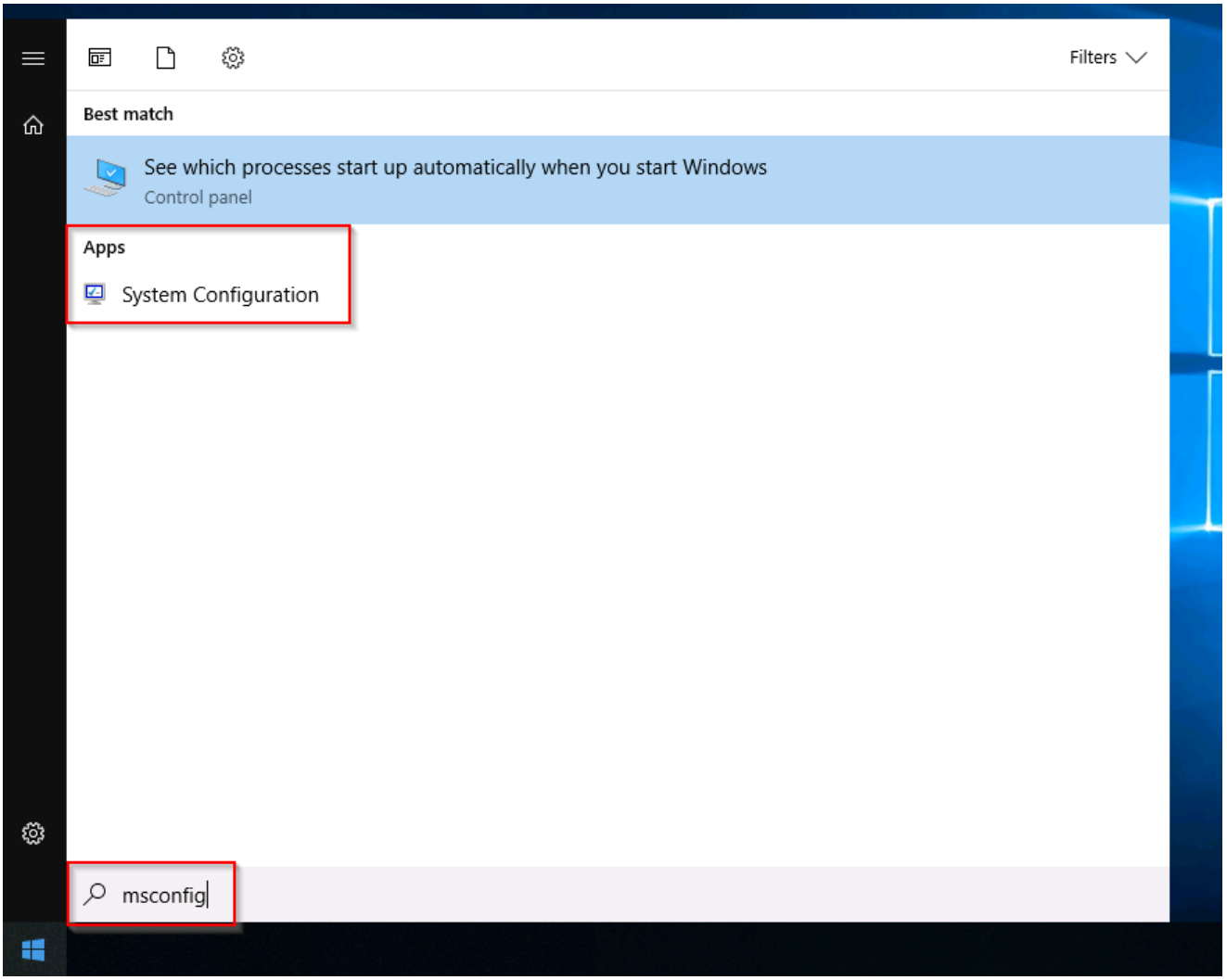
Windows Fundamentals

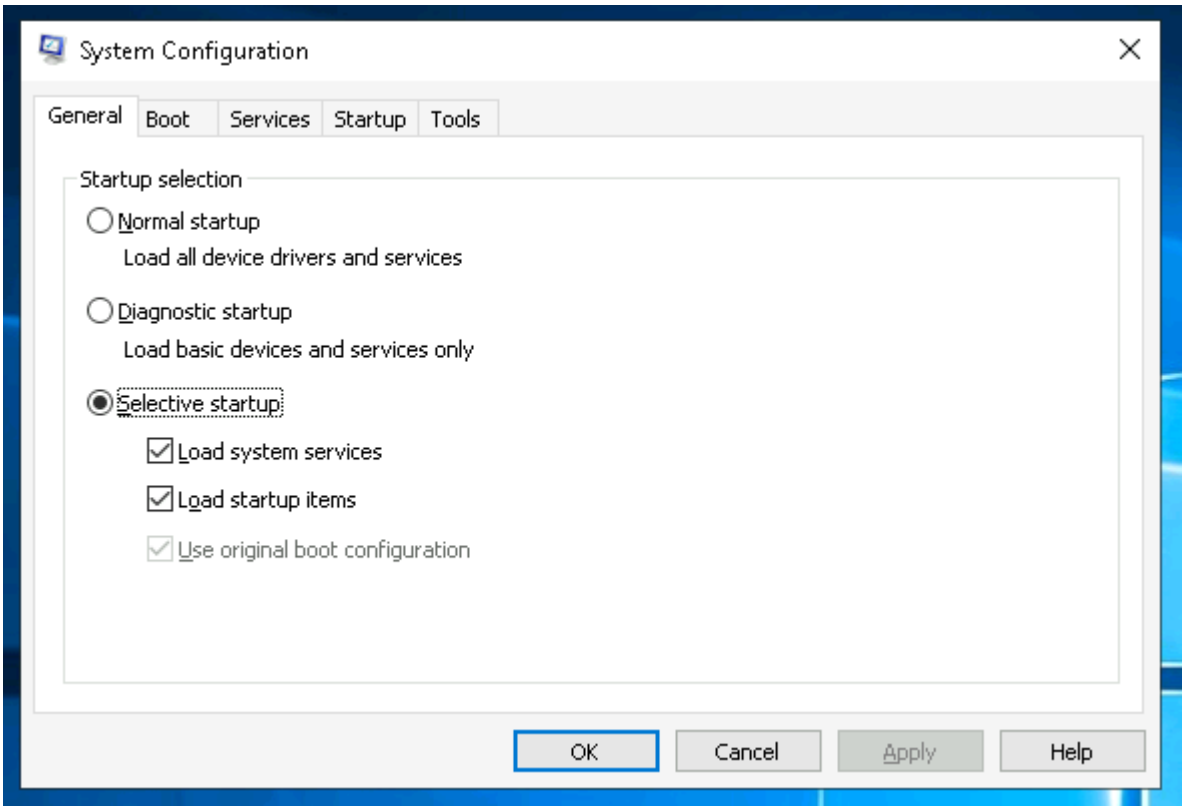
System Configuration

The **System Configuration** utility (`MSConfig`) is for advanced troubleshooting, and its main purpose is to help diagnose startup issues.



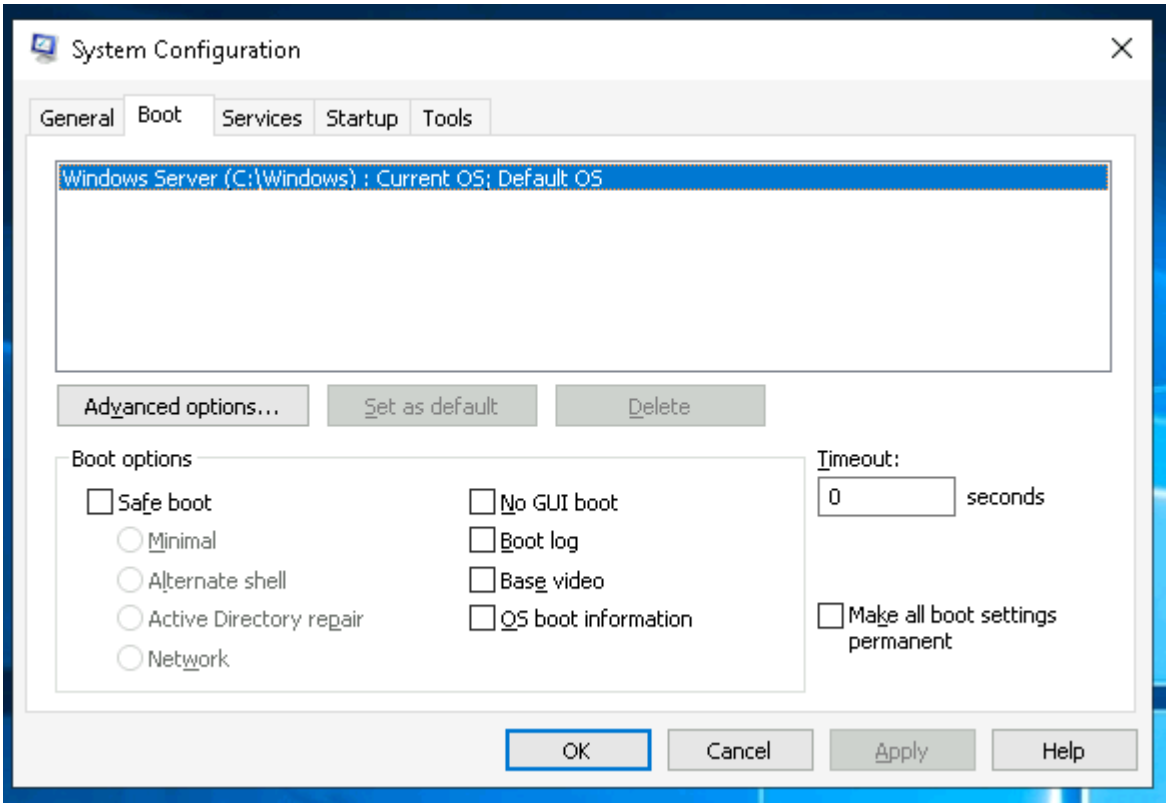
he utility has five tabs across the top. Below are the names for each tab. We will briefly cover each tab in this task.

1. General
2. Boot
3. Services
4. Startup
5. Tools

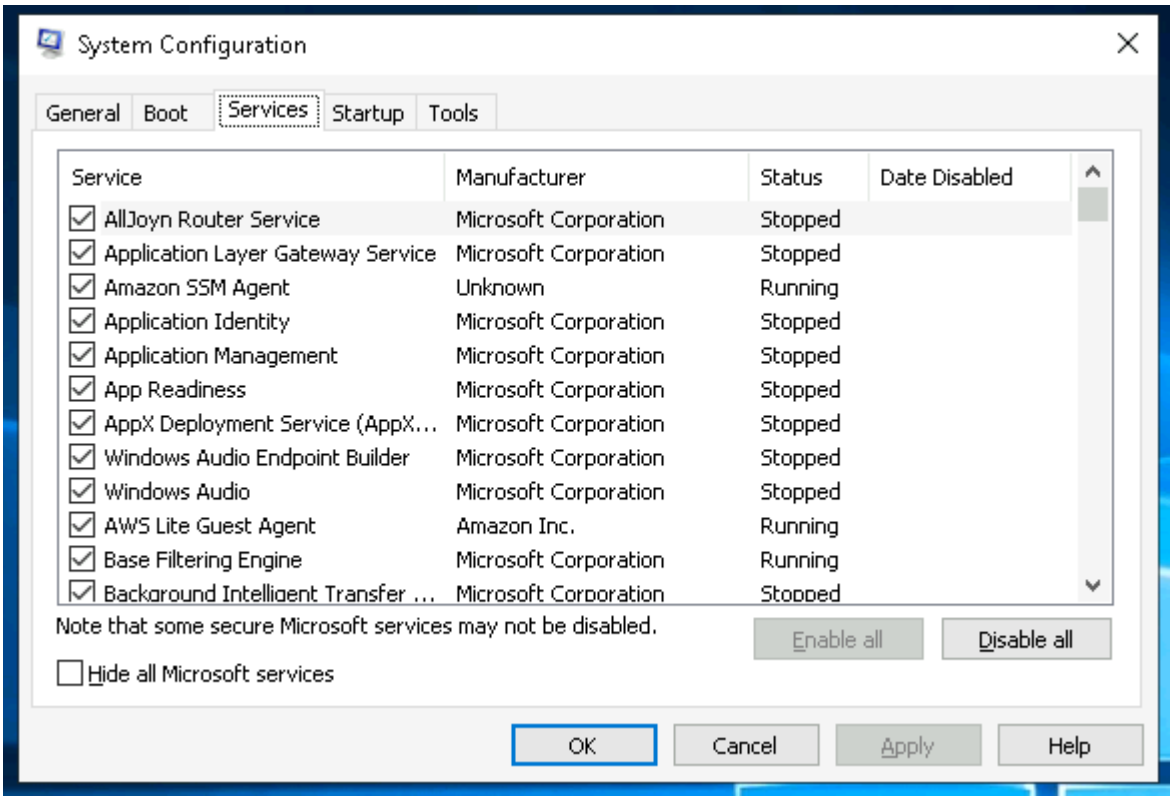


In the **General** tab, we can select what devices and services for Windows to load upon boot. The options are: **Normal**, **Diagnostic**, or **Selective**.

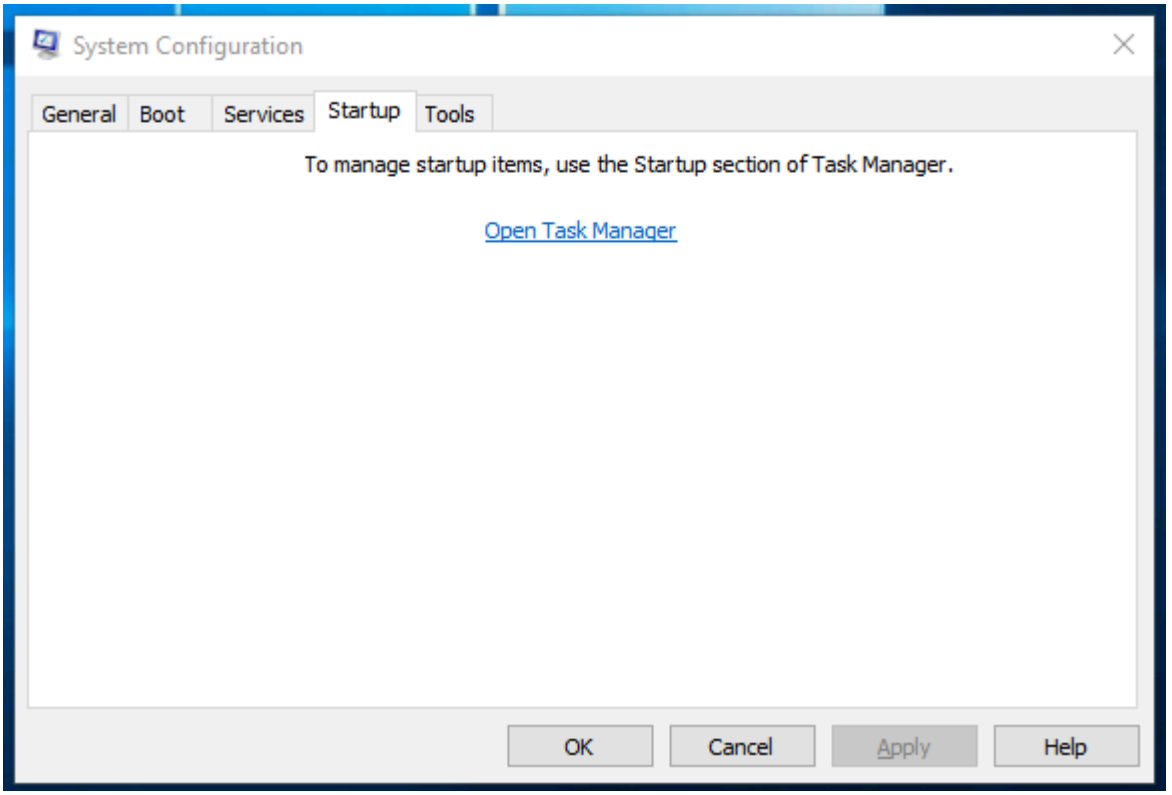
In the **Boot** tab, we can define various boot options for the Operating System.



The **Services** tab lists all services configured for the system regardless of their state (running or stopped). A service is a special type of application that runs in the background.



In the **Startup** tab, you won't see anything interesting in the attached VM. Below is a screenshot of the Startup tab for **MSConfig** from my local machine.



As you can see, Microsoft advises using **Task Manager (** `taskmgr` **)** to manage (enable/disable) startup items. The System Configuration utility is **NOT** a startup management program.

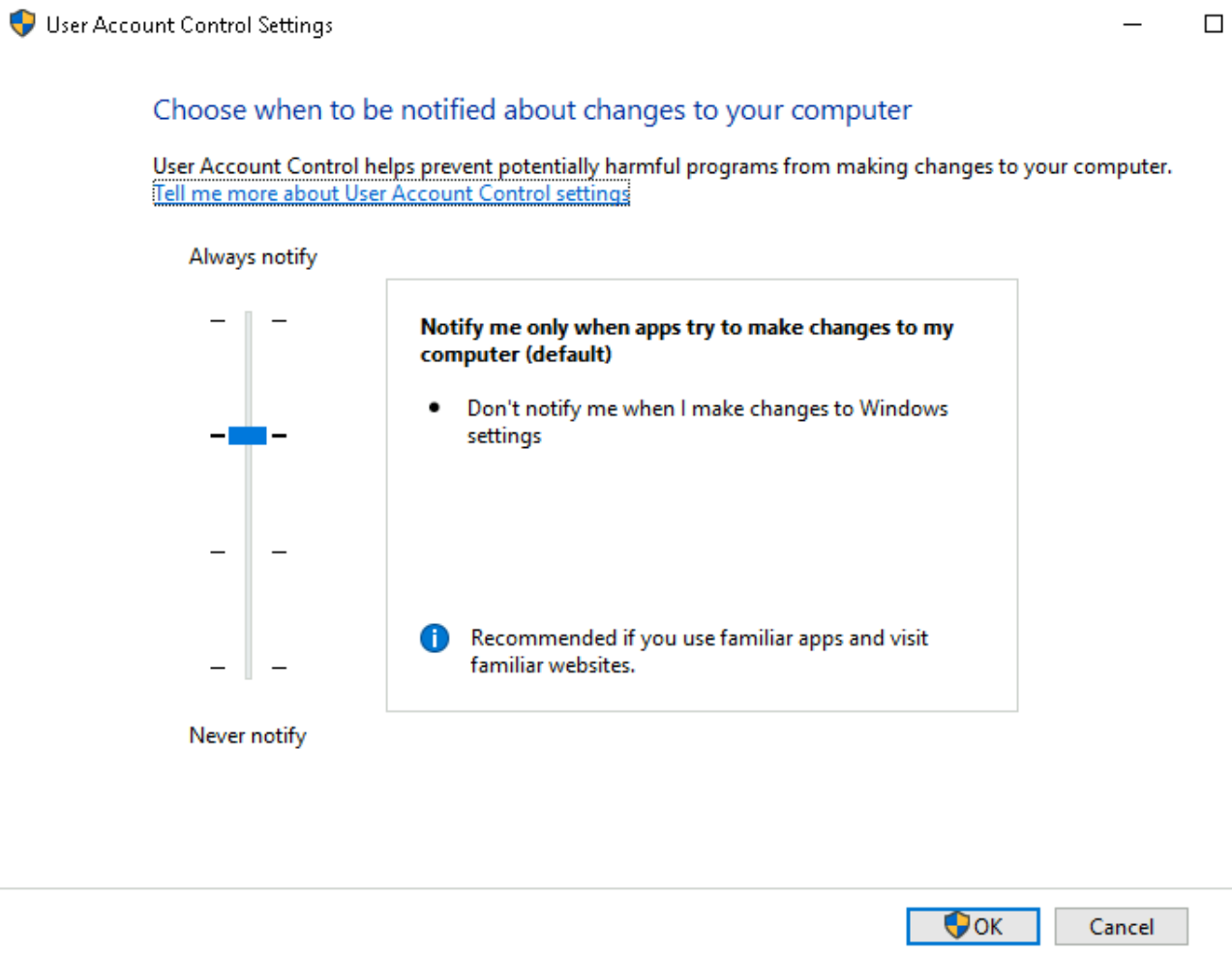
User Account Control (UAC)

The UAC settings can be changed or even turned off entirely (not recommended). You can move the slider to see how the setting will change the UAC settings and Microsoft's stance on the setting.

This slider has four security levels, each of which controls how Windows alerts you when apps or users try to make changes at the system level. They fall into four standard categories as explained below:

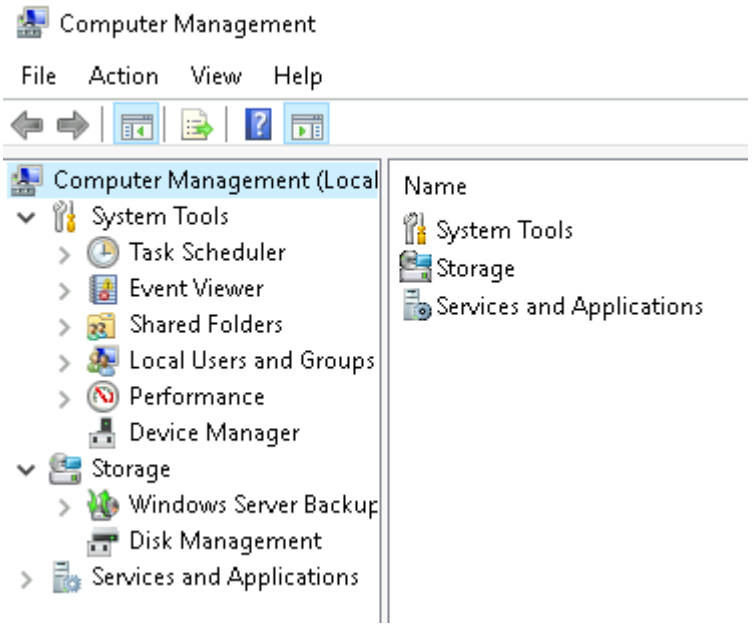
- **Always notify:** This is the highest security. Windows notifies you whenever any apps or you yourself try to make changes, and the desktop dims (Secure Desktop).
- **Notify for apps**: Windows notifies only when *apps* try to make changes, but not when you change Windows settings. This option is enabled by default.
- **Notify without dimming:** Same as above (Notify for apps), but this time the screen does not dim.
- **Never notify:** Notifications are turned off. Windows won't warn you about any changes made by you or any apps.

You can find the current level by looking at the position of the slider in the `User Account Control settings` window, as shown below:



Computer Management

The **Computer Management** (`compmgmt`) utility has three primary sections: System Tools, Storage, and Services and Applications.

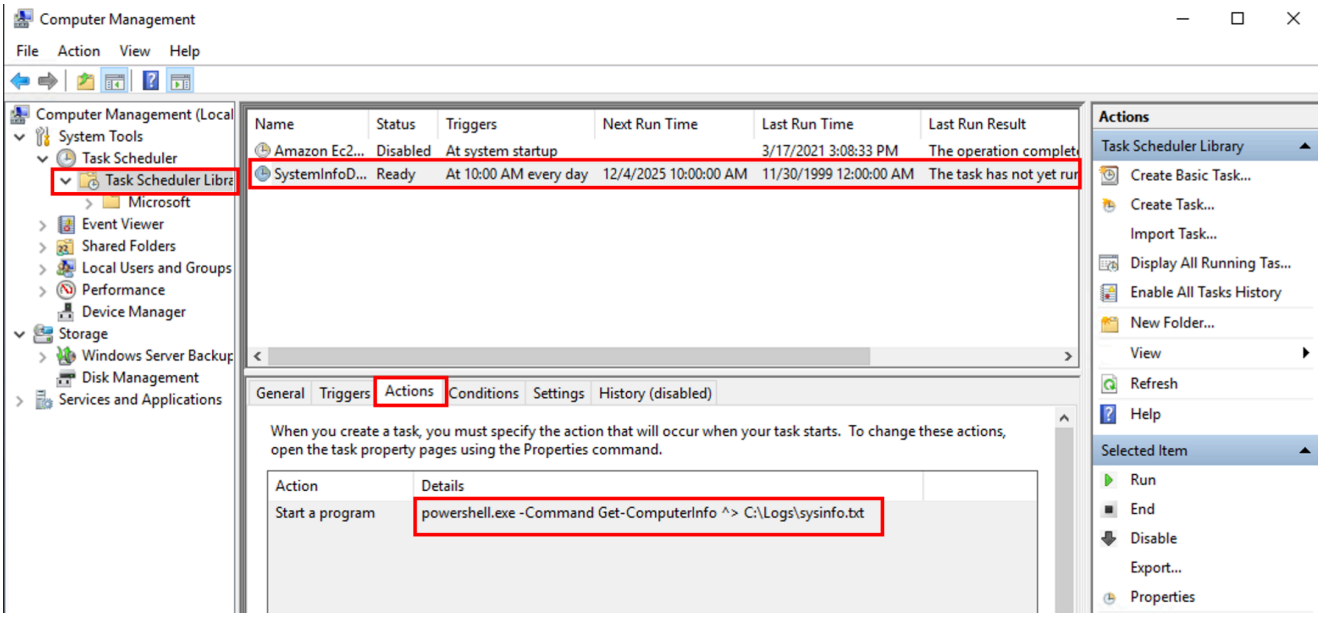


System Tools

Task Scheduler. Per Microsoft, with Task Scheduler, we can create and manage common tasks that our computer will carry out automatically at the times we specify.

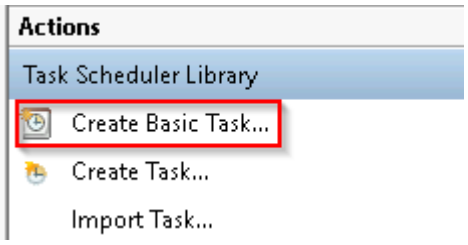
A task can run an application, a script, etc., and tasks can be configured to run at any point. A task can run at log in or at log off. Tasks can also be configured to run on a specific schedule, for example, every five mins.

To view the scheduled tasks that are present on the system, click `Task Scheduler Library` . This will display all the scheduled tasks of the system. You can click on any of them to view their details. The screenshot below shows a scheduled task named `SystemInfoDailyLog` configured to run `every day at 10:00 AM` . Here, you will see the program or command that will run when the task is triggered.



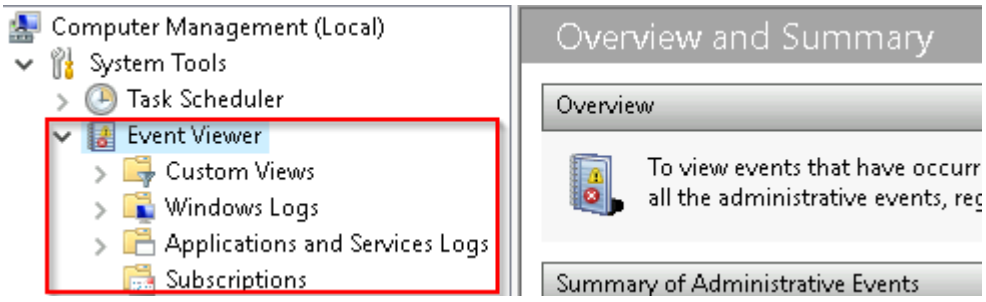
It is also important to note that some scheduled tasks are not recurring and are made to run just once at a specific time. In this case, we would see something like `At 2:50 PM on 6/15/2025` as the trigger.

To create a basic task, click on `Create Basic Task` under **Actions** (right pane).



Event Viewer.

Event Viewer allows us to view events that have occurred on the computer. These records of events can be seen as an audit trail that can be used to understand the activity of the computer system. This information is often used to diagnose problems and investigate actions executed on the system.



Event Viewer has three panes.

1. The pane on the left provides a hierarchical tree listing of the event log providers. (as shown in the image above)
2. The pane in the middle will display a general overview and summary of the events specific to a selected provider.
3. The pane on the right is the actions pane.

There are five types of events that can be logged. Below is a table from docs.microsoft.com providing a brief description for each.

The following table describes the five event types used in event logging.

Event type	Description
Error	An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event.
Information	An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.
Success Audit	An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event.
Failure Audit	An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event.

The standard logs are visible under Windows Logs. Below is a table from docs.microsoft.com providing a brief description for each.

The event log contains the following standard logs as well as custom logs:

Log	Description
Application	Contains events logged by applications. For example, a database application might record a file error. The application developer decides which events to record.
Security	Contains events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can start auditing to record events in the security log.
System	Contains events logged by system components, such as the failure of a driver or other system component to load during startup.
CustomLog	Contains events logged by applications that create a custom log. Using a custom log enables an application to control the size of the log or attach ACLs for security purposes without affecting other applications.

Shared Folders is where you will see a complete list of shares and folders shared that others can connect to.

Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC

In the above image, under Shares, are the default share of Windows, C $, and default remote administration shares created by Windows, such as ADMIN$.

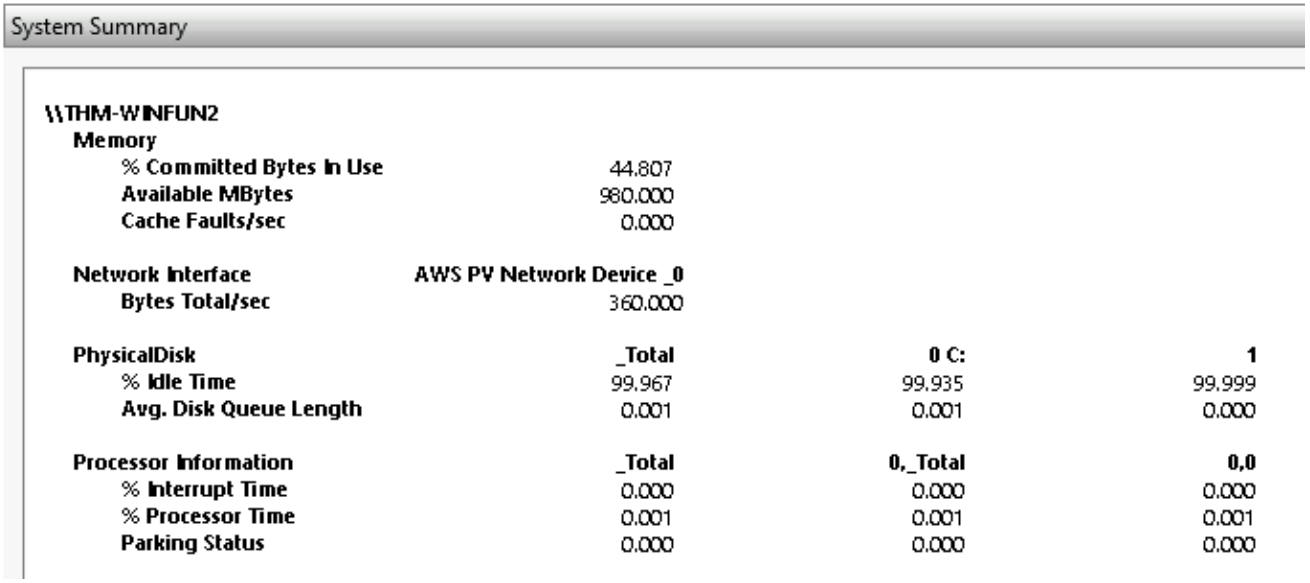
As with any object in Windows, you can right-click on a folder to view its properties, such as Permissions (who can access the shared resource).

Under **Sessions**, you will see a list of users who are currently connected to the shares. In this VM, you won't see anybody connected to the shares.

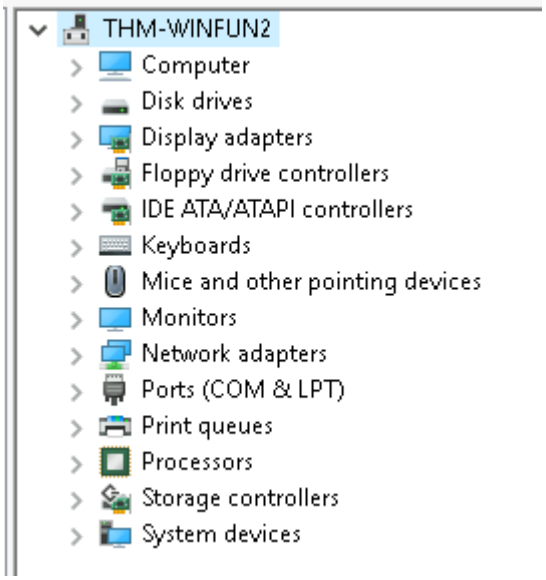
All the folders and/or files that the connected users access will list under **Open Files**.

In **Performance**, you'll see a utility called **Performance Monitor** (`perfmon`).

Perfmon is used to view performance data either in real-time or from a log file. This utility is useful for troubleshooting performance issues on a computer system, whether local or remote.



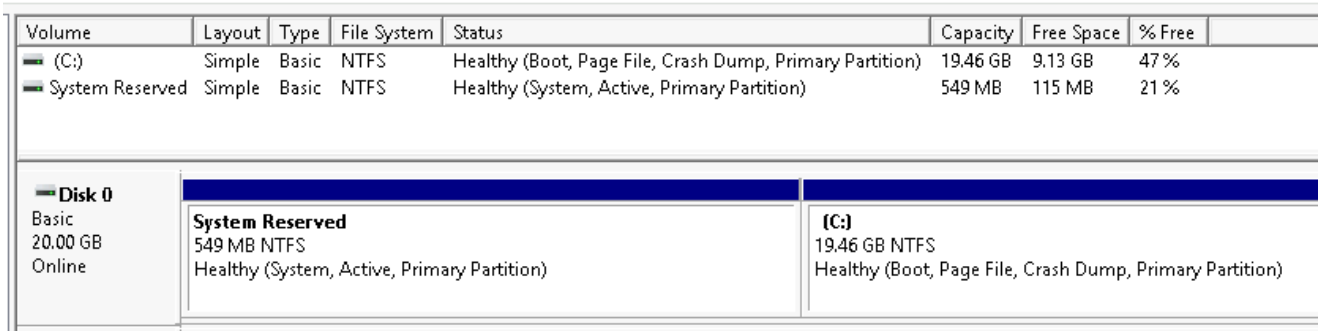
Device Manager allows us to view and configure the hardware, such as disabling any hardware attached to the computer.



Storage

Under Storage is **Windows Server Backup** and **Disk Management**. We'll only look at Disk Management in this room.

Note: Since the virtual machine is a Windows Server operating system, there are utilities available that you will typically not see in Windows 10.

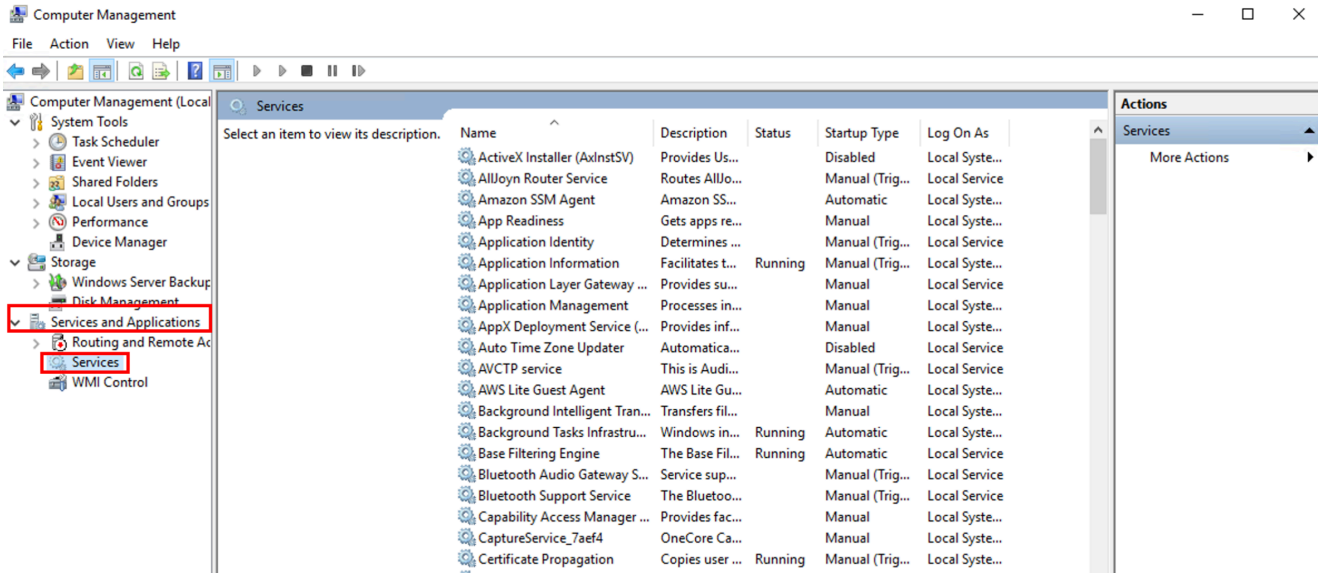


Disk Management is a system utility in Windows that enables you to perform advanced storage tasks. Some tasks are:

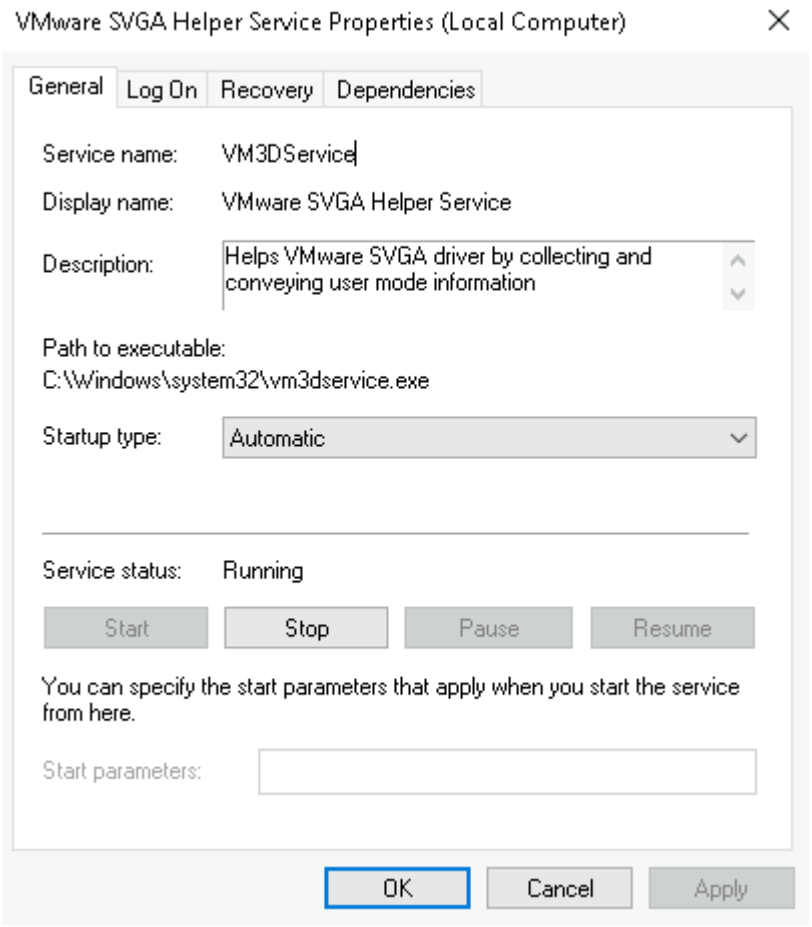
- Set up a new drive
- Extend a partition
- Shrink a partition
- Assign or change a drive letter (ex. E:)

Services and Applications

Recall from the previous task, a service is a special type of application that runs in the background. You can see all the services and their statuses by clicking the Services button given under the Services and Applications section, as shown below:



The services shown above have their display names, status, and other values. If you want to get more information about any service, right-click on the service and click `properties`. Here, you will see additional details, such as the service name (which differs from the display name), the path to its executable, its startup type, and other relevant information.



There is a field known as Startup type in a service's Properties window, as shown above. It determines how and when the service is configured to start. We can set a service to `Automatic`, which means it starts every time the system boots, or `Manual`, which means it only starts when another process or user triggers this service, or `Disabled`, which means it should not run at all. The service shown in the screenshot above is set to `Automatic`.

System Information

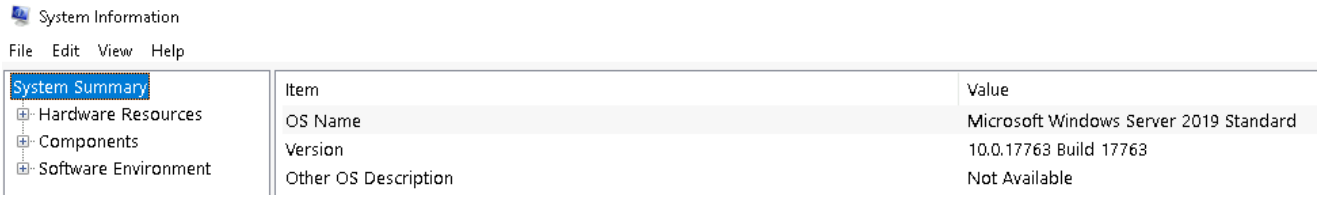
What is the **System Information** (`msinfo32`) tool?

Per Microsoft, "*Windows includes a tool called Microsoft System Information (Msinfo32.exe). This tool gathers information about your computer and displays a comprehensive view of your hardware, system components, and software environment, which you can use to diagnose computer issues.*"

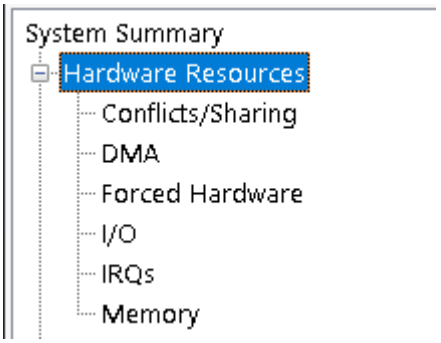
The information in **System Summary** is divided into three sections:

- **Hardware Resources**
- **Components**
- **Software Environment**

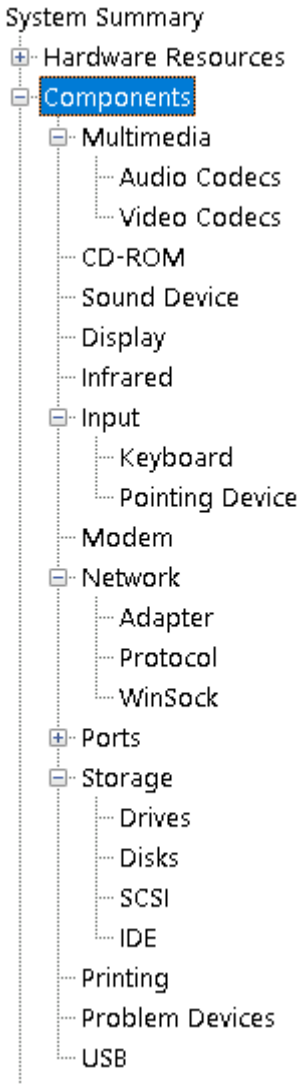
System Summary will display general technical specifications for the computer, such as processor brand and model.



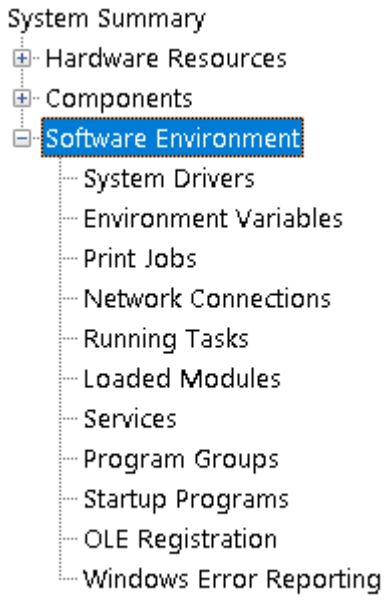
The information displayed in **Hardware Resources** is not for the average computer user. If you want to learn more about this section, refer to the official Microsoft page.



Under **Components**, you can see specific information about the hardware devices installed on the computer. Some sections don't show any information, but some sections do, such as **Display** and **Input**.



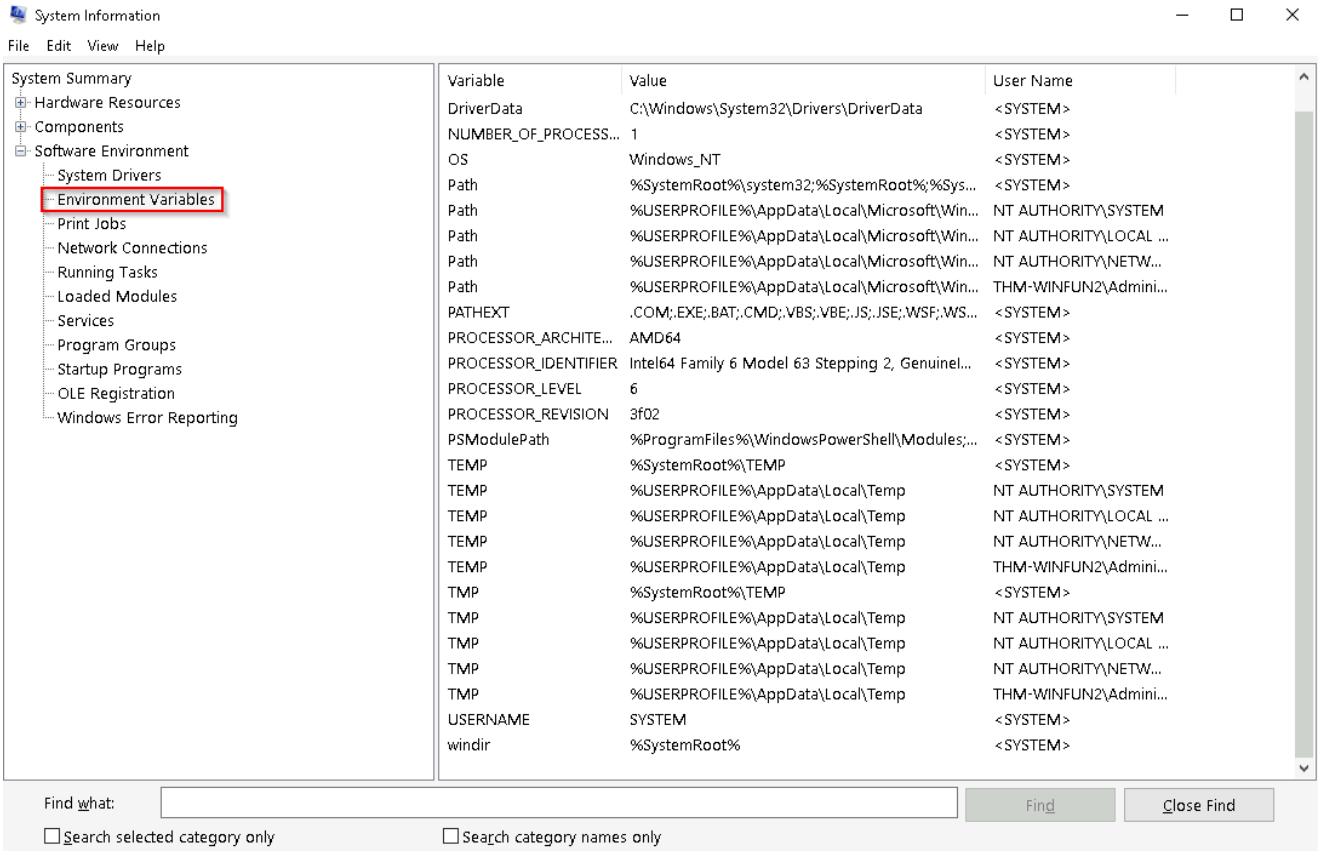
In the **Software Environment** section, you can see information about software baked into the operating system and software you have installed. Other details are visible in this section as well, such as the **Environment Variables** and **Network Connections**.



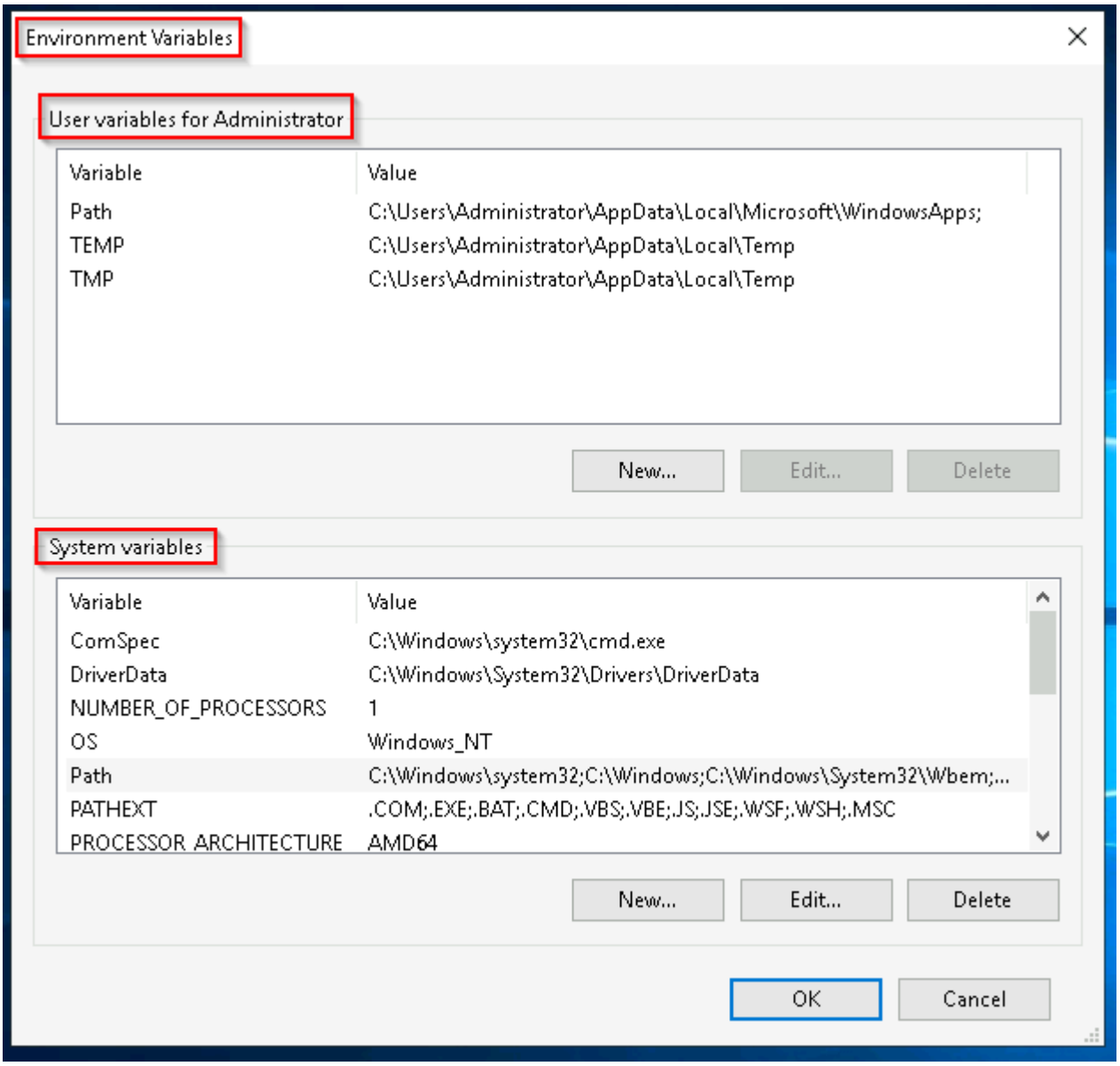
Per Environment variables store information about the operating system environment. This information includes details such as the operating system path, the number of processors used by the operating system, and the location of temporary folders.

The environment variables store data that is used by the operating system and other programs. For example, the WINDIR environment variable contains the location of the Windows installation directory. Programs can query the value of this variable to determine where Windows operating system files are located".

Click on `Environment Variables` to see the assigned values for the virtual machine.

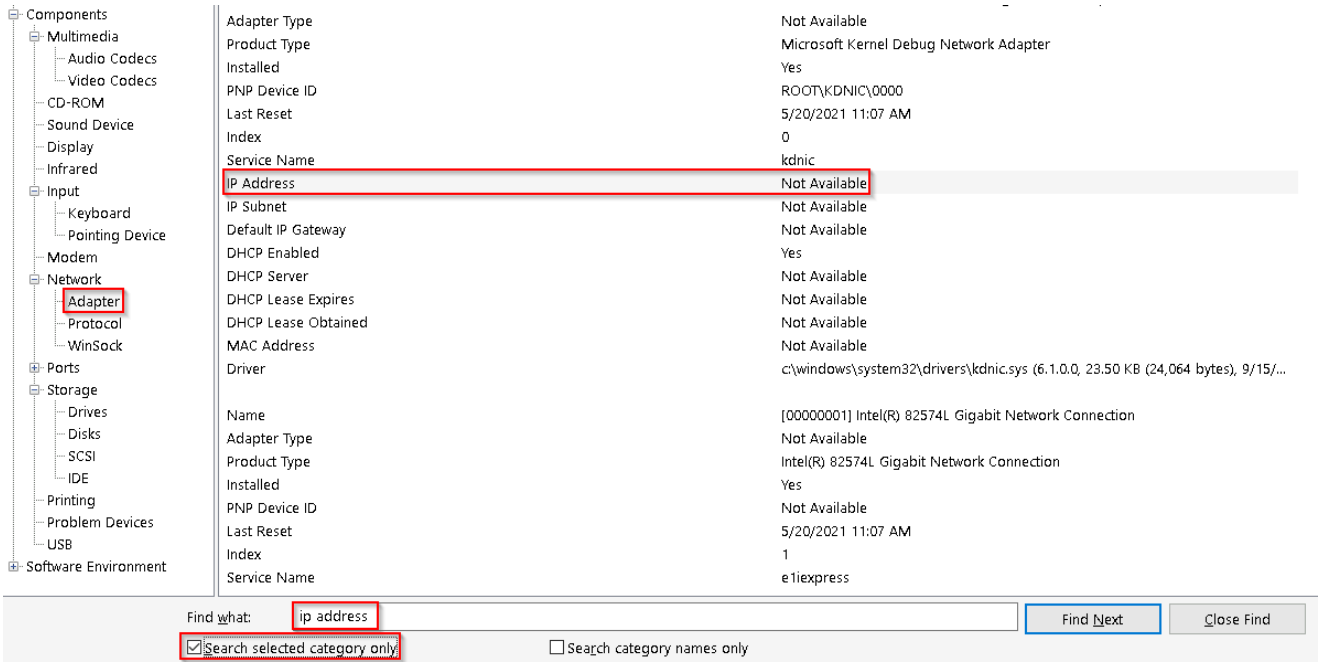


Another method to view environment variables is `Control Panel > System and Security > System > Advanced system settings > Environment Variables` **OR** `Settings > System > About > system info > Advanced system settings > Environment Variables`.



The detour is over. Let's redirect our attention back to `msinfo32` and pick up where we left off.

Towards the very bottom of this utility, there is a search bar. Please give it a go. Select Components and search for `IP address`.



Windows Registry

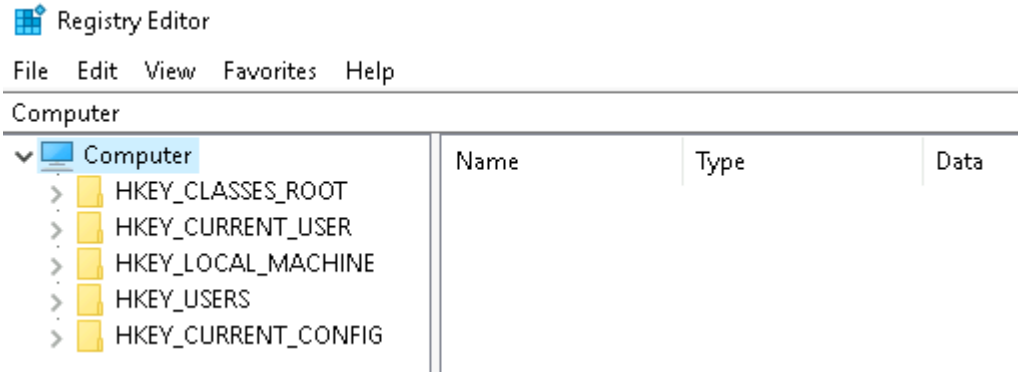
The **Windows Registry** (per Microsoft) is a central hierarchical database used to store information necessary to configure the system for one or more users, applications, and hardware devices.

The registry contains information that Windows continually references during operation, such as:

- Profiles for each user
- Applications installed on the computer and the types of documents that each can create
- Property sheet settings for folders and application icons
- What hardware exists on the system
- The ports that are being used.

Warning: The registry is for advanced computer users. Making changes to the registry can affect normal computer operations.

There are various ways to view/edit the registry. One way is to use the **Registry Editor** (`regedit`).

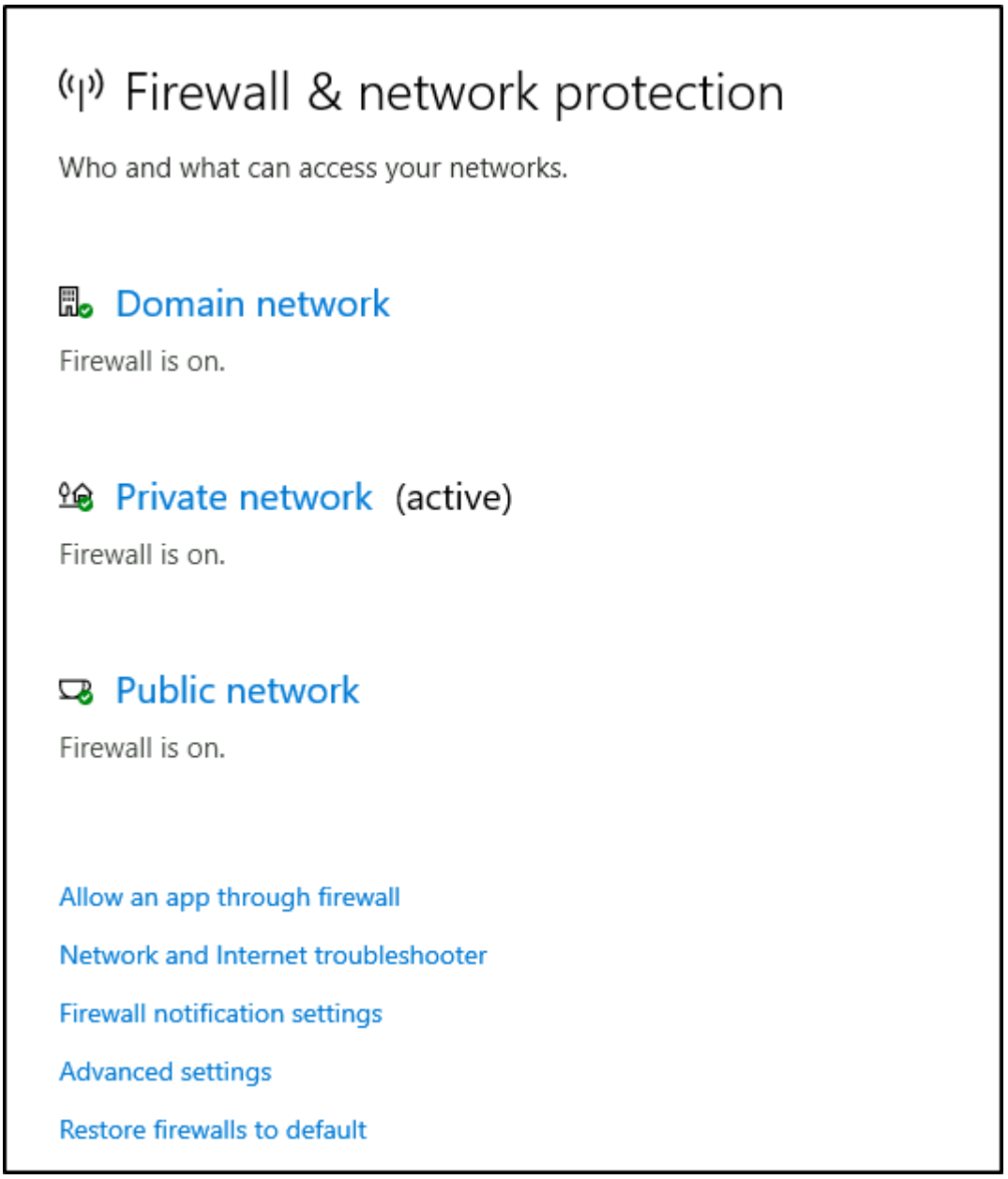


Firewall & network protection

What is a **firewall**?

Traffic flows into and out of devices via what we call ports. A firewall is what controls what is - and more importantly isn't - allowed to pass through those ports. You can think of it like a security guard standing at the door, checking the ID of everything that tries to enter or exit".

The below image will reflect what you will see when you navigate to **Firewall & network protection**.



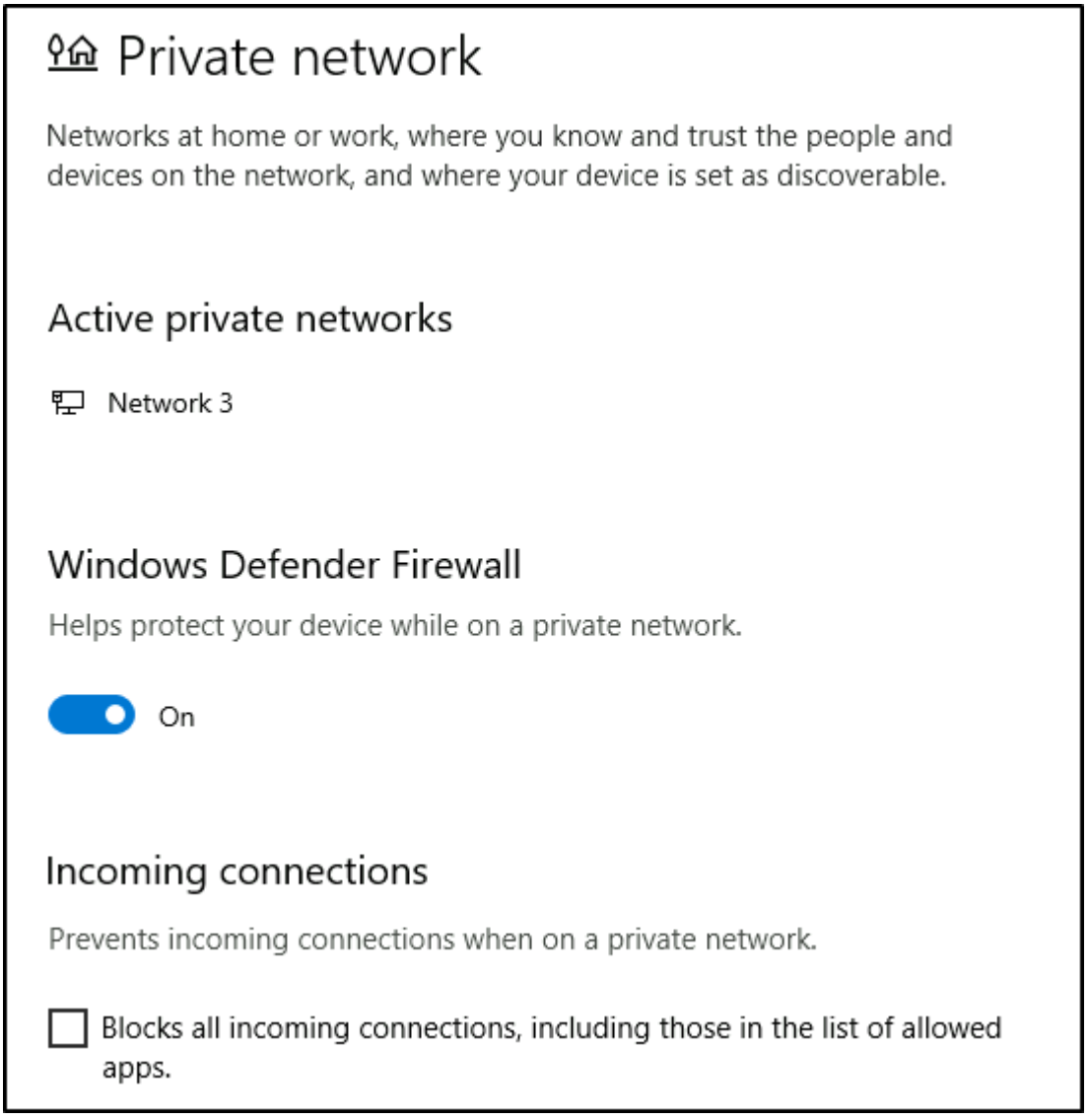
Note: Each network may have different status icons for you.

Q. What is the difference between the 3 (**Domain**, **Private**, and **Public**)?

Windows Firewall offers three firewall profiles: domain, private and public".

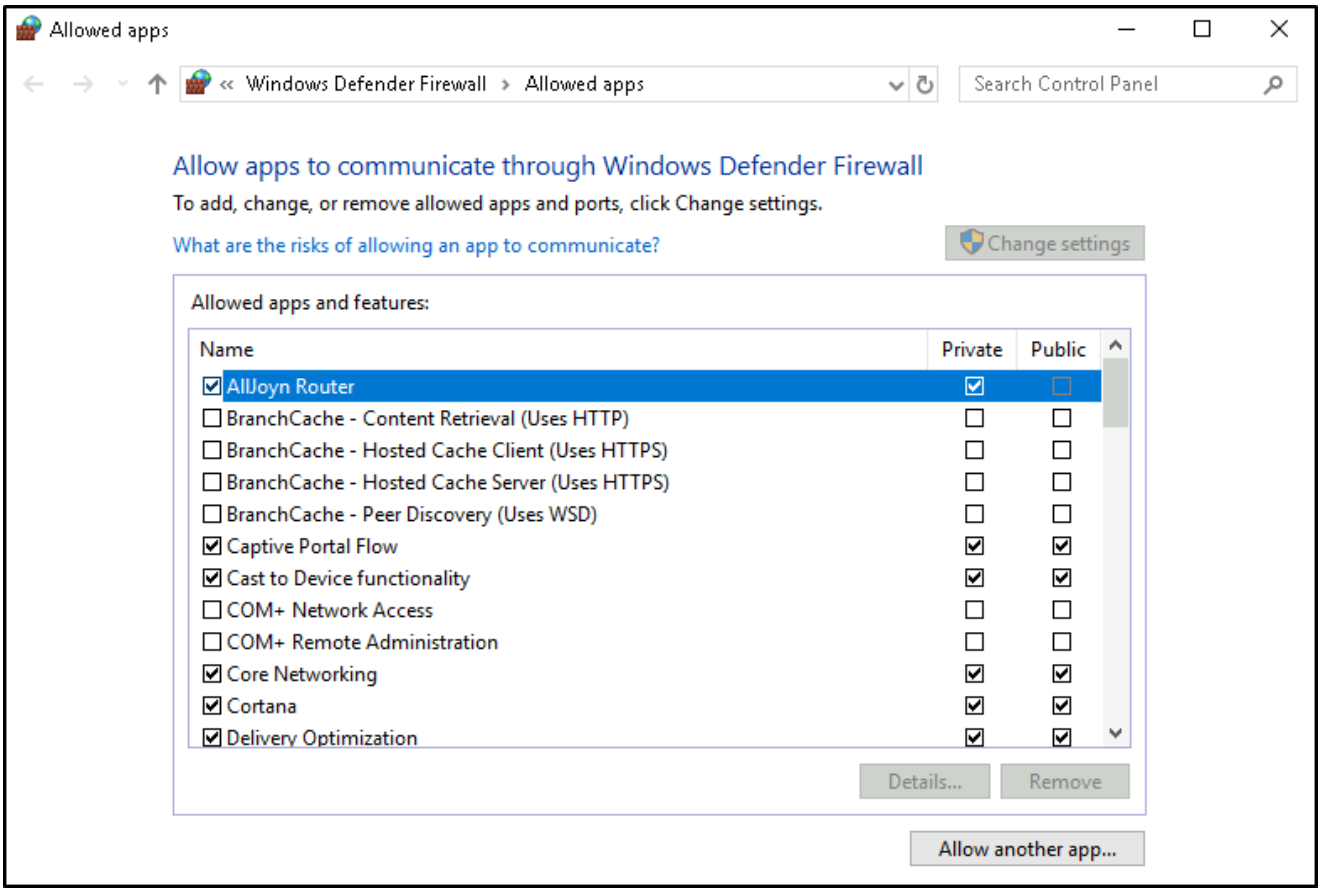
- **Domain** - *The domain profile applies to networks where the host system can authenticate to a domain controller.*
- **Private** - *The private profile is a user-assigned profile and is used to designate private or home networks.*
- **Public** - *The default profile is the public profile, used to designate public networks such as Wi-Fi hotspots at coffee shops, airports, and other locations.*

If you click on any firewall profile, another screen will appear with two options: **turn the firewall on/off** and **block all incoming connections**.



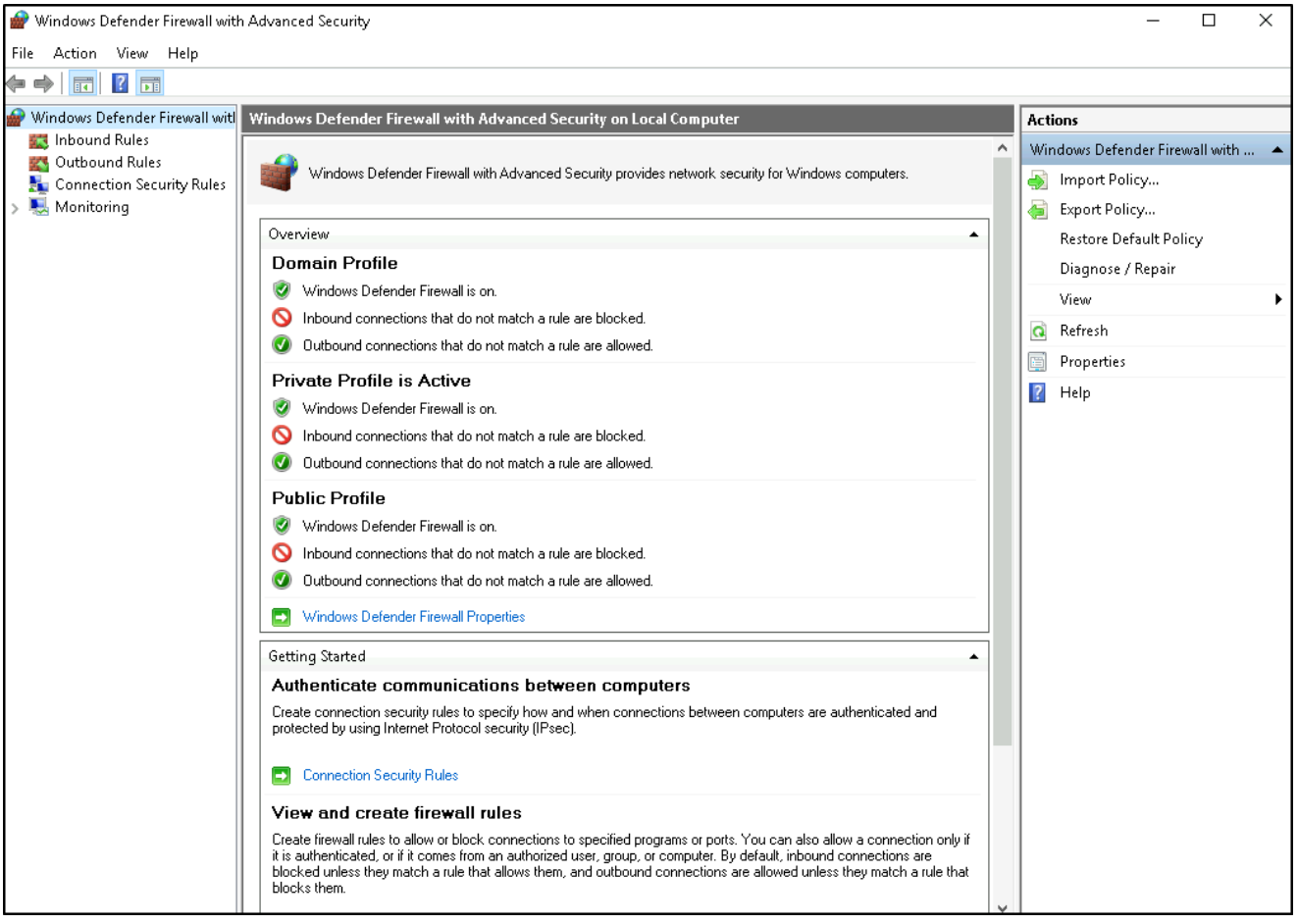
Warning: Unless you are **100%** confident in what you are doing, it is recommended that you leave your Windows Defender Firewall enabled.

Allow an app through firewall



You can view what the current settings for any firewall profile are. In the above image, several apps have access in the Private and/or Public firewall profile. Some of the apps will provide additional information if it's available via the `Details` button.

Advanced Settings



Configuring the **Windows Defender Firewall** is for advanced Windows users. Refer to the following Microsoft documentation on best practices here.

Tip: Command to open the Windows Defender Firewall is `WF.msc`.

What is **BitLocker**?

Per Microsoft, "*BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers*".

What is the **Trusted Platform Module** (**TPM**)?

"*Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM*".

VSS

Volume Shadow Copy Service (VSS) coordinates the required actions to create a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data that is to be backed up.

Volume Shadow Copies are stored on the System Volume Information folder on each drive that has protection enabled.

If VSS is enabled (**System Protection** turned on), you can perform the following tasks from within **advanced system settings**.

- **Create a restore point**
- **Perform system restore**
- **Configure restore settings**
- **Delete restore points**