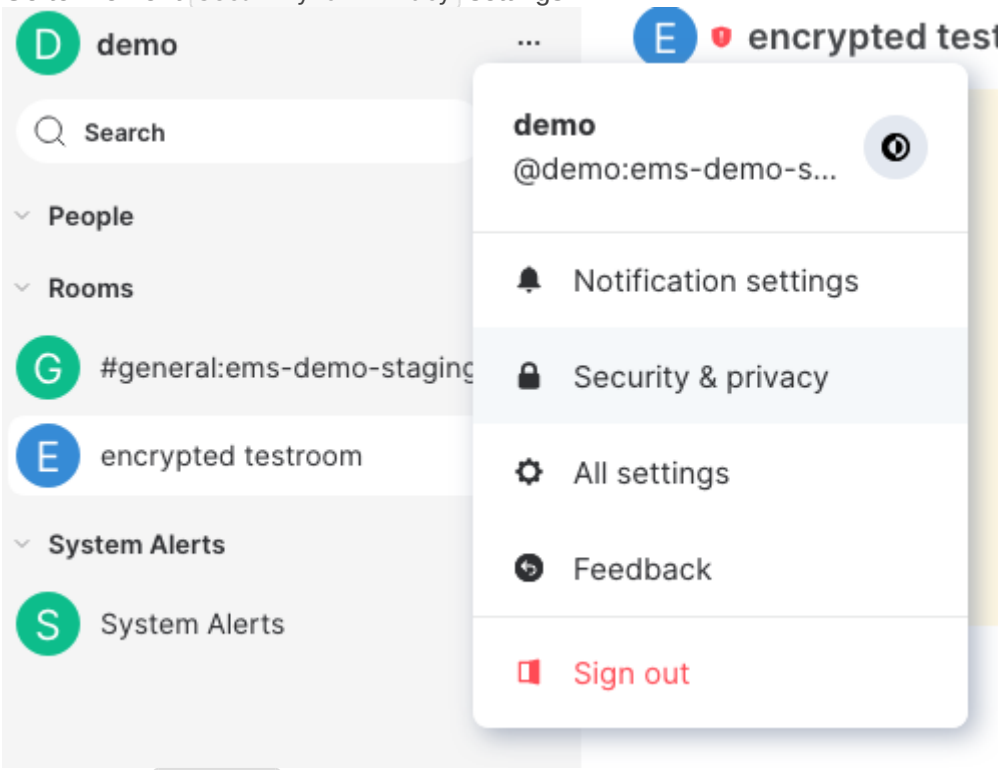
Cross Signing

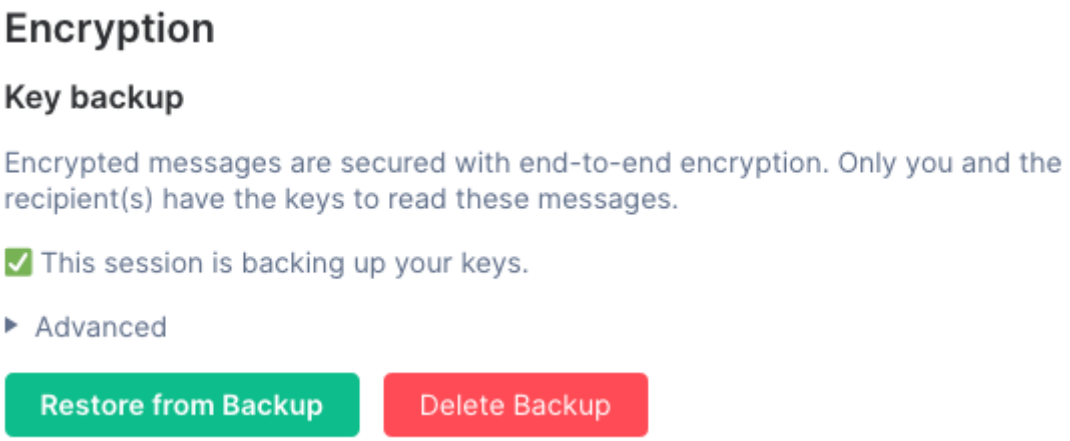
- Check Status
- Export and Import E2E Room Keys
- Reset Cross Signing
- Set up Cross Signing
- Verify new Login

Check Status

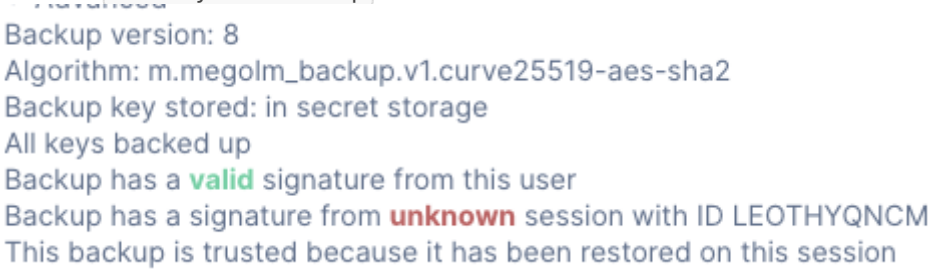
1. Go to Element `Security & Privacy` settings



2. Expand the `Advanced` section



3. Look for `All keys backed up`

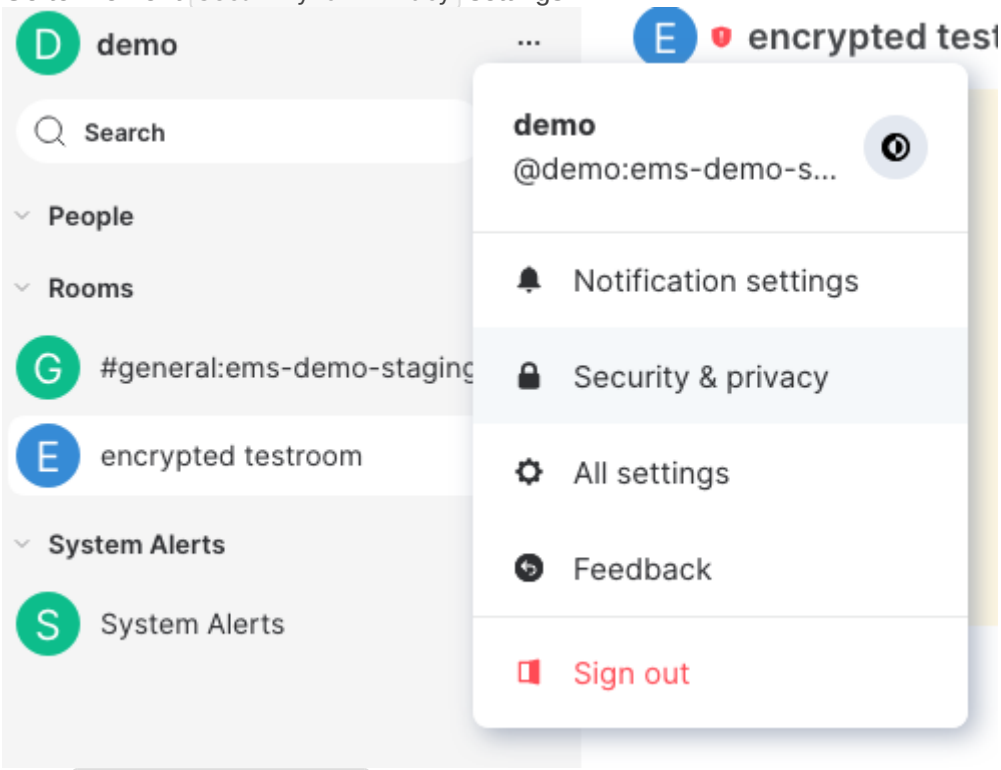


Export and Import E2E Room Keys

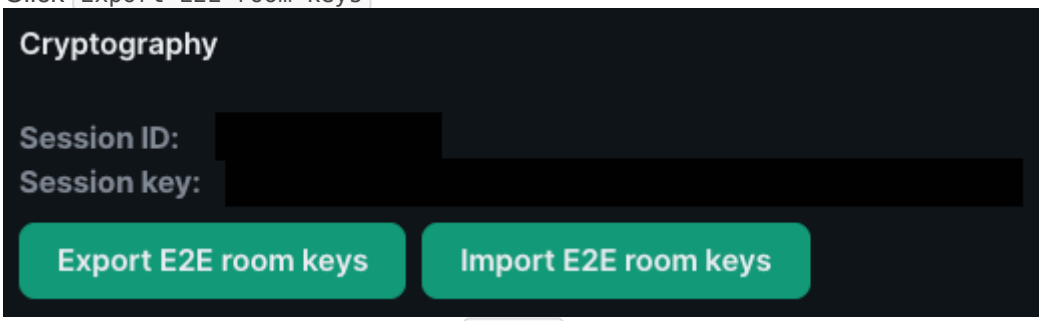
Element Web and Desktop

Export

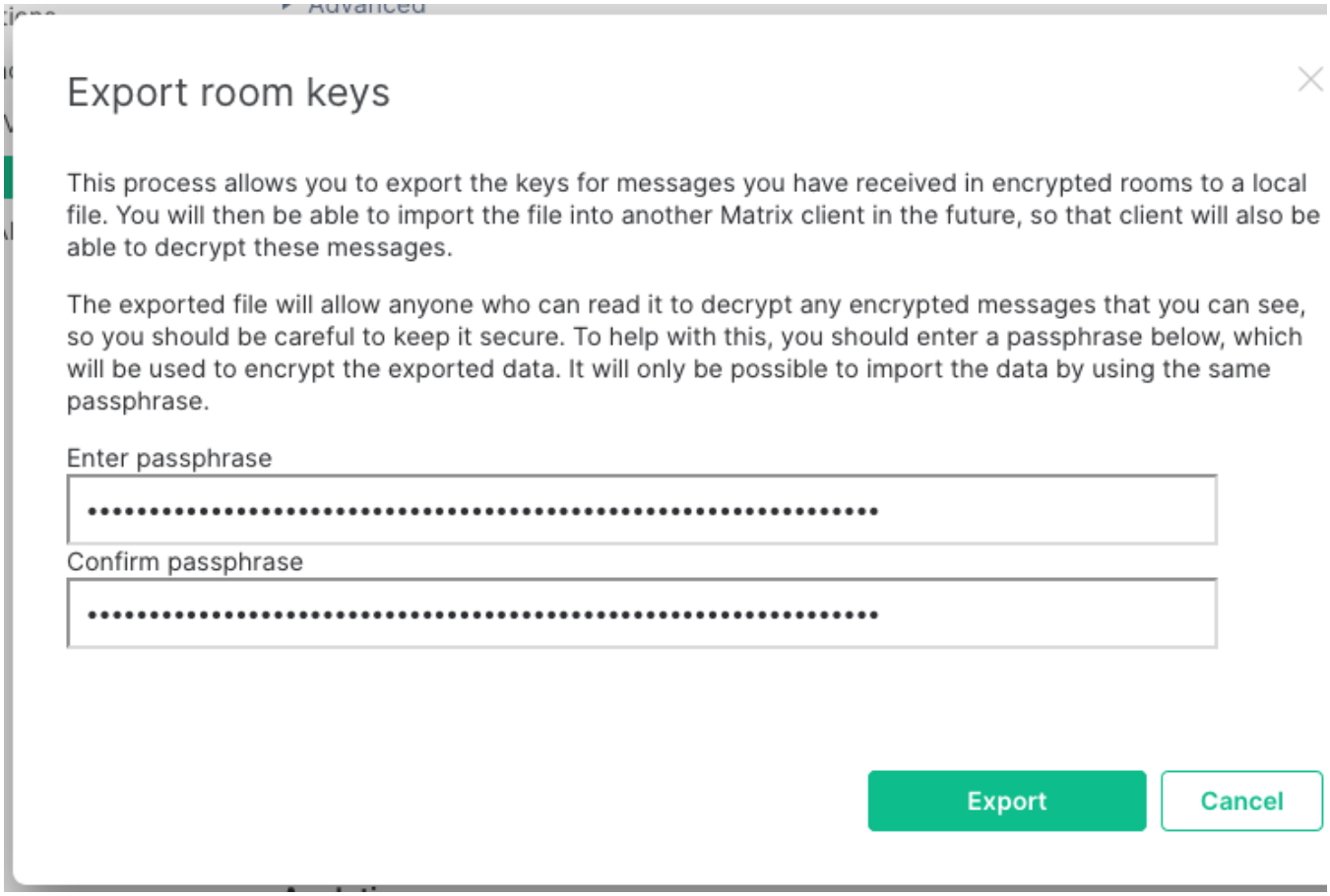
1. Go to Element `Security & Privacy` settings



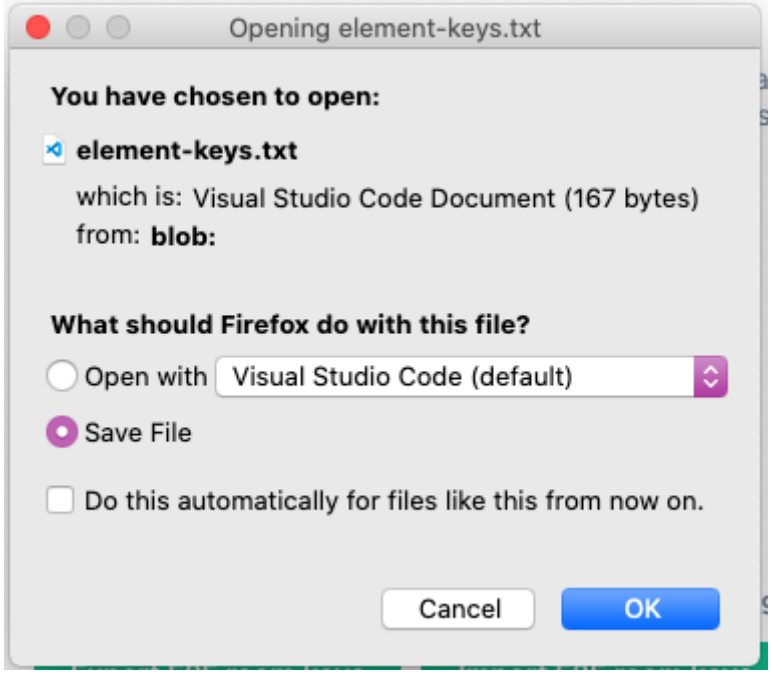
2. Click `Export E2E room keys`



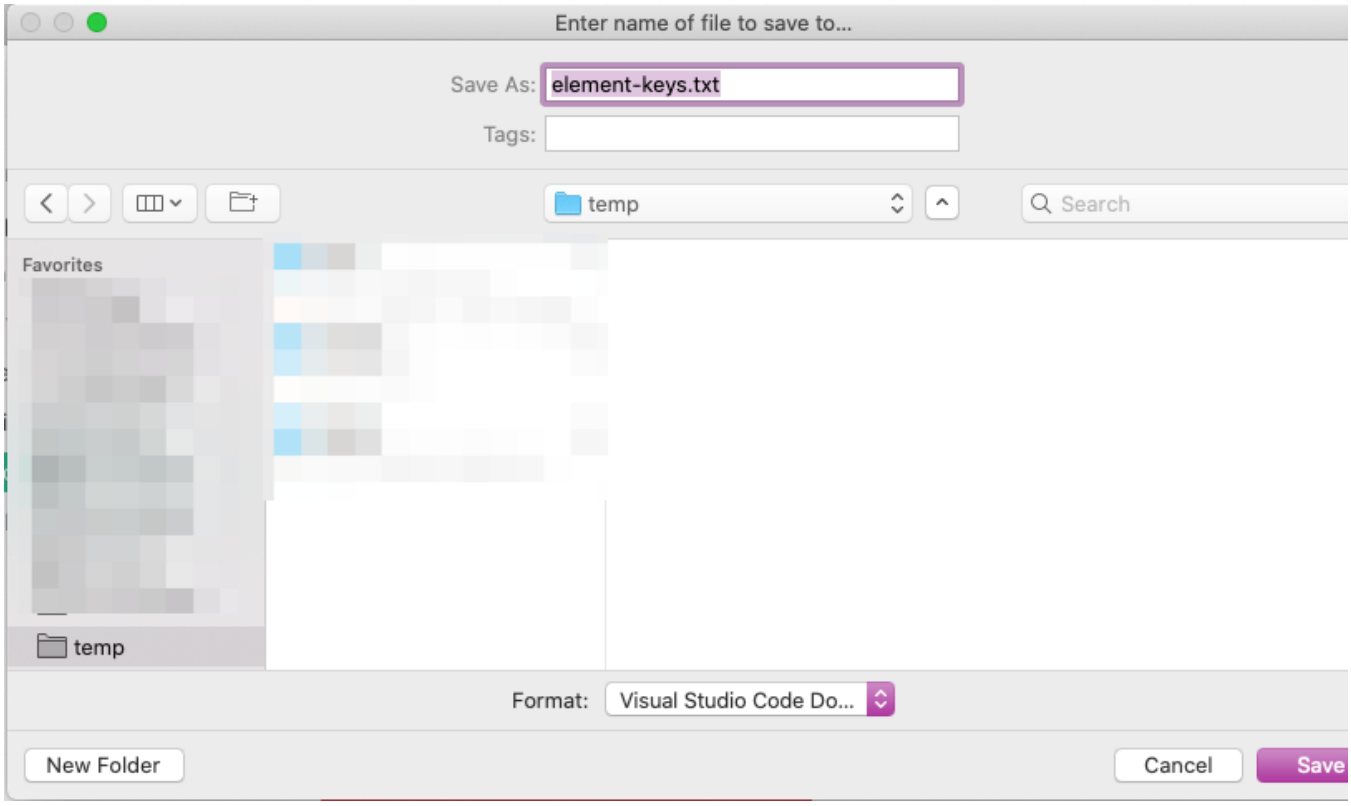
3. Enter a secure passphrase and click `Export`



4. Choose to save the file

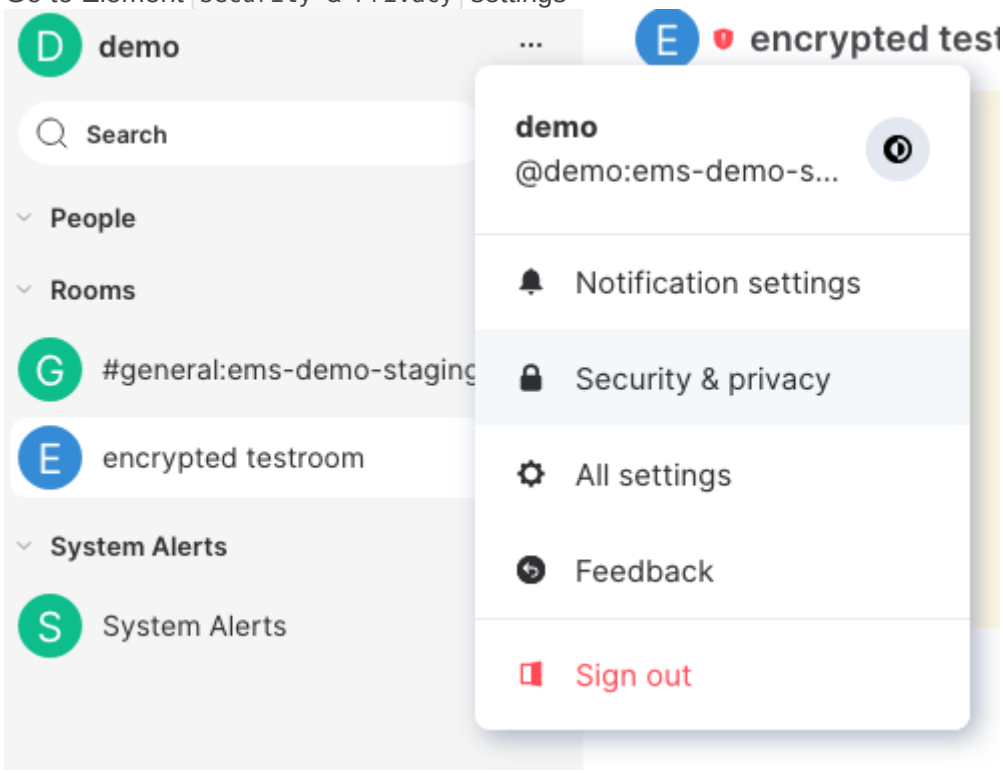


5. Select a directory on your computer

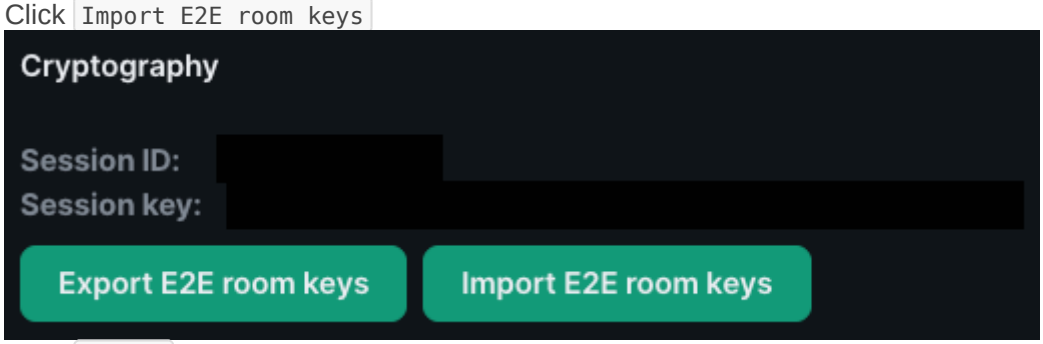


Import

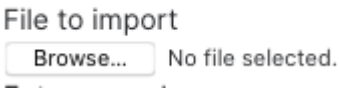
1. Go to Element `Security & Privacy` settings



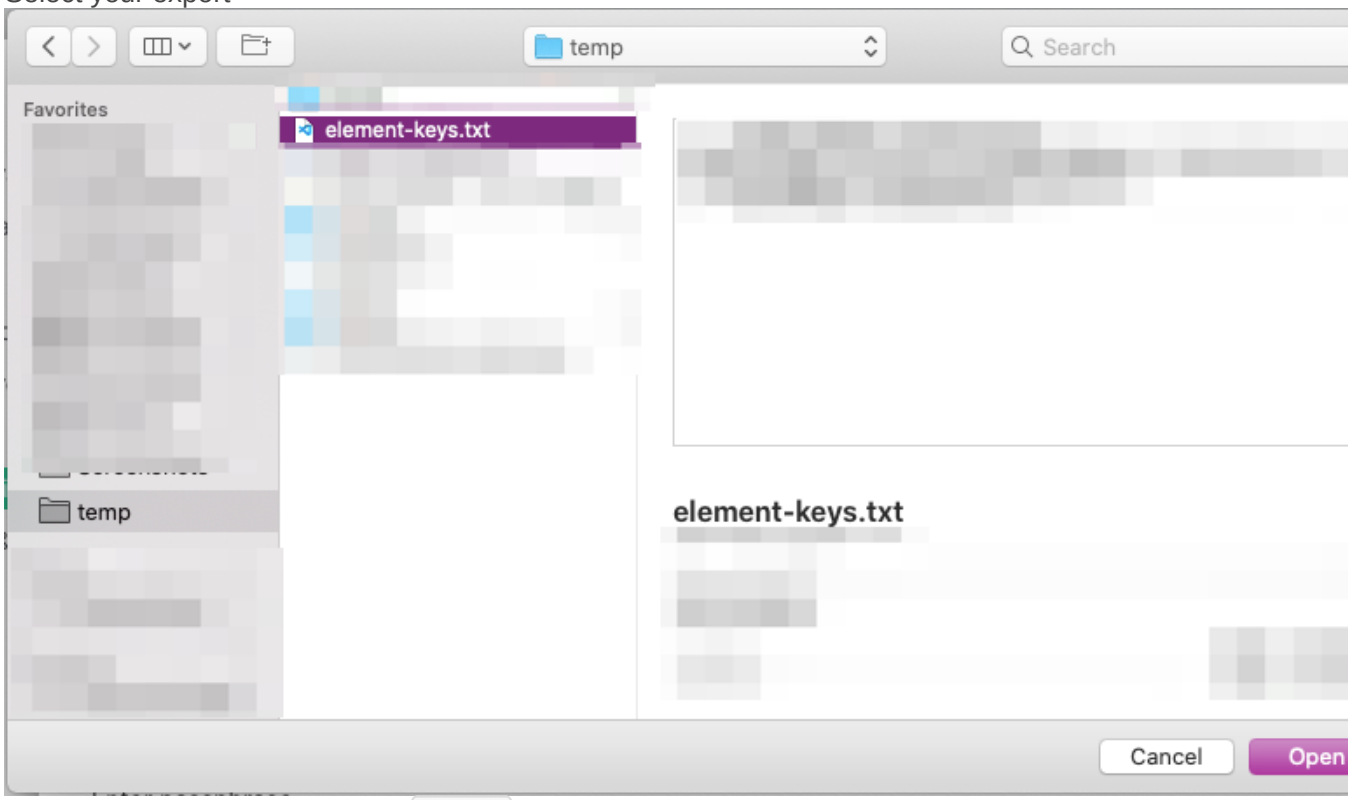
2. Click `Import E2E room keys`



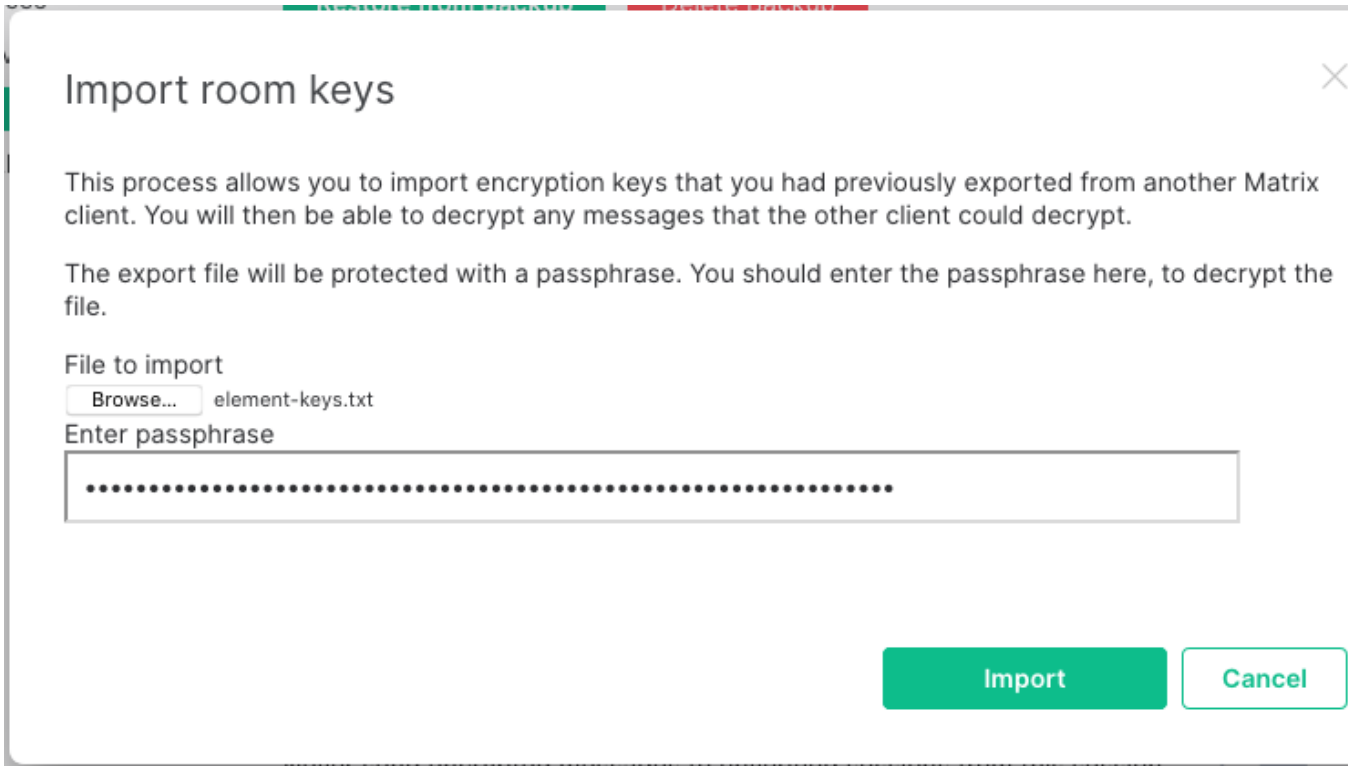
3. Click `Browse`



4. Select your export



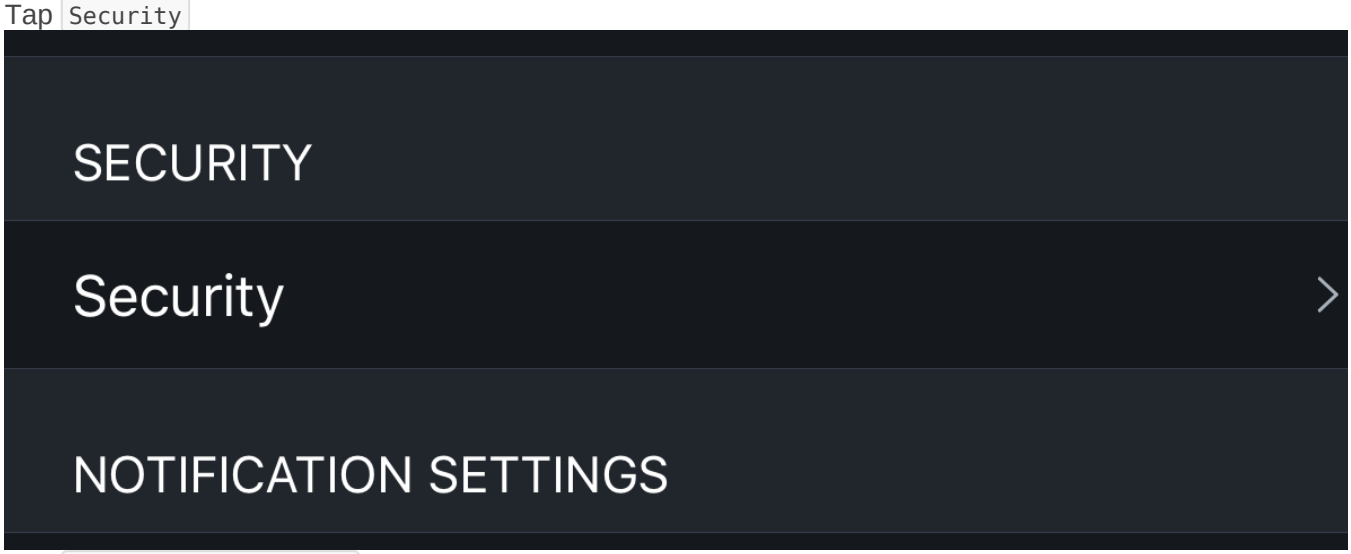
5. Enter your passphrase and click `Import`



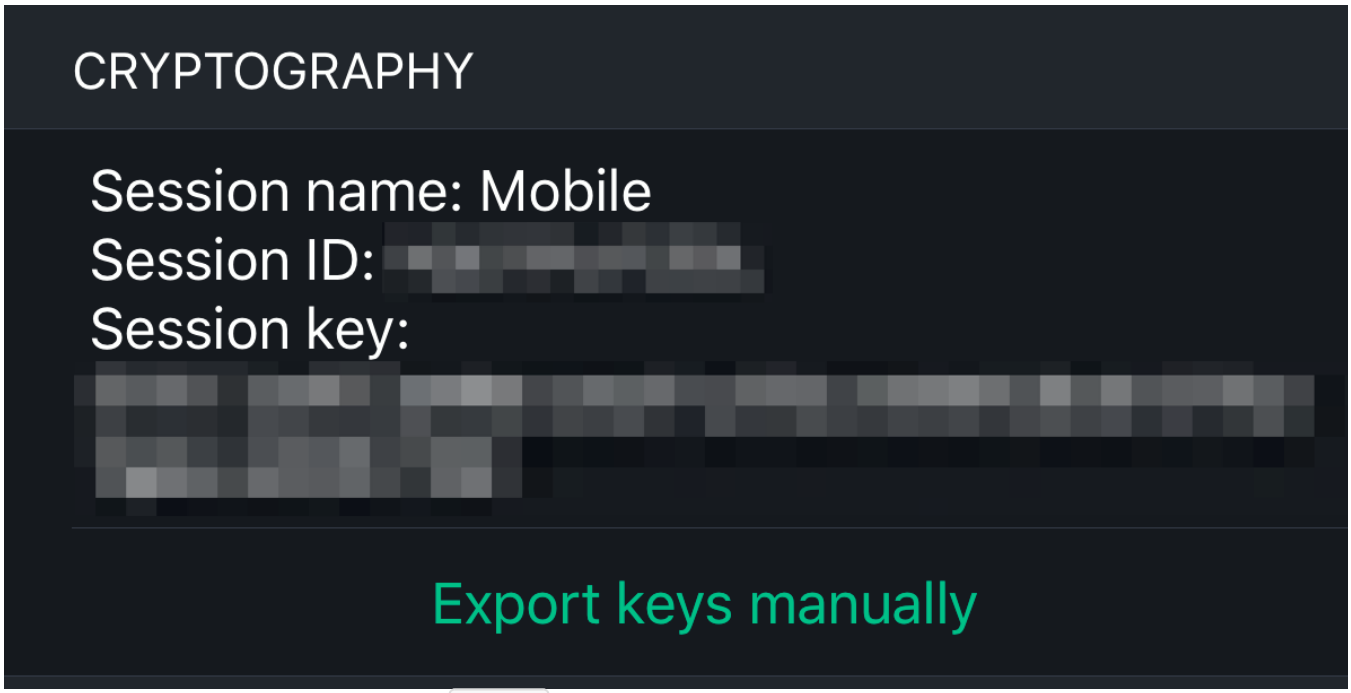
Element iOS

Export

1. Tap the cog in the top left of Element
2. Tap `Security`



3. Tap `Export keys manually`



4. Enter a secure passphrase and tap `Export`

Export room keys

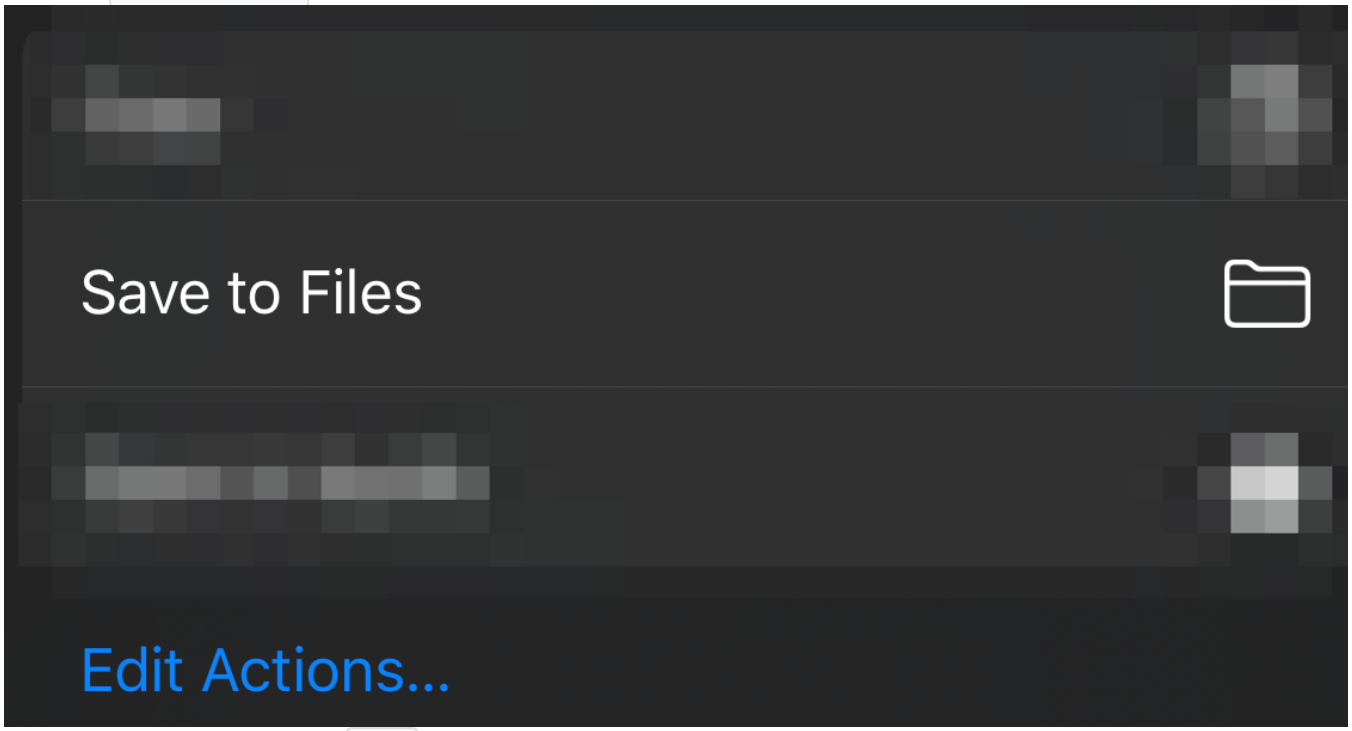
This process allows you to export the keys for messages you have received in encrypted rooms to a local file. You will then be able to import the file into another Matrix client in the future, so that client will also be able to decrypt these messages.

The exported file will allow anyone who can read it to decrypt any encrypted messages that you can see, so you should be careful to keep it secure.

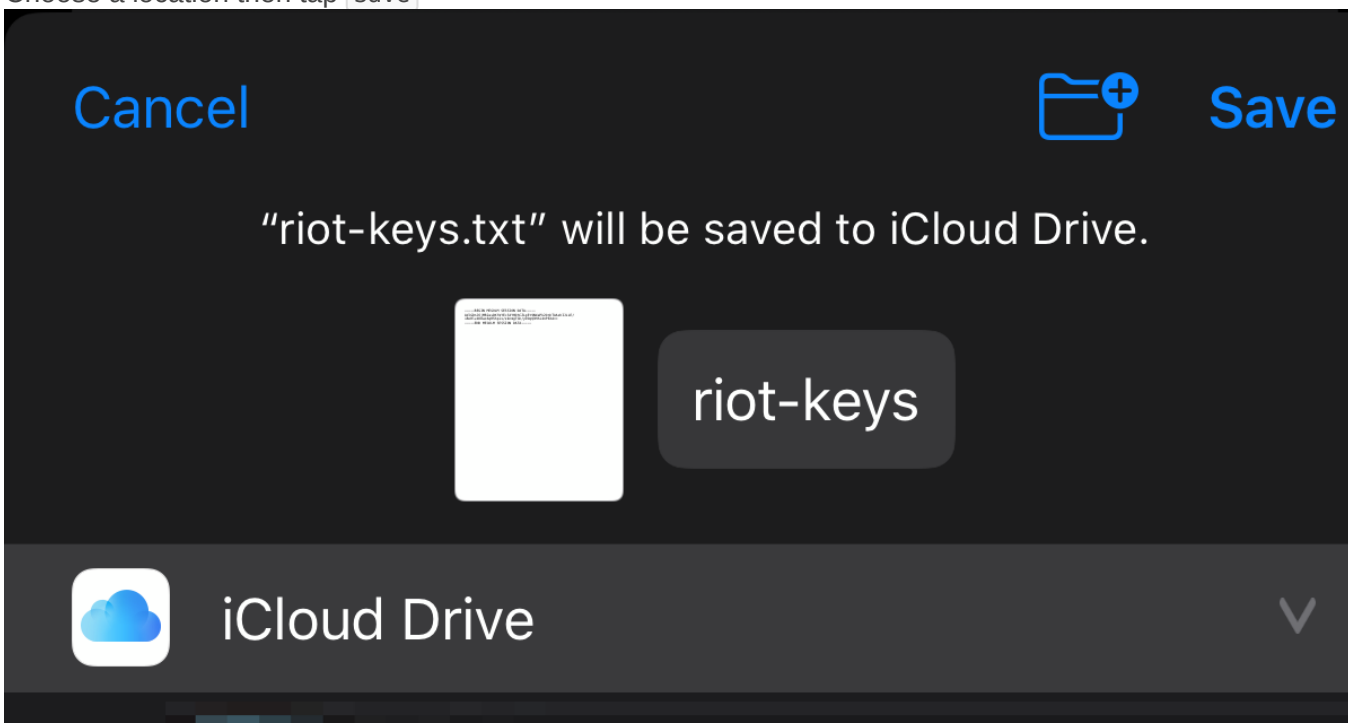
Cancel

Export

5. Choose `Save to Files`



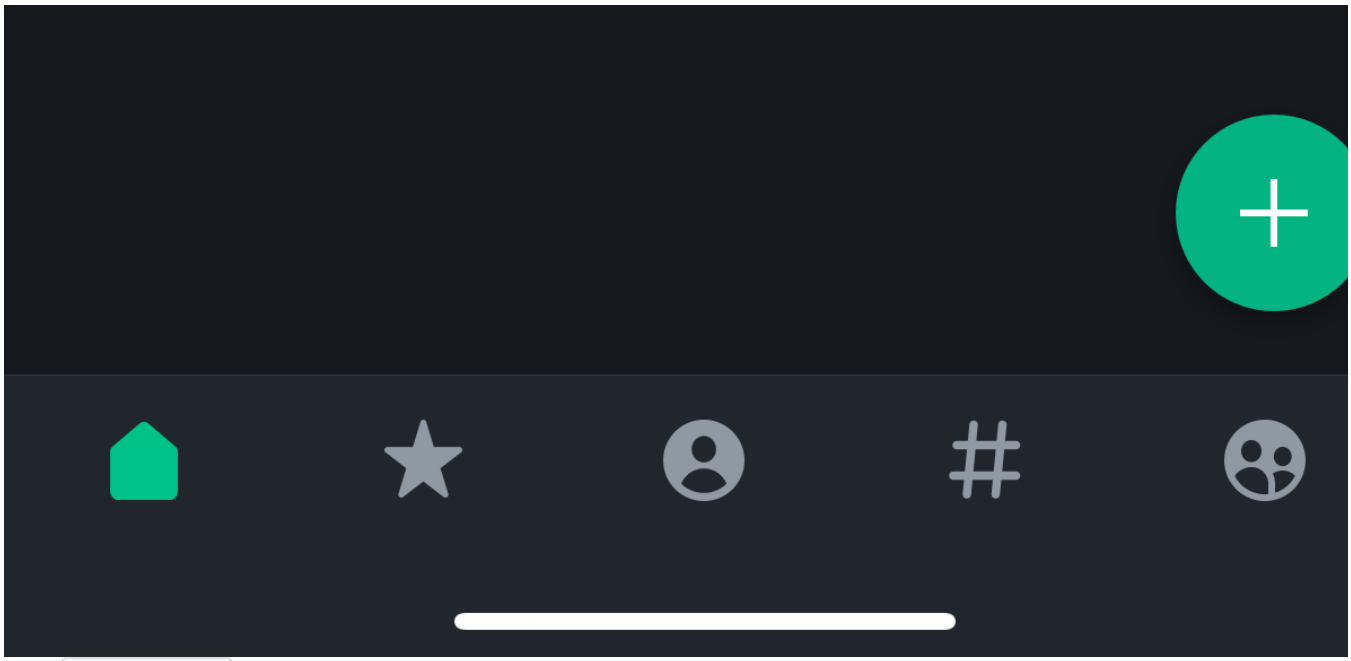
6. Choose a location then tap `Save`



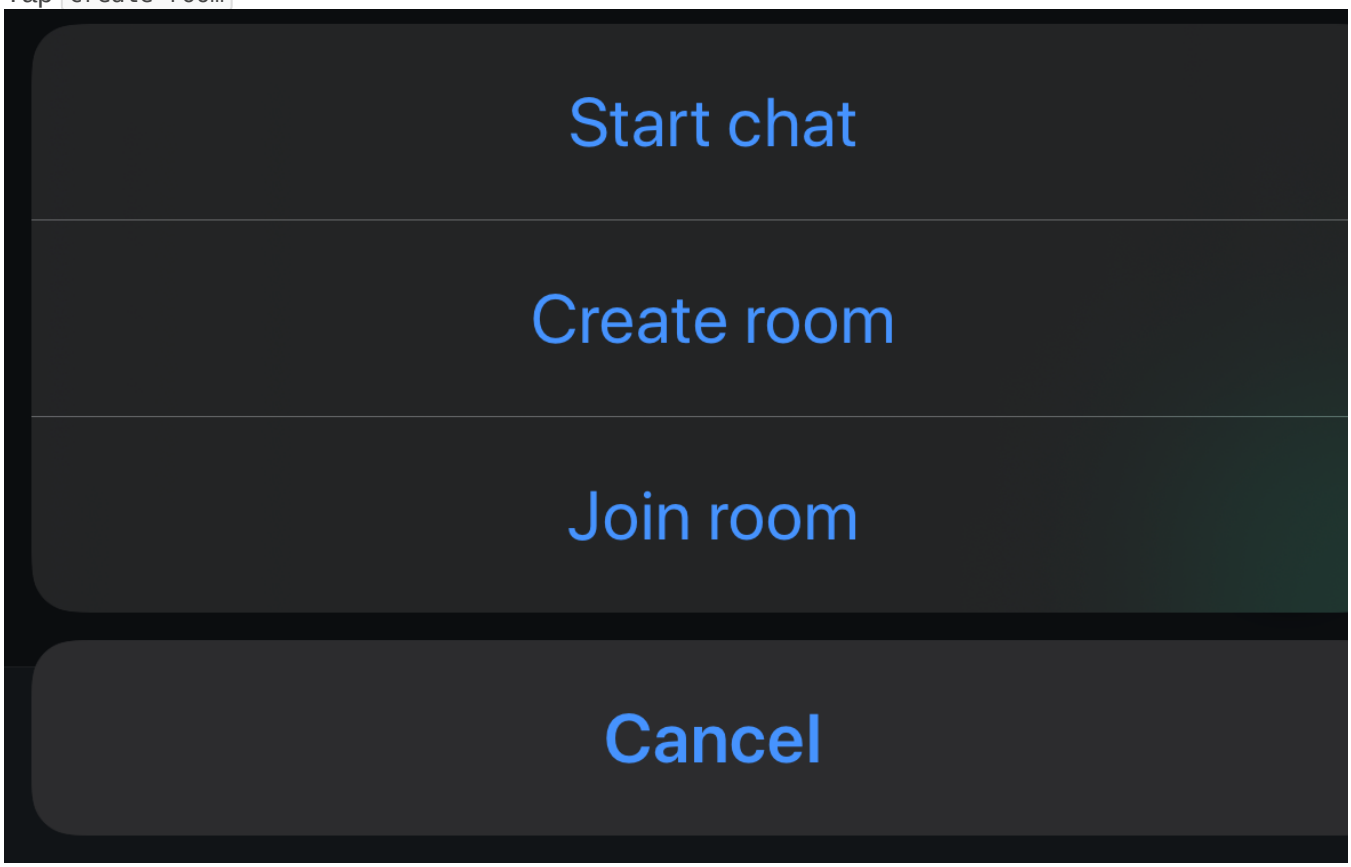
Import

This is a temporary solution until this issue is resolved

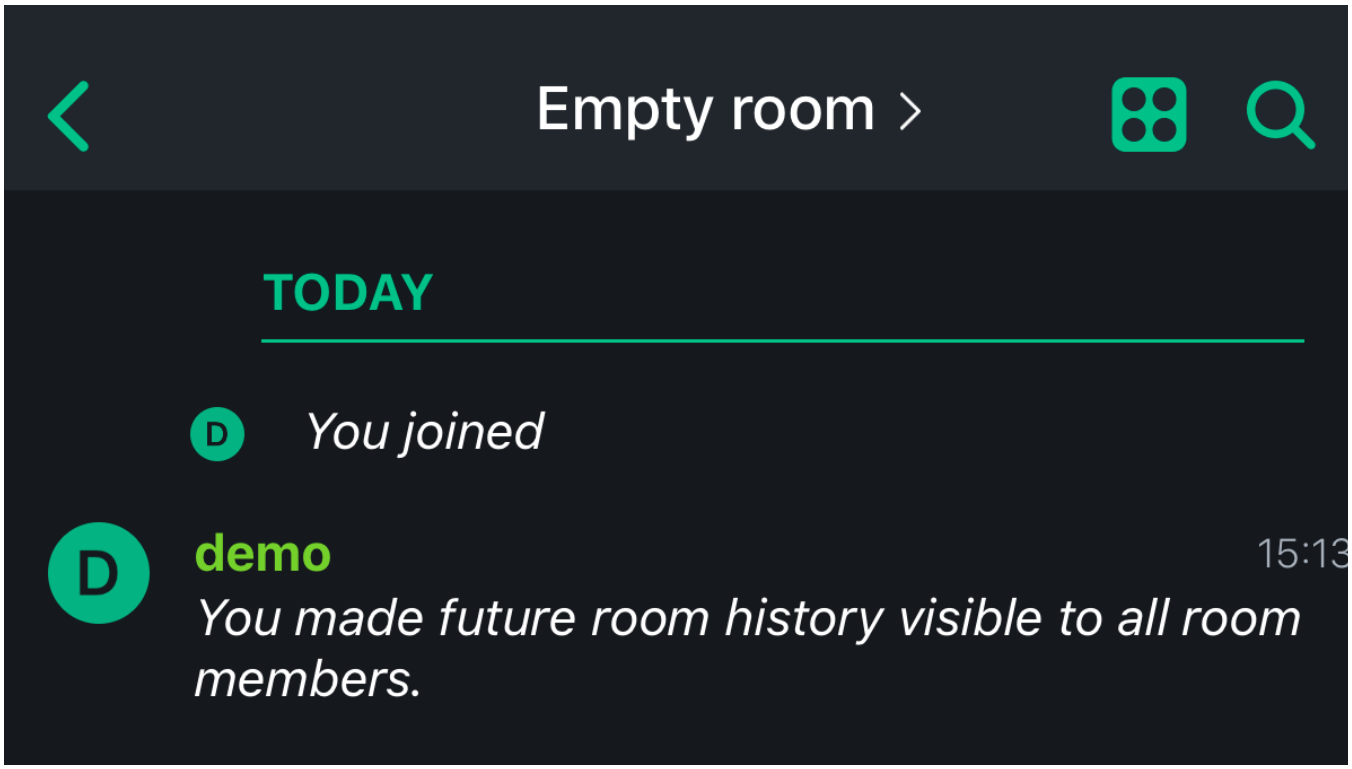
1. Tap the ▢ in the bottom right corner



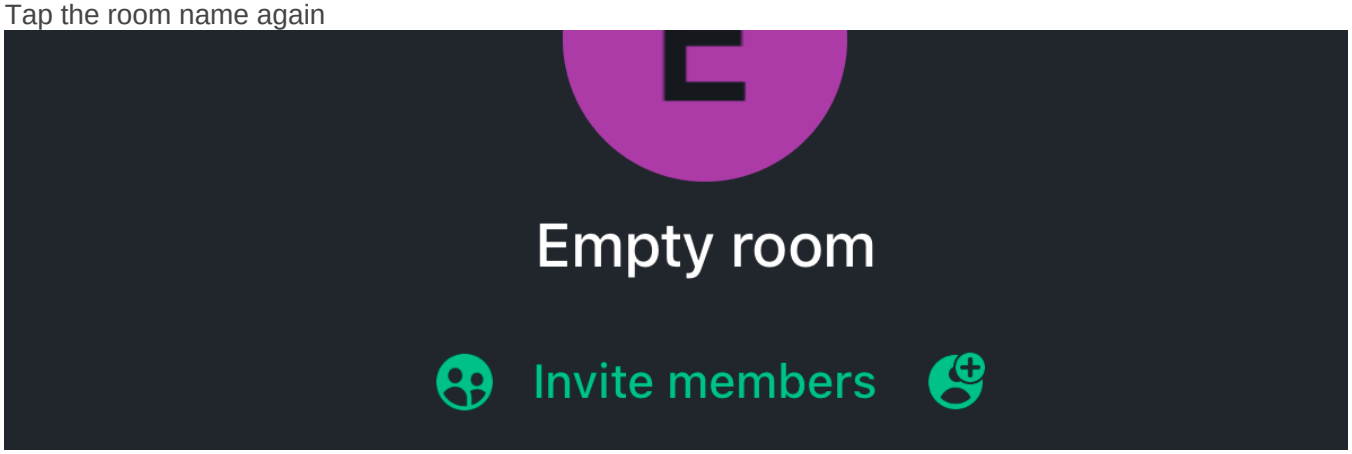
2. Tap `Create room`



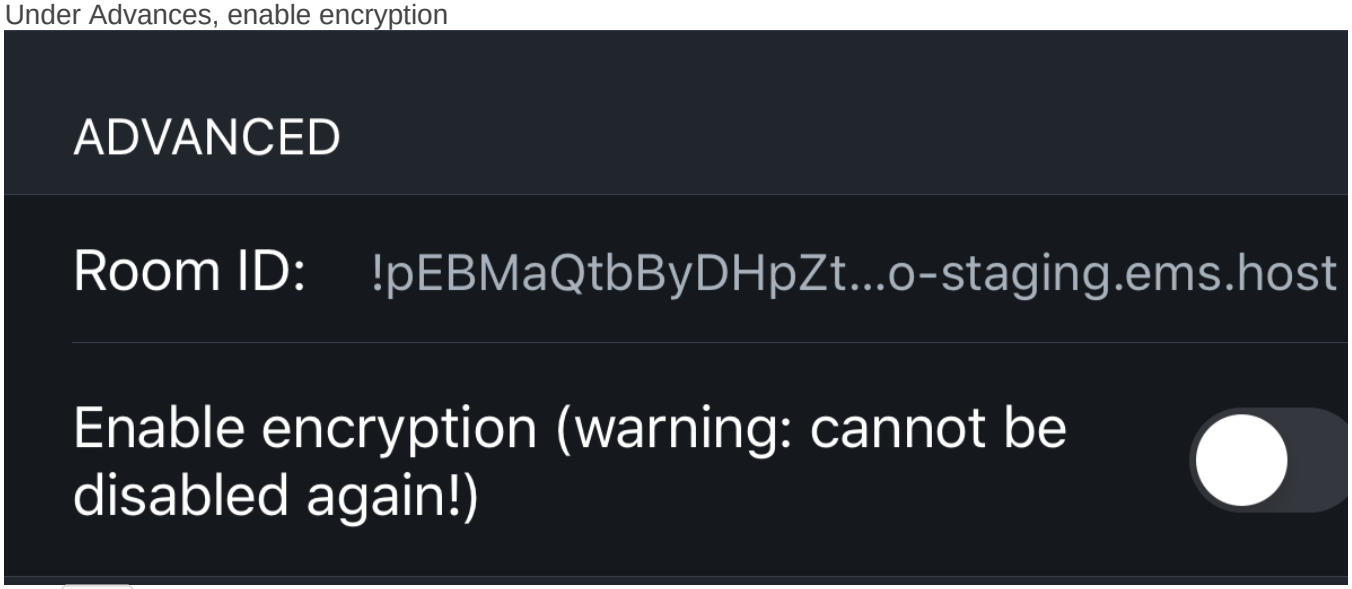
3. Tap the room name (Empty room) at the top



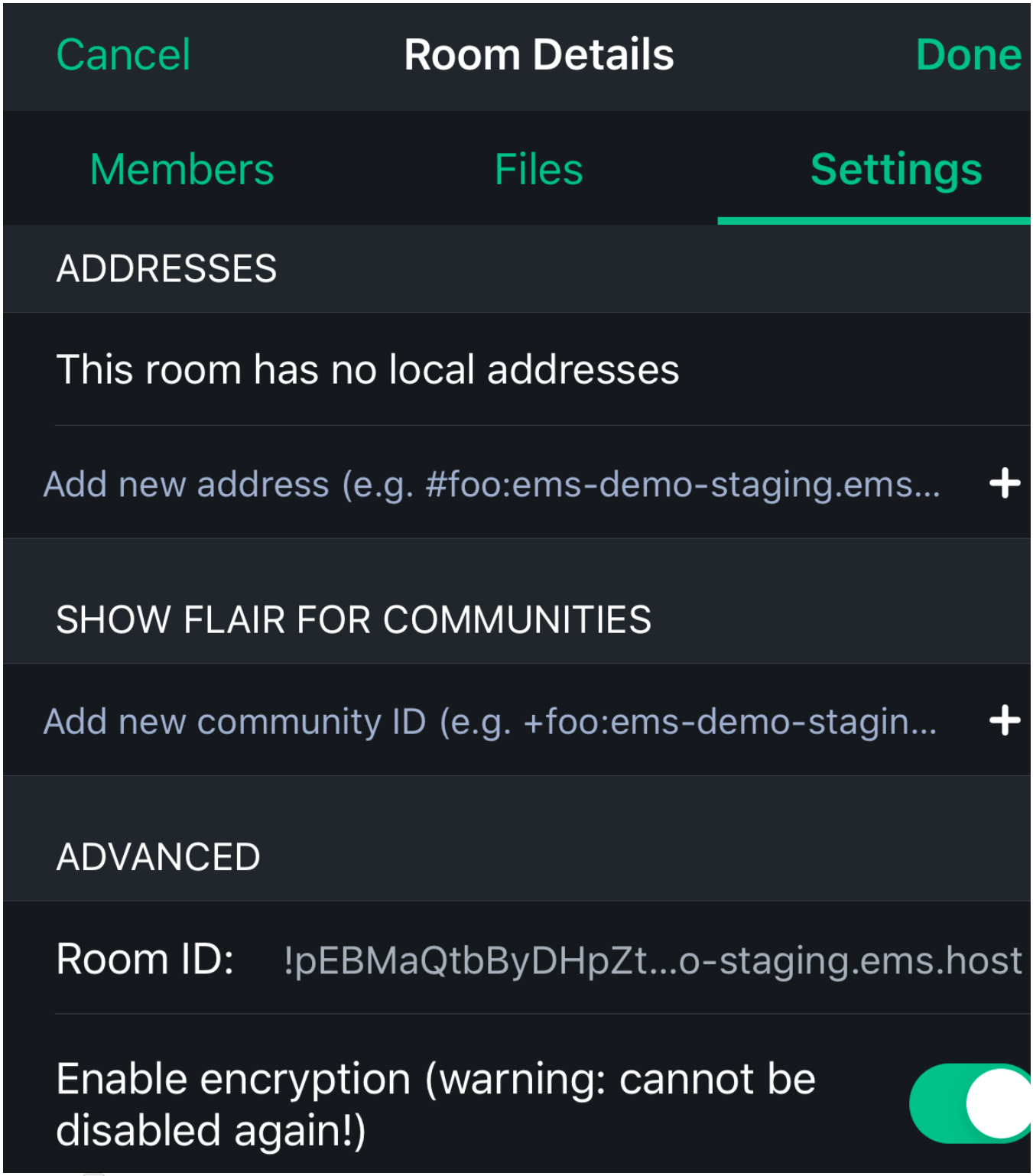
4. Tap the room name again



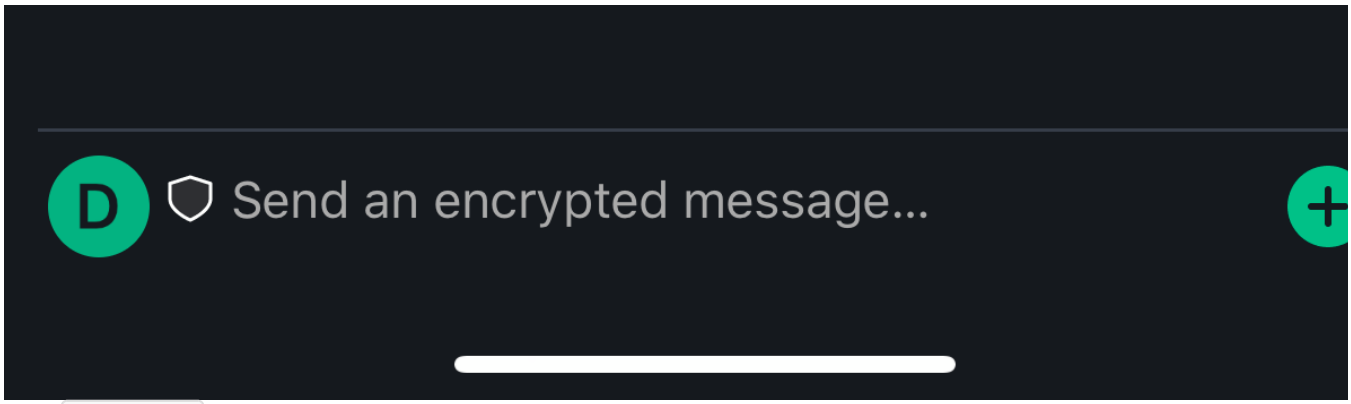
5. Under Advances, enable encryption



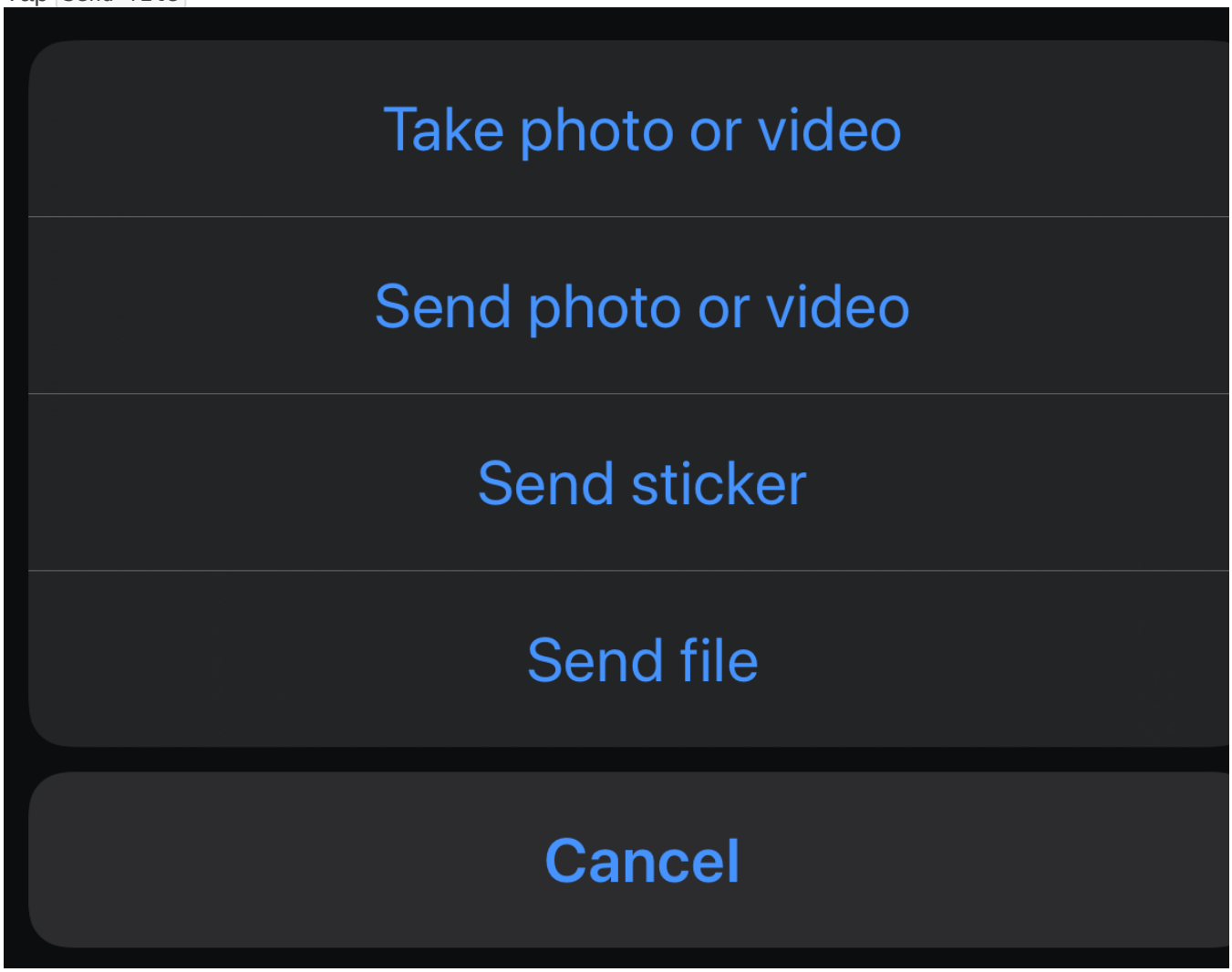
6. Tab `Done` in the top right



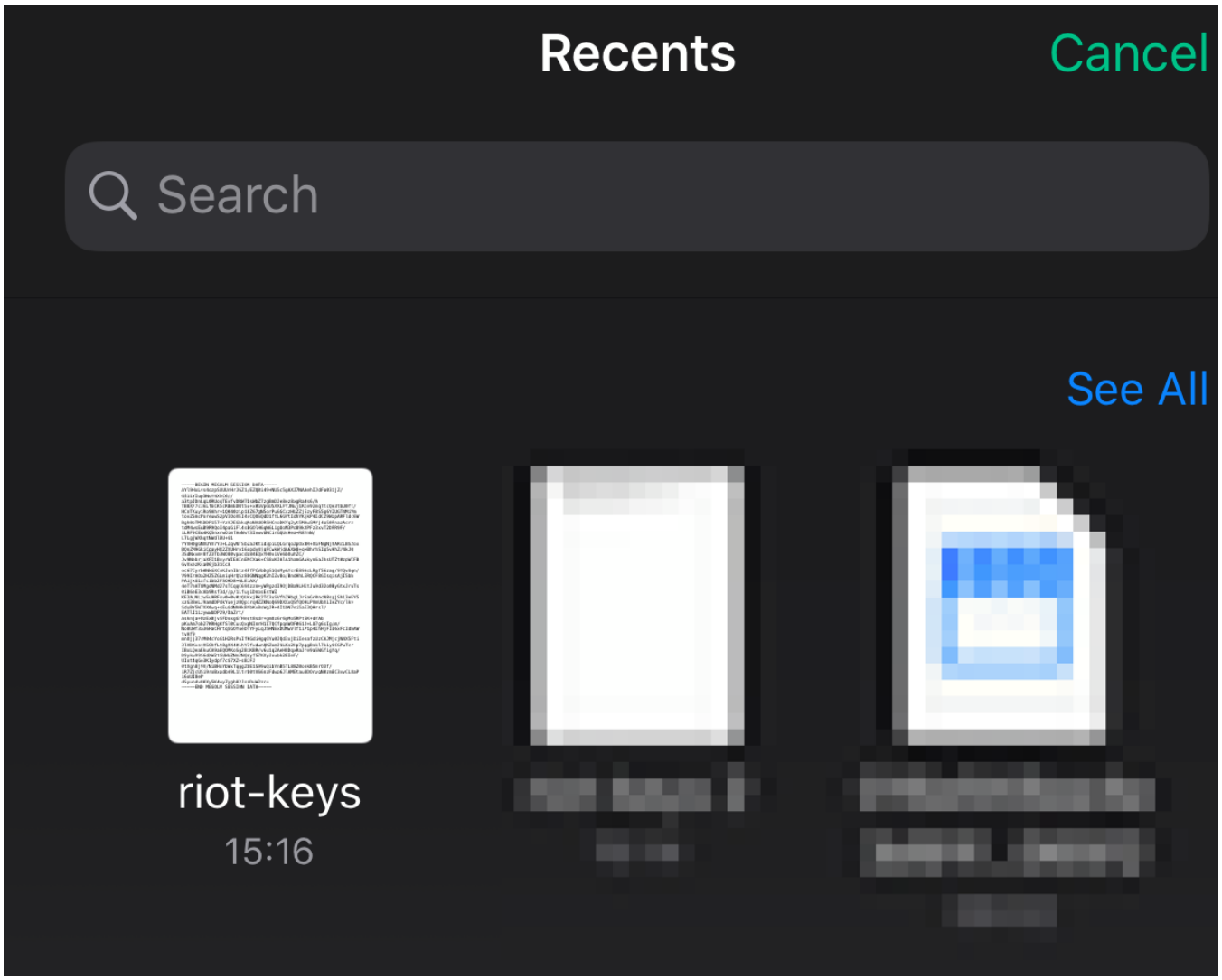
7. Tab the to send a file



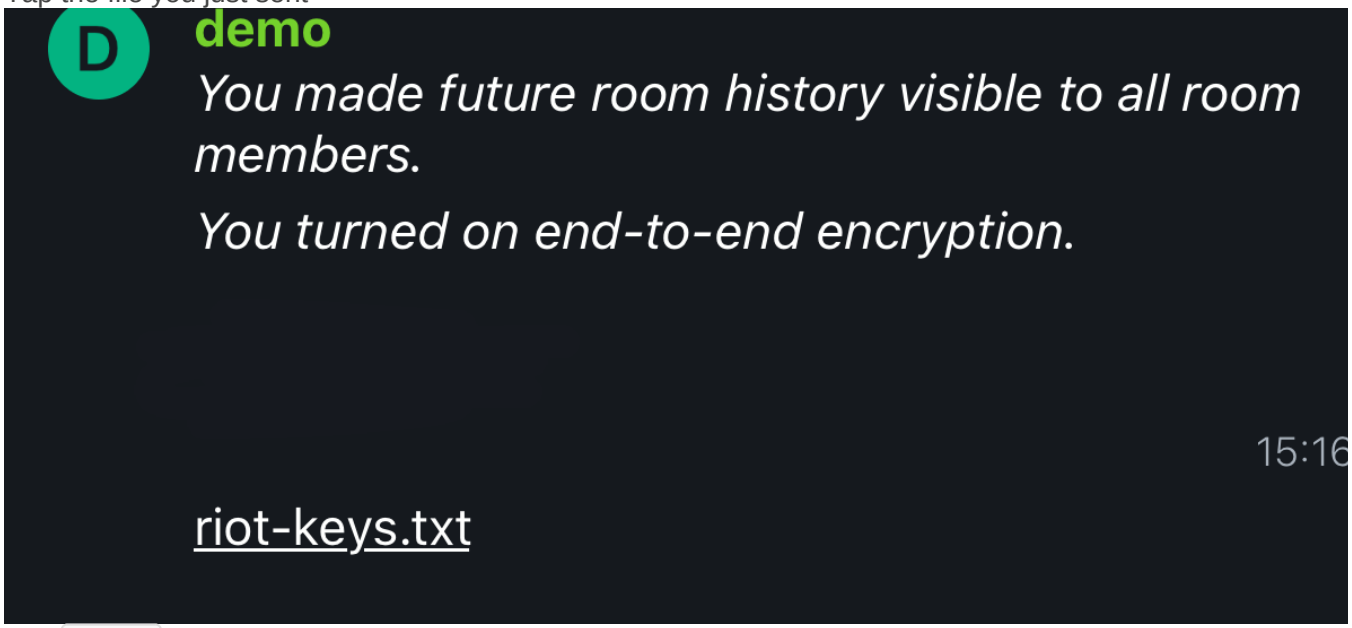
8. Tap `Send file`



9. Browse to and select your export

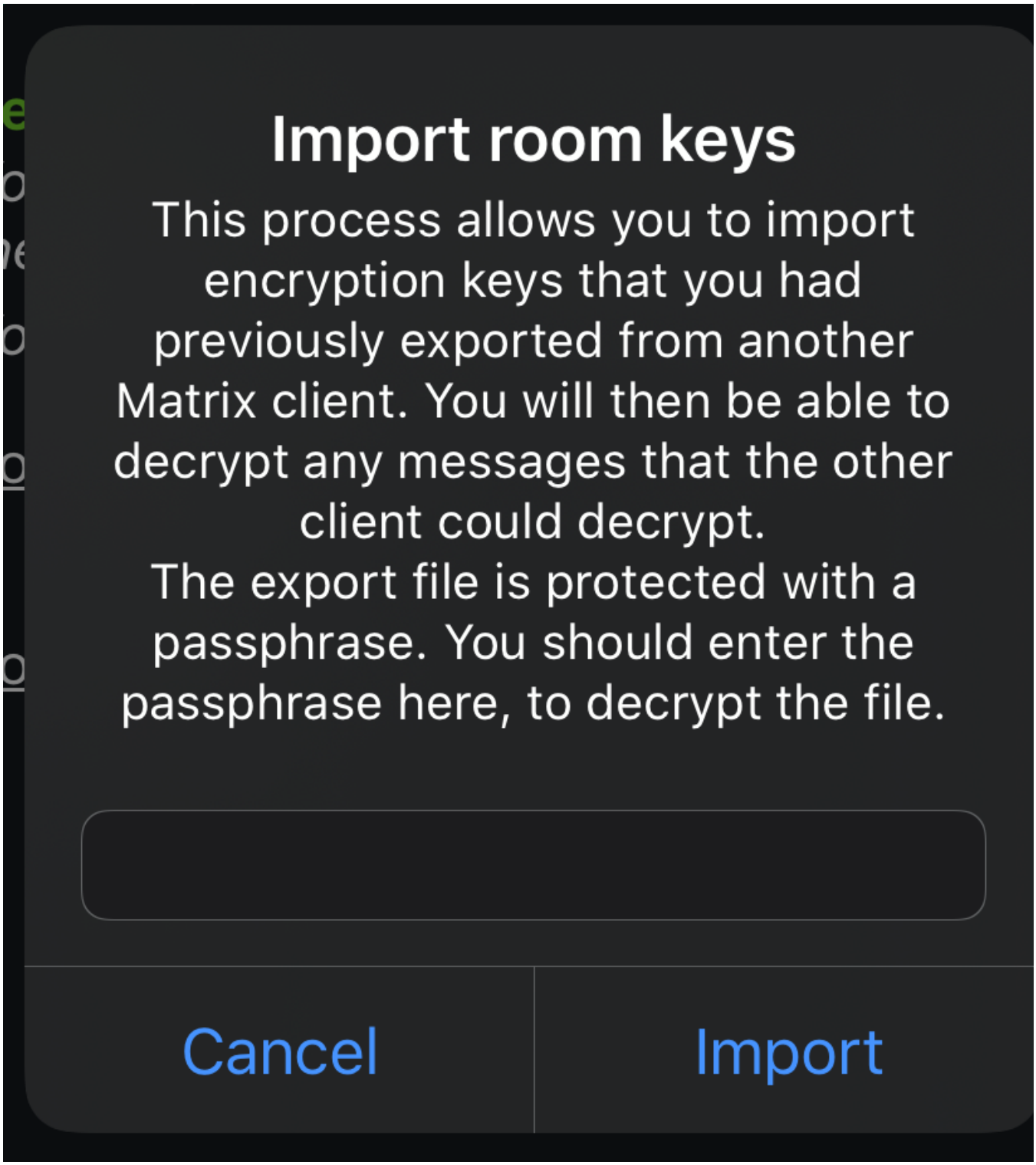


10. Tap the file you just sent



11. Tap `Import`

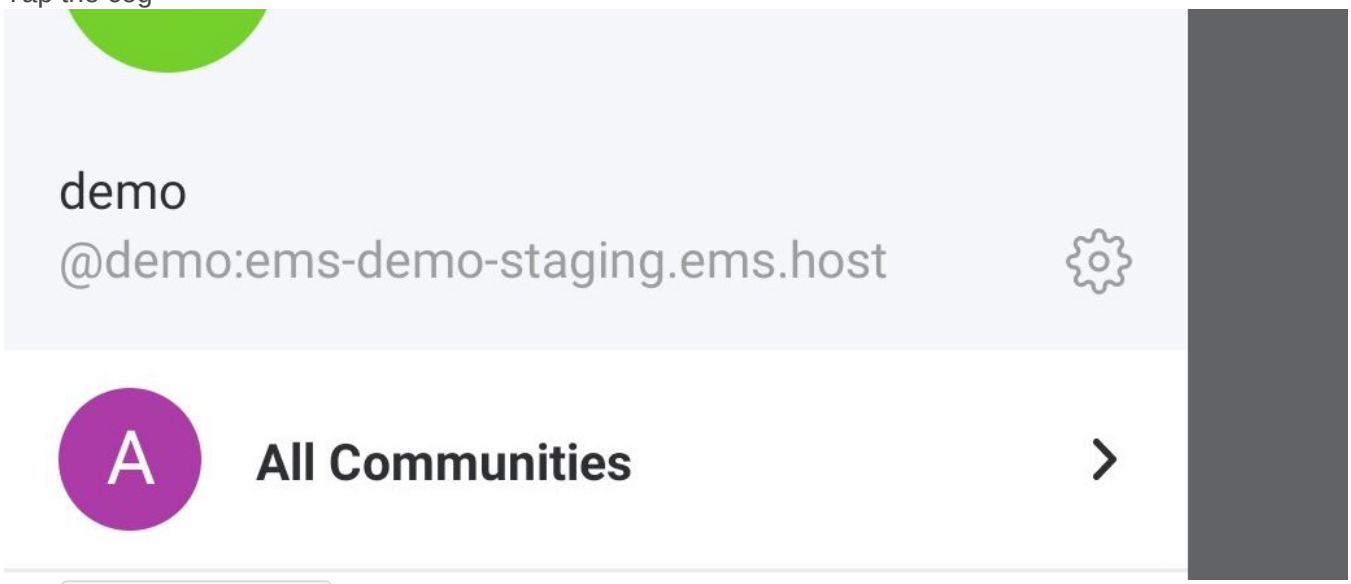
12. Enter your passphrase and tap `Import`



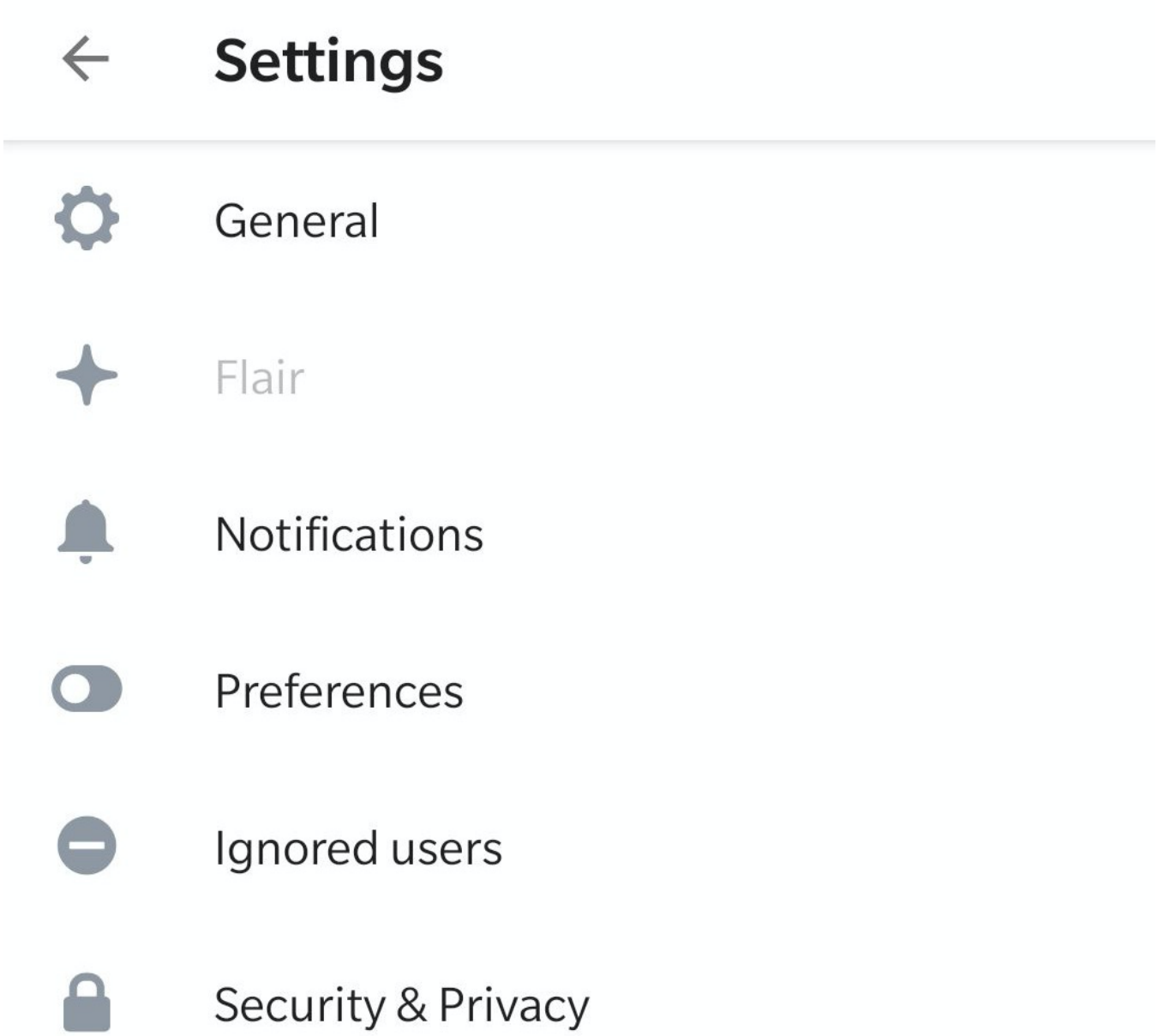
Element Android

Export

1. Tap your user picture in the top right
2. Tap the cog

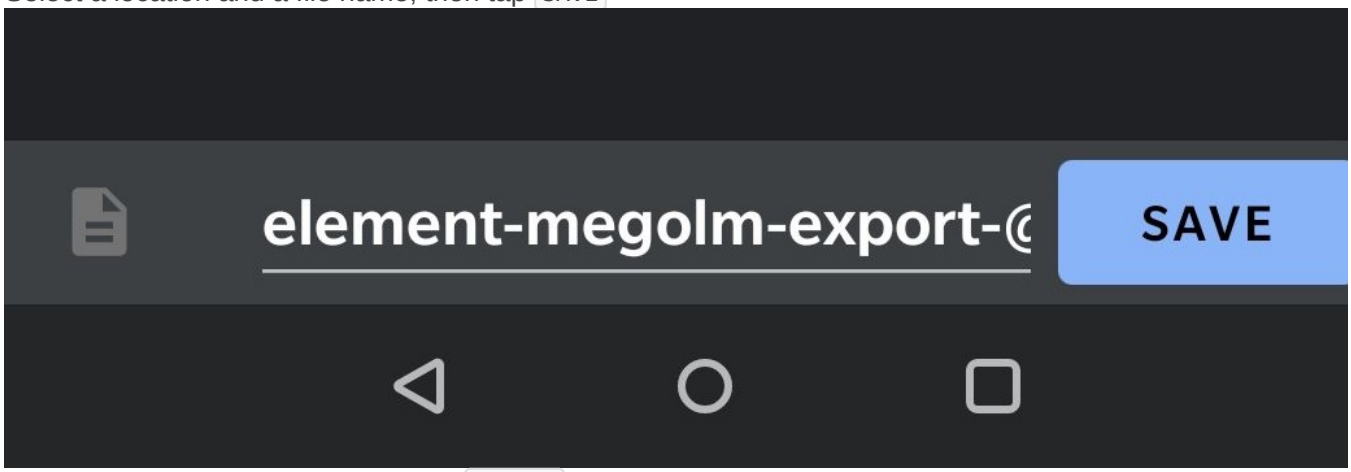


3. Tap `Security & Privacy`

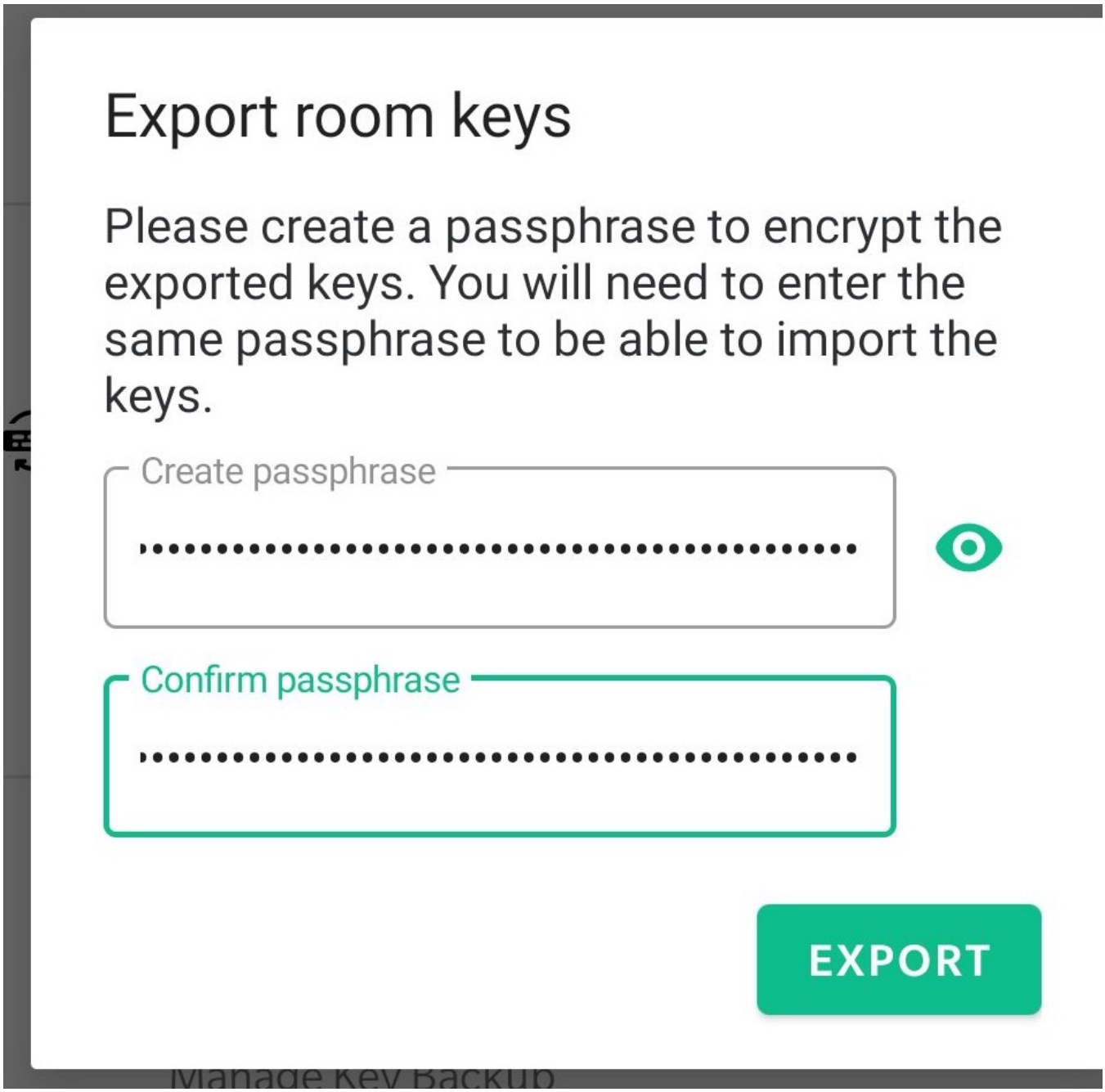


4. Tap `Export E2E room keys`

5. Select a location and a file name, then tap `SAVE`

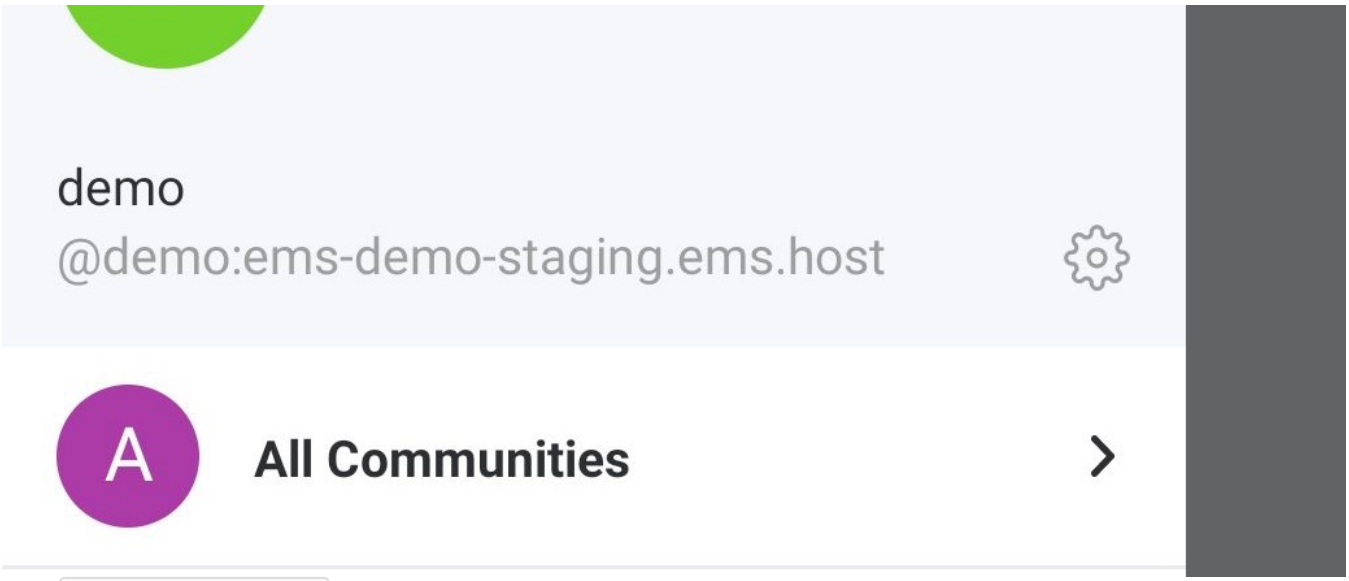


6. Enter a secure passphrase, then tap `EXPORT`

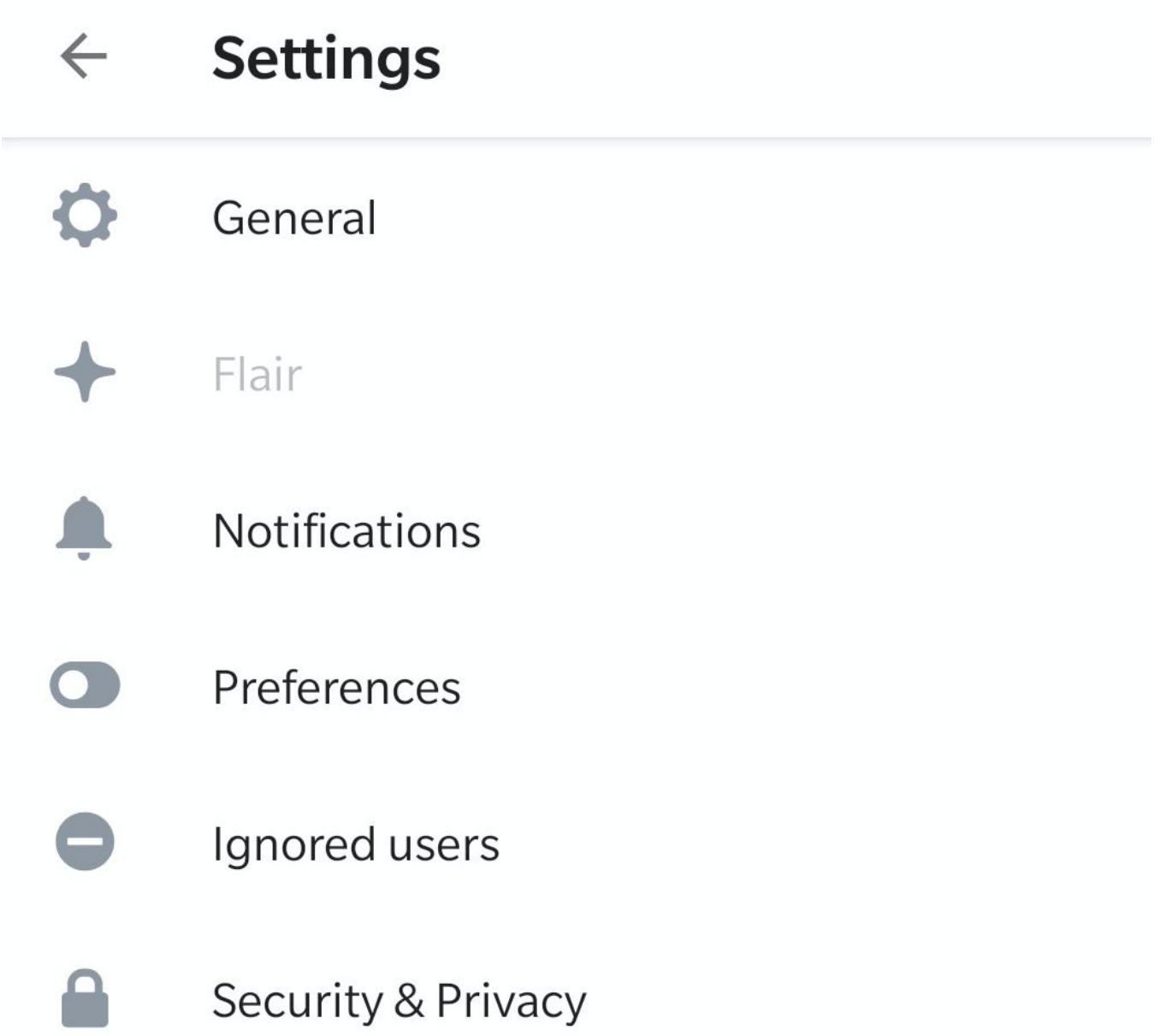


Import

1. Tap your user picture in the top right
2. Tap the cog

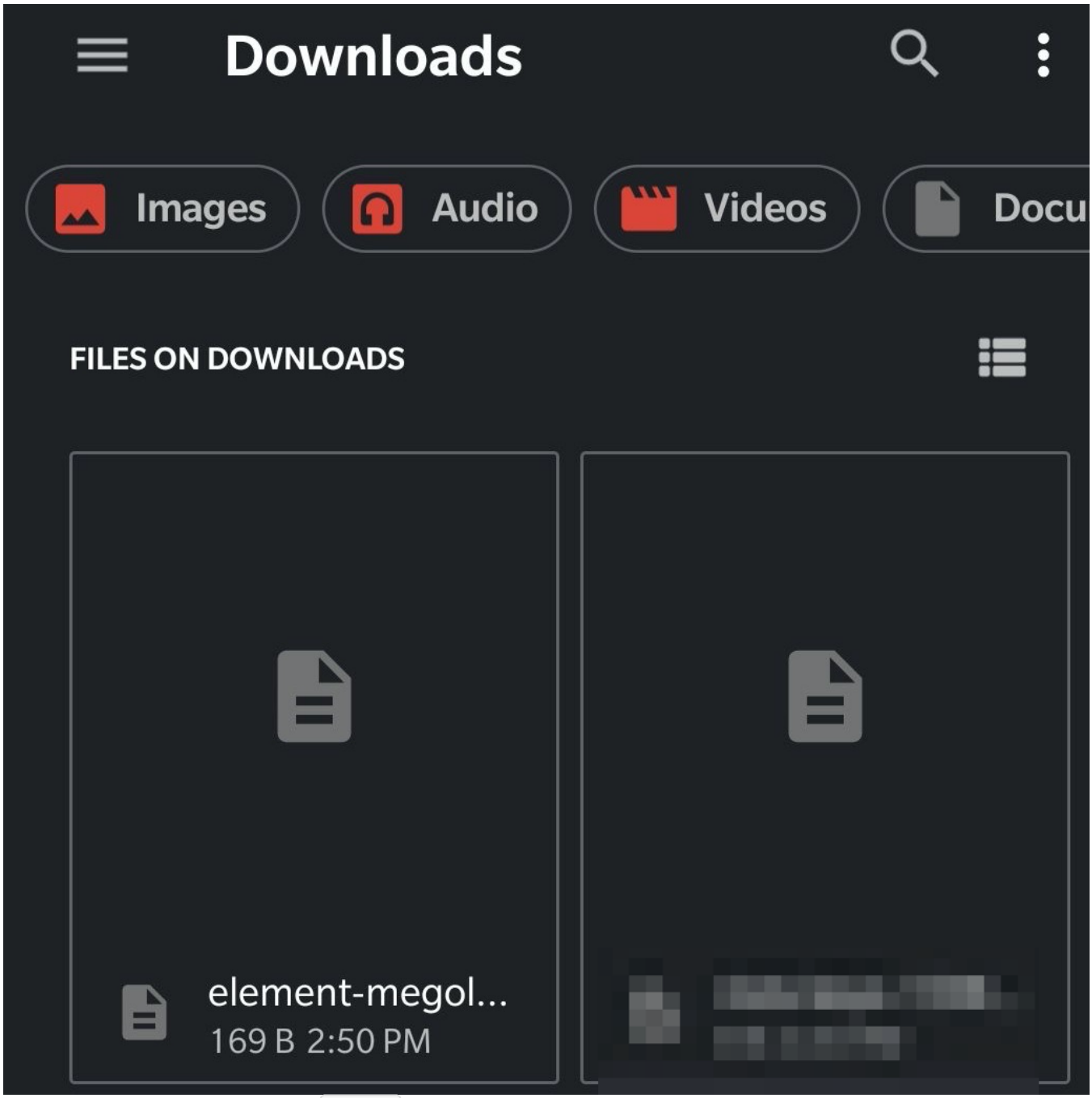


3. Tap `Security & Privacy`

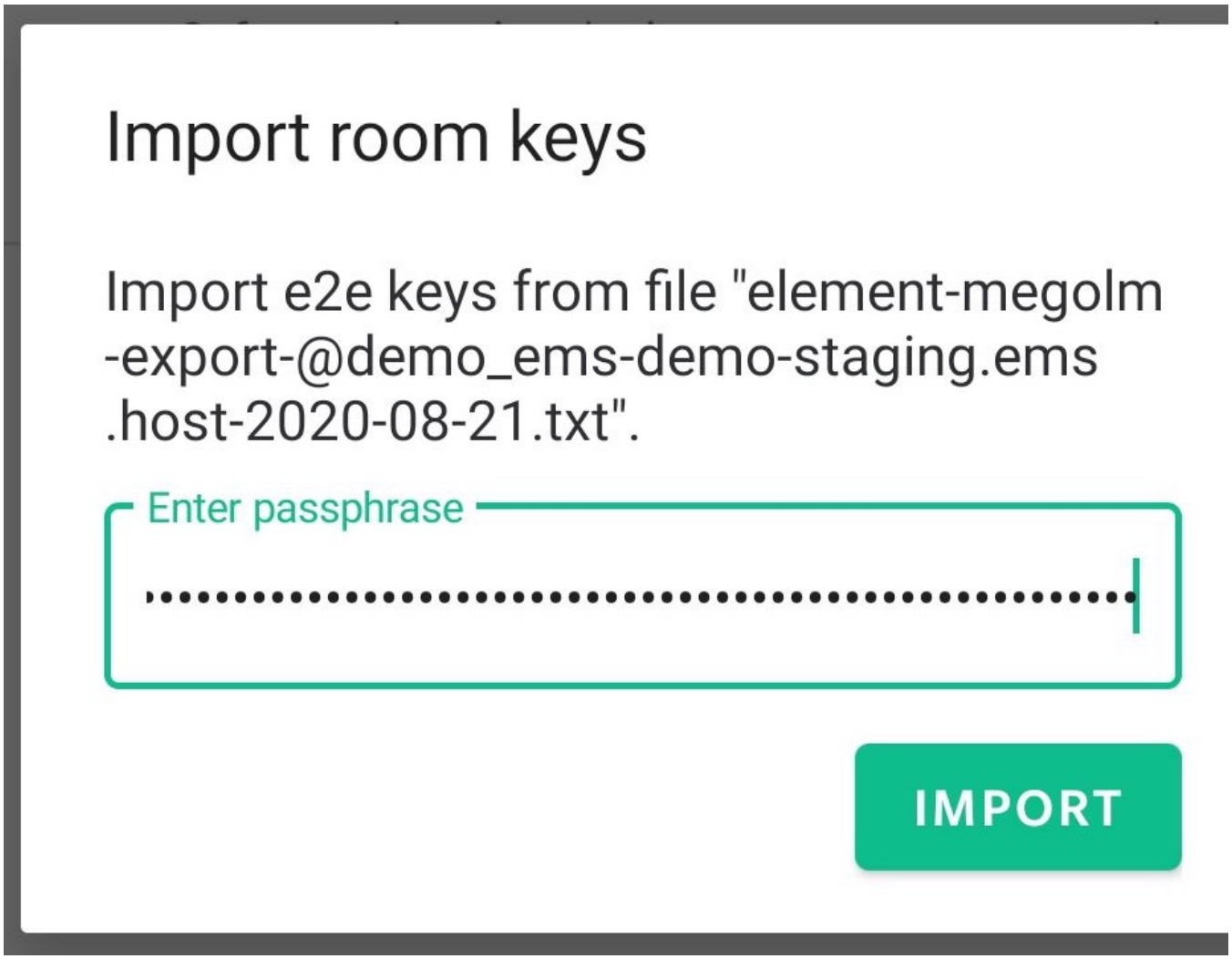


4. Tap `Import E2E room keys`

5. Browse to and select your export



6. Enter your passphrase and tap `IMPORT`


Import room keys
Import e2e keys from file "element-megolm-export-@demo_ems-demo-staging.ems.host-2020-08-21.txt".
Enter passphrase
IMPORT

Reset Cross Signing

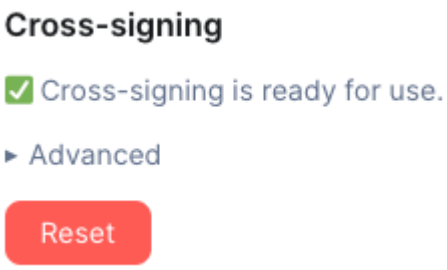
Only do this if you have forgotten or lost your cross signing backup passphrase.

Please read through the entire document before starting to make sure you understand the consequences of doing this.

- **If you have an active session**
- **If you DO NOT have an active session**

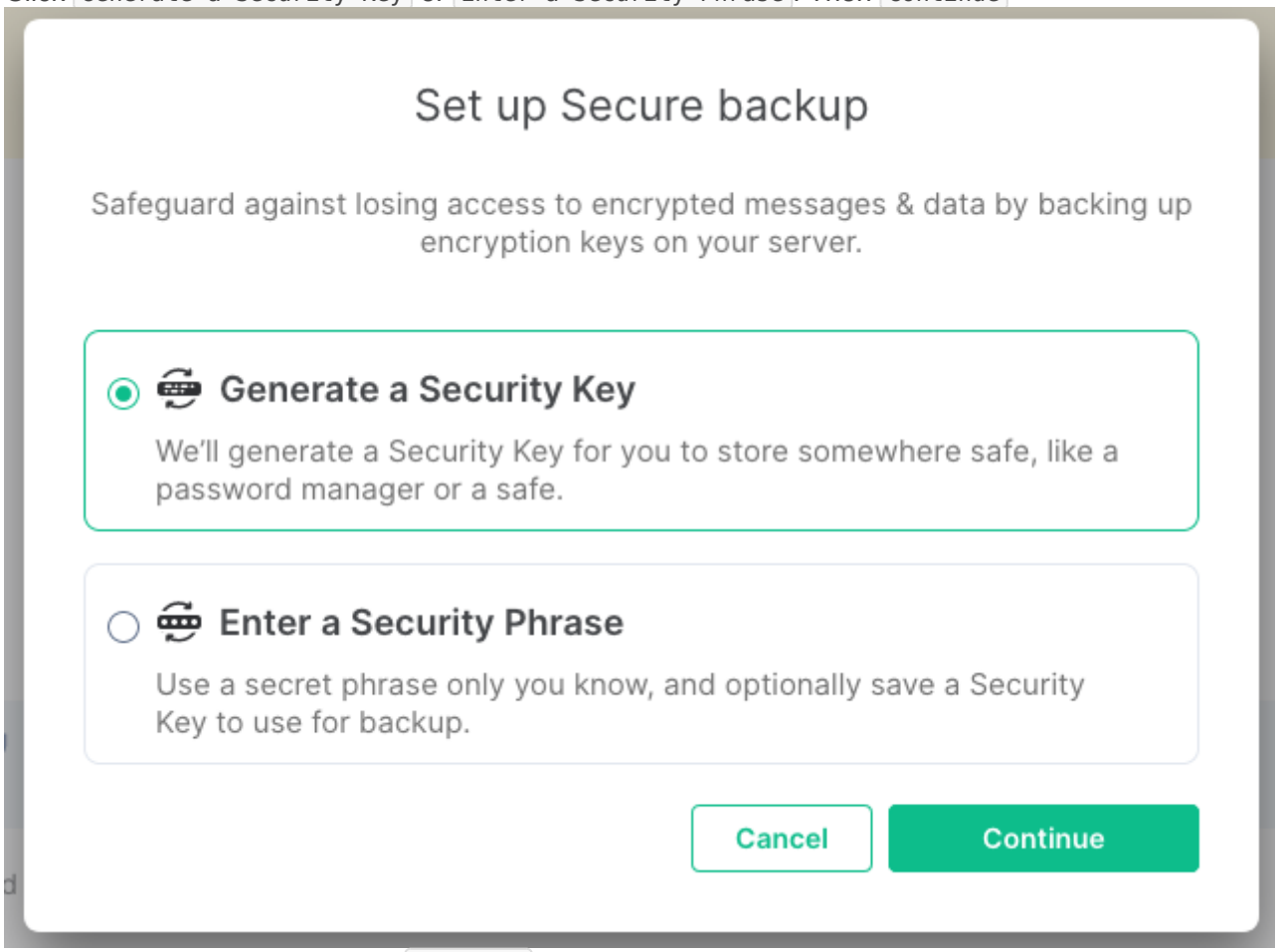
If you have an active session

1. You may wish to backup your keys before doing this just to be on the safe side if something goes wrong: See Export and Import E2E Room Keys
2. Click `Reset` in the `Cross-signing` section

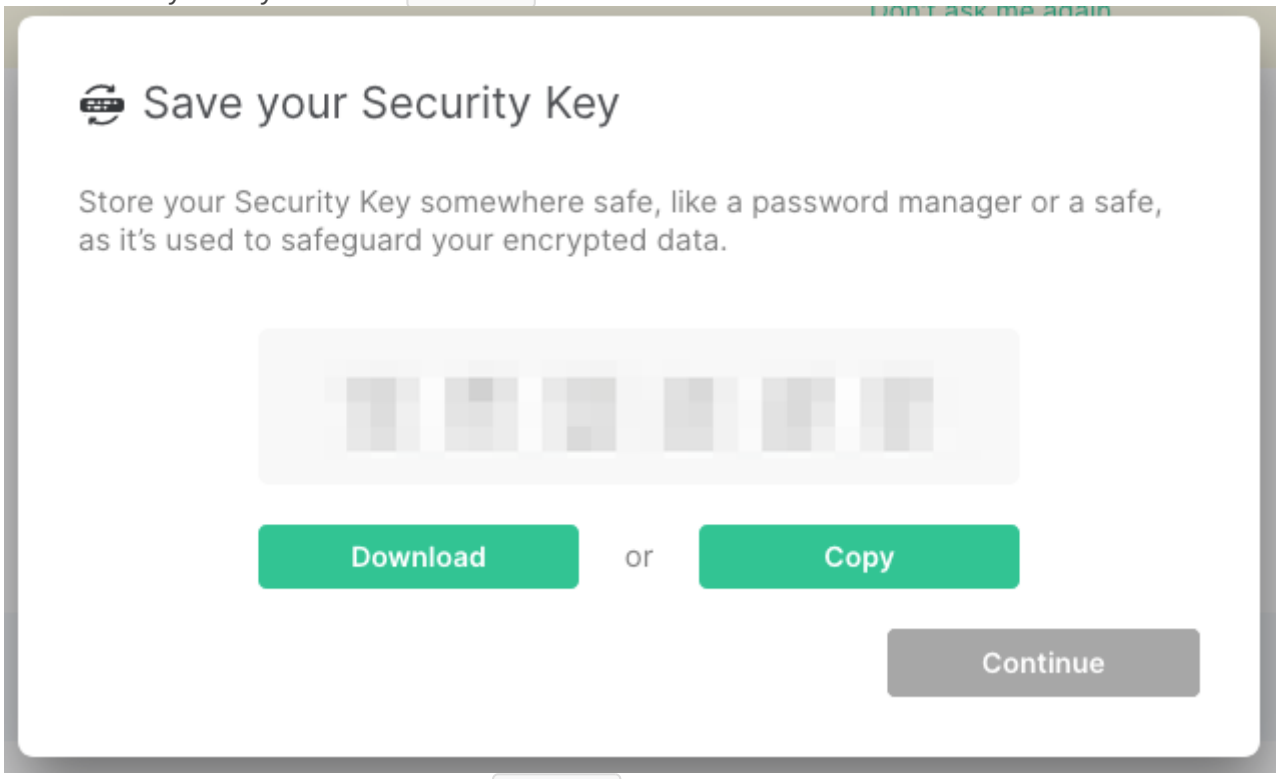


3. Click `Clear cross-signing keys`

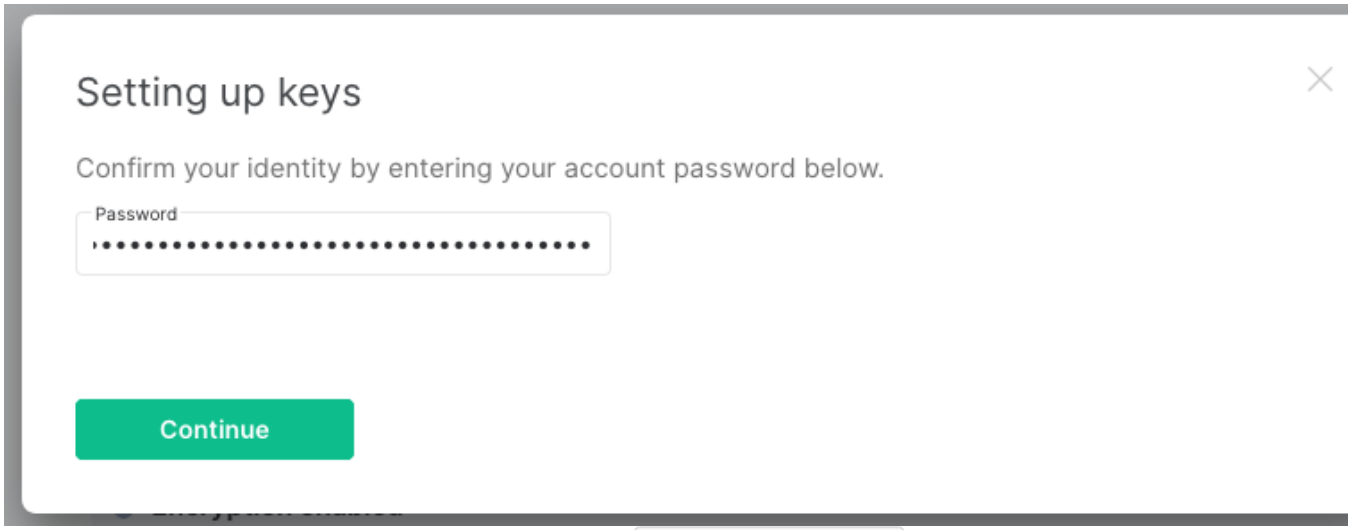
4. Click `Generate a Security Key` or `Enter a Security Phrase`. Then `Continue`



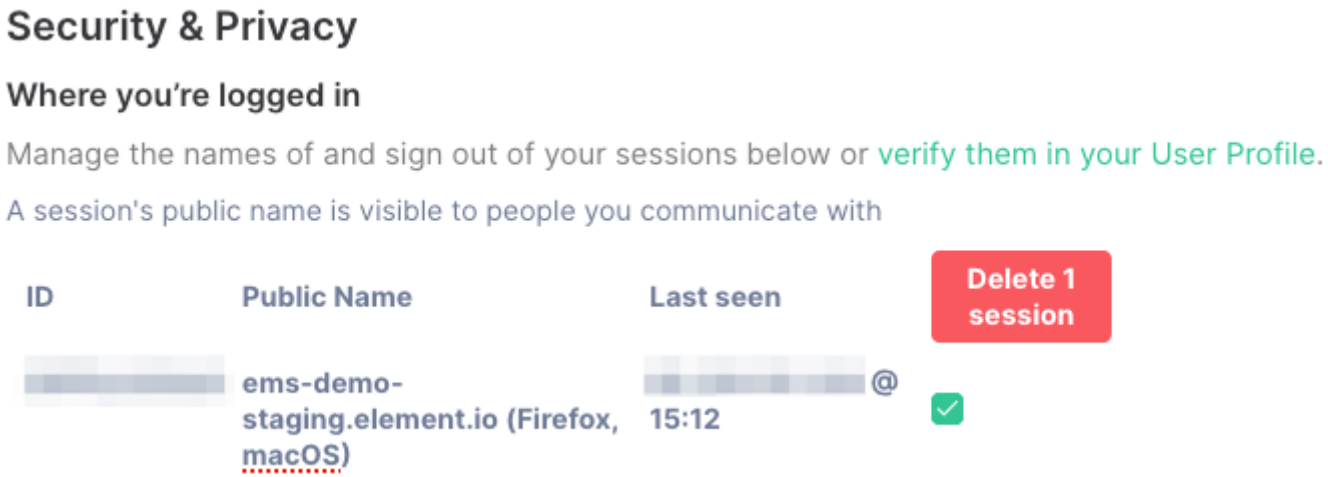
5. Take note of your key then click `Continue`



6. Enter your account password and click `Continue`



7. You can delete any untrusted sessions in Element `Security & Privacy` settings. Select the sessions you want to remove and click `Delete 1 session`

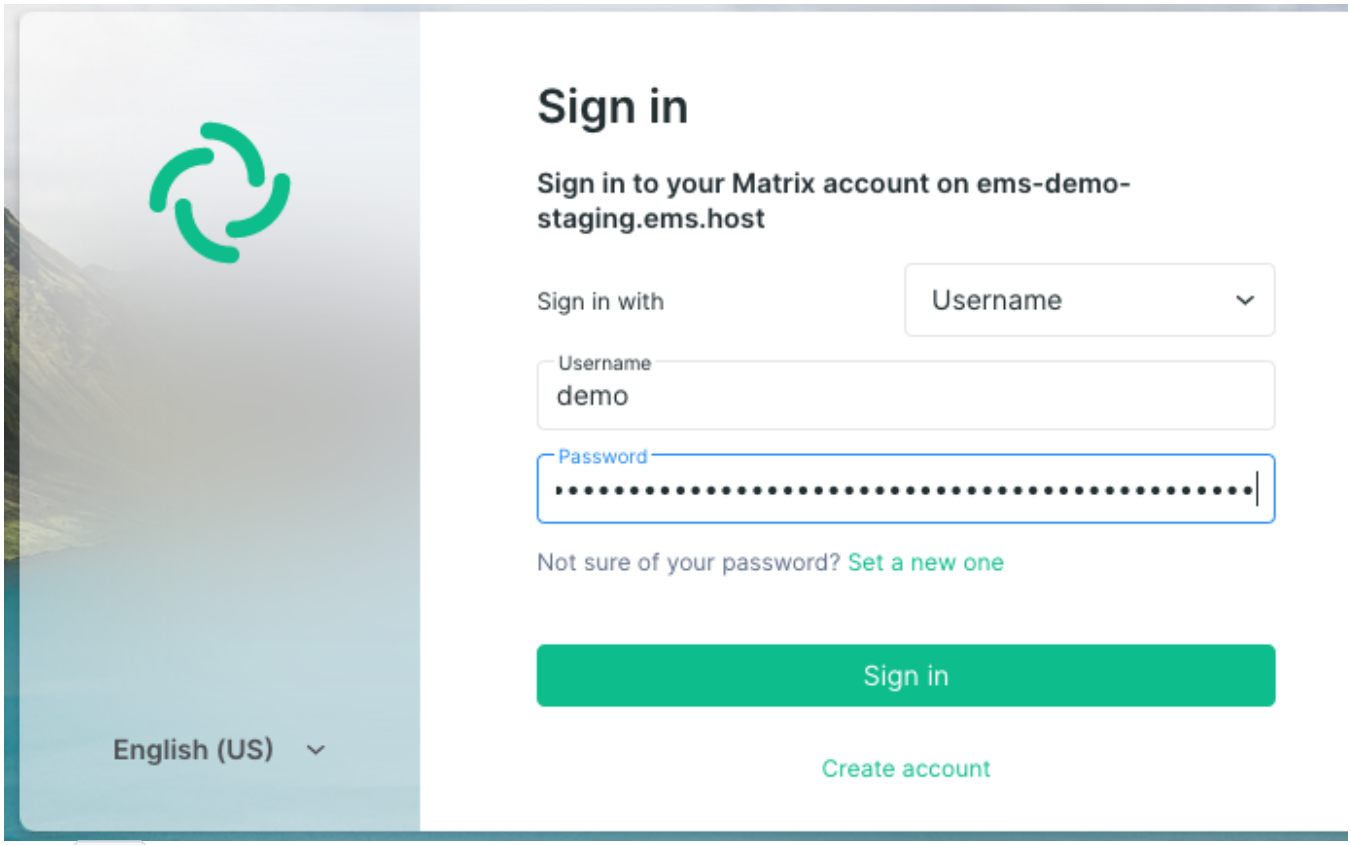


8. Optionally, Sign out old devices no longer needed

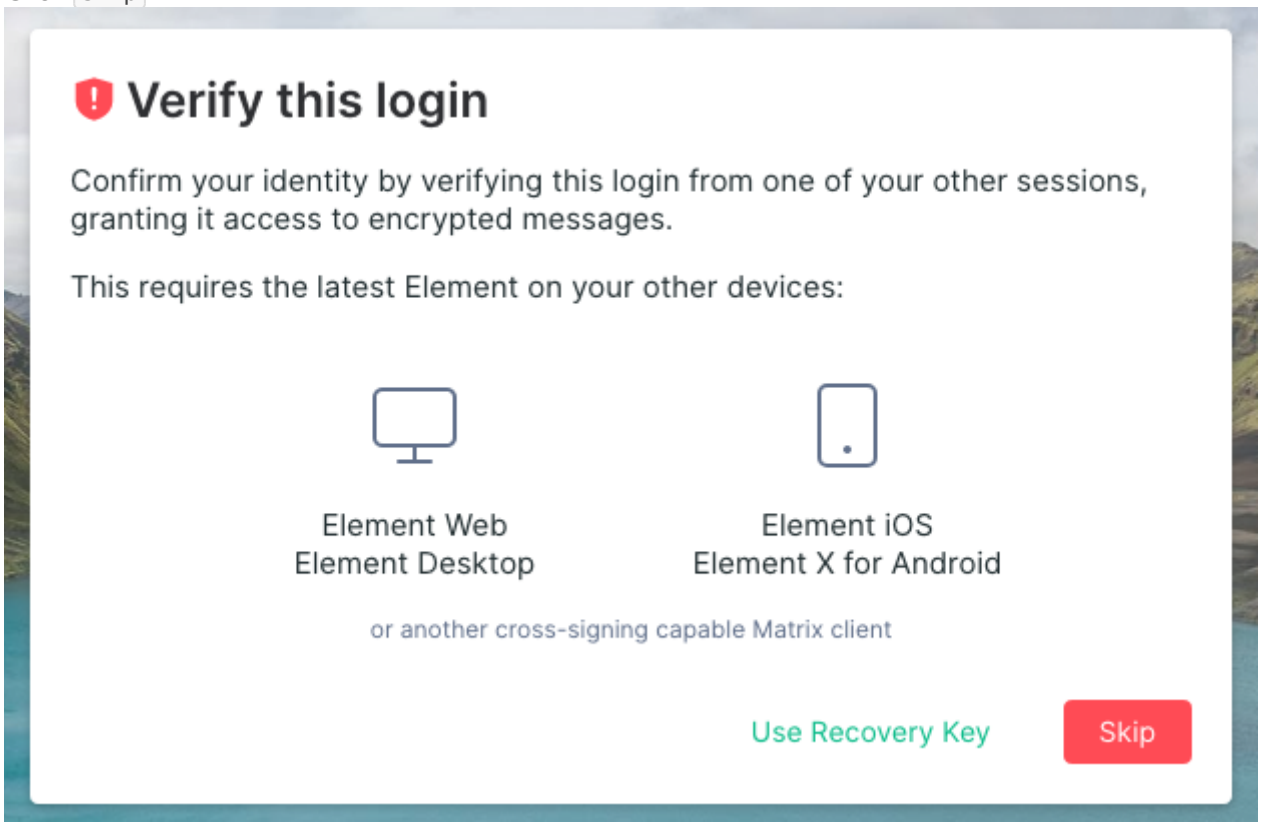
If you DO NOT have an active session

Doing this will destroy all your keys and you will NOT be able to access any historical encrypted messages.

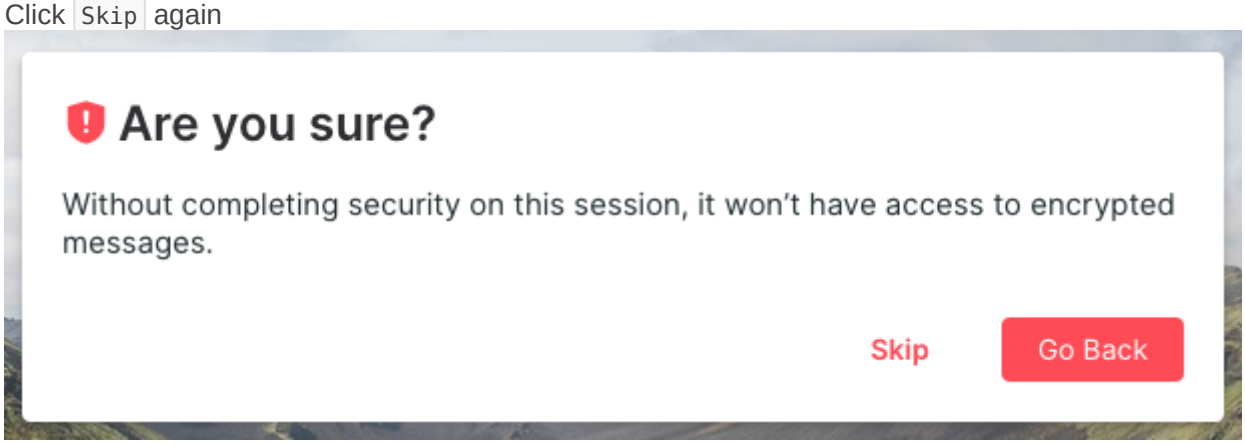
1. Log in to Element


Sign in
Sign in to your Matrix account on ems-demo-staging.ems.host
Sign in with
Username
Username
demo
Password
Not sure of your password? Set a new one
Sign in
English (US)
Create account

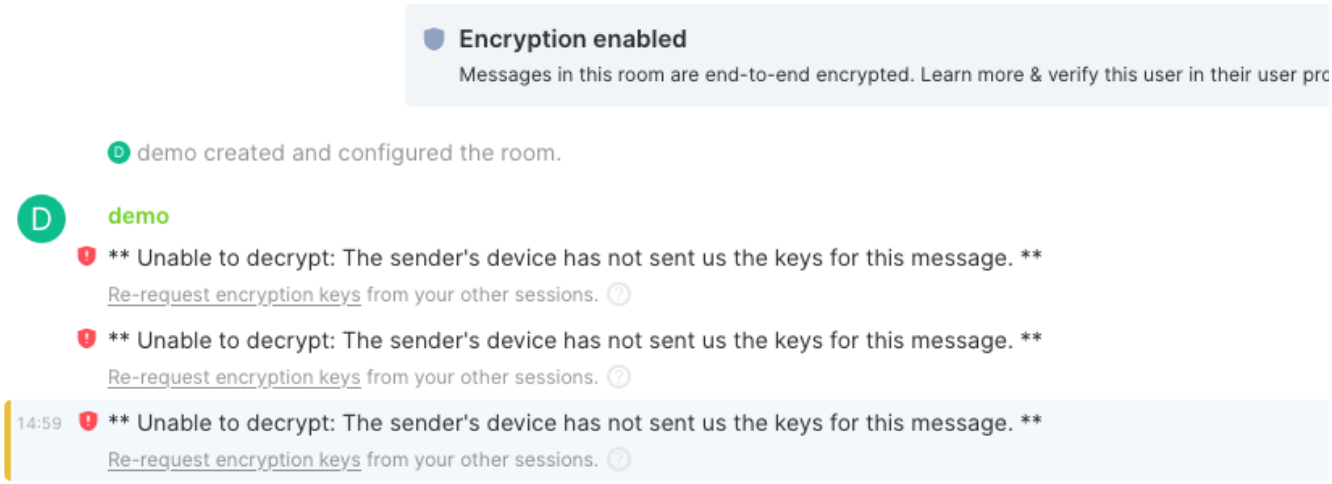
2. Click `Skip`


Verify this login
Confirm your identity by verifying this login from one of your other sessions, granting it access to encrypted messages.
This requires the latest Element on your other devices:
Element Web
Element Desktop
Element iOS
Element X for Android
or another cross-signing capable Matrix client
Use Recovery Key
Skip

3. Click `Skip` again



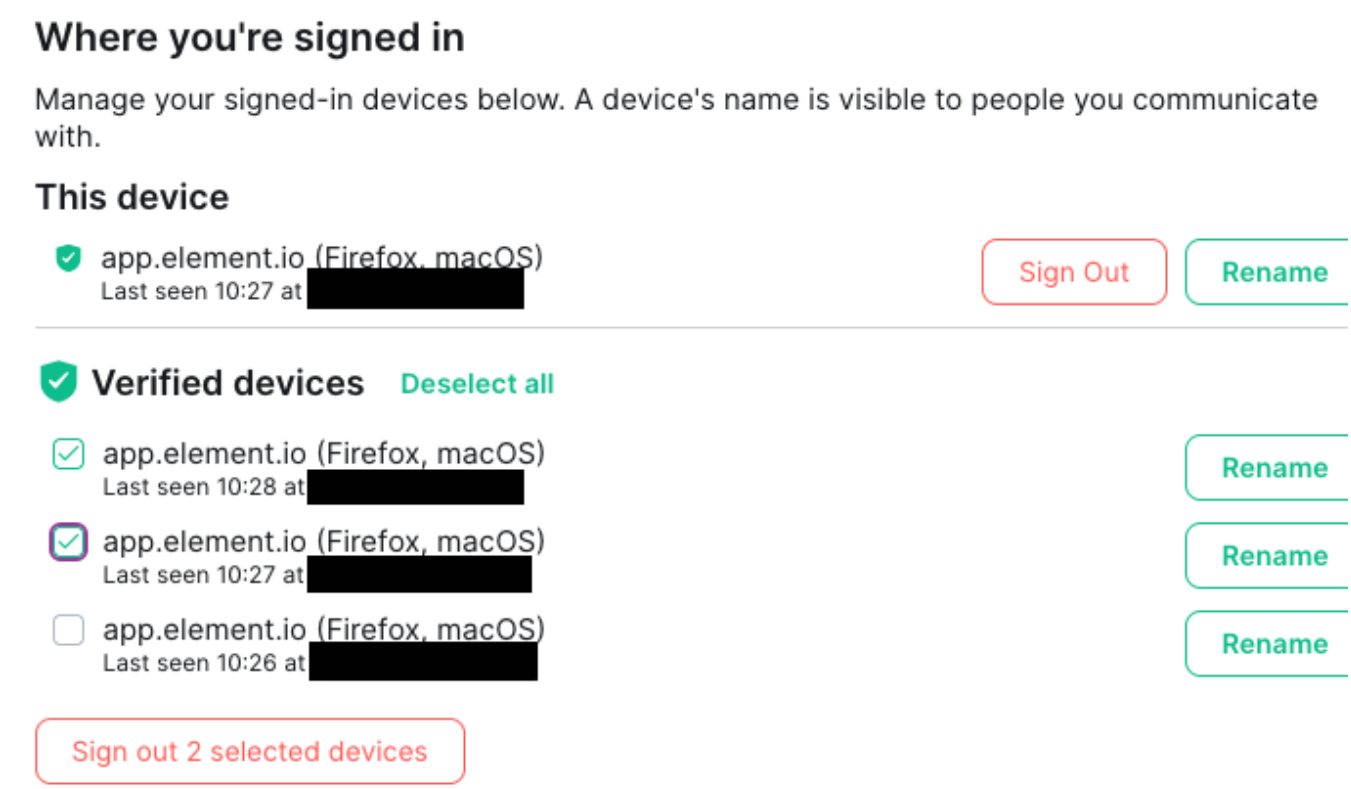
4. Do not connect to Key Backup or verify session when asked
5. Note that you will not be able to decrypt any previous messages after doing this



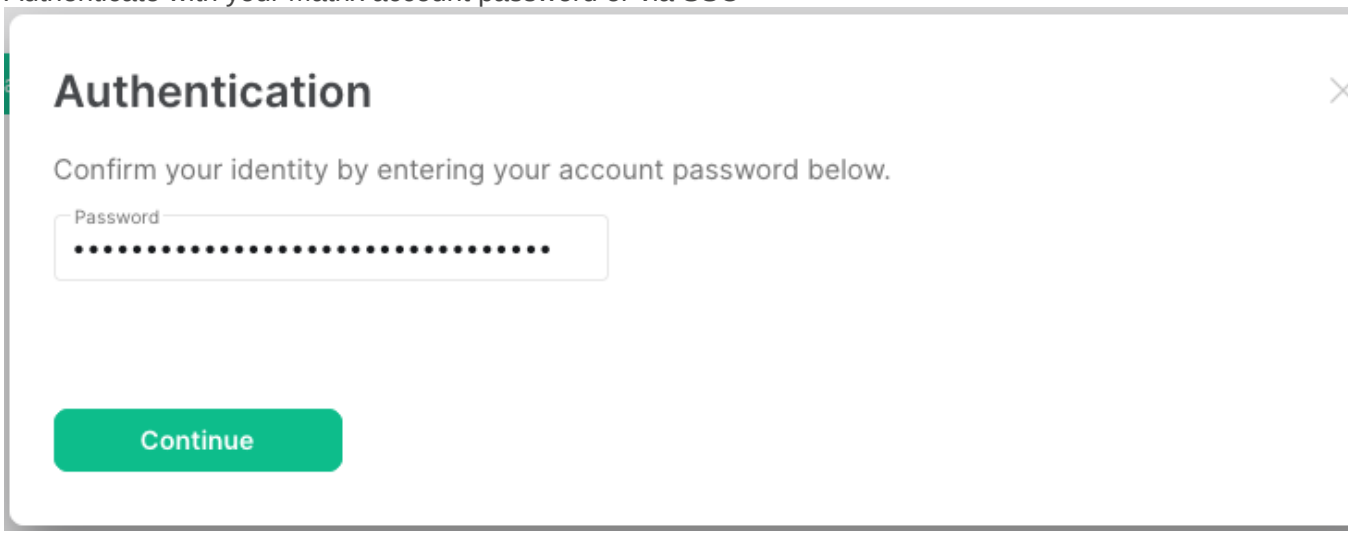
6. Follow the steps from If you have an active session

Sign out old devices

1. Go to Element `Security & Privacy` settings
2. Select the devices you wish to sign out



3. Click `Sign out n selected devices`
4. Authenticate with your Matrix account password or via SSO



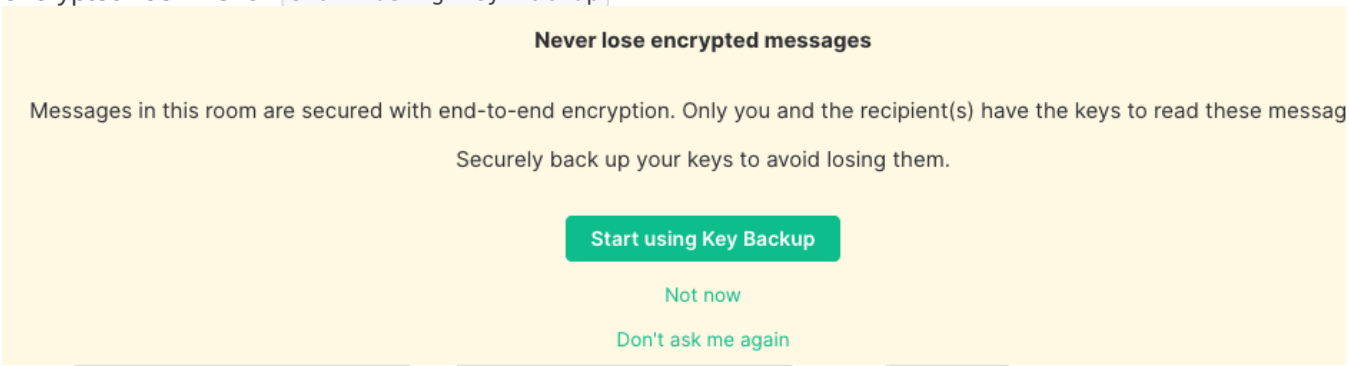
Set up Cross Signing

On first login to a new account

1. Sign up or log in
2. Click `Generate a Security Key` or `Enter a Security Phrase`. Then click `Continue`
3. Take note of your key, then click `Continue`

If you did not set it up on first login, or if you did not get asked

1. If you do not have key backup configured, you will be asked to set it up the first time you enter an encrypted room. Click `Start using Key Backup`

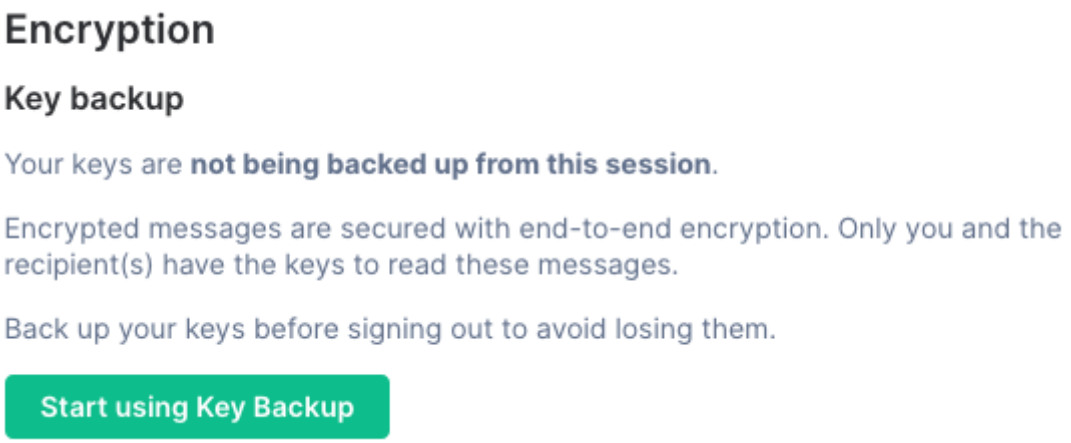


2. Click `Generate a Security Key` or `Enter a Security Phrase`. Then `Continue`
3. Take note of your key, then click `Continue`
4. Enter your account password, then click `Continue`

If you clicked Don't ask me again

1. Go to Element `Security & Privacy` settings

2. Click `Start using Key Backup`

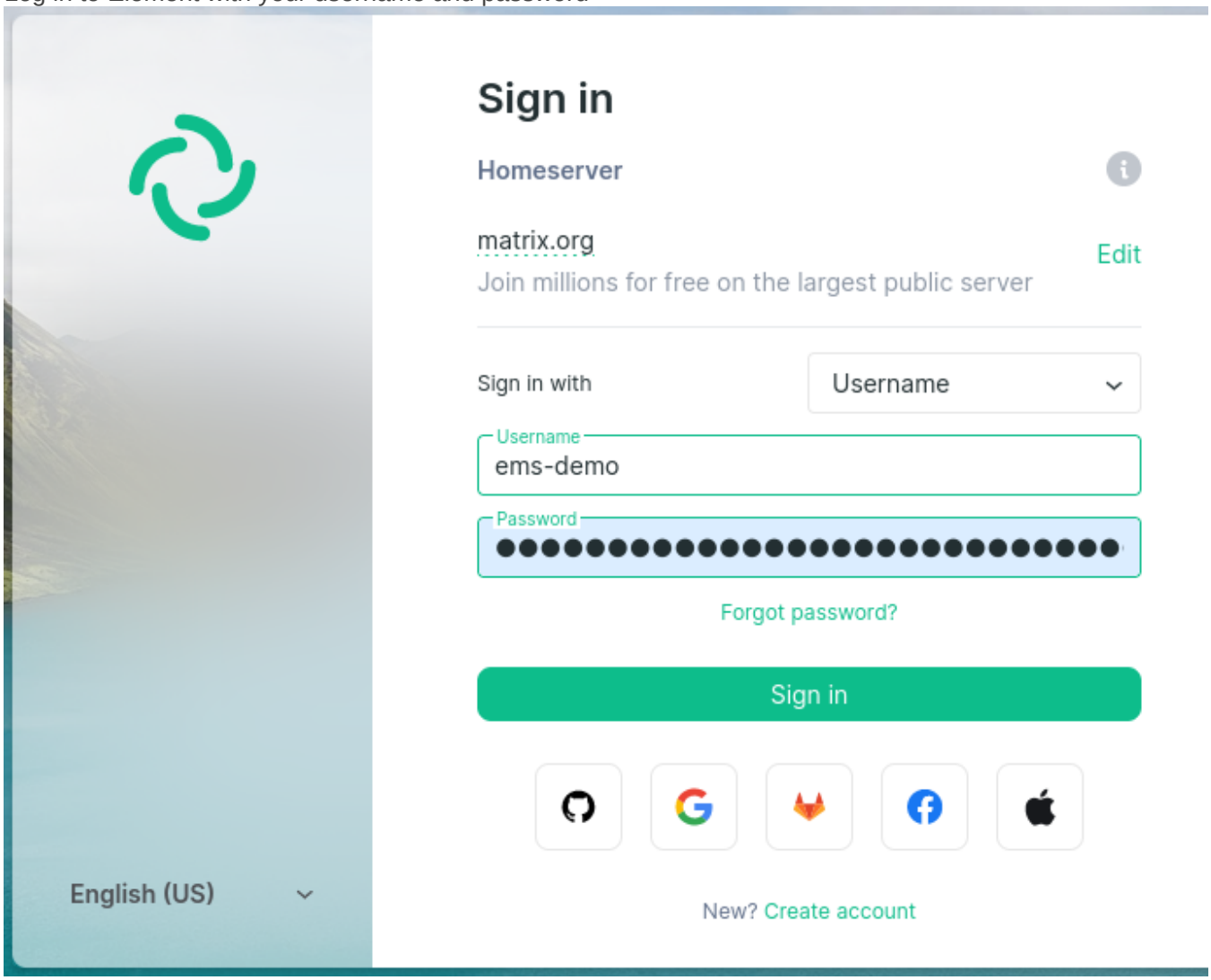


3. Click `Generate a Security Key` or `Enter a Security Phrase`. Then `Continue`
4. Take note of your key, then click `Continue`
5. Enter your account password, then click `Continue`

Verify new Login

When you log in to a new device/session, you must verify the login and connect it to cross signing and secret storage to access your backed up encryption keys for historical messages. This assumes you already have configured cross signing, see Set up Cross Signing.

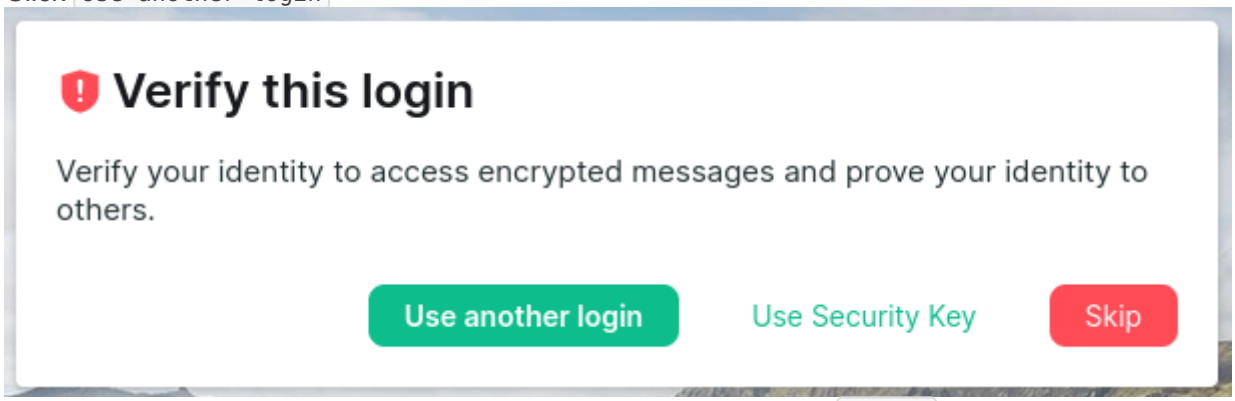
1. Log in to Element with your username and password



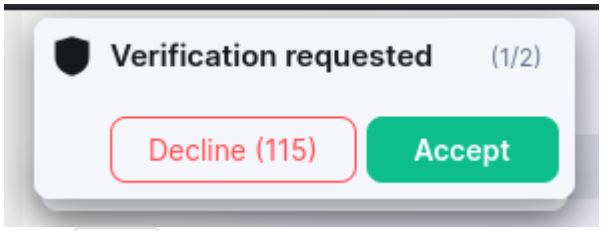
2. Choose one of the methods below for cross signing

Compare emojis using another login

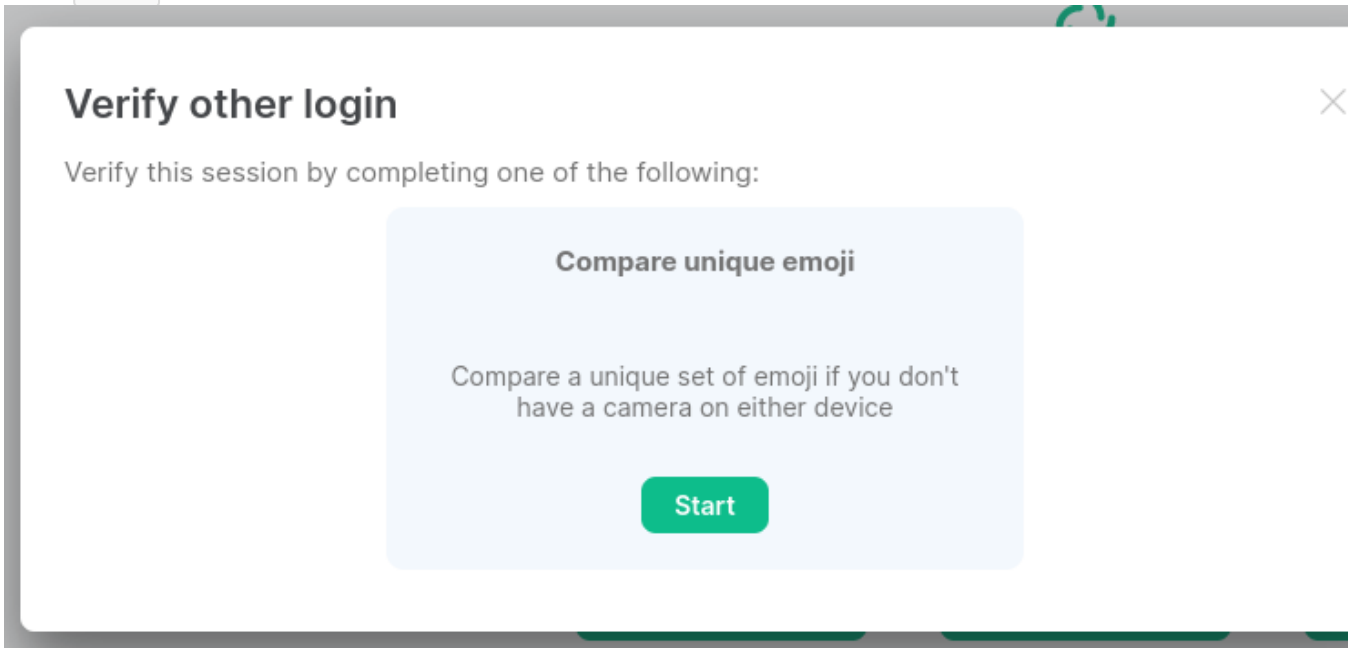
1. Click `Use another login`



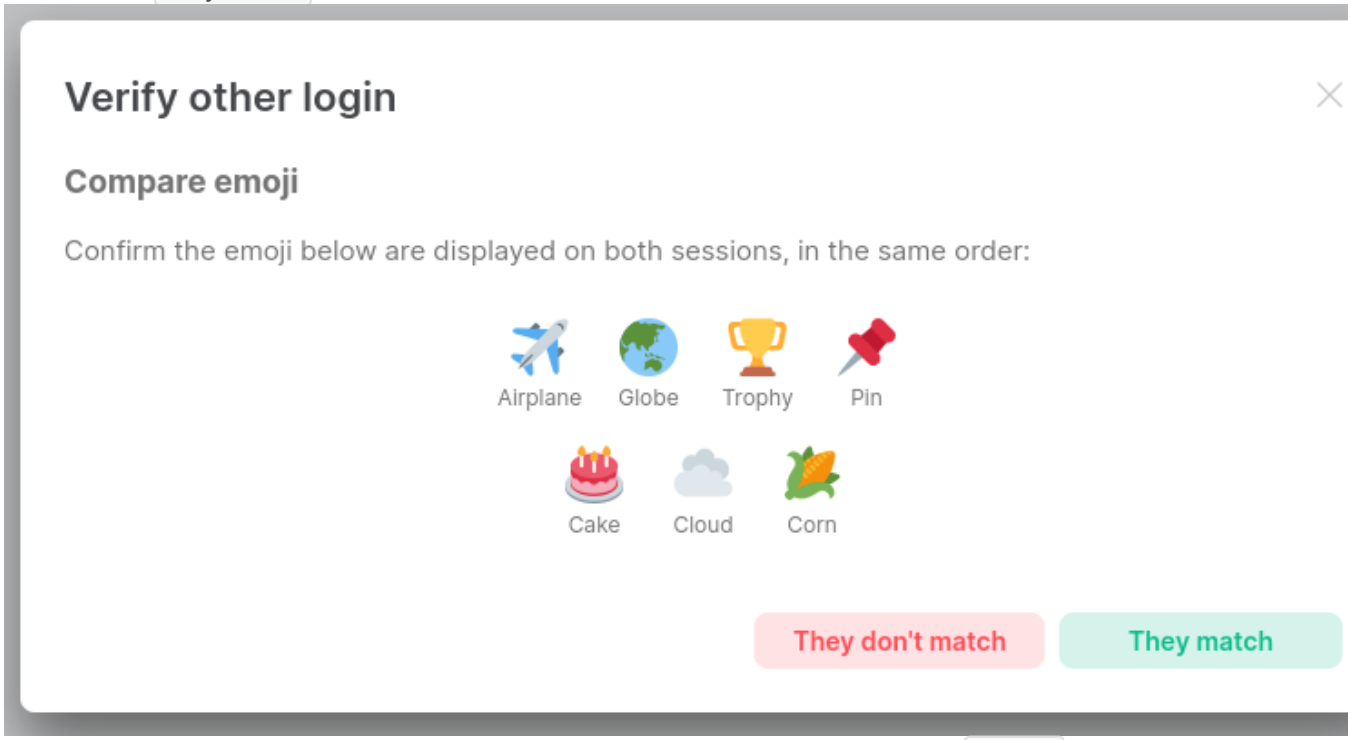
2. On another device/session that is connected to cross signing, click `Accept`



3. Click `Start`



4. Compare the emojis on your new and old sessions. They should be the same emojis and in the same order. Click `They match` on both sessions

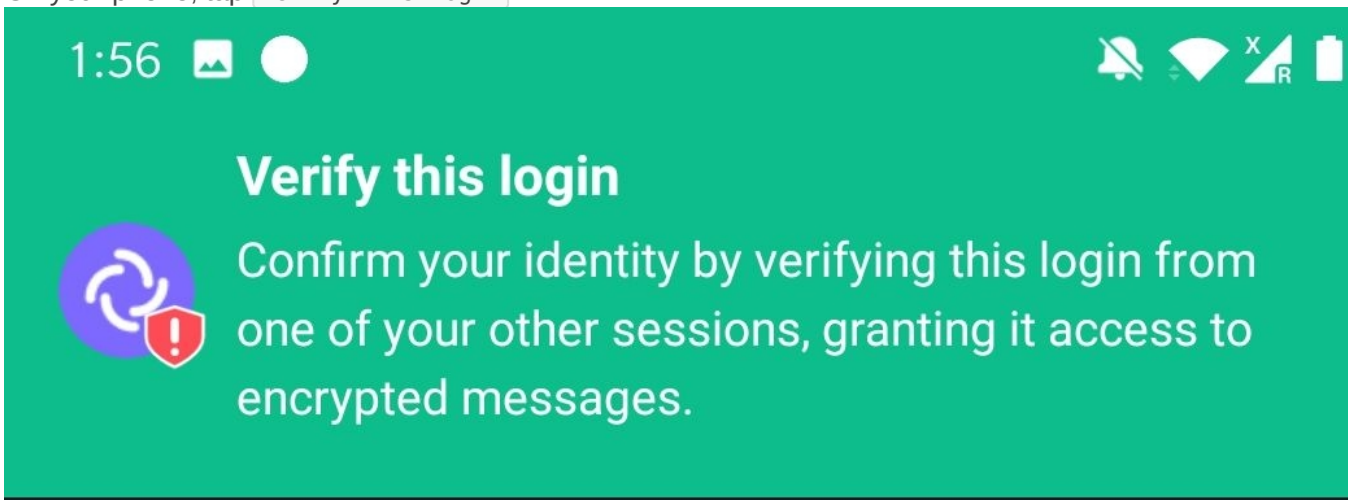


5. If all was successful, you should get this green shield on both sessions. Click `Got it`. Your new device/session is now verified and will download your backed up message encryption keys

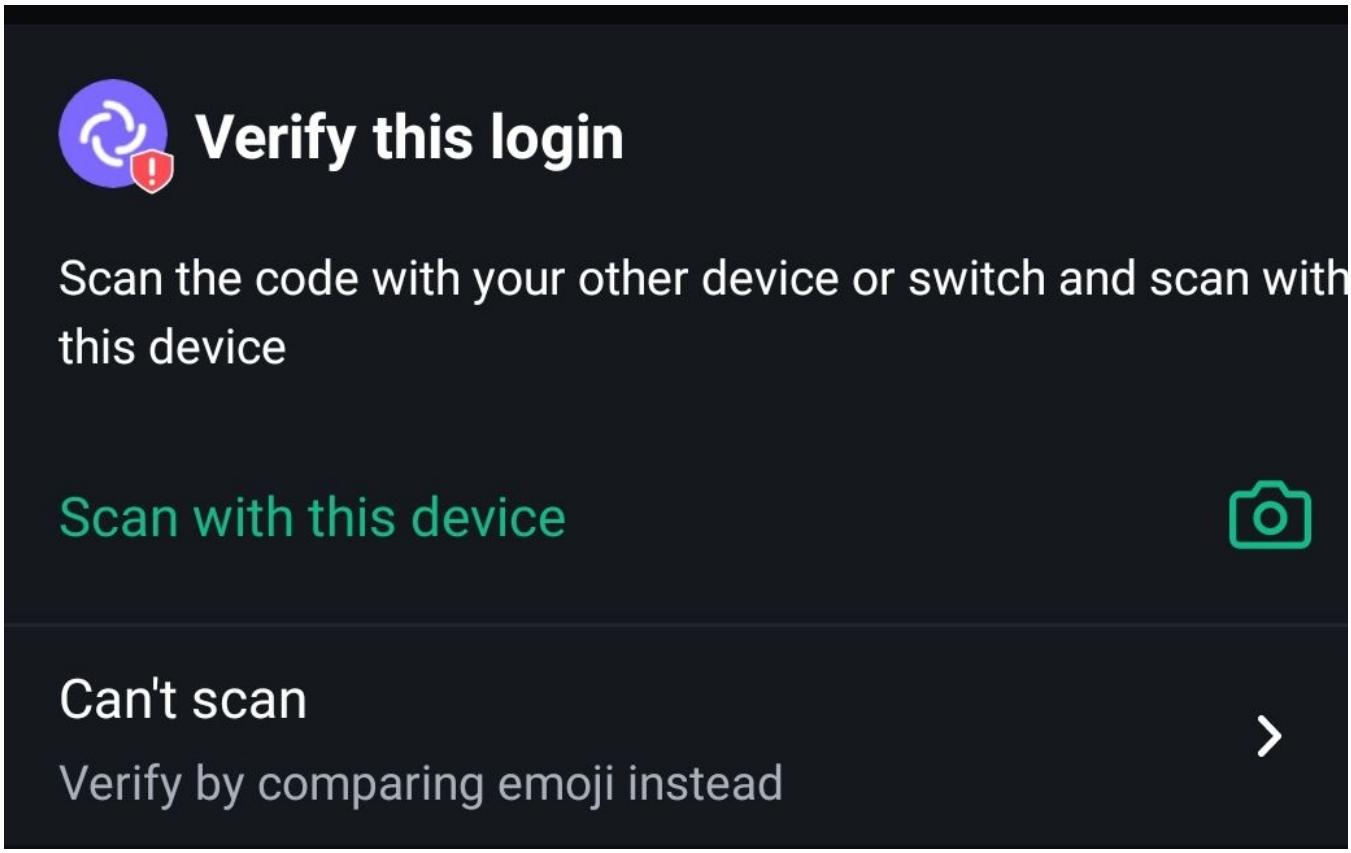
Scan QR code on another login

Login is here demonstrated on Element Android

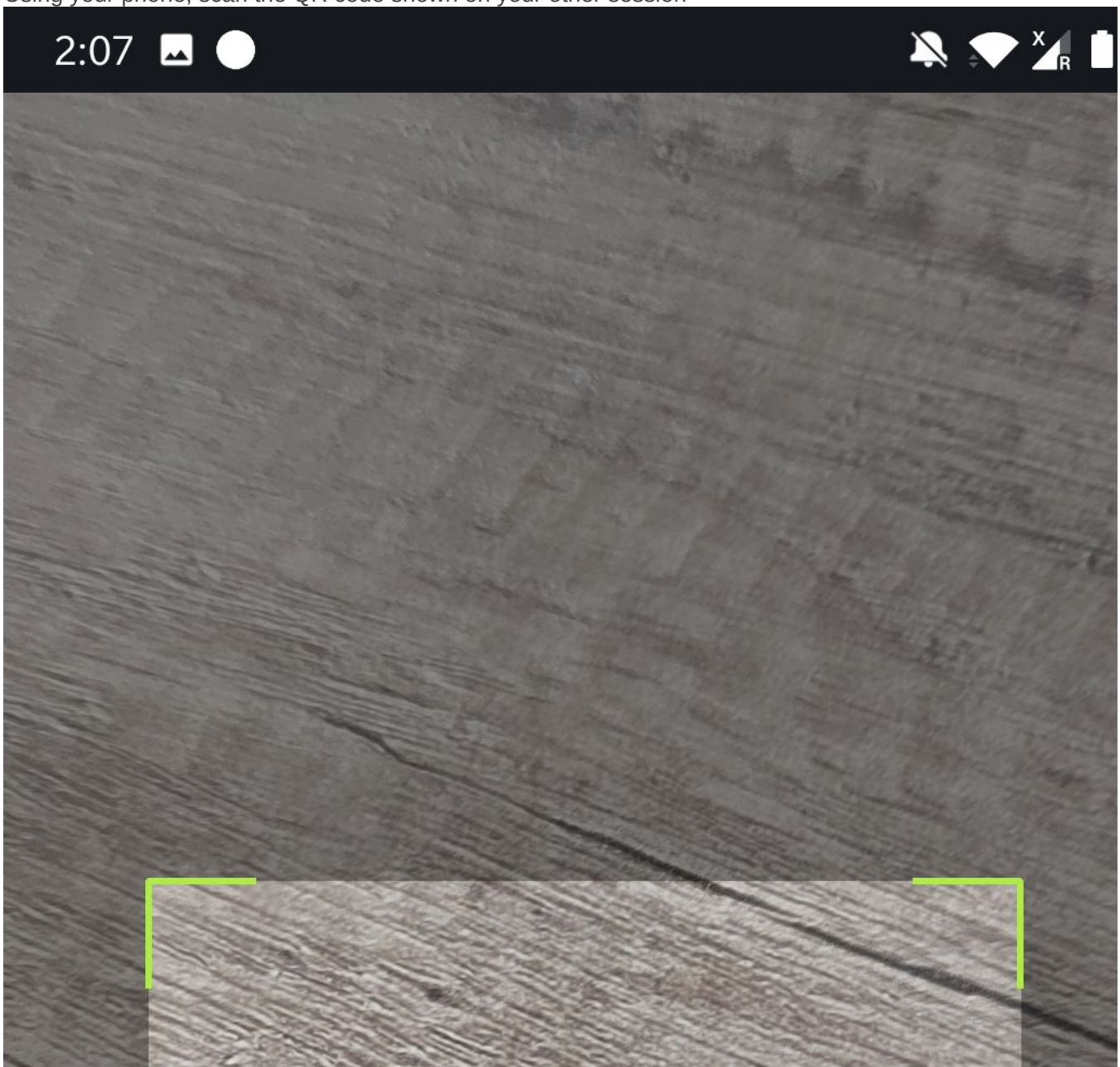
1. On your phone, tap `Verify this login`

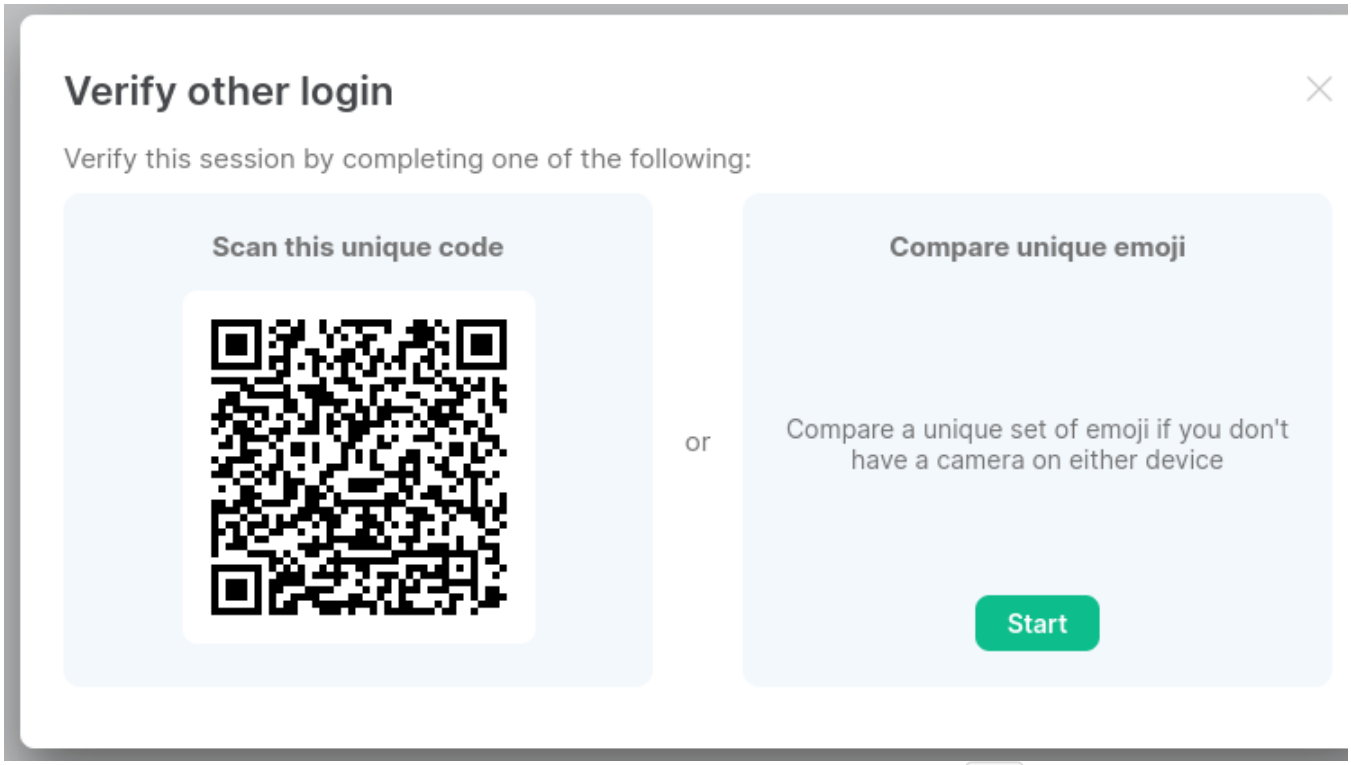


2. Your phone is now waiting for you to accept from another device
3. On another device/session that is connected to cross signing, click `Accept`
4. On your phone, tab `Scan with this device`

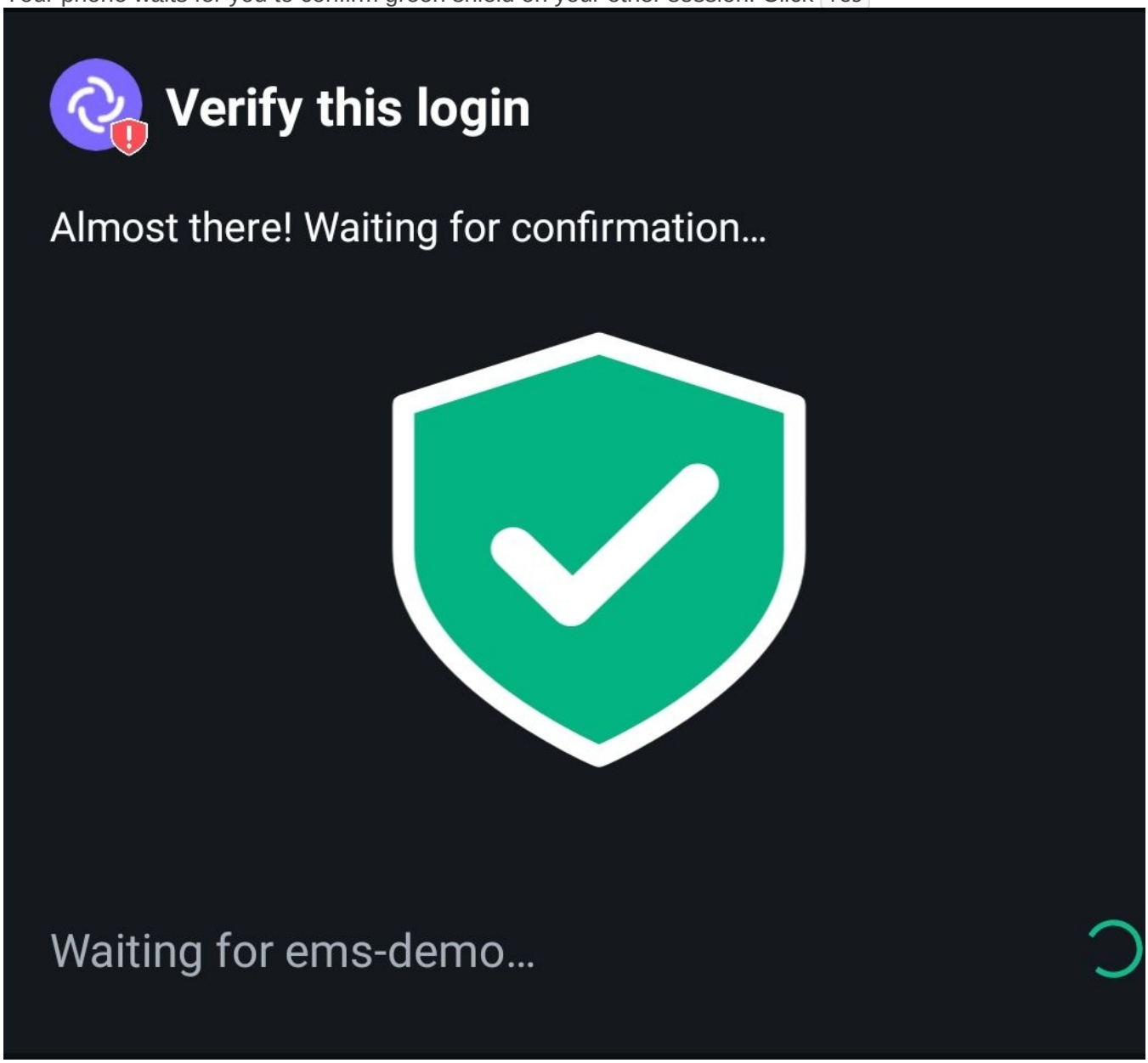


5. Using your phone, scan the QR code shown on your other session





6. Your phone waits for you to confirm green shield on your other session. Click `Yes`



Verify other login

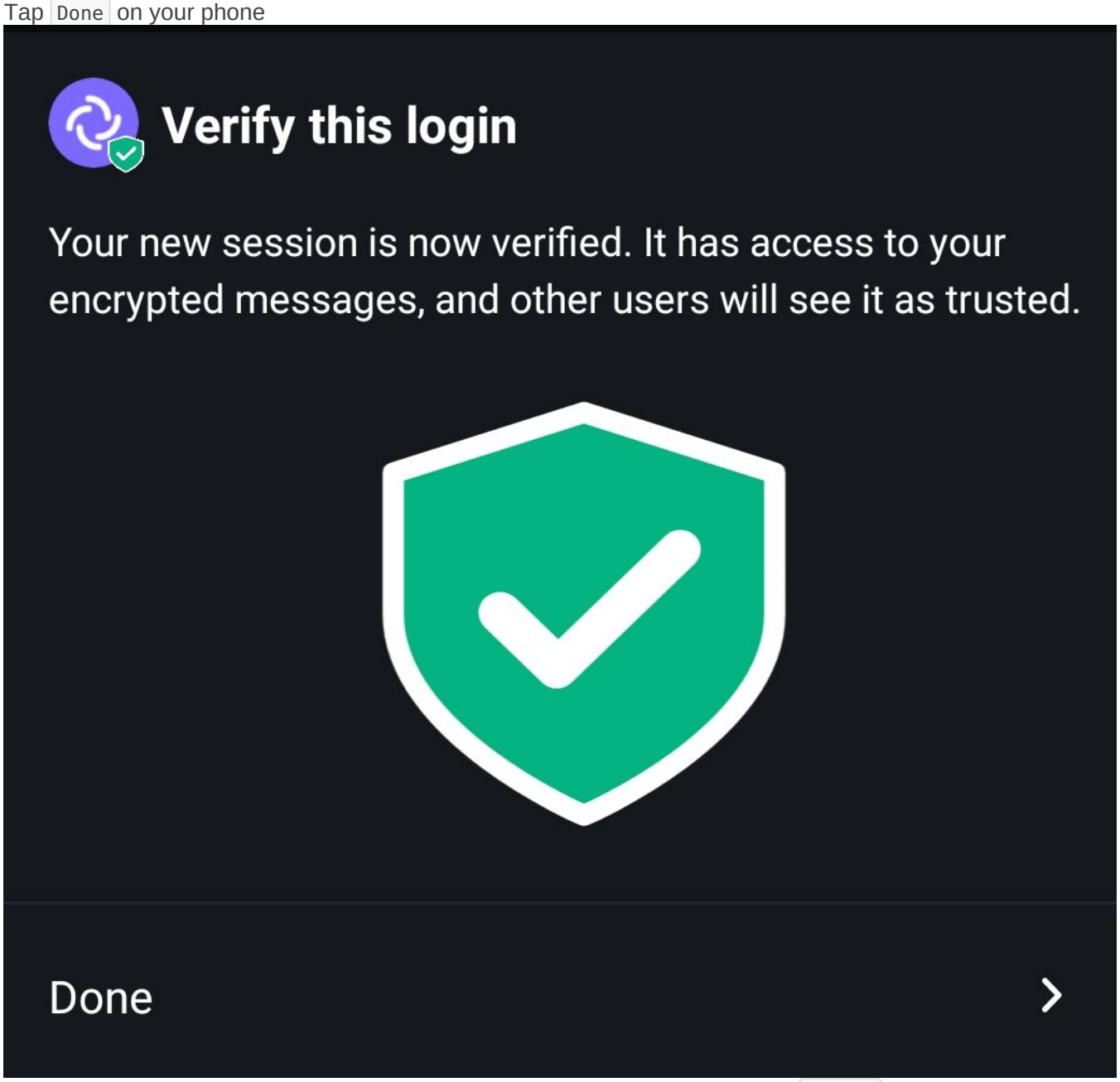
Verify by scanning

Almost there! Is your other session showing the same shield?

No

Yes

7. Tap `Done` on your phone

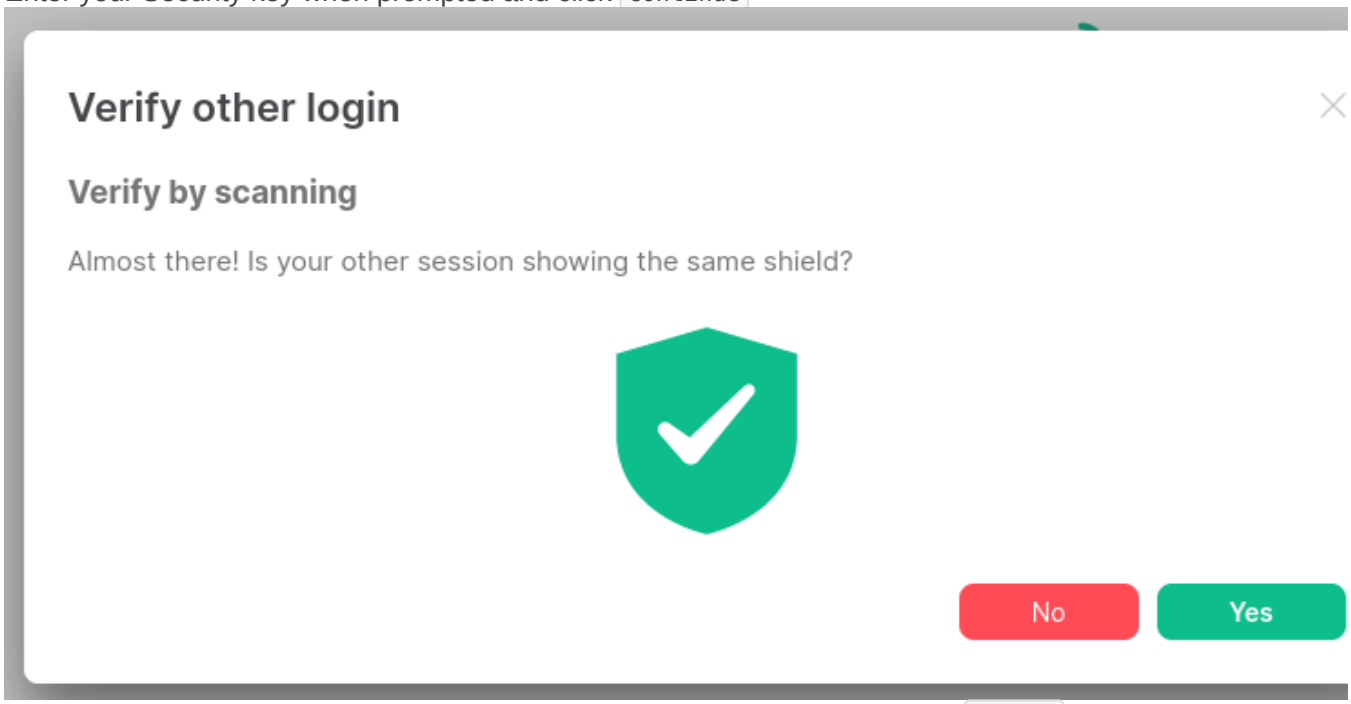


8. If all was successful, you should get this green shield on both sessions. Click `Got it`. Your new device/session is now verified and will download your backed up message encryption keys

Using your Security Key

1. Click `Use Security Key`

2. Enter your Security key when prompted and click `Continue`



3. If all was successful, you should get this green shield on both sessions. Click `Got it`. Your new device/session is now verified and will download your backed up message encryption keys