OAuth2-enabled email proxy application

O2Popper User's Guide

macOS Version

for Version 3.0.1 (Build: 2022-12-26)

MURATA Yasuhisa

NIPS Technical Division

Introduction

This application was developed for the purpose of enabling continuous use of mail software and systems that do not support OAuth2.

There are also erroneous transmission prevention functions.

I hope you can use it.

Notice

To use this application for the first time, it is now necessary to obtain "Client ID" and "Client Secret" for OAuth2. (The one prepared by the author is because the limit of 100 free users has been reached.)

Please refer to "How to get Client ID and Client Secret" on the website of this application.

Note:

Accounts belonging to the same organization as the author are not eligible.

Contents

1. Environment
2. Installation
3. Options
4. New functions

Environment

I have confirmed the operation on macOS 11 Big Sur.
It may not work with older versions

I have confirmed that it works in combination with the following mail clients.

- Apple Mail
- Thunderbird

Installation

You can download the installer from the following URL.

https://www.nips.ac.jp/~murata/o2popper/downloads/

Before installing this app, open the "Terminal" app and
Execute "sudo spctl --master-disable" to give permission to execute the downloaded
application. (You will be prompted to enter the password.)

After installation, execute "sudo spctl --master-enable" to restore the original state.

When you open the downloaded dmg file, you will see "O2Popper" icon.
Place it in the "Applications" folder by dragging and dropping.
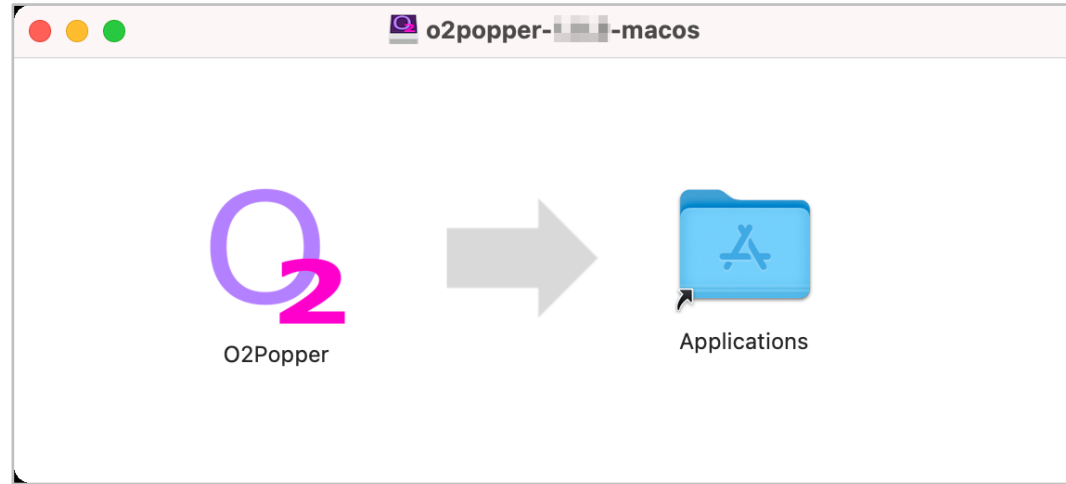
Next, double-click "O2Popper" placed in the "Applications" folder to start this application.

If the following screen is displayed, the downloaded application is not allowed to be executed. Click "Move to Trash" and execute "sudo spctl --master-disable" again.

"O2Popper" is damaged and can't be opened. You should move it to the Trash.

Firefox downloaded this file today at 14:49 from **www.nips.ac.jp**.

Move to Trash   Cancel

Click "Open" when the following screen is displayed.

"O2Popper" is an app
downloaded from the Internet.
Are you sure you want to open it?

Firefox downloaded this file today at
14:49 from **www.nips.ac.jp**.

Open

Show Web Page

Cancel
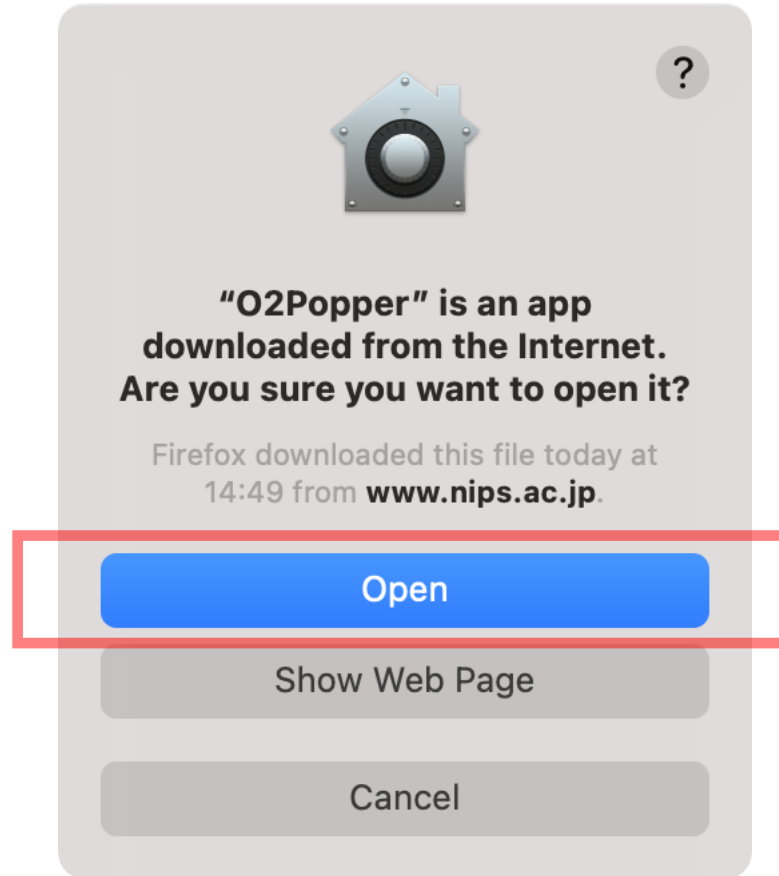
When this application is started normally, the icon of this application will be displayed in the system tray at the upper right of the screen.

If you want to start this application automatically when you log in, open "Users & Groups" in "System Preferences…" of macOS and add it to "Login Items".
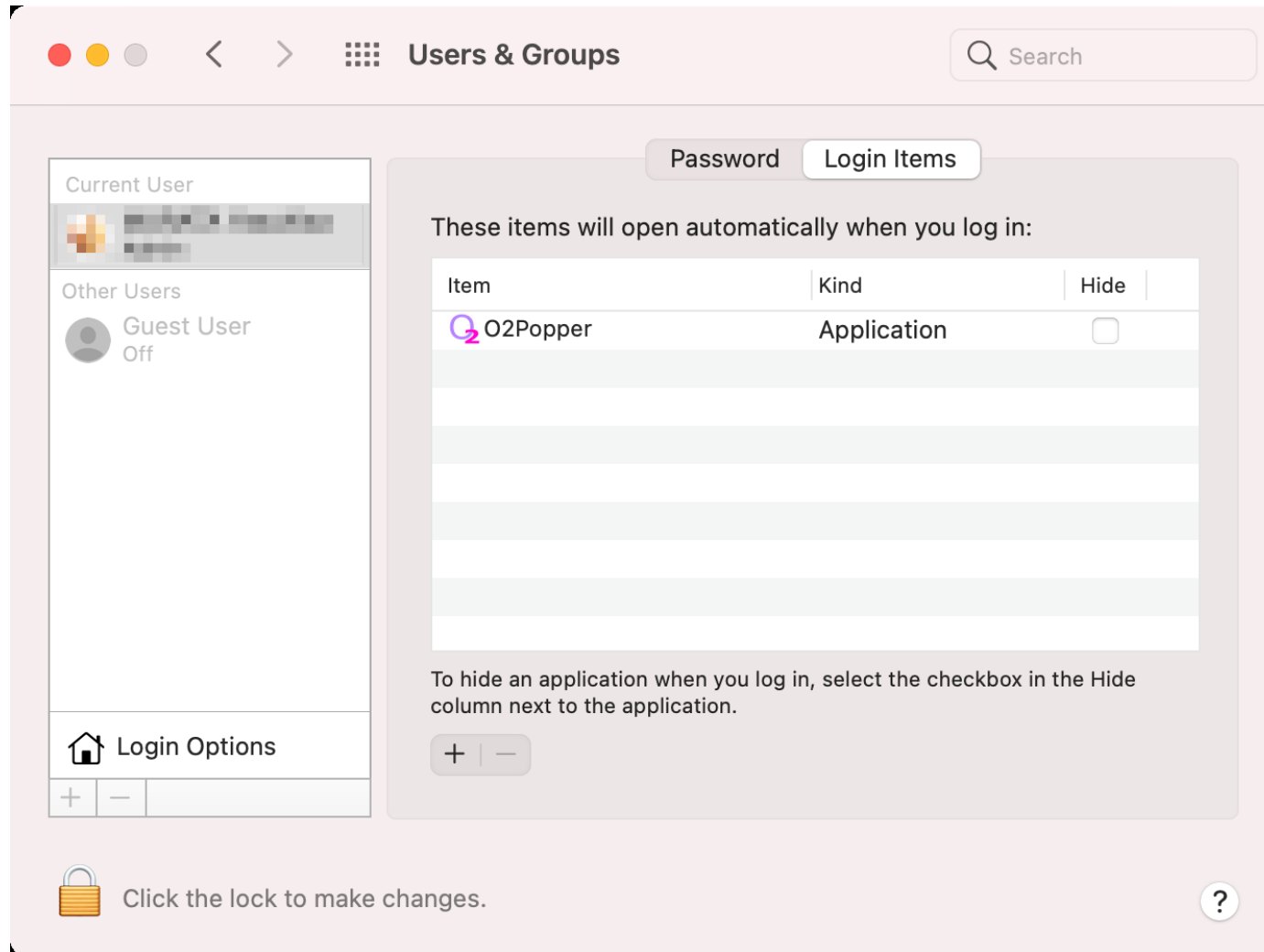
You need to make the initial settings first.
Click the icon of this application to display the menu. Select "Settings..." in this.

The setting screen is as follows.
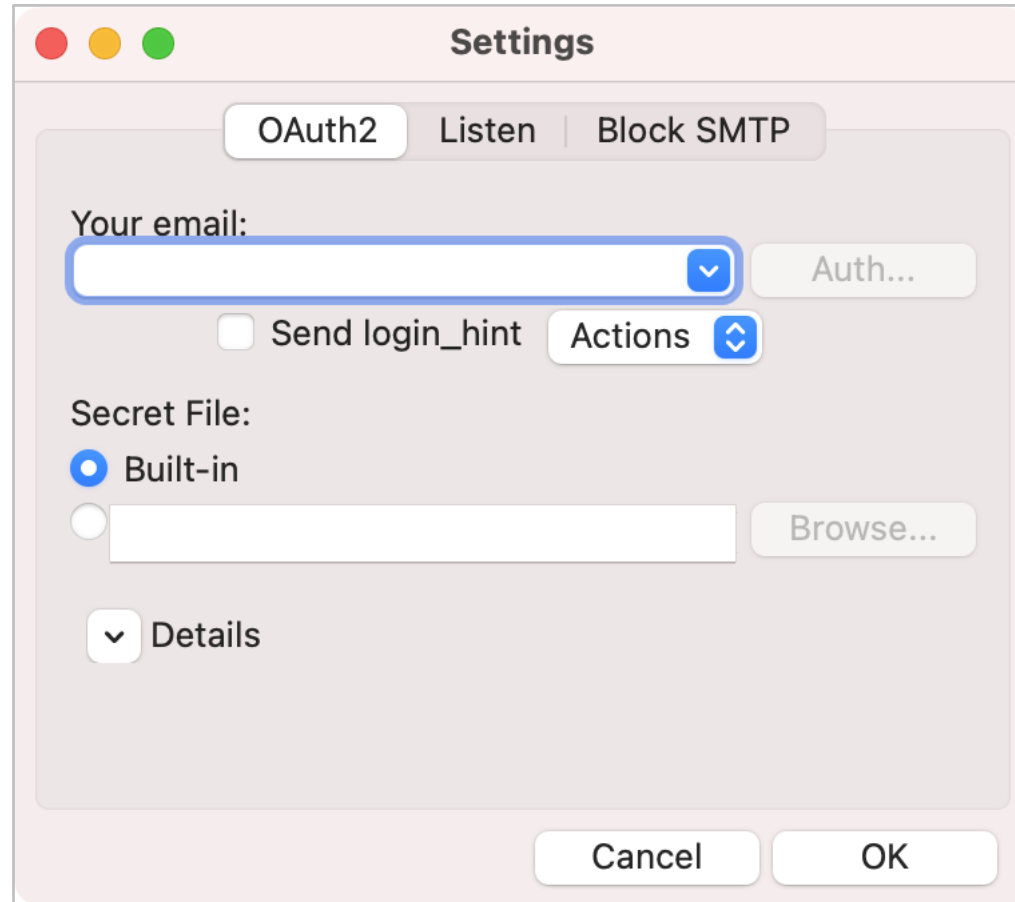
If you prepare a secret file for OAuth2 yourself, specify the file as follows.
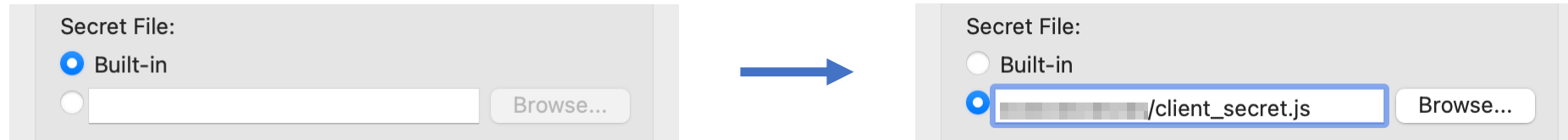
You can also enter "Client ID" and "Client Secret" directly as follows.

If you want to use the secret file prepared by the author, leave it as "Built-in".

When authorizing OAuth2, if you use the secret file prepared by the author,
"Google hasn't verified this app"
may be displayed.

Enter your email address and click the "Auth…" button.
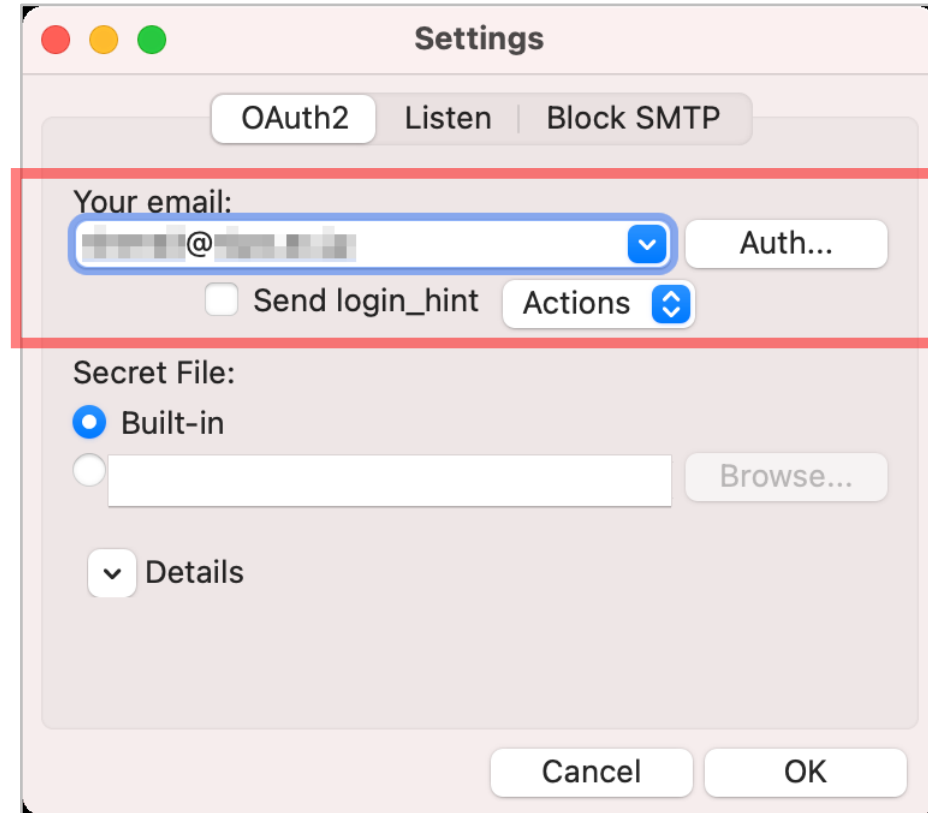
Note: If you check "Send login_hint", you can skip the "Choose an account" screen that appears after this.

The OS standard web browser starts and the Google account authentication screen is displayed.
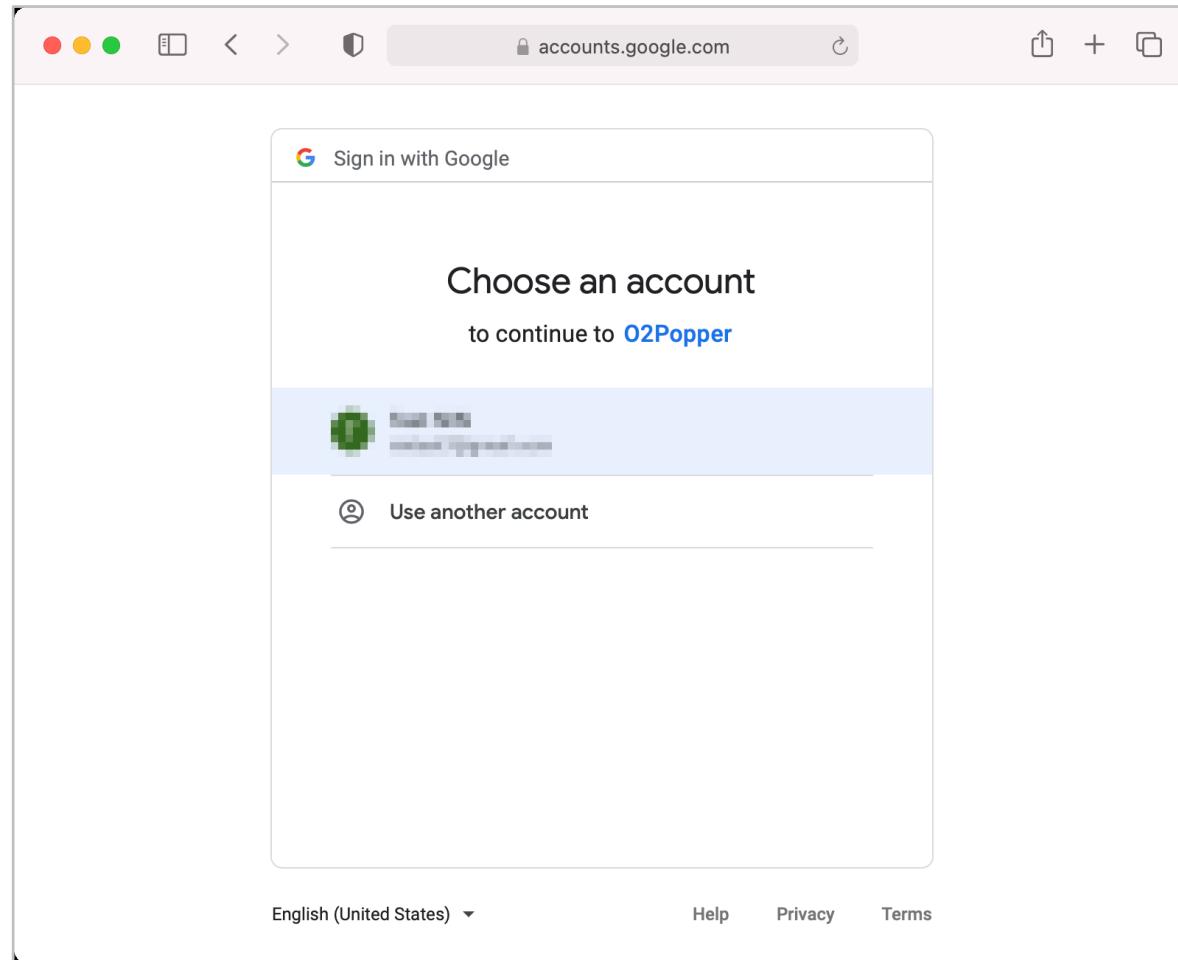
If the following screen is displayed after the Google account has been authenticated, click the "Advanced" link.
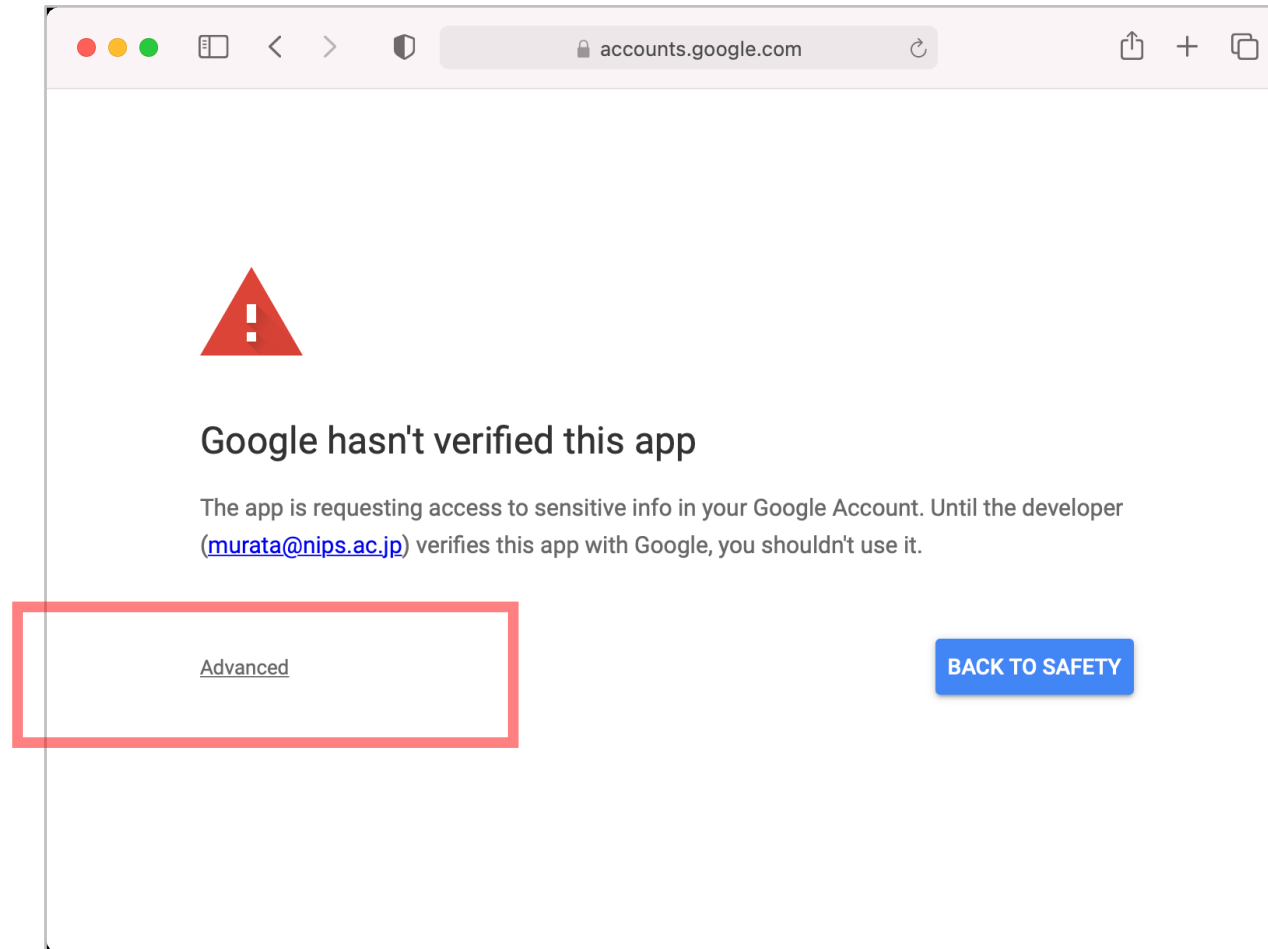
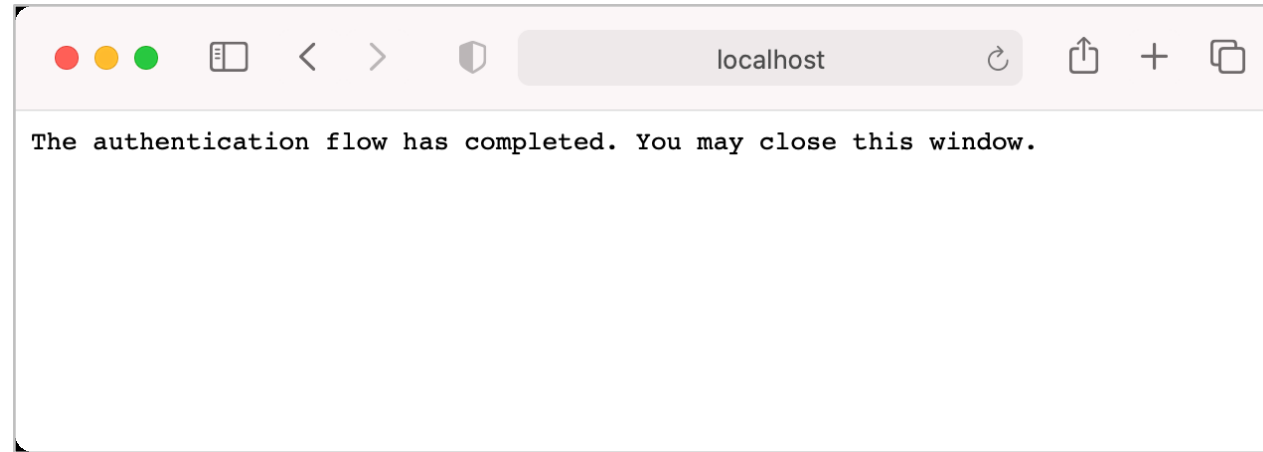After clicking the "Advanced" link, click the "Go to O2Popper (unsafe)" link at the bottom of the screen.
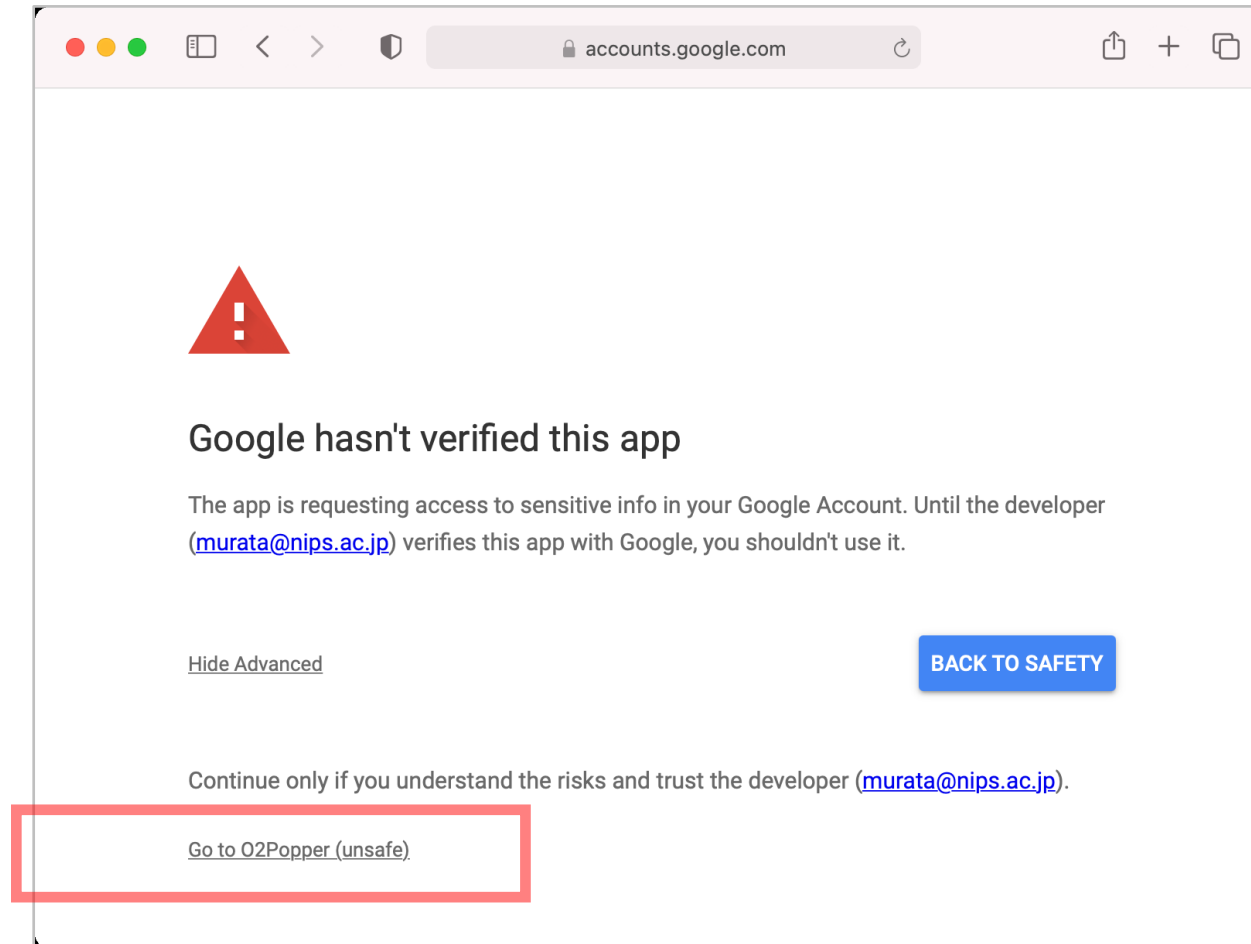
If the following screen is displayed, click the "Allow" button.
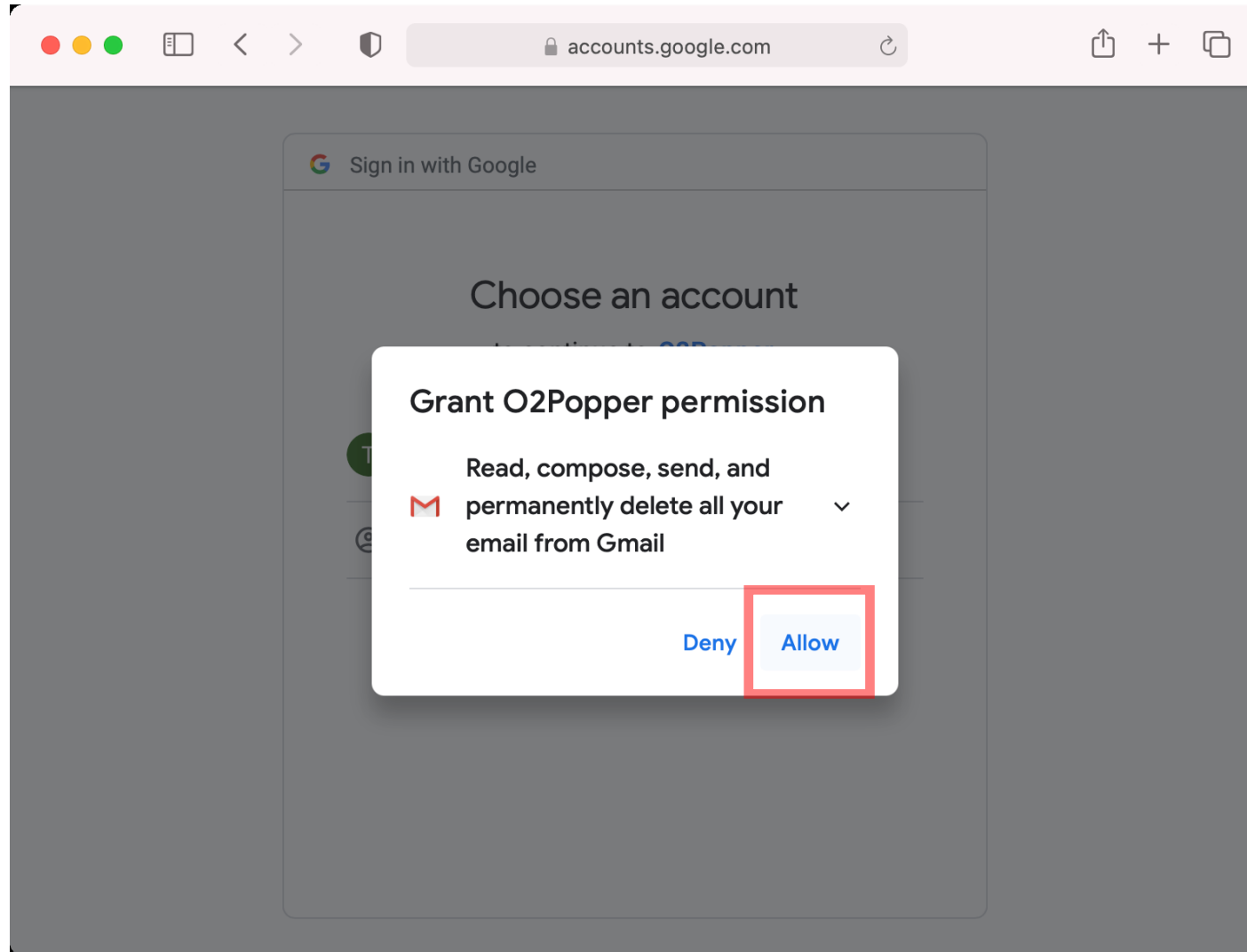
If the following screen is displayed, click the "Allow" button.
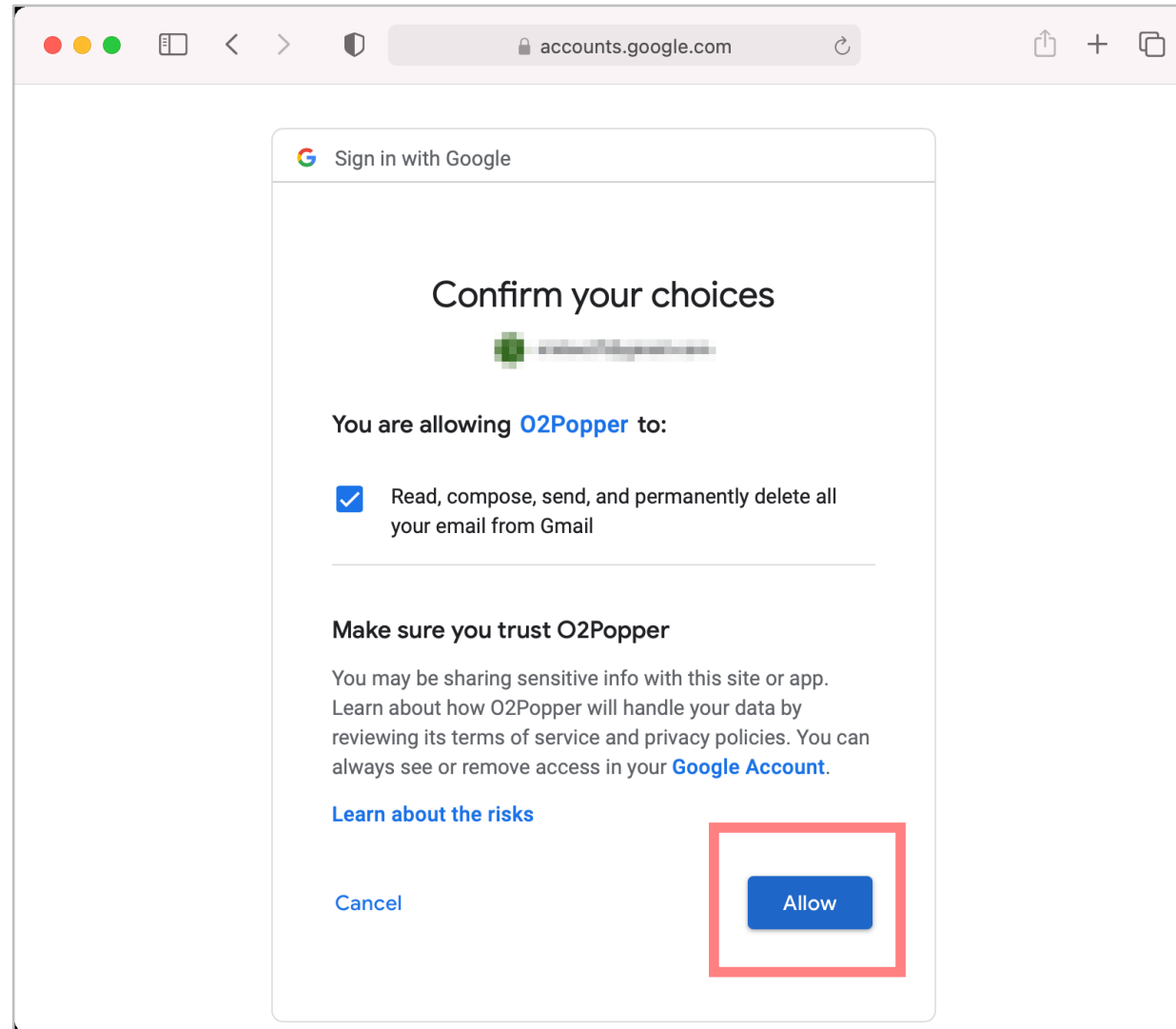
If "Authorization" is successful, the web browser will display the following screen.

If "Authorization" is successful, this application will display the following screen.
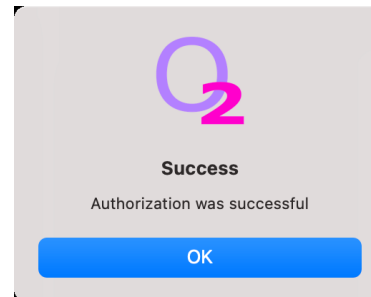
If you close the web browser in the middle of "Authorization", control will not return to this application.
In this case, start the web browser again and access the following URL.

http://localhost:8080

An error will occur, but control will return to this application.

When "Authorization" is completed, click the "OK" button to close the setting screen.
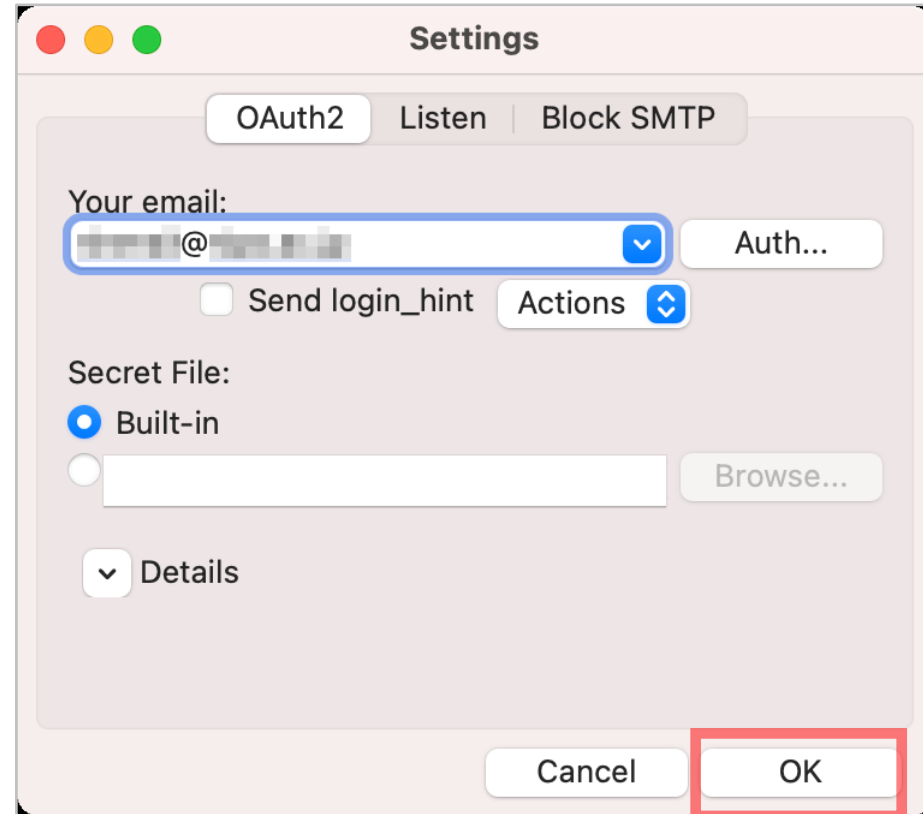
Next, set up your email client (Apple Mail, Thunderbird, etc.) as follows.

Incoming Mail (POP) Server	localhost Requires SSL: No Port: 8110
Outgoing Mail (SMTP) Server	localhost Requires SSL: No Port: 8025
Account Name, User Name, or Email address	Your email address
Password	Appropriate string Note: Not used for authentication.

Note: If the above port number is used by another application, change it to another value on the setting screen of this application, and change the value of the mail client according to this application.

Apple Mail configuration example:
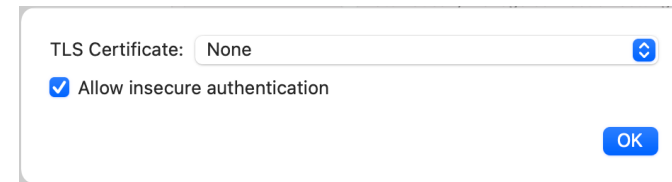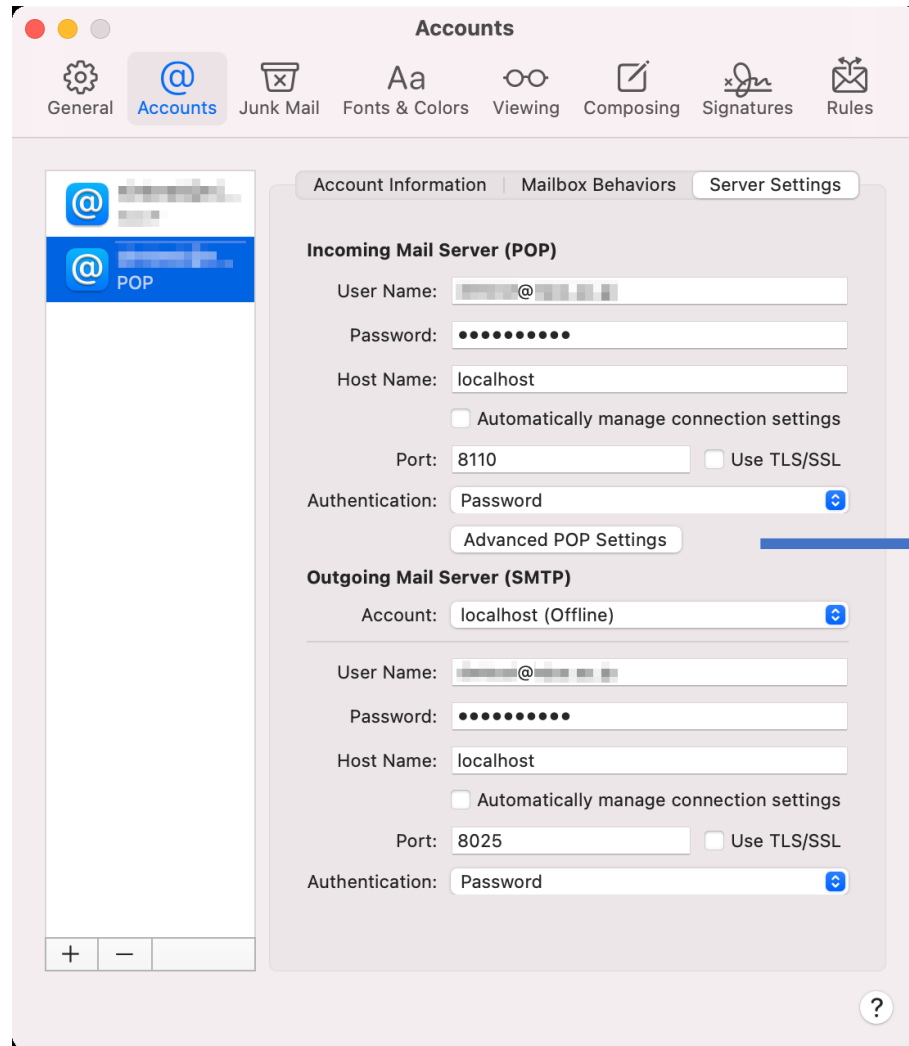
Thunderbird configuration example:
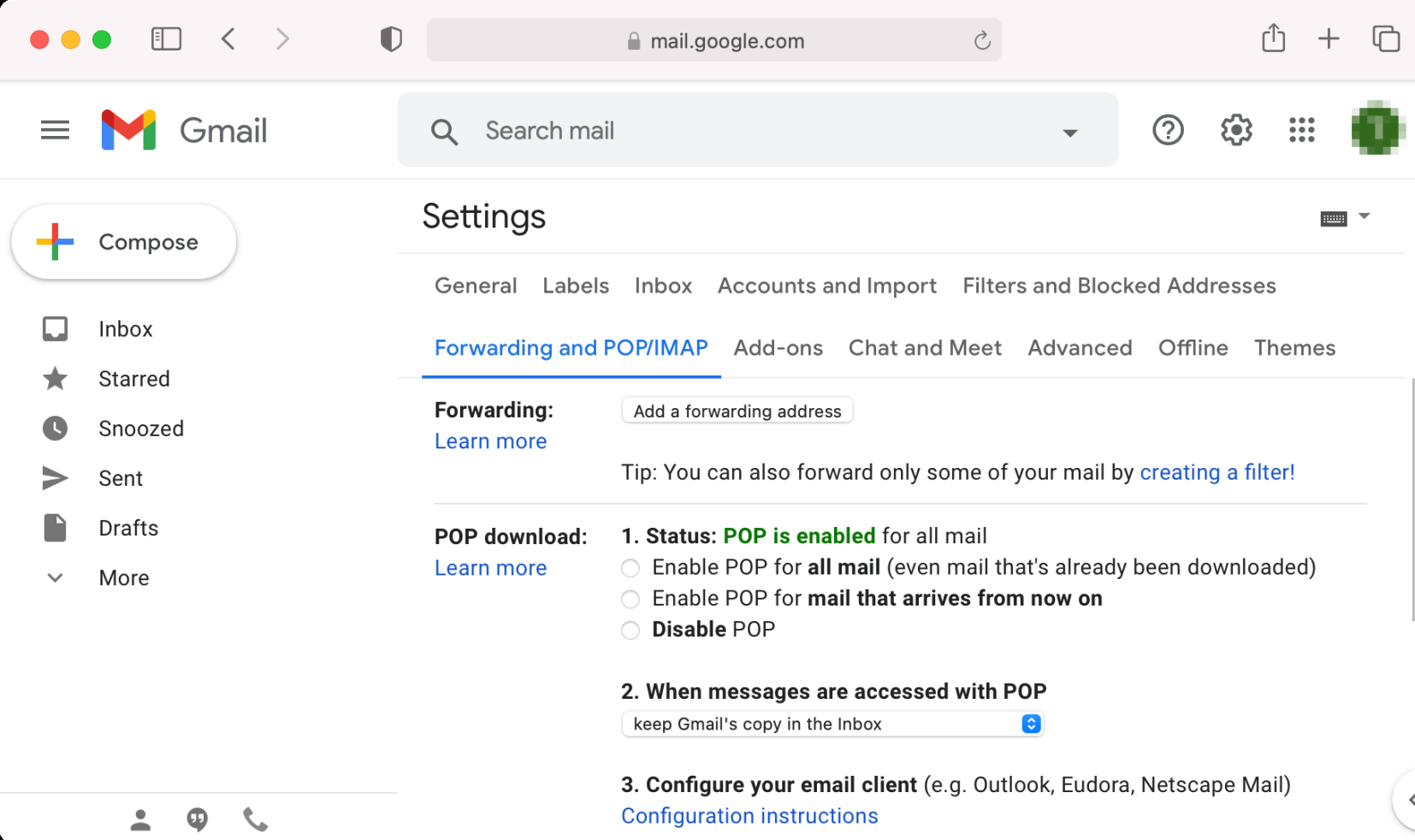
If you want to receive emails by POP, please enable POP on Gmail side.

After completing the settings of the mail client and Gmail, select "Monitor…" from the menu of this application.

Click the "Start" button on the monitor to start receiving SMTP and POP.
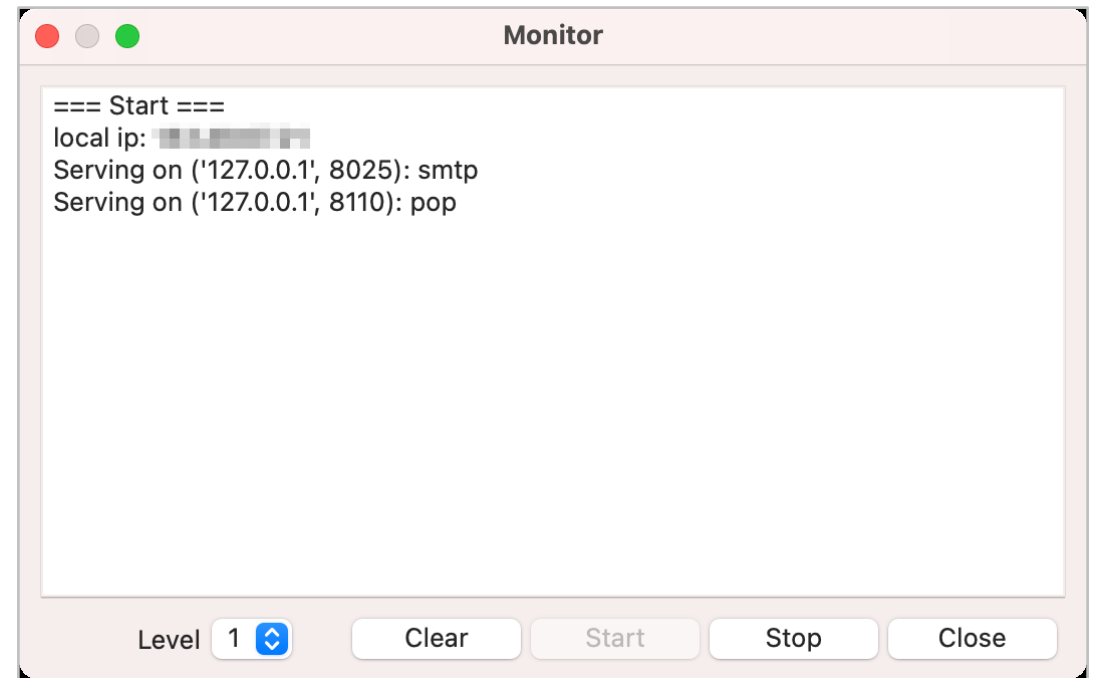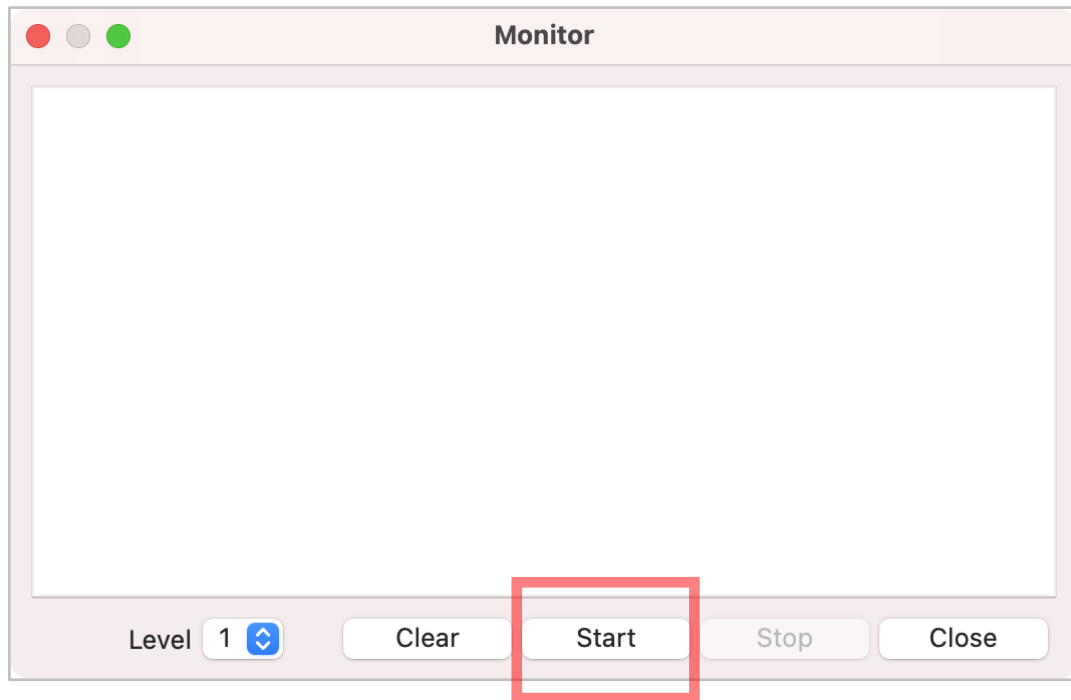
Start sending and receiving email client. If the output is as follows, it is successful.

When received by POP:

When sent by SMTP:

Note:
    Lines with purple text starting with "<<<" are the responses from Gmail's POP and SMTP servers.

If it does not work, there may be a problem with the settings on the security software side.

The settings for sending and receiving between this application and the Gmail server are as follows.

Incoming Mail (POP) Server   pop.gmail.com
                                Port: 995

Outgoing Mail (SMTP) Server   smtp.gmail.com
                                Port: 465

Make sure that the security software has not blocked the communication or modified the communication contents.
If you cannot solve the problem, I recommend that you consult with a detailed person near you.

The compatibility between the mail client and this application may be poor.
You cannot use a mail client that outputs protocol commands in an order not expected by this application. I would appreciate it if you could let the author know.

If you are using Avast as your security software, uncheck "Scan secure connections" in "Email Shield".
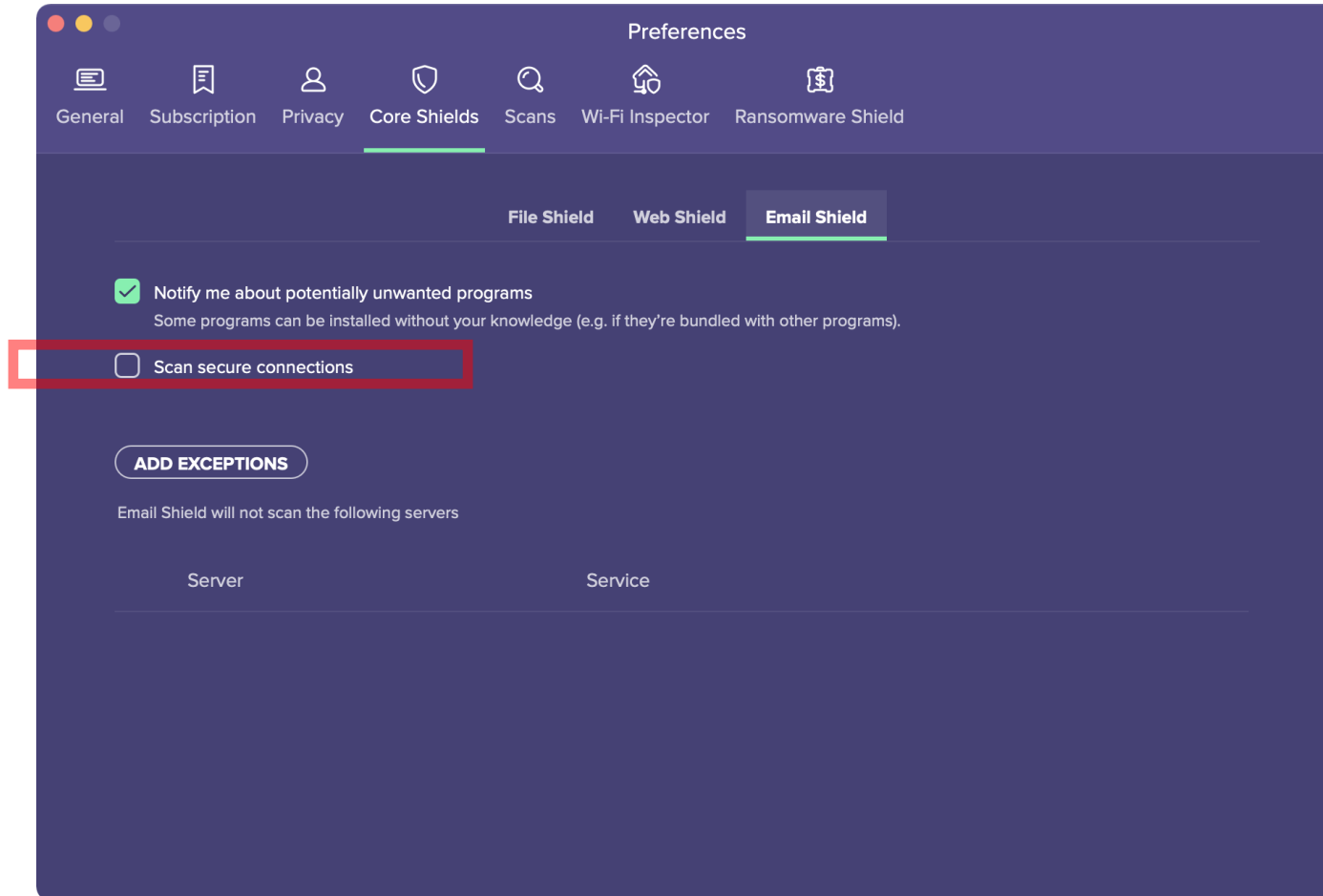
Close the monitor when you have successfully sent and received emails. (Reception is stopped when the monitor screen is closed.) If you want to start receiving automatically when this application starts, change "Initial State" in "Listen" on the setting screen to "Start" and click the "OK" button.
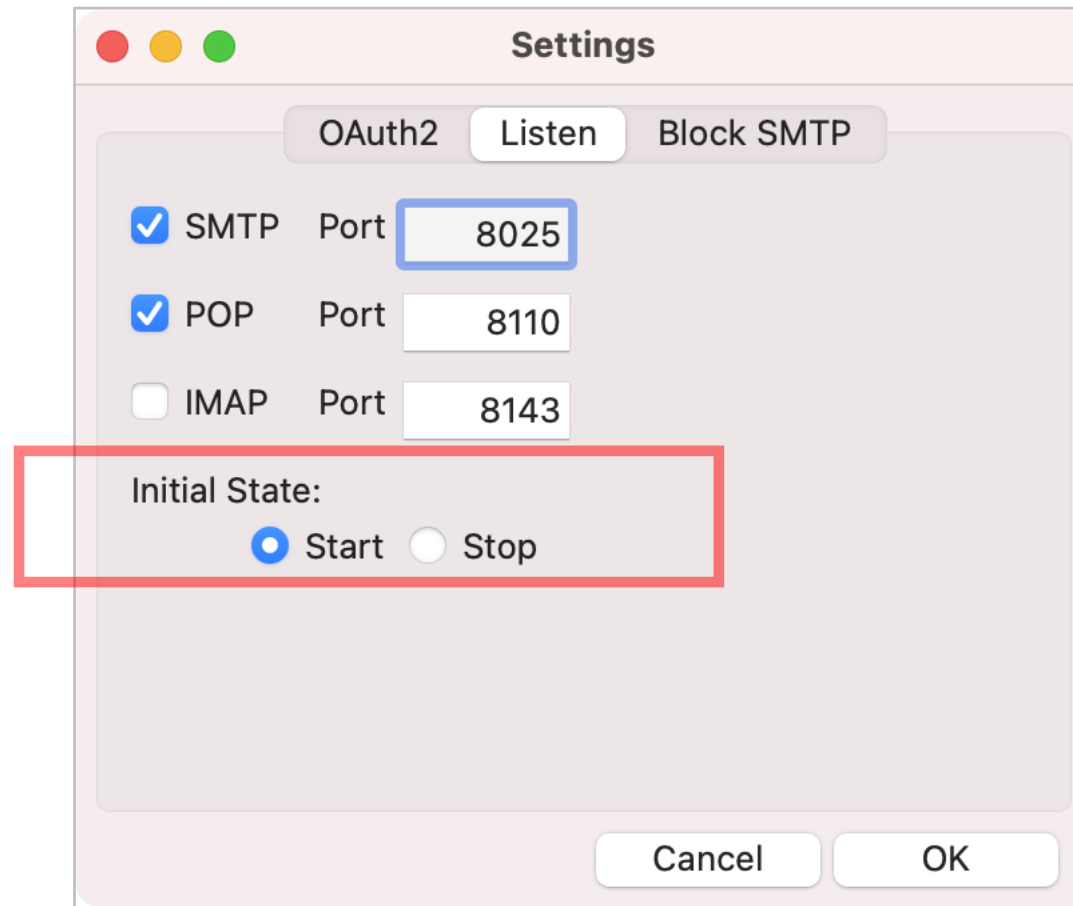
Select "Start" on the menu screen to start receiving.
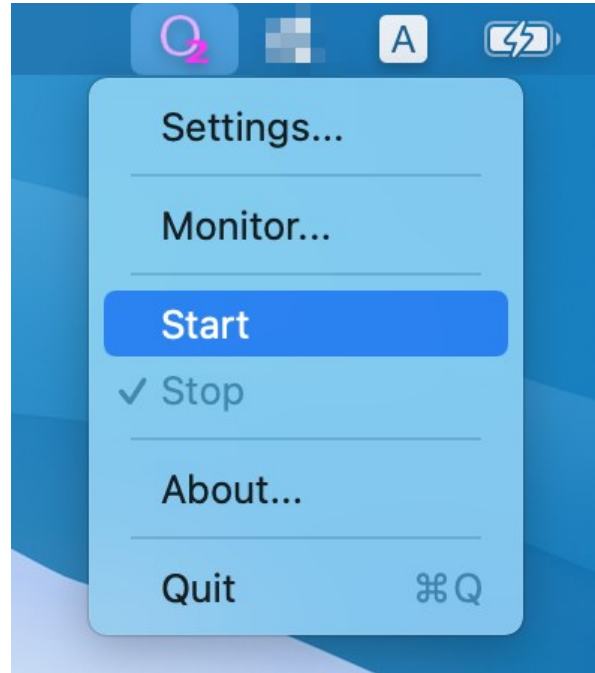
Options

There are erroneous transmission prevention functions. Please adjust on the setting screen.

To+Cc Max:

    Specify the maximum total number of addresses that can be specified for To and Cc of the destination. If this value is exceeded, it will not be sent as an error. Set to 0 for unlimited. 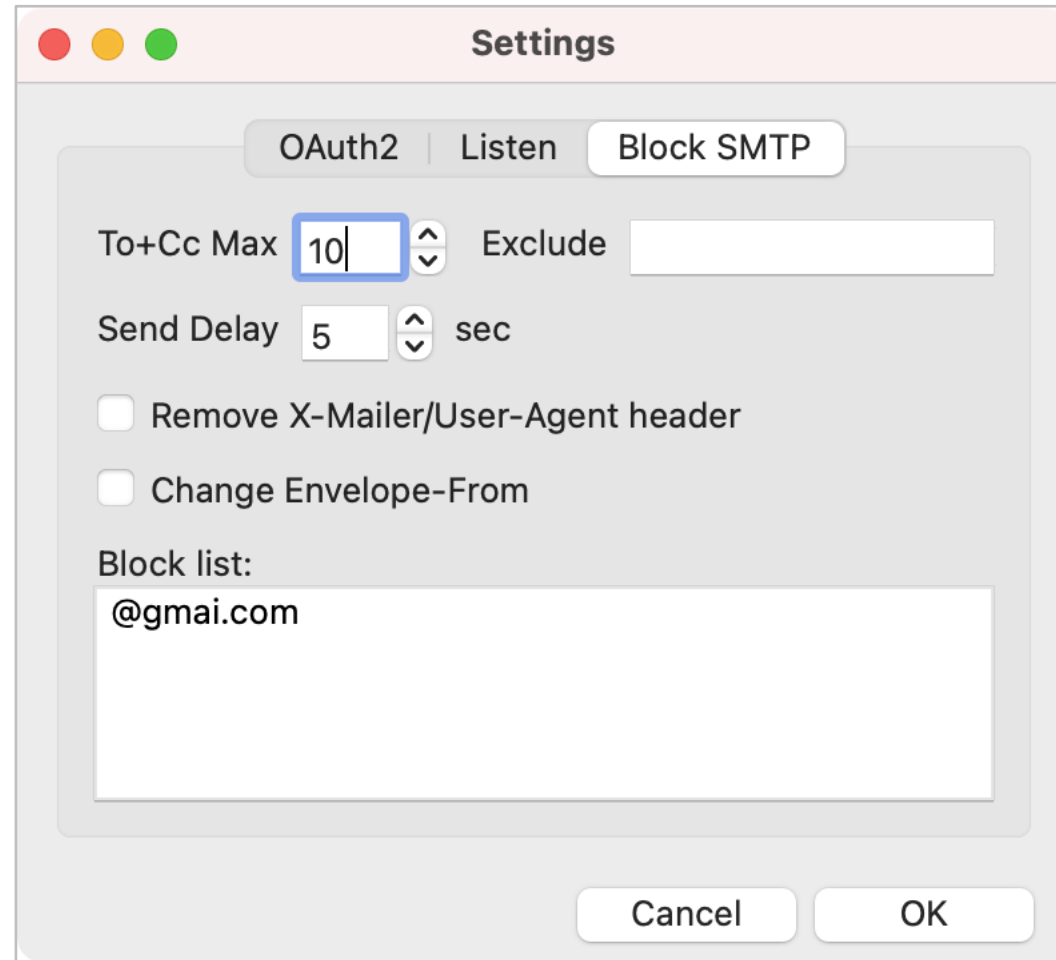It was implemented to prevent accidents in which Cc and Bcc are mistakenly transmitted in large quantities. Specify the addresses you do not want to be included in the address count in the "Exclude" field.
Note: Names containing "@" may be counted excessively.
Note: If a substring of the address is specified in the "Exclude" field, it will be judged as a suffix match. It is not case sensitive.
You can specify multiple conditions by separating them with a single-byte space or a single-byte comma (,).

Send Delay:

    You can cancel the transmission within the specified number of seconds. You can specify up to 30 seconds, and if you set it to 0, it will be sent without delay.

☐ Remove X-Mailer/User-Agent header
☐ Change Envelope-From
Block list:
@gmai.com

Remove X-Mailer/User-Agent header:

If checked, the X-Mailer header and User-Agent header will be deleted before sending.
If you do not want the other party to know the type and version information of the email software you are using, please check it.

Change Envelope-From:

If checked, the Envelope From will be changed to the email address used for OAuth2 authentication and sent. If the sender of the email is a group address, problems such as "cannot post" or "error email does not arrive" may occur.
This is a function to avoid such problems.

Block list:

Please specify the address you want to block sending.
If a substring of the address is specified, it is judged by a suffix match.
It is not case sensitive.
You can specify multiple conditions by separating them with single-byte spaces, single-byte commas, and line breaks.
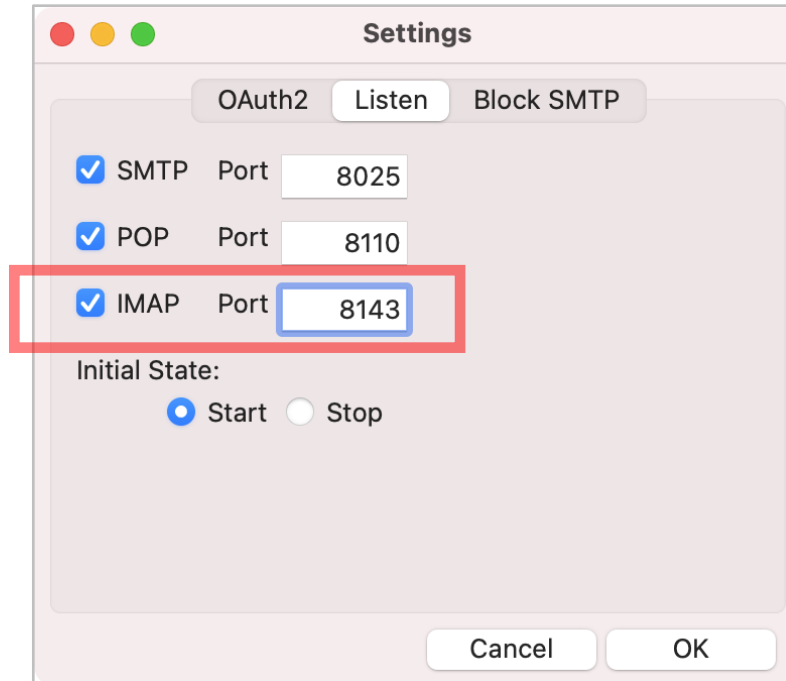
New functions

From version 3.0.0, you can set multiple accounts.
If you pull down "Actions" and select "Add", you can set up the second account.
You can switch your account settings from the "Your email" pulldown.
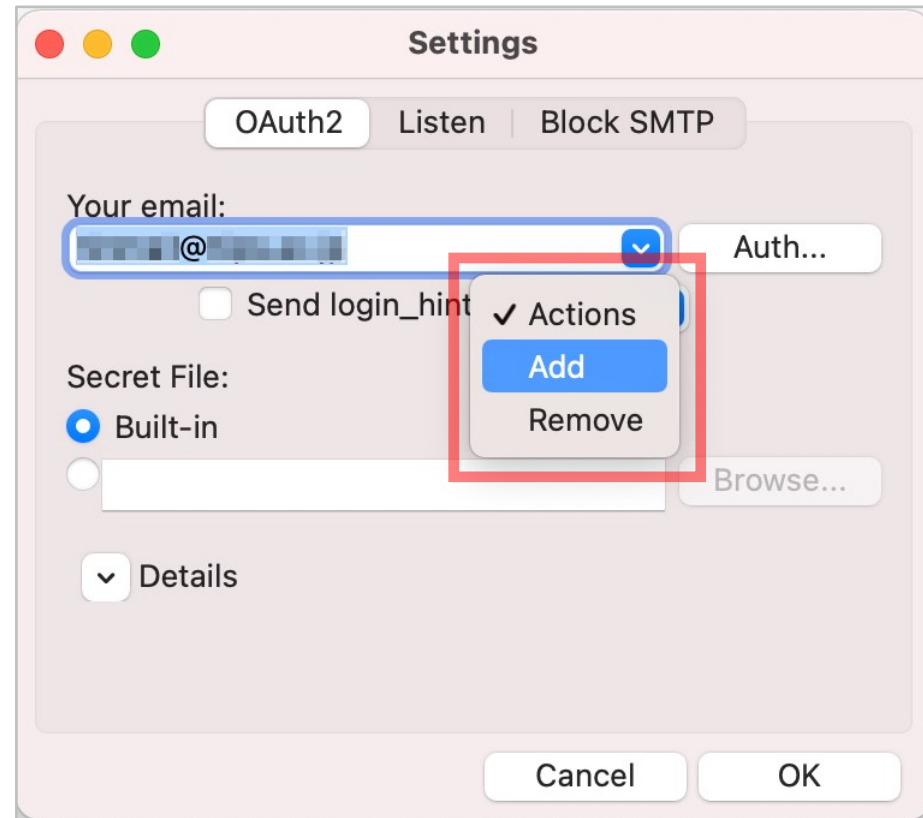
From version 3.0.0, supports IMAP.
If you want to use IMAP, check "IMAP" on the "Listen" tab on the "Settings" screen.

Set up your email client as follows.

Incoming Mail (IMAP) Server   localhost
                                     Requires SSL: No
                                     Port: 8143