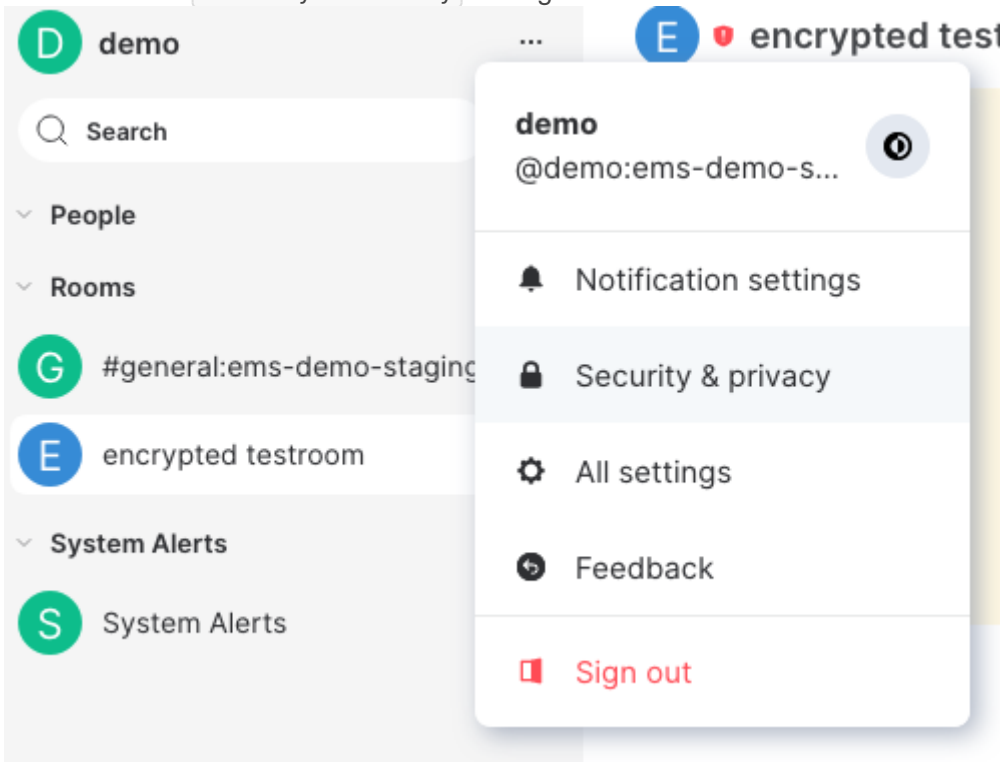


Cross Signing

- [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

Encryption

Key backup

Encrypted messages are secured with end-to-end encryption. Only you and the recipient(s) have the keys to read these messages.

This session is backing up your keys.

▶ Advanced

[Restore from Backup](#)

[Delete Backup](#)

3. Look for **All keys backed up**

Backup version: 8

Algorithm: m.megolm_backup.v1.curve25519-aes-sha2

Backup key stored: in secret storage

All keys backed up

Backup has a **valid** signature from this user

Backup has a signature from **unknown** session with ID LEOTHYQNCM

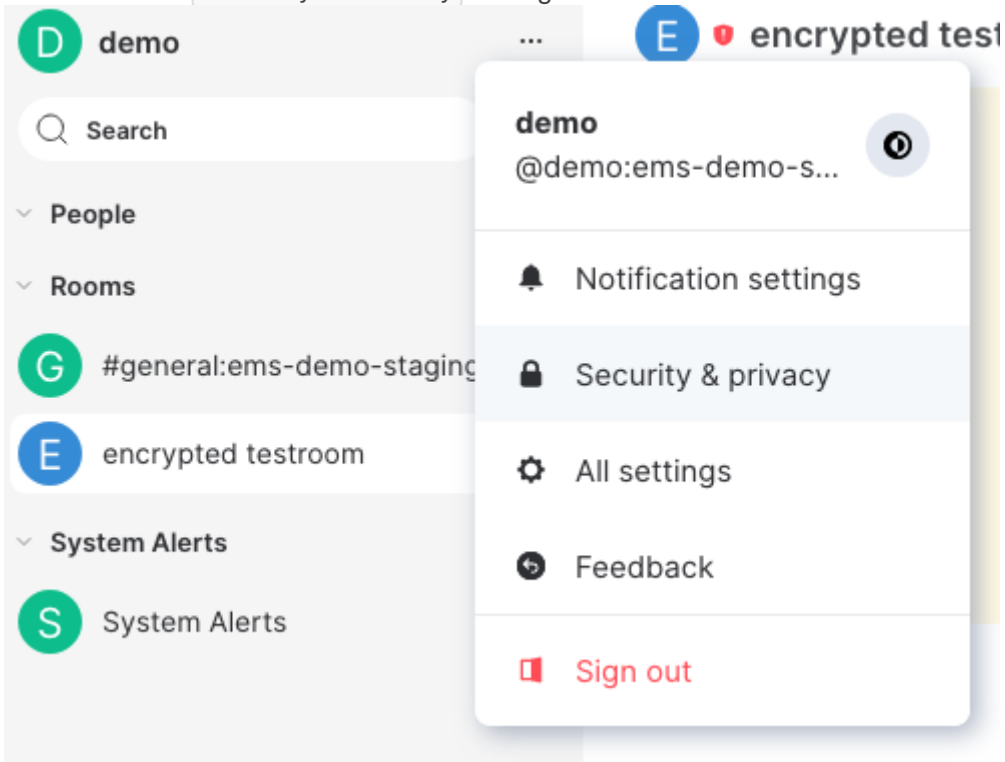
This backup is trusted because it has been restored on this session

Export and Import E2E Room Keys

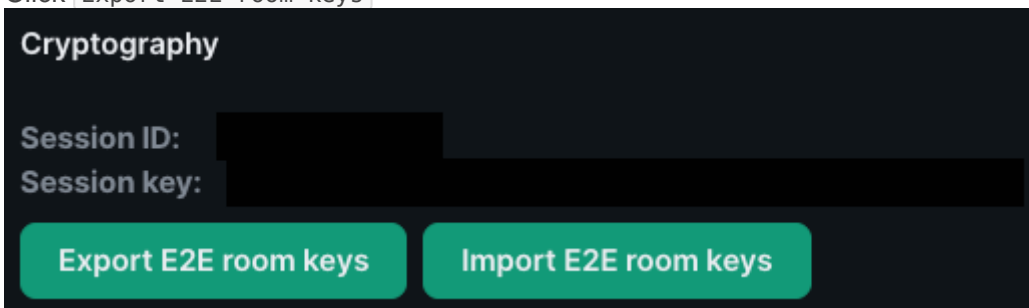
Element Web and Desktop

Export

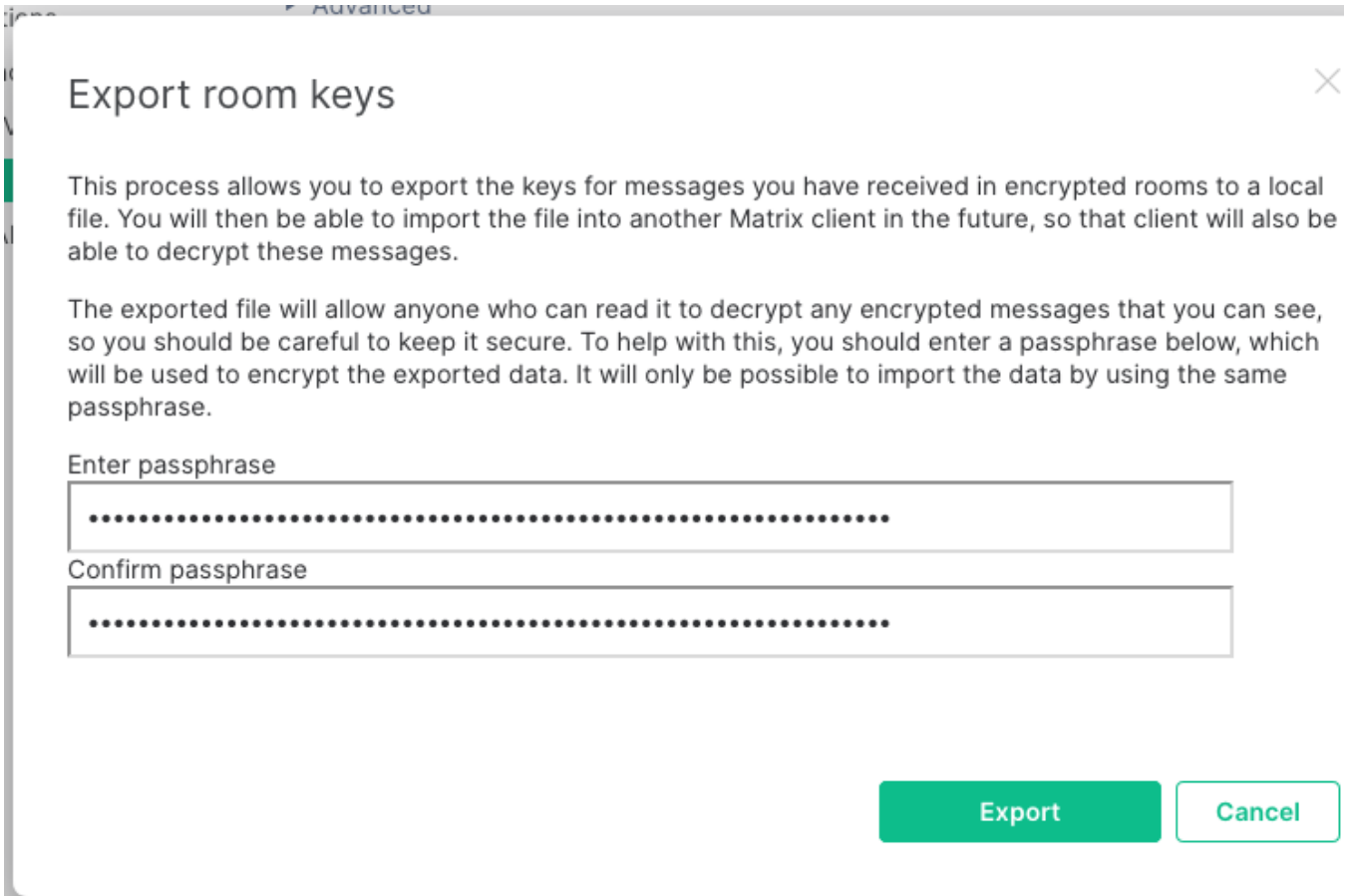
1. Go to Element `Security & Privacy` settings



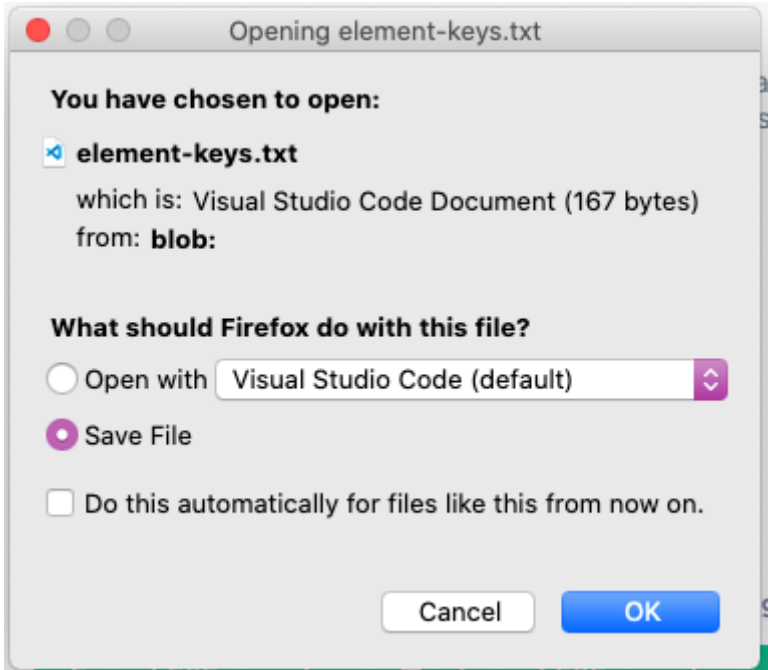
2. Click `Export E2E room keys`



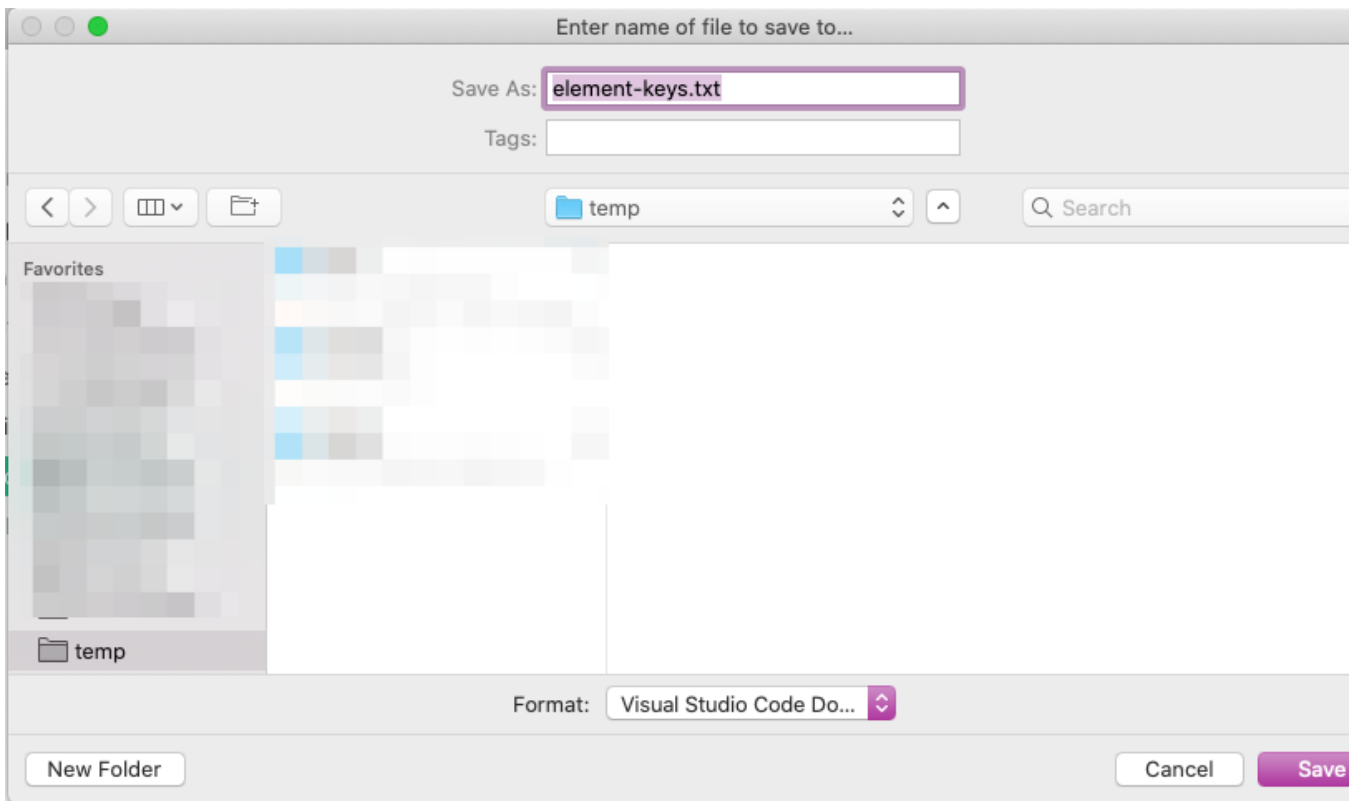
3. Enter a secure passphrase and click `Export`



4. Choose to save the file

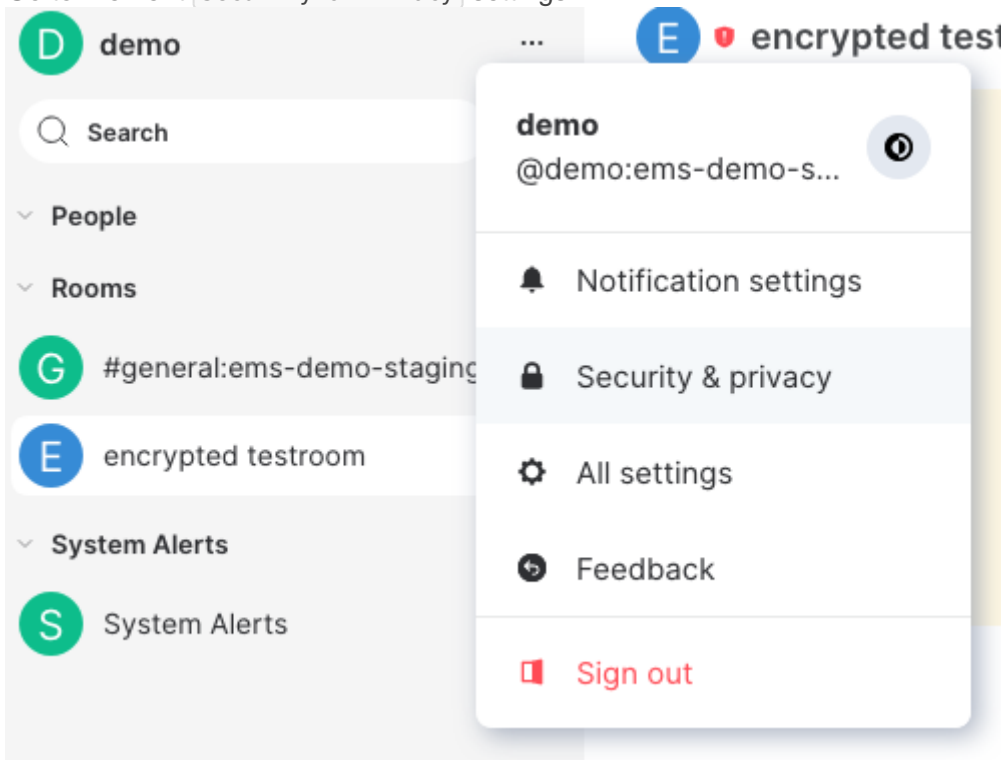


5. Select a directory on your computer

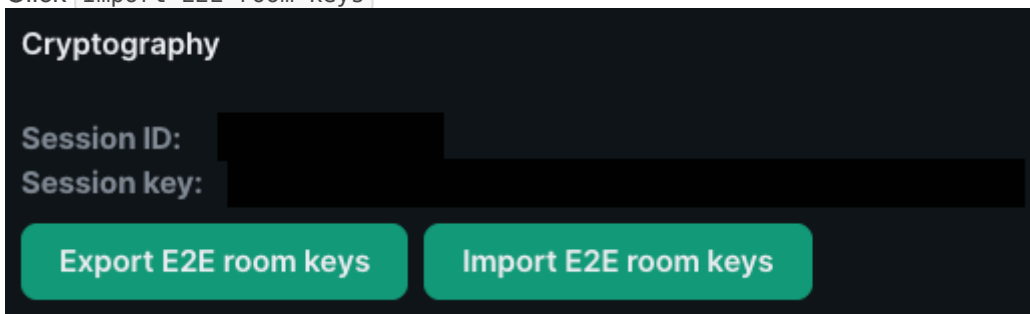


Import

1. Go to Element Security & Privacy settings



2. Click `Import E2E room keys`

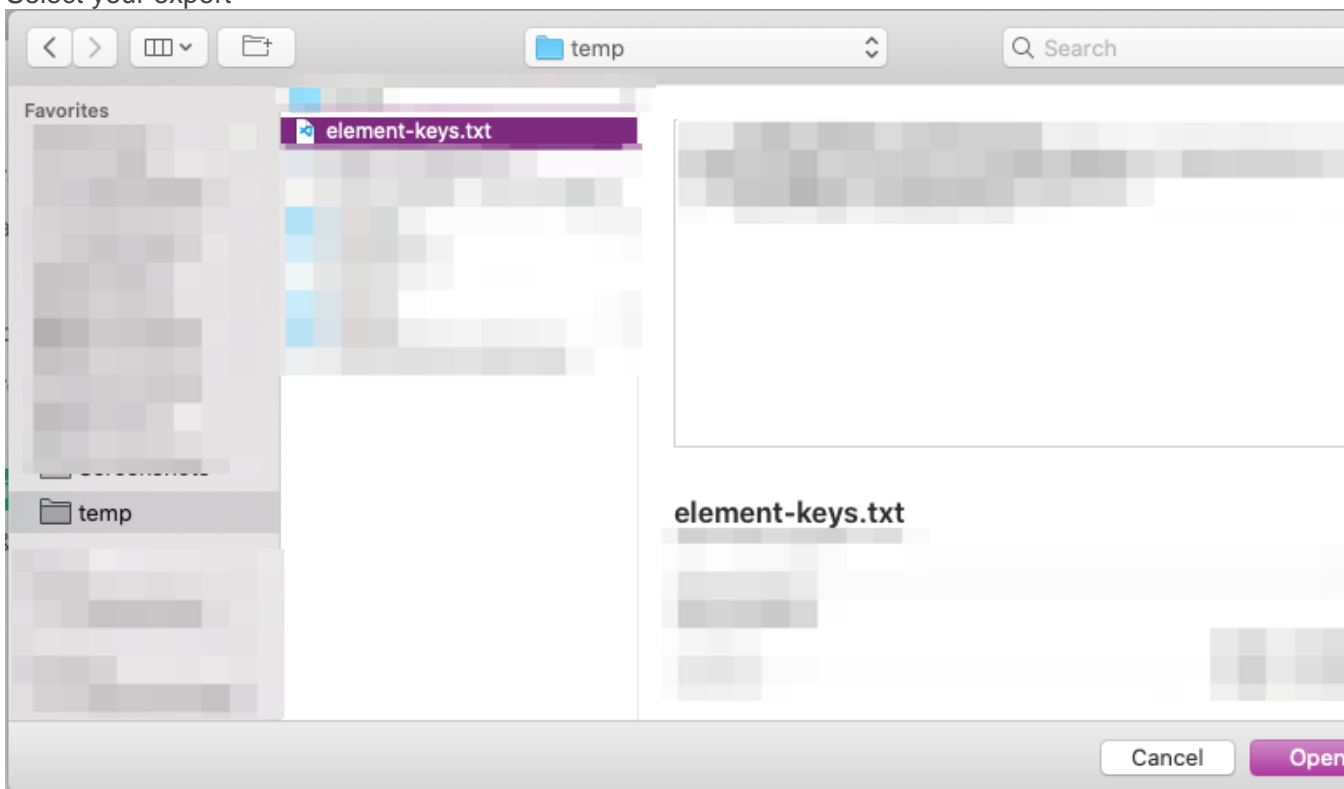


3. Click `Browse`

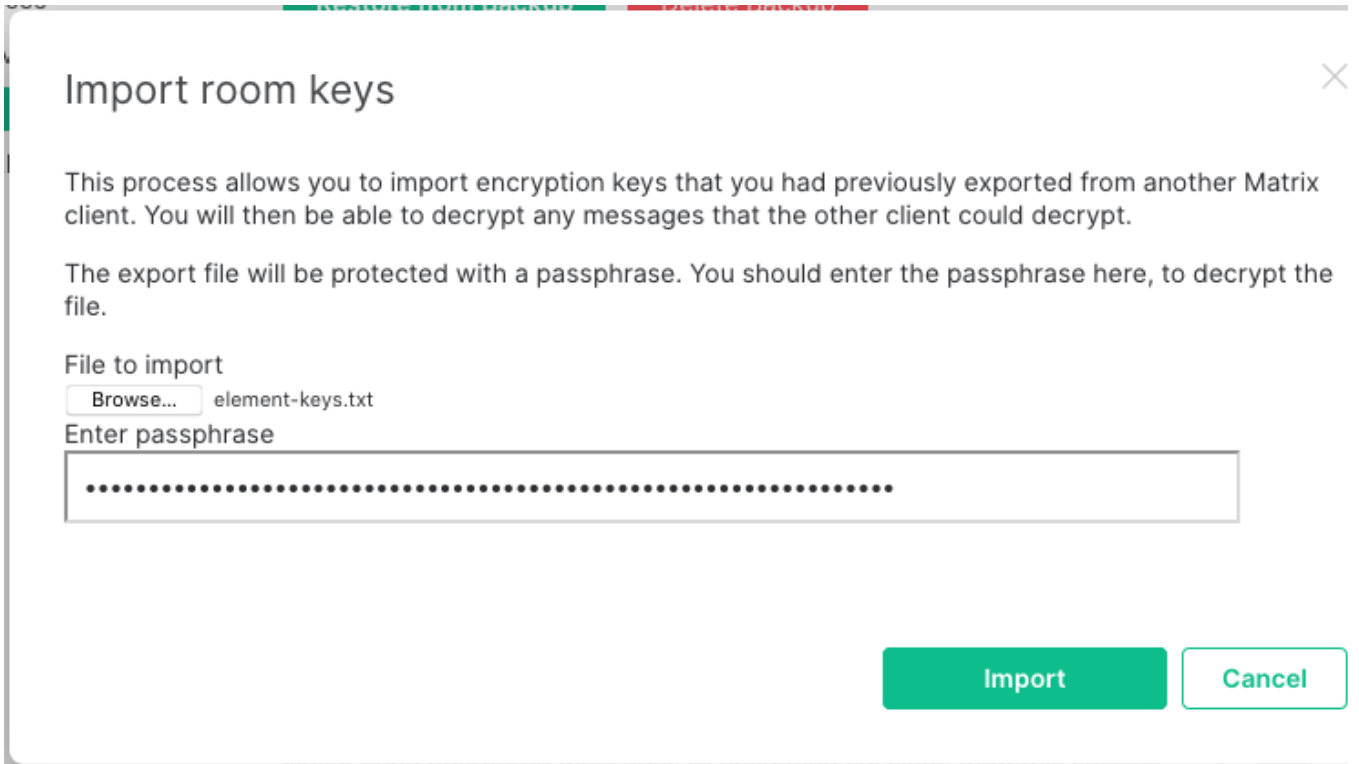
File to import

`Browse...` No file selected.

4. Select your export



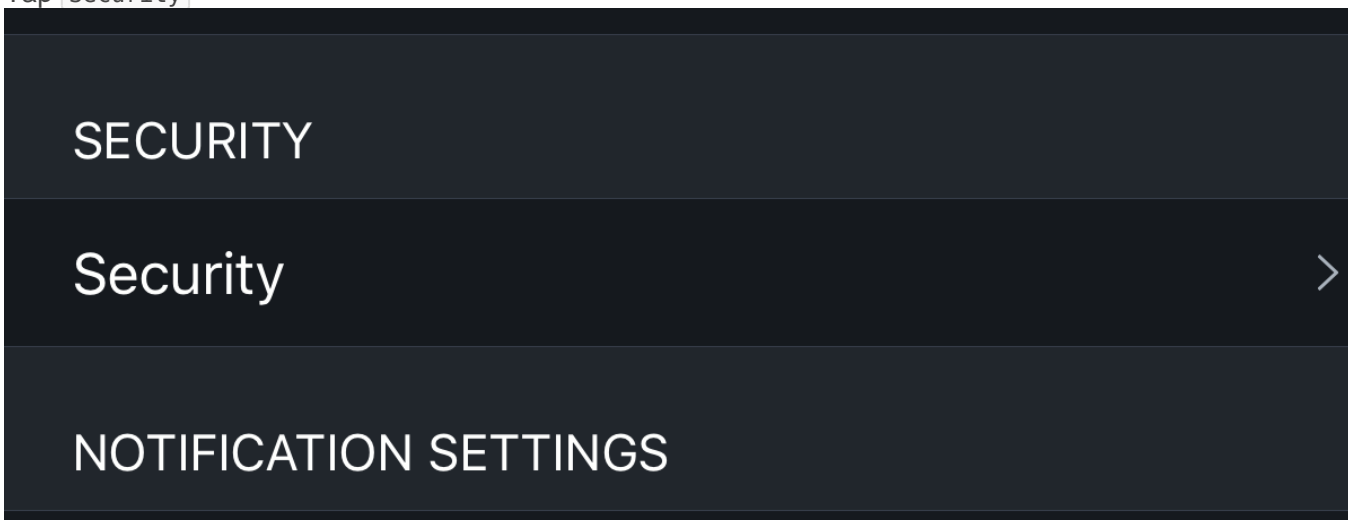
5. Enter your passphrase and click `Import`



Element iOS

Export

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



3. Tap `Export keys manually`

CRYPTOGRAPHY

Session name: Mobile

Session ID: [REDACTED]

Session key:

[REDACTED]

[Export keys manually](#)

4. Enter a secure passphrase and tap

Export room keys

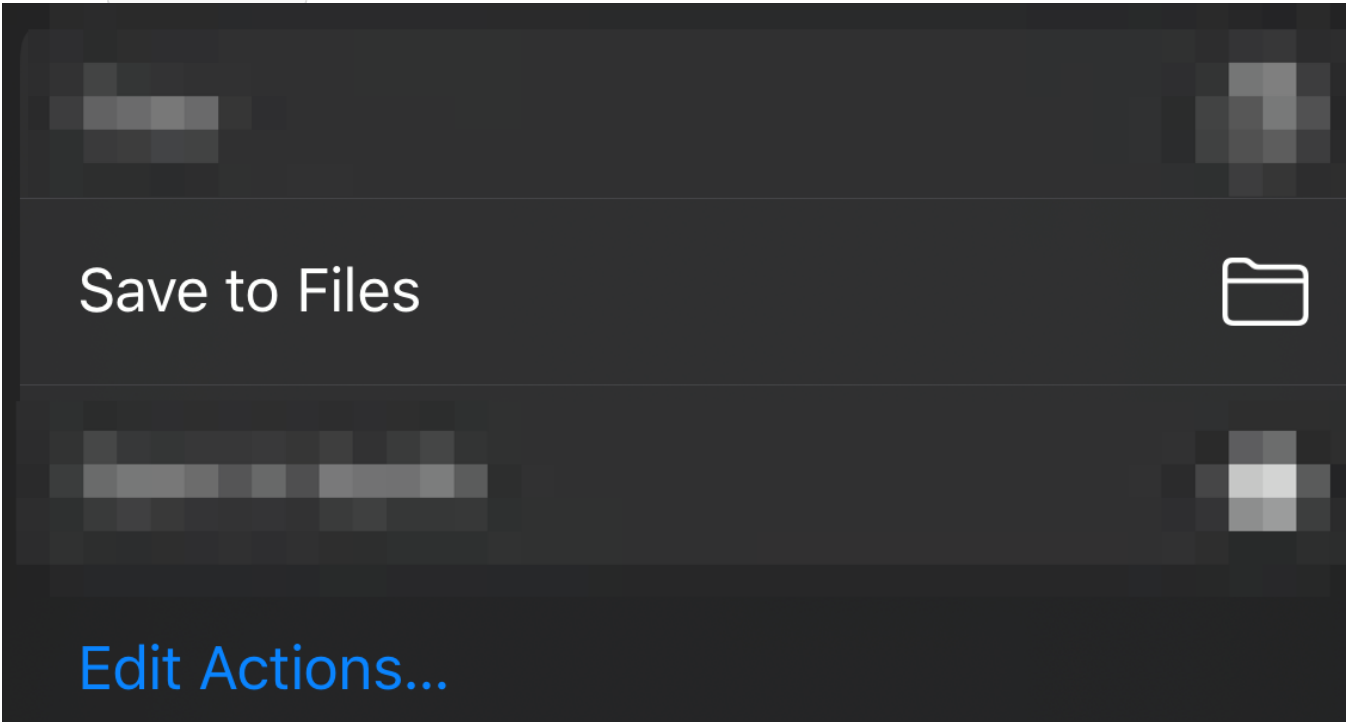
This process allows you to export the keys for messages you have received in encrypted rooms to a local file. You will then be able to import the file into another Matrix client in the future, so that client will also be able to decrypt these messages.

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.

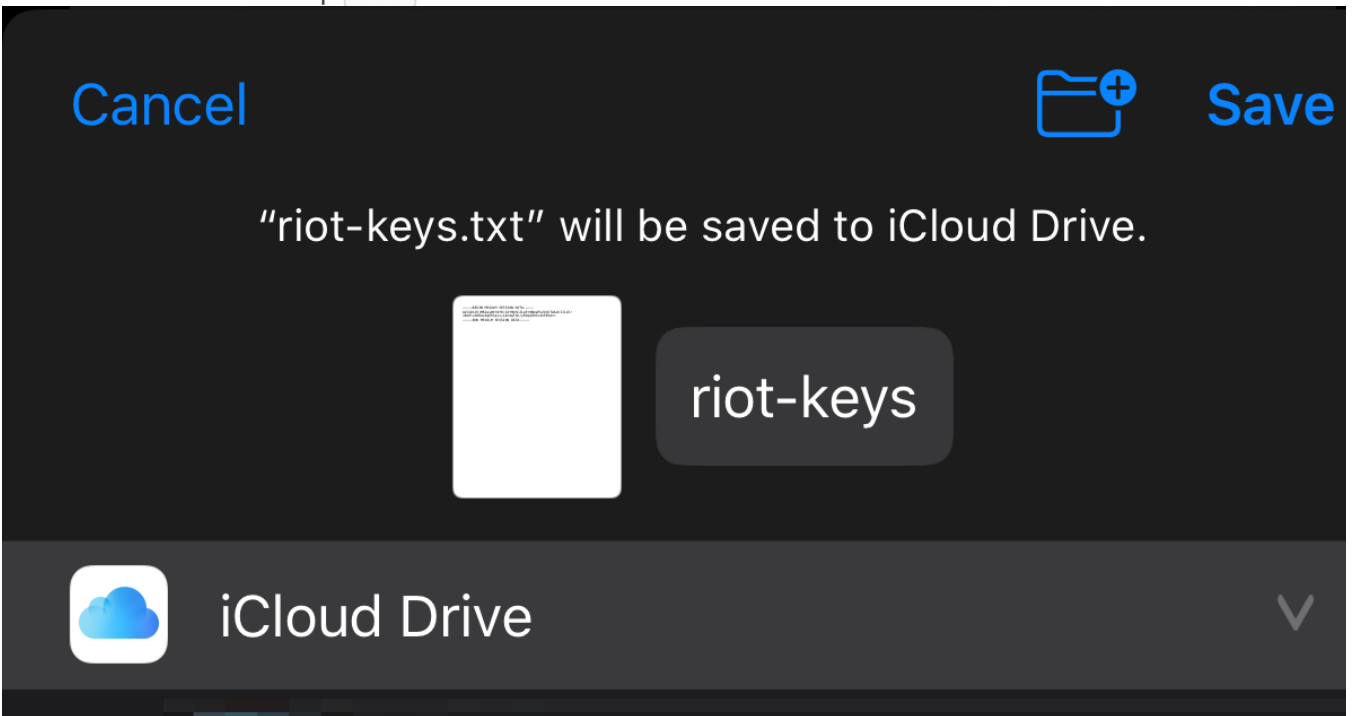
Cancel

Export

5. Choose `Save to Files`




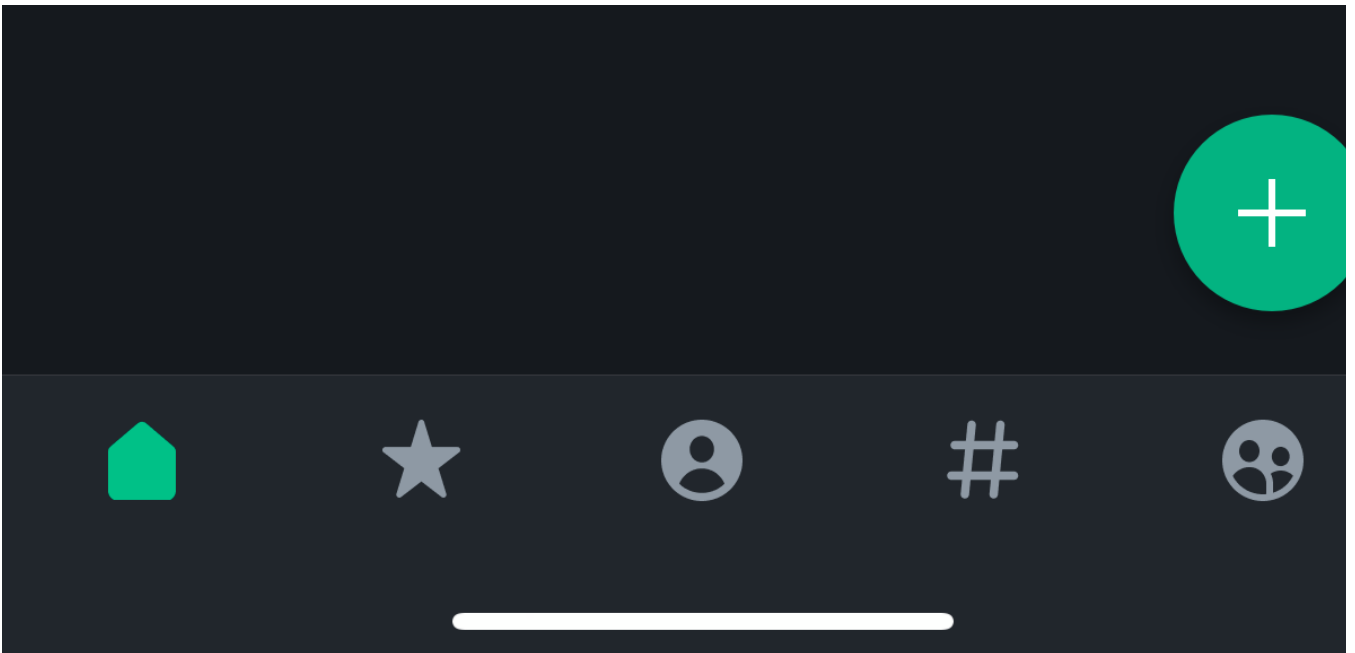
6. Choose a location then tap `Save`



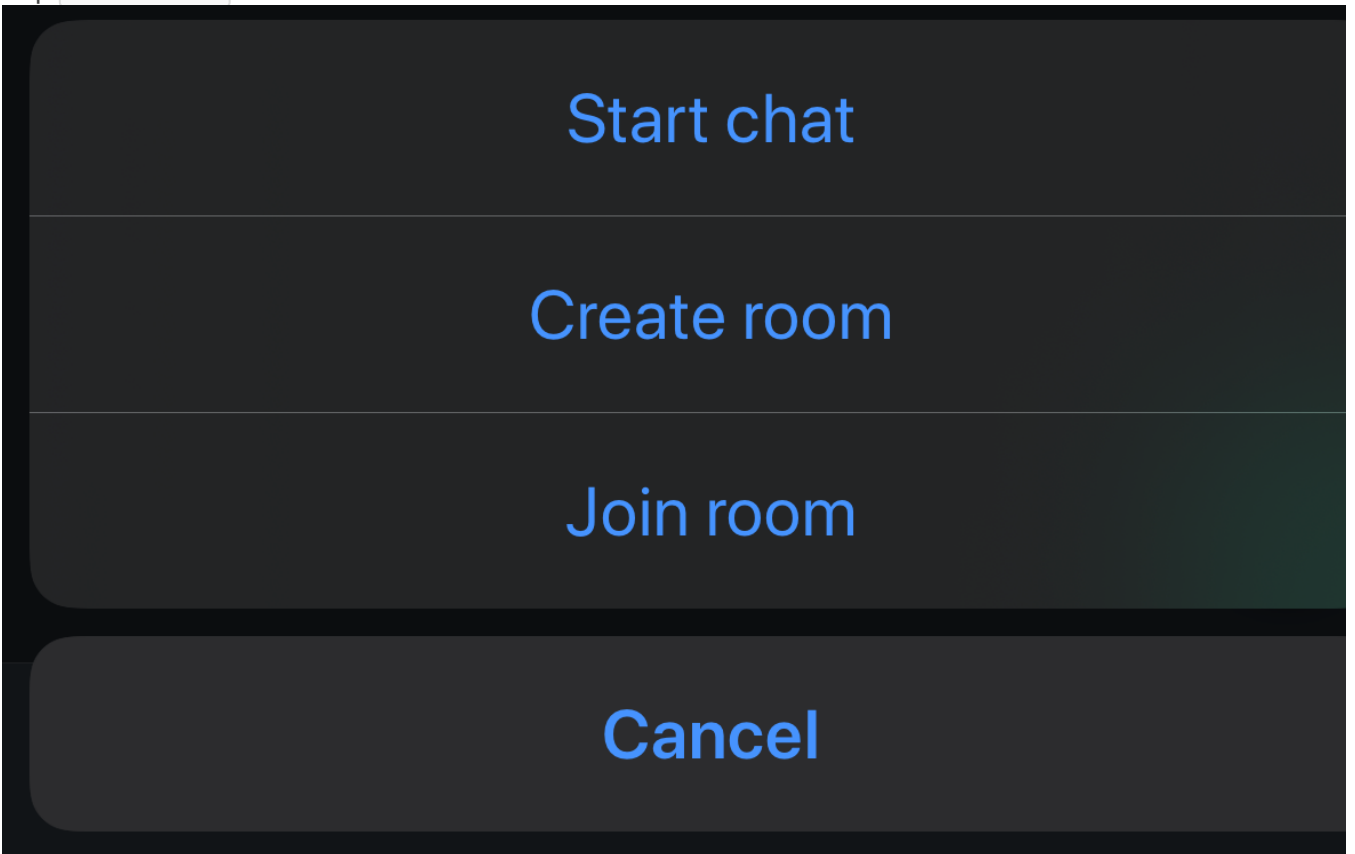
Import

This is a temporary solution until [this issue](#) is resolved

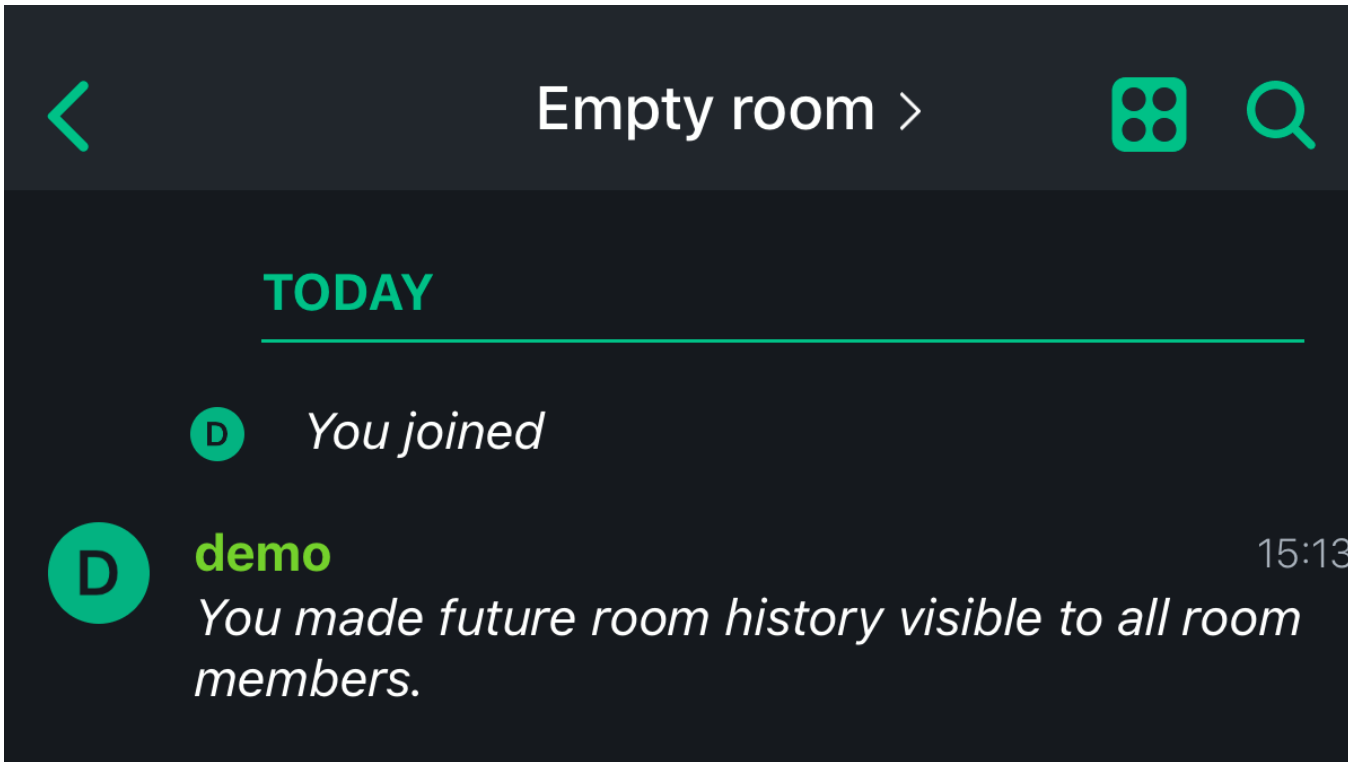
1. Tap the  in the bottom right corner



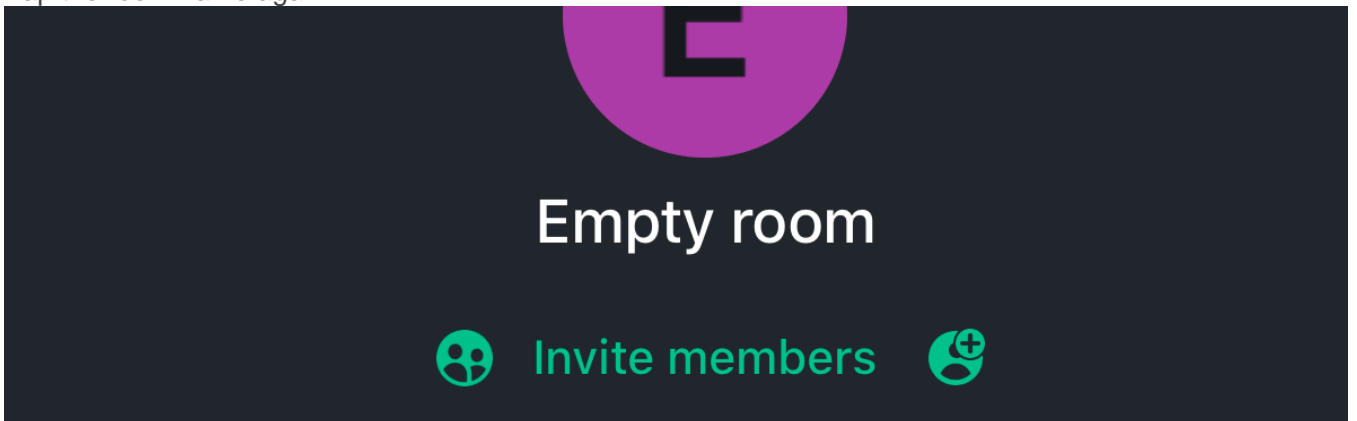
2. Tap `Create room`



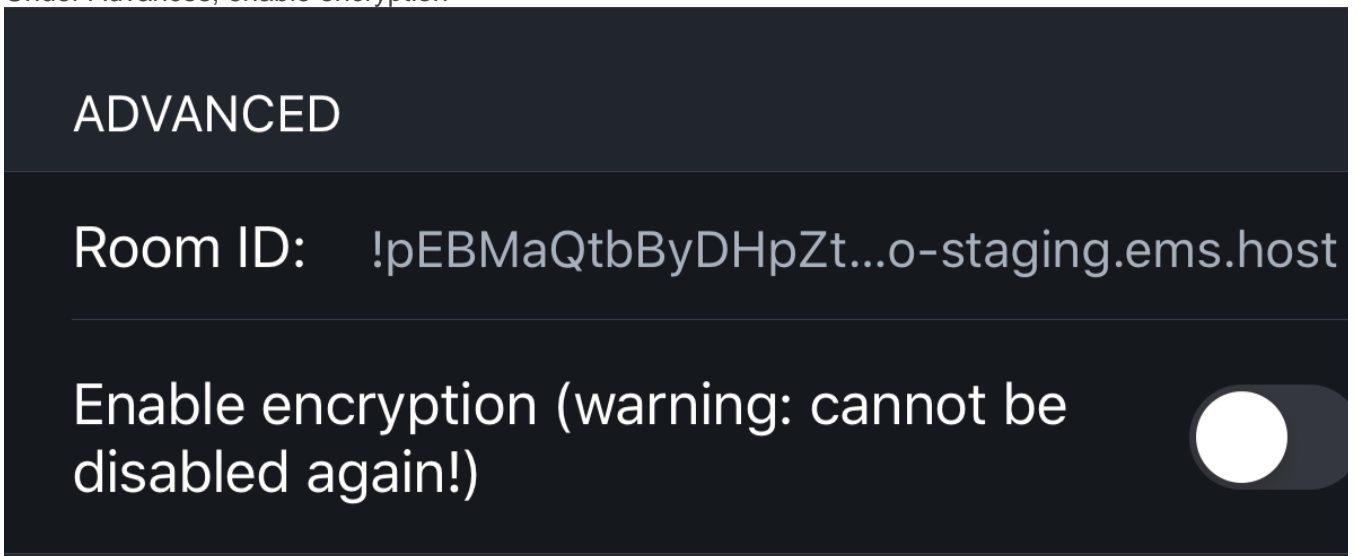
3. Tap the room name (Empty room) at the top



4. Tap the room name again



5. Under Advances, enable encryption



6. Tap `Done` in the top right

Cancel

Room Details

Done

Members

Files

Settings

ADDRESSES

This room has no local addresses

Add new address (e.g. #foo:ems-demo-staging.ems...



SHOW FLAIR FOR COMMUNITIES

Add new community ID (e.g. +foo:ems-demo-stagin...



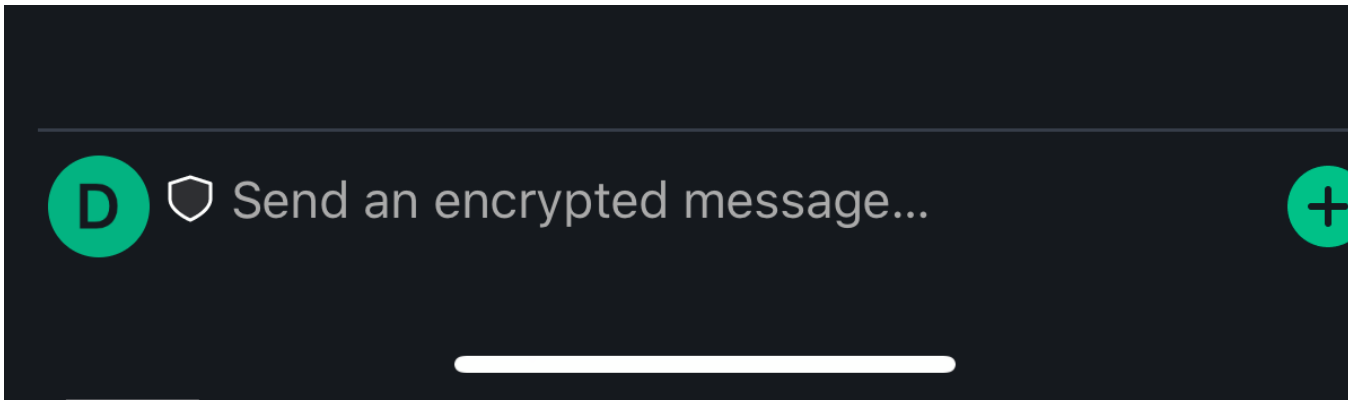
ADVANCED

Room ID: !pEBMaQtBByDHPZt...o-staging.ems.host

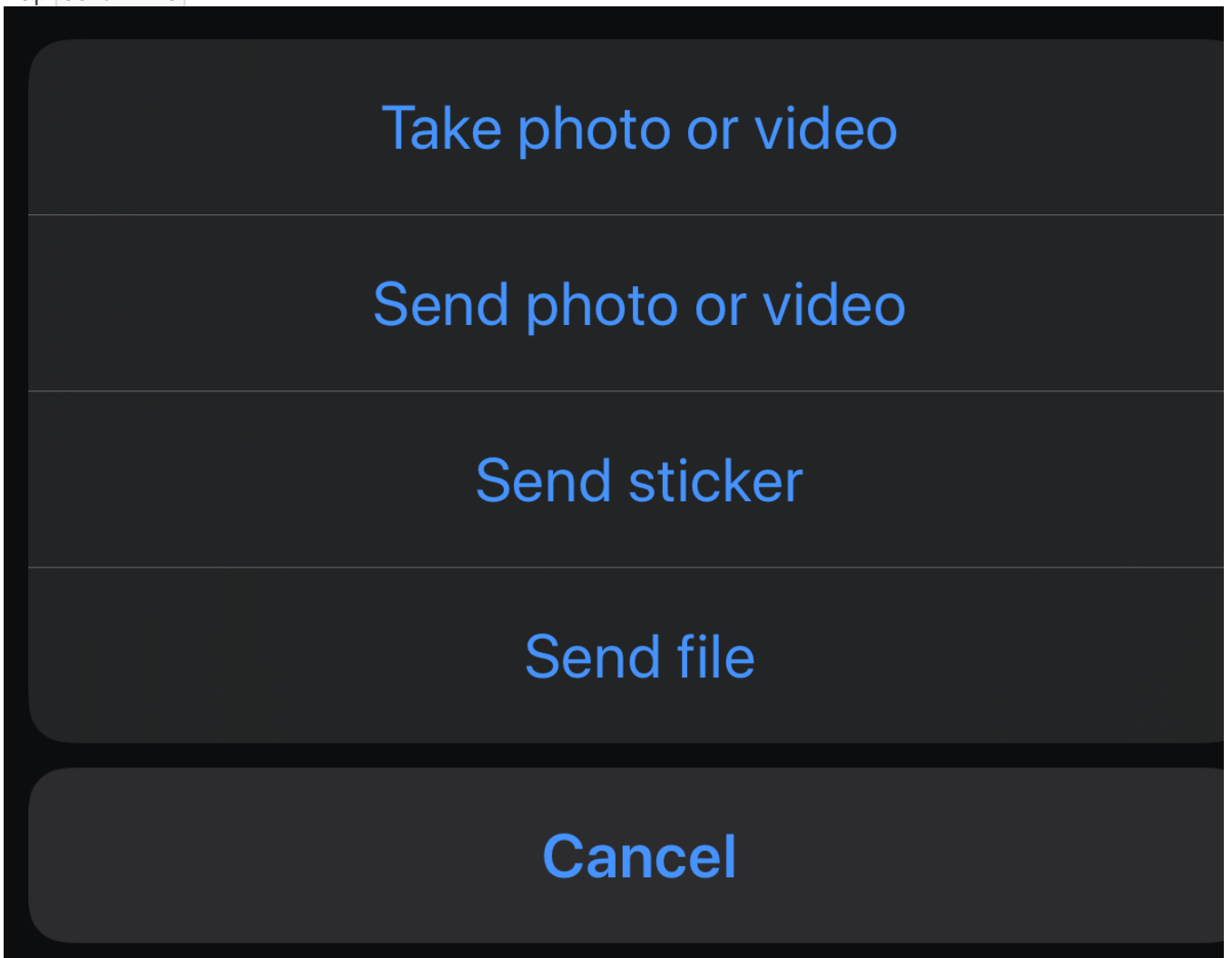
Enable encryption (warning: cannot be disabled again!)



7. Tap the  to send a file



8. Tap `Send file`



9. Browse to and select your export

Recents

Cancel

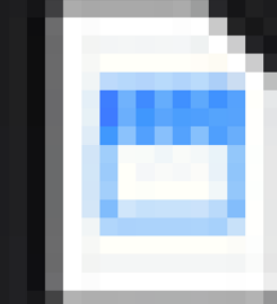
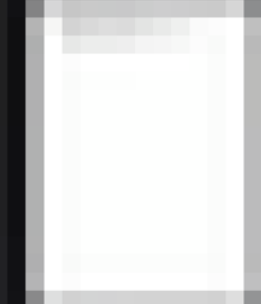
Search

See All



riot-keys

15:16



10. Tap the file you just sent



demo

You made future room history visible to all room members.

You turned on end-to-end encryption.

15:16

riot-keys.txt

11. Tap **Import**

This file contains encryption keys
exported from a Matrix client.
Do you want to view the file content or
import the keys it contains?

View

Import...

12. Enter your passphrase and tap

Import room keys

This process allows you to import encryption keys that you had previously exported from another Matrix client. You will then be able to decrypt any messages that the other client could decrypt.

The export file is protected with a passphrase. You should enter the passphrase here, to decrypt the file.

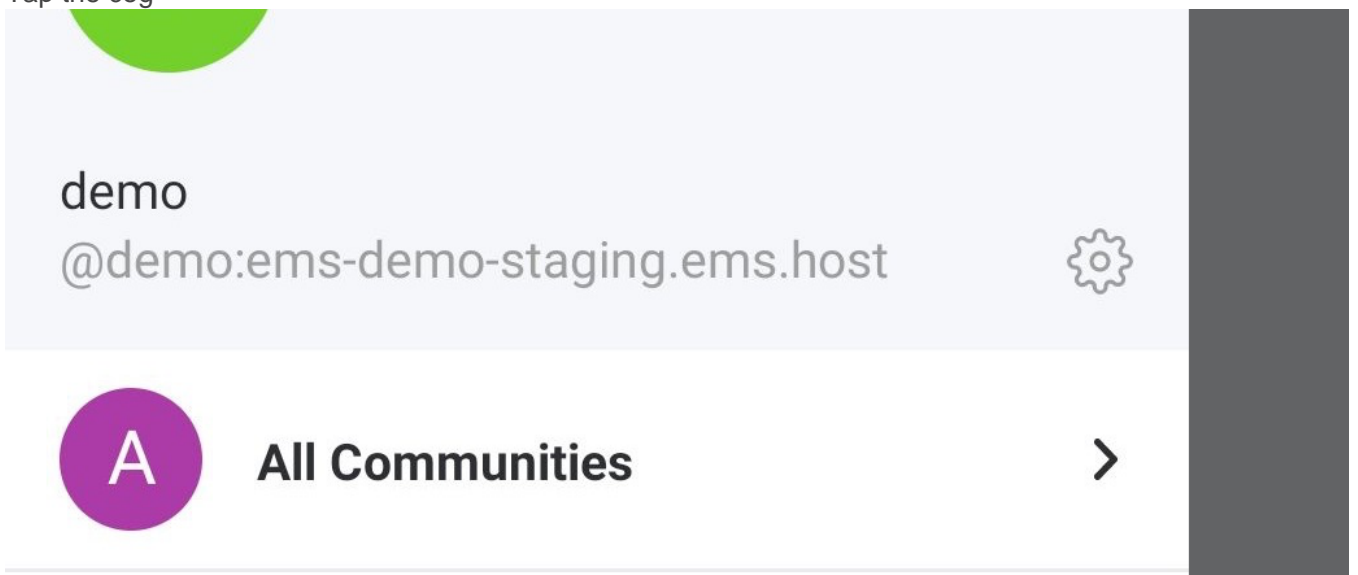
Cancel

Import

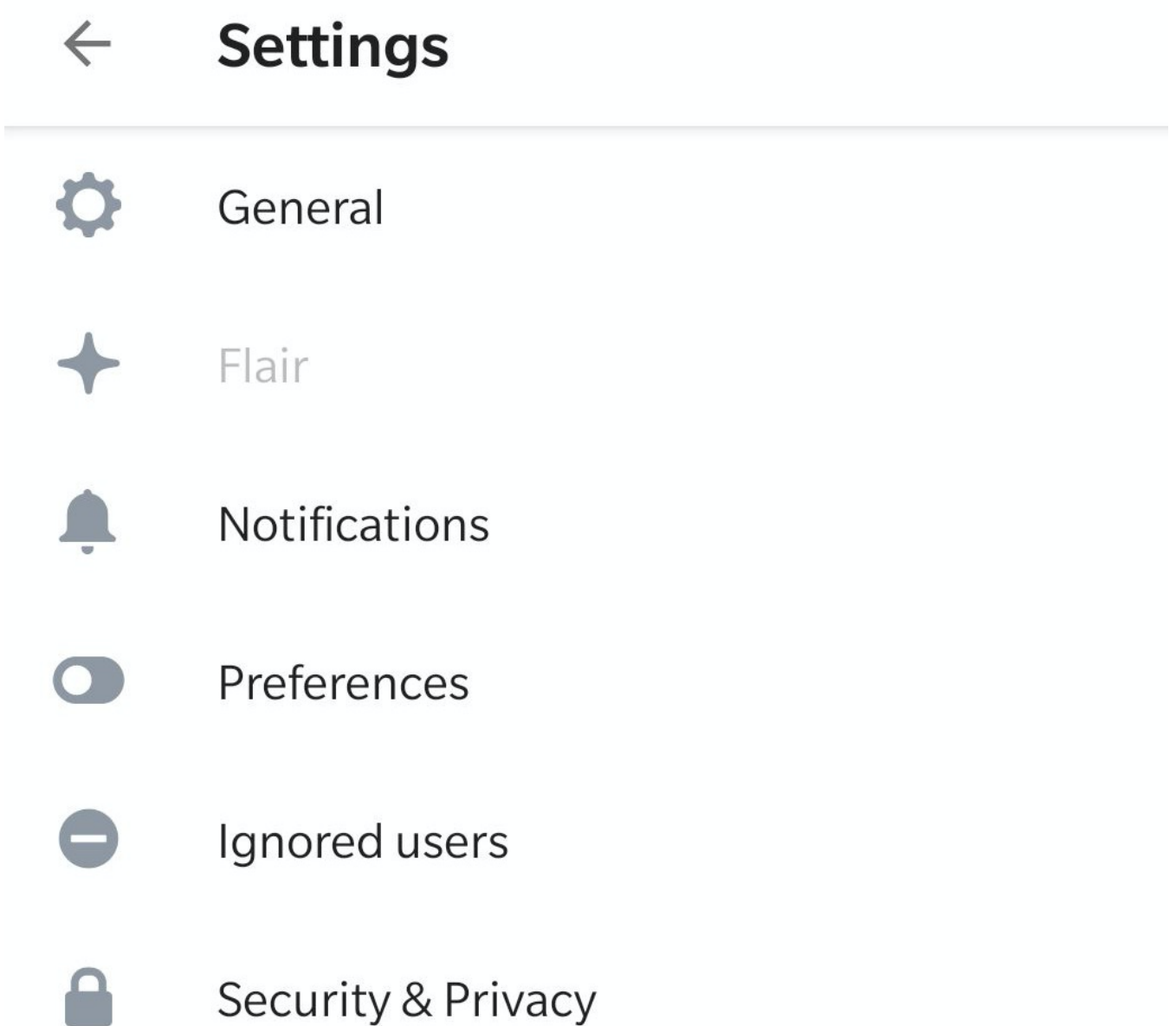
Element Android

Export

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



3. Tap Security & Privacy



4. Tap **Export E2E room keys**

Cryptography Keys Management

Encrypted Messages Recovery

Manage Key Backup

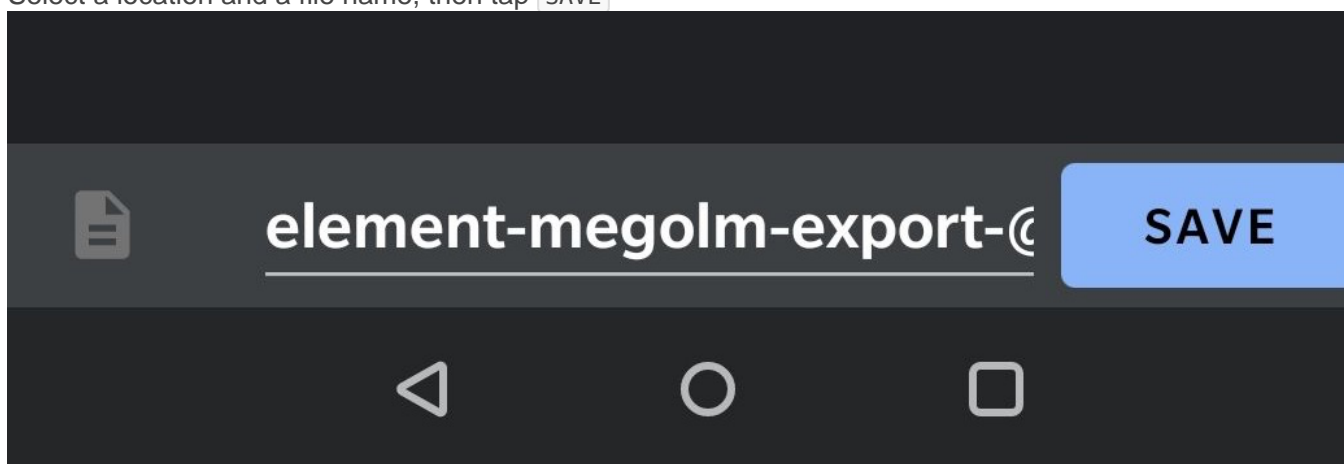
Export E2E room keys

Export the keys to a local file

Import E2E room keys

Import the keys from a local file

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



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

Export room keys

Please create a passphrase to encrypt the exported keys. You will need to enter the same passphrase to be able to import the keys.

Create passphrase



Confirm passphrase

EXPORT

Manage Key Backup

Import

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

demo

@demo:ems-demo-staging.ems.host



All Communities



3. Tap `Security & Privacy`



Settings



General



Flair



Notifications



Preferences



Ignored users



Security & Privacy

4. Tap `Import E2E room keys`

Cryptography Keys Management

Encrypted Messages Recovery

Manage Key Backup

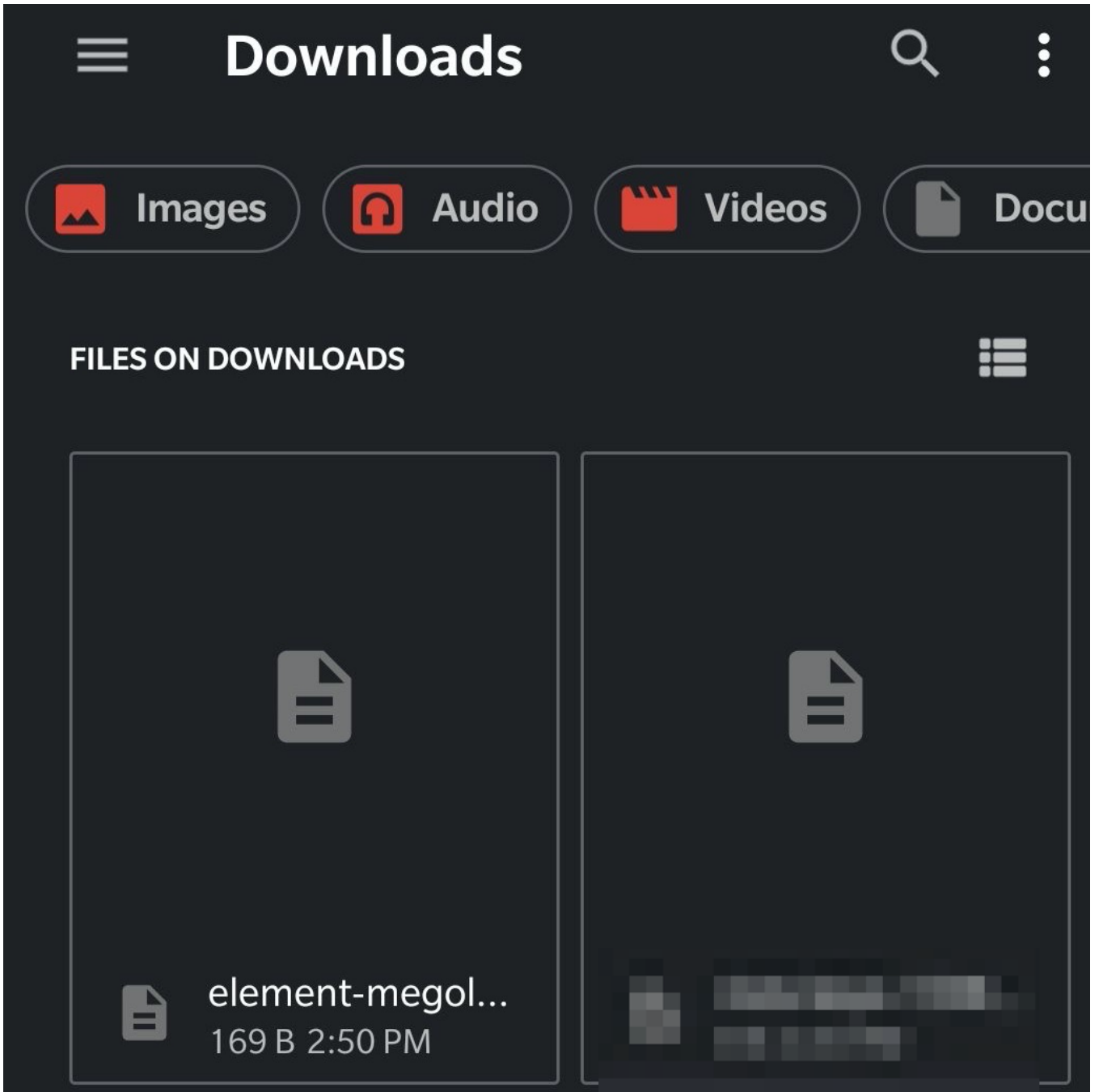
Export E2E room keys

Export the keys to a local file

Import E2E room keys

Import the keys from a local file

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

Cross-signing

✔ Cross-signing is ready for use.

▶ Advanced

Reset

3. Click `Clear cross-signing keys`

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

Set up Secure backup

Safeguard against losing access to encrypted messages & data by backing up encryption keys on your server.

Generate a Security Key
We'll generate a Security Key for you to store somewhere safe, like a password manager or a safe.

Enter a Security Phrase
Use a secret phrase only you know, and optionally save a Security Key to use for backup.

`Cancel` `Continue`

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

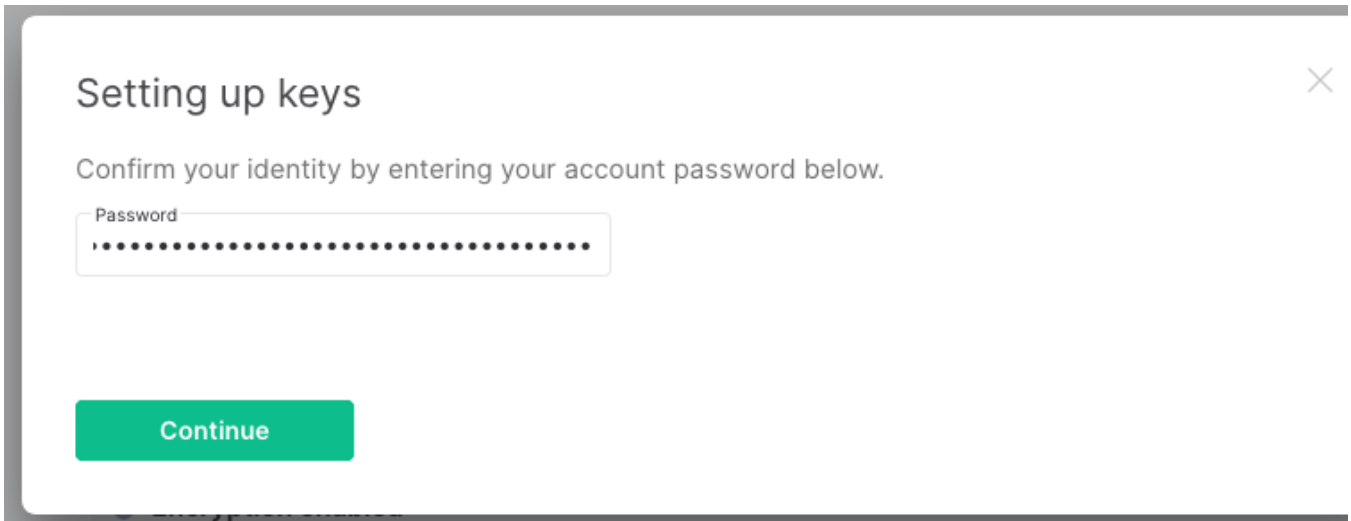
Save your Security Key

Store your Security Key somewhere safe, like a password manager or a safe, as it's used to safeguard your encrypted data.

`Download` or `Copy`

`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](#)

Security & Privacy

Where you're logged in

Manage the names of and sign out of your sessions below or [verify them in your User Profile](#).

A session's public name is visible to people you communicate with


ID	Public Name	Last seen	
[blurred]	ems-demo-staging.element.io (Firefox, macOS)	[blurred] @ 15:12	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

[Create account](#)


English (US) 

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

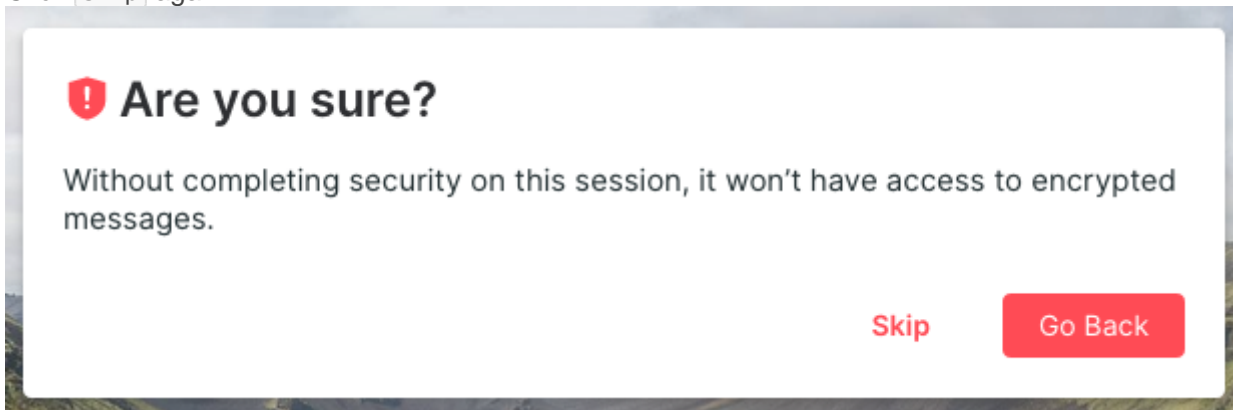


Element iOS
Element X for Android

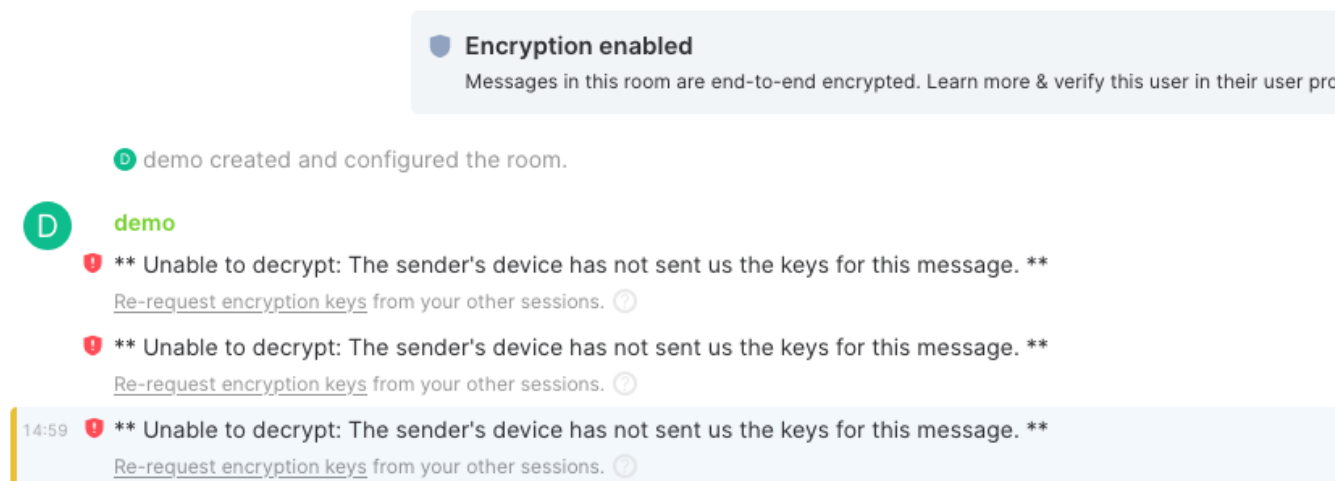
or another cross-signing capable Matrix client

[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

Where you're signed in

Manage your signed-in devices below. A device's name is visible to people you communicate with.

This device

app.element.io (Firefox, macOS)
Last seen 10:27 at [REDACTED]

Sign Out

Rename

Verified devices [Deselect all](#)

app.element.io (Firefox, macOS)
Last seen 10:28 at [REDACTED]

Rename

app.element.io (Firefox, macOS)
Last seen 10:27 at [REDACTED]

Rename

app.element.io (Firefox, macOS)
Last seen 10:26 at [REDACTED]

Rename

Sign out 2 selected devices

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

Authentication

Confirm your identity by entering your account password below.

Password

.....

Continue

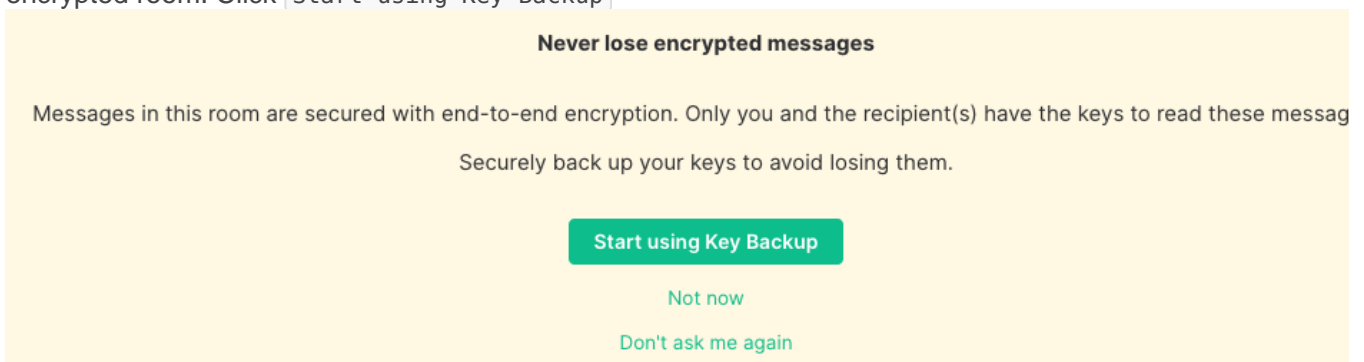
Set up Cross Signing

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`

Encryption

Key backup

Your keys are **not being backed up from this session.**

Encrypted messages are secured with end-to-end encryption. Only you and the recipient(s) have the keys to read these messages.

Back up your keys before signing out to avoid losing them.

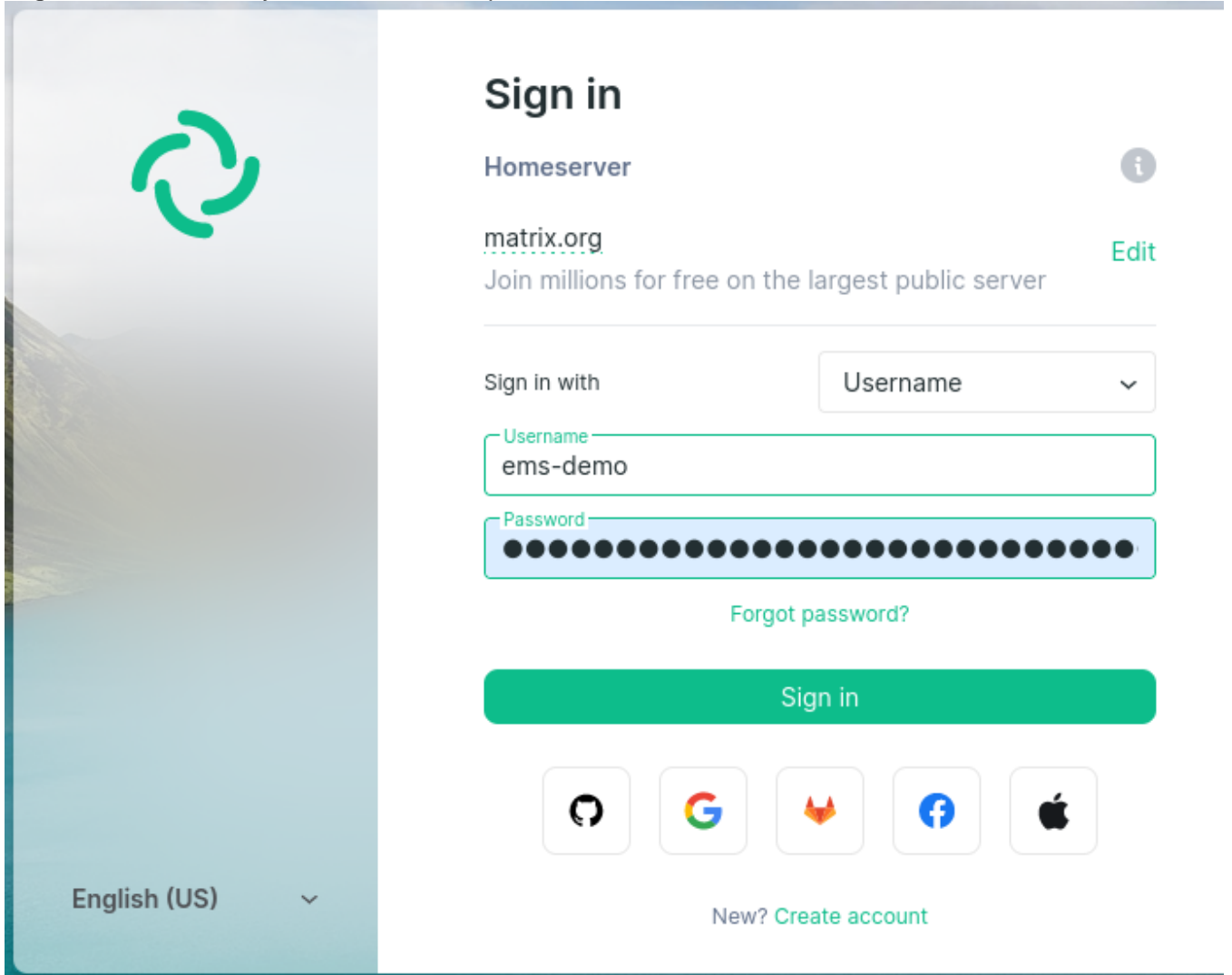
`Start using Key Backup`

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

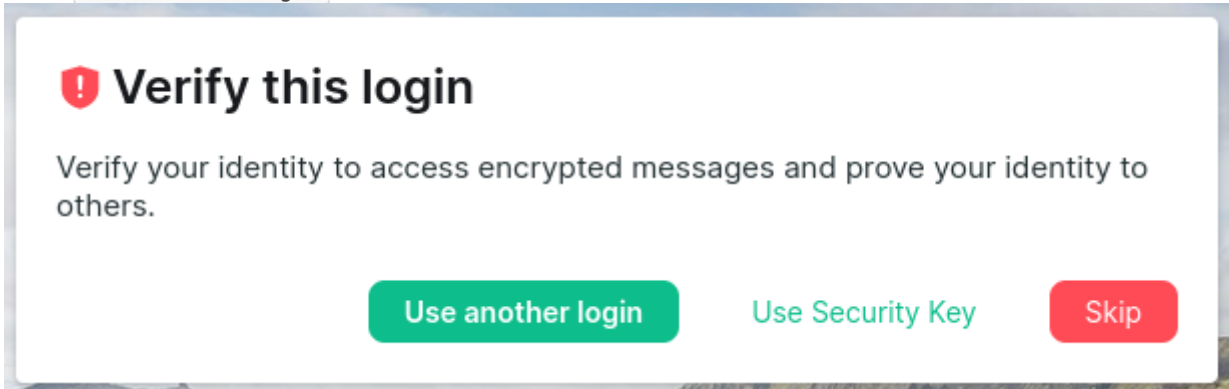


The screenshot shows the Element login interface for the homeserver `matrix.org`. The page features a green circular logo on the left and a 'Sign in' section on the right. The 'Sign in' section includes a dropdown menu for 'Sign in with' set to 'Username', a text input field for the username 'ems-demo', and a password input field with a strength indicator. Below the password field is a 'Forgot password?' link. A large green 'Sign in' button is positioned below the password field. At the bottom of the login section, there are five social login options: GitHub, Google, Nextcloud, Facebook, and Apple. A 'New? Create account' link is located at the bottom right of the page. The language is set to 'English (US)' in the bottom left corner.

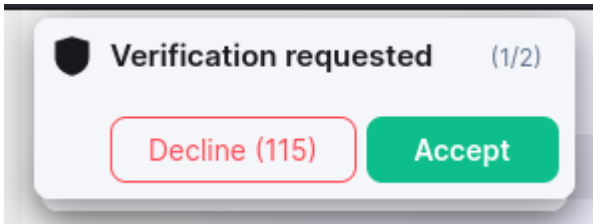
2. Choose one of the methods below for cross signing

Compare emojis using another login

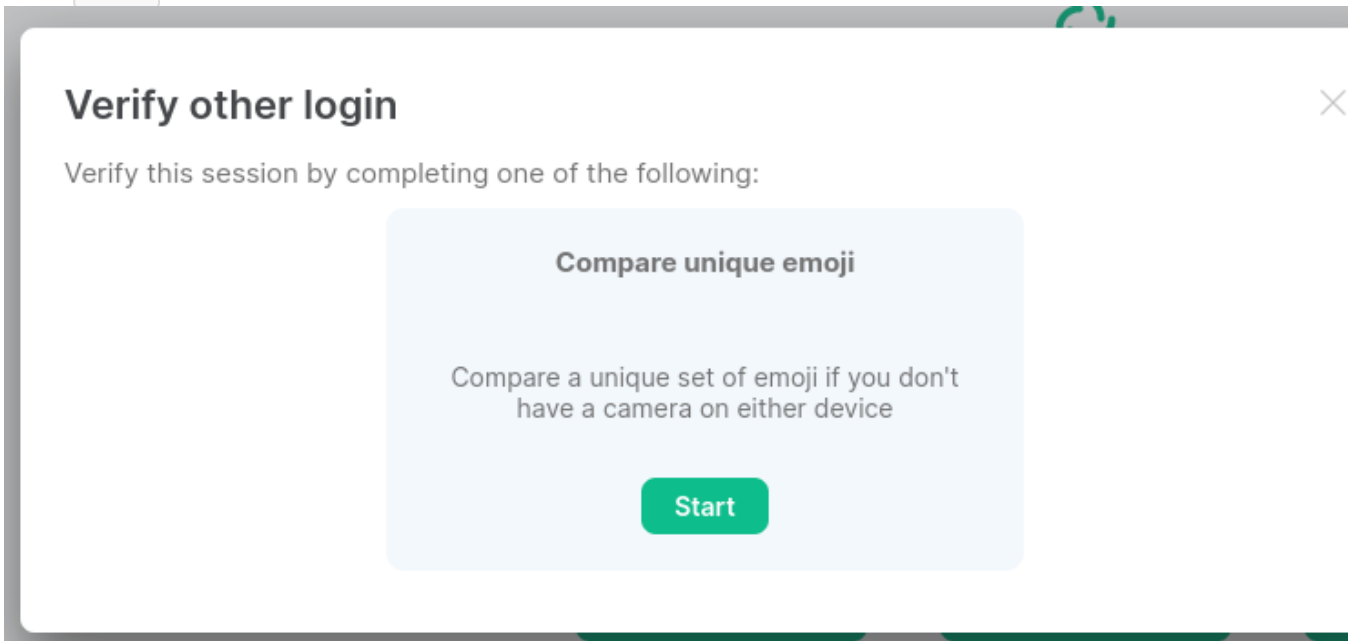
1. Click `Use another login`



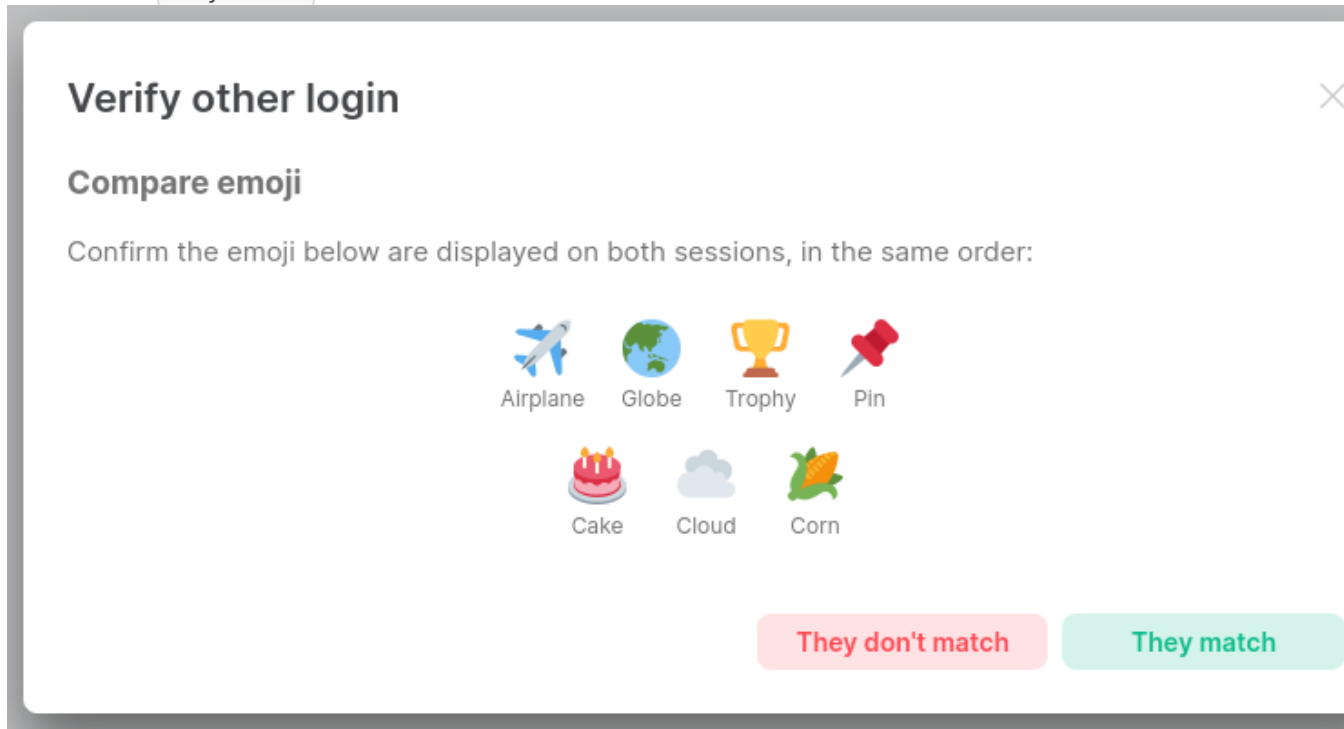
2. On another device/session that is connected to cross signing, click `Accept`



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

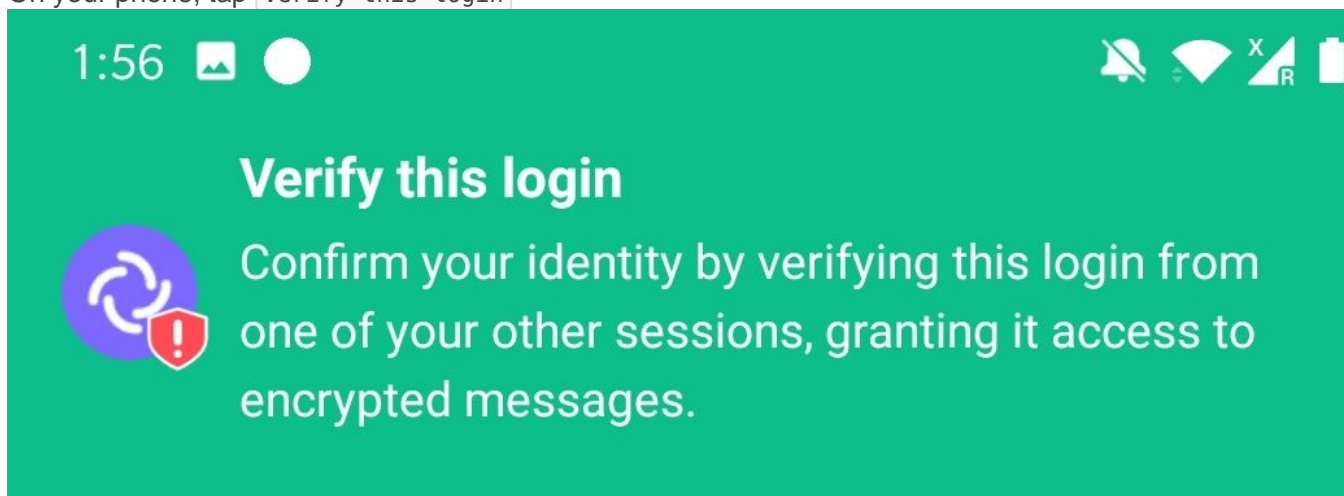


5. If all was successful, you should get this green shield on both sessions. Click `Got it`. Your new device/session is now verified and will download your backed up message encryption keys

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, tap `Scan with this device`



Verify this login

Scan the code with your other device or switch and scan with this device

Scan with this device



Can't scan

Verify by comparing emoji instead



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

2:07



Verify other login



Verify this session by completing one of the following:

Scan this unique code



or

Compare unique emoji

Compare a unique set of emoji if you don't have a camera on either device

Start

6. Your phone waits for you to confirm green shield on your other session. Click [Yes](#)



Verify this login

Almost there! Waiting for confirmation...



Waiting for ems-demo...



Verify other login



Verify by scanning

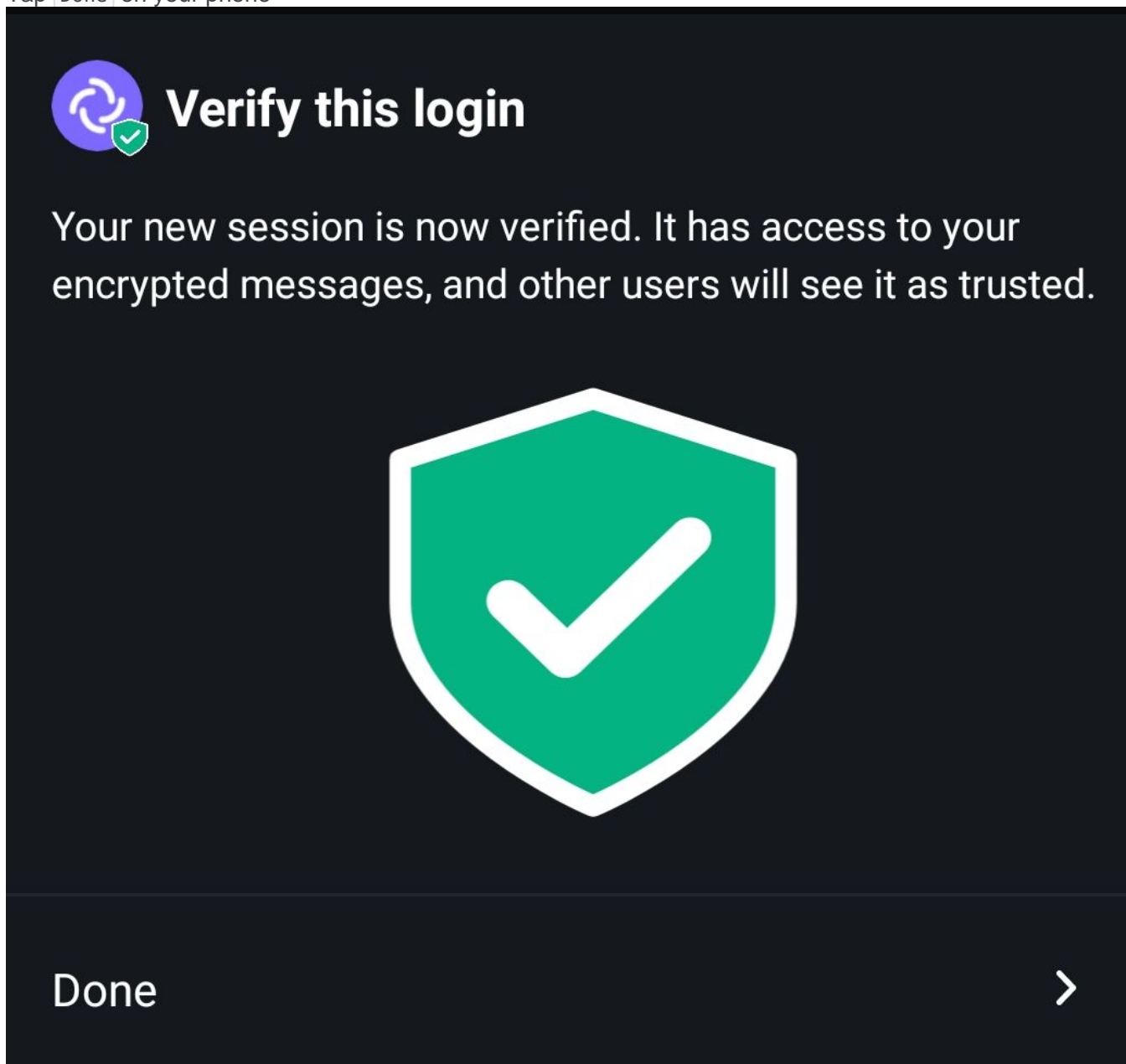
Almost there! Is your other session showing the same shield?



No

Yes

7. Tap **Done** on your phone

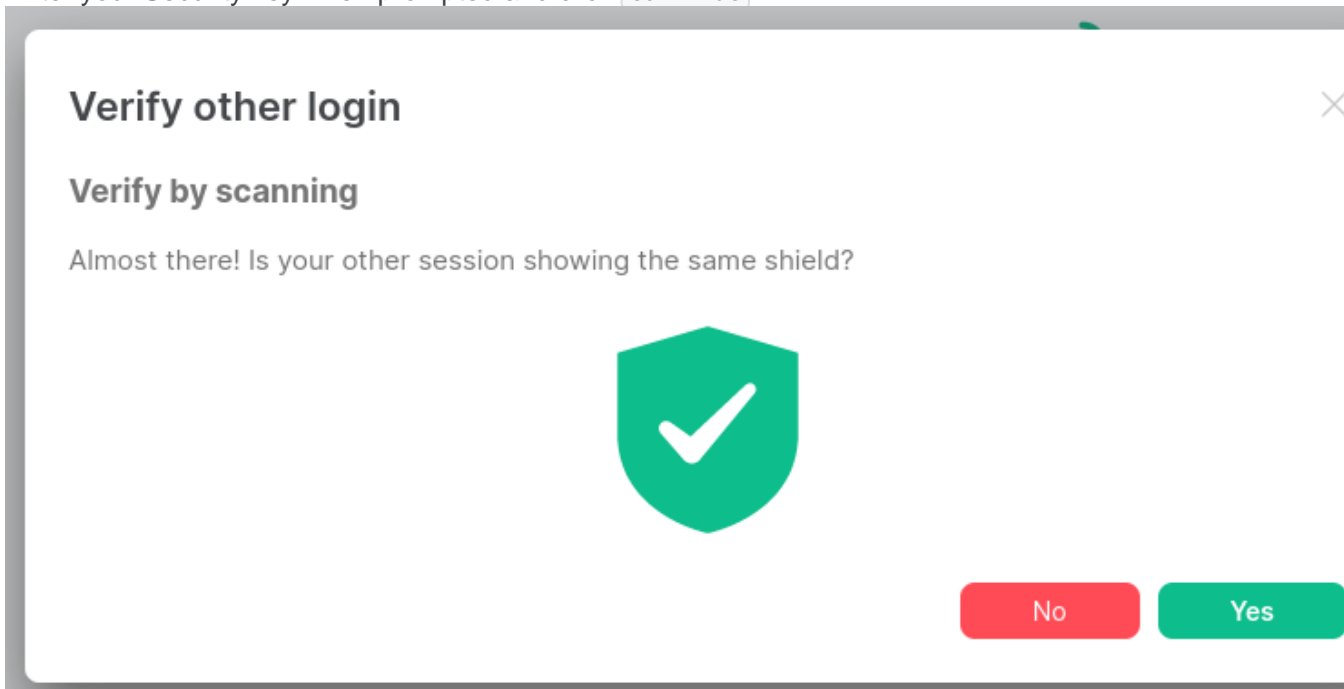


8. If all was successful, you should get this green shield on both sessions. Click **Got it**. Your new device/session is now verified and will download your backed up message encryption keys

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