Windows 10 Install Proof of Concept for Tetra Shillings Accounting LLC

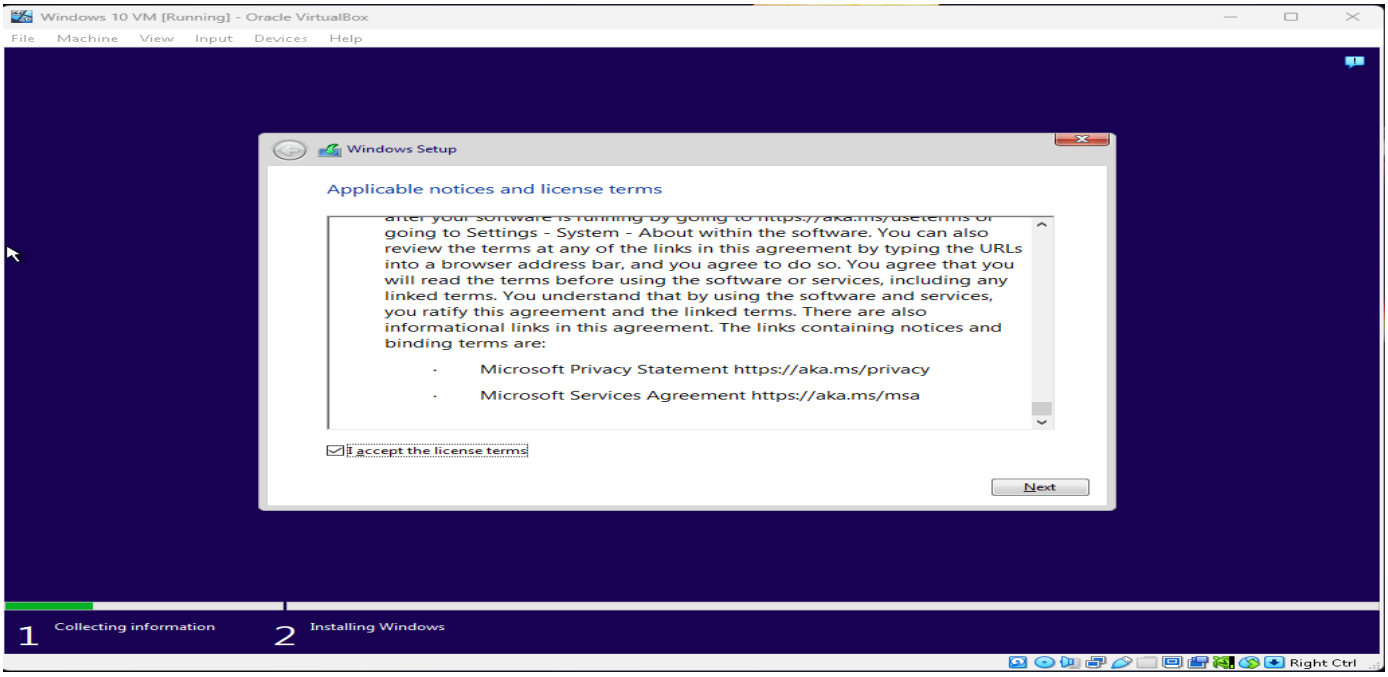
Prepared by:
Michael Lambinicio

Introduction

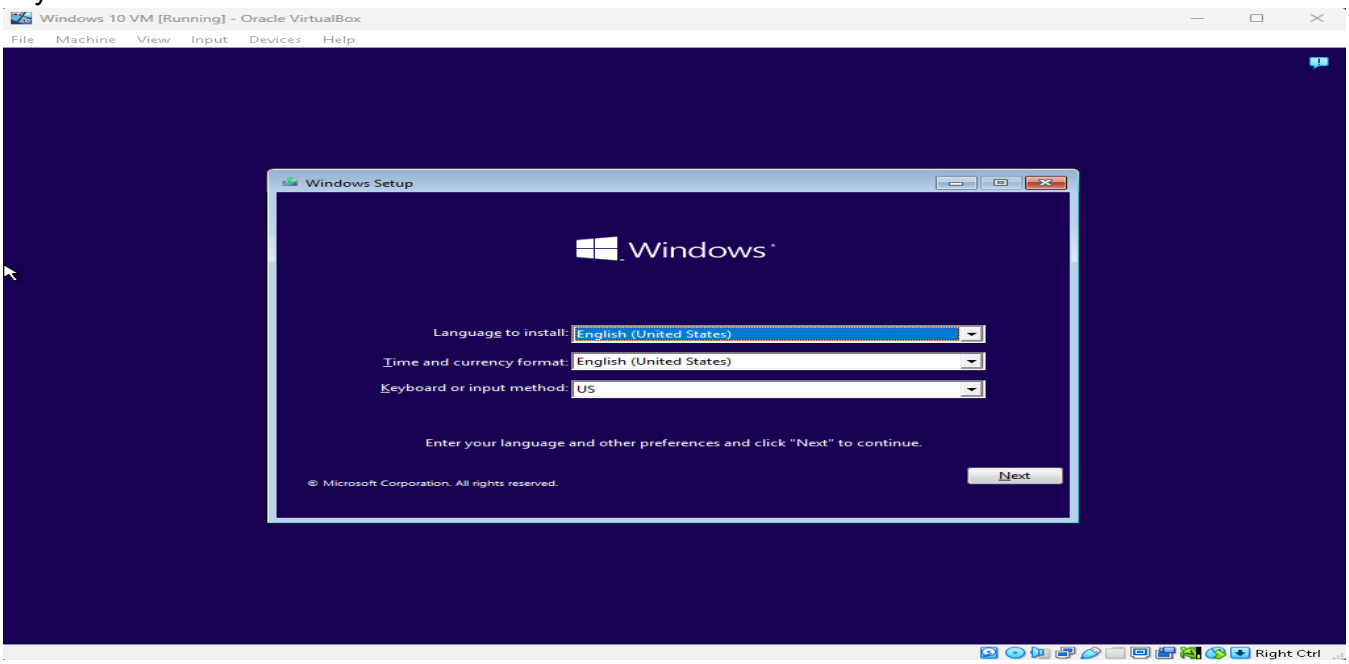
The purpose of this packet is to provide Tetra Shillings proof of concept to installing Windows 10 on all of its workstations. This will give play-by-play details on the process for a successful installation of Windows 10. Part 2 will help configure Windows 10 after it is installed such as how to add members to your group, giving access to folders and setting up policies so every ender user will have an easy transition with Windows 10 software.

Part 1: Windows Installation

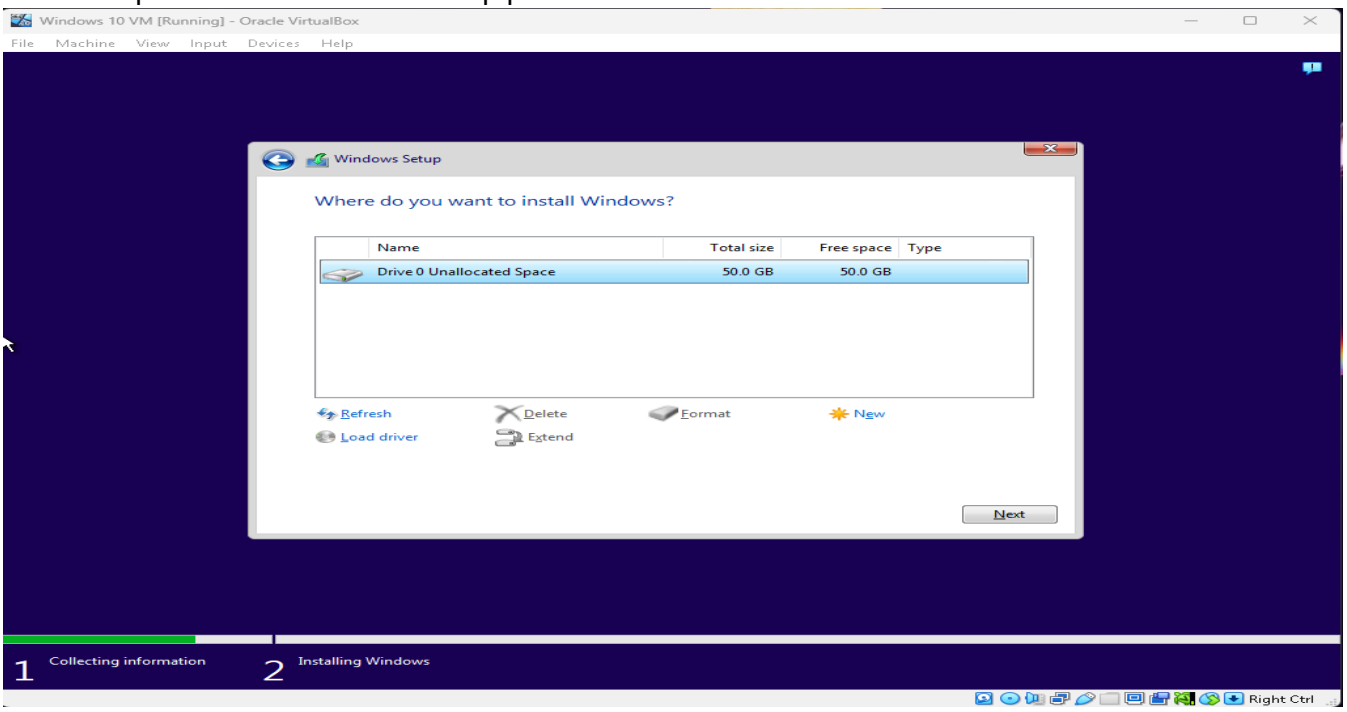
License acceptance screenshot – The picture below is the license agreement explaining the terms of using the software and must be accepted in order to continue with the installation.



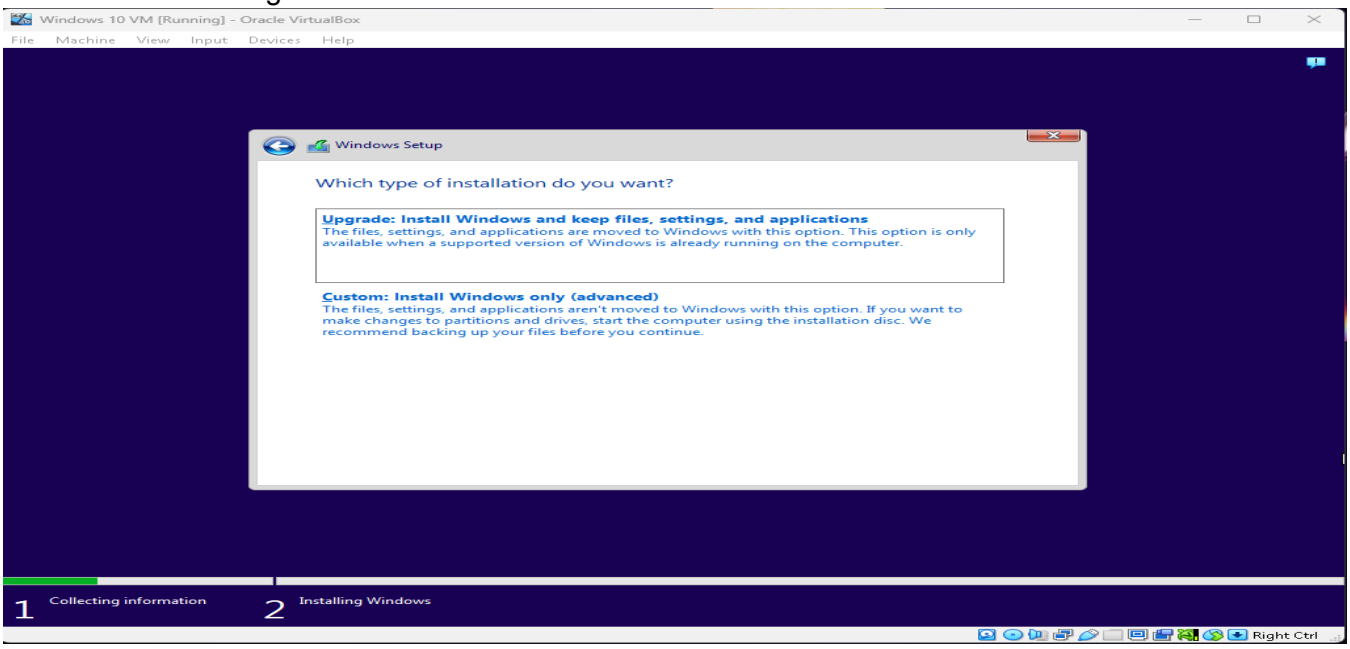
OS version screenshot – The first step in the installation process is letting you know that you will be installing the Windows 10 software. It allows you to choose your language, time and keyboard. Click next to continue.



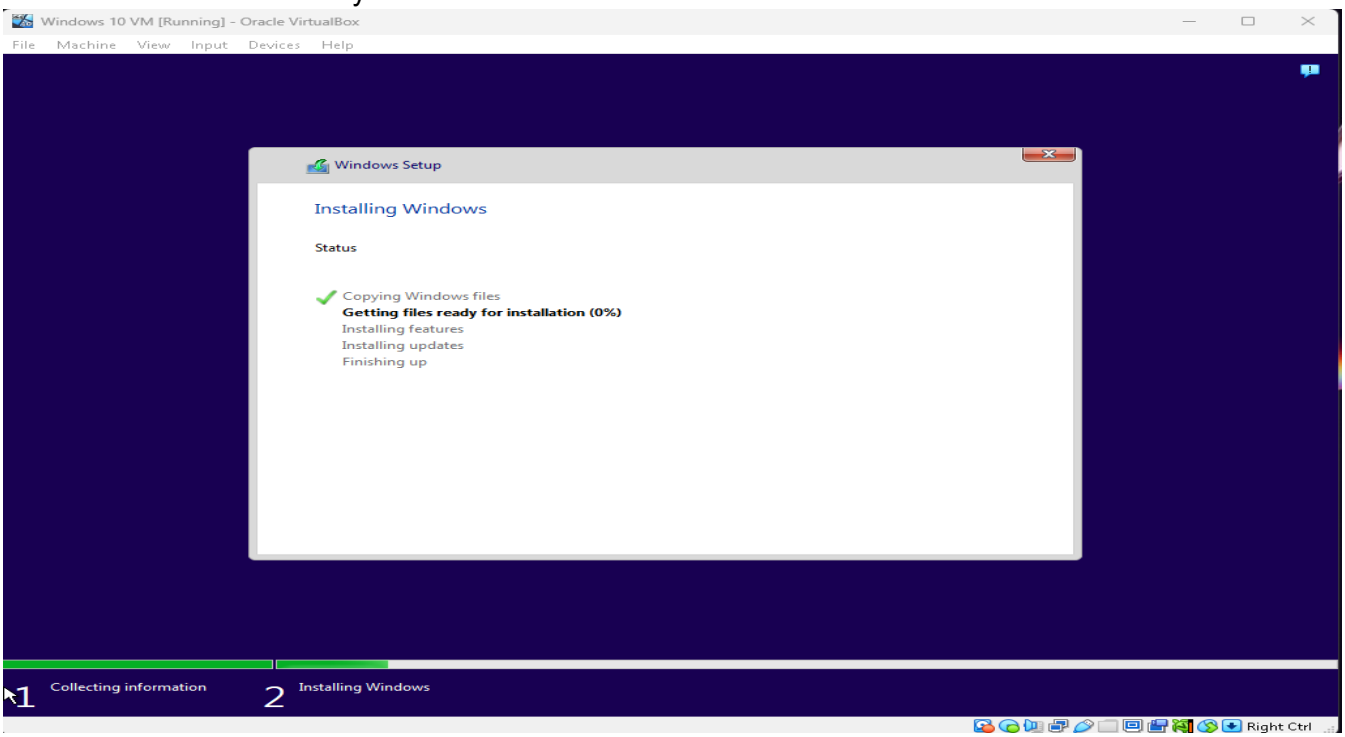
Disk configuration screenshot – The next step in the installation is going to ask where you would you like to install Windows. It will provide you with a window of what drive is available with unallocated space to install Windows on. Most administrators would use the default settings unless a specific drive has been setup prior to install. Click next on the chosen disk drive.



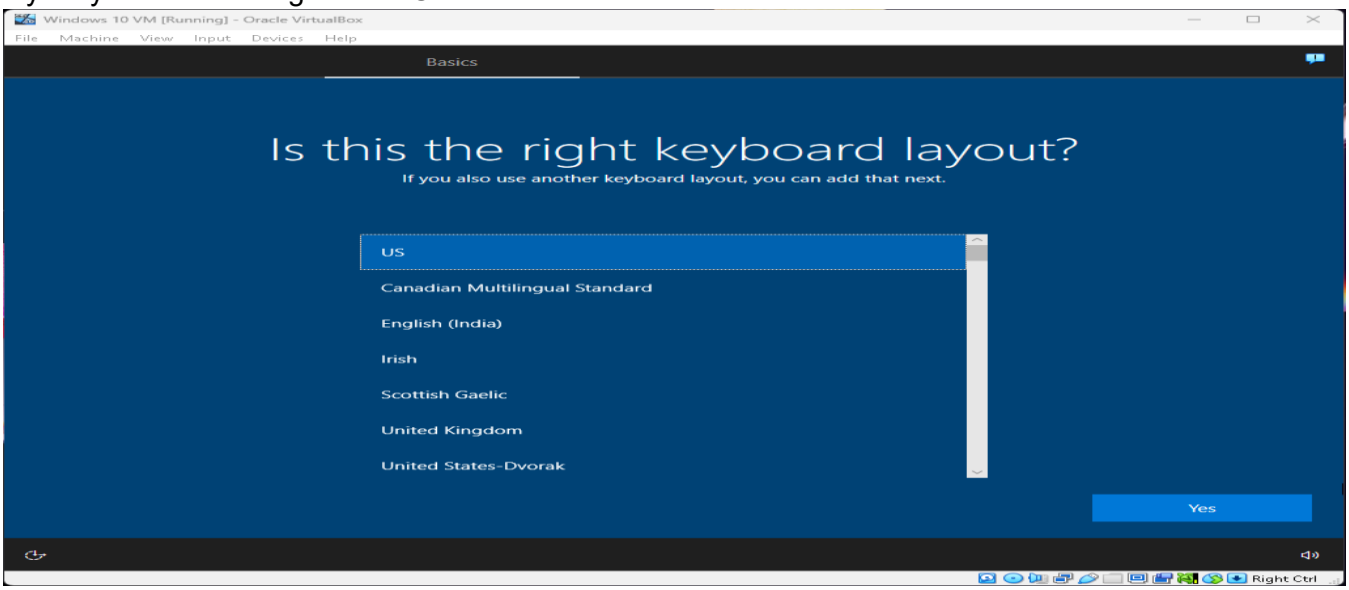
Custom installation vs. upgrade installation – Next, you will choose whether you would like to upgrade or do custom/fresh installation of Windows. Upgrading Windows will maintain all files, folders and data currently on the computer. Custom install will give you a clean installation of Windows and erasing all files currently on the disk drive. It is highly recommended to backup all files first before doing the custom installation.



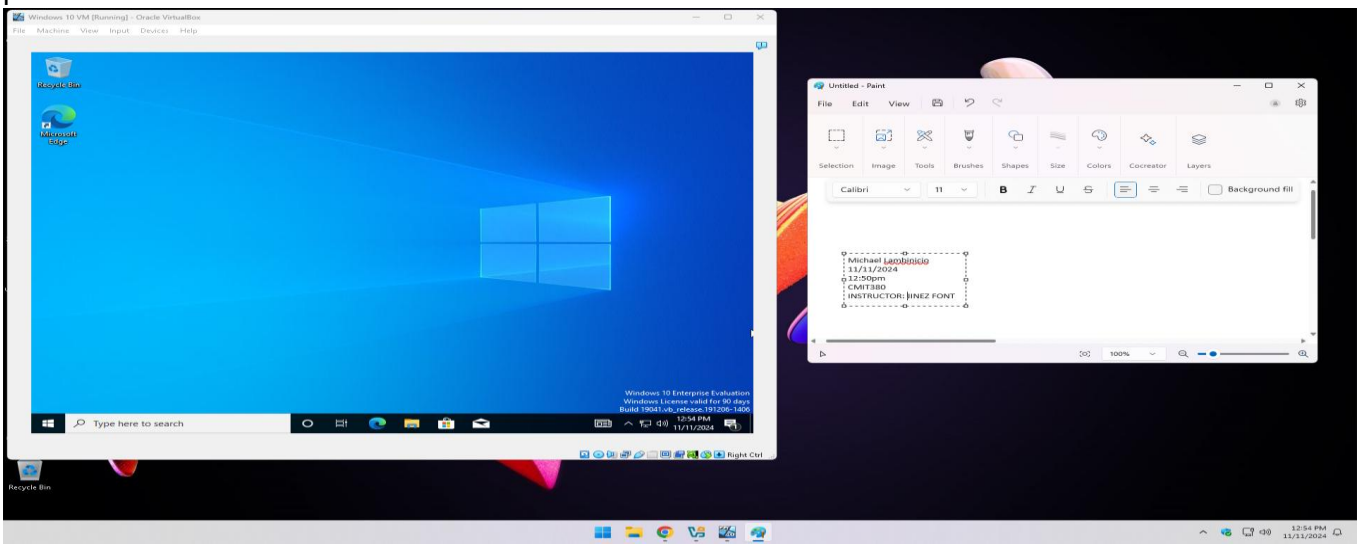
Installation of Windows – After your selection on your installation, Windows will start installing Windows on the disk drive you selected earlier.



Region/keyboard screenshot – After the installation is complete, it will ask you which keyboard layout you will be using. Select US and click “Yes”.

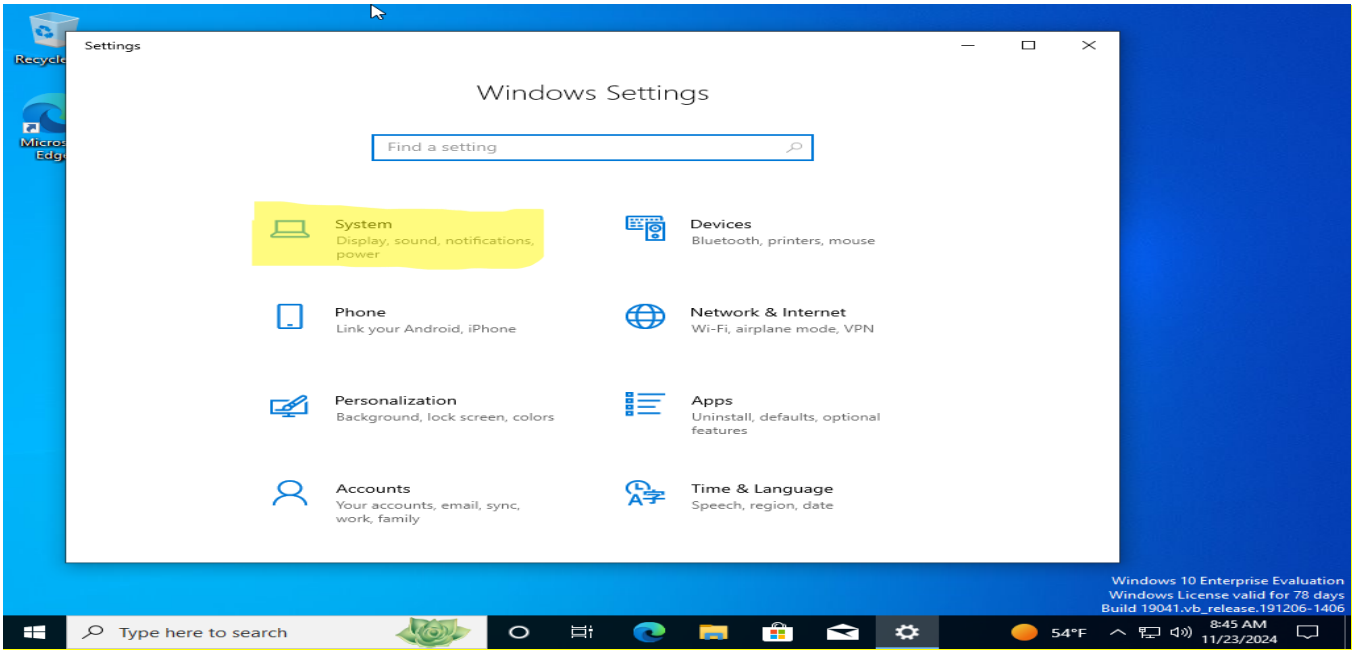


The picture below shows the completed installation of Windows 10 operating system on a previous machine.

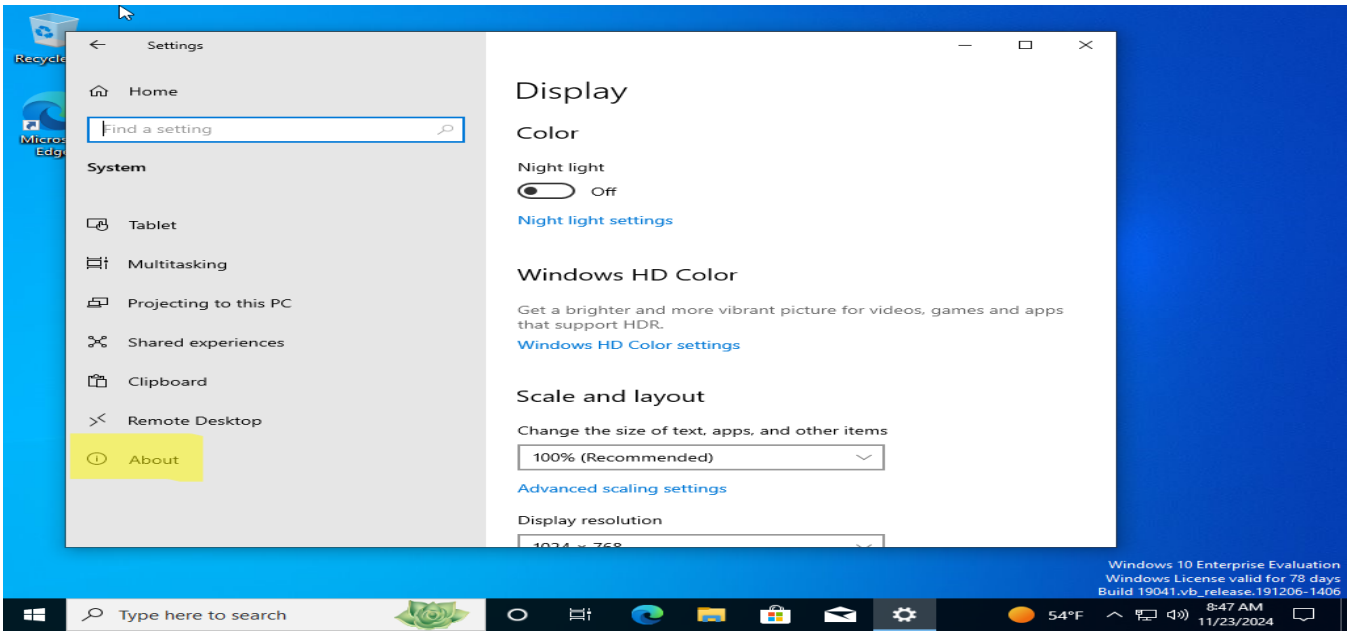


Part 2: Windows Configuration

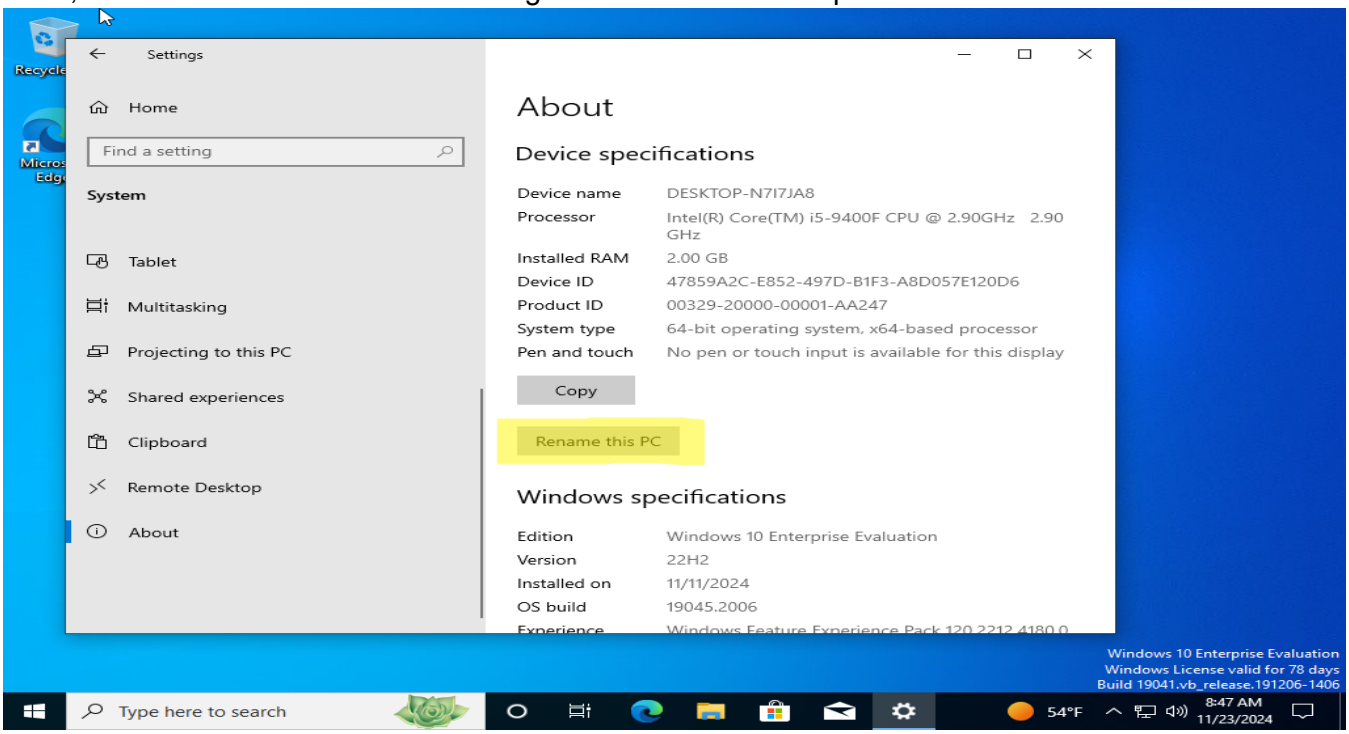
Step 1: Computer name screenshot – The screenshots below are steps to change your computer name. First, click START and select SETTINGS. Then choose SYSTEM.



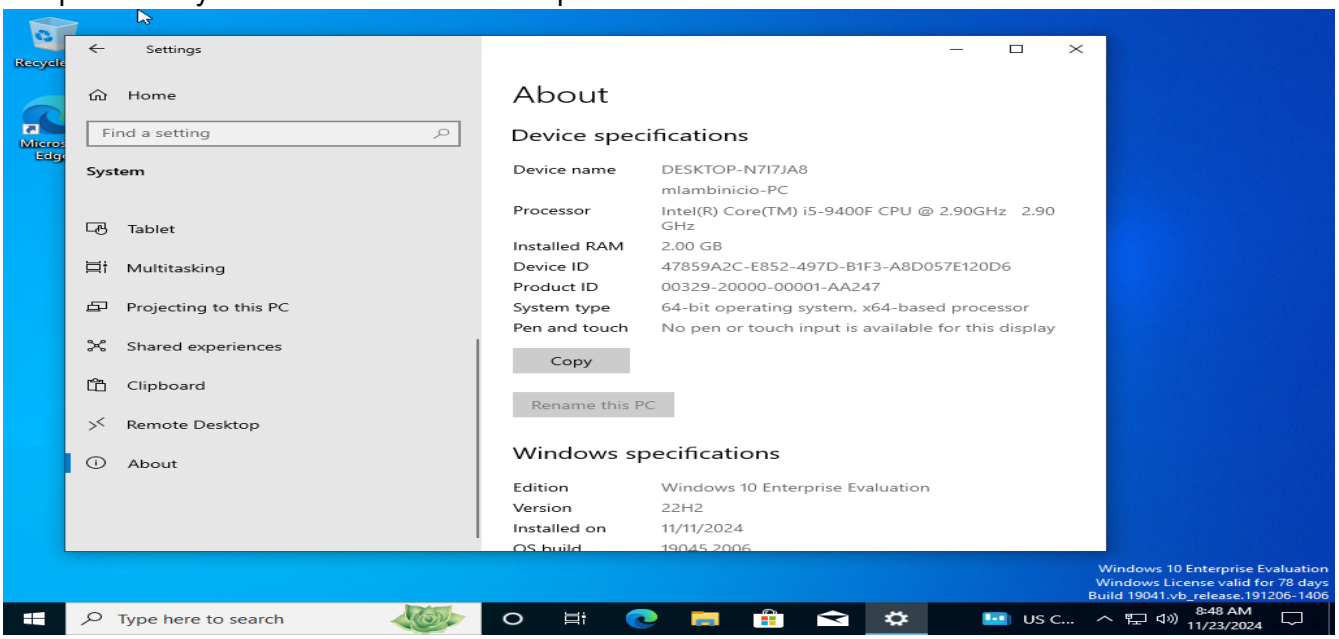
After, select About on the left side of the next screen.



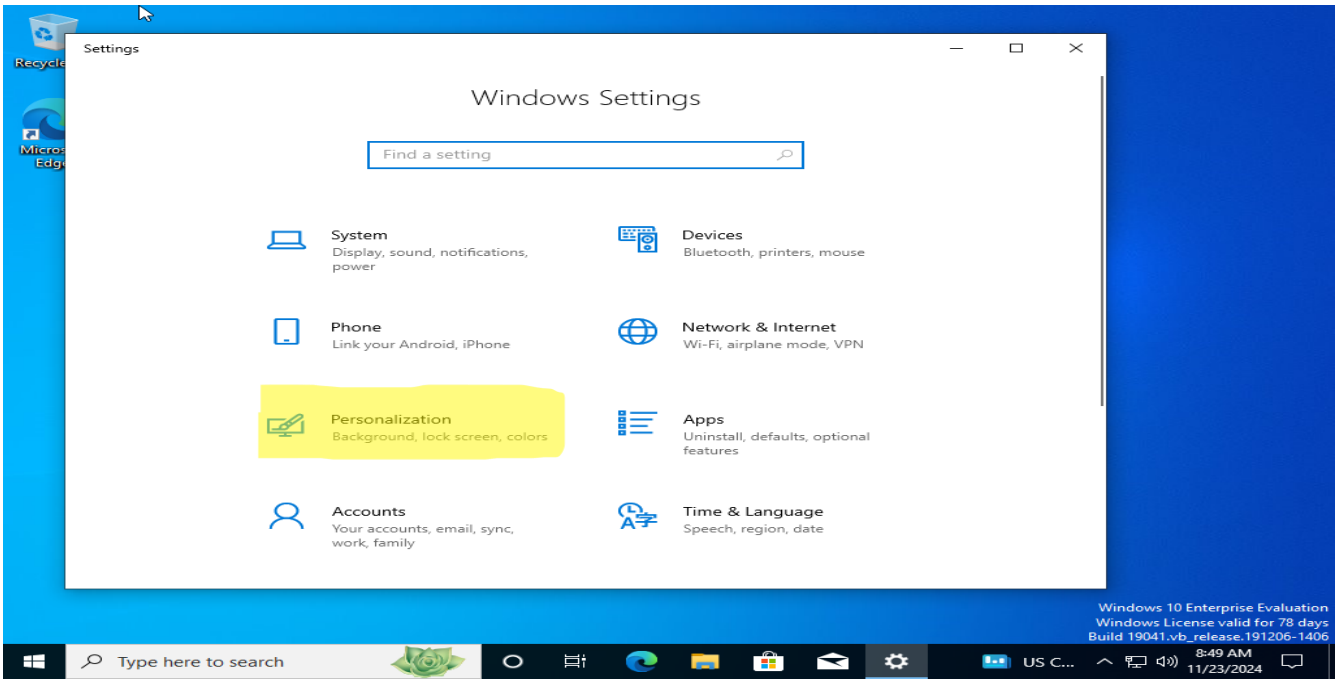
Then, select RENAME THIS PC to change the name of the computer.



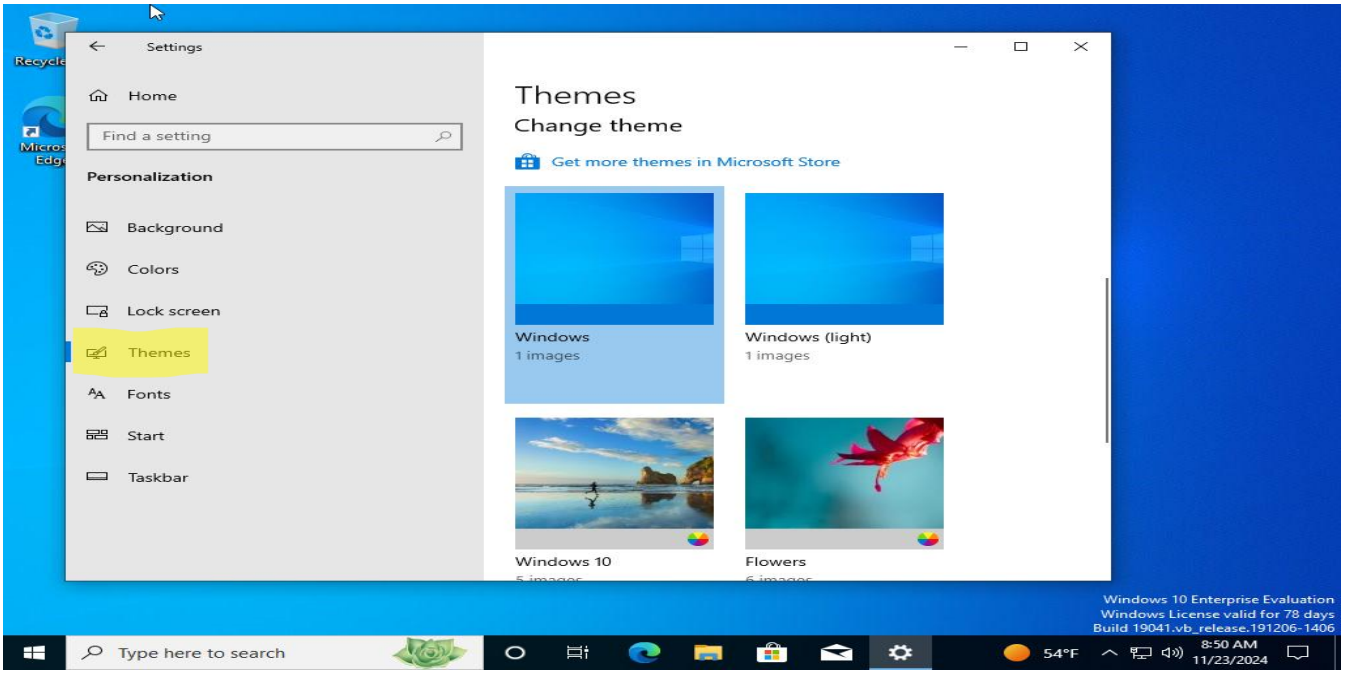
After you have changed the name, it will show the new name under the previous name of the computer until you restart. Restart the computer for the new name to take effect.



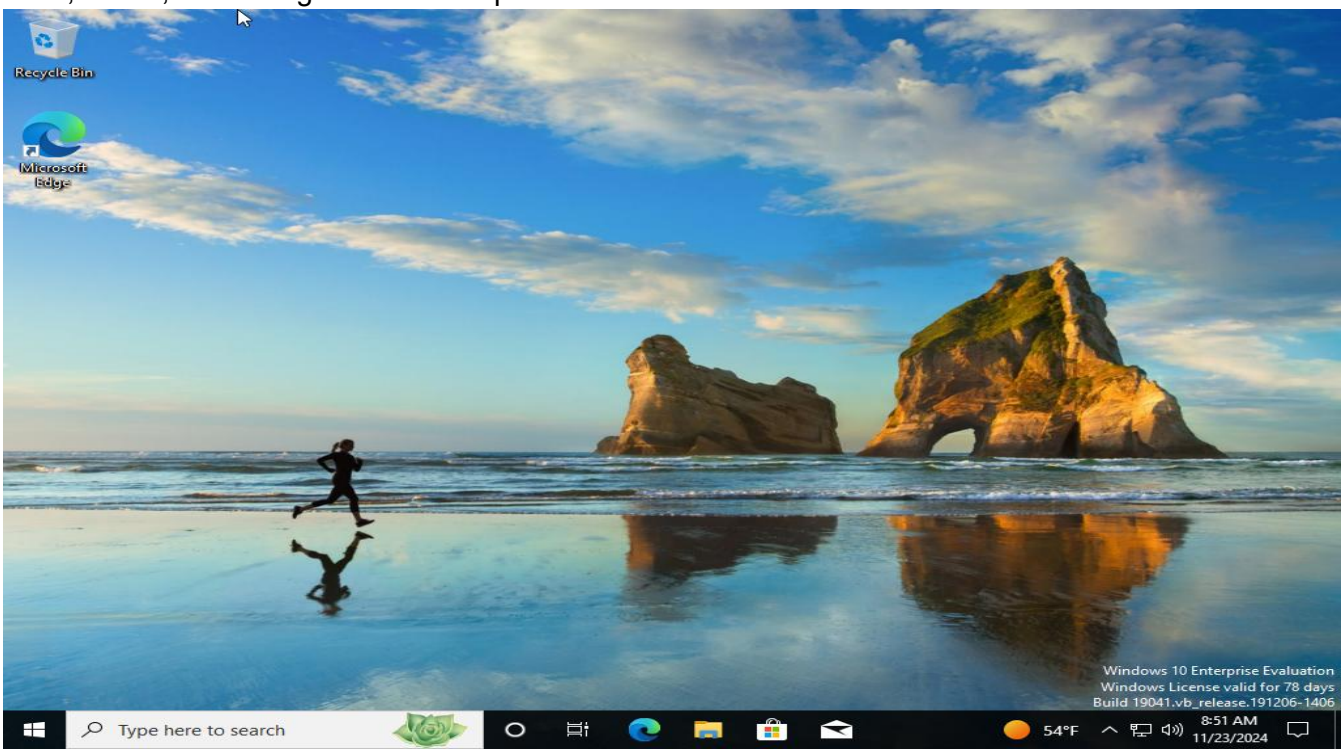
Step 2: Desktop theme screenshot – You will also have the ability to have a little personalization to your computer and changing the theme if you choose. Changing the them will allow you to choose, colors, fonts, backgrounds and more. First go to the settings from the Windows start menu and choose PERSONALIZATION.



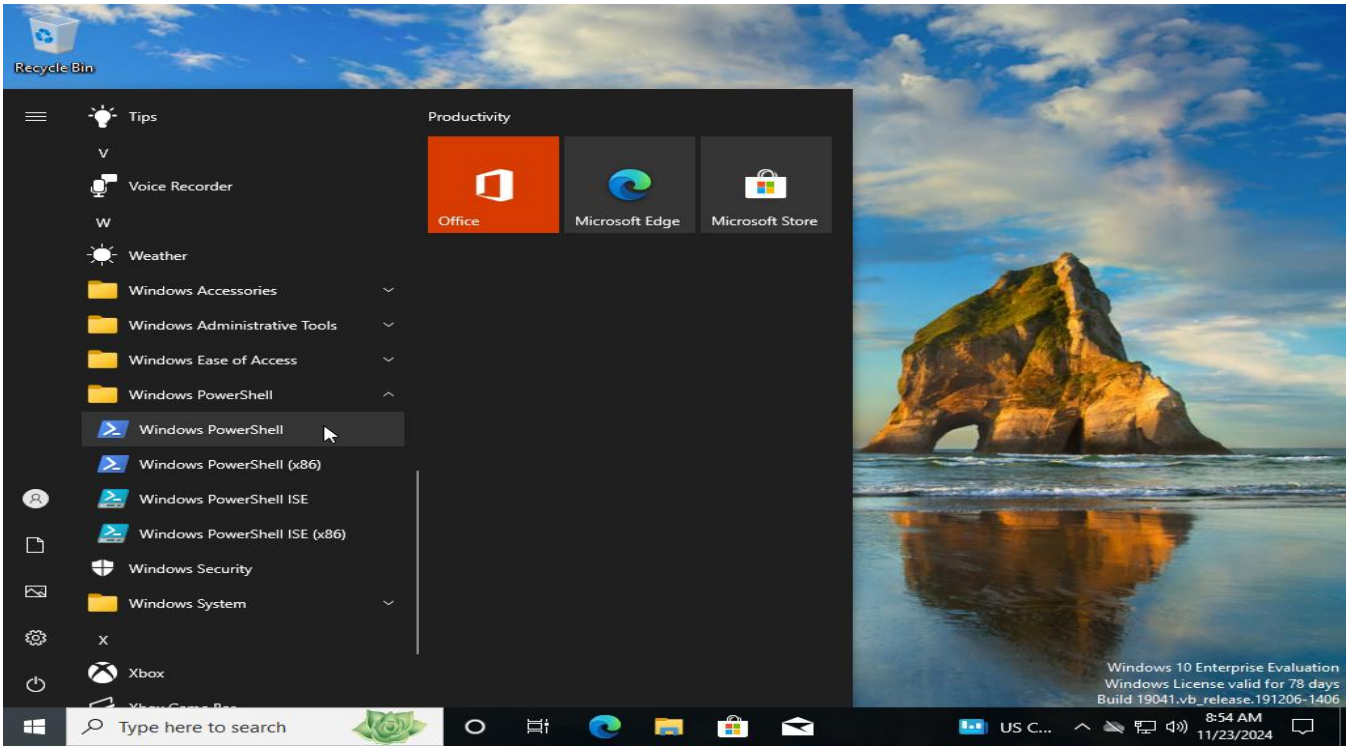
Then, click on THEMES on the left side of the next screen.



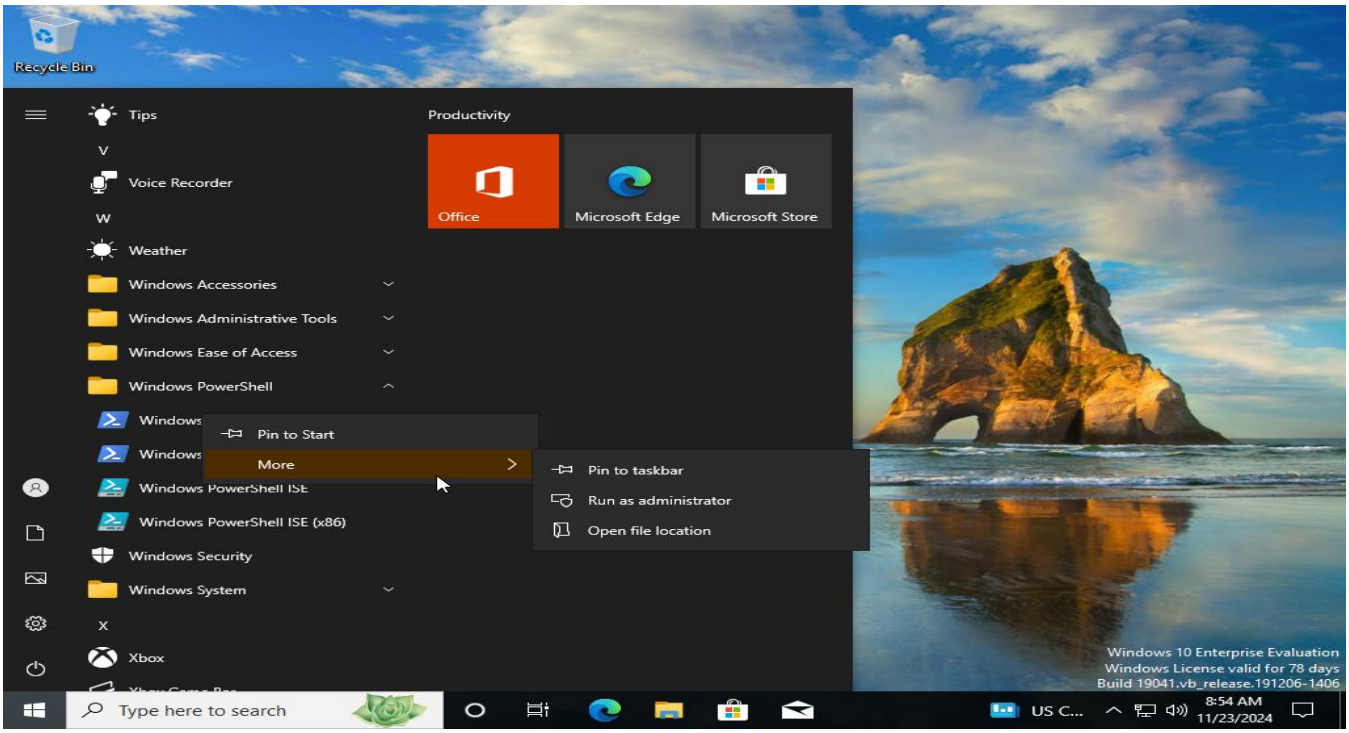
After you have selected your new theme, it will take a few seconds for Windows to convert the fonts, colors, and backgrounds. Example is shown below.



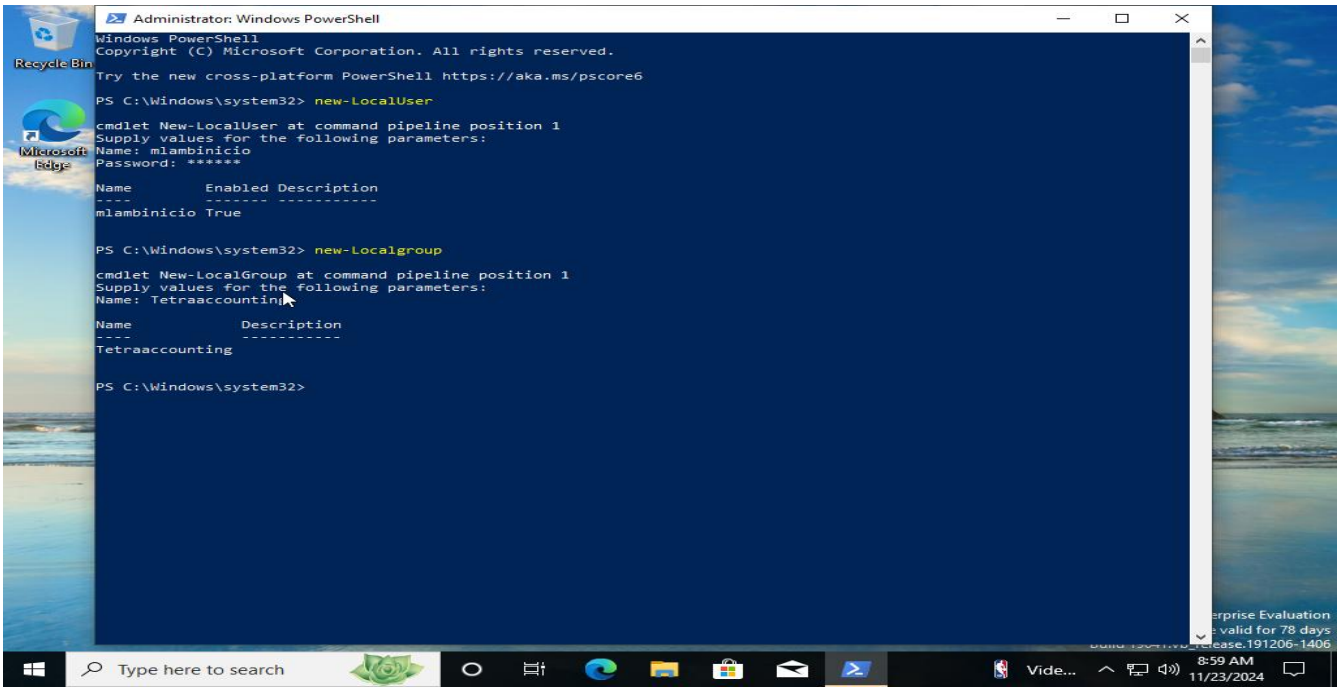
Step 3: Local user account screenshot – To create a local user account, it would require the use of Windows Powershell. You can get to this from the start menu, going to ALL APPS, and scrolling all the way down to WINDOWS POWERSHELL folder.



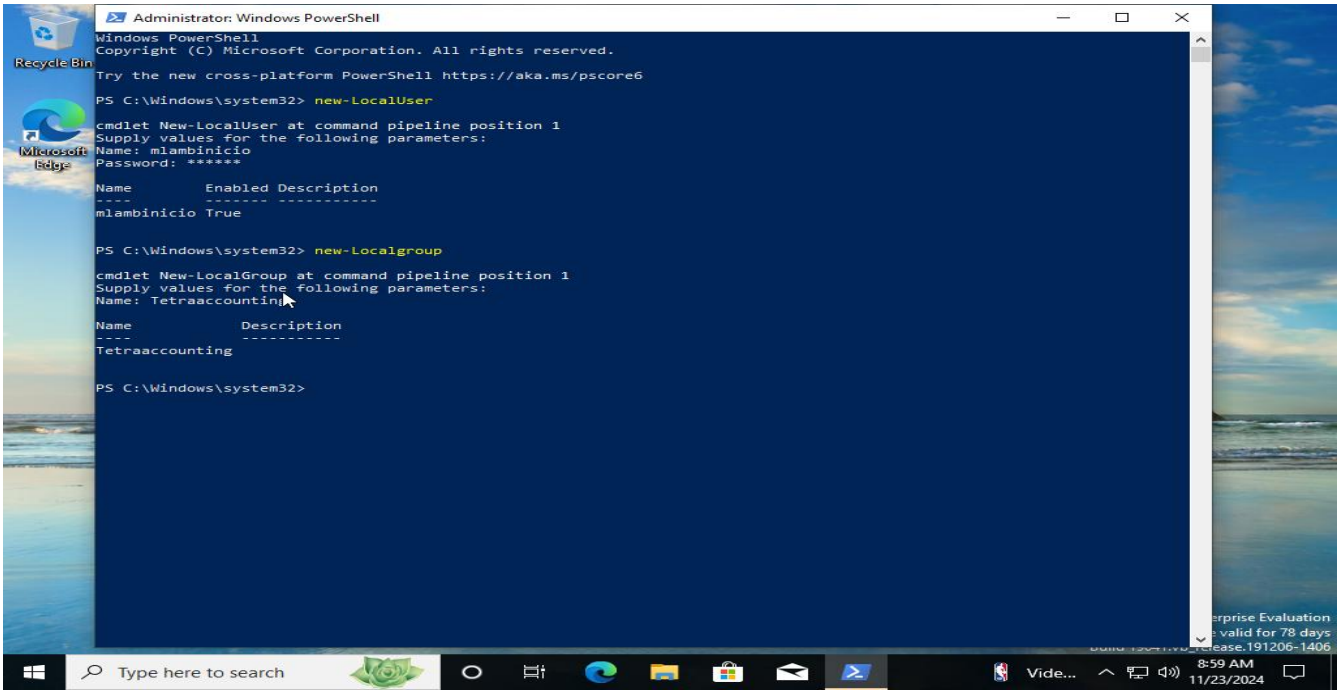
To ensure you have a full control and able to make changes, it is suggested to run as the administrator. Right click on Windows Powershell and highlight MORE and select RUN AS ADMINISTRATOR.



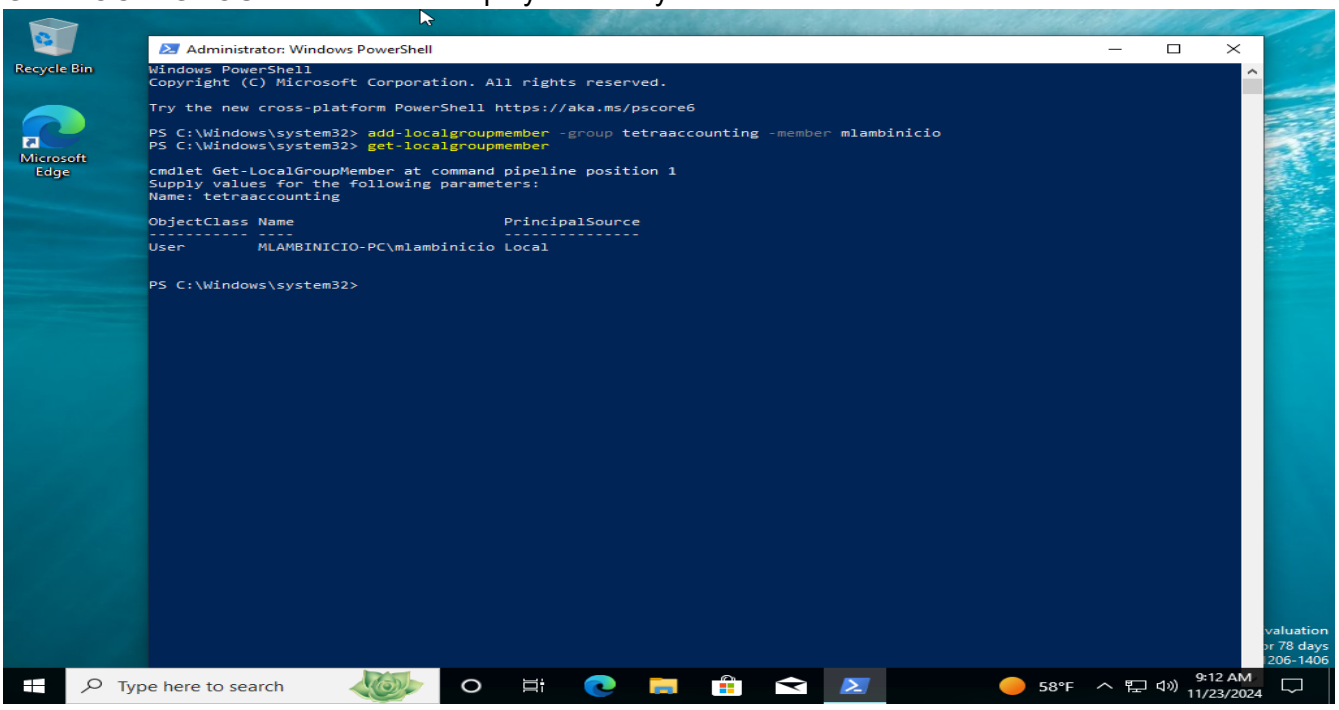
When the Powershell window pop ups, you would add a new user with command line text. Type NEW-LOCALUSER to add a new user. Then type the first initial and full last name of the user. In the password section, type the account password to authorize the change. If successful, it will show the new user account as shown below.



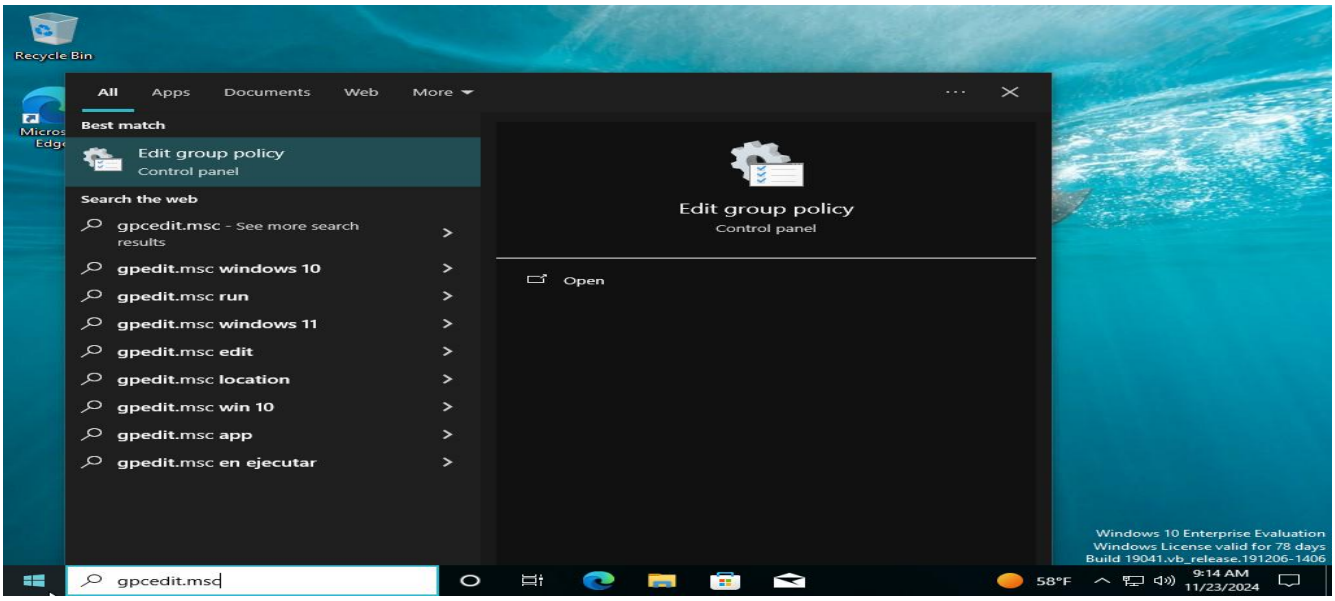
Step 4: Local group account screenshot – To add a local group account, in the same Powershell window, type NEW-LOCALGROUP. Then, type the name of the group. Below is TETRAACCOUNTING. Since you are using the same Powershell window, it will not ask for a password since you are on the same session. If you started a brand new session, it would ask for the account password. It will display the new group if typed in correctly.



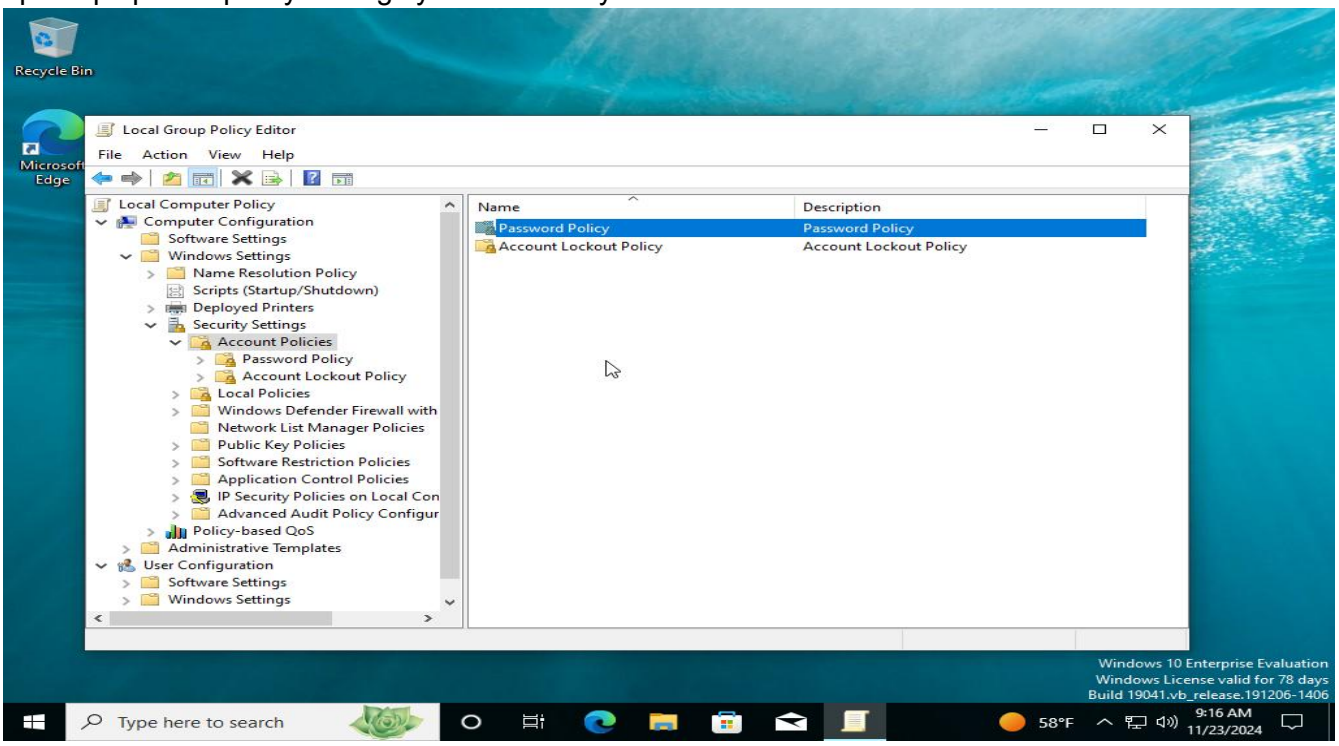
Step 5: Add user to local group screenshot – To add new user to the local group account, you would type on one line ADD-LOCALGROUPMEMBER -GROUP TETRAACCOUNTING -MEMBER USER ACCOUNT NAME. To verify if you added the user account correctly, type GET-LOCALGROUPMEMBER to display the newly added user account.



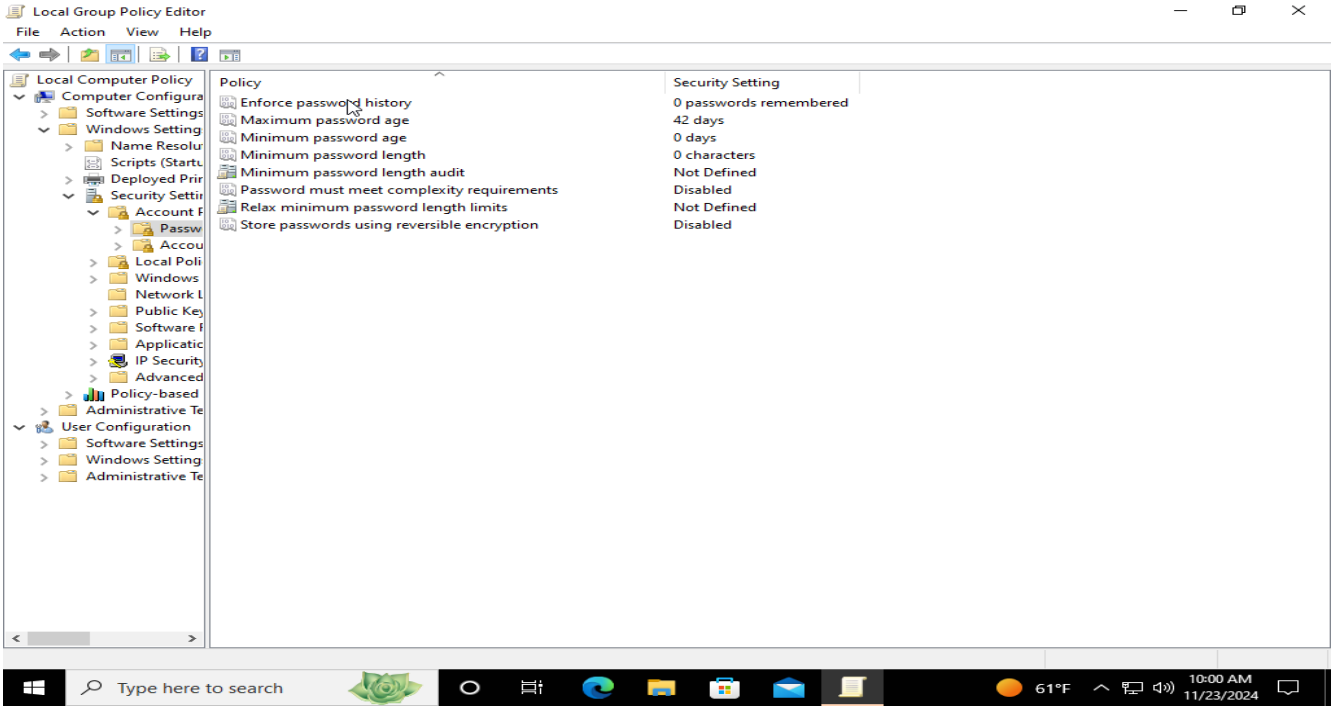
Step 6: Local group policy screenshot – To create a password policy, you would need to open the group policy settings. To do this, click START and type GPCEDIT.MSC.



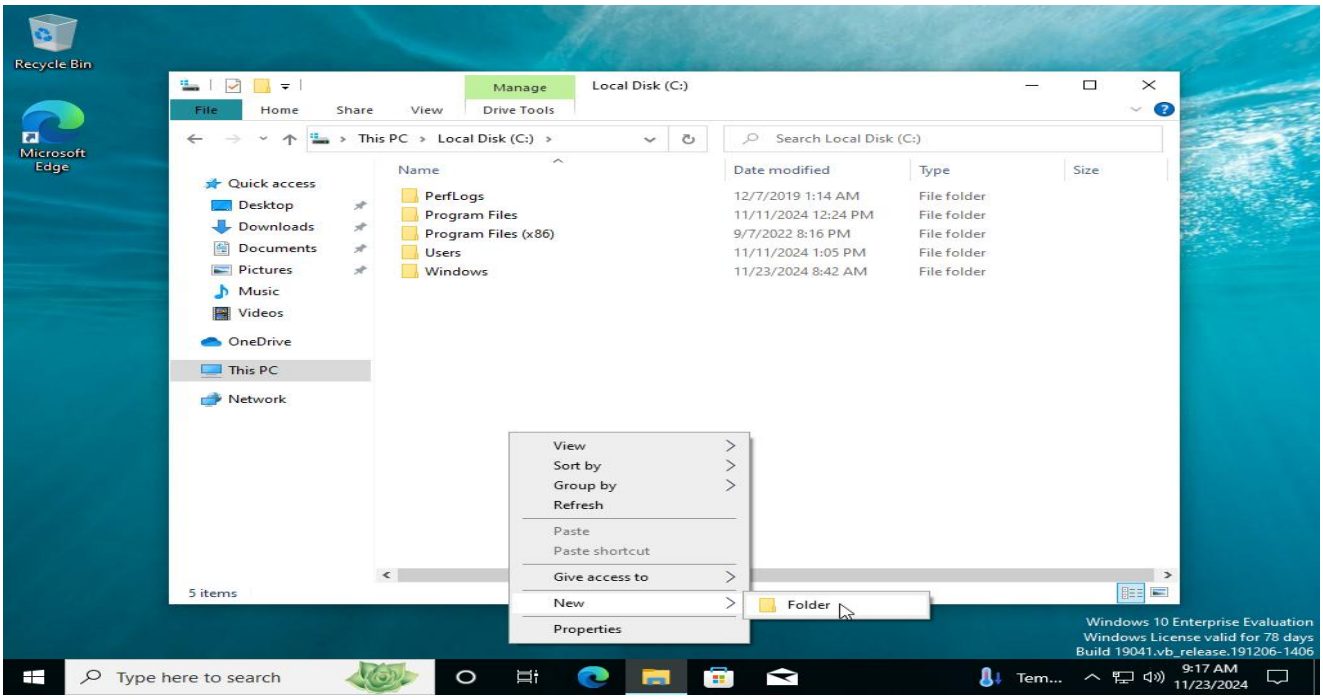
When the group policy editor window opens, double click WINDOWS SETTINGS on the left pane. Then double click ACCOUNT POLICIES. After, double click PASSWORD POLICY. To open up specific policy settings you can modify.



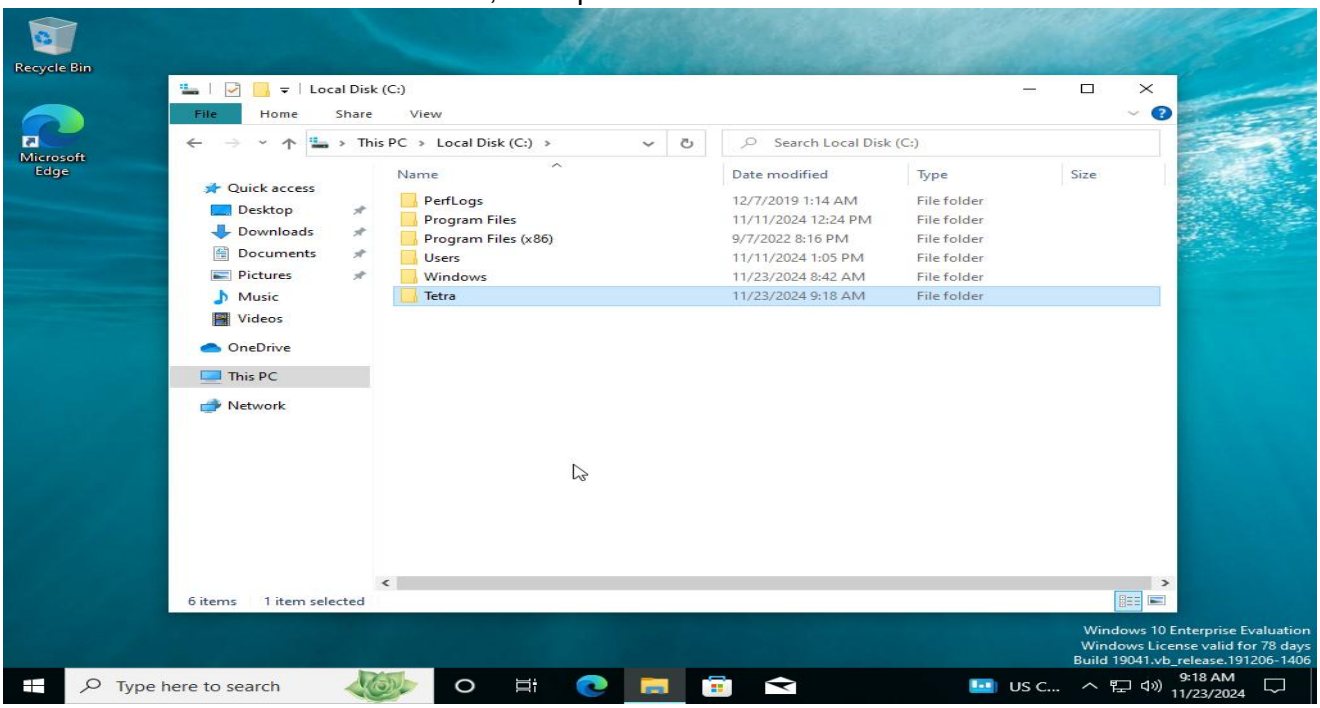
Below are the policies attributes to change that would be required of every user.



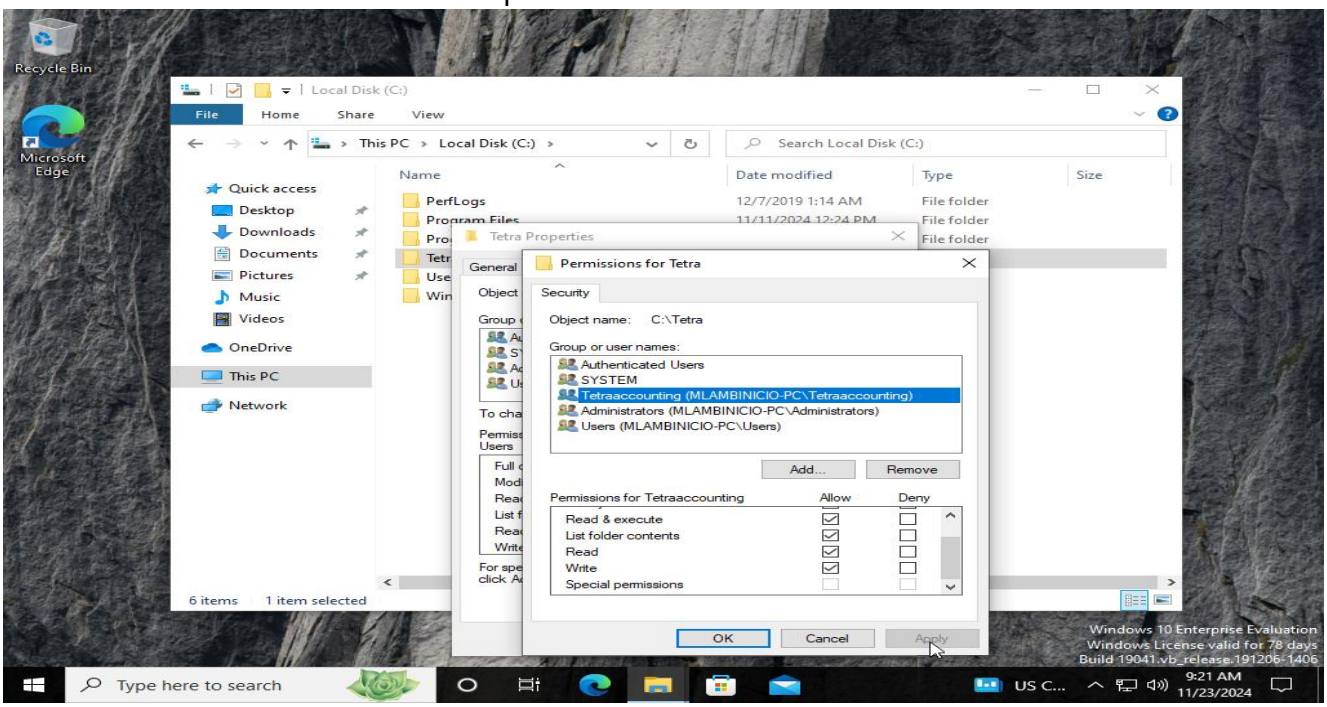
Step 7: Folder creation screenshot – To create a new folder for the group, open the FILE EXPLORER window. Choose THIS PC on the left pane and double click on C: drive. Anywhere on the right pane, right click and choose NEW, then FOLDER.



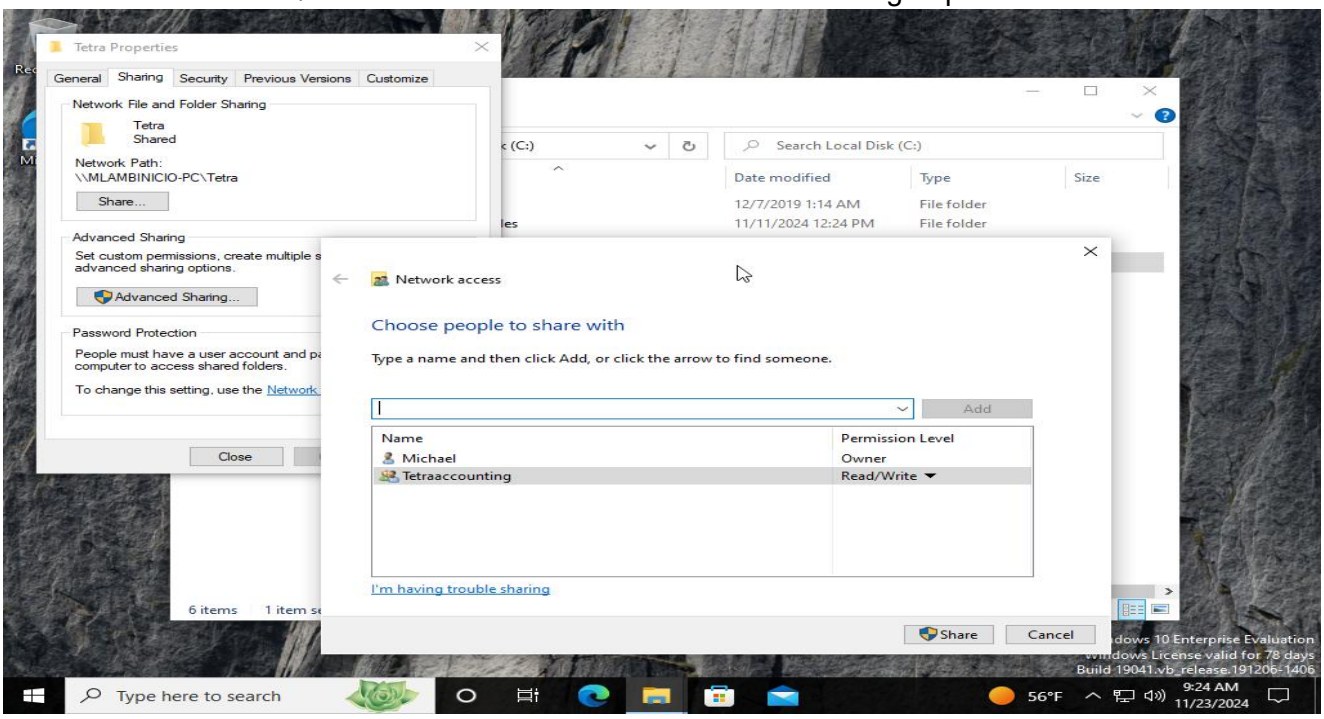
You can name the new folder TETRA, example is shown below.



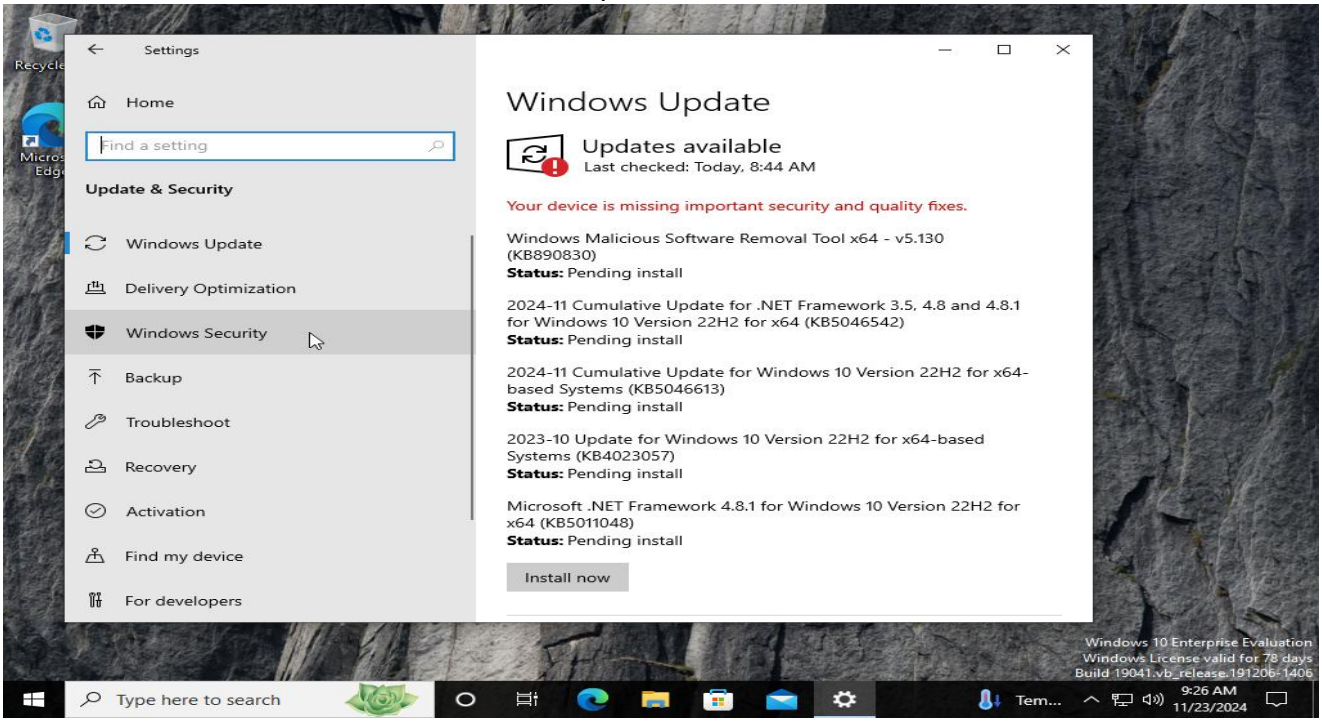
Step 8: Folder permissions screenshot – To set folder permissions for the Tetraaccounting group and its users to read and write in the Tetra folder, right click on the folder and choose PROPERTIES. Click on the SECURITY TAB and click ADD under GROUP OR USER NAMES. Type in TETRAACCOUNTING and click OK. Then click on Tetraaccounting and in the permissions for Tetraaccounting, scroll to the bottom and verify that the ALLOW checkboxes for READ and WRITE are checked. Example is below.



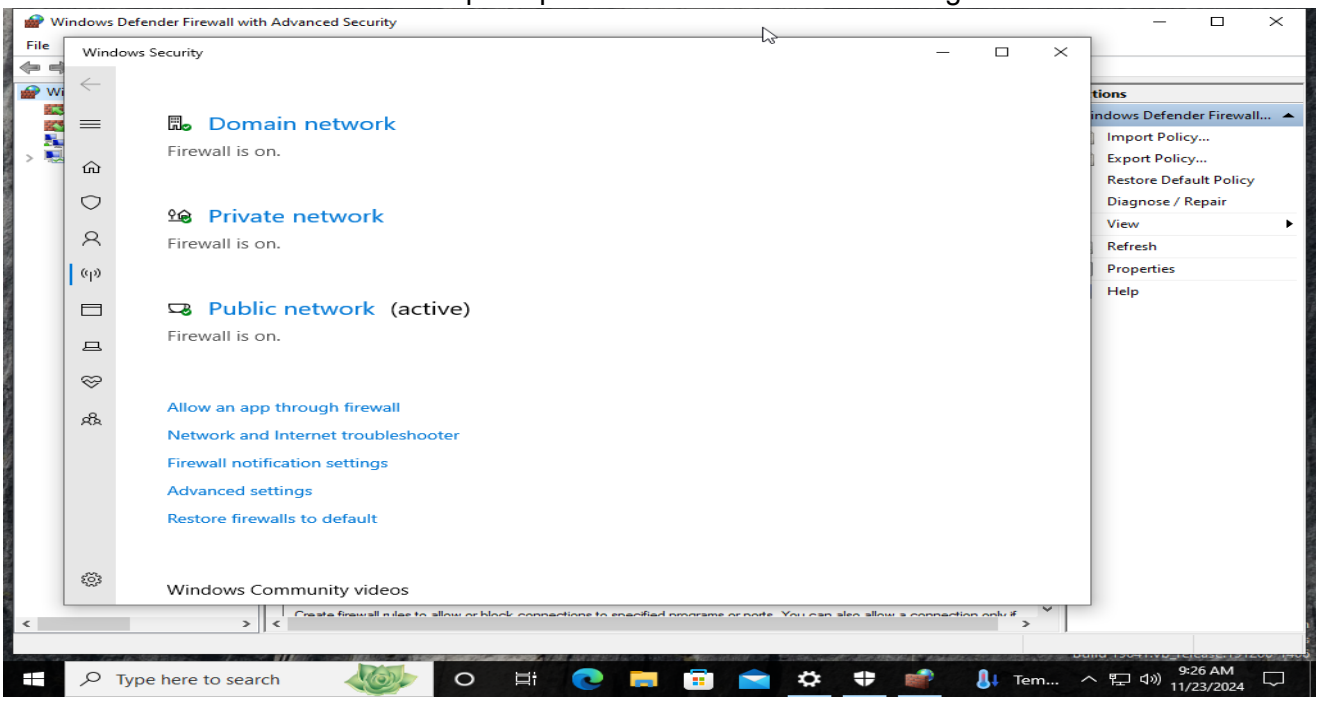
To verify that it can also be seen on the network, open the Tetra folder properties and choose the SHARE button. In the next window, click the drop down menu and choose Tetraaccounting from the list. When it shows in the box below, click the PERMISSION LEVEL on the right pane of it and choose READ/WRITE. Then click SHARE to share it to the group and members.



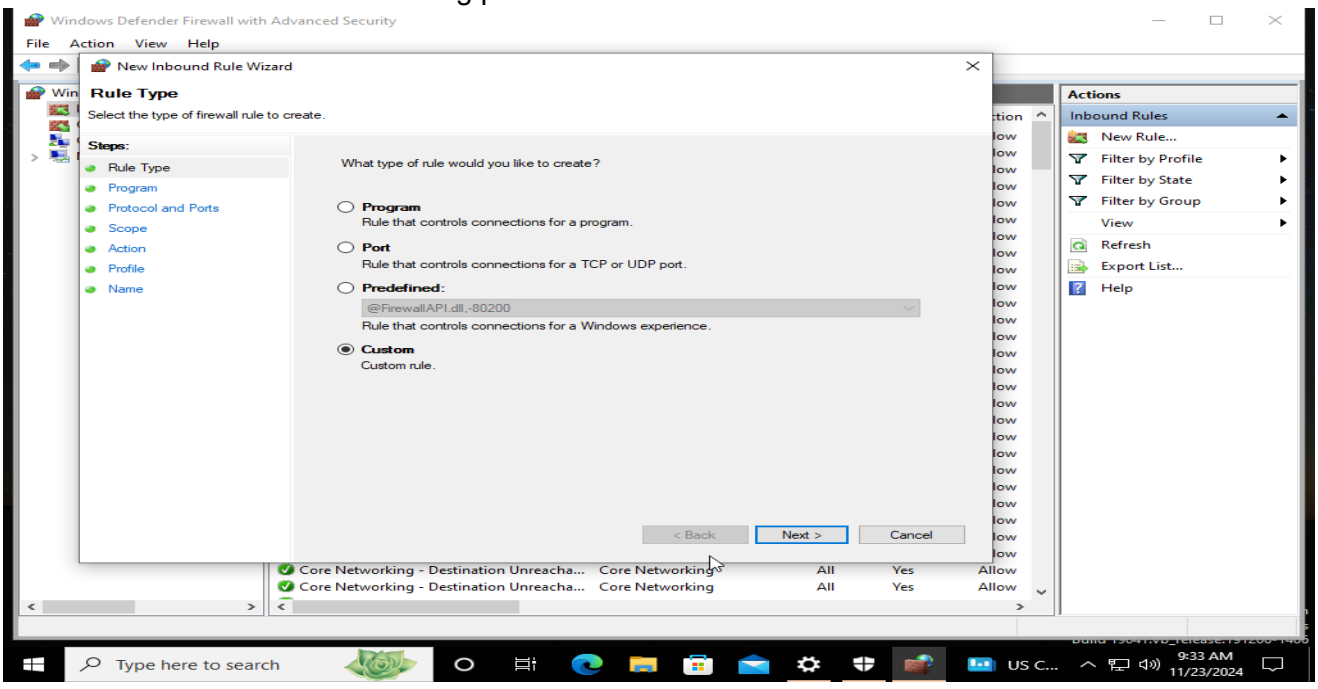
Step 9: Firewall configuration screenshot – To configure and block ICMPv4, start at the settings window. Then, choose WINDOWS UPDATE at the bottom of the left screen. Choose WINDOWS SECURITY as shown in the example.



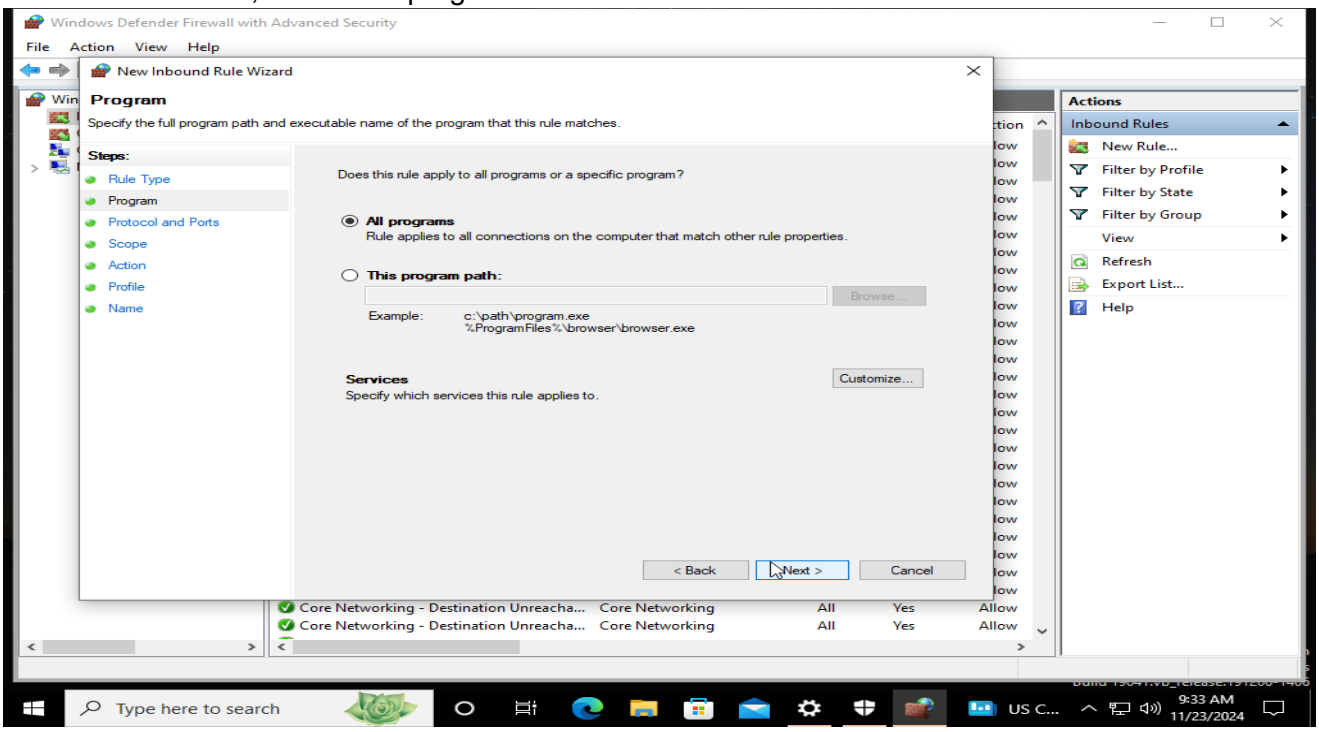
Choose ADVANCE SETTINGS to open up WINDOWS FIREWALL settings.



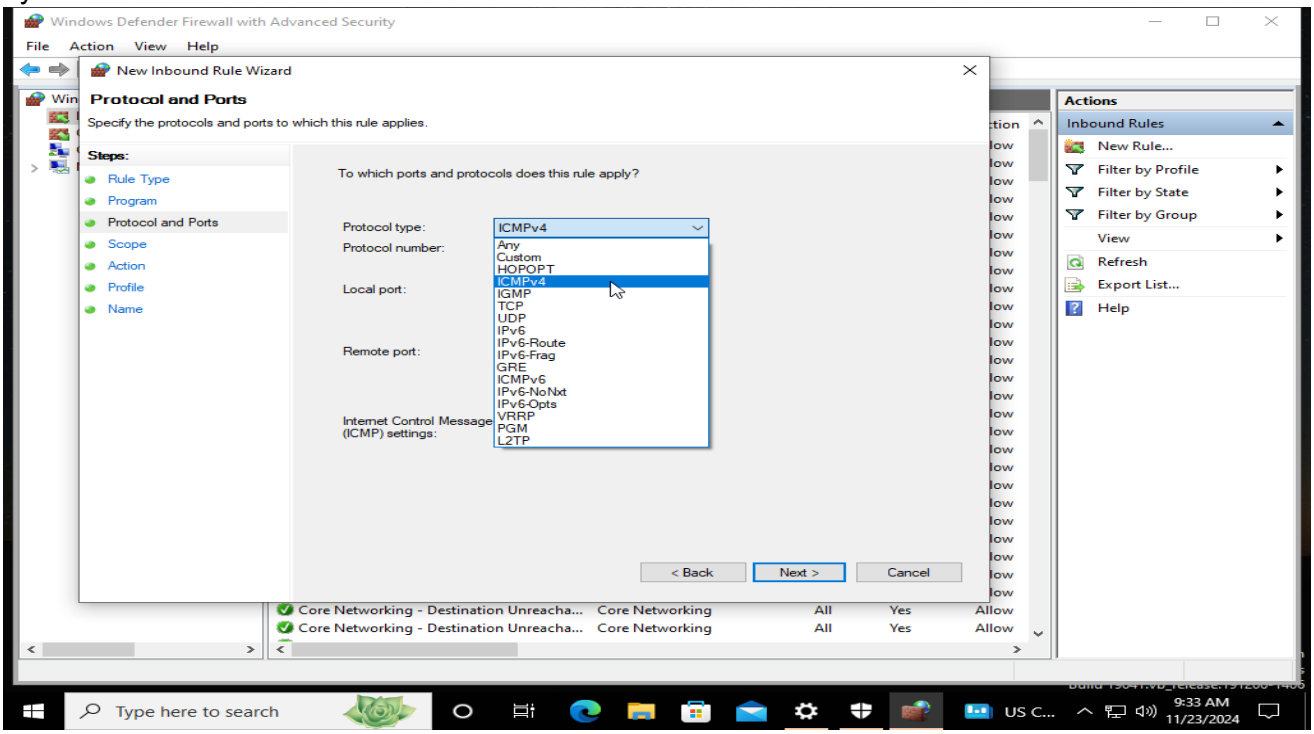
On the right pane, choose NEW RULE to open the new inbound rule wizard. Then select custom to start the ICMPv4 blocking process.



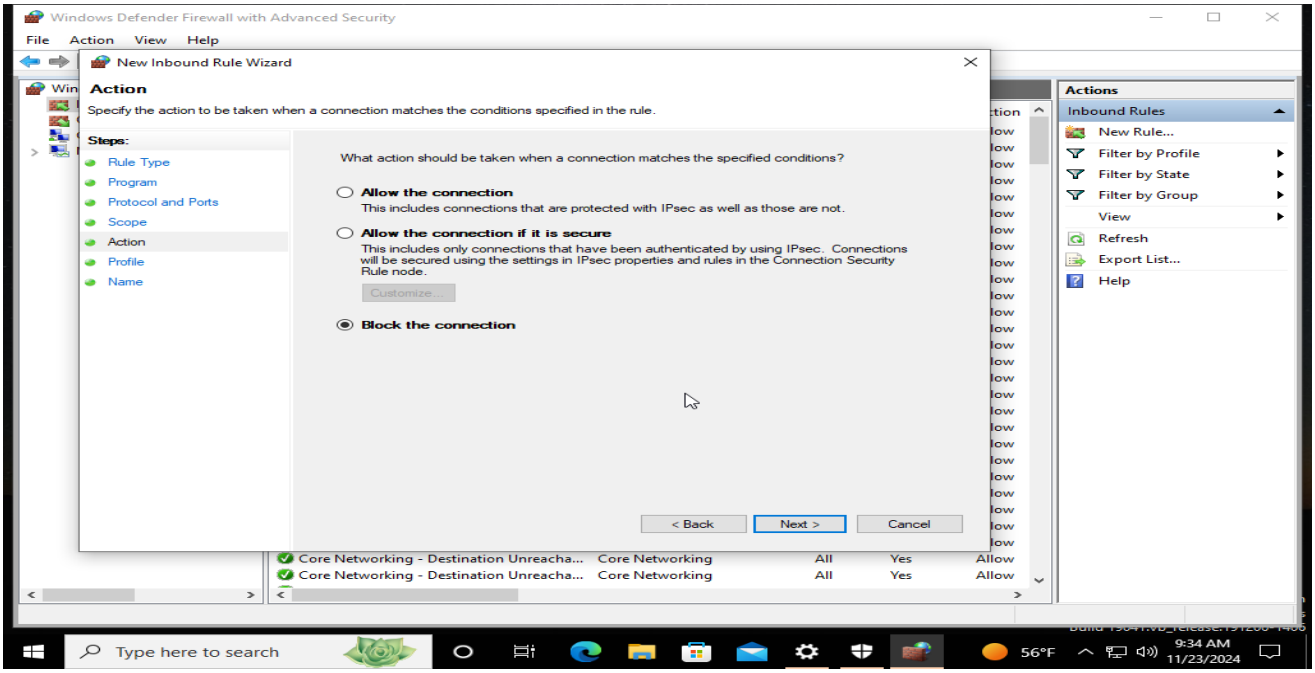
On the next screen, choose all programs.



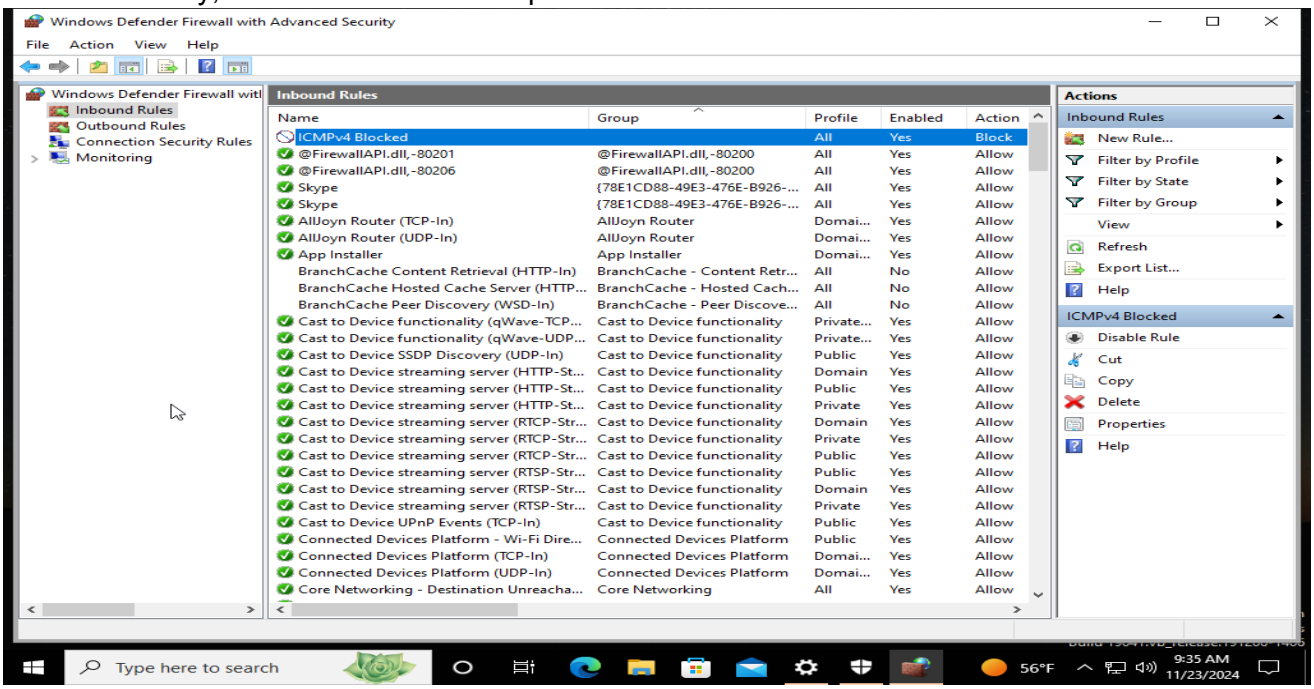
Then choose ICMPv4 in the protocol type. Leave the default selections on the next two screens by click next.



When you get to the action portion of the rule, choose BLOCK THE CONNECTION and click next.



If done correctly, it should show at the top of the screen that the ICMPv4 has been blocked.



Part 3: Windows 10 Upgrade Project Risk Factors

Two of the most important issues to consider before performing an upgrade to a workstation are the hardware components and their compatibility and knowing if you just want to do an upgrade, or complete fresh installation of an operating system. When you change your operating system, your hardware may be affected due to compatibility. If the hardware is outdated, it may not be supported on the updated operating system, or the hardware manufacturer may not support that current model any longer. Testing all old current hardware first to see if they are updatable and swapping out those components would ensure all workstations are in current operable status. Assuming all the workstations have the same original hardware, if swapping certain components is needed, then it would be easier to obtain those components in bulk so all firmware, drivers, etc. would be the same and updating would be easier.

The second is doing an upgrade of the operating system or clean install. Upgrading is a simplified process to have a seamless update to the workstations operating system without having to make too many changes to the workstation. One concern in doing this would be that because the upgrade would preserve the old operating system just in case you would like to rollback to it, it may cause a dual boot asking which operating system you would like to start if the workstation had to perform restarts when updating, etc. It would be time-consuming, and the solution would be to delete the preserved system. When doing a clean install of an operating system, all data at each workstation would have to be saved to a backup server or drive in order do this. If this isn't part of the first step when doing a clean installation, the major risk of losing all valuable data would be costly to the organization. The reward for doing a clean installation is that any errors or problems that occur would be easy to trace since there aren't too many software applications, devices and firmware updates to conflict with the possible issues.

Sources / References

[1] "How to Enable ICMP (PING) through the Windows Firewall with Advanced Security using Group Policy | Hammer Software," *hammer-software.com*. https://hammer-software.com/how-to-enable-icmp-ping-through-the-windows-firewall-with-advanced-security-using-group-policy/