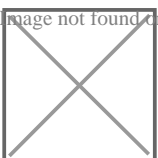


Osprey Approach: Passwords and Security

This help guide was last updated on
Jun 3rd, 2020

The latest version is always online at
<https://support.pracctice.com/?p=16965>

Image not found or type unknown



Who is this guide for?

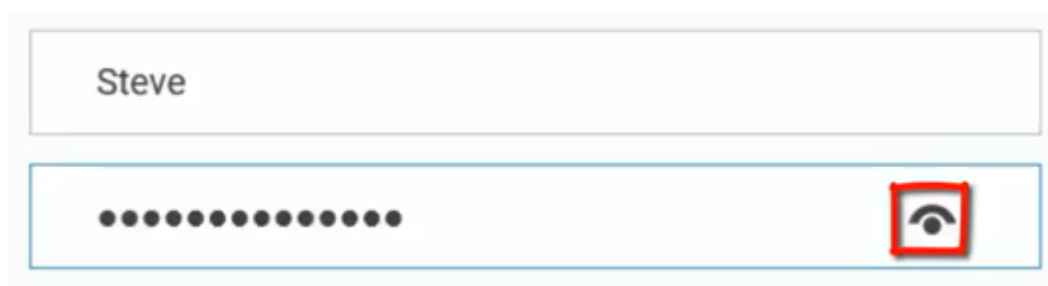
Any Users and System Supervisors

Osprey allows you to customise how your users log into the software. Supervisor users are able to set password length and complexity, as well as assigning a number of incorrect login attempts, with the option to lock the account should an incorrect password be entered a number of times.

We have also produced a short video if you prefer to watch these steps.

Logging in

The login screen allows you to view your password after you have entered it to check it is correct. Just hold down the left mouse button on the icon shown below to view your entered password:

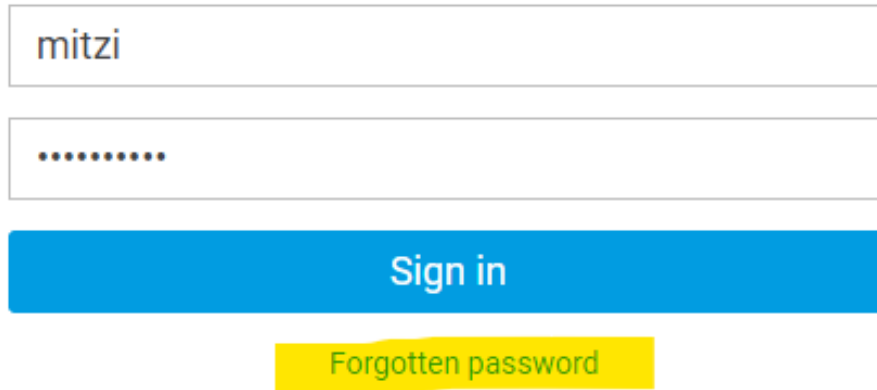


The image shows a login form with two input fields. The top field is a text box containing the name 'Steve'. The bottom field is a password box containing ten black dots. To the right of the password box is a square icon with an eye, which is highlighted with a red square border, indicating it is the target for a mouse click to toggle password visibility.

Resetting forgotten passwords

Step 1

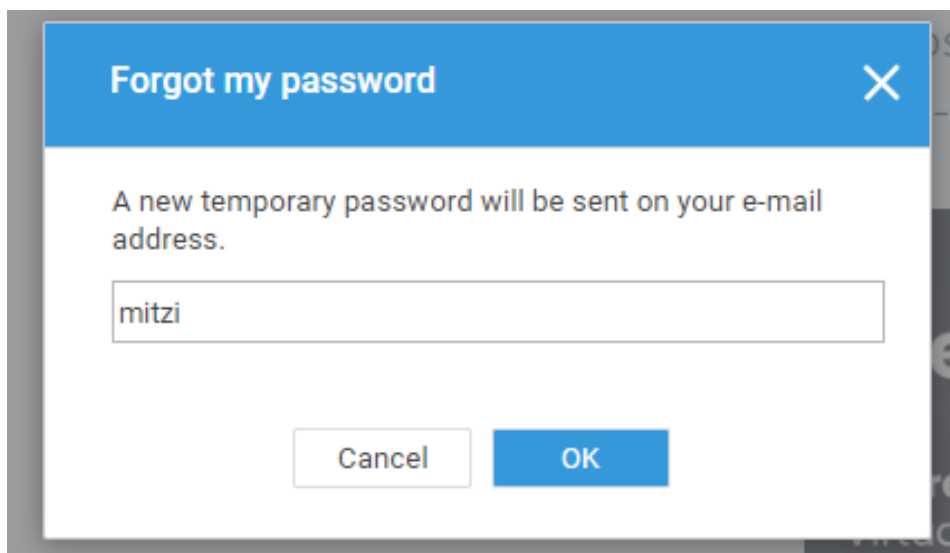
Users can reset forgotten passwords by clicking the Forgotten password link on the login screen:



The image shows a login form with two input fields. The first field contains the text 'mitzi'. The second field contains a series of dots representing a password. Below the fields is a blue 'Sign in' button. Below the button is a yellow button labeled 'Forgotten password'.

Step 2

Now enter the User Name for the password reset and click OK:



The image shows a dialog box titled 'Forgot my password' with a close button (X) in the top right corner. The dialog contains the text: 'A new temporary password will be sent on your e-mail address.' Below this text is an input field containing the text 'mitzi'. At the bottom of the dialog are two buttons: 'Cancel' and 'OK'.

Step 3

An email will be sent to the email address registered against the user account containing a new randomly generated password.

Password reset successfully



support@pracctice.net

To  Mitzi Broom

Dear MITZI,

Your new temporary password is: SYLmSQyx

Please log in with ths password and choose a new one.

Pracctice email system signature AMENDED

Step 4

Logging in with this password will then prompt the user to change their password to something more memorable.



Osprey Approach Test

[Forgotten password](#)

Please fill and confirm your new password below.

The User Profile

Once logged in, you can make changes to your user settings through the User Profile area, accessible in the top right hand corner of the software:



- To change your password, enter your current password, your new password in the New Password/Confirm Password boxes, and click Save:

CHANGE PASSWORD ▼

 Save

Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

- To turn on Two Steps Authentication tick the box and click Save. This feature means that after entering your password, you will also be required to enter a code sent to your email address prior to being able to access the system. A greyed out ticked box means that your Supervisor has already set Two Steps Authentication:

TWO STEPS AUTHENTICATION ▼

 Save

Enabled	<input checked="" type="checkbox"/>
---------	-------------------------------------

- To set your Outlook password for use with Exchange integration, enter it into the Password/Confirm Password boxes below your email address and click Save:

EXCHANGE INTEGRATION ▼

 Save


Email Address	<input type="text" value="mitzi@pracctice.net"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

- To upload a profile picture, click the Browse button, choose the file you want to upload and click the Upload button, then Save:

PROFILE PICTURE ▼

 Save

[Browse](#)

 Upload

Your profile photo will now appear in place of the User Profile icon:

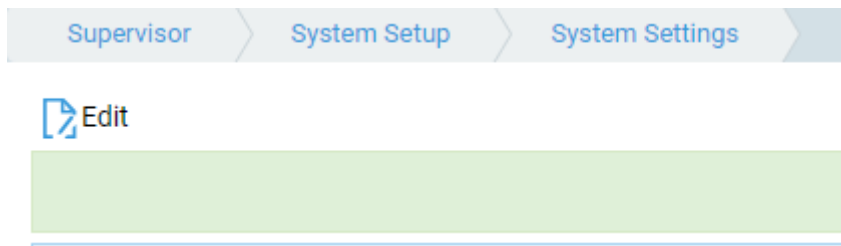


Supervisor Settings

Supervisor users also have further control over security settings. To change how users log into the software, follow the steps below.

Step 1

Navigate to Supervisor > System Setup > System Settings, and click Edit.









Step 2

Scroll down the page to the section marked Authentication:

AUTHENTICATION

Two Steps Authentication:	<input checked="" type="checkbox"/>
Allow Overwrite Two Steps Authentication:	<input type="checkbox"/>
Minimum Password Length:	8 characters ▼
Password Complexity Requirement:	Must mix alpha and numeric ▼
Password Expires In:	90 days ▼
Remembered Passwords:	None ▼
Maximum Invalid Login Attempts:	10 attempts ▼

AUTHENTICATION

Two Steps Authentication:	<input checked="" type="checkbox"/>
Allow Overwrite Two Steps Authentication:	<input type="checkbox"/>
Minimum Password Length:	8 characters 
Password Complexity Requirement:	Must mix alpha and numeric 
Password Expires In:	90 days 
Remembered Passwords:	None 
Maximum Invalid Login Attempts:	10 attempts 
Lockout effective minutes:	30 minutes 

Edit settings as required.

- Two Steps Authentication – Ticking this ensures that upon successfully entering their login details users will be asked to enter a code emailed to them.
- Allow Overwrite Two Steps Authentication – Ticking this means that users can decide whether or not they want to use the Two Steps Authentication – if ticked, users will be able to untick the Two Steps Authentication setting within their own User Profile area.
- Minimum Password Length – choose between 5, 8 or 10 characters.
- Password Complexity Requirement – choose between No Restriction (users can use letters or numbers only) or Must mix alpha and numeric.
- Password Expires In – choose between Never/30 Days/60 Days/90 Days/a Year. When set, will require the user to change their password after the set number of days.
- Remembered Passwords – choose between None/3 passwords/5 passwords. When set, will remember the last 3 or 5 passwords per user, meaning that these cannot be used again.
- Maximum Invalid Login Attempts – choose between No Limit/3 attempts/5 attempts/10 attempts. When set, will lock the user out after the specified number of failed attempts to log in.
- Lockout Effective Minutes – choose between Forever (must be unlocked by a supervisor)/15 minutes/30 minutes/1 hour/2 hours. When set, upon the Maximum Invalid Login Attempts being reached, the user will be locked out for the specified length of time. Where Forever has been chosen, only a supervisor user can unlock the user enabling them to log in again. To unlock a locked user, navigate to Supervisor > System Setup > Users, right click the user and select Unlock.

Save your changes once completed.