Educate
Engage
Inspire

Presented by

In partnership with

Module 5

Microsoft Windows security tools

cybertaipan.csiro.au

Learning objectives

Participants will understand where basic Windows operating system security tools are located:

- *Control Panel and Windows Settings*
- *Administrative tools*
- *Security and maintenance*
- *Windows Defender security centre*
- *Windows Defender firewall*
- *Windows update*

Participants will learn how to manage Windows accounts and how accounts can affect security.

Section 1

Basic security policies and tools

Note on Windows security tools

Windows has several versions (Professional, Home, etc.)

Each version has sets of security tools with different looks, capabilities, and ways to access them.

This training unit has several options for accessing almost all the security tools to perform specific tasks.

In any case, the search capability in the Windows versions will assist users and administrators in finding the appropriate tool for a task.

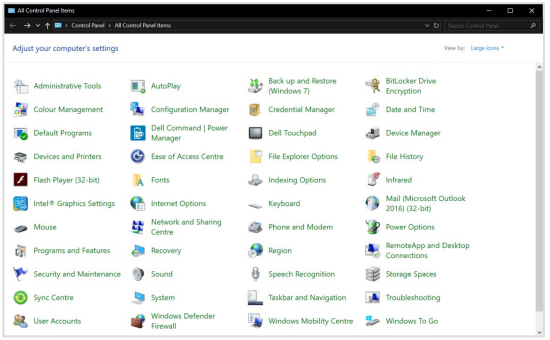
Security and administration tools

Windows has several components with groups of security and administration tools.

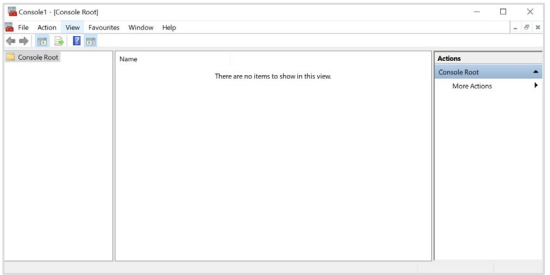
You must be an administrator to use most of the tools.

Some of the components are:

- *Windows Settings*
- *Control Panel*
- *Microsoft Management Console (MMC) for advanced settings*



Control Panel

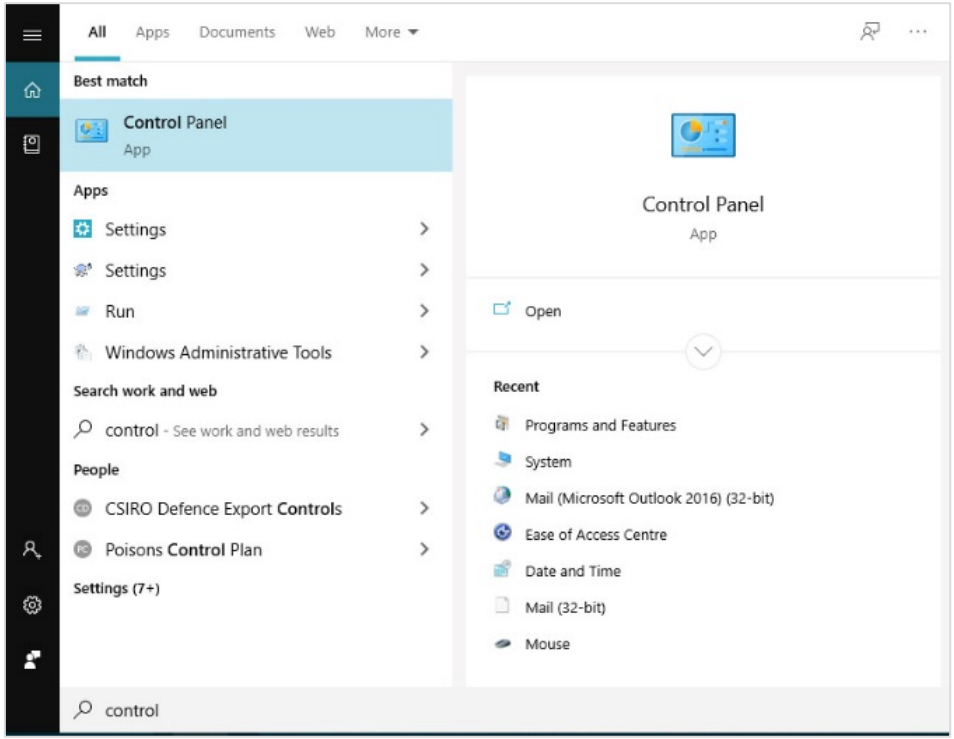


MMC

Windows search bar

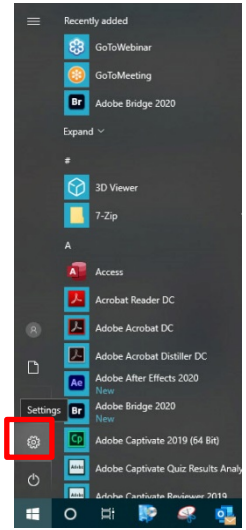
Windows 10 has a search bar that can bring up anything you need on your system.

You can use the search bar to find any of these upcoming areas if you don’t know the direct path.

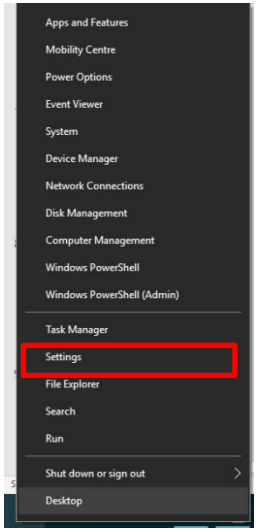


Windows Settings

Where many of the basic system changes and configurations can be set within a Windows 10 operating system is a little different depending on the version of the operating system.



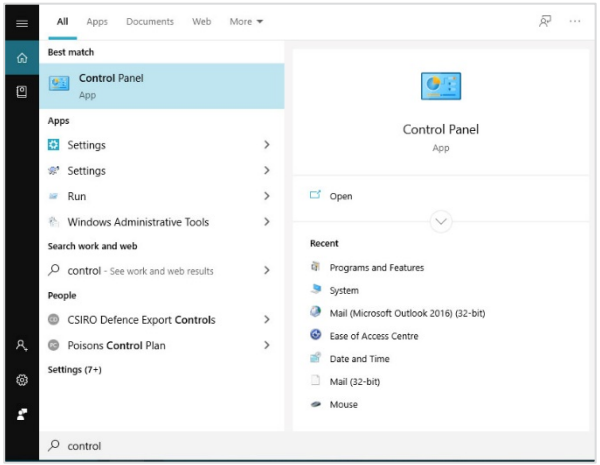
Click Start → Settings icon



OR Right Click Start → Settings

Control Panel and search

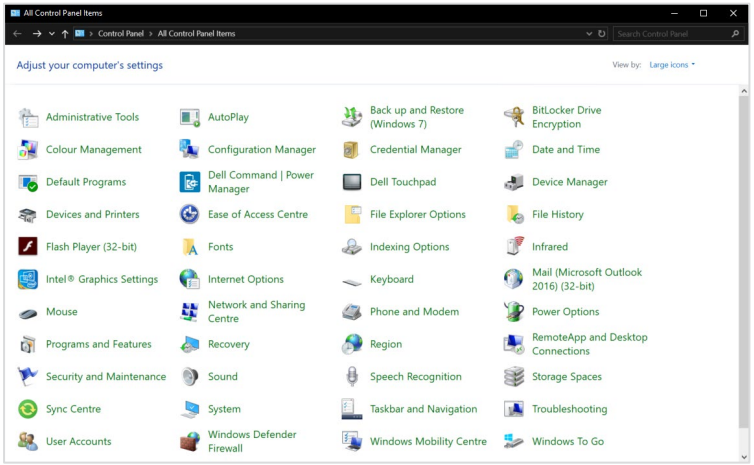
Control Panel resides in Windows 10 and is more robust than Settings. If you do not see it on your Start menu, you may search for it. Search may be used to find most configuration and security tools within Windows.



OR Click ‘Type here to search’

→ Type ‘Control Panel’

→ Click ‘Control Panel’

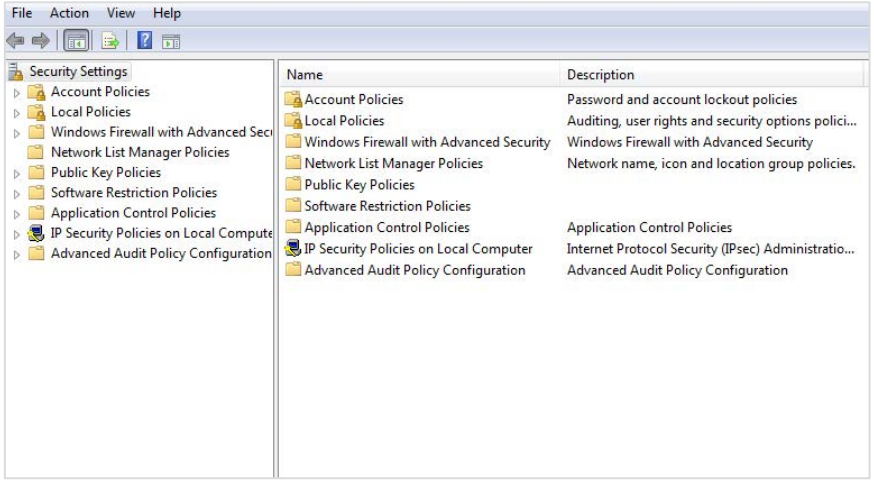


Basic local security policies

Controls security settings on user computers within a network.

Control Panel→ Administrative Tools → Local Security Policy

OR Search → Administrative Tools → Local Security Policy



Password policies

Modify policies to require users create strong passwords.

Remember CLOUDS Not SUN (Module Four)

In Administrative Tools: Click Account Policies → Password Policies

Policies	Recommended settings
Password history *The number of old passwords the computer remembers and does not allow a user to reuse.*	*90 days for users* *30 for admins*
Maximum password age *How long a user can keep the same password.*	*10 - 30 days*
Minimum password age *How long a user must keep a password before changing it.*	
Minimum password length *How many characters passwords must have.*	*10 characters*
Complexity requirements *Whether users must use at least three of the following in their passwords: upper case letters, lower case letters, numbers, symbols.*	*Enable*
Reversible encryption *Whether the password file on the computer can be decrypted.*	*Disable*

Account lockout policies

Even if you have the strongest password possible, if you give hackers unlimited attempts to break it, they eventually will.

Account policies govern unsuccessful attempts to log in to an account.

Click Account Policies → Account Lockout Policies

Policies	Recommended settings
Account lockout duration *The number of minutes an account remains locked before being automatically unlocked.*	*30 minutes*
Account lockout threshold *The number of failed logon attempts that causes a user account to be locked.*	*3-10 invalid log in attempts*
Reset account lockout counter after *The number of minutes that must elapse before the failed logon attempt threshold counter is reset to 0.*	*30 minutes*

Windows Defender security centre

Window Defender is an important defensive tool in Windows.

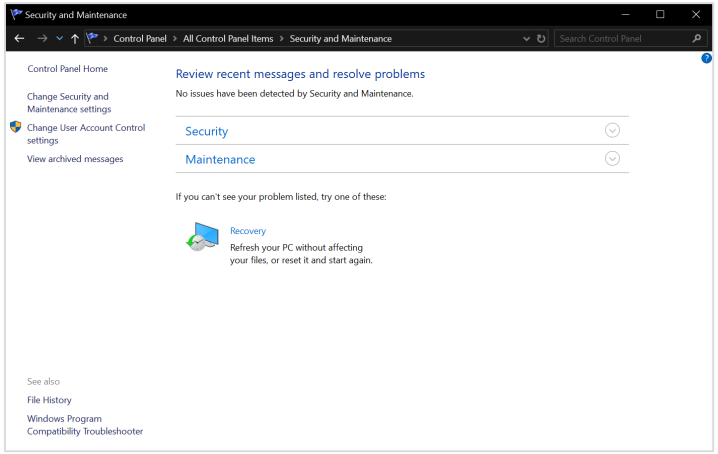
To open Windows Defender:

Click Start → Settings→ Windows Settings → Update & Security → Windows Security

OR Click Start → Control Panel→ System and Security → Security and Maintenance→ Security

Notifies you if Windows identifies problems with, or updates for:

- *Windows Updates*
- *Internet security settings*
- *Network firewall*
- *Spyware and related protections*
- *User Account Control*
- *Virus protections*
- *Windows Backups*



Windows Defender and Anti-Malware

Click Start → Settings→ Windows Settings → Update and Security → Windows Security

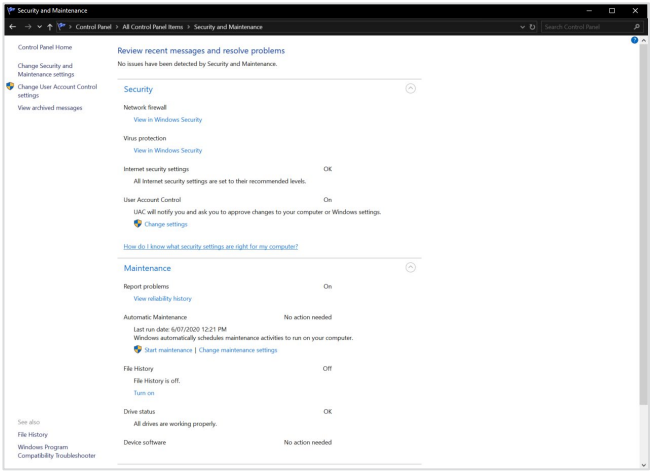
OR

Click Start → Control Panel→ System and Security → Security and Maintenance→ Security

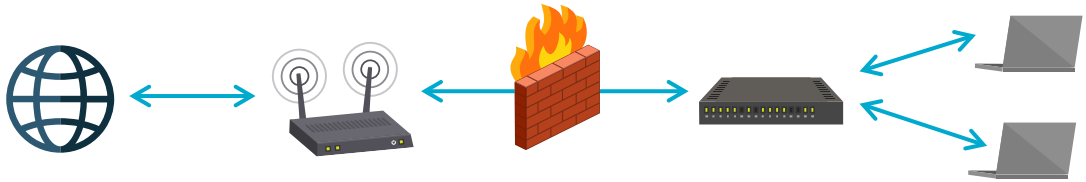
Anti-malware programs should be updated regularly.

Windows Defender is an anti-malware component of Microsoft Windows. You can download a supplementary anti-virus program.

- *Windows offers a free program called Windows Security Essentials.*
- *If you choose a different anti-malware program, disable Windows Defender first to avoid compatibility issues.*



Firewalls



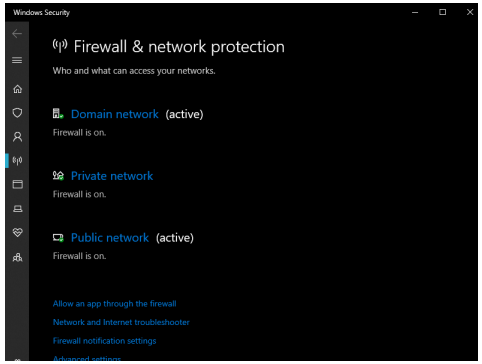
Reject or allow data packets through to users based on custom settings.

Essential to security and should always be turned ‘on’ and use ‘Recommended Settings’ at a minimum.

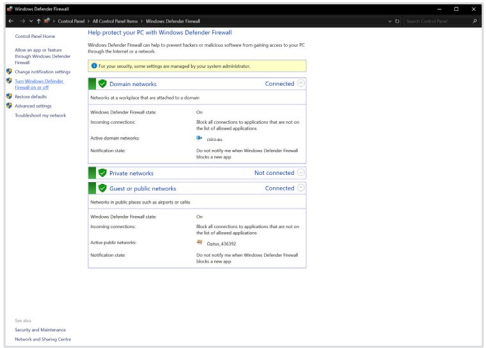
Click Start → Windows Settings→ Update and Security → Windows Security → Firewall & network protection

OR Right Click Start → Control Panel→ Windows (Defender) Firewall

OR Search → Firewall



Windows Security



Windows Defender Firewall

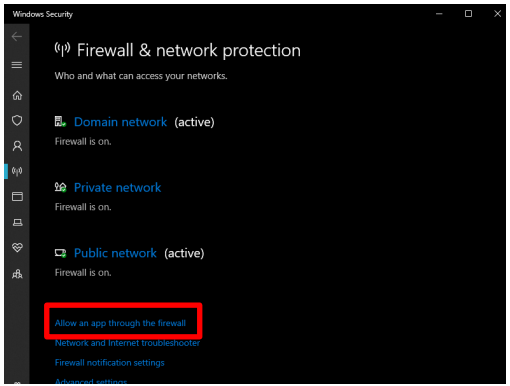
Note: Both firewall settings are for the same firewalls.

Enabling Windows Firewall exceptions

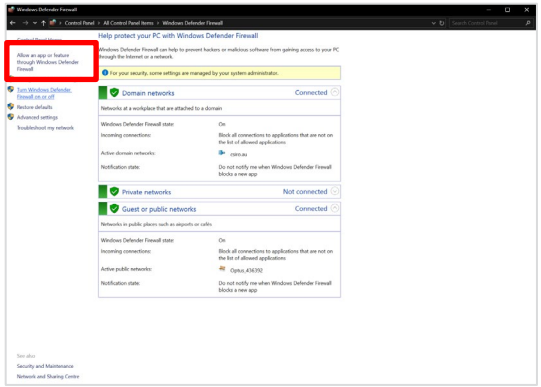
Allows trusted programs to connect without being blocked by adding them to your Windows Firewall Exceptions list.

For each network type, you can customise whether you want the programs allowed through.

Click Start → Windows Settings → Update and Security → Windows Security → Firewall & network protection
OR Control Panel → System and Security → Windows (Defender) Firewall



Windows Security



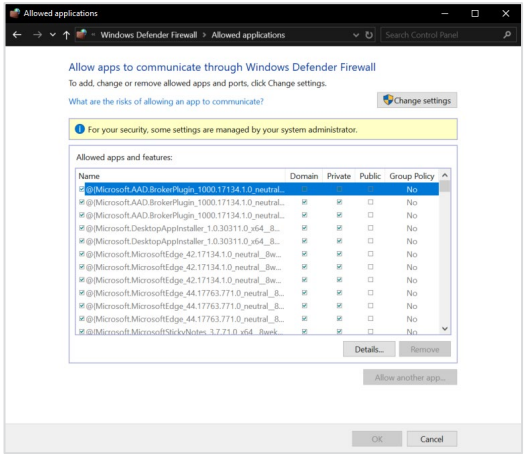
Windows Defender Firewall

Enabling Windows Firewall exceptions

For each network type, you can customise whether you want the programs allowed through.

It’s much safer to allow only certain programs through your firewall than to open an entire port to traffic.

Ports are numbers that identifies one side of a connection between two computers.



Common exceptions

Core networking

Regular Microsoft Windows services that retrieve data from the internet.
If you don't enable this exception across all three types of networks, some Microsoft services and programs will not run properly.

File and printer sharing

Allows you to share the contents of selected folders and locally attached printers with other computers.

Remote assistance

Allows a user to temporarily remotely control another Windows computer over a network or the internet to resolve issues.

Remote desktop

Allows users to access their user accounts and files remotely.

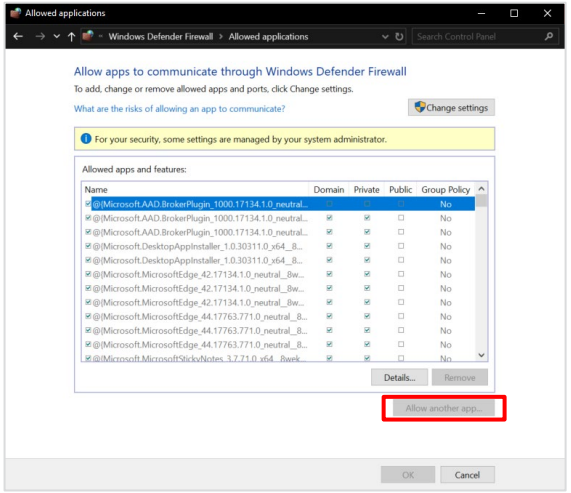
UPnP framework (Universal Plug-and-Play)

Allows devices to connect to and automatically establish working configurations with other devices on the same network.

Adding Windows Firewall exceptions

If the program you want to allow through your firewall does not already appear on your exceptions list, click the ‘Allow another program’ option and select the program from the menu.

You might have to click ‘Browse” and find the program yourself if it’s not listed.



Windows Update

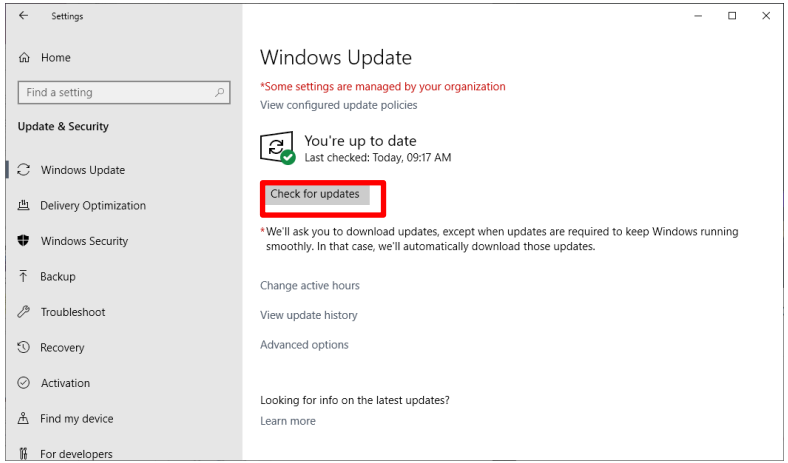
Prevent or fix known problems in Windows software or improve user experience.

Should be installed regularly.

To avoid missing updates, allow Windows Update to check for them daily and install them automatically.

Windows Settings → Updates and Security → Windows Security → Windows Update

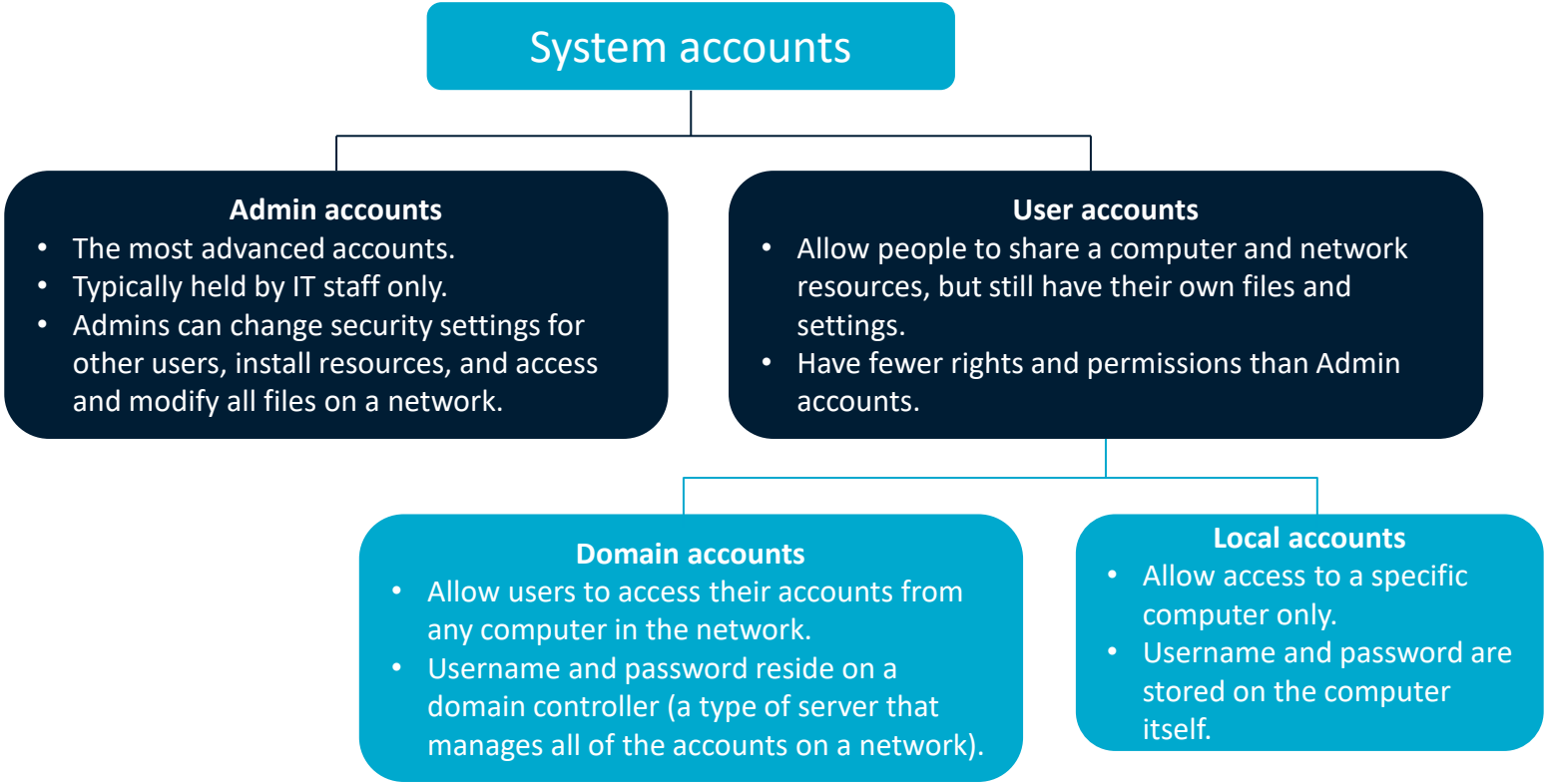
OR Search → Windows Update



Section 2

Account management

Account groups



Microsoft Management Console (MMC)

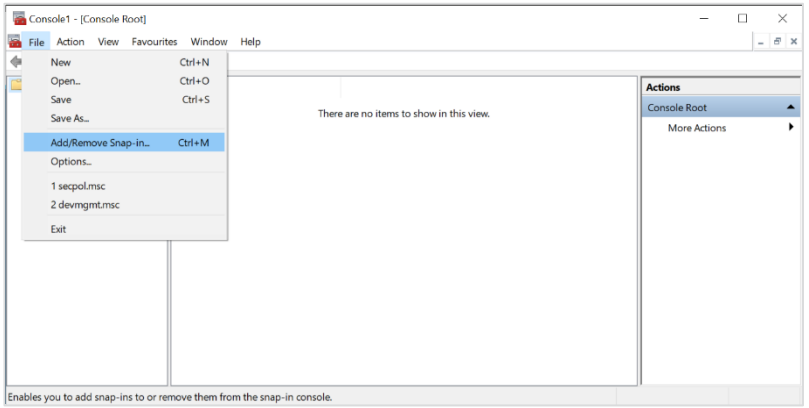
The Windows component that allows administrators to make group and detailed security settings is the Microsoft Management Console or MMC.

MMC can be found using Search. It cannot be accessed through Windows Settings or the Control Panel.

MMC allows settings to be made to user and group permissions.

Snap-ins are the tools the MMC accesses to make settings. Snap-ins must be opened in MMC. They do not automatically appear when MMC is executed.

To access MMC
Search → 'mmc' → Click 'Yes' to allow changes to computer
To access Snap-ins in MMC
Click File → Add/Remove Snap-ins



The following slides will show you how to control user access through Control Panel and through the Local Users and Groups Console. Other methods exist and you can choose which to use based on personal preference.

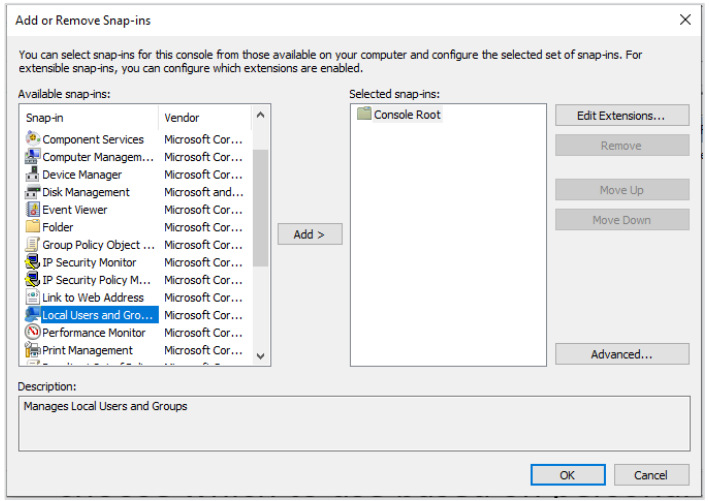
Local Users and Groups console

Windows categorises accounts as User or Administrator so that it can automatically apply the relevant permissions and rights.

Define a user's level of access by categorising their account as a User or Administrator.

To set up the Local Users and Groups console:

Start Menu → Search 'mmc' → Click 'Yes' to allow changes to computer → Click 'File' → 'Add/Remove Snap-ins' → Select 'Local Users and Groups' → Select 'Add' → Select 'Finish' → Click 'OK'.



The following slides will show you how to control user access through Control Panel and through the Local Users and Groups Console. Other methods exist and you can choose which to use based on personal preference.

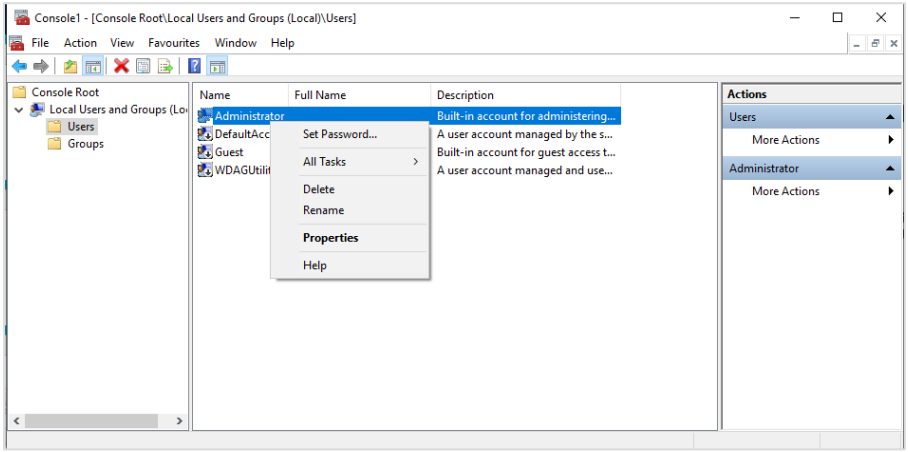
Best practice:

Secure the built-in Administrator account

Add a password.

Obfuscate (hide) the account by changing the name.

Attackers will target known Admin accounts because successfully infiltrating those accounts will give them advanced permissions and access to the network.



Restrict use of the account.

Use the ‘Properties’ menu to remove unnecessary accounts from the Administrators group.

Best practice:

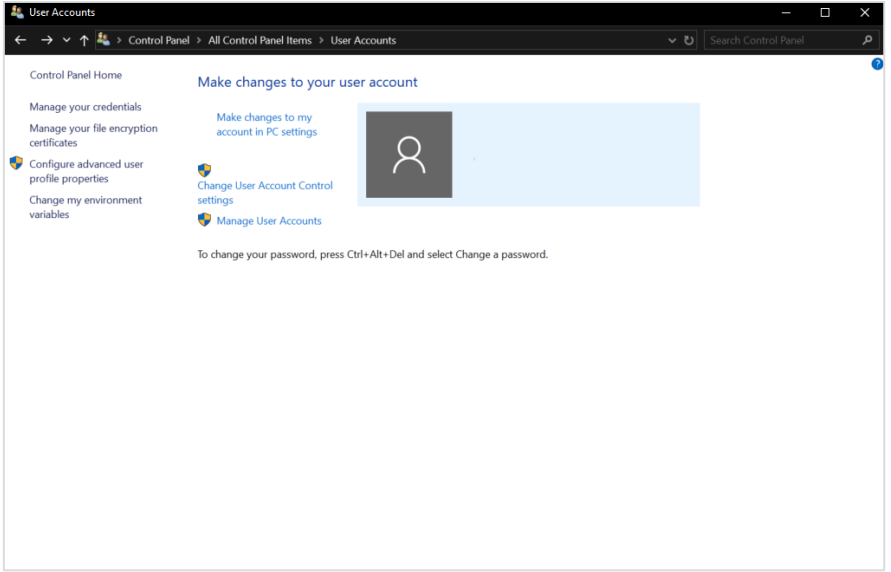
Restrict Administrator group membership

Settings and Control Panel options

Windows Settings → Accounts → Family and other people → Click User name

OR Control Panel → User Accounts → User accounts → Manage another account

Click User name

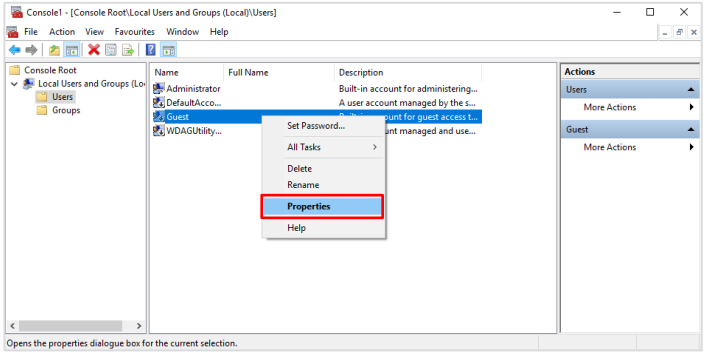


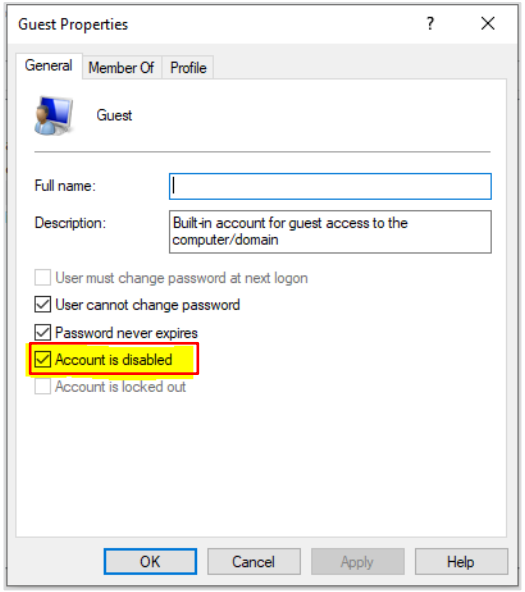
Best practice:

Disable the built-in Guest account

Disable this account so people cannot anonymously access a computer.

While someone on a Guest account will not have direct access to other users' information, they can still significantly disrupt the resources of the local computer.





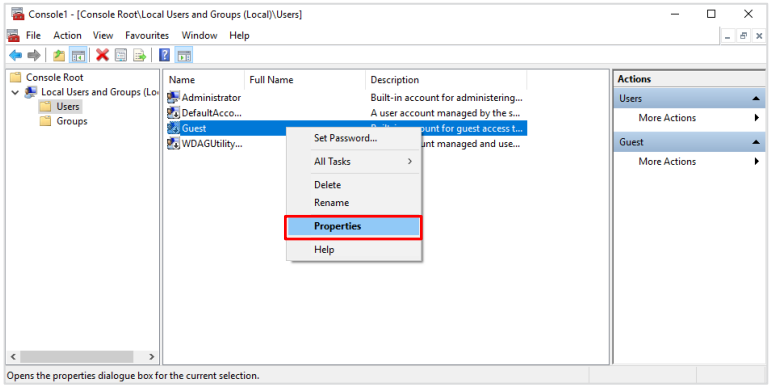
Best practice:

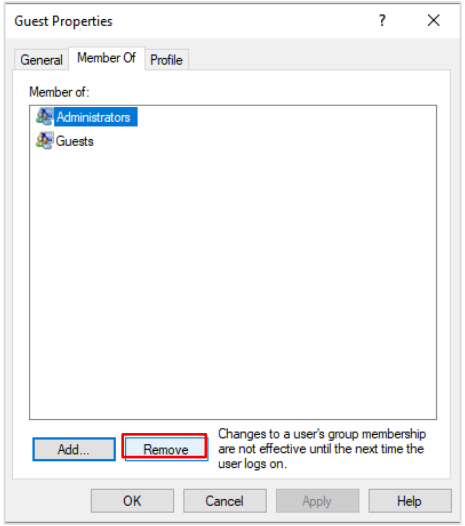
Restrict Administrator group membership

Administrator accounts allow people to efficiently make changes across a network or computer and to monitor and control the use of shared resources.

Because of those advanced permissions, administrator accounts need to be especially well-protected and limited to only a few individuals.

Remove unnecessary users from the Administrators group.



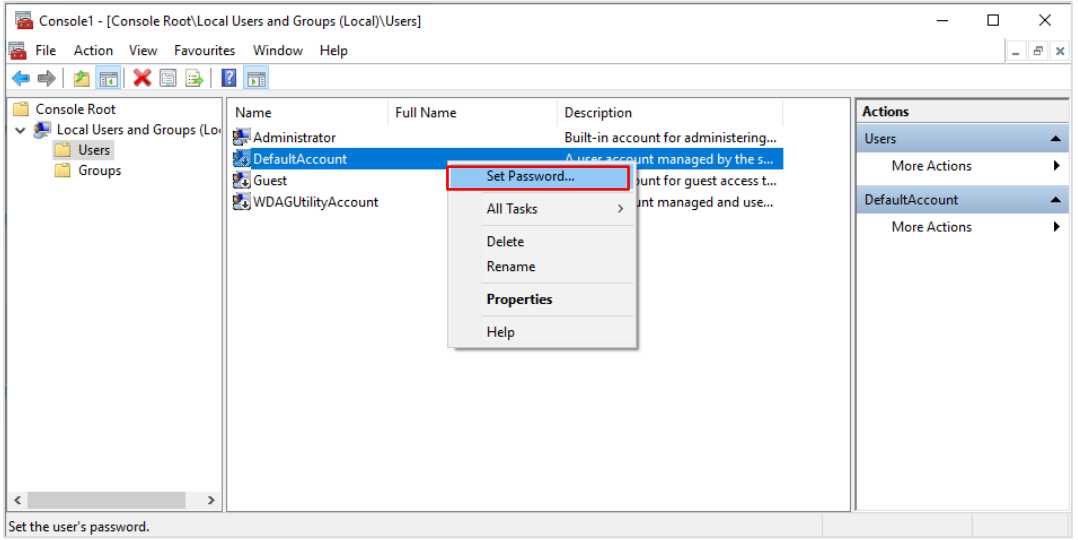


Best practice:

Set passwords for all accounts

Make sure all accounts are password protected

Users → Right click username → Set password

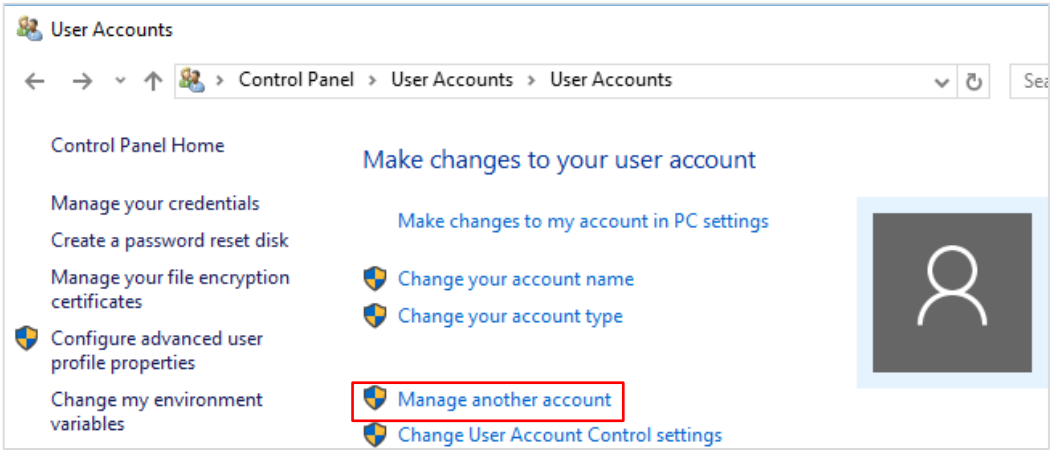


Best practice:

Set passwords for all accounts

Windows Settings will not allow the changing of passwords for all accounts.

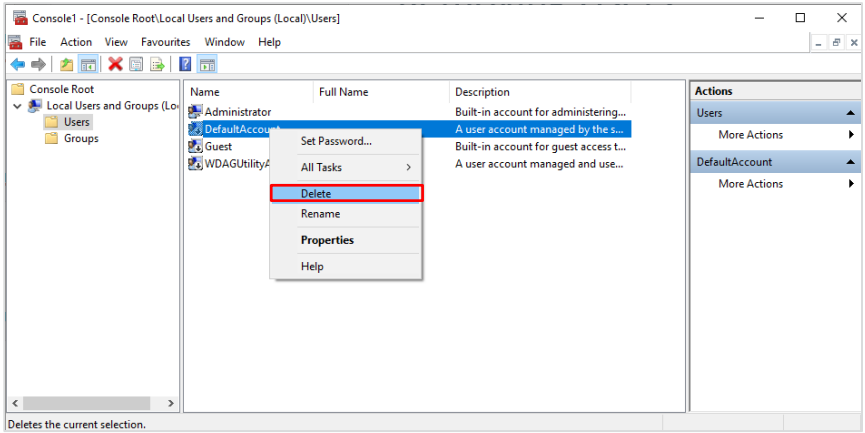
Use Control Panel → User Accounts → User Accounts → Manage another account → Click User Name

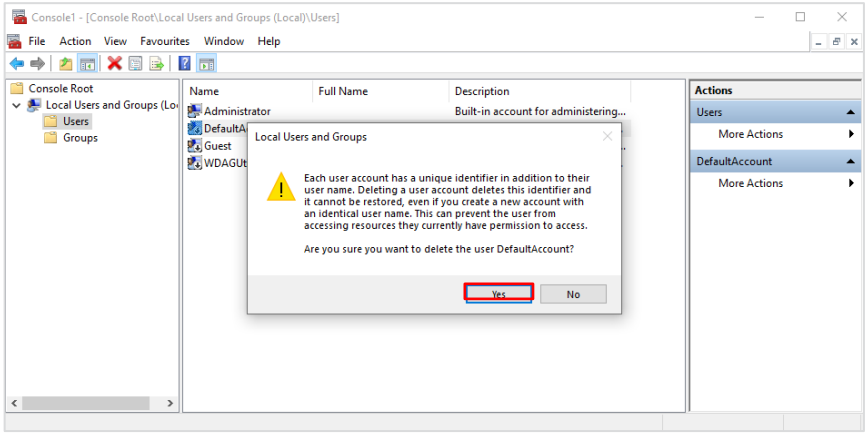


Removing Users

Only current, authorised employees should have access to an organisation’s network.

Make sure your user directory is up-to-date and remove unnecessary accounts.



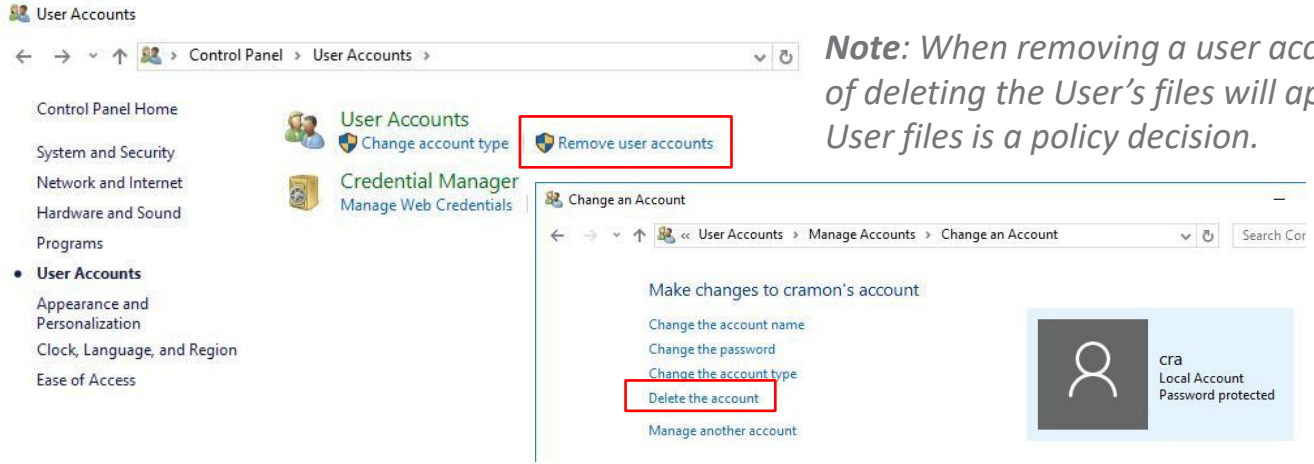


Removing Users

Windows Settings and Control Panel options:

Windows Settings → Accounts → Family and other people → Click User name → Click Remove

OR Control Panel → User Accounts → Remove User Accounts → Click User name → Click Delete the account

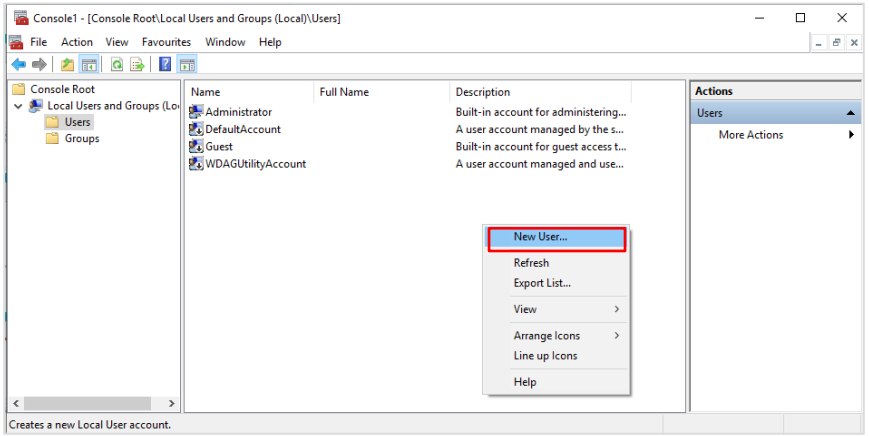


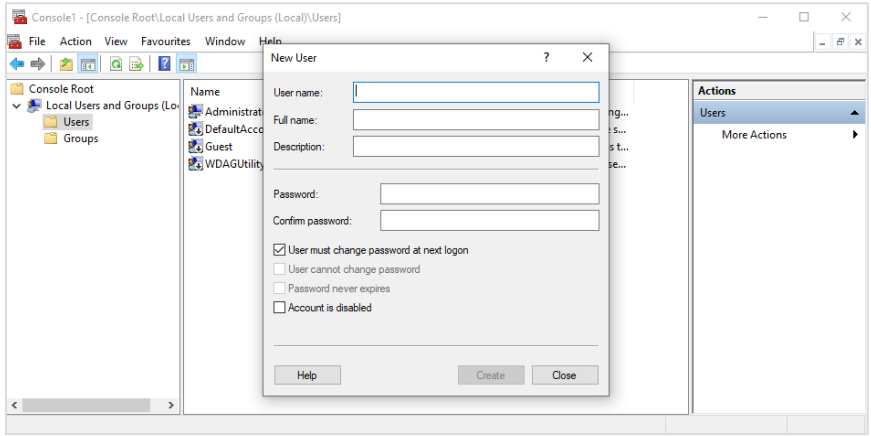
***Note**: When removing a user account the option of deleting the User's files will appear. Deleting User files is a policy decision.*

Adding Users

Console option

When adding new accounts, make sure to put the account in the right User Group and password protect the new User's account.





Adding Users

Windows Settings and Control Panel options

Windows Settings → Accounts → Family and other people → Click + Add someone else to this PC

Note: You may choose to add a user without sign-in information or a Microsoft account.

OR Control Panel → User Accounts → User Accounts → Manage another account →

Click Add a new user in PC settings