2FA Authenticator

by TypingDNA

Technical white paper

The 2FA Authenticator for your Chrome browser, secured with your typing pattern

What is the 2FA Authenticator?

The 2FA Authenticator makes TOTP based 2FA available for anyone, anywhere. You don't need a phone, you don't need an extra device, or any extra sensor on your computer. It works with your keyboard right in your Chrome browser.

It works exactly like any other TOTP authenticators (such as Google Authenticator) but does not require to be installed on your phone. It works as a Chrome extension. Also, the 2FA Authenticator further secures your secret codes with your typing pattern (the TypingDNA technology).

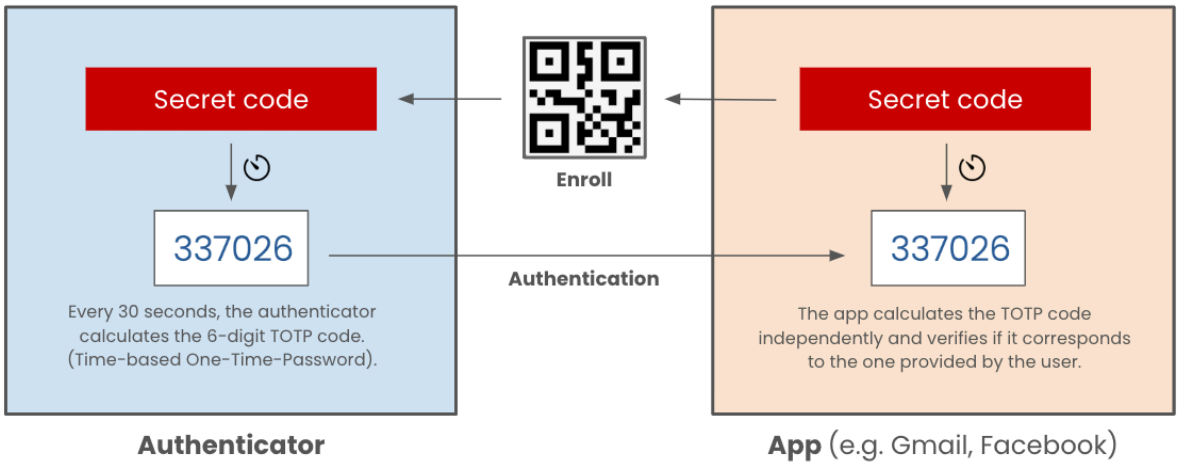
Versions

2FA Authenticator is available in 2 variants:

- **Secured/Premium**
  - Allows you to store all your secret codes and generate TOTP codes on the fly.
  - Your secret codes are kept locally, encrypted at rest with an encryption key that is kept online, protected with a password and your typing pattern (the TypingDNA technology).

- **Unsecured/Free**
  - Allows you to store all your secret codes and generate TOTP codes on the fly.
  - Your secret codes are not extra protected. Anyone who has access to your computer could be able to access, copy and use your codes. This is the level of most other online authenticators.

How do TOTP authenticators work?



The above sketch represents a system consisting of an authenticator and an app that uses the TOTP (Time-based One-Time-Password) authentication mechanism for 2FA. Any such system uses the following codes:

1. Secret codes

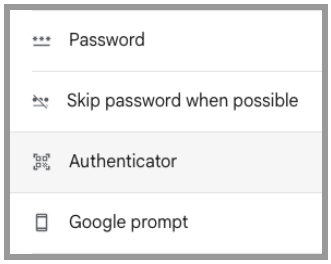
Or simply "secrets" these are the codes you scan in the form of a QR code when you enroll in a new TOTP 2FA service. These secrets are only exchanged at enrollment. After that, both the client app (your authenticator app) and the server app (the app where you want to use it) will know the base secret for your TOTP codes.

2. TOTP/6-digit codes

Sometimes called simply "codes", "2FA codes", "tokens" or "OTP codes". TOTP stands for Time-based One-Time-Passwords. These are tokens that re-generate every 30 seconds using a HASH function that takes as params your secret code and the current time (absolute time). These tokens are used to verify that the other party has the correct secret code, also known as authentication, or second factor authentication. This type of verification can be carried out without sending/compromising the secret code itself.

Step by Step, how do TOTP authenticators work:

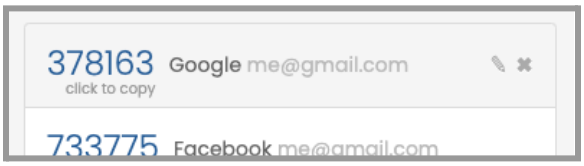
To further explain the process we will use Gmail as an example. To proceed once logged in the app, go to Security > 2FA, and look for an "Authenticator" option.



1. Enroll

First time you use an authenticator, you will have to enroll the secret code in your authenticator app as a new account. Typically you will record it with the name of the app and your username (e.g. Google : myemail@gmail.com). The page you want to secure (Gmail in our example) will typically show a QR code (and under it the actual 16/32/64 char alphanumeric code) that you have to introduce in your authenticator app (2FA Authenticator, Google Authenticator, etc).

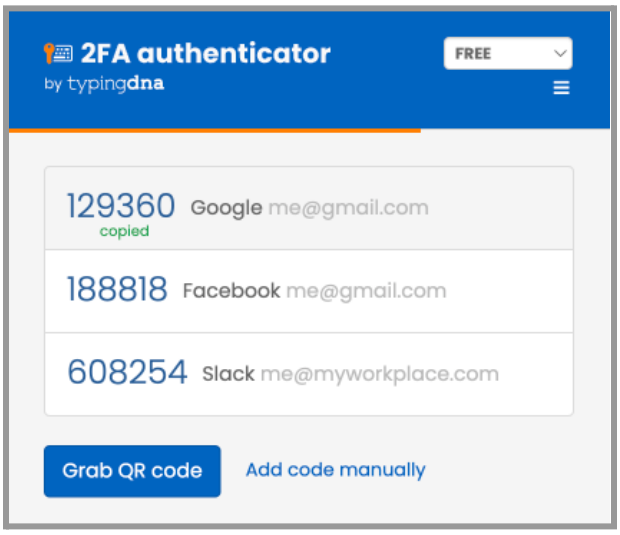
Once you add a new account by scanning the QR (or manually), to finish enrollment you will be asked to provide the first code from your Authenticator app.



2. Authentication

Now that you have enrolled your Gmail secret code in your authenticator. You will be able to see/copy the 6-digit TOTP codes the app generates. Typically you would manually type the code in your app (during login), sometimes you can copy and paste the code, and with our 2FA Authenticator, when you click on the code, the app attempts to inject it in the appropriate text field in the active webpage.

Note that many apps today will verify to make sure you are a real person (to protect against automated attacks), and will wait for you to manually enter the code, or at least one character. So if copy and paste does not work, you will have to manually delete the last character of the 6-digit code and type it again, so that it looks like it was manually entered.

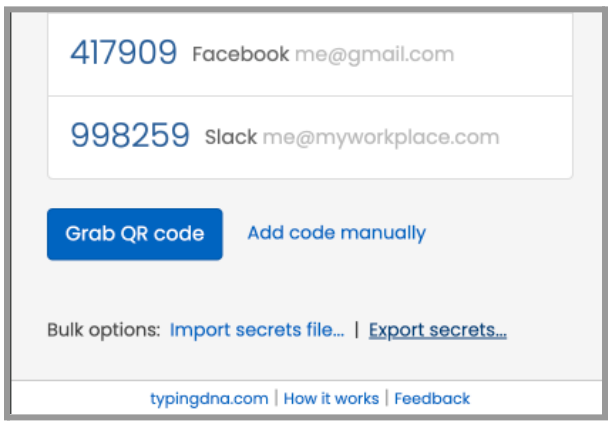


3. Migration

Many TOTP authenticators don't allow you to view the secret codes on your device, in some cases they do let you see it, but it's a rather complicated process, and migration is not easy either. They do this mostly because they don't want you to be able to migrate easily to other providers.

In the 2FA Authenticator, you can simply click the edit icon and you will be able to view the code and a generated QR that you can scan on your phone, to have it in 2 places, just in case. This makes the 2FA Authenticator also a vault for secret codes, a place to keep a copy of your secret codes. Please keep in mind that the secret codes are never sent to our cloud, they are solely stored on your device, locally. You are responsible to keep backups of your secret codes.

To migrate your codes from the 2FA Authenticator, you can always use the import/export secrets functionality, which you can find right below your TOTP codes.



FAQ

How is 2FA Authenticator different?

Any TOTP authenticator has to be able to store a secret code, and to generate the 6-digit code whenever requested. However, most authenticators run on a mobile device (such as Google Authenticator). Our 2FA Authenticator works as a Chrome extension, allowing you to generate your 6-digit codes without the need to use a mobile device. That being said, you can still use a mobile device as a backup TOTP authenticator.

In addition, our 2FA Authenticator has the ability to encrypt and protect your secret codes, at rest, by using your typing pattern (the TypingDNA technology also known as typing biometrics authentication). This is considered a much safer way to protect your codes and allow you to run 2FA authentication in your apps without compromising your security posture.

Where are my secret codes stored?
Your secret codes are stored 100% locally on your computer, in your Chrome browser storage. We encrypt your codes with either a generic key for Free accounts, or a personalized unique key that is held in the cloud, protected with your typing pattern and a password, for Secured/Premium accounts.

Locally the secret codes are stored at the location you installed the extension - on that particular Device/OS/OSUser/ChromeBrowser/ChromeUser, in the local storage, tagged with a hash of your Email Address (if the address is known).

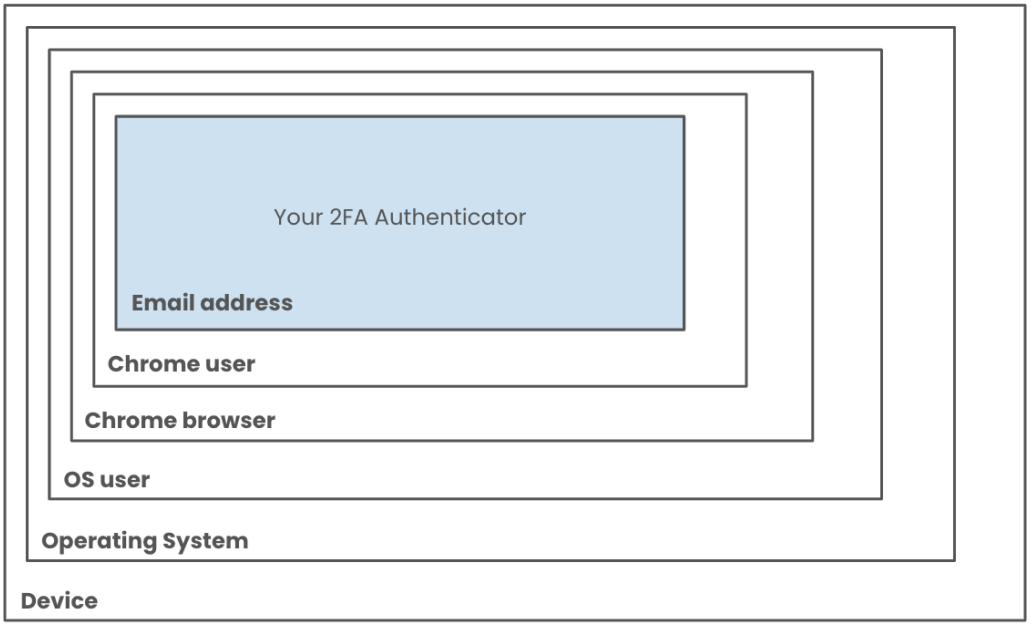
What do you store in the cloud?
If you use a Secured account, even if you just create a Secured/Premium account, or log into the Premium version, every time you create a Secured account with us, the account is created locally to store the secret codes (encrypted with a master encryption key), however the encryption key will be stored in our authentication cloud, protected with your credentials and your typing pattern.
When you log in we collect the following:
1. Your unique ID combining: Device + OS + OS User + Chrome Browser + Chrome User + Email Address.
2. Your Email address (to be able to reset your account/password, and to activate your Premium license).
3. Your Password (for extra security).
4. Your Typing Pattern (the way you type your credentials above).
5. Commercial license details (if any).

Note that we don't store your secret codes online. In order to migrate secret codes from one Device/OS/OSUser/ChromeBrowser/ChromeUser/EmailAddress to another you will need to use the migration method described above.

What happens if I lose my device? Can I retrieve my secret codes from your service?
No. If at any point you lose your device, or ability to log into your Chrome browser, at the location where your 2FA Authenticator was installed, there is NOTHING we can technically do to help you restore your codes, as they were only saved on that particular Device/OS/OSUser/ChromeBrowser/ChromeUser/

with your email address. Even if you try to create a separate local account with the same email address on a separate location, you will not be able to access your codes that are saved on the initial location. We say “location” instead of “device” because one device can have multiple operating systems on it, which can have multiple users, which can have multiple Chrome browsers installed, which can have multiple Chrome users logged in, under which you may keep your 2FA Authenticator installed.

Below image shows where your 2FA Authenticator sits in regard to your device, Chrome browser, etc.



Local ID = Device + OS + OS user + Chrome browser + Chrome user + Email

If however, you lose your ability to get to this particular location, you will have to reach out to all your apps, and change your 2FA codes, store them in a new location. If you got a Premium license, as long as you create a new local account with the same email address you will get the Premium features included, but your secret codes will not be automatically migrated.

To prevent such loss, we recommend always keeping backups of your secret codes. Please see the migration section above.

Can I reset my typing pattern and password?

Yes, you can reset both your typing pattern and your password altogether. You need to open the exact Chrome extension, in the location where you created your account (on the exact same Device/OS/OSUser/ChromeBrowser/ChromeUser). Then select “Unsecured/Premium” in the top-right corner and click the Menu button below. Then, click the “Ask for a reset code” button. Immediately after, we’ll send an email message with a temporary reset code that you will have to paste in the above page, then click the “Reset password” button. After this you will be taken through the standard enrollment process, where you will have to put in exactly the same email address, and a new password. During this

step, we will also collect your typing biometrics (how you type the email address and password, just the timings between keys, not the actual keys that you type).

Can I create multiple local accounts with the same email address?
Yes, it is possible to create local accounts on separate locations using exactly the same email address, and they will always be completely different local accounts that don't communicate with each other. The only thing that we enabled, is if you have a commercial account with us, you can use Premium local accounts, and log in with the same email address on up to 5 unique locations (different Device/OS/OSuser/ChromeBrowser/ChromeUser). Each of these accounts can have different passwords, as they are separate accounts.

Can I create multiple local accounts on the same device?
Yes, you can create and log into multiple local accounts on the same device/location (same Device/OS/OSuser/ChromeBrowser/ChromeUser), however, since your commercial account is tight to your email address only a subscribed email address will be able to use the Premium features (for up to 5 unique installs).

I used the Secured account for Free in the past, but now it is only available for Premium users. What can I do?
Until April 2024, all accounts were secured in the same way, freely. We made the change to create the Unsecured+Free version and the Secured+Premium version, because many of our users expressed that they don't need the added security and they actually prefer to not have to log in the app, while others expressed that they would be willing to pay for the added security, and asked us to keep it.

Any user can still access the Secured/Premium version, even if now it is labeled as "Secured/Premium". Once logged in however you will not be able to see your TOTP codes, nor your secret codes. However if you have any secret codes, they are still protected in the same way as before. Going forward, you will be able to either buy a Premium subscription/license, or to export your secret codes to a file. Once you export the secret codes, you can switch to our Free version, and import your codes there. You will be able to use the app in the same way as before, but you will not have to log in anymore. This, however, comes at the expense of reduced security (due to the fact that the Free version does not use your email address, password and typing pattern to keep your secret codes encrypted).

For more information please visit the 2FA Authenticator (by TypingDNA) webpage.