

Multi-factor Authentication

A user guide to setting up your
account with Authy



What is Multi-Factor Authentication (MFA)?

- Multi-Factor Authentication (MFA) is an additional method of verification to the traditional username and password you currently use to login In-Form
- It is an additional layer of security to help protect your data
- It is a method you might already be using (i.e.: Online Banking login).
- Once MFA enabled, all users will only be able to login to In-Form using any of the authentication methods
- No Client or personal information will be stored on the phone used for MFA

What is changing?



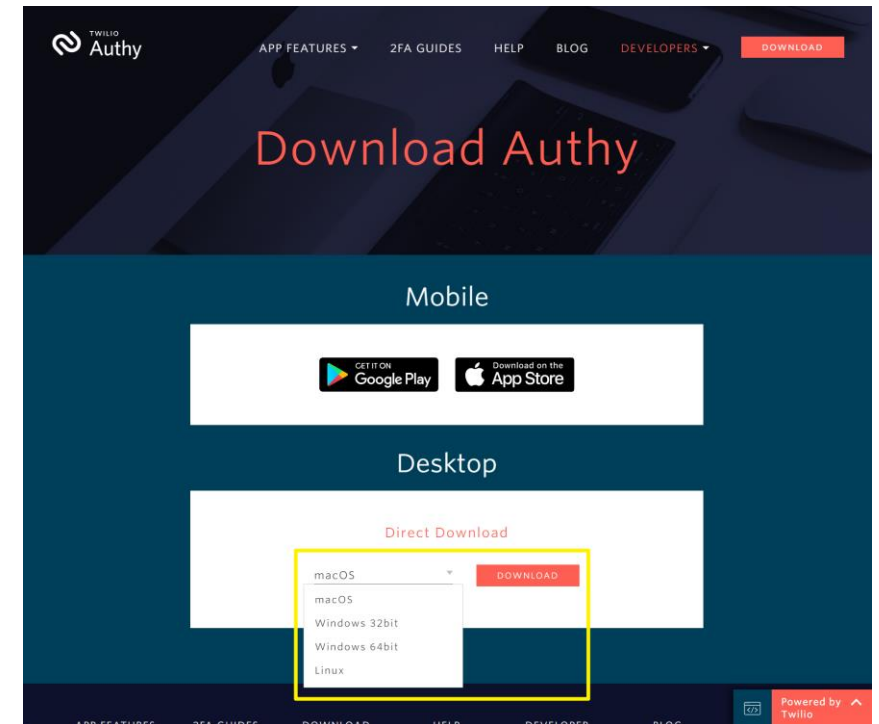
- To enable MFA you will need either your phone or desktop app to verify your login
- Verification must be via an app linked to their In-Form username (either on a smartphone, or desktop)

Setting up Authy – third party authenticator



1. MFA permission assigned (this will be done by System Administrator)
2. Log out of In-Form (When you next login you will be prompted to use a secondary authentication method)
3. Download the Authy desktop app from the Authy website: <https://authy.com/download/>

Select the download option that fits your organisation



Setting up Authy – third party authenticator



4. Follow the instructions on the Authy app to set up your Authy account.

Note: You will need to provide a phone number but this does not have to be a mobile number. You will also have to select the country identifier for the number, this is likely to be United Kingdom (+44).

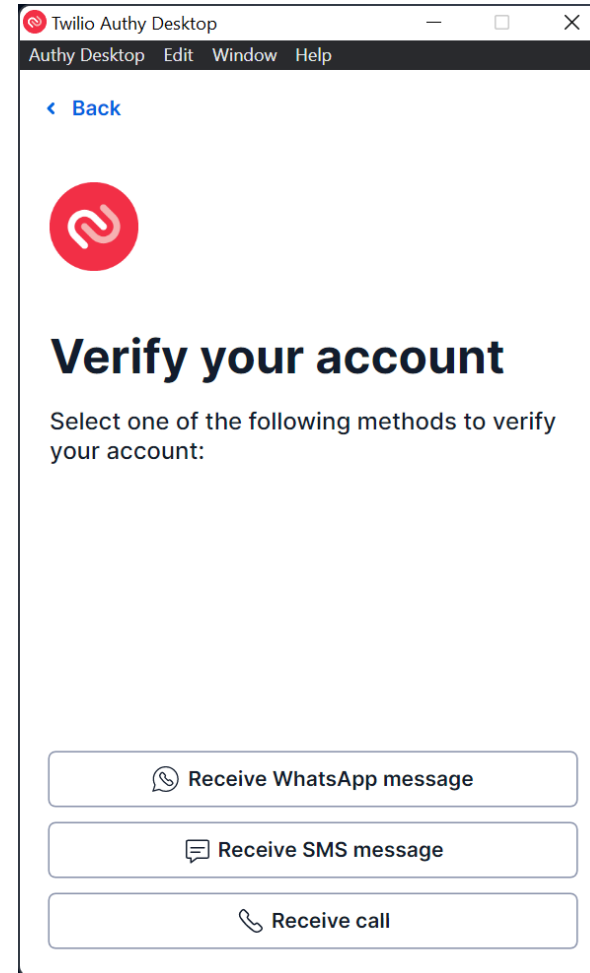
A screenshot of the Twilio Authy Desktop application window. The window title is 'Twilio Authy Desktop' and it has a menu bar with 'Authy Desktop', 'Edit', 'Window', and 'Help'. The main content area features the Authy logo (a red circle with a white 'A' icon) and the text 'Hi there,' followed by 'To get started, login or create an Authy account with your phone number.' Below this is a form with two input fields: 'Country code' with a dropdown menu showing '+44' and 'Phone number' with a text input field. A yellow rectangular box highlights these two fields. Below the form is a blue 'Submit' button. At the bottom, there is a small grey box with the text: 'By logging in or creating an account, you acknowledge that you read the [Privacy Notice](#).'

Setting up Authy – third party authenticator



5. After the number is entered you will; have to verify this number via either a WhatsApp message, SMS or phone call.

If you select WhatsApp you will receive a WhatsApp message with a code. If you select SMS then you will receive a SMS text message with a code. If you select phone call then your phone will ring and an automated voice will tell you the code.



Setting up Authy – third party authenticator



6. Once you have selected an option you need to enter the code into the verification box.

You are now ready to open Salesforce.

A screenshot of the Twilio Authy Desktop application window. The window title is 'Twilio Authy Desktop' and it has a menu bar with 'Authy Desktop', 'Edit', 'Window', and 'Help'. The main content area shows the Authy logo at the top, followed by the heading 'SMS message sent'. Below this, it says 'Enter the verification code we sent to' followed by a blurred phone number. There are six empty input boxes for the verification code. At the bottom, there are two buttons: 'Code can be resent in 24 seconds' and '← Use a different verification method'.

Setting up Authy – third party authenticator



7. Open your In-Form login page and enter your username and password to login.

You will be prompted to connect to the Salesforce Authenticator.

You need to select 'Choose Another Verification Method' located at the bottom of the window.

The image shows a screenshot of the 'Connect Salesforce Authenticator' screen. At the top is a blue padlock icon with a white checkmark. Below it is the title 'Connect Salesforce Authenticator'. A text box explains that for security, the user must connect the Salesforce Authenticator app, which sends notifications for verification. It lists three steps: 1. Download the app from the App Store or Google Play, 2. Open the app and tap to add the account, and 3. Enter the unique two-word phrase shown in the app. Below the text is a 'Two-Word Phrase' input field. At the bottom are 'Cancel' and 'Connect' buttons, and a link 'Choose Another Verification Method' which is highlighted with a yellow box.

Connect Salesforce Authenticator

For security reasons, you have to connect Salesforce Authenticator to your account. The app sends a notification when we need to verify your identity, and you verify with just a tap. You can also enable location services to have the app verify you automatically from trusted locations. The app provides codes to use as an alternate verification method.

1. Download Salesforce Authenticator from the [App Store](#) or [Google Play](#) and install it on your mobile device.
2. Open the app and tap to add your account.
3. The app shows you a unique two-word phrase. Enter the phrase below.

Two-Word Phrase

[Choose Another Verification Method](#)

Setting up Authy – third party authenticator



8. Select 'Use verification codes from an authenticator app'.

A screenshot of the Salesforce authentication interface. At the top is the Salesforce logo (a blue cloud with the word 'salesforce' in white). Below it is the heading 'Choose a Verification Method'. A white box contains the question 'How would you like to verify your identity?'. There are two radio button options: 'Use the Salesforce Authenticator mobile app' (unselected) and 'Use verification codes from an authenticator app' (selected and highlighted with a yellow border). Below the options is a blue 'Continue' button.

salesforce

Choose a Verification Method

How would you like to verify your identity?

☐ Use the Salesforce Authenticator mobile app

☒ Use verification codes from an authenticator app

Continue

Setting up Authy – third party authenticator



9. You will be shown a QR code that can be scanned on your mobile.

Authy is a desktop app so select 'I Can't Scan the QR Code' at the bottom of the window.

The image shows a screenshot of the Salesforce 'Connect an Authenticator App' interface. At the top is the Salesforce logo. Below it is the title 'Connect an Authenticator App'. The main text explains that the user should connect an authenticator app that generates verification codes. A list of three steps is provided: 1. Download and install an authenticator app on your mobile device. 2. Use the app to scan this QR code. 3. Enter the code generated by the app. A QR code is displayed in the center. Below the QR code is a 'Verification Code' input field. At the bottom are 'Back' and 'Connect' buttons. A yellow box highlights the link 'I Can't Scan the QR Code' at the very bottom, with the text 'Choose Another Verification Method' underneath it.

salesforce

Connect an Authenticator App

Connect an authenticator app that generates verification codes. You can use the codes when we need to verify your identity.

1. Download and install an authenticator app on your mobile device.
2. Use the app to scan this QR code.
3. Enter the code generated by the app.

Verification Code

[Back](#) [Connect](#)

[I Can't Scan the QR Code](#)
Choose Another Verification Method

Setting up Authy – third party authenticator



10. You will then be shown a key that needs to be copied and pasted into the Authy app.

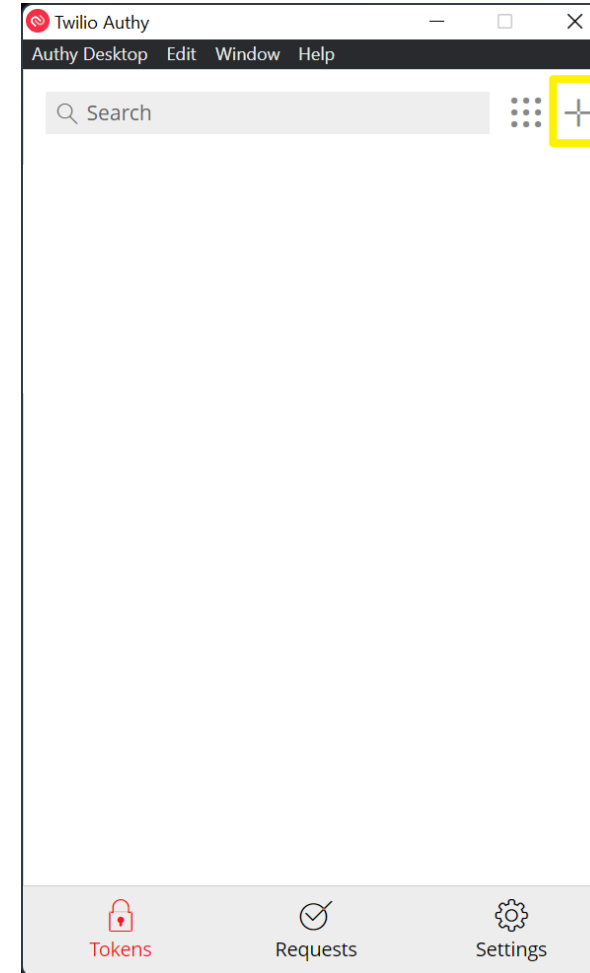
You can manually copy this if you are more comfortable with that.

A screenshot of the Salesforce 'Connect an Authenticator App' interface. At the top is the Salesforce logo. Below it is the title 'Connect an Authenticator App'. The main content area contains instructions: 'On your mobile device, go to the authenticator app and enter this key.' followed by 'Some versions of Salesforce Authenticator don't support manual key entry. Use a different app, or contact your Salesforce administrator for help.' Below this is a yellow-bordered box labeled 'Key' containing the text 'MUP7KHCSNGAIAY5KB6Y2HXHFNUETD3Y5'. Underneath the box, it says 'Now enter the verification code your app displays.' followed by a 'Verification Code' label and an empty input field. At the bottom are two buttons: 'Back' and 'Connect'.

Setting up Authy – third party authenticator



11. In Authy, select the + icon in the top right corner of the app.



Setting up Authy – third party authenticator



12. Paste the Key from step 10 into the field and select 'Add Account'.

A screenshot of the Twilio Authy desktop application window. The window has a title bar with 'Twilio Authy' and standard OS controls. Below the title bar is a menu bar with 'Authy Desktop', 'Edit', 'Window', and 'Help'. The main content area shows a red back arrow and the text 'Add Account'. Below this is a paragraph explaining that accounts can be added via email, Facebook, or Dropbox, but QR codes are not supported; instead, users must enter a code. A yellow rectangular box highlights the input field labeled 'Enter Code given by the website', which contains the example text 'i.e: sw3g lkzc rt2d pnwo as3k uysd wisd'. Below the input field is a red 'Add Account' button. At the bottom of the window is a navigation bar with three icons: a padlock for 'Tokens', a checkmark for 'Requests', and a gear for 'Settings'.

Setting up Authy – third party authenticator



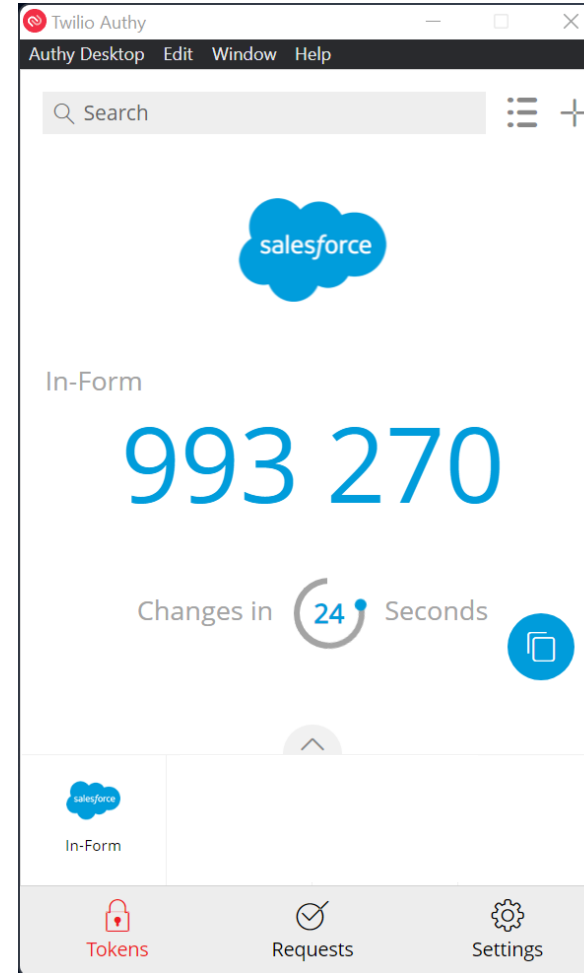
13. Enter a name for the account (such as 'In-Form') and select Salesforce from the list below. Then select 'Save' to finalise the account connection.

A screenshot of the Twilio Authy Desktop application window. The window title is 'Twilio Authy' and it has a menu bar with 'Authy Desktop', 'Edit', 'Window', and 'Help'. The main content area is titled 'Account Name and Logo' with a back arrow. Below this is a text input field containing 'In-Form', which is highlighted with a yellow border. Underneath is a list of service providers: Rackspace, RelateIQ, Salesforce (selected with a green checkmark), Slack, Snapchat, and Stripe. At the bottom of the list is a 'Token length' section with radio buttons for '6-digit' (selected), '7-digit', and '8-digit'. Below the list are two buttons: a red 'Save' button and a red 'Delete' link. The bottom of the window has a navigation bar with three icons: 'Tokens' (a padlock), 'Requests' (a checkmark), and 'Settings' (a gear).

Setting up Authy – third party authenticator



14. Authy will then show you a code and a timer for how long that code is valid. This is what you need as the secondary verification for Salesforce.



Setting up Authy – third party authenticator



15. Go back to your In-Form login screen and enter the verification code from Authy. Select connect and you should have access to In-Form.

Note: Be aware of the time limits on the Authy codes and ensure there is enough time left with the code you are using.

The image shows a screenshot of the Salesforce 'Connect an Authenticator App' screen. At the top is the Salesforce logo. Below it, the title 'Connect an Authenticator App' is displayed. The main content area contains instructions: 'On your mobile device, go to the authenticator app and enter this key.' followed by 'Some versions of Salesforce Authenticator don't support manual key entry. Use a different app, or contact your Salesforce administrator for help.' Below this, the word 'Key' is followed by the key 'MUP7KHCSNGAIAY5KB6Y2HXHFNUETD3Y5'. A horizontal line separates this from the next section, which says 'Now enter the verification code your app displays.' Below this is a 'Verification Code' input field with the code '993270' entered. The input field is highlighted with a yellow border. At the bottom are two buttons: 'Back' and 'Connect'.

Using multi-device with

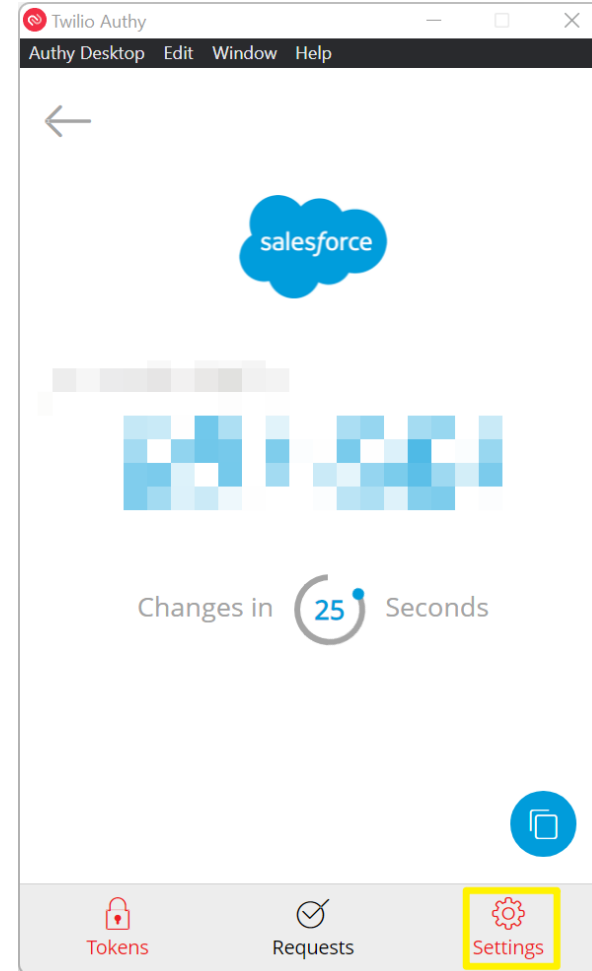
Authy



Setting up multi-device



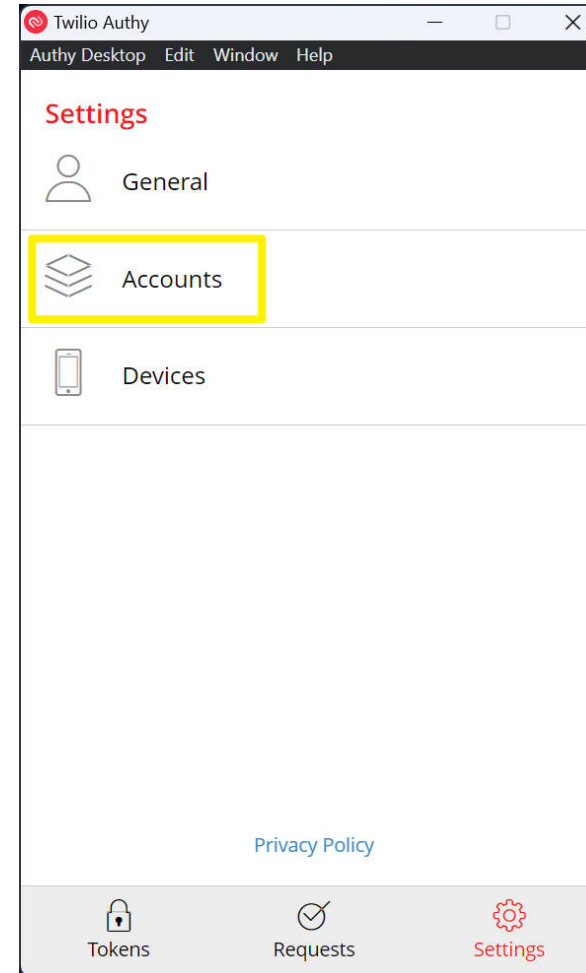
1. With the Authy app open select 'Settings' from the navigation bar at the bottom.



Setting up multi-device



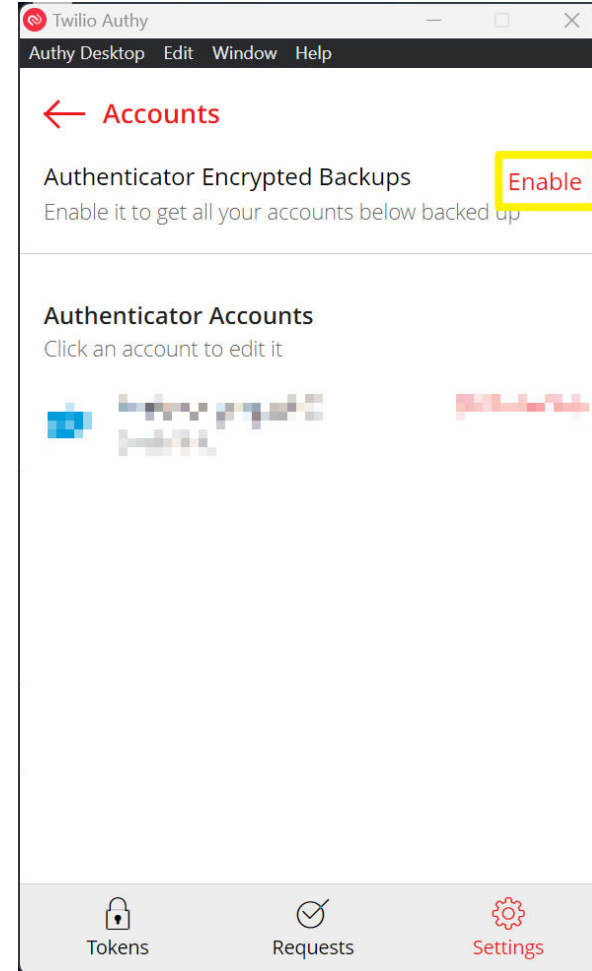
2. Select 'Accounts' from the following menu.



Setting up multi-device



3. Select 'Enable' next to Authenticator Encrypted Backups.

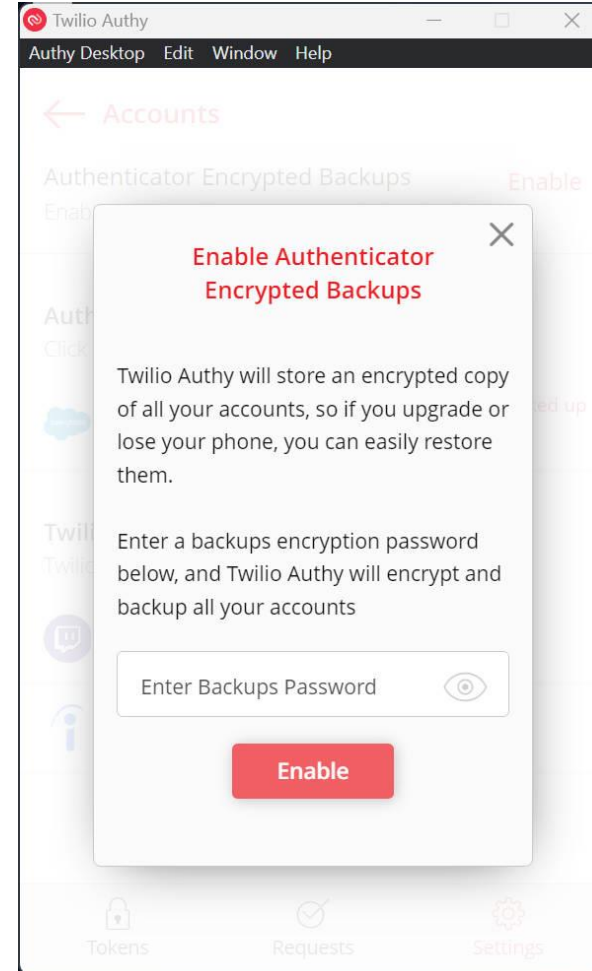


Setting up multi-device



4. Enter a password to enable backups and select the 'Enable' button.

Note: In-Form does not have access to this password and cannot reset it. Please ensure the password is memorable enough to remember.

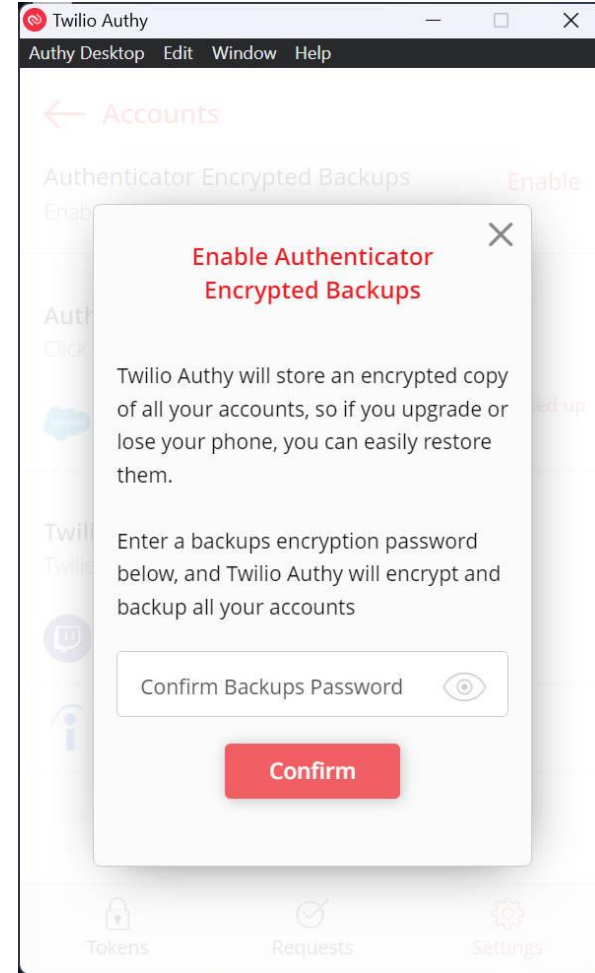


Setting up multi-device



5. Enter your password again from step 4 and select the 'Confirm' button.

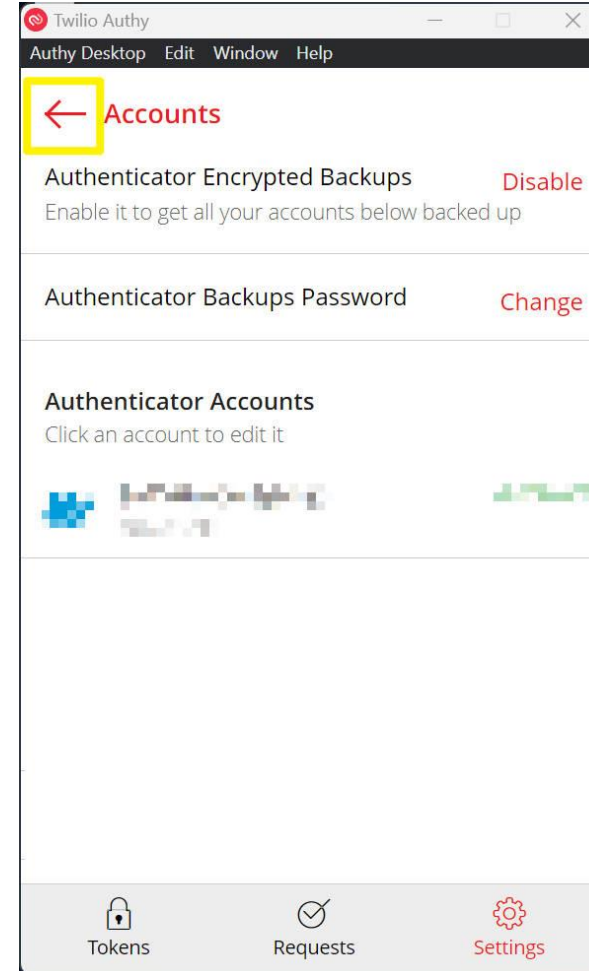
Note: In-Form does not have access to this password and cannot reset it. Please ensure the password is memorable enough to remember.



Setting up multi-device



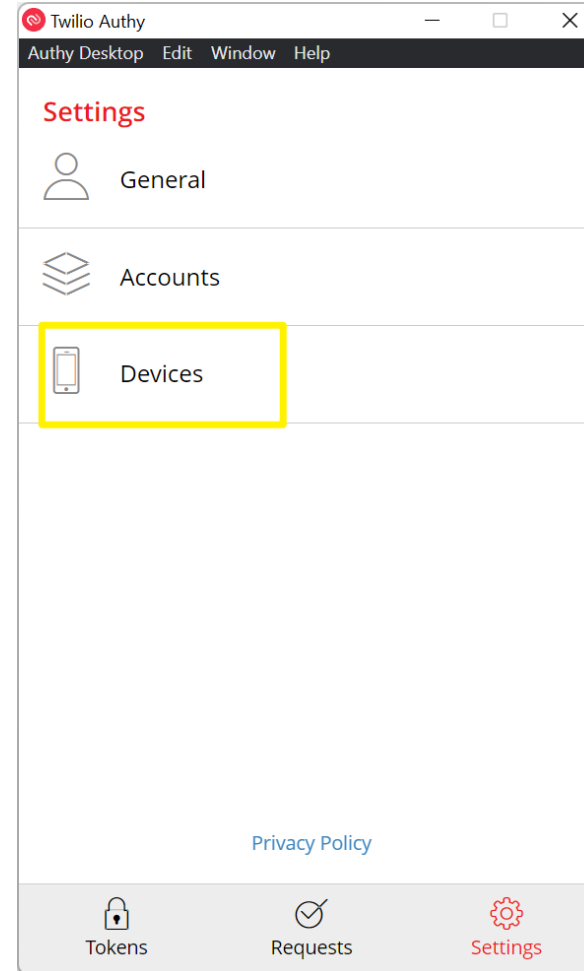
6. Select the back button at the top of the page.



Setting up multi-device



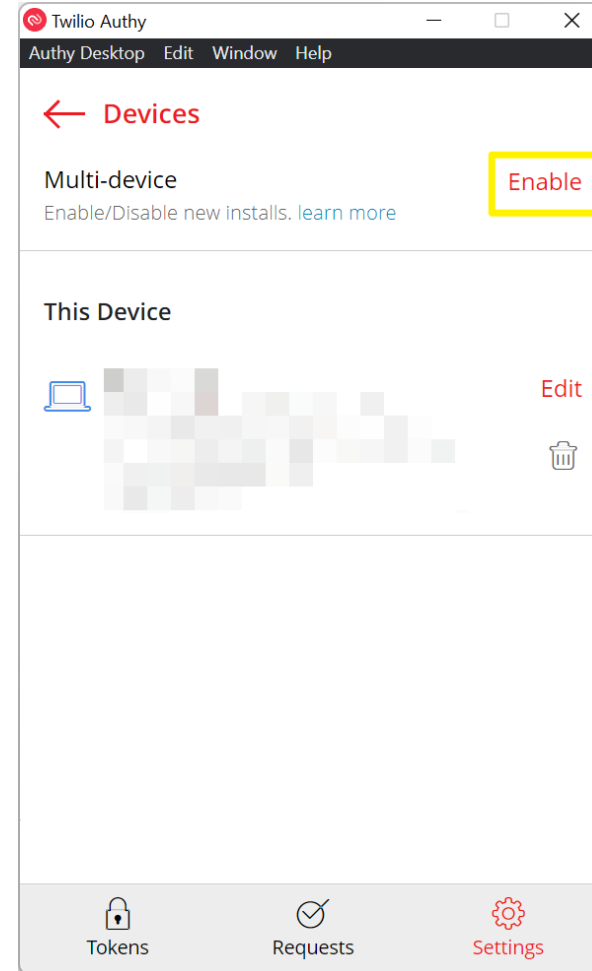
7. Select 'Devices' from the following menu.



Setting up multi-device



8. Select 'Enable' next to Multi-device.



Setting up multi-device



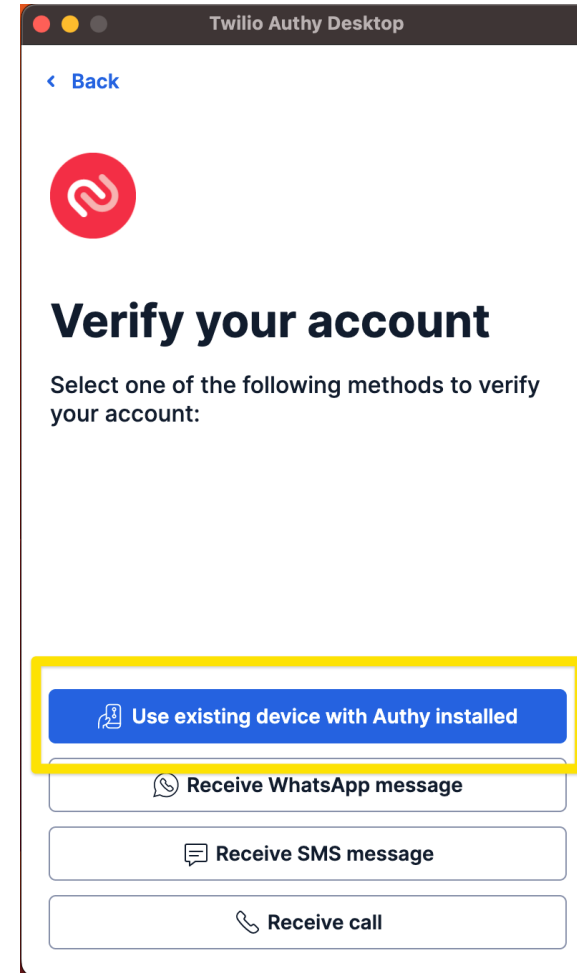
9. Install Authy on your second desktop device. Download the Authy desktop app from the Authy website: <https://authy.com/download/>
10. Once installed enter the phone number you used to set up Authy on your first desktop.

A screenshot of the Twilio Authy Desktop application window. The window title is 'Twilio Authy Desktop'. The menu bar includes 'Authy Desktop', 'Edit', 'Window', and 'Help'. The main content area features the Authy logo, the text 'Hi there,', and instructions: 'To get started, login or create an Authy account with your phone number.' Below this is a form with two input fields: 'Country code' (containing '+44') and 'Phone number' (containing a vertical bar). A yellow rectangular box highlights these two input fields. Below the form is a blue 'Submit' button. At the bottom, a light gray box contains the text: 'By logging in or creating an account, you acknowledge that you read the [Privacy Notice](#).'

Setting up multi-device



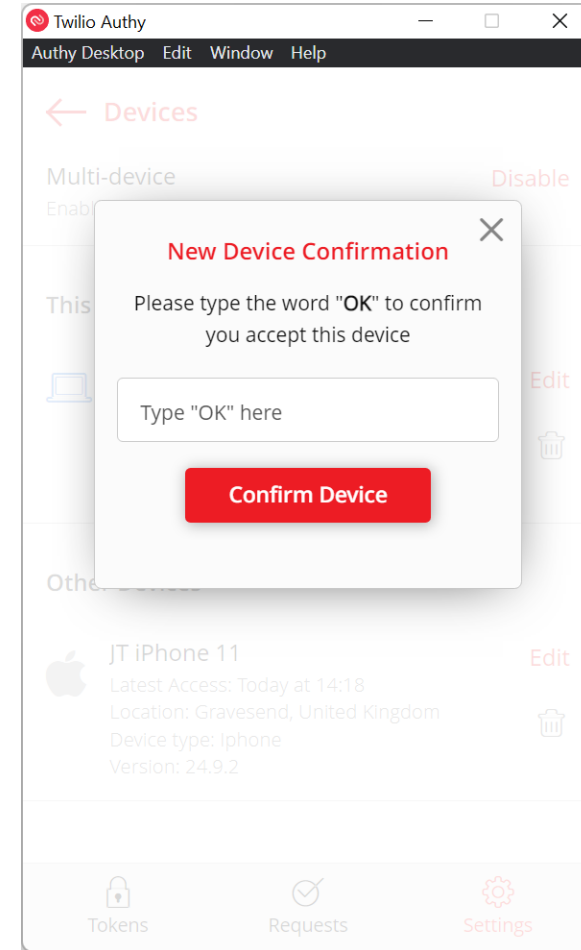
11. On the next screen select 'Use existing device with Authy installed'.



Setting up multi-device



12. Back on your first desktop, you should see a prompt to approve the new device. Type 'OK' into the field and select 'Confirm Device'.

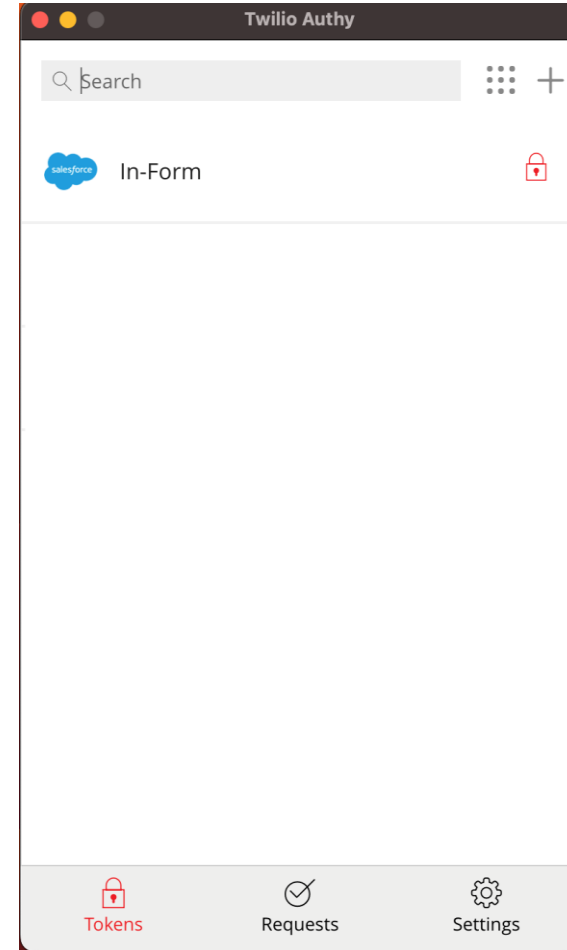


Setting up multi-device



13. You should now see the In-Form option on your second desktop Authy app.

You can now use Authy on either desktop to generate a validation code to log into In-Form.



Setting up multi-device



Note: Authy multi-device can be set up on more than 2 devices.

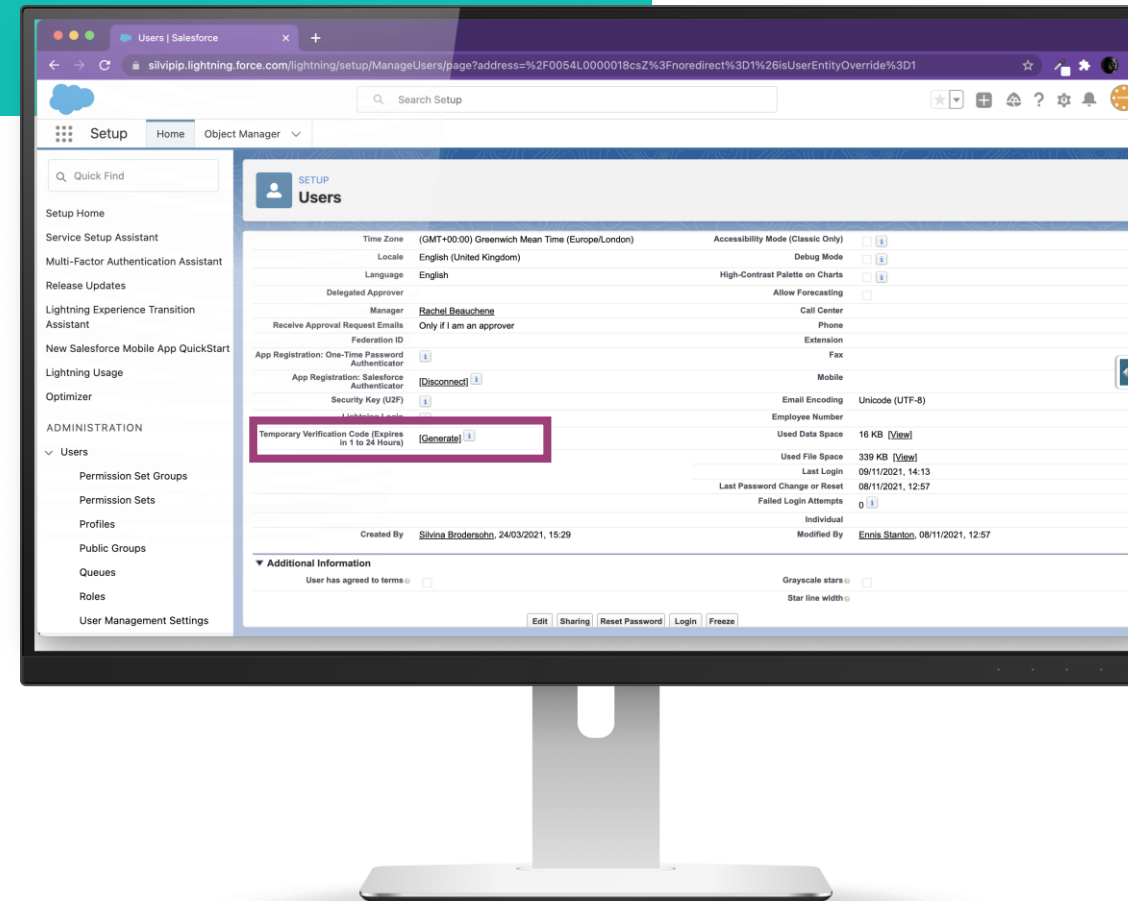
To set up any additional devices please follow steps 9 – 13 from the previous section.

What happens if you cannot access your app for validating your identity?

“I can't access my app”

Email your Key Contact or our Support team, they can create a temporary password for you to use and log in.

You will receive an email with a code valid for a specific period of time for you to access your In-Form account



The complete **client relationship**
and **service management** solution.

-  www.in-form.org.uk
-  inform.sales@homelesslink.org.uk
-  [In_FormUK](#)
-  [In-Form](#)
-  Raise a case from your In-Form system