

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?



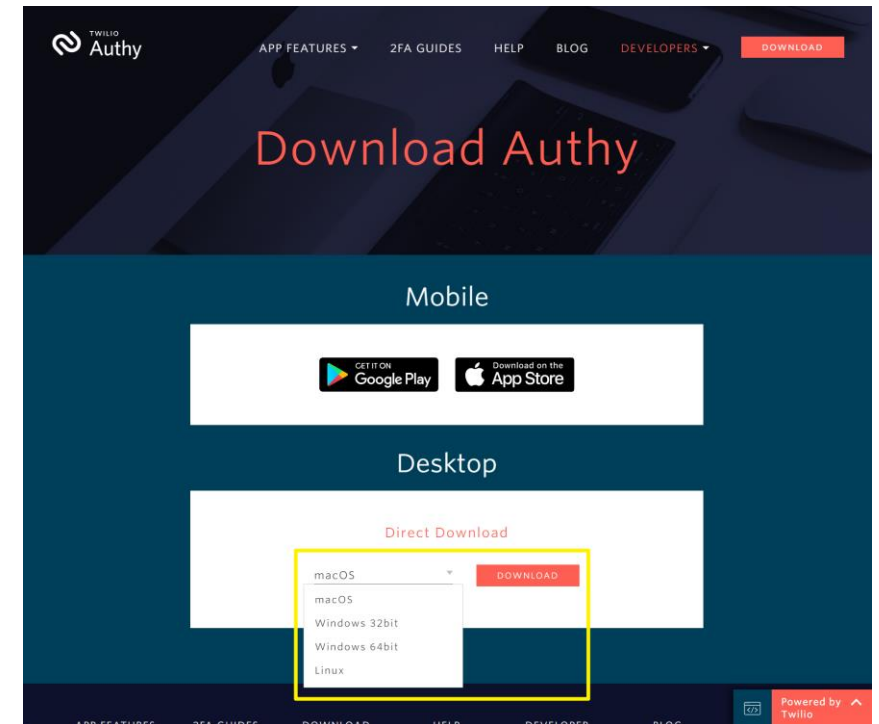
- To enable MFA you will need either your phone or desktop app to verify your login
- Verification must be via an app linked to their In-Form username (either on a smartphone, or desktop)

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).

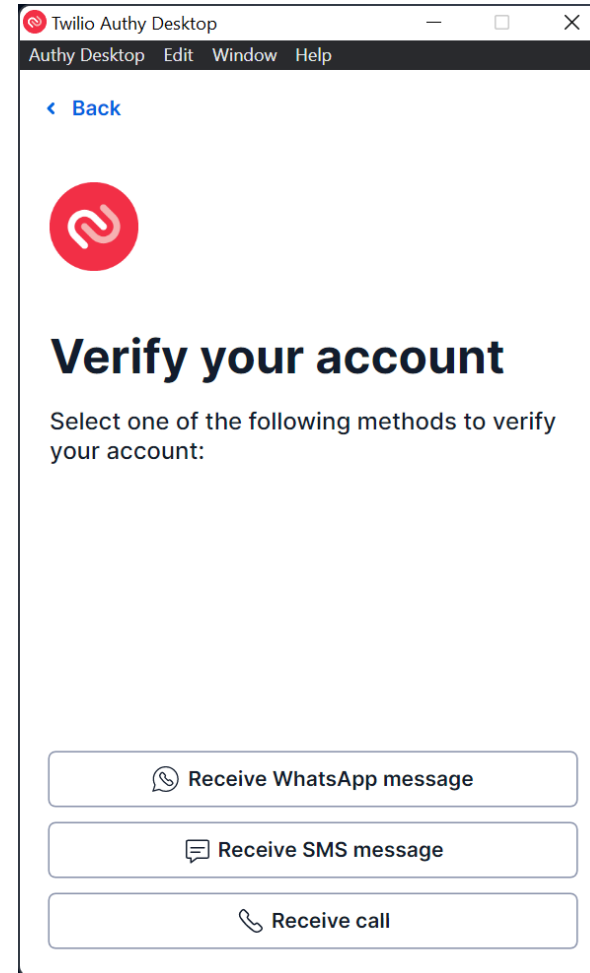
A screenshot of the Twilio Authy Desktop application window. The window title is 'Twilio Authy Desktop'. The interface shows the Authy logo, the text 'Hi there,', and instructions to login or create an account with a phone number. There are two input fields: 'Country code' with '+44' and 'Phone number' which is empty. A yellow rectangular box highlights these two input fields. Below the fields is a blue 'Submit' button. At the bottom, there is a small grey box with 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'. The menu bar includes 'Authy Desktop', 'Edit', 'Window', and 'Help'. The main content area features 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'.

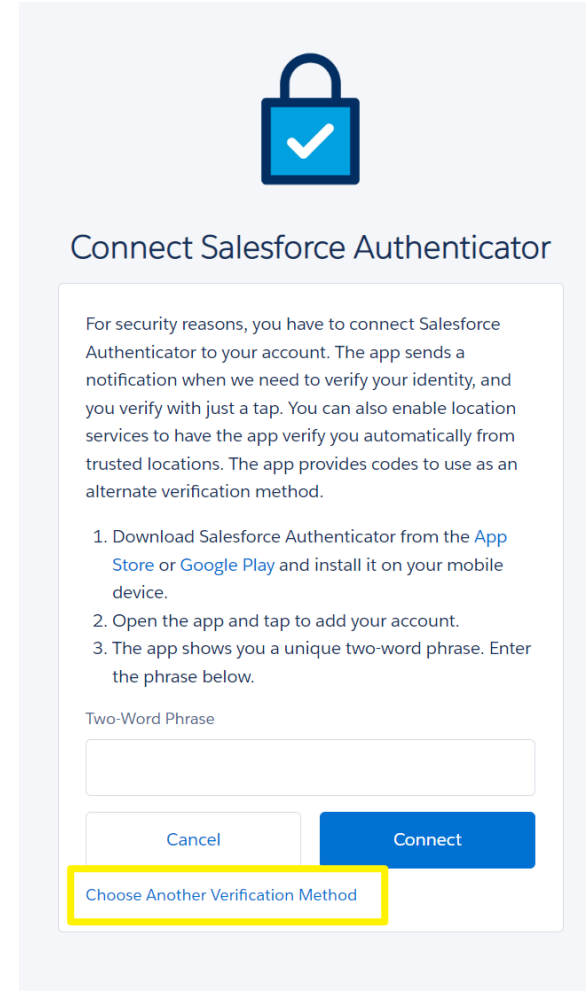
Setting up Authy – third party authenticator



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.

A screenshot of the 'Connect Salesforce Authenticator' window. At the top is a blue padlock icon with a white checkmark. Below it is the title 'Connect Salesforce Authenticator'. The main text explains that for security, the user must connect the Salesforce Authenticator app to their account, which sends notifications for verification. It lists three steps: 1. Download the app from the App Store or Google Play and install it. 2. Open the app and tap to add the account. 3. The app shows a unique two-word phrase, which the user must enter. Below the text is a 'Two-Word Phrase' input field. At the bottom are two buttons: 'Cancel' and 'Connect'. A yellow box highlights a link at the very bottom that says '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'. Underneath is a white box containing the question 'How would you like to verify your identity?'. There are two radio button options: 'Use the Salesforce Authenticator mobile app' (which is unselected) and 'Use verification codes from an authenticator app' (which is selected and highlighted with a yellow border). Below these options is a blue button labeled '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 says: 'Connect an authenticator app that generates verification codes. You can use the codes when we need to verify your identity.' Below this are three numbered steps: 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 two buttons: 'Back' and 'Connect'. Below the 'Back' button is a link that says 'I Can't Scan the QR Code' (highlighted with a yellow box in the original image) and '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.

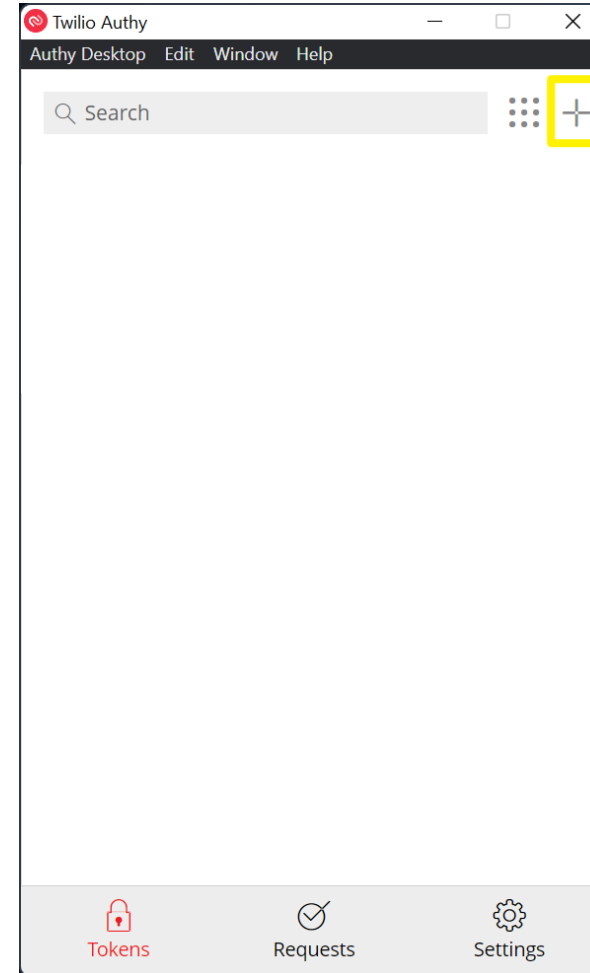
You can manually copy this if you are more comfortable with that.

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 title is 'Twilio Authy' and it has a menu bar with 'Authy Desktop', 'Edit', 'Window', and 'Help'. The main content area is titled 'Add Account' with a back arrow. Below the title, there is a paragraph of text: 'You can add Authenticator accounts such as Gmail, Facebook, Dropbox and many more using Twilio Authy. For the time being it is not possible to scan QR codes, but you can add accounts by entering the code provided by the service in which you want to enable 2FA.' Below this text is a text input field with a yellow border, containing the text 'i.e: sw3g lkzc rt2d pnwo as3k uysd wisd'. Below the input field is a red button labeled 'Add Account'. 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



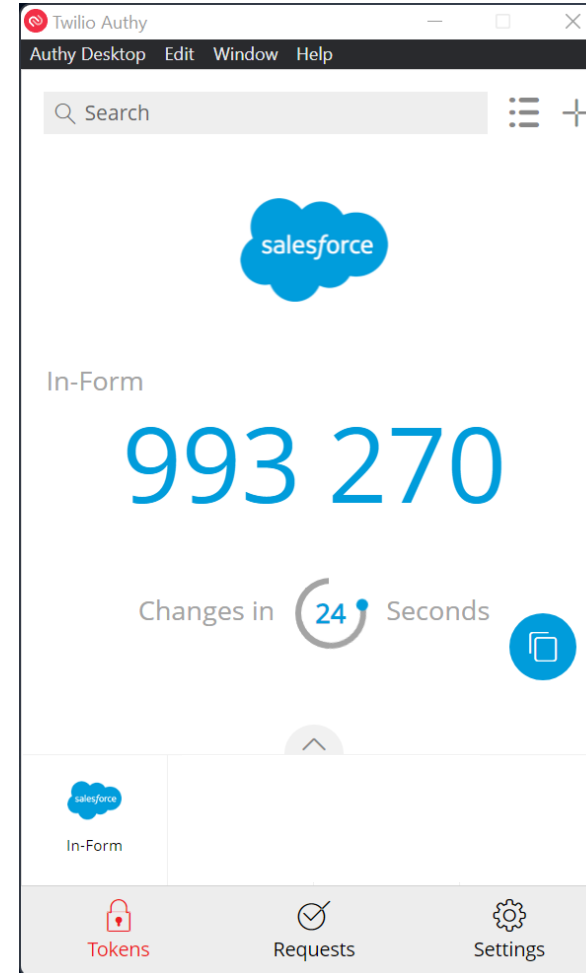
13. Enter a name for the account (such as 'In-Form') and select Salesforce from the list below. Then select 'Save' to finalise the account connection.

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. At the very bottom is a navigation bar with three icons: 'Tokens' (a lock), '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 In-Form.



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.

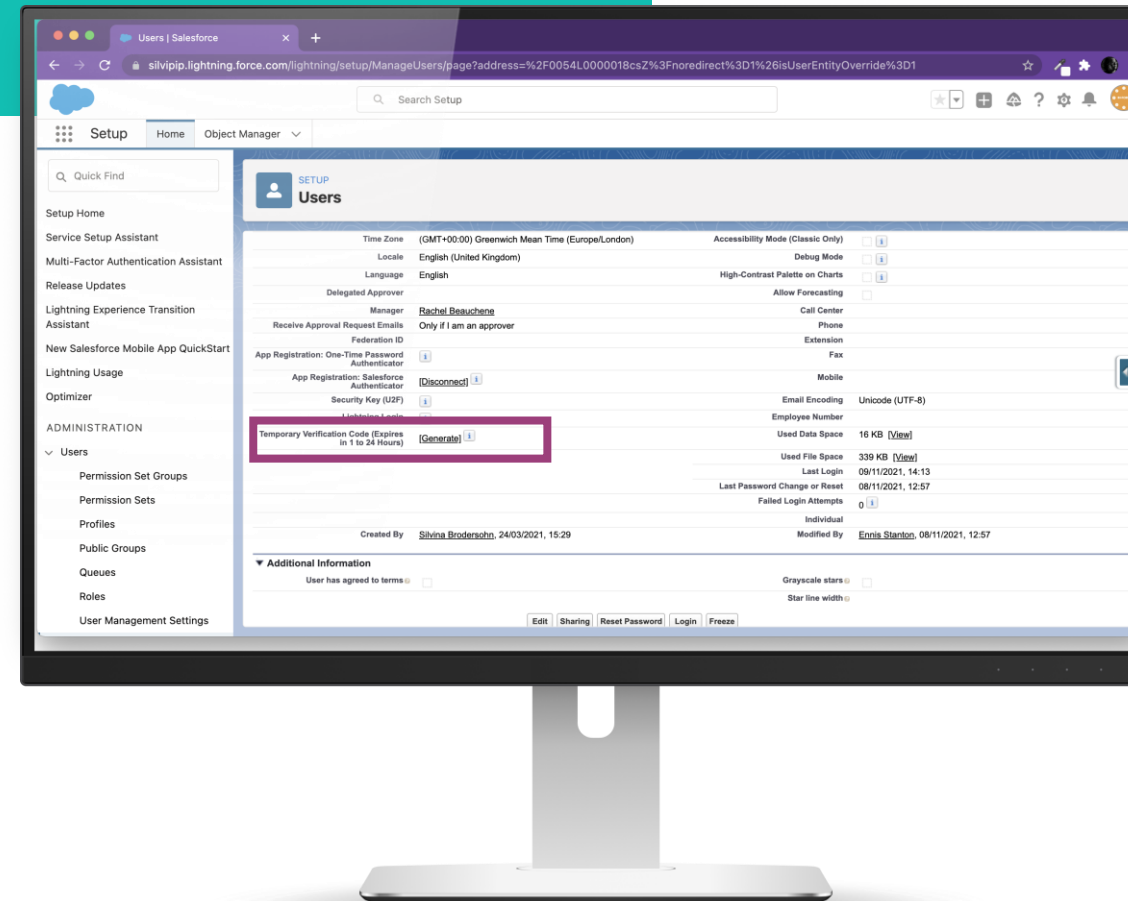
The image shows a screenshot of the Salesforce 'Connect an Authenticator App' screen. At the top is the Salesforce logo. Below it, the title 'Connect an Authenticator App' is displayed. The main content area contains instructions: 'On your mobile device, go to the authenticator app and enter this key.' followed by a note: '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'. Then, it says 'Now enter the verification code your app displays.' followed by a 'Verification Code' input field containing '993270'. At the bottom are two buttons: 'Back' and 'Connect'.

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