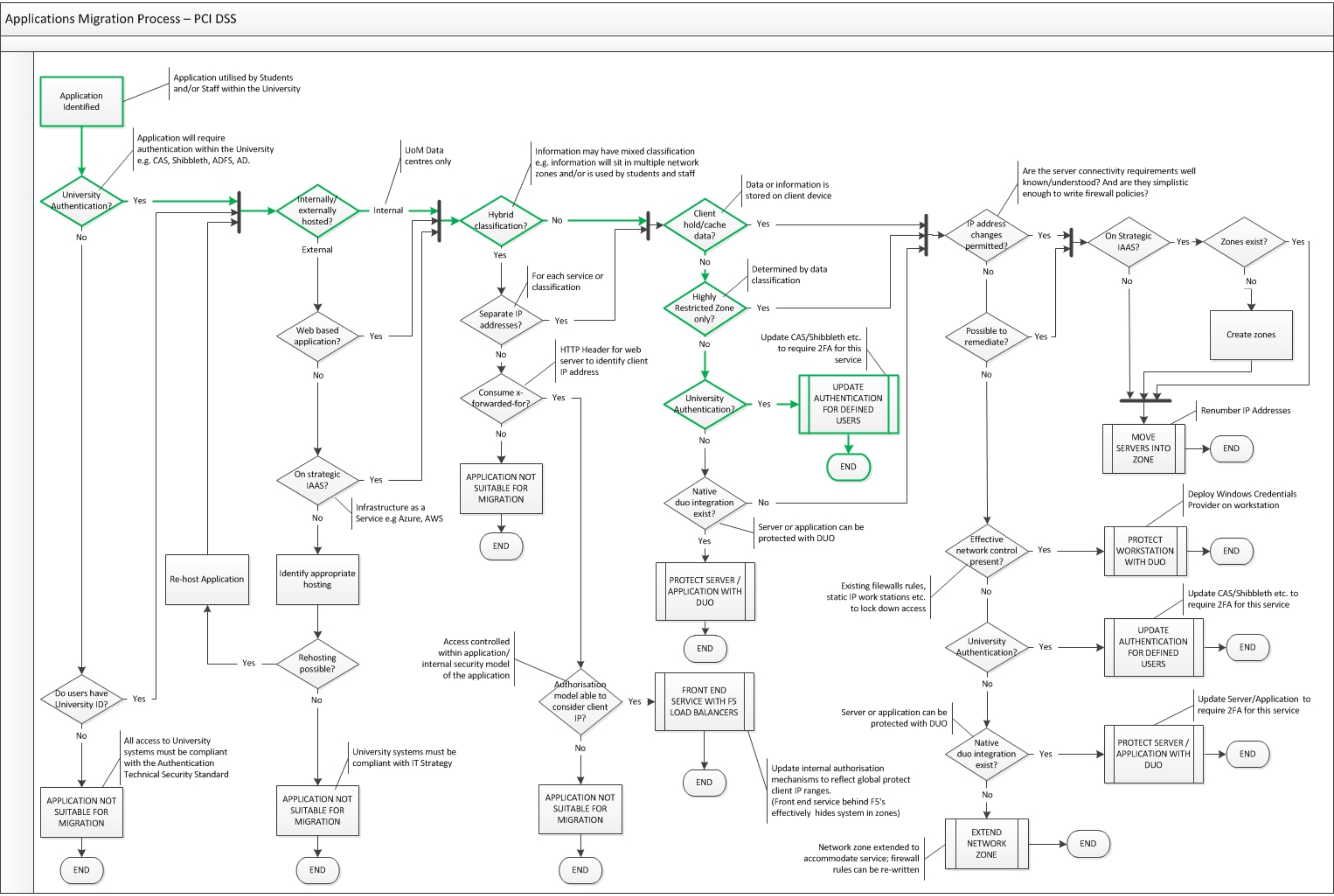
MANCHESTER 1824
The University of Manchester

Two Factor Authentication (2FA) and Linux
University of Manchester

Matt Foster
Enterprise Architect Security

Protection Decisions



Applications Migration Process – PCI DSS

Application Identified

Application utilised by Students and/or Staff within the University

University Authentication?

Application will require authentication within the University e.g. CAS, Shibbleth, ADFS, AD.

Yes

No

Do users have University ID?

Yes

No

APPLICATION NOT SUITABLE FOR MIGRATION

All access to University systems must be compliant with the Authentication Technical Security Standard

END

Re-host Application

Internally/ externally hosted?

Internal

UoM Data centres only

External

Web based application?

Yes

No

On strategic IAAS?

Yes

No

Infrastructure as a Service e.g Azure, AWS

Identify appropriate hosting

Rehosting possible?

Yes

No

APPLICATION NOT SUITABLE FOR MIGRATION

University systems must be compliant with IT Strategy

END

Hybrid classification?

Information may have mixed classification e.g. information will sit in multiple network zones and/or is used by students and staff

No

Yes

Separate IP addresses?

For each service or classification

Yes

No

Consume x-forwarded-for?

HTTP Header for web server to identify client IP address

Yes

No

APPLICATION NOT SUITABLE FOR MIGRATION

END

Access controlled within application/ internal security model of the application

Authorisation model able to consider client IP?

Yes

No

APPLICATION NOT SUITABLE FOR MIGRATION

END

FRONT END SERVICE WITH F5 LOAD BALANCERS

END

Update internal authorisation mechanisms to reflect global protect client IP ranges.
(Front end service behind F5's effectively hides system in zones)

Client hold/cache data?

Data or information is stored on client device

Yes

No

Highly Restricted Zone only?

Determined by data classification

Yes

No

University Authentication?

Yes

No

UPDATE AUTHENTICATION FOR DEFINED USERS

Update CAS/Shibbleth etc. to require 2FA for this service

END

Native duo integration exist?

No

Yes

Server or application can be protected with DUO

PROTECT SERVER / APPLICATION WITH DUO

END

IP address changes permitted?

Are the server connectivity requirements well known/understood? And are they simplistic enough to write firewall policies?

Yes

No

Possible to remediate?

Yes

No

Effective network control present?

Existing filewalls rules, static IP work stations etc. to lock down access

Yes

No

PROTECT WORKSTATION WITH DUO

Deploy Windows Credentials Provider on workstation

END

University Authentication?

Yes

No

UPDATE AUTHENTICATION FOR DEFINED USERS

Update CAS/Shibbleth etc. to require 2FA for this service

END

Native duo integration exist?

Server or application can be protected with DUO

Yes

No

PROTECT SERVER / APPLICATION WITH DUO

Update Server/Application to require 2FA for this service

END

EXTEND NETWORK ZONE

Network zone extended to accommodate service; firewall rules can be re-written

END

On Strategic IAAS?

Yes

No

Zones exist?

Yes

No

Create zones

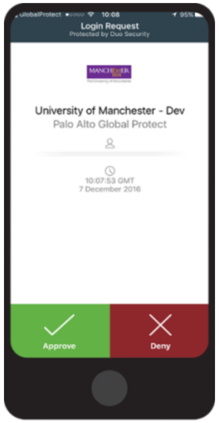
MOVE SERVERS INTO ZONE

Renumber IP Addresses

END

So what?

2FA – the token isn't (necessarily) the client ….



Login Request
Protected by Duo Security

University of Manchester - Dev
Palo Alto Global Protect

10:07:53 GMT
7 December 2016

Smart phone on Android, iOS, Windows Phone

Tap 'Accept' on your smartphone

OTP code option can be used with no connectivity

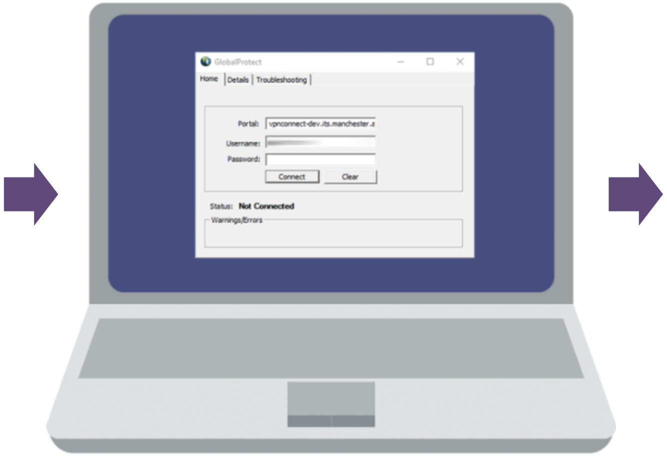
A traditional mobile phone

Use a text message or phone call to generate your passcode

Hardware token / keyfob

No connectivity required

What will you see: OpenVPN
Needed for ”fat client” access to Email



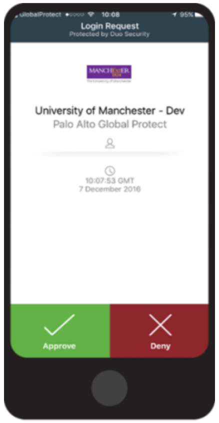
Portal: vpnconnect-dev.its.manchester.a

Username:

Password:

Status: **Not Connected**

Warnings/Errors



Login Request
Protected by Duo Security

University of Manchester - Dev
Palo Alto Global Protect

10:07:53 GMT
7 December 2016

Login to Linux as normal

Log in to OpenVPN (the virtual private network) when prompted using username and password through network manager or similar

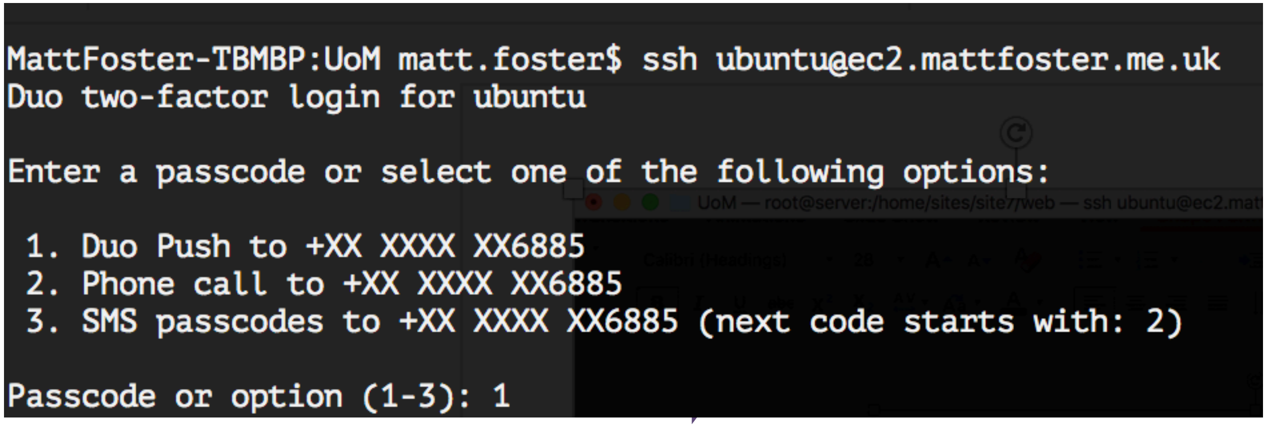
Authenticate with 2FA

Access granted

There is no native Palo Alto client for the Global Protect VPN today for Linux. So a parallel OpenVPN infrastructure has been built to support Linux users.

What you will see: SSH sessions (e.g., zrek)

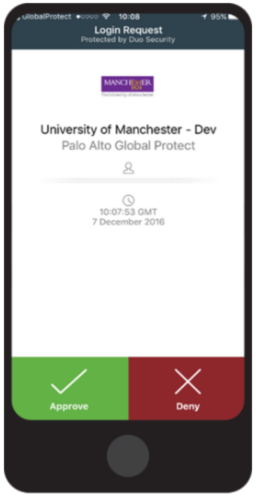
Login with your username

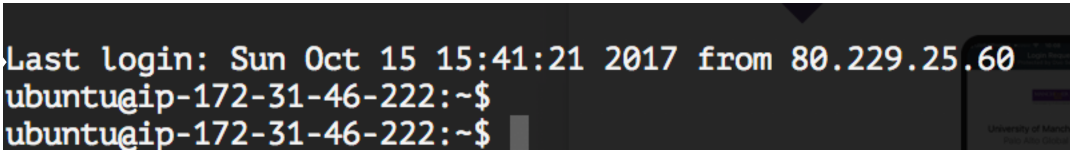


```
MattFoster-TBMBP:UoM matt.foster$ ssh ubuntu@ec2.mattfoster.me.uk
Duo two-factor login for ubuntu

Enter a passcode or select one of the following options:

 1. Duo Push to +XX XXXX XX6885
 2. Phone call to +XX XXXX XX6885
 3. SMS passcodes to +XX XXXX XX6885 (next code starts with: 2)

Passcode or option (1-3): 1
```

Choose authentication method

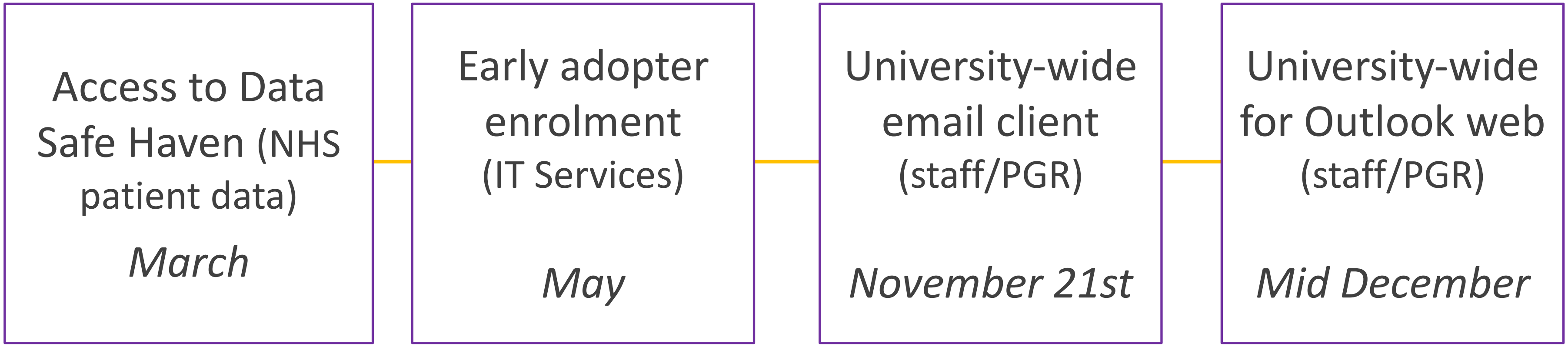
Authenticate using 2FA





```
Last login: Sun Oct 15 15:41:21 2017 from 80.229.25.60
ubuntu@ip-172-31-46-222:~$
ubuntu@ip-172-31-46-222:~$
```

Timeline…



Access to Data Safe Haven (NHS patient data)

March

Early adopter enrolment (IT Services)

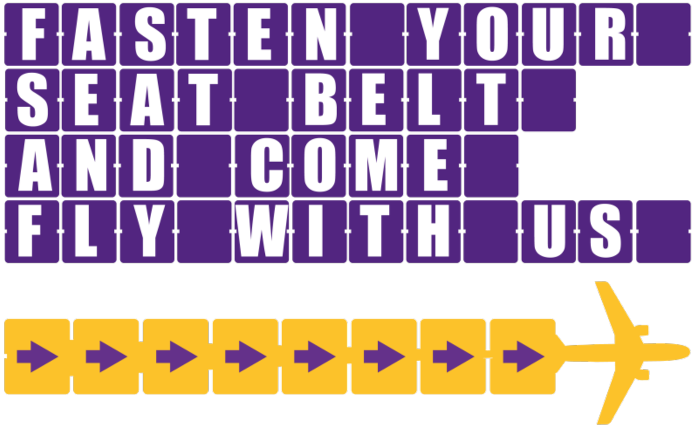
May

University-wide email client (staff/PGR)

November 21st

University-wide for Outlook web (staff/PGR)

Mid December



MANCHESTER
1824
The University of Manchester

Further information

Cyber security website

http://www.itservices.manchester.ac.uk/cybersecurity/

Mailing List

csp@manchester.ac.uk

Linux and VPN FAQs

How do I install the VPN?

- Debian and RedHat packages are being made available
- Manual installation and profile configuration instructions will be made available for those unable or unwilling to use the supplied packages.
- Your system will need to be able to support OpenVPN 2.4, lower versions will not work.

Why can’t I just use the Cisco VPN?

- The Cisco VPN service does not support the new authentication methods, and is due to be retired in the near future.

What else is different to the Cisco VPN?

- The OpenVPN configuration is a ”split tunnel” rather than a “full tunnel”. Only the traffic that needs to be transmitted via the VPN will be routed via it. As a result of this your routing table will be modified when the VPN client connects.
- You will have to re-authenticate every 12 hours.
- You will have to use the VPN regardless of which network you are connected to for access to email, even connected to the campus wired network.

What about certificates?

- OpenVPN uses certificates internally to validate the authenticity of the session. The University is not using certificates to authenticate users or devices in the OpenVPN service.
- But I heard that I would need a device certificate to be trusted and access Highly Restricted systems and information?
  - Yes, this is the case, and is enforced via the Palo Alto Global Protect VPN. There is no way to access the Highly Restricted Zone from an OpenVPN connection.
  - As systems migrate to Highly Restricted this will be assessed on a case be case basis.

Email and 2FA FAQs

- **How many times will I need to use 2FA?**
  - At least once a day to access email – stay on for 12 hour period
  - No need to repeat if you use the same device and stay on campus (even if you move between buildings)
  - Do need to 2FA again if you go home or go to a different location
  - Always need to use 2FA when using Outlook web application (OWA)

- **What if I’m abroad with no network signal?**
  - Can use Duo mobile application ‘OTP’ codes, pre-generated SMS codes or key fob tokens

- **Do I have to use 2FA on my ipad or mobile device?**
  - No if you’re using the built-in mail application
  - Yes if you’re using OWA
  - If you want to use a new device you will need to use 2FA when you first set it up

- **What if I can’t or don’t want to use a mobile for 2FA or I don’t want to incur costs (especially abroad)**
  - Use the key fob type device
  - Smartphone users can use OTP for no cost
  - For SMS delivery users are not typically charged for receiving SMS messages abroad
  - Duo phone calls will depend on contract
  - Push notifications require minimal data