



WorkED | SYSTEM HARDENING



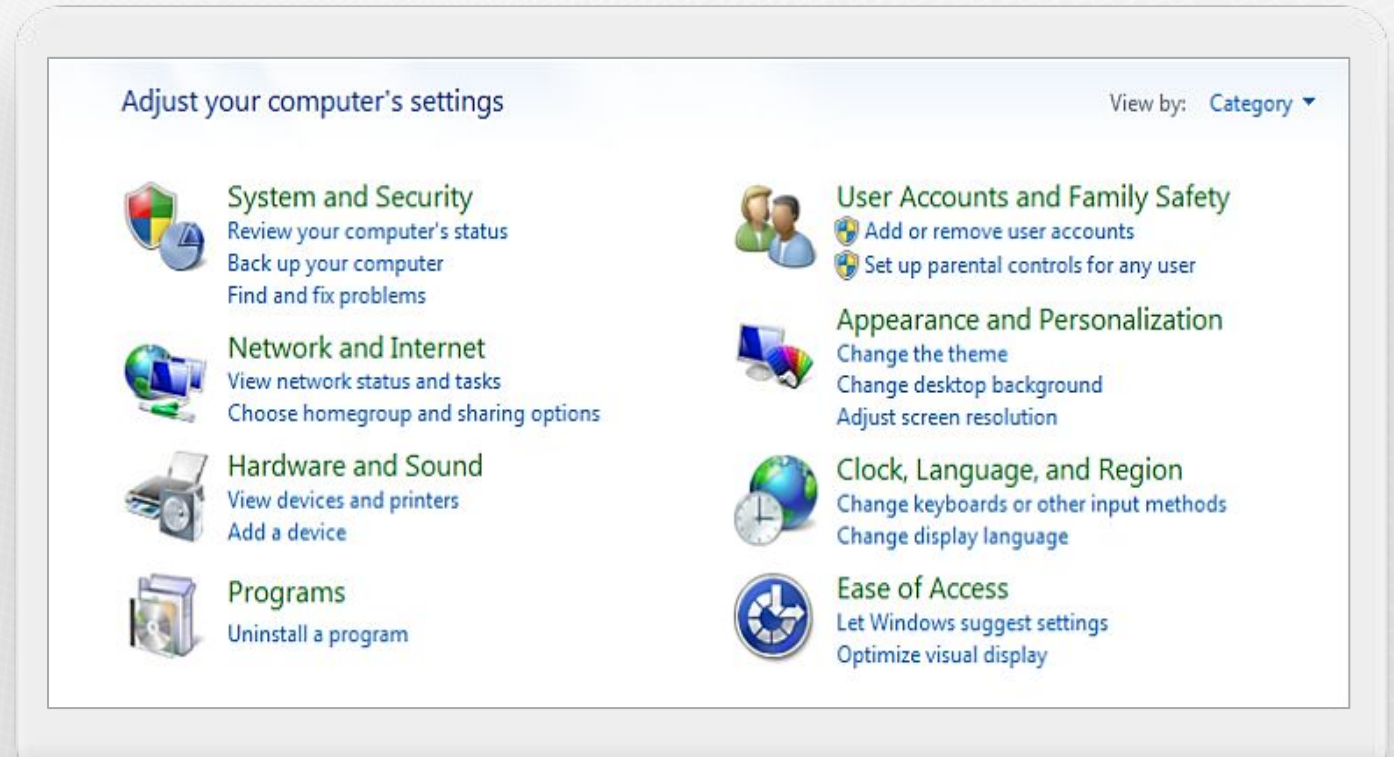
WorkED

SECTION ONE

BASIC SECURITY POLICIES & TOOLS

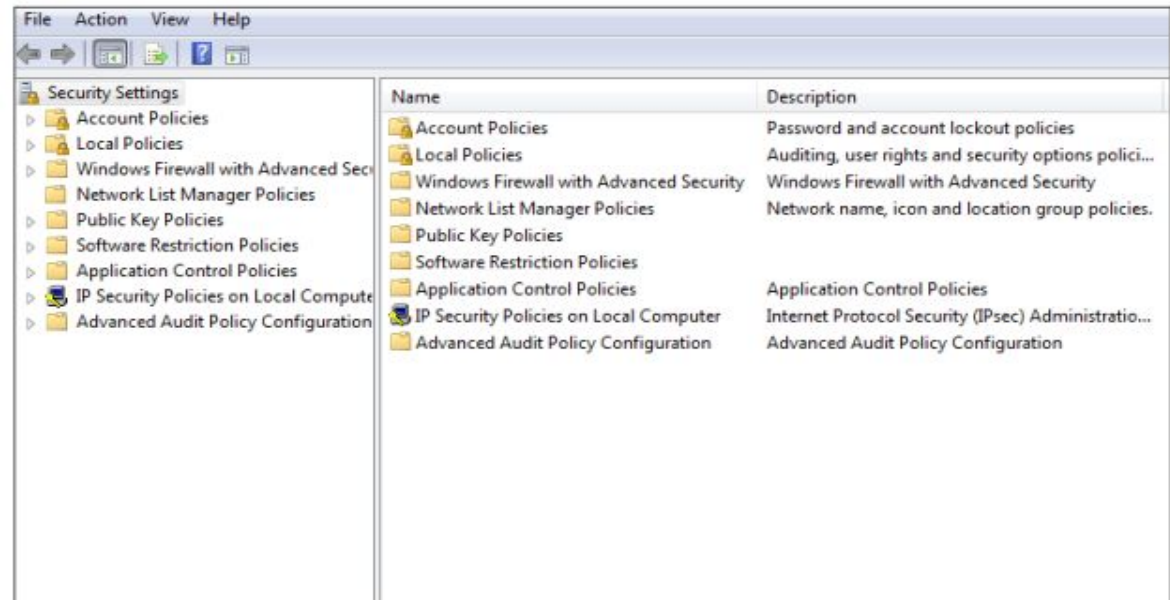
CONTROL PANEL

- Where many of the **basic system changes** and configurations can be made with a Windows operating system
- **Click Start -> Control Panel**



BASIC LOCAL SECURITY POLICIES

- Controls **security settings** on user computers within a network
- Click **System and Security -> Administrative Tools -> Local Security Policy**



PASSWORD POLICIES

- Modify policies **to require** users create strong passwords
Remember CLOUDS Not SUN (Unit Four)
- 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	8 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

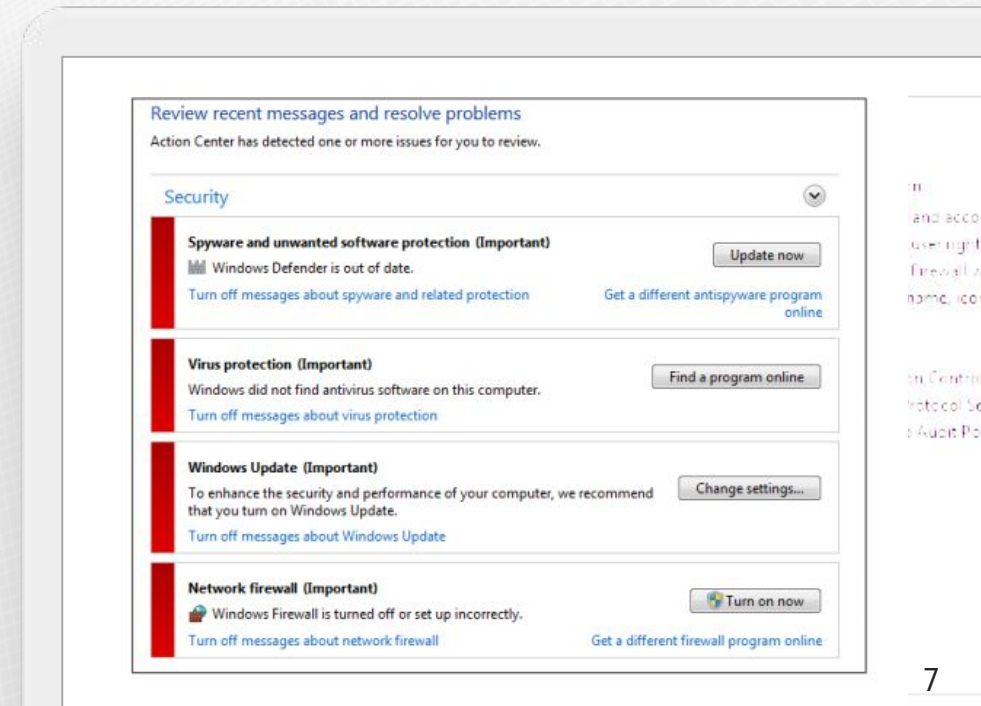
ACCOUNT LOCKOUT POLICIES

- 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 login attempts that causes a user account to be locked out	5-50 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

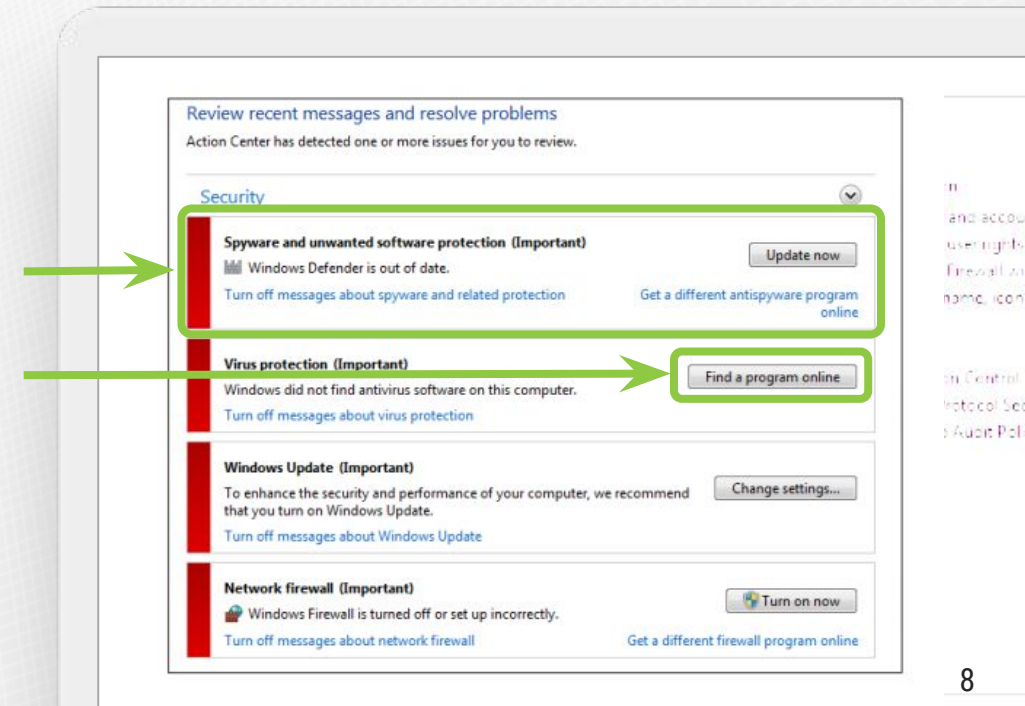
ACTION CENTER

- Click Start -> Control Panel -> System and Security -> Action Center
- **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 Troubleshooting



WINDOWS DEFENDER AND ANTI-MALWARE

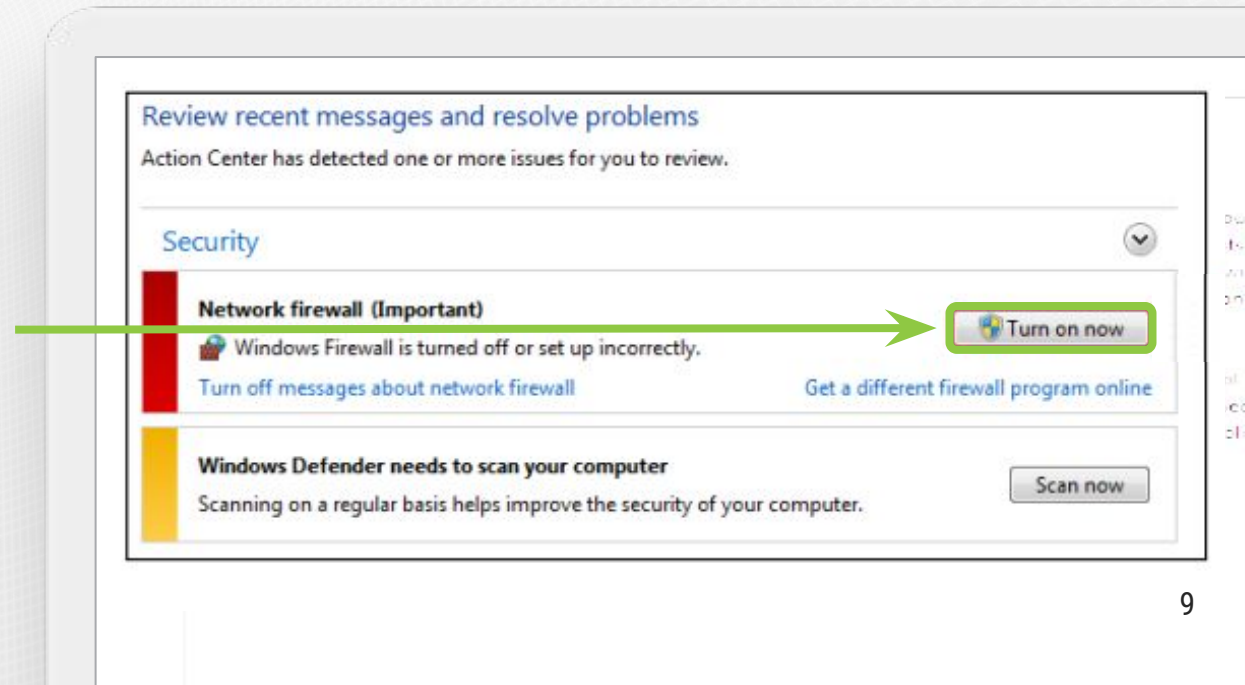
- Click Start -> Control Panel System -> and Security
- Anti-malware programs should be **updated regularly**
- Windows Defender is a **very basic** built-in spyware protection program on Windows - It only protects against known spyware, not viruses, worms or other malware
- Download a **supplementary 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.



WorkED

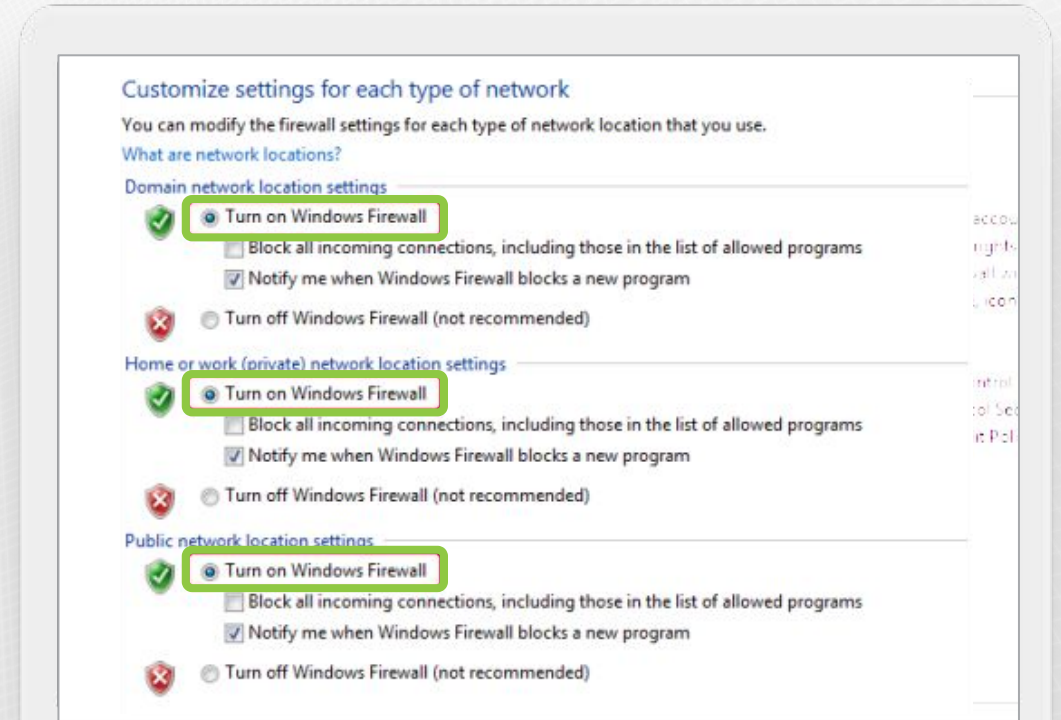
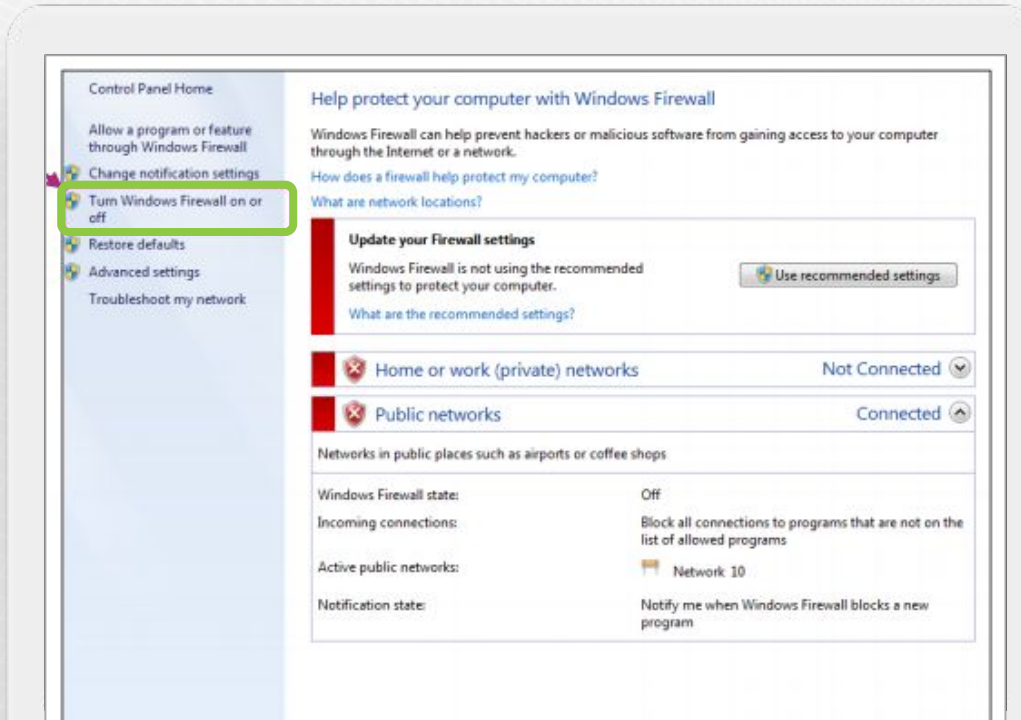
FIREWALLS

- **Reject or allow** data packets through to users based on custom settings
- Essential to security and should **always be turned 'on'**
- **Control Panel -> System and Security -> Windows Firewall -> Turn on now**



WINDOWS FIREWALL CUSTOM SETTINGS

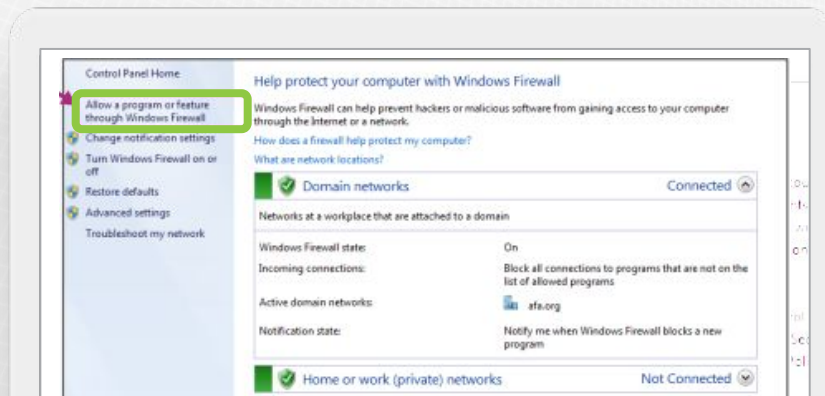
- For **more** advanced settings: **Control Panel -> System and Security -> Windows Firewall**
- Customize firewall settings for each type of network (e.g. Home, Public, Work)



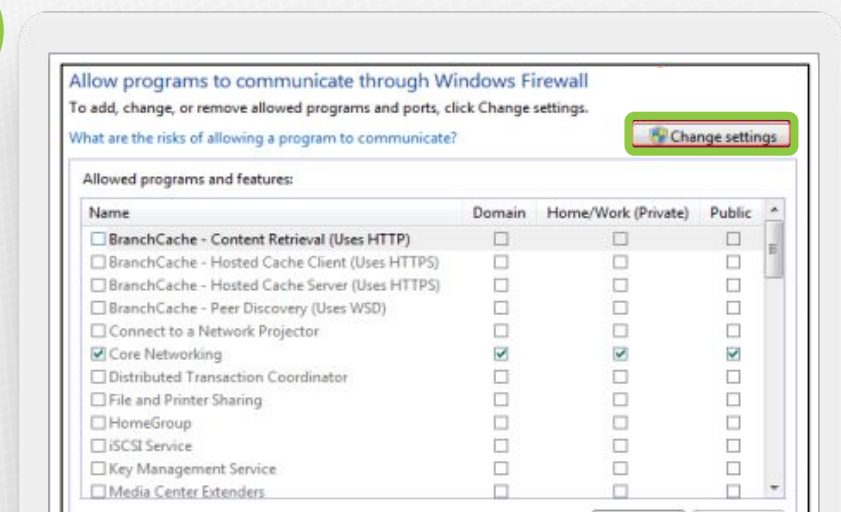
ENABLING WINDOWS FIREWALL EXCEPTIONS

- **Allow 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
- 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
- **Control Panel System and Security -> Windows Firewall**

1



2



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

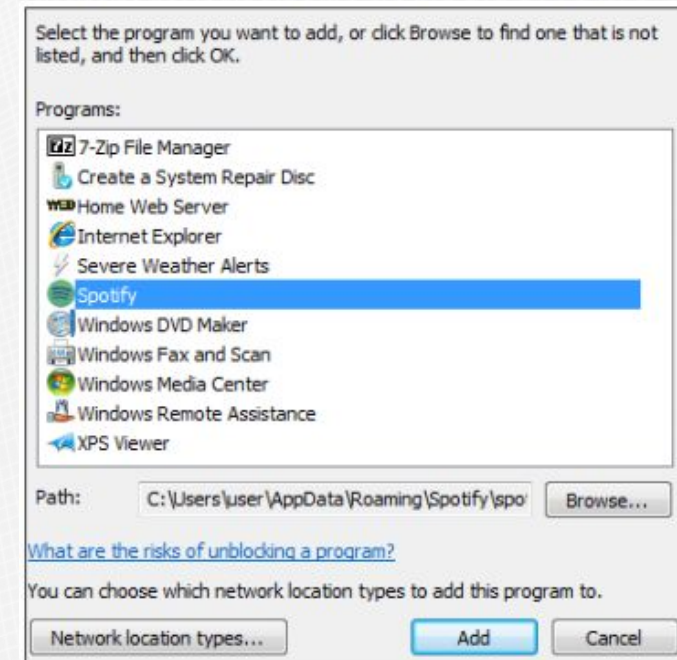
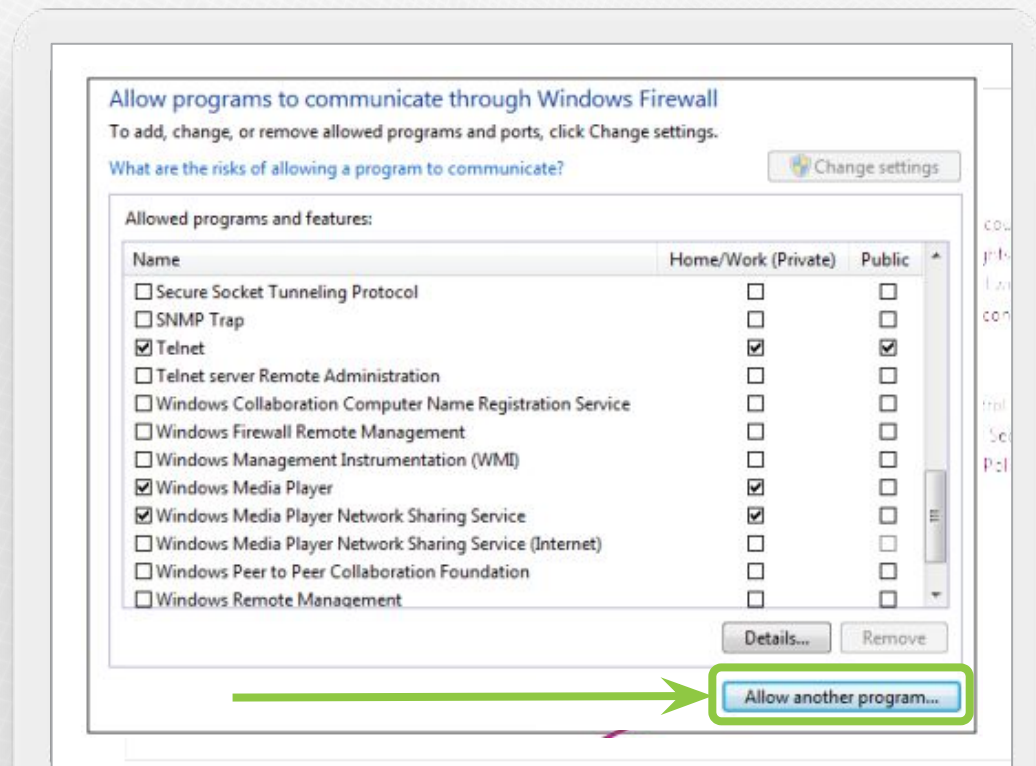
Allows users to access their user accounts and files remotely

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

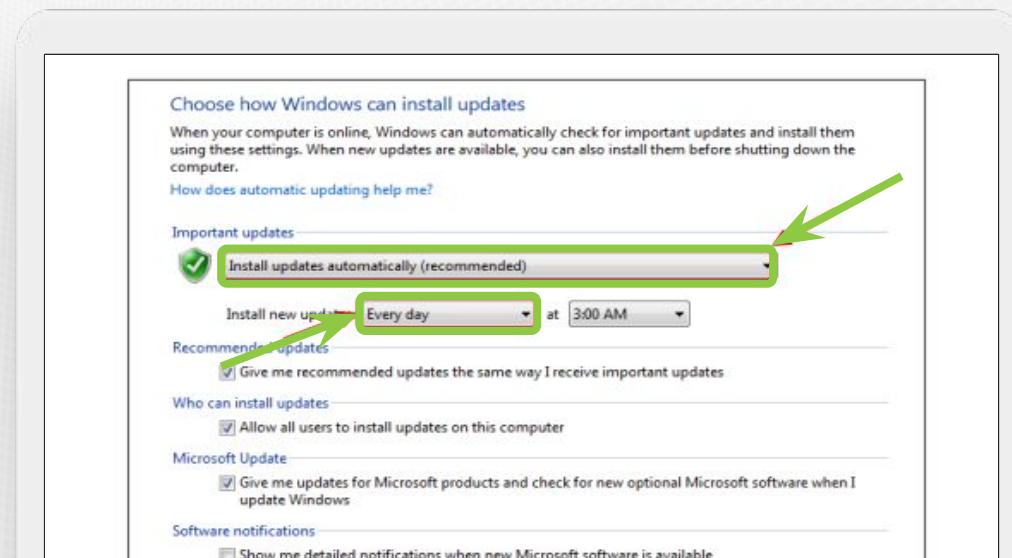


WINDOWS UPDATES

- **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

- **Control Panel -> System and Security -> Windows Update**



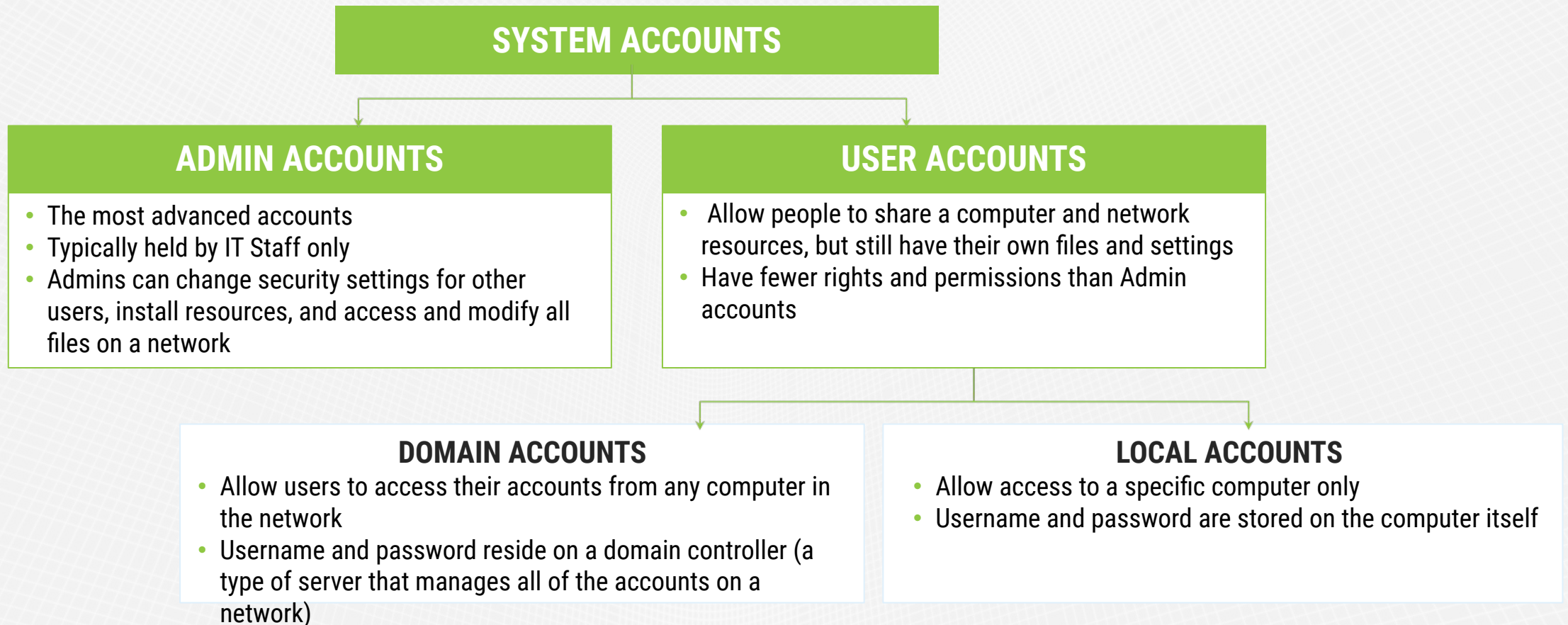


WorkED

SECTION TWO

ACCOUNT MANAGEMENT

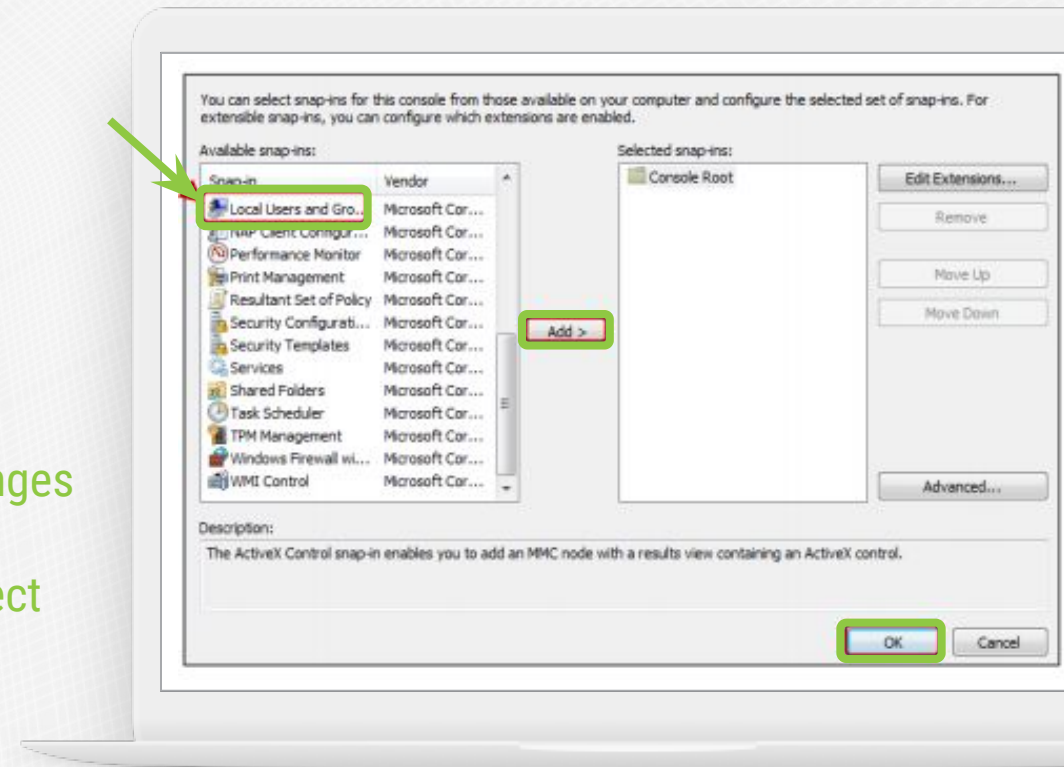
ACCOUNT GROUPS



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:

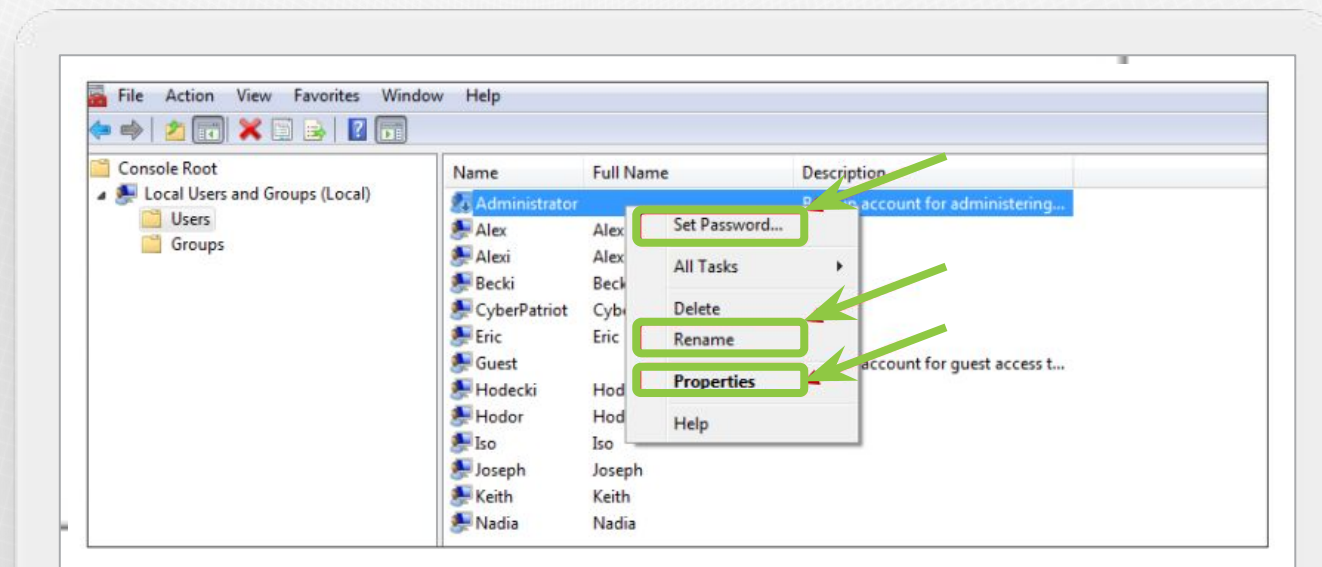
Start Menu -> Search "mmc" -> Click "yes" to allow changes to computer -> Click File -> Add or Remove Snap-ins -> Select "Local Users and Groups" -> When prompted, select "Add to Local Computer"



WorkED

SECURE THE BUILT-IN ADMINISTRATOR ACCOUNT

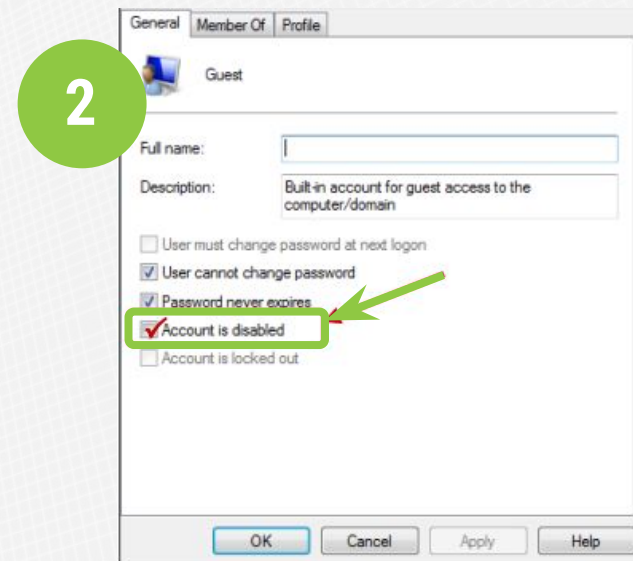
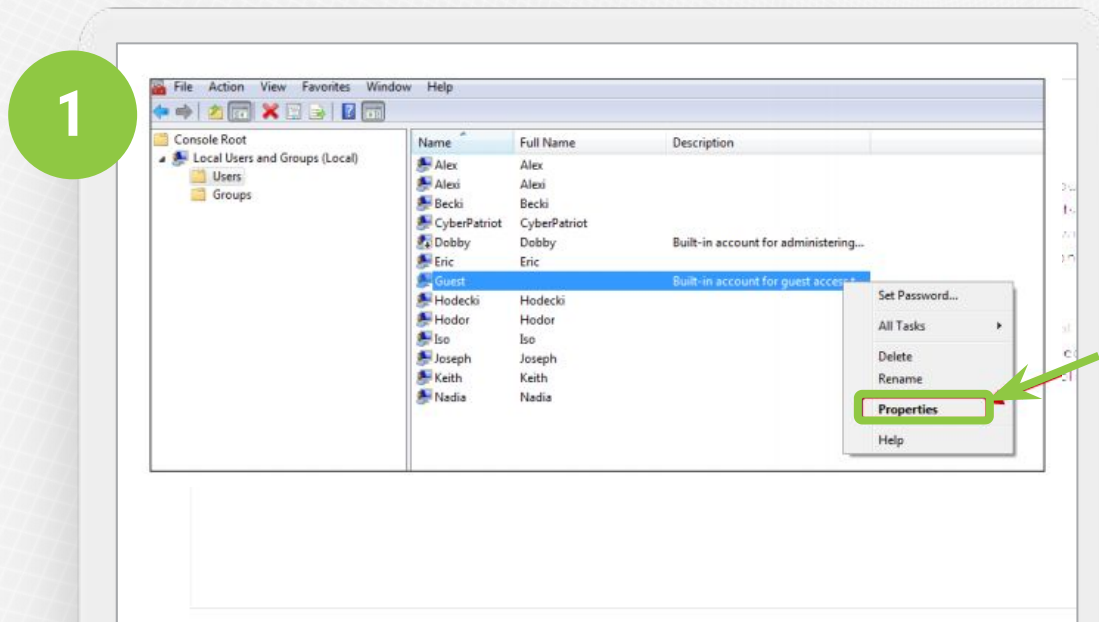
- Add a **password** (Right Click)
- Obfuscate the account by changing the name **Attackers will target** known **Admin accounts** because successfully infiltrating those accounts will give them advanced permissions and access to the network
- **Restrict use** of the account - Use the Properties menu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



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









DISABLE THE GUEST ACCOUNT

CONTROL PANEL OPTION

- Control Panel -> User Accounts -> Add or remove user accounts

1

Choose the account you would like to change


 Hodor Standard user	 Iso Standard user
 Joseph Standard user	 Keith Administrator Password protected
 Nadia Standard user	 Guest Guest account

2

What do you want to change about the guest account?

[Change the picture](#)

[Turn off the guest account](#)


Guest
Guest account

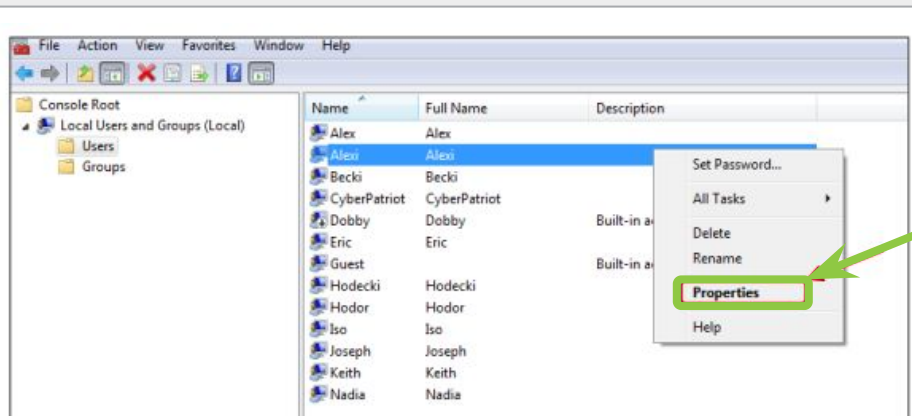
WorkED

RESTRICT ADMINISTRATOR GROUP MEMBERSHIP

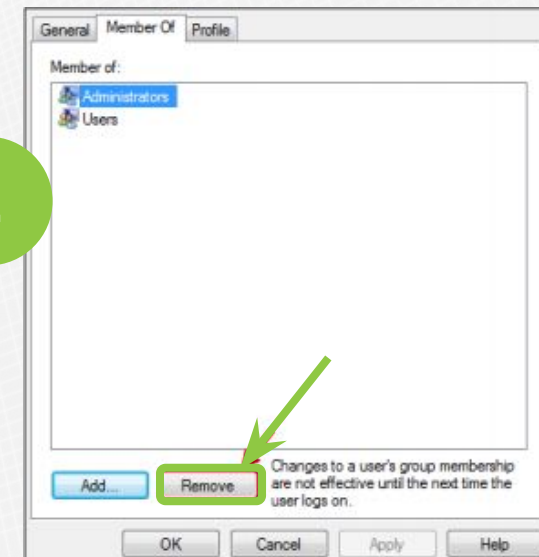
CONSOLE OPTION

- 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




RESTRICT ADMINISTRATOR GROUP MEMBERSHIP

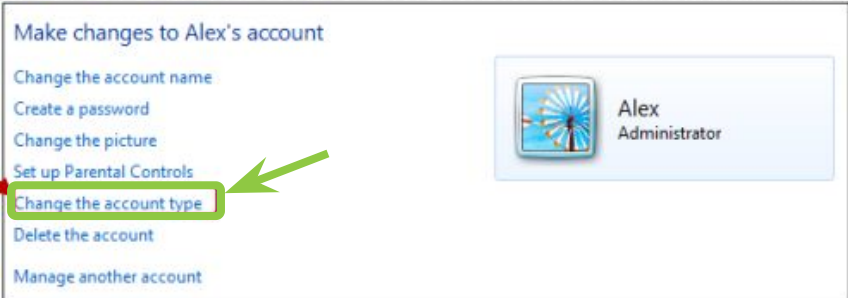
CONTROL PANEL OPTION

- Control Panel -> User Accounts -> Manage another account

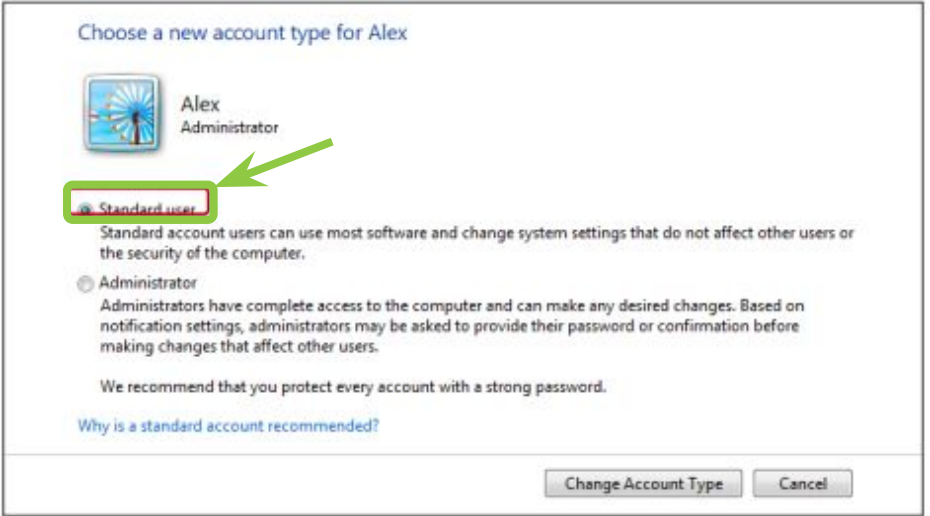
1 Choose the account you would like to change



2 Make changes to Alex's account



3 Choose a new account type for Alex



Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

☐ Administrator
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

[Why is a standard account recommended?](#)

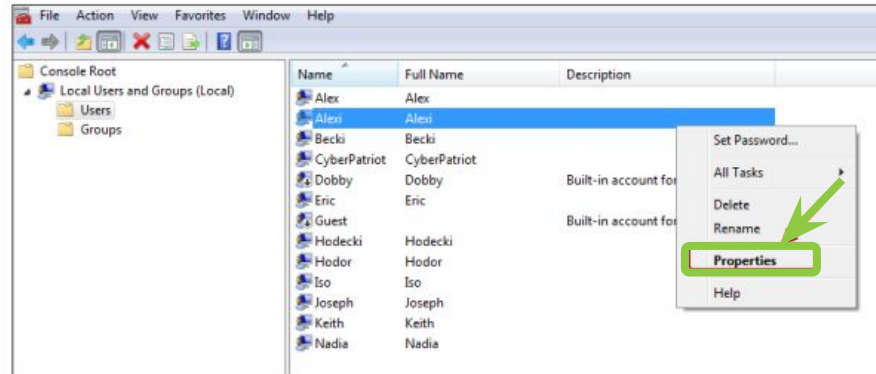
Change Account Type Cancel

SET PASSWORDS FOR ALL ACCOUNTS

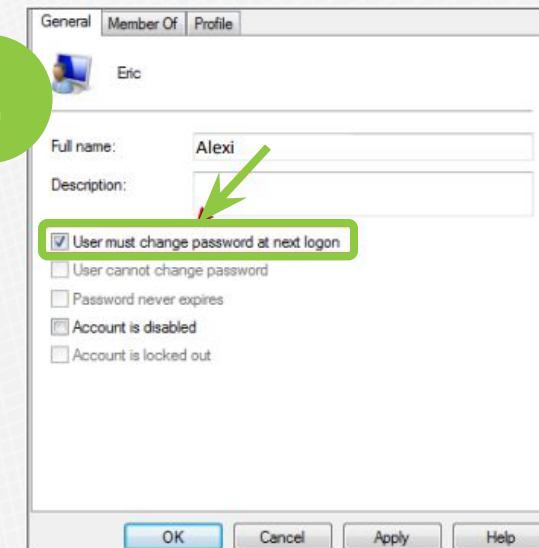
CONSOLE OPTION

- Make sure **all accounts** are password protected

1



2



SET PASSWORDS FOR ALL ACCOUNTS

CONTROL PANEL OPTION

- Control Panel -> User Accounts -> Manage another account

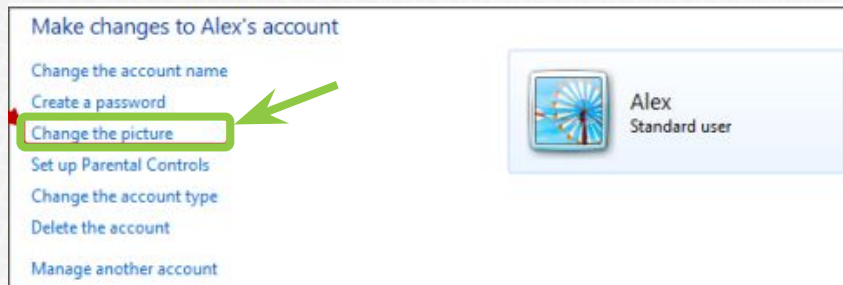
1



3



2

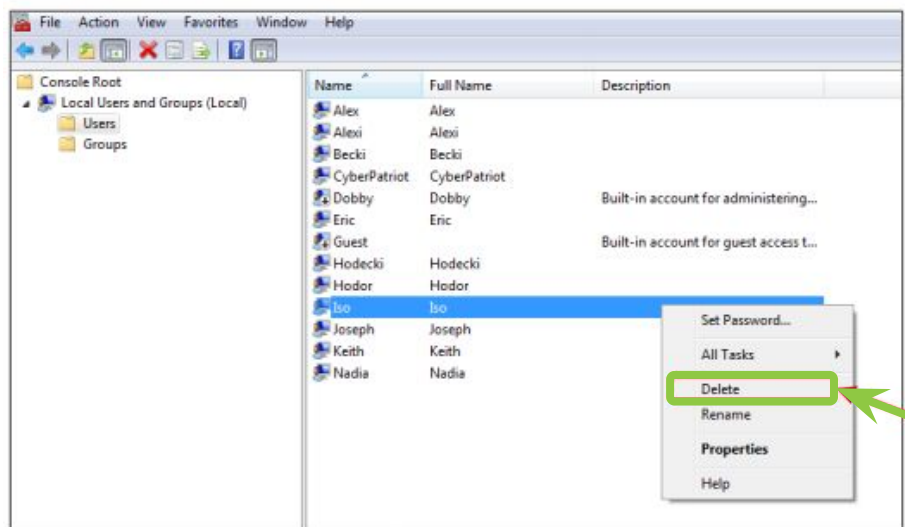


REMOVING USERS

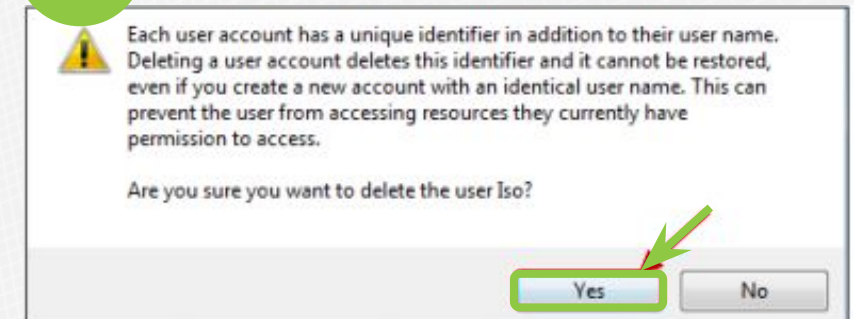
CONSOLE OPTION

- **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

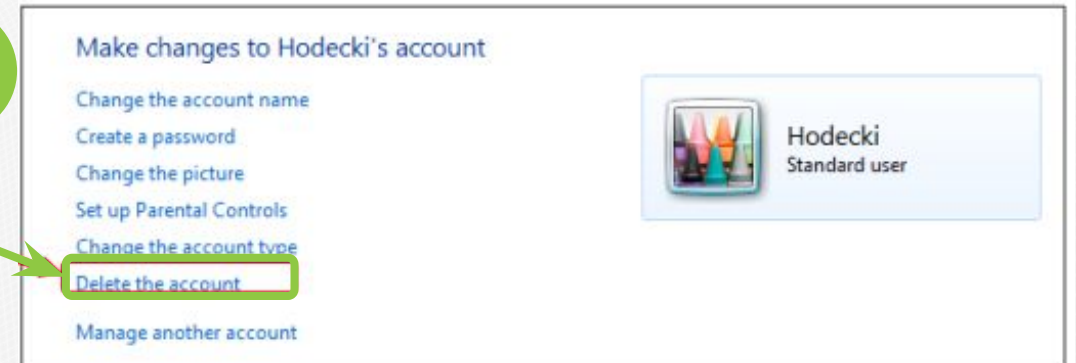
CONTROL PANEL OPTION

- Control Panel -> User Accounts -> Add or remove user accounts

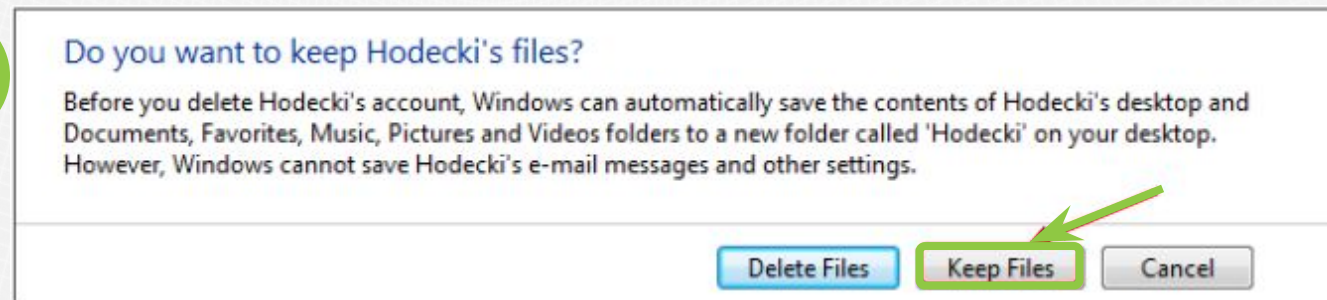
1



2



3

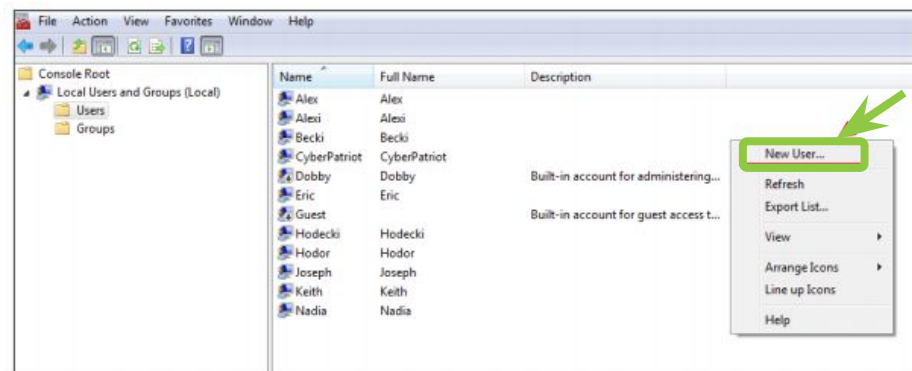


ADDING USERS

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

A screenshot of the 'New User' dialog box in Windows XP. The dialog has fields for 'User name:', 'Full name:', and 'Description:'. Below these are 'Password:' and 'Confirm password:' fields, both masked with dots. At the bottom, there are four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password', 'Password never expires', and 'Account is disabled'. 'Help', 'Create', and 'Close' buttons are at the bottom right.

User name: Hedwig
Full name: Hedwig
Description:
Password:
Confirm password:
☒ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Account is disabled
Help Create Close

ADDING USERS

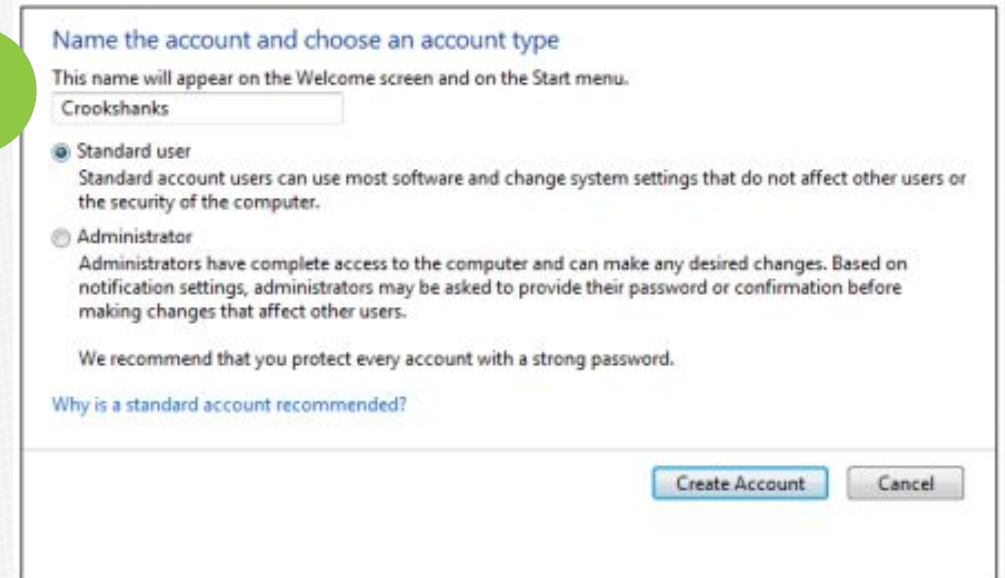
CONTROL PANEL OPTION

- Control Panel -> User Accounts -> Add or remove user accounts

1



2





WorkED

SYSTEM HARDENING

QUESTIONS?

THANK YOU