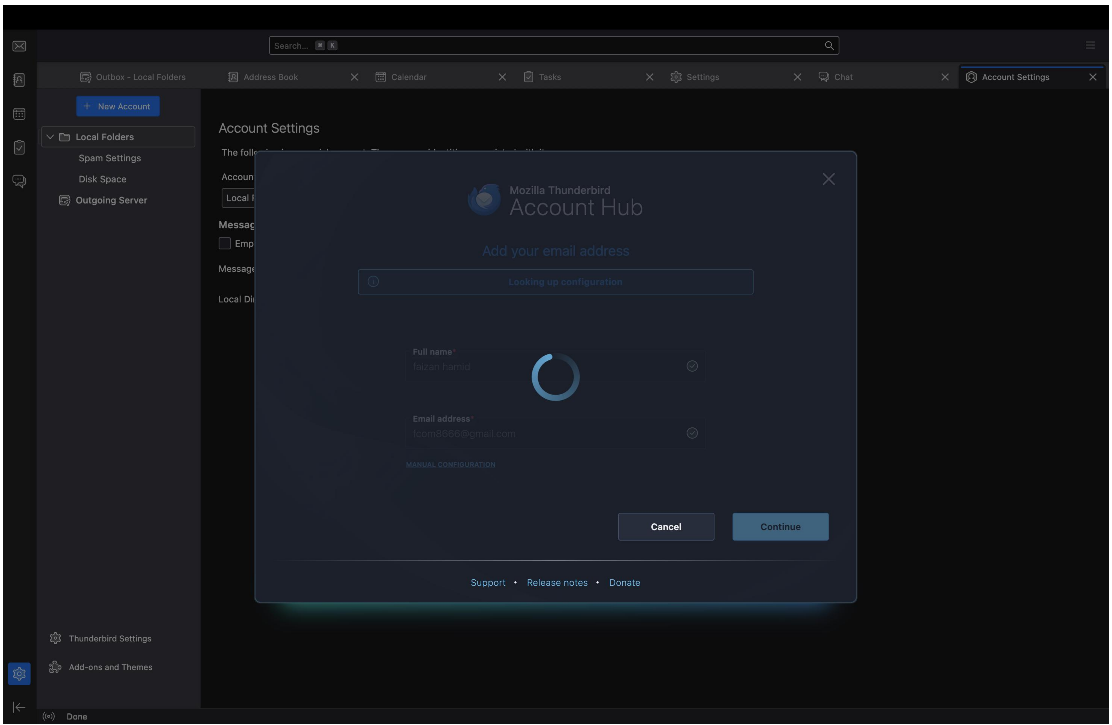


Account Settings

Mozilla Thunderbird
Account Hub

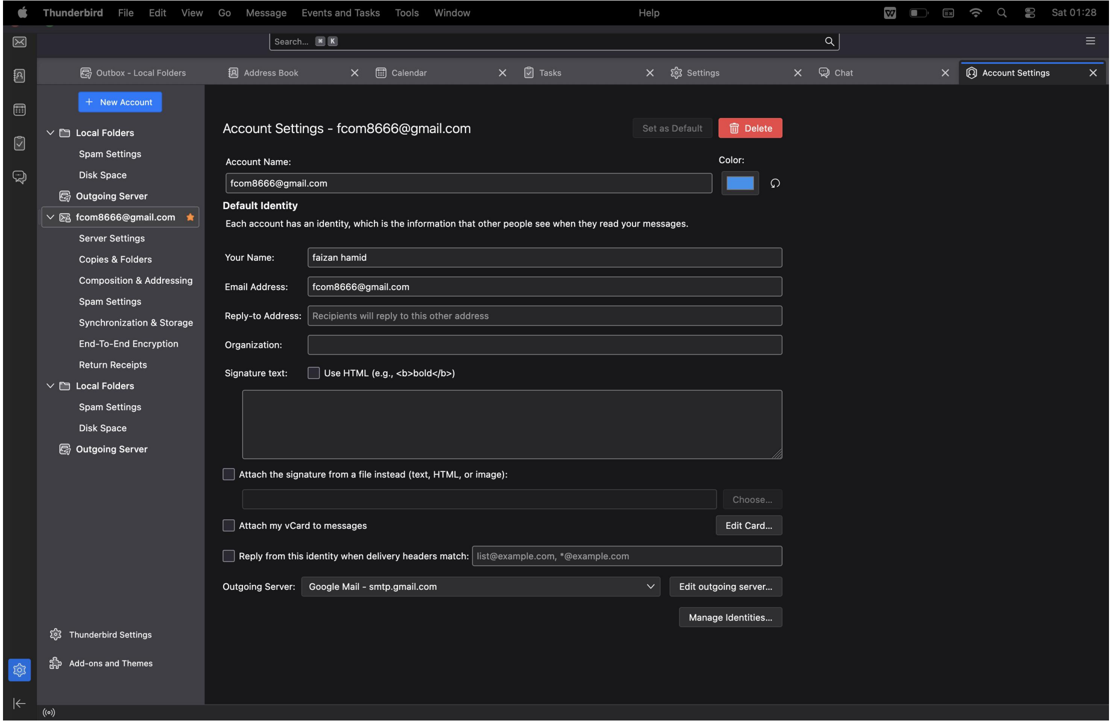
Add your email address

Looking up configuration

Full name*
faizan hamid

Email address*
fcom8666@gmail.com

MANUAL CONFIGURATION



Account Settings - fcom8666@gmail.com

Account Name: fcom8666@gmail.com

Color:

Default Identity

Each account has an identity, which is the information that other people see when they read your messages.

Your Name: faizan hamid

Email Address: fcom8666@gmail.com

Reply-to Address: Recipients will reply to this other address

Organization:

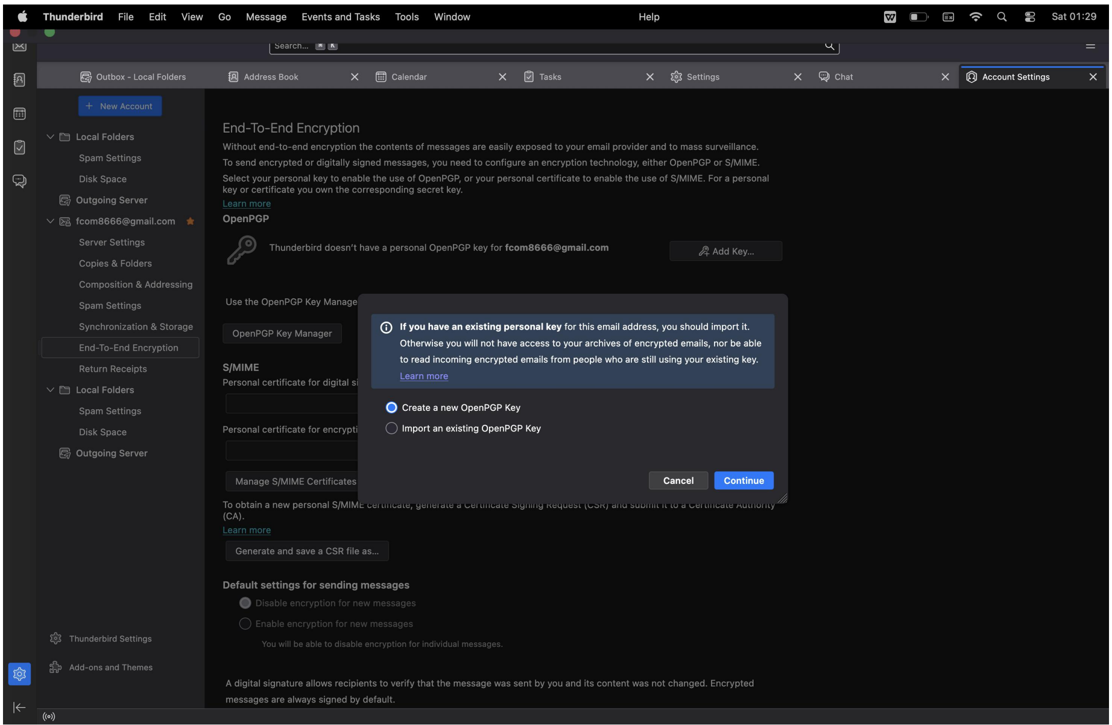
Signature text: □ Use HTML (e.g., <b>bold</b>)

□ Attach the signature from a file instead (text, HTML, or image):

□ Attach my vCard to messages

□ Reply from this identity when delivery headers match: list@example.com, *@example.com

Outgoing Server: Google Mail - smtp.gmail.com



End-To-End Encryption

Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.

Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key.

Learn more

OpenPGP

Thunderbird doesn't have a personal OpenPGP key for **fcom8666@gmail.com**

Add Key...

Use the OpenPGP Key Manage

OpenPGP Key Manager

S/MIME

Personal certificate for digital si

Personal certificate for encrypti

Manage S/MIME Certificates

To obtain a new personal S/MIME certificate, generate a Certificate Signing Request (CSR) and submit it to a Certificate Authority (CA).

Learn more

Generate and save a CSR file as...

Default settings for sending messages

● Disable encryption for new messages

○ Enable encryption for new messages

You will be able to disable encryption for individual messages.

A digital signature allows recipients to verify that the message was sent by you and its content was not changed. Encrypted messages are always signed by default.

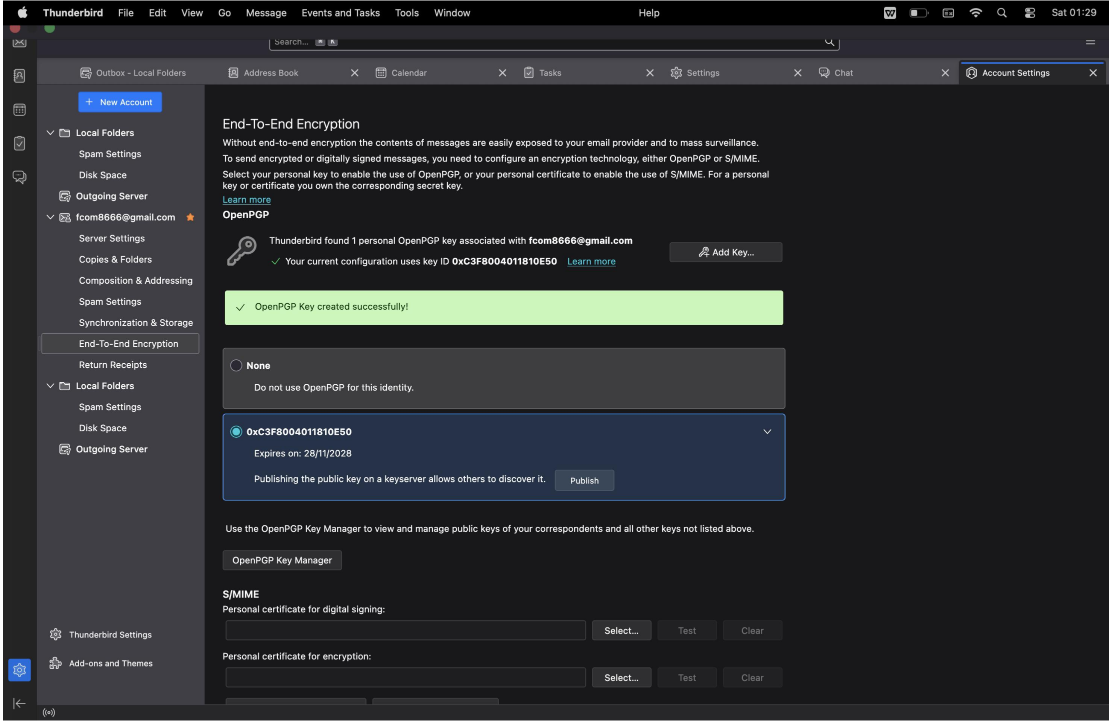
If you have an existing personal key for this email address, you should import it. Otherwise you will not have access to your archives of encrypted emails, nor be able to read incoming encrypted emails from people who are still using your existing key.

Learn more

● Create a new OpenPGP Key

○ Import an existing OpenPGP Key

Cancel Continue



End-To-End Encryption

Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance.

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.

Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key.

Learn more

OpenPGP

Thunderbird found 1 personal OpenPGP key associated with **fcom8666@gmail.com**

✓ Your current configuration uses key ID **0xC3F8004011810E50** Learn more

Add Key...

✓ OpenPGP Key created successfully!

○ **None**

Do not use OpenPGP for this identity.

● **0xC3F8004011810E50**

Expires on: 28/11/2028

Publishing the public key on a keyserver allows others to discover it. Publish

Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.

OpenPGP Key Manager

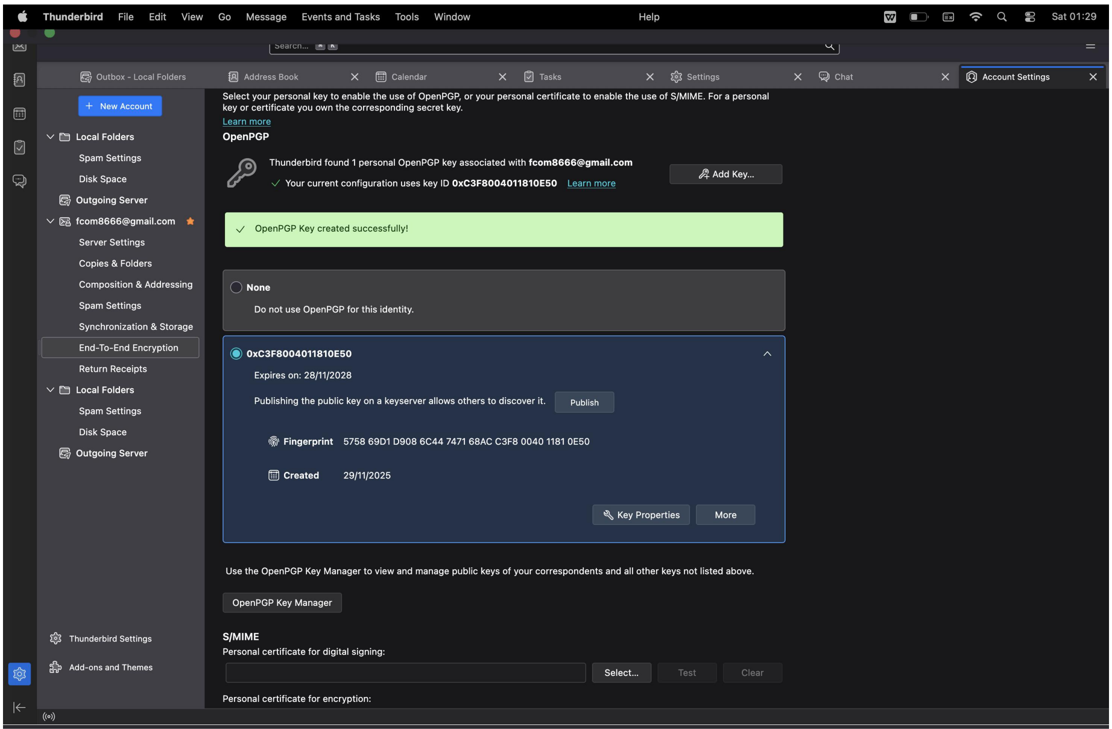
S/MIME

Personal certificate for digital signing:

Select... Test Clear

Personal certificate for encryption:

Select... Test Clear



Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key.

Learn more

OpenPGP

Thunderbird found 1 personal OpenPGP key associated with **fcom8666@gmail.com**

✓ Your current configuration uses key ID **0xC3F8004011810E50** Learn more

✓ OpenPGP Key created successfully!

○ **None**

Do not use OpenPGP for this identity.

● **0xC3F8004011810E50**

Expires on: 28/11/2028

Publishing the public key on a keyserver allows others to discover it.

Fingerprint 5758 69D1 D908 6C44 7471 68AC C3F8 0040 1181 0E50

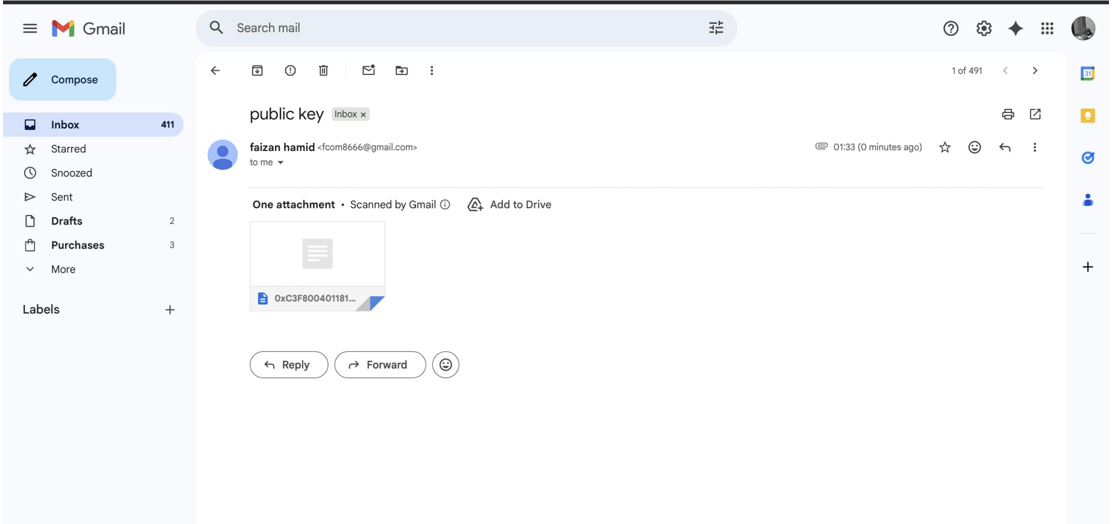
Created 29/11/2025

Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.

S/MIME

Personal certificate for digital signing:

Personal certificate for encryption:



public key Inbox ×

faizan hamid <fcom8666@gmail.com>
to me

01:33 (0 minutes ago)

One attachment • Scanned by Gmail ⓘ Add to Drive

0xC3F800401181...