THE UNIVERSITY of ADELAIDE

INFORMATION TECHNOLOGY AND DIGITAL SERVICES

Multi-Factor Authentication – Okta

Introduction

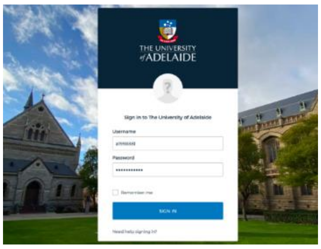
To help maintain the security of our systems and data at The University of Adelaide you will be required to sign in using two authentication modes. One is using your university ‘a’ number and password. The other is using a Multi-Factor Authentication (MFA) tool called Okta.

The steps below will walk you through the process to register and sign in using OKTA for the first time and how to add or modify your Okta authentication modes.

Signing in with Okta for the first time

When you attempt to sign in to an application protected by Okta, you will be redirected to Okta to register or authenticate

- Log in to Okta with your ‘a’ number (example – a1234567) as your **Username** and use your existing University of Adelaide **Password**



THE UNIVERSITY of ADELAIDE

Sign in to The University of Adelaide

Username

[illegible]

Password

••••••••••••

□ Remember me

SIGN IN

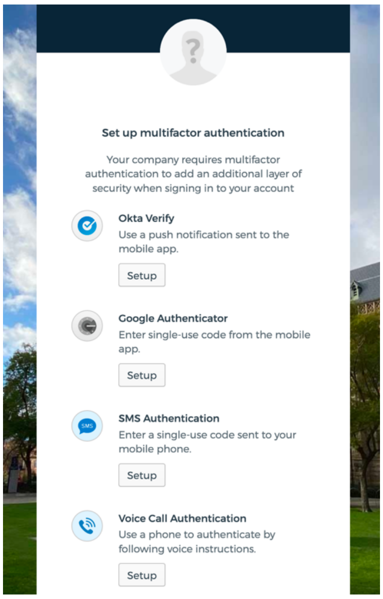
Need help signing in?

Setting up your Authentication methods

The simplest way to use MFA is to use **Okta Verify** by downloading the Okta Verify app on your mobile device. Below you will find the other supported methods of authentication through Okta.

To set up your authentication options, click the ‘**Setup’** button for your preferred options.

- **Okta Verify**
  For this option you will need to download the Okta Verify app on your mobile device. The app looks like this: ✓
- **Google Authenticator**
  Okta supports Goggle Authenticator. When you open the app on your mobile device, you will receive a code that generally lasts for around 30 second and then changes. The app looks like this G
- **SMS Authentication**
  For this option you’ll need to enter your mobile phone number and ensure you have your phone to receive the SMS code. The code is what you will type into Okta to gain access to the secured systems. There is a 5 minute expiry on the SMS code
- **Voice Call Authentication**
  For this option, when a code is required you will receive a call with a voice telling you the code to type in. You may use your mobile or landline number



Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your account

Okta Verify
Use a push notification sent to the mobile app.
Setup

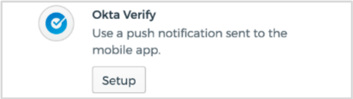
Google Authenticator
Enter single-use code from the mobile app.
Setup

SMS Authentication
Enter a single-use code sent to your mobile phone.
Setup

Voice Call Authentication
Use a phone to authenticate by following voice instructions.
Setup

Setting up Okta Verify as your MFA Factor

1. Click **Setup** under the Okta Verify option

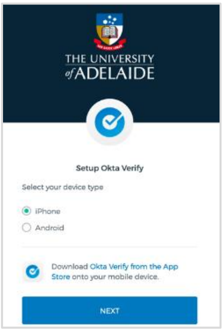


Okta Verify

Use a push notification sent to the mobile app.

Setup

2. Select your device type from either **iPhone** or **Android**



THE UNIVERSITY of ADELAIDE

Setup Okta Verify

Select your device type

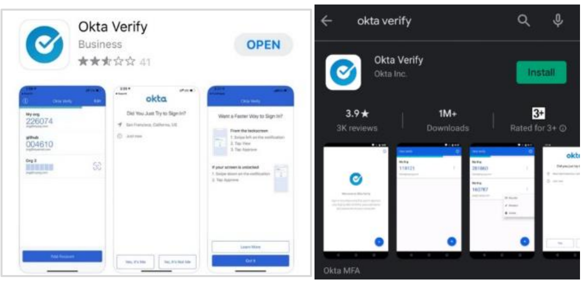
● iPhone

○ Android

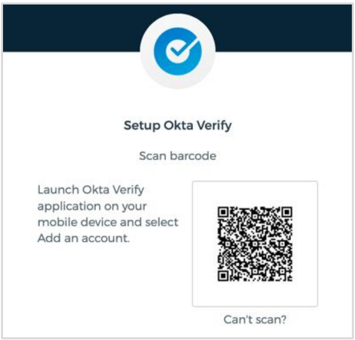
Download Okta Verify from the App Store onto your mobile device.

NEXT

3. Download the app on your mobile device before you click Next



4. Once downloaded and installed open the **Okta Verify** app to your mobile device
5. Back in your browser, click **next**
6. Use the Okta Verify app on your mobile device to scan the QR code



Setup Okta Verify

Scan barcode

Launch Okta Verify application on your mobile device and select Add an account.

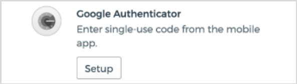
Can't scan?

You are now enrolled with **Okta Verify** as an MFA factor. You can enrol in another MFA factor or click **Finish** to continue

INFORMATION TECHNOLOGY AND DIGITAL SERVICES

Setting Google Authenticator as your MFA Factor

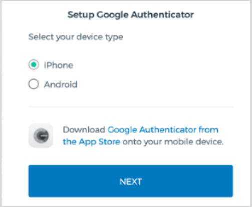
1. Click **Setup** under the Google Authenticator option



Google Authenticator

Enter single-use code from the mobile app.

2. Select your device type from either **iPhone** or **Android**



Setup Google Authenticator

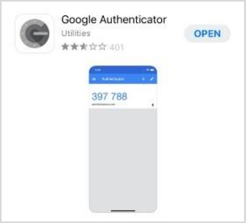
Select your device type

● iPhone

○ Android

Download Google Authenticator from the App Store onto your mobile device.

3. Don't click Next until you have downloaded the App
4. Download the **Google Authenticator** app to your device



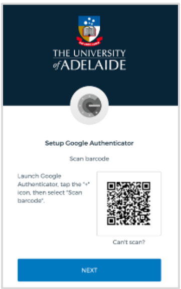
Google Authenticator

Utilities

★★★☆☆ 401

397 788

5. Once installed, click **next** on your browser
6. Use the Google Authenticator app to scan the QR code. *You may need to open your mobile devices camera and point it at the QR code.*
7. Click **Next** when done

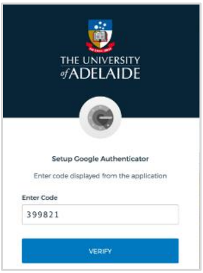


Setup Google Authenticator

Scan barcode

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

8. Enter the code from Google Authenticator and click **Verify**



Setup Google Authenticator

Enter code displayed from the application

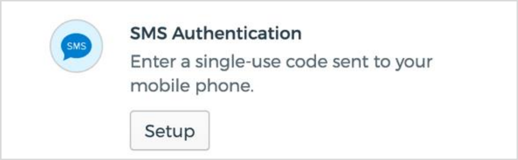
Enter Code

399821

9. You are now enrolled with **Google Authenticator** as an MFA factor.
10. You can enrol in another MFA factor or click **Finish** to continue

Setting up SMS as your MFA Factor

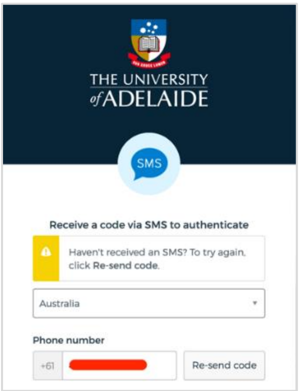
1. Click **Setup** under SMS Authentication



SMS Authentication

Enter a single-use code sent to your mobile phone.

2. Select country as **Australia** (unless you have an overseas number)
3. Enter your mobile **phone number**
4. Click **Send Code**. *If you do not use the code within 5 minutes, but still need to access the system, you can receive a new code by clicking Re-send code*



THE UNIVERSITY of ADELAIDE

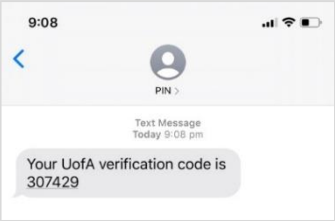
Receive a code via SMS to authenticate

Haven't received an SMS? To try again, click Re-send code.

Australia

Phone number: +61 [redacted]

5. You will receive a **One Time PIN** to your mobile number



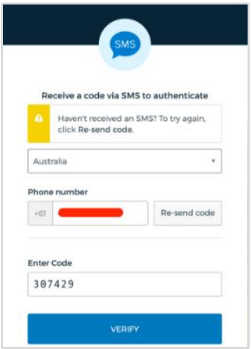
9:08

PIN >

Text Message
Today 9:08 pm

Your UofA verification code is 307429

6. Type the code you received in your SMS in the box labelled **Enter Code** and click **Verify** as your second authentication to access the system



Receive a code via SMS to authenticate

Haven't received an SMS? To try again, click Re-send code.

Australia

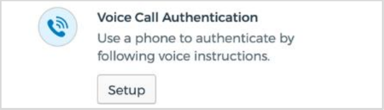
Phone number: +61 [redacted]

Enter Code: 307429

7. You are now enrolled with **SMS Authentication** as an MFA factor.
8. You can enrol in another MFA factor or click **Finish** to continue

Setting Voice Call as your MFA Factor

1. Click **Setup** under the Voice Call Authentication option

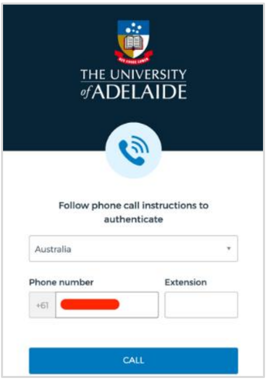


Voice Call Authentication

Use a phone to authenticate by following voice instructions.

Setup

2. Select the **Country Name Australia** and enter your mobile **Phone Number** followed by clicking **Call.** If you prefer not to use your mobile, you can also enter a landline phone number



THE UNIVERSITY of ADELAIDE

Follow phone call instructions to authenticate

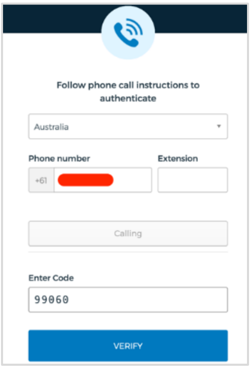
Australia

Phone number: +61 [redacted]

Extension:

CALL

3. You will receive a phone call that will speak your code. *Note: It is likely that the number that calls you will be a +1 number from the US*
4. Enter the One Time PIN in the box labelled **Enter Code** and click **Verify**



Follow phone call instructions to authenticate

Australia

Phone number: +61 [redacted]

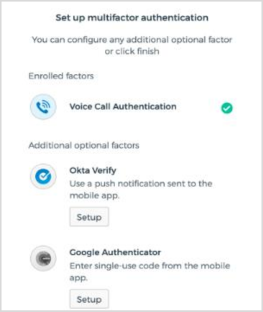
Extension:

Calling

Enter Code: 99060

VERIFY

5. You are now enrolled with **Voice Call Authentication** as an MFA factor.
6. You can enrol in another MFA factor or click **Finish** to continue



Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

Voice Call Authentication ✓

Additional optional factors

Okta Verify

Use a push notification sent to the mobile app.

Setup

Google Authenticator

Enter single-use code from the mobile app.

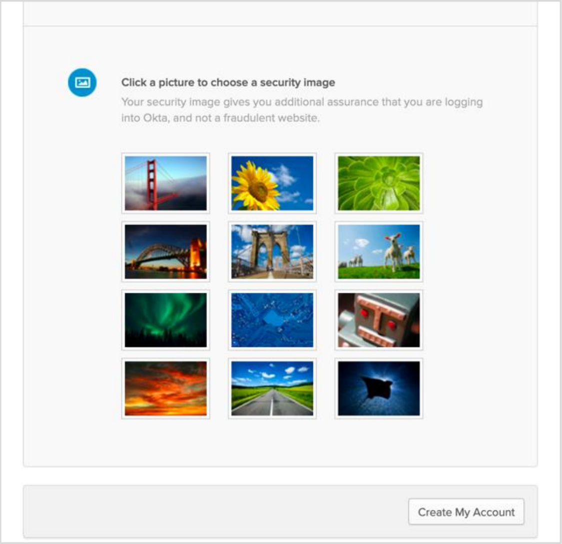
Setup

Final step to set up MFA

After you have set up your MFA, you will be asked to select a security image.

This image will be displayed the next time you sign in with Okta to confirm that you’re signing in at the correct website.

Click on an image and click **Create My Account**



Click a picture to choose a security image

Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website.

Once you have registered at least one authentication mode and selected your security image, you will be signed in and redirected back to the system you were trying to sign into

In future sign ins, you will be asked to use your University username and password as well as your enrolled MFA to authenticate.

Contact Us

For further support or questions, please contact the ITDS Service Desk on +61 8 8313 3000 or servicedesk@adelaide.edu.au