



Introduction

We're modifying how all laptop users access the Royal Mail network remotely through the VPN. There are two main changes; the latest, more stable VPN client from Cisco and an extra security code, utilising the OneLogin system (which is increasingly making more RMG and other sites easier to access and more secure at the same time).

Why are we doing this?

To enhance the protection against unauthorised access to our critical systems and prevent data breaches we need to make it harder for hackers to get into our network.

But I change regularly my password, isn't that enough?

Until now, we've had just one layer of security – your password – to protect your account. Now, even if someone gets hold of your laptop and password, they won't be able to use the VPN without your phone.

Ok, sounds like a good idea but is it difficult to setup / use?

We're glad you're on board! The good news is that once you have the new VPN client on your laptop and you have completed the initial setup steps, the only difference will be entering the extra security code after your usual Windows login name and password when you first connect to VPN.

How do I get it?

We're deploying the new Cisco AnyConnect VPN client to all Royal Mail laptops during April 2017.

Before you can start to use it there are a couple of things to check and setup; firstly, that your mobile telephone number is correct in [People Finder](#), secondly, you need to setup [OneLogin](#) "Multi-Factor Authentication" (read on).

What is Multi-Factor Authentication (MFA)?



High-profile data breaches are making headlines weekly, and the number of incidents continues to rise. Multi-Factor Authentication (MFA) has become the norm to prevent unauthorised users from accessing corporate data with passwords alone. There are a variety of different "factors" that you will have been likely using for a long time outside of work, such as when contacting your bank. Some examples include, asking for two random digits for a secret password or response to a personal question (e.g. mother's maiden name). However even these are not as secure as they used to be and so are gradually being replaced with other methods, like fingerprints and temporary security codes on your phone.

RMG have selected the additional security code to mobile phones. This can be done by either downloading an app (for smartphones) or using SMS text messages.

Should I use the app or should I get texts sent to me?

If you have a smartphone, then please use the app. It's a free download from the app store, and once it's installed it doesn't even need a mobile signal to work. If you don't have a smartphone, get the codes sent to you by text message instead.

How do I get started?

You'll need to download the app onto your phone, and then verify it on the Royal Mail network. Or, to get codes sent by text, you'll need to confirm your mobile number, and verify it on the Royal Mail network. There are step-by-step instructions below.

Get the app

If you've got a smartphone, it's easy to download the app. On your phone, tap one of the icons below for your smartphone type, and it will take you straight to the download page.

1. Download the app for your phone



Microsoft or
Nokia

<https://www.microsoft.com/en-us/store/p/onelogin-otp/9nblgggzkrbj>

Android

<https://play.google.com/store/apps/details?id=com.onelogin.newotp>

iPhone

<https://itunes.apple.com/gb/app/onelogin-otp/id509252983?mt=8>

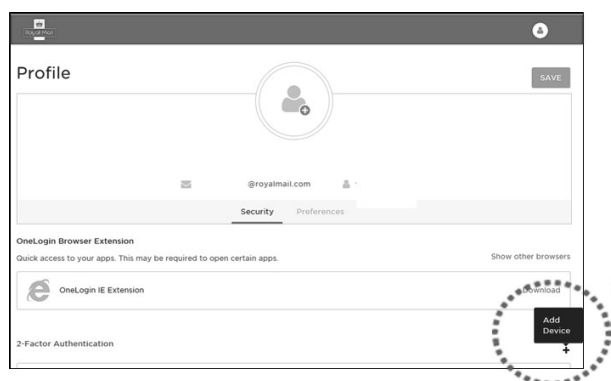
2. Verify the app with the Royal Mail network

Full instructions are below and you can also watch this [video tutorial](#).

You need to do this step on your laptop, while on the Royal Mail network (either in an office or connected using the old Cisco VPN). On your laptop, go here: <https://royalmail.onelogin.com/profile/>

NB: You should see the page below, if not, click your name in the upper right, then select Profile.

Scroll down to find “2-Factor Authentication” and click on the plus sign to its right.



You will then see the “Add 2-Factor Method” window:

Add 2-Factor Method

Choose Vendor: OneLogin OTP

Name: OneLogin 1

Credential ID: [Empty]

Enter two consecutive OTPs to register your device

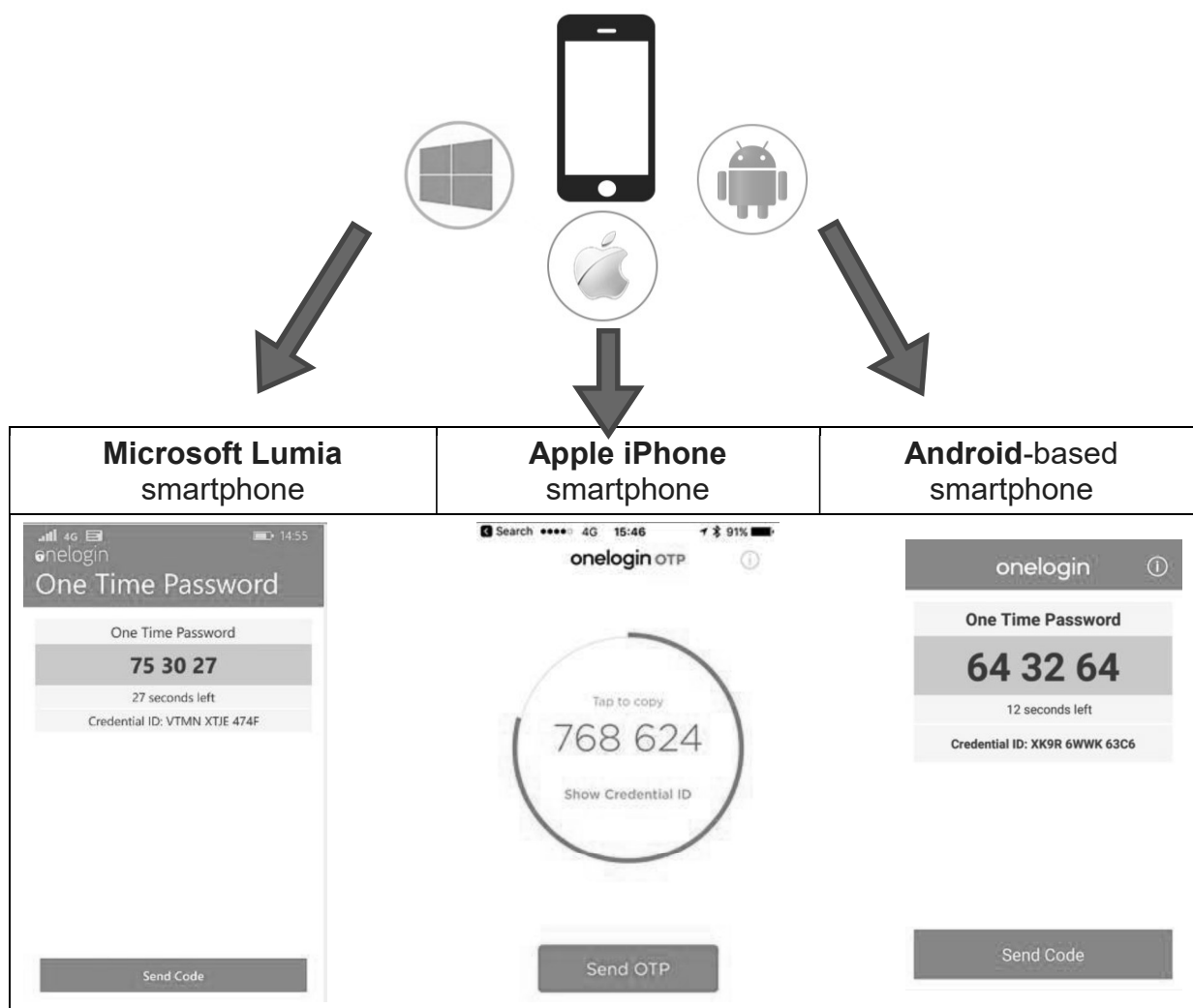
OTP 1: [Empty]

OTP 2: [Empty]

CANCEL CONTINUE

Open the Onelogin app on your smartphone (images will vary depending on your phone type) and you will see a 6 digit random code which will be replaced every 30 seconds.

If it's not showing, tap on the “Show Credential ID” text, and you'll see an ID – 3 sets of 4 characters, e.g. T8BV W4WK JEC6. Type that ID code into the “Credential ID” box on your computer. Then enter the first 6-digit code you see in the OTP 1 box, wait until the code changes, then type the next code in the OTP 2 box and click Continue.



Get codes texted to your phone

If you've got a mobile phone, but it's not a smartphone, you can get codes sent to you by text instead.

1. Make sure your RMG mobile phone number is in People Finder:

<http://intranet.royalmailgroup.net/peoplefinder/>

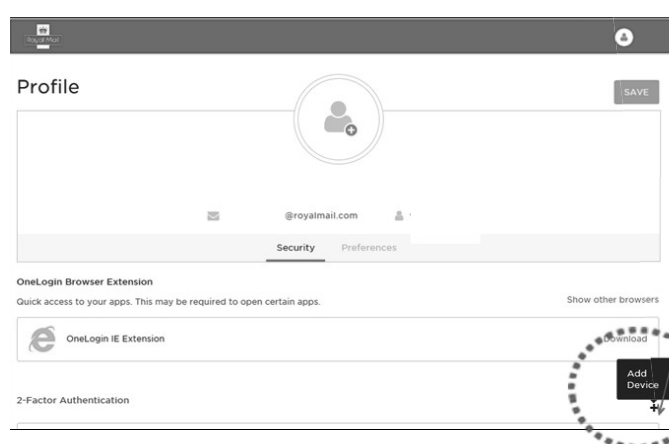
If your mobile number is wrong or missing, you can click the "My Profile" link on the upper right and then click the "pencil" icon to edit/add your correct number.



2. Verify your phone with the Royal Mail network

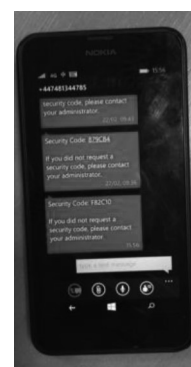
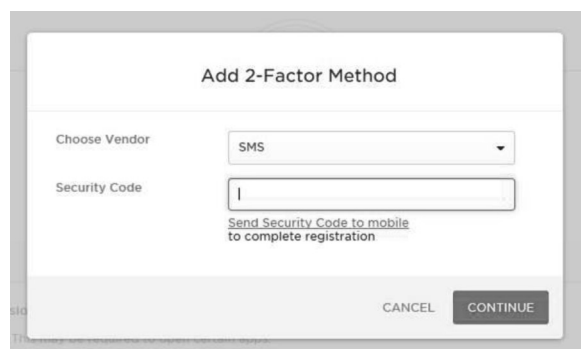
On your laptop, go here: <https://royalmail.onelogin.com/profile/>

Scroll down to find "2-Factor Authentication" and click on the plus sign to its right



Select SMS from the "Choose Vendor" dropdown menu then click the Send Security Code to mobile link.

You will then receive a text message to the mobile phone you have registered on People Finder with a 6 digit Security Code. Enter this into the Security Code box and click Continue.



Phew! I've made it this far; can you remind me how easy it is to log on to the new VPN?

Once the new AnyConnect VPN client has been installed on your laptop, you start using it immediately (Note: This new process will only work with the new AnyConnect client), until then please continue to use the old Cisco VPN) .



Step 1: Start the new "Cisco AnyConnect Secure Mobility Client" program from your Windows Start menu.

Step 2: Click on Connect

Step 3: Enter your username and password

Step 4: If you've got the app, tap on the app now to make it show you a code. If you've registered your phone for texts, you should get a text in a moment with your code in it.

Step 5: Enter the security code (also known as a One Time Password or OTP) from your app, or from the text you've just received.

Watch the video

You're in!

When does the old VPN get turned off?

We currently anticipate terminating the old VPN early in May however, we will have a checkpoint to confirm that users are successfully using the new system before completing the switch. To ensure we complete the transition as quickly as possible and get the benefit of the enhanced network and data protection, it is important that everyone completes the required activities and we will produce regular reports and reminder notifications.

We will also be removing the old VPN client from all laptops and so anyone that has not completed the switch by the end of the support period, risks losing laptop remote access to Royal Mail Group systems.

What if something goes wrong?

Whilst we've made every effort to make things as smooth as possible, sometimes things just go wrong. Don't panic! If the user instructions don't help, you can contact the IT Helpdesk who should be able to resolve your problem.

For a limited period of time, the old VPN will still be available so you can still log on using that but please do make the switch as soon as possible and certainly before the switch off date – keep looking for comms updates and on the Intranet for news of this.