

SmartPay 2FA Setup Guide

SmartPay 2FA Setup Guide

SmartPay 6 comes with the option to include two factor authentication (2FA) as an extra security measure when logging into a site. This guide aims to cover the different types and how to manage it.

Types of 2FA

SmartPay supports Two Factor Authentication in two different ways:

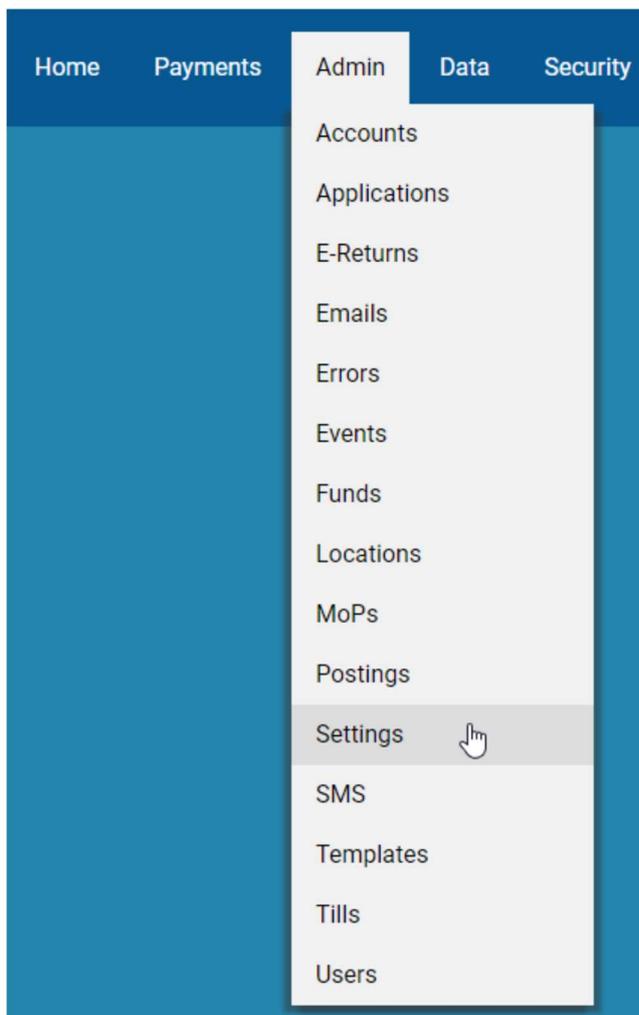
- Via Smartphone, using Google or Microsoft Authenticator.
- Via SMS. Note that SMS messages are chargeable at the standard rate.

For info on how to get Google Authenticator, [click here](#).

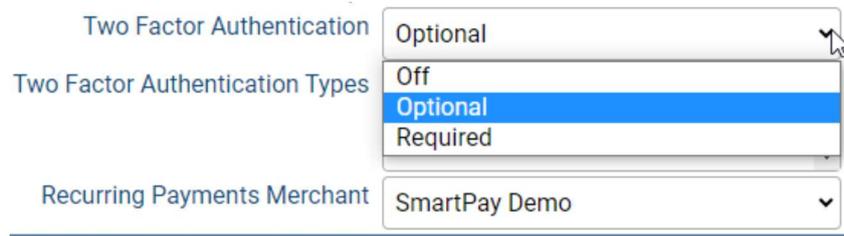
To find out more about Microsoft Authenticator, [click here](#).

Enabling 2FA

Navigate to **Admin**, via the main menu at the top of the screen, then click **Settings**. Note that you may not see the exact options listed in the example below, depending on your user permissions.

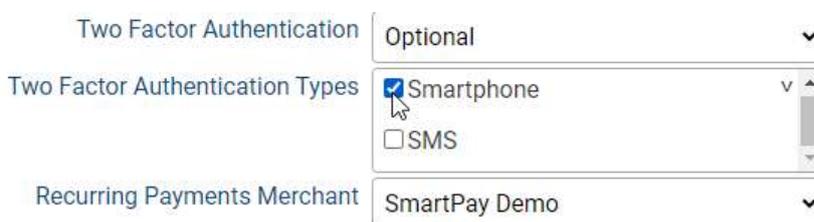


In the Settings menu, scroll down until you see **Two Factor Authentication**. Ensure that this is set to either **Optional** or **Required** depending on your needs.



A screenshot of a settings interface. It features three rows of controls. The first row is labeled 'Two Factor Authentication' and has a dropdown menu set to 'Optional'. The second row is labeled 'Two Factor Authentication Types' and has a dropdown menu with 'Off', 'Optional', and 'Required' options; 'Optional' is highlighted in blue. The third row is labeled 'Recurring Payments Merchant' and has a dropdown menu set to 'SmartPay Demo'.

In the box just below that, ensure that one of the Two Factor Authentication Types- Smartphone or SMS- is ticked.



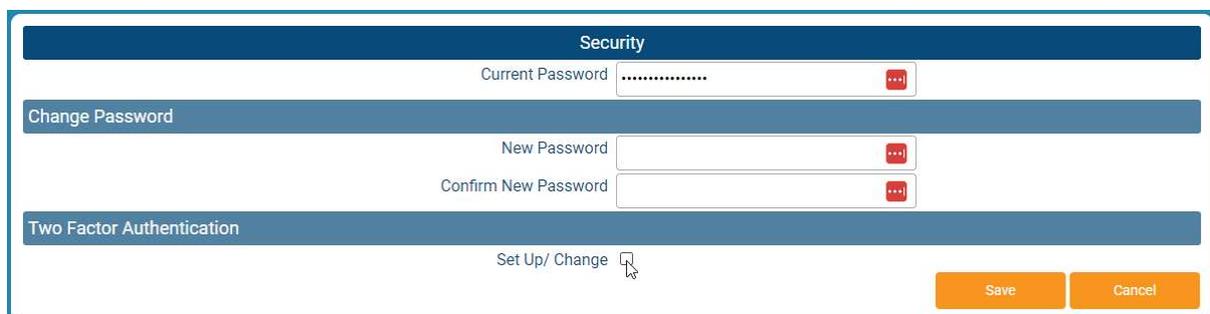
A screenshot of a settings interface. It features three rows of controls. The first row is labeled 'Two Factor Authentication' and has a dropdown menu set to 'Optional'. The second row is labeled 'Two Factor Authentication Types' and has a list with two items: 'Smartphone' with a checked checkbox and 'SMS' with an unchecked checkbox. The third row is labeled 'Recurring Payments Merchant' and has a dropdown menu set to 'SmartPay Demo'.

Users

Click the **Security** link in the menu bar. Note that if 2FA is set to 'Required' in the system settings, you will be pushed here after login.



Under 'Two Factor Authentication' select **Set Up/ Change**.



A screenshot of a 'Security' settings page. The page has a dark blue header with the word 'Security'. Below the header, there are three sections. The first section is 'Change Password' and contains three input fields: 'Current Password', 'New Password', and 'Confirm New Password', each with a red eye icon to its right. The second section is 'Two Factor Authentication' and contains a link labeled 'Set Up/ Change' with a mouse cursor pointing at it. At the bottom right of the page, there are two orange buttons: 'Save' and 'Cancel'.

Follow the on-screen instructions to set up 2FA- either scan the QR code or enter the manual code using the relevant authenticator app if using smartphone type, or mobile number for SMS.

Security

Current Password

Change Password

New Password

Confirm New Password

Two Factor Authentication

Set Up/ Change

1. Select Option Off Smartphone

2. Get Google Authenticator For Your Phone [\[Click Here For Help\]](#)

3. Scan QR Code



... Or Enter Manual Code

4. Enter Authentication Code (From Your Phone)

There is an option to 'Remember This Device Today', meaning that you are only required to go through the 2FA procedure once, and then subsequent logins via the same browser on the same day will only require the Email Address and Password.

Two Factor Authentication

Enter Authentication Code (From Your Phone)

Remember This Device Today

Resetting 2FA

If you change your phone or need to re-install Google Authenticator, an administrator can reset your profile by going into your user screen and setting **Two Factor Authentication** to 'Off'.

TwoFactor Authentication

Failed Logins

Last Updated