MFA WITH THE MICROSOFT AUTHENTICATOR APP

1 Background

As an NWU user, you may already have a multifactor authentication (MFA) method set up to access the Microsoft 365 environment. Please take note of the following important information:

If you use **SMS (Phone)** as the MFA method for Microsoft 365, please note that Microsoft will retire SMS authentication on **1 February 2027.**

To ensure uninterrupted access to Microsoft 365, set up the **Microsoft or Google Authenticator app** as an alternative MFA method.

If you use an older phone or experience issues with push notifications, you can use TOTP (Time-based One-Time Password) verification codes instead.

2 Download and Install Microsoft Authenticator (recommended)

2.1 Android Devices

1. Open the **Google Play Store**.
2. Search for **Microsoft Authenticator**.
3. Select **Microsoft Authenticator** published by Microsoft Corporation.
4. Tap **Install**.
5. Once installation is complete, open the app.

2.2 Apple iPhone/iPad

1. Open the **Apple App Store**.
2. Search for **Microsoft Authenticator**.
3. Select **Microsoft Authenticator** published by Microsoft Corporation.
4. Tap **Get**.
5. Open the app after installation.

Notes:

You can use an alternative authenticator app, such as Google Authenticator, if preferred (see **Point 6** for setup). Microsoft Authenticator supports both push notifications and TOTP verification codes, while Google Authenticator supports only TOTP verification codes.

Older Huawei devices that do not have Google Play Services may still use Microsoft Authenticator or another TOTP-compatible authenticator application, depending on the device model and operating system version. Look at the available options on the Huawei AppGallery.

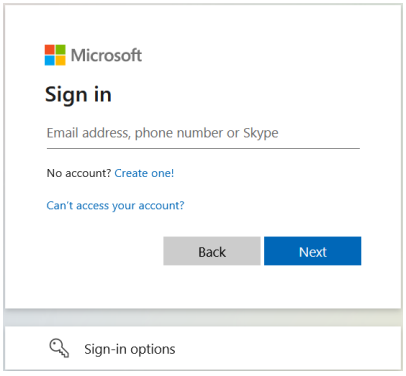
3 Steps to set up multifactor authentication with the Authenticator App.

Follow the instructions to set up the **Microsoft Authenticator app** and configure **push notifications with number matching** as your primary MFA method.

- Open a web browser and go to https://www.office.com/



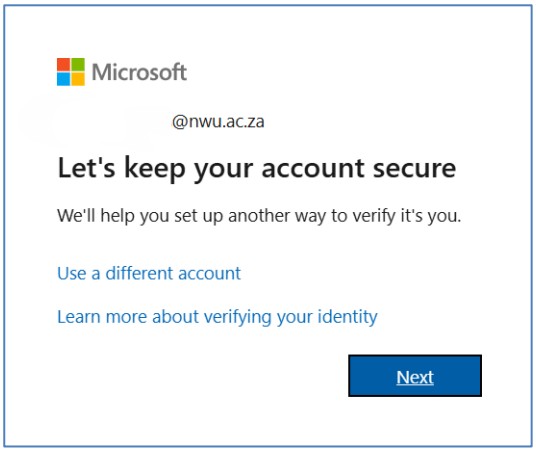
- Click Sign in
- Enter your NWU email address and click Next.



- Enter your password and click Sign in.

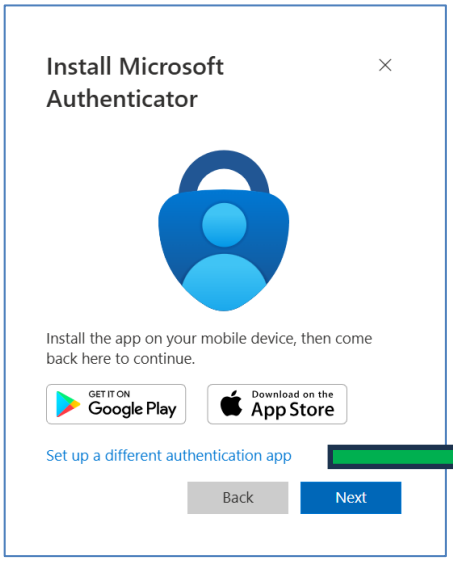


- When MS MFA is enabled for your account, Microsoft will prompt you to secure it.



Click Next in the **BROWSER ON PC**

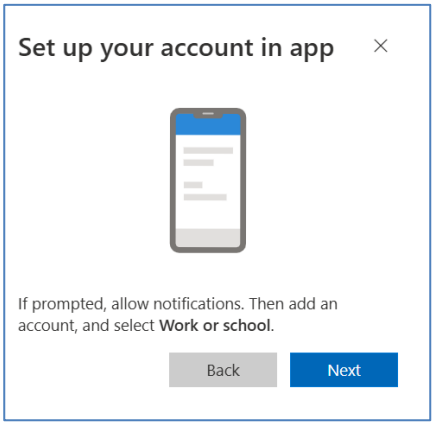
- If not already installed, download and install the MS Authenticator app from the relevant app store on the **DEVICE/PHONE** – See point 2.



Select this option if you prefer to use an authenticator app other than Microsoft Authenticator.

- Please note that you may use an alternative authenticator app, such as Google Authenticator, by clicking on “Set up a different authentication app.” If you choose to use a different app, follow the on-screen instructions to complete the setup, or follow the steps in Point 6 for the Google Authenticator App. Otherwise, follow the steps below to continue with the Microsoft Authenticator App.

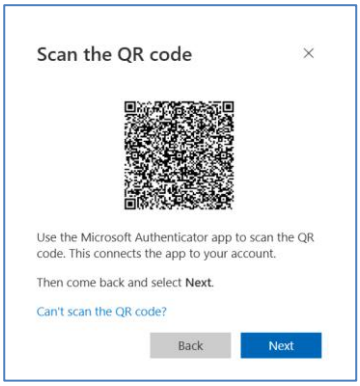
- Click Next in the **BROWSER ON PC**.



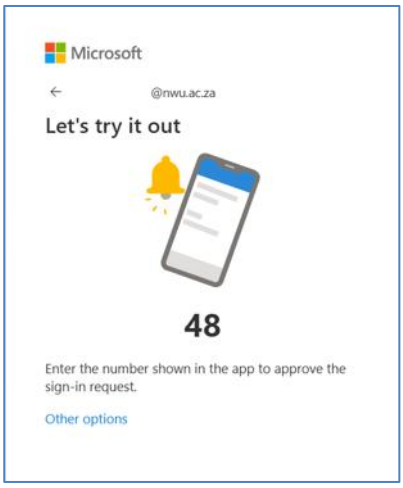
- Switch to the **DEVICE/PHONE** - IN THE AUTHENTICATOR APP, and if prompted, allow notifications.

  1. Click the + sign to add an account - select "Work or school account".
  2. Select Scan QR Code.

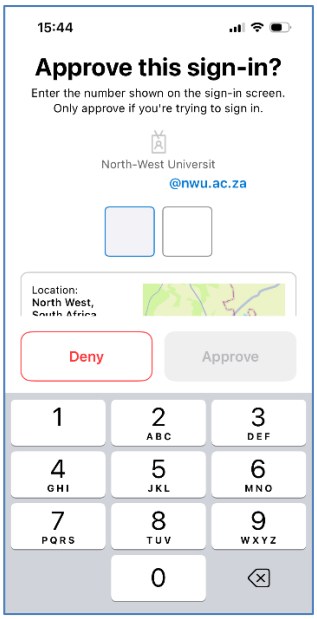
- In the **BROWSER ON PC**, click Next.



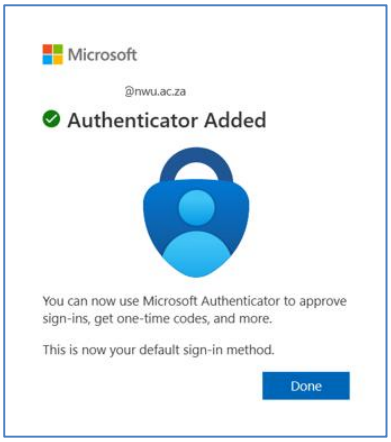
- Scan the QR code with your **DEVICE/PHONE,** then click Next in the **BROWSER ON PC**.



- Microsoft will send a code to the **DEVICE/PHONE**. Enter the code on your **DEVICE/PHONE,** then select **APPROVE.**



- You will receive a message in the **BROWSER ON PC** that the App was successfully added.



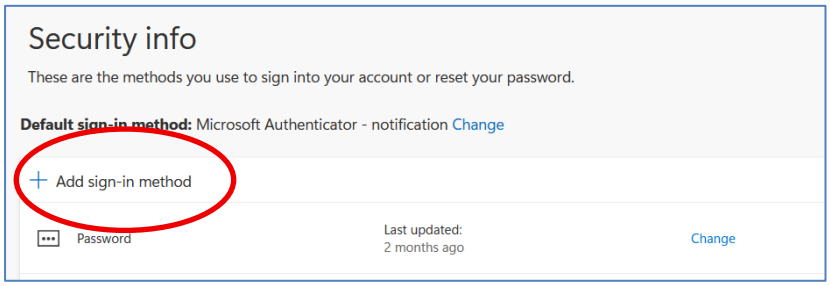
- Click Done. The setup of the Microsoft Authenticator App is complete.

4 I already have an SMS/Phone method. How can I add the Microsoft Authenticator?

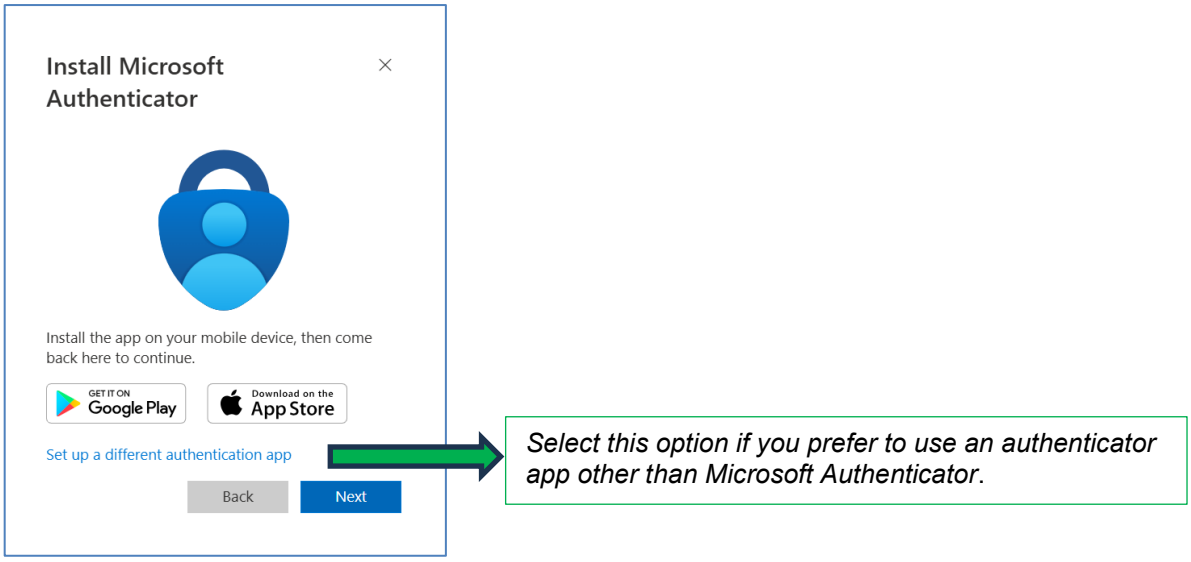
First, install the Authenticator app – see Point 2. After installing the app, follow the steps below.

- Open a web browser and go to: https://mysignins.microsoft.com/security-info
- Sign in using your NWU credentials.

  Select **Add sign-in method**.

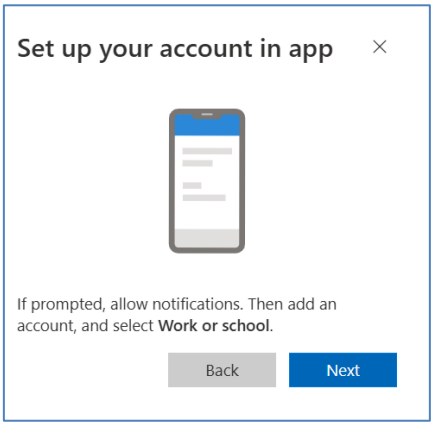


- Choose the Authenticator app.
- If not already installed, download and install the MS Authenticator app from the relevant app store on the **DEVICE/PHONE** – See point 2.



Please note that you may use an alternative authenticator app, such as Google Authenticator, by clicking on “Set up a different authentication app.” If you choose to use a different app, follow the on-screen instructions to complete the setup, or follow the steps in Point 6 for the Google Authenticator App. Otherwise, follow the steps below to continue with the Microsoft Authenticator App.

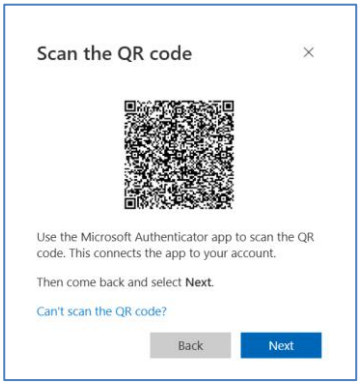
- Click Next in the **BROWSER ON PC**.



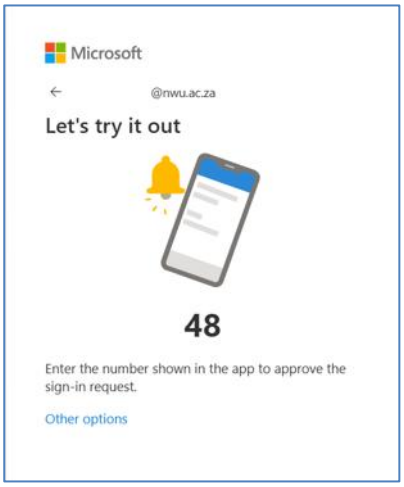
- Switch to the **DEVICE/PHONE** - IN THE AUTHENTICATOR APP and if prompted, allow notifications.

  1. Click the + sign to add an account - select "Work or school account".
  2. Select Scan QR Code.

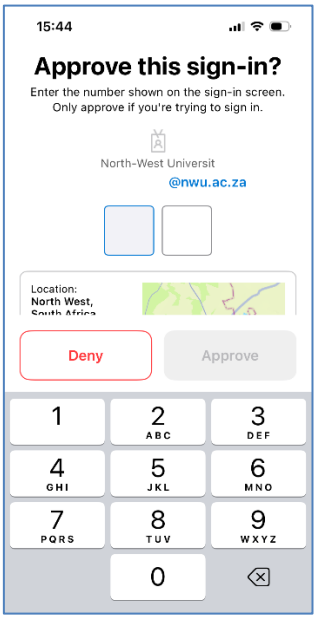
- In the **BROWSER ON PC**, click Next.



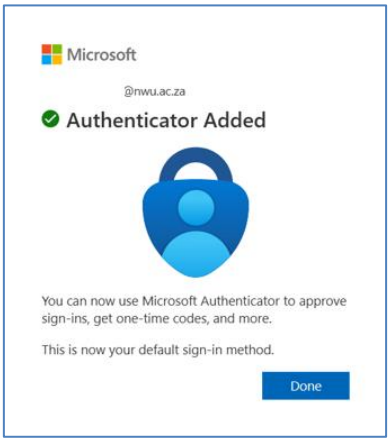
- Scan the QR code with your **DEVICE/PHONE,** then click Next in the **BROWSER ON PC**.



- Microsoft will send a code to the **DEVICE/PHONE**. Enter the code on your **DEVICE/PHONE,** then select **APPROVE.**



- You will receive a message in the **BROWSER ON PC** that the App was successfully added.



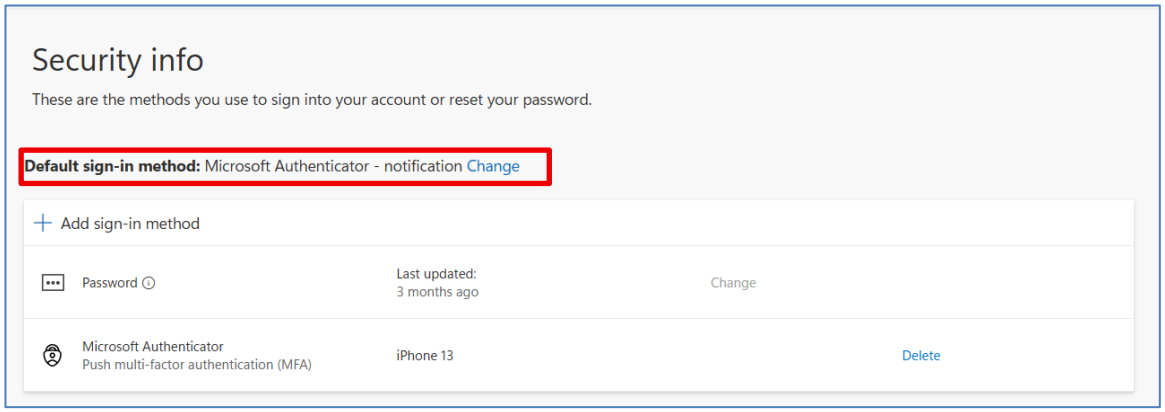
- Click Done. The setup of the Microsoft Authenticator App is complete.

5 Microsoft Authenticator App: Set TOTP as the Default Sign-in Method

You can change your default multifactor authentication to use the six-digit code displayed in the Microsoft Authenticator app. This code will change every 30 seconds.

Note: After adding Microsoft Authenticator, you may need to sign out and sign back in before you can change the **Default sign-in method** shown below.
Open: https://mysignins.microsoft.com/security-info

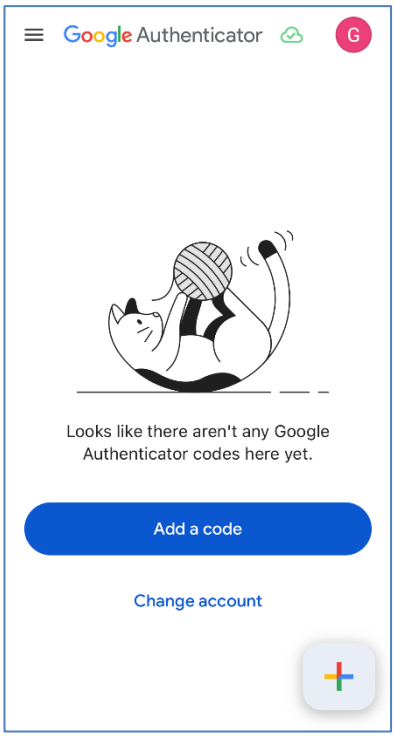
- Select **Change** next to **Default sign-in method**.



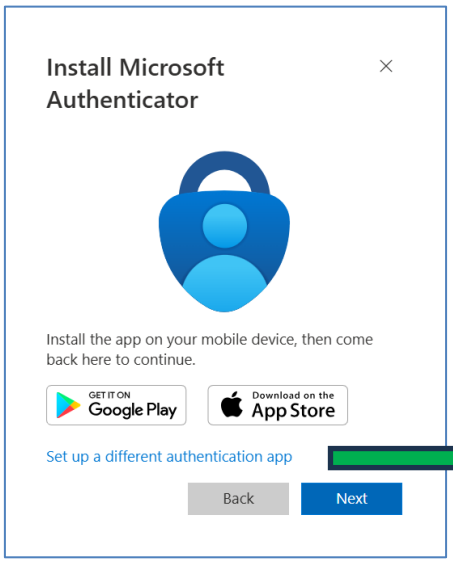
- Choose: **Authenticator App or Hardware Token - Code**
- Select **Confirm**.
- Save the change.
- The default authentication method will now be TOTP verification codes instead of push notifications.
- When you changed the Default sign-in method to the Microsoft Authenticator app, the Phone method can be deleted.
- 

6 Set up the Google Authenticator as your multifactor authentication method

- From the **DEVICE/PHONE**: Download and install the Google Authenticator app from the Google Play Store or Apple App Store.
- Open the Google Authenticator app on the **DEVICE/PHONE.**
- On the **DEVICE/PHONE**: Select Add a code



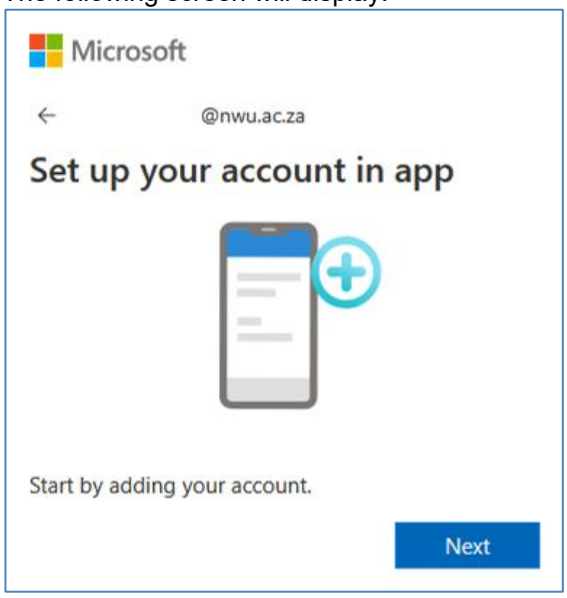
- When you reach this screen in a **BROWSER ON PC**, either while setting up multifactor authentication for the first time or adding this as an alternative to SMS (https://mysignins.microsoft.com/security-info), follow the steps below.



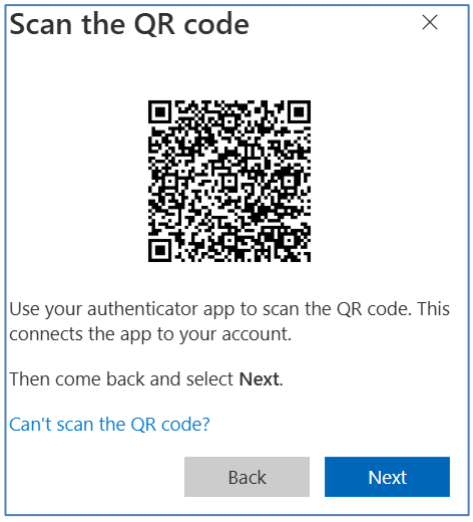
Select this option if you prefer to use an authenticator app other than Microsoft Authenticator.

- Select **SETUP A DIFFERENT AUTHENTICATION APP** and click on Next.

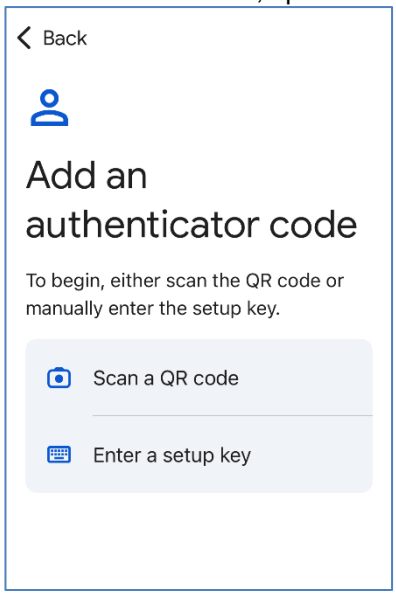
- The following screen will display:



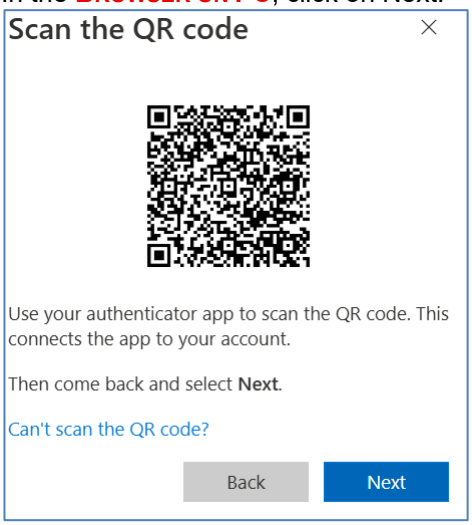
- Click Next
- In the **BROWSER ON PC**, the following screen will display:



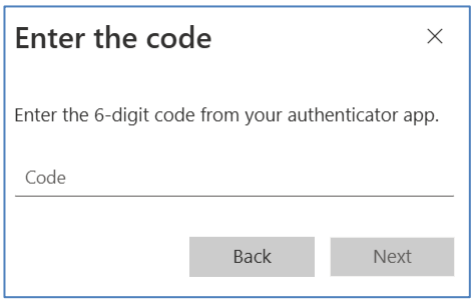
- ON THE **DEVICE/PHONE**, open the Google Authenticator app and select **SCAN A QR CODE**



- Scan the code with your **DEVICE/PHONE**.
- In the **BROWSER ON PC**, click on Next.



- Enter the 6-digit code in your **BROWSER ON PC** that will display in your Google Authenticator app and click on Next.



- You will receive a message in the browser that the App was successfully added

