

How to setup Authenticator – Firefox

Introduction

Authenticator ensures that our accounts are protected with multiple layers of security to keep our information safe. Follow this guide to set up Authenticator in your Firefox browser.

Pre-requisites:

1. Windows or MacOS desktop or laptop device
2. Internet connection
3. Firefox Installed

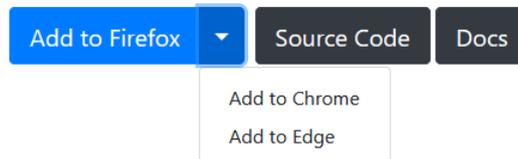
Setup guide:

1. Please use Firefox browser to visit: <https://authenticator.cc/>
2. Click “Add to Firefox” (the browser being used should be auto detected)



Authenticator

Two-factor authentication in your browser



3. Select “Add to Firefox” on top right corner and click add extension for “Add Authenticator” pop up:

4. Notice of removal from Authenticator which applies to all browsers:

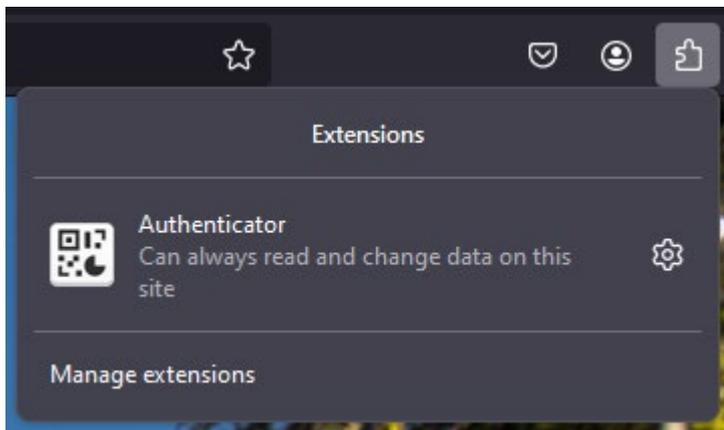
Firefox Issues

Reinstalling Authenticator with your storage location set to 'local' will cause data loss.

- Can't remember your password or lost your secrets and don't have a backup? See [Lost Codes](#)
- Want to help translate or have an issue with translation? [Check our Crowdin page](#)
- Have a bug or feature request? [File an issue](#) or [Tweet with @AuthExtension](#)

Translate Edit

5. In Firefox, you will need to give permission to the extension. Select the jigsaw puzzle icon and then click "Manage Extensions"

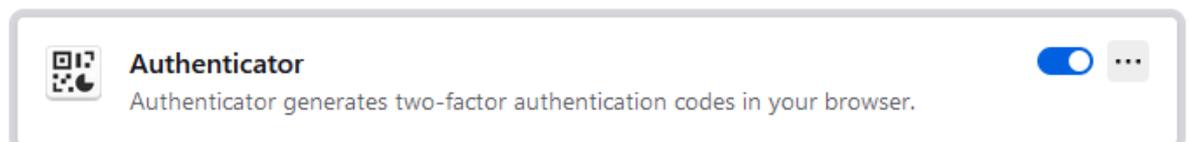


6. Now under the enabled section click on Authenticator to open the settings:

Manage Your Extensions



Enabled



7. Select the "Permissions" tab and enable "Access your data for all websites"

**Authenticator** Authenticator generates two-factor authentication codes in your browser. ☑️ ⋮

Details **Options** **Permissions**

Optional permissions for added functionality:

- Input data to the clipboard
- Access your data for all websites
- Access your data for sites in the https://dropboxapi.com domain
- Access your data for https://www.google.com
- Access your data for https://www.googleapis.com
- Access your data for https://accounts.google.com
- Access your data for https://graph.microsoft.com
- Access your data for https://login.microsoftonline.com

[Learn more about permissions](#)

8. Now login to flinders.okta.com in a new tab and it should now prompt you to setup Google Authenticator:

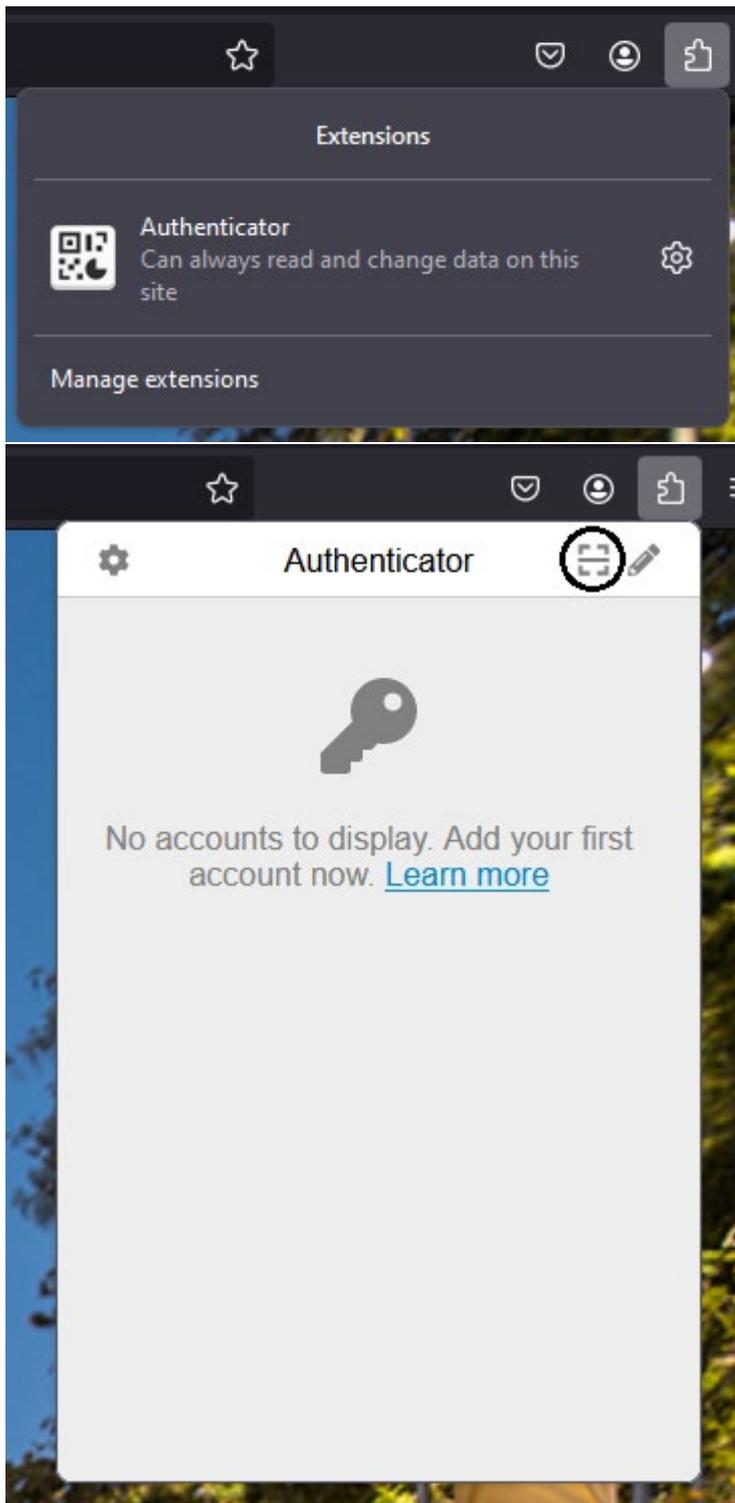
Set up security methods

Security methods help protect your Okta account by ensuring only you have access.

Set up required

**Google Authenticator**
Enter a temporary code generated from the Google Authenticator app.
Used for access
Set up →

9. Open up your Authenticator extension again by clicking the jigsaw puzzle and press the QR scanner icon to add an account:



10. Your screen will appear opaque and allow you to drag a selection field over the QR code, **please make sure the coverage area is just the QR code otherwise it will not register correctly:**

Set up Google Authenticator

Scan barcode

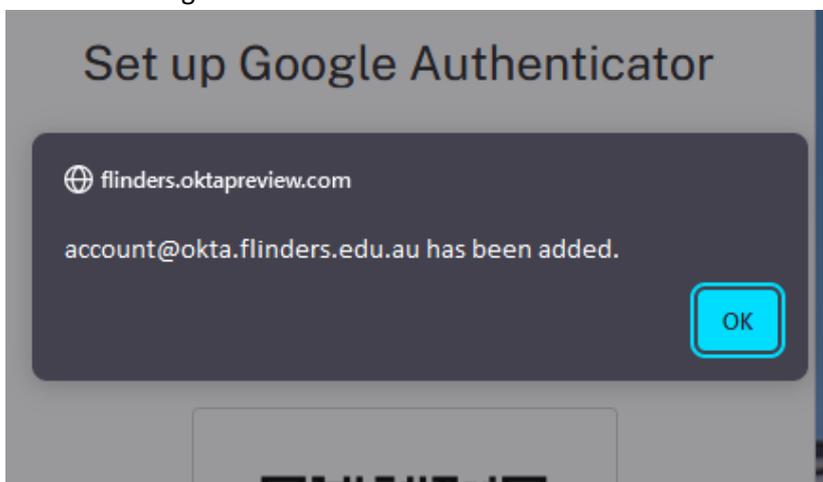
Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".



Can't scan?

Next

11. A successful registration will show the notification below:



12. Now when you open your Authenticator extension it should have the Google Authenticator code cycling through. You will need to use this code to authenticate when logging into your Flinders account.

