Two Factor Authentication - USER GUIDE

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 optional and is provided at no extra cost.

Content

Sign up to the Two Factor Authentication service

Before you start

Decide which device you will install Google Authenticator on. You will use Google Authenticator in future to generate your 2FA passcode whenever you log in to Online Services.

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

We support:

- Google Authenticator app on iOS for the iPhone/iPad
- Google Authenticator app for Android devices
- Google Authenticator app for Blackberry devices
- Microsoft Windows Authenticator app for Windows 8 devices
- Google Authenticator plug-in for the Firefox browser

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

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'

Go to Online Services

Open Google Authenticator

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

Click here to see an example

OR

Scan the **QR code** from Online Services

The account will be set up as Nominet Online Services

Get your passcode

- Open Google Authenticator and select the Nominet account

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

Online Services

Would you like to sign up for 2 Factor Authentication? *

* If you do not see this message, go to 'Login settings' in Online Services and select Two-Factor Authentication – 'Add/manage devices'

Step 1 – Introducing 2FA

Click **Yes** to set up 2 Factor Authentication on your account

Step 2 – Download Google Authenticator app or plugin

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

Go to your device

Step 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**

Step 4 – Complete 2FA set-up

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

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

Welcome to Online Services

Back to main contents

Setting up your account in Google Authenticator

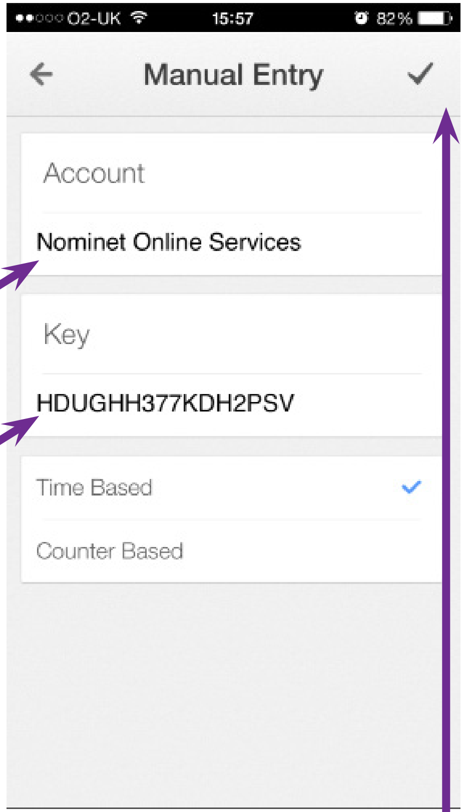
Google Authenticator

Enter a name for your account.

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

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

Select ‘Done’



Account

Nominet Online Services

Key

HDUGHH377KDH2PSV

Time Based ✓

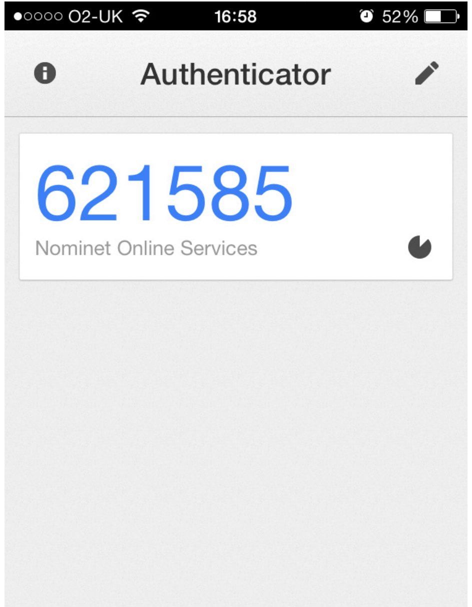
Counter Based

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*

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



621585

Nominet Online Services

Tip

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

Back to main contents

Log in to Online Services using Two Factor Authentication

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

Start here...

Online Services

Enter your email and password

Click to log in

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

Go to your device

Google Authenticator
- installed on a device of your choice

Get your passcode

- Open **Google Authenticator** and select the Nominet Account

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

Go to Online Services

Enter 2FA **passcode**:
e.g. 123456

Welcome to Online Services

Back to main contents

Add a new device

Before you start

You need to know which device you plan to add.

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

We support:

- Google Authenticator app on iOS for the iPhone/iPad
- Google Authenticator app for Android devices
- Google Authenticator app for Blackberry devices
- Microsoft Windows Authenticator app for Windows 8 devices
- Google Authenticator plug-in for the Firefox browser

Tip

To **replace a device** simply follow the steps for:

a) Delete a device

b) Add a new device

Google Authenticator

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'

Go to Online Services

Open Google Authenticator

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

Click here to see an example

OR

Scan the **QR code** from Online Services

The account will be set up as Nominet Online Services

Get your passcode

- Open Google Authenticator and select the Nominet account

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

Online Services

Login to Online Services using 2 Factor Authentication

Go to 'Login Settings'

Select 'Manage 2 Factor Authentication devices'

Select 'Add/manage devices'

Go to your device

Step 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**

Step 4 – Complete 2FA set-up

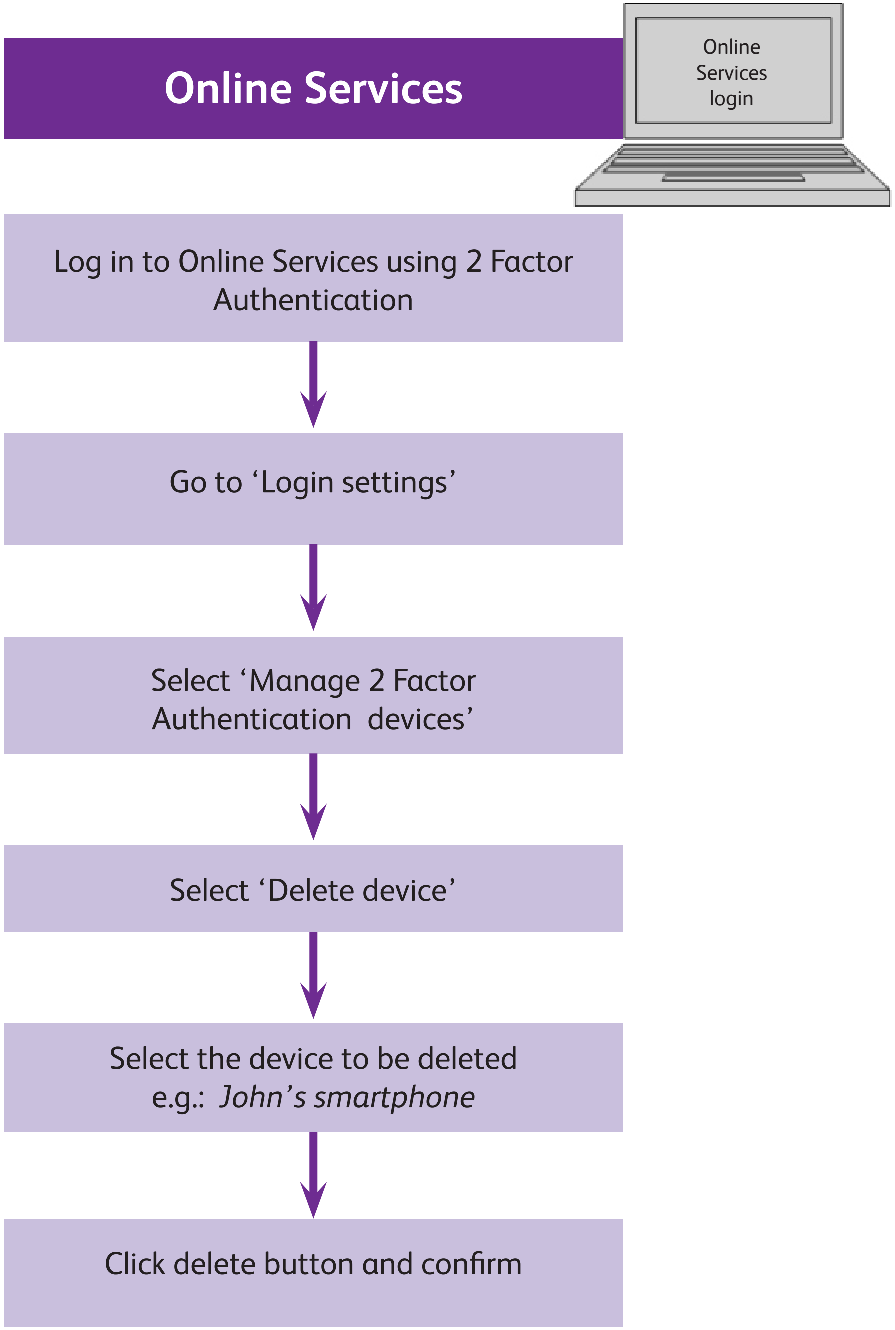
You will be prompted to enter your 6 digit **passcode....**

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

Welcome to Online Services

Back to main contents

Delete a device



Online Services

Log in to Online Services using 2 Factor Authentication

Go to ‘Login settings’

Select ‘Manage 2 Factor Authentication devices’

Select ‘Delete device’

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

Click delete button and confirm

Tip

To **replace a device** simply follow the steps for:
a) Delete a device
b) Add a new device

Note:
If the device you are deleting is the last device on the account, you will receive notification that 2FA has been deactivated for this account

Back to main contents

Frequently Asked Questions

- Is 2FA turned on by account or by contact?
- How many devices can I set up per Online Services contact?
- If I have set-up more than one device, which one do I use to generate my 6 digit passcode?
- I have more than one contact login – can I set up 2FA across all my logins using the same device?
- I have already set up a passphrase – do I need 2FA as well?
- What platforms are supported by Google Authenticator?
- How often will I have to input a 2FA passcode?
- How do I turn off 2FA?
- Initially, I did not want to activate 2FA on my account. How do I set it up now?
- If I don't like using 2FA can I revert back to using the passphrase?

Back to main contents

Frequently Asked Questions

Is 2FA turned on by account or by contact?

2FA is linked to a contact i.e. the email address used to login to Online Services. You can set it up for some or all of your contacts.

How many devices can I set up per Online Services contact?

The recommended way of managing access to Online Services is that contact logins are used by a single user only. A single user should find 5 devices sufficient for the 2FA login process.

If I have set-up more than one device, which one do I use to generate my 6 digit passcode?

You can use any of the devices associated with your contact login. The app on each one will generate a unique and valid 6 digit code for you to input into Online Services when you log in.

I have more than one contact login – can I set up 2FA across all my logins using the same device?

Yes, you can use the same device for multiple contact logins. Make sure you name each account name within Google Authenticator something to help you identify the login it applies to, e.g. ‘Nominet OS john@mydomain.com’.

I have already set up a passphrase – do I need 2FA as well?

The existing passphrase system already provides an additional layer of security when logging into Online Services. 2FA is a more secure system because it requires the use of an additional device. If you opt to set up 2FA, this will replace your existing passphrase login.

Back to main contents

Frequently Asked Questions

What platforms are supported by Google Authenticator?

We support the following platforms:

Google Authenticator app on iOS for the iPhone/iPad

Google Authenticator app for Android devices

Google Authenticator app for Blackberry devices

Microsoft Windows Authenticator app for Windows 8 devices

Google Authenticator plug-in for the Firefox browser

There are many third party implementations of Google Authenticator, including applications for PalmOS, Chrome OS and Java. If you can successfully get the app to work with Online Services then it is fine for you to use it. However Nominet advisors cannot provide any support for these implementations and we cannot vouch for their security.

Back to main contents

Frequently Asked Questions

How often will I have to input a 2FA passcode?

You will need to input a 6 digit passcode from the Google Authenticator app every time you login to Online Services.

How do I turn off 2FA?

Log in to Online Services and go to 'Login Settings'. You will need to delete all devices associated with the contact to deactivate 2FA. The **instructions** explain the processes.

Initially, I did not want to activate 2FA on my account. How do I set it up now?

Logon to Online Services and go to 'Login settings' and 'Manage 2FA' from within Online Services. The **instructions** explain the set up processes.

If I don't like using 2FA can I revert back to using the passphrase?

Yes. You can deactivate 2FA by logging in to Online Services and go to 'Login Settings'. You will need to delete each of the devices associated with the contact to deactivate 2FA. The **instructions** explain the processes for deleting a device.

You can then add the passphrase back from within the 'Login Settings'.

Back to main contents

Troubleshooting

- **I get an error when inputting my 16 digit set up key**
- **I've got a message that my account is locked**
- **My 2FA passcode doesn't work when logging in**
- **What happens if I have lost the device with 2FA installed?**

I get an error when inputting my 16 digit set up key

Please check that the characters have been inputted correctly. The 16 digit setup key will not contain the number zero '0' or the number one '1'. If you are still having difficulties please contact our **Customer Service team** on **+44 (0)1865 332233** or by emailing **support@nominet.org.uk.**

I've got a message that my account is locked

If you enter the wrong passcode 8 times you will be locked out of your account. If this happens you will need to vailidate your identity with our **Customer Service team** on **+44 (0)1865 332233** or by emailing **support@nominet.org.uk.**

If anyone else uses the same contact email as you for Online Services, they may have been locked out of the account without your knowledge. An email confirming this will have been sent to the email address used for the account.

Back to main contents

Troubleshooting

My 2FA passcode doesn’t work when logging in

The 2FA passcode is time sensitive so it could be a time related issue. Ensure you are reading the passcode and immediately entering it into Online Services.

Check that the date and time on your device are correct. You should also ensure you are using the correct timezone on your device for where you are situated. It is recommended that your device is set to update the date, time & timezone automatically if this feature is available.

If you have multiple contact logins you need to make sure the 2FA passcode is the correct one for the contact login you are using.

If anyone else uses the same contact email as you for Online Services, they may have been locked out of the account without your knowledge. An email confirming this will have been sent to the email address used for the account.

If you are still having difficulties please contact our Customer Service team on **+44 (0)1865 332233** or by emailing support@nominet.org.uk.

Back to main contents

Troubleshooting

What happens if I have lost the device with 2FA installed?

If you have another device associated with your contact login then you should:
Login to Online Services using the other device
Go to ‘Login Settings’ and ‘Manage 2 factor authentication devices’
Delete the device that has been lost

If you don’t have another device associated with your contact login then you will need to contact our **Customer Service team** on **+44 (0)1865 332233** or by emailing **support@nominet.org.uk.**

Once we are able to verify your identity we will delete the lost device from your contact login for you.

Back to main contents

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 pass code
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. The passphrase system will still exist for those who would like to keep using it but if you opt to set up 2FA, the 2FA system and login will replace your passphrase log in.

Back to main contents