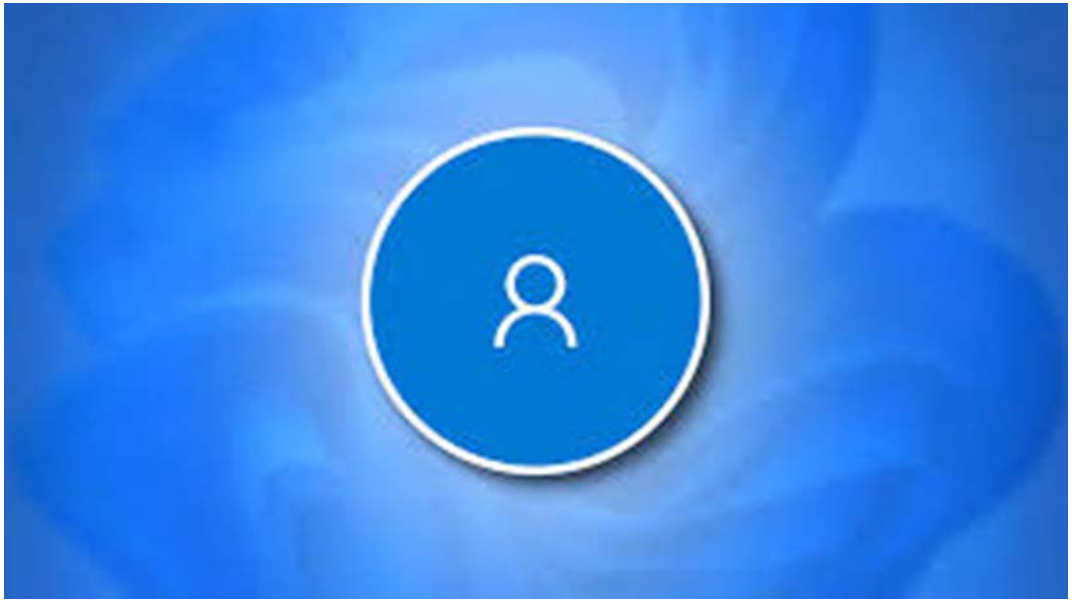
CH 5: Sharing Resources and Wrights Management

Manage Users

Configure Shared Resources

Configure Active Directory Accounts and Policies

Topic A: Manage Users



User and Group Accounts

- Groups
  - Built-in local groups
  - Administrators
  - Users
  - Guests
  - Power Users
  - System Groups
  - System and Service Accounts

User account: The logon ID that identifies each user.

Security group: A collection of user accounts that can be assigned permissions in the same way as a single user object.

User and Group Accounts

- System Groups
  Windows Home
  - Everyone
  - Authenticated Users
  - Creator Owner
  - Interactive
  - Network
- System and Service Accounts
  - LocalSystem
  - LocalService
  - NetworkService

- Only In Professional, and Enterprise editions of Windows
- Local Users and Groups management console provides an interface for managing both user and group accounts.
- It is not available in Starter or Home editions.

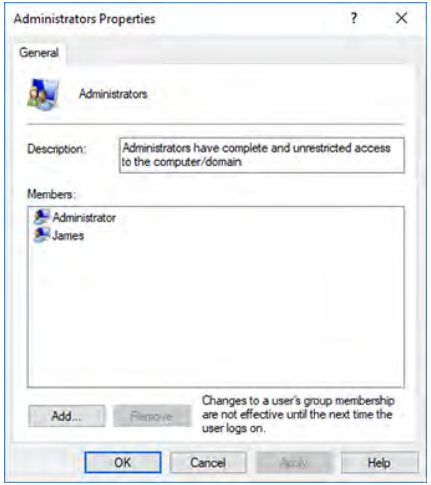
Home editions of Windows allow the use of two groups only:

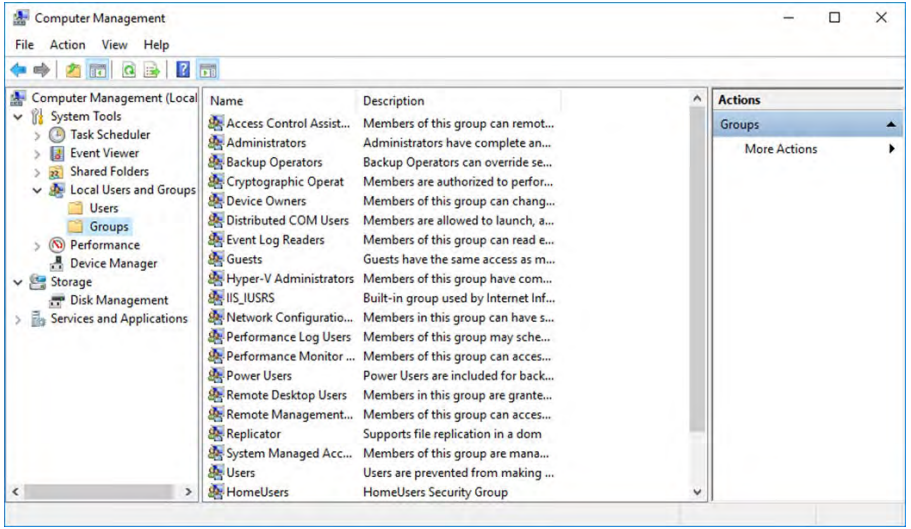
Standard or
Administrator User

For Windows Pro Administrators, Users, Guests, and Power Users

Local Users and Groups

- Create new user
- Rename and delete user accounts
- Add a user to a group
- Use **net user username password /add** commands



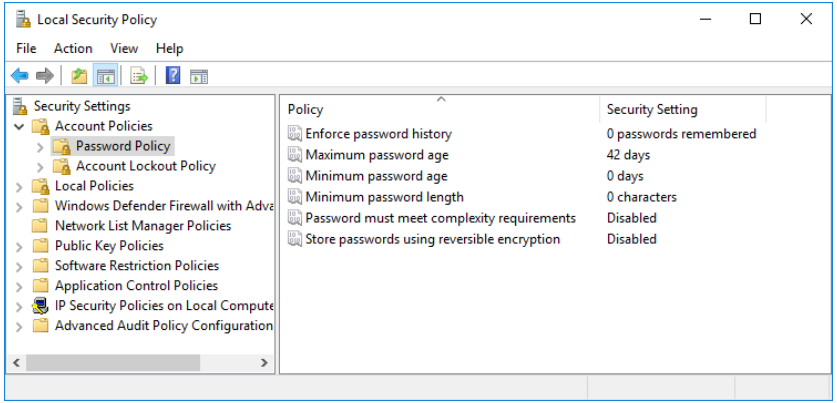


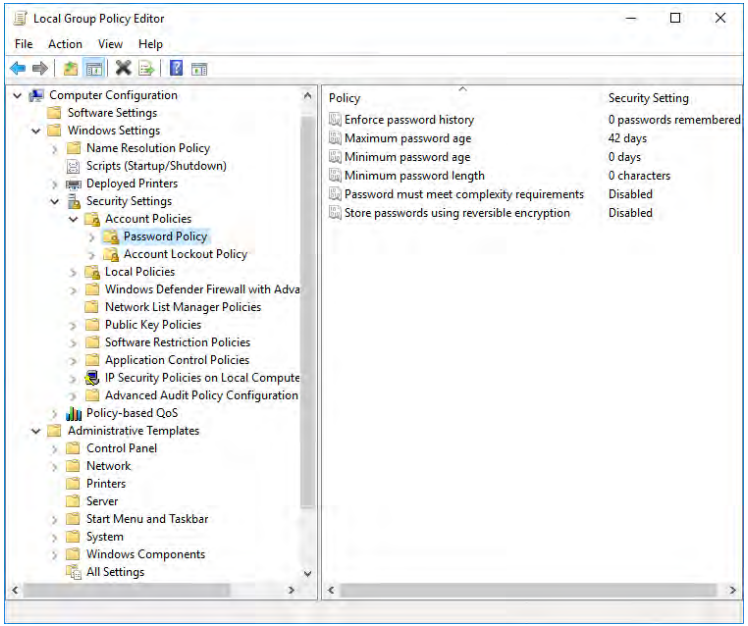
Local Security Policy

only avilable in bussines edtion oif windows

Policies: A subset of a security profile, and a document that outlines the specific requirements and rules everyone must meet

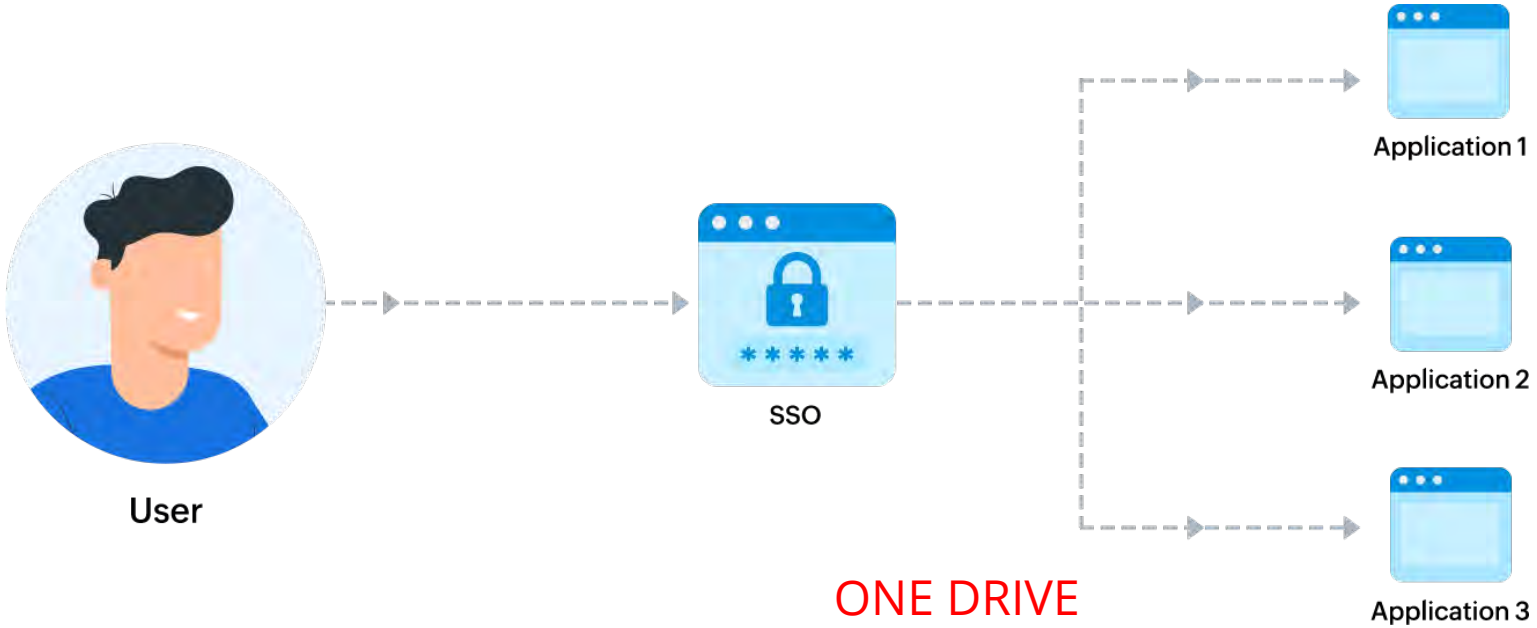
Located in Admin Tools





SSO and Credential Manager

Single Sign-On (SSO): Any authentication technology that allows a user to authenticate once and receive authorizations for multiple services.

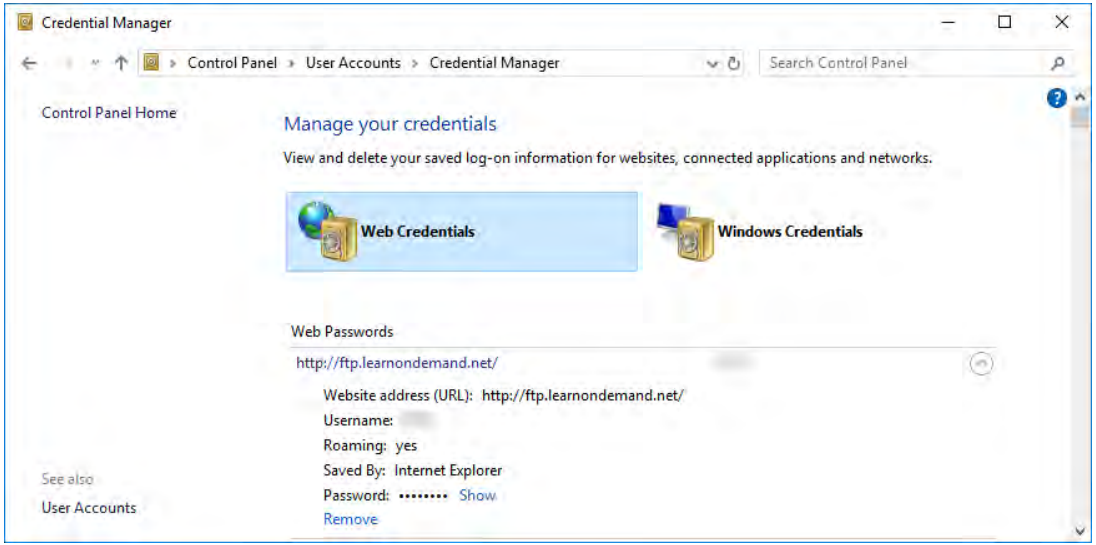


SSO and Credential Manager

Single Sign-On (SSO): SSO is not available for many services. Most users do not try to remember each password for every website or network they use.

Instead, they use the OS to save (or cache) the password.

You can view cached passwords for websites and Windows/network accounts using the Control Panel app **Credential Manager**.

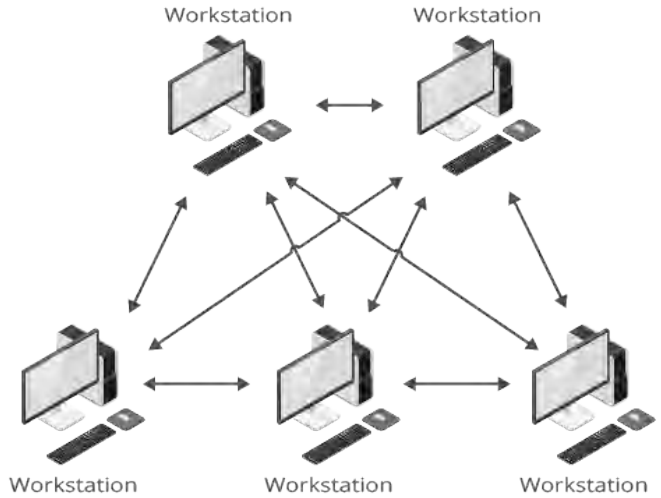


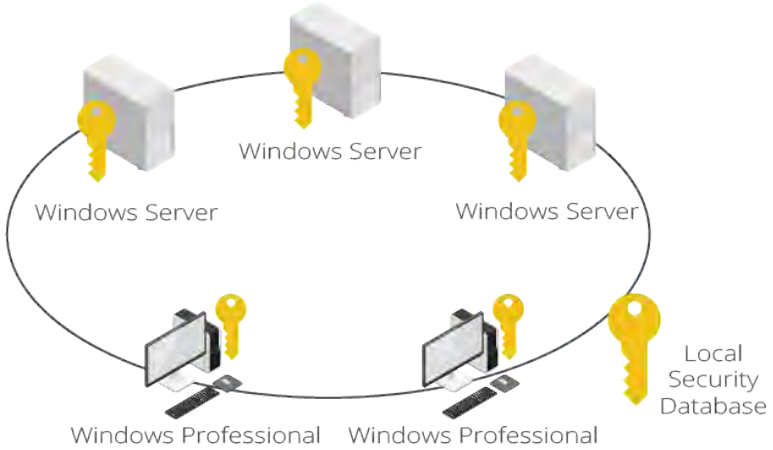
Topic B: Configure Shared Resources

Workgroups

Peer-to-peer network: A network with no dedicated server and each computer acts as both a server and a client.

Workgroup: A small group of computers on a network that share resources in a peer-to-peer fashion.



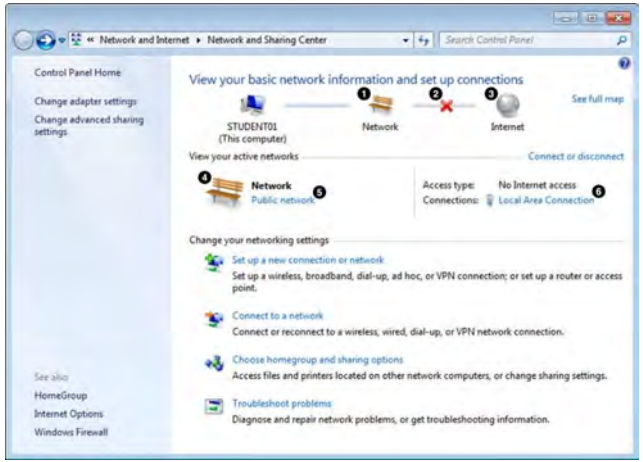


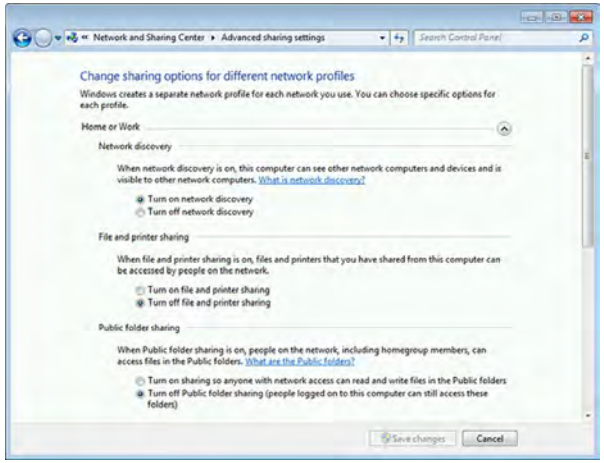
Homegroups

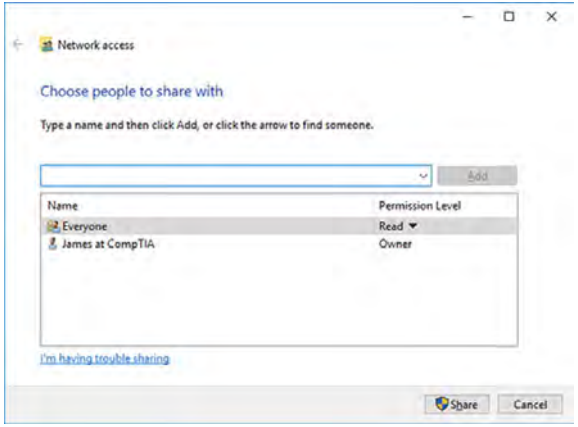
Homegroup: Windows networking feature designed to allow Windows 7 and later home networks to share files and printers easily through a simple password protection mechanism.

(**Not in Win11 -10**)

Network and Sharing Center







Network Share Configuration

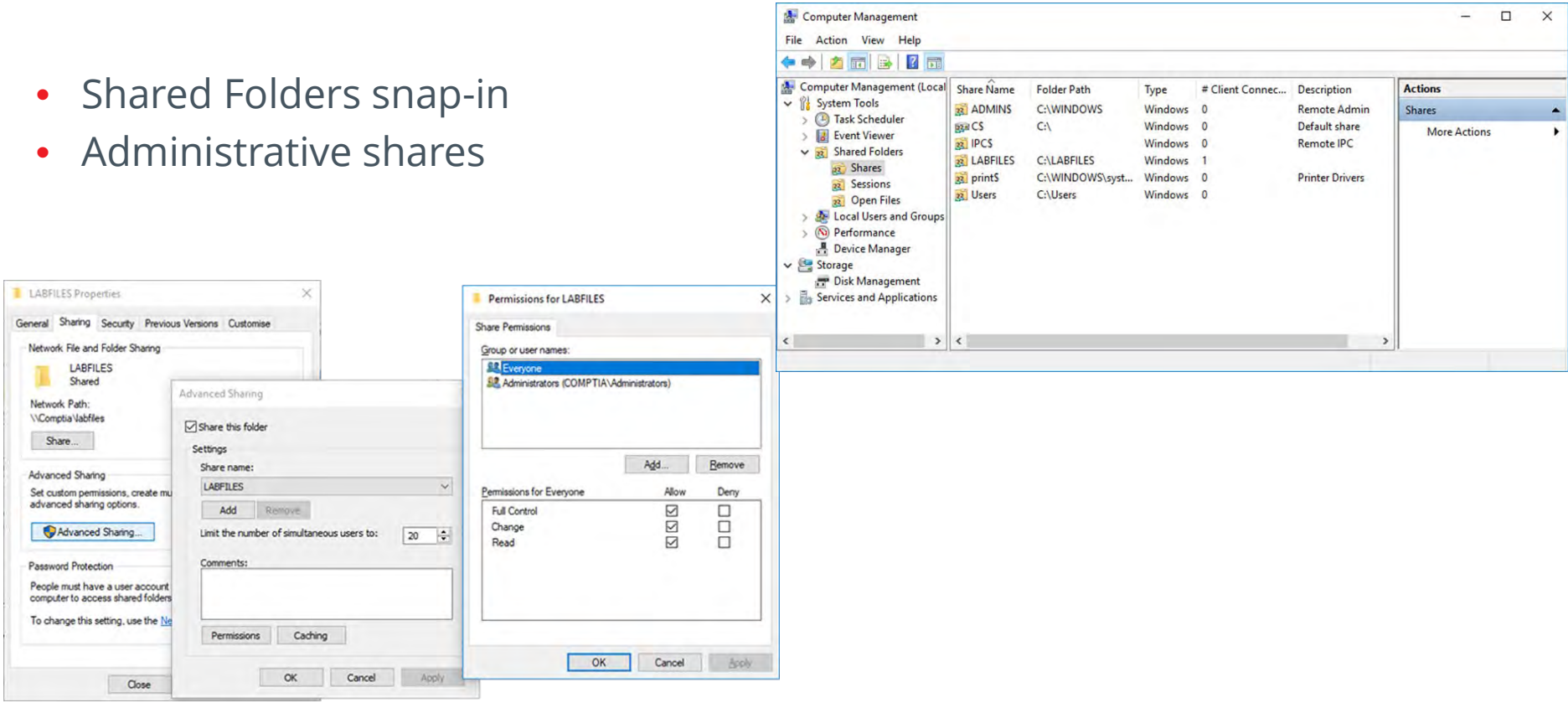
- Share name and Maximum number of users allowed to connect at any one time

- Share Permissions
  - Full Control—allows users to read, edit, create, and delete files. Also, to assign permissions to other users and groups.
  - Change—this is like full control but does not allow the user to set permissions for others.
  - Read—users are permitted to connect to the resource, run programs, and view files only.

Most of the time, the shared folder permission is set to Full Control. The effective permissions are managed using **NTFS** security.

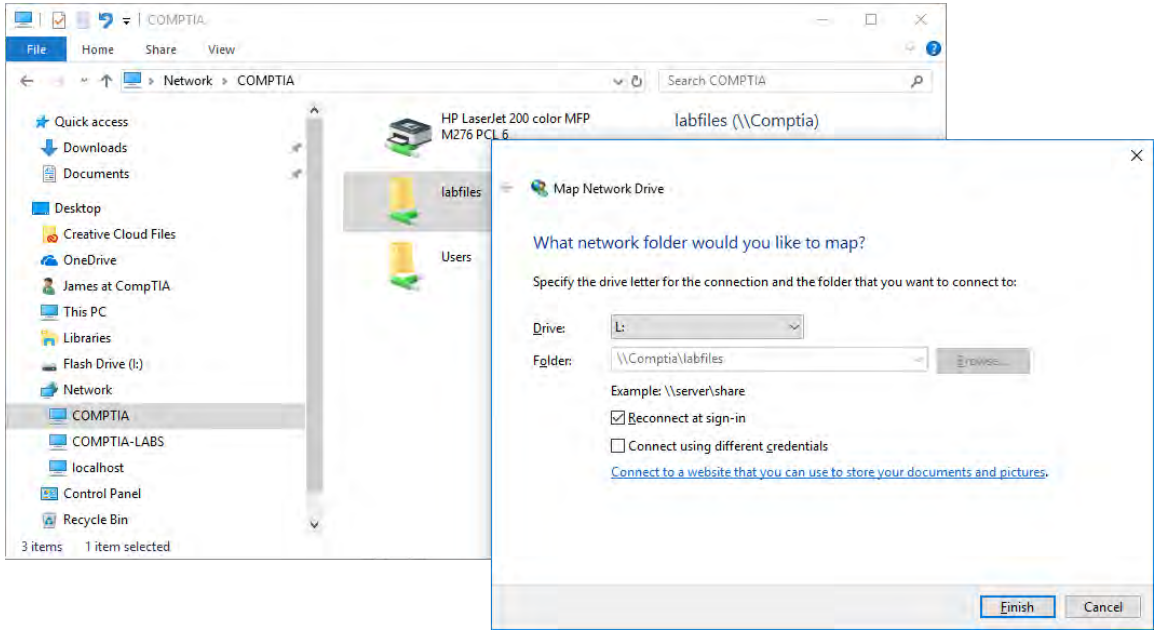
Network Share Configuration

- Shared Folders snap-in
- Administrative shares

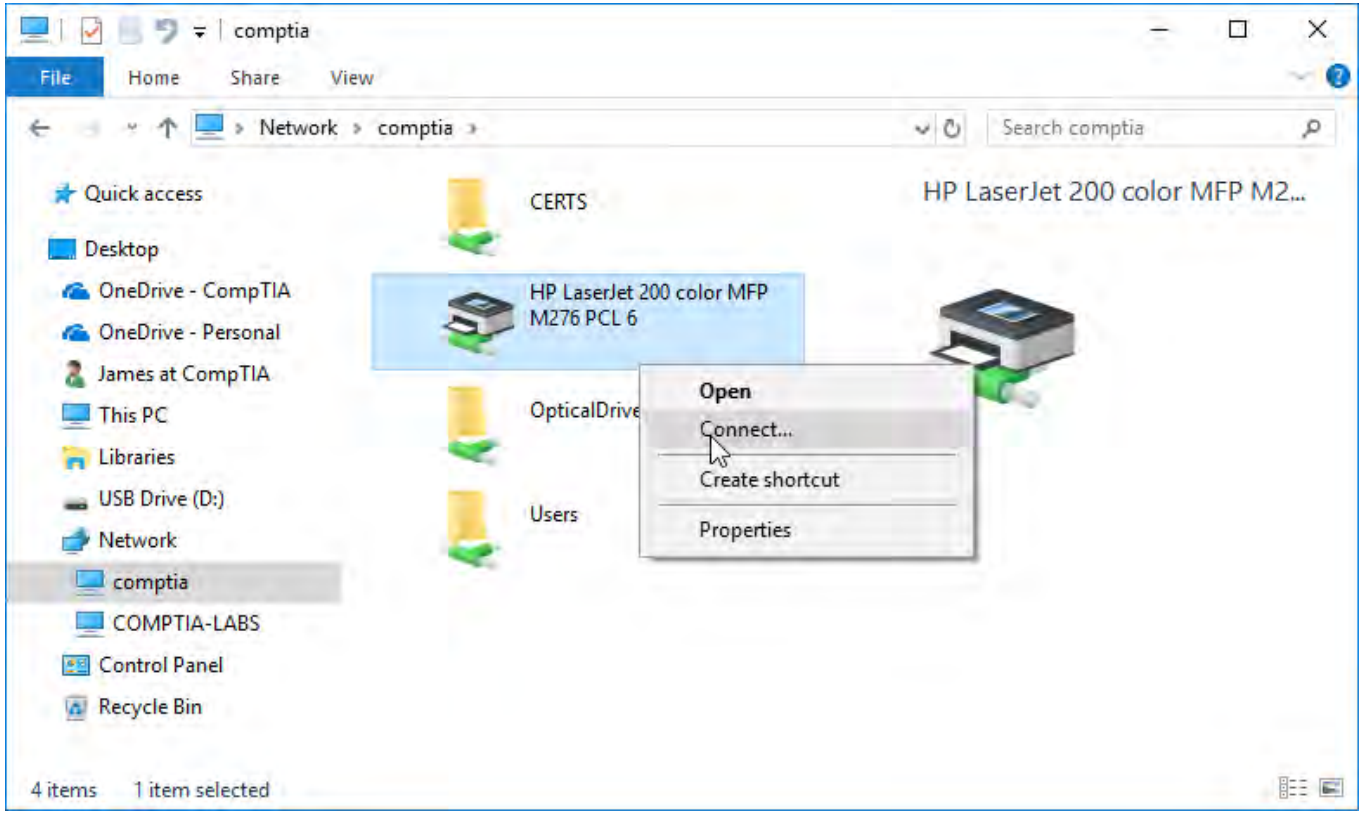


Network Share Configuration

Network drive: A local share that has been assigned a drive letter.



Network Share Configuration



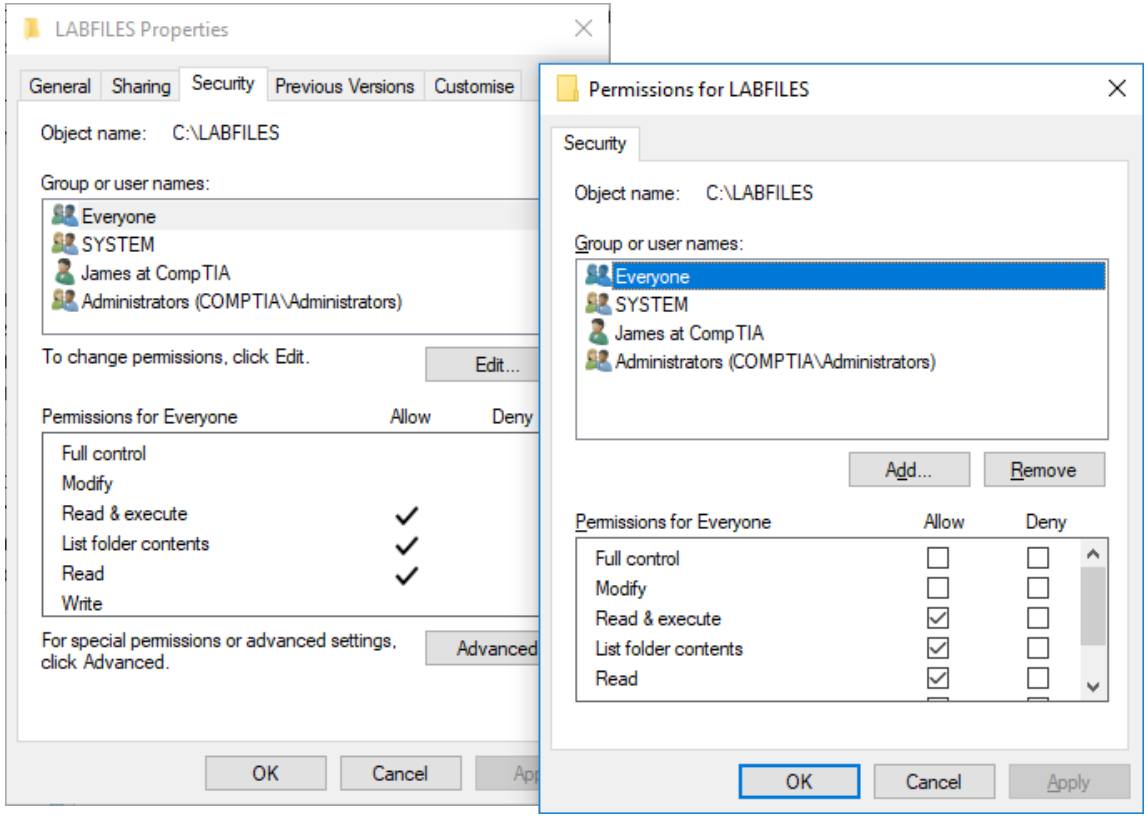
The net Commands

You can also manage accounts at the command line using the **net user** command.

You need to execute these commands in an administrative command prompt:

- net /?
- net use /?
- net use *DeviceName* *ComputerName**ShareName*
- net use *DeviceName* /delete
- net use * /delete
- net view

NTFS File and Folder Permissions



NTFS File and Folder Permissions

Folder Permission	Allows
Read	View files and subfolders including their attributes, permissions, and ownership.
Write	Create new folders and files, change attributes, view permissions and ownership.
List	View the names of files and subfolders.
Read & Execute	Pass-through folders for which no permissions are assigned, plus read and list permissions.
Modify	Includes Read/Execute and Write permissions, as well as the ability to rename and delete the folder.
Full Control	All the above, plus changing permissions, taking ownership, and deleting subfolders and files.

NTFS File and Folder Permissions

File Permission	Allows
Read	Read the contents of the file and view attributes, ownership, and permissions.
Write	Overwrite the file and view attributes, ownership, and permissions.
Read & Execute	Read permissions, plus the ability to run applications.
Modify	Includes Read/Execute and Write permissions, as well as the ability to rename and delete the file.
Full Control	All the above, plus changing permissions, taking ownership.

NTFS File and Folder Permissions

Effective Permissions and Allow vs. Deny

- Permissions usually applied at one of 3 levels:
  - 1 For application folders, the read/execute permission is granted to the appropriate group.
  - 2 For data areas, the modify or read permission is assigned as appropriate.
  - 3 To home directories (personal storage areas on a network), full control is assigned to the relevant user.

NTFS File and Folder Permissions

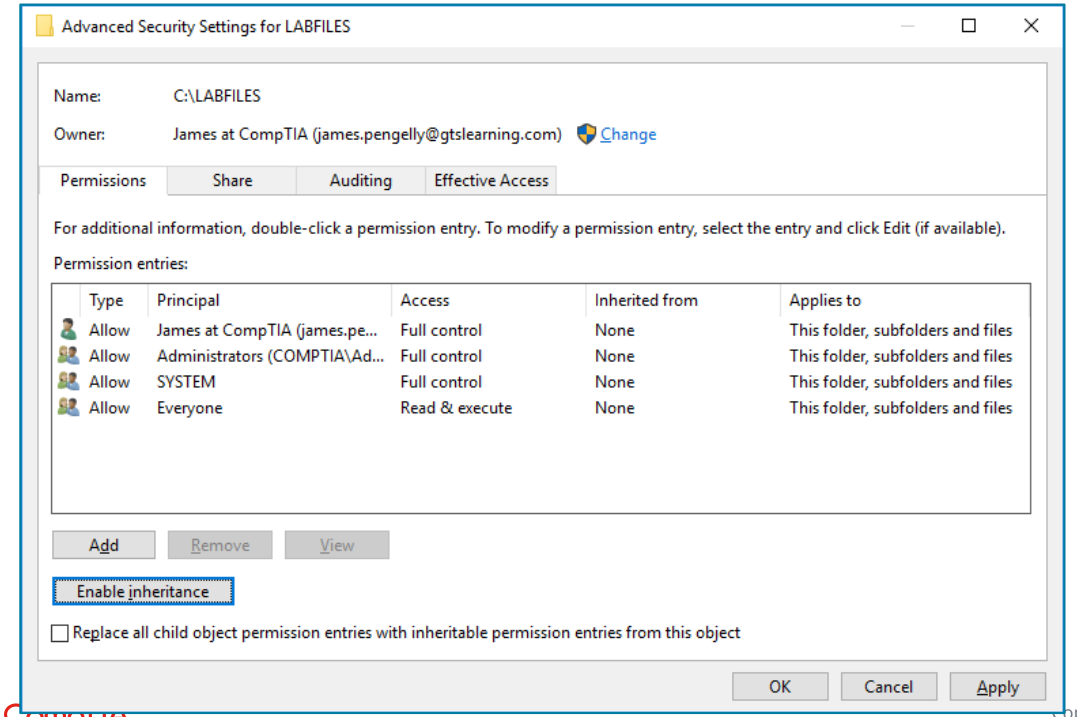
- Best Practice
  - If an account is not granted an "allow" permission, an implicit deny is applied.
  - Share permissions only protect the resource when it is accessed across the network.
  - NTFS permissions are used to protect the resource from unauthorized local access.

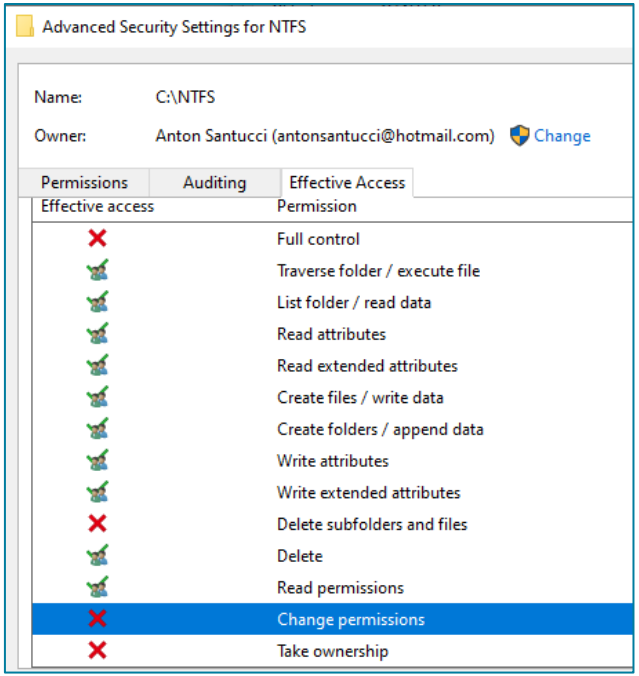
NTFS File and Folder Permissions

- Best Practice
  - When either Share or NTFS permissions are set at the root folder all files and subdirectories inherit the same permissions.
  - If both share and NTFS permissions are applied to the same resource, the most restrictive applies (when the file or folder is accessed over the network).
  - If the group "Everyone" has Read permission to a share and the "Users" group is given Modify permission through NTFS permissions, the effective permissions for a member of the "Users" group will be Read (Most Restrictive).
  - If the same user is in two different NTFS groups, the permission outcome is the Least Restrictive.

NTFS File and Folder Permissions

- Advanced Settings
- Ownership





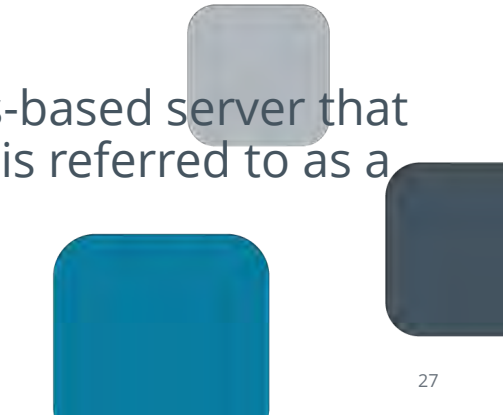
NTFS File and Folder Permissions (Not on Test)

Action	Effect
Moving files and folders on the same NTFS volume	• Destination folder: Write permission. • Source folder: Modify permission. • NTFS permissions are retained.
Moving files and folders to a different NTFS volume	• Destination folder: Write permission. • Source folder: Modify permission. • NTFS permissions are inherited from the destination folder and the user becomes the Creator/Owner.
Copying files and folders on the same NTFS volume or different NTFS volumes	• Destination folder: Write permission. • Source folder: Read permission. • NTFS permissions are inherited from the destination folder and the user becomes the Creator/Owner.
Moving files and folders to a FAT or FAT32 partition	• Source folder: Modify permission. • All permissions and NTFS attributes (such as encryption) are lost.

Topic C: Configure Active Directory Accounts and Policies

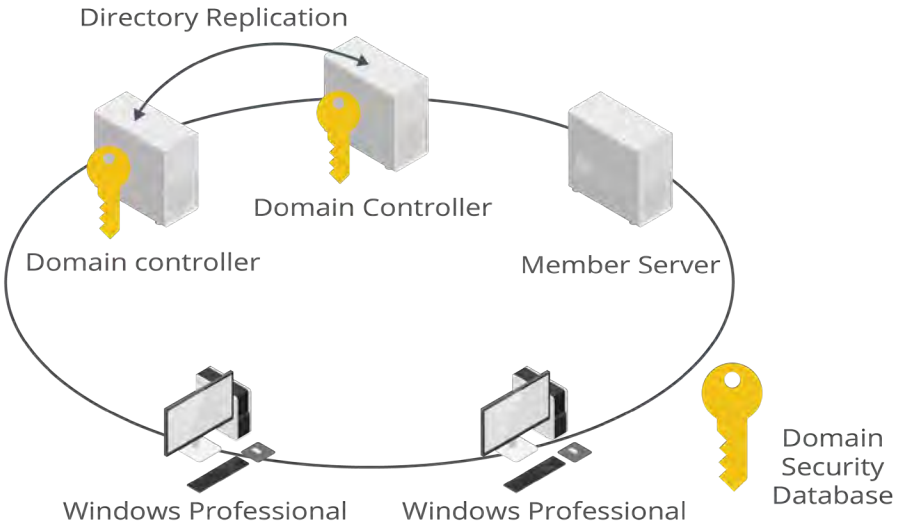
Windows Active Directory Domains

- **Local accounts:** An account that is only associated with the computer on which it was created.
- **Local Security Accounts database:** A local (non-network) database where local system account information is stored.
- **Security Accounts Manager (SAM):** The Windows local security account database where local system account information is stored.
- **Windows Server Domain Controller (DC):** Any Windows-based server that provides domain authentication services (logon services) is referred to as a domain controller (DC).



Active Directory Components

Active Directory Domain Services (AD DS): The database that contains the users, groups, and computer accounts in a Windows Server domain.



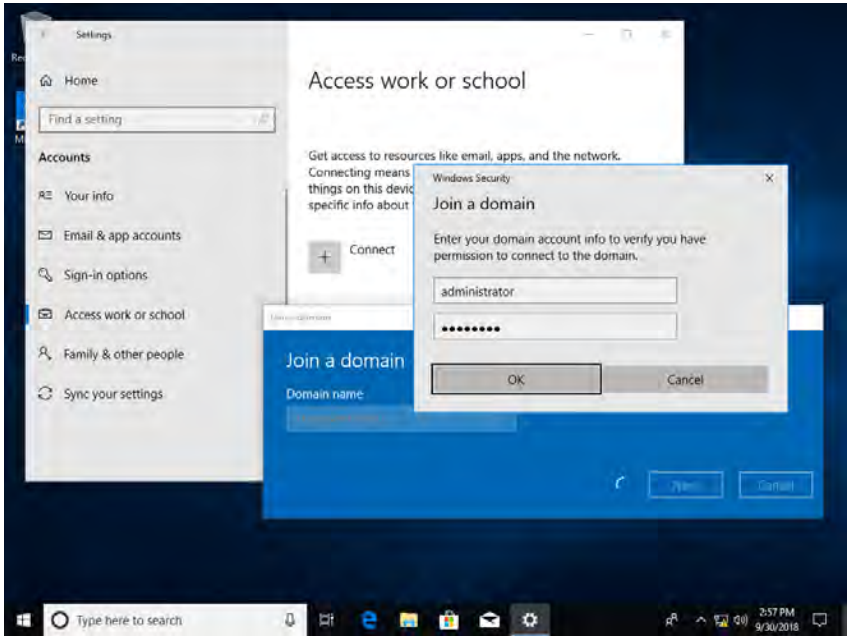
Active Directory Components

Member servers: Any server-based systems that have been configured into the domain, but do not maintain a copy of the Active Directory database.(such as Exchange or SQL Server)

Organizational Units (OUs): In Windows Active Directory, a way of dividing the domain up into different administrative realms.

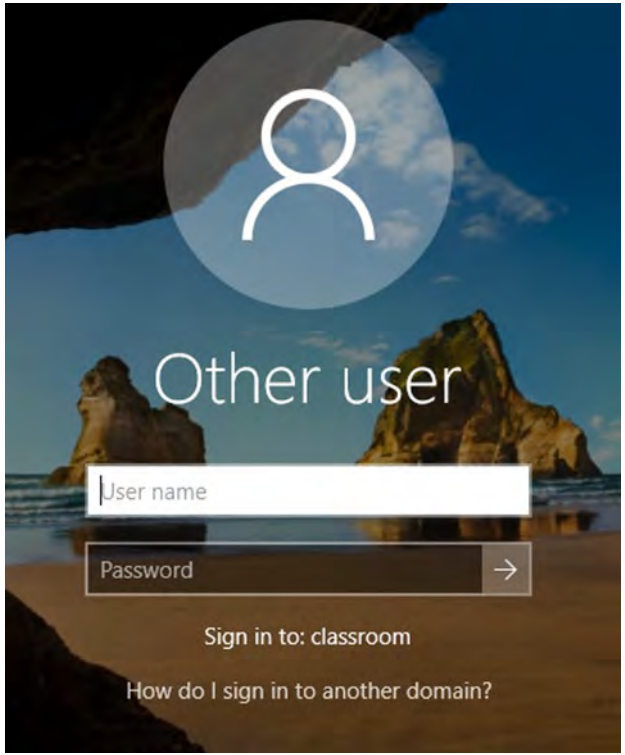
Domain Membership

- The computer has a computer account object.
- Computer users can log on to the domain with domain user accounts.
- The computer and its users are subject to centralized settings:
  - Domain security
  - Configuration
  - Policy settings



Domain Membership

- Certain domain accounts automatically become members of local groups on the computer.



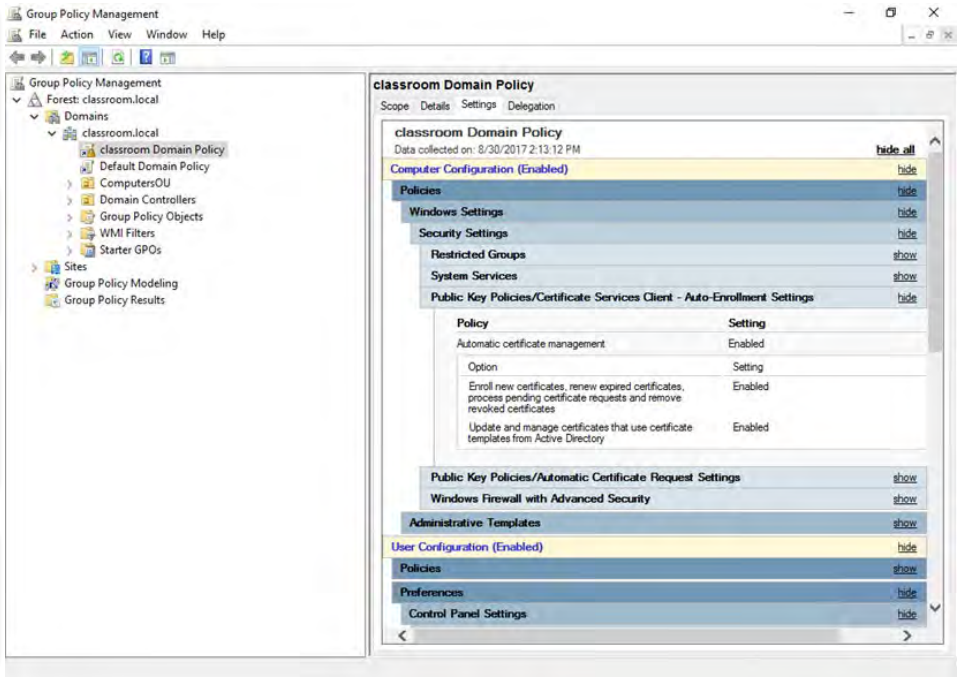
Group Policy Objects

GPO: A means of applying security settings (as well as other administrative settings) across a range of computers and users.

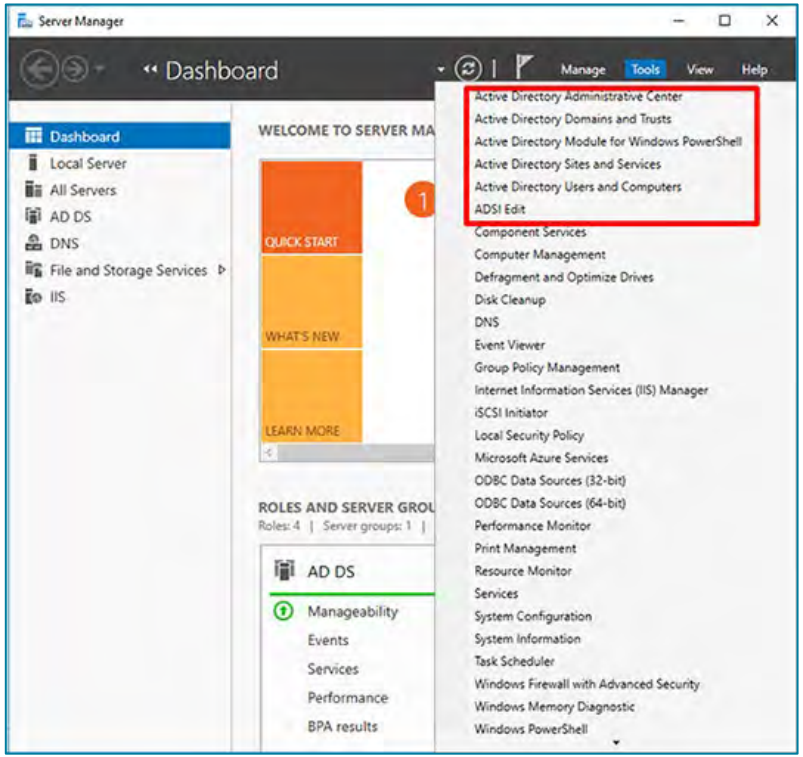
Administrative templates: Group Policy files for registry-based policy management, which have the .ADM file extension.

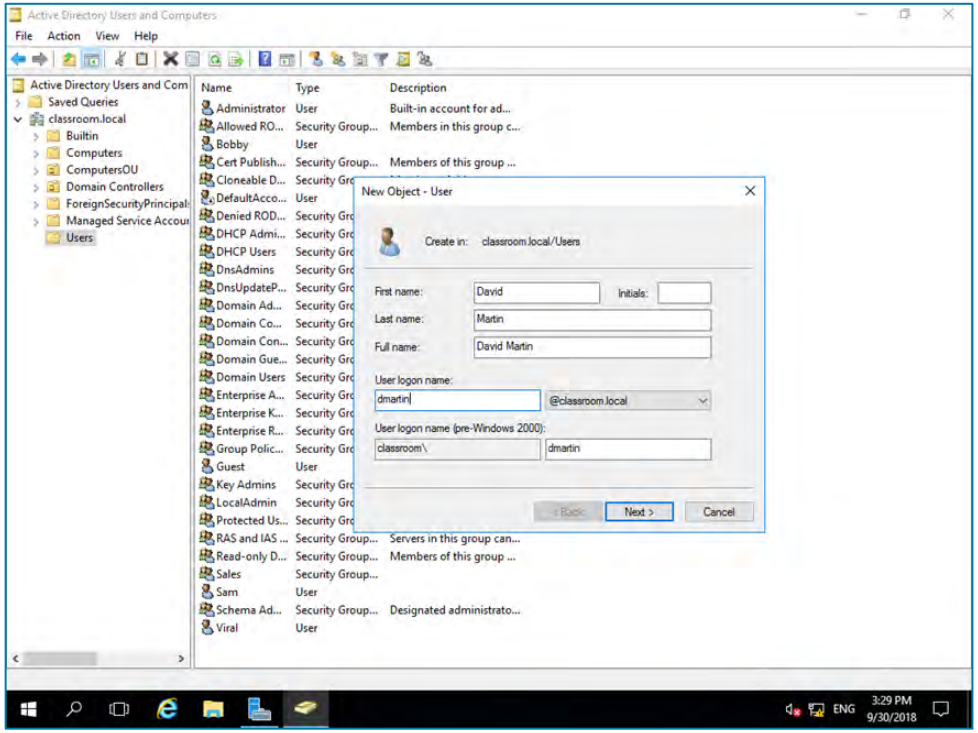
Security templates: Settings for services and policy configuration for a server operating in a particular application role.

RSoP: A Group Policy report showing all of the GPO settings and how they affect the network.



Basic AD Functions





Logon Scripts

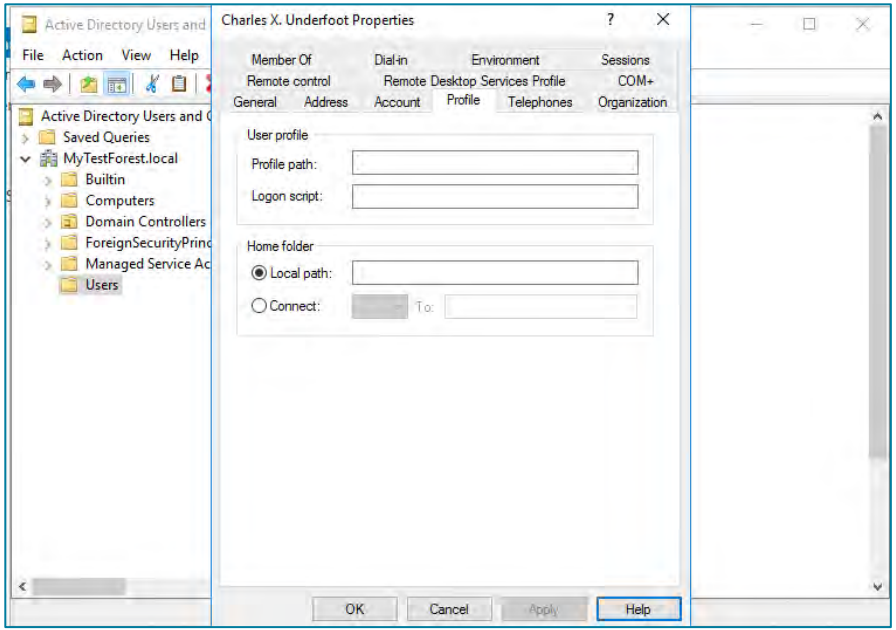
Windows logon scripts
Linux login scripts

Logon script: A file containing commands that run each time a user logs on to a computer to set up the user environment.

SSO: Any authentication technology that allows a user to authenticate once and receive authorizations for multiple services.

Home Folder

Home folder: A private network storage area located in a shared network server folder in which users can store personal files.



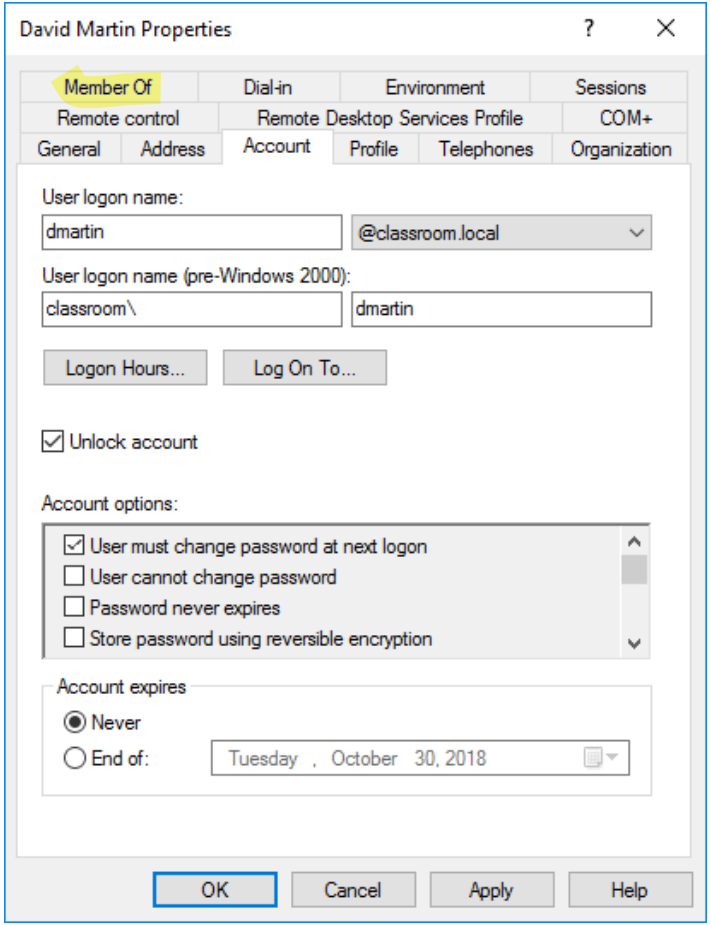
Folder Redirection

Folder redirection: A Microsoft Windows technology that allows an administrative user to redirect the path of a local folder (such as the user's home folder) to a folder on a network share, making the data available to the user when they log into any computer on the network where the network share is located.

Roaming profiles: A Microsoft Windows technology that redirects user profiles to a network share so that the information is available when the user logs into any computer on the network where the network share is located.

Offline files: Files (or folders) from a network share that are cached locally.

Account Locks and Password Resets



Domain Membership