

OAuth utilities for IBM SOAR apps

Table of Contents

- [Release Notes](#)
 - [Overview](#)
 - [Key Features](#)
 - [Requirements](#)
 - [Installation](#)
 - [Install](#)
 - [Configuration](#)
 - [Usage](#)
 - [Configure OAuth 2.0 credentials](#)
 - [Google Gmail](#)
 - [Microsoft Outlook 365](#)
 - [Troubleshooting & Support](#)
-

Release Notes

Version	Date	Notes
1.0.0	07/2022	Initial Release

Overview

OAuth utilities

The OAuth Utilities package provides tools and utilities to support OAuth for IBM SOAR apps.

Key Features

- A utility to generate an OAuth 2.0 authorization code flow refresh token for an IBM SOAR app.
-

Requirements

Python Environment

Both Python 3.6 and python 3.9 are supported. Additional package dependencies might exist for each of these packages:

- Jinja2>=30.0.0
- six>=39.0.0
- urllib3>=0.18.2
- requests>=0.18.2
- flask>=2.0.3
- pyOpenSSL>=0.18.2
- click>=8.0.4

Prerequisites

- Utility `oauth2_generate_refresh_token`: An OAuth 2.0 identity provider service with an app or project configured to allow user access to a 3rd party application.

Configuration

- Utility `oauth2_generate_refresh_token`: The following settings must be provided for the OAuth 2.0 service.

```
client_id
client_secret
scope
token_url
auth_url
```

Permission

- Utility `oauth2_generate_refresh_token`: The provided OAuth 2.0 configuration settings must have required access to the 3rd party app.

Installation

Install

You can download the `oauth-utils` app packages from the [IBM Resilient Community](#) or [IBM X-Force App Exchange](#).

Complete the following steps to install the `oauth-utils` Python package:

1. Ensure that your python environment is up to date, as follows:

```
pip install --upgrade pip
pip install --upgrade setuptools
```

2. Go to the folder where the downloaded app is located and unzip. For example:

```
unzip oauth-utils-1.0.0-00001.zip
```

3. The app zip file contains a python package. Install the package using the following command:

```
pip install --upgrade oauth-utils-1.0.0.tar.gz
```

4. If running in browser mode, install optional python modules using the following command:

```
pip install --upgrade oauth-utils-1.0.0.tar.gz[browser]
```

Package Configuration

Utility: `oauth2_generate_refresh_token`

Required Settings

The following table provides the settings required to execute this utility. These settings are either read from an `app.config` file or provided as command-line arguments.

Setting/Argument	Required	Example	Cli usage	Description
client_id	Yes	1234567a-abc8-90d1-2efa3-123456789abcd	-ci or --client_id <CLIENT_ID>	OAuth 2.0 application or project client ID.
client_secret	Yes	ABCDEF-123456789abcd123456789a_aWX4	-ci or --client_secret <CLIENT_SECRET>	OAuth 2.0 application or project client Secret.
scope	Yes	https://mail.myservice.com/	-sc or --scope <SCOPE>	OAuth 2.0 application or project scope.
token_url	Yes	https://myservice.com/o/oauth2/token	-tu or --token_url <TOKEN_URL>	OAuth 2.0 application or project token url.
auth_url	Yes	https://myservice.com/o/oauth2/auth	-au or --auth_url <AUTH_URL>	OAuth 2.0 application or project authorization url.

NOTE: The settings are all read either from an app.config file or as command-line arguments. These operations are mutually exclusive.

NOTE: The settings are read from an app.config file if one is located in the environment. Alternative app.config files can be selected using the -c or --config_file option.

Arguments

The following table provides additional optional command-line arguments which can be used to execute this utility.

Argument	Required	Example	Description
browser	No	-b or --browser	Browser mode. Use a browser to control the flow and run a callback listener.
config_file	No	-c or --config_file <path_to_config_file>/app.config	Location of app.config file to override default.
port	No	-p or --port 4000	TCP port used for callback url and listener (default is 8080).
timeout	No	-t or --timeout 90	Timeout callback listener after timeout (seconds).
app_name	No	-a or --app_name fn_outbound_email	The app name to read if more than one app is defined in an app.config file.

Usage

The OAuth Utilities for SOAR app supplies various subcommands to help with OAuth support for apps in a SOAR environment.

```
$ oauth-utils
usage:
  $ oauth-utils <subcommand> ...
  $ oauth-utils -v <subcommand> ...
  $ oauth-utils oauth2_generate_refresh_token
  $ oauth-utils oauth2_generate_refresh_token -b
  $ oauth-utils oauth2_generate_refresh_token -c <path_to_config_file>/app.config -a
<app_name>
  $ oauth-utils -h
```

Tools to manage OAuth for IBM SOAR apps

optional arguments:

```
-h, --help          show this help message and exit
-v, --verbose       Set the log level to DEBUG
```

Utility: oauth2_generate_refresh_token

A utility to generate a refresh token for an OAuth 2.0 service (to be used with an IBM SOAR app).

```
usage: $ oauth-utils <subcommand> ...
  $ oauth-utils -v <subcommand> ...
  $ oauth-utils oauth2_generate_refresh_token
  $ oauth-utils oauth2_generate_refresh_token -b
  $ oauth-utils oauth2_generate_refresh_token -c <path_to_config_file>/app.config -a
<app_name>
  $ oauth-utils -h oauth2_generate_refresh_token
  [-h] [-c CONFIG_FILE] [-t TIMEOUT] [-b] [-a APP_NAME] [-p PORT]
  [-ci CLIENT_ID] [-cs CLIENT_SECRET] [-sc SCOPE] [-tu TOKEN_URL]
  [-au AUTH_URL]
```

A utility to generate a refresh token for an OAuth 2.0 service (to be used with an IBM SOAR app).

The parameters used for the OAuth 2.0 service can be taken either from an app.config file or manually from the command line.

(For further information please refer to the auth_utils documentation.)

optional arguments:

```
-h, --help          show this help message and exit
-c CONFIG_FILE, --config_file CONFIG_FILE
                    Location of app.config file
-t TIMEOUT, --timeout TIMEOUT
                    Timeout callback listener after timeout (seconds)
-b, --browser       Use browser and listener
-a APP_NAME, --app_name APP_NAME
                    Specify the app name
-p PORT, --port PORT
                    Specify port for callback url and listener
-ci CLIENT_ID, --client_id CLIENT_ID
                    Specify OAuth 2.0 application client ID
-cs CLIENT_SECRET, --client_secret CLIENT_SECRET
                    Specify OAuth 2.0 application client secret
-sc SCOPE, --scope SCOPE
                    Specify OAuth 2.0 application scope
-tu TOKEN_URL, --token_url TOKEN_URL
                    Specify OAuth 2.0 application token url
```

```
-au AUTH_URL, --auth_url AUTH_URL  
Specify OAuth 2.0 application authorization url
```

Configure OAuth 2.0 credentials

To use the `oauth2_generate_refresh_token` utility, set up an app or project for an OAuth 2.0 identity provider service from which you can get the required configuration settings, such as:

```
client_id  
client_secret  
scope  
token_url  
auth_url
```

The setup procedure varies depending on the provider. This document provides examples for 2 well known services [Google Gmail](#) and [Microsoft Outlook 365](#). These examples can be used to send email using SMTP.

Google Gmail

Endpoints

Google Authorization endpoint - used by client to obtain authorization from the resource owner.

```
auth_url=https://accounts.google.com/o/oauth2/auth
```

Google Token endpoint - used by client to exchange an authorization grant or refresh token for an access token.


```
token_url=https://accounts.google.com/o/oauth2/token
```

Create the new project.

- As the SMTP email user, log in to [Google cloud](#) and create a Google cloud project.
- Give your project a name, change the project ID if needed, and click the [Create](#) button.


☰ Google Cloud

New Project


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

[MANAGE QUOTAS](#)

Project name *
Outbound Email


Project ID *
outbound-email-356413 

Project ID can have lowercase letters, digits or hyphens. It must start with a lowercase letter and end with a letter or number.

Location *
 No organisation [BROWSE](#)

Parent organisation or folder

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

 **Create Project: Outbound Email** 16 minutes ago

[SELECT PROJECT](#)

Configure OAuth Consent Screen.

- In the APIs and Services section, click OAuth Consent Screen and set the user type to **External**. Click on **Create**.

The screenshot shows the Google Cloud console interface. At the top, there is a blue header with the Google Cloud logo, 'Outbound Email' dropdown, and a search bar. Below the header, the left sidebar is titled 'API APIs and services' and contains a list of options: 'Enabled APIs and services', 'Library', 'Credentials', 'OAuth consent screen' (highlighted), 'Domain verification', and 'Page usage agreements'. The main content area is titled 'OAuth consent screen' and contains the following text: 'Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.' Below this is the 'User Type' section with two radio button options: 'Internal' (unselected) and 'External' (selected). The 'Internal' option has a help icon and text: 'Only available to users within your organisation. You will not need to submit your app for verification. [Learn more about user type](#)'. The 'External' option also has a help icon and text: 'Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)'. At the bottom of the main content area is a blue 'CREATE' button.

- Enter a name for your application and provide an email address where Google might contact you.

The screenshot shows the 'Edit app registration' page in the Google Cloud console. The top header is identical to the previous screenshot. The left sidebar is also identical. The main content area is titled 'Edit app registration' and features a progress indicator with four steps: 1. OAuth consent screen (active, marked with a red exclamation point), 2. Scopes, 3. Test users, and 4. Summary. Below the progress indicator is the 'App information' section. It includes a sub-header 'App information' and a descriptive text: 'This shows in the consent screen, and helps end users know who you are and contact you'. There are two input fields: 'App name *' with the value 'Outbound Email' and a description 'The name of the app asking for consent'; and 'User support email *' with the value 'outbemail@gmail.com' and a description 'For users to contact you with questions about their consent'.

APIs and services

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

Edit app registration

Application Terms of Service link
Provide users a link to your public Terms of Service

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

+ ADD DOMAIN

Developer contact information

Email addresses *
outbemail@gmail.com ✕

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

SAVE AND CONTINUE CANCEL

- Provide one or more Scopes for Google APIs. Click the **Add Or Remove Scopes** button and add `https://mail.google.com/` to the list of scopes. Click **Save** and **Continue**.

Manually add scopes

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

ADD TO TABLE

UPDATE

API APIs and services

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

Edit app registration

Scopes EDIT

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

Test users EDIT

0 users (0 test, 0 other) / 100 user cap ?

Filter Enter property name or value ?

User information
No rows to display

[BACK TO DASHBOARD](#)

- Since a User Type of **External** is used, you need to add a user who has access to the app. In this example, the test user is the same as the app user. Click **Add Users**, and add the user. Click **Save** and **Continue**.

Test users

[+ ADD USERS](#)

Filter Enter property name or value ?

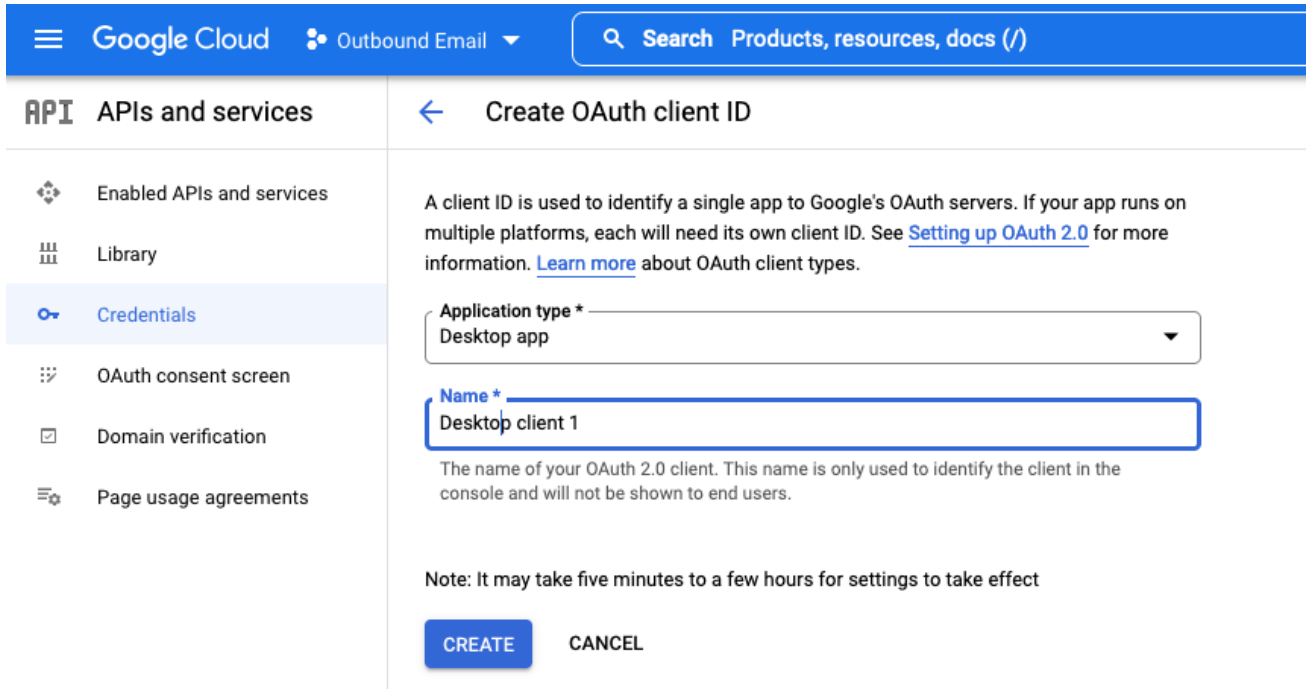
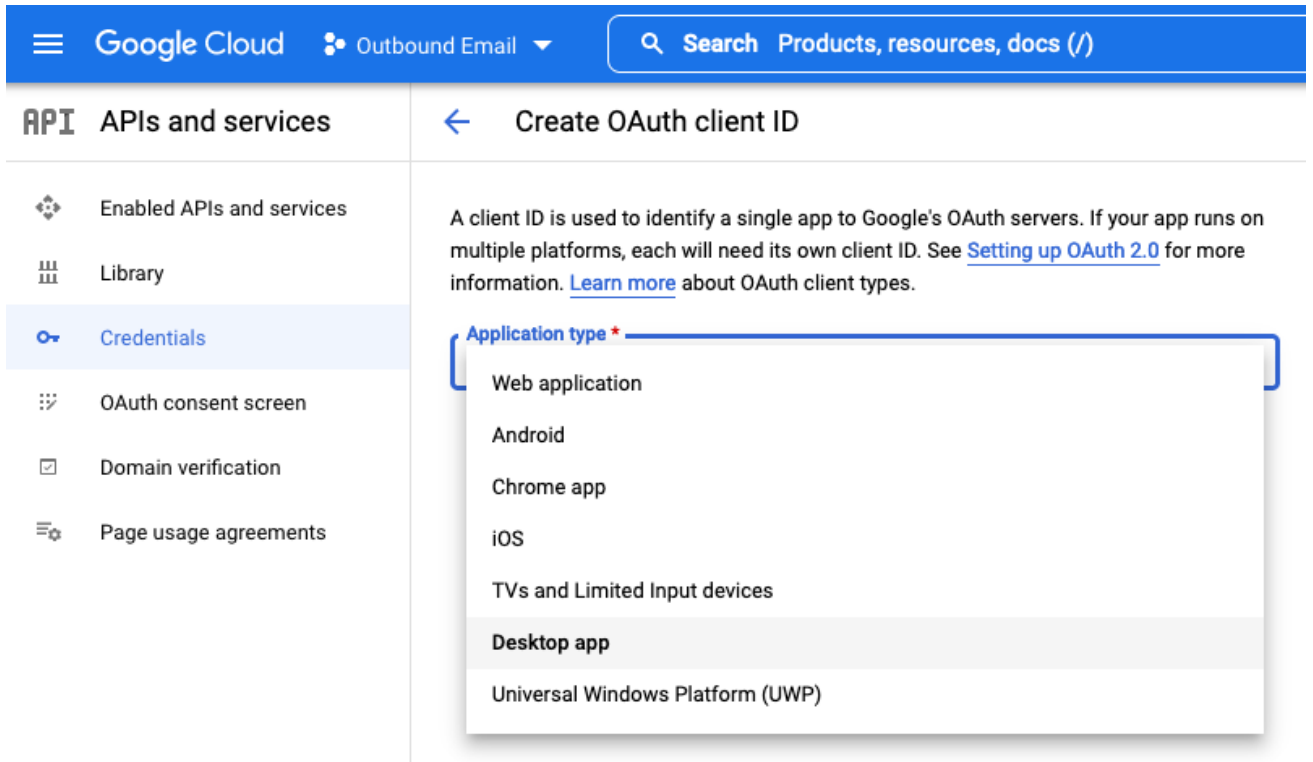
User information	
outbemail@gmail.com	🗑️

Configure Credentials.

- In the APIs & Services section, click **Credentials** and then click **Create credentials**.

The screenshot shows the Google Cloud console interface. At the top, there is a blue header with the Google Cloud logo, 'Outbound Email' dropdown, and a search bar containing 'Search Products, resources, docs (/)'. Below the header, the left sidebar is titled 'APIs and services' and contains several menu items: 'Enabled APIs and services', 'Library', 'Credentials' (which is highlighted in blue), 'OAuth consent screen', 'Domain verification', and 'Page usage agreements'. The main content area is titled 'Credentials' and includes a '+ CREATE CREDENTIALS' button and a 'DELETE' button. Below this, there is a text instruction: 'Create credentials to access your enabled APIs. [Learn more](#)'. The 'API keys' section shows a table header with 'Name' and 'Creation date' (with a downward arrow), and a message 'No API keys to display'. The 'OAuth 2.0 Client IDs' section also shows a table header with 'Name' and 'Creation date' (with a downward arrow).

- Select **OAuth Client ID** to create a new client ID then select **Desktop app**. The client ID is used to verify application identify to Google's OAuth servers.



- When the OAuth client is created you are presented with a screen showing your client ID and secret.

OAuth client created

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



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

Your Client ID

337895628616-h4epvnbqv5946aun1u9qg7kqp6tu5c1j.apps.googleusercontent.com



Your Client Secret

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



↓ DOWNLOAD JSON

OK

You can now add these credentials and scope to an app.config file or alternatively use as command-line arguments for the `oauth2_generate_refresh_token` utility.

```
client_id=337895628616-h4epvnbqv5946aun1u9qg7kqp6tu5c1j.apps.googleusercontent.com
client_secret=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
scope=https://mail.google.com/
token_url=https://accounts.google.com/o/oauth2/token
auth_url=https://accounts.google.com/o/oauth2/auth
```

- Ensure you are logged out of any Google accounts.
- Execute the `oauth2_generate_refresh_token` utility using the new credentials as command line arguments.

```
$ oauth-utils oauth2_generate_refresh_token -ci=337895628616-
h4epvnbqv5946aun1u9qg7kqp6tu5c1j.apps.googleusercontent.com -cs=GOCSPX-
3QE_9IPDjkAMvup3xoLFkaUfb-UX -sc=https://mail.google.com/ -
tu=https://accounts.google.com/o/oauth2/token -
au=https://accounts.google.com/o/oauth2/auth
```

Running from command line.

Using OAuth2 discrete settings from command-line arguments.

To authorize a token, copy the following URL into a browser and follow the directions then enter the generated callback URL below:

```
https://accounts.google.com/o/oauth2/auth?
state=6a3290f368de76e0dc83d7a380ca91e8950a57ff2aabc94c706b3418743e2743&scope=https%3A%
2F%2Fmail.google.com%2F&client_id=337895628616-
h4epvnbqv5946aun1u9qg7kqp6tu5c1j.apps.googleusercontent.com&response_type=code&respons
e_mode=query&redirect_uri=https%3A%2F%2Flocalhost%3A8080%2Fcallback
```

Enter callback URL:

- Enter the URL in a browser, log in as the SMTP email user, and follow the directions by clicking **Continue** in each presented screen.

 Sign in with Google

Sign in

to continue to **Outbound Email**

Email or phone

[Forgot email?](#)

[Create account](#)


Next

 Sign in with Google

Outbound Email wants access to your Google Account

 outbemail@gmail.com

When you allow this access, **Outbound Email** will be able to

 Read, compose, send and permanently delete all your email from Gmail. [Learn more](#)

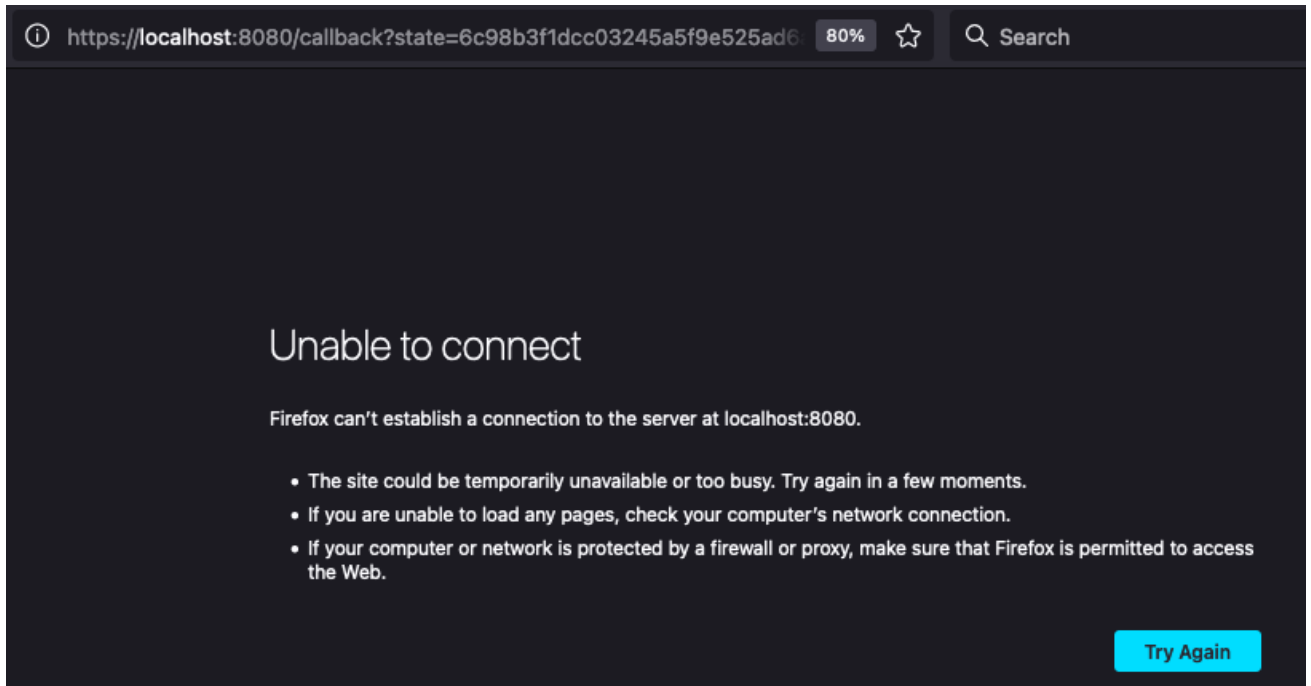
Make sure that you trust Outbound Email

You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

See Outbound Email's privacy policy and Terms of Service.

- Eventually the user is presented with an **Unable to connect** message in the browser and a callback URL in the browser location window.



- Enter the callback address from the browser location window on the command line.

```
Enter callback URL: https://localhost:8080/callback?
state=6c98b3f1dcc03245a5f9e525ad6ac11983dc26dadebeb497492462aa166e19f0&code=4/0AdQt8qj
MgTn0h42tSkJRafz_uNmJiv0LsanTp9NUoj1YDBRr7oW94nqXADDHD1BIe6Bz6g&scope=https://mail.goo
gle.com/
```

```
refresh_token=1//07JEwfJ_7KNbWCgYIARAAGAcSNwF-
L9IrH71Z4sT_VsmL4k03rSaw4fEKKTpetFVhf6dfxDBuPxqB-KkE2DJEo_8Xo1h0kfP_RyY
```

- Add the resultant `refresh_token` to the `app.config` file for the required app.

NOTE: In the example, we used a test user with User Type of `External`. Selecting User Type `Internal` allows the application to access the Google API without having to go through the verification process.

See: [Setting up OAuth 2.0 with Google Cloud](#)

Microsoft Outlook 365

Endpoints

Microsoft Authorization endpoint - used by client to obtain authorization from the resource owner.

```
auth_url=https://login.microsoftonline.com/<tenant_id>/oauth2/v2.0/authorize
```

Microsoft Token endpoint - used by client to exchange an authorization grant or refresh token for an access token.

```
token_url=https://login.microsoftonline.com/<tenant_id>/oauth2/v2.0/token
```

App Registration

- As the SMTP email user, log in to the [Microsoft Azure Portal](#) and authenticate.
- Under [Azure services](#), click on [Azure Active Directory](#).



Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

[View](#) [Learn more](#)

- Click on [App Registrations](#) > [New Registration](#).

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation menu. The main heading is 'outbemail | App registrations' under 'Azure Active Directory'. A left-hand navigation pane lists various options, with 'App registrations' selected. The main content area has tabs for 'New registration', 'Endpoints', 'Troubleshooting', 'Refresh', 'Download', and 'Preview'. A 'New registration' notification banner is displayed. Below the banner, there are tabs for 'All applications', 'Owned applications', and 'Deleted applications'. A search bar is present with the placeholder text 'Start typing a display name or application (client) ID to filter these r...' and an 'Add filters' button.

- Give your application a name. For [Redirect URI](#) select [Web](#) and enter <https://localhost:8080/callback>. Click [Register](#).

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

Home > outbemail >

Register an application

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

Outbound Email ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (outbemail 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 ✓ https://localhost:8080/callback ✓

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

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

Register

- Copy and save the Application (client) ID and Directory (tenant) ID locally.

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

Home > outbemail >

Outbound Email

Search (Cmd+/) Delete Endpoints Preview features

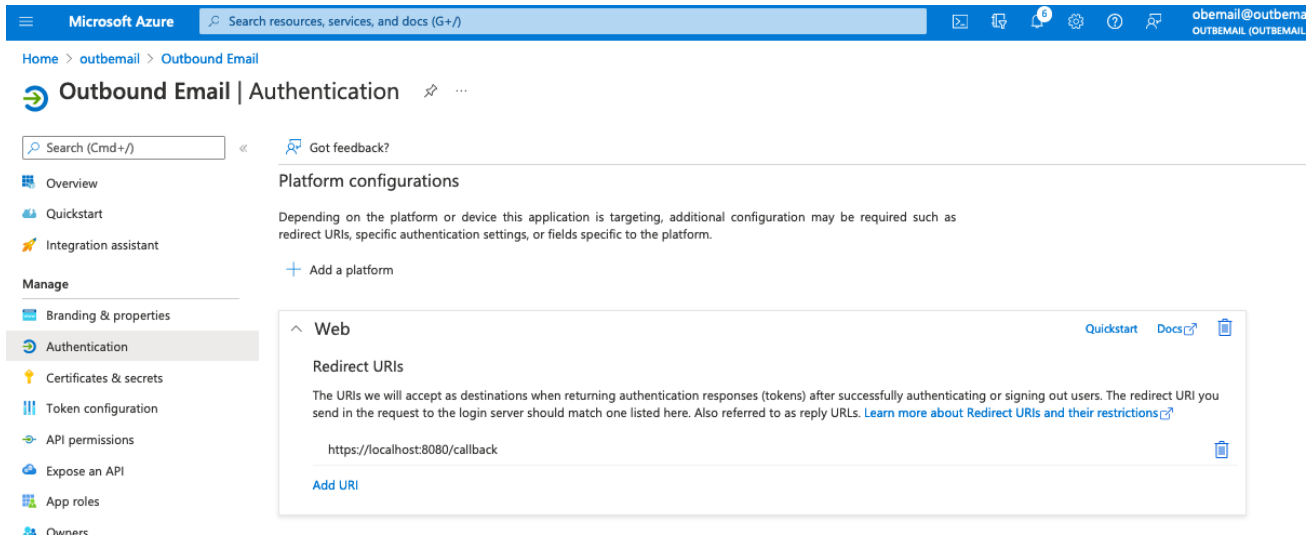
- Overview
- Quickstart
- Integration assistant
- Manage
- Branding & properties
- Authentication

Essentials

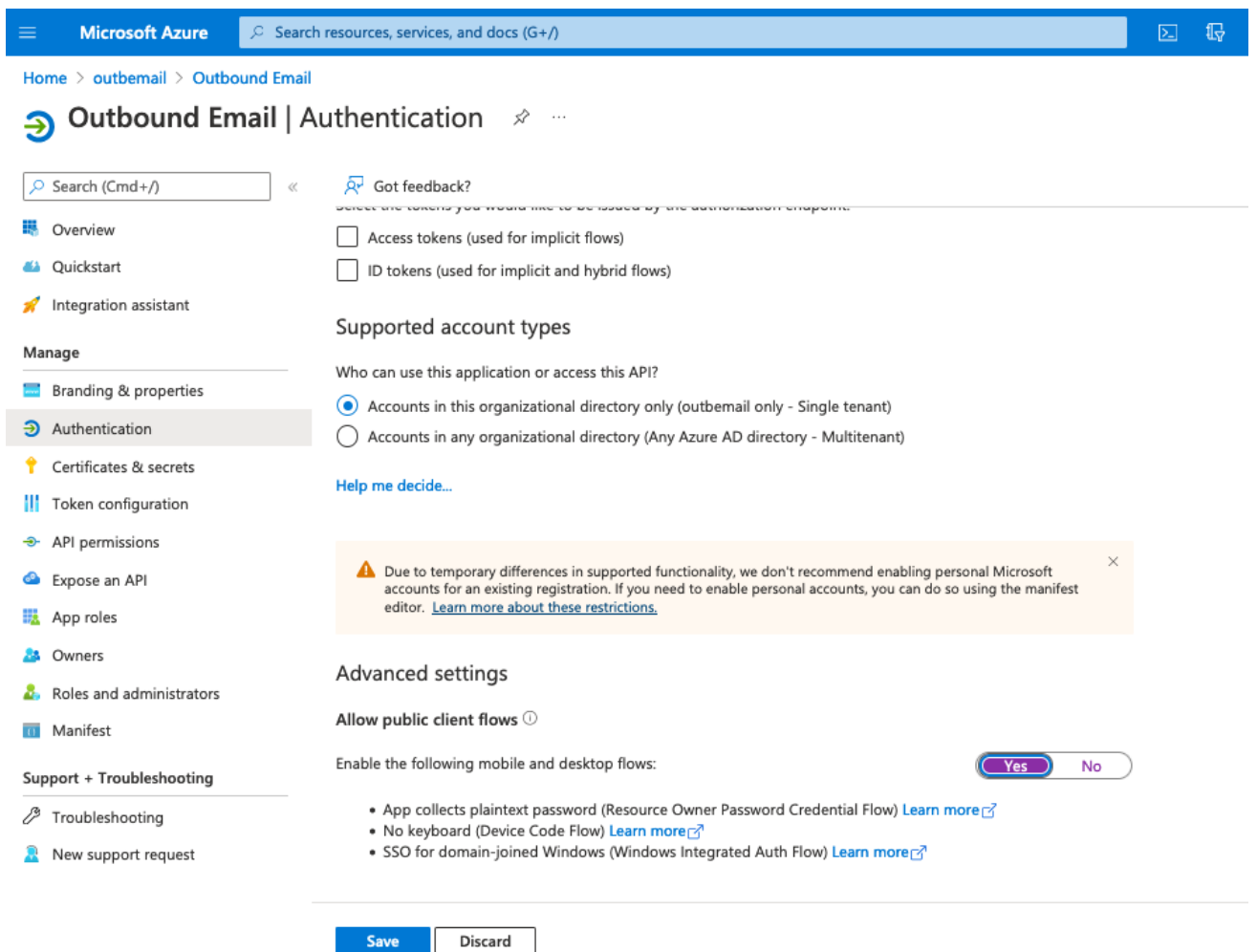
Display name	: Outbound Email	Client credentials	: Add a certificate or secret
Application (client) ID	: 1c22e8d1-daf0-407e-b576-0778cc3cd812	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: 17f997ff-bb96-439e-9006-1c3492d82719	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: c06fa6c3-5dd0-48c9-9a4b-7edbf1904269	Managed application in L...	: Outbound Email
Supported account types	: My organization only		

Authentication

- Under **Manage** on the left menu, select **Authentication**.

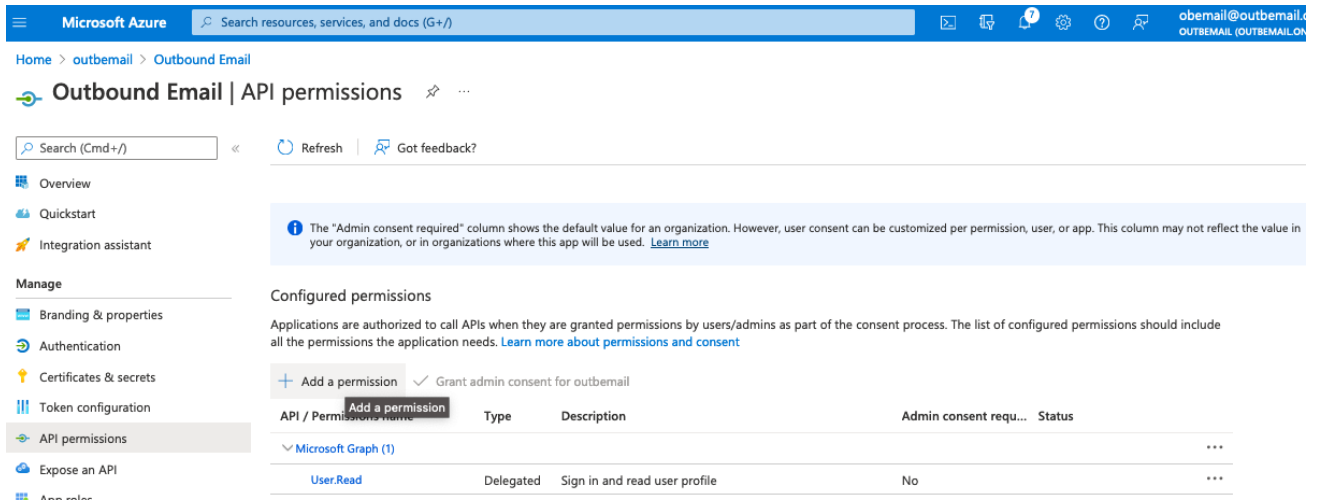


- Select **Yes** for **Enable the following mobile and desktop flows** then click **Save**.



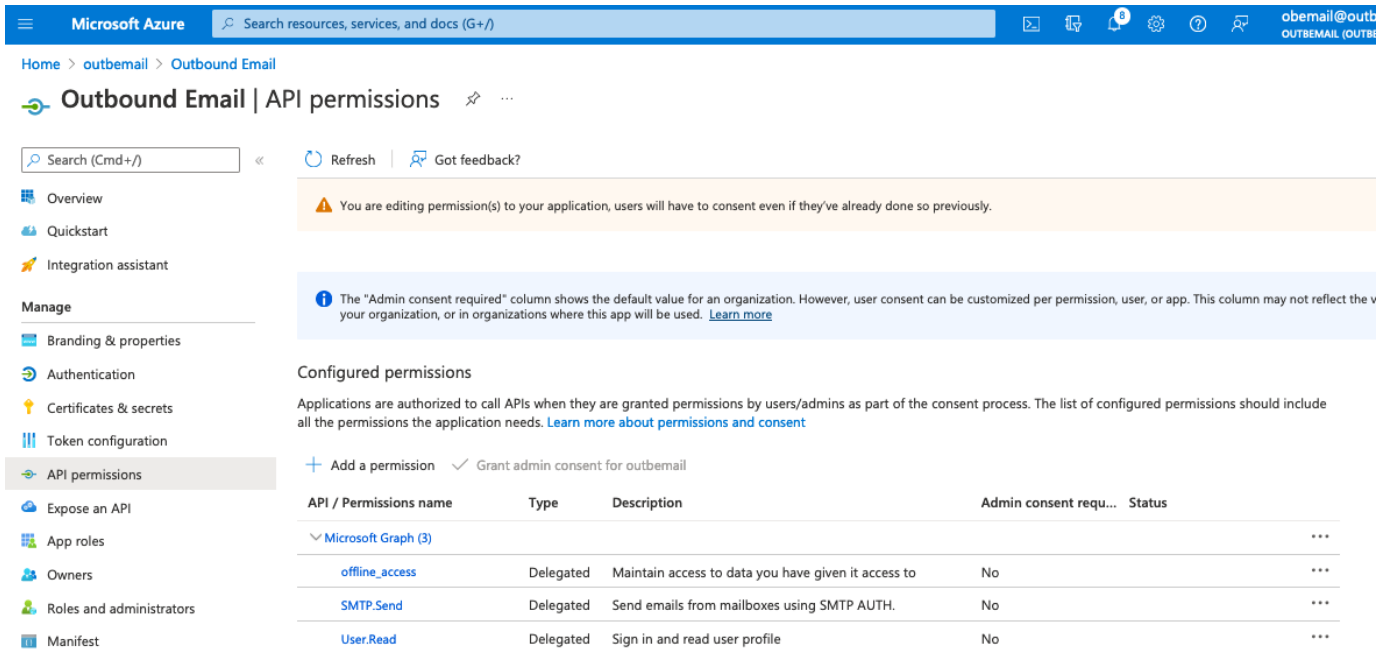
API Permissions

- On the left side under **Manage**, select **API Permissions**.
- Click **Add a permission**.



- On the Request API permission screen, select Microsoft Graph.
- In Graph API, choose Delegated permissions.
- Add the following permissions.

```
offline_access
SMTP.Send
```



- You need an admin user account to Grant admin consent for <user> to enable these permissions.

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

Home > Outbound Email > Outbound Email

Outbound Email | Permissions

Enterprise Application

Refresh Review permissions Got feedback?

Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the admin integrating an application and enabling self-service access or assigning users directly to the application. [Learn](#)

To request additional permissions for this application, use the [application registration](#).

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to grant admin consent.

Grant admin consent for outbemail

Admin consent User consent

Permissions requested

Review for your organization

Outbound Email

[App info](#)

This application is not published by Microsoft.

This app would like to:

- ✓ Maintain access to data you have given it access to
- ✓ Sign in and read user profile
- ✓ Send emails from mailboxes using SMTP AUTH.

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel Accept

Create client secret

- On the left side under **Manage**, select **Certificate and secrets**.
- Click **New client secret**.

- Enter a name for the client secret.

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

Home > Outbound Email

Outbound Email | Certificates & secrets

Search (Cmd+) Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

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	Secret ID
New client secret			

Add a client secret

Description:

Expires:

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

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

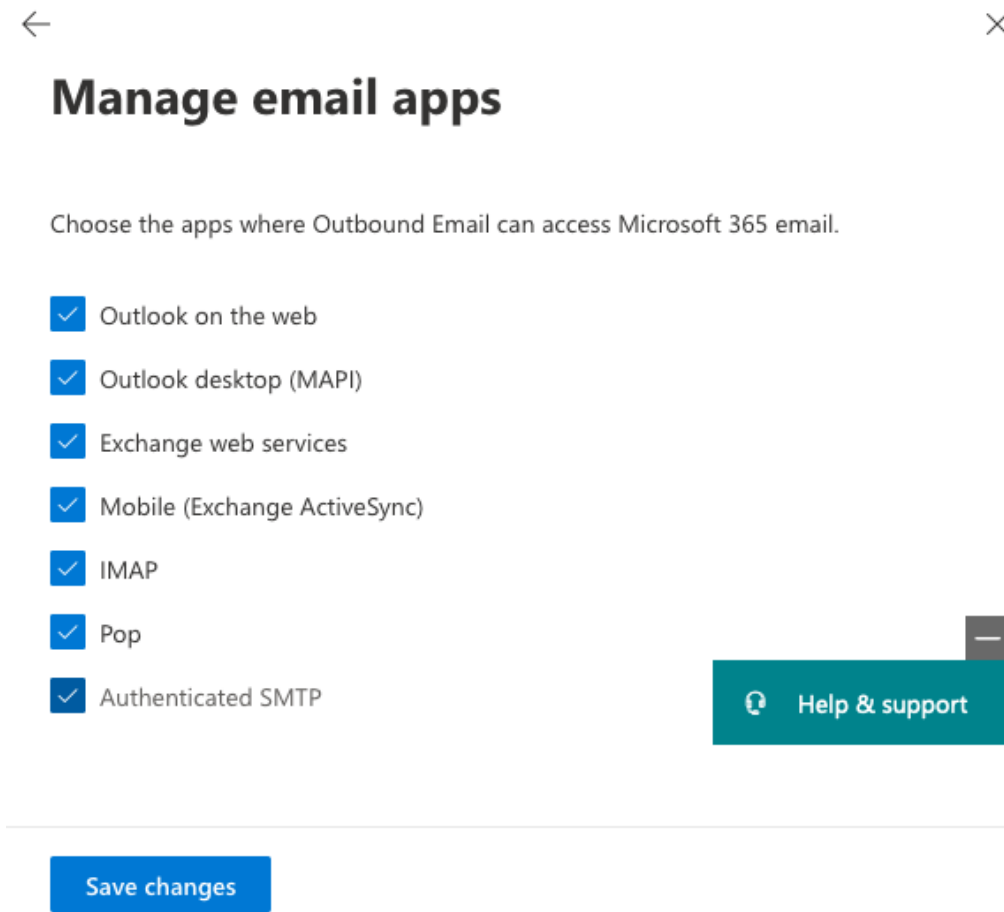
+ New client secret

Description	Expires	Value	Secret ID
OB Secret	1/19/2023	OT48Q~enmvy5HpCpub2maQxCVdhvEg...	4b4a148d-0e07-4c84-b22c-058d446d58ea

- Save the secret **Value** locally. This is be used as the value for the `client_secret` setting/argument.

Authenticated SMTP

- Log in to [Microsoft 365 admin center](#) as an admin user and go to [Users > Active users](#).
- Select the SMTP user, and click [Mail](#).
- In the Email apps section, click [Manage email apps](#).
- Verify the [Authenticated SMTP](#) setting is checked.
- Click [Save changes](#).



You can now add credentials and scope obtained above to an `app.config` file or alternatively use as command line arguments for the `oauth2_generate_refresh_token` utility.

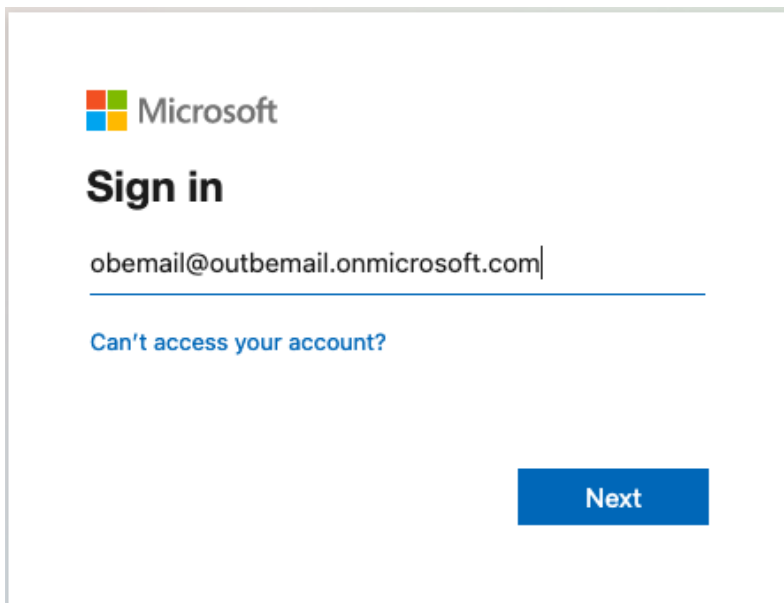
```
client_id=1c22e8d1-daf0-407e-b576-0778cc3cd812
client_secret=0T48Q~enmvy5HpCpub2maQxCVdhvEgowkT1WBbGc
scope=offline_access https://outlook.office365.com/SMTP.Send
token_url=https://login.microsoftonline.com/c06fa6c3-5dd0-48c9-9a4b-7edbf1904269/oauth2/v2.0/token
auth_url=https://login.microsoftonline.com/c06fa6c3-5dd0-48c9-9a4b-7edbf1904269/oauth2/v2.0/authorize
```

- Ensure you are logged out of any Microsoft accounts.
- Using the browser mode option, execute the `oauth2_generate_refresh_token` utility using the new credentials in the `app.config` file.

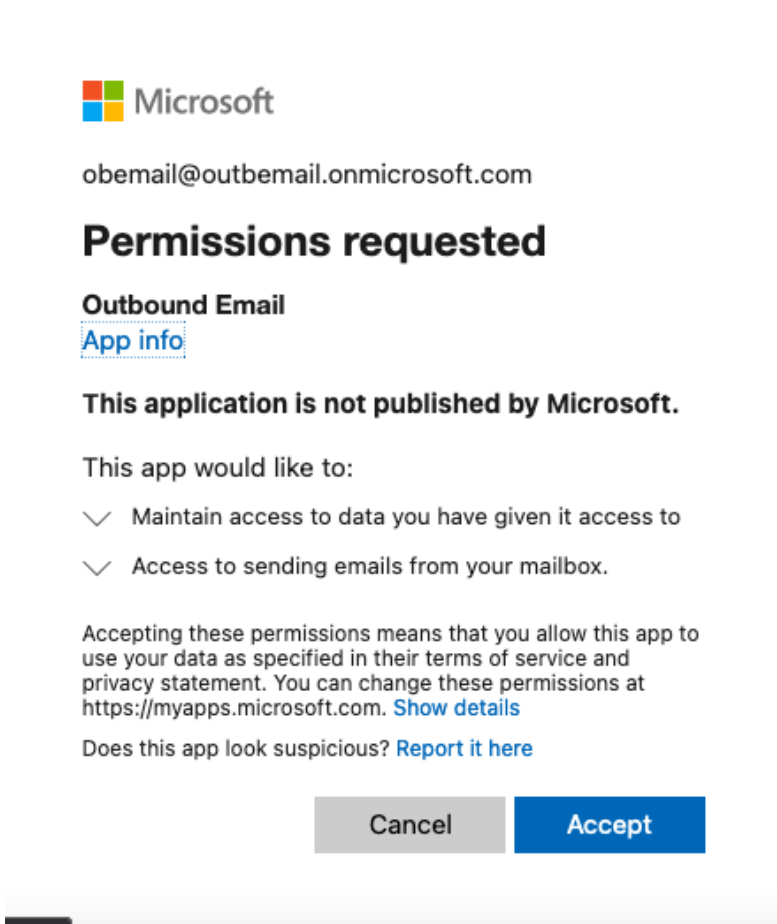
```
$ oauth-utils oauth2_generate_refresh_token -b
Running with callback listener and web browser.
Reading OAuth2 settings from app.config file /Users/johnpren/.resilient/app.config.
/Users/johnpren/ws/venv_3.6.8_oauth-utils/lib/python3.6/site-
packages/werkzeug/serving.py:469: CryptographyDeprecationWarning: Python 3.6 is no
longer supported by the Python core team. Therefore, support for it is deprecated in
cryptography and will be removed in a future release.
  from cryptography import x509
Starting callback listener on port 8080.
Starting browser.
```

A web browser is launched, and the rest of the process is be completed using the browser.

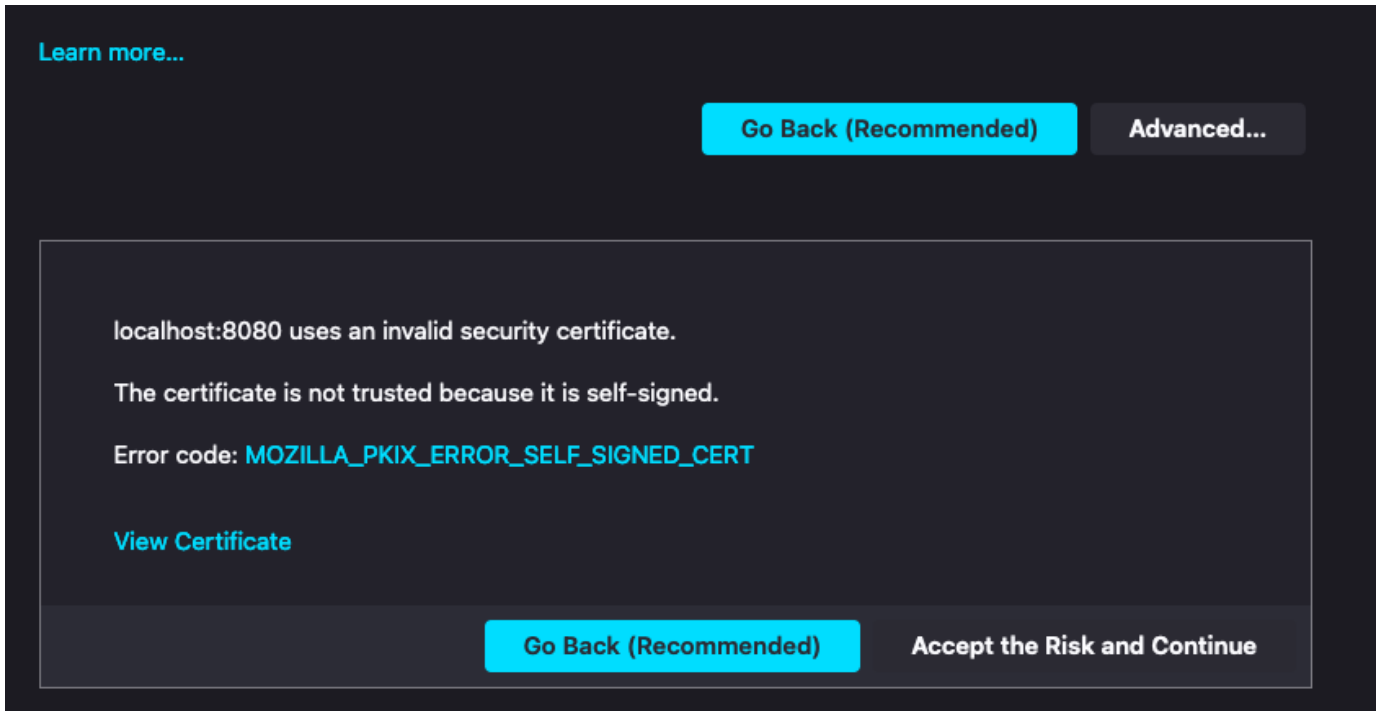
- In the browser, sign in as the SMTP email user.



- Follow the directions by clicking **Accept**.



- The browser is redirected to the callback URL (default port 8080) and is processed by a local listener.
- If you are satisfied that it is redirected to the correct location, click **Accept the Risk and Continue**.



A refresh token is displayed in the browser.

Refresh token

```
refresh_token= 0.AXkAw6ZvwnBdyUiaS37b8ZBCadHolhzw2n5AtXYHeMw82BKUAPg-AgABAAEAAAD--
DLA3V07Qrddgj7WevrAgDs_wQA9P_2z5Uk2Om9r6Vc4PgFNWU3TQ8g2xx5kGD9NhWrYrvn2Cc3IjBXzbVJdvOfUGHzPYWuY9UYi3lobch8XfHDL0tt3l84EhkpprarXDzsX3uyLZCg5mYTIAXvmVksOJTFQ_ZPq7E
6TTA4oFzNe-GWgV78sd0Y4o3TDIYY1CMKyxPnSM7Bwa3L7RAVlqgB4NZR0P9Zknqx7WB14I63dGOleTCz6IADxWV9nA4-
az7tqjOe88CacJnKRRzBUOFEITSNrwDz2hniFRvxgNP_duPJ3t0leLZCH209diAQFhCwM2D7fXzltvin6cQENt3g1Ll_meFmJWkjzJ0mMw1VQ9mlsKm2asES9ca7-
zVE6ME0GDLK9s6U8MwRCiSuROlmmUajUF6eWmiFM3yEFU3z2MC8kv9j6Gj6jxyek2YNiWzRoIZ-
ei2MluLBKrx5TLhKpSz6j_P0WiFW1BH2bH2GSPobTgJnJXruQs3S3WGpFM0SXFtWYyxFCCbU1qsgnxXp3miEKVGFQAQBw26pirkYKR0tX_m7UB01QxCqN8eFwxpRENQpX01xEIXQbACwQQZyppEt1aQ2rXtgJ4tJfI
XwXiKUHMapYB5XPoVXrtB0KE7GwgSETxltT4H5T74OUX2-RkcK7iNjB7Gta1eTb1JXH3coQhzWB0SCN1qkOwqtrTpf812DQTi5Pz6eYLMg7DAK9fDBE7_E82wW
```

- Add the resultant `refresh_token` to the `app.config` file for the required app.

See: [Using OAuth 2.0 with Microsoft for Office 365 users](#)

Troubleshooting & Support

Refer to the documentation listed in the Requirements section for troubleshooting information.

For Support

This is a IBM Community provided package. Please search the Community ibm.biz/soarcommunity for assistance.