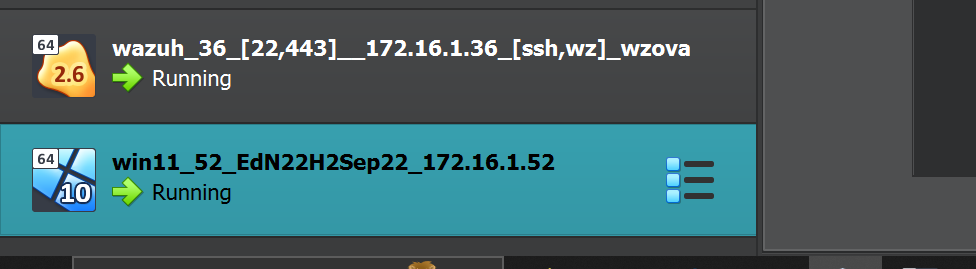
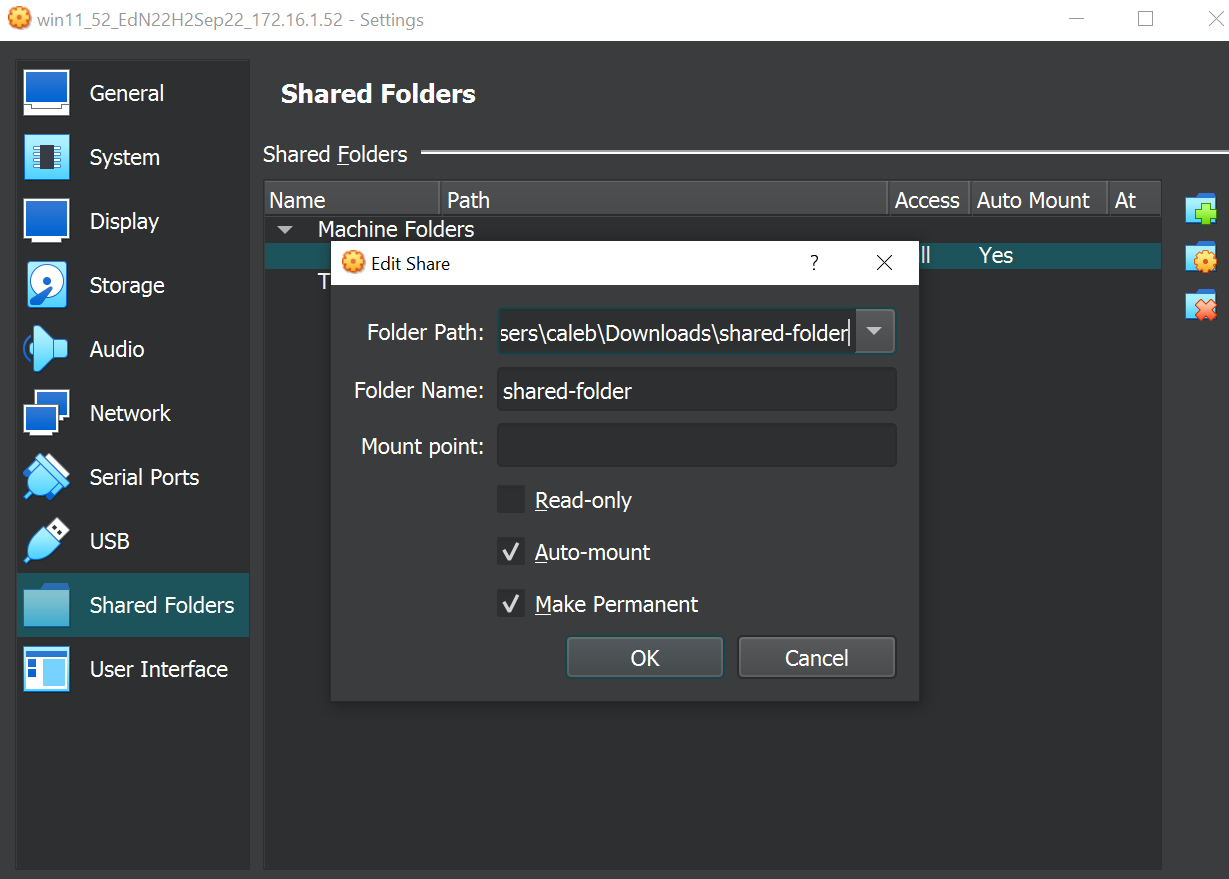
# Topic 2 Implement safeguard CIS 2.5 Allowlist Authorised Software

Your boss uses the Win11 virtual machine. Download the Win11 virtual machine from the uni website and import it into Virtualbox.



Setup a shared folder on Win11 for your scripts.



To implement an allowlist of authorised software you will configure Windows Defender Application Control (WDAC) in Win11. The following instructions are a guide. You can make improvements as you see fit.

1. Create a PowerShell script called defend.ps1.

2. Pre-test: write a function testWDAC() that:

a. Attempts to run an “unauthorised” app such as keyfinder.exe and checks whether the app has been run successfully, for example, using Get-Process.

3. Document your code.

a. Clean up your code using PSScriptAnalzyer

PS> Invoke-ScriptAnalyzer defend.ps1

b. Run the code and collect testing screenshots for your portfolio.

c. Commit your code to your Git repository.

4. Write a function setupWDAC() that compiles a block WDAC policy to a .cip file using ConvertFrom-CIPolicy

5. Add code to your script that checks the first argument of the command line:

a. If the first argument is testWDAC, call the testWDAC () function. For example, the following command line would call testWDAC(): defend.ps1 testWDAC

b. Improve your code to call the other functions in your script based on the command line argument.

6. Write a function enableWDAC() that uses citool.exe to apply the WDAC block policy (.cip)

7. Post-test: rerun testWDAC() to check if the “unauthorised” app is now blocked.

8. Write a function resetWDAC() that removes the WDAC block policy using citool.exe