INTRODUCTION

Two factor authentication (or 2FA) is a two step verification process that provides an extra layer of security for you when accessing your account within online services.

The benefits of 2FA are a higher level of protection for your Online Services account and the data held within it. This is because 2FA reduces the risk of an intruder gaining access to it.

2FA is free and Nominet has used **RFC 6238** for implementing 2FA which is based on time based passcodes.

SIGN UP TO THE TWO-FACTOR AUTHENTICATION (2FA) SERVICE

Before you start

You need to decide which device you will use to generate your 2FA. The Google Authenticator is widely used and recommended by Nominet. Another frequently used application is Authy apps.

The device could be a smartphone, tablet, laptop or PC.

The following steps in this user guide walk you through the Google Authenticator process.

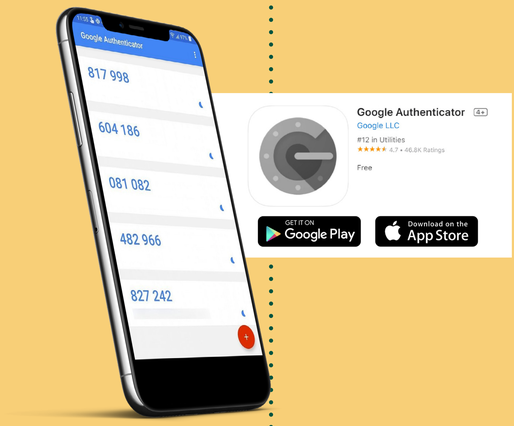
We advise you to set your device to Automatic Time Updates if available. You can usually find this option under 'Settings / Date & Time'.

GOOGLE AUTHENTICATOR

1

We recommend that you start by **downloading Google Authenticator** on your chosen device:

- Open the relevant app store
- Search for and download Google Authenticator. If you are using a Windows phone, search for 'Authenticator'



2

Open Google Authenticator

- Enter 'account' name - we suggest Nominet Online Services
- Enter the set up key from Online Services

3

Scan the **QR code** from Online Services

The account will be set up as Nominet Online Services

4

Get your passcode

Open Google Authenticator and select the Nominet account

Your one-time passcode is displayed: e.g. 123456

ONLINE SERVICES

1

Introducing 2FA

- Click **Yes** to set up Two-factor authentication on your account

2

Download Google Authenticator app or plugin

You should now have a Google Authenticator app or plugin on your chosen device

3

Device set up

- Your 2FA set-up key is generated: e.g. 12345C7891B3456A

- Name your device so you can easily identify it within Online Services later e.g. Richard's smartphone
- Click **next**

4

Complete 2FA set-up

You will be prompted to enter your 6 digit **passcode...**

5

Enter your **6 digit passcode** e.g. 123456 & click **'Activate 2FA'**

Welcome to Online Services

SETTING UP YOUR ACCOUNT

in Google Authenticator

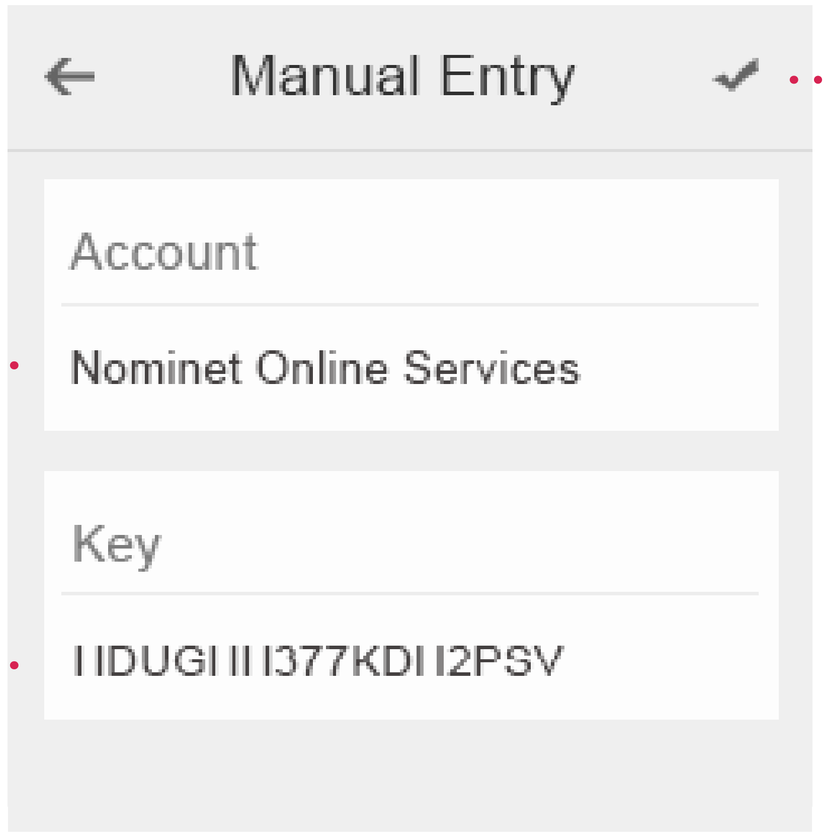
1

Enter a name for your account.

We suggest Nominet Online Services so you can easily find us again.

2

Enter the 16 character set up key which has been generated in Online Services



3

Select ‘Done’

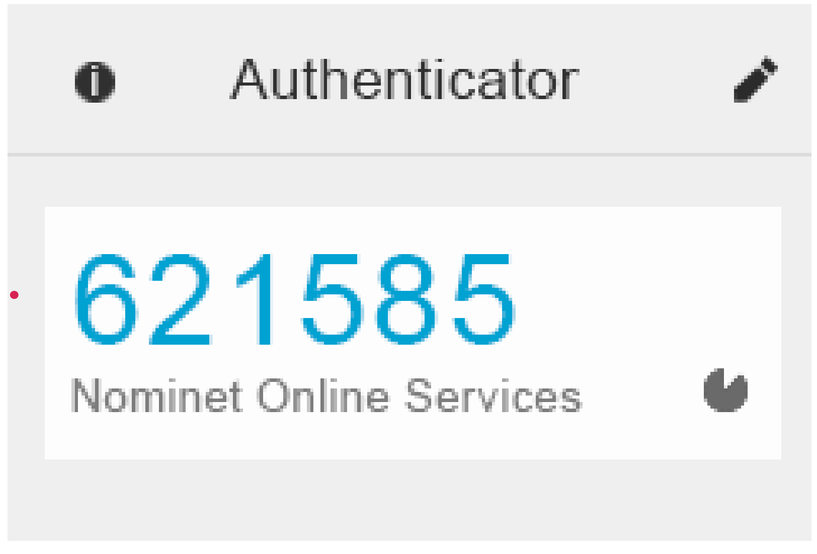
Alternatively you can scan the QR code from Online Services into your device.

The account name will automatically be set up as Nominet Online Services

4

Google Authenticator will now generate a new 6 digit passcode every 30 seconds.

Use this to complete your 2FA set up process and when you log in to Online Services in future



TIP

We advise you to set your device to Automatic Time Updates.

LOG IN TO ONLINE SERVICES

Using Two-factor authentication

Use this process whenever you log into Online Services in future.

1

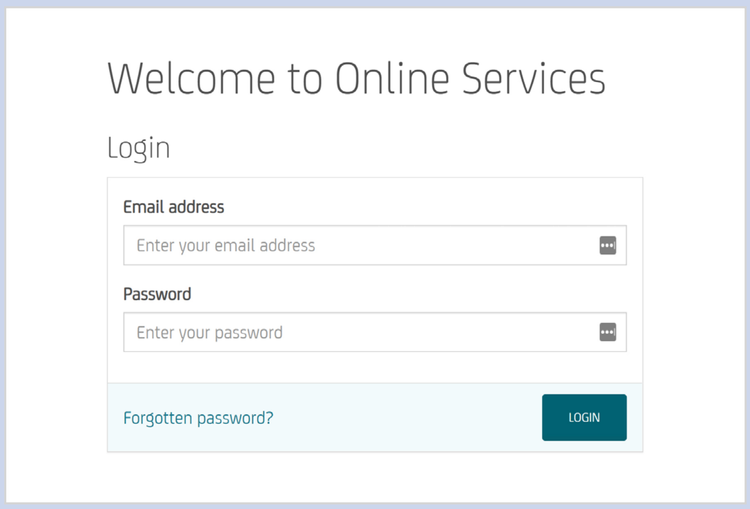
Start here

2

Online Services

3

Enter your email and password



4

You will be prompted to enter your 6 digit 2FA passcode

GO TO YOUR DEVICE

5

Get your passcode

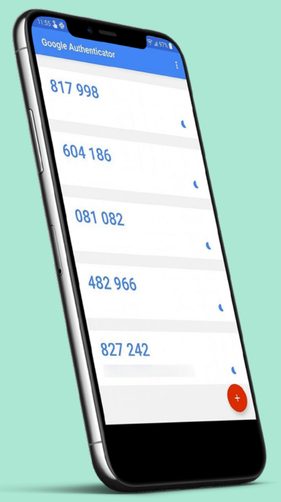
Open Google Authenticator and select the Nominet account

Your one-time passcode is displayed: e.g. 123456

GO TO ONLINE SERVICES

6

Enter 2FA passcode: e.g. 123456



Welcome to Online Services

ADD A NEW DEVICE

You need to know which device you plan to add.

The device could be a smartphone, tablet, laptop or PC.

The following steps walk you through the Google Authenticator process.

TIP

To replace a device simply follow the steps for:

a) Delete a device

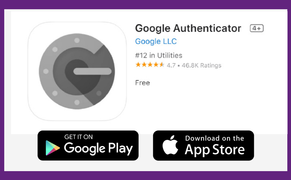
b) Add a new device

GOOGLE AUTHENTICATOR

1

We recommend that you start by **downloading Google Authenticator** on your chosen device:

- Open the relevant app store
- Search for and download Google Authenticator. If you are using a Windows phone, search for 'Authenticator'



2

Open Google Authenticator

- Enter 'account' name - we suggest Nominet Online Services
- Enter the set up key from Online Services

3

Scan the **QR code** from Online Services

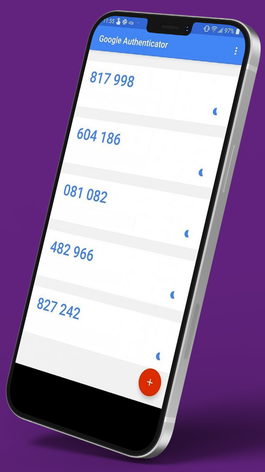
The account will be set up as Nominet Online Services

4

Get your passcode

Open Google Authenticator and select the Nominet account

Your one-time passcode is displayed: e.g. 123456



ONLINE SERVICES

ADD A DEVICE

1 **Login to Online Services using Two-factor authentication**

2 **Go to 'Login Settings'**

3 **Select 'Manage Two-factor authentication devices'**

4 **Select 'Add/manage devices'**

5

Device set up

- Your 2FA set-up key is generated: e.g. 12345C7891B3456A
- Name your device so you can easily identify it within Online Services later e.g. Richard's smartphone
- Click **next**

6

Complete Two-factor authentication set-up

You will be prompted to enter your 6 digit **passcode...**

7 Enter your **6 digit passcode** e.g. 123456 & click **'Activate 2FA'**

DELETE A DEVICE

1 **Login to Online Services using Two-factor authentication**

2 **Go to 'Login Settings'**

3 **Select 'Manage Two-factor authentication devices'**

4 **Select 'Delete device'**

5 **Select the device to be deleted e.g.: John's smartphone**

6 **Click delete button and confirm**

Welcome to Online Services

GLOSSARY

2FA or Two-Factor Authentication

2FA is a two step verification process which provides an extra layer of security for you when accessing your account within Online Services.

2FA passcode

A time-limited 6 digit code generated by the Google Authenticator app or plugin and which is needed alongside your username and password each time you log into Online Services if you have signed up for the 2FA service. The Google Authenticator app or plugin generates a new, unique passcode every 30 seconds.

2FA set-up key

Referred to as the ‘secret key’ in Google Authenticator, this 16 character code links the device which hosts your 2FA app or plugin with Online Services.

Contact email

The email address you use to log into Online Services.

Google Authenticator

The 2FA app or plugin that is used to implement 2FA within Nominet Online Services.

Password

The password you use to log into Online Services.

Passphrase

The additional passphrase you may have set up (that you use) to log into Online Services once you have entered your username and password.

The passphrase provides an additional layer of security when logging into Online Services, but 2FA improves on this by requiring the user to generate a passcode on a separate device.