

Kofax eFlow ePortal

Overview Guide

Version: 2.0.1

Date: 2020-10-22

The logo for KOFAX, consisting of the word "KOFAX" in a bold, blue, sans-serif font.

© 2005–2020 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Table of Contents

Preface.....	6
Chapter 1: About Kofax eFlow ePortal.....	7
ePortal process.....	7
ePortal terms.....	8
Connection.....	9
Filtering.....	10
Conversion.....	10
Collection creation.....	10
Archiving.....	11
Chapter 2: Installation.....	12
System requirements.....	12
Installation procedure.....	12
Upgrade instructions.....	15
Chapter 3: Configuration.....	16
Configuration file.....	16
Connection string.....	16
Features.....	16
Stations.....	17
Station properties.....	17
Sections.....	18
Section properties.....	18
Backward compatibility of configuration files.....	18
Chapter 4: Connectors.....	19
POP3 connector.....	19
Unsynchronized mode.....	19
Synchronized mode.....	19
Configuration.....	19
POP3_OAUTH connector.....	19
Unsynchronized mode.....	20
Synchronized mode.....	20
Autorun mode.....	20
Configuration.....	20
IMAP connector.....	66
Unsynchronized mode.....	66

Synchronized mode.....	66
Encoding.....	66
IMAP Folder.....	66
Filter.....	66
Configuration.....	67
IMAP_GMAIL connector.....	67
Unsynchronized mode.....	67
Synchronized mode.....	67
Autorun mode.....	67
Configuration.....	68
EWS connector.....	90
About EWS.....	90
Unsynchronized mode.....	90
Synchronized mode.....	90
Exchange server version.....	90
Connect without credentials.....	90
Impersonation.....	91
Configuration.....	91
EXCHANGE_ONLINE connector.....	91
Unsynchronized mode.....	91
Synchronized mode.....	91
Autorun mode.....	91
Configuration.....	92
File connector.....	115
Unsynchronized mode.....	115
Configuration.....	115
EML connector.....	116
Unsynchronized mode.....	116
Configuration.....	116
Archive connector.....	116
Configuration.....	117
Chapter 5: Filtering.....	118
Filtering process.....	118
AcceptedDoc.....	118
AttachedDoc or DocAttachment.....	119
AttachedFile or FileAttachment.....	119
RejectedFile.....	119
Linking AcceptedDoc.....	119

Chapter 6: Conversion.....	120
Available converters.....	120
Configuration.....	120
Chapter 7: Collection creation.....	121
Configuration.....	121
Chapter 8: Acknowledgement.....	122
Configuration.....	122
Acknowledgement templates.....	123
Acknowledgement of email attachments.....	123

Preface

The Kofax eFlow ePortal Overview Guide describes about ePortal station. Kofax eFlow ePortal is an Add-on to Kofax eFlow platform. Once configured, the ePortal station can automatically import electronic data and emails into eFlow. The ePortal station reads the emails from the configured email account and creates collections for eFlow. The collections are imported into the eFlow and then further processed by eFlow.

Chapter 1

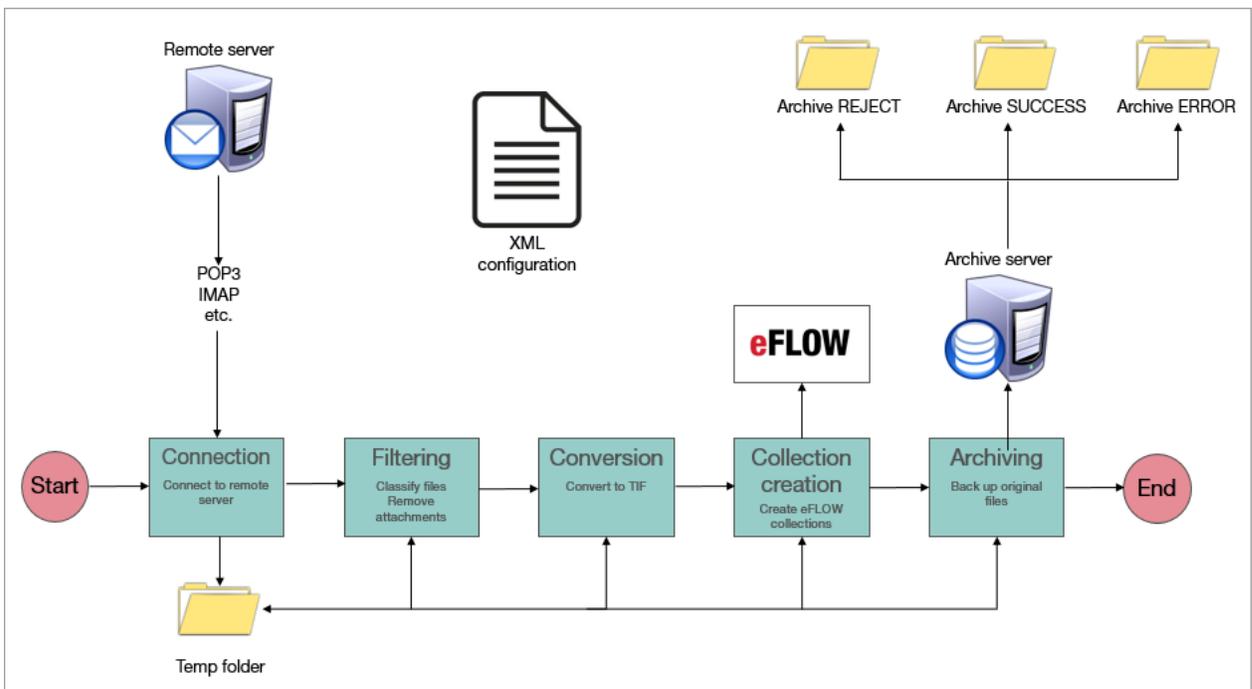
About Kofax eFlow ePortal

The purpose of the ePortal station is to import electronic documents, emails, into eFlow.

ePortal process

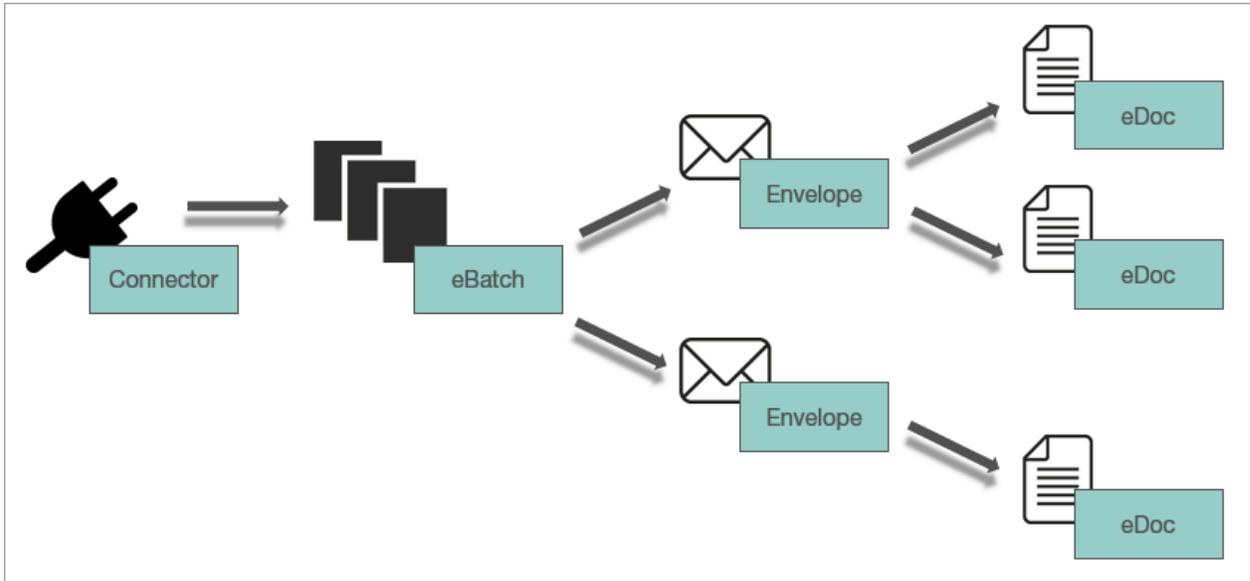
The process of importing documents into eFlow with ePortal comprises actions to extract, filter, convert, organize, and archive the data.

The following figure illustrates the ePortal processing stages. Each of these stages can be controlled using the ePortal configuration file.



Each of these stages processes an envelope object created by an ePortal connector.

ePortal terms



Term	Explanation
Connector	ePortal connectors retrieve documents from remote servers.
eDoc	<p>An eDoc (electronic document) is any kind of document that is available on the remote server. For example:</p> <ul style="list-style-type: none"> • An email • An email attachment • A TIF, PDF, XML, or other type of file
Envelope	<p>A simple envelope contains at least one eDoc as well as meta data.</p> <ul style="list-style-type: none"> • Reporting data • Global status: The envelope status • Detailed status: The eDoc status • Temp folder architecture <p>Typically, an email is an envelope: it contains none, one or several documents.</p> <p>There can be two files on the remote server with the same name, such as a TIF and an XML file. Complex files, such as ZIP or EML are parsed before they are imported.</p> <p>Using an envelope object enables every ePortal stage to process any combination of documents, such as TIF; email; TIF + XML; TIF + JPG + PRD + XML; and so on.</p> <p>The envelope meta data 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.</p>
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 configuration file.

Term	Explanation
Mail Account	<p>A Mail Account allows the ePortal connector to connect to a remote server.</p> <p>The following properties are used:</p> <ul style="list-style-type: none"> • ID • Description • Username • Password (If basic authentication is applicable for the connector) • Client ID (If OAuth is applicable for the connector) • Tenant ID (If OAuth is applicable for the connector) • Client secret ID (If OAuth is applicable for the connector) <p>Several accounts can be added to the <MailAccounts> section of the configuration file, but an ePortal connector can only use the account that is linked to the station by its ID and is enabled.</p>
eDoc provider	A remote server on which electronic documents reside.
Mailbox	An electronic document source from which ePortal retrieves files.

Connection

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. Check in the configuration file how many 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. An 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 connector
- POP3_OAUTH connector
- IMAP connector
- IMAP_GMAIL connector
- EWSi connector
- EWSO connector
- EXCHANGE_ONLINE connector
- File connector
- EML connector
- EML_ARCHIVE connector
- FTP connector

- SMTP connector
- MSG connector

Filtering

The ePortal filtering has the following purposes:

- Classify the eDoc of the envelope as:

Type	Description
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, an XML file.
RejectedFile	A file to be removed as an unwanted attachment. Files can be rejected depending on their size, name or extension.

- Link AttachedDocs and AttachedFiles with their main AcceptedDoc.

Conversion

Converters are used for the following purposes:

- Convert the following file types to TIF CCITT4: 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, PPTX
- Create JPGs from colour images.
- Create PRD files from searchable PDFs.

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

Collection creation

In the collection creation stage, first prepares all eDocs of the envelope for import as a collection into eFlow. You can configure the following options for importing the eDoc of an envelope.

- Create one collection per attachment.
- Create one collection for all attachments by merging the attachments with the main document.
- For emails only, add the email body at the beginning or the end of the collection or remove it.

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

The output of the collection creation step 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:
 - The eBatch, such as SourceID (AccountID: ID of the mailAccount, such as GmailAccount1, FilePortal1, ScanPortal1) and Source (SourceType: FilePortal, ScanPortal, IMAP, POP3, FTP, ARCH, EML, and so on).
 - The envelope, such as remoteID or Email_From.
 - The eDoc, such as 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.
6. The original file is attached to the collection as a collection attachment.

Archiving

There are three types of archives:

- **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 eDoc to be imported.

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 occurred during processing.

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

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

Chapter 2

Installation

This topic explains how to install ePortal 2.0.1.

System requirements

ePortal 2.0.1 requires the following:

- eFlow 5.2.1 or higher
- A Microsoft SQL database
- .NET 4.7.2 or higher
- Per ePortal instance an eInvoicePortalPDF license. Refer to the "Manage licenses" section, in the *Kofax eFlow Administrative User Guide* for information on installing licenses.

Installation procedure

1. Download the Kofax eFlow ePortal installation package from [Kofax Fulfillment Site](#).
2. Run the MSI file. We recommend selecting the **Complete installation** option in the installation wizard. If you want to install specific ePortal features or change the default installation path, select the **Custom installation** option instead.

Select the server and database on which to install ePortal, as well as the authentication mode. You can also leave these fields blank and install the database manually using the 00_run_scripts.bat file (see step 3).

If you did not change the default installation path, a new folder Kofax eFlow ePortal is available in the C:\Program Files (x86)\TIS\Kofax eFlow ePortal. This folder contains all files required to complete the installation, including custom code samples, a testing CAB, and scripts to create the ePortal SQL database.

The remaining files (executables and all relevant DLLs) are copied to the Bin folder.

3. Create the ePortal database:

Note This step is only necessary if you do not select a server and database in the installation wizard.

- a. In the C:\Program Files (x86)\TIS\Kofax eFlow ePortal\DBScripts folder, edit the file 00_run_scripts.bat to correspond to your SQL server settings.

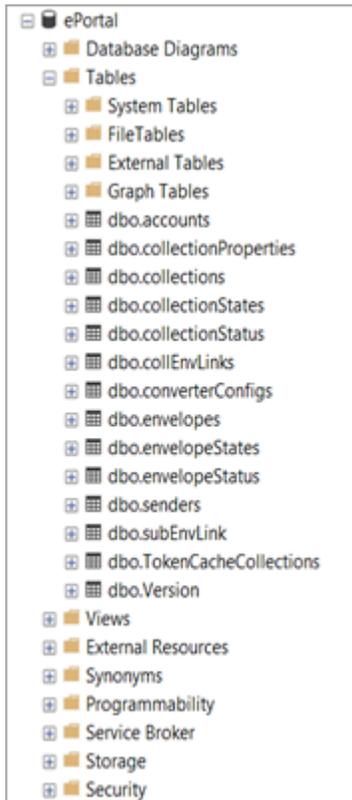
Depending on the operating system you are using, you may encounter some permissions issues. To resolve these issues:

- Give the installing user the appropriate permissions or copy the DBScripts folder to another location and run it from there.
- Set a specific location for the scripts. For example, if you copied the script files to the c:\temp folder, for each script, add the path C:\temp\DBScripts\10_CreateDB.sql.

See the following figure for example.

```
sqlcmd -v dbName=%DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 10_CreateDB.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 20_CreateTables.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 30_CreateStoredProcedures.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_0001_Version.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_0002to003.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_003.SupportTools.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_00042to0043.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_00043to0052.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_0048.SupportTools.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_0056to0057.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_0057_to_1_0_2_0.sql
sqlcmd -d %DB_NAME% %AUTHENTICATION_STRING% -S %SQLINSTANCE% -i 40_1_0_2_0_to_2_0_1_0.sql
```

- b. Run as administrator the file 00_run_scripts.bat. A new database ePortal should be available on the SQL server specified in the file.



4. Use the eFlow Administrative module to install the demo cab `C:\Program Files (x86)\TIS\Kofax eFlow ePortal\Cab\SimpleDemoEPortal.cab`.
5. To add an ePortal station to an existing application, in the Design module, add a simple auto station and add the following events:
 - **On Login Events:** `TIS.Import.ePortal.ePortalStation:ePortalStation:OnLogin`
 - **OnPreGetCollection:** `TIS.Import.ePortal.ePortalStation:ePortalStation:OnPreGetCollections`

Refer to the *Kofax eFlow Design User Guide* for information on adding events.

6. If you added an ePortal station to your application, copy `ePortal.AppConfig` from `SimpleDemoEPortal.cab` in `C:\Program Files (x86)\TIS\Kofax eFlow ePortal\Cab` folder to the Setup folder of your application. To access `ePortal.AppConfig`, change the `.cab` file extension to `.zip`.
7. The Setup folder path will be as the follows:


```
C:\ProgramData\TIS\eFlow 6\AppData\Server\SimpleDemoEportal\Setup
```

Here `SimpleDemoEportal` is the application name (You can give another name for the application as per your choice).

8. Configure ePortal.AppConfig in the Setup folder of the application.

The following example shows how to set up a Gmail account using POP3 connectivity. See the [Configuration](#) chapter for more information on configuration.

- a. In ePortal.AppConfig, check that the connection string node and username and password are correct.

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

- b. In the <Stations><ActiveAccounts> section, change the following parameter to the active account you would like to use.

```
<ActiveAccount Id="account1gmailPop3SSL " Enabled="true" />
```

- c. In the <Sections><MailAccounts> section, add the mail account from the previous section. See the following code for example.

```
<MailAccount Id="account1gmailPop3SSL" DisplayName="My Gmail POP
  SSL=YES profile" Host="pop.googlemail.com" Port="995" SSL="true"
  IgnoreCertificateErrors="false" UserName="YourEnCryptedLogin"
  Password="YourEnCryptedPassword" Protocol="POP3">
```

- d. You can now send an email to the email account and process an image with one of the SimpleDemoEPortal_EFLOW5 stations eportal1 or eportal2.

Upgrade instructions

Install the new ePortal 2.0.1 (see the [Installation procedure](#)). It will upgrade the existing ePortal 2.0 automatically.

To update SQL scripts from the previous versions to the new version, run each of the scripts in the appropriate order. The scripts can be found at:

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

Note If you specify the server and database in the installation wizard, you do not need to update the SQL scripts manually. The wizard updates the scripts and the ePortal database automatically, preserving existing data.

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.

Chapter 3

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 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 IMAP, POP3, POP3_OAUTH, EXCHANGE_ONLINE, IMAP_GMAIL, EWS, 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="account2gmailIMAPSSL" Enabled="true" />
    <ActiveAccount Id="YourSMTPAccount" 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.
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="account1gmailPop3SSL">
        ...
      </MailAccount>
    </MailAccounts>
  </Section>
</Sections>
```

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 4

Connectors

ePortal uses connectors to retrieve data from remote servers, such as email servers. ePortal provides the following connectors.

POP3 connector

The POP3 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 connector can only read or delete emails.

Once all 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. Synchronized mode does not delete the emails from the mailbox after they have been imported.

Configuration

```
<MailAccount Id="account1gmailPop3SSL" DisplayName="My Gmail POP SSL=YES profile"  
Host="pop.googlemail.com" Port="995" SSL="true" UserName="XXXXXX" Password="XXXXX"  
Protocol="POP3">
```

POP3_OAUTH connector

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

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. 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 eportal.appconfig file, you need to manually authorize yourself in ePortal station by entering configured mail account credentials and permissions consent.

Scenario 2: When your email account password expires or changes, then you need to re-authorize yourself by opening ePortal station manually.

After that, enable the autorun mode for the ePortal station.

Configuration

Any application that implements OAuth standard to authenticate and authorize its users 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, which is subjected to the individual organization IT policies.

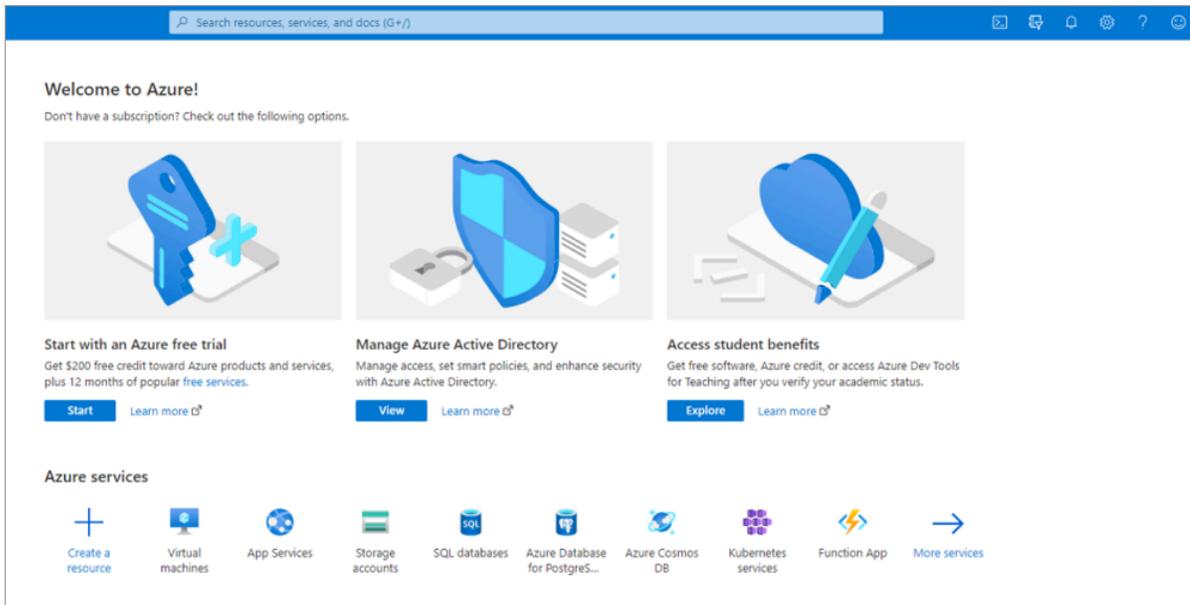
Azure cloud configuration for Office 365

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

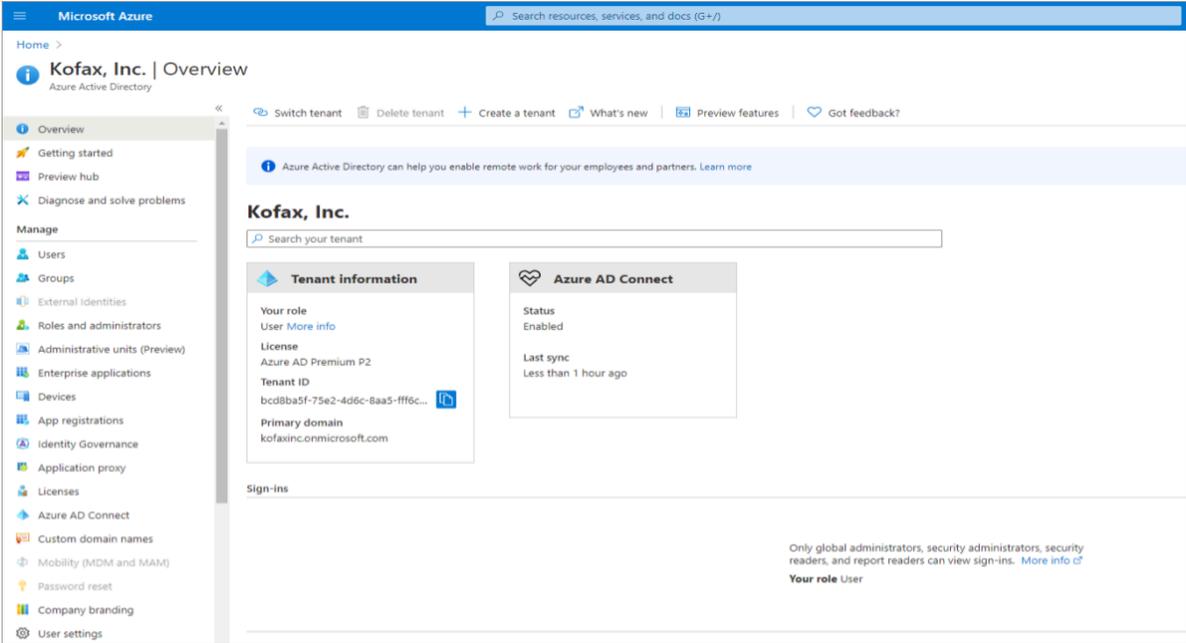
Note The figures used in the following instructions are taken from Microsoft Azure site, the appearance and user interfaces might change occasionally.

1. Sign in to <https://portal.azure.com> using your work account. Follow the on-screen instructions to complete the sign-in procedure.

After completion of sign-in procedure, the Azure home page appears.



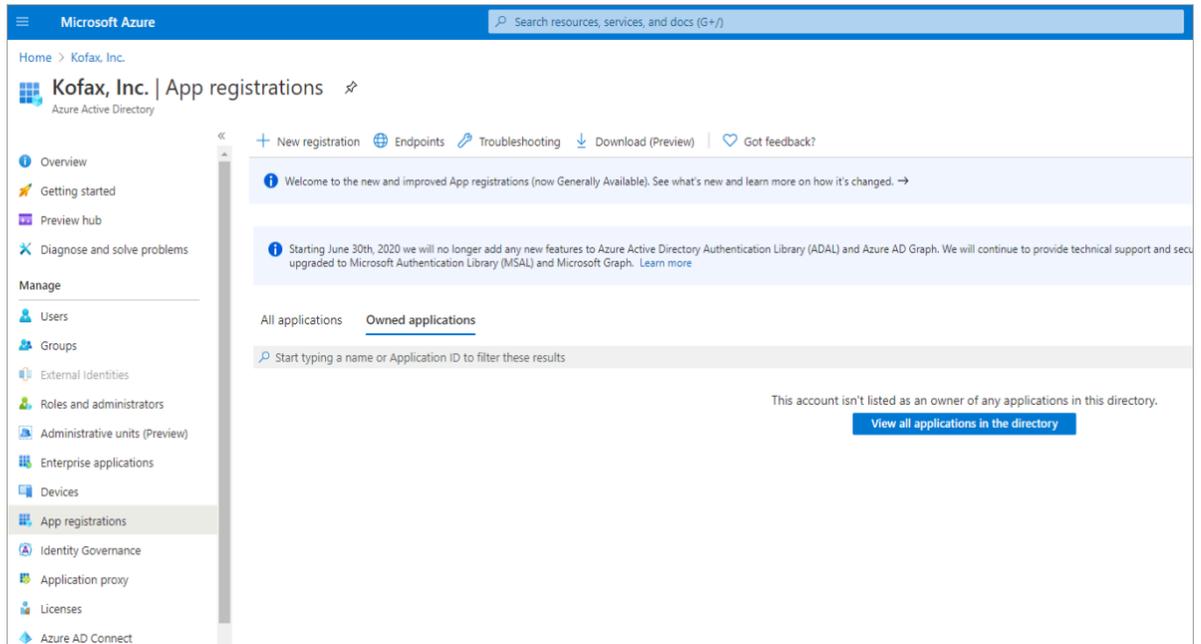
- 2. On the Azure home page, under **Manage Azure Active Directory**, click **View**. The **Overview** page appears.



Manage App registrations

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

1. In the left pane, under **Manage**, click **App registrations**.
The **App registrations** page appears.



2. Click New registration.

The **Register an application** page appears.

Microsoft Azure Search resources, services, and docs (G+)

Home > Kofax, Inc. >

Register an application

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

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (Kofax, Inc. only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[Help me choose...](#)

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

Web

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

Register

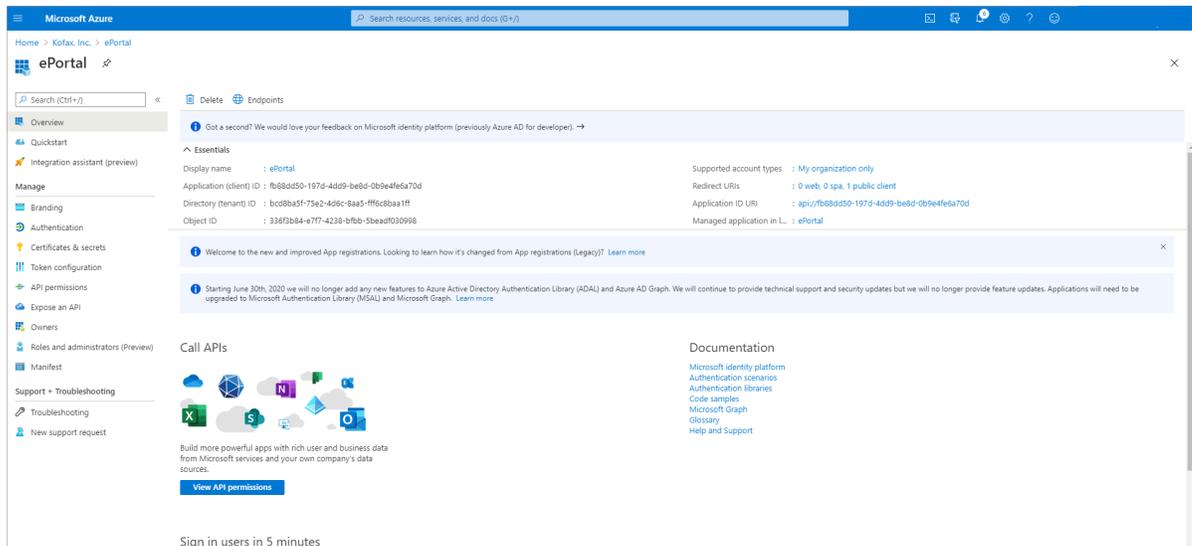
3. In the **Name** field, enter the application name that to be displayed to the users.

4. Under **Supported account types**, select **Accounts in this organizational directory only (Kofax, Inc. only - Single tenant)**.

Note Select this option if you are building a line-of-business (LOB) application. This option is not available if you are not registering the application in a directory. This option maps to Azure AD only single tenant and is the default unless you are registering the app outside of a directory. In cases where the app is registered outside of a directory, the default is Azure AD multi-tenant and personal Microsoft accounts.

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

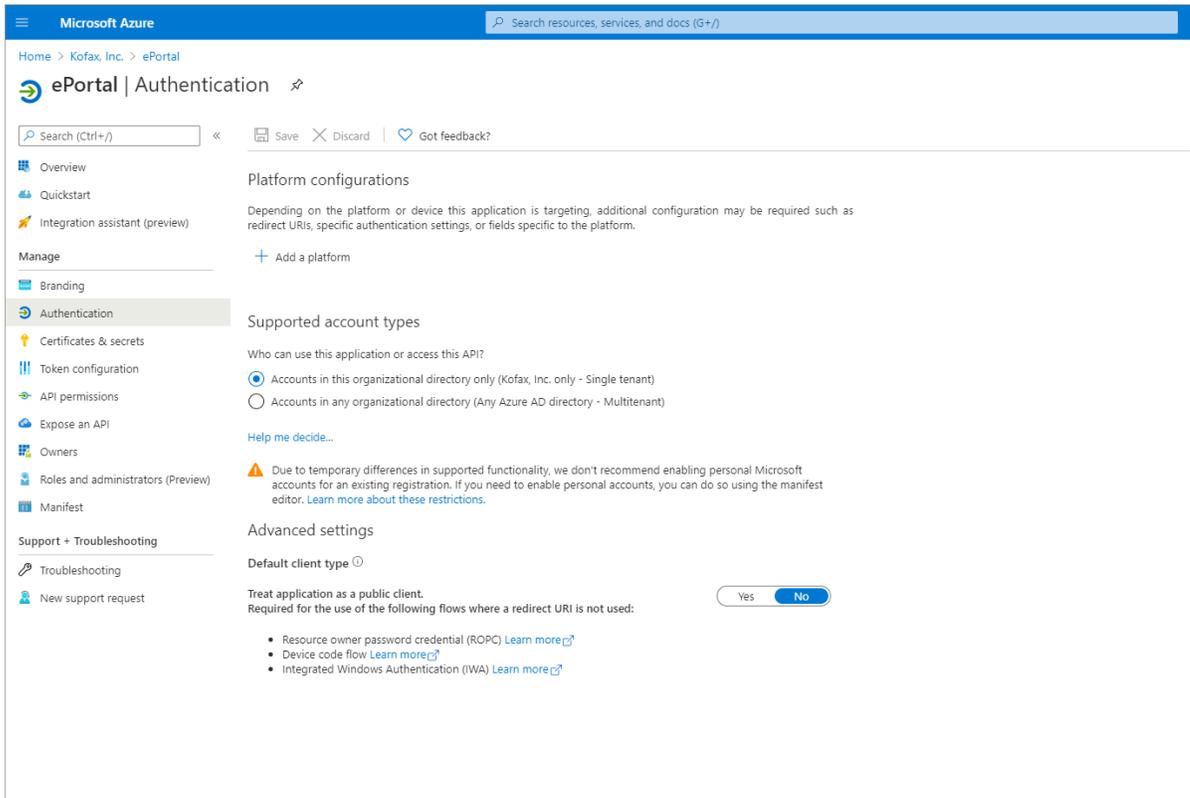
The following page appears.



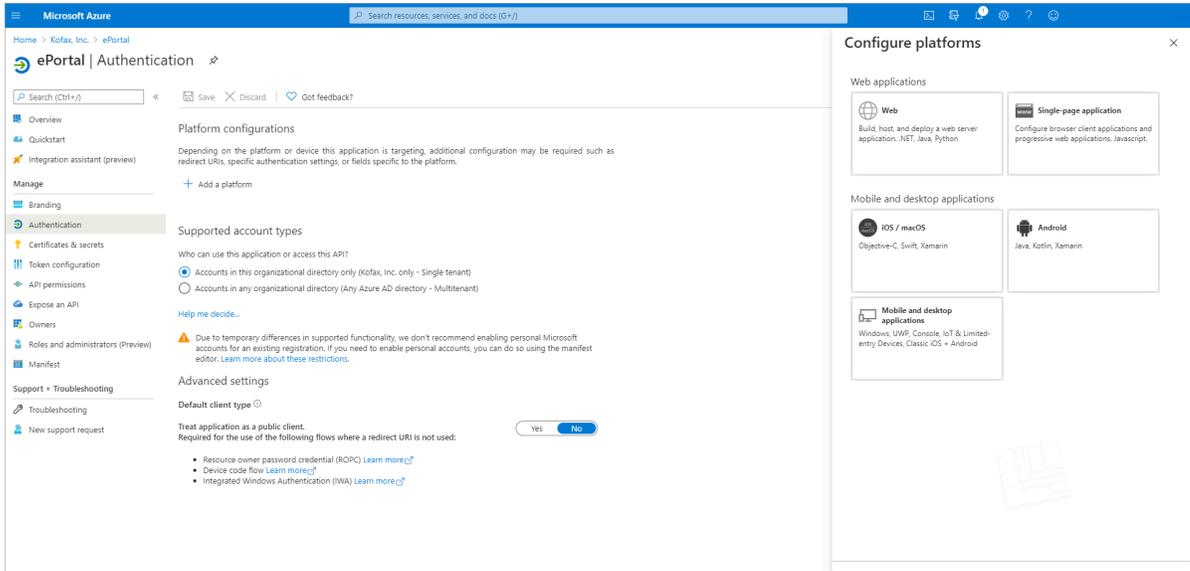
Manage authentication

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

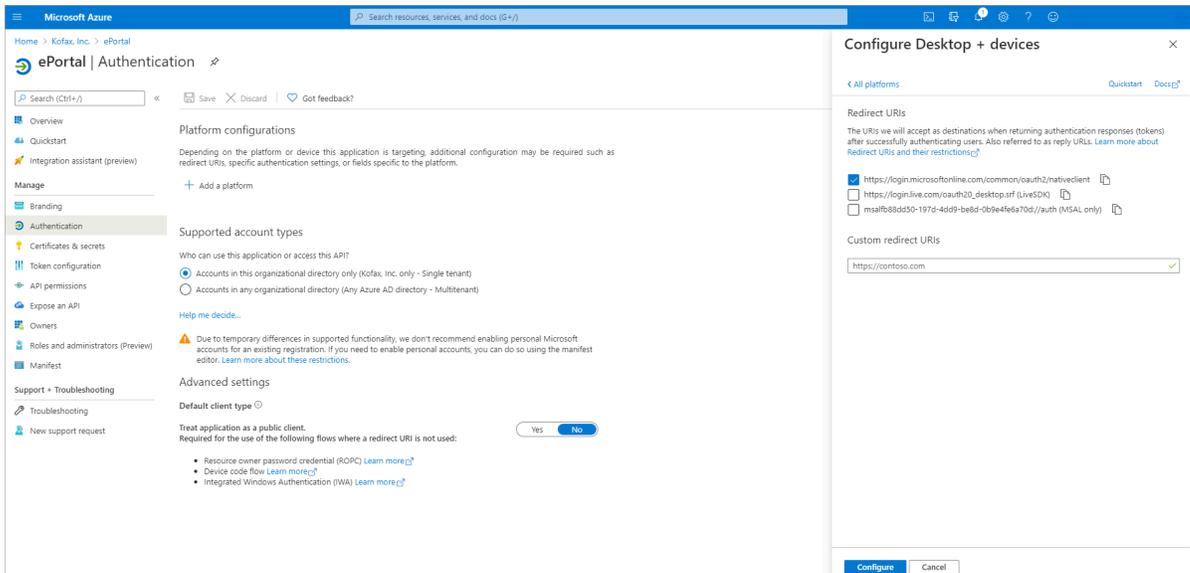
1. In the left pane under **Manage**, click **Authentication**.
The **Authentication** page appears.



- 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.



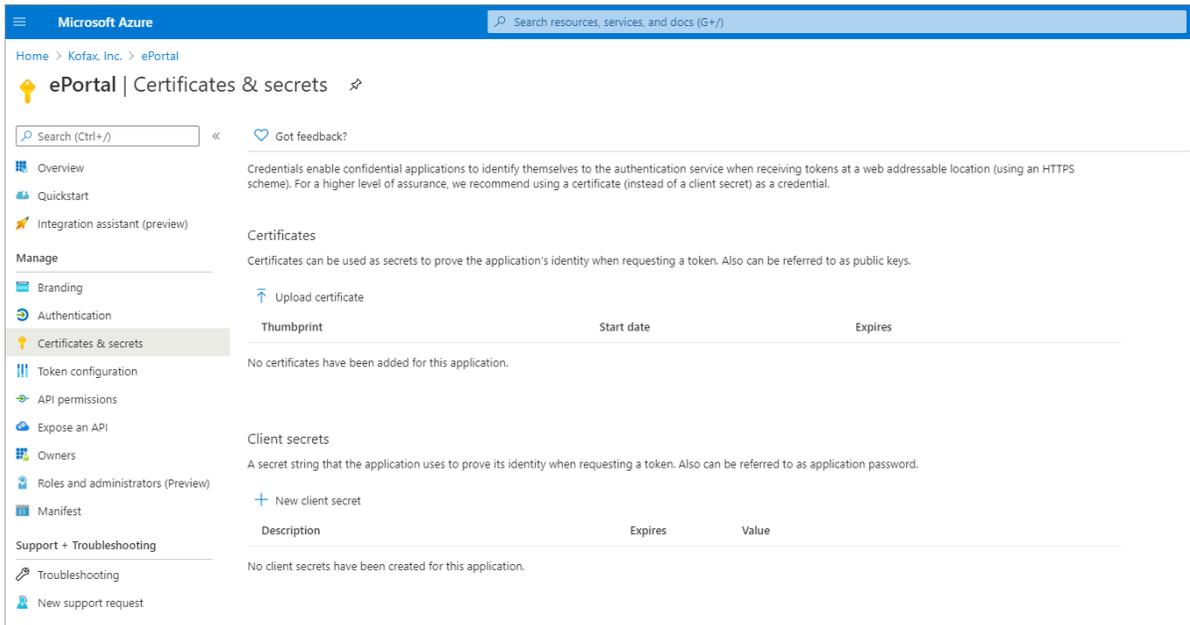
4. Select **https://login.microsoftonline.com/common/oauth2/nativeclient**, and click **Configure**. On the **Authentication** page, under **Redirect URIs**, you can see the selected option.

The screenshot displays the Microsoft Azure portal interface for configuring an application. The left-hand navigation pane includes sections for Overview, Quickstart, Integration assistant, Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators, Manifest), and Support + Troubleshooting. The main content area is titled 'Platform configurations' and includes a section for 'Mobile and desktop applications'. Within this section, the 'Redirect URIs' are listed, with the first one, 'https://login.microsoftonline.com/common/oauth2/nativeclient', being selected. Below the URIs, the 'Supported account types' are configured to 'Accounts in this organizational directory only (Kofax, Inc. only - Single tenant)'. A warning message is present regarding personal Microsoft accounts.

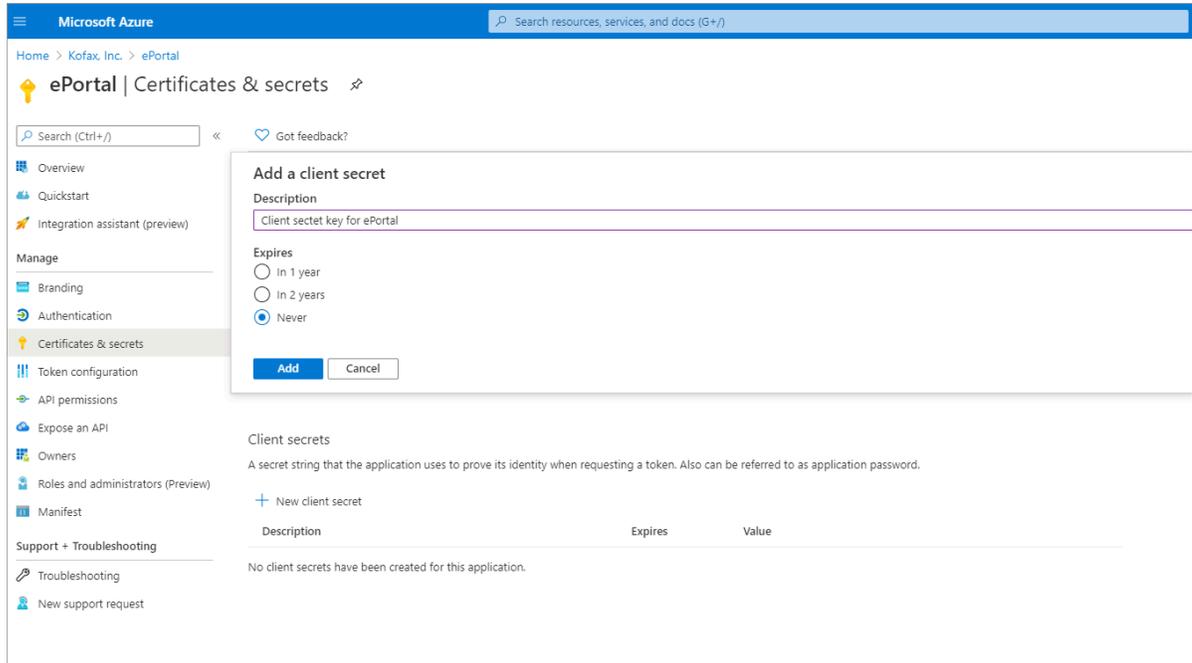
Manage certificates and secrets

Upload certificate or create client secrets to enable confidential applications.

1. In left pane, under **Manage**, click **Certificate & secrets**.
The **Certificate & secrets** page appears.



2. Under **Client secrets**, click **New Client secret**.
The **Add a client secret** section 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 client secret details.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the current location: Home > Kofax, Inc. > ePortal. The main heading is 'ePortal | Certificates & secrets'. A search bar and a 'Got feedback?' link are present. The left sidebar contains navigation options: Overview, Quickstart, Integration assistant (preview), Manage (Branding, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators (Preview), Manifest), and Support + Troubleshooting (Troubleshooting, New support request). The main content area features a message: 'Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.' Below this, the 'Certificates' section explains their use and provides an 'Upload certificate' link. A table shows 'No certificates have been added for this application.' The 'Client secrets' section explains their use and provides a '+ New client secret' link. A table lists the client secret details:

Description	Expires	Value
Client secret key for ePortal	12/31/2299	do1Hq,0xDy18H6j8.7d-J5WvaPIOb,_t

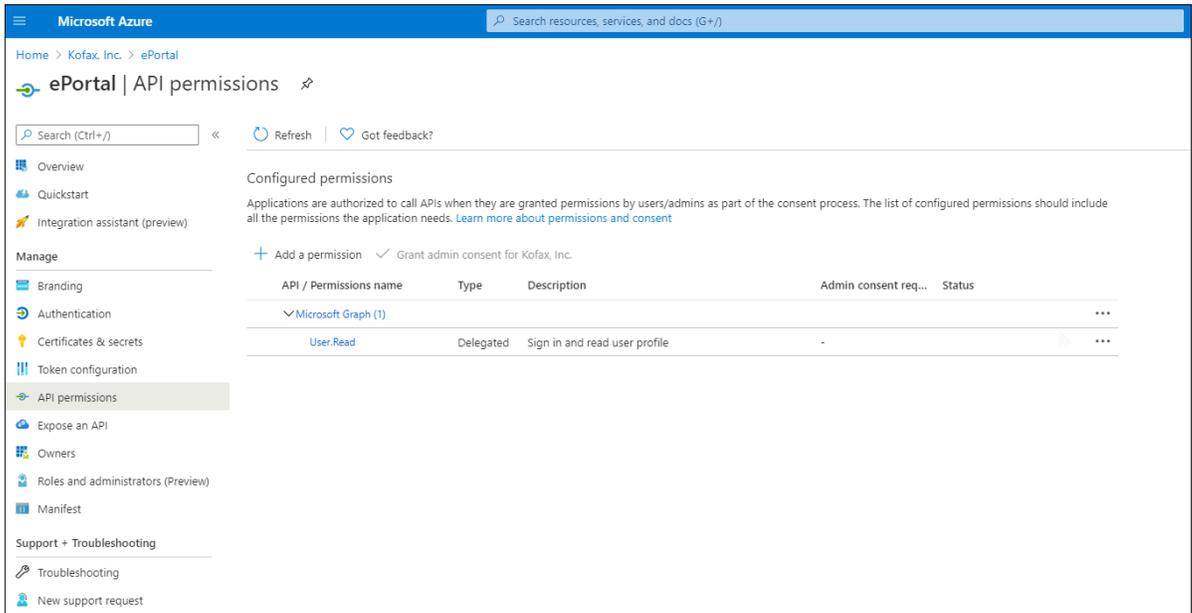
A 'Copy to clipboard' button is visible next to the value.

Note Note down the Client secrets value to refer in the future activities.

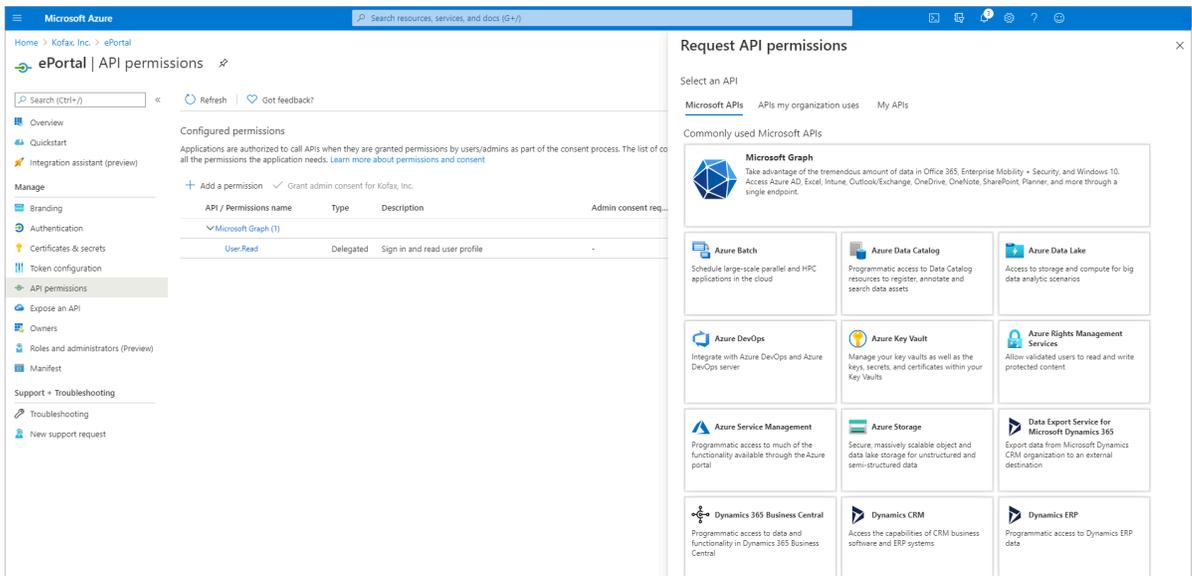
Manage API permissions

Add the required permissions to authorize applications to call APIs.

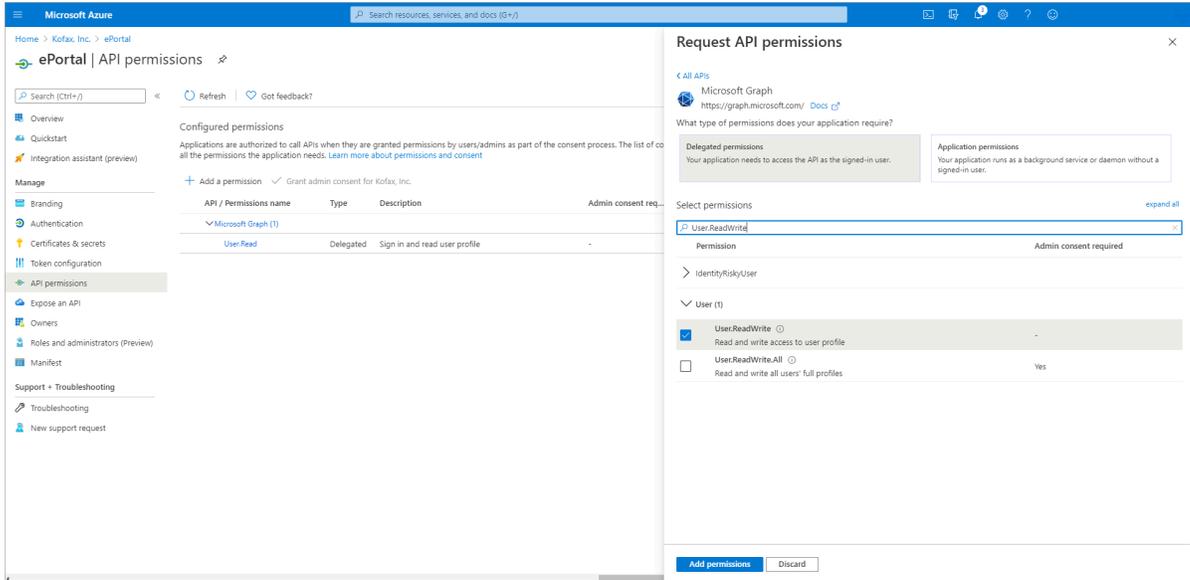
1. In the left pane, under **Manage**, click **API permissions**.
The **API permissions** page appears.



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**.

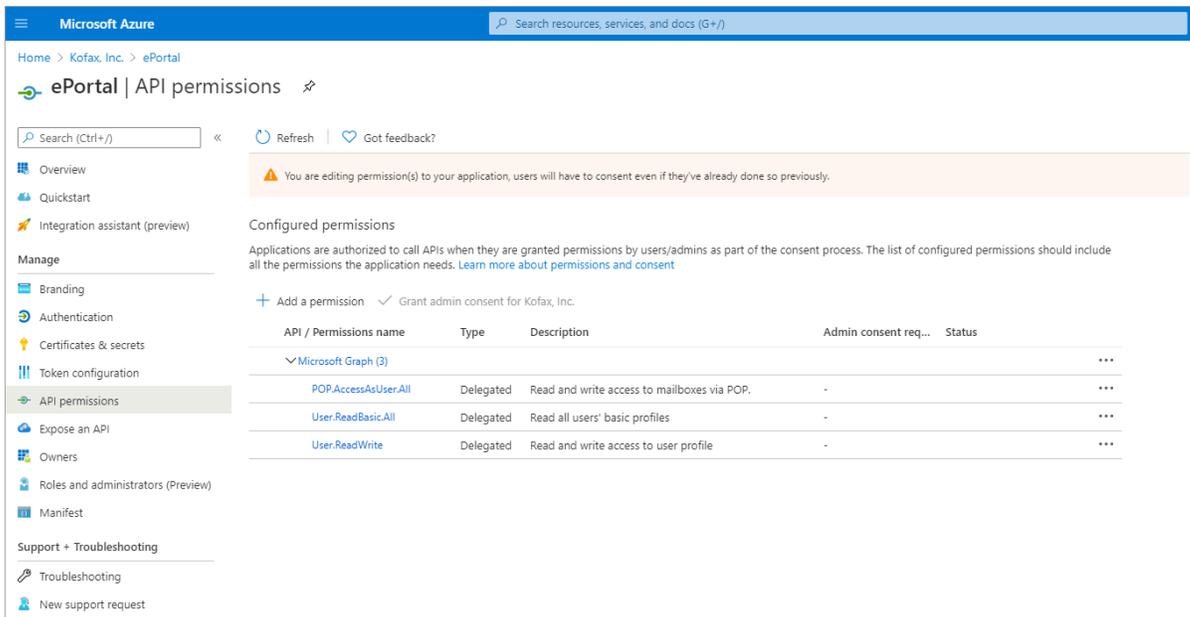


4. Click **Delegated permissions > Select Permission**, and then select the following three permissions.

- Pop.AccessAsUser.All
- User.ReadBasic.All
- User.ReadWrite

5. Click **Add permissions**.

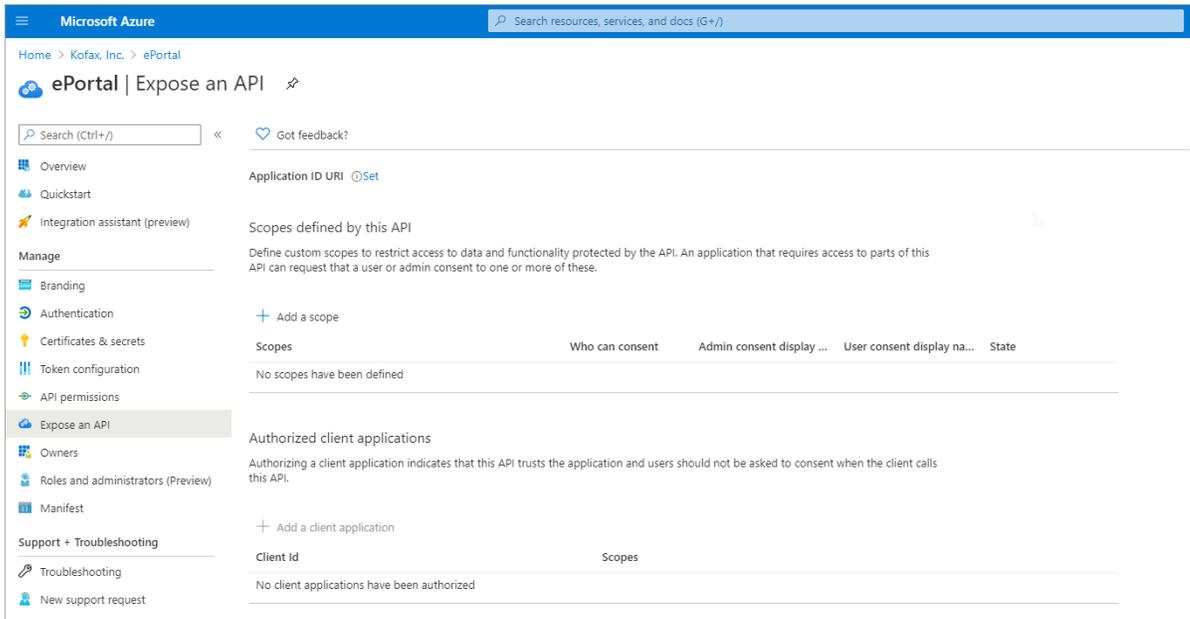
On the **API permissions** page, under **API / Permissions name**, you can see all the three permissions.



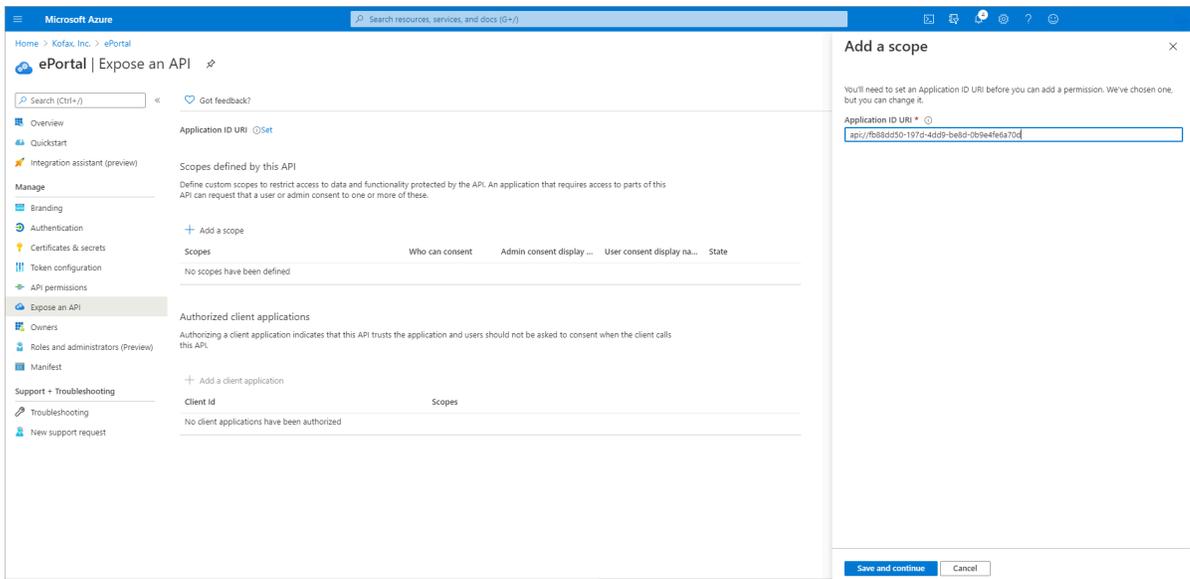
Manage exposing an API

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

1. In the left pane, under **Manage**, click **Expose an API**.
The **Expose an API** page appears.

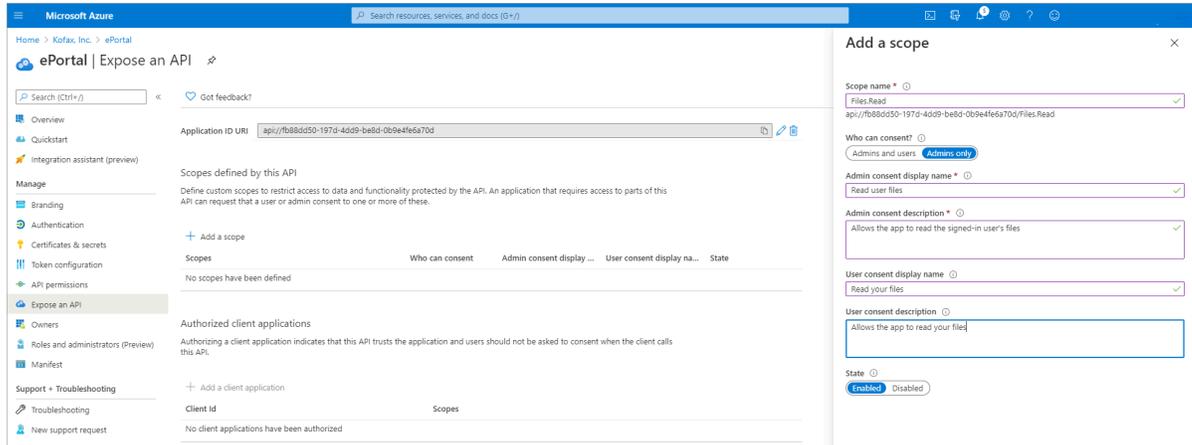


2. Under **Scopes defined by this API**, click **Add a scope**.
The **Add a scope** section appears on the right side of the page.



3. Click **Save and continue**.

The **Add a scope** section appears on the right side of the page.



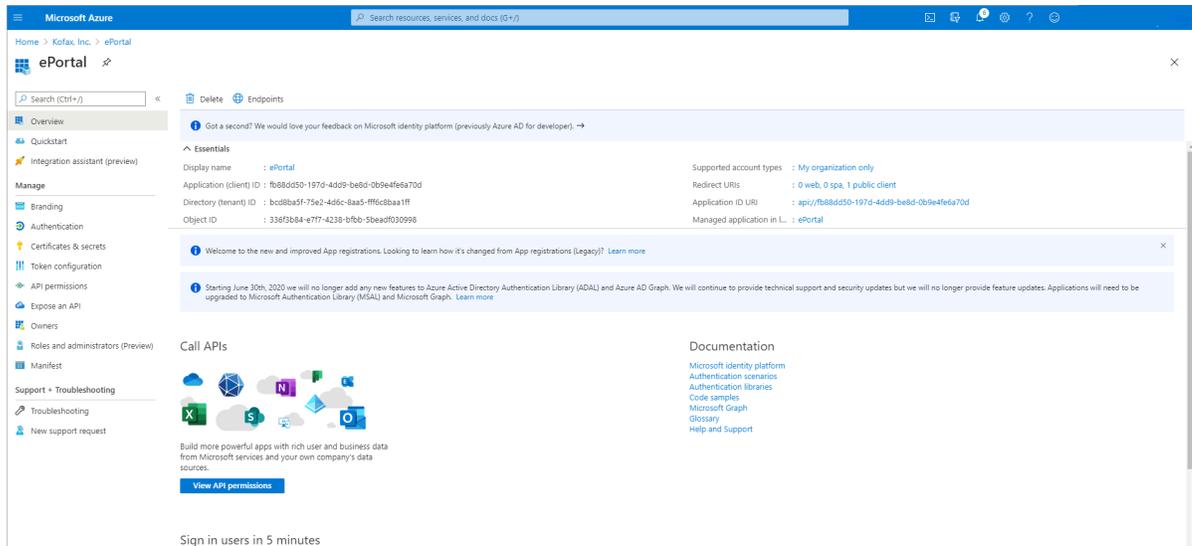
4. For **Who can consent?**, select **Admins only**.

5. For **State**, select **Enabled**.

6. Click **Add scope**.

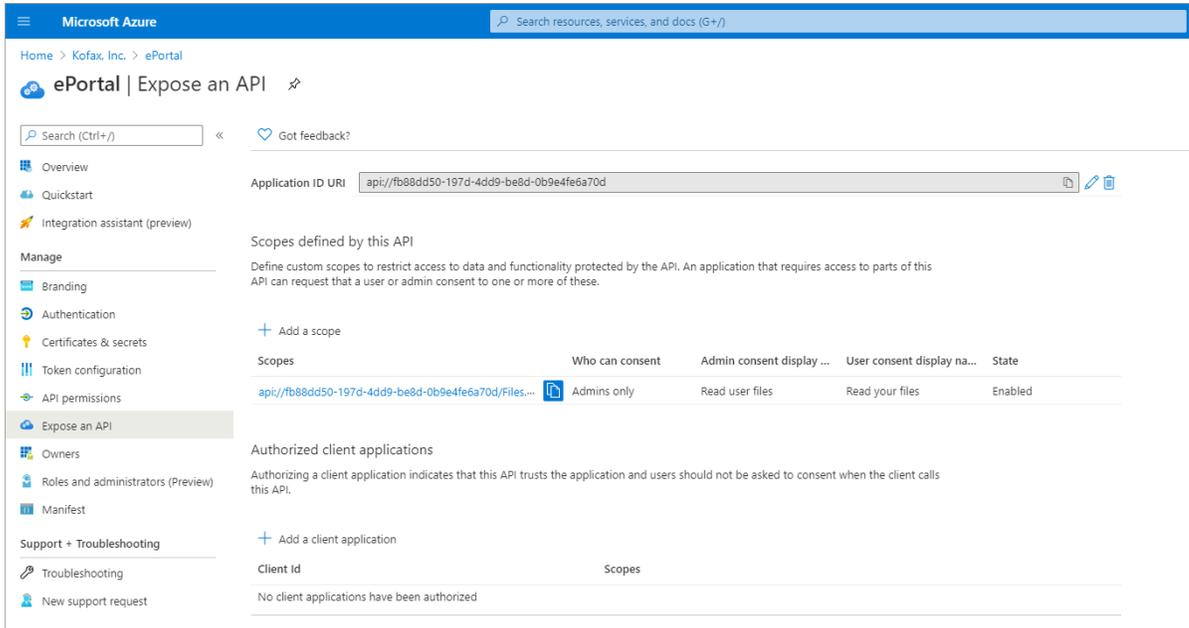
7. In the left pane, click **Overview**.

The **Overview** page appears.

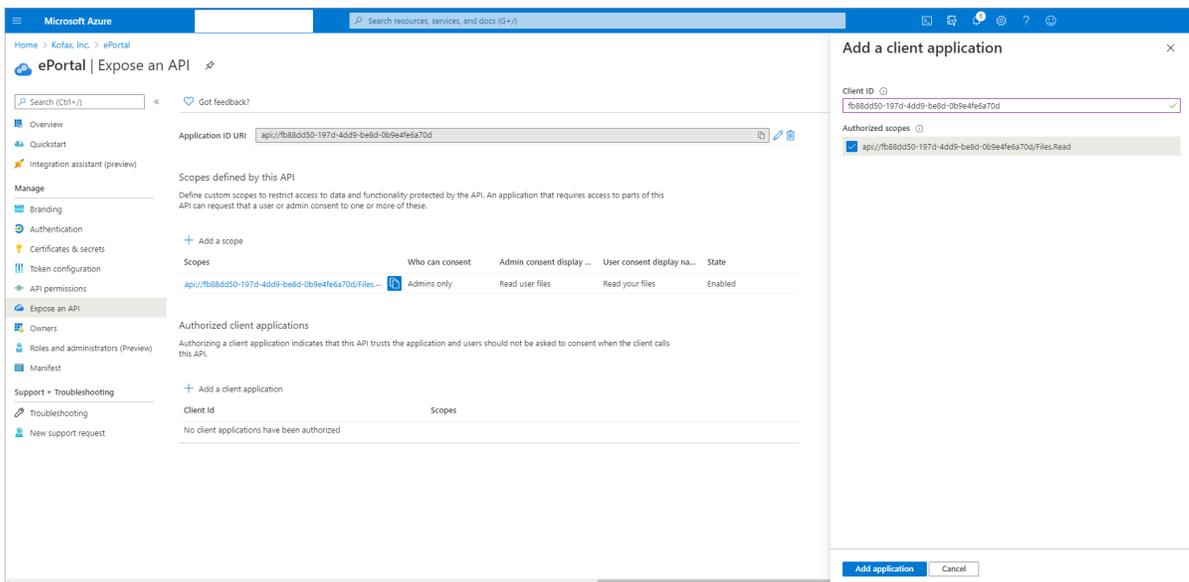


8. Note down the **Application (client) ID**.

- In the left pane, click **Expose an API**.
The **Expose an API** page appears.



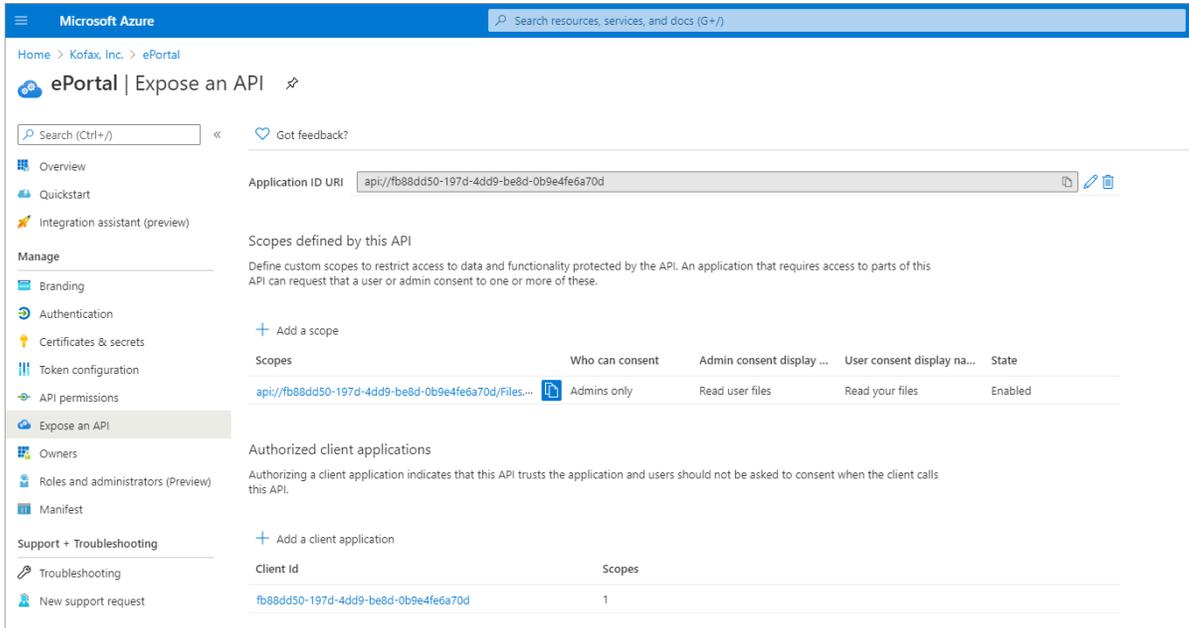
- Under **Authorized Client applications**, click **Add a client application**.
The **Add a client application** section appears on the right side of the page.



- In the **Client ID** field, paste the copied client ID.
- 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

The **Owners** page allows you see the owners of the ePortal.

In the left pane, under **Manage**, click **Owners**.

The **Owners** page appears. In this page you can see the owners of the ePortal.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Kofax, Inc. > ePortal

ePortal | Owners

Search (Ctrl+F) << + Add owners Remove owners Got feedback?

Overview
Quickstart
Integration assistant (preview)

Manage

Name	Email	User name	Job Title	Type
<input type="checkbox"/> John Doe	John.Doe@kofax.com	John.Doe@kofax.com	Mission Director	Member

In addition to users with permission to manage any applications, the users listed here can view and edit this application registration.

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators (Preview)
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Note An admin can add more than one owners.

Manage roles and administrators (Preview)

The **Roles and administrators (Preview)** page allows you to see the various administrative roles.

In the left pane, under **Manage** click **Roles and administrators (Preview)**.

The **Roles and administrators (Preview)** page appears. In this page you can see administrative roles.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Kofax, Inc. > ePortal

ePortal | Roles and administrators (Preview)

Search (Ctrl+F) << Refresh Preview features Got feedback?

Overview
Quickstart
Integration assistant (preview)

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators (Preview)
Manifest
Support + Troubleshooting
Troubleshooting
New support request

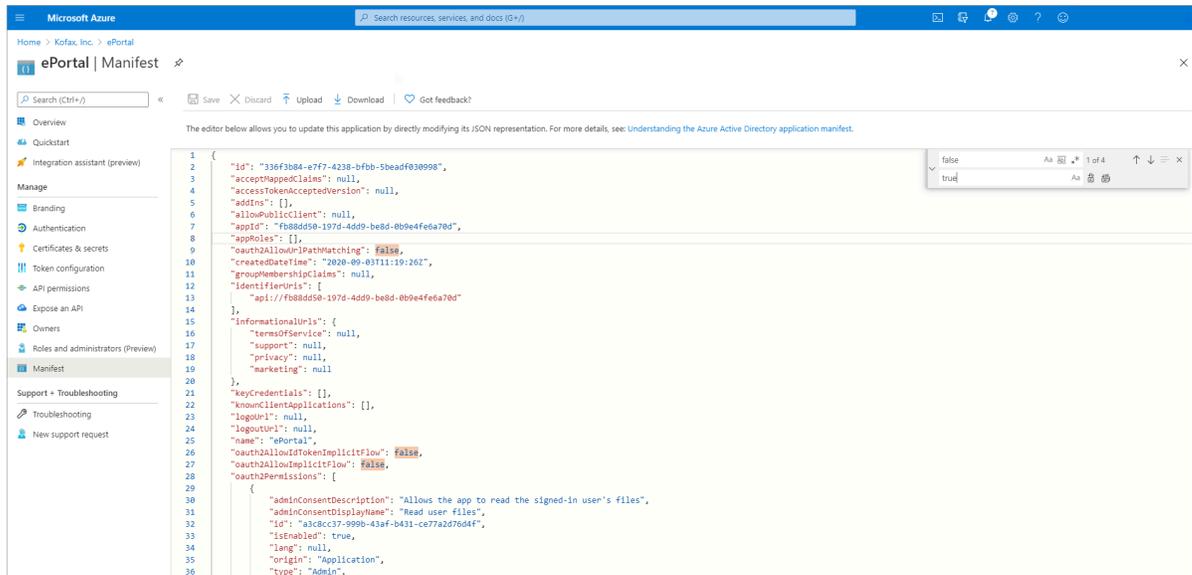
Administrative roles
Administrative roles can be used to grant access to specific areas of this resource. Assign owners using the owner tab to grant full access to this resource.
Assignable roles are roles that can be assigned here to allow managing this resource. Directory-level roles have inherited access to this resource and can only be assigned at the directory level here

Role	Description	Type
Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in
Application developer	Can create application registrations independent of the 'Users can register applications' setting.	Built-in
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	Built-in
Directory readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	Built-in
Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.	Built-in
Global reader	Can read everything that a global administrator can, but not update anything.	Built-in
Hybrid identity administrator	Can enable, deploy, configure, manage, monitor, and troubleshoot cloud provisioning and authentication services.	Built-in
Security administrator	Can read security information and reports, and manage configuration in Azure AD and Office 365.	Built-in

Manage manifest

The Manifest page opens an editor where you can update the application by directly modifying its JSON representation.

1. In the left pane, under **Manage**, click **Manifest**.
The **Manifest** page appears.



2. Replace all "false" with "true", 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. In the left pane, under **Manage**, click **Branding**.
The **Branding** page appears.

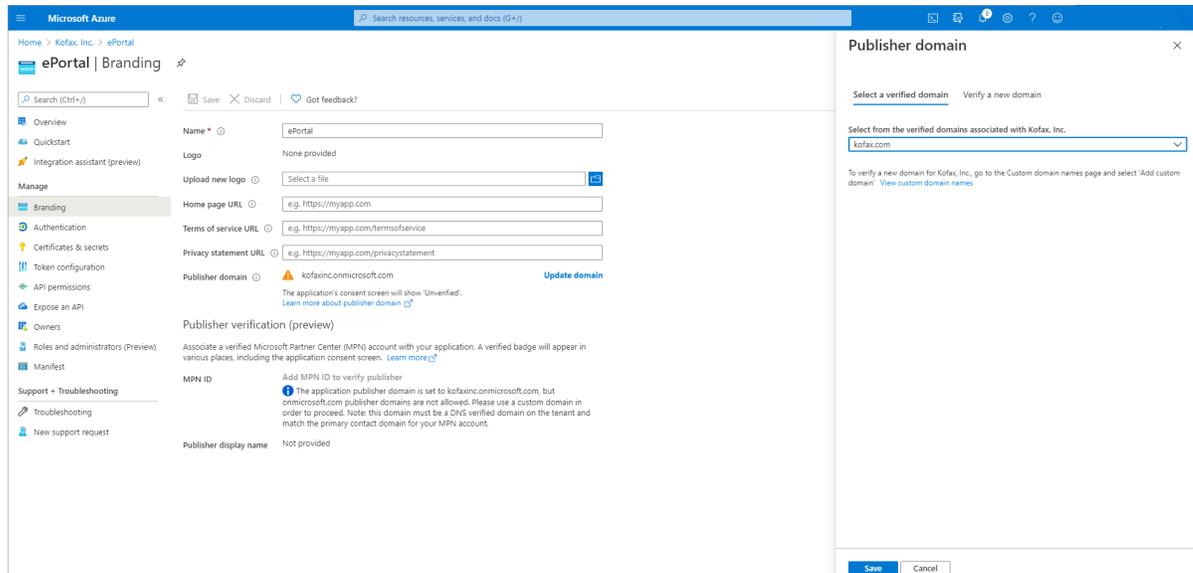
The screenshot displays the Microsoft Azure portal interface for the 'ePortal | Branding' page. The left-hand navigation pane is expanded to the 'Manage' section, with 'Branding' selected. The main content area contains the following configuration fields:

- Name ***: A text input field containing 'ePortal'.
- Logo**: A section with the text 'None provided' and an 'Upload new logo' button with a file icon.
- Home page URL**: A text input field containing 'e.g. https://myapp.com'.
- Terms of service URL**: A text input field containing 'e.g. https://myapp.com/termservice'.
- Privacy statement URL**: A text input field containing 'e.g. https://myapp.com/privacystatement'.
- Publisher domain**: A text input field containing 'kofaxinc.onmicrosoft.com' with an 'Update domain' button. A warning icon and message state: 'The application's consent screen will show 'Unverified'. [Learn more about publisher domain](#)'.
- Publisher verification (preview)**: A section with a heading and a paragraph: 'Associate a verified Microsoft Partner Center (MPN) account with your application. A verified badge will appear in various places, including the application consent screen. [Learn more](#)'.
- MPN ID**: A section with the heading 'Add MPN ID to verify publisher' and a message: 'The application publisher domain is set to kofaxinc.onmicrosoft.com, but onmicrosoft.com publisher domains are not allowed. Please use a custom domain in order to proceed. Note: this domain must be a DNS verified domain on the tenant and match the primary contact domain for your MPN account.'
- Publisher display name**: A text input field containing 'Not provided'.

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.

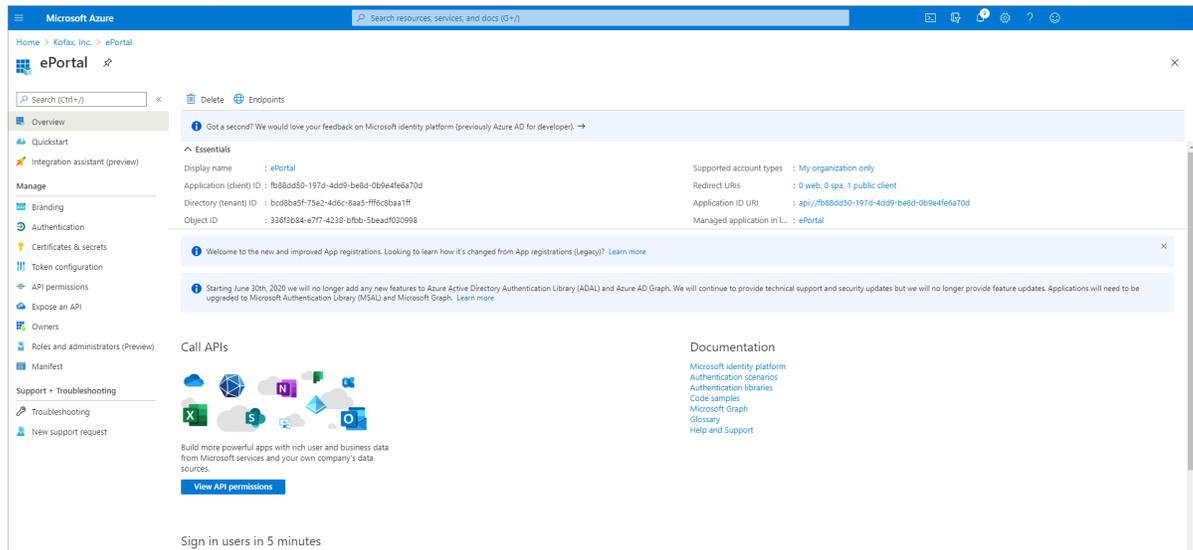


4. On the **Select a verified domain** tab, select a domain that is associated with your organization from the list.

5. Click **Save**.

6. In the left pane, click **Overview**.

The **Overview** page appears.



7. Keep a note of **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>
  <Subfolder>0</Subfolder>
  <SharedMailbox />
  <Filter />
  <Impersonate Enabled = "false" />
</ MailAccount >
```

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

2. Open C:\ProgramData\TIS\<eFlow6>\AppData\Server\<Application_name>\Setup\EPortal.AppConfig, and paste the copied content under <MailAccounts/> section.
3. Change Id, DisplayName, UserName, TenantID and ClientID.

Note Go to #25 for help.

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

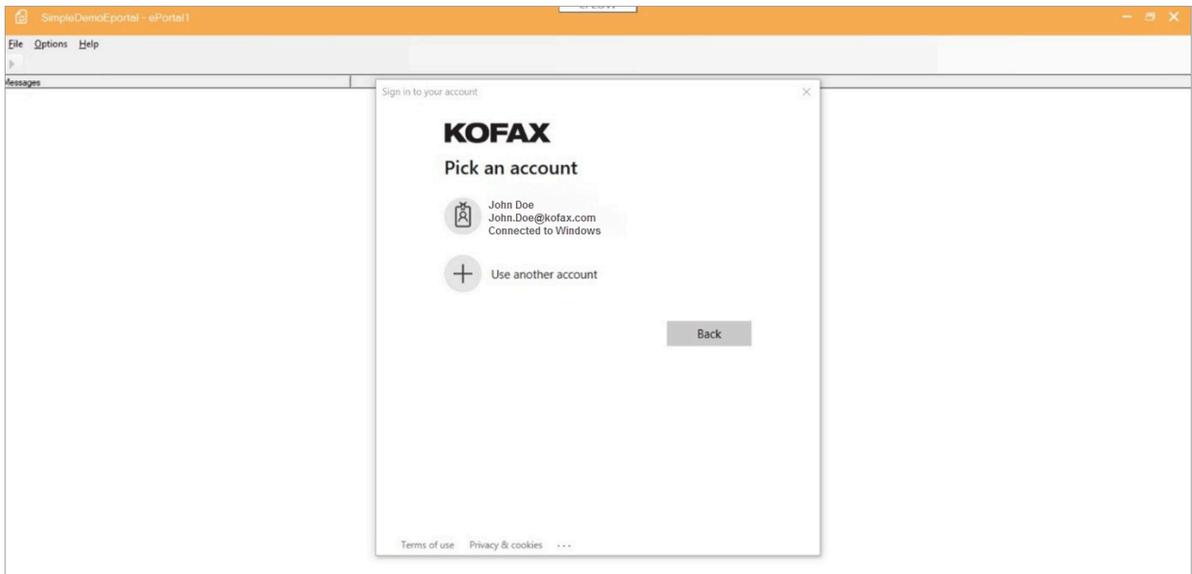
Do the following to run the **ePortal manual station**.

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

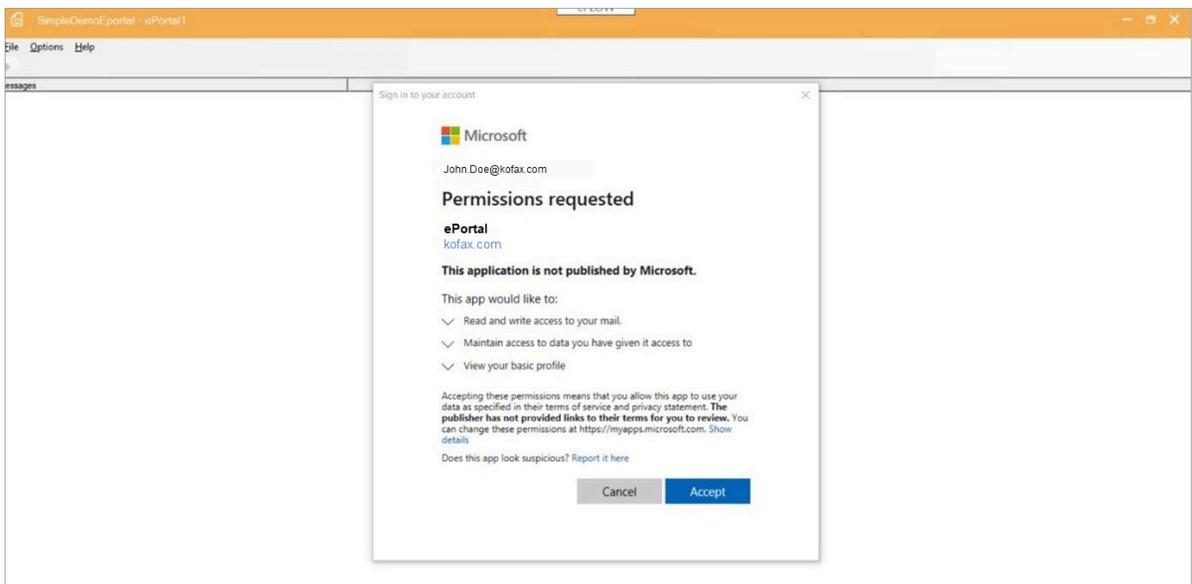
Important If your default browser is Internet Explorer, make sure that JavaScript is enabled.

2. If the given username in eportal.appconfig (email id) is not outlook configured with the computer using ePortal.

The following page appears.

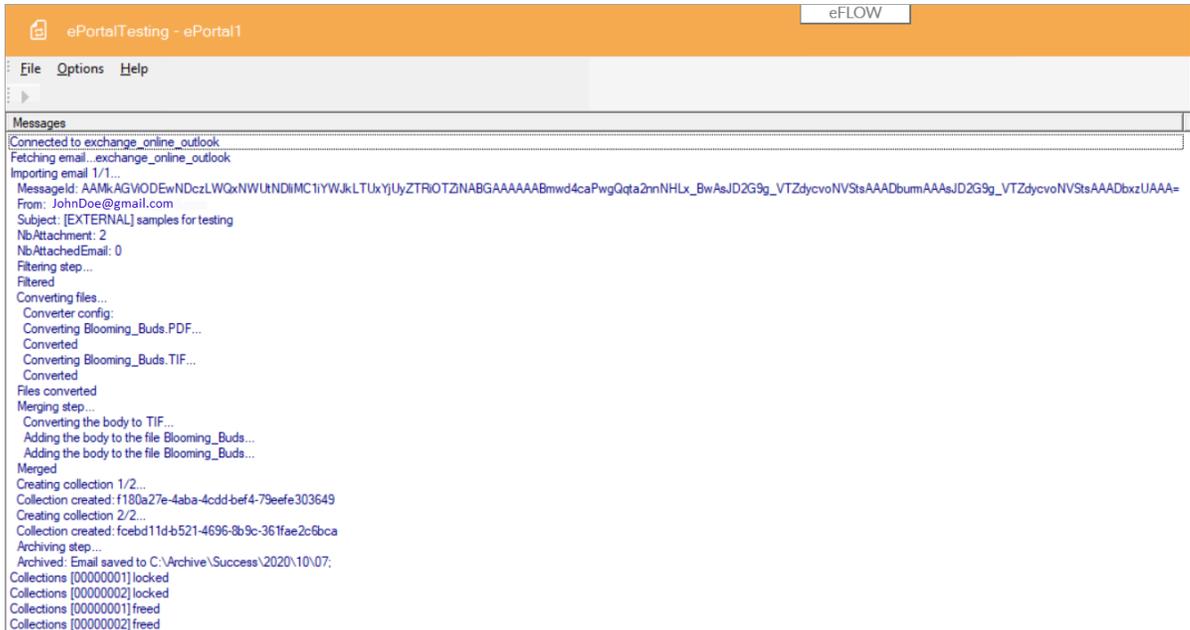


3. Select an account, and then enter your password to sign in. After sign-in, the following page appears.



4. Click **Accept**.

5. After accepting the permission, the **ePortal Manual station** will start to fetch the outlook messages from the configured folder.



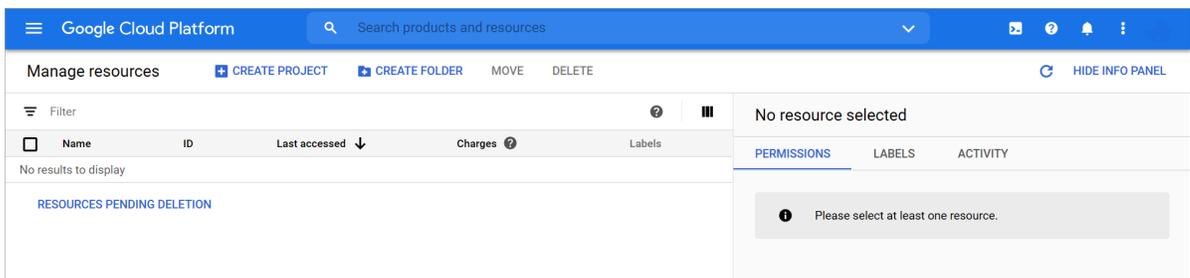
Google cloud configuration for Gmail

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

Note The figures used in the following instructions are taken from Google site, the appearance and user interfaces might change occasionally.

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

The **Google Cloud Platform** main page appears.



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

Google Cloud Platform

New Project

 You have 12 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name * ?

Project ID: gmailoauth-288511. It cannot be changed later. [EDIT](#)

Location * [BROWSE](#)

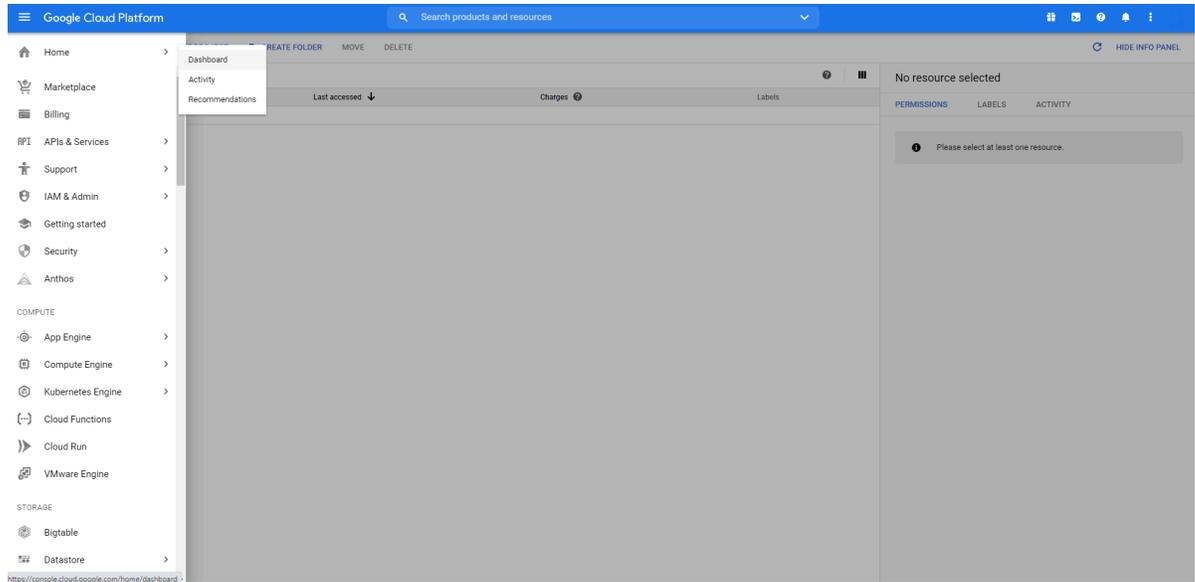
Parent organization or folder

[CREATE](#) [CANCEL](#)

3. In the **Project name** * field, enter a name for the project.
4. In the **Location** field, select location as "No organization".

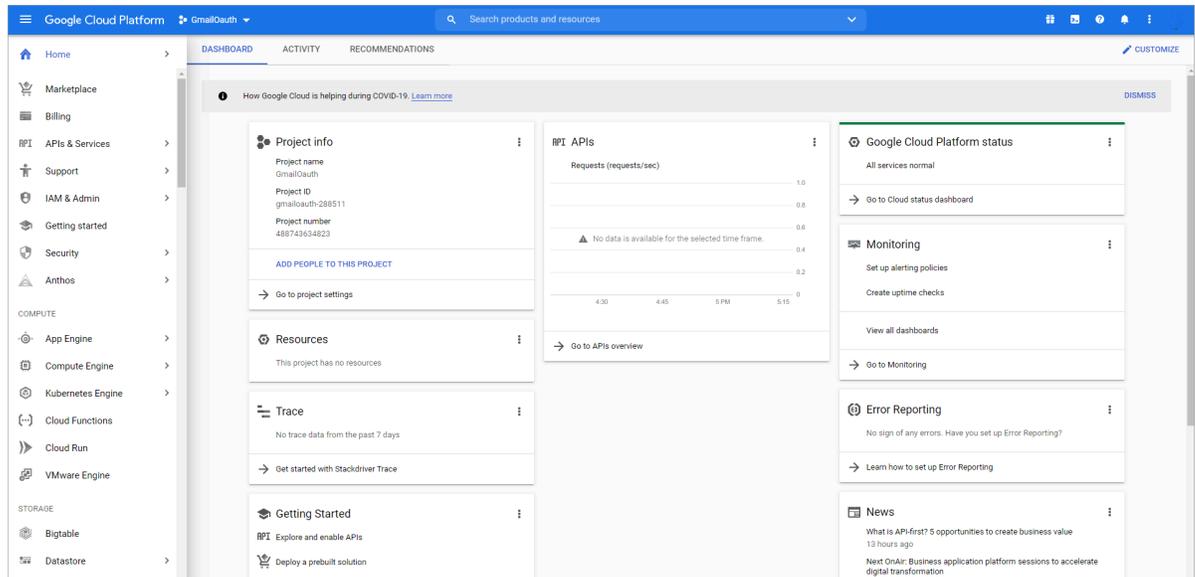
5. Click **CREATE**.

The following page appears.

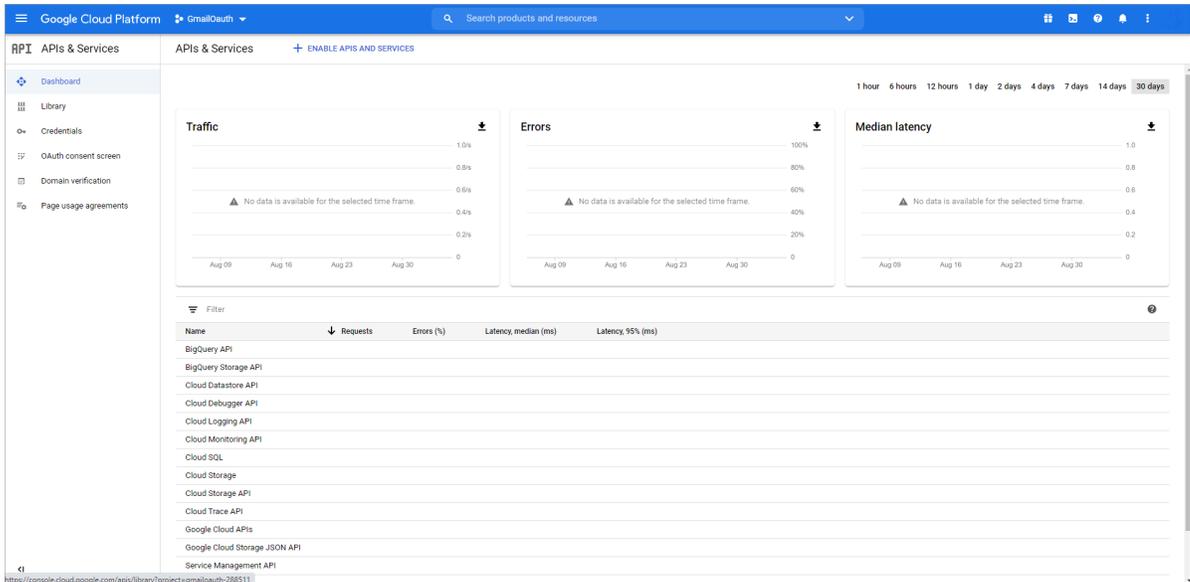


6. In the left pane, select **Home > Dashboard**.

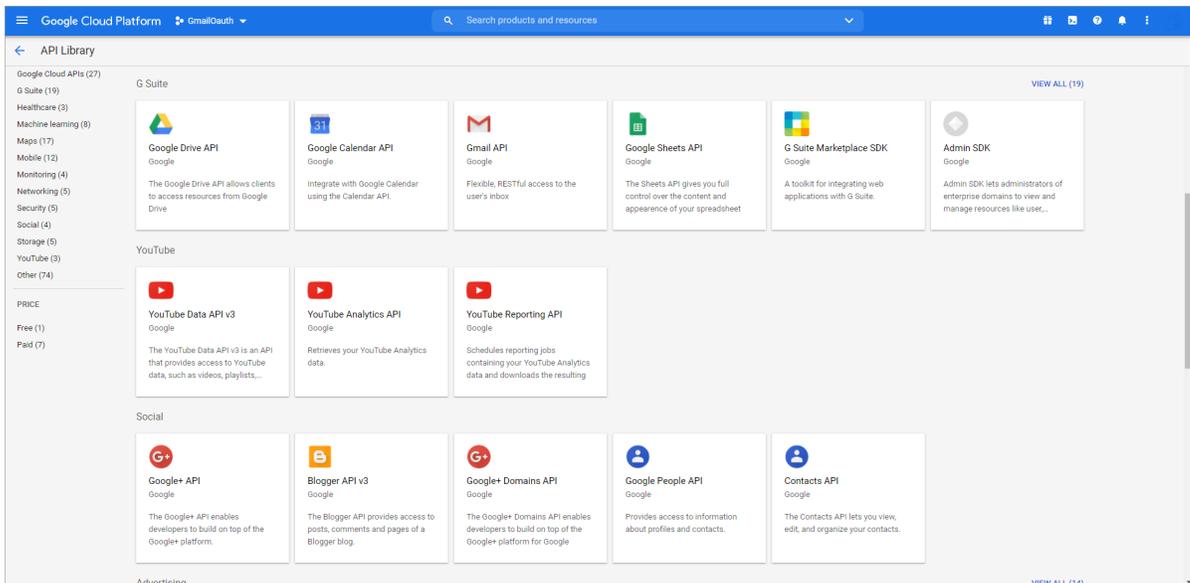
The **Dashboard** page appears.



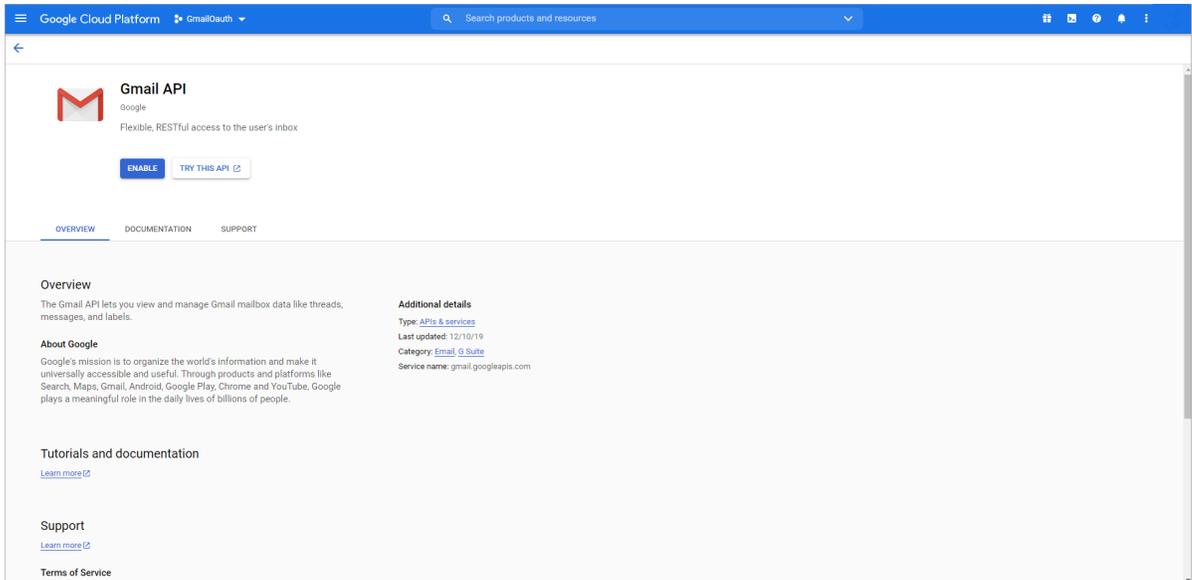
- Under **Getting Started**, click **Explore and enable APIs**.
The **APIs & Services** page appears.



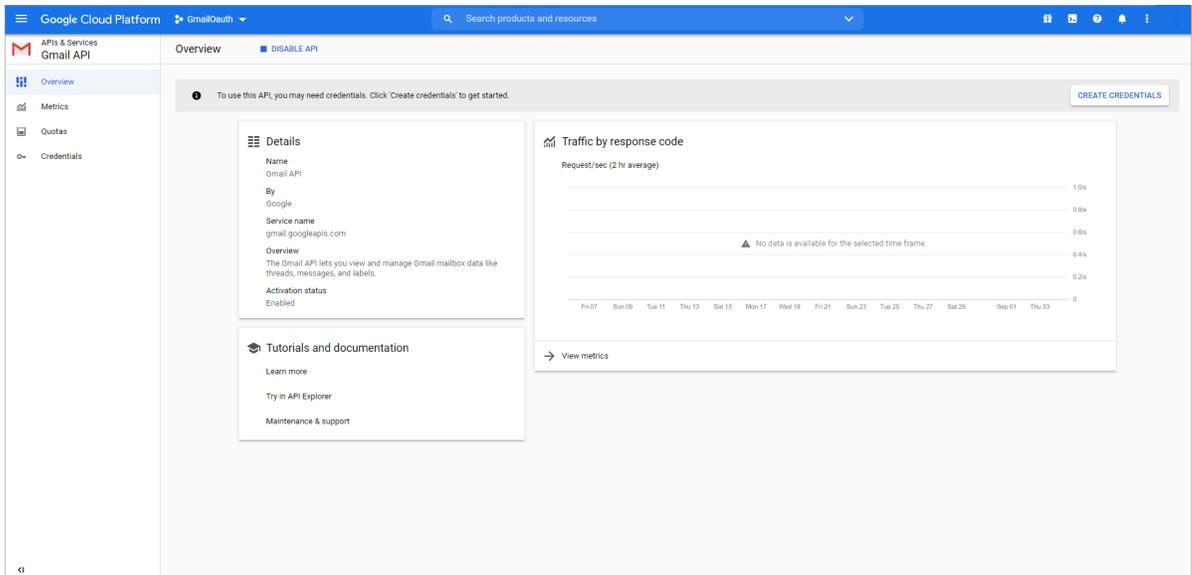
- In the left pane, click **Library**.
The **API Library** page appears.



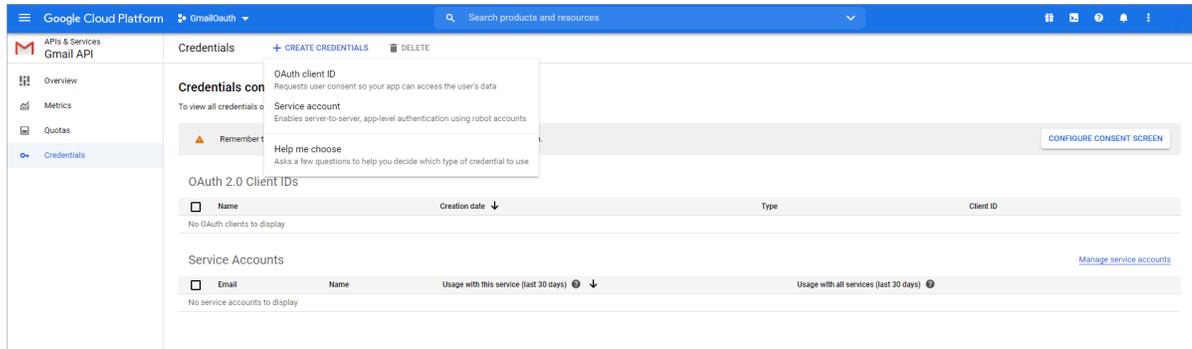
- Under G Suite, click **Gmail API**.
The **Gmail API** page appears.



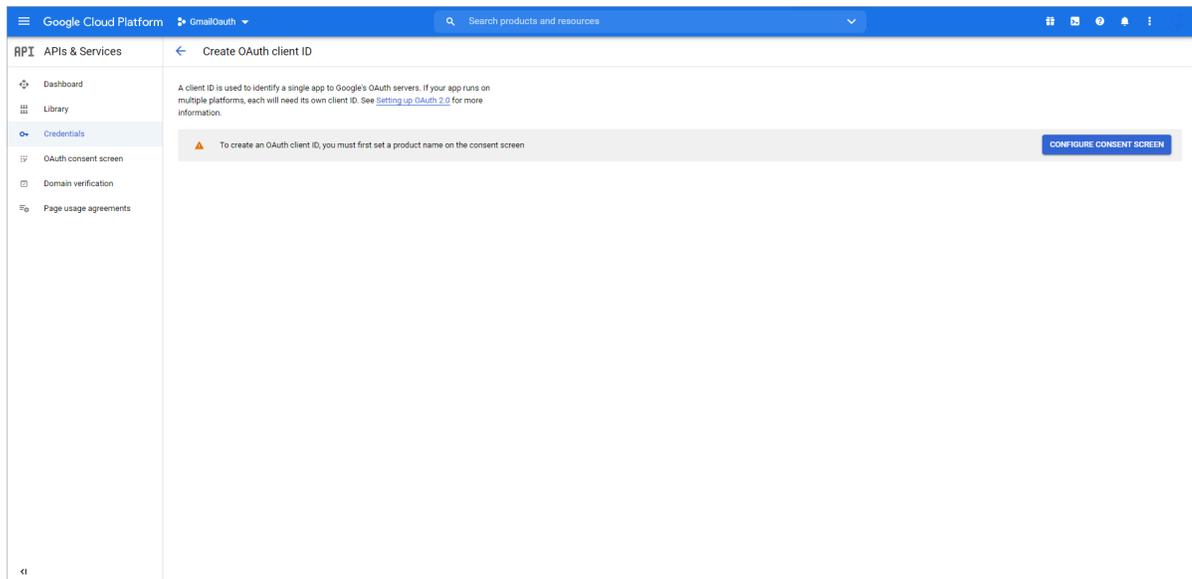
- Click **Enable**.
The **Overview** page appears.



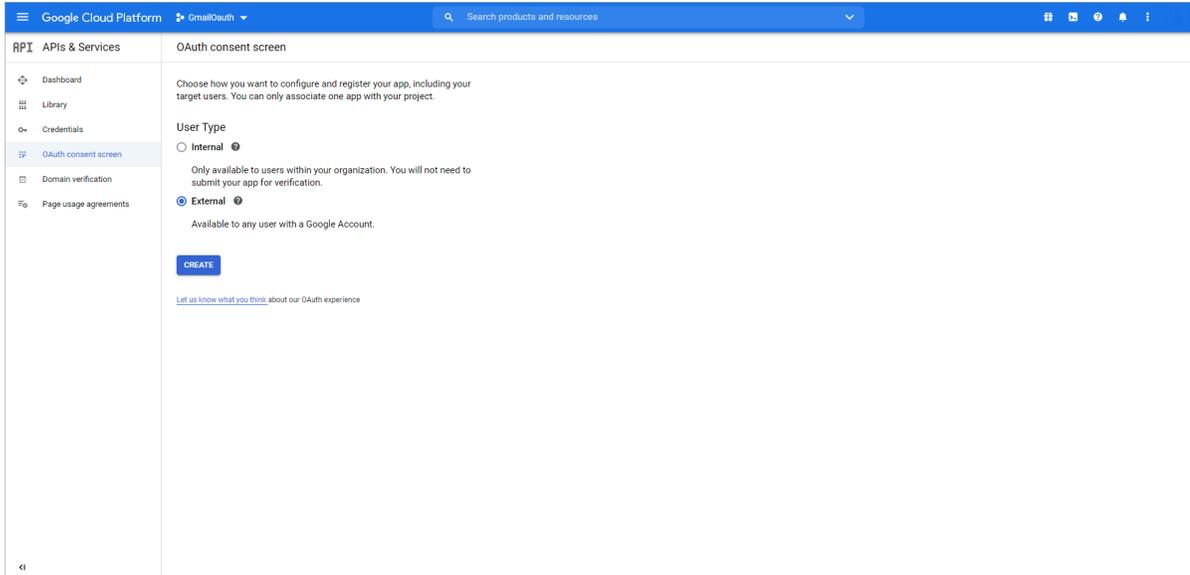
- In the left pane, click **Credentials**.
The **Credentials** page appears.



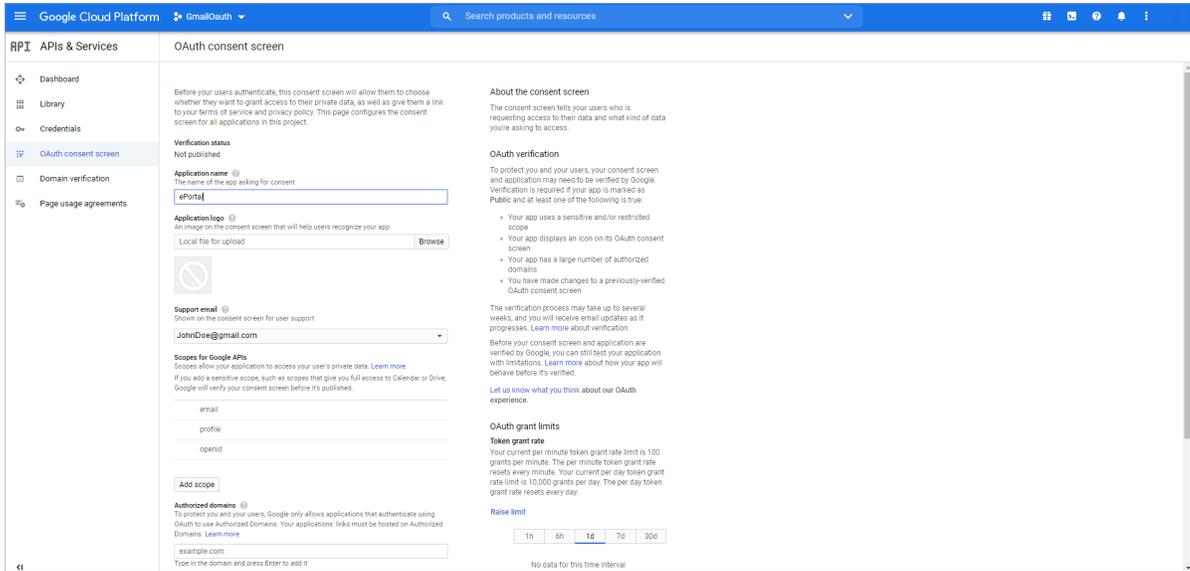
- Click **CREATE CREDENTIALS > OAuth client ID**.
The **Create OAuth client ID** page appears.



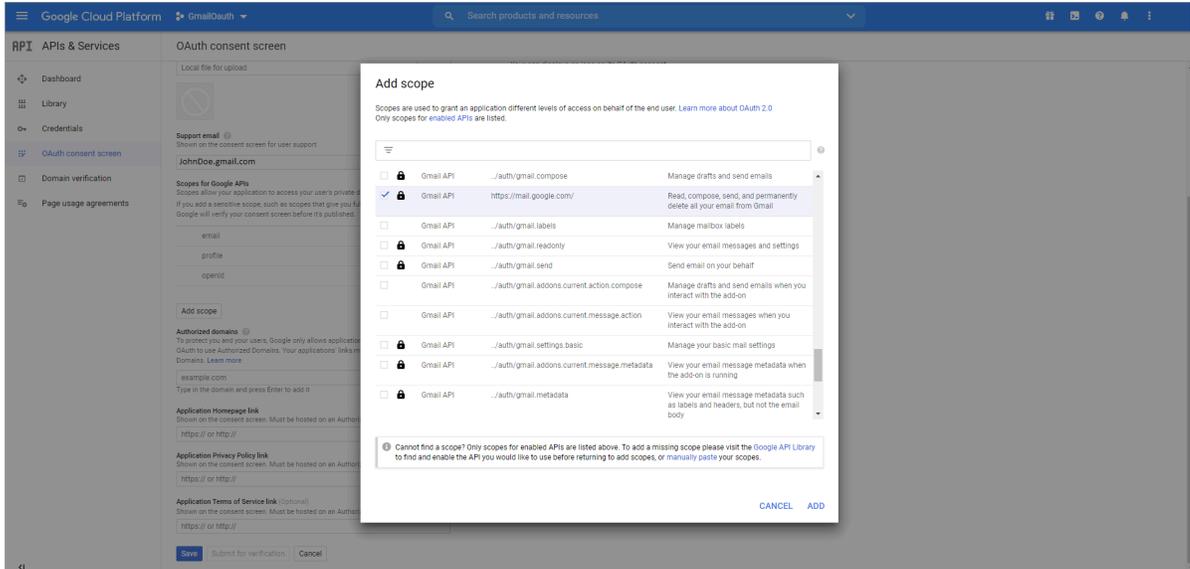
- Click **CONFIGURE CONSENT SCREEN**.
The **OAuth consent screen** page appears.



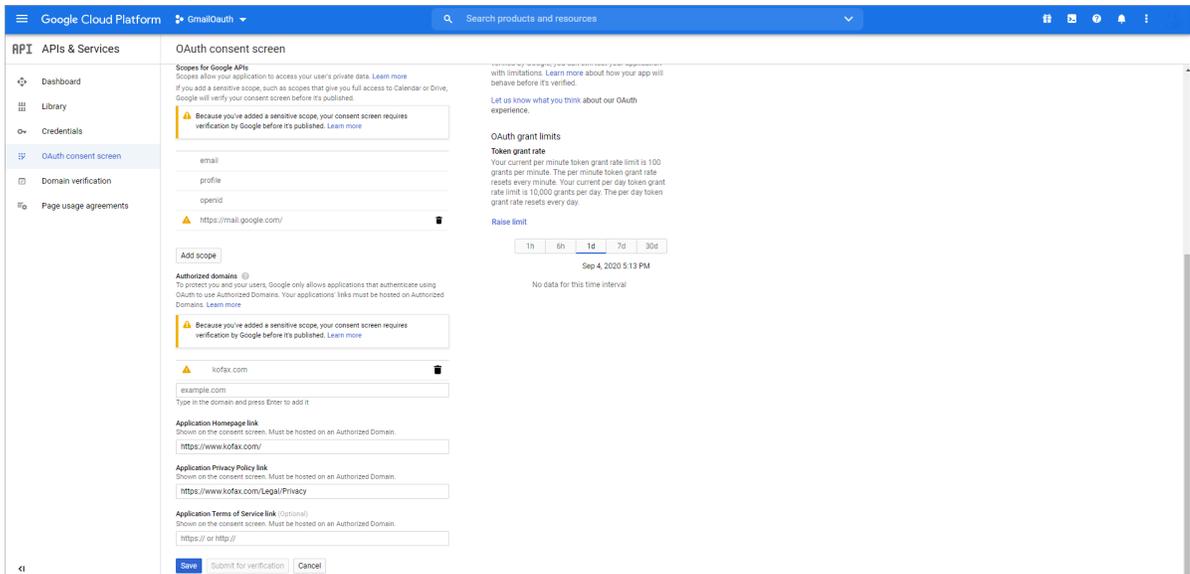
- Under **User Type**, select **External**, and click **CREATE**.
The **OAuth consent screen** page appears.



- In the **Application name** field, enter application name as "ePortal", and click **Add scope**. The **Add scope** Web dialog appears.

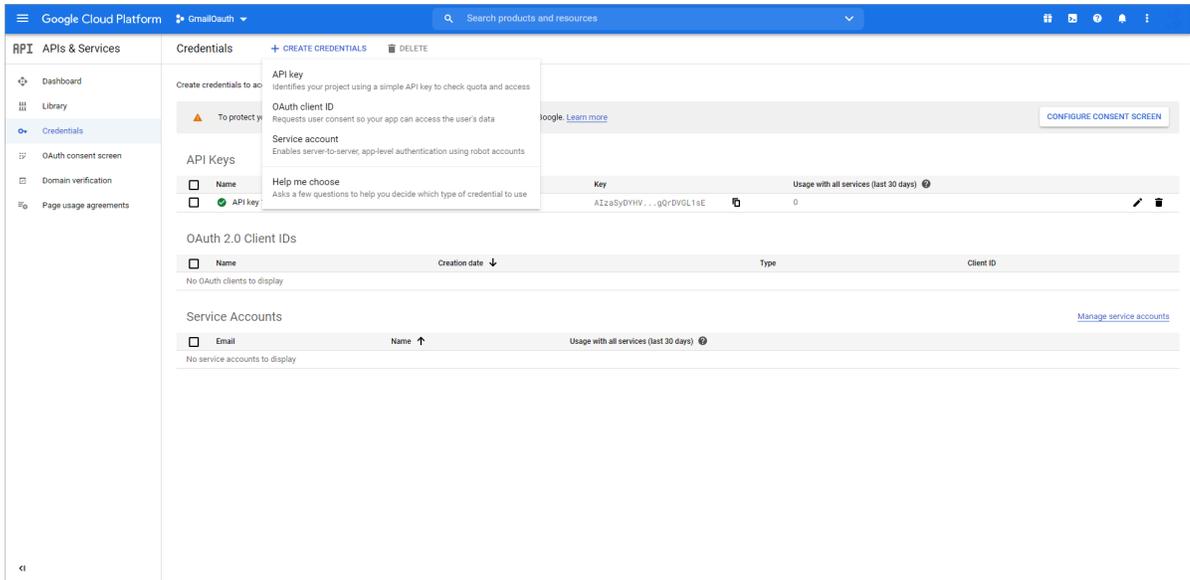


- Select the **Gmail API** option that has **https://mail.google.com/**, and then click **ADD**. You return to the **OAuth consent screen** page.

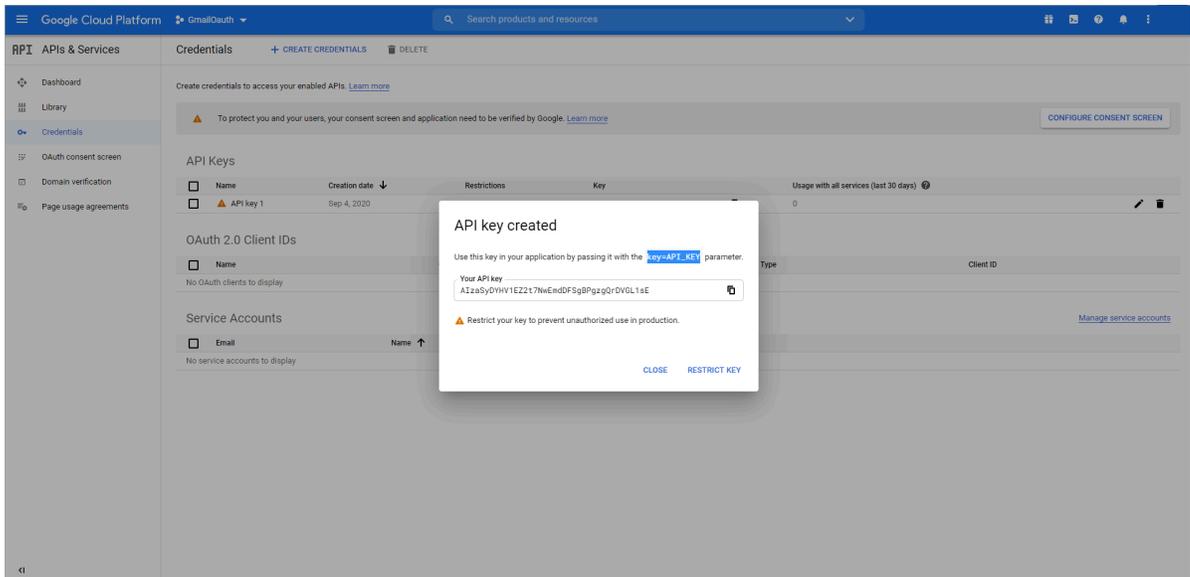


- In the **Authorized domains** field, enter domain name without https or http, and press enter.
- In the **Application Homepage link** field, enter application home page link with http or https.
- In the **Application Privacy Policy link** field, enter application privacy policy link.
- Click **Save**.

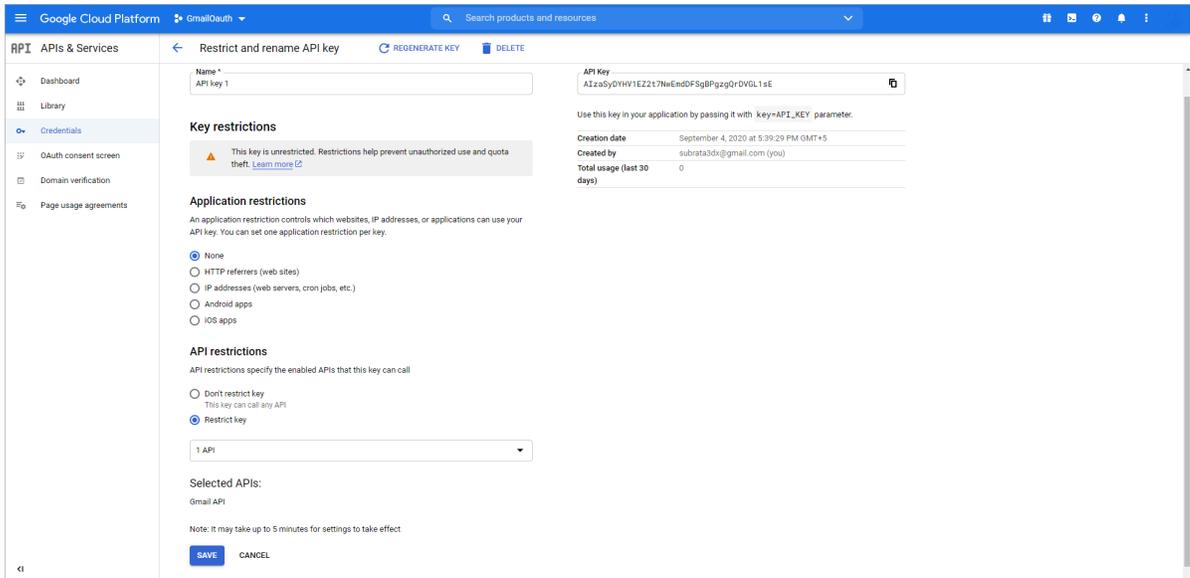
- In the left pane, click **Credentials**.
The **Credentials** page appears.



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



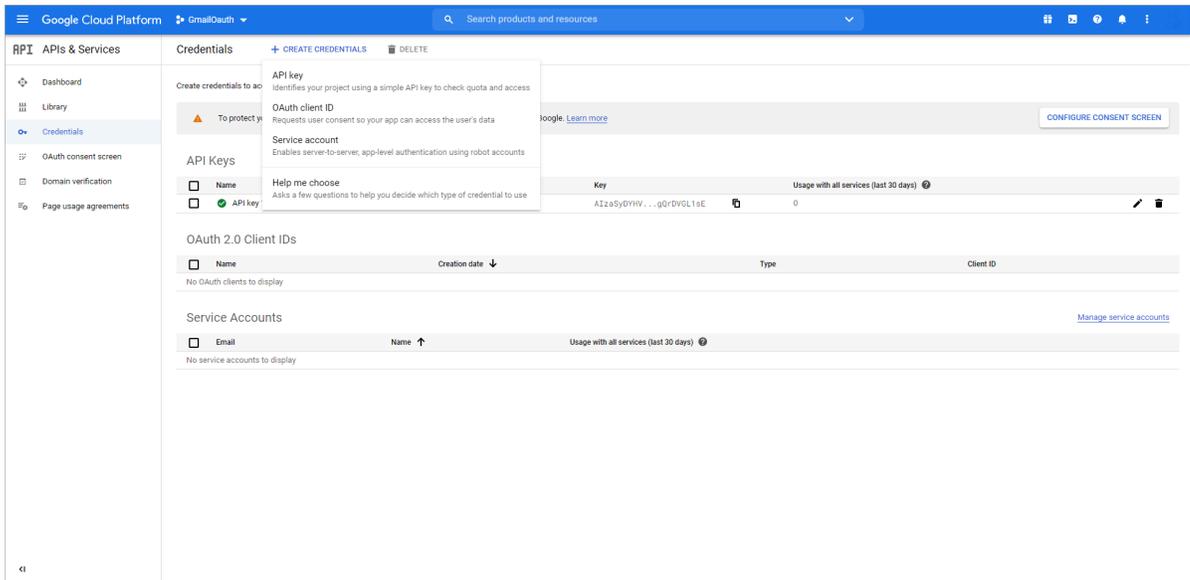
23. Click **RESTRICT KEY**. The **Restrict and rename API key** page appears.



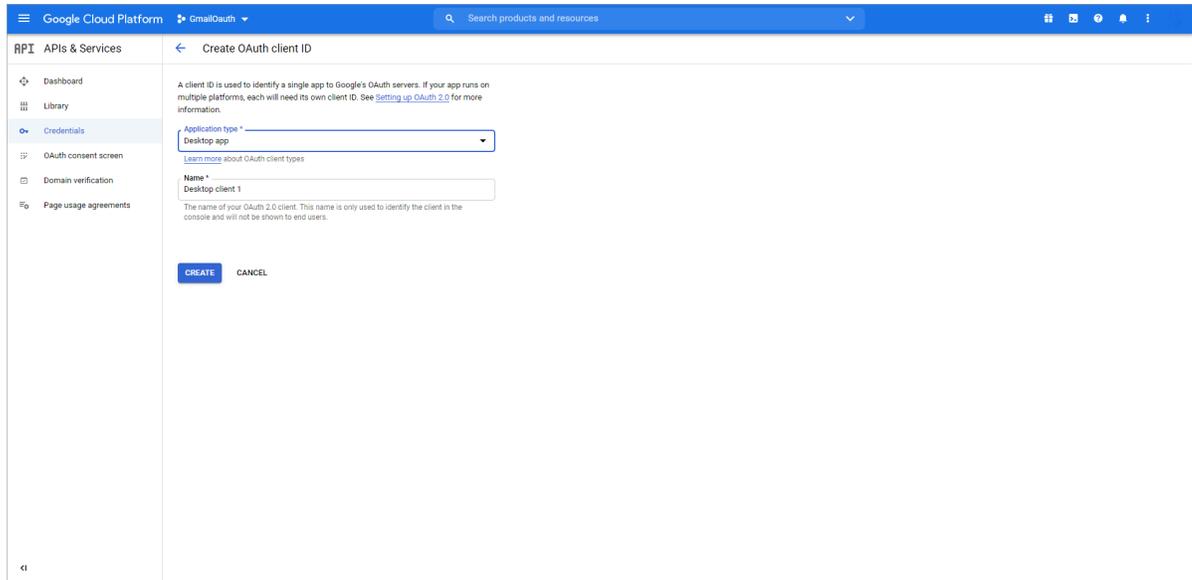
24. Under **Application restrictions**, select **None**.

25. Under **API restrictions**, select **Restrict key**.

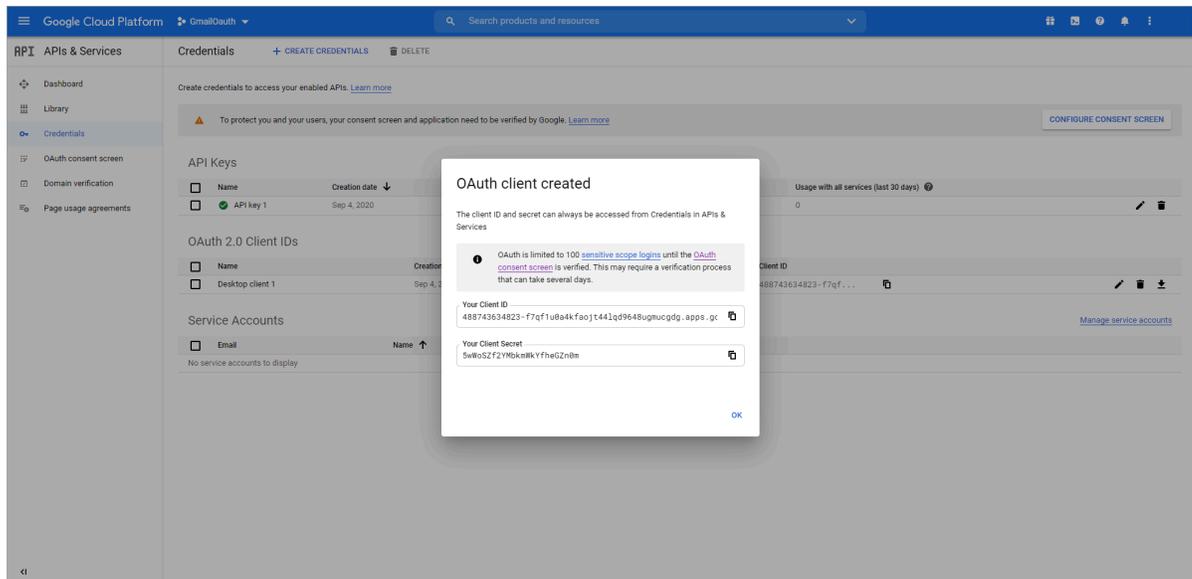
26. Click **Save**.



27. In the left pane, click **Credentials**, and then click **CREATE CREDENTIALS > OAuth client ID**. The **Create OAuth client ID** page appears.

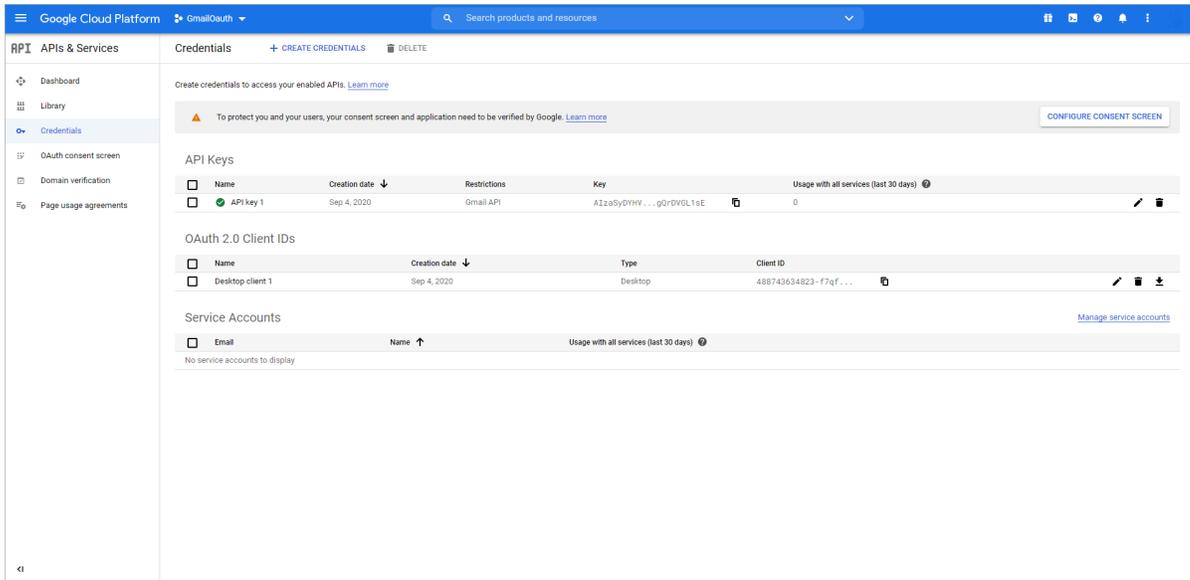


28. From the **Application type** list, select **Desktop app**, and click **CREATE**. The **OAuth client created** Web dialog appears.

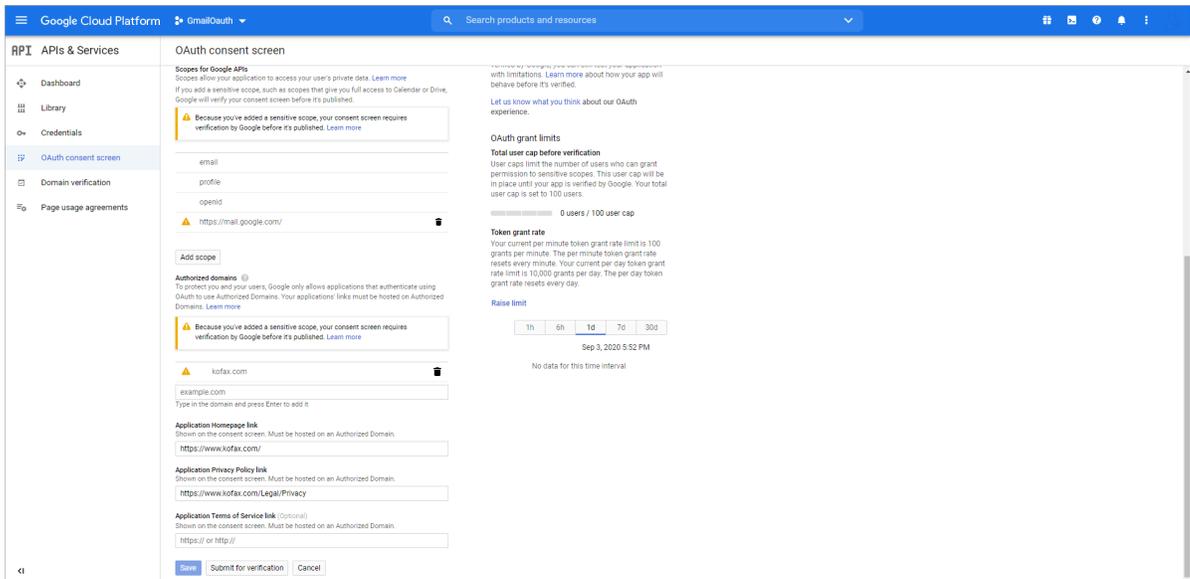


Important Note down your Client ID and Client Secret as you will require them in Application configuration.

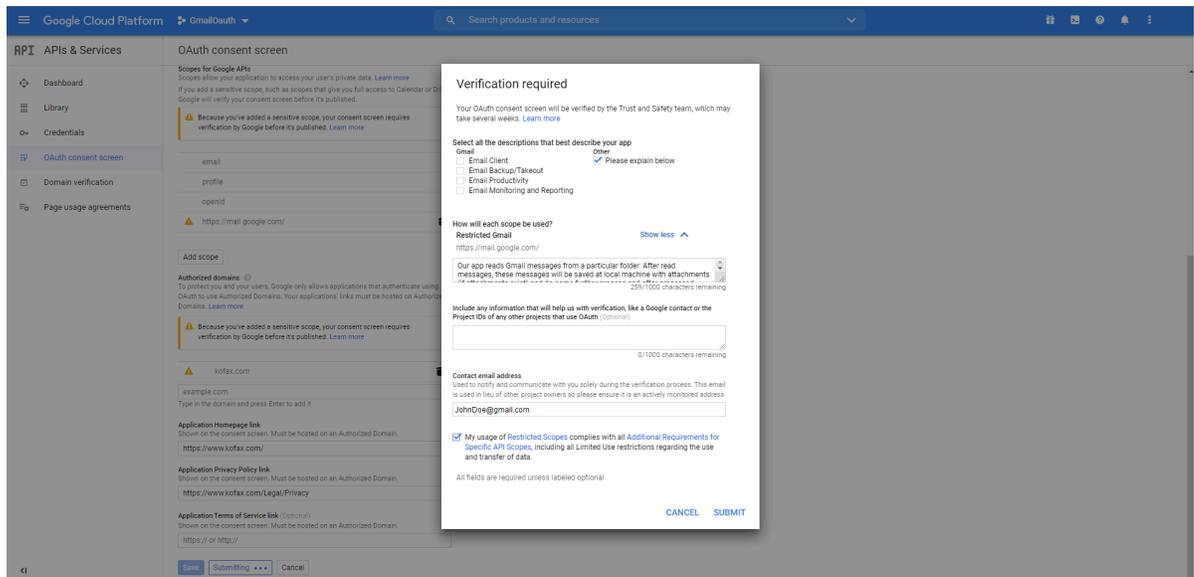
29. Click **OK**. The following page appears.



30. In the left pane, click **OAuth consent screen**. The **OAuth consent screen** appears.



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



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

For example, see the following explanation.

"Our app 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."

33. In the **Contact email address** field, enter your contact email address.
34. Click **Submit**.

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

35. 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="89205223141133cjceblm8f0oimb67jn67raffn5h1.apps.googleusercontent.com"
ClientSecretID="MiVbIAJpGwBxpUjFkxIF8ven">
<MailEncoding>UTF-8</MailEncoding>
<DefaultCharset>UTF-8</DefaultCharset>
<Folders>
  <Folder>ALL MAIL</Folder>
</Folders>
<Subfolder>0</Subfolder>
<SharedMailbox />
<Filter />
<Impersonate Enabled = "false" />
```

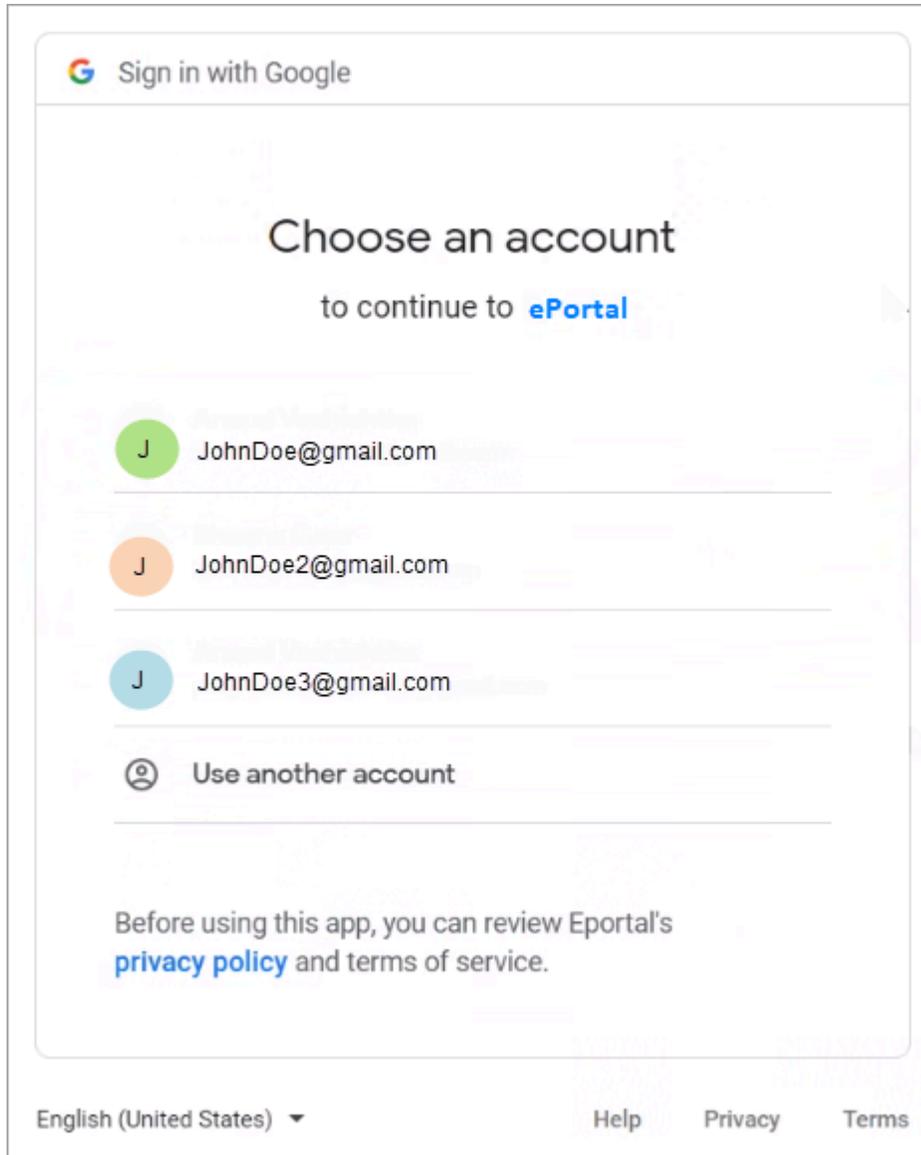
```
</ MailAccount >
```

Note Host URL can be pop.gmail.com.

36. Open C:\ProgramData\TIS\<eFlow6>\AppData\Server\<Application_name>\Setup\EPortal.AppConfig, and paste the copied content under <MailAccounts/> section.
37. Change the Id, Displayname, UserName, ClientID and ClientSecretID, and then save the file.

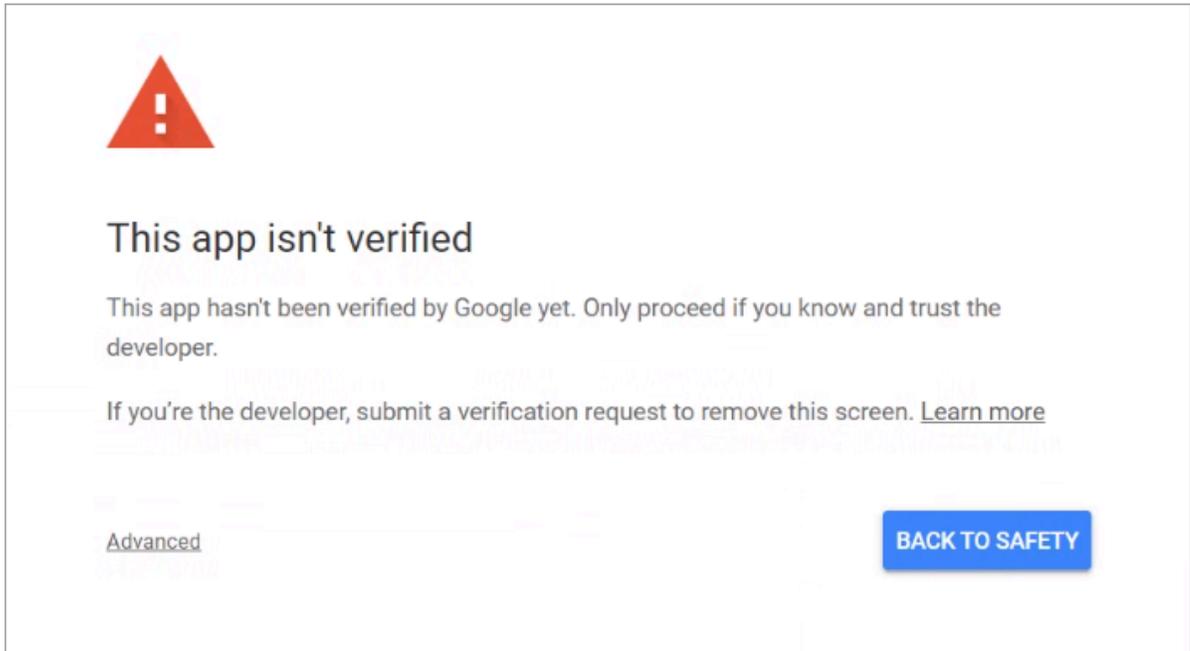
Tip You had noted the Client ID and Client Secret.

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



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

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



40. Since app is not verified, click **Advanced**.
The following page appears.



This app isn't verified

This app hasn't been verified by Google yet. Only proceed if you know and trust the developer.

If you're the developer, submit a verification request to remove this screen. [Learn more](#)

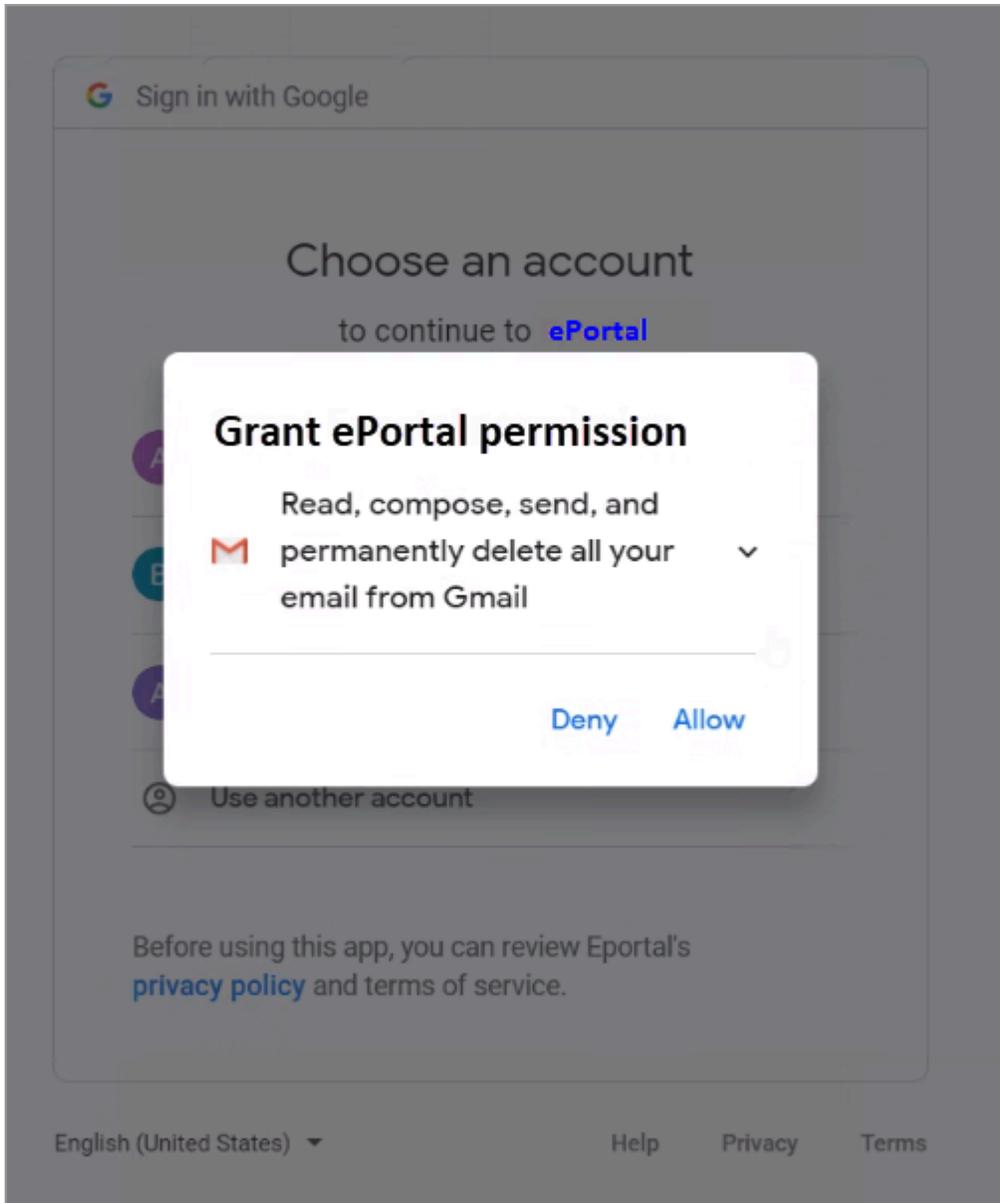
[Hide Advanced](#) [BACK TO SAFETY](#)

Google hasn't reviewed this app yet and can't confirm it's authentic. Unverified apps may pose a threat to your personal data. [Learn more](#)

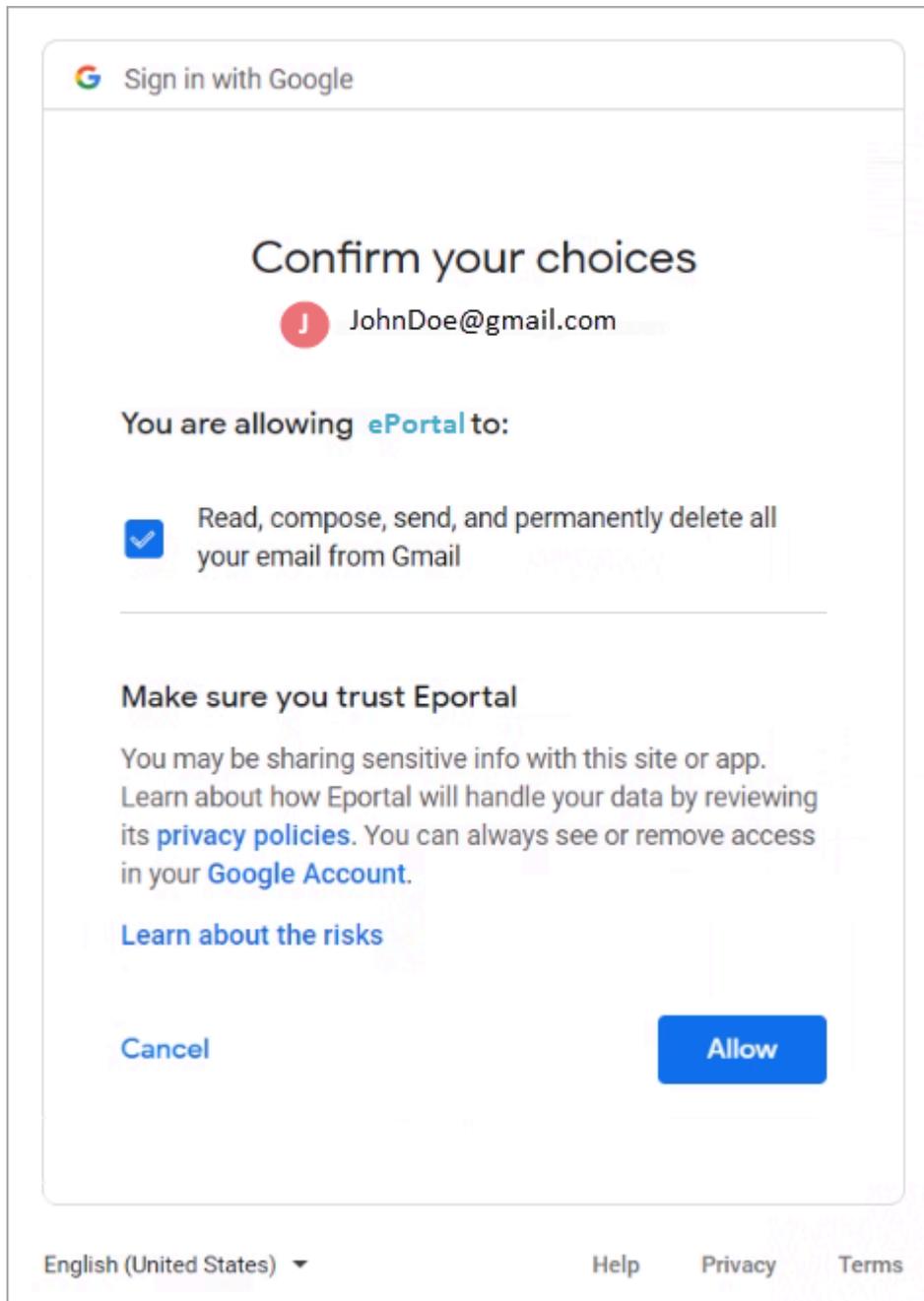
[Go to ePortal \(unsafe\)](#)

41. Click **Go to ePortal (unsafe)**.

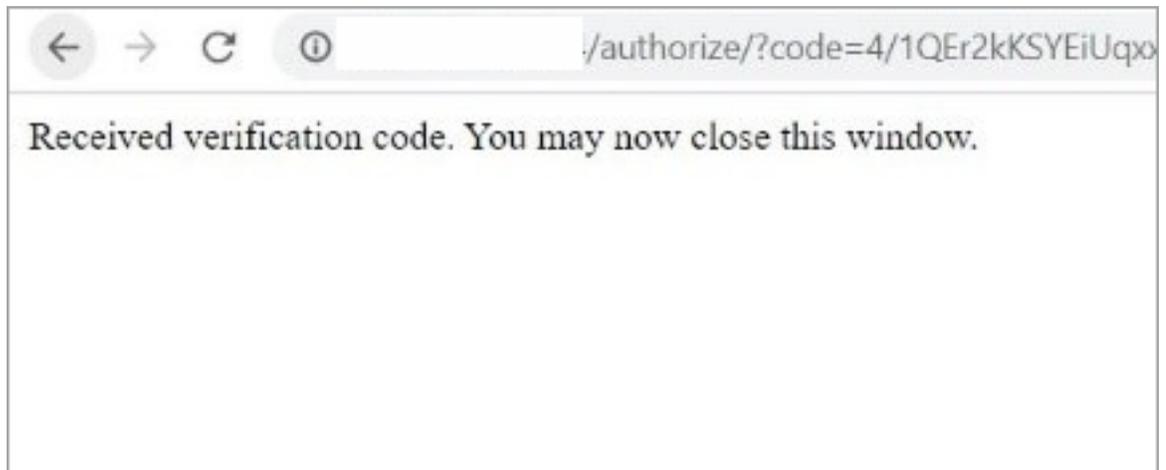
The **Grant ePortal permission** Web dialog appears.



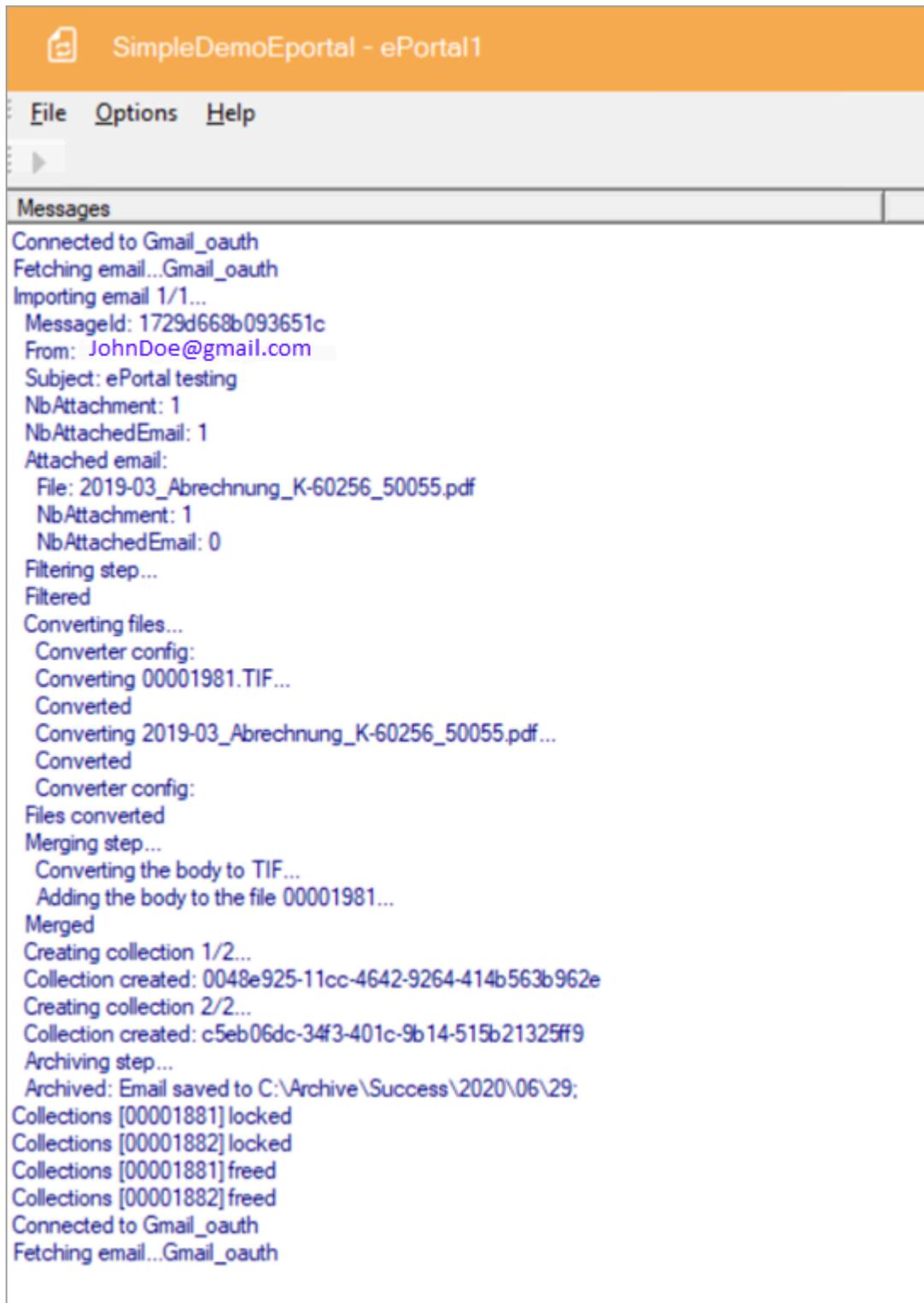
42. Click **Allow**. The **Confirm your choices** page appears.



43. Click **Allow**. The following page appears.



44. After accepting the permission, **ePortal Manual station** will start to fetch the Gmail messages from the configured folder.



IMAP connector

The IMAP 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 it or move it.

Unsynchronized mode

Depending on the archive configuration, unsynchronized mode deletes, moves, or sets as read the emails in the mailbox after they have been imported into the eFlow workflow.

By default, ePortal sets imported files as READ, so when ePortal retrieves emails with the IMAP filter UNSEEN, it will import only new emails.

Synchronized mode

Not required for the IMAP protocol.

Encoding

ePortal supports the following character sets:

- ASCII
- UTF-7
- UTF-8 for
 - BigEndianUnicode
 - Unicode
- UTF-32

You can add the values to the configuration file in the connector <MailEncoding> section.

IMAP Folder

By default, emails are retrieved from the Inbox folder, but you can use any other folder.

You can also move emails to another IMAP folder during the Archiving stage.

Filter

By default, the filter is set to UNSEEN, which means that the connector only retrieves unread emails. You can use any IMAP search key to specify which emails should be retrieved. For example:

Purpose	Search key
Get all emails with either "INVOICE" or "IMPORTANT" in the subject.	OR (SUBJECT \ "INVOICE\") (SUBJECT \ "IMPORTANT \")
Get all emails since 8 th August 2015	SINCE \ "8-Aug-2015"
Get all unread emails	UNSEEN

Purpose	Search key
Get all emails that were not answered	NOT ANSWERED
Get all unread emails with size > 10 KB	UNSEEN LARGER 10200

Configuration

```
<MailAccount Id="account2gmailIMAPSSL" DisplayName="My Gmail IMAP SSL=YES profile"
Host="imap.googlemail.com" Port="993" SSL="true" UserName="XXXX" Password="XXXX"
Protocol="IMAP">
  <Folders>
    <Folder>INBOX</Folder>
  </Folders>
  <Filter>UNSEEN</Filter>
</MailAccount>
```

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 mail account configuration in Eportal.AppConfig.

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 it or move it. For that we use Gmail api. 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 will only import 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 mail account in IMAP_GMAIL protocol in eportal.appconfig file, you need to manually authorize yourself in ePortal station by entering configured mail account credentials and permissions consent.

Scenario 2: When your email account password expires or changes, then you need to reauthorize yourself by opening ePortal station manually.

After that, enable the autorun mode for the ePortal station.

Configuration

Any application that implements OAuth standard to authenticate and authorize its users 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, which is subjected to the individual organization IT policies.

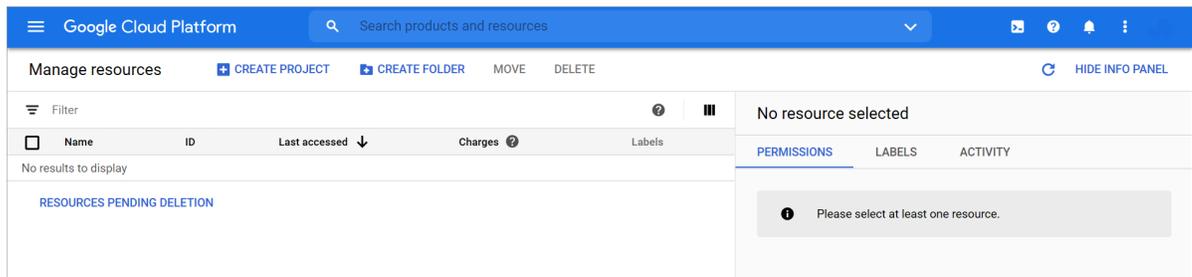
Google cloud configuration for Gmail

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

Note The figures used in the following instructions are taken from Google site, the appearance and user interfaces might change occasionally.

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

The **Google Cloud Platform** main page appears.



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

Google Cloud Platform

New Project

 You have 12 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name * ?

Project ID: gmailoauth-288511. It cannot be changed later. [EDIT](#)

Location * [BROWSE](#)

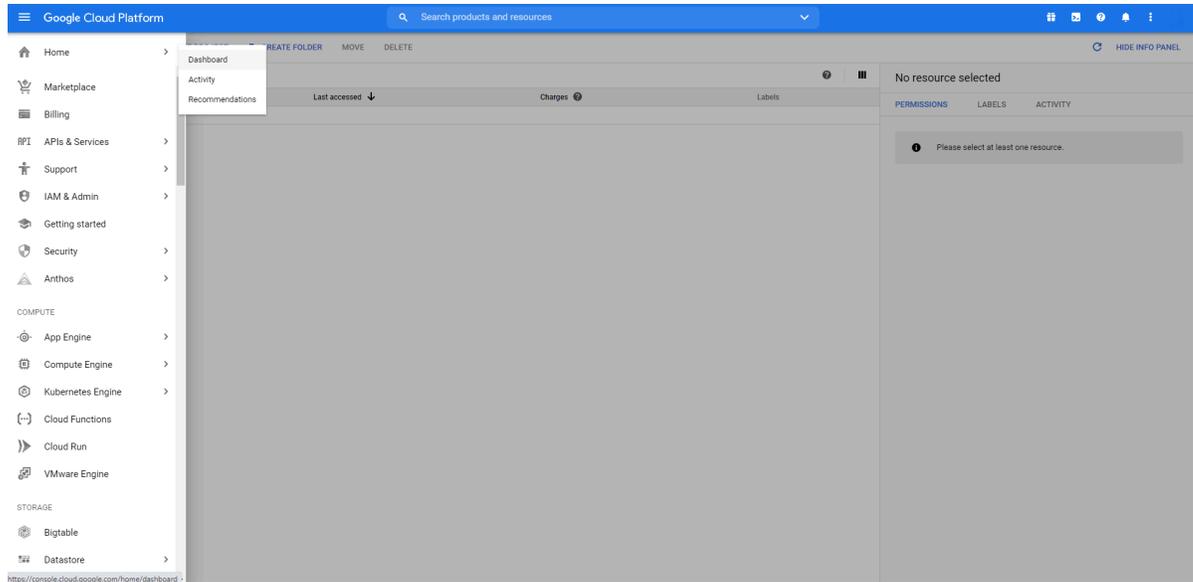
Parent organization or folder

[CREATE](#) [CANCEL](#)

3. In the **Project name *** field, enter a name for the project.
4. In the **Location** field, select location as "No organization".

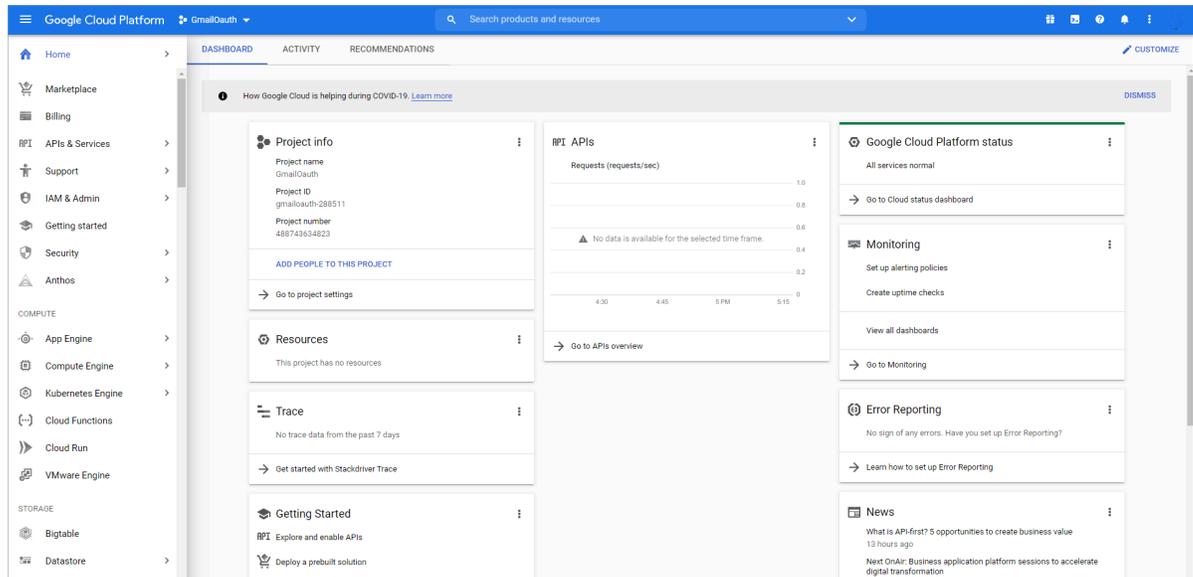
5. Click **CREATE**.

The following page appears.

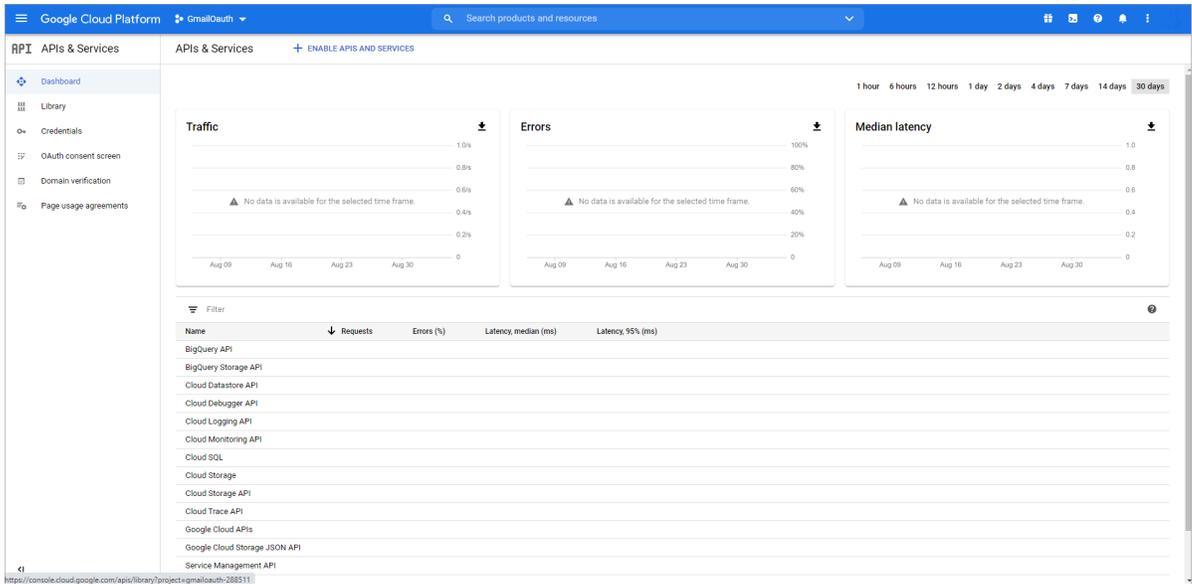


6. In the left pane, select **Home > Dashboard**.

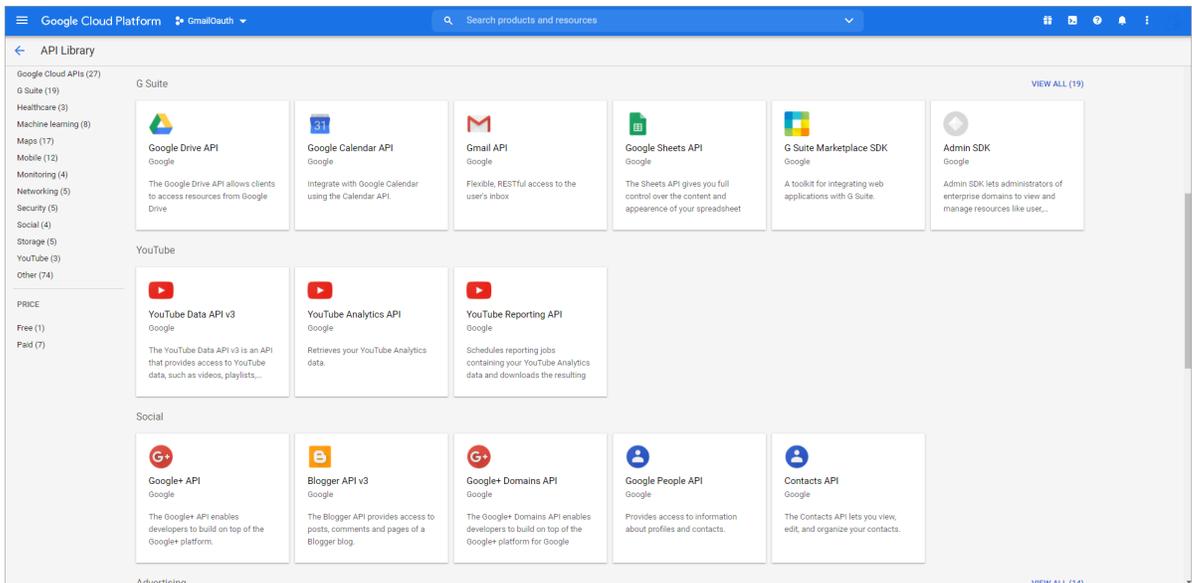
The **Dashboard** page appears.



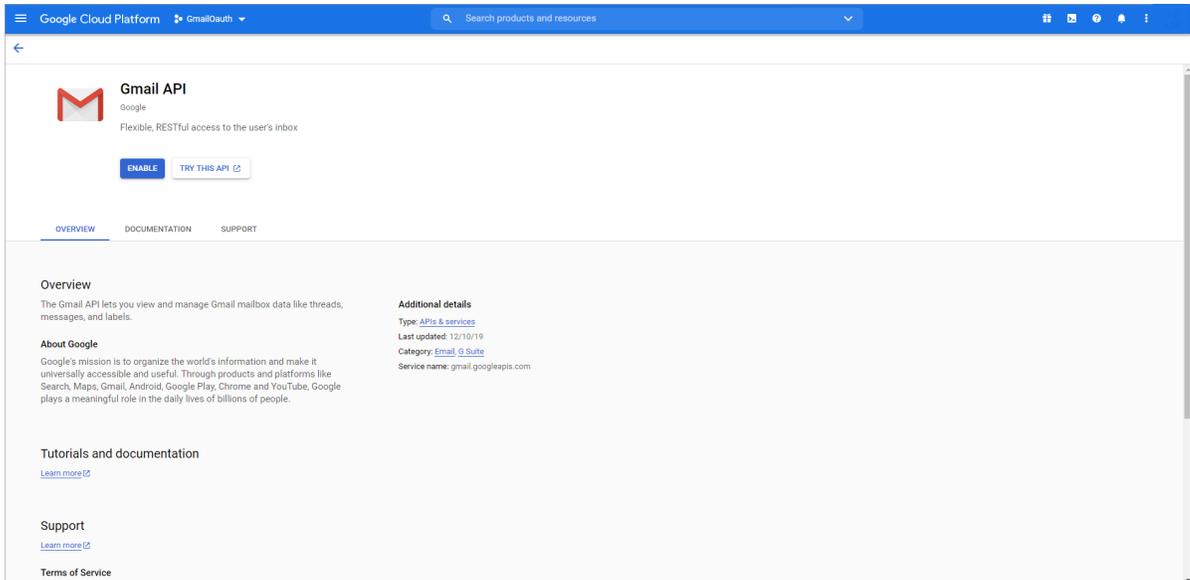
- Under **Getting Started**, click **Explore and enable APIs**.
The **APIs & Services** page appears.



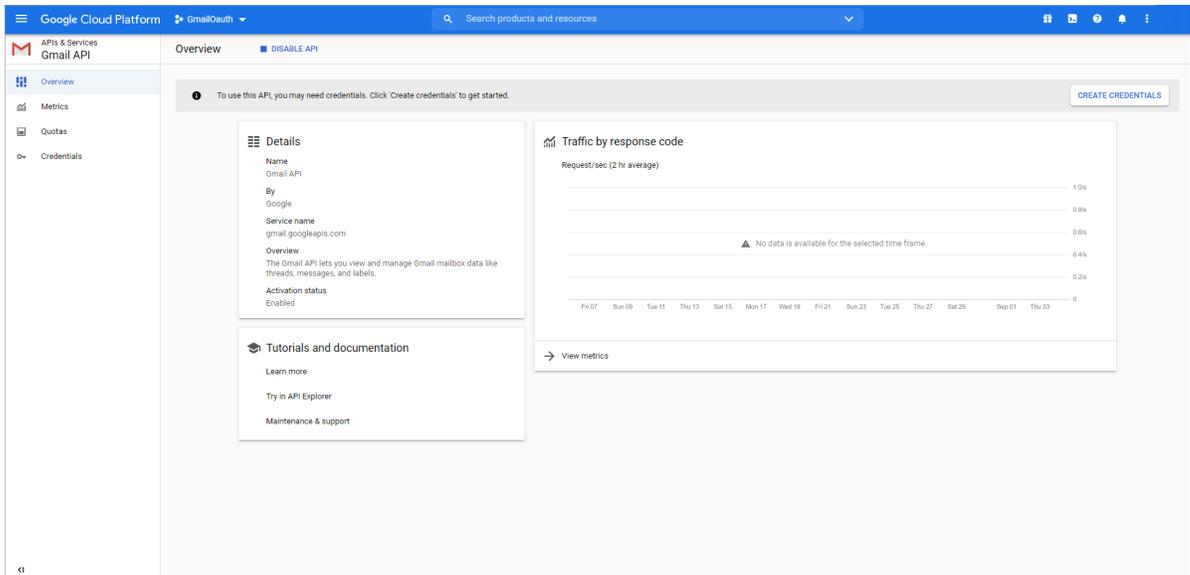
- In the left pane, click **Library**.
The **API Library** page appears.



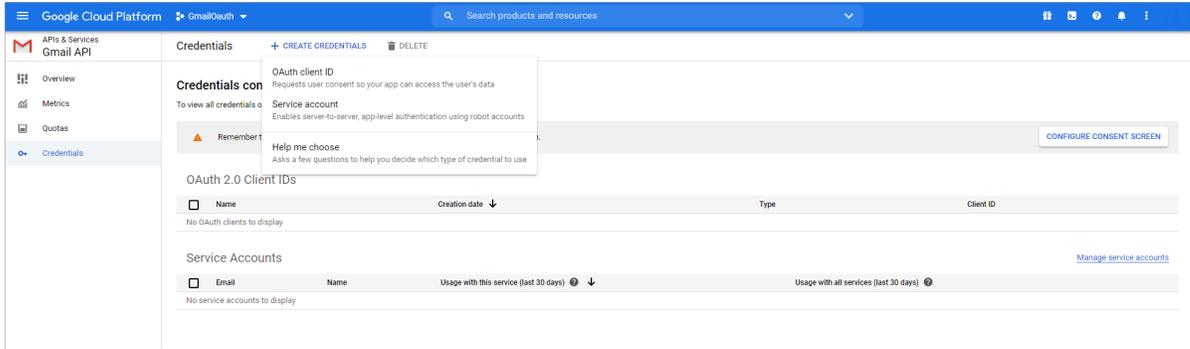
- 9. Under G Suite, click **Gmail API**.
The **Gmail API** page appears.



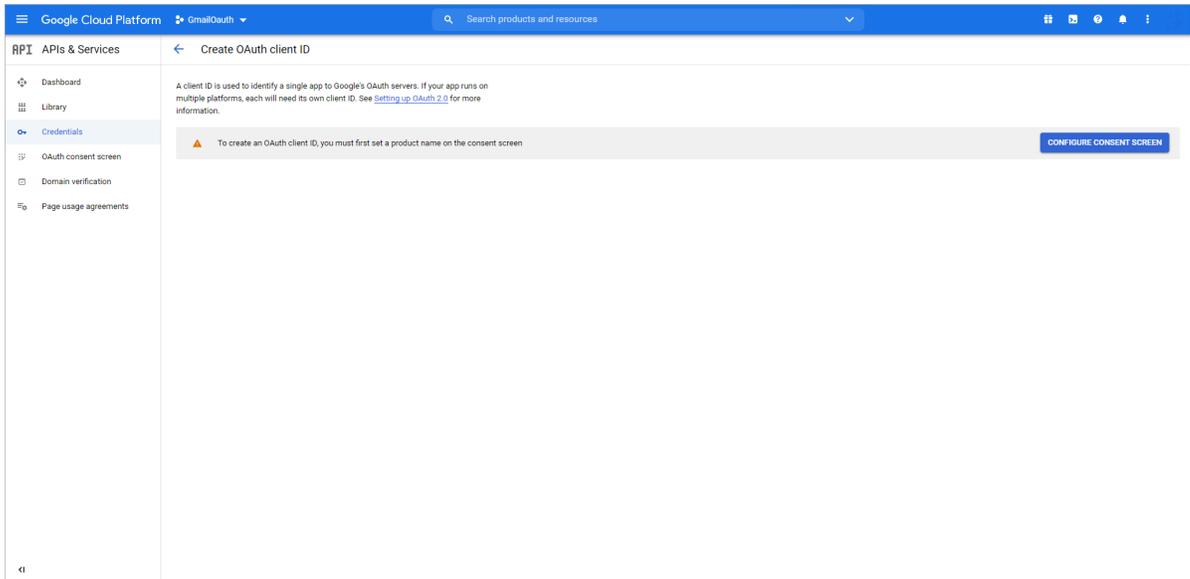
- 10. Click **Enable**.
The **Overview** page appears.



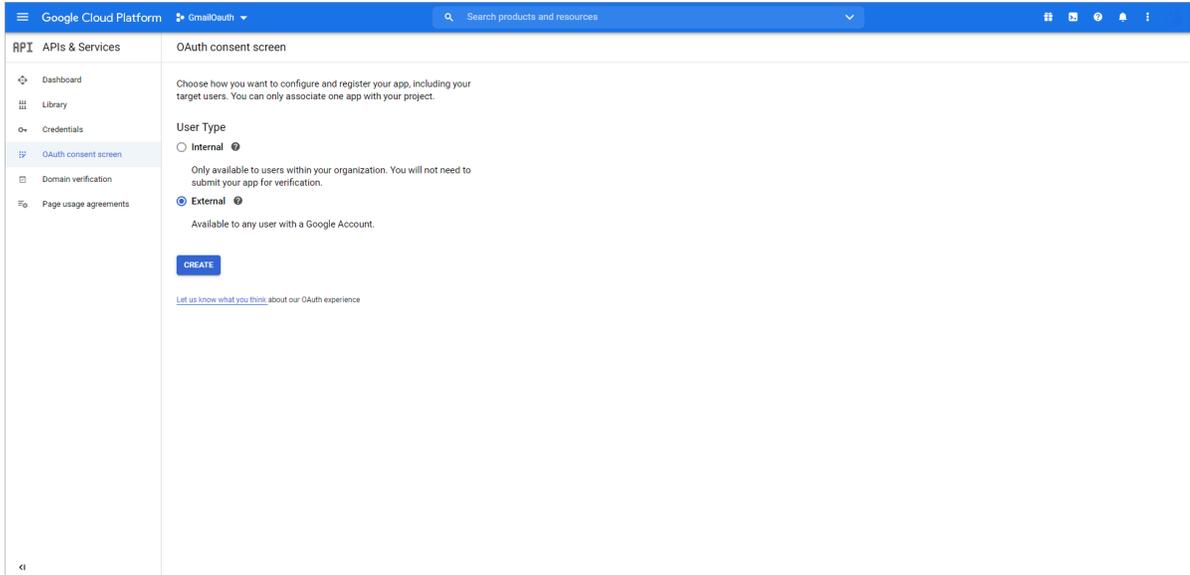
- 11. In the left pane, click **Credentials**.
The **Credentials** page appears.



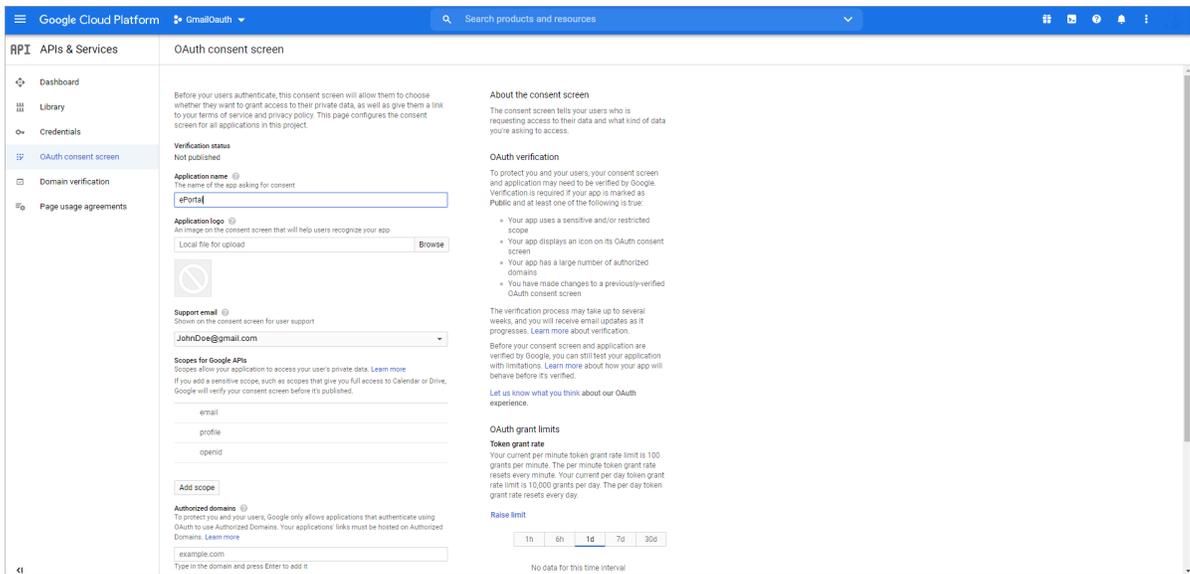
- 12. Click **CREATE CREDENTIALS > OAuth client ID**.
The **Create OAuth client ID** page appears.



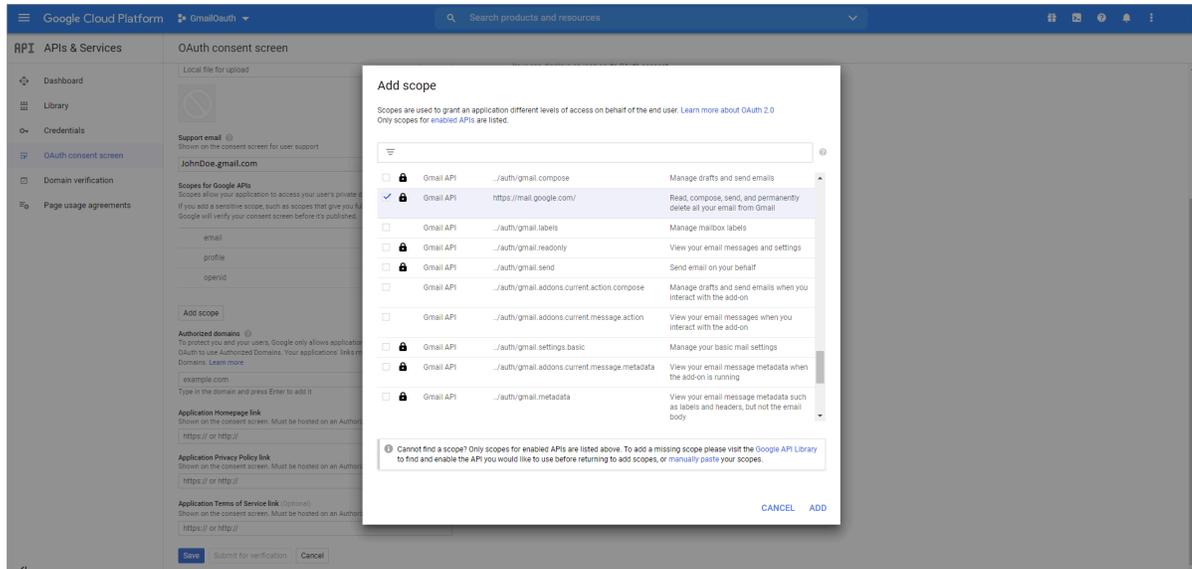
- Click **CONFIGURE CONSENT SCREEN**.
The **OAuth consent screen** page appears.



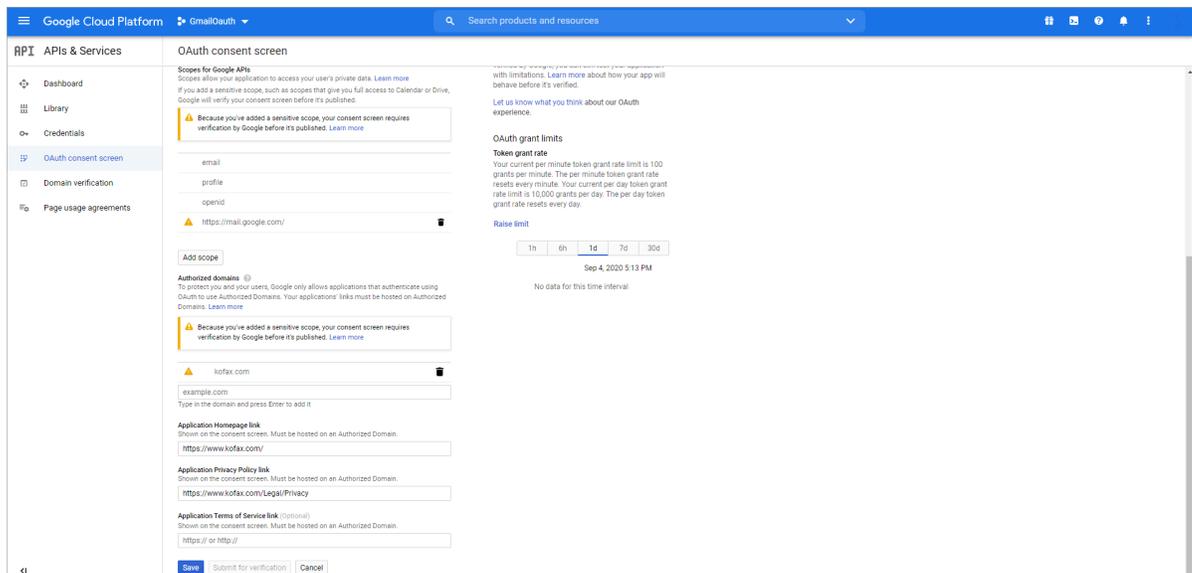
- Under **User Type**, select **External**, and click **CREATE**.
The **OAuth consent screen** page appears.



15. In the **Application name** field, enter application name as "ePortal", and click **Add scope**. The **Add scope** Web dialog appears.

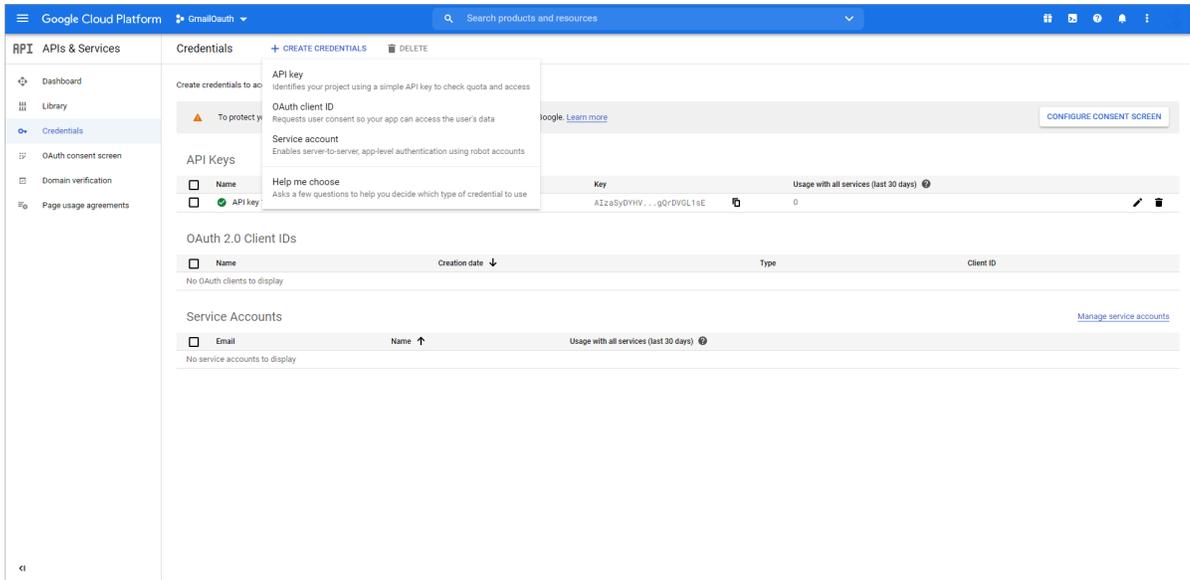


16. Select the **Gmail API** option that has **https://mail.google.com/**, and then click **ADD**. You return to the **OAUTH consent screen** page.

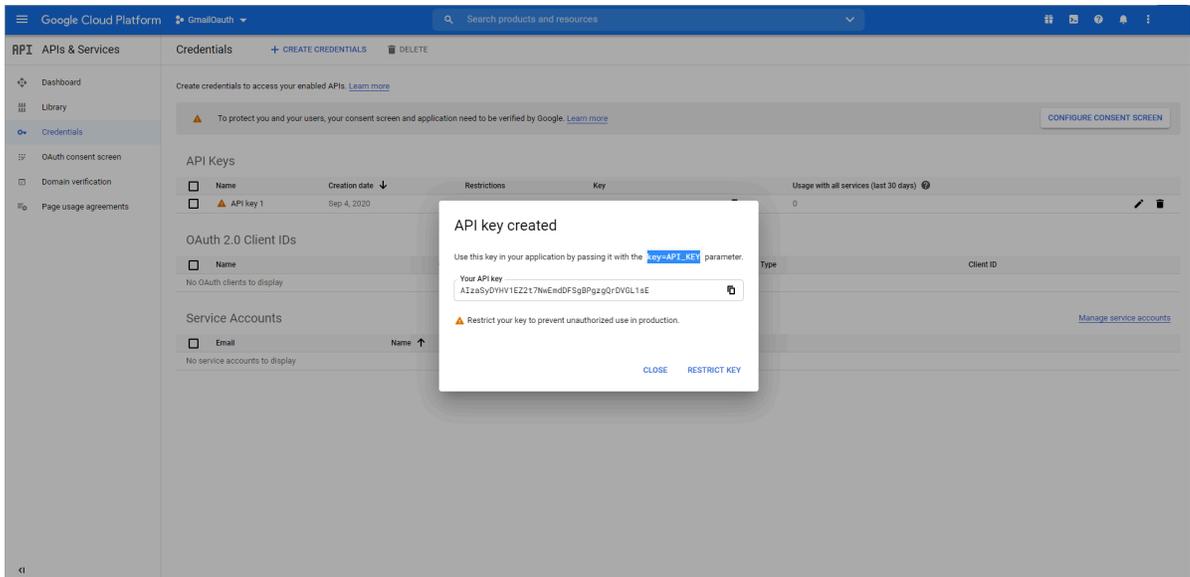


17. In the **Authorized domains** field, enter domain name without https or http, and press enter.
18. In the **Application Homepage link** field, enter application home page link with http or https.
19. In the **Application Privacy Policy link** field, enter application privacy policy link.
20. Click **Save**.

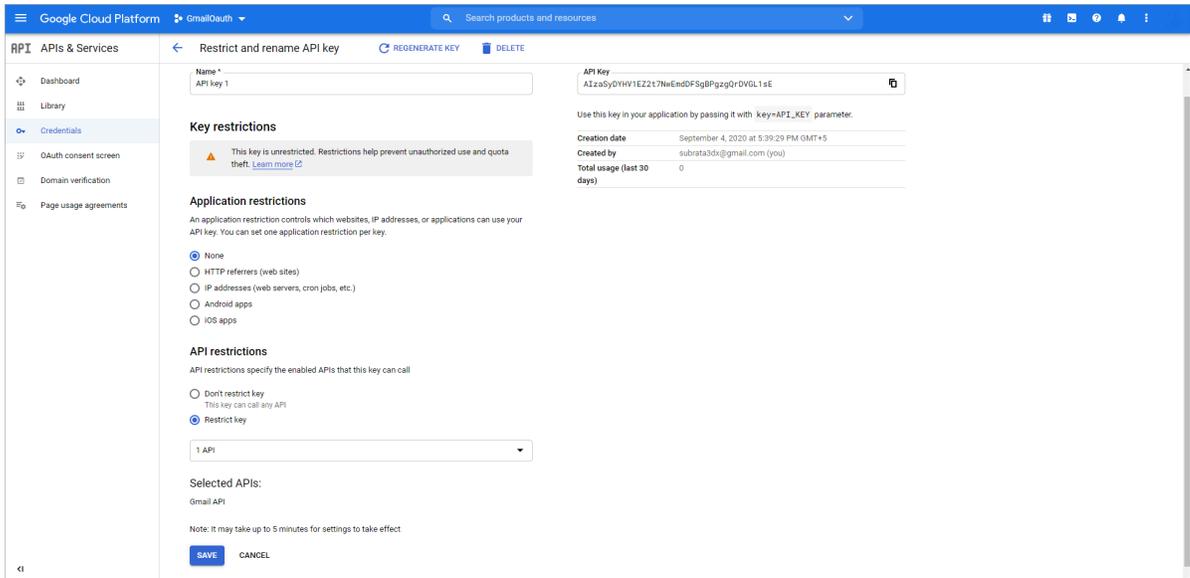
- 21. In the left pane, click **Credentials**.
The **Credentials** page appears.



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



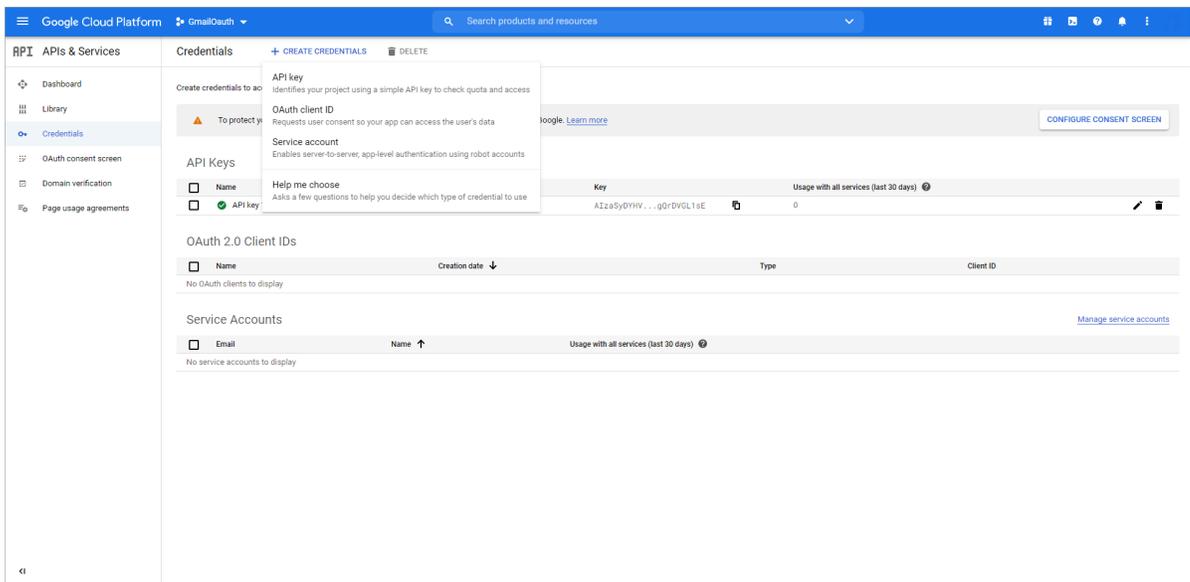
23. Click **RESTRICT KEY**. The **Restrict and rename API key** page appears.



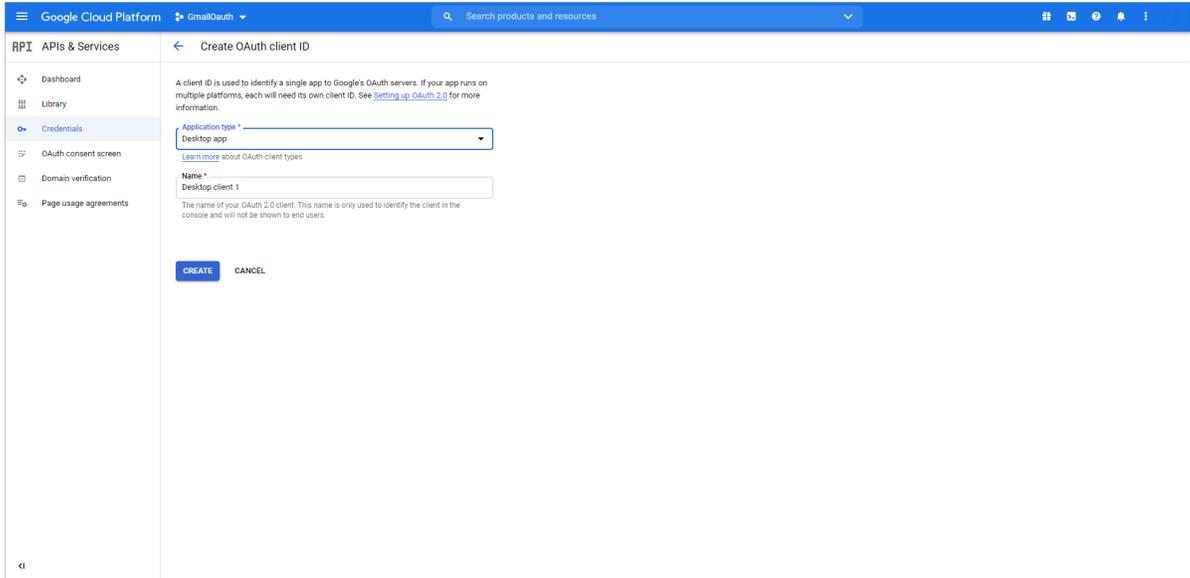
24. Under **Application restrictions**, select **None**.

25. Under **API restrictions**, select **Restrict key**.

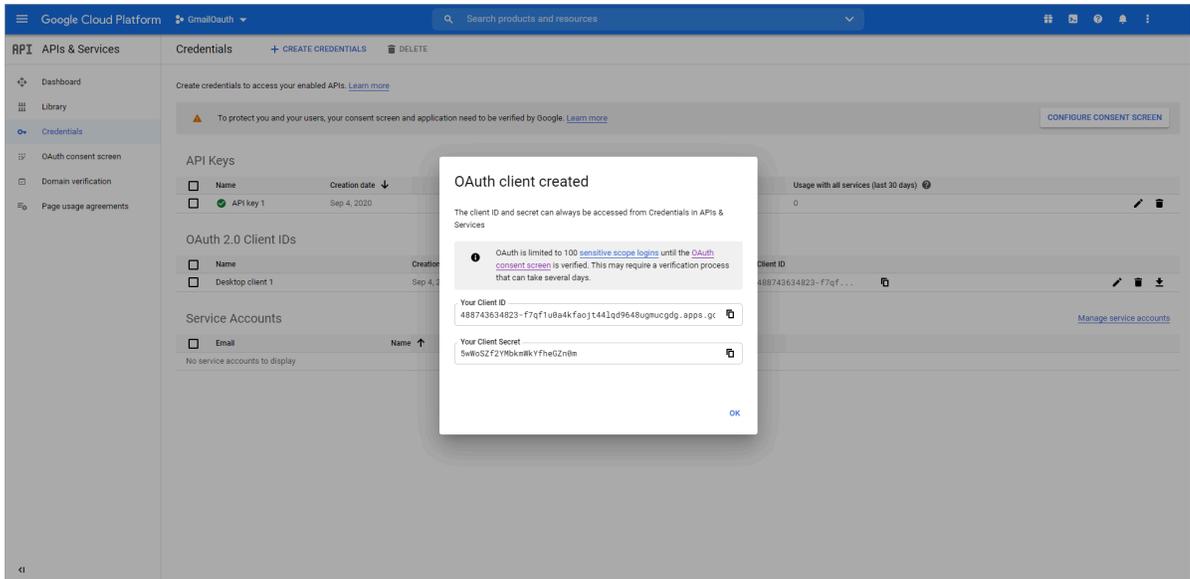
26. Click **Save**.



- In the left pane, click **Credentials**, and then click **CREATE CREDENTIALS > OAuth client ID**. The **Create OAuth client ID** page appears.

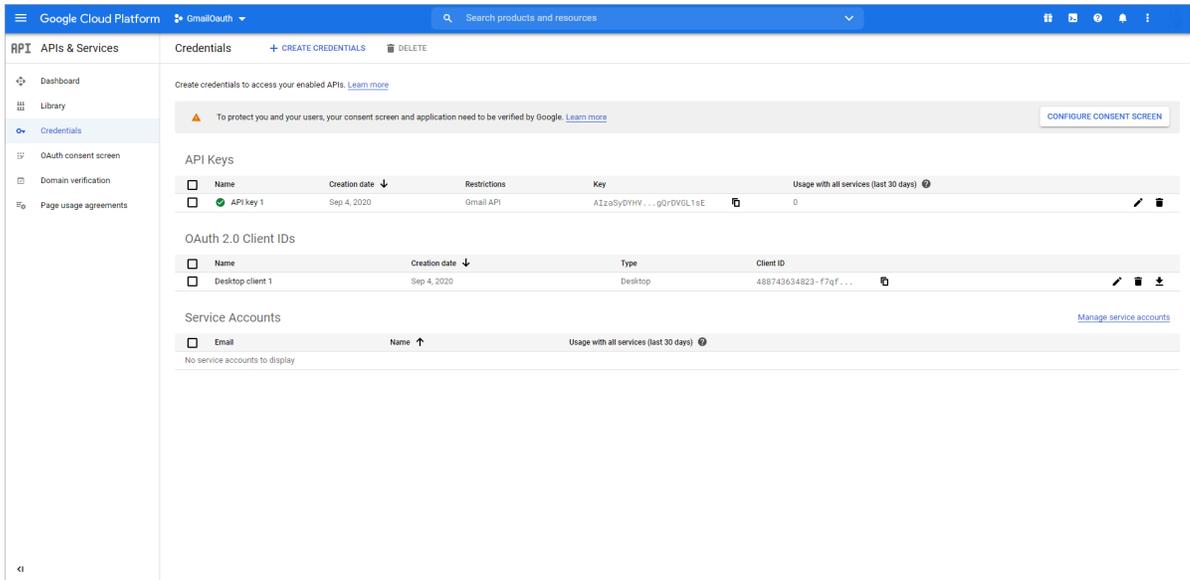


- From the **Application type** list, select **Desktop app**, and click **CREATE**. The **OAuth client created** Web dialog appears.

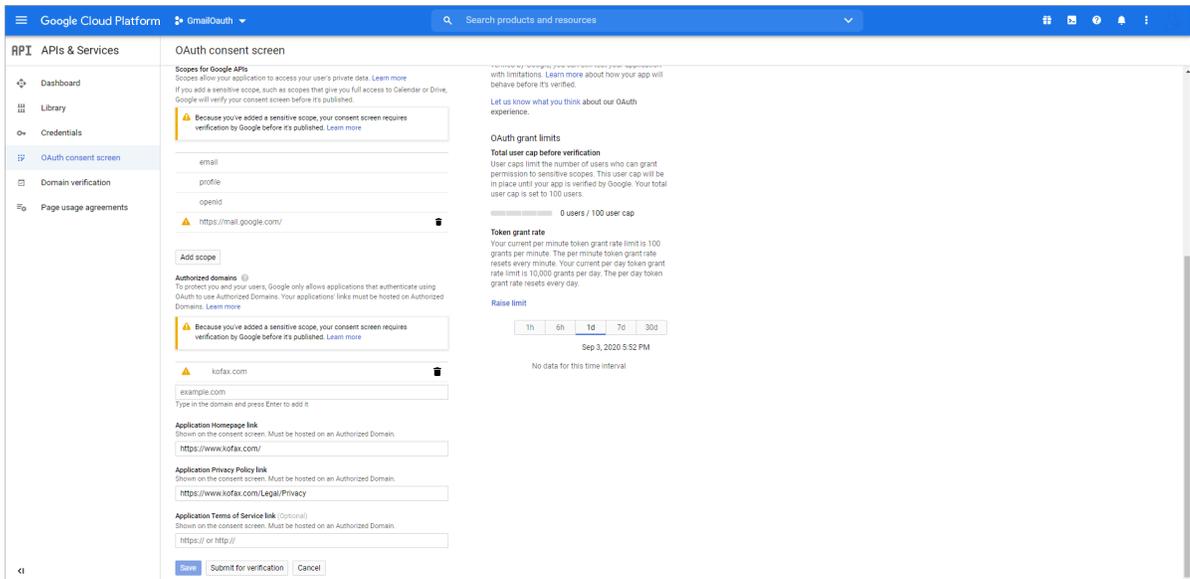


Important Note down your Client ID and Client Secret as you will require them in Application configuration.

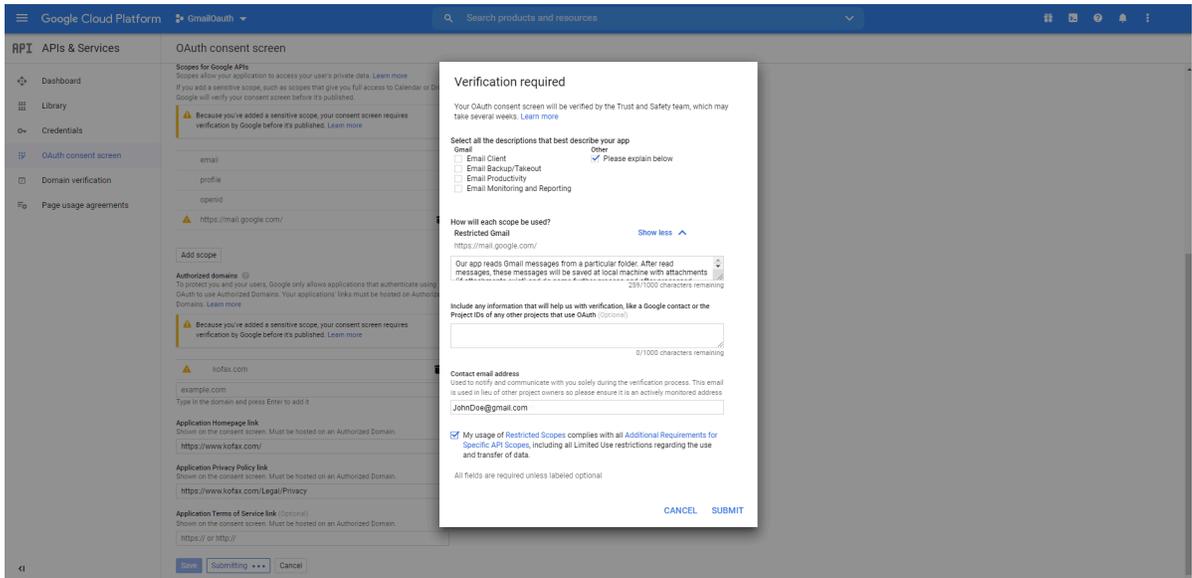
29. Click **OK**. The following page appears.



30. In the left pane, click **OAuth consent screen**. The **OAuth consent screen** appears.



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



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

For example, see the following explanation.

"Our app 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."

33. In the **Contact email address** field, enter your contact email address.
34. Click **Submit**.

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

35. 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-
ulbikaamqkjvhlpkn4ftf575sllqlok.apps.googleusercontent.com"
  ClientSecretID="AkRN0wB-Y0RbqBoLJapsSnV8">
  <MailEncoding>UTF-8</MailEncoding>
  <DefaultCharset>UTF-8</DefaultCharset>
  <Folders>
    <Folder>Eportal_Input</Folder>
  </Folders>
  <Subfolder>0</Subfolder>
  <SharedMailbox />
  <Filter>UNSEEN</Filter>
  <Impersonate Enabled="false" />
```

</MailAccount>

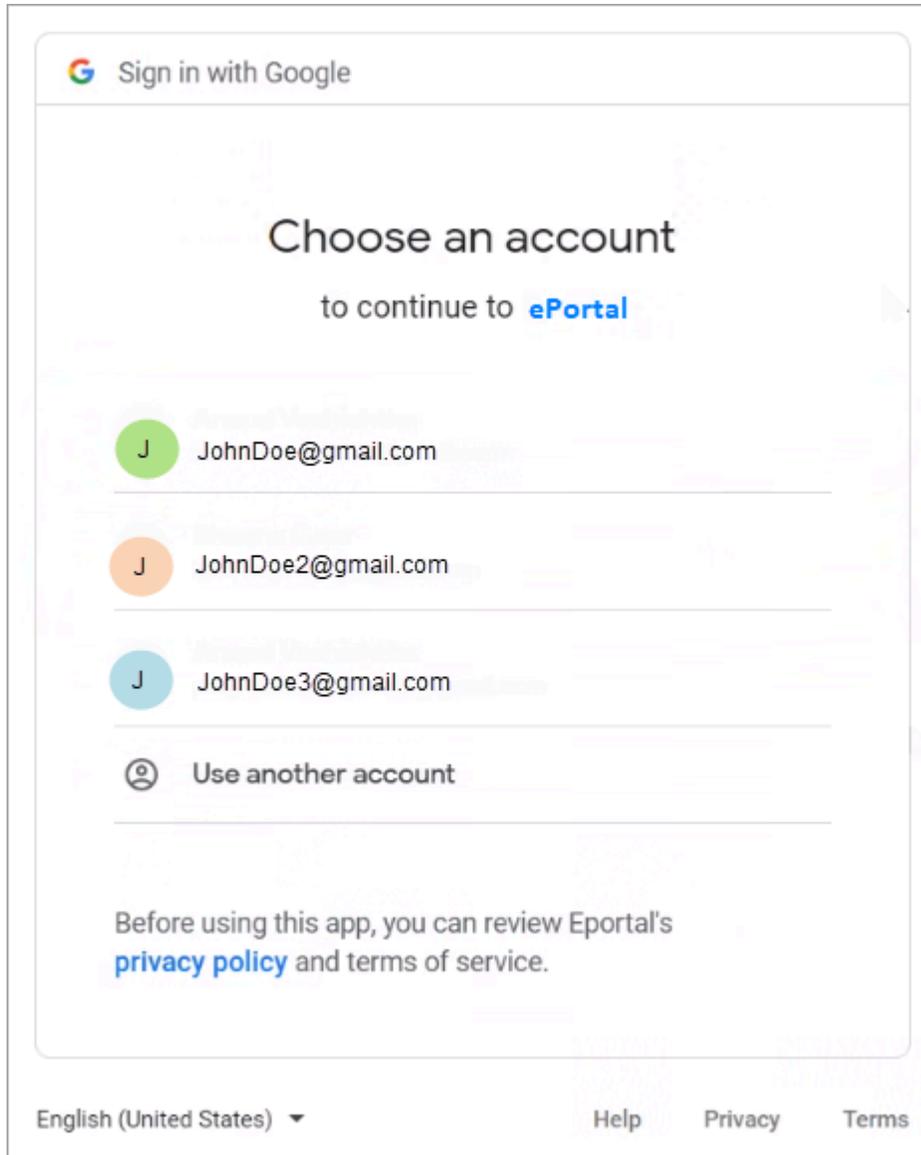
36. Open C:\ProgramData\TIS\<eFlow6>\AppData\Server\<Application_name>\Setup\EPortal.AppConfig, and paste the copied content under <MailAccounts/> section.

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

37. Change UserName, ClientID and ClientSecretID, and save the file.

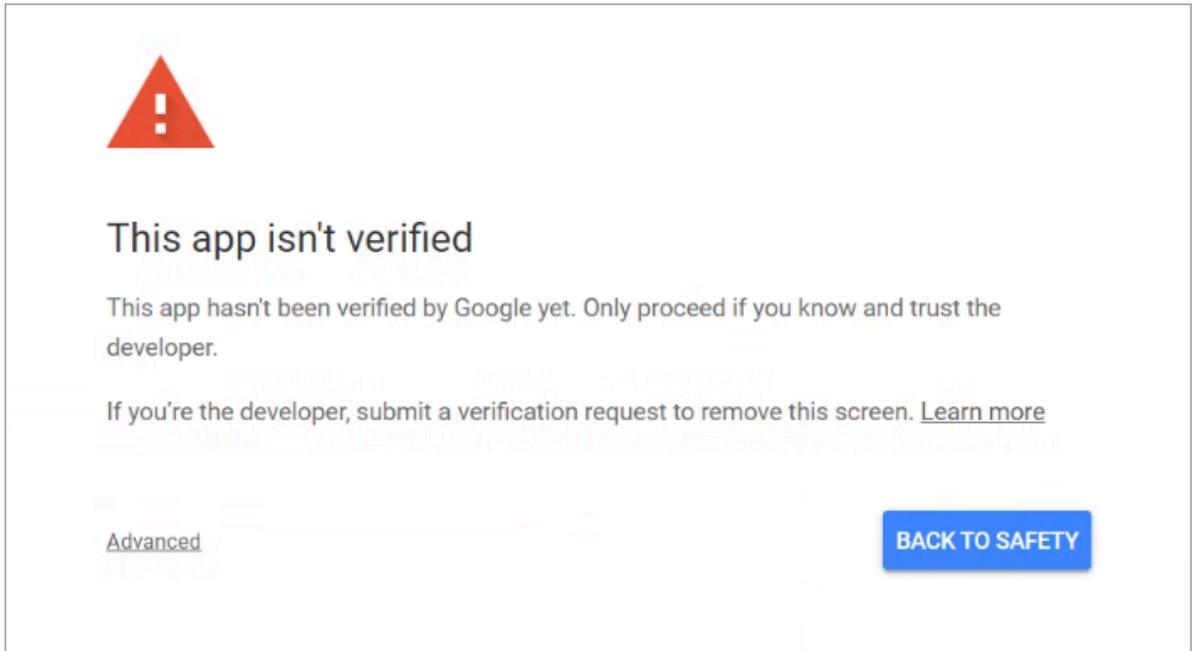
Note Go to #22 for help.

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



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

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



40. Since app is not verified, click **Advanced**.
The following page appears.



This app isn't verified

This app hasn't been verified by Google yet. Only proceed if you know and trust the developer.

If you're the developer, submit a verification request to remove this screen. [Learn more](#)

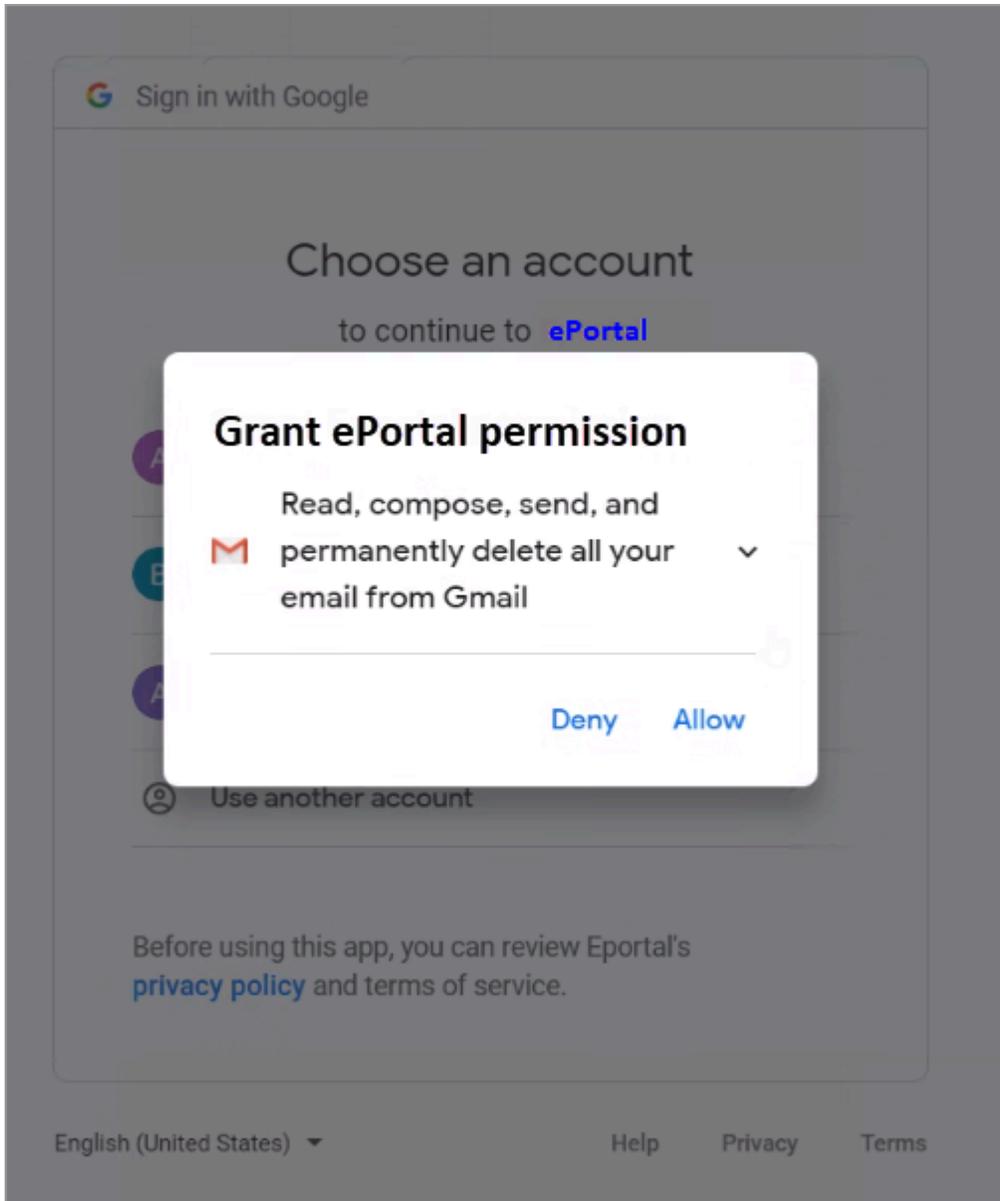
[Hide Advanced](#) [BACK TO SAFETY](#)

Google hasn't reviewed this app yet and can't confirm it's authentic. Unverified apps may pose a threat to your personal data. [Learn more](#)

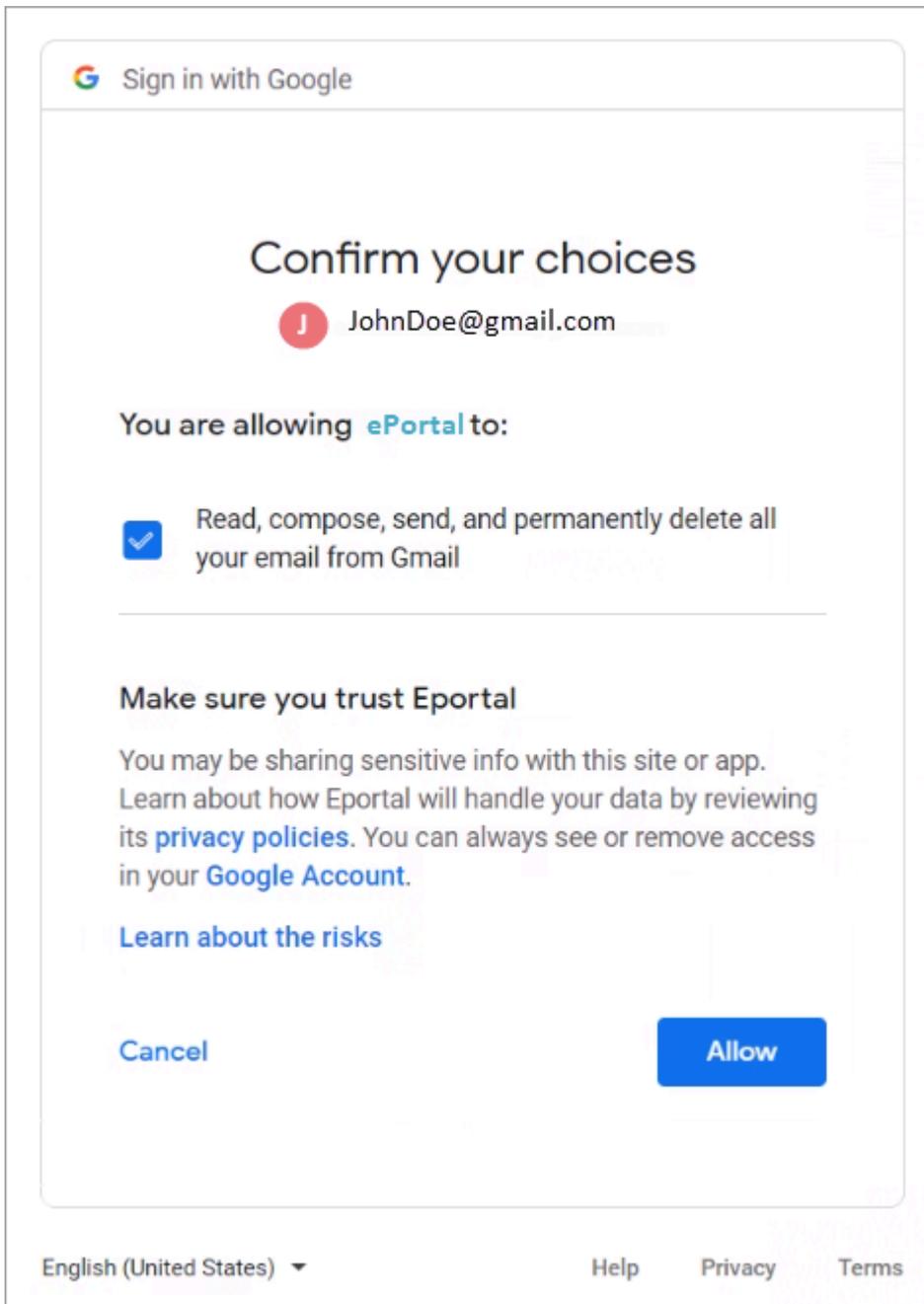
[Go to ePortal \(unsafe\)](#)

41. Click **Go to ePortal (unsafe)**.

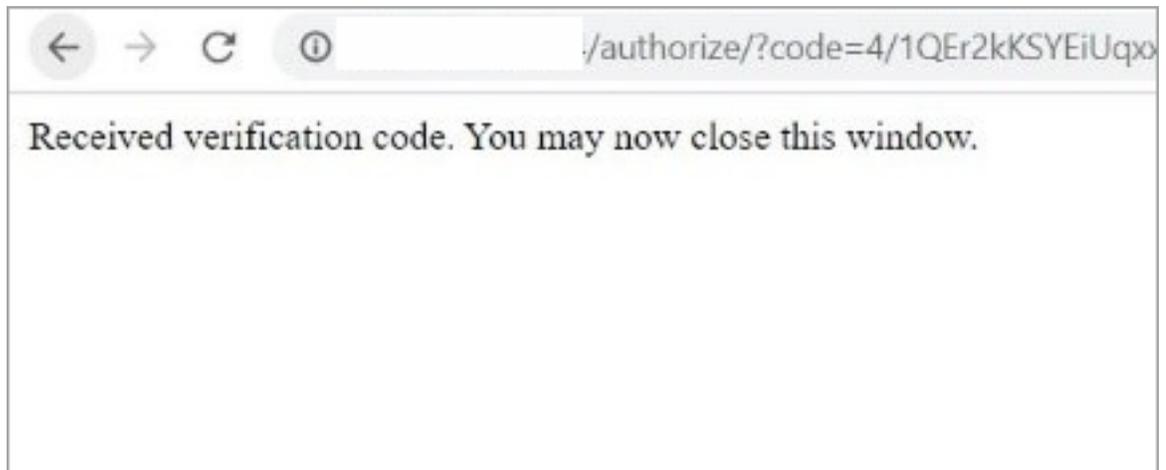
The **Grant ePortal permission** Web dialog appears.



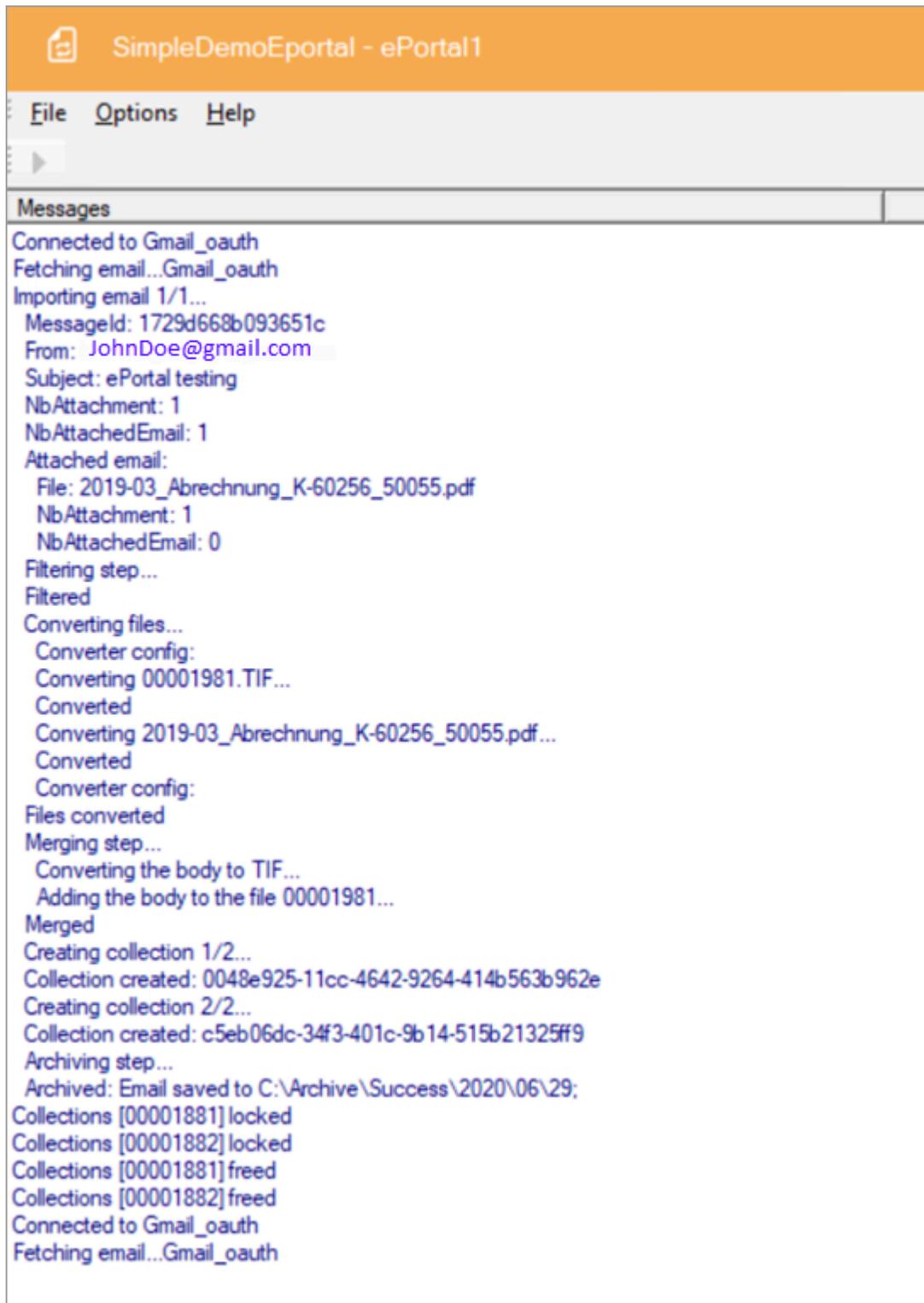
42. Click **Allow**. The **Confirm your choices** page appears.



43. Click **Allow**. The following page appears.



44. After accepting the permission, **ePortal Manual station** will start to fetch the Gmail messages from the configured folder.



EWS connector

The EWS connector retrieves a batch of emails from a Microsoft Exchange Server or Office 365 using the EWS (Exchange Web Services) protocol. After all emails from the batch are parsed, the connector returns an eBatch that can be processed by each ePortal stage.

About EWS

EWS - Exchange Web Services - provides the functionality to enable client applications to communicate with a Microsoft Exchange server. EWS provides access to the same data that is available through Microsoft Office Outlook. EWS clients can integrate Outlook data into Line-of-Business (LOB) applications. SOAP provides the messaging framework for messages sent between the client application and the Exchange server. The SOAP messages are sent by HTTP on port 443.

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 EWS filter IsRead=false, it will only import new emails.

Synchronized mode

Not implemented.

Exchange server version

The EWS protocol depends on the EXCHANGE server and must be specified in the configuration file.

ePortal supports the following Exchange versions:

- Exchange2013
- Exchange2010_SP2
- Exchange2010_SP1
- Exchange2010
- Exchange2007_SP1

Connect without credentials

To connect to the Exchange server with the same account while ePortal is running, in the <MailAccounts> section of the ePortal.AppConfig do the following:

- Leave UserName empty
- Set the password to Use Default/Domain Credentials

Impersonation

The EWS connector supports impersonation. Impersonation enables an account on an Exchange server to perform actions using the permissions that are associated with another account.

It may be necessary to connect to different email accounts with the same user. The only way to achieve this is to use impersonation.

Configuration

```
<MailAccount Id="EWSAccount_Read" DisplayName="Exchange connector" Host="outlook.office365.com" Port="0" SSL="true"
  UserName="HRTPL@HRTPLTEST.onmicrosoft.com" Password="*****"
  Protocol="EWSi">
  <Folders>
    <Folder>INBOX</Folder>
  </Folders>
  <Filter>IsRead=false</Filter>
  <ExchangeVersion>Exchange2010_SP1</ExchangeVersion>
  <Impersonate Enabled="false" UserName="" Domain="" Password=""
  Description="To execute the connector with another user account"/>
</MailAccount>
```

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 Eportal.AppConfig.

The EXCHANGE_ONLINE connector retrieves a batch of emails from a Microsoft Exchange Server or Office 365 using Microsoft graph api and OAuth2.0 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 mail account in EXCHANGE_ONLINE protocol in eportal.appconfig file, you need to manually authorize yourself in ePortal station by entering configured mail account credentials and permissions consent.

Scenario 2: When your email account password expires or changes, then you need to re-authorize yourself by opening ePortal station manually.

After that, enable the autorun mode for ePortal station

Configuration

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

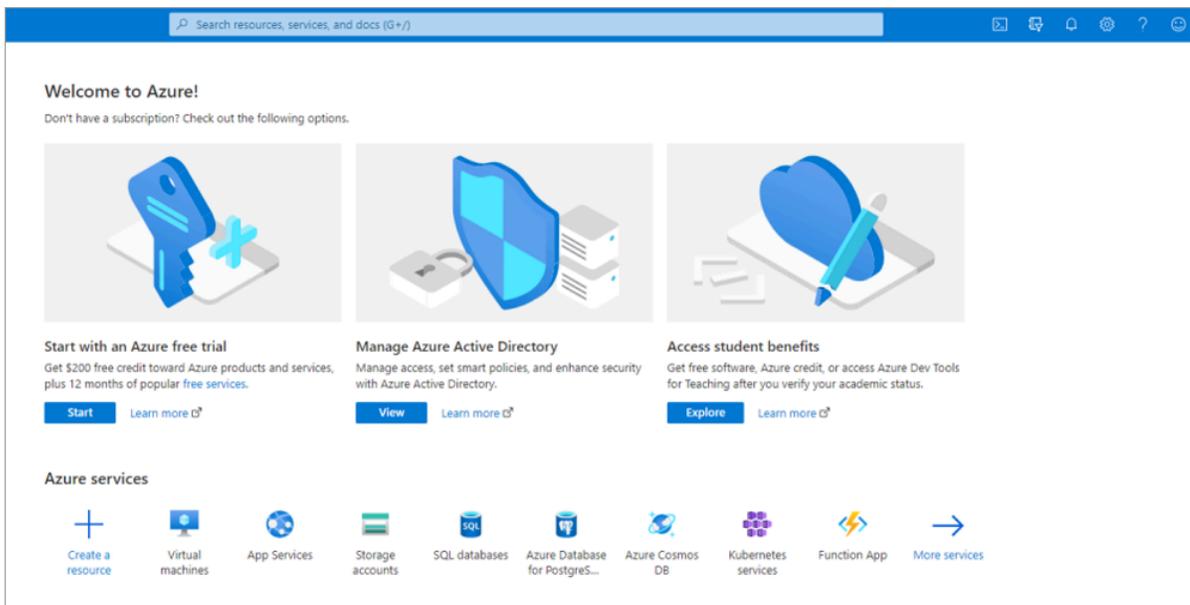
The following step-by-step procedure explains how to register an ePortal app, and the minimum set of privileges needed for it. More granular role-based access privileges are possible, which is subjected to the individual organization IT polices.

Azure cloud configuration for Office 365

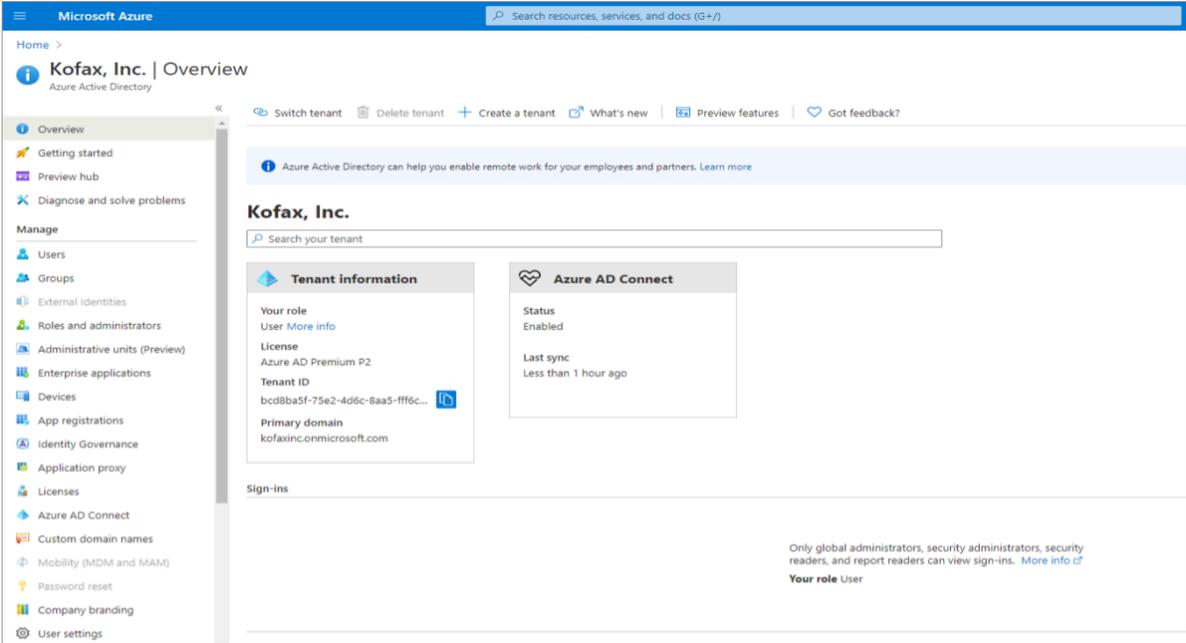
This section describe the Azure cloud configuration for Office 365. After you configure Azure cloud, ePortal can automatically can read mails from Outlook.

Note The figures used in the following instructions are taken from Microsoft Azure site, the appearance and user interfaces might change occasionally.

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



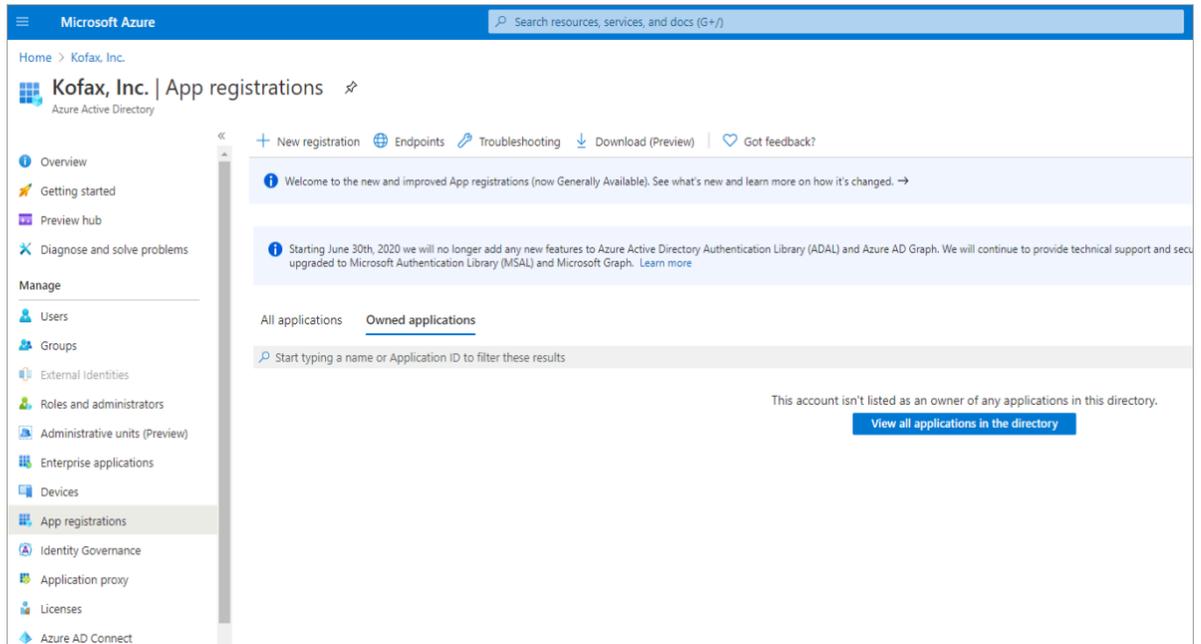
- 2. On the Azure home page, under **Manage Azure Active Directory**, click **View**. The **Overview** page appears.



Manage App registrations

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

1. In the left pane, under **Manage**, click **App registrations**.
The **App registrations** page appears.



2. Click New registration.

The **Register an application** page appears.

The screenshot shows the Microsoft Azure portal interface for registering an application. The breadcrumb trail is 'Home > Kofax, Inc. > Register an application'. The page title is 'Register an application'. There is a search bar at the top right with the text 'Search resources, services, and docs (G+/)'. The main content area contains the following sections:

- Name:** A text input field with a red asterisk indicating it is required. Below the field is the text: 'The user-facing display name for this application (this can be changed later).' The field is currently empty.
- Supported account types:** A section titled 'Who can use this application or access this API?' with three radio button options:
 - Accounts in this organizational directory only (Kofax, Inc. only - Single tenant)
 - Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 - Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 - Personal Microsoft accounts onlyA link 'Help me choose...' is located below the options.
- Redirect URI (optional):** A section with the text: 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' It contains a dropdown menu set to 'Web' and a text input field containing 'e.g. https://myapp.com/auth'.

At the bottom of the form, there is a link: 'By proceeding, you agree to the Microsoft Platform Policies' and a blue 'Register' button.

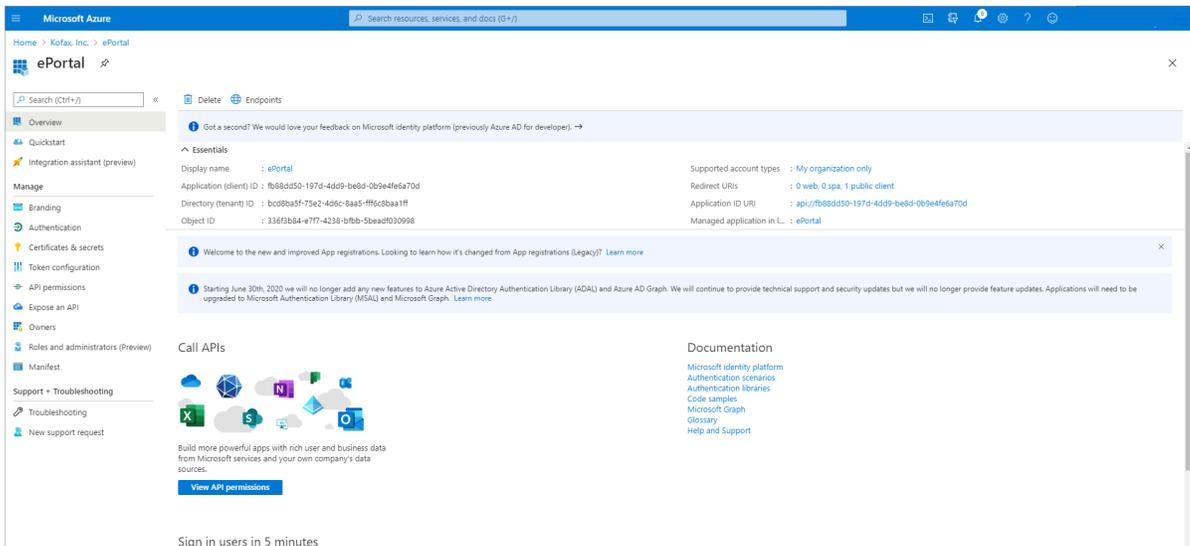
3. In the **Name** field, enter the application name that to be displayed to the users.

4. Under **Supported account types**, select **Accounts in this organizational directory only (Kofax, Inc. only - Single tenant)**.

Note Select this option if you are building a line-of-business (LOB) application. This option is not available if you are not registering the application in a directory. This option maps to Azure AD only single tenant and is the default unless you are registering the app outside of a directory. In cases where the app is registered outside of a directory, the default is Azure AD multi-tenant and personal Microsoft accounts.

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

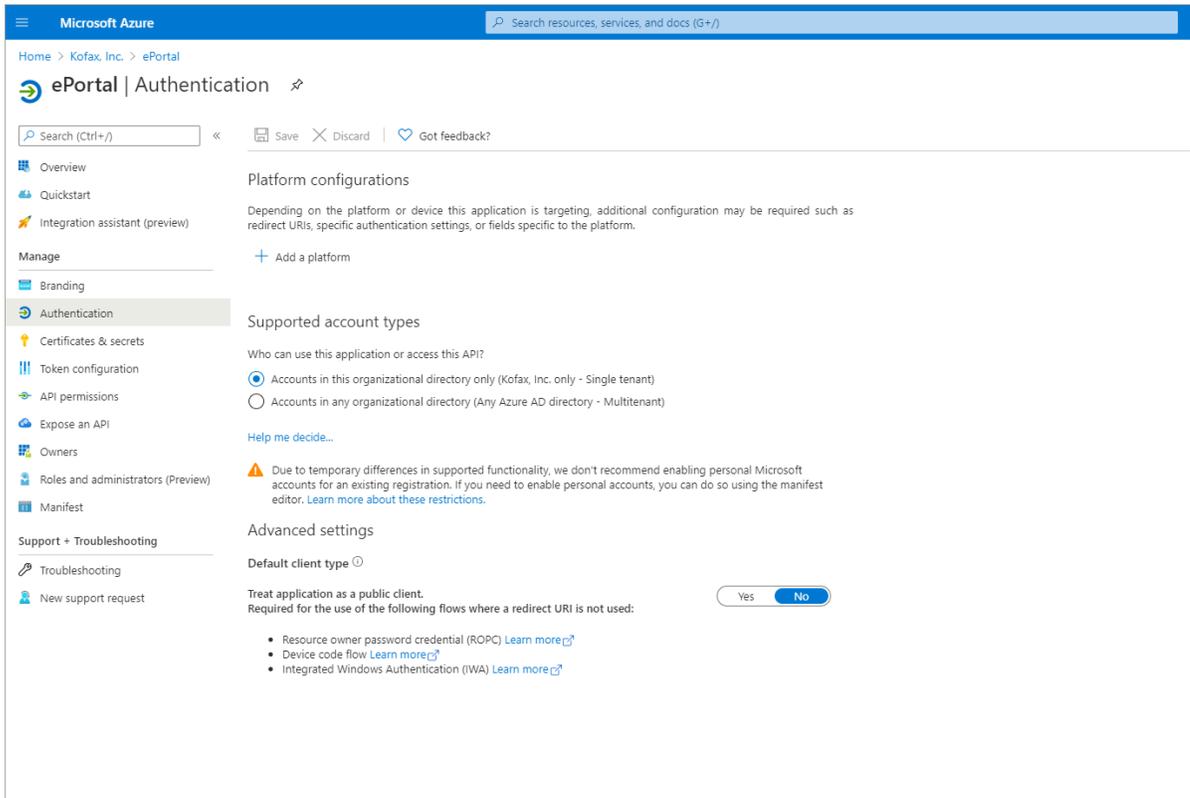
The following page appears.



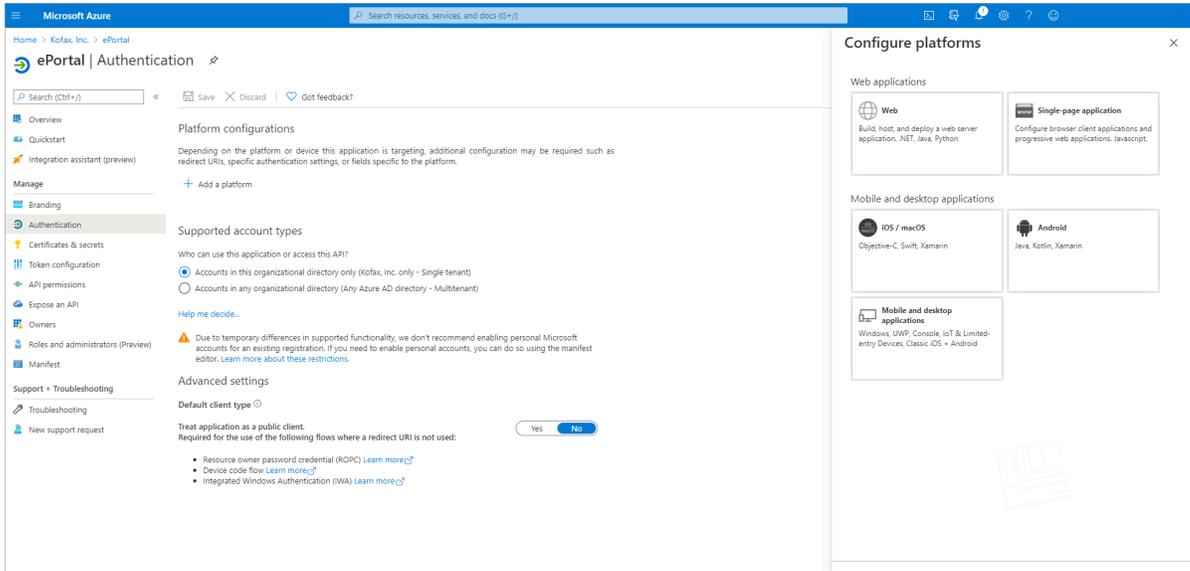
Manage authentication

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

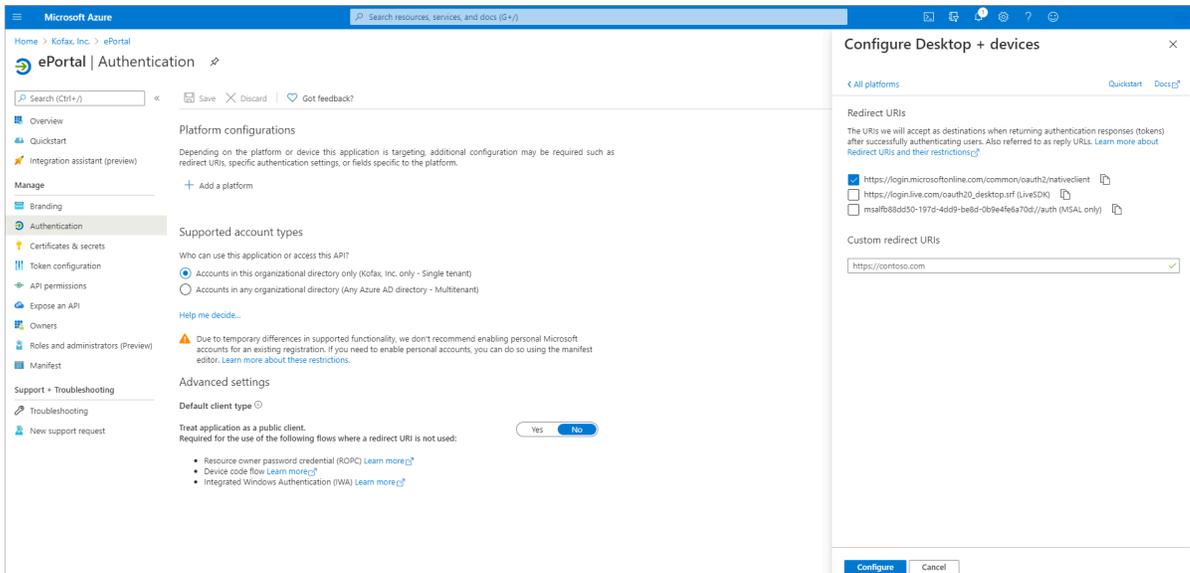
1. In the left pane under **Manage**, click **Authentication**.
The **Authentication** page appears.



- 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.



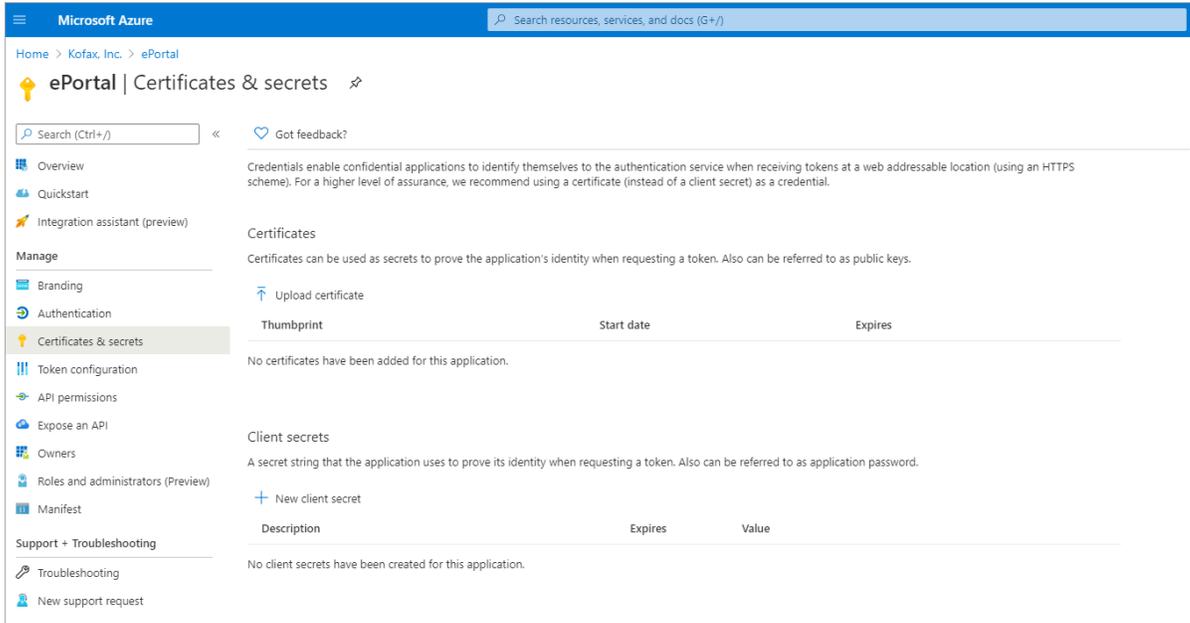
4. Select **https://login.microsoftonline.com/common/oauth2/nativeclient**, and click **Configure**. On the **Authentication** page, under **Redirect URIs**, you can see the selected option.

The screenshot displays the Microsoft Azure portal interface for configuring an application. The left-hand navigation pane is open to the 'Authentication' section. The main content area is titled 'Platform configurations' and includes a section for 'Mobile and desktop applications'. Within this section, the 'Redirect URIs' are listed, with the first one, 'https://login.microsoftonline.com/common/oauth2/nativeclient', checked. Below the URIs, the 'Supported account types' are configured to 'Accounts in this organizational directory only (Kofax, Inc. only - Single tenant)'. A warning message is present regarding personal Microsoft accounts.

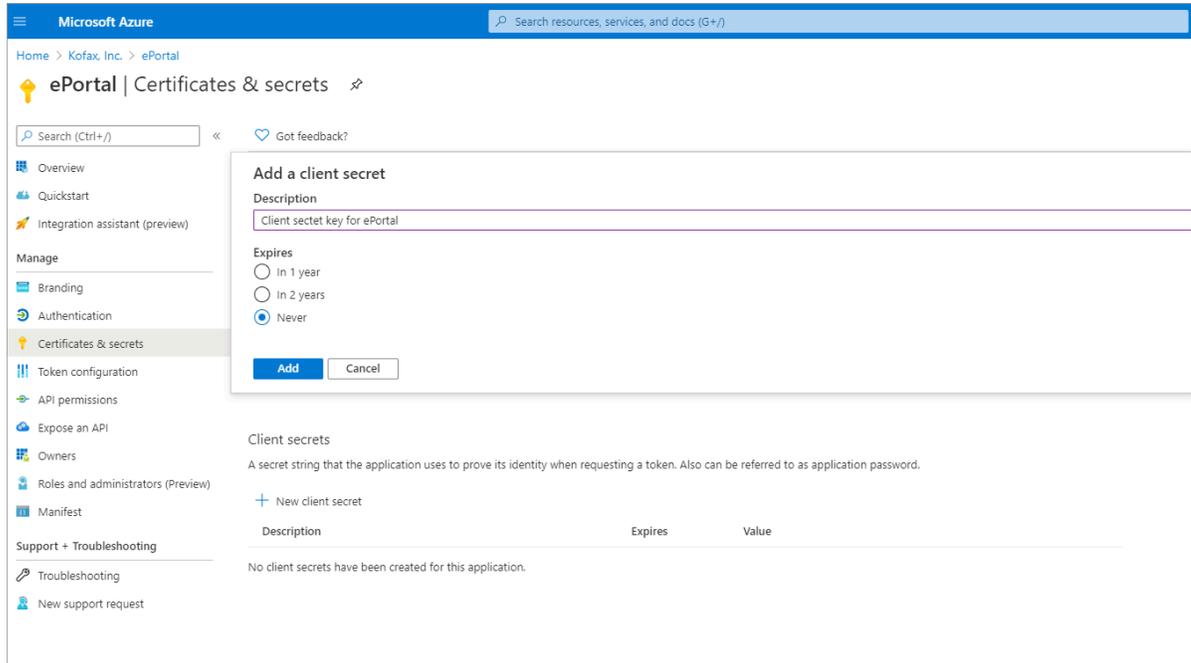
Manage certificates and secrets

Upload certificate or create client secrets to enable confidential applications.

1. In left pane, under **Manage**, click **Certificate & secrets**.
The **Certificate & secrets** page appears.



2. Under **Client secrets**, click **New Client secret**.
The **Add a client secret** section 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 client secret details.

Microsoft Azure

Home > Kofax, Inc. > ePortal

ePortal | Certificates & secrets

Search (Ctrl+/) Got feedback?

Overview
Quickstart
Integration assistant (preview)

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators (Preview)
Manifest

Support + Troubleshooting

Troubleshooting
New support request

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value
Client secret key for ePortal	12/31/2299	do1Hq,0xDy18H6j&.7d-j5WvaPIOb,_t

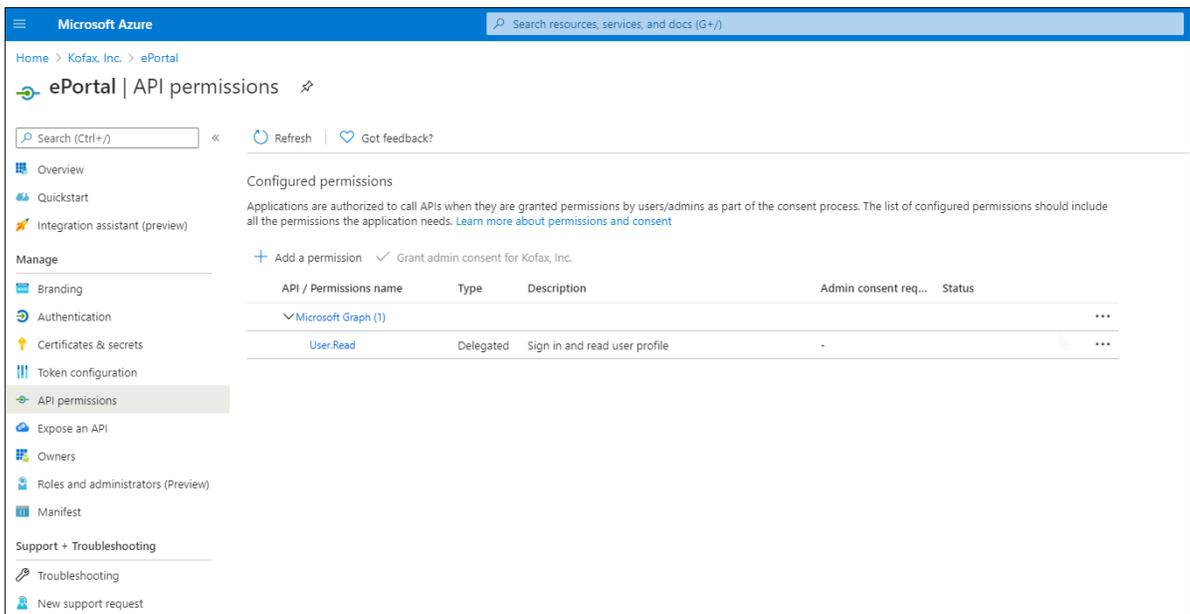
Copy to clipboard

Note Note down the Client secrets value to refer in the future activities.

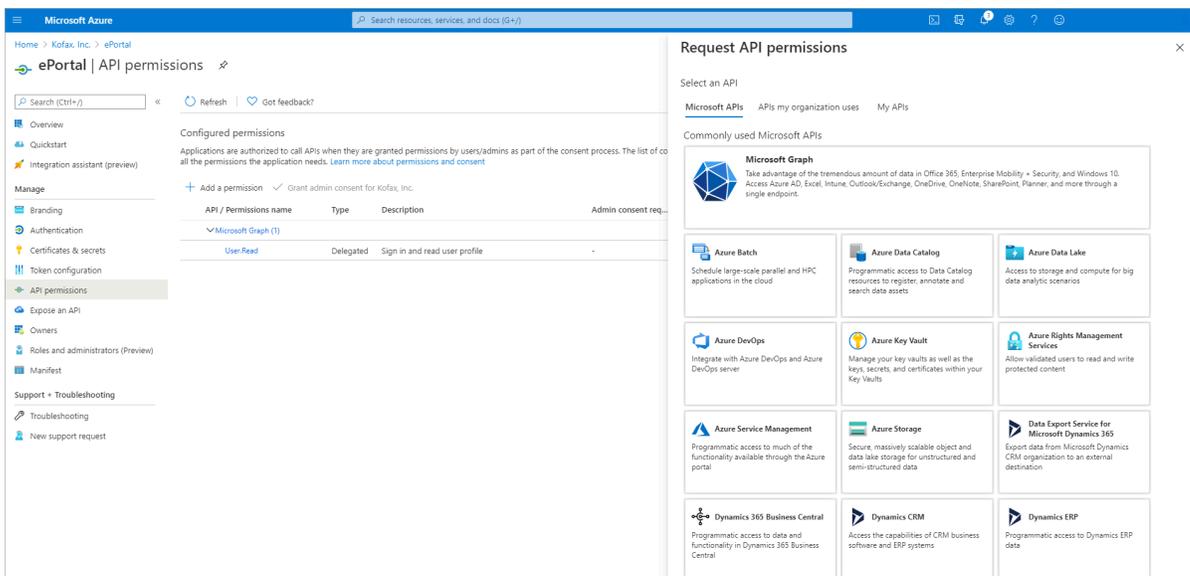
Manage API permissions

Add the required permissions to authorize applications to call APIs.

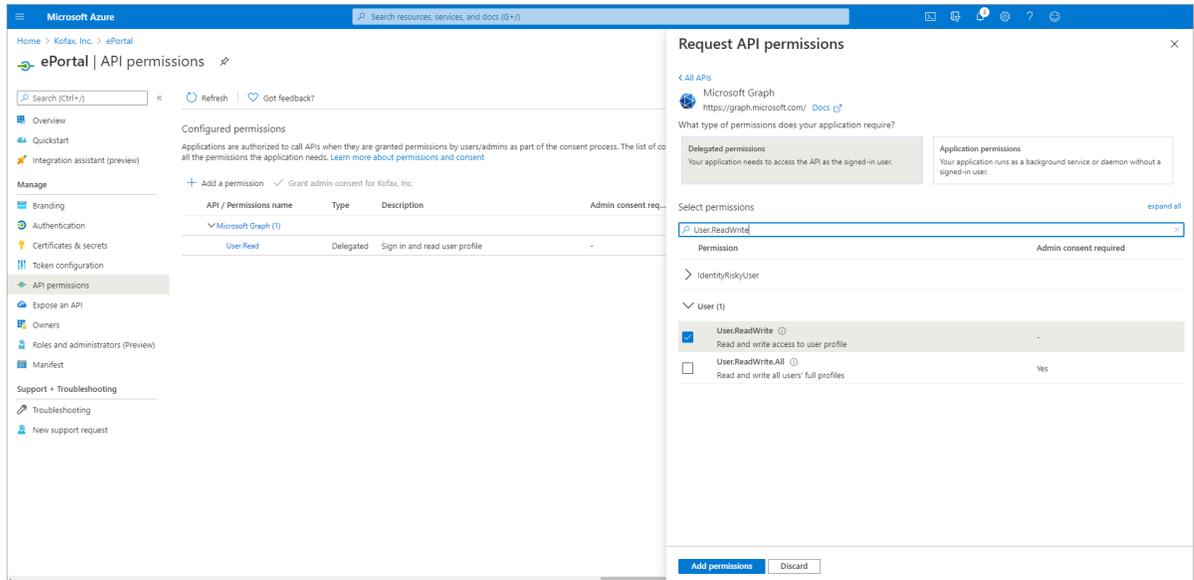
1. In the left pane, under **Manage**, click **API permissions**.
The **API permissions** page appears.



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**.

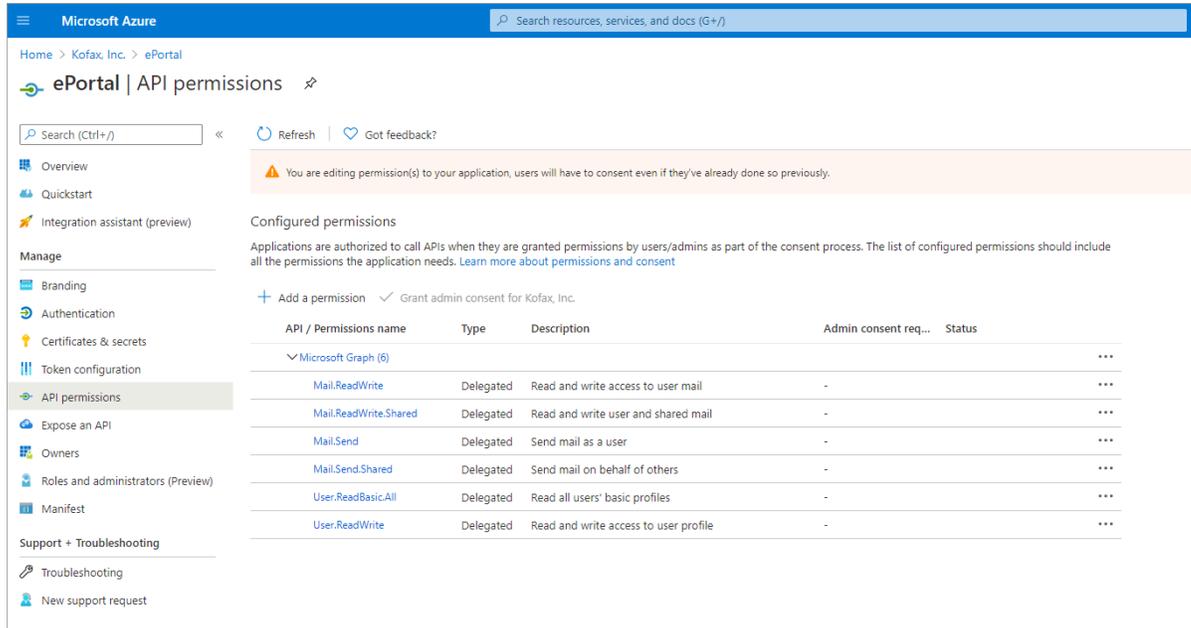


4. Click **Delegated permissions > Select Permission**, and then select the following six permissions.

- 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 the six permissions.

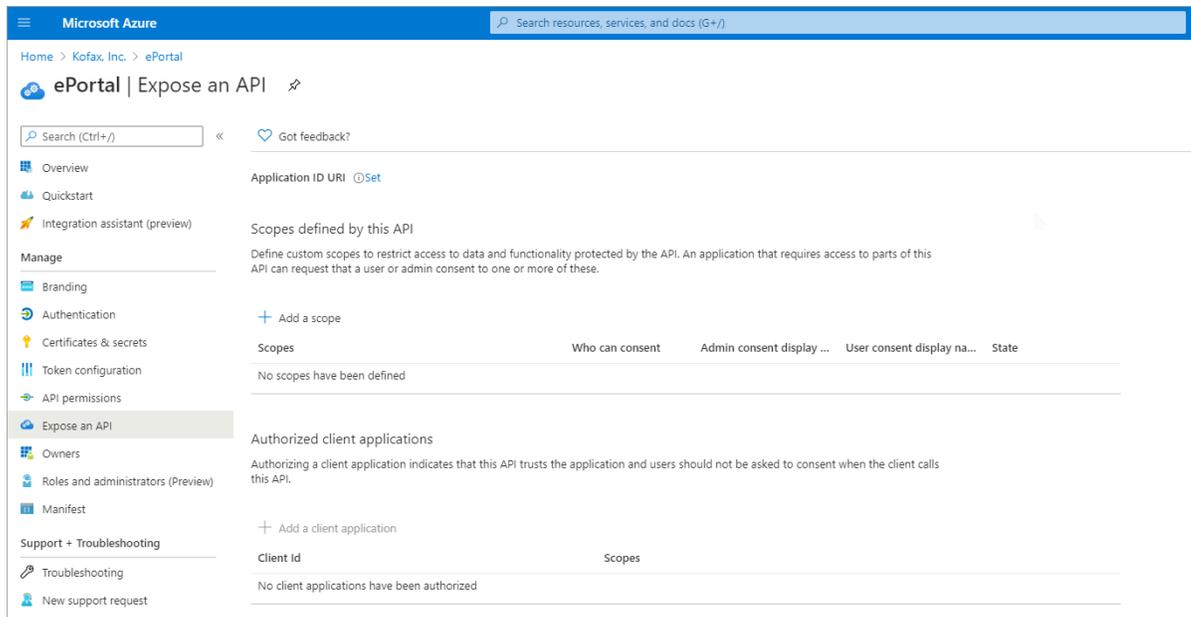


Manage exposing an API

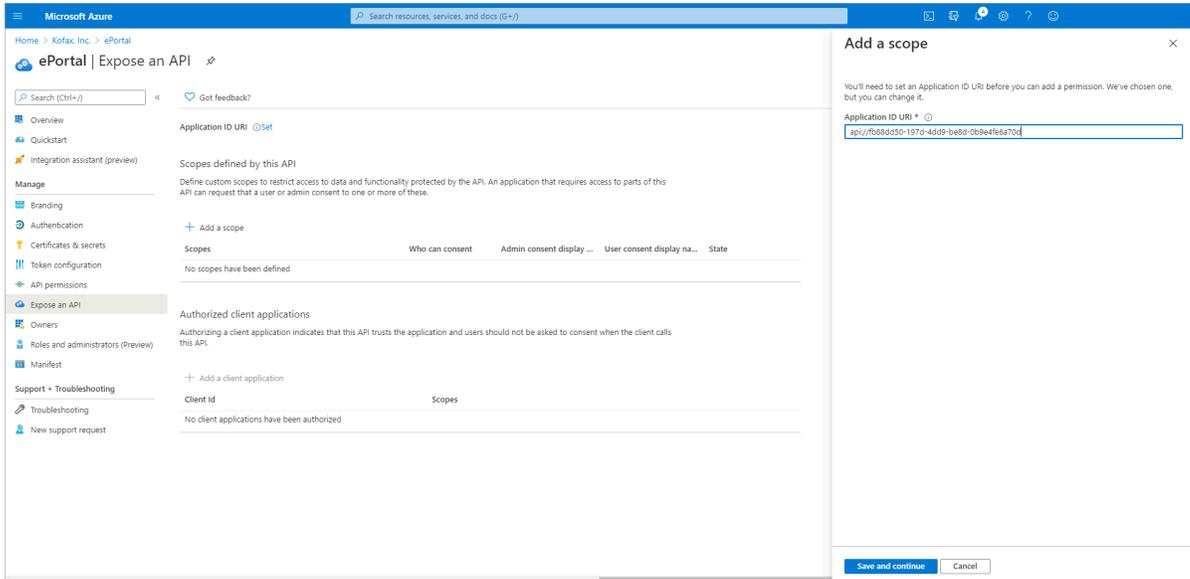
Define scope to allow or restrict access to data or functionality protected by an API.

1. In the left pane, under Manage, click Expose an API.

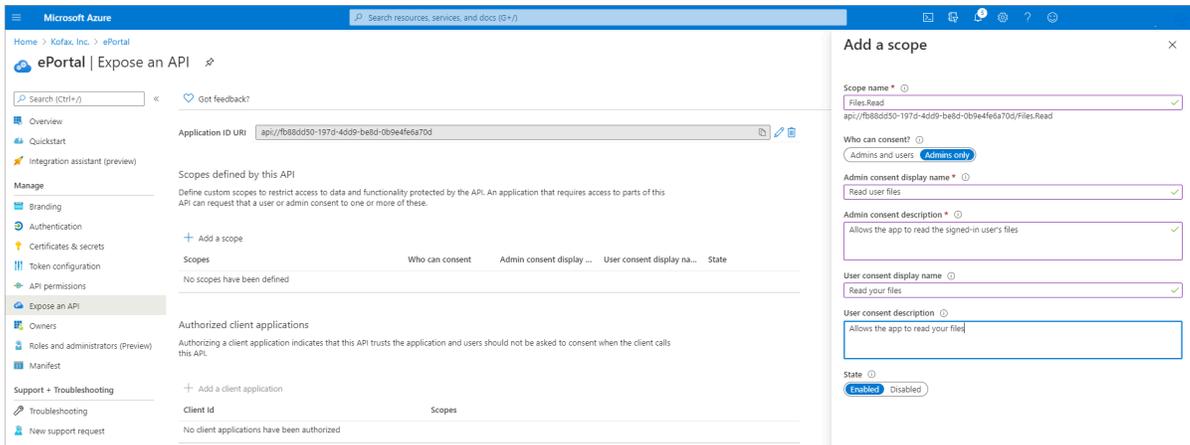
The **Expose an API** page appears.



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

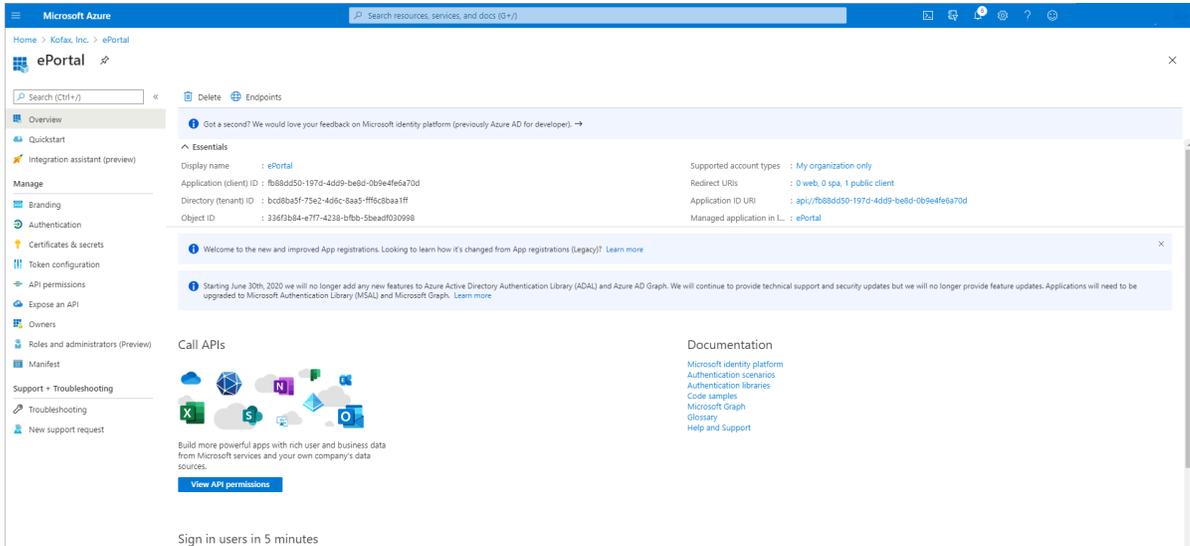


3. Click **Save and continue**.
The **Add a scope** section appears on the right side of the page.

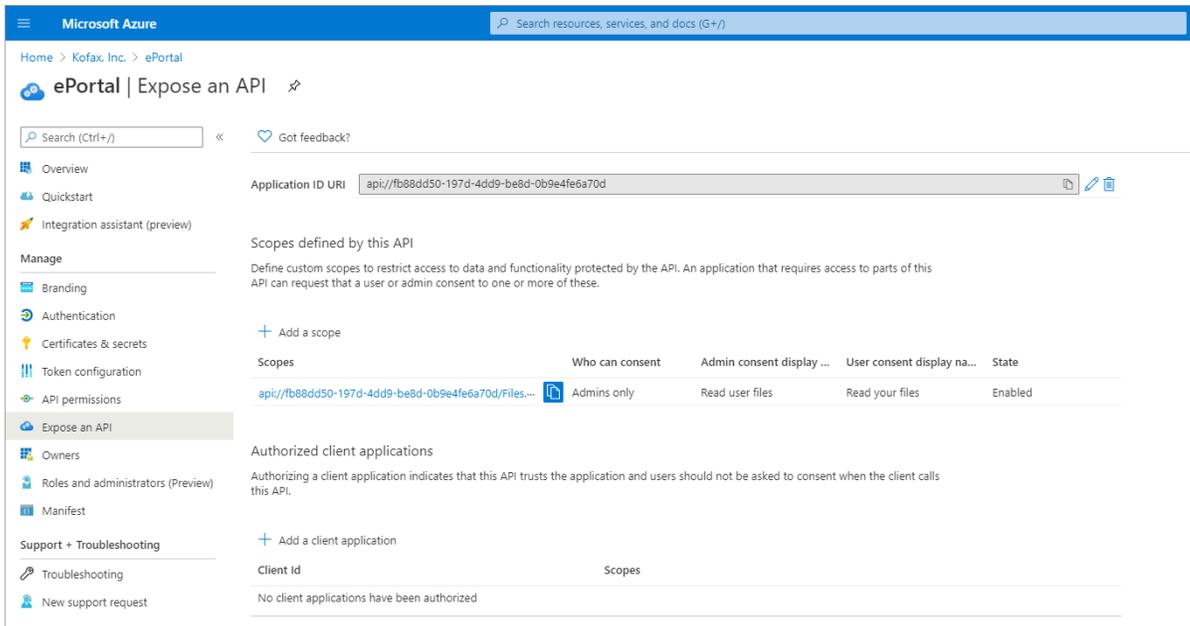


4. For **Who can consent?**, select **Admins only**.
5. For **State**, select **Enabled**.
6. Click **Add scope**.

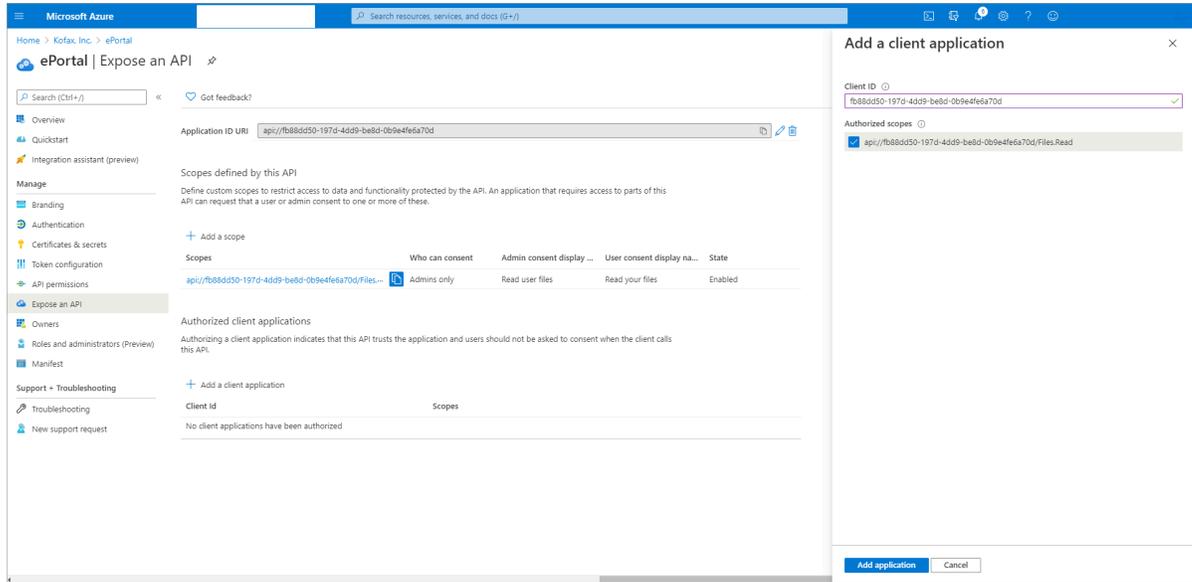
- In the left pane, click **Overview**.
The **Overview** page appears.



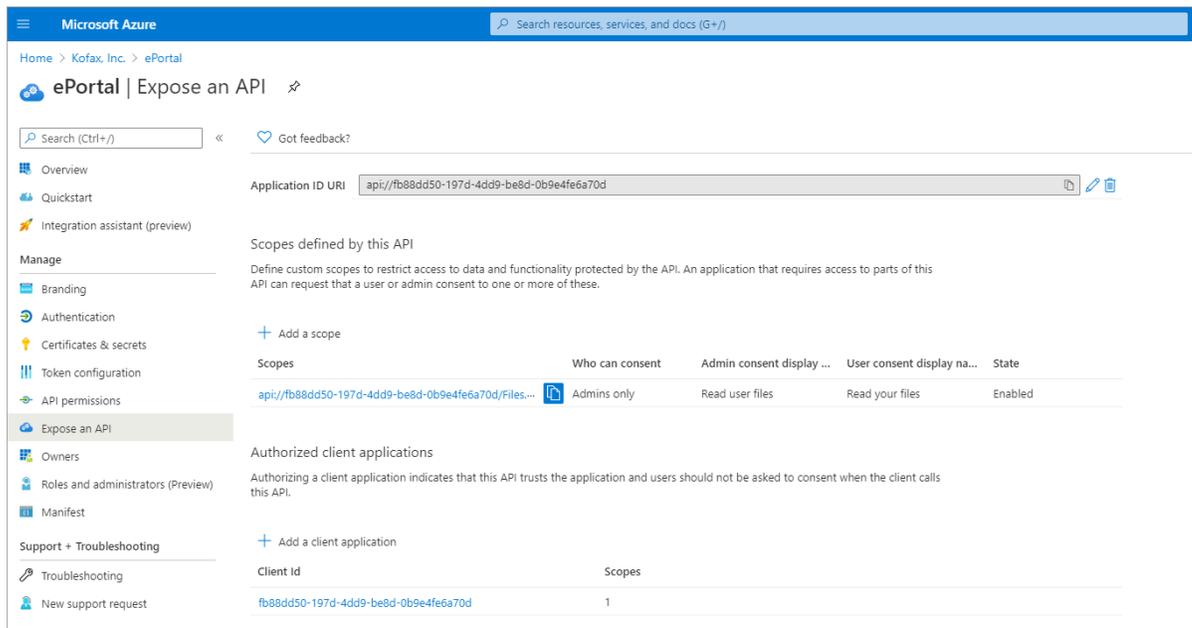
- Note down the **Application (client) ID**.
- In the left pane, click **Expose an API**.
The **Expose an API** page appears.



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



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

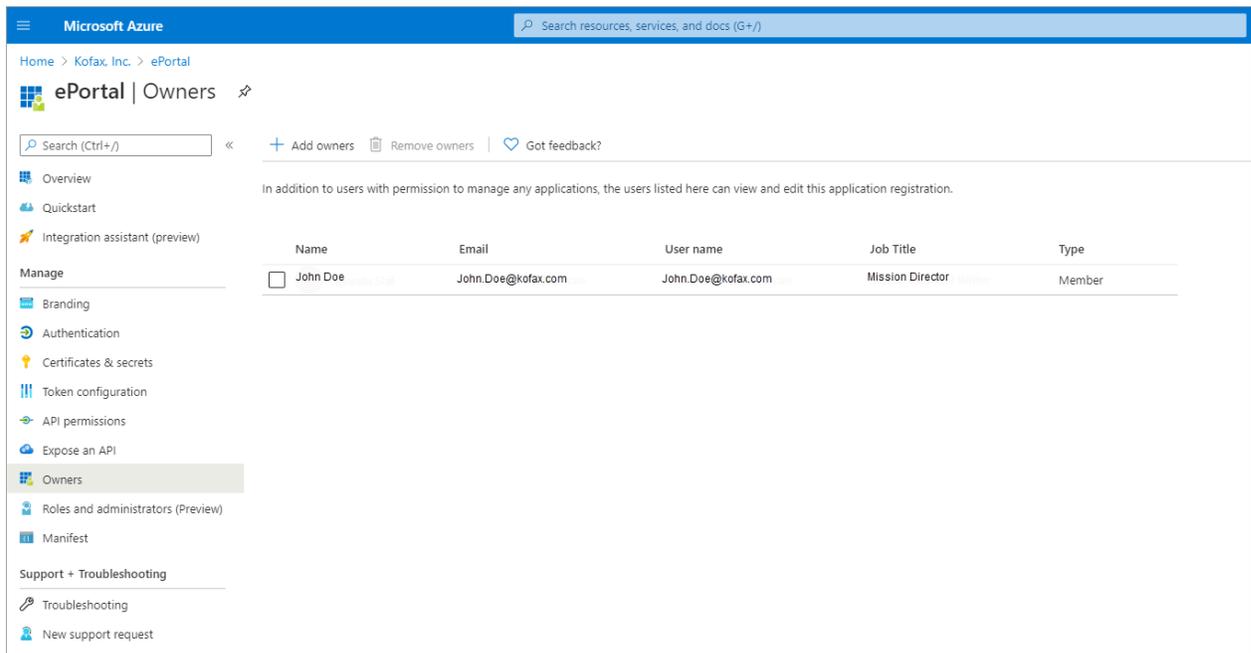


Manage owners

The **Owners** page allows you see the owners of the ePortal.

In the left pane, under **Manage**, click **Owners**.

The **Owners** page appears. In this page you can see the owners of the ePortal.



The screenshot shows the Microsoft Azure portal interface for managing ePortal owners. The breadcrumb path is Home > Kofax, Inc. > ePortal. The page title is ePortal | Owners. Below the title, there is a search bar and navigation links: + Add owners, Remove owners, and Got feedback?. The main content area contains a table of owners with the following columns: Name, Email, User name, Job Title, and Type. The table has one row for John Doe, with Job Title Mission Director and Type Member. The left sidebar shows the Manage section with various options, and the Owners option is highlighted.

Name	Email	User name	Job Title	Type
<input type="checkbox"/> John Doe	John.Doe@kofax.com	John.Doe@kofax.com	Mission Director	Member

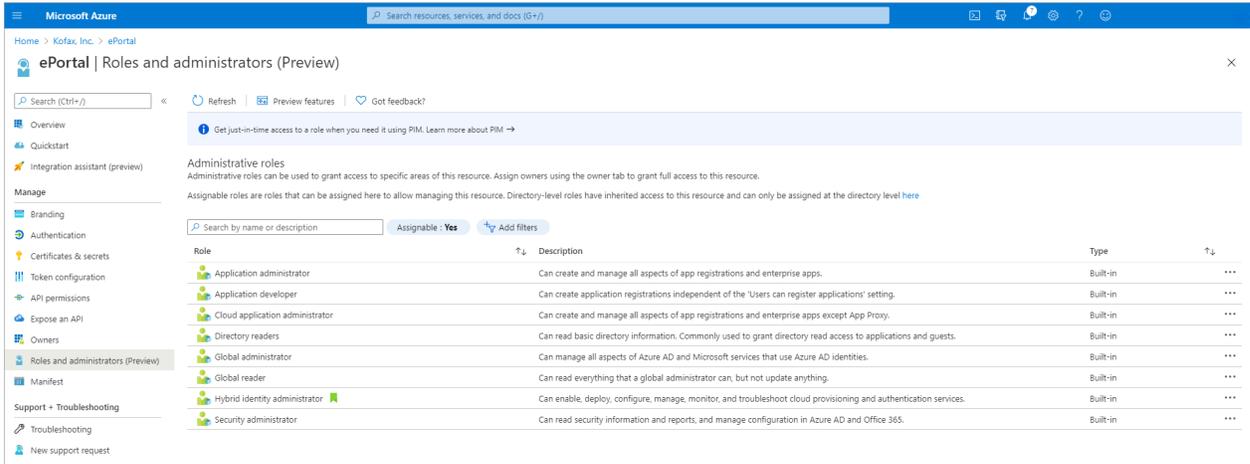
Note An admin can add more than one owners.

Manage roles and administrators (Preview)

The **Roles and administrators (Preview)** page allows you to see the various administrative roles.

In the left pane, under **Manage** click **Roles and administrators (Preview)**.

The **Roles and administrators (Preview)** page appears. In this page you can see administrative roles.

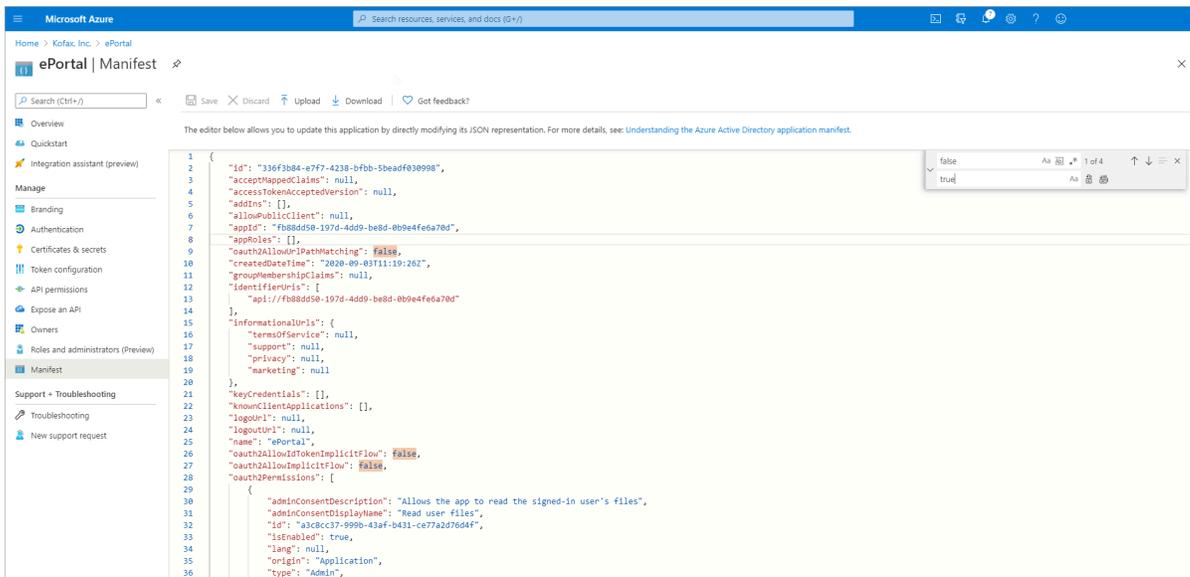


Manage manifest

The Manifest page opens an editor where you can update the application by directly modifying its JSON representation.

1. In the left pane, under **Manage**, click **Manifest**.

The **Manifest** page appears.

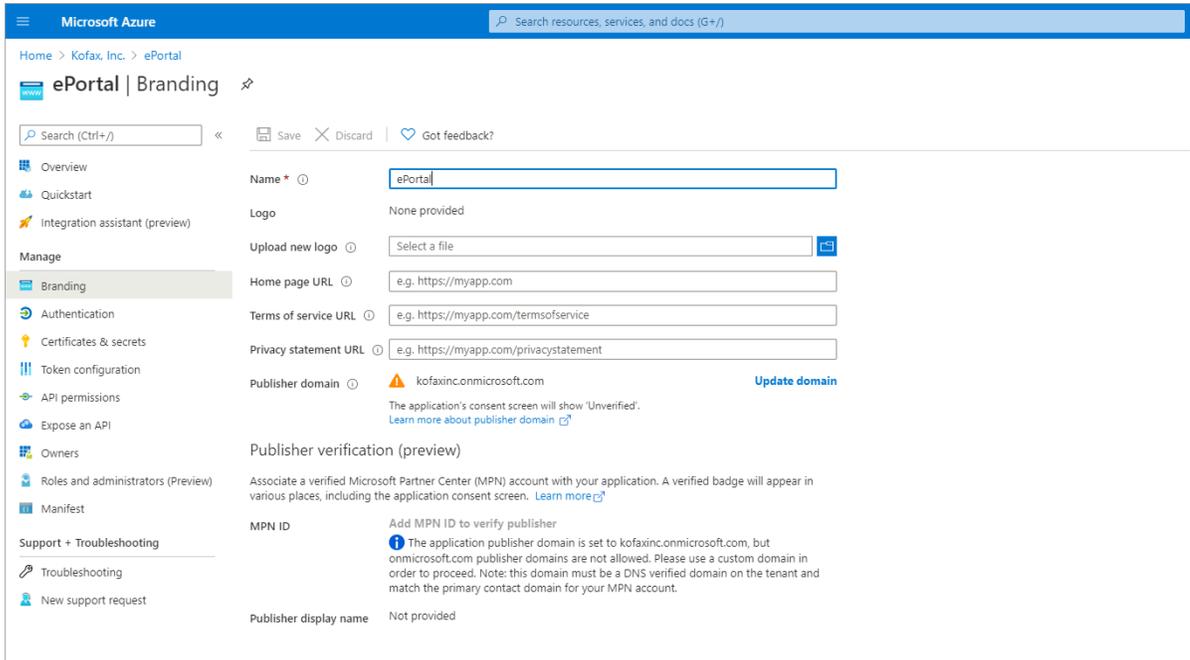


2. Replace all "false" with "true", and click **Save**.

Manage branding

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

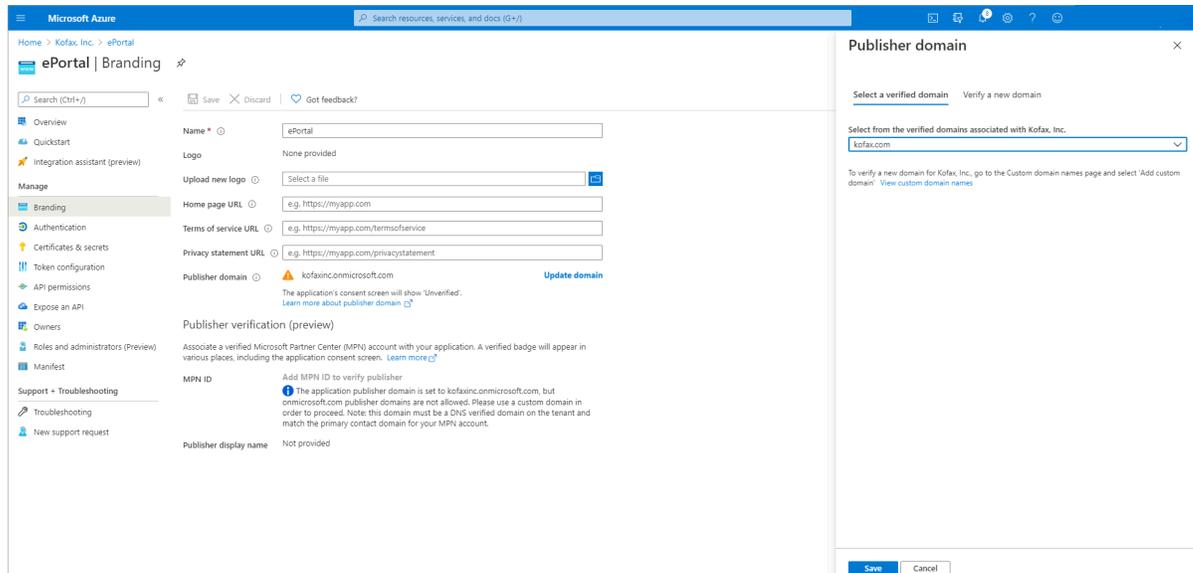
1. In the left pane, under **Manage**, click **Branding**.
The **Branding** page appears.



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.

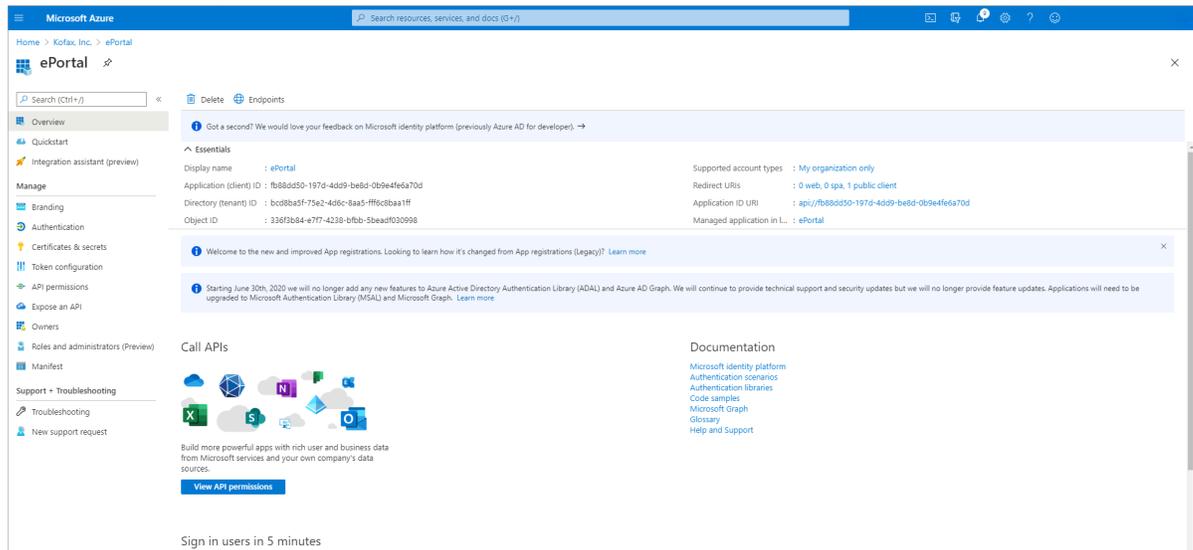


4. On the **Select a verified domain** tab, select a domain that is associated with your organization from the list.

5. Click **Save**.

6. In the left pane, click **Overview**.

The **Overview** page appears.



7. Keep a note of **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>
<Subfolder>0</Subfolder>
<SharedMailbox />
<Filter>IsRead=false</Filter>
<ExchangeVersion>Exchange2013</ExchangeVersion>
<Impersonate Enabled="false" />
</MailAccount>
```

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

Note 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.

Note Go to #25 for help.

Run the ePortal manual station

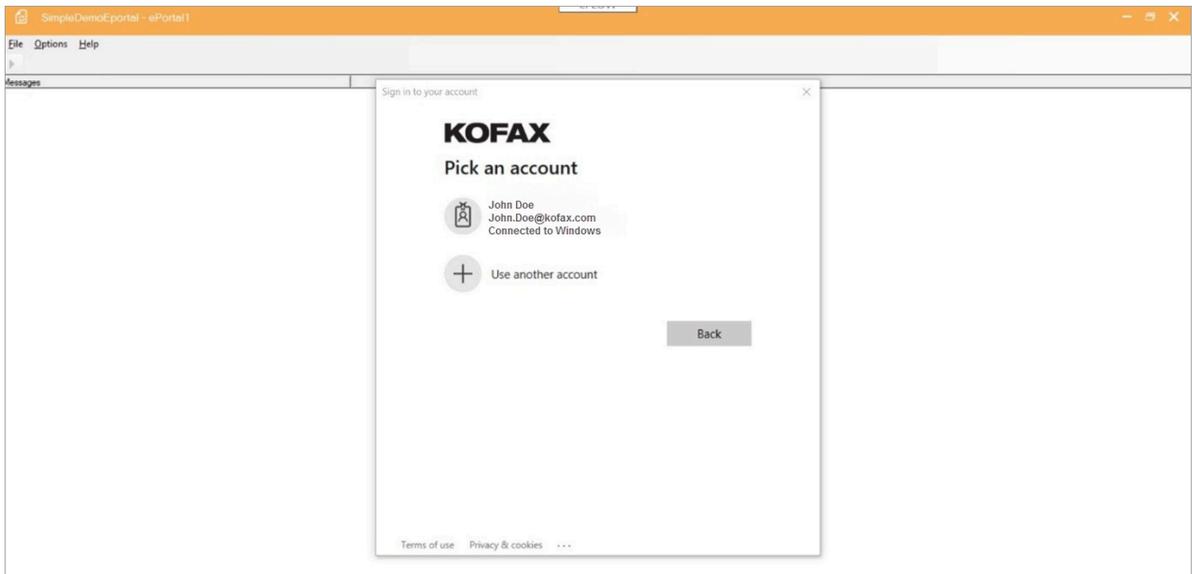
Do the following to run the ePortal manual station.

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

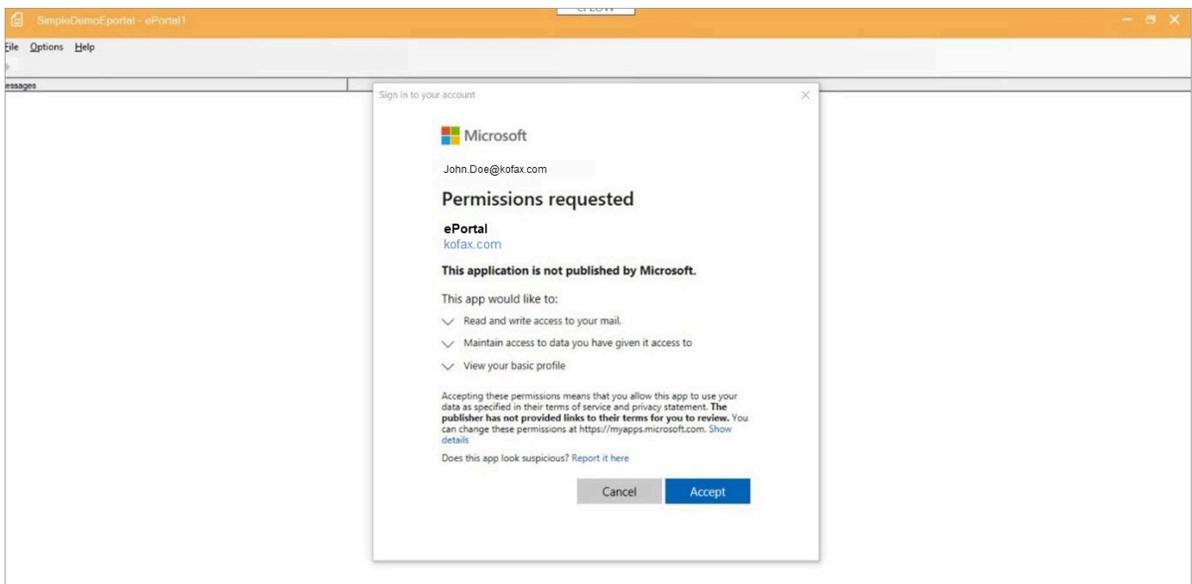
Important If your default browser is Internet Explorer, make sure that JavaScript is enabled.

2. If the given username in eportal.appconfig (email id) is not outlook configured with the computer using ePortal.

The following page appears.

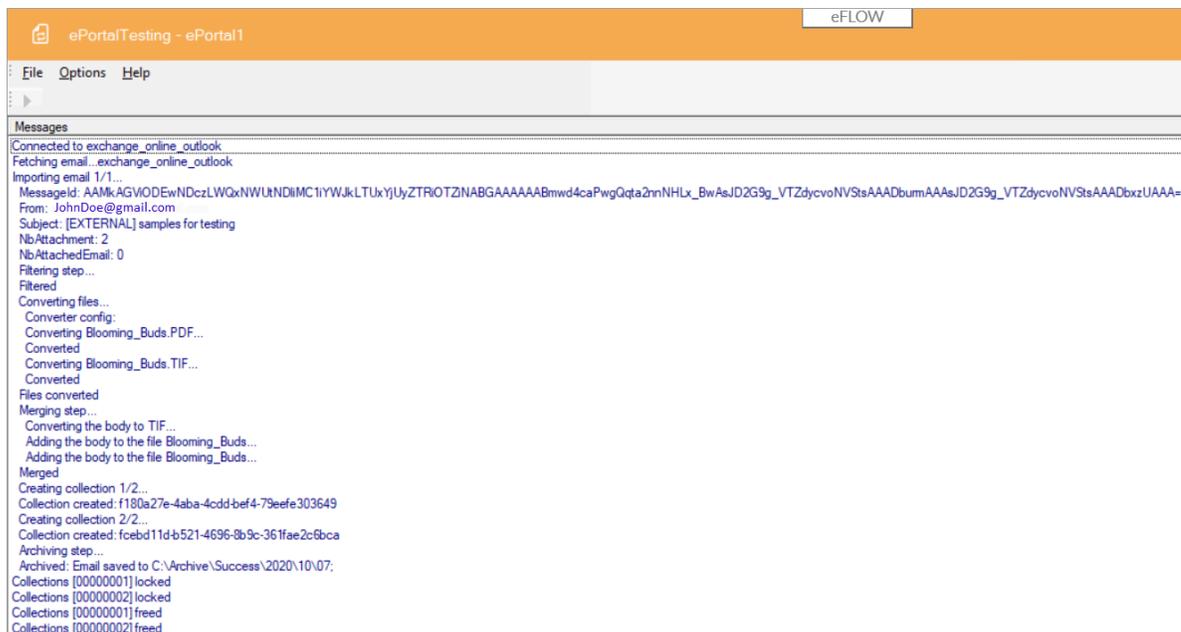


3. Select an account, and then enter your password to sign in. After sign-in, the following page appears.



4. Click **Accept**.

5. After accepting the permission, the **ePortal Manual station** will start to fetch 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 of 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 of 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:

- 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>
```

Chapter 5

Filtering

The purpose of the ePortal filters are used to do the following:

1. Classify the eDoc of the envelope as:
 - AcceptedDoc
 - AttachedDoc (DocAttachment)
 - AttachedFile (FileAttachment)
 - RejectedFile
2. Link AttachedDocs (DocAttachment) and AttachedFiles (FileAttachment) to their main AcceptedDoc.

Filtering process

The eDocs are filtered in the following order:

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

eDocs are filtered according to the following:

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

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 or DocAttachment

The AttachedDoc is the image to be 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 or FileAttachment

The AttachedFile is the file to be attached to the eFlow collection as an eFlow file attachment. The file is not merged with the collection. For example, you want to 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 images with signatures (PNG files).

Linking AcceptedDoc

The file name of 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, < and > must be replaced by { 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 6

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 convertor to perform such tasks.

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

Available converters

Currently the following convertors 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, PPTX File. The list is constantly being updated.)
- Winnovative (html, htm, mht)
- PRD – PDFtools (searchable PDF)

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 7

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, which means they will not be processed by the OCR engines.
- Attaching the original email attachments to the collection so that they can be exported.

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 8

Acknowledgement

The Acknowledgement feature allows you to send an email to the sender to inform them that their files have been processed.

The acknowledgement email is sent after the imported email is archived. You must configure acknowledgement for each archive: SUCCESS, REJECT, ERROR.

Configuration

1. Set up an SMTP account:

```
<MailAccount Id="account1gmailSMTP" DisplayName="My Gmail Smtп SSL=NO profile"
Host="smtp.googlemail.com" Port="587" SSL="true" UserName="xxx"
Password="xxx" Protocol="SMTP">
</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="account1gmailPop3SSL" Enabled="true" />
  <ActiveAccount Id="account1gmailSMTP" 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 acknowledgement emails. ePortal provides default templates in the C:\Program Files (x86)\TIS\Kofax eFlow ePortal\Runtime\Template\ folder.

- 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 file C:\Program Files (x86)\TIS\Kofax eFlow ePortal\Runtime\Template\AvailableTags.html lists the variables you can use.

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

Acknowledgement of email attachments

The acknowledgement mail can inform the sender which files were accepted and which were rejected. You can integrate this in the acknowledgement 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}