T-LEVELS | Institute for Apprenticeships & Technical Education

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Cyber Security

Assignment 1 - Pass

Guide standard exemplification materials (GSEMs)

v1.0: Specimen assessment materials
31 August 2023
603/6901/2

Internal reference: DSS-GSEM-16

NCFE

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

Cyber Security

Guide standard exemplification materials (GSEMs)

Assignment 1 - Pass

Contents

Contents **2**

Introduction **3**

Assignment 1 .... **4**

Task 1: project proposal 4

Student evidence 6

Task 2: set-up – devices, network and access 18

Student evidence 18

Examiner commentary **38**

Overall grade descriptors 39

Document information **41**

Change History Record 41

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 many different types of firewall available for Willow, the main types are packet filtering (simplest type of firewall, which examines incoming and outgoing packets), stateful inspection (similar to a packet filtering firewall, but it also keeps track of the state of connections between devices), next-generation firewalls (NGFWs) (more feature-rich than traditional firewalls and may include additional services such as intrusion detection and prevention, VPN and anti-virus protection), application-level gateway (ALG) (designed to work with specific types of applications, such as FTP or VoIP, providing more control over the traffic).

Based upon the types listed above, I have categorised them as hardware and software firewalls, this classification is explained below and some features of the different types of firewalls are discussed.
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

Comparitech – https://www.comparitech.com

Business.org - https://www.business.org/

Forcepoint - https://www.forcepoint.com/

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. A main advantage of using a hardware firewall is the ability to have a central point of management for Willow and any changes to the settings are effective across the whole network.

Although having a dedicated piece of hardware to act as a firewall is a good choice for larger companies with multiple subnets containing multiple computers, they can be a bit of an overkill for an SME. They also need a member of staff with the skillset to manage and update them to ensure they contain the latest security updates.

Pros

- protect multiple devices at the same time with a single administration point making it easier to manage
- protects the network perimeter so malicious traffic should never reach other assets inside the network at Willow
- have their own resources that can be upgraded in many instances, this includes software services such as IDS
- higher reliability because hardware firewalls are designed specifically for network security.improved network performance by offloading some of the security processing from your computers and servers

Cons

- more expensive.
- requires staff with the correct skills to manage it
- needs to be in a secure environment

- provides a single point of failure which can lead to security vulnerability exposure on the network and perimeter

Software Firewalls

A software firewall installs directly onto a device and as such only protects that device. It also has to share the device's resources. This increases the administration of the device as updates need to be applied to all devices and could be time consuming for staff at Willow.

Pros

- very good protection for a single device
- gives admins complete control of firewall at a granular device level
- software readily available and relatively inexpensive
- software firewalls can be installed on a single device, which means Willow can control their security settings for each device
- easier to set up and configure than hardware firewalls.
- some offer additional security controls such as malware protection

Cons

- consumes resources of the device it is installed on
- requires configuration to be done on the device it is installed on
- only protects the device it is installed on
- increased manual maintenance which could result in more errors
- may not be compatible with certain types of software or hardware

Information Source

It is important to ensure that the information sources used to compare firewalls are acknowledged as reliable sources that are free from bias. Where possible I tried to use multiple sources, content that was not sponsored by the manufacturer or developer of the technology and supplied information related to the products strengths and as well as weaknesses.

Source Reference

I have used Comparitech (https://www.comparitech.com/) for the technical details of the Firewall Comparison. 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/) 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

Price £550.00 Incl. VAT

User Reviews

The Firepower 1100 user reviews rate the product fairly positively.

Pros

- simple graphical user interface (GUI) based functionality; this would help the skill level of staff at Willow because there would be no need to learn command line syntax like on some other technologies
- realtime throughput of traffic, this would be ideal for Willow because they have remote workers, so this would help get an overall view of traffic across the business
- ease of implementation as all GUI based this would help the skill level of staff at Willow because there would be no need to learn command line syntax like on some other technologies

Cons

- real time logging to console is limited
- all GUI so cannot be scripted

Legal/Security Requirements

As these are physical devices there will be a need to provision in a secure area and employees responsible for installation must adhere to the health and safety work act. Licenses need to be bought to avoid legal issues relating to software piracy. 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 but requires a subject matter expert (SME) 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.

Perimeter 81

Price

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

User Reviews

The user reviews are good typically scoring 85%.

In addition, the general consensus is:

Pros

- ease of use and has all the features required for Willow
- flexible remote access environment e for configuring the system
- provides services including packet checking and signature recognition

Cons

- occasional issues with connectivity and performance
- software can be resource hungry

Tech Spec

- supports multiple OS including Windows and Mac
- supports whitelisting and blacklisting
- secure web gateway (SWG) blocking high risk websites

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

Firewall Solution Choice and Rationale

Perimeter 81 is the recommended choice here.

Product research

Anti-virus

There are multiple discussions available on the internet that give a rundown of the types of ant-ivirus as well as their pros and cons, the ones I used were:

National Cyber Security Centre – https://www.ncsc.gov.uk

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

Comparitech – https://www.comparitech.com

Business.org - https://www.business.org/

When considering an anti-virus, it is important to look at the overall requirements before searching for a product. It's worth pointing out that many modern anti-virus programs use a combination of the following techniques to provide protection against malware and cyber threats:

- signature-based anti-virus are the most traditional type of ant-virus software, which rely on a database of known malware signatures - this gets updated regularly.

Heuristic-based anti-virus use behaviour-based analysis to detect and block malware. Cloud-based anti-virus rely on a network of remote servers to analyse files and detect malware. Behavioural anti-virus software use machine learning algorithms to detect potential malware. 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 and they state on their website *“Capterra is committed to providing our visitors an unbiased reviews catalog with content from other community members. Though every reviewer is entitled to--and encouraged to share--their own opinion, Capterra is vigilant against attempts to deceive others through their review's content.”*
- they are acknowledged as the world’s leading software review and selection platform
- they have a trustpilot.com rating of 4.2

Capabilities Required

When looking at anti-virus software it is important to look at the capabilities of each product and ensure they offer adequate cover for the devices.

Recommendation

In order to accurately assess which anti-virus is best I will evaluate the top 2 anti-virus products (based upon requirements) from the Capterra website, these are:

- Antivirus Pro
- Trend Micro

These products meet the minimum specs stated above but we also need to consider the support available.

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:

- malware detection
- automation
- data security
- endpoint protection
- identity theft protection
- phishing protection
- real-time monitoring
- real-time alerts
- VPN support

Anti-virus product comparison

Product	Pros	Cons
Antivirus Pro Cost: No cost provided by vendor	• meets minimum spec • cloud • email/helpdesk	• no on-premises • no webinars • no documentation • no FAQ/forum • no knowledge base • no pricing provided by vendor
Trend Micro Cost: $14.89 pa	• on-premises	• does not meet minimum spec • no cloud • no webinars

		• no documentation • no videos

Legal/Security Requirements

There is a requirement to purchase licenses for the devices that will need to be reviewed. In addition, as these check files on user computers, user behaviour is particularly important. The Data Protection Act 2018 will need to be adhered to when using the digital infrastructure at Willow. The way information is accessed, stored, and modified needs to be considered, these points should be addressed in existing company policies such as acceptable use and information systems security.

Anti-virus Solution Choice and Rationale

Based upon the above comparison:

- we must rule out Trend Micro as it does not offer automatic scans, identity protection and VPN support so does not meet the minimum spec
- we must rule out Trend Micro as it does not offer cloud support, this leaves Antivirus Pro as the only product that meets minimum spec and is a cloud-based solution, this will suit the size of the IT team at Willow and will provide protection against malware for the daily business processes that they undertake, for example, remote working.

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

Product research

Virtual Private Network (VPN)

I will now discuss the different types of VPN that Willow could use, each type of VPN has its strengths and weaknesses, and the choice of which type to use will depend on the specific needs of the organisation.

- remote access VPN is used by individuals or employees to connect to a business network securely from remote locations - it allows users to access company resources, such as files and applications, as if they were in the office
- Site-to-Site VPN connects two or more networks together over the internet. It is commonly used by businesses to connect their branch offices or data centres securely
- mobile VPN provides a secure connection for mobile devices, such as smartphones and tablets, to a business network - it is particularly useful for employees who work remotely or travel frequently

I would recommend that Willow use a remote access VPN for the remote workers to access the company network.

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.

There are multiple discussions available on the internet that give a rundown of the types of VPNs 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

Business.org - https://www.business.org/https://www.business.org/

Capabilities Required

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

- the provider offers services that cater specifically to businesses
- speed and stability
- strong security
- number of simultaneous connections

Recommendation

Looking at the VPN products available, I have discounted all but the following 2 products that will be evaluated:

- Perimeter 81
- NordLayer

Perimeter 81

Perimeter 81 is a business VPN that allows businesses to setup private VPN servers. Staff can securely connect to these from anywhere. The VPN allows you to manage network activity via an online dashboard. This allows staff to securely access files, apps, and other resources. Some of the main features that would benefit Willow include:

- network segmentation to isolate sensitive data
- connect offices in different locations
- allows remote access via cloud
- if you do not deploy your own VPN, you can choose from 700 public servers in 36 locations around the world
- 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

Pros

- deploy your own server or choose from public ones
- supports site-to-site VPNs
- ability to host apps and files on the VPN server
- encryption
- network segmentation

Cons

- more expensive than other solutions

NordLayer

NordLayer is a service for small to medium sized businesses that can be easily set up providing secure remote access to both the office network and to the internet.

Pricing: £7 per use per month.

The key features of the product are:

- dedicated IP option
- remote access and site-to-site
- device security scanning
- Site-to-Site
- remote access
- device security check

Pros

- fast and reliable connections
- military-grade 256-bit encryption for great privacy
- strict no-logs policy ideal for privacy-conscious users
- unlimited bandwidth and no data caps

Cons

- desktop based app can be confusing
- no sign out code

Legal/Security Requirements

The use of a VPN is legal in most countries, including the UK. There is a requirement to purchase licenses for the devices that will be using the software. The Data Protection Act 2018 will need to be adhered to when using a VPN and the way information is accessed, stored and modified needs to be considered, these points should be addressed in existing company policies, but the creation of a remote working policy may be required.

VPN Solution Choice and Rationale

Although Perimeter 81 is £1 per user per month more than NordLayer it has a much wider feature set. It would also cut down the management and maintenance as they share a common admin platform.

For the following reasons the recommended VPN solution is Perimeter 81.

User Access Control

The VPN will provide a layer of access control for network users when working remotely, but 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.

Server Level

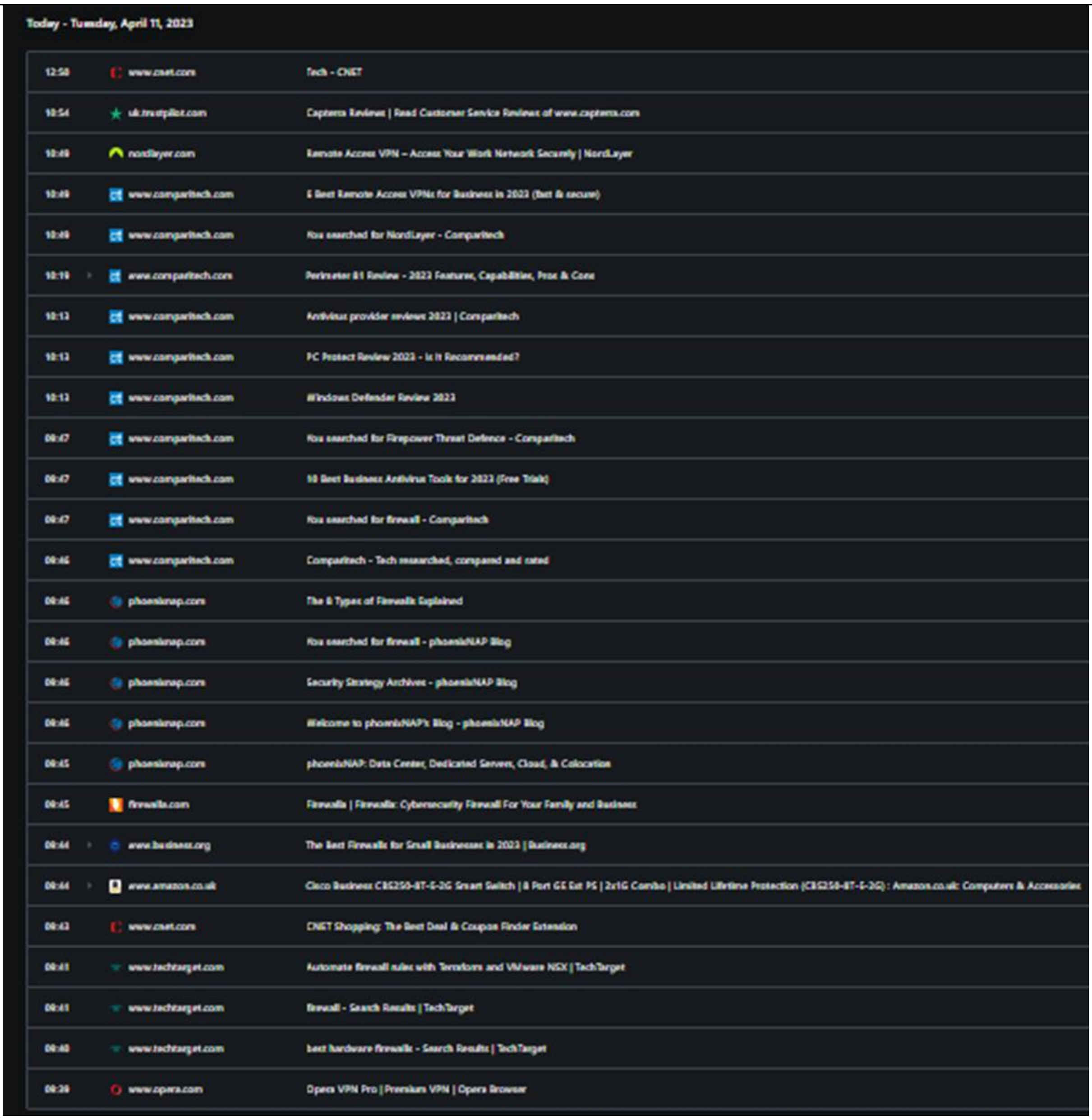
Setting up a server as a domain controller will allow the rollout of user groups/organisational units, permissions and authentication methods. This will then allow all end devices to join the domain and be controlled centrally, this will also allow security policies and windows updates to be rolled out to all devices.

Overall Conclusion

The choices made best suit the needs of Willow due to their size and the nature of the business, the benefit of a single administration point for the firewall technology, the antivirus is a cloud based solution and is ideal for the small IT team at Willow to maintain and is also well suited for protecting the remote working team at the company, the VPN will cut down the management and maintenance as they share a common administration platform. All 3 solutions will support future growth for Willow and be ideal for the size of their IT team and are a perfect match to work together and are excellent choices for a SME.

Research Evidence

Browser History

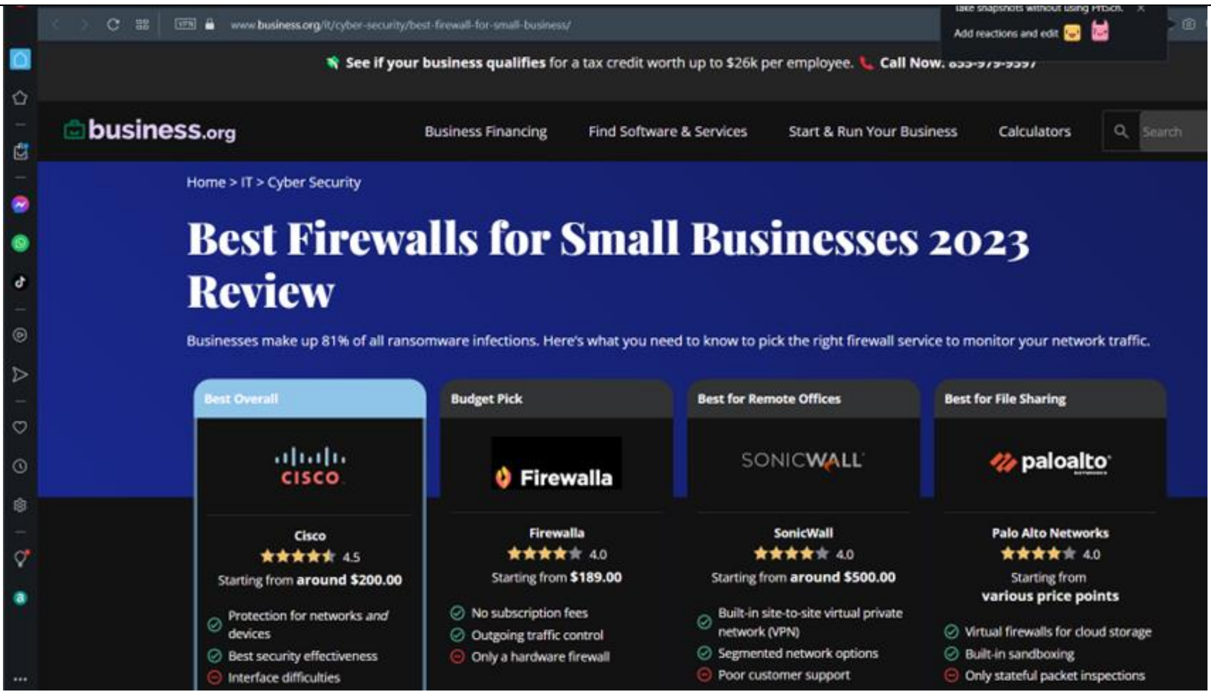


Today - Tuesday, April 11, 2023

12:50	www.cnet.com	Tech - CNET
10:54	uk.trustpilot.com	Capterra Reviews | Read Customer Service Reviews of www.capterra.com
10:49	nordlayer.com	Remote Access VPN – Access Your Work Network Securely | NordLayer
10:49	www.comparitech.com	6 Best Remote Access VPNs for Business in 2023 (fast & secure)
10:49	www.comparitech.com	You searched for NordLayer - Comparitech
10:19	www.comparitech.com	Perimeter 81 Review - 2023 Features, Capabilities, Pros & Cons
10:13	www.comparitech.com	Antivirus provider reviews 2023 | Comparitech
10:13	www.comparitech.com	PC Protect Review 2023 - Is It Recommended?
10:13	www.comparitech.com	Windows Defender Review 2023
09:47	www.comparitech.com	You searched for Firepower Threat Defence - Comparitech
09:47	www.comparitech.com	10 Best Business Antivirus Tools for 2023 (Free Trials)
09:47	www.comparitech.com	You searched for firewall - Comparitech
09:46	www.comparitech.com	Comparitech - Tech researched, compared and rated
09:46	phoenixnap.com	The 8 Types of Firewalls Explained
09:46	phoenixnap.com	You searched for firewall - phoenixNAP Blog
09:46	phoenixnap.com	Security Strategy Archives - phoenixNAP Blog
09:46	phoenixnap.com	Welcome to phoenixNAP's Blog - phoenixNAP Blog
09:45	phoenixnap.com	phoenixNAP: Data Center, Dedicated Servers, Cloud, & Colocation
09:45	firewalla.com	Firewalla | Firewalla: Cybersecurity Firewall For Your Family and Business
09:44	www.business.org	The Best Firewalls for Small Businesses in 2023 | Business.org
09:44	www.amazon.co.uk	Cisco Business CBS250-8T-E-2G Smart Switch | 8 Port GE Ext PS | 2x1G Combo | Limited Lifetime Protection (CBS250-8T-E-2G) : Amazon.co.uk: Computers & Accessories
09:43	www.cnet.com	CNET Shopping: The Best Deal & Coupon Finder Extension
09:41	www.techtarget.com	Automate firewall rules with Terraform and VMware NSX | TechTarget
09:41	www.techtarget.com	firewall - Search Results | TechTarget
09:40	www.techtarget.com	best hardware firewalls - Search Results | TechTarget
09:39	www.opera.com	Opera VPN Pro | Premium VPN | Opera Browser

Screenshots

Business.org


www.business.org/it/cyber-security/best-firewall-for-small-business/
Add reactions and edit
business.org
Business Financing
Find Software & Services
Start & Run Your Business
Calculators
Search

See if your business qualifies for a tax credit worth up to $26k per employee. Call Now.

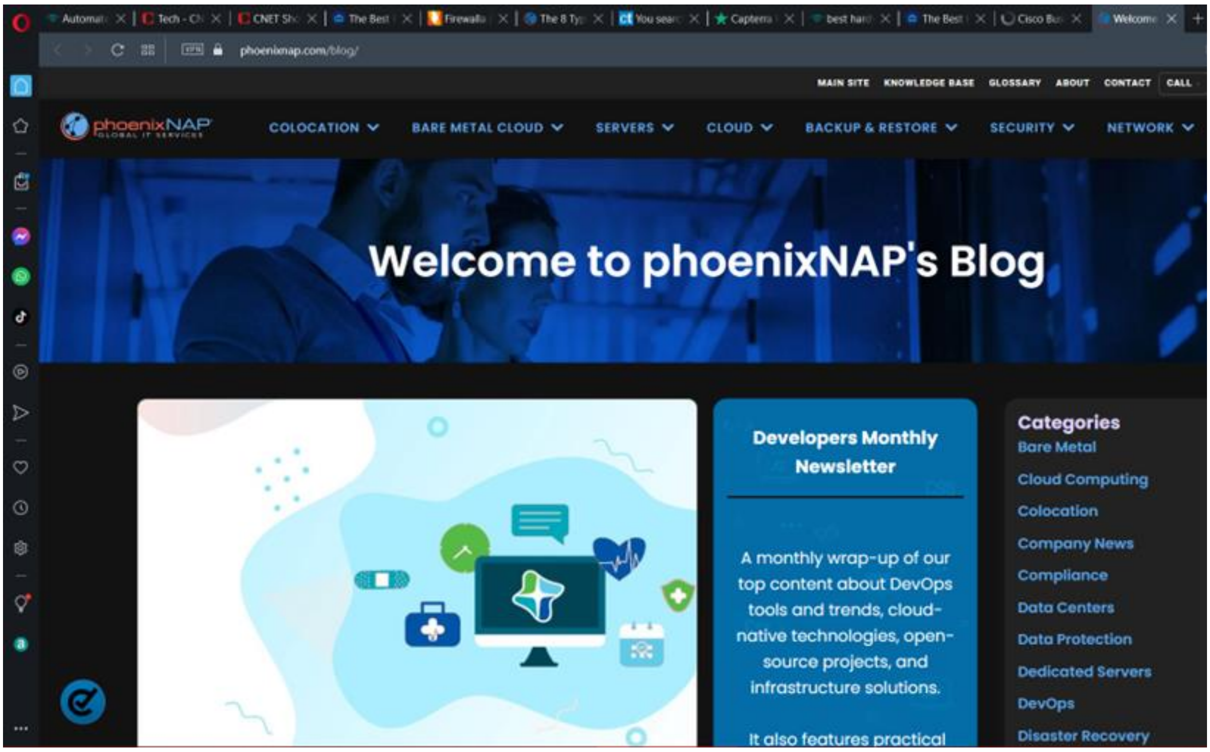
Home > IT > Cyber Security

Best Firewalls for Small Businesses 2023 Review

Businesses make up 81% of all ransomware infections. Here's what you need to know to pick the right firewall service to monitor your network traffic.

Best Overall	Budget Pick	Best for Remote Offices	Best for File Sharing
Cisco	Firewalla	SonicWall	Palo Alto Networks
★★★★★ 4.5	★★★★★ 4.0	★★★★★ 4.0	★★★★★ 4.0
Starting from **around $200.00**	Starting from **$189.00**	Starting from **around $500.00**	Starting from **various price points**
✓ Protection for networks *and* devices ✓ Best security effectiveness ⊖ Interface difficulties	✓ No subscription fees ✓ Outgoing traffic control ⊖ Only a hardware firewall	✓ Built-in site-to-site virtual private network (VPN) ✓ Segmented network options ⊖ Poor customer support	✓ Virtual firewalls for cloud storage ✓ Built-in sandboxing ⊖ Only stateful packet inspections

Phoenixnap.com



Welcome to phoenixNAP's Blog

Developers Monthly Newsletter

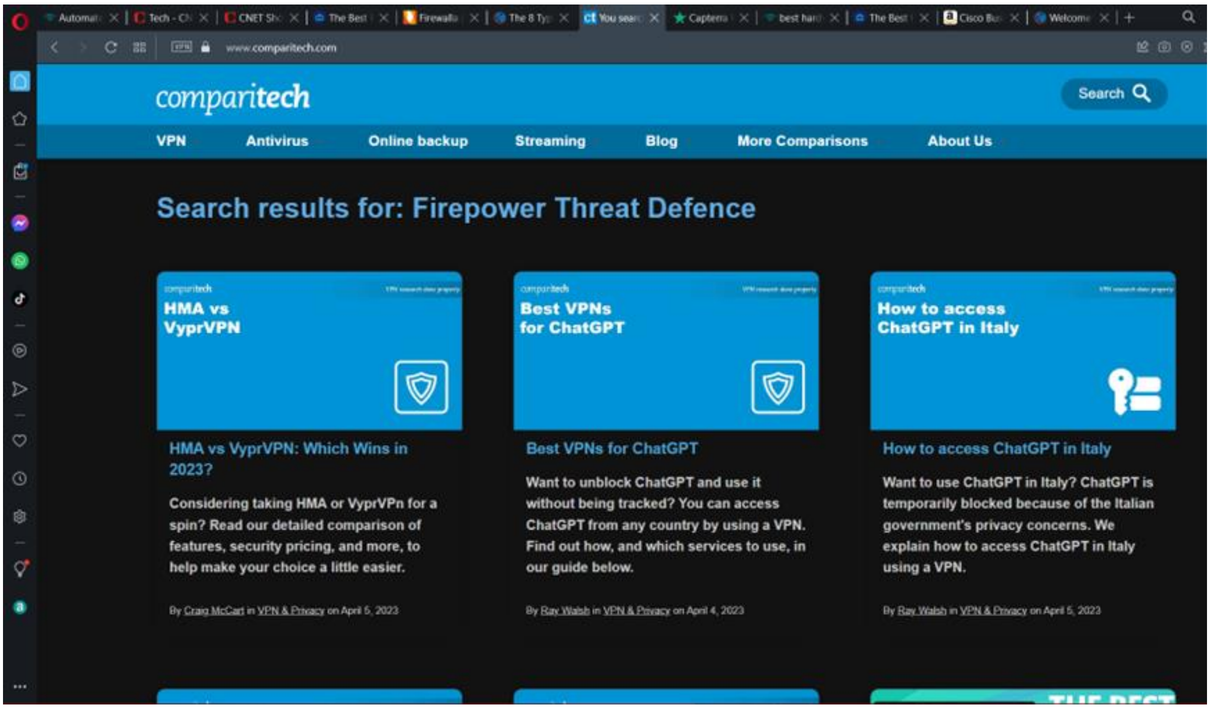
A monthly wrap-up of our top content about DevOps tools and trends, cloud-native technologies, open-source projects, and infrastructure solutions.

It also features practical

Categories

- Bare Metal
- Cloud Computing
- Colocation
- Company News
- Compliance
- Data Centers
- Data Protection
- Dedicated Servers
- DevOps
- Disaster Recovery

Comparitech.com



Search results for: Firepower Threat Defence

HMA vs VyprVPN: Which Wins in 2023?

Considering taking HMA or VyprVPn for a spin? Read our detailed comparison of features, security pricing, and more, to help make your choice a little easier.

By Craig McCart in VPN & Privacy on April 5, 2023

Best VPNs for ChatGPT

Want to unblock ChatGPT and use it without being tracked? You can access ChatGPT from any country by using a VPN. Find out how, and which services to use, in our guide below.

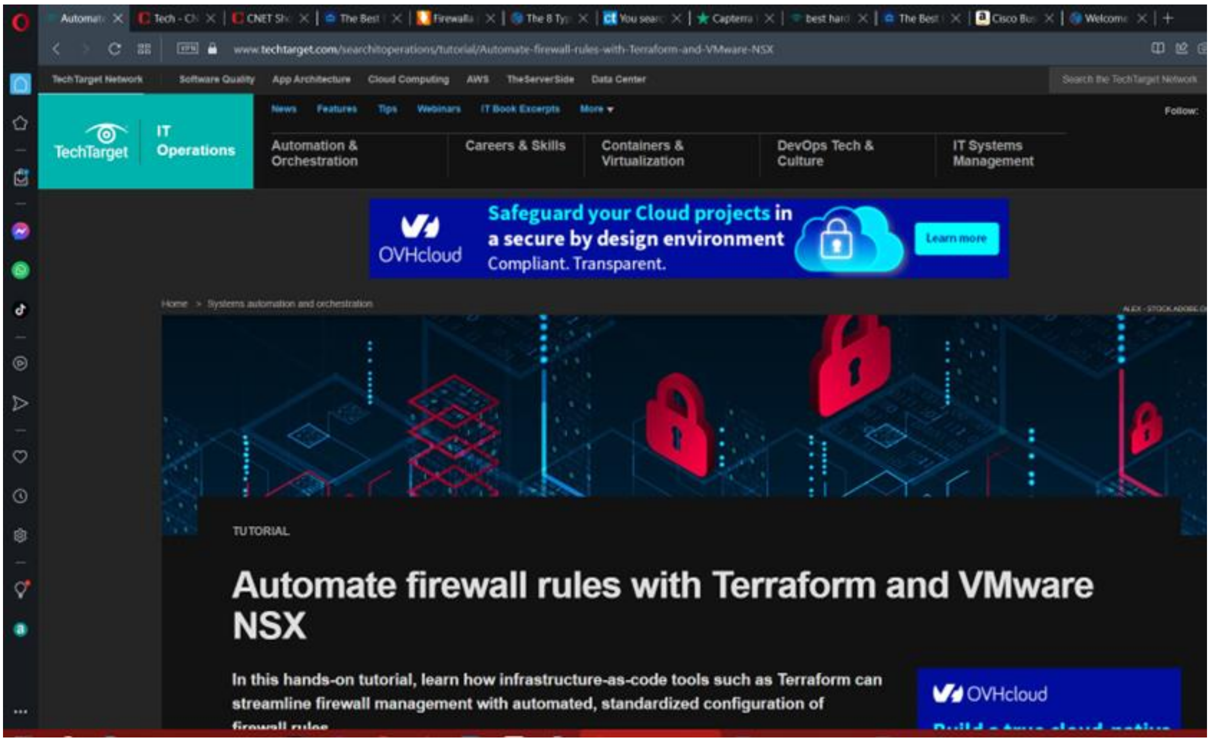
By Ray Walsh in VPN & Privacy on April 4, 2023

How to access ChatGPT in Italy

Want to use ChatGPT in Italy? ChatGPT is temporarily blocked because of the Italian government's privacy concerns. We explain how to access ChatGPT in Italy using a VPN.

By Ray Walsh in VPN & Privacy on April 5, 2023

Techtarget.com



TUTORIAL

Automate firewall rules with Terraform and VMware NSX

In this hands-on tutorial, learn how infrastructure-as-code tools such as Terraform can streamline firewall management with automated, standardized configuration of firewall rules

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

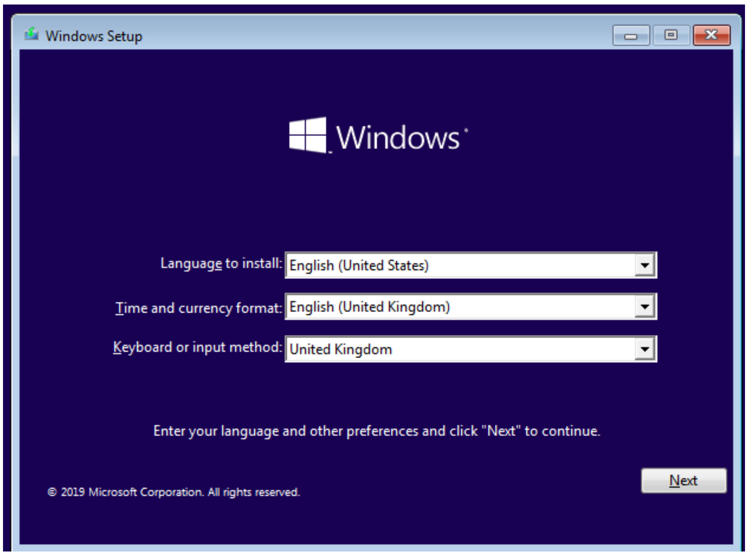
You will submit evidence including but not limited to:

- 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)



Language to install: English (United States)

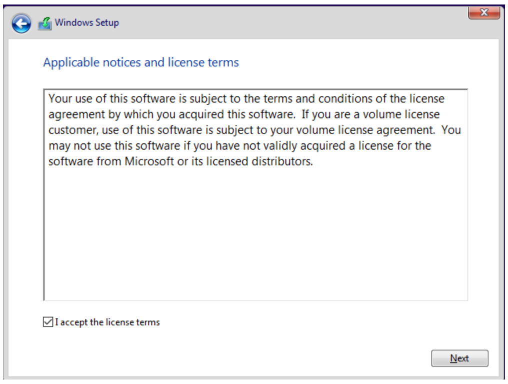
Time and currency format: English (United Kingdom)

Keyboard or input method: United Kingdom

Enter your language and other preferences and click "Next" to continue.

© 2019 Microsoft Corporation. All rights reserved.

5. Click Install Now
6. You will see a message that Setup is starting
7. Select Windows 10
8. Select I Accept License,

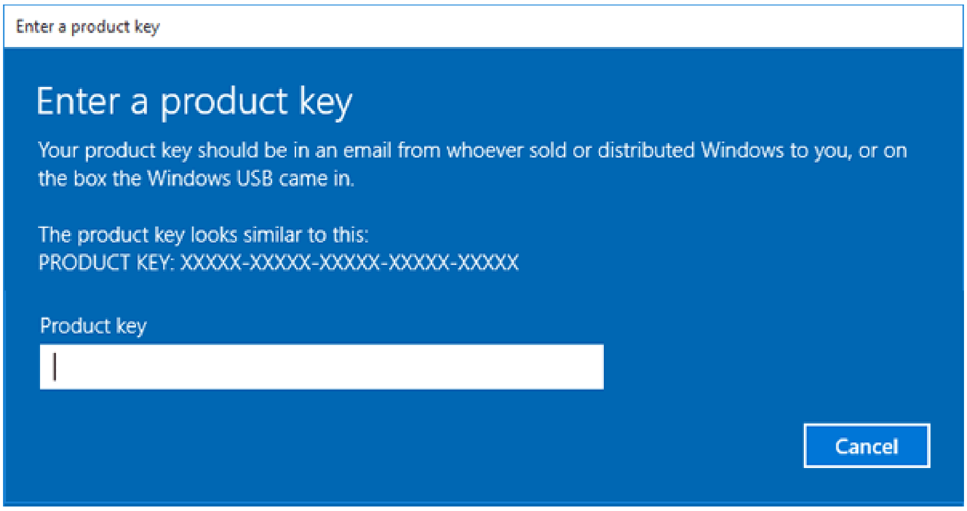


Applicable notices and license terms

Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. If you are a volume license customer, use of this software is subject to your volume license agreement. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.

☑ I accept the license terms

9. A window will pop up asking you to enter a product key during the installation. Please enter the product key at this stage. If you do not have the product key available, click I don’t have a product key and the installation will continue. If you’re prompted again, just do the same until installation is complete. You will need to enter a product key soon after installation to ensure that the installation is a legitimate copy of windows.



Enter a product key

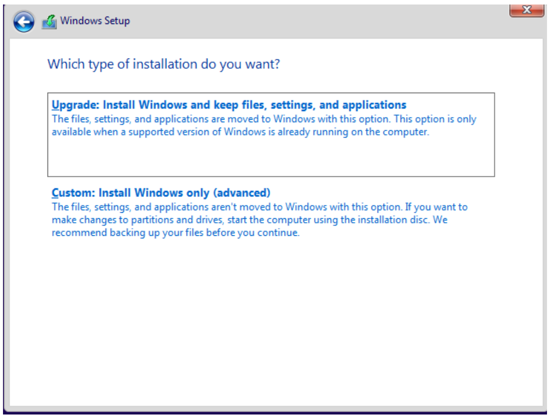
Enter a product key

Your product key should be in an email from whoever sold or distributed Windows to you, or on the box the Windows USB came in.

The product key looks similar to this:
PRODUCT KEY: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Product key

10.Select Custom Install



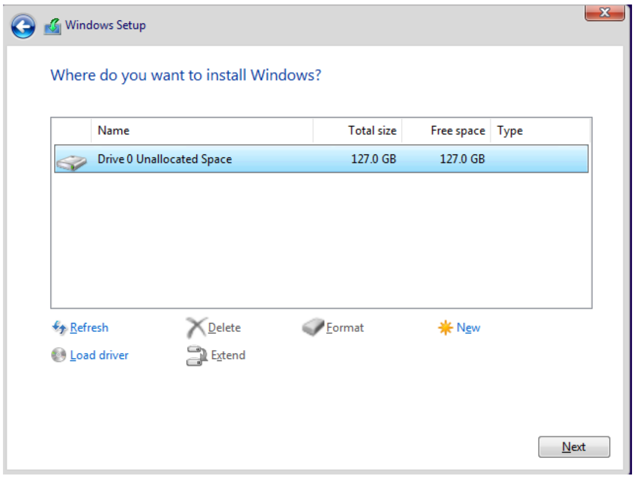
Windows Setup

Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

11. Select Unallocated Space



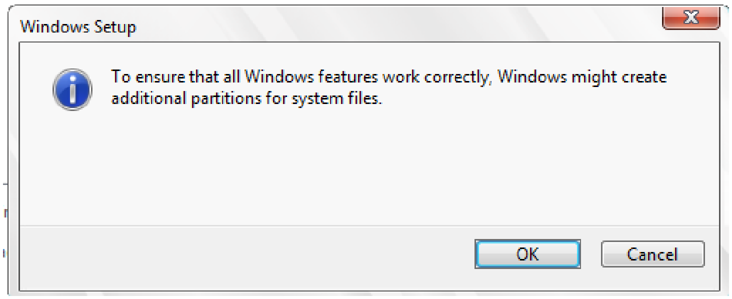
Windows Setup

Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Unallocated Space	127.0 GB	127.0 GB	

12. Click New and then Apply

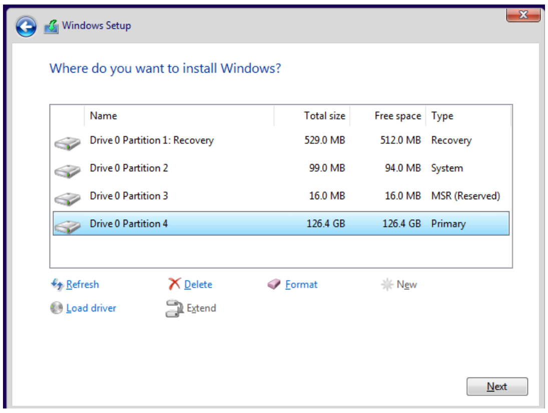
13. Select OK



Windows Setup

To ensure that all Windows features work correctly, Windows might create additional partitions for system files.

14. Click Next



Windows Setup

Where do you want to install Windows?

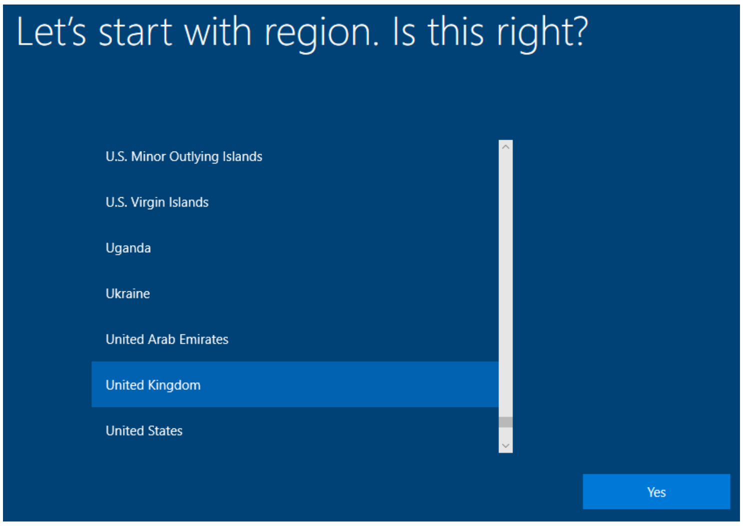
Name	Total size	Free space	Type
Drive 0 Partition 1: Recovery	529.0 MB	512.0 MB	Recovery
Drive 0 Partition 2	99.0 MB	94.0 MB	System
Drive 0 Partition 3	16.0 MB	16.0 MB	MSR (Reserved)
Drive 0 Partition 4	126.4 GB	126.4 GB	Primary

15. Windows will run through the install steps

16. When finished, a Getting Ready message will appear

17. Then a Just a moment message will appear

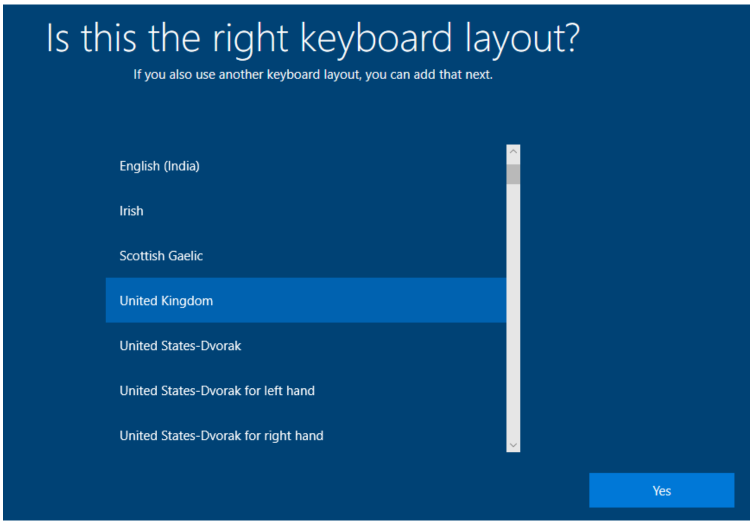
18. Next select United Kingdom as the region



Let’s start with region. Is this right?

U.S. Minor Outlying Islands
U.S. Virgin Islands
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States

19. Select United Kingdom as the keyboard



Is this the right keyboard layout?

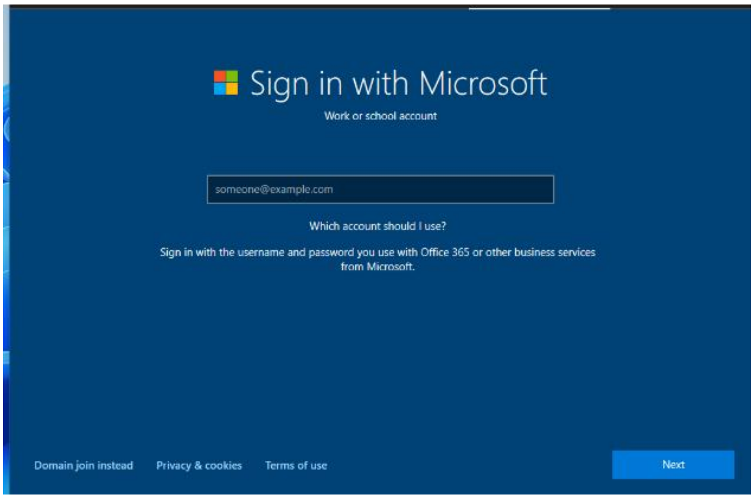
If you also use another keyboard layout, you can add that next.

- English (India)
- Irish
- Scottish Gaelic
- United Kingdom
- United States-Dvorak
- United States-Dvorak for left hand
- United States-Dvorak for right hand

20. Click Skip when prompted for an additional keyboard

21. Windows will do the setup

22. Click Domain Join



Sign in with Microsoft

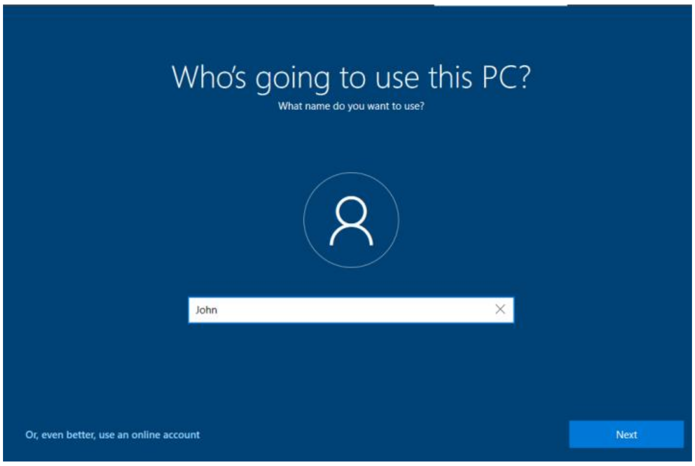
Work or school account

someone@example.com

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.

23. Add the local username

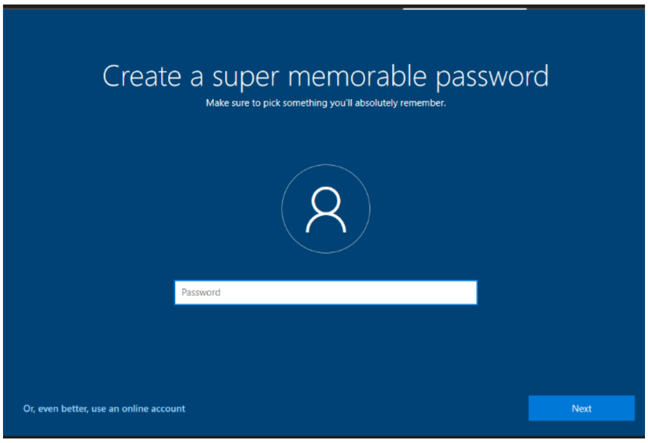


Who's going to use this PC?

What name do you want to use?

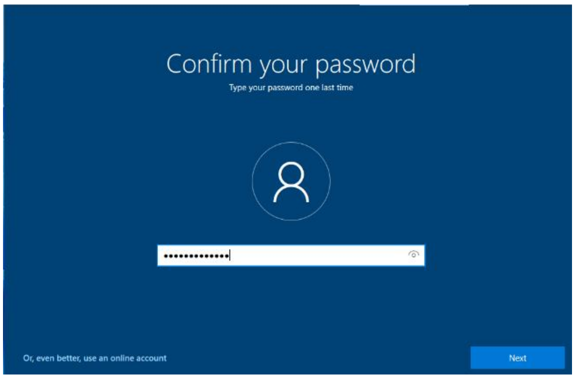
John

24. Create a password



Create a super memorable password

Make sure to pick something you'll absolutely remember.

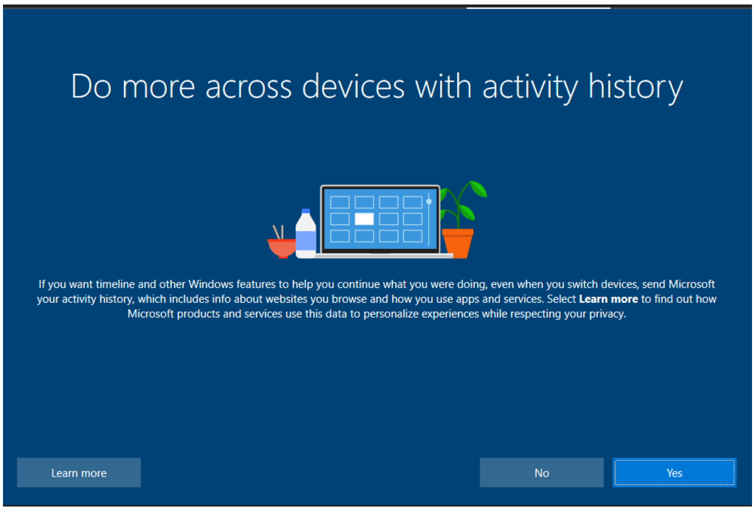


Confirm your password

Type your password one last time

25. Confirm password

26. Select no to the next screen

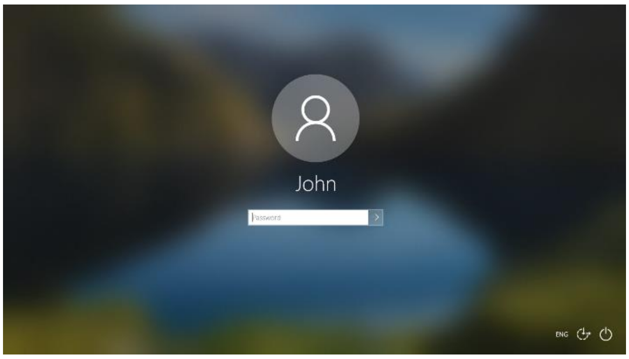


Do more across devices with activity history

If you want timeline and other Windows features to help you continue what you were doing, even when you switch devices, send Microsoft your activity history, which includes info about websites you browse and how you use apps and services. Select **Learn more** to find out how Microsoft products and services use this data to personalize experiences while respecting your privacy.

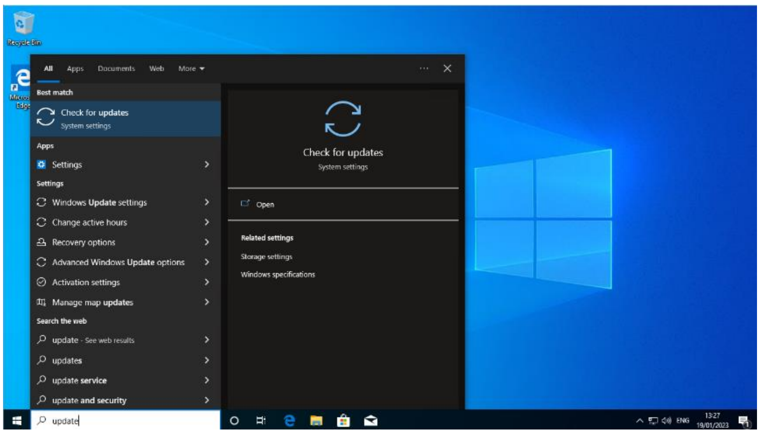
27. Select Decline for the next screen
28. Do not use speak recognition
29. Select no for Location
30. Select No for Find My Device as it is a desktop
31. Select Basic data
32. Select No to improve inking
33. Select no to Tailored experiences
34. Select No to Advertising ID

35. The computer will then get ready
36. A message will appear stating it may take several minutes
37. You will eventually be prompted to log in



38. You will now see a desktop

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



Best match
Check for updates
System settings

Apps
Settings

Settings
Windows Update settings
Change active hours
Recovery options
Advanced Windows Update options
Activation settings
Manage map updates

Search the web
update - See web results
updates
update service
update and security

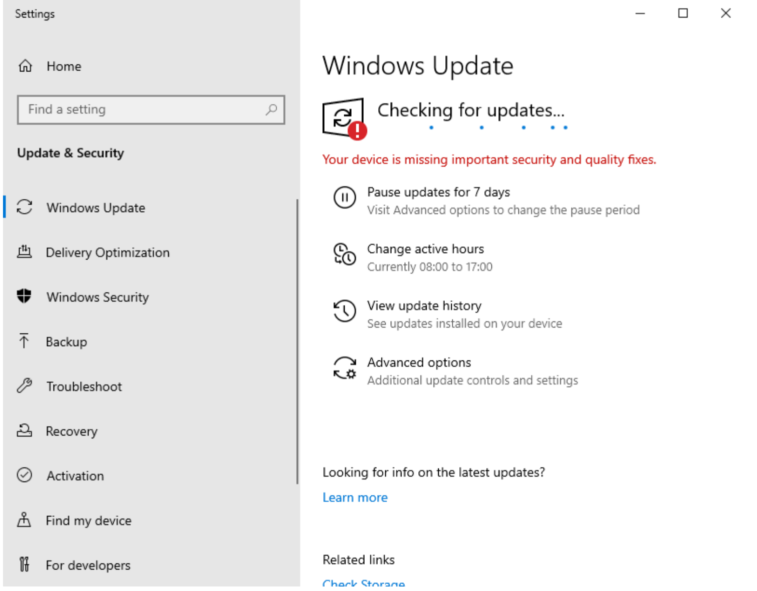
update

Check for updates
System settings

Open

Related settings
Storage settings
Windows specifications

40. Click Check, and the PC will then check for updates



Windows Update

Checking for updates...

Your device is missing important security and quality fixes.

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 08:00 to 17:00

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

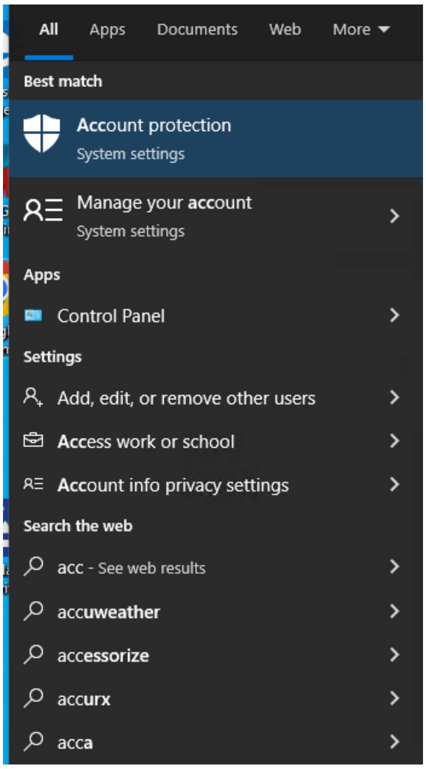
Looking for info on the latest updates?
Learn more

Related links
Check Storage

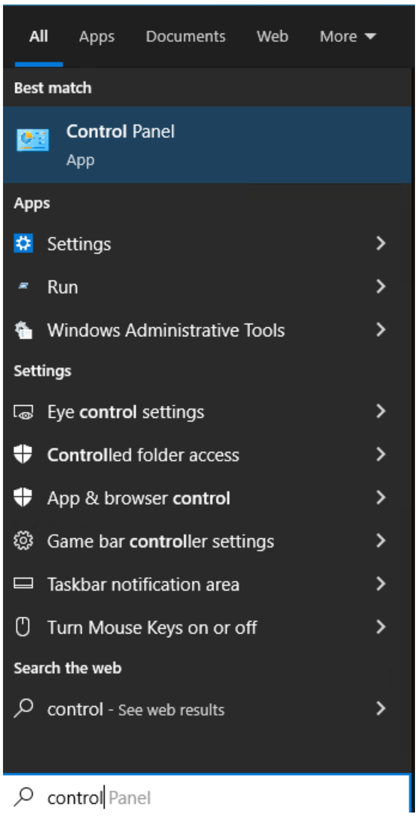
41. The PC will then start downloading and installing updates

Create Accounts

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



2. Type Control Panel and select it from menu

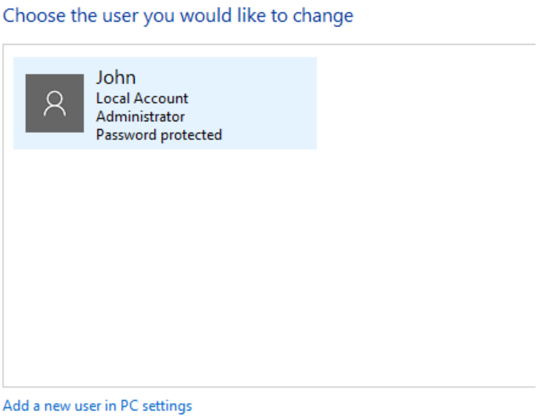


control Panel

3. Select User Accounts

4. Select Manage another account

5. Select add a new user

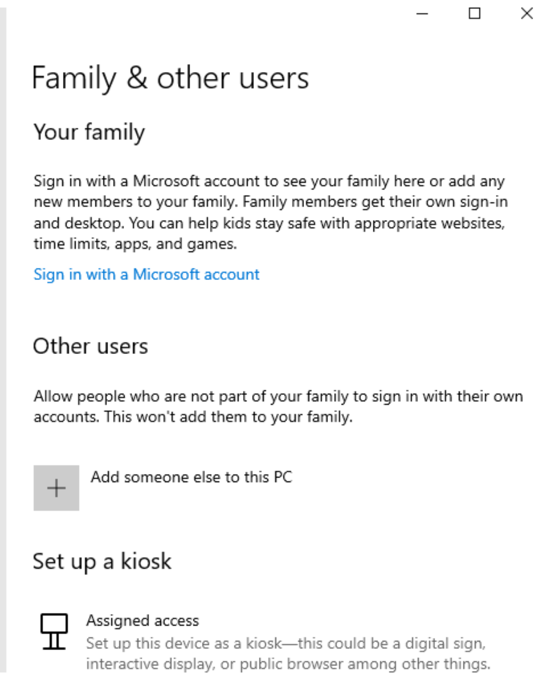


Choose the user you would like to change

John
Local Account
Administrator
Password protected

Add a new user in PC settings

6. Select Add someone else



Family & other users

Your family

Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games.

Sign in with a Microsoft account

Other users

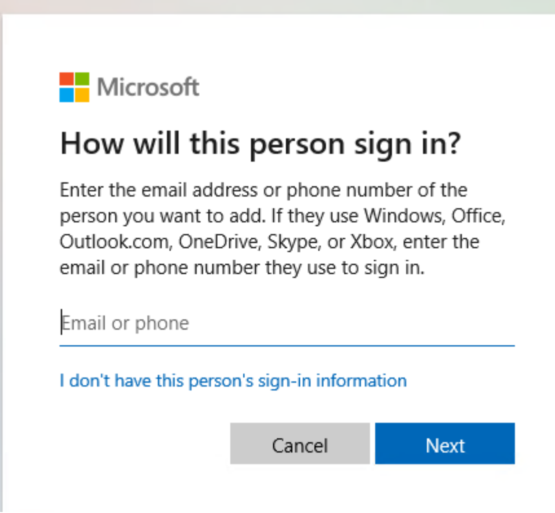
Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

Add someone else to this PC

Set up a kiosk

Assigned access
Set up this device as a kiosk—this could be a digital sign, interactive display, or public browser among other things.

7. Select I don’t have this person’s sign-in information



Microsoft

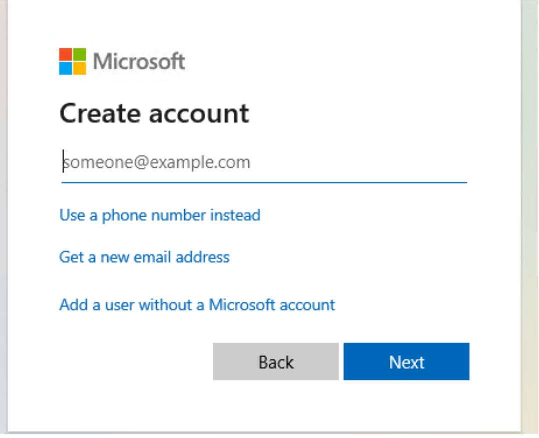
How will this person sign in?

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

8. Select Add a user without a Microsoft account



Microsoft

Create account

someone@example.com

Use a phone number instead

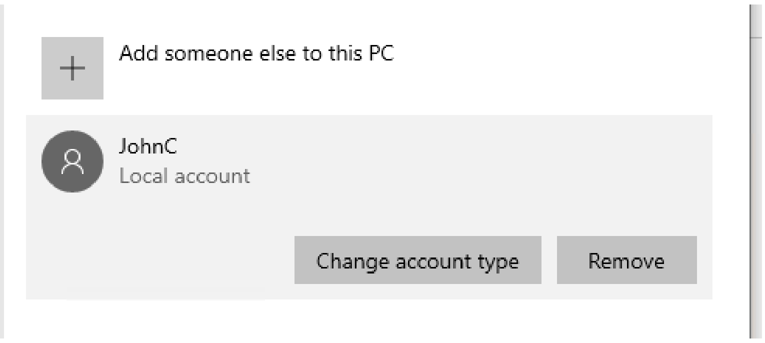
Get a new email address

Add a user without a Microsoft account

9. Type the username and password

10. Answer the security questions

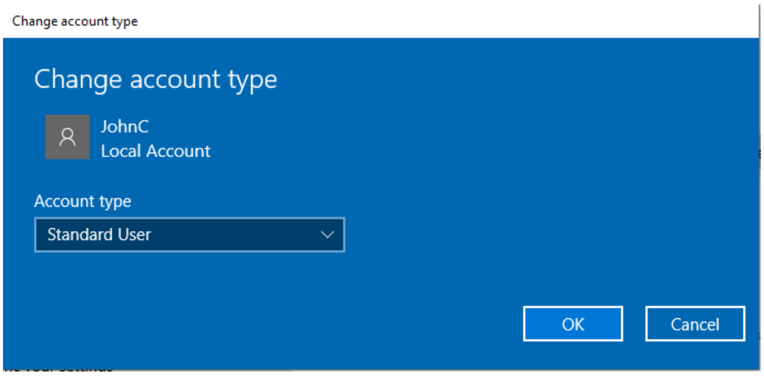
11.The user account will be created as a standard user



Add someone else to this PC

JohnC
Local account

12.Change account type



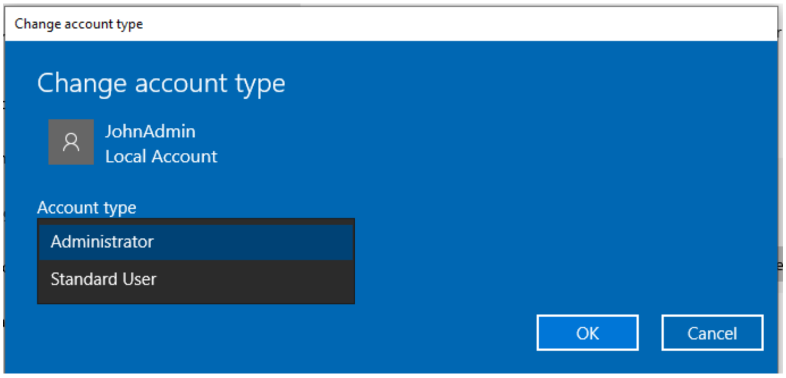
Change account type

JohnC
Local Account

Account type: Standard User

13. Run through the steps again to create an admin account (JohnAdmin)

1414. Make JohnAdmin an administrator account by selecting Administrator from the dropdown

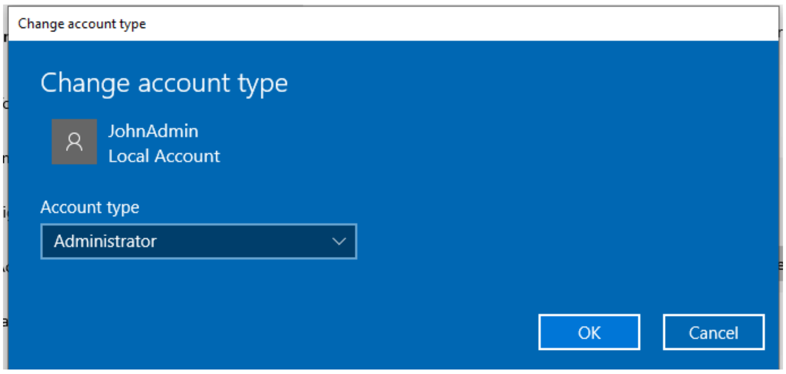


Change account type

JohnAdmin
Local Account

Account type

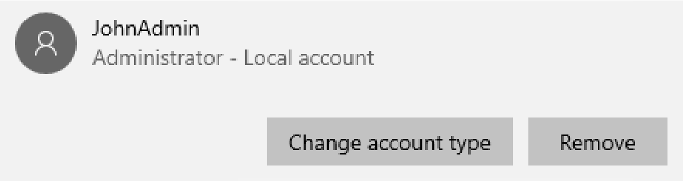
15. You will see that JohnAdmin is an administrator



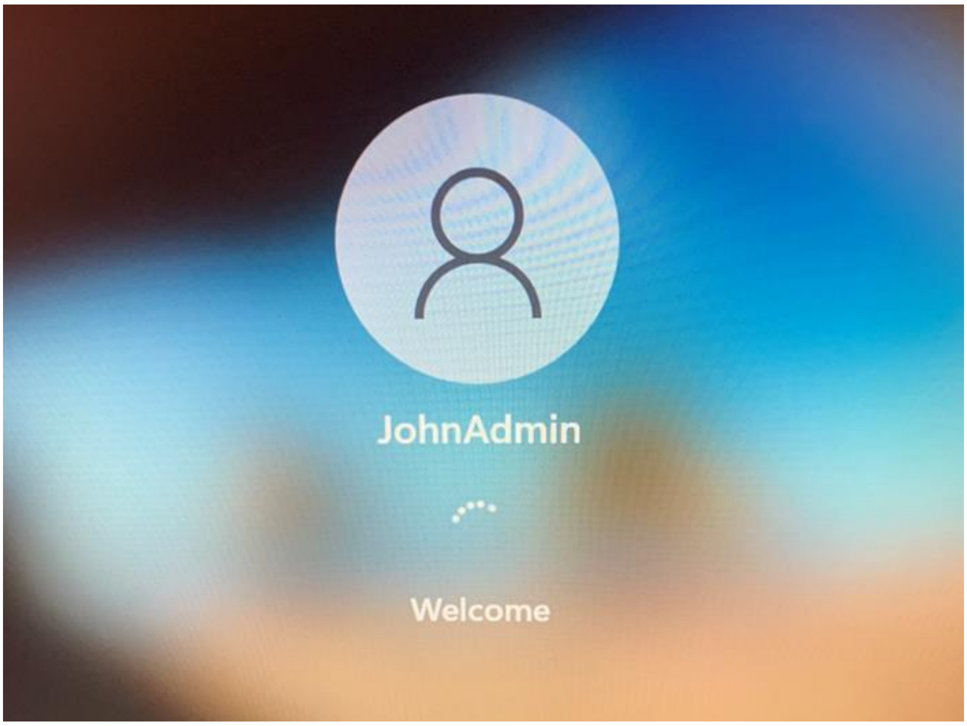
Change account type

JohnAdmin
Local Account

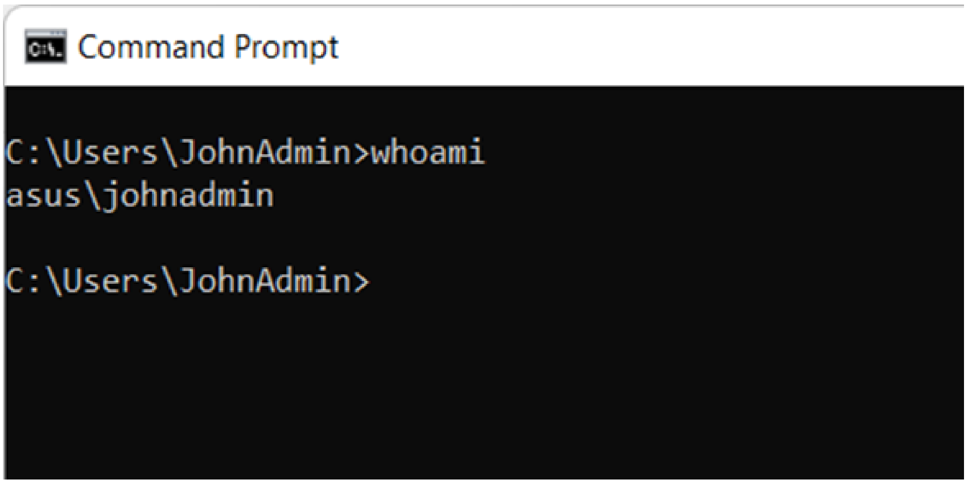
Account type: Administrator


JohnAdmin
Administrator - Local account

16. JohnAdmin account logging in



17. Whoami command to demonstrate logged in user is JohnAdmin



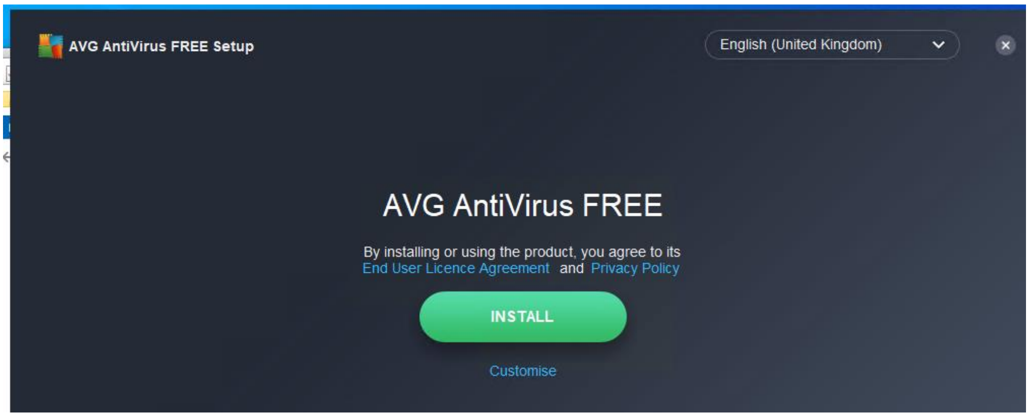
```
C:\Users\JohnAdmin>whoami
asus\johnadmin

C:\Users\JohnAdmin>
```

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



AVG AntiVirus FREE Setup

English (United Kingdom)

AVG AntiVirus FREE

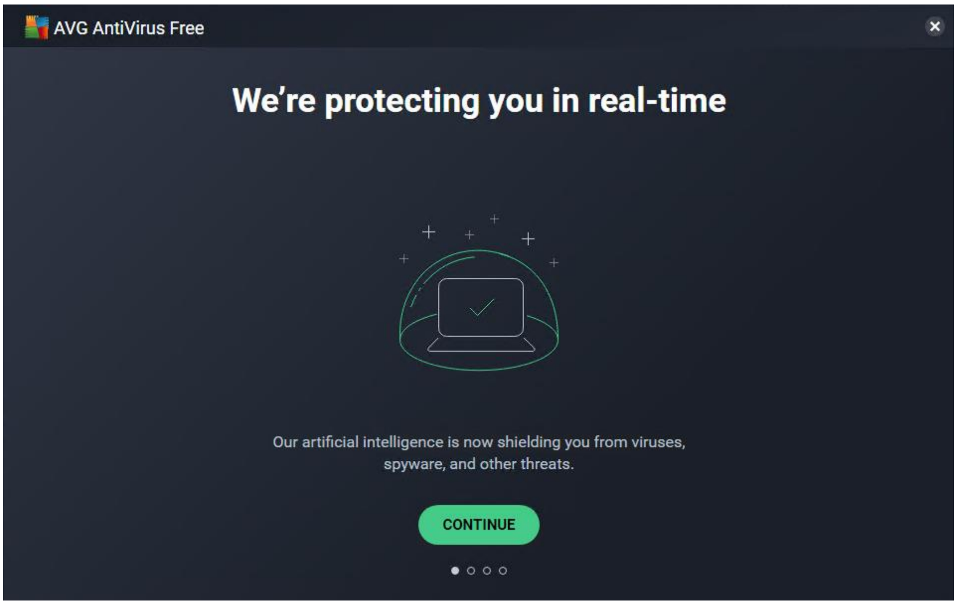
By installing or using the product, you agree to its End User Licence Agreement and Privacy Policy

INSTALL

Customise

5. Install will commence

6. When complete click Continue 4 times



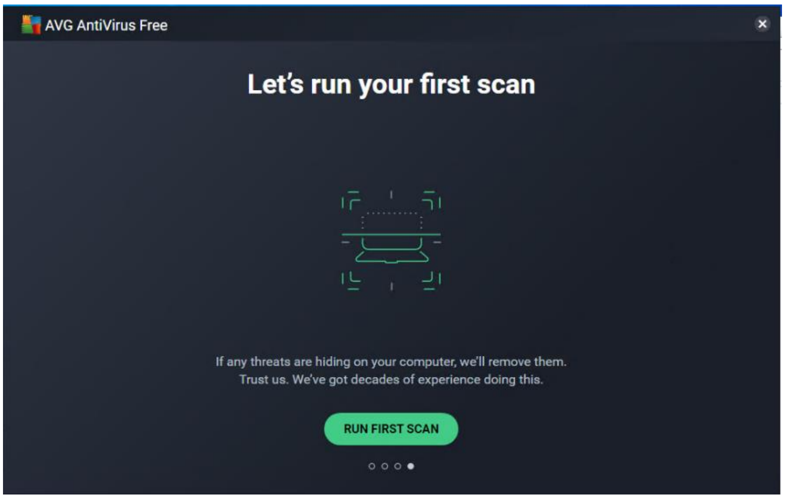
AVG AntiVirus Free

We're protecting you in real-time

Our artificial intelligence is now shielding you from viruses, spyware, and other threats.

CONTINUE

7. Run first scan

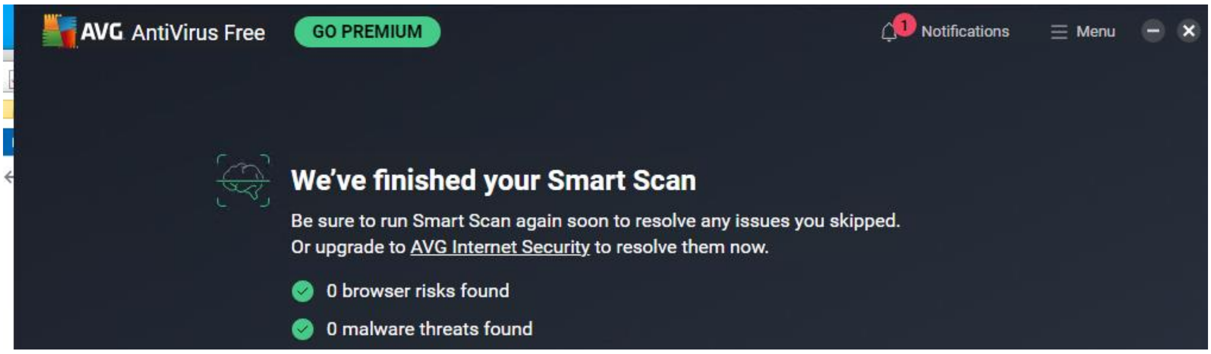


AVG AntiVirus Free

Let's run your first scan

If any threats are hiding on your computer, we'll remove them.
Trust us. We've got decades of experience doing this.

5. Scan will complete and show details



We've finished your Smart Scan

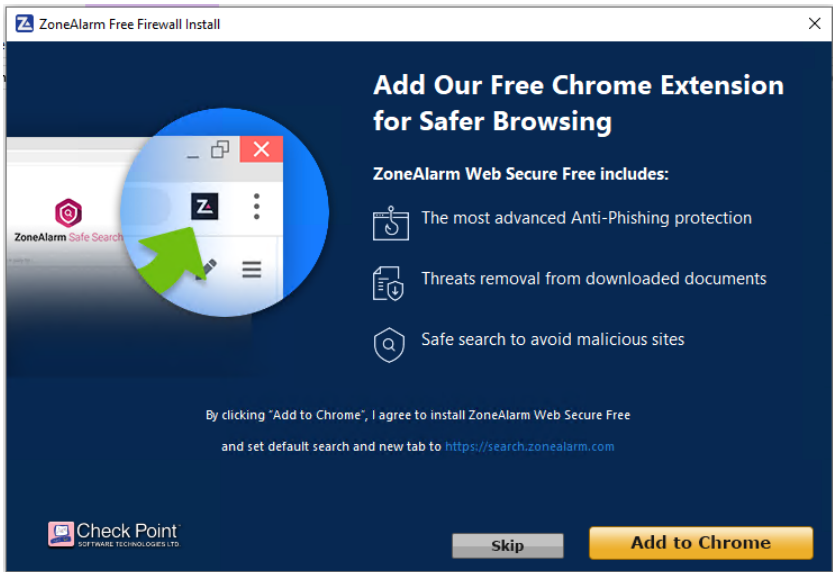
Be sure to run Smart Scan again soon to resolve any issues you skipped.
Or upgrade to AVG Internet Security to resolve them now.

0 browser risks found

0 malware threats found

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


ZoneAlarm Free Firewall Install
ZoneAlarm Safe Search
Check Point SOFTWARE TECHNOLOGIES LTD.
Skip
Add to Chrome

Add Our Free Chrome Extension for Safer Browsing

ZoneAlarm Web Secure Free includes:

The most advanced Anti-Phishing protection

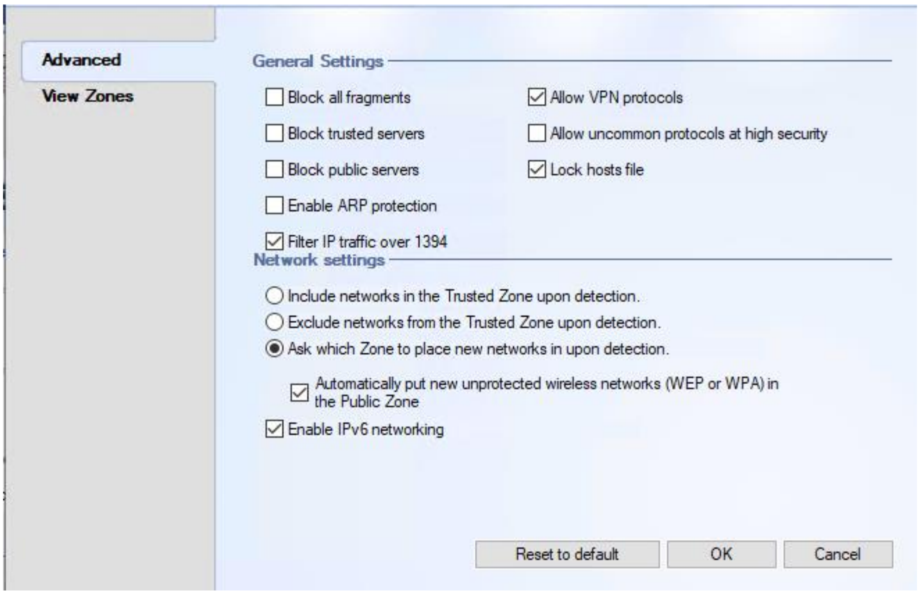
Threats removal from downloaded documents

Safe search to avoid malicious sites

By clicking "Add to Chrome", I agree to install ZoneAlarm Web Secure Free and set default search and new tab to https://search.zonealarm.com

6. Firewall will install

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



General Settings

☐ Block all fragments
☐ Block trusted servers
☐ Block public servers
☐ Enable ARP protection
☑ Filter IP traffic over 1394
☑ Allow VPN protocols
☐ Allow uncommon protocols at high security
☑ Lock hosts file

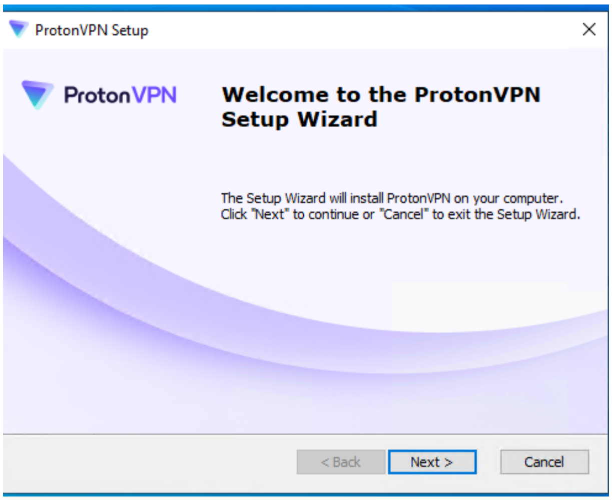
Network settings

○ Include networks in the Trusted Zone upon detection.
○ Exclude networks from the Trusted Zone upon detection.
● Ask which Zone to place new networks in upon detection.
☑ Automatically put new unprotected wireless networks (WEP or WPA) in the Public Zone
☑ Enable IPv6 networking

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 the click Next
3. Click Next to check prerequisites

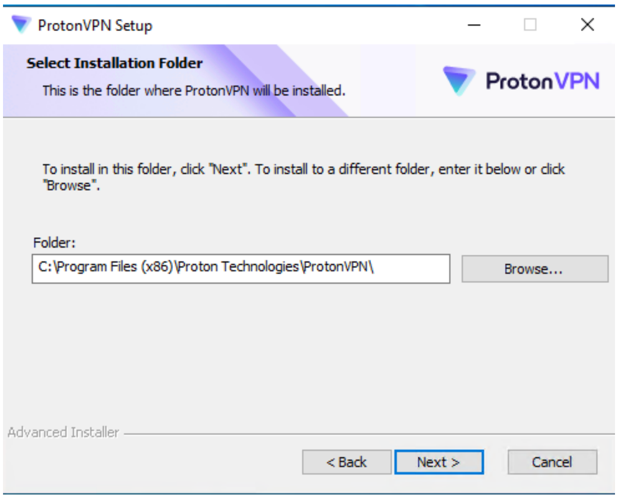
4. Accept prerequisites by clicking Next
5. Software will install
6. Click next



Welcome to the ProtonVPN Setup Wizard

The Setup Wizard will install ProtonVPN on your computer.
Click "Next" to continue or "Cancel" to exit the Setup Wizard.

7. Click next



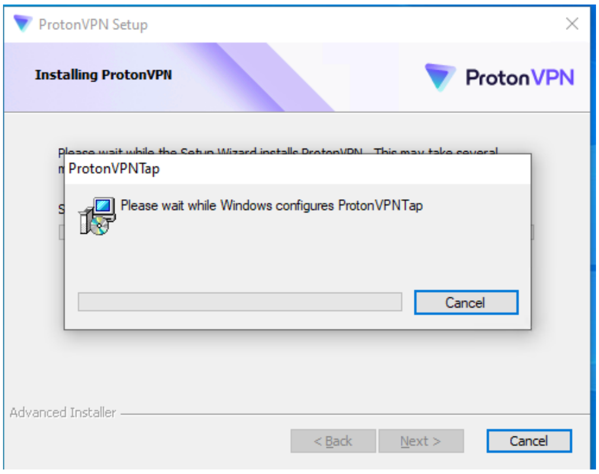
Select Installation Folder

This is the folder where ProtonVPN will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files (x86)\Proton Technologies\ProtonVPN\

8. Software will install



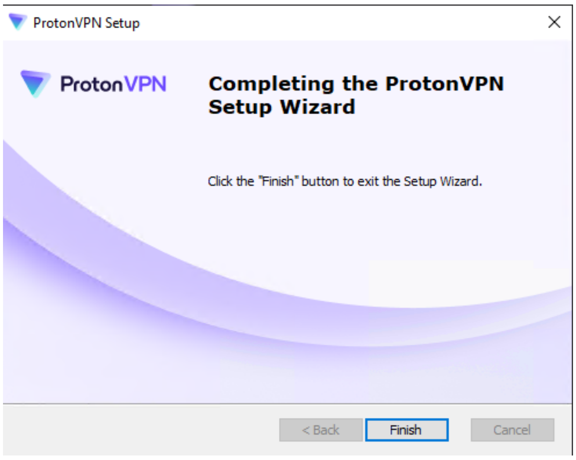
Installing ProtonVPN

Please wait while the Setup Wizard installs ProtonVPN. This may take several

ProtonVPNTap

Please wait while Windows configures ProtonVPNTap

9. Click Finish

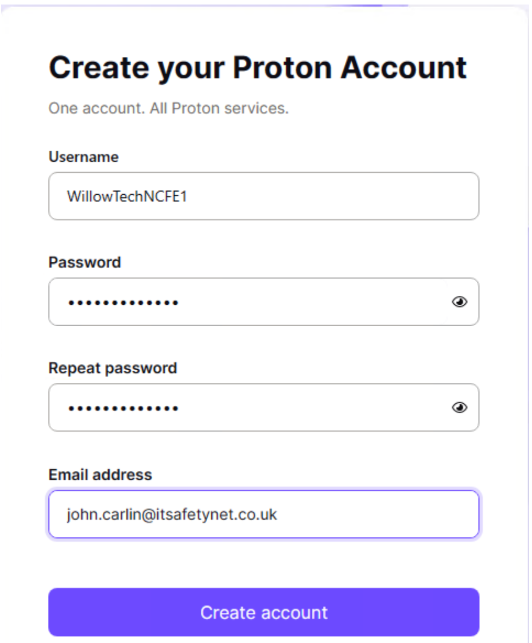


ProtonVPN Setup

Completing the ProtonVPN Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

10. Create Proton account



Create your Proton Account

One account. All Proton services.

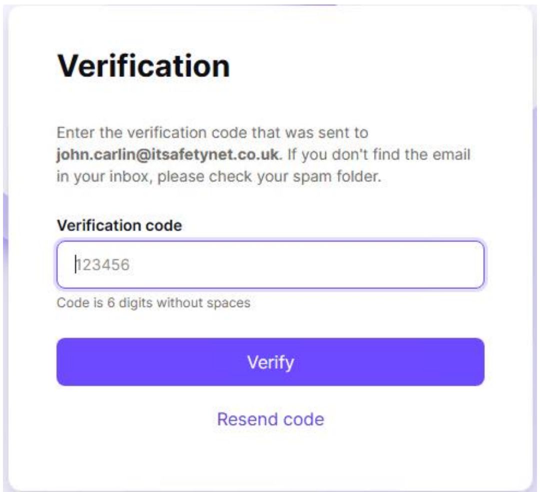
Username: WillowTechNCFE1

Password: •••••••••••••

Repeat password: •••••••••••••

Email address: john.carlin@itsafetynet.co.uk

11.Enter verification code



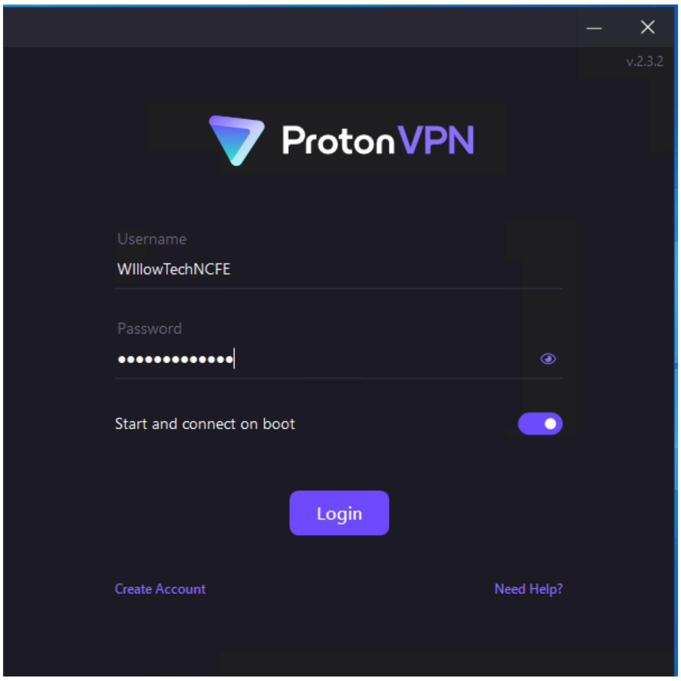
Verification

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: 123456

Code is 6 digits without spaces

12. Login with account and password just set up

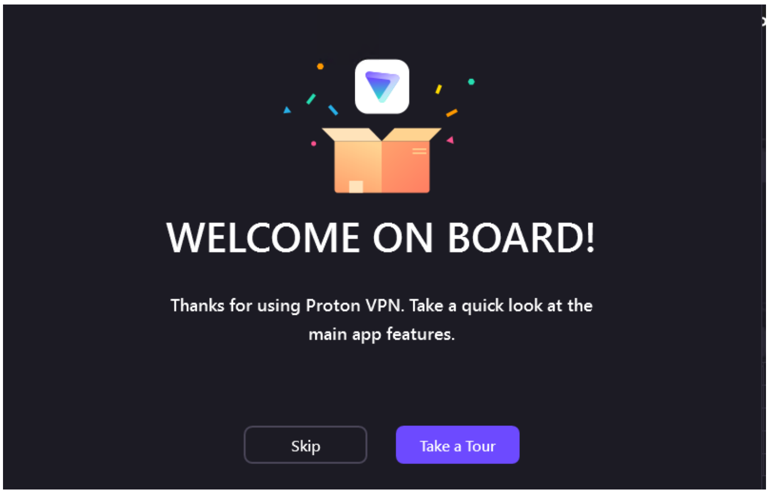


Username
WIllowTechNCFE

Password
•••••••••••••

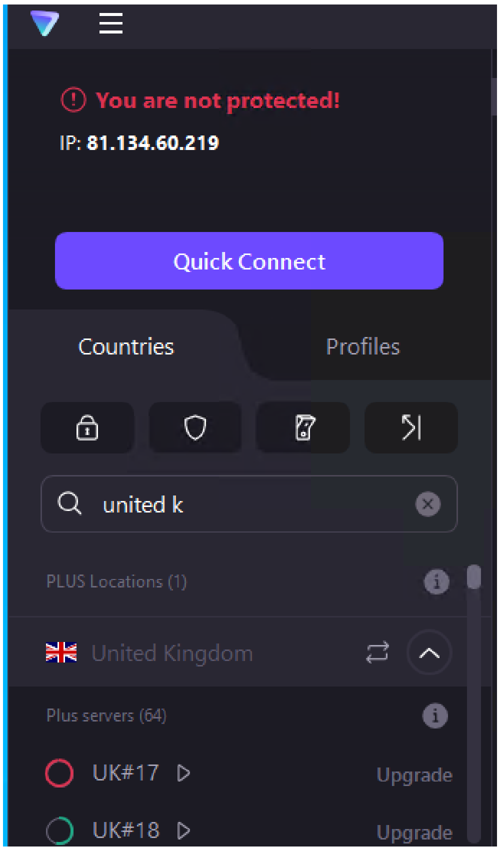
Start and connect on boot

13.Skip tour


WELCOME ON BOARD!

Thanks for using Proton VPN. Take a quick look at the main app features.

14. Click quick connect button to create a secure VPN connection



You are not protected!

IP: 81.134.60.219

united k

PLUS Locations (1)

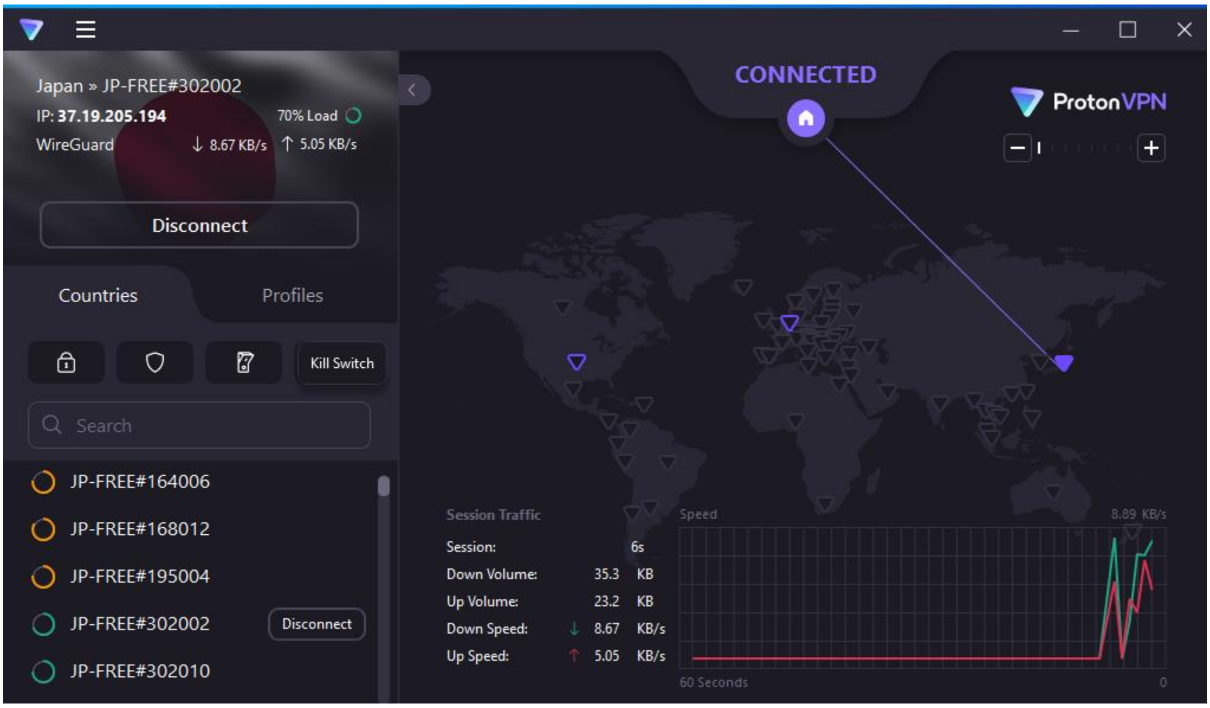
United Kingdom

Plus servers (64)

UK#17 Upgrade

UK#18 Upgrade

15. You are connected to VPN server in Japan, connection is now secure and VPN software is working correctly



Japan » JP-FREE#302002

IP: 37.19.205.194 70% Load

WireGuard ↓ 8.67 KB/s ↑ 5.05 KB/s

CONNECTED

JP-FREE#164006

JP-FREE#168012

JP-FREE#195004

JP-FREE#302002 Disconnect

JP-FREE#302010

Session Traffic

Session:	6s	
Down Volume:	35.3	KB
Up Volume:	23.2	KB
Down Speed:	↓ 8.67	KB/s
Up Speed:	↑ 5.05	KB/s

16. Testing table

Test	**Outcome**
Install Windows OS	OS installed
Create account**s**	Accounts created for JohnC and JohnAdmin. JohnAdmin set as administrator account type
Login to Windows	JohnAdmin successfully logged in
Install AVG	Installation successful
Run AVG scan	Scan runs and found no malware
Install firewall	Firewall installed with no problems
Create firewall rule	Firewall rule created successfully to set to filter IP and lock the local host file
Install VPN	VPN software installed successfully
Create VPN user account	John’s account created successfully
Login to VPN account	Login success and welcome aboard message displayed.
Confirm VPN connection	VPN connection successfully connected to server in Japan with IP 37.19.205.194

Examiner commentary

Overall this student response is good however, there is still room for a much greater level of detail and research. In many cases the student has chosen a source for analysis but has not fully determined the suitability of this source.

Task 1

The student's analysis of the firewall included an adequate set of minimum requirements. There were missed opportunities for the students to demonstrate other additional options that were available. The analysis was good but would have benefitted from a deeper analysis of pros, cons and cost. This would have helped to provide a more justifiable solution. The student’s response was also very generalised and could have been better contextualized towards the scenario, although some of the bullet points do reference the scenario. This is highlighted for hardware firewalls but the student could have developed their response further by suggesting that it could support future growth for Willow and be ideal for the size of their IT team.

The rationale for the final choice was well thought-out but the response has not considered all the pros and cons. As such, the final choice may not have been approached in as logical a manner as it otherwise could have been. In all cases 2 products have been chosen for comparison but little reasoning supplied for these choices. This has resulted in a final summary that might be accurate for the 2 products compared but not if these were the best 2 to compare. The student showed an understanding of the software programs but has missed opportunities to explain the impact that their capabilities may have on the business. The student gave a good explanation of the legal requirements that needed to be addressed but did not include full references to relevant legal statutes. This would have been clearer for the reader if all legislation had been addressed in one section of the project proposal so they could easily see a comparison of the software and legislative requirements. The student's project proposal provided an evaluation of the products but in many instances this just consisted of recommendations rather than justification. This would have benefited from clearer justifications for the recommendations made. Overall, the student’s project proposal was fairly clear and in the main logically formatted.

Task 2

The student carried out a good set up of the virtual machine (VM) with the required software program but has missed some areas, such as what to do if Windows 10 was not activated with a key. This however does not affect the installation of the operating system. They have tested the VM to ensure it was operating as expected and included screenshots to evidence this. The student provided good evidence of the setup and testing along with some screenshots, although this would have benefitted from further screenshots evidencing the whole process. Due to this the procedure has not been fully captured and in some places the narrative could have been followed incorrectly due to lack of visual evidence. The student successfully remediated any issues, and this was evidenced through their narrative. This was mostly backed up with screenshots that demonstrated they understood the functionality of the software. The students has concluded with a table that highlights the stages of the task and the outcome of each. This would have benefited from further detail, for example an additional column showing expected outcomes or any remedial action required.

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

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.

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