

Explorer Online Mobile User Guide

Overview

This article will cover the basic functionality of Medical-Objects Explorer Online Mobile. If you have any questions or require any further information, please contact the Helpdesk on (07) 5456 6000.

Medical-Objects Explorer Online is a web-based solution that allows you to send and receive patient documents from your own personal web browser on a mobile device.

Requirements

Explorer Online Mobile was designed to run on modern mobile devices running Android or iOS.

Please take note of the browser requirements below.

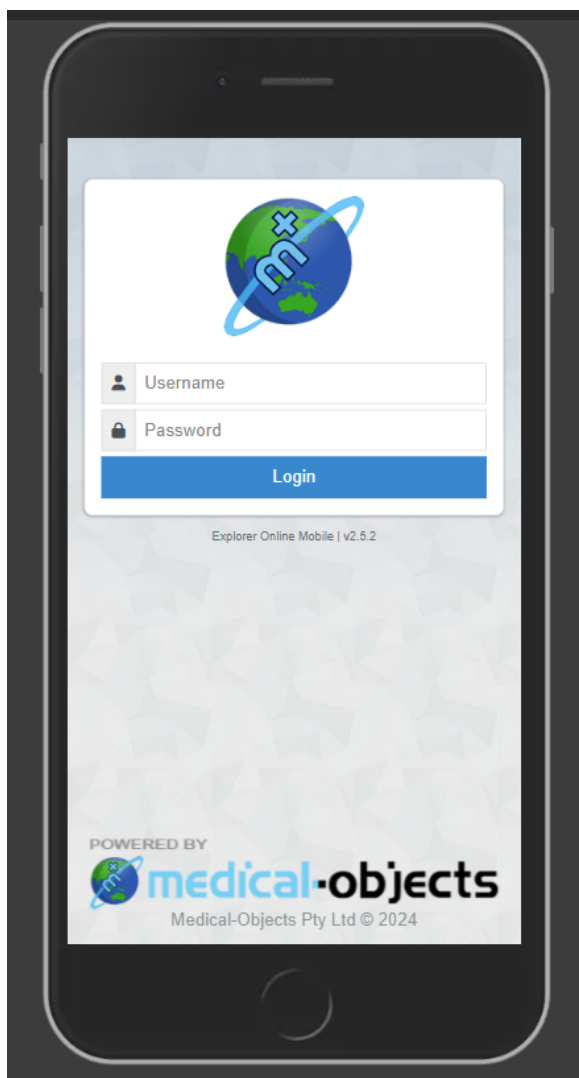
Supported Browsers

- Microsoft Edge
- Google Chrome
- Mozilla FireFox
- Opera
- Safari

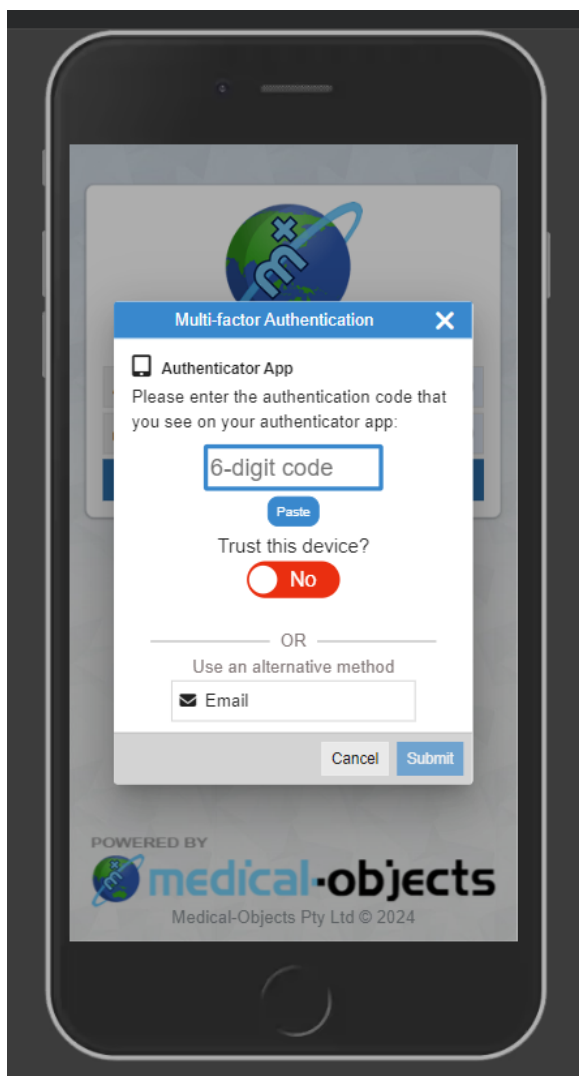
Logging in and out

When first loading Explorer Online Mobile, you will be presented with a login screen. Simply enter in your username and password and select **Login** to proceed.

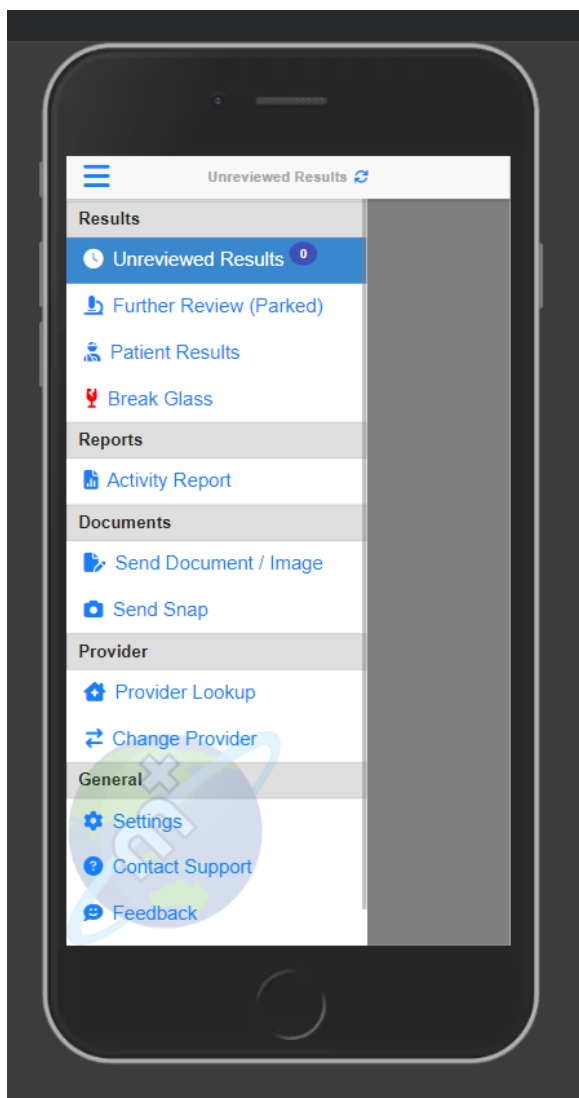
1	Overview
2	Requirements
3	Logging in and out
4	User Settings
5	Setting up Multi-Factor Authentication
5.1	Authenticator App (MFA)
5.2	Email (MFA)
5.3	SMS (MFA)
5.4	Managing Trusted Devices
5.5	MFA F.A.Q
6	Installing as PWA (Progressive Web App)



If Multi-factor Authentication is enabled for the user, you may be prompted to enter an authentication code. Decide whether you would like to set your device as a trusted device (this will allow you to skip these Multi-factor Authentication steps for 30 days on the selected device). Simply use the toggle button below **Trust this device** to select your choice, then select **Submit**.



Once logged in, you can **Logout** again or **Change Provider** by simply opening the **Menu** in the top left-hand corner of the screen.



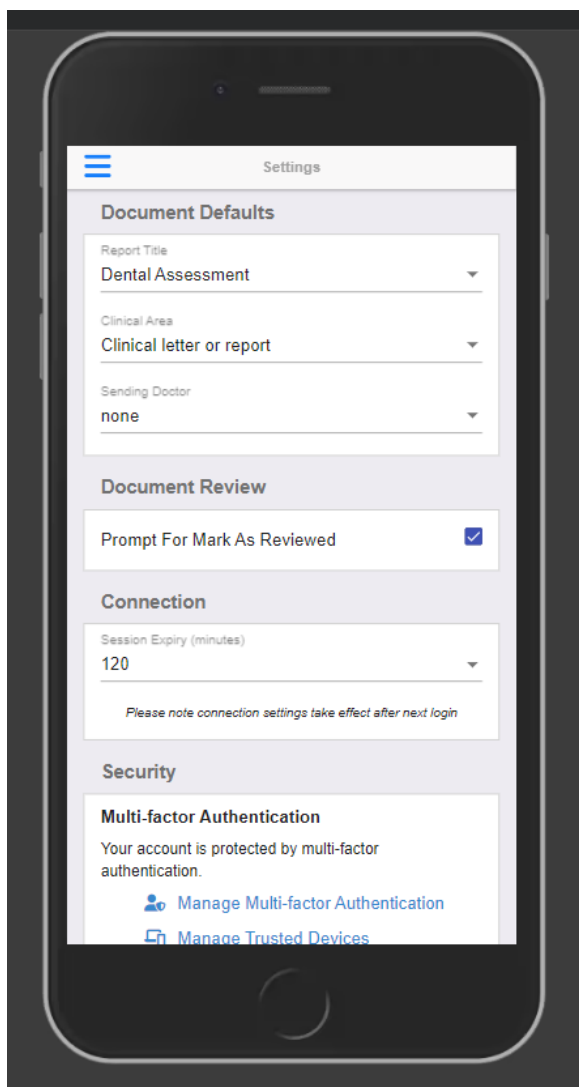
Tip!

You will be automatically logged out after 10 minutes of inactivity. You can change this via the **Settings** option in the **Menu**.

User Settings

The User Settings allow you to set your Document Defaults, whether to be prompted for Mark As Reviewed, set the Session Expiry time and manage Multi-factor Authentication.

To make changes to the User Settings, open the **Menu** in the top left-hand corner of the screen and select the **Settings** option.



Setting up Multi-Factor Authentication

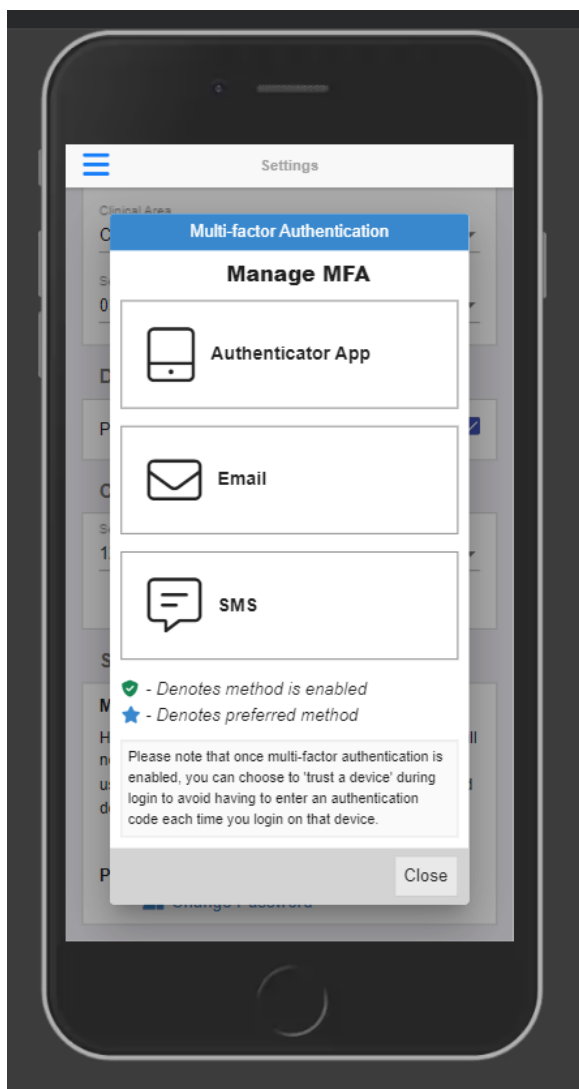
Multi-factor authentication is a security feature that helps protect your account in addition to your password. With Multi-factor Authentication, a special login code together with your username and password will need to be entered each time someone tries to access your account from a computer or device that isn't recognised.

In order to generate the special login codes, you will need to install a free app which supports the Time-based One-time Password Algorithm (TOTP) such as Google Authenticator, Authy and Microsoft Authenticator. There are many others, and some of these apps also support generating codes from desktop computers.

Multi-factor Authentication can be enabled through the following steps.

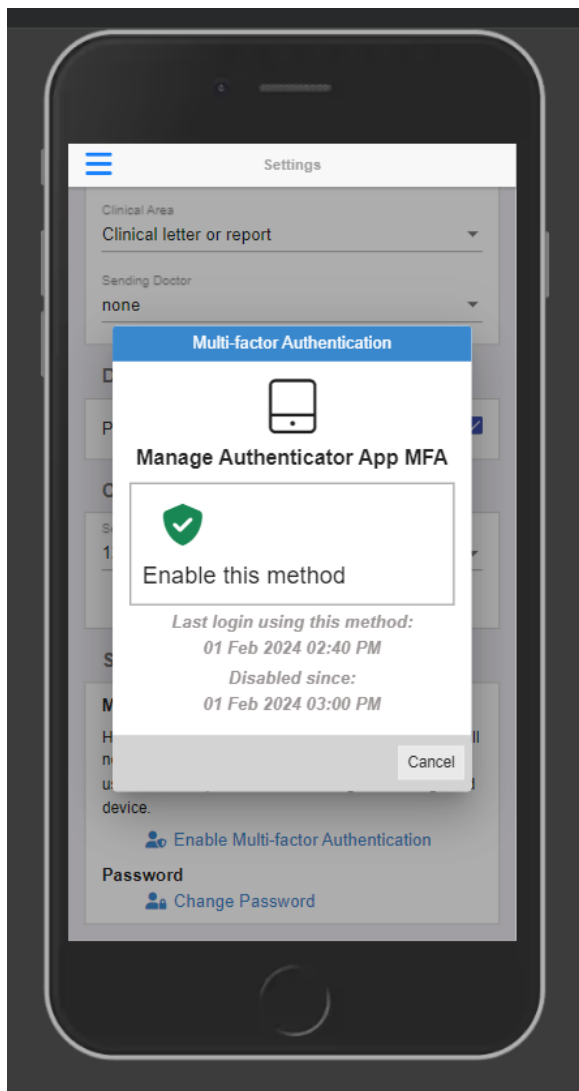
Once you have logged in, Multi-factor Authentication can be enabled by selecting **Enable Multi-factor Authentication** in the 'Security' section of the **Settings** page.

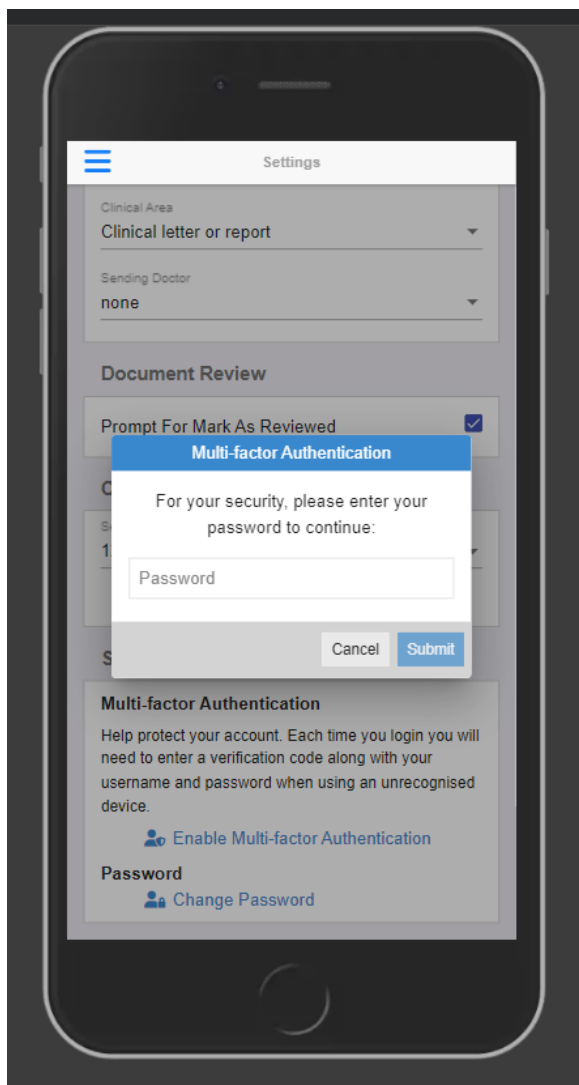
There may be multiple methods for enabling Multi-factor Authentication. Select your preferred method.



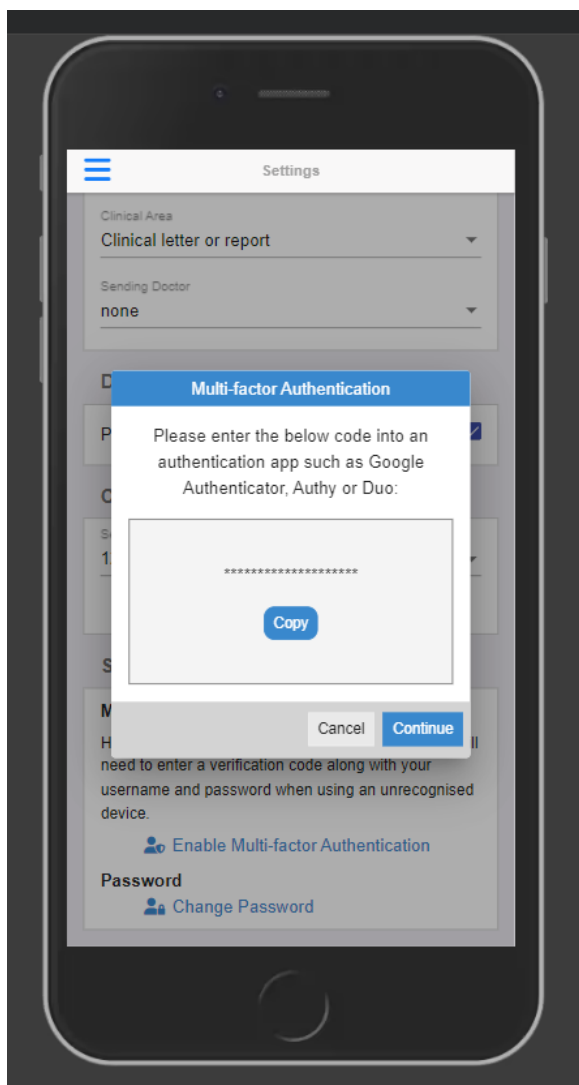
Authenticator App (MFA)

If you have selected **Authenticator App**, you can enable Multi-factor Authentication by selecting **Enable this method** and entering your password when prompted.

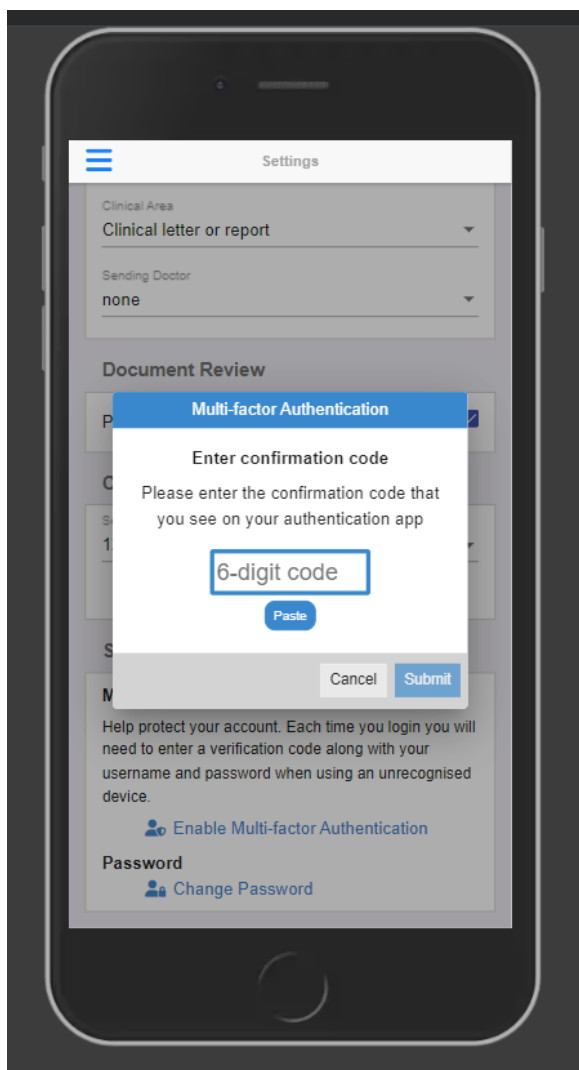




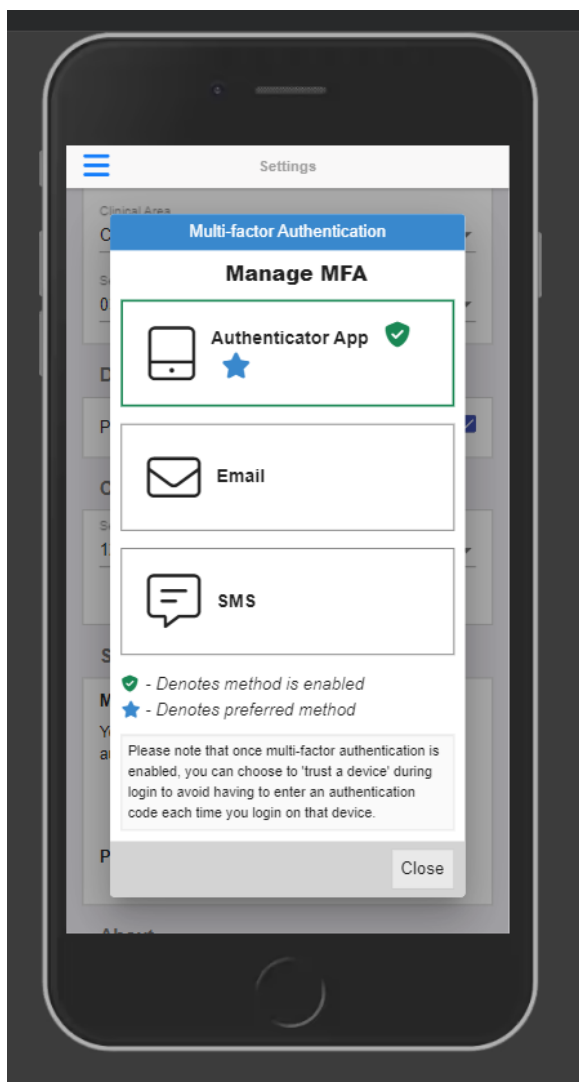
Copy the provided code and after entering the code in your Authenticator app, select **Continue**.



Enter the code your Authenticator app provided you, then select **Submit**.

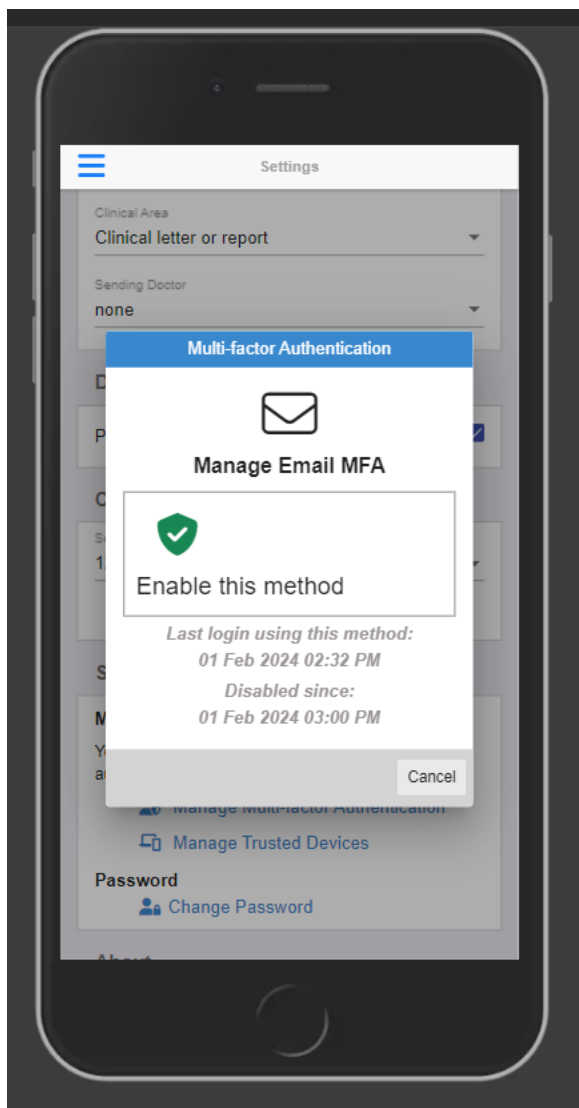


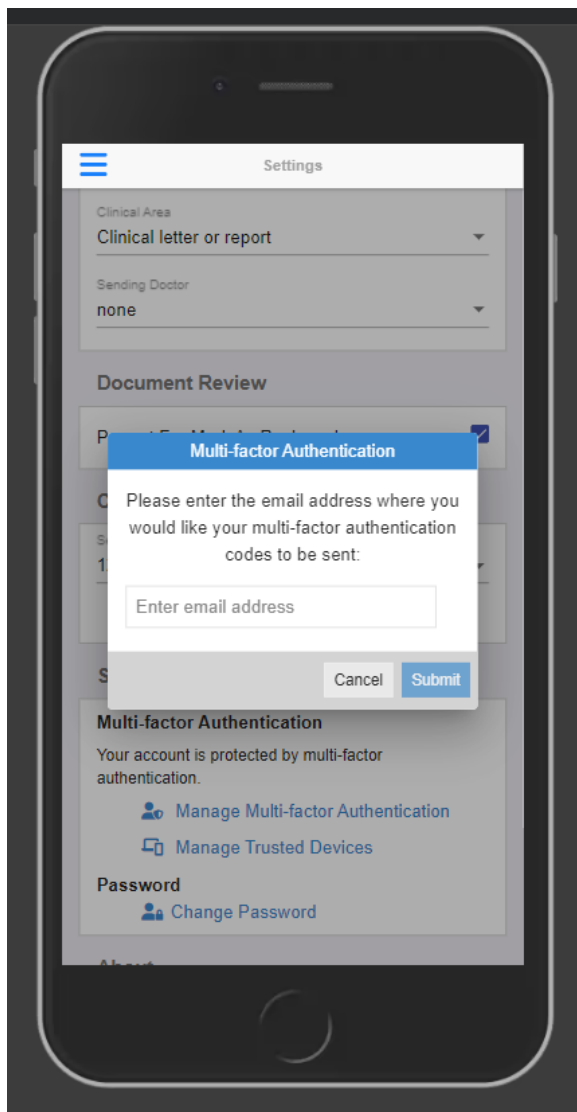
Your Multi-factor Authentication is now set up.

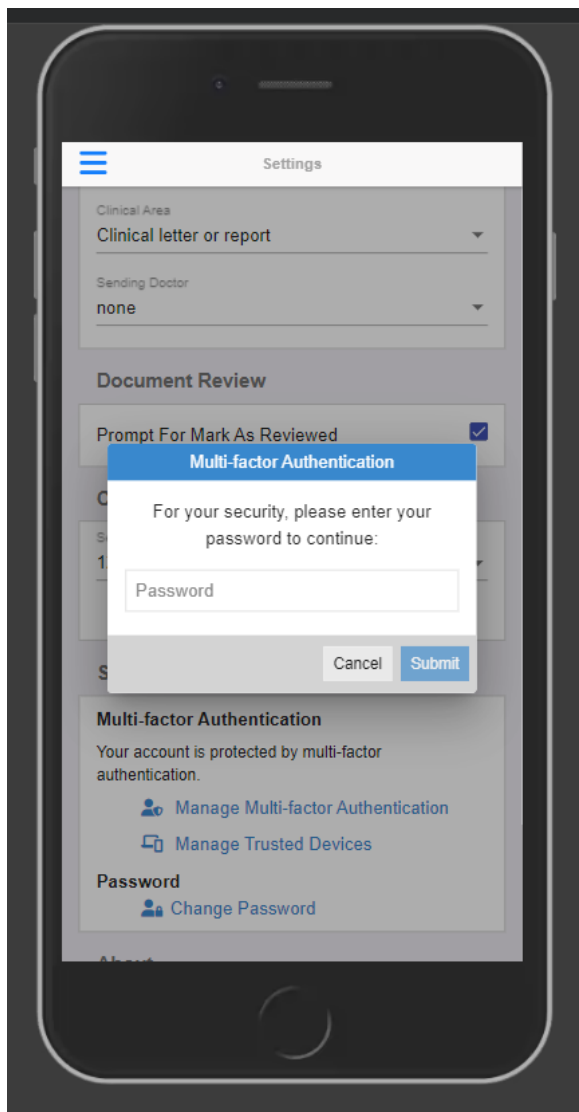


Email (MFA)

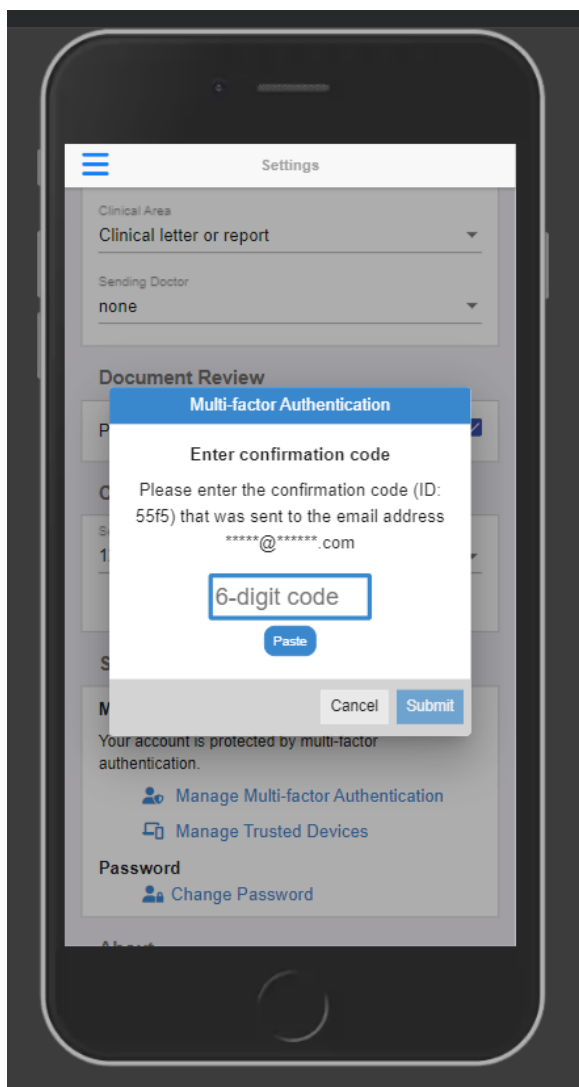
If you have selected **Email**, you can enable Multi-factor Authentication by selecting **Enable this method** and entering the email address where you would like to receive the Authentication codes and your password when prompted.



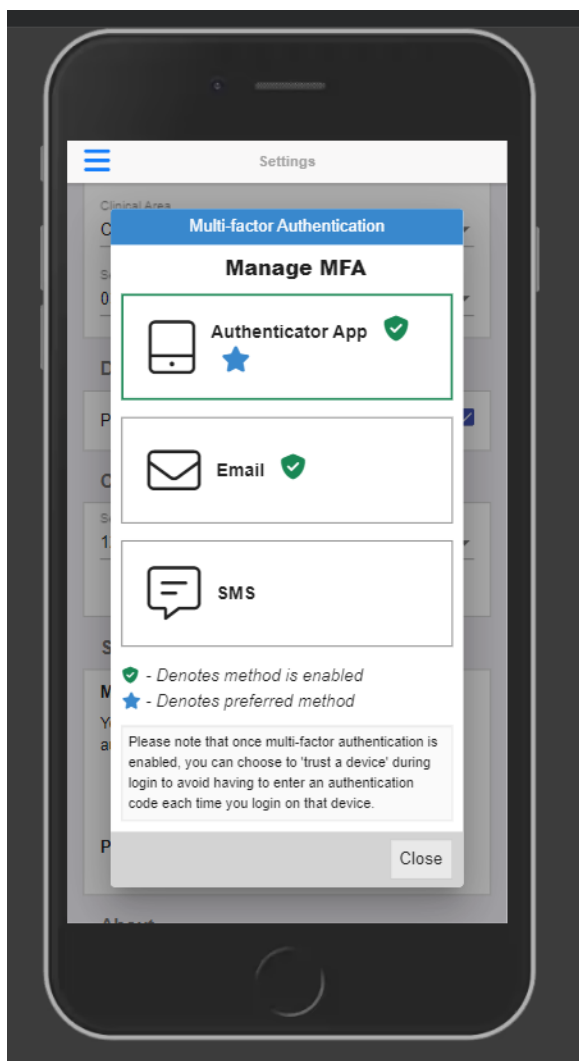




Enter the code that was sent to the email address you provided, then select **Submit**.



Your Multi-factor Authentication is now set up.



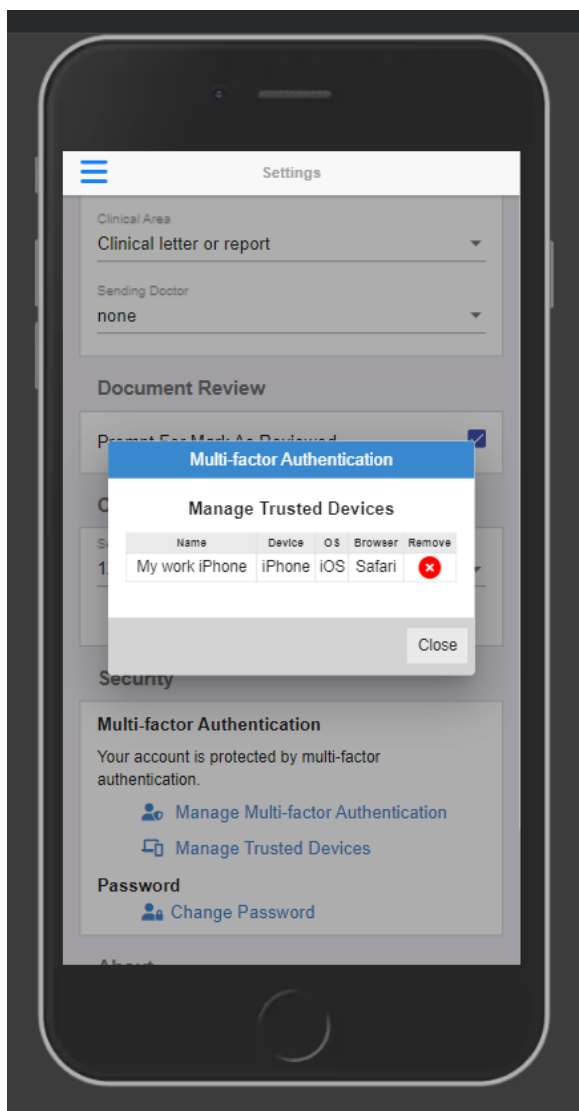
SMS (MFA)

If available in the menu, a similar process can be followed to enable SMS Multi-factor Authentication.

Managing Trusted Devices

Locate the 'Security' section of the **Settings** page in the **Menu** and select **Manage Trusted Devices**.

A list of trusted devices, if there are any, should display. Simply select "Remove" to delete a trusted device.



Please note: Trusted devices will allow you to skip the Multi-factor Authentication steps for 30 days - once the 30 days expires, they will show as "Expired Trusted Device". This means the next time you log into the portal on this device, you will be prompted to enter the code you receive from your Authenticator app.

MFA F.A.Q

What is Multi-factor Authentication?

Multi-factor Authentication is a security feature that helps protect your account in addition to your password. With Multi-factor Authentication, a special login code together with your username and password will need to be entered each time someone tries to access your account from a computer or device we don't recognise.

What do I need to be able to use it?

In order to generate the special login codes, you will need to install an app which supports the Time-based One-time Password Algorithm (TOTP) such as Google Authenticator, Authy, Microsoft Authenticator or Duo. There are many others, and some of these apps also support generating codes from desktop computers.

Do I always need to enter a code when logging in?

During login, you can choose not to use Multi-factor Authentication again on that specific device by setting it as a 'trusted device'. If you select this option, that device will only ask for your username and password when logging in for the next 30 days. You will still be protected, because when you or anyone else tries to sign in to your account from an unrecognised device, Multi-factor Authentication will be required.

Browser third party cookies need to be enabled for Explorer Online Mobile and Multi-factor Authentication to operate correctly. They are usually enabled by default.

You should not choose to trust a public device.

How do I enable Multi-factor Authentication?

To enable Multi-factor Authentication, you will need to use your Authenticator app to the code generated by Explorer Online Mobile. Your app will then generate a confirmation code which you need to enter when prompted by Explorer Online Mobile.

Your account will now be Multi-factor Authentication enabled, and you will need to generate a code with your Authenticator app whenever prompted by Explorer Online Mobile during login.

Can this be made mandatory for everyone at the organisation?

Multi-factor Authentication can be made mandatory for all users. This will force each account on login to enable Multi-factor Authentication (if it is not already enabled). Please contact our helpdesk (helpdesk@medicalobjects.com) if you would like this enabled.

How do I reset my Mutli-factor Authentication?

If you have lost your device or app which was used to enable Multi-factor Authentication, email helpdesk@medicalobjects.com for assistance.

Installing as PWA (Progressive Web App)

You can install Explorer Online Mobile as a web app on your mobile device.

In a mobile browser, navigate to the Explorer Online Mobile login page and open the browser's menu. You should see an option to "Install" or "Add to Home Screen".