the requested permissions.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value that will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for Default Directory

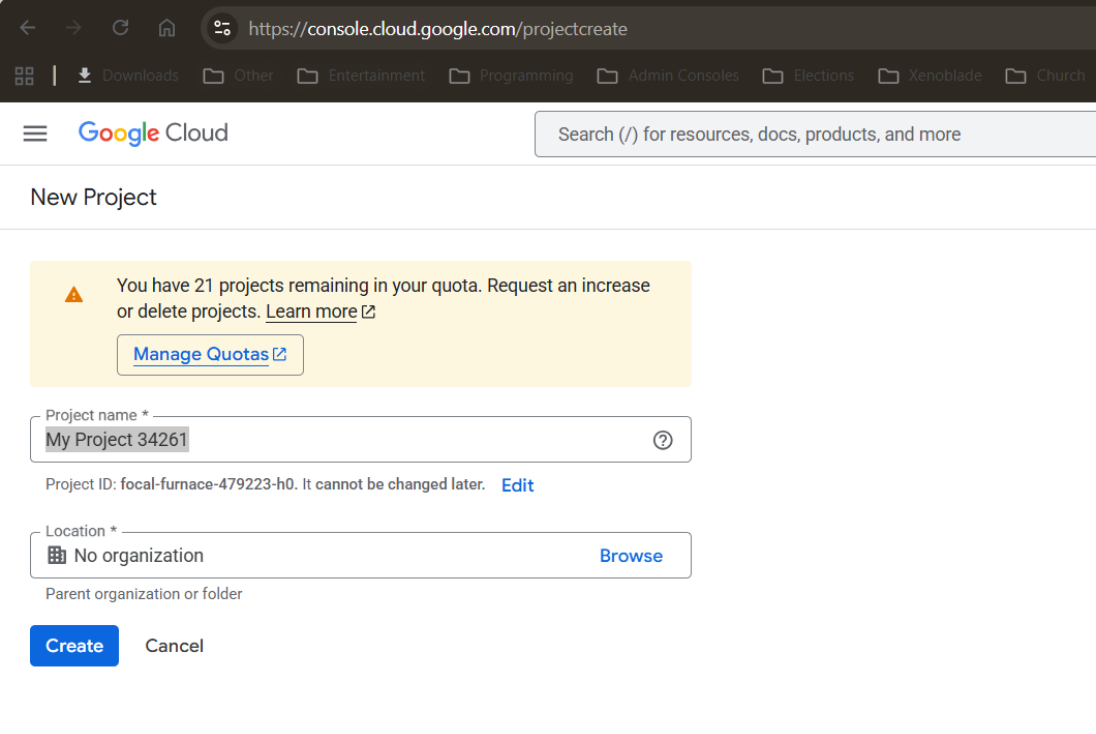
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
SMTP.Send	Delegated	Send emails from mailboxes using SMTP AUTH.	No	Granted for Default Dire...
User.Read	Delegated	Sign in and read user profile	No	Granted for Default Dire...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Gmail

- Create a project in Google Cloud

<https://console.cloud.google.com/projectcreate>



The screenshot shows the Google Cloud console's 'New Project' page. At the top, the browser address bar displays 'https://console.cloud.google.com/projectcreate'. Below the browser, the Google Cloud logo is on the left, and a search bar is on the right. The main heading is 'New Project'. A yellow warning box states: 'You have 21 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)'. Below this, there is a 'Project name *' field containing 'My Project 34261' and a help icon. Underneath, the 'Project ID' is shown as 'focal-furnace-479223-h0', with a note that it cannot be changed later and an 'Edit' link. The 'Location *' field shows 'No organization' with a 'Browse' link. At the bottom, there are 'Create' and 'Cancel' buttons.

https://console.cloud.google.com/projectcreate

Google Cloud

Search (/) for resources, docs, products, and more

New Project

 You have 21 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[Manage Quotas](#)

Project name *
My Project 34261

Project ID: focal-furnace-479223-h0. It cannot be changed later. [Edit](#)

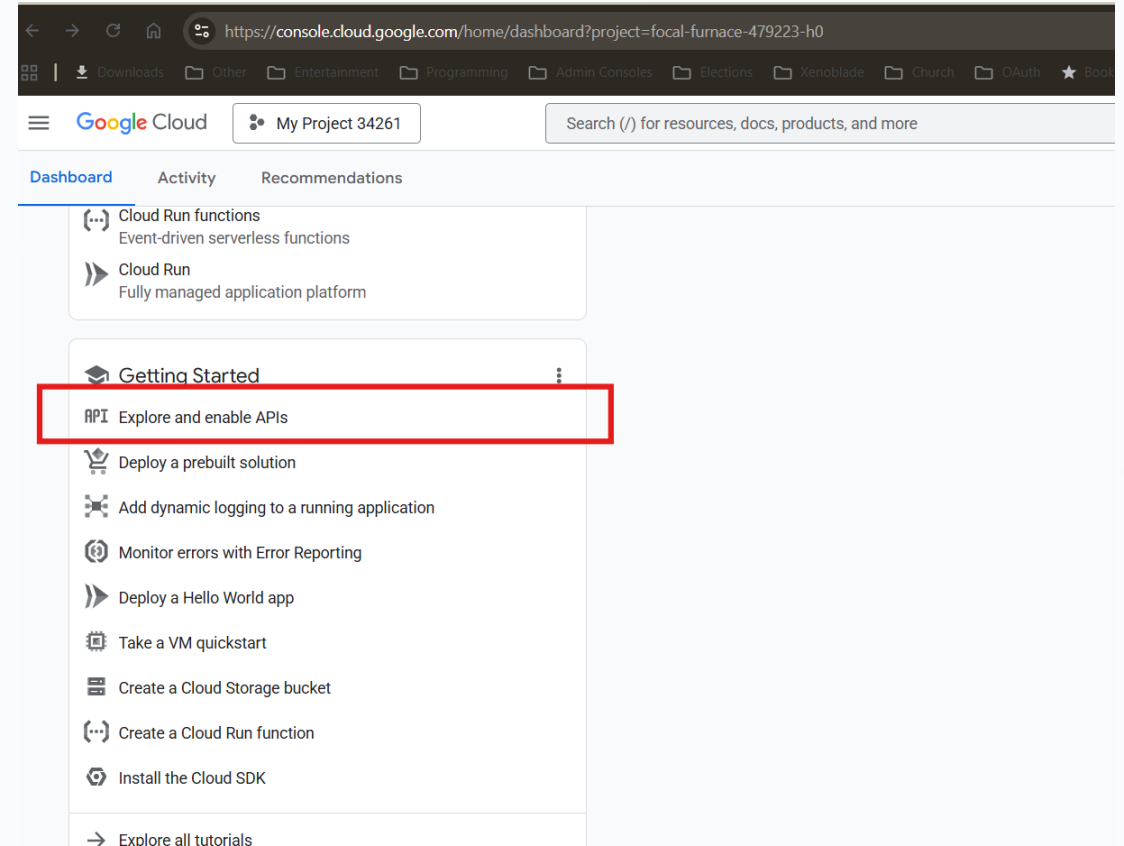
Location *
No organization [Browse](#)

Parent organization or folder

[Create](#) [Cancel](#)

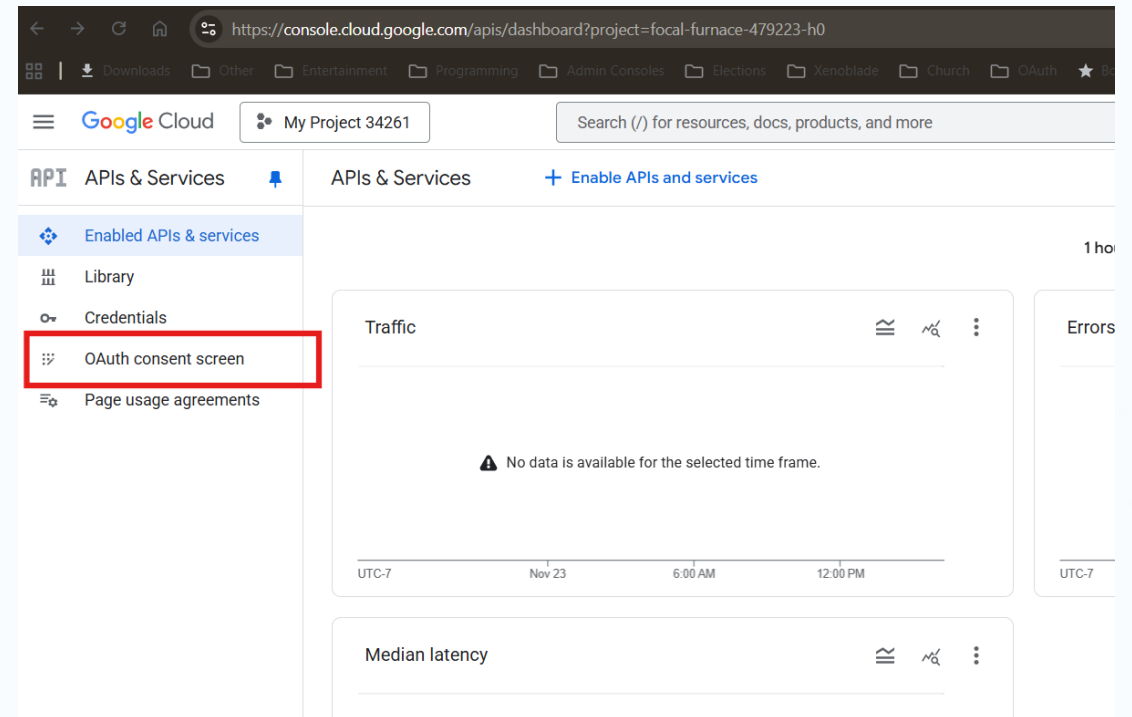
Gmail

- In the new project, select “Explore and enable APIs”



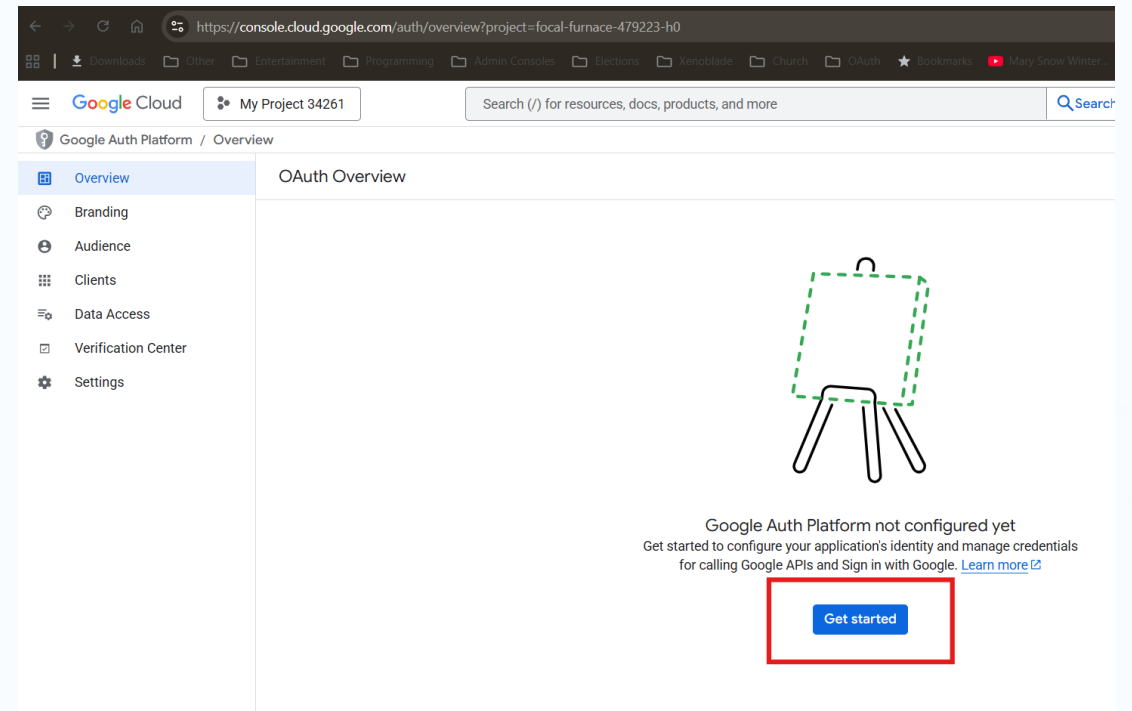
Gmail

- Select “Oauth consent screen”



Gmail

- Click on Get Started



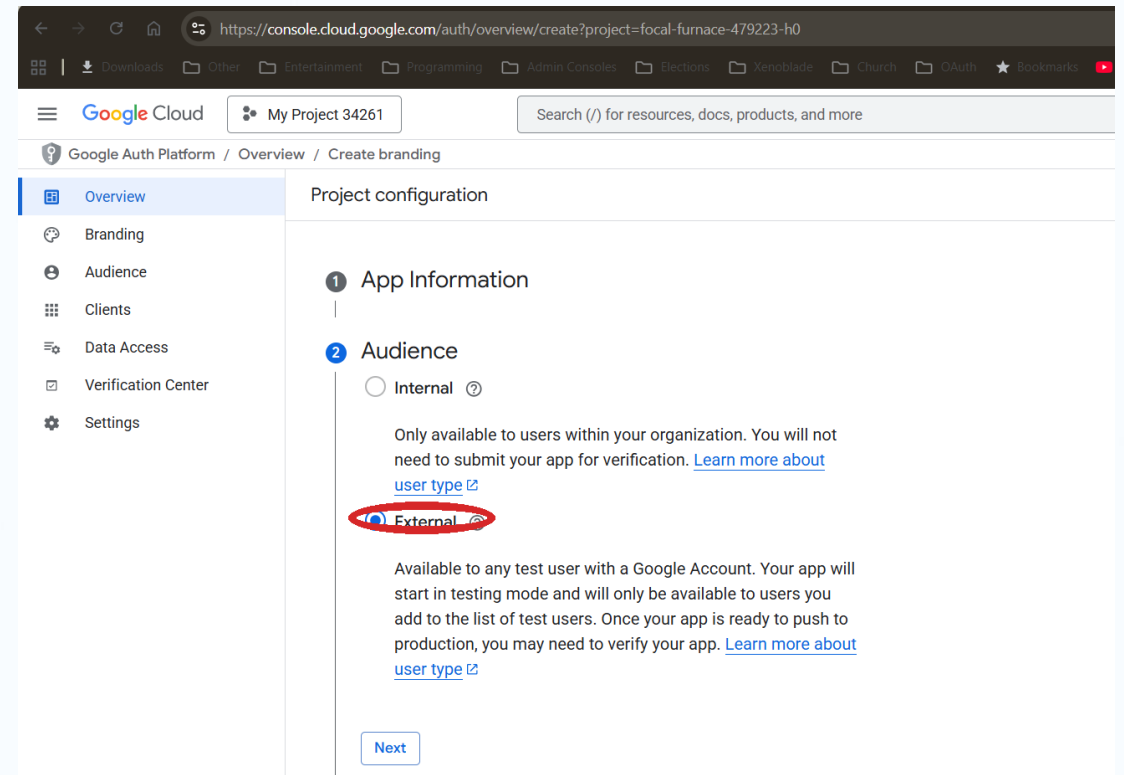
Gmail

- Provide App Information

The screenshot displays the Google Cloud console interface for configuring a new application. The top navigation bar includes the Google Cloud logo, the project name 'My Project 34261', and a search bar. Below this, the breadcrumb trail shows 'Google Auth Platform / Overview / Create branding'. A left-hand sidebar lists the configuration steps: Overview (selected), Branding, Audience, Clients, Data Access, Verification Center, and Settings. The main content area is titled 'Project configuration' and shows a progress indicator with four steps: 1. App Information (active), 2. Audience, 3. Contact Information, and 4. Finish. In the 'App Information' step, there are two required fields: 'App name *' with the value 'My Demo App' and a description 'The name of the app asking for consent', and 'User support email *' with the value 'bruce.armstrong.ba@gmail.com' and a description 'For users to contact you with questions about their consent. [Learn more](#)'. A 'Next' button is positioned below these fields. At the bottom of the configuration area, there are 'Create' and 'Cancel' buttons.

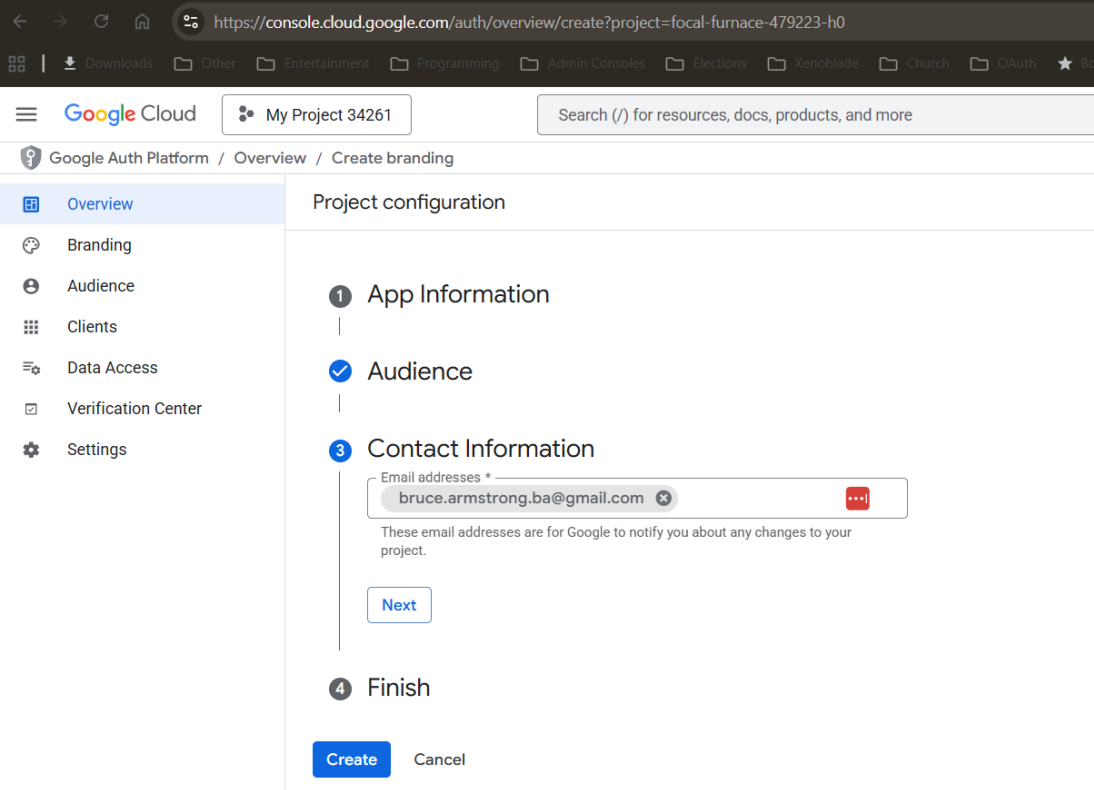
Gmail

- Define the audience



Gmail

- Provide contact information



The screenshot shows the Google Cloud console interface for creating a Google Auth Platform project. The browser address bar displays the URL: `https://console.cloud.google.com/auth/overview/create?project=focal-furnace-479223-h0`. The Google Cloud logo and 'My Project 34261' are visible at the top. The left sidebar contains a navigation menu with the following items: Overview (selected), Branding, Audience, Clients, Data Access, Verification Center, and Settings. The main content area is titled 'Project configuration' and shows a progress indicator with four steps: 1 App Information, 2 Audience (checked), 3 Contact Information (active), and 4 Finish. Under the 'Contact Information' step, there is a field for 'Email addresses *' containing the email 'bruce.armstrong.ba@gmail.com'. Below this field, a note states: 'These email addresses are for Google to notify you about any changes to your project.' A 'Next' button is located below the note. At the bottom of the page, there are 'Create' and 'Cancel' buttons.

Gmail

- Agree to terms and finish

https://console.cloud.google.com/auth/overview/create?project=focal-furnace-479223-h0

Google Cloud My Project 34261 Search (/) for resources, docs, products, and more

Google Auth Platform / Overview / Create branding

Overview

Branding

Audience

Clients

Data Access

Verification Center

Settings

Project configuration

1 App Information

Audience

Contact Information

4 Finish

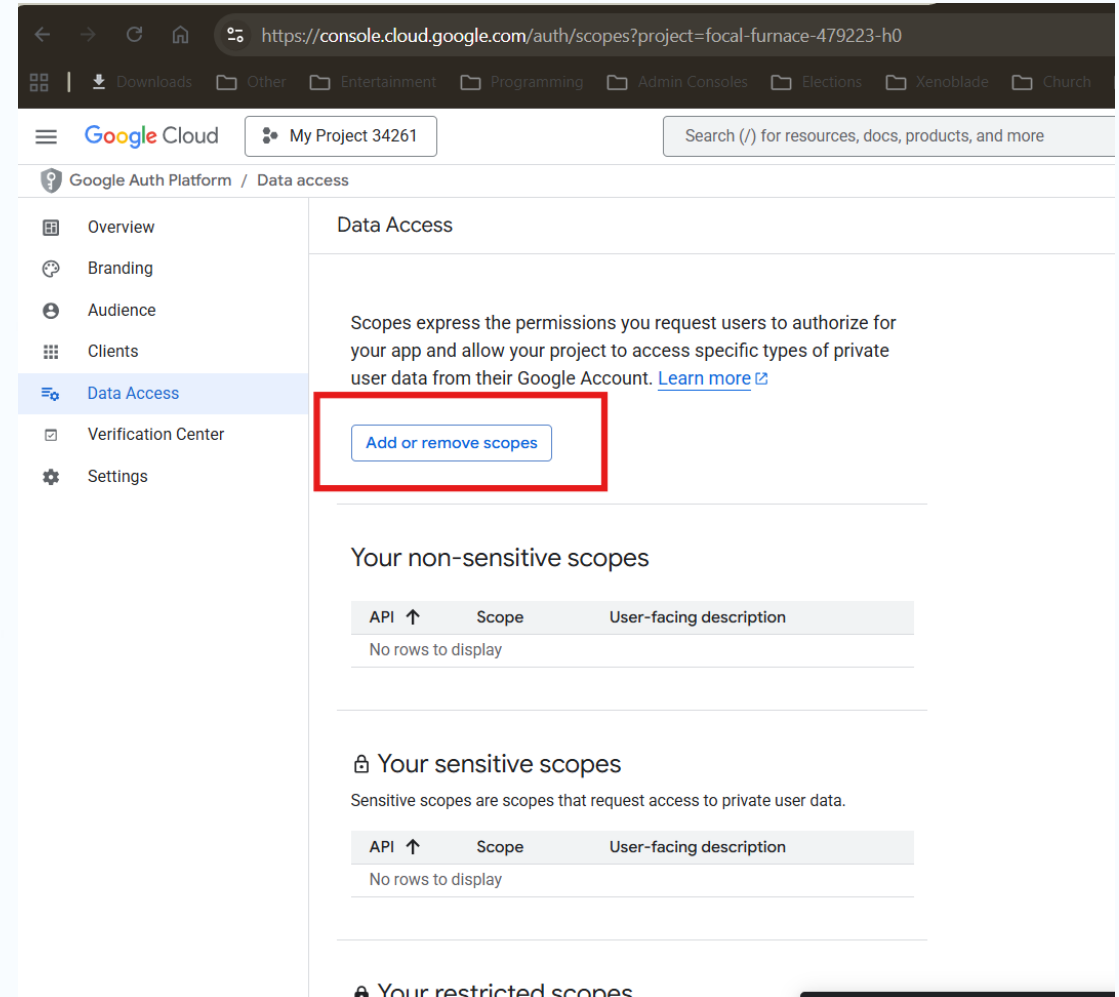
☒ I agree to the [Google API Services: User Data Policy](#)

Continue

Create Cancel

Gmail

- Under Data Access, click Add or Remove Scopes



Gmail

- Add the userinfo.email, profile, and openid scopes

×

Update selected scopes

i

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

Enter property name or value

?

	API ↑	Scope	User-facing description
☒		.../auth/userinfo.email	See your primary Google Account email address
☒		.../auth/userinfo.profile	See your personal info, including any personal info you've made publicly available
☒		openid	Associate you with your personal info on Google
☐	Analytics Hub API	.../auth/bigquery	View and manage your data in Google BigQuery and see the email address for your Google Account
☐	Analytics Hub API	.../auth/cloud-platform	See, edit, configure, and delete your Google Cloud data and see the email address for your Google Account.
☐	BigQuery API	.../auth/bigquery.readonly	View your data in Google BigQuery
☐	BigQuery API	.../auth/cloud-platform.read-only	View your data across Google Cloud services and see the email address of your Google Account
☐	BigQuery API	.../auth/devstorage.full_control	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
☐	BigQuery API	.../auth/devstorage.read_only	View your data in Google Cloud Storage
☐	BigQuery API	.../auth/devstorage.read_write	Manage your data in Cloud Storage and see the email address of your Google Account

Rows per page: 10 ▾ 1 – 10 of 25 < >

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

Gmail

- Manually add the <https://mail.google.com/> scope

The screenshot shows the Google OAuth consent screen. At the top, there's a browser address bar with tabs for 'OAuth', 'Bookmarks', 'Mary Snow Winter...', and 'PB 2025: Database...'. Below the address bar is a table of scopes. The first three rows are checked: '.../auth/userinfo.email', '.../auth/userinfo.profile', and 'openid'. The remaining rows are unchecked and include 'Analytics Hub API', 'BigQuery API', and 'BigQuery API' with various permissions. Below the table, there's a section titled 'Manually add scopes' with instructions. At the bottom, a text input field contains 'https://mail.google.com/' and an 'Add to table' button. The entire bottom section is highlighted with a red rectangle.

☒	...	/auth/userinfo.email	See your primary Google Account email address
☒	...	/auth/userinfo.profile	See your personal info, including any personal info you've made publicly available
☒		openid	Associate you with your personal info on Google
☐	Analytics Hub API	.../auth/bigquery	View and manage your data in Google BigQuery and see the email address for your Google Account
☐	Analytics Hub API	.../auth/cloud-platform	See, edit, configure, and delete your Google Cloud data and see the email address for your Google Account.
☐	BigQuery API	.../auth/bigquery.readonly	View your data in Google BigQuery
☐	BigQuery API	.../auth/cloud-platform.read-only	View your data across Google Cloud services and see the email address of your Google Account
☐	BigQuery API	.../auth/devstorage.full_control	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
☐	BigQuery API	.../auth/devstorage.read_only	View your data in Google Cloud Storage
☐	BigQuery API	.../auth/devstorage.read_write	Manage your data in Cloud Storage and see the email address of your Google Account

Rows per page: 10 1 – 10 of 25

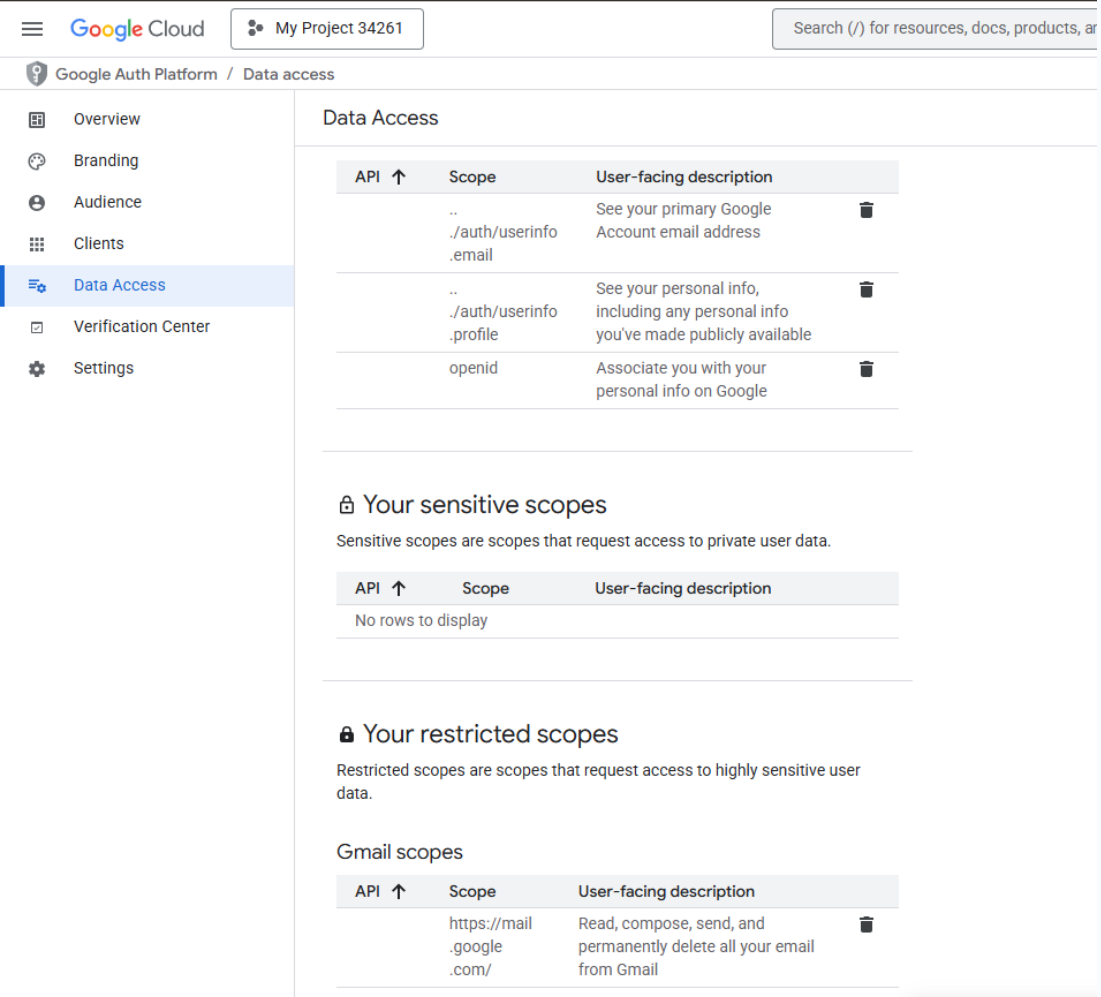
Manually add scopes

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

Gmail

- It should look like this when you're done



The screenshot shows the Google Cloud console interface for a project named "My Project 34261". The left sidebar contains navigation links: Overview, Branding, Audience, Clients, Data Access (highlighted), Verification Center, and Settings. The main content area is titled "Data Access" and displays a table of API scopes.

API	Scope	User-facing description	
...	./auth/userinfo.email	See your primary Google Account email address	
...	./auth/userinfo.profile	See your personal info, including any personal info you've made publicly available	
...	openid	Associate you with your personal info on Google	

Below the table, there are sections for "Your sensitive scopes" and "Your restricted scopes".

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

API	Scope	User-facing description
No rows to display		

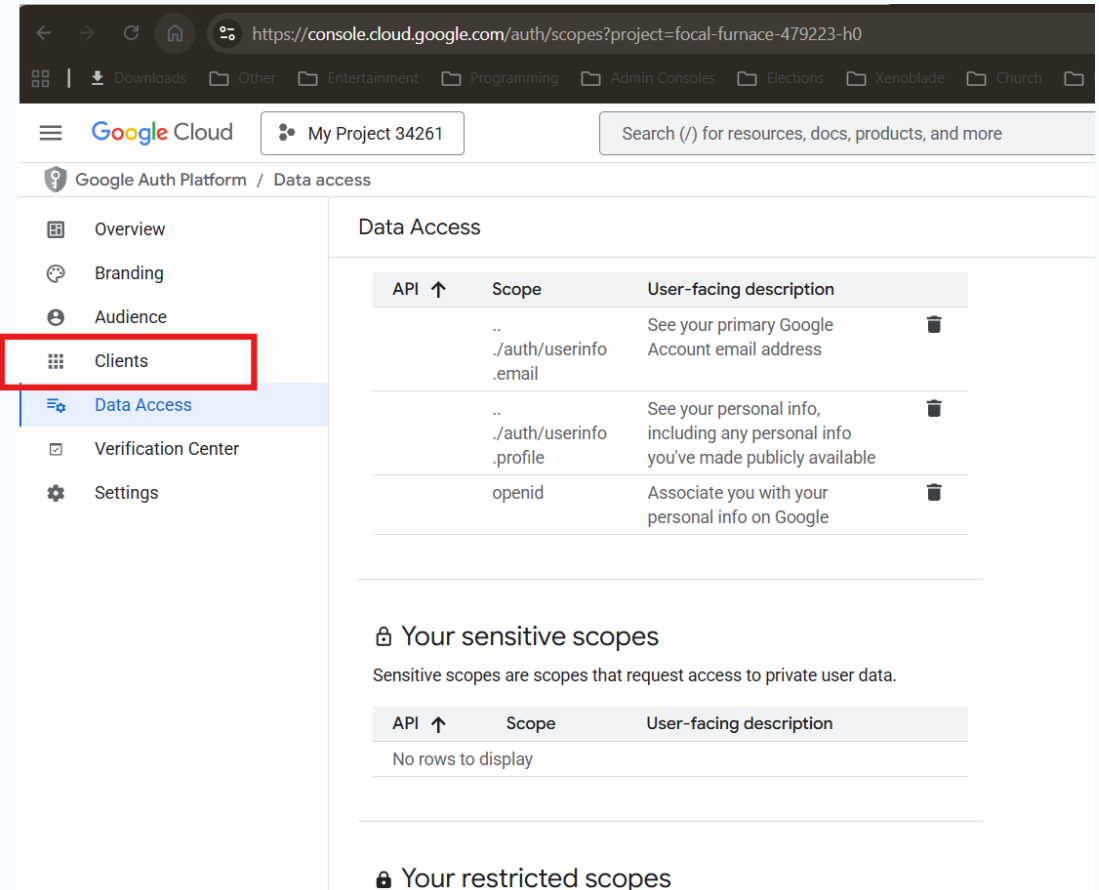
Your restricted scopes
Restricted scopes are scopes that request access to highly sensitive user data.

Gmail scopes

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

Gmail

- Click Clients



The screenshot shows the Google Cloud console interface. The left-hand navigation menu includes 'Overview', 'Branding', 'Audience', 'Clients' (highlighted with a red box), 'Data Access', 'Verification Center', and 'Settings'. The main content area is titled 'Data Access' and displays a table of scopes. Below the table, there are sections for 'Your sensitive scopes' and 'Your restricted scopes'.

API ↑	Scope	User-facing description	
	..	See your primary Google Account email address	🗑️
	../auth/userinfo.email		
	..	See your personal info, including any personal info you've made publicly available	🗑️
	../auth/userinfo.profile		
	openid	Associate you with your personal info on Google	🗑️

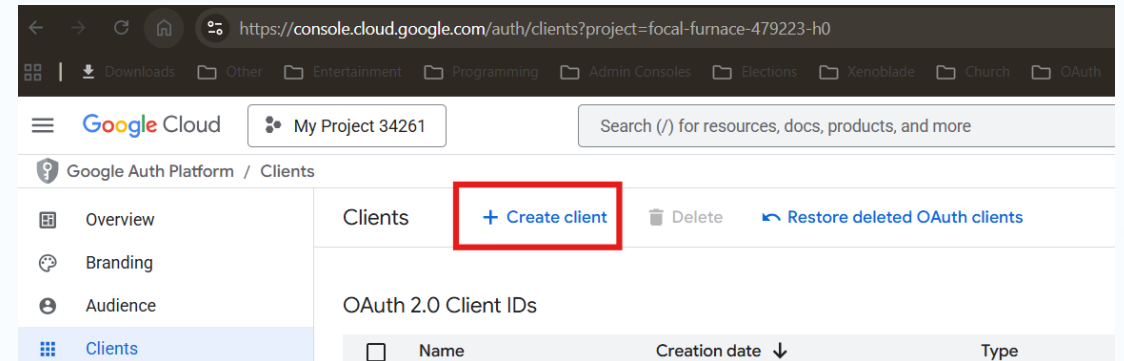
Your sensitive scopes
Sensitive scopes are scopes that request access to private user data.

API ↑	Scope	User-facing description
No rows to display		

Your restricted scopes

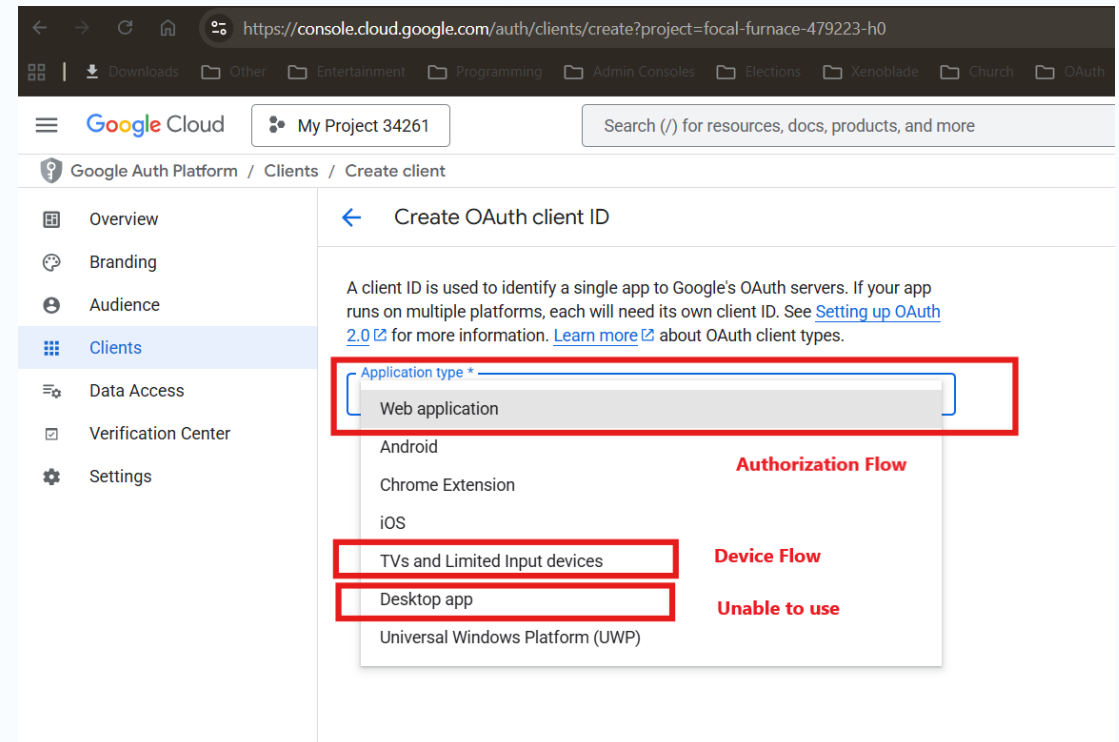
Gmail

- Click Create Client



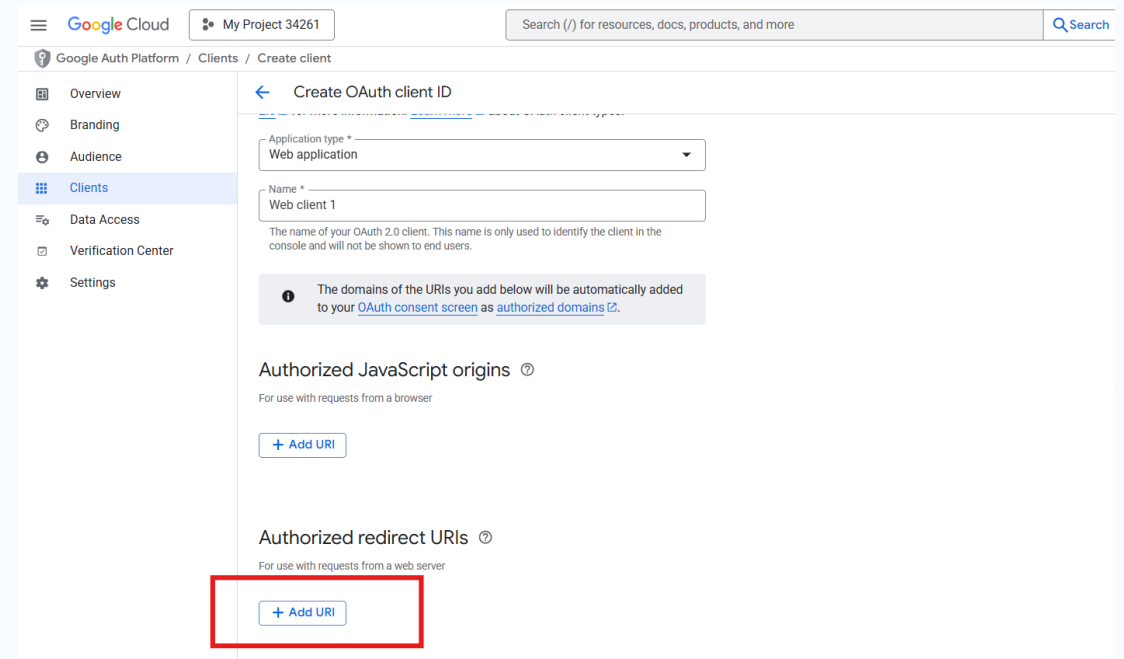
Gmail

- There are several Application Types, each with a different flow.



Gmail – Authorization Flow

- We'll use Web Application for Authorization flow
- Give it a name
- Add the redirect URI



Google Cloud My Project 34261 Search (/) for resources, docs, products, and more

Google Auth Platform / Clients / Create client

Create OAuth client ID

Application type *
Web application

Name *
Web client 1

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.

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

Authorized redirect URIs ⓘ
For use with requests from a web server

+ Add URI

Gmail – Authorization Flow

- Click Create

https://console.cloud.google.com/auth/clients/create?project=focal-furnace-479223-h0

Google Cloud My Project 34261 Search (/) for resources, docs, products, and more

Google Auth Platform / Clients / Create client

Overview
Branding
Audience
Clients
Data Access
Verification Center
Settings

Create OAuth client ID

Name *
Web client 1

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.

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

Authorized JavaScript origins ②

For use with requests from a browser

+ Add URI

Authorized redirect URIs ②

For use with requests from a web server

URIs 1 *
http://localhost:8090

+ Add URI

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

Create Cancel

Gmail – Authorization Flow

- Record the Client ID and Client Secret

OAuth client created

The client ID can always be accessed from Clients tab under Google Auth Platform.

i OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Client ID

[redacted]

⚠ Starting in June 2025, you will no longer be able to view or download the client secret once you close this dialog. Make sure you have copied or downloaded the information below and securely stored it.

Client secret

[redacted]

Creation date November 23, 2025, 4:38:48 PM GMT-7

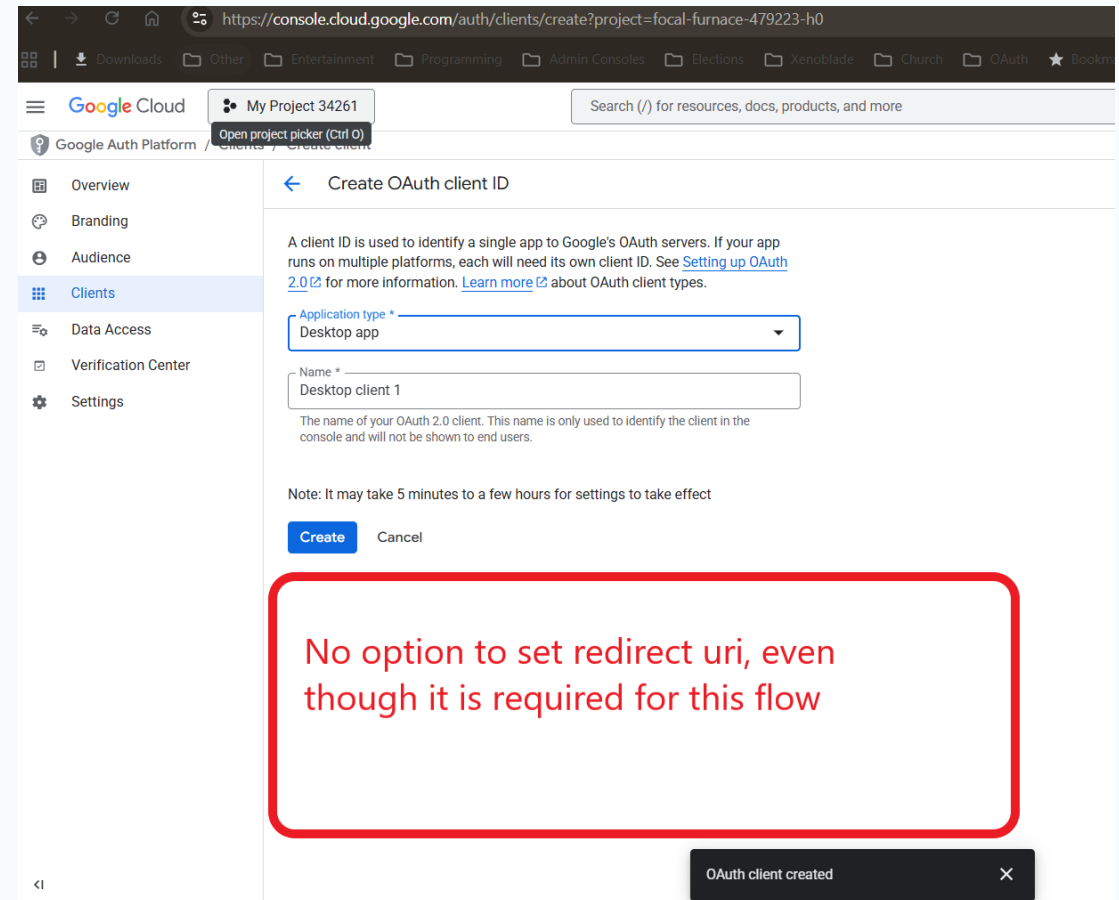
Status  Enabled

 Download JSON

OK

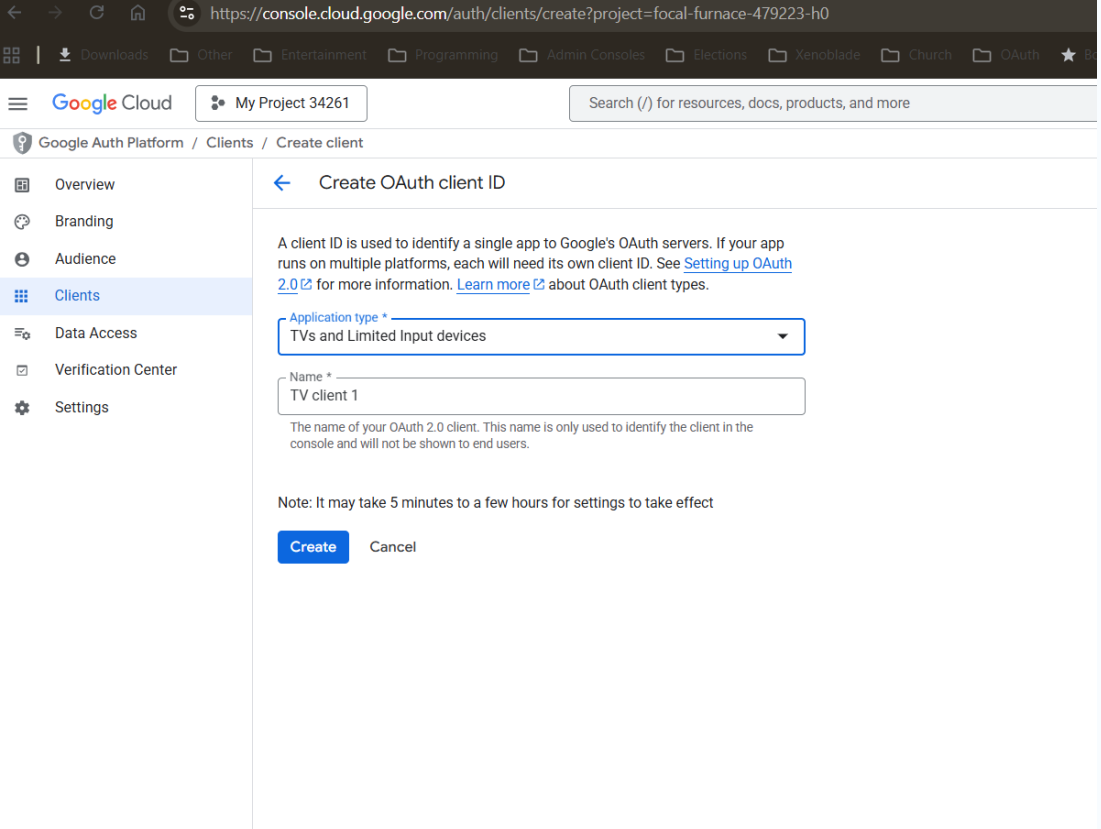
Gmail - Desktop

- The Desktop Client also uses Authentication flow and requires a redirect URI
- However, the Google admin windows don't allow us to provide the redirect URI, making this particular client useless



Gmail – Device Authorization Flow

- The TV and Limited input device client uses Device Authorization Flow
- Unfortunately, Google only supports a limited number of scopes for this client
- Sending email is not one of the supported scopes
- Will demonstrate nonetheless in case you want to use for other purposes (e.g., SSO)



The screenshot shows the Google Cloud Console interface for creating an OAuth client ID. The browser address bar displays the URL: `https://console.cloud.google.com/auth/clients/create?project=focal-furnace-479223-h0`. The page title is "Create OAuth client ID". On the left, a sidebar menu lists various sections: Overview, Branding, Audience, Clients (highlighted), Data Access, Verification Center, and Settings. The main content area contains a text block explaining that a client ID identifies an app to Google's OAuth servers. Below this, there is a dropdown menu for "Application type" with "TVs and Limited Input devices" selected. A text input field for "Name" contains "TV client 1". A note states: "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." At the bottom, a note mentions that settings may take 5 minutes to a few hours to take effect. Two buttons, "Create" and "Cancel", are located at the bottom right.

Google Cloud | My Project 34261 | Search (/) for resources, docs, products, and more

Google Auth Platform / Clients / Create client

← Create OAuth client ID

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 *
TVs and Limited Input devices

Name *
TV client 1

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.

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

Create Cancel

Gmail – Device Authorization Flow

- Capture the Client ID and Client Secret

OAuth client created

The client ID can always be accessed from Clients tab under Google Auth Platform.

i OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Client ID

[redacted]

⚠ Starting in June 2025, you will no longer be able to view or download the client secret once you close this dialog. Make sure you have copied or downloaded the information below and securely stored it.

Client secret

[redacted]

Creation date November 23, 2025, 4:38:48 PM GMT-7

Status Enabled

Download JSON

OK

Sample Code

The sample code you can download for this session has the full implementation for Authentication and Device Authentication flows for both Azure and Google

```
If tab_1.tabpage_auth.rb_username_password.checked THEN

    client.AuthType = 2
    client.Username = tab_1.tabpage_auth.sle_username.text
    client.Password = tab_1.tabpage_auth.sle_password.text

Else

    client.AuthType = 5
    client.Username = tab_1.tabpage_auth.sle_username.text
    client.xoauth2accesstoken = ls_authtoken

End If
```

Session Agenda (Recap)

- Authentication vs Authorization
- Why use OAuth2 for SMTP Authentication
- OAuth2 Flows
 - Authorization Flow
 - Device Authorization Flow
- Configuring Azure
- Configuring Gmail
- Sample Code

Thank you

Connect with Us



community.appeon.com

Discussions, tech articles and videos, free online training, and more.



facebook.com/AppeonPB

Encourage us with a “like”, see cool pics, and get notified of upcoming events.



x.com/AppeonPB

Follow Appeon and community members to get the latest tech news.



linkedin.com/company/appeon

Build up your career profile, and stay in contact with other professionals.



youtube.com/Appeon

Share important Appeon videos with others; no account registration required.

Q&A Time

