

## Lab 8.1.7 Configuring Microsoft Defender Firewall on a Windows Host

*From TestOut CompTIA Security+ Course*

In this lab I will be configuring Microsoft Defender Firewall on an Windows Host/Endpoint according to the

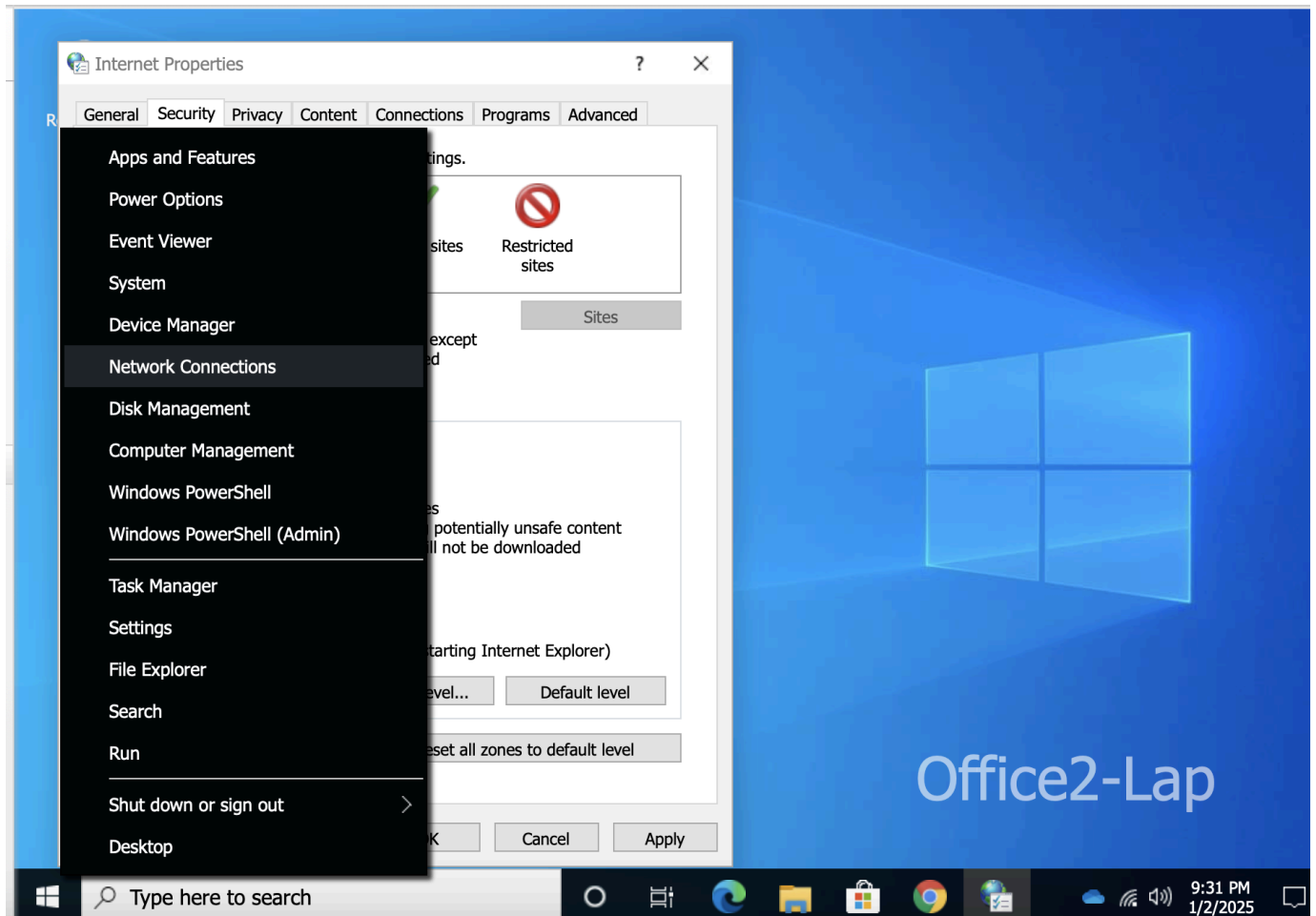
**The scenario for this lab is as follows:**

“You have a new laptop that is running Windows 10. You notice a security message that indicates that Windows Firewall has been disabled. The laptop is currently connected to your organization’s network, and the Domain network profile settings are in effect. You plan to travel this week and connect the laptop to various airport Wi-Fi hotspots. You need to enable Windows Firewall for any public network.

**In this lab, your task is to configure Windows Firewall as follows:**

- **Turn on the Windows Firewall for the Public network profile.**
- **In addition to the programs and ports currently allowed, allow the following service and programs through the firewall for only the Public network profile:**
  - **A service named Key Management Service**
  - **An application named Arch98**
  - **An application named Apconf”**

First of all, it’s a big Red Flag that the Windows Firewall is disabled. To start, I will navigate to **Network Connections** by right clicking the Start Menu and selecting it.

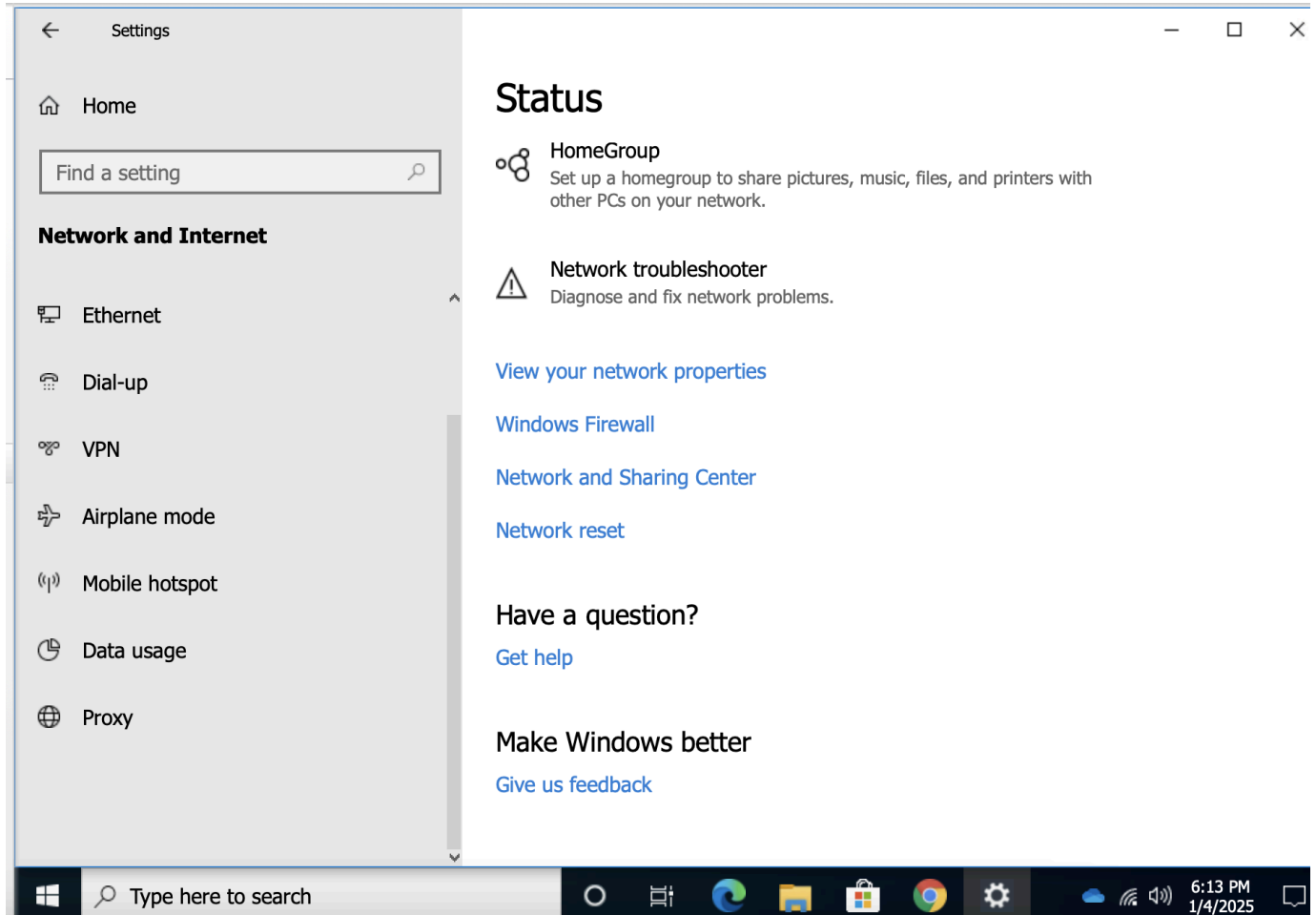


After Clicking **Network Connections** I will scroll down to the **Windows Firewall** setting in the right pane of the Network and Internet window that pops up.

Robert Carpenter

[github.com/robertmcarpenter](https://github.com/robertmcarpenter)

Thurs December 26th 2024

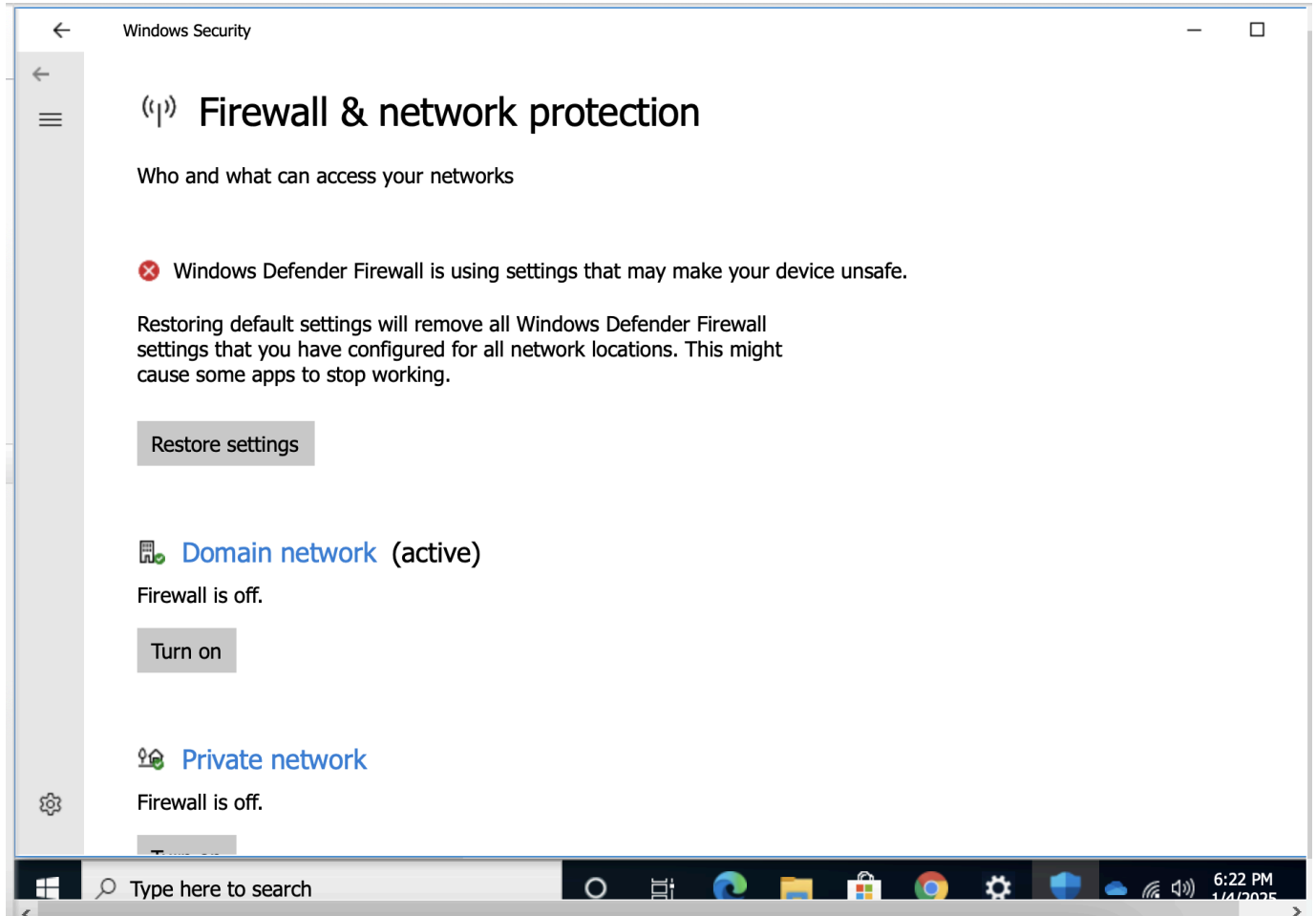


Clicking this brings up the **Windows Security** configuration window, which we can use to access the Firewall settings.

Robert Carpenter

[github.com/robertmcarpenter](https://github.com/robertmcarpenter)

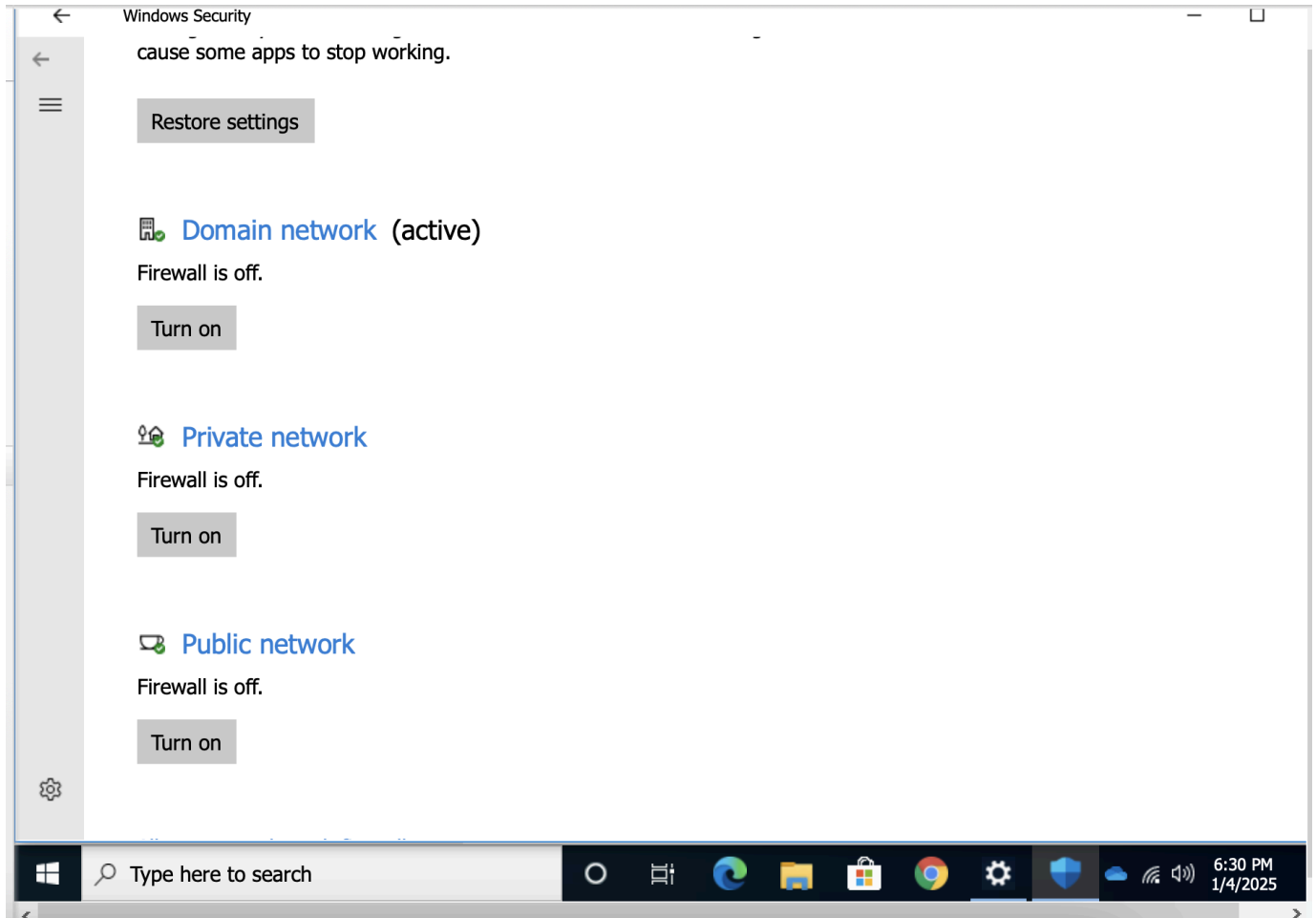
Thurs December 26th 2024



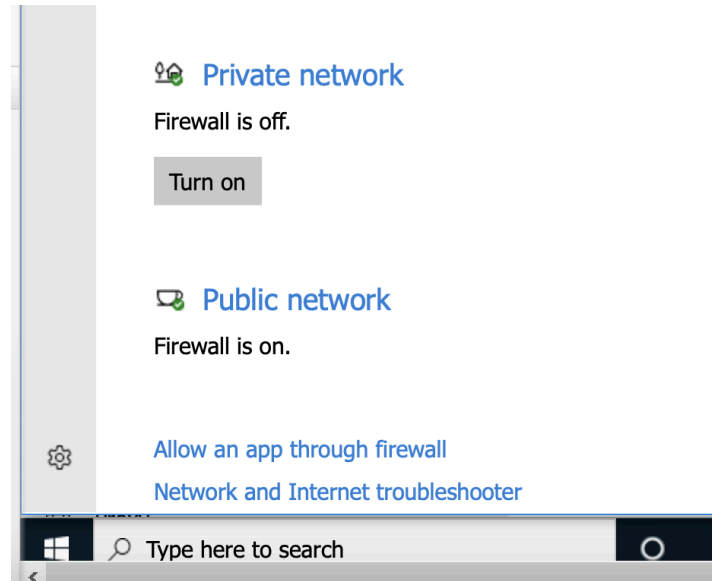
Robert Carpenter

[github.com/robertmcarpenter](https://github.com/robertmcarpenter)

Thurs December 26th 2024



As you can see all 3 settings of **Domain** , **Private** , and **Public** Firewalls are all turned off. We'll need to click the button to turn them ALL back on. In this case however the lab asks us to simply turn on the Firewall for Public Networks since the Domain's Network Profile is already installed on the machine. A Domain or Private Firewall might pose an issue or conflict with already configured settings within the Domain's Network profile config for devices connected.

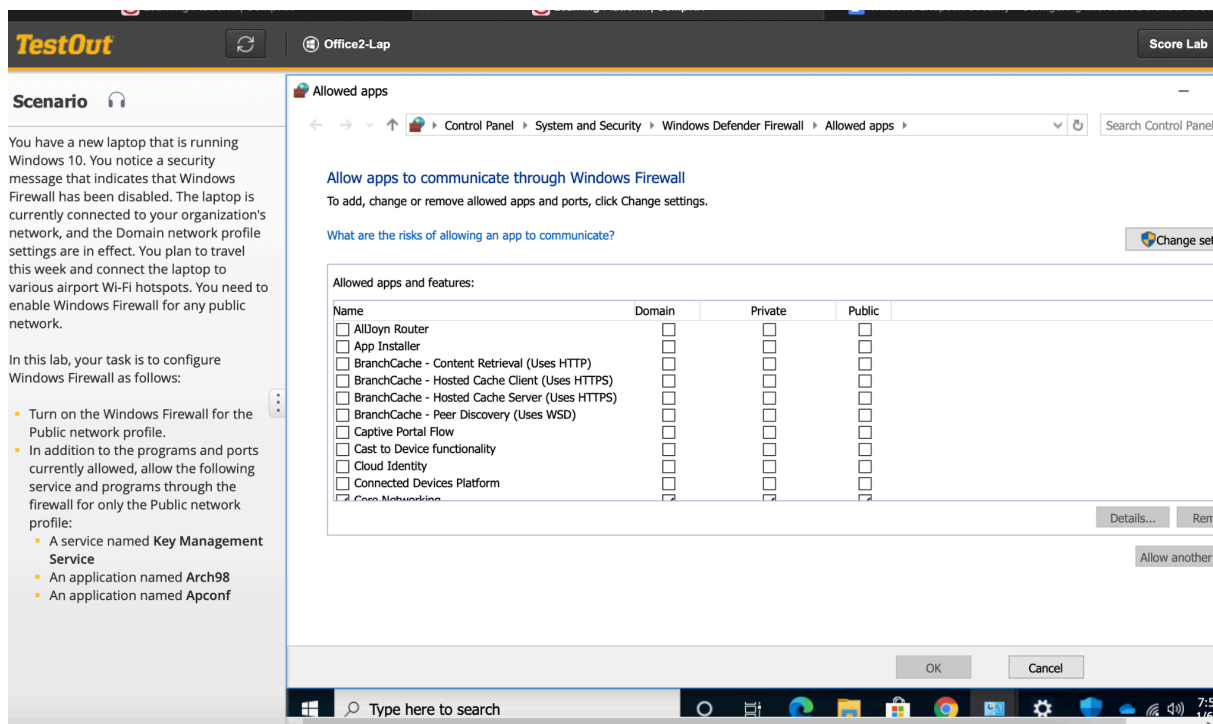


After I've turned on the **Public Firewall** I can now click the shortcut below it labeled **Allow an app through firewall** in order to move on to the next part of this lab. I need to allow the following through the Firewall:

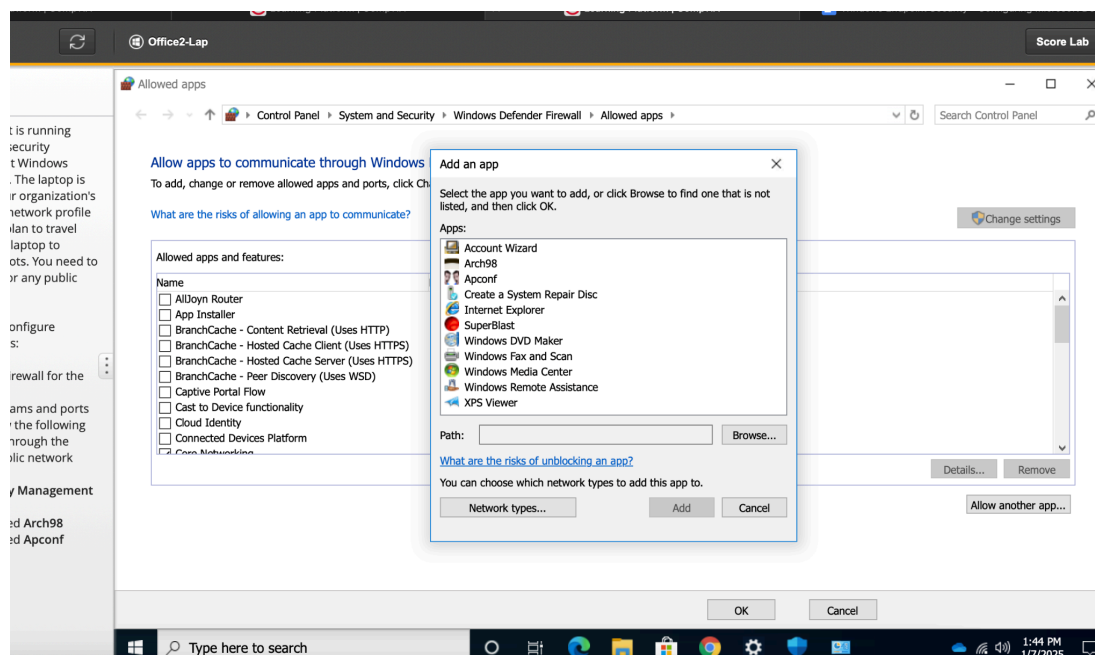
- **A service named Key Management Service**
- **An application named Arch98**
- **An application named Apconf**

Clicking "**Allow an app through Firewall**" brings up the following Window:

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Thurs December 26th 2024

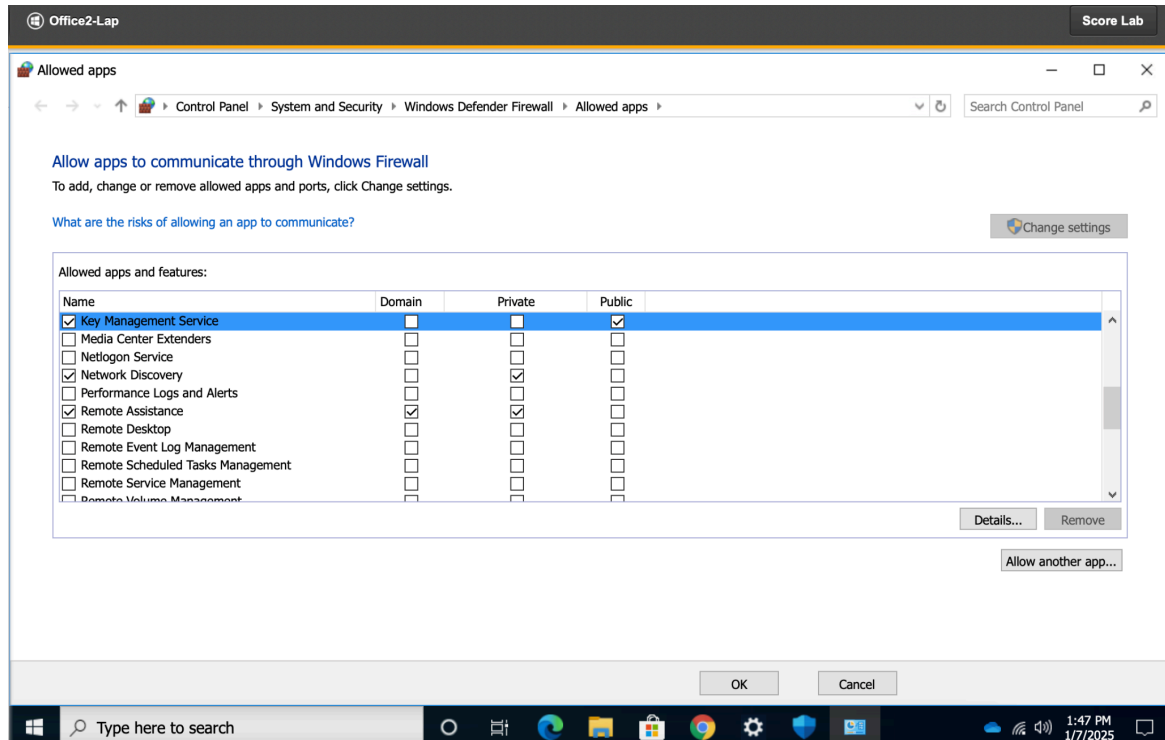


First, I will click **Allow another App** since I don't see the application **Arch98**:



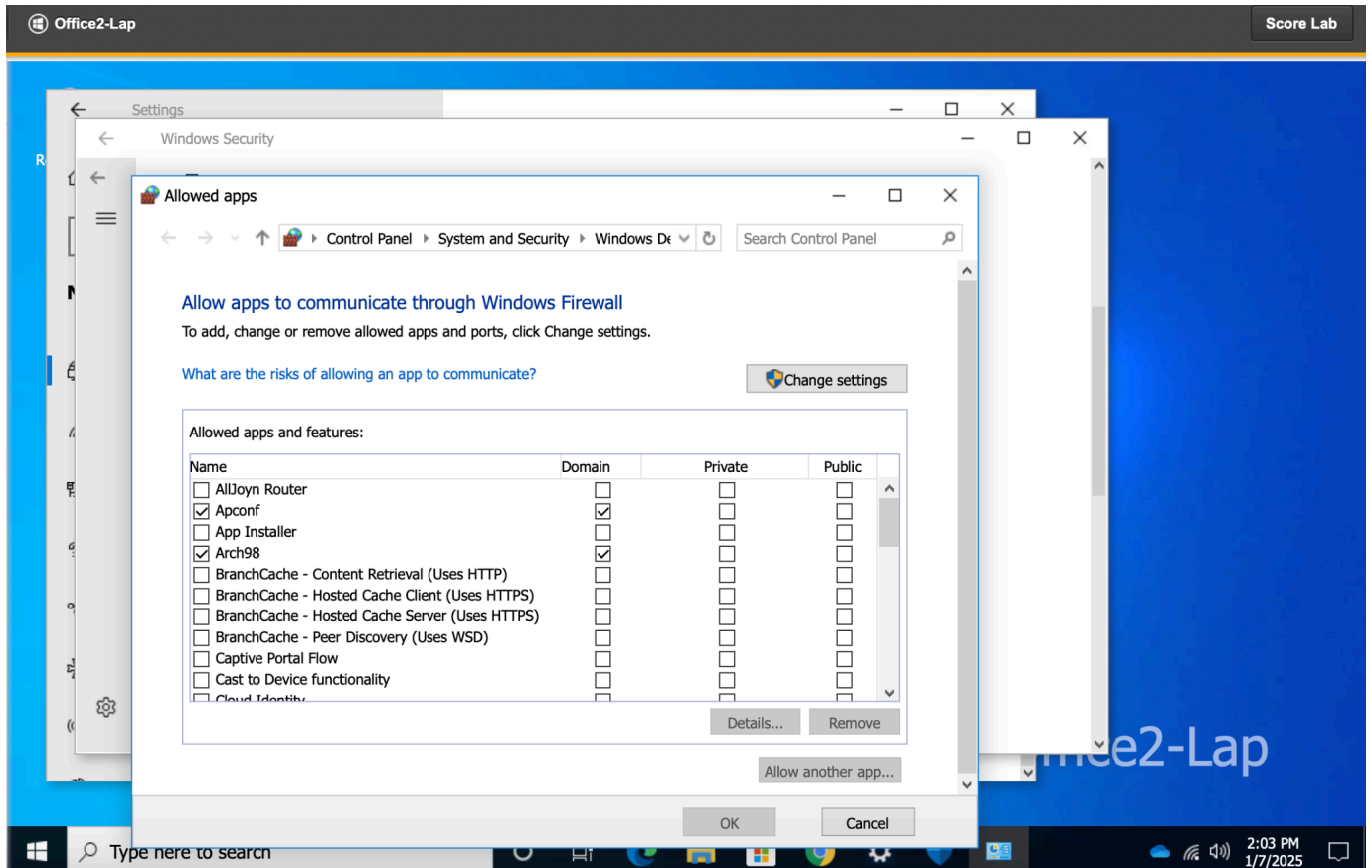
From here I will select **Arch98** then click **Add**. After clicking **Add** I will clear the **Domain** and **Private** check boxes for **Key Management Service**.

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Thurs December 26th 2024



Lastly, I need to add another application through the firewall called **Apconf**. Again I will click **Allow another app**.. And pick it from the list.





After allowing these apps and services I will click **Ok**.

And that concludes this lab! I've successfully done the following:

- Turn on the Windows Firewall for the Public network profile.
- In addition to the programs and ports currently allowed, allow the following service and programs through the firewall for only the Public network profile:
  - A service named **Key Management Service**
  - An application named **Arch98**
  - An application named **Apconf**

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Thurs December 26th 2024

The screenshot displays a web browser window with multiple tabs. The active tab is titled 'Windows Endpoint Security - Configuring Microsoft Def...'. The main content area shows a 'Lab Report' for 'Windows Security'. The report indicates a 'Score: 4/4 (100%)' and 'Time Spent: 02:20'. Below this, a 'TASK SUMMARY' section lists 'Required Actions' that have all been completed with checkmarks. The actions are: 'Turn Windows Firewall on', 'Allow Key Management Service through the Public firewall only', 'Allow the Arch98 program through the Public firewall only', and 'Allow the Apconf program through the Public firewall only'. Each action has a 'Show Details' link. In the background, a 'Scenario' page is visible, providing context for the lab. It states that the user has a new laptop running Windows 10 and that the Windows Firewall has been disabled. The task is to configure Windows Firewall as follows: turn it on for the Public network profile, and allow the Key Management Service, Arch98, and Apconf programs through the Public firewall only. A Windows Security window is also visible in the background, showing the 'Windows Defender Firewall' settings.

Scenario

You have a new laptop that is running Windows 10. You notice a security message that indicates that Windows Firewall has been disabled. The laptop is currently connected to your organization's network, and the Domain network profile settings are in effect. You plan to travel this week and connect the laptop to various airport Wi-Fi hotspots. You need to enable Windows Firewall for any public network.

In this lab, your task is to configure Windows Firewall as follows:

- Turn on the Windows Firewall for the Public network profile.
- In addition to the programs and ports currently allowed, allow the following service and programs through the firewall for only the Public network profile:
  - A service named Key Management Service
  - An application named Arch98
  - An application named Apconf

Windows Security

### Lab Report

Time Spent: 02:20

Score: 4/4 (100%)

TASK SUMMARY

Required Actions

- ✓ Turn Windows Firewall on
- ✓ Allow Key Management Service through the Public firewall only [Show Details](#)
- ✓ Allow the Arch98 program through the Public firewall only [Show Details](#)
- ✓ Allow the Apconf program through the Public firewall only [Show Details](#)

Have a question?

Windows Endpoint Security - Configuring Microsoft Defender Firewall (Software Based) - Google Docs

docs.google.com