Kofax eFlow ePortal
User's Guide

Version: 2.1.0

Date: 2022-11-28

KOFAX

Table of Contents

Preface

This guide describes how to configure the Kofax eFlow ePortal application and connectors, and also provides information on filters, conversion, collection creation, and acknowledgment.

The Kofax eFlow ePortal application is an add-on application to the Kofax eFlow platform, which uses an eFlow station called ePortal. When configured, the ePortal station can read emails and electronic data, create collections, and automatically import them into the eFlow workflow. The collections are then processed further by eFlow.

Product documentation

The full documentation set for Kofax eFlow ePortal is available on the Product documentation page.

The documentation set includes the following items:

Name	Description
Kofax eFlow ePortal Installation Guide	Provides instructions for installing the Kofax eFlow ePortal application.
Kofax eFlow ePortal User's Guide	Provides information on the application configuration, connectors, filtering, conversion, collection creation, and acknowledgment.
Kofax eFlow ePortal Release Notes	Details the list of newly added features, resolved issues, known issues with an applicable workaround, and the changes made since the previous release.
Kofax eFlow ePortal Technical Specifications	Describes the prerequisites and the required hardware and software to work with the ePortal application.

Offline documentation

To access the documentation offline, download the KofaxeFlowePortalDocumentation_2.1.0_EN.zip file from the Kofax Fulfillment Site and extract it on a local drive available to your users.

Training

Kofax offers both classroom and online training to help you make the most of your product. To learn more about training courses and schedules, visit the Kofax Education Portal on the Kofax website.

Getting help with Kofax products

The Kofax Knowledge Base repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base:

1. Go to the Kofax website home page and select **Support**.
2. When the Support page appears, select **Customer Support** > **Knowledge Base**.

The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.

  Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.

  Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.

From the Knowledge Base home page, you can:

- Access the Kofax Community (for all customers).

  Click the **Community** link at the top of the page.
- Access the Kofax Customer Portal (for eligible customers).

  Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Customer Portal**.
- Access the Kofax Partner Portal (for eligible partners).

  Click the **Support** link at the top of the page. When the Customer & Partner Portals Overview appears, click **Log in to the Partner Portal**.
- Access Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

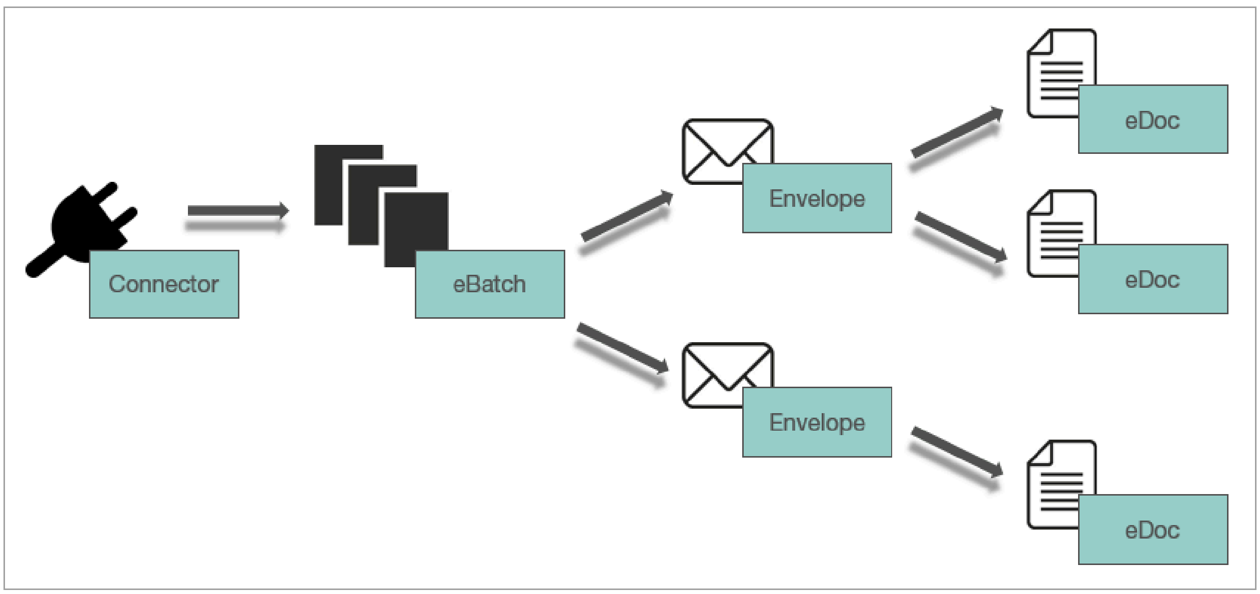
  Go to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

About Kofax eFlow ePortal

This chapter illustrates the data flow of the Kofax eFlow ePortal application and explains the different process stages and terms used in the ePortal application. The purpose of the ePortal application is to import electronic documents and emails into the eFlow workflow.

ePortal terms



Term	Description
Connector	ePortal connectors retrieve documents from remote servers.
eBatch	An eBatch is a list of envelopes to be processed by an ePortal connector. The maximum number of envelopes to process at once is defined in the `<MaxWorkUnit>` property in the `<Stations>` section of the ePortal.AppConfig file.

Term	Description
Envelope	An envelope contains at least one eDoc as well as metadata. • Reporting data • Global status: The envelope status • Detailed status: The eDoc status • Temp folder architecture Typically, an email is an envelope: It contains none, one or several documents. There can be two files on the remote server with the same name, with .TIF and .XML format. Complex files, such ZIP or EML are parsed before they are imported. Using an envelope object enables every ePortal stage to process a combination of documents, such as TIF, Email, TIF + XML, TIF + JPG + PRD + XML, and so on. The envelope metadata is only used by the ePortal connectors for archiving and setting user tags. For example, the email subject can be set as a user tag.
eDoc	An electronic document is a document that is available on the remote server. For example: • Email • Email attachment • TIF, PDF, XML, or more
Mail Account	A Mail Account allows the ePortal connector to connect to a remote server. It includes the following properties: • ID • Description • Username • Password (If basic authentication applies to the connector) • Client ID (If OAuth is applies for the connector) • Tenant ID (If OAuth is applies for the connector) • Client secret ID (If OAuth is applies for the connector) You can add several accounts to the `<MailAccounts>` section of the ePortal.AppConfig file, but an ePortal connector can only use the account that is linked to the station by its ID and is enabled.
eDoc provider	An eDoc provider is a remote server on which electronic documents reside.
Mailbox	A Mailbox is an electronic document source from which ePortal retrieves files.

ePortal process

The process of importing documents into the eFlow workflow with the Kofax eFlow ePortal application comprises actions, such as extracting, filtering, converting, organizing, and archiving the data.

ePortal process stages

The ePortal includes the following process stages:

Connecting

ePortal uses connectors to retrieve data from remote servers, such as email servers. For more information on connector configuration, see Connector.

Filtering

The ePortal filters are used to classify the eDoc of the envelope and link the AttachedDocs (DocAttachment), AttachedFiles (FileAttachment) to their main AcceptedDoc. For more information on filtering, see Filtering.

Converting

The ePortal converters are used to convert various file types to TIF CCITT4, create JPGs from color images, and create PRD files from searchable PDFs. For more information on converter configuration, see Conversion.

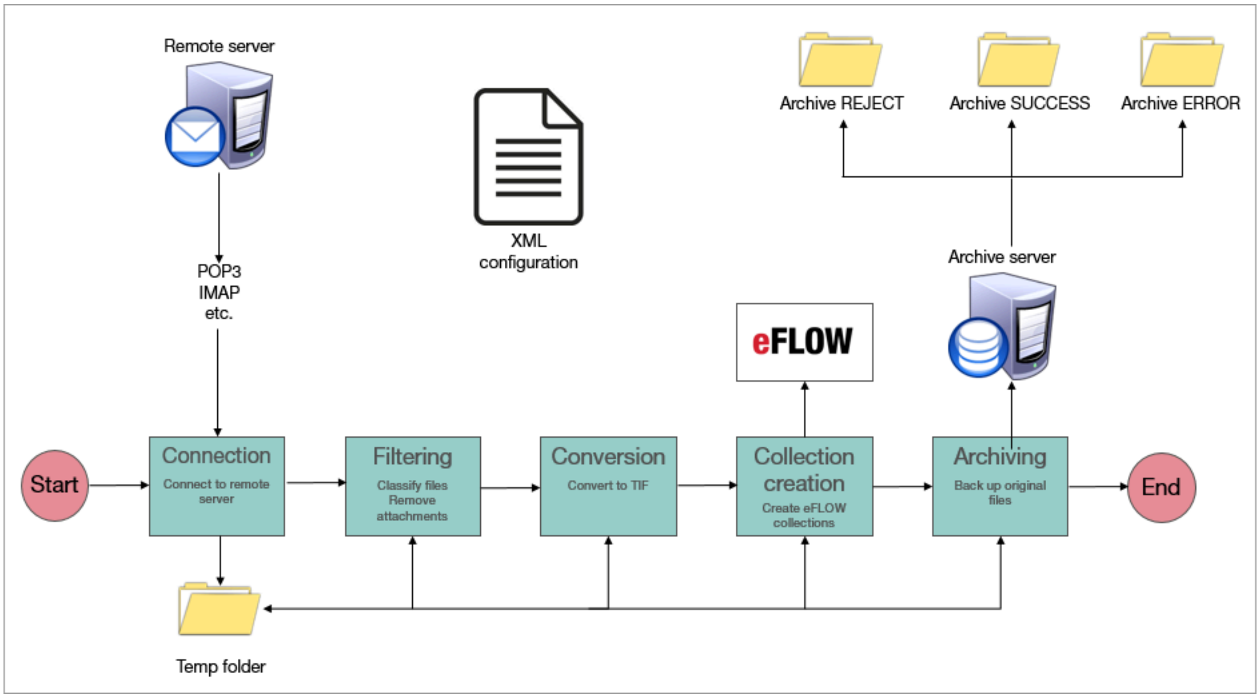
Collection creating

The ePortal prepares all eDocs of the envelope as a collection to import into eFlow. For more information on collection creation configuration, see Collection creation.

Archiving (Acknowledgment)

There are three types of archives: Success, Rejected and Error. An acknowledgment email for each types of archiving can be configured and sent to inform the senders that their files have been processed. For information on acknowledgment configuration, see Acknowledgment.

The process stages can be controlled using the ePortal configuration file EPortalApp.Config. The following figure illustrates the process stages of the ePortal application.



Each stage processes an envelope object created by ePortal connector.

Chapter 2

ePortal configuration

You can configure ePortal using the EPortal.AppConfig file located in the `Setup` folder of the eFlow application.

The following is an example for the `Setup` folder path.

```
C:\ProgramData\TIS\eFlow 6\AppData\Server\<APP NAME>\Setup
```

Configuration file

The configuration file includes the following sections:

- Connection string
- Features
- Stations
- Section

The following is the structure of the configuration file.

```
<?xml version="1.0" encoding="utf-8"?>
<Configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema">
 <DefaultStation>Default</DefaultStation>
 <DefaultSection>Default</DefaultSection>
 <ConnectionString Value="DATA SOURCE=.\EFLOW;INITIAL CATALOG=ePortal">
    <UserName>5B4C62489605D01B</UserName>
    <Password>5B4C62489605D01B</Password>
 </ConnectionString>
 <Features> ... </Features>
 <Stations> ... </Stations>
 <Sections> ... </Sections>
 </Configuration>
```

Connection string

The `<ConnectionString>` section is used to connect to the ePortal database.

```
<ConnectionString Value="DATA SOURCE=.\EFLOW;INITIAL CATALOG=ePortal">
  <UserName>sa</UserName>
  <Password>sa</Password>
 </ConnectionString>
```

Features

The `<Features>` section contains the configuration for filtering, conversion, collection creation, and archiving of images.

```
<Features>
    <Filtering> ... </Filtering>
    <Conversion> ... </Conversion>
    <CollectionCreation> ... </CollectionCreation>
    <Archives> ... </Archives>
<Features>
```

Stations

The `<Stations>` section contains the configuration of the connectors to each ePortal station, such as POP3_OAUTH, EXCHANGE_ONLINE, IMAP_GMAIL, EML, or FILE.

The configuration contains a node defining the default station, followed by nodes for specific stations. If a station-specific configuration is defined, that configuration is used. If no station-specific configuration is found, the default station configuration is used.

```
<DefaultStation>ABC</DefaultStation>
 <Stations>
    <Station Name="ABC">
      <...>
    </Station>
    <Station Name="DEF">
      <...>
    </Station>
  </Stations>
```

In the above example the following configurations are used:

- For an ePortal station named ABC, the <Station Name="ABC"> configuration is used.
- For an ePortal station named DEF, the <Station Name="DEF"> configuration is used.
- For an ePortal station named XYZ, the default <DefaultStation> configuration is used.

Station properties

```
<Station Name="YourStationName">
      <QueryWF Enabled="false" />
      <MaxWorkUnit Value="10" />
      <Acknowledgement Enabled="true" />
      <UpdatePriority Enabled="true" />
      <ActiveAccounts>
        <ActiveAccount Id="Gmail_oauth" Enabled="true" />
        <ActiveAccount Id="smtp_oauth_exchange" Enabled="true" />
      </ActiveAccounts>
    </Station>
```

Property	Description
QueryWF	Checks in the eFlow database whether the collection was created correctly.
MaxWorkUnit	Number of emails/files to process per eBatch.

Property	Description
Acknowledgement	Enables acknowledgment emails. You must also activate acknowledgment in the archive configuration.
UpdatePriority	Sets the eFlow collection priority according to the email priority, such as High importance or Low importance.
ActiveAccount	ID of an account defined in the `<Sections>` section.

Sections

The `<Sections>` section defines the specific working folder and the mail accounts used by an ePortal station when processing on a specific server.

For example, for a specific server, you can define a `<QA>` section and a `<Production>` section.

The section that is used by default is defined in the `<DefaultSection>`.

```
<DefaultSection>Default</DefaultSection>
```

Example:

```
<Sections>
  <Section Name="Default">
    <WorkDir>C:\Temp\ePortal</WorkDir>
    <MachineNames>
        <MachineName>NAME_OF_CLIENT1</MachineName>
        <MachineName>NAME_OF_CLIENT2</MachineName>
    </MachineNames>
    <MailAccounts>
       <MailAccount Id="Gmail_oauth">
          ...
```

Section properties

Property name	Description
WorkDir	Defines the path to the folder in which temporary files are created before being imported into eFlow.
MachineNames	Can be empty or set to a specific server name to use the same account with different configurations, such as a test configuration and a production configuration.
MailAccounts	List of accounts used by the ePortal connector to import emails or files into eFlow. See Connectors for more information.

Backward compatibility of configuration files

The older configuration files ePortal.xml and EPortal.AppConfig are still supported. However, to support new features, the new settings must be added manually to the file or replaced with the latest configuration.

When you install a new version of ePortal, the ePortal engine checks the configuration file version to decide whether updates are needed. The configuration file is updated with default values.

Chapter 3

Connectors

ePortal uses connectors to retrieve data from remote servers, such as email servers. The connectors perform the following actions:

1. Connect or disconnect to or from an eDoc provider such as an email server, an SMTP server, or an FTP server. The connector uses the mail accounts defined in the ePortal station configuration to connect to the server.
2. In the EPortal.AppConfig file, check the number of remote files to import as an eBatch.
3. Return an eBatch containing a list of files to import in the eFlow workflow. An envelope can contain one or more eDocs, wherein eDoc is the file that is to be imported.
4. Delete, move, or change the remote file properties when it is archived. Depending on the configuration, the file is archived in the SUCCESS, REJECT, or ERROR archive.

ePortal provides the following connectors:

- POP3_OAUTH connector
- IMAP_GMAIL connector
- EXCHANGE_ONLINE connector
- File connector
- EML connector
- Archive connector

POP3_OAUTH connector

POP3_OAUTH connector is an upgraded version of the POP3 connector, which implements OAuth for secure delegate access. This connector does not require a password for the mail account configuration in EPortal.AppConfig file.

The POP3_OAUTH connector retrieves a batch of emails from a POP3 server. The emails are parsed by the envelope (MessageHandler). Each envelope has a unique ID on the POP3 server that enables the connector to retrieve it. The POP3_OAUTH connector can only read or delete emails. Once all the emails in the batch are parsed, the connector returns an eBatch that can be processed by each ePortal stage.

Unsynchronized mode

Unsynchronized mode checks the mailbox for unread messages and deletes the emails in the mailbox after they have been imported into the eFlow workflow.

Synchronized mode

Synchronized mode first synchronizes the ePortal database with the POP3 server and then checks the database for unread messages. The synchronized mode does not delete the emails from the mailbox after they have been imported.

Autorun mode

Disable the autorun mode in the following scenarios and run the ePortal manual station.

Scenario 1: Whenever you add a new mail account in POP3_OAUTH protocol in the EPortal.AppConfig file, you need to manually authorize yourself in the ePortal station by entering configured mail account credentials and permissions consent.

Scenario 2: When the password for your email account expires or changes, re-authorize yourself by opening the ePortal station manually.

Enable the autorun mode for the ePortal station.

Configuration

Any application that implements the OAuth standard to authenticate and authorize its users, the application needs to be registered with the corresponding Application/Web servers.

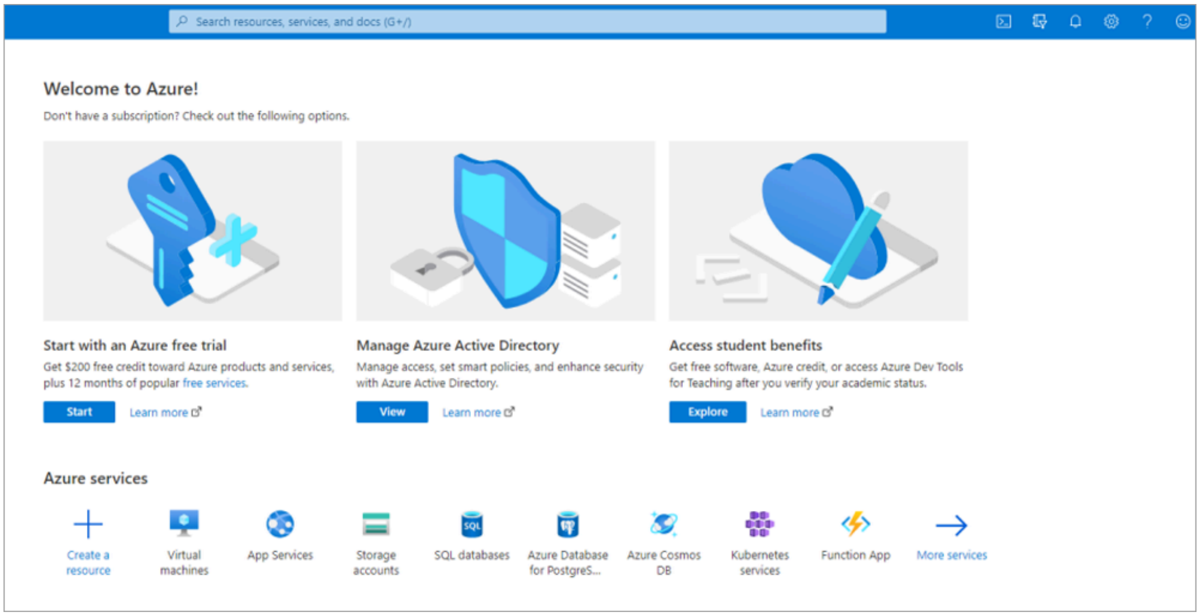
The following step-by-step procedure explains how to register an ePortal app and the minimum set of privileges needed for it. More granular role-based access privileges are possible, but this is subject to the IT policies of the individual organizations.

Azure cloud configuration for Office 365

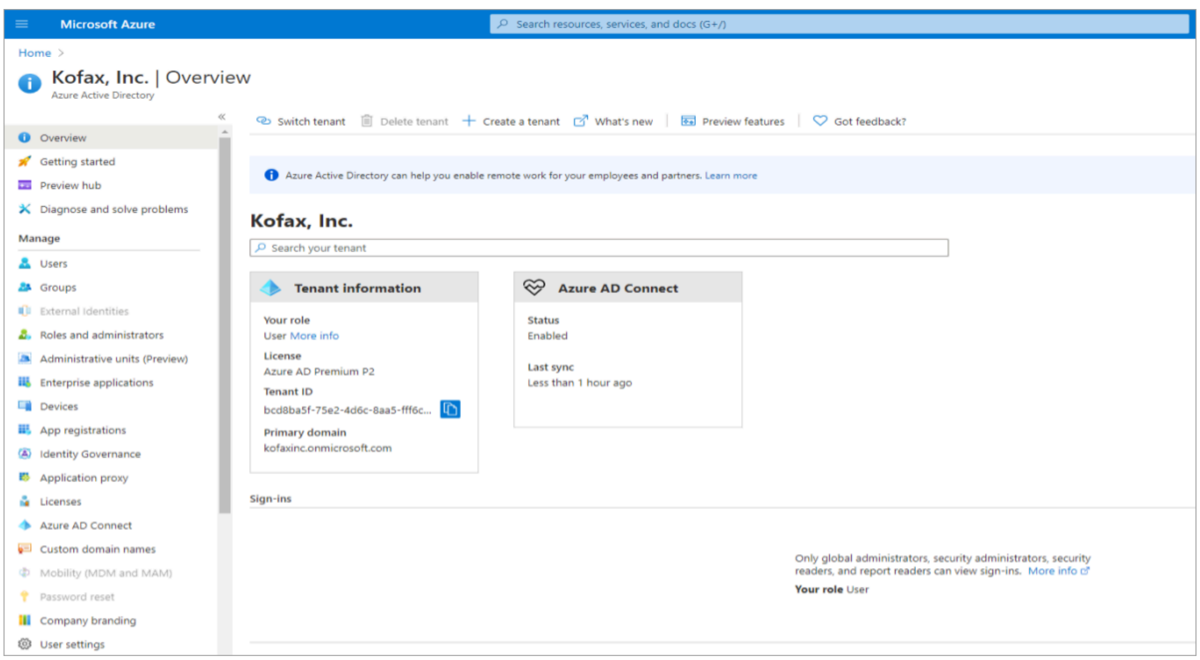
This section describes the Azure cloud configuration for Office 365. After you configure Azure cloud, ePortal can automatically read emails from Outlook.

The figures and user interfaces used in the following procedure are taken from the Microsoft Azure website and they might change occasionally. Hence, we request you to follow the latest procedure mentioned in the Microsoft Azure website, which is updated time-to-time. If you still face issues while authorizing your application, we recommend you take assistance from a user who has expertise in authorizing an application.

1. Sign in to `https://portal.azure.com` using your work account. Follow the on-screen instructions to complete the sign-in procedure.
   After a successful sign-in, the Azure home page appears.



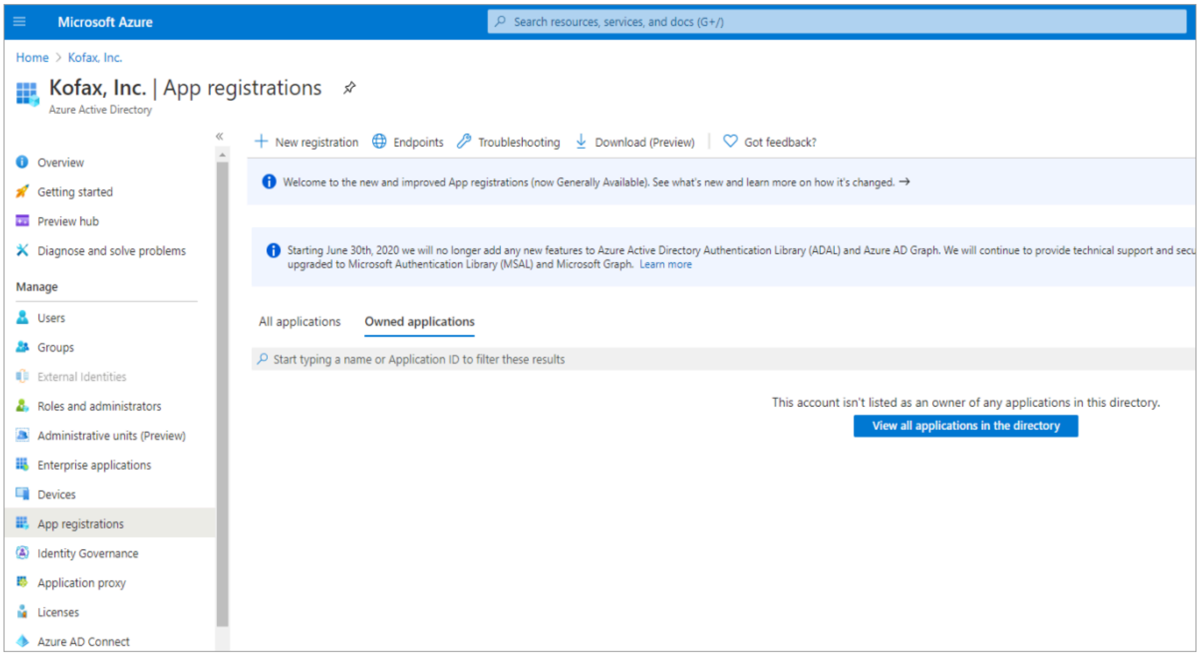
2. On the Azure home page, under **Manage Azure Active Directory**, click **View**.
   The **Overview** page appears.



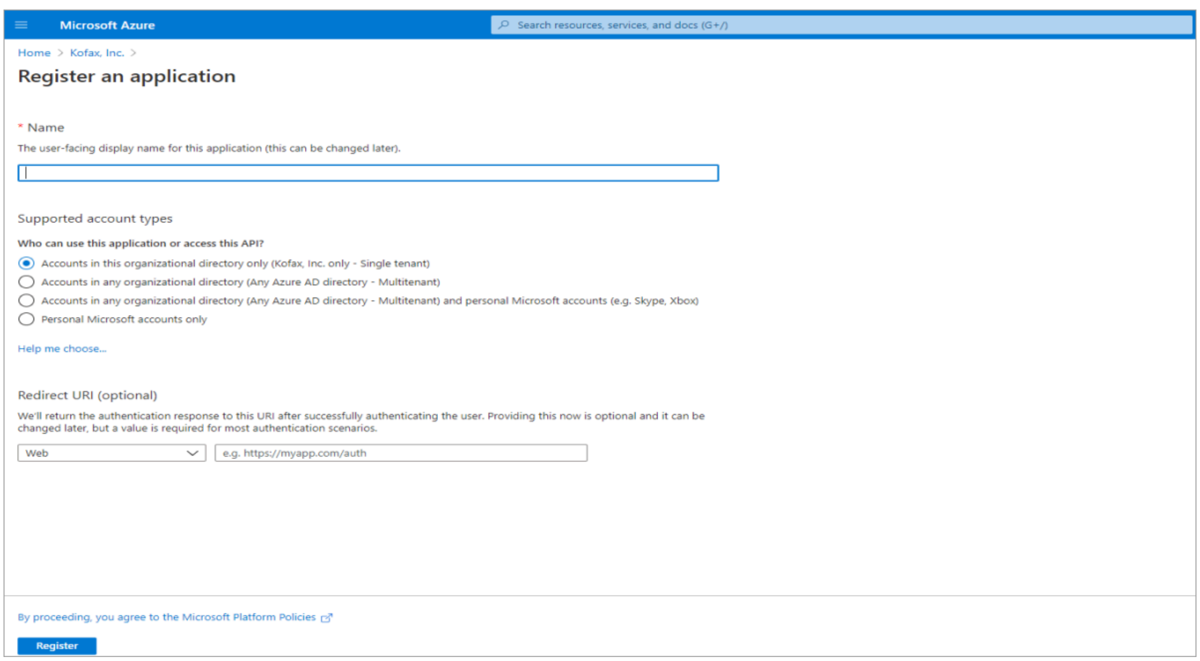
Manage App registrations

Register your application. You can register your application in a directory or outside of a directory.

1. On the left sidebar, under **Manage**, click **App registrations**.
   The **App registrations** page appears.



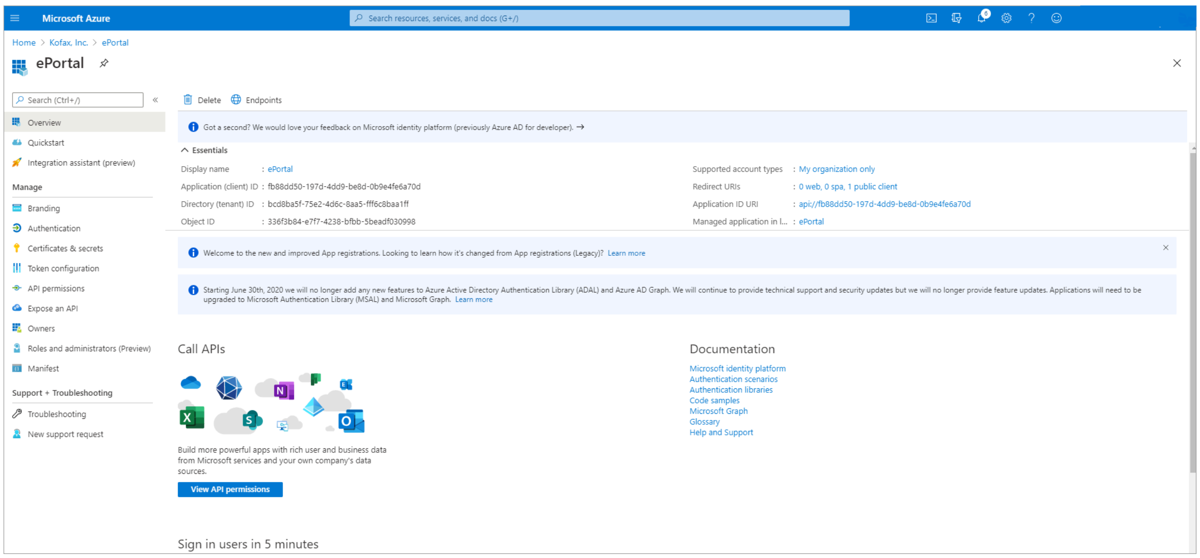
2. Click **New registration**.
   The **Register an application** page appears.



3. In the **Name** field, type the application name that is to be displayed to the users.
4. Under **Supported account types**, select **Accounts in this organizational directory only (Kofax, Inc. only - Single tenant)**.

> Select this option if you want to build a Line-of-Business (LOB) application. It maps only a single tenant to Azure AD (Active Directory). This is the default option and is only available if you register your application in a directory. The default is Azure AD multi-tenant and personal Microsoft accounts if you register the application outside of a directory.

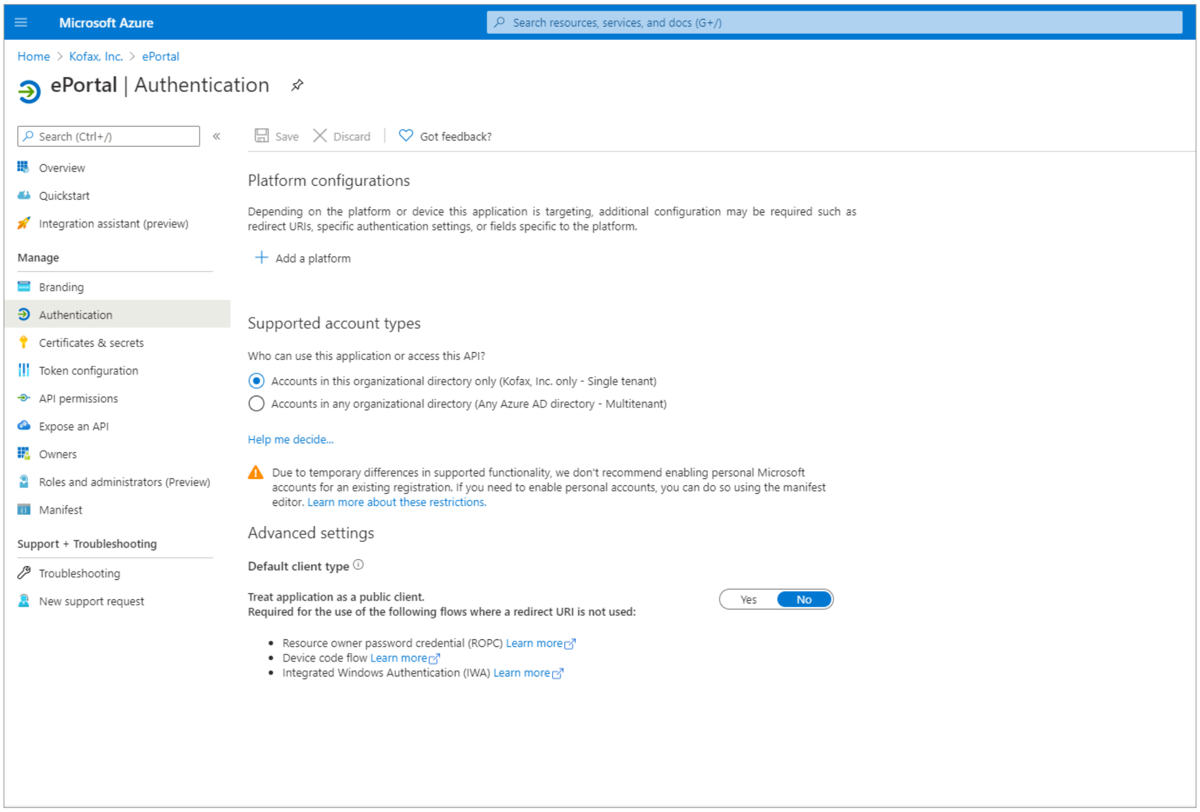
5. Under **Redirect URI (optional)**, select **Public client/native (mobile & desktop)** from the list and click **Register**.
   The following page appears.



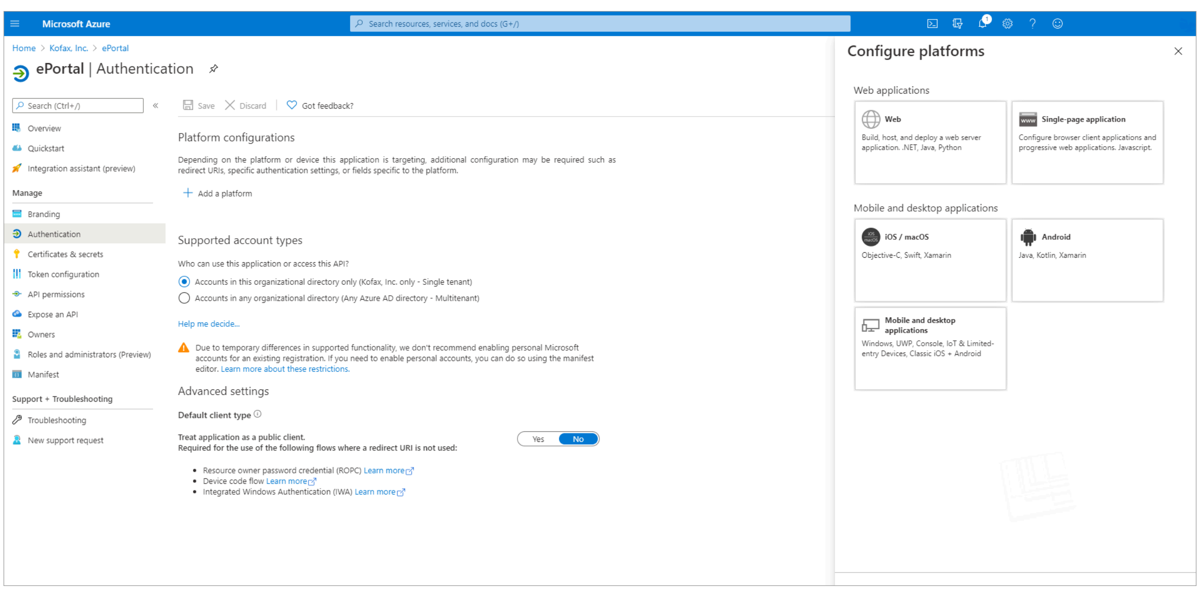
Manage authentication

You can configure application settings based on the platform or device you are targeting.

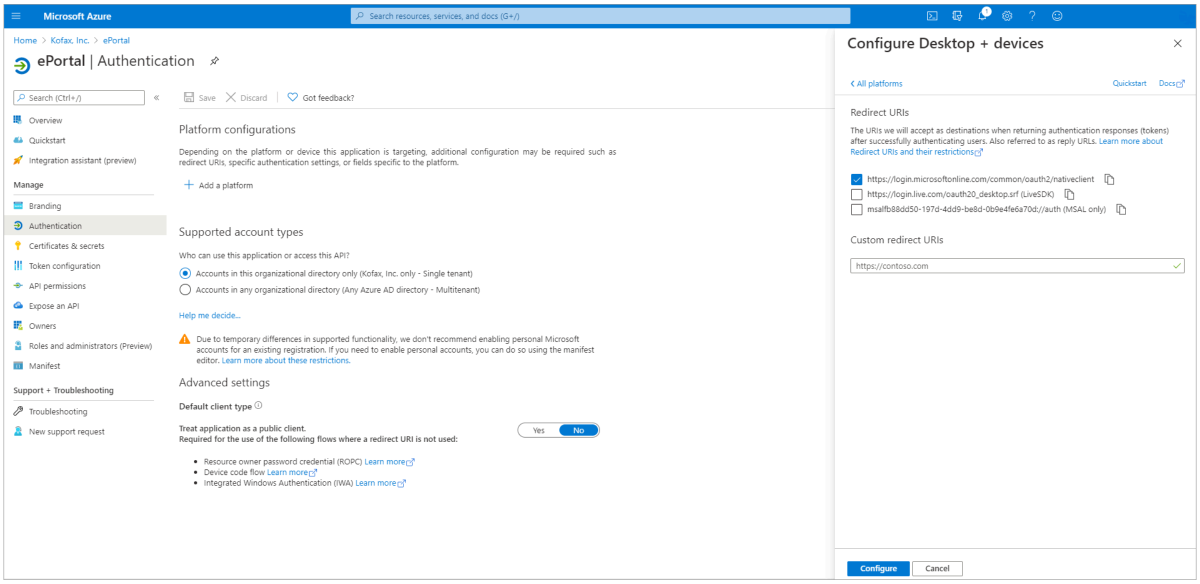
1. On the left sidebar, under **Manage**, click **Authentication**.
   The **Authentication** page appears.



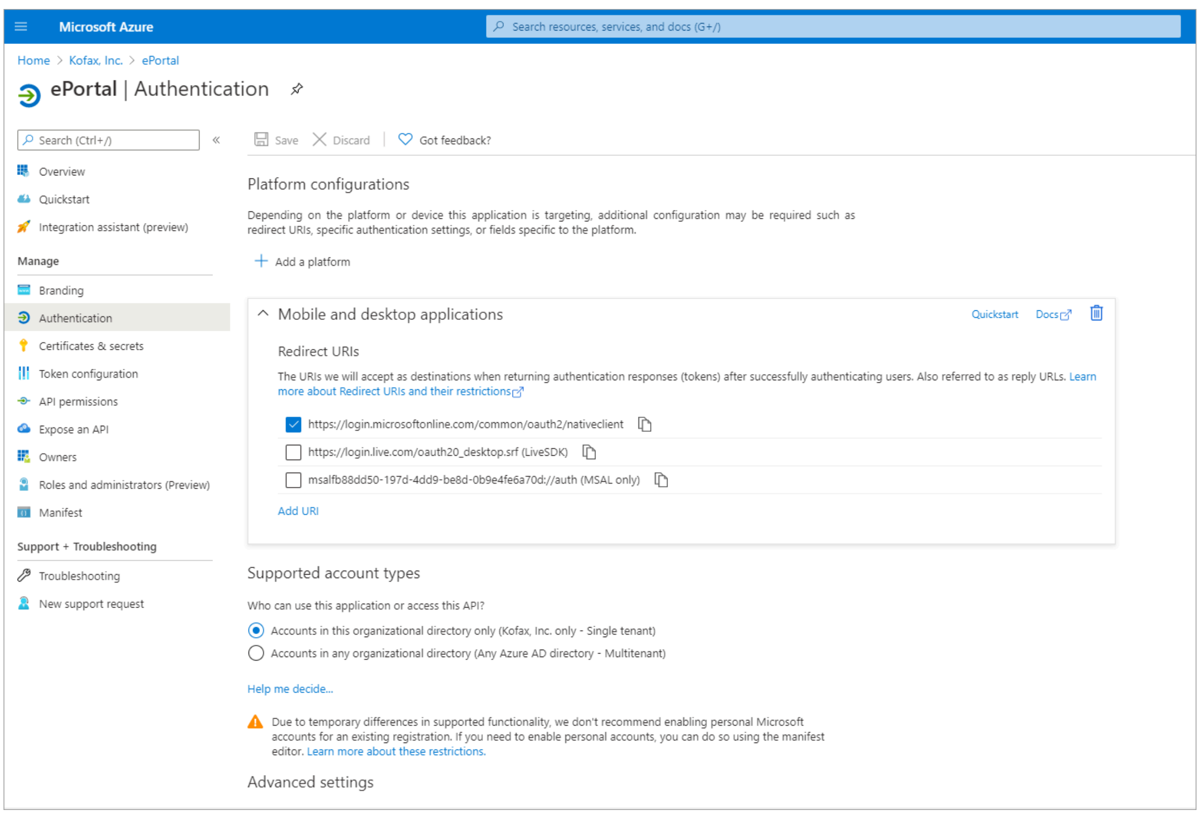
2. Under **Platform configurations**, click **Add a platform**.
   The **Configure platforms** section appears on the right side of the page.



3. Click **Mobile and desktop applications**.
   The **Configure Desktop + devices** section appears on the right side of the page.



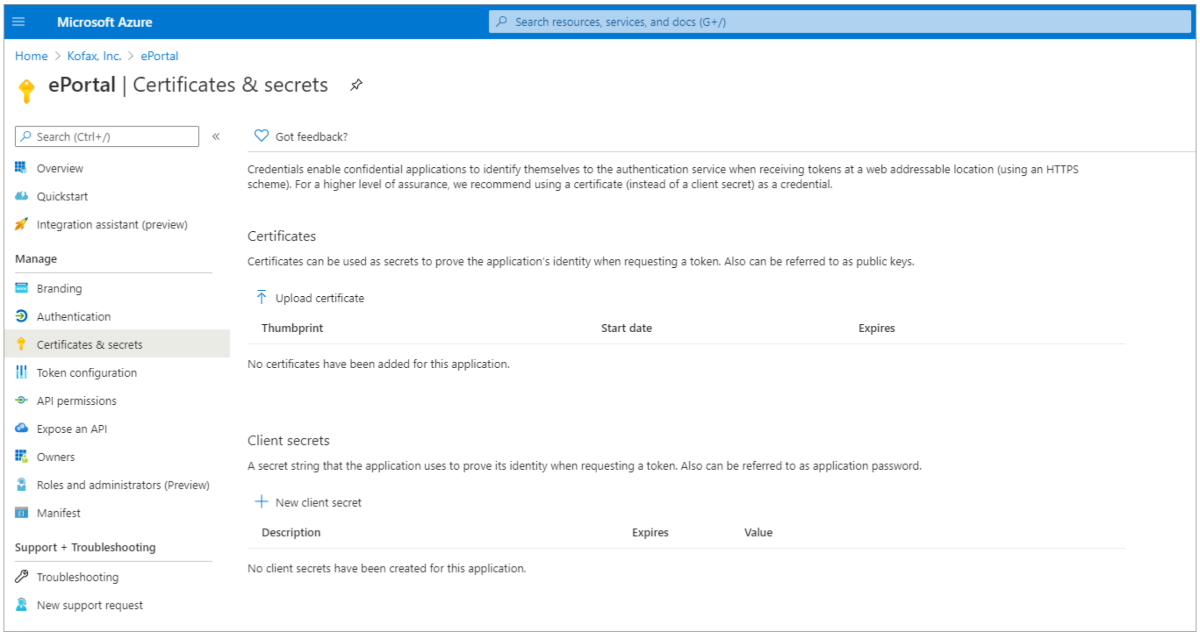
4. Select **https://login.microsoftonline.com/common/oauth2/nativeclient**, and click **Configure**.
   On the **Authentication** page, under **Redirect URIs**, you can see the selected option.



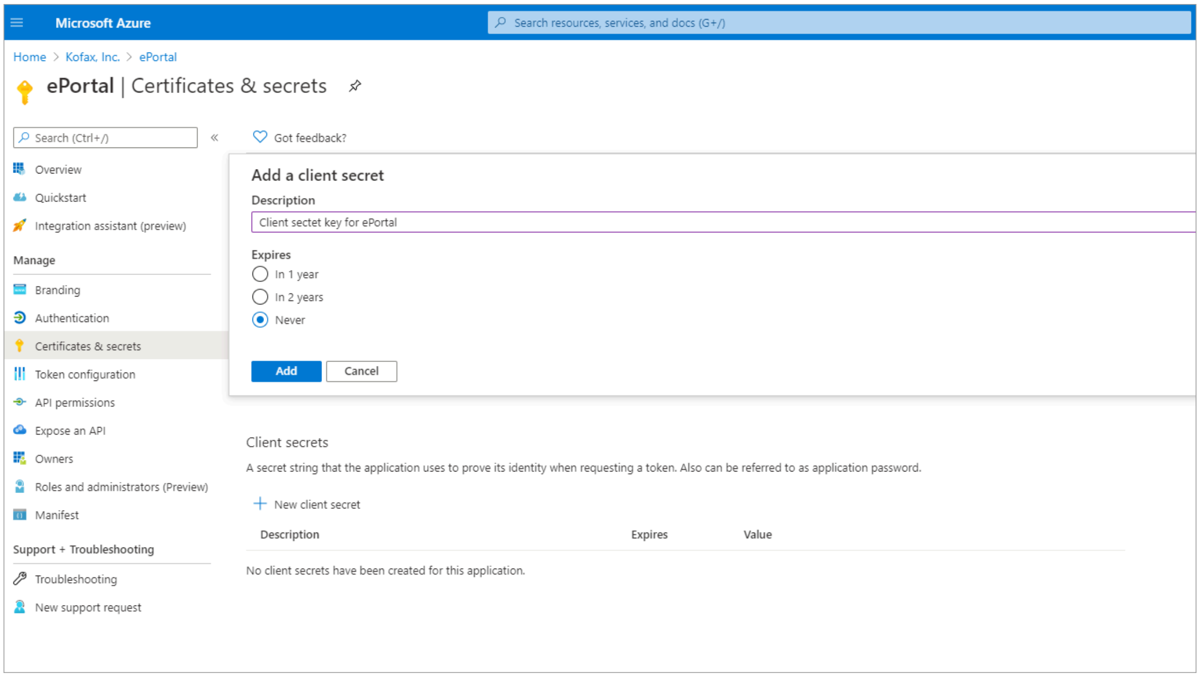
Manage certificates and secrets

Upload certificates or create client secrets to enable confidential applications.

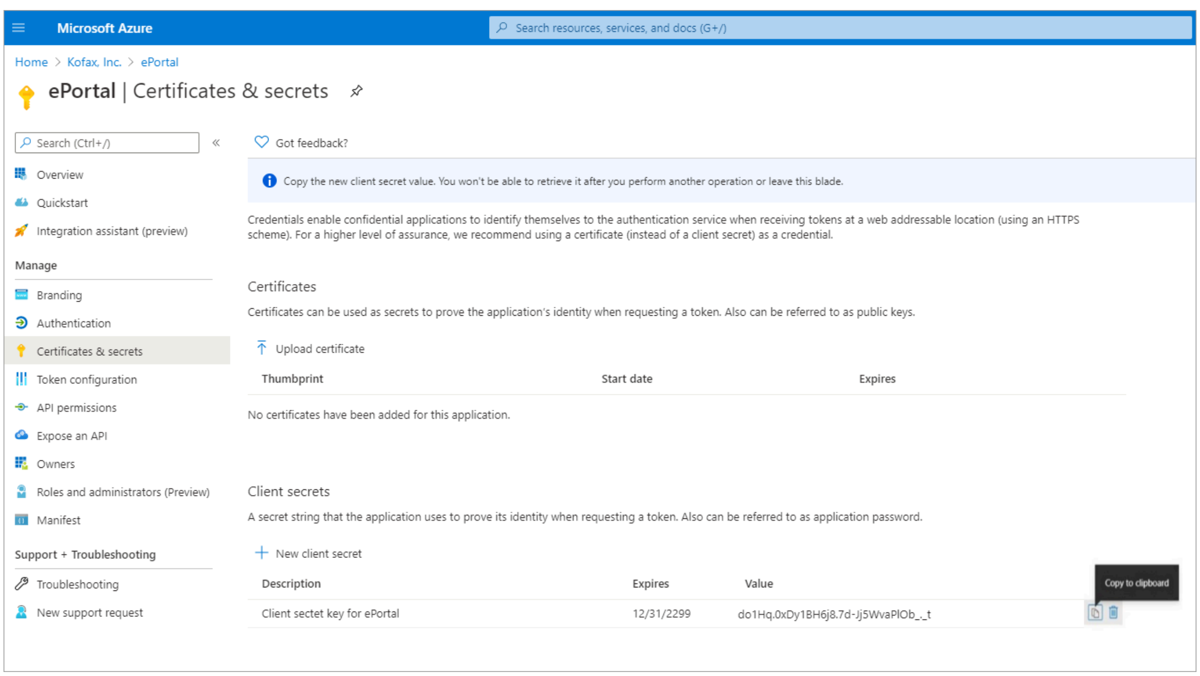
1. On the left sidebar, under **Manage**, click **Certificate & secrets**.
   The **Certificate & secrets** page appears.



2. Under **Client secrets**, click **New client secret**.
   The **Add a client secret** pop-up appears.



3. In the **Description** box, enter a description.
4. Under **Expires**, select **Never**.
5. Click **Add**.
   On the **Certificates & secrets** page, under **Client secrets**, you can see the client secret details.

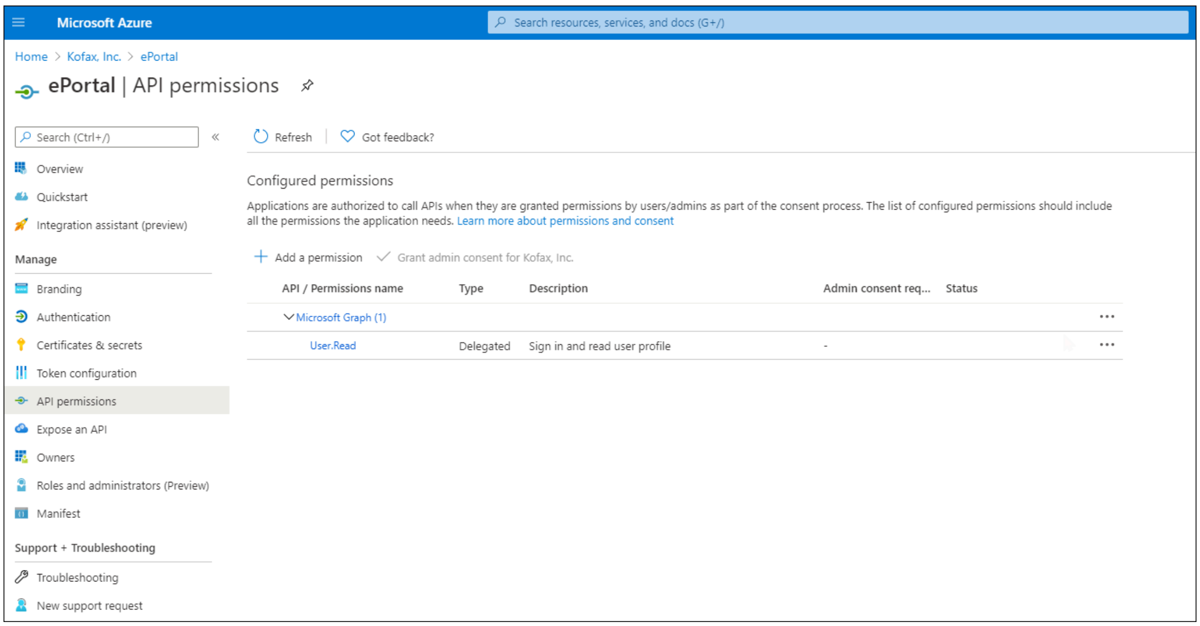


Note down the Client secrets value which can be referred in future activities.

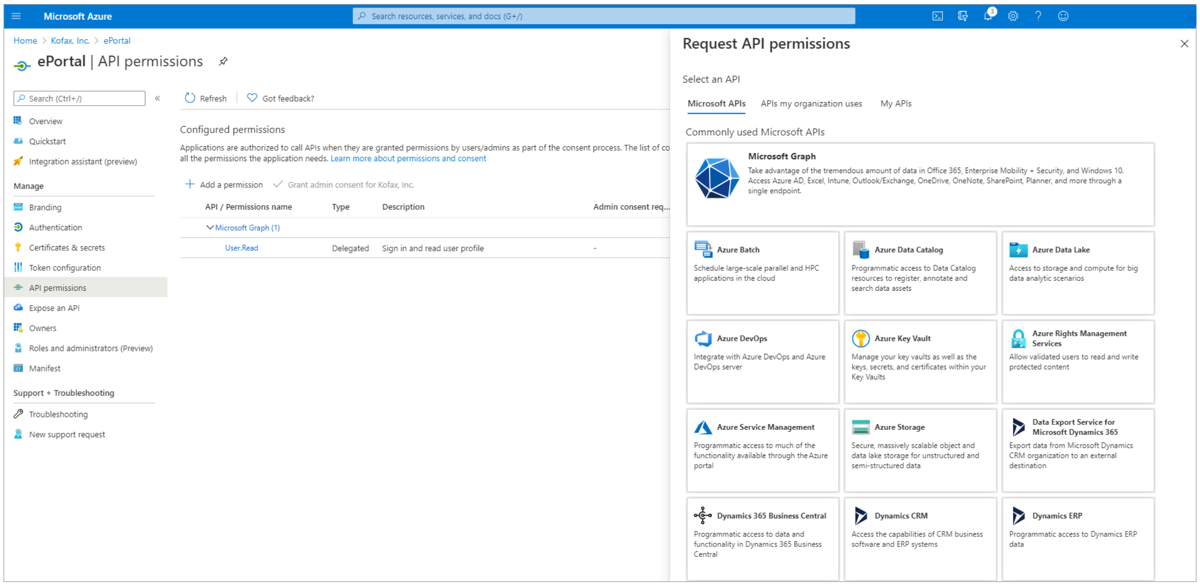
Manage API permissions

Add the required permissions to authorize applications to call APIs.

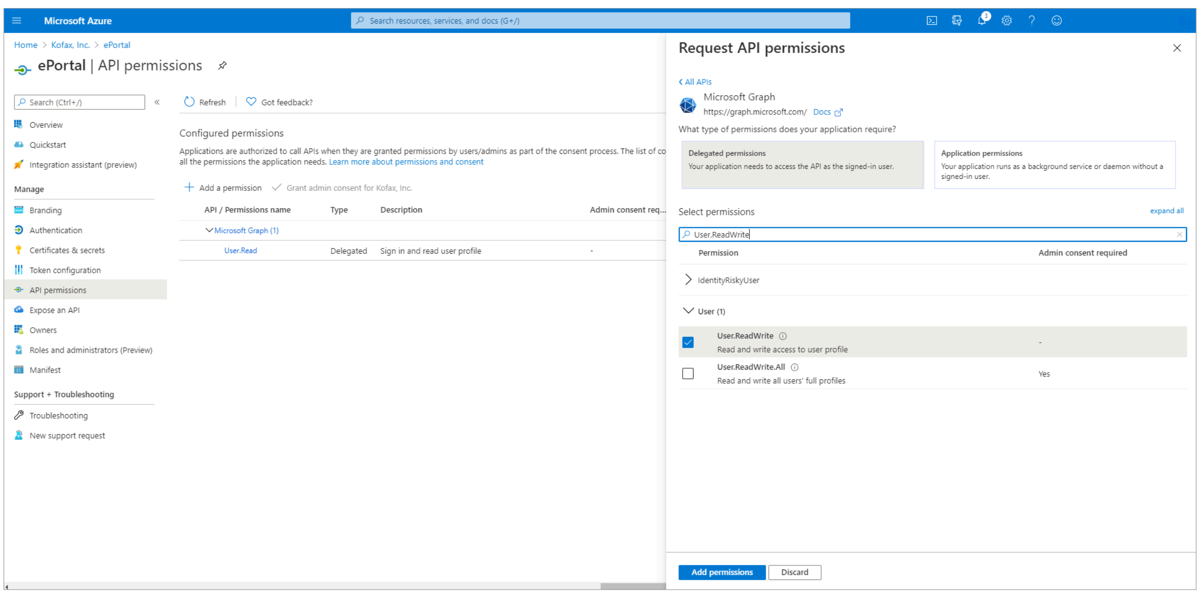
1. On the left sidebar, under **Manage**, click **API permissions**.
   The **API permissions** page appears.



2. Under **Configured permissions**, click **Add a permission**.
   The **Request API permissions** section appears on the right side of the page.

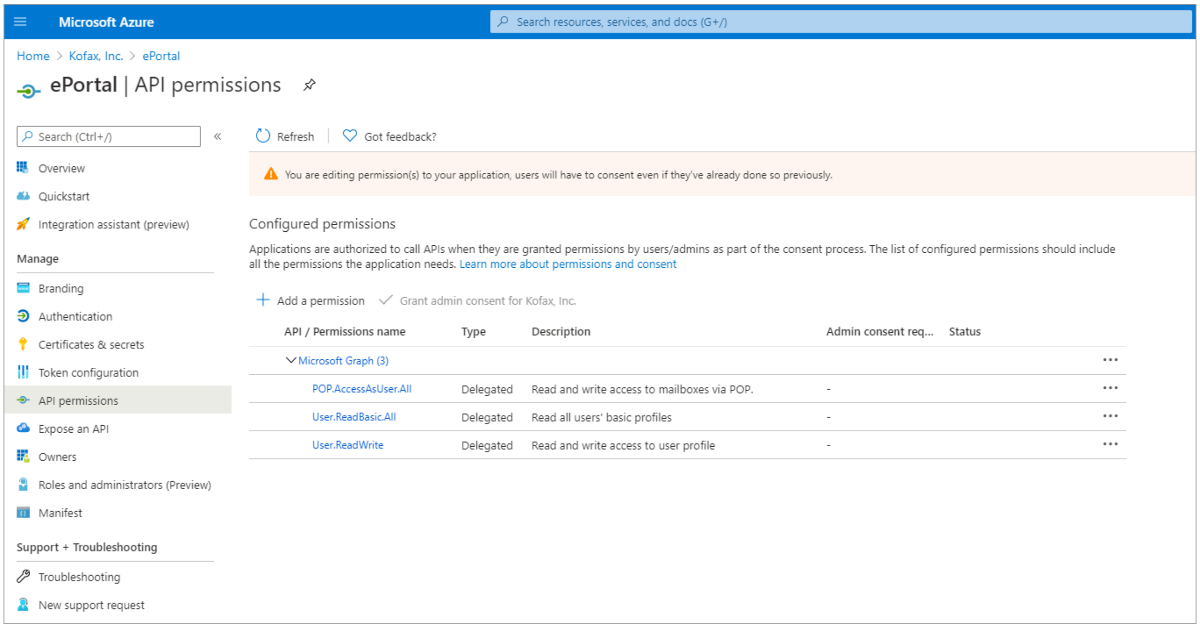


3. Click **Microsoft Graph**.



4. Click **Delegated permissions** > **Select Permission**, and then select the following three permissions.
   - Pop.AccessAsUser.All
   - User.ReadBasic.All
   - User.ReadWrite
5. Click **Add permissions**.

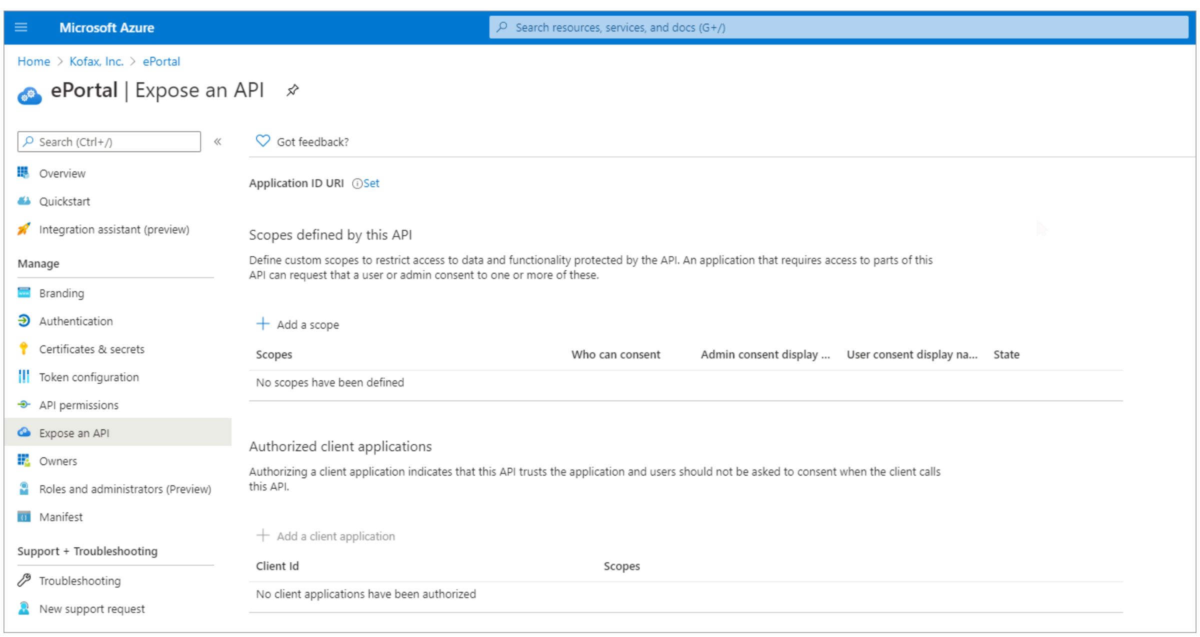
   On the **API permissions** page, under **API / Permissions name**, you can see all three permissions.



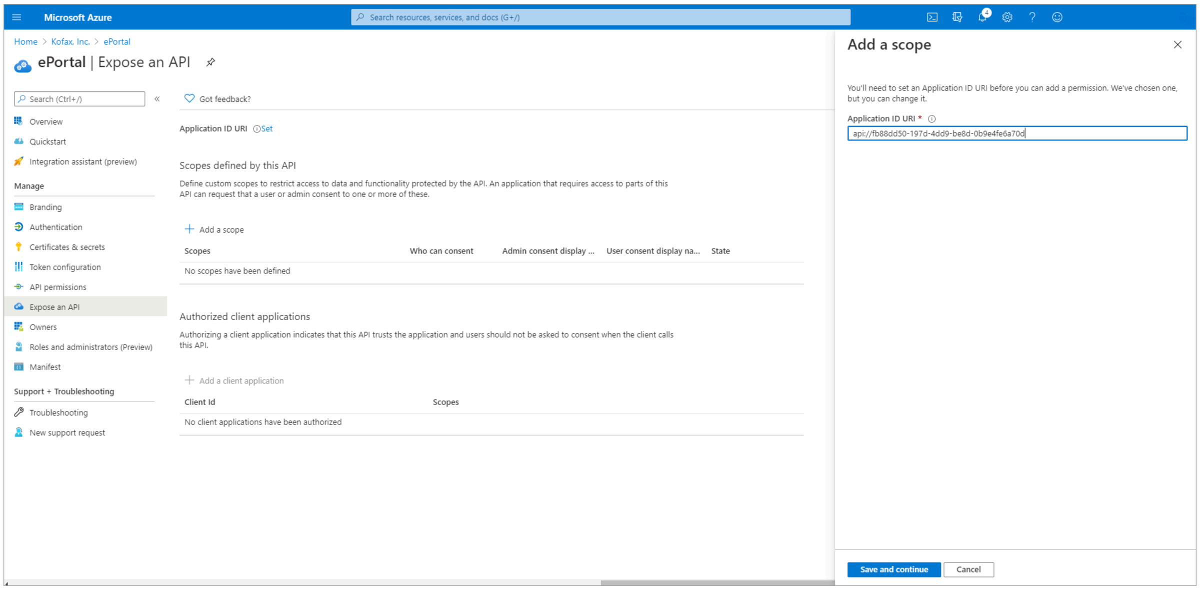
Manage exposing an API

Define the scope to allow or restrict access to data or functionality protected by an API.

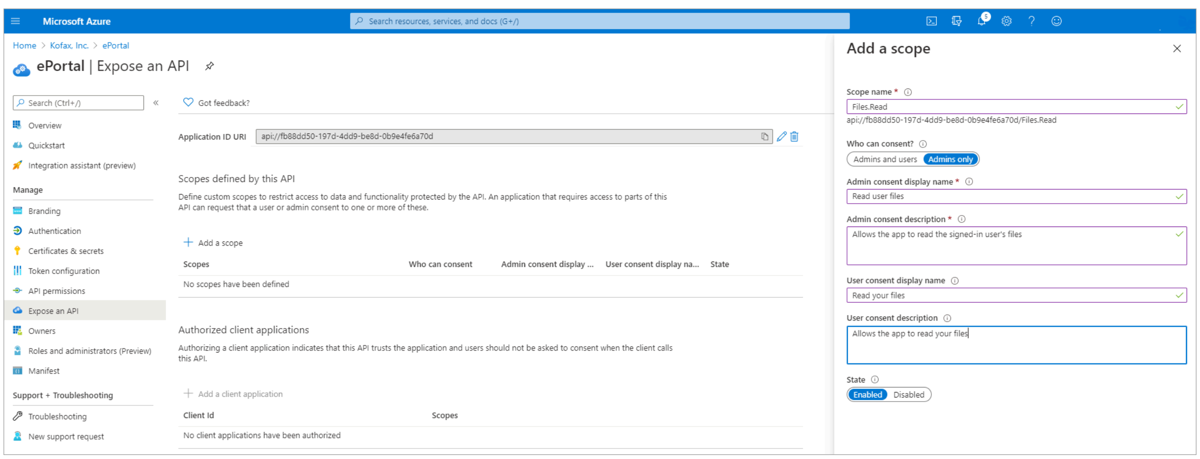
1. On the left sidebar, under **Manage**, click **Expose an API**.
   The **Expose an API** page appears.



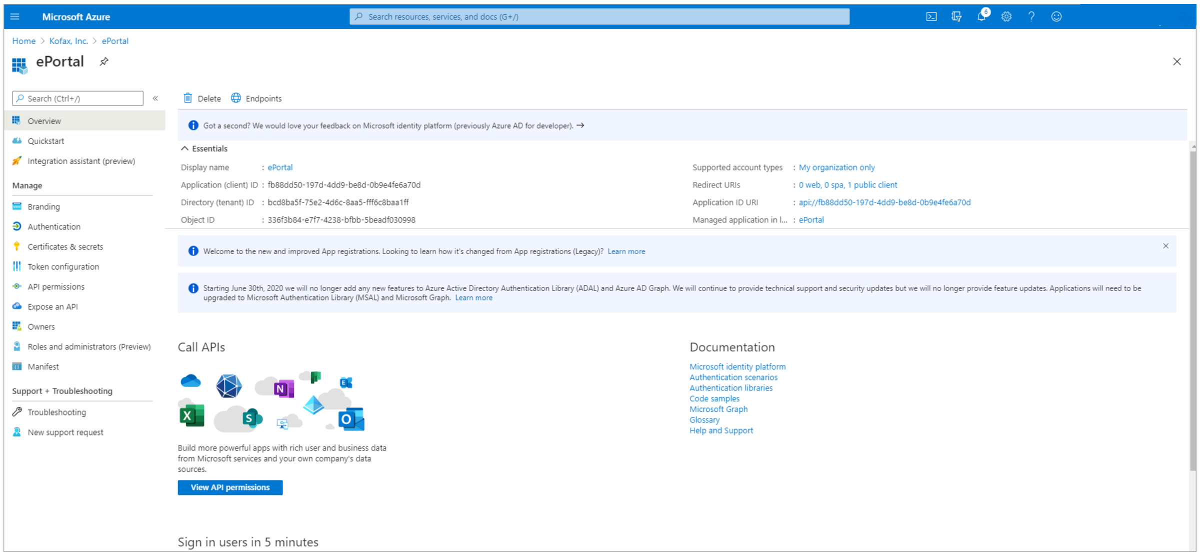
2. Under **Scopes defined by this API**, click **Add a scope**.
   The **Add a scope** section appears on the right side of the page.



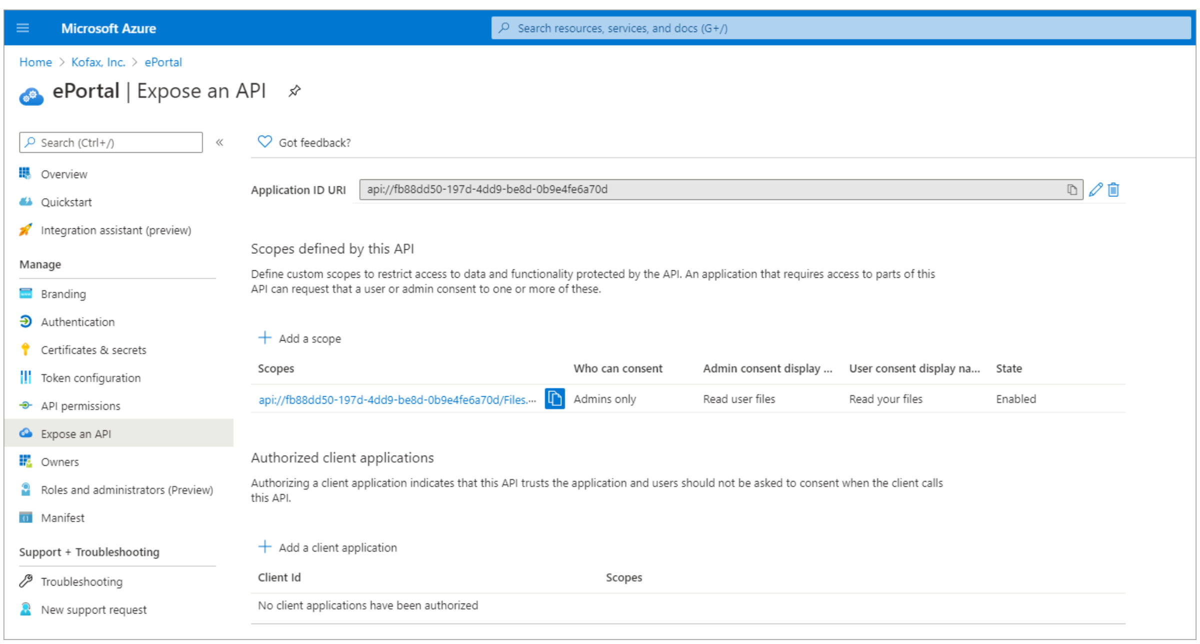
3. Click **Save and continue**.



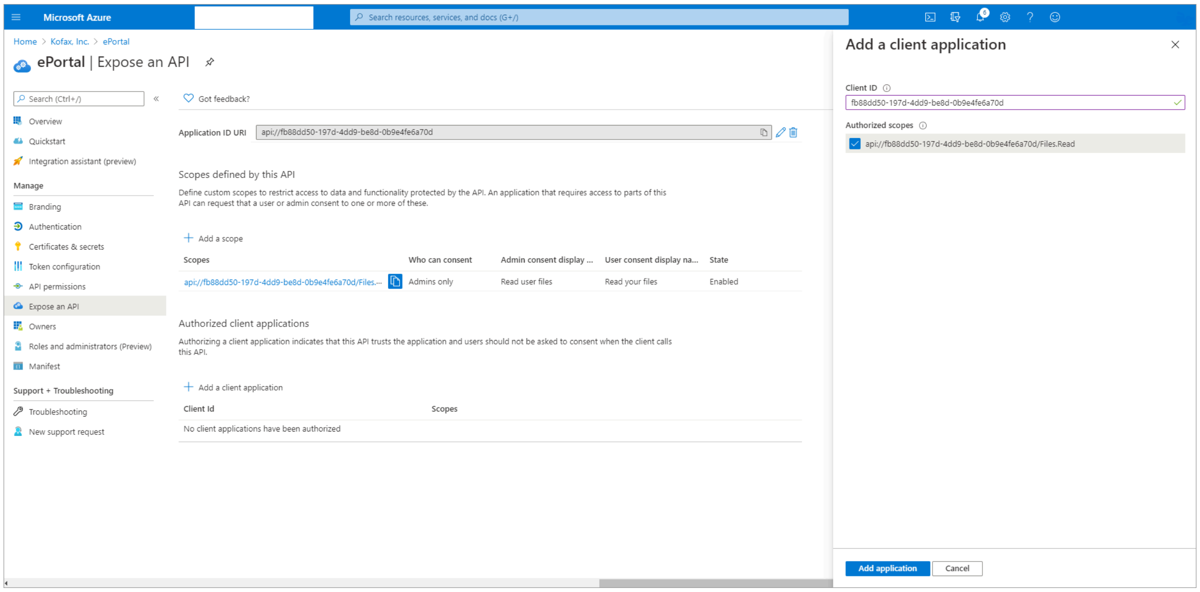
4. For **Who can consent?**, select **Admins only**.
5. For **State**, select **Enabled**.
6. Click **Add scope**.
7. On the left sidebar, click **Overview**.
   The **Overview** page appears.



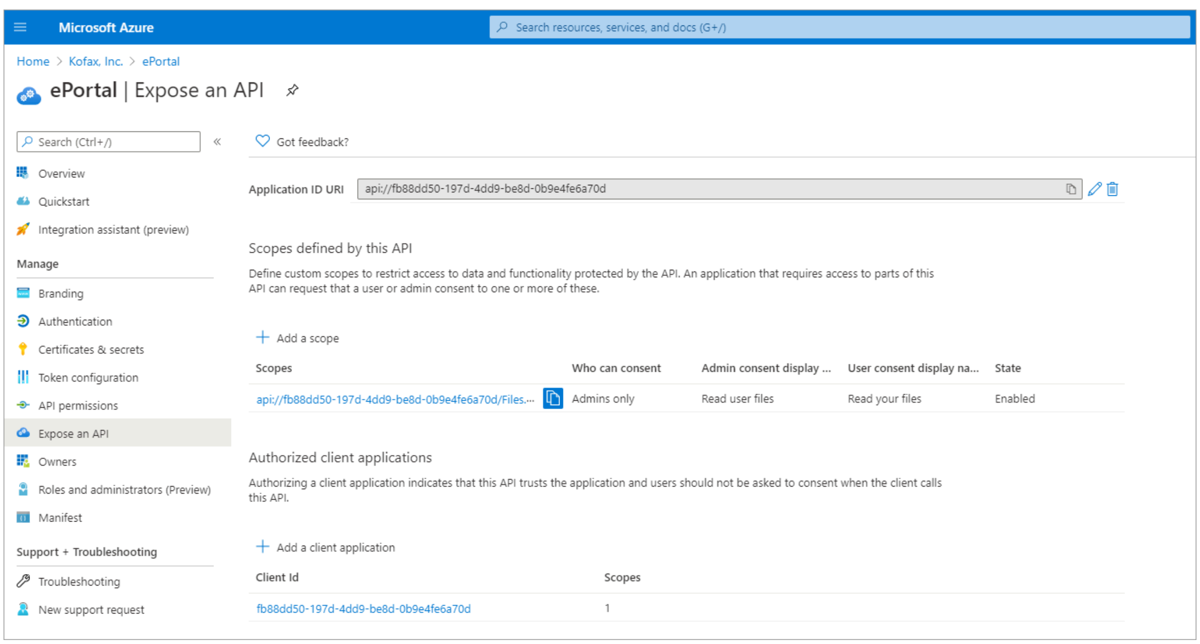
8. Note down the **Application (client) ID**.
9. On the left sidebar, click **Expose an API**.
   The **Expose an API** page appears.



10. Under **Authorized client applications**, click **Add a client application**.
    The **Add a client application** section appears on the right side of the page.



11. In the **Client ID** field, paste the copied client ID.
12. Under **Authorized scopes**, select the check box.
13. Click **Add application**.
    You can see that the required values are available on the **Expose an API** page.

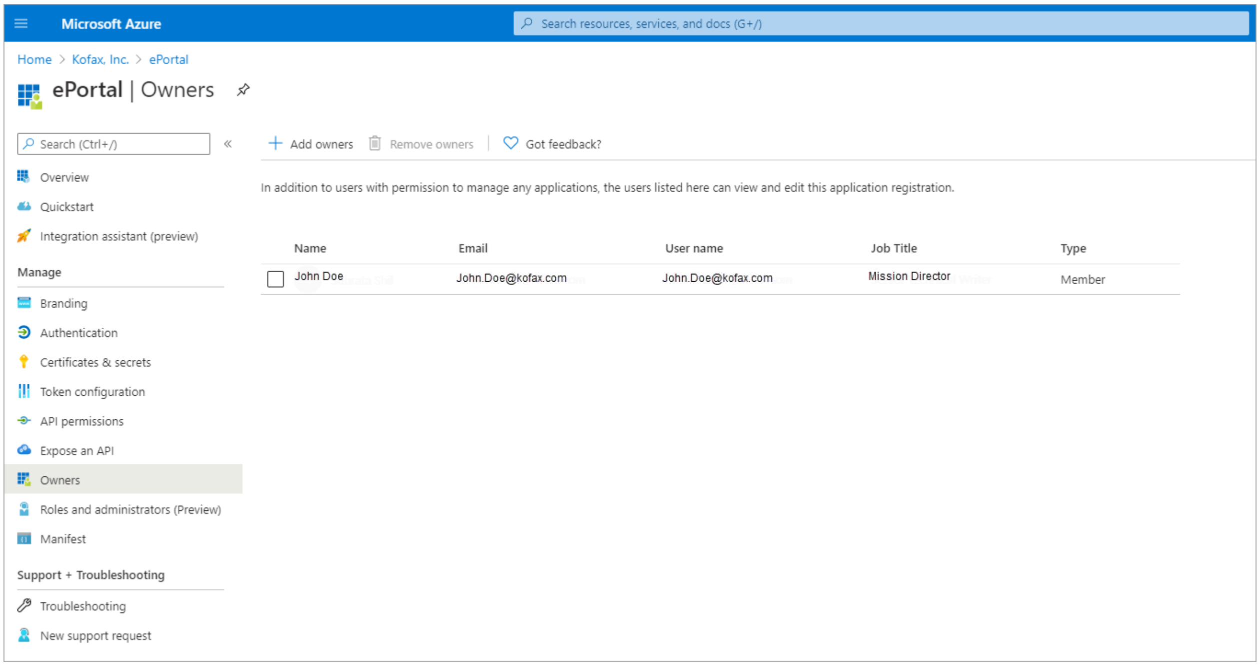


Manage owners

Use the **Owners** page to see the owners of ePortal.

On the left sidebar, under **Manage**, click **Owners**.

The **Owners** page appears.

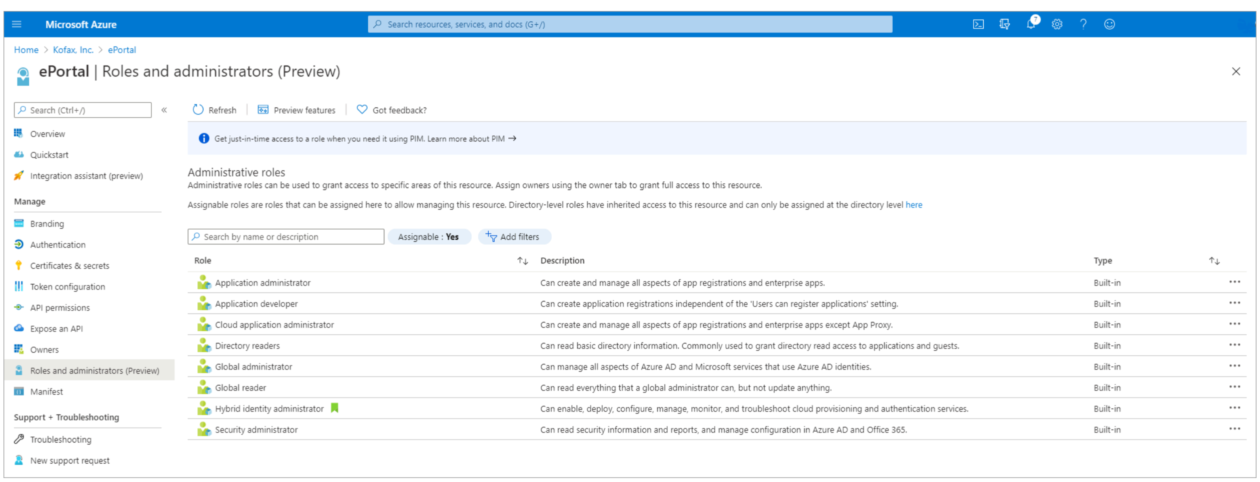


An admin can add more than one owner.

Manage roles and administrators (Preview)

Use the **Roles and administrators (Preview)** page to see the various administrative roles. On the left sidebar, under **Manage** click **Roles and administrators (Preview)**.

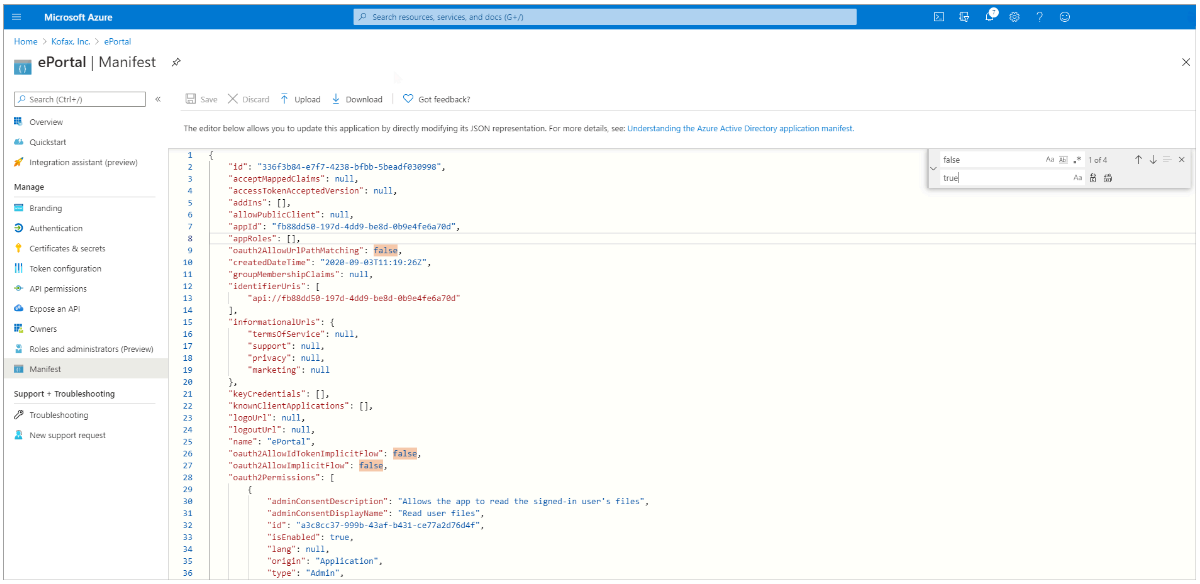
The **Roles and administrators (Preview)** page appears.



Manage manifest

Use the Manifest page to update the application by directly modifying its JSON representation.

1. On the left sidebar, under **Manage**, click **Manifest**.
   The **Manifest** page opens with an editor.

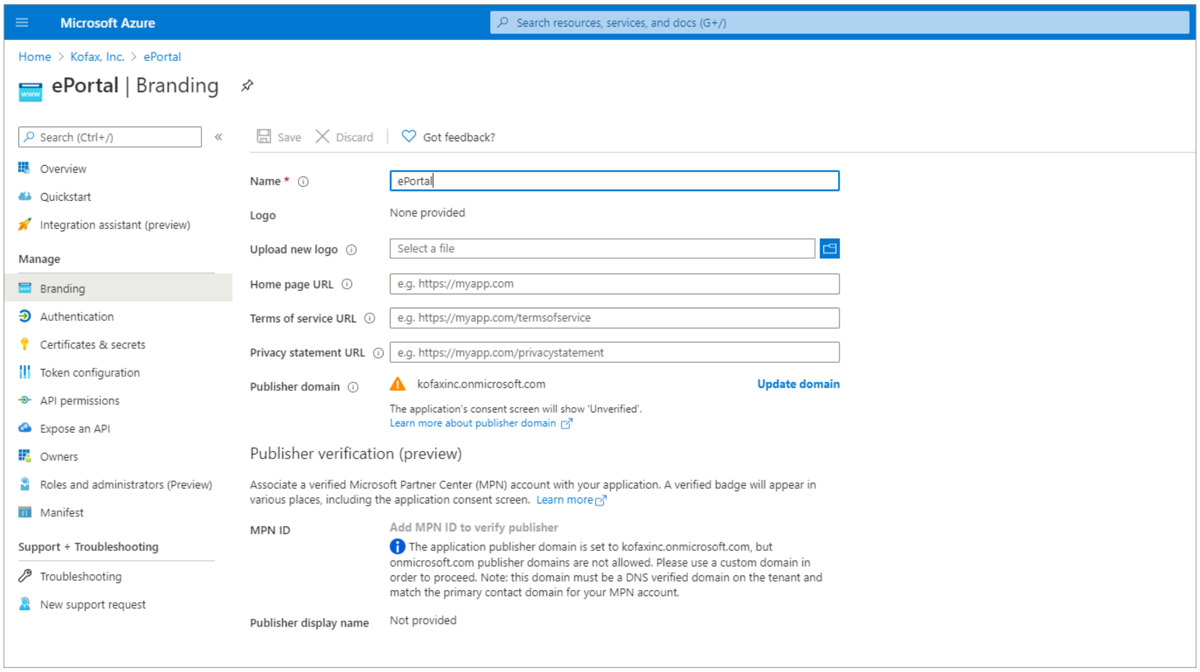


2. Replace "false" with "true" for all the occurrences and click **Save**.

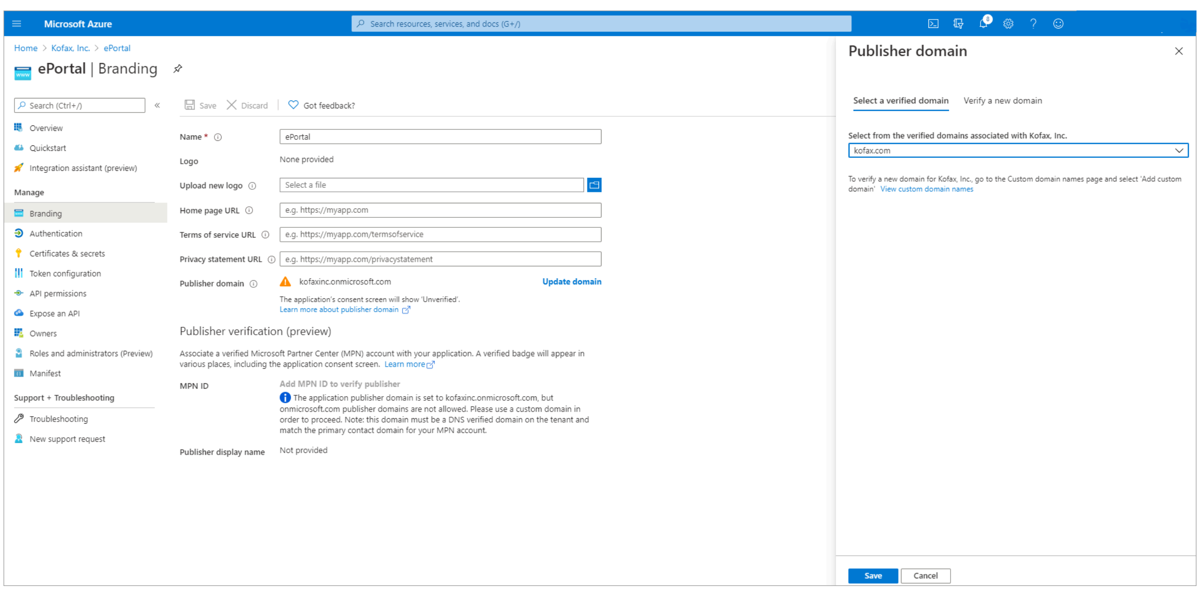
Manage branding

The Branding page lets you define the logo, Home page URL, Terms of service URL, and other branding details.

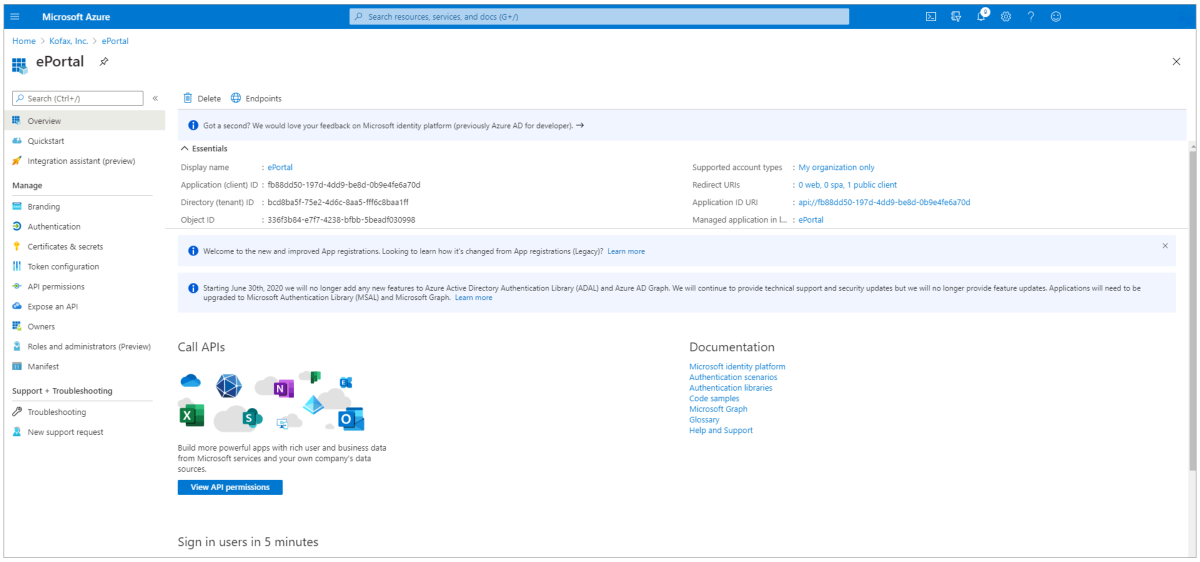
1. On the left sidebar, under **Manage**, click **Branding**.
   The **Branding** page appears.



2. Optional. To upload a new logo, click and select the logo you want to upload.
3. Click **Update domain**.
   The **Publisher domain** section appears on the right side of the page.



4. On the **Select a verified domain** tab, select a domain that is associated with your organization from the list.
5. Click **Save**.
6. On the left sidebar, click **Overview**.
   The **Overview** page appears.



7. Note down the **Application (client) ID** and **Directory (tenant) ID** for future reference.

Configure EPortal.AppConfig

Configure the EPortal.AppConfig file for your email account.

1. Copy the following XML content.

```
<MailAccount Id = "pop3_oauth_outlook" DisplayName="pop3_oauth_outlook"
       Host="outlook.office365.com" Port="995" SSL="true"
 IgnoreCertificateErrors="false"
       UserName="abc.xyz@kofax.com" Protocol="POP3_OAUTH"
 TenantID="bcd8ba5f-75e2-4d6c-8aa5-fff6c8baa1ff"
 ClientID="ce82dd43-79c0-4445-957e-54f4e2ce430b">
       <MailEncoding>UTF-8</MailEncoding>
       <DefaultCharset>UTF-8</DefaultCharset>
       <Folders>
       <Folder>INBOX</Folder>
       </Folders><Filter />
       <Impersonate Enabled = "false" />
  </ MailAccount >
```

> Host for pop3 outlook is outlook.office365.com.

2. Open the EPortal.AppConfig file located at `C:\ProgramData\TIS\<eFlow6>\AppData\Server\<Application_name>\Setup`, and paste the copied content under the `<MailAccounts/>` section.
3. Change the ID, DisplayName, UserName, TenantID, and ClientID.
4. Copy the following XML content.

```
<ActiveAccount Id="pop3_oauth_outlook" Enabled="true" />
```

5. In the EPortal.AppConfig file under `<ActiveAccounts>` section, paste the copied content, and save the file.

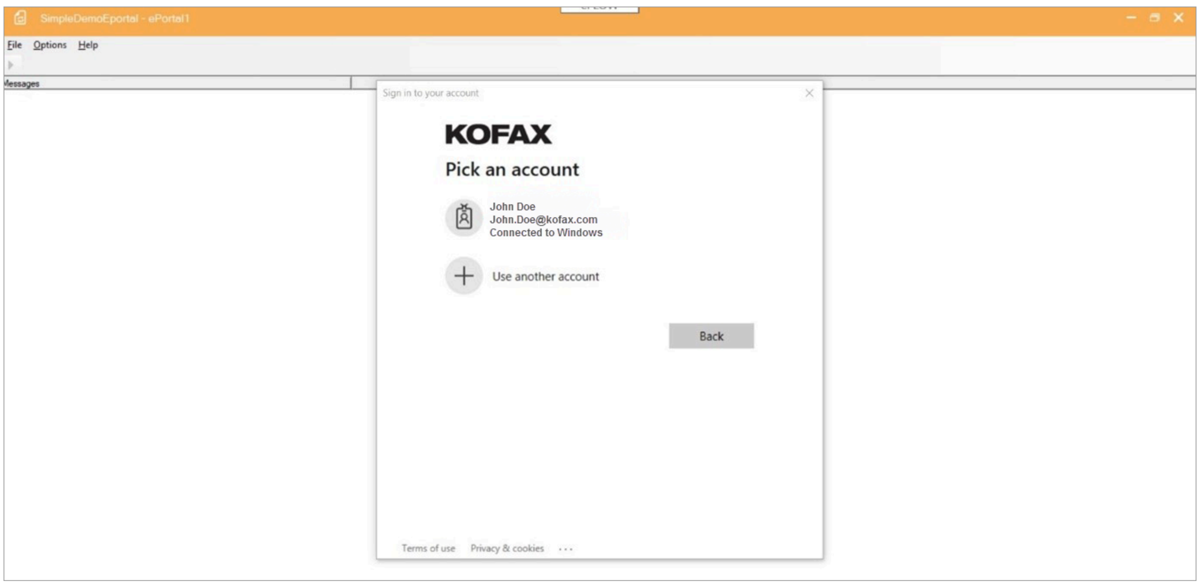
Run the ePortal manual station

Do the following to run the ePortal manual station.

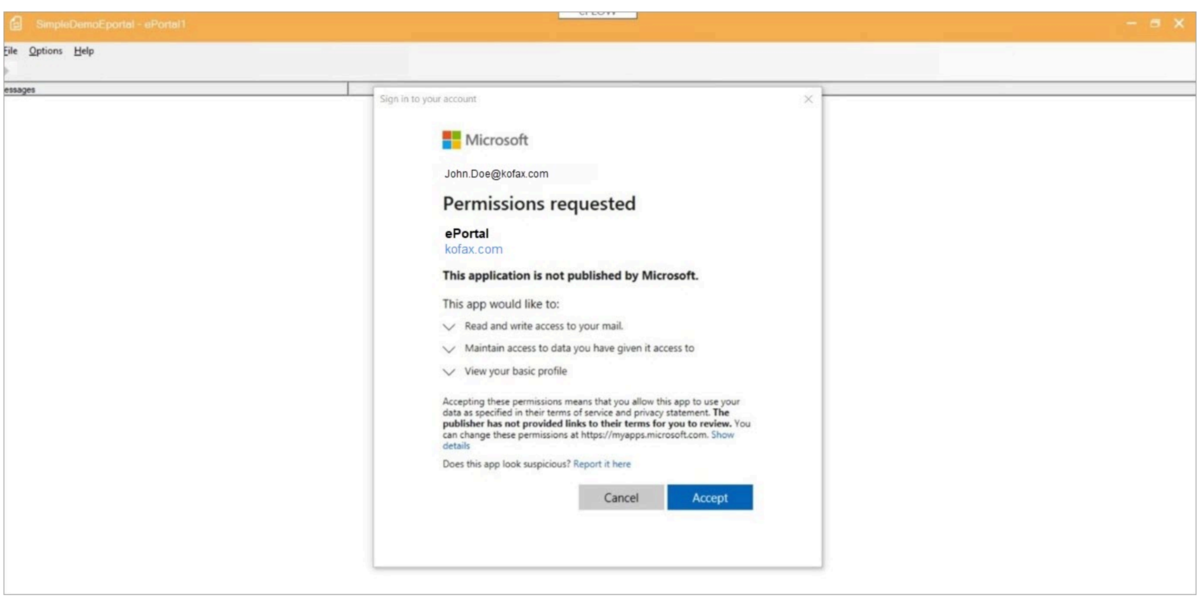
1. In the **eFlow LaunchPro**, from the **Stations** list, select **ePortal manual station**.

   If your default browser is Internet Explorer, make sure that JavaScript is enabled.

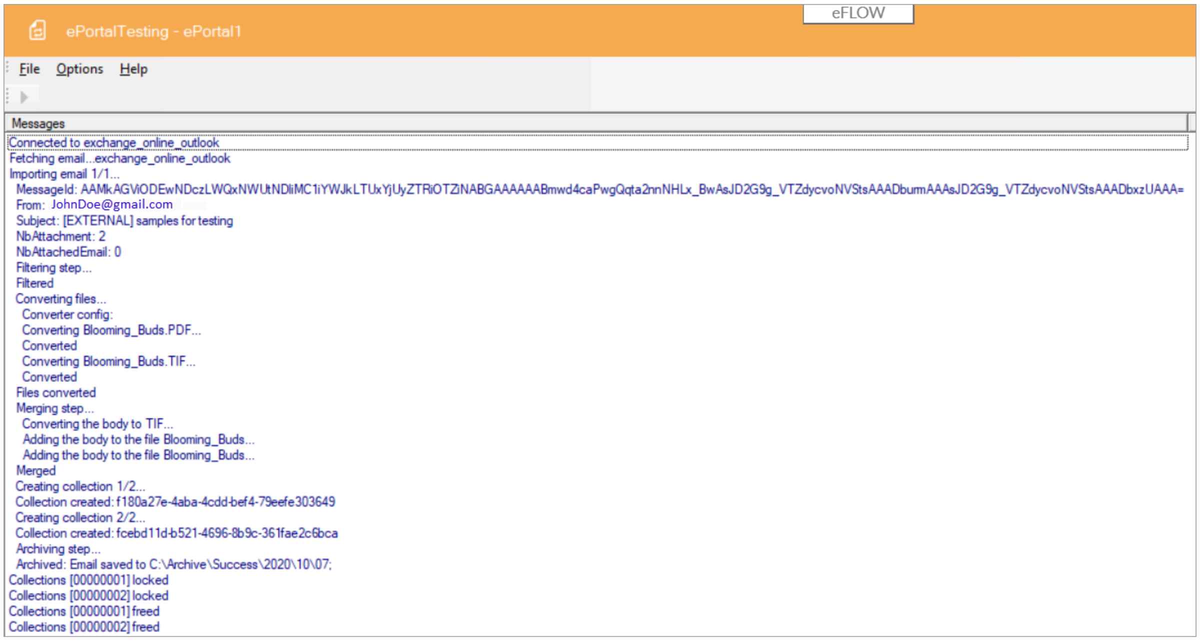
2. If the username (email id) for Outlook is not configured in the EPortal.AppConfig file for the computer using ePortal, the following page appears.



3. Select an account, and then type your password to sign in.
   After a successful sign-in, the following page appears.



4. Click **Accept**.
5. After accepting the permission, the **ePortal Manual station** starts fetching the Outlook messages from the configured folder.



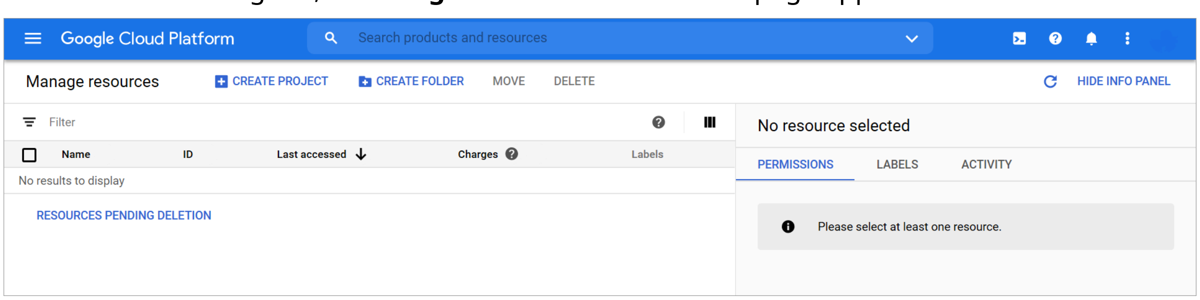
Google cloud configuration for Gmail

You can create a new project, enable, and configure it for Gmail.

The figures and user interfaces used in the following procedure are taken from Google's website and they might change occasionally. Hence, we request you to follow the latest procedure mentioned in Google's website, which is updated time-to-time. If you still face issues while authorizing your application, we recommend you to take assistance from a user who has expertise in authorizing an application.

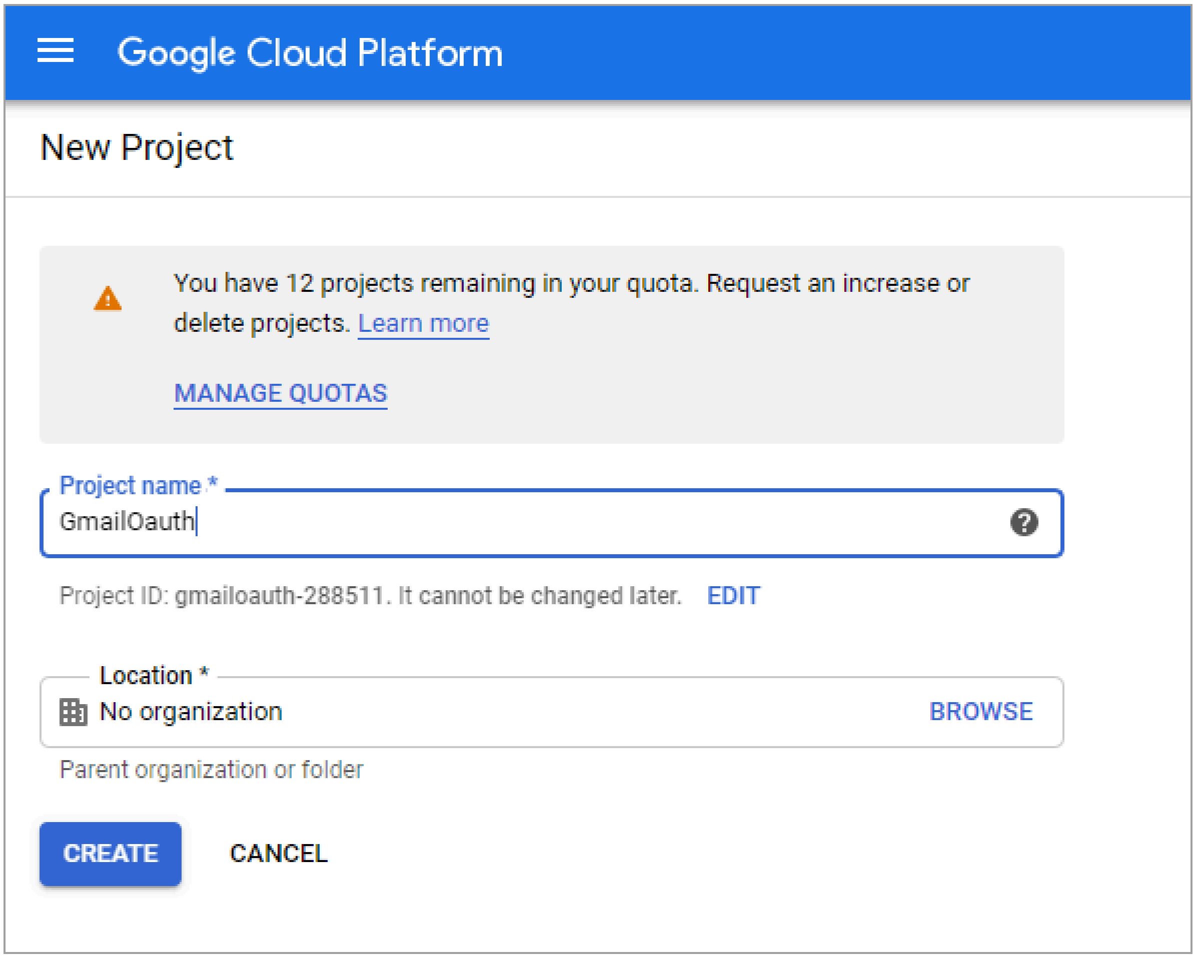
1. Go to https://console.cloud.google.com and follow the on-screen instructions to sign into the Google Cloud Platform.

   After a successful sign-in, the **Google Cloud Platform** main page appears.

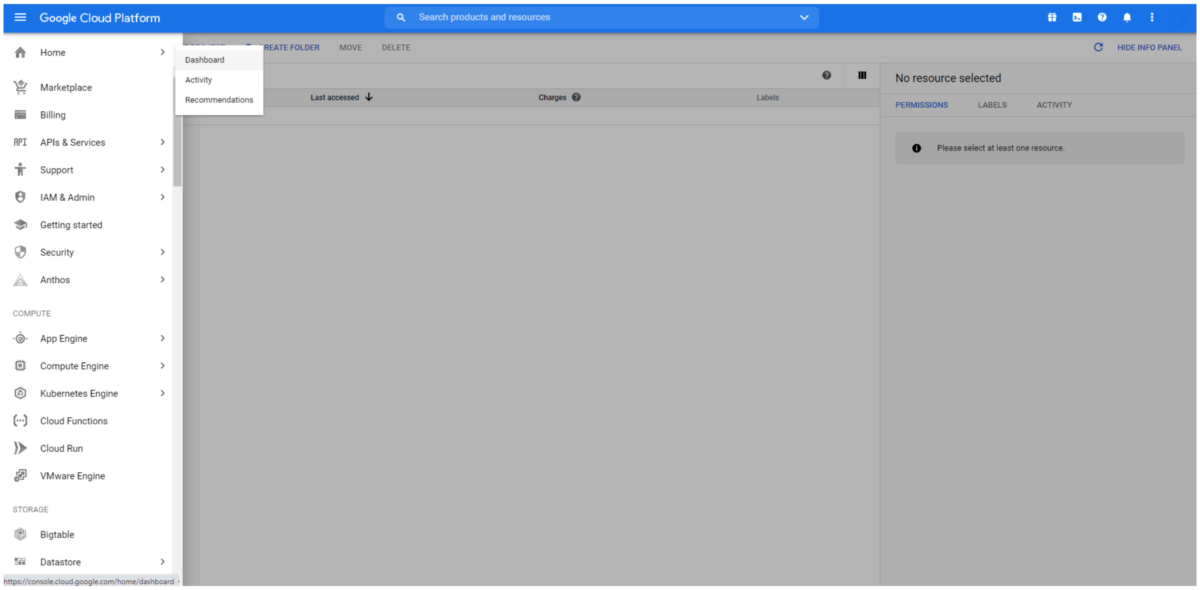


2. On the **Google Cloud Platform** main page, click **CREATE PROJECT**.

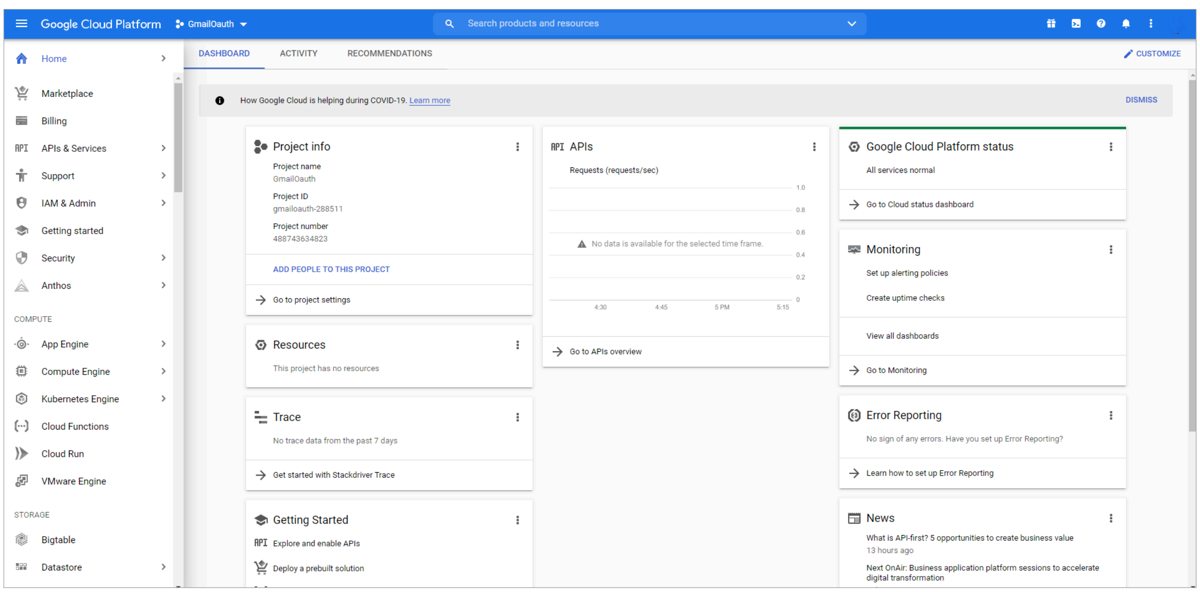
The **New Project** page appears.



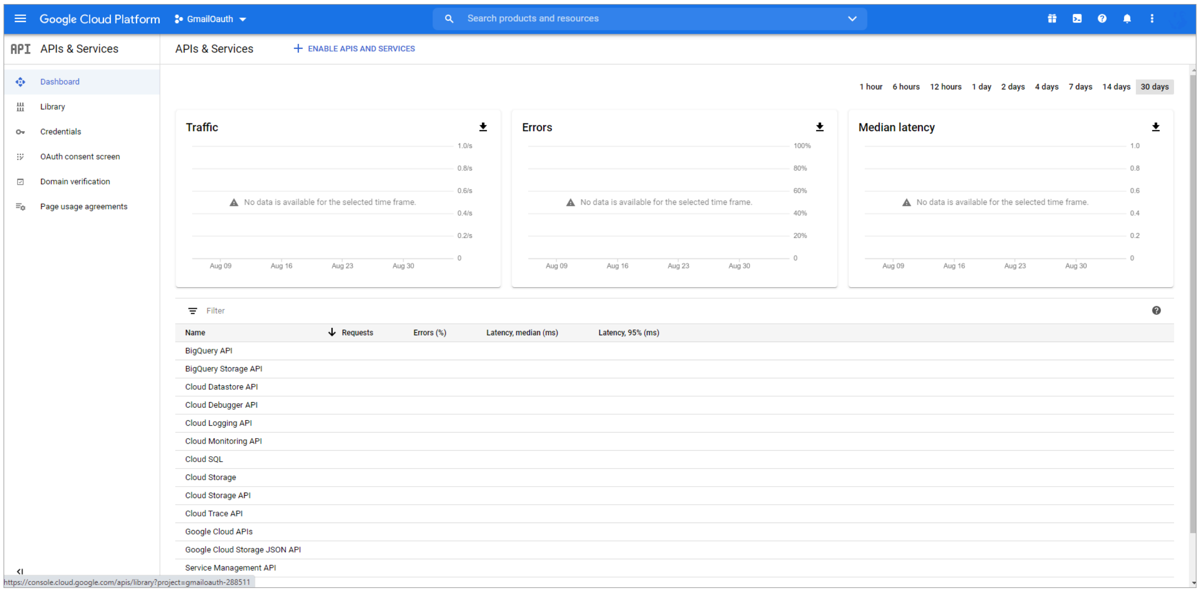
3. In the **Project name *** field, type a name for the project.
4. In the **Location** field, select the location as "No organization".
5. Click **CREATE**.
   The following page appears.



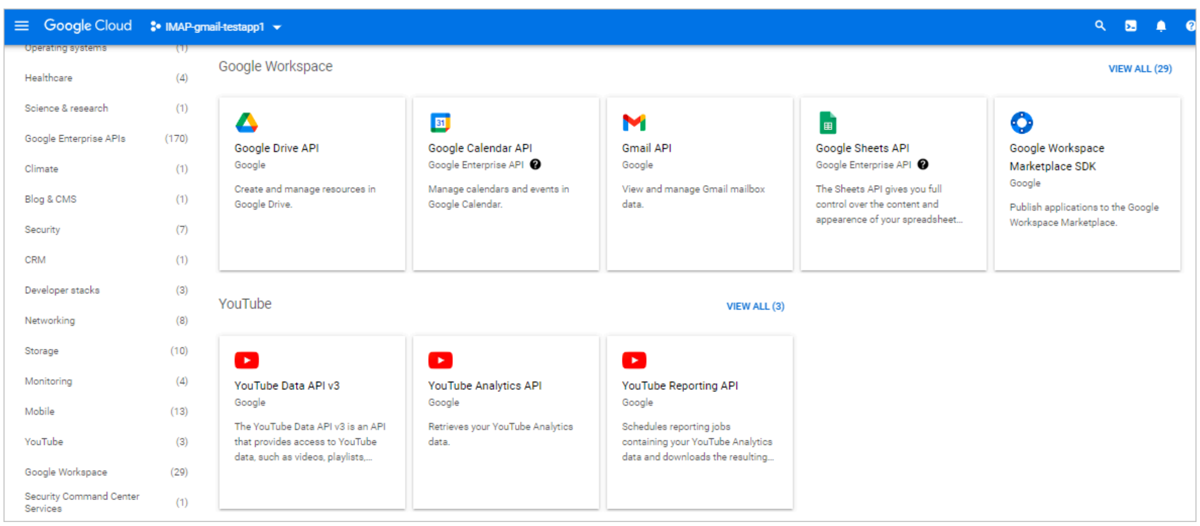
6. On the left sidebar, select **Home** > **Dashboard**.
   The **Dashboard** page appears.



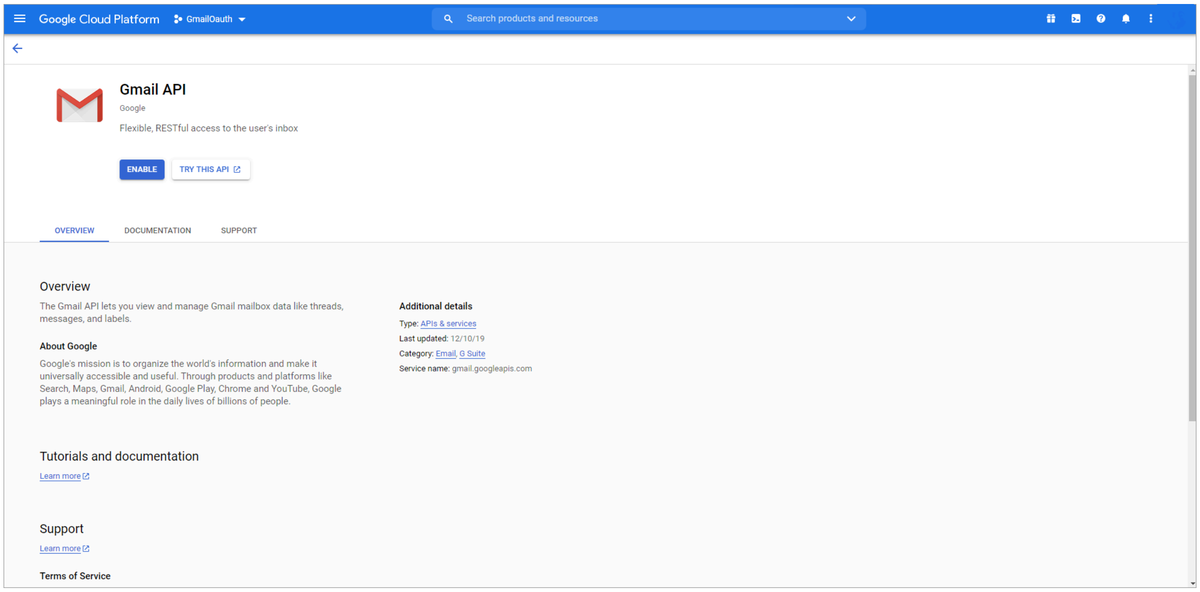
7. Under **Getting Started**, click **Explore and enable APIs**.
   The **APIs & Services** page appears.



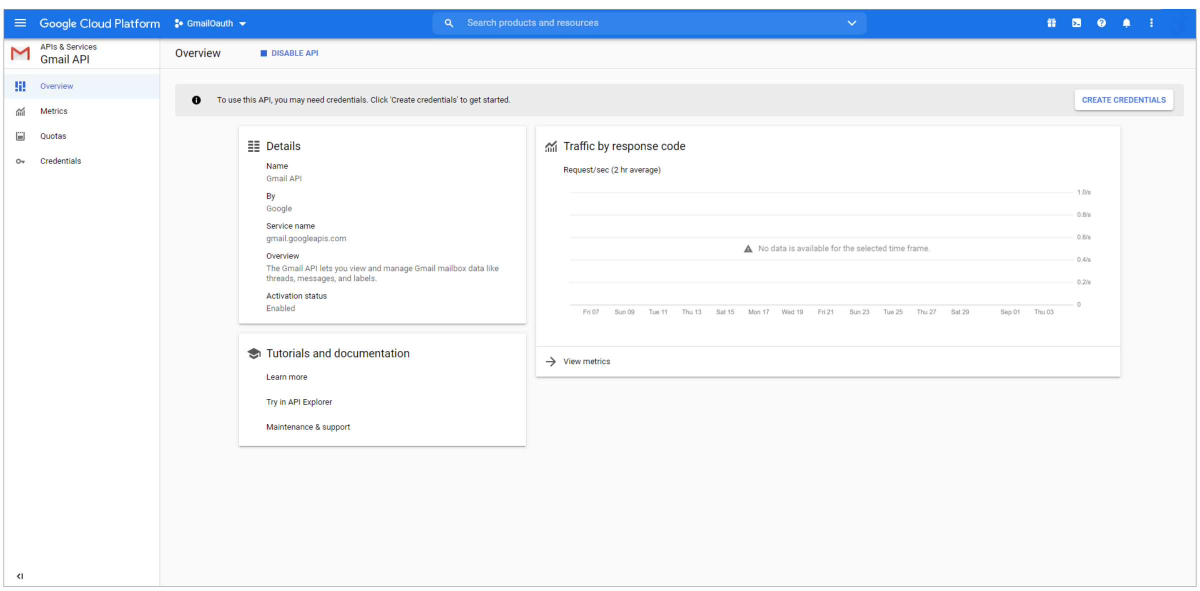
8. On the left sidebar, click **Library**.
   The **API Library** page appears.



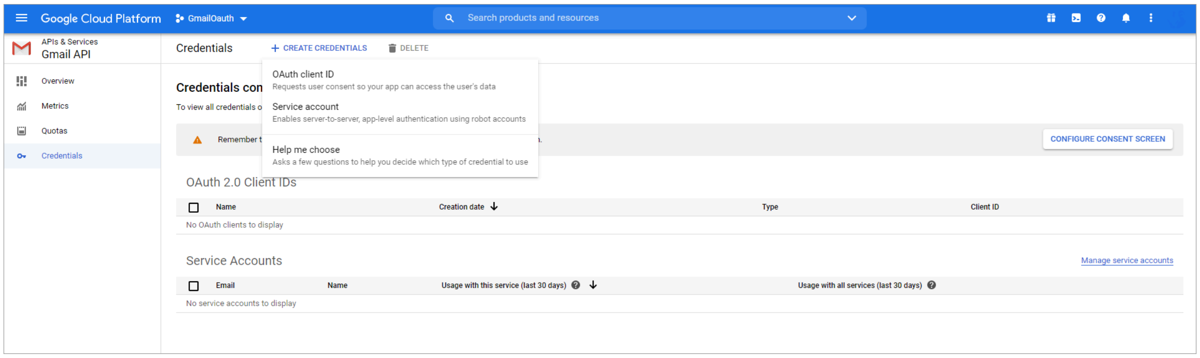
9. Under **Google Workspace**, click **Gmail API**.
   The **Gmail API** page appears.



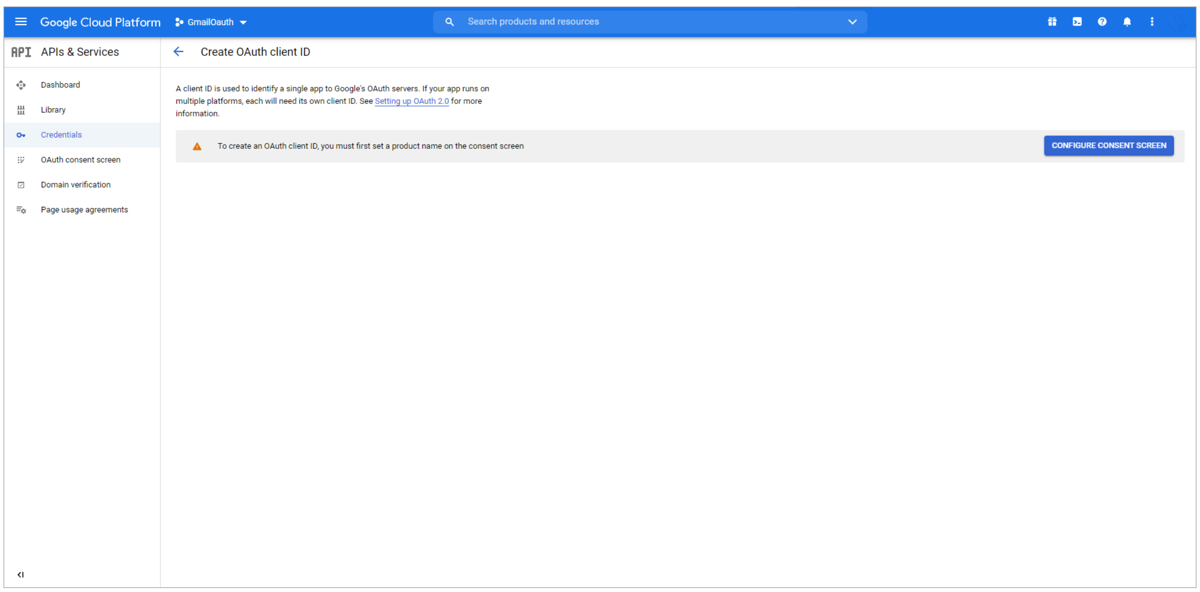
10. Click **Enable**.
    The **Overview** page appears.



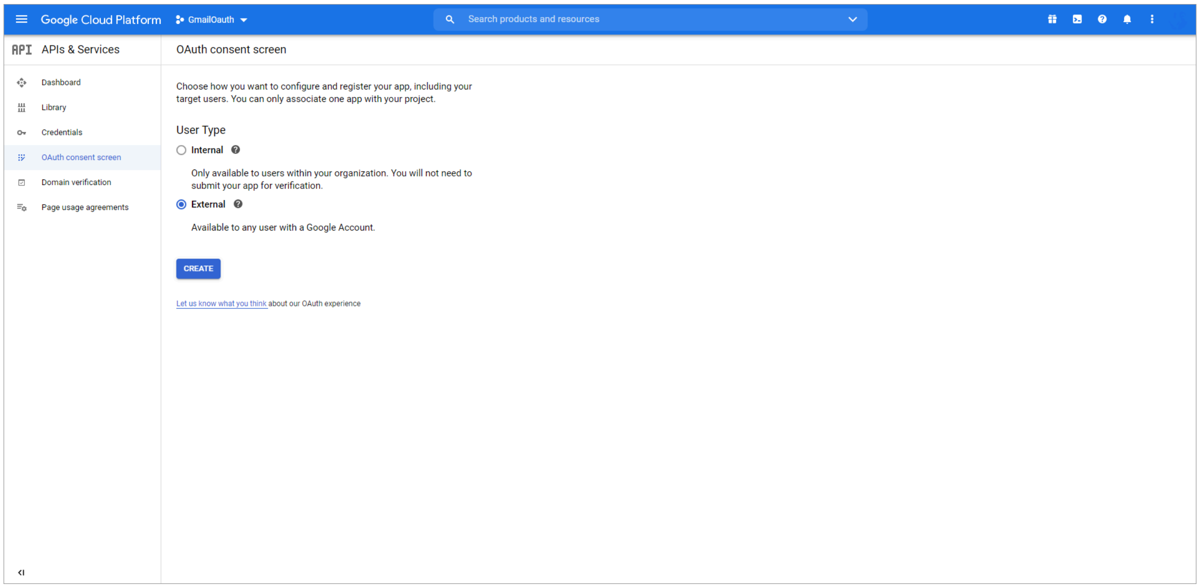
11. On the left sidebar, click **Credentials**.
    The **Credentials** page appears.



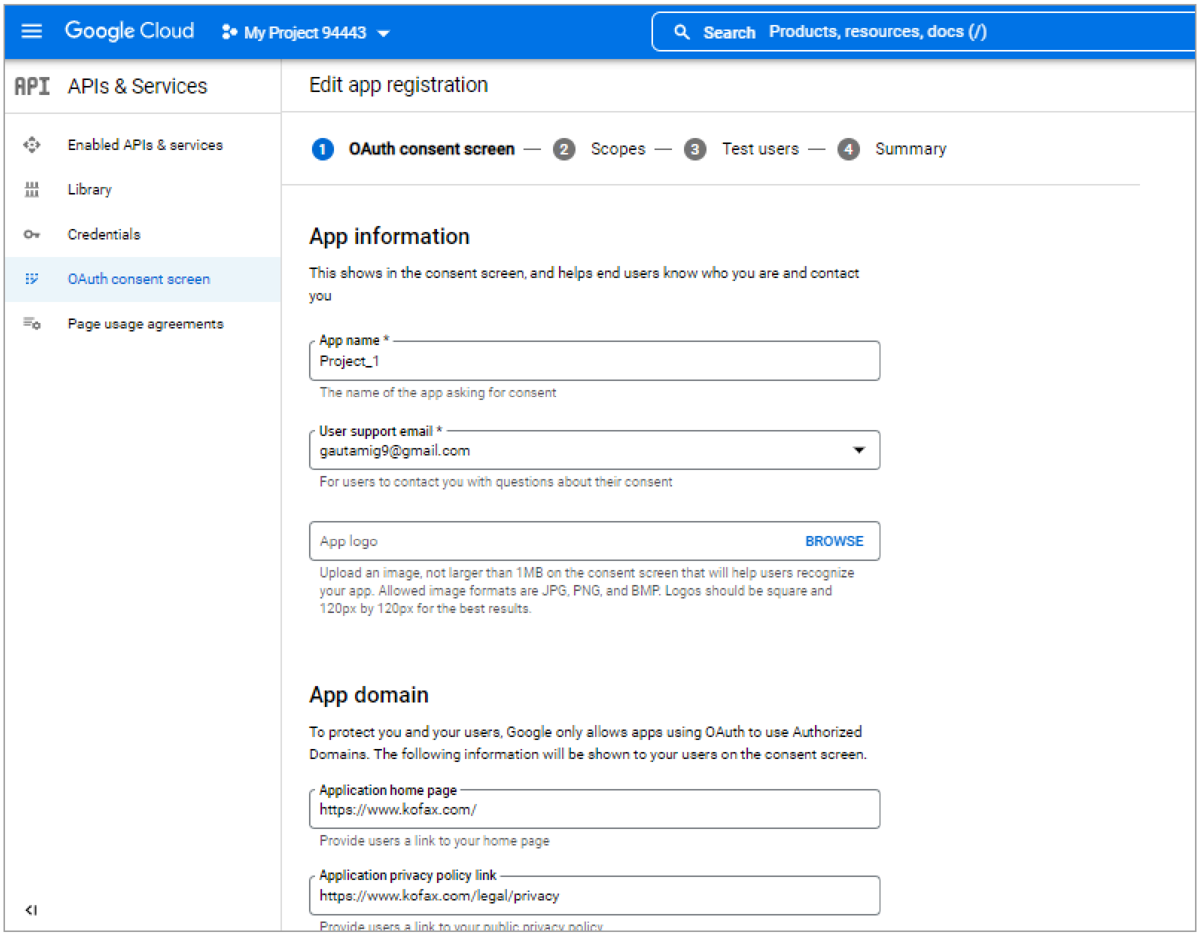
12. Click **CREATE CREDENTIALS** > **OAuth client ID**.
    The **Create OAuth client ID** page appears.



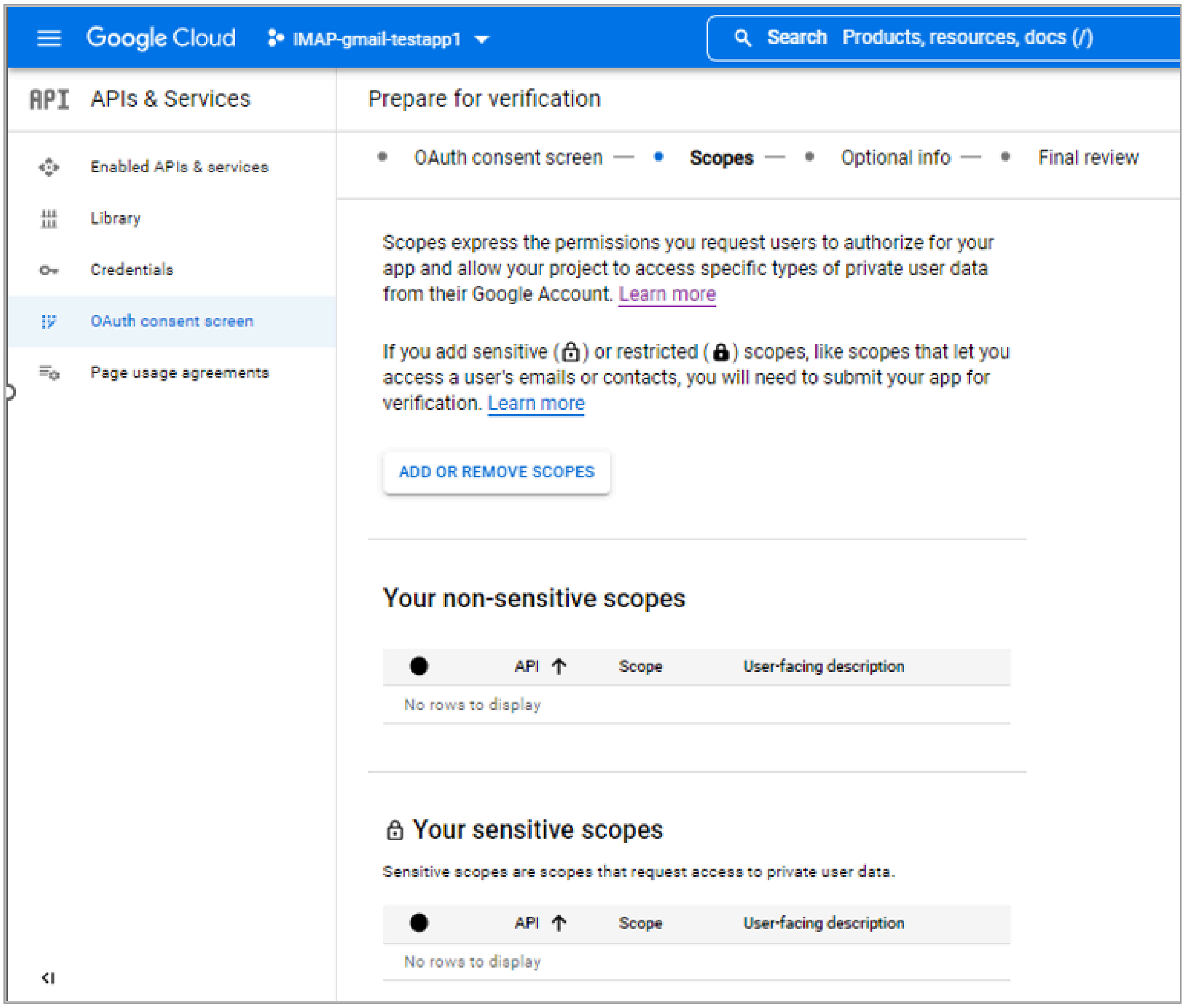
13. Click **CONFIGURE CONSENT SCREEN**.
    The **OAuth consent screen** page appears.



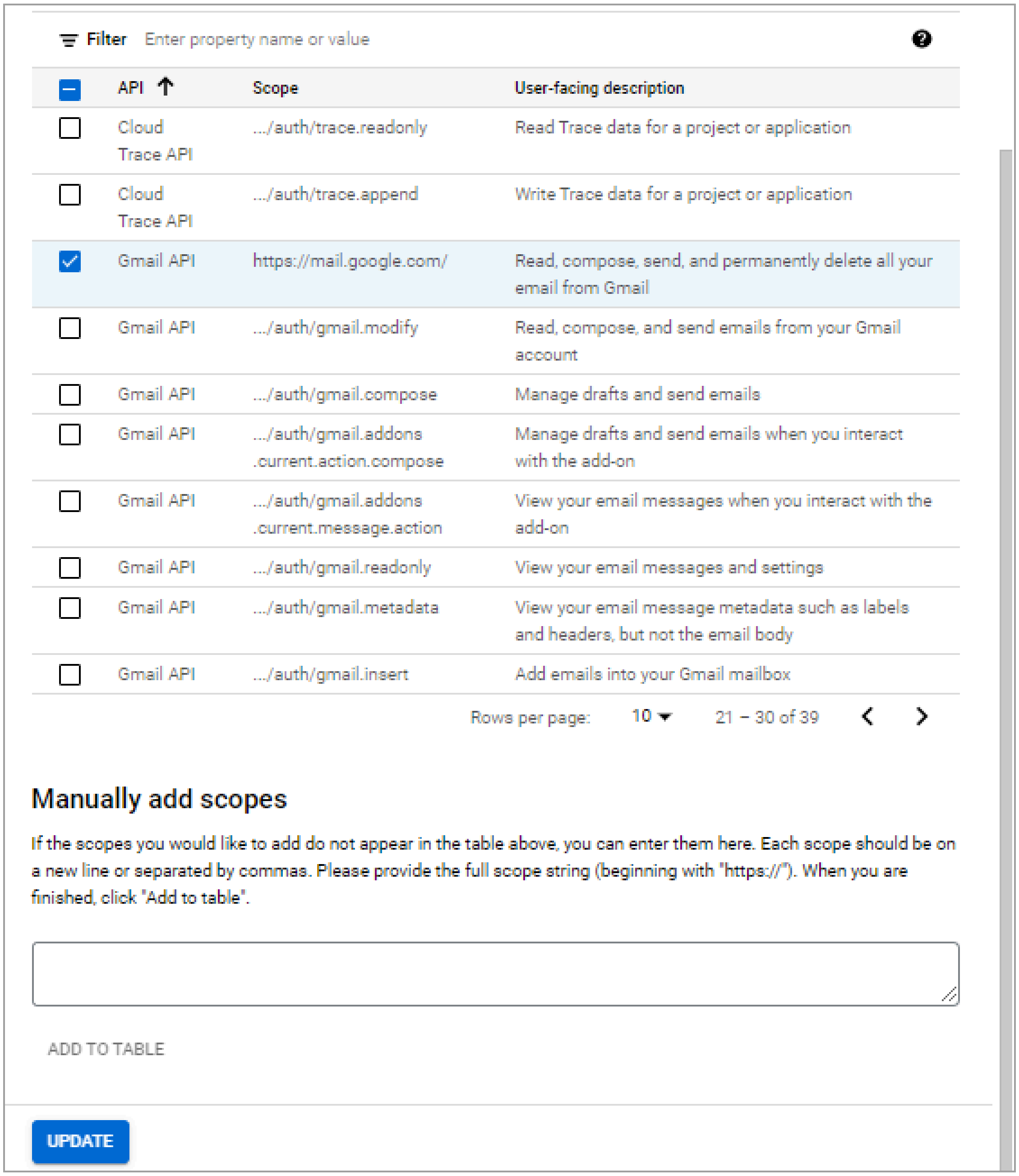
14. Under **User Type**, select **External** and click **CREATE**.
The **Edit app registration** page appears.



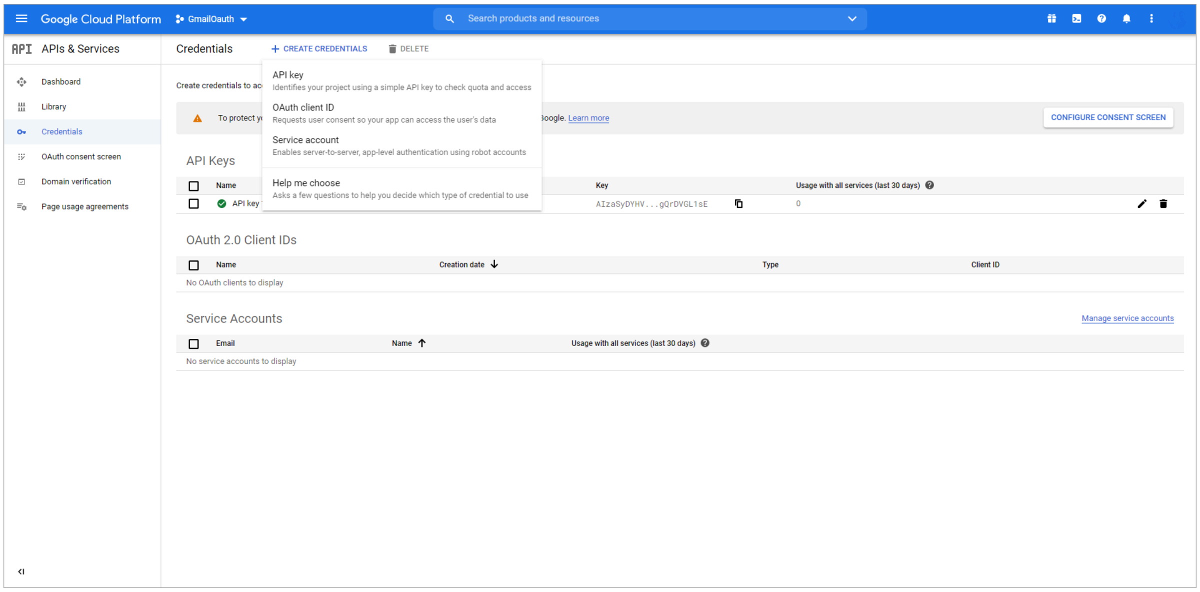
15. In the following fields provide with the required information:
    - **App name**: Name of the application.
    - **User support email**: User support email.
    - **Application home page**: Application home page link with HTTP or HTTPS.
    - **Application privacy policy link**: Application privacy policy link.
    - **Application term of service link**: Link for terms of service.
    - **Authorized domain**: Type the domain name without HTTPS or HTTP.
16. Click **SAVE AND CONTINUE**. The **Scopes** page appears.



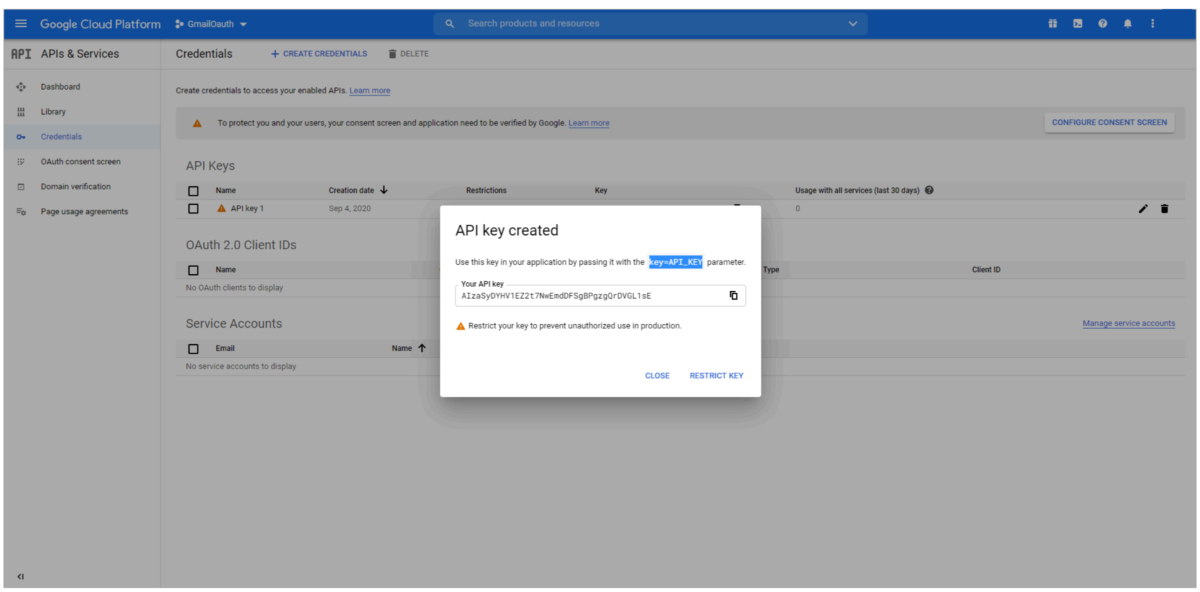
17. Click **ADD OR REMOVE SCOPES**.
18. Select the **Gmail API** option that has **https://mail.google.com/**, and then click **UPDATE**.



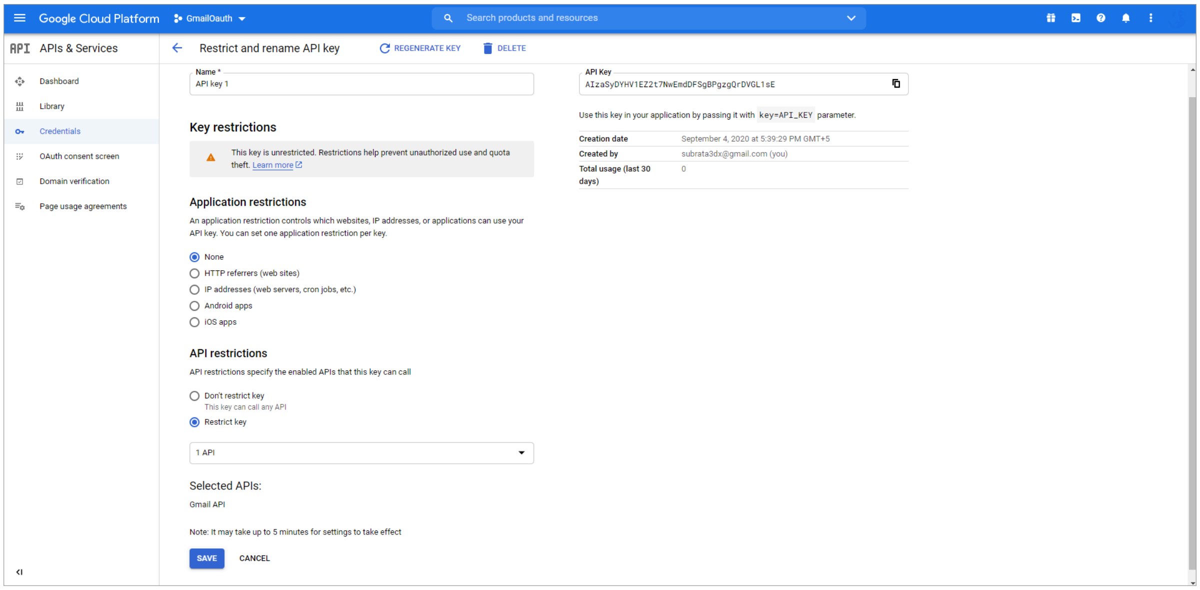
19. On the left sidebar, click **Credentials**.
    The **Credentials** page appears.



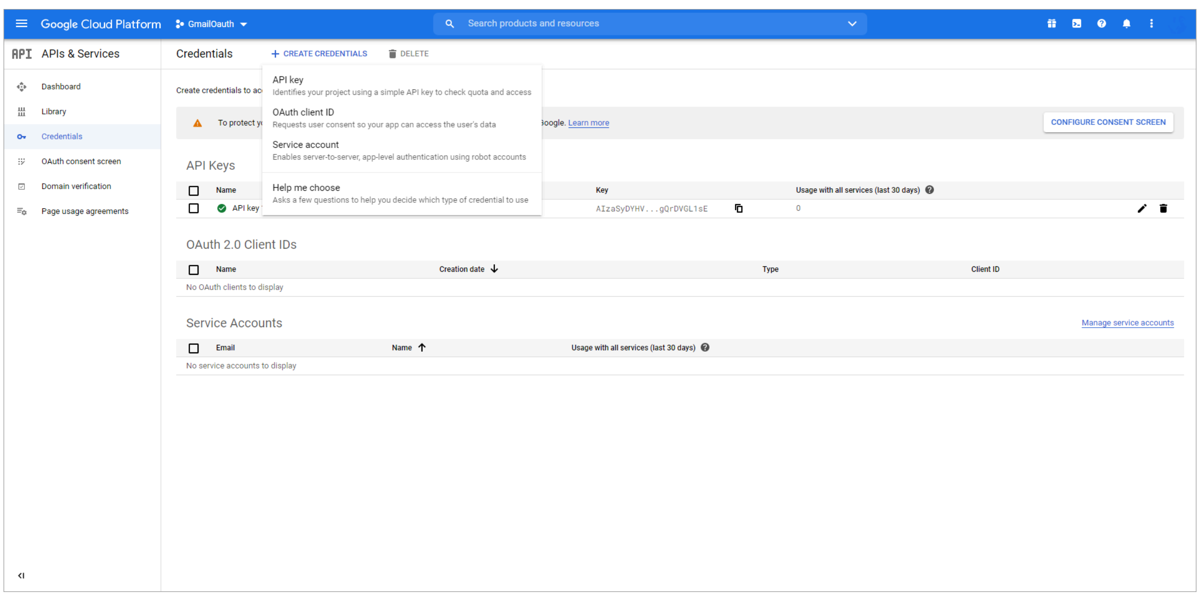
20. Click **CREATE CREDENTIALS** > **API key**.
The **API key created** Web dialog appears.



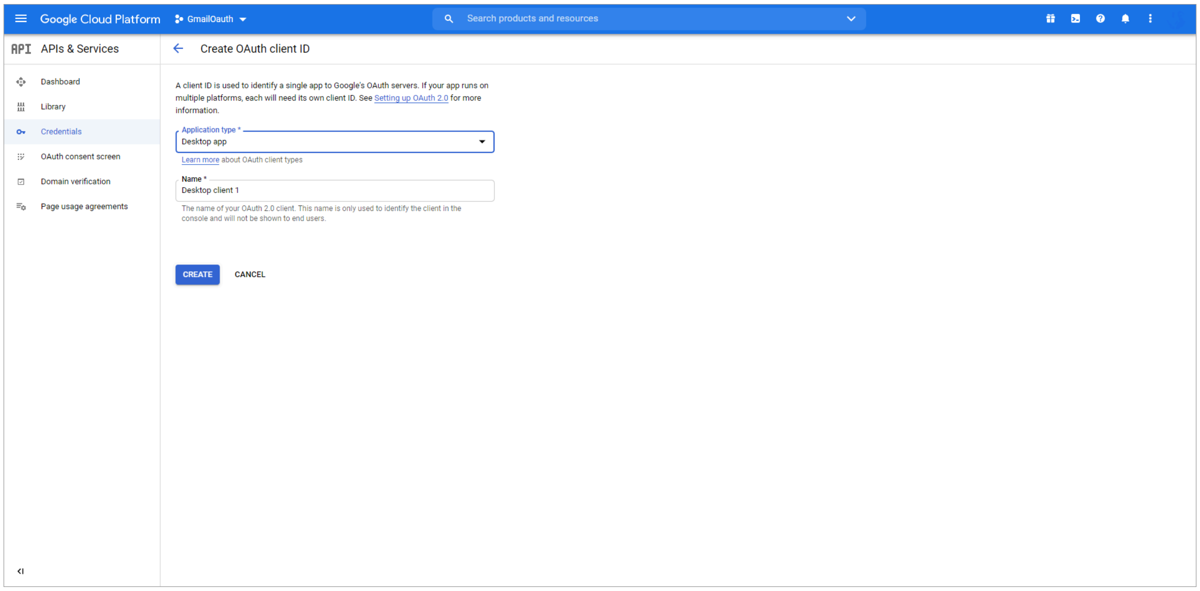
21. Click **RESTRICT KEY**. The **Restrict and rename API key** page appears.



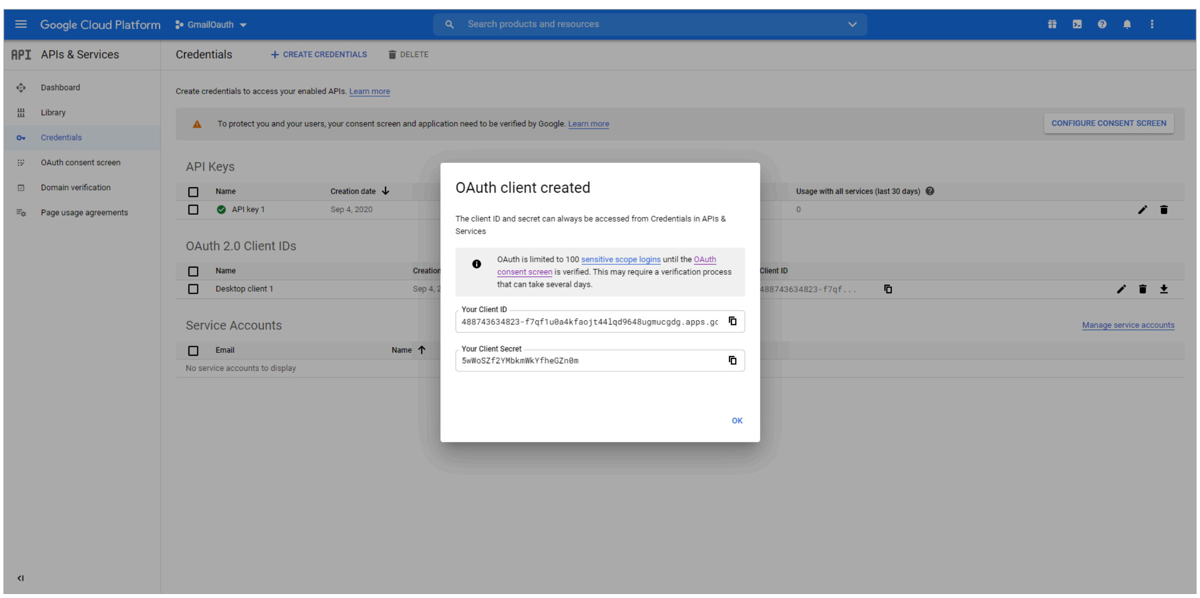
22. Under **Application restrictions**, select **None**.
23. Under **API restrictions**, select **Restrict key**.
24. Click **Save**.



25. On the left sidebar, click **Credentials** and then click **CREATE CREDENTIALS** > **OAuth client ID**.
    The **Create OAuth client ID** page appears.

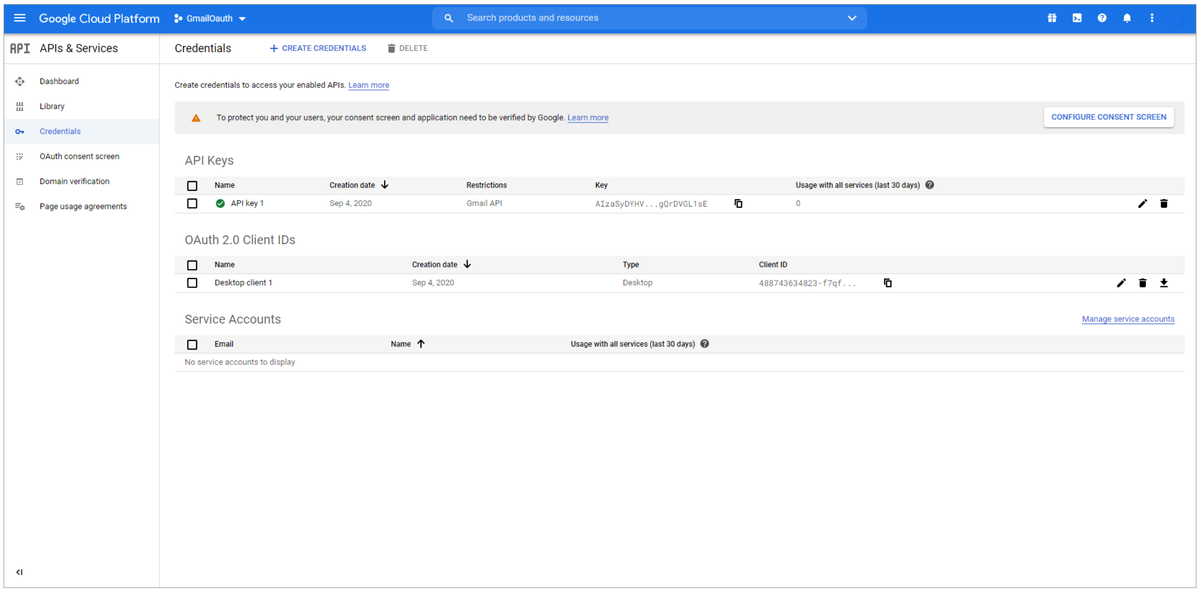


26. From the **Application type** list, select **Desktop app** and click **CREATE**.
The **OAuth client created** Web dialog appears.

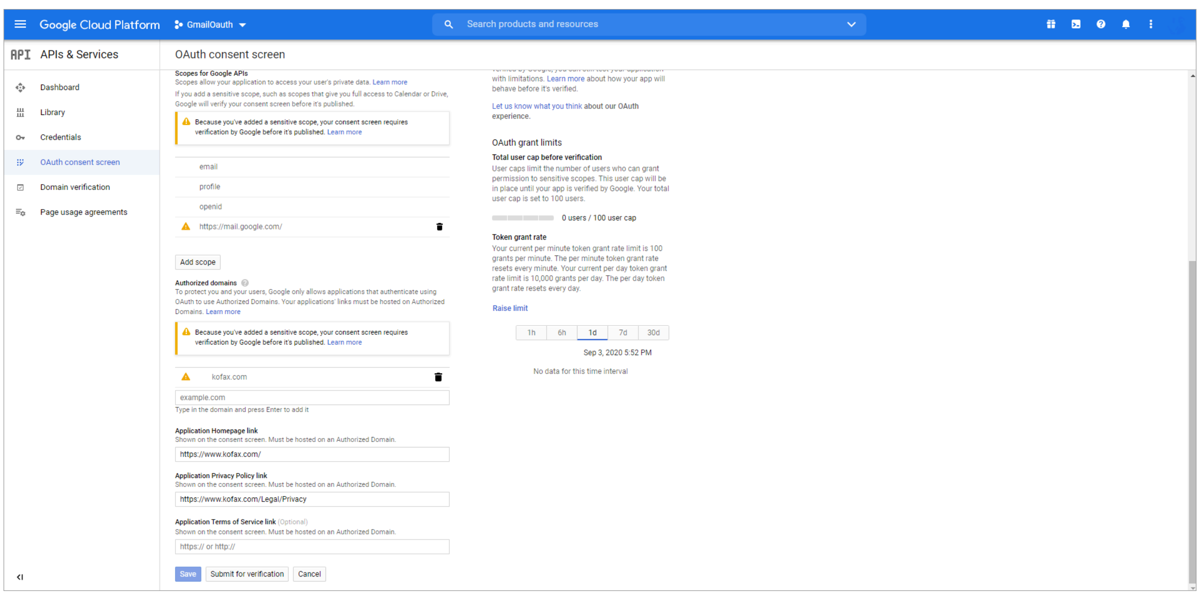


ⓘ Note down your Client ID and Client Secret as you will require them in Application configuration.

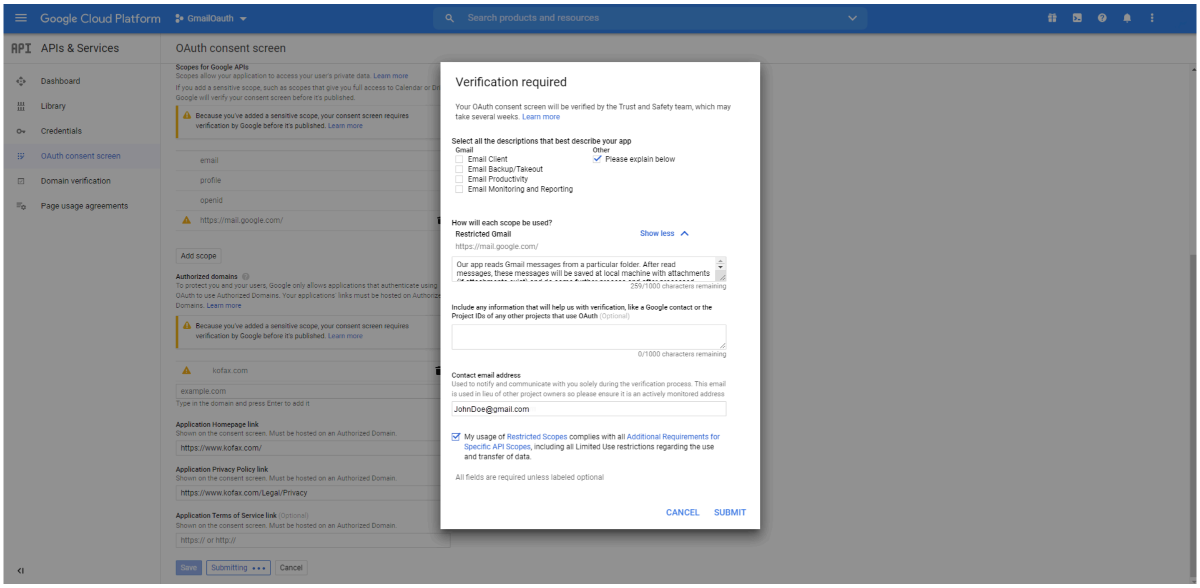
27. Click **OK**. The following page appears.



28. On the left sidebar, click **OAuth consent screen**.
    The **OAuth consent screen** appears.



29. Click **Submit for verification**. The **Verification required** Web dialog appears.



30. Select the **Please explain below** check box, and in the **How will each scope be used?** field, provide a meaningful explanation.

    For example, see the following explanation.

```
"Our application will read Gmail messages from a particular Gmail folder.
After reading messages, the messages will be saved on a local computer
with attachments (if any attachments exist) and will do further process.
If the process is  successful, messages will be deleted from the
Gmail folder."
```

31. In the **Contact email address** field, enter your contact email address.
32. Click **Submit**.

> At this point, the OAuth consent screen is verified, but application is yet to be verified. Unverified app does not impact anything.

33. Copy the following XML content.

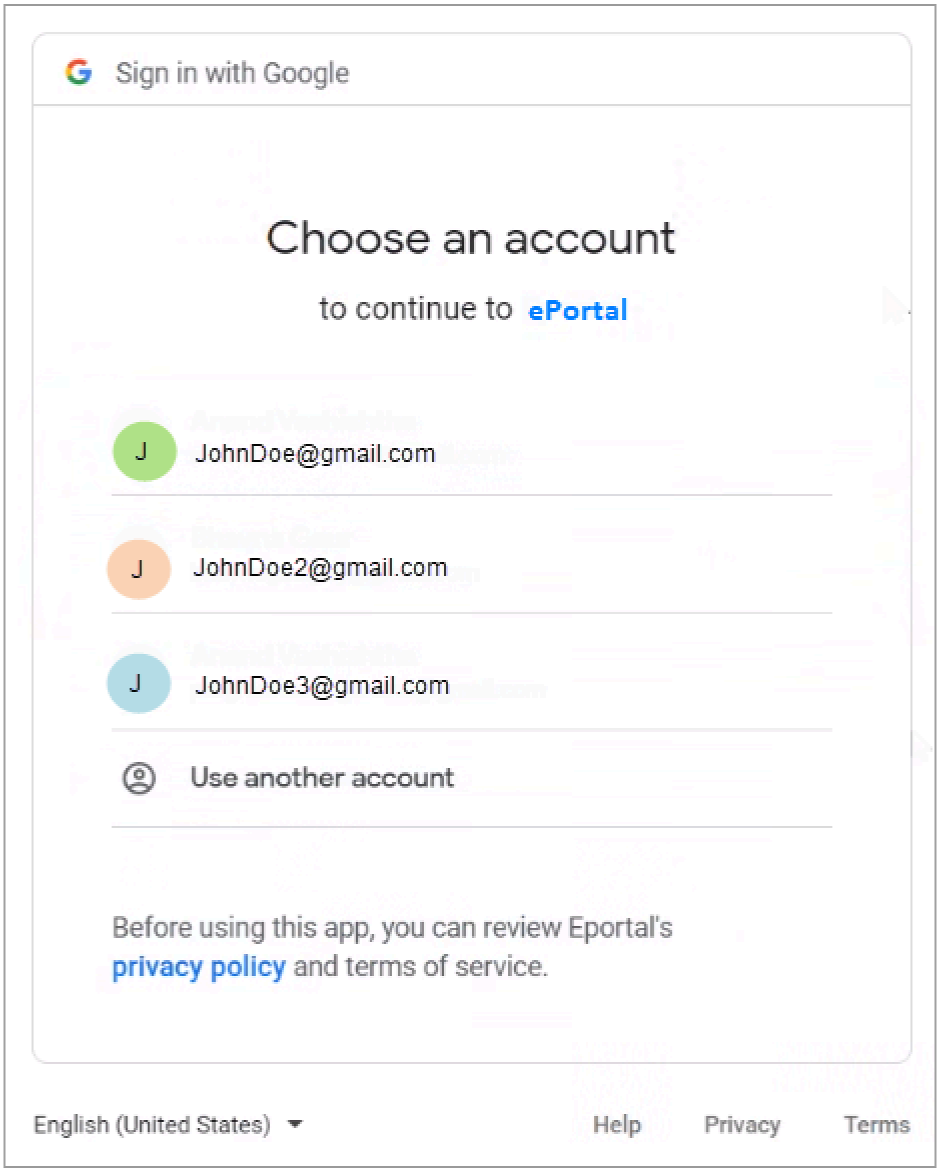
```
<MailAccount Id = "pop3_oauth_testmail" DisplayName="pop3_oauth_testmail"
 Host="pop.googlemail.com" Port="995" SSL="true" IgnoreCertificateErrors="false"
 UserName="ProgramTesting@gmail.com" Protocol="POP3_OAUTH"
 ClientID="89205223141133cjceblmui8f0oimb67jn67raffn5hl.apps.googleusercontent.com"
 ClientSecretID="MiVbIAJpGwBxpUjFkxIF8ven">
<MailEncoding>UTF-8</MailEncoding>
<DefaultCharset>UTF-8</DefaultCharset>
<Folders>
  <Folder>ALL MAIL</Folder>
</Folders>
<Filter />
<Impersonate Enabled = "false" />
 </ MailAccount >
```

34. Open the EPortal.AppConfig file, located at C:\ProgramData\TIS\<eFlow6>\AppData\Server\<Application_name>\Setup, and paste the copied content under <MailAccounts/> section.

35. Change the Id, Displayname, UserName, ClientID, ClientISecretID, and then save the file.

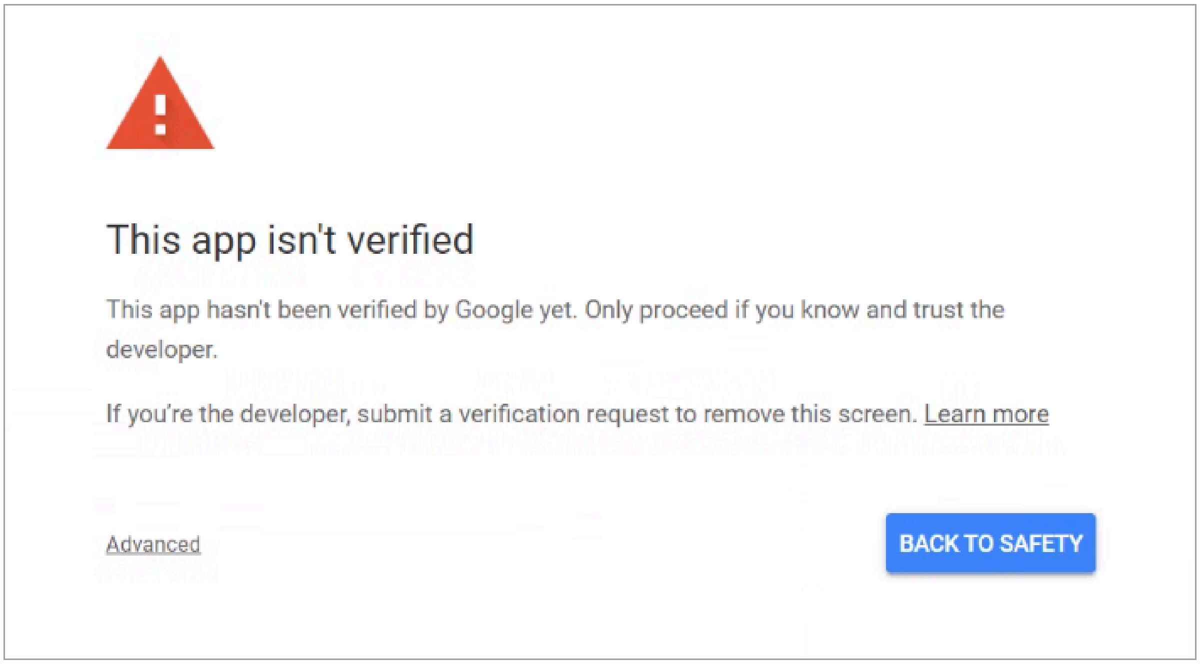
    Note down the Client ID and Client Secret which can be referred in future activities.

36. In the **eFlow LaunchPro**, on the **Stations** list, select **ePortal manual station**.
    If opened for the first time the following page appears.

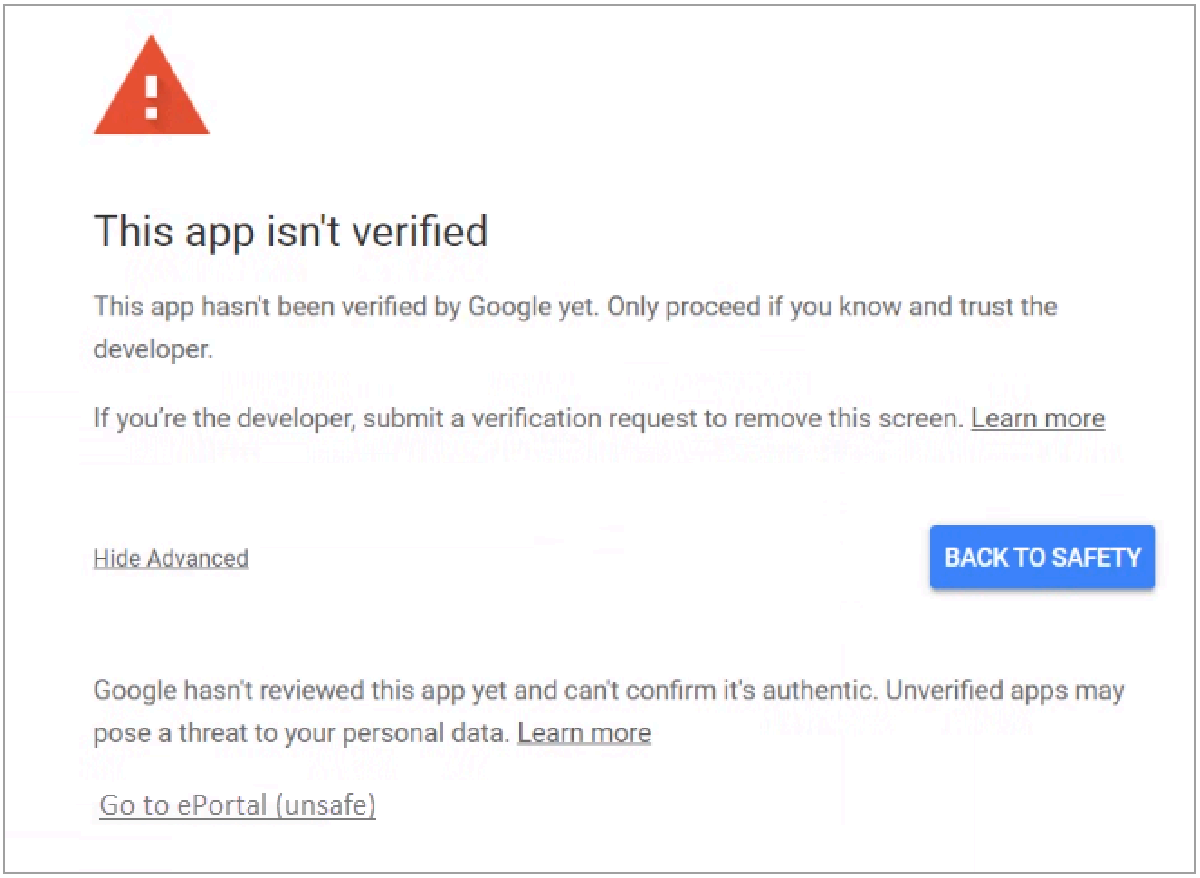


37. Select the Gmail account that you provided as the contact email address. The following page appears.

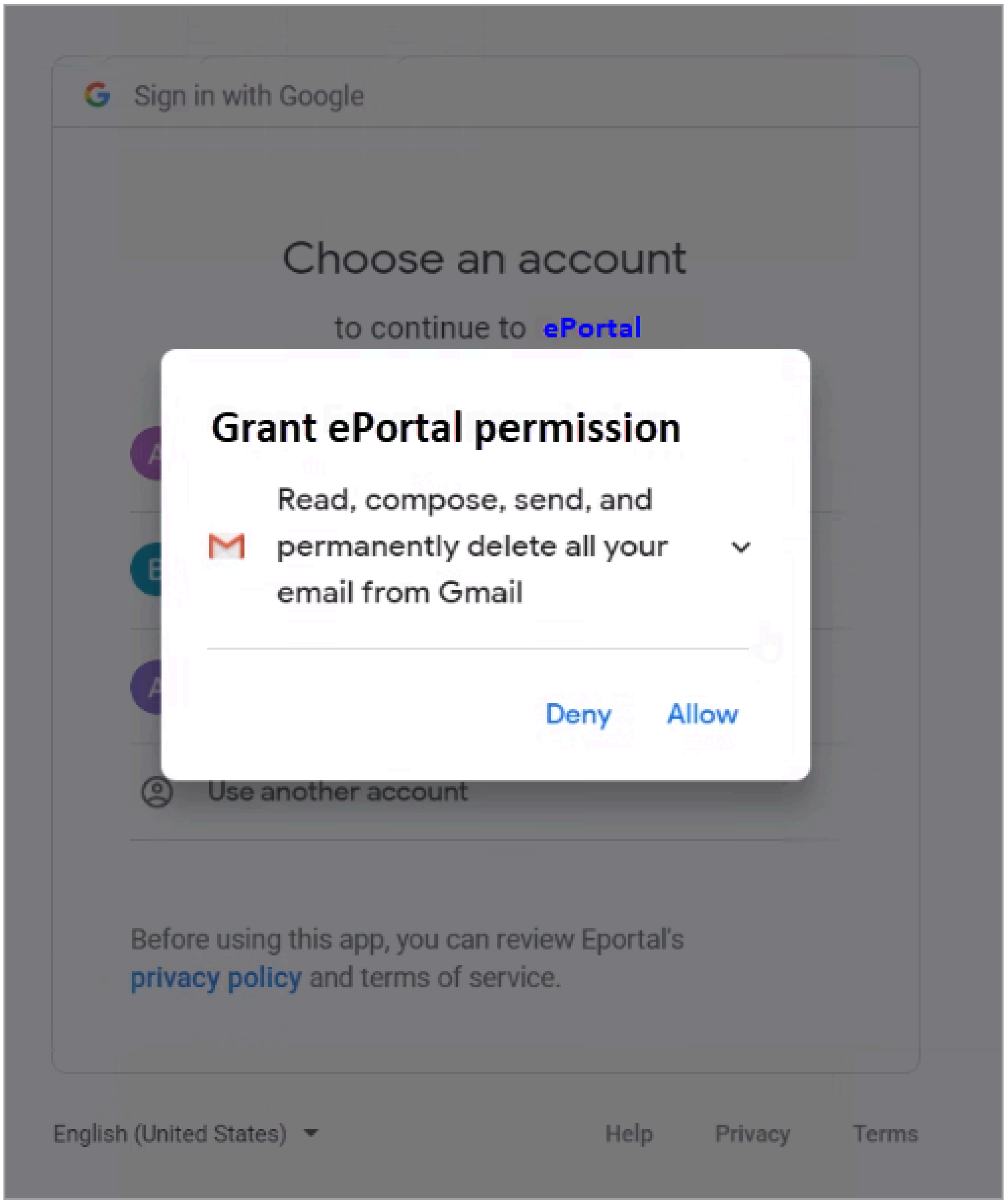
If your Gmail account is not signed in from the computer where you are using the ePortal, then you need to sign in using your Gmail username and password.



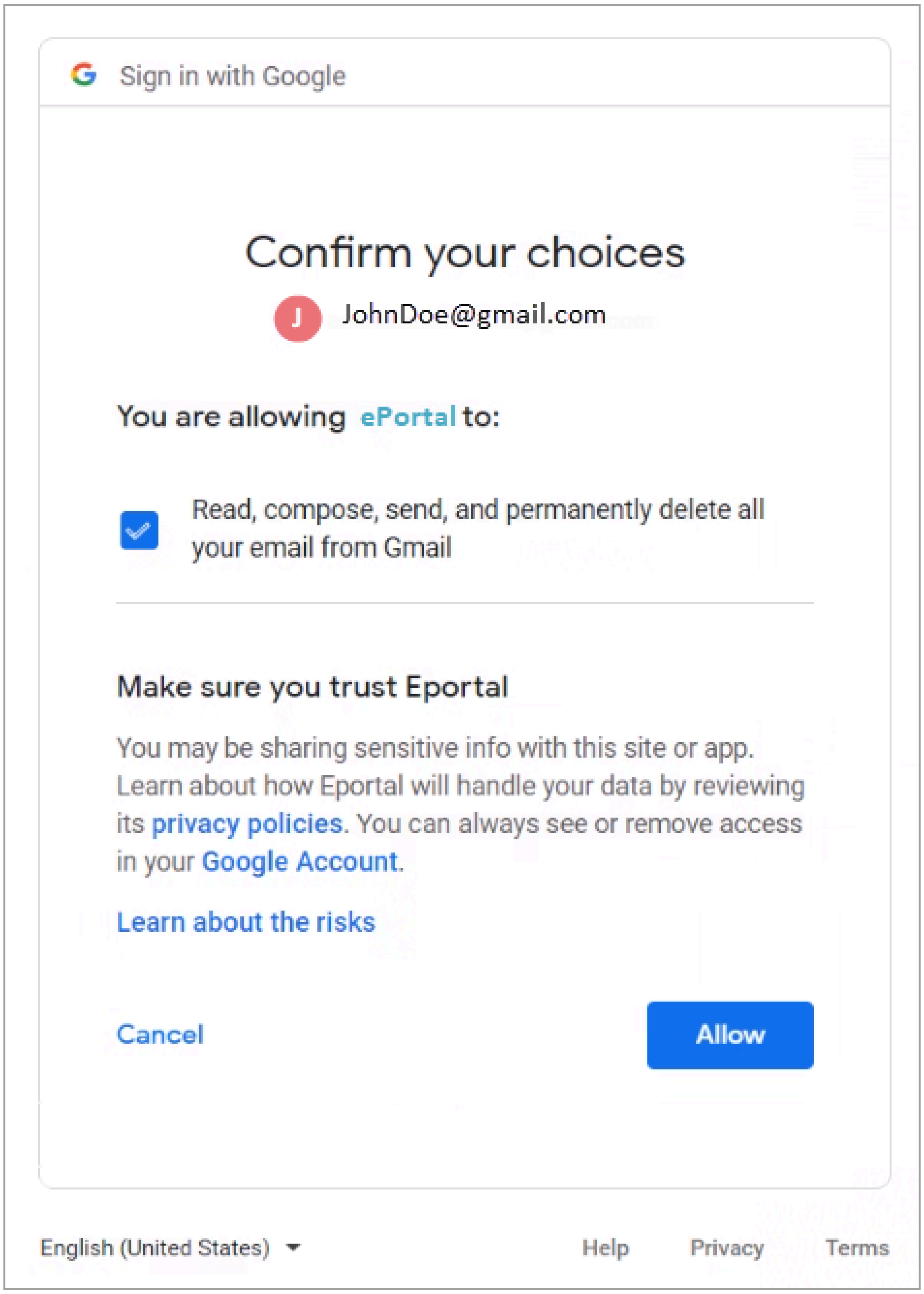
38. Click **Advanced**.
    The following page appears.



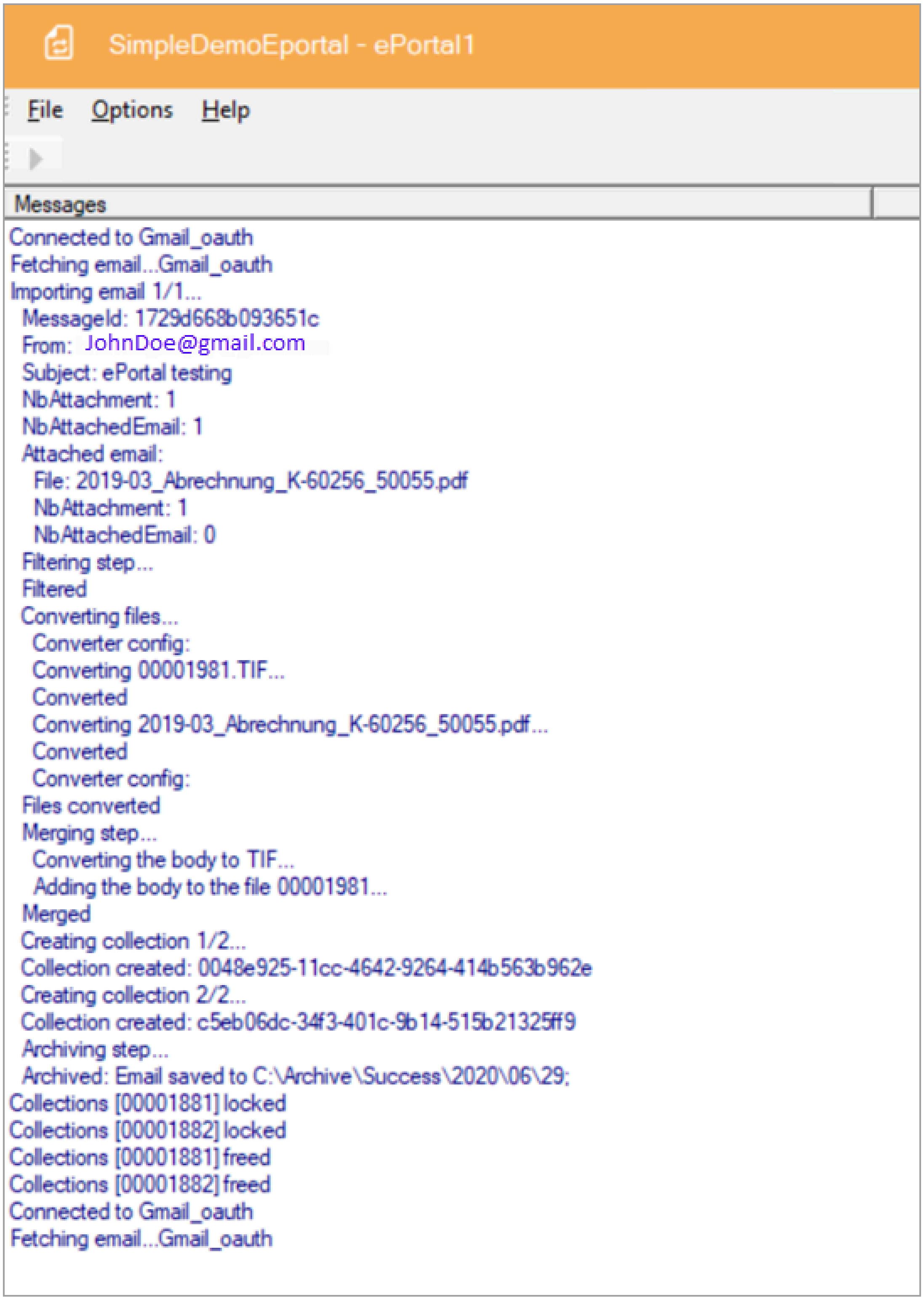
39. Click **Go to ePortal (unsafe)**.
    The **Grant ePortal permission** Web dialog appears.



40. Click **Allow**. The **Confirm your choices** page appears.



41. Click **Allow**.
42. After accepting the permission, the **ePortal Manual station** starts fetching the Gmail messages from the configured folder.


SimpleDemoEportal - ePortal1
File Options Help
Messages
Connected to Gmail_oauth
Fetching email...Gmail_oauth
Importing email 1/1...
MessageId: 1729d668b093651c
From: JohnDoe@gmail.com
Subject: ePortal testing
NbAttachment: 1
NbAttachedEmail: 1
Attached email:
File: 2019-03_Abrechnung_K-60256_50055.pdf
NbAttachment: 1
NbAttachedEmail: 0
Filtering step...
Filtered
Converting files...
Converter config:
Converting 00001981.TIF...
Converted
Converting 2019-03_Abrechnung_K-60256_50055.pdf...
Converted
Converter config:
Files converted
Merging step...
Converting the body to TIF...
Adding the body to the file 00001981...
Merged
Creating collection 1/2...
Collection created: 0048e925-11cc-4642-9264-414b563b962e
Creating collection 2/2...
Collection created: c5eb06dc-34f3-401c-9b14-515b21325ff9
Archiving step...
Archived: Email saved to C:\Archive\Success\2020\06\29;
Collections [00001881] locked
Collections [00001882] locked
Collections [00001881] freed
Collections [00001882] freed
Connected to Gmail_oauth
Fetching email...Gmail_oauth

IMAP_GMAIL connector

IMAP_GMAIL connector is an upgraded version of IMAP connector, which implements OAuth for secure delegate access. This connector does not require password for the email account configuration in the EPortal.AppConfig file.

The IMAP_GMAIL connector retrieves a batch of emails from an email server using the IMAP protocol. With the IMAP protocol it is possible to set a message as read, delete, or move; and we use Gmail API for this. Gmail API use the OAuth 2.0 protocol for authentication and authorization. Google supports common OAuth 2.0 scenarios such as those for web server, client-side, installed, and limited-input device applications.

Unsynchronized mode

Depending on the archive configuration, the emails in the mailbox are deleted, moved, or set as read after the eDocs are imported into the eFlow workflow.

By default, ePortal sets imported files as READ, so when ePortal retrieves emails with the exchange online filter `IsRead=false`, it only imports new emails.

Synchronized mode

Not required.

Autorun mode

Disable the autorun mode in the following scenarios and run the ePortal manual station.

Scenario 1: Whenever you add a new email account in IMAP_GMAIL protocol, in the EPortal.AppConfig file, manually authorize yourself in ePortal station by entering configured email account credentials and permissions consent.

Scenario 2: When the password for your email account expires or changes, authorize yourself again by opening ePortal station manually.

Enable the autorun mode for the ePortal station.

Configuration

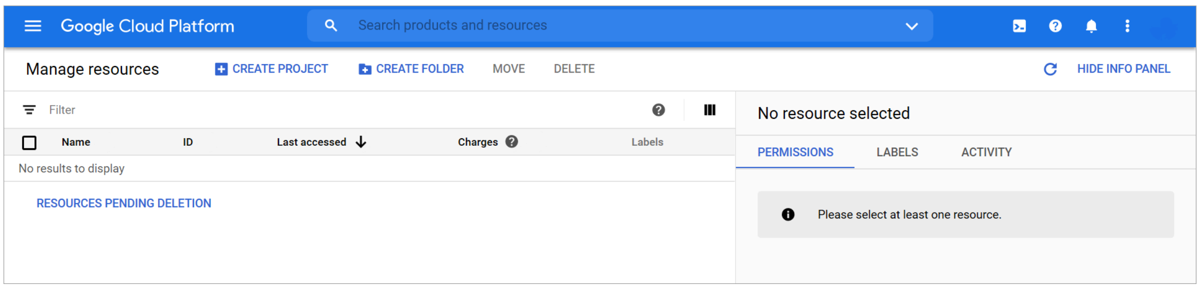
Any application that implements OAuth standards to authenticate and authorize its users, it needs to be registered with the corresponding Application/Web servers.

The following step-by-step procedure explains how to register an ePortal application, and the minimum set of privileges needed for it. More granular role-based access privileges are possible, but this is subjected to the IT policies of the individual organizations.

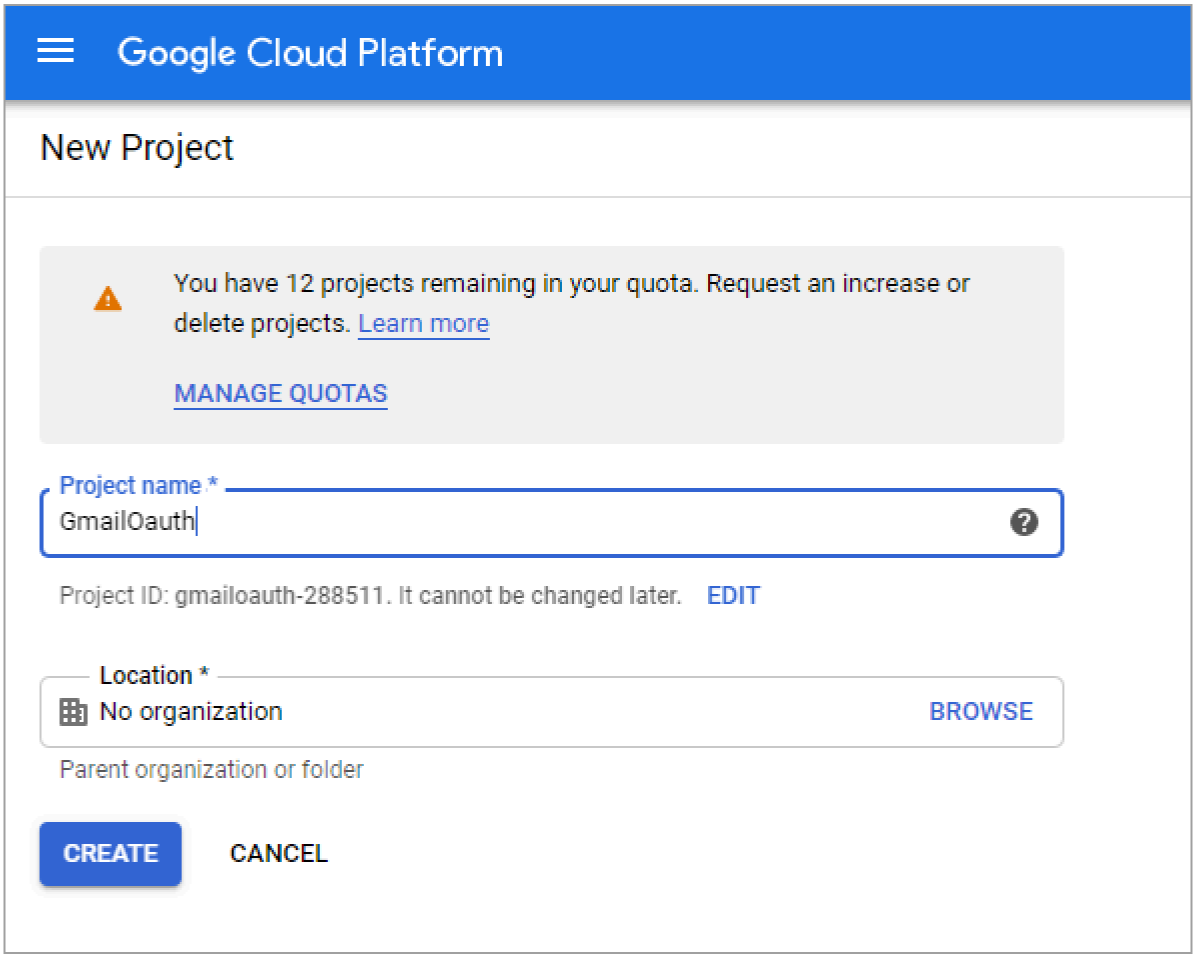
Google cloud configuration for Gmail

You can create a new project, enable, and configure it for Gmail.

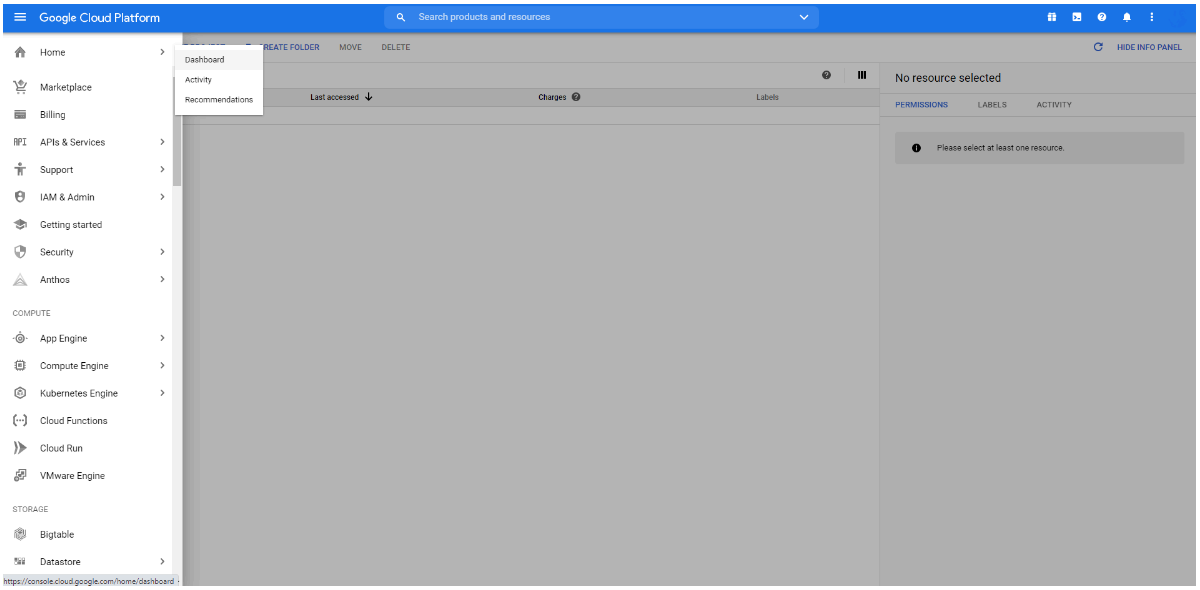
The figures and user interfaces used in the following procedure are taken from the Google's website and they might change occasionally. Hence, we request you to follow the latest procedure mentioned in the Google's website, which is updated time-to-time. If you still face issues while authorizing your application, we recommend to take assistance from the user who has expertise in authorizing an application.

1. Go to https://console.cloud.google.com and follow the on-screen instructions to sign into the Google Cloud Platform.
   After a successful sign-in, the **Google Cloud Platform** main page appears.
   

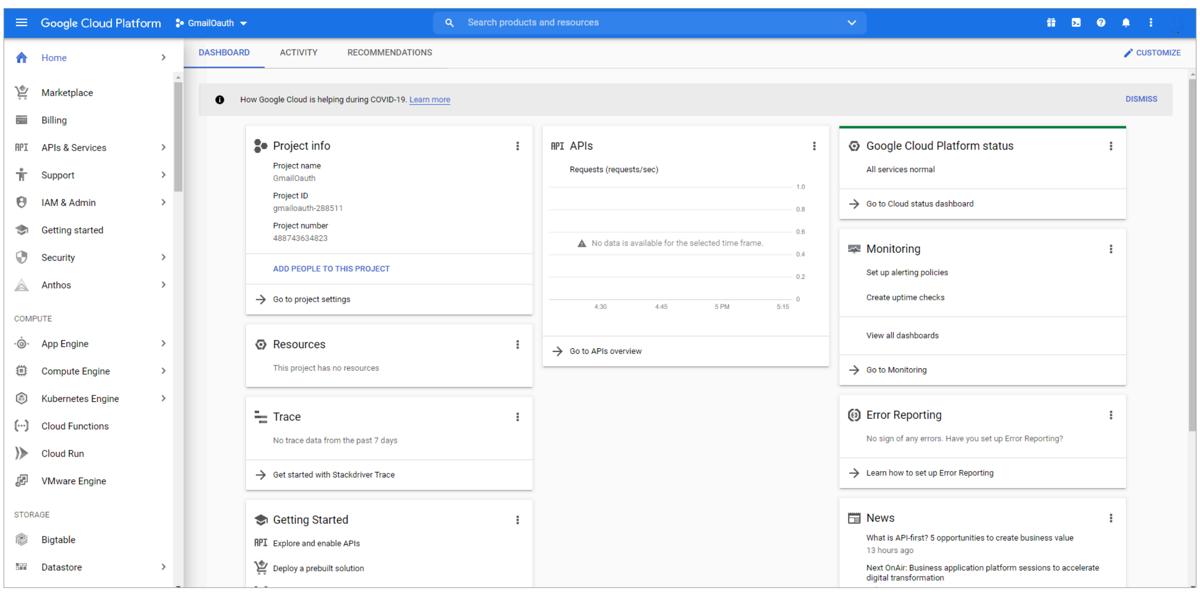
2. On the **Google Cloud Platform** main page, click **CREATE PROJECT**.
   The **New Project** page appears.



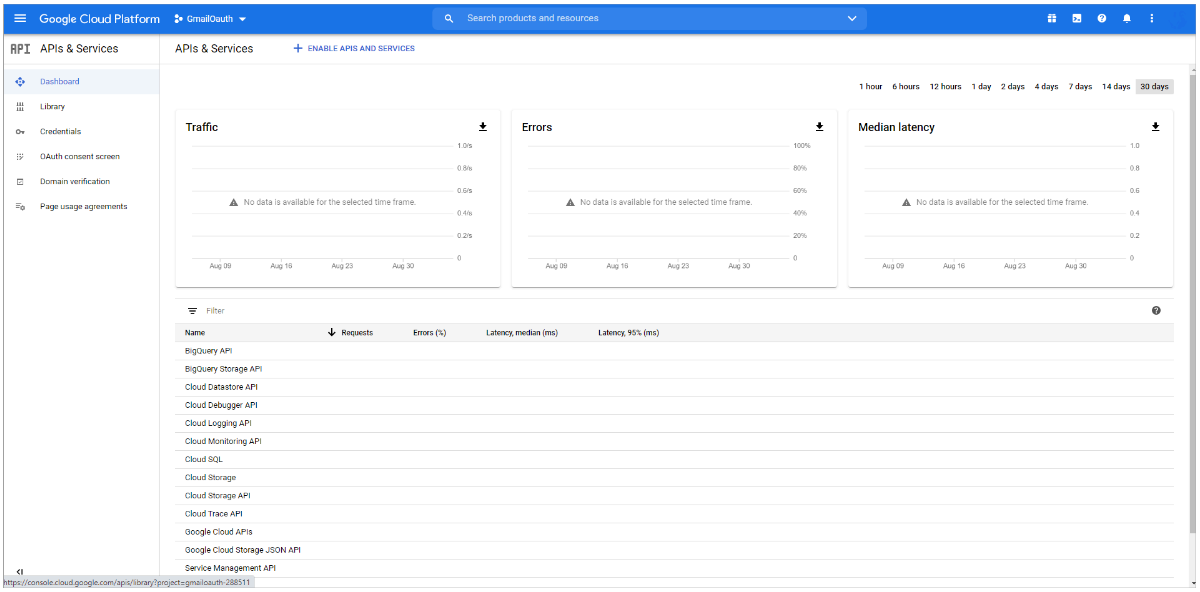
3. In the **Project name *** field, type a name for the project.
4. In the **Location** field, select the location as "No organization".
5. Click **CREATE**.
   The following page appears.



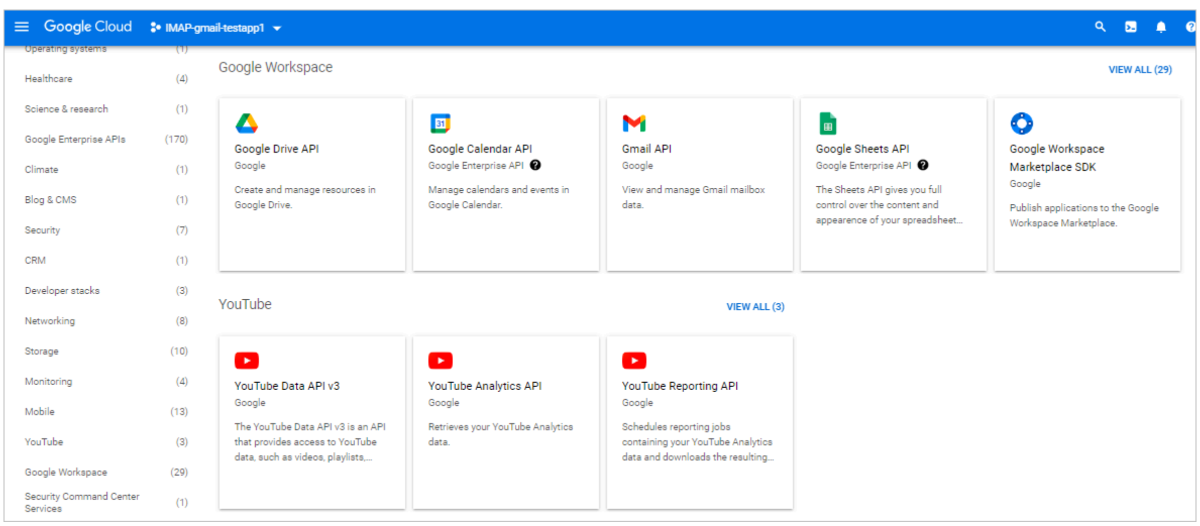
6. On the left sidebar, select **Home** > **Dashboard**.
   The **Dashboard** page appears.



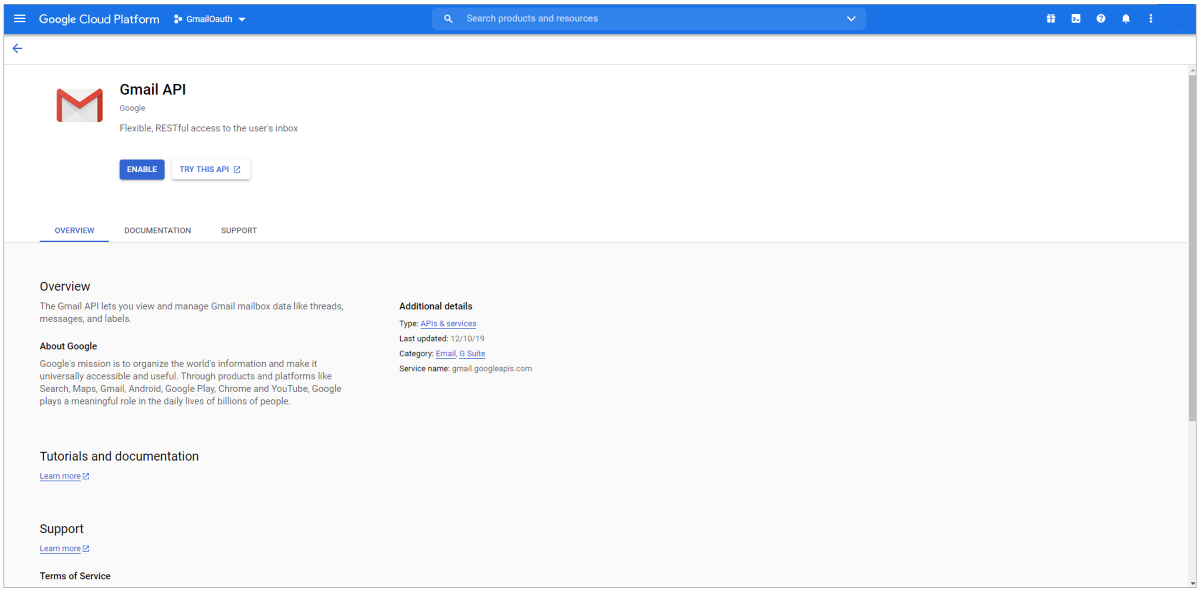
7. Under **Getting Started**, click **Explore and enable APIs**.
   The **APIs & Services** page appears.



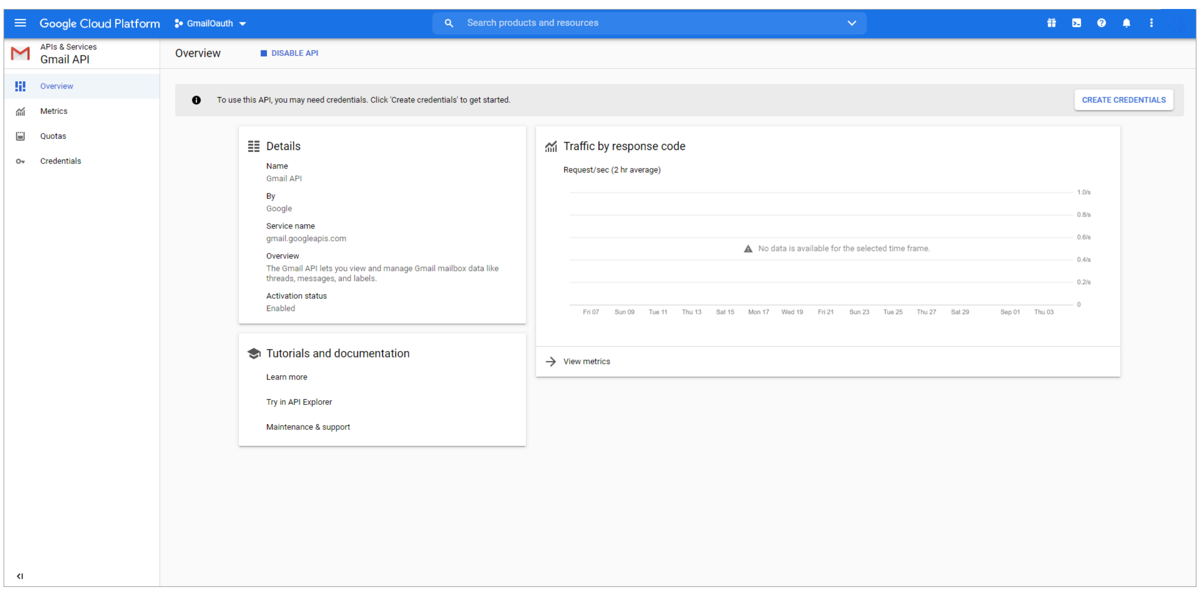
8. On the left sidebar, click **Library**.
   The **API Library** page appears.



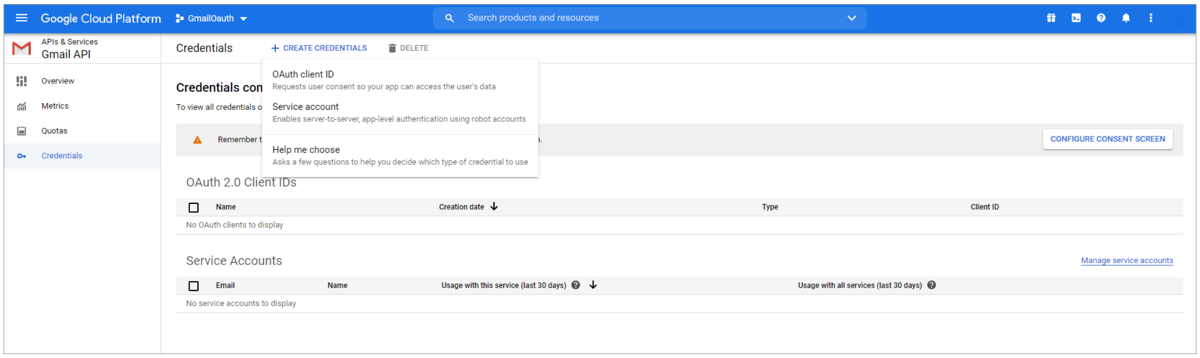
9. Under **Google Workspace**, click **Gmail API**.
   The **Gmail API** page appears.



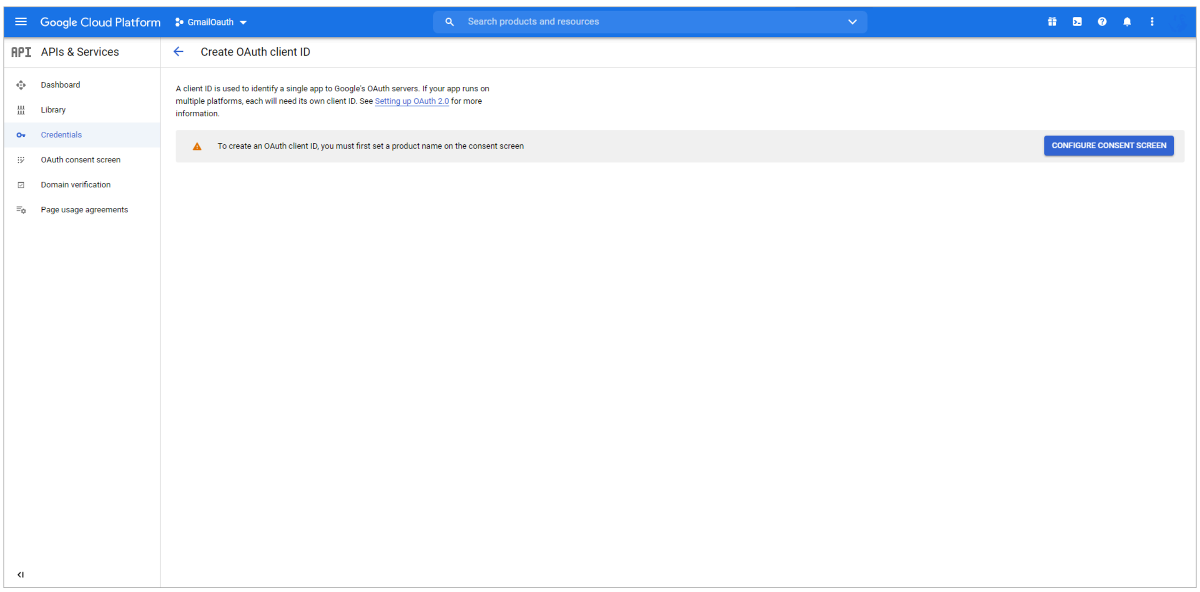
10. Click **Enable**.
The **Overview** page appears.



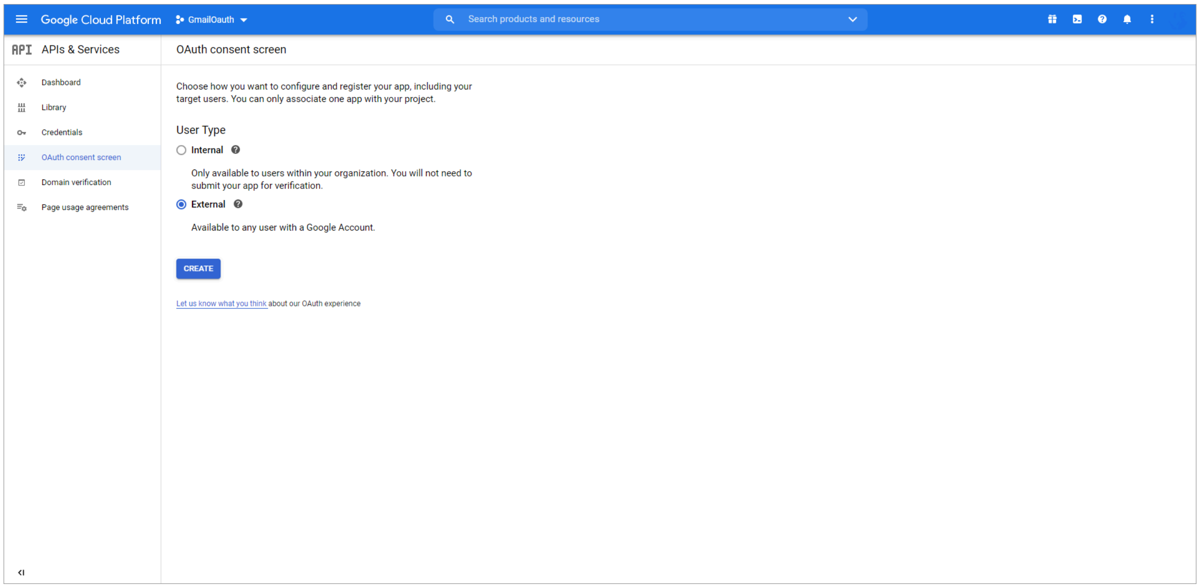
11. On the left sidebar, click **Credentials**.
The **Credentials** page appears.



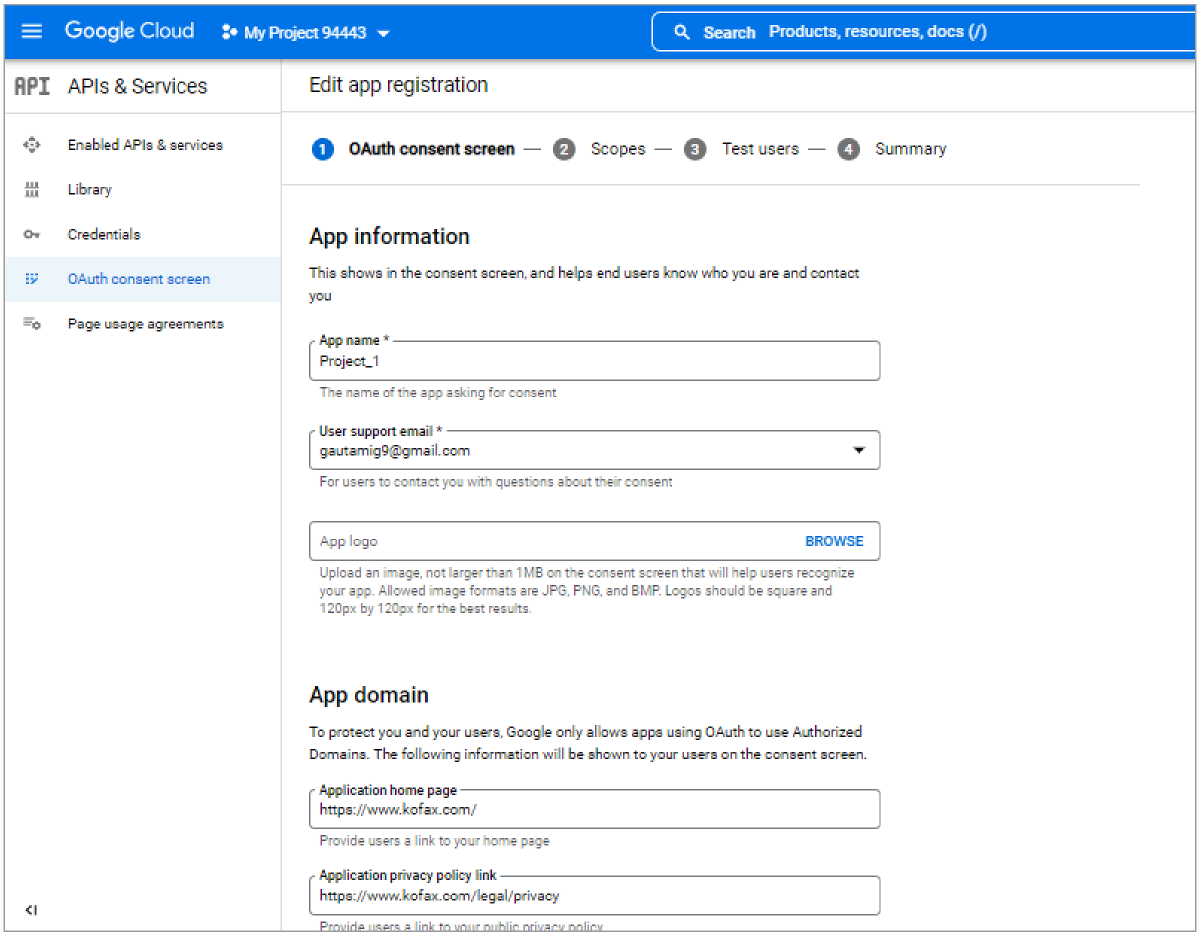
12. Click **CREATE CREDENTIALS** > **OAuth client ID**.
    The **Create OAuth client ID** page appears.



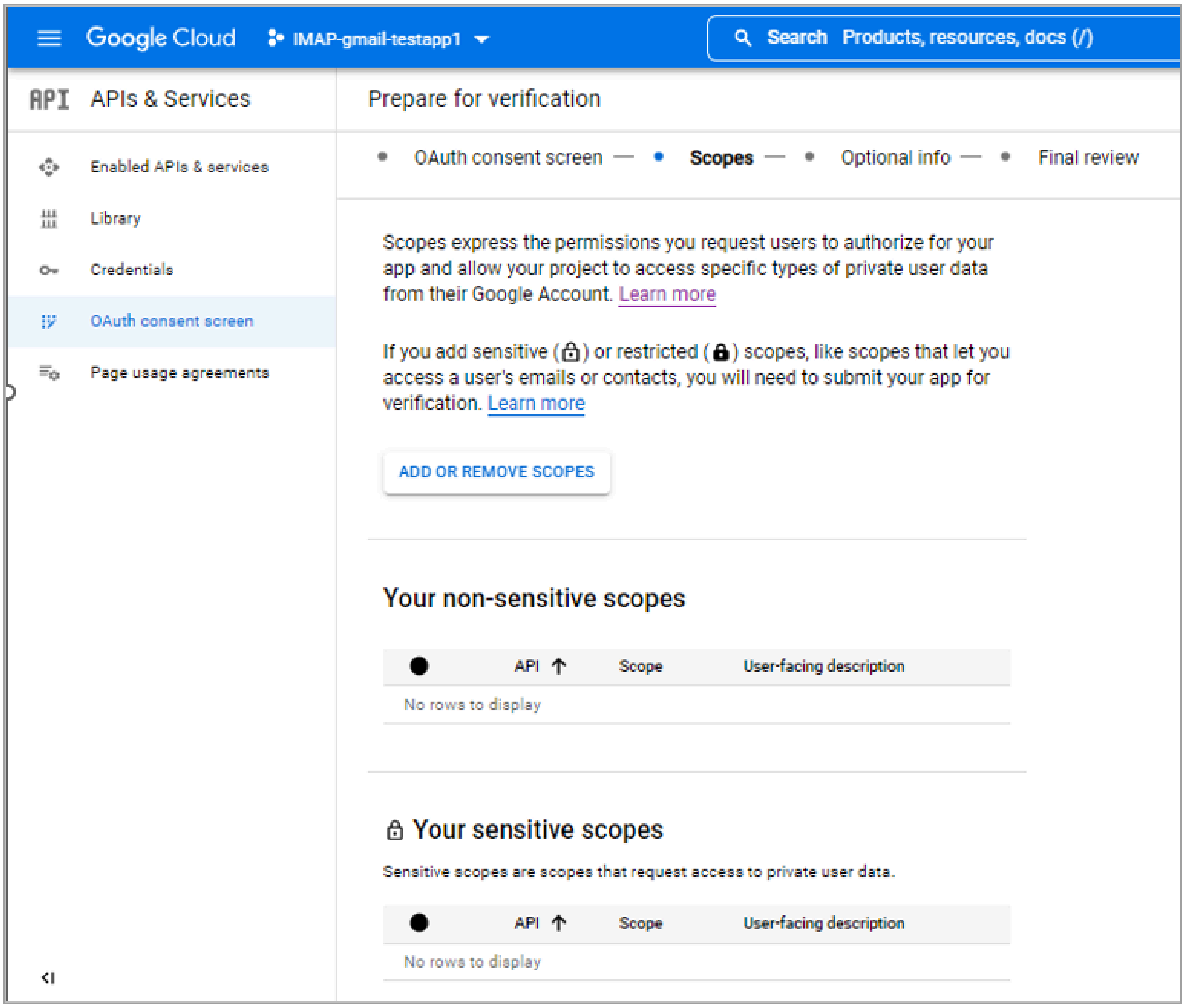
13. Click **CONFIGURE CONSENT SCREEN**.
    The **OAuth consent screen** page appears.



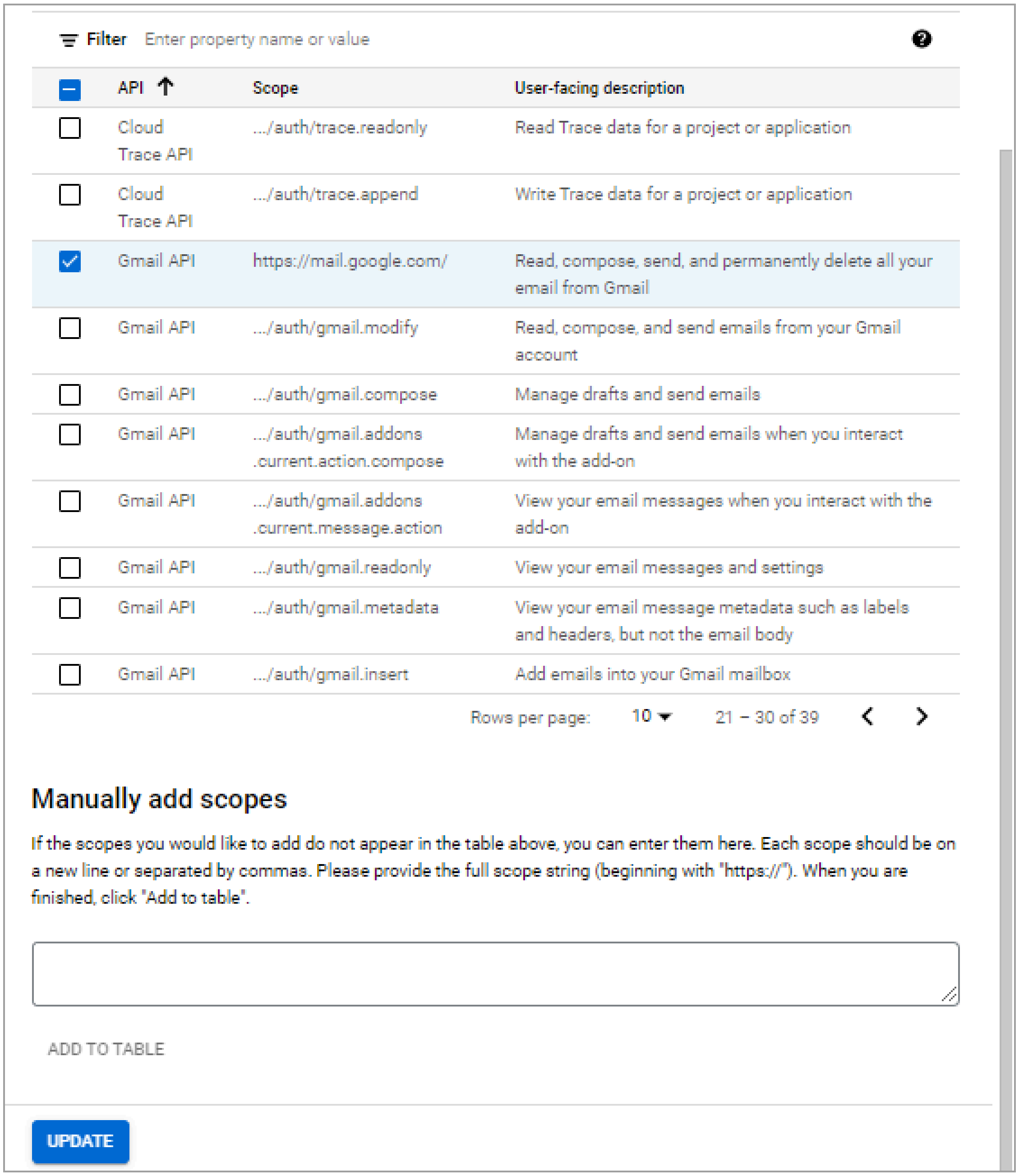
14. Under **User Type**, select **External** and click **CREATE**.
The **Edit app registration** page appears.



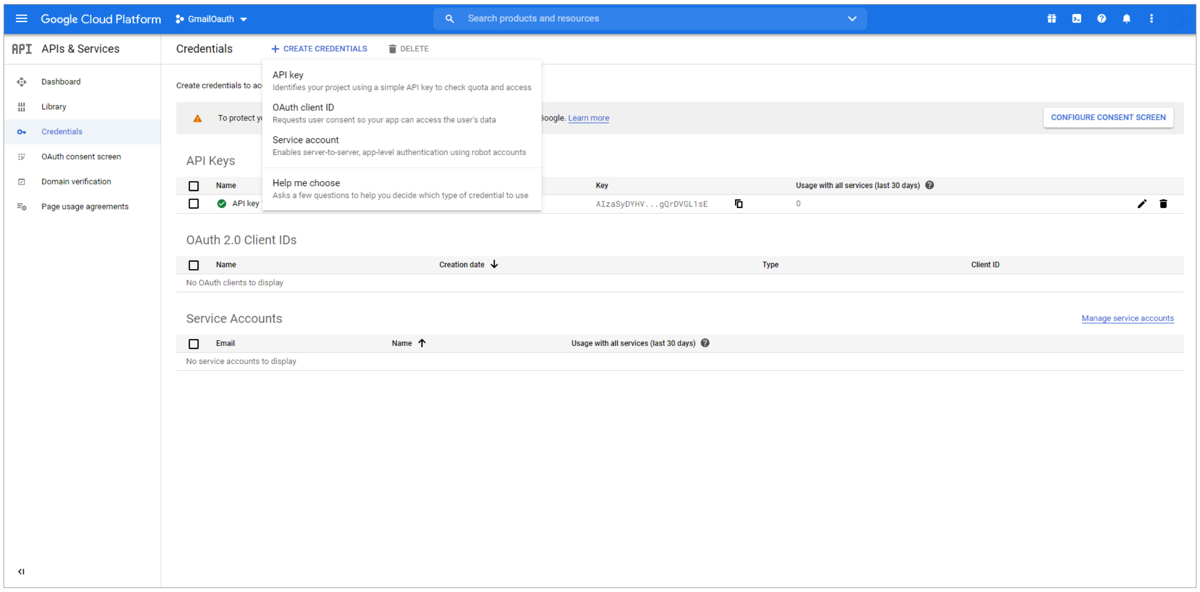
15. In the following fields provide with the required information:
    - **App name**: Name of the application.
    - **User support email**: User support email.
    - **Application home page**: Application home page link with HTTP or HTTPS.
    - **Application privacy policy link**: Application privacy policy link.
    - **Application term of service link**: Link for terms of service.
    - **Authorized domain**: Type the domain name without HTTPS or HTTP.
16. Click **SAVE AND CONTINUE**. The **Scopes** page appears.



17. Click **ADD OR REMOVE SCOPES**.
18. Select the **Gmail API** option that has **https://mail.google.com/**, and then click **UPDATE**.

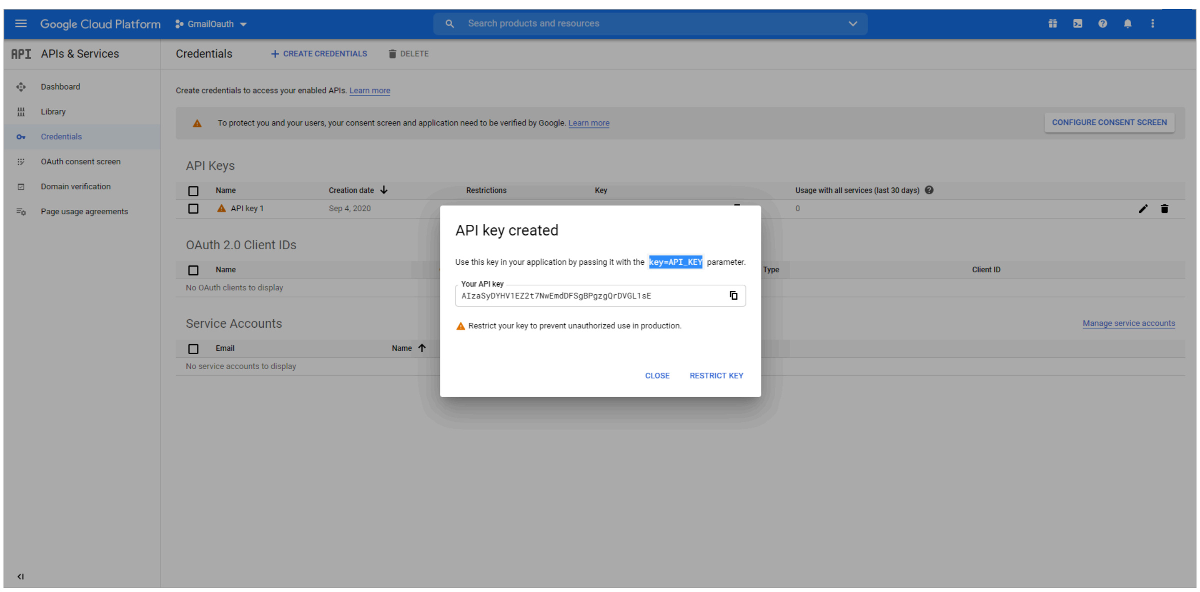


19. On the left sidebar, click **Credentials**.
    The **Credentials** page appears.

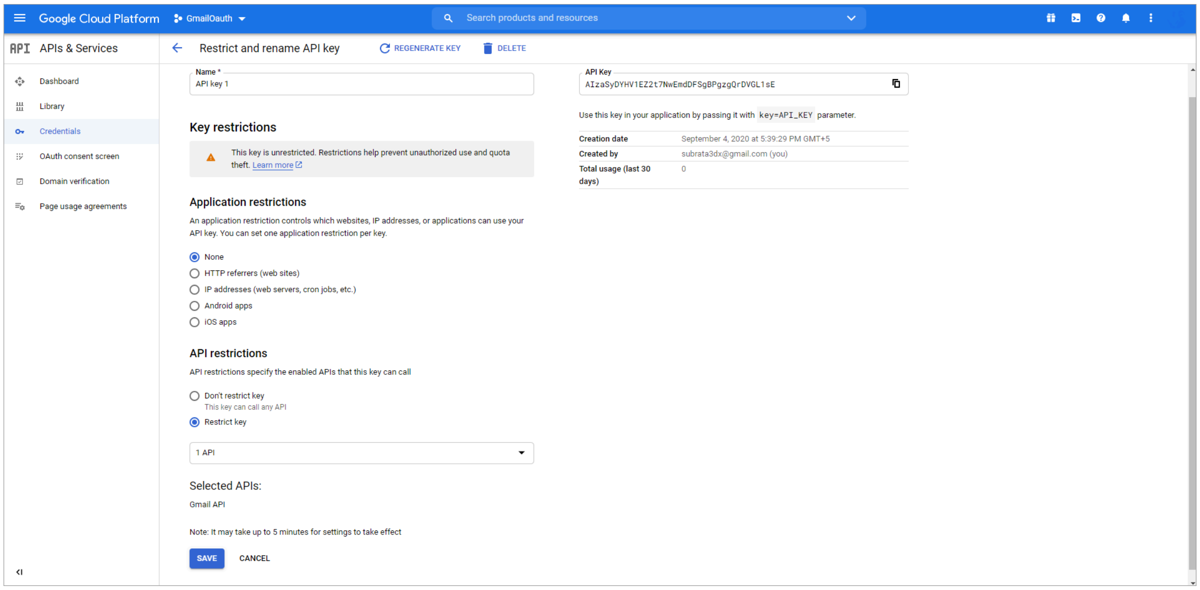


20. Click **CREATE CREDENTIALS** > **API key**.

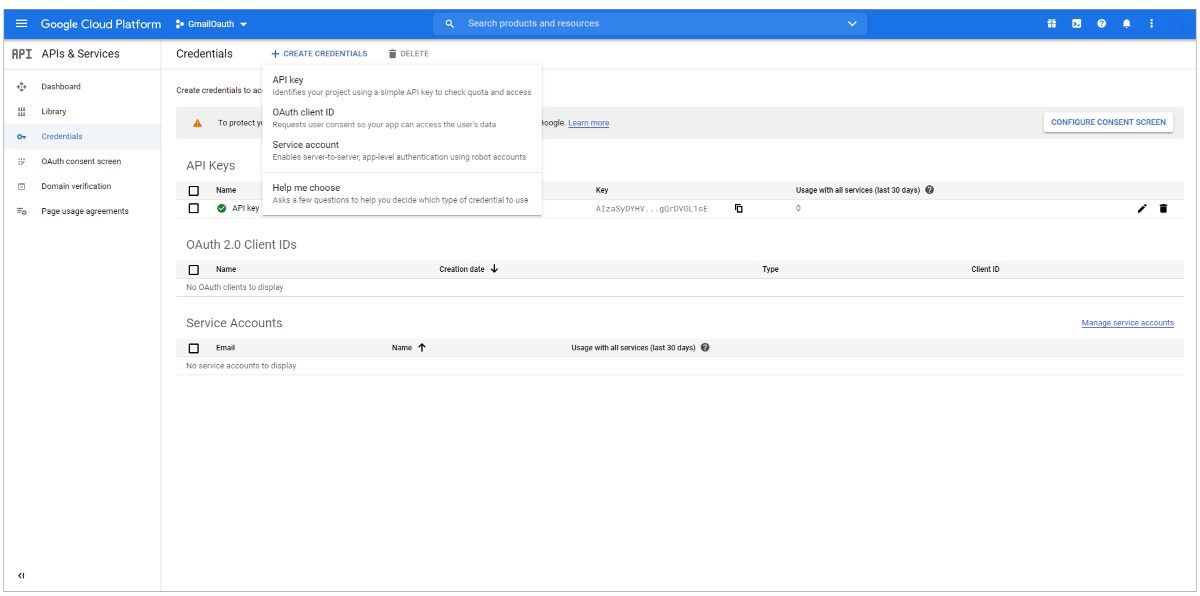
The **API key created** Web dialog appears.



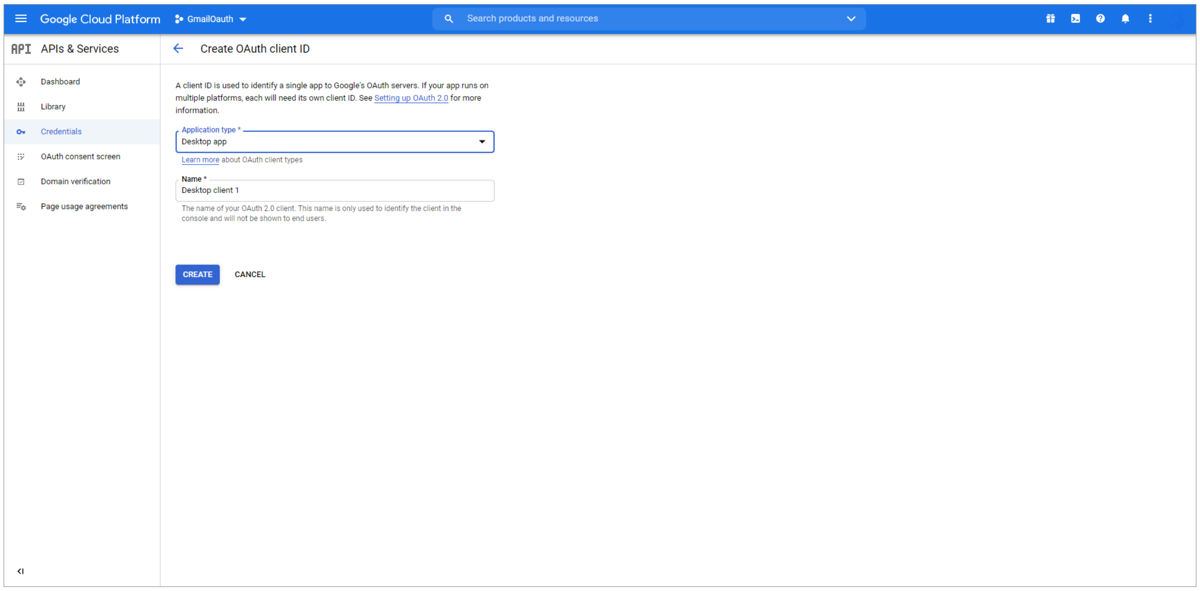
21. Click **RESTRICT KEY**. The **Restrict and rename API key** page appears.



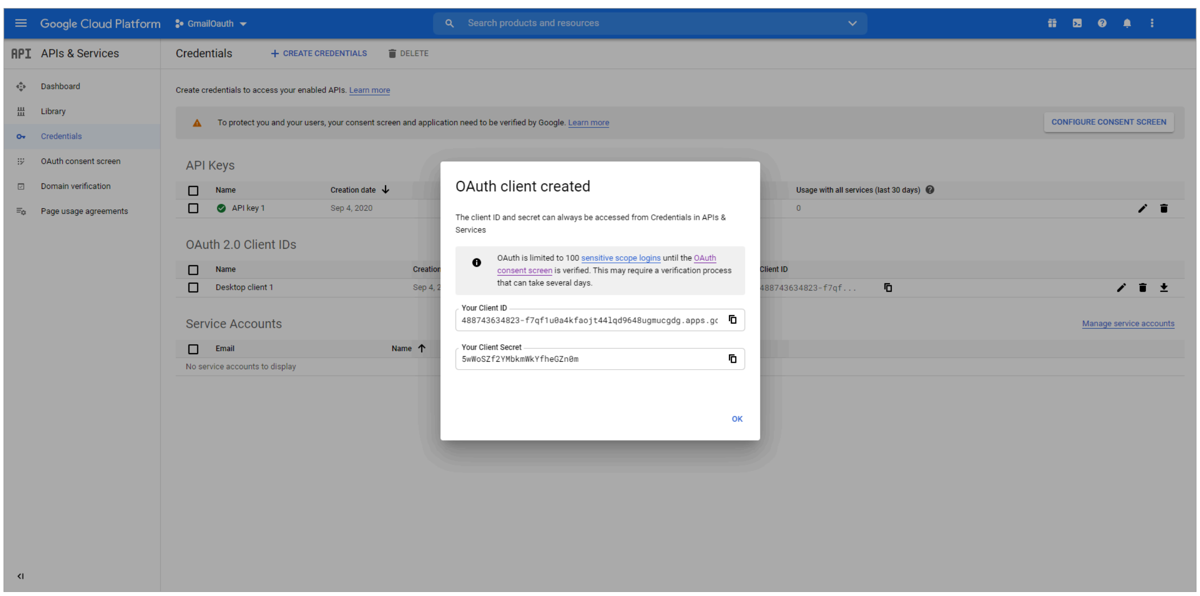
22. Under **Application restrictions**, select **None**.
23. Under **API restrictions**, select **Restrict key**.
24. Click **Save**.



25. On the left sidebar, click **Credentials** and then click **CREATE CREDENTIALS** > **OAuth client ID**. The **Create OAuth client ID** page appears.

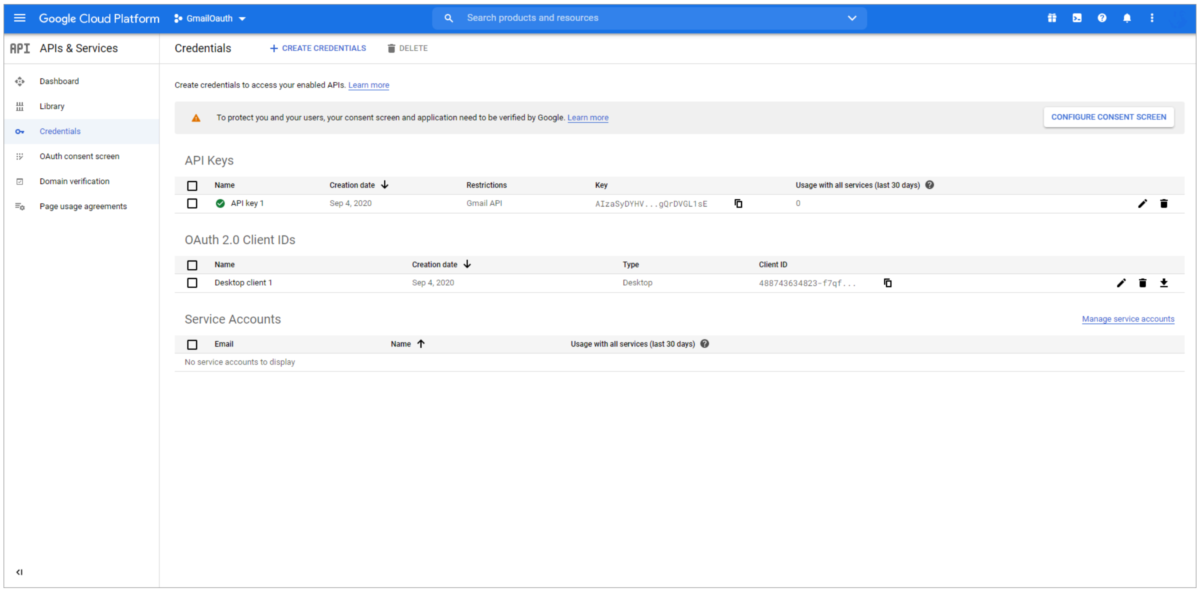


26. From the **Application type** list, select **Desktop app** and click **CREATE**.
The **OAuth client created** Web dialog appears.

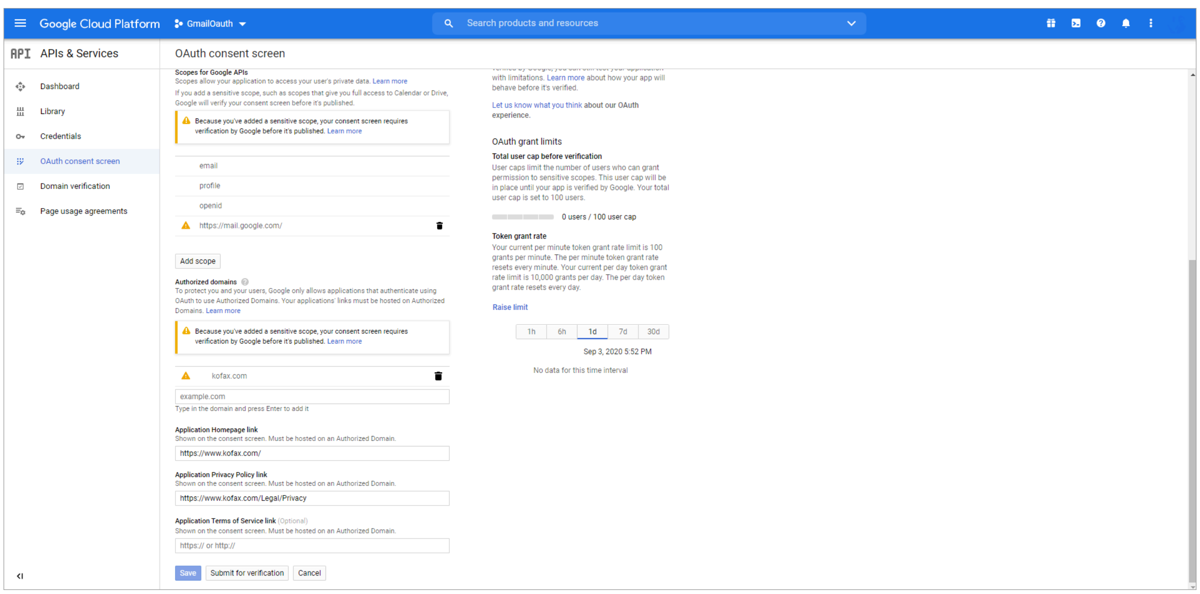


ⓘ Note down your Client ID and Client Secret as you will require them in Application configuration.

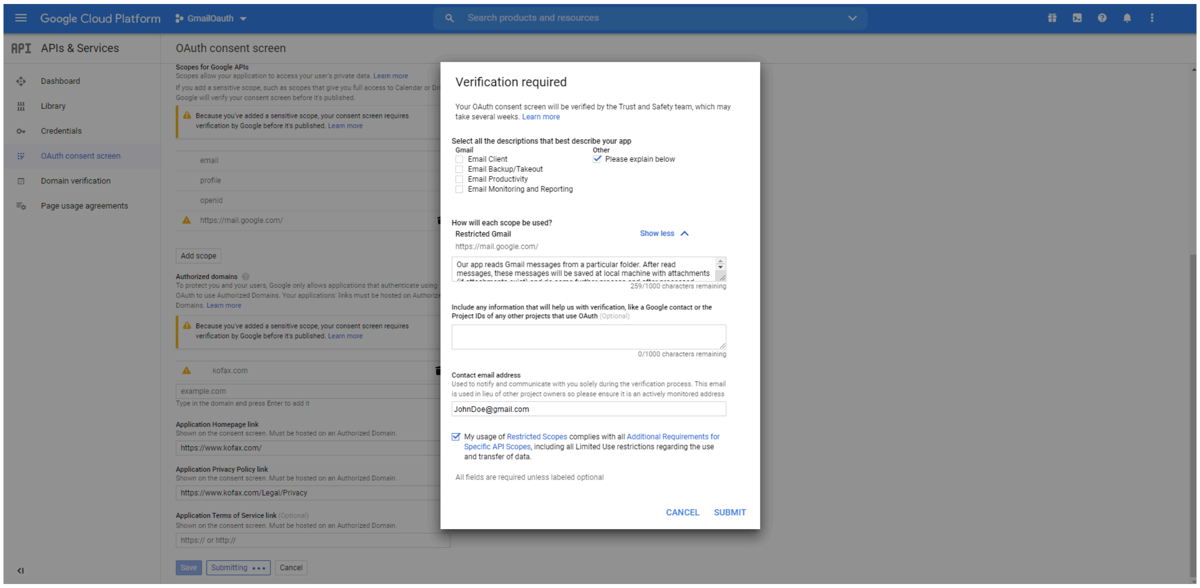
27. Click **OK**. The following page appears.



28. On the left sidebar, click **OAuth consent screen**.
    The **OAuth consent screen** appears.



29. Click **Submit for verification**. The **Verification required** Web dialog appears.



30. Select the **Please explain below** check box, and in the **How will each scope be used?** field, provide a meaningful explanation.

For example, see the following explanation.

```
"Our application will read Gmail messages from a particular Gmail folder.
After reading messages, the messages will be saved on a local computer
with attachments (if any attachments exist) and will do further process.
If the process is  successful, messages will be deleted from the
Gmail folder."
```

31. In the **Contact email address** field, enter your contact email address.

32. Click **Submit**.

> At this point, the OAuth consent screen is verified, but application is yet to be verified. Unverified app does not impact anything.

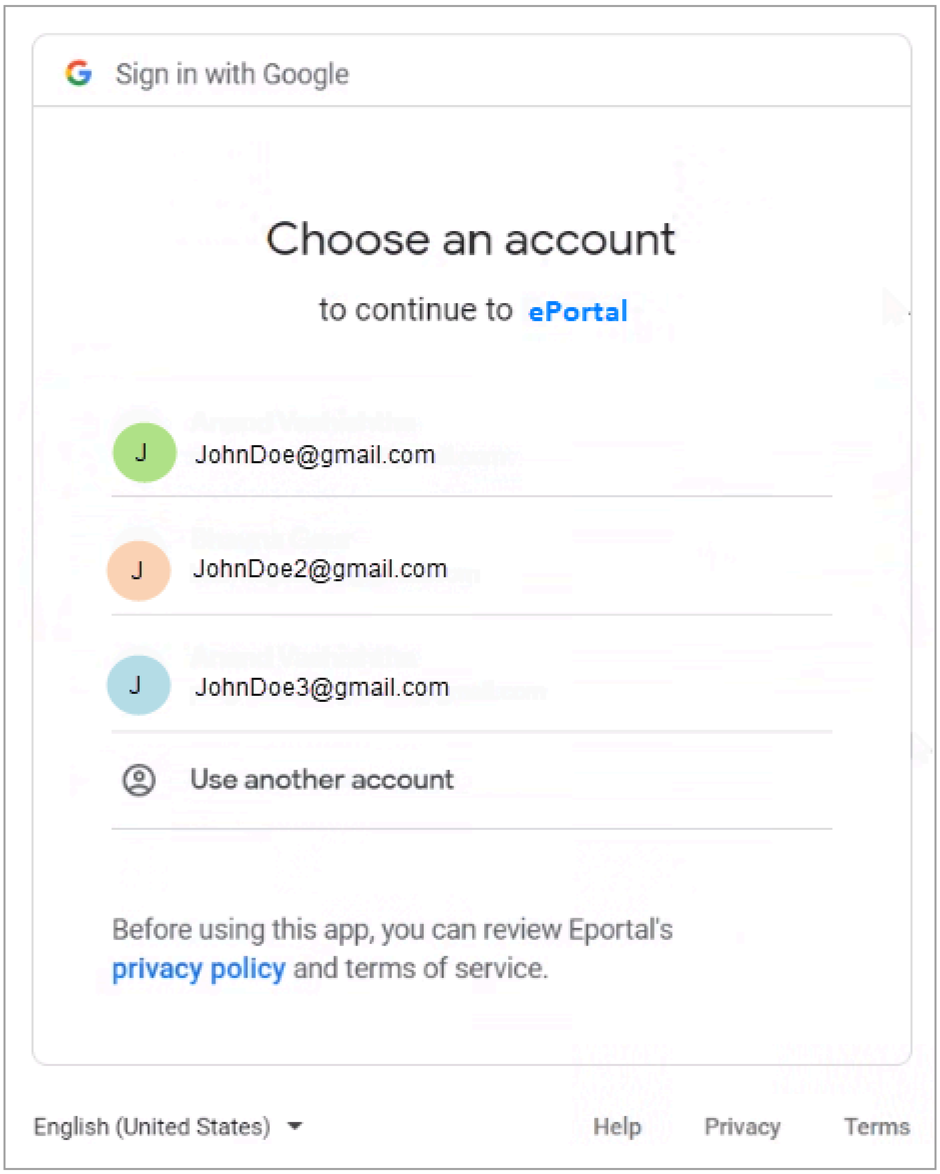
33. Copy the following XML content.

```
<MailAccount Id="Gmail_oauth" DisplayName="Gmail_oauth" Host="" Port="0"
 SSL="true"
          IgnoreCertificateErrors="false"
          UserName="abc.xyz@gmail.com" Protocol="IMAP_GMAIL"
          ClientID="178056894859-
ulbikaamqkjv1h1pkn4ftf575sllqlok.apps.googleusercontent.com"
          ClientSecretID="AkRN0wB-Y0RbqBoLJapsSnV8">
          <MailEncoding>UTF-8</MailEncoding>
          <DefaultCharset>UTF-8</DefaultCharset>
          <Folders>
            <Folder>Eportal_Input</Folder>
          </Folders>
          <Filter>UNSEEN</Filter>
          <Impersonate Enabled="false" />
          </MailAccount>
```

34. Open `C:\ProgramData\TIS\<eFlow6>\AppData\Server\<Application_name>\Setup\EPortal.AppConfig`, and paste the copied content under `<MailAccounts/>` section.

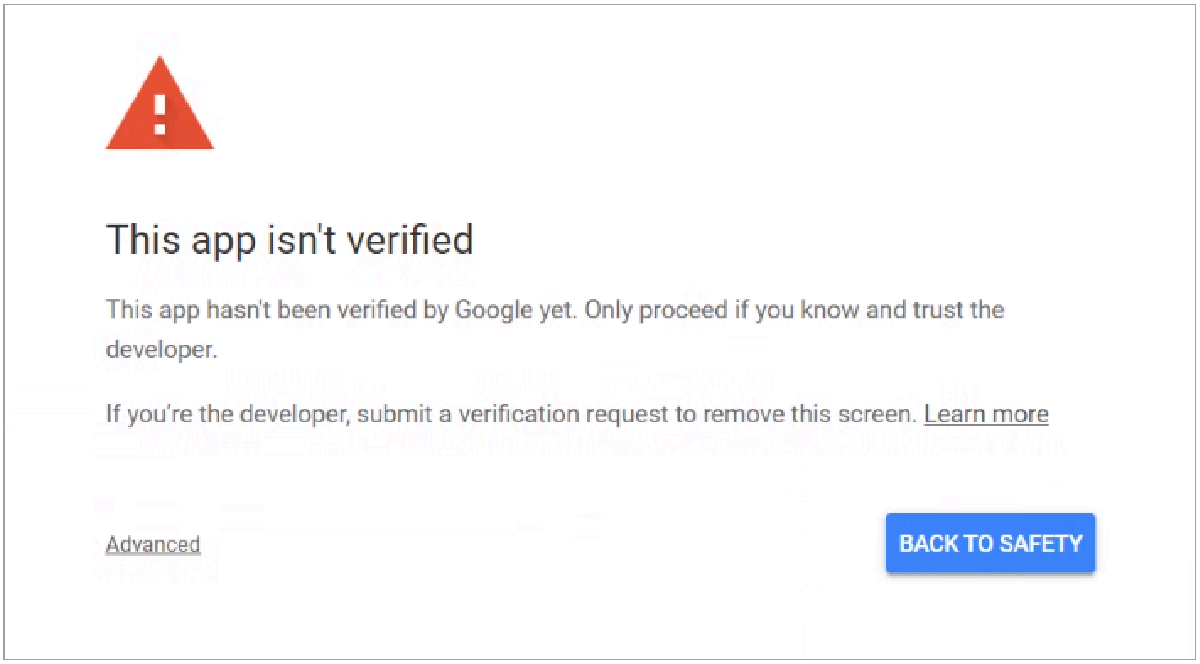
    If messages are in sub-folder of Gmail, then the folder structure will be like the following: <Folder>/Eportal_Input/<sub-folder name>/<Folder>

35. Change UserName, ClientID and ClientISecretID, and save the file.
36. In the **eFlow LaunchPro**, on the **Stations** list, select **ePortal manual station**.
    If opened for the first time the following page appears.

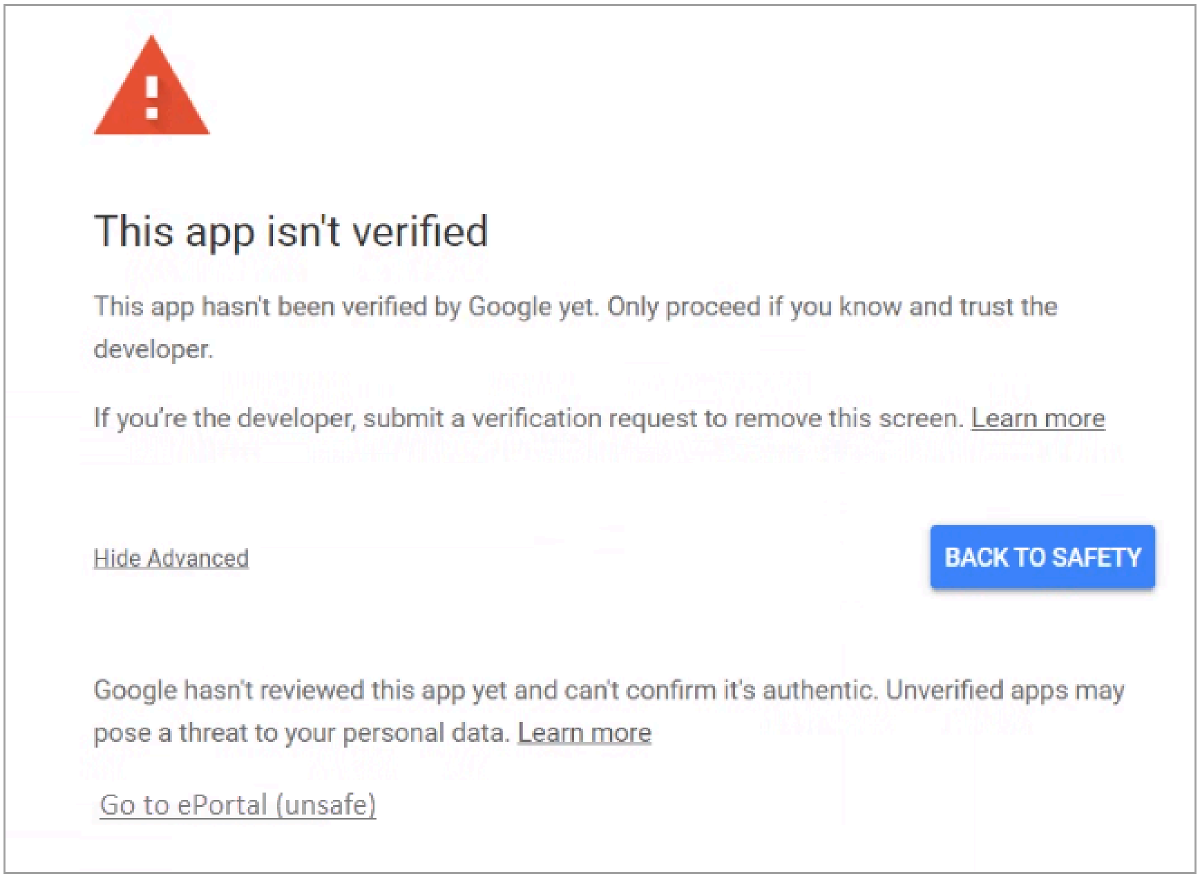


37. Select the Gmail account that you provided as the contact email address. The following page appears.

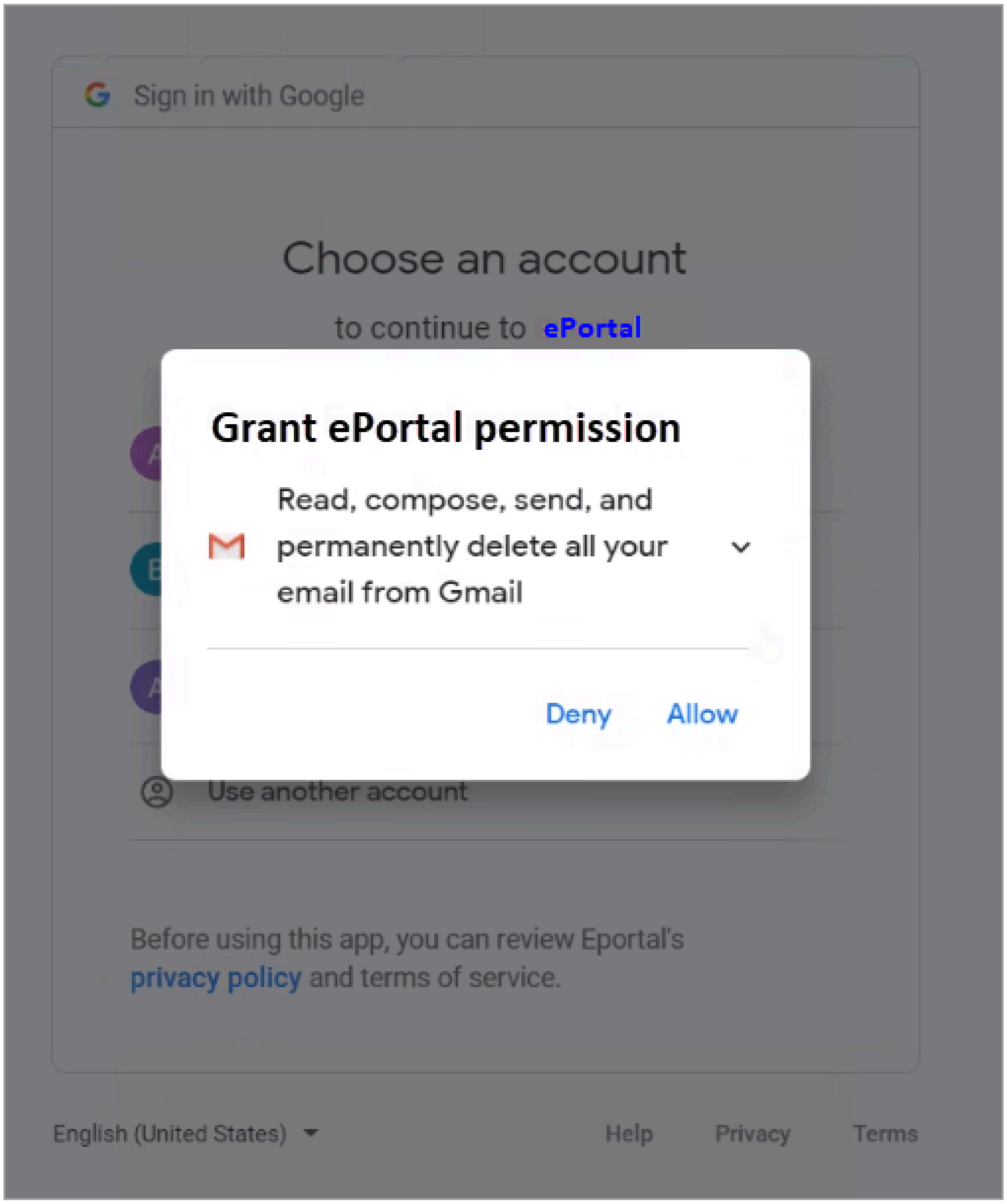
   If your Gmail account is not signed in from the computer where you are using the ePortal, then you need to sign in using your Gmail username and password.



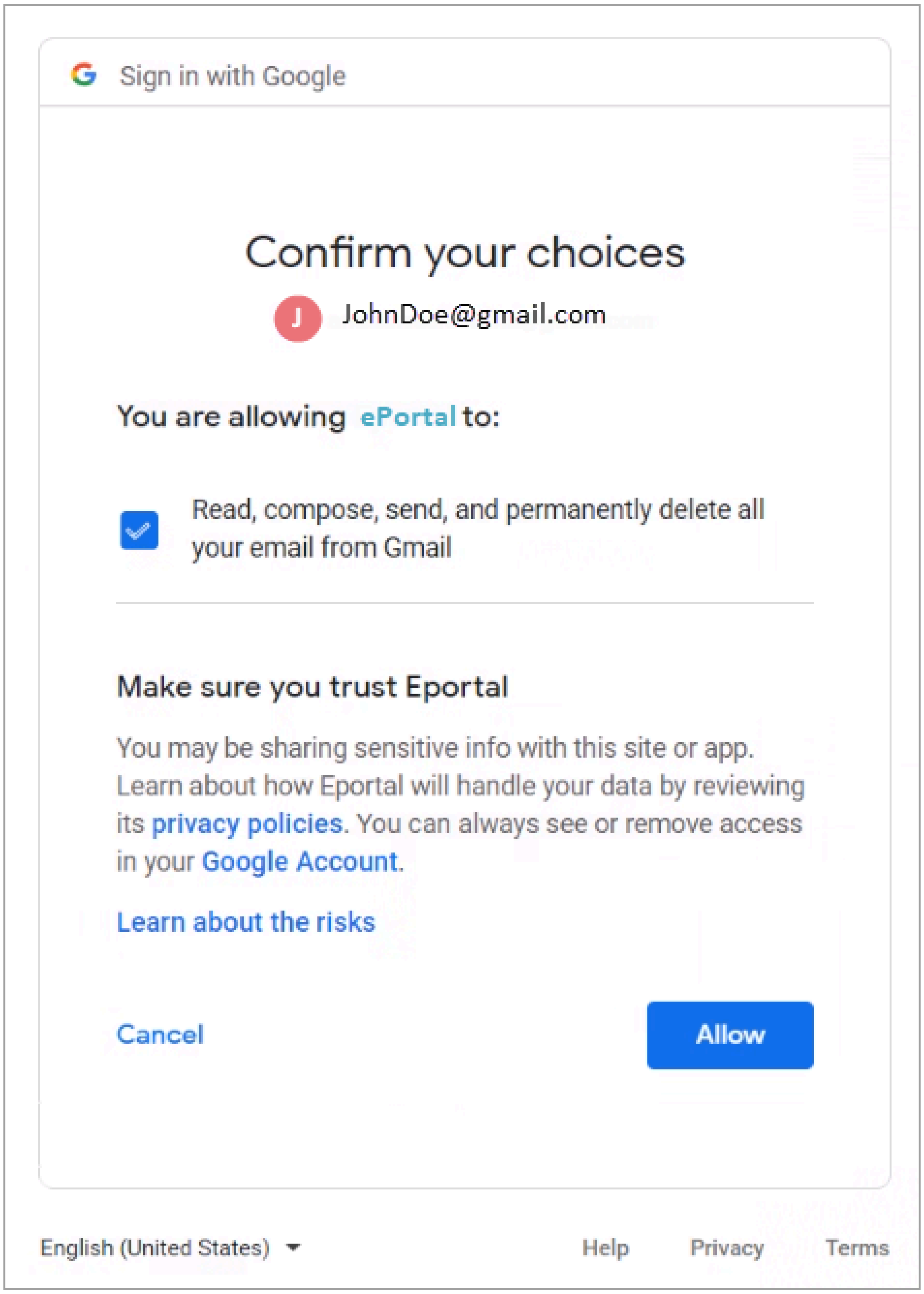
38. Click **Advanced**.
   The following page appears.



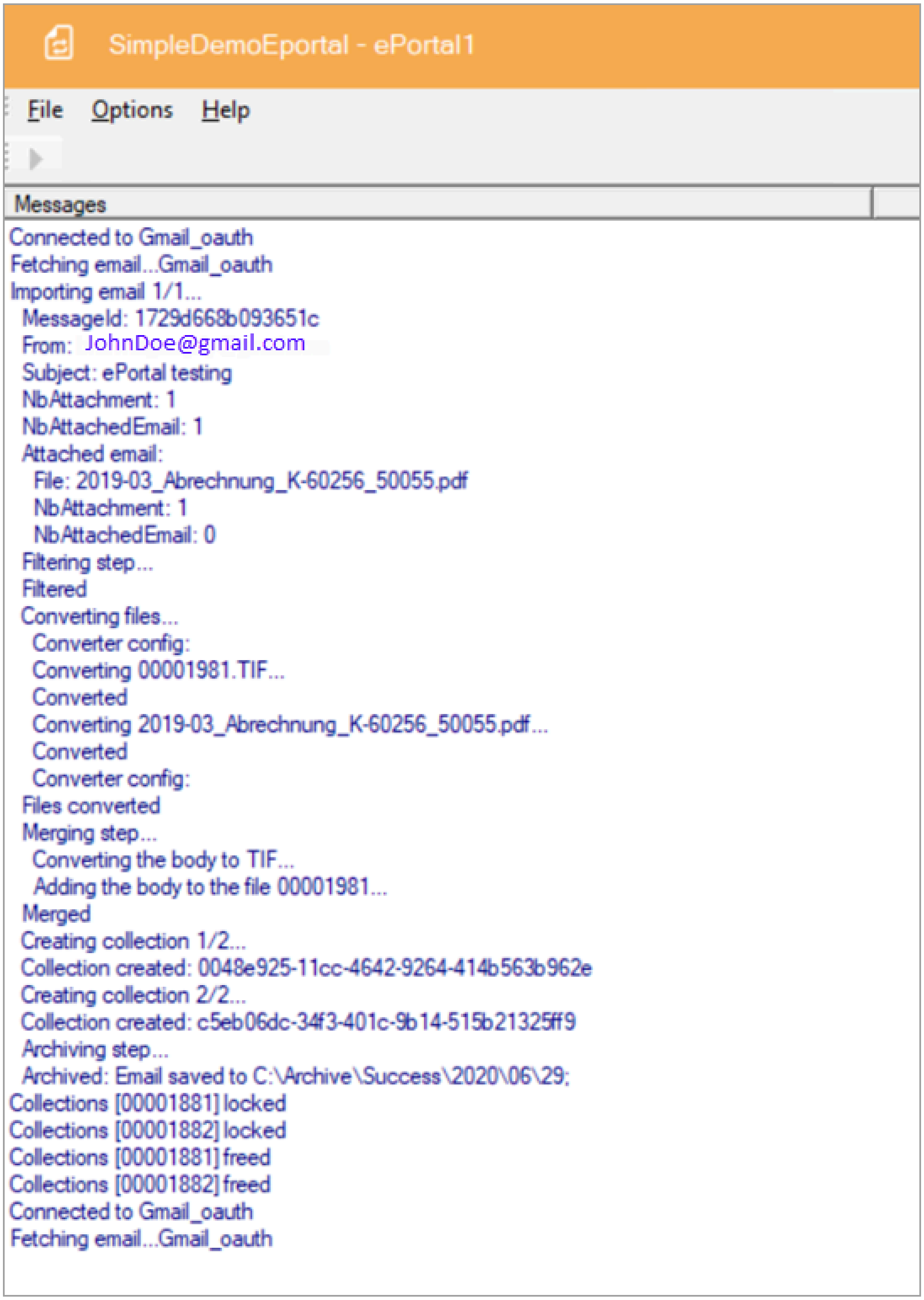
39. Click **Go to ePortal (unsafe)**.
    The **Grant ePortal permission** Web dialog appears.



40. Click **Allow**. The **Confirm your choices** page appears.



41. Click **Allow**.
42. After accepting the permission, the **ePortal Manual station** starts fetching the Gmail messages from the configured folder.


SimpleDemoEportal - ePortal1
File
Options
Help
Messages
Connected to Gmail_oauth
Fetching email...Gmail_oauth
Importing email 1/1...
MessageId: 1729d668b093651c
From: JohnDoe@gmail.com
Subject: ePortal testing
NbAttachment: 1
NbAttachedEmail: 1
Attached email:
File: 2019-03_Abrechnung_K-60256_50055.pdf
NbAttachment: 1
NbAttachedEmail: 0
Filtering step...
Filtered
Converting files...
Converter config:
Converting 00001981.TIF...
Converted
Converting 2019-03_Abrechnung_K-60256_50055.pdf...
Converted
Converter config:
Files converted
Merging step...
Converting the body to TIF...
Adding the body to the file 00001981...
Merged
Creating collection 1/2...
Collection created: 0048e925-11cc-4642-9264-414b563b962e
Creating collection 2/2...
Collection created: c5eb06dc-34f3-401c-9b14-515b21325ff9
Archiving step...
Archived: Email saved to C:\Archive\Success\2020\06\29;
Collections [00001881] locked
Collections [00001882] locked
Collections [00001881] freed
Collections [00001882] freed
Connected to Gmail_oauth
Fetching email...Gmail_oauth

EXCHANGE_ONLINE connector

EXCHANGE_ONLINE connector is an upgraded version of EWS connector, which implements OAuth for secure delegate access. This connector does not require password for the mail account configuration in the EPortal.AppConfig file.

The EXCHANGE_ONLINE connector retrieves a batch of emails from a Microsoft Exchange Server or Office 365 using Microsoft graph API and Oauth 2.0 mechanism in Azure cloud. After all emails from the batch are parsed, the connector returns an eBatch that can be processed by each ePortal stage.

Unsynchronized mode

Depending on the archive configuration, the emails in the mailbox are deleted, moved, or set as read after the eDocs are imported into the eFlow workflow.

By default, ePortal sets imported files as READ, so when ePortal retrieves emails with the exchange online filter `IsRead=false`, it will only import new emails.

Synchronized mode

Not required.

Autorun mode

Disable autorun mode in below scenarios and run the ePortal manual station.

Scenario 1: Whenever you add a new email account in EXCHANGE_ONLINE protocol, in the EPortal.AppConfig file, manually authorize yourself in ePortal station by entering configured email account credentials and permissions consent.

Scenario 2: When the password for your email account expires or changes, re-authorize yourself by opening ePortal station manually.

Enable the autorun mode for ePortal station.

Configuration

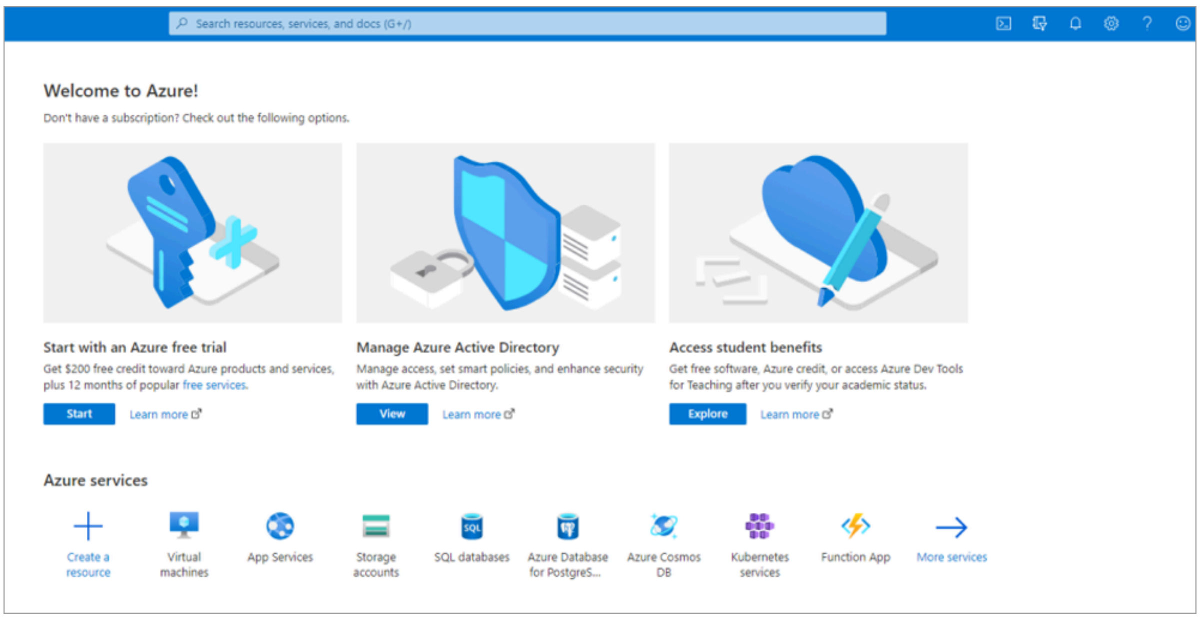
Any application that implements OAuth standard to authenticate and authorize its users, the application needs to be registered with the corresponding Application/Web servers.

The following step-by-step procedure explains how to register an ePortal application, and the minimum set of privileges needed for it. More granular role-based access privileges are possible, but this is subjected to the IT polices of the individual organizations.

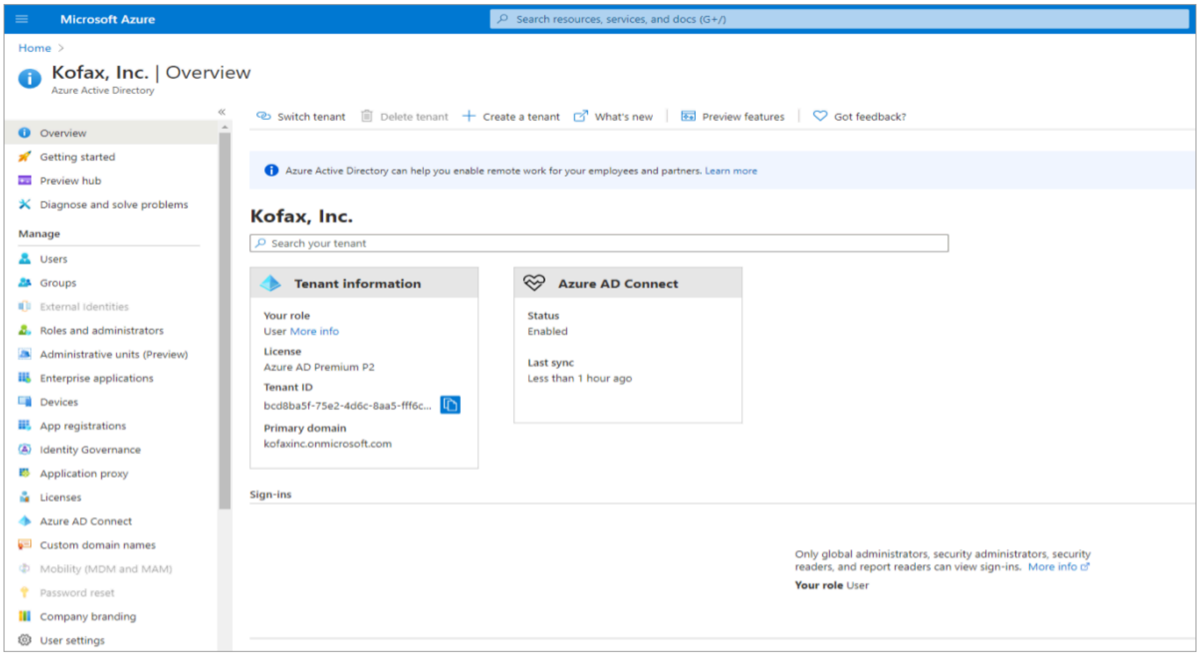
Azure cloud configuration for Office 365

This section describe the Azure cloud configuration for Office 365. After you configure Azure cloud, ePortal automatically can read emails from Outlook.

The figures and user interfaces used in the following procedure are taken from the Microsoft Azure website and they might change occasionally. Hence, we request you to follow the latest procedure mentioned in the Microsoft Azure website, which is updated time-to-time. If you still face issues while authorizing your application, we recommend to take assistance from the user who has expertise in authorizing an application.

1. Sign in to `https://portal.azure.com` using your work account. Follow the on-screen instructions to complete the sign in procedure.
   After a successful sign-in, the Azure home page appears.
   

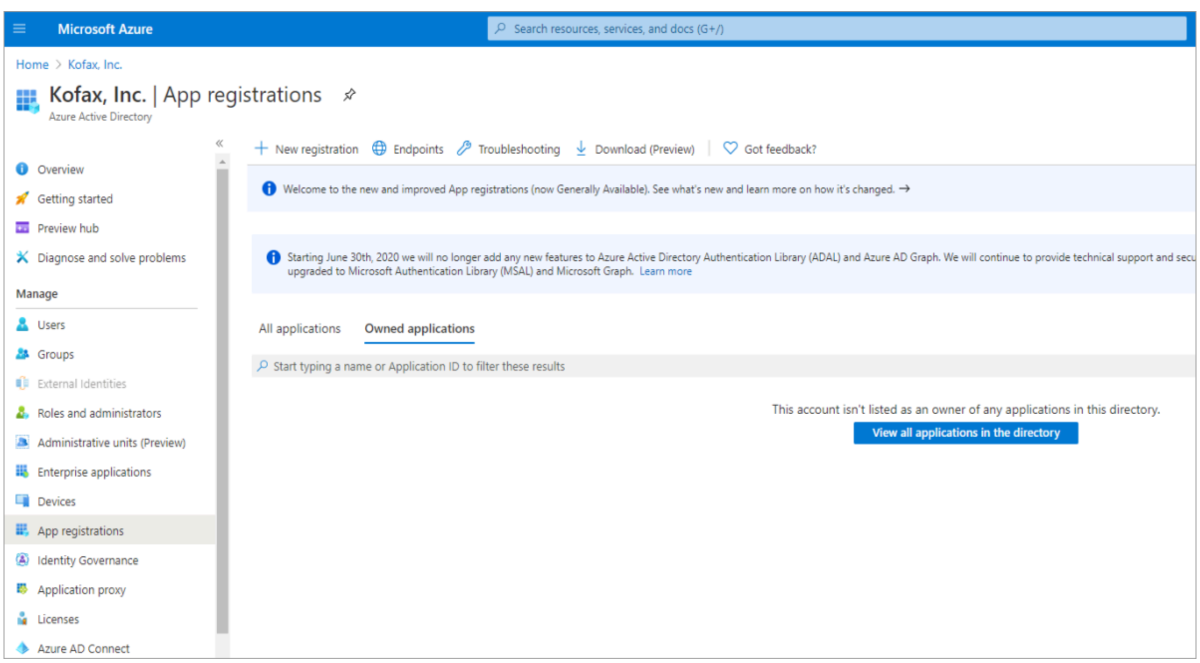
2. On the Azure home page, under **Manage Azure Active Directory**, click **View**.
   The **Overview** page appears.



Manage App registrations

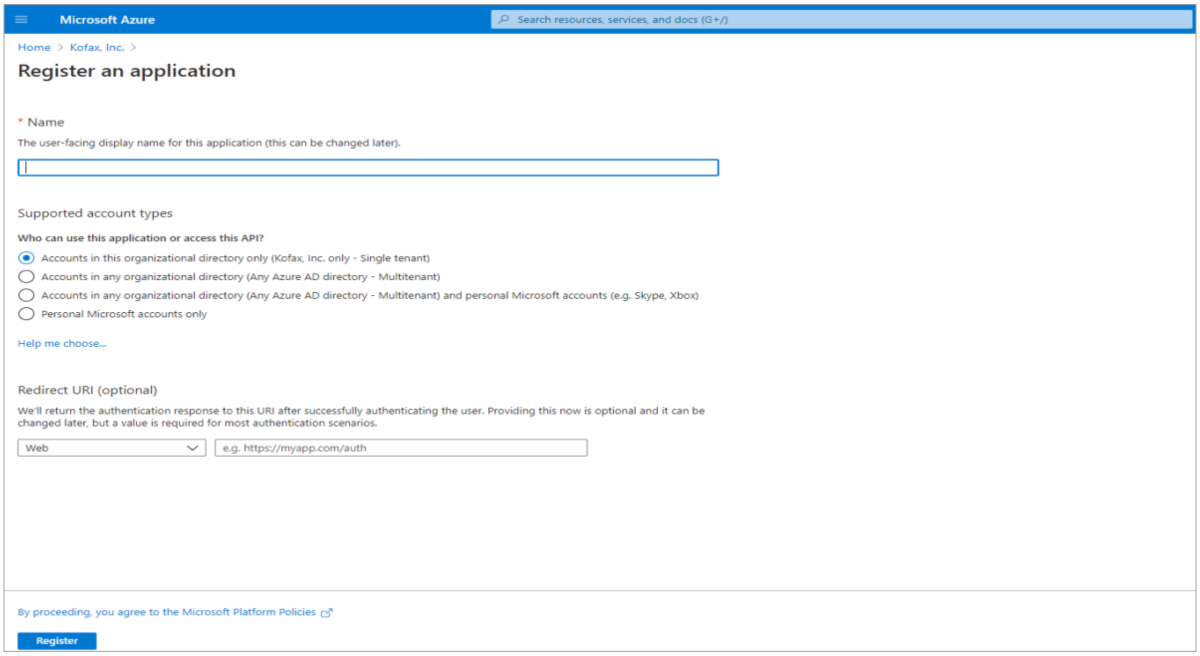
Register your application. You can register your application in a directory or outside of a directory.

1. On the left sidebar, under **Manage**, click **App registrations**.
   The **App registrations** page appears.



2. Click **New registration**.

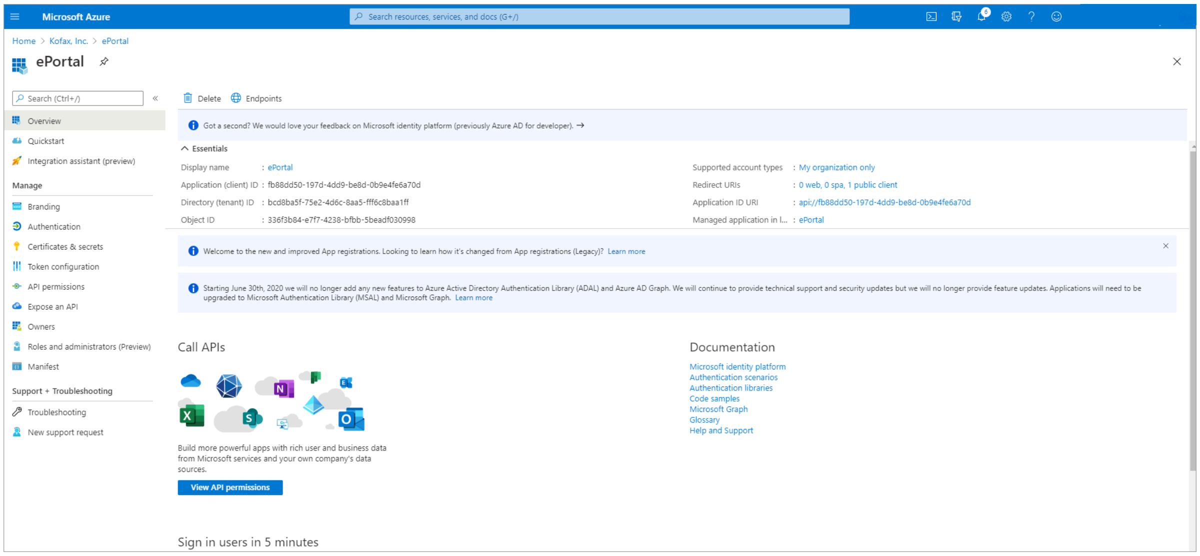
The **Register an application** page appears.



3. In the **Name** field, type the application name that is to be displayed to the users.
4. Under **Supported account types**, select **Accounts in this organizational directory only (Kofax, Inc. only - Single tenant)**.

   Select this option if you want to build a Line-of-Business (LOB) application. It maps only a single tenant to Azure AD (Active Directory). This is the default option and is only available if you register your application in a directory. The default is Azure AD multi-tenant and personal Microsoft accounts if you register the application outside of a directory.

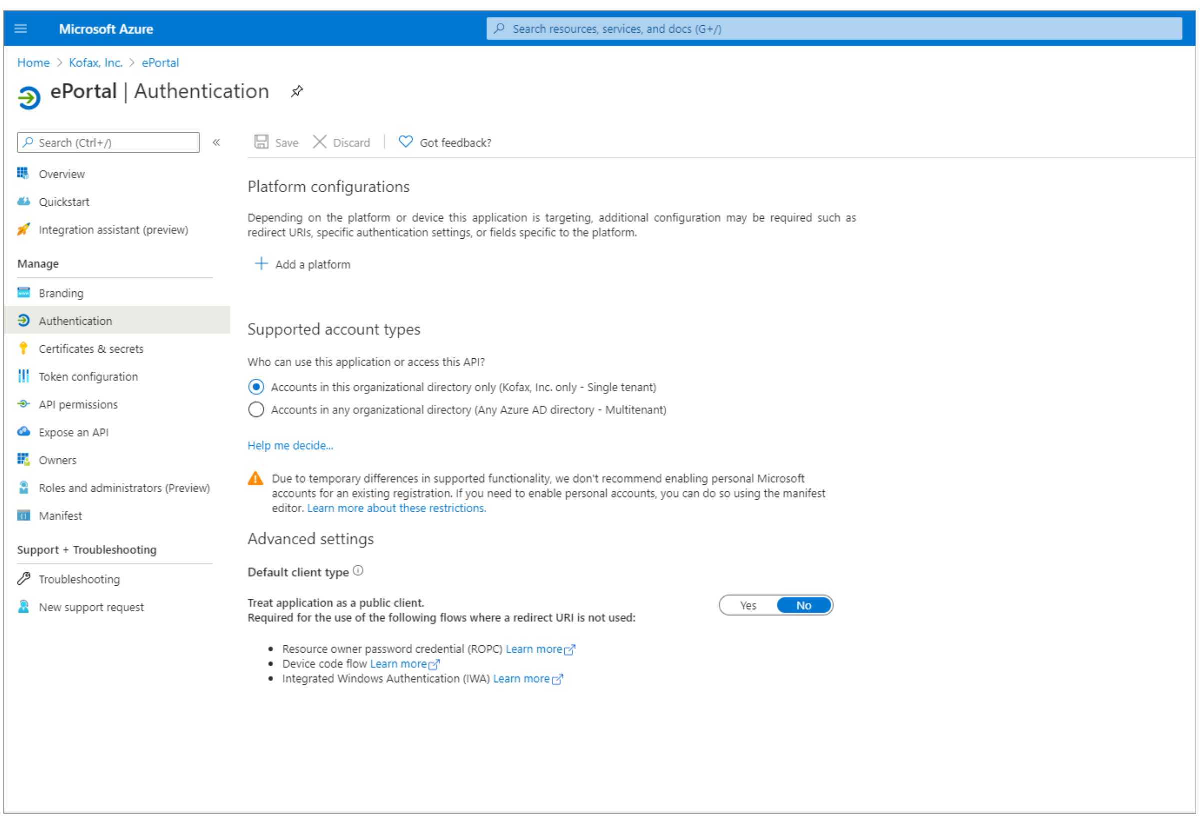
5. Under **Redirect URI (optional)**, select **Public client/native (mobile & desktop)** from the list and click **Register**.
   The following page appears.



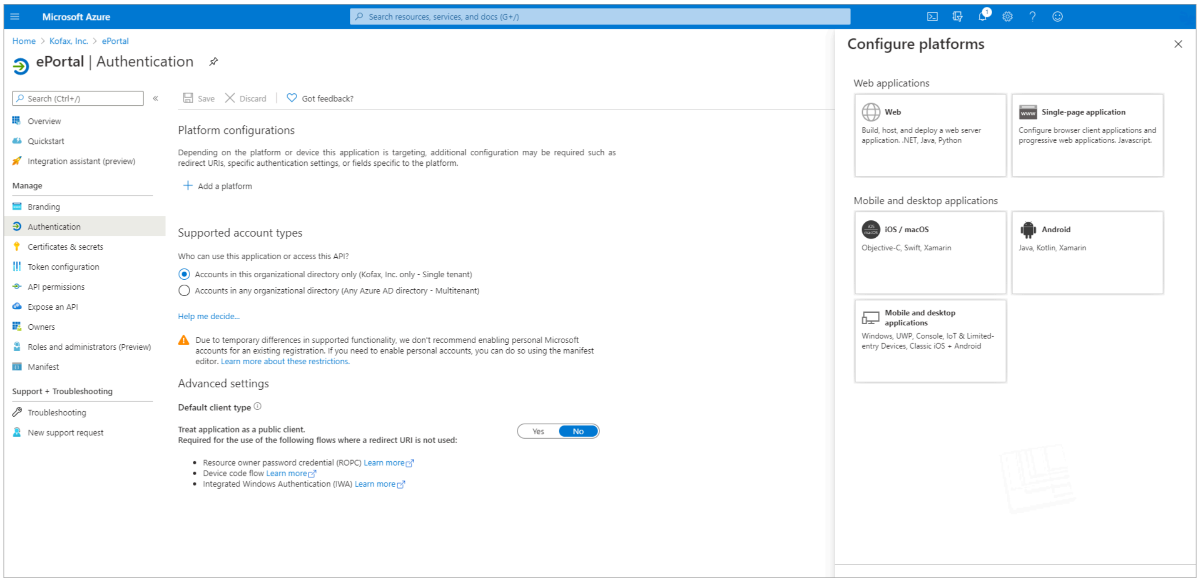
Manage authentication

You can configure application settings based on the platform or device you are targeting.

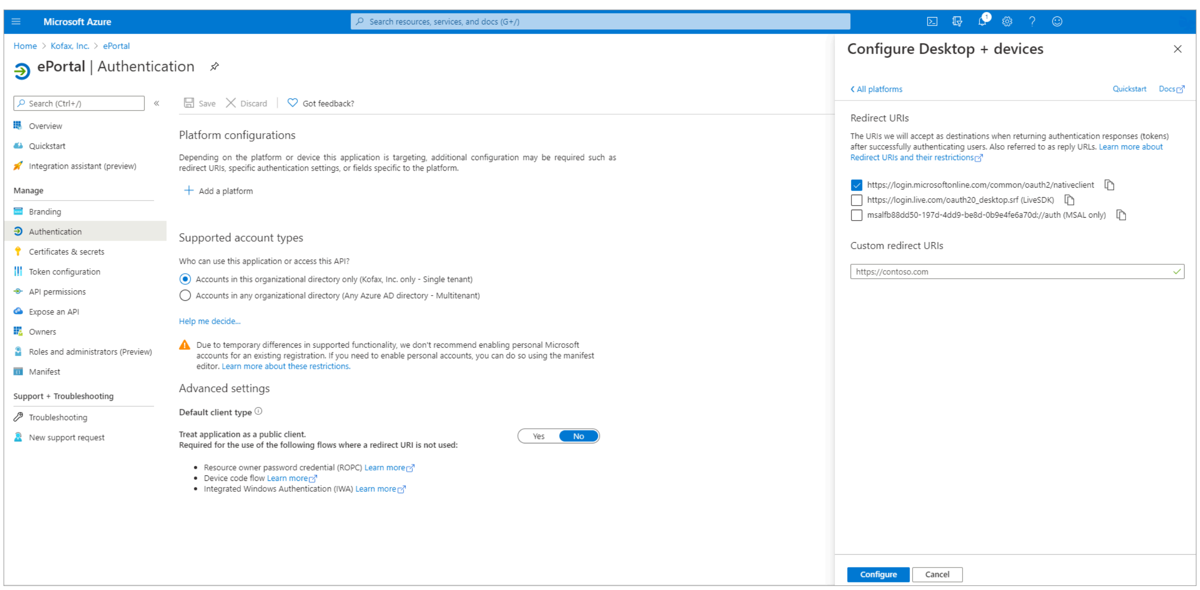
1. On the left sidebar, under **Manage**, click **Authentication**.
   The **Authentication** page appears.



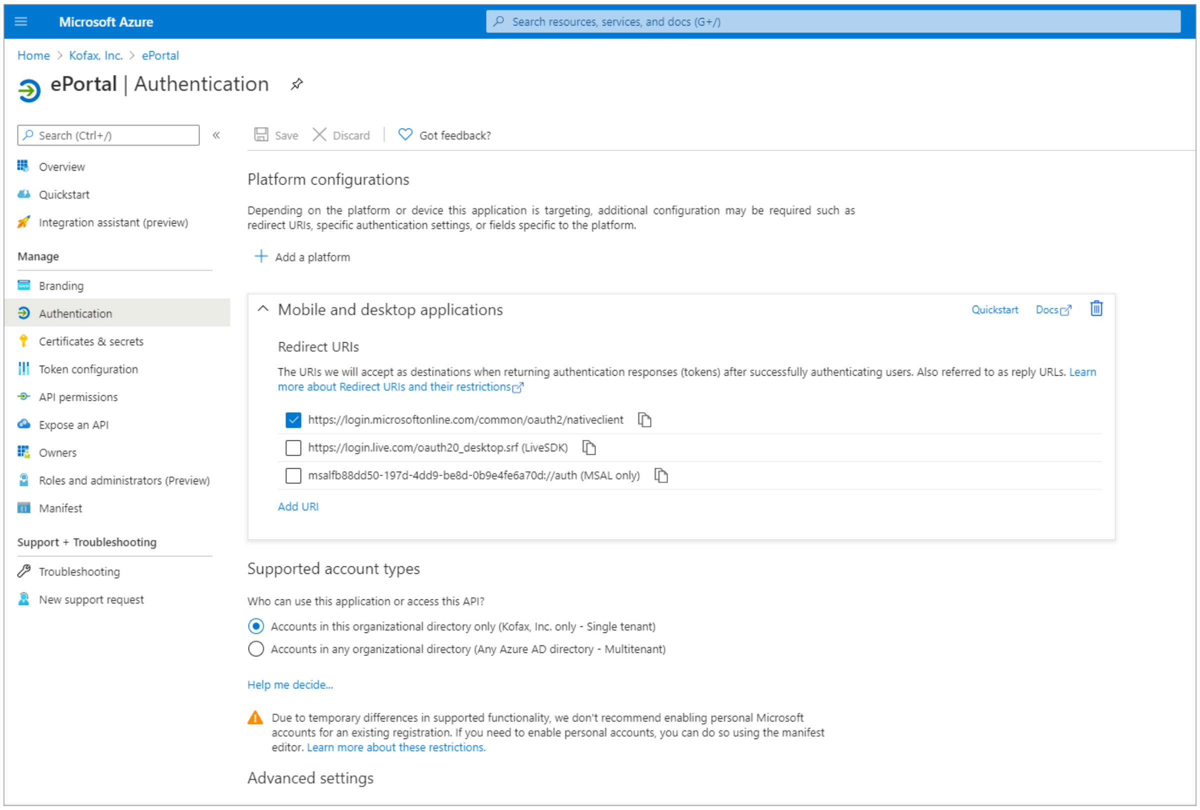
2. Under **Platform configurations**, click **Add a platform**.
   The **Configure platforms** section appears on the right side of the page.



3. Click **Mobile and desktop applications**.
   The **Configure Desktop + devices** section appears on the right side of the page.



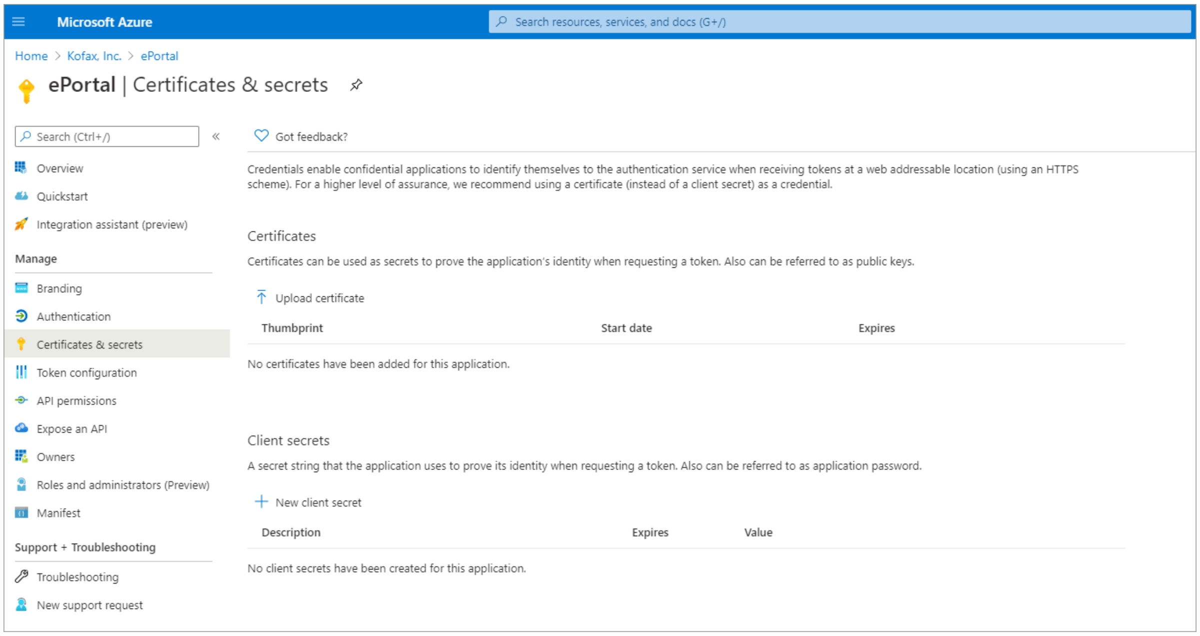
4. Select **https://login.microsoftonline.com/common/oauth2/nativeclient**, and click **Configure**.
   On the **Authentication** page, under **Redirect URIs**, you can see the selected option.



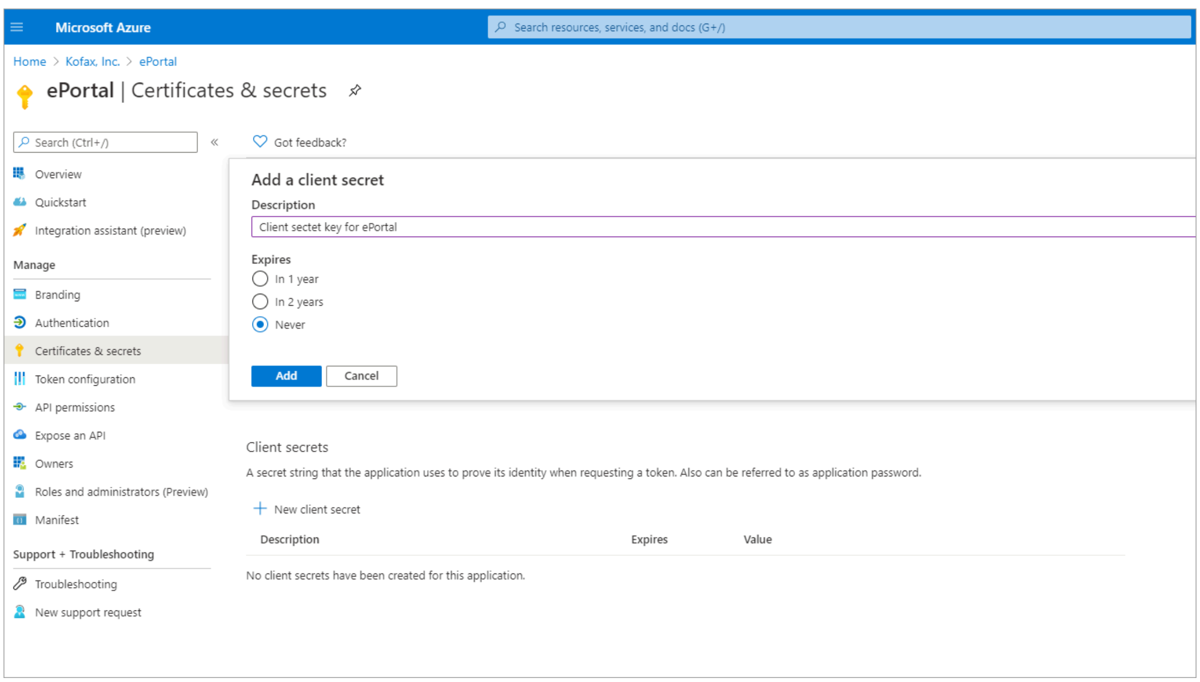
Manage certificates and secrets

Upload certificates or create client secrets to enable confidential applications.

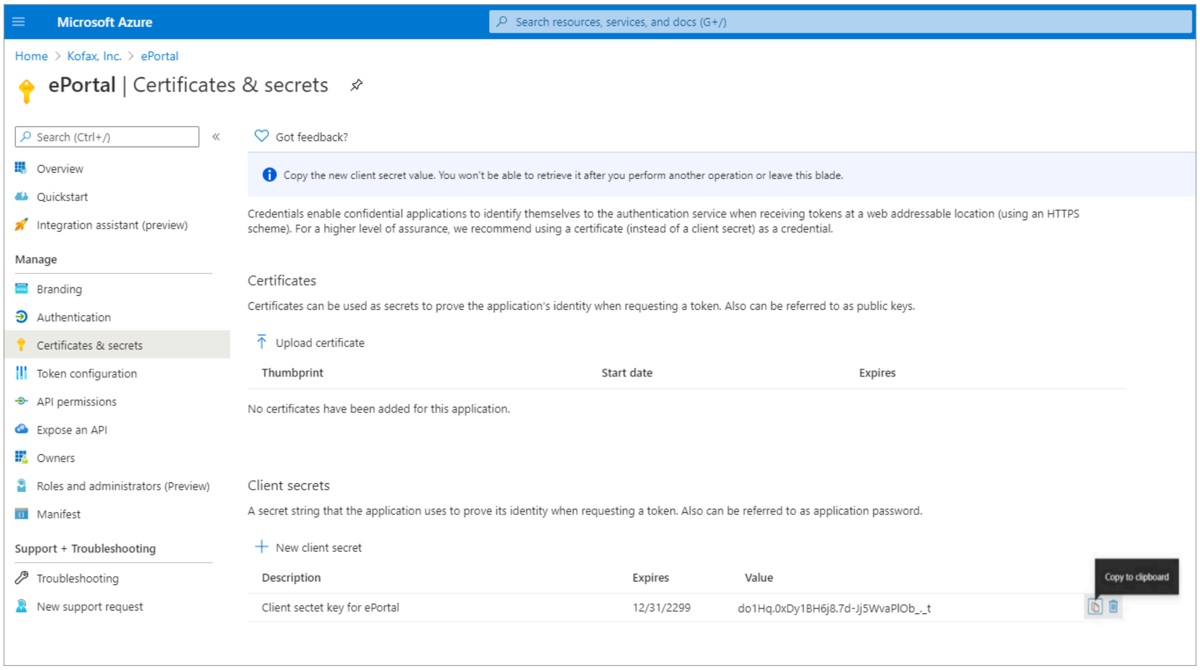
1. On the left sidebar, under **Manage**, click **Certificate & secrets**.
   The **Certificate & secrets** page appears.



2. Under **Client secrets**, click **New client secret**.
   The **Add a client secret** pop-up appears.



3. In the **Description** box, enter a description.
4. Under **Expires**, select **Never**.
5. Click **Add**.
   On the **Certificates & secrets** page, under **Client secrets**, you can see the client secret details.

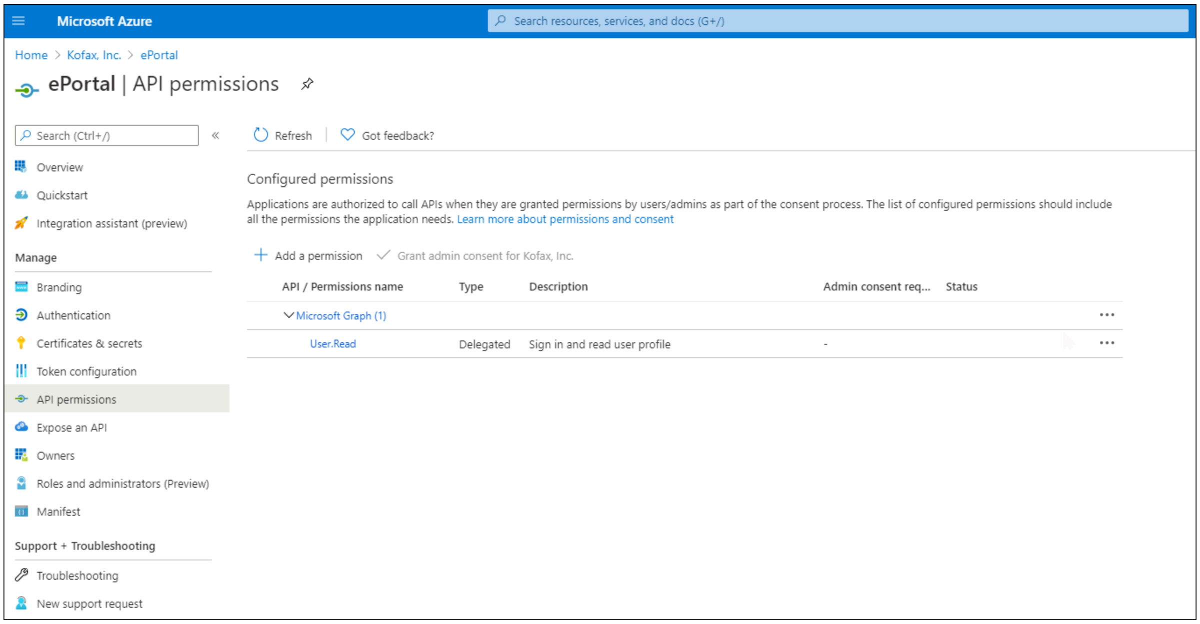


Note down the Client secrets value which can be referred in future activities.

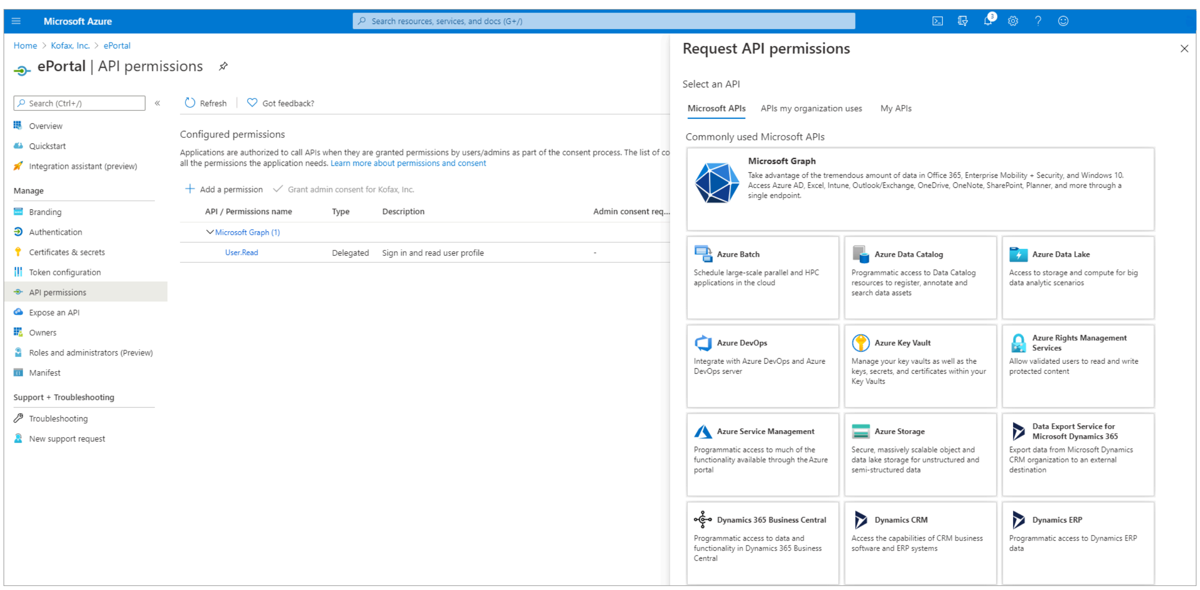
Manage API permissions

Add the required permissions to authorize applications to call APIs.

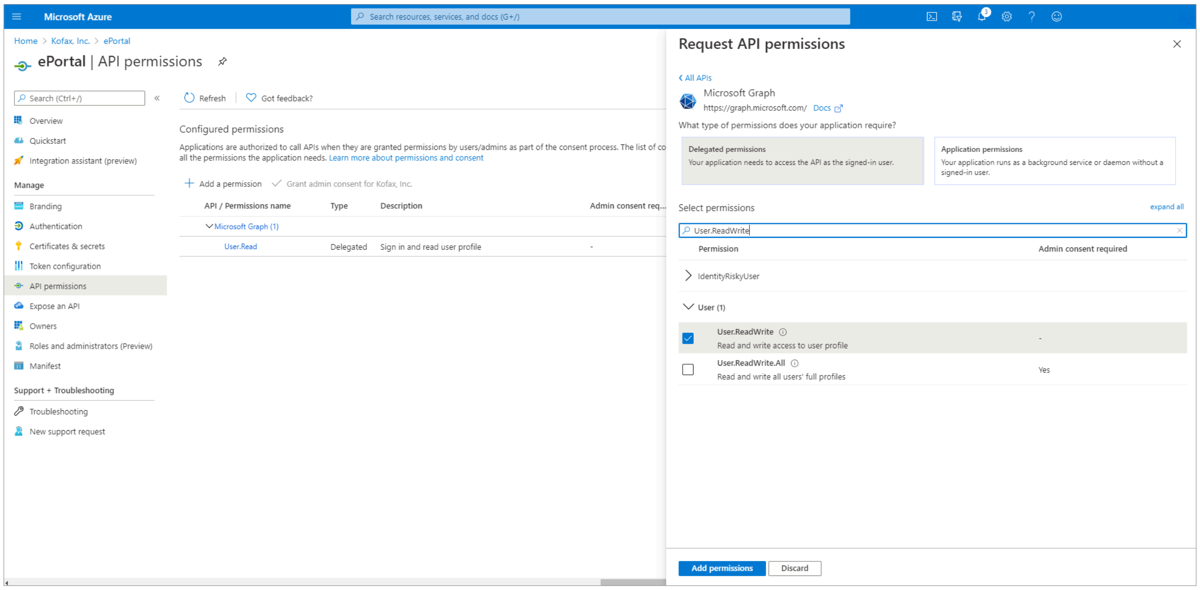
1. On the left sidebar, under **Manage**, click **API permissions**.
   The **API permissions** page appears.



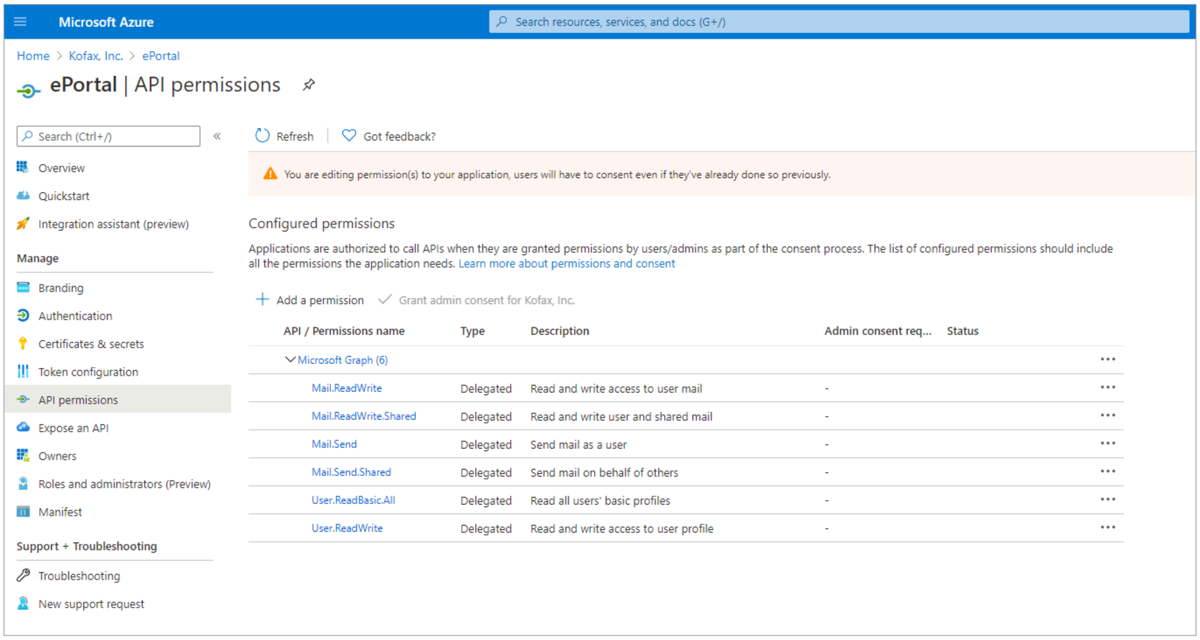
2. Under the **Configured permissions**, click **Add a permission**.
   The **Request API permissions** section appears on the right side of the page.



3. Click **Microsoft Graph**.



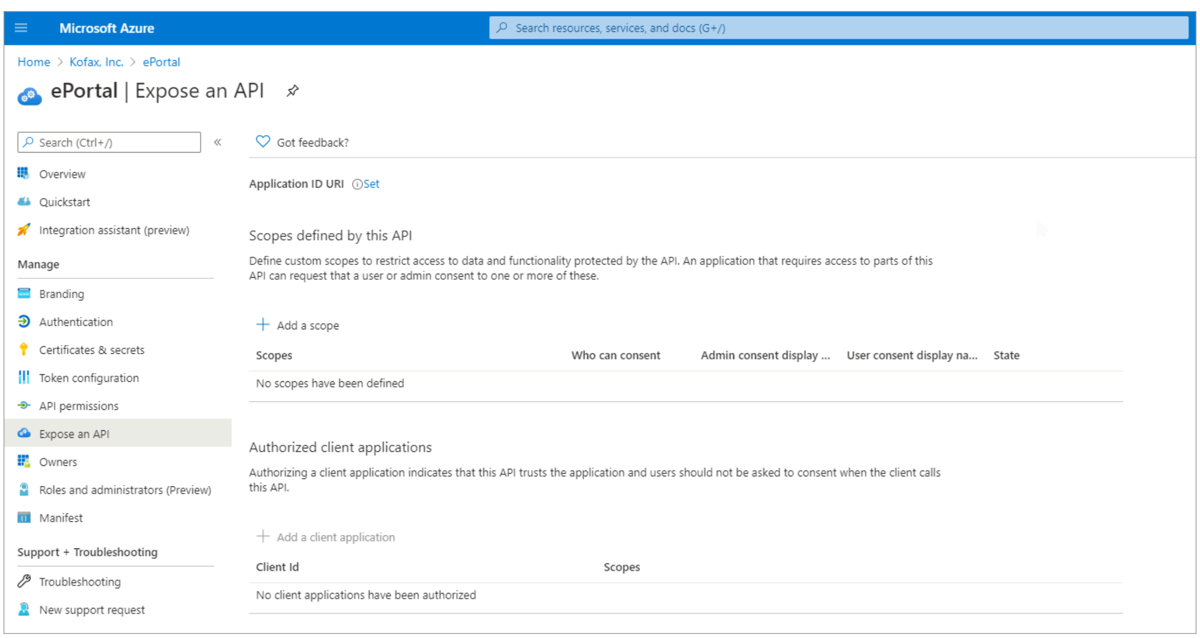
4. Click **Delegated permissions** > **Select Permission**, and then select the following six permissions:
   - Mail.ReadWrite
   - Mail.ReadWrite.Shared
   - Mail.Send
   - Mail.Send.Shared
   - User.ReadBasic.All
   - User.ReadWrite
5. Click **Add permissions**.
   On the **API permissions** page, under **API / Permissions name**, you can see all six permissions.



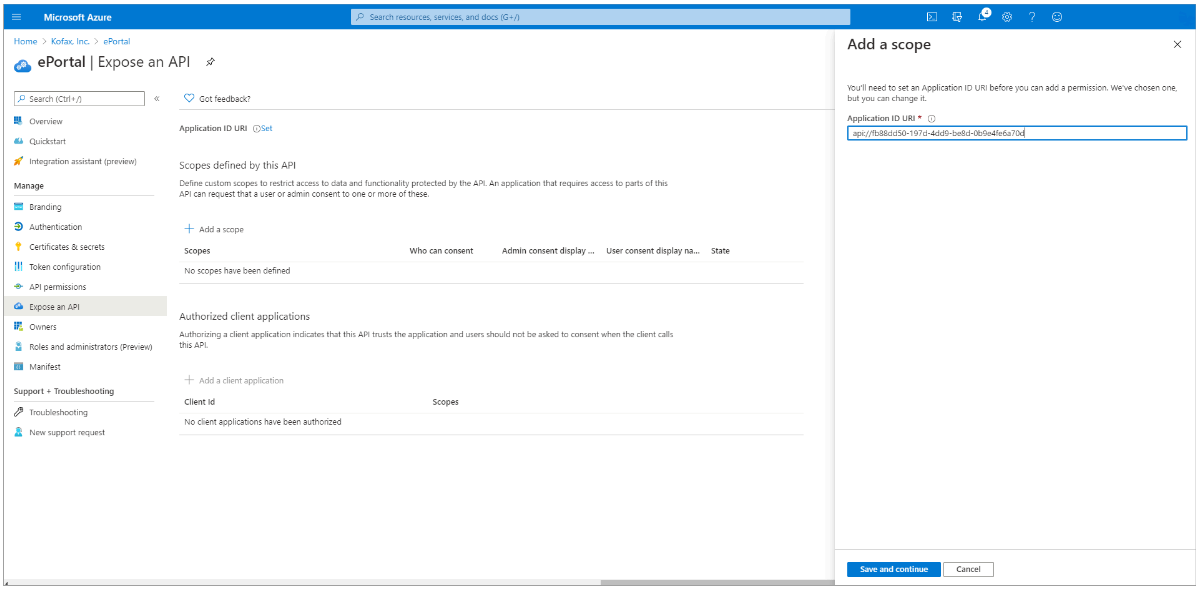
Manage exposing an API

Define the scope to allow or restrict access to data or functionality protected by an API.

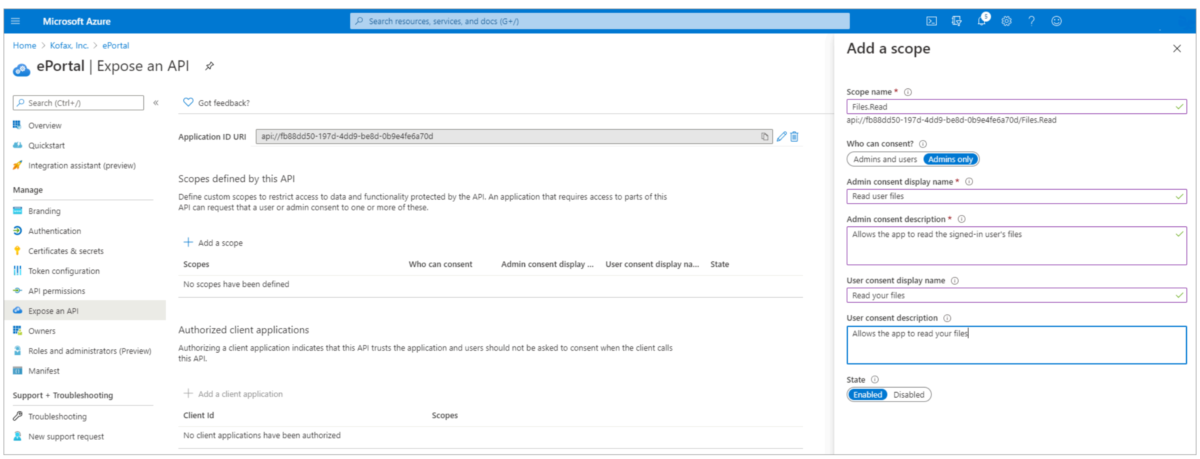
1. On the left sidebar, under **Manage**, click **Expose an API**.
   The **Expose an API** page appears.



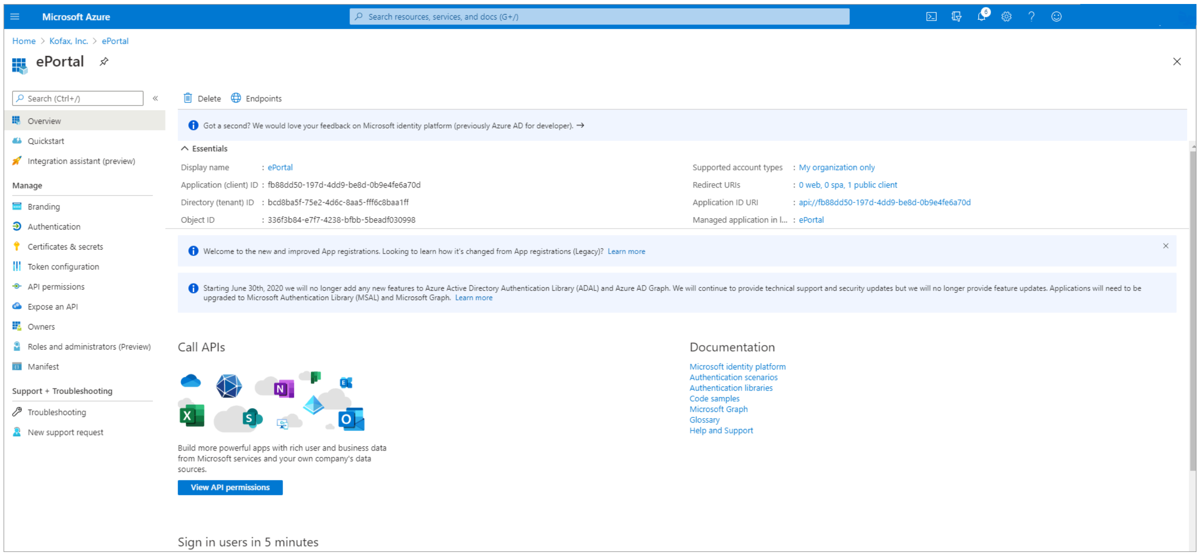
2. Under **Scopes defined by this API**, click **Add a scope**.
   The **Add a scope** section appears on the right side of the page.



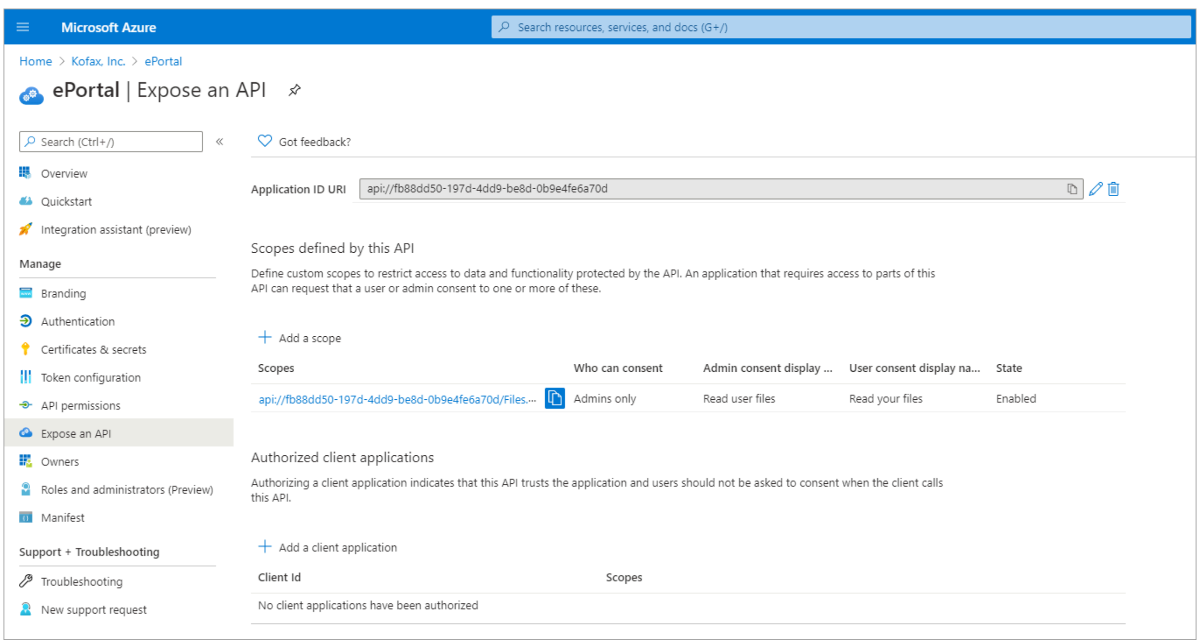
3. Click **Save and continue**.



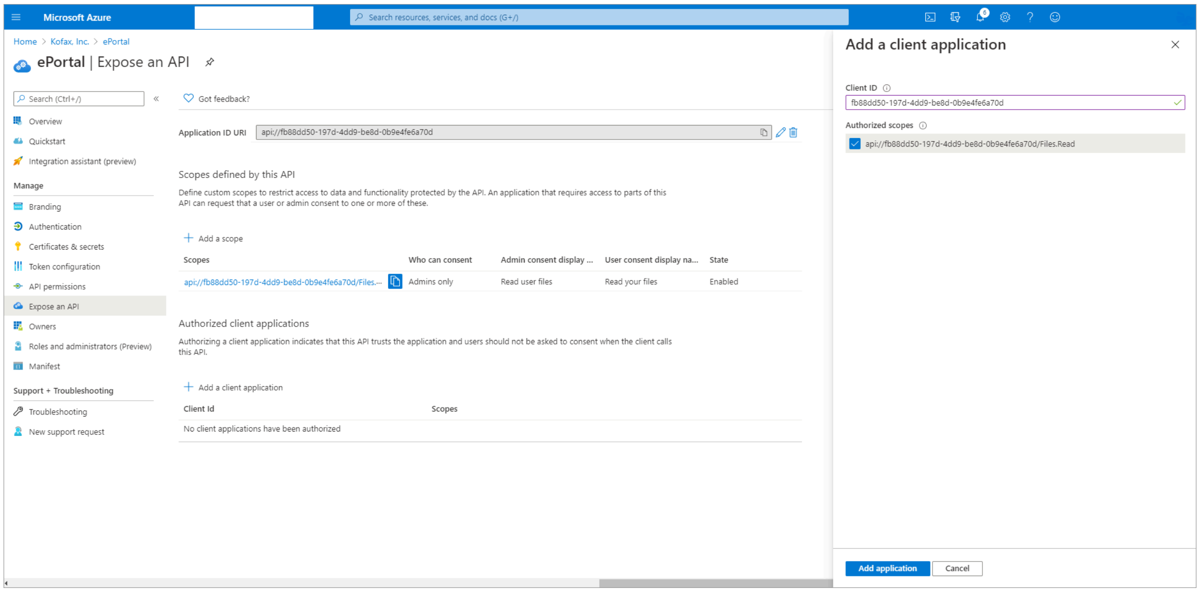
4. For **Who can consent?**, select **Admins only**.
5. For **State**, select **Enabled**.
6. Click **Add scope**.
7. On the left sidebar, click **Overview**.
   The **Overview** page appears.



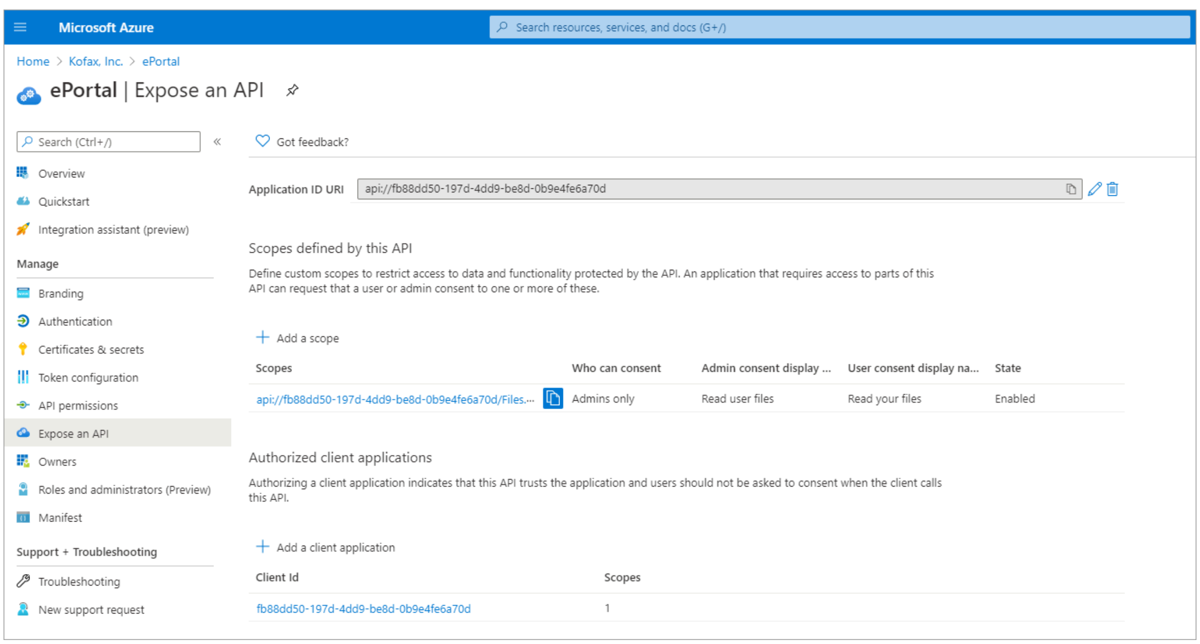
8. Note down the **Application (client) ID**.
9. On the left sidebar, click **Expose an API**.
   The **Expose an API** page appears.



10. Under **Authorized client applications**, click **Add a client application**.
    The **Add a client application** section appears on the right side of the page.



11. In the **Client ID** field, paste the copied client ID.
12. Under **Authorized scopes**, select the check box.
13. Click **Add application**.
    You can see that the required values are available on the **Expose an API** page.

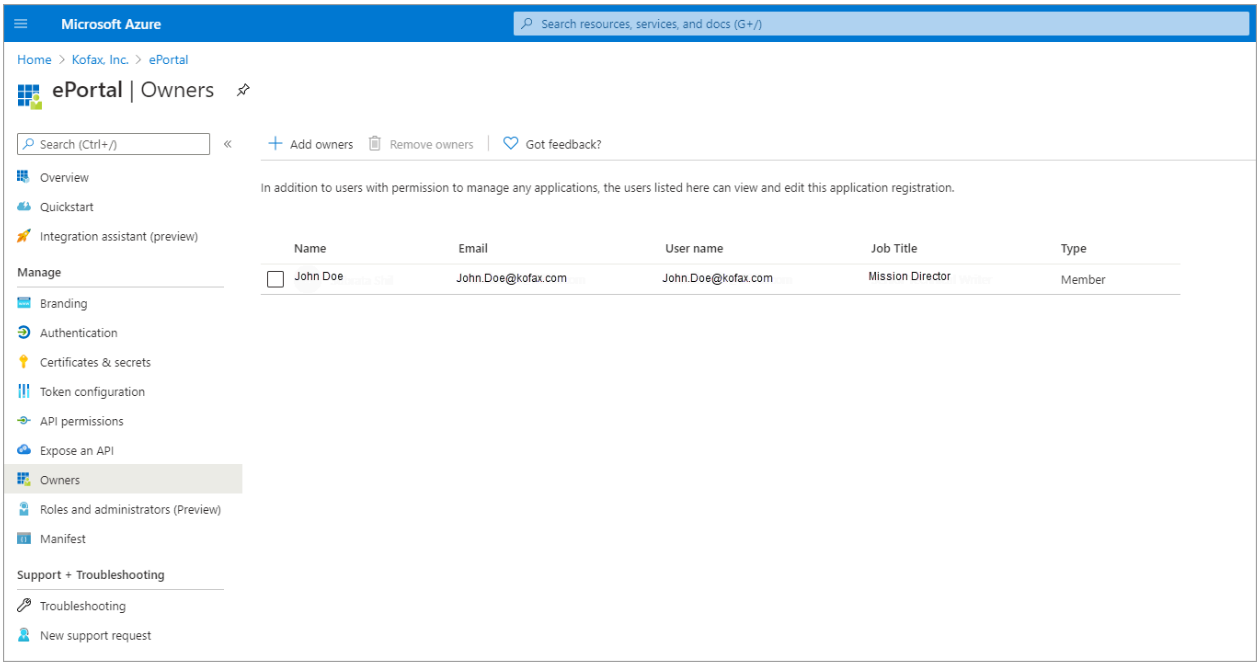


Manage owners

Use the **Owners** page to see the owners of ePortal.

On the left sidebar, under **Manage**, click **Owners**.

The **Owners** page appears.

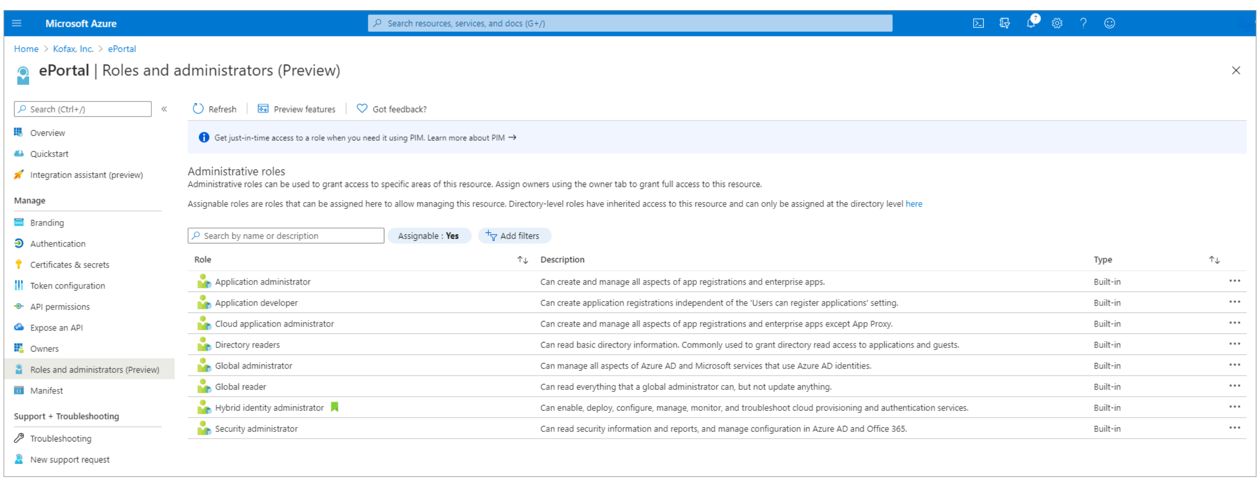


An admin can add more than one owner.

Manage roles and administrators (Preview)

Use the **Roles and administrators (Preview)** page to see the various administrative roles. On the left sidebar, under **Manage** click **Roles and administrators (Preview)**.

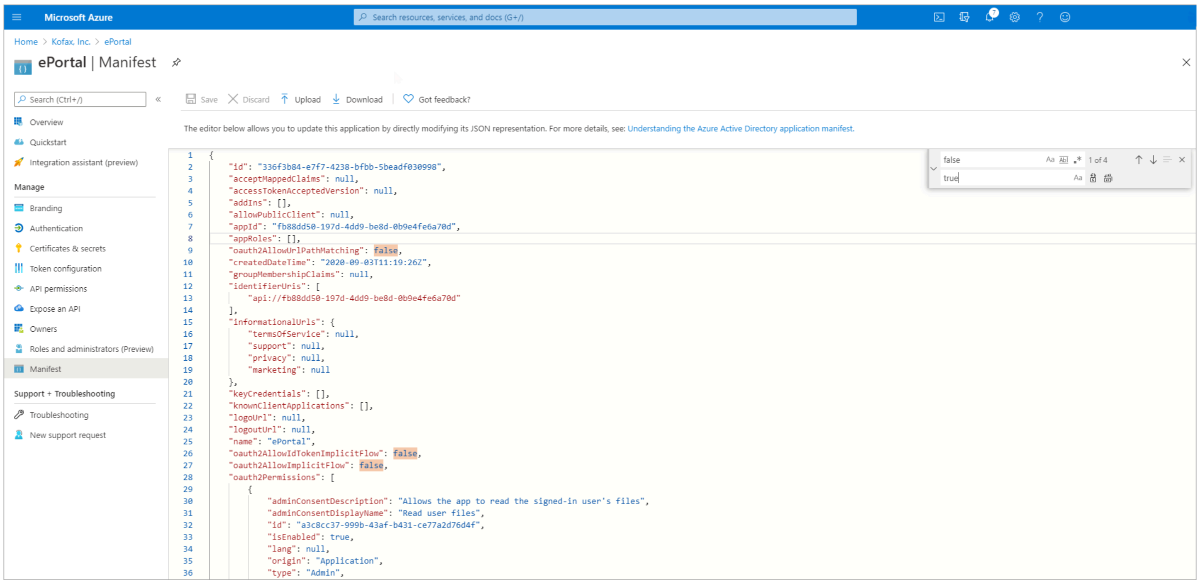
The **Roles and administrators (Preview)** page appears.



Manage manifest

Use the Manifest page to update the application by directly modifying its JSON representation.

1. On the left sidebar, under **Manage**, click **Manifest**.
   The **Manifest** page opens with an editor.

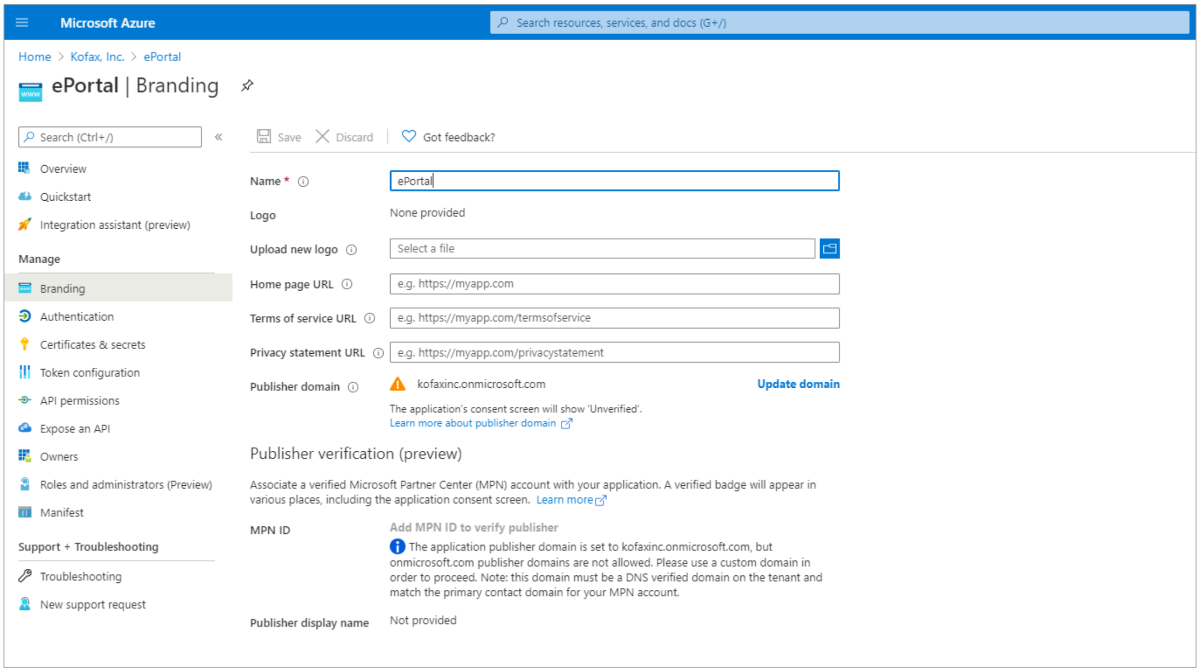


2. Replace "false" with "true" for all the occurrences and click **Save**.

Manage branding

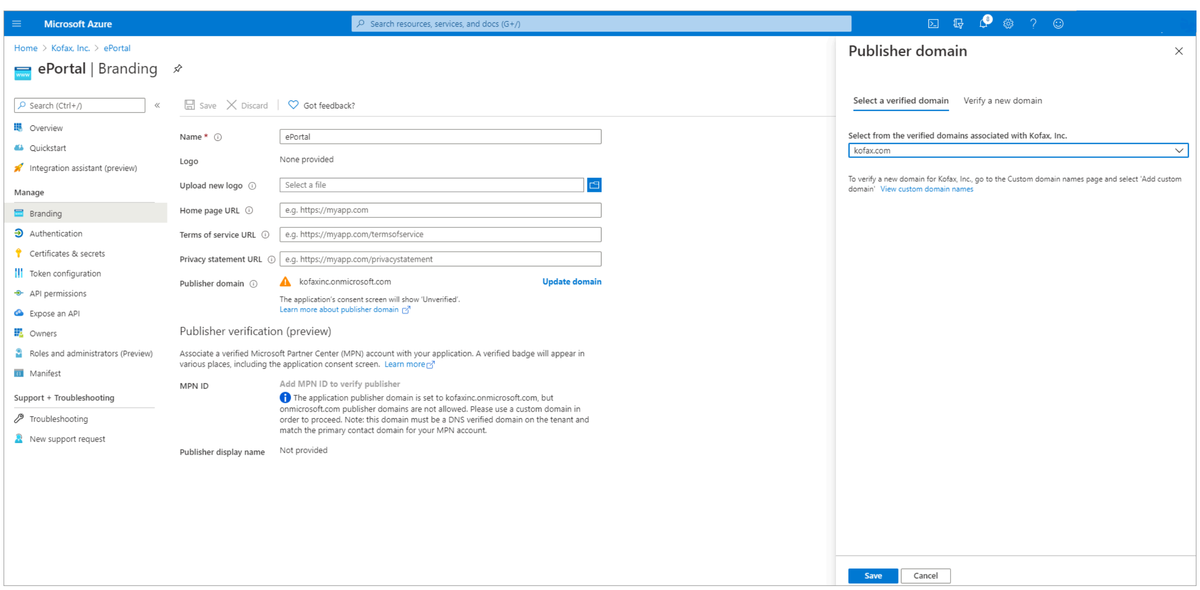
The Branding page lets you define the logo, Home page URL, Terms of service URL, and other branding details.

1. On the left sidebar, under **Manage**, click **Branding**.
   The **Branding** page appears.



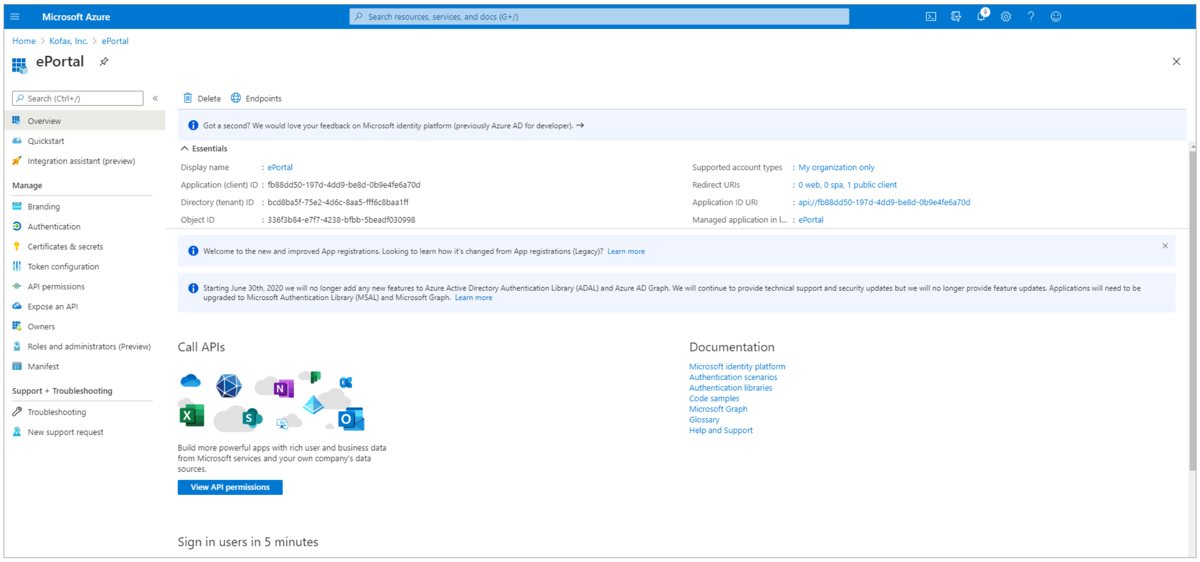
2. Optional. To upload a new logo, click and select the logo you want to upload.
3. Click **Update domain**.

   The **Publisher domain** section appears on the right side of the page.



4. On the **Select a verified domain** tab, select a domain that is associated with your organization from the list.
5. Click **Save**.
6. On the left sidebar, click **Overview**.

   The **Overview** page appears.



7. Note down the **Application (client) ID** and **Directory (tenant) ID** for future reference.

Configure EPortal.AppConfig

Configure the EPortal.AppConfig file for your email account.

1. Copy the following XML content.

```
<MailAccount Id="exchange_online_outlook" DisplayName="Oauth_outlook_mails"
 Host="https://graph.microsoft.com/" Port="0" SSL="true"
 IgnoreCertificateErrors="false" UserName="user.namexyz@kofax.com"
 Protocol="EXCHANGE_ONLINE" TenantID="bcd8ba5f-75e2-4d6c-8aa5-fff6c8baa1ff"
 ClientID="e3267ec1-edfc-4022-a3a2-a048459e5b00">
<MailEncoding>UTF-8</MailEncoding>
<DefaultCharset>UTF-8</DefaultCharset>
<Folders>
<Folder>Eportal_Input</Folder>
</Folders>
<Filter>IsRead=false</Filter>
<ExchangeVersion>Exchange2013</ExchangeVersion>
<Impersonate Enabled="false" />
</MailAccount>
```

2. Open the EPortal.AppConfig file, located at C:\ProgramData\TIS\<eFlow6>\AppData\Server\<Application_name>\Setup, and paste the copied content under <MailAccounts/> section, and then save the file.

   If messages are in sub-folder of Outlook, then folder structure will be like the following: <Folder>/Eportal_Input/<sub-folder Name>/<Folder>

3. Change UserName, TenantID, and ClientID.

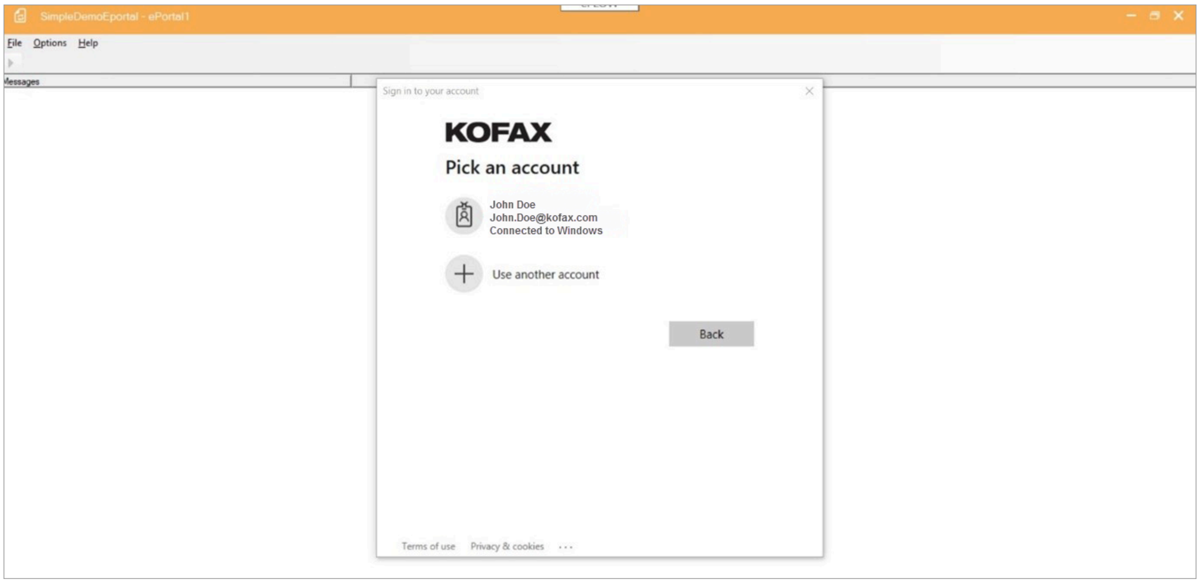
Run the ePortal manual station

Do the following to run the ePortal manual station.

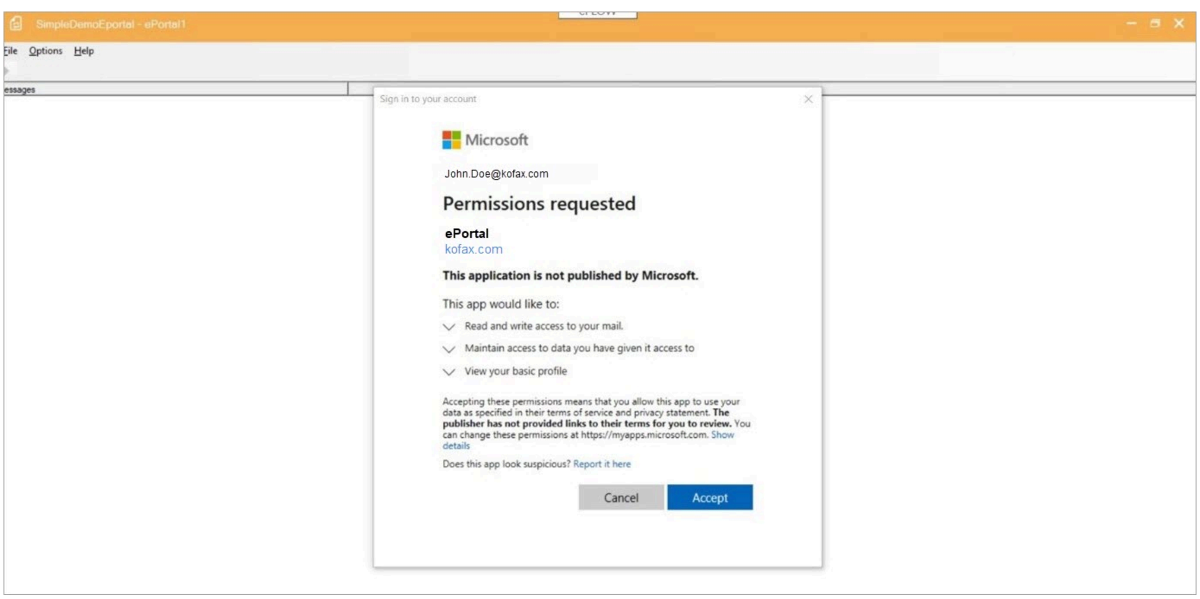
1. In the **eFlow LaunchPro**, from the **Stations** list, select **ePortal manual station**.

> If your default browser is Internet Explorer, make sure that JavaScript is enabled.

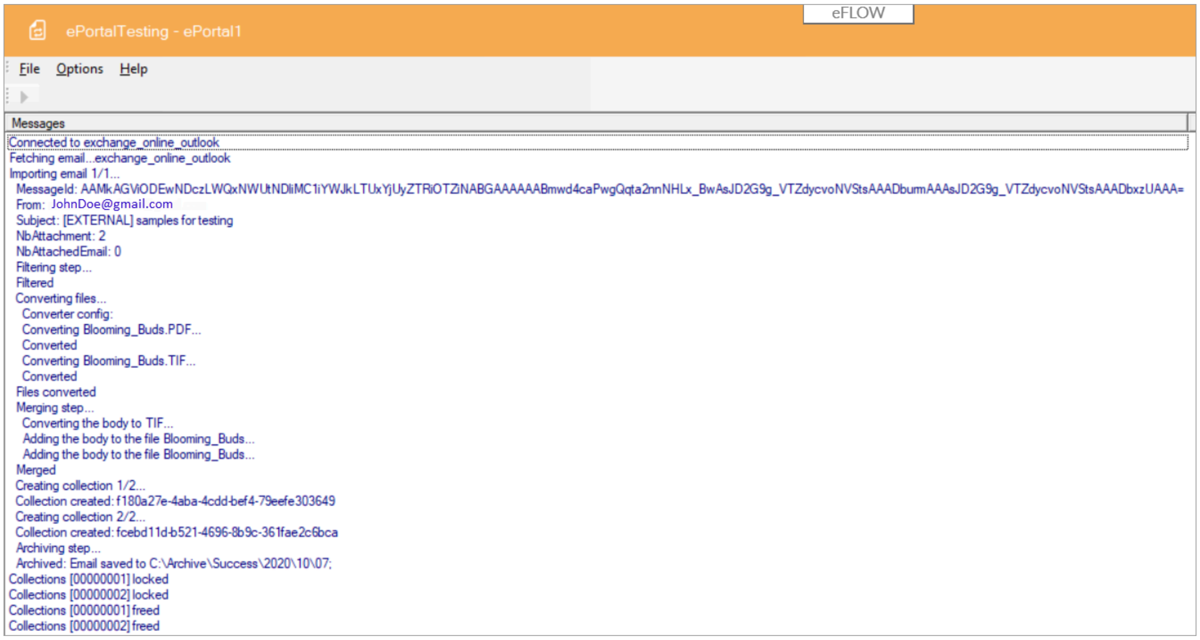
2. If the username (email id) for Outlook is not configured in the EPortal.AppConfig file for the computer using ePortal, the following page appears.



3. Select an account, and then type your password to sign in.
   After a successful sign-in, the following page appears.



4. Click **Accept**.
5. After accepting the permission, the **ePortal Manual station** starts fetching the Outlook messages from the configured folder.



File connector

The File connector retrieves files from a local file system.

In general, you should use eFlow Collect stations rather than the File connector to import files unless you need conversions that the eFlow core stations do not support.

Unsynchronized mode

Unsynchronized mode checks for available files in the import folder.

By default, when file are imported, ePortal does not delete them.

To delete or move the original files, in the `<Archives>` section, set `<DeleteOnRemote Enabled="true">` for each archive.

If you set the Move option in the Archives configuration, the files are moved to a backup folder after they are imported. This backup folder is a relative path to the import folder.

Configuration

```
<MailAccount Id="fileImport" DisplayName="FileImport" Host="C" Port="0" SSL="false"
 UserName="" Password="" Protocol="FILE">
   <Folders>
       <Folder>C:\Temp</Folder>
   </Folders>
   <Filter>*.pdf</Filter>
 </MailAccount>
```

EML connector

The EML connector imports EML files from a specific folder.

The EML files are parsed to retrieve the attachment files and create the eDoc.

The ID of the envelope is updated in the database and has the same name as the EML file.

After all emails from the batch have been parsed, the connector returns an eBatch object which can be processed by all ePortal stages.

Unsynchronized mode

Unsynchronized mode checks for available files in the import folder.

By default, after files are imported, ePortal does not delete them.

To delete or move the original files, in the `<Archives>` section, set `<DeleteOnRemote Enabled="true">` for each archive.

If you set the Move option in the Archives configuration, the files are moved to a backup folder after they are imported. This backup folder is a relative path to the import folder.

Configuration

```
<MailAccount Id="EmlImportFolder" DisplayName="EML import folder" Host="" Port="0"
 SSL="false" UserName="" Password="" Protocol="EML">
    <Folders>
      <Folder>C:\ePortal\IMPORT</Folder>
    </Folders>
    <Filter></Filter>
 </MailAccount>
```

Archive connector

The Archive connector reads EML files from the archive folder. It is used to re-process emails and recreate collections that were archived as an .eml file.

The difference between the EML connector and the Archive connector is that the Archive connector uses the EML file name to retrieve it from the ePortal database using following:

- The original user tags SourceID, Source, ImportSetId and ImportSetName
- The original collection name

Thus the name of the .eml file is the envelope ID which is used in the reporting database.

Configuration

```
<MailAccount Id="EmlImportArchive" DisplayName="Import Archive folder" Host="" Port="0"
 Ssl="false" UserName="" Password="" Protocol="EML_ARCHIVE">
```

```
    <Folders>
       <Folder>C:\ePortal\ARCHIVE\IMPORT</Folder>
    </Folders>
    <Filter></Filter>
 </MailAccount>
```

SMTP_OAUTH connector

The SMTP_OAUTH connector allows you to send acknowledgments for the imported emails after they are processed. The subject and the body of the acknowledgment mail can be configured as per your requirement. They can also be configured based on the emails processed for each Success, Reject, Error scenarios.

The eEmails are imported into the ePortal station using connecters, such as EXCHAGE_ONLINE and IMAP_GMAIL. In the ePortal station using the SMTP_OAUTH connector, for the read emails acknowledgment mails can be configured according to the statuses (Success, Reject or Error) of the collections.

SMTP_OAUTH outgoing connector can be configured in two ways in ePortal using:

- Microsoft host
- Gmail host

Microsoft host

This topic details how to register and configure an application for SMTP_OAUTH connector, and also details how to run the ePortal manual station from eFlow LaunchPro.

App registration

Any application that implements OAuth standard to authenticate and authorize its users, it needs to be registered with the corresponding Application/Web servers.

If you have already registered an application for EXCHANGE_ONLINE connector in Azure portal, then the same Client ID and Tenant ID can be used for configuring SMTP_OAUTH connector in ePortal.

If you haven't registered any applications, then follow the application registration steps mentioned in EXCHANGE_ONLINE configuration. The resulted Client ID and Tenant ID can be used for both EXCHANGE_ONLINE and SMTP_OAUTH connectors.

Configure the EPortal.AppConfig file

1. After completion of application registration, copy the following text and paste in the Eportal.AppConfig file under the `<MailAccounts/>` section.

```
<MailAccount Id="smtp_oauth_exchange" DisplayName="smtp_oauth_exchange"
 Host="https://graph.microsoft.com/" Port="0" SSL="true"
 IgnoreCertificateErrors="false" UserName="abc.xyz@kofax.com"
 Protocol="SMTP_OAUTH" TenantID="bcd8ba5f-75e2-4d6c-8cc5-fff6c8baa1ff"
 ClientID="e3267ec1-edfc-3423-a3a2-a048459e5b00">
               <MailEncoding>UTF-8</MailEncoding>
              <DefaultCharset>UTF-8</DefaultCharset>
              <Impersonate Enabled="false" />
```

```
                        </MailAccount>
```

2. Change the ID, DisplayName, UserName, TenantID, and ClientID as needed by your application.
3. Copy and paste the below code under `ActiveAccounts` section:

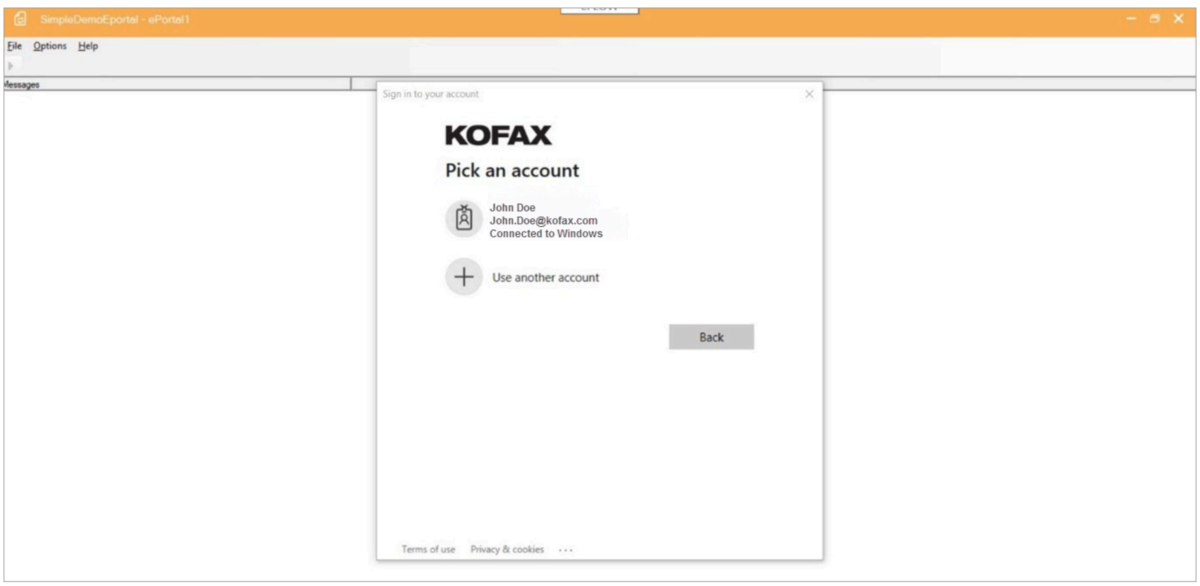
```
<ActiveAccount Id=" smtp_oauth_exchange " Enabled="true" />
```

Run the ePortal manual station

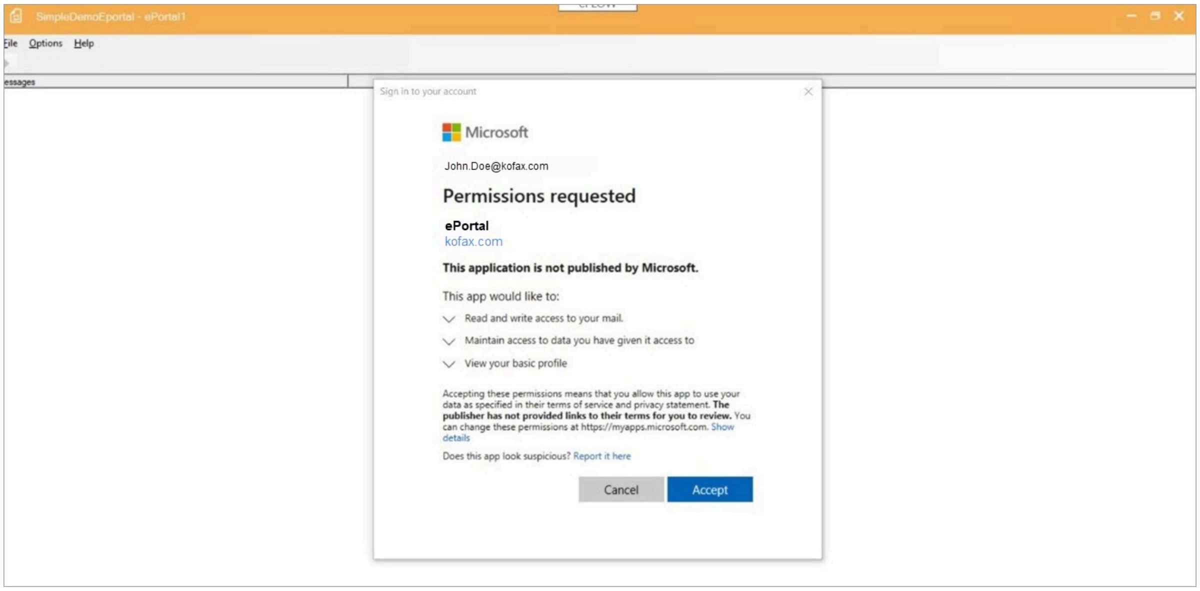
1. In the **eFlow LaunchPro**, from the **Stations** list, select **ePortal manual station**.

> If your default browser is Internet Explorer, make sure that JavaScript is enabled.

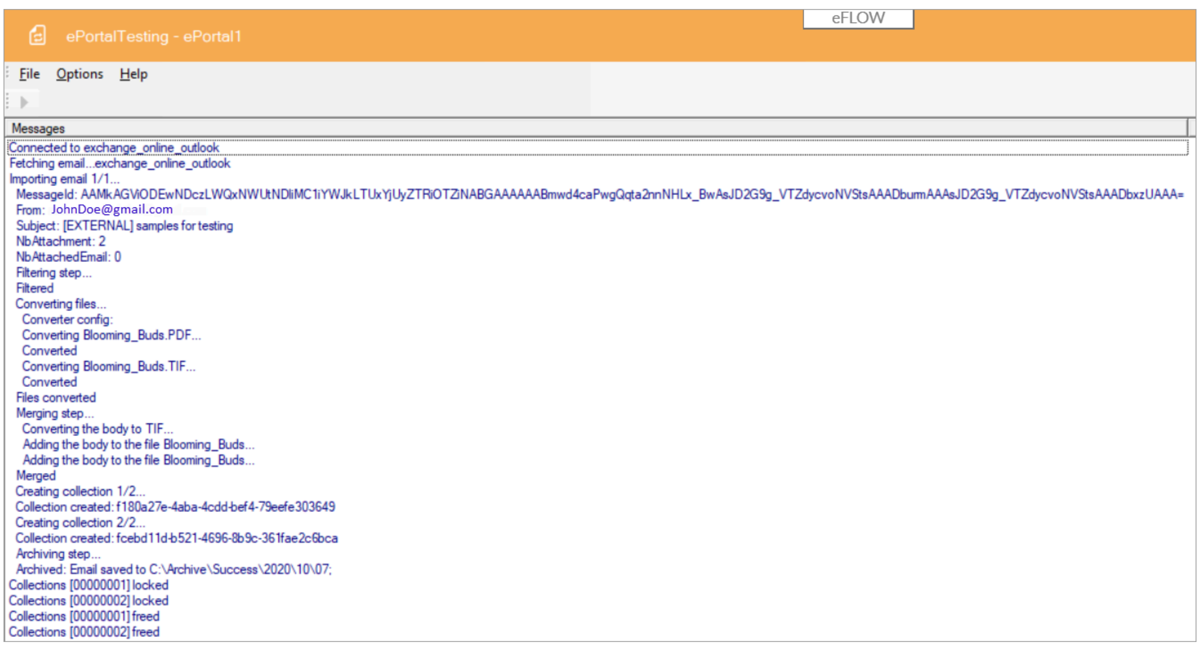
1. If the username (email id) for Outlook is not configured in the EPortal.AppConfig file for the computer using ePortal, the following page appears.



2. Select an account, and then type your password to sign in.
   After a successful sign-in, the following page appears.



3. Click **Accept**.
4. After accepting the permission, the **ePortal Manual station** starts fetching the Outlook messages from the configured folder.



Gmail host

This topic details how to register and configure an application for SMTP_OAUTH connector, and also details how to run the ePortal manual station from eFlow LaunchPro.

Application registration

Any application that implements OAuth standard to authenticate and authorize its users, it needs to be registered with the corresponding Application/Web servers.

If you have already registered an application for IMAP_GMAIL connector in Google cloud, then same Client ID and ClientSecret ID can be used for configuring SMTP_OAUTH connector in ePortal.

If you haven't registered any application in Google cloud for IMAP_GMAIL connector, then follow the application registration steps mentioned in IMAP_GMAIL connector configuration. The resulted Client ID and ClientSecret ID can be used for both IMAP_GMAIL and SMTP_OAUTH connectors.

Configure the EPortal.AppConfig file

1. After completion of application registration, copy the following text and paste in the EPortal.AppConfig file under the `<MailAccounts/>` section.

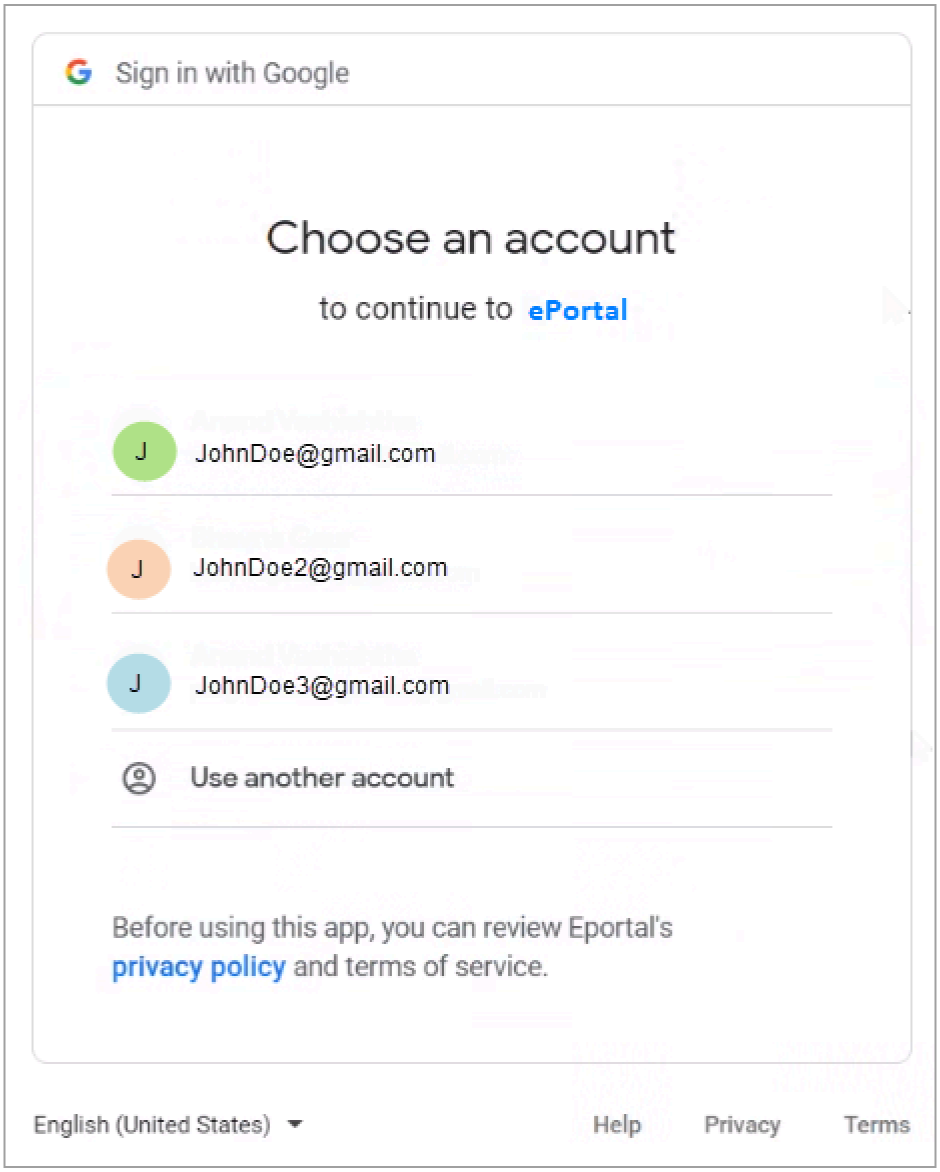
   ```
   <MailAccount Id="smtp_oauth_gmail" DisplayName="smtp_oauth_gmail"
       Host="https://mail.google.com/" Port="0" SSL="true"
    IgnoreCertificateErrors="false" UserName="abcXYZ@gmail.com" Protocol="SMTP_OAUTH"
    ClientID="892052231411-33cjawertui8f0oimb67jn67raffn5hl.apps.googleusercontent.com"
    ClientSecretID="MiVbIAJpwedxxpUjFkxIF8ven">
             <MailEncoding>UTF-8</MailEncoding>
             <DefaultCharset>UTF-8</DefaultCharset>
             <Impersonate Enabled="false" />
           </MailAccount>
   ```

2. Change the ID, DisplayName, UserName, ClientID, and ClientISecretID as needed by your application.
3. Copy and paste the following text under `ActiveAccounts` section.

   ```
   <ActiveAccount Id="smtp_oauth_gmail" Enabled="true" />
   ```

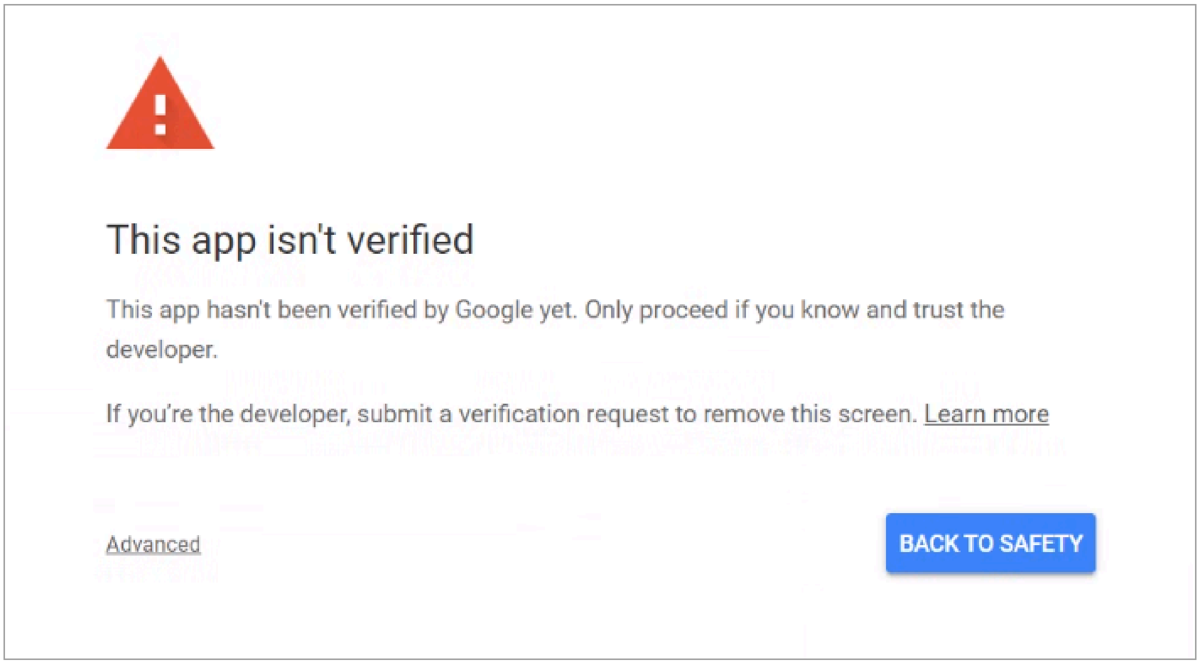
Run the ePortal manual station

1. In the **eFlow LaunchPro**, on the **Stations** list, select **ePortal manual station**.
   If opened for the first time the following page appears.

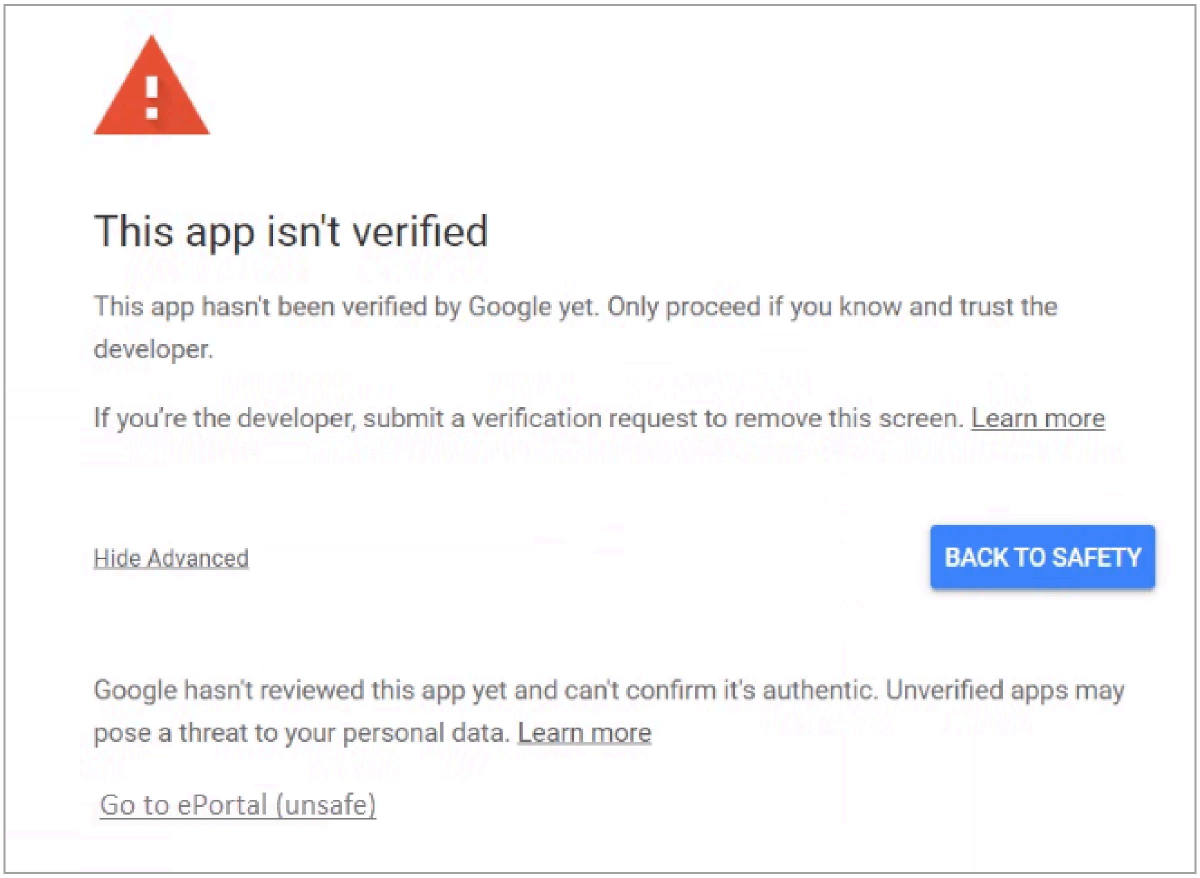


2. Select the Gmail account that you provided as the contact email address. The following page appears.

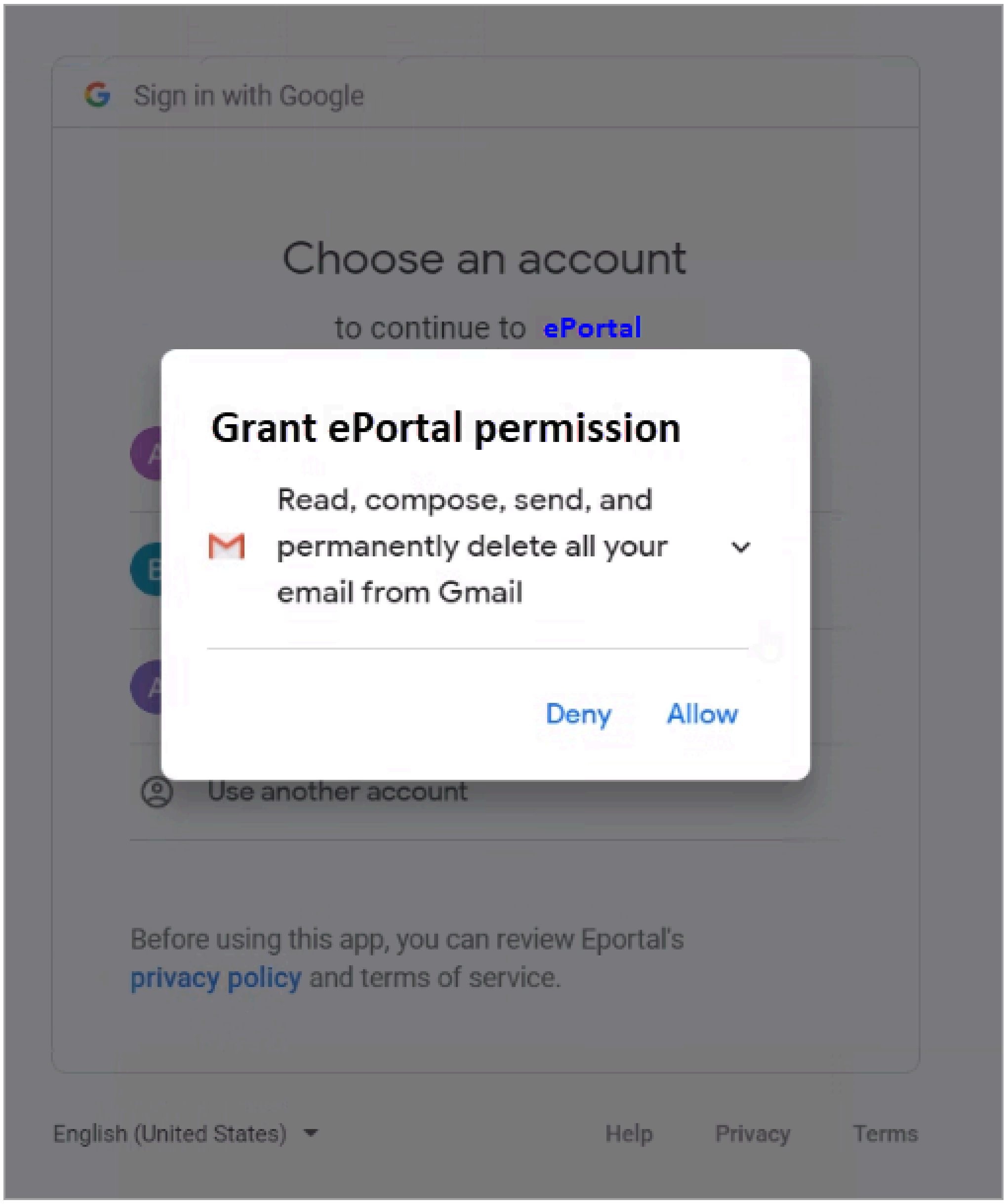
> If your Gmail account is not signed in from the computer where you are using the ePortal, then you need to sign in using your Gmail username and password.



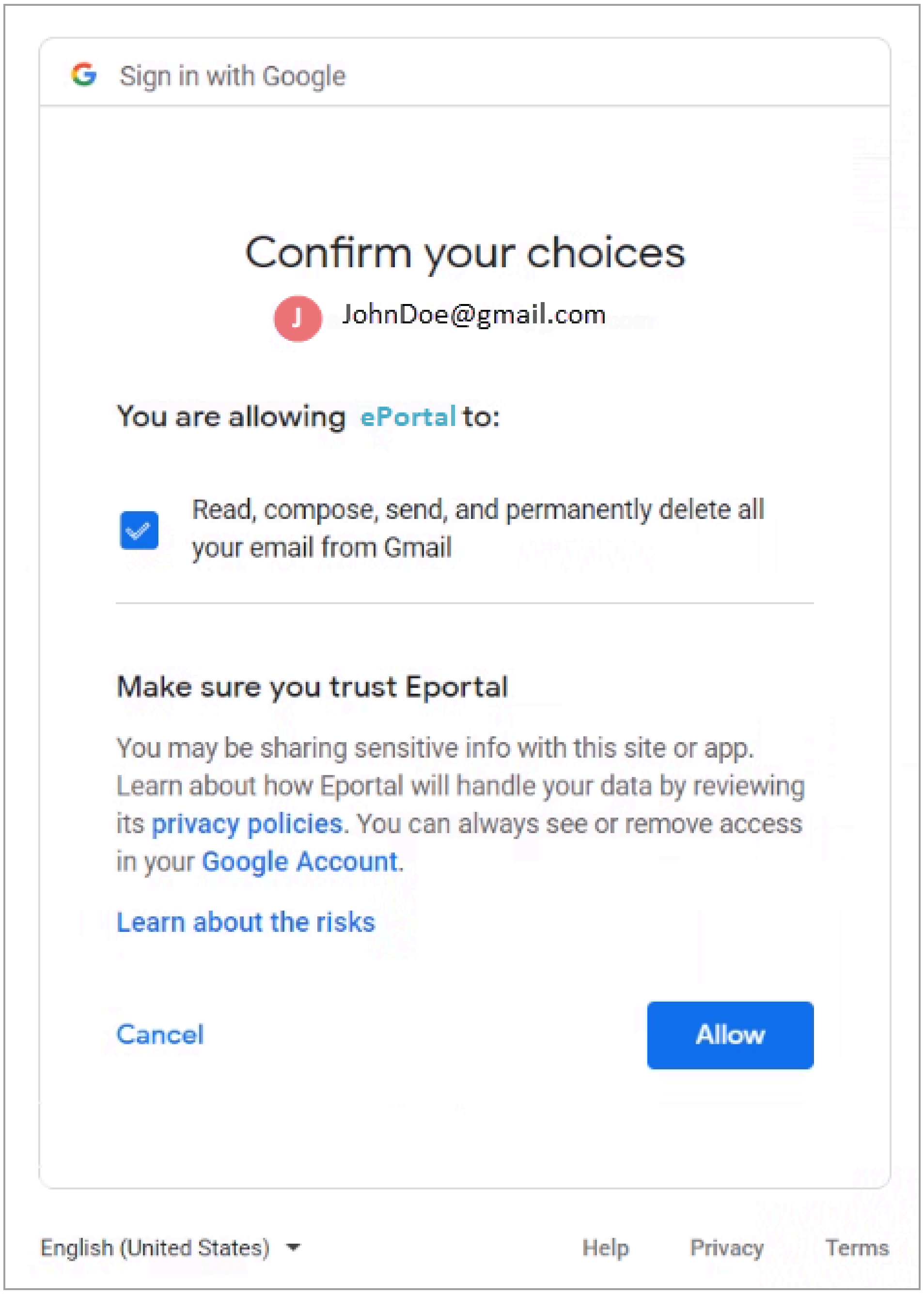
3. Click **Advanced**.
   The following page appears.



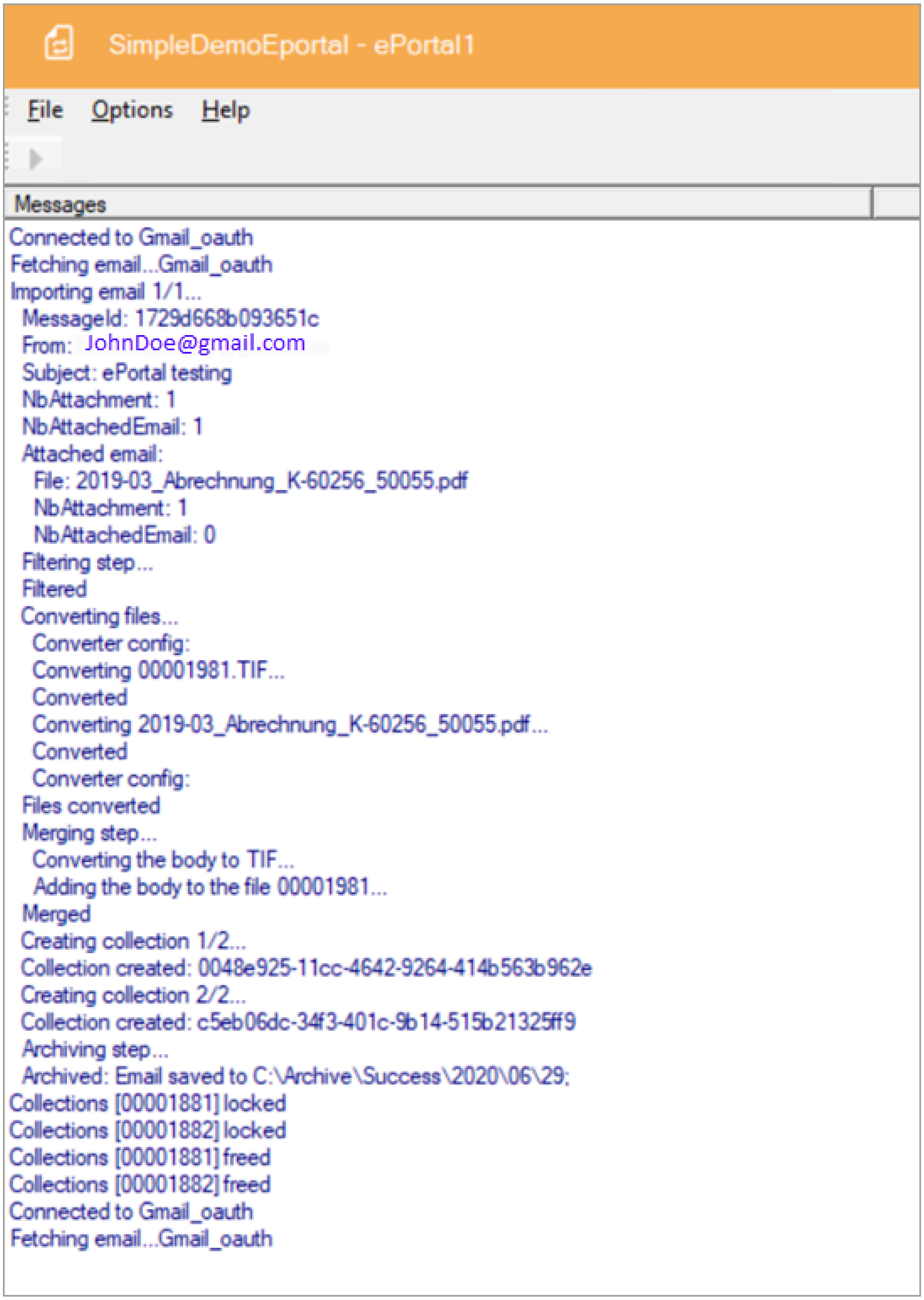
4. Click **Go to ePortal (unsafe)**.
   The **Grant ePortal permission** Web dialog appears.



5. Click **Allow**. The **Confirm your choices** page appears.



6. Click **Allow**.
7. After accepting the permission, the **ePortal Manual station** starts fetching the Gmail messages from the configured folder.


SimpleDemoEportal - ePortal1
File
Options
Help
Messages
Connected to Gmail_oauth
Fetching email...Gmail_oauth
Importing email 1/1...
MessageId: 1729d668b093651c
From: JohnDoe@gmail.com
Subject: ePortal testing
NbAttachment: 1
NbAttachedEmail: 1
Attached email:
File: 2019-03_Abrechnung_K-60256_50055.pdf
NbAttachment: 1
NbAttachedEmail: 0
Filtering step...
Filtered
Converting files...
Converter config:
Converting 00001981.TIF...
Converted
Converting 2019-03_Abrechnung_K-60256_50055.pdf...
Converted
Converter config:
Files converted
Merging step...
Converting the body to TIF...
Adding the body to the file 00001981...
Merged
Creating collection 1/2...
Collection created: 0048e925-11cc-4642-9264-414b563b962e
Creating collection 2/2...
Collection created: c5eb06dc-34f3-401c-9b14-515b21325ff9
Archiving step...
Archived: Email saved to C:\Archive\Success\2020\06\29;
Collections [00001881] locked
Collections [00001882] locked
Collections [00001881] freed
Collections [00001882] freed
Connected to Gmail_oauth
Fetching email...Gmail_oauth

Chapter 4

Filtering

The ePortal filters are used to classify the eDoc of the envelope and link the AttachedDocs (DocAttachment), AttachedFiles (FileAttachment) to their main AcceptedDoc.

The eDoc is classified as mentioned in the following table.

Type	Description
AcceptedDoc	The AcceptedDoc is the main file that is processed by eFlow, such as an invoice.
AttachedDoc (DocAttachment)	A file to be merged with the main document.
AttachedFile (FileAttachment)	A file to be attached to the collection so that it can be exported by an export station, or used in another station. For example, XML file.
RejectedFile	A file to be removed as an unwanted attachment. Files can be rejected depending on their size, name or extension.

eDocs are filtered according to the following:

- A regular expression on the full name (name + extension)
- Size in bytes

Filtering eDocs

The ePortal filters the eDocs in the following order:

1. The ePortal filter identifies whether the eDoc is accepted.
2. If the eDoc is not accepted, the filter tries to identify if it is a DocAttachment.
3. If the file is not identified as a DocAttachment, the filter tries to identify it as FileAttachment.
4. If the eDoc cannot be classified, it is rejected.

AcceptedDoc

The AcceptedDoc is the main file that is processed by eFlow, such as an invoice.

```
     <Accepted Description="List of files that will be imported">
        <RegularExpression Enabled="true" Value="^(?{invoiceGUID}((?!_ATTACH).)*)\.
(tif|tiff|pdf)$"/>
        <MinSize Enabled="false" Value="" />
        <MaxSize Enabled="false" Value=""/>
```

```
      </Accepted>
```

AttachedDoc

The AttachedDoc or DocAttachment is the image that is merged with the accepted eDoc as an eFlow page attachment.

```
<DocAttachment description="List of files that will be attached to the collection as
 is">
        <RegularExpression Enabled="true" Value="(?{invoiceGUID}.*)_ATTACH.*\.(tif|
tiff|pdf)$"/>
        <MinSize Enabled="false" Value=""/>
        <MaxSize Enabled="false" Value=""/>
      </DocAttachment>
```

AttachedFile

The AttachedFile or FileAttachment is the file that is attached to the eFlow collection as an eFlow file attachment. The file is not merged with the collection. For example, you can save an XML file so that it can be exported by an export station or used in another station.

```
<FileAttachment Description="List of files that will be attached to the collection as
 is">
        <RegularExpression Enabled="true" Value="(^\.(png))$"/>
        <MinSize Enabled="false" Value=""/>
        <MaxSize Enabled="false" Value=""/>
      </FileAttachment>
```

RejectedFile

Rejected files are deleted. Typically, these are the images with signatures (PNG files).

Linking AcceptedDoc

The AcceptedDoc and AttachedDoc or AttachedFile must have a common name, which can be defined using the group name of the regular expression.

To make this more readable in the configuration file, replace '<' and '>' with '{' and '}'.

For example, Invoice1.PDF, Invoice1_ATTACH.PDF and Invoice2_ATTACH.PDF can be linked together with the following regular expression:

AcceptedDoc: ^(?{invoiceGUID}((?!_ATTACH).)*)\.(tif|tiff|p)$

AttachedDoc: (?{invoiceGUID}.*) _ATTACH.*\.(tif|tiff|pdf)$

There can be more than one group name. ePortal checks every group name and if both regular expressions have the group name, they are compared.

Chapter 5

Conversion

As electronic document providers or email servers can import a wide variety of document types into the system, conversion to files and formats that eFlow can process is a critical step in the ePortal process.

There are many third-party tools and libraries that allow you to convert from one document type to another. ePortal also has its own internal converter to perform such tasks.

To provide more flexibility, the integration of converters into ePortal is done through a plug-ins model.

Available converters

The following converters are available:

- ePortal internal (default)
- Aspose: TIF, TIFF, JPG, JPEG, BMP, GIF, PNG, PDF, DOC, DOCX, DOCM, DOT, DOTX, HTML, HTM, XHTML, MHT, MHTML, ODT, RTF, TXT, XML, XLS, XLTX, XLSX, XLTM, XLSM, ODS, CSV, PPS, PPT, POT, ODP, PPSX, POTX, and PPTX File.
- Winnovative: MHTML, HTM, and MHT.
- PRD – PDFtools: Searchable PDF

If no converter is defined for a specific file type, the envelope is rejected.

Configuration

When multiple converters are enabled, ePortal first checks for a suitable converter for the specific file. If two converters can convert the same file extension, the first one in the list is chosen.

```
<Conversion Description="Use to convert pdf, jpg, tif images to tif CCITT4 with the
 appropriate resolution">
      <ConverterPlugins Description="List of available dlls that can convert images">
       <ConverterPlugin Name="BasicConverter" Enabled="true"
 AssemblyName="TiS.Import.ePortal.Converter.Basic, Version=0.0.3.0, Culture=neutral" />
        <ConverterPlugin Name="NeeviaConverter" Enabled="false"
 AssemblyName="TiS.Import.ePortal.Converter.Neevia, Version=0.0.3.0, Culture=neutral" /
>
        <ConverterPlugin Name="AsposeConverter" Enabled="false"
 AssemblyName="TiS.Import.ePortal.Converter.Aspose, Version=0.0.3.0, Culture=neutral" /
>
```

```
       <ConverterPlugin Name="PRDConverter" Enabled="false"
AssemblyName="TiS.Import.ePortal.Converter.PRD, Version=0.0.3.0, Culture=neutral" />
     </ConverterPlugins>
     <Resolution>300</Resolution>
     <BinarizeThreshold>128</BinarizeThreshold>
     <GenerateJPG>false</GenerateJPG>
   </Conversion>
```

Chapter 6

Collection creation

Collection creation controls how emails are imported into eFlow from ePortal.

The following options are possible:

- One collection per attachment.
- One collection per email (all attachments are merged to create a single TIF file).
- Adding the email body at the beginning or at the end of the collection.
- Setting some pages as eFlow attachments so that they are not processed by the OCR engines.
- Attaching the original email attachments to the collection so that they can be exported.

When two eDocs are merged, it is possible that one is imported, and the other is rejected.

The output of the collection creation is an eFlow collection per eDoc:

1. An eFlow collection is created for every eDoc of every envelope of the eBatch created by the connector, provided the eDoc was not rejected due to merging or filtering.
2. The UserTags of the collection are updated from the following configuration elements:
   - The eBatch: SourceID, for example AccountID of the mailAccount, such as GmailAccount1.
   - The envelope: remoteID or Email_From.
   - The eDoc: FileName.
3. The UserTag used for routing is updated, such as PRD_Created.
4. The email body or the images can be set as a page attachment.
5. All files specified in the Filtering stage are attached.

The original file is attached to the collection as a collection attachment.

Configuration

```
    <CollectionCreation Description="Use to merge images before to be imported"/>
      <Email>
        <MergeImages Enabled="false" description="merge all images of the email"/>
        <MergeBody Enabled="true" Description="merge the body with the image"/>
          <BodyFirst Enabled="false" Description="if false the body will be the last
image"/>
          <PageAttachment Description="set page as eFlow attachment"/>
            <Body Enabled="true"/>
            <Images Enabled="false"/>
          </PageAttachment>
```

```
        <TextFilter Enabled="false" Value=""/>
        <TxtConverter Enabled="true" Description="2 solutions: HTML with XSLT or TXT
(quicker)">
          <From Caption="From:" />
          <To Caption="To:"/>
          <Subject Caption="Subject:"/>
          <Date Caption="Sent:" FormatString="MMMM dd, yyyy"/>
        </TxtConverter>
      </MergeBody>
    </Email>
    <FileAttachment Description="Attached the original file to the collection"/>
      <OriginalFiles Enabled="false"/>
    </FileAttachment>
  </CollectionCreation>
```

Chapter 7

Acknowledgment

The Acknowledgment feature enables you to send emails to the senders to inform them that their files have been processed. The acknowledgment email is sent after the imported email is archived.

- **SUCCESS**: When the collection is created in eFlow.
- **REJECTED**: When an envelope is rejected. For example, if the envelope is empty and does not contain any eDoc.

  An envelope may be empty in the following situations:
  - The email has no attachments.
  - The files in the envelope do not adhere to the regular expression of the filter or are too large or too small.
  - The files in the envelope cannot be converted to TIF.
- **ERROR**: When an error occurs during processing.

Each archive has its own configuration and can behave differently. Some of the settings are:

- Archive path
- Forward the envelope to another mail account
- Send an acknowledgment
- Delete the remote file
- Move the remote file

Configuration

1. Set up an SMTP account.

```
<MailAccount Id="smtp_oauth_exchange" DisplayName="smtp_oauth_exchange"
 Host="https://graph.microsoft.com/" Port="0" SSL="true"
 IgnoreCertificateErrors="false" UserName="abc.xyz@kofax.com"
 Protocol="SMTP_OAUTH" TenantID="bcd8ba5f-75e2-4d6c-8cc5-fff6c8baa1ff"
 ClientID="e3267ec1-edfc-3423-a3a2-a048459e5b00">
              <MailEncoding>UTF-8</MailEncoding>
             <DefaultCharset>UTF-8</DefaultCharset>
             <Impersonate Enabled="false" />
               </MailAccount>
```

2. Enable `<Acknowledgement>` in the `<Stations>` section:

```
<Acknowledgement Enabled="true" />
```

You can exclude specific stations from sending acknowledgement emails to the sender.

```
<Station Name="Default">
 <QueryWF Enabled="false" />
 <MaxWorkUnit Value="10" />
```

```
 <Acknowledgement Enabled="false" />
 <UpdatePriority Enabled="true" />
 <ActiveAccounts>
   <ActiveAccount Id="Gmail_oauth" Enabled="true" />
   <ActiveAccount Id="smtp_oauth_exchange" Enabled="true" />
 </ActiveAccounts>
</Station>
```

3. Enable `<Acknowledgement>` in the `<Archives>` section:

```
<Acknowledgement Enabled="true" Description="Send an Email to the sender of the
 rejected email ">
     <Subject>Rejected doc: {SUBJECT:30}</Subject>
     <Body>The electronic document you submitted: "{SUBJECT}" was rejected.
 \nIt can be tracked down in our system under the reference number:\n
 {GUID}\n\nYou may contact the system administrator for more details at:\n
 Support_eportal@bigcorp.com </Body>
     <BodyHtml Enabled="false"  FileName="%EPORTAL%\
Template\Reject_Acknowledgment.html" Description=""/>
     <From>
       <MailBox Address="reject@eportal.com" />
     </From>
  </Acknowledgement>
```

Acknowledgement templates

You can use HTML templates for the acknowledgment emails. The default templates are available in the following folder.

`C:\Program Files (x86)\TIS\Kofax eFlow ePortal\Runtime\Template`

- If `<BodyHtml Enabled="false">`, ePortal uses the text from the parameter <Body> to create the body text of the email.
- If `<BodyHtml Enabled="true">`, ePortal uses an HTML template to create the body.

You can add variables to the email message. The variables are available in the AvailableTags.html file at the following location:

`C:\Program Files (x86)\TIS\Kofax eFlow ePortal\Runtime\Template`

`%EPORTAL%` is replaced with the content of the environment variable created with the MSI.

Acknowledgment of email attachments

The acknowledgment mail can inform the sender which files were accepted, and which were rejected. You can integrate this in the acknowledgment email as a simple HTML list:

```
<ul> <li>File 1 - collectionName1</li> <li>File 2 - collectionName2</li></ul>
```

You can include the eDoc properties {FileName} {CollectionName} {State} {Note} as well as custom eDoc properties.

To add a variable to the template, use the following syntax:

```
{Envelop_variable:"Text with eDoc variable"}
```

For example:

```
{IMPORTSET:"{FileName} {CollectionName}"}
{IMPORTSET:"{FileName}"}
{IMPORTSET:"the collection {CollectionName} was created with the email attachment
 {FileName}"}
```

Example of email sent:

List of attachments* DOC1.tif 00001427_1_EU00000502

List of rejected attachments* template.xlsx: The image must be TIF, PDF or JPG.

To list	Use variable
Imported files	{IMPORT_SET}
Rejected files	{REJECT_SET}
Merged files	{ATTACHED_DOC_SET}
Collection attachments	{ATTACHED_FILE_SET}