# Users, Groups, and Permissions

## Chapter 13

CompTIA A+ (220-110x)

Mike Meyers and Steve Nicholson

Episode: **Introduction to Users and Groups**

Objective(s):

Core 2: 1.8 Explain common OS types and their purposes.

Core 2: 2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

## Episode Description

The Microsoft NT File System (NTFS) enables fine control of multiple users accessing resources on a single computer. To do this, every person accessing a single computer must have their own user account. Windows also has groups which combine users with common resource needs.

## Key Terms

- 1:32 - Objective term - NTFS (New Technology File System)
- 2:17 - Allow vs. Deny
- 2:27 - Objective term - NTFS permissions
- 3:14 - Objective term - Users and groups
- Objective term - File and folder attributes
- Objective term - Inheritance



# Quick Review

- Windows combined with NTFS gives tremendous control over resources
- NTFS permissions are assigned to user accounts
- A group is a container for user accounts
- Permissions are assigned to groups for easy administration


Episode: Managing Users and Groups
Objective(s):
Core 2: 1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
Core 2: 2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.



## Episode Description

Every version of Windows has some utility to create, maintain, and remove users and groups from a system. Local Users and Groups gives the most granular settings, but for quick setup you can always add and edit accounts in the User Accounts Control Panel applet.



## Key Terms

- 2:49 - Objective term - Administrator vs. standard user
- 2:47 - Administrator group
- 3:41 - User Accounts in Control Panel
- 4:14 - Objective term - You can add users via Microsoft account or local account
- 5:44 - Objective term - Local Users and Groups
- 6:41 - Objective term - Guest account
- 7:18 - Objective term - Power Users

# Quick Review

- Settings > Accounts enables basic account creation
- User Accounts in Control Panel provides more account control
- Local Users and Groups provides the most control over users and group

# Episode: **NTFS Permissions**

Objective(s): Core 2: 2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.



## Episode Description

NTFS permissions are powerful and a bit complicated to those unfamiliar with them. You can apply permissions for files or folders to user accounts (although it is considered better to apply them to groups and add user accounts to those groups).



## Key Terms

- 0:36 - Objective term - NTFS permissions
- 1:54 - Objective term - NTFS permission attributes for a folder
- 5:39 - Objective term - Inheritance
- 6:21 - Deny enables explicit permissions in order to stop inheritance

# Quick Review

- All files and folders on an NTFS formatted drive have NTFS permissions
- Folder permissions include Full Control, Modify, Read and Execute, List Folder Contents, Read, Write
- File permissions include Full Control, Modify, Read and Execute, Read, and Write
- Inheritance is when a new folder or file gets the permissions of the folder in which it was created

Episode: **Linux and macOS Permissions**

Objective(s): Core 2: 2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

## Episode Description

While macOS and Linux lack NTFS's fine control of resources, they do still have permissions, and a good tech should understand how they work. Additionally, there are specific tools used to control permissions.

## Key Terms

- 0:21 - Owner, group, and everyone
- 1:13 - Read (R), write (W), execute (X) attributes

# Quick Review

- Linux and macOS permissions use the owner, group, and everyone
- Each of these three can have read, write, or execute permissions
- These are assigned by changing the file or folder properties


Episode: File Explorer
Objective(s):
Core 2: 1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
Core 2: 2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.



## Episode Description

Techs use File Explorer to access and manipulate files and folders on their local machines and on networks. By default, File Explorer works well, but a good tech should know about the many features of this tool.

## Key Terms

- 1:24 - Navigation pane
- 1:41 - Preview pane
- 1:53 - Details pane
- 2:41 - Quick access
- 3:29 - This PC
- 3:52 - Drives
- 4:03 - Cloud services
- 4:23 - Network



## Key Terms

- 4:53 - Objective term - General options
- 6:16 - Objective term - View options
- 6:26 - Objective term - Show hidden files, folders, and drives
- 6:32 - Objective term - Attributes
- 8:12 - Objective term - Indexing
- 9:24 - Objective term - Hide extensions
- 9:40 - File association



# Quick Review

- File Explorer is the primary tool for folder and file manipulation in Windows
- File Explorer is highly customizable
- There are multiple ways to do the same job in File Explorer


CompTIA A+ (220-110x)
Mike Meyers and Steve Nicholson

## Episode Description

The process of sharing resources using NTFS makes more sense with examples. Certain features (especially Allow/Deny and Inheritance) make more sense when you see the process in action.



## Key Terms

- 0:26 - Microsoft LAN Manager
- 0:52 - Objective term - NTFS vs. share permissions
- 2:50 - Universal Naming Convention (UNC)
- 3:00 - Objective term - Network path:  C:\Fred
- 3:16 - \\MikesPC\FredC
- 8:20 - Objective term - Mapping drives
- 9:37 - Objective term - When sharing resources via workgroups, remember each computer has its own login information



# Quick Review

- Windows networking has both NTFS and Share permissions
- Shared resources have a UNC name
- Resources are first offered for sharing, then others access the shared resource
- Shared resources can be mapped to a drive letter

# Episode: **Security Policies**

Objective(s):

- Core 2: 1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.
- Core 2: 2.1 Summarize various security measures and their purposes.
- Core 2: 2.6 Given a scenario, configure a workstation to meet best practices for security

## Episode Description

NTFS permissions control files and folders, but there are plenty of other resources that need control. Security Policies control factors like logon attempts, printer access, and password length/complexity.

## Key Terms

- 0:39 - Local Security Policy
- 1:25 - Objective term - Password best practices
- 3:38 - Objective term - Account Lockout Policy
- 5:23 - Objective term - Restrict logon based on place or time
- 6:53 - Objective term - Domain policies



# Quick Review

- Security policies define a broad spectrum of security features
- We use the Local Security Policy application to manage policies
- Account policies enable login and password rules