User Guide to Duo Two Factor Authentication

June 2020 - v1.7

This manual aims to walk you through the most common tasks that involve Duo authentication. If you don’t find a section below that helps, please let the IT Helpdesk know so that we can improve this document for future users.

1 -- Why is the university implementing 2FA?

2 -- When and how do I use Duo?

3 -- I connect and work on a desktop or laptop, do I install Duo on these?

4 -- How do I enroll my phone to use the SMS method?

5 -- How do I test my Duo registered device?

6 -- How do I enroll a device to use the Duo Mobile App?

7 -- How do I use the SMS method?

8 -- I changed my mobile device or have deleted the Duo Mobile app but kept the phone number - how do I use the Duo app again?

9 -- I changed handset but kept the phone number - How do I use the SMS method again?

10 -- I use the Duo Mobile app but need to login to protected systems when I have no phone signal or wifi?

11 -- Can I use more than one device with Duo?

12 -- I have a new phone and new number - How do I enroll it with Duo?

13 -- How do I log into the Virtual Desktop System (VDS)?

14 -- I can’t login with my hardware token?

15 -- My Duo device is lost or stolen?

16 -- I’m going abroad, can I still use Duo?

17 -- How do I download the mobile app?

18 -- I select push notification when logging in to a system but nothing happens?

19 -- How can I get further assistance?
1 -- Why is the university implementing 2FA?

If someone on the internet were to capture your username and password then currently they could log in to the campus network via the VPN and access any system you have access to. It is possible to guess your password if you have a powerful computer and enough time. You could also be tricked into disclosing it through phishing attacks. Therefore the University’s network and data are very vulnerable to attacks from malicious activity.

Over the past couple of years educational institutions have been hit by attacks caused by this, including one university being crippled for a long time when all its systems were held ransom. York has also been hit, leading to a BBC News article that declared that student personal data had been stolen.

If an attacker needs not only your password to prove identity, but to also possess an object in order to login, it is extremely difficult for them to gain access. Two factor authentication protects systems by asking users to provide their identity in this way.

At York the two factor authentication technology we use is by a company called Duo. The second factors we currently use are:

- The Duo Mobile app
- Passcodes received via a text message
- A hardware token (staff only)

This technology is exactly the same as used by all major banks for internet banking logins and transactions. Almost every University in the UK has already implemented some form of 2FA (also known as multi factor auth MFA) or is about to do so.
2 -- When and how do I use Duo?

The university will start to protect systems that permit access to campus resources from the internet and also systems that contain sensitive data. More systems will be protected throughout 2020/21. The protection only occurs when you log in. The protected systems will ask for the normal username/password and then request a Duo authentication.

The Duo authentication process will require you to do one of two actions:

1) Use the Duo Mobile app by selecting PUSH notification on the system you are logging onto. The app on your mobile will ask you if the login attempt is genuine. You press ‘Approve’ and your login process completes.

2) Type a passcode into the login screen. This passcode could come from
   a) Duo Mobile app
   b) hardware token
   c) text message
   d) bypass code issued by the IT Helpdesk

Important: The device you use for Duo (e.g. your mobile phone) isn’t necessarily the device you are using to log onto protected systems. If you normally work on a laptop or desktop you will continue to do so. For example, if you use a windows laptop to logon to the VPN you will use the software to connect, type your username and password and then use your mobile phone to perform Duo authentication. Once you are logged on the phone is set aside and you continue to work on the laptop.

You don’t install the Duo app on any laptop/desktop, only on device(s) you use to prove your identity during the login process.

This short video shows someone using Duo to logon to their company’s protected system: https://www.youtube.com/watch?v=JN0Hj0pKZ7U
3 -- I connect and work on a desktop or laptop, do I install Duo on these?

No. The mobile registered for Duo is only used during the login process to prove your identity. You log in and work as normal on your laptop/desktop. The registered device acts like a key to open an extra security door that appears on your laptop screen as you access university resources.

Video demonstration:  Authenticate with Duo Push on Android - Duo Security

This short video shows someone using their laptop. They want to log on to a protected system (in their case email). They use their mobile phone during the logon process after which they continue to work on their laptop.

If you use a Windows PC to connect to the VPN or other protected resource, you will continue to do that when you start to use Duo. After the normal username and password screen for that resource a Duo authentication screen will appear. At that point you’ll need your mobile device momentarily to get a passcode or approve a push notification. You won’t use your mobile device again until the next time you log in.

Some people might log in to a protected system on a mobile device. For example you might log in to the VPN using an iPad that coincidentally is registered with Duo as a second factor. In this case the same device is used to prove identity during login as well as used to access the protected resources. This is a special case and for the majority of people the mobile is used once during login and then work continues on a PC.

There is no Duo software for desktops/laptops. Only Android and Apple mobile devices (mobile phones, tablets and watches).
4 -- How do I enroll my phone to use the SMS method?

This method assumes you want to only use text messages to receive passcodes for Duo authentication. No software installation is required.

1) Go to the webpage https://duo.york.ac.uk/

2) Login with your normal university username and password

3) If you already have a Duo registered device (regardless if it is working/available to you) you will need to perform a Duo authentication. If that is not possible read the other sections in this document to see if they can help you through the process. If you can’t get past this stage then phone the IT Helpdesk to gain a bypass code.
Once past authentication select add another device or if you have no devices registered with Duo you will be asked to enrol your first device. Select mobile phone on the first screen.

4) Enter your phone number on the second screen

5) Select Other on the next screen
6) The process is complete and you will be presented with the **My Settings & Devices** screen. We recommend you test using Duo by closing the browser, going back to [https://duo.york.ac.uk](https://duo.york.ac.uk) and performing the “How to Test Duo” procedure shown in another section.
5 -- How do I test my Duo registered device?

You can test that your Duo device is working at any time by logging into any protected system. If you perform a Duo authentication and get to the resource you expect everything is working. You can also perform this test on the self service portal (https://duo.york.ac.uk). This also requires you to authenticate with Duo.

1) Go to the webpage https://duo.york.ac.uk and login with your normal username and password

2) The image below shows the Duo authentication screen. If you have multiple devices on your Duo account use the pull down box to select the one you are testing. Next select either Passcode or Push from the green buttons.

   If you are using the push notification method on the mobile app click send me a push.

   If you have a text message with passcodes, a hardware token, a passcode from the mobile app or a bypass code click Enter a Passcode and type the number into the box. Then click Log In.

   If you are a SMS user and need new codes click Enter a passcode after which a blue bar appears at the bottom of the screen permitting you to get a new set of ten passcodes via text message before completing this step.
Successful use of Duo will display the “My Settings & Devices” page. The test is complete and you can close the browser.

This screen is also where you can adjust your settings such as deleting phones that you no longer have or re-linking a new installation of the mobile app.
6 -- How do I enroll a device to use the Duo Mobile App?

First, download the app for your Android or Apple device (phone, tablet or watch). Only fairly recent versions of the OS will work. If you go to the normal store and the app doesn't show this is because your phone is too old to use the technology. We recommend using the SMS option instead.

Once the app is installed use a web browser on another device to go to the self service portal (https://duo.york.ac.uk). Log in with your normal university username and password if asked. If you have no devices currently registered to your Duo account you’ll be asked to register one as soon as you login. Otherwise click + add another device once you get to the main menu.

If you want both Duo Mobile app functionality and SMS functionality select mobile phone on the first screen followed by your phone number on the second screen. If you don’t want to register your phone number (and therefore not use the SMS method) select tablet on the first screen (even if the device is a phone).

Choose the type of device on the next screen.

Click I have Duo Mobile Installed on the next screen
On your mobile open the Duo Mobile app and click the + sign. Point the phone at the screen with the barcode so your phone can see it. This completes the process.

We recommend that you test the Duo Technology at this point using the instructions in the section **How do I test the Duo technology?**
7 -- How do I use the SMS method?

The SMS method allows you to prove you are in possession of your registered mobile phone by entering a 7 digit passcode as you login to protected systems. These passcodes are sent in bundles of ten in a text message.

Assuming you have enrolled your phone number with Duo (see appropriate section in this document if not) the next step is to request a text message.

**Web based systems & VPN**

If you are logging onto web systems that have the full Duo interface such as the VPN and the self service portal you’ll need to click **Enter a Passcode** in the first Duo screen.

A blue bar appears at the bottom of this screen (you might need to scroll down to see it) allowing you to click **Send me new codes**.
Doing so will mean you get a single text message containing 10 passcodes. You might see the sender as DUOSEC. It should take less than 20 seconds. This is an example text message:

![Image of Duo authentication interface]

Note that a hint is displayed showing which is the next passcode to use. Each passcode in your text message starts with a unique number (1xxxxx, 2xxxxx…). This helps you keep track of which one to use as each passcode can only be used once.

If you are ever unsure of which passcode to use or if you have used them all, delete all the Duo text messages on your phone and request a new text message.

If you receive a new text message all codes from all previous text messages are invalid. Each passcode within a text message can be used in any order but only once.

Once you have a valid text message you can enter the first unused passcode into the system that is requesting Duo authentication. This video shows the process of logging in with a passcode. Note that the user is accessing a system on his laptop. The phone is only used as part of the login process.

https://www.youtube.com/watch?v=57CVU0GQk0I
Non Web Systems

Some systems aren’t capable of displaying the Duo web pages like in the examples above. The virtual desktop system and all command line systems are examples. Here you can enter the passcode by typing it into the appropriate box or at the prompt.

If you need a new set of codes type the word **sms** and you’ll be sent them straight away. If you use the Duo Mobile app you can type the word **push** to use that method. Below you can see the OTP box you use for the virtual desktop service. You type a passcode, the word push or the word sms into the box next to OTP.

![Duo integration example](image)

Here is a typical command line prompt with Duo integration where you select numerical options. Some command line prompts such as the linux VPN client don’t have the menu but require you to enter a passcode, sms or push.

![Command line prompt example](image)
8 -- I changed my mobile device or have deleted the Duo Mobile app but kept the phone number - how do I use the Duo app again?

Each installation of the Duo Mobile app contains a unique code which is shared only with the Duo cloud service. If you change the device or wipe the software from your phone that link is broken. You won’t be able to use the Duo Mobile app until the link is fixed.

If you still use the same mobile phone number and this was registered with Duo you can use the SMS method to login to the self service portal (https://duo.york.ac.uk). Once in, you can reactivate Duo to fix the link between your installation of the mobile app and the cloud service. To get into the portal using SMS

1) Click the green Enter a Passcode button
2) Scroll down and click Text me new codes in the blue bar
3) When the text message arrives enter the first 6 digit passcode into the box to the left of the green Log In button and then click the button

To re-activate the link on the self service portal (after checking Duo Mobile is installed) log in using a different computer/device to the phone you are reactivating and then click Device Options next to your device.

Then click on Reactivate Duo Mobile.

Click I have Duo Mobile Installed
On your phone open Duo Mobile and click the + symbol. Point the phone’s camera at the screen with the barcode. The process completes.
9 -- I changed handset but kept the phone number - How do I use the SMS method again?

There is no action to take if you continue to have access to a phone with the registered number. The Duo text messages will go to the new handset the next time you request one. We recommend testing this out by using the test method outlined in this document.
10 -- I use the Duo Mobile app but need to login to protected systems when I have no phone signal or wifi?

An advantage of the Duo Mobile app is that you can use it when there is no data signal to the phone. This includes labs where this isn’t permitted, areas where wifi & 4G are weak or when travelling abroad.

Open the Duo Mobile app and click on the University logo. A six digit passcode is revealed. Use this to log into any protected system in the normal way.
11 -- Can I use more than one device with Duo?

Yes. You can have one or several devices on your Duo account. For example you might want to use a personal mobile sometimes but also the convenience of using an Android tablet/iPad sometimes. One device could use the Duo Mobile app while another uses just the SMS method.

To add additional devices return to the self service portal. Authenticate with the first device and select the option to add another device.

Below shows the screen with multiple devices setup. Note the default device. If you use some systems where you type the word push (e.g. command line systems) then this device receives that push notification. You can also select that push notifications are sent automatically as you are logging on to make the process even quicker.
12 -- I have a new phone and new number - How do I enroll it with Duo?

This section assumes you previously registered a device with Duo (i.e. it isn’t your first ever registration with Duo). In this circumstance you won’t be able to proceed using the self service portal. You will need to contact the IT Helpdesk by phone during normal office hours. They will ask you to prove your identity using your security questions and then help you resolve the issue.

You may be given a bypass code. This is a long number which you use in exactly the same way as a passcode gained from a text message or hardware token. Use the bypass code to login to the self service portal and delete the old device before adding your new device.
The VDS doesn’t have web pages that can display all the normal Duo options. So you’ll authenticate slightly differently to systems like the VPN. First enter your short username and password. Note the erroneous text that suggests you type an email address. So abc123 is correct, abc123@york.ac.uk would fail.

Next a pop-up box appears. Only the OTP (one time password) textbox is used. Use the table below to work out what to enter before clicking OK.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>What to type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware token</td>
<td>enter the passcode</td>
<td></td>
</tr>
<tr>
<td>Mobile app</td>
<td>type the word push</td>
<td>You can alternatively type a passcode from within the app</td>
</tr>
<tr>
<td>SMS</td>
<td>type an unused passcode from your most recent text message</td>
<td>If you need new passcodes type the word sms and click OK. You’ll need to start the authentication process again as it will seem like you have failed authentication. That is normal.</td>
</tr>
</tbody>
</table>

If you can’t login to this system it is a good idea to test your Duo authentication method out with the self service portal (https://duo.york.ac.uk). See the section above for details.
14 -- I can’t login with my hardware token?

If nothing appears on the screen when you press the button then the device is dead. Please contact the IT Support team to request a new one. They can be contacted via itsupport@york.ac.uk or 01904 32 3838 (9am to 5pm, Monday to Friday).

If the number that appears doesn’t work even after a couple of goes then this might be the result of the token getting out of sync. Both the token and the Duo server know what number should appear on the screen next. If the button on the token is pressed more than 5 times without logging on then the server will have a different idea of what the next number is compared with the token.

To fix this you will need to phone the IT Helpdesk who will ask you to go through a short procedure where you’ll read out 3 codes in a row. This re-syncs the token.

It isn’t possible to do that without phoning the helpdesk as it needs an administrator to enter the three codes into the Duo admin console in real time.
15 -- My Duo device is lost or stolen?

Please phone the IT Support team immediately. They can prevent your account from being accessed as soon as they know. They can also issue a temporary bypass code to get you connected until a replacement device can be arranged.

They can be contacted via itsupport@york.ac.uk or 01904 32 3838 (9am to 5pm, Monday to Friday).
16 -- I’m going abroad, can I still use Duo?

Yes, all the methods will work when abroad and the IT Helpdesk can provide temporary methods to authenticate if your situation means your normal Duo device won’t work.

If you have a mobile device with the mobile app or a hardware token, you can get passcodes from it without needing any kind of signal. Continue to use it as normal.

If you use the SMS method this will also work where you can receive text messages (roaming). Be aware some providers charge for you to receive text messages when abroad. Check with your provider if this is a concern.

If you normally use a mobile device for Duo but don’t want to take this abroad, the IT Helpdesk can provide a temporary method to keep you connected. This might be a hardware token if you are on a longer trip or a bypass code if a short trip. You’ll need to do this well in advance of your departure.
17 -- How do I download the mobile app?

Only download the app from the links provided which link to an app with this logo:

![DUO logo](image)

The mobile app is only supported on the recent, supported versions of operating systems. The app stores do not show incompatible apps so if you can’t see the app it is because your mobile device is running a version that is too old. We recommend the SMS method instead.

**Android**


The app requires Android version 6.0 or greater.

**Apple**


Requires iOS 11.0 and watchOS 2.0 or later. Compatible with iPhone, iPad and iPod touch.
18 -- I select push notification when logging in to a system but nothing happens?

Self Test
Before troubleshooting your push notification issue, perform a Duo check using section 5. This will ensure the problem isn’t with the system you are logging into. If you get the same result with the self service portal continue with this section. If push notifications work on that system then please contact the IT helpdesk.

Triage
If you select Push Notifications on the system you are logging into but you don’t see anything appear on your mobile one of two things could be happening:

- The app receives the push but settings on the phone prevent it from displaying
- The app isn’t talking to the Duo cloud service and so does not receive the Push

To work out which is happening do the following:

1) Open the mobile app.
2) Go to the self service portal https://duo.york.ac.uk
3) Log in and select push notification

If the app displays a green request to approve then the problem is only with the phone’s notifications (where messages appear regardless of what app you’re using). If you see nothing then the issue is the communication between phone and the internet.

Troubleshoot a Communication Issue
If you see nothing in the above test follow section 8 of this guide to re-establish the connection between your phone and the Duo service. Once complete, test again with the above steps. If that doesn’t fix the issue contact the IT helpdesk.

Troubleshoot a Notification Issue
To troubleshoot notification issues work through the relevant help document:

19 -- How can I get further assistance?

The IT Support team can be contacted via itsupport@york.ac.uk or 01904 32 3838 (9am to 5pm, Monday to Friday).