Windows Configuration and Monitoring

(Cisco Networking Academy – Operating Systems for IT)

Overview

Windows operating systems are built to support robust networking, configuration, and monitoring capabilities, essential for both everyday users and IT professionals. The **Network and Sharing Center** allows users to configure, verify, and troubleshoot network settings, while **Change Adapter Settings** and **TCP/IPv4 properties** help customize how a system connects to networks, including DHCP and static configurations.

To **access shared resources**, Windows utilizes the **SMB protocol** and the **UNC path format** (e.g., \\servername\sharename\file). Features like **administrative shares** (e.g., C$, admin$) and **Remote Desktop Protocol (RDP)** enhance network accessibility and remote administration—but also present security risks if not properly managed.

For performance and incident response, Windows provides **monitoring tools** like **Task Manager** and **Resource Monitor** to observe real-time usage of system resources, manage applications and services, and identify potential threats. These utilities are fundamental for maintaining system health, spotting malware, and optimizing overall performance.

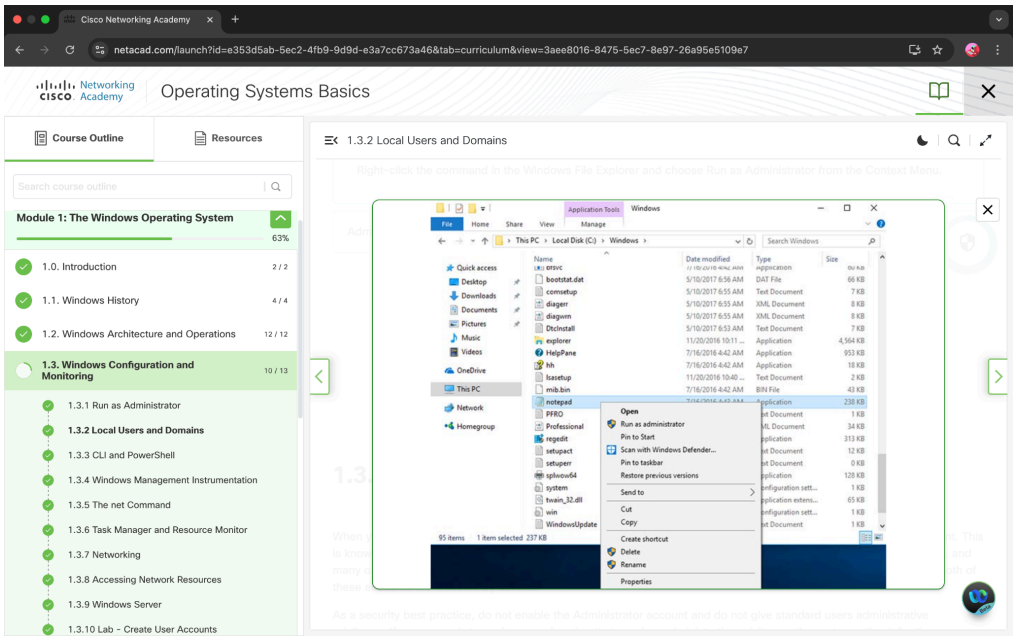
1.1 Run as Administrator

As a security best practice, it is not advisable to log on to Windows using the Administrator account or an account with administrative privileges. This is because any program that is executed while logged on with those privileges will inherit administrative privileges. Malware that has administrative privileges has full access to all the files and folders on the computer.

Sometimes, it is necessary to run or install software that requires the privileges of the Administrator. To accomplish this, there are two different ways to install it. how can we write it in a report give me in short and mention steps

Two common methods to run programs as Administrator:

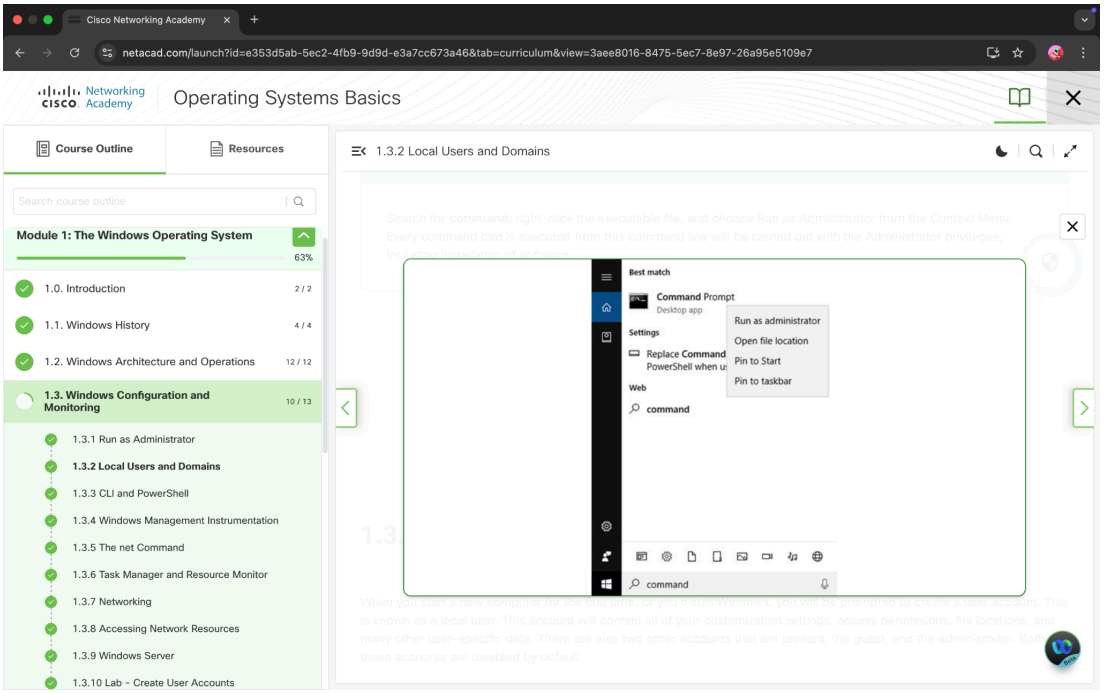
1. **Using the Context Menu:**



* Right-click the program or installer.

- Select **Run as administrator** from the menu.
- Approve the User Account Control (UAC) prompt if it appears.

2. **Using Command Prompt as Administrator:**



***** Open the Start menu, type **cmd**.

- Right-click **Command Prompt** and select **Run as administrator**.
- In the elevated Command Prompt, type the program's name or path to run it with admin privileges.

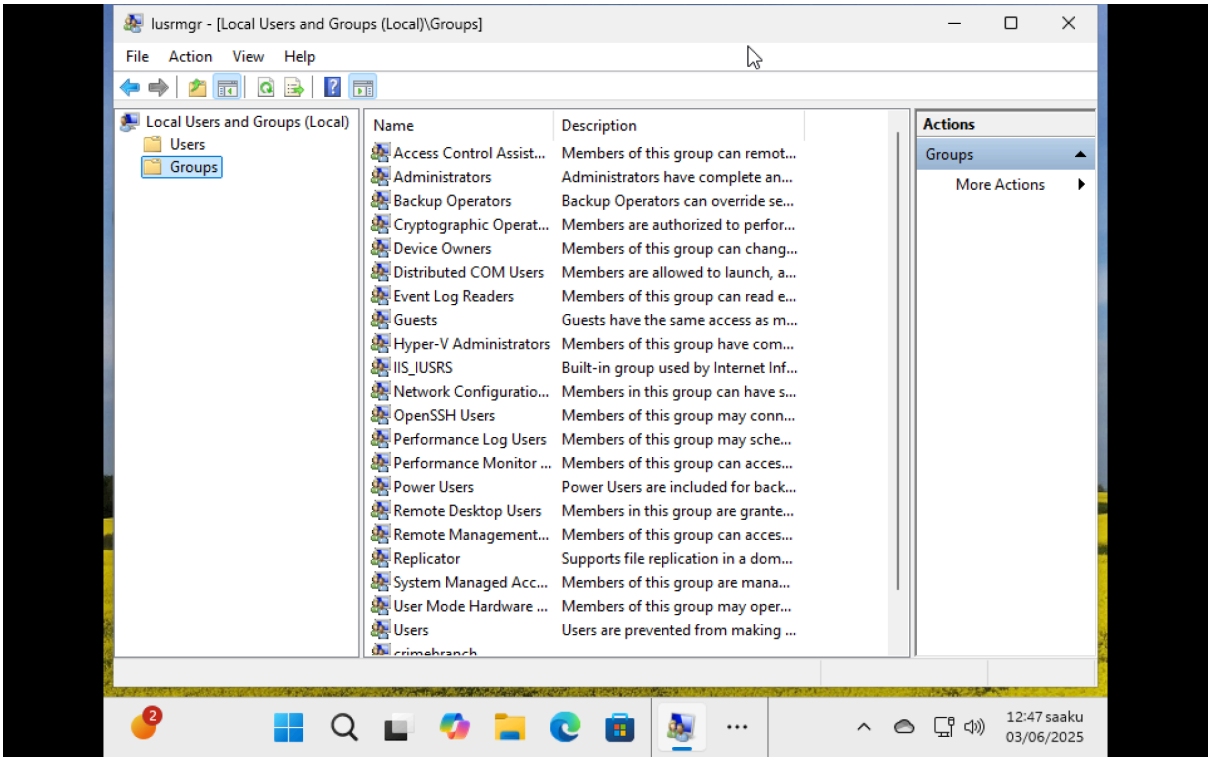
1.2 Local Users and Domains

When Windows is first installed or a new computer is started, you are prompted to create a **local user account**. This account stores personal settings, access permissions, and file locations specific to the user. Windows also includes two default accounts—**Administrator** and **Guest**—both of which are disabled by default for security reasons.

Security best practices include:

- **Do not enable the Administrator account** for everyday use.
- Avoid giving standard users administrative privileges.
- When a task requires administrative rights, the system prompts for the Administrator password to authorize only that specific action. This helps prevent unauthorized software installation or file access.
- The **Guest account** should remain disabled because it provides a default environment with limited privileges and no password, which poses a security risk.

Windows simplifies user management through **groups**, which are collections of users sharing specific permissions. Users can belong to multiple groups, inheriting all permissions from those groups. Some permissions, like "explicit deny," override others when conflicts occur.



Steps to Open Local Users and Groups Management Console (lusrmgr.msc):

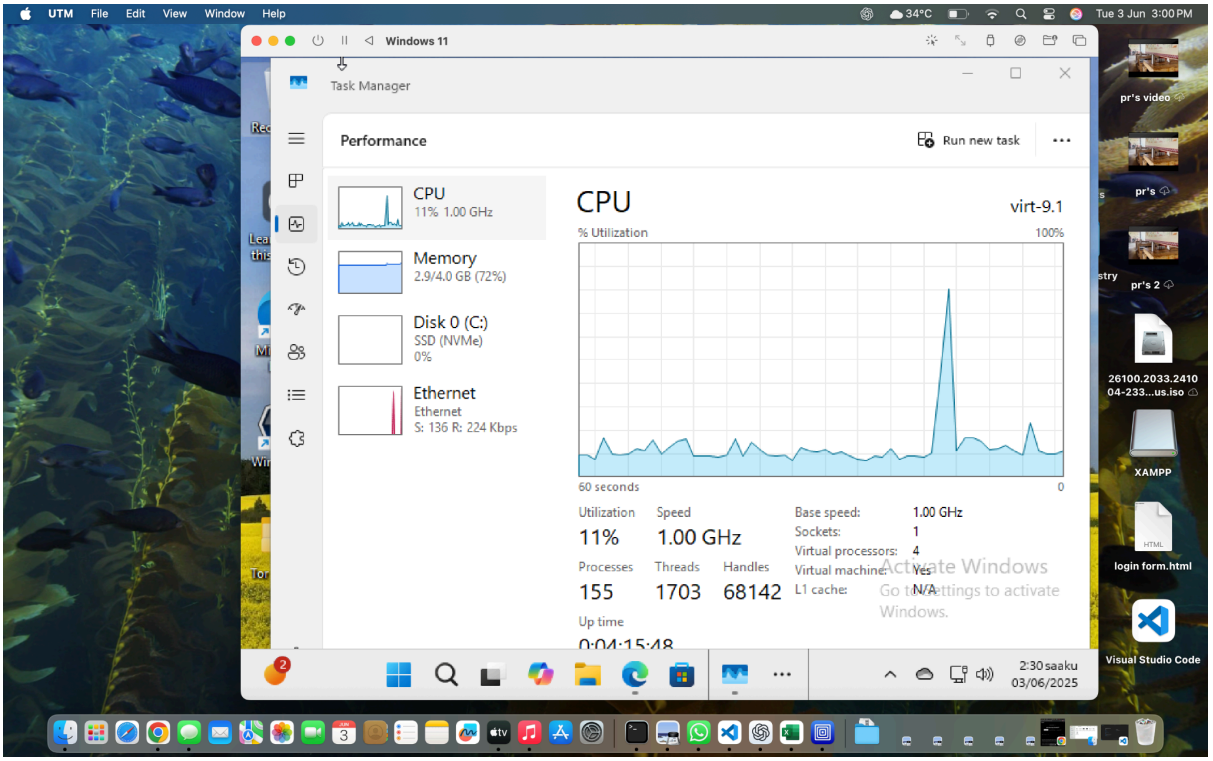
1. Press **Windows Key + R** to open the **Run** dialog box.
2. Type **lusrmgr.msc** into the Run box.
3. Press **Enter** or click **OK**.
4. The **Local Users and Groups** window will open, showing two folders: **Users** and **Groups**.
5. From here, you can manage user accounts and groups on the local computer.

1.3 Task Manager and Resource Monitor

Windows provides two essential tools for monitoring and managing system performance and processes: **Task Manager** and **Resource Monitor**. These tools are crucial for administrators and security analysts, especially when troubleshooting issues or investigating suspected malware activity.

Task Manager

Task Manager gives a snapshot of running applications, services, and processes, along with system resource usage such as CPU, memory, disk, and network. It helps identify processes that are causing problems or consuming excessive resources.



Key Tabs in Task Manager:

- **Processes:**

  Lists all currently running programs and background processes. Displays CPU, memory, disk, and network usage per process. Allows users to end problematic processes or view their properties.

- **Performance:**

  Shows overall CPU, memory, disk, and network usage with detailed graphs and statistics, helping diagnose performance bottlenecks.

- **App History:**

  Tracks resource usage over time for applications, highlighting those consuming unusual amounts of CPU or network resources.

- **Startup:**

  Displays all programs and services that automatically start when Windows boots. Administrators can disable unnecessary startup items to improve boot time and

performance.

- **Users:**

  Lists all logged-in users and the resources their processes are using. Admins can disconnect users if needed.

- **Details:**

  Offers advanced process management like setting CPU priority and affinity (which CPU cores a process can use). Includes the **Analyze wait chain** feature to detect if a process is stalled or waiting on another.

- **Services:**

  Shows running and stopped services, along with their Process IDs (PIDs). Provides quick access to the Services console for deeper management.

Resource Monitor

When detailed insight into system resource usage is needed, Resource Monitor offers granular information about CPU, memory, disk, and network activity per process.

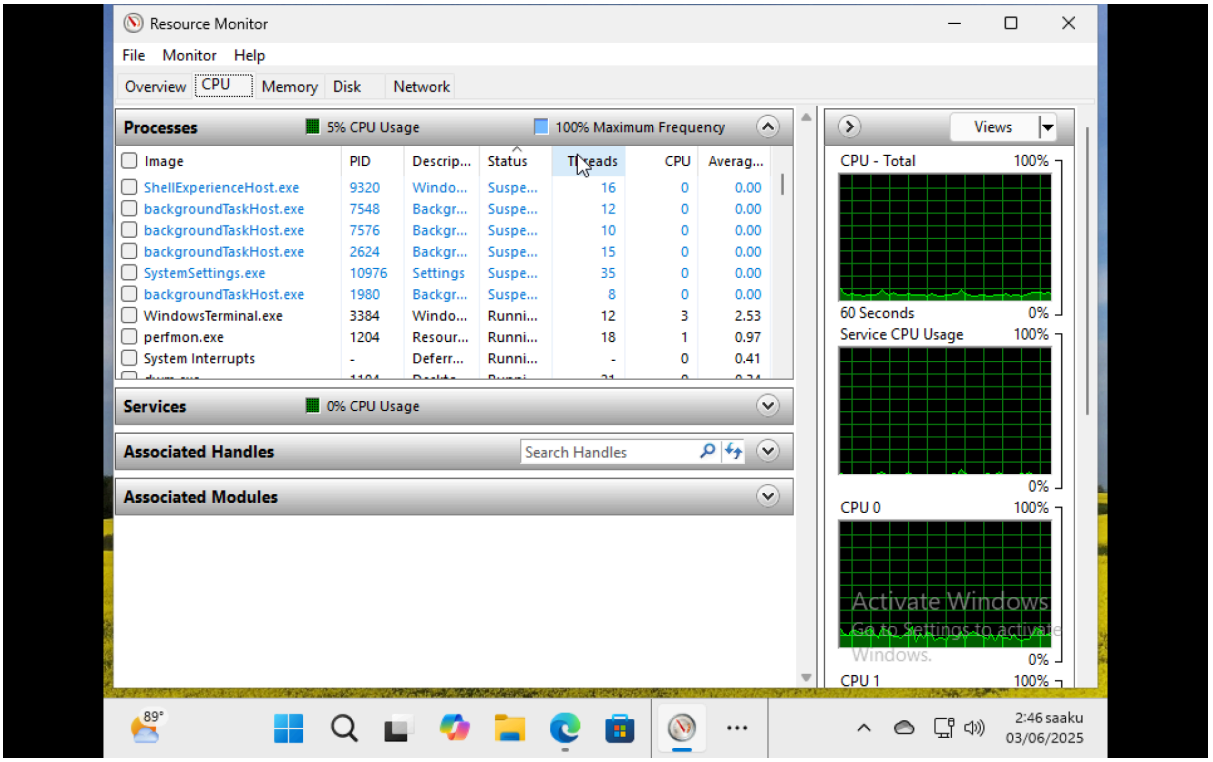


Fig:Resource Monitor

Key Tabs in Resource Monitor:

- **Overview:**

  Displays a general summary of all resource usage. Selecting a specific process filters all tabs to focus on that process.

- **CPU:**

  Lists process IDs, thread counts, CPU cores used, and CPU utilization. Shows services, handles, and modules related to each process.

- **Memory:**

  Details memory consumption statistics per process, including RAM usage.

- **Disk:**

  Shows disk read/write activity per process and summarizes storage device usage.

- **Network:**

  Displays processes using the network, including read/write data stats, active TCP connections, and listening ports. This is vital for detecting unauthorized network activity or suspicious communications.

1.5 Networking Configuration in Windows

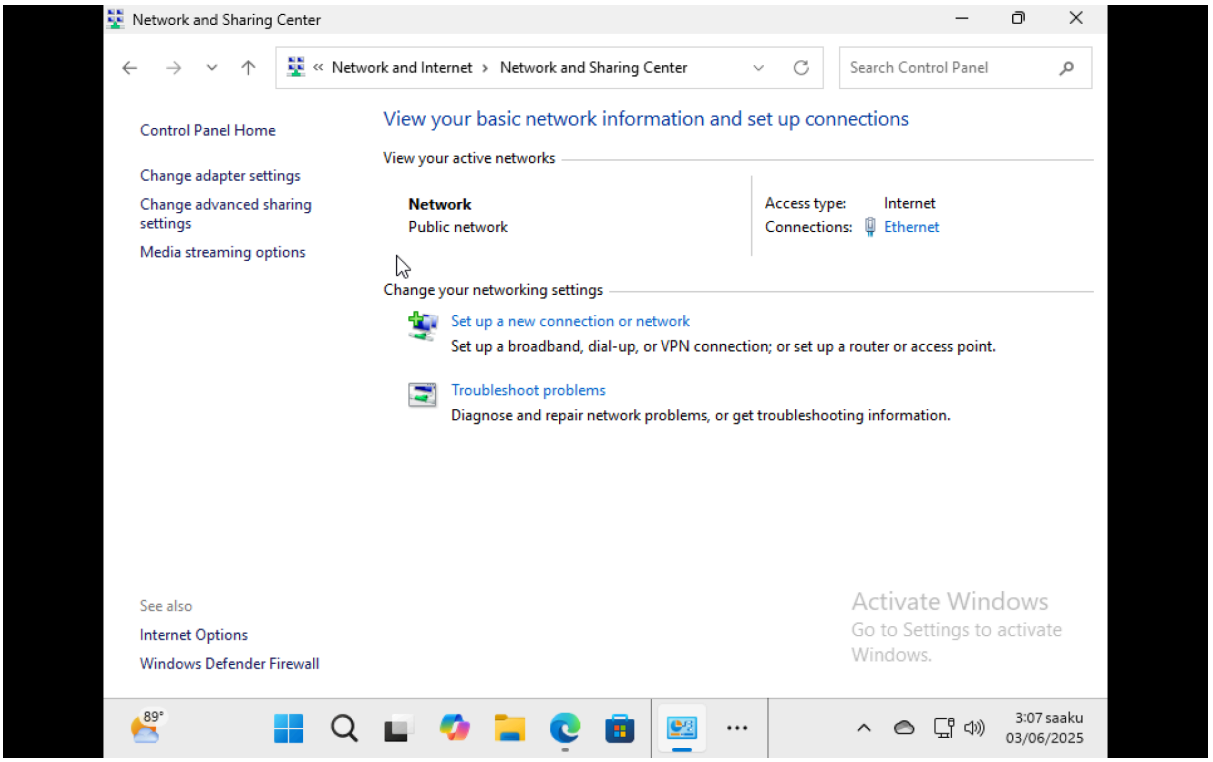
One of the most essential features of any operating system is its ability to connect to a **network**. Without it, users can't access shared resources, local servers, or the internet. In Windows, networking properties and connections are managed through the **Network and Sharing Center**.

Network and Sharing Center

The **Network and Sharing Center** provides an overview of active network connections and their types (wired or wireless). It also displays whether the system is connected to the internet and whether the network is set as **Private**, **Public**, or **Guest**.

From this tool, users can:

- View and manage current network connections.
- Set up new network connections or troubleshoot issues.
- Access advanced sharing settings.
- Change adapter settings (for static IP setup, DNS changes, etc.).



Note: Windows 10 version 1803 and later removed the HomeGroup feature.

Change Adapter Settings

To configure network adapter settings:

1. **Open Network and Sharing Center.**
2. Click **Change adapter settings** from the left panel.
3. This shows all available adapters (Ethernet, Wi-Fi, VPN, etc.).

From here:

- **Right-click** on the desired adapter and choose **Properties**.
- In the list, click **Internet Protocol Version 4 (TCP/IPv4)** or **TCP/IPv6** depending on the network protocol.
- Click **Properties** to modify the IP configuration.

IPv4 Configuration Options:

- **Obtain an IP address automatically**: Used when a DHCP server is available on the network.
- **Use the following IP address**: Allows manual configuration of the:
    - IP Address
    - Subnet Mask
    - Default Gateway
    - Preferred and Alternate DNS Servers

Click **OK** to save the changes.

1.6 Accessing Network Resources in Windows

Windows uses networking for critical services like **web browsing**, **email**, **file sharing**, and **remote management**. One key protocol that enables file and resource sharing in a Windows environment is **SMB (Server Message Block)**.

File Sharing and Permissions

To **share resources** (like folders), you must:

- Choose what to share (folder or drive).
- Set **permissions** (Read, Write, Modify, Full Control, or Deny).
- Optionally use **Access Control Lists (ACLs)** to enforce granular access based on user or group.

This is crucial from a **security perspective** to ensure only authorized users can access or modify shared data.

Administrative Shares

Windows automatically creates **hidden shares** for system management purposes. These are called **administrative shares** and are recognizable by the $ at the end of the share name.

Common admin shares:

- C$, D$, E$: Root of each drive.

- ADMIN$: The Windows installation directory.
- PRINT$: Network printers folder.

1.6.1 Remote Desktop Access (RDP)

Used to **control remote Windows PCs**.

Steps:

1. Open **Remote Desktop Connection** (mstsc).
2. Enter the **remote IP/hostname**.
3. Enter **remote credentials**.

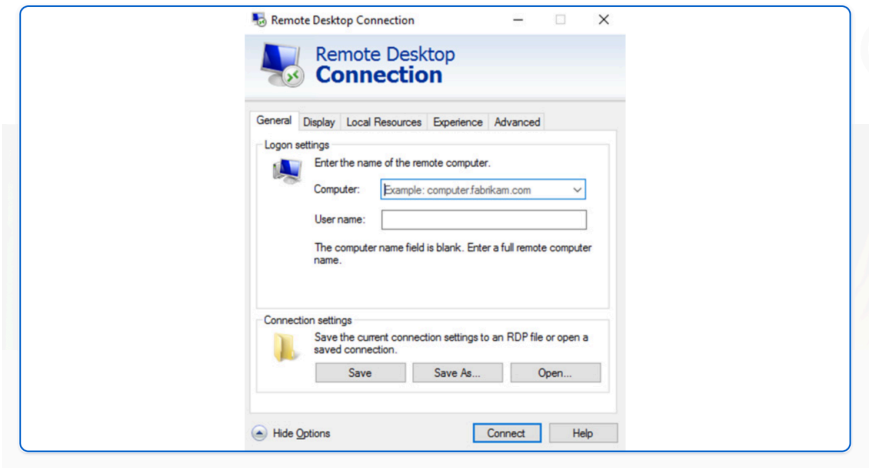


Fig: Remote Desktop

Reference:https://www.netacad.com/courses/operating-systems-basics?courseLang=en-US