

Basics of Cyber Security

Contents

| | | | |
|--|-----------|---|----|
| What is Cyber Security and why is it important? | 4 | | |
| What is cybercrime? | 5 | | |
| What to do to help against cybercrime | 6 | | |
| What is a system administrator? | 7 | | |
| User Accounts | 7 | | |
| Windows | 7 | | |
| Ubuntu | 10 | | |
| Cyber Security tools | 11 | | |
| Firewall | 11 | | |
| Windows Firewall | 11 | | |
| Windows: how to alter the firewall settings | 12 | | |
| Ubuntu Firewall | 15 | | |
| Ubuntu: how to alter the firewall settings | 17 | | |
| Passwords | 19 | | |
| What makes a good password? | 19 | | |
| Windows - reset a user's password | 19 | | |
| | | Windows - enforcing and editing a password policy | 20 |
| | | Ubuntu - reset a user's password | 21 |
| | | Ubuntu - enforcing and editing a password policy | 22 |
| | | Adding & removing a program on Windows & Ubuntu | 24 |
| | | Windows | 25 |
| | | Ubuntu | 26 |
| | | System Updates | 28 |
| | | How to update Windows | 29 |
| | | How to update Ubuntu | 30 |
| | | Anti-Virus | 32 |
| | | What is Anti-Virus Software? | 32 |
| | | How to enable anti-virus on Windows | 30 |
| | | How to enable anti-virus on Ubuntu | 35 |



As part of this guide, you will:

- identify why Cyber Security is important,
- describe the role of a system administrator,
- define a firewall and demonstrate how to alter the settings in Windows and Ubuntu,
- describe what makes a good password,
- demonstrate how to change a user's password in Windows and Ubuntu,
- demonstrate how to edit the password policy within the settings of Windows and Ubuntu for all users
- demonstrate how to add and remove programs in Windows and Ubuntu,
- define the importance of system updates and demonstrate how to update and enforce automatic updates,
- describe what an anti-virus is and how to enable it in Windows and Ubuntu.

What is Cyber Security and why is it important?

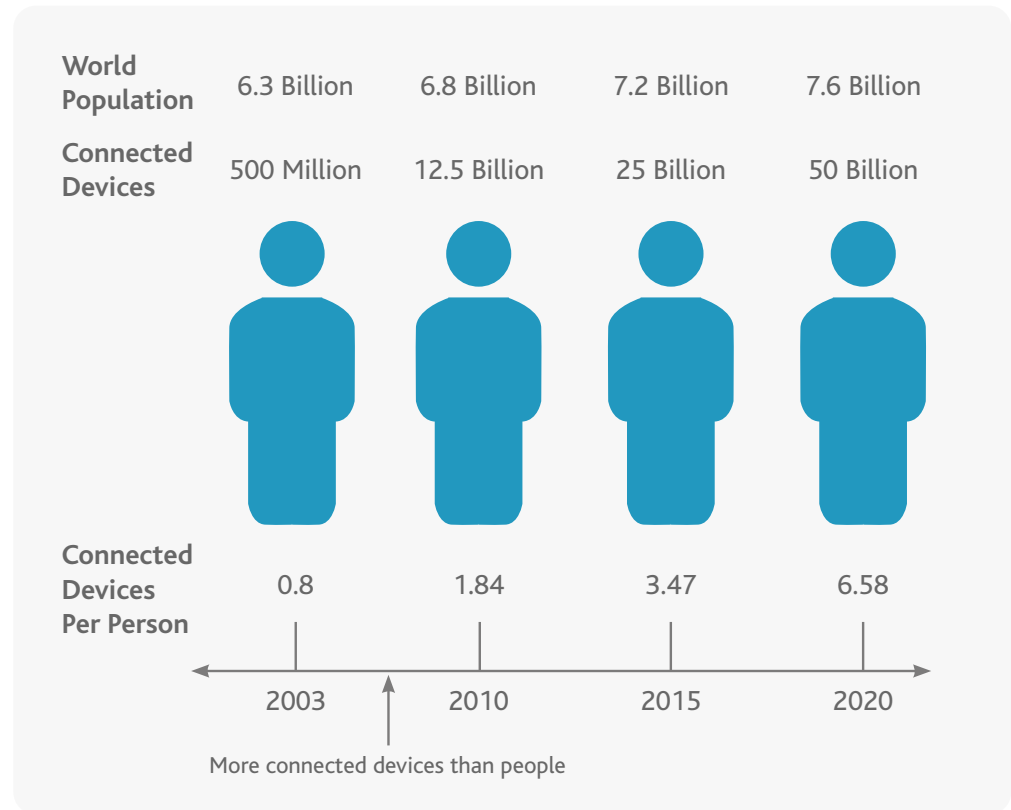
Most people today have a device they rely on to socialise, communicate, complete work for business and school as well as playing games, shopping, general information searching and booking holidays. The list is always growing and new ways to interact online and use technology will always be a developing industry.



Technology has gone from standalone devices to globally connected devices through the internet to the internet of things (IoT).

Standalone devices are not connected to anything else.

The internet is a global network of connected devices. With all this technology and people using it, there comes risks. Everybody uses personal information on devices and online to help utilise it for a specific function. Cyber Security is about protecting this.



Cyber Security is about protecting the devices we use and the services we access from cybercrime.

What is Cybercrime?

Cybercrime is a major threat to anyone using the internet and millions of people have already had their information stolen and may not know about it.

IBM president and CEO Ginni Rometty in 2015 described cybercrime as *“the greatest threat to every profession, every industry, every company in the world.”* <https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/>

Cybercrime is defined as any illegal act that involves the use of a computing device, either as the object of the crime or the tool in the crime.

There are three main categories relating to cybercrime as they relate to property, individuals, and government. This is a growing criminal industry as new ways to damage, exploit and steal through technology emerge.

Cyber Security fact In 2020 the average number of devices per household was 10. With the development of IoT the number of connected devices globally in 2021 will be 46 billion.

Some examples of cybercrime include:

1. Viruses
2. Malware
3. DoS Attacks
4. Phishing
5. Cyberstalking
6. Identity theft
7. Botnets
8. Social Engineering
9. PUPs
10. Prohibited/illegal content
11. Online scams
12. Exploit Kits

For more details on types of cybercrimes [click here](#).

Cyber Security facts:

- The estimated global cost of cybercrime will be \$6 trillion by 2021.
- 48% of data security breaches are as a result of malicious intent.
- Ransomware costs in 2019 were estimated to have been around \$11.5 billion.

What to do to help against cybercrime

It is important that everyone knows about how to be safe and stay safe against potential cybercrimes. Things to consider include:

- When visiting any website, be vigilant about what information it is asking you for, what needs to be filled in, what cookies they want to apply etc
- Ensure that suspicious emails are flagged and reported, not just deleted as this helps inform cybercrime departments/ companies on current potential threats.
- Never click a link that you do not recognise or looks wrong either on a website or within an email or advert.
- Use a Virtual private network (VPN) wherever possible. A VPN extends a private network over a public one and ensures all data shared is the same as sharing on a private network.
- Ensure you have anti-virus software installed on all devices and updated.
- Ensure passwords are strong.

We will look at some of these in more detail within the next section of this guide.

Cyber Security facts:

<https://www.ibm.com/uk-en/security/data-breach> - IBM report on how much a data breach costs.

Key findings:

- **2021 had the highest average cost in 17 years**
Data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the 17-year history of this report
- **Remote work due to COVID-19 increased cost**
The average cost was USD 1.07 million higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor.
- **Compromised credentials caused the most breaches**
The most common initial attack vector, compromised credentials, was responsible for 20% of breaches at an average breach cost of USD 4.37 million.

What is a System Administrator?

The main aspects of the system administrator are:

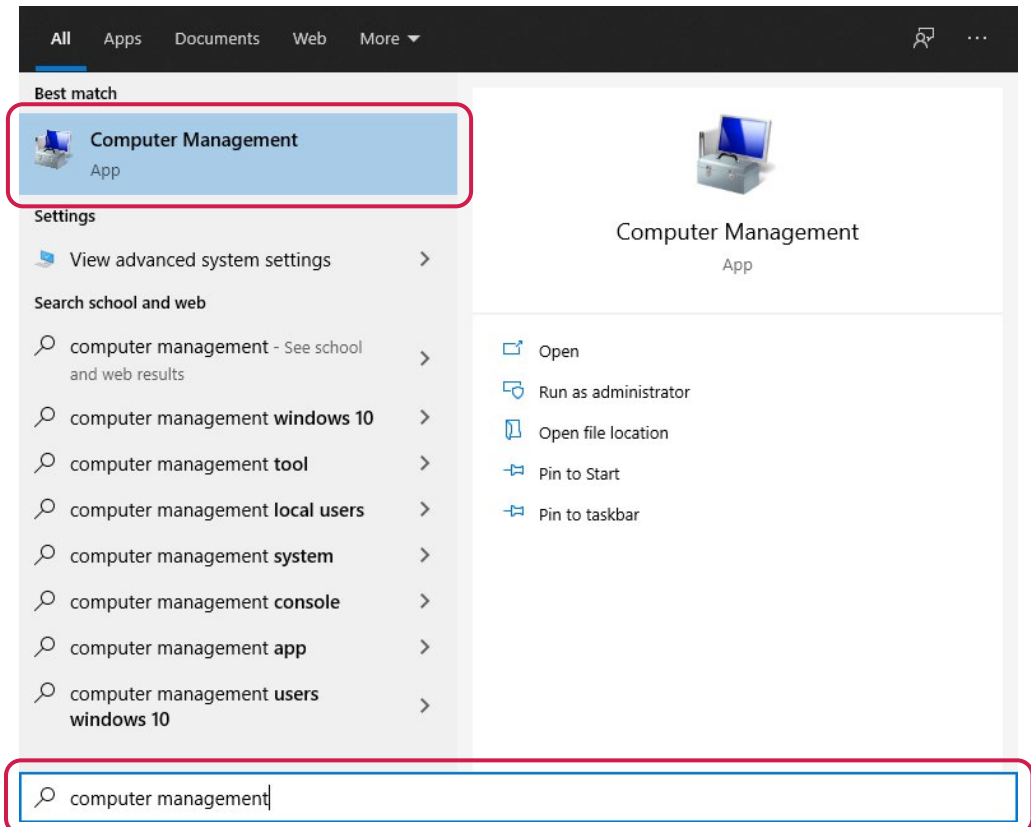
- System upkeep
- System configuration
- Ensuring system operation continues for all users and the server.

User Accounts

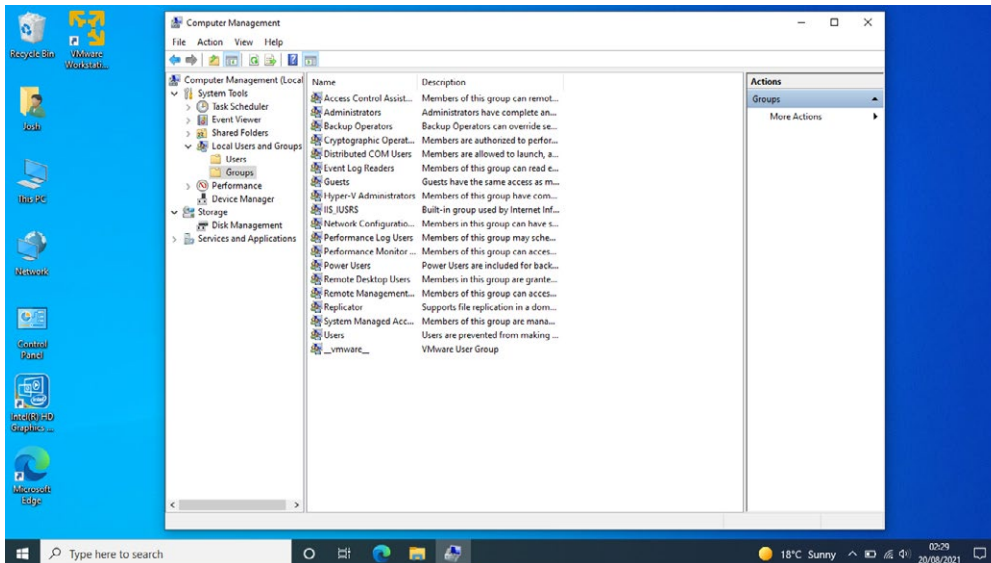
One of the main aspects of the system administrator's role is to maintain user accounts and the permissions they have within the network. You can view your systems user accounts in the following ways:

Windows

1. Using the search icon on the bottom left of the screen, type in **Computer Management** and select it, when located.

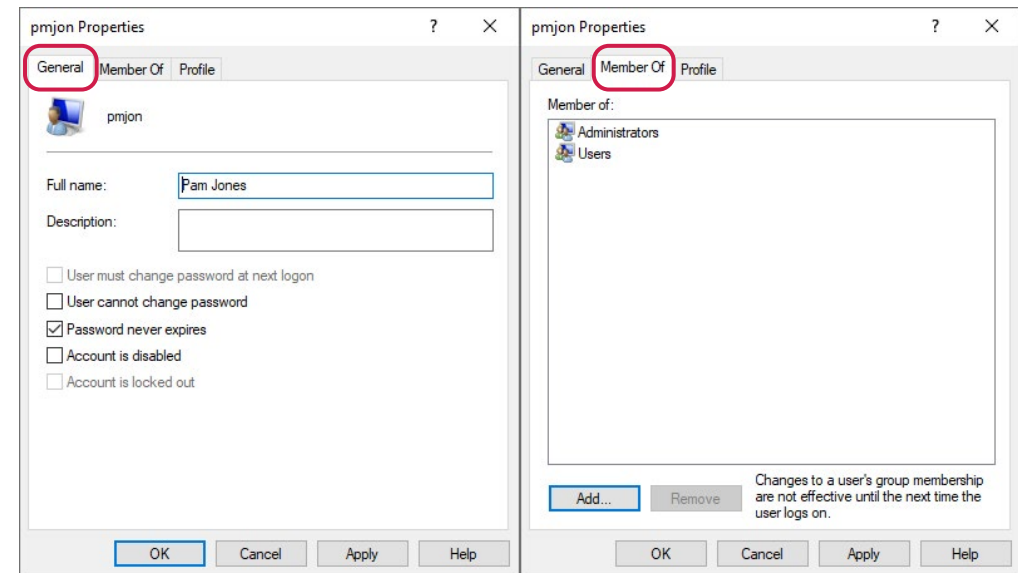


2. Select on the left-hand side **Local Users and Groups**. There are two folders within this dropdown: **Users** and **Groups**.



3. **Users** = These are the user accounts and the settings for that user.

You can double click on a user to see additional information regarding password permissions set and the groups that the user is a member of.



- This user is within the groups
 - **Administrators** – have complete and unrestricted access to the computer/domain
 - **Users** – are prevented from making accidental or intentional system-wide changes and can run most applications
- They can change their own password, the password set never expires and the account is enabled.

There are lots of different groups set on a device and these can be **local** groups if they are set on a personal device. You can also preview all the groups set on the device by using **Command Prompt**.

- Open **Command Prompt** by searching for it and open as a program.
- Enter the command `net localgroup` and press enter to see the list of possible groups

```

Command Prompt
(c) Microsoft Corporation. All rights reserved.
C:\Users\pmj\>net localgroup

Aliases for \\DESKTOP-751CAGV
-----
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
The command completed successfully.
  
```

- You can check this against **Computer Management** and see the same groups as well as a brief outline of what they have permission to do.

| Name | Description |
|-------------------------------------|--|
| Access Control Assistance Operators | Members of this group can remotely query authorization attributes and permissions for resources on this computer. |
| Administrators | Administrators have complete and unrestricted access to the computer/domain. |
| Backup Operators | Backup Operators can override security restrictions for the sole purpose of backing up or restoring files. |
| Cryptographic Operators | Members are authorized to perform cryptographic operations. |
| Device Owners | Members of this group can change system-wide settings. |
| Distributed COM Users | Members are allowed to launch, activate and use Distributed COM objects on this machine. |
| Event Log Readers | Members of this group can read event logs from local machine. |
| Guests | Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted. |
| Hyper-V Administrators | Members of this group have complete and unrestricted access to all features of Hyper-V. |
| IIS_IUSRS | Built-in group used by Internet Information Services. |
| Network Configuration Operators | Members in this group can have some administrative privileges to manage configuration of networking features. |
| Performance Log Users | Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer. |
| Performance Monitor Users | Members of this group can access performance counter data locally and remotely. |
| Power Users | Power Users are included for backwards compatibility and possess limited administrative powers. |
| Remote Desktop Users | Members in this group are granted the right to logon remotely. |
| Remote Management Users | Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user. |
| Replicator | Supports file replication in a domain. |
| System Managed Accounts Group | Members of this group are managed by the system. |
| Users | Users are prevented from making accidental or intentional system-wide changes and can run most applications. |

- Within **Command Prompt** you can see what groups your account belongs to by typing in `whoami /groups` and press enter.

```

Command Prompt
Microsoft Windows [Version 10.0.19042.1137]
(c) Microsoft Corporation. All rights reserved.

C:\Users\pjohn\whoami /groups

GROUP INFORMATION
-----
Group Name                                     Type                SID                               Attributes
-----
Mandatory Label\Medium Mandatory level       Label                S-1-16-18192
Everyone                                     Well-known group    S-1-1-0
NT AUTHORITY\Local account and member of Administrators group Well-known group    S-1-5-32-544
MULTIMEDIA Administrators                   Alias                S-1-5-32-544
MULTIMEDIA Users                           Well-known group    S-1-5-32-545
NT AUTHORITY\INTERACTIVE                    Well-known group    S-1-5-4
CONSOLE LOGON                               Well-known group    S-1-2-1
NT AUTHORITY\Authenticated Users            Well-known group    S-1-5-11
NT AUTHORITY\This Organization               Well-known group    S-1-5-15
MicrosoftAccount\pjohns@gmail.com         User                 S-1-11-06-3823654863-68364-18864-2661722203-1597681003-44444351-3000829486-121056005-4273471160-09014955
NT AUTHORITY\Local account                  Well-known group    S-1-5-113
LOCAL                                       Well-known group    S-1-2-0
NT AUTHORITY\Cloud Account Authentication    Well-known group    S-1-5-64-36
  
```

Ubuntu

Using the command prompt type in the command `groups` and press enter. The list of the groups you as the logged in user have access to are then listed.

```

pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ groups
pj adm cdrom sudo dip plugdev lpadmin lxd sambashare
pj@pj-Aspire-TC-780:~$
  
```

To look at the groups another user has set you can use the command `groups username` for example

`groups guest`

You can also see all the users set on a device by using the command

`compgen -u`

Cyber Security facts:

If a user has access to specific groups, they may be able to edit or delete other users and cause a security issue. It is important to ensure users have the correct permissions.

Cyber Security Tools

Firewall

A firewall is essential to a networks security as it monitors and controls the incoming and outgoing network traffic. The decisions are made based on the rules set within the firewall settings and these settings act as the barrier from your device within a trusted network to a wider untrusted network like the internet.

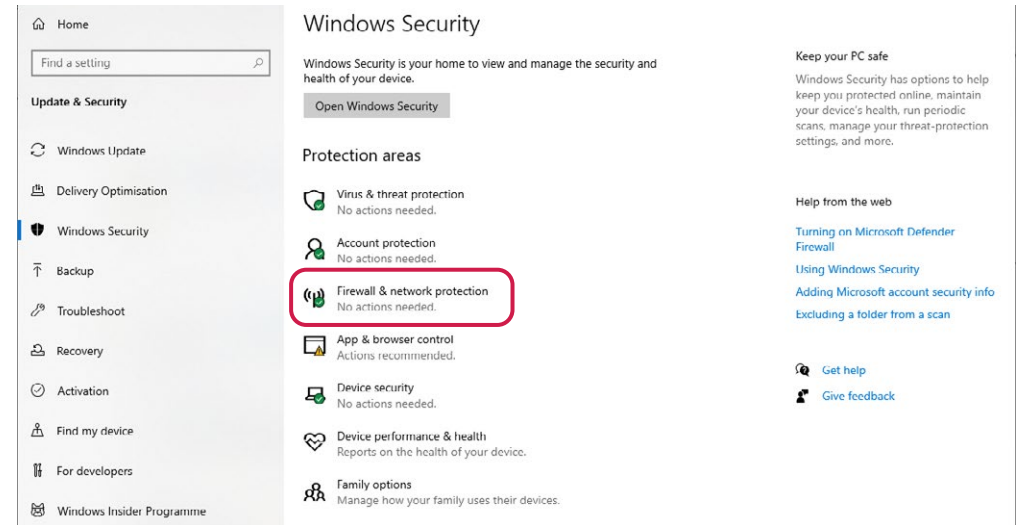


Windows Firewall

The default firewall on Microsoft is Microsoft Defender Firewall. Let's look at how to turn it on and off.

Following the steps below to open or type in **firewall** in the search programs option:

Start -> Settings -> Update & Security -> Windows Security -> Firewall & Network Protection



- Select the network profile
- Under Microsoft Defender **Firewall**, you will see an option to edit the setting to on or off.
 - If you cannot see the option to turn on or off, you may not have permission as a user to edit this setting.
 - If you use software like Avast as a free downloadable antivirus that has a firewall built in, you will likely have Microsoft Defender Firewall switched off. You instead need to look at the settings within the anti-virus package.

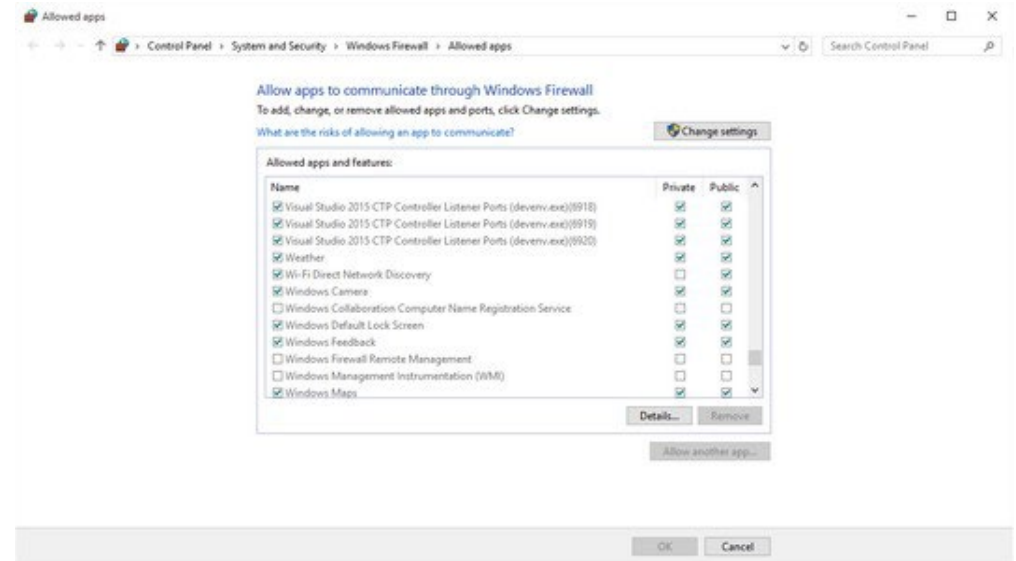
Cyber-Security Fact:

Turning off a firewall leaves your computing device vulnerable to unauthorised attacks, this is the case for any device that is connected to a large open network like the internet.

Windows: How to alter the firewall settings

There may be a time that you want to allow a certain piece of software to run on a machine that the firewall is blocking. To add a new rule or exception to the firewall:

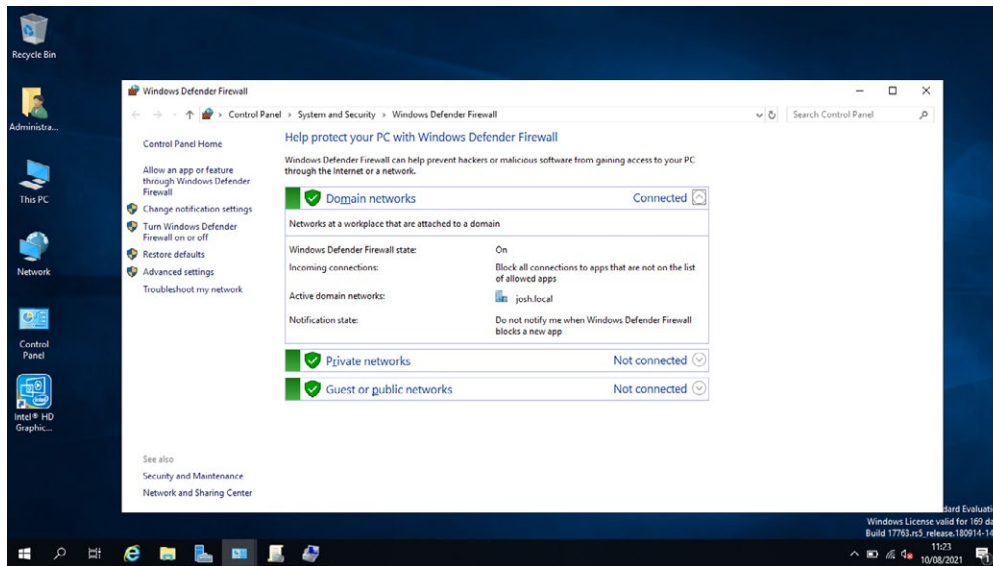
- Type **Firewall** into the search programs area and this will open the Firewall & Network Protection area.
- Select the **Allow an APP through the firewall**.
- You will be presented with a long list of programs that are available to allow or disallow.
- You can select a software to be allowed and select if this is allowed for private or public connections.



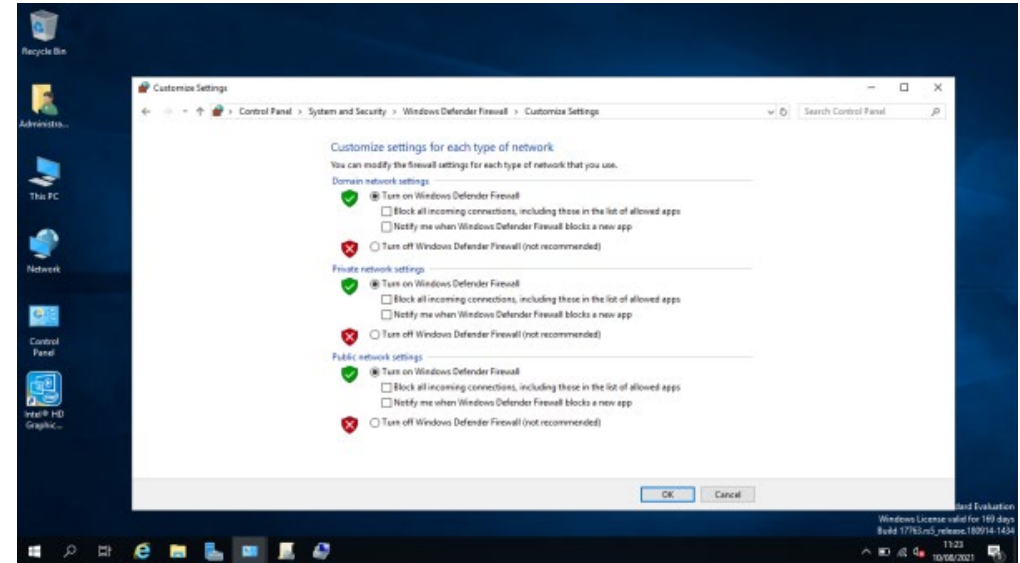
Cyber Security fact:

Remember that changing settings is allowing packets of data to enter the device and you need to be sure that this is a safe and secure application that will not cause harm to your device.

In the program search option type in **Windows Defender Firewall**, you will open the settings showing the status of the firewall.







You can access and customise the settings here to turn on and off the firewall as well as receive notifications and block all incoming connections.



Control Panel Home

Allow an app or feature through Windows Defender Firewall

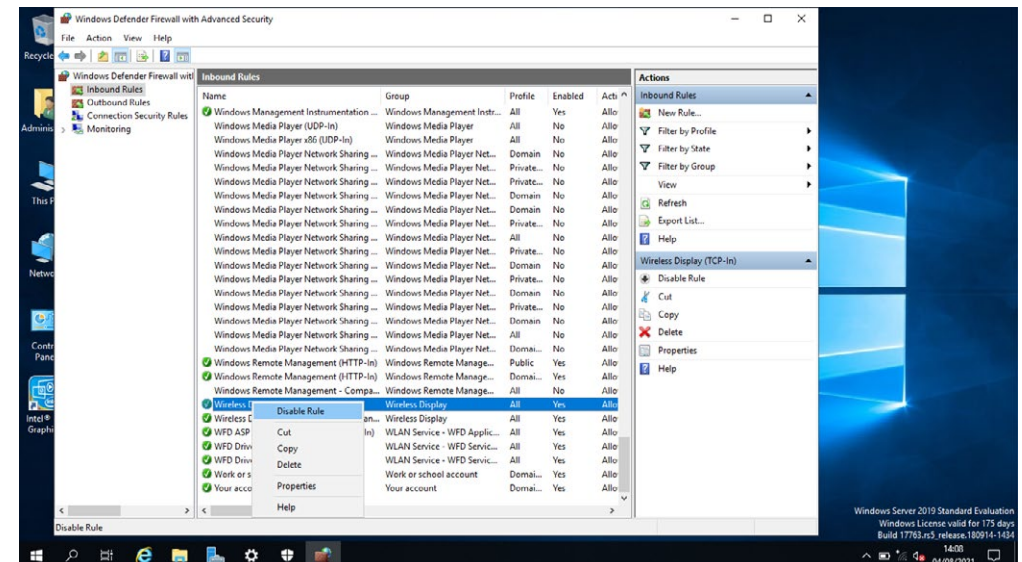
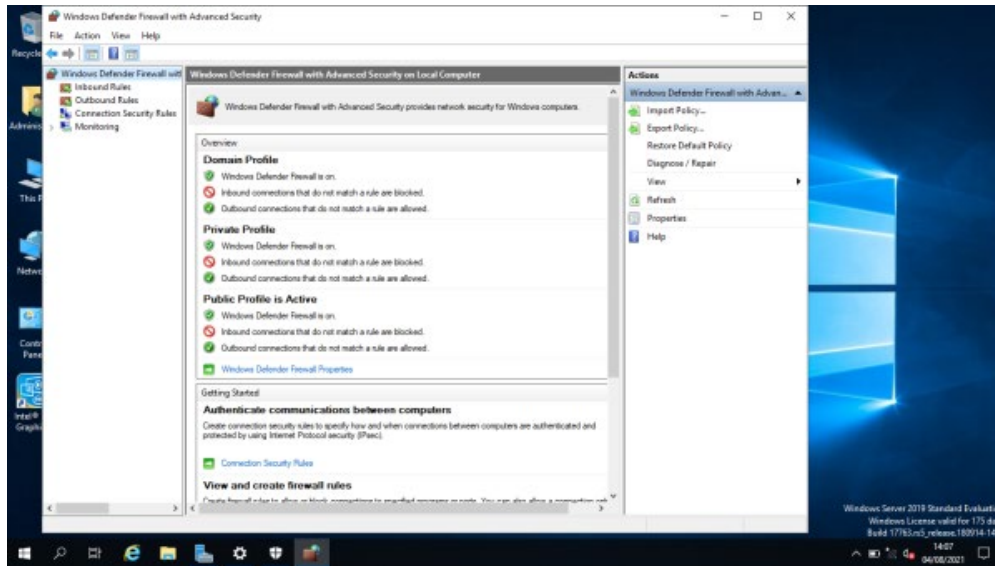
-  Change notification settings
-  Turn Windows Defender Firewall on or off
-  Restore defaults
-  **Advanced settings**

Troubleshoot my network

Move back to the Windows Defender Firewall settings and on the left-hand side select **Advanced settings** to see initially the same information about the firewall status but it also allows access to the rules set up within the firewall.

On the left-hand side if you select **Inbound Rules**, you will be presented with a long list of rules, the green ticks next to the rule highlights the ones that have been enabled.

You can right click on them to select **disable rule** or **enable rule** to ensure it is no longer allowed or now allowed through the firewall.

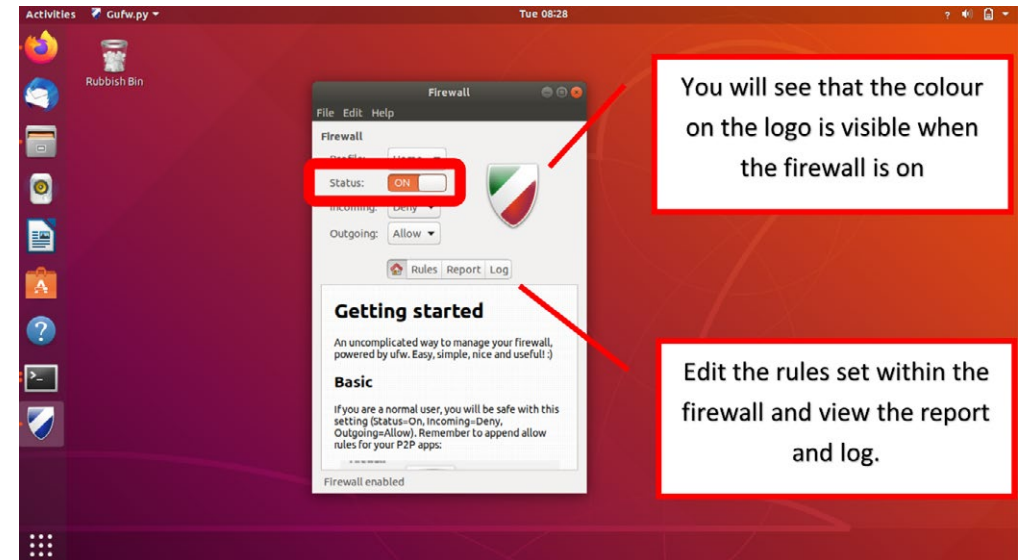
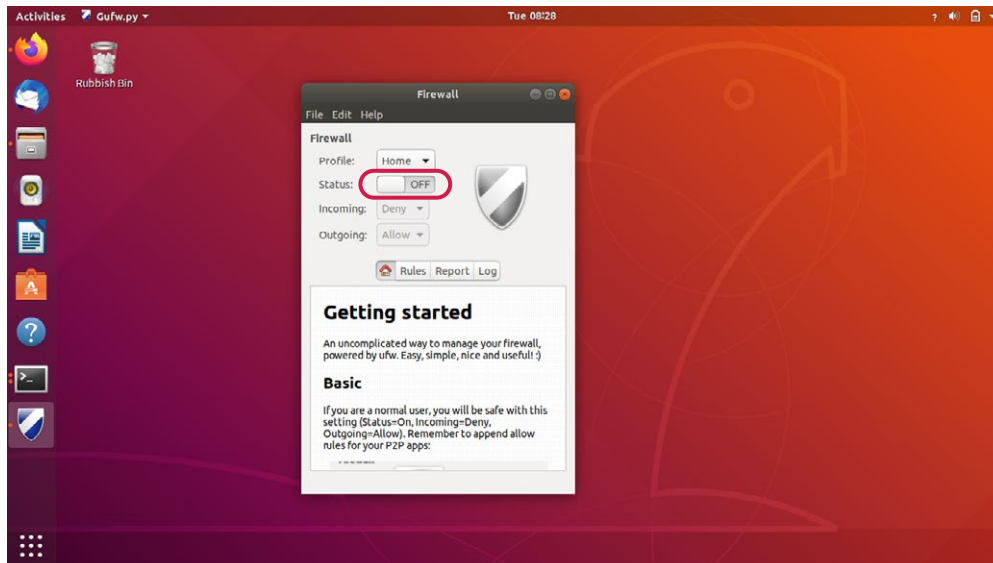


Ubuntu Firewall

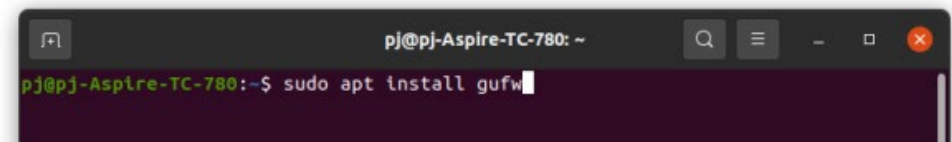
The default firewall on Ubuntu is UFW (Uncomplicated Firewall). Let's look at how to turn it on and off. You can access the firewall in two ways:

Option 1 is through the Graphical Uncomplicated Firewall (GUFW).

- If you search the programs for **Firewall**, you will open the GUFW.
- There is a toggle next to the heading **Status** and you can turn your firewall on and off.



If you can not locate the GUFW, you may need to install it first, open the terminal and add the command line `sudo apt install gufw`



You will be prompted to add the password and the process will be shown on the terminal for installing the software.

Remember using **sudo** is acting as an administrator so it will ask you for your password the first time you access.

```

pj@pj-Aspire-TC-780: ~
└─$ sudo apt install gufw
[sudo] password for pj:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed
  gufw
0 to upgrade, 1 to newly install, 0 to remove and 9 not to upgrade.
Need to get 860 kB of archives.
After this operation, 3,539 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu focal-updates/universe amd64 gufw all
20.04.1-1ubuntu1 [860 kB]
Fetched 860 kB in 0s (2,237 kB/s)
Selecting previously unselected package gufw.
(Reading database ... 186725 files and directories currently installed.)
Preparing to unpack .../gufw_20.04.1-1ubuntu1_all.deb ...
└─$
Progress: [ 20%] [#####.....]
    
```

```

pj@pj-Aspire-TC-780: ~
└─$ sudo ufw status
[sudo] password for pj:
Status: inactive
pj@pj-Aspire-TC-780: ~$
    
```

To enable the firewall, use the command:
sudo ufw enable

```

pj@pj-Aspire-TC-780: ~
└─$ sudo ufw status
[sudo] password for pj:
Status: inactive
pj@pj-Aspire-TC-780: ~$ sudo ufw enable
Firewall is active and enabled on system startup
pj@pj-Aspire-TC-780: ~$
    
```

Option 2 is through the **terminal**.

Open the terminal and add the following command to check the status of the firewall:
sudo ufw status

To **disable** the firewall, use the command:
`sudo ufw disable`

```
pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ sudo ufw status
[sudo] password for pj:
Status: inactive
pj@pj-Aspire-TC-780:~$ sudo ufw enable
Firewall is active and enabled on system startup
pj@pj-Aspire-TC-780:~$ sudo ufw disable
Firewall stopped and disabled on system startup
pj@pj-Aspire-TC-780:~$
```

Use the command to check the status of the firewall to see it is now **active**.

Ubuntu: How to alter the firewall settings

In Ubuntu you can edit the settings to open and close specific ports within the firewall settings. For a full list of ports please [click here](#).

An example would be to open port #80 and #443

- Port 80 = HTTP Protocol
- Port 443 = HTTPS Protocol

There are two ways to open these ports:

Option 1

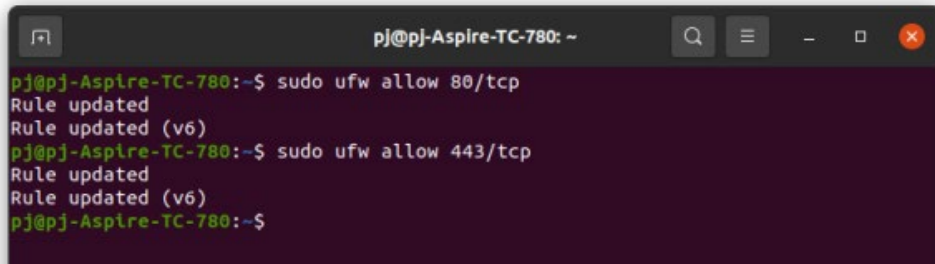
```
sudo ufw allow http
sudo ufw allow https
```

```
pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ sudo ufw enable
Firewall is active and enabled on system startup
pj@pj-Aspire-TC-780:~$ sudo ufw allow http
Rule added
Rule added (v6)
pj@pj-Aspire-TC-780:~$ sudo ufw allow https
Rule added
Rule added (v6)
pj@pj-Aspire-TC-780:~$
```

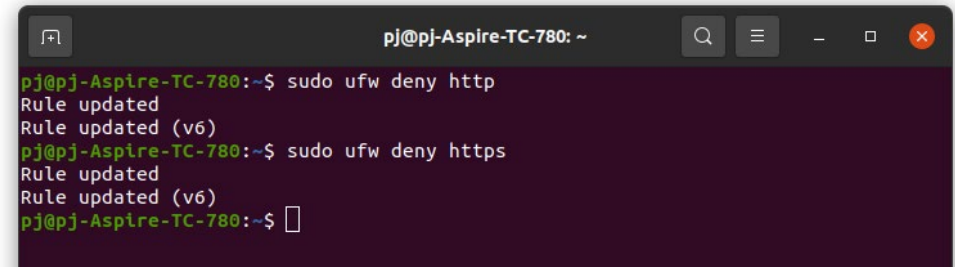
Option 2

```
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
```

To close the ports, you replace **allow** with **deny**



```
pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ sudo ufw allow 80/tcp
Rule updated
Rule updated (v6)
pj@pj-Aspire-TC-780:~$ sudo ufw allow 443/tcp
Rule updated
Rule updated (v6)
pj@pj-Aspire-TC-780:~$
```



```
pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ sudo ufw deny http
Rule updated
Rule updated (v6)
pj@pj-Aspire-TC-780:~$ sudo ufw deny https
Rule updated
Rule updated (v6)
pj@pj-Aspire-TC-780:~$
```



```
pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ sudo ufw allow 80/tcp
Rule updated
Rule updated (v6)
pj@pj-Aspire-TC-780:~$ sudo ufw allow 443/tcp
Rule updated
Rule updated (v6)
pj@pj-Aspire-TC-780:~$ sudo ufw deny 80/tcp
Rule updated
Rule updated (v6)
pj@pj-Aspire-TC-780:~$ sudo ufw deny 443/tcp
Rule updated
Rule updated (v6)
pj@pj-Aspire-TC-780:~$
```

Passwords

What makes a good password?

A good password is defined as a mixture of upper- and lower-case letters, numbers, and symbols. It also needs to be not easy to guess and preferably over 8 characters long.

For example, if you are trying to guess the password of a user. The first passwords you may try are combinations of children's names and their birthdates or the user's birthdate.

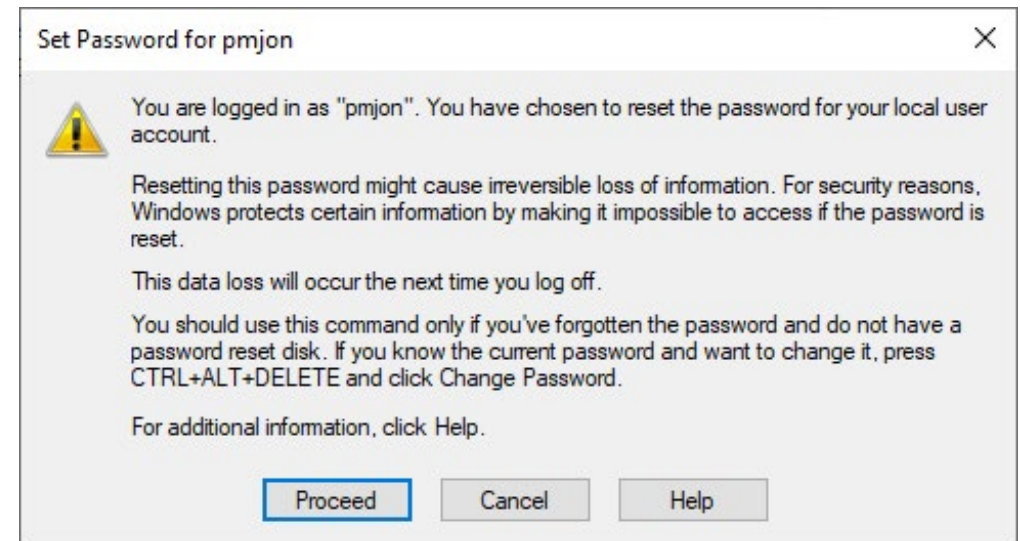
Look at this [link](#) to see how a system algorithm is used to determine if a password is strong enough.

Windows - Reset a user's password

Type in **Computer Management** in the program search area and on the left-hand side open the following dropdown menus:

- Local users and groups
- Users

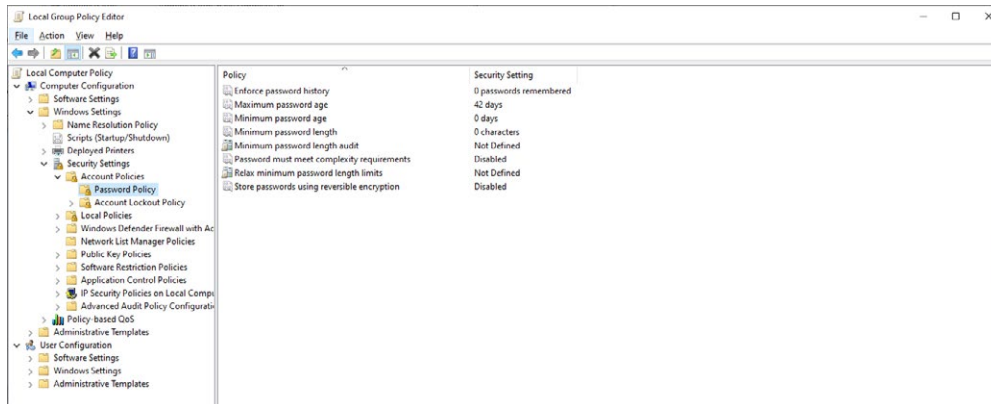
Right click on a user and select **Set password** and you will see the below pop up to check you are sure you want to set a password for a user. Click **Proceed** and follow the steps to set a password.



Windows – enforcing and editing a password policy

Type in **Local Group Policy Editor** in the program search area and on the left-hand side open the following dropdown menus:

- Windows Settings
- Security Settings
- Account Policies
- Password Policy



Double click on any of the rows to access and edit the settings for enforcing and editing the password policy for the users.

| Policy | Security Setting |
|---|------------------------|
| Enforce password history | 0 passwords remembered |
| Maximum password age | 42 days |
| Minimum password age | 0 days |
| Minimum password length | 0 characters |
| Minimum password length audit | Not Defined |
| Password must meet complexity requirements | Disabled |
| Relax minimum password length limits | Not Defined |
| Store passwords using reversible encryption | Disabled |

For example – on the example above, the password minimum length is not set and could be edited to a minimum of 8 characters to ensure a stronger password is used. Can you see any other settings that could be changed to ensure a strong password is added?

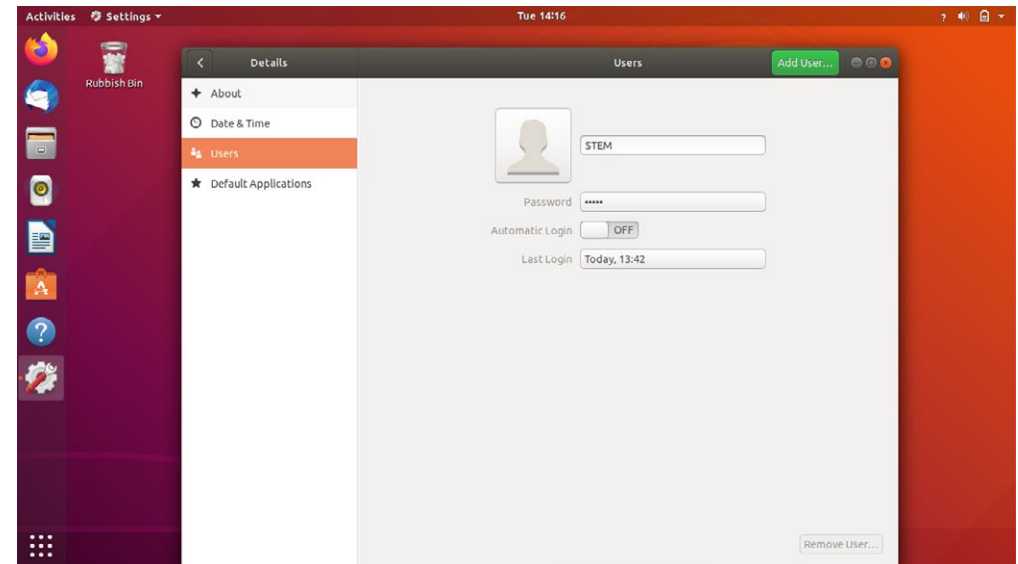
Ubuntu - Reset a user's password

Open the settings application and locate users on the left-hand options to view the current users available within the system.

You will be able to do the following within this area:

- Change the user's password
- Remove the user
- Add a new user
- View a user's account activity log – when they have logged in to the system
- Set a user to automatically login without a password
 - ** More details on adding and removing users can be found in the Windows & Ubuntu Advanced Cyber Security resources.

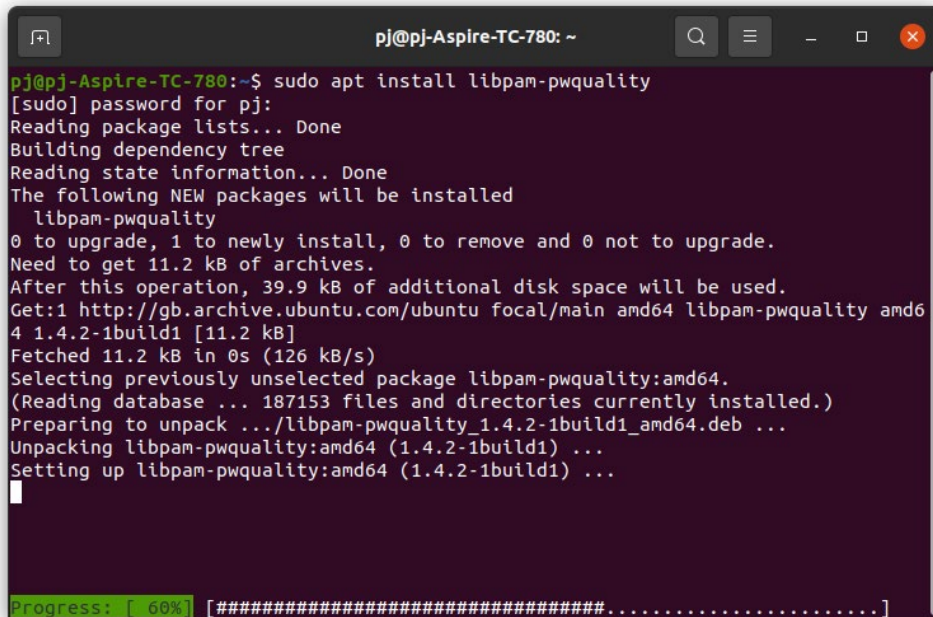
Double click on any of the rows to access and edit the settings for enforcing and editing the password policy for the users.



Ubuntu - Enforcing and editing a password policy

The first task is to ensure you have the correct application to allow you to enforce the password policy. To install the application, you need to open the terminal and use the command line:

```
sudo apt install libpam-pwquality
```



```
pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ sudo apt install libpam-pwquality
[sudo] password for pj:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed
  libpam-pwquality
0 to upgrade, 1 to newly install, 0 to remove and 0 not to upgrade.
Need to get 11.2 kB of archives.
After this operation, 39.9 kB of additional disk space will be used.
Get:1 http://gb.archive.ubuntu.com/ubuntu focal/main amd64 libpam-pwquality amd6
4 1.4.2-1build1 [11.2 kB]
Fetched 11.2 kB in 0s (126 kB/s)
Selecting previously unselected package libpam-pwquality:amd64.
(Reading database ... 187153 files and directories currently installed.)
Preparing to unpack ../libpam-pwquality_1.4.2-1build1_amd64.deb ...
Unpacking libpam-pwquality:amd64 (1.4.2-1build1) ...
Setting up libpam-pwquality:amd64 (1.4.2-1build1) ...

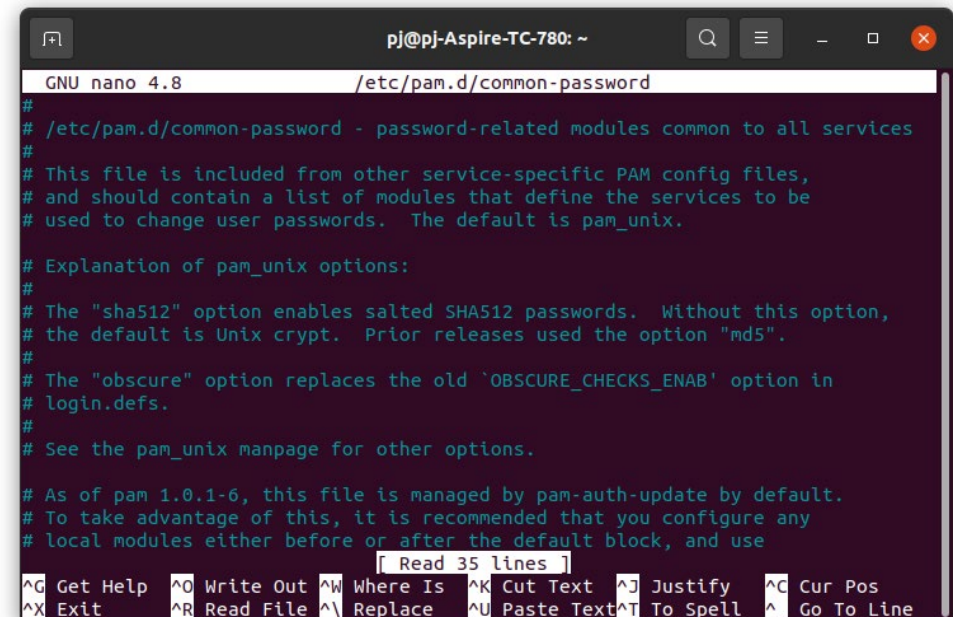
Progress: [ 60%] [#####.....]
```

Once installed you need to create a backup of the password quality file and add the following command line in the terminal:

```
sudo cp /etc/pam.d/common-password /etc/pam.d/
common-password.backup
```

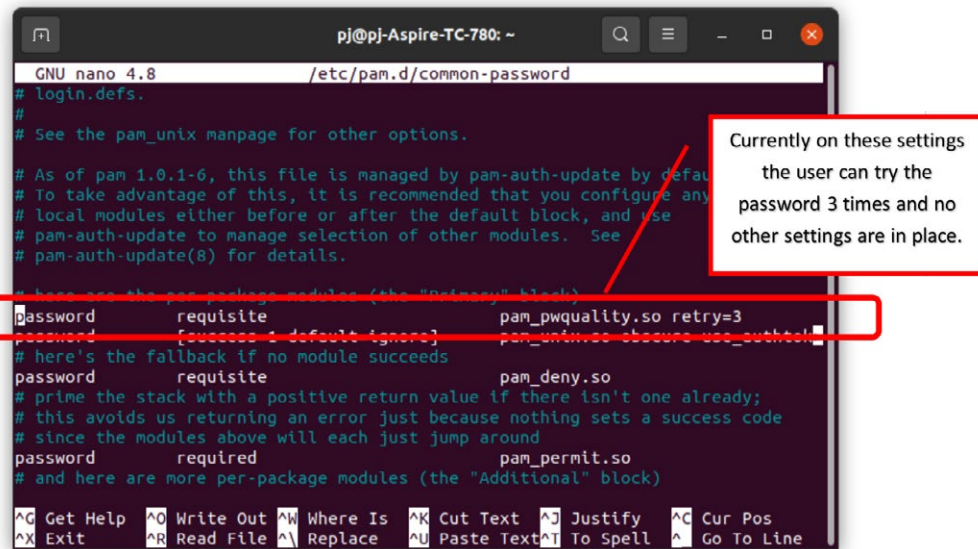
You can now access and edit the password enforcement policy by typing the following command to see the current settings:

```
sudo nano /etc/pam.d/common-password
```



```
GNU nano 4.8 /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
[ Read 35 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

Use your arrows to move down the terminal window and locate the section of the displayed code with **password**, **requisite** and the parameters set for the password policy.



```

GNU nano 4.8 /etc/pam.d/common-password
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Default" block)
password requisite pam_pwquality.so retry=3
password [success=1 default=ignore] pam_unix.so obscure use_authtok
# here's the fallback if no module succeeds
password requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)

```

You can navigate to the line in question with the arrows and directly type into the line any of the following to help strengthen the password policy.

| Parameter | Description |
|-------------------------|--|
| retry | No. of consecutive times a user can enter an incorrect password. |
| minlen | Minimum length of password |
| difok | No. of character that can be similar to the old password |
| lcredit | Min No. of lowercase letters |
| ucredit | Min No. of uppercase letters |
| dcredit | Min No. of digits |
| ocredit | Min No. of symbols |
| reject_username | Rejects the password containing the username |
| enforce_for_root | Also enforce the policy for the root user |

After any changes have been made to the password policy, you will need to reboot the system to apply them. To do this use the command line:

`sudo reboot`

Adding & removing a program on Windows & Ubuntu

It is important to add and remove programs safely on which ever device or operating system you are using as a program installed that you do not know, could contain malicious malware.

Cyber Security fact:

Most common passwords found during research from the NCSC (National Cyber Security Centre) with the number of times used too, showing the top passwords used and easiest to hack.

| Most used in total | Names | Premier League football teams | Musicians | Fictional characters |
|--------------------|-------------------|-------------------------------|---------------------|----------------------|
| 123456 (23.2m) | ashley (432,276) | liverpool (280,723) | blink182 (285,706) | superman (333,139) |
| 123456789 (7.7m) | michael (425,291) | chelsea (216,677) | 50cent (191,153) | naruto (242,749) |
| qwerty (3.8m) | daniel (368,227) | arsenal (179,095) | eminem (167,983) | tigger (237,290) |
| password (3.6m) | jessica (324,125) | manutd (59,440) | metallica (140,841) | pokemon (228,947) |
| 11111 (3.1m) | charlie (308,939) | everton (46,619) | slipknot (140,833) | batman (203,116) |

Cyber Security fact:

Derived from 'malicious software', malware includes viruses, trojans, worms or any code or content that can damage computer systems, networks, or devices.

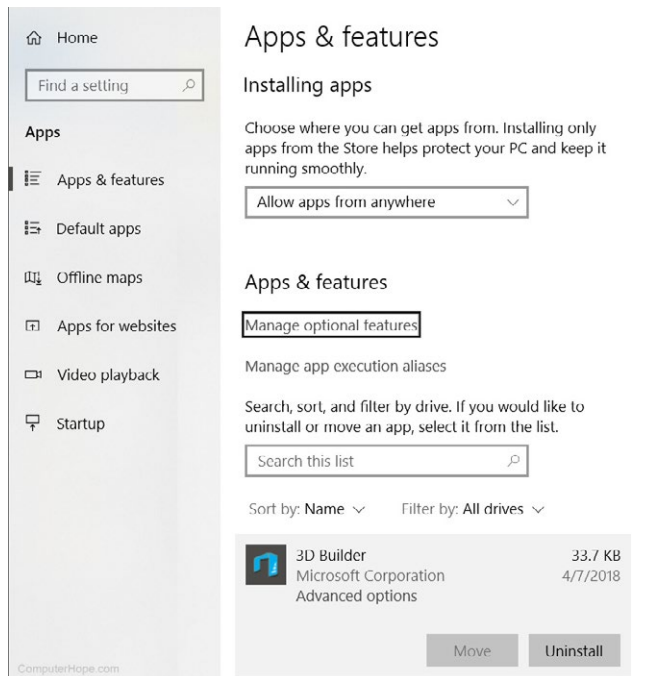
<https://www.ncsc.gov.uk/>

Good management of software is essential to keep a device safe from malware and ransomware. This can be through updating versions of software to ensuring software is safe when installing from reputable sources only.

Windows

Type in **Apps and Features** in the program search area and you can manage how windows installs programs as well as uninstall them.

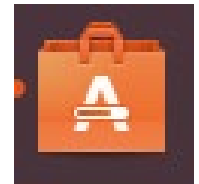
When you open this area, you will be presented with a long list of applications and features that you can edit or uninstall. Always check you do not need an application before removing it.



To install a program on Windows you can download an executable (.exe) file from a website if you know it is a safe and secure location to get it from. Or you can access the **Microsoft Store** to look at a range of applications, both paid for and free, that can be added to your device.

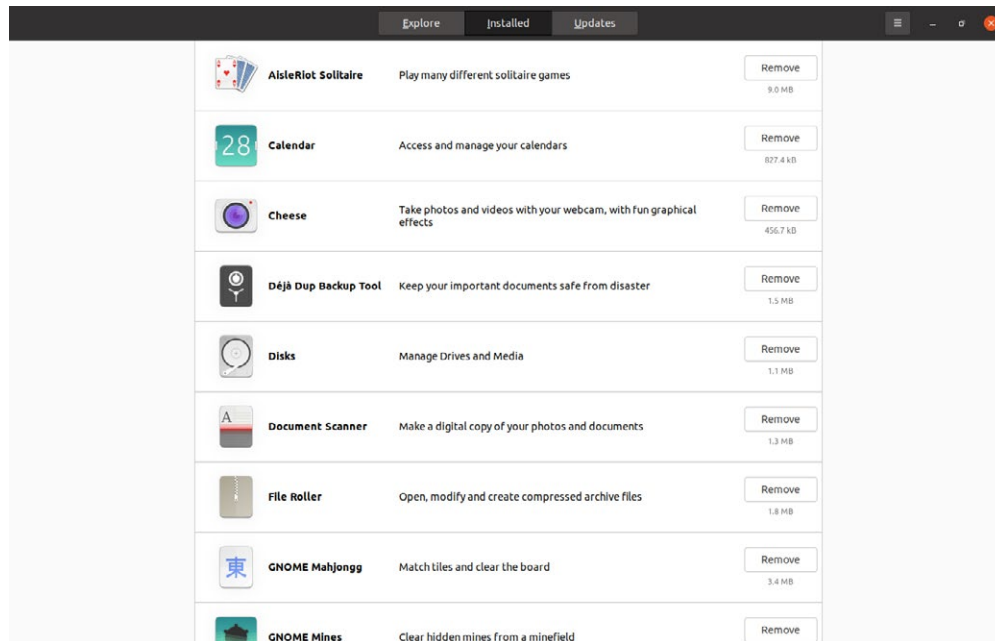
Ubuntu

To view the applications that are installed on the device you can click on the **Activities** icon on the dock.



You will open as default the explore area to see possible applications to install. On the top navigation bar select **installed**.

You will then see a list of applications that are installed on the device and be able to remove them from this location to by clicking the **remove** button against the application.



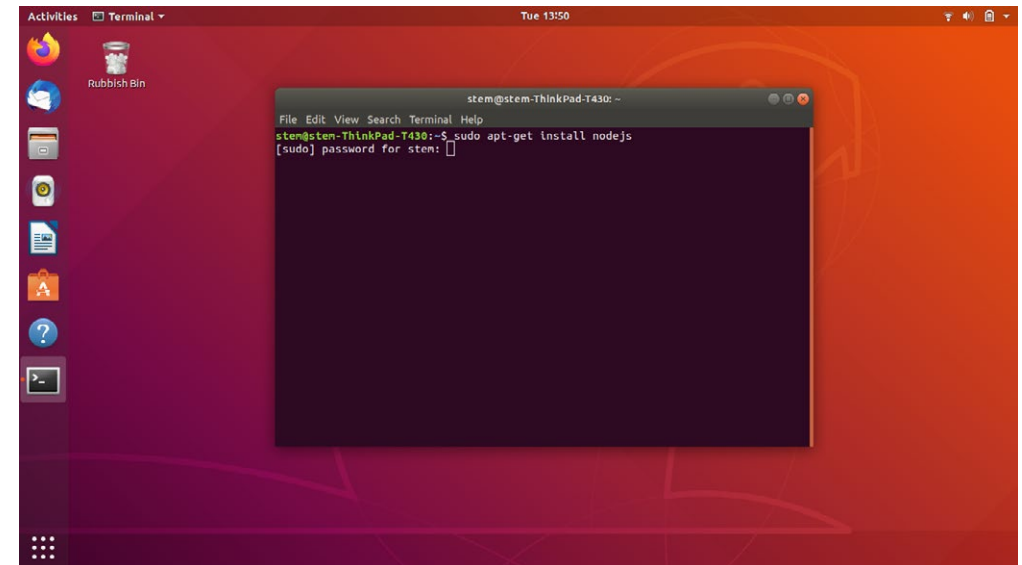
We have looked at installing a program briefly in other areas for example installing the GFW (Graphical Uncomplicated Firewall), and the process is similar for all installations.

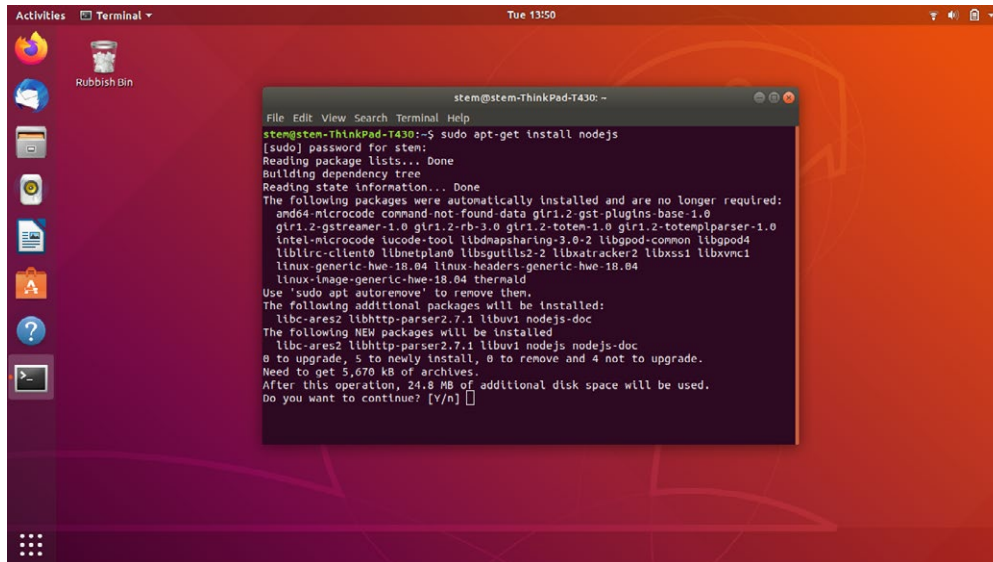
Open the **Terminal** and to install a new program to need to work as administrator so need to start with **sudo**.

We want to install Node.js so need to use the command line:

```
sudo apt-get install nodejs
```

The main part of the command line to remember is using **sudo apt** and **install**.





System Updates

When an operating system is installed on a device, as well as applications, it is a version of it that is installed. As new features are developed or new fixes put in place to combat vulnerabilities or bugs that have been found, the system requires an update to allow these changes to be implemented on your device.

The updates that are released are sent from manufacturers or developers and will continue to do so until the company decides the system is no longer supported.

For security these updates may also contain **security patches** and **new security features**. It is essential to have these updates on your system to allow your device to continue to be safe against new identified threats.

A **security patch** is developed once a known flaw has been identified that could be used in an attack on the system or device. Ensuring all new **security features** are also updated, makes it harder for an attack to succeed.

It is important to keep the following up to date:

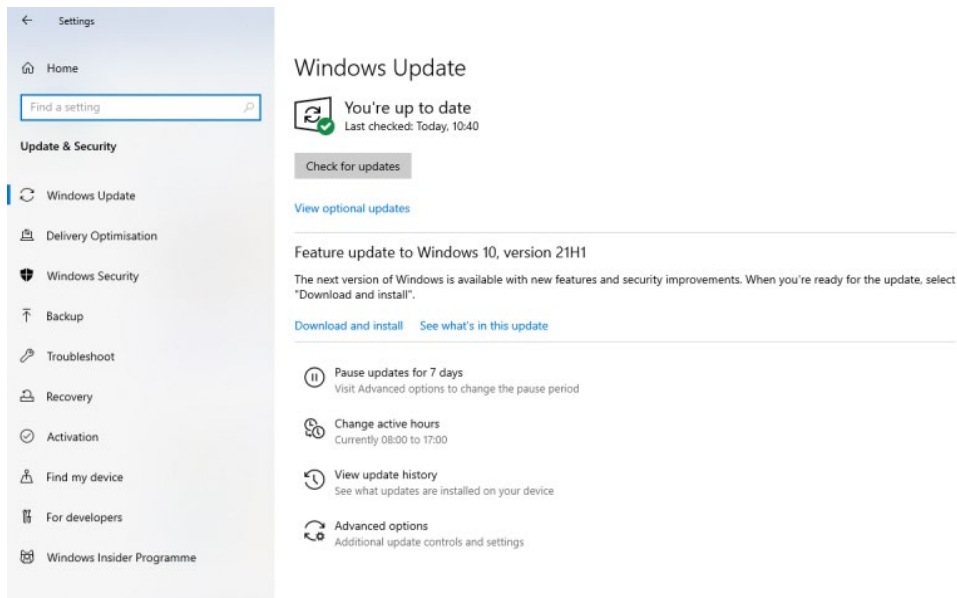
- Operating system
- Web browsers and extensions
- Any software or apps you download and install yourself
- Anti-virus software

If you do not update your systems, you are open to attack from outside the system and place your device at risk.

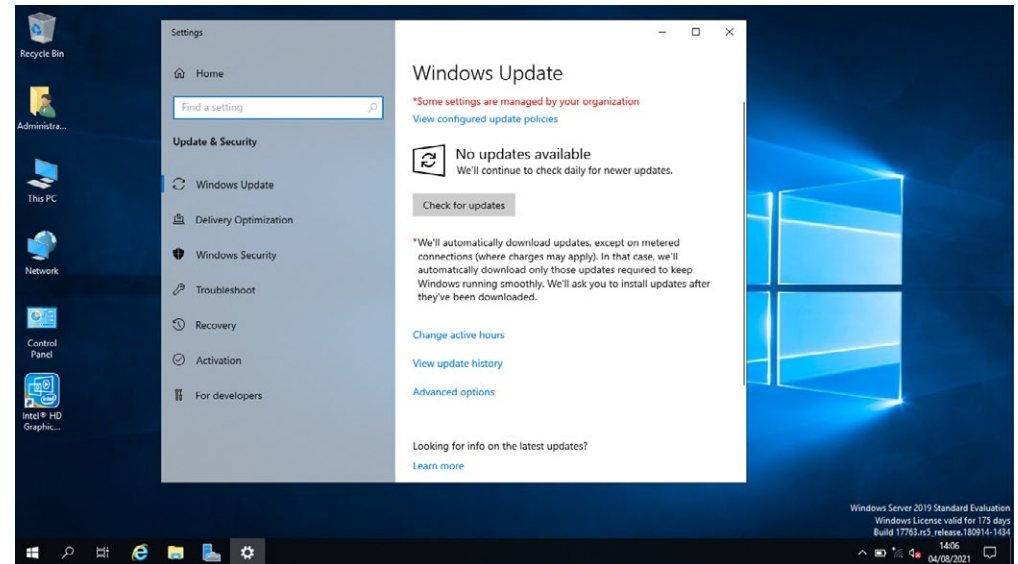
How to update Windows

To update Windows, open Settings and then select **Update and Security**.

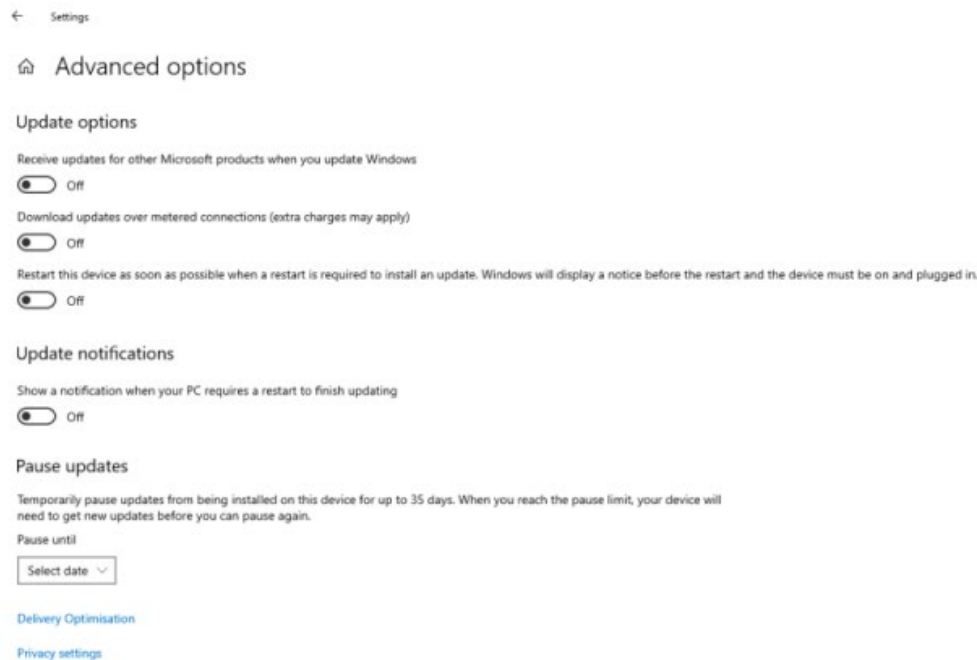
You will then see the view below of **Windows Update**. As you can see Windows is up to date but there is a feature update available that can be downloaded. It is important to check this and ensure all updates are actioned.



You may open yours and see a slightly different view, but in both cases, you can click the button **check for updates** and follow the guidance for any updates that need to be made.



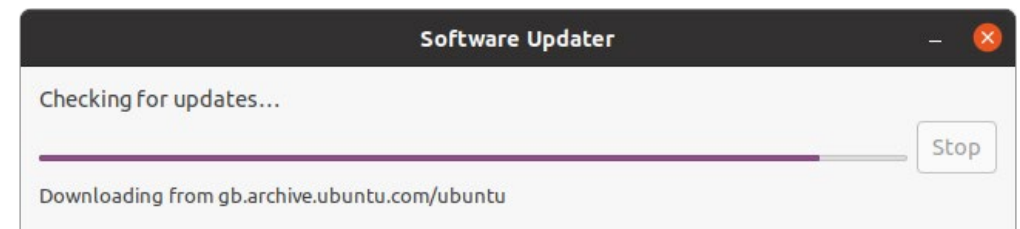
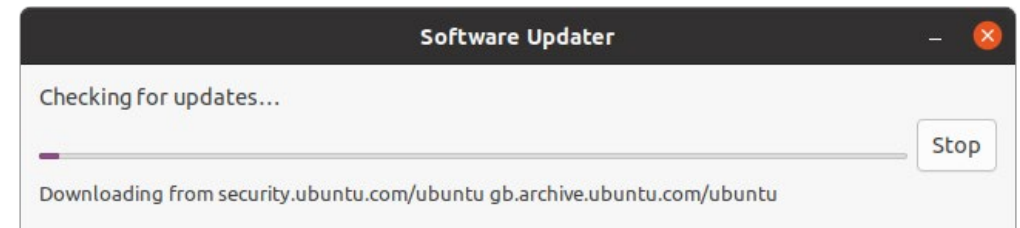
Within the **Windows Update** view, select **Advanced Options**. This will allow you to enforce updates to automatically take place as well as automatically restart to install an update and receive notifications.



How to update Ubuntu

Launch the **Software Updater**, this can be done by opening the APP drawer and searching for it.

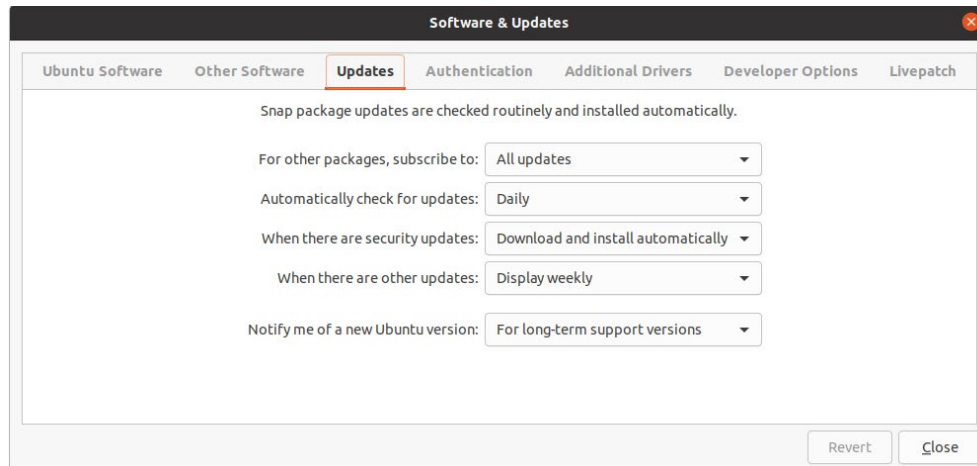
The software updater will automatically run at this point and download any updates.



Once it has completed the update it will display that all is now up to date. You can exit at this point by clicking **OK** or you can select **Settings & Livepatch** button to view and edit the settings for updates.

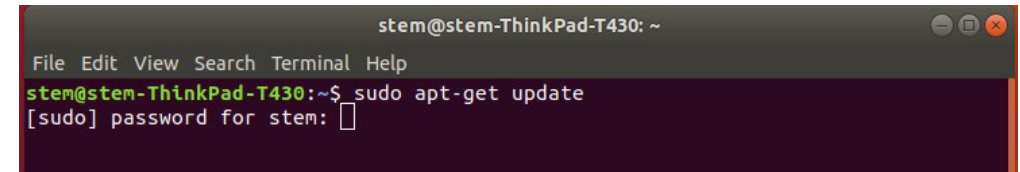


Within the updates section you can set specific settings for how and when updates take place.

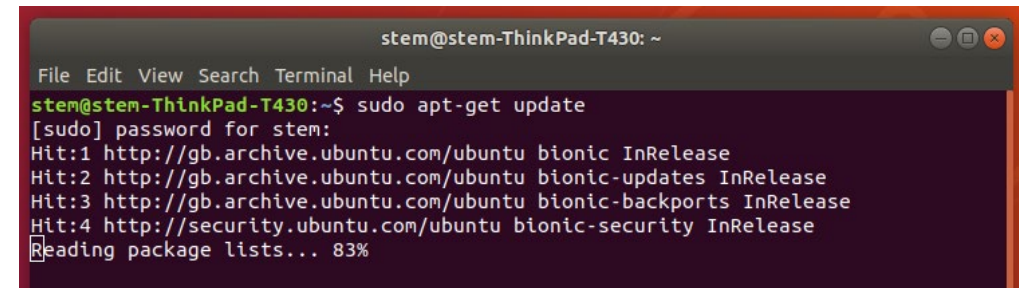


You can also do this through the terminal with the following command line:

`sudo apt-get update`



You will be prompted for the password and then the updates will be displayed and the progress within the terminal.



Anti-Virus

What is Anti-Virus Software?

The main purpose of anti-virus software is to identify potential threats in the system and prevent, detect, and remove them.

It is essential that the anti-virus software you use is up to date. The software has a database of known viruses/threats to look for, with more threats/viruses being developed, the anti-virus software must be told about them to be able to protect you from them.

To ensure your system is fully protected from all known threats/viruses, the anti-virus software needs to be up to date and running regular scans of the system to look for, detect and remove them.

Most new anti-virus software automatically runs updates but is always something to ensure is set up correctly.

Key points to remember:

1. When starting a new device for the first time, run a full scan.
2. Ensure the anti-virus software is set to receive updates automatically.
3. Ensure the anti-virus software is set to scan all new files e.g. downloaded files from the internet, USB drives, external drives etc.

Cyber Security fact:

Malicious software - known as malware - is code that can harm your computers and laptops, and the data on them. Your devices can become infected by inadvertently downloading malware that's in an attachment linked to a dubious email, or hidden on a USB drive, or even by simply visiting a dodgy website.

Once it's on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even erase it completely. For this reason, it's important that you always use antivirus software, and keep it up to date to protect your data and devices.

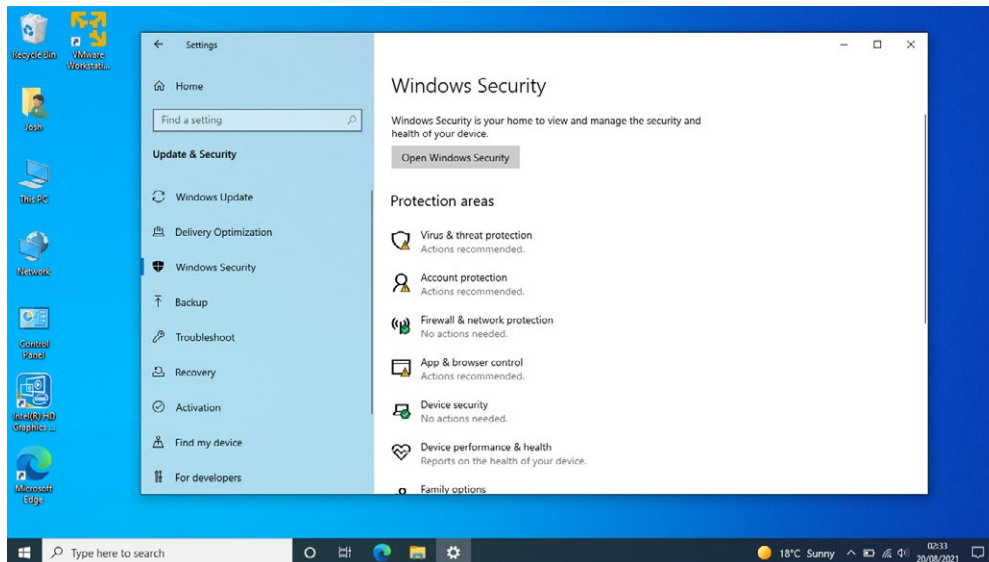
<https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product>

How to enable anti-virus on Windows

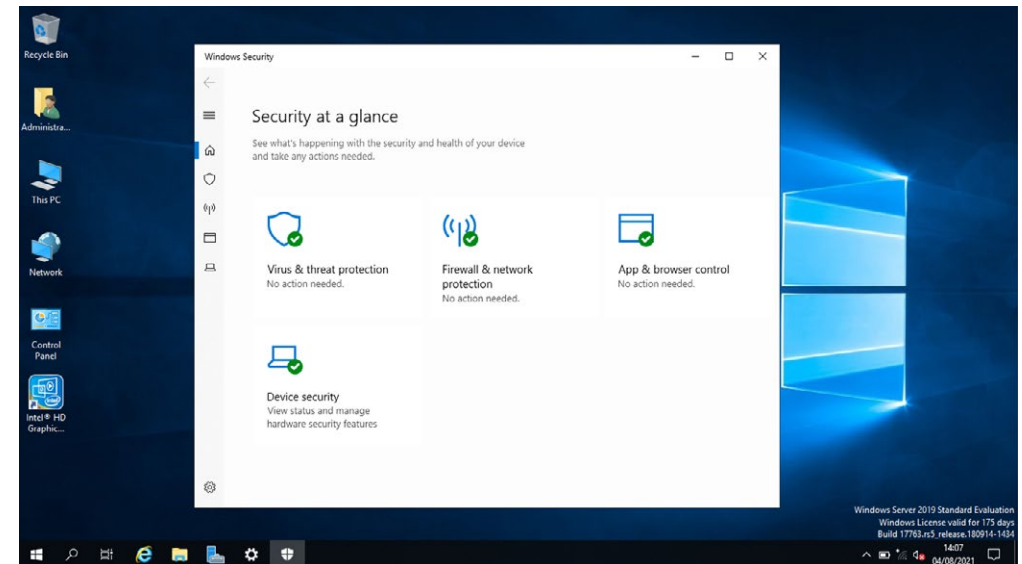
Windows has inbuilt anti-virus protection that needs to be switched on and updated to ensure protection for the device. There are other packages that a user can download and use as virus protection, but Windows Security is the default.

To view the status of your anti-virus on Windows you need to open the **Settings**, select **Update & Security**, select **Windows Security**.

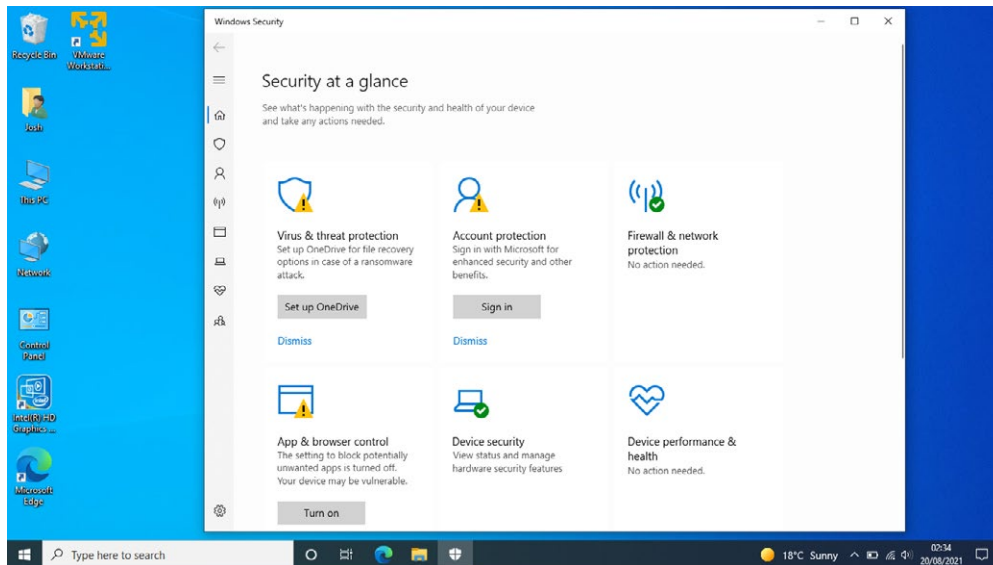
Select **Open Windows Security** to view actions required.



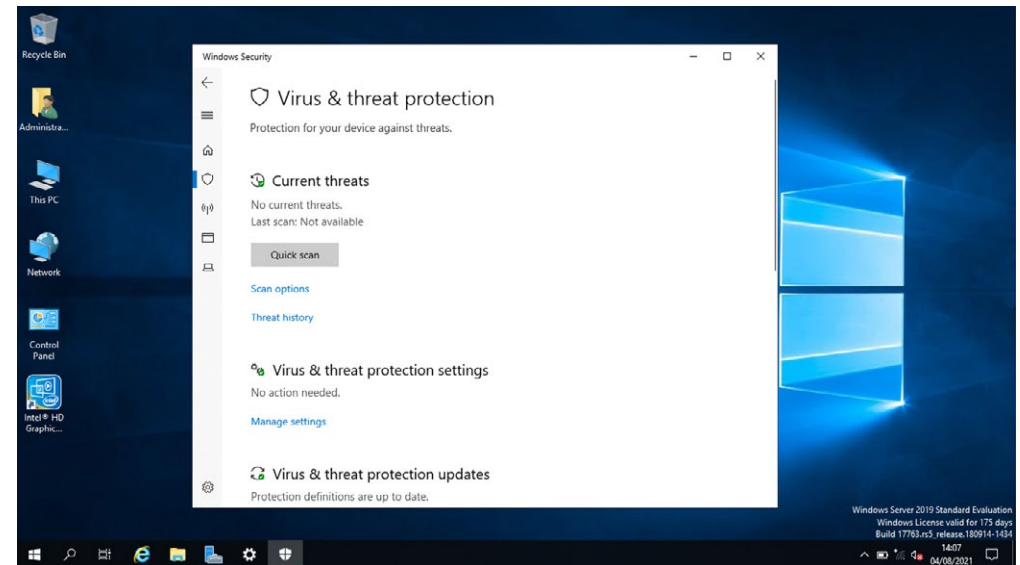
You will be able to see the status of the anti-virus software for security, this is what a protected system looks like, green ticks against each section.



If a system has actions to update or turn on elements, it will have a hazard symbol; a yellow triangle with an exclamation mark in the middle. It will also give advice of what needs to be done to rectify the issue or update.



Double click on the **Virus and threat protection** section, this allows you to run a scan, manage settings and check for updates.



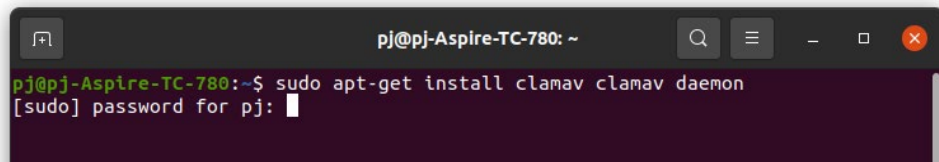
How to enable anti-virus on Ubuntu

Whereas Windows operating system has a built-in anti-virus software to help secure the device from the start, Ubuntu does not. Linux based devices are less likely to need anti-virus software as viruses are rare, they are not written to attack them.

However, if you are transferring files from Windows to Linux, or vice versa, you will need a software to scan for viruses.

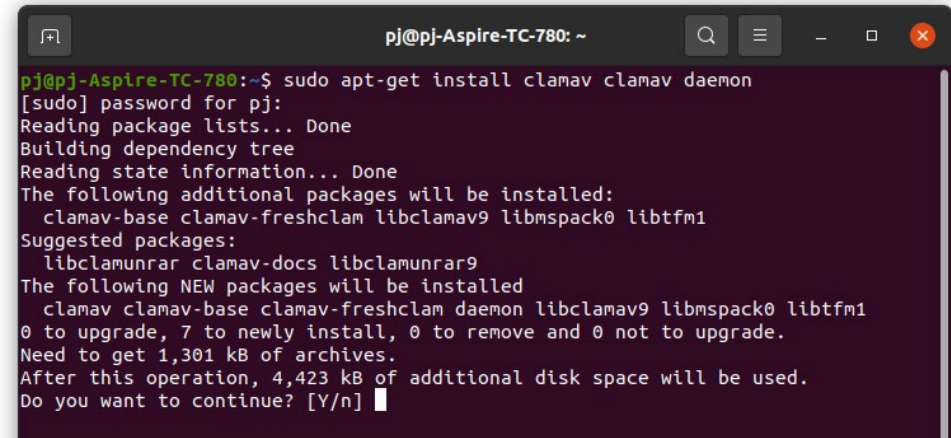
A popular open-source anti-virus software is **ClamAV**. Open the terminal and enter the command line:

```
sudo apt-get install clamav clamav-daemon
```



```
pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ sudo apt-get install clamav clamav-daemon
[sudo] password for pj:
```

The installation will ask for a Y/N answer regarding disk space being used, type Y and press enter.

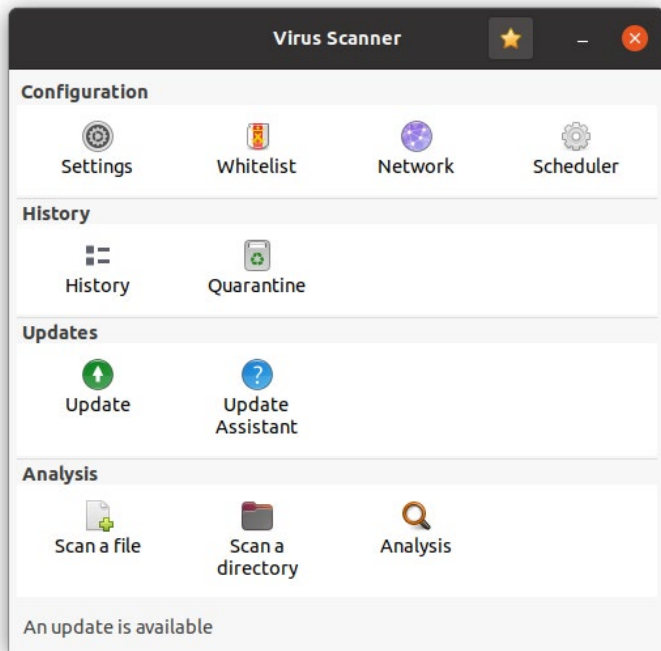


```
pj@pj-Aspire-TC-780: ~
pj@pj-Aspire-TC-780:~$ sudo apt-get install clamav clamav-daemon
[sudo] password for pj:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
 clamav-base clamav-freshclam libclamav9 libmspack0 libtftm1
Suggested packages:
 libclamunrar clamav-docs libclamunrar9
The following NEW packages will be installed
 clamav clamav-base clamav-freshclam daemon libclamav9 libmspack0 libtftm1
0 to upgrade, 7 to newly install, 0 to remove and 0 not to upgrade.
Need to get 1,301 kB of archives.
After this operation, 4,423 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

To install the graphical user interface for ClamAV use the following command line:

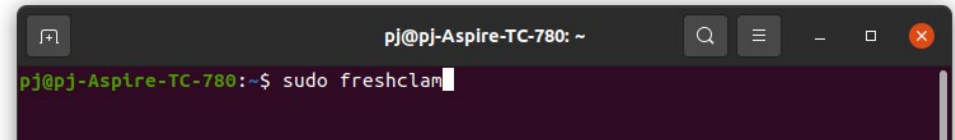
```
sudo apt install clamtk
```

You can now locate Clamtk in the APP Drawer, open the software and you can now check for updates and that they are happening automatically, run a scan and view the analysis.



Within the terminal you can update the virus database by using the command line:

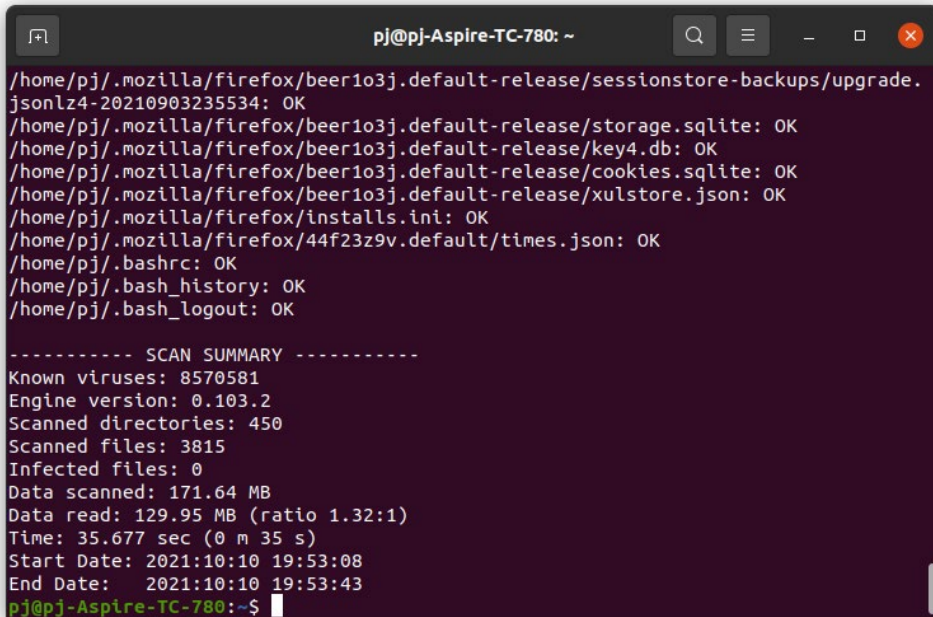
```
sudo freshclam
```



To run a scan on the home directory you can use the command line:

```
sudo clamscan -r /home
```

You will see the terminal fill as it runs through all the files and directories, leave until the scan has completed and you are presented with a scan summary. The scan summary will outline the number of files and directories scanned and any infected files.



```
pj@pj-Aspire-TC-780: ~
/home/pj/.mozilla/firefox/beer103j.default-release/sessionstore-backups/upgrade.
jsonlz4-20210903235534: OK
/home/pj/.mozilla/firefox/beer103j.default-release/storage.sqlite: OK
/home/pj/.mozilla/firefox/beer103j.default-release/key4.db: OK
/home/pj/.mozilla/firefox/beer103j.default-release/cookies.sqlite: OK
/home/pj/.mozilla/firefox/beer103j.default-release/xulstore.json: OK
/home/pj/.mozilla/firefox/installs.ini: OK
/home/pj/.mozilla/firefox/44f23z9v.default/times.json: OK
/home/pj/.bashrc: OK
/home/pj/.bash_history: OK
/home/pj/.bash_logout: OK

----- SCAN SUMMARY -----
Known viruses: 8570581
Engine version: 0.103.2
Scanned directories: 450
Scanned files: 3815
Infected files: 0
Data scanned: 171.64 MB
Data read: 129.95 MB (ratio 1.32:1)
Time: 35.677 sec (0 m 35 s)
Start Date: 2021:10:10 19:53:08
End Date: 2021:10:10 19:53:43
pj@pj-Aspire-TC-780:~$
```