

CPOMS Authenticator App 'Soft Key' Setup

Step 1 - Download the CPOMS Authenticator App

The new soft key user must firstly download the '**CPOMS Authenticator**' app to their chosen device, i.e. their smart phone, tablet or iPad.

You can find the CPOMS Authenticator app by simply searching for the name in your app store, or by using one of the below hyperlinks:-



Apple App Store

<https://apps.apple.com/gb/app/cpoms-authenticator/id1093080934>



Google Play

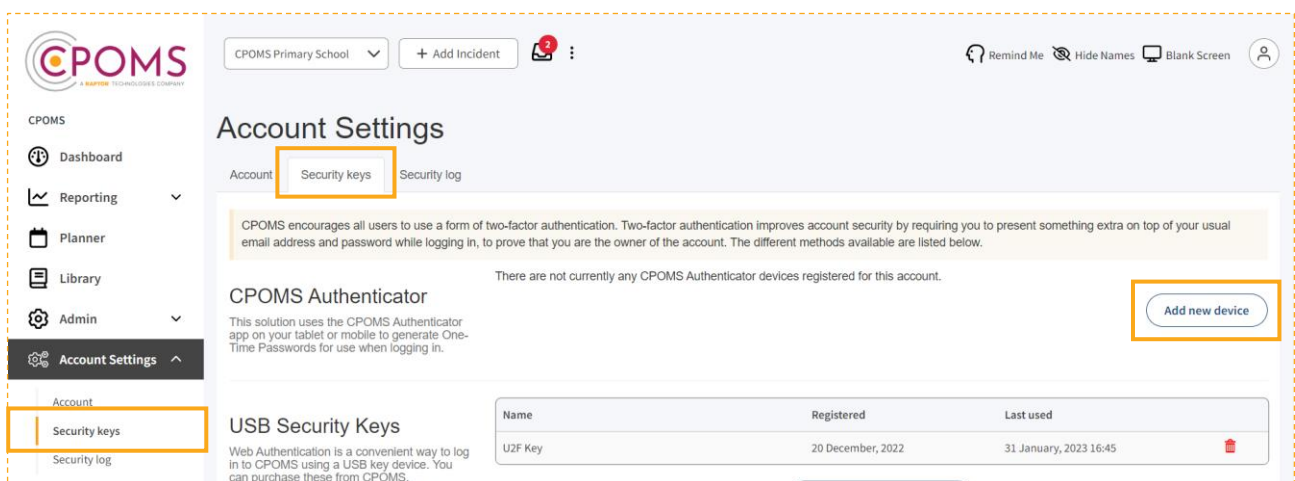
https://play.google.com/store/apps/details?id=uk.co.meritec.cpomsauthenticator&hl=en_GB

Step 2 - Log in to your CPOMS Account

Once you have downloaded the app, please log in to your CPOMS account, on a separate device to the one you have downloaded the app to. If you already have an existing key, please log in with it.

If you are using CPOMS for the first time, you will need to request an initial password by navigating to the CPOMS login page and entering your email address. On the next page, when prompted for a password, choose '**Forgot Password**' and follow the simple steps on-screen.

Once you have logged in to CPOMS, click on the '**Account Settings**' section, and then click on the '**Security Keys**' tab. Under the sub-heading for **CPOMS Authenticator**, please click on '**Add new device**'.



The screenshot shows the CPOMS web interface. The left sidebar has 'Account Settings' selected. The main content area is titled 'Account Settings' and has three tabs: 'Account', 'Security keys' (which is highlighted with an orange box), and 'Security log'. Below the tabs, there is a message about two-factor authentication. Under the 'CPOMS Authenticator' section, it says 'There are not currently any CPOMS Authenticator devices registered for this account.' and there is an 'Add new device' button highlighted with an orange box. Below this is a table for 'USB Security Keys'.

Name	Registered	Last used
U2F Key	20 December, 2022	31 January, 2023 16:45

Once you have clicked on 'Add new device', it will create a QR code for you to scan within your CPOMS Authenticator App.

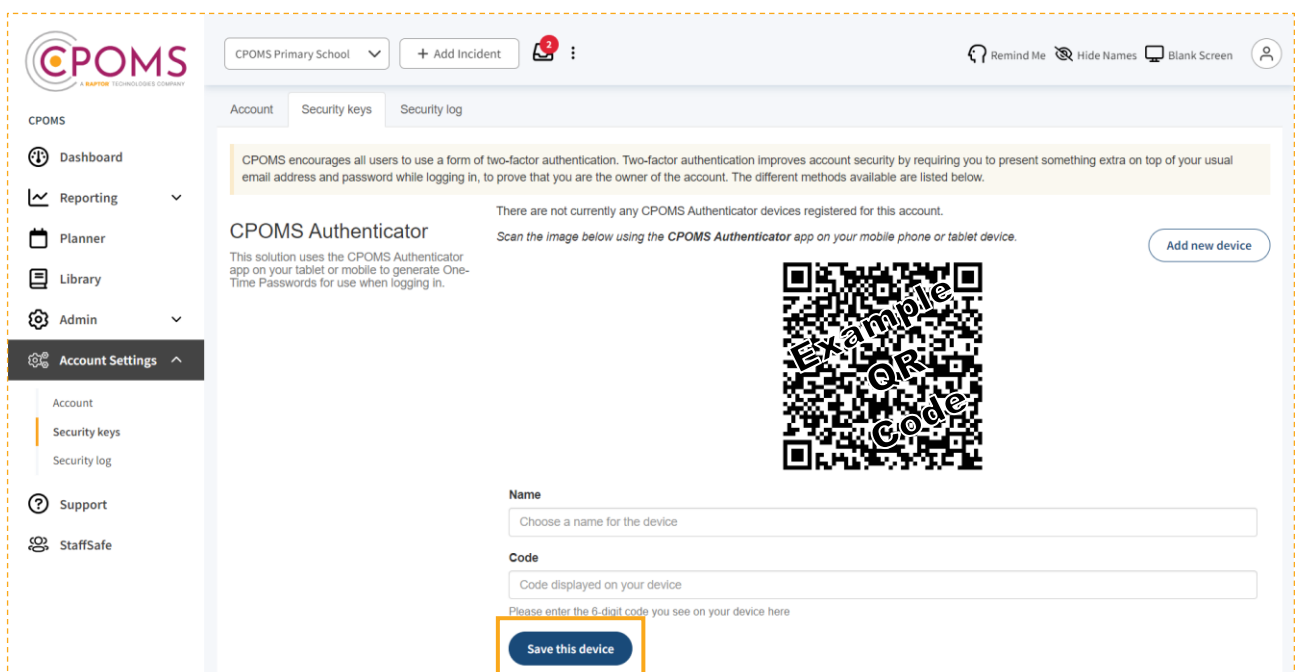
To scan the QR code, simply open up the app and tap the 'Scan QR Code' message. Now point your device camera towards this image. Once the app has scanned the QR code, it will begin generating random numbers. *For security purposes, the numbers will change every 30 seconds as the circle goes round.*

***Please continue with the below points to ensure your app is setup correctly and saves to your account.**

Next, beneath the QR code image on screen, enter a 'Name' for your device *i.e. iPad/ My Phone*.

In 'Code' type in the current 6-digit code which is now appearing in your app.

Lastly click 'Save this device'.



CPOMS Primary School | + Add Incident | Remind Me | Hide Names | Blank Screen | User Profile

Account | Security keys | Security log

CPOMS encourages all users to use a form of two-factor authentication. Two-factor authentication improves account security by requiring you to present something extra on top of your usual email address and password while logging in, to prove that you are the owner of the account. The different methods available are listed below.

CPOMS Authenticator
This solution uses the CPOMS Authenticator app on your tablet or mobile to generate One-Time Passwords for use when logging in.

There are not currently any CPOMS Authenticator devices registered for this account.
Scan the image below using the CPOMS Authenticator app on your mobile phone or tablet device.

Example QR Code

Add new device

Name
Choose a name for the device

Code
Code displayed on your device

Please enter the 6-digit code you see on your device here

Save this device

Once saved, your new Soft Key will appear listed in the CPOMS Authenticator section.

Unverified will appear next to its name until you use the app to login, this is nothing to worry about.

CPOMS Authenticator
This solution uses the CPOMS Authenticator app on your tablet or mobile to generate One-Time Passwords for use when logging in.

Successfully added new two-factor authentication method.

Name	Registered	Last used	
iPhone XR	Unverified	09 March, 2024	N/A

Step 3 - Elevate your Access

Log out of CPOMS and log back in again. It will now ask you to authenticate your login using the app.

When prompted, enter the 6-digit number appearing in your app currently, and click **'Authenticate'**.



The image shows a 'Two Factor Authentication' screen. At the top is the CPOMS logo. Below it, the text 'Two Factor Authentication' is centered. Underneath is a label 'CPOMS Authenticator Code' followed by a text input field. Below the input field is a paragraph of instructions: 'Open the CPOMS Authenticator app on your registered device and press Send Code, otherwise enter the code yourself if your device is not connected to the internet'. At the bottom of the form is a red button labeled 'Authenticate'.

If you are in a higher-level user group, your access will now change to reflect your user group permissions.

When you log in to CPOMS in the future, your app will give you the option to **'approve'** or **'deny'** a log in, rather than typing in the code manually each time. Alongside this option, it will display the approximate location of where the login took place (based on the IP address), so you can easily differentiate whether it was you who initiated the login before you choose to click 'approve'.

Permissions

Access permissions in CPOMS are set by the User Group the user has been placed in.

A CPOMS **Admin Key Holder** can check and update permissions via the CPOMS **'Admin'** area > **'Users'** tab.

Your current user groups will be listed to the right-hand side of this tab under the title **'User Groups'**. To check, or edit, a user group, simply click on the relevant user group name here - *or you may create a new one if required under the 'New Group' option.*

To change an existing users User Group - Go to **'Admin'** > **'Users'** and click on the users name from your list of users. In their profile, click on the **'Permissions'** tab, amend their user group from the drop-down options available and **'Save details'**.

If you would like to restrict your key users by class or year group, navigate to **'Admin'** > **'Groups'**. [Full instructions for this process can be sent on request.](#)

CPOMS 'Soft Key' - FAQs

I have got a new phone?

If you have got a new phone and no longer have access to your previous Soft Key/ App, to set up your new phone you must firstly **remove your previous key**.

A CPOMS **Admin Key Holder** in school can remove the key for you, within the '**Admin**' section, '**Users**' tab by clicking into your/ the user's name (into your/ the user's profile) and '**Security Keys**'.

Tick '**I confirm that I have read and understand this notice**', and the '**Remove this user's 2FA devices**' button to remove the key from the user's profile.

In the case that [redacted] loses or no longer has access to all of their registered two-factor authentication devices listed below, you can remove them, enabling them to register new devices when they next log in.
In the time between removing the devices and registering new ones, the user account will not be able to access areas of the system restricted to two-factor users only. Please note, Merilock keys will not be removed.

☒ I confirm that I have read and understand this notice.

Name	Type	Date Registered	Last Used
Iphone	TOTP	09 March, 2024	09 March, 2024 09:36

Remove this user's 2FA devices

Once the previous key has been removed, you may setup a new Soft Key following the original CPOMS 'Soft Key' Setup instructions (Page 1). Please log out and back in before you begin this process.

My app is asking me to 'Scan QR Code'?

If your app reverts to the 'Scan QR Code' message, it means your app needs to be reconfigured. To do this, you must firstly **remove your previous key**.

A CPOMS **Admin Key Holder** in school can remove the key for you, within the '**Admin**' section, '**Users**' tab by clicking into your/ the user's name (into your/ the user's profile) and '**Security Keys**'.

Tick '**I confirm that I have read and understand this notice**', and the '**Remove this user's 2FA devices**' button to remove the key from the user's profile.

In the case that [redacted] loses or no longer has access to all of their registered two-factor authentication devices listed below, you can remove them, enabling them to register new devices when they next log in.
In the time between removing the devices and registering new ones, the user account will not be able to access areas of the system restricted to two-factor users only. Please note, Merilock keys will not be removed.

☒ I confirm that I have read and understand this notice.

Name	Type	Date Registered	Last Used
Iphone	TOTP	09 March, 2024	09 March, 2024 09:36

[Remove this user's 2FA devices](#)

Once the previous key has been removed, you may setup a new Soft Key following the original CPOMS 'Soft Key' Setup instructions (Page 1). Please log out and back in before you begin this process.

I cannot access 'Security Keys'?

If you cannot click on the 'Security Keys' tab (within 'Account Settings') to set up a Soft Key, it may be that the system thinks you have a key already. This can occur if perhaps you started the process previously or have got a new phone, or that you have logged in without using your current key.

If you still have access to the previous key please click '**Elevate your access**' to the top right.

If you do not have access to the previous key, you must **remove the previous key** to start the process again.

A CPOMS **Admin Key Holder** in school can remove the key for you, within the '**Admin**' section, '**Users**' tab by clicking into your/ the user's name (into your/ the user's profile) and '**Security Keys**'.

Tick '**I confirm that I have read and understand this notice**', and the '**Remove this user's 2FA devices**' button to remove the key from the user's profile.

In the case that [redacted] loses or no longer has access to all of their registered two-factor authentication devices listed below, you can remove them, enabling them to register new devices when they next log in.
In the time between removing the devices and registering new ones, the user account will not be able to access areas of the system restricted to two-factor users only. Please note, Merilock keys will not be removed.

☒ I confirm that I have read and understand this notice.

Name	Type	Date Registered	Last Used
Iphone	TOTP	09 March, 2024	09 March, 2024 09:36

[Remove this user's 2FA devices](#)

Once the previous key has been removed, you may setup a new Soft Key following the original CPOMS 'Soft Key' Setup instructions (Page 1). Please log out and back in before you begin this process.

My location on the app is not accurate?

The location shown on the app is actually taken from the location of your I.P address, so it can sometimes appear to be further afield.

To put your mind at rest you can check the location of your I.P address before choosing to 'approve'.

Simply search 'What's my IP' in a search engine (*i.e. Google*) on your app device and click on <https://whatismyipaddress.com>, which is usually the first result. This will then confirm the location of your I.P address, which you can check matches against the location shown in your app.

Or if you would prefer, you can choose to type in the numbers manually into CPOMS, rather than clicking on the approve option.

Error message 'Incorrect or out of date code'?

If you receive an error message which says 'Incorrect or out of date code', when logging in to CPOMS with your key, it means the date and time on the device of your app is out of sync with our servers (it may be slightly fast or slow).

Usually the way to fix this is to amend the date and time setting on the device of your app to 'set automatically'. This ensures the date and time is set identically to our servers.

Error message 'No usable date' when trying to scan the QR code?

This sometimes occurs if you are trying to scan the QR code via the normal camera on your device, rather than through the CPOMS Authenticator App. To scan the QR code, please ensure you have firstly opened the CPOMS Authenticator App and tapped 'Scan QR Code'. Please then point the camera toward the QR code image when prompted.

For further assistance on any of the above please do not hesitate to contact us on

01756 797766 or support@cpoms.co.uk.

