

DPAU Account Activation Guides

DPAU Analysis Environment is hosted on Monash Secure eResearch Platform (Monash SeRP). To access the DPAU Analysis Environment, the first step is to create and activate your Monash account. Upon approval of your application, DPAU will submit an account creation request on your behalf, and you will receive an email notifying you when the account has been created. Information required to create your account including: First Name, Last Name, Role, Email, Mobile Number and Institution.

The account activation steps are outlined below, with screenshots.

Troubleshooting

If you experience any troubles accessing the SeRP Analysis Environment your account, please contact Monash SeRP support on safehavens@monash.edu. For any other questions and/or issues, please contact DPAU on dpau@unsw.edu.au.

Account Activation Link

Once you receive your activation link by email, click the link to start the activation process.

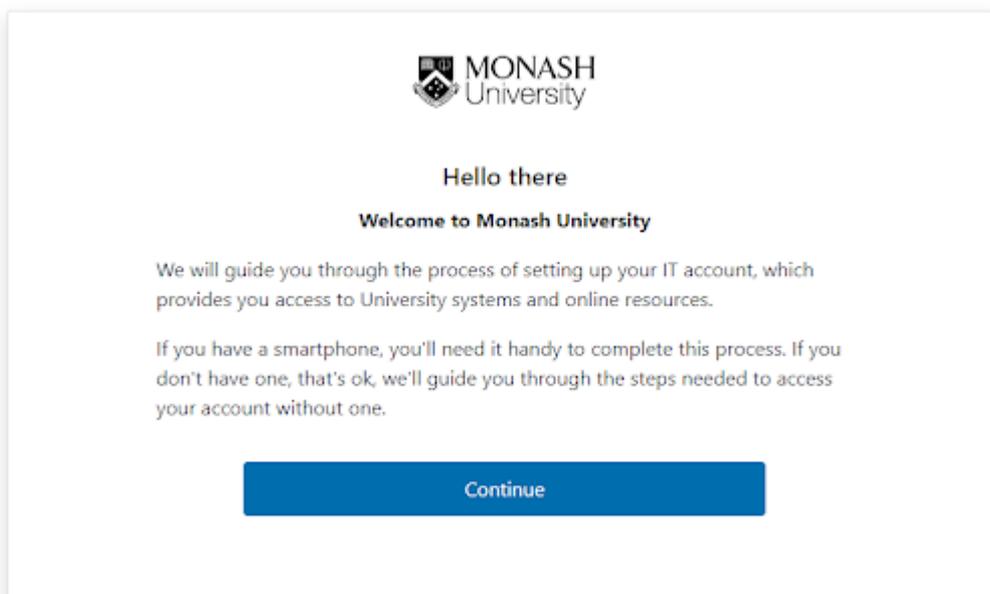
The system will step you through the activation process and help you set up multi-factor authentication (MFA). We highly recommend you also take up the self-service options for backup codes and password reset - this can save you a lot of time if you forget your password or lose your phone.

The activation process is best done using a computer. If this isn't an option, you can still activate your account on your smartphone, however this involves a few extra steps.

If the account activation link expired, please visit the Monash University Identity Management Services 'I've forgotten my password' page (<https://identity.monash.edu/sspr>). Please enter your details (assigned email address, eg. ext-jsmith@monash.edu and last three digits of the mobile number you provided) this method will trigger a recovery code to be sent to your mobile phone, you will then be able to create a new password or access the account.

Steps to Activate Your Account

1. Click the activation link in your email. You'll see a welcome screen.





2. Read and agree to the terms and conditions.



Acceptable Use Policy

The use of Monash University systems is subject to the terms and conditions set out in the [IT Acceptable Use Policy](#).

I accept the terms and conditions of the IT Acceptable Use Policy

[Continue](#)

[Back](#)

3. Opt into Google Additional Services (if you want to).



Opt in for Google's Additional Services

Monash University uses Google's 'G Suite' products for email and collaboration. As part of setting up your account, you automatically get access to Gmail, Calendar, Google Docs, Google Drive, Google Sites, and Google chat.

If you would like to access Google's Additional Services with your University account, such as YouTube and Blogger, you must read and personally agree to Google's [Terms of Service](#) and [Privacy Policy](#). Please note, that breaching Google's Terms of Service may result in your loss of access to all Google G Suite services.

If you don't want to opt in now, you can do it later.

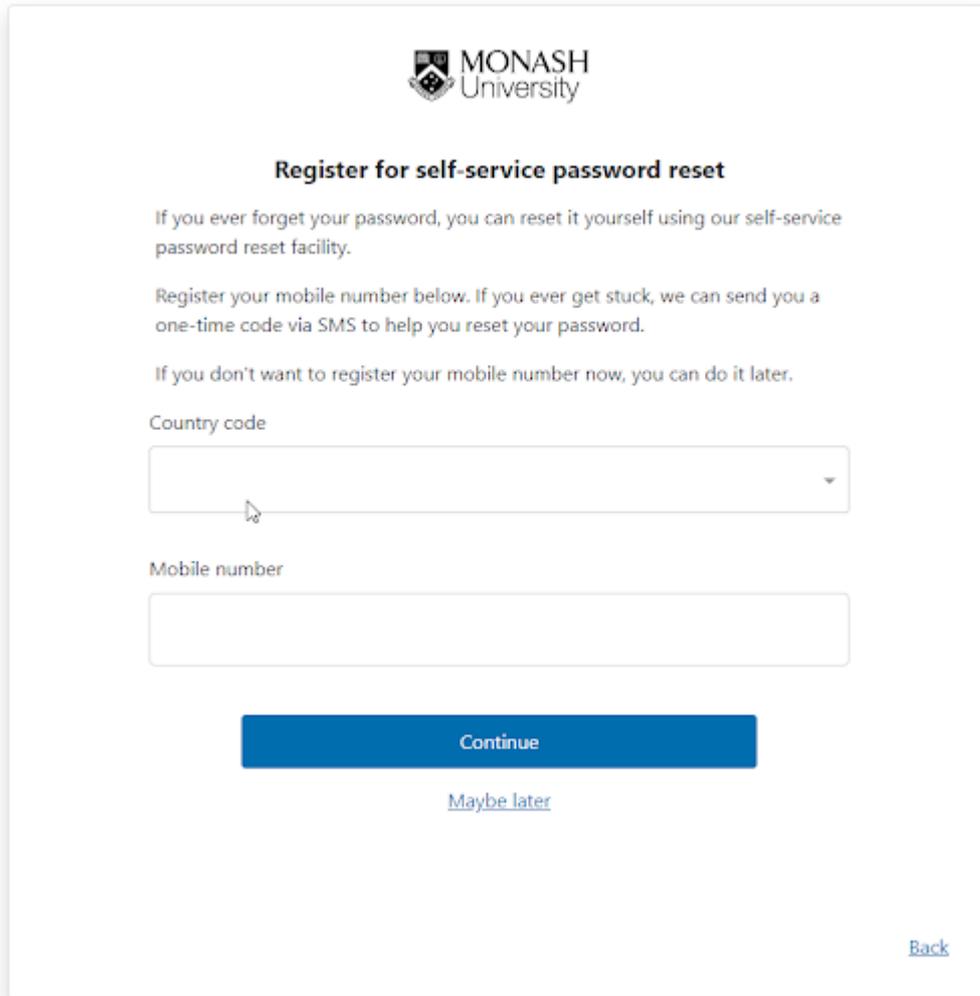
I do not want to use Google's Additional Services with my University account

I want to use Google's Additional Services with my University account. I have read and accept Google's [Terms of Service](#) and [Privacy Policy](#)

[Continue](#)

[Back](#)

4. Register your mobile number for self-service password reset (**highly recommended**).



The screenshot shows a web page for Monash University titled "Register for self-service password reset". It includes the Monash University logo at the top. The main heading is "Register for self-service password reset". Below this, there are three paragraphs of text: "If you ever forget your password, you can reset it yourself using our self-service password reset facility.", "Register your mobile number below. If you ever get stuck, we can send you a one-time code via SMS to help you reset your password.", and "If you don't want to register your mobile number now, you can do it later." There are two input fields: "Country code" (a dropdown menu) and "Mobile number" (a text box). Below the input fields is a blue "Continue" button and a link labeled "Maybe later". At the bottom right, there is a "Back" link.

5. Set a password.

Note:

- We require a strong password for security reasons. For guidance on creating a strong password, see article <https://mon.clients.squiz.net/esolutions-site/accounts-passwords/strong-passwords>.
- We recommend the use of password generator.



Set a password

Password Requirements

- Passwords that are 13 characters or longer only require lower case letters
- Passwords must contain at least 8 characters
- Passwords between 8 and 13 characters require at least 3 of the following 4 categories of characters:
 - Uppercase letters
 - Lowercase letters
 - Numbers
 - Symbols
- Your new password can't be one of the last 24 passwords you have used
- Passwords must not contain your username or any part of your name
- You have to wait 24 hours after changing your password to be able to change it again
- **All passwords are checked against a database of over 1 billion stolen passwords. If you try and use a password that is found in this database, it will be rejected.**

Password

Confirm password

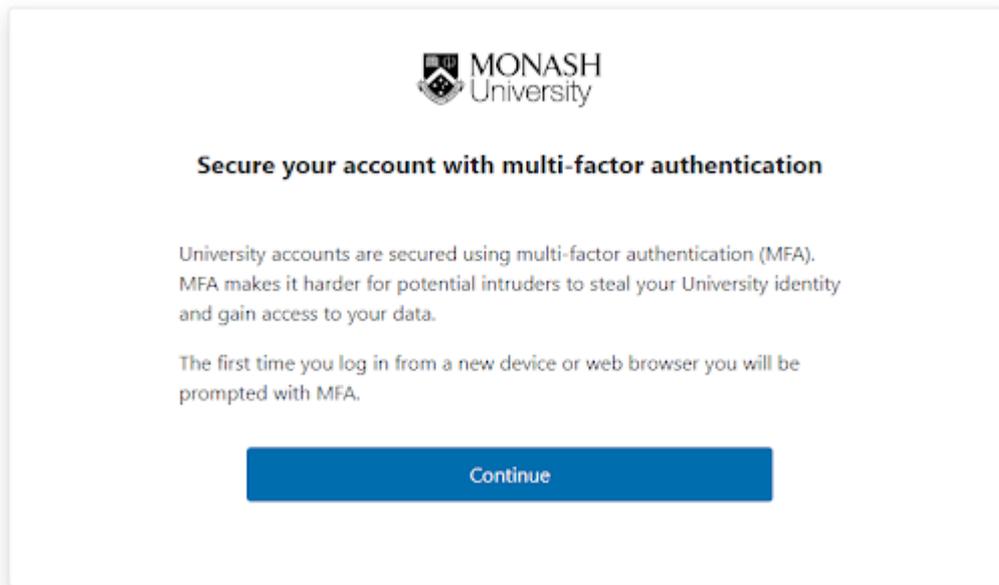
[Continue](#)

[Get Help](#)

[Back](#)



6. Secure your Monash account with multi-factor authentication (MFA).



If you have a smartphone, you can use either the Okta Verify app (**recommended**) or Google Authenticator for MFA. If you don't have a smartphone, or don't wish to use your smartphone for MFA, you can request a USB device (YubiKey or a U2F). You can also use your own U2F security key.

For further information on Multi-Factor Authentication, see <https://mon.clients.squiz.net/esolutions-site/accounts-passwords/multi-factor-authentication>

	RECOMMENDED		
	Okta Verify app	Google Authenticator app	YubiKey (USB device)
What's required	<ul style="list-style-type: none"> Okta Verify app on a phone or tablet Apple: iOS 11 or higher Android 4.4 or higher 	<ul style="list-style-type: none"> Google Authenticator or other compatible authenticator app on a phone or tablet Apple: iOS 7.0 or higher Android: 2.3.3 or higher 	<ul style="list-style-type: none"> A USB security key provided by Monash A laptop or computer with a USB port
How it works	Accept a push notification in the app or Type in a six-digit code generated by the app when offline	Type in a six-digit code generated by the app	Plug in the YubiKey to a USB port and press the button on it
Supports push notifications	Yes	No	No
Mobile device compatible	Yes	Yes	No
Available offline	Yes	Yes	Yes
Works with VPN	Yes	Yes	Yes
Can be installed on more than one device	No (but Google Authenticator can be used as a backup factor)	Yes	N/A



- a. Install the Okta Verify app on your smartphone.



Install Okta Verify app

Before you can register for multi-factor authentication, you need to install **Okta Verify app** on your smartphone.

Once registered, Okta Verify will send you a convenient push notification when you sign in from a new device. You can simply tap the notification to approve your login.

Choose your smartphone type

Apple

Google / Android

[Continue](#)

[I already have Okta Verify](#)

[I can't install Okta Verify](#)

[I don't have a smartphone](#)

[Back](#)



Install Okta Verify app

Install Okta Verify app on your smartphone. We can send the app download link to your mobile number. **** * 953. [Send it to a different mobile number](#)

Alternatively, you can search for "Okta Verify" in your app store and install it manually.

[Send me the link](#)

[I have installed Okta Verify](#)

[I can't install Okta Verify](#)

[Back](#)



- b. Scan the barcode. (if the QR code fails, see [here](#))



Scan barcode with Okta Verify app

Open Okta Verify app on your smartphone and select Add Account.



Scan the barcode using Okta Verify app and wait.

[I can't scan the barcode](#)

[Back](#)

7. Store a copy of your backup codes (highly recommended).



Backup codes

These are your backup codes. Each code can only be used a single time. As you use them, take note of which codes have been used.

Backup codes
8995-6817-2561
9061-2568-6441
8139-2922-3263
5002-6212-9175
7660-3663-3356

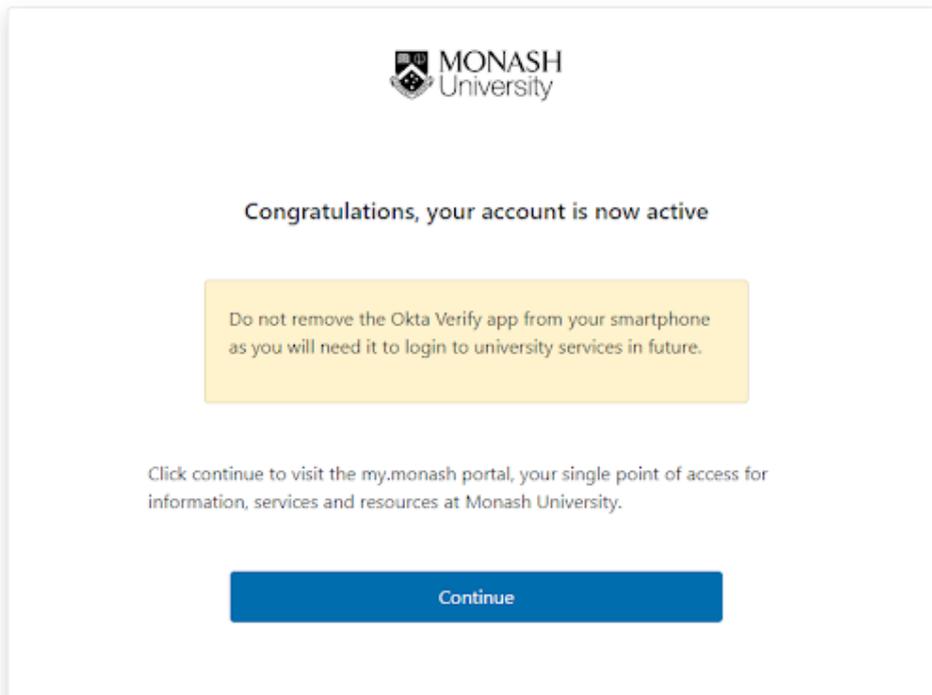
Once you leave this page, these codes cannot be shown again. Store these safely using the options below.

[Email](#) [Download](#) [Print](#)

[Done](#)



8. You have now finished activating your account.

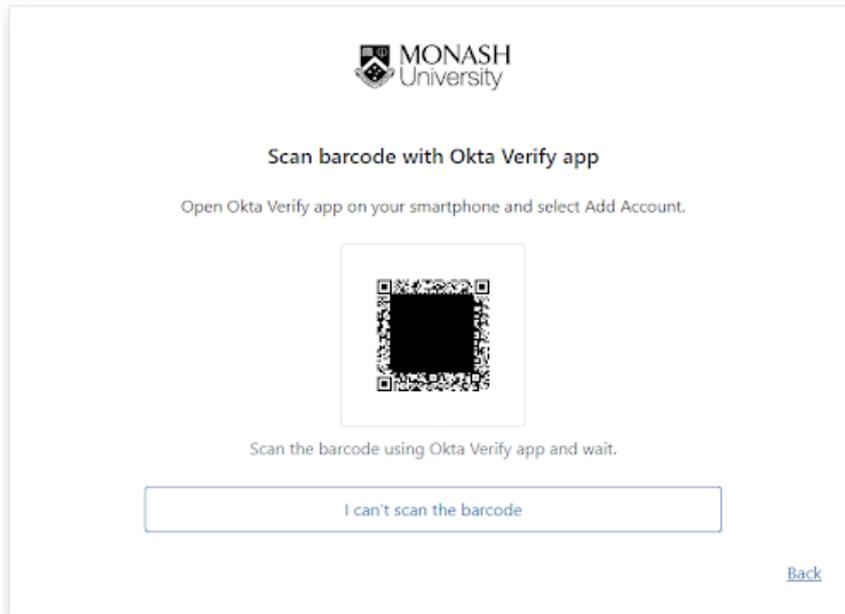


9. **Do not remove the Okta Verify app from your smartphone - you need this to log into the DPAU Analysis Environment.**
10. After successful activation, if you select “continue”, a login screen will appear. It is not necessary to login at this point, as DPAU Analysis is accessed from a Virtual Private Network (VPN) and a secure portal, and these steps are outlined [here](#). However, if you wish to view your Monash account and access your Monash email, use your Monash ID, e.g. ext-jsmith or the full email address, eg. ext-jsmith@monash.edu as required.

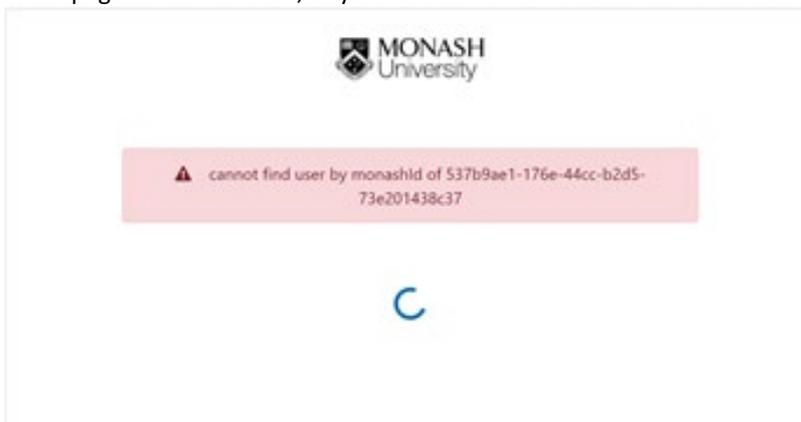


FAQ: What should I do if the QR code fails?

- If the QR code fails, there is an option to select "I can't scan the barcode" which should then provide a manual option to add the account to Okta.



- If this page was not loaded, or you could not select the "I can't scan the barcode" option



- If you can remember the password you used when initially attempting to create the account, please visit [my.monash](https://my.monash.edu) and enter your Monash email (ext-xxxx@monash.edu) and password. You will then be prompted to configure Multi Factor Authentication again and prompted to Install Okta Verify app. If you prefer, you can select 'I can't install Okta Verify' and you will be given the option to use Google Authenticator app instead. <https://www.monash.edu/esolutions/accounts-passwords/multi-factor-authentication>
- If you cannot remember the password you used, you will need to create a new password, please use the Monash University [Identity Management Services](#) website and follow the link to 'I've forgotten my password'. Please enter your Monash email (ext-xxxx@monash.edu). This method will trigger a recovery code to be sent to your mobile phone, allowing you to proceed with creating a new password and MFA setup.