bitwarden | Help Center Article

PASSWORD MANAGER > VAULT BASICS

Integrated Authenticator

View in the help center:
https://bitwarden.com/help/integrated-authenticator/

Integrated Authenticator

Password Manager integrated authentication is an alternative solution to dedicated authentication apps like Bitwarden Authenticator, which you can use to verify your identity for websites and apps that use two-step login. Integrated authentication generates six-digit time-based one-time passwords (TOTPs) using SHA-1 and rotates them every 30 seconds.

> **ⓘ Note**
>
> Storing keys is available to all accounts. Generating TOTP codes is available with Premium or membership to a paid organization (Families, Teams, or Enterprise).

If you are new to using TOTPs for two-step login, refer to the Field Guide to Two-step Login for more information.

Generate TOTP codes

In Bitwarden Password Manager, you can generate TOTPs using two methods:

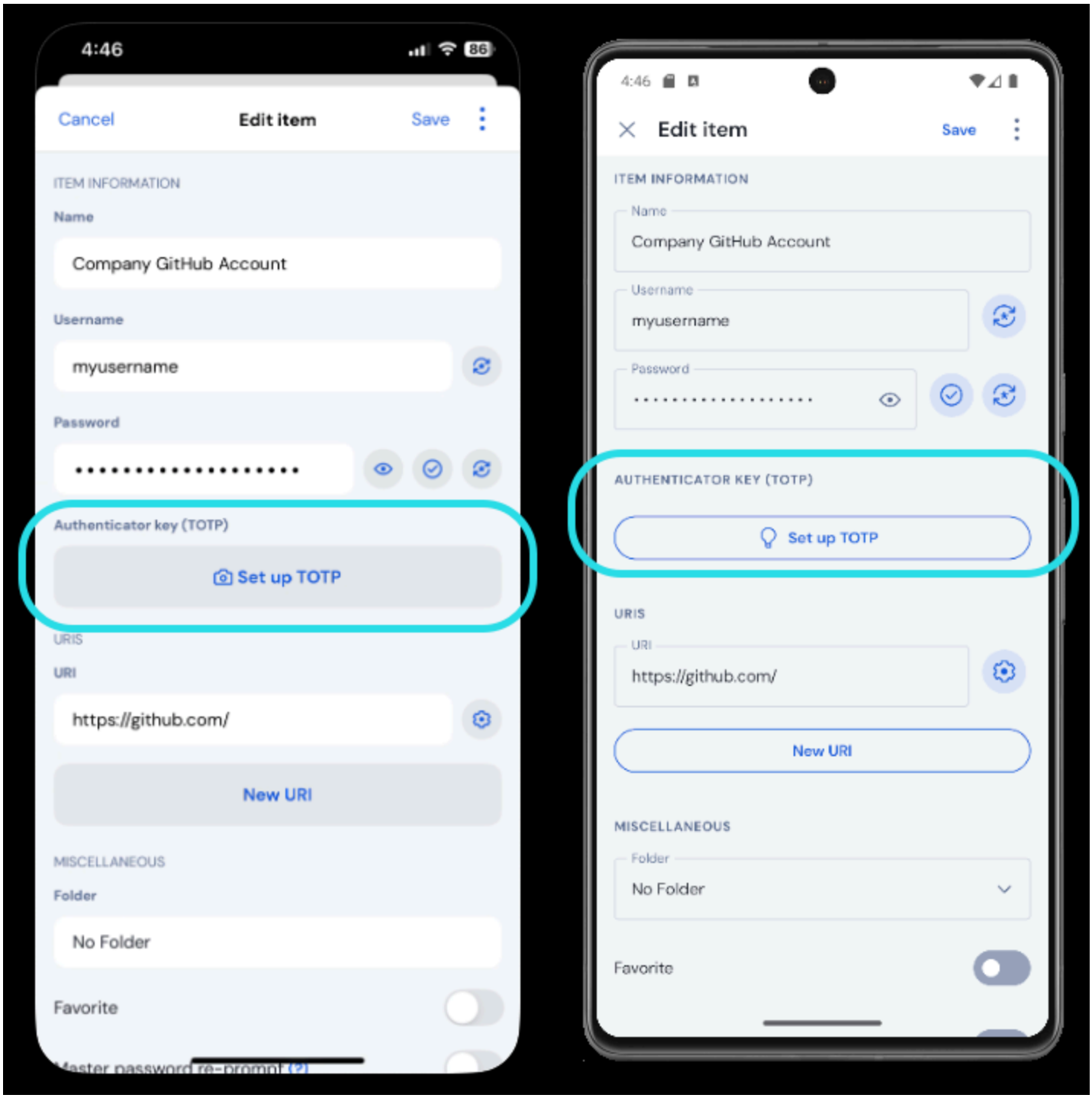
- From a Bitwarden mobile app or browser extension by **scanning a QR code**.
- From any Bitwarden app by **manually entering a secret**.

Scan a QR code

Complete the following steps to set up integrated authentication from your app of choice:

⇒Mobile

1. **Edit** the vault item for which you want to generate TOTPs.
2. Tap the **Set up TOTP** button:



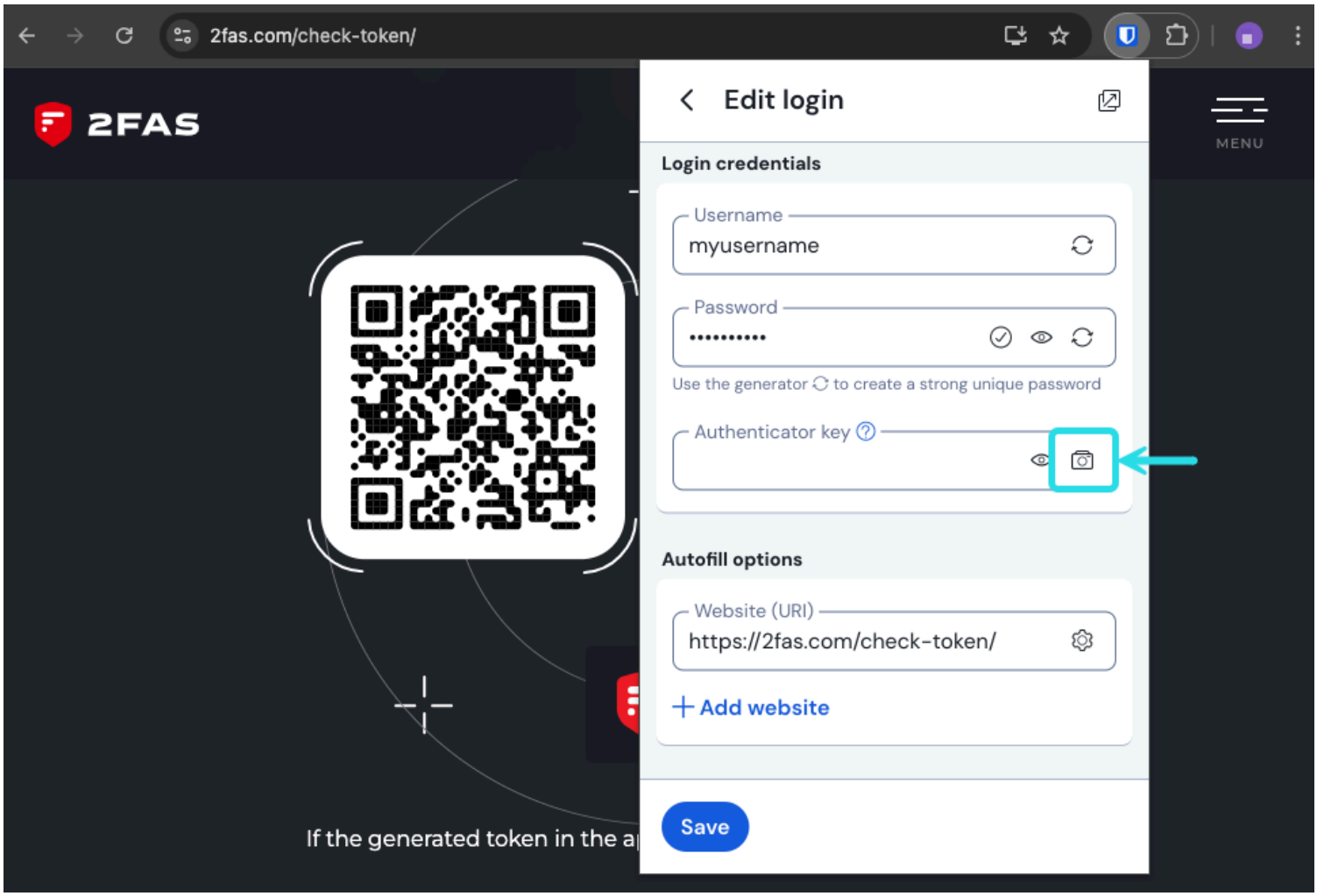
Set up TOTP on mobile

3. Scan the QR code and tap **Save** to begin generating TOTPs.

⇒Browser extension

1. **Edit** the vault item for which you want to generate TOTPs.

2. Select the **TOTP** button, which will scan the authenticator QR code from the current webpage. The full QR code must be visible on-screen.



Browser extension TOTP scan

3. Tap **Save** once the code has been entered to begin generating TOTPs.

Once set up, integrated authentication will continuously generate six-digit TOTPs rotated every 30 seconds, which you can use as a secondary step for two-step login to connected websites or apps. You can update the TOTP seed at any time using the icon on the Edit Item screen.

Manually enter a secret

Complete the following steps to manually enter a secret key:

1. **Edit** the vault item for which you want to generate TOTPs.
2. Select the **Authenticator key** field. On mobile apps, you can alternatively select **Set up authenticator key** → **Enter key manually** from the Edit view.
3. Paste the secret key into the **Authenticator Key** field and save the item.

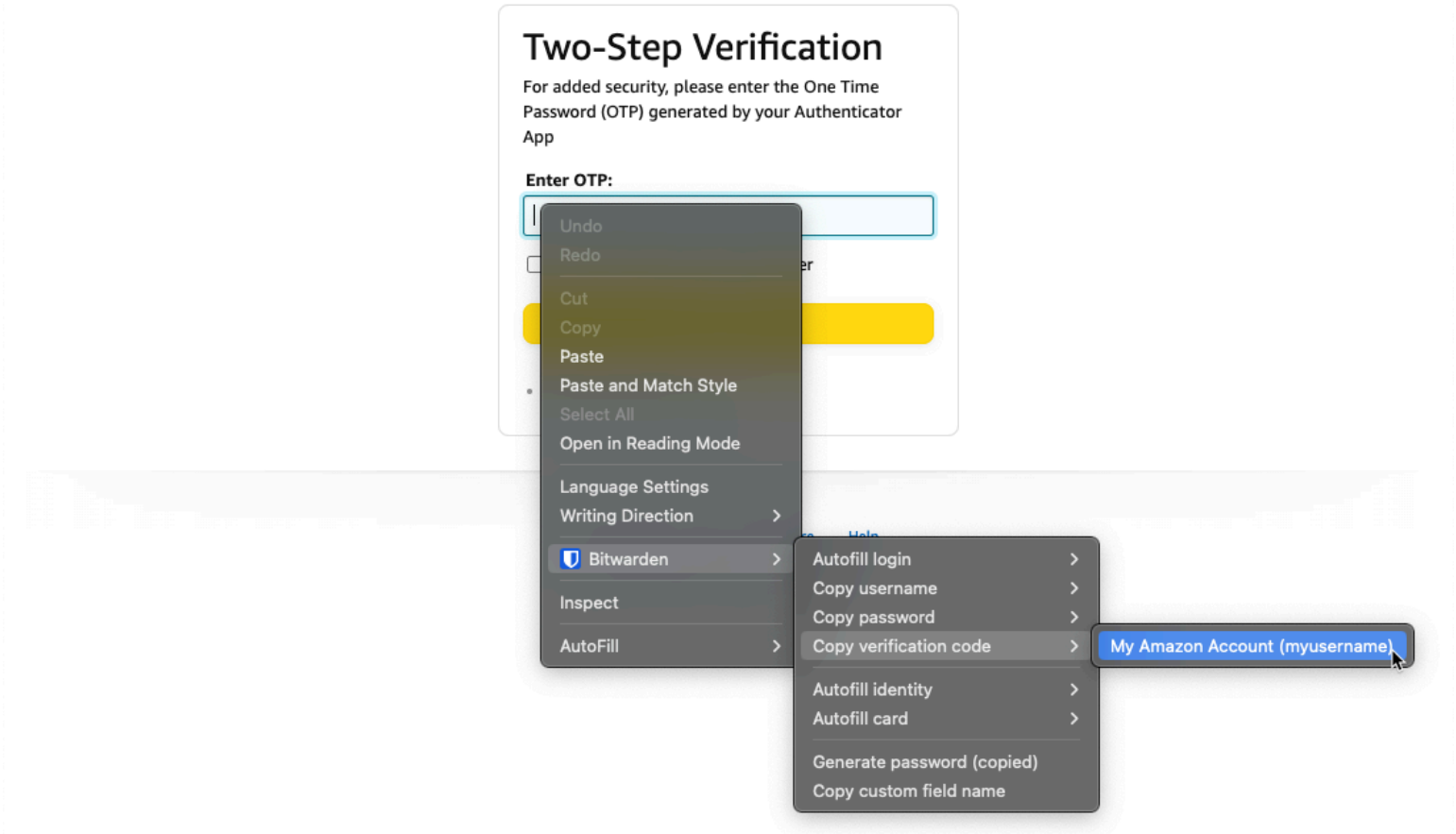
Once set up, integrated authentication will continuously generate six-digit TOTPs rotated every 30 seconds, which you can use as a secondary step for two-step login to connected websites or apps. You can edit the TOTP seed at any time using the icon on the Edit Item screen.

Use generated codes

> **Tip**
> TOTPs rely on time-based code generation. If your device has an incorrect time compared to the server, it will generate codes that don't work. If you are having trouble with your TOTP codes, set your device's time and time zone to **Automatic**.

Bitwarden browser extensions and iOS (version 18.0 or newer) will autofill your TOTP code, unless the **Autofill on page load** option is active. In that case, the browser extension also copies the TOTP code to your clipboard for easy pasting into the form.

On browser extensions, you can also copy the TOTP code from the context menu:



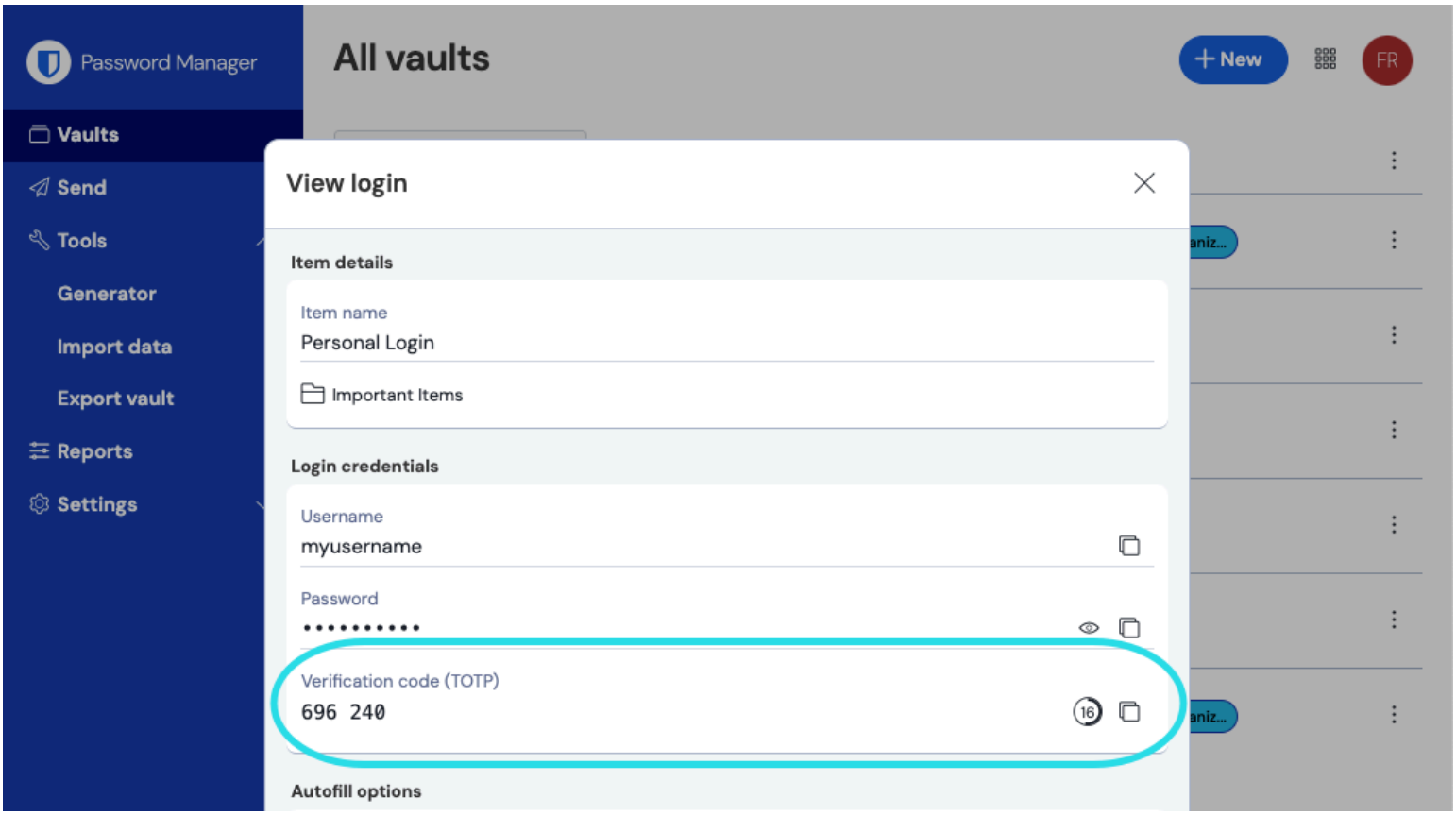
Browser Extension context menu

> **Tip**
> Automatic TOTP copying can be turned off on browser extensions using **Settings → Autofill → Copy TOTP automatically**, which will be on by default. Additionally, use the nearby **Clear clipboard** option to set an interval with which to clear copied values.

Viewing TOTP codes

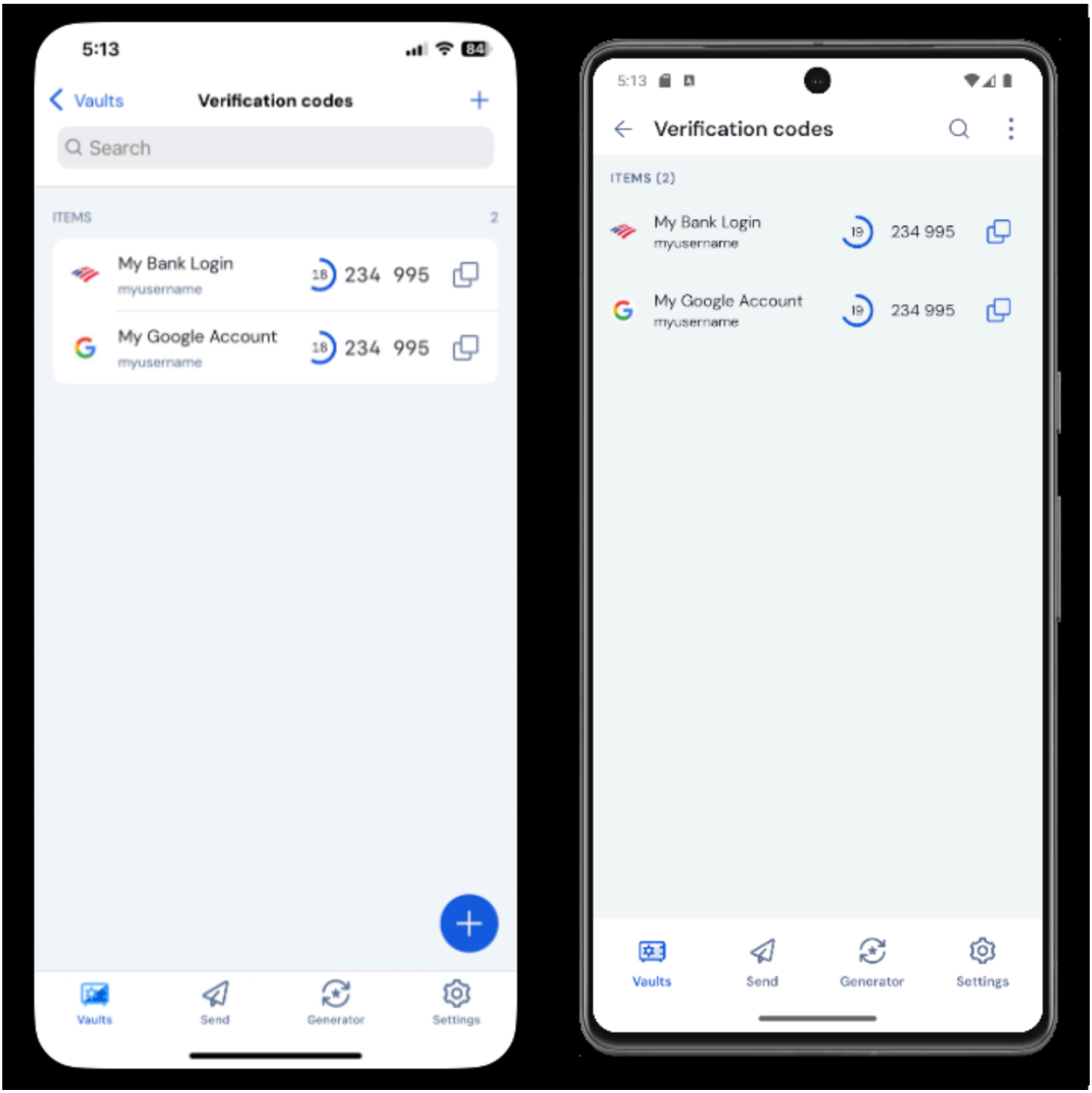
> **Tip**
> As long as you have access to your Bitwarden vault, you'll be able to view generated codes, even if you're logged in to Bitwarden while the device is offline.

All Bitwarden apps display your rotating TOTP code inside the vault item, which can be copied and pasted just like a username or password:



Copy a TOTP code

Mobile apps also have a dedicated Verification Codes screen that lists active TOTPs for quick copying:



Verification codes on mobile

Troubleshooting

TOTP codes are generated based on the system clock of your device. If your generated codes are not working or invalid, the most likely reason is that your device clock has become out-of-step from the Bitwarden server. To re-sync the clock on your device:

⇒Windows

Navigate to **Start** → **Settings** → **Time & language** → **Date & time**, and turn the **Set time automatically** option off and back on.

If this doesn't work, use the following PowerShell commands to set your timezone, being sure to replace the timezone name with the right one from this list, and restart your computer:

```
Plain Text

Set-TimeZone -Id "Central Standard Time"
```

```
Plain Text

Restart-Computer
```

⇒macOS

Navigate to **System Settings → General → Date & Time**, and turn the **Set time and date automatically** and **Set time zone automatically using your currently location** options off and back on.

⇒Android

Navigate to **Settings → System → Date & time**, and turn the **Set time automatically** option off and back on.

⇒iOS

Navigate to **Settings → General → Date & Time**, and turn the **Set Automatically** option off and back on.

Support for more parameters

By default, Bitwarden will generate six-digit TOTPs using SHA-1 and rotate them every 30 seconds, however some websites or services will expect different parameters. Parameters can be customized in Bitwarden by manually editing the `otpauth://totp/` URI for your vault item.

Parameter	Description	Values	Sample Query
Algorithm	Cryptographic algorithm used to generate TOTPs.	-sha1 -sha256 -sha512 -otpauth	`algorithm=sha256`
Digits	Number of digits in the generated TOTP.	1-10	`digits=8`
Period	Number of seconds with which to rotate the TOTP.	Must be > 0	`period=60`

For example:

```
Bash

otpauth://totp/Test:me?secret=JBSWY3DPEHPK3PXP&algorithm=sha256&digits=8&period=60
```

Learn more about using `otpauth://` URIs here.

Set a default on iOS

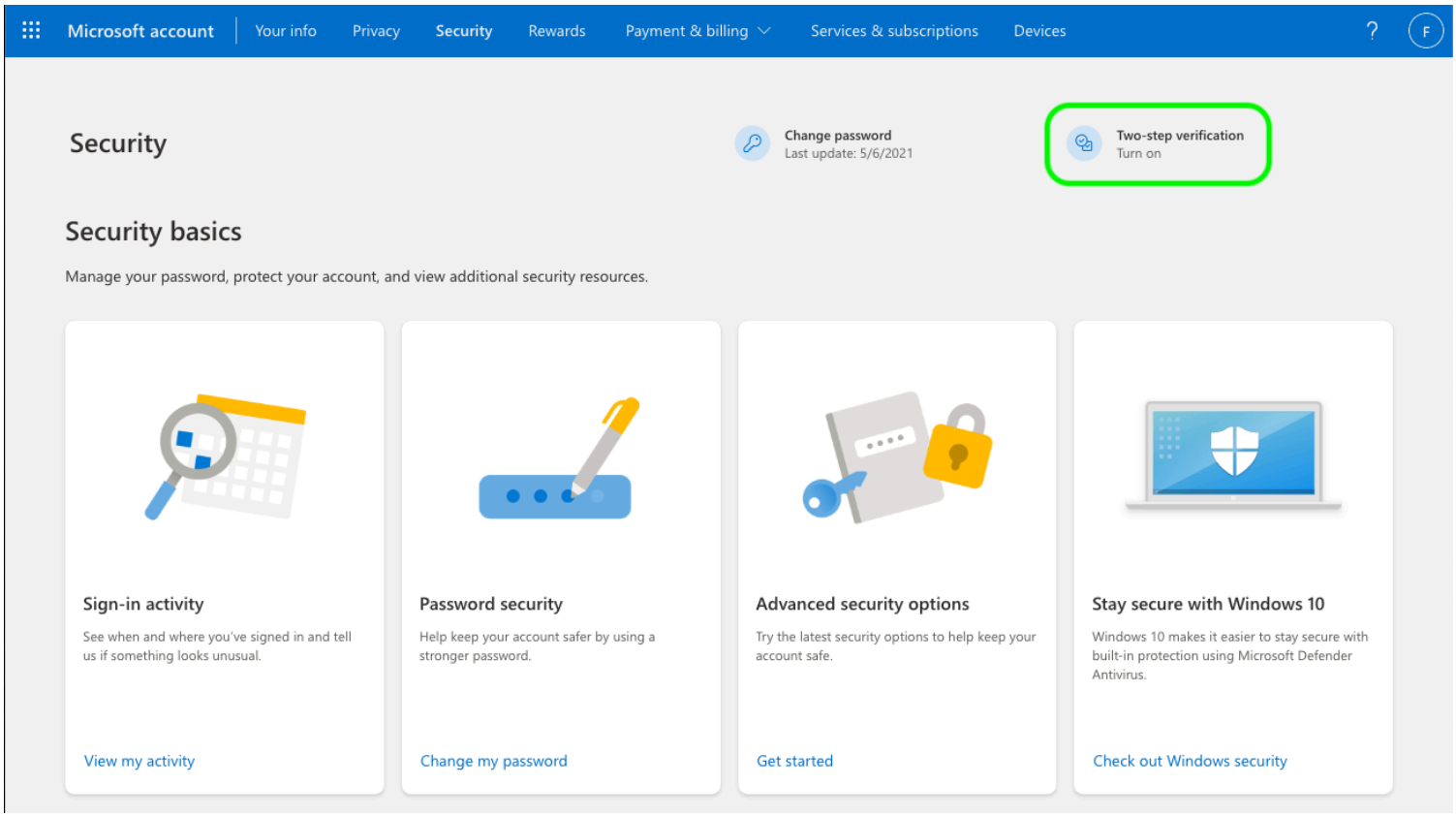
iOS users running iOS 16+ can set any application as the default for storing verification codes when scanning codes directly from the camera app, including Bitwarden Authenticator and Password Manager integrated authentication. To set this up:

1. Open the iOS **Settings** app on your device.
2. Tap **General**.
3. Tap **AutoFill & Passwords**.
4. In the **Verification Codes** section, choose an app from the **Set Up Codes In** dropdown.

Azure and Office 365

By default, Microsoft Azure and Office 365 accounts expect the use of Microsoft Authenticator for TOTPs. If you want to use Bitwarden Password Manager integrated authentication to generate TOTPs for your Microsoft Azure or Office 365 accounts, you'll need to complete the following steps:

1. In Microsoft, navigate to your account settings page. Depending on whether yours is a personal or business account, this may be `account.microsoft.com` or `myaccount.microsoft.com`.
2. Depending on whether yours is a personal or business account, open your **Security dashboard** or select **Security info**. If you're going through the **Security dashboard**, you'll need to also select **Two-step verification** from that screen.



Turn on 2FA

3. Select either the Two-step verification **Turn on** button or **Add sign-in method** button and choose Authenticator app from the dropdown.
4. During the setup procedure, you'll see a dropdown menu for the verification method. Select **Authenticator App** or **An app**.
5. Proceed until you see a blue "different authenticator app" hyperlink. Select the hyperlink when you see it.
6. Continue until you see a QR code, at which point you can follow the normal instructions here.

Steam Guard TOTPs

The Bitwarden Authenticator (TOTP) can be used as an alternative means of TOTP generation for Steam using a `steam://` prefix followed by your secret key.

Generated `steam://` TOTPs are by default alphanumeric and five digits, as opposed to traditional six-digit numeric TOTPs.

> **⚠ Warning**
>
> To use this functionality, you will need to manually extract your Steam account's secret using a third-party tool. There are tools such as SteamTimeIdler that can help you accomplish this, however such **extraction tools are not officially supported by Bitwarden or Steam**. Use these tools at your own risk.