

Forum:[Hack Forums](#)

Thread: [Exporting Authy codes to Ente Auth, a YubiKey or another authenticator](#)

7 - October 15, 2026, 6:05 am

This is how I moved my codes out of Authy using an iPhone, a computer and my Authy backup password. No jailbreak was needed. I tried emulating, I tried everything... until I did this.

The idea is straightforward: capture the encrypted backup that Authy sends to your phone, then decrypt it locally with your backup password. Once you have the actual authentication keys, you can import them elsewhere.

Keep Authy working until you have checked the replacement codes. You do not need to delete or reinstall it.

What you need

An iPhone with Authy already signed in and generating working codes.

Authy backups enabled and synced.

Your Authy backup password. This is different from the PIN or Face ID used to open the app.

A computer on the same Wi-Fi network.

Python and mitmproxy on the computer.

This guide covers ordinary authenticator/TOTP accounts. Authy-specific push approvals and proprietary tokens may need separate handling.

1. Prepare the computer

Install Python from [python.org](#) if necessary.

Create a folder for the export. Open a terminal in that folder and run:

```
Code python -m venv .venv
Activate the environment.
```

Windows:

```
Code .venv\Scripts\activate
macOS or Linux:
```

```
Code source .venv/bin/activate
Then install the tools:
```

```
Code python -m pip install mitmproxy cryptography
Some systems use python3 instead of python.
```

2. Start the proxy

Run:

Code `mitmweb --listen-host 0.0.0.0 --listen-port 8080 --allow-hosts "^api.authy.com(:443)?$"`
Leave that terminal running.

mitmweb also opens a local browser interface, normally at:

Code `http://127.0.0.1:8081`

The phone connects to port 8080. Port 8081 is the interface you use on the computer.

Find your computer's local Wi-Fi IP address. It will usually look something like:

Code `192.168.1.100`

Use your actual address, not that example.

If a firewall prompt appears, allow the connection on your private network. On Linux, you may need a temporary firewall rule allowing TCP port 8080 from your local network. Do not disable the entire firewall.

3. Connect the iPhone

On the iPhone, open:

Settings -> Wi-Fi -> (i) beside your connected network -> Configure Proxy -> Manual

Enter:

Server: your computer's local IP address

Port: 8080

Authentication: Off

Tap Save.

Temporarily disconnect any VPN if it prevents the phone from reaching the computer.

Before touching Authy, open an ordinary website in Safari. If nothing loads, fix the proxy connection first. There is no point troubleshooting Authy while the phone cannot reach the proxy.

4. Install and trust the certificate

In Safari, type this exact address:

Code `http://mitm.it`

Use http for this installation step.

Download the iOS certificate and allow the profile download.

Then open:

Settings -> General -> VPN & Device Management

Select the downloaded mitmproxy profile and install it.

Downloading the profile is not the same as installing it.

After installation, open:

Settings -> General -> About -> Certificate Trust Settings

Enable full trust for mitmproxy.

If it does not appear there, go back to VPN & Device Management and check that the profile was actually installed.

5. Capture Authy's encrypted tokens

Open Authy normally, then close and reopen it once.

In mitmweb on the computer, look for requests to:

Code `api.authy.com`

The request you want is a GET whose path ends with:

Code `/authenticator_tokens`

A useful response contains something like:

```
Code {
  "authenticator_tokens": [
    {
      "name": "Example account",
      "encrypted_seed": "...",
      "salt": "...",
      "unique_iv": "...",
      "key_derivation_iterations": 100000
    }
  ]
}
```

Those encrypted seeds are what you need.

If Authy is not making a fresh request:

Try making a harmless label change to one account, then close and reopen Authy. A rename may produce an update request first; that is useful evidence that traffic is getting through, but it is not necessarily the full token list.

Leave backups enabled. Do not switch them off to force a sync.

That caused unnecessary trouble during my export.

6. Make sure you capture the full list

Authy may send a list of accounts it already knows about in an apps query parameter. This can result in an empty or partial response.

On the authenticated GET /authenticator_tokens request:
Use mitmweb's request editor.

Bind the apps query parameter.

Clear its value, leaving apps=.

Keep the other authentication parameters unchanged.

Replay the GET promptly while its authentication values are still valid.

Do not replay an update or delete request by mistake.

Save the full response body as:

Code authenticator_tokens.json

Check how many records it contains against the number of accounts in Authy.

Do not post the request URL online. It contains authentication information. The JSON response also belongs in your private backup folder.

7. Decrypt the export

There are community tools that decrypt this JSON using your Authy backup password.

One documented workflow is:

[Export-Authy-Tokens — instructions and Python exporter](#)

Download and inspect the script, then follow its current usage instructions. Enter your backup password locally when prompted.

The usual decryption uses:

PBKDF2-HMAC-SHA1 to derive the key.

The iteration count and salt stored with each token.

AES-256-CBC with the token's IV.

You do not need to manually calculate any of that.

A failed record does not automatically mean your password is wrong.

During my export, 75 records decrypted and passed validation. One record decrypted but did not contain a valid Base32 secret. The sensible result was to export the working records and keep the

failed encrypted record for investigation.

Do not discard the original capture.

8. Clean up the names

Before importing, separate each entry into:

Code Provider: Hostinger
Account: you@example.com
Rather than:

Code Provider: Hostinger
Account: Hostinger: Hostinger: you@example.com
Authy sometimes leaves the provider field empty while putting the useful name in the account label.
Examples include:

Code 12345678 @ GoDaddy
Hostinger: you@example.com
Proxmox VE - customer: root@pam
Keep server names, customer names and domain context where they distinguish accounts.

An email address alone does not prove which service the code belongs to. If the source label is unclear, keep it for review rather than inventing a provider.

Also, two entries showing the same six-digit code are not enough to prove they are duplicates. Compare the underlying secret and OTP settings. Different URL labels may still be worth preserving even when they share a secret.

9. Import into Ente Auth

Ente accepts a plain-text file containing one OTPAuth URI per line:

Code
otpauth://totp/Example:you%40example.com?secret=BASE32SECRET&issuer=Example&algorithm=SHA1&digits=6&period=30
In Ente, open:

Settings -> Data -> Import codes -> Plain text

Select the exported TXT file.

Check several codes against Authy, preferably near the beginning of a new 30-second interval.

If you are replacing an existing Ente list:
Export the complete existing list first.

Combine it with the Authy export so existing Ente-only accounts are not lost.

Move the old entries to Trash rather than permanently deleting them.

Import the cleaned list.

Make sure you are viewing All, not Trash.

That last point matters: otherwise you may be looking at the old unnamed entries and think the cleanup failed.

10. Add the codes to a YubiKey

For normal six-digit authenticator codes, use Yubico Authenticator and the YubiKey's OATH application.

The similarly named Yubico OTP application is a different feature.

You can add credentials using:

A QR code generated locally from the OTPAuth URI.

Manual entry of the provider, account and secret.

YubiKey Manager's oath accounts uri command for scripted imports.

Do not upload your OTPAuth URIs to an online QR-code generator. Generate the images locally.

Capacity:

YubiKey firmware 5.7 and later: up to 64 OATH credentials.

Older firmware: up to 32 OATH credentials.

Passkey capacity is separate. A 5C NFC does not hold 100 ordinary TOTP accounts just because it supports a larger number of passkeys.

For two backup keys, add the same chosen credentials to both. Accounts spread across two keys are not a mirrored backup.

Keep the original export: you cannot rely on exporting the secrets back out of a YubiKey later.

[Yubico's OATH capacity documentation](#)

[YubiKey Manager OATH commands](#)

11. Disconnect and keep your backup

When finished:

Set the iPhone's Wi-Fi proxy back to Off.

Remove the temporary mitmproxy profile and certificate trust.

Stop mitmweb.

Remove any temporary firewall rule you added.

Keep the original encrypted capture and your cleaned export somewhere private.

The decrypted TXT files, JSON exports and QR codes contain the actual authentication secrets. Store them as carefully as your other recovery material.

Keep Authy available until you have checked the imported codes and successfully used the accounts that matter.

If it does not work

Nothing loads on the iPhone

Check the proxy IP, port, saved Wi-Fi settings, VPN and computer firewall. Test Safari before Authy.

Safari shows a certificate warning

The certificate is not correctly trusted, or you installed a different certificate from the one the running proxy uses. Fix that before continuing.

Authy connects but no keys appear

Look for the GET token-list request, not just POST updates. Check whether the apps filter is excluding accounts.

Authy disconnects during TLS

Check certificate trust first. Certificate pinning is another possibility, but a failed handshake alone does not prove it.

An Android emulator gives an integrity-token error

That is a different problem from knowing your backup password. Both the standard Android emulator and BlueStacks failed Authy's integrity checks during my attempt. The working route was the already-authorized iPhone.

The password works for most entries but one fails

Keep the successful entries and preserve the failed original. Do not throw away an otherwise valid export.

Ente still looks unnamed after importing

Check that you are viewing the active list rather than Trash. Then inspect whether the provider was genuinely missing from Authy's metadata.