

How to Set Up Your MFA

A guide to setting up, using, and removing each Multi-Factor Authentication option on your Sprintax account: Authenticator App, SMS, and Passkeys.

What is MFA, and why do I need it?

Multi-Factor Authentication (MFA) is an extra verification step that confirms it's really you signing in. After you sign in as usual, you'll be asked to verify your identity a second way: with a code from an authenticator app, a text message to your phone, or a passkey stored on your device.

This second step matters because your Sprintax account is used to prepare and file sensitive tax documents on your behalf. MFA is required by the IRS and this is the safeguard that confirms it's genuinely you authorizing the signature of tax forms, protecting your personal and financial information from unauthorized access.

Three ways to verify

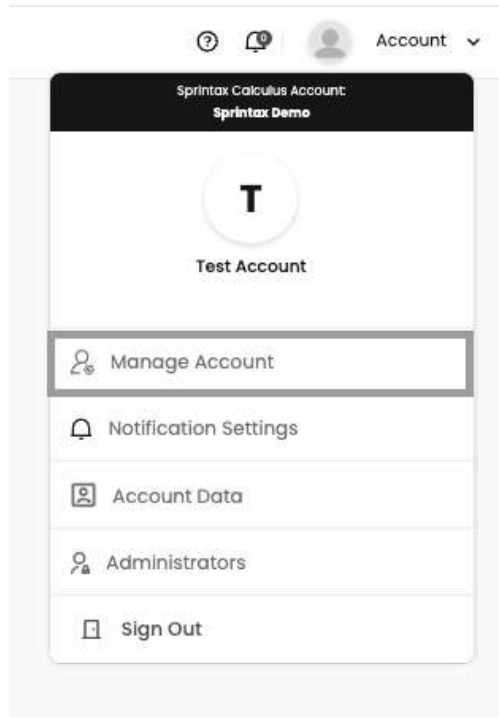
You can set up MFA using an Authenticator App, SMS (text message), or a Passkey. You only need one method to sign in, but you can set up more than one for backup. Each is covered below, with setup and removal steps.

Where to Start

In order to enable any form of MFA for any Sprintax account, you must navigate to the Sprintax Identity Server. This step will look slightly different depending on whether you are accessing Calculus as an Institutional Administrator or as a User.

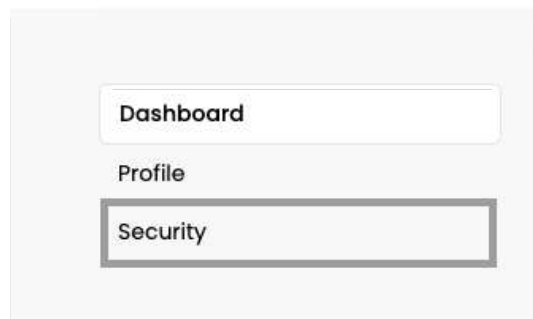
Administrator:

- Log in to your Sprintax Calculus account.
- In the top-right corner, click **Account** and select **Manage Account**.



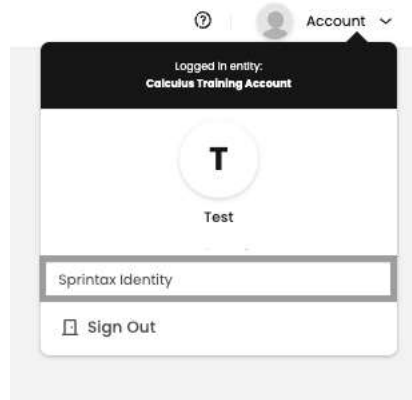
- From the left-hand menu, click **Security**.

sprintax



User:

- Log in to your Sprintax Calculus account.
- In the top-right corner, click **Account** and select **Sprintax Identity**.



- From the left-hand menu, click **Security**.



How to Enable / Disable Each Form of MFA

1. Authenticator App

An authenticator app (such as Microsoft Authenticator, Google Authenticator, or similar) generates a time-based verification code on your smartphone, which you enter when signing in to Sprintax Calculus.

Setting up MFA with an Authenticator App

Step 1: Add an Authenticator App

- Navigate to the Security section in Sprintax Identity.
- Scroll down to the **Authenticator app** section.
- Click **Add Authenticator**.

Authenticator app

Enable two-factor authentication (2FA) for enhanced security on your account.



Two-factor authentication (2FA) is not enabled

Use an authenticator app (e.g., Google Authenticator, MS Authenticator) to generate one-time passcodes for an extra layer of security when verifying your identity during login.

Add Authenticator +

- Enter a name for the authenticator (for example: *My Phone, Sprintax etc.*).

Add name to the authenticator

Display name*

Cancel
Verify

Step 2: Connect Your Authenticator App

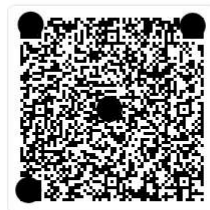
- A new window will appear with a QR code.

Setup authenticator app

Use an authenticator app like 1Password , Authy , Google Authenticator , Microsoft Authenticator to generate one-time passcode for an extra layer of security when verifying your identity during login.

Scan the QR code

Use your authenticator app or browser extension to scan.



Unable to scan?



Verify the passcode from your app*

XXXXXXX

Cancel

Verify

- Open your authenticator app on your smartphone.
- In the app, go to Settings or Add new account.
- Scan the QR code displayed in your Sprintax account.

Step 3: Confirm and Activate

- After scanning the QR code, your authenticator app will generate a verification code.
- Enter this code into Sprintax Calculus when prompted.

Verify the passcode from your app*

XXXXXXX

- A confirmation message will appear in the top-right corner of your screen, indicating that MFA has been successfully activated.



Your two-factor authentication is activated



Removing an Authenticator App

Step 1: Remove MFA from Sprintax

- Navigate to the **Security** section in Sprintax Identity.
- Scroll down to the **Authenticator App** section.
- Locate your authenticator and select **Remove**.

Authenticator app

Enable two-factor authentication (2FA) for enhanced security on your account.

Name	Date Added	Status
Sprintax	21.05.2026	Confirmed
		...
		Rename
		Remove

Authenticator +

- You will see a confirmation message that MFA has been disabled.



Two-factor authentication is disabled



Step 2: Remove the Account from Your Authenticator App

- Open your authenticator app.
- Delete or remove the Sprintax Calculus account from the app.

This ensures that you can successfully re-enable MFA in the future if needed.

2. SMS (Text Message)

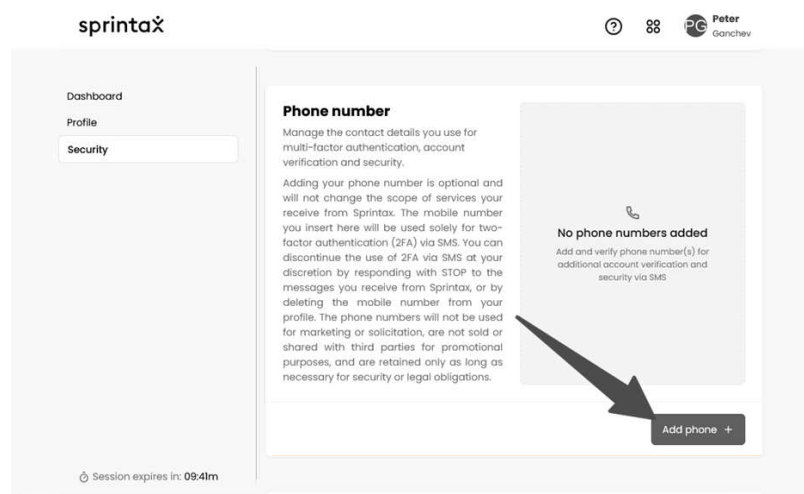
You can register your phone number through Sprintax Identity to receive a one-time verification code by text message each time you sign in.

Please Note

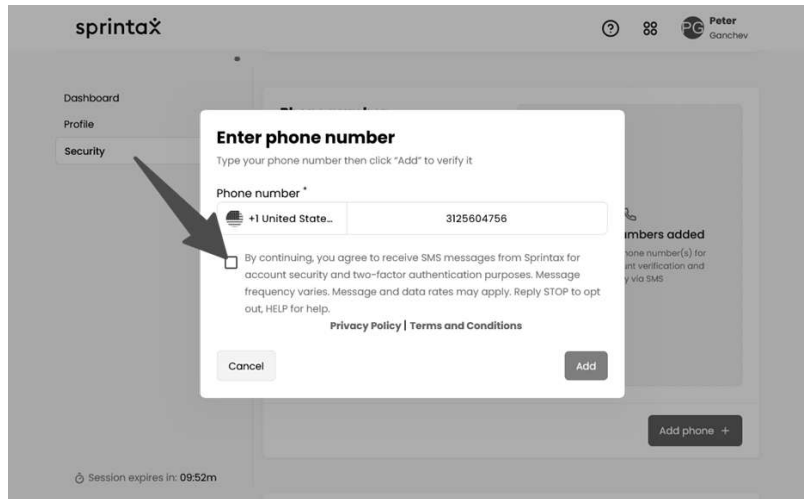
SMS MFA isn't available for phone numbers from every country. See **Countries & Territories Where SMS MFA is Supported** for the full list of supported countries and territories.

Setting up MFA with SMS

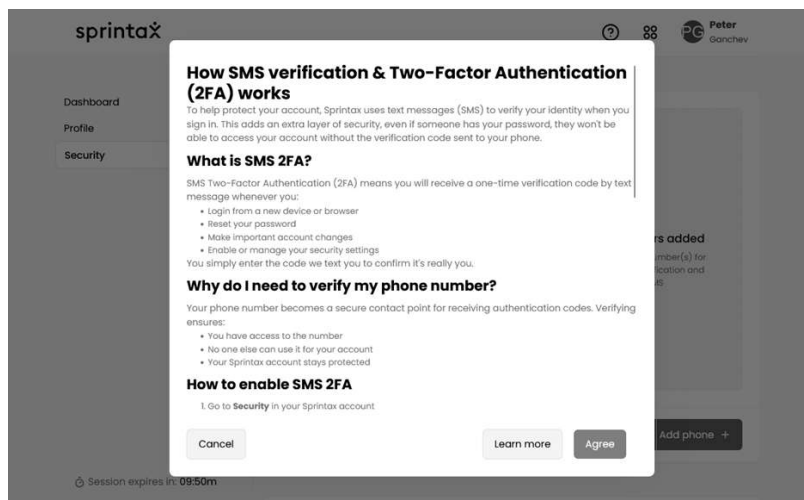
- Navigate to the Security section in Sprintax Identity.
- Scroll down to the **Phone Number** section.
- Click **Add phone**.



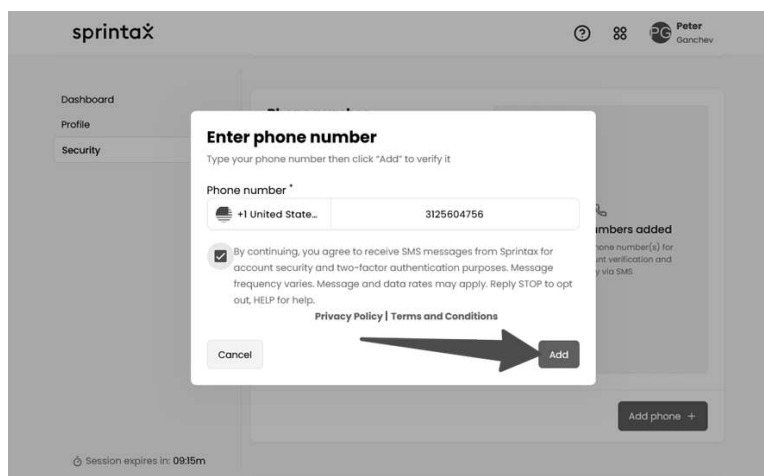
- Enter the phone number and review the conditions.



- Scroll to the end of the instructions and click **Agree**.

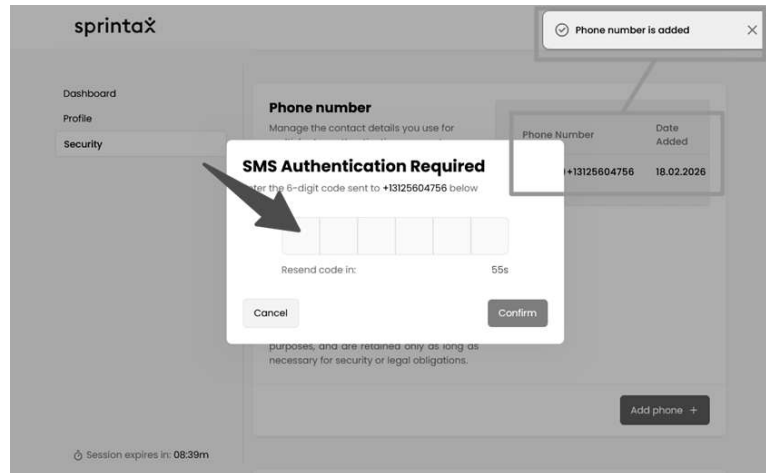


- Click **Add** to save the phone number.



Verifying your phone number

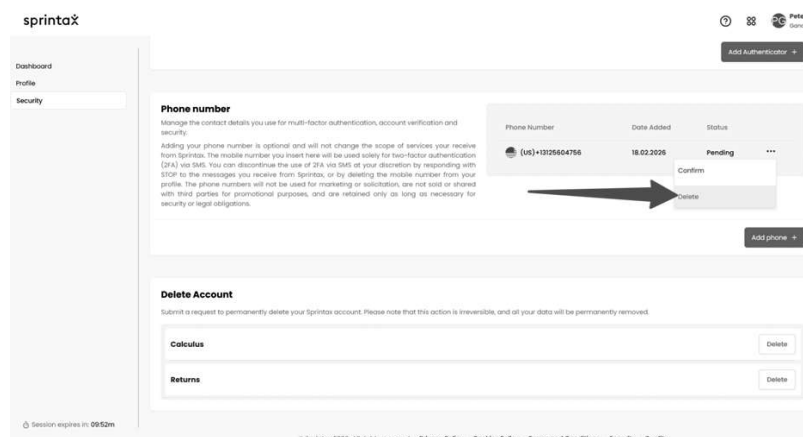
Once the phone number is added, the system will send an SMS containing a 6-digit verification code. Enter this code in the verification field to confirm your phone number.



After successful verification, the phone number will appear in your account and can be used for SMS MFA when logging in.

Removing a Phone Number

- Navigate to the Security section in Sprintax Identity.
- Scroll down to the **Phone Number** section.
- Click the three dots beside the phone number.
- Select **Delete**.



Removing the number will stop the system from sending SMS verification codes to that device.

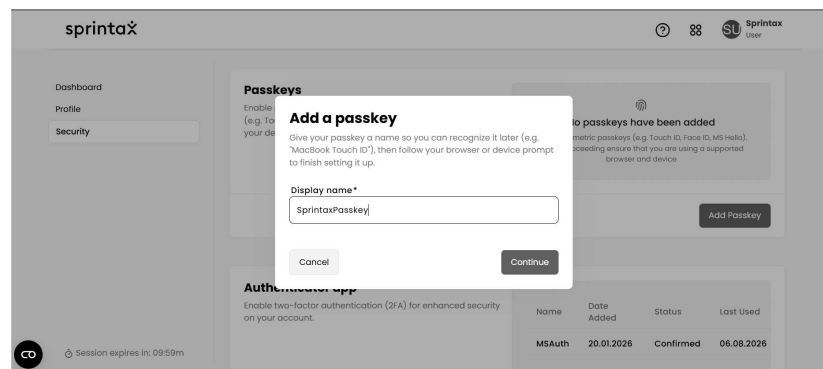
3. Passkeys

A passkey is a form of authenticating your account using your device's own security, such as Face ID, Touch ID, Windows Hello, or a PIN.

Setting up a Passkey

Step 1: Add your passkey

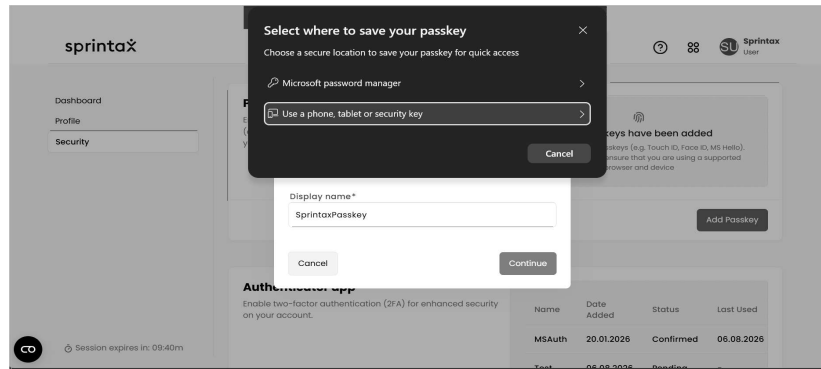
- Navigate to the Security section in Sprintax Identity.
- Scroll down to the **Passkey** section.
- Select **Add Passkey** to begin.
- Give the passkey a display name so you can recognize it later, for example "Work laptop" or "My phone."
- Select **Continue** when you're done.



Step 2: Choose where to save it

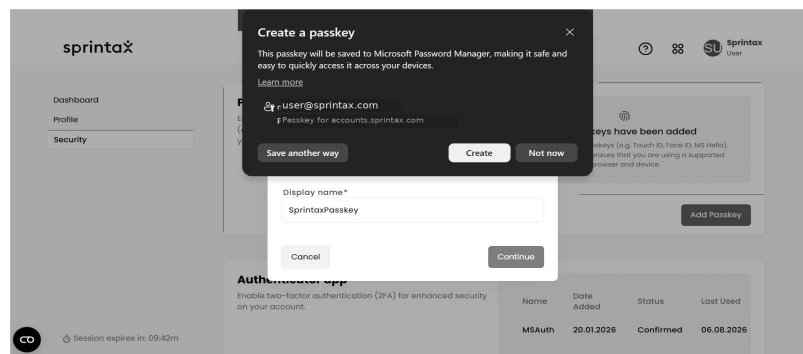
Your browser will ask where you'd like to save the passkey. Pick the option that matches how you want to sign in:

- Save on this device: store the passkey on the device you're using, unlocked with a fingerprint, face, or PIN.
- Use a phone, tablet, or security key: save the passkey on your phone and confirm by scanning a QR code.

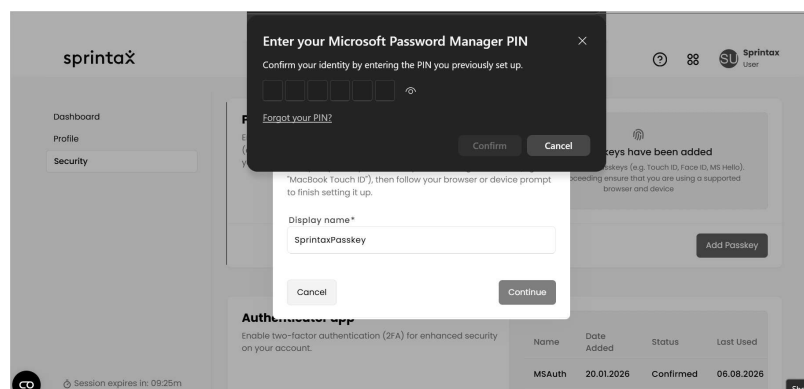


Option A: Save on this device

- Your browser confirms it will save the passkey (for example, to Microsoft Password Manager on Windows, iCloud Keychain on Apple devices, or Google Password Manager on Android). Select Create to continue.



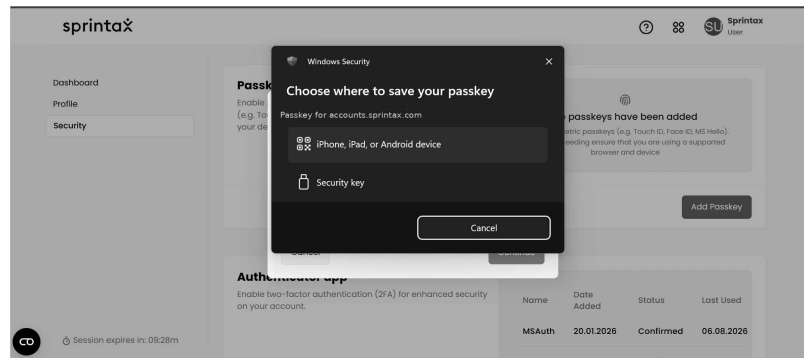
- Enter the PIN you previously set up (or use Face ID / Touch ID / Windows Hello) and confirm. This never leaves your device — Sprintax never sees it.



Once confirmed, your passkey is created.

Option B: Use a phone, tablet, or security key

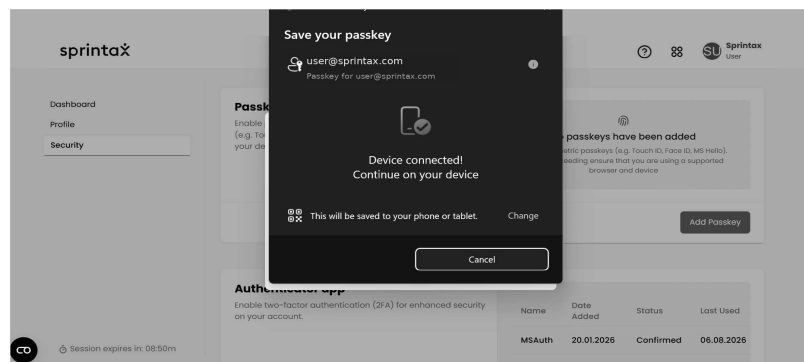
- Your browser asks which device to use. Select “iPhone, iPad, or Android device” (or “Security key” if you use a hardware key).



- A QR code appears. Scan it with your phone's camera and follow the prompt on your phone.

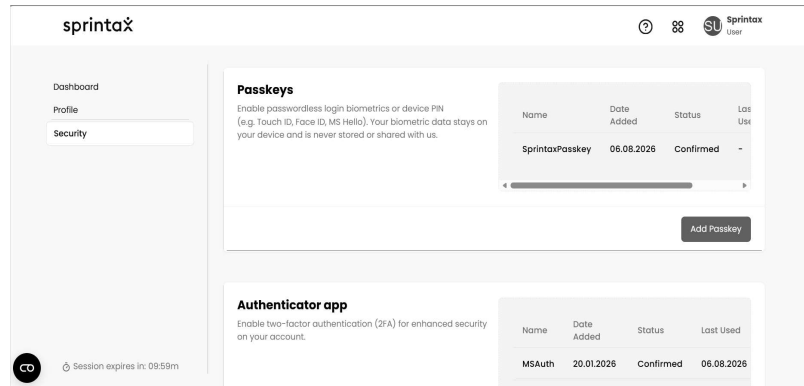


- Once your phone connects, finish the prompt on your phone to complete the passkey.



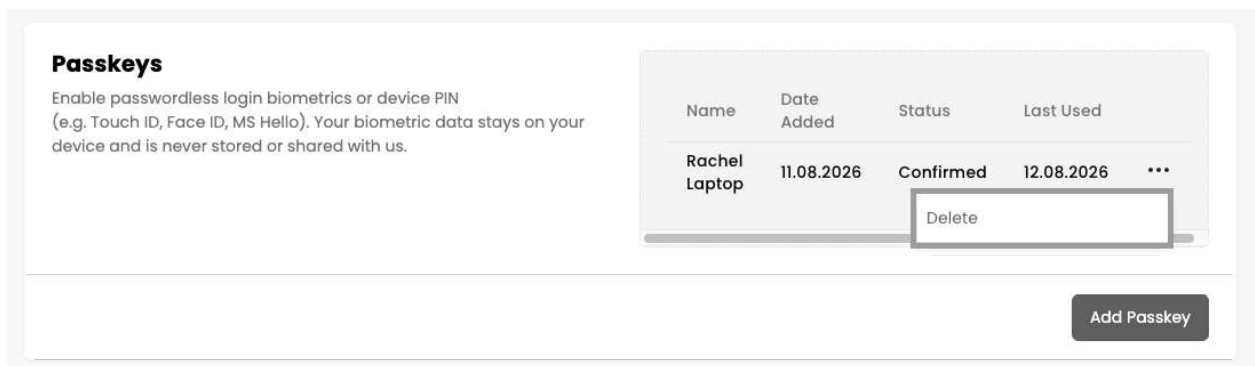
Passkey added successfully

However you chose to save it, you'll see a “Passkey added successfully” confirmation, and it's now ready to use as your verification step the next time you sign in.



Removing a Passkey

- Navigate to the Security section in Sprintax Identity.
- Scroll down to the **Passkey** section.
- Open the actions menu (the “...” beside the passkey)
- Select **Delete**.



- Confirm the deletion. Once confirmed, the passkey is removed and can no longer be used to sign in. If you cancel, the passkey stays active and nothing changes.

Troubleshooting

MFA not working?

If you are unable to complete MFA, one of the situations below may apply:

- Authenticator app was deleted: if you removed the app from your device without first disconnecting it from Sprintax Calculus, MFA will no longer work. Reinstalling the app and reconnecting will not resolve this.
- You switched devices: if you changed phones or tablets, your account may still be linked to the authenticator app on your previous device.

What to do in either case: contact Sprintax support. They can provide you with a special reset link, valid for 24 hours, to reset your MFA and set it up again.