



# Get started with 2-factor authentication (2FA)

Sage

**Verify it's you**

Check your authenticator app for a code.

Enter your 6-digit code

☒ Remember me on this device for 30 days.

Continue

[Verify a different way instead](#)

[Go to help \(opens in a new tab\)](#)

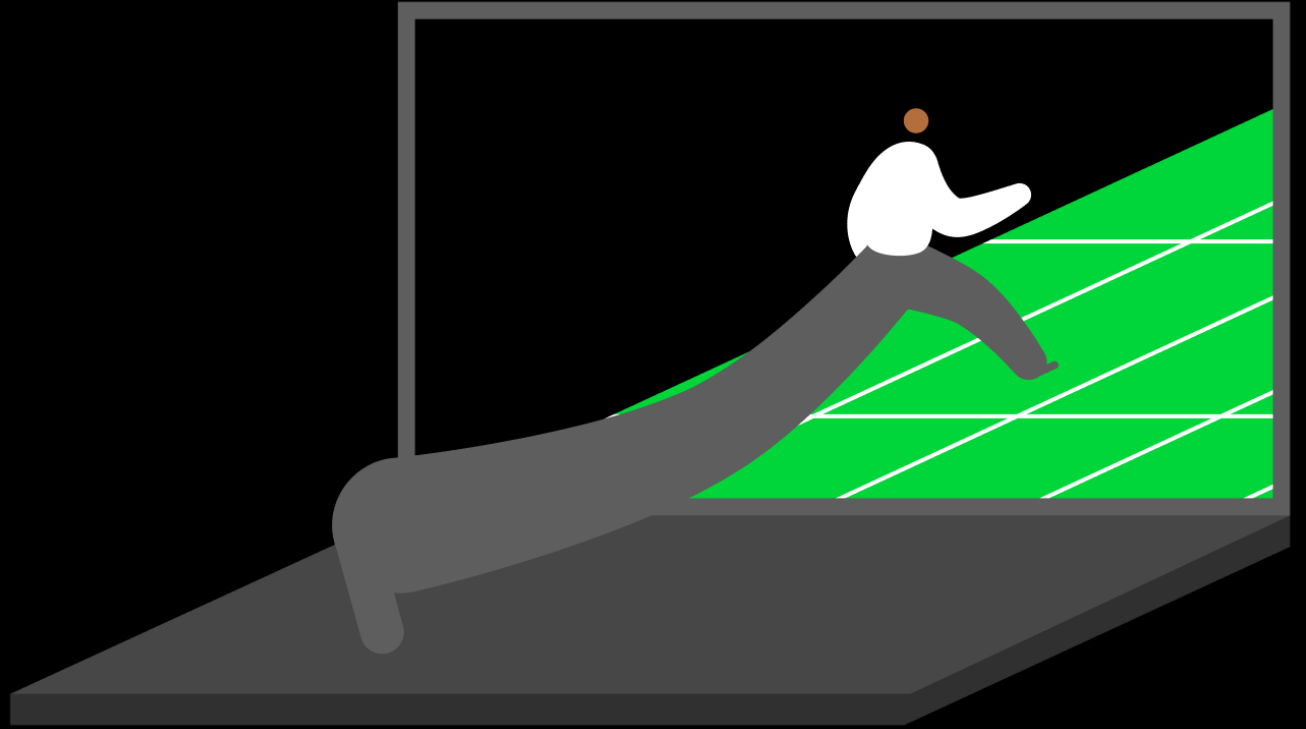


# What are we covering in today's webinar?

- Introduction to 2FA
- Security and why it is important
- *How does 2FA impact me?*
- *Important questions answered*
- How to set up and use 2FA
- When will I need to start using 2FA?
- Live Q&A



# How does 2FA impact me?



# How will 2FA impact my product?

## Scenario 1

### **Connected Services** (all versions)

- Bank feeds
- Remote Data Access
- Invoice Finance
- GoCardless
- Supplier payments
- Sage Connect

## Scenario 2

### **Introduce AI tools in v31**

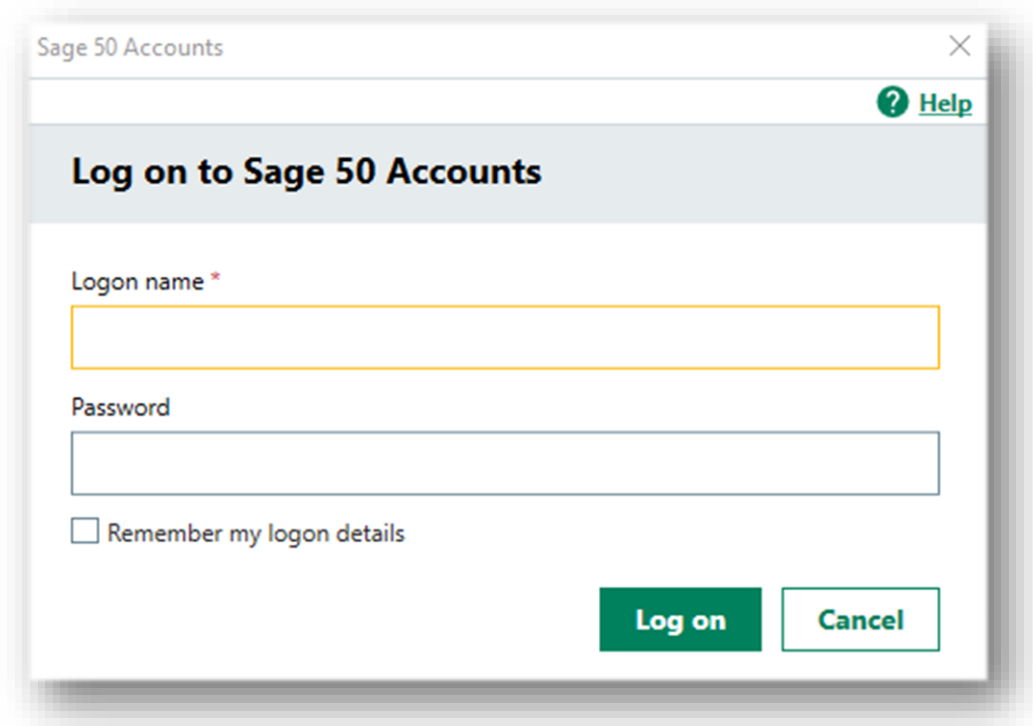
- AI tools
- Launch of 'Sage Copilot'

## Scenario 3

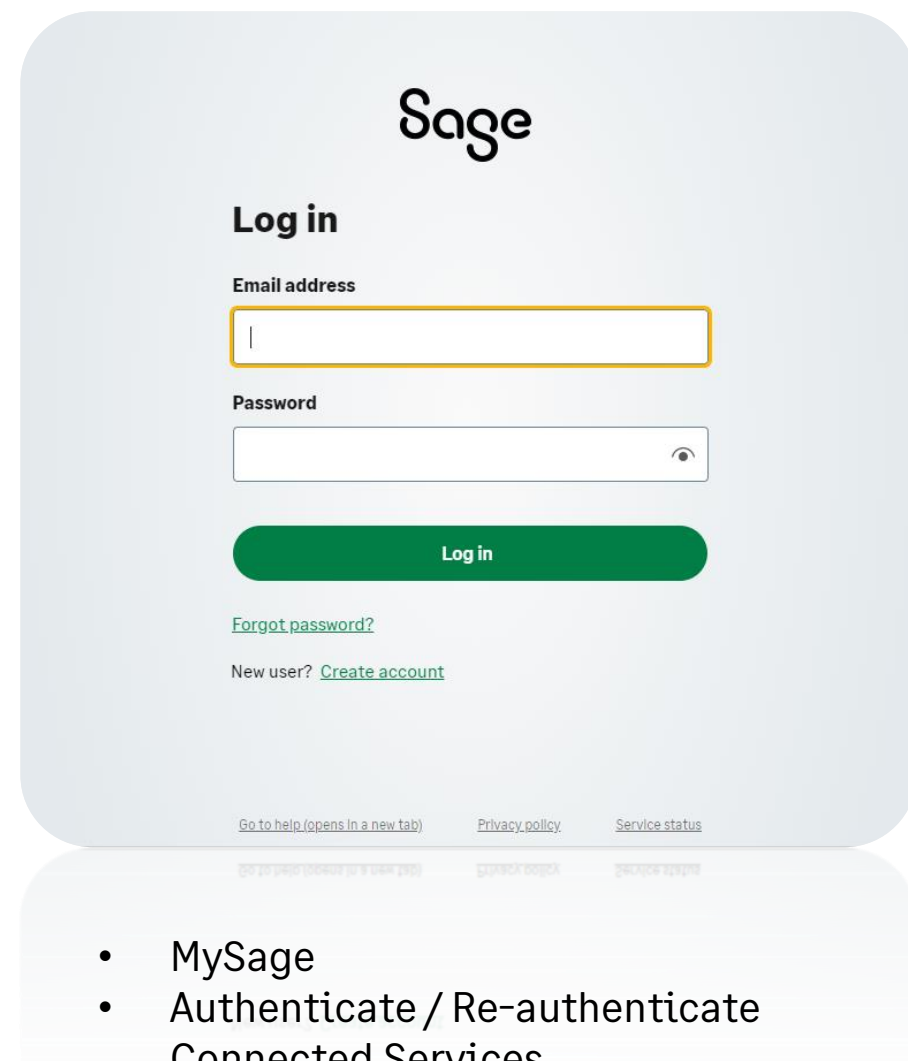
### **Get 2FA Ready!**

- Product roadmap
- Phased approach





- Log in to the software



- MySage
- Authenticate / Re-authenticate Connected Services.

# Sage account Eco-system



# Important questions answered



# FAQ

## Why am I not able to use an email to receive a code?

We believe in using the best and most secure methods to protect your data. However, emails are where cyber criminals will target first to gain access, so we consider using an authentication app or text/phone call more secure.

## What if I don't want to use my personal device/mobile?

If you do not wish to use your personal number, an authenticator app on your phone does not use/store any personal data. Alternatively, you can use a landline in an office to receive a call as long as an extension number is not required.

## What if we are unable to use mobile or landline?

Desktop authentication is available to use but this is not a method we recommend as we do not consider this the most secure option. It is important to note that some desktop authenticators do charge, whereas **mobile authenticator apps are free**. If you do have any issues using a desktop authentication it is not something we support.

Additionally, you will only be able to authenticate from that location.

## Which version of Sage 50 Accounts will require 2FA?

All versions will support 2FA. For connected services users, 2FA will be triggered when re-authentication is required, which can be up to 6 months. In V31, Copilot users can authenticate daily or every 30 days.

## Mobile authentication apps are offering free trial or trying to charge?

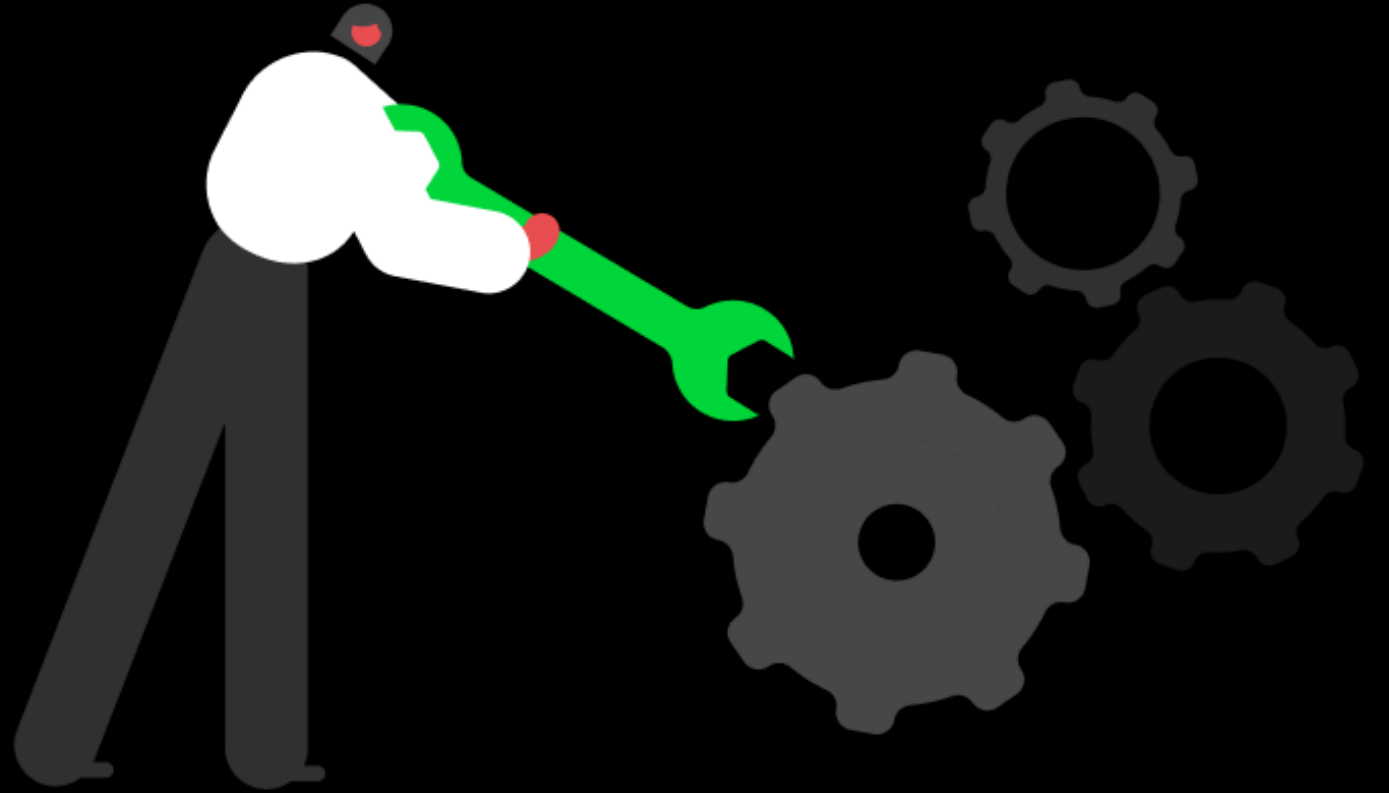
The three recommendations do not charge to use. If you are unsure, try visiting the providers website to ensure you are downloading the correct app.

# FAQ





# How easy is it to use?




# Set up 2FA in 3 simple steps

- 1 Receive a unique link to your email address.
- 2 Set up to authenticate via:
  - Text – 5 codes per hour
  - Phone call – 5 codes per hour
  - Authenticator App – No limit
- 3 Make a note of your recovery code.

## Sage

### Set up using an app

Scan the QR code with an authenticator app, then enter the 6-digit code it generates. Use an app like Microsoft Authenticator, Google Authenticator or Authy.



[Cannot scan the QR code?](#)

THEN

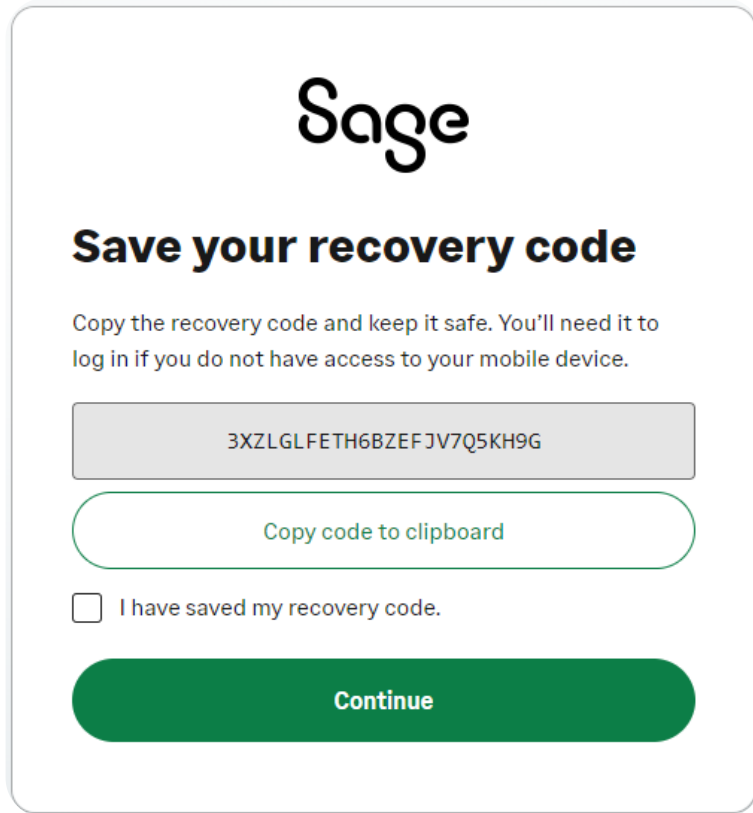
Enter your 6-digit code

[Continue](#)

[Set up with a text or phone call](#)

[Go to help \(opens in a new tab\)](#)

# Account recovery



The screenshot shows the Sage account recovery setup screen. At the top is the Sage logo. Below it is the heading 'Save your recovery code'. A paragraph explains that the user must copy the recovery code and keep it safe for login if they lose access to their mobile device. A grey box displays the recovery code '3XZLGLFETH6BZEFJV7Q5KH9G'. Below the code is a button labeled 'Copy code to clipboard'. There is a checkbox labeled 'I have saved my recovery code.' and a large green 'Continue' button at the bottom.

**Sage**

## Save your recovery code

Copy the recovery code and keep it safe. You'll need it to log in if you do not have access to your mobile device.

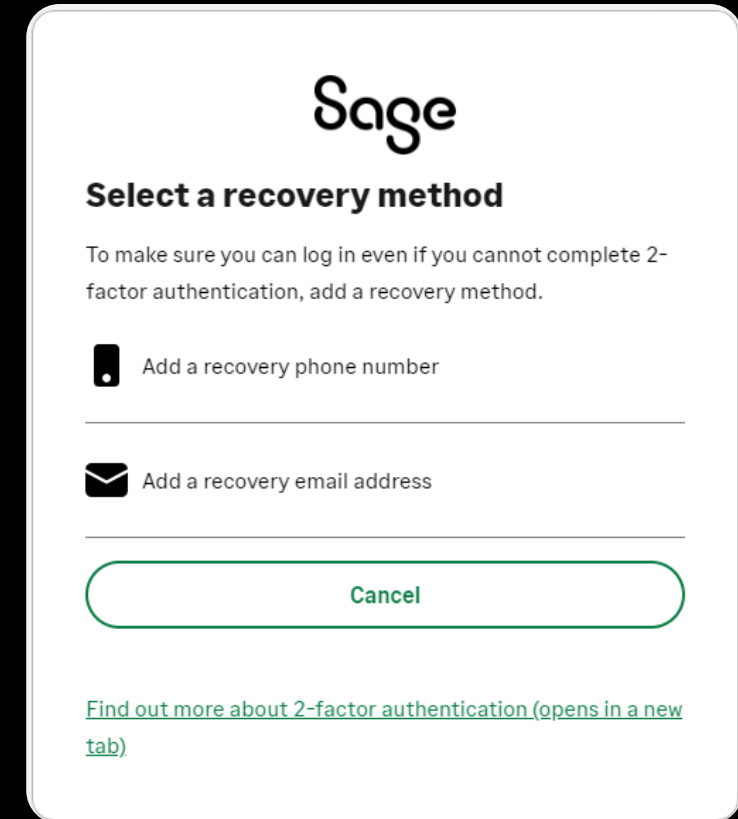
3XZLGLFETH6BZEFJV7Q5KH9G

Copy code to clipboard

☐ I have saved my recovery code.

Continue

- One time use – New one provided once utilised.
- Keep somewhere safe but where you gain access at ease.





The screenshot shows the Sage account recovery setup screen for selecting a recovery method. At the top is the Sage logo. Below it is the heading 'Select a recovery method'. A paragraph explains that to ensure login even if 2-factor authentication cannot be completed, a recovery method must be added. There are two options: 'Add a recovery phone number' with a phone icon and 'Add a recovery email address' with an email icon. A 'Cancel' button is at the bottom. A link at the bottom says 'Find out more about 2-factor authentication (opens in a new tab)'.

**Sage**

## Select a recovery method

To make sure you can log in even if you cannot complete 2-factor authentication, add a recovery method.

 Add a recovery phone number

 Add a recovery email address

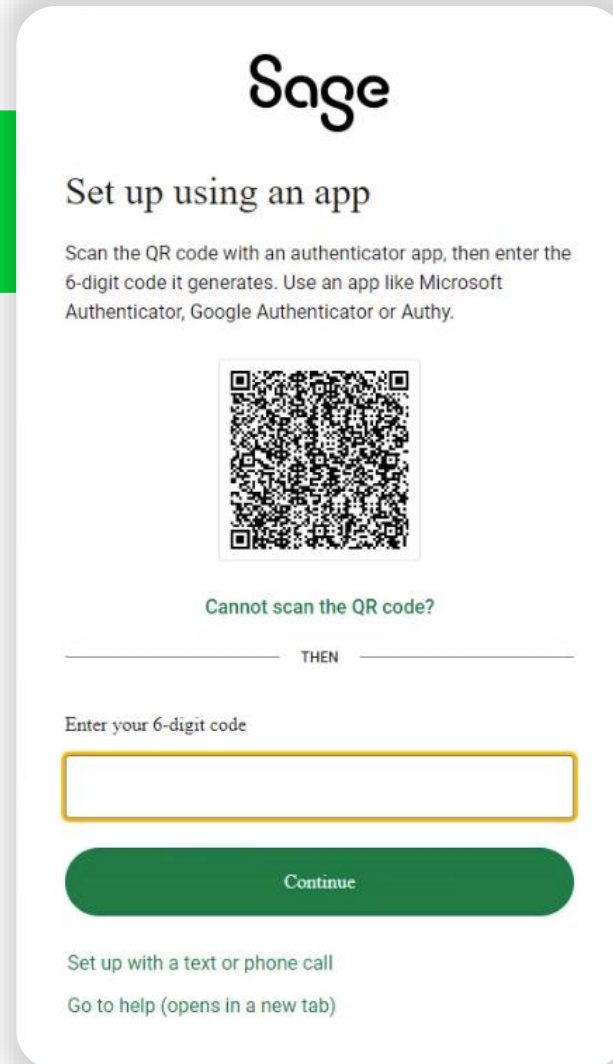
Cancel

[Find out more about 2-factor authentication \(opens in a new tab\)](#)

- Phone number cannot be the same as the authentication method.
- Email address must be different to the sage account.

# Summary & Considerations


- Make sure to use the QR code scanner within your Authentication App **not** the phones camera app.
- You can authenticate via a call to a landline if an extension number is not required.
- Copy and paste the recovery code to a safe place.
- ‘Remember this device for 30 days’ option will be available per user with a Sage account for **each** company.

A screenshot of the Sage app setup screen. At the top is the Sage logo. Below it is the heading 'Set up using an app'. A paragraph of text instructs the user to scan a QR code with an authenticator app and enter the 6-digit code it generates, mentioning Microsoft Authenticator, Google Authenticator, or Authy. A QR code is displayed in the center. Below the QR code is a link 'Cannot scan the QR code?'. A horizontal line with the word 'THEN' in the middle separates this from the next section. Below the line is the text 'Enter your 6-digit code' followed by a text input field with a yellow border. Below the input field is a green 'Continue' button. At the bottom, there are two links: 'Set up with a text or phone call' and 'Go to help (opens in a new tab)'.

Sage

## Set up using an app

Scan the QR code with an authenticator app, then enter the 6-digit code it generates. Use an app like Microsoft Authenticator, Google Authenticator or Authy.



[Cannot scan the QR code?](#)

THEN

Enter your 6-digit code

[Continue](#)

[Set up with a text or phone call](#)

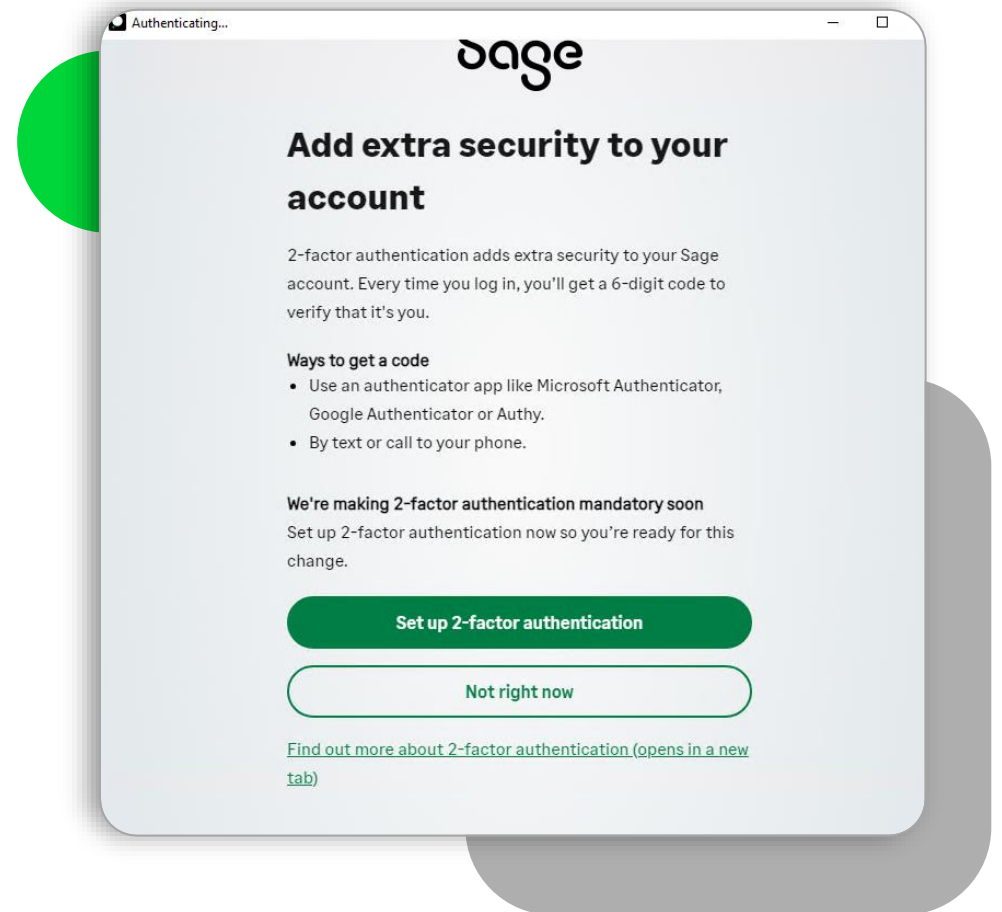
[Go to help \(opens in a new tab\)](#)

# Next Steps

**Get Started**

**Update Details**

**FAQ**



# When do I need to start using 2FA?



# Our roll out plan for 2-factor authentication

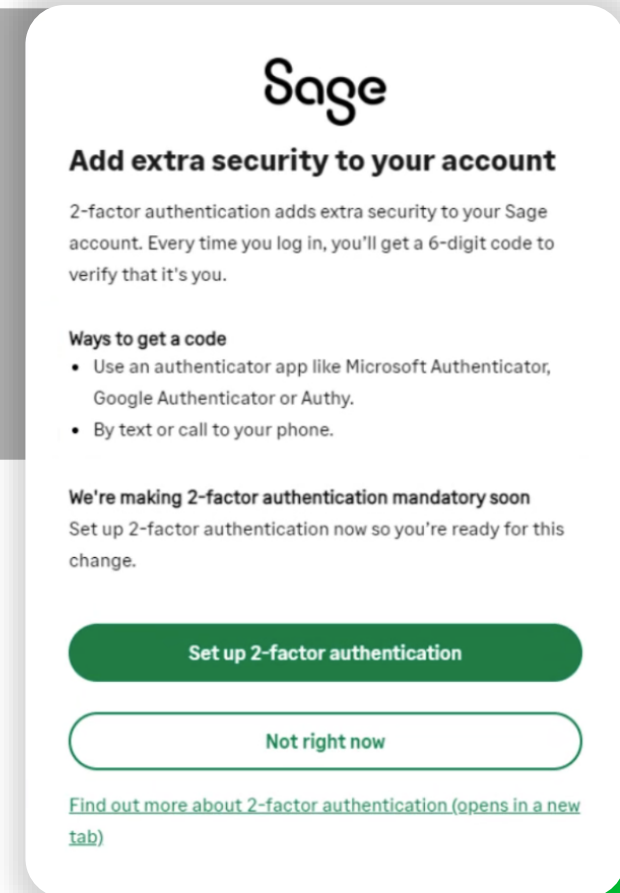
- In May 2024 we began rolling this out across our many products therefore you may have already been prompted for 2FA.
- **A mandation date will be communicated to all customers in due course.**
- Starting with Sage Copilot and Connected services users initially.
- Get a head start and set up unique profiles for your users and enable two factor authentication now.



Active 2FA users  
across all products  
in UKI.



Active 2FA users  
across 50 Accounts  
in UKI.



# Important information for **RDA users**

For **customers using remote data access**, please follow the same guidance we have just covered, with some important **additional considerations**:

- All individual RDA users will need their own unique login, **sharing logins will no longer work**.
- This is required, even if they are not accessing the product remotely.
- This will trigger an automated email invite for the user, which can then be ignored.
- Once unique users have been setup with a unique Sage Account, they can begin setting up 2FA.





# Summary

- No changes will take place until **a mandation date has been agreed** unless you have other products linked to your Sage account.
- Starting with Sage Copilot and Connected services users initially, then all users eventually.
- 2FA will only impact connected service users when they need to authenticate.
  - Not necessarily at the point of logging in.
- Each user requires a unique username and email address.
  - Free email providers are available.
- If you already have a Sage account for other products or online services, this can also be utilised for 50 Accounts.
- Each user will create their own Sage Account and set up 2FA.

Create a Sage  
account and  
set up 2FA

Help Centre

2-factor  
authentication  
Hub

# Help and resources

## FAQ: Common 2-factor authentication (2FA) questions

Created on 28 February 2024 | Last modified on 20 June 2024

### Summary

Answers to common 2FA questions and issues.

### Answers

#### How do I receive codes?

You can get a 6-digit code using an Authenticator App on your smartphone. This is the recommended option as it means you can get codes anytime and don't need a phone signal or WiFi access.

If you already have an Authenticator App, you can use it with your Sage Account. If not, you need to download one; at Sage, we use Microsoft Authenticator.

If you don't have a smartphone, you can also receive a 6-digit code via Text Message (SMS), Phone calls or by using a desktop authenticator app.

#### What if I don't have my device?

FAQ for 2FA

Sage

Products Solutions Accountants Partners Shop Blog Support

Trust and Security

Overview Security Privacy AI ethics

Search

Login

## Keep data secure with Sage 2-factor authentication

2-factor authentication (2FA) is essential to keeping your data safe. Learn how to improve cyber security, make sure you can log in securely to Sage products, and get set up in 6 simple steps.

Need support with 2FA set up? [Follow these simple steps.](#)

Need support with 2FA log in? [Contact support.](#)

[Get up to speed](#) [Watch a 2FA overview](#)

Sage

Add extra security to your account

Enter your 6-digit code

Set up using an authenticator app

### Protect your data with Sage 2FA

Phishing attempts, use of personal devices, and weak passwords can put your data at risk. 2FA

2FA Security information

'--have i been pwned?

Check if your email address is in a data breach

email address

pwned?

Using Have I Been Pwned is subject to the terms of use

Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

Why 1Password?

810

pwned websites

14,128,624,041

pwned accounts

115,796

pastes

228,889,153

paste accounts

Largest breaches

772,904,991 Collection #1 accounts

Recently added breaches

319,613 Instituto Nacional de Deportes de

Has my email been in a breach?



# If you want to find out more, or sign-up for early access to **Sage Copilot**



## Register for Early Access

See how you can get ahead with Sage Copilot. Complete the form and be among the first to experience its powerful features. Once it's available for your Sage product, we'll be in touch.

**Click here to sign up**

## Request early access

Email address

Please enter your full email address

First name

Last name

Country

United Kingdom

☐ I am an accountant or bookkeeper

We would like to use the contact details you have provided above to send you Sage marketing emails, and you can opt out at any time. Please see our [Privacy Notice](#) for details of how we use your personal data.

☐ Yes please

☐ No thanks

Would you like to receive SMS messages to learn more about Sages products and offers?

☐ Yes please, I want to receive SMS communications

Register



# Thank you!

**Please take a minute to [complete the survey](#) as you leave.**

You'll receive a follow-up email containing links to register for future webinars and watch recordings.

