12.5.3 User and Group Facts

This lesson covers the following topics:

- User accounts
- Groups

User Accounts

The ability to use a computer is controlled through a *user account*.

- The user account identifies a specific user.
- *Logon* is the process of authenticating to the computer by supplying a user account name and the password associated with that user account.
- On Windows systems, the ability to perform actions on a computer, such as modifying system settings or installing hardware, are called *rights*.
- Access to files, folders, and printers is controlled through *permissions*. Permissions identify what the user can do with the associated object.
- Windows 10 offers five basic types of user accounts: the built-in Administrator account, user accounts with administrative privileges, standard accounts, the Guest account, and Microsoft accounts.

You can manage users from the Accounts setting. Go to Accounts by following these steps:

1. Select **Start**.
2. Select **Settings**.
3. Select **Accounts**.

The table below shows capabilities of each account.

Account Type	Capabilities
Built-in Administrator Account	The Administrator account has all rights and permissions on the computer. This account is hidden from normal view. It doesn't show up on the usual login screen.
User Accounts with Administrative Privileges	User accounts with administrative privileges. This is the account that most users typical use when they think of an Administrator account.
Standard Account	This account is hidden from normal view. It doesn't show up on the usual login screen.
Guest Account	The has very limited capabilities, usually restricted to logging on, viewing files, and running some programs. As a security measure, Windows XP and later automatically disable the Guest account in order to prevent unauthorized logon to the system.
Microsoft Accounts	Take advantage of many of the newest Windows 10 features. To set up a Microsoft account, you must use a valid e-mail address. A Microsoft account provides the following features: ▪ Allows you to log in to a computer on which you haven't previously set up a local user account. ▪ Provides access to Office 365, Windows Phone accounts, and OneDrive. ▪ Allows you to download apps from the Windows Store. ▪ Syncs your settings across multiple computers.

- Rights and permissions can be assigned to multiple users by using *groups*. Privileges assigned to the group are granted to all group members.
- On a Windows system, users and groups are stored in one of three locations:
  - Local accounts are stored on each computer and control access to resources on that computer.
  - Domain accounts are stored in a central database called Active Directory. A domain controller is a special server that stores user accounts, groups, and the rights and permissions assigned to them.
  - Online accounts are stored online by Microsoft.

Groups

Windows systems have default groups that are created automatically. These groups have pre-assigned rights, permissions, and group memberships. These groups can be renamed, but not deleted. In most cases, you should not modify the membership or privileges of these groups without understanding how they are used. Additionally, many Windows features or 3rd party applications installed on the system may create additional groups.

The following table lists some of the default groups used on Windows systems:

Group Name	Capabilities

Administrators	Members of the Administrators group have complete and unrestricted access to the computer, including every system right. The Administrator user account and any other account designated as a "computer administrator" is a member of this group.
Backup Operators	Members of the Backup Operators group can back up and restore files (regardless of permissions), log on locally, and shut down the system. Members of this group cannot change security settings.
Power Users	Modern versions of Windows no longer use the Power Users group, although it still exists for backwards compatibility. This group was originally used in Windows XP and earlier. Its members can: ▪ Create user accounts ▪ Modify or delete accounts they created ▪ Create local groups ▪ Modify group membership for groups they created ▪ Modify group membership for the Power Users, Users, and Guests groups ▪ Change the system date and time ▪ Install applications Power Users were not allowed to: ▪ Change membership of the Administrators or Backup Operators groups ▪ Take ownership of files ▪ Back up or restore files ▪ Load or unload device drivers ▪ Manage security and auditing logs In modern versions of Windows, you should avoid assigning users to be members of the Power Users group unless an application or service specifically requires it.
Users	Members of the Users group can use the computer but cannot perform system administration tasks and might not be able to run some legacy applications. ▪ Members cannot share folders. ▪ Members cannot install printers if the driver isn't already installed on the system. ▪ Members cannot view or modify system files. ▪ Any user created with Local Users and Groups is automatically a member of this group. ▪ User accounts designated as "standard" or "limited use" accounts are members of this group. ▪ A user account created as a "computer administrator" is made a member of this group (in addition to being a member of the Administrators group).
Guests	Members of the Guests group have limited rights (similar to members of the Users group). Members can shut down the system.
Cryptographic Operators	Members of the Cryptographic Operators group are allowed to perform cryptographic operations.
Event Log Readers	Members of the Event Log Readers group are allowed to use Event Viewer to read the system's event logs.
Network Configuration Operators	Members of the Network Configuration Operators group have limited administrative privileges to allow them to manage the system's network configuration.
Remote Desktop Users	Members of the Remote Desktop Users group are allowed to access the system remotely using the Remote Desktop Client.
Performance Monitor Users	Members of the Performance Monitor Users group can access performance counter data on the system.
Performance Log Users	Members of the Performance Log Users group are allowed to schedule logging of performance counters, enable trace providers, and collect event traces on the system.
Hyper-V Administrators	Members of the Hyper-V Administrators group are allowed to use Hyper-V on the system to create and manage virtual machines.