

Set Up Multi-Factor Authentication (MFA)

To keep your account secure, Multi-Factor Authentication (MFA) is required for the SIA portal. MFA adds a layer of security (on top of a username and password) to help prevent unauthorized access and protect data. When you sign in for the first time, or when you are setting up MFA for the first time, you will need to have an authenticator app on your mobile device.

You can choose one of the following authenticator apps:

- Salesforce Authenticator
- Google Authenticator
- Microsoft Authenticator
- Authy

You'll need:

- A smartphone or tablet
- Access to the app store on your device
- Your username and password for the Commissioning Platform

Changing or replacing your MFA device

If you:

- Get a new phone
- Lose access to your authenticator app
- Want to change authenticator apps

Please email servicedesk@sia.govt.nz to reset your MFA.

Step 1: Sign in to the portal

- Go to the SIA portal login page.
- Enter your username and password.
- When prompted, select Set up MFA.
- A QR code should be displayed on screen.

Step 2: Choose and install an Authenticator App

Install one of the apps listed on the following pages on your mobile device before continuing.



Social Investment Agency
Toi Hau Tāngata



Set Up Multi-Factor Authentication (MFA)

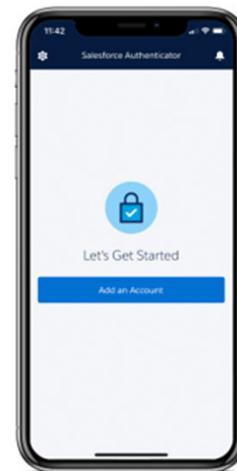
Option A: Salesforce Authenticator

Best for: Easiest setup and push notifications (no codes to type).

- Install **Salesforce Authenticator** from the App Store or Google Play.
- Open the app and tap **Add an Account**.
- Choose **Scan QR Code**.
- Scan the QR code shown on your computer screen.
- Confirm the account name shown in the app.

Signing in with Salesforce Authenticator

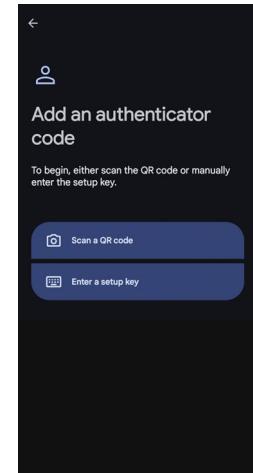
- When you log in, you'll receive a **push notification**.
- Open the app and tap **Approve**.



Option B: Google Authenticator

Best for: Simple, offline one-time passcodes.

- Install **Google Authenticator** from the App Store or Google Play.
- Open the app and tap **+**.
- Select **Scan QR Code**.
- Scan the QR code shown on your computer screen.
- A 6-digit code will appear in the app.



Signing in with Google Authenticator

- Enter the **6-digit code** shown in the app when prompted.
- Codes refresh every 30 seconds.



Set Up Multi-Factor Authentication (MFA)

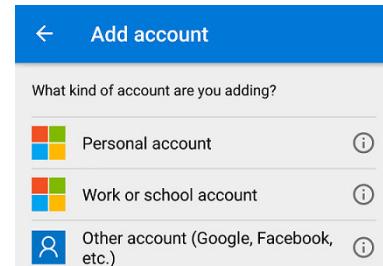
Option C: Microsoft Authenticator

Best for: Users already using Microsoft MFA for work accounts.

- Install **Microsoft Authenticator** from the App Store or Google Play.
- Open the app and tap **+**.
- Choose **Other account**.
- Scan the QR code shown on your computer screen.
- The account will be added to the app.

Signing in with Microsoft Authenticator

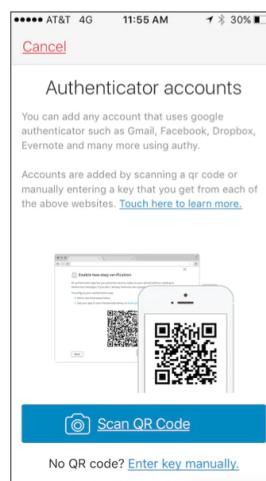
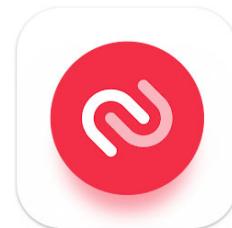
- Enter the **6-digit code** shown in the app when prompted.



Option D: Authy

Best for: Users who want cloud backup and multi-device support.

- Install **Authy** from the App Store or Google Play.
- Open Authy and register using your mobile number or email.
- Tap Add Account (or **+**).
- Select **Scan QR Code**.
- Scan the QR code shown on your computer screen.
- The account will appear in your Authy list.



Signing in with Authy

- Enter the **6-digit code** shown in the app when prompted.

