



# T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

## Cyber Security

Assignment 1 – Distinction

Guide standard exemplification materials (GSEMs)

## T Level Technical Qualification in Digital Support Services Occupational specialism assessment (OSA)

# Cyber Security

## Guide standard exemplification materials (GSEMs)

Assignment 1 - Distinction

## Contents

<b>Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
<b>Assignment 1</b> .....	<b>4</b>
Task 1: project proposal .....	4
Student evidence .....	6
Task 2: set-up – devices, network and access .....	23
Student evidence .....	23
<b>Testing table</b> .....	<b>52</b>
<b>Examiner commentary</b> .....	<b>53</b>
Overall grade descriptors .....	54
<b>Document information</b> .....	<b>56</b>
Change History Record .....	56

## Introduction

The material within this document relates to the Cyber Security occupational specialism sample assessment. These exemplification materials are designed to give providers and students an indication of what would be expected for the lowest level of attainment required to achieve a pass or distinction grade.

The examiner commentary is provided to detail the judgements examiners will undertake when examining the student work. This is not intended to replace the information within the qualification specification and providers must refer to this for the content.

After each live assessment series, authentic student evidence will be published with examiner commentary across the range of achievement.

# Assignment 1

## Brief

Willow Technology are aware of the continuous technological improvements and updates that are currently available and have asked you to research the current market and create a project proposal for how Willow Technology could improve the security of their current systems and software. This proposal will be submitted to the board and will be addressed in the budget for next year.

Additionally, at the beginning of next week, a new colleague will be joining the team. You have been asked to set up a device so that they are able to work remotely most of the time and will be able to log in when working in the office, which uses hot desks if the need arises. In addition to configuring the laptop, you will also have to install any software agreed to by your line manager, as well as set up an administrative account for yourself and one for the new colleague.

## Task 1: project proposal

Time limit

5 hours 30 minutes

You can use the time how you want, but all parts of task 1 must be completed within the time limit.

(30 marks)

## Instructions for students

You are required to complete a project proposal that compares 2 available security products (for example, comparing 2 different vendor-based firewalls) and recommend which would be best for the company. Additionally, you will need to recommend the most appropriate method for user access solutions.

You will provide a rationale to justify any recommendations you make, stating why you feel the product/solution chosen is better than any other available whilst considering price, reviewer feedback from other users and certification.

You should create a project proposal that includes:

- your research into the following three secure software solutions:
  - firewall
  - anti-virus
  - virtual private network (VPN) to ensure that any internet connection remains secure and private
- for each one of these you should compare 2 similar products and recommend the best solution based on price, user reviews, technical specification and if applicable, certification
- references to sources used for validating the credibility of the software chosen
- any legal/security requirements that need to be addressed when considering the software chosen and how this software may be used
- recommendations for the most appropriate methods to implement user access control for the device either locally, remotely, or both

## **Evidence required for submission to NCFE**

The following evidence should be submitted:

- a project proposal

## Student evidence

### Project proposal

#### Product research

##### Firewalls

When considering a firewall, it is important to look at the overall requirements before embarking on the search for a product. There are several different types of firewall that will vary based on the security needed.

#### Common Firewall Types

Packet filtering firewall	This is the most common firewall type and operates by monitoring outgoing and incoming packets and allowing them to pass or be dropped based on the source and destination Internet Protocol (IP) addresses, protocols and ports. This is the easiest firewall to configure and can be hardware or software based for example Windows Defender Firewall. Willow could employ this type of firewall to apply rules organisation wide.
Circuit-level gateway	A circuit-level gateway firewall helps in providing security between UDP and TCP connections. Willow could employ this type of firewall to allow access to traditional web apps hosted in data centres using the same log-on credentials and authentication techniques they use to access mobile apps and cloud services.
Application-level gateway (also known as proxy firewalls)	This is basically a firewall proxy that filters unwanted network traffic and is used to provide security between computers and services on a network. Willow could employ this functionality to deny access to the resources of private networks to distrusted users over the Internet.
Stateful inspection firewalls	This type of firewall monitors the state of any active connections and uses the information to permit or deny the network packets through the firewall. This is achieved by monitoring requests and checking entries it contains. Willow could employ this type of firewall to improve overall security on the network.
Next-generation firewall (NGFW)	A next-generation firewall (NGFW) is a security appliance that deals with network traffic and applies rules to block suspicious traffic and activity. NGFWs employ the capabilities of traditional firewalls but they also build on them to provide additional services for example Advanced Malware Protection.

#### Information Source

There are multiple discussions available on the internet that give a rundown of the types of firewalls as well as their Pros and Cons, the ones I used were: -

Phoenixnap – <https://phoenixnap.com>

TechTarget – <https://www.techtarget.com/>

Comparitech – <https://www.comparitech.com>

Performance Networks – <https://www.performancenetworks.co.uk/>

CBT Nuggets – <https://www.cbtnuggets.com>

GetApp – <https://www.getapp.com/>

Cisco – <https://www.cisco.com/>

Based upon delivery method there are 3 different categories of firewalls available:

- hardware Firewall
- software Firewall
- cloud Based Firewalls, also known as Firewall as a Service

### Hardware Firewalls

A hardware firewall is a dedicated piece of hardware whose role is to filter incoming and outgoing network traffic applying a set of rules that either allows or blocks the traffic. Unlike a software firewall, a hardware firewall has its own CPU, Memory, etc. so does not consume resources from any other host on the network. Firewalls fall into 5 main categories.

Having a dedicated piece of hardware to act as a firewall is a good choice for all business sizes in the current climate, for example, remote working and the increase of cyber related attacks. Cisco provide advanced security appliances at affordable prices and are cost effective devices to provide redundancy, i.e., to have 2 either working active/active each sharing the role or active/passive where one is primary and the other is a failover, only coming online if the primary fails.

### Pros

- protect multiple devices at the same time, hardware firewalls can be the default gateway for the premises at Willow and oversee all incoming and outgoing traffic
- protects the network perimeter so malicious traffic should never reach other assets, this can be achieved through packet filtering and stateful inspection employing a NGFW
- have their own resources that can be upgraded in many instances – firmware updates and additional subscription services can be applied when needed, for example, Cisco security appliances with Firepower
- single administration point as opposed to having to manage a firewall on all devices – Cisco Adaptive Security Device Manager (ASDM) has functionality for central management of multiple devices, this will also support any future growth that may be required at Willow
- can act as a VPN endpoint allowing secure access for remote users to internal systems, this is a very important feature due to the increase of remote working in recent years – most business firewall routers will have functionality for VPN access

### Cons

- more expensive especially if deployed as a redundant pair
- requires in-house expertise to manage

- will not protect against insider threats as the threat actor is already inside the perimeter
- needs to be deployed in a secure controlled, environment such as a comms cabinet
- needs redundant power in case of power fluctuations or power outages

### **Software Firewalls**

A software firewall installs directly onto a device such as a laptop or computer and, as such, only protects that device. It also has to share the devices resources such as CPU and memory and needs to be installed on every device the company wants to protect. This also increases the administration of the device as updates, etc. need to be applied to all devices that have the firewall installed.

#### **Pros**

- very good protection for a single device, for example, Windows defender firewall on all company laptops, PCs and end devices at Willow – this can be controlled using security policies on Windows server and any required updates can be rolled out using Windows server update services (WSUS)
- isolates all endpoints from each other unless a rule is created to allow access, this can help when there is evidence of compromise or other suspicious activity at Willow
- gives admins complete control of firewall at a granular device level, this can be achieved centrally via Windows Server Active Directory or Azure Active Directory at Willow
- software readily available and relatively inexpensive, for example, Windows Defender Firewall is a feature of all recent Windows operating systems

#### **Cons**

- consumes the CPU, memory, etc. of the device it is installed on
- requires configuration to be done on all devices the firewall is installed on
- increased day-to-day maintenance as it is manual
- increased chance of manual error
- not all firewalls support all types, for example Windows and Mac, so there may be a need to buy separate solutions increasing admin

### **Firewall as a Service**

Firewall as a Service (FWaaS) relies on technology in the cloud. A user or application connects to the FWaaS via the internet, and the service applies domain rules, URL filtering, and other security that physical firewall appliances would normally use. It aims to replace all the hardware firewalls deployed to protect a company's traffic on all sites, along with any remote devices. As this is a service it means that the provider handles all provisioning, management, updates, etc. so the company do not need any specific firewall SME in-house staff.

#### **Pros**

- the service provider handles admin tasks related to the platform including installation, provisioning, patching, etc. this can free up time for other IT related work



- the company can scale up the provision to meet future demand with no capital cost; cloud providers for example AWS, have elasticity built into their systems to allow for expansion and contraction with ease, this can be done instantly and could potentially be financially rewarding for Willow
- scaling up provision can happen very quickly, often instantly, this has benefits as detailed in the previous bullet point
- there is no need for in-house hardware or the associated power, security, etc. this will be financially rewarding for Willow and removes vulnerabilities and threats related to on site physical infrastructure, for example theft
- cloud providers typically offer 99.8% uptime SLA equating to no more than 2 hours planned outage per calendar month (24 X 7), this relieves Willow of this burden, and they can rest assured that their systems will be reliable and robust
- onboarding new sites and assets is much simpler and faster with no need for additional hardware, the built-in elasticity of cloud infrastructure makes this process very seamless and future growth and changes to working patterns at Willow will be manageable and achievable

### **Cons**

- as this is a service, there is a lack of detail on how the provider runs the firewalls
- as all rules, etc. are applied to the backend service migrating to a new supplier is more difficult
- traffic flows through a third party via the internet so there could be latency requiring a better internet connection

### **Recommendation**

Stand-alone firewalls would be too much administration and only protect the device they are installed on so for business use I would recommend that this type of firewall is not suitable.

We therefore need to look at the top products in the Hardware Firewall and Firewall as a Service categories and compare them.

### **Anti-virus**

#### **Information Source**

It is important to ensure that the information source used to compare anti-virus is impartial, not aligned with any vendor or reseller and acknowledged as a reliable source. For the purposes of determining the best anti-virus packages I have chosen to use Capterra for the following reasons:

- they are a free and trusted comparison platform with 15 years of experience
- they are acknowledged as the world's leading software review and selection platform

#### **Capabilities Required**

When looking at anti-virus software it is important to look at the capabilities of each product and ensure they offer a minimum of:

- anomaly/malware detection
- automatic scans
- data security
- endpoint protection software

- identity theft protection
- phishing protection
- real-time monitoring
- real-time alerts
- threat response
- VPN support

### **Recommendation**

In order to properly assess which anti-virus is best I will be using Capterra to evaluate the top 4 anti-virus products based upon requirements, these are:

- Antivirus Pro
- Bitdefender
- McAfee
- Cisco AMP (Advanced Malware Protection)

### **Virtual Private Network (VPN)**

#### **Information Source**

As with Firewalls and Anti-virus software it is important to ensure that information sources are impartial and not aligned with a vendor. After looking at the available sources I will be using TechRadar (<https://www.techradar.com>) as they have been in business since 2007 and they do not take any payment for product reviews. They also test products in real life with a minimum number of days functional testing before they write their reviews.

#### **Capabilities Required**

The VPN product should support the following capabilities as a minimum:

- dedicated IP
- IP allow listing
- custom DNS
- network segmentation
- Site-to-Site
- smart Remote Access
- biometrics
- unlimited Network Tunnels
- device posture check
- automatic WiFi Security
- sign out code
- phone support

## Recommendation

Looking at the VPN products available, I have discounted all but the following 3 products that will be evaluated:

- Perimeter 81
- NordLayer
- Cisco ASA 1100 VPN

## Product Comparison

### Firewalls

#### Source Reference

I have used Comparitech (<https://www.comparitech.com>) for the technical details of the Firewall Comparison as they are the leading industry resource for B2B data professionals and technology buyers. Founded in 2015, they have a team of 30 security researchers, writers, developers, and editors covering a wide range of cyber security topics. They extensively test and review products including VPNs, password managers, ID theft protection, anti-virus, network monitoring tools, and firewalls.

Using their website, the top 2 products include a hardware solution (Firepower Threat Defence) and a Firewall as a Service solution (perimeter 91).

I am also using TrustRadius (<https://www.trustradius.com>) and GetApp (<https://www.getapp.com/>) to get reviews from actual users of the products so we not only know the technical aspects but get an insight into real world use.

### Firepower Threat Defence (Cisco ASA 1100)

Price £550.00 Incl. VAT

#### User reviews

The Firepower 1100 user review is fairly positive with 26 of the 29 reviewers giving a positive scoring.

#### Pros

- simple graphical user interface (GUI) based functionality through the Cisco ASDM interface, this also has real time monitoring of interfaces and includes a packet tracer interface for network configuration and design
- vast resources for configuration and implementation, for example videos, handbooks and training materials
- excellent support services from Cisco for example forums, FAQs, online helpdesks and live chat
- real time throughput of traffic, this makes these devices very efficient and provides excellent network monitoring data
- ease of implementation as all GUI based, as well as robust command line interface (CLI) implementations on all Cisco ASA devices

#### Cons

- real time logging to console is limited
- to ensure redundancy will need 2 X Firepower 1100
- need to have staff with Cisco skillset

## **Tech spec**

The Firepower 1100 has a wide feature set:

### **Legal/Security Requirements**

There is a requirement to purchase licenses for the devices that will need to be reviewed. In addition, as these are physical devices there will be a need to provision in a secure area with adequate, redundant power, etc. Firewalls will block suspicious and malicious traffic when configured correctly, so in turn, reducing the risks of the company failing to meet Data Protection 2018 rules. Staff also have a responsibility with their behaviour when dealing with electronic documents and using data accurately in accordance with data protection legislation.

### **Summary**

The Firepower 1100 is a very capable device that will also provide malware protection and VPN capability but may require additional skills to manage and update the device with the associated training. It also requires a secure location to house it along with connections from that environment to any networking subnet the firewall has to control, I believe Willow technology will be able implement Firepower 1100 because they are targeted at small to medium businesses.

## **Perimeter 81**

### **Price**

£15 per user per month so £300 per month.

### **User Reviews**

The user reviews are good with a score of 8.5 out of 10, so 85%.

In addition, the general consensus is:

### **Pros**

- ease of use, the system is very intuitive and clutter free and has all the features required for Willow
- flexible remote access environment that provides an intuitive interface for configuring the system, this would be beneficial at Willow for remote administration
- behavioural Analytics are employed that would provide Willow with smarter security monitoring with the ability to monitor traffic and observe unusual activity and departures from network operations
- provides services including packet checking, signature recognition and real-time blocking of malicious sites and data, this is ideal for Willow because of their working patterns and typical online usage

### **Cons**

- occasional issues with connectivity and performance scalability
- no SSL security
- software can be resource hungry when completing certain operations

## **Tech Spec**

Perimeter 81 is a Secure Access Service Edge that has a Firewall as a Service solution as part of its design. A SASE comprises of technology used to deliver wide area network (WAN) and security controls as a cloud computing service directly to the source of connection, rather than a data centre. This also helps organizations support dispersed users and their devices with digital transformation and application

The solution supports: -

- Firewall as a Service (FWaaS) allowing multiple OS to use the virtual firewall
- endpoint security ensuring any endpoints connected are protected against malware
- Secure Web Gateway (SWG) blocking high risk websites, enforcing compliance, prevents malware and protects remote users
- Cloud Access Security Brokers (CASB) – enforces corporate security policies when accessing cloud resources

### **Legal/Security Requirements**

The product is fully cloud based and the data centres have SOC 1, SOC 2 and SOC 3 certification as well as ISO27001 certification so they are a secure environment. The product also supports 2 factor authentication.

### **Summary**

Perimeter 81 may seem like a more expensive option, but the following should be noted:

- no expensive hardware to buy and deploy
- no ongoing maintenance as the product is supplied as a service
- it forms part of a much larger offering that also provides VPN access
- it can be lined to many remote sites

### **Firewall Solution Choice and Rationale**

Perimeter 81 does not require expensive hardware, is managed as a service so does not require expensive skillsets for internal staff to support and it forms part of a larger cloud offering expanded to a SASE solution. For these reasons Perimeter 81 is the recommended firewall solution

I have chosen the Cisco ASA 1100 firewall, Cisco offers the industry's first threat-focused next-generation firewall and includes features such as unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint. Secure Firewall Management Center is a visual interface that helps monitor the system and is user friendly and intuitive.

### **Anti-virus**

Using Capterra I will evaluate the top 4 anti-virus products based upon requirements:

- Antivirus Pro
- Bitdefender
- McAfee
- Cisco AMP (Advanced Malware Protection)

These 4 products meet the minimum specs stated above in section 1.1.2.2 but we also need to take training and the support on offer when evaluating.

### **Anti-virus capabilities**

When looking at anti-virus software it is also important to look at the capabilities of each product and ensure they offer a minimum of:

- anomaly/malware detection
- automatic scans
- data security
- endpoint protection software
- identity theft protection
- phishing protection
- real-time monitoring
- real-time alerts
- threat response
- VPN support

**Anti-virus product comparison**

Product	Pros	Cons
Antivirus Pro Cost: \$ 29.00 per annum	<ul style="list-style-type: none"> <li>• meets minimum spec</li> <li>• cloud</li> <li>• email/helpdesk</li> </ul>	<ul style="list-style-type: none"> <li>• no on-premises</li> <li>• no live online</li> <li>• no webinars</li> <li>• no documentation</li> <li>• no videos</li> <li>• no FAQ/forum</li> <li>• no knowledge base</li> <li>• no 24/7 (live rep)</li> <li>• no pricing provided by vendor</li> </ul>
Bitdefender Cost: \$15.00 per annum	<ul style="list-style-type: none"> <li>• meets minimum spec</li> <li>• on-premises</li> <li>• live online</li> <li>• documentation</li> <li>• email/helpdesk</li> <li>• FAQs/forum</li> <li>• knowledge base</li> <li>• phone support</li> </ul>	<ul style="list-style-type: none"> <li>• no cloud</li> <li>• no webinars</li> <li>• no videos</li> <li>• no 24/7 (live rep)</li> </ul>
McAfee Cost: \$23.99 one-off	<ul style="list-style-type: none"> <li>• meets minimum spec</li> <li>• cloud</li> </ul>	<ul style="list-style-type: none"> <li>• no on-premises</li> <li>• no live online</li> <li>• no webinars</li> </ul>

		<ul style="list-style-type: none"> <li>• no documentation</li> <li>• no videos</li> <li>• no 24/7 (live rep)</li> </ul>
Cisco AMP (Advanced Malware Protection) Cost: \$53.76	<ul style="list-style-type: none"> <li>• uses global threat intelligence data from Cisco Threat Grid and Cisco Talos</li> <li>• is on the same device (Cisco ASA 1100) as the firewall and VPN, so is a central point for security at Willow</li> </ul>	<ul style="list-style-type: none"> <li>• some false positives of found malwares</li> <li>• price is a bit expensive especially if your network has many devices</li> </ul>

### Anti-virus Solution Choice and Rationale

Based upon the above comparison we must rule out Bitdefender as it does not offer cloud support this leaves Antivirus Pro as a possibility, a product that meets minimum spec and cloud requirements.

I have chosen Cisco AMP for the fact that it offers excellent malware protection, and the other deciding factor is that it will be part of the Cisco ASA 1100 and will provide Willow with a central point for malware protection, firewall and VPN.

Taking the above into account, the rational choice for anti-virus product is therefore **Cisco AMP**.

### Virtual Private Network (VPN)

When looking at a VPN provider it is important to consider those that have specifically been setup for Business VPN. There are many public VPN providers but the size and capability of their VPN offering means that they are not set up to support a business. The following capabilities should be available:

- the provider offers services that cater specifically to businesses
- speed and stability
- strong security
- number of simultaneous connections
- apps for Android, iOS, Windows, and MacOS

As detailed in section 1.1.3.3 above, I have slimmed down the VPN products for review and selection to:

- Perimeter 81
- Cisco ASA 1100 VPN

### Perimeter 81

Perimeter 81 is a specialist business VPN that allows businesses to deploy private VPN servers that staff can securely connect to from anywhere in the world. They allow admins. to manage network activity for all staff via an online dashboard. This will allow employees to securely access files, apps, and other resources securely from remote locations.

Pricing: £8 per user per month

The key features of the product are:

- dedicated IP
- IP allow listing
- custom DNS
- network segmentation
- Site-to-Site
- smart remote access
- biometrics and multi-factor authentication (MFA)
- unlimited network tunnels
- device posture check
- automatic WiFi Security
- sign out code
- phone support

Perimeter 81:

- caters to businesses with unique security features like network segmentation to isolate sensitive data from breaches
- allows your business to connect offices in different locations using site-to-site VPNs to connect the 2 networks
- allows remote access via cloud VPNs and can easily be scaled up as needed

All data is encrypted with 256-bit AES. If you do not deploy your own VPN, you can choose from 700 public servers in 36 locations around the world. Businesses can monitor access to the VPN by logging and inspecting all traffic that passes through it.

Apps are available for Windows, MacOS, Linux, iOS, Android, and Chrome.

### **Pros**

- caters specifically to businesses
- deploy your own server or choose from public ones
- supports site-to-site VPNs
- host apps and files on the VPN server
- strong encryption
- supports network segmentation
- can be linked to a cloud infrastructure that includes Firewall as a Service

### **Cons**

- compared to some VPN solutions the cost per user is more expensive



## Cisco ASA 1100 VPN

Cisco ASA 1100 VPN is a VPN for small to medium sized businesses that can be easily set up to provide 2 main types of service. These are outlined below.

### Remote Access VPN

A remote access virtual private network (VPN) enables users to connect to a private network remotely using a VPN. Employees who need to access their company's network from off-site locations or people who want to securely connect to a private network from a public area frequently use this kind of VPN.

Cisco have a product called AnyConnect VPN that offers full network access. The remote user will use the AnyConnect client to connect to the Cisco ASA.

### Site-to-Site VPN

Site-to-Site IPsec VPN Tunnels are used to allow the secure transmission of data, voice and video between 2 sites (for example, offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the 2 sites.

Every user account can be managed from a single, centralised control panel.

Pricing: AnyConnect Plus is offered as a perpetual license in addition to the 1, 3 or 5 year terms. Cisco also offers a perpetual VPN-only license.

The key features of the product are:

- remote access
- Site-to-site
- phone support
- posture enforcement
- web security features
- roaming protection

### Pros

- has everything Willow requires
- fast and reliable connections
- remote access control
- real time monitoring
- supports AES-256 and 3DES-168
- supports multi-factor authentication (MFA)
- supports both SSL and IPsec VPN options
- unlimited bandwidth and no data caps
- apps for Windows, MacOS, iOS, Linux and Android

### Cons

- can be more expensive than other less feature rich alternatives
- can be harder to configure

### **VPN Solution Choice and Rationale**

Perimeter has a wide feature set and is very cost effective for Willow, but I have chosen the more robust and feature rich option that has a big advantage of integrating with the Firewall and Anti-Virus and provides all of the security requirements on one physical device.

For these reasons the recommended VPN solution is **Cisco ASA VPN using Anyconnect.**

### **Overall Rationale for Anti-Virus, Firewall and VPN**

The Cisco 1100 ASA will provide anti-virus, firewall and VPN all in one physical device, this will meet all the requirements that Willow require, these devices are modular, so they can be expanded with additional functionality when required. Cisco also provide additional subscription options for additional services if the need arises. Multiple ASA devices can be controlled from one control panel which means that future expansion of the infrastructure at Willow will be achievable.

### **User Access Control**

The VPN will provide a layer of access control for network users when working remotely. The NCSC government website (<https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks>) contains information regarding the correct use of VPN technology and should be accessed by policy makers. One of the most crucial elements to get right is the security of the connections, if this is not correct then it can lead to data breaches that could incur fines and loss of reputation when made public. The use of protocols including IPsec and OpenVPN and the avoidance of less secure protocols like PPTP is required.

As well as the VPN, there also needs to be additional access controls that covers all users, regardless of location when accessing the network for example, on-site or remote. Below are the recommended controls to improve security for Willow.

### **Device Level**

User accounts need to set up and configured on the personal device, this can be achieved through joining devices to the Active Directory domain at Willow. This will provide central authentication and provide access to all services the user would normally use for example, Office 365 apps including, office, teams and OneDrive. Additional security can be configured through Microsoft's Windows Hello feature allows you to sign in to your computer using biometric methods such as facial or fingerprint recognition. Multi Factor Authentication can also be used when connecting to the domain, this can be achieved through username, password and code sent via SMS.

### **Server Level**

Setting up a server as a domain controller will allow the rollout of user groups/organisational units, permissions and advanced authentication methods, I.e. Multi Factor Authentication (MFA), MFA is commonly achieved through SMS, but additional alternatives include:

- Windows Hello for Business.
- Microsoft Authenticator app.
- FIDO2 security key (preview)
- OATH hardware tokens (preview)
- OATH software tokens
- voice call verification.

There are additional methods for controlling access to resources, which include; Discretionary Access Control (DAC), Mandatory Access Control (MAC), Attribute-based Access Control (ABAC), and Role-Based Access Control (RBAC).

Role based access methods can be employed on the server to manage permissions. The advantage to Willow of RBAC is that control can be achieved at user level through the assignment of roles, and roles are assigned permissions, such as create, read, update, and delete. Roles can be grouped together to establish role groups.

The methods discussed above would allow all end devices to join the domain and be controlled centrally, this will also allow security policies and Windows updates to be rolled out to all devices and if Willow were to move to a cloud model, the user access control methods could be migrated to Microsoft Azure.

**Legal/security requirements**

**Computer Misuse Act**

The Computer Misuse Act covers the following offences:

- unauthorised access to computer material (hacking)
- unauthorised access with intent to commit or facilitate commission of further offences (spyware/ransomware)
- unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer (denial of service)

Protection against these types of attack require a firewall and anti-virus:

Offence	Prevented by firewall	Prevented by anti-virus
Hacking	Yes	No
Denial of service	Yes	No
Ransomware	No	Yes
Spyware	No	Yes

As can be seen in the table above, a combination of firewall and anti-virus products will protect against computer misuse.

**Fraud Act 2006**

The Fraud Act 2006 seeks to protect against acts of fraud however perpetrated, in this instance the fraud is targeted at computer users (phishing, vishing, spear phishing, identity theft). This requires both a firewall and anti-virus:

Exploit	Prevented by firewall	Prevented by anti-virus
Phishing	No	Yes
Vishing	Yes	No
Spear phishing	Yes	No

Identity theft	No	Yes
----------------	----	-----

As can be seen in the table above, a combination of firewall and anti-virus products will protect against most computer-based fraud attempts.

**Theft Act 1990**

The Theft Act 1990 covers theft using a computer and this can include data theft, breach of confidence and Criminal Copyright Theft.

Unfortunately, firewall and anti-virus solutions will not protect against these, there needs to be a measure put in place that can assess data flowing into and out of the computer network. This would need a data loss prevention (DLP) solution that could inspect data from multiple systems such as email or Teams, and quarantining messages where a ruleset was triggered indicating a possible information protection (IP) issue.

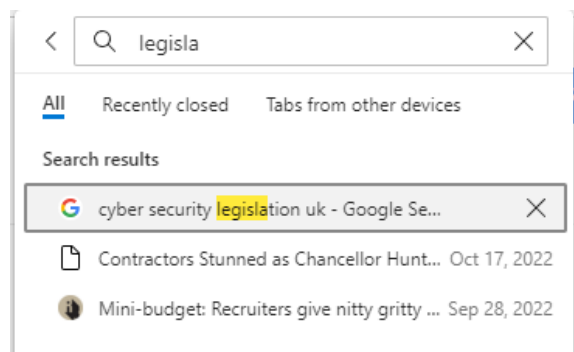
### Browser history firewalls

A screenshot of a browser search history window for the term 'firewall'. The search bar at the top contains 'firewall' with a search icon on the left and a close icon on the right. Below the search bar are three tabs: 'All' (selected), 'Recently closed', and 'Tabs from other devices'. A 'Top results' section contains five entries: 'software firewalls - Google Search' (Nov 7, 2022), 'Firewall Software - Price Comparison &...' (Nov 7, 2022), 'What is Software Firewall? Difference b...' (Nov 6, 2022), 'Top 10 BEST Free Firewall Software For ...' (Nov 7, 2022), and 'Comodo Firewall | Get Best Personal Fir...' (Nov 6, 2022). Below this is an 'All results' section with ten entries, including 'Top 10 BEST Free Firewall Software For ...' (Nov 7, 2022), 'Top 10 BEST Free Firewall Software For ...' (Nov 7, 2022), 'Firewall Software - Price Comparison &...' (Nov 7, 2022), 'Firewall Software - Price Comparison &...' (Nov 7, 2022), 'Firewall Software - Price Comparison &...' (Nov 7, 2022), 'software firewalls - Google Search' (Nov 7, 2022), 'windows defender firewall - Google Se...' (Nov 6, 2022), 'Configuring Windows Firewall Rules Us...' (Nov 6, 2022), 'Turn Microsoft Defender Firewall on or ...' (Nov 6, 2022), and 'Turn Microsoft Defender Firewall on or ...' (Nov 6, 2022). The final entry is 'windows 10 enterprise firewalls - Googl...' (Nov 6, 2022).

### Browser history anti-virus

A screenshot of a browser search history window for the term 'antivirus'. The search bar at the top contains 'antivirus' with a search icon on the left and a close icon on the right. Below the search bar are three tabs: 'All' (selected), 'Recently closed', and 'Tabs from other devices'. A 'Top results' section contains five entries: 'Antivirus Pro vs Bitdefender Antivirus Plu...' (Nov 8, 2022), 'antivirus software features list - Google S...' (Nov 7, 2022), 'AntiVirus - Price Comparison & Reviews ...' (Nov 8, 2022), 'AntiVirus - Price Comparison & Reviews ...' (Nov 8, 2022), and 'AntiVirus - Price Comparison & Reviews ...' (Nov 7, 2022). Below this is an 'All results' section with ten entries: 'Antivirus Pro vs Bitdefender Antivirus Plu...' (Nov 8, 2022), 'AntiVirus - Price Comparison & Reviews ...' (Nov 8, 2022), 'AntiVirus - Price Comparison & Reviews ...' (Nov 8, 2022), 'Antivirus Pro vs Bitdefender Antivirus Plu...' (Nov 7, 2022), 'AntiVirus - Price Comparison & Reviews ...' (Nov 7, 2022), 'AntiVirus - Price Comparison & Reviews ...' (Nov 7, 2022), 'AntiVirus - Price Comparison & Reviews ...' (Nov 7, 2022), 'antivirus software features list - Google S...' (Nov 7, 2022), and 'Microsoft Start' (Aug 24, 2022).

## Browser history legislation



## References and resources

[Cybersecurity Laws and Regulations Report 2022 England & Wales \(iclg.com\)](#)

[Firewall Software - Price Comparison & Reviews - Capterra UK 2022](#)

[Antivirus Pro vs Bitdefender Antivirus Plus vs McAfee Total Protection vs Trend Micro Antivirus + Comparison - Capterra UK 2022](#)

## Task 2: set-up – devices, network and access

### Time limit

5 hours 30 minutes

You can use the time how you want, but all parts of task 2 must be completed within the time limit.

(20 marks)

### Instructions for students

Install the supplied OS on the device that has been provided to you (laptop/computer/ virtual machine) and configure a local administration account and a local user account.

Secure the device through the installation of the supplied software:

- firewall
- anti-virus
- virtual private network (VPN) to ensure the user has a private and secure internet connection
- demonstrate your ability to complete the installation by correctly configuring the supplied software
- run a scan to check everything works and if any software programs have not been successfully installed and configured, undertake remedial action to rectify the issue

Whilst doing this task, you must create a log that demonstrates:

- the steps followed for the installation of all software programs that have been installed
- evidence of the supplied software functioning correctly
- results of any scans you have run, and all remedial action undertaken if problems are identified

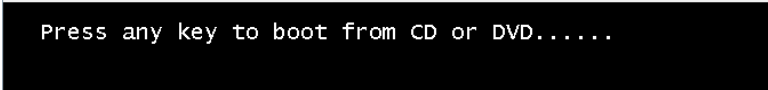
The log may include screenshots as appropriate.

### Evidence required for submission to NCFE

You will submit evidence including but not limited to:

- log

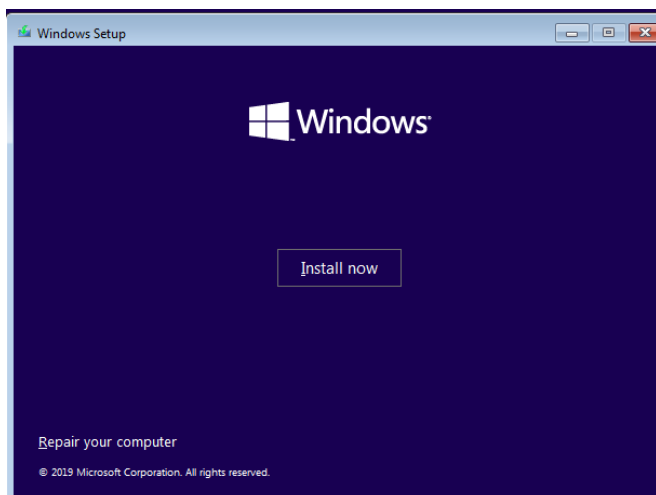
### Student evidence

1. Insert media (USB or CD) and boot the system from the media, you may need to enter the system BIOS to enable booting from external media. If so, query the motherboard/BIOS manufacturers manual to find out how to do this
2. Upon boot you will see a message asking you to press a key to boot from a CD or DVD  

3. You will be presented with the initial screen to select language, time and currency format and keyboard or input method

4. Switch all to United Kingdom except Language to install on boot from Windows 10 media is English (United States)

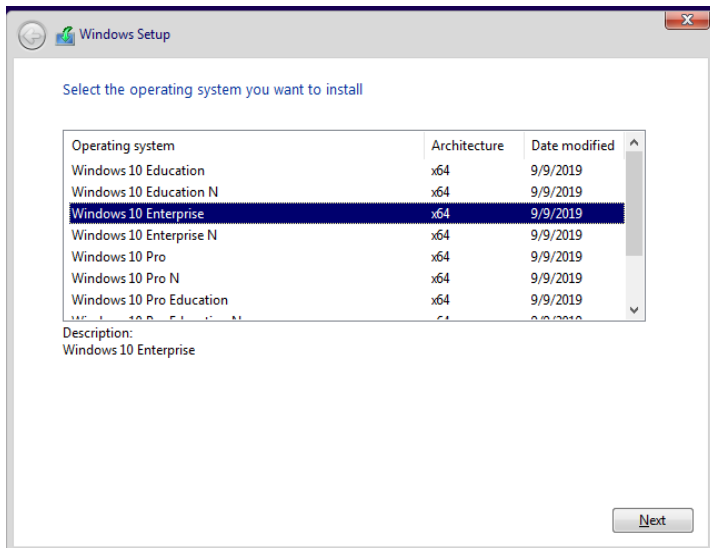


5. Click Install Now

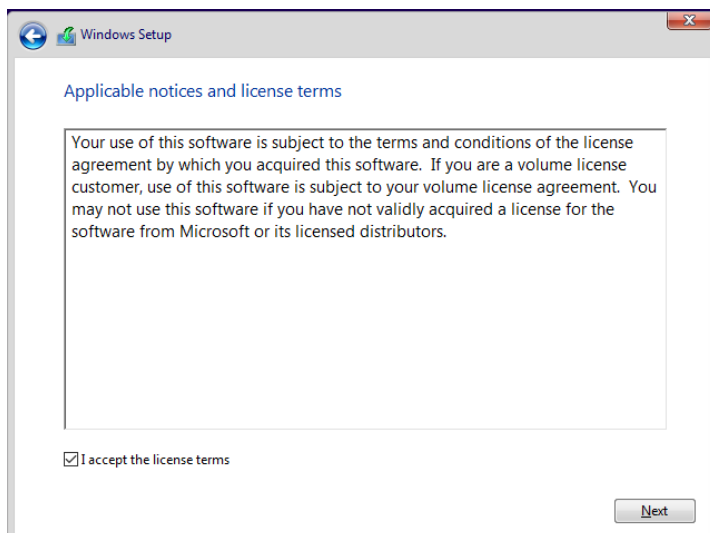


6. You will see a message that setup is starting
7. Select Windows 10 Enterprise

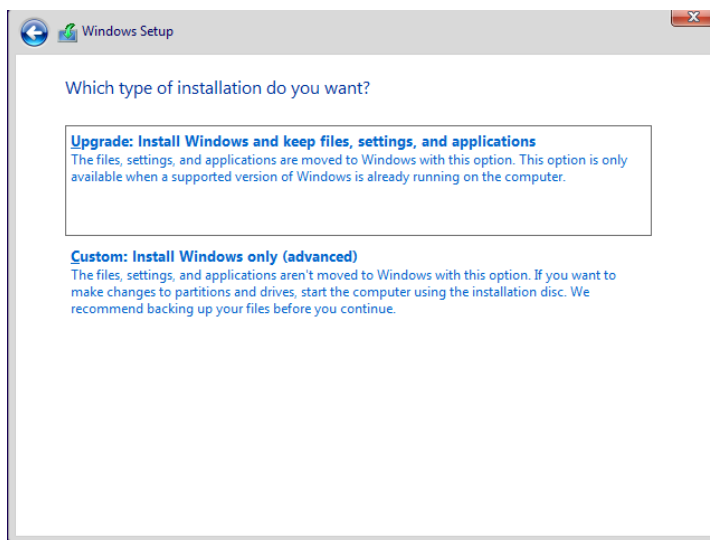




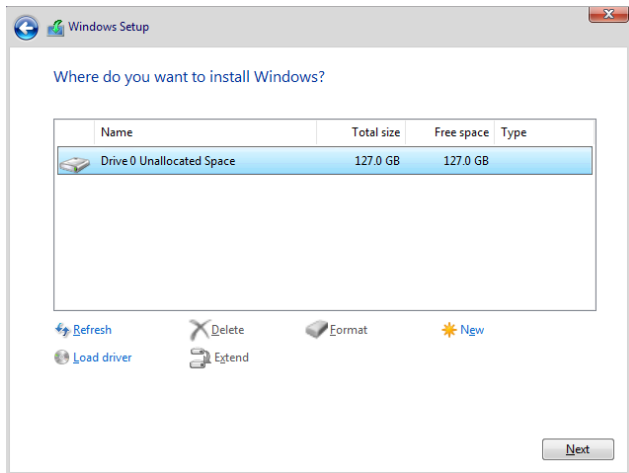
### 8. Select I Accept License



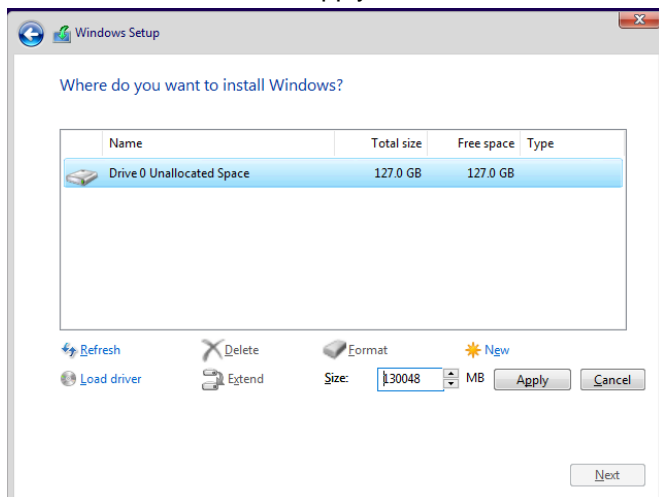
### 9. Select Custom Install



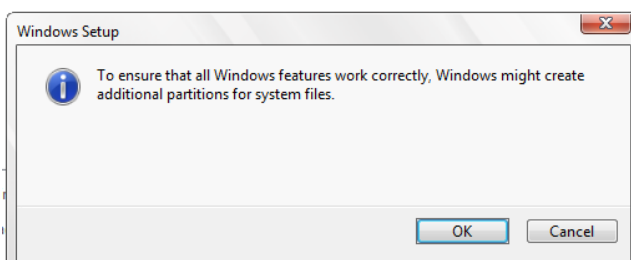
### 10. Select Unallocated Space



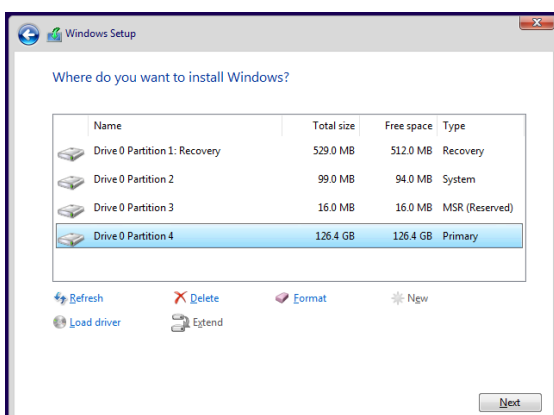
### 11. Click New and then Apply



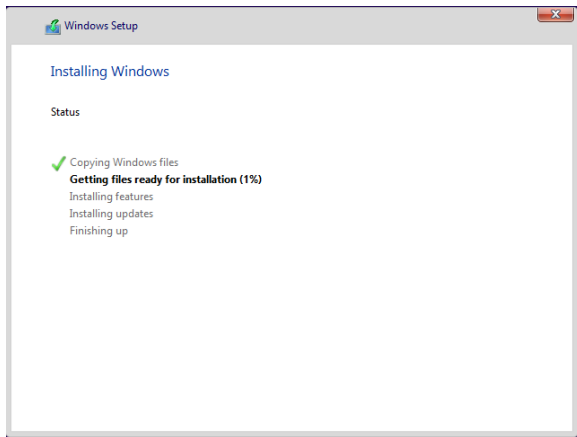
### 12. Select OK to let Windows create partitions



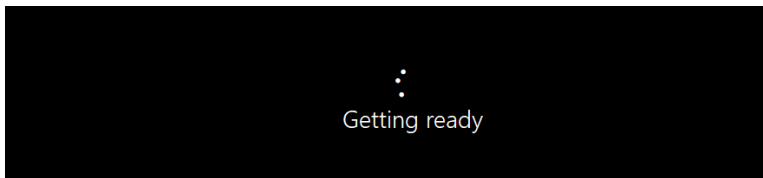
### 13. Select Primary and then Next



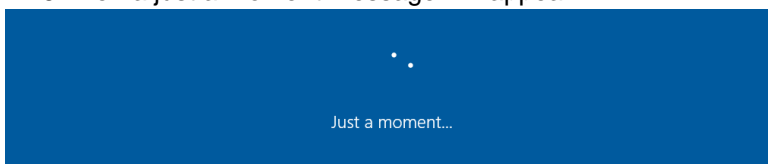
14. Windows will run through the install steps



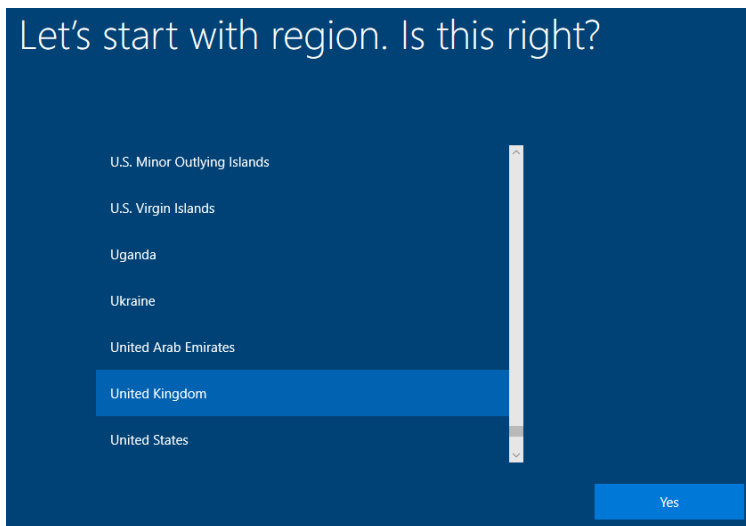
15. When finished, a Getting Ready message will appear



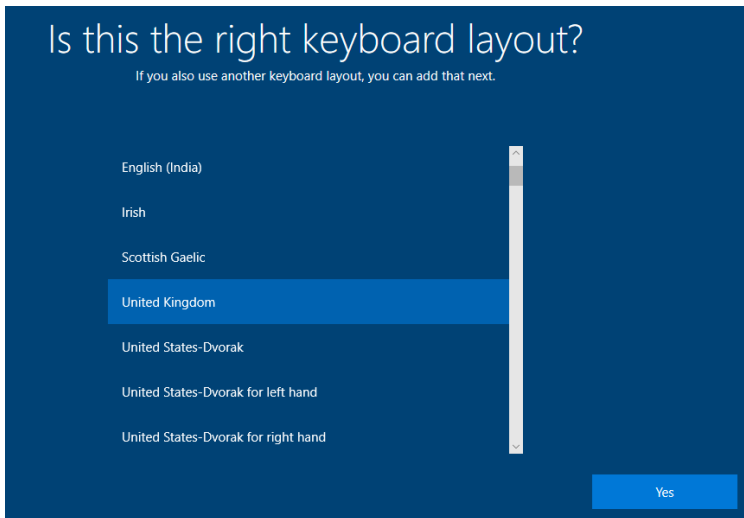
16. Then a just a moment message will appear



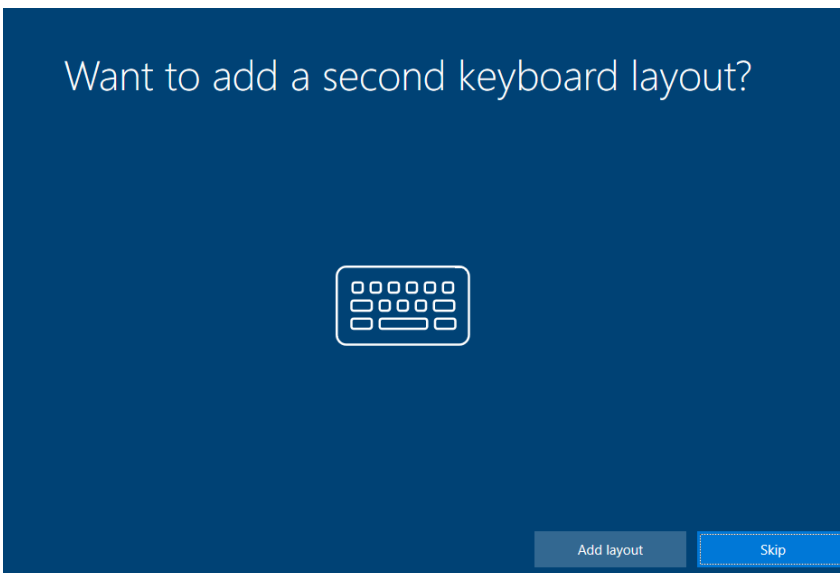
17. Next select United Kingdom as the region



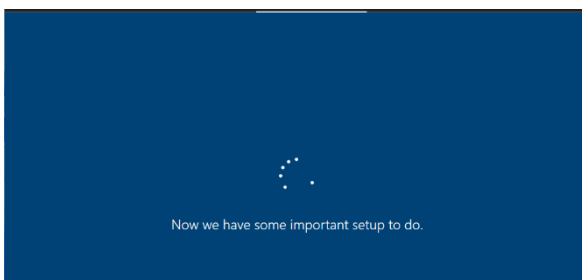
18. Select United Kingdom as the keyboard



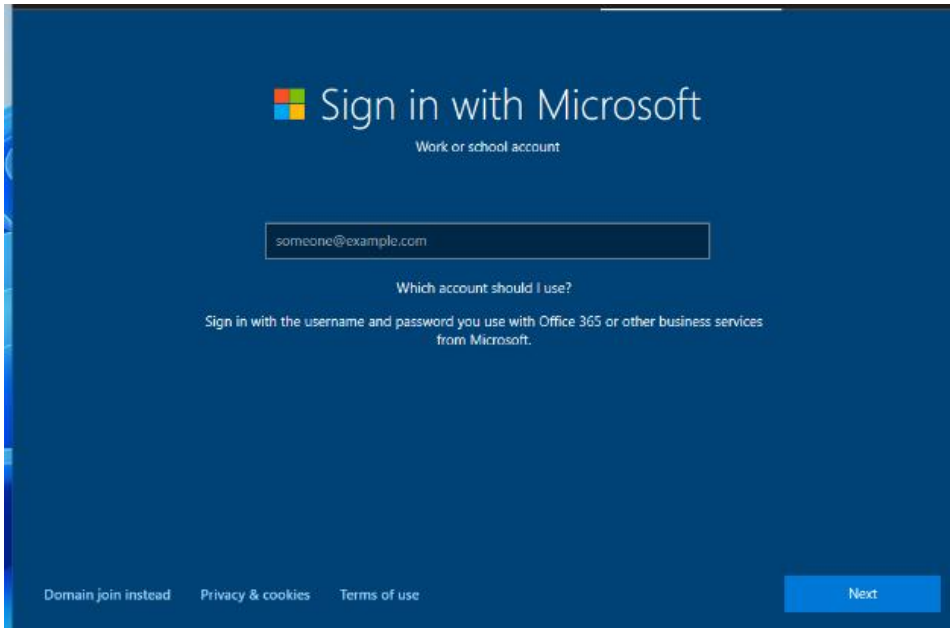
19. Click Skip when prompted for an additional keyboard



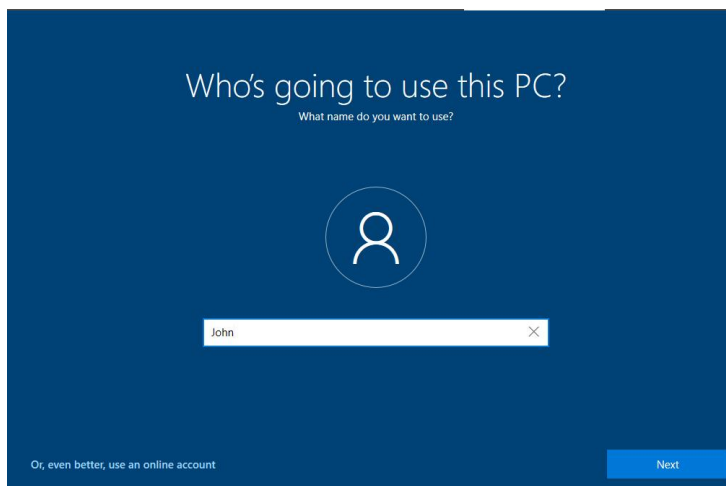
20. Windows will do the setup



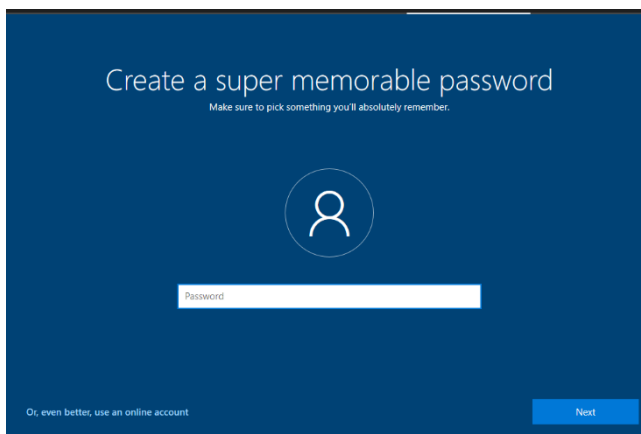
### 21. Click Domain Join



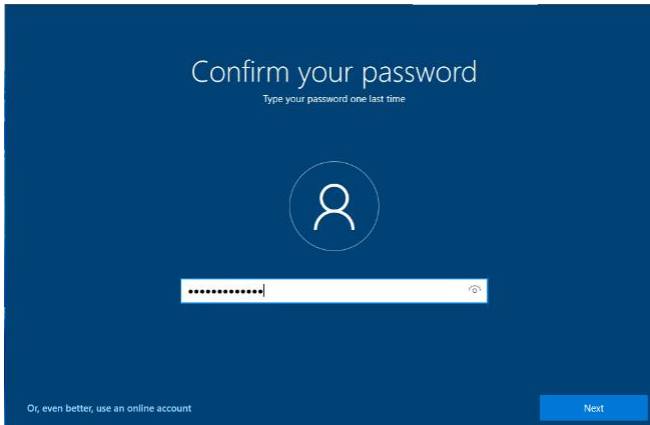
### 22. Add the local username



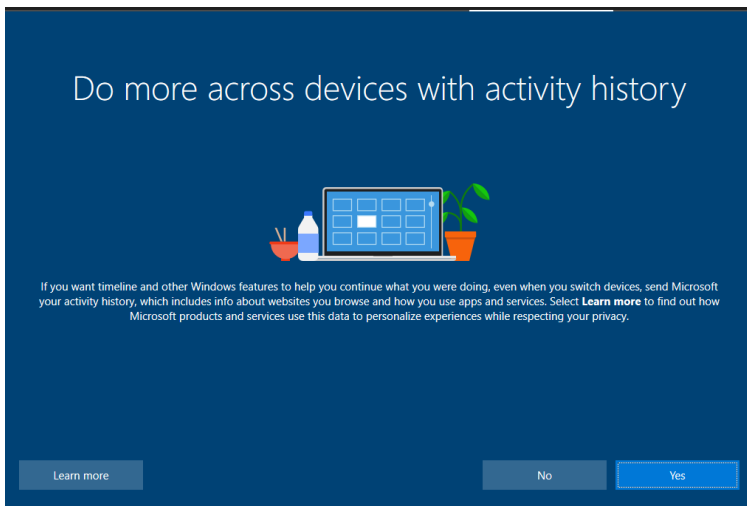
### 23. Create a password



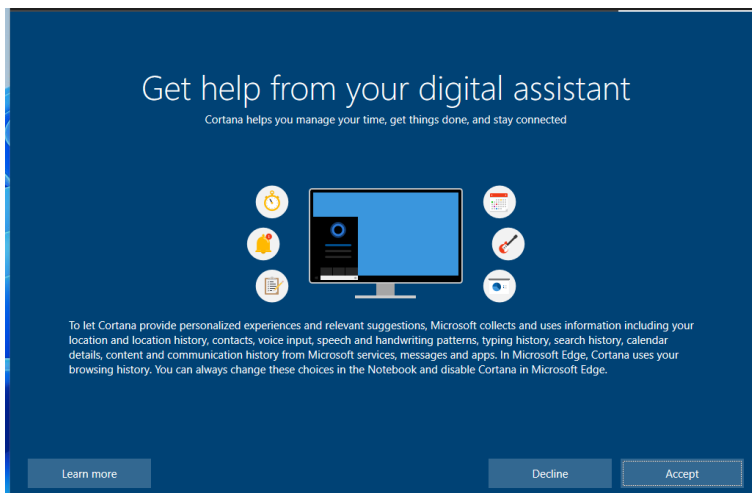
### 24. Confirm password



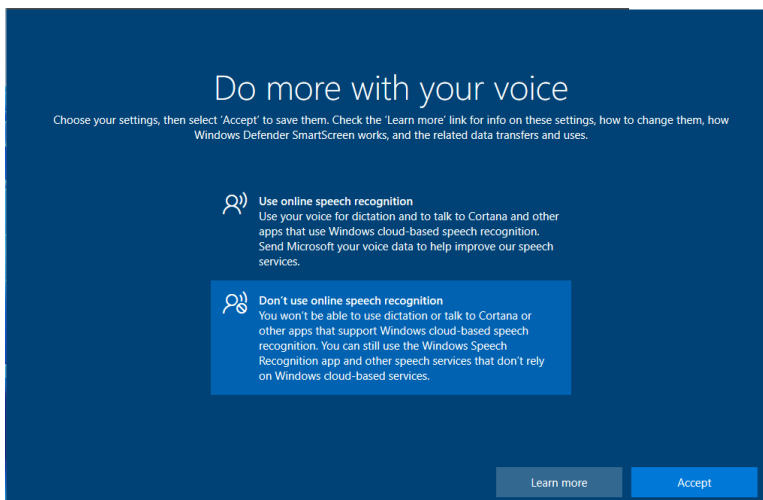
### 25. Select no to the next screen



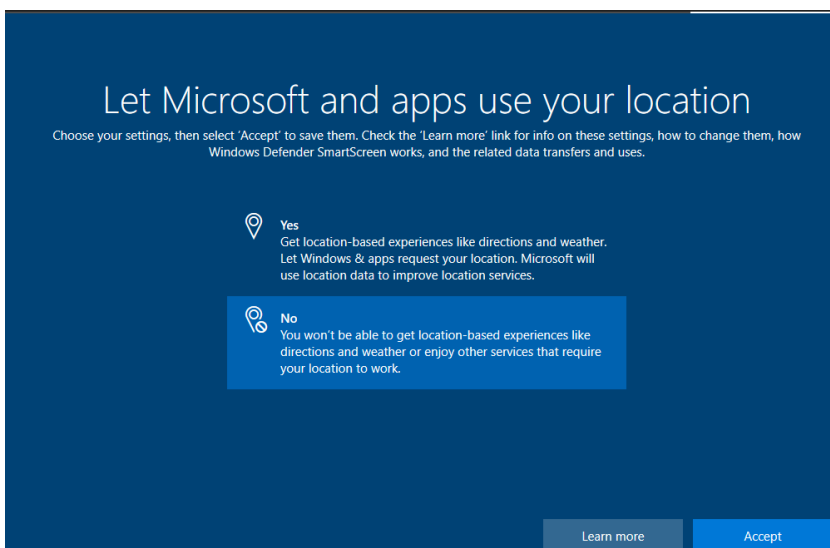
### 26. Select Decline for the next screen



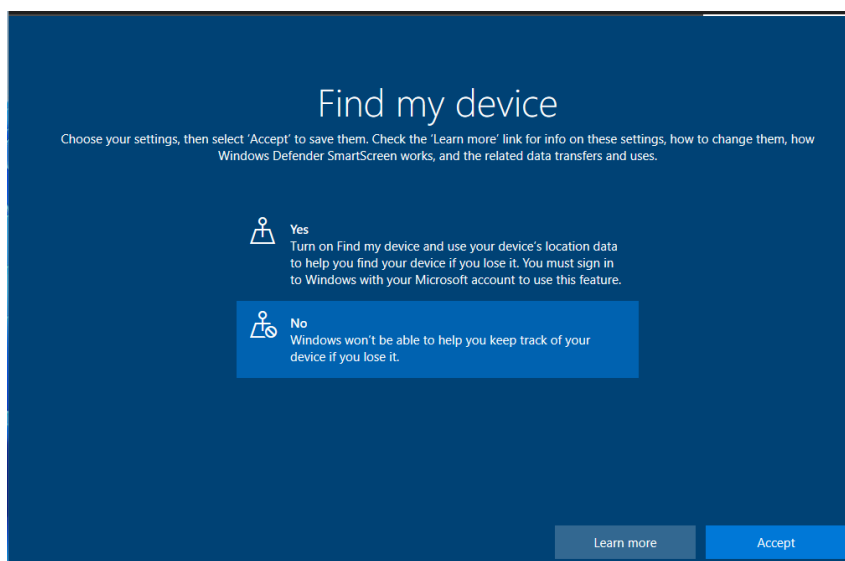
### 27. Do not use speak recognition



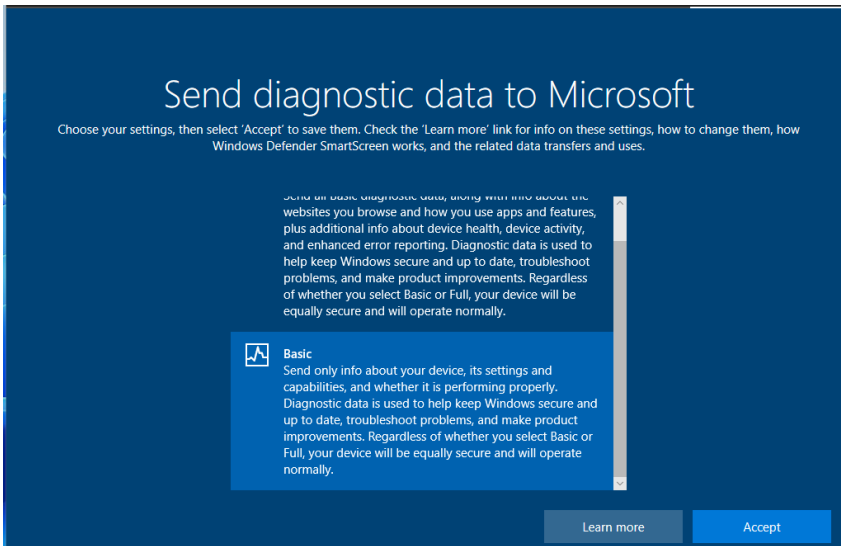
### 28. Select no for Location



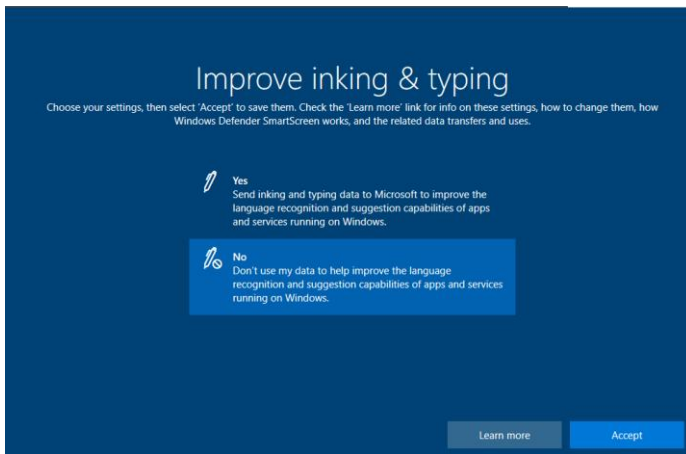
### 29. Select No for Find My Device as it is a desktop



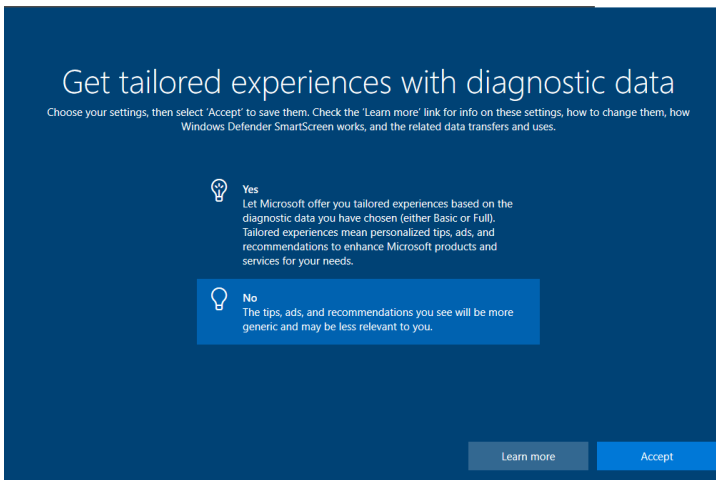
### 30. Select Basic data



### 31. Select No to improve inking

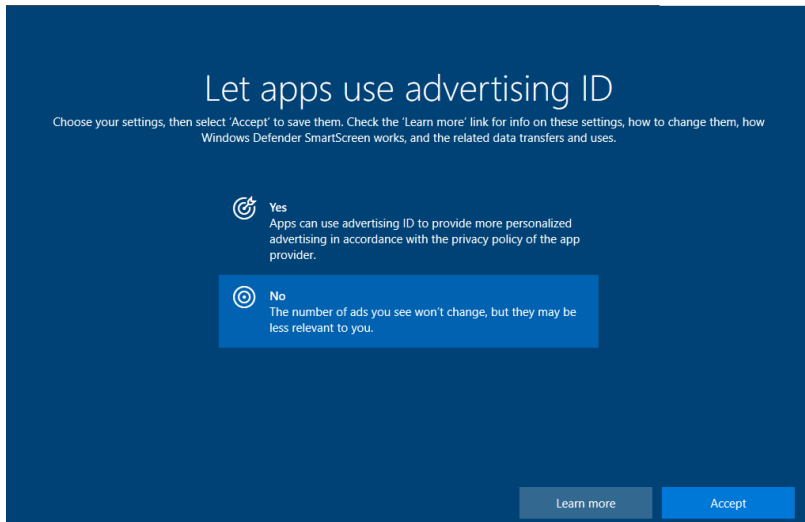


### 32. Select no to Tailored experiences

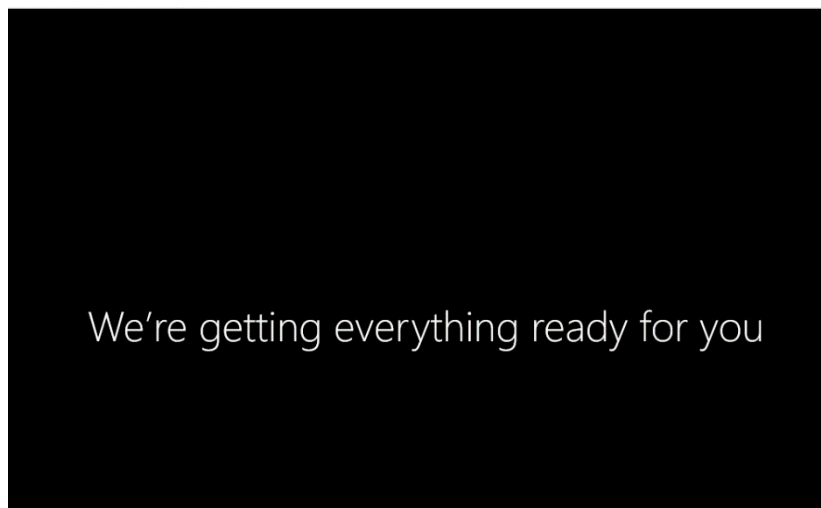




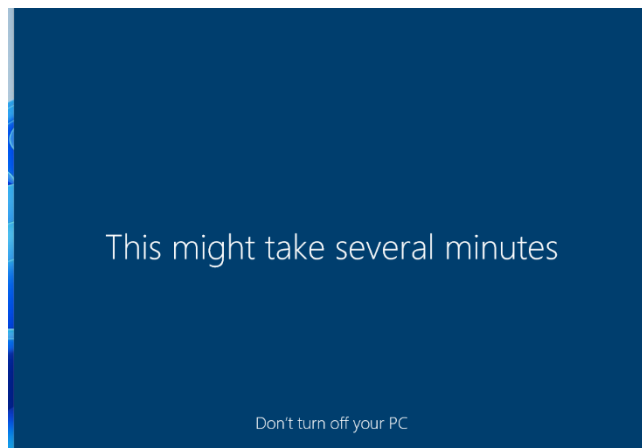
### 33. Select No to Advertising ID



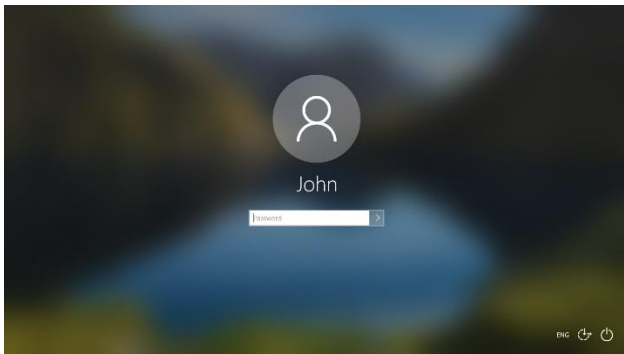
### 34. The computer will then get ready



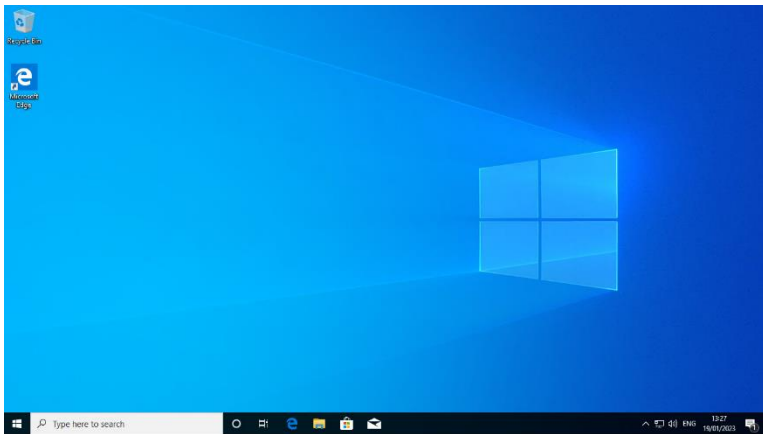
### 35. A message will appear stating it may take several minutes



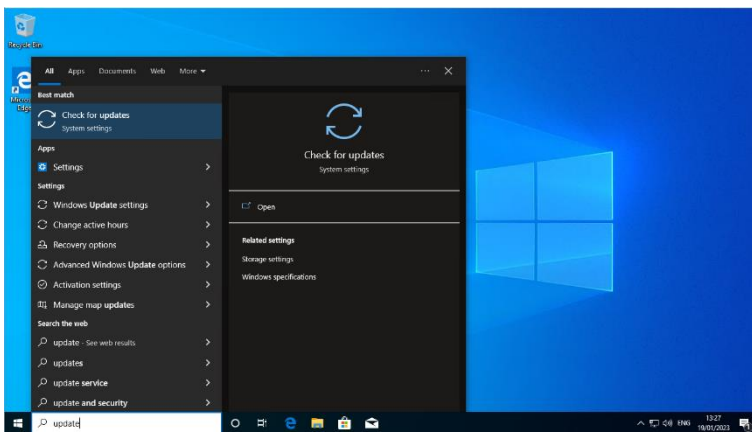
36. You will eventually be prompted to log in



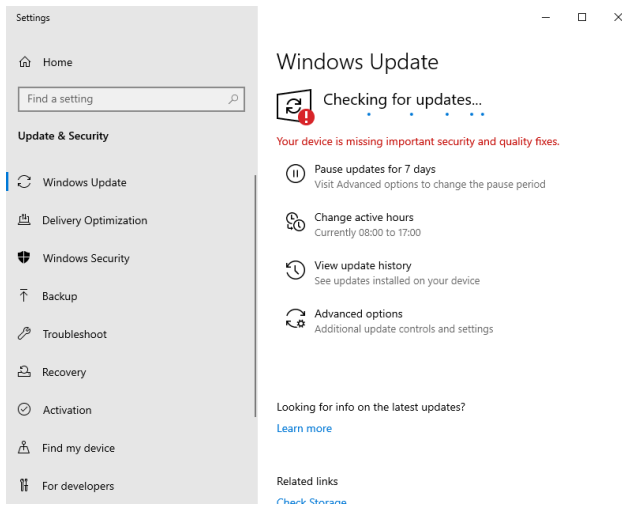
37. You will now see a desktop



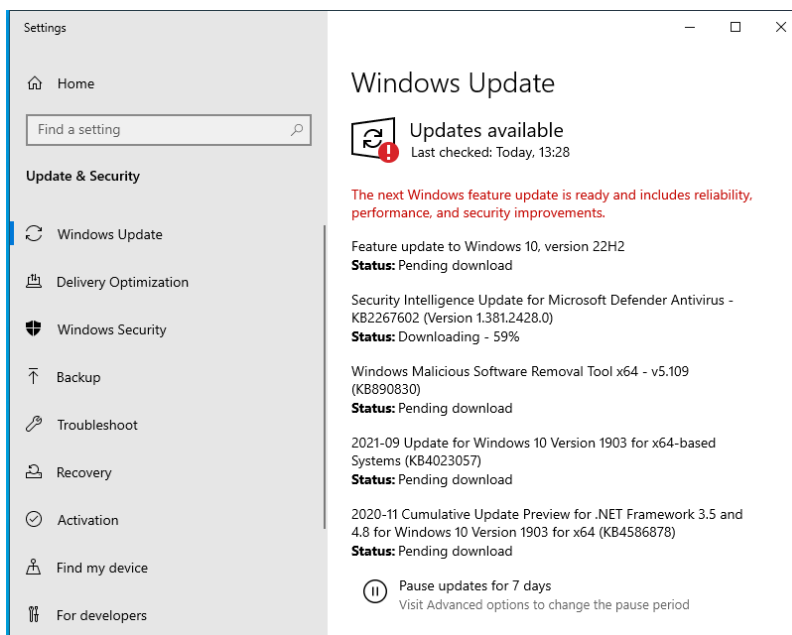
38. Start typing Update in search and select Check for updates



### 39. Click Check and the PC will then check for updates

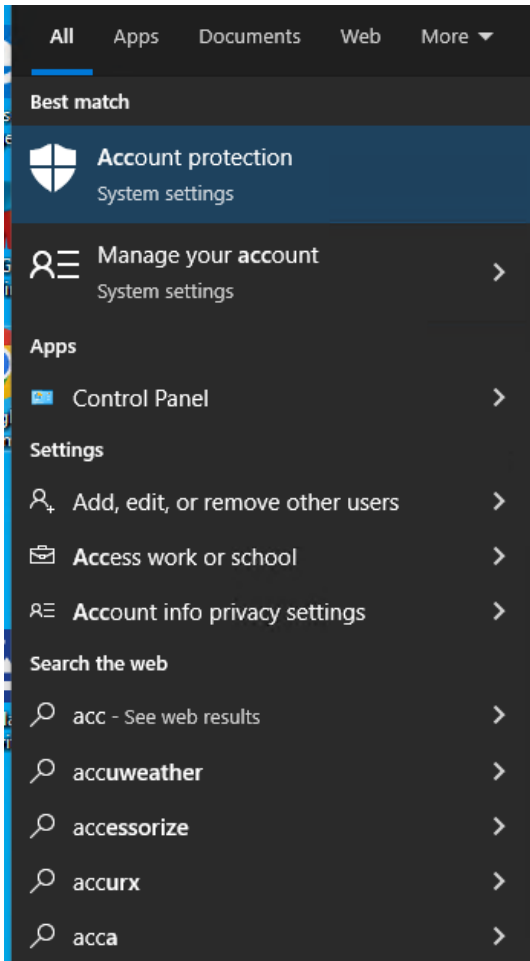


### 40. The PC will then start downloading and installing updates

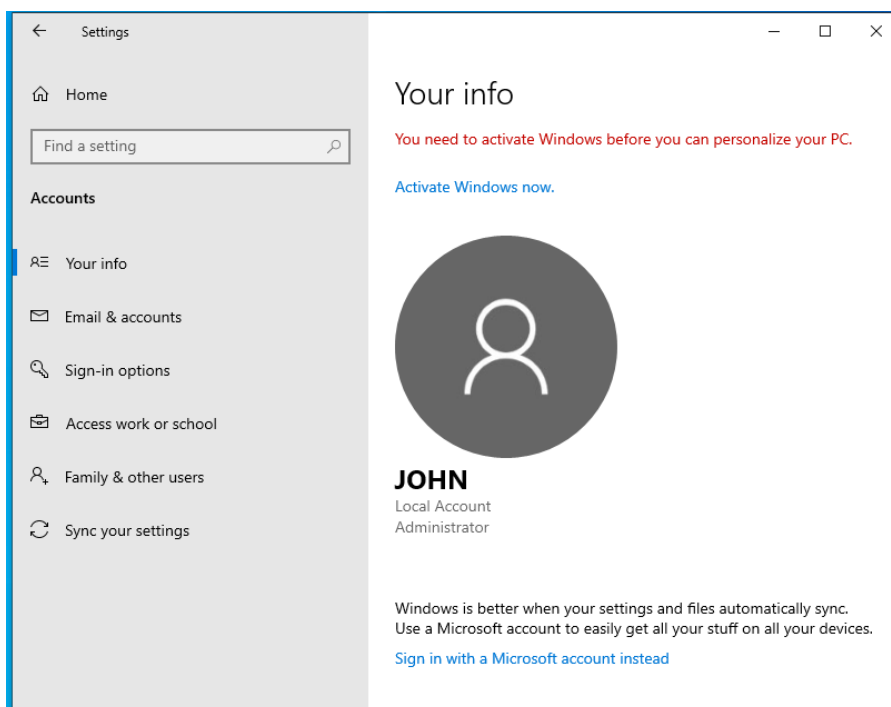


## Create Accounts

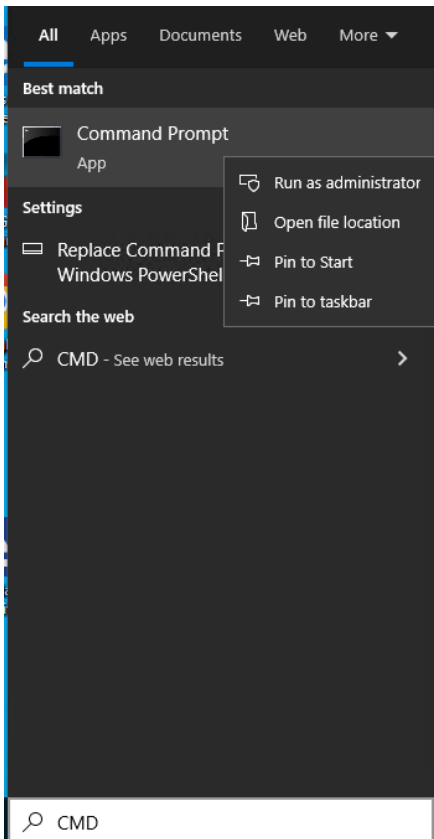
1. Type accounts in the search window and select Manage your account



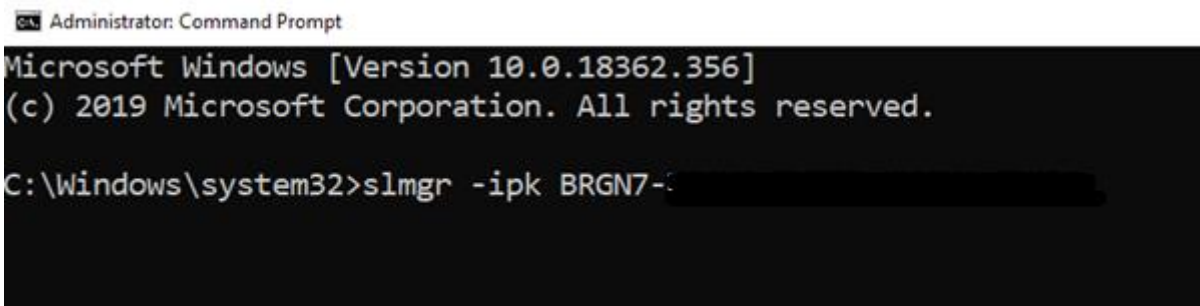
2. You may see a window telling you to activate Windows



3. We need to enter the key so type Command in the search window, right-click command prompt and choose Run as administrator

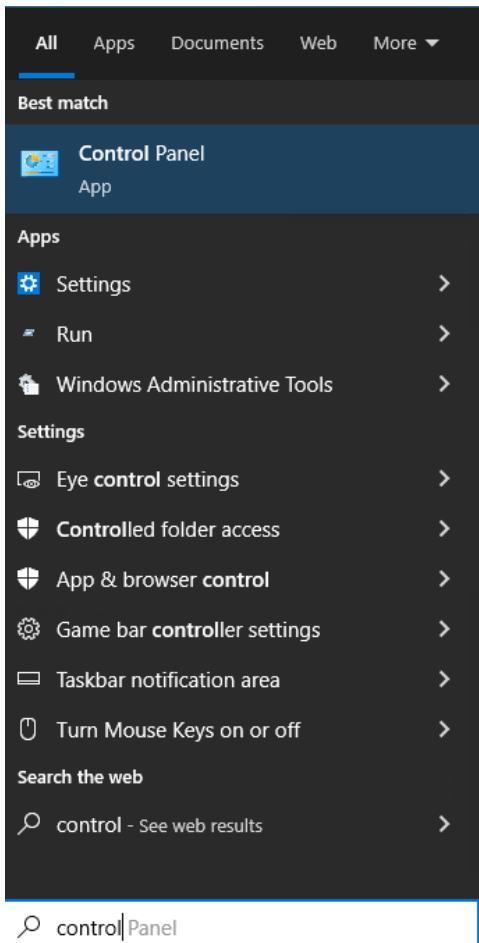


4. If prompted by User Account Control, select yes and you will see a command window
5. Type `slmgr -ipk` then the key (blocked out below to protect key) and press enter

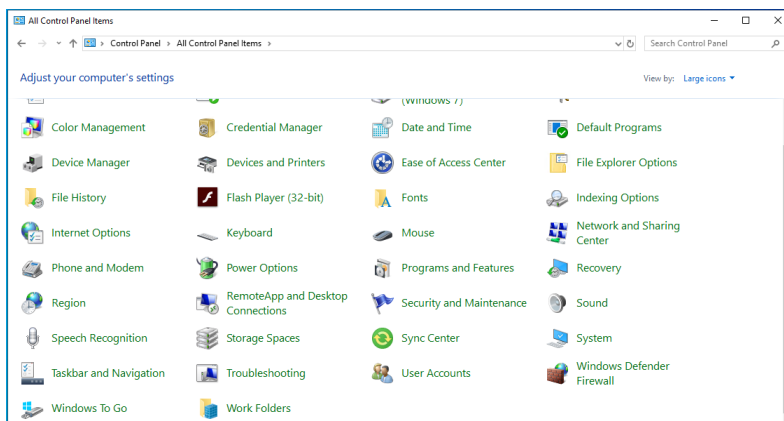


6. You will see that a window pops up to advise the key is installed

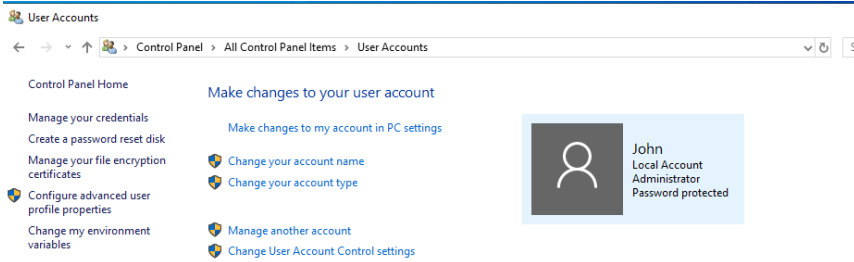
7. Type Control Panel and select it from menu



8. Select User Accounts

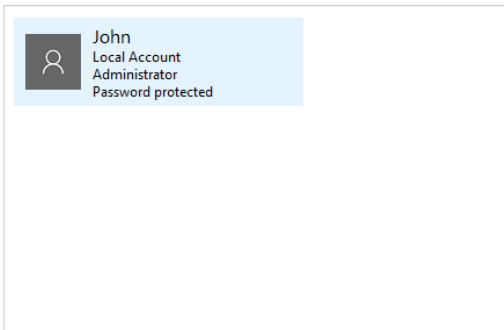


## 9. Select Manage another account



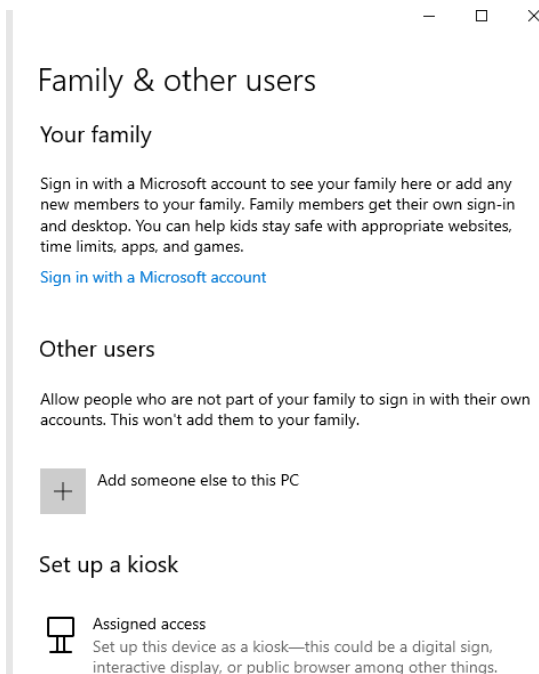
## 10. Select add a new user

Choose the user you would like to change

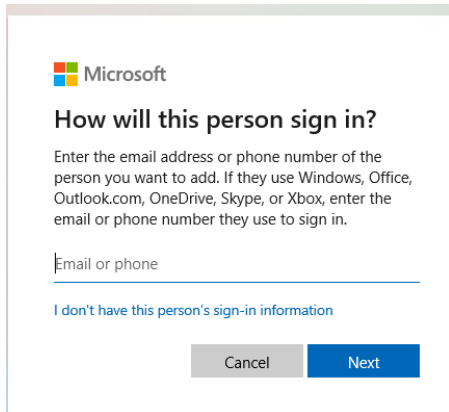


[Add a new user in PC settings](#)

## 11. Select Add someone else



### 12. Select I don't have this person's sign-in information



Microsoft

#### How will this person sign in?

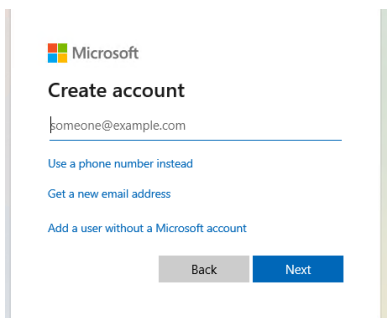
Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

Email or phone

[I don't have this person's sign-in information](#)

Cancel Next

### 13. Select Add a user without a Microsoft account



Microsoft

#### Create account

someone@example.com

[Use a phone number instead](#)

[Get a new email address](#)

[Add a user without a Microsoft account](#)

Back Next

### 14. Type the username and password

Microsoft account ×

#### Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

#### Who's going to use this PC?

User name

#### Make it secure.

Enter password

Re-enter password

Next Back

#### Who's going to use this PC?

JohnD ×

#### Make it secure.

●●●●●●●●

●●●●●●●●



15. Answer the security questions

### In case you forget your password

What was your first pet's name? ▼

Rover

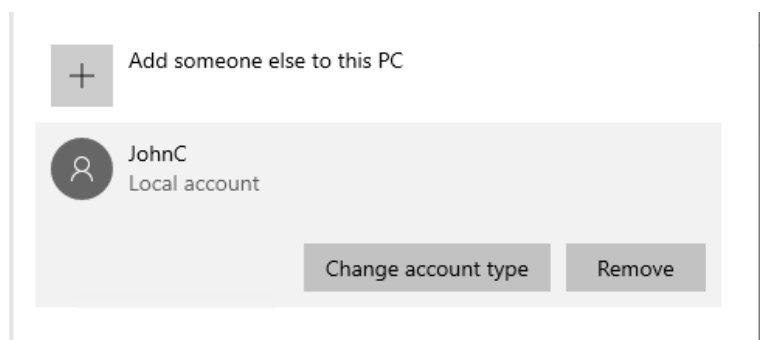
What's the name of the city where you were born? ▼

London

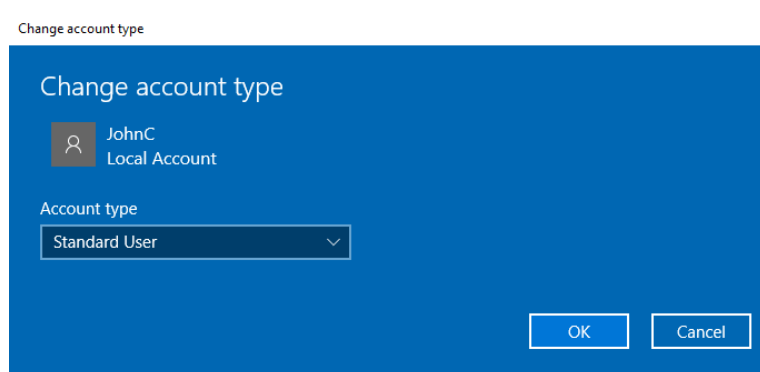
What's the first name of your oldest cousin? ▼

Eric ×

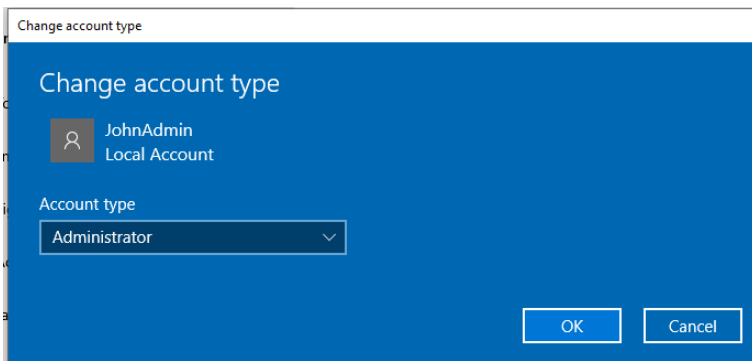
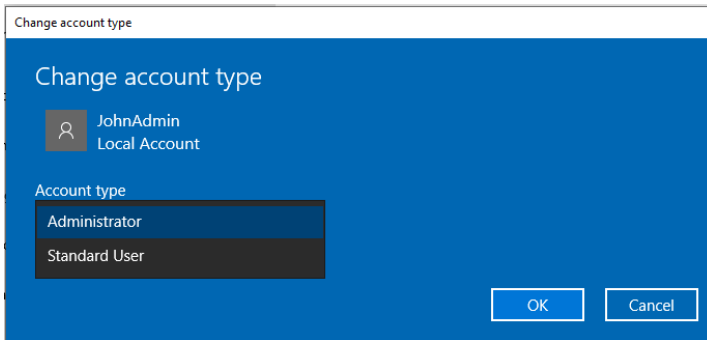
16. The user account will be created as a standard user



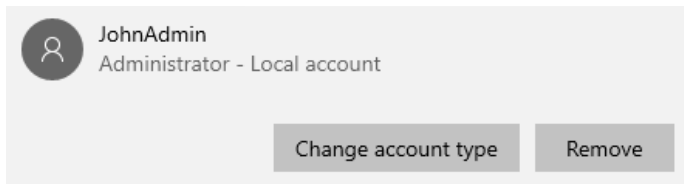
17. Run through the steps again to create an admin account



18. Make JohnAdmin an administrator account by selecting Administrator from the dropdown

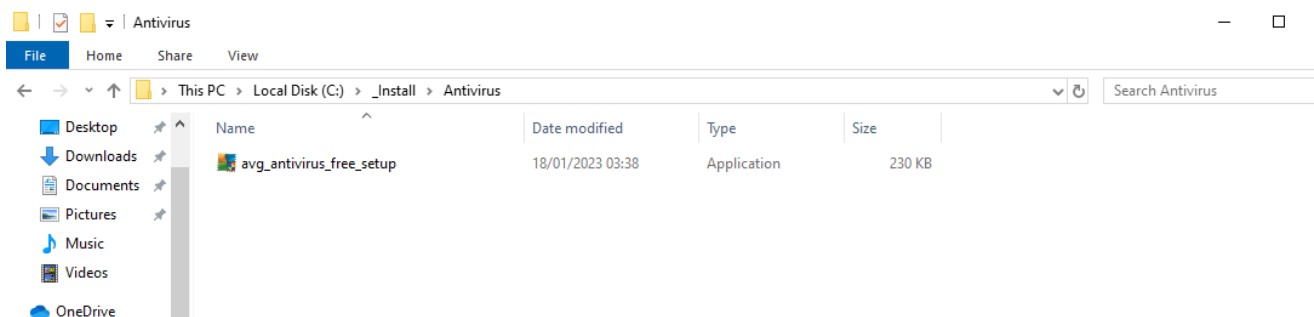


19. You will see that JohnAdmin is an administrator

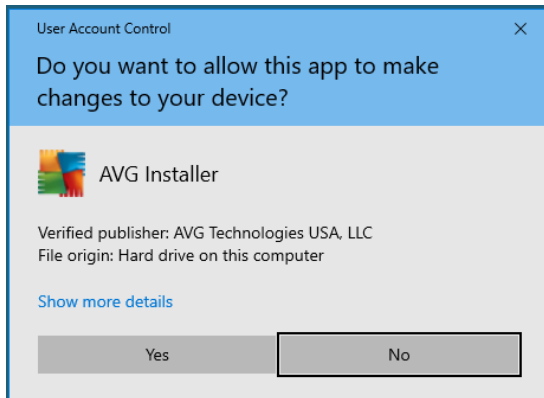


## Anti-virus

1. Access install file in anti-virus folder



2. Double-click and accept User Access Control by clicking Yes



3. Install initiation will commence



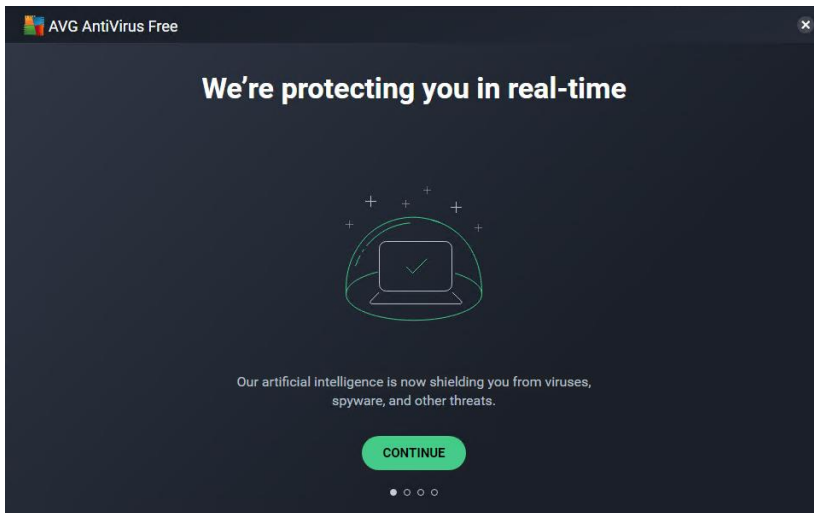
4. Select install



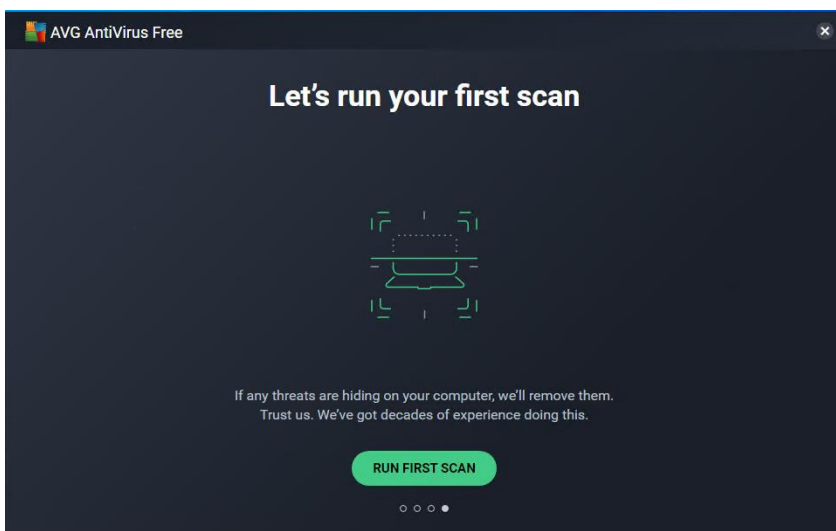
5. Install will commence



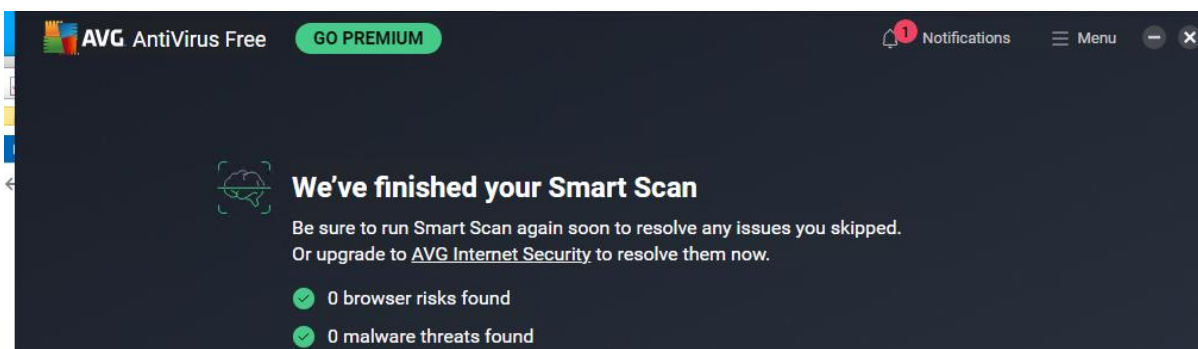
6. When complete click Continue 4 times



7. Run first scan

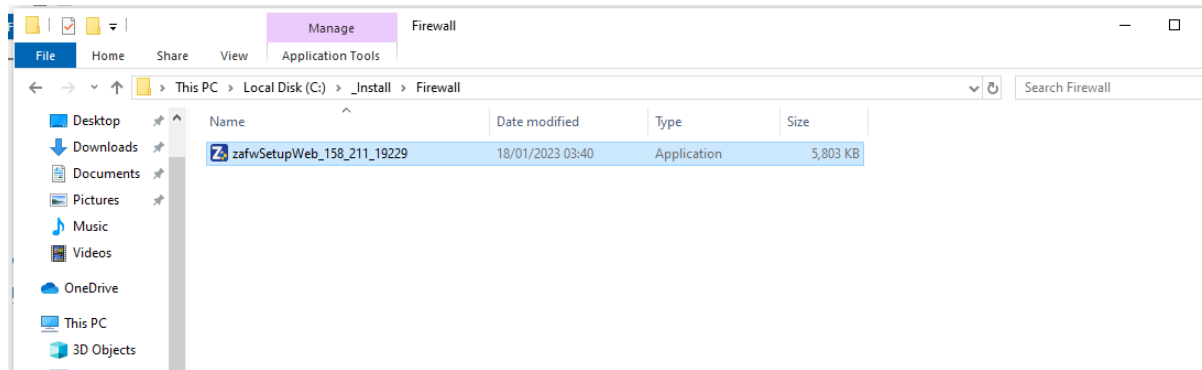


8. Scan will complete and show details

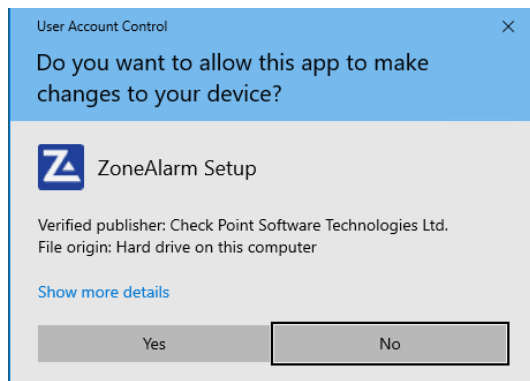


# Firewall

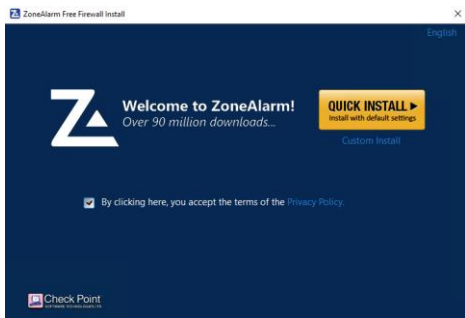
## 1. Double-click install file



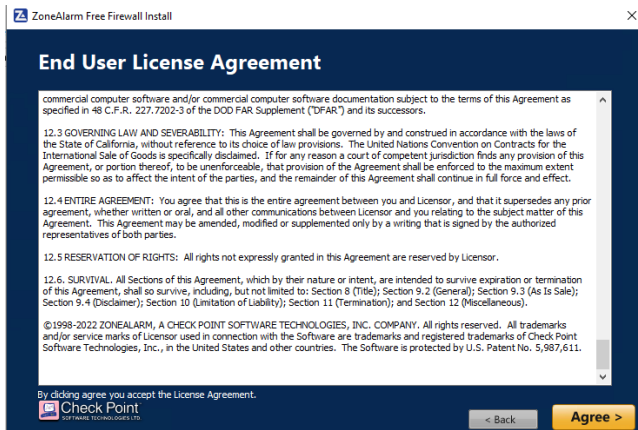
## 2. Select Yes to user account control message



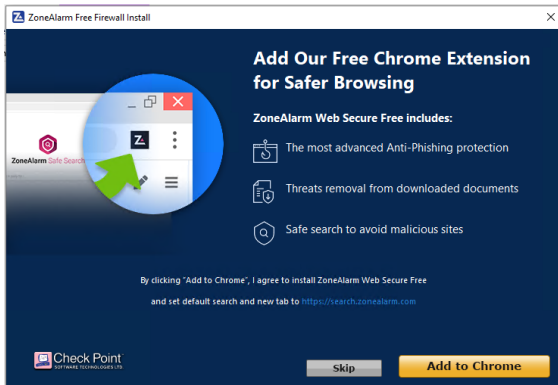
## 3. Select Quick Install



## 4. Click Agree to agreement

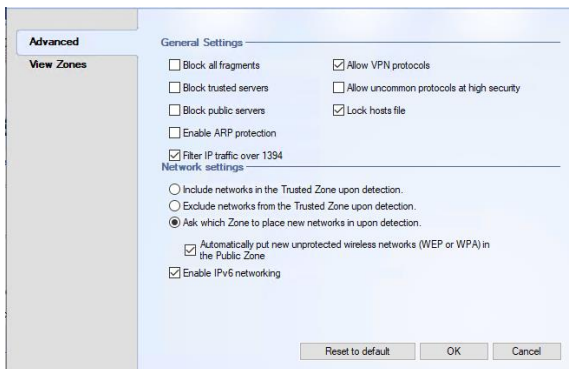


5. Click Skip on Add to chrome popup



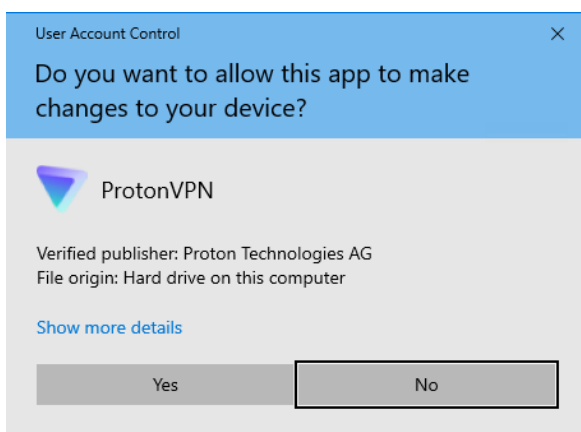
6. Firewall will install

7. When complete you can see it is set to filter IP and lock the local host file

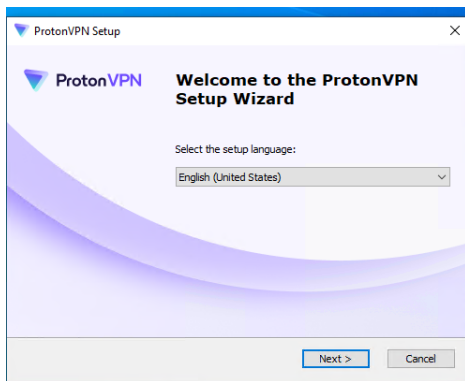


## VPN

1. Double-click install file and accept user account control message by clicking Yes

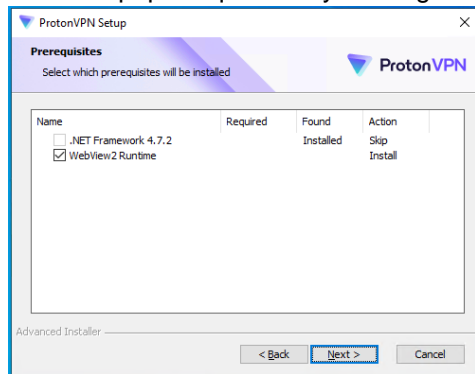


2. English United States is the only English setting so Select and then click Next

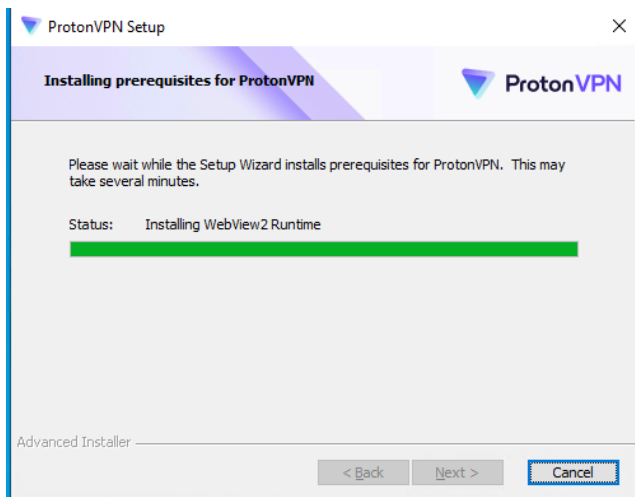


3. Click Next to check prerequisites

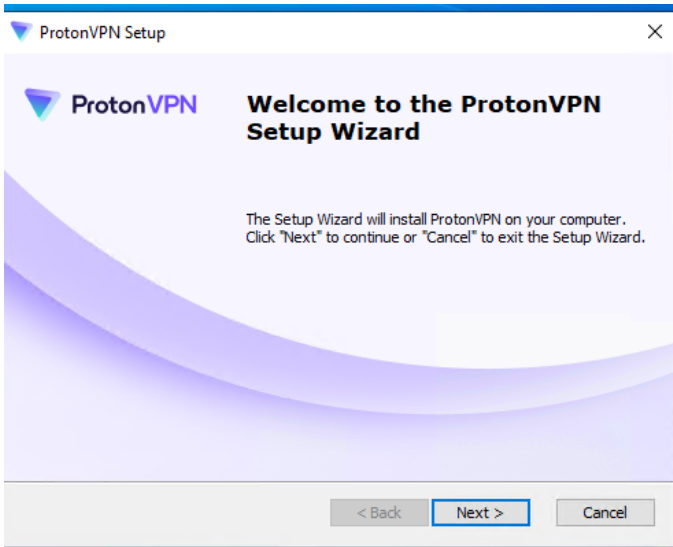
4. Accept prerequisites by clicking Next



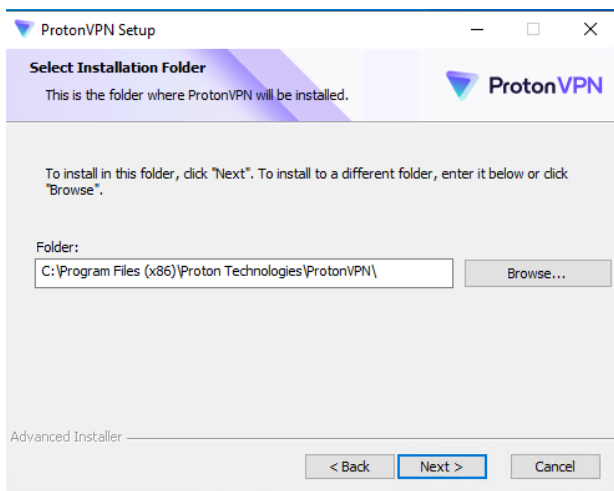
5. Software will install



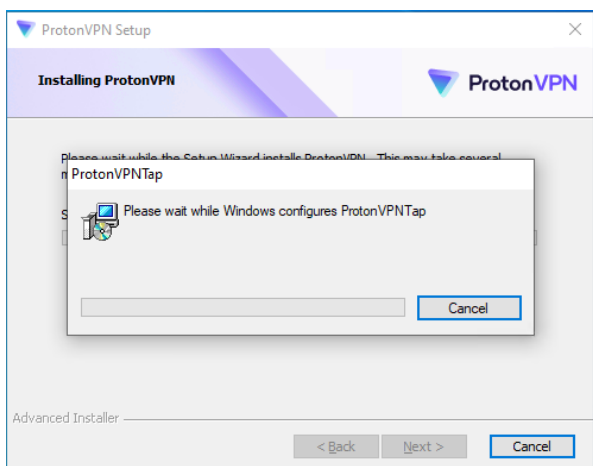
6. Click next



7. Click Next

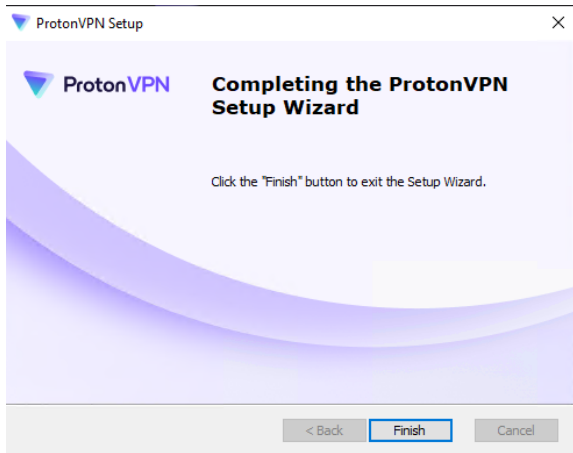


8. Software will install

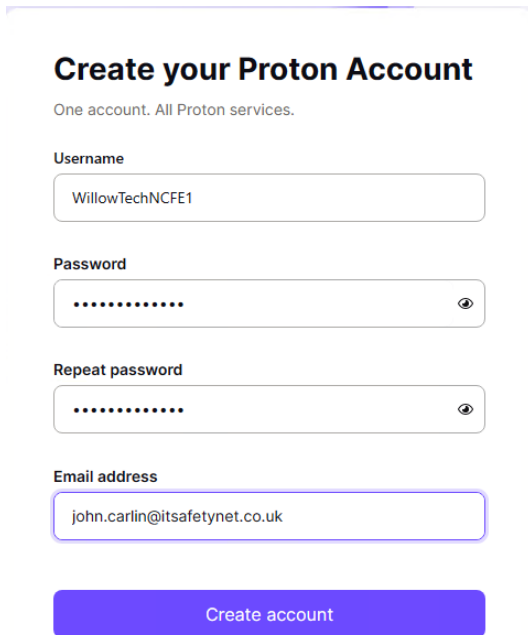




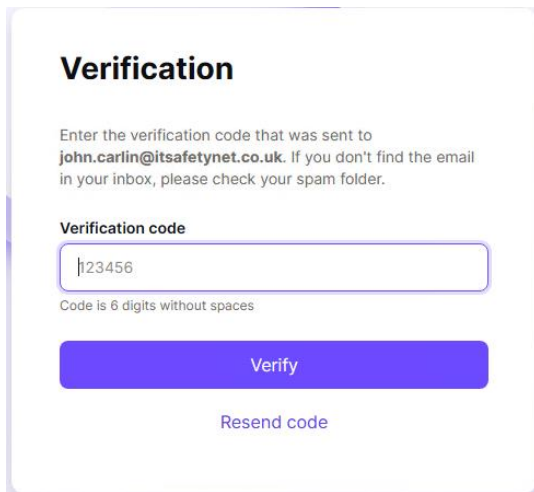
### 9. Click Finish



### 10. Create Proton account

A screenshot of a web form titled "Create your Proton Account". Below the title is the text "One account. All Proton services." The form contains four input fields: "Username" with the value "WillowTechNCFE1", "Password" (masked with dots), "Repeat password" (masked with dots), and "Email address" with the value "john.carlin@itsafetynet.co.uk". At the bottom of the form is a blue button labeled "Create account".

### 11. Enter verification code



**Verification**

Enter the verification code that was sent to **john.carlin@itsafetynet.co.uk**. If you don't find the email in your inbox, please check your spam folder.

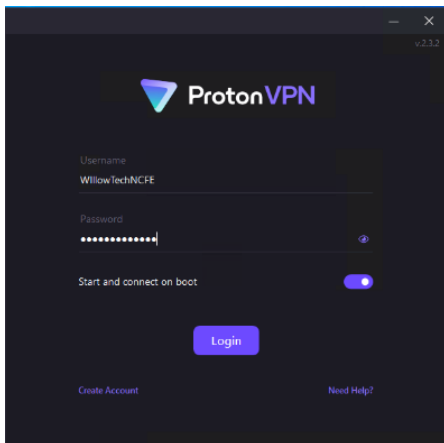
**Verification code**

Code is 6 digits without spaces

**Verify**

[Resend code](#)

### 12. Login with account and password just set up



**ProtonVPN**

Username  
WillowTechNCFE

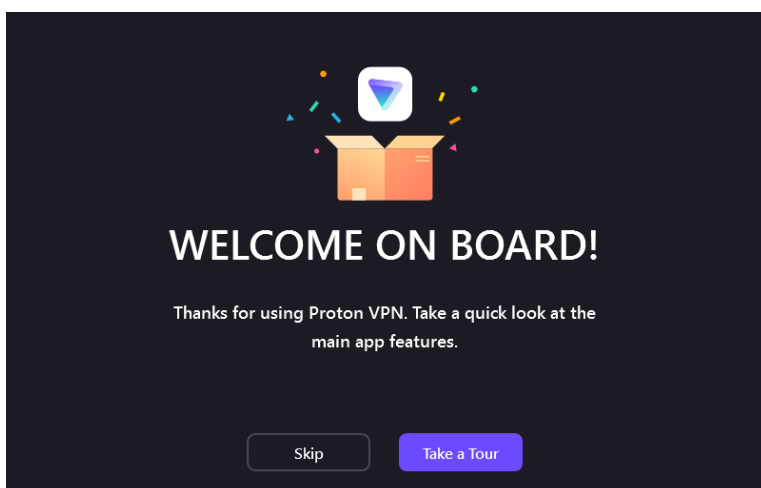
Password  
••••••••

Start and connect on boot

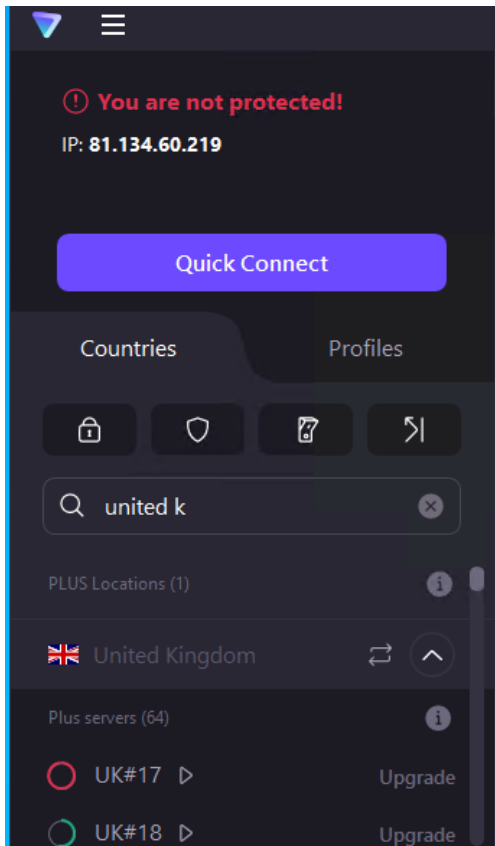
**Login**

[Create Account](#) [Need Help?](#)

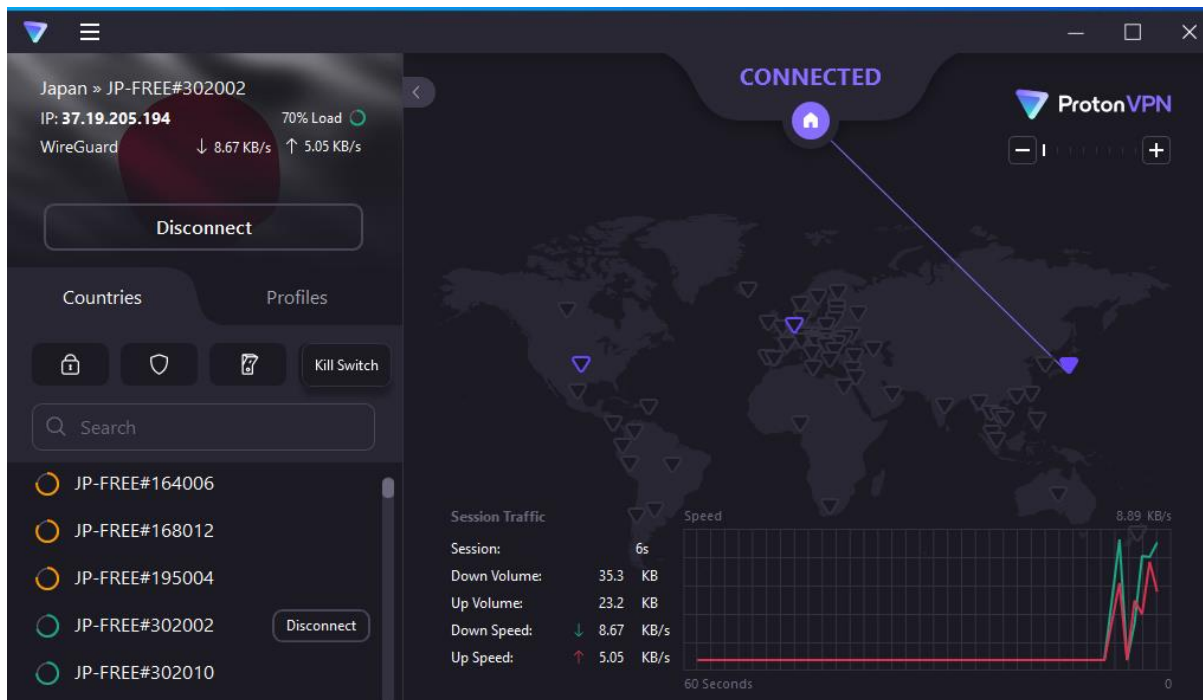
### 13. Skip tour



### 14.Quick Connect



### 15.You are connected



## Testing table

Test	Expected Outcome	Actual Outcome	Remedial Action (if Required)
<b>Install Windows OS</b>	OS successfully installed	OS installed	N/A
<b>Check for updates</b>	Check for updates in Windows update center	Updates installed	N/A
<b>Create account</b>	Create a Microsoft account	Account created for JohnAdmin and set as administrator account type	N/A
<b>Login to Windows</b>	Login to Windows	JohnAdmin successfully logged in	N/A
<b>Install AVG</b>	Software installation success	Installation successful	N/A
<b>Run AVG scan</b>	Scan runs	Scan runs and found no malware	N/A
<b>Install firewall</b>	Firewall installs successfully	Firewall installed with no problems	N/A
<b>Create firewall rule</b>	Firewall rule created successfully (set to filter IP and lock the local host file )	Firewall rule created successfully to set to filter IP and lock the local host file	N/A
<b>Install VPN</b>	VPN software installs successfully	VPN software installed successfully	N/A
<b>Create VPN user account</b>	User account setup successfully	John's account created successfully	N/A
<b>Login to VPN account</b>	Login success	Login success and welcome aboard message displayed!	N/A
<b>Confirm VPN connection</b>	VPN connection confirmed	VPN connection successfully connected to server in Japan with IP 37.19.205.194	N/A

## Examiner commentary

Overall this student response is mainly excellent and well written throughout however, there is still room for further detail and research. The student has confirmed that the source of analysis is reliable and justified this within the narrative.

### Task 1

The analysis of the firewall included a comprehensive set of minimum requirements all products had to meet. Although it does meet the recommendations set out in the assessment this could be further improved by widening the research range of products. The rationale for the final choice was very well thought out, took account of the cost, pros and cons and was approached in a logical manner. The student showed a detailed understanding of the software programs and the impact of their capabilities. The learner gave an excellent explanation of the legal requirements that need to be addressed including references to relevant legal statutes. However, the student could have added more in-depth information and structured this more appropriately so that all the legislation was considered in one place in the document, allowing the reader to see the full implications if everything was implemented. The student demonstrated excellent coverage of the legal requirements required by the implementation of the firewall and anti-virus products including a logical comparison structure such as a comparison grid for the products, for example anti-virus. It should also be noted that the student has gone beyond the brief by exploring a wider range of products. This has however helped justify their decision in making a recommendation. The student's project proposal not only covered how to evaluate and deploy the products but also included technical and non-technical aspects. The student's project proposal was concise, clear, logical and easy to read.

### Task 2

The student carried out a structured set up of the virtual machine (VM) with the required software program and the provided image, they thoroughly tested the VM to ensure it was operating as expected. The student provided extensive evidence of the setup and testing along with screenshots, an easy to follow narrative and a logical, step by step well thought out narrative and comprehensive screenshots. The student demonstrated that they thoroughly understood the functionality of the software packages, configured the fire wall and carried out anti-virus scans and reporting. However, although the firewall and anti-virus software was tested this was limited to one test for each and further testing would have provided additional evidence. For example, the anti-virus is shown completing a full scan but further evidence showing scheduled scans would have demonstrated that the software had been fully configured. The student provided an excellent and well-written log demonstrating that the correct steps were followed for all software programs that have been installed.

## Overall grade descriptors

Grade	Demonstration of attainment
Pass	The student is able to develop a project proposal to research and compare the current software available and justify their recommendations.
	The student is able to install supplied software onto a device and ensure it is all correctly configured.
	The student is able to identify and explain the difference between cyber attacks and software issues, and how a cyber attack could take place.
	The student is able to investigate the issues on the virtual machine provided and explain the most effective remedial action to take to mitigate any problems.
	The student is able to evaluate a network with regards to cyber security.
	The student is able to ensure that company resources and data are fully protected.
	The student is able to perform a security risk assessment of the site and the network.
	The student is able to recommend physical, administrative, and technical controls.
	The student is able to create a disaster recovery plan including recommendations in the case of service outages.
	The student is able to explain how remedial actions will protect the company, which includes considerations for security, manageability and upgradeability in relation to cyber security policies.
Distinction	The student is able to develop an in-depth project proposal to research and compare the current software available and comprehensively justify their recommendations.
	The student is able to install supplied software onto a device, demonstrating excellent capabilities in ensuring it is all correctly configured.
	The student is able to comprehensively identify and explain the difference between cyber attacks and software issues, and evidence a detailed understanding of how a cyber attack could take place.
	The student is able to thoroughly investigate the issues present on the virtual machine provided and fully justify the most effective remedial action to take to mitigate any problems.
	The student is able to carry out an in-depth evaluation of a network with regard to cyber security and identify areas of improvement.
	The student is able to perform an in-depth security risk assessment of the site and the network, identify areas of concern and give a rationale for each.

	The student is able to recommend physical, administrative, and technical controls and justify their recommendations.
	The student is able to create an in-depth disaster recovery plan, including justifications for recommendations in the case of service outages.
	The student is able to demonstrate in-depth knowledge and give a thorough explanation of how remedial actions will protect the company, which includes considerations for security, manageability and upgradeability in relation to cyber security policies.

## Document information

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2023.

'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education.

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

'Institute for Apprenticeships & Technical Education' and logo are registered trade marks of the Institute for Apprenticeships and Technical Education.

Owner: Head of Assessment Design

## Change History Record

Version	Description of change	Approval	Date of issue
v1.0	Published final version	June 2023	31 August 2023