Osprey Approach: Two-Factor Authentication

This help guide was last updated on
May 8th, 2024

The latest version is always online at
https://support.ospreyapproach.com/?p=64372

Click here for a printer-friendly version

Osprey™ Approach

This guide will provide all the information you need to successfully set up two-factor authentication for Osprey

What is 2FA and how is it more secure?

Two Factor Authentication (2FA) is an extra layer of security in addition to your username and password. You may have used this already with online services like banking, shopping or social media that send you a text message with a code. Osprey uses your email address instead.

As standard you will have two-factor authentication switched on at go live.

1. **Each time you sign in** using your password **you will be emailed a one-time security code** that is only available for a short period of time.
2. When you sign in, you'll be asked to enter the security code from your email.
3. **After you enter the code**, you'll be signed in to your account.

This increases the security on your account because even if somebody guesses your password, they won't be able to access your account without also having access to your emails.

The SRA Guidance

The Solicitors Regulatory Authority, in their Priority Risks Information and Cyber Security report, state that in order to mitigate risk you should **"use two-factor authentication for emails and log-ins where possible."**

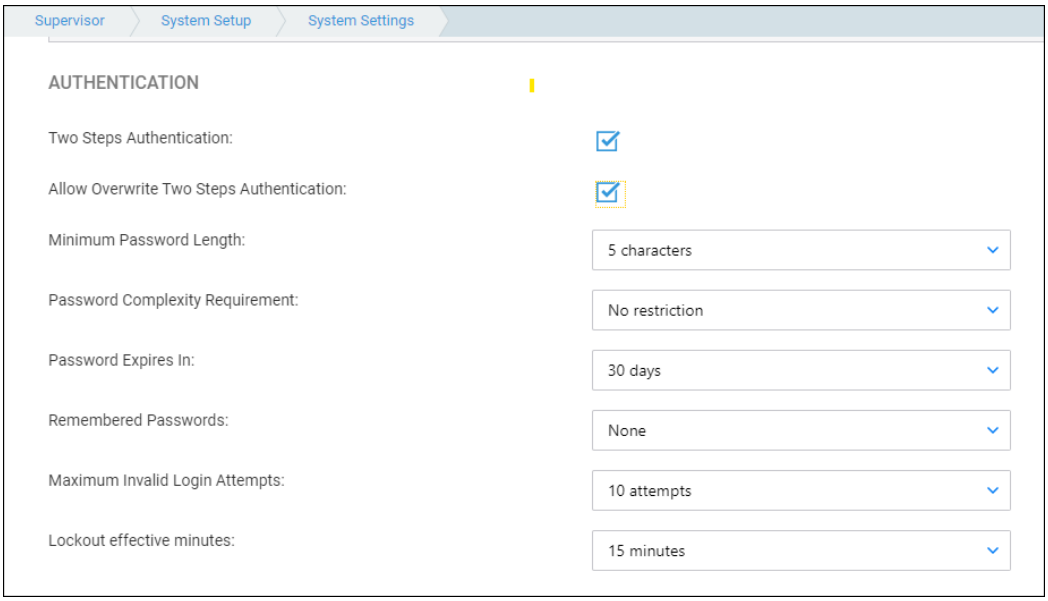
They also recommend that "**you and all staff avoid predictable passwords**."

Both of these security mechanisms are provided as standard in Osprey.

Set up Two-factor Authentication

You can apply authentication settings to all users. Navigate to the Supervisor area, select System Setup and then click on System Settings.

Click the Edit button at the top of the screen and then scroll to the bottom of the page.



- **Two Steps Authentication** – Tick this box to enable 2 Factor Authentication for all users.
- **Allow Overwrite Two Steps Authentication** – When ticked, this allows users to disable/enable 2FA for their profile if 2FA is switched on.
- **Minimum Password Length** – Set minimum password length requirement.
  Passwords must exceed 5/8/10 Characters
- **Password Complexity** – Select *Must mix alpha and numeric* to enforce passwords to contain a combination of letters and numbers.
- **Password Expires** – allows you to set the number of days after which the password must be renewed. *Options include Never/30 Days/60 Days/90 Days/1 Year*
- **Maximum Invalid Login Attempts** – Set the number of incorrect tries before the account is locked. Supervisors will be able to unlock the account from the Users screen.
  Options include No Limit/3 Attempts/5 Attempts/10 Attempts
- **Lockout Effective Minutes** – will set the amount of time an account is locked following invalid login.
  Options include Forever/15 Minutes/30 Minutes/1 Hour/2 Hou

Overwriting Two-factor Authentication

If users are allowed to override 2 Factor Authentication, they can do so in their user profile. Click the User Profile icon in the top right corner.

You can change password here, or 2-Factor Authentication can be enabled or disabled by ticking or unticking the Enabled check box.

Helpful Security Hints

- Use two-factor authentication where possible
- **Use strong passwords** – minimum of 8 characters alpha/numeric
- **Do not share credentials** – not only is this a breach of your license it also poses considerable risk and entirely invalidates your computer generated audits

- **When a user leaves, immediately deactivate access** – do not repurpose the user account. Create a new user account. Users should not be logging on under someone else's name.
- **Review access levels** – ensure each user has access levels appropriate to their use of Osprey. Do not provide users with access to data or functions that they do not need.
- **Do not autosave passwords** – ensure that under no circumstances any passwords or username are saved by default. Both computers and mobile devices will offer this to you. Always choose the "Never save my password" option
- **Ensure mobile devices have strong pin codes** – ideally 8 characters, alpha numeric. Do not use your date of birth or year of your birth or the same digit multiple times. These are often the codes hackers will try first
- **Ensure mobile devices are enrolled in Mobile Device Management** – if your staff have access to emails and company data on their devices you must have the facility to remotely wipe those same devices should they be lost or stolen.