# Setting Up Google Authenticator

## Multi-factor Authentication

### Quick Reference Guide

## Overview

The process of logging into some AIG applications will now require a Multi-factor Authentication (MFA). This means that each time a user logs in, the login is required to be verified through a secondary means of verification (mobile application, SMS, or phone call).

**NOTE:** For questions relating to the multifactor authentication roll-out, including privacy related questions, review the FAQ.

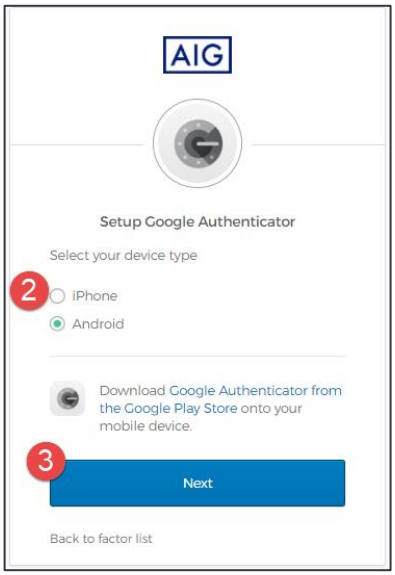
**NOTE:** Click here for additional information about the Google Authenticator application, including regarding personal information collected by Google Authenticator. Google Authenticator is a third-party application, and AIG does not manage or have access to any personal information that may be collected by the Google Authenticator application.

## Setup Google Authenticator

Google Authenticator provides a code on the user's mobile device (corporate or personal) that is then entered into the login authenticator on the computer to verify the login.

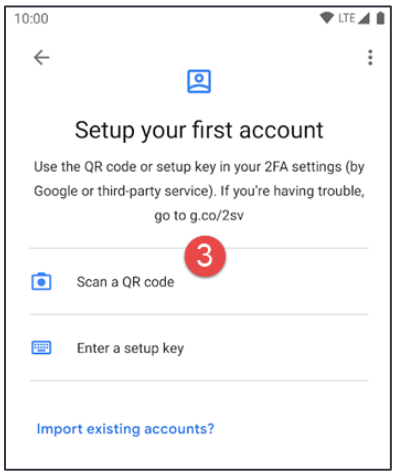
To set up Google Authenticator:

1. Click the **Setup** button in the **Google Authenticator** option.
2. Click the **iPhone** or **Android** radio button to set up the appropriate device type.
3. Click the **Next** button.

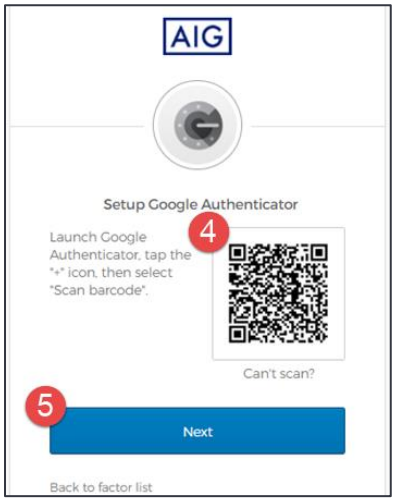



To set up **Google Authenticator** on mobile device:

1. Install Okta Verify by clicking on the links below.
   - iOS
   - Android
2. Launch **Google Authenticator** on the mobile device.
3. Select **Scan a QR code**. The QR code scanner opens.




4. Use the mobile device to scan the **QR code** on the computer screen. The account will be added to Google Authenticator.
5. Click the **Next** button on the **Setup Google Authenticator** screen.




6. Enter the six-digit code provided in Google Authenticator into the **Enter Code** field on the **Setup Google Authenticator** screen.
7. Click the **Verify** button. Google Authenticator will display in the **Enrolled factors** list.