AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT 7

Microsoft Windows Security Tools

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 Center
  - 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

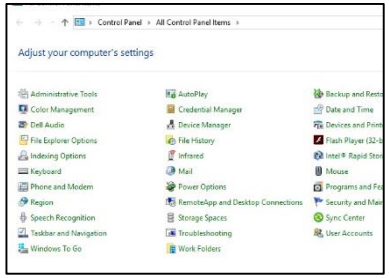
- Windows has several versions (Professional, Home, etc.)
- Each version has sets of security tools with different looks, capabilities, and ways to access them.
- This training unit has several options for accessing almost all the security tools to perform specific tasks.
- In any case, the **search** capability in the Windows versions will assist users and administrators in finding the appropriate tool for a task.

Security and Administration Tools

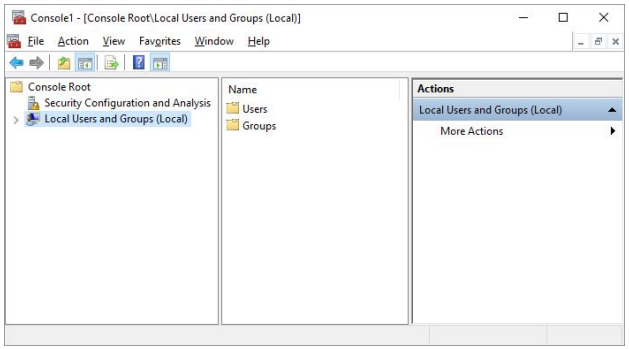
- Windows has several components with groups of security and administration tools.
- You must be an **administrator** to use most of the tools

Some of the components are:

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



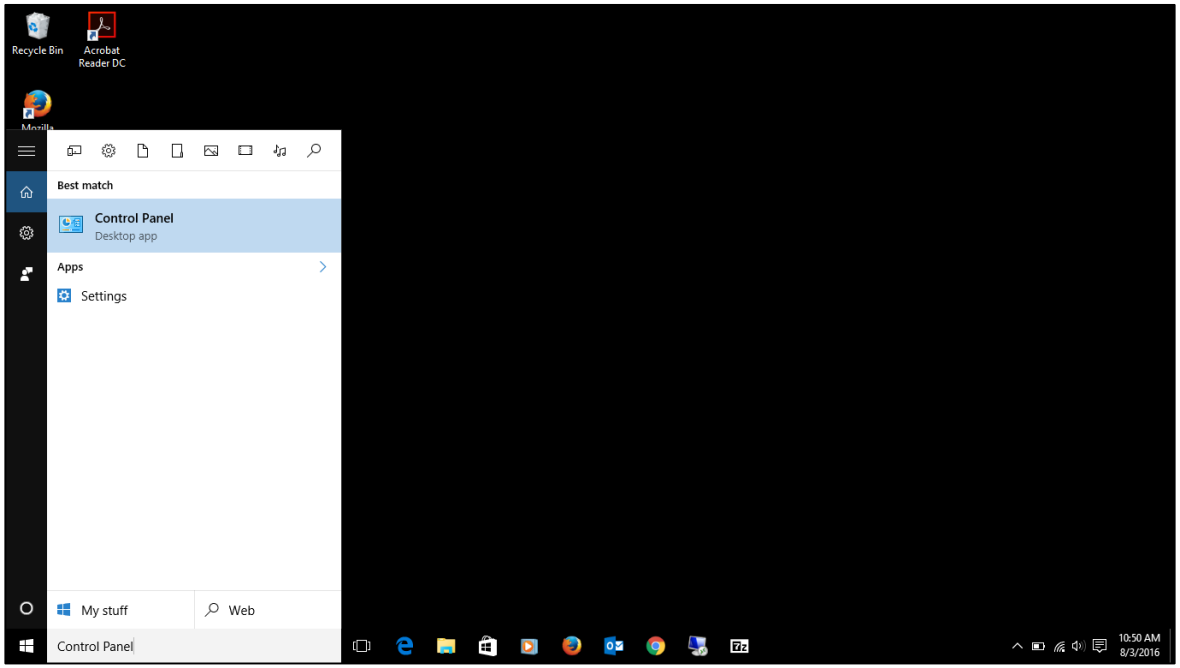
Control Panel



MMC

Windows Search Bar

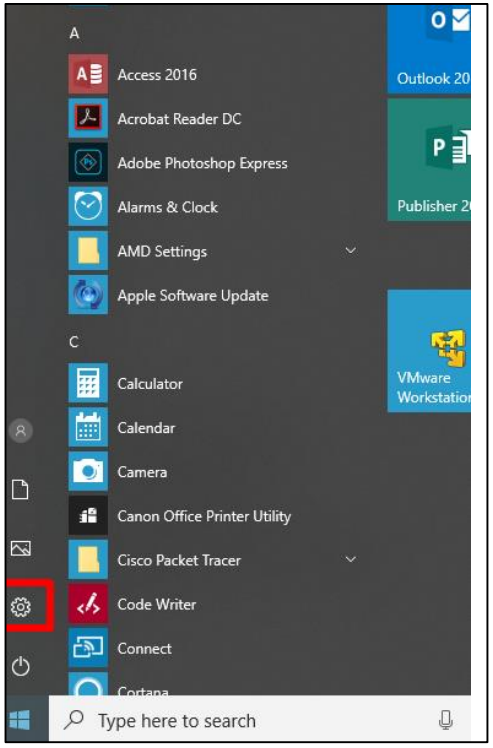
- Windows 10 has a search bar that can bring up anything you need on your system
- You can use the search bar to find any of these upcoming areas if you don't know the direct path



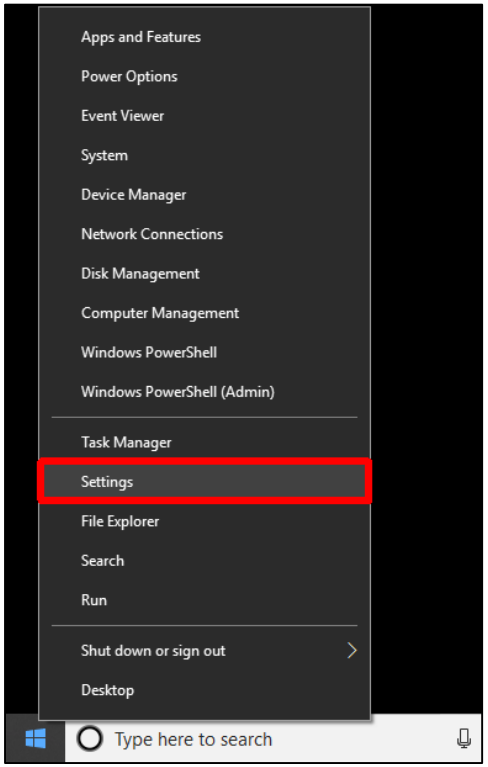
Windows Settings

- 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



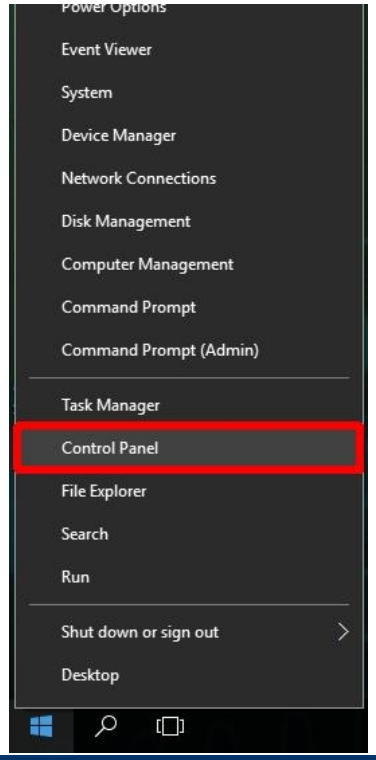
OR Right Click Start → Settings

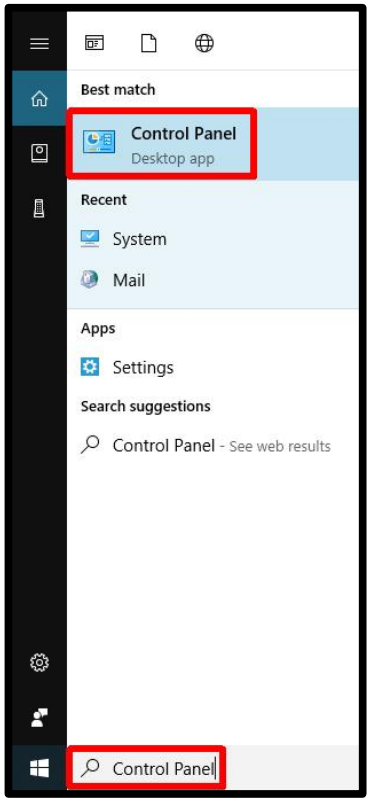


Control Panel and Search

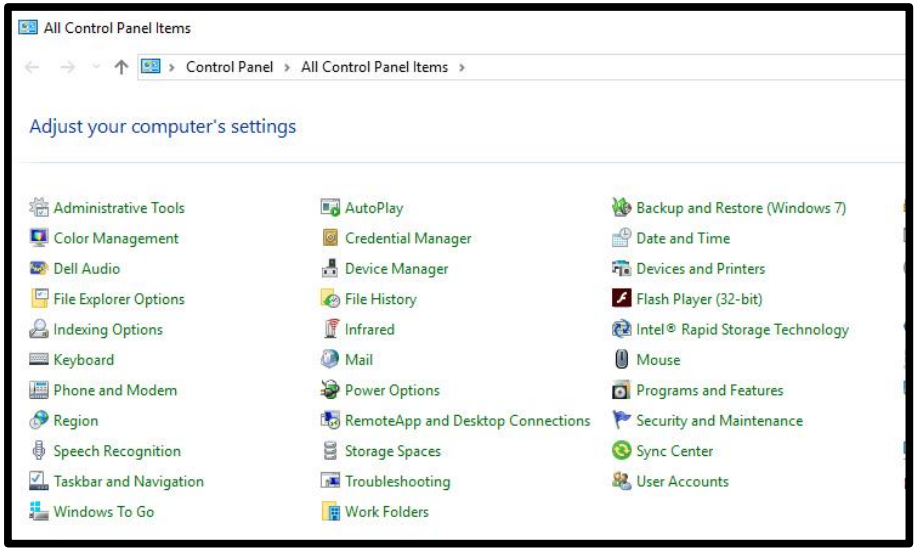
- Control Panel resides in Windows 10 and is more robust than Settings. If you do not see it on your Start menu, you may search for it. Search may be used to find most configuration and security tools within Windows.

Right Click Start → Control Panel





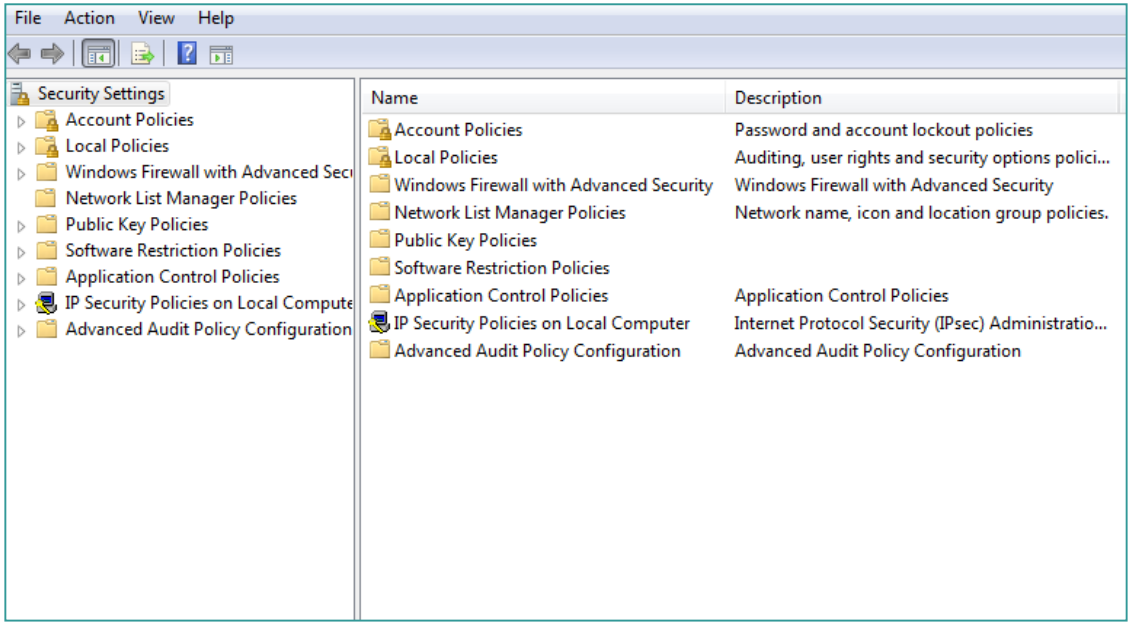
OR Click "Type here to search" → Type Control Panel → Click Control Panel



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 (Unit 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	5 passwords remembered
Maximum password age: how long a user can keep the same password	90 days for users, 30 for admins
Minimum password age: how long a user must keep a password before changing it	10-30 days
Minimum password length: how many characters passwords must be	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

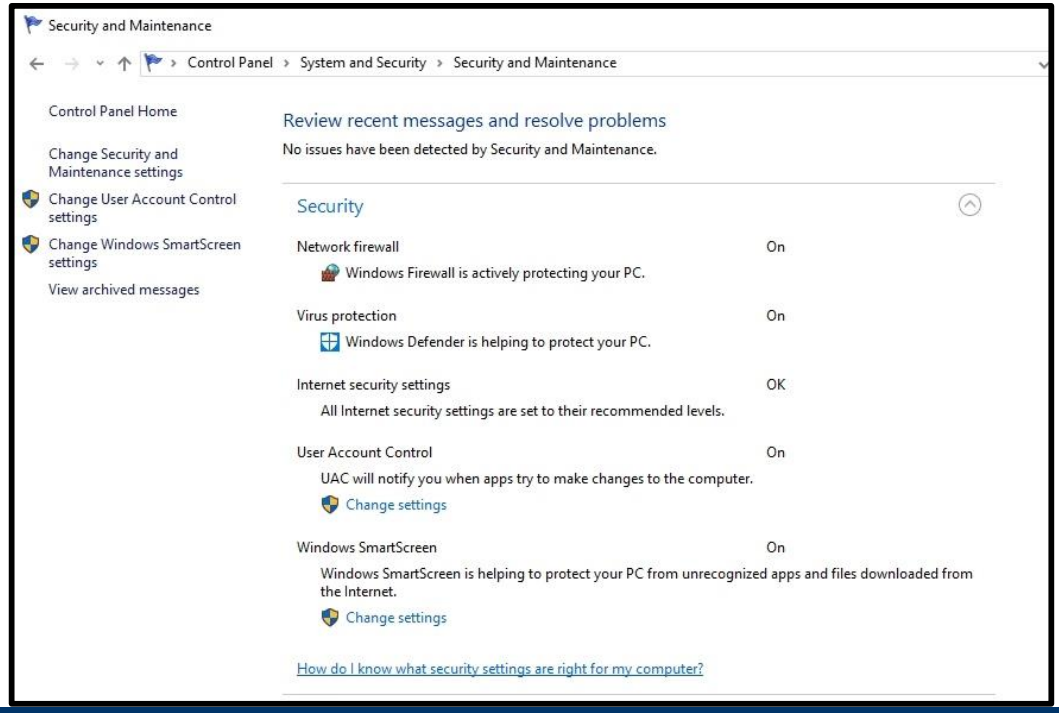
- Even if you have the strongest password possible, if you give hackers unlimited attempts to break it, they eventually will
- Account policies govern unsuccessful attempts to log into an account
- Click Account Policies → Account Lockout Policies

Policies:	Recommended settings:
Account lockout duration: the number of minutes a locked-out account remains locked before automatically becoming unlocked	30 minutes
Account lockout threshold: the number of failed logon attempts that causes a user account to be locked out	3-10 invalid login 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 Center

Window Defender is an important defensive tool in Windows. To open Windows Defender:

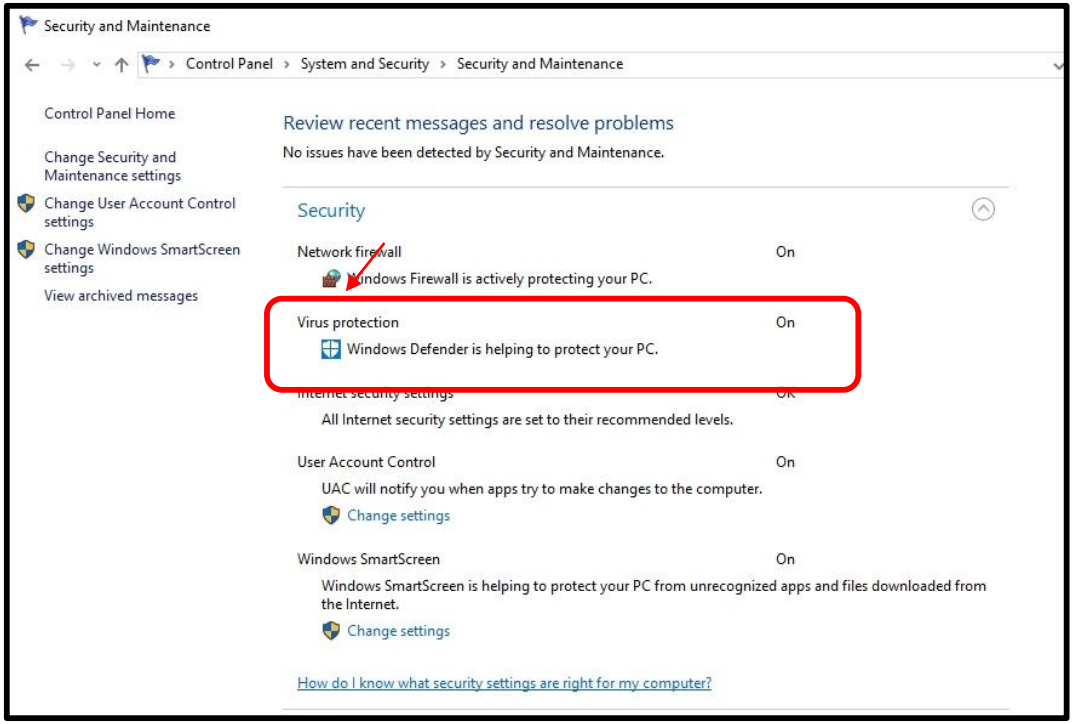
- Click Start → Settings→ Windows Settings → Update and Security → Windows Security
- **OR** Click Start → Control Panel→ System and Security → Security and Maintenance→ Security
- Notifies you if Windows identifies problems with or updates for:
  - Windows Updates
  - Internet security settings
  - Network firewall
  - Spyware and related protection
  - User Account Control
  - Virus protections
  - Windows Backups



Windows Defender and Anti-Malware

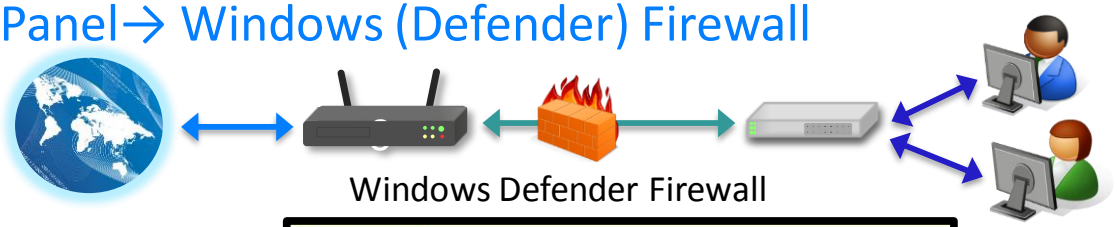
- Click Start → Settings→ Windows Settings → Update and Security → Windows Security
- **OR** Click Start → Control Panel→ System and Security → Security and Maintenance→ Security

- Anti-malware programs should be updated regularly
- Windows Defender is an anti-malware component of Microsoft Windows. 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

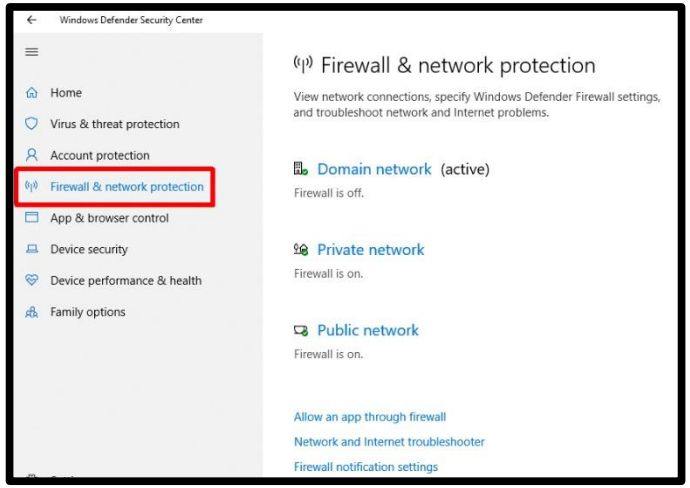


Firewalls

- 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

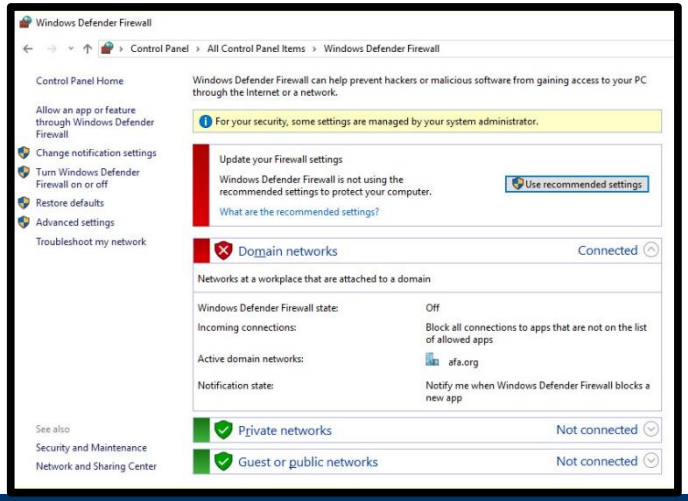


Windows Defender Security Center



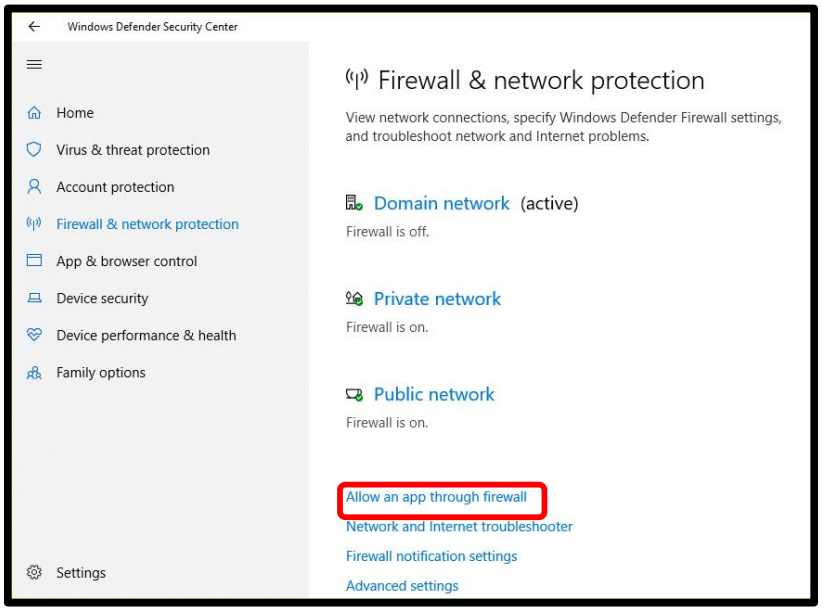
Note: Both firewall settings are for the same firewalls.

Windows Defender Firewall

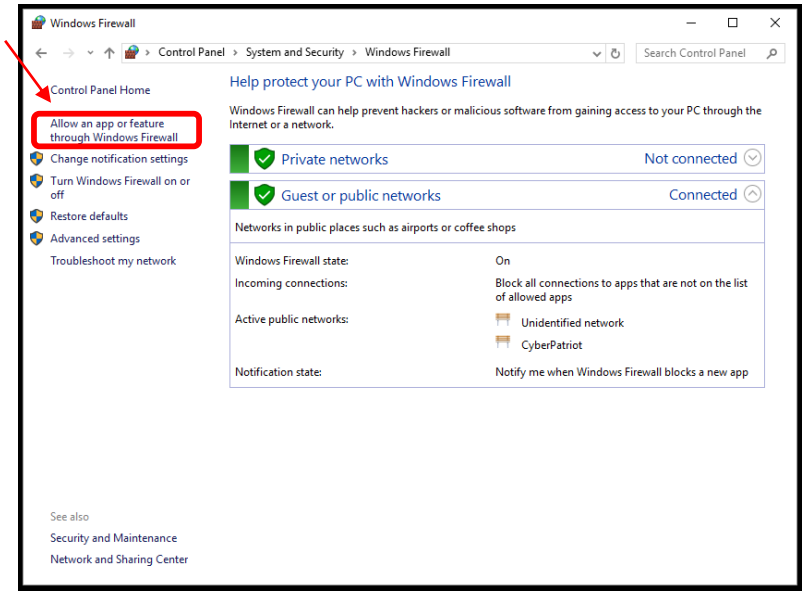


Enabling Windows Firewall Exceptions

- Allows trusted programs to connect without being blocked by adding them to your Windows Firewall Exceptions list
  - For each network type, you can customize 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



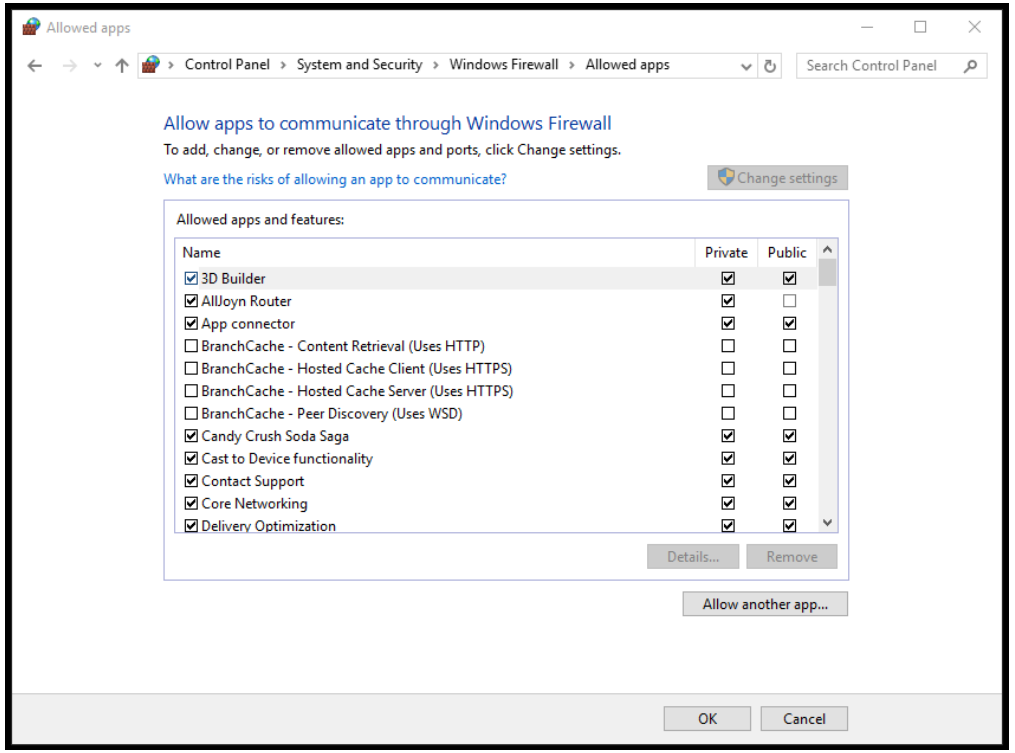
Windows Defender Security Center



Windows (Defender) Firewall

Enabling Windows Firewall Exceptions

- For each network type, you can customize 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

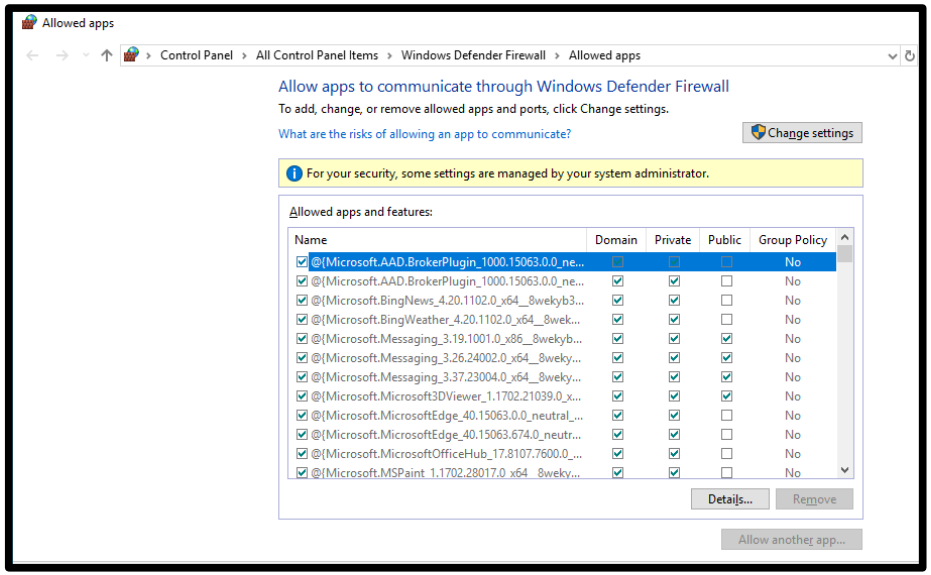


Common Exceptions

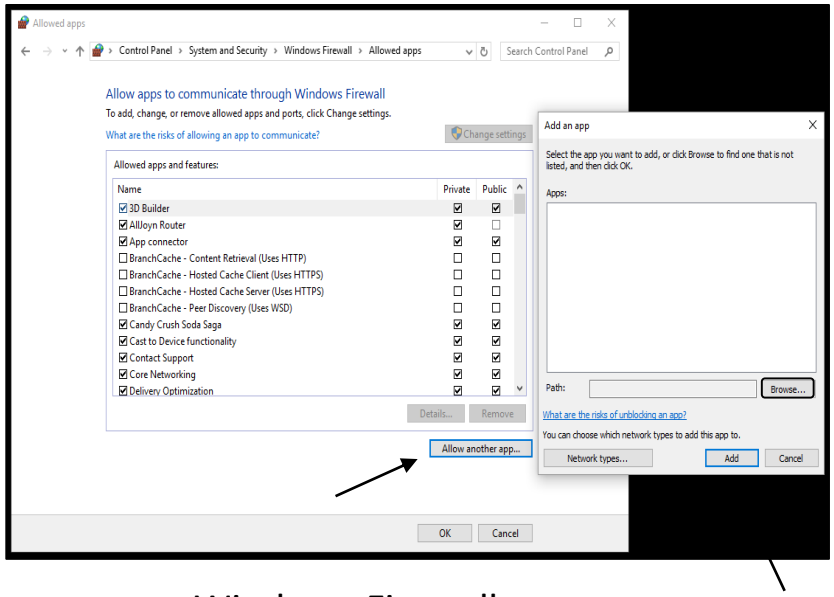
- Core Networking
  - Regular Microsoft Windows services that retrieve data from the Internet
  - If you don't enable this exception across all three types of networks, some Microsoft services and programs will not run properly
- File and Printer Sharing
  - Allows you to share the contents of selected 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” and select the program from the menu
  - You might have to click “Browse” and find the program yourself if it’s not listed



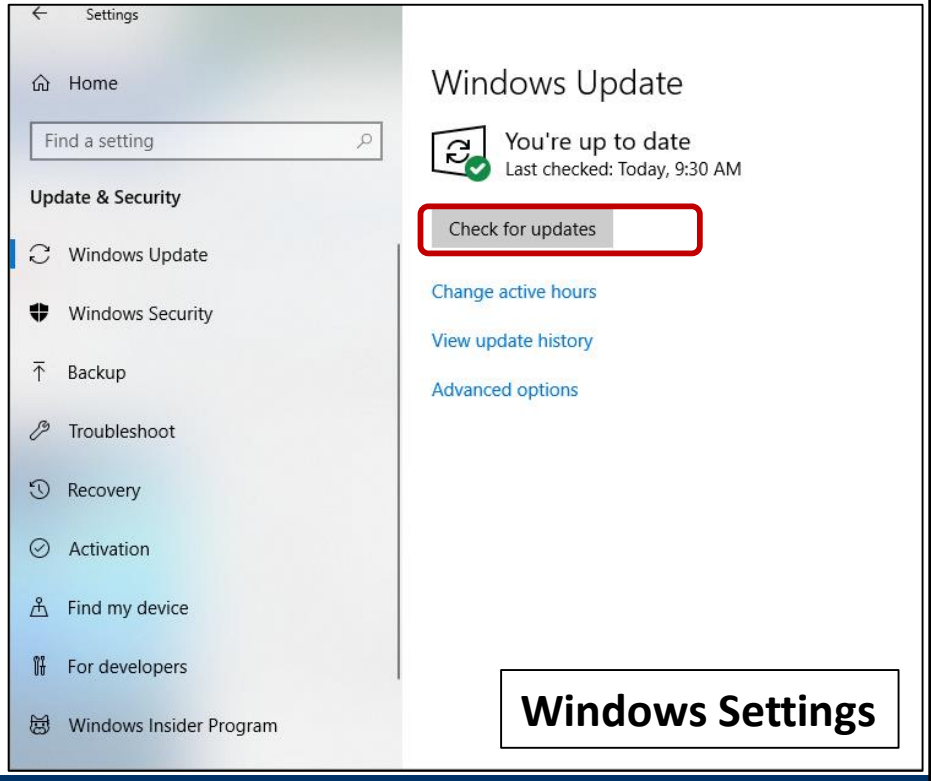
Windows Defender Firewall

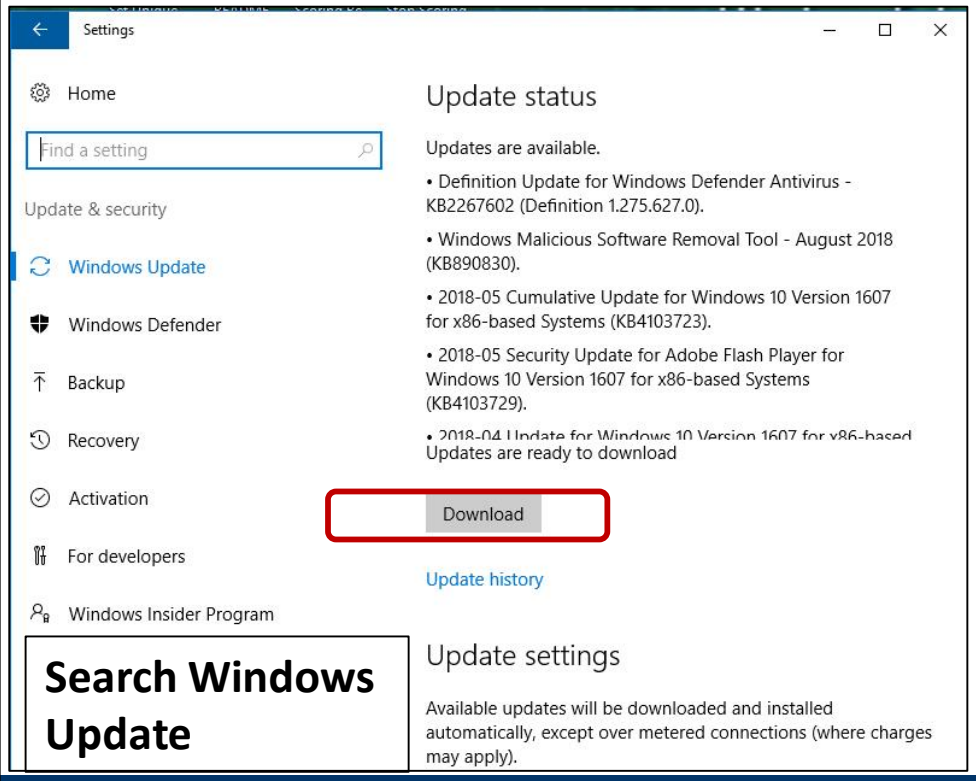


Windows Firewall

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

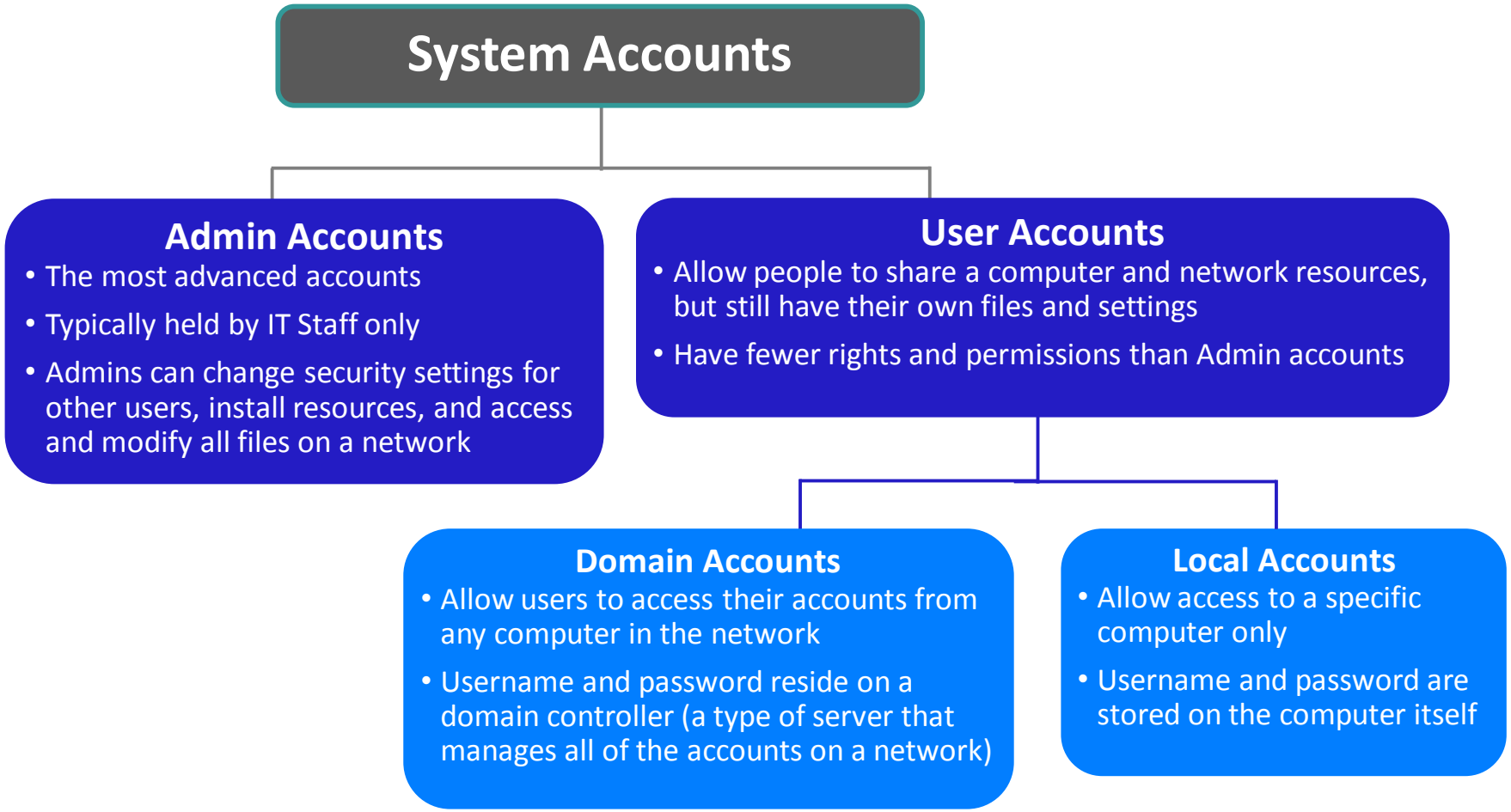




SECTION 2

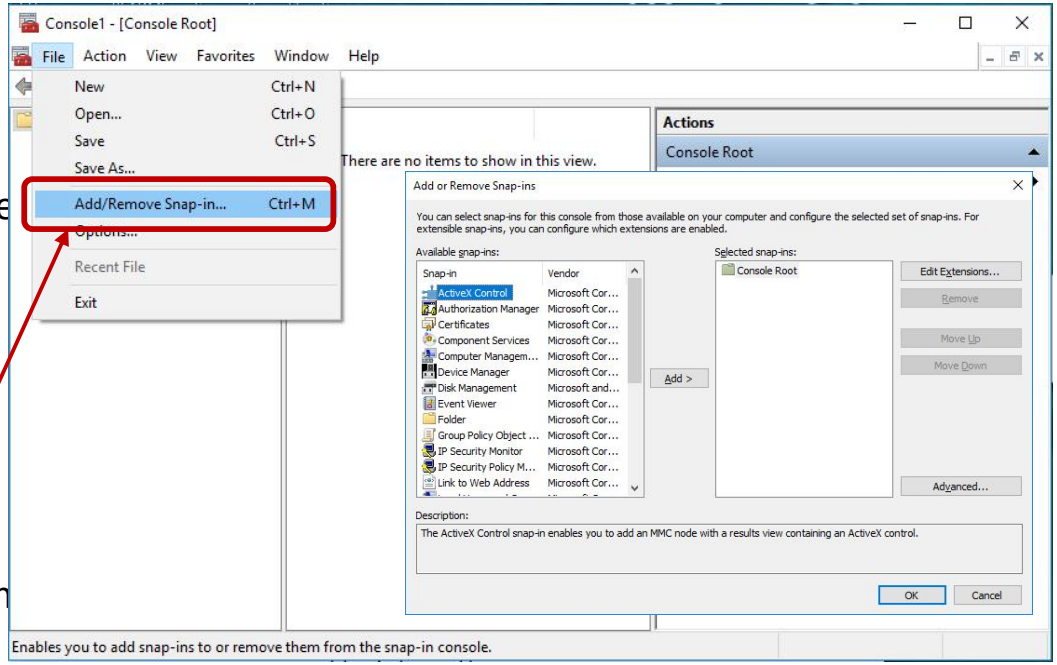
Account Management

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 Control Panel.
- MMC allows settings to be made to user and group permissions.
- **Snap-ins** are the tools the MMC accesses to making settings. Snap-ins must be opened in MMC. They **do not** automatically appear when MMC is executed.

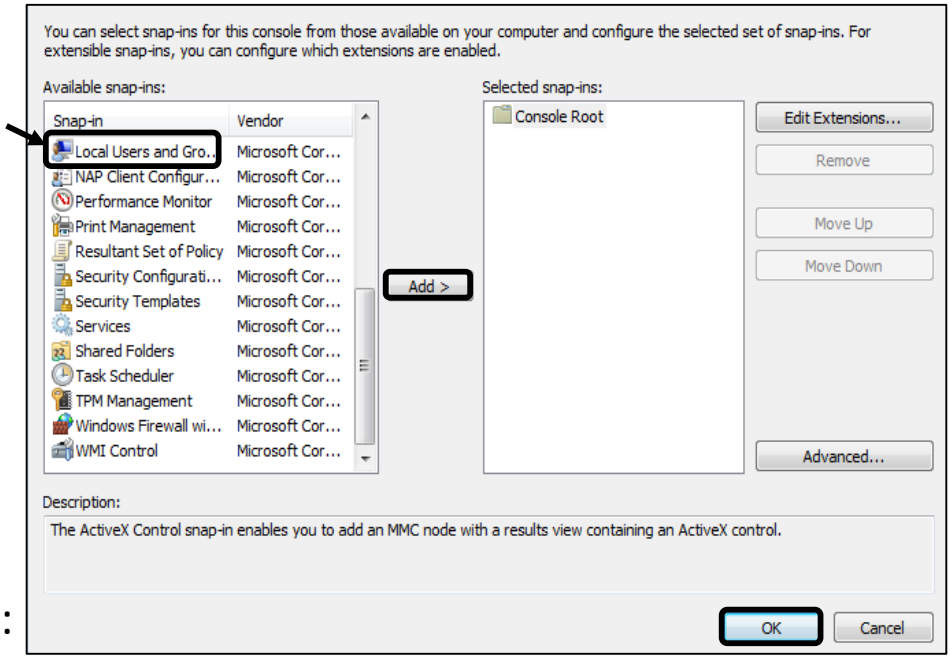


- **To access MMC:** Search → "mmc"→ Click "yes" to allow changes to computer
- **To access Snap-ins in MMC:** Click File → Add/Remove Snap-ins

*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 categorizes accounts as user or administrator accounts so that it can automatically apply the relevant permissions and rights
- Define a user's level of access by categorizing his or her account as a user or administrator



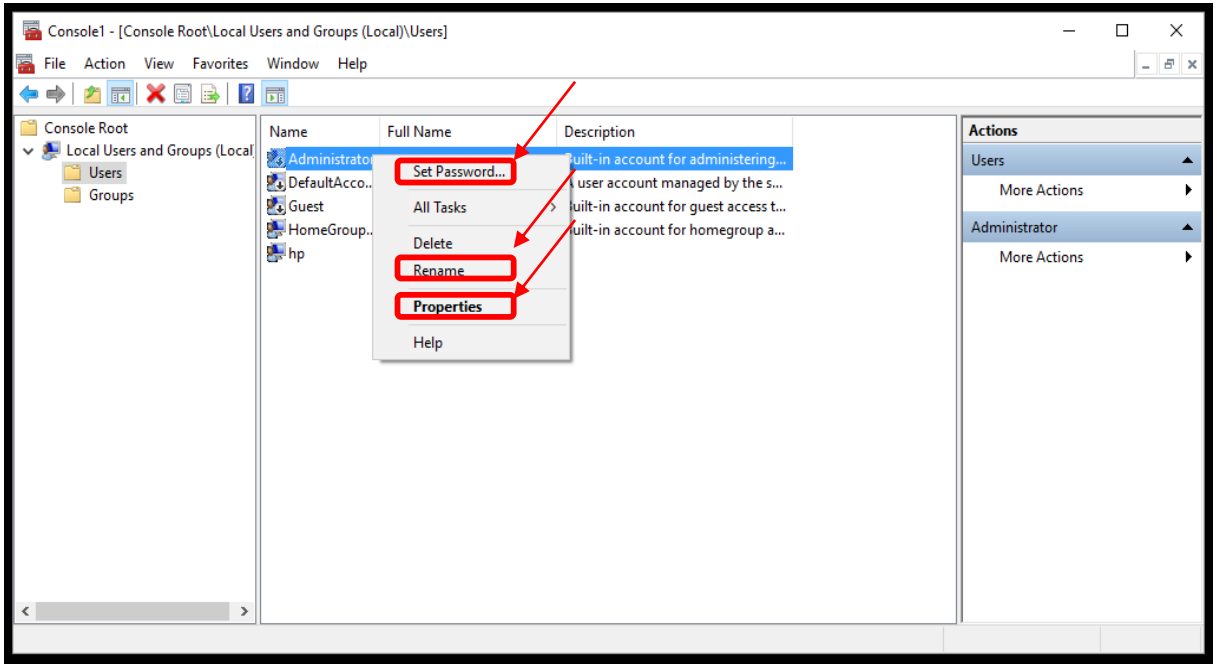
- To set up the Local Users and Groups Console:

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

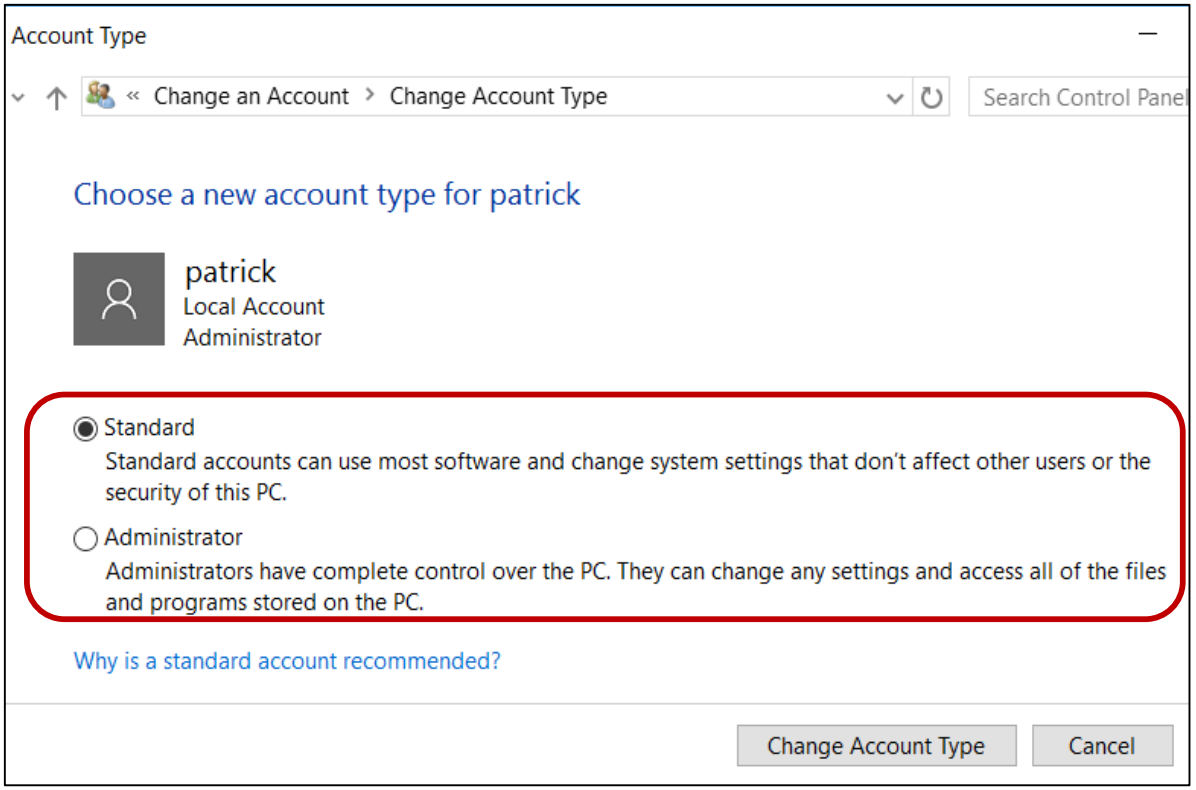
- Add a password
- Obfuscate (hide) the account by changing the name
  - Attackers will target known Admin accounts because successfully infiltrating those accounts will give them advanced permissions and access to the network
- Restrict use of the account
  - Use the Properties menu to remove unnecessary 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

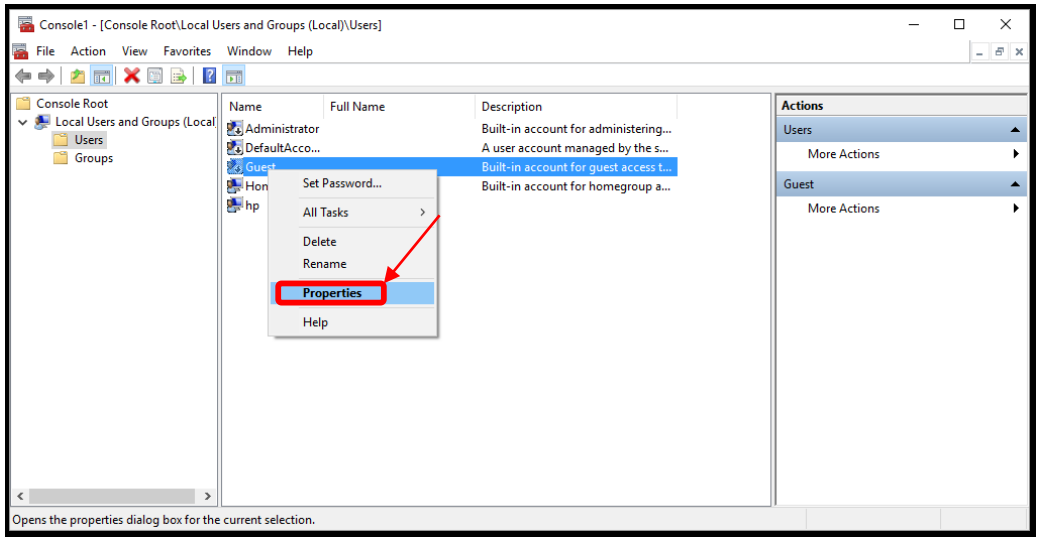


Best Practice: Disable the Built-in Guest Account

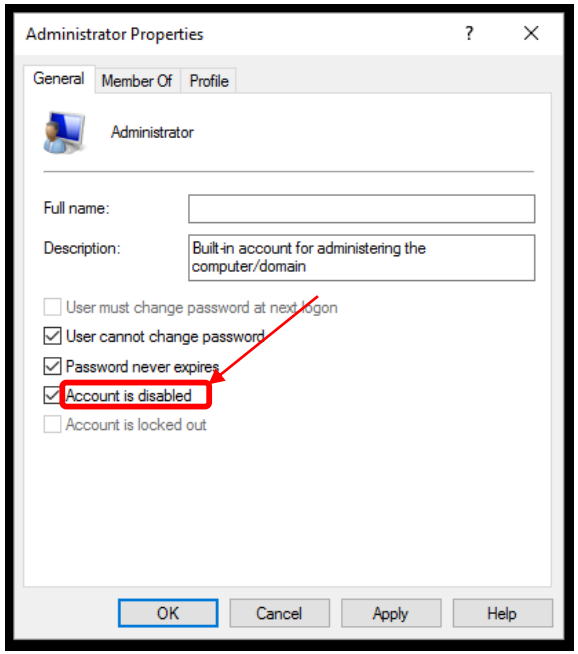
Console option:

- 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, he or she can still significantly disrupt the resources of the local computer

1.



2.

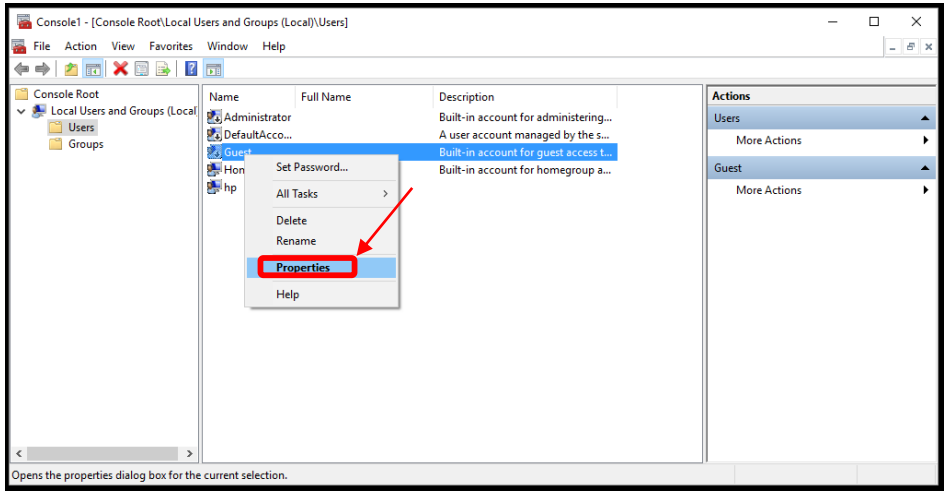


Best Practice: Restrict Administrator Group Membership

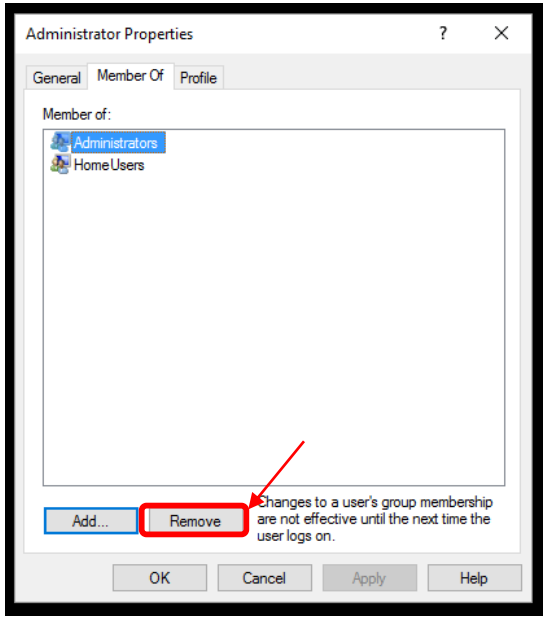
Console option:

- 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

1.



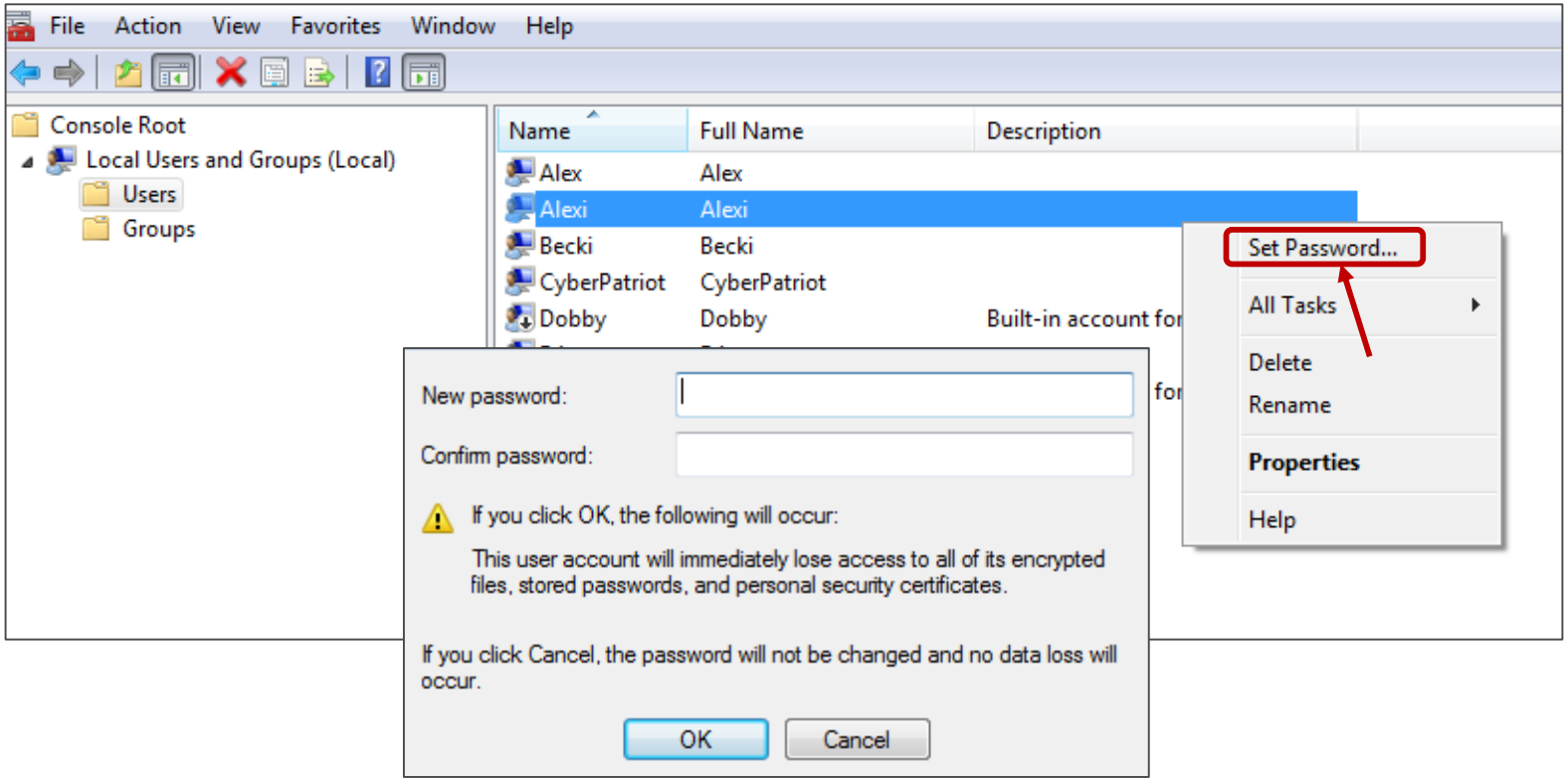
2.



Best Practice: Set Passwords for all Accounts

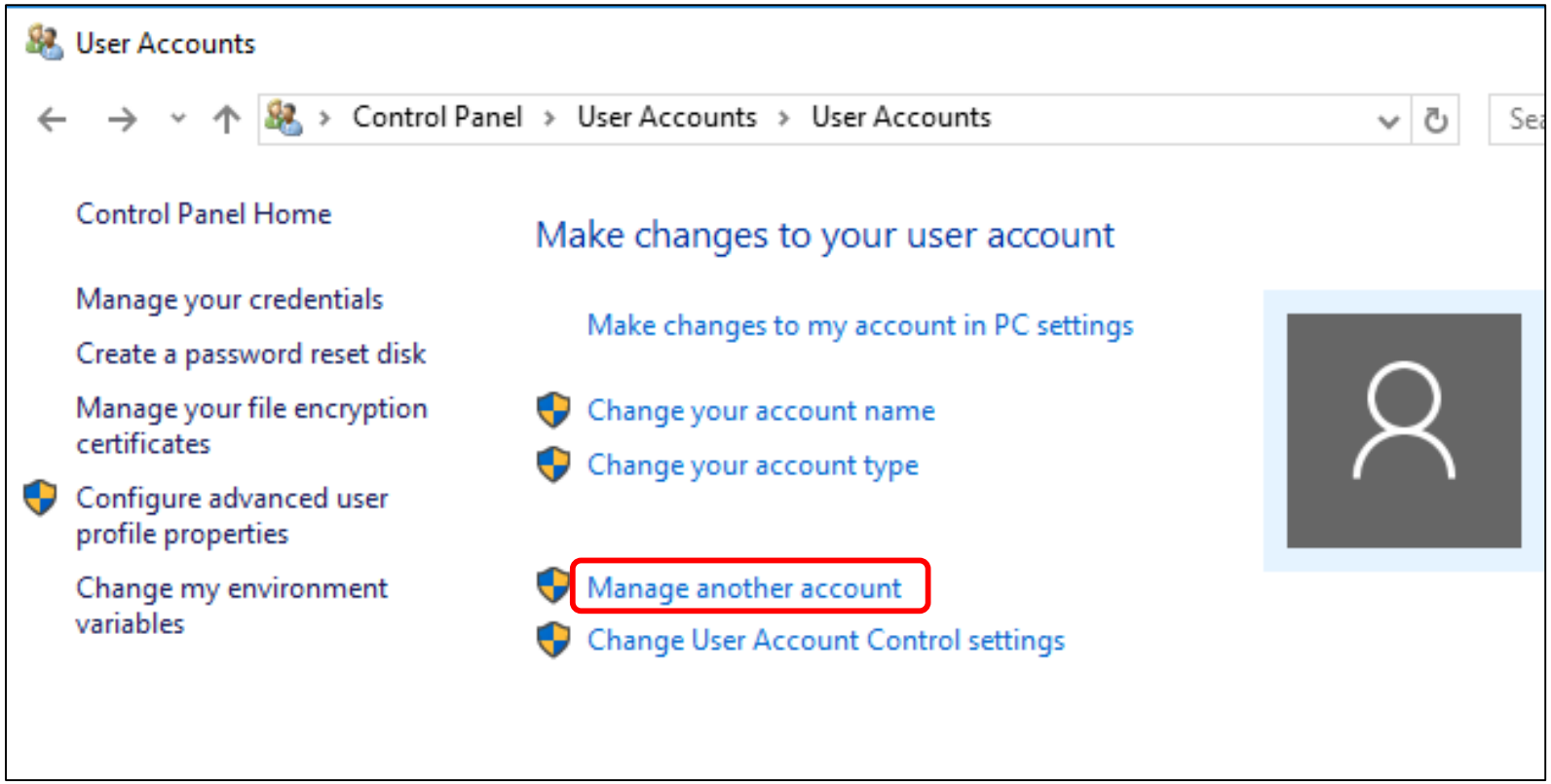
Console option:

- Make sure all accounts are password protected*
- Users → Right click name → 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

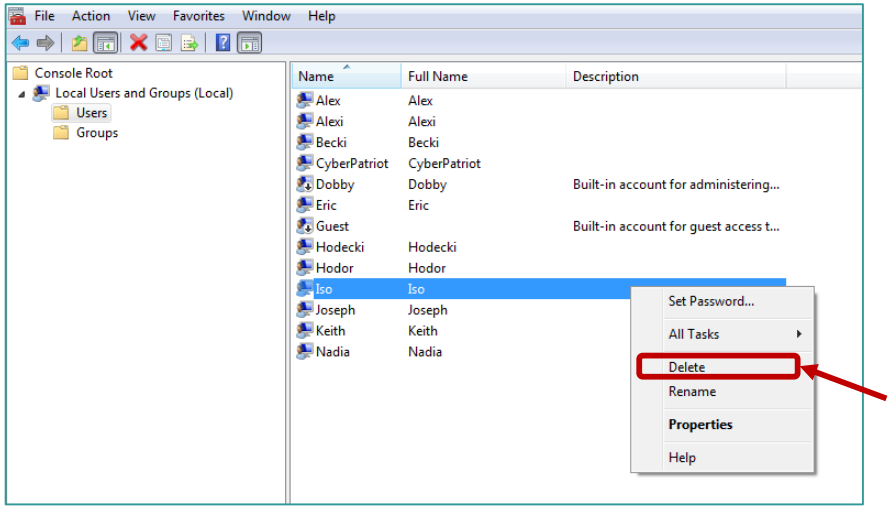


Removing Users

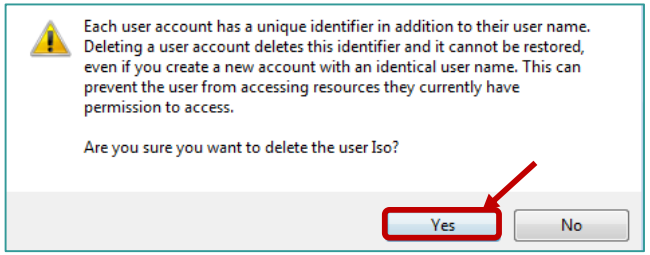
Console option:

- Only current, authorized employees should have access to a organization's network
- Make sure your user directory is up-to-date and remove unnecessary accounts

1.



2.

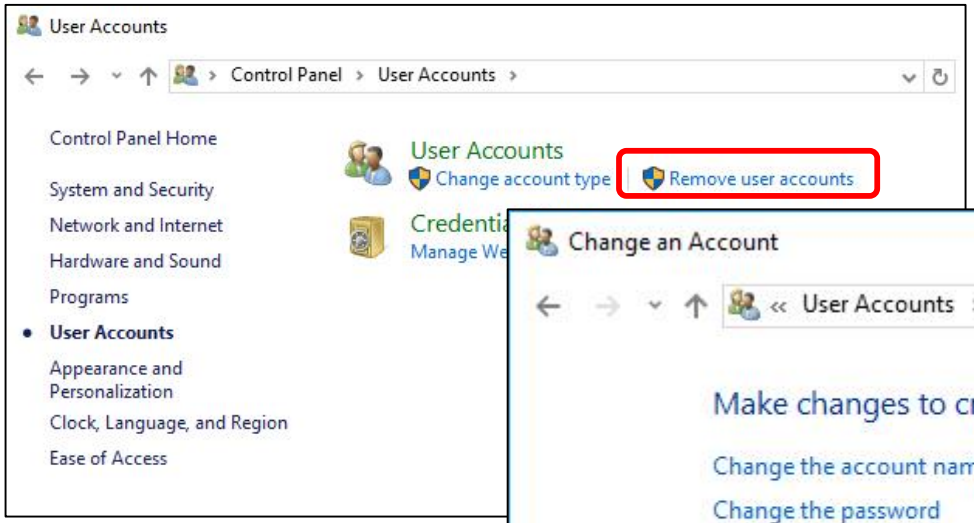


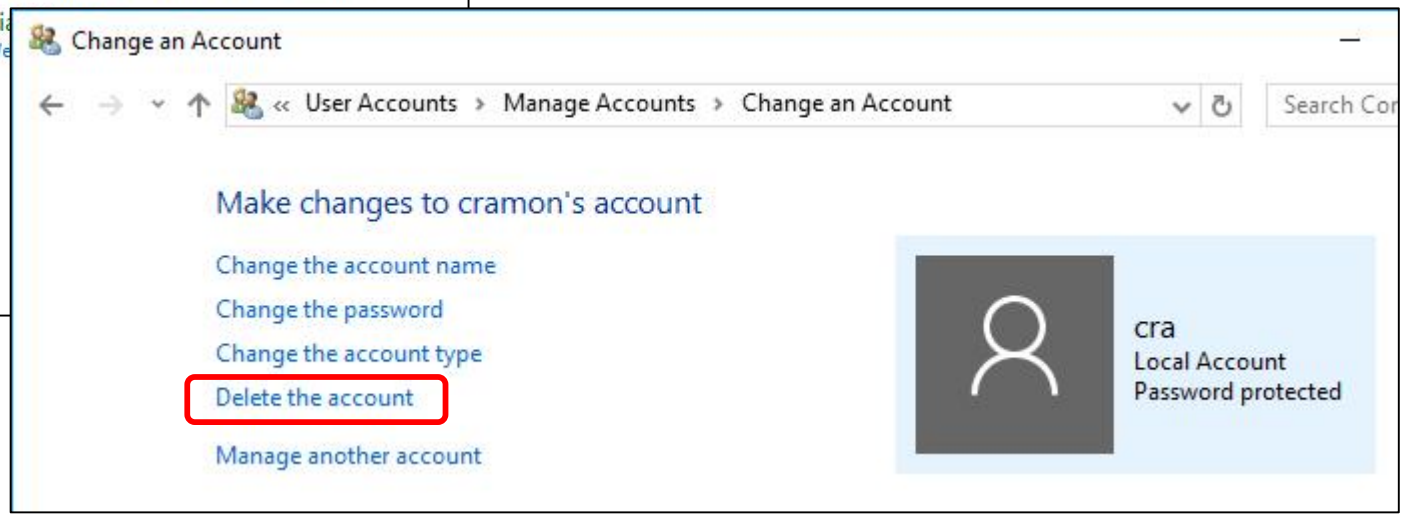
Removing Users

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.



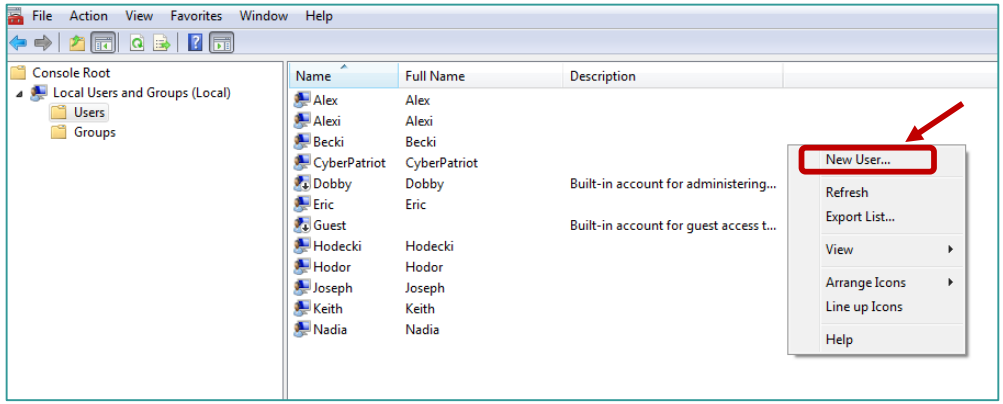


Adding Users

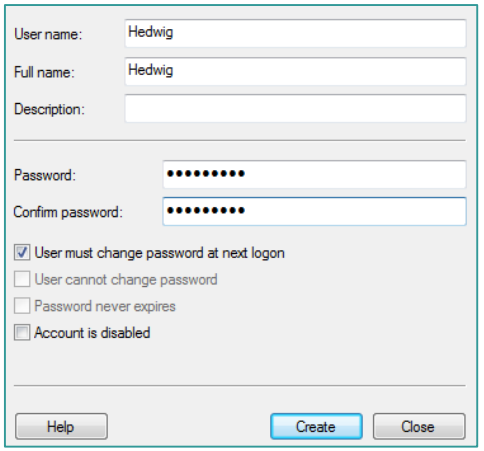
Console option:

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

1.



2.



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