



AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## UNIT FIVE

### Microsoft Windows Security



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## SECTION ONE

### Basic Security Policies and Tools

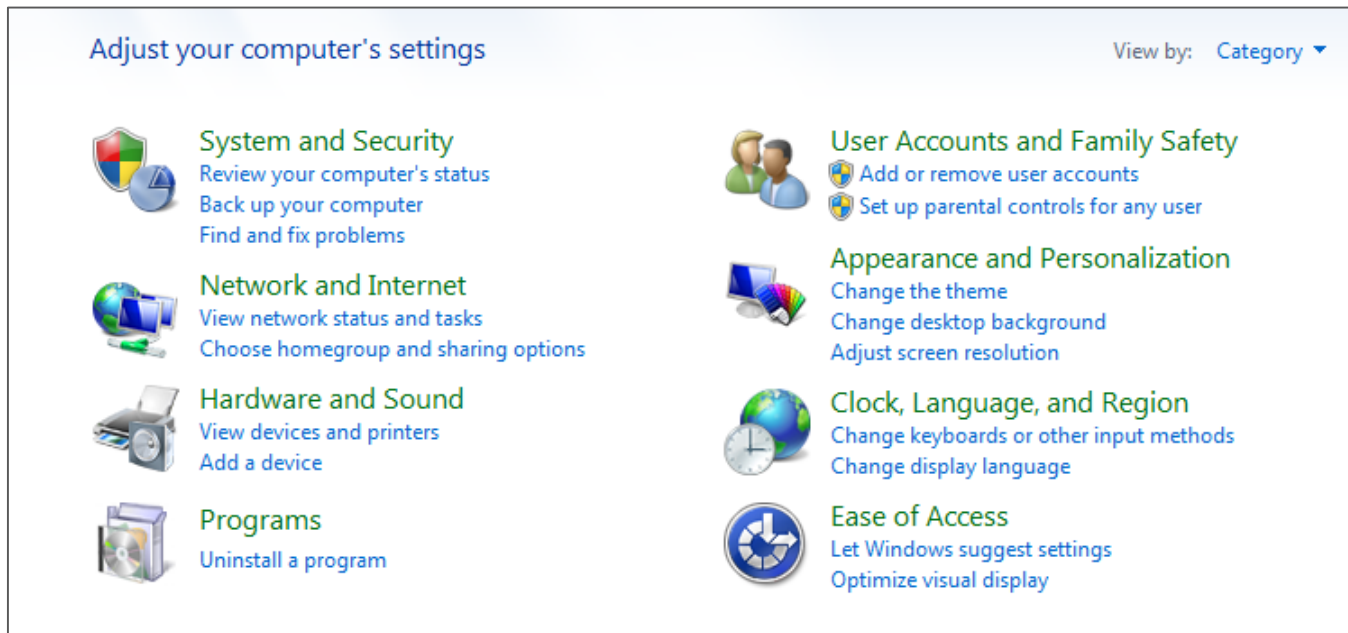


[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



# 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

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration



# Password Policies

- Modify policies to require users create strong passwords
  - Remember CLOUDS Not SUN (Unit Four)
- [Click Account Policies](#) → [Password Policies](#)

## Policies:

**Password history:** the number of old passwords the computer remembers and does not allow a user to reuse

**Maximum password age:** how long a user can keep the same password

**Minimum password age:** how long a user must keep a password before changing it

**Minimum password length:** how many characters passwords must be

**Complexity requirements:** whether users must use at least three of the following in their passwords: upper case letters, lower case letters, numbers, symbols

**Reversible encryption:** whether the password file on the computer can be decrypted

## Recommended settings:

5 passwords remembered

90 days for users, 30 for admins

10-30 days

8 characters

Enable

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:

**Account lockout duration:** the number of minutes a locked-out account remains locked before automatically becoming unlocked

**Account lockout threshold:** the number of failed logon attempts that causes a user account to be locked out

**Reset account lockout counter after:** the number of minutes that must elapse before the failed logon attempt threshold counter is reset to 0

## Recommended settings:

30 minutes

3-10 invalid login attempts

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

Review recent messages and resolve problems  
Action Center has detected one or more issues for you to review.

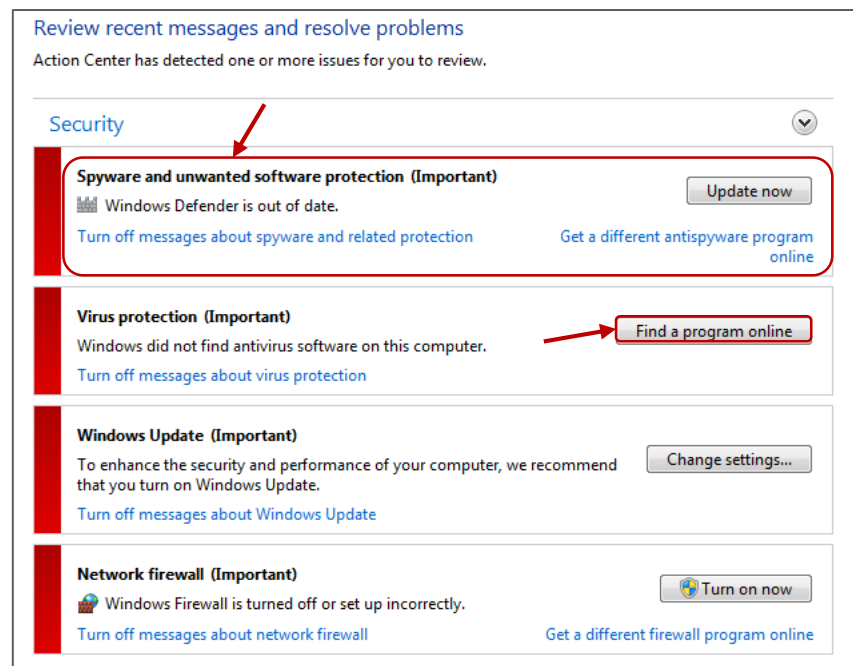
**Security**

- Spyware and unwanted software protection (Important)**  
Windows Defender is out of date.  
[Update now](#)  
[Turn off messages about spyware and related protection](#) [Get a different antispysware program online](#)
- Virus protection (Important)**  
Windows did not find antivirus software on this computer.  
[Find a program online](#)  
[Turn off messages about virus protection](#)
- Windows Update (Important)**  
To enhance the security and performance of your computer, we recommend that you turn on Windows Update.  
[Change settings...](#)  
[Turn off messages about Windows Update](#)
- Network firewall (Important)**  
Windows Firewall is turned off or set up incorrectly.  
[Turn on now](#)  
[Get a different firewall program online](#)



# Windows Defender and Anti-Malware

- Control Panel → System and Security → Action Center
- 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.

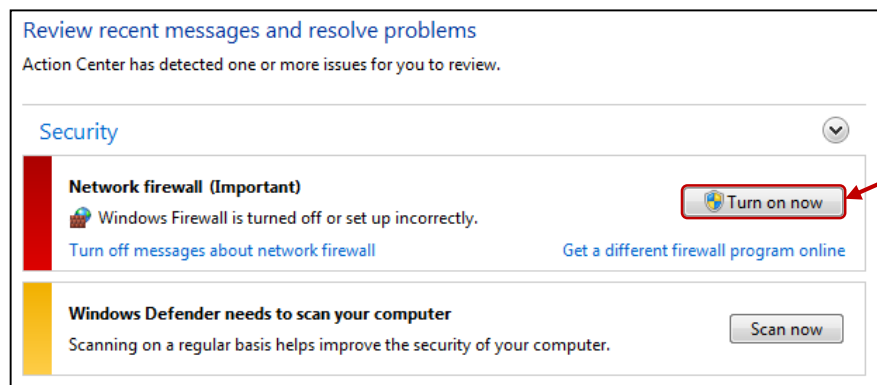
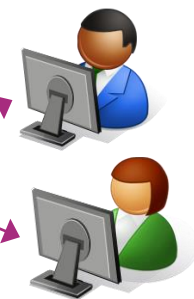
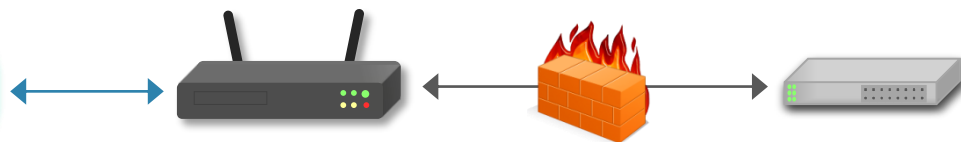






# Firewalls

- 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 → Action Center → 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)

Control Panel Home

- Allow a program or feature through Windows Firewall
- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network

### Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?  
What are network locations?

**Update your Firewall settings**  
Windows Firewall is not using the recommended settings to protect your computer. [Use recommended settings](#)  
[What are the recommended settings?](#)

**Home or work (private) networks** Not Connected

**Public networks** Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: Off  
Block all connections to programs that are not on the list of allowed programs

Incoming connections:  Block all incoming connections, including those in the list of allowed programs

Active public networks: Network 10

Notification state: Notify me when Windows Firewall blocks a new program

### Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

#### Domain network location settings

Turn on Windows Firewall  
 Block all incoming connections, including those in the list of allowed programs  
 Notify me when Windows Firewall blocks a new program

Turn off Windows Firewall (not recommended)

#### Home or work (private) network location settings

Turn on Windows Firewall  
 Block all incoming connections, including those in the list of allowed programs  
 Notify me when Windows Firewall blocks a new program

Turn off Windows Firewall (not recommended)

#### Public network location settings

Turn on Windows Firewall  
 Block all incoming connections, including those in the list of allowed programs  
 Notify me when Windows Firewall blocks a new program

Turn off Windows Firewall (not recommended)



# 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.

Control Panel Home

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

**Domain networks** Connected

Networks at a workplace that are attached to a domain

Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on the list of allowed programs

Active domain networks: afa.org

Notification state: Notify me when Windows Firewall blocks a new program

**Home or work (private) networks** Not Connected

**Public networks** Connected

Networks in public places such as airports or coffee shops

Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on the list of allowed programs

Active public networks: Unidentified network

Notification state: Notify me when Windows Firewall blocks a new program

2.

Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

**Change settings**

Allowed programs and features:

Name	Domain	Home/Work (Private)	Public
<input type="checkbox"/> BranchCache - Content Retrieval (Uses HTTP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Hosted Cache Client (Uses HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Hosted Cache Server (Uses HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Peer Discovery (Uses WSD)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Connect to a Network Projector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Core Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Distributed Transaction Coordinator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> File and Printer Sharing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> HomeGroup	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> iSCSI Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Key Management Service	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Media Center Extenders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Details... Remove

Allow another program...



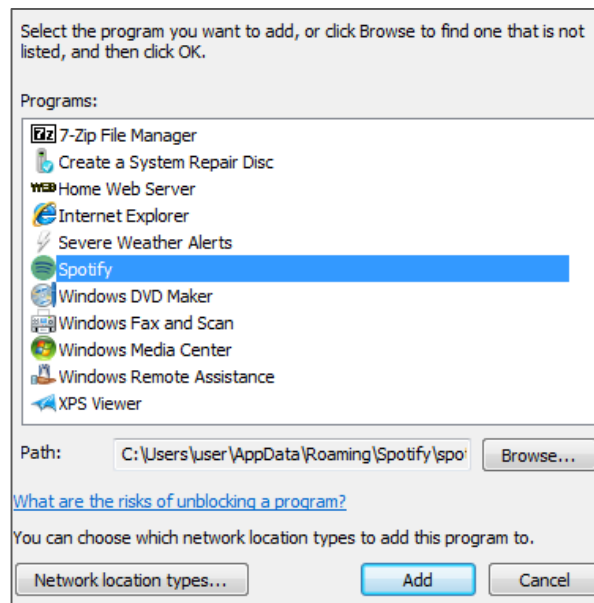
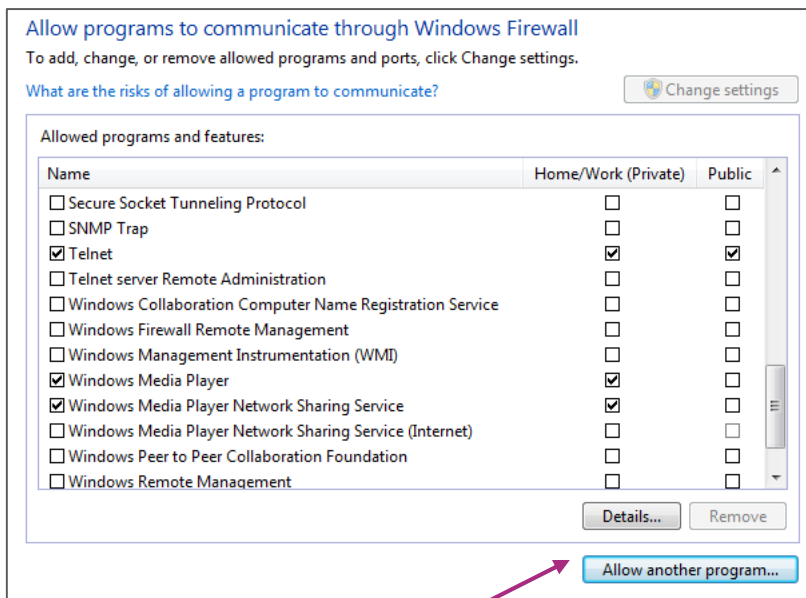
# Common Exceptions

- **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

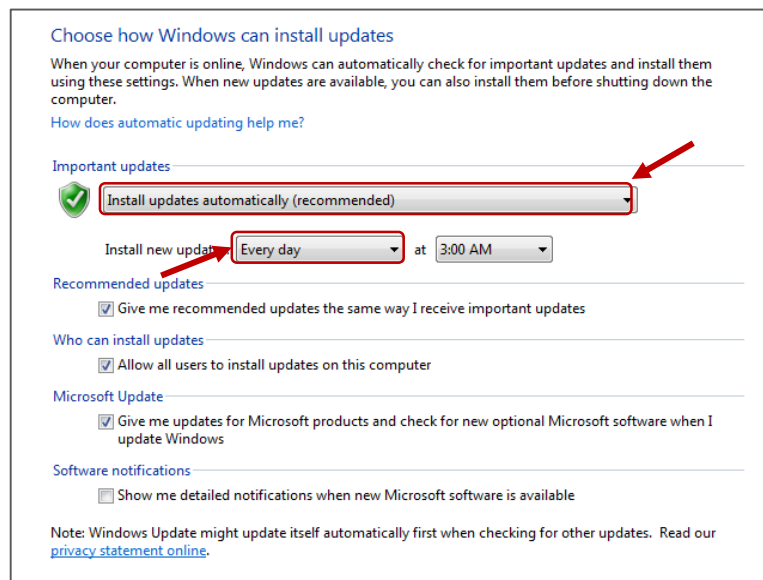
- If the program you want to allow through your firewall does not already appear on your exceptions list, click the “Allow another program” and select the program from the menu





# 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





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## SECTION TWO

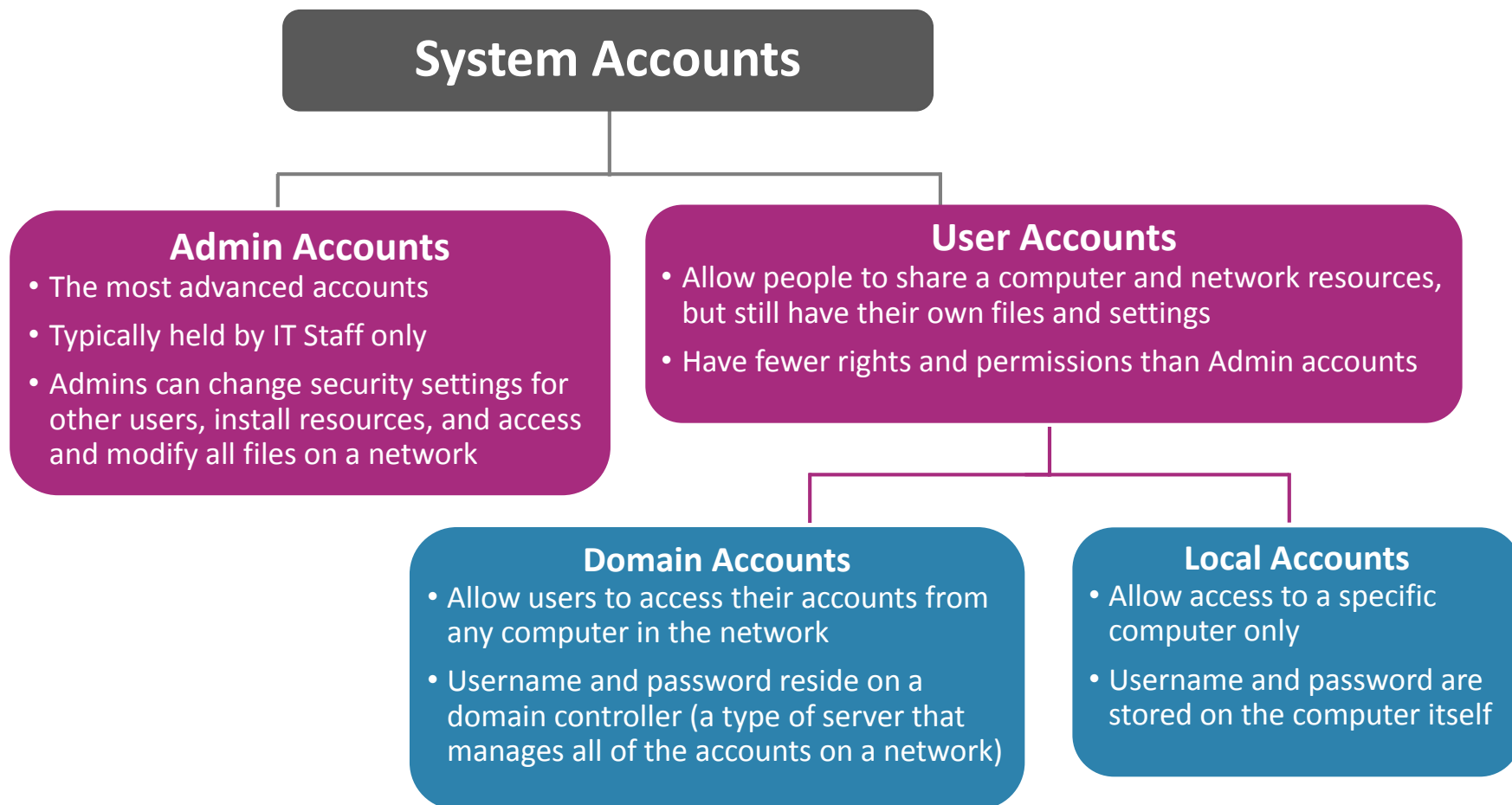
### Account Management



[www.uscyberpatriot.org](http://www.uscyberpatriot.org)



# Account Groups

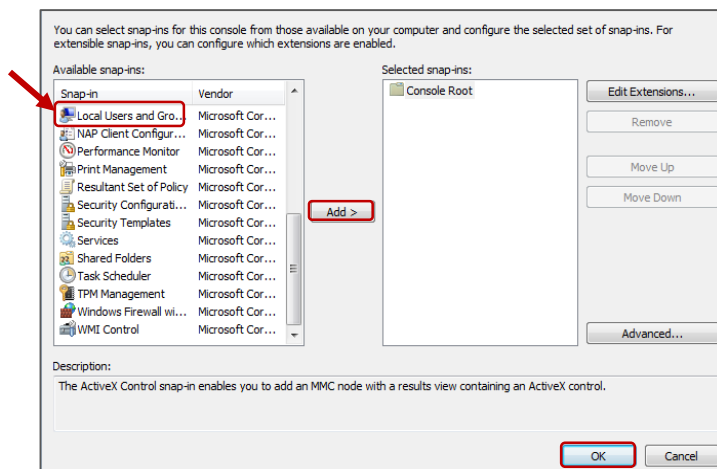






# Local Users and Groups Console

- 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”

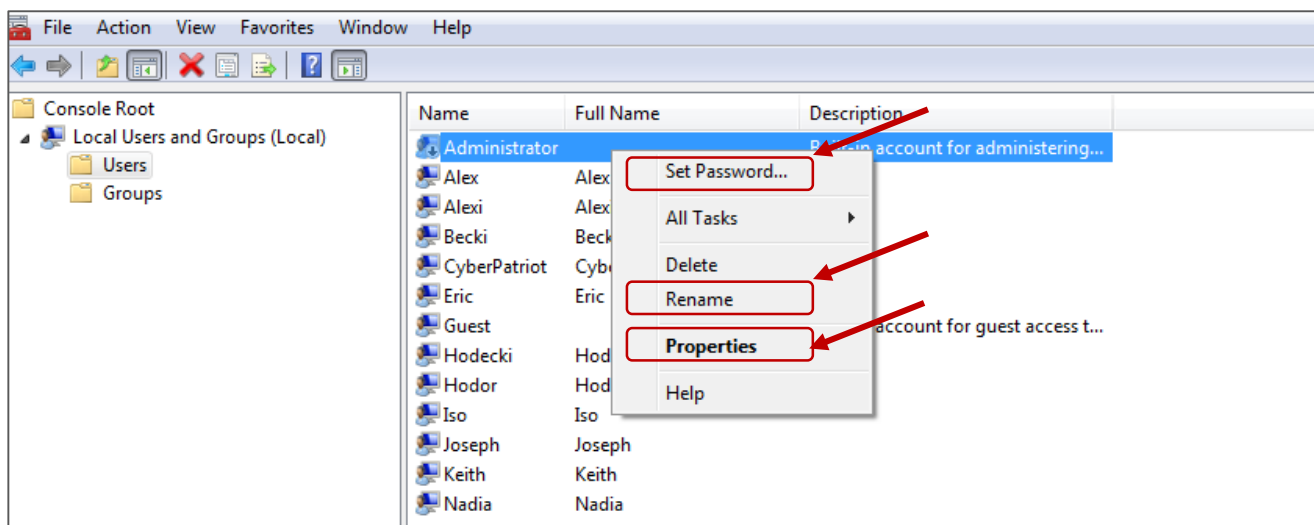


\*The following slides will show you how to control user access through Control Panel and through the Local Users and Groups Console. Other methods exist and you can choose which to use based on personal preference.



# Best Practice: Secure the Built-in Administrator Account

- Add a password
- Obfuscate 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

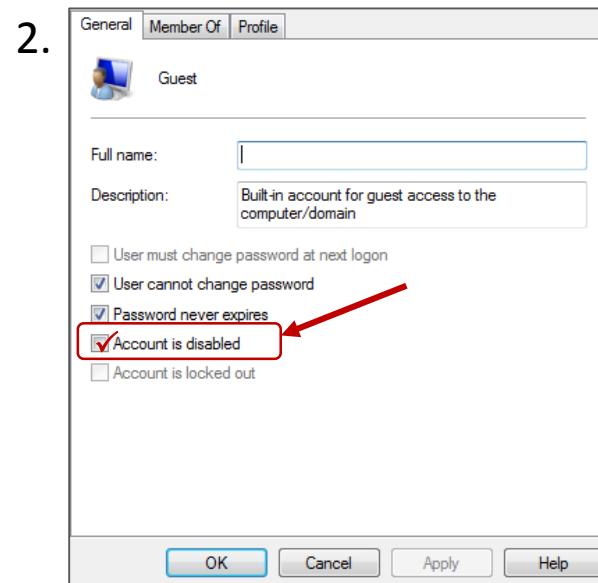
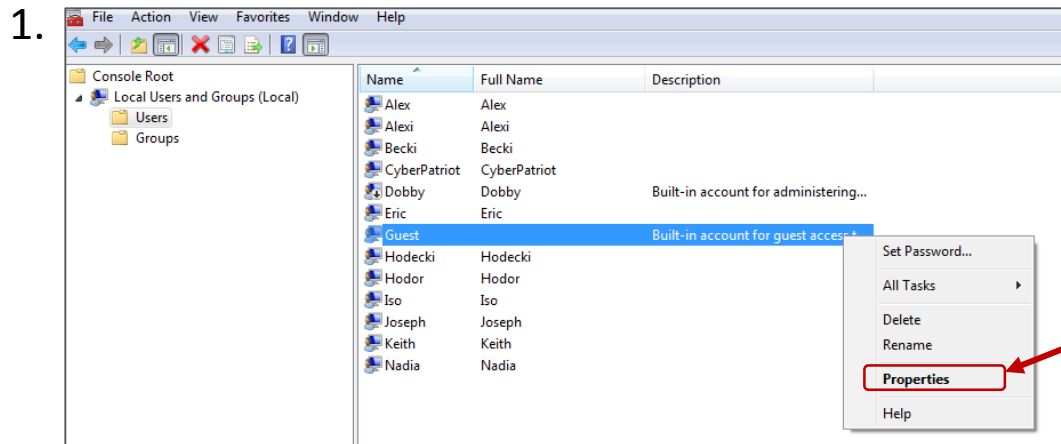




# Best Practice: Disable the Built-in Guest Account

## 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











# Best Practice: 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?

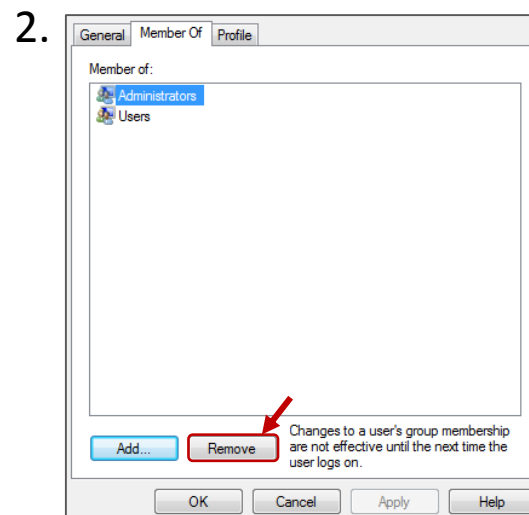
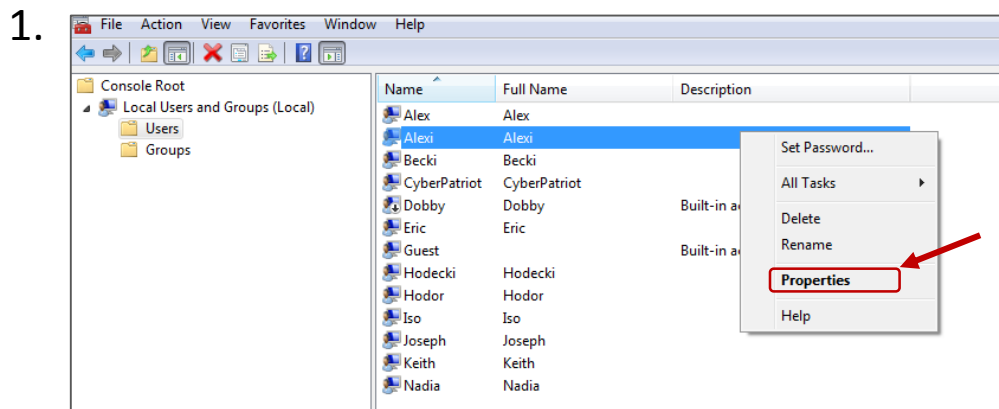
<p>Change the picture</p> <p>Turn off the guest account</p>	 Guest Guest account
---	---



# 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





# Best Practice: Restrict Administrator Group Membership

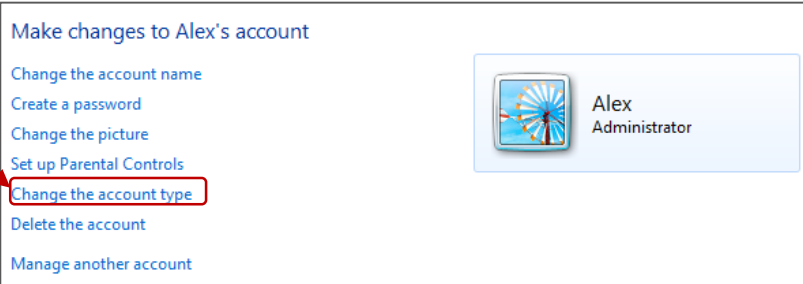
## Control Panel option:

- Control Panel → User Accounts → Manage another account

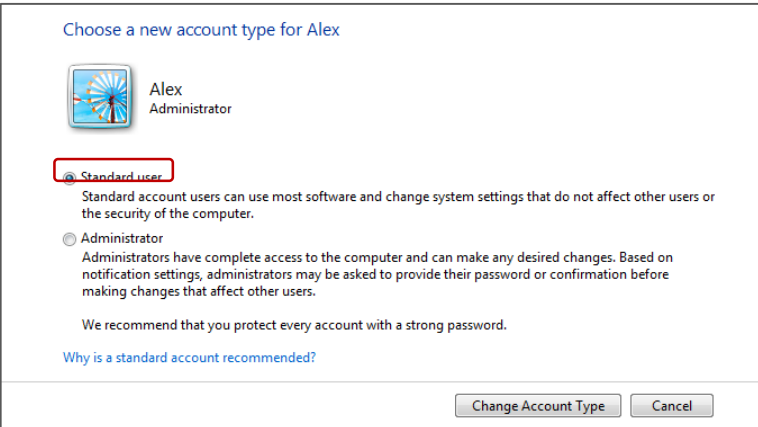
1. Choose the account you would like to change



2. Make changes to Alex's account



3. Choose a new account type for Alex

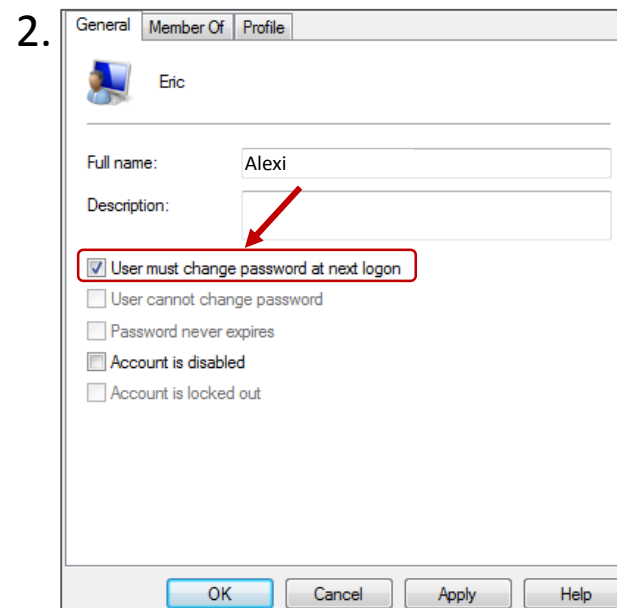
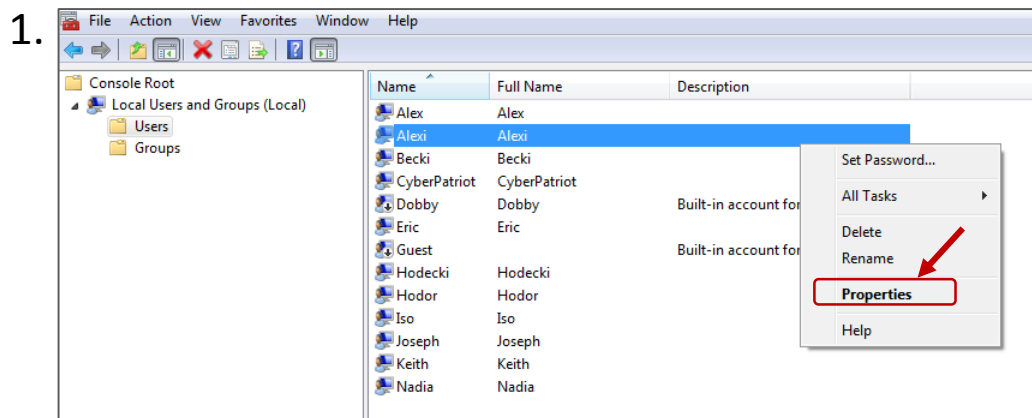




# Best Practice: Set Passwords for all Accounts

## Console option:

- Make sure all accounts are password protected

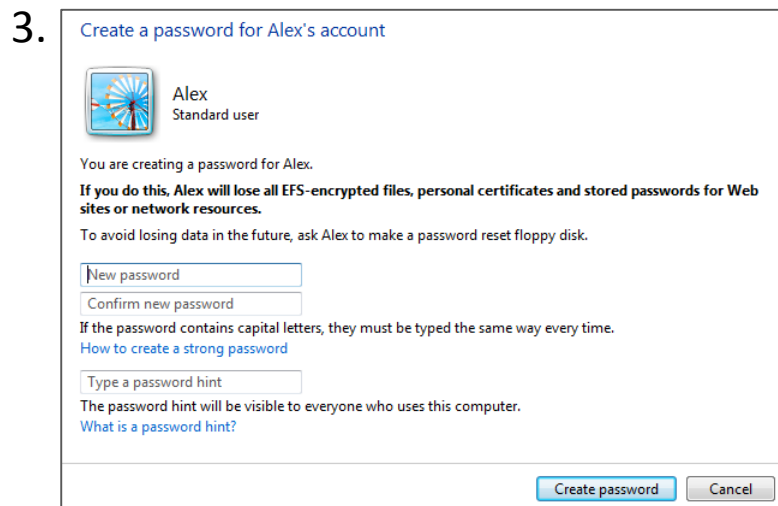
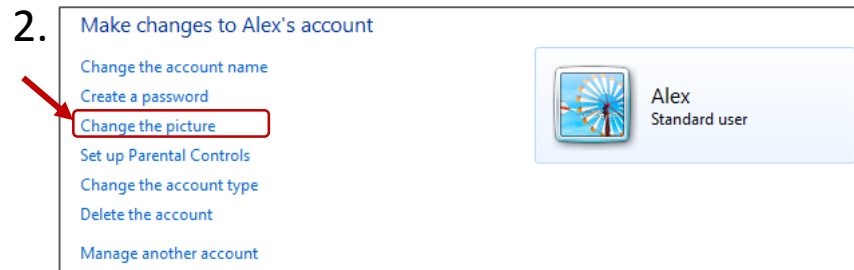




# Best Practice: Set Passwords for all Accounts

## Control Panel option:

- Control Panel → User Accounts → Manage another account



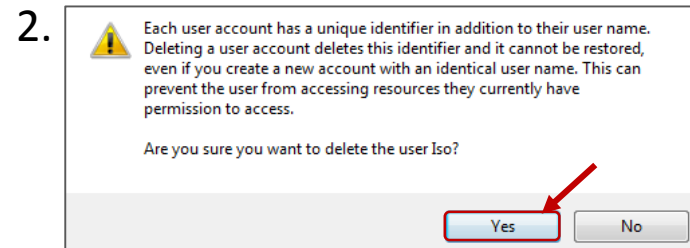
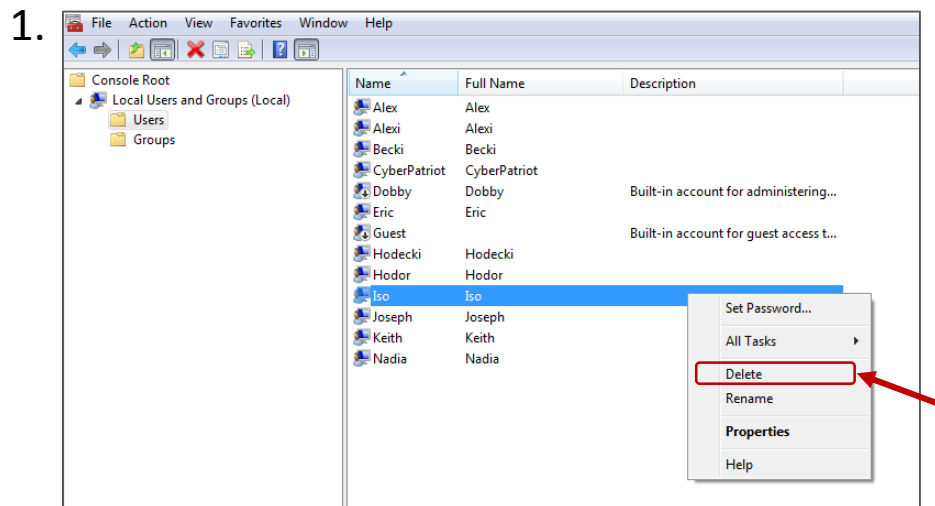




# Removing Users

## 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









# Removing Users

## Control Panel option:


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

1. Choose the account you would like to change

 Eric Administrator Password protected	 Hedwig Standard user Password protected
 Hodecki Standard user	 Hodor Standard user

2. Make changes to Hodecki's account

- Change the account name
- Create a password
- Change the picture
- Set up Parental Controls
- Change the account type
- Delete the account
- Manage another account

 Hodecki  
Standard user

3. Do you want to keep Hodecki's files?

Before you delete Hodecki's account, Windows can automatically save the contents of Hodecki's desktop and Documents, Favorites, Music, Pictures and Videos folders to a new folder called 'Hodecki' on your desktop. However, Windows cannot save Hodecki's e-mail messages and other settings.

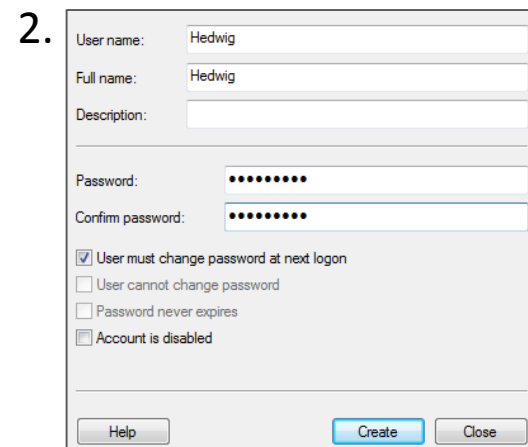
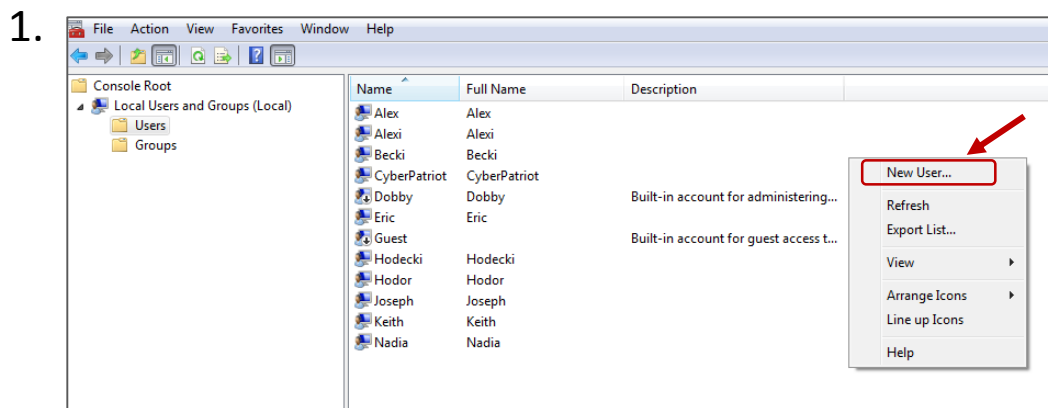
Delete Files   **Keep Files**   Cancel



# 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

## Control Panel option:

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

### 1. Choose the account you would like to change

CyberPatriot  
Administrator

Alex  
Standard user  
Password protected

Alexi  
Standard user  
Password protected

Becki  
Standard user

Eric  
Administrator  
Password protected

Hedwig  
Standard user  
Password protected

**Create a new account**  
What is a user account?

### 2. Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

Crookshanks

Standard user

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?](#)

Create Account

Cancel