Getting started with 2 factor authentication

Client user guide

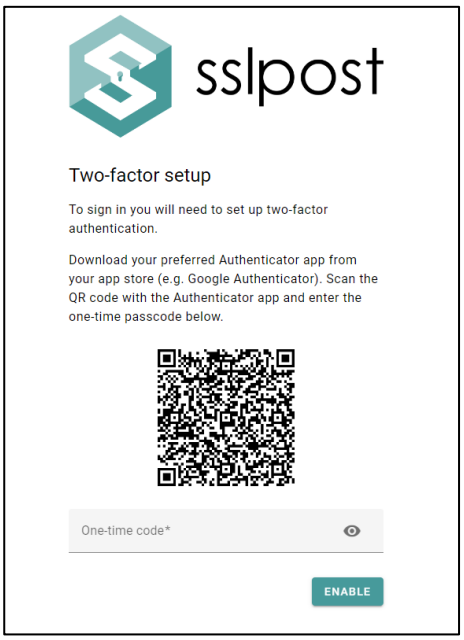
Version: 2
Issued by: SSLPost
Date: May 2025

Two factor authentication (2FA) is an additional layer of security for your private data. It ensures that a simple user name and password is strengthened by the addition of a one-time code that needs to be entered before access to your secure ELMhub portal is permitted.

You can access your ELMhub on your laptop, desktop, mobile phone or tablet. You will need a device that allows an Authenticator App (such as a mobile phone) to perform this additional security step. If you are using a mobile phone to access your ELMhub, you can use the same phone to access your Authenticator App to complete 2FA. If you are using a laptop or desktop, you will need a mobile phone or (App and camera enabled) tablet.

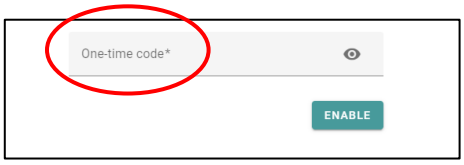
Getting started – Authenticator App

1. If 2FA has been added to your account, when you next log in you will be presented with this screen.

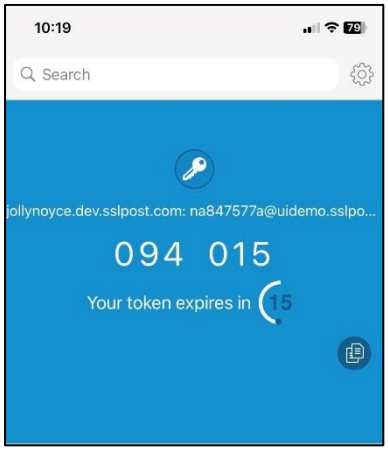


2. Using your mobile device, download a proprietary Authenticator App from your Apple or Android store. Popular examples include Twilio Authy, Google Authenticator and Microsoft Authenticator.

3. Scan the QR code using your chosen Authenticator App on your mobile device and complete the onscreen instructions. Once added, you will then need to enter the one-time code from your Authenticator App into the One Time Code box on the screen.

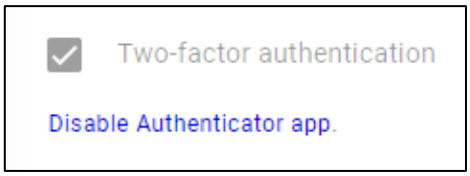


4. An example of the one-time code from Twilio Authy looks like this. Other authentication apps may vary.

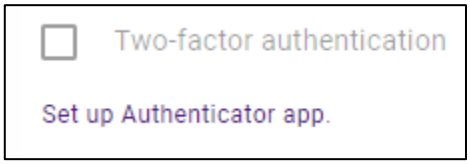


5. When you log in to your secure ELMhub portal in future, you will be asked to use your Authenticator App to add the relevant one-time pass code to the screen.

6. You can also go to your SETTINGS within your ELMhub to turn on or off the 2FA functionality (unless your organisation has deemed 2FA mandatory)



7. If you manually turn 2FA back on in your SETTINGS, you will be presented with this screen which will allow you to set up 2FA again.



8. Please note: We do not provide support for third party Authentication Apps. Should you encounter difficulties with the Authenticator App you have chosen, please contact the provider or choose another Authenticator App.

9. If you use a proprietary Authenticator and change your device, please inform support@sslpost.com as the new device will require registering before it can be used for 2FA.

Getting started – Emailed based 2FA

1. If your organisation has set your account up to capture email addresses upon registration, then 2FA can be set up for email.

2. You will be emailed a PIN number upon login/resets that will need to be entered to then gain access to your ELMhub portal. The PIN will be sent to the email address entered at registration on your account set up.