Frequently Asked Questions: GOView Multi-Factor Authentication

How do I set up multi-factor authentication on my GOView account?

1. Download an authenticator app via the app store on your preferred mobile or tablet device. **Microsoft Authenticator** or **Google Authenticator** are recommended.

2. **Login** to GOView on your work computer or laptop using your username (work email address) and password.

3. **Scan the QR code** that appears on your work computer or laptop using your authenticator app. Enter the **6-digit numerical code** in the **Verification Code** field that appears under the QR code and click **Verify**. Multi-factor authentication will now be set up. Please note, you will only need to scan the QR code **once**: for subsequent log-ins you will only need to enter in a verification code number from your GOView account in your Authenticator app.

4. **Each time you need to login to GOView,** enter your username and password and the verification code field will appear. Open the authenticator app on your mobile/tablet device to generate the 6-digit verification code and enter in this code in the verification code field and click "Verify".

When will I need to set up multi-factor authentication on my GOView account?

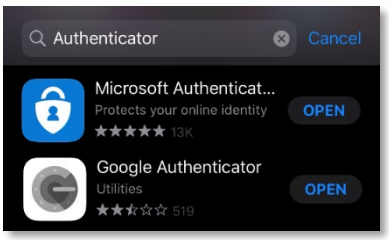
Existing GOView users will be required to set up multi-factor authentication by scanning a QR code that appears when logging into GOView for the first time from **Friday, 16 April 2021.**

New GOView users will be required to set up multi-factor authentication by scanning a QR code that appears when logging into GOView for the first time after access is approved.

How do I download an authenticator app on an iOS device?

1. On your iOS device, search for and open the 'App Store' app and search '**Authenticator**'.

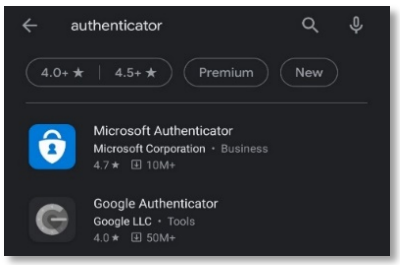
2. Download **Google Authenticator** or **Microsoft Authenticator**.



How do I download an authenticator app on an Android device?

1. On your android device, search for and open the 'Play Store' app and search '**Authenticator**'.

2. Download **Google Authenticator** or **Microsoft Authenticator**.



How often will I be required to complete multi-factor authentication?

Each time you need to login to GOView, you will need to generate the 6-digit verification code from your authenticator app on your mobile/tablet device. Enter your username and password and the verification code to login to GOView on your work laptop or computer.

FAQs:
GOView Multi-Factor Authentication

Do I need to scan the QR code each time I log in to GOView?

No – you will only need to scan the QR code **once** when you set up multi-factor authentication for your GOView account. After that, you will just be required to open up the relevant authenticator app and enter the 6-digit numerical code in addition to your username and password.

I wasn't prompted to scan a QR code and I'm unable to set up multi-factor authentication/log in to GOView – what should I do?

Please contact the DPC Appointments, Boards and Committees team for assistance at boards@dpc.nsw.gov.au or 02 9228 5454.

Do I enter a space in the middle of the 6-digit numerical code?

No – you will need to enter the 6-digit numerical code **without spaces** in order for it to be entered successfully.

Can I set up multi-factor authentication on multiple mobile devices?

No – you are only able to set up multi-factor authentication for your GOView account on one device.

My QR code isn't scanning – what should I do?

If you're having problems scanning the QR code, try out the following tips:

- Brighten the screen of your work computer/laptop
- Make sure you're not tilting your camera – ensure your mobile device is level with your computer screen when scanning the QR code
- Try changing the distance between your mobile device/camera and the QR code

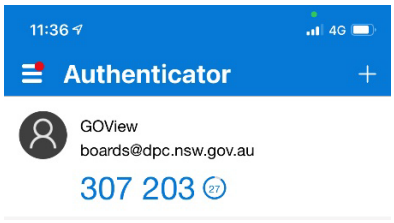
Will my 6-digit numerical verification code be the same every time I log in?

No - your unique 6-digit numerical verification code will refresh every **30 seconds** – make sure your code is still on screen when you enter it.

I already have an account for eCabinet in my Authenticator app – can I use the same verification code?

No – you will need to set up a separate GOView account in your Authenticator app. Your GOView account will be clearly labelled as such:

FAQs:
GOView Multi-Factor Authentication



If my screen is inactive for a long period, will I be automatically logged out of the GOView system?

Yes, session timeout in GOView occurs after two hours of 'inactivity'. Activity includes clicking buttons or links, navigating to different screens / pages, and entering text in text fields. Once you have been logged out, you will be required to open up the relevant authenticator app and enter the 6-digit numerical code in addition to your username and password to log in in the usual way.

I've lost the mobile device which my multi-factor authentication for GOView is registered to – what should I do?

You will be required to set up multi-factor authentication on a new device. Please contact the Appointments, Boards and Committees team at boards@dpc.nsw.gov.au or 02 9228 5454 to reset your account.

I need to access GOView but I've left the mobile device which my multi-factor authentication is registered with at home – what should I do?

Please contact the DPC Appointments, Boards and Committees team for assistance at boards@dpc.nsw.gov.au or 02 9228 5454.

How do I change the device I use to complete multi-factor authentication on GOView?

If you need to change the device you complete multi-factor authentication for GOView with, please contact the Appointments, Boards and Committees team at boards@dpc.nsw.gov.au or 02 9228 5454 to organise this.

What should I do if I delete my authenticator app?

Try re-downloading your authenticator app and check whether authentication for your GOView account is still linked. If GOView authentication is no longer linked, you will need to set up multi-factor authentication again. Please contact the Appointments, Boards and Committees team at boards@dpc.nsw.gov.au or 02 9228 5454.

What should I do if I don't have a mobile device?

As required under the NSW Cyber Security Policy, mitigation strategies are being introduced across all NSW Government platforms to limit the extent of cyber security incidents. This includes **multi-factor authentication**, which is being introduced for all NSW Government platforms when users perform a privileged action or access an important (sensitive/high-availability) data repository.
Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

FAQs:
GOView Multi-Factor Authentication

If you do not own a mobile device, we suggest that you speak to your manager. For further information or for advice regarding the NSW Cyber Security Policy please contact cybersecuritypolicy@customerservice.nsw.gov.au.