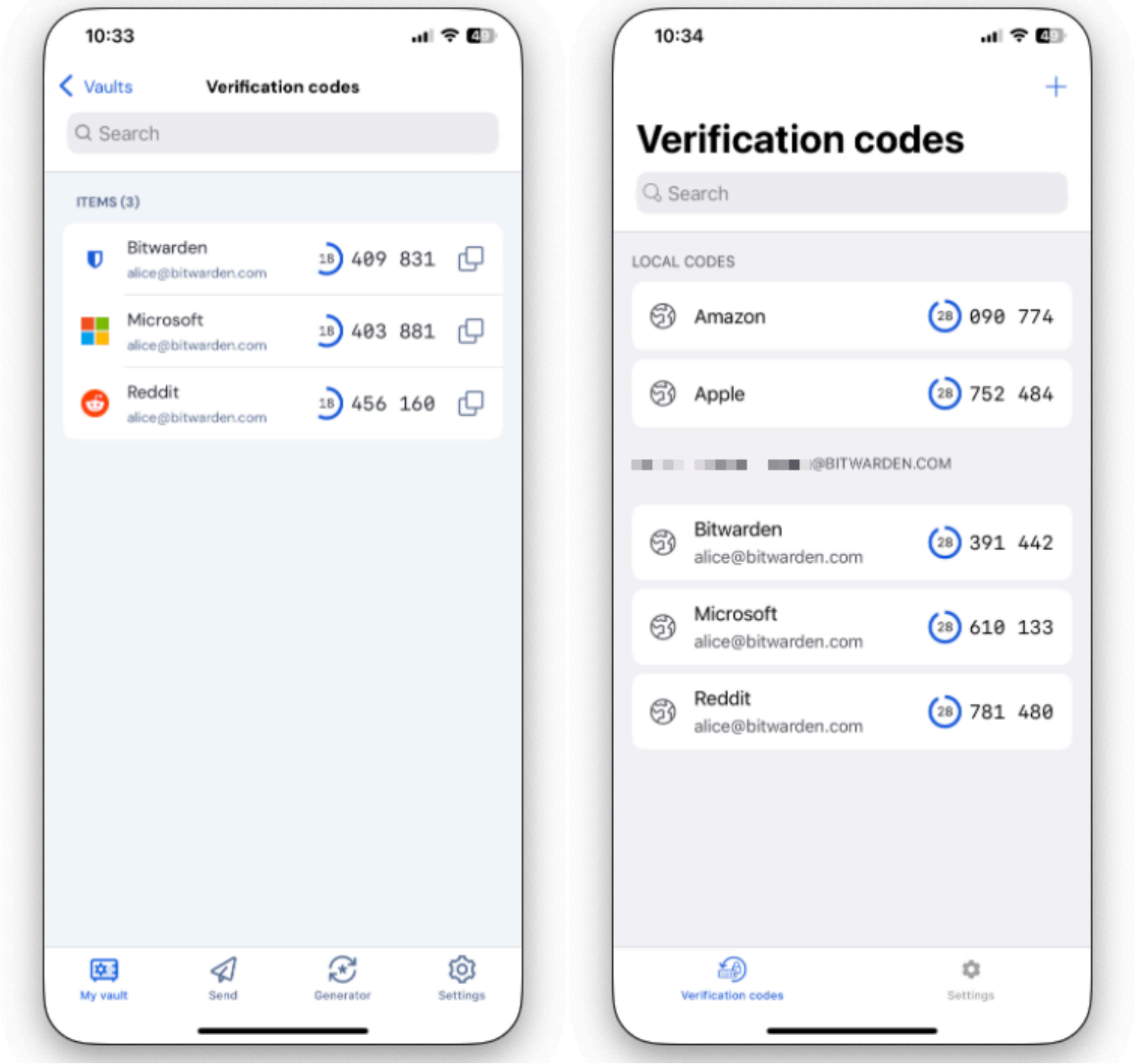
BITWARDEN AUTHENTICATOR

Sync Verification Codes

Sync Verification Codes

If you use both Bitwarden Authenticator and Password Manager, you can seamlessly sync verification codes between the two.



Sync between Password Manager (Left) and Authenticator (Right)

Syncing can be as bi-directional as you want it to be, meaning:

- You can sync codes to Authenticator from all your Password Manager accounts, or just from those you specifically choose.
- You can easily copy local codes into Password Manager, or keep them only accessible by Authenticator.

Set up sync

To set up TOTP syncing:

1. Ensure that both Bitwarden Authenticator and Bitwarden Password Manager are installed on your device, and that in Password Manager you're logged in to accounts you want to sync with.

2. In Password Manager, navigate to **Settings** → **Account security** and toggle on the **Allow authenticator syncing** option.

> **ⓘ Note**
>
> You can sync with as many Bitwarden Password Manager accounts as you want, but you'll need to toggle this option separately for each.

3. In Bitwarden Authenticator, validate that any codes stored in Password Manager are listed under your Bitwarden account's heading rather than under **Local Codes**.

Sync, once set up, happens automatically, meaning:

- You won't need to manually refresh Authenticator to get codes you've recently added or updated in Password Manager.
- You won't need to manually unlock Password Manager to gain access to the required data in Authenticator. More on how this is accomplished in the next section.

How it works

Though the core key exchange workflows are the same from platform-to-platform, the secure storage and communication methods that facilitate sync between Password Manager and Authenticator are specific to Android or iOS:

⇒Android

1. When the option to **Allow authenticator sync** is activated in Password Manager:
    1. A **global symmetric key** is generated by the Password Manager client and shared with Authenticator through the Android Interface Definition Language (AIDL).

> **Tip**
>
> AIDL is an Inter-Process Communication (IPC) abstraction that allows Authenticator and Password Manager to securely interface without any other component of your device having access to exchanged information.

2. Your pre-existing **account encryption key** is locally persisted, which will allow Password Manager item data to be decrypted when TOTP sync requires it.

2. When Authenticator is opened, as long as the **Allow authenticator sync** option is activated:
    1. A request is made to Password Manager through AIDL.
    2. Password Manager, in response to the request, temporarily decrypts your item data with the persisted **account encryption key** and re-encrypts that data with the **global symmetric key**.
    3. A subset of re-encrypted data, specifically authenticator keys, display names, and usernames, are sent to Authenticator through AIDL. No sensitive data is passed unencrypted through AIDL.
3. Authenticator receives your re-encrypted authenticator keys, display names, and usernames and decrypts that data with the shared **global symmetric key**.

⇒iOS

1. When the option to **Allow authenticator sync** is activated in Password Manager:
    1. A **global symmetric key** is generated by the Password Manager client and written to a Keychain shared by Password Manager and Authenticator.
    2. A subset of item data, including authenticator keys, display names, and usernames, are encrypted using the **global symmetric key** and written to the App Group's shared container.

> **Tip**
>
> **Keychain** uses access groups to allow secure local sharing of cryptographic keys or other data between apps made by the same developer.
>
> **App Groups** use secure local storage locations called shared containers to allow apps made by the same developer to access shared data and some inter-process communication (IPC).

2. When Authenticator is opened, as long as the **Allow authenticator sync** option is activated:
    1. Authenticator retrieves the **global symmetric key** from the shared Keychain.
    2. Authenticator retrieves encrypted authenticator keys, display names, and usernames from the App Group.
3. Authenticator locally decrypts your authenticator keys, display names, and usernames with the **global symmetric key**.

If, at any time, you deactivate the **Allow authenticator sync** option or fully log out of Bitwarden Password Manager:

- Encrypted authenticator keys, display names, and usernames, previously stored in an App Group, are deleted.

- The **global symmetric key** is deleted, but only if all users deactivate sync or logout.