AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## UNIT SEVEN

# Microsoft Windows Security Tools

www.uscyberpatriot.org

# Learning Objectives

- Participants will understand where basic Windows operating system security tools are located
  - Control Panel
  - Administrative Tools
  - Action Center
  - Windows Firewall
  - Windows Update
- Participants will learn how to manage Windows accounts and how accounts can affect security

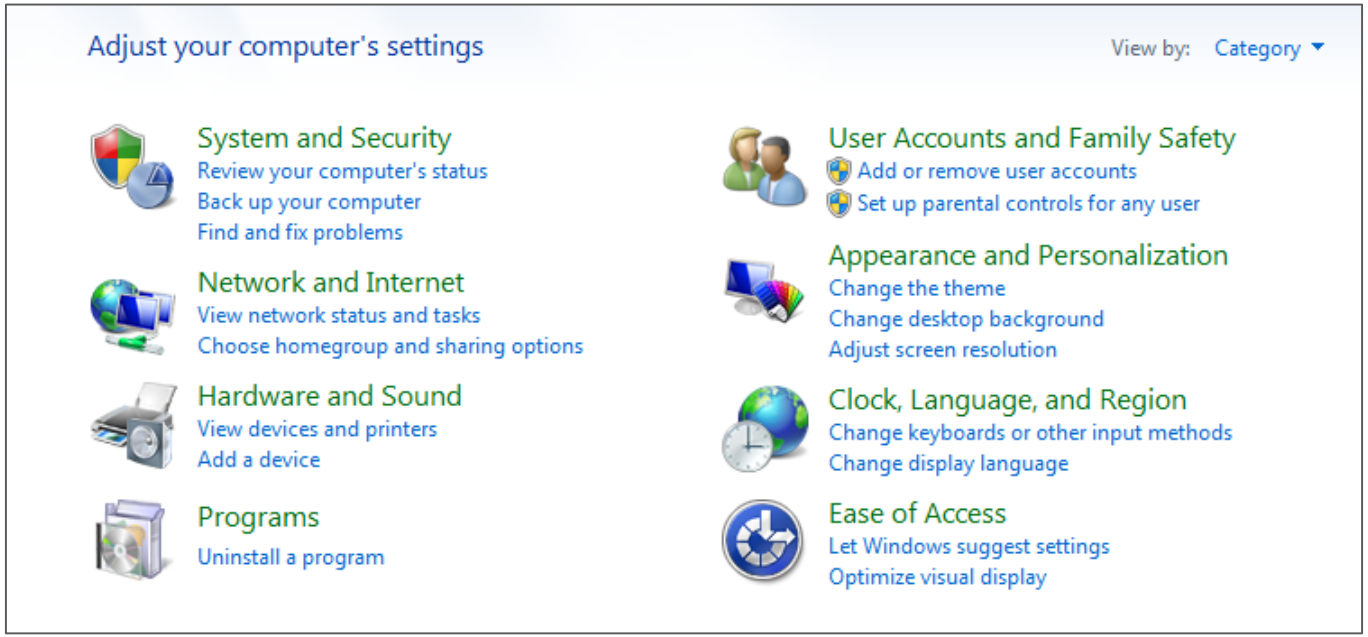
© Air Force Association

## SECTION ONE

# Basic Security Policies and Tools

# Control Panel

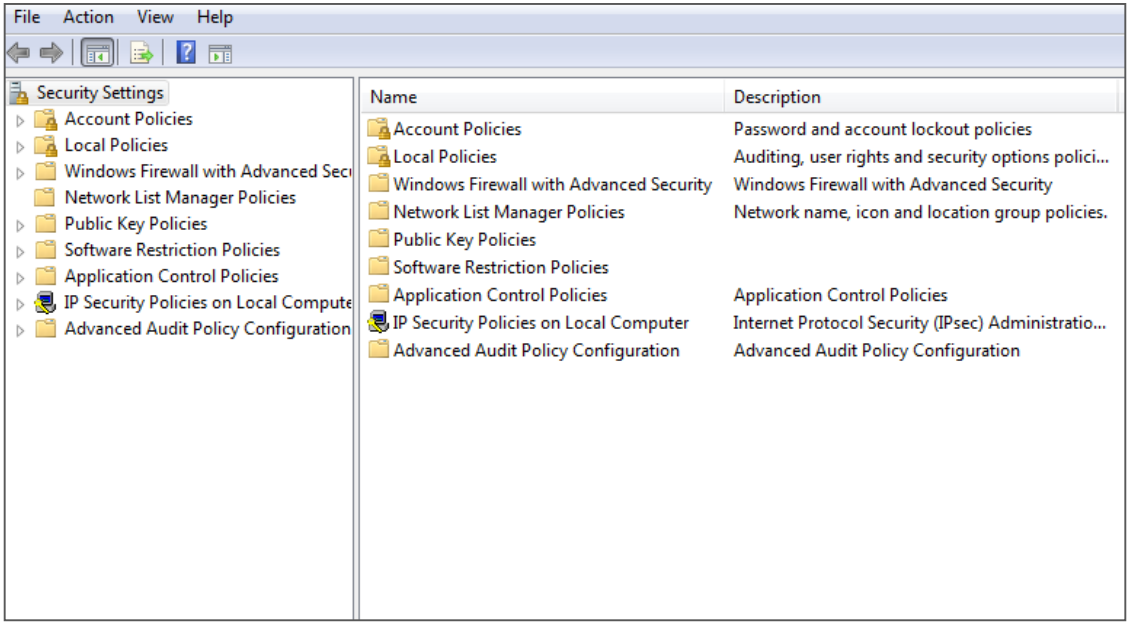
- Where many of the basic system changes and configurations can be set within a Windows operating system
- Click Start → Control Panel




© Air Force Association

# Basic Local Security Policies

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




© Air Force Association

# 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 |

© Air Force Association

# 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

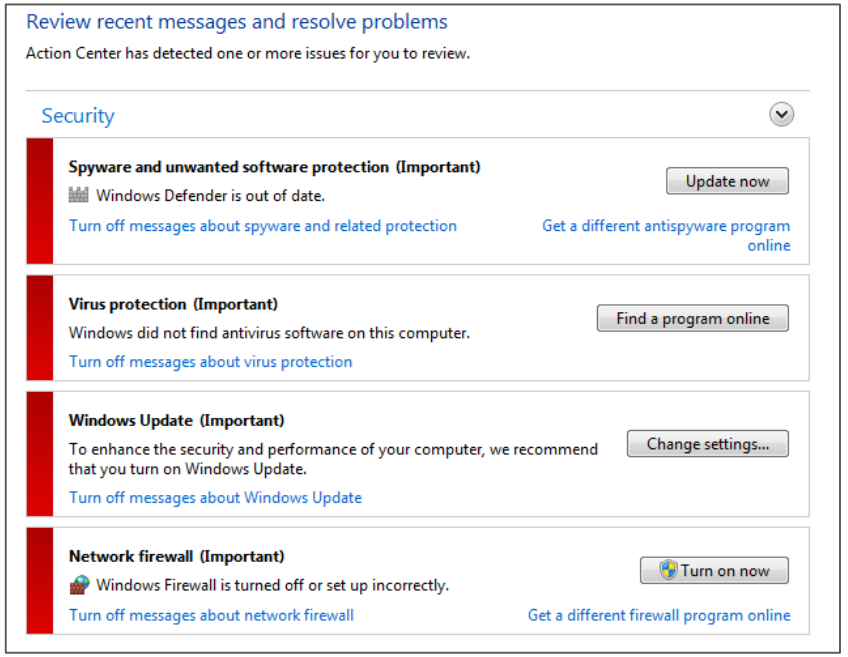
| Policies: | Recommended settings: |
| --- | --- |
| Account lockout duration: the number of minutes a locked-out account remains locked before automatically becoming unlocked | 30 minutes |
| Account lockout threshold: the number of failed logon attempts that causes a user account to be locked out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

© Air Force Association

# Action Center

- Click Start → Control Panel → System and Security → Action Center
- Notifies you if Windows identifies problems with or updates for:

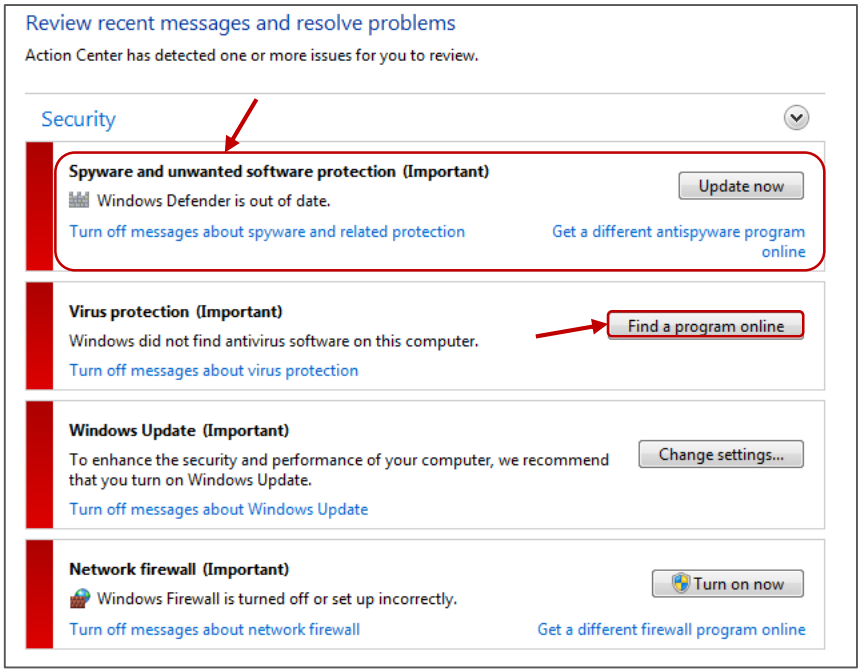
  - Windows Updates
  - Internet security settings
  - Network firewall
  - Spyware and related protection
  - User Account Control
  - Virus protections
  - Windows Backups
  - Windows Troubleshooting




© Air Force Association

# Windows Defender and Anti-Malware

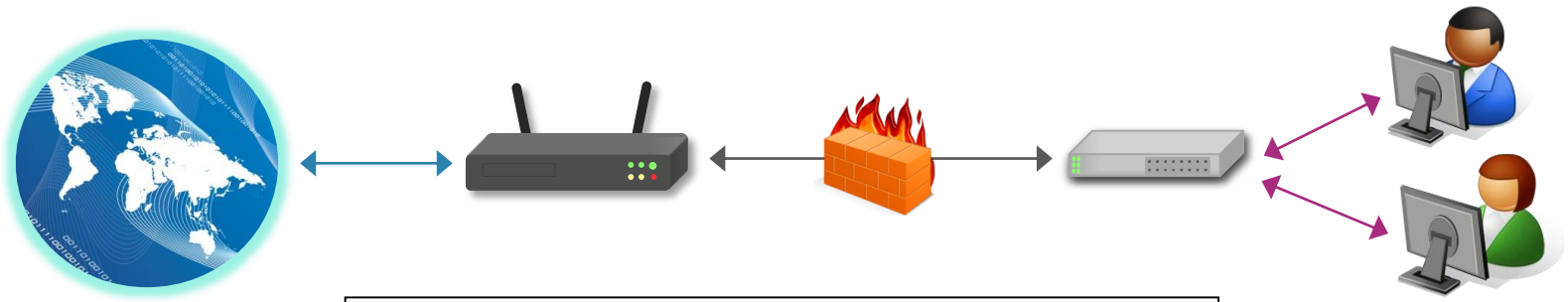
- Control Panel → System and Security → Action Center
- Anti-malware programs should be updated regularly
- Windows Defender is a very basic built-in spyware protection program in Windows
  - It only protects against known spyware, not viruses, worms or other malware
- Download a supplementary anti-virus 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

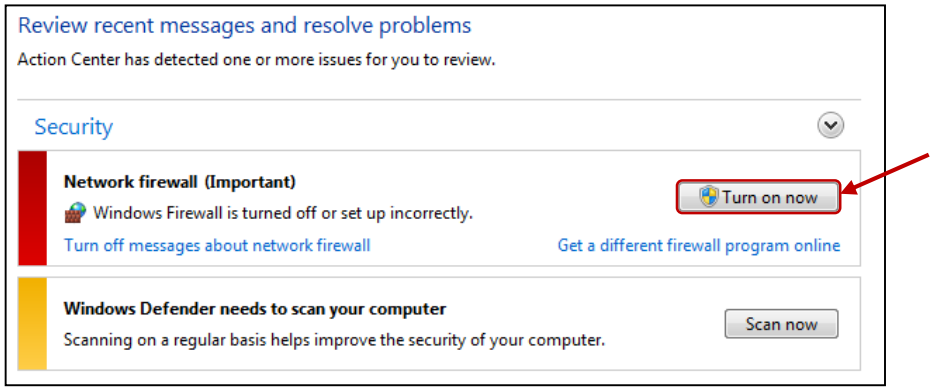



© Air Force Association

# 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

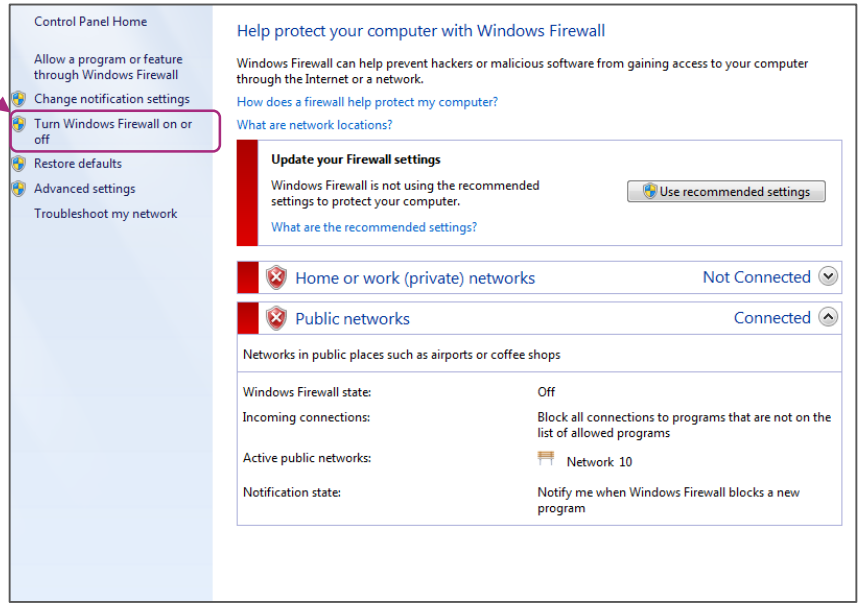


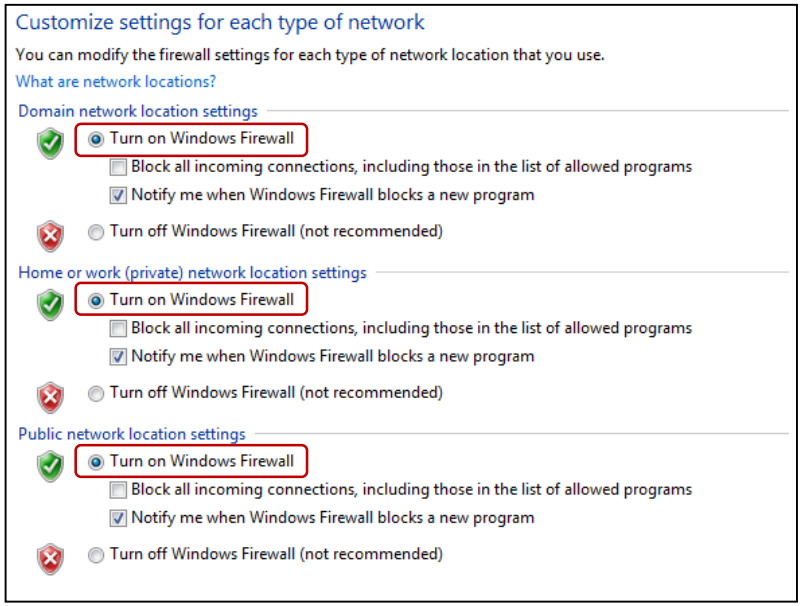



© Air Force Association

# 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)



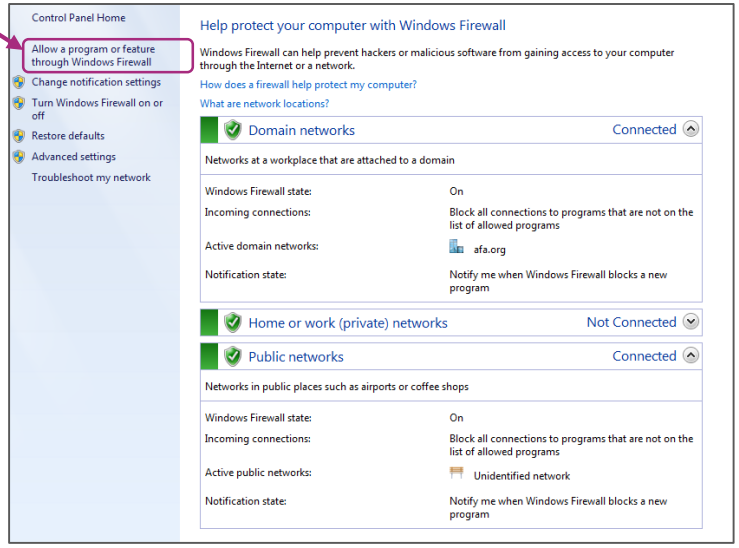




© Air Force Association

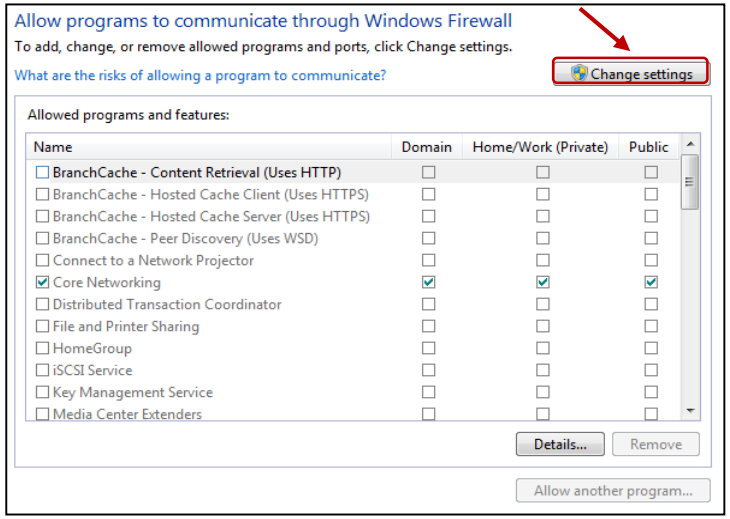
# Enabling Windows Firewall Exceptions

- 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.




© Air Force Association

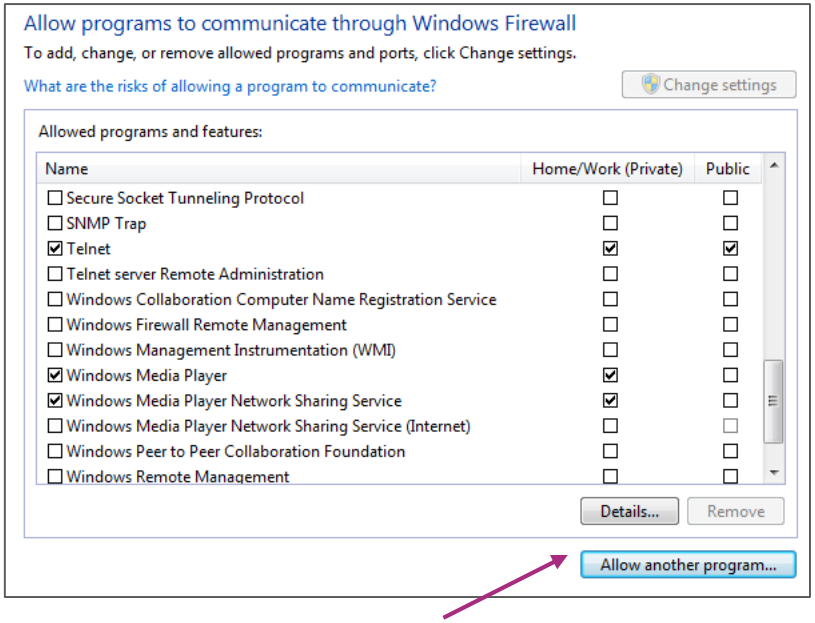
# Common Exceptions

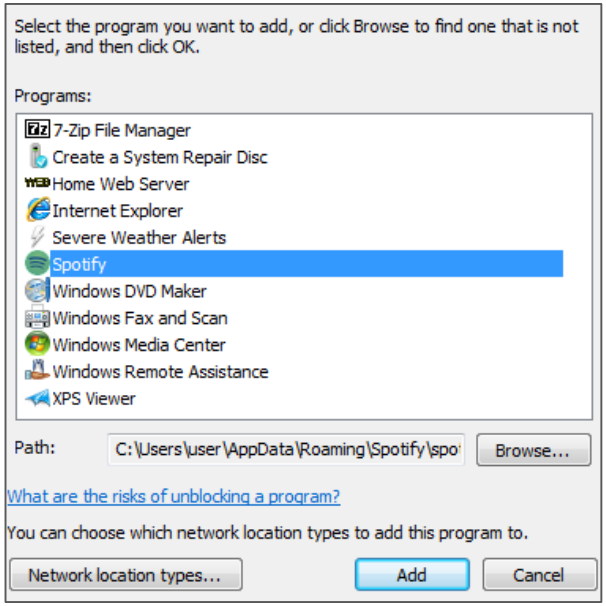
- Core Networking
  - Regular Microsoft Windows services that retrieve data from the Internet
  - If you don't enable this exception across all three types of networks, some Microsoft services and programs will not run properly
- File and Printer Sharing
  - Allows you to share the contents of selected 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

© Air Force Association

# 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

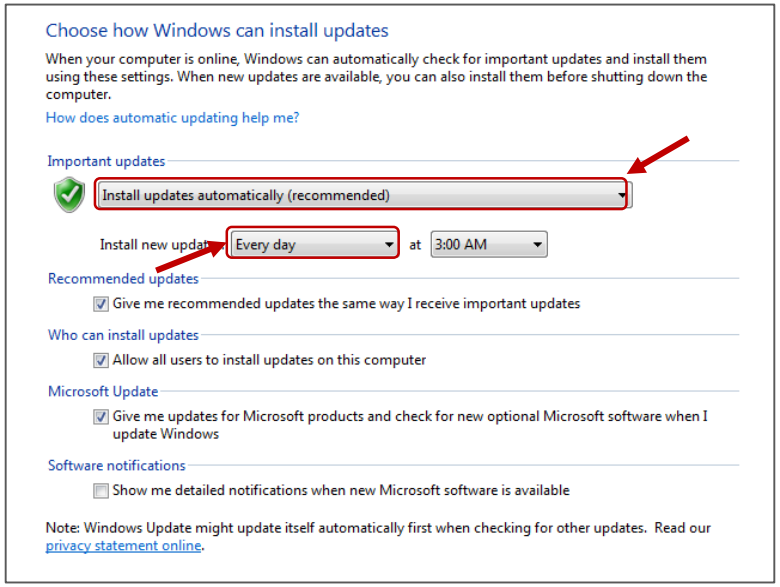



© Air Force Association

# 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

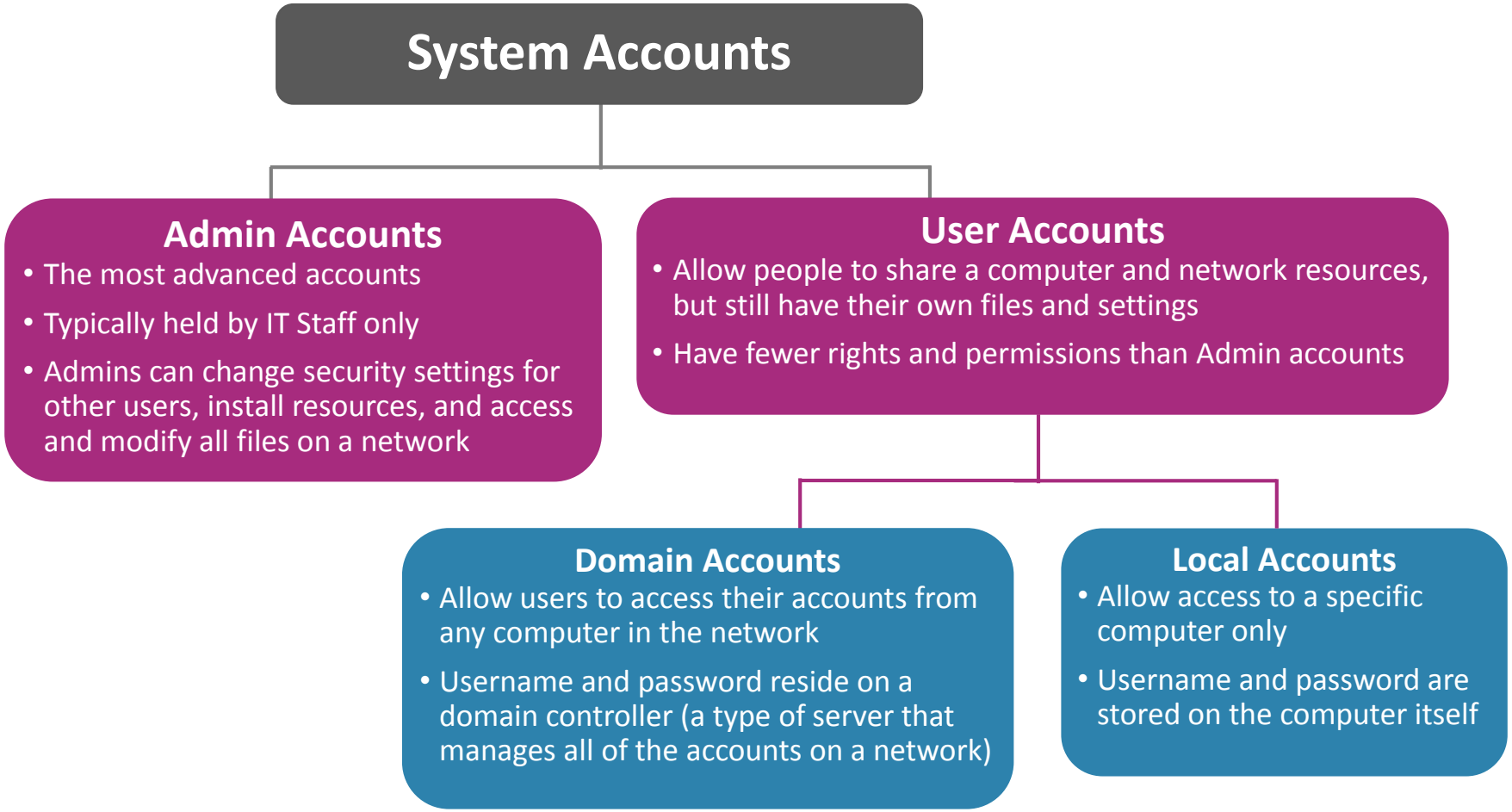



© Air Force Association

# SECTION TWO

## Account Management

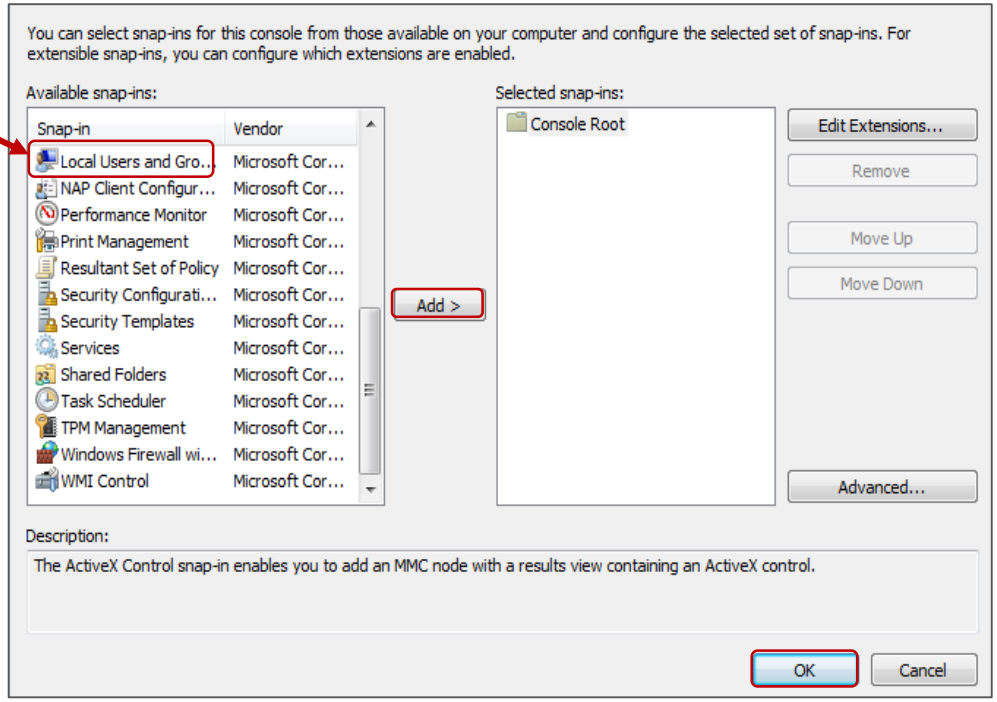
# Account Groups




© Air Force Association

# 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"

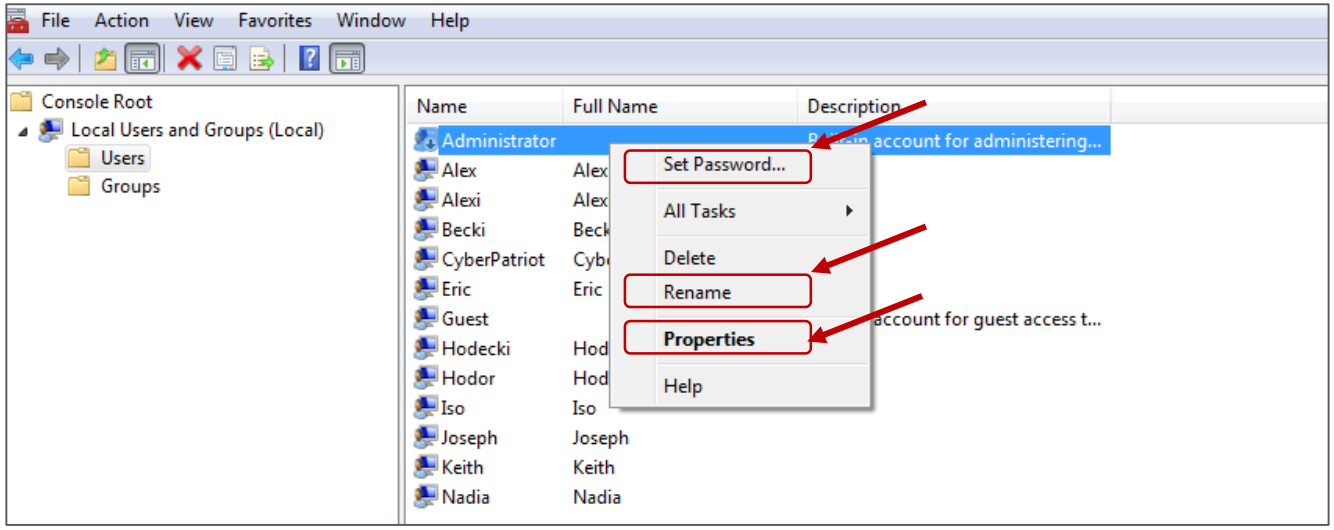



*The following slides will show you how to control user access through Control Panel and through the Local Users and Groups Console. Other methods exist and you can choose which to use based on personal preference.

© Air Force Association

# 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



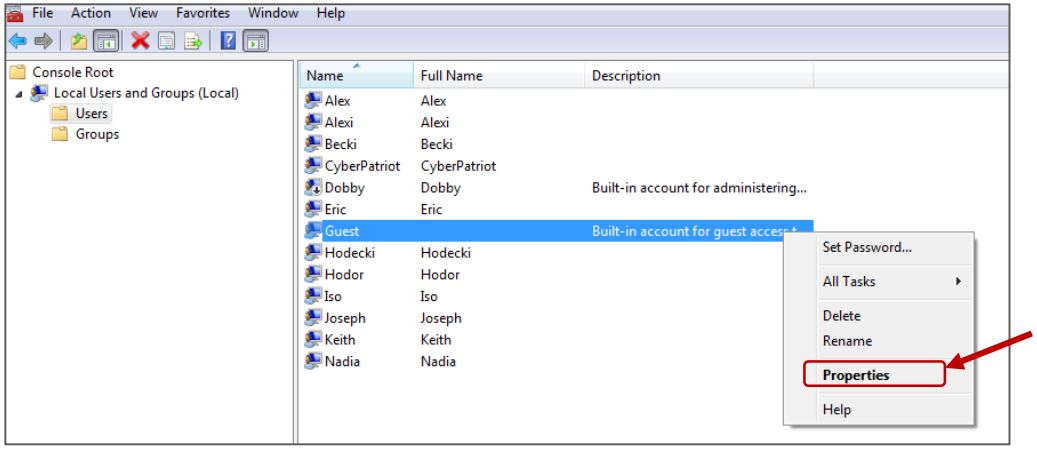

© Air Force Association

# Best Practice: Disable the Built-in Guest Account

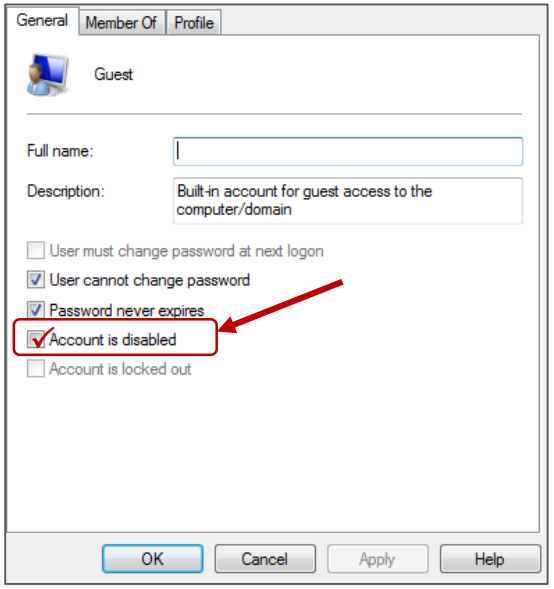
**Console option:**

- 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.



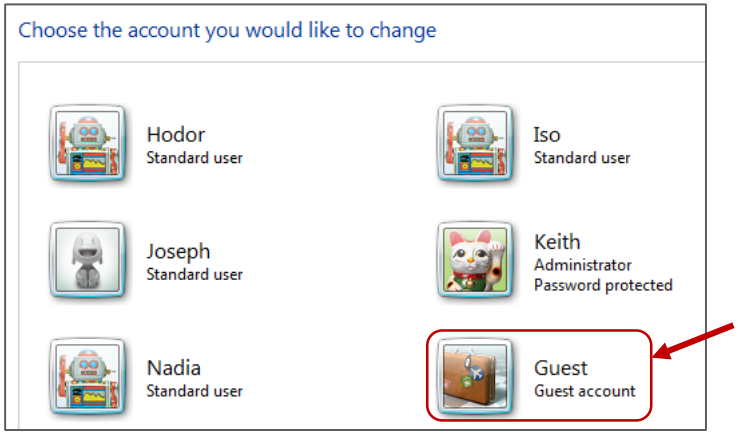

© Air Force Association

# Best Practice: Disable the Built-in Guest Account

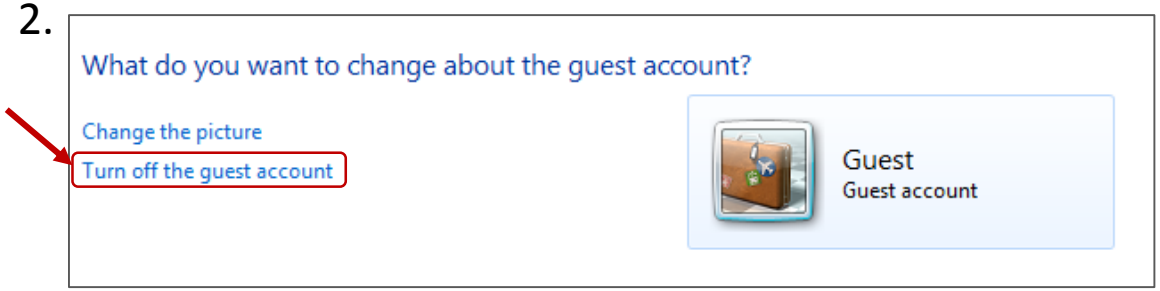
**Control Panel option:**

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

1.




2.



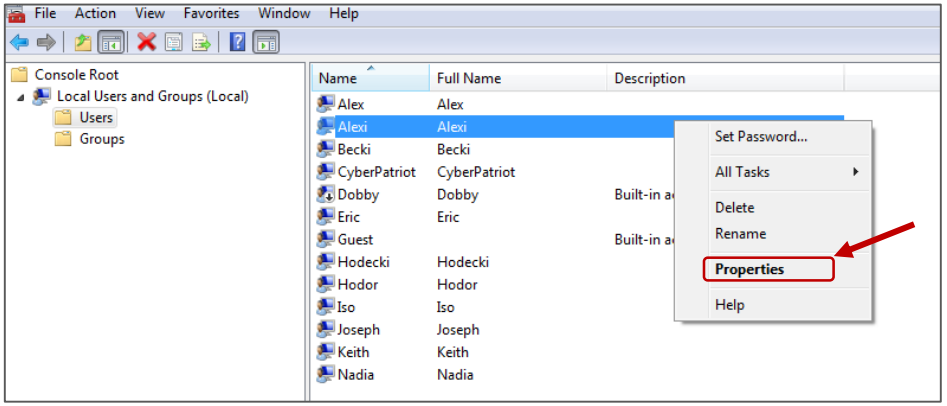

© Air Force Association

# Best Practice: Restrict Administrator Group Membership

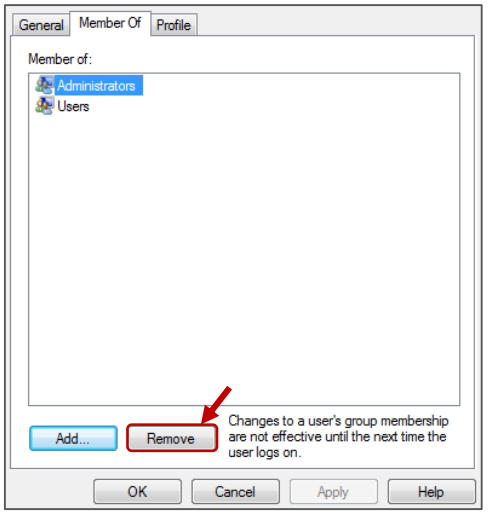
**Console option:**

- 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.




© Air Force Association

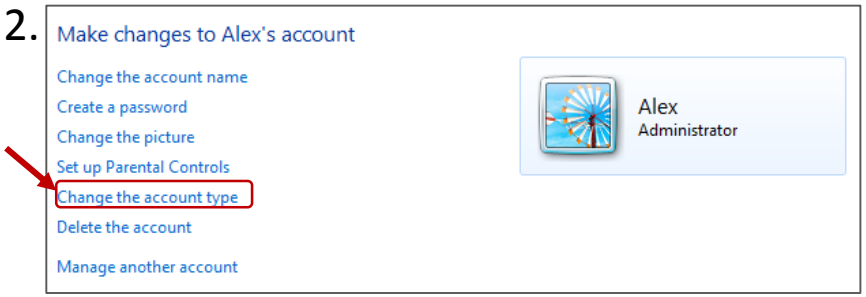
# Best Practice: Restrict Administrator Group Membership

**Control Panel option:**

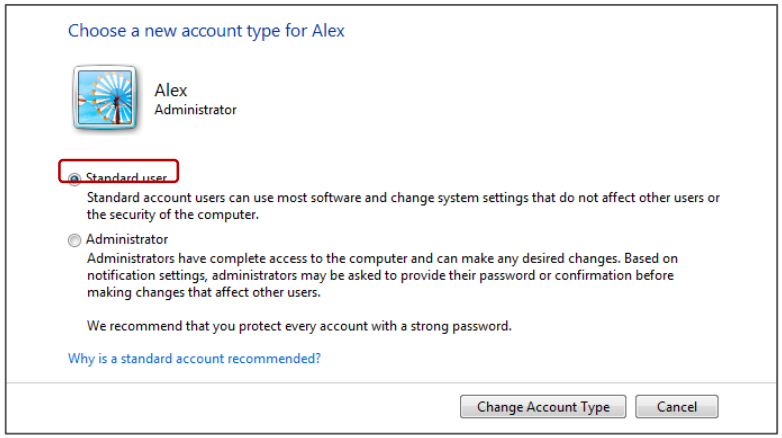
- Control Panel → User Accounts → Manage another account

1.

2.




3.



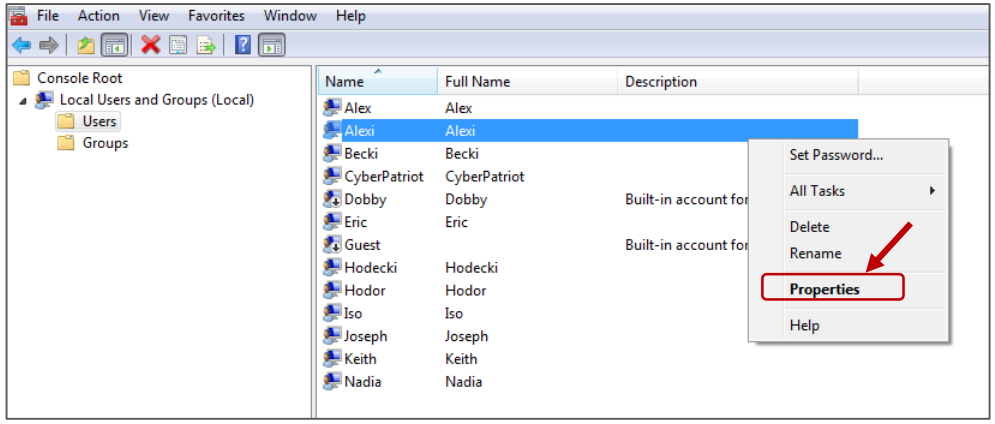

© Air Force Association

# Best Practice: Set Passwords for all Accounts

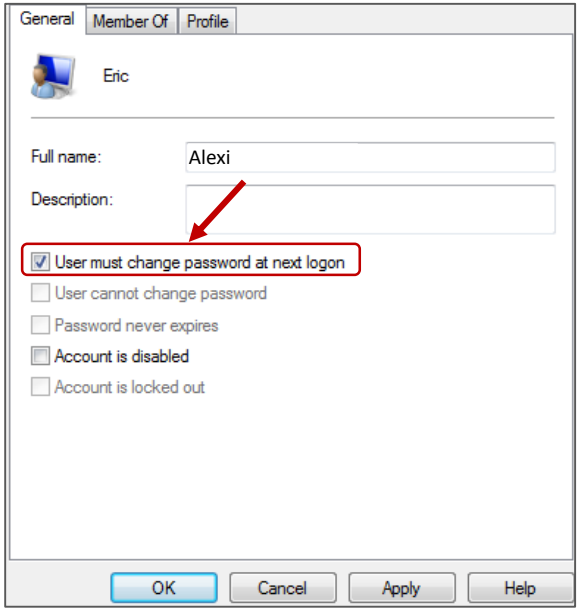
**Console option:**

- Make sure all accounts are password protected

1.




2.




© Air Force Association

# Best Practice: Set Passwords for all Accounts

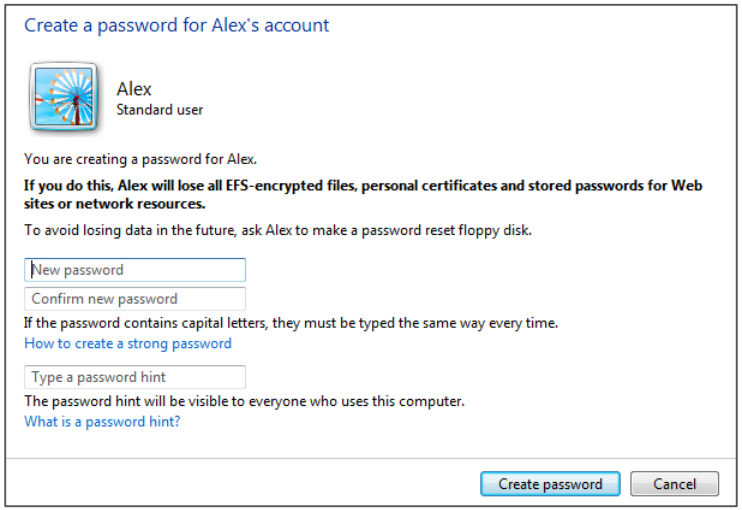
**Control Panel option:**

- Control Panel → User Accounts → Manage another account

1.

2.

3.



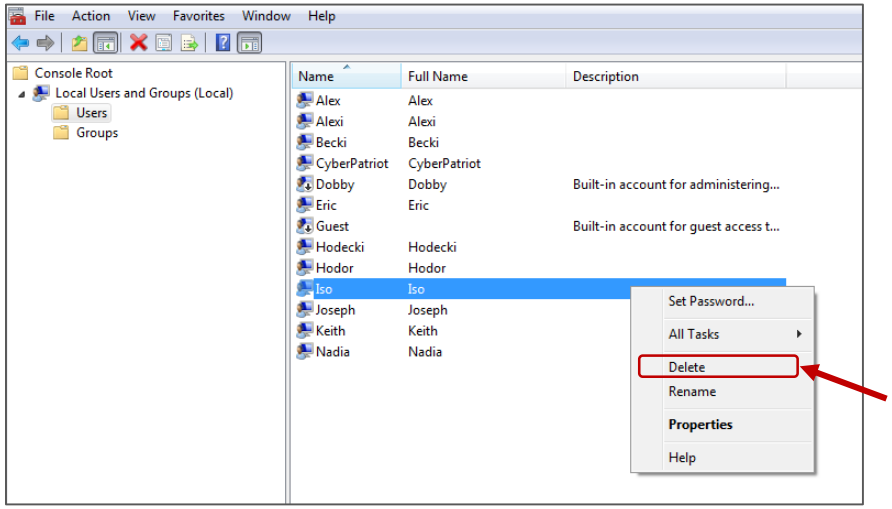

© Air Force Association

# Removing Users

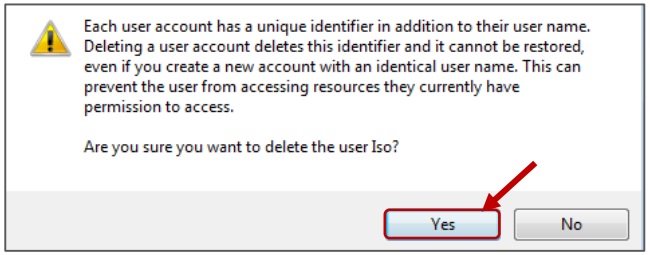
**Console option:**

- 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.



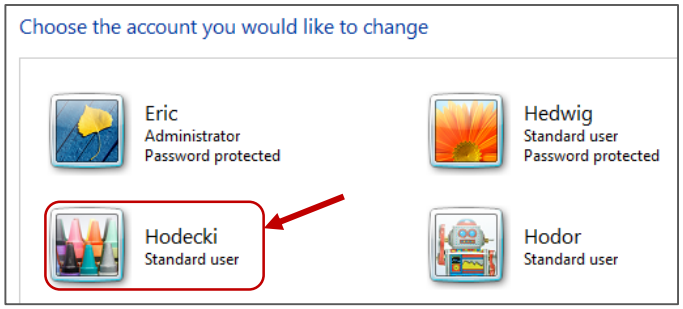

© Air Force Association

# Removing Users

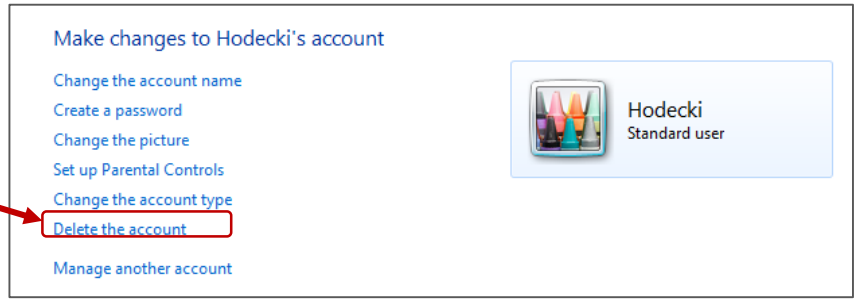
**Control Panel option:**

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

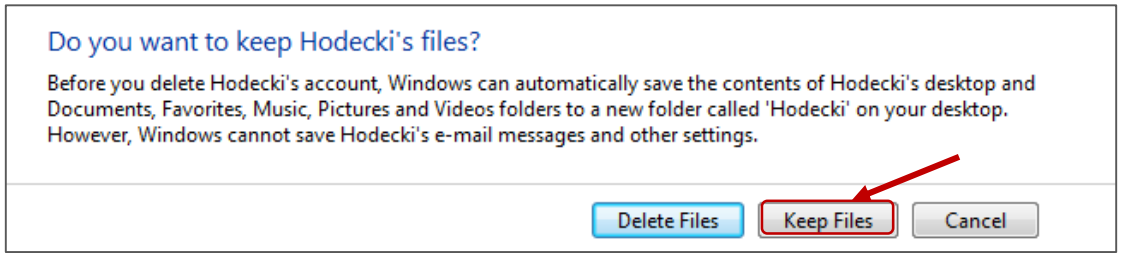
1.




2.




3.



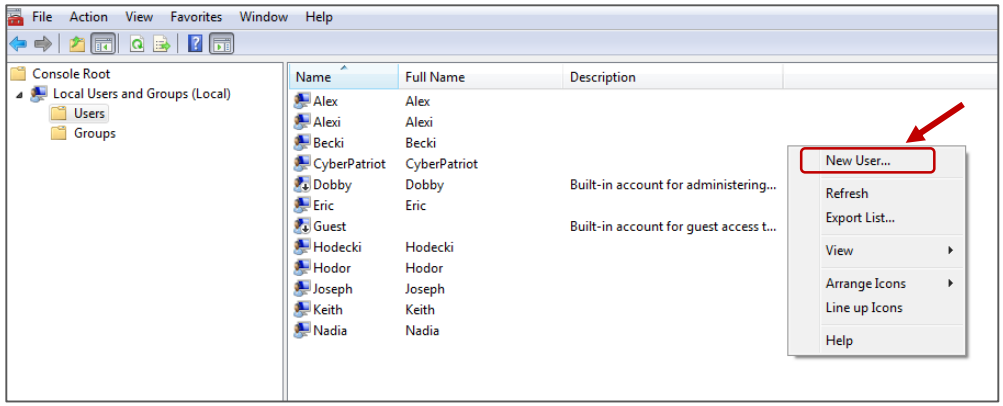

© Air Force Association

# Adding Users

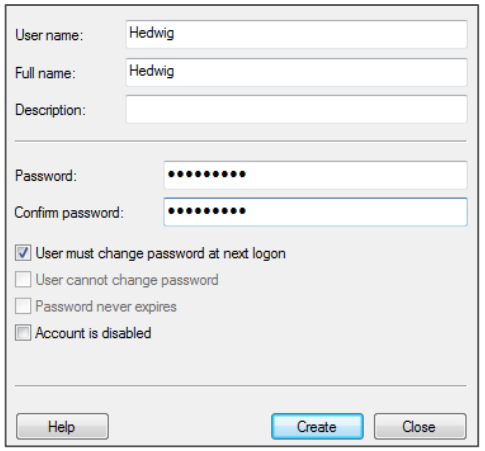
**Console option:**

- 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.




© Air Force Association

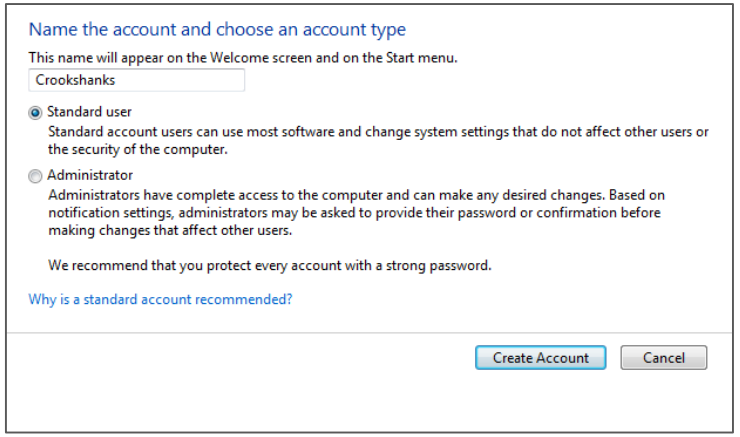
# Adding Users

**Control Panel option:**

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

1.

2.




© Air Force Association