Your Portal

Guide to Two-Factor Authentication

This guide will explain what two-factor authentication is and how you can enable it in Your Portal if you wish to.

What is two-factor authentication?

Two-factor authentication (2FA) is a two-step process for logging into online accounts. When 2FA is enabled, it means you have to enter more information than just a password to log into an online account. Many services now use 2FA to log into online accounts; for example, online banking and government services.

2FA adds an extra layer of security to help prevent unauthorized access to an online account. It is a very solid measure to have in place against common password attacks.

Can I enable 2FA in Your Portal?

It is possible to enable 2FA when you are logging into Your Portal. While this is not compulsory, at St Patrick's Mental Health Services (SPMHS), we recommend enabling 2FA in Your Portal.

If you enable 2FA in Your Portal, you will need to:

- download an authenticator app to your personal smartphone
- enter a code from the authenticator app to Your Portal every time you log in.

If you are already using an authenticator app for 2FA with other online services, you do not need to download another one. If you are downloading an authenticator app for the first time, there are many you can choose from; however, many people tend to use Microsoft Authenticator or Google Authenticator.

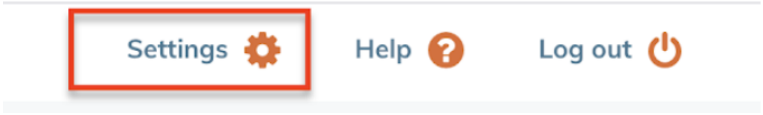
It is important that you only use an authenticator app on your personal smartphone, rather than one on any other person's device. You will receive a code to the authenticator app every time you log on to Your Portal, so you need access to your personal smartphone to get this.

There is usually a 30-second time limit on codes that are sent to the authenticator app. If you do not enter the code from the authenticator app to Your Portal within the time limit, you will need a new code to log on. You can prompt the authenticator app for a new code.

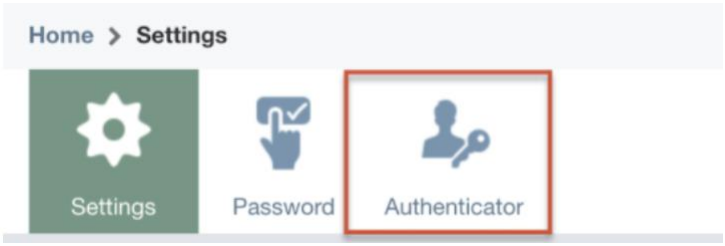
How can I set up 2FA in Your Portal?

To set up 2FA in Your Portal:

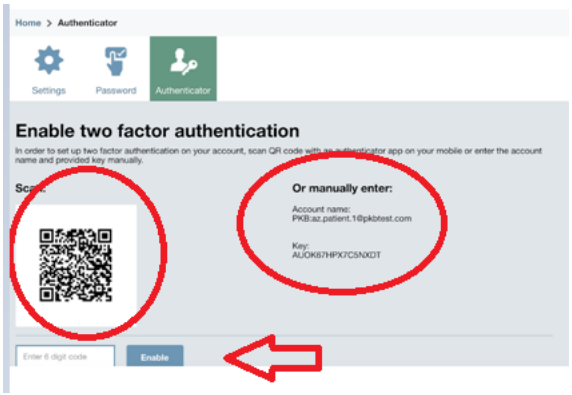
1. Log into Your Portal
2. Click ‘Settings’ at the top of the homepage



3. Click on the ‘Authenticator’ tab which appears; this will bring you to a new page with a QR code and text information

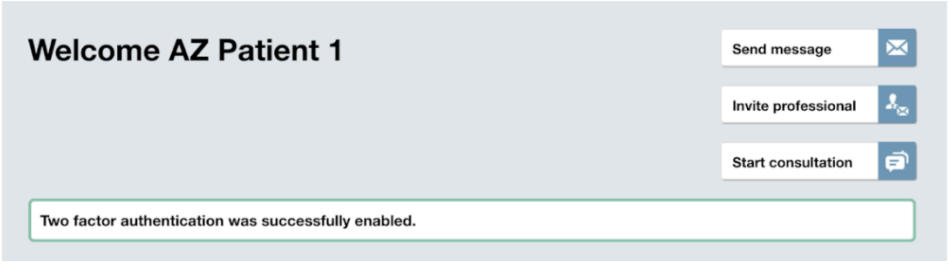


4. Open the authenticator app on your smartphone
5. Scan the QR code or manually enter the text information showing in Your Portal

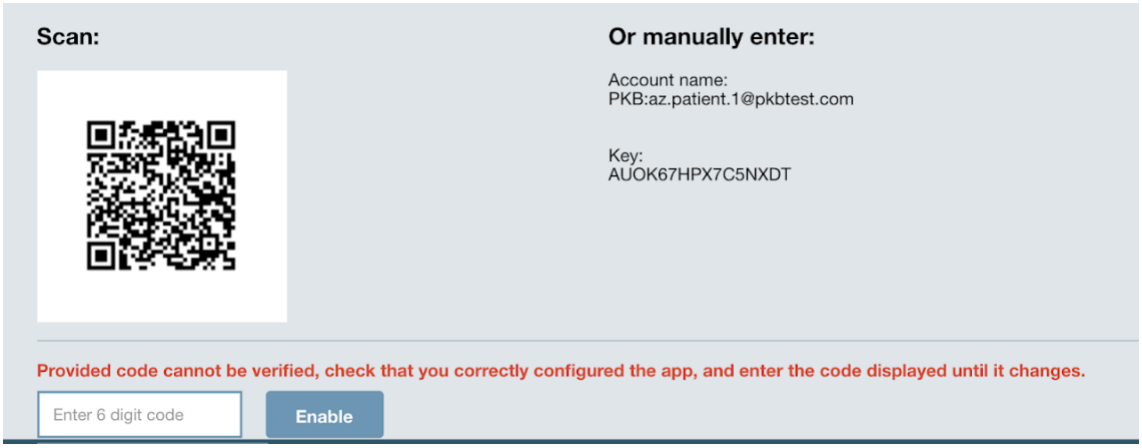


6. Add the code which displays on your smartphone to Your Portal
7. Click ‘Enable’.

If the code is correct, 2FA will be enabled. You will be returned to the homepage of Your Portal and see a ‘success’ message when you scroll down the page.



You will see an error message in Your Portal if the code was wrong or incomplete. Enter the code on your smartphone and click 'Enable' to try again.

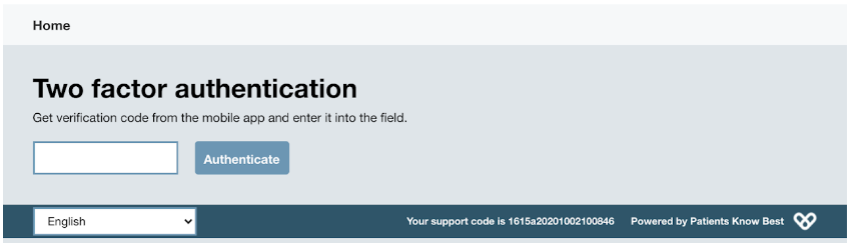


If you are logged into Your Portal to begin setting up 2FA but do not complete it straight away, please note that your session is timed out automatically after 30 minutes if you do not actively use the portal in that time. You will need to log in again and get a new code to complete setting up 2FA.

How do I log into Your Portal after 2FA has been set up?

Once 2FA is set up, any time you wish to log on to Your Portal, you will simply need to:

1. Go to the Your Portal log-in page
2. Enter your email address and password
3. Enter, when prompted, the code that shows on the authenticator app on your phone
4. Click 'Authenticate'.



The code which is sent to your authenticator app may have a 30-second time limit. If you do not enter the code into Your Portal within the time limit, you will need a new code. You can follow steps within the authenticator app to get a new code.

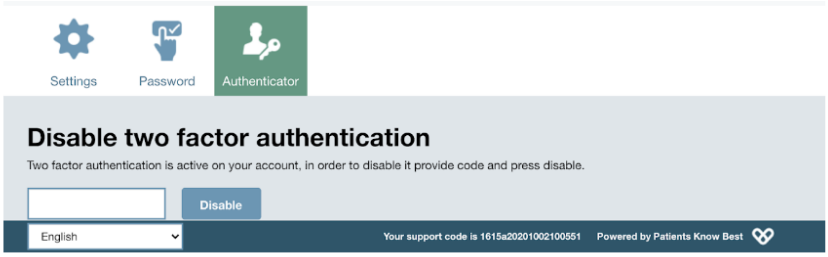
If you are logged into Your Portal, your session is timed out automatically after 30 minutes if you do not actively use it in that time. You will need to log in again and get a new code as part of this if you wish to continue the session.

Can I disable 2FA?

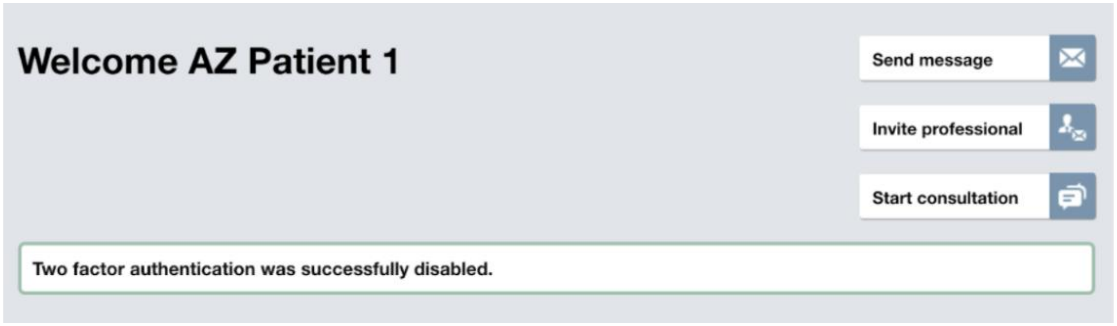
It is possible to disable 2FA in Your Portal after you have set it up.

To do this:

1. Log on to Your Portal
2. Go to 'Settings'
3. Click 'Authenticator'
4. Enter the code showing on the authenticator app on your smartphone
5. Click 'Disable' in Your Portal.



You will be returned to the Your Portal homepage after this and a message to confirm 2FA has been disabled will be seen when you scroll down the page.



Please note that, after you have disabled the 2FA in Your Portal, you must also remove the "Your Portal" account from your authenticator app.

You can set 2FA back up after you have disabled it, if you wish to do so. You can follow the steps in the "How can I set up 2FA in Your Portal?" section above to set 2FA back up.

Who do I contact for help?

If you have any issues or questions when using Your Portal, the Service User IT Support (SUITS) team here at SPMHS is here to help.

You can contact SUITS by calling 01 249 3629 or emailing suits@stpatricks.ie.

Please note that authenticator apps are third party apps. While SUITS can provide guidance, these apps are separate from Your Portal and other digital services provided by SPMHS. This means that:

- if you are preparing to change or delete your authenticator app for any reason, it's important that you always disable 2FA in Your Portal first, then remove the "Your Portal" account from your authenticator app before changing or deleting it
- in some cases, if you are having difficulties with 2FA, SUITS may need to reach out to the helpdesk in Patients Know Best (PKB), the portal provider, for support; this may be needed, for example, if you have lost your smartphone, or if you changed your smartphone and the authenticator app didn't transfer. PKB may then disable 2FA in Your Portal and you may need to follow the steps above to set it up again.