Lab - Operating System Security (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

# Objectives

In this lab, you will configure Microsoft Defender Antivirus and Windows Defender Firewall.

Part 1: Microsoft Defender Antivirus

Part 2: Windows Defender Firewall

# Recommended Equipment

* A Windows device

# Instructions

## Microsoft Defender Antivirus

Microsoft Defender Antivirus is built into Windows and managed by Windows Security. It offers real-time protection against malware, viruses, and other security threats. It also receives the latest updates for virus and threat protection.

### Activate/deactivate

* + - 1. Navigate to the Windows Security dashboard. Click **Start** > **Settings** > **Update & Security** > **Windows Security**.

Note: Windows 11: Click **Start** > **Settings** > **Privacy & Security** > **Windows Security**.

* + - 1. Click **Virus & threat protection** to view the options for device protection against threats.
      2. Under the Current threats heading, you can start a quick scan and view the protection history.
      3. Click **Manage settings** under the Virus & threat protection settings.
      4. Within these settings, you can temporarily turn off real-time protection and access the latest threat protection with cloud-delivered protection. You can also modify the controlled folder access, notifications, and the exclusion settings by adding or removing files, folders, file types, and processes.
      5. Click **Back** to exit Virus & threat protection settings when done exploring.

### Updated definitions

The definitions are automatically downloaded as part of Windows Update, but you can download the definition manually.

* + - 1. Under the Virus & threat protection updates heading, click **Check for updates**.
      2. In the Protection updates, click **Check for updates**.

#### Question:

Which version has security intelligence? When was the version created and last updated?

Type your answers here.

Answers will vary. The answer depends on when Windows Security is updated and when Microsoft published updates.

## Windows Defender Firewall

### Activate/deactivate

* + - 1. If needed, navigate to the Windows Security dashboard.
      2. Click **Firewall & network protection**.

#### Question:

Name the three types of networks that can be protected and list their firewall status.

Type your answers here.

Answers will vary. The three types of networks are domain, private and public networks. The firewall is on for all the networks.

* + - 1. Click the **Private network** to view the settings.

#### Question:

What are the available settings?

Type your answers here.

Answers will vary. You can choose to block all incoming connections or turn off the Microsoft Defender Firewall.

* + - 1. Click **Back**.

### Application security

You can configure Windows Defender Firewall to allow or block a specific application through the Windows Defender Firewall.

* + - 1. In **Firewall & network protection** window, click **Allow an app through firewall**.
      2. Click **Change settings** to select the network profile types where the app is allowed or blocked. Or click **Allow another app** to select the app using the executable file.
      3. Close the window when done.

### Port security

You can configure the firewall behavior for a specific protocol. For example, ping requests and replies are blocked by default. In this step, you will allow IPv4 pings (ICMPv4) through the firewall by creating a custom inbound filtering rule.

* + - 1. In **Firewall & network protection** window, click **Advanced settings**. Click **Yes** to allow changes to Windows Security when prompted.
      2. Click **Inbound Rules**. Click **New Rule**.
      3. Click **Actions** and select **Properties** to view the default policy for inbound and outbound traffic.
      4. In the New Inbound Rule Wizard, click **Custom**. Click **Next** to continue.
      5. Click **Next** to use the All-programs settings.
      6. In the **Protocol and Ports** step, select **ICMPv4** and click **Next** to continue.
      7. In the Scope step, click **Next** to apply this rule to all IP addresses.
      8. In the Action step, click **Next** to allow the connection.
      9. In the Profile step, click **Next** to apply this rule to all the network profile types.
      10. Enter a name for this rule and click **Finish**. Now you have a custom rule that allows ICMPv4 through the firewall. You can disable this rule as needed by right-clicking the rule and selecting **Disable Rule**.

End of document