

Master Sword Publishing's Information Technology Infrastructure Documentation

Capstone Project

Jayce Mangum
Computer Security & Network Technology
Lake Washington Institute of Technology
Professor Linda Epps
Spring 2026

Table of Contents

Master Sword Publishing Virtual Machine Environment Setup

Scenario Information.....	5
Overview	5
Master Sword Publishing Topology	5
macOS 26 Tahoe Virtual Machine Installation.....	6
macOS Setup Assistant & Parallel Tools Installation	8
Windows 11 Professional Virtual Machine	16
Windows 11 Out of Box Experience & Parallels Tools Installation	21
Windows Server 2025 Virtual Machine	26
Windows Server Installation & Setup.....	31
Ubuntu Desktop 26.04 LTE Virtual Machine	40
Ubuntu Desktop Installation & Setup Wizard	44
Ubuntu Server 26.04 LTE Virtual Machine	51
Ubuntu Server Installation & Setup.....	55
Kali Linux 2026 Virtual Machine	62
Kali Linux Install & Setup	66

MSPUB Active Directory & DNS Deployment

Scenario Information.....	72
Installation and Configuration of DNS and AD DS.....	73

MSPUB Network: IP Addressing, DNS Configuration Settings, & Domain Join

Scenario Infoformation.....	89
Configuring Network Settings in Windows 11	89
Adding Windows 11 Client to the MSPUB Domain	92
Configuring Network Settings in Ubuntu Desktop.....	95
Adding Ubuntu Desktop to the MSPUB Domain	99
Configuring Network Settings in macOS	102
Binding macOS to the MSPUB Domain.....	106
Configuring Network Settings in Kali Linux.....	110
Configuring Network Settings in Windows Server 2025.....	113
Adding a Windows Server to the MSPUB Domain as a Secondary Domain Controller	117
Configuring Network Settings in Ubuntu Server 26.04 LTE	119
Verifying All Virtual Machines Resolve Each Other on the Network.....	123

Security Features of Operation Systems

Windows 11 & Windows Server 2025	130
Ubuntu Desktop & Server 26.04 LTE	146
macOS 26 Tahoe.....	155
Kali Linux.....	160

Troubleshooting Scenarios

Scenario 1: Routing & DNS Misconfiguration	165
Scenario 2: User Account Locked Out	173
Scenario 3: Low Disk Space Issue.....	179
Scenario 4: Virtual Machine Network Issue	189

Master Sword Publishing Automation with Python Scripts

Automated Web Server System Configuration Script.....	198
User Management Script	211

Master Sword Publishing Network Hardware Configuration

Network Overview	228
Configuring UniFi Routers an Switches	229
Scenario Overview	229
Objective.....	229
Equipment Being Used.....	229
VLANs to Implement Table	229
UniFi Dream Machine Pro Out-of-Box Setup	229
Adopting UniFi Switches	232
Configuring Dual WAN Failover	234
Creating VLANs	236
Configuring Switches.....	241
Configuring Firewall/ACLs	247
Configuring UniFi Wireless Access Points (WAPs)	253
Scenario.....	253
Objective.....	253
Equipment Being Used.....	253
Wireless Networks	253
Configuring Wireless Networks in UniFi OS	256
Testing Network Elements	259
Download the Config File	261

Master Sword Publishing's Security Awareness Campaign & Incident Response Plan

Overview	262
----------------	-----

Security Awareness Campaign	262
Scenario	262
Objective.....	262
Phishing Email Campaign Details	262
Configuring AWS Resources for Fake Login	262
Add the DNS Records from AWS to GoDaddy.....	271
Logging Clicks with AWS Lambda	272
Creating the Phishing Email.....	279
Phishing Email Results	281
Source Code.....	283
Incident Response Plan	296
Scenario	296
Objective.....	296
Master Sword Publishing Incident Response Plan	296
Executive Summary	296
Purpose	296
Standards Alignment	296
Scope.....	297
Incident Response Team	297
Incident Response Lifecycle.....	297
Roles and Responsibilities.....	300
Incident Severity Classification.....	301
Communication & Escalation Procedures	306
Evidence Collection & Preservation.....	307
Continuous Improvement	308
Legal & Regulatory Considerations	310
Document Control	310

References

Master Sword Publishing Virtual Machine Environment Setup

Scenario Information

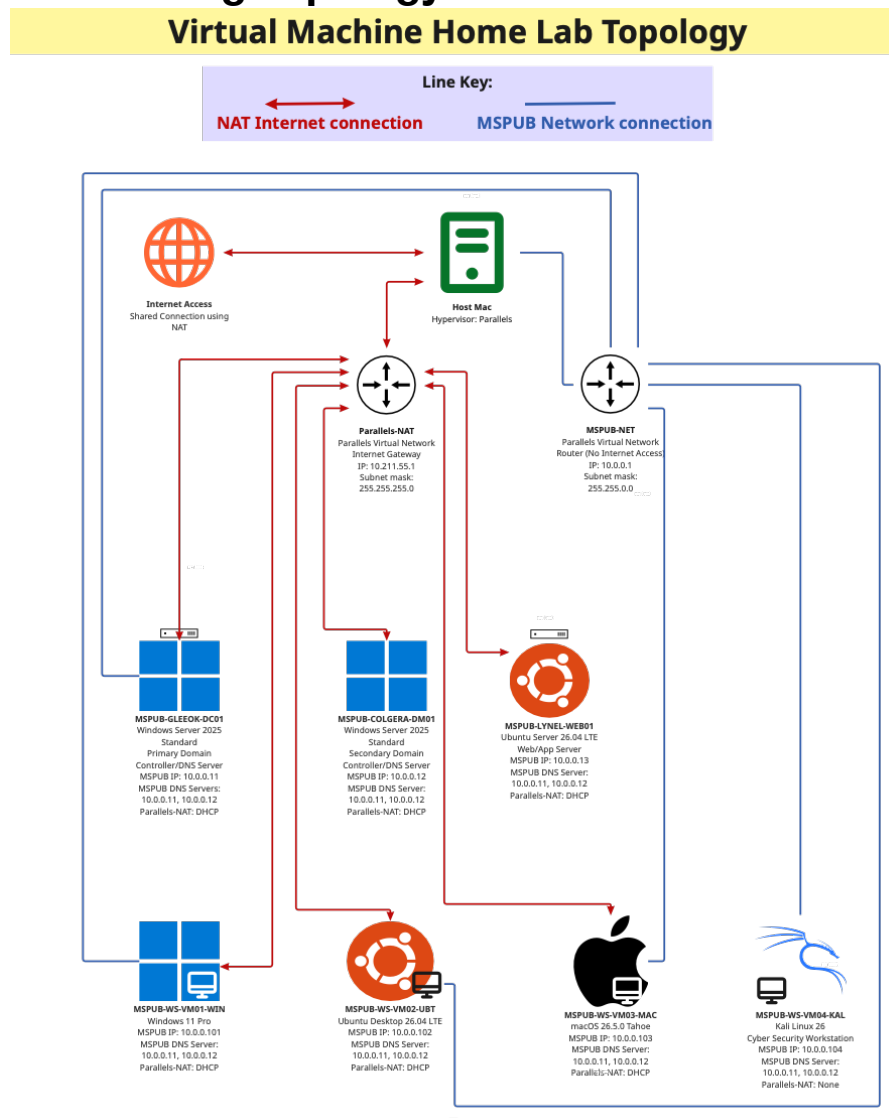
A startup company called Master Sword Publishing is rapidly growing. They currently have seven employees. They have decided to hire a new Information Technology/Cybersecurity team: two IT staff and one cyber operations person. This new IT staff is to design and maintain a new internal computer network. MSPUB's current infrastructure has no servers, only independent computers that are poorly managed.

Overview

Using Miro create a topology designing Master Sword Publishing's new IT infrastructure. It must include two Windows servers and one Linux Web/App server, three primary machines with mixed operating systems (Windows, macOS, Linux), and one Kali Linux terminal for cybersecurity use only.

Using a hypervisor (Parallels), create the topology in a virtual home lab environment. Demonstrate virtual machine creation for each virtual machine as well as the initial operating system installation and setup process. Document the process.

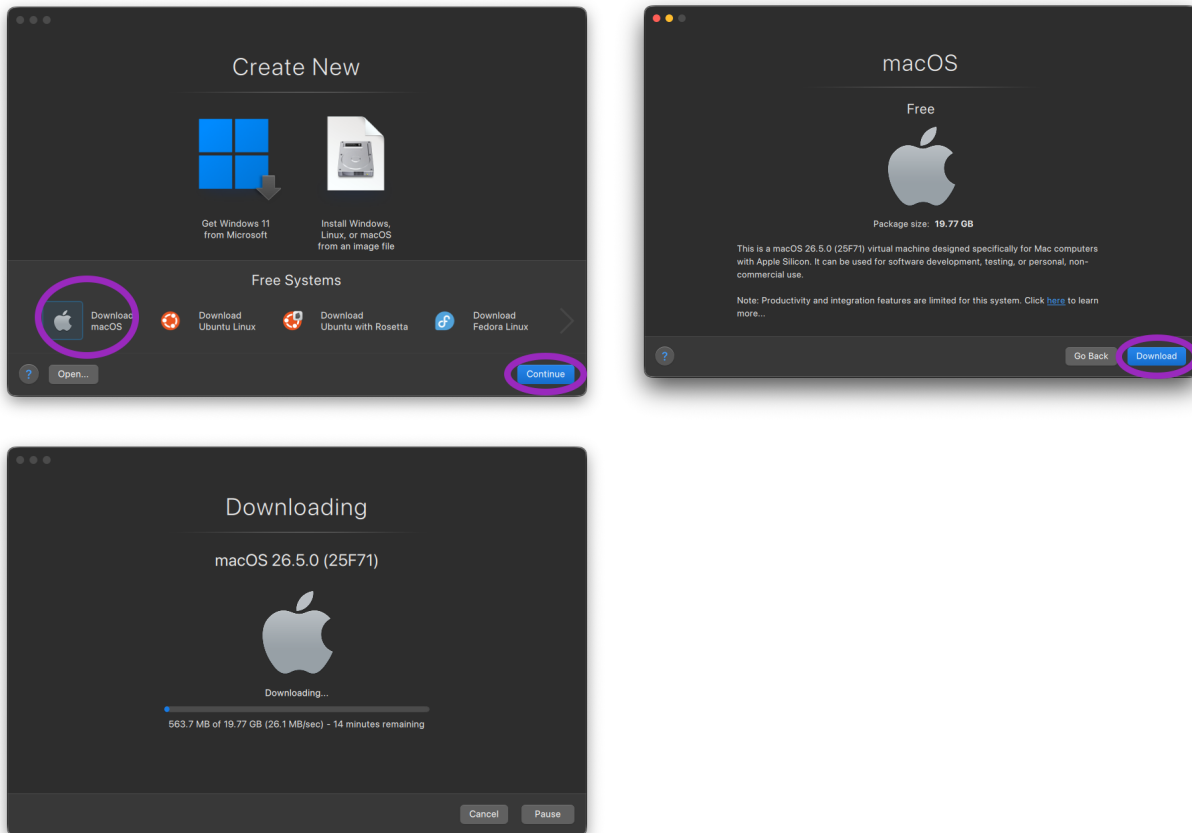
Master Sword Publishing Topology



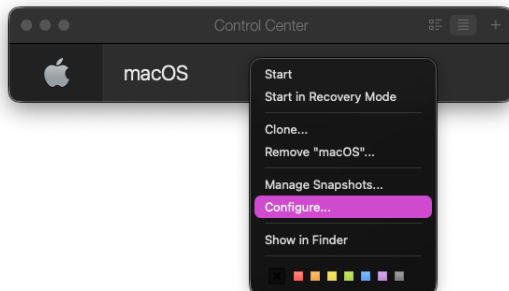
macOS 26 Tahoe Virtual Machine Installation

When creating an macOS virtual machine it is important to know the minimum system requirements for the operating system, which can be found on Apple's website, <https://support.apple.com/en-us/122867>. One thing to keep in mind a macOS can only be installed on Macintosh Hardware, which includes virtualization, as well as there are only two official hypervisors that come with native support if the host system is an Apple Silicon Mac. macOS 26 Tahoe will work on limited Intel based Macs as well as any M-series processors. You must have at least a minimum of 50 gigabytes of storage and 8 gigabytes of RAM.

1. In Parallels to create a new select "Download macOS" and click on "Continue". Click "Download" on the macOS details window to begin downloading the operating system.

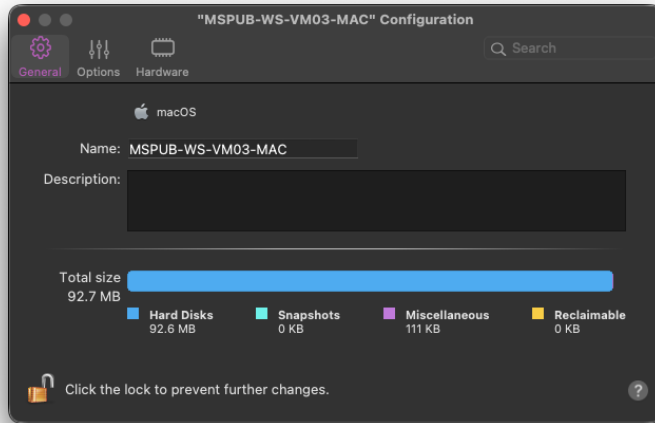


2. After macOS finishes downloading and installing to a new VM, it can be found in Parallels Control Center. To configure the new VM, right click "macOS" in Parallels Control Center and select "Configure..."

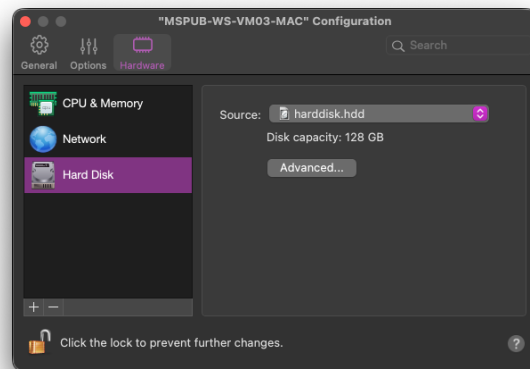
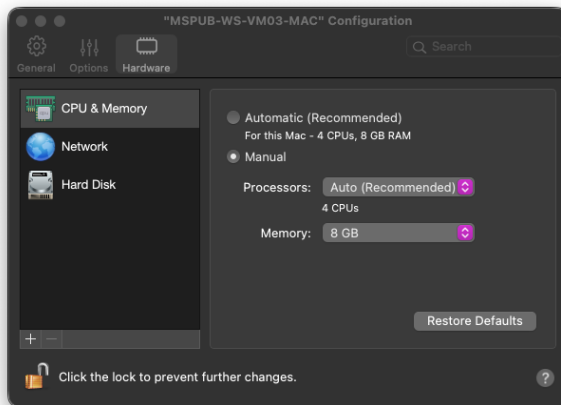


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

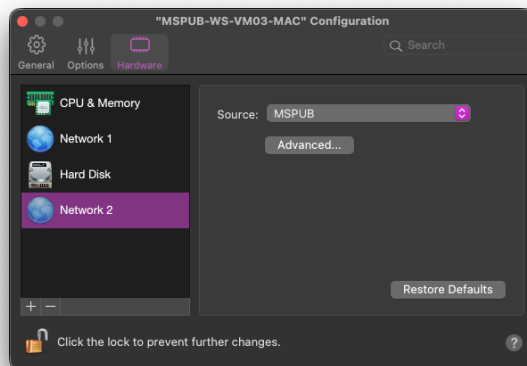
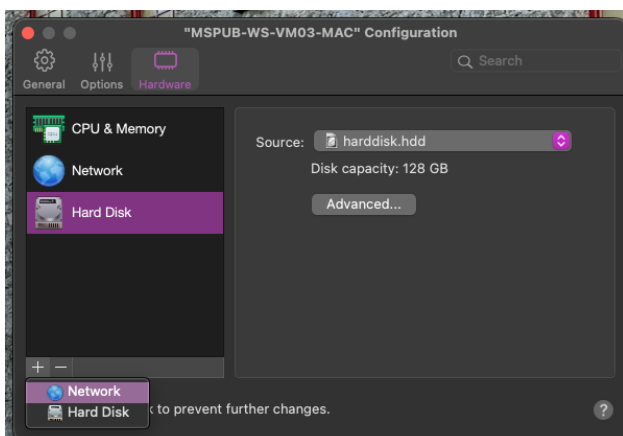
3. In the “macOS” Configuration window, under the general tab give it a new name. In this case it will be called, “MSPUB-WS-VM03-MAC,” which will change the name of the window.



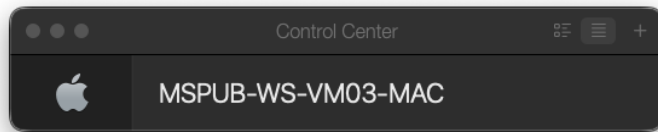
4. Under “Hardware” in the “MSPUB-WS-VM03-MAC” Configuration window, choose “CPU & Memory” choose “Manual.” Under the Processors drop down keep the default to “Auto,” for Memory, choose “8 GB.” On the left pane select, “Hard Disk” to confirm enough storage has been allocated to the VM, in this case 128 GB has been given to the VM, you can adjust it as needed by clicking “Advanced...”



5. In the same “MSPUB-WS-VM03-Mac” Configuration window click the “+” button in the lower left corner, and select “Network” to add an additional Network Adapter. “Network 2” should be selected, under Source choose “MSPUB” or another secondary predefined subnet source, if your VM requires a secondary network. Network 1, shares the host Mac’s internet connection, using NAT. We will keep Network 1 as default. Close the “MSPUB-WS-VM03-MAC” Configuration window.



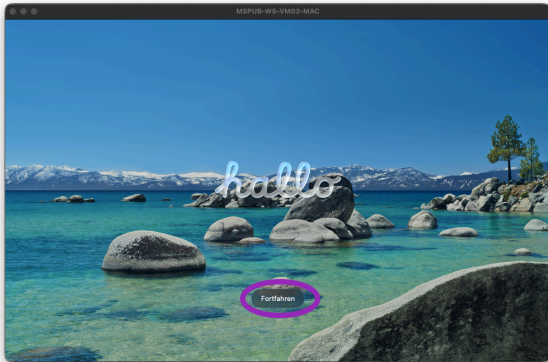
6. In Control Center, click on the Apple logo to start the virtual machine.



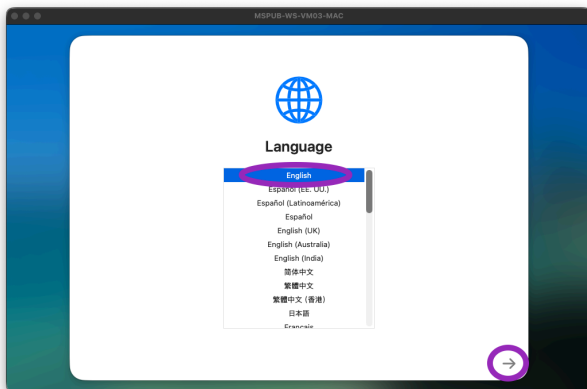
macOS Setup Assistant & Parallel Tools Installation

Parallel installs a specialized virtual machine image of macOS, so it doesn't take you through the traditional macOS Installation Assistant for physical Mac hardware. After the Virtual Machine has been created and macOS has finished installing, you will be greeted with the Setup Assistant which will guide you through configuring language settings, country or region, accessibility settings, and creating a new user account.

1. At the scrolling languages "Hello" screen click continue to enter the macOS Setup Assistant.

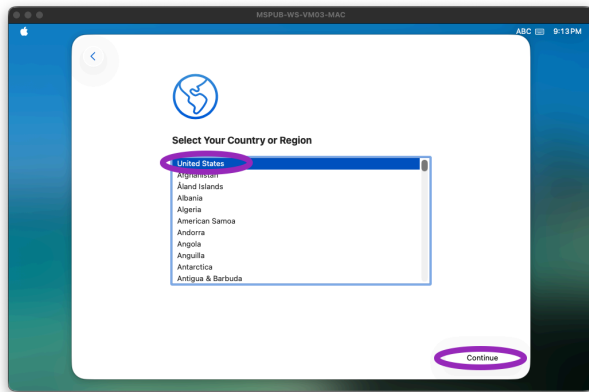


2. Select the language you want macOS to use for the system, in this case "English" has been selected. Click the right pointing arrow to continue.

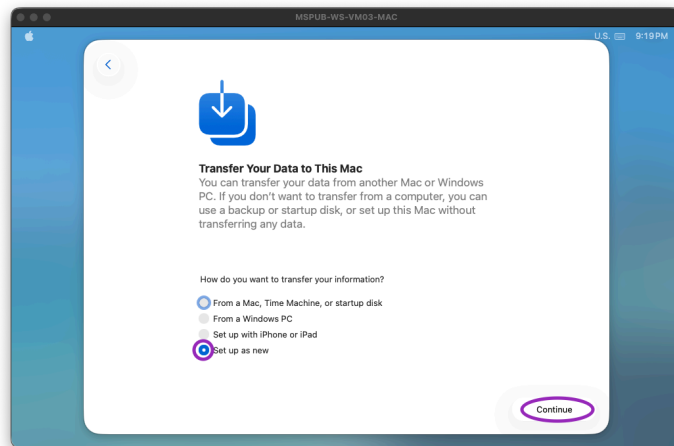


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

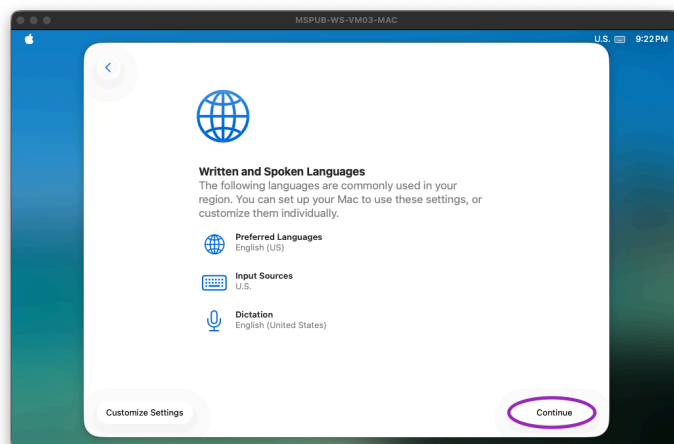
3. Select the country or region which will determine configure the keyboard layout, currency, and other country specific settings, in this case “United States” is selected. Click “Continue”.



4. If this were a new Mac users have the option to transfer files, apps, and settings from an older Mac or Windows PC. If users don't have access to their old Mac and they have a backup of the system stored in iCloud they may choose “Setup with iPhone or iPad” to sign them in and choose their iCloud backup. Since this is a virtual machine select, “Set up as new.” Click “Continue.”



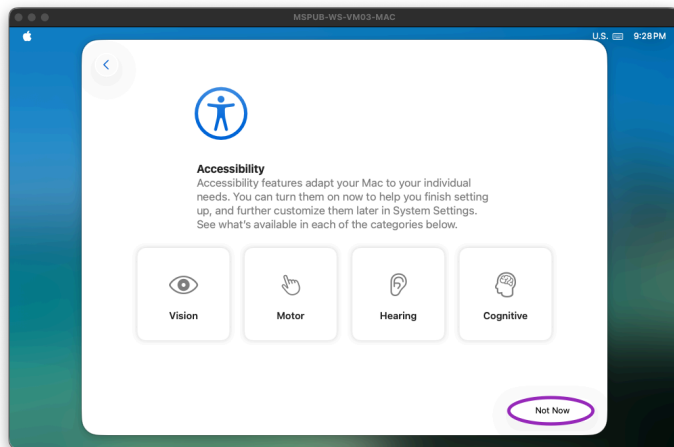
5. macOS will confirm it has selected the correct Written and Spoken Languages for the user. If they need to be changed, they can be manually configured. If these settings are correct click on “Continue.”



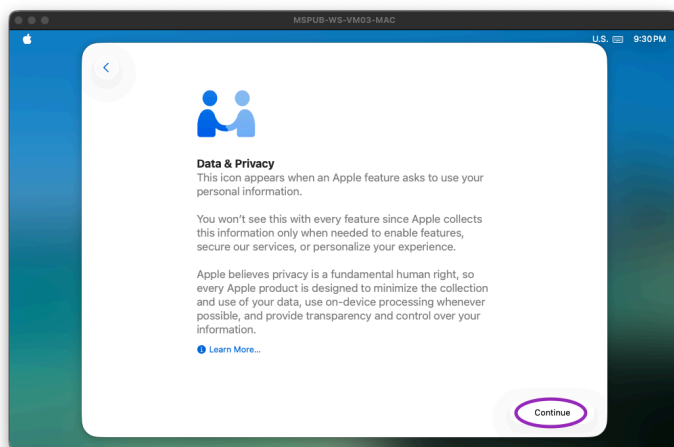
6. macOS has tons of Accessibility settings for users that may have disabilities making their Mac more accessible to them based on their needs, such as people who have vision impairments, motor skills,

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

hearing loss, or even cognitive disabilities. For the purposes of this lab click “Not Now.”

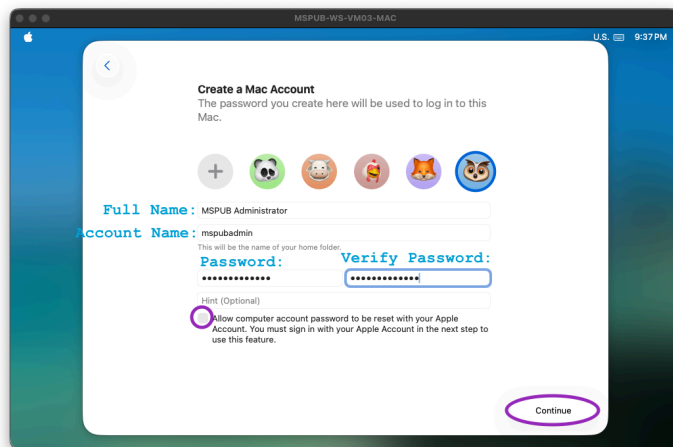


7. The next screen goes over Apple’s Data & Privacy policies. Click “Continue” to accept.



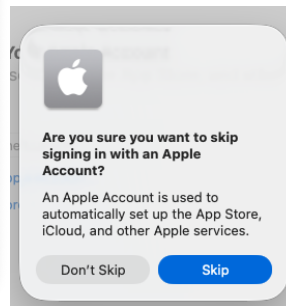
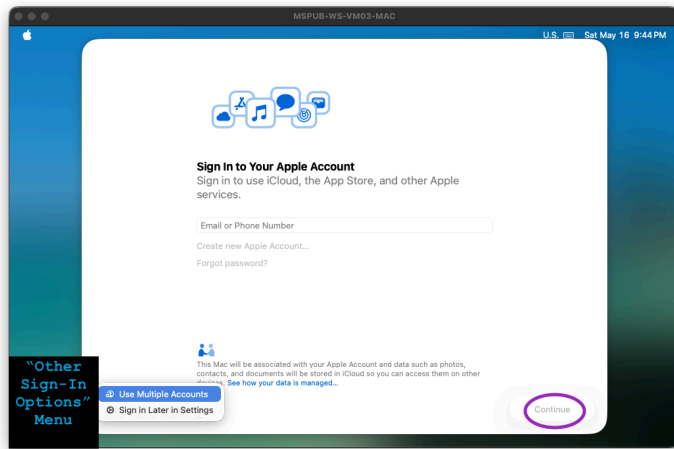
8. Create a new user account. For this lab’s purposes, fill in the following information, then click “Continue”:

- Full Name: **MSPUB Administrator**
- Account Name: **mspubadmin**
- Password: **CSNT253_2026#**
- Verify Password: **CSNT253_2026#**
- Deselect: *Allow computer account password to be reset with your Apple Account*

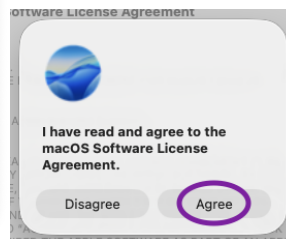
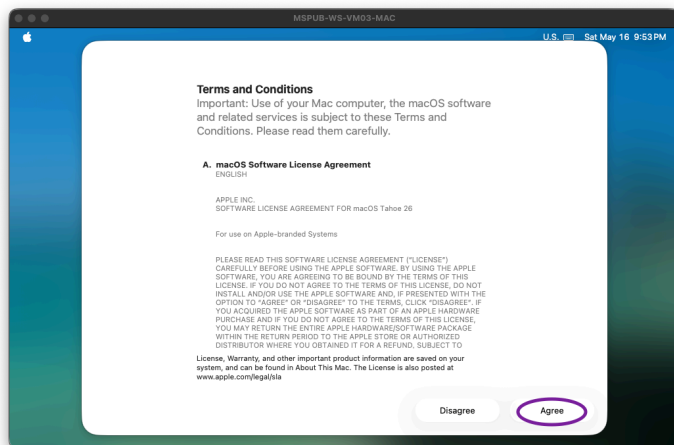


9. You will be asked to sign into an Apple Account. To bypass this click on “Other Sign-In Options,” then select “Use Multiple Accounts” and click “Continue.” Click “Skip” on the confirmation popup message.

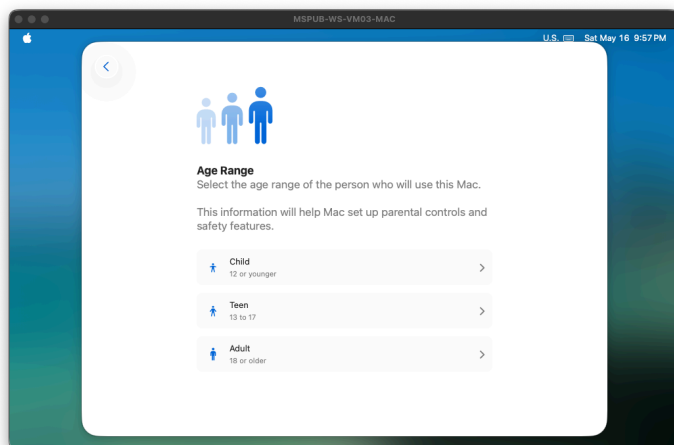
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



10. Read through the Terms and Conditions and click “Agree.” Click “Agree” again on the popup message.

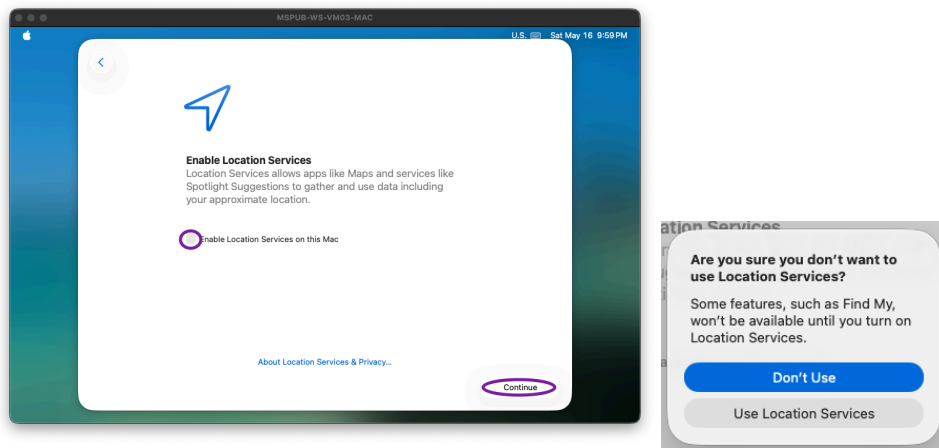


11. Choose the age range of the primary user.

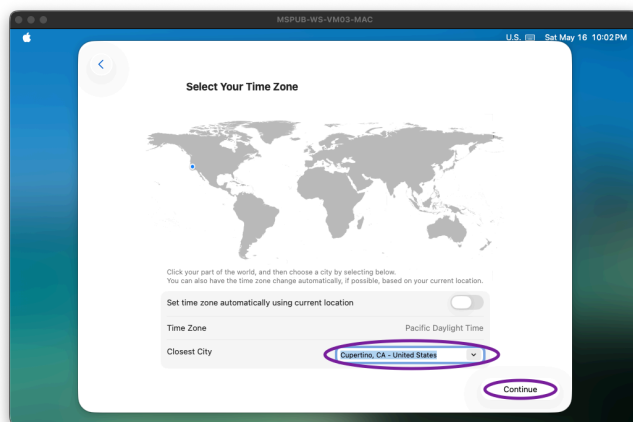


12. Keep Location Services disabled, by ensuring that “Enable Location Services on this Mac” is deselected. Click “Continue.” Click “Don’t Use” on the popup message.

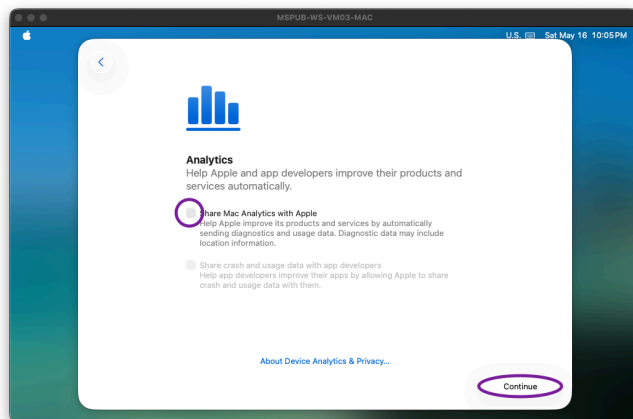
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



13. Choose the closest city to you in the drop down menu to set the Time Zone. In this case “Cupertino, CA” is the closest city which is in the Pacific Time Zone. Click “Continue.”

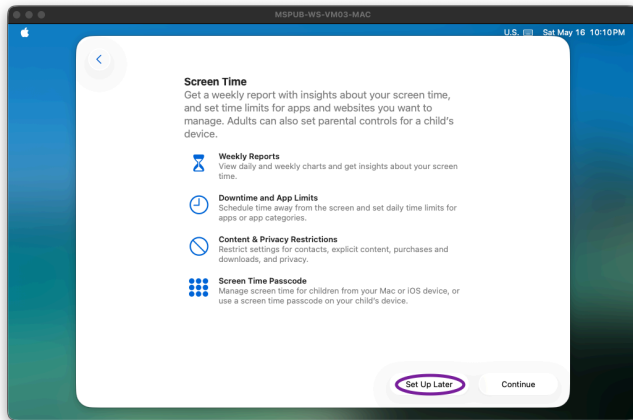


14. Deselect “Share Mac Analytics with Apple.” Click “Continue.”

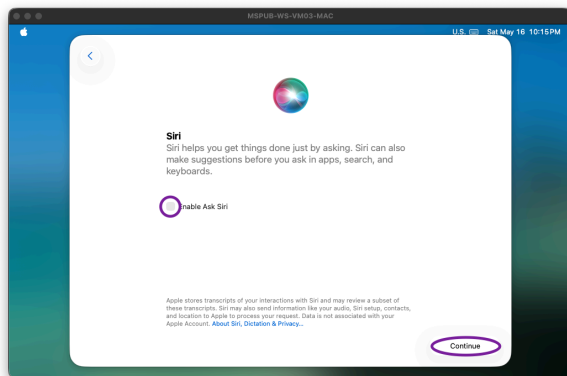


15. macOS allows you to set specified Screen Time usage across different apps, which is used in place of Parental Controls. It will also send parents a report of their child's app usage and internet history. This is also usefully if you want to set up limitation for social media apps for yourself. For this lab choose “Set Up Later.”

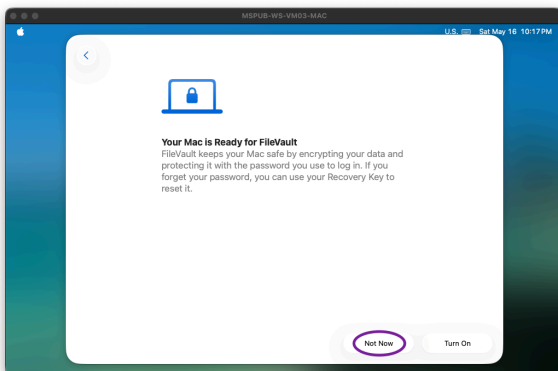
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



16. You can setup Apple's personal assistant, Siri right in Setup Assistant, for this lab deselect "Enable Ask Siri." If this were a newer Mac, the Siri setup screen is replaced with Apple Intelligence (AI) setup instead. Click "Continue."

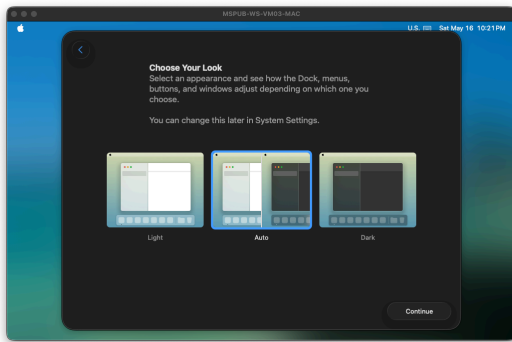


17. For now leave FileVault turned off, this will be configured in another lab section from System Settings instead. Click "Not Now." Click "Continue" on the popup window.

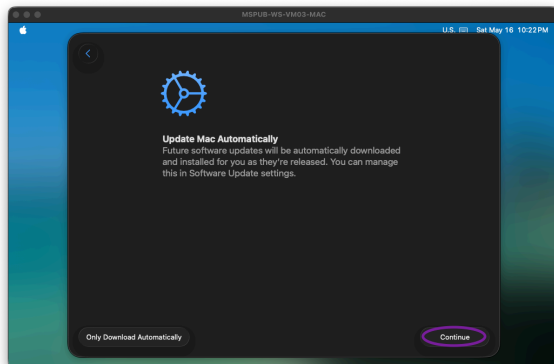


18. Select a theme, light mode, dark mode, or auto (switches between light and dark modes depending on the time of day). Click "Continue."

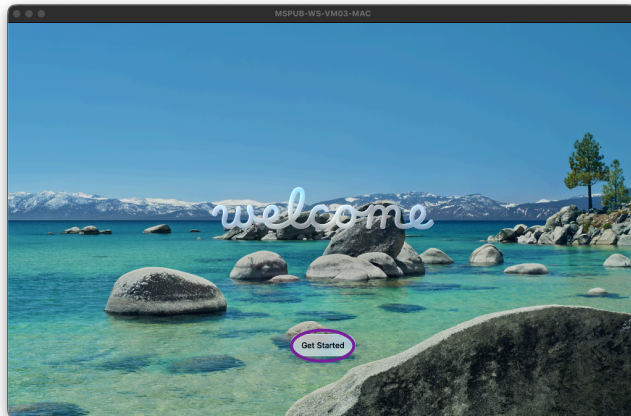
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



19. Click “Continue” to leave Automatic Software Updates turned on. Or “Only Download Automatically” to manually install updates later. For this lab click “Continue.”



20. macOS Setup Assistant is now complete. Click “Get Started” on the Welcome screen to take you to the macOS Desktop.



21. On the macOS Desktop double click the “Parallels Tools” icon. Double click “Install.” A GateKeeper window will popup asking you to authenticate with your user account and password. MSPUB Administrator should be pre-populated in the User Name field. Type in the password, “CSNT253_2026#” then click “OK.” This will install special drivers for the virtual machine. Once installed, click “Restart” to reboot the Mac VM.

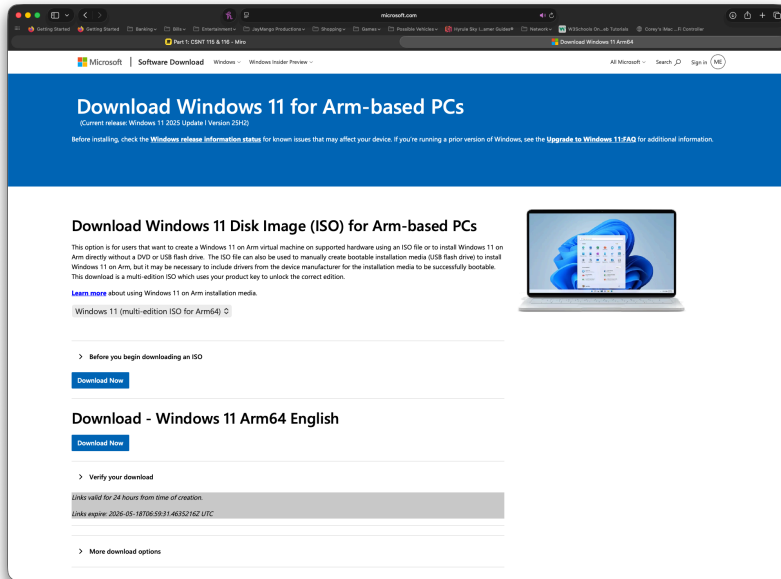
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



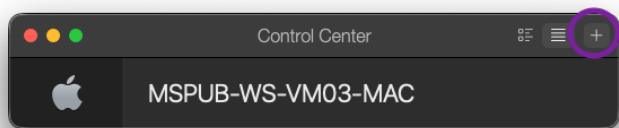
Windows 11 Professional Virtual Machine

When creating an Windows 11 Professional virtual machine it is important to know the minimum system requirements for the operating system, these can be found on Microsoft's website, <https://www.microsoft.com/en-us/windows/windows-11-specifications>. At least 1GHz and 2 CPU core, 4 gigabytes of RAM, 64 gigabytes of storage, and a TPM 2.0 chip are required prior to installation. This system will be installed using Parallels for Mac, and the ARM64 version will be installed.

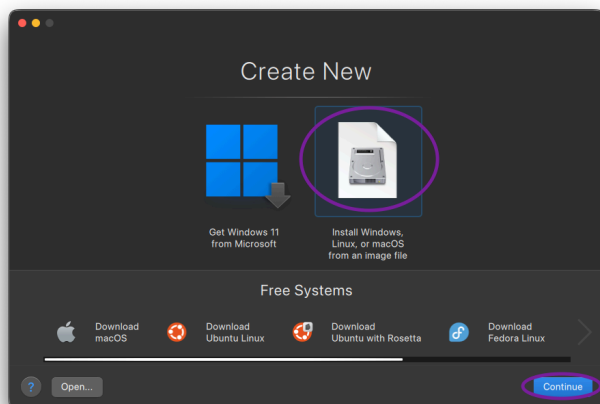
1. First, you will need to download Windows 11 ARM64 from Microsofts website, <https://www.microsoft.com/en-us/software-download/windows11arm64>.



2. From Parallels Control Center click the “+” in the upper right corner of the window to create a new virtual machine.

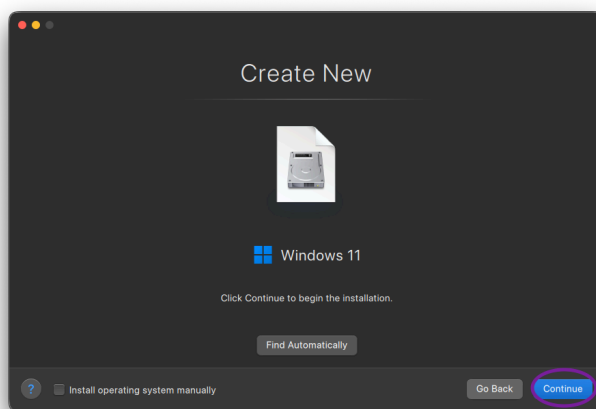
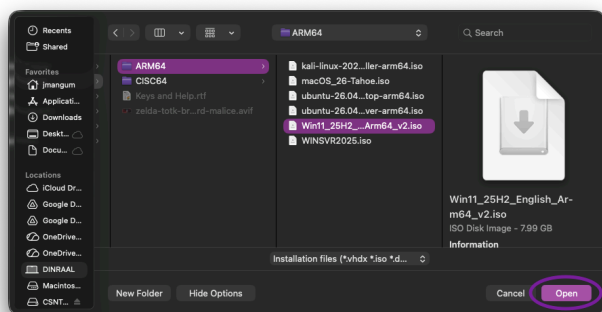
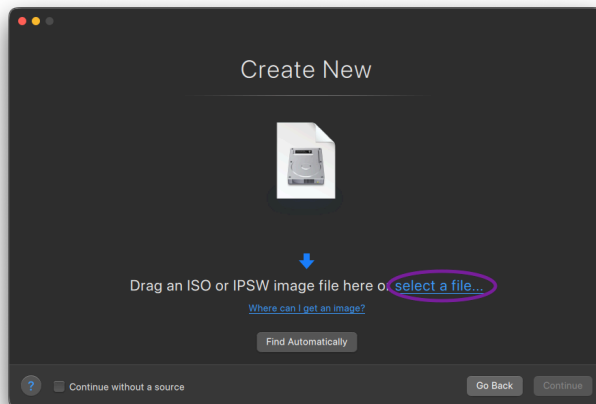
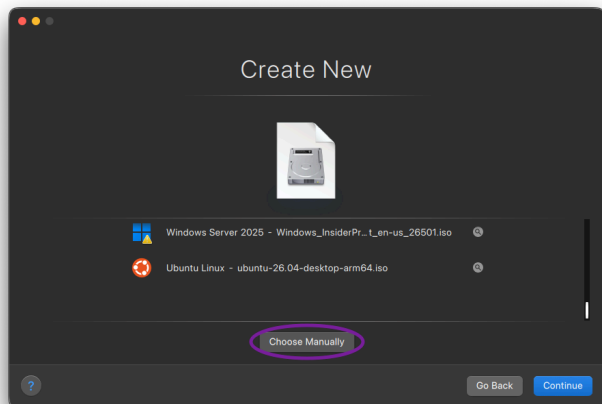


3. On the Create New window click on “Install Windows, Linux, or macOS from an image file.” Click “Continue.”

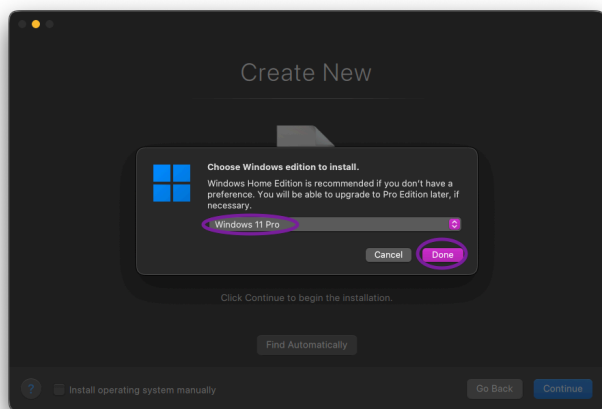


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Click the “Choose Manually” button. Click “select a file...” Navigate and select the Windows 11 ISO file, then click “Open.” Parallels will automatically recognize the operating system. Click “Continue.”

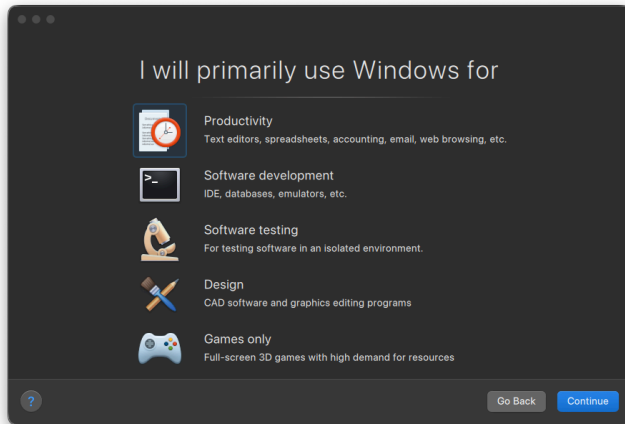


- Select the edition “Windows 11 Pro” from the drop down menu and click “Done”

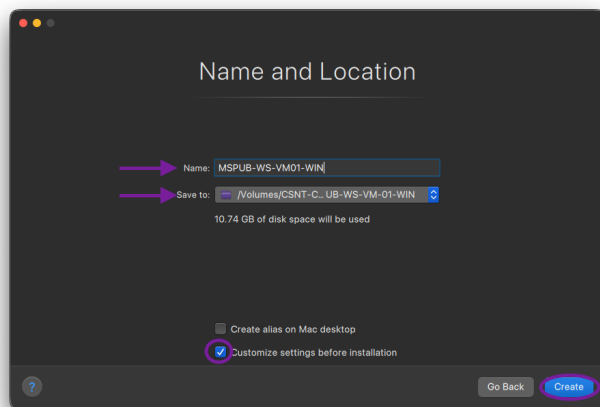


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

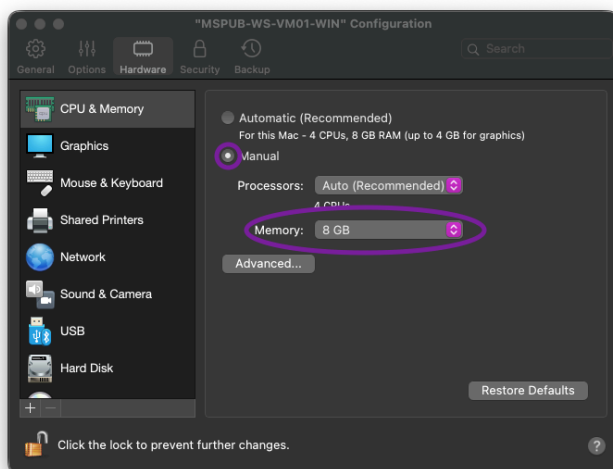
6. You can select what the VM will be used for. For this lab accept the default, “Productivity” and click continue.



7. Name the VM “MSPUB-WS-VM01-WIN” and choose a destination to save the VM. Select “Customize settings before installation.” Click “Create.”

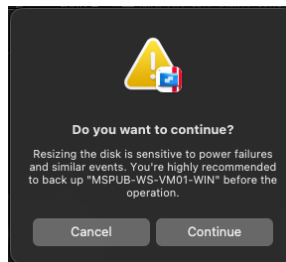
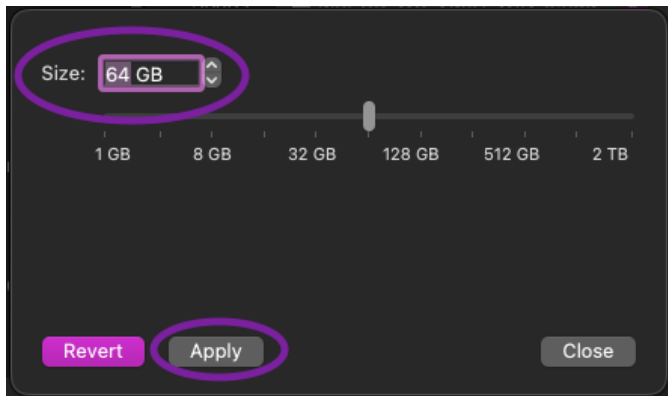
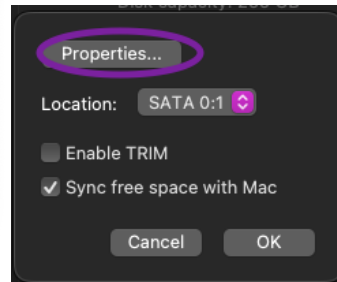
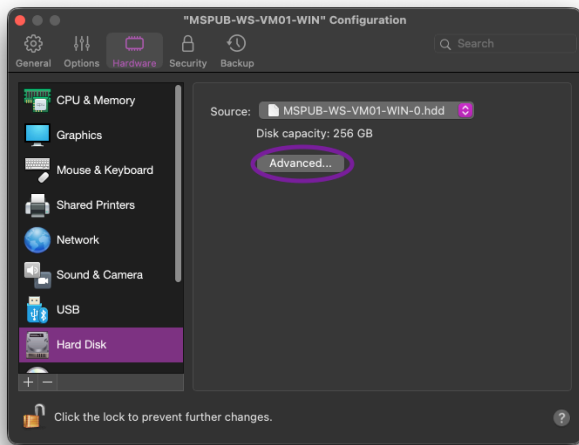


8. In the “MSPUB-WS-VM01-WIN” Configuration window click “Hardware” at the top, then select “CPU & Memory” and select “Manual.” Leave Processors set to “Auto.” Choose “8 GB” under the Memory dropdown menu.

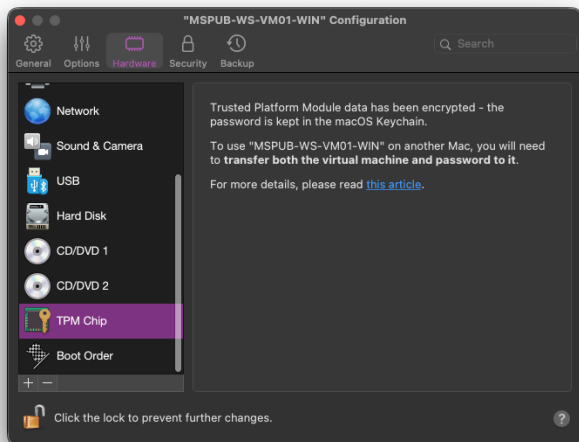


9. Click on “Hard Disk” in the “MSPUB-WS-VM01-WIN” Configuration window and click on “Advanced...” Click “Properties...” on the popup window. Reduce the size to “64 GB” and click “Apply” then “Close.” Click “Continue” in the warning popup window. Close the “Size” popup window. Click “OK” on the “Properties” window.

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

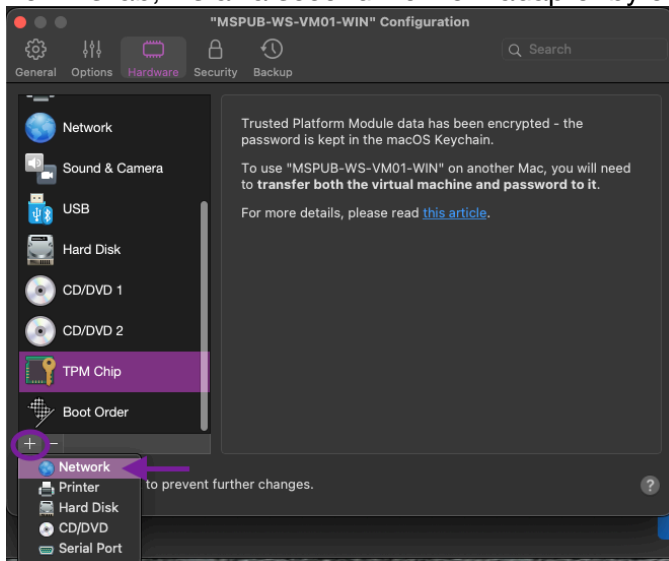


10. Scroll down the hardware list to ensure there is a TPM Chip installed.

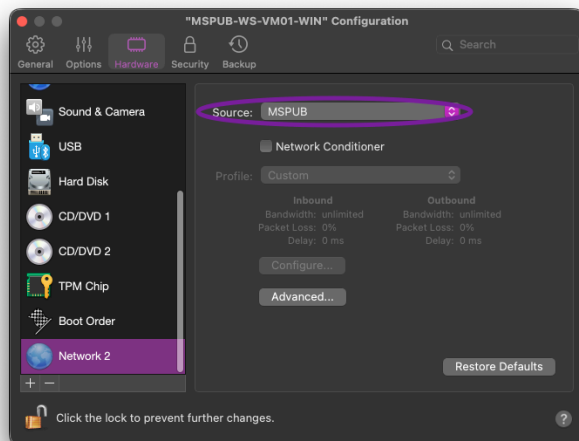


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

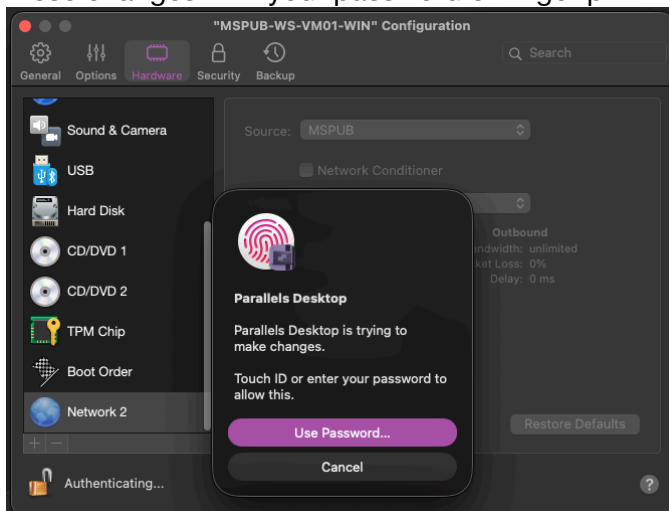
11. For this lab, install a second Network adapter by clicking the plus in the lower left and select “Network.”



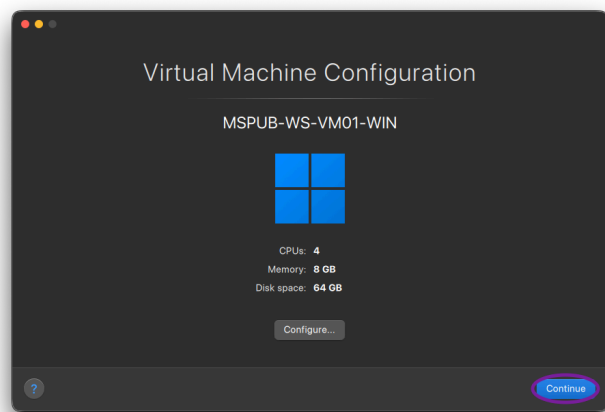
12. Configure Network 2 with the predefined source “MSPUB” in dropdown menu.



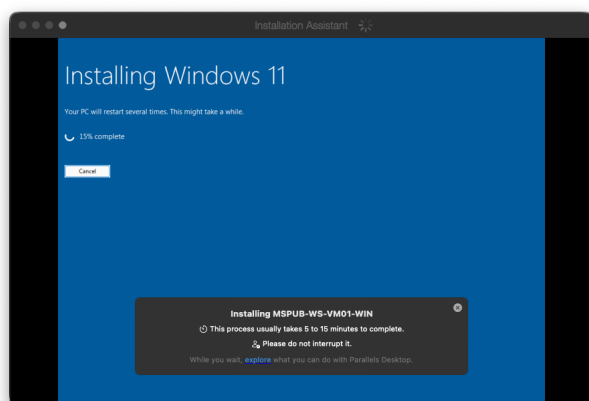
13. Click the “Lock” icon in the lower left to prevent further changes. Close the “MSPUB-WS-VM01-WIN” Configuration window, by clicking the red dot in the upper left corner. You may be required to authenticate these changes with your password or finger print.



14. Click “Continue” on the Virtual Machine Configuration screen.



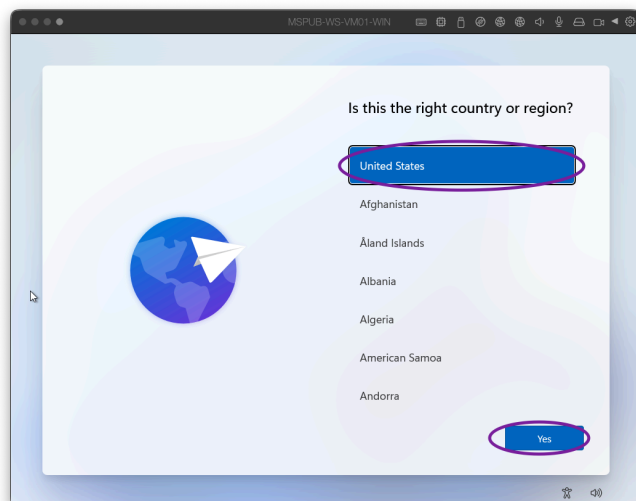
15. The VM will launch and begin installing the operating system automatically. No user input is required during the automated Installation Assistant process. It may take up to 15 or more minutes to install.



Windows 11 Out of Box Experience & Parallels Tools Installation

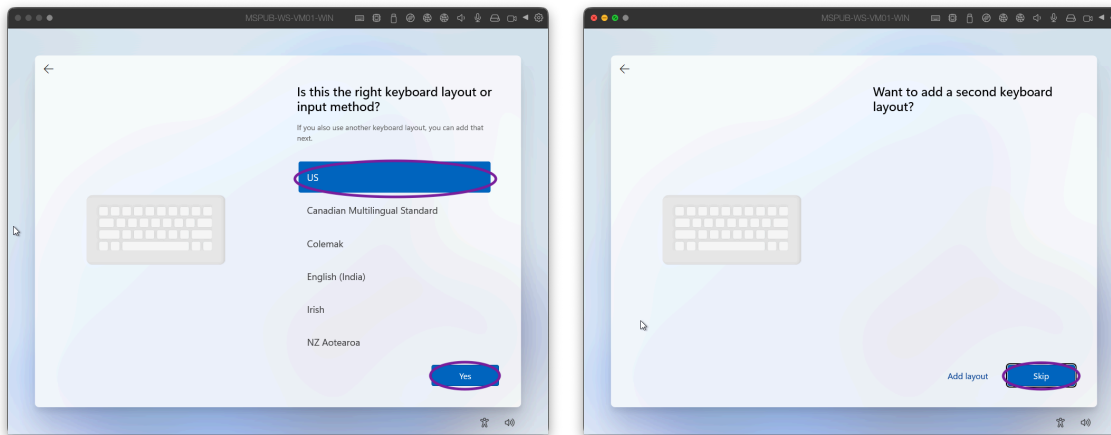
Microsoft has made it harder for users to bypass the Microsoft Account sign-in process. I will not be going through the traditional Out of Box Experience setup wizard, but will bypass it completely with a command.

1. Select the country or region you are in, in this case the “United States” is selected. Click “Yes.”

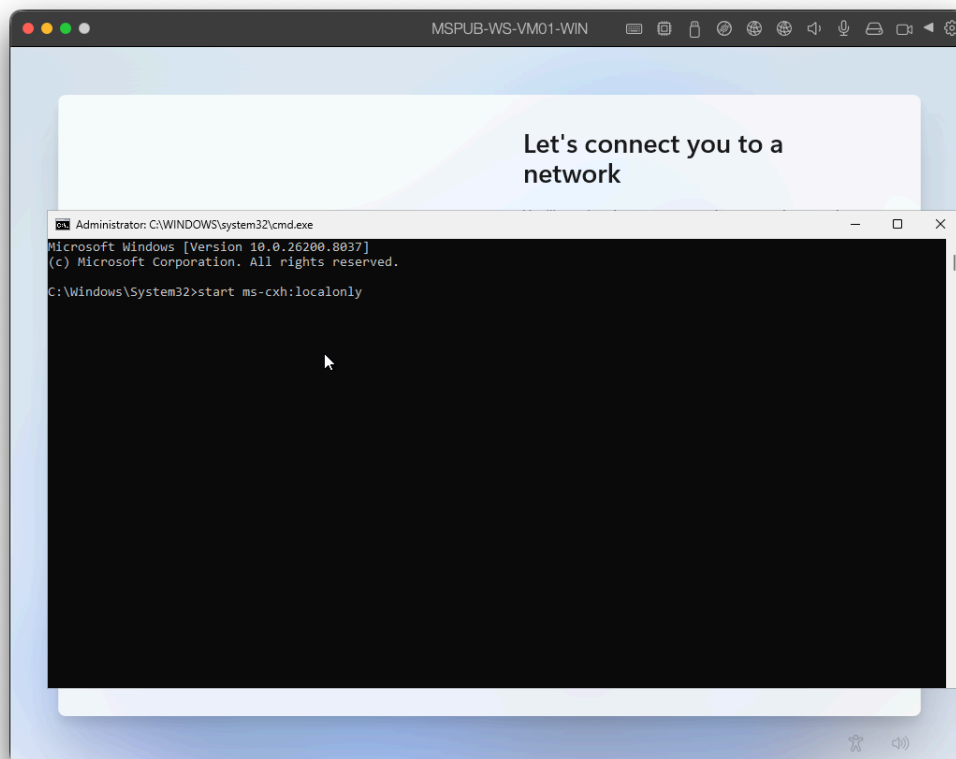


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

2. Select the keyboard layout, in this case “US” is selected. Click “Yes.” Don’t add a second keyboard layout. Click “Skip.”



3. At the the “Let’s connect you to a network” screen press Shift+F10 to open a Command Prompt window. (Some keyboard requires you to press Shift+FN+F10). Type “start ms-cxh:localonly” and press enter.

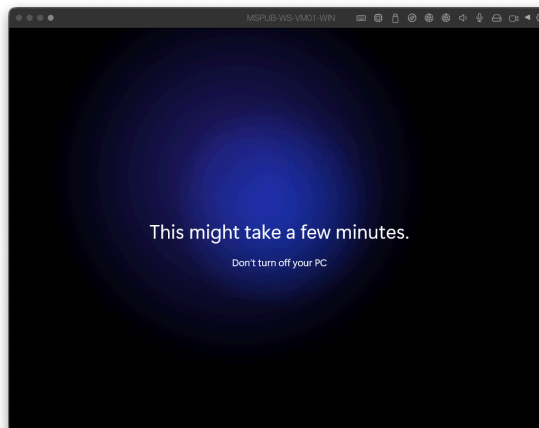
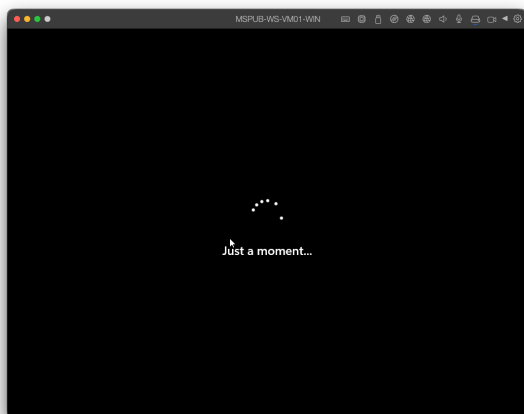


4. This will open the Microsoft account creation window. Fill in the following information, then click “Next”:
 - User Name: **mspubadmin**
 - Password: **CSNT253_2026#**
 - Renter Password: **CSNT253_2026#**

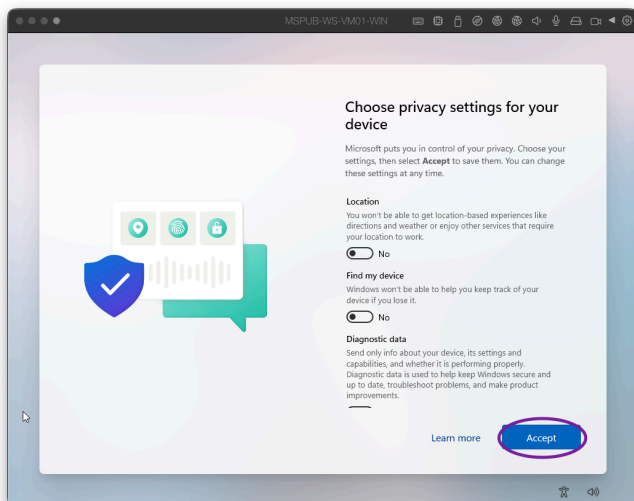
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Select 3 Security questions from the drop downs and type the answers

5. Windows will now reboot. Then setup the Local Account, without requiring the use of a Microsoft Account.

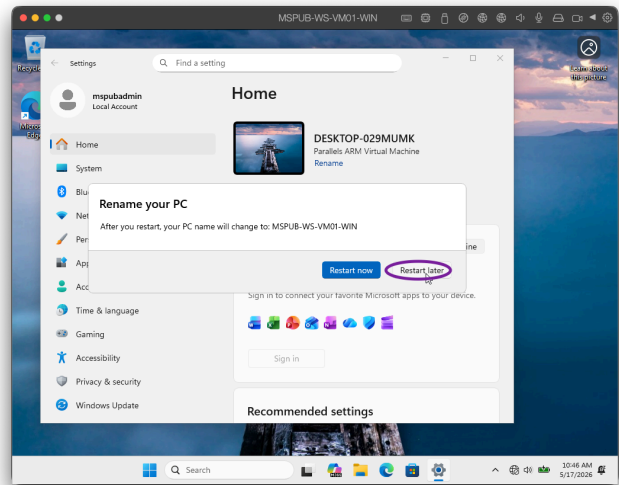
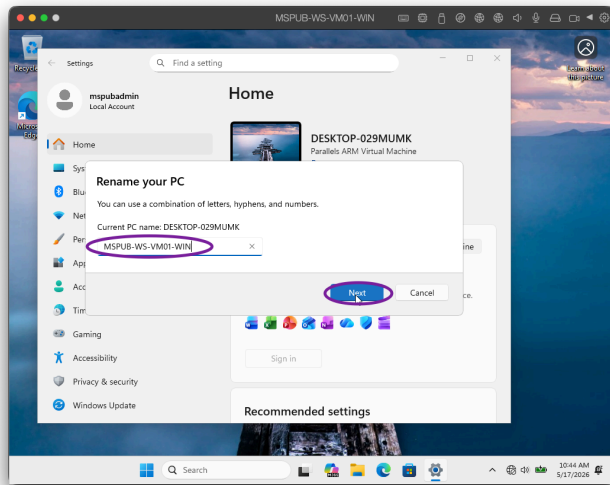
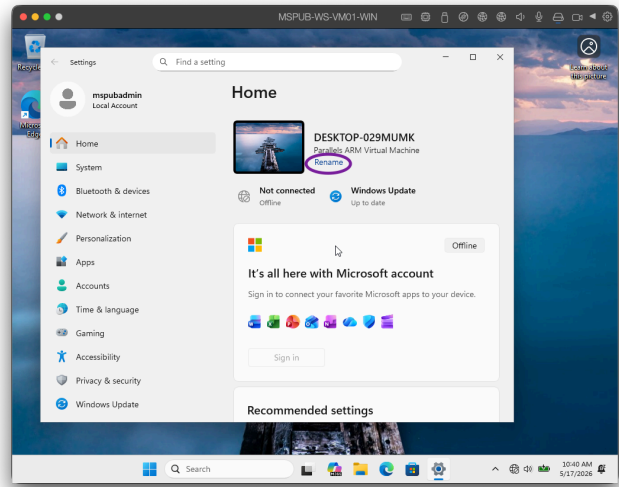
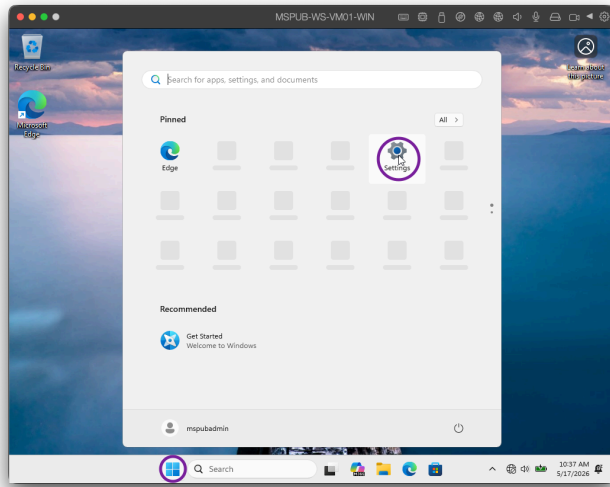


6. Once it's completed creating the Local Account, deselect everything on the privacy settings windows and click "Accept."

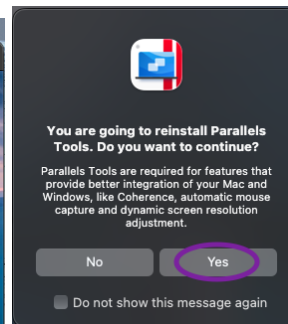
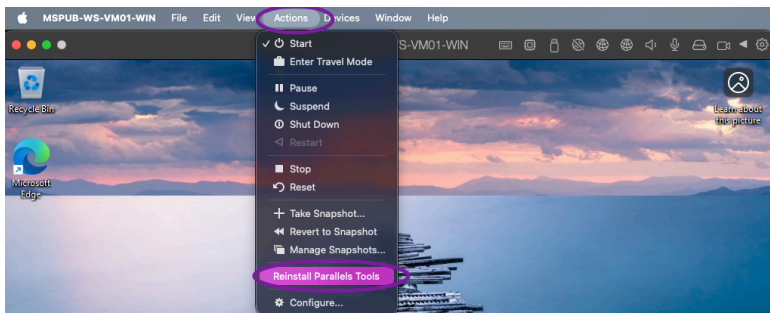


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

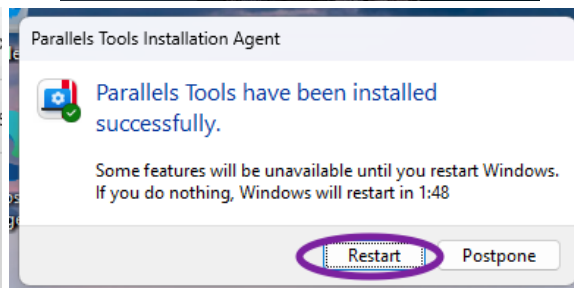
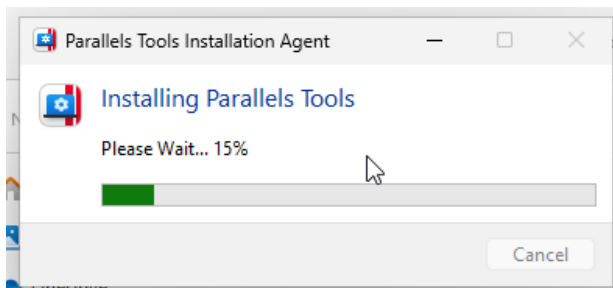
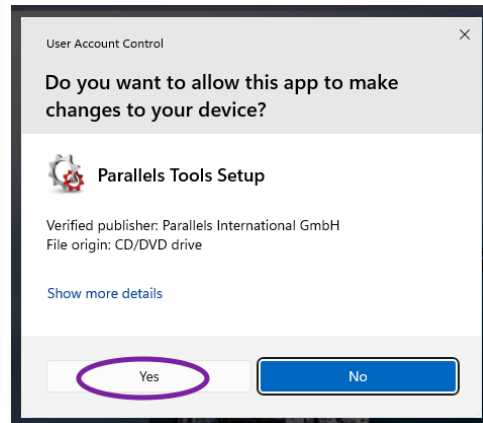
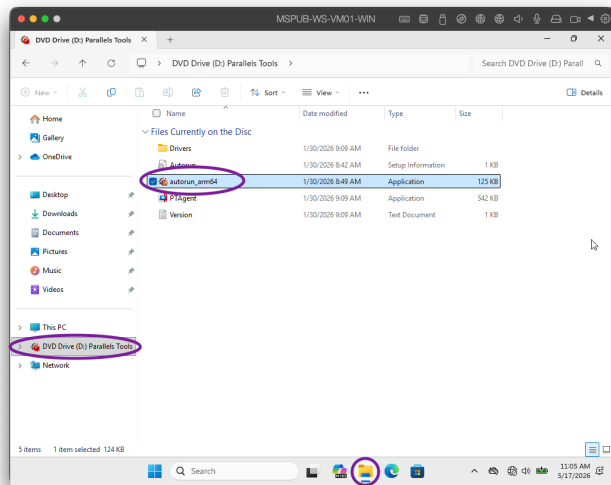
7. The Windows 11 Desktop will be displayed. Since the computer name was not entered during the OOB, this can be changed by clicking the “Windows charm” on the taskbar and clicking “Settings.” From the “Home” section click “Rename.” Name the VM “MSPUB-WS-VM01-WIN” and click “Next.” Click “Restart later.” The VM will be restarted after Parallels Tools is installed. Close the Settings window by clicking the “X” in the upper right corner.



8. Parallels Tools are a set of Virtual Machine drivers that enables features of the Parallels Hypervisor. To install: on the hosts menu bar click on “Actions.” Select “Reinstall Parallels Tools.” Click “Yes” to confirm Parallels Tools to be installed. The Parallels Tools installation media will be mounted to the virtualize CD/DVD ROM drive. Open “File Explorer” from the Taskbar and click “DVD Drive (D:) Parallels Tools” on the left Navigation pane. Double-click “autorun_arm64.” Click “Yes” on the User Account Control (UAC) dialog to allow the installation. Parallels Tools will begin to install the drivers onto the virtual machine. Once Parallels Tools has finished installing the VM will need to be restarted. Click “Restart.”



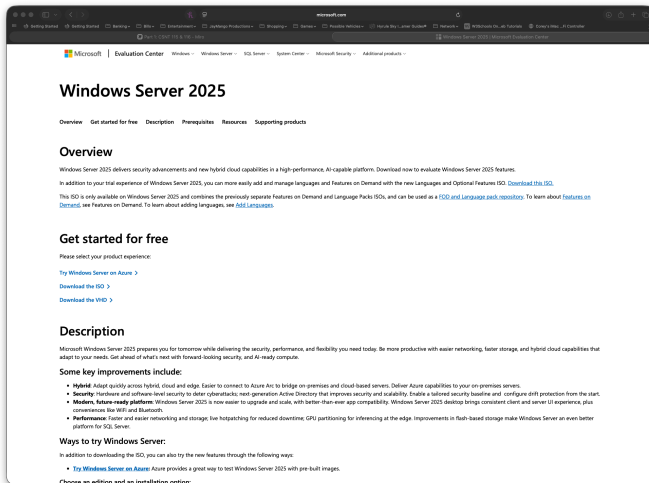
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



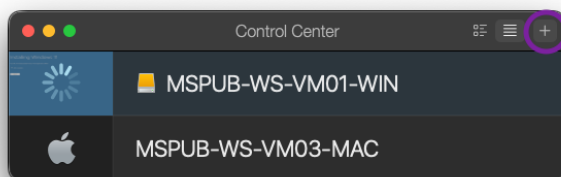
Windows Server 2025 Virtual Machine

Before creating Windows Server 2025 virtual machine it is important to know the minimum system requirements for the operating system. These can be found on Microsoft website, <https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements?tabs=cpu&pivots=windows-server-2025>. The minimum requirements are: 1.4 GHz 64-bit processor, 4 gigabytes of RAM, and 32 GB of storage.

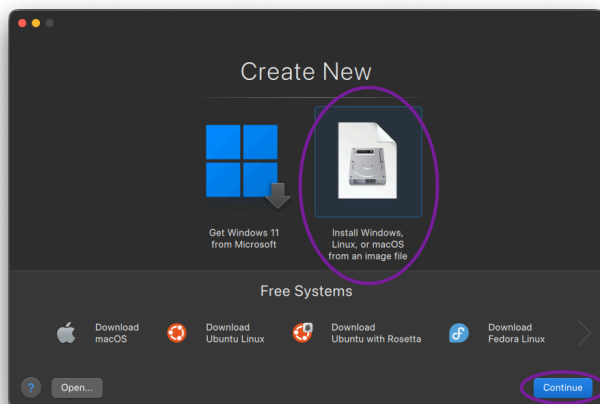
1. Download a copy of Windows Server 2025 from Microsoft's website, <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2025>.



2. In Parallels Control Center click the “+” button in the upper right corner to create a new virtual machine.

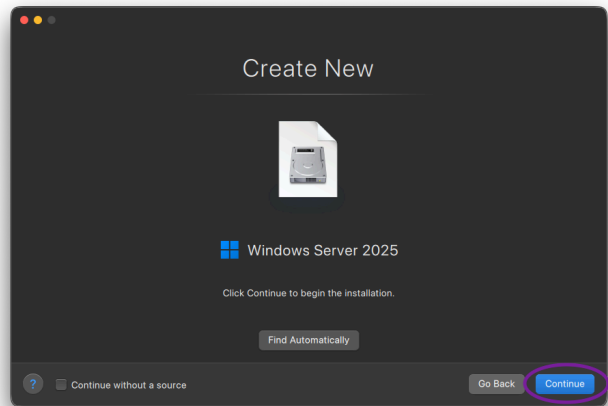
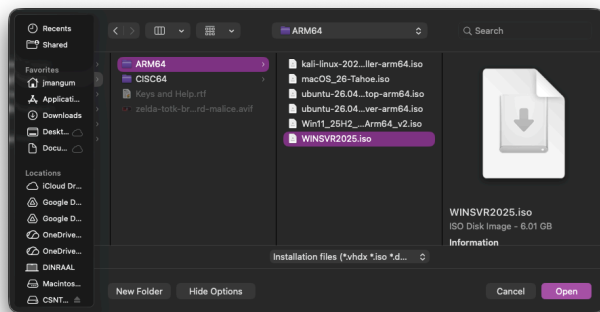
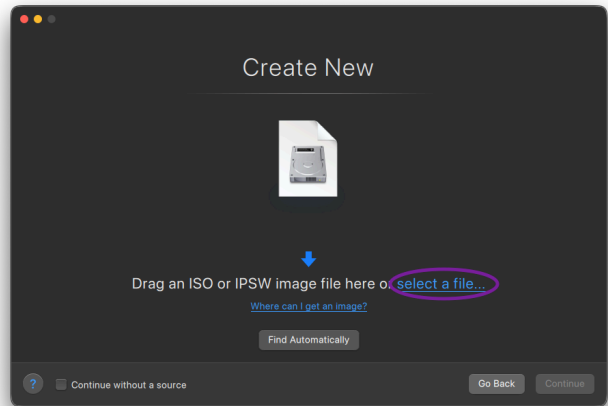
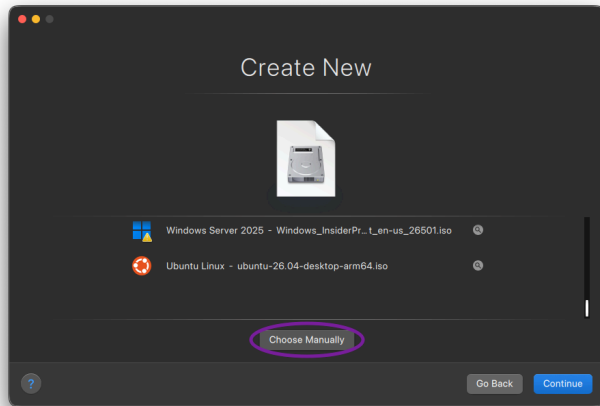


3. Click on “Install Windows, Linux, or macOS from an image file.” Click “Continue”

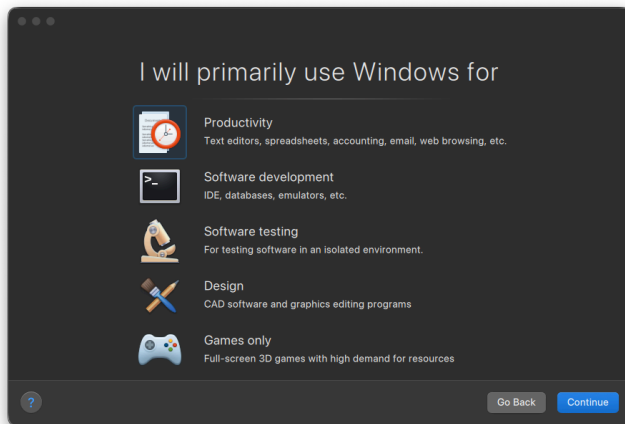


4. Click the “Choose Manually” button. Click “select a file...” Navigate and select the Windows Server 2025 ISO file, then click “Open.” Parallels will automatically recognize the operating system. Click “Continue.”

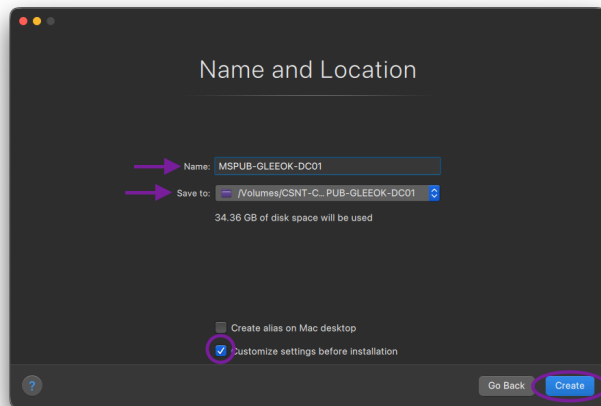
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



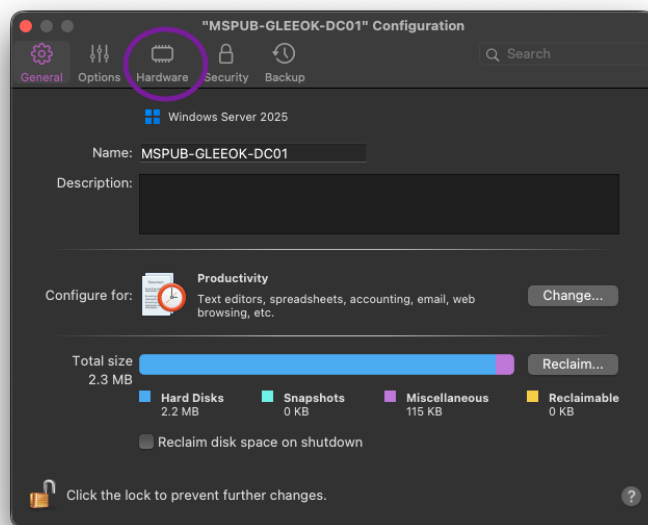
5. You can select what the VM will be used for. For this lab accept the default, “Productivity” and click continue.



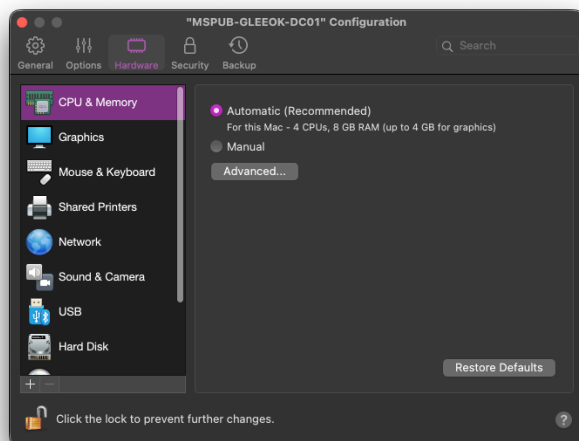
6. Name the new virtual machine “MSPUB-GLEEOK-DC01” and choose a location to save the VM. Select “Customize settings before installation.” Click “Create.”



7. On the “MSPUB-GLEEOK-DC01” Configuration window click on “Hardware” in the toolbar at the top.

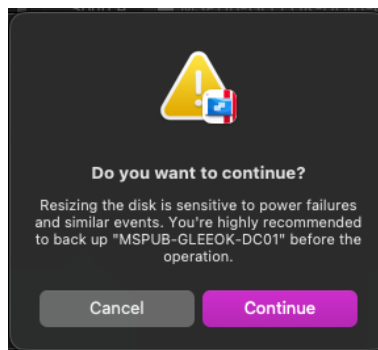
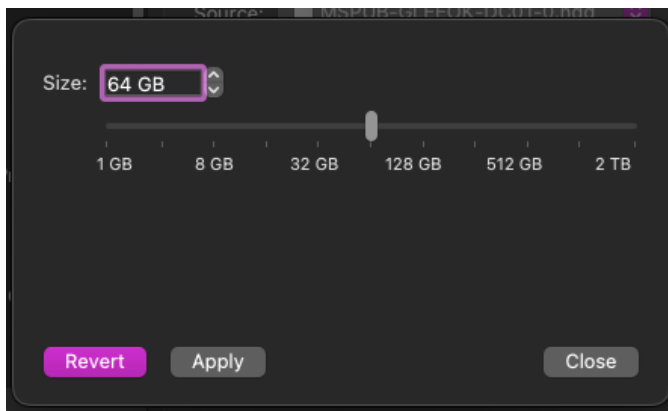
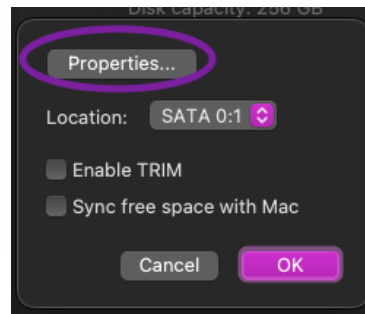
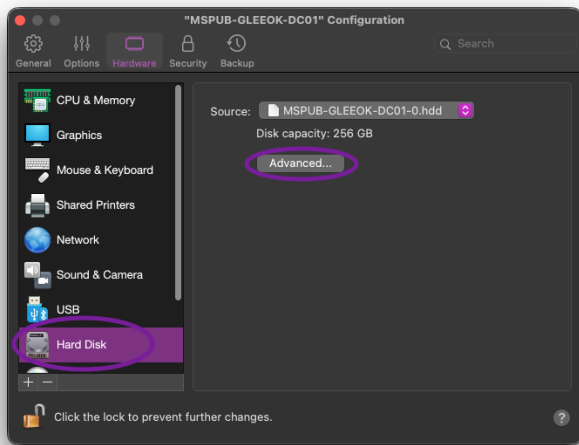


8. Leave the defaults for “CPU & Memory.”

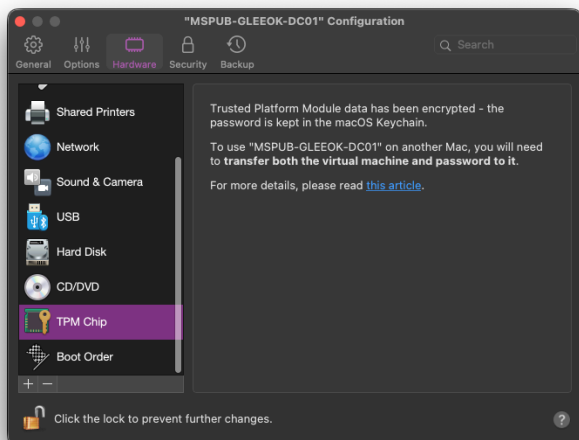


9. Click on “Hard Disk” in the “MSPUB-WS-VM01-WIN” Configuration window and click on “Advanced...” Click “Properties...” on the popup window. Reduce the size to “64 GB” and click “Apply” then “Close.” Click “Continue” in the warning popup window. Close the “Size” popup window. Click “OK” on the “Properties” window.

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

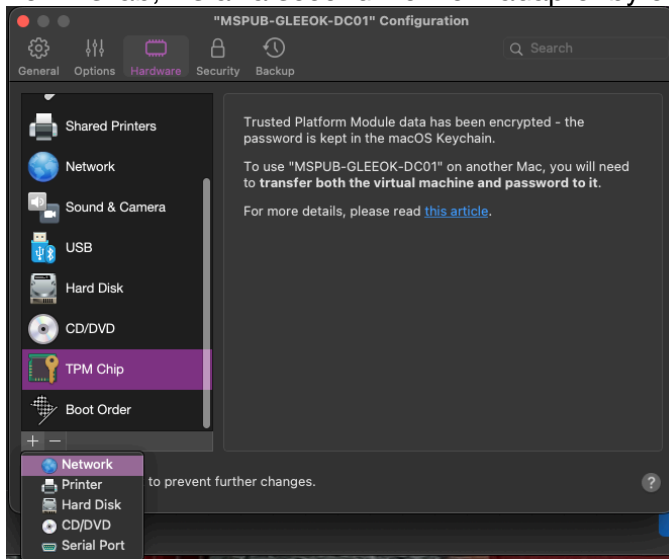


10. Scroll down the hardware list to ensure there is a TPM Chip installed.

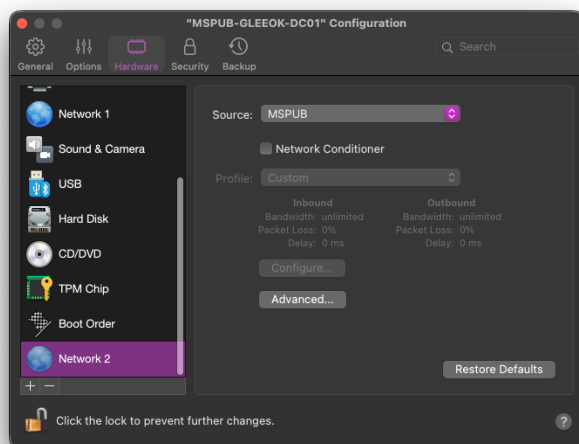


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

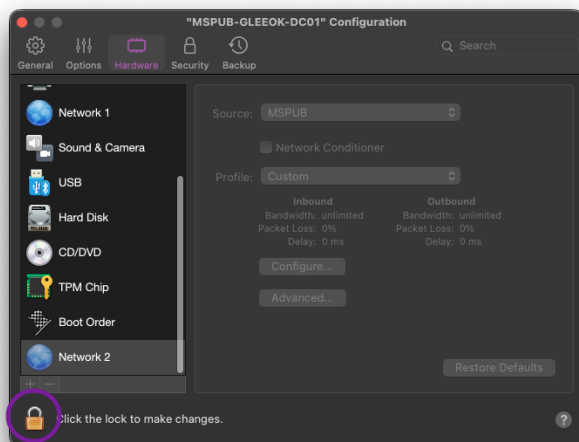
11. For this lab, install a second Network adapter by clicking the plus in the lower left and select “Network.”



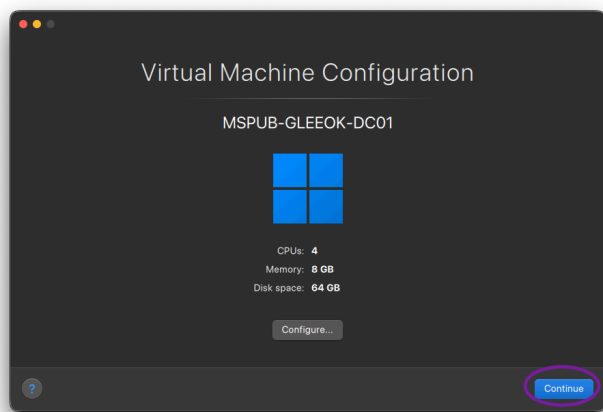
12. Configure Network 2 with the predefined source “MSPUB” in dropdown menu.



13. Click the “Lock” icon in the lower left to prevent further changes. Close the “MSPUB-WS-VM01-WIN” Configuration window, by clicking the red dot in the upper left corner. You may be required to authenticate these changes with your password or finger print.

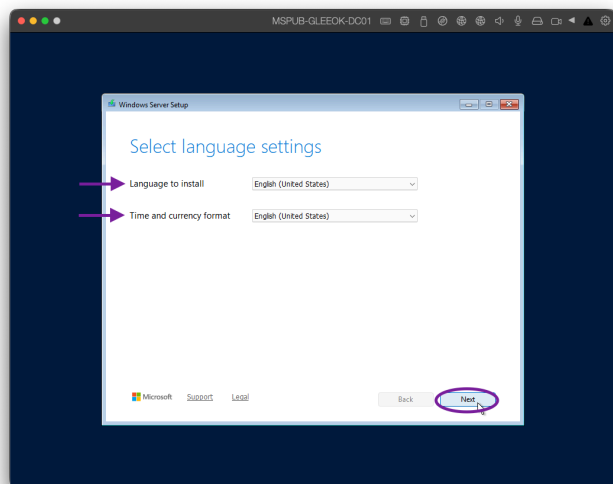


14. Click “Continue” on the Virtual Machine Configuration screen.

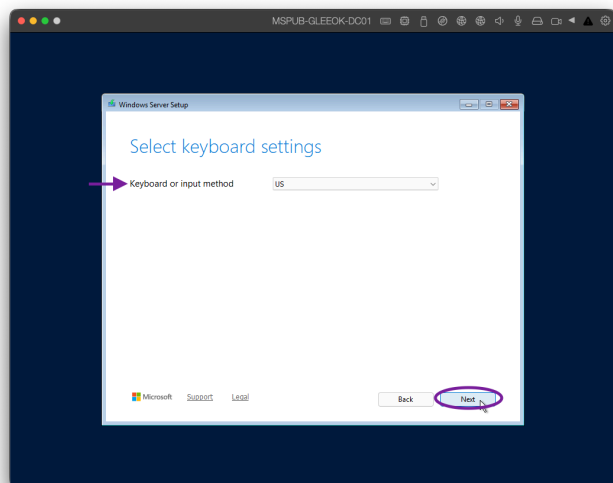


Windows Server Installation & Setup

1. The VM will automatically start. The Windows Server Setup will be displayed. Select a Language and Time and Currency Format to install from the drop down, in this case “English (United States)” is selected for both. Click “Next.”

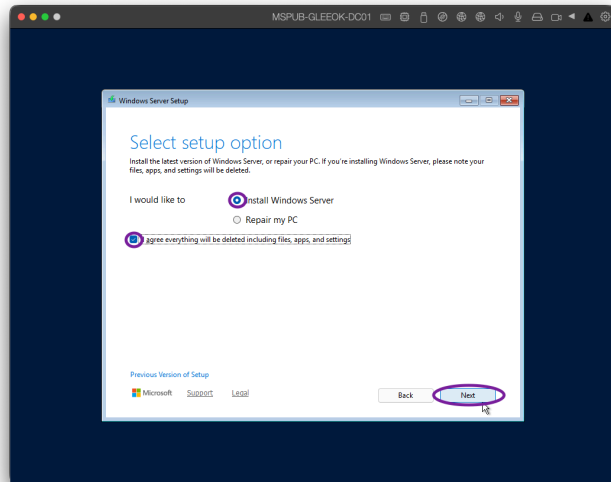


2. Select a Keyboard or input method from the drop down menu. In this case “US” is selected. Click “Next.”

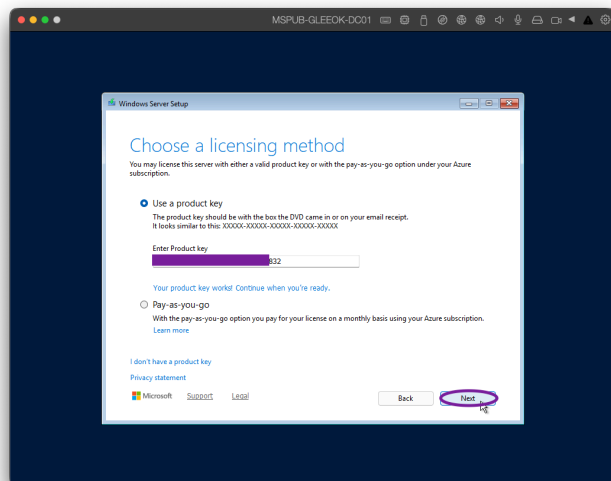


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

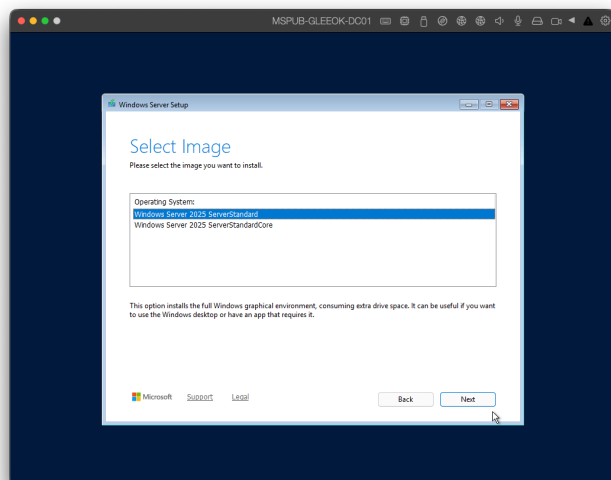
3. Select “Install Windows Server.” Select “I agree everything will be deleted including files, apps, and settings.” Click “Next.”



4. Enter in a Windows Server Product Key or select “Pay-as-you-go.” In this case an Evaluation Product Key was entered. Click “Next.”

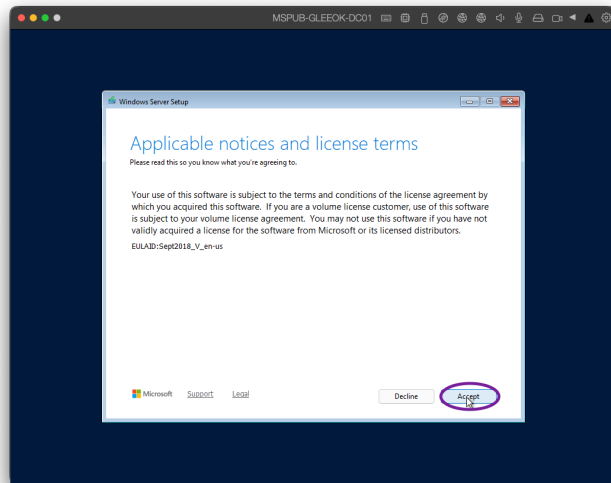


5. Select an Image from the list. In this case “Windows Server 2025 ServerStandard” was selected. Click “Next.”

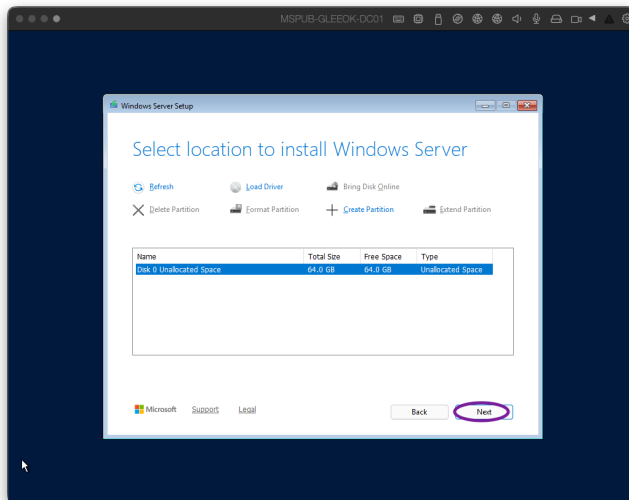


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

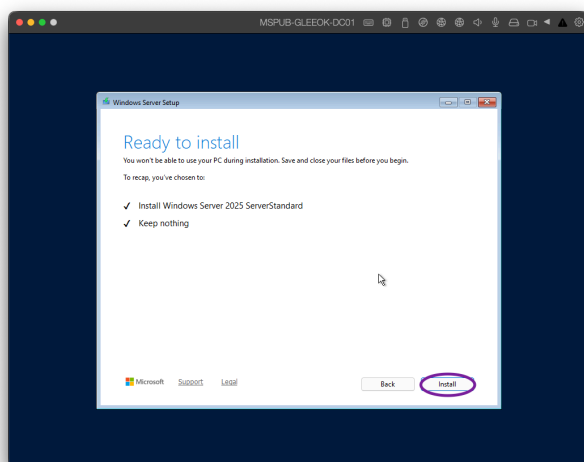
6. Read the Applicable notices and license terms the click “Accept”



7. Select a disk for the operating system to be installed on. Click “Next.”

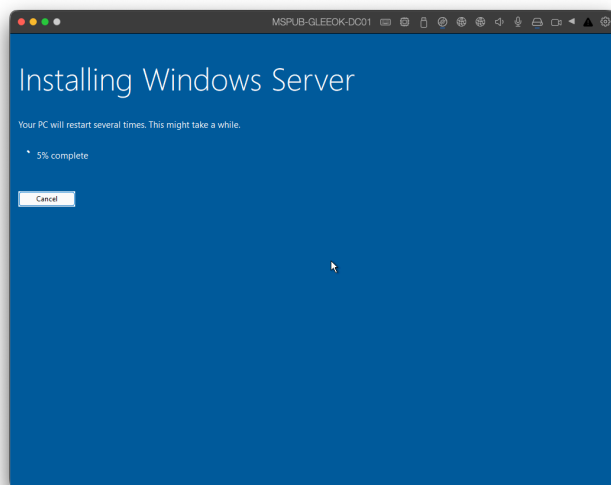


8. Click “Install.”



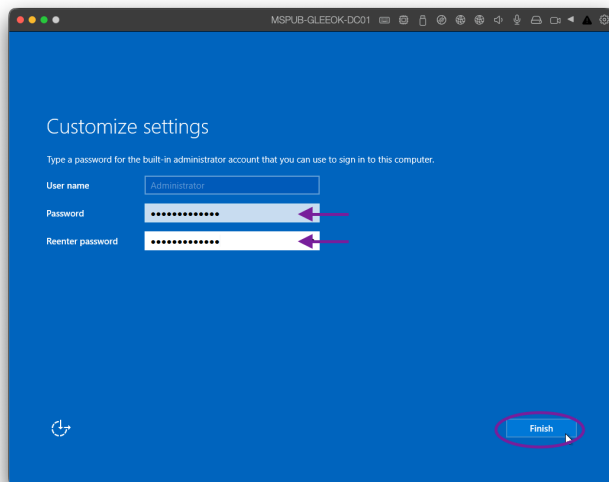
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

9. Windows Server will now be installed. This may take 15 or more minutes to complete.

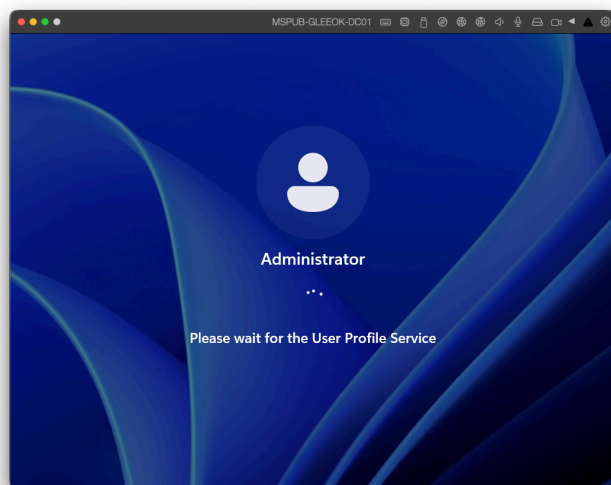


10. Once Windows Server 2025 has finished installing you will be required to create the Administrator account password. Type the following, then click “Finish”:

- Password: **CSNT253_2026#**
- Reenter Password: **CSNT253_2026#**

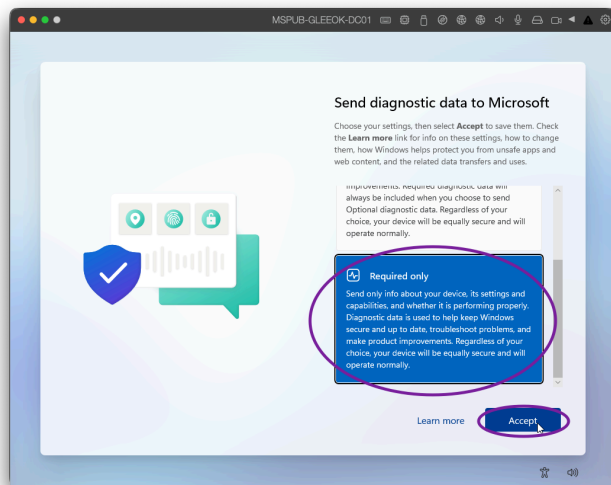


11. The VM will automatically restart. Press CTRL+ALT+Delete on the keyboard and sign into the Administrator account using the password “CSNT253_2026#” and pressing enter.

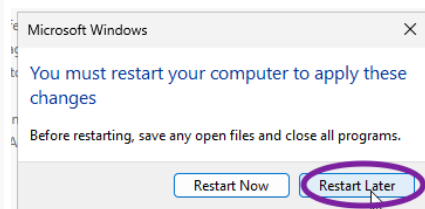
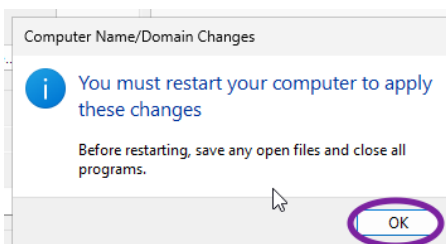
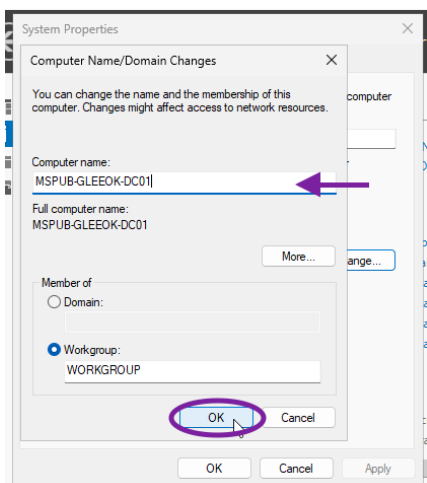
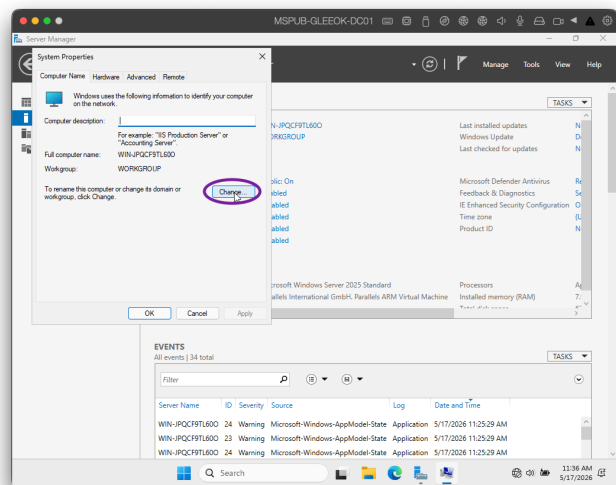
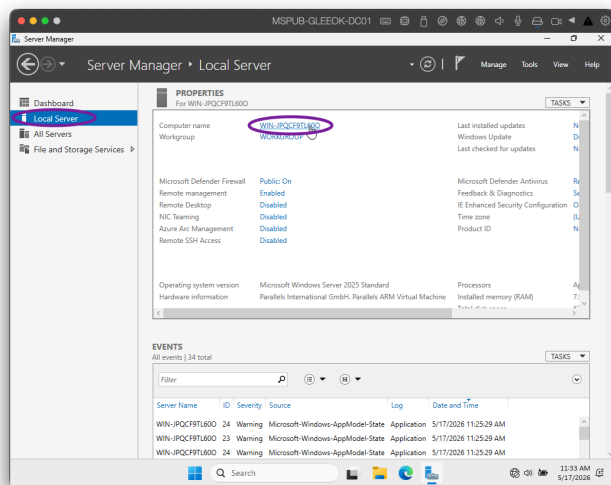


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

12. On the Send diagnostic data to Microsoft screen scroll down and click “Required only.” Click “Accept.”

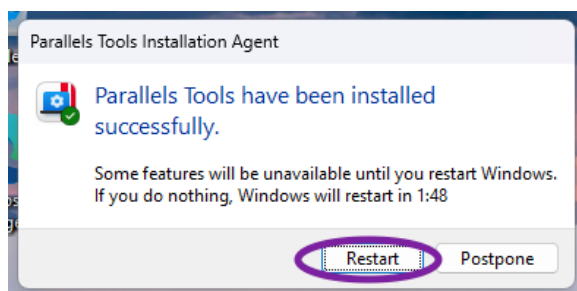
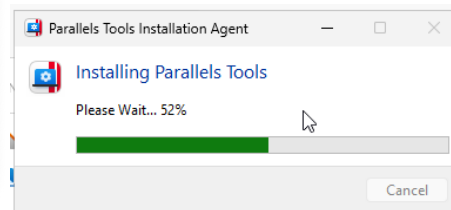
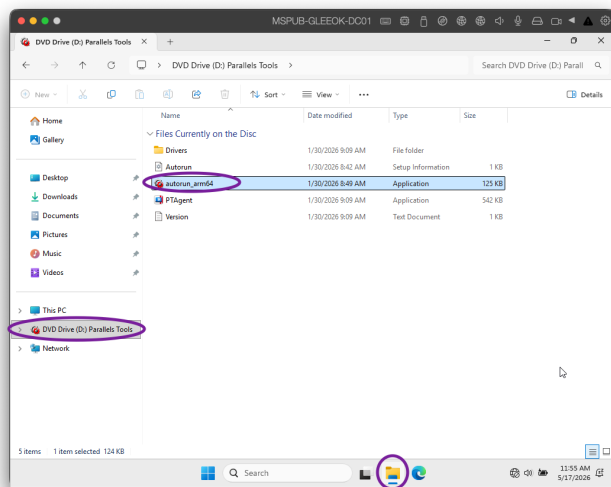
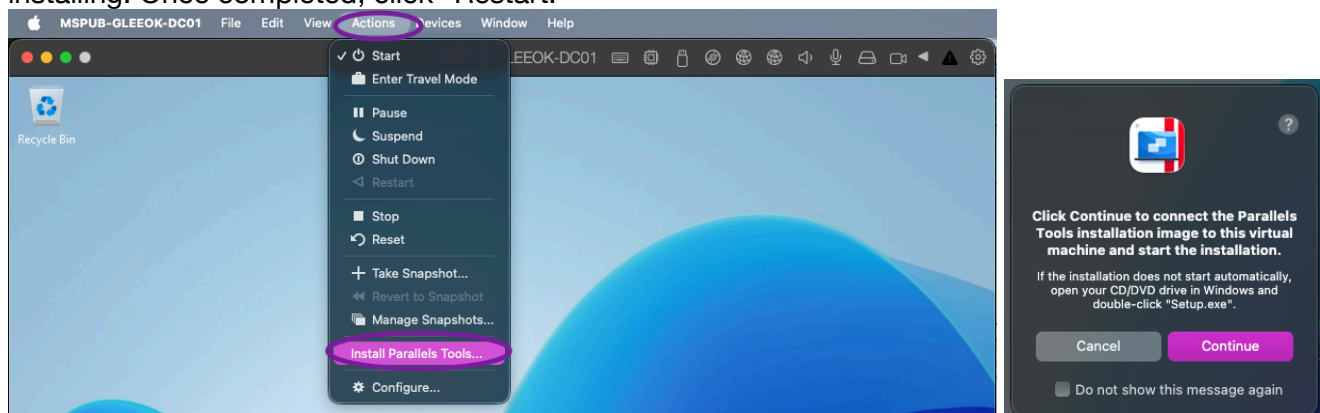


13. Close the “Try Windows Admin Center and Azure Arc today” window. This server will need to be renamed from the default that was set during the Windows Server installation. On the Server Manager click “Local Server” on the left pane. Click on the randomly generated computer name hyper link. Click “Change...” in the System Properties window. In the Computer name field and type “MSPUB-GLEEOK-DC01.” Leave the member of settings as default. Click “OK.” Click “OK” in the Computer Name/Domain Changes dialog box. Click “Close” on the System Properties window. Click “Restart Later.” The VM will be restarted after installing Parallels Tools. Close Server Manager by clicking the “X” in the upper right corner.



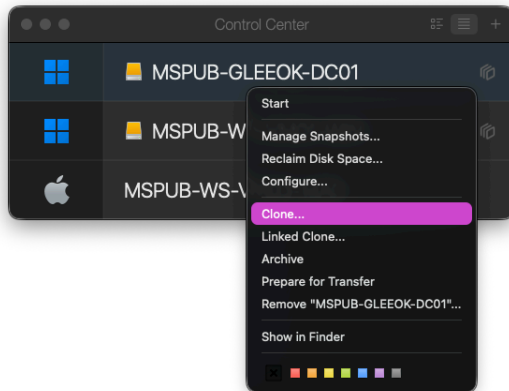
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

14. Parallels Tools is a set of virtual machine drivers for the system. To install Parallels Tools, from the host machine's menu bar click "Actions" and select "Install Parallels Tools..." Click "Continue" to mount the Parallels Tools installation media to the VM. Open "File Explorer" from the taskbar. Click "DVD Drive (D:) Parallels Tools" on the left navigation pane. Double-click "autorun_arm64." Parallels Tools will begin installing. Once completed, click "Restart."

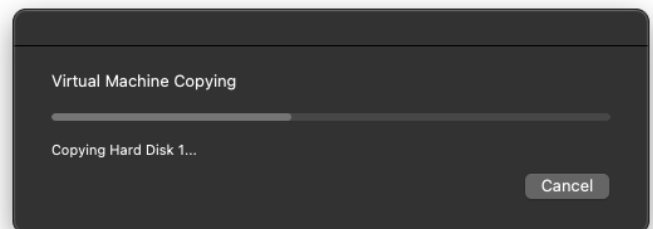
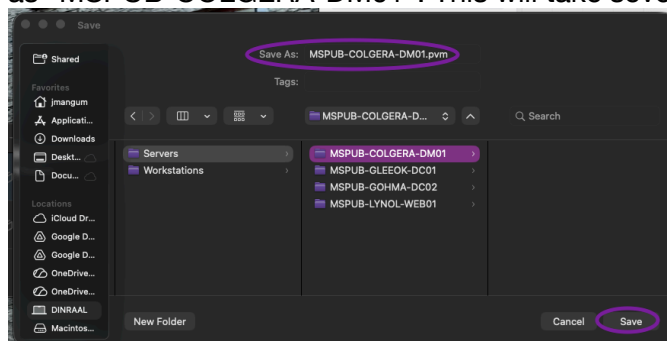


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

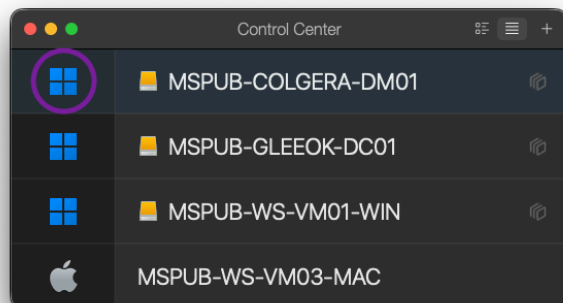
15. This VM will be cloned to create a second Windows Server 2025 virtual machine. From Parallels Control Center right click “MSPUB-GLEEOK-DC01” and select “Clone...”



16. In the Save window Save the cloned VM “MSPUB-COLGERA-DM01.pvm” and choose a location to save the cloned VM. Click “Save.” The Virtual Machine will begin cloning “MSPUB-GLEEOK-DC01” and save it as “MSPUB-COLGERA-DM01”. This will take several minutes.

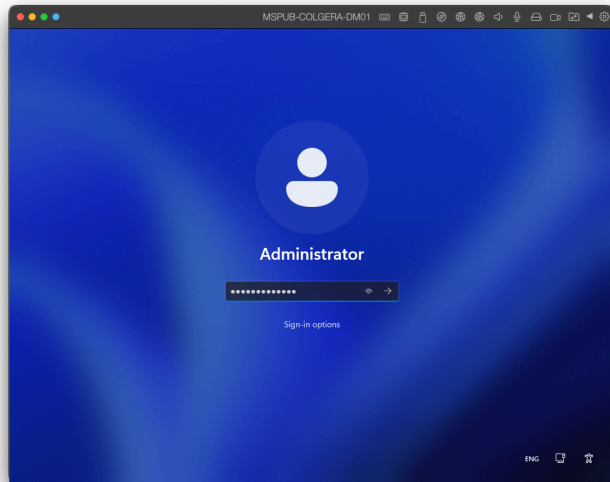


17. Once the cloning has been completed it will show in the Parallels Control Center. Start “MSPUB-COLGERA-DM01” by clicking the Windows Logo next to name.

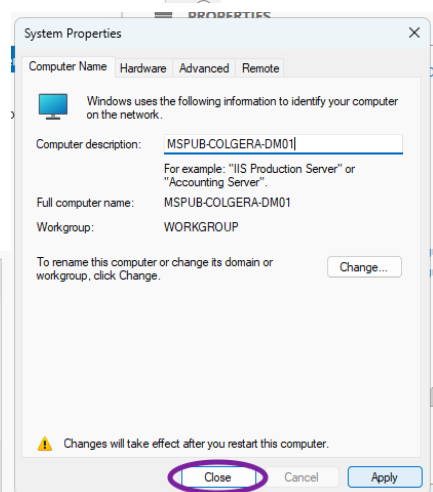
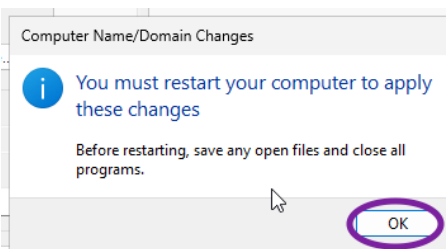
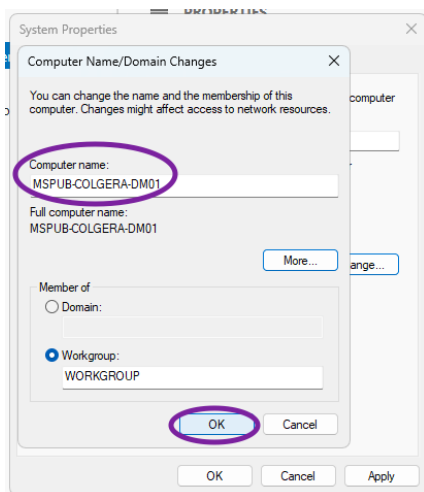
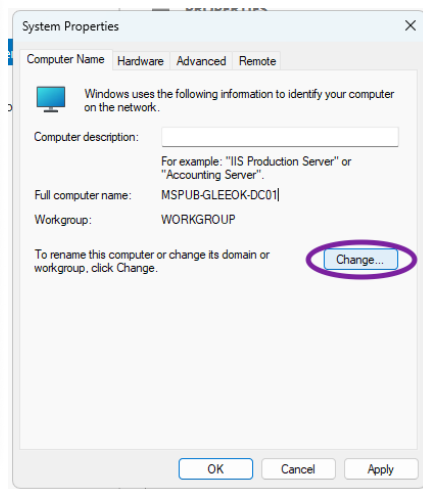
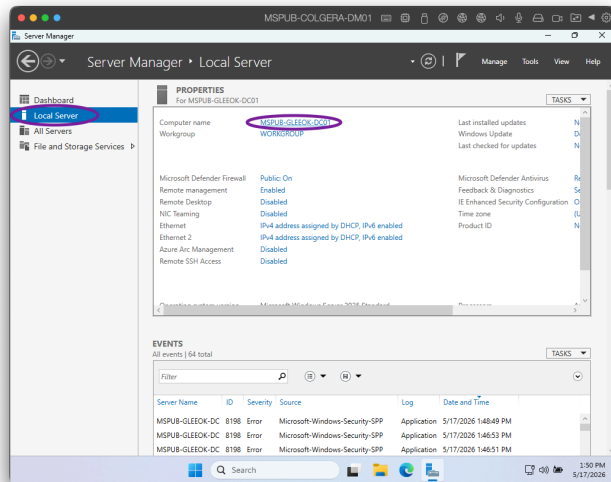


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

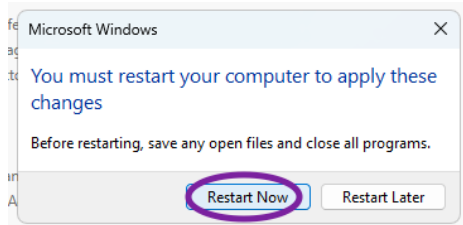
18. Login by pressing CTRL-ALT-DEL on the keyboard and type in the Administrator password, "CSNT253_2026#".



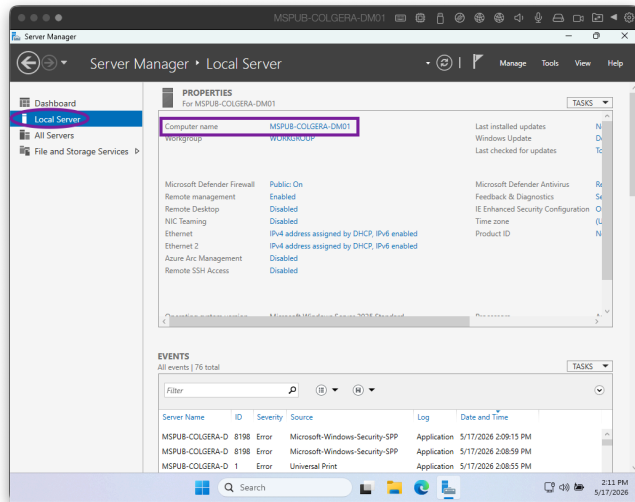
19. This machine needs to be renamed to reflect the virtual machine file. On Server Manager click "Local Server" on the left pane. Click the Computer name: "MSPUB-GLEEK-DC01." Click "Change..." in the System Properties window. In the Computer Name/Domain Changes window change the Computer name to "MSPUB-COLGERA-DM01." Leave the Member of settings as their defaults and click "OK." Click "OK" on the Computer Name/Domain Changes dialog. Click "Close" on the System Properties window. Click "Restart Now" on the dialog box to restart the VM.



Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



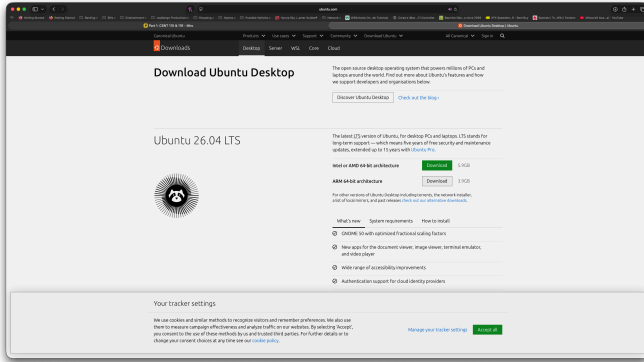
20. Once the VM restarted, login using the Administrator account credentials. Confirm the Computer name has been changed by clicking “Local Server” in server manager.



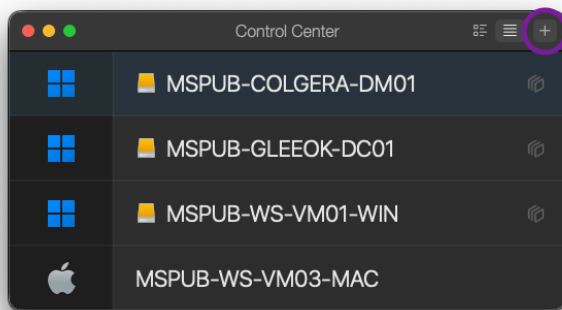
Ubuntu Desktop 26.04 LTE Virtual Machine

Before creating a new Ubuntu Desktop virtual machine it is important to know the minimum system requirements so that the Virtual Machine settings can be set accurately for the operating system. The minimum requirements can be found on Canonical's website, <https://ubuntu.com/download/desktop>. The systems requirements for Ubuntu Desktop 26.04 LTE are: 2 GHz dual-core processor, 6 gigabytes of RAM, and at least 25 GB of storage space. This virtual machine will be created using Parallels on macOS.

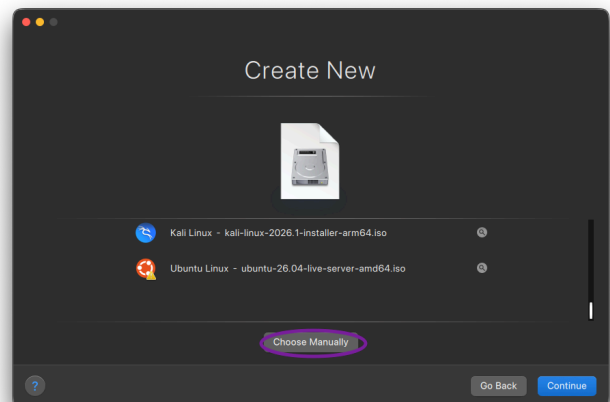
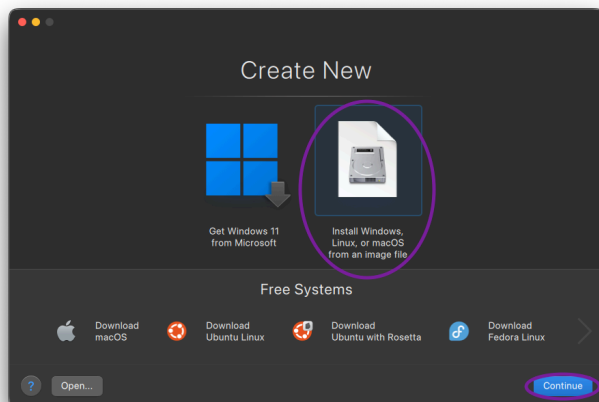
1. Download the Ubuntu Desktop 26.04 LTS ARM 64 ISO file from Canonical's website, <https://ubuntu.com/download/desktop>.

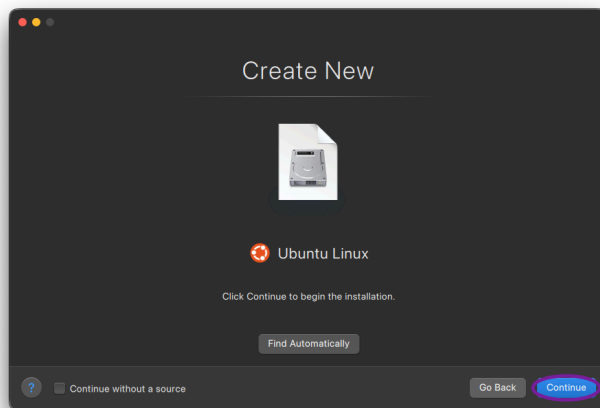
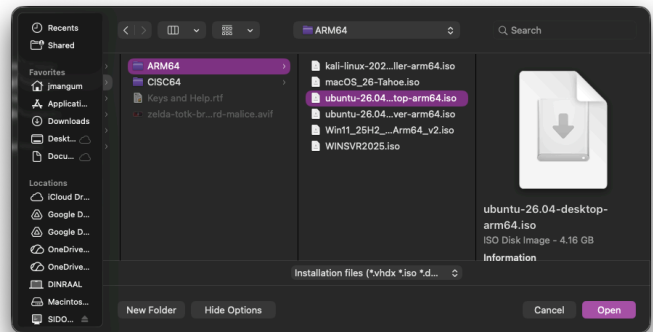
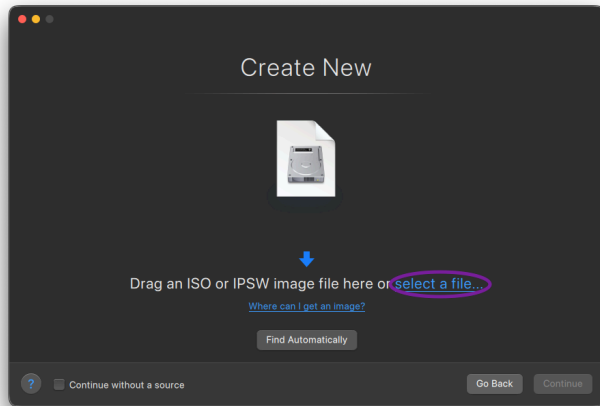


2. On Parallels Control Center click the “+” button in the upper left to create a new VM.

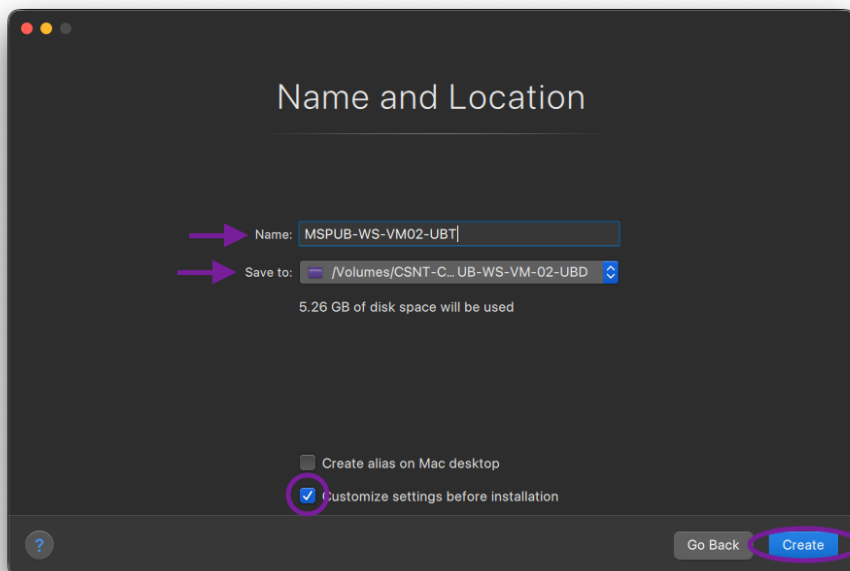


3. In the Create New window click on “Install Windows, Linux, or macOS from an image file.” Click “Continue.” Click the “Choose Manually” button. Click the “select a file...” hyperlink. Navigate to the Ubuntu Desktop 26.04 LTE ARM64 ISO file and click “Open.” Parallels will detect the operating system automatically. Click “Continue.”

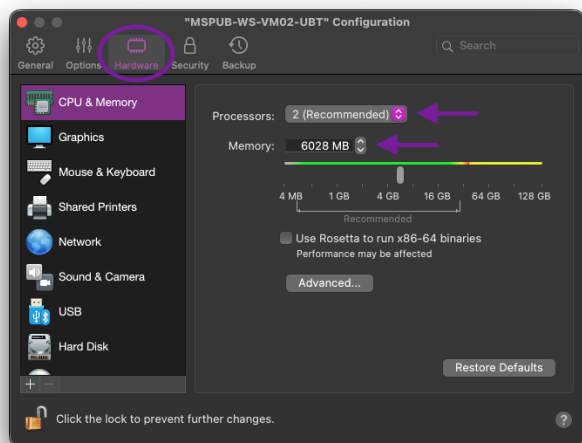




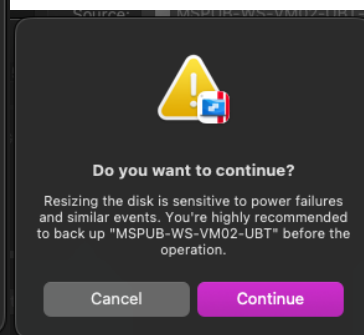
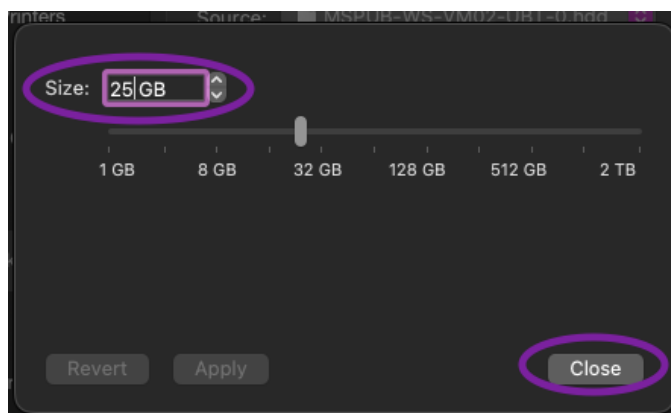
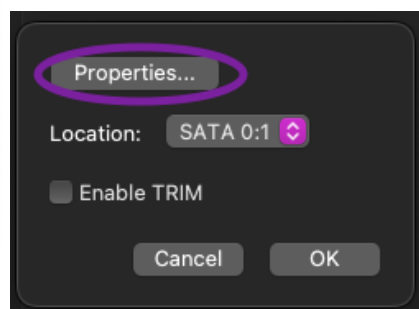
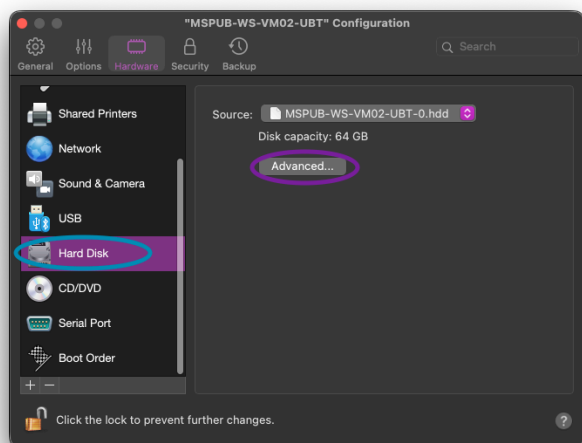
4. In the Name and Location window, Name the new VM “MSPUB-WS-VM02-UBT.” Choose a Save to location to save the VM. Select “Customize settings before installation.” Click “Create.”



5. In the “MSPUB-WS-VM02-UBT” Configuration window click on “Hardware” in the top toolbar, and select “CPU & Memory” on the left pane. Set Processes to “2” from the drop down menu and change the Memory to “6028” MB (~6GB).

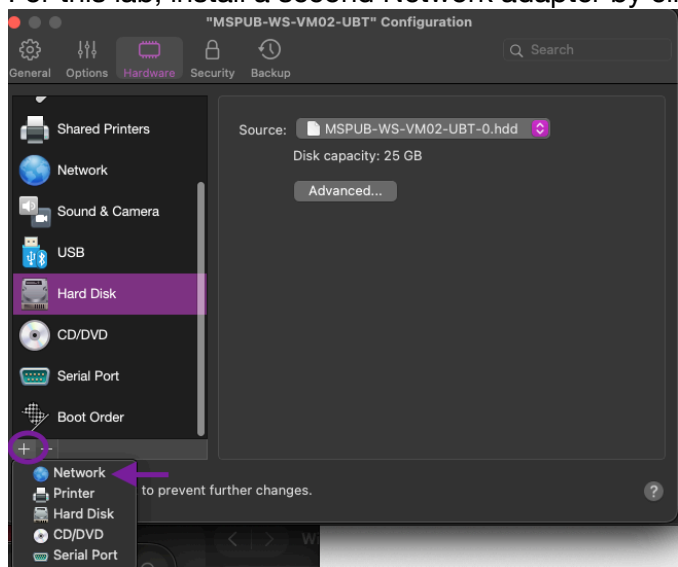


6. In the “MSPUB-WS-VM02-UBT” Configuration windows select Hard Disk on the left pane. Click the “Advanced...” button. Click “Properties...” in the popup window. Reduce the size to “25 GB” and click “Apply.” Click “Continue” on the Warning popup. Click “Close” on the Size window. Click “OK” on the properties window.

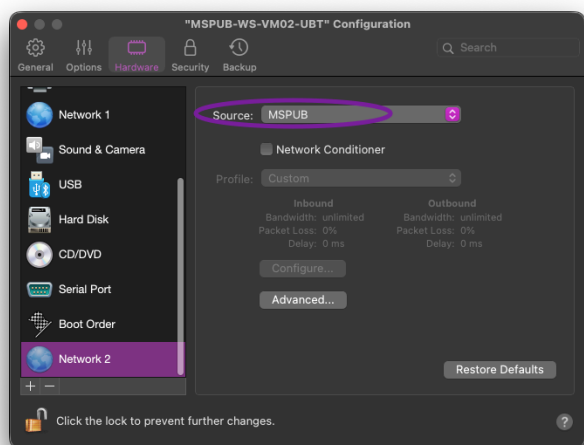


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

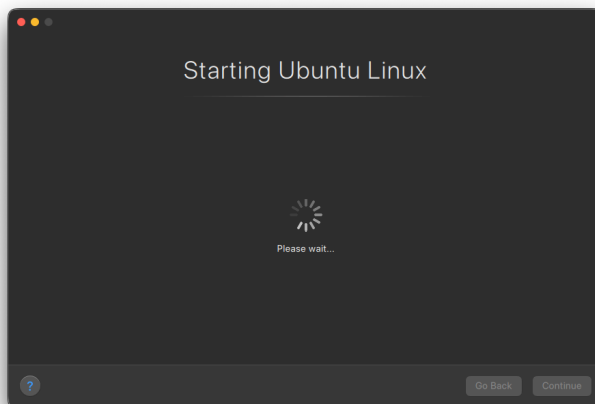
7. For this lab, install a second Network adapter by clicking the plus in the lower left and select “Network.”



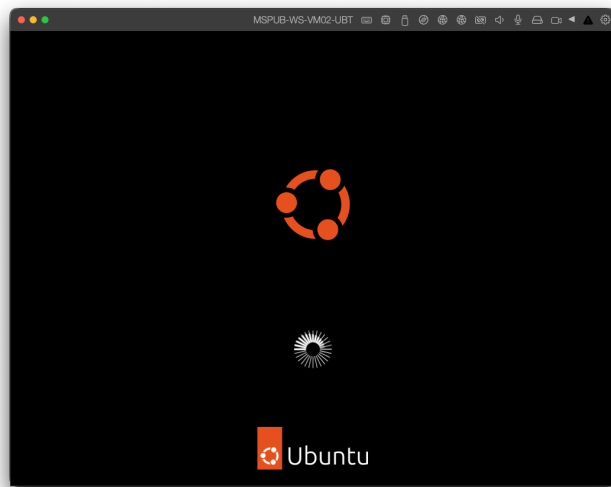
8. Configure Network 2 with the predefined source “MSPUB” in dropdown menu. Close the “MSPUB-WS-VM02-UBT” Configuration window.



9. Click “Continue” on the Virtual Machine Configuration window to create the Virtual Machine.

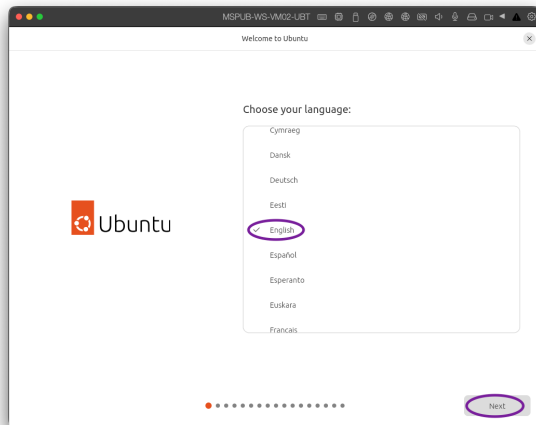


10. MSPUB-WS-VM02-UBT should automatically open and load the Ubuntu Desktop ISO.

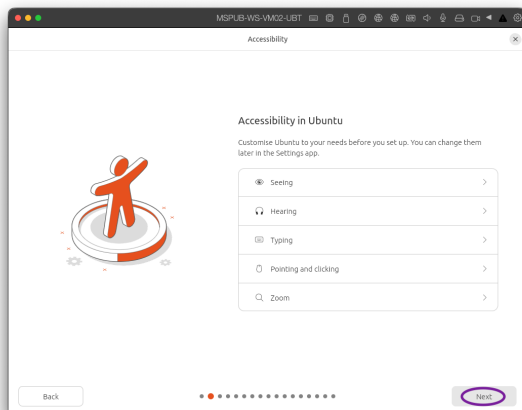


Ubuntu Desktop Installation & Setup Wizard

1. In the Ubuntu installer, choose your language, in this case “English” is selected. Click “Next.”

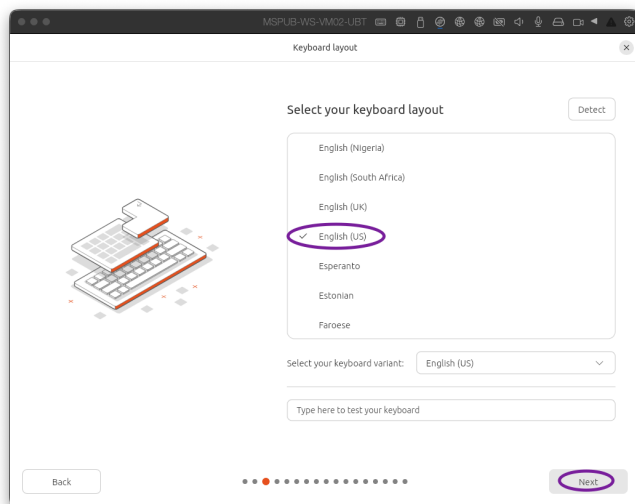


2. Ubuntu Desktop allows users to setup Accessibility settings automatically from the installer. For this lab skip this setup by clicking “Next.”

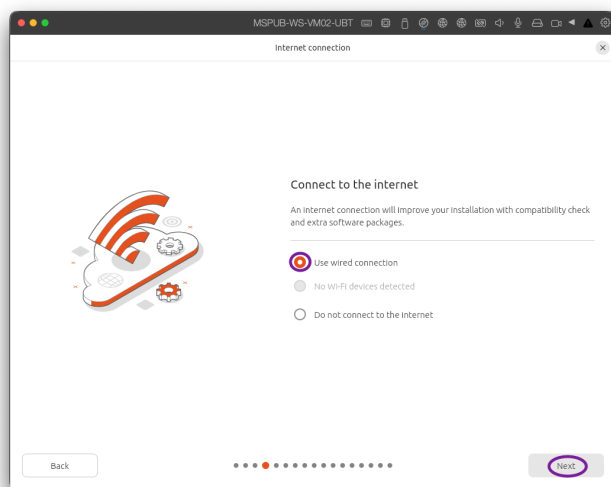


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

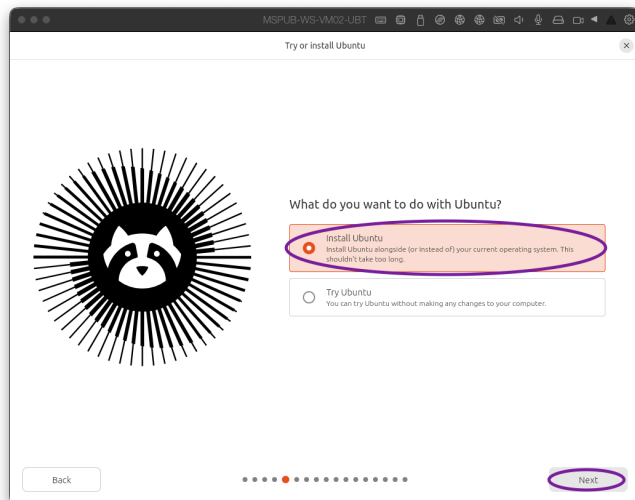
3. Select a keyboard layout, in this case “English (US)” has been selected. Click “Next.”



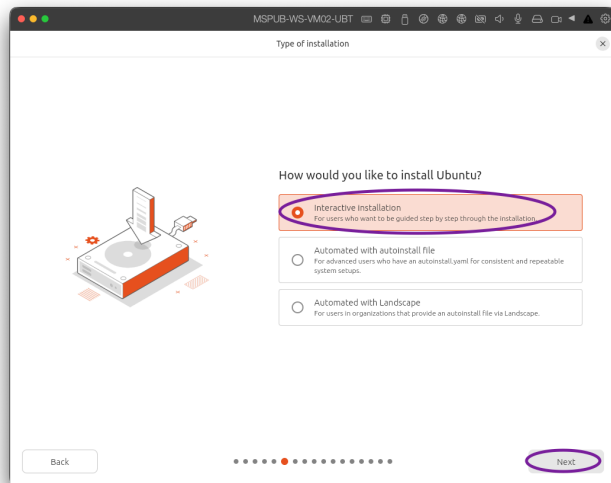
4. Accept the defaults for the Internet connection setup, by clicking “Next.”



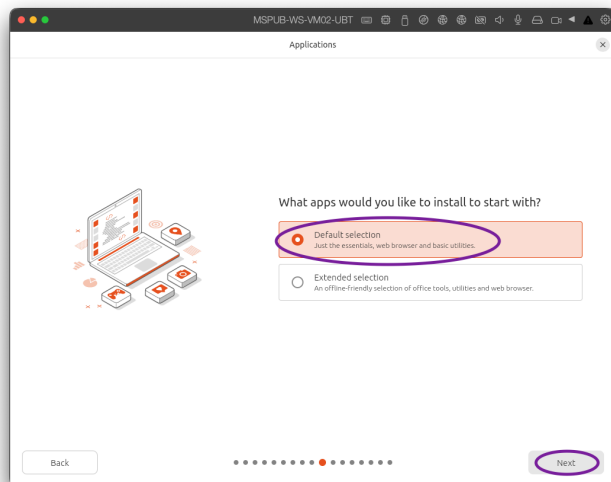
5. On the Try or install Ubuntu screen, select “Install Ubuntu” and click “Next.”



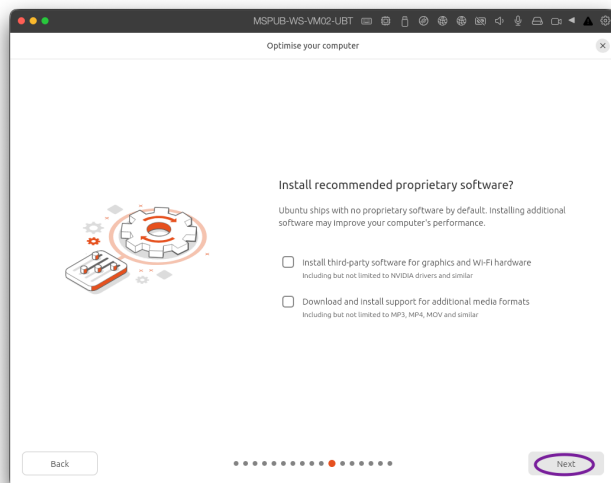
6. Ubuntu allows users to install a custom image if they have one. For this lab select “Interactive installation” and click “Next.”



7. Select the applications that will be installed. For this lab choose, “Default selection” and click “Next.”

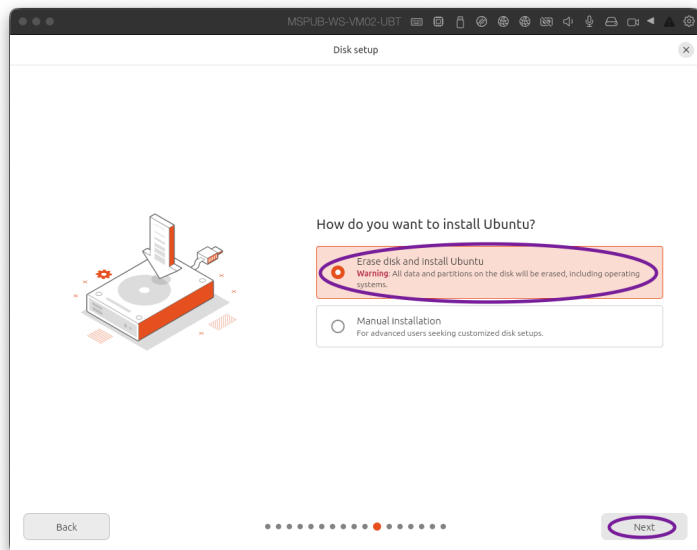


8. If this were being installed on actual hardware Ubuntu allows the installer to search the web for third party drives. As well as, if you need to install different media formats it can also automatically browse the web to install them. For this lab leave everything un-selected and click “Next.”

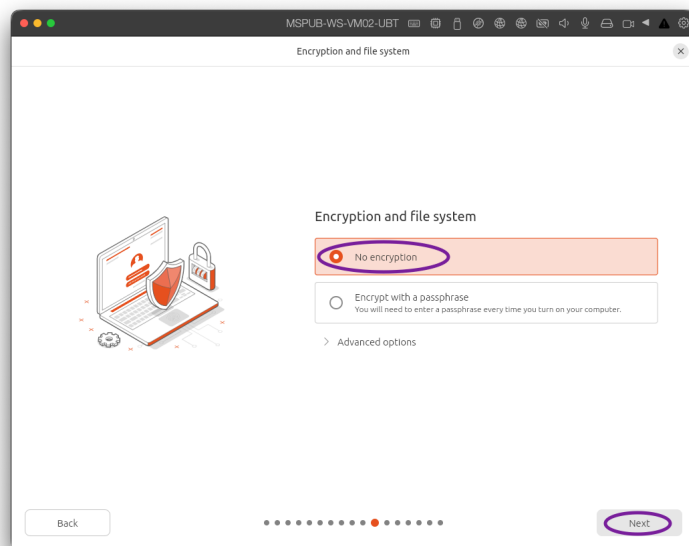


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

9. Since this is a new virtual machine, choose “Erase disk and Install Ubuntu.” For an advanced installation if you were going to dual boot a system you can choose Manual installation to set customized drive partitions. Click “Next.”



10. For now Encryption will be disabled. This will be setup in a later lab. Select “No encryption” and click “Next.”



11. In the “Create you account” window apply the following, then click “Next”:
- Your Name: **MSPUB Administrator**
 - Your Computer’s Name: **MSPUB-WS-VM02-UBT**
 - Your Username: **mspubadmin**
 - Password: **CSNT253_2026#**
 - Confirm Password: **CSNT253_2026#**

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Select “Require my password to log in”

The screenshot shows the 'Create your account' window in the Ubuntu installer. The window has a title bar with the text 'MSPUB-WS-VM02-UBT' and a close button. The main title is 'Create your account'. Below the title, there are five input fields, each with a label and a green checkmark indicating it is valid:

- Your Name:** MSPUB Administrator
- Your Computer's Name:** MSPUB-WS-VM02-UBT
- Your username:** mspubadmin
- Password:** CSNT253_2026# (with a 'Hide' button and 'Strong password' indicator)
- Confirm Password:** CSNT253_2026#

Below the input fields, there are two checkboxes:

- ☒ Require my password to log in
- ☐ Use Active Directory

At the bottom of the window, there is a 'Back' button on the left and a 'Next' button on the right, which is circled in purple. A progress bar with 12 dots is located at the bottom center, with the 12th dot being red.

12. Choose a city on the map for the timezone, in this case “Seattle (Washington, United States) has been selected).” Click “Next.”

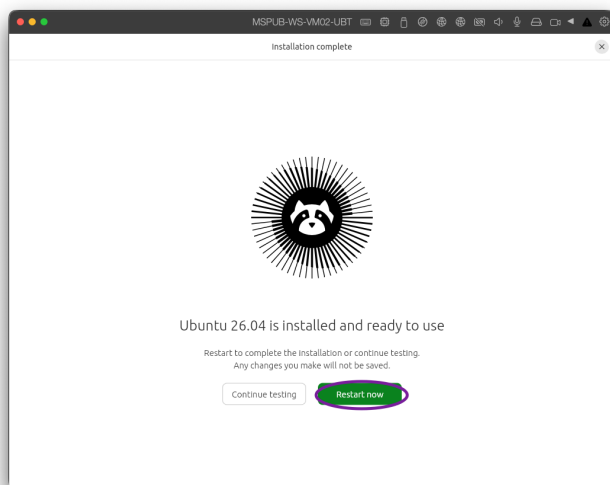
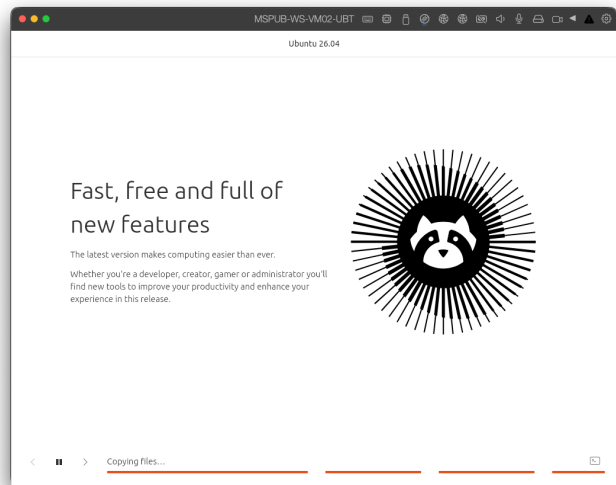
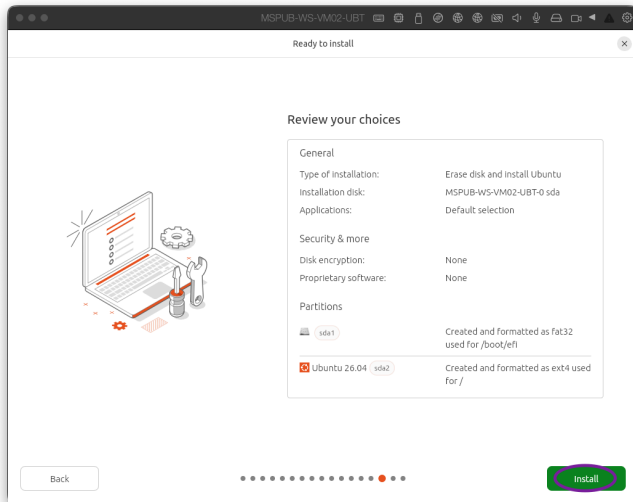
The screenshot shows the 'Select your timezone' window in the Ubuntu installer. The window has a title bar with the text 'MSPUB-WS-VM02-UBT' and a close button. The main title is 'Select your timezone'. Below the title, there are two input fields:

- Location:** Seattle (Washington, United States)
- Timezone:** America/Los Angeles

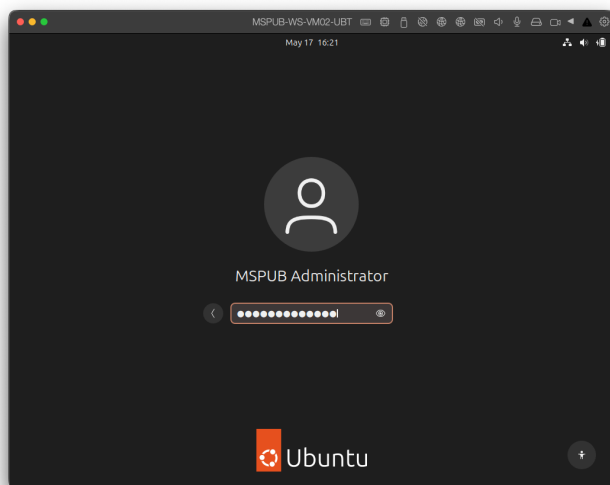
Below the input fields, there is a world map with a red pin indicating the selected location, Seattle (Washington, United States). At the bottom of the window, there is a 'Back' button on the left and a 'Next' button on the right, which is highlighted. A progress bar with 12 dots is located at the bottom center, with the 12th dot being red.

13. Review the settings on the “Ready to install” windows then click “Install.” Ubuntu 26.04 will begin to install. This may take 15 minutes or more to complete. Once the installer has completed, click “Restart now.”

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



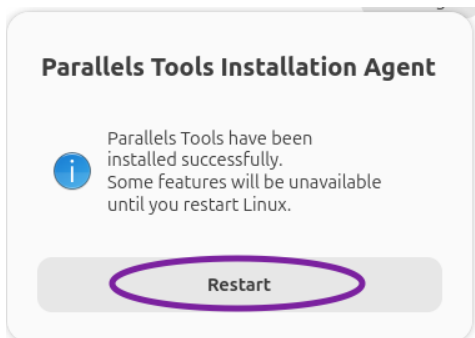
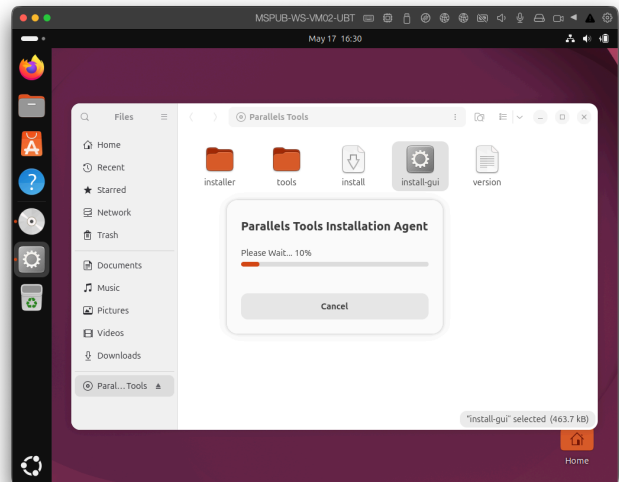
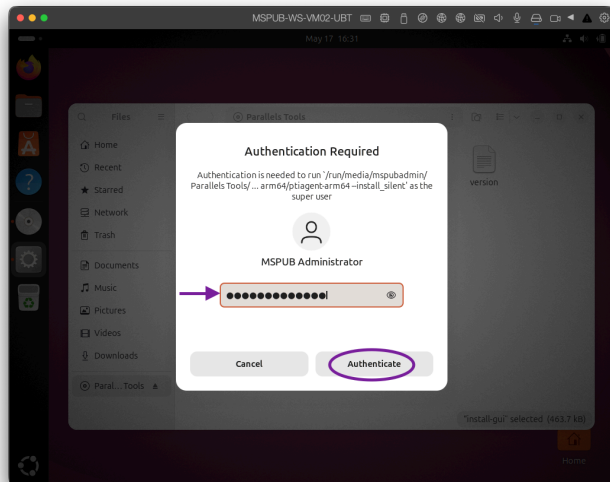
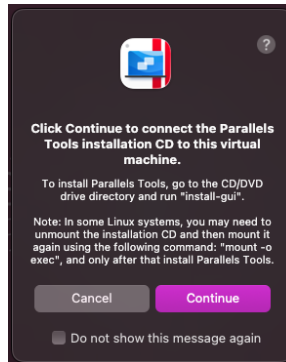
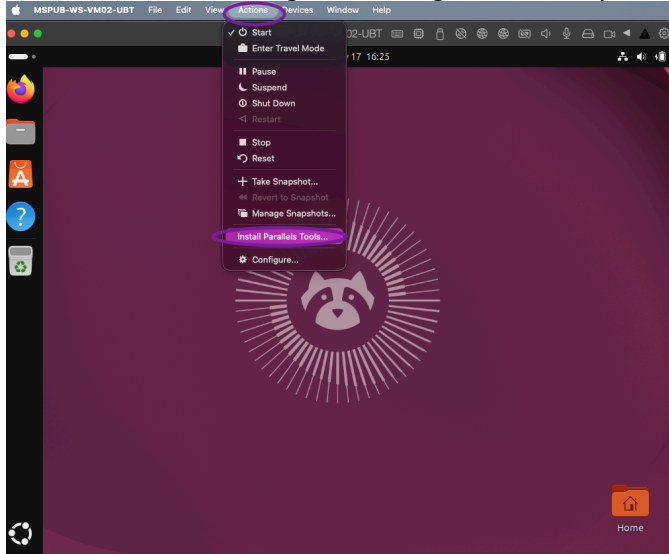
14. Once the VM reboots, login by clicking “MSPUB Administrator” and enter in the password “CSNT253_2026#”



15. Parallels Tools is a set of virtual machine drivers for the system. To install Parallels Tools, from the host machine’s menu bar click “Actions” and select “Install Parallels Tools...” Click “Continue” to mount the Parallels Tools installation media to the VM. Open the “Parallels Tools” disc on the left-side bar. Double-click “install-gui.” Authenticated with the MSPUB Administrator credentials and click “Authenticate.”

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

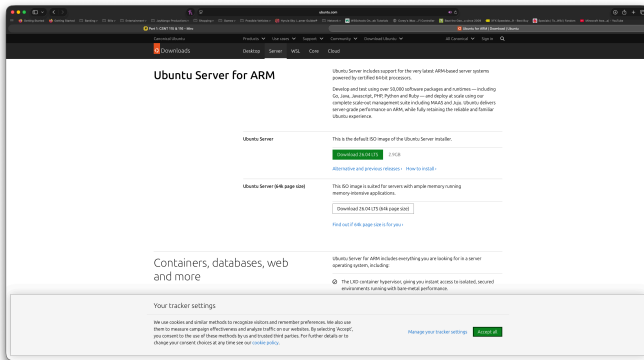
Parallels Tools will begin installing. Once completed, click “Restart.”



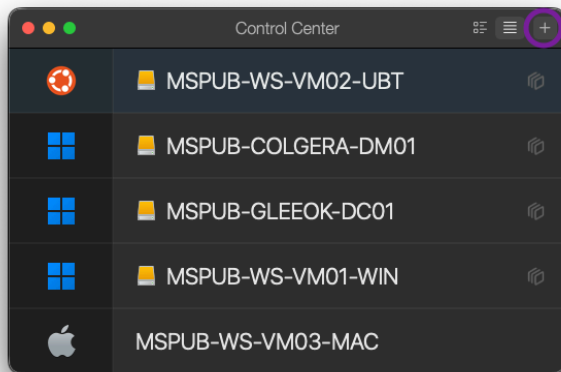
Ubuntu Server 26.04 LTE Virtual Machine

Before creating a new Ubuntu Server 26.04 LTE virtual machine it is important to know the minimum system requirements for the operating system. These can be found on Canonical's website, <https://ubuntu.com/download/server#system-requirements-tab-lts>. Ubuntu Server 26.04 LTE's minimum requirements are at least 1.5 gigabytes of memory and 5 gigabytes of storages.

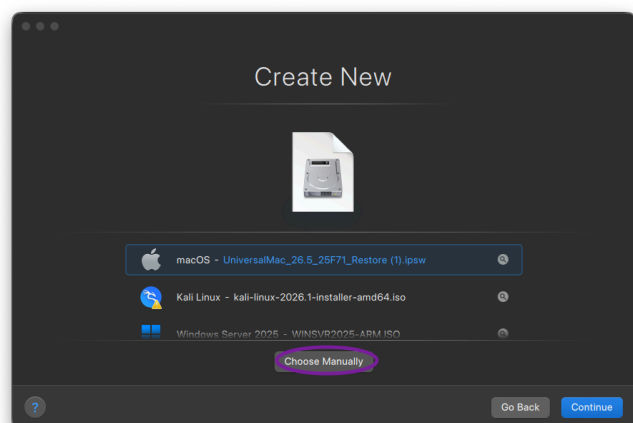
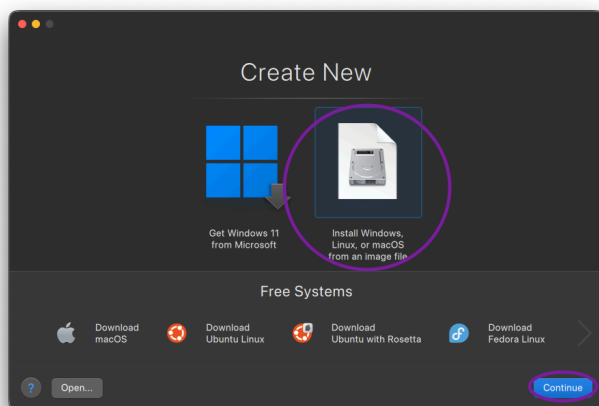
1. Download the Ubuntu 26.04 LTE ARM64 ISO from Canonical's website, <https://ubuntu.com/download/server/arm>.

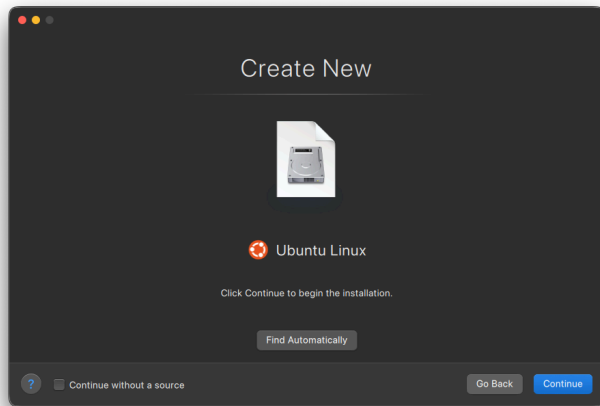
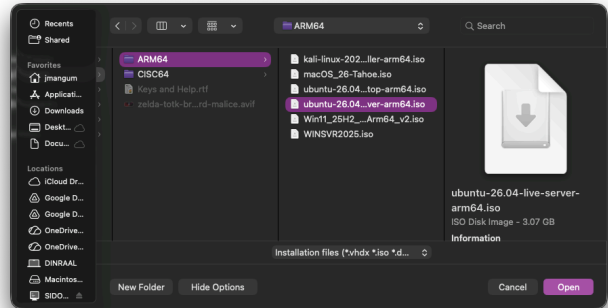
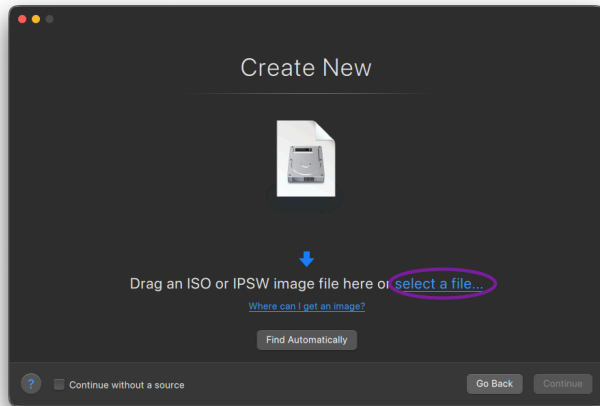


2. On Parallels Control Center click the “+” in upper right corner.

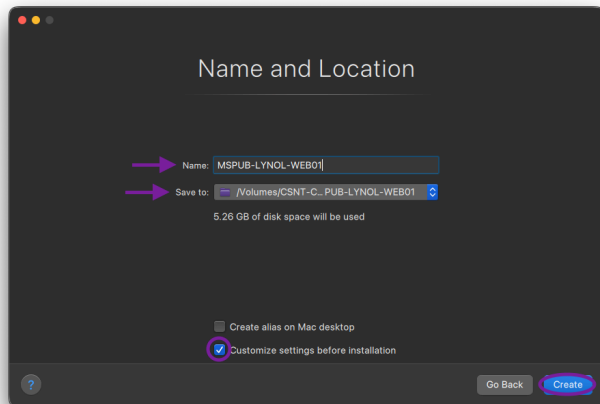


3. In the Create New window click “Install Windows, Linux, or macOS from an image file.” Click “Continue.” Click on the “Choose Manually” button. Click on “select a file...” hyperlink. Navigate to the Ubuntu Server 26.04 LTE ARM ISO and click “Open.” Parallels will automatically detect the operating system. Click on “Continue.”



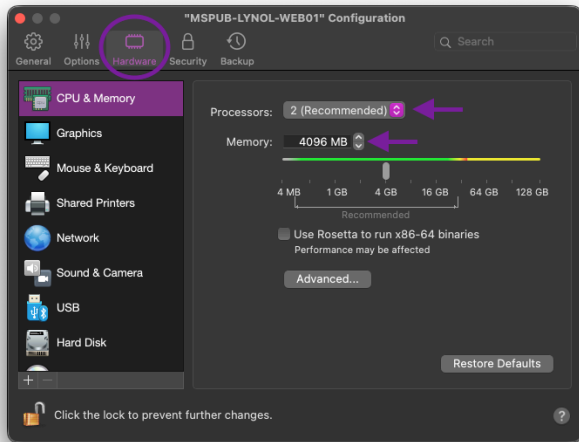


4. On the Name and Location window, name the virtual machine “MSPUB-LYNOL-WEB01.” Choose a location to save the virtual machine. Select “Custom settings before installation.” Click “Create.”

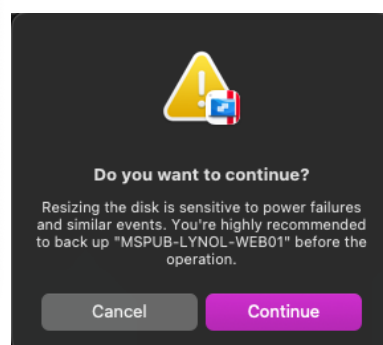
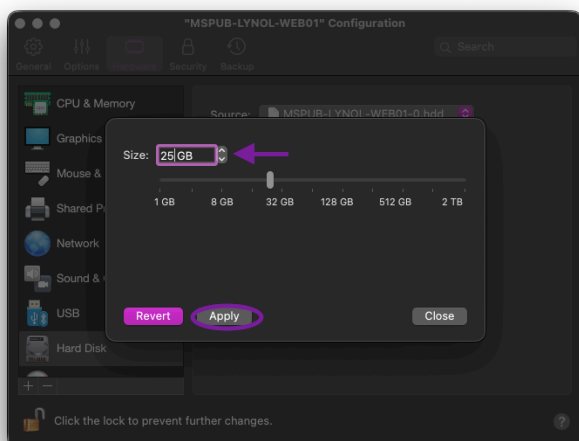
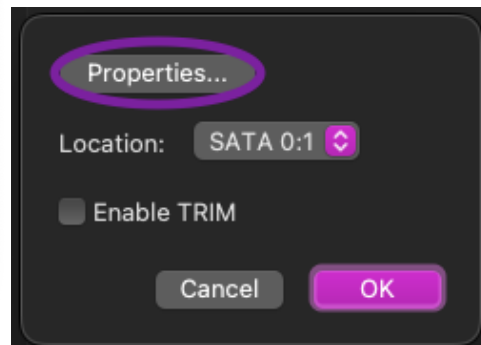
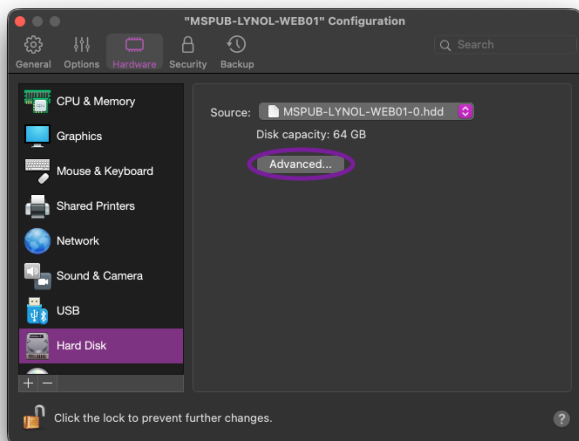


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- On the “MSPUB-LYNEL-WEB01” Configuration window click on “Hardware.” Leave the defaults for “CPU & Memory,” Processors set to “2” and Memory set to “4096 MB” (~4 GB).

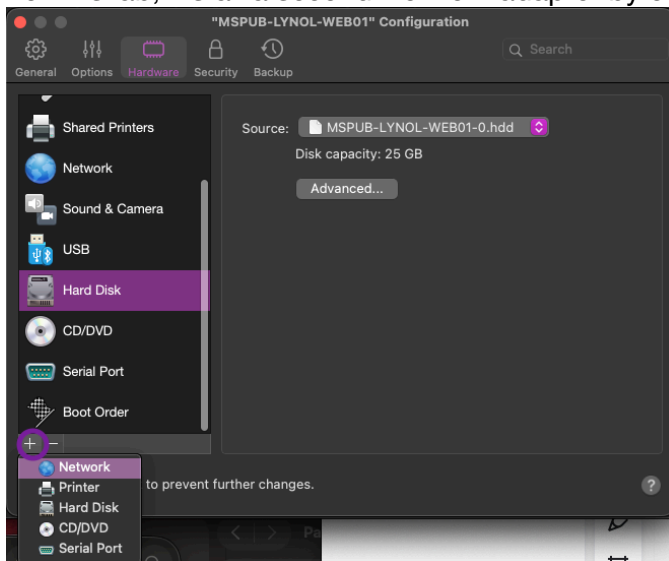


- In the “MSPUB-LYNEL-WEB01” Configuration windows select Hard Disk on the left pane. Click the “Advanced...” button. Click “Properties...” in the popup window. Reduce the size to “25 GB” and click “Apply.” Click “Continue” on the Warning popup. Click “Close” on the Size window. Click “OK” on the properties window.

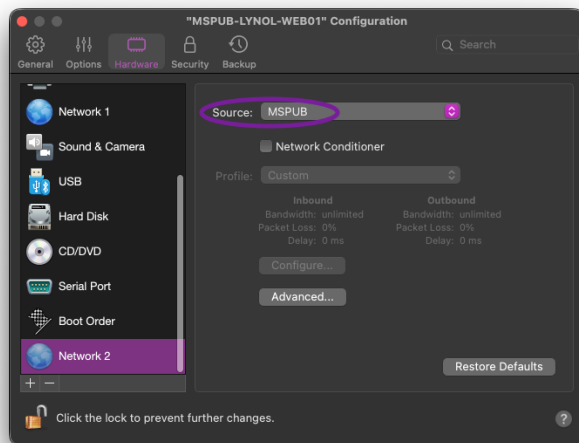


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

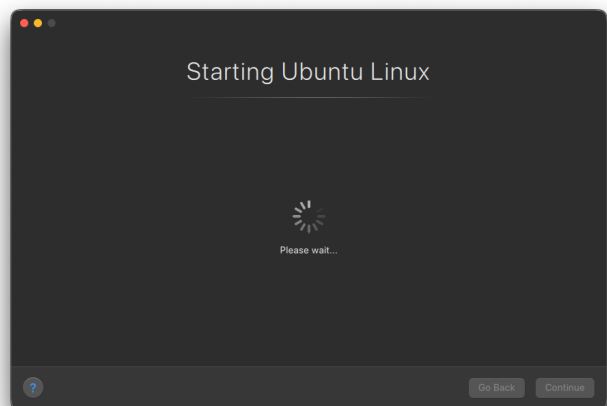
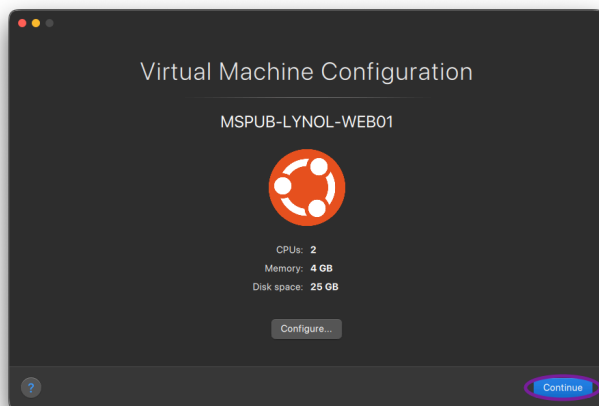
7. For this lab, install a second Network adapter by clicking the plus in the lower left and select “Network.”



8. Configure Network 2 with the predefined source “MSPUB” in dropdown menu. Close the “MSPUB-LYNOL-WEB01” Configuration window.

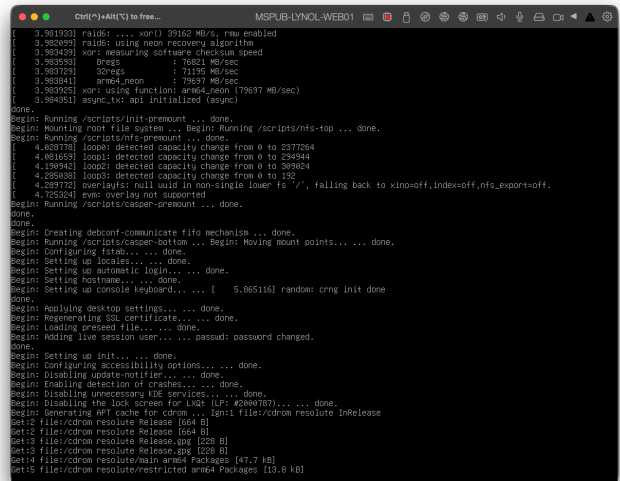
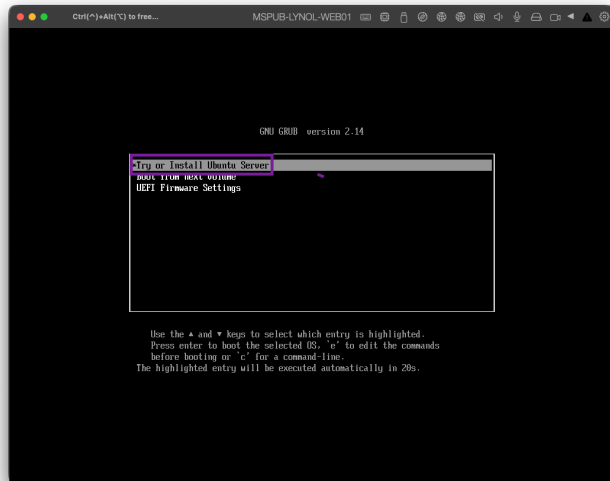


9. Click “Continue” on the Virtual Machine Configuration window to create the Virtual Machine. The virtual will be created

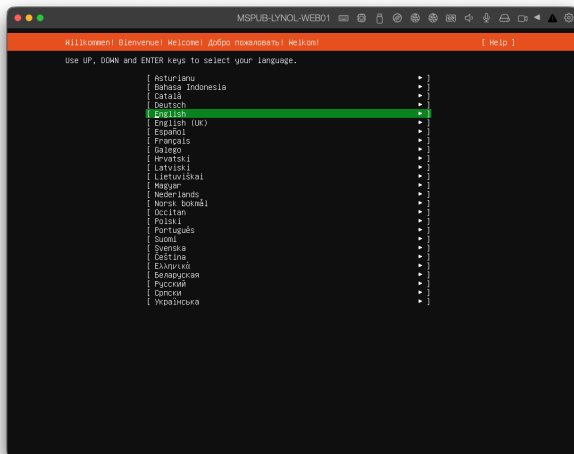


Ubuntu Server Installation & Setup

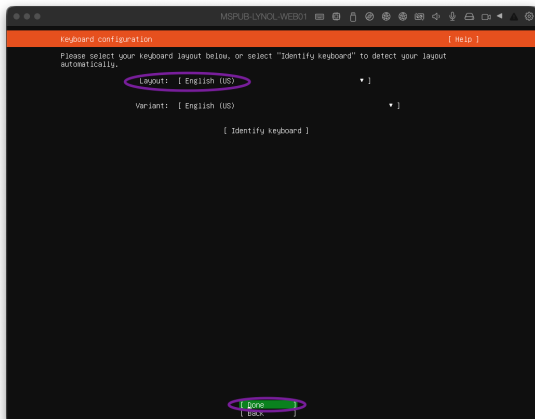
1. In GNU GRUB boot selector using the keyboard arrow key select “Try or Install Ubuntu Server” and press enter. The Ubuntu Server 26.06 LTE will begin to load.



2. Using the keyboard arrow keys, select the system's language and press enter. In this case English has been selected.

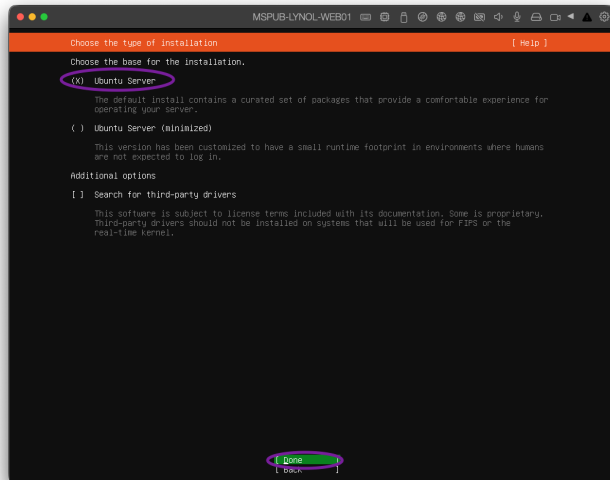


3. Using the arrow keys choose the keyboard layout and using enter to confirm. Select “Done” and press enter when finished. In this case “English (US)” has been selected.

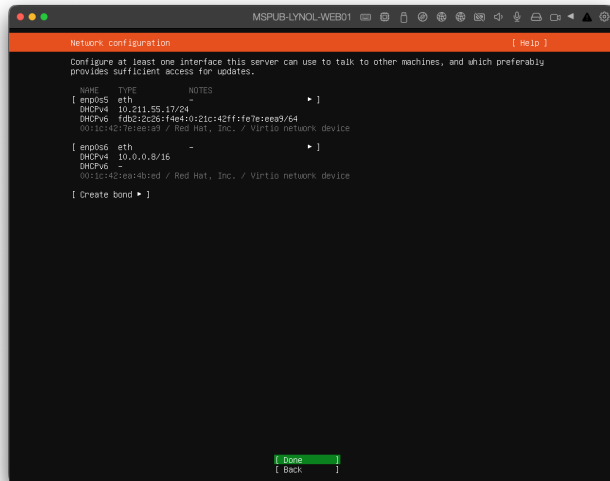


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

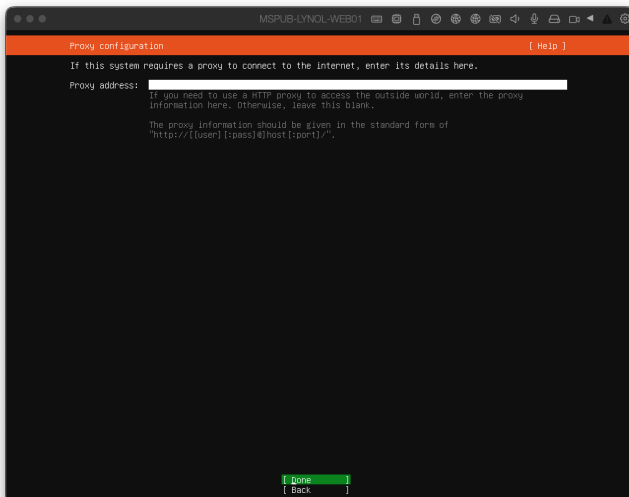
- Using the arrow keys on the keyboard choose “Ubuntu Server” for the installation base and press enter. Select “Done” and press enter once finished.



- Leave the defaults on the Network configuration, select “Done” and press enter.

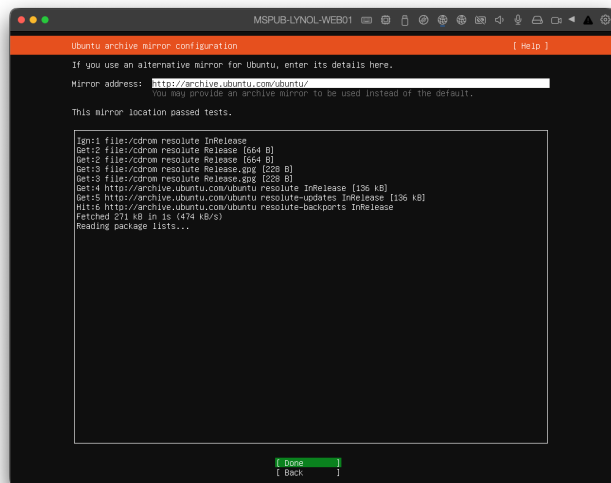


- Skip the Proxy configuration, select “Done” and press enter.

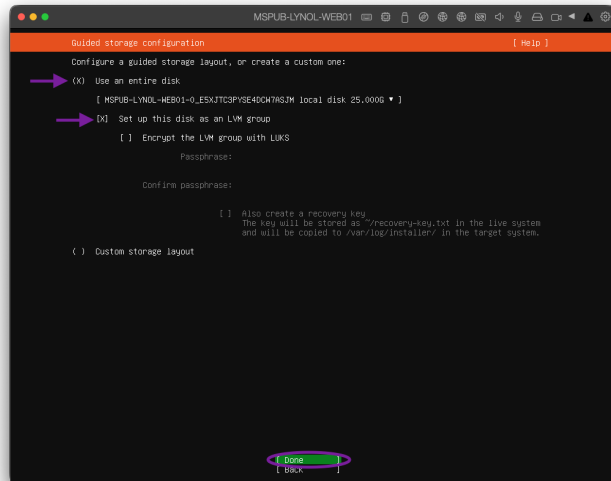


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

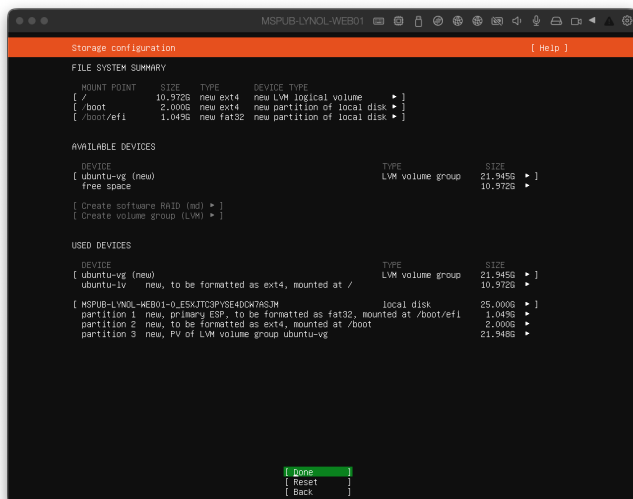
7. Leave the Ubuntu archive mirror configuration as defaults, select done and press enter.



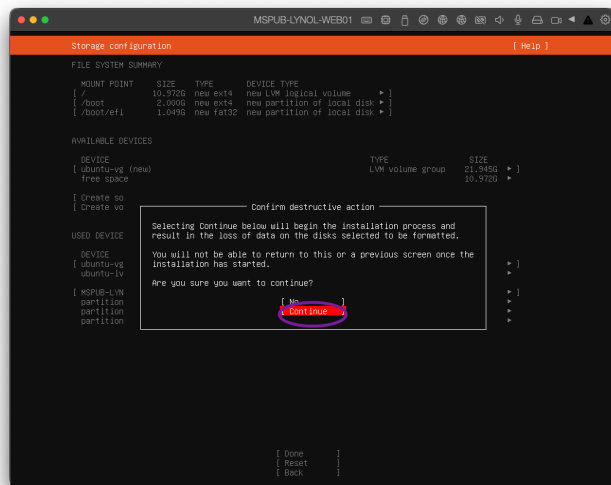
8. For the Guided storage configuration, select “Use an entire disk”, leave the disk as the default, select “Setup up this disk as an LVM group.” Select “Done” and press enter once finished.



9. Leave the Storage configuration as defaults. Select “Done” and press enter.

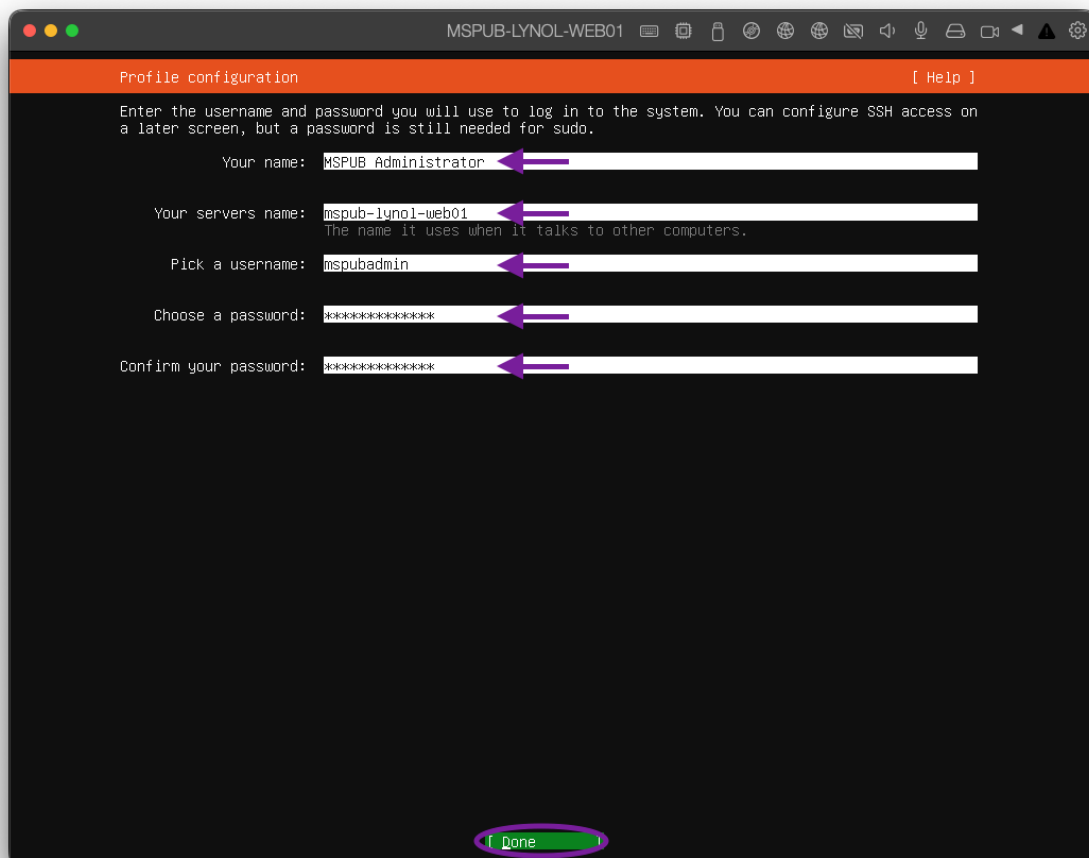


10. Select “Continue” in the Confirm destructive action dialogue and press enter.



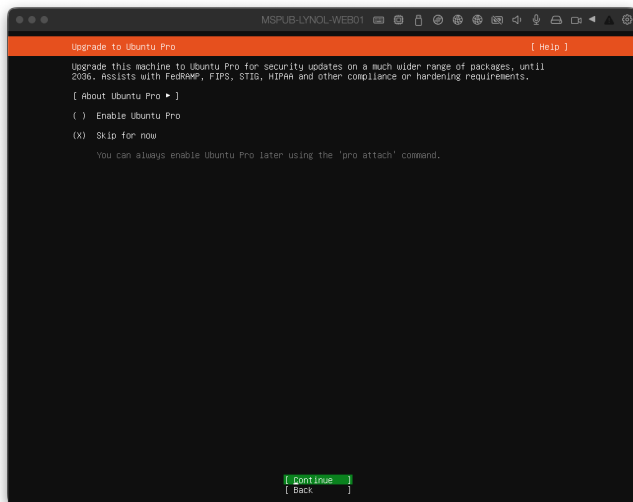
11. Fill out the following information for the Profile configuration using the arrow keys to navigate the fields:

- Your Name: **MSPUB Administrator**
- Your Servers name: **MSPUB-LYNEL-web01**
- Pick a username: **mispubadmin**
- Choose a password: **CSNT253_2026#**
- Confirm your password: **CSNT253_2026#**
- Select “Done” and press enter once complete

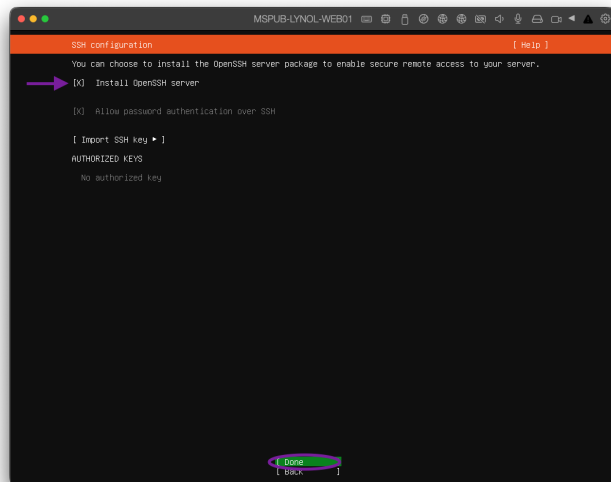


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

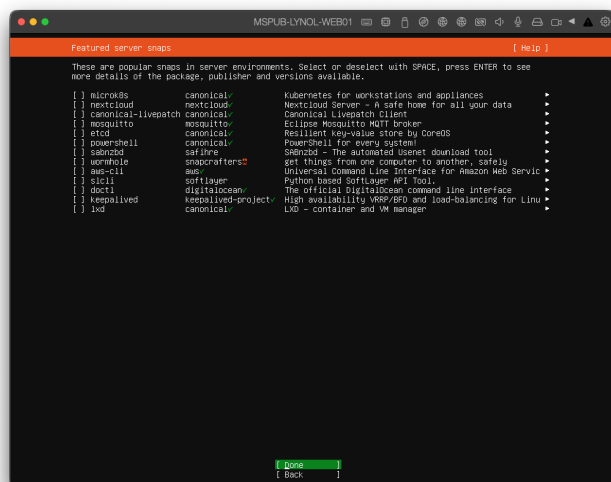
12. Select “Skip for now” for Upgrade to Ubuntu Pro. Select “Continue” and press enter.



13. For the SSH (Secure Shell Protocol) configuration, select “Install OpenSSH server.” Select “Done” and press enter once finished.

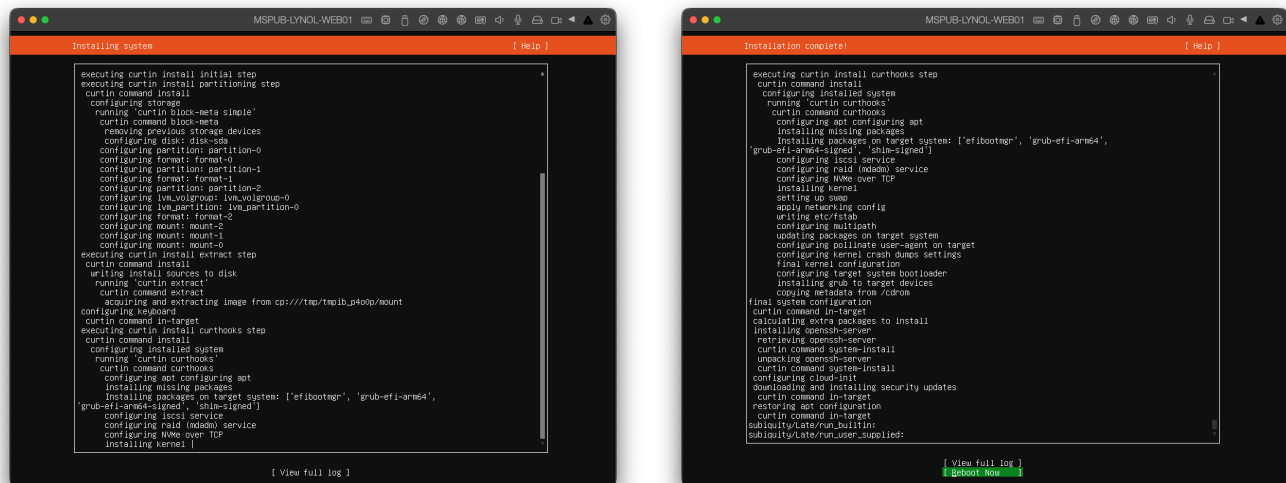


14. Skip the Featured server snaps by selecting “Done” and pressing enter.

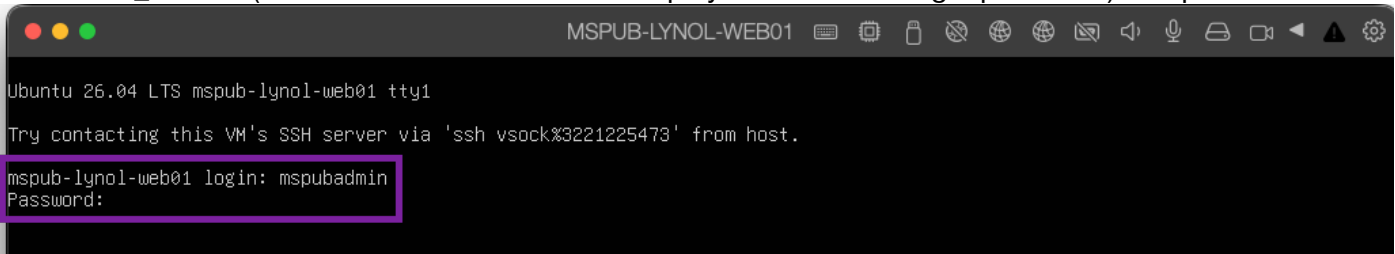


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

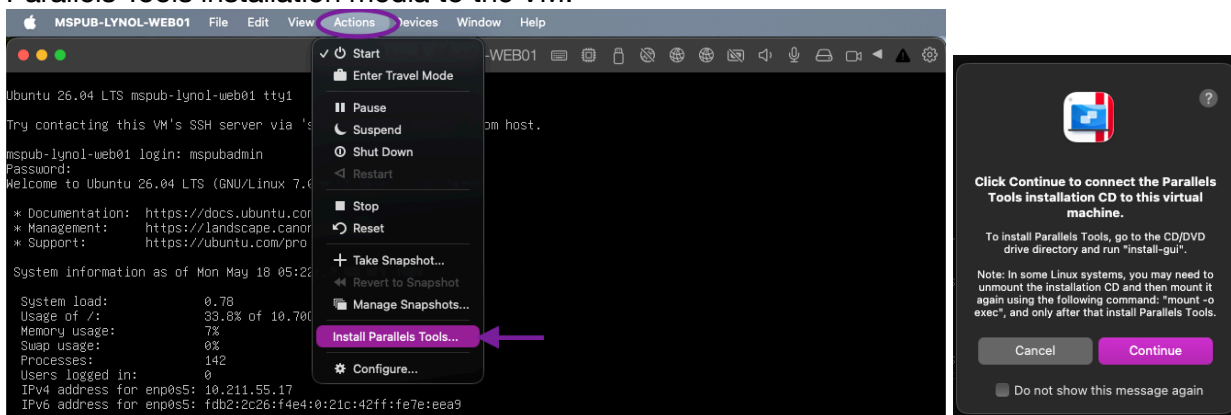
15. Ubuntu server will begin installing. This may take more than 15 minutes to complete. Once completed select “Reboot Now” and press enter.



16. Once the VM reboots login by typing the username “mispubadmin” and press enter. Type the password “CSNT253 2026#” (it is normal for no text to be displayed when entering a password) and press enter.



16. Parallels Tools is a set of virtual machine drivers for the system. To install Parallels Tools, from the host machine’s menu bar click “Actions” and select “Install Parallels Tools...” Click “Continue” to mount the Parallels Tools installation media to the VM.



17. To update the package list in Ubuntu Server type the command:
`sudo apt-get install -y dkms libelf-dev linux-headers-$(uname -r) build-essential gcc make`
Type in the the MSPUB Administrator password to authenticate the sudo command.

```
mispubadmin@mispub-lynol-web01:~$ sudo apt-get install -y dkms libelf-dev linux-headers-$(uname -r) build-essential gcc make
[sudo: authenticate] Password: ****
```

18. Mount the Parallels Tools installation media by typing the commands: (It is normal for there to be no response after typing some commands)
- `sudo mkdir -p /media/cdrom`

- `sudo mount -o exec /dev/sr0 /media/cdrom`

```
msspubadmin@msspub-lynol-web01:~$ sudo mkdir -p /media/cdrom
msspubadmin@msspub-lynol-web01:~$ sudo mount -o exec /dev/sr0/media/cdrom
mount: /dev/sr0/media/cdrom: can't find in /etc/fstab.
msspubadmin@msspub-lynol-web01:~$ sudo mount -o exec /dev/sr0 /media/cdrom
[ 743.815734] /dev/sr0: Can't open blockdev
mount: /media/cdrom: WARNING: source write-protected, mounted read-only.
msspubadmin@msspub-lynol-web01:~$
```

19. To install the Parallels Tools drivers type the following commands:

- `cd /media/cdrom`
- `sudo ./install`

```
msspubadmin@msspub-lynol-web01:~$ cd /media/cdrom
msspubadmin@msspub-lynol-web01:/media/cdrom$ sudo ./install
```

- Parallels Tools will begin installing. Once completed you will receive an “installed successfully” message

```
Started installation of Parallels Guest Tools version '26.2.2.57373'
installer:%0.000000

Mon May 18 05:38:14 UTC 2026
Start installation or upgrade of Guest Tools
installer:%10.000000
installer:%20.000000
installer:%30.000000
installer:%40.000000
installer:%50.000000
installer:%60.000000
installer:%70.000000
installer:%80.000000
installer:%90.000000
Parallels Guest Tools were installed successfully!
msspubadmin@msspub-lynol-web01:/media/cdrom$
```

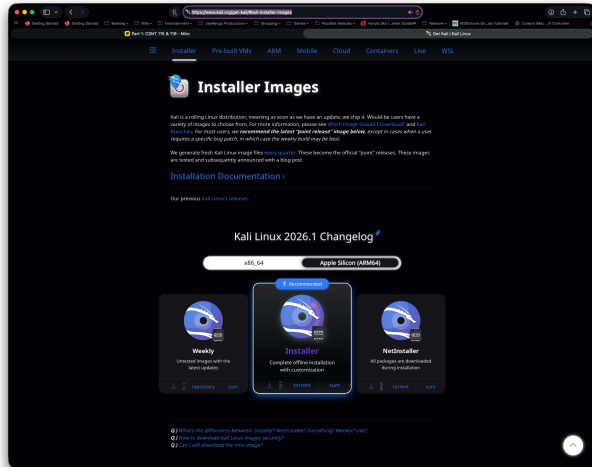
20. To reboot the VM type the command:

`sudo shutdown -r now`

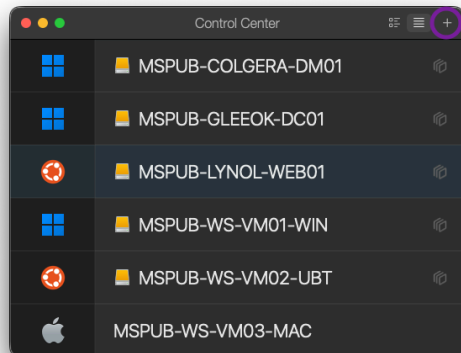
Kali Linux 2026 Virtual Machine

Before creating a Virtual Machine for Kali Linux 2026.1, it is important to know the minimum system requirements. These can be found on Kali Linux’s website, <https://www.kali.org/docs/installation/>. The minimum requirements are: 1.0 GHz processor, 2 gigabytes of RAM, and 20 GB of storage.

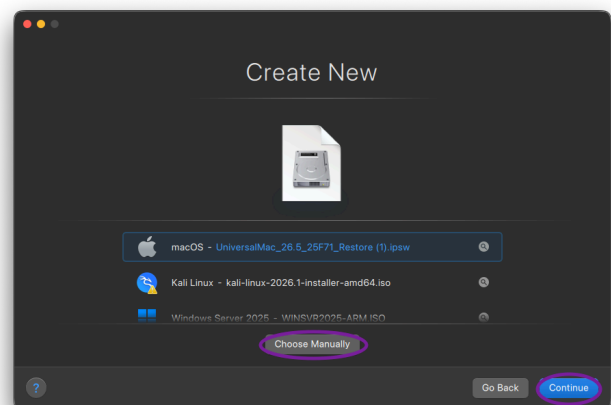
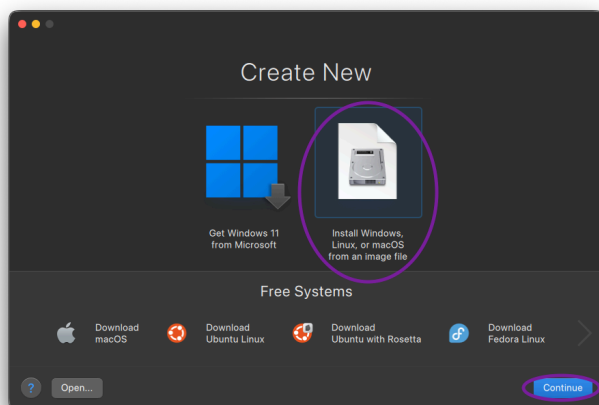
1. Download the Kali Linux 2026.1 ISO file from Kali Linux’s website, <https://www.kali.org/get-kali/#kali-installer-images>.

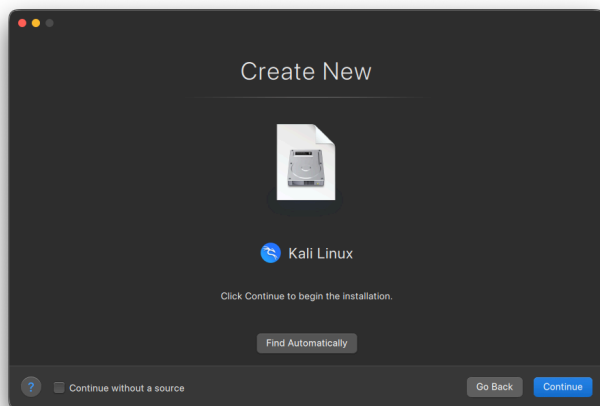
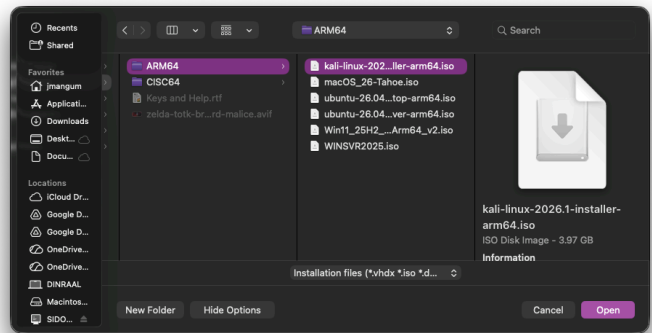
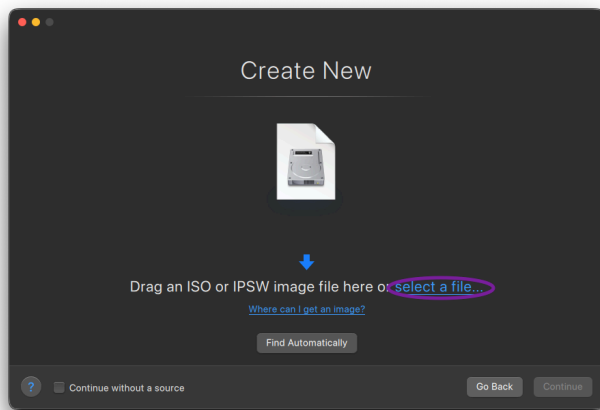


2. In Parallels Control Center click on the “+” button to create a new virtual machine.

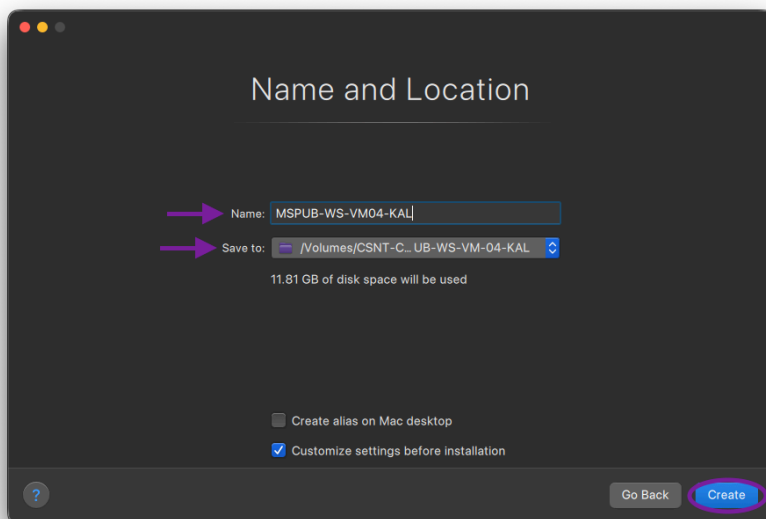


3. On the Create New window click on “Install Windows, Linux, or macOS from an image file.” Click “Continue.” Click the “select a file...” hyperlink. Navigate to the Kali Linux 2026 ARM ISO file and click “Open.” Parallels will automatically detect the operating system. Click “Continue.”

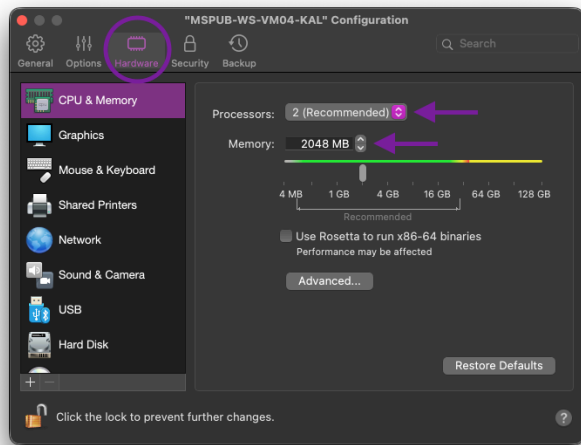




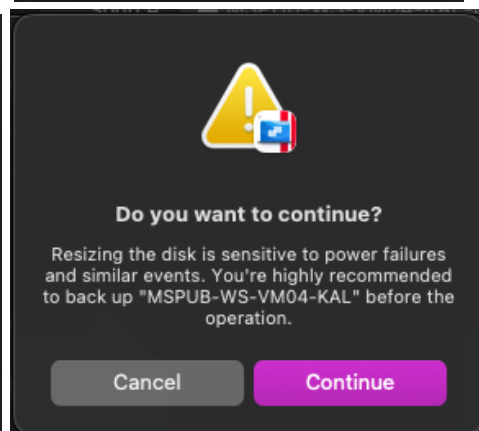
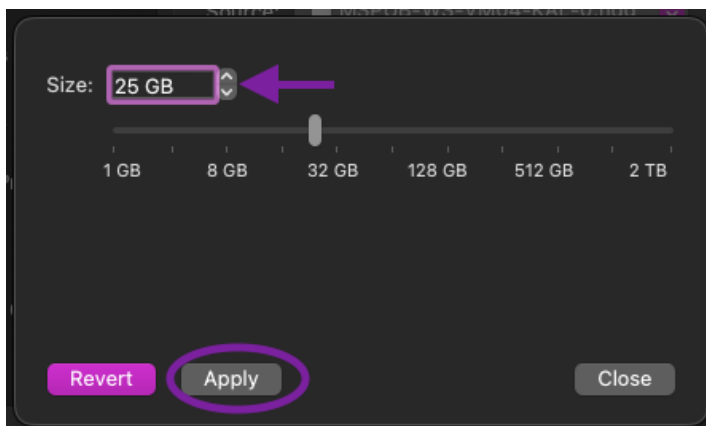
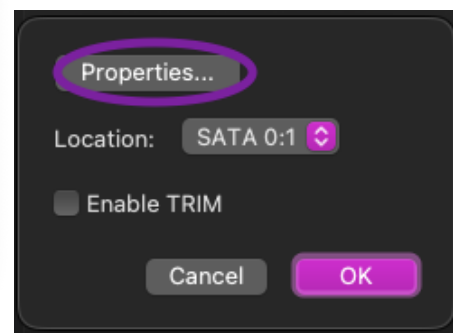
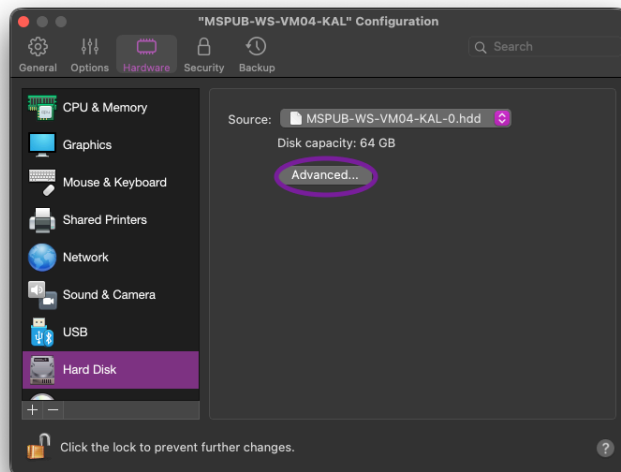
4. On the Name and Location window name the new virtual machine “MSPUB-WS-VM04-KAL.” Choose a location to save the VM. Select “Customize settings before installation.” Click “Create.”



5. On the “MSPUB-WS-VM04-KAL” Configuration window click on “Hardware” on the top toolbar. For “CPU & Memory” leave the defaults as, Processor “2” and Memory “2048 MB” (~2 GB).

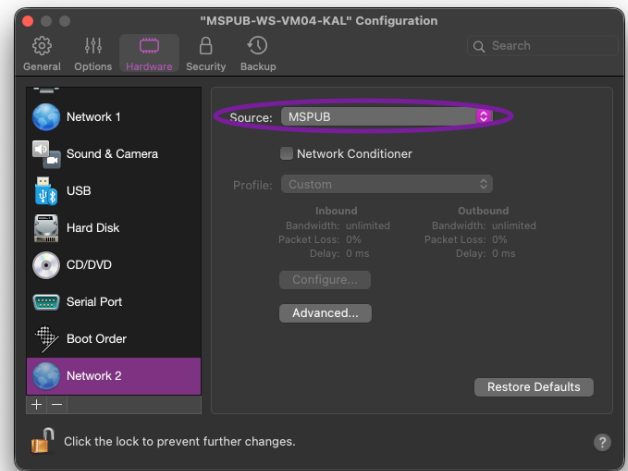
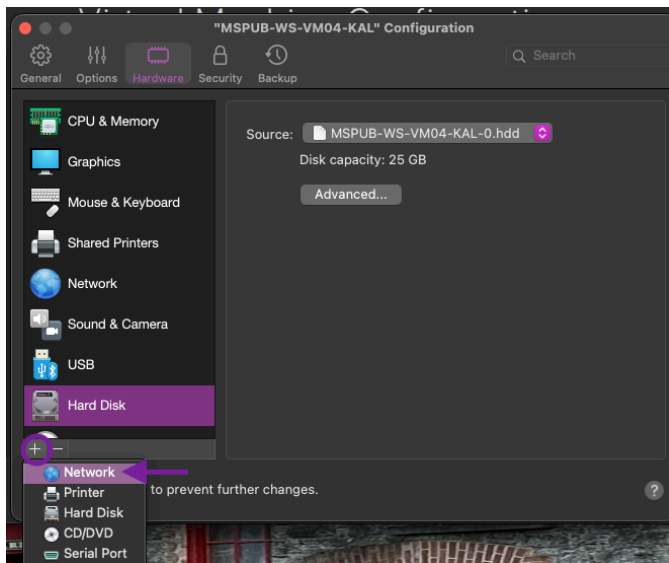


- On the left pane of the “MSPUB-WS-VM04-KAL” Configuration window click on “Hard Disk.” Click “Advanced.” Click “Properties...” Reduce the storage size to “25 GB.” Click “Apply.” Click “Continue” on the warning message popup. Click close on the “Size Properties” window. Click “OK” on the Advanced options window.



- At the lower left of the left pane of the “MSPUB-WS-VM03-KAL” Configuration window click on the “+” button and select “Network.” Change the source of Network 2 to the predefined, “MSPUB.” Close the “MSPUB-WS-VM04-KAL” Configuration window by clicking the red circle in the upper left corner.

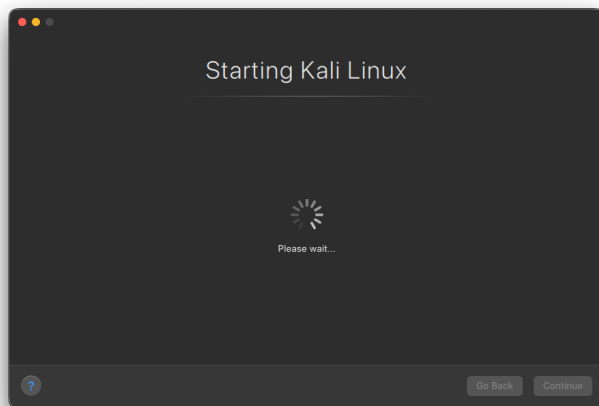
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



- Click "Continue" on the Virtual Machine Configuration window.

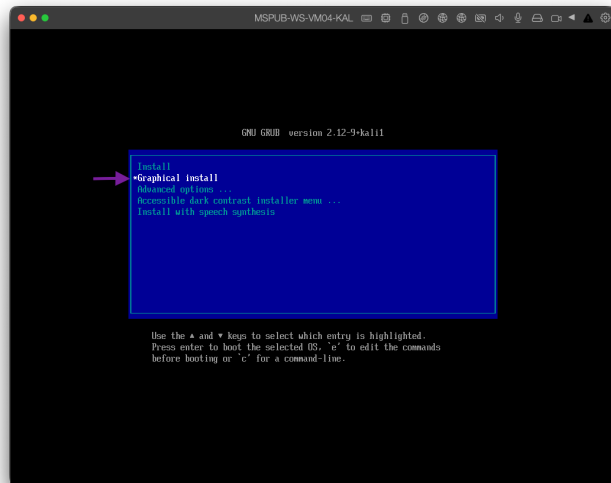


- The virtual machine will automatically boot.

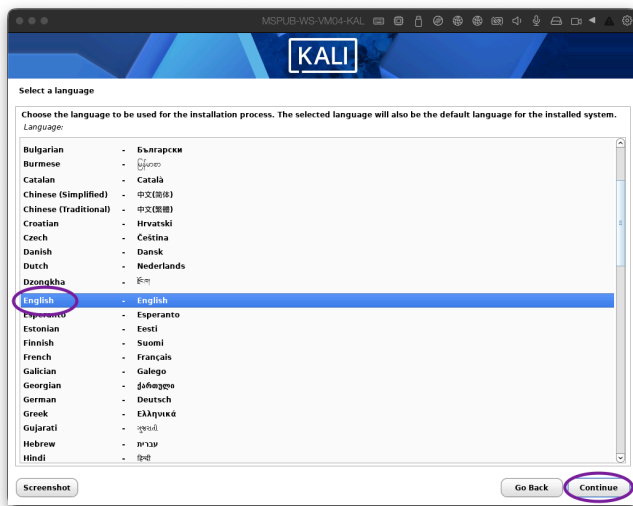


Kali Linux Install & Setup

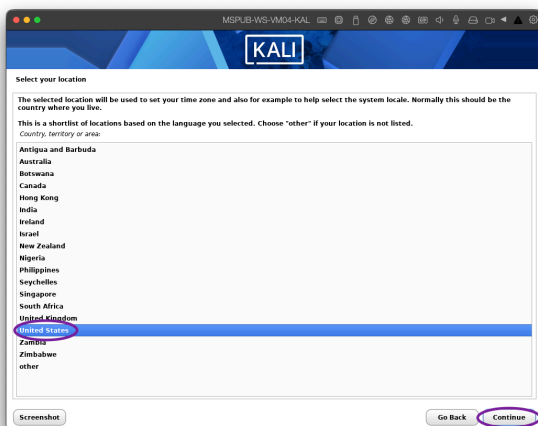
1. Once the Kali Linux installer has booted up, use the arrow keys to select “Graphical install” and press enter to continue.



2. Once the installer graphical installer launched select a language, in this case English has been selected. Click “Continue.”

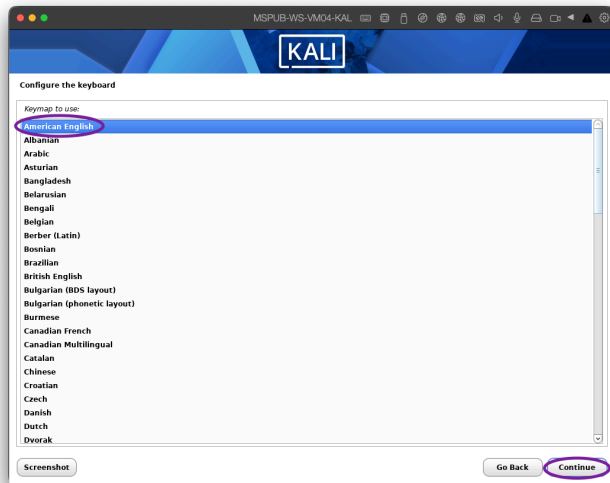


3. Select the location the machine is located, in this case “United States” is selected. Click “Continue.”

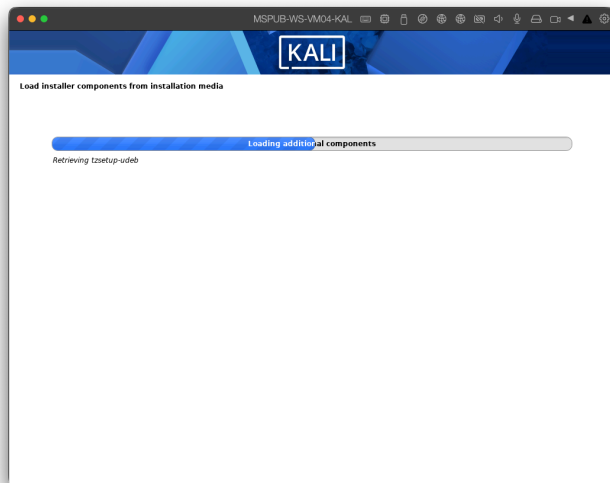


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

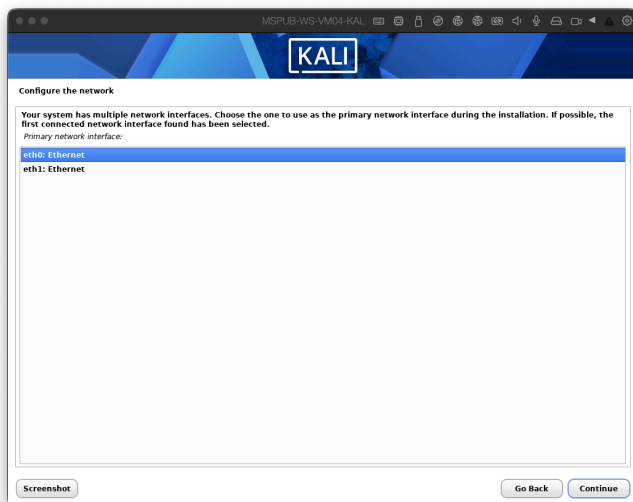
4. Select a keyboard key mapping language, in this case “American English” is selected. Click “Continue.”



5. Kali Linux will apply the settings to installer.

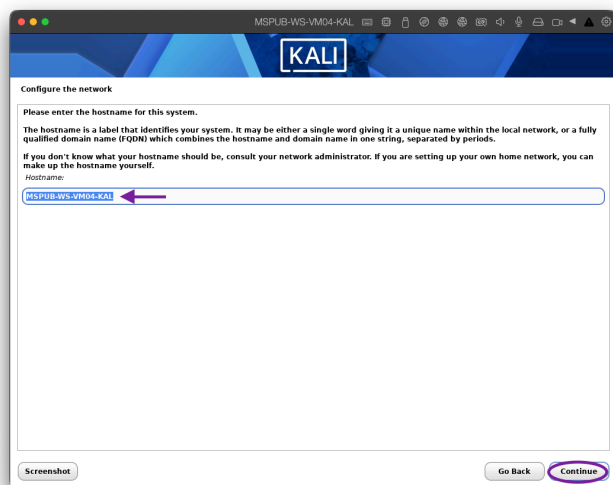


6. Choose “eth0:Ethernet” as the network adapter. Click “Continue.”



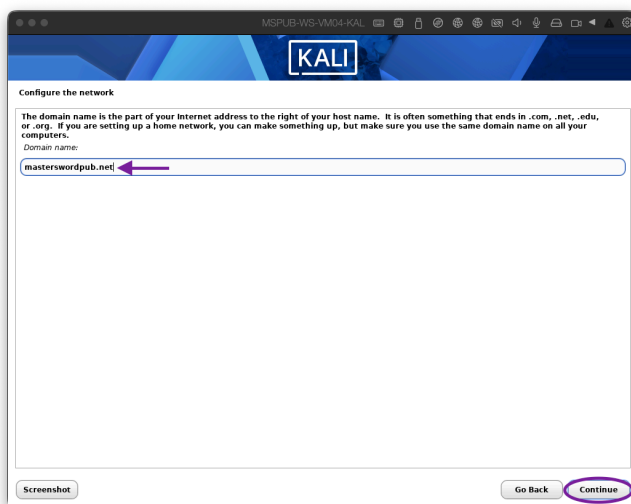
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

7. Enter the hostname "MSPUB-WS-VM04-KAL." Click "Continue."



The screenshot shows the 'Configure the network' window in Kali Linux. The hostname field is filled with 'MSPUB-WS-VM04-KAL'. The 'Continue' button is circled in purple.

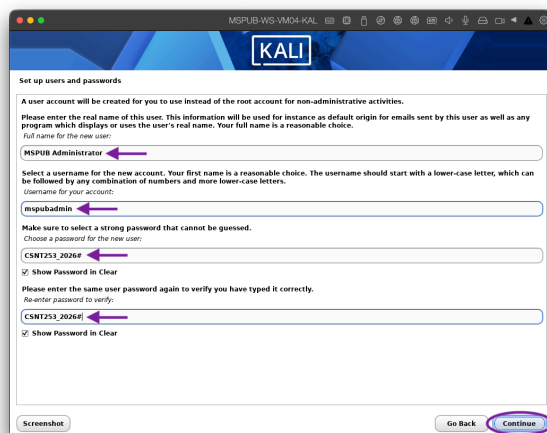
8. Change the domain name as "masterswordpub.net." Click "Continue."



The screenshot shows the 'Configure the network' window in Kali Linux. The domain name field is filled with 'masterswordpub.net'. The 'Continue' button is circled in purple.

9. Create a new user using the following information, and click "Continue" when completed:

- Full Name of the new user: **MSPUB Administrator**
- Username for your account: **mspubadmin**
- Choose a password: **CSNT253_2026#**
- Re-enter password: **CSNT253_2026#**



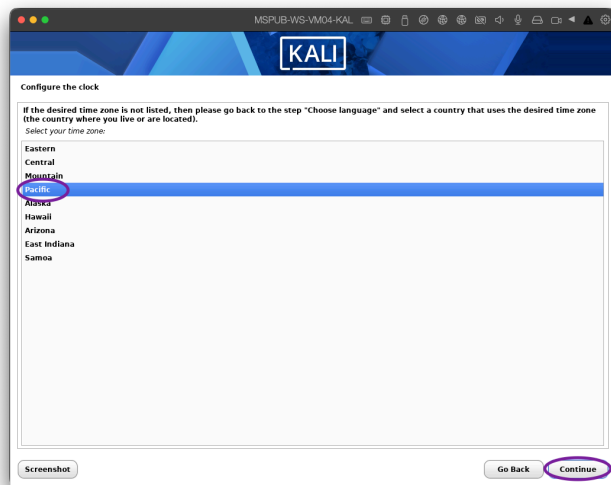
The screenshot shows the 'Set up users and passwords' window in Kali Linux. The new user information is as follows:

- Full name for the new user: MSPUB Administrator
- Username for the new user: mspubadmin
- Choose a password for the new user: CSNT253_2026#
- Re-enter password to verify: CSNT253_2026#

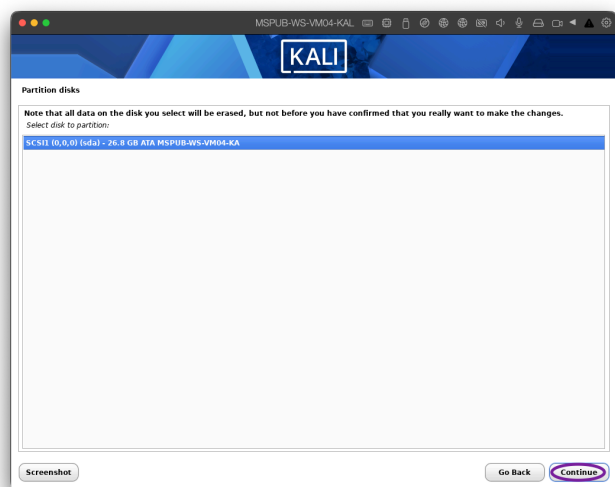
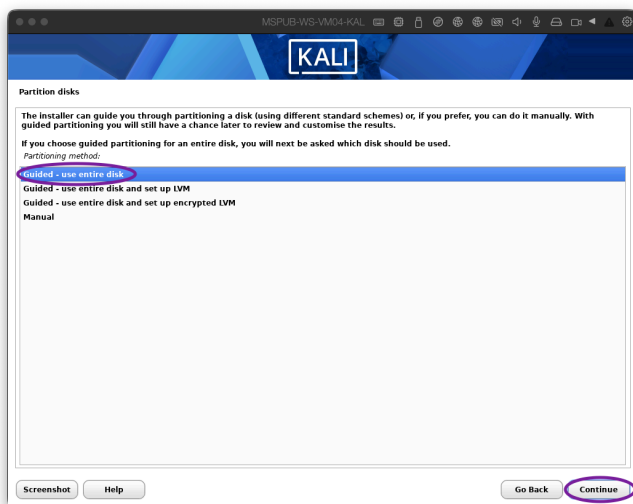
The 'Continue' button is circled in purple.

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

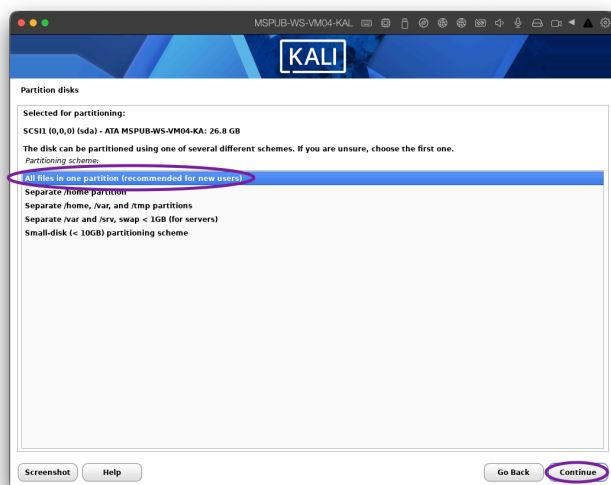
10. Select the time zone the machine is in, in this case “Pacific” has been selected. Click “Continue.”



11. For Partition disks select “Guided - use entire disk.” Click “Continue.” Click “Continue” again.

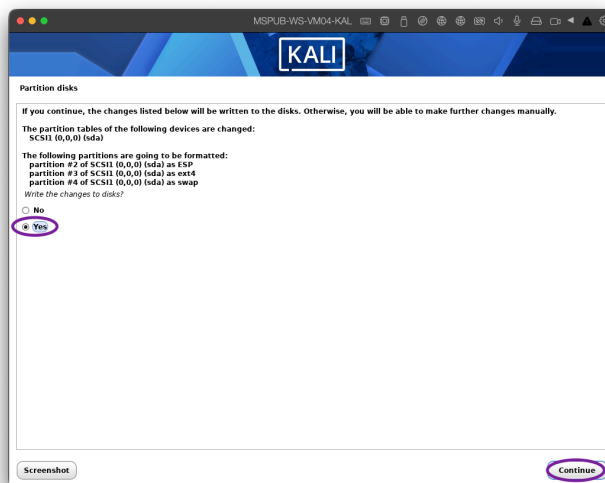
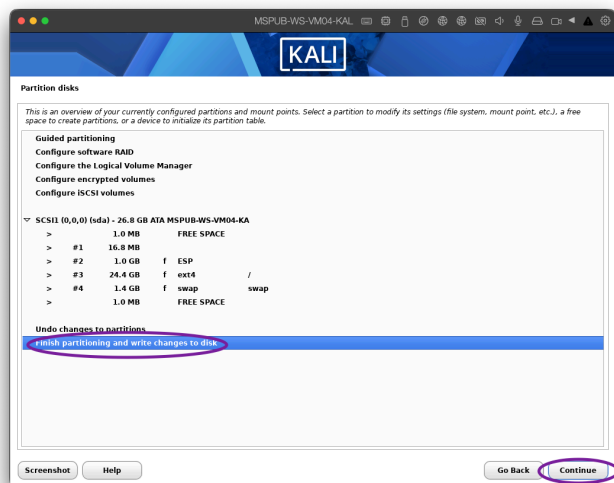


12. Select “All files in one partition” for the Partitioning scheme. Click “Continue.”

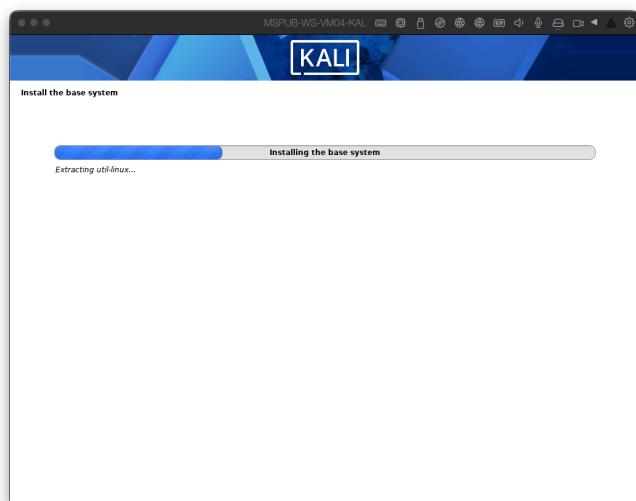


13. On the confirmation screen select “Finish partitioning and write changes to disk.” Click “Continue.” Select “Yes” on the second confirmation screen. Click “Continue.”

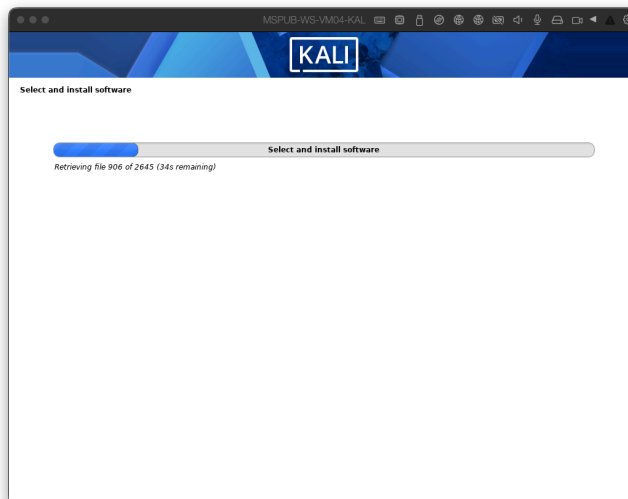
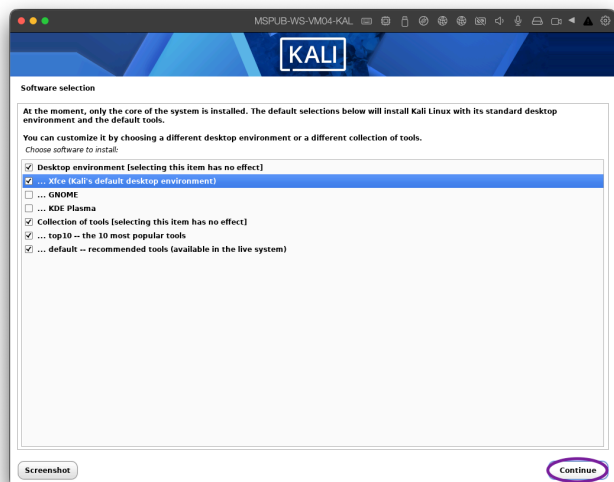
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



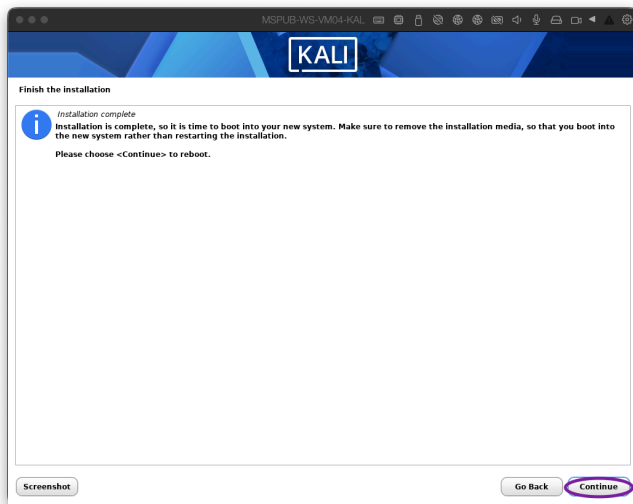
14. The installer will begin partitioning the virtual hard disk and begin installing the operating system.



15. For the Software selection install the defaults and click continue. The software packages will be installed.

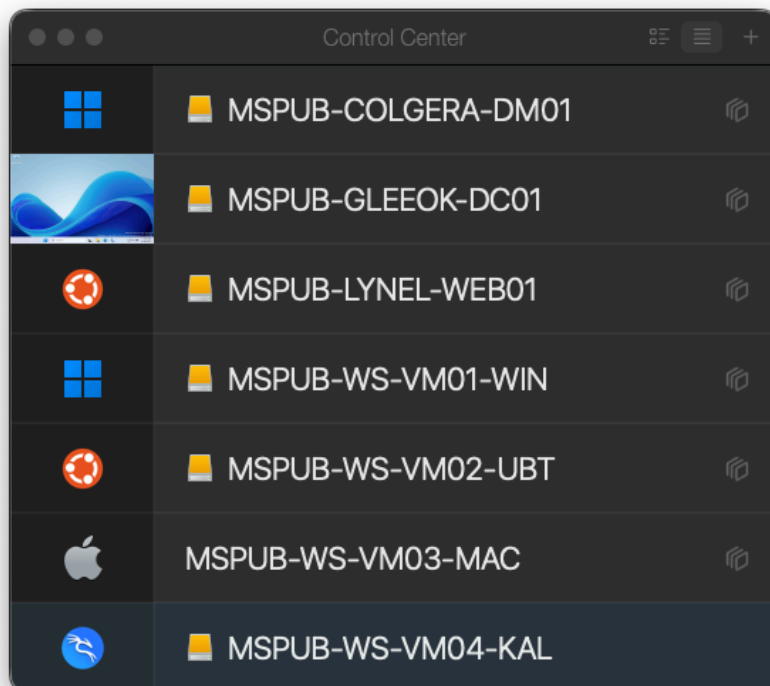


16. Once the installation completes click “Continue.” To restart the VM.



17. Parallels Tools is not compatible with Kali Linux 2026. They will not be installed in this VM.

The Master Sword Publishing Virtual Machine Environment is now complete. All VMs will be contained in Parallels Control Center.



MSPUB Active Directory & DNS Deployment

Scenario Information

Master Sword Publishing (MSPUB) recently expanded their on-premises infrastructure and hired an internal IT team to implement centralized authentication, user management, and internal name resolution services using Microsoft Server 2025 Active Directory Domain Services (AD DS) and Domain Name System (DNS). Previously, all workstations operated independently using local user accounts, making account management, workstation access, and resource administration difficult to maintain across the organization. MSPUB management requested that all employees be able to securely log into any authorized workstation within the organization using centralized domain credentials. To improve administrative efficiency and support future infrastructure growth, MSPUB selected the custom domain name: masterswordpub.net.

The MSPUB IT Department has been assigned the responsibility of configuring the first domain controller, MSPUB-GLEEOK-DC01, to host Active Directory Domain Services (AD DS) and DNS services for the environment. The environment currently contains ten employees distributed across four organization departments:

- Administration
- Publishing
- Information Technology/Security Operations
- Online Services

The following objectives have been identified for the initial deployment phase:

- Configure AD DS
- Configure integrated DNS services
- Promote MSPUB-GLEEOK-DC01 to a domain controller
- Create the masterswordpub.net domain forest
- Create Organizational Units (OUs) for each department
- Create employee user accounts
- Configure workstation domain membership
- Validate DNS name resolution and domain authentication
- Verify users can authenticate to domain-joined workstations

The IT Department has requested an employee roster to help determine user names and import user information.

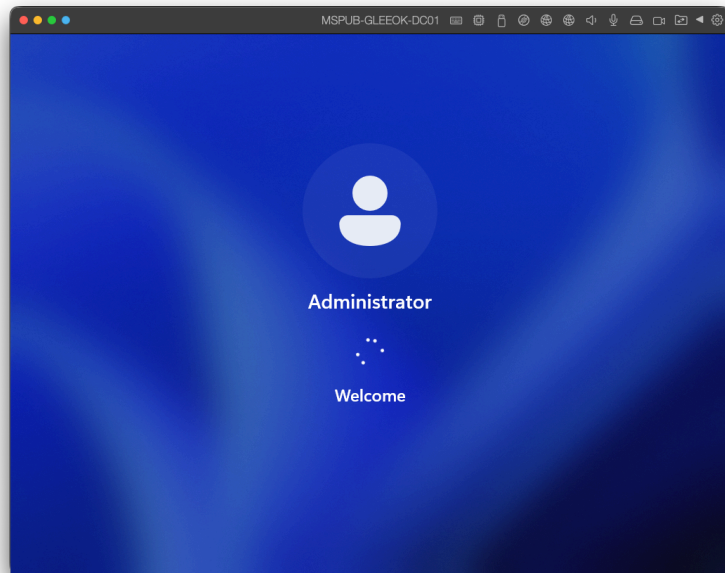
Name	User Name	Department	Title
Zelda Princess	z.princess	Administration	Owner
Impa Sheikah	i.sheikah	Administration	CFO
Purah Sheikah	p.sheikah	Information Technology/ Cyberseucirty	Director
Robbie Sheikah	r.sheikah	Information Technology/ Cyberseucirty	Help Desk Assistant
Link Hero	l.hero	Information Technology/ Cyberseucirty	Cybersecurity Administrator
Midna Twili	m.twili	Online Services	Senior Developer
Sidon Zora	s.zora	Publishing	Manager
Riju Gerudo	r.gerudo	Publishing	Editor
Yunobo Goron	y.goron	Publishing	Writer
Tulin Rito	t.rito	Publishing	Illustrator

Users will be given a temporary password of Hyrul3W@rr10r\$ which a change password request will be executed upon first login.

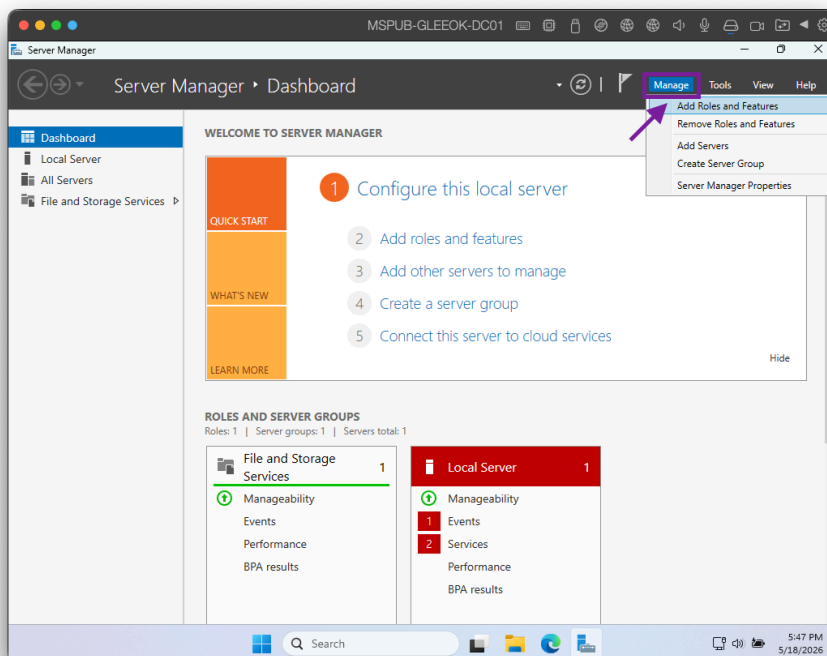
Installation and Configuration of DNS and AD DS

The IT Department configured MSPUB-GLEEOK-DC01 as follows:

1. Log into MSPUB-GLEEOK-DC01 as the Administrator using the password “CSNT253_2026#”.

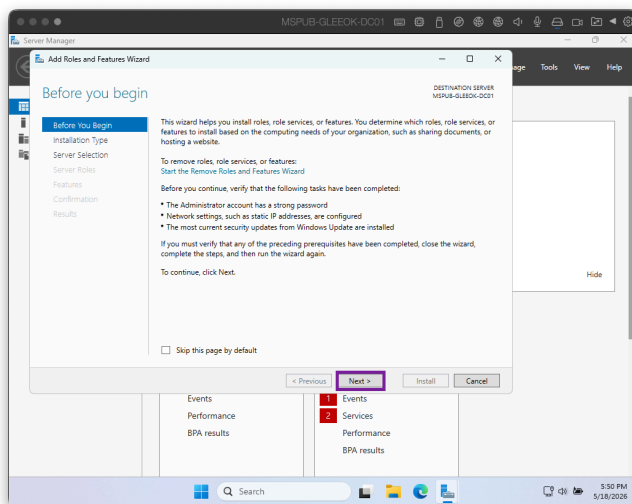


2. Server Manager will automatically open. In server manager install the resources AD DS and DNS.
 1. In Server Manger click “Manage” and select “Add Roles and Features.”

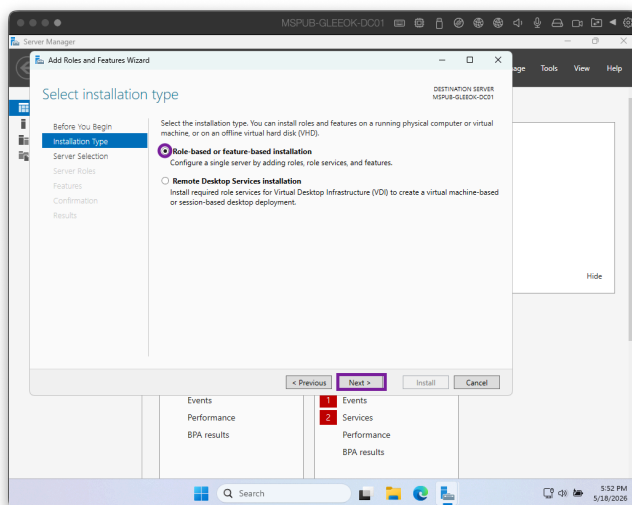


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

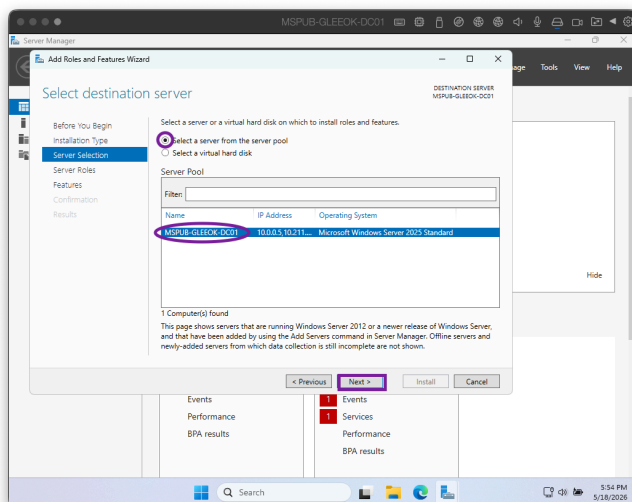
2. On the Before you begin screen click “Next.”



3. For Select installation type select “Role-based or feature-based installation.” Click “Next.”

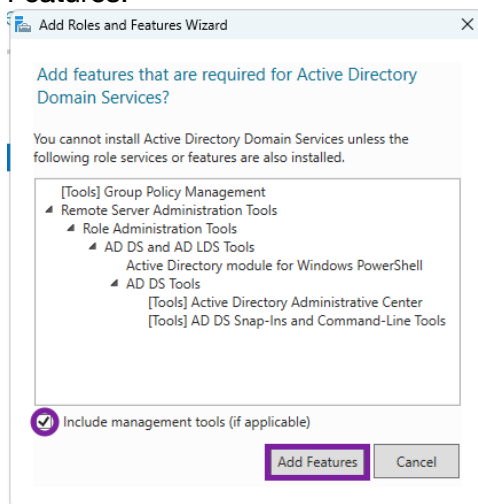


4. For Select destination, “Select a server from the server pool” is selected as well as “MSPUB-GLEEOK-DC01.” Click “Next.”

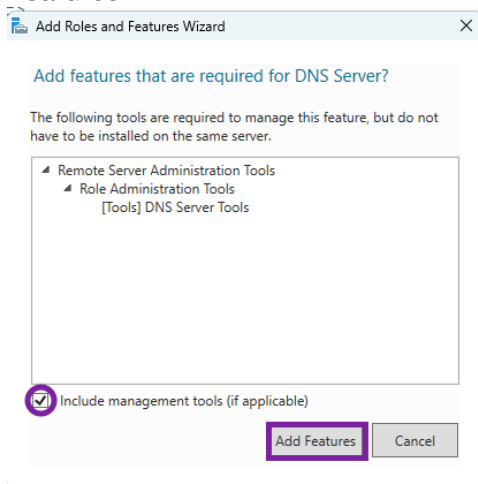


5. For the Select server roles select the following services to be installed:
 - Tick “Active Directory Domain Services” (AD DS)

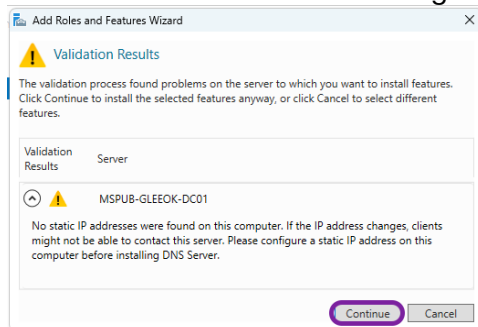
- On the Add feature window ensure “Include management tools” is ticked, then click “Add Features.”



- Tick “DNS Server”
- On the Add feature window ensure “Include management tools” is ticked, then click “Add Features.”

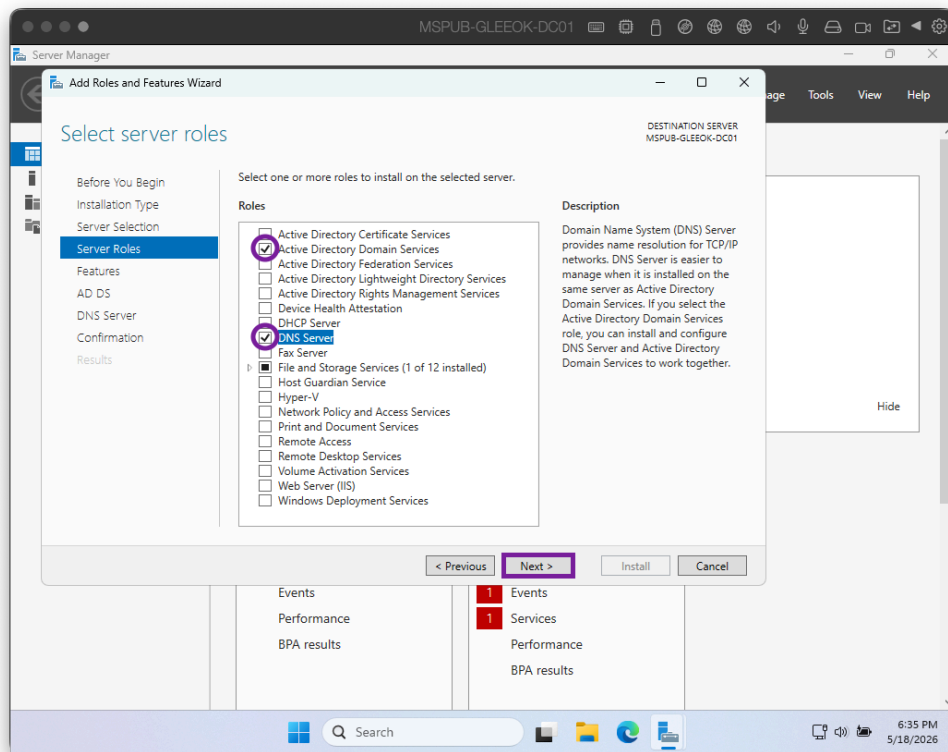


- On the Validation Results warning dialog (if prompted), click “Continue.”

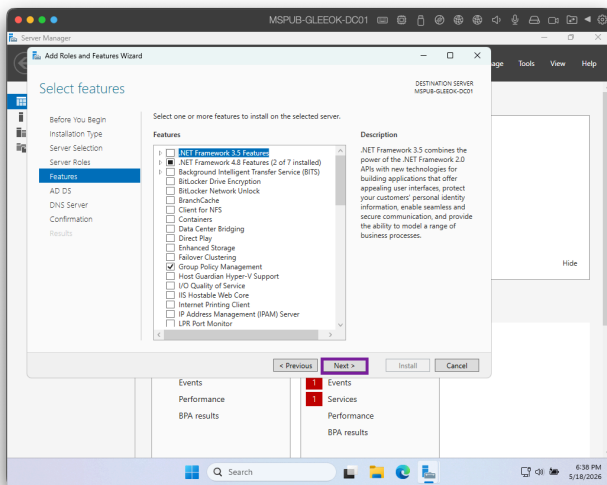


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Click “Next: once all features have been selected.

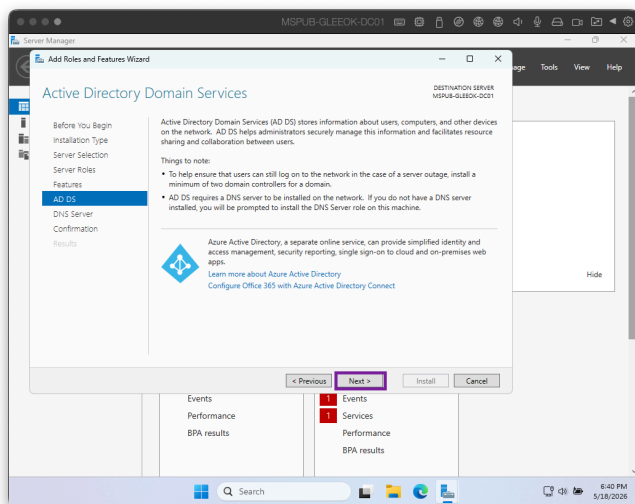


- No additional features will be installed at this time, click “Next.”

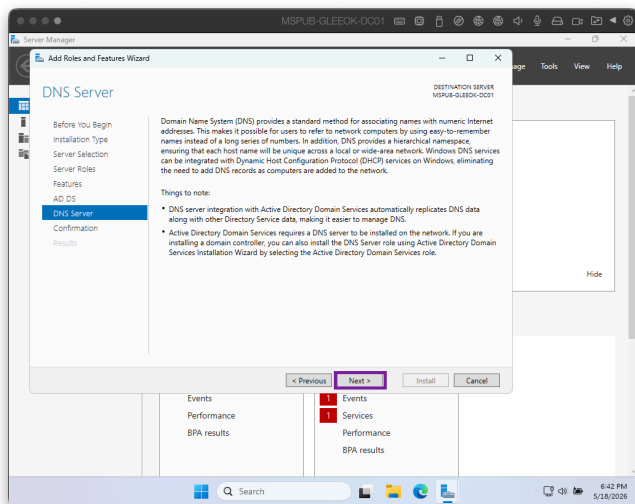


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

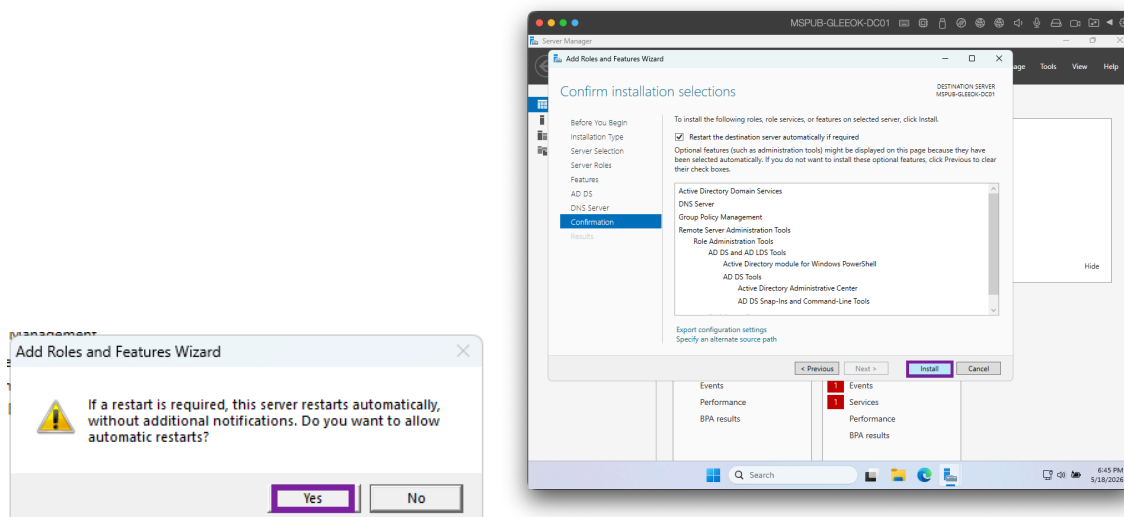
7. Read over the information on Active Directory Domain Services, then click “Next.”



8. Read over the DNS Server information, then click “Next.”

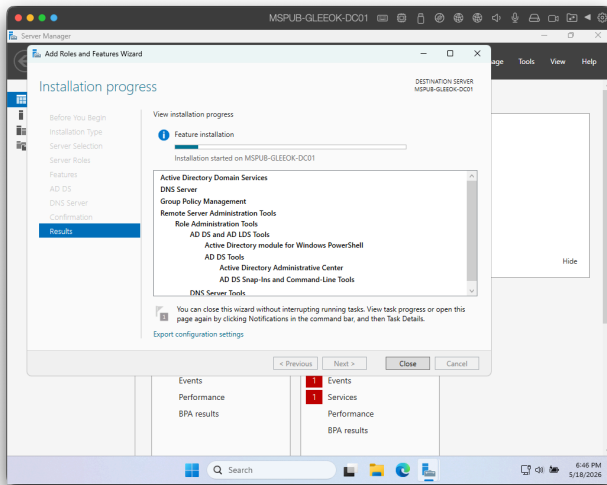


9. Look over the Confirm installation selections. Tick “Restart the destination server automatically if required.” On the warning dialog box click “Yes.” Click “Install”

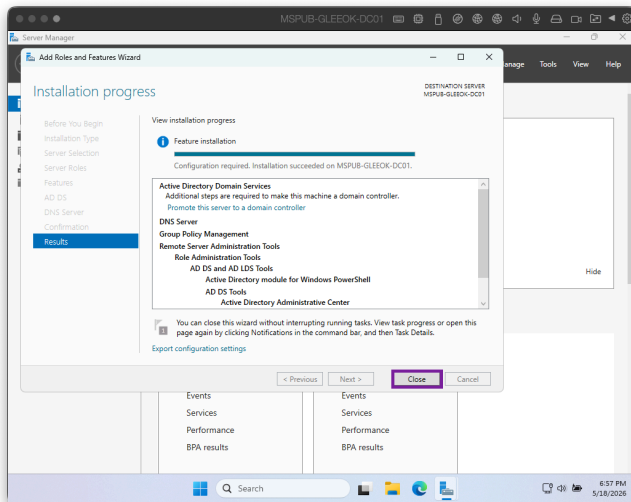


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

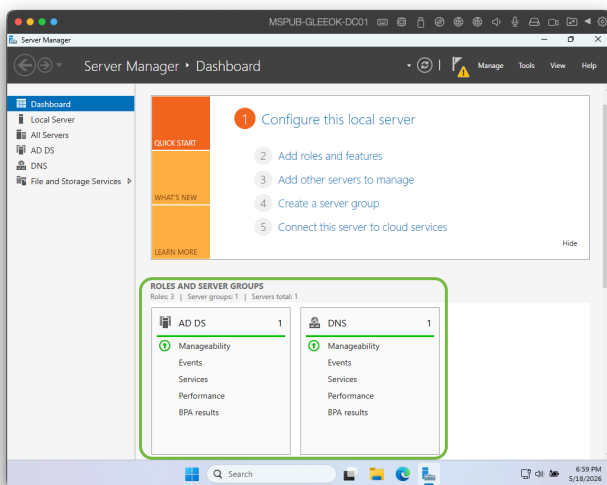
10. The new Server Roles will be installed. This may take several minutes to complete.



11. Once the installations are completed. Close the Add Roles and Features Wizard.



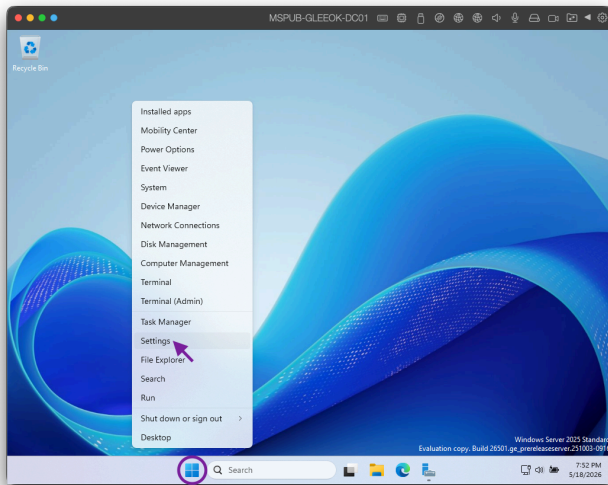
12. The new roles will be displayed under Roles and Server Groups within Server Manager. Ignore the flag with the attention icon for now, AD DS will be configured later. First DNS will be configured.



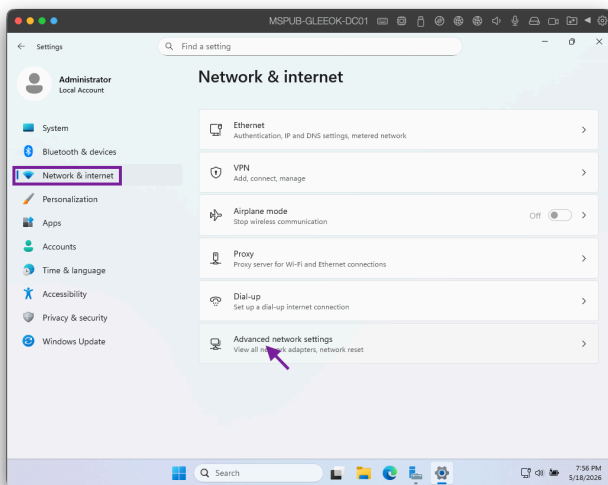
3. Before configuring DNS, a Static IP address needs to be set for MSPUB-GLEEOK-DC01.

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

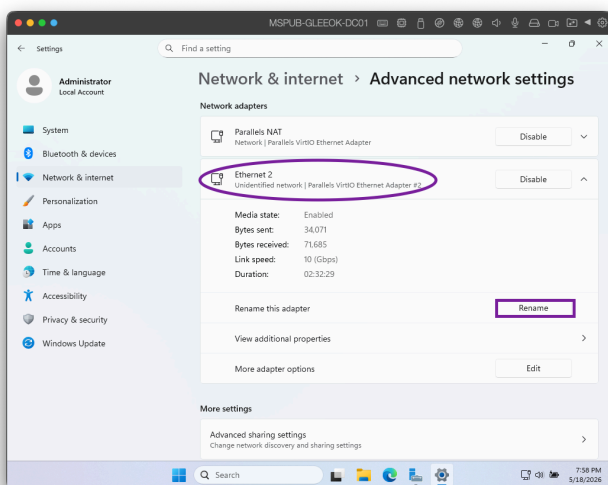
1. Right-click the “Windows charm” and select “Settings.”



2. In Settings on the left, click “Network & Internet.” Select “Advanced network settings.”

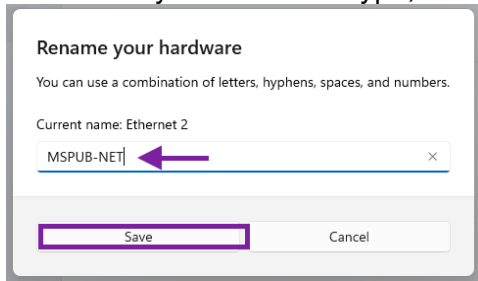


3. Expand “Ethernet 2.” Next to Rename this adapter, click the “Rename” button.

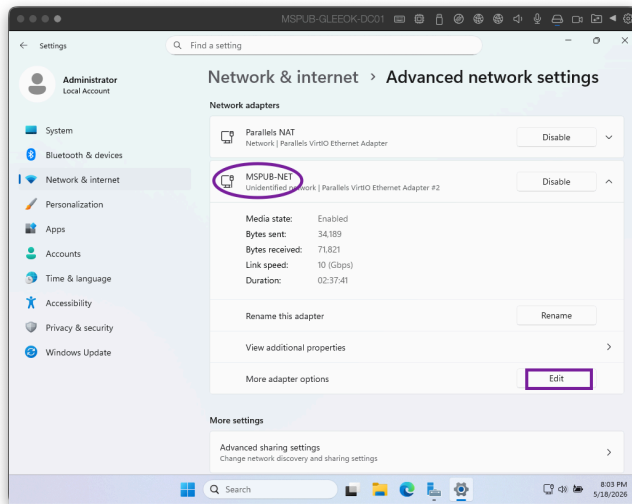


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

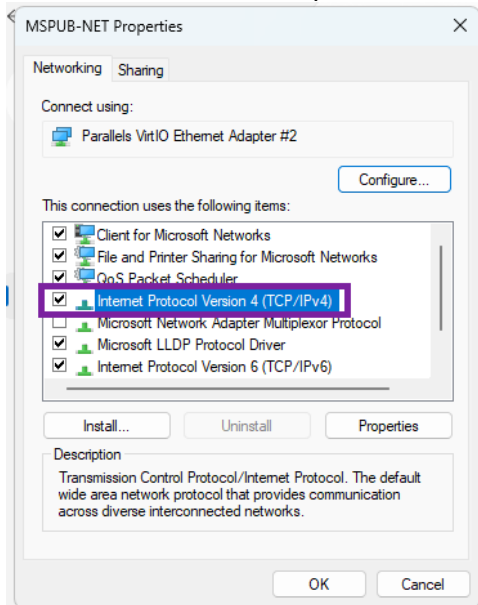
4. In Rename your hardware type, “MSPUB-NET” and click “Save.”



5. In Settings > Network & internet > Advanced network settings > MSPUB-NET, under More adapter options, click “Edit.”

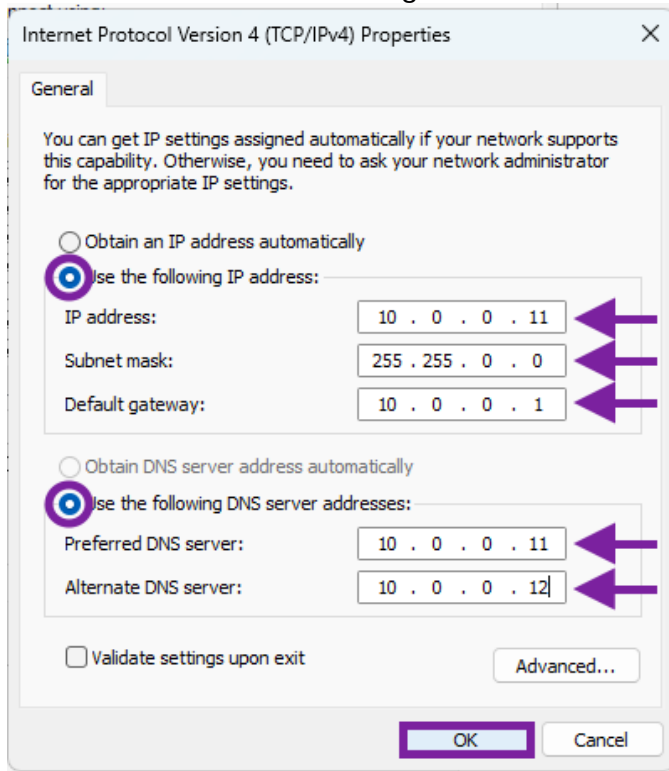


6. In the MSPUB-NET Properties windows double-click “Internet Protocol Version 4 (TCP/IPv4).”

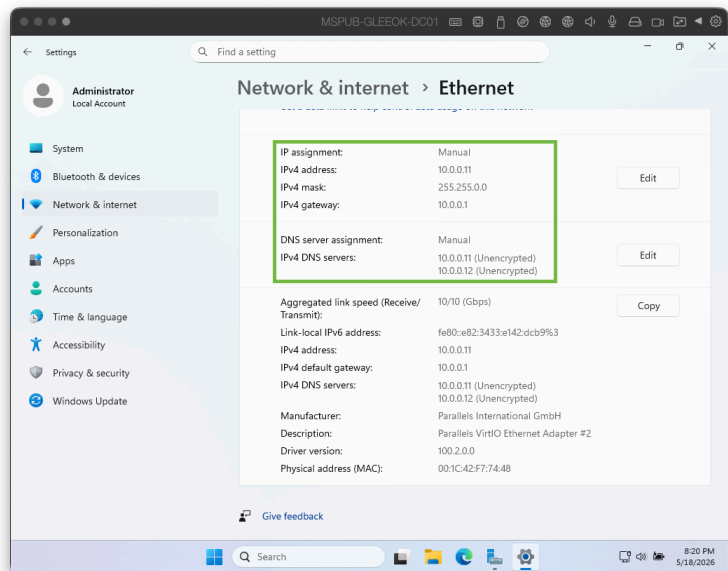
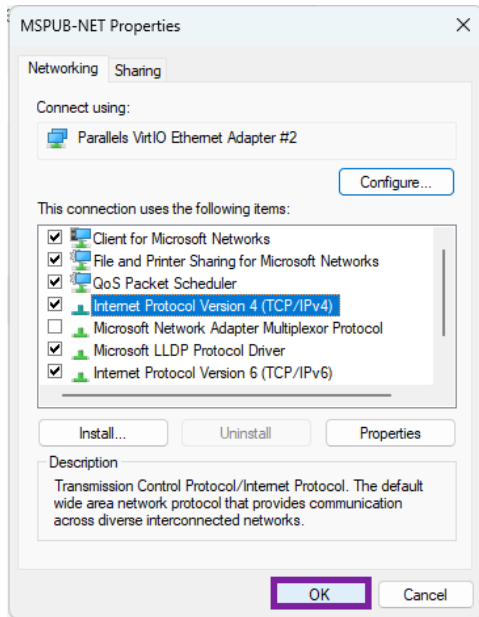


7. In the Internet Protocol Version 4 (TCP/IPv4) Properties windows configure the following:
- Select “Use the following IP address:
 - IP address: **10.0.0.11**
 - Subnet mask: **255.255.0.0**
 - Default gateway: **10.0.0.1**
 - Select “Use the following DNS server addresses”
 - Preferred DNS server: **10.0.0.11**

- Alternate DNS server: **10.0.0.12**
- Once all fields have been configured click “OK.”

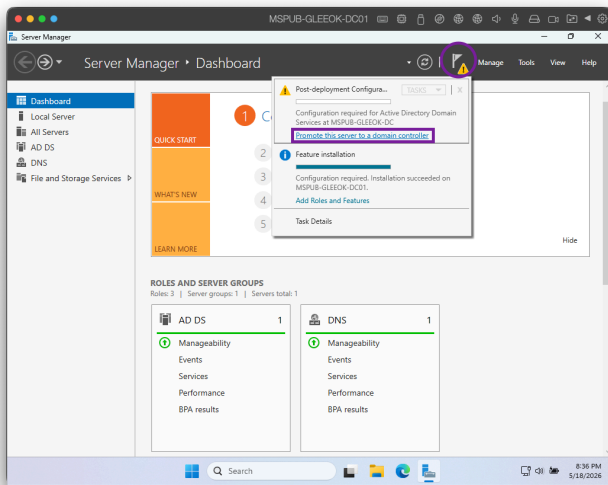


8. Back on the MSPUB-NET properties window click “OK.” The IP Address and DNS settings have been configured. For this lab it is okay that MSPUB-NET has no internet connection, Parallels NAT gives the VM internet access.

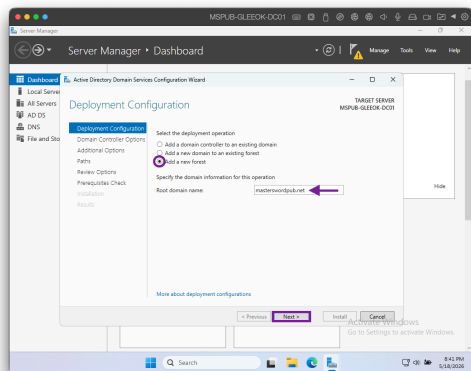


9. Close the Settings window by clicking the “X” in the upper right of the window.
4. If Server Manager was minimized, restore it from the Taskbar. Active Directory Domain Services (AD DS) will be configured with the masterswrodpub.net domain.
 1. In Server Manager click the “Flag” with the attention icon. There will be a Post-deployment Configuration notification, click the “Promote this server to a domain controller” hyperlink.

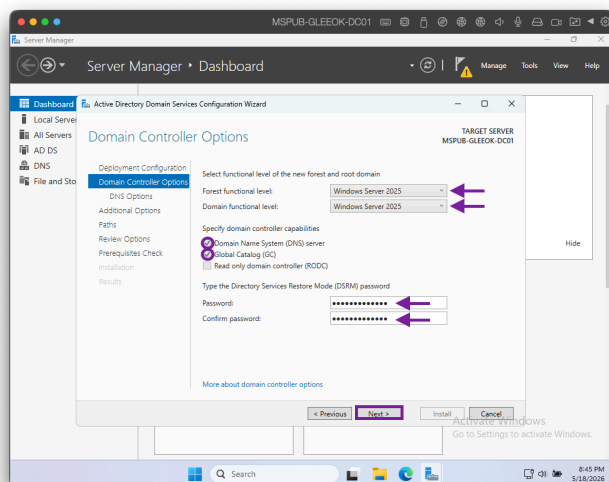
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



2. In Deployment configuration select “Add a new forest.” In the Root domain name field type “masterswordpub.net” and click “Next.”



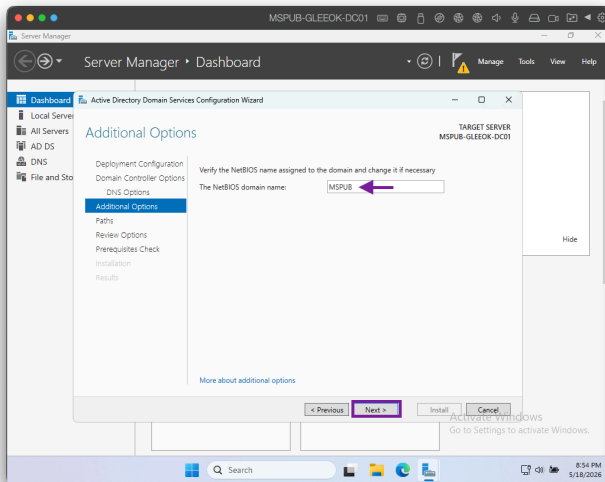
3. In Domain Controller Options configure the following:
 - Forest functional level: **Windows Server 2025**
 - Domain functional level: **Windows Server 2025**
 - **Tick:** Domain Name System (DNS) server
 - **Tick:** Global Catalog (GC)
 - Password: **CSNT253_2026#**
 - Confirm Password: **CSNT253_2026#**
 - Once configured click “Next”



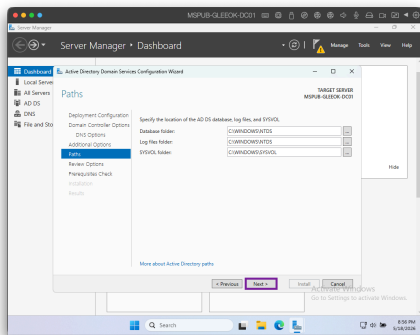
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Ignore the warning on DNS Options and click “Next.”

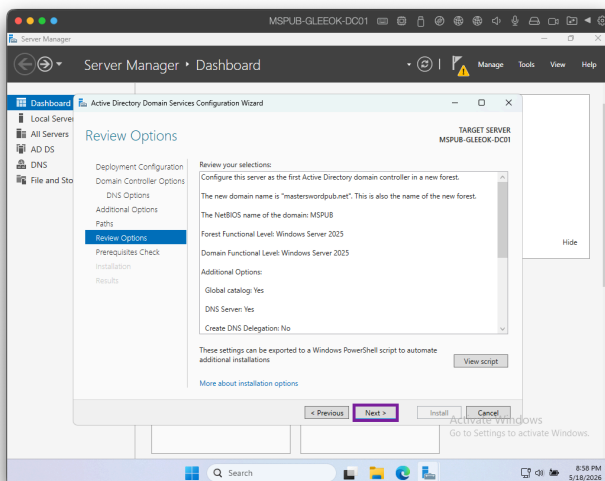
4. In Additional Options, change the NetBIOS domain name to “MSPUB” and click “Next.”



5. In Paths, leave the default and click “Next.”

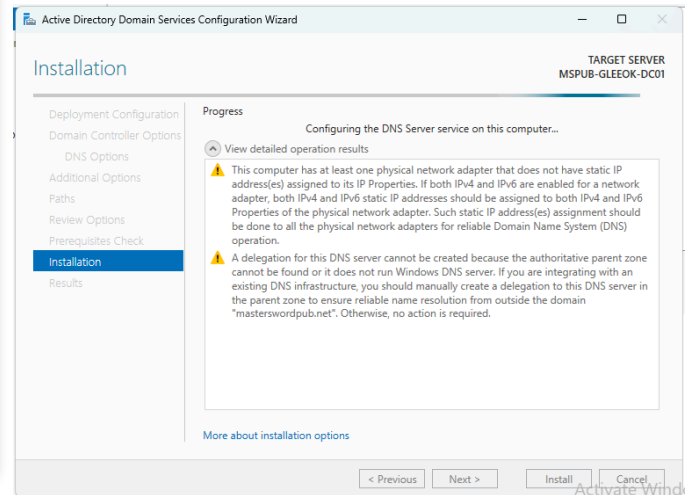
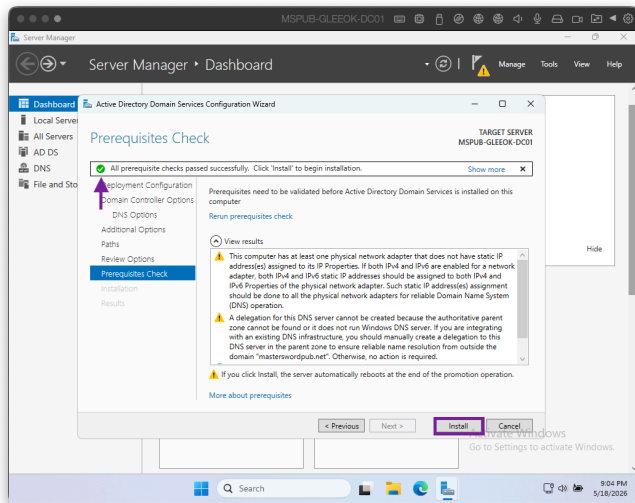


6. In Review Options, scroll through to confirm the confirmation, if everything looks correct click “Next.”

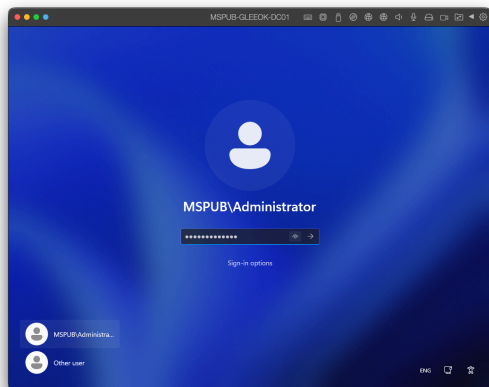


7. Active Directory Domain Services Configuration Wizard will run Prerequisites Checks. If the results give you a green check mark towards the top click Install, if it shows anything else fix the issues. The warnings shown in the results for this lab are normal and fine to proceed. Click “Install.” The configuration will begin installation.

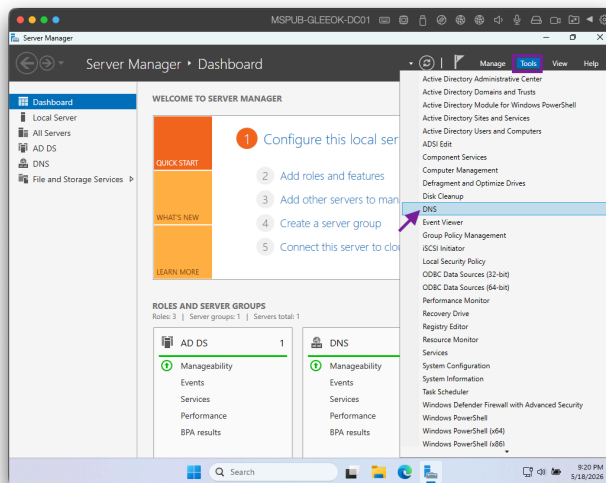
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



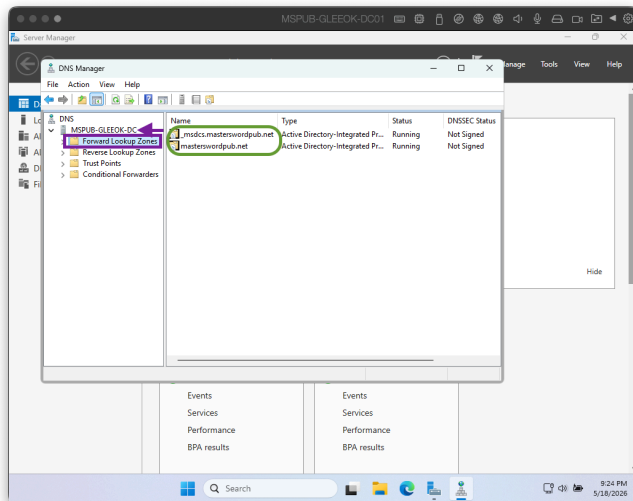
8. Once the installation has completed, the server will reboot automatically. It may take several minutes while it finishes applying the AD DS settings. Once the server restarts AD DS should now be setup. To login type the NetBIOS with the username “MSPUB/Administrator” using the password “CSNT253_2026#”.



9. Verify that DNS show the masterswordpub.net Forward Lookup Zones by:
1. Clicking “Tools” in Server Manager and selecting “DNS.”

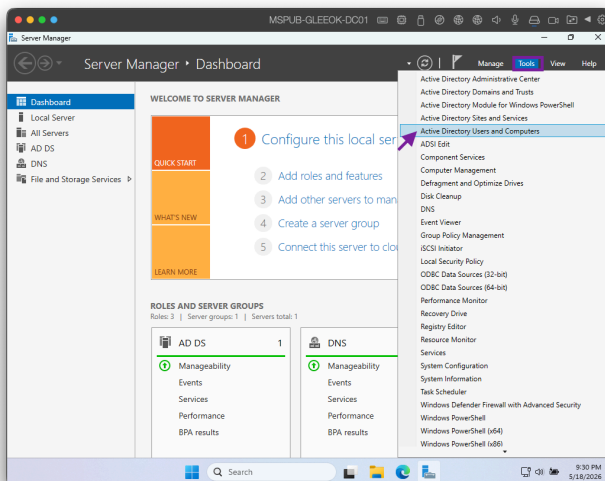


2. In DNS Manager expand “MSPUB-GLEEOK-DC” and selecting “Forward Lookup Zones.” It should display, “msdcs.masterswordpub.net” and “masterswordpub.net” and DNS has been setup correctly during the AD DS installation. Close DNS Manager.

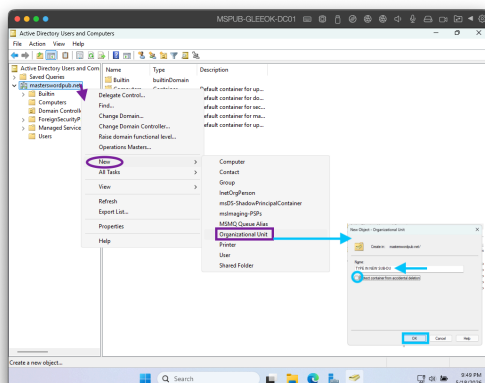


5. The masterswordpub.net FDQN (MSPUB NetBIOS) can now be configured with Organizational Units (OUs), add clients, and users using Active Directory Users and Computers.

1. In Server Manager click “Tools” and select “Active Directory Users and Computers.”



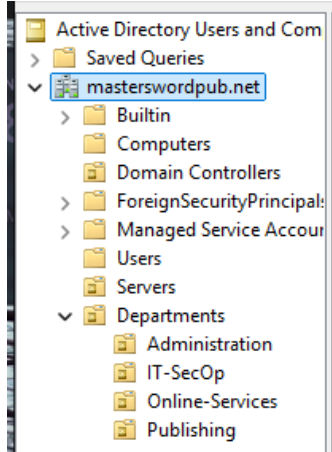
2. In Active Directory Users and Computers, expand “masterswordpub.net” to show the default Organizational Units (OUs). The only default OU that will be used is Computers. Custom ones will be created for Servers, and each department. To create a new OU, right click the parent OU, hover over “New,” and select “Organizational Unit.” The New Object -Organizational Unit opens, fill in the Name of the OU and deselect “Protect container from accidental deletion,” and click “OK.” Create New OUs within the appropriate OU hierarchy.



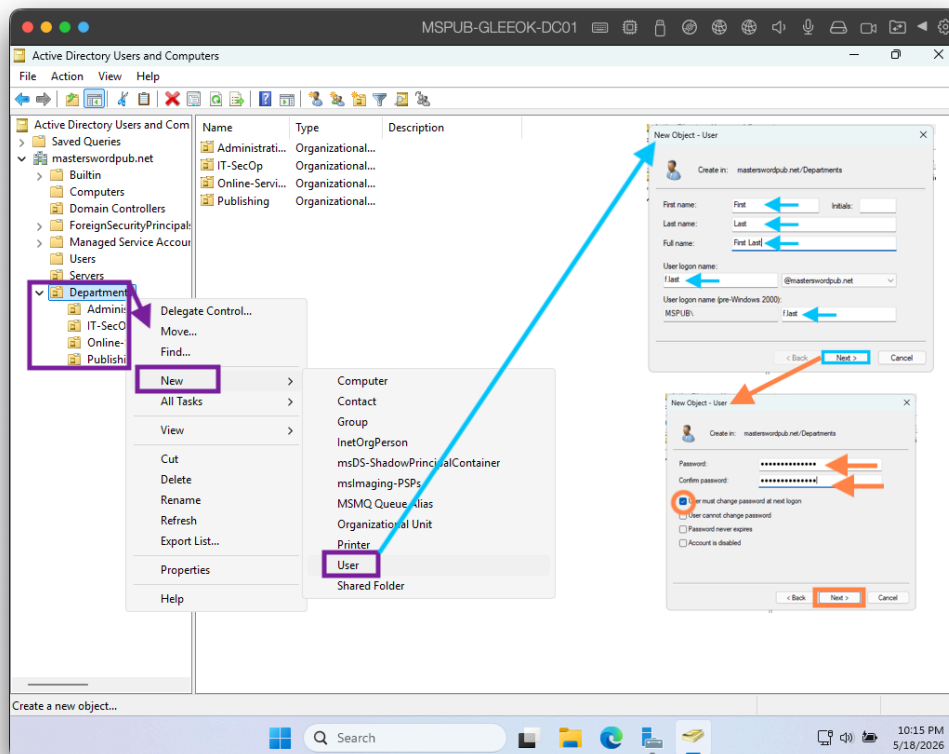
- masterswordpub.net

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Computers
- **Servers** (Create)
- **Departments** (Create)
 - **Administration** (Create)
 - **IT-SecOp** (Create)
 - **Online-Services** (Create)
 - **Publishing** (Create)
- This is what the structure will look like:

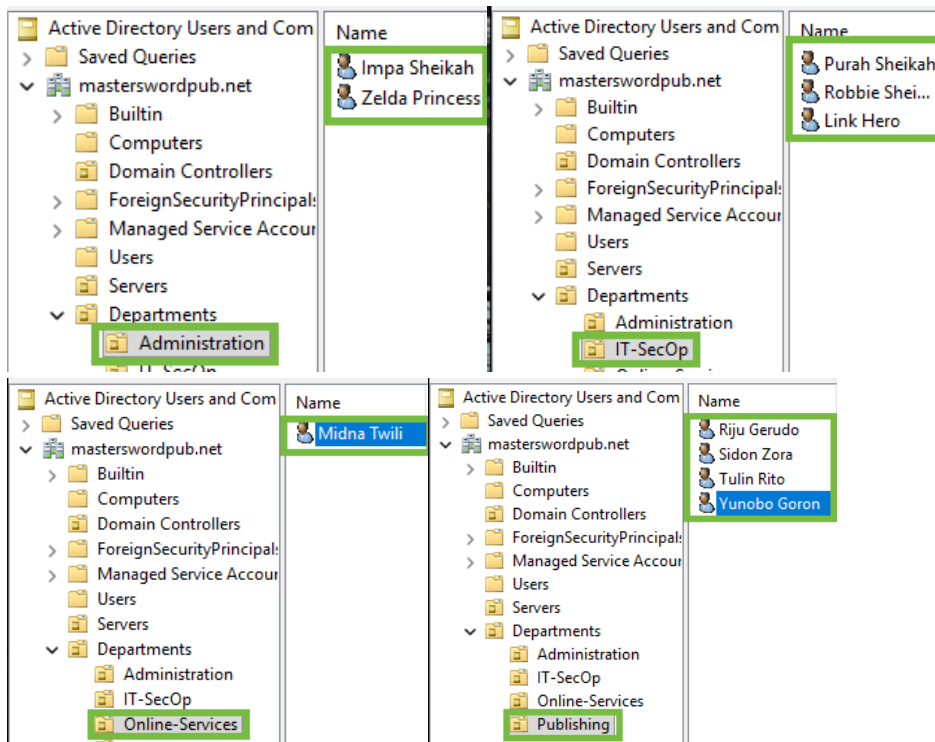


3. The Employee user accounts will need to be added to each of their respective Department OU. To create a new user right click the Department OU, hover-over “New”, select “User.” In the New Object - User window enter in the users First Name, Last Name, Full Name, and User logon Name (f.lastname), then click “Next.” Enter the default password, “Hyrul3W@rr10r\$” and confirm it. Tick, “User must change password at next logon,” then click “Next.” Verify the information, and click “Finish.” Use the Employee Roster to add all 10 user accounts.

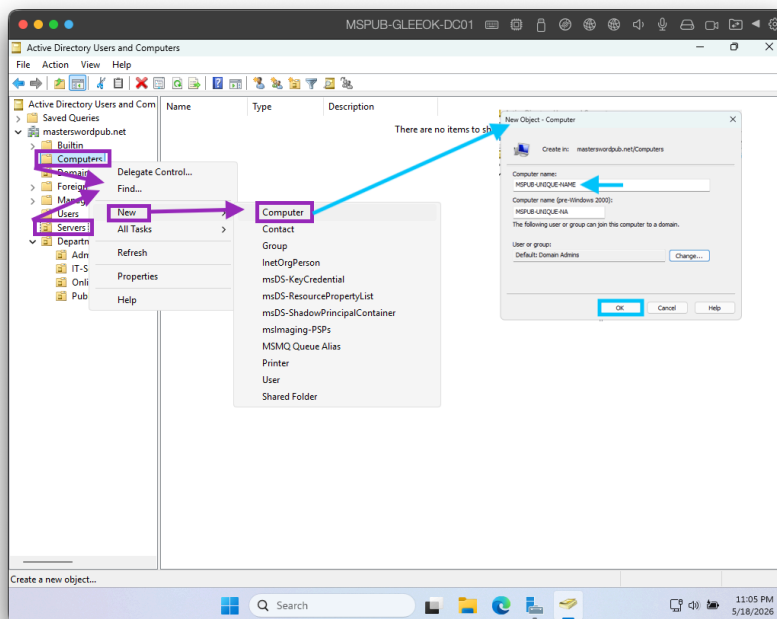


The users should in each department OU as follows:

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



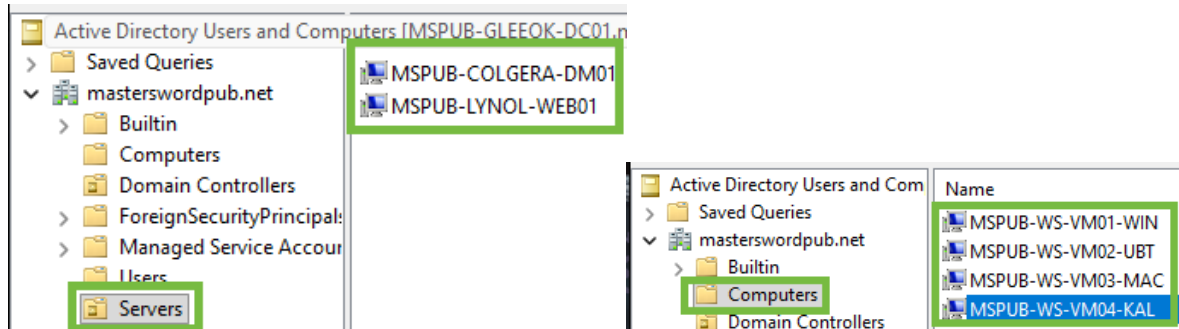
- Computers and servers will need to have placeholders added to their respective OUs. To add a new Computer right click the OU, hover-over “New,” and click “Computer.” In the New Object - Computer window enter in the unique computer name, then click “OK.”



Add the following Computer in their respective OUs:

- Servers:
 - MSPUB-COLGERA-DM01
 - MSPUB-LYNEL-WEB01
- Computers:
 - MSPUB-WS-VM01-WIN
 - MSPUB-WS-VM02-UBT
 - MSPUB-WS-VM03-MAC
 - MSPUB-WS-VM04-KAL

- The structure should look like this:



5. Close Active Directory Users and Computers.

MSPUB Network: IP Addressing, DNS Configuration Settings, & Domain Join

Scenario Information

With the new implementations of MSPUB-GLEEOK-DC01 using Active Directory Domain Services (AD DS) and DNS, the client machines and additional two servers need to be configured. New IP schema needs to be configured, DNS settings need to be updated, as well as the systems joining the new Domain Services.

MSPUB-GLEEOK-DC01 DNS & AD DS Settings:

FQDN	NetBIOS	IP Address	Router/Gateway	Subnet Mask	DNS
<u>masterswordpub.net</u>	MSPUB	10.0.0.11	10.0.0.1	255.255.0.0	10.0.0.11 10.0.0.12

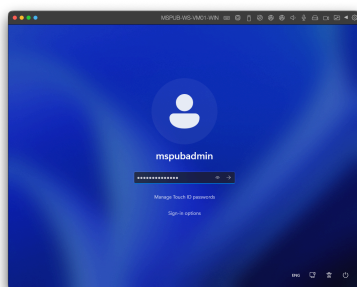
The following settings will be configured on each of the 4 client devices:

Hostname	IP Address	Router/Gateway	Subnet Mask	DNS
MSPUB-WS-VM01-WIN	10.0.0.101	10.0.0.1	255.255.0.0	10.0.0.11 10.0.0.12
MSPUB-WS-VM02-UBT	10.0.0.102	10.0.0.1	255.255.0.0	10.0.0.11 10.0.0.12
MSPUB-WS-VM03-MAC	10.0.0.103	10.0.0.1	255.255.0.0	10.0.0.11 10.0.0.12
MSPUB-WS-VM04-KAL	10.0.0.104	10.0.0.1	255.255.0.0	10.0.0.11 10.0.0.12
MSPUB-COLGERA-DM01	10.0.0.12	10.0.0.1	255.255.0.0	10.0.0.11 10.0.0.12
MSPUB-LYNEL-WEB01	10.0.0.13	10.0.0.1	255.255.0.0	10.0.0.11 10.0.0.12

Configuring Network Settings in Windows 11

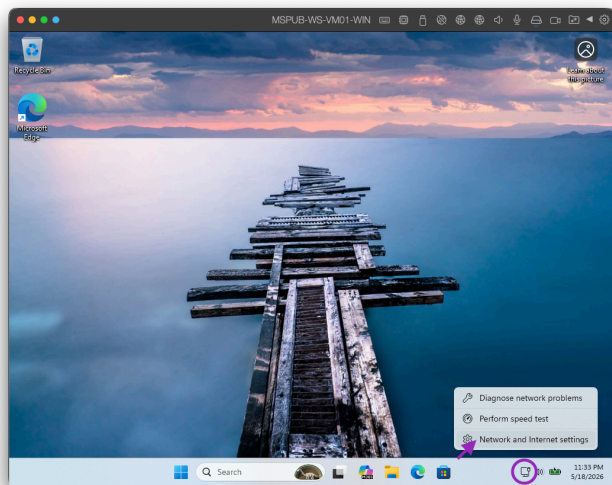
The Windows client MSPUB-WS-VM01-WIN will be configured with a Static IP address 10.0.0.101 and must point to the DNS server configured on MSPUB-GLEEOK-DC01, 10.0.0.11, to be able to connect to the Active Directory.

1. Log into MSPUB-WS-VM01-WIN using the “mspubadmin” user and type the password “CSNT253_2026#”.

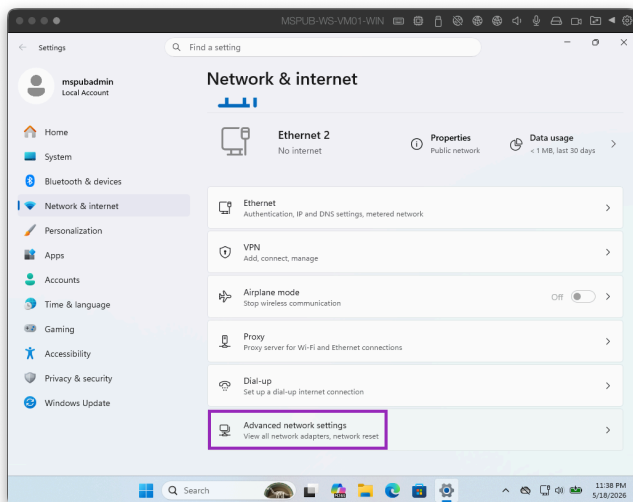


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

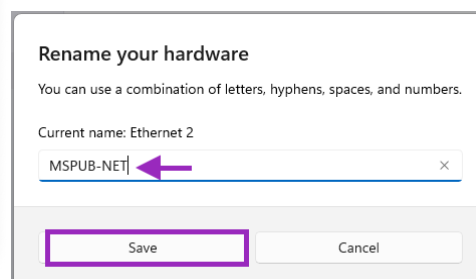
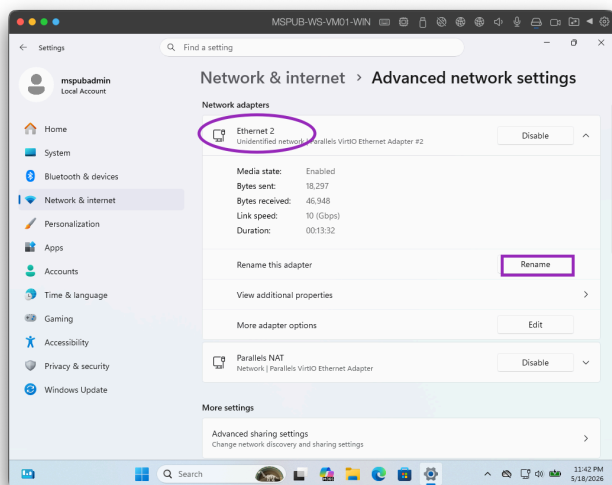
2. On the taskbar right click the “Network icon” and select “Network and Internet settings.”



3. On Network & internet settings click “Advanced network settings.”

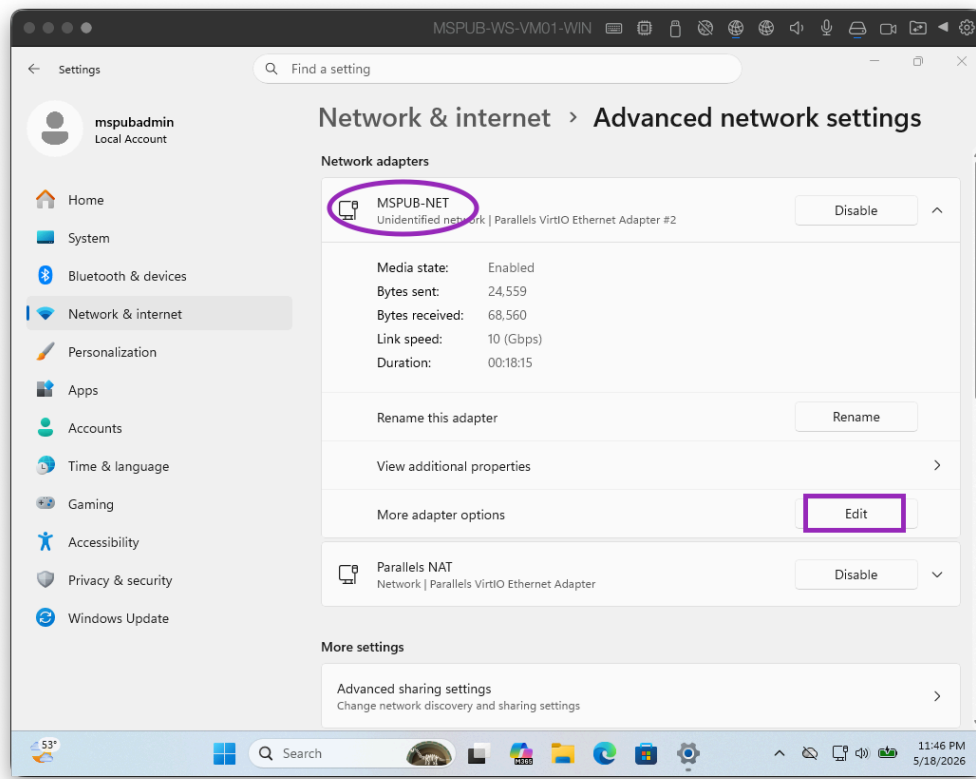


4. On Advanced network settings expand “Ethernet 2.” Under Rename this adapter click “Rename.” Change the name to “MSPUB-NET” and click “Save.”

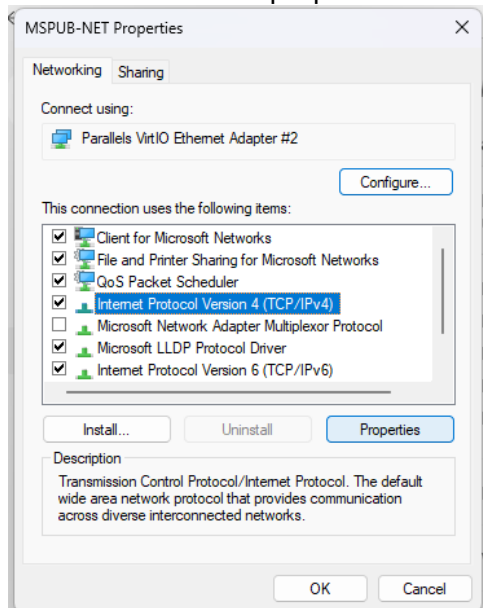


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

5. Ethernet 2 has been renamed to MSPUB-NET. Under More adapter options click “Edit.”



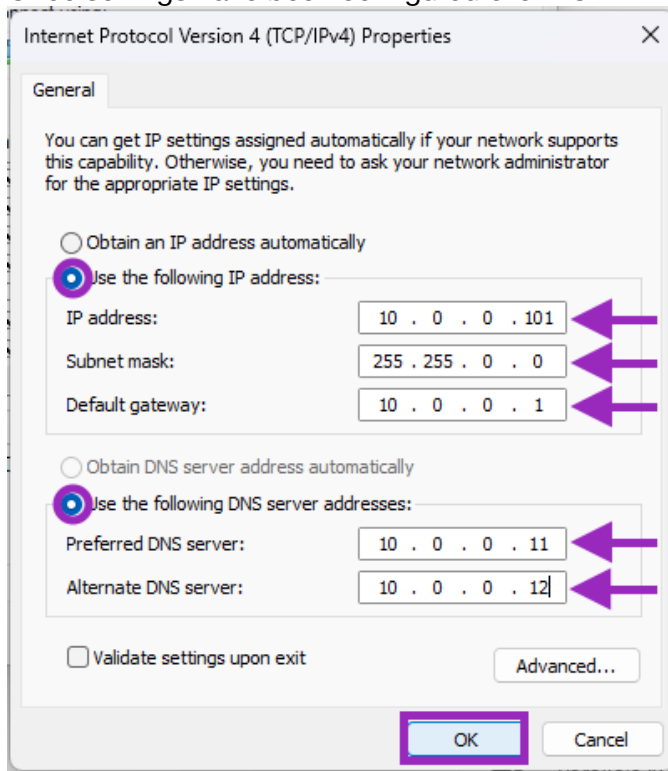
6. In the MSPUB-NET properties windows double click “Internet Protocol Version 4 (TCP/IPv4)”.



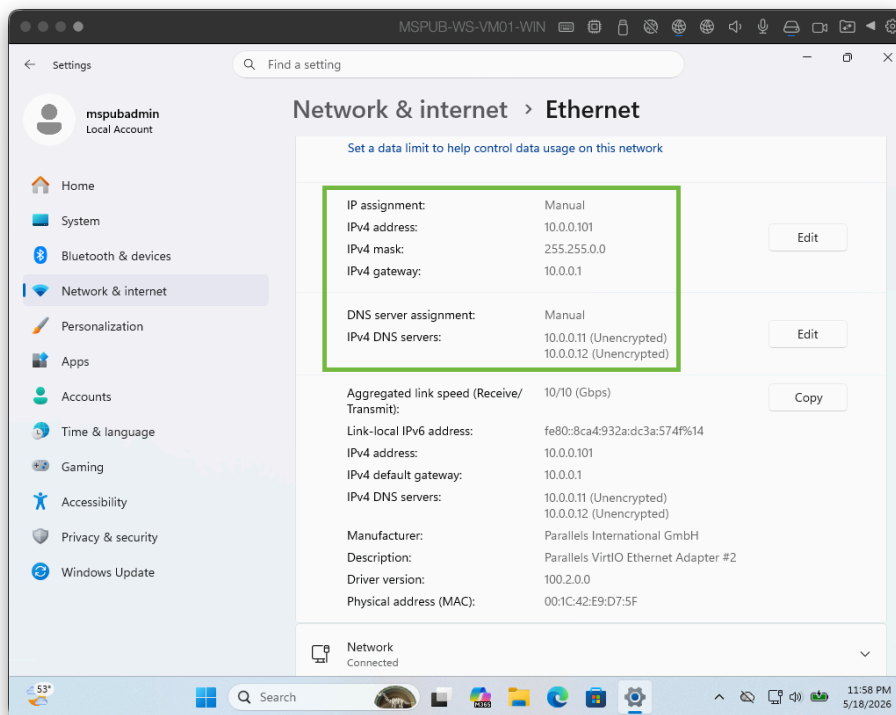
7. In the Internet Protocol Version 4 (TCP/IPv4) Properties window configure the following:

- Select “Use the following IP address:”
 - IP address: **10.0.0.101**
 - Subnet mask: **255.255.0.0**
 - Default gateway: **10.0.0.1**
- Select “Use the following DNS server address:”
 - Preferred DNS Server: **10.0.0.11**
 - Alternate DNS Server: **10.0.0.12**

- Once settings have been configured click “OK.”



- Click “OK” on the MSPUB-NET Properties. The IP and DNS settings are now applied. Close the Settings window.



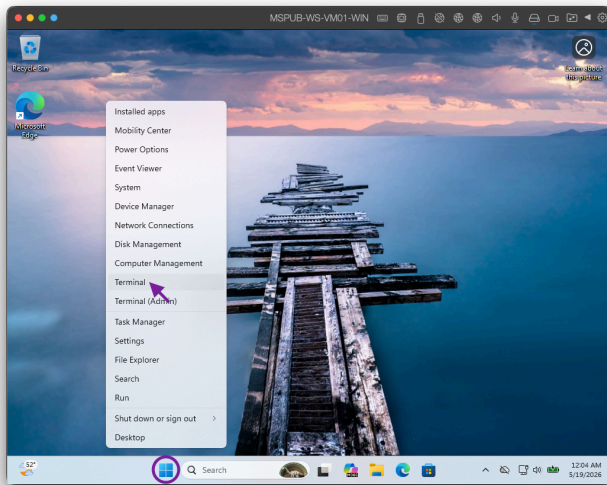
Adding Windows 11 Client to the MSPUB Domain

Now that the DNS are configured, MSPUB-WS-VM01-WIN can be added to the MSPUB Active Directory hosted MSPUB-GLEEOK-DC01.

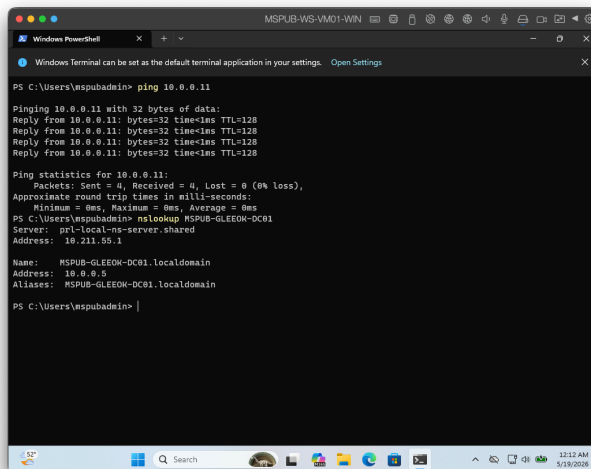
- Confirm that this client can look up the Domain Control and Ping the server by IP address.

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

1. From the Taskbar right click the “Windows charm” and click “Terminal.”

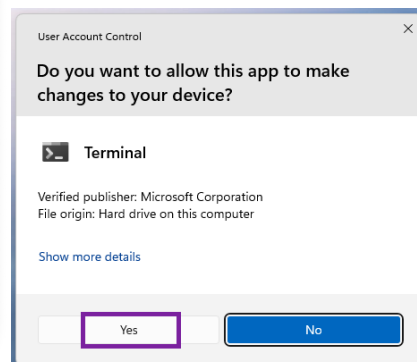
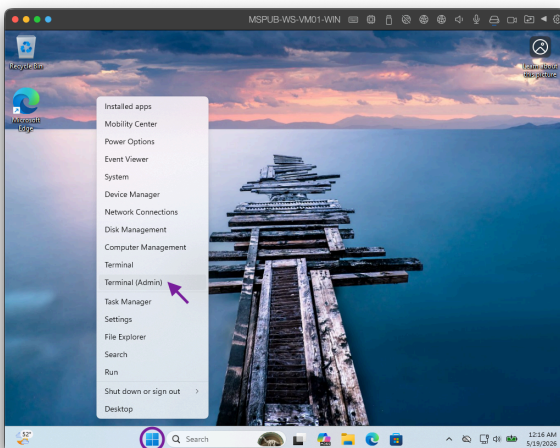


2. Enter in the following commands:
 - ping 10.0.0.11 - there should be no packet loss
 - nslookup MSPUB-GLEEK-DC01 - it should return with the IP address 10.0.0.11
 - Close the Terminal window.



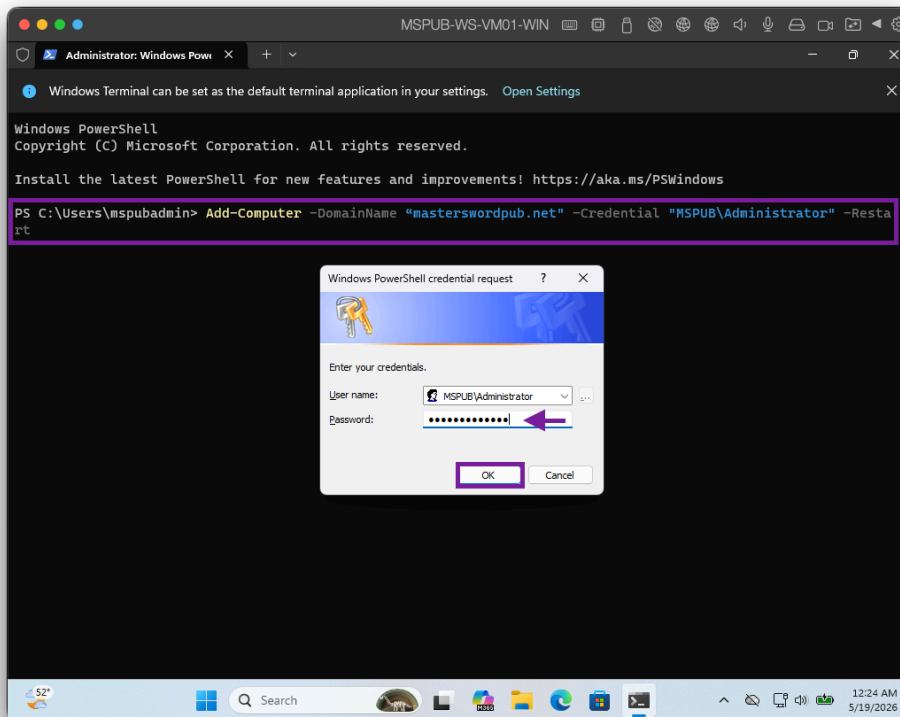
10. This VM can now be added to the domain, using Terminal with administrative rights:

1. Right click the “Windows charm” on the Taskbar and select “Terminal (Admin).” Click “Yes” on the User Account Control (UAC) popup.



Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

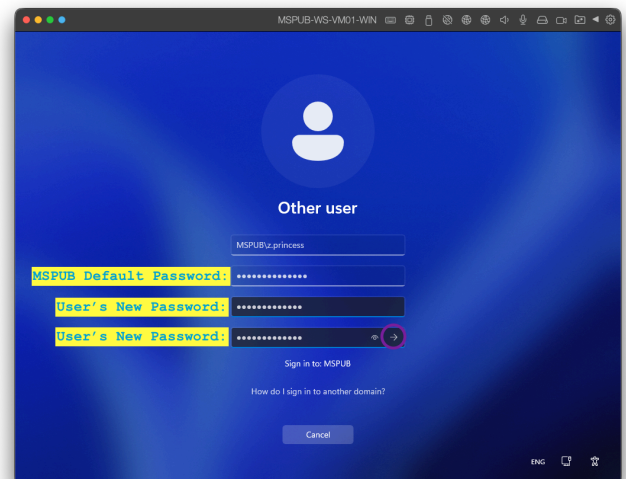
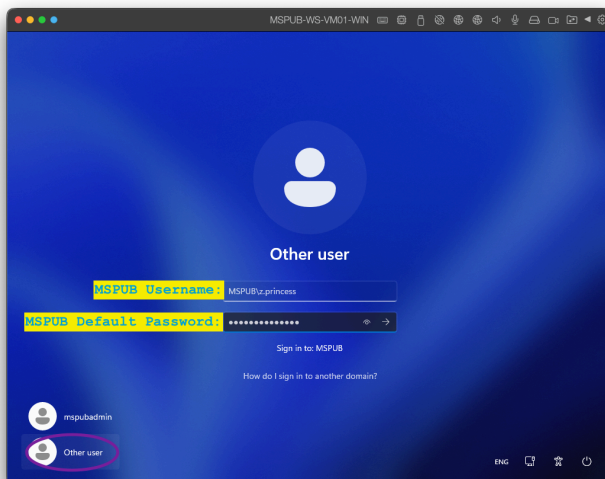
2. In the Terminal type the following command and press enter:
Add-Computer -DomainName "masterswordpub.net" -Credential "MSPUB\Administrator" -Restart
When prompted enter in the password for MSPUB\Administrator account on the domain controller, "CSNT253_2026#" and click "OK."



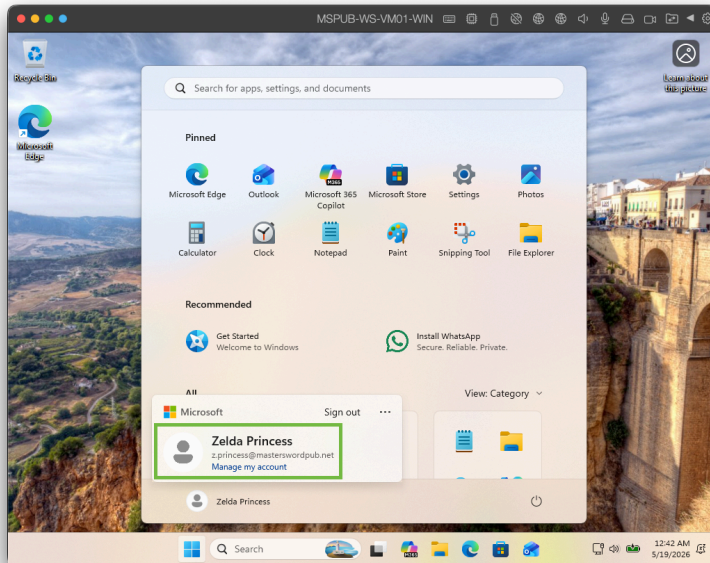
3. Type "Y" to accept the shortened computer name change and press enter. The VM will then restart. It may take a few moments for the machine to restart and apply the domain's Active Directory settings.

```
NetBIOS name will be truncated.  
The NetBIOS name of the computer is limited to 15 bytes, which is 15 characters in this case. The NetBIOS  
name will be shortened to "MSPUB-WS-VM01-W", which may cause conflicts under NetBIOS name resolution. Do you  
wish to continue?  
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
```

4. Once the machine reboots test that a user within the active directory can sign in by clicking "Other User." In the example it was tested using the username MSPUB\z.princess with the password, "Hyrul3W@rr10r\$". Note: the user will be required to change their password, use "CSNT253_2026#".



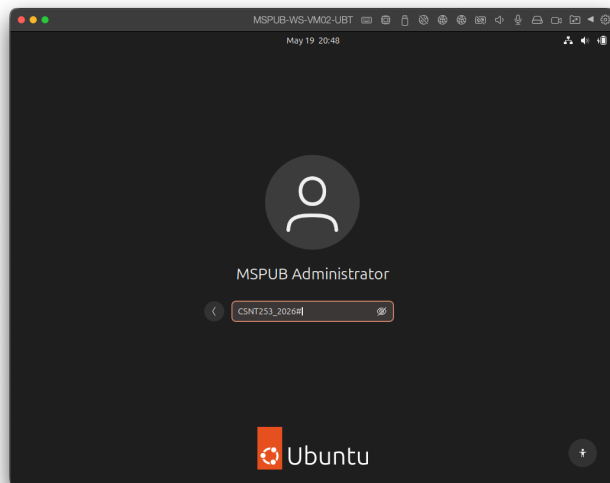
5. MSPUB-WS-VM01-WIN has successfully joined the masterswordpub.net domain. The user can now login using their MSPUB username and password.



Configuring Network Settings in Ubuntu Desktop

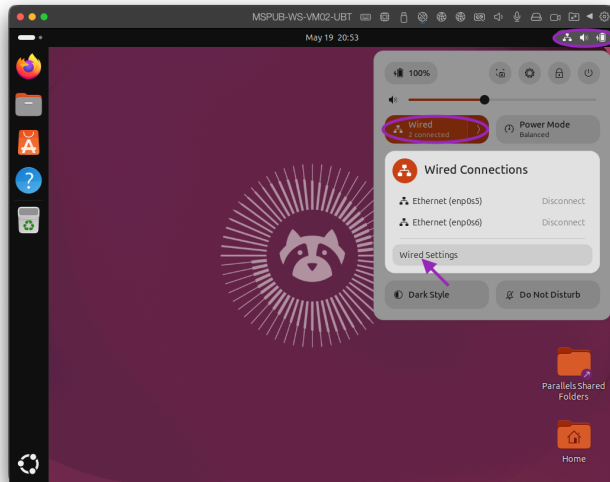
The Ubuntu Desktop client MSPUB-WS-VM02-UBT will be configured with a Static IP address, 10.0.0.102 and must point to the DNS server configured on MSPUB-GLEEOK-DC01, 10.0.0.11, to be able to connect to the Active Directory.

1. On MSPUB-WS-VM02-UBT login using the “MSPUB Administrator” account using the password “CSNT253_2026#.”

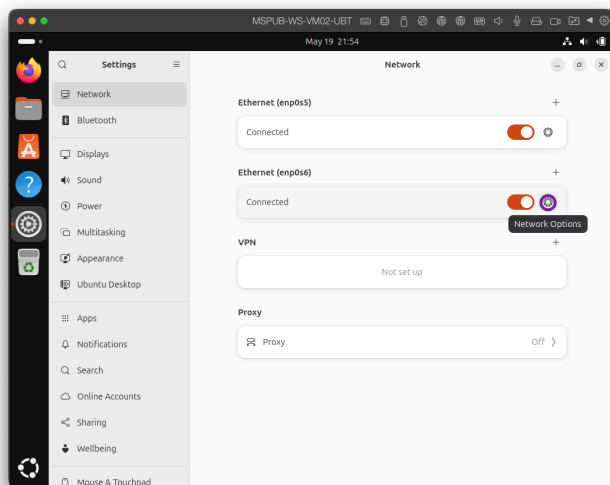


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

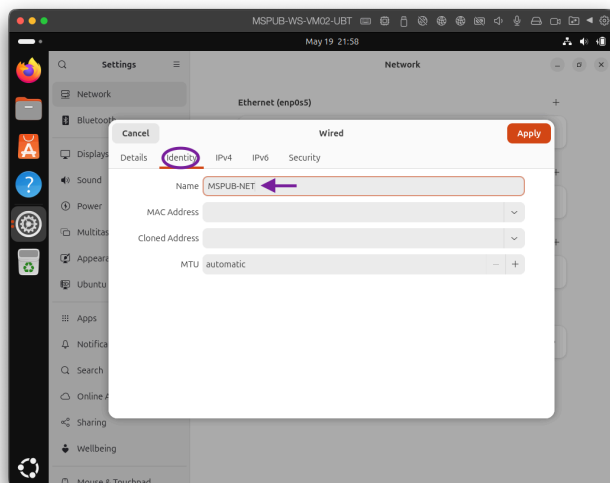
- Click on the “Indicators menu” in the top right. Click on “Wired” (will display as Wireless if connected to WiFi instead). Click on “Weird Settings.”



- This will open Settings > Network. Click on the “Network Options” gear under Ethernet (enp0s6).



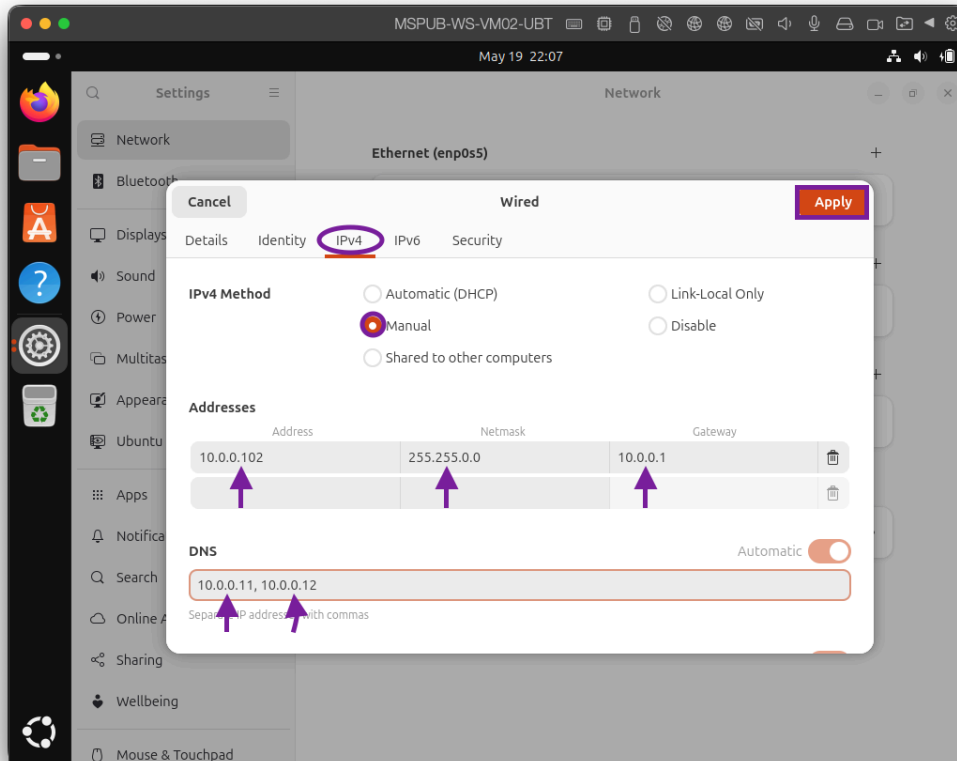
- In the Network Options: Wired window click the “Identify” tab. Rename the “Wired connection 1” to “MSPUB-NET.”



- Click on the “IPv4” tab. Configure the following:

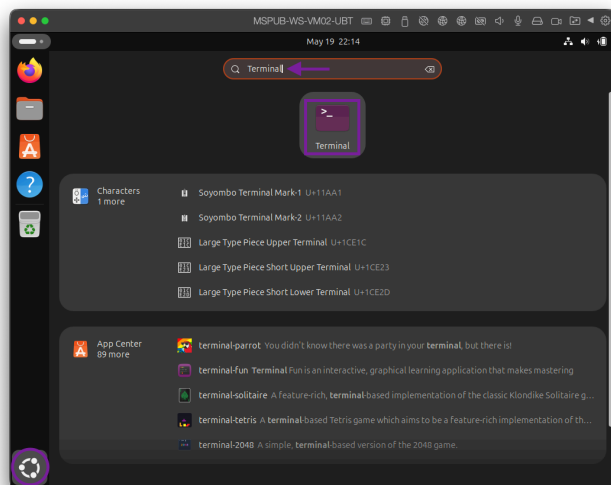
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- IPv4 Method: **Manual**
- Addresses
 - Address: **10.0.0.102**
 - Netmask: **255.255.0.0**
 - Gateway: **10.0.0.1**
- DNS: **10.0.0.11, 10.0.0.12**
- Click “Apply” once configured.



6. Close the Settings window.

7. To confirm the new settings have been applied there is a command that will be used to check. Click on the “Ubuntu charm” in the lower left corner of the taskbar and type “Terminal” in the search field. Click “Terminal.”



8. In the Terminal window type, “ifconfig” and press enter. Look for enp0s6 and it will display the updated IP address and subnet mask.


```

mspubadmin@MSPUB-WS-VM02-UBT:~$ ifconfig
enp8s5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.211.55.16 netmask 255.255.255.0 broadcast 10.211.55.255
    inet6 fe80::21c:42ff:fe5e:5fe6 prefixlen 64 scopeid 0x20<link>
    inet6 fdb2:2c26:f4e4:0:21c:42ff:fe5e:5fe6 prefixlen 64 scopeid 0x0<global>
    ether 00:1c:42:5e:5f:e0 txqueuelen 1000 (Ethernet)
    RX packets 85041 bytes 123892365 (123.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24372 bytes 1416748 (1.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp8s6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.102 netmask 255.255.0.0 broadcast 10.0.255.255
    inet6 fe80::a1a:9177:f9e:7712 prefixlen 64 scopeid 0x20<link>
    ether 00:1c:42:bf:3c:ec txqueuelen 1000 (Ethernet)
    RX packets 1556 bytes 186718 (186.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 755 bytes 90716 (90.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

mspubadmin@MSPUB-WS-VM02-UBT:~$
  
```

9. While Terminal is open make sure MSPUB-GLEEOK-DC01 can be pinged and looked. Type the following commands into Terminal:
 - **ping -c 5 10.0.0.11**
 - **nslookup MSPUB-GLEEOK-DC01**
 - After pinging there should be no packet loss and nslook should resolve the IP address (10.0.0.11) for MSPUB-GLEEOK-DC01.

```

mspubadmin@MSPUB-WS-VM02-UBT:~$ ping -c 5 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data:
 64 bytes from 10.0.0.11: icmp_seq=1 ttl=128 time=0.733 ms
 64 bytes from 10.0.0.11: icmp_seq=2 ttl=128 time=0.810 ms
 64 bytes from 10.0.0.11: icmp_seq=3 ttl=128 time=0.936 ms
 64 bytes from 10.0.0.11: icmp_seq=4 ttl=128 time=1.20 ms
 64 bytes from 10.0.0.11: icmp_seq=5 ttl=128 time=1.18 ms

--- 10.0.0.11 ping statistics ---
 5 packets transmitted, 5 received, 0% packet loss, time 4085ms
 rtt min/avg/max/mdev = 0.733/0.970/1.195/0.188 ms

mspubadmin@MSPUB-WS-VM02-UBT:~$ nslookup MSPUB-GLEEOK-DC01
Server:      127.0.0.53
Address:     127.0.0.53#53

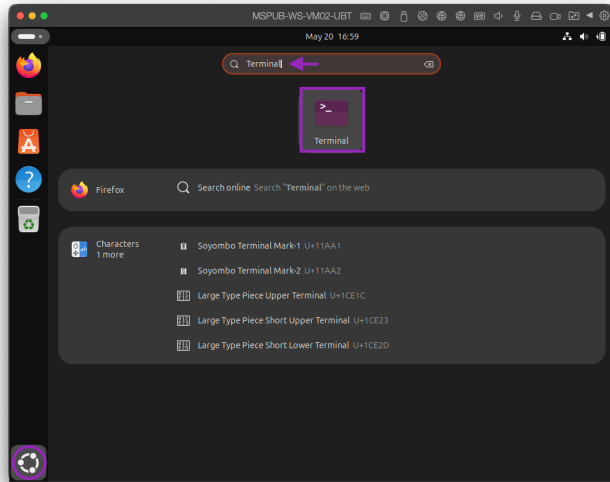
Non-authoritative answer:
MSPUB-GLEEOK-DC01.localdomain canonical name = MSPUB-GLEEOK-DC01.localdomain.
Name:   MSPUB-GLEEOK-DC01.localdomain
Address: 10.0.0.5
MSPUB-GLEEOK-DC01.localdomain canonical name = MSPUB-GLEEOK-DC01.localdomain.

mspubadmin@MSPUB-WS-VM02-UBT:~$
  
```

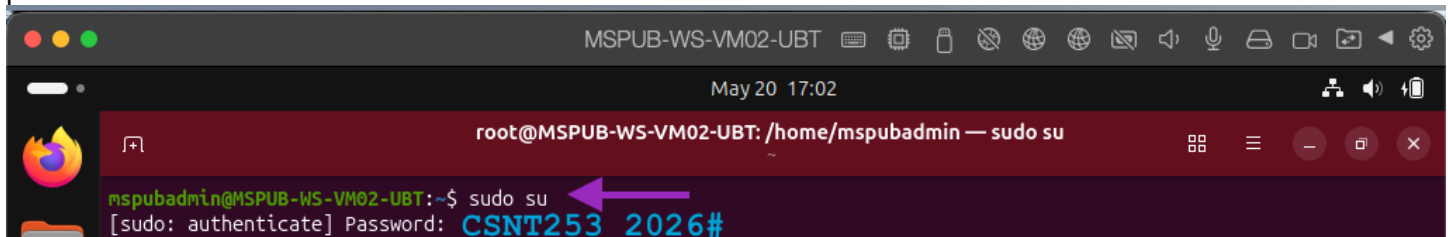
Adding Ubuntu Desktop to the MSPUB Domain

Now that the DNS are configured, MSPUB-WS-VM02-UBT can be added to the MSPUB Active Directory hosted MSPUB-GLEEOK-DC01. In newer versions of Ubuntu Desktop there is no GUI interface to configure Active Directory post installation. Entering commands in Terminal is the only way to configure AD.

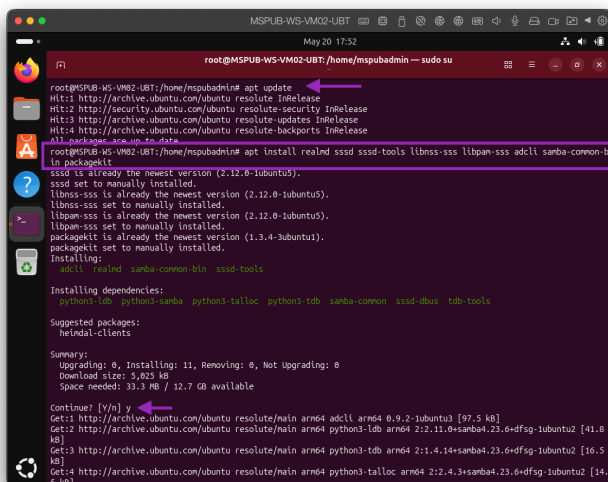
1. On the left taskbar click on the “Ubuntu charm.” Type “Terminal” in the search field. Click “Terminal.”



2. In terminal type “sudo su” to switch to the Root user. You maybe required to enter in the mspubadmin password to continue.



3. Type these commands separately:
 - sudo apt update
 - sudo apt install realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin packagekit
 - Type “Y” if prompted throughout the dependencies installation (Note: it may take several minutes to install these 6 packages).



Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

4. To make sure the machine can see the AD domain type “sudo realm discover masterswordpub.net”

```
root@MSPUB-WS-VM02-UBT: /home/mspubadmin — sudo su
root@MSPUB-WS-VM02-UBT:/home/mspubadmin# realm discover masterswordpub.net
masterswordpub.net
type: kerberos
realm-name: MASTERSWORDPUB.NET
domain-name: masterswordpub.net
configured: no
server-software: active-directory
client-software: sssd
required-package: sssd-tools
required-package: sssd
required-package: libnss-sss
required-package: libpam-sss
required-package: adcli
required-package: samba-common-bin
root@MSPUB-WS-VM02-UBT:/home/mspubadmin#
```

5. If the AD domain is visible type “sudo realm join -v masterswordpub.net -U Administrator” to join the domain. Enter the username “Administrator” with the password “CSNT253_2026#”

```
root@MSPUB-WS-VM02-UBT:/home/mspubadmin# realm join masterswordpub.net -U Administrator
Password for Administrator: CSNT253_2026#
root@MSPUB-WS-VM02-UBT:/home/mspubadmin#
```

6. Since there is no response message, verify that the machine has joined the AD domain.

```
root@MSPUB-WS-VM02-UBT: /home/mspubadmin — sudo su
root@MSPUB-WS-VM02-UBT:/home/mspubadmin# realm list
masterswordpub.net
type: kerberos
realm-name: MASTERSWORDPUB.NET
domain-name: masterswordpub.net
configured: kerberos-member
server-software: active-directory
client-software: sssd
required-package: sssd-tools
required-package: sssd
required-package: libnss-sss
required-package: libpam-sss
required-package: adcli
required-package: samba-common-bin
login-formats: %u@masterswordpub.net
login-policy: allow-realm-logins
root@MSPUB-WS-VM02-UBT:/home/mspubadmin#
```

7. It is important to allow Domain Users to have their own directories so to enable Home Directory Creation type the following commands:

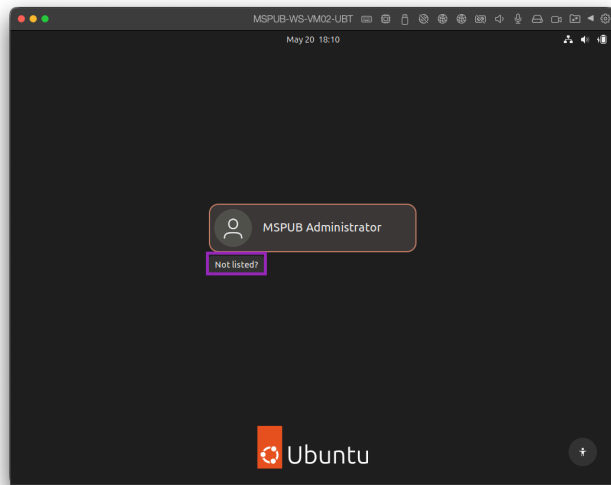
- sudo pam-auth-update --enable mkhomedir
- Sudo systemctl restart sssd

```
root@MSPUB-WS-VM02-UBT: /home/mspubadmin — sudo su
root@MSPUB-WS-VM02-UBT:/home/mspubadmin# sudo pam-auth-update --enable mkhomedir
root@MSPUB-WS-VM02-UBT:/home/mspubadmin# sudo pam-auth-update
root@MSPUB-WS-VM02-UBT:/home/mspubadmin# sudo systemctl restart sssd
root@MSPUB-WS-VM02-UBT:/home/mspubadmin#
```

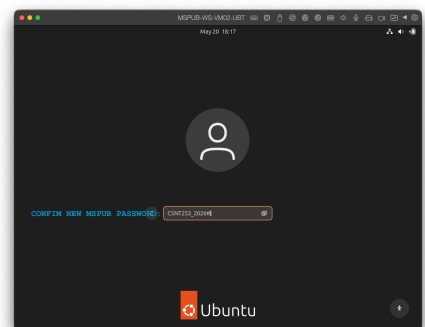
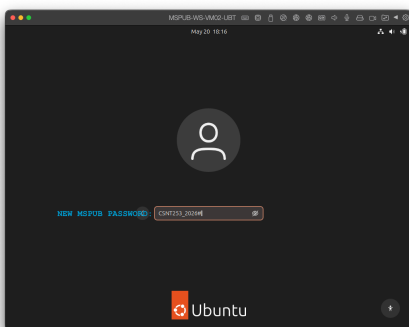
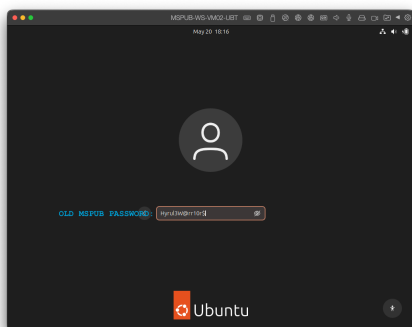
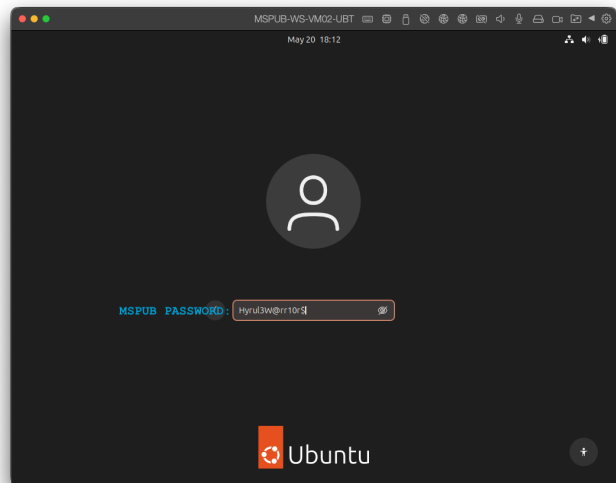
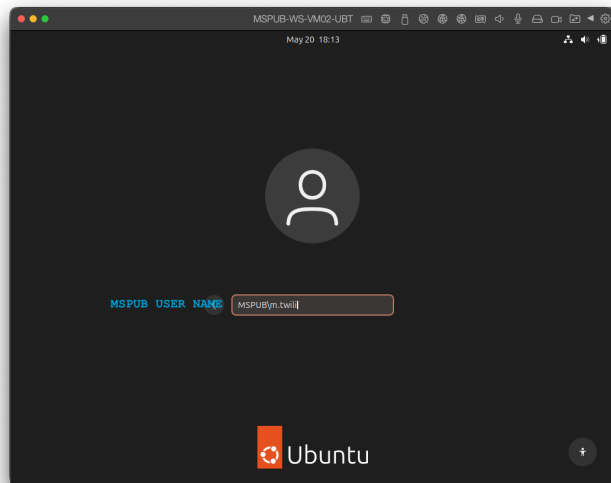
8. Type “sudo reboot” to restart the system.

```
root@MSPUB-WS-VM02-UBT:/home/mspubadmin# sudo reboot
```

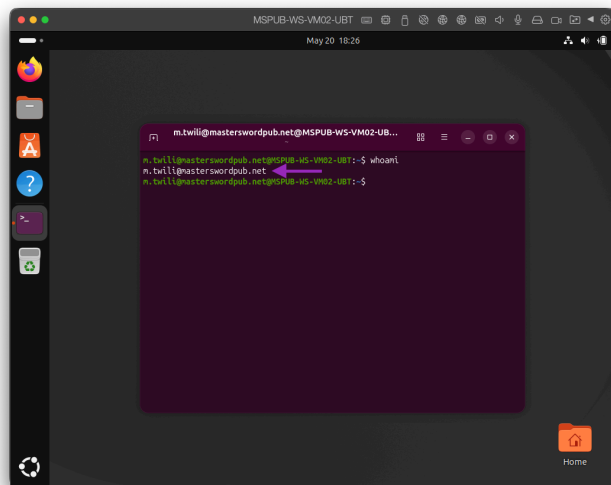
9. Click on the “Not listed?” Hyperlink on the login window.



10. Login using one of the MSPUB Domain User accounts and passwords. In the example it was tested using the username MSPUB\m.twili with the password, “Hyru13W@rr10r\$”. Note: the user will be required to change their password, use “CSNT253_2026#”. If prompted to “Create a mobile account?” Click “Create Now.”



11. Once logged in MSPUB-WS-VM02-UBT has successfully joined the MSPUB Domain.



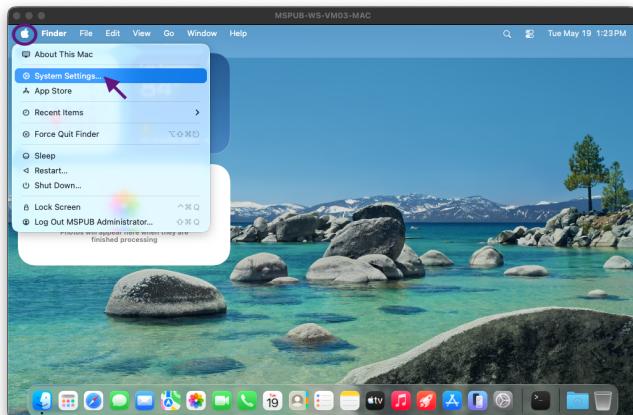
Configuring Network Settings in macOS

The macOS client MSPUB-WS-VM03-MAC will be configured with a Static IP address, 10.0.0.103 and must point to the DNS server configured on MSPUB-GLEEOK-DC01, 10.0.0.11, to be able to connect to the Active Directory.

1. On MSPUB-WS-VM03-MAC login using the “MSPUB Administrator” user account using the password “CSNT253_2026#”.

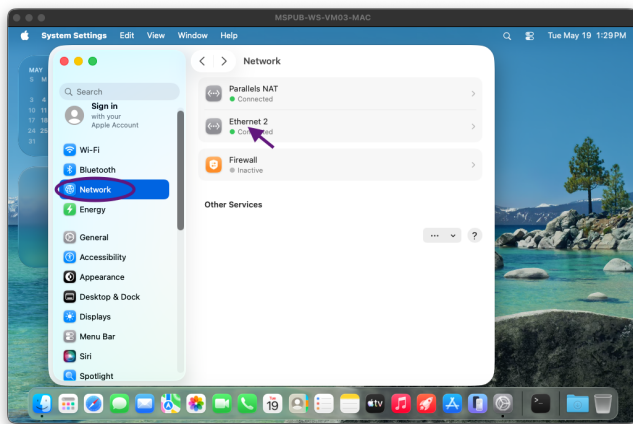


2. From the Menu Bar at the top, click the “Apple menu” and select “System Settings...”

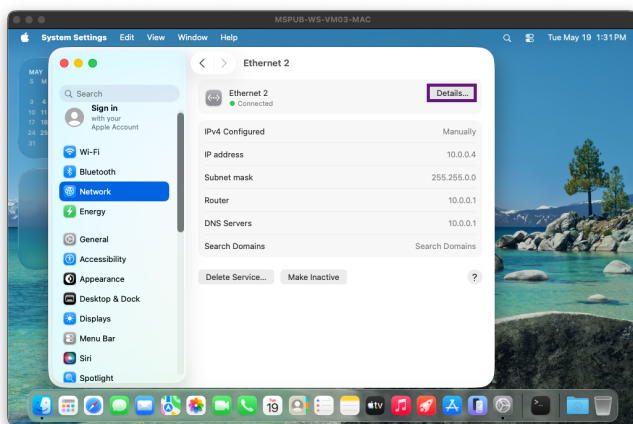


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

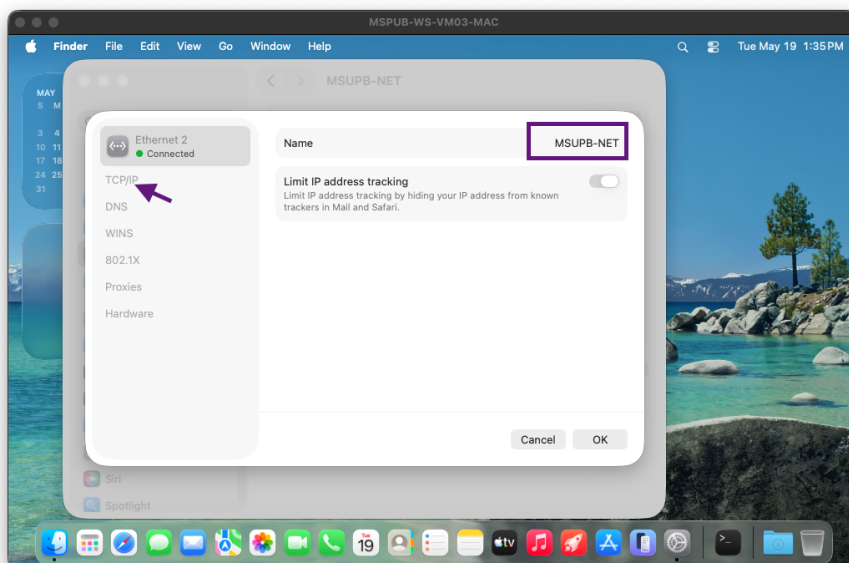
3. On the left pane of System Settings click “Network” then click “Ethernet 2.”



4. Click “Details” toward the right of “Ethernet 2: Connected.”



5. Rename the “Ethernet 2” to “MSPUB-NET.” Then click “TCP/IP” on the left pane.

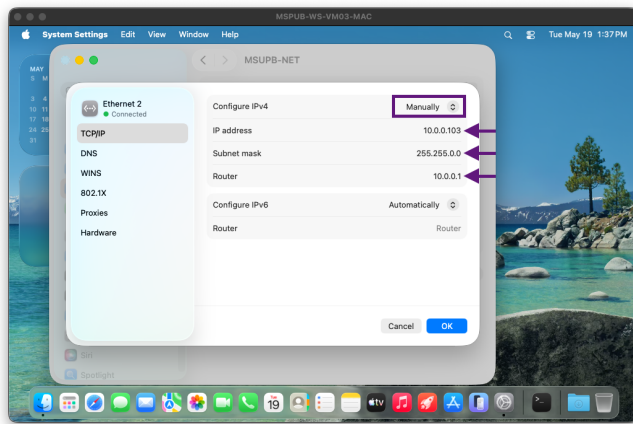


6. Set the TCP/IP settings as follows:

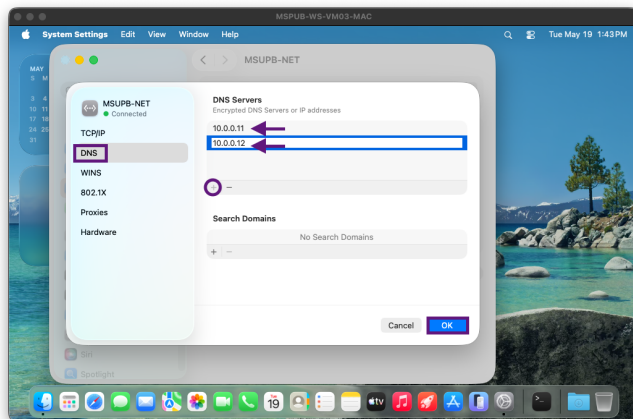
- Configure IPv4: **Manually**
- IP address: **10.0.0.103**
- Subnet mask: **255.255.0.0**

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

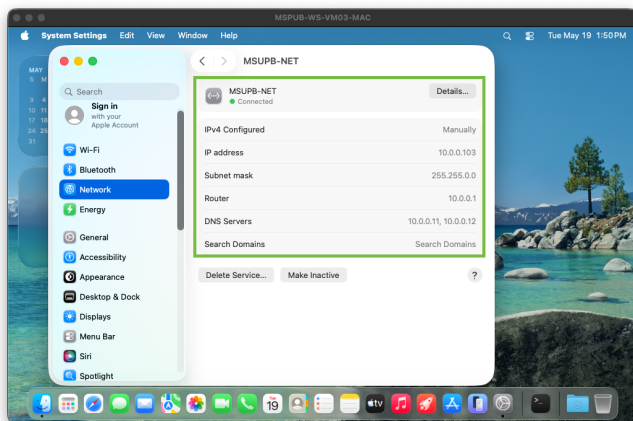
- Router: **10.0.0.1**



7. Click on “DNS” on left pane. Under DNS Servers click on the “+” to add a new DNS Server. Add the following DNS Server IP addresses:
 - **10.0.0.11** (*MSPUB-GLEEOK-DC01*)
 - **10.0.0.12** (*MSPUB-COLGERA-DM01*)
 - Click “OK” once completed.



8. Back in System Settings > Network the settings should be the new IP and DNS Servers configuration will be updated. Close System Settings by clicking the “Red dot” in the upper left corner.



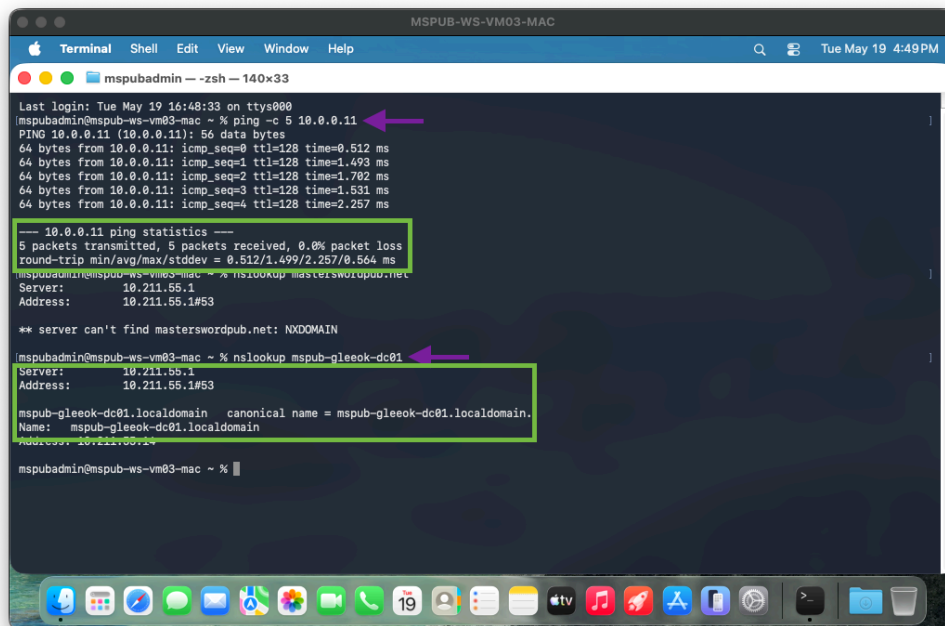
9. To make sure the Mac can communicate with MSPUB-GLEEOK-DC01 you will use the commands ping and nslookup. Click on the “Magnify Glass” toward the right of the Menu Bar to open Spotlight and search for “Terminal.” Click on the “Terminal” search result.

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

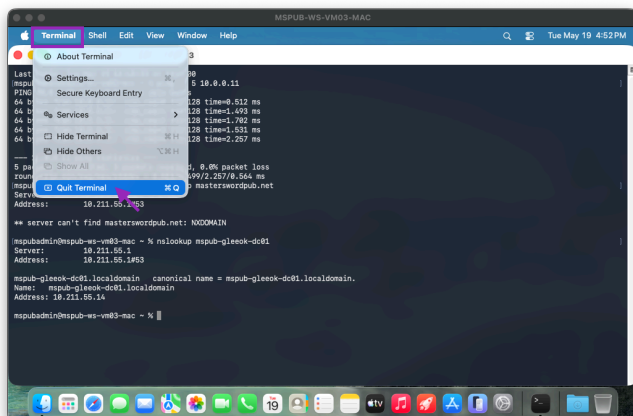


10. Type the following commands in the Terminal window:

- `ping -c 5 10.0.0.11`
- `nslookup MSPUB-GLEEOK-DC01`



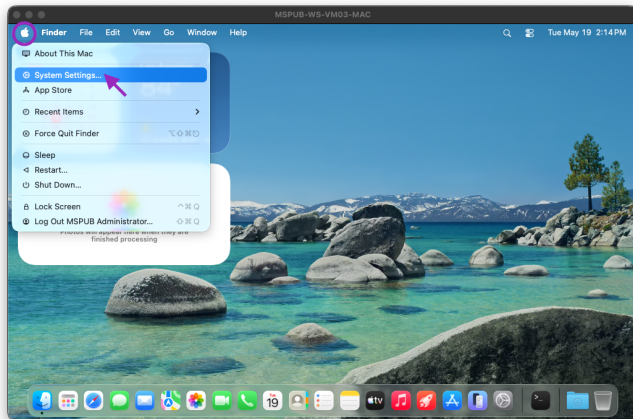
11. There should be no packet loss and the IP Address should resolve to MSPUB-GLEEOK-DC01. Close the terminal by clicking “Terminal” in the Menu Bar and click “Quit Terminal.”



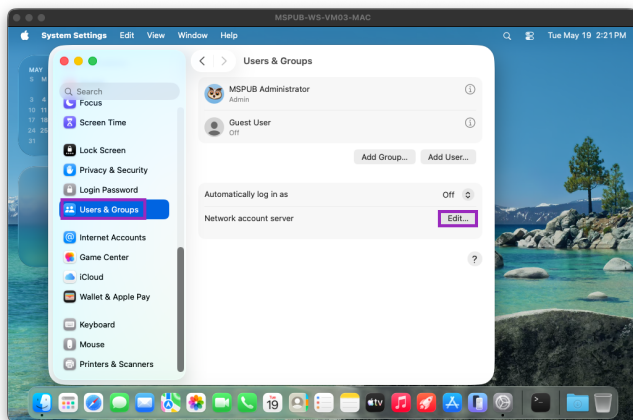
Binding macOS to the MSPUB Domain

Now that the DNS settings have been applied to MSPUB-WS-VM03-MAC, it can now be bound to the MSPUB Active Directory hosted on MSPUB-GLEEOK-DC01.

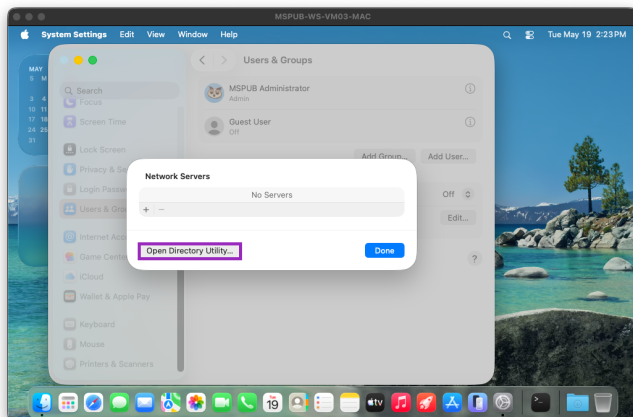
1. On the Menu Bar click the “Apple menu” and select “System Settings.”



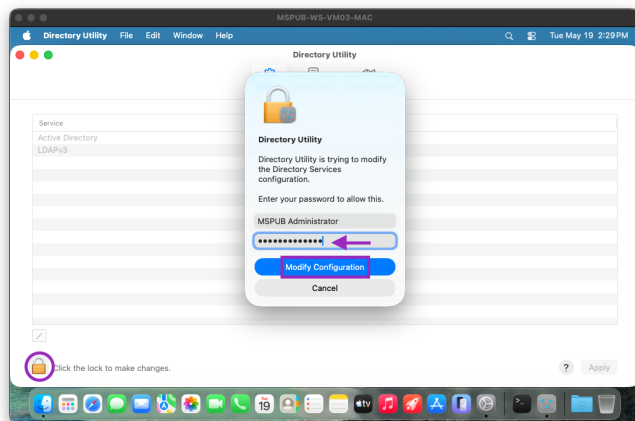
2. In System Settings scroll down and click “Users & Groups.” In Users & Groups click “Edit..” To the right of Network account server.



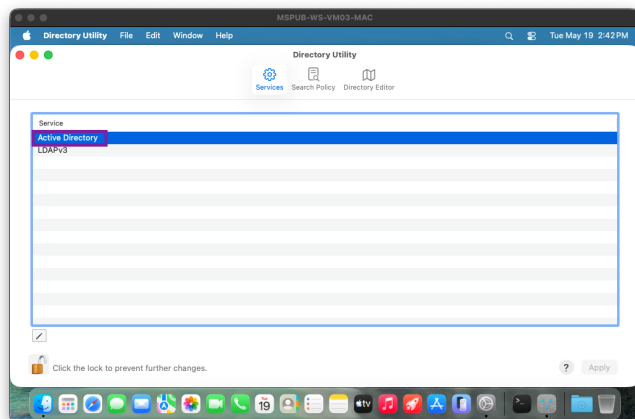
3. On the Network Servers dialog box click “Open Directory Utility...”



4. The Directory Utility will open and should be locked from making changes. Click on the “Padlock icon” in the lower left to all editing. The Authorization dialog will open, enter the MSPUB Administrator password, “CSNT253_2026#” and click “Modify Configuration.”

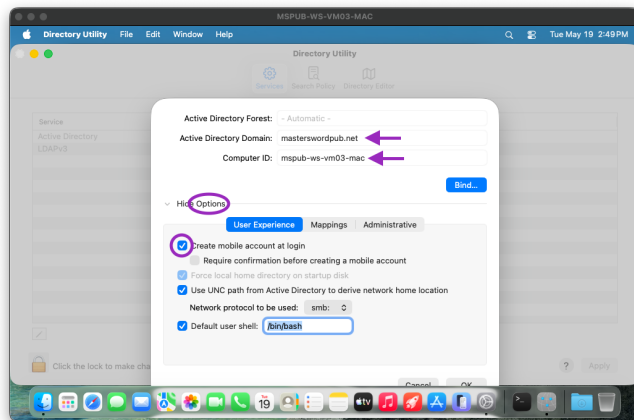


5. Double click “Active Directory”



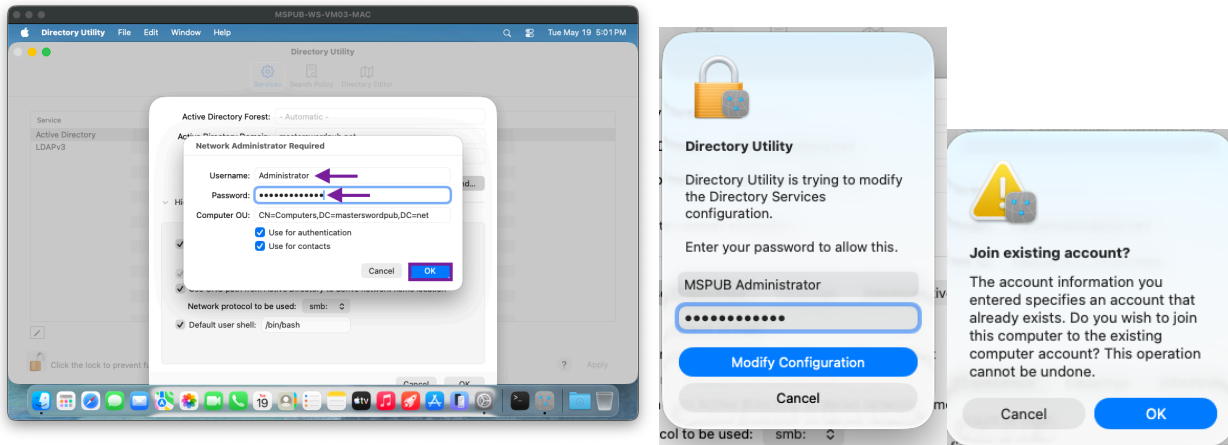
6. In the Active Directory settings configure the following:

- Active Directory Domain: **masterswordpub.net**
- Computer ID: **mspub-ws-vm03-mac**
- Expand Show Options:
 - In the “User Experience” tab
 - **Tick:** Create mobile account at login
- Click “Bind...” once the settings have been configured

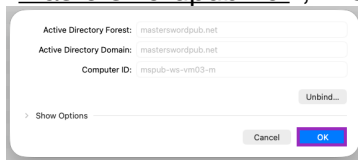


- ### 7. You will be prompted to enter in a domain administrators username and password. Use the username “Administrator” with the password “CSNT253_2026#” then click “OK.” You will need to authenticate the changes using the local Mac’s MSPUB Admin credentials. Confirm Joining the existing account and click “OK.”

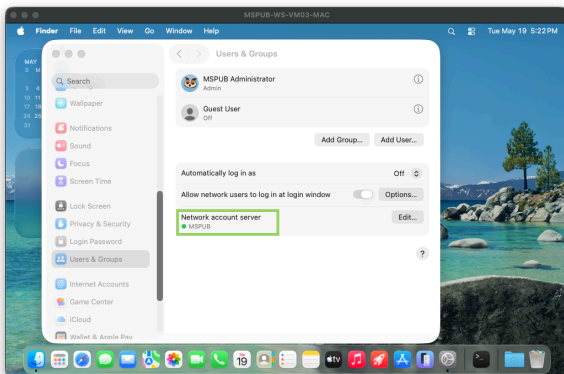
Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



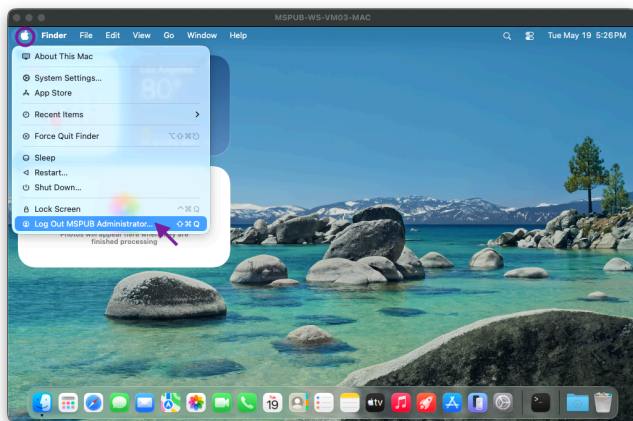
8. After the Active Directory Utility finishing joining, the Active Directory field will update to **“masterswordpub.net”**, this means the AD has successfully been joined. Click **“OK.”**



9. Close Directory Utility by click the **“Red circle”** in the upper left. In the System Settings > Users & Groups the Network account server should have updated to display MSPUB with a green connection dot. If there are ever any issues this status dot will display as either yellow or red.



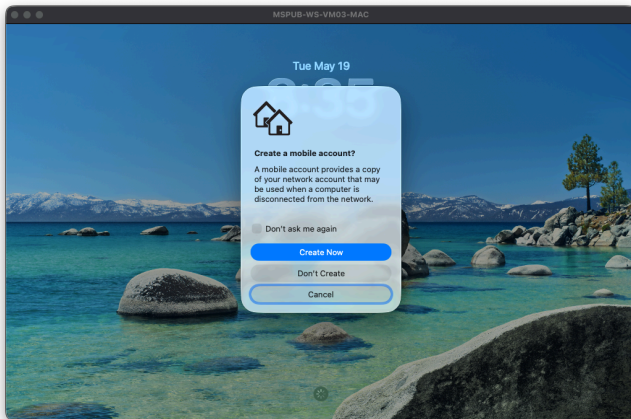
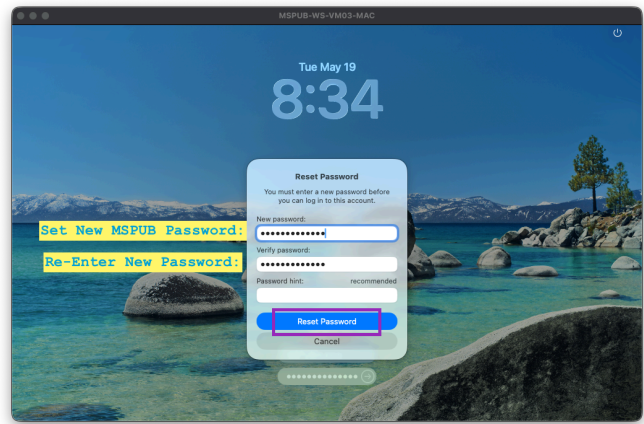
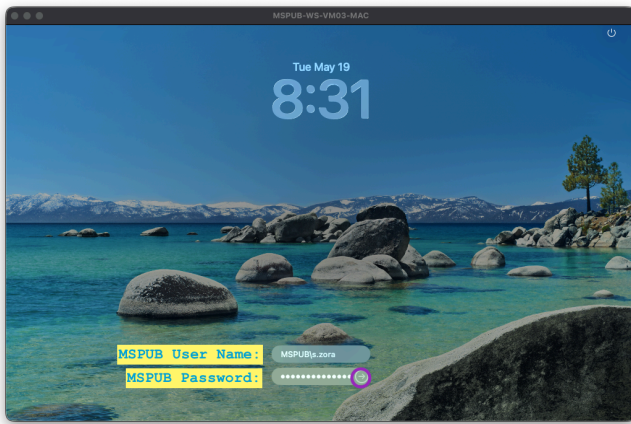
10. Verify you can login as another domain user, but clicking the **“Apple menu”** in the Menu Bar and selecting **“Log Out.”**



11. Notice the login window has changed to enter in a user name and password, instead of selecting a user account then entering the password. In the example it was tested using the username **MSPUB\s.zora** with the password, **“Hyru13W@rr10r\$”**. Note: the user will be required to change their password, use

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

“CSNT253_2026#”. If prompted to “Create a mobile account?” Click “Create Now.”



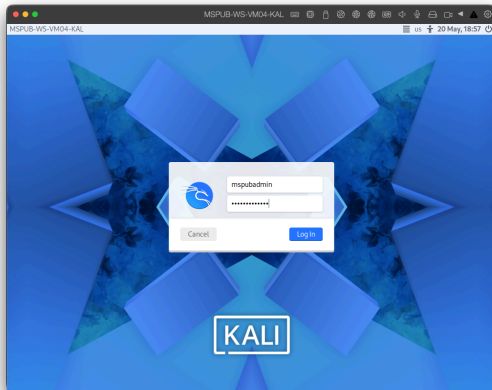
12. This Mac has been successfully added to the Active Directory Domain once the account has successfully loaded to the macOS Desktop.



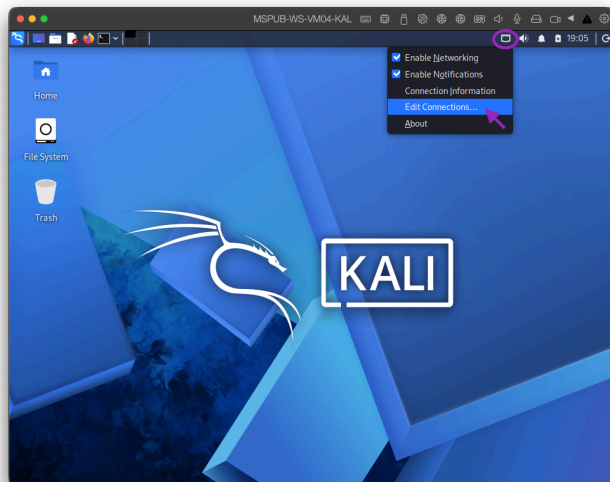
Configuring Network Settings in Kali Linux

The Kali Linux client MSPUB-WS-VM04-KAL will be configured with a Static IP address, 10.0.0.104 and must point to the DNS server configured on MSPUB-GLEEOK-DC01, 10.0.0.11.

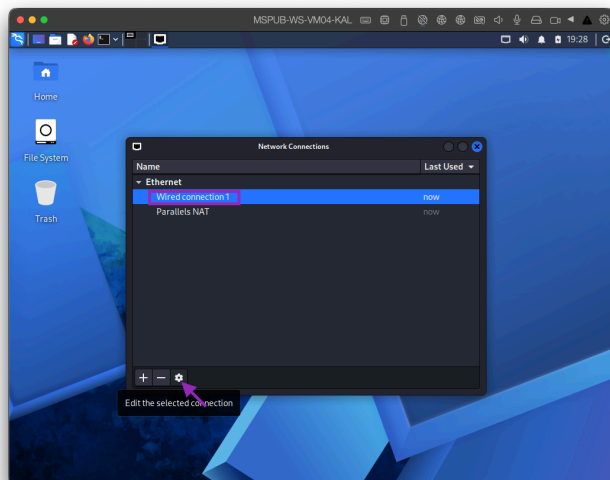
1. On MSPUB-WS-VM04-KAL login using the username “mspubadmin” with the password “CSNT253_2026#”.



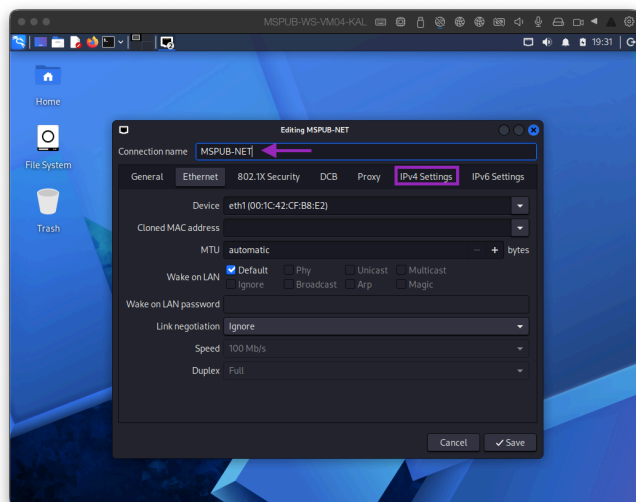
2. Right-click the “Network icon” in the upper right of the toolbar. Select “Edit Connections...”



3. In Network Connections select “Wired connection 1” and click the “Settings gear.”

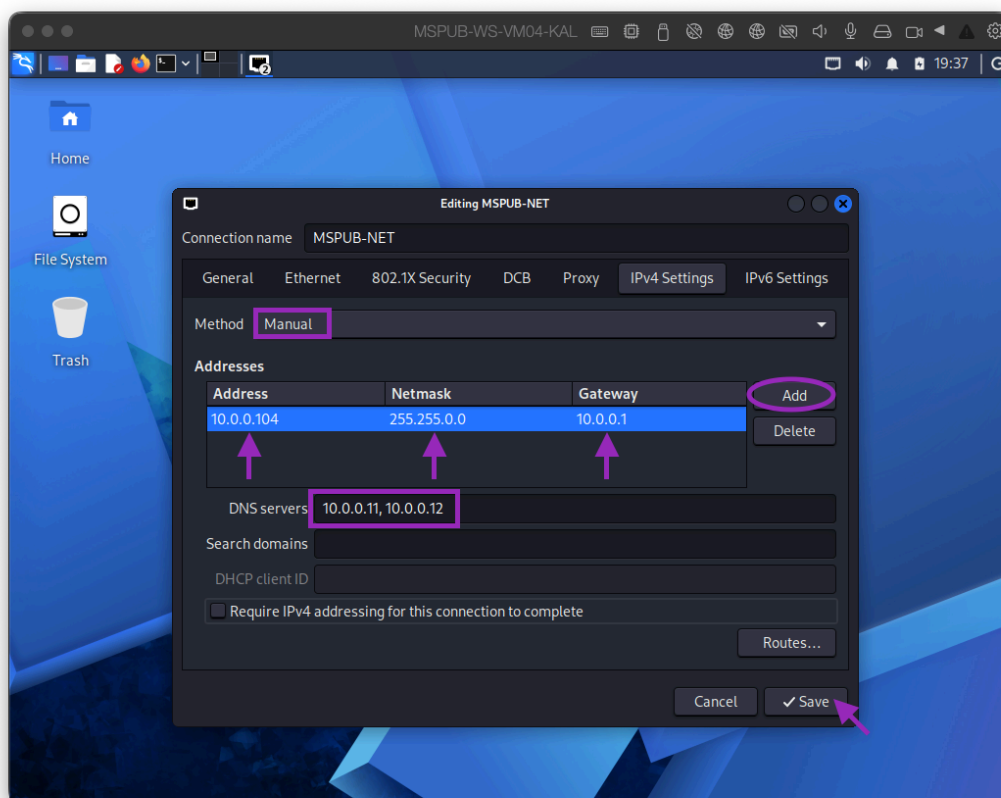


4. In the Editing Wired connection 1 window rename it to “MSPUB-NET.” Then click the “IPv4 Settings” tab.



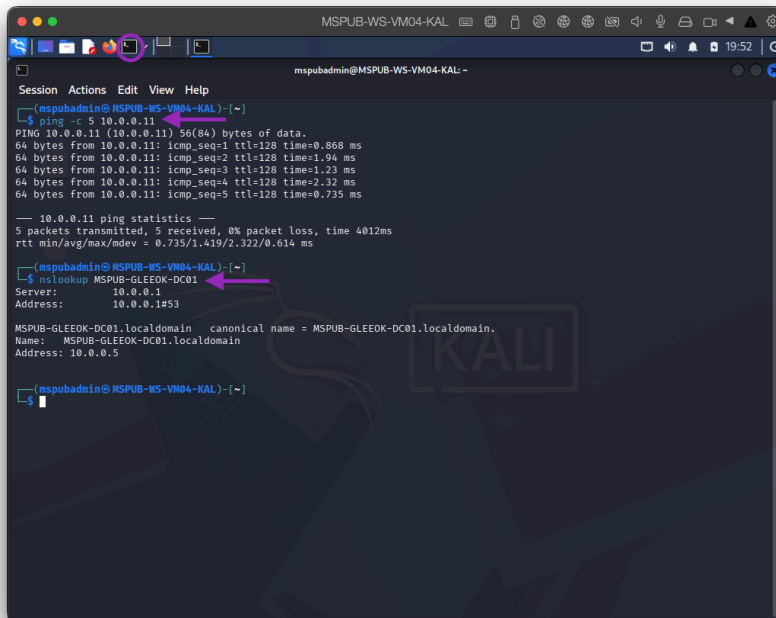
5. In IPv4 Settings configure the following:

- Method: **Manual**
- Click “Add”
 - Address: **10.0.0.104**
 - Netmask: **255.255.0.0**
 - Gateway: **10.0.0.1**
- DNS Servers: **10.0.0.11, 10.0.0.12**
- Click “Save” once configured



6. In the the toolbar in at the top open “Terminal” and type the following commands in the Terminal window:

- `ping -c 5 10.0.0.11`
- `nslookup MSPUB-GLEEOK-DC01`
- Pinging MSPUB-GLEEOK-DC01 should be successful with no packet loss. Nslookup should resolve its IP address.



```

MSPUB-WS-VM04-KAL
mspubadmin@MSPUB-WS-VM04-KAL:~$ ping -c 5 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data:
64 bytes from 10.0.0.11: icmp_seq=1 ttl=128 time=0.868 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=128 time=1.94 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=128 time=1.23 ms
64 bytes from 10.0.0.11: icmp_seq=4 ttl=128 time=2.32 ms
64 bytes from 10.0.0.11: icmp_seq=5 ttl=128 time=0.735 ms

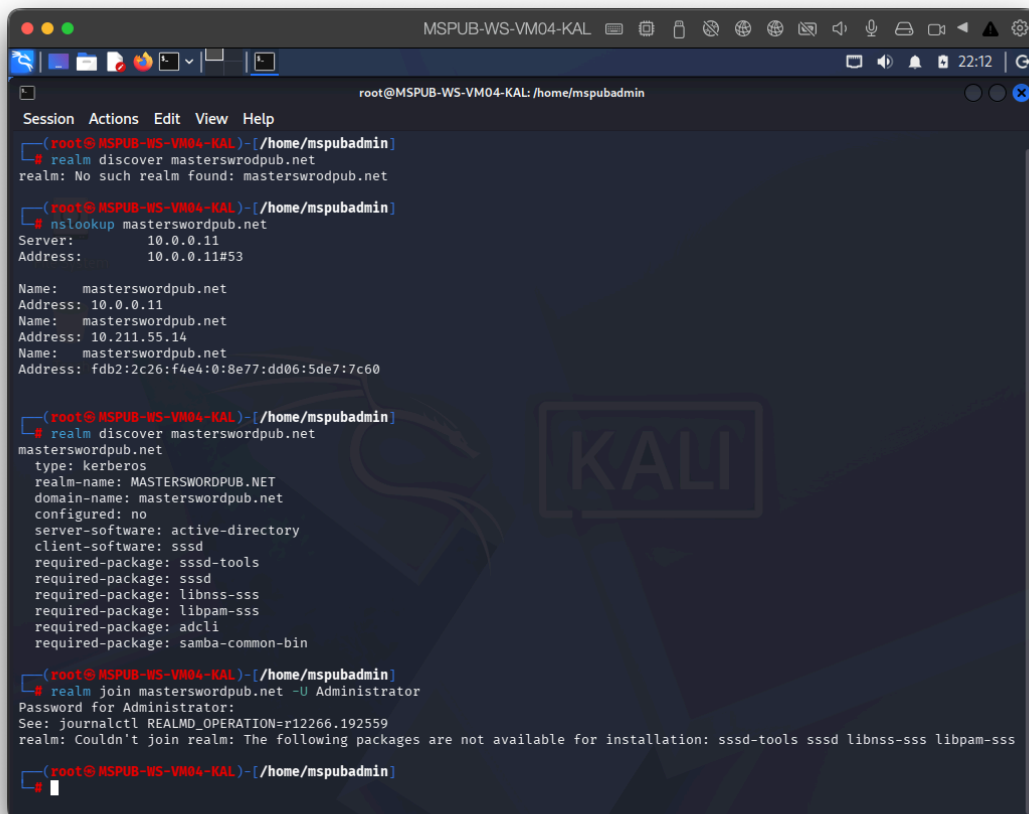
--- 10.0.0.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 0.735/1.419/2.322/0.614 ms

mspubadmin@MSPUB-WS-VM04-KAL:~$ nslookup MSPUB-GLEEOK-DC01
Server:
  10.0.0.1
Address:
  10.0.0.1#53

MSPUB-GLEEOK-DC01.localdomain canonical name = MSPUB-GLEEOK-DC01.localdomain.
Name:   MSPUB-GLEEOK-DC01.localdomain
Address: 10.0.0.5

```

Kali will not be added to the domain at this time, due to the SSSD dependancies not being developed for the ARM64 version of Kali Linux 2026, yet. There for it will be unsuccessful at joining the MSPUB domain, due to improper authentication issues. However, Kali can see the domain and resolves the IP address correctly for masterswordpub.net.



```

MSPUB-WS-VM04-KAL
root@MSPUB-WS-VM04-KAL: /home/mspubadmin

root@MSPUB-WS-VM04-KAL:~# realm discover masterswordpub.net
realm: No such realm found: masterswordpub.net

root@MSPUB-WS-VM04-KAL:~# nslookup masterswordpub.net
Server:
  10.0.0.11
Address:
  10.0.0.11#53

Name:   masterswordpub.net
Address: 10.0.0.11
Name:   masterswordpub.net
Address: 10.211.55.14
Name:   masterswordpub.net
Address: fdb2:2c26:f4e4:0:8e77:dd06:5de7:7c60

root@MSPUB-WS-VM04-KAL:~# realm discover masterswordpub.net
masterswordpub.net
type: kerberos
realm-name: MASTERSWORDPUB.NET
domain-name: masterswordpub.net
configured: no
server-software: active-directory
client-software: sssd
required-package: sssd-tools
required-package: sssd
required-package: libnss-sss
required-package: libpam-sss
required-package: adcli
required-package: samba-common-bin

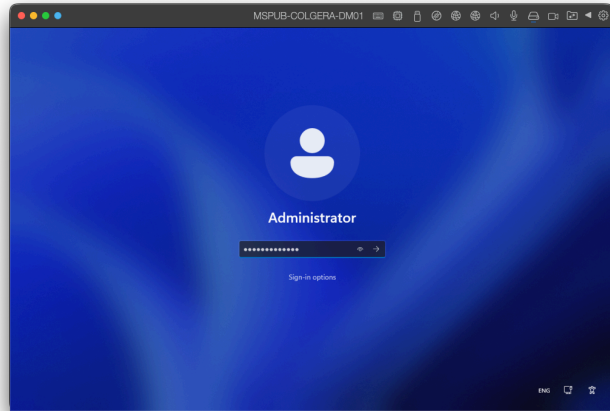
root@MSPUB-WS-VM04-KAL:~# realm join masterswordpub.net -U Administrator
Password for Administrator:
See: journalctl REALMD_OPERATION=r12266.192559
realm: Couldn't join realm: The following packages are not available for installation: sssd-tools sssd libnss-sss libpam-sss

```

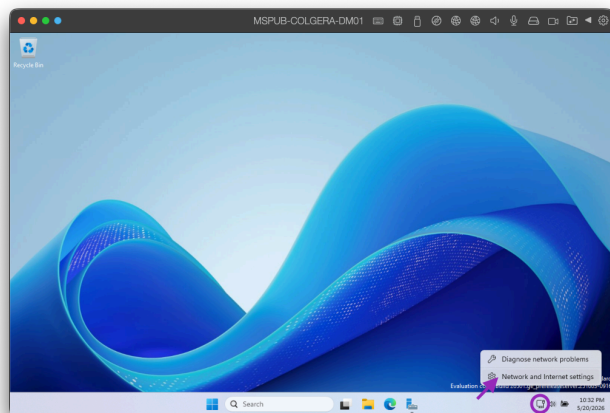
Configuring Network Settings in Windows Server 2025

The Windows Server 2025 virtual machine MSPUB-COLGERA-DM01 will be configured with a Static IP address, 10.0.0.12 and must point to the DNS server configured on MSPUB-GLEEOK-DC01, 10.0.0.11, to be able to connect to the Active Directory Domain.

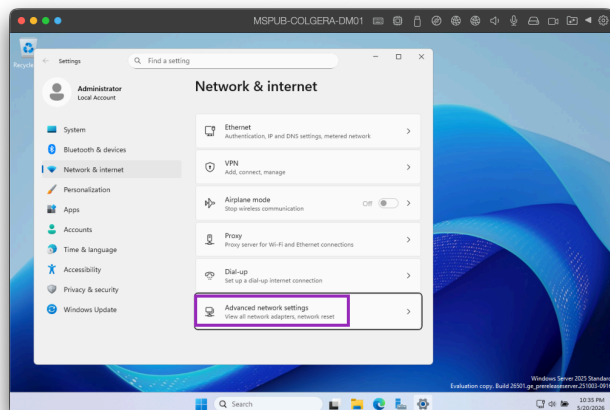
1. On MSPUB-COLGERA-DM01 login using the Administrator user account and the password “CSNT253_2026#”.



2. Right click the “Network icon” on the Taskbar in the lower right and select “Network and Internet settings.”

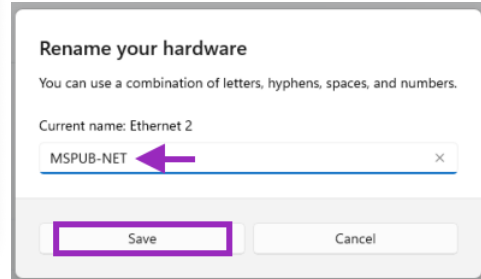
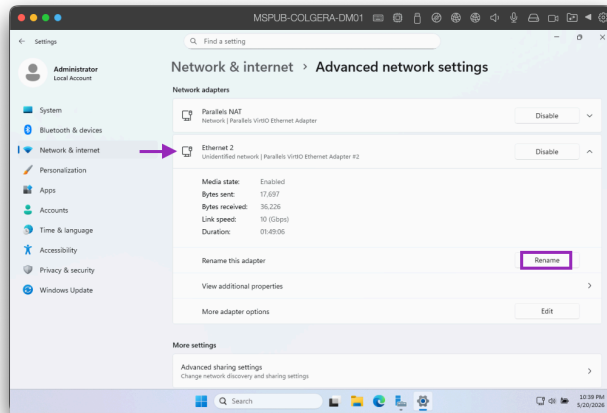


3. In Network and Internet Settings click on “Advanced network settings.”

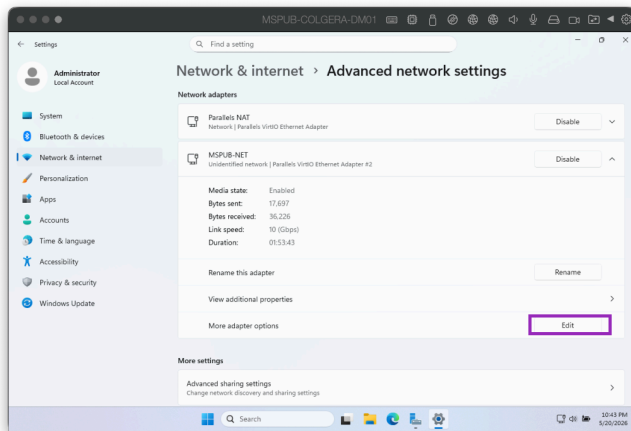


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

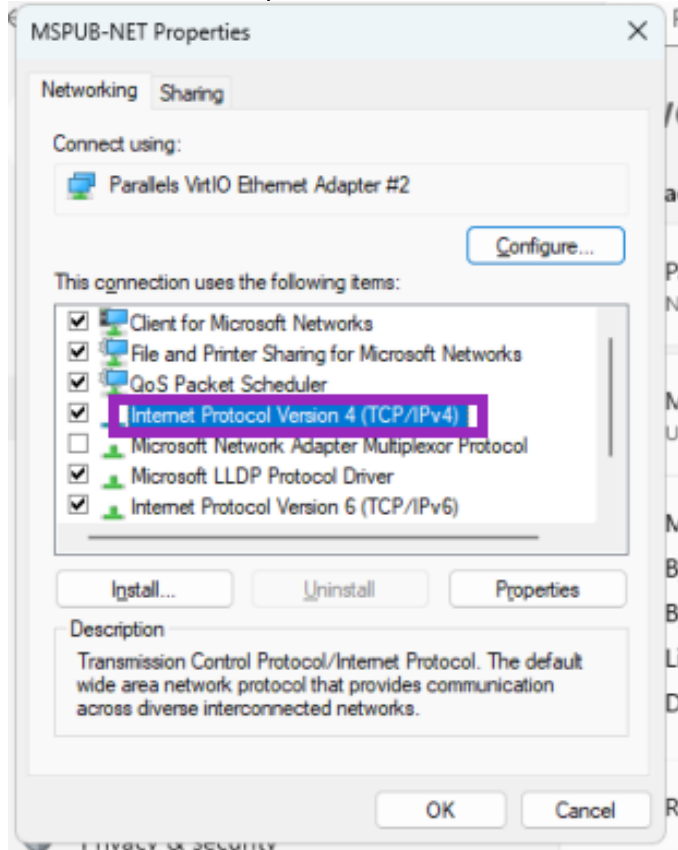
4. In Advanced network settings expand “Ethernet 2.” Click “Rename.” In the Rename your hardware dialog name the adapter “MSPUB-NET.” Click “Save.”



5. Back on Advanced network settings click “Edit” to the right of More adapter options.

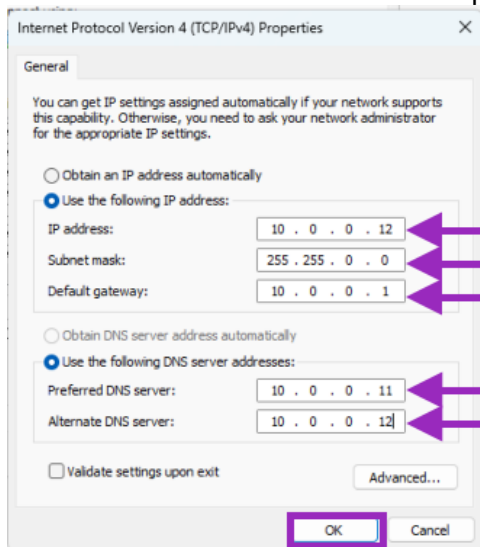


6. In MSPUB-NET Properties window double-click “Internet Protocol Version 4 (TCP/IPv4).”



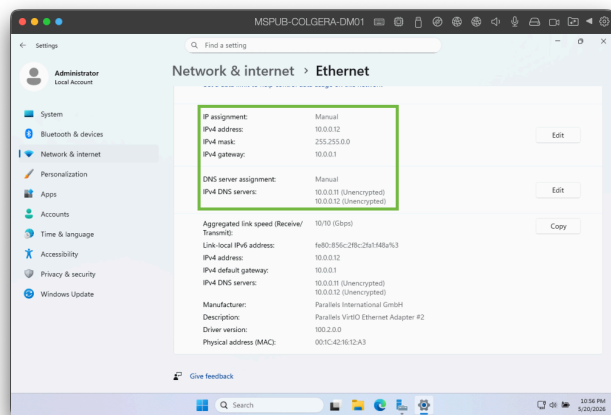
7. In the Internet Protocol Version 4 (TCP/IPv4) Properties window, configure the following settings:

- **Select** Use the following IP address:
 - IP address: **10.0.0.12**
 - Subnet mask: **255.255.0.0**
 - Default gateway: **10.0.0.1**
- **Select** Use the following DNS server addresses:
 - Preferred DNS: **10.0.0.11**
 - Secondary DNS: **10.0.0.12**
- Click “OK.”
- Click “OK” on the MSPUB-NET Properties window.

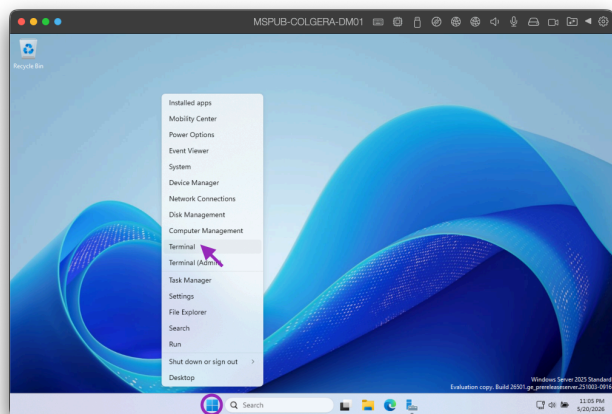


Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

8. The new IP Address and DNS Servers have been applied.

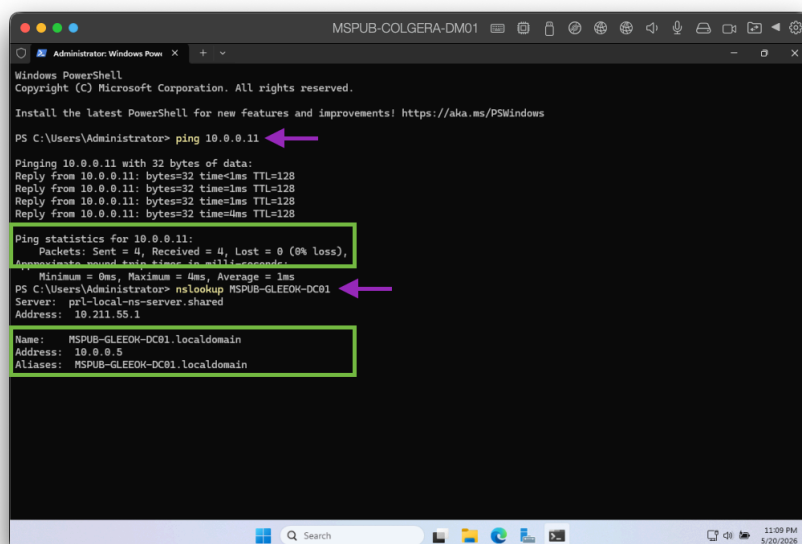


9. On the taskbar right-click the “Windows charm.” Click on “Terminal.”



10. In Terminal type the following commands:

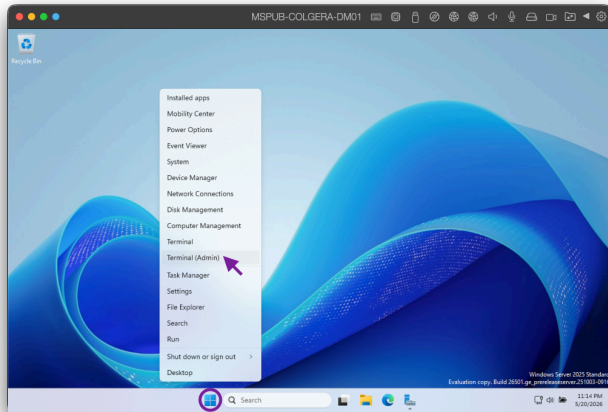
- ping 10.0.0.11
- nslookup masterswordpub.net
- Pinging MSPUB-GLEEOK-DC01 should return with no packet loss and nslookup should resolve its IP address.



Adding a Windows Server to the MSPUB Domain as a Secondary Domain Controller

Now that the DNS settings and IP settings have been configured on MSPUB-COLGERA-DM01 it can now be added to the masterswordpub.net Active Directory. Since this is another server it will act as a secondary Domain Controller in the even MSPUB-GLEEOK-DC01 goes offline. This allows for redundancy within the network. This will be configured using PowerShell command-lets.

1. MSPUB-COLGERA-DM01 is now apart of the masterswordpub.net Active Directory Domain. Now it can be promoted to a secondary Active Directory and DNS server. Right-click the “Windows charm” and select “Terminal (Admin).”



2. In terminal type the following command to Install AD Domain Services and DNS with management tools: `Install-WindowsFeature AD-Domain-Services,DNS -IncludeManagementTools`

```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator.MSPUB> Install-WindowsFeature AD-Domain-Services,DNS -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
-----
True      No          Success      {Active Directory Domain Services, DNS Ser...
```

3. Once installation is complete type the following command to promote the server to an additional domain controller: (You will be required to enter in the “MSPUB\Administrator” username and password) `Install-ADDSDomainController -DomainName “masterswordpub.net” -InstallDns -Credential (Get-Credential) -SiteName “Default-First-Site-Name” -ReplicationSourceDC “MSPUB-GLEEOK-DC01.masterswordpub.net” -DatabasePath “C:\Windows\NTDS” -LogPath “C:\Windows\NTDS” -SysvolPath “C:\Windows\SYSVOL”`

```
PS C:\Users\Administrator.MSPUB> Install-ADDSDomainController -DomainName “masterswordpub.net” -InstallDns -Credential (Get-Credential) -SiteName “Default-First-Site-Name” -ReplicationSourceDC “MSPUB-GLEEOK-DC01.masterswordpub.net” -DatabasePath “C:\Windows\NTDS” -LogPath “C:\Windows\NTDS” -SysvolPath “C:\Windows\SYSVOL”

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
```

4. When prompted enter the following:
 - SafeModeAdministratorPassword: **CSNT253_2026#**
 - Confirm SafeModeAdministratorPassword: **CSNT253_2026#**
 - Type “**A**” anytime it needs you to confirm an operation
5. The server will restart once the installation is complete. Once restarted, log back in as the MSPUB\Administrator user account. To verify replication is working open a new “Terminal (Admin)” session. Use the following commands:

Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Repadmin /replsummary
 - You should receive successful replication messages from inbound (COLEGRA) and outbound (GLEEOK)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator.MSPUB> Repadmin /replsummary
Replication Summary Start Time: 2026-05-22 10:29:21

Beginning data collection for replication summary, this may take awhile:
.....

Source DSA      largest delta  fails/total  %    error
MSPUB-COLGERA-DM01 04m:40s      0 / 5      0    0

Destination DSA largest delta  fails/total  %    error
MSPUB-GLEEOK-DC    04m:41s      0 / 5      0    0

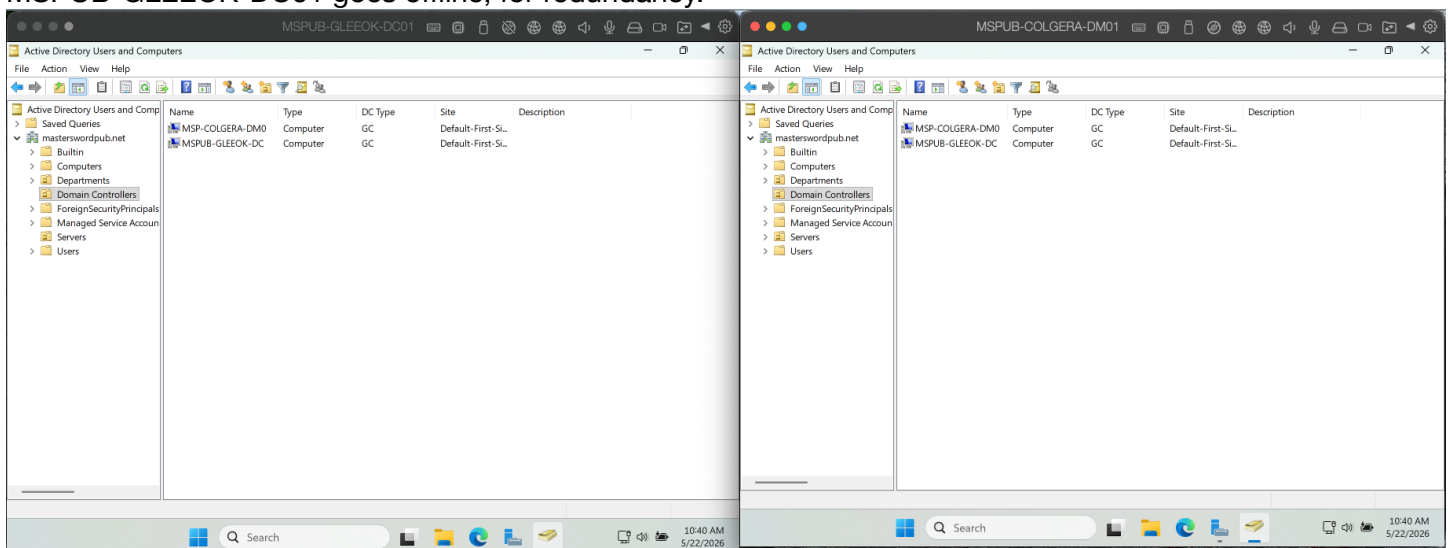
PS C:\Users\Administrator.MSPUB>
```

- Get-ADDomainController -Filter *
 - You should see both MSPUB-GLEEOK-DC01 and MSPUB-COLGERA-DM01 in the results

```
PS C:\Users\Administrator.MSPUB> Get-ADDomainController -Filter *

Name                           Site                               Role
-----
MSPUB-GLEEOK-DC01               Default-First-SL...               DC
MSPUB-COLGERA-DM01             Default-First-SL...               DC
```

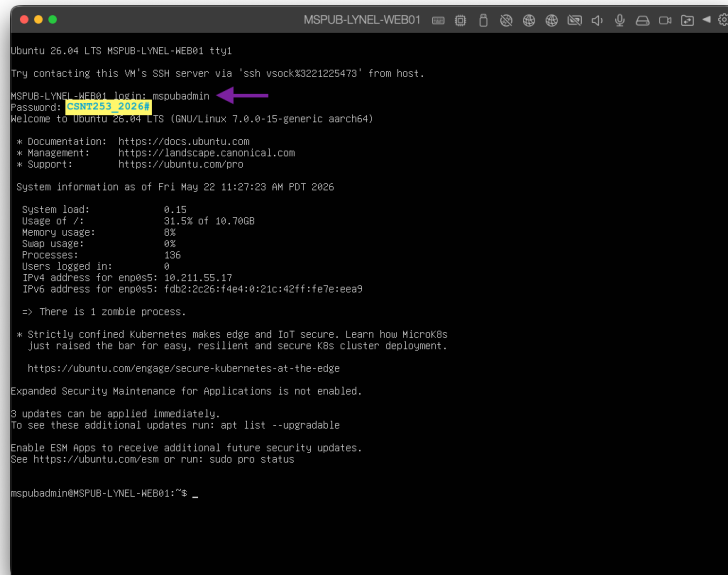
6. MSPUB-COLGERA-DM01 is now setup as a secondary Domain Controller with AD DS in the event MSPUB-GLEEOK-DC01 goes offline, for redundancy.



Configuring Network Settings in Ubuntu Server 26.04 LTE

The Ubuntu Server virtual machine MSPUB-LYNEL-WEB01 will be configured with a Static IP address, 10.0.0.13 and must point to the DNS server configured on MSPUB-GLEEOK-DC01, 10.0.0.11, to be able to connect to the Active Directory Domain later on. Ubuntu Server does not contain a graphical user interface (GUI), so it will be configured all using its command line interface (CLI).

1. On MSPUB-LYNEL-WEB01 login using the username “mspubadmin” when prompted for the password type “CSNT253_2026#” (note it is normal if no characters are displayed when entering a password in CLI).



```

MSPUB-LYNEL-WEB01
Ubuntu 26.04 LTS MSPUB-LYNEL-WEB01 tty1
Try contacting this VM's SSH server via 'ssh vsockX3221225473' from host.
MSPUB-LYNEL-WEB01 login: mspubadmin
Password: CSNT253_2026#
Welcome to Ubuntu 26.04 LTS (GNU/Linux 7.0.0-15-generic aarch64)

 * Documentation:  https://docs.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Fri May 22 11:27:23 AM PDT 2026
System load:          0.15
Usage of /:            31.5% of 10.7GB
Memory usage:         8%
Swap usage:           0%
Processes:            136
Users logged in:      0
IPv4 address for enp0s5: 10.211.55.17
IPv6 address for enp0s5: fd02:2c26:f4e4:0:21c:42ff:fe7e:eea9
=> There is 1 zombie process.

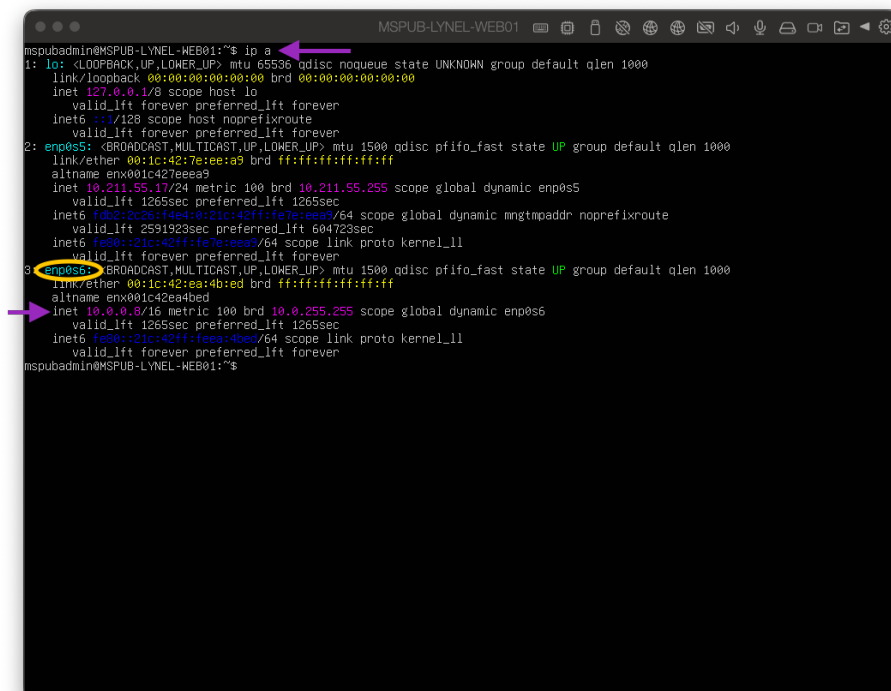
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.
3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

mspubadmin@MSPUB-LYNEL-WEB01:~$

```

2. To determine which network adapter needs to be configured type the following command:
“ip a”
Look for the adapter that current has 10.0.0.x for the inet value. In this example it is enp0s6

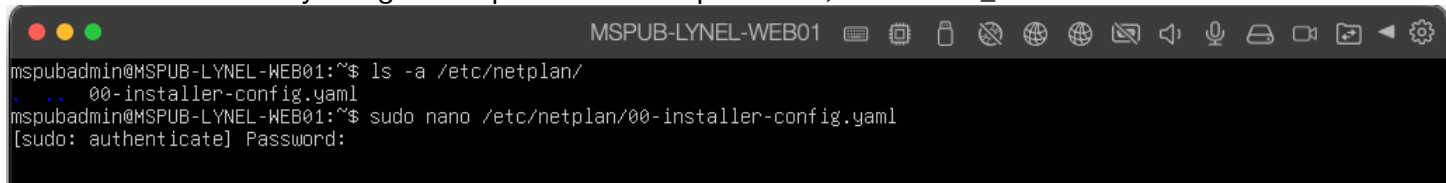


```

mspubadmin@MSPUB-LYNEL-WEB01:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:1c:42:7e:ee:a9 brd ff:ff:ff:ff:ff:ff
    altname enx001c427eea9
    inet 10.211.55.17/24 metric 100 brd 10.211.55.255 scope global dynamic enp0s5
        valid_lft 1265sec preferred_lft 1265sec
    inet6 fd02:2c26:f4e4:0:21c:42ff:fe7e:eea9/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 2591923sec preferred_lft 604723sec
    inet6 fe80::21c:42ff:fe7e:eea9/64 scope link proto kernel_l1
        valid_lft forever preferred_lft forever
3: enp0s6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:1c:42:ea:4b:ed brd ff:ff:ff:ff:ff:ff
    altname enx001c42ea4bed
    inet 10.0.0.13/16 metric 100 brd 10.0.255.255 scope global dynamic enp0s6
        valid_lft 1265sec preferred_lft 1265sec
    inet6 fe80::21c:42ff:feea:4bed/64 scope link proto kernel_l1
        valid_lft forever preferred_lft forever
mspubadmin@MSPUB-LYNEL-WEB01:~$

```

3. Check to see if there is a Netplan configuration file (either 50-cloud-init.yaml, 01-network-manager-all.yaml, or 00-installer-config.yaml) by typing “ls -a /etc/netplan/” in this example it is 00-installer-config.yaml. Open this file by typing “sudo nano /etc/netplan/00-installer-config.yaml” you will be required to authenticate sudo by using the mspubadmin user password, “CSNT253_2026#”

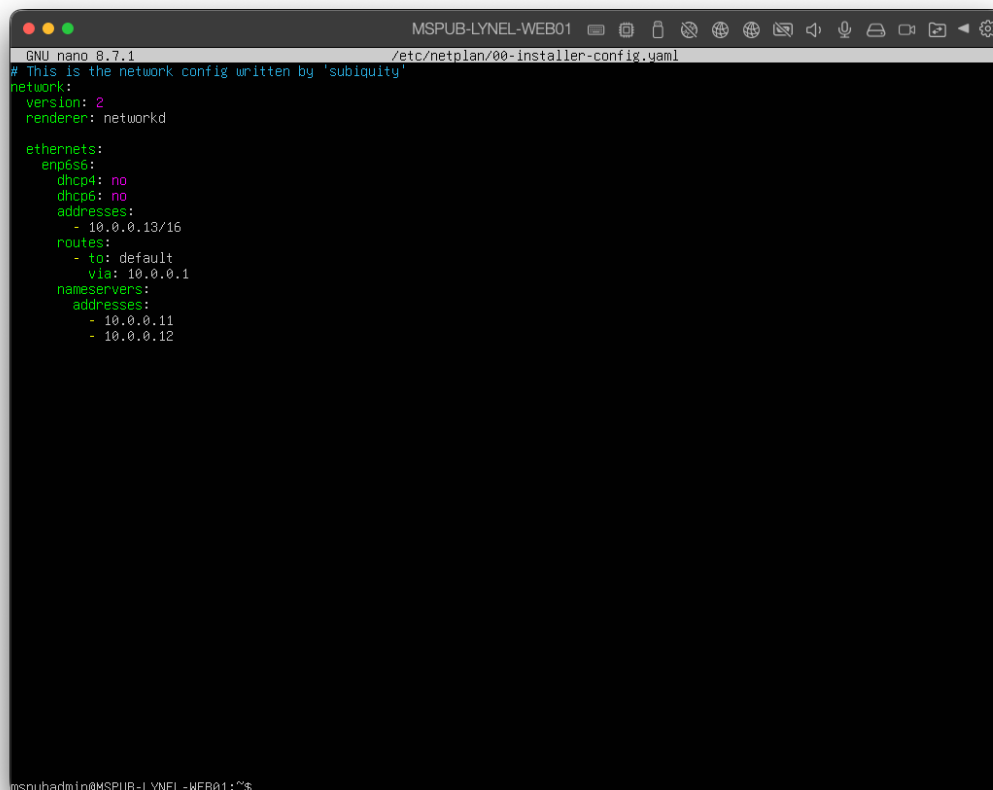


```
mspubadmin@MSPUB-LYNEL-WEB01:~$ ls -a /etc/netplan/
.  ..  00-installer-config.yaml
mspubadmin@MSPUB-LYNEL-WEB01:~$ sudo nano /etc/netplan/00-installer-config.yaml
[sudo: authenticate] Password:
```

4. Delete everything contained in this file currently. Then type the following exactly:
network:
version: 2
renderer: networkd

```
ethernets:
  enp0s6:
    dhcp4: no
    dhcp6: no
    addresses:
      - 10.0.0.13/16
    routes:
      - to: default
      - via: 10.0.0.1
    nameservers:
      addresses:
        - 10.0.0.11
        - 10.0.0.12
```

Press CTRL+O, Enter, CTRL+X to save and exit Nano text editor.



```
GNU nano 8.7.1 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd

ethernets:
  enp6s6:
    dhcp4: no
    dhcp6: no
    addresses:
      - 10.0.0.13/16
    routes:
      - to: default
      - via: 10.0.0.1
    nameservers:
      addresses:
        - 10.0.0.11
        - 10.0.0.12

mspubadmin@MSPUB-LYNEL-WEB01:~$
```

5. After the changes to the Netplan config have been saved test it by typing the command:
`sudo netplan try`

If there are no errors, press "Enter" to accept the settings

```
msspubadmin@MSPUB-LYNEL-WEB01:~$ sudo netplan try
Do you want to keep these settings?

Press ENTER before the timeout to accept the new configuration

Changes will revert in 109 seconds
Configuration accepted.
msspubadmin@MSPUB-LYNEL-WEB01:~$
```

6. Check to confirm the IP address settings have been applied by typing:
`ifconfig`

`enp0s6` should show the inet as 10.0.0.13 and net mask as 255.255.0.0

```
msspubadmin@MSPUB-LYNEL-WEB01:~$ ifconfig
enp0s5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.211.55.18 netmask 255.255.255.0 broadcast 10.211.55.255
    inet6 fdb2:2c26:f4e4:0:21c:42ff:fe7e:eea9 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::21c:42ff:fe7e:eea9 prefixlen 64 scopeid 0x20<link>
    ether 00:1c:42:7e:ee:a9 txqueuelen 1000 (Ethernet)
    RX packets 344 bytes 170107 (170.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 98 bytes 10573 (10.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.13 netmask 255.255.0.0 broadcast 10.0.255.255
    inet6 fe80::21c:42ff:fe8a:4bed prefixlen 64 scopeid 0x20<link>
    ether 00:1c:42:ea:4b:ed txqueuelen 1000 (Ethernet)
    RX packets 100 bytes 9314 (9.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 4378 (4.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 84 bytes 7304 (7.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 84 bytes 7304 (7.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msspubadmin@MSPUB-LYNEL-WEB01:~$
```

7. To test DNS type:
`nslookup masterswordpub.net`
It should resolve to 10.0.0.11 and 10.0.12


```

mspubadmin@MSPUB-LYNEL-WEB01:~$ nslookup masterswordpub.net
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   masterswordpub.net
Address: 10.0.0.12
Name:   masterswordpub.net
Address: 10.0.0.11
Name:   masterswordpub.net
Address: 10.211.55.21
Name:   masterswordpub.net
Address: 10.211.55.14
Name:   masterswordpub.net
Address: fdb2:2c26:f4e4:0:4133:ae01:afef:88f2
Name:   masterswordpub.net
Address: fdb2:2c26:f4e4:0:270:c74e:d3f5:22fd
Name:   masterswordpub.net
Address: fdb2:2c26:f4e4:0:8e77:dd06:5de7:7c60

```



8. Confirm that pinging MSPUB-GLEEOK-DC01 and MSPUB-COLEGERA-DM01 works by typing:
- ```

ping -c 5 10.0.0.11
ping -c 5 10.0.0.12

```

There should be 0 packet loss

```

mspubadmin@MSPUB-LYNEL-WEB01:~$ ping -c 5 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data.
64 bytes from 10.0.0.11: icmp_seq=1 ttl=128 time=0.775 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=128 time=0.996 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=128 time=1.15 ms
64 bytes from 10.0.0.11: icmp_seq=4 ttl=128 time=1.20 ms
64 bytes from 10.0.0.11: icmp_seq=5 ttl=128 time=1.03 ms

--- 10.0.0.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4061ms
rtt min/avg/max/mdev = 0.775/1.031/1.200/0.148 ms
mspubadmin@MSPUB-LYNEL-WEB01:~$ ping -c 5 10.0.0.12
PING 10.0.0.12 (10.0.0.12) 56(84) bytes of data.
64 bytes from 10.0.0.12: icmp_seq=1 ttl=128 time=1.16 ms
64 bytes from 10.0.0.12: icmp_seq=2 ttl=128 time=1.35 ms
64 bytes from 10.0.0.12: icmp_seq=3 ttl=128 time=0.658 ms
64 bytes from 10.0.0.12: icmp_seq=4 ttl=128 time=0.849 ms
64 bytes from 10.0.0.12: icmp_seq=5 ttl=128 time=0.794 ms

--- 10.0.0.12 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 0.658/0.962/1.348/0.254 ms

```

At this time MSPUB-LYNEL-WEB01 will not be joining the MSPUB Active Directory. This will be covered in Part 2 with a script.

## Verifying All Virtual Machines Resolve Each Other on the Network

In a home lab it is important that all machines can communicate with each other. To test this use the commands “ping \*ipaddress\*” and “nslookup \*hostname\*” for each machine on the network in the operating system’s command line interface (CLI) application.

Before testing make sure every VM is running at the same time.

### Host Names and IP Addresses to Test

| Hostname           | IP Address |
|--------------------|------------|
| MSPUB-WS-VM01-WIN  | 10.0.0.101 |
| MSPUB-WS-VM02-UBT  | 10.0.0.102 |
| MSPUB-WS-VM03-MAC  | 10.0.0.103 |
| MSPUB-WS-VM04-KAL  | 10.0.0.104 |
| MSPUB-GLEEOK-DC01  | 10.0.0.11  |
| MSPUB-COLGERA-DM02 | 10.0.0.12  |
| MSPUB-LYNEL-WEB01  | 10.0.0.13  |

#### 1. MSPUB-WS-VM01-WIN

In a Terminal window type the command “ping \*10.0.0.x\*”. All should reply with no packet lost.

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> ping 10.0.0.102

Pinging 10.0.0.102 with 32 bytes of data:
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.102:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator> ping 10.0.0.103

Pinging 10.0.0.103 with 32 bytes of data:
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.103:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping 10.0.0.104

Pinging 10.0.0.104 with 32 bytes of data:
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.104:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:

```

Handwritten annotations in blue on the right side of the terminal window:

- MSPUB-WS-VM02-UBT (next to the first ping results)
- MSPUB-WS-VM03-MAC (next to the second ping results)
- MSPUB-WS-VM04-KAL (next to the third ping results)

```

Administrator: Windows PowerShell
MSPUB-WS-VM01-WIN

Ping 10.0.0.11 with 32 bytes of data:
Reply from 10.0.0.11: bytes=32 time<1ms TTL=128
Reply from 10.0.0.11: bytes=32 time<1ms TTL=128
Reply from 10.0.0.11: bytes=32 time<1ms TTL=128
Reply from 10.0.0.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.11:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping 10.0.0.12

Ping 10.0.0.12 with 32 bytes of data:
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.12:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping 10.0.0.13

Ping 10.0.0.13 with 32 bytes of data:
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.13:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

## 2. MSPUB-WS-VM02-UBT

In a Terminal window type the command “ping -c 4 \*10.0.0.x\*”. All should reply with no packet lost.

```

MSPUB-WS-VM02-UBT
May 22 17:08
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT: ~
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ ping -c 4 10.0.0.101
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data:
64 bytes from 10.0.0.101: icmp_seq=1 ttl=128 time=0.918 ms
64 bytes from 10.0.0.101: icmp_seq=2 ttl=128 time=1.07 ms
64 bytes from 10.0.0.101: icmp_seq=3 ttl=128 time=0.948 ms
64 bytes from 10.0.0.101: icmp_seq=4 ttl=128 time=1.01 ms

--- 10.0.0.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/ndev = 0.918/0.985/1.067/0.057 ms
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ ping -c 4 10.0.0.103
PING 10.0.0.103 (10.0.0.103) 56(84) bytes of data:
64 bytes from 10.0.0.103: icmp_seq=1 ttl=64 time=0.445 ms
64 bytes from 10.0.0.103: icmp_seq=2 ttl=64 time=0.926 ms
64 bytes from 10.0.0.103: icmp_seq=3 ttl=64 time=0.425 ms
64 bytes from 10.0.0.103: icmp_seq=4 ttl=64 time=0.392 ms

--- 10.0.0.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/ndev = 0.392/0.547/0.926/0.219 ms
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ ping -c 4 10.0.0.104
PING 10.0.0.104 (10.0.0.104) 56(84) bytes of data:
64 bytes from 10.0.0.104: icmp_seq=1 ttl=64 time=1.42 ms
64 bytes from 10.0.0.104: icmp_seq=2 ttl=64 time=0.604 ms
64 bytes from 10.0.0.104: icmp_seq=3 ttl=64 time=0.614 ms
64 bytes from 10.0.0.104: icmp_seq=4 ttl=64 time=0.259 ms

--- 10.0.0.104 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3036ms
rtt min/avg/max/ndev = 0.259/0.724/1.421/0.426 ms
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ ping -c 4 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data:
64 bytes from 10.0.0.11: icmp_seq=1 ttl=128 time=0.734 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=128 time=0.533 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=128 time=0.431 ms
64 bytes from 10.0.0.11: icmp_seq=4 ttl=128 time=0.445 ms

--- 10.0.0.11 ping statistics ---

```

```

MSPUB-WS-VM02-UBT
May 22 17:11
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT: ~
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ ping -c 4 10.0.0.12
PING 10.0.0.12 (10.0.0.12) 56(84) bytes of data.
64 bytes from 10.0.0.12: icmp_seq=1 ttl=128 time=0.434 ms
64 bytes from 10.0.0.12: icmp_seq=2 ttl=128 time=1.47 ms
64 bytes from 10.0.0.12: icmp_seq=3 ttl=128 time=1.76 ms
64 bytes from 10.0.0.12: icmp_seq=4 ttl=128 time=0.895 ms

--- 10.0.0.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.434/1.138/1.759/0.511 ms
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ ping -c 4 10.0.0.13
PING 10.0.0.13 (10.0.0.13) 56(84) bytes of data.
64 bytes from 10.0.0.13: icmp_seq=1 ttl=64 time=0.845 ms
64 bytes from 10.0.0.13: icmp_seq=2 ttl=64 time=0.648 ms
64 bytes from 10.0.0.13: icmp_seq=3 ttl=64 time=0.460 ms
64 bytes from 10.0.0.13: icmp_seq=4 ttl=64 time=0.461 ms

--- 10.0.0.13 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.460/0.603/0.845/0.159 ms
administrator@masterswordpub.net@MSPUB-WS-VM02-UBT:~$

```

**MSPUB-COLGERA-DM01**

**MSPUB-LYNEL-DM01**

### 3. MSPUB-WS-VM03-MAC

In a Terminal window type the command “ping -c 4 \*10.0.0.x\*”. All should reply with no packet lost.

```

MSPUB-WS-VM03-MAC
Fri May 22 5:21PM
administrator -- bash -- 140x33
To update your account to use zsh, please run 'chsh -s /bin/zsh'.
For more details, please visit https://support.apple.com/kb/HT208050.
MSPUB-WS-VM03-MAC:~ administrator$ ping -c 4 10.0.0.101
PING 10.0.0.101 (10.0.0.101): 56 data bytes
64 bytes from 10.0.0.101: icmp_seq=0 ttl=128 time=0.866 ms
64 bytes from 10.0.0.101: icmp_seq=1 ttl=128 time=0.568 ms
64 bytes from 10.0.0.101: icmp_seq=2 ttl=128 time=0.829 ms
64 bytes from 10.0.0.101: icmp_seq=3 ttl=128 time=0.507 ms

--- 10.0.0.101 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.507/0.693/0.866/0.157 ms
MSPUB-WS-VM03-MAC:~ administrator$ ping -c 4 10.0.0.102
PING 10.0.0.102 (10.0.0.102): 56 data bytes
64 bytes from 10.0.0.102: icmp_seq=0 ttl=64 time=0.593 ms
64 bytes from 10.0.0.102: icmp_seq=1 ttl=64 time=0.458 ms
64 bytes from 10.0.0.102: icmp_seq=2 ttl=64 time=0.434 ms
64 bytes from 10.0.0.102: icmp_seq=3 ttl=64 time=0.435 ms

--- 10.0.0.102 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.434/0.480/0.593/0.066 ms
MSPUB-WS-VM03-MAC:~ administrator$ ping -c 4 10.0.0.104
PING 10.0.0.104 (10.0.0.104): 56 data bytes
64 bytes from 10.0.0.104: icmp_seq=0 ttl=64 time=0.784 ms
64 bytes from 10.0.0.104: icmp_seq=1 ttl=64 time=0.602 ms
64 bytes from 10.0.0.104: icmp_seq=2 ttl=64 time=0.395 ms
64 bytes from 10.0.0.104: icmp_seq=3 ttl=64 time=0.388 ms

--- 10.0.0.104 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.388/0.542/0.784/0.164 ms
MSPUB-WS-VM03-MAC:~ administrator$

```

**MSPUB-WS-VM01-WIN**

**MSPUB-WS-VM02-UBT**

**MSPUB-WS-VM04-KAL**

```

MSPUB-WS-VM03-MAC:~ administrator$ ping -c 4 10.0.0.11
PING 10.0.0.11 (10.0.0.11): 56 data bytes
64 bytes from 10.0.0.11: icmp_seq=0 ttl=128 time=0.530 ms
64 bytes from 10.0.0.11: icmp_seq=1 ttl=128 time=0.534 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=128 time=0.529 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=128 time=0.495 ms
--- 10.0.0.11 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.495/0.522/0.534/0.016 ms
MSPUB-WS-VM03-MAC:~ administrator$ ping -c 4 10.0.0.12
PING 10.0.0.12 (10.0.0.12): 56 data bytes
64 bytes from 10.0.0.12: icmp_seq=0 ttl=128 time=0.480 ms
64 bytes from 10.0.0.12: icmp_seq=1 ttl=128 time=0.601 ms
64 bytes from 10.0.0.12: icmp_seq=2 ttl=128 time=0.588 ms
64 bytes from 10.0.0.12: icmp_seq=3 ttl=128 time=0.564 ms
--- 10.0.0.12 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.480/0.558/0.601/0.047 ms
MSPUB-WS-VM03-MAC:~ administrator$ ping -c 4 10.0.0.13
PING 10.0.0.13 (10.0.0.13): 56 data bytes
64 bytes from 10.0.0.13: icmp_seq=0 ttl=64 time=2.167 ms
64 bytes from 10.0.0.13: icmp_seq=1 ttl=64 time=0.488 ms
64 bytes from 10.0.0.13: icmp_seq=2 ttl=64 time=0.408 ms
64 bytes from 10.0.0.13: icmp_seq=3 ttl=64 time=0.421 ms
--- 10.0.0.13 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.408/0.871/2.167/0.749 ms
MSPUB-WS-VM03-MAC:~ administrator$

```

## 4. MSPUB-WS-VM04-KAL

In a Terminal window type the command “ping -c 4 \*10.0.0.x\*”. All should reply with no packet lost.

```

MSPUB-WS-VM04-KAL:~ mspubadmin$ ping -c 4 10.0.0.101
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.
64 bytes from 10.0.0.101: icmp_seq=1 ttl=128 time=0.512 ms
64 bytes from 10.0.0.101: icmp_seq=2 ttl=128 time=11.7 ms
64 bytes from 10.0.0.101: icmp_seq=3 ttl=128 time=0.591 ms
64 bytes from 10.0.0.101: icmp_seq=4 ttl=128 time=0.438 ms
--- 10.0.0.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3041ms
rtt min/avg/max/mdev = 0.438/3.307/11.687/4.838 ms
MSPUB-WS-VM04-KAL:~ mspubadmin$ ping -c 4 10.0.0.102
PING 10.0.0.102 (10.0.0.102) 56(84) bytes of data.
64 bytes from 10.0.0.102: icmp_seq=1 ttl=64 time=0.260 ms
64 bytes from 10.0.0.102: icmp_seq=2 ttl=64 time=0.274 ms
64 bytes from 10.0.0.102: icmp_seq=3 ttl=64 time=0.329 ms
64 bytes from 10.0.0.102: icmp_seq=4 ttl=64 time=0.220 ms
--- 10.0.0.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.220/0.270/0.329/0.039 ms
MSPUB-WS-VM04-KAL:~ mspubadmin$ ping -c 4 10.0.0.103
PING 10.0.0.103 (10.0.0.103) 56(84) bytes of data.
64 bytes from 10.0.0.103: icmp_seq=1 ttl=64 time=0.379 ms
64 bytes from 10.0.0.103: icmp_seq=2 ttl=64 time=0.388 ms
64 bytes from 10.0.0.103: icmp_seq=3 ttl=64 time=0.359 ms
64 bytes from 10.0.0.103: icmp_seq=4 ttl=64 time=0.363 ms
--- 10.0.0.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3062ms
rtt min/avg/max/mdev = 0.359/0.372/0.388/0.011 ms
MSPUB-WS-VM04-KAL:~ mspubadmin$

```



```

MSPUB-WS-VM04-KAL
mspubadmin@MSPUB-WS-VM04-KAL: ~
Session Actions Edit View Help

(mspubadmin@MSPUB-WS-VM04-KAL)-[~]
$ ping -c 4 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data:
64 bytes from 10.0.0.11: icmp_seq=1 ttl=128 time=1.58 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=128 time=0.355 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=128 time=0.416 ms
64 bytes from 10.0.0.11: icmp_seq=4 ttl=128 time=0.353 ms

--- 10.0.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3045ms
rtt min/avg/max/mdev = 0.353/0.676/1.580/0.522 ms

(mspubadmin@MSPUB-WS-VM04-KAL)-[~]
$ ping -c 4 10.0.0.12
PING 10.0.0.12 (10.0.0.12) 56(84) bytes of data:
64 bytes from 10.0.0.12: icmp_seq=1 ttl=128 time=1.46 ms
64 bytes from 10.0.0.12: icmp_seq=2 ttl=128 time=1.18 ms
64 bytes from 10.0.0.12: icmp_seq=3 ttl=128 time=1.35 ms
64 bytes from 10.0.0.12: icmp_seq=4 ttl=128 time=1.05 ms

--- 10.0.0.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.054/1.261/1.457/0.154 ms

(mspubadmin@MSPUB-WS-VM04-KAL)-[~]
$ ping -c 4 10.0.0.13
PING 10.0.0.13 (10.0.0.13) 56(84) bytes of data:
64 bytes from 10.0.0.13: icmp_seq=1 ttl=64 time=2.69 ms
64 bytes from 10.0.0.13: icmp_seq=2 ttl=64 time=0.659 ms
64 bytes from 10.0.0.13: icmp_seq=3 ttl=64 time=0.311 ms
64 bytes from 10.0.0.13: icmp_seq=4 ttl=64 time=0.628 ms

--- 10.0.0.13 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.311/1.073/2.694/0.945 ms

(mspubadmin@MSPUB-WS-VM04-KAL)-[~]
$

```

## 5. MSPUB-GLLEOK-DC01

In a Terminal window type the command “ping \*10.0.0.x\*”. All should reply with no packet lost.

```

MSPUB-GLLEOK-DC01
Administrator: Windows Pow
PS C:\Users\Administrator> ping 10.0.0.101

Pinging 10.0.0.101 with 32 bytes of data:
Reply from 10.0.0.101: bytes=32 time<1ms TTL=128
Reply from 10.0.0.101: bytes=32 time<1ms TTL=128
Reply from 10.0.0.101: bytes=32 time<1ms TTL=128
Reply from 10.0.0.101: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.101:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping 10.0.0.102

Pinging 10.0.0.102 with 32 bytes of data:
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.102:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping 10.0.0.103

Pinging 10.0.0.103 with 32 bytes of data:
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.103:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:

```

```

PS C:\Users\Administrator> ping 10.0.0.104

Pinging 10.0.0.104 with 32 bytes of data:
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.104:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> ping 10.0.0.12

Pinging 10.0.0.12 with 32 bytes of data:
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128
Reply from 10.0.0.12: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.12:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator> ping 10.0.0.13

Pinging 10.0.0.13 with 32 bytes of data:
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.13:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:

```

**MSPUB-WS-VM04-KAL**

**MSPUB-COLGERA-DM01**

**MSPUB-LYNEL-WEB01**

## 6. MSPUB-COLGERA-DM01

In a Terminal window type the command “ping \*10.0.0.x\*”. All should reply with no packet lost.

```

PS C:\Users\Administrator.MSPUB> ping 10.0.0.101

Pinging 10.0.0.101 with 32 bytes of data:
Reply from 10.0.0.101: bytes=32 time<1ms TTL=128
Reply from 10.0.0.101: bytes=32 time<1ms TTL=128
Reply from 10.0.0.101: bytes=32 time<1ms TTL=128
Reply from 10.0.0.101: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.101:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator.MSPUB> ping 10.0.0.102

Pinging 10.0.0.102 with 32 bytes of data:
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64
Reply from 10.0.0.102: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.102:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator.MSPUB> ping 10.0.0.103

Pinging 10.0.0.103 with 32 bytes of data:
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64
Reply from 10.0.0.103: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.103:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:

```

**MSPUB-WS-VM01-WIN**

**MSPUB-WS-VM02-UBT**

**MSPUB-WS-VM03-MAC**

```

Administrator: Windows Pow
MSPUB-COLGERA-DM01

PS C:\Users\Administrator.MSPUB> ping 10.0.0.104

Pinging 10.0.0.104 with 32 bytes of data:
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64
Reply from 10.0.0.104: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.104:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator.MSPUB> ping 10.0.0.11

Pinging 10.0.0.11 with 32 bytes of data:
Reply from 10.0.0.11: bytes=32 time<1ms TTL=128
Reply from 10.0.0.11: bytes=32 time<1ms TTL=128
Reply from 10.0.0.11: bytes=32 time<1ms TTL=128
Reply from 10.0.0.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.11:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator.MSPUB> ping 10.0.0.13

Pinging 10.0.0.13 with 32 bytes of data:
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64
Reply from 10.0.0.13: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.0.13:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:

```

MSPUB-WS-VM04-KAL

MSPUB-GLEEOK-DC01

MSPUB-LYNEL-WEB01

## 7. MSPUB-LYNEL-WEB01

In a Terminal window type the command “ping -c 4 \*10.0.0.x\*”. All should reply with no packet lost.

```

MSPUB-LYNEL-WEB01

mspubadmin@MSPUB-LYNEL-MED01:~$ ping -c 4 10.0.0.101
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data:
64 bytes from 10.0.0.101: icmp_seq=1 ttl=128 time=1.99 ms
64 bytes from 10.0.0.101: icmp_seq=2 ttl=128 time=0.625 ms
64 bytes from 10.0.0.101: icmp_seq=3 ttl=128 time=0.945 ms
64 bytes from 10.0.0.101: icmp_seq=4 ttl=128 time=0.755 ms

--- 10.0.0.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3034ms
rtt min/avg/max/mdev = 0.255/0.987/0.950/0.320 ms
mspubadmin@MSPUB-LYNEL-MED01:~$ ping -c 4 10.0.0.102
PING 10.0.0.102 (10.0.0.102) 56(84) bytes of data:
64 bytes from 10.0.0.102: icmp_seq=1 ttl=64 time=0.660 ms
64 bytes from 10.0.0.102: icmp_seq=2 ttl=64 time=0.564 ms
64 bytes from 10.0.0.102: icmp_seq=3 ttl=64 time=0.392 ms
64 bytes from 10.0.0.102: icmp_seq=4 ttl=64 time=0.471 ms

--- 10.0.0.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.256/0.547/0.650/0.125 ms
mspubadmin@MSPUB-LYNEL-MED01:~$ ping -c 4 10.0.0.103
PING 10.0.0.103 (10.0.0.103) 56(84) bytes of data:
64 bytes from 10.0.0.103: icmp_seq=1 ttl=64 time=0.433 ms
64 bytes from 10.0.0.103: icmp_seq=2 ttl=64 time=0.589 ms
64 bytes from 10.0.0.103: icmp_seq=3 ttl=64 time=0.365 ms
64 bytes from 10.0.0.103: icmp_seq=4 ttl=64 time=0.490 ms

--- 10.0.0.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.266/0.449/0.590/0.095 ms
mspubadmin@MSPUB-LYNEL-MED01:~$ ping -c 4 10.0.0.104
PING 10.0.0.104 (10.0.0.104) 56(84) bytes of data:
64 bytes from 10.0.0.104: icmp_seq=1 ttl=64 time=0.630 ms
64 bytes from 10.0.0.104: icmp_seq=2 ttl=64 time=0.514 ms
64 bytes from 10.0.0.104: icmp_seq=3 ttl=64 time=0.402 ms
64 bytes from 10.0.0.104: icmp_seq=4 ttl=64 time=0.284 ms

--- 10.0.0.104 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms
rtt min/avg/max/mdev = 0.254/0.517/0.530/0.122 ms
mspubadmin@MSPUB-LYNEL-MED01:~$

```

MSPUB-WS-VM01-WIN

MSPUB-WS-VM02-UBT

MSPUB-WS-VM03-MAC

MSPUB-WS-VM04-KAL

```

MSPUB-LYNEL-WEB01

mspubadmin@MSPUB-LYNEL-MED01:~$ ping -c 4 10.0.0.11
PING 10.0.0.11 (10.0.0.11) 56(84) bytes of data:
64 bytes from 10.0.0.11: icmp_seq=1 ttl=128 time=0.493 ms
64 bytes from 10.0.0.11: icmp_seq=2 ttl=128 time=0.438 ms
64 bytes from 10.0.0.11: icmp_seq=3 ttl=128 time=0.701 ms
64 bytes from 10.0.0.11: icmp_seq=4 ttl=128 time=0.295 ms

--- 10.0.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3953ms
rtt min/avg/max/mdev = 0.255/0.494/0.701/0.160 ms
mspubadmin@MSPUB-LYNEL-MED01:~$ ping -c 4 10.0.0.12
PING 10.0.0.12 (10.0.0.12) 56(84) bytes of data:
64 bytes from 10.0.0.12: icmp_seq=1 ttl=128 time=0.456 ms
64 bytes from 10.0.0.12: icmp_seq=2 ttl=128 time=0.560 ms
64 bytes from 10.0.0.12: icmp_seq=3 ttl=128 time=0.769 ms
64 bytes from 10.0.0.12: icmp_seq=4 ttl=128 time=0.895 ms

--- 10.0.0.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3085ms
rtt min/avg/max/mdev = 0.255/0.543/0.895/0.143 ms
mspubadmin@MSPUB-LYNEL-MED01:~$

```

MSPUB-GLEEOK-DC01

MSPUB-COLGERA-DM01



# Security Features of Operation Systems

## Windows 11 & Windows Server 2025

Microsoft includes security features for Windows 11 and Windows Server 2025 built directly into the Operating Systems. These features will be enabled on the Windows client virtual machine as well as the Windows Server Domain Controller (DC) and Domain Manager (DM).

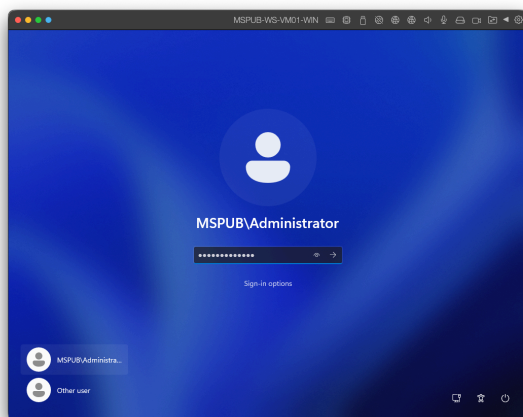
### Securing Windows 11 Client

Microsoft ships Windows 11 with numerous security features built into the operating system. These features include Microsoft Defender Antivirus, Windows Defender Firewall, Secure Boot, Automatic Windows Updates, and User Account Control (UAC) to help protect the platform. Additionally Microsoft has required a Trusted Platform Module (TPM) 2.0 chip to be installed and enabled on all motherboards prior to the installation of Windows 11. In this lab environment all clients connect to Active Directory, so it use Active Directory Domain Authentication to log in users. The features will be enabled on MSPUB-WS-VM01-WIN:

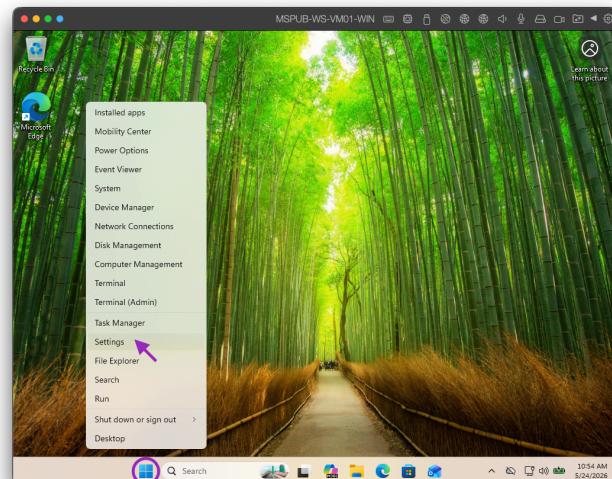
#### 1. Microsoft Defender Antivirus

Microsoft Defender Antivirus will be enabled to provide real-time protection against malware, ransomware, and other malicious software threats. Regular signature updates will also be configured through Windows Update to help maintain current threat protection.

- a. On MSPUB-WS-VM01-WIN login using MSPUB\Administrator with the password “CSNT253\_2026#”

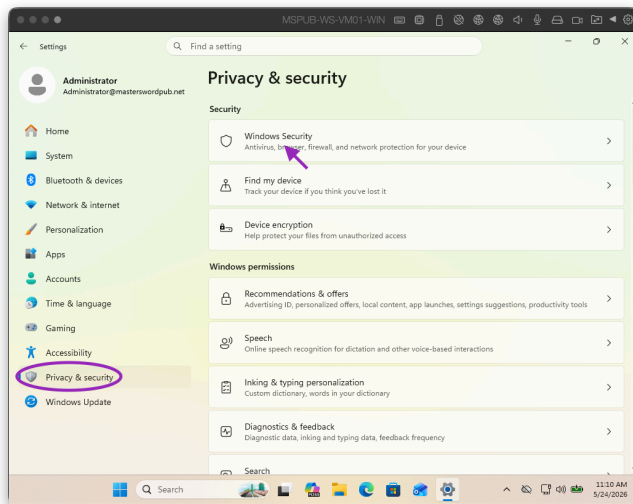


- b. Open “Settings” by right-clicking the “Windows charm” on the Taskbar.

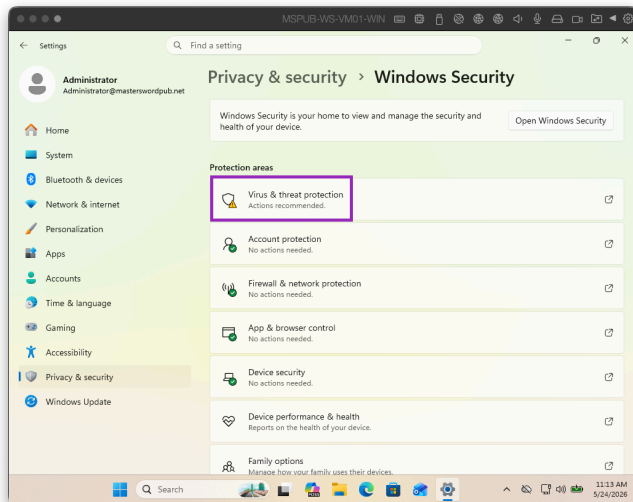


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

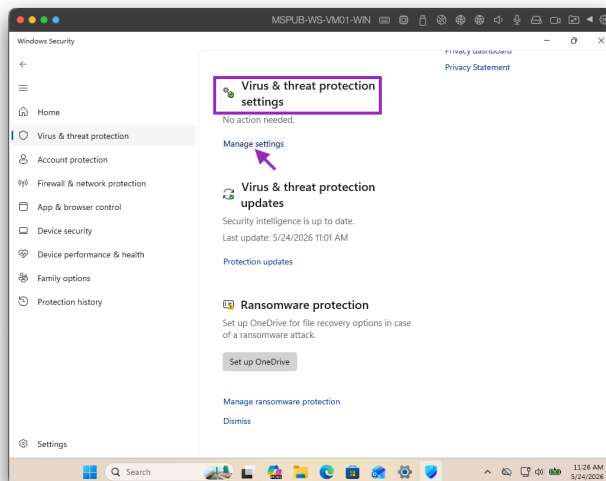
- c. In Setting click “Privacy and security on the left pane. Click “Windows Security.”



- d. In “Windows Security,” click “Virus & threat protection.”



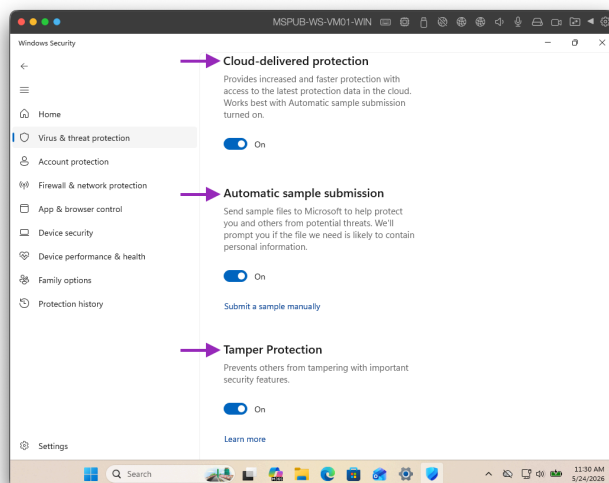
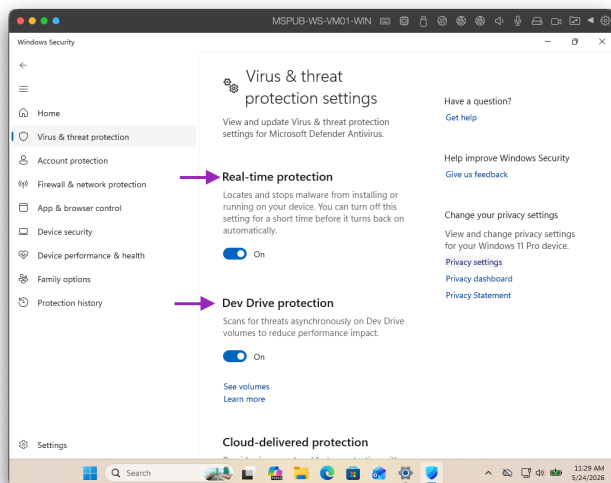
- e. Scroll down to Virus & threat protection settings, and click the “Mange settings” hyperlink.



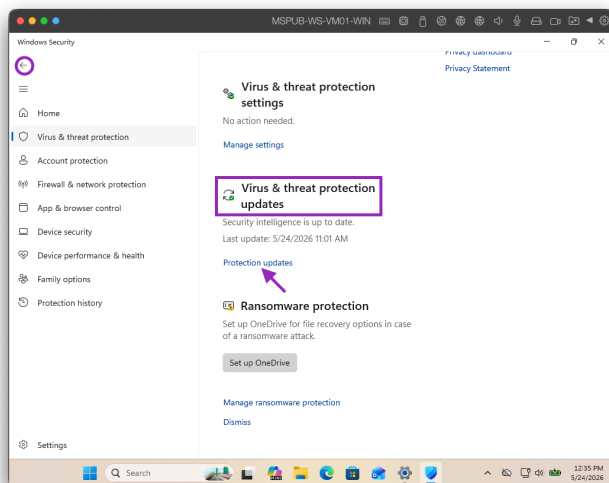
- f. Ensure that the following are enabled (“On”):
- Real-time protection

## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Dev Drive protection
- Cloud-delivered protection
- Automatic sample submission (This sends potential threats to Microsoft to help improve Windows security).
- Tamper Protections

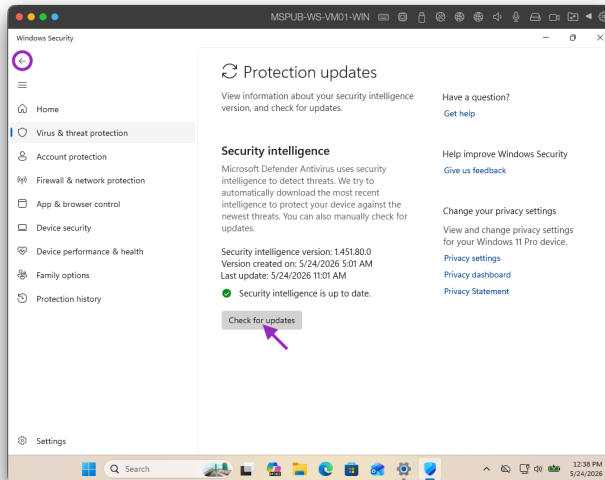


- g. Click the “back arrow” in the upper left and click the “Protection updates” hyperlink under Virus & threat protection updates.

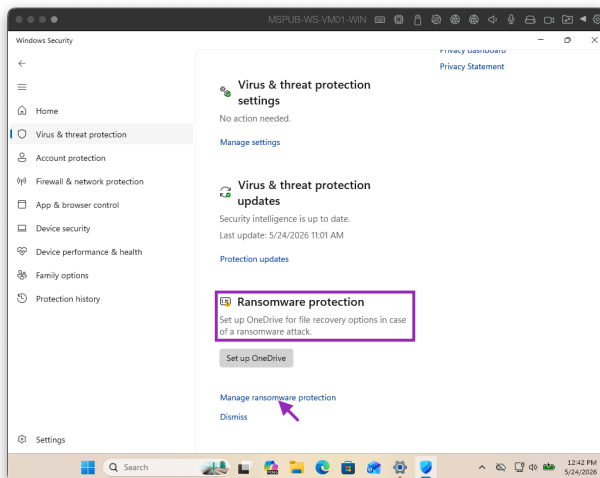


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

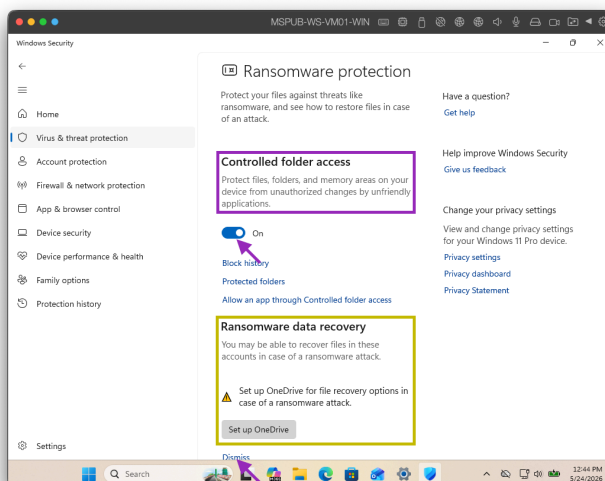
- h. Click the “Check for updates” button, if there are any updates install them. Then click the “Back arrow” in the upper left.



- i. Scroll down to Ransomware protection, and click the “Manage ransomware protection” hyperlink.

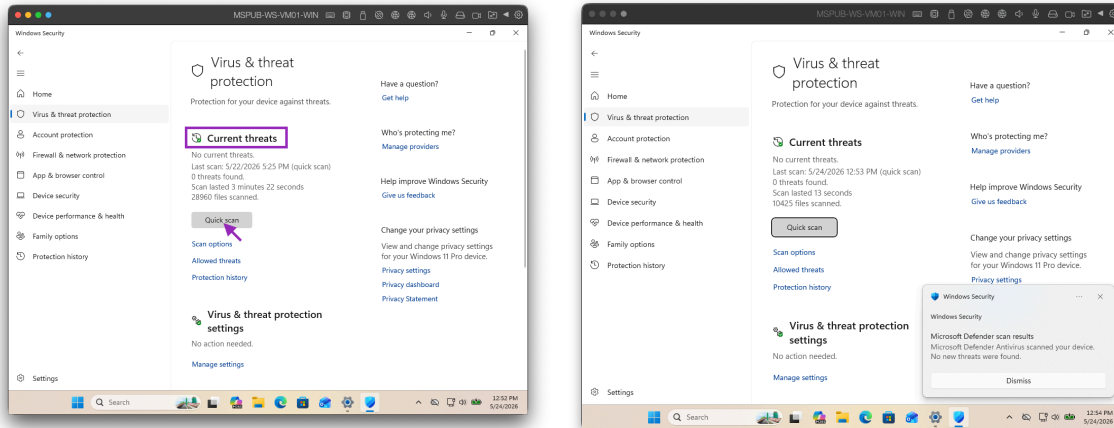


- j. Under Controlled folder access, enable (“turn on”) this feature. If there is a Microsoft Account enabled for the user click on “Set up OneDrive” to log into a Microsoft Account. This may be use if users need to recover data after a Ransomware attack. For this lab, there is no Microsoft Account associated with the MSPUB domain, so click “Dismiss” to skip this part. Click the back arrow in the upper left.



## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

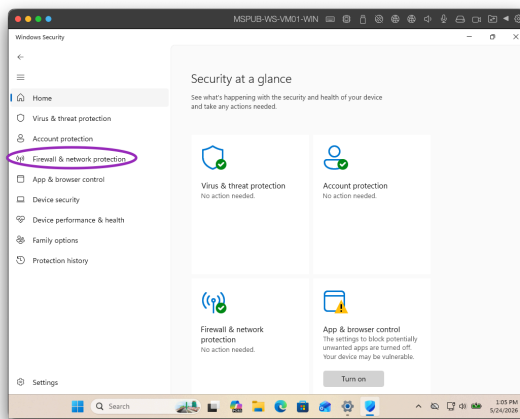
- k. Click the “Quick Scan” button under Current threats to run a scan virus scan of the system. When it is complete. Windows Defender will send a notification when it’s completed with the results. Click “Home” on the left pane once completed.



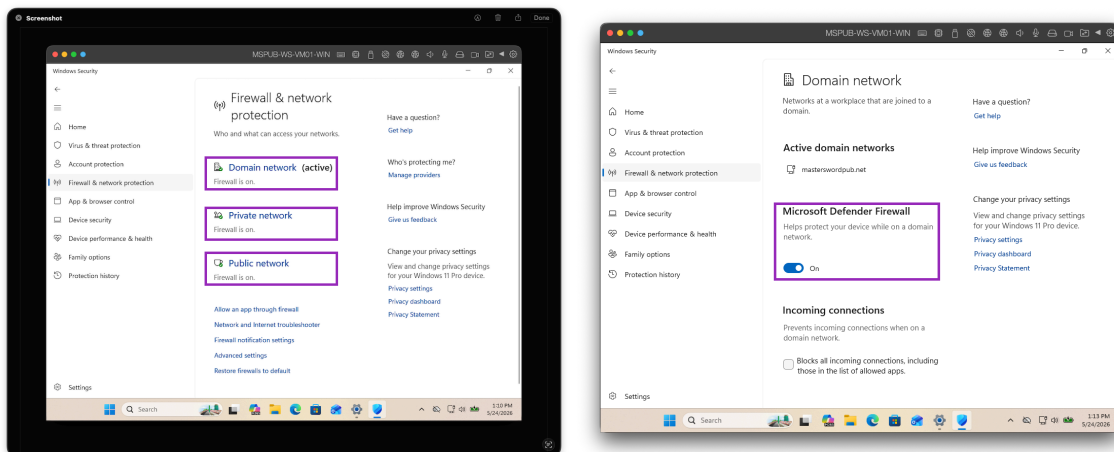
## 2. Windows Defender Firewall

Windows Defender Firewall will be enabled to monitor and filter inbound and outbound network traffic. Firewall profiles for Domain, Private, and Public networks will be configured to reduce unauthorized access to the workstation.

- a. In Windows Security click, “Firewall & network protection” on the left pane.

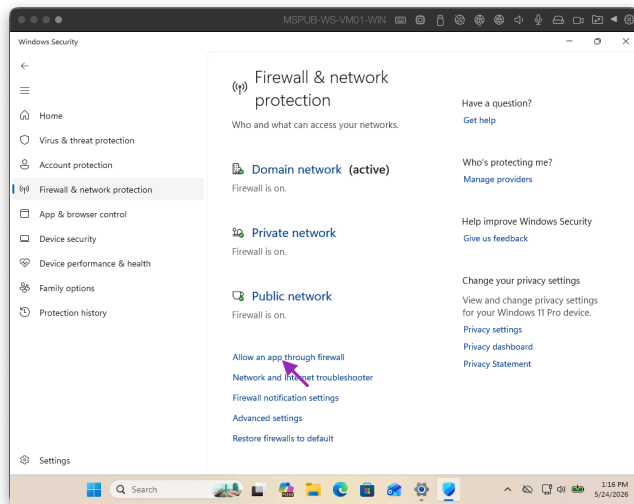


- b. Ensure that all three profiles, Domain network, Private network, and Public network say “Firewall is on.” If any of them say “Firewall is off,” click on the profile and enable it under Microsoft Defender Firewall.

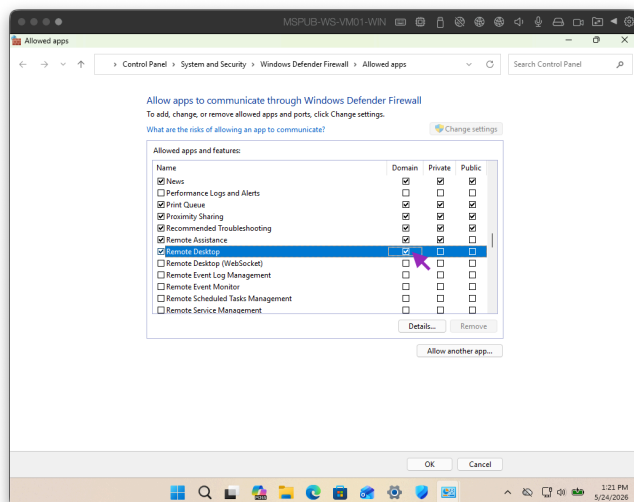


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

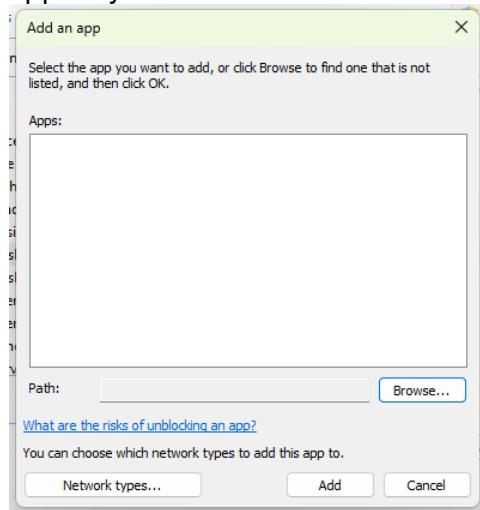
- c. To add a Firewall rule click “Allow an app through firewall” hyperlink.



- d. In this example Remote Desktop (RDP, port 3389), will be enabled on the Domain. Scroll down the list and find “Remote Desktop,” tick the box under “Domain.” Click “OK” to save the changes.



- An alternative way to add firewall rules is to click the “Allow another app...” This is useful when the service isn’t automatically in the list Windows Defender compiles. Browse and locate the app you would like to add. Click “Network types...” to specify which profiles the app may have allowed access.



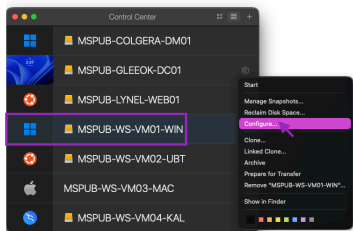
- e. Close all windows and shutdown the machine.

### 3. Trusted Platform Module (TPM) 2.0 & Secure Boot

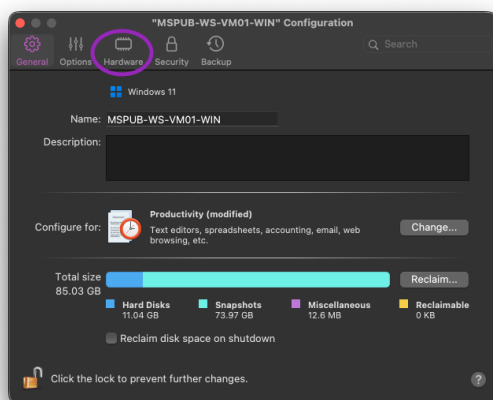
Virtual TPM 2.0 was enabled prior within the hypervisor (Parallels) to support Windows 11 security requirements and improve credential and encryption protection capabilities. On physical hardware this is a chip installed on the motherboard. It has to be enabled in the UEFI/BIOS settings, otherwise Windows 11 will not boot.

Secure Boot will be enabled through the virtual machine firmware settings to help prevent unauthorized operating systems and boot loaders from loading during system startup. On physical hardware this is configured through a systems Unified Extensible Firmware Interface (UEFI) or Basic Input/Output System (BIOS).

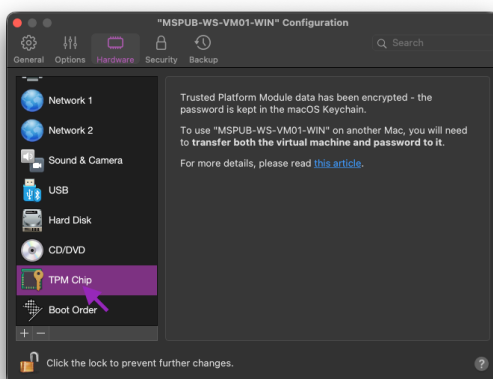
- a. With MSPUB-WS-VM01-WIN shutdown, on the host machine Parallels Control Center will be open. Right-click MSPUB-WS-VM01-WIN and select “Configure...”



- b. On the “MSPUB-WS-VM01-WIN” Configuration window, click “Hardware.”



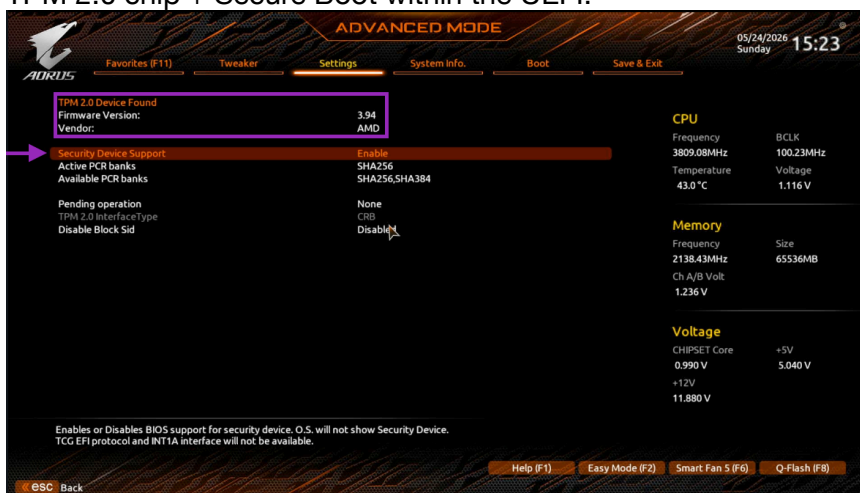
- c. Click “TPM Chip” for more information. If one needs to be added click the “+” button and select “TPM Chip.” In most cases when you create a Windows 11 VM inside of Parallels it will automatically add it when creating this virtual hardware. Having a TPM Chip installed will automatically enable Secure Boot.



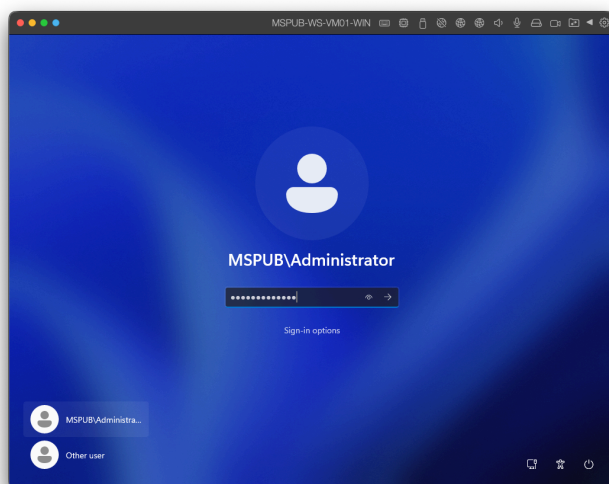


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

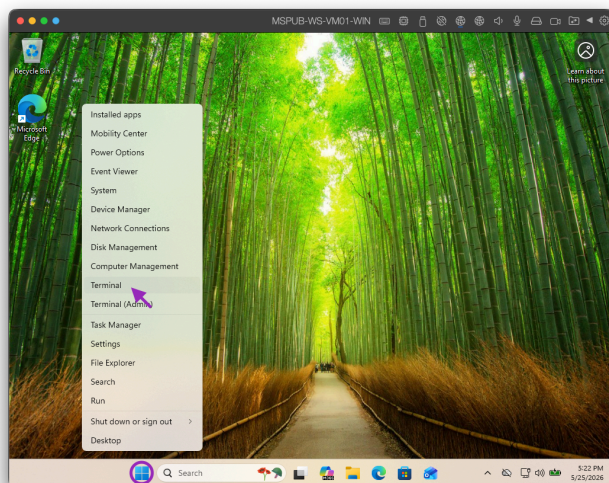
- This example is for physical hardware on a Gigabyte Aorus system showing where to enable the TPM 2.0 chip + Secure Boot within the UEFI.



- d. On MSPUB-WS-VM01-WIN login using the MSPUB\Administrator credentials.



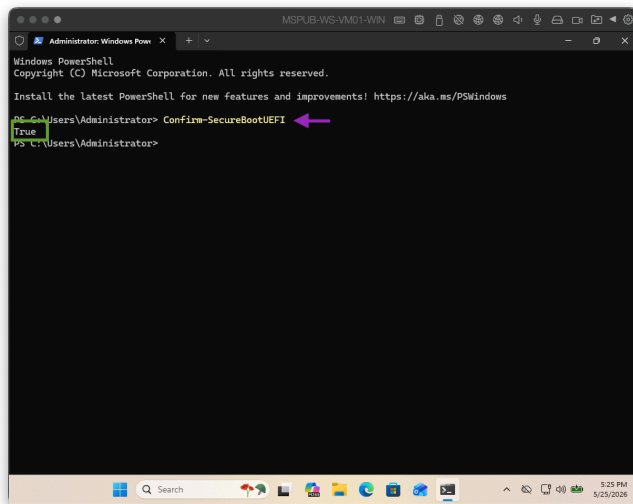
- e. Right click the "Windows charm" on the taskbar and click "Terminal."



- f. In Terminal type the following command to double check the status of Secure Boot: Confirm-SecureBootUEFI



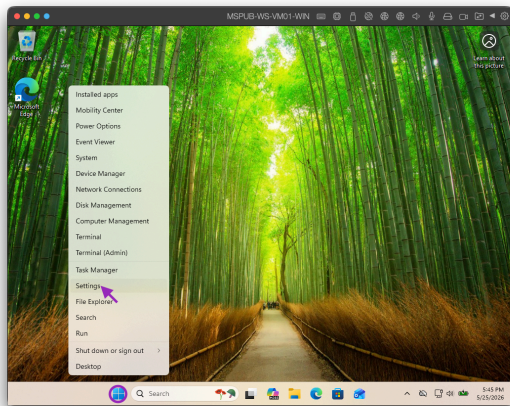
If enabled it will reply with the word “True.” Close Terminal.



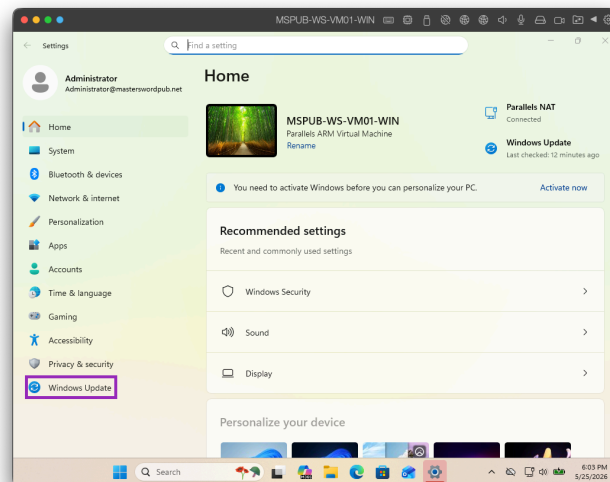
#### 4. Automatic Windows Updates

Windows Updates will be configured to automatically download and install virtual security updates and patches to help mitigate known vulnerabilities within the Windows operating system.

- Right-click the “Windows charm” and select “Settings.”

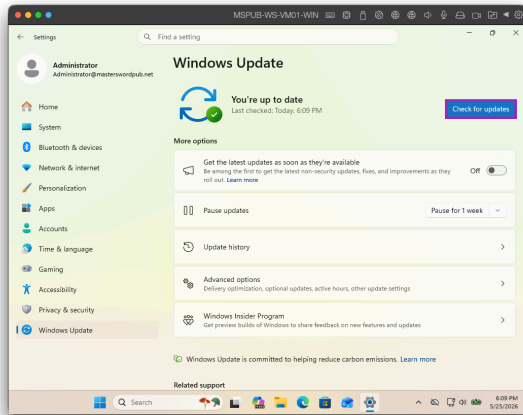


- In Settings on the left pane click “Windows Update.”

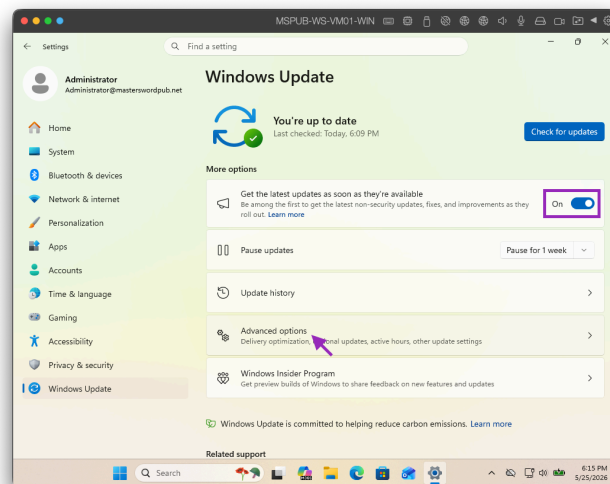


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

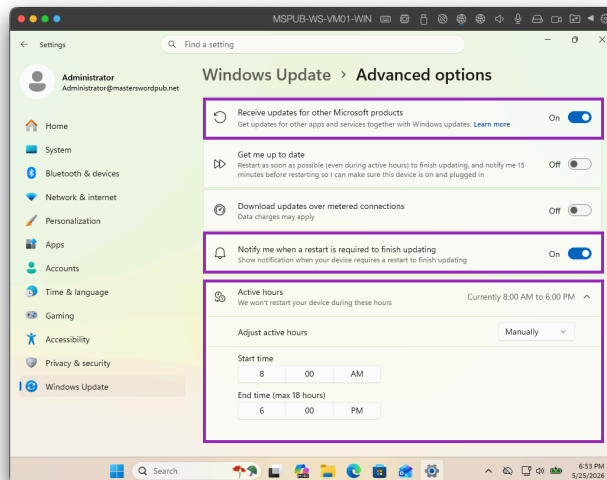
- c. In Windows Update click the “Check for updates” button. If there are any detected, install them (note: that some updates require the machine to restart).



- d. Enable “Get the latest updates as soon as they’re available.” Then click “Advanced options.”



- e. In Advanced options enable the following:
- Receive updates for other Microsoft products
  - Notify me when a restart is required to finishing updating
  - Set the active hours from 8:00am to 6:00pm

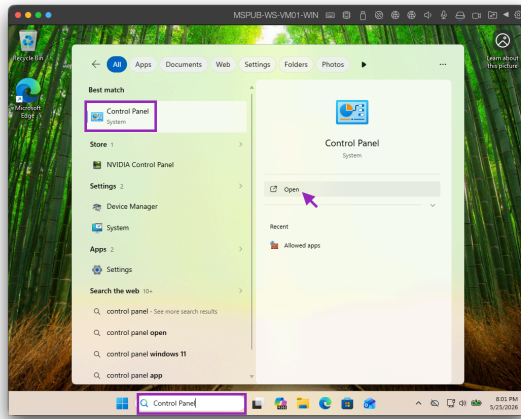


### f. Close Settings

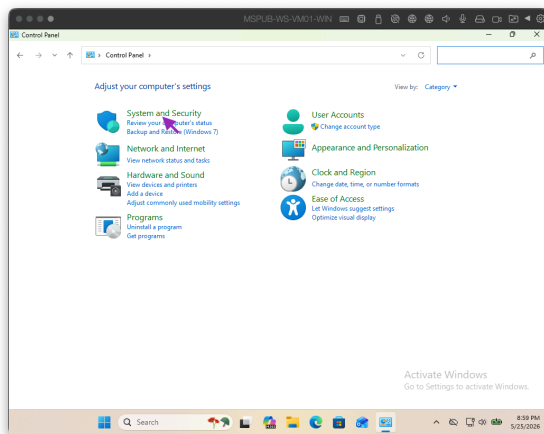
## 5. User Account Control (UAC)

User Account Control (UAC) will be enabled to reduce the risk of unauthorized administrative changes by requiring elevate permissions for system-level modifications.

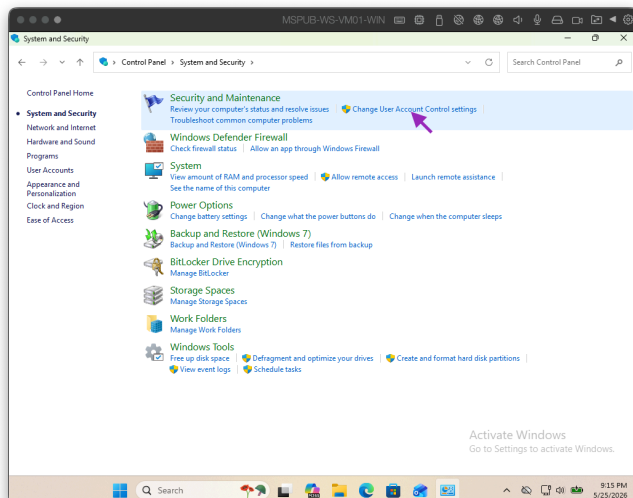
- a. Click on “Search” on the Taskbar and type “Control Panel.” Hover over the “Control Panel” search result and click on “Open.”



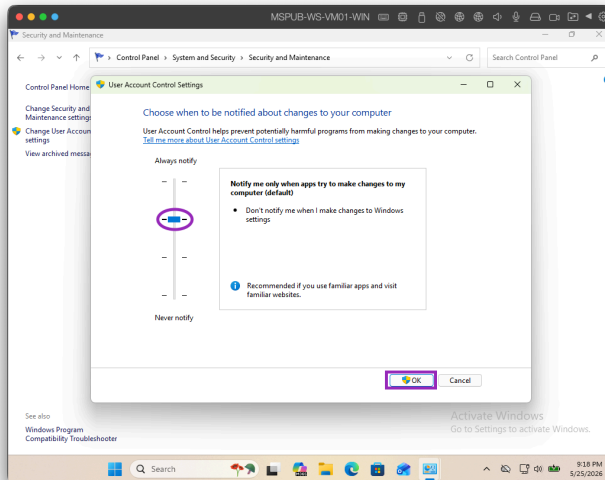
- b. In Control Panel click on the “System and Security” hyperlink.



- c. Under Security and Maintenance click on “Change User Account control settings” hyperlink.



- d. Change the UAC indicator to the third notch of the slider, “Notify me only when apps try to make changes to my computer.” Click “OK.”

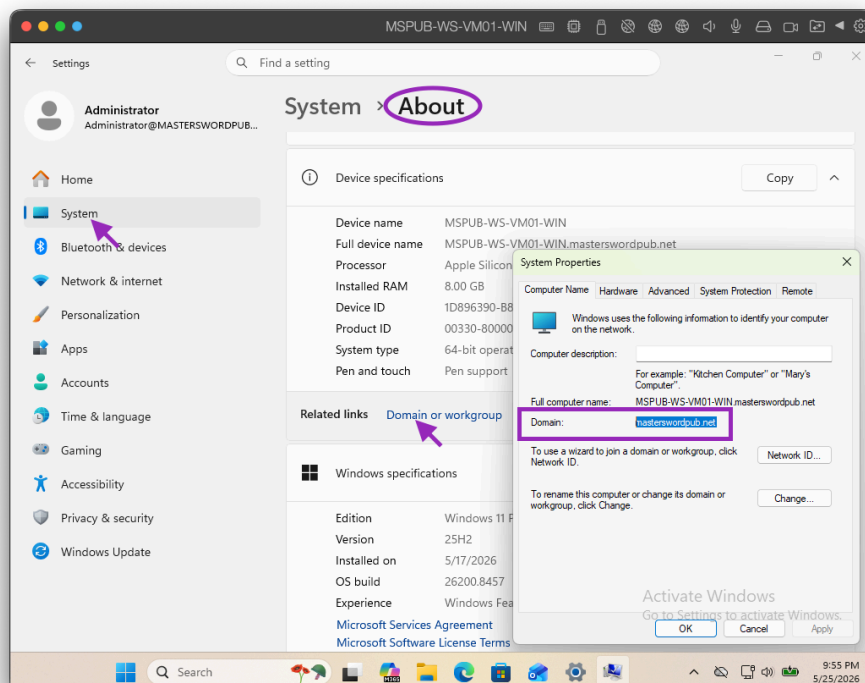


- e. Close Control Panel.

## 6. Active Directory Domain Authentication

Since MSPUB-WS-VM01-WIN was previously joined to the **masterswordpub.net** Active Directory domain, it provides centralized authentication and account management.

Joining the **masterswordpub.net** Active Directory Domain was completed previously by first giving MSPUB-WS-VM01-WIN a static IP address, 10.0.0.101. DNS was configured to point to the Domain Controller and Domain Manager servers, 10.0.0.11 and 10.0.12. Then it was added to the domain by using the “Add-Computer -DomainName” command in Terminal. This can also be done through the Windows GUI by going to Settings > System > About > Domain or Workgroup and setting it to **masterswordpub.net**. After a restart the machine can communicate with the centralized Active Directory environment to authenticate user credentials.

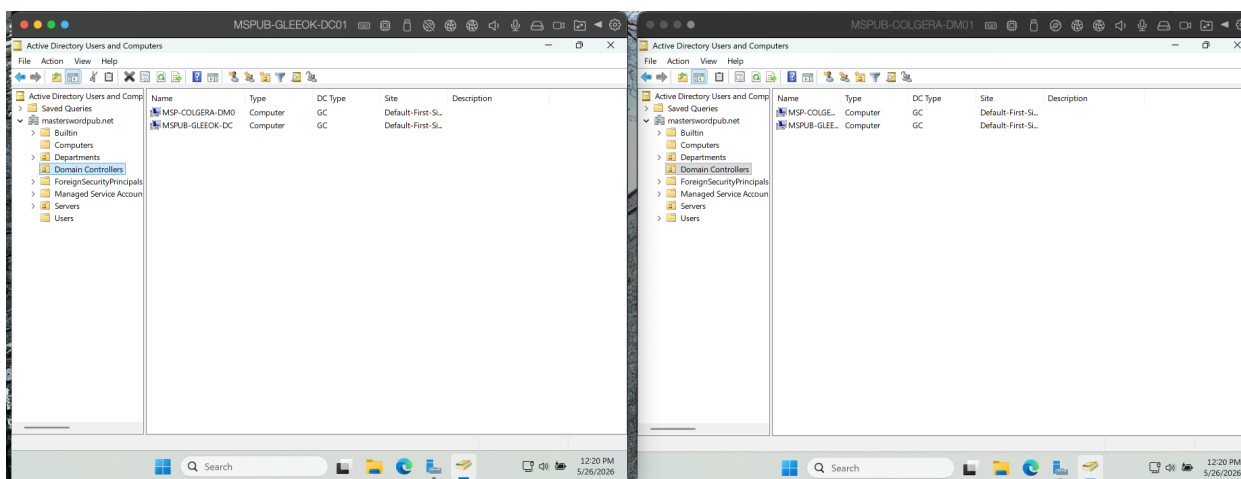


## Securing Windows Server 2025 Servers

Like Windows 11, Windows Server ships with additional security features for servers. These features include Active Directory Domain Services (AD DS), DNS Redundancy, DFS Replication (DFSR), Redundant Domain Controllers, and PowerShell Administration.

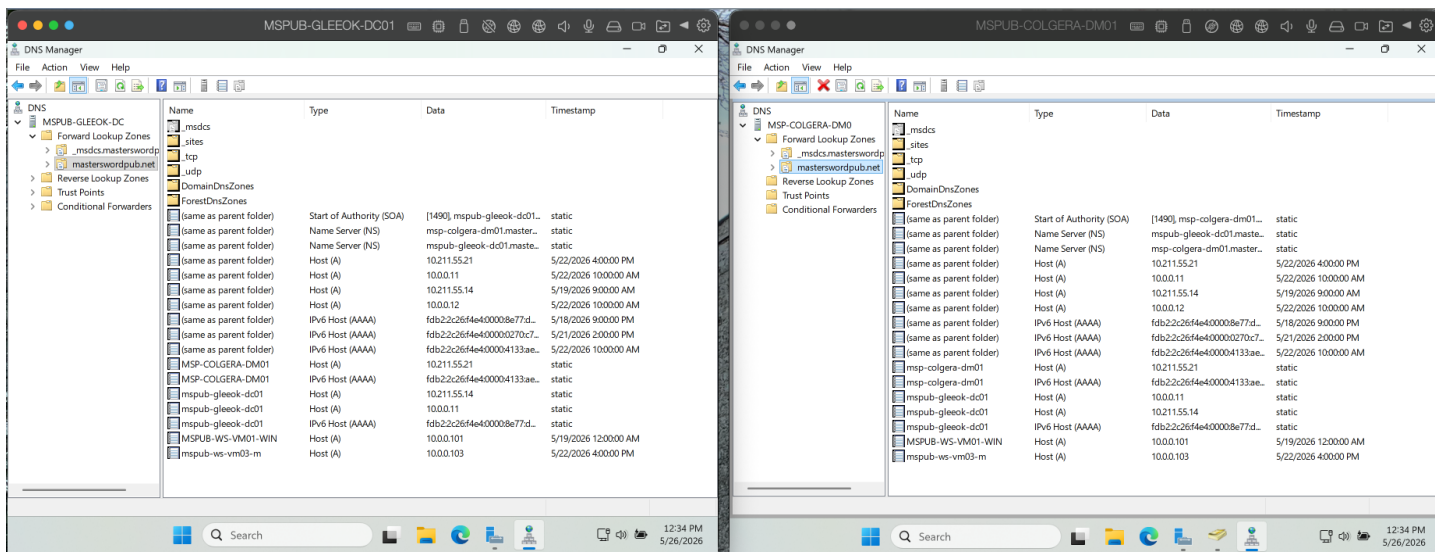
### 1. Active Directory Domain Services (AD DS)

AD DS was previously configured on both servers. MSPUB-GLEEOK-DC01 as the primary and MSPUB-COLGERA-DM01 as the secondary. Active Directory Domain Services was implemented to centralize authentication, authorization, and identity management. AD DS can be installed either by going to Managed > Add Roles and Features on Server Manager and selecting “Active Directory Domain Services” or by entering in the Terminal command, “Install-WindowsFeature AD-Domain-Services -IncludeManagementTools.” Both servers were promoted to Domain Controllers for the **masterswordpub.net** domain in Server Manager.



### 2. DNS Redundancy

Both MSPUB-GLEEOK-DC01 and MSPUB-COLGERA-DM01 were configured as DNS servers to provide redundant name resolution services. DNS Server was installed from Manage > Add Roles and Features and selecting DNS Server, or by typing the command “Install-WindowsFeature DNS -IncludeManagementTools” into Terminal. Redundant DNS infrastructure was implemented to improve reliability and fault tolerance within the **masterswordpub.net** domain.





### 3. DFS Replication (DFSR)

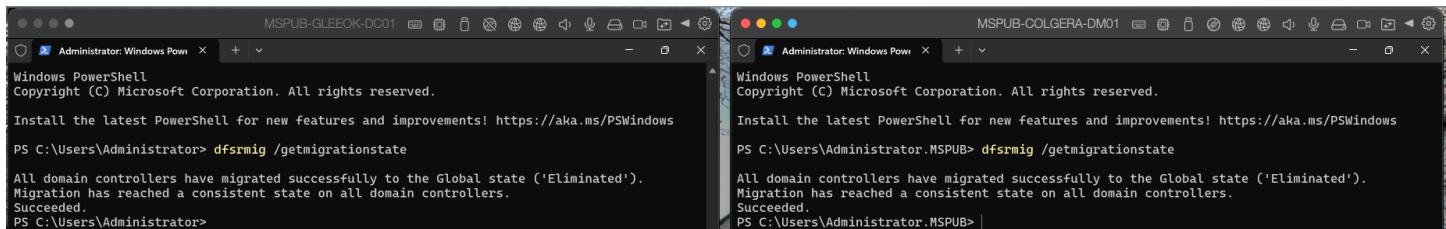
SYSVOL replication was migrated from FRS to DFSR to support modern Active Directory replication. To change the DFSR state in Terminal type the following commands:

- `dfsrmig /setglobalstate 1`
  - Wait for the “successful” reply once it has been completed switching the state.
- `dfsrmig /setglobalstate 2`
  - Wait for the “successful” reply once it has been completed switching the state.
- `dfsrmig /setglobalstate 3`
  - Wait for the “successful” reply once it has been completed switching the state.

Verify the current DFSR status by typing the command:

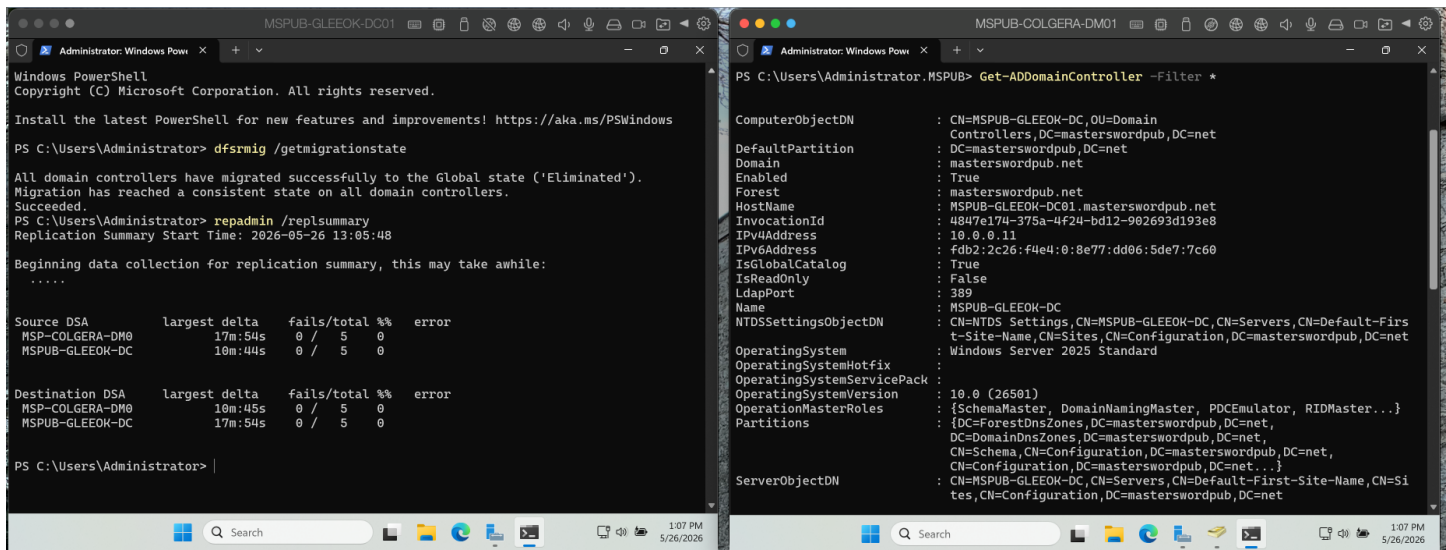
- `dfsrmig /getmigrationstate`

SYSVOL replication was modernized using DFS Replication.



### 4. Redundant Domain Controllers

A secondary domain controller was deployed to improve authentication and DNS redundancy. MSPUB-COLGERA-DM01 was promoted by installing AD DS and DNS Server and using the command, “Install-ADDSDomainController -DomainName “masterswordpub.net” -InstallDns -Credential (Get-Credential) -SiteName “Default-First-Site-Name” -ReplicationSourceDC “MSPUB-GLEEOK-DC01.masterswordpub.net” -DatabasePath “C:\Windows\NTDS” -LogPath “C:\Windows\NTDS” -SysvolPath “C:\Windows\SYSVOL” in Terminal. After install and a reboot, replication can be verified by using the commands “repadmin /replsummary” and “Get-ADDomainController -Filter \*” to display the DCs. The environment gained authentication redundancy and improved fault tolerance.



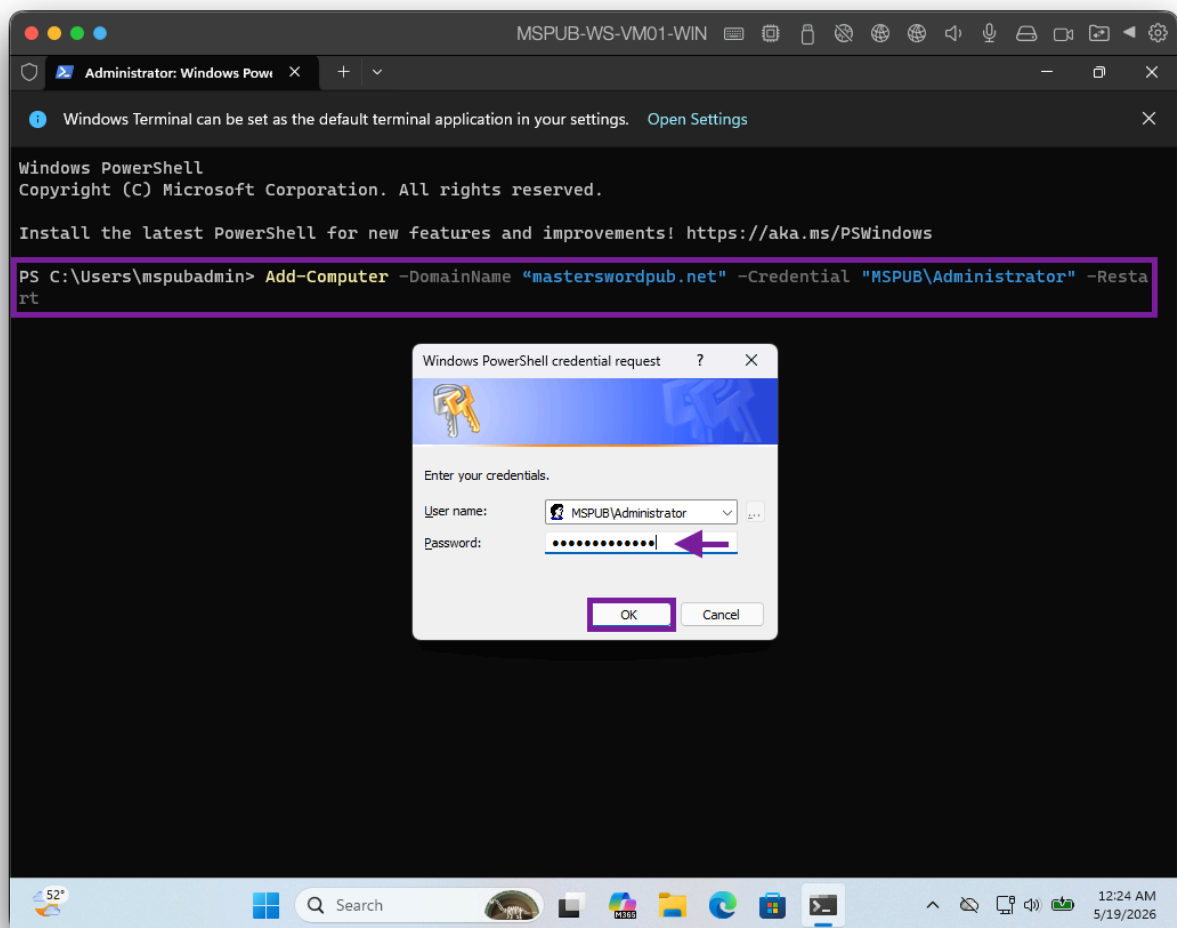
### 5. PowerShell Administration

PowerShell was used to automate server administration and Active Directory configuration tasks. These tasks were automated and standardized through PowerShell scripting and remote administration tools.

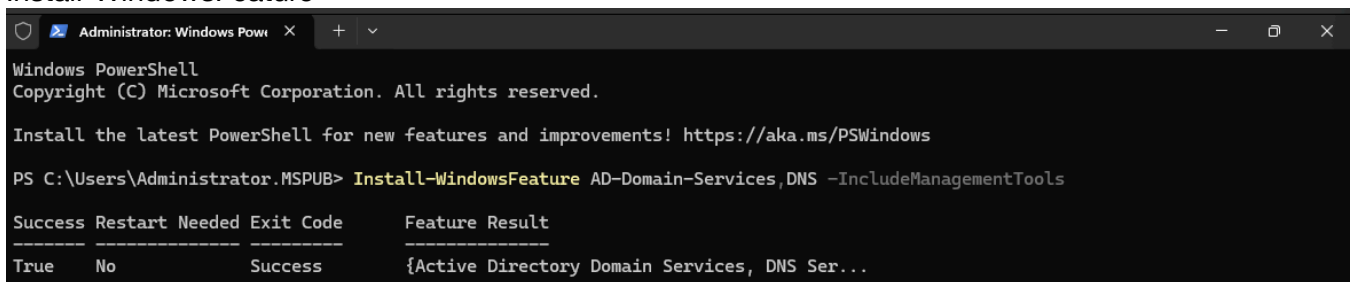
## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

The following were used:

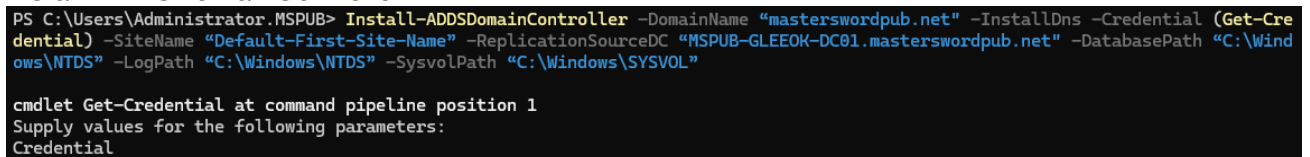
- Add-Computer



- Install-WindowsFeature



- Install-ADDSDomainController



- repadmin

```
PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2026-05-26 13:05:48

Beginning data collection for replication summary, this may take awhile:
.....

Source DSA largest delta fails/total %% error
MSP-COLGERA-DM0 17m:54s 0 / 5 0
MSPUB-GLEEOK-DC 10m:44s 0 / 5 0

Destination DSA largest delta fails/total %% error
MSP-COLGERA-DM0 10m:45s 0 / 5 0
MSPUB-GLEEOK-DC 17m:54s 0 / 5 0
```

- dfsrmig

```
PS C:\Users\Administrator> dfsrmig /getmigrationstate

All domain controllers have migrated successfully to the Global state ('Eliminated').
Migration has reached a consistent state on all domain controllers.
Succeeded.
```



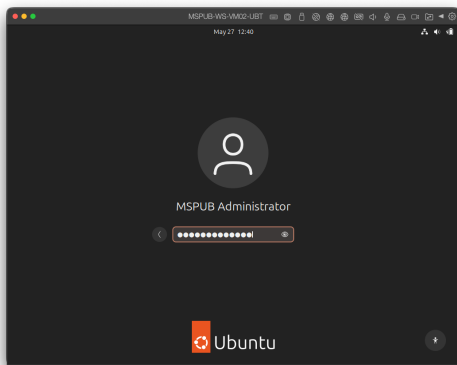
## Ubuntu Desktop & Server 26.04 LTE

Ubuntu Desktop and Server both have their own security solutions, which are basically the same. Ubuntu Desktop is typically used for Client Side, since it has a Graphical User Interface (GUI), whereas Ubuntu Server has no GUI and is strictly Command Line Interface (CLI) only. When thinking about Ubuntu there are several things that need to get hardened upon a new install. Linux administration, server hardening (if a server), enterprise networking, least privilege access, and package/security management. MSPUB-WS-VM02-UBT has the desktop client installed as the operating system, so enabling these security features will be demonstrated on this machine using the GUI. MSPUB-LYNEL-WEB01 has Ubuntu Server, so everything demonstrated will be using commands.

### Securing Ubuntu Desktop (GUI + CLI)

This section will cover how to enable security features within the graphical user interface version of Ubuntu Desktop. UFW Firewall, Least Privilege Administration, and System Updates and Package Management. These will be configured on MSPUB-WS-VM02-UBT.

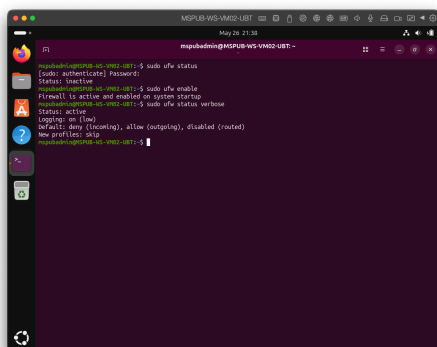
- On MSPUB-WS-VM02-UBT login using the username “MSPUB Administrator” and the password “CSNT253\_2026#” (do not use the Domain Administrator).



### 1. Uncomplicated Firewall (UFW) Configuration

Uncomplicated Firewall (UFW) was enabled to help restrict unauthorized inbound network access while allowing required administrative and domain-related traffic. Even though this is GUI, setting up UFW requires it to be done in the Terminal.

- Open Terminal from the “Ubuntu charm” on the lower left.
- To check if UFW is installed type:  
`sudo ufw status`
- If disabled enable it with the command:  
`sudo ufw enable`
- To verify the firewall status use the command:  
`sudo ufw status verbose`

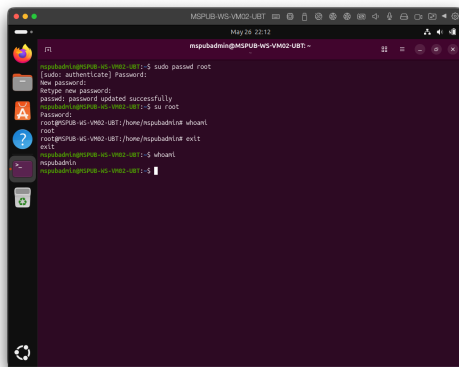


The Ubuntu Desktop system has been configured with host-based firewall protections.

### 2. Least Privilege Administration

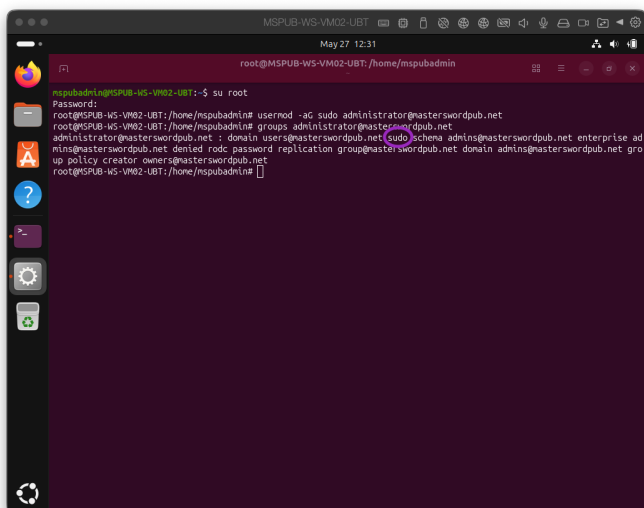
Administrative tasks were performed using sudo privileges previously rather than directly operating as the root user. It is always a good idea to change the root password and not leave the default. The MSPUB Administrator account should be able to do this by default. This will be done using Terminal commands.

- Open Terminal from the “Ubuntu charm” on the lower left.
- To change the root password type the command:  
`sudo passwd root`
- When prompted authenticate the sudo command with the MSPUB Administrator password “CSNT253\_2026#”
- When prompted enter the password the new password “M@5t3r\$w0rdPub%” and verify it.
- The password will be changed. Switch to the root user using the command:  
`su root`
- Enter the new password.
- The user in the terminal has switched to the root account. This will give you elevated privileges without the need of the sudo command. Confirm with the “whoami” command.
- Type “exit” to return to the non-privileged user.



Additionally users can be placed in specified system groups to grant and deny access to certain commands, files, and packages. To add a user to a group, in terminal use the following commands:

- In terminal use the following command to add a user to the Admin user group to grant the domain user MSPUB\Administrator sudo access:  
`sudo usermod -aG sudo administrator@masterswordpub.net`
- Authenticate the sudo command with the local MSPUB Admin password.
- Verify the change by typing these two commands:  
groups administrator@masterswordpub.net

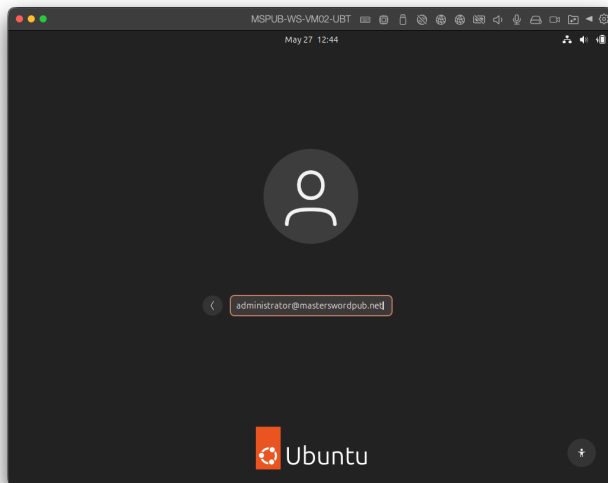


- Type “exit” twice to close the terminal
- Logout of MSPUB Administrator

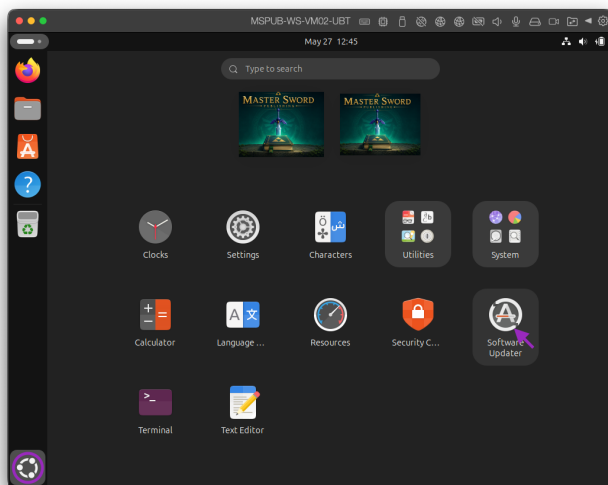
### 3. System Updates and Package Management

System updates are regularly applied to maintain current security patches and package versions. The Ubuntu Desktop workstation will remain updated with current security and stability patches. To install updates do the following:

- Login as the MSPUB\Administrator account



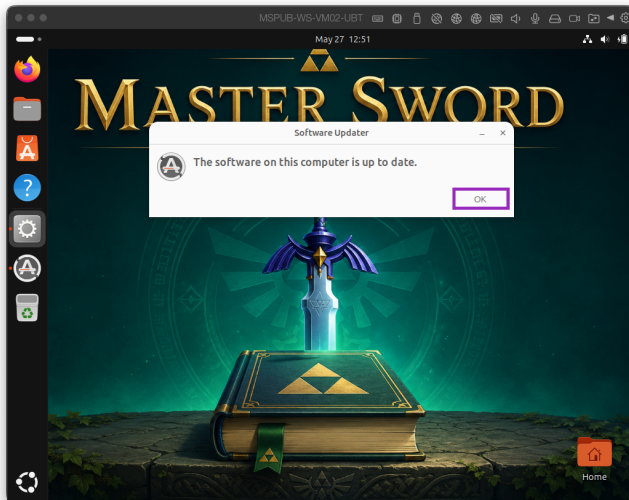
- Click the “Ubuntu charm” in the lower left corner and select “Software Updater”



- Ubuntu will search and download updates click the “Details” arrow to show a list of Security updates and Other updates. Leave them all selected and click “Install Now.”



- Once the packages are finished installing click “OK.” Ubuntu should now be up-to-date.



### Securing Ubuntu Server (CLI Only)

Securing Ubuntu Server has the same security features as Ubuntu Desktop, however is strictly done using the command line interface (CLI) as there is no graphical user interface (GUI). The same three elements will be configured as above as well as OpenSSH Administration, since most of the time companies will use the SSH protocol to manage Ubuntu Servers instead of going to the actual server terminal.

- Log into MSPUB-LYNEL-WEB01 using the mspubadmin user credentials

```
MSPUB-LYNEL-WEB01
ubuntu 26.04 LTS MSPUB-LYNEL-WEB01 tty1
Try contacting this VM's SSH server via 'ssh vscd3221225473' from host.
MSPUB-LYNEL-WEB01 login: mspubadmin
Password:
Welcome to Ubuntu 26.04 LTS (GNU/Linux 7.8.0-35-generic aarch64)

 * Documentation: https://docs.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/support

System information as of Wed May 27 01:43:59 PM PDT 2026

System load: 0.15 Processes: 137
Usage of /: 31.7% of 38.7GB Memory usage: 0%
Swap usage: 0% IP address for enp0s1: 10.0.0.13

 * There is a pending process.
 * Strictly configured Kubernetes makes edge and IoT secure. Learn how MicroK8s
 just raised the bar for easy, resilient and secure K8s cluster deployment.
 https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo apt update
mspubadmin@MSPUB-LYNEL-WEB01:~$
```

## 1. UFW Firewall Hardening

Uncomplicated Firewall (UFW) will be enabled to help restrict unauthorized inbound network access while allowing required administrative and domain-related traffic. Host-based firewall protections will be implemented while maintaining administrative SSH access. Use the following commands to enable UFW:

- Enable UFW by typing:  
sudo ufw enable
- Authenticate the sudo command with the mspubadmin password
- Allow the required services:  
sudo ufw allow ssh
- Verify UFW configuration  
sudo ufw status

```
mspubadmin@MSPUB-LYNEL-WEB01:~$ sudo ufw enable
[sudo: authenticate] Password:
Firewall is active and enabled on system startup
mspubadmin@MSPUB-LYNEL-WEB01:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
mspubadmin@MSPUB-LYNEL-WEB01:~$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

mspubadmin@MSPUB-LYNEL-WEB01:~$ _
```

## 2. Least Privileged Access

Administrative tasks were performed using sudo privileges previously rather than directly operating as the root user. It is always a good idea to change the root password and not leave the default. The MSPUB Administrator account should be able to do this by default. This will be done using commands.

- To change the root password type the command:  
sudo passwd root
- When prompted authenticate the sudo command with the MSPUB Administrator password “CSNT253\_2026#”
- When prompted enter the password the new password “M@5t3r\$w0rdPub%” and verify it.
- The password will be changed. Switch to the root user using the command:  
su root
- Enter the new password.
- The user in the terminal has switched to the root account. This will give you elevated privileges without the need of the sudo command. Confirm with the “whoami” command.
- Type “exit” to return to the non-privileged user.

```
mspubadmin@MSPUB-LYNEL-WEB01:~$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
mspubadmin@MSPUB-LYNEL-WEB01:~$ su root
Password:
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# whoami
root
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# _
```

At this time MSPUB-LYNEL-WEB01 has not joined the MSPUB domain. So an additional user will be added manually to add to a group. Groups can be setup to allow or deny access to files or commands.

- Add a new test user by typing the following command:  
`sudo adduser mspubtestuser`
- Enter in the following information when prompted:  
New Password: **CSNT253\_2026#**  
Retype New Password: **CSNT253\_2026#**  
Full Name: MSPUB TestUser  
Press Enter for the remaining fields to skip them
- Type “Y” when asked if the information is correct
- Use the command to add the user to the sudoers group:  
`sudo usermod -aG sudo mspubtestuser`
- Verify the user was added with the command:  
`groups mspubtestuser`  
sudo should show in the group lists for mspubtestuser
- Delete the MSPUB TestUser account by using the command:  
`sudo deluser --remove-home mspubtestuser`

```
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# sudo adduser mspubtestuser
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mspubtestuser
Enter the new value, or press ENTER for the default
 Full Name []: MSPUB TestUser
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] Y
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# sudo usermod -aG sudo mspubtestuser
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# groups mspubtestuser
mspubtestuser : mspubtestuser sudo users
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# sudo deluser --remove-home mspubtestuser
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# _
```

### 3. OpenSSH Administration

OpenSSH allows users and administrators to connect to the server remotely from a Terminal session or other Secure Shell client program. MSPUB-LYNEL-WEB01 will be configured to support secure remote administration. This will be tested using another client machine to ensure SSH protocol connections on the local network.

- Update the package files to ensure OpenSSH installs the current version:  
`sudo apt update`
- Install OpenSSH with the command:  
`sudo apt install openssh-server -y`
- Once installation is finished verify the service was installed by typing:  
`sudo systemctl status ssh`
- To ensure OpenSSH opens during system boot type:  
`sudo systemctl enable ssh`

```

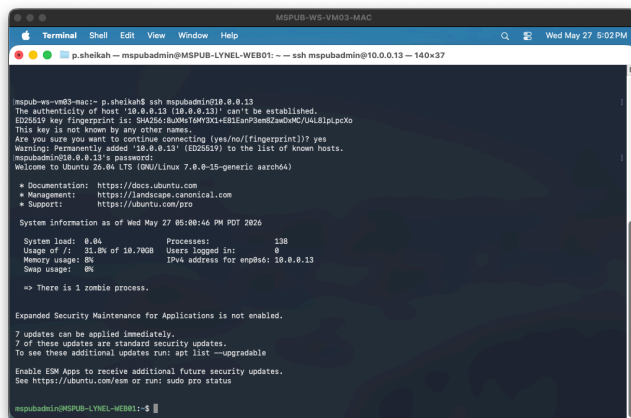
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# sudo apt update
0% [Working]

Get:1 http://security.ubuntu.com/ubuntu resolute-security InRelease [136 kB]
0% [Waiting for headers] [1 InRelease 2,533 B/136 kB 2%]

Hit:2 http://archive.ubuntu.com/ubuntu resolute InRelease
Get:3 http://archive.ubuntu.com/ubuntu resolute-updates InRelease [136 kB]
Get:4 http://security.ubuntu.com/ubuntu resolute-security/main arm64 Packages [97.4 kB]
Get:5 http://security.ubuntu.com/ubuntu resolute-security/main Translation-en [31.6 kB]
Get:6 http://security.ubuntu.com/ubuntu resolute-security/main arm64 Components [2,848 B]
Get:7 http://security.ubuntu.com/ubuntu resolute-security/universe arm64 Packages [52.4 kB]
Get:8 http://security.ubuntu.com/ubuntu resolute-security/universe Translation-en [18.8 kB]
Get:9 http://security.ubuntu.com/ubuntu resolute-security/universe arm64 Components [39.8 kB]
Hit:10 http://archive.ubuntu.com/ubuntu resolute-backports InRelease
Get:11 http://archive.ubuntu.com/ubuntu resolute-updates/main arm64 Packages [104 kB]
Get:12 http://archive.ubuntu.com/ubuntu resolute-updates/main Translation-en [33.4 kB]
Get:13 http://archive.ubuntu.com/ubuntu resolute-updates/main arm64 Components [9,956 B]
Get:14 http://archive.ubuntu.com/ubuntu resolute-updates/universe arm64 Packages [56.2 kB]
Get:15 http://archive.ubuntu.com/ubuntu resolute-updates/universe Translation-en [19.9 kB]
Get:16 http://archive.ubuntu.com/ubuntu resolute-updates/universe arm64 Components [46.0 kB]
Fetched 784 kB in 1s (566 kB/s)
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# sudo apt install openssh-server -y
openssh-server is already the newest version (1:10.2p1-2ubuntu3.2).
Summary:
 Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 7
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/ssh.service' -> /usr/lib/systemd/system/ssh.service'.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service' -> /usr/lib/systemd/system/ssh.service'.
root@MSPUB-LYNEL-WEB01:/home/mspubadmin# sudo systemctl status ssh
* ssh.service - OpenSSH Secure Shell server
 Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
 Active: inactive (dead)
 TriggeredBy: • ssh.socket
 Docs: man:sshd(8)
 man:sshd_config(5)
root@MSPUB-LYNEL-WEB01:/home/mspubadmin#

```

- Verify by using a different client machine that has an SSH client. In this example MSPUB-WS-VM03-MAC will connect using a Terminal SSH session. To connect type the command: `ssh mspubadmin@10.0.0.13`
- Accept the connect by typing “yes”
- Enter the password for the mspubadmin account
- The connection from MSPUB-WS-VM03-MAC to MSPUB-LYNEL-WEB01 is established
- Type “exit” to logout



```

MSPUB-WS-VM03-MAC
Terminal Shell Edit View Window Help
p.sheikhah ~ mspubadmin@MSPUB-LYNEL-WEB01: ~ — ssh mspubadmin@10.0.0.13 — 140x37

mspub-ws-vm03-mac~ p.sheikhah ssh mspubadmin@10.0.0.13
The authenticity of host '10.0.0.13 (10.0.0.13)' can't be established.
ED25519 key fingerprint is SHA256:Bu0h7wvWz1+451wPm2wmcW3kAlp1pko
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.13' (ED25519) to the list of known hosts.
mspubadmin@10.0.0.13's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 7.6.0-15-generic aarch64)

 * Documentation: https://docs.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Wed May 27 05:08:46 PM PDT 2024

System load: 0.04 Processes: 138
Usage of /: 21.0% of 10.70GB Users logged in: 0
Memory usage: 0% IP address for enp4s6: 10.0.0.13
Swap usage: 0%

=> There is 1 zombie process.

Expanded Security Maintenance for Applications is not enabled.

7 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

mspubadmin@MSPUB-LYNEL-WEB01:~$

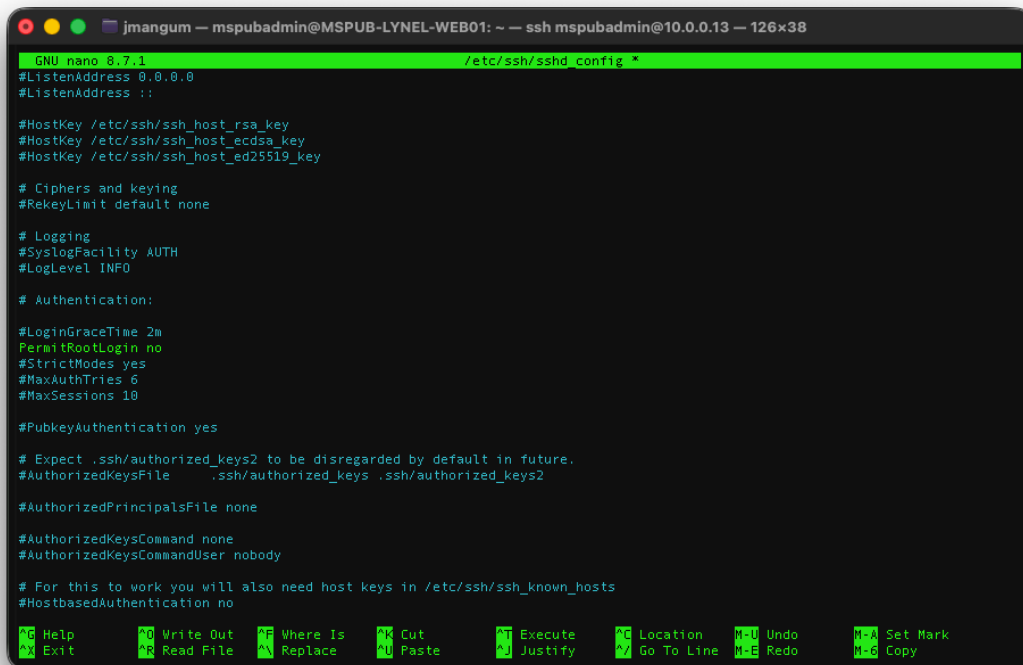
```

It is also a good idea to disable the root user from being able to login via the SSH protocol. To do that use the following commands:

- Edit the SSH Configuration file using Nano Text Editor:  
`sudo nano /etc/ssh/sshd_config`
- Authenticate using the mspubadmin password



- Find #PermitRootLogin and change it to: PermitRootLogin



```
GNU nano 8.7.1 /etc/ssh/sshd_config
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

Ciphers and keying
#RekeyLimit default none

Logging
#SyslogFacility AUTH
#LogLevel INFO

Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

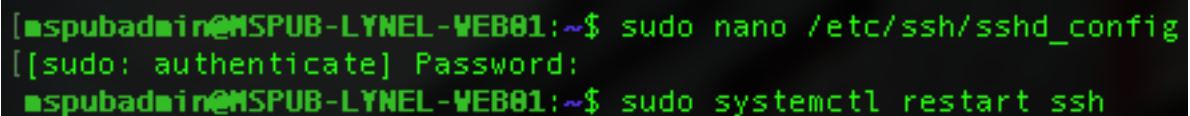
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no

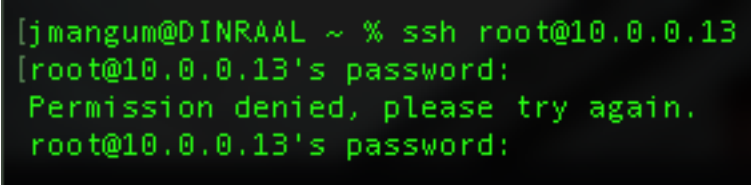
Help Write Out Where Is Cut Execute Location M-U Undo M-A Set Mark
Exit Read File Replace Paste Justify Go To Line M-E Redo M-G Copy
```

- Press CTRL+O to save changes and CTRL+X to exit.
- Restart the SSH service by typing: (if connected via SSH currently, your connection will be dropped)  
`sudo systemctl restart ssh`



```
[mspbadm@MSPUB-LYNEL-WEB01:~]$ sudo nano /etc/ssh/sshd_config
[[sudo: authenticate] Password:
mspbadm@MSPUB-LYNEL-WEB01:~$ sudo systemctl restart ssh
```

- Try logging into the root user via SSH now, in the host machine's Terminal or SSH client:  
`ssh root@10.0.0.13`
- The connection will fail.



```
[jmgangum@DINRAAL ~ % ssh root@10.0.0.13
[root@10.0.0.13's password:
Permission denied, please try again.
root@10.0.0.13's password:
```

#### 4. System Updates and Package Management

Since there is no GUI there are commands that can be run to update the system and its packages. Enter the following to update the system:

- Update the packages list by typing:  
`sudo apt update`
- Install the the packages with dependancies by typing:  
`sudo apt upgrade -y`



- System and packages will be updated

```

jmanqum — mspubadmin@MSPUB-LYNEL-WEB01: ~ — ssh mspubadmin@10.0.0.13 — 169x97

[mspubadmin@MSPUB-LYNEL-WEB01:~]$ sudo apt update
Ign:1 http://archive.ubuntu.com/ubuntu resolute InRelease
Ign:2 http://archive.ubuntu.com/ubuntu resolute-updates InRelease
Ign:3 http://archive.ubuntu.com/ubuntu resolute-backports InRelease
Ign:4 http://security.ubuntu.com/ubuntu resolute-security InRelease
Ign:3 http://archive.ubuntu.com/ubuntu resolute-backports InRelease
Ign:2 http://archive.ubuntu.com/ubuntu resolute-updates InRelease
Ign:1 http://archive.ubuntu.com/ubuntu resolute InRelease
Ign:4 http://security.ubuntu.com/ubuntu resolute-security InRelease
Ign:3 http://archive.ubuntu.com/ubuntu resolute-backports InRelease
Ign:2 http://archive.ubuntu.com/ubuntu resolute-updates InRelease
Err:1 http://archive.ubuntu.com/ubuntu resolute InRelease
 Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::6814:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to archive.ub
untu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable)
Err:2 http://archive.ubuntu.com/ubuntu resolute-updates InRelease
 Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::6814:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to archive.ub
untu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable)
Err:3 http://archive.ubuntu.com/ubuntu resolute-backports InRelease
 Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::6814:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to archive.ub
untu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable)
Err:4 http://security.ubuntu.com/ubuntu resolute-security InRelease
 Cannot initiate the connection to security.ubuntu.com:80 (2686:4788:10::6814:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to security.
ubuntu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable) Could not connect to security.ubuntu.com:80 (172.66.152.176), connection timed out Could no
t connect to security.ubuntu.com:80 (172.66.152.176), connection timed out
 Cannot initiate the connection to security.ubuntu.com:80 (2686:4788:10::6814:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to security.
ubuntu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable)
Err:4 http://security.ubuntu.com/ubuntu resolute-security InRelease
 Cannot initiate the connection to security.ubuntu.com:80 (2686:4788:10::6814:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to security.
ubuntu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable) Could not connect to security.ubuntu.com:80 (172.66.152.176), connection timed out
 Cannot initiate the connection to security.ubuntu.com:80 (2686:4788:10::6814:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to security.
ubuntu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable)
7 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: Failed to fetch http://archive.ubuntu.com/ubuntu/dists/resolute/InRelease Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::6814:1cf6). -
connect (101: Network is unreachable) Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable)
Warning: Failed to fetch http://archive.ubuntu.com/ubuntu/dists/resolute-updates/InRelease Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::6814:1
cf6). - connect (101: Network is unreachable) Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable)
Warning: Failed to fetch http://archive.ubuntu.com/ubuntu/dists/resolute-backports/InRelease Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::6814
:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to archive.ubuntu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachable)
Warning: Failed to fetch http://security.ubuntu.com/ubuntu/dists/resolute-security/InRelease Cannot initiate the connection to security.ubuntu.com:80 (2686:4788:10::681
4:1cf6). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2686:4788:10::ac42:98b8). - connect (101: Network is unreachab
le)
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
[mspubadmin@MSPUB-LYNEL-WEB01:~]$ sudo apt upgrade -y
Upgrading:
 libcrypt20 libssh2-1t64 vim vim-common vim-runtime vim-tiny xxd

Summary:
 Upgrading: 7, Installing: 0, Removing: 0, Not Upgrading: 0
 7 standard LTS security updates
 Download size: 0 B / 11.6 MB
 Freed space: 68.6 KB

(Reading database... 106709 files and directories currently installed.)
Preparing to unpack ./libcrypt20_1:12.0-2ubuntu0.1_arm64.deb...
Unpacking libcrypt20:arm64 (1:12.0-2ubuntu0.1) over (1:12.0-2)...
Setting up libcrypt20:arm64 (1:12.0-2ubuntu0.1)...
(Reading database... 106709 files and directories currently installed.)
Preparing to unpack ./vim_2:9.1.2141-1ubuntu4.2_arm64.deb...
Unpacking vim (2:9.1.2141-1ubuntu4.2) over (2:9.1.2141-1ubuntu4.1)...
Preparing to unpack ./vim-common_2:9.1.2141-1ubuntu4.2_all.deb...
Unpacking vim-common (2:9.1.2141-1ubuntu4.2) over (2:9.1.2141-1ubuntu4.1)...
Preparing to unpack ./vim-tiny_2:9.1.2141-1ubuntu4.2_arm64.deb...
Unpacking vim-tiny (2:9.1.2141-1ubuntu4.2) over (2:9.1.2141-1ubuntu4.1)...
Preparing to unpack ./vim-runtime_2:9.1.2141-1ubuntu4.2_all.deb...
Unpacking vim-runtime (2:9.1.2141-1ubuntu4.2) over (2:9.1.2141-1ubuntu4.1)...
Preparing to unpack ./4-xxd_2:9.1.2141-1ubuntu4.2_arm64.deb...
Unpacking xxd (2:9.1.2141-1ubuntu4.2) over (2:9.1.2141-1ubuntu4.1)...
Preparing to unpack ./5-libssh2-1t64_1:11.1-1ubuntu0.26.04.1_arm64.deb...
Unpacking libssh2-1t64:arm64 (1:11.1-1ubuntu0.26.04.1) over (1:11.1-1build2)...
Setting up xxd (2:9.1.2141-1ubuntu4.2)...
Setting up vim-common (2:9.1.2141-1ubuntu4.2)...
Setting up libssh2-1t64:arm64 (1:11.1-1ubuntu0.26.04.1)...
Setting up vim-runtime (2:9.1.2141-1ubuntu4.2)...
Setting up vim (2:9.1.2141-1ubuntu4.2)...
Setting up vim-tiny (2:9.1.2141-1ubuntu4.2)...
Processing triggers for libc-bin (2.43-2ubuntu2)...
Processing triggers for man-db (2.13.1-1build1)...
Scanning processes...

Scanning candidates...

Scanning linux images...

Running kernel seems to be up-to-date (ABI upgrades are not detected).

Restarting services...
systemctl restart fwupd.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
[mspubadmin@MSPUB-LYNEL-WEB01:~]$

```

## macOS 26 Tahoe

Apple has built multiple security features directly into macOS. These features help protect user accounts, system files, network communications, and application integrity. Security settings focus on encryption, malware prevention, system hardening, and account protection. FileVault Disk Encryption, macOS Firewall, Gatekeeper Application Security, XProtect Malware Protection, Lockdown Mode, Automatic System Updates, and Open Directory Integration.

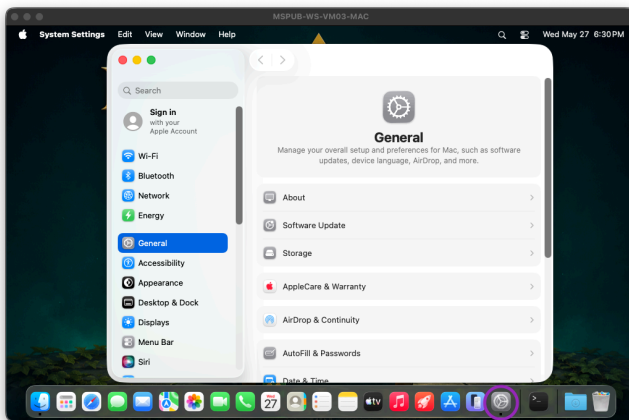
- On MSPUB-WS-VM03-MAC login as the mspub\administrator account.



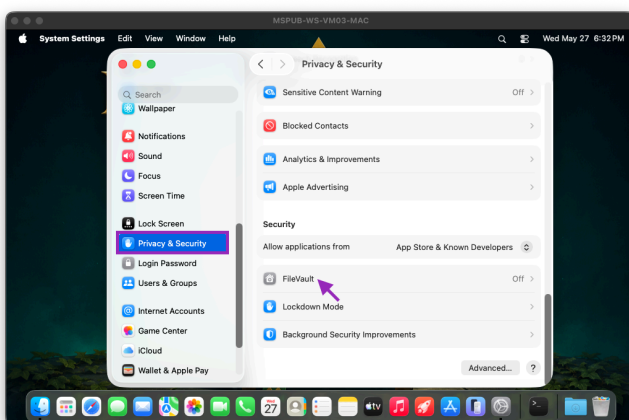
### 1. FileVault Disk Encryption

FileVault will be enabled to encrypt the macOS system drive to help protect sensitive data from unauthorized physical access.

- From the Dock at the bottom click on “System Settings.”

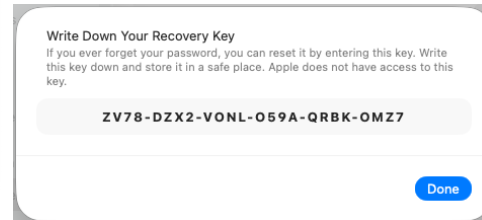
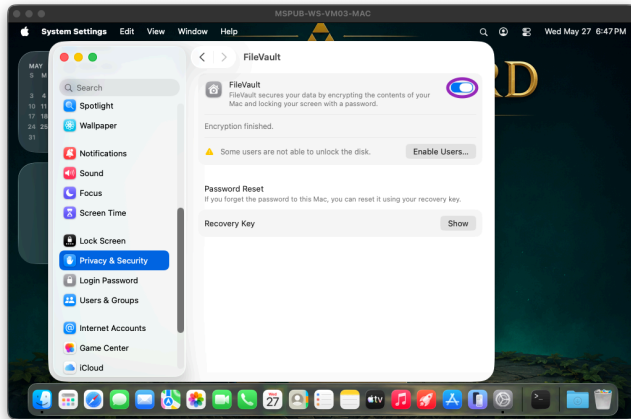


- On the left of System Settings scroll down and click “Privacy & Security.” Then on the right scroll down to “FileVault.”



## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

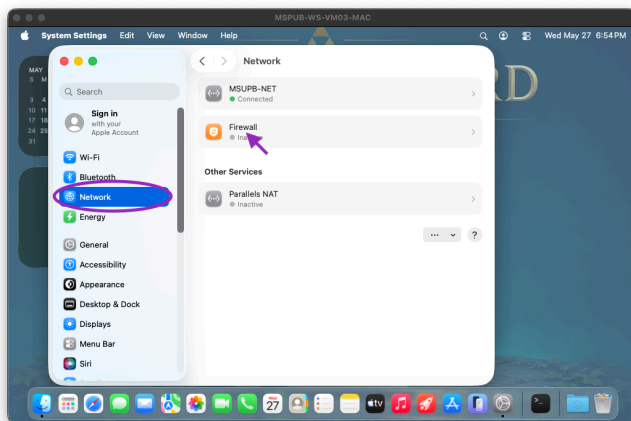
- Toggle the switch next to FileVault to the “On” position. Authenticate the change with the mspubadministrator password. Take note of the Recovery Key, in case the disk ever needs to be decrypted.



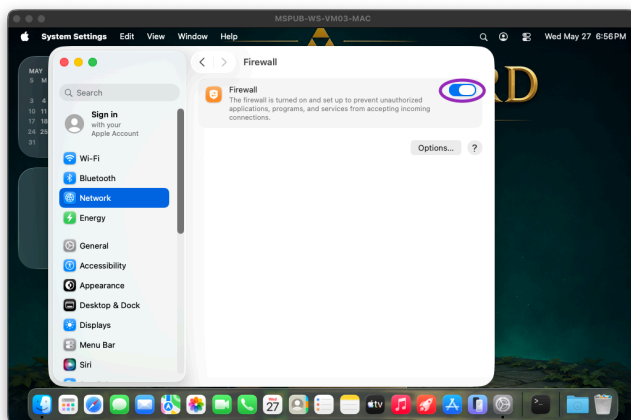
## 2. macOS Firewall

The built-in macOS firewall will be enabled to restrict unauthorized inbound network connections.

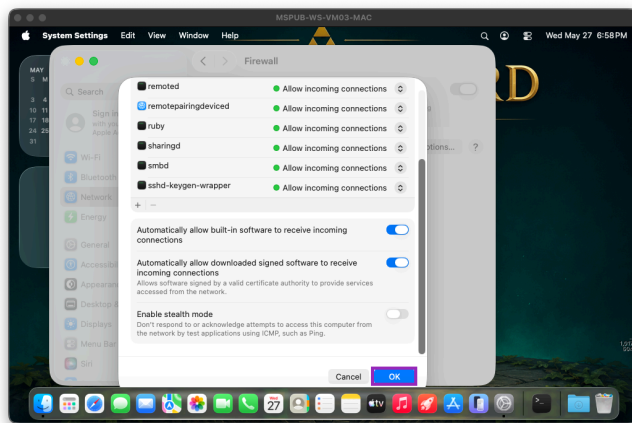
- On the left of System Settings scroll up to find “Network.” Then select “Firewall.”



- Toggle the switch next to Firewall to the “On” position.



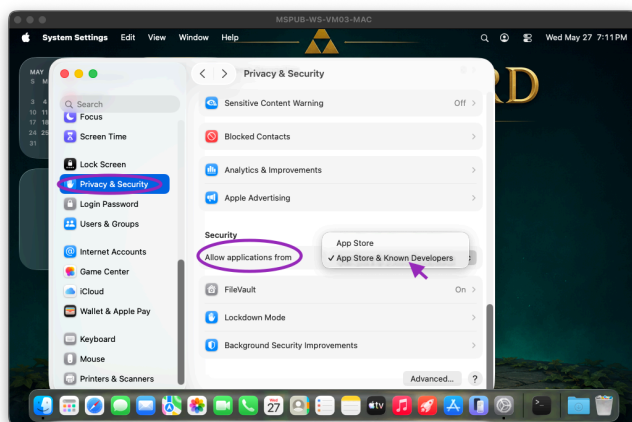
- Ensure that all required rules are allowed/denied. If a rule needs to be added click on the “+” button then click “OK” to save.



### 3. Gatekeeper Application Security

Gatekeeper will be enabled to help prevent unauthorized or untrusted applications from executing on the system. This will first validate the application signatures before allowing the software to execute on the system.

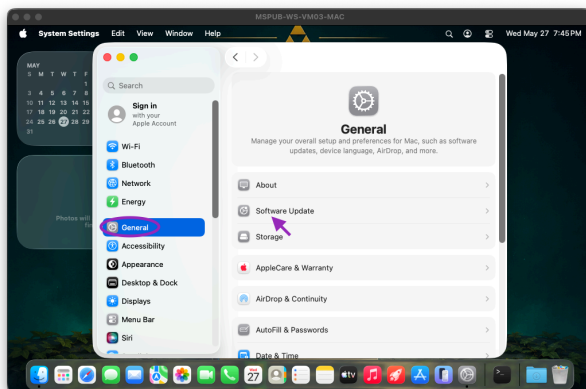
- In System Settings on the left scroll down and select Privacy and Security. Then on the right scroll down to “Allow applications from” and select “App Store & Known Developers.”



### 4. XProtect Malware Protection & Automatic System Updates

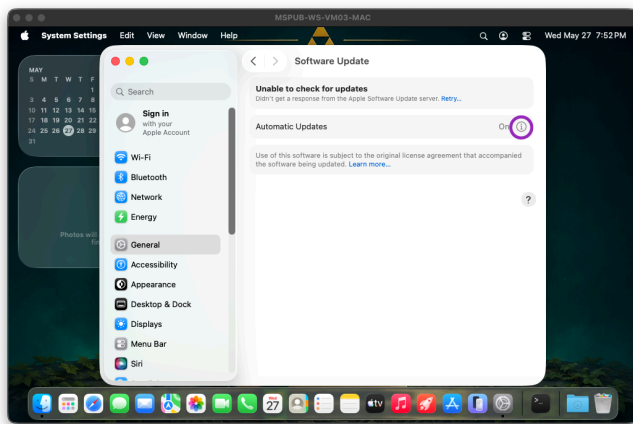
Apple XProtect will remain enabled to provide built-in malware signature detection and threat mitigation. Additionally, automatic macOS updates will be enabled to ensure the workstation receives security patches and systems updates. To confirm these settings are enabled do the following:

- In System Settings on the left select “General.” Then select “Software Update.”

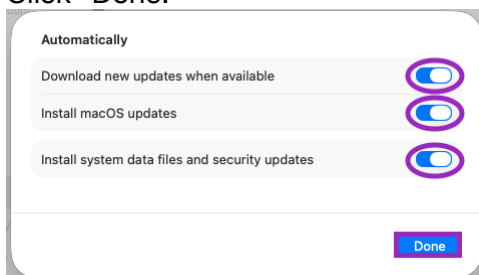


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

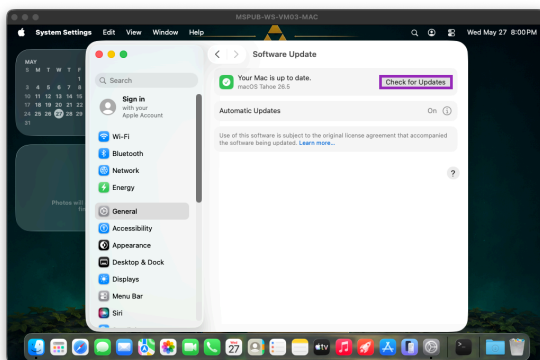
- Click the “I” button next to “Automatic Updates.”



- Ensure the following switches are turned “On:”
  - Download new updates when available
  - Install macOS updates
  - Install system data files and security updates
- Click “Done.”



- Click the “Check for Updates” button. If there are any install them. (The system may need to reboot once finished).

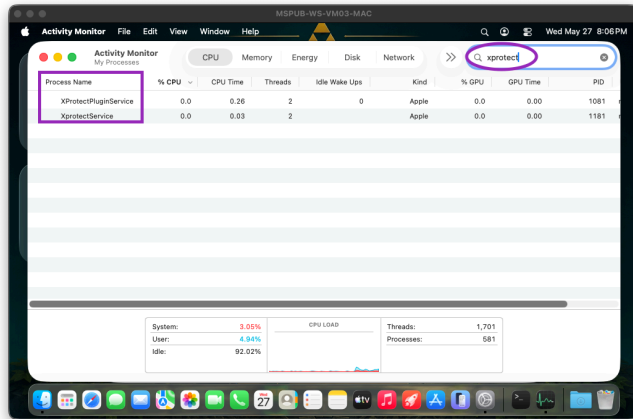


- To ensure XProtect is running click on the “Magnify Glass” in the Menu Bar to open Spotlight. Search for “Activity Monitor.” Click on the “Activity Monitor” search result.



## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- In Activity Monitor click the “Search field” and type “XProtect.” It will show the XProtectPluginService and XprotectService as active. The system is actively monitoring for Malware and Viruses in the background.

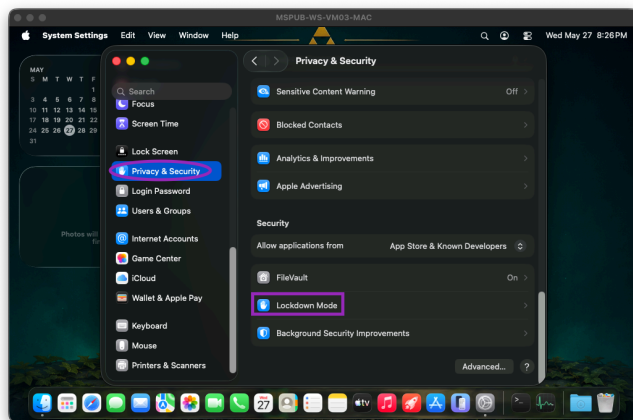


- Close Activity Monitor.

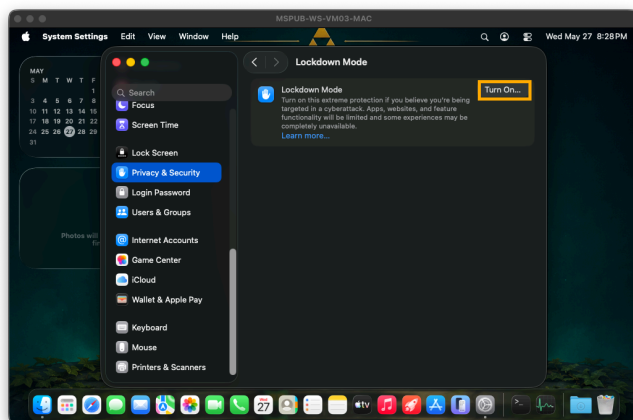
### 5. Lockdown Mode

Lockdown Mode should only be enabled if the system is believed to be an attack surface in the event of a Cyberattack. Lockdown mode will restrict high-risk services and advanced communication features inside of macOS. It is essentially an a quarantine feature built inside of the operating system. This will not be enabled on this VM, this is just to show where to enable it, incase the Mac becomes infected.

- In System Settings on the left scroll down and select “Privacy & Security.” On the right scroll down to and select “Lockdown Mode.”



- Click “Turn On...” in the event of a cyberattack.

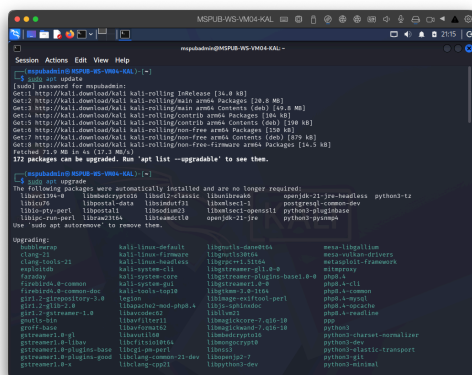




- On MSPUB-WS-VM04-KAL logon as the “mspubadmin” user account. All tasks will be done using Terminal located in the top toolbar.

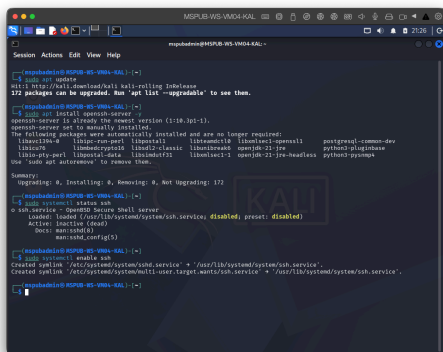
## 1. Package Management and System Updates

- Update the package repositories by using the command:  
`sudo apt update`
- Authenticate with the mspubadmin password.
- Install the available updates by using the command:  
`sudo apt upgrade -y`
- The system will install all updated packages.



## 2. SSH Administration

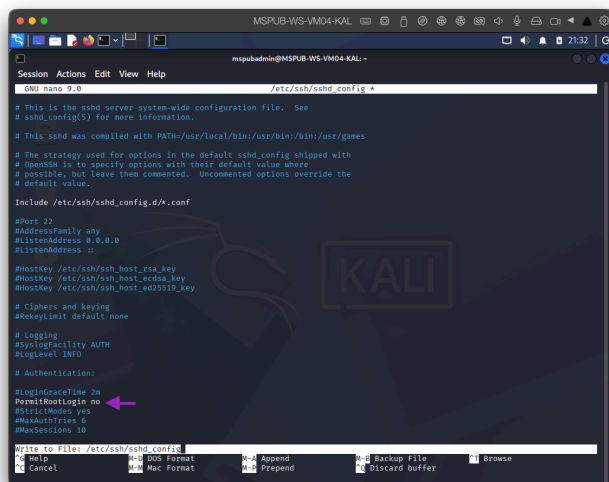
- Install OpenSSH with the following command:  
`sudo apt install openssh-server -y`
- Verify SSH has been installed:  
`sudo systemctl status ssh`
- Enable SSH services:  
`sudo systemctl enable ssh`



## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

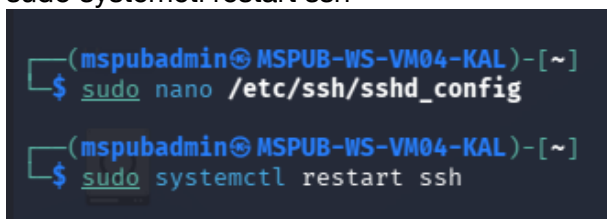
It is a good idea to disable the root user from being able to connect to the system via SSH. Do the following to disable root access:

- Edit the SSH Configuration file using Nano Text Editor:  
`sudo nano /etc/ssh/sshd_config`
- Authenticate using the mspubadmin password
- Find `#PermitRootLogin` and change it to:  
`PermitRootLogin`

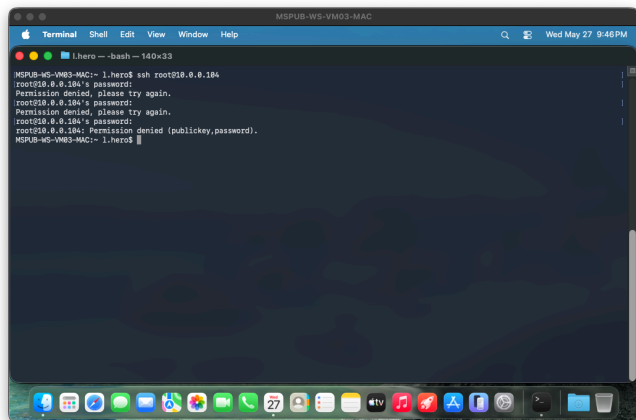


Press CTRL+O to save changes and CTRL+X to exit.

- Restart the SSH service by typing: (if connected via SSH currently, your connection will be dropped)  
`sudo systemctl restart ssh`



- Test that the root user cannot login using the Secure Shell Protocol from another machine. In this example MSPUB-WS-VM03-MAC will be used using a Terminal session. The connection will fail.



### 3. Least Privilege Administration

Administrative tasks were performed using sudo privileges previously rather than directly operating as the root user. It is always a good idea to change the root password and not leave the default. The MSPUB



Administrator account should be able to do this by default. This will be done using Terminal commands.

- Open Terminal from the “Ubuntu charm” on the lower left.
- To change the root password type the command:  
sudo passwd root
- When prompted authenticate the sudo command with the MSPUB Administrator password “CSNT253\_2026#”
- When prompted enter the password the new password “M@5t3r\$w0rdPub%” and verify it.
- The password will be changed. Switch to the root user using the command:  
su root
- Enter the new password.
- The user in the terminal has switched to the root account. This will give you elevated privileges without the need of the sudo command. Confirm with the “whoami” command.
- Type “exit” to return to the non-privileged user.

```
(mspubadmin@ MSPUB-WS-VM04-KAL) - [~]
$ sudo passwd root
New password:
Retype new password:
passwd: password updated successfully

(mspubadmin@ MSPUB-WS-VM04-KAL) - [~]
$ su root
Password:
(root@ MSPUB-WS-VM04-KAL) - [/home/mspubadmin]
whoami
root

(root@ MSPUB-WS-VM04-KAL) - [/home/mspubadmin]
exit

(mspubadmin@ MSPUB-WS-VM04-KAL) - [~]
$
```

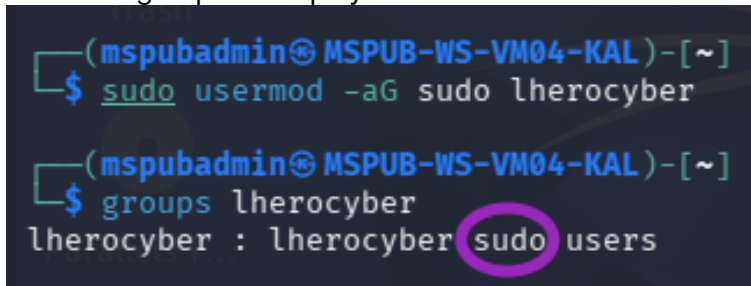
The Cybersecurity team will have their own dedicated non-domain users to be able to easily connect to the Kali Linux workstation. Additionally users can be placed in specified system groups to grant and deny access to certain commands, files, and packages. To create a new user and add a user to a group, in terminal use the following commands:

- Create a new user called lherocyber using the command:  
sudo adduser lherocyber
- Fill out the following fields when prompted:
  - New password: **CSNT253\_2026#**
  - Retype new password: **CSNT253\_2026#**
  - Full Name: **Link Hero Cyber**
  - Press enter to skip the remaining fields
  - Type “Y” to confirm the information is correct

```
(mspubadmin@ MSPUB-WS-VM04-KAL) - [~]
$ sudo adduser lherocyber
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lherocyber
Enter the new value, or press ENTER for the default
 Full Name []: Link Hero Cyber
 Room Number []:
 Work Phone []:
 Home Phone []:
 Other []:
Is the information correct? [Y/n] Y
```

## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

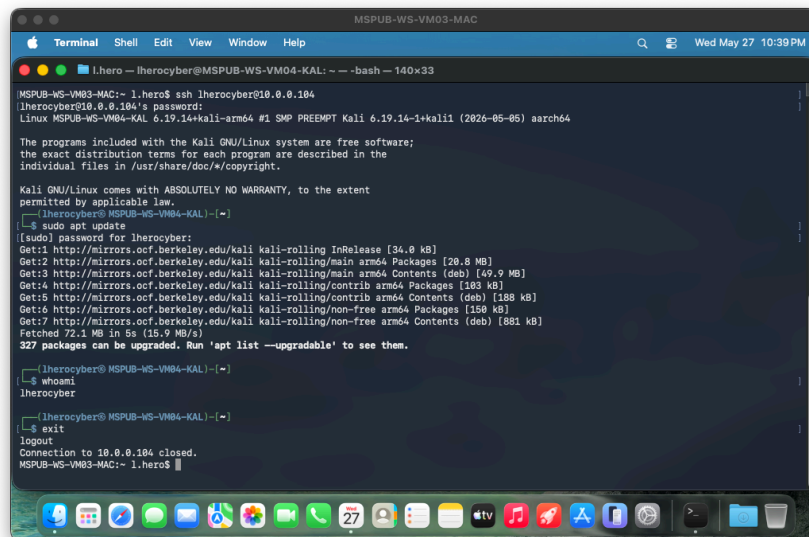
- Use the following command to add lherocyber to the sudoers group:  
sudo usermod -aG sudo lherocyber
- Authenticate the sudo command with the local MSPUB Admin password.
- Verify the change by typing these two commands:  
groups lherocyber
- The sudo group will display



```
(mspubadmin@MSPUB-WS-VM04-KAL)-[~]
$ sudo usermod -aG sudo lherocyber

(mspubadmin@MSPUB-WS-VM04-KAL)-[~]
$ groups lherocyber
lherocyber : lherocyber sudo users
```

- From another machine make sure the new user can use Secure Shell to access the system. In this example MSPUB-WS-VM03-MAC logged in is l.hero is using the ssh command in Terminal.
  - ssh **lherocyber@10.0.0.104**
  - enter in the password
  - Test the sudo command by entering:  
sudo apt update
  - Authenticate with lherocyber's password
  - Type "whoami" to verify lherocyber is logged into the Kali machine
  - Type exit to logout



```
MSPUB-WS-VM03-MAC: ~ l.hero$ ssh lherocyber@10.0.0.104
lherocyber@10.0.0.104's password:
Linux MSPUB-WS-VM04-KAL 6.19.14-kali-arm64 #1 SMP PREEMPT Kali 6.19.14-1-kali1 (2026-05-05) aarch64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
lherocyber@MSPUB-WS-VM04-KAL:~$
lherocyber@MSPUB-WS-VM04-KAL:~$ sudo apt update
[sudo] password for lherocyber:
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease [34.0 kB]
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main arm64 Packages [20.8 MB]
Get:3 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main arm64 Contents (deb) [49.9 MB]
Get:4 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib arm64 Packages [183 kB]
Get:5 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib arm64 Contents (deb) [188 kB]
Get:6 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free arm64 Packages [150 kB]
Get:7 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free arm64 Contents (deb) [881 kB]
Fetched 72.1 MB in 5s (15.9 MB/s)
327 packages can be upgraded. Run 'apt list --upgradable' to see them.
lherocyber@MSPUB-WS-VM04-KAL:~$
lherocyber@MSPUB-WS-VM04-KAL:~$ whoami
lherocyber
lherocyber@MSPUB-WS-VM04-KAL:~$
lherocyber@MSPUB-WS-VM04-KAL:~$ exit
logout
Connection to 10.0.0.104 closed.
MSPUB-WS-VM03-MAC:~ l.hero$
```

## 4. Configuring UFW in Kali

Uncomplicated Firewall (UFW) was enabled to help restrict unauthorized inbound network access while allowing required administrative and domain-related traffic.

- Install UFW by entering the command:  
sudo apt update  
sudo apt install ufw  
sudo apt install ufw
- Authenticate the sudo command with the mspubadmin password
- Enable UFW by typing:  
sudo ufw enable
- Allow the required services:  
sudo ufw allow ssh

- Verify UFW configuration  
sudo ufw status

```
jmanung — mspubadmin@MSPUB-WS-VM04-KAL: ~ — ssh mspubadmin@10.0.0.104 — 148x97

[jmanung@INRAAL ~ % ssh mspubadmin@10.0.0.104
mspubadmin@10.0.0.104's password:
Linux MSPUB-WS-VM04-KAL 6.19.14-kali-ara64 #1 SMP PREEMPT Kali 6.19.14-1-kali1 (2026-05-05) aarch64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 27 22:49:50 2026 from 10.0.0.2
~(mspubadmin@MSPUB-WS-VM04-KAL)-[~]
[~]$ sudo apt update
[~]$ sudo apt install ufw
The following packages were automatically installed and are no longer required:
libavc1394-0 libipc-run-perl libpostall libteamctl0 libx1secl-openssl1 postgresql-common-dev
libc6u76 libbedcrypt016 libsd2-classic libunibreak6 openjdk-21-jre python3-pluginbase
libio-pty-perl libpostal-data libstdutf31 libx1secl-1 openjdk-21-jre-headless python3-pysnmp4
Use 'sudo apt autoremove' to remove them.

Installing:
ufw

Suggested packages:
rsyslog

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 327
Download size: 169 kB
Space needed: 880 kB / 5,985 MB available

Get:1 http://kali.download/kali kali-rolling/main arm64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 0s (853 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database... 431055 files and directories currently installed.)
Preparing to unpack ../archives/ufw_0.36.2-9_all.deb...
Unpacking ufw (0.36.2-9)...
Setting up ufw (0.36.2-9)...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' -> '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2026.2.5)...
Processing triggers for man-db (2.13.1-1+b1)...

[~]$ sudo ufw enable
[~]$ sudo ufw allow ssh
[~]$ sudo ufw status
```

## MSPUB Kali Linux Use Statement

Kali Linux workstations are isolated within the MSPUB lab environment and will be used exclusively for authorized internal testing and security validation activities. It has been configured within the MSPUB virtual network. Restricted testing activities authorized within the MSPUB Network and has verified communication only with internal MSPUB infrastructure.

Kali Linux has been deployed strictly for education, administrative, and authorized security testing purposes within the MSPUB environment. All penetration testing and administrative activities will be limited to authorized internal systems within the isolated environment.

# Troubleshooting Scenarios

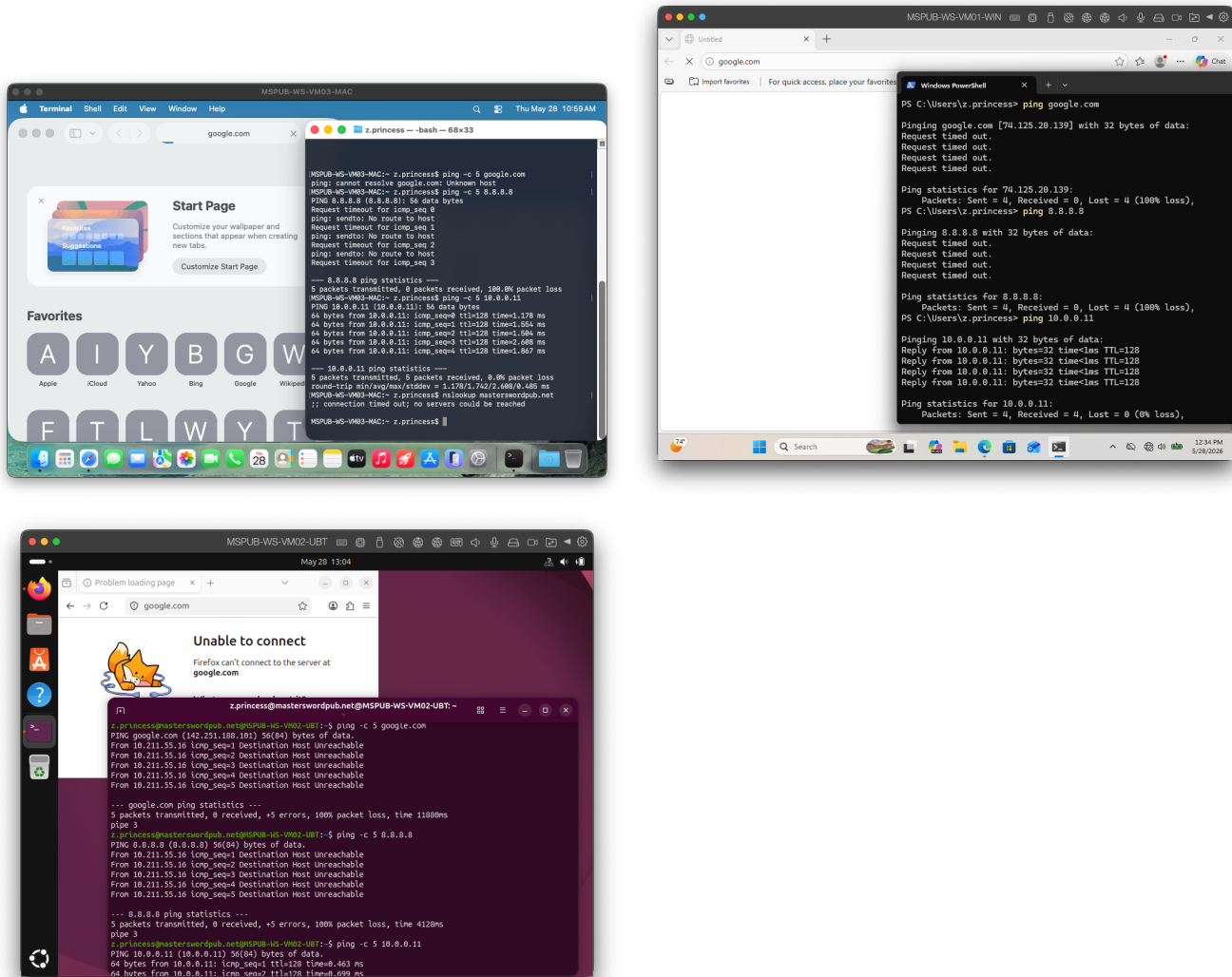
## Scenario 1: Routing & DNS Misconfiguration

### Scenario Description:

Zelda is the owner of Master Sword Publishing. She is having issues connecting to the internet. She is reporting that she is no longer able to access any websites she regularly uses. She requested assistance through the MSPUB IT Service Desk. A junior IT technician attempted to resolve the issue, but after unsuccessful troubleshooting, escalated the ticket to you.

### Symptoms:

- As defined by the user, websites are unable to load.
- Pinging by website IP address fails. Pinging internal servers is successful.



### Troubleshooting Steps:

- Test pinging by IP vs. Hostname
- Inspect Network settings

### Tools to use:

## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

### • macOS/Linux:

- Terminal
  - ifconfig -a
  - ping -c
  - nslookup
  - dig

### • Windows:

- Command Prompt
  - ipconfig /all
  - ping
  - nslookup

### Root Cause:

Upon looking into the issue it has been discovered that the DNS server settings are incorrectly configured after a manual network change. It is currently set to 192.168.255.254.

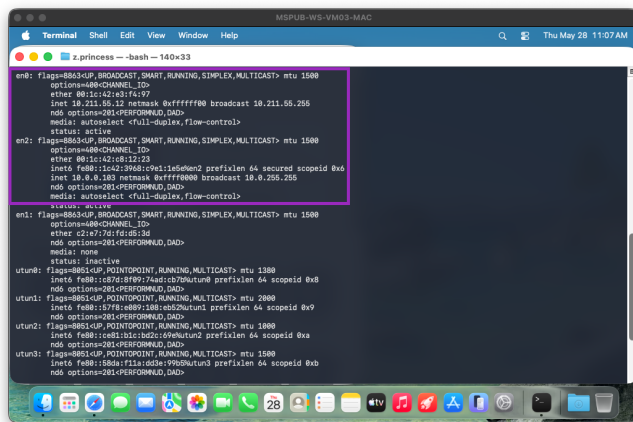
### Resolution:

The DNS server had changed to 10.0.0.1, but the user's computer was still set to the older settings of 192.168.255.254. Once the DNS server settings were updated to the new server 10.0.0.1, they were able to resume website browsing.

### Validation Testing:

#### • macOS

- Using the Terminal command "ifconfig -a" to display network configuration. Looking at the Ethernet Network Adapters, en0 and en2.



```
z.princess ~ - ssh - 140x33
msb: flags=883<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=40<CHANNEL_IO>
ether 08:01:42:83:14:92
inet 10.211.55.17 netmask 0xfffff0 broadcast 10.211.55.255
nd6 options=20<PERFORMNUD,DAD>
media: autoselect <full-duplex,flow-control>
status: active

en2: flags=883<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=40<CHANNEL_IO>
ether 08:01:42:83:12:23
inet6 fe80::1c4d:3968:c9e1:1d56%en2 prefixlen 64 secured scopeid 0x6
inet 10.0.0.183 netmask 0xffff0000 broadcast 10.0.255.255
nd6 options=20<PERFORMNUD,DAD>
media: autoselect <full-duplex,flow-control>
status: active

em1: flags=883<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=40<CHANNEL_IO>
ether 02:17:76:1f:0d:34
nd6 options=20<PERFORMNUD,DAD>
media: none
status: inactive

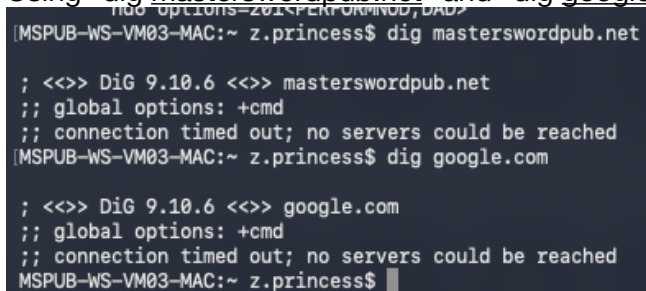
utun0: flags=801<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1300
inet6 fe80::c87d:1879:74ad:cb70%utun0 prefixlen 64 scopeid 0xb
nd6 options=20<PERFORMNUD,DAD>

utun1: flags=801<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2800
inet6 fe80::1578:e8b9:1a81:e52a%utun1 prefixlen 64 scopeid 0x9
nd6 options=20<PERFORMNUD,DAD>

utun2: flags=801<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1800
inet6 fe80::ce81:1b1c:b22c:09e4%utun2 prefixlen 64 scopeid 0xa
nd6 options=20<PERFORMNUD,DAD>

utun3: flags=801<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
inet6 fe80::158a:f23a:6d56:992b%utun3 prefixlen 64 scopeid 0xb
nd6 options=20<PERFORMNUD,DAD>
```

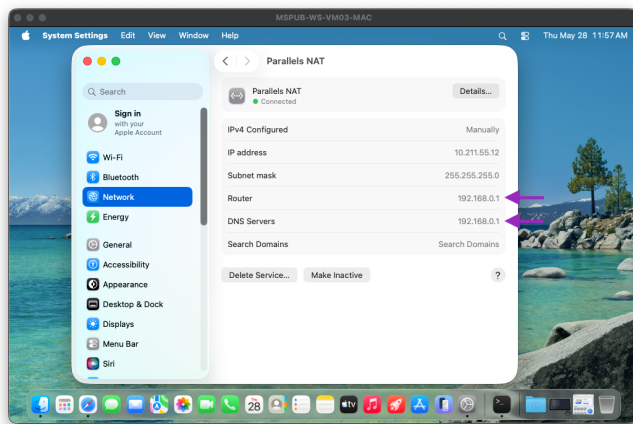
- Using "dig masterswordpub.net" and "dig google.com" to check DNS.



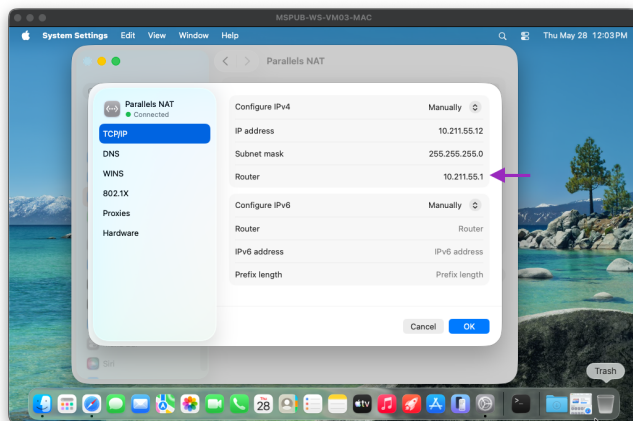
```
MSPUB-WS-VM03-MAC:~ z.princess$ dig masterswordpub.net
; <<>> DiG 9.10.6 <<>> masterswordpub.net
;; global options: +cmd
;; connection timed out; no servers could be reached
MSPUB-WS-VM03-MAC:~ z.princess$ dig google.com
; <<>> DiG 9.10.6 <<>> google.com
;; global options: +cmd
;; connection timed out; no servers could be reached
MSPUB-WS-VM03-MAC:~ z.princess$
```

## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

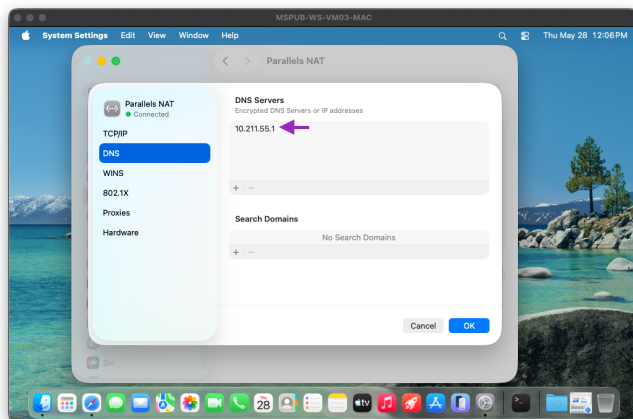
- Checking DNS settings in the Network Settings Pane.



- Updating TCP/IP Router settings to 10.211.55.1.



- Updating DNS Settings to point to the correct router.





## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Testing ping, nslookup, dig again:

```
mspub-ws-vm03-mac:~ z.princess$ ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=12.424 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=13.777 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=13.209 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=9.739 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=13.285 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.739/12.487/13.777/1.441 ms
mspub-ws-vm03-mac:~ z.princess$ ping -c 5 google.com
PING google.com (142.251.188.139): 56 data bytes
64 bytes from 142.251.188.139: icmp_seq=0 ttl=128 time=15.809 ms
64 bytes from 142.251.188.139: icmp_seq=1 ttl=128 time=14.785 ms
64 bytes from 142.251.188.139: icmp_seq=2 ttl=128 time=23.904 ms
64 bytes from 142.251.188.139: icmp_seq=3 ttl=128 time=14.936 ms
64 bytes from 142.251.188.139: icmp_seq=4 ttl=128 time=20.073 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 14.785/17.901/23.904/3.567 ms

mspub-ws-vm03-mac:~ z.princess$ nslookup masterswordpub.net
Server:
 10.211.55.1
Address:
 10.211.55.1#53

** server can't find masterswordpub.net: NXDOMAIN

mspub-ws-vm03-mac:~ z.princess$ nslookup google.com
Server:
 10.211.55.1
Address:
 10.211.55.1#53

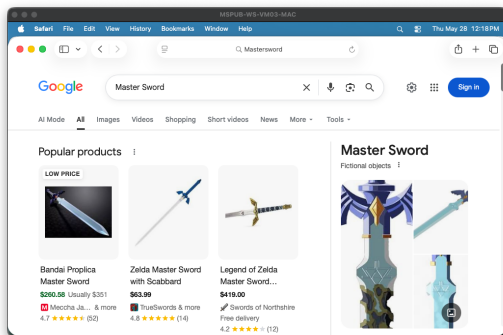
Non-authoritative answer:
Name: google.com
Address: 142.251.188.100
Name: google.com
Address: 142.251.188.113
Name: google.com
Address: 142.251.188.138
Name: google.com
Address: 142.251.188.101
Name: google.com
Address: 142.251.188.102
Name: google.com
Address: 142.251.188.139
```

```
Terminal Shell Edit View Window Help
z.princess ~ -bash - 140x36

mspub-ws-vm03-mac:~ z.princess$ dig masterswordpub.net
; <<> Dig 9.18.6 <<> masterswordpub.net
; global options: <cmd>
; Set answer:
;--HEADER-- opcode: QUERY, status: NXDOMAIN, id: 52184
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
; QUESTION SECTION:
; masterswordpub.net.
; IN A
; AUTHORITY SECTION:
; net. 881 IN SOA a-gltd-servers.net. ns1ld.verisign-grs.com. 1779995344 1800 900 604800 900
; Query time: 8 msec
; SERVER: 10.211.55.1#53(10.211.55.1)
; WHEN: Thu May 28 12:09:22 PDT 2020
; MSG SIZE rcvd: 120

mspub-ws-vm03-mac:~ z.princess$ dig google.com
; <<> Dig 9.18.6 <<> google.com
; global options: <cmd>
; Set answer:
;--HEADER-- opcode: QUERY, status: NOERROR, id: 29900
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
; QUESTION SECTION:
; google.com.
; IN A
; ANSWER SECTION:
; google.com. 24 IN A 142.251.188.113
```

- Testing web browsing to google.com.



## Windows

- Checking network settings with “ipconfig /all” command in Terminal. Checking the Parallels NAT and MSPUB-NET network adapters. MSPUB-NET is accurate which explains why there is a response from the domain controller. On Parallels NAT the Default Gateway and DNS Servers are incorrect explaining why there is no internet access.

```
Windows PowerShell
Mode Type: Hybrid
ZIP: Enabled
WIND: Proxy Enabled
DNS Suffix Search List: masterswordpub.net

Ethernet adapter Parallels NAT:

Connection-specific DNS Suffix . :
Description : Parallels VirtIO Ethernet Adapter
Physical Address. : 08-1C-42-4C-10-0C
Dhcp Enabled. : No
Autconfiguration Enabled : Yes
IPv4 Address. : 10.211.55.11(Preferred)
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.0.1
DNS Servers : 192.168.0.1
NetBIOS over Tcpip. : Enabled

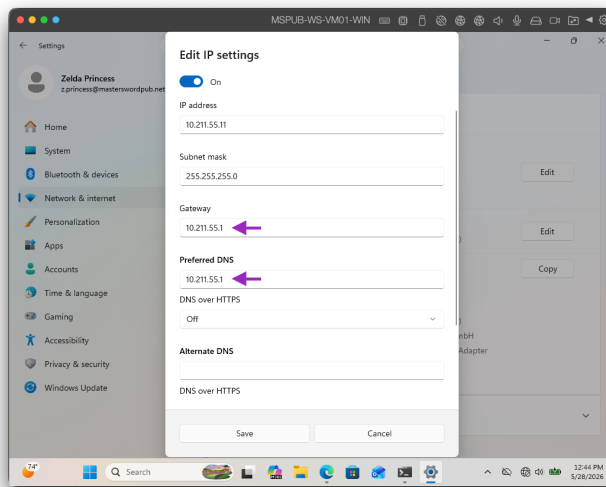
Ethernet adapter MSPUB-NET:

Connection-specific DNS Suffix . :
Description : Parallels VirtIO Ethernet Adapter #2
Physical Address. : 08-1C-42-4C-10-0C
Dhcp Enabled. : No
Autconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::bca8:92da:dca3:57bf%10(Preferred)
IPv4 Address. : 10.0.0.101(Preferred)
Subnet Mask : 255.255.0.0
Default Gateway : 10.0.0.1
DHCPv6 IAID : 002646019
DHCPv6 Client DUID. : 00-01-00-11-98-0C-8A-00-1C-42-4C-10-0C
DNS Servers : 10.0.0.11
 10.0.0.12
NetBIOS over Tcpip. : Enabled
```

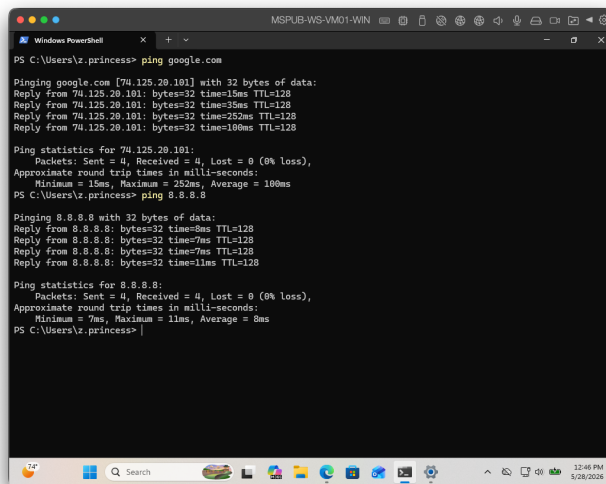


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

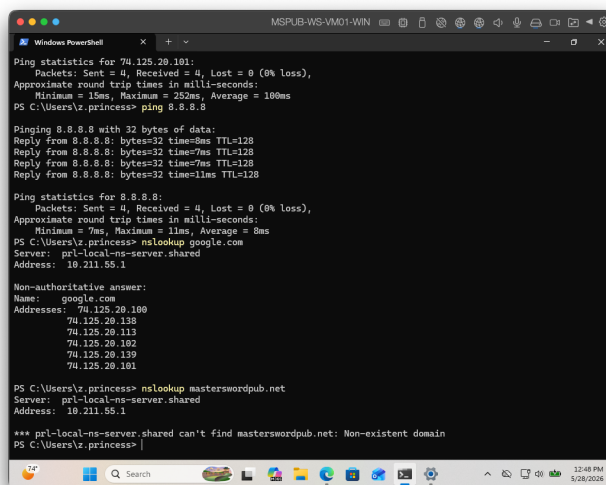
- Editing the network settings on the Parallels NAT adapter.



- Testing outbound ping to [google.com](https://www.google.com) and 8.8.8.8

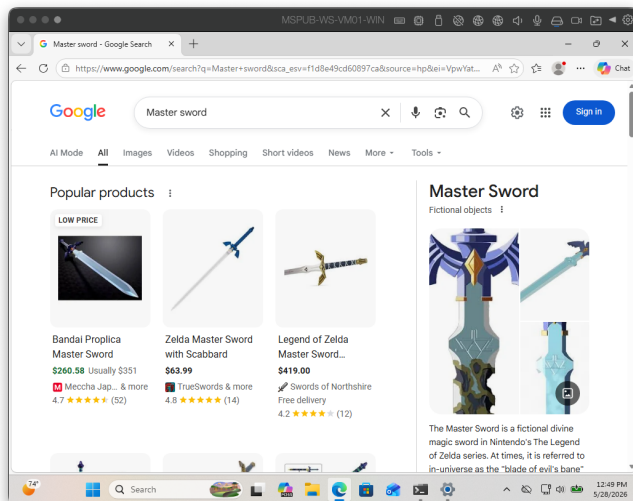


- Testing outbound nslookup to [google.com](https://www.google.com) and [masterswordpub.net](https://www.masterswordpub.net)

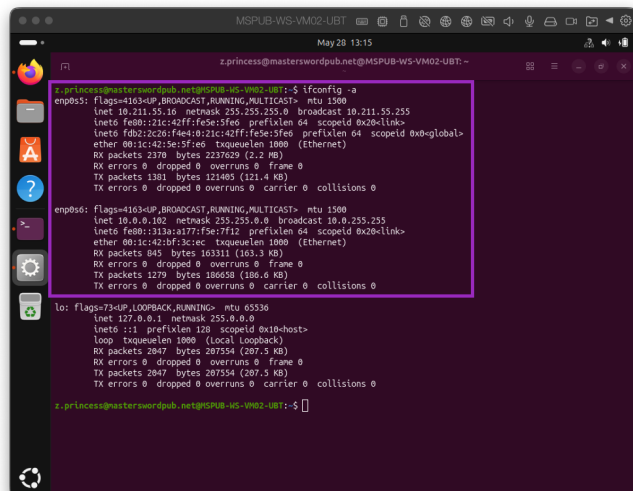


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

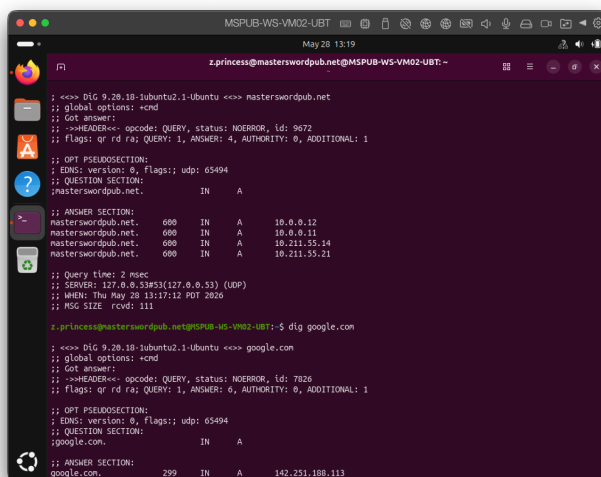
- Testing web browsing to google.com



- **Linux**
  - Using the Terminal command "ifconfig -a" to display network configuration. Looking at the Ethernet Network Adapters, enp0s5 and enp0s6.

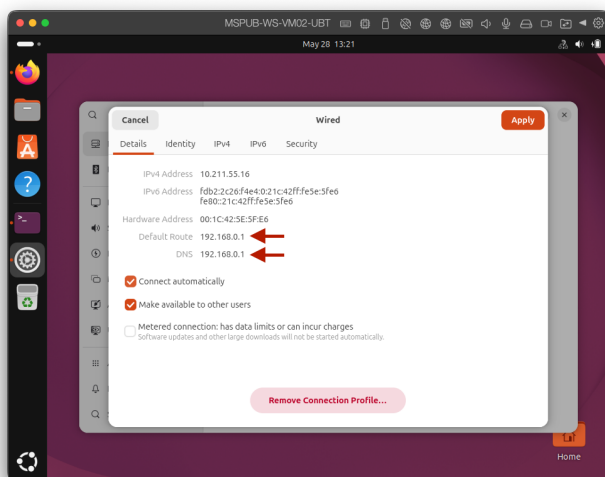


- Using "dig masterswordpub.net" and "dig google.com" to check DNS.

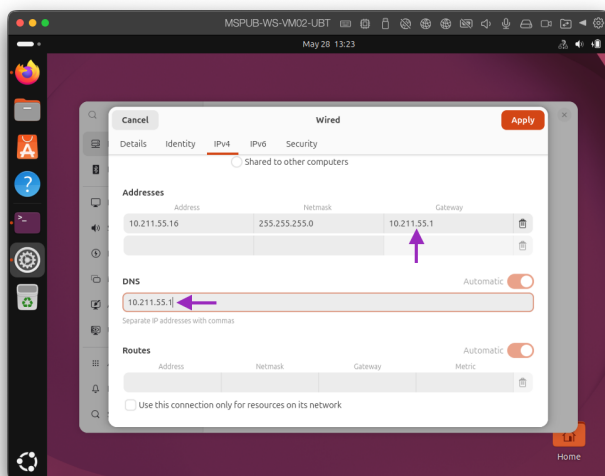


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Checking the enp0s5 Network Settings. Wrong Default Route and DNS servers.



- Updating the Gateway and DNS to 10.211.55.1



- Testing ping to google.com and 8.8.8.8

```
z.princess@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ ping -c 5 google.com
PING google.com (142.251.188.101) 56(84) bytes of data:
64 bytes from ts-in-f101.1e100.net (142.251.188.101): icmp_seq=1 ttl=128 time=13.1 ms
64 bytes from ts-in-f101.1e100.net (142.251.188.101): icmp_seq=2 ttl=128 time=13.9 ms
64 bytes from ts-in-f101.1e100.net (142.251.188.101): icmp_seq=3 ttl=128 time=13.4 ms
64 bytes from ts-in-f101.1e100.net (142.251.188.101): icmp_seq=4 ttl=128 time=13.5 ms
64 bytes from ts-in-f101.1e100.net (142.251.188.101): icmp_seq=5 ttl=128 time=548 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 401ms
rtt min/avg/max/ndev = 13.122/120.356/547.887/213.765 ms
z.princess@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=7.90 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=8.57 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=8.18 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=11.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=8.35 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 400ms
rtt min/avg/max/ndev = 7.903/8.926/11.638/1.372 ms
```

- Testing nslookup for google.com and masterswordpub.net

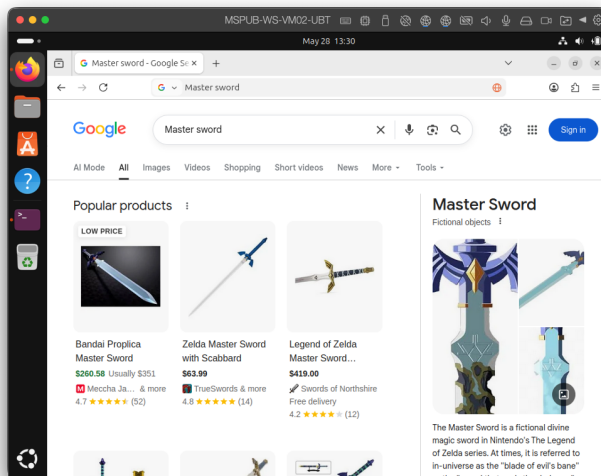
```
z.princess@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ nslookup google.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: google.com
Address: 142.251.188.100
Name: google.com
Address: 142.251.188.102
Name: google.com
Address: 142.251.188.101
Name: google.com
Address: 142.251.188.113
Name: google.com
Address: 142.251.188.138
Name: google.com
Address: 142.251.188.139

z.princess@masterswordpub.net@MSPUB-WS-VM02-UBT:~$ nslookup masterswordpub.net
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: masterswordpub.net
Address: 10.0.0.12
Name: masterswordpub.net
Address: 10.0.0.11
Name: masterswordpub.net
Address: 10.211.55.14
Name: masterswordpub.net
Address: 10.211.55.21
Name: masterswordpub.net
Address: fdb2:2c26:f4e4:0:8e77:dd06:5de7:7c60
Name: masterswordpub.net
Address: fdb2:2c26:f4e4:0:270:c74e:d3f5:22fd
Name: masterswordpub.net
Address: fdb2:2c26:f4e4:0:4133:ae01:afeb:88f2
```

- Testing web browsing to google.com



## Scenario 2: User Account Locked Out

### Scenario Description:

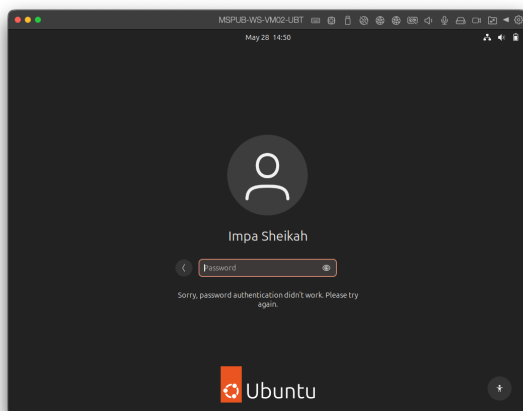
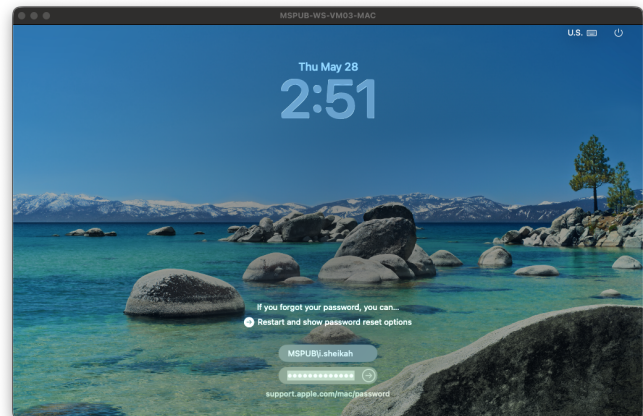
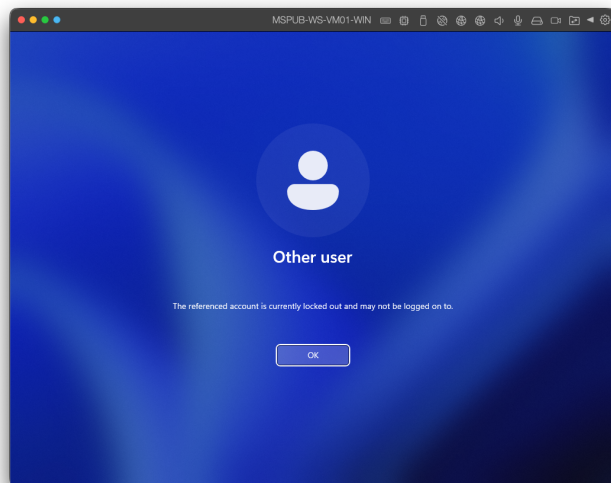
Impa, an employee for Master Sword Publishing contacted the IT department reporting she is unable to log into their workstation using their MSPUB Active Directory credentials. The user stated they repeatedly received an “Account Locked Out” message after multiple unsuccessful login attempts. As the system administrator, you were assigned to investigate the issue, identify the cause of the account lockout, and restore the user’s access to the MSPUB domain environment.

### Symptoms:

- Unable to authenticate to the domain
- “Account Locked Out” message displayed during login attempts
- Repeated failed login attempts
- User unable to access domain resources

### Troubleshooting Steps:

- Verify user lockout on the Domain Controller
- Unlock the user account on the Domain Controller
- Set Default Password
- Require Password Reset on next successful login.
- Verify user is able to login



### Tools to use:

- **Windows Server**
  - Active Directory Users & Computers
  - User Account
- **Windows 11:**
  - Testing Login
  - Resetting Password
- **macOS:**
  - Testing Login
  - Resetting Password
- **Linux:**
  - Testing Login
  - Resetting Password

### Root Cause:

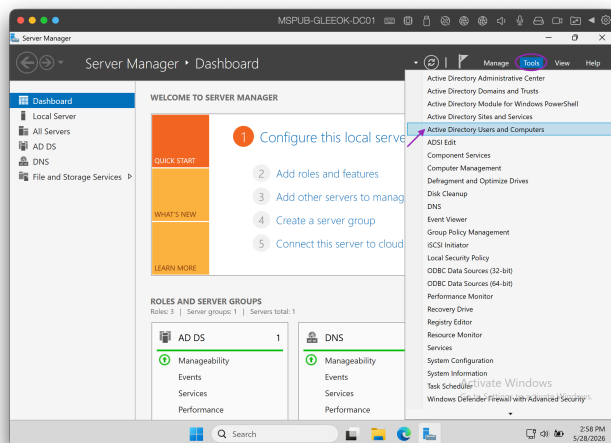
The Active Directory user account became locked after exceeding the allowed number of failed authentication attempts configured within the domain environment.

### Resolution:

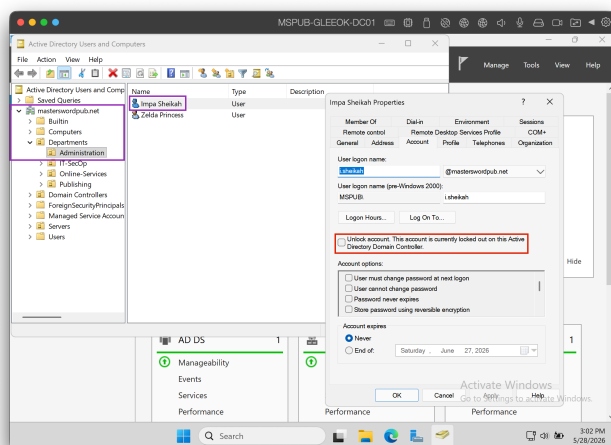
The user account was successfully unlocked within Active Directory and the password was reset. The user regained access to the MSPUB domain environment and successfully authenticated to the workstation.

### Validation Testing:

- **Windows Server**
  - Accessing Active Directory Users and Computers from Server Manager

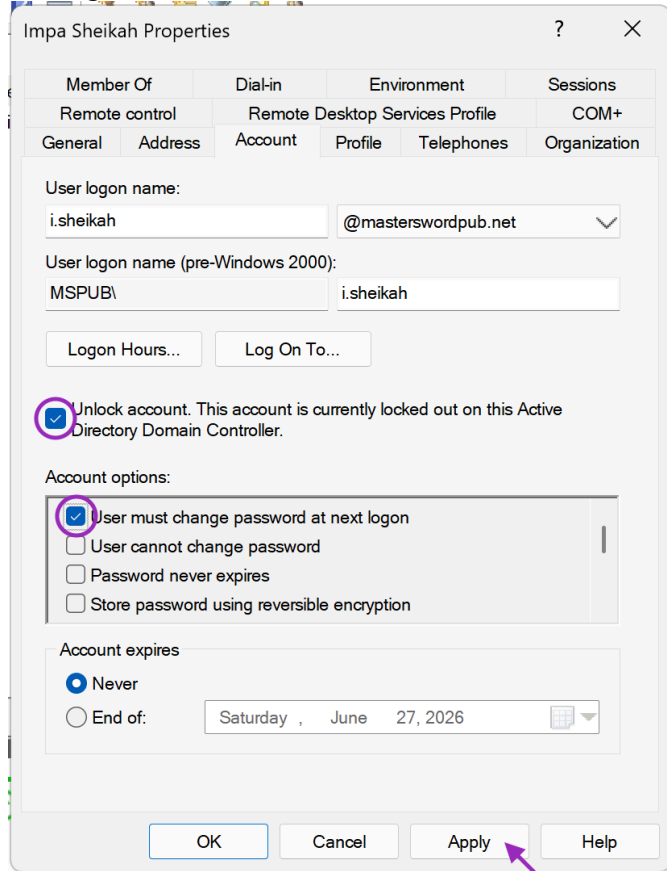


- Navigating to [masterswordpub.net](https://masterswordpub.net) > Departments > Administration and double clicking the User's Name (Impa Sheikah) to check if the user account shows as locked out.

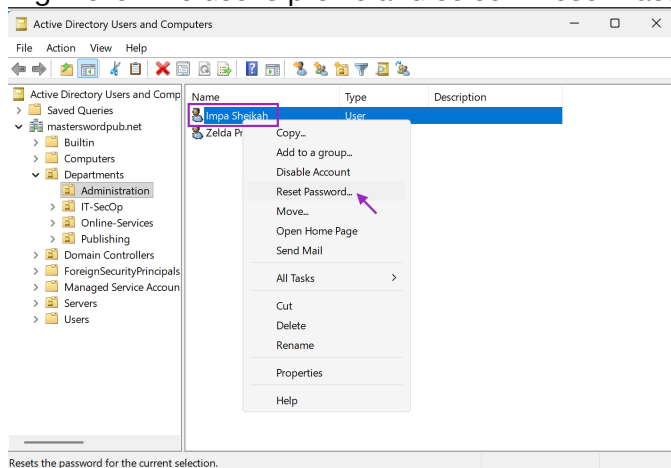


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

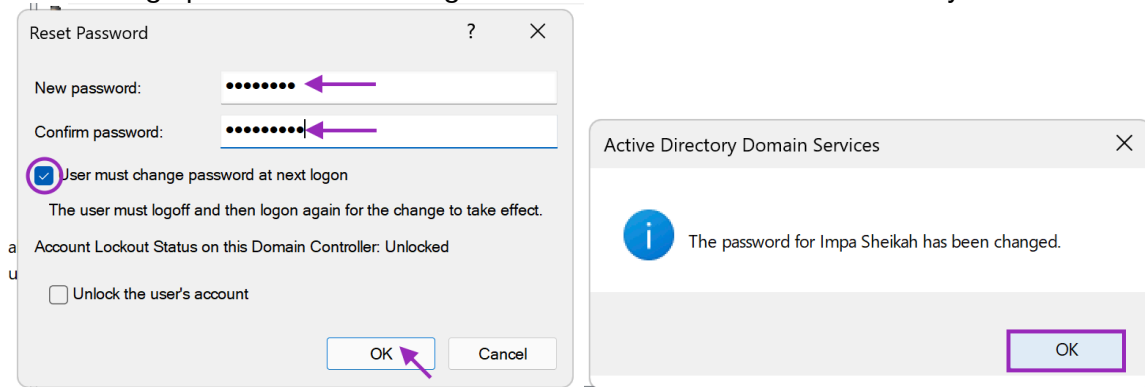
- Ticking the box to unlock the user's account and ticking "User must change password at next logon."



- Right click the user's profile and select "Reset Password..."



- Setting a temporary password to give the user to make sure they can log in after unlock. Verify the "User must change password at next logon" box is ticked. Password set to: Hyrul369!

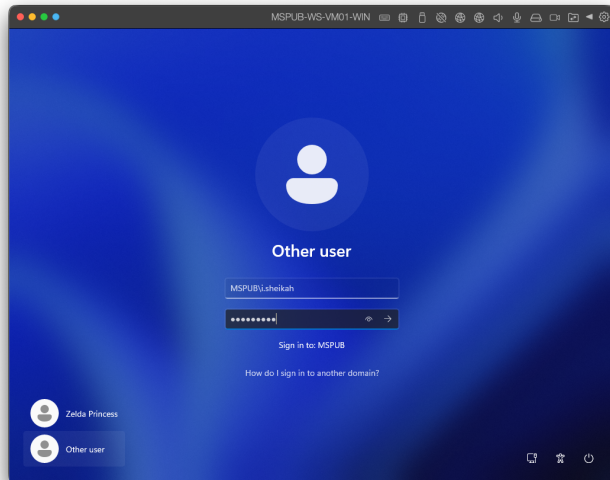




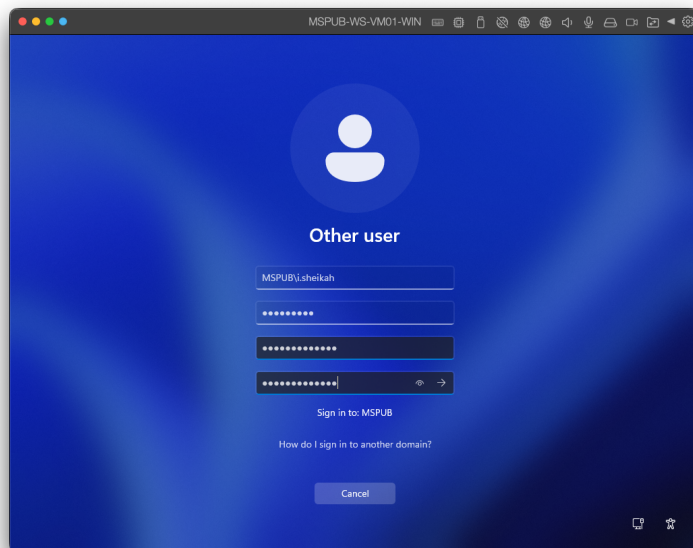
## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- **Windows 11 Client**

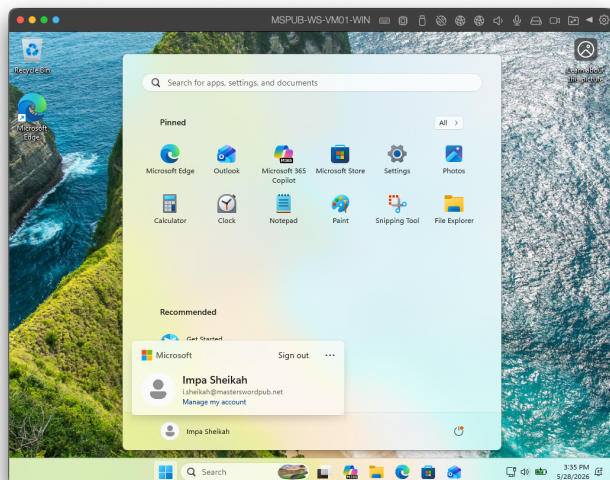
- Have the user try logging in with the new temporary password.



- Have the user reset their password.

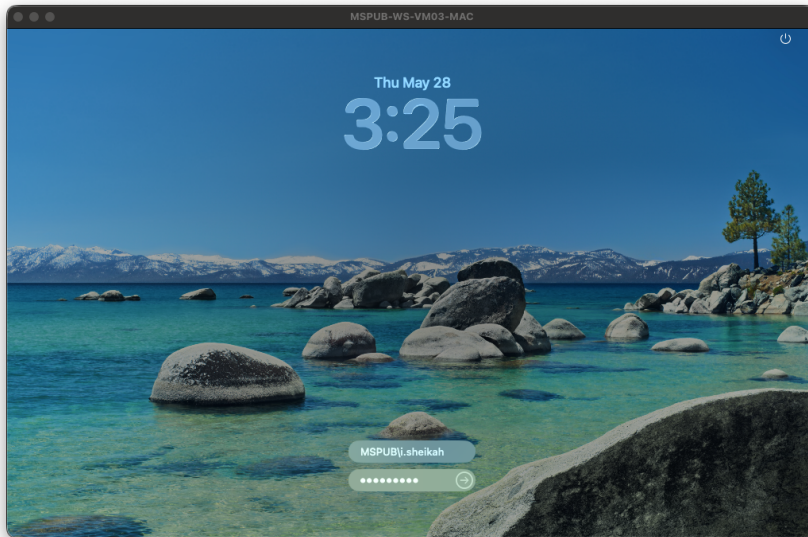


- The user is now able to log into their workstation.

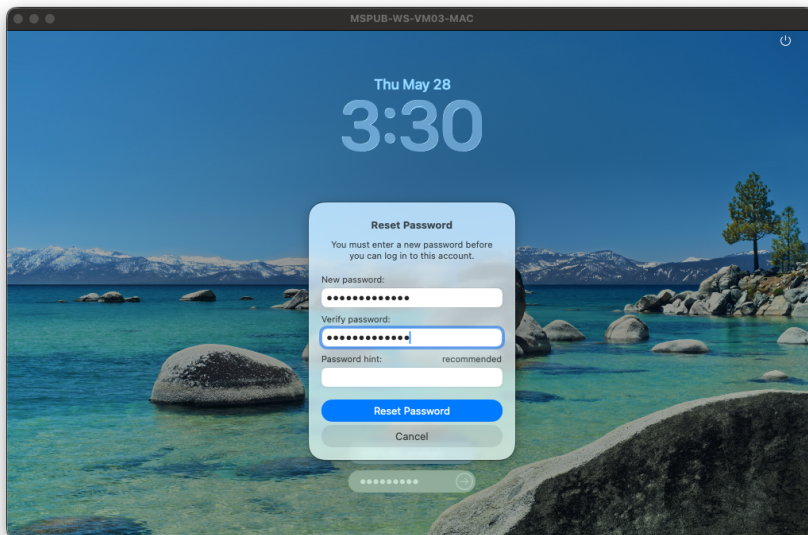


- **macOS Client**

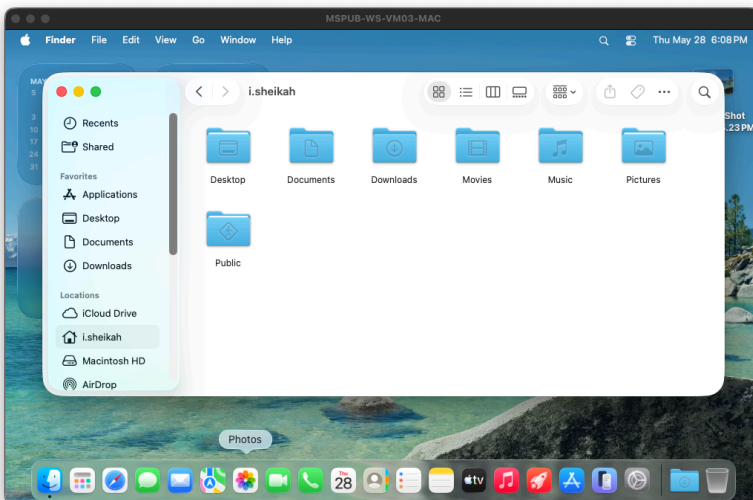
- Have the user try logging in with the new temporary password.



- Have the user reset their password.

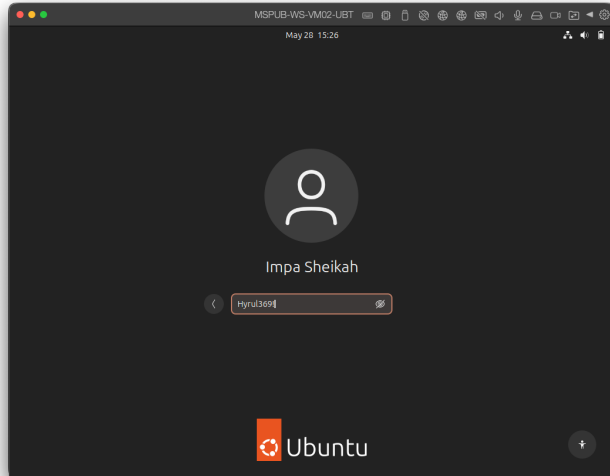


- The user is now able to log into their workstation.

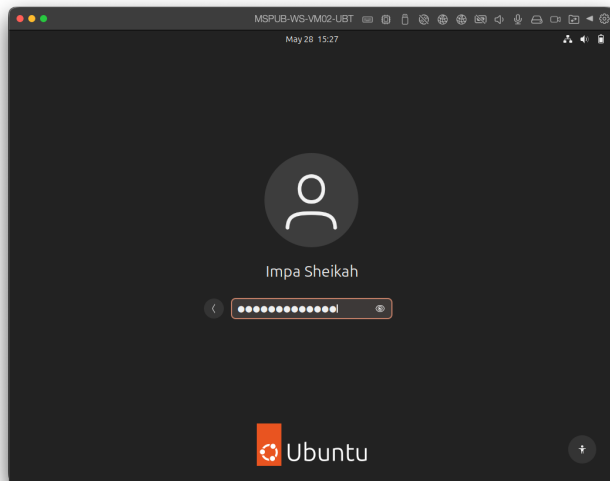


- **Linux Client**

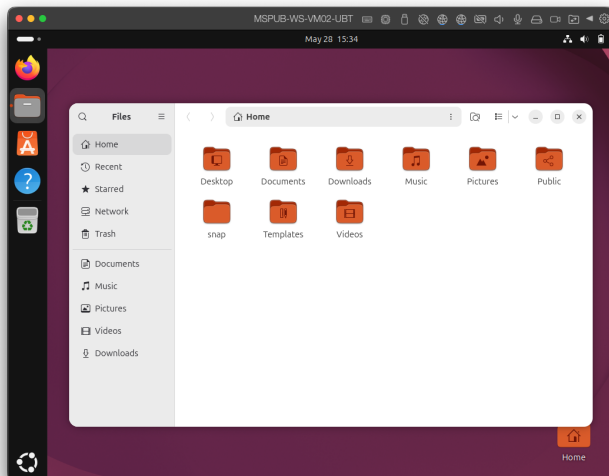
- Have the user try logging in with the new temporary password.



- Have the user reset their password.



- User is now able to login to the workstation.



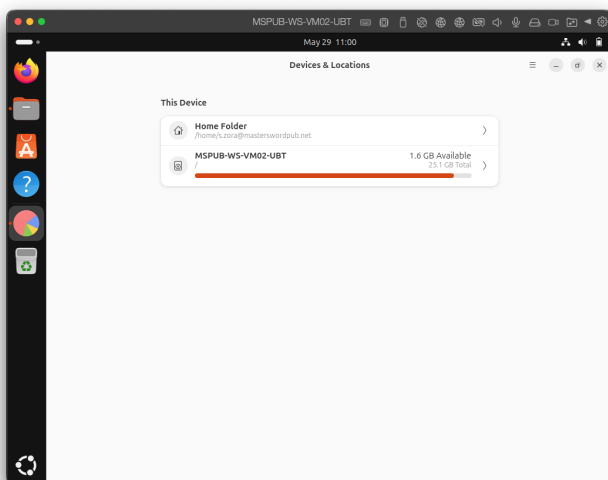
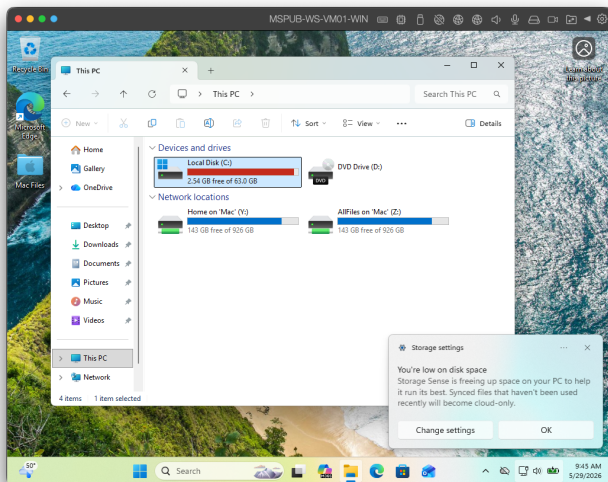
### Scenario 3: Low Disk Space Issue

#### Scenario Description:

Sidon works in the Publishing Department at Master Sword Publishing and recently reported that her workstation has become extremely slow during normal operation. Applications frequently freeze, system updates fail to install, and users are receiving notifications indicating that disk storage is critically low. An IT Service Ticket was submitted to the MSPUB IT Department after the user was unable to complete daily tasks due to degraded system performance. Initial troubleshooting confirmed that the workstation remained connected to the network and all core services were operational. The issue was escalated for further investigation.

#### Symptoms:

- System performance is significantly degraded
- Applications freeze or crash unexpectedly
- Operating system updates fail to install
- Low disk space warnings appear
- Temporary files and logs continue consuming storage space



#### Troubleshooting Steps:

- Review available disk storage capacity
- Identify large files, temporary data, and unnecessary applications



## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Analyze storage usage by directory or application
- Remove unnecessary files and clear temporary storage
- Verify sufficient free space is restored
- Validate normal system performance after cleanup

### Tools to use:

- **Windows:**
  - Disk Cleanup
  - Storage Settings
  - File Explorer
- **macOS:**
  - Storage Management
  - Finder
  - Disk Utility
- **Linux:**
  - df -h
  - du -sh
  - lsblk
  - GNOME Disk Utility

### Root Cause:

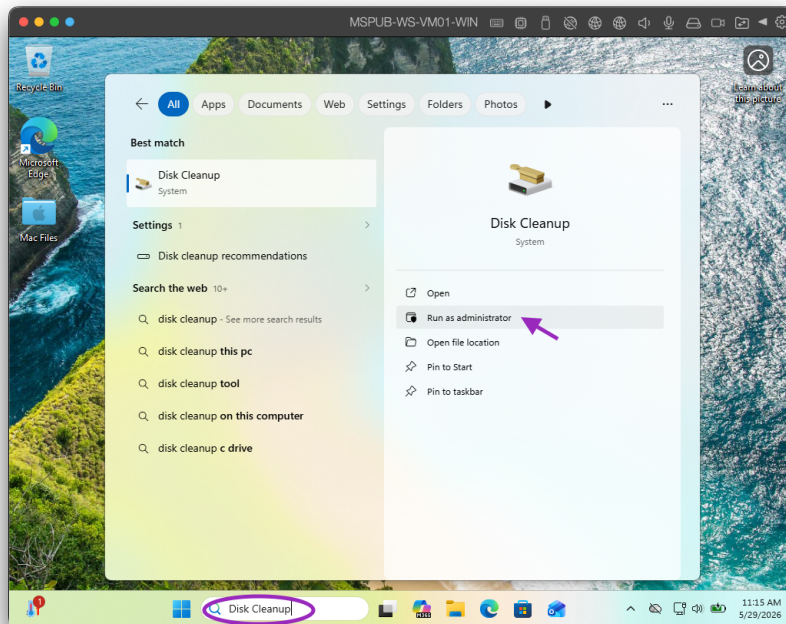
The workstation storage drive became critically low on available space due to accumulated temporary files, outdated system logs, and large unused files.

### Resolution:

Unnecessary files, temporary data, and unused applications were removed from the workstation. Storage optimization tools were used to reclaim disk space and restore normal operating conditions.

### Validation Testing:

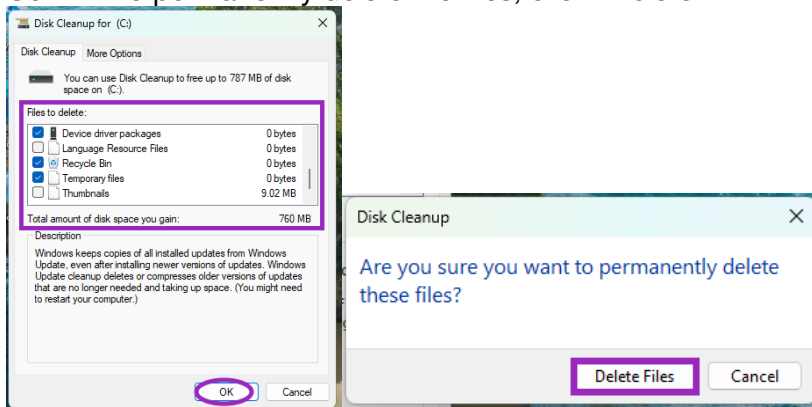
- **Windows**
  - Search for “Disk Cleanup” on the Taskbar and select “Run as administrator.”



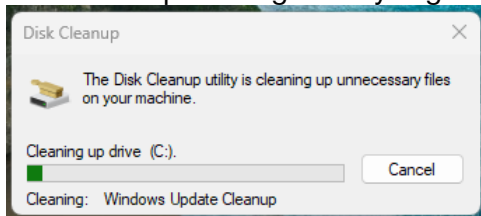
- Scroll through the files to delete and select:
  - Windows Update Cleanup
  - Downloaded Program Files
  - Temporary Internet Files
  - Recycle Bin
  - Temporary files
  - And any other storage hogs
- Click “OK” when completed.

## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

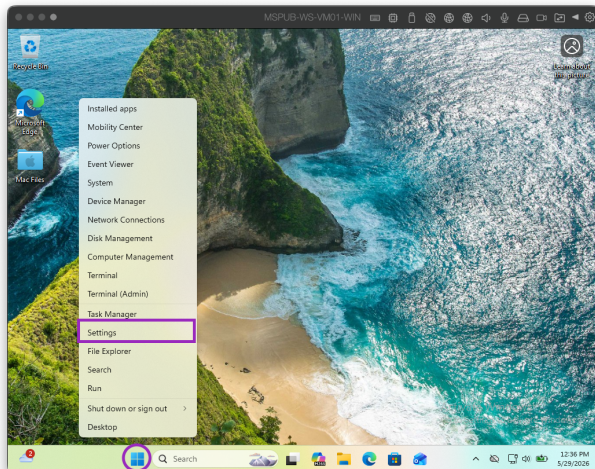
- Confirm to permanently delete the files, click “Delete.”



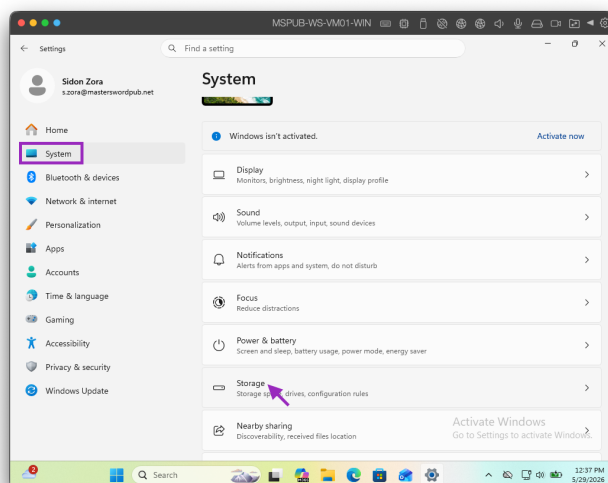
- Disk Cleanup will begin analyzing the disk and removing the selected files



- Open “Settings” by right clicking the Windows charm on the Taskbar.

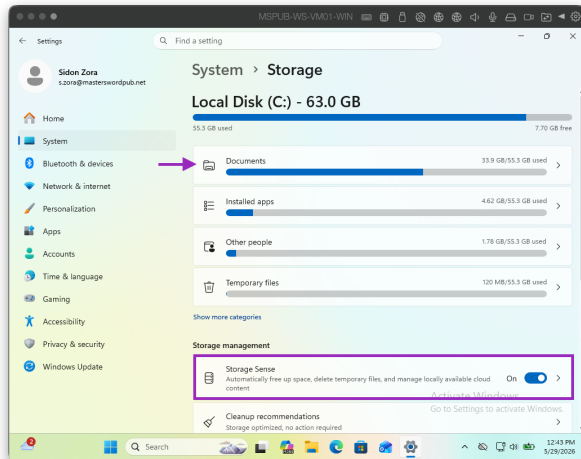


- In Settings on the left select “System” then click “Storage” on the right

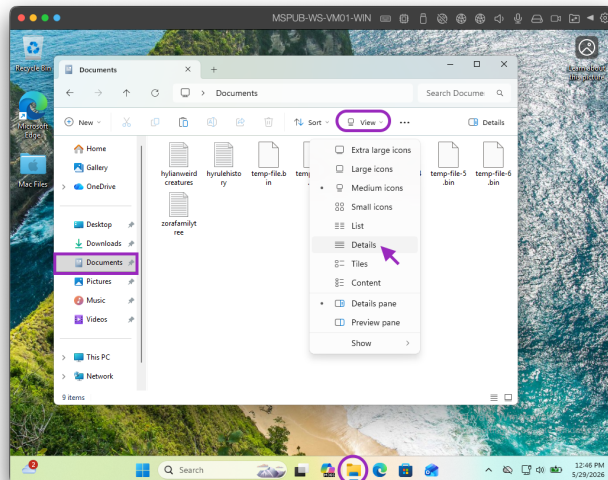


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

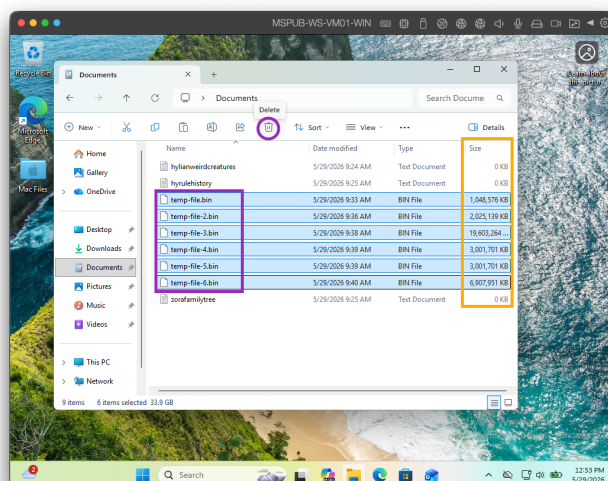
- This shows what type of files are consuming the most amount of space on the disk. Also on this screen ensure “Storage Sense” is turned “On.” Looking at this screen it shows that Documents folder is using a significant amount of space.



- Open “File Explorer” from the Taskbar. Navigate to the user’s Documents folder. Change the icon view by going to “View” in the toolbar and selecting “Details.”



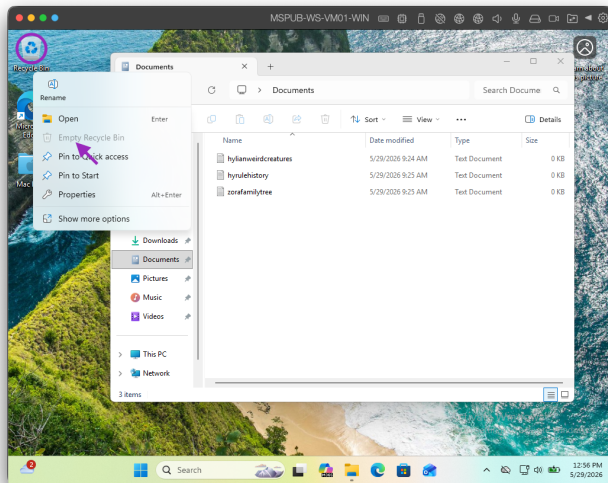
- Notice in the Size column that there are 6 temporary files consuming multi-gigabytes of storage. If the user no longer needs these files delete by highlighting them all and click the trash can icon in the toolbar.



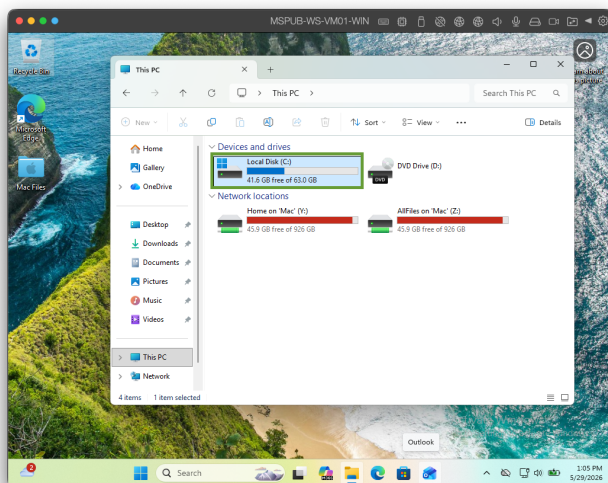


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Right click the “Recycle Bin” on the desktop and select “Empty” to permanently delete the files.



- Confirm the free space has been restored by selecting “This PC” on the left pane of File Explorer.

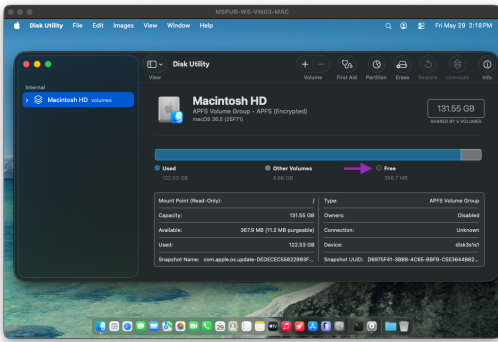


- **macOS**
  - From the Dock click on “Apps.” Scroll down to Other and click on “Disk Utility.”



- This will show you the amount of space currently being used on the system. Or if a new disk was installed where it gets formatted for the Mac’s filesystem. Here it shows that there are currently 357.3MB of storage free and 122.53GB is being used.

## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting



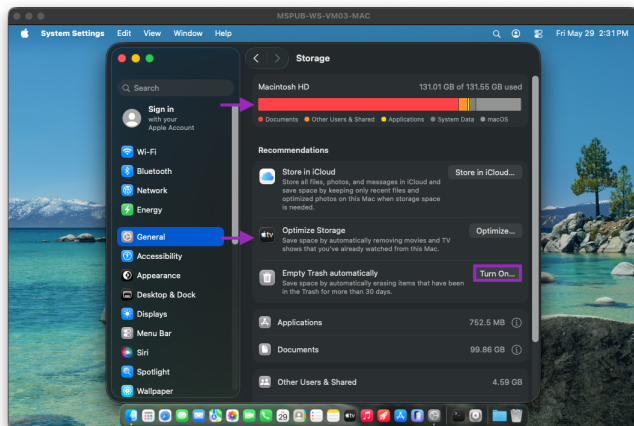
- Click the “Apple menu” in the Menubar and select “System Settings...”



- In settings click “General” on the left panel then select “Storage” on the right.

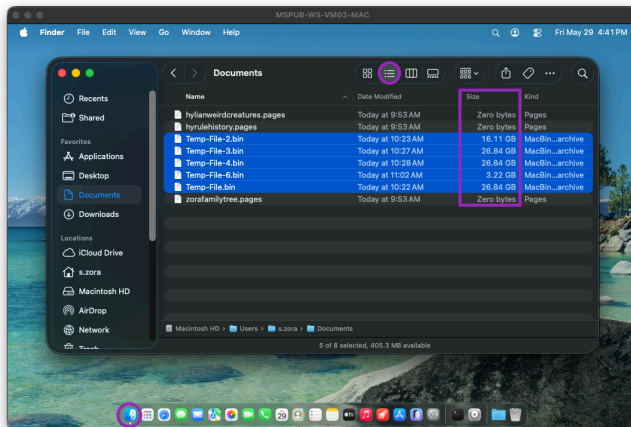


- Storage shows which categories are consuming most of the disk space. This is showing that there are documents using significant amounts of storage. The disk can also be optimized to automatically remove unused videos, files, and apps. Turn on “Empty Trash automatically” to automatically erase items in the trash for 30 days.

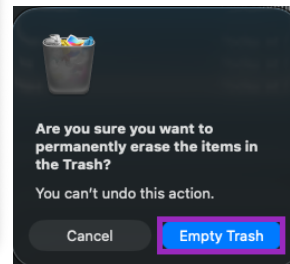
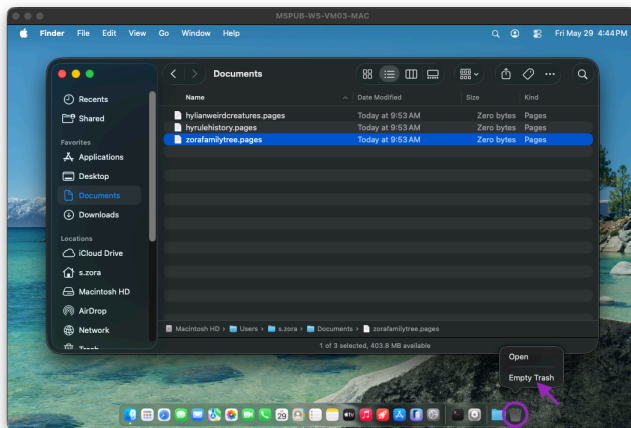


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

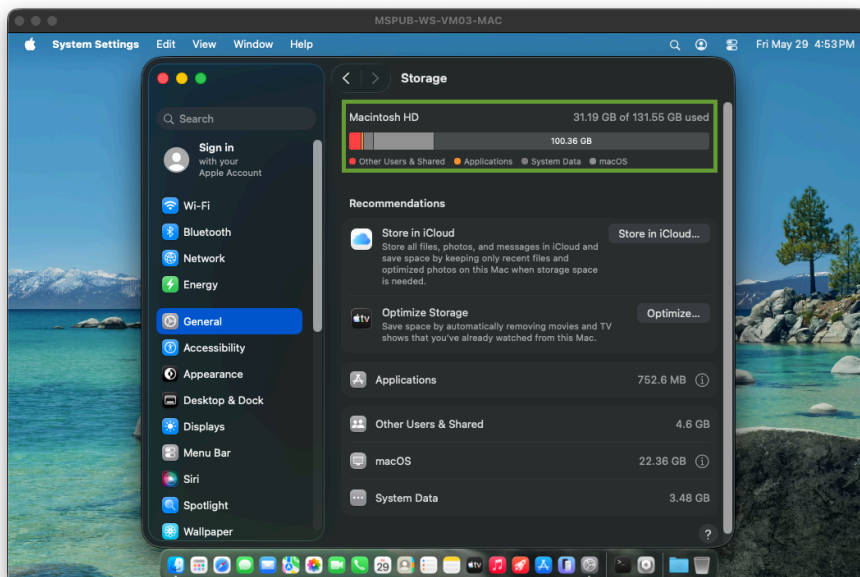
- Open a “Finder” window and navigate to the User’s Documents. Change the view to “List” to see more metadata about each file. Looking at the size column there are five files consuming a significant amount of data. If the user no longer needs these files highlight them then press “Command+Delete” to move them to the trash.



- Right-click the “Trash” icon in the dock and select “Empty Trash.” Confirm with clicking “Empty Trash.”

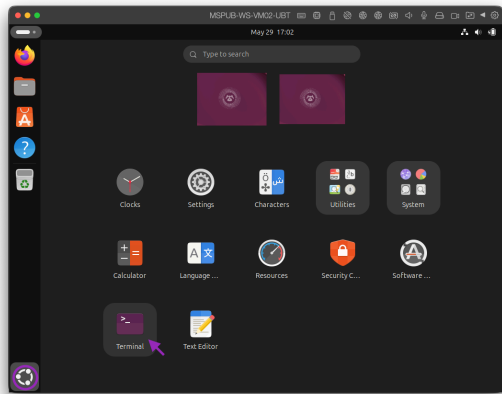


- Back in System Settings > General > Storage confirm the free space has been reallocated.



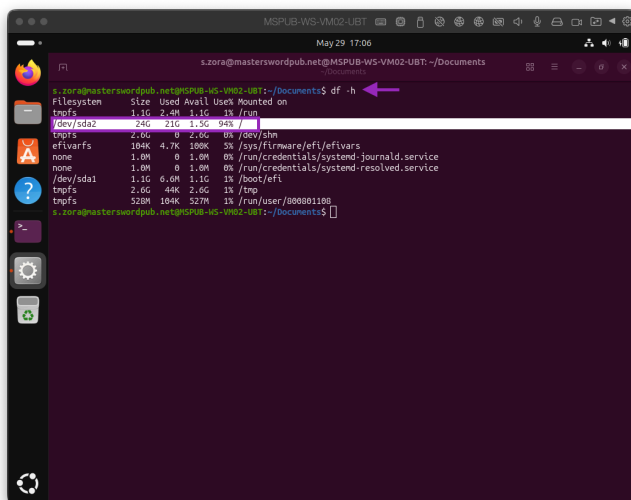
- **Linux**

- Open “Terminal” from the “Ubuntu charm” on the sidebar.



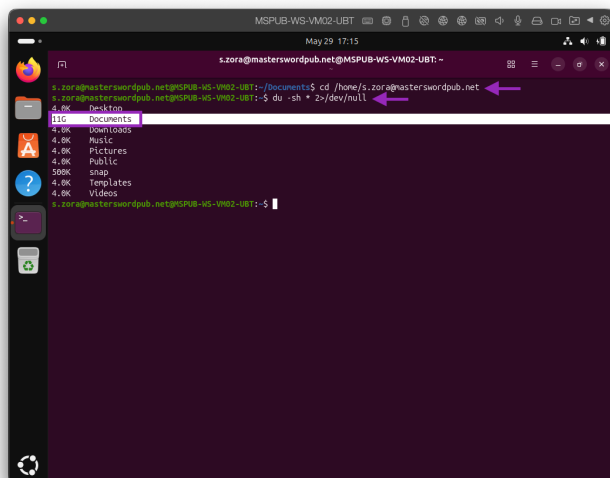
- Check the current disk usage by entering the command:  
df -h

With this command it shows the usage of the disks. This shows that the user is currently using 94% of the system disk.



- To identify where these large files are located enter the following commands:  
cd /home/s.zora@masterswordpub.net  
du -sh \* 2>/dev/null

This will show that 11GB of data is located in the users Documents directory.



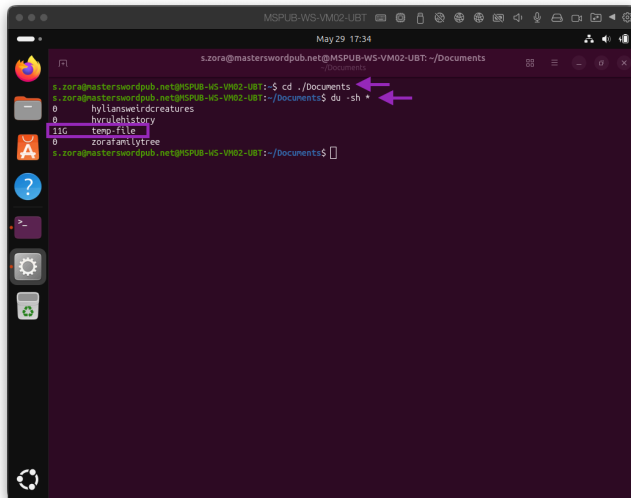
## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Change the directory to the user's Documents and show the file sizes by using the following commands:

```
cd ./Documents
```

```
du -sh *
```

This will show that there is one file consuming 11GB of disk space



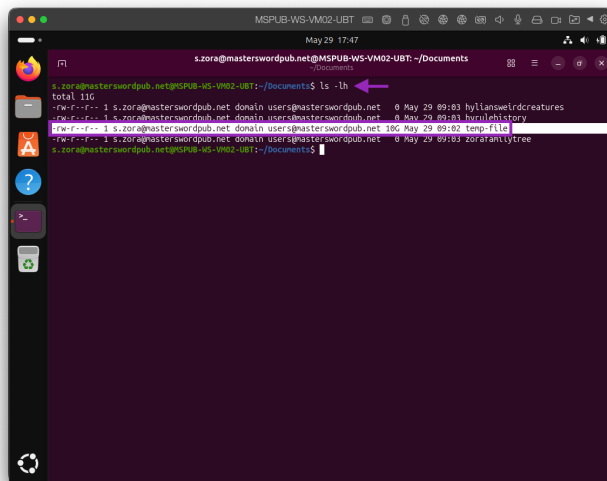
A terminal window titled 'MSPUB-WS-VM02-UBT' showing the execution of the 'du -sh \*' command in the '/Documents' directory. The output lists four files: 'hyllansweirdcreatures' (0), 'hyllanhistory' (0), 'temp-file' (11G), and 'zoratanlytree' (0). Red arrows point to the 'cd ./Documents' and 'du -sh \*' commands in the input history.

```
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT: ~/Documents
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$ cd ./Documents
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$ du -sh *
0 hyllansweirdcreatures
0 hyllanhistory
11G temp-file
0 zoratanlytree
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$
```

- Verify the file sizes by using the following command:

```
ls -lh
```

This will confirm which file is responsible for storage issues

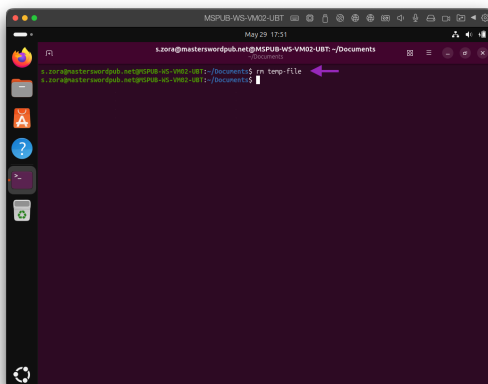


A terminal window titled 'MSPUB-WS-VM02-UBT' showing the execution of the 'ls -lh' command in the '/Documents' directory. The output shows the file 'temp-file' with a size of 10G. Red arrows point to the 'cd ./Documents' and 'ls -lh' commands in the input history.

```
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT: ~/Documents
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$ ls -lh
total 11G
-rw-r--r-- 1 s.zora@masterswordpub.net domain users@masterswordpub.net 0 May 29 09:03 hyllansweirdcreatures
-rw-r--r-- 1 s.zora@masterswordpub.net domain users@masterswordpub.net 0 May 29 09:03 hyllanhistory
-rw-r--r-- 1 s.zora@masterswordpub.net domain users@masterswordpub.net 10G May 29 09:03 temp-file
-rw-r--r-- 1 s.zora@masterswordpub.net domain users@masterswordpub.net 0 May 29 09:03 zoratanlytree
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$
```

- If the user no longer needs this file delete it with the following command:

```
rm temp-file
```



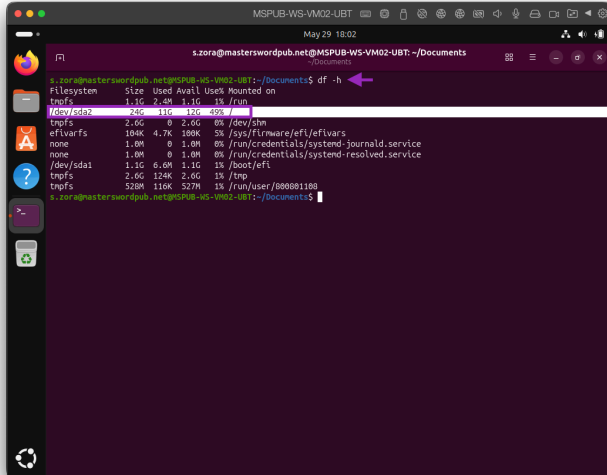
A terminal window titled 'MSPUB-WS-VM02-UBT' showing the execution of the 'rm temp-file' command in the '/Documents' directory. A red arrow points to the 'rm temp-file' command in the input history.

```
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT: ~/Documents
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$ rm temp-file
s.zora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$
```

## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Confirm the disk space has been recovered with the following command:  
df -h

This shows that the disk space has been restored



A terminal window titled 'MSPUB-WS-VM02-UBT' showing the output of the 'df -h' command. The output is a table with columns: Filesystem, Size, Used, Avail, Use%, and Mounted on. The table lists various filesystems including tmpfs, /dev/sda1, and /dev/sda2, along with their respective sizes, used space, available space, and usage percentages. A purple arrow points to the 'df -h' command prompt.

```
s.sora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$ df -h
```

| Filesystem | Size | Used | Avail | Use% | Mounted on                                |
|------------|------|------|-------|------|-------------------------------------------|
| tmpfs      | 1.1G | 2.4M | 1.1G  | 1%   | /run                                      |
| /dev/sda2  | 2.0G | 11G  | 43G   | 43%  | /                                         |
| tmpfs      | 2.0G | 0    | 2.0G  | 0%   | /dev/shm                                  |
| efivarfs   | 104K | 4.7K | 100K  | 5%   | /sys/firmware/efi/efivars                 |
| none       | 1.0M | 0    | 1.0M  | 0%   | /run/credentials/systemd-journald.service |
| none       | 1.0M | 0    | 1.0M  | 0%   | /run/credentials/systemd-resolved.service |
| /dev/sda1  | 1.1G | 6.6M | 1.1G  | 1%   | /boot/efi                                 |
| tmpfs      | 2.0G | 124K | 2.0G  | 1%   | /tmp                                      |
| tmpfs      | 520M | 110K | 520M  | 1%   | /run/user/1000001100                      |

```
s.sora@masterswordpub.net@MSPUB-WS-VM02-UBT:~/Documents$
```



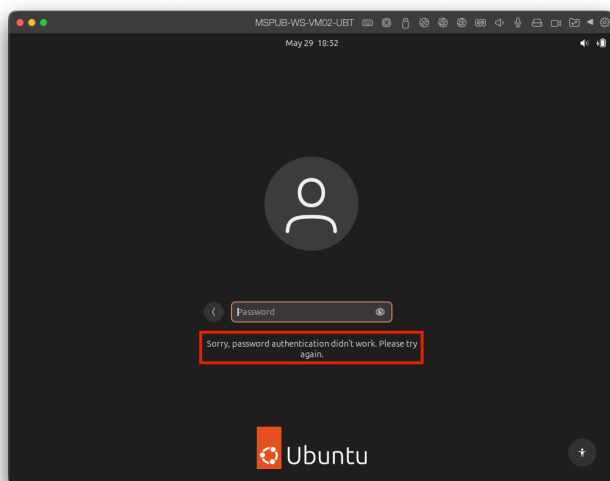
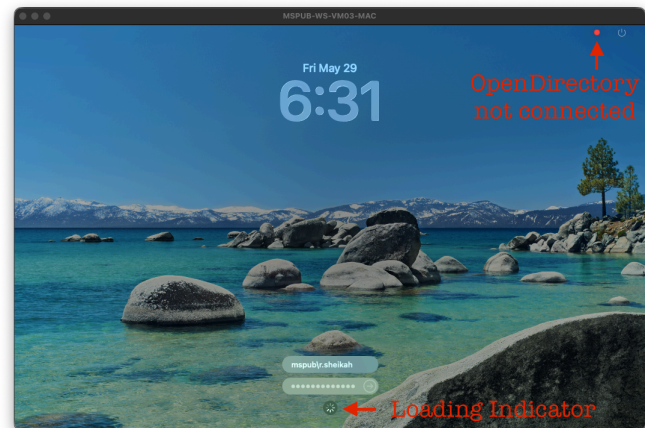
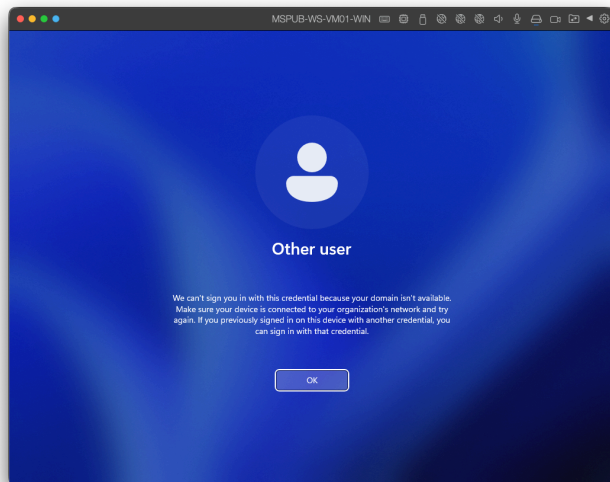
## Scenario 4: Virtual Machine Network Issue

### Scenario Description:

Robbie from MSPUB IT Department reported that a newly deployed virtual machine using Parallels was unable to access the internal network resources or connect to the internet after deployment within the Master Sword Publishing virtualized environment. The workstation appeared to function normally; however, all network communication attempts failed. An IT Service Ticket was submitted after the user was unable to access shared services, internal websites, or cloud-based applications. Initial troubleshooting verified that the virtual machine operating system was functioning properly, but network connectivity remained unavailable.

### Symptoms:

- Virtual machine unable to access the internet
- Internal network resources inaccessible
- Users cannot login using domain accounts
- No response from ping requests
- DHCP address not assigned correctly
- Network adapter appears disconnected or improperly configured



### Troubleshooting Steps:

- Verify virtual machine network adapter status



## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Inspect Parallels network adapter configuration
- Confirm correct network mode selection (NAT, Bridged, or Host-Only)
- Renew DHCP lease and validate IP address assignment
- Test connectivity to gateway, DNS server, and external resources
- Restart Parallels network services if necessary

### Tools to use:

- **Parallels**
  - Parallels Network Settings
- **Windows:**
  - ipconfig /all
  - ping
  - tracert
- **macOS/Linux:**
  - ifconfig
  - ip addr
  - ping
  - netstat

### Root Cause:

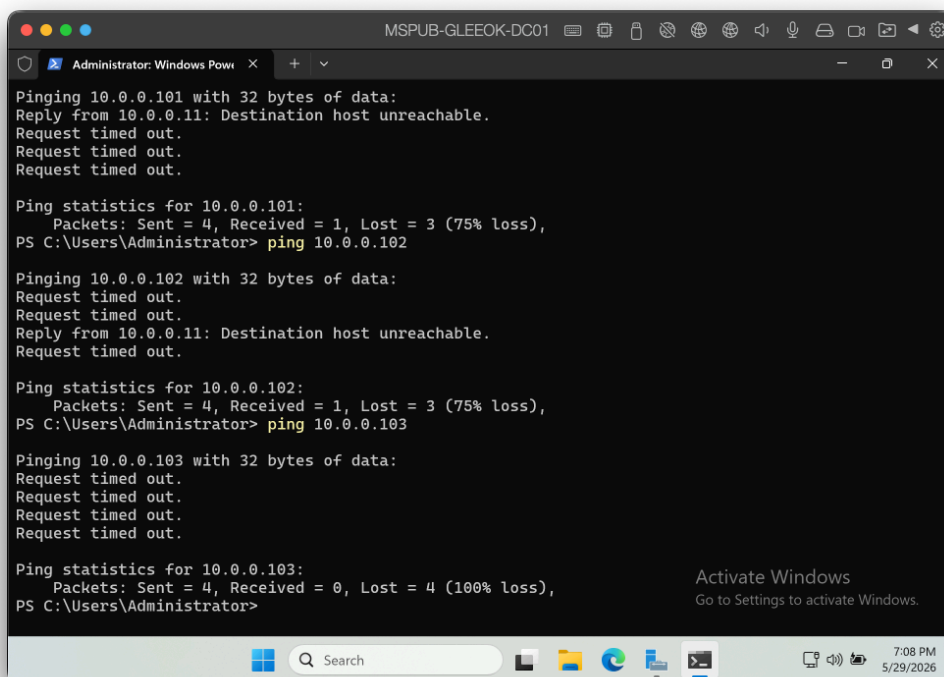
The virtual machine network adapter was incorrectly configured within Parallels, preventing the system from obtaining proper network connectivity and communication with internal and external resources.

### Resolution:

The Parallels network adapter configuration was corrected and assigned to the appropriate network mode. Network connectivity was restored after renewing the DHCP lease and validating proper communication with network resources.

### Validation Testing:

- **MSPUB-COLGERA-DM01**
    - Use “Terminal” on the Domain Manager to ping the offline machines:
      - ping 10.0.0.101
      - ping 10.0.0.102
      - ping 10.0.0.103
- This shows no responses from MSPUB-WS-VM01-WIN, MSPUB-WS-VM02-UBT, MSPUB-WS-VM03-MAC have no response.



```
MSPUB-GLEEOK-DC01
Administrator: Windows PowerShell
Pinging 10.0.0.101 with 32 bytes of data:
Reply from 10.0.0.11: Destination host unreachable.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.101:
 Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
PS C:\Users\Administrator> ping 10.0.0.102

Pinging 10.0.0.102 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.0.0.11: Destination host unreachable.
Request timed out.

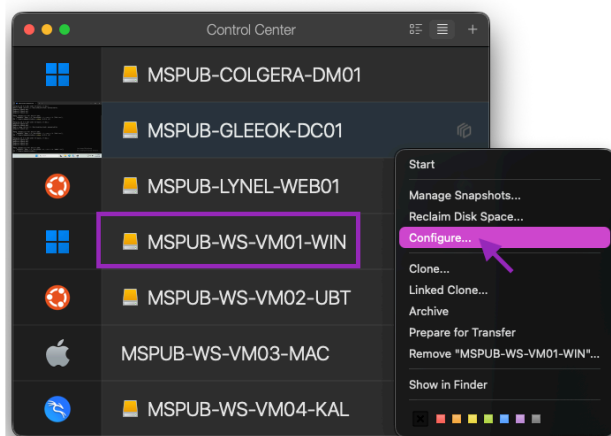
Ping statistics for 10.0.0.102:
 Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
PS C:\Users\Administrator> ping 10.0.0.103

Pinging 10.0.0.103 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

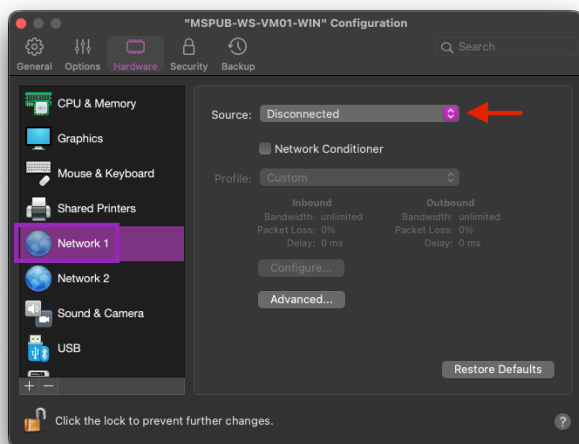
Ping statistics for 10.0.0.103:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator>
```

- **Parallels Host Machine**

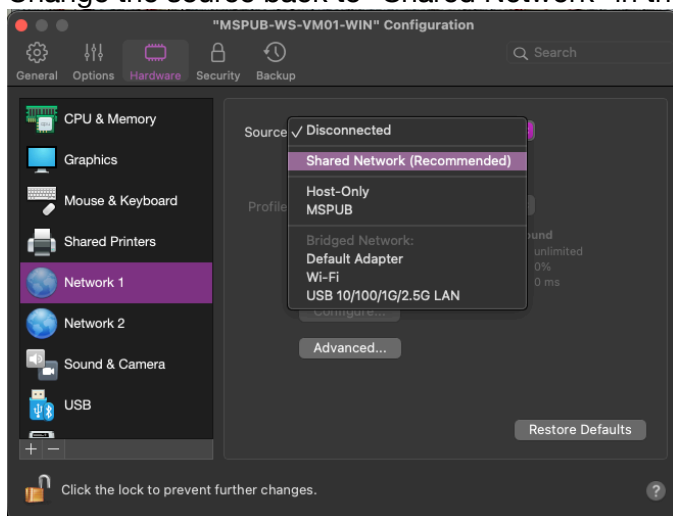
- In Parallels Control Center right click MSPUB-WS-VM01-WIN and select “Configure.”



- Click “Network 1” and check the source. This shows the virtual network card is disabled.

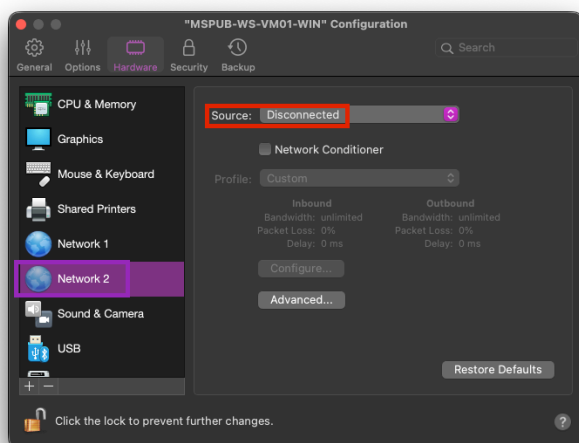


- Change the source back to “Shared Network” in the drop down menu.

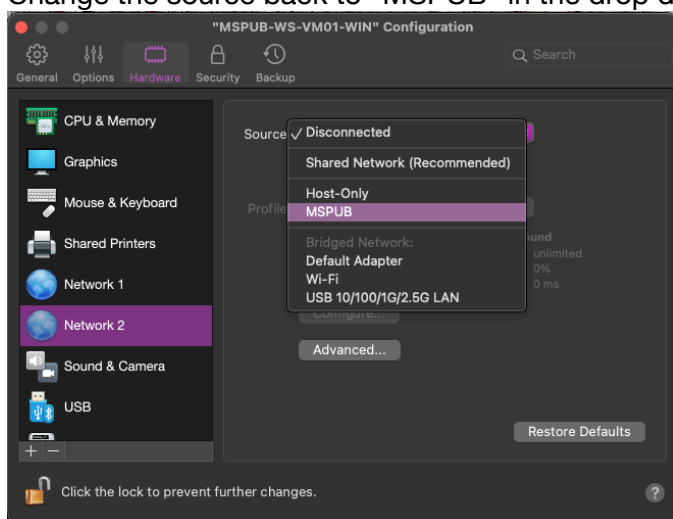


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

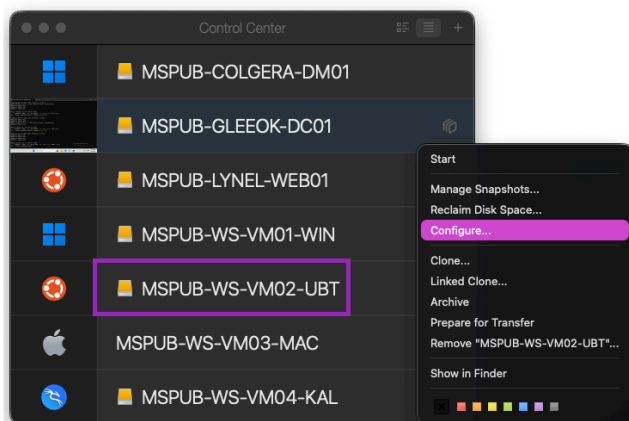
- Select “Network 2” on the left pane. The source also shows the virtual network card is disabled.



- Change the source back to “MSPUB” in the drop down menu. Close the configuration window.

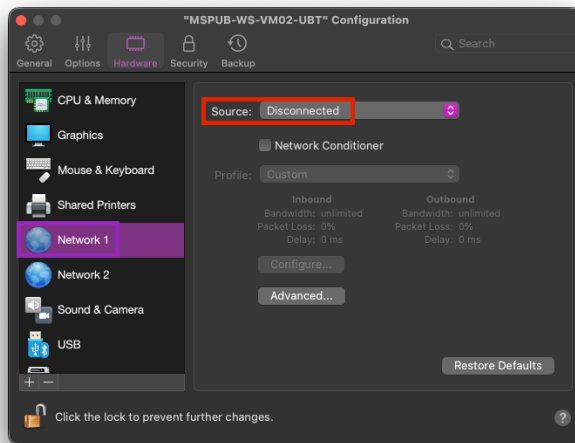


- In Parallels Control Center right click MSPUB-WS-VM02-UBT and select “Configure.”

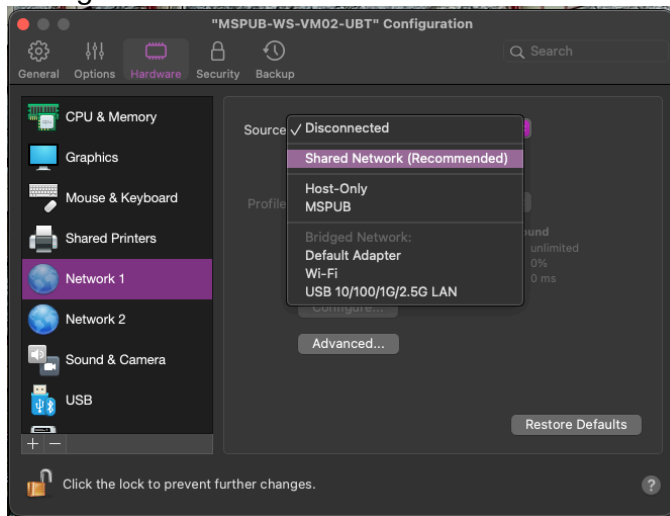


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

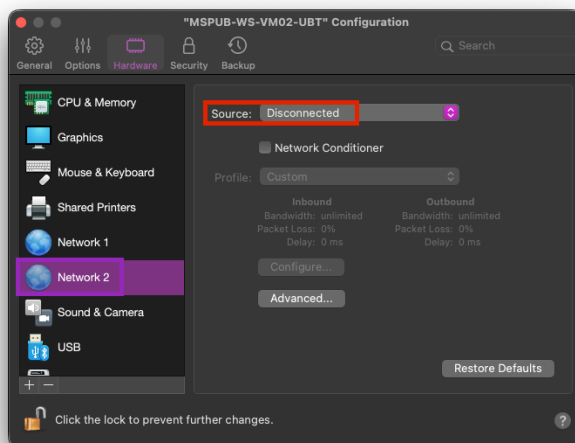
- Click “Network 1” and check the source. This shows the virtual network card is disabled.



- Change the source back to “Shared Network” in the drop down menu.

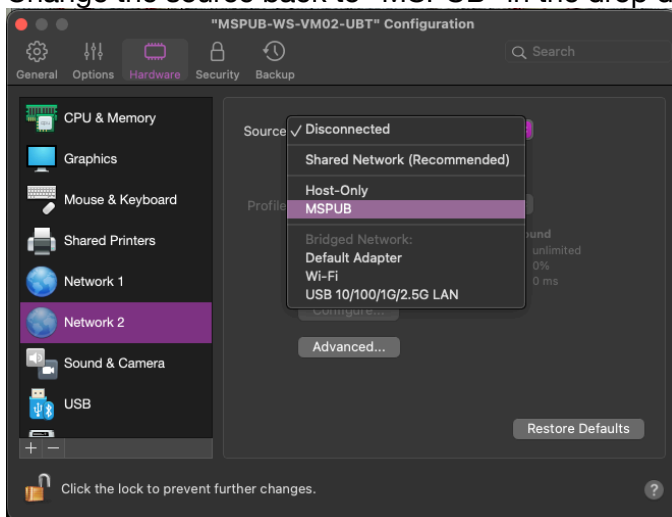


- Select “Network 2” on the left pane. The source also shows the virtual network card is disabled.

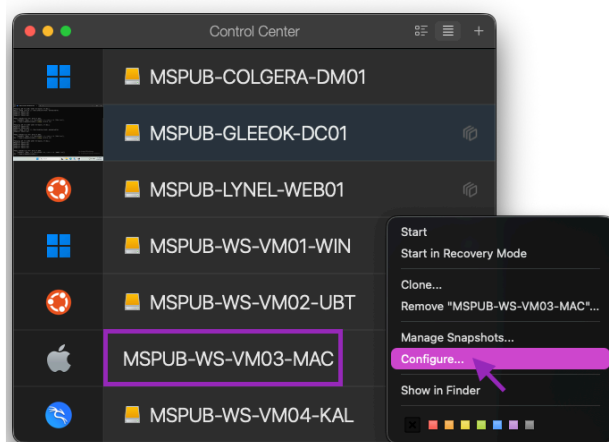


## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

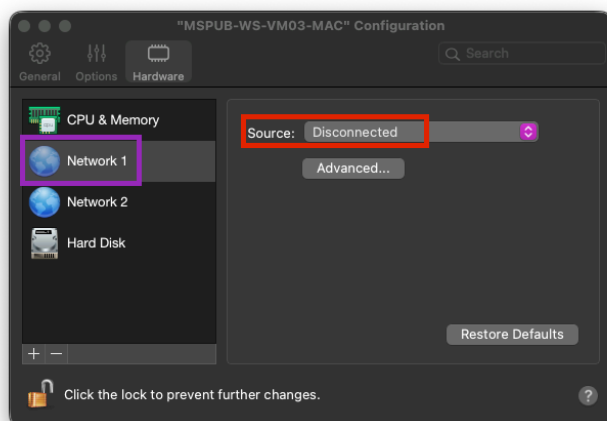
- Change the source back to “MSPUB” in the drop down menu. Close the configuration window.



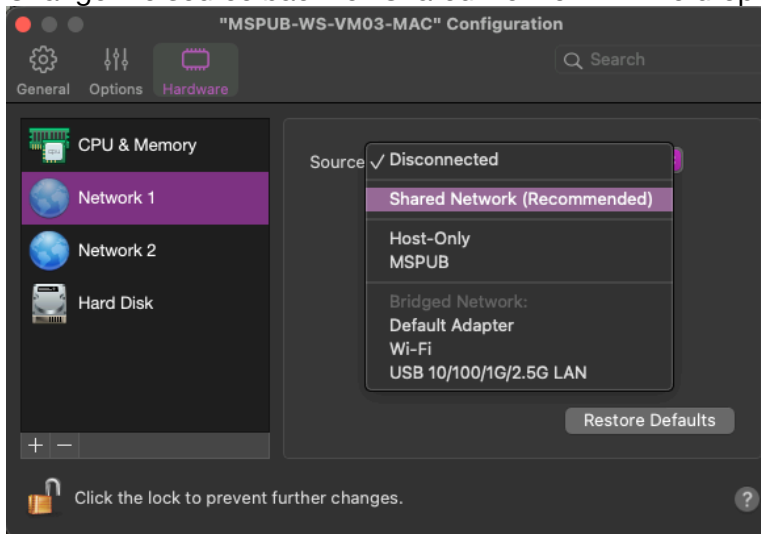
- In Parallels Control Center right click MSPUB-WS-VM03-MAC and select “Configure.”



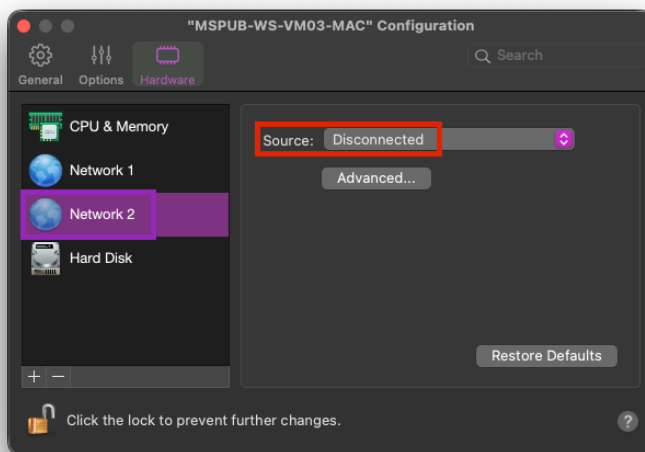
- Click “Network 1” and check the source. This shows the virtual network card is disabled.



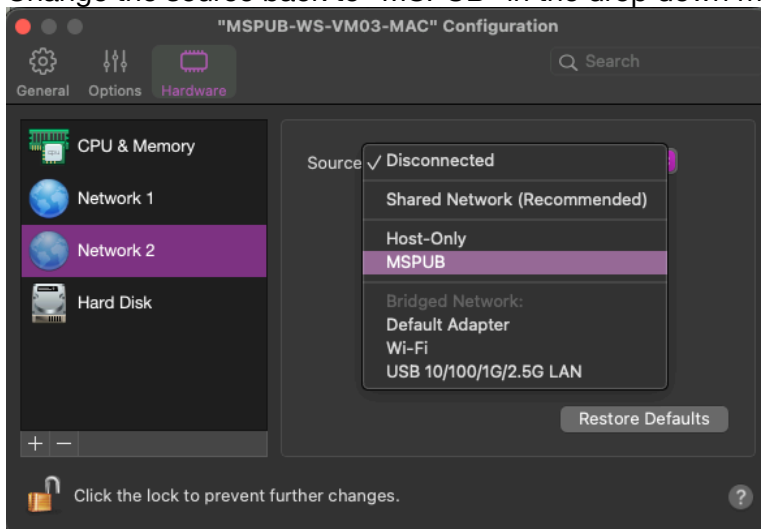
- Change the source back to “Shared Network” in the drop down menu.



- Select “Network 2” on the left pane. The source also shows the virtual network card is disabled.



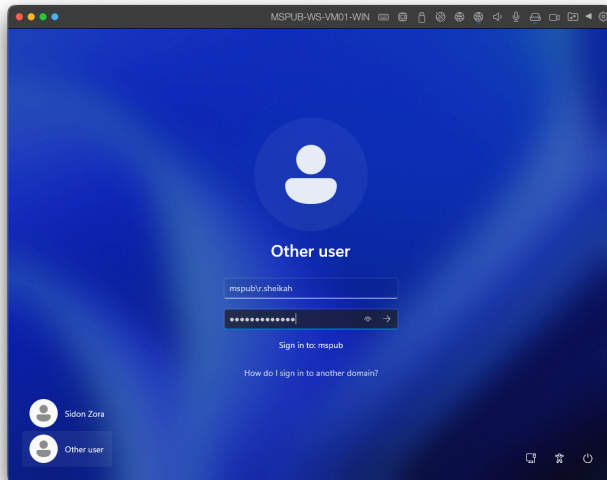
- Change the source back to “MSPUB” in the drop down menu. Close the configuration window.



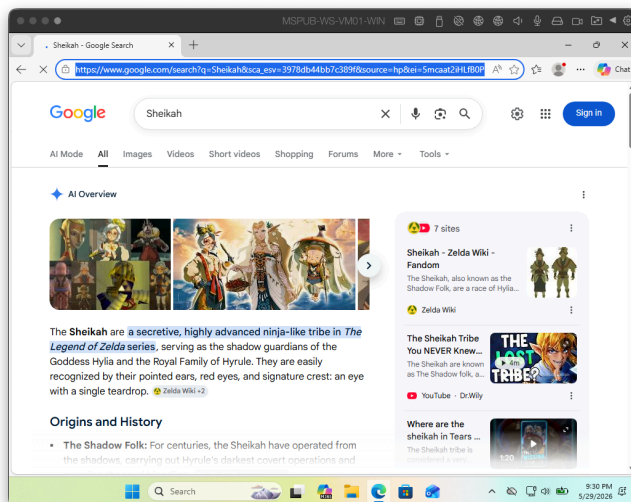
## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- **Windows**

- Launch MSPUB-WS-VM01-WIN. Have the user try logging in with their MSPUB credentials.

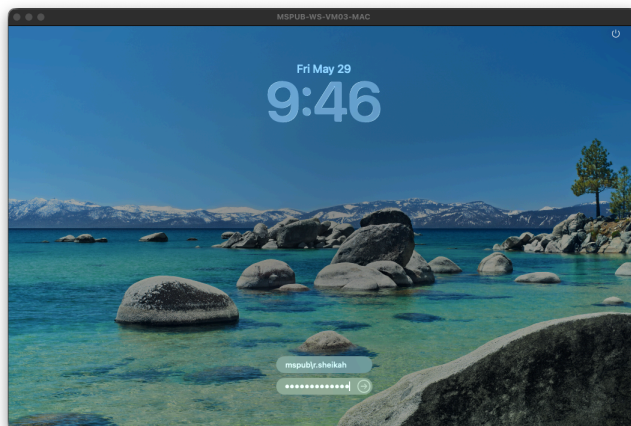


- Confirm webpages will load by launching the web browser and going to google.com.



- **macOS**

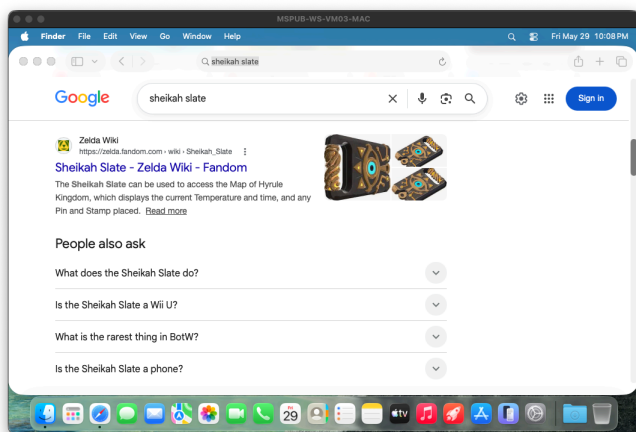
- Launch MSPUB-WS-VM03-MAC. Have the user try logging in with their MSPUB credentials.





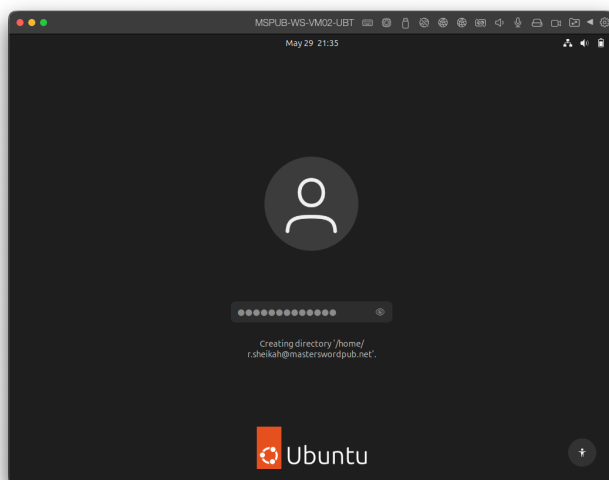
## Part 1: Software Essentials & Hardware: Home Lab & Troubleshooting

- Confirm webpages will load by launching the web browser and going to google.com.

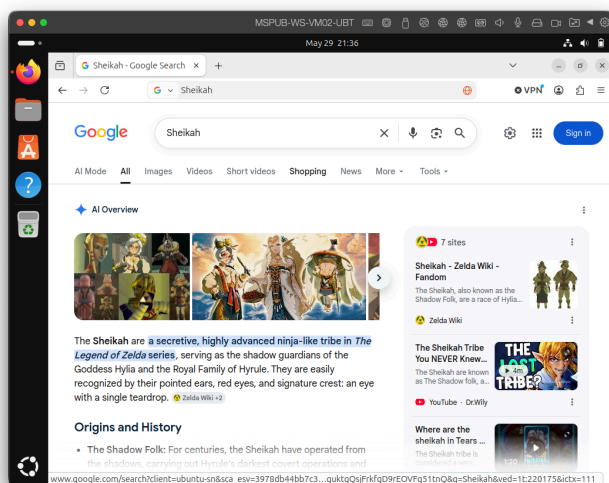


- **Linux**

- Launch MSPUB-WS-VM02-UBT. Have the user try logging in with their MSPUB credentials.



- Confirm webpages will load by launching the web browser and going to google.com.



# Master Sword Publishing Automation with Python Scripts

## Automated Web Server System Configuration Script

### Scenario Overview

Master Sword Publishing (MSPUB) recently deployed MSPUB-LYNEL-WEB01, an Ubuntu Server intended to host an internal company website for the [masterswordpub.net](http://masterswordpub.net) domain. The Online Services department needs a reliable web server environment where the internal web content can be developed, hosted, and tested.

To reduce manual configuration errors and improve deployment consistency, the MSPUB IT Department will create a Python-based automated system configuration script. This script will configure the Ubuntu Server by installing required packages, enabling essential services, configuring firewall rules, creating the internal web directory, deploying a basic MSPUB landing page, and logging all major actions.

### Objective

Develop a Python automation script that streamlines the initial configuration of the MSPUB Ubuntu web server.

### Planned Features

- Update package repositories
- Install Nginx
- Install and enable OpenSSH
- Configure SFTP support
- Configure UFW firewall rules
- Allow HTTP, SSH, and SFTP traffic
- Create the MSPUB web directory
- Create SFTP upload directory
- Create publishing group
- Deploy a basic internal landing page
- Set appropriate file permissions
- Enable and start required services
- Record actions in a log file
- Include basic error handling and validation

### Systems Used

- MSPUB-LYNEL-WEB01
- MSPUB-UBTSVR-TESTWORLD
- Ubuntu Server 26.04
- Python 3
- Sublime Text
- Nginx
- OpenSSH
- UFW Firewall

### Script Design

The script was developed using a modular function-based approach. Each major configuration task was separated into individual functions to improve readability, maintainability, and troubleshooting capabilities.

Major functions included:

- check\_root()
- log\_action()
- run\_command()
- system\_updater()
- install\_packages()
- configure\_firewall()
- create\_web\_directory()
- create\_sftp\_directory()
- create\_publishing\_group()
- deploy\_landing\_page()
- configure\_nginx\_site()
- enable\_services()
- verify\_config()

This design allowed individual components of the deployment process to be tested independently while maintaining a clear workflow.

## Part 2: Open-Source OSs & Shells and Scripts: System Configuration & User Management Scripts

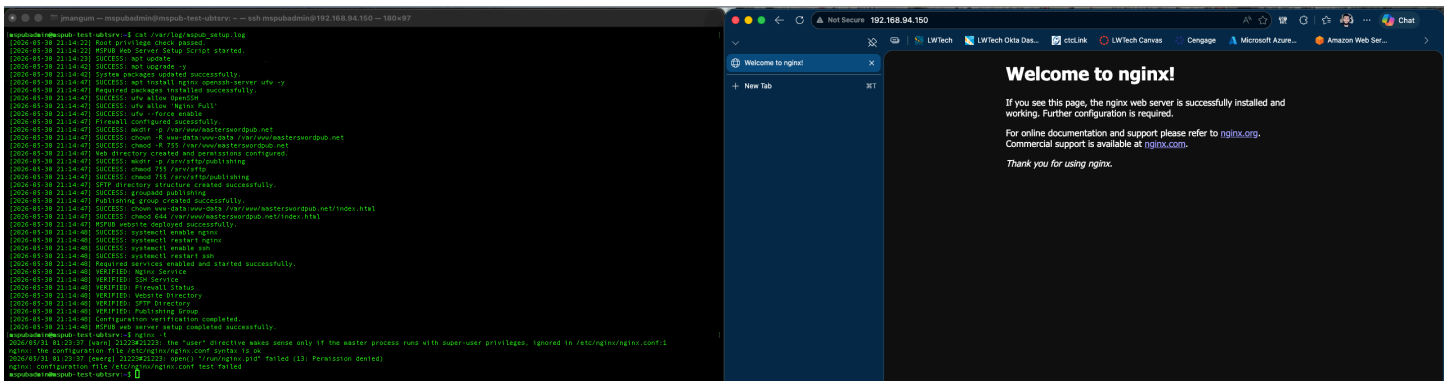
### Testing & Validation

The script was initially tested on a dedicated Ubuntu Server test virtual machine prior to deployment on the production MSPUB-LYNEL-WEB01 server.

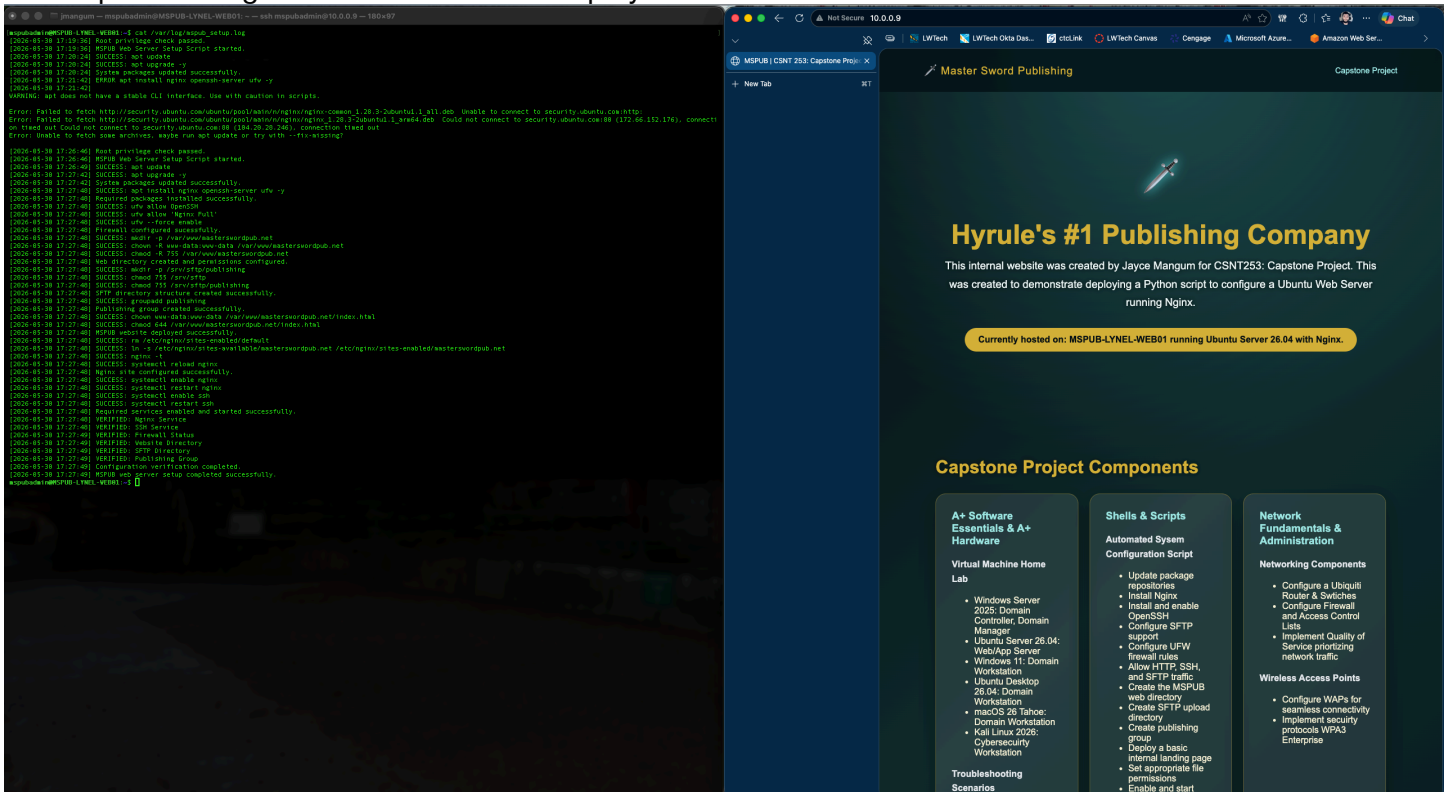
Testing included:

- Python syntax validation using `py_compile`
- Package installation verification
- Firewall configuration verification
- Directory creation verification
- Group creation verification
- Nginx service validation
- OpenSSH service validation
- Website deployment validation

Initial testing identified an issue where Nginx continued serving as the default Ubuntu landing page. Investigation revealed that the default Nginx site configuration remained enabled. The script was modified to automatically remove the default configuration, enable the MSPUB virtual host, validate the configuration using `nginx -t`, and reload the Nginx service.

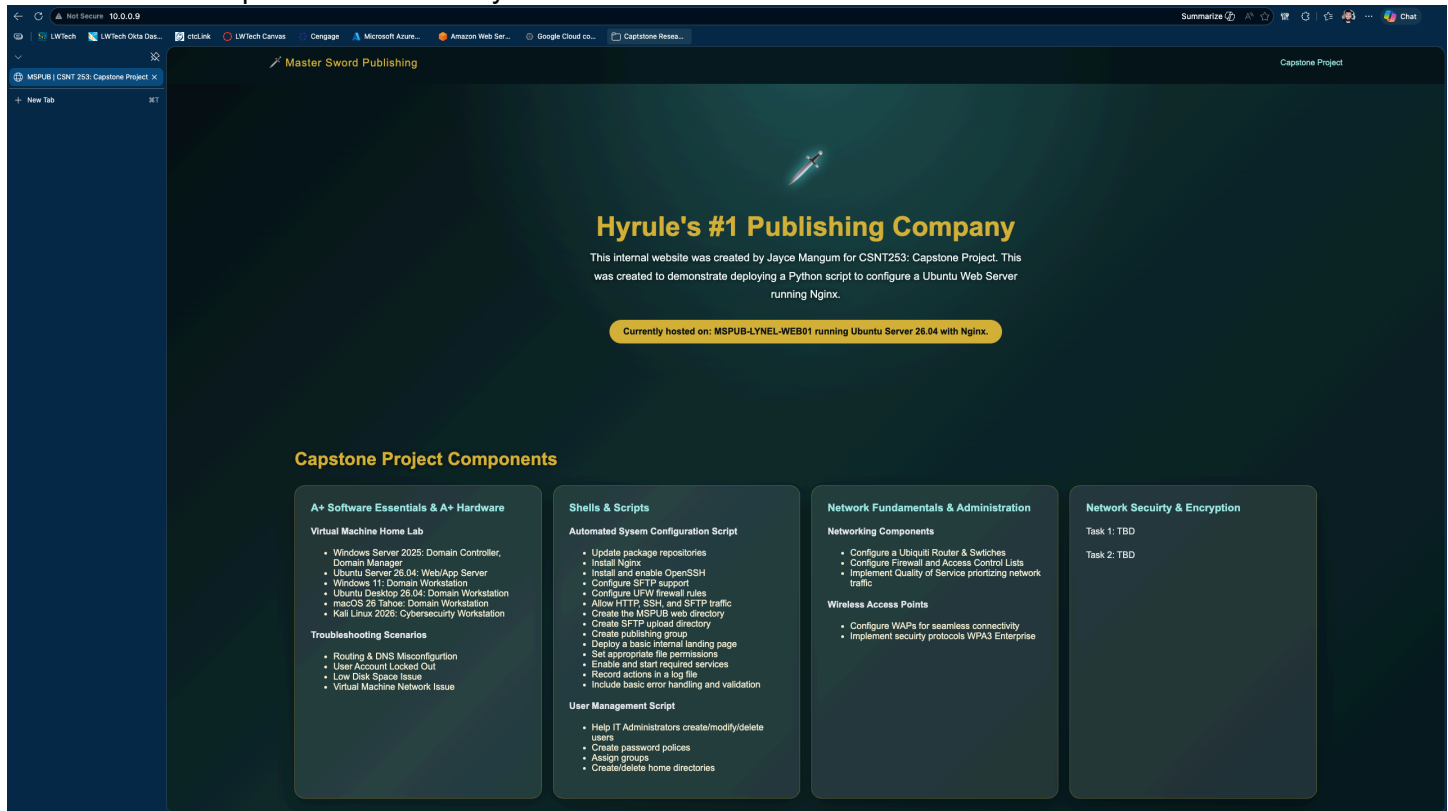


Subsequent testing confirmed successful deployment of the MSPUB website.



### Results

The automation script successfully configured the Ubuntu Server environment without requiring manual installation of services or creation of required directories. The MSPUB landing page was successfully deployed and served through Nginx. Firewall rules were configured, SFTP infrastructure was created, and all validation checks passed successfully.



### Challenges Encountered

A few issues occurred during development and testing. The most significant challenge involved Python indentation errors and Nginx virtual host configuration. These issues were resolved through incremental testing, syntax validation, and functional testing on a dedicated test virtual machine.

```
Scripts — -zsh — 80x24

Last login: Thu May 28 09:58:07 on ttys000
jmangum@DINRAAL ~ % cd /Volumes/CSNT-CAPPJ/Scenario\ Documents/Part02-LinuxScripts/Scripts
jmangum@DINRAAL Scripts % python3 -m py_compile mspub-webserver-setup.py
[Sorry: IndentationError: unexpected indent (mspub-webserver-setup.py, line 44)]
jmangum@DINRAAL Scripts % python3 -m py_compile mspub-webserver-setup.py
[Sorry: IndentationError: unexpected indent (mspub-webserver-setup.py, line 44)]
jmangum@DINRAAL Scripts % python3 -m py_compile mspub-webserver-setup.py
[Sorry: IndentationError: unexpected indent (mspub-webserver-setup.py, line 81)]
jmangum@DINRAAL Scripts % python3 -m py_compile mspub-webserver-setup.py
jmangum@DINRAAL Scripts %
```

### msspub-webserver-setup v3.py Source Code

The script was written using Sublime Text with Python syntax highlighting:

[Download msspub-webserver-setup V3.py](#)

```
#!/usr/bin/env python3

import os
import subprocess
import logging
import shutil
from datetime import datetime

LOG_FILE = "/var/log/msspub_setup.log"
LOG_DIR = "/var/log"

def main():
 check_root()
 log_action("MSPUB Web Server Setup Script started.")
 system_updater()
 install_packages()
 configure_firewall()
 create_web_directory()
 create_sftp_directory()
 create_publishing_group()
 deploy_landing_page()
 configure_nginx_site()
 enable_services()
 verify_config()

 print("\nMSPUB Web Server Setup Complete!")
 log_action("MSPUB web server setup completed successfully.")

def log_action(message):
 """Write script activity to the log file."""
 timestamp = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
 with open(LOG_FILE, "a") as log:
 log.write(f"[{timestamp}] {message}\n")

def run_command(command):
 """Run a Linux command and log success or failure."""
 try:
 result = subprocess.run(
 command,
 shell=True,
 check=True,
 text=True,
 capture_output=True
)
 log_action(f"SUCCESS: {command}")
 return result.stdout
```

```

except subprocess.CalledProcessError as error:
 log_action(f"ERROR {command}")
 log_action(error.stderr)
 print(f"Command failed: {command}")
 print(error.stderr)
 exit(1)

def check_root():
 """Verify the script is running with root privileges."""
 if os.geteuid() != 0:
 print("The MSPUB Webserver Setup script must be run with sudo
privileges.")
 exit(1)

 log_action("Root privilege check passed.")

def system_updater():
 """Update Ubuntu package repositories and installed packages."""
 print ("Updating system packages...")

 run_command("apt update")
 run_command("apt upgrade -y")

 log_action("System packages updated successfully.")

def install_packages():
 """Install required packages for the MSPUB web server."""
 print("Installing required packages...")

 packages = [
 "nginx",
 "openssh-server",
 "ufw"
]

 package_list = " ".join(packages)
 run_command(f"apt install {package_list} -y")

 log_action("Required packages installed successfully.")

def configure_firewall():
 """Configuring UFW firewall rules."""
 print("Configuring firewall rules...")

 run_command("ufw allow OpenSSH")
 run_command("ufw allow 'Nginx Full'")
 run_command("ufw --force enable")

 log_action("Firewall configured sucessfully.")

```

```

def create_web_directory():
 """Create the MSPUB web directory and set permissions."""
 print("Creating web directory...")

 web_dir = "/var/www/masterswordpub.net"

 run_command(f"mkdir -p {web_dir}")
 run_command(f"chown -R www-data:www-data {web_dir}")
 run_command(f"chmod -R 755 {web_dir}")

 log_action("Web directory created and permissions configured.")

def create_sftp_directory():
 """Create SFTP directory structure for the Publishing department."""
 print("Creating SFTP directory...")

 sftp_dir = "/srv/sftp/publishing"

 run_command(f"mkdir -p {sftp_dir}")
 run_command(f"chmod 755 /srv/sftp")
 run_command(f"chmod 755 {sftp_dir}")

 log_action("SFTP directory structure created successfully.")

def create_publishing_group():
 """Create the Publishing group for SFTP access."""
 print("Creating publishing group...")

 group_name = "publishing"

 group_exists = subprocess.run(
 f"getent group {group_name}",
 shell=True,
 text=True,
 capture_output=True
)

 if group_exists.returncode == 0:
 log_action("Publishing group already exists.")
 print("Publishing group already exists.")
 else:
 run_command(f"groupadd {group_name}")
 log_action("Publishing group created successfully.")

def deploy_landing_page():
 """Deploy a basic MSPUB internal website landing page."""
 print("Deploying MSPUB landing page...")

 source_file = "mspub_index.html"
 destination_file = "/var/www/masterswordpub.net/index.html"

```



```

 if not os.path.exists(source_file):
 log_action(f"ERROR: {source_file} not found.")
 print(f"Error: {source_file} not found. Please upload {source_file} to
server.")
 exit(1)

 shutil.copy(source_file, destination_file)

 run_command(f'chown www-data:www-data {destination_file}')
 run_command(f"chmod 644 {destination_file}")

 log_action("MSPUB website deployed successfully.")

def configure_nginx_site():
 """Configure Nginx to server the MSPUB website."""
 print("Configuring Nginx site...")

 site_config = "/etc/nginx/sites-available/masterswordpub.net"
 enabled_site = "/etc/nginx/sites-enabled/masterswordpub.net"
 default_site = "/etc/nginx/sites-enabled/default"

 nginx_config = """server {
listen 80;
listen [::]:80;

server_name masterswordpub.net www.masterswordpub.net;

root /var/www/masterswordpub.net;
index index.html;

location / {
 try_files $uri $uri/ =404;
}
}
"""

 with open(site_config, "w") as file:
 file.write(nginx_config)

 if os.path.exists(default_site):
 run_command(f"rm {default_site}")

 if not os.path.exists(enabled_site):
 run_command(f"ln -s {site_config} {enabled_site}")

 run_command("nginx -t")
 run_command("systemctl reload nginx")

 log_action("Nginx site configured successfully.")

def enable_services():

```

```

"""Enable and start required services."""
print("Enabling and starting services...")

services = [
 "nginx",
 "ssh"
]

for service in services:
 run_command(f"systemctl enable {service}")
 run_command(f"systemctl restart {service}")

log_action("Required services enabled and started successfully.")

def verify_config():
 """Verify web server configuration."""
 print("Verifying configuration...")

 checks = [
 ("Nginx Service", "systemctl is-active nginx"),
 ("SSH Service", "systemctl is-active ssh"),
 ("Firewall Status", "ufw status"),
 ("Website Directory", "test -d /var/www/masterswordpub.net"),
 ("SFTP Directory", "test -d /srv/sftp/publishing"),
 ("Publishing Group", "getent group publishing")
]

 for check_name, command in checks:
 try:
 result = subprocess.run(
 command,
 shell=True,
 check=True,
 text=True,
 capture_output=True
)

 log_action(f"VERIFIED: {check_name}")
 print(f"[PASS] {check_name}")

 except subprocess.CalledProcessError:
 log_action(f"FAILED: {check_name}")
 print(f"[FAIL] {check_name}")

 log_action("Configuration verification completed.")

if __name__ == "__main__":
 main()

```



```

.section {
 padding: 70px 10%;
}
.section h2 {
 color: #d4af37;
 margin-bottom: 28px;
 font-size: 2rem;
 text-shadow: 0 0 10px rgba(0,0,0,0.6);
}
.sword {
 font-size: 4rem;
 text-shadow: 0 0 20px #5ce1e6;
}
h1 {
 font-size: 3rem;
 color: #d4af37;
 margin-bottom: 12px;
}
.subtitle {
 max-width: 800px;
 margin: 0 auto;
 font-size: 1.2rem;
 line-height: 1.7;
 color: #eef8f8;
 text-shadow: 0 0 8px rgba(0, 0, 0, 0.8);
}
.badge {
 display: inline-block;
 margin-top: 28px;
 padding: 12px 24px;
 border-radius: 999px;
 background: #d4af37;
 color: #061014;
 font-weight: bold;
}
.cards {
 display: grid;
 grid-template-columns: repeat(auto-fit, minmax(220px, 1fr));
 gap: 20px;
 margin-top: 24px;
}
.card {
 background: rgba(255, 255, 255, 0.10);
 border: 1px solid rgba(212, 175, 55, 0.35);
 border-radius: 18px;
 padding: 28px;
 box-shadow: 0 14px 35px rgba(0, 0, 0, 0.35);
 backdrop-filter: blur(4px);
 transition: transform 0.2s ease;
}
.card:hover {

```

```

 transform: translateY(-4px);
 }
 .card h3 {
 color: #9ee7e5;
 margin-top: 0;
 }
 .card p {
 line-height: 1.6;
 color: #e5e7eb;
 }
 footer {
 text-align: center;
 padding: 24px;
 color: #b9c7c7;
 border-top: 1px solid rgba(212, 175, 55, 0.25);
 }
</style>
</head>

<body>
 <header>
 <nav>
 <div class="logo">🗡 Master Sword Publishing</div>
 <div class="nav-link">Capstone Project</div>
 </nav>
 </header>

 <main>
 <section class="hero">
 <div class="sword">🗡</div>
 <h1>Hyrule's #1 Publishing Company</h1>
 <p class="subtitle">
 This internal website was created by Jayce Mangum for
 CSNT253: Capstone Project. This was created to demonstrate deploying a Python
 script to configure a Ubuntu Web Server running Nginx.
 </p>

 <div class="badge">Currently hosted on: MSPUB-LYNEL-WEB01 running
 Ubuntu Server 26.04 with Nginx.</div>
 </section>

 <section class="section">
 <h2>Capstone Project Components</h2>

 <div class="cards">
 <div class="card">
 <h3>A+ Software Essentials & A+ Hardware</h3>
 <p>
 Virtual Machine Home Lab
 </p>
 </div>
 </div>
 </section>
 </main>
</body>
</html>

```

## Part 2: Open-Source OSs & Shells and Scripts: System Configuration & User Management Scripts

```
Windows Server 2025: Domain Controller,
Domain Manager
Ubuntu Server 26.04: Web/App Server
Windows 11: Domain Workstation
Ubuntu Desktop 26.04: Domain
Workstation
macOS 26 Tahoe: Domain Workstation
Kali Linux 2026: Cybersecurirty

</p>
<p>
Troubleshooting Scenarios

Routing & DNS Misconfigurtion
User Account Locked Out
Low Disk Space Issue
Virtual Machine Network Issue

</p>
</div>
<div class="card">
<h3>Shells & Scripts</h3>
<p>
Automated Sysem Configuration Script

Update package repositories
Install Nginx
Install and enable OpenSSH
Configure SFTP support
Configure UFW firewall rules
Allow HTTP, SSH, and SFTP traffic
Create the MSPUB web directory
Create SFTP upload directory
Create publishing group
Deploy a basic internal landing page
Set appropriate file permissions
Enable and start required services
Record actions in a log file
Include basic error handling and
validation

</p>
<p>
User Management Script

Help IT Administrators create/modify/
delete users

```

```

 Create password polices
 Assign groups
 Create/delete home directories

</p>
</div>

<div class="card">
 <h3>Network Fundamentals & Administration</h3>
 <p>
 Networking Components

 Configure a Ubiquiti Router &
 Switches
 Configure Firewall and Access Control
 Lists
 Implement Quality of Service
 priortizing network traffic

 </p>
 <p>
 Wireless Access Points

 Configure WAPs for seamless
 connectivity
 Implement securirty protocols WPA3
 Enterprise

 </p>
</div>
<div class="card">
 <h3>Network Secuirty & Encryption</h3>
 <p>
 Task 1: TBD
 </p>
 <p>
 Task 2: TBD
 </p>
</div>
</div>
</section>
</main>

<footer>
 Created by Jayce Mangum, Spring Quarter 2026, at <a href="https://
www.lwtech.edu/">LWTech.
</footer>
</body>

</html>

```



## User Management Script

### Scenario Overview

The Publishing Department is continuing to grow, and the MSPUB IT Department requires an automated method for managing user accounts on the web server. Administrators currently create accounts manually, which is time-consuming and can lead to configuration inconsistencies. A Python-based user management script will be developed to automate account administration tasks.

### Objective

Develop a Python-based user management utility that simplifies Linux account administration on MSPUB-LYNEL-WEB01. The script will provide administrators with a menu-driven interface for managing users and groups, reducing the potential for configuration errors. The solution will improve efficiency, consistency, and scalability as the organization continues to expand.

### Planned Features

- Install predefined MSPUB department groups
- Create custom Linux groups
- Create new user accounts
- Delete existing user accounts
- Assign users to groups
- Force password changes at next login
- Display existing user accounts
- Log administrative actions
- Verify administrative privileges before execution
- Provide a menu-driven interface for administrators
- Set new user account default password
- Bulk User Import/Delete from CSV file with auto-generated samples

### Systems Used

- MSPUB-LYNEL-WEB01
- MSPUB-UBTSVR-TESTWORLD
- Ubuntu Server 26.04
- Python 3
- Sublime Text
- OpenSSH/SFTP
- Linux File System Permissions
- Linux User Management Utilities
  - useradd
  - userdel
  - usermod
  - groupadd
  - getent
  - chage

### Script Design

The MSPUB User Management System was developed using Python and follows a menu-driven interface. Administrators are presented with a series of options that allow them to manage user accounts, Linux groups, and bulk user operations.

The script utilizes Python's subprocess module to execute Linux administrative commands such as useradd, userdel, groupadd, usermod, chage, and chpasswd. Administrative actions are reordered using a custom logging function which stores activity within a centralized log file for auditing and troubleshooting purposes.

Individual user accounts are automatically generated using a first initial and surname naming convention. Newly created users are assigned a temporary password and are required to change their password upon first login.

To support larger deployments, the script includes CSV-based batch import and batch deletion functionality. Static CSV files are stored with the MSPUB administrative directory and can be edited by administrators prior to execution. During batch operations, the script validates users and groups, automatically creates missing groups when necessary, and records all actions within the activity log.

Major functions:

- check\_root()
- log\_action()
- run\_command()
- create\_default\_groups()
- create\_custom\_group()
- create\_user()
- delete\_user()
- assign\_user\_group()
- force\_password\_change()
- list\_users()
- batch\_user\_import()
- bulk\_delete\_users()
- display\_menu()
- main()

Predefined MSPUB department groups:

- administration
- publishing
- it-cyber
- online-services

Each administrative action will be logged to provide accountability and assist with troubleshooting.

### **Results**

The MSPUB User Management System was successfully developed, tested, and validated within the Ubuntu Server test environment. All planned functionality was implemented and tested successfully before production deployment.

Testing confirmed the following features:

- Installation of MSPUB department groups
- Creation of custom Linux groups
- Individual user account creation
- User deletion
- User-to-group assignment
- Forced password changes
- User account listing
- CSV batch user imports
- CSV bulk user deletions
- Activity logging
- Default password assignment

The script successfully generated user accounts, created and assigned groups, enforced password change policies, and recorded administrative actions within the system log. Batch operations were able to create and remove multiple user accounts using administrator-maintained CSV files. Testing verified that existing users were skipped appropriately and missing users were handled gracefully during deletion operations.

Overall, the project met all design objectives and provides a functional administrative tool that can be used within both the MSPUB capstone environment and future Linux deployments.

**Main Menu:**

```
mspubadmin@mspub-test-ubtsrv:~/scripts/usragat$ sudo python3 mspub-usermgmt_v2.py
[[sudo: authenticate] Password:

<=====>
| | /\
| | MSPUB USER MANAGEMENT SYSTEM /_/\
| | /__V__\
<=====>

Options:

1. Install MSPUB Department Groups
2. Create Custom Group
3. Create New User
4. Delete Existing User
5. Assign User to Group
6. Force Password Change
7. List Users
8. Bulk User Import from CSV
9. Bulk User Deletion from CSV

X. Exit

[Select an option: 8
```

## Bulk User Add & Deletion Feature

```
Bulk User Import

CSV file location: /opt/asgpub-usragat/batch-usr-iaport.csv

Instructions:
1. Open the CSV file in a text editor.
2. Add one user per line using this format:
 first_name,last_name,group_name
 per the HSPUB naming convention for usernames first_name = first initial dot last_name = full last name. E.g. p.sheikh
3. Save the CSV file before continuing.
4. Existing users will be skipped.
5. Missing groups will be created automatically.
/nCSV file Example:
r.sheikh,lt-cyber
l.hero,lt-cyber
z.princess,administration

Ready to begin the import? n
[atsd IMPORT] 6/10681168
```

```
Bulk User Deletion

CSV file location: /opt/mspub-usrmgmt/bulk-usr-delete.csv

Instructions:
1. Open the CSV file in a text editor.
2. Add one user per line using this format:
 username
3. Save the CSV file before continuing.
4. User listed in the file will be deleted with their home directories.

Example:
 z.princess
 i.sheikah

[Are you sure you want to delete all users listed in this file? (y/n): n
Bulk user deletion cancelled.
```

## Script Log

```

[mspubadmin@mspub-test-ubtsrv:~/scripts/usrmgmt$ cat /var/log/mspub_user_mgmt.log
[2026-05-31 07:13:44] Root privilege check passed.
[2026-05-31 07:15:01] SUCCESS: groupadd administration
[2026-05-31 07:15:01] Created group: administration
[2026-05-31 07:15:01] Group already exists: publishing
[2026-05-31 07:15:01] SUCCESS: groupadd it-cyber
[2026-05-31 07:15:01] Created group: it-cyber
[2026-05-31 07:15:01] SUCCESS: groupadd online-services
[2026-05-31 07:15:01] Created group: online-services
[2026-05-31 07:15:24] SUCCESS: groupadd test-group
[2026-05-31 07:15:24] Created custom group: test-group
[2026-05-31 07:15:57] SUCCESS: useradd -m -s /bin/bash -G test-group j.mangum
[2026-05-31 07:15:57] Created user j.mangum and assigned to group test-group
[2026-05-31 07:15:57] SUCCESS: echo 'j.mangum:Hyrul3Warr10r$' | chpasswd
[2026-05-31 07:15:57] MSPUB default password assigned to j.mangum
[2026-05-31 07:15:57] SUCCESS: chage -d 0 j.mangum
[2026-05-31 07:15:57] Forced password change at next login for j.mangum
[2026-05-31 07:17:05] Group assignment failed. User does not exist: it-cyber
[2026-05-31 07:17:30] SUCCESS: usermod -aG it-cyber j.mangum
[2026-05-31 07:17:30] Added j.mangum to group it-cyber
[2026-05-31 07:18:01] SUCCESS: chage -d 0 j.mangum
[2026-05-31 07:18:01] Forced password change for j.mangum
[2026-05-31 07:18:13] Displayed user list.
[2026-05-31 07:18:29] Exited MSPUB User Management System.
[2026-05-31 07:21:23] Root privilege check passed.
[2026-05-31 07:21:35] SUCCESS: userdel -r j.mangum
[2026-05-31 07:21:35] Deleted user: j.mangum
[2026-05-31 07:21:42] Displayed user list.
[2026-05-31 07:21:50] Exited MSPUB User Management System.
[2026-05-31 07:33:42] Root privilege check passed.
[2026-05-31 07:34:00] SUCCESS: useradd -m -s /bin/bash -G test-group j.mangum
[2026-05-31 07:34:00] Created user j.mangum and assigned to group test-group
[2026-05-31 07:34:00] MSPUB default password assigned to j.mangum
[2026-05-31 07:34:00] SUCCESS: chage -d 0 j.mangum
[2026-05-31 07:34:00] Forced password change at next login for j.mangum
[2026-05-31 07:34:12] Exited MSPUB User Management System.
[2026-05-31 21:02:28] Root privilege check passed.
[2026-05-31 21:03:08] SUCCESS: mkdir -p ./scripts/usrmgmt/
[2026-05-31 21:07:08] Root privilege check passed.
[2026-05-31 21:07:12] SUCCESS: mkdir -p /opt/mspub-usrmgmt/
[2026-05-31 21:07:12] SUCCESS: chmod 664 /opt/mspub-usrmgmt/batch-usr-import.csv
[2026-05-31 21:07:12] Created sample batch import CSV file: /opt/mspub-usrmgmt/batch-usr-import.csv
[2026-05-31 21:07:28] Batch import cancelled by administrator.
[2026-05-31 21:07:31] Exited MSPUB User Management System.
[2026-05-31 21:08:23] Root privilege check passed.
[2026-05-31 21:08:32] SUCCESS: useradd -m -s /bin/bash -G publishing l.hero
[2026-05-31 21:08:32] Batch import assigned default password to l.hero
[2026-05-31 21:08:32] SUCCESS: chage -d 0 l.hero
[2026-05-31 21:08:32] Batch import created user l.hero in group publishing. Default password set. Change password next logon: TRUE
[2026-05-31 21:08:32] SUCCESS: useradd -m -s /bin/bash -G administration z.princess
[2026-05-31 21:08:32] Batch import assigned default password to z.princess
[2026-05-31 21:08:32] SUCCESS: chage -d 0 z.princess
[2026-05-31 21:08:32] Batch import created user z.princess in group administration. Default password set. Change password next logon: TRUE
[2026-05-31 21:08:32] SUCCESS: useradd -m -s /bin/bash -G publishing s.zora
[2026-05-31 21:08:32] Batch import assigned default password to s.zora
[2026-05-31 21:08:32] SUCCESS: chage -d 0 s.zora
[2026-05-31 21:08:32] Batch import created user s.zora in group publishing. Default password set. Change password next logon: TRUE
[2026-05-31 21:08:32] Batch user import completed.
[2026-05-31 21:09:14] Exited MSPUB User Management System.
[2026-05-31 21:10:34] Root privilege check passed.
[2026-05-31 21:10:42] Displayed user list.
[2026-05-31 21:10:56] SUCCESS: chmod 644 /opt/mspub-usrmgmt/bulk-usr-delete.csv
[2026-05-31 21:10:56] Created sample batch removal CSV file: /opt/mspub-usrmgmt/bulk-usr-delete.csv
[2026-05-31 21:11:01] Bulk user deletion cancelled by administrator.
[2026-05-31 21:11:02] Exited MSPUB User Management System.
[2026-05-31 21:13:11] Root privilege check passed.
[2026-05-31 21:13:18] SUCCESS: userdel -r z.princess
[2026-05-31 21:13:18] Bulk delete removed user: z.princess
[2026-05-31 21:13:18] Bulk delete skipped missing user: i.sheikah
[2026-05-31 21:13:18] Bulk delete skipped missing user: p.sheikah
[2026-05-31 21:13:18] Bulk user deletion completed.
[2026-05-31 21:13:51] Displayed user list.
[2026-05-31 21:13:58] Exited MSPUB User Management System.
[2026-05-31 21:43:44] Root privilege check passed.
[2026-05-31 21:44:02] Batch import cancelled by administrator.
[2026-05-31 21:44:09] Bulk user deletion cancelled by administrator.
[2026-05-31 21:45:41] Exited MSPUB User Management System.
mspubadmin@mspub-test-ubtsrv:~/scripts/usrmgmt$

```

## Challenges Encountered

Several challenges were encountered during the developmental and testing phases of the MSPUB User Management System. The most common issue involved Python syntax and indentation errors. Because Python relies heavily on proper indentation, several debugging sessions were required to correct improperly aligned code blocks and nested functions. Additional syntax errors were encountered involving missing commas, unterminated triple-quoted strings, and incorrectly formatted function calls.

```

UserCreationMenu -- -zsh -- 80x24

Last login: Sat May 30 18:08:56 on ttye000
[jmangum@OINRAAL ~ % cd /Volumes/CSNT-CAPPJ/Scenario/ Documents/Part02-LinuxScrip
ts/Scripts/UserCreationMenu
jmangum@OINRAAL UserCreationMenu % python3 -m py_compile mspub-usermgmt_v1.py
File "mspub-usermgmt_v1.py", line 292
 print(r"""
 ^
SyntaxError: unterminated triple-quoted string literal (detected at line 341)
[jmangum@OINRAAL UserCreationMenu % python3 -m py_compile mspub-usermgmt_v1.py
File "mspub-usermgmt_v1.py", line 251
 stdout=subprocess.DEVNULL
 ^^^^^^^^^^^^^^^^^^^^^^^
SyntaxError: invalid syntax. Perhaps you forgot a comma?
[jmangum@OINRAAL UserCreationMenu % python3 -m py_compile mspub-usermgmt_v1.py
File "mspub-usermgmt_v1.py", line 285
 except Exception as error:
 ^^^^^
SyntaxError: invalid syntax
[jmangum@OINRAAL UserCreationMenu % python3 -m py_compile mspub-usermgmt_v1.py
jmangum@OINRAAL UserCreationMenu %

```

```

[aspubadmin@aspub-test-ubtsrv:~/scripts/usrmgmt$ sudo python3 mspub-usermgmt_v1.py
Traceback (most recent call last):
 File "/home/aspubadmin/scripts/usrmgmt/mspub-usermgmt_v1.py", line 341, in <module>
 main()
 ^^
 File "/home/aspubadmin/scripts/usrmgmt/mspub-usermgmt_v1.py", line 313, in main
 check_root()
 File "/home/aspubadmin/scripts/usrmgmt/mspub-usermgmt_v1.py", line 16, in check_root
 log_action("Root privilege check passed.")
 ^^^
 File "/home/aspubadmin/scripts/usrmgmt/mspub-usermgmt_v1.py", line 24, in log_action
 log.write(f"[[timestamp]] {message}\n")
 ^^^^^^^^^
NameError: name 'timestamp' is not defined. Did you mean: 'timestamp'?
aspubadmin@aspub-test-ubtsrv:~/scripts/usrmgmt$

```

Another challenge involved the implementation of a default password assignment. The original solution used shell piping through the `chpasswd` command; however, special characters contained within the default password caused inconsistent results during testing. The issue was resolved by replacing shell-based password assignment with Python's `subprocess.run()` function, which passes credentials directly to `chpasswd` and eliminates shell interpretation issues.

```

Exiting MSPUB User Management System.
[aspubadmin@aspub-test-ubtsrv:~/scripts/usrmgmt$ su j.mangum
[Password:
su: Authentication failure
[aspubadmin@aspub-test-ubtsrv:~/scripts/usrmgmt$ su j.mangum
[Password:
su: Authentication failure
[aspubadmin@aspub-test-ubtsrv:~/scripts/usrmgmt$ sudo passwd j.mangum
[New password:
[Retype new password:
passwd: password updated successfully
[aspubadmin@aspub-test-ubtsrv:~/scripts/usrmgmt$ su j.mangum
[Password:
[j.mangum@aspub-test-ubtsrv:/home/aspubadmin/scripts/usrmgmt$ exit
exit

```

|                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> 150 151     default_passwd = "Hyrule3Warr10r\$" 152 153     run_command( 154         f'echo '{username}:{default_passwd}'   chpasswd' 155     ) 156 157     log_action(f"MSPUB default password assigned to {username}") 158 </pre> | <pre> 156 157     password_process = subprocess.run( 158         ["chpasswd"], 159         input=f'{username}:{DEFAULT_PASSWORD}\n', 160         text=True, 161         capture_output=True 162     ) 163 164     if password_process.returncode == 0: 165         log_action(f"MSPUB default password assigned to {username}") </pre> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Additional testing identified file path and directory creation issues related to CSV bulk import and bulk deletion features. These issues were resolved by implementing automatic directory creation and sample CSV generation when required files were not present.

```

10 IMPORT_CSV_FILE = "/opt/mspub-usrmgmt/batch-usr-import.csv"
11 REMOVE_CSV_FILE = "/opt/mspub-usrmgmt/bulk-usr-delete.csv"

```

```

208
209 def prepare_batch_csv_file():
210 """Create the batch import CSV file if it does not already exist"""
211
212 csv_dir = "/opt/mspub-usrmgmt/"
213
214 if not os.path.exists(csv_dir):
215 run_command(f"mkdir -p {csv_dir}")
216
217 if not os.path.exists(IMPORT_CSV_FILE):
218 sample_content = """first_name,last_name,group_name
219 l,hero,publishing
220 z,princess,administration
221 s,zora,publishing
222 """
223
224 with open(IMPORT_CSV_FILE, "w") as file:
225 file.write(sample_content)
226
227 run_command(f"chmod 644 {IMPORT_CSV_FILE}")
228 log_action(f"Created sample batch import CSV file: {IMPORT_CSV_FILE}")
229

```

```

408
409 def prepare_remove_csv_file():
410 """Create the batch user removal CSV file if it does not already exist."""
411
412 csv_dir = "/opt/mspub-usrmgmt/"
413
414 if not os.path.exists(csv_dir):
415 run_command(f"mkdir -p {csv_dir}")
416
417 if not os.path.exists(REMOVE_CSV_FILE):
418 sample_content = """username
419 z,princess
420 i,sheikah
421 p,sheikah
422 """
423
424 with open(REMOVE_CSV_FILE, "w") as file:
425 file.write(sample_content)
426
427 run_command(f"chmod 644 {REMOVE_CSV_FILE}")
428 log_action(f"Created sample batch removal CSV file: {REMOVE_CSV_FILE}")
429

```

### mspub-usermgmt v2.py Source Code

[Download mspub-usermgmt v2.py](#)

[Download example batch usr import.csv](#)

[Download example bulk usr delete.csv](#)

```
#!/usr/bin/env python3
```

```

import os
import subprocess
import csv
from datetime import datetime

```

```

LOG_FILE = "/var/log/mspub_user_mgmt.log"
DEFAULT_PASSWORD = "Hyru13Warr10r$"
IMPORT_CSV_FILE = "/opt/mspub-usrmgmt/batch-usr-import.csv"
REMOVE_CSV_FILE = "/opt/mspub-usrmgmt/bulk-usr-delete.csv"

```

```

def check_root():
 """Verify the script is running with root privileges."""
 if os.geteuid() != 0:
 print("The MSPUB User Management Script must be run with sudo
privileges.")
 exit(1)

```

```
 log_action("Root privilege check passed.")
```

```

def log_action(message):
 """Write script activity to the log file."""
 timestamp = datetime.now().strftime("%Y-%m-%d %H:%M:%S")

 with open(LOG_FILE, "a") as log:
 log.write(f"[{timestamp}] {message}\n")

```

```

def run_command(command):
 """Run a Linux command and log success or failure."""

```

```

try:
 result = subprocess.run(
 command,
 shell=True,
 check=True,
 text=True,
 capture_output=True
)

 log_action(f"SUCCESS: {command}")
 return result.stdout

except subprocess.CalledProcessError as error:
 log_action(f"ERROR: {command}")
 log_action(error.stderr)
 print(f"Command failed: {command}")
 print(error.stderr)
 return None

Group Creation
def install_default_groups():
 """Create the default MSPUB department groups."""
 print("\nInstalling MSPUB department groups...")

 groups = [
 "administration",
 "publishing",
 "it-cyber",
 "online-services"
]

 for group in groups:
 group_exists = subprocess.run(
 f"getent group {group}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if group_exists.returncode == 0:
 print(f"Group already exists: {group}")
 log_action(f"Group already exists: {group}")
 else:
 run_command(f"groupadd {group}")
 print(f"Created group: {group}")
 log_action(f"Created group: {group}")

 print("MSPUB department groups installation complete.")

```



```

def create_custom_group():
 """Create a custom Linux group."""
 group_name = input("\nEnter custom group name: ").strip().lower()

 if not group_name:
 print("Group name cannot be blank.")
 return

 group_exists = subprocess.run(
 f"getent group {group_name}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if group_exists.returncode == 0:
 print(f"Group already exists: {group_name}")
 log_action(f"Group already exists: {group_name}")
 else:
 run_command(f"groupadd {group_name}")
 print(f"Created custom group: {group_name}")
 log_action(f"Created custom group: {group_name}")

User Creation
def create_user():
 """Create a new Linux user account and optionally assign group."""
 first_name = input("\nEnter employee first name initial: ").strip().lower()
 last_name = input("Enter employee full last name: ").strip().lower()
 group_name = input("Enter MSPUB group name for this user: ").strip().lower()

 if not first_name or not last_name:
 print("First name and last name cannot be blank.")
 return

 username = f"{first_name}.{last_name}"

 user_exists = subprocess.run(
 f"id {username}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if user_exists.returncode == 0:
 print(f"User already exists: {username}")
 log_action(f"User already exists: {username}")
 return

 if group_name:
 group_exists = subprocess.run(

```

```

 f"getent group {group_name}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if group_exists.returncode != 0:
 print(f"Group does not exist: {group_name}")
 create_group = input("Create this group now? (y/n):
").strip().lower()

 if create_group == "y":
 run_command(f"groupadd {group_name}")
 log_action(f"Created group during user creation: {group_name}")
 else:
 print("User creation cancelled.")
 return

 run_command(f"useradd -m -s /bin/bash -G {group_name} {username}")
 log_action(f"Created user {username} and assigned to group {group_name}")
else:
 run_command(f"useradd -m -s /bin/bash {username}")
 log_action(f"Created user {username} without group assignment")

password_process = subprocess.run(
 ["chpasswd"],
 input=f"{username}:{DEFAULT_PASSWORD}\n",
 text=True,
 capture_output=True
)

if password_process.returncode == 0:
 log_action(f"MSPUB default password assigned to {username}")
else:
 log_action(f"Password assignment failed for {username}:
{password_process.stderr}")
 print(f"Password assignment failed for {username}.")
 print(password_process.stderr)

run_command(f"chage -d 0 {username}")
log_action(f"Forced password change at next login for {username}")

print(f"User created successfully: {username}")
print(f"Temporary password: {DEFAULT_PASSWORD}")

def delete_user():
 """Delete an existing Linux user account."""
 username = input("\nEnter username to delete: ").strip().lower()

 if not username:

```

```

 print("Username cannot be blank.")
 return

 user_exists = subprocess.run(
 f"id {username}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if user_exists.returncode != 0:
 print(f"User does not exist: {username}")
 log_action(f"Delete failed. User does not exist: {username}")
 return

 confirm = input(f"Are you sure you want to delete {username}? (y/n):")
 confirm = confirm.strip().lower()

 if confirm == "y":
 run_command(f"userdel -r {username}")
 print(f"Deleted user: {username}")
 log_action(f"Deleted user: {username}")
 else:
 print("User deletion cancelled.")
 log_action(f"User deletion cancelled for {username}")

def prepare_batch_csv_file():
 """Create the batch import CSV file if it does not already exist"""

 csv_dir = "/opt/mspub-usrmgmt/"

 if not os.path.exists(csv_dir):
 run_command(f"mkdir -p {csv_dir}")

 if not os.path.exists(IMPORT_CSV_FILE):
 sample_content = """first_name,last_name,group_name
l,hero,publishing
z,princess,administration
s,zora,publishing
"""

 with open(IMPORT_CSV_FILE, "w") as file:
 file.write(sample_content)

 run_command(f"chmod 664 {IMPORT_CSV_FILE}")
 log_action(f"Created sample batch import CSV file:
{IMPORT_CSV_FILE}")

def batch_user_import():
 """Create multiple users from a static CSV file."""

```

```

prepare_batch_csv_file()

print("\nBulk User Import")
print("-" * 40)
print(f"CSV file location: {IMPORT_CSV_FILE}")
print("\nInstructions:")
print("1. Open the CSV file in a text editor.")
print("2. Add one user per line using this format: ")
print(" first_name,last_name,group_name")
print(" per the MSPUB naming convention for usernames first_name =")
first_initial_dot_last_name = full_last_name. E.g. p.sheikah")
print("3. Save the CSV file before continuing.")
print("4. Existing users will be skipped.")
print("5. Missing groups will be created automatically.")
print("/nCSV file Example:")
print(" r,sheikah,it-cyber")
print(" l,hero,it-cyber")
print(" z,princess,administration")

confirm = input("\nReady to begin the import? ").strip().lower()

if confirm != "y":
 print("Batch import cancelled.")
 log_action("Batch import cancelled by administrator.")
 return

with open(IMPORT_CSV_FILE, "r") as csv_file:
 reader = csv.DictReader(csv_file)

 for row in reader:
 first_name = row["first_name"].strip().lower()
 last_name = row["last_name"].strip().lower()
 group_name = row["group_name"].strip().lower()

 if not first_name or not last_name or not group_name:
 log_action("Batch import skipped incomplete row.")
 continue

 username = f"{first_name}.{last_name}"

 user_exists = subprocess.run(
 f"id {username}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if user_exists.returncode == 0:
 print(f"User already exists, skipped: {username}")
 log_action(f"Batch import skipped existing user: {username}")

```

```

 continue

 group_exists = subprocess.run(
 f"getent group {group_name}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if group_exists.returncode != 0:
 run_command(f"groupadd {group_name}")
 log_action(f"Batch import created group: {group_name}")

 run_command(f"useradd -m -s /bin/bash -G {group_name} {username}")

 password_process = subprocess.run(
 ["chpasswd"],
 input=f"{username}:{DEFAULT_PASSWORD}\n",
 text=True,
 capture_output=True
)

 if password_process.returncode == 0:
 log_action(f"Batch import assigned default password to
{username}")
 else:
 log_action(f"Batch import password assignment failed for
{username}: {password_process.stderr}")
 print(f"Password assignment failed for {username}")

 run_command(f"chage -d 0 {username}")

 print(f"Created user: {username}")
 log_action(f"Batch import created user {username} in group
{group_name}. Default password set. Change password next logon: TRUE")

 print("Batch user import completed.")
 log_action("Batch user import completed.")

Assignment
def assign_user_group():
 """Assign an existing user to an existing group."""
 username = input("\nEnter username: ").strip().lower()
 group_name = input("Enter group name: ").strip().lower()

 if not username or not group_name:
 print("Username and group name cannot be blank.")
 return

 user_exists = subprocess.run(
 f"id {username}",

```

```

 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if user_exists.returncode != 0:
 print(f"User does not exist: {username}")
 log_action(f"Group assignment failed. User does not exist: {username}")
 return

 group_exists = subprocess.run(
 f"getent group {group_name}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if group_exists.returncode != 0:
 print(f"Group does not exist: {group_name}")
 log_action(f"Group assignment failed. Group does not exist:
{group_name}")
 return

 run_command(f"usermod -aG {group_name} {username}")

 print(f"Added {username} to {group_name}")
 log_action(f"Added {username} to group {group_name}")

def force_password_change():
 """Force a user to change their password at next login."""
 username = input("\nEnter username: ").strip().lower()

 if not username:
 print("Username cannot be blank.")
 return

 user_exists = subprocess.run(
 f"id {username}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if user_exists.returncode != 0:
 print(f"User does not exist: {username}")
 log_action(f"Password reset failed. User does not exist: {username}")
 return

 run_command(f"chage -d 0 {username}")

```

```

print(f"Password change required for {username}")
log_action(f"Forced password change for {username}")

Other Features
def list_users():
 """Display local users with home directories."""
 print("\nMSPUB User Accounts")
 print("-" * 40)

 try:
 with open("/etc/passwd", "r") as passwd_file:
 for line in passwd_file:
 fields = line.split(":")

 username = fields[0]
 uid = int(fields[2])
 home = fields[5]

 if uid >= 1000 and home.startswith("/home"):
 print(username)

 log_action("Displayed user list.")

 except Exception as error:
 print(f"Error displaying users: {error}")
 log_action(f"Error displaying users: {error}")

def prepare_remove_csv_file():
 """Create the batch user removal CSV file if it does not already exist."""

 csv_dir = "/opt/mspub-usrmgmt/"

 if not os.path.exists(csv_dir):
 run_command(f"mkdir -p {csv_dir}")

 if not os.path.exists(REMOVE_CSV_FILE):
 sample_content = """username
z.princess
i.sheikah
p.sheikah
"""

 with open(REMOVE_CSV_FILE, "w") as file:
 file.write(sample_content)

 run_command(f"chmod 644 {REMOVE_CSV_FILE}")
 log_action(f"Created sample batch removal CSV file: {REMOVE_CSV_FILE}")

def bulk_delete_users():
 """Delete multiple users from a static CSC file."""

```



```

prepare_remove_csv_file()

print("\nBulk User Deletion")
print("-" * 40)
print(f"CSV file location: {REMOVE_CSV_FILE}")
print("\nInstructions:")
print("1. Open the CSV file in a text editor.")
print("2. Add one user per line using this format:")
print(" username")
print("3. Save the CSV file before continuing.")
print("4. User listed in the file will be deleted with their home
directories.")
print("\nExample:")
print(" z.princess")
print(" i.sheikah")

confirm = input("\nAre you sure you want to delete all users listed in this
file? (y/n): ").strip().lower()

if confirm != "y":
 print("Bulk user deletion cancelled.")
 log_action("Bulk user deletion cancelled by administrator.")
 return

with open(REMOVE_CSV_FILE, "r") as csv_file:
 reader = csv.DictReader(csv_file)

 for row in reader:
 username = row["username"].strip().lower()

 if not username:
 log_action("Bulk delete skipped blank username row.")
 continue

 user_exists = subprocess.run(
 f"id {username}",
 shell=True,
 stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL
)

 if user_exists.returncode != 0:
 print(f"User does not exist, skipped: {username}")
 log_action(f"Bulk delete skipped missing user: {username}")
 continue

 run_command(f"userdel -r {username}")
 log_action(f"Bulk delete removed user: {username}")

print("Bulk user deletion completed.")
print("Returning to main menu.")

```

```

log_action("Bulk user deletion completed.")

Menu
def display_menu():
 print(r"""
<=====>
| | /\
| | MSPUB USER MANAGEMENT SYSTEM /__\
| | /_\/_\

<=====>

Options:

1. Install MSPUB Department Groups
2. Create Custom Group
3. Create New User
4. Delete Existing User
5. Assign User to Group
6. Force Password Change
7. List Users
8. Bulk User Import from CSV
9. Bulk User Deletion from CSV

X. Exit
""")

def main():
 check_root()

 while True:
 display_menu()
 choice = input("Select an option: ").strip().lower()

 if choice == "1":
 install_default_groups()
 elif choice == "2":
 create_custom_group()
 elif choice == "3":
 create_user()
 elif choice == "4":
 delete_user()
 elif choice == "5":
 assign_user_group()
 elif choice == "6":
 force_password_change()
 elif choice == "7":
 list_users()
 elif choice == "8":
 batch_user_import()
 elif choice == "9":

```

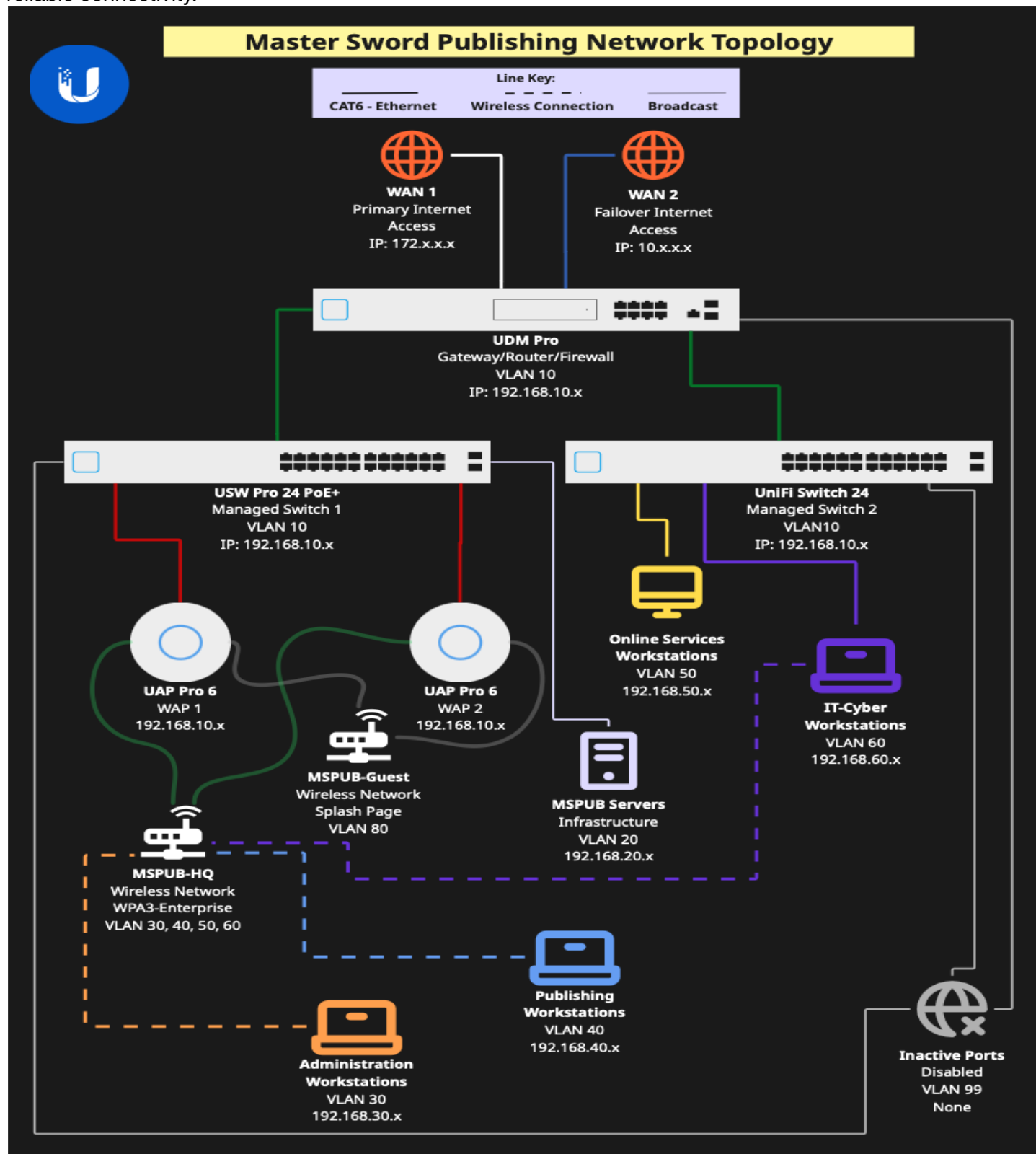
```
 bulk_delete_users()
 elif choice == "x":
 print("Exiting MSPUB User Management System.")
 log_action("Exited MSPUB User Management System.")
 break
 else:
 print("Invalid option. Please enter a valid option.")

if __name__ == "__main__":
 main()
```

# Master Sword Publishing Network Hardware Configuration

## Network Overview

Master Sword Publishing is expanding its office infrastructure and requires a segmented network architecture capable of supporting multiple departments and wireless clients. The IT Department will deploy a Ubiquiti UniFi-based network consisting of a router, managed switch, and wireless access point to provide secure and reliable connectivity.



## Configuring UniFi Routers and Switches

### Scenario Overview

Master Sword Publishing is expanding its office infrastructure and requires a segmented network capable of supporting multiple departments, servers, and internet connectivity. The existing flat network presents security and management challenges because all devices reside on the same broadcast domain. The MSPUB IT Department will deploy a UniFi-based routing and switching solution utilizing VLANs, DHCP services, and redundant WAN connectivity to improve performance, scalability, and network organization.

### Objective

Configure the UDM Pro, managed switches, VLANs, and dual-WAN connectivity to create a secure and scalable network infrastructure capable of supporting multiple business department and server resources.

### Equipment Being Used

- UniFi Dream Machine Pro (UDMP)
  - Gateway, Router, Firewall
- UniFi Switch Pro 24-Port PoE+ (USW24)
  - Managed Switch
- UniFi Switch 24 (USW24)
  - Managed Switch
- UniFi OS Dashboard
  - Web Portal GUI

### VLANs to Implement Table

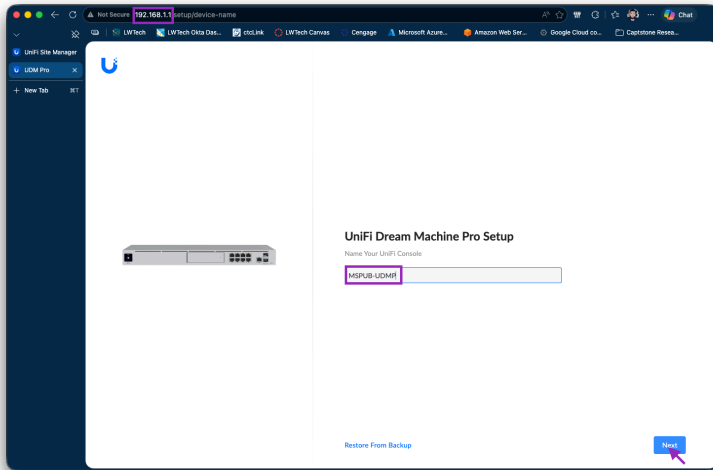
| Purpose                  | Infrastructure              | Servers                     | Administration              | Publishing                  | Online Services             | IT-Cyber                     | Guest Network              | Blackhole (Disabled Ports) |
|--------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|------------------------------|----------------------------|----------------------------|
| Minimum Host Requirement | 5                           | 3                           | 2                           | 4                           | 1                           | 4                            | 254                        | 0                          |
| CIDR                     | 192.168.10.0 /29            | 192.168.20.0 /29            | 192.168.30.0 /29            | 192.168.40.0 /29            | 192.168.50.0 /30            | 192.168.60.0/28              | 192.168.80.0 /24           | No DHCP                    |
| Gateway                  | 192.168.10.1                | 192.168.20.1                | 192.168.30.1                | 192.168.40.1                | 192.168.50.1                | 192.168.60.1                 | 192.168.80.1               | None                       |
| Mask                     | 255.255.255.248             | 255.255.255.248             | 255.255.255.248             | 255.255.255.248             | 255.255.255.252             | 255.255.255.240              | 255.255.255.0              | N/A                        |
| IP Address Range         | 192.168.10.2 - 192.168.10.6 | 192.168.20.2 - 192.168.20.6 | 192.168.30.2 - 192.168.30.6 | 192.168.40.2 - 192.168.40.6 | 192.168.50.2 - 192.168.50.2 | 192.168.60.2 - 192.168.60.14 | 192.168.80.2 - 192.168.254 | N/A                        |
| Broadcast                | 192.168.10.7                | 192.168.20.7                | 192.168.20.7                | 192.168.40.7                | 192.168.50.3                | 192.168.60.15                | 192.168.80.255             | None                       |
| Usable Hosts             | 6                           | 6                           | 6                           | 6                           | 2                           | 10                           | 254                        | 0                          |
| VLAN ID                  | 10                          | 20                          | 30                          | 40                          | 50                          | 60                           | 80                         | 255                        |

### UniFi Dream Machine Pro Out-of-Box Setup

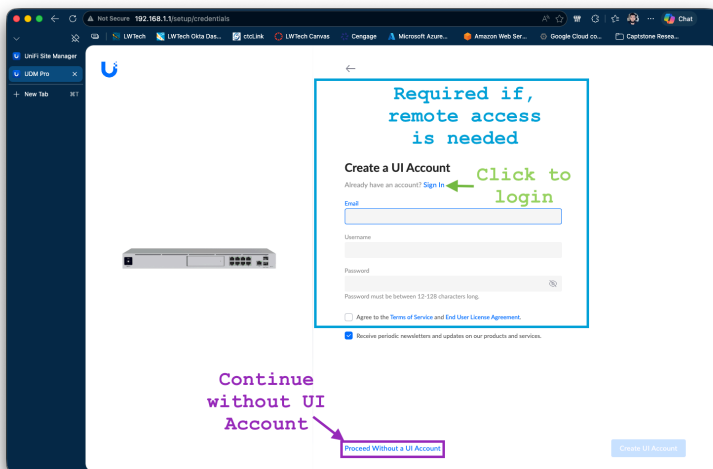
This process will demonstrate the out-of-box setup of the UniFi Dream Machine Pro (UDMP).

1. In a web browser type “192.168.1.1” into the address bar. After a short animation the Setup Wizard will begin. In the Name Your UniFi Console field type “MSPUB-UDMP” then click “Next.”

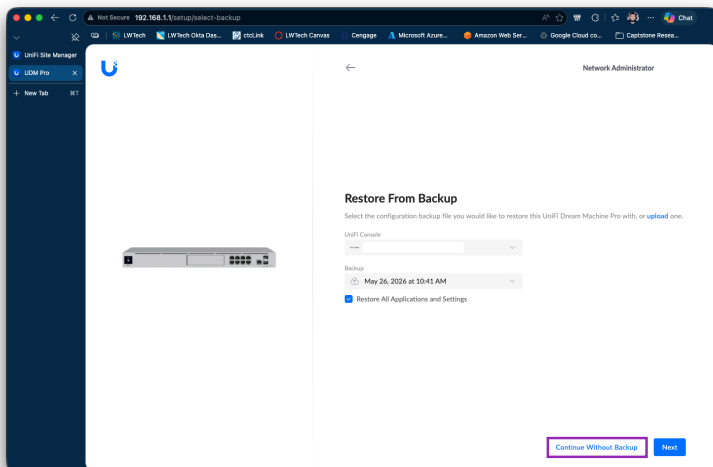
## Part 3: Network Fundamentals & Administration



2. For this lab I will be adding it to my personal UI Account for remote access purposes. Sign in, if there is one associated with the business, create one if required. Otherwise, click “Proceed Without a UI Account.”

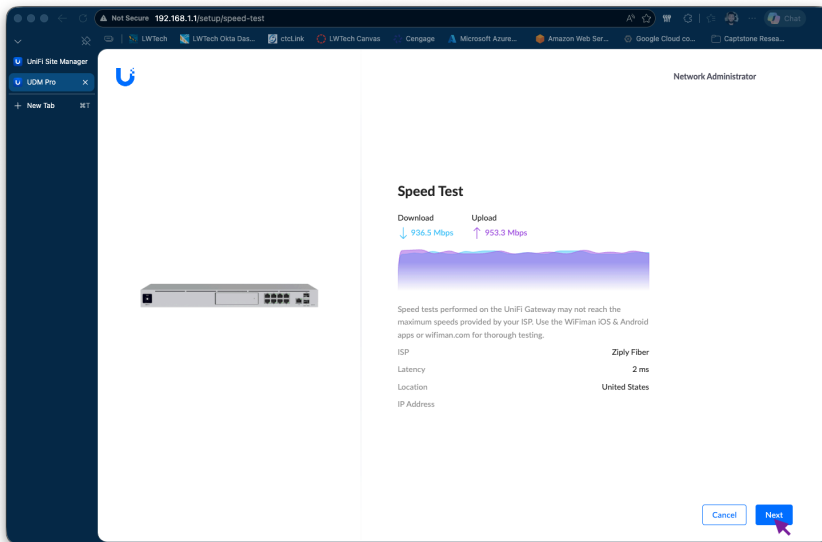


3. If restoring from a backup upload the file, or if there is UI Cloud back choose the console and backup to restore from, make sure “Restore All Applications and Settings are applied. For this lab click “Continue Without Backup” to configure a new device.

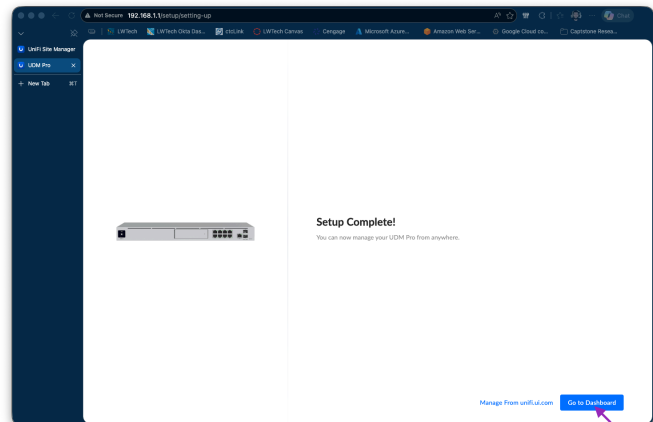
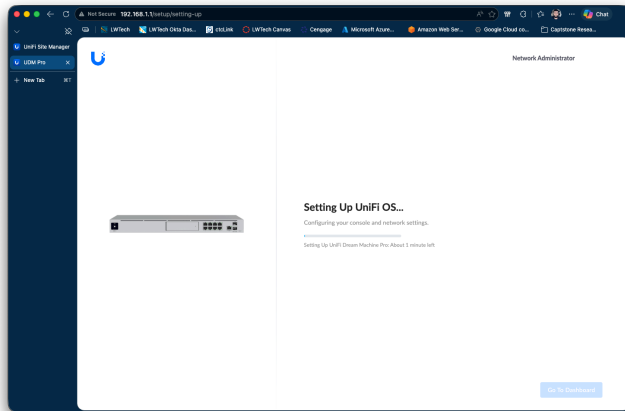


## Part 3: Network Fundamentals & Administration

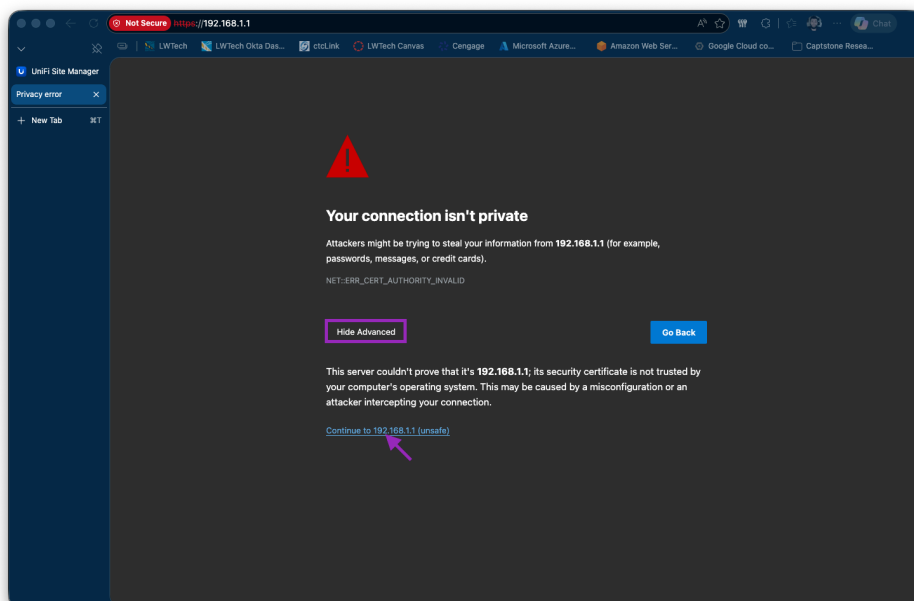
4. An ISP Speed Test will begin, which will detect the upload and download speeds the UDMP is receiving, as well as detect the ISP and Public IP Address. Click “Next” once completed.



5. The UDMP will finish setting up. Once it completes, click “Go to Dashboard.”

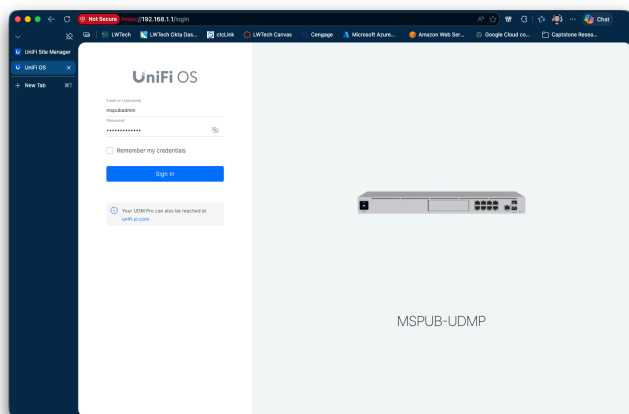


6. If a Your connection isn't private page is displayed click “Advanced” and select “Continue to 192.168.1.1 (unsafe).”

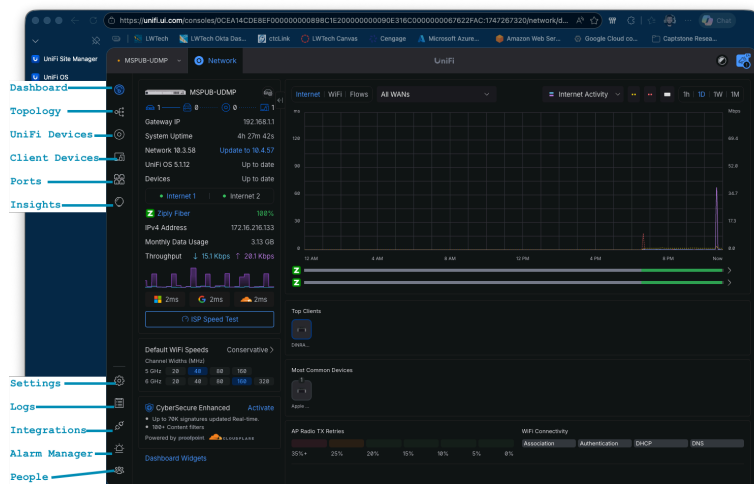


## Part 3: Network Fundamentals & Administration

7. Login with the login credentials either created during the setup process, or your existing UI Account credentials.



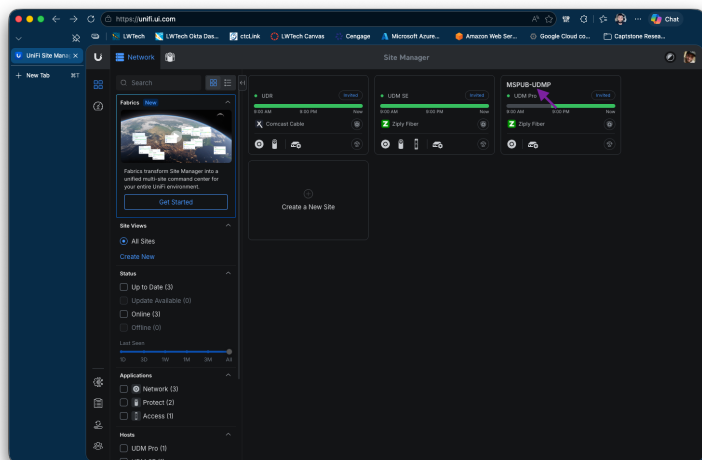
8. This is the main Dashboard which shows live network traffic, device statuses, the most active client devices as well as wifi information. The toolbar on the left is the main navigation to configure the network.



## Adopting UniFi Switches

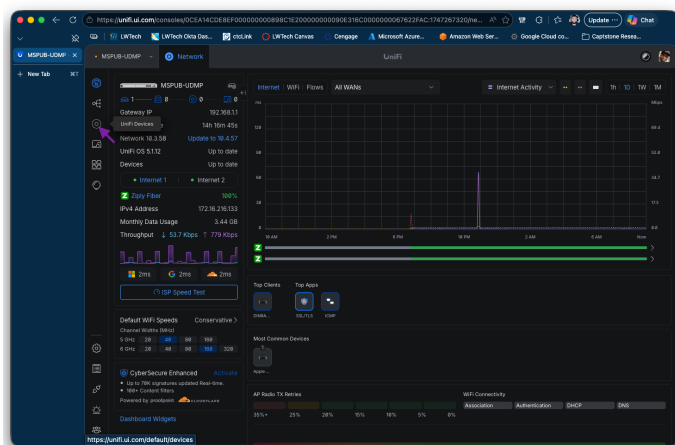
UniFi devices need to be assigned to a UniFi Gateway, CloudKey, Router, or Dream Machine. This is called Adopting, which will add the devices to the network, so they can be configured.

1. If managing multiple UniFi networks, you will see the Site Manager when logging into your UniFi account. In Site Manager click the “MSPUB-UDMP” tile.

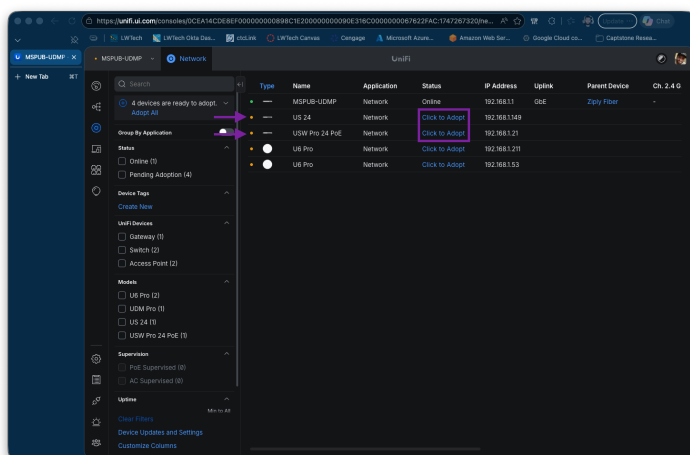




- From the Dashboard, on the toolbar to the left click “UniFi Devices.”



- The UniFi Devices page shows only details about the network hardware on the network. Green indicators mean the device has been adopted. Amber means the device is pending adoption or there's an update to the firmware. Red means there's a critical issue or the device is offline. There are two switches that need to be adopted. Click on “Click to Adopt” to the right of “US 24” and “USW Pro 24 PoE” under the Status column. Ignore the two access points for now. The status will change to Adopting or Process bar, initializing the device. This may take a few minutes.

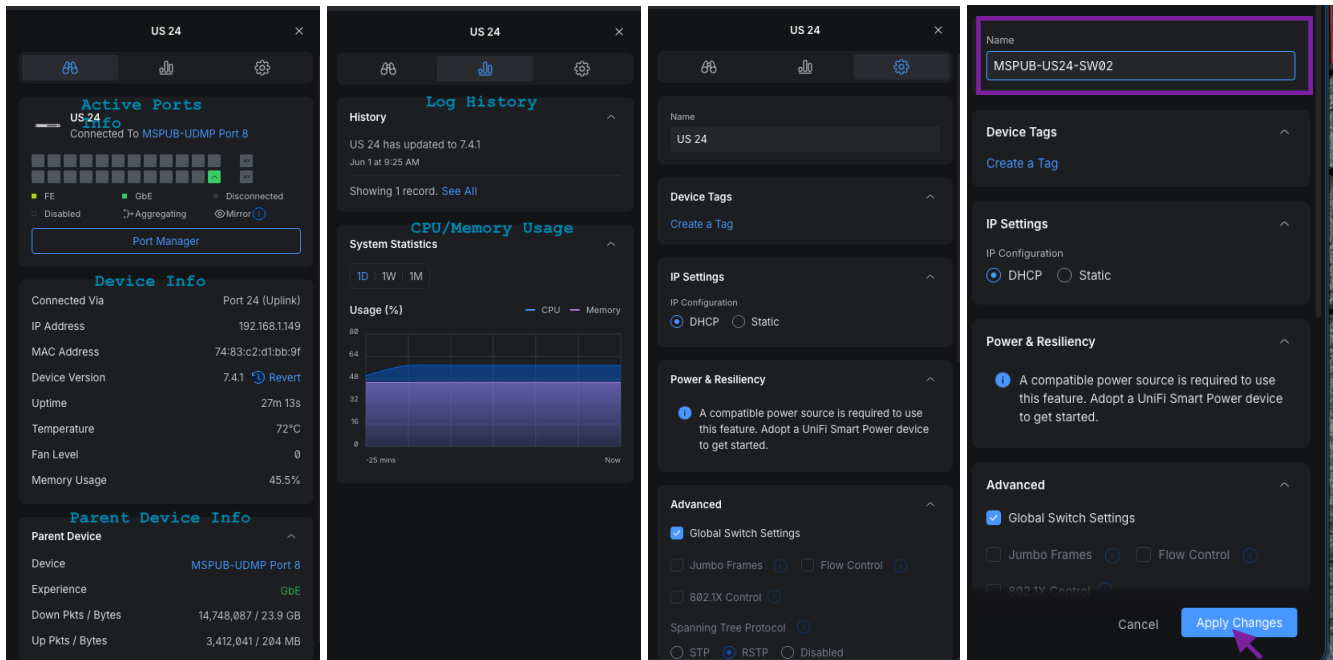


| Type | Name           | Application | Status         | IP Address    | Uplink | Parent Device | Ch. 2.4 G |
|------|----------------|-------------|----------------|---------------|--------|---------------|-----------|
| —    | MSPUB-UDMP     | Network     | Online         | 192.168.1.1   | GbE    | Ziply Fiber   | -         |
| —    | US 24          | Network     | Click to Adopt | 192.168.1.149 | -      | Ziply Fiber   | -         |
| —    | USW Pro 24 PoE | Network     | Click to Adopt | 192.168.1.21  | -      | Ziply Fiber   | -         |
| ●    | U6 Pro         | Network     | Click to Adopt | 192.168.1.211 | -      | -             | -         |
| ●    | U6 Pro         | Network     | Click to Adopt | 192.168.1.53  | -      | -             | -         |

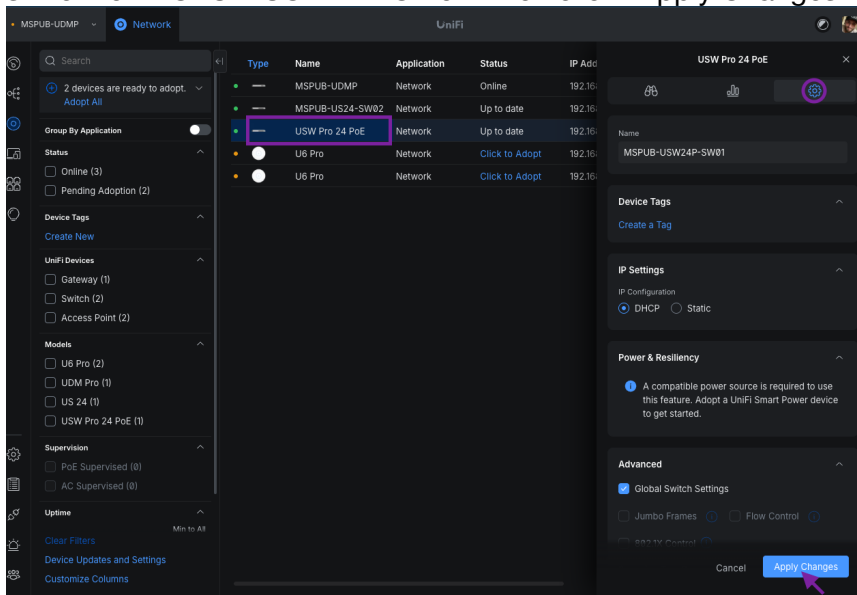
- Once Adoption has completed the status will change to either “Up to date” or “Pending updates.” The Uplink shows what kind of connection the device has, FE, GbE, 2.5G, 5G, 10G, 25G, depending on the network speed provided by the ISP and Device. The parent device shows which piece of hardware the device is connected to as well as which port.

| Type | Name           | Application | Status         | IP Address    | Uplink | Parent Device      | Ch. 2.4 G |
|------|----------------|-------------|----------------|---------------|--------|--------------------|-----------|
| —    | MSPUB-UDMP     | Network     | Online         | 192.168.1.1   | GbE    | Ziply Fiber        | -         |
| —    | US 24          | Network     | Up to date     | 192.168.1.149 | GbE    | MSPUB-UD... Port 8 | -         |
| —    | USW Pro 24 PoE | Network     | Up to date     | 192.168.1.21  | GbE    | MSPUB-UD... Port 7 | -         |
| ●    | U6 Pro         | Network     | Click to Adopt | 192.168.1.211 | -      | -                  | -         |
| ●    | U6 Pro         | Network     | Click to Adopt | 192.168.1.53  | -      | -                  | -         |

- Click “US 24” to display the Properties Pop-out Menu. This displays more information about the device as well as the ability to configure the switch. Overview shows active ports being used and device information. Insights shows log information and system statistics for CPU usage and Memory of the device. Settings where the switch can be configured. For now rename this switch to “MSPUB-US24-SW02” then click “Apply Changes.”

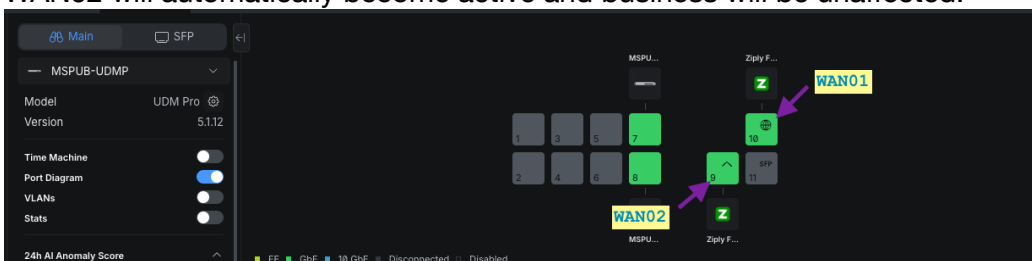


- Click on “USW Pro 24 PoE” to access the Properties Pop-Out Menu. Click “Settings” and rename this switch to “MSPUB-USW24P-SW01” then click “Apply Changes.”



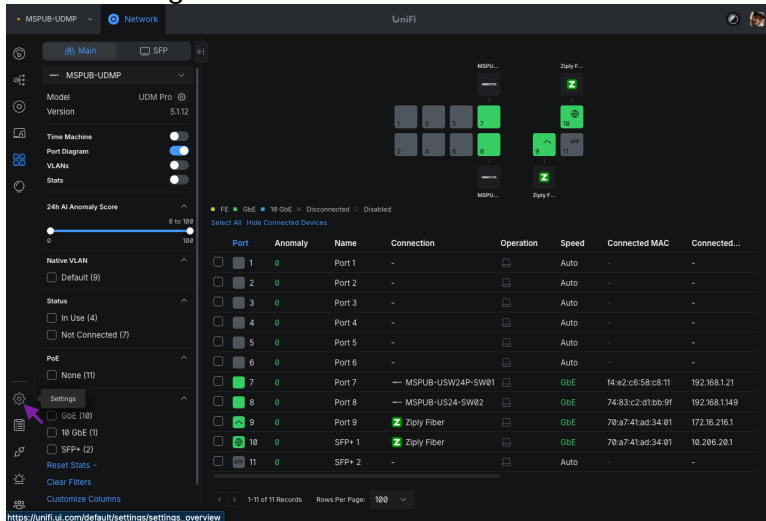
## Configuring Dual WAN Failover

Looking at MSPUB-UDMP in port manager there are two Wide Area Network (WAN) Uplinks on the RJ45 WAN port 9 and SFP port 10. One port can become the primary WAN and the other the failover WAN. Port 10 will be configured as the primary WAN01 and port 9 will become the failover WAN02. This will create redundancy, in the event WAN01 is disconnected, due to an ISP outage, cable break, or other disaster, WAN02 will automatically become active and business will be unaffected.

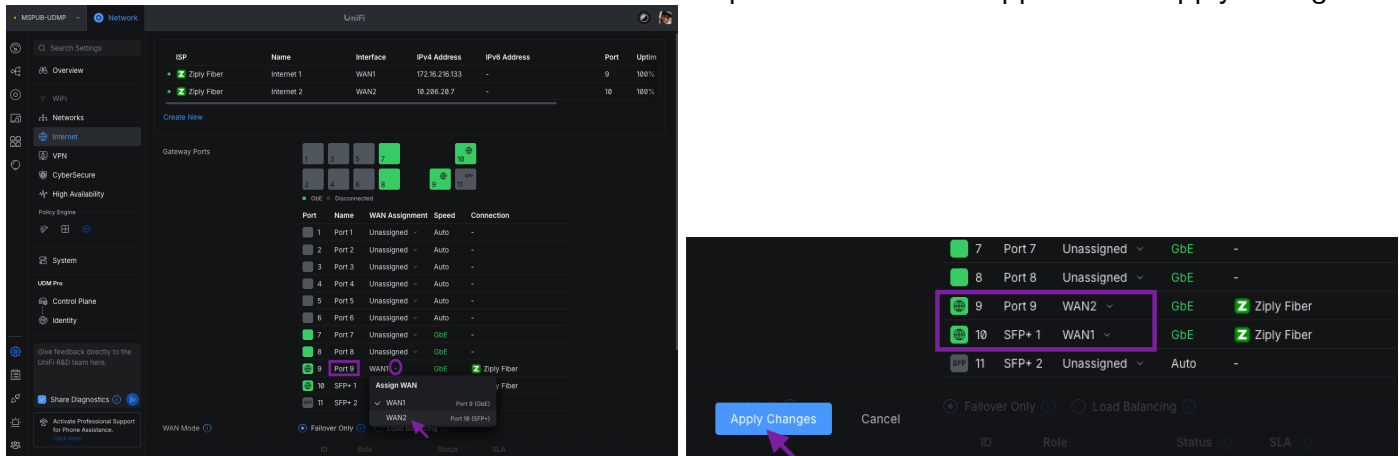


## Part 3: Network Fundamentals & Administration

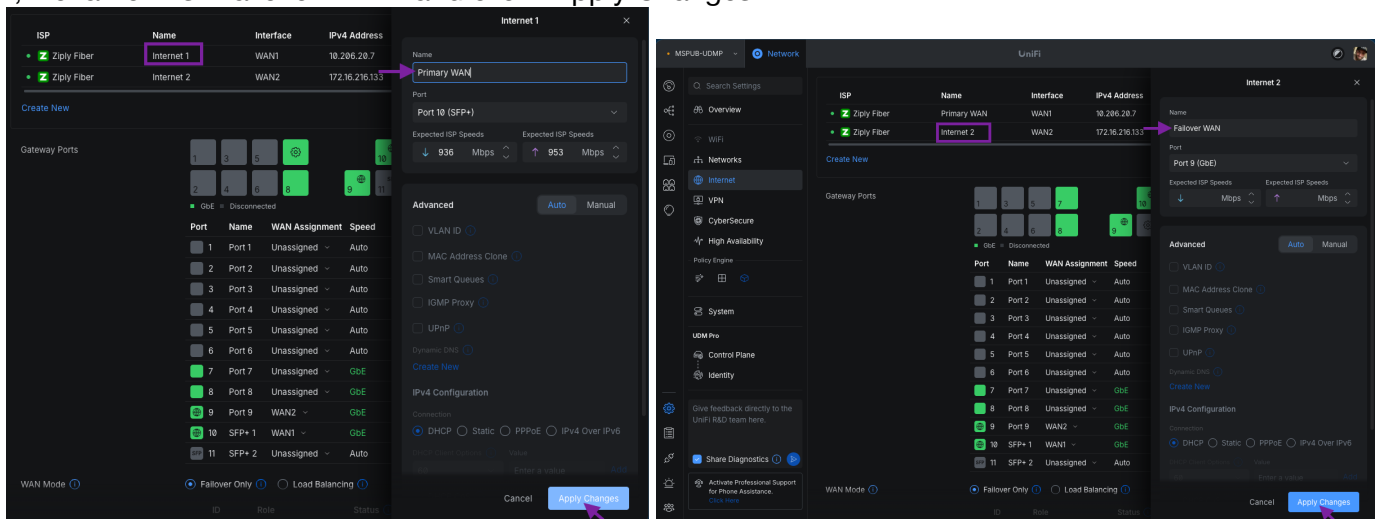
### 1. Click “Settings” on the left toolbar.



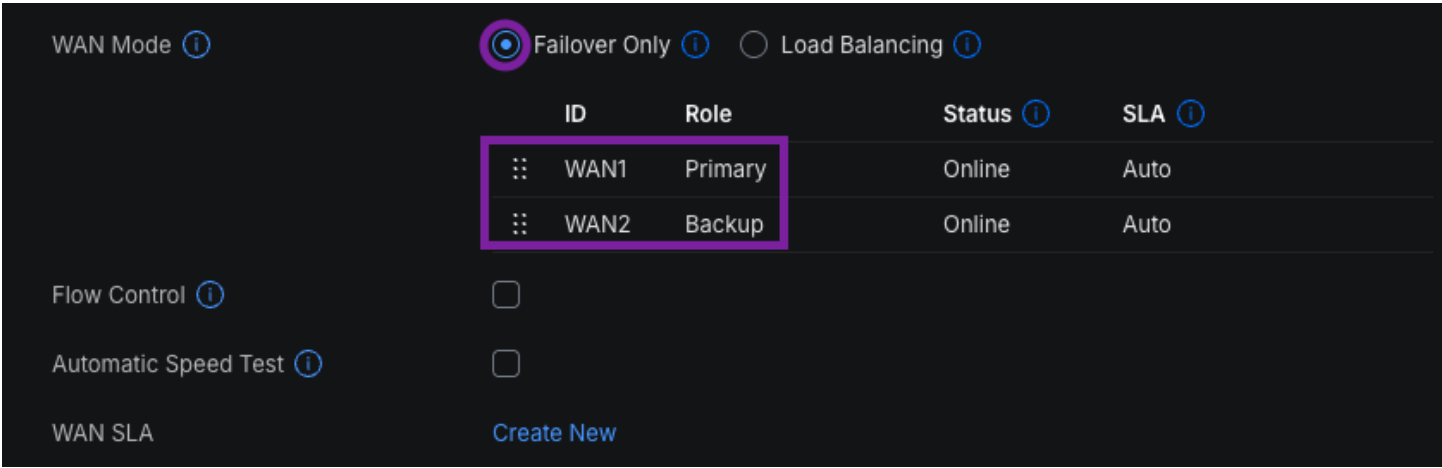
### 2. Swap the WAN order by click the arrow next to the port under WAN Assignment. Port 9 should become WAN2 and SFP+ 1 should become WAN1. Once those ports have been swapped click “Apply Changes.”



### 3. At the top click “Internet 1,” rename this “Primary WAN” and click “Apply Changes.” Then click “Internet 2,” rename this “Failover WAN” and click “Apply Changes.”

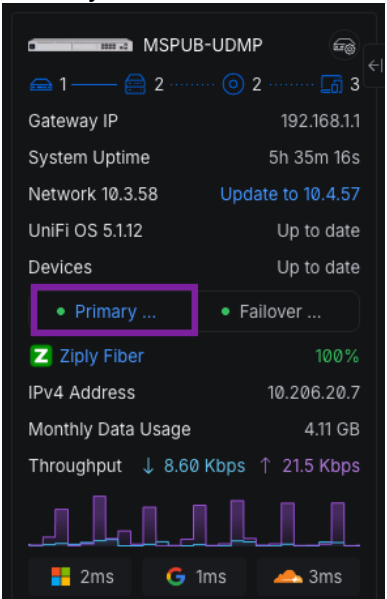


### 4. Scroll down to “WAN Mode” ensure “Failover Only” is selected and reorder WAN1 to the top by clicking and dragging the 6 dots on the left. Load Balancing can be enabled to distribute all network traffic evenly across the WANs. For now MSPUB will have its WAN mode set to Failover Only.

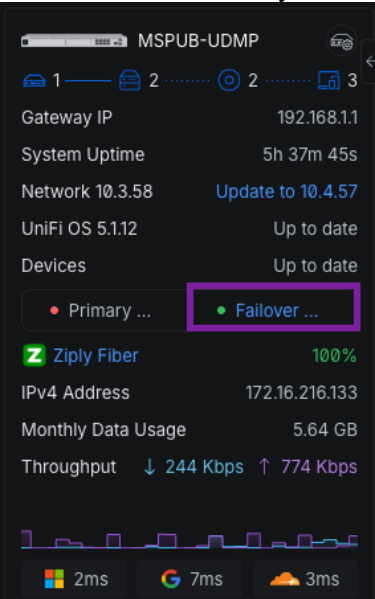


5. To test this, disconnect the Ethernet/Fiber cable plugged into the SFP+ optic on port 10. There should be no disruption, aside from Port 10 becoming offline and the console sending a notification say WAN1 has been disconnected.

Primary is still active.



Failover automatically took over when Primary was disconnected.



Creating VLANs

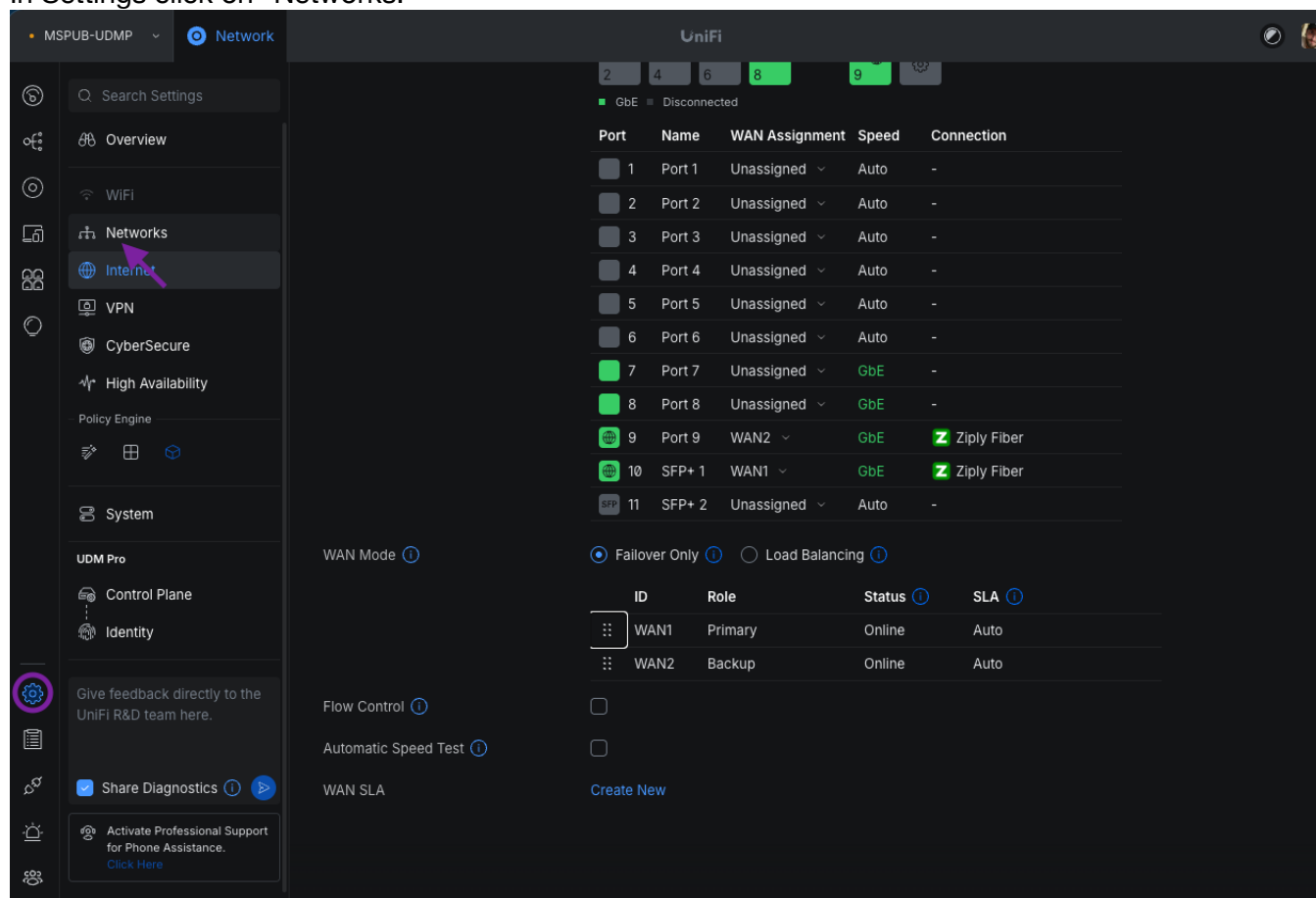
Virtual Local Area Networks or VLANs help segment a network into different subnets to separate devices. Although the UniFi will do the segmentation math for us depending on the VLAN CIDRs, the table below is the breakdown of MSPUB’s needs. The segmentation can be adjusted as needed as MSPUB continues to grow. The UniFi console can support up to 40 VLANs with IDs ranging from 0 to 255.

| Purpose                  | Infrastructure   | Servers          | Administration   | Publishing       | Online Services  | IT-Cyber         | Guest Network    | Blackhole (Disabled Ports) |
|--------------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|----------------------------|
| Minimum Host Requirement | 5                | 3                | 2                | 4                | 1                | 10               | 254              | 0                          |
| CIDR                     | 192.168.10.0 /29 | 192.168.20.0 /29 | 192.168.30.0 /29 | 192.168.40.0 /29 | 192.168.50.0 /30 | 192.168.60.0/ 28 | 192.168.80.0 /24 | No DHCP                    |
| Gateway                  | 192.168.10.1     | 192.168.20.1     | 192.168.30.1     | 192.168.40.1     | 192.168.50.1     | 192.168.60.1     | 192.168.80.1     | None                       |

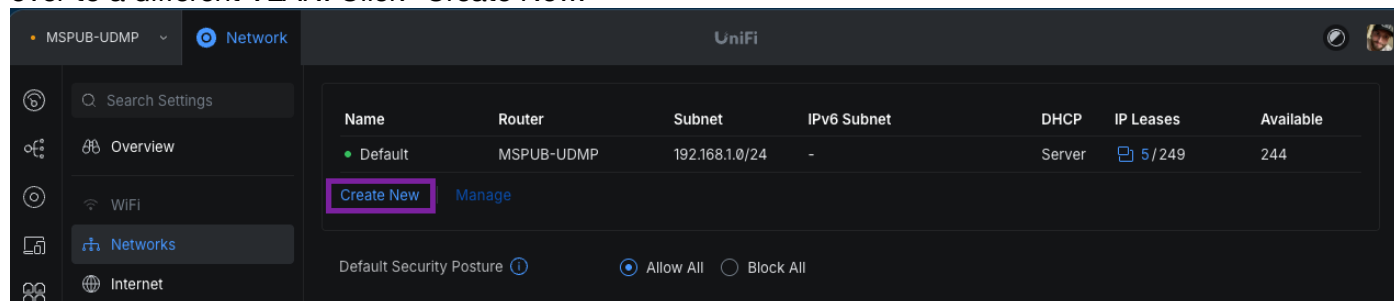
## Part 3: Network Fundamentals & Administration

| Mask             | 255.255.255.248             | 255.255.255.248             | 255.255.255.248             | 255.255.255.248             | 255.255.255.252             | 255.255.255.240              | 255.255.255.0              | N/A  |
|------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|------------------------------|----------------------------|------|
| IP Address Range | 192.168.10.2 - 192.168.10.6 | 192.168.20.2 - 192.168.20.6 | 192.168.30.2 - 192.168.30.6 | 192.168.40.2 - 192.168.40.6 | 192.168.50.2 - 192.168.50.2 | 192.168.60.2 - 192.168.60.14 | 192.168.80.2 - 192.168.254 | N/A  |
| Broadcast        | 192.168.10.7                | 192.168.20.7                | 192.168.20.7                | 192.168.40.7                | 192.168.50.3                | 192.168.60.15                | 192.168.80.255             | None |
| Usable Hosts     | 6                           | 6                           | 6                           | 6                           | 2                           | 13                           | 254                        | 0    |
| VLAN ID          | 10                          | 20                          | 30                          | 40                          | 50                          | 60                           | 80                         | 255  |

### 1. In Settings click on “Networks.”



### 2. At the top, there is already a “Default” network which will be deleted once the UniFi devices are switched over to a different VLAN. Click “Create New.”



### 3. This is the Network Properties pop-out menu. Switch the mode from Auto to “Manual” towards the bottom, then configure the following settings:

## Part 3: Network Fundamentals & Administration

- Name: **Infrastructure**
- Router: **MSPUB-UDMP**
- Disable: **Auto-Scale Network**
- IPv4 Address: **192.168.10.1**
- Netmask: **29**
- VLAN ID: **10**
- Ensure **Allow Internet Access**, **Auto Default Gateway**, **Auto DNS Servers**, and **Ping Conflict Detection** are enabled.
- Leave the remaining settings as defaults and click “Create.”

4. Repeat steps 2 and 3 for **Servers (VLAN 20)**, **Administration (VLAN 30)**, **Publishing (VLAN 40)**, **Online Services (VLAN 50)**, and **IT-Cyber (VLAN 60)**, based on the segmentation table above. The Guest network and Blackhole will be configured differently.

| Name              | VLAN ID | Router     | Subnet          | IPv6 Subnet | DHCP   | IP Leases | Available |
|-------------------|---------|------------|-----------------|-------------|--------|-----------|-----------|
| • Default         | 1       | MSPUB-UDMP | 192.168.1.0/24  | -           | Server | 5 / 249   | 244       |
| • Infrastructure  | 10      | MSPUB-UDMP | 192.168.10.0/29 | -           | Server | 0 / 5     | 5         |
| • Servers         | 20      | MSPUB-UDMP | 192.168.20.0/29 | -           | Server | 0 / 5     | 5         |
| • Administration  | 30      | MSPUB-UDMP | 192.168.30.0/29 | -           | Server | 0 / 5     | 5         |
| • Publishing      | 40      | MSPUB-UDMP | 192.168.40.0/29 | -           | Server | 0 / 5     | 5         |
| • Online Services | 50      | MSPUB-UDMP | 192.168.50.0/30 | -           | Server | 0 / 1     | 1         |
| • IT-Cyber        | 60      | MSPUB-UDMP | 192.168.60.0/28 | -           | Server | 0 / 13    | 13        |

Create New | Manage

5. The Guest network, will be completely isolated from the primary network. This will be configured to a wireless network later on. Create a new network and configure with the following settings:
- Name: **Guest**
  - Router: **MSPUB-UDMP**
  - **Disable**: Auto-Scale Network
  - IPv4 Address: **192.168.80.1**
  - Netmask: **24**
  - VLAN ID: **80**
  - **Enable**: Guest Network
  - **Enable**: Internet Access
  - **Enable**: Ping Conflict Detection
  - Lease Time: **7200** Seconds (~2 hours)
  - Click “Create” once configured

Create New Network

Name  
Guest

Router  
MSPUB-UDMP

IPv4

☐ Auto-Scale Network

IPv4 Address  
192.168.80.1

Netmask  
24

Gateway IP 192.168.80.1

Broadcast IP 192.168.80.255

Usable IPs 253

IP Range 192.168.80.1 - 192.168.80.254

Subnet Mask 255.255.255.0

DHCP Pool Size 249

DHCP Range 192.168.80.6 - 192.168.80.254

VLAN ID  
80

Auto Manual

☐ Additional IPs

☒ Guest Network

☐ Isolate Network

☒ Allow Internet Access

DHCP Mode  
☐ None ☒ DHCP Server ☐ DHCP Relay

DHCP Range  
Start 192.168.80.6 Stop 192.168.80.254

☐ DHCP Guarding

☒ Auto Default Gateway

☒ Auto DNS Server

Lease Time  
7200 Sec

Domain Name

Cancel Create

6. For the Blackhole network, this will be applied to all unused disabled ports, which if connected to will be completely isolated, with no internal network access nor Internet access. Create a new network and configure with the following settings:
- Name: **Blackhole**
  - Router: **MSPUB-UDMP**
  - **Disable**: Auto-Scale Network
  - IPv4 Address: **192.168.255.254**
  - Netmask: **30**
  - VLAN ID: **255**
  - **Enable**: Isolate Network
  - **Disable**: Internet Access
  - Select **None** under DHCP Mode
  - Click “Create.”

Create New Network

Name: Blackhole

Router: MSPUB-UDMP

IPv4

☐ Auto-Scale Network

IPv4 Address: 192.168.255.254

Netmask: 30

Gateway IP: 192.168.255.254

Broadcast IP: 192.168.255.255

Usable IPs: 1

IP Range: 192.168.255.253 - 192.168.255.254

Subnet Mask: 255.255.255.252

DHCP Pool Size: -

DHCP Range: -

VLAN ID: 255

Auto Manual

☐ Additional IPs

☐ Guest Network

☒ Isolate Network

☐ Allow Internet Access

DHCP Mode

☒ None ☐ DHCP Server ☐ DHCP Relay

☐ DHCP Guarding

IPv6

Interface Type

☒ None ☐ Prefix Delegation ☐ Static

Cancel Create



## Part 3: Network Fundamentals & Administration

- The VLANs have been created. These can now be configured to switches, specific ports and wireless access points.

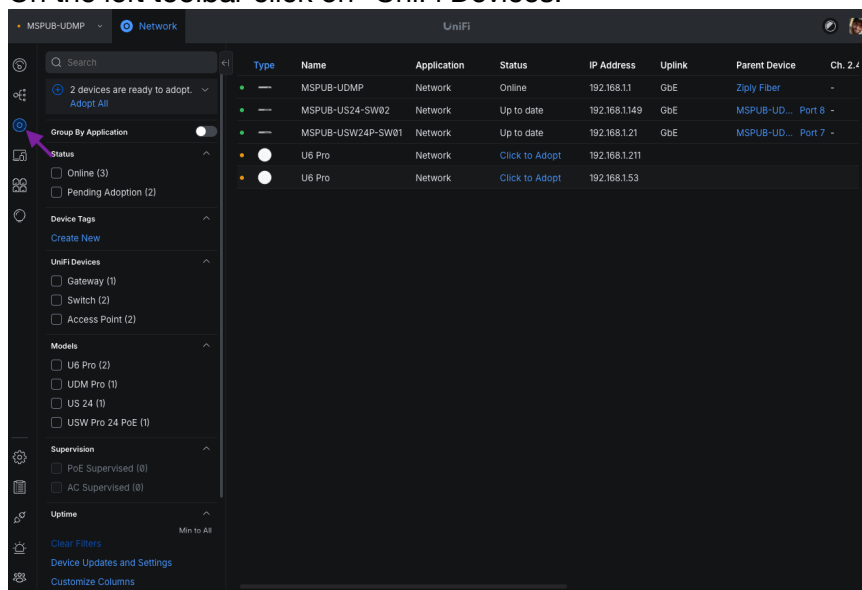
| Name            | VLAN ID | Router     | Subnet             | IPv6 Subnet | DHCP   | IP Leases | Available |
|-----------------|---------|------------|--------------------|-------------|--------|-----------|-----------|
| Default         | 1       | MSPUB-UDMP | 192.168.1.0/24     | -           | Server | 5 / 249   | 244       |
| Infrastructure  | 10      | MSPUB-UDMP | 192.168.10.0/29    | -           | Server | 0 / 5     | 5         |
| Servers         | 20      | MSPUB-UDMP | 192.168.20.0/29    | -           | Server | 0 / 5     | 5         |
| Administration  | 30      | MSPUB-UDMP | 192.168.30.0/29    | -           | Server | 0 / 5     | 5         |
| Publishing      | 40      | MSPUB-UDMP | 192.168.40.0/29    | -           | Server | 0 / 5     | 5         |
| Online Services | 50      | MSPUB-UDMP | 192.168.50.0/30    | -           | Server | 0 / 1     | 1         |
| IT-Cyber        | 60      | MSPUB-UDMP | 192.168.60.0/28    | -           | Server | 0 / 13    | 13        |
| Guest           | 80      | MSPUB-UDMP | 192.168.80.0/24    | -           | Server | 0 / 249   | 249       |
| Blackhole       | 255     | MSPUB-UDMP | 192.168.255.252/30 | -           | None   | -         | -         |

[Create New](#) | [Manage](#)

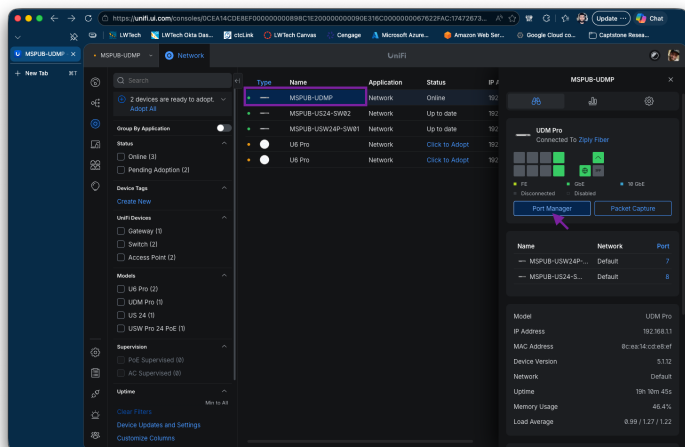
## Configuring Switches

The switches can now be configured now that VLANs have been configured.

- On the left toolbar click on “UniFi Devices.”

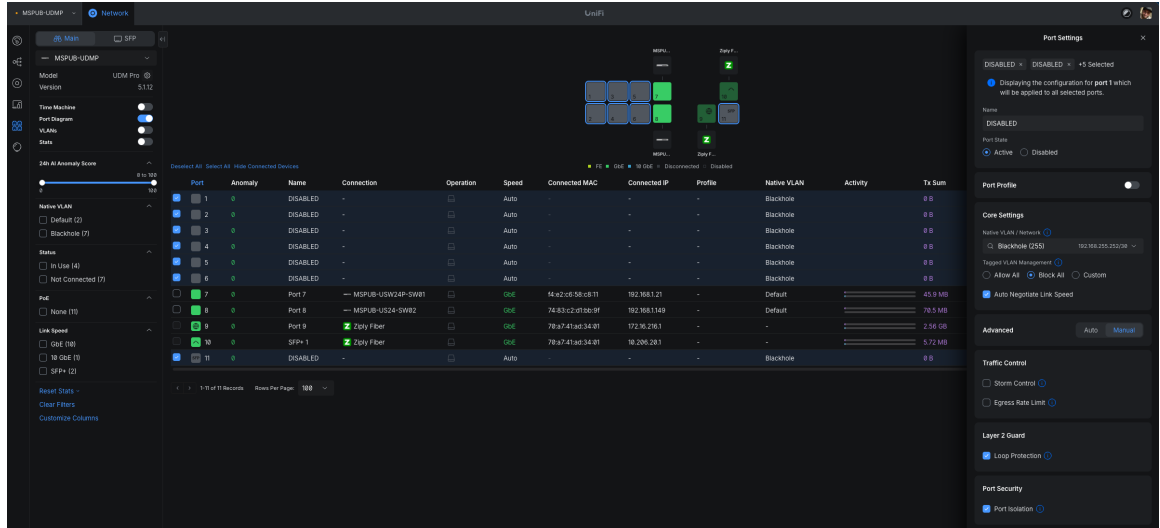


- Click “MSPUB-UDMP” to open the properties pop-out menu.
  - Click on the “Port Manager” to open the Port Manager for MSPUB-UDMP.

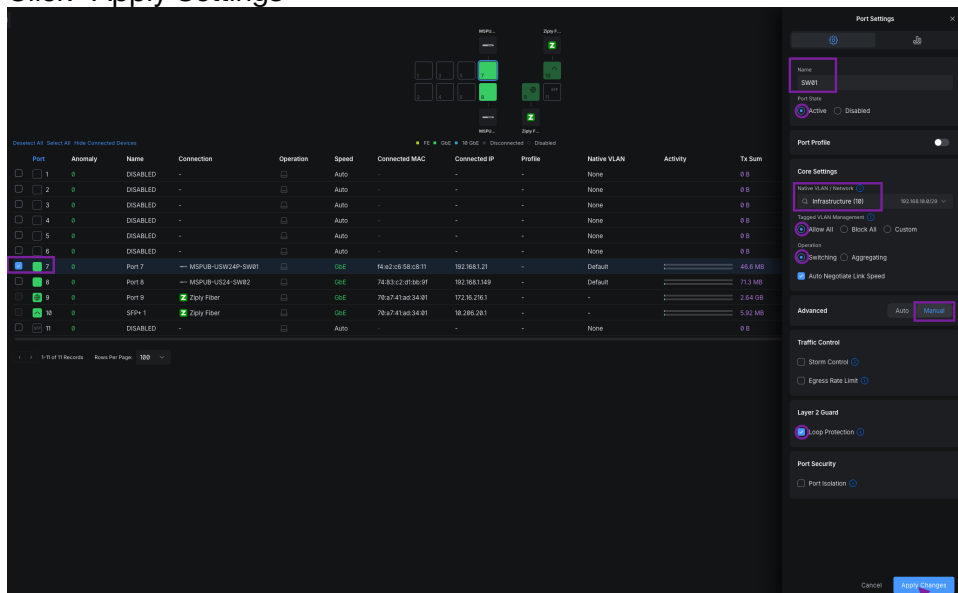


## Part 3: Network Fundamentals & Administration

2. Select all the gray ports to edit their settings simultaneously (ports 1-6 & 11)
  - In the Port Settings pop-out configure the following in this order:
    - Name: **DISABLED**
    - Native VLAN/Network: **Blackhole (255)**
    - Tagged VLAN Management: **Block all**
    - Advanced: **Manual**
    - **Enable:** Loop Protection
    - **Enable:** Port Isolation
    - Click “Apply Settings”
    - Port State: **Disabled**
    - Click “Apply Settings”
    - This will ensure if these ports accidentally get re-enabled they will default to the Blackhole VLAN

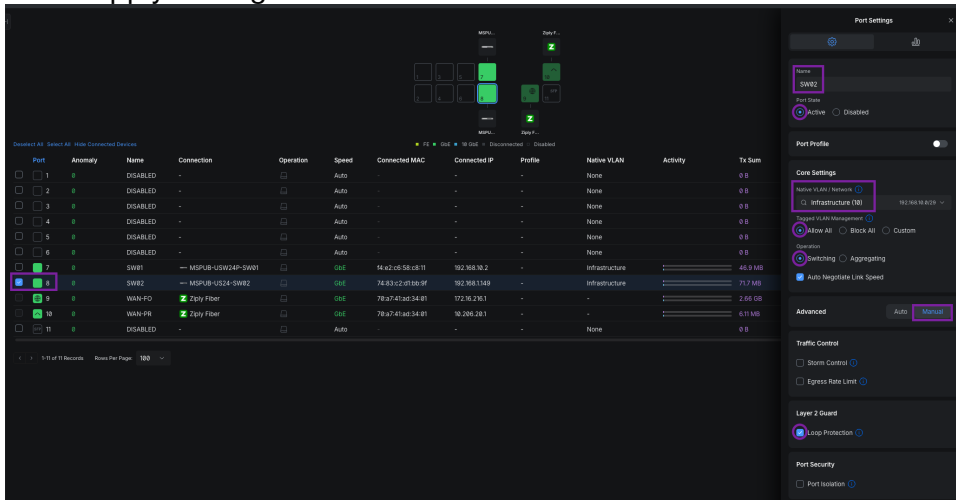


3. Select Port 7, in the Port Settings pop-out configure the following:
  - Name: **SW01**
  - Port State: **Active**
  - Name VLAN/Network: **Infrastructure (10)**
  - Tagged VLAN Management: **Allow All**
  - Operation: **Switching**
  - Advanced: **Manual**
  - **Enable:** Loop Protection
  - Click “Apply Settings”

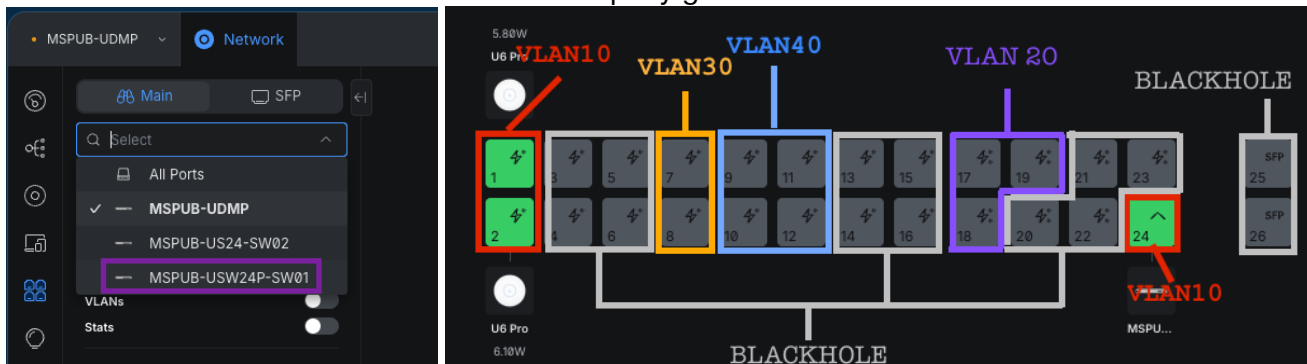


## 4. Select Port 8, in the Port Settings pop-out configure the following:

- Name: **SW02**
- Port State: **Active**
- Name VLAN/Network: **Infrastructure (10)**
- Tagged VLAN Management: **Allow All**
- Operation: **Switching**
- Advanced: **Manual**
- **Enable:** Loop Protection
- Click “Apply Settings”

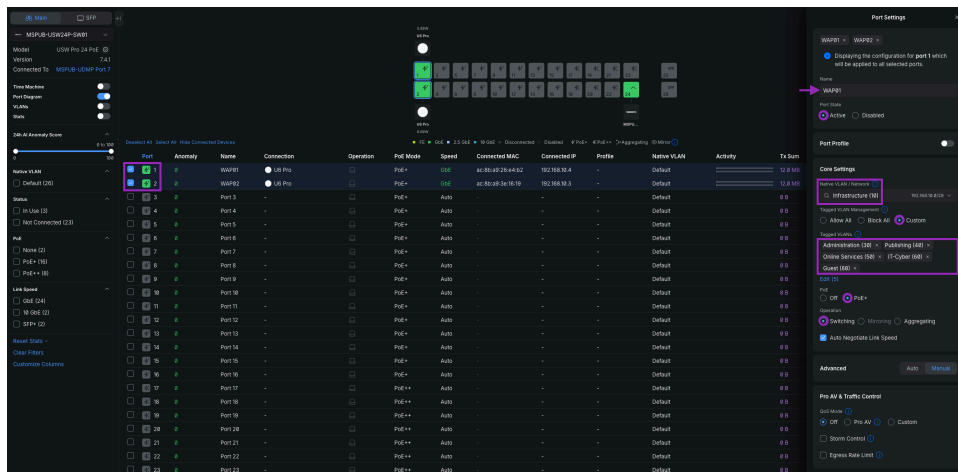


3. From the drop-down menu towards the upper-left, select MSPUB-USW24P-SW01. This switches ports are going to be broken up into 4 sections. 2 ports are going to be enabled with PoE+ and part of the Infrastructure (VLAN10) for 2 wireless access points on ports 1 & 2. Servers (VLAN20) will be on ports 17-19. Administration (VLAN30) computers on ports 7 & 8. Publishing (VLAN40) computers on ports 9-12. The uplink on port 24. And the remaining ports 3-6, 13-16, 20-23, and 25-26 will be blackholes for now, but can be activated as needed while the company grows.



1. Select ports 1-2, and configure the following settings: (note: to rename them individually select each individually and then name them. The initial settings can be the same.)

- Name: **WAP01** and **WAP02**
- Port State: **Active**
- Native VLAN/Network: **Infrastructure (20)**
- Tagged VLAN Management: **Custom**
  - Select: **Administration, Publishing, Online Services, IT-Cyber, Servers, Guest**
- PoE: **PoE+**
- Operation: **Switching**
- Advanced: **Manual**
- **Enable:** Loop Protection
- Click “Apply Changes”



2. Select ports 7-8, and configure the following settings:
  - Name: **ADM**
  - Port State: **Active**
  - Native VLAN/Network: **Administration (30)**
  - Tagged VLAN Management: **Custom**
    - Select: **Servers**
  - PoE: **Off**
  - Operation: **Switching**
  - Advanced: **Manual**
  - **Enable:** Loop Protection
  - Click “Apply Changes”
3. Select ports 9-12, and configure the following settings:
  - Name: **PUB**
  - Port State: **Active**
  - Native VLAN/Network: **Publishing (40)**
  - Tagged VLAN Management: **Custom**
    - Select: **Servers**
  - PoE: **Off**
  - Operation: **Switching**
  - Advanced: **Manual**
  - **Enable:** Loop Protection
  - Click “Apply Changes”
4. Select ports 17-19, and configure the following settings:
  - Name: **SRV**
  - Port State: **Active**
  - Native VLAN/Network: **Servers (20)**
  - Tagged VLAN Management: **Custom**
    - Select: **Administration, Publishing, Online Services, IT-Cyber**
  - PoE: **Off**
  - Operation: **Switching**
  - Advanced: **Manual**
  - **Enable:** Loop Protection
  - Click “Apply Changes”
5. Select port 24, and configure the following settings:
  - Name: **UDM**
  - Port State: **Active**
  - Native VLAN/Network: **Infrastructure (10)**
  - Tagged VLAN Management: **Custom**

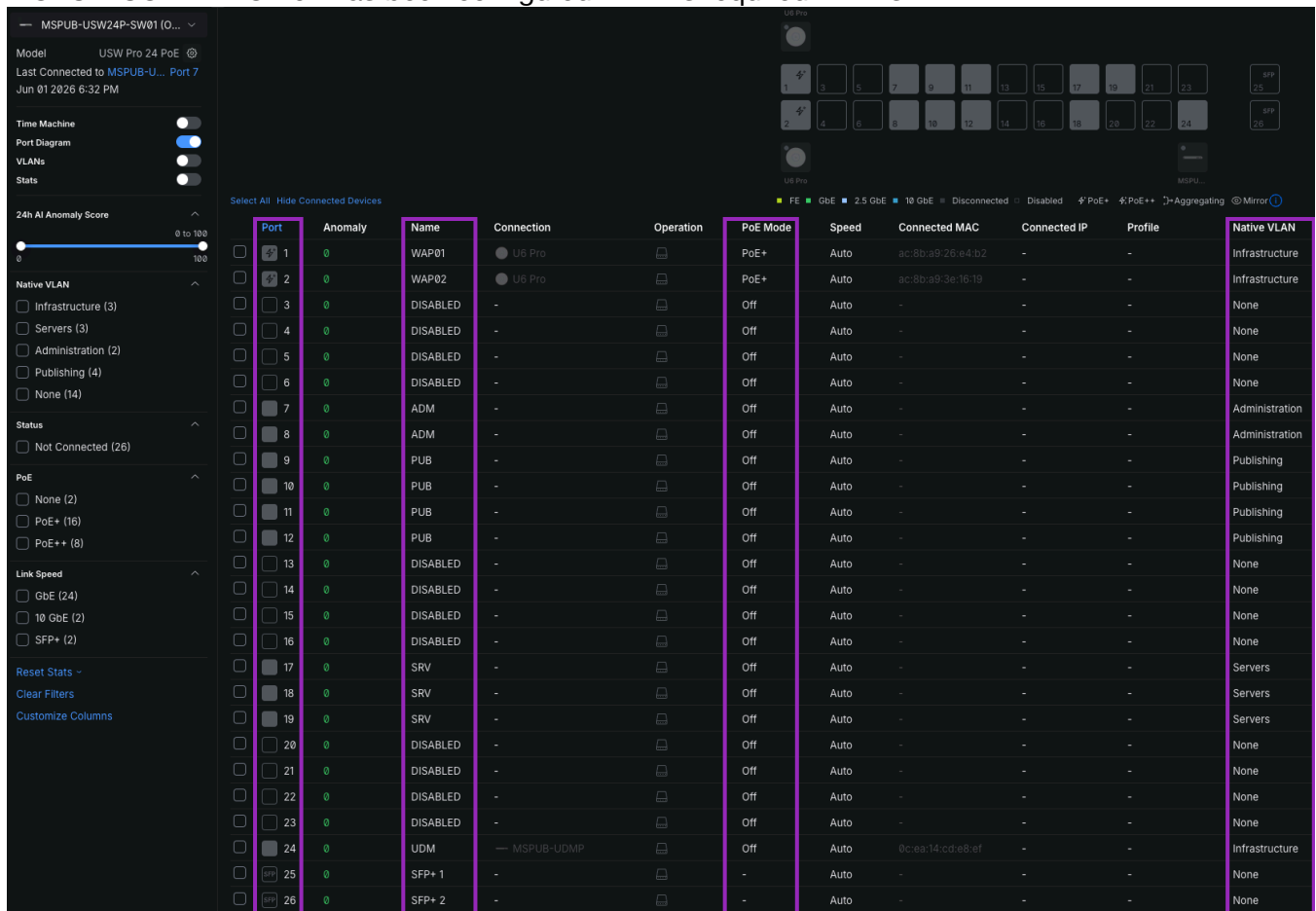
## Part 3: Network Fundamentals & Administration

- Select: **Administration, Publishing, Online Services, IT-Cyber, Servers**
- PoE: **OFF**
- Operation: **Switching**
- Advanced: **Manual**
- **Enable**: Loop Protection
- Click “Apply Changes”

### 6. Select ports 3-6, 13-16, 20-23, and 25-26, then configure the following:

- Name: **DISABLED**
- Native VLAN/Network: **Blackhole (255)**
- Tagged VLAN Management: **Block all**
- Advanced: **Manual**
- **Enable**: Loop Protection
- **Enable**: Port Isolation
- Click “Apply Settings”
- Port State: **Disabled**
- Click “Apply Settings”
- This will ensure if these ports accidentally get re-enabled they will default to the Blackhole VLAN

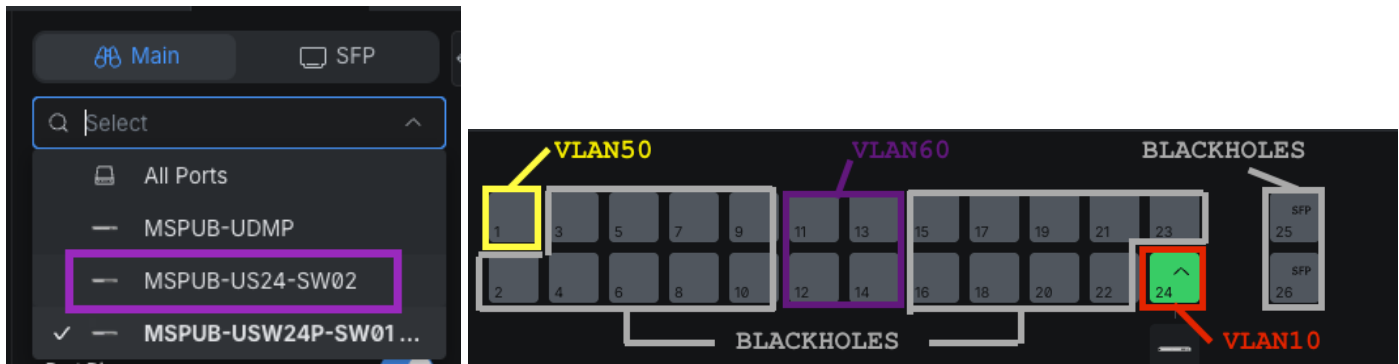
### 7. MSPUB-USW24P-SW01 has been configured with it's required VLANs.



The screenshot displays the configuration interface for MSPUB-USW24P-SW01. On the left, there are tabs for Time Machine, Port Diagram, VLANs, and Stats. Below these is a 24h AI Anomaly Score slider. The main area shows a table of port configurations. The table has columns for Port, Anomaly, Name, Connection, Operation, PoE Mode, Speed, Connected MAC, Connected IP, Profile, and Native VLAN. The ports are listed from 1 to 26. Ports 1 and 2 are WAP01 and WAP02 respectively. Ports 3-6, 13-16, 20-23, and 25-26 are all set to Disabled. Ports 7-12 are ADM, PUB, and SRV. Ports 17-19 are SRV. Port 24 is UDM. Ports 25 and 26 are SFP+ 1 and SFP+ 2 respectively. The Native VLAN for ports 1-6, 13-16, 20-23, and 25-26 is Infrastructure. The Native VLAN for ports 7-12, 17-19, and 24 is Administration. The Native VLAN for ports 17-19, 24, and 25-26 is Servers. The Native VLAN for ports 25 and 26 is None.

| Port | Anomaly | Name     | Connection | Operation | PoE Mode | Speed | Connected MAC     | Connected IP | Profile | Native VLAN    |
|------|---------|----------|------------|-----------|----------|-------|-------------------|--------------|---------|----------------|
| 1    | 0       | WAP01    | U6 Pro     | On        | PoE+     | Auto  | ac:8b:a9:26:e4:b2 | -            | -       | Infrastructure |
| 2    | 0       | WAP02    | U6 Pro     | On        | PoE+     | Auto  | ac:8b:a9:3e:16:19 | -            | -       | Infrastructure |
| 3    | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 4    | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 5    | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 6    | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 7    | 0       | ADM      | -          | Off       | Off      | Auto  | -                 | -            | -       | Administration |
| 8    | 0       | ADM      | -          | Off       | Off      | Auto  | -                 | -            | -       | Administration |
| 9    | 0       | PUB      | -          | Off       | Off      | Auto  | -                 | -            | -       | Publishing     |
| 10   | 0       | PUB      | -          | Off       | Off      | Auto  | -                 | -            | -       | Publishing     |
| 11   | 0       | PUB      | -          | Off       | Off      | Auto  | -                 | -            | -       | Publishing     |
| 12   | 0       | PUB      | -          | Off       | Off      | Auto  | -                 | -            | -       | Publishing     |
| 13   | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 14   | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 15   | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 16   | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 17   | 0       | SRV      | -          | Off       | Off      | Auto  | -                 | -            | -       | Servers        |
| 18   | 0       | SRV      | -          | Off       | Off      | Auto  | -                 | -            | -       | Servers        |
| 19   | 0       | SRV      | -          | Off       | Off      | Auto  | -                 | -            | -       | Servers        |
| 20   | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 21   | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 22   | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 23   | 0       | DISABLED | -          | Off       | Off      | Auto  | -                 | -            | -       | None           |
| 24   | 0       | UDM      | MSPUB-UDMP | Off       | Off      | Auto  | 8c:ea:14:cd:e8:ef | -            | -       | Infrastructure |
| 25   | 0       | SFP+ 1   | -          | -         | -        | Auto  | -                 | -            | -       | None           |
| 26   | 0       | SFP+ 2   | -          | -         | -        | Auto  | -                 | -            | -       | None           |

4. From the drop-down menu towards the upper-left, select MSPUB-USW24-SW02. This switch does not have PoE capabilities. The switches ports are going to be broken up into 4 sections. Port 1 will be designated for Online Services (VLAN50). Ports 11-14 will be assigned to IT-Cyber (VLAN60). Then ports 2-10, 15-23, and 25-26 will be blackholes for the time being. These can be changed as the company grows.



1. Select port 1, and configure the following:
  - Name: **OLS**
  - Port State: **Active**
  - Native VLAN/Network: **Online Services (50)**
  - Tagged VLAN Management: **Custom**
    - Select: **Servers**
  - Operation: **Switching**
  - Advanced: **Manual**
  - **Enable:** Loop Protection
  - Click “Apply Changes”
  
2. Select ports 11-14, and configure the following:
 Name: **ITC**
  - Port State: **Active**
  - Native VLAN/Network: **IT-Cyber (60)**
  - Tagged VLAN Management: **Custom**
    - Select: **Infrastructure, Administration, Publishing, Online Services, Servers, Guest, Blackhole**
  - Operation: **Switching**
  - Advanced: **Manual**
  - **Enable:** Loop Protection
  - Click “Apply Changes”
  
3. Select ports 2-10, 15-23, and 25-26, and configure the following:
  - Name: **DISABLED**
  - Native VLAN/Network: **Blackhole (255)**
  - Tagged VLAN Management: **Block all**
  - Advanced: **Manual**
  - **Enable:** Port Isolation
  - Click “Apply Settings”
  - Port State: **Disabled**
  - Click “Apply Settings”
  - This will ensure if these ports accidentally get re-enabled they will default to the Blackhole VLAN
  
4. Select port 24, and configure the following:
  - Name: **UDM**
  - Port State: **Active**
  - Native VLAN/Network: **Infrastructure (10)**
  - Tagged VLAN Management: **Custom**
    - Select: **Administration, Publishing, Online Services, IT-Cyber, Servers**
  - PoE: **OFF**
  - Operation: **Switching**
  - Advanced: **Manual**

- **Enable:** Loop Protection
- Click “Apply Changes”

### 5. MSPUB-USW24-SW02 has been configured with it's required VLANs.

The screenshot shows the configuration page for MSPUB-USW24-SW02. On the left, there are various configuration tabs like Time Machine, Port Diagram, VLANs, and Status. The main area displays a table of ports with columns: Port, Anomaly, Name, Connection, Operation, Speed, Connected MAC, Connected IP, Profile, and Native VLAN. Ports 1-23 are disabled. Port 24 is connected to MSPUB-UDMP and has a native VLAN of Default. Ports 25 and 26 are disabled with a native VLAN of Blackhole.

| Port | Anomaly | Name     | Connection | Operation | Speed | Connected MAC     | Connected IP | Profile | Native VLAN     |
|------|---------|----------|------------|-----------|-------|-------------------|--------------|---------|-----------------|
| 1    | 0       | OLS      | -          | Auto      | Auto  | -                 | -            | -       | Online Services |
| 2    | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 3    | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 4    | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 5    | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 6    | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 7    | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 8    | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 9    | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 10   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 11   | 0       | ITC      | -          | Auto      | Auto  | -                 | -            | -       | IT-Cyber        |
| 12   | 0       | ITC      | -          | Auto      | Auto  | -                 | -            | -       | IT-Cyber        |
| 13   | 0       | ITC      | -          | Auto      | Auto  | -                 | -            | -       | IT-Cyber        |
| 14   | 0       | ITC      | -          | Auto      | Auto  | -                 | -            | -       | IT-Cyber        |
| 15   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 16   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 17   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 18   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 19   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 20   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 21   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 22   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 23   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 24   | 70      | UDM      | MSPUB-UDMP | GbE       | 10000 | 00:0a:14:c0:e8:ef | 192.168.1.1  | -       | Default         |
| 25   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |
| 26   | 0       | DISABLED | -          | Auto      | Auto  | -                 | -            | -       | Blackhole       |

## Configuring Firewall/ACLs

Firewall policies will be configured to isolate guest traffic from internal resources while allowing business departments access to required server infrastructure. Access control policies will be implemented within firewall rules, to limit inter-VLAN communication and ensure only authorized departments can access internal server resources.

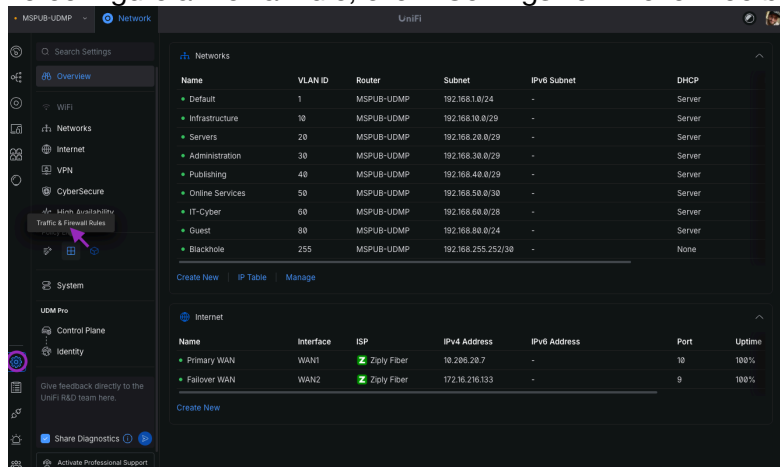
### Firewall/ACL Rules

| Rule Name                        | Type   | Action | Protocol | Source                                | Destination                                           | Port | Position          | Purpose                                    |
|----------------------------------|--------|--------|----------|---------------------------------------|-------------------------------------------------------|------|-------------------|--------------------------------------------|
| Block Guest to Internal          | LAN In | Drop   | All      | Network: Guest: IPv4 Subnet           | List: Internal Network - Infrastructure (VLANs 10-60) | Any  | Before Predefined | Prevent guest access to internal resources |
| Allow Admin to Servers           | LAN In | Accept | All      | Network: Administration : IPv4 Subnet | Network: Servers: IPv4 Subnet                         | Any  | Before Predefined | Administrative access to servers           |
| Allow IT-Cyber Management        | LAN In | Accept | All      | Network: IT-Cyber: IPv4 Subnet        | List: All VLANs                                       | Any  | Before Predefined | Network and server management              |
| Allow Publishing to Servers      | LAN In | Accept | All      | Network: Publishing: IPv4 Subnet      | Network: Servers: IPv4 Subnet                         | Any  | Before Predefined | Access publishing resources                |
| Allow Online Services to Servers | LAN In | Accept | All      | Network: Online Services: IPv4 Subnet | Network: Servers: IPv4 Subnet                         | Any  | Before Predefined | Web and content management                 |

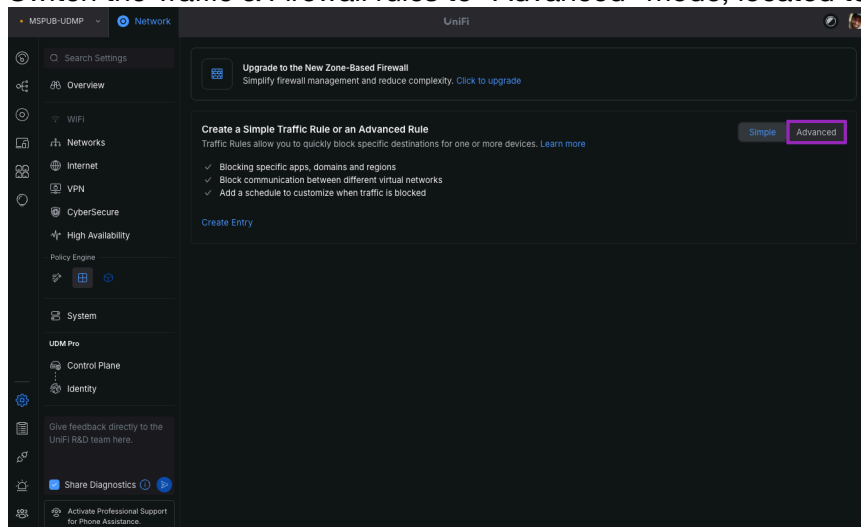
## Part 3: Network Fundamentals & Administration

| Rule Name                  | Type   | Action | Protocol | Source                          | Destination | Port | Position          | Purpose                       |
|----------------------------|--------|--------|----------|---------------------------------|-------------|------|-------------------|-------------------------------|
| <b>Block Disabled VLAN</b> | LAN In | Drop   | All      | Network: Blackhole: IPv4 Subnet | Any         | Any  | Before Predefined | Prevent use of inactive ports |

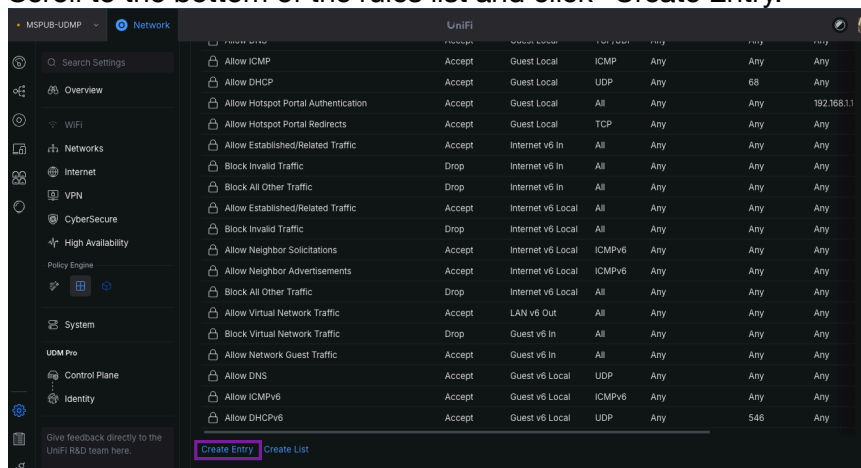
1. To configure a firewall rule, click “Settings” on the left toolbar.



2. Switch the Traffic & Firewall rules to “Advanced” mode, located towards the right.



3. Scroll to the bottom of the rules list and click “Create Entry.”





## Part 3: Network Fundamentals & Administration

### 4. Configure the following settings for a new Firewall/Traffic rule.

- Type: **LAN In**
- Name: **Block Guest to Internal**
- Action: **Drop**
- Protocol: **All**
- **Enable:** Before Predefined
- Source Type: **Network**
- Network: **Guest**
- Network Type: **IPv4 Subnet**
- Destination Type: **List**
- Address Group: Click “New” to create a new list
  - Name: **Internal Network - Infrastructure**
    - Add the following subnets:
      - 192.168.10.0/29
      - 192.168.20.0/29
      - 192.168.30.0/29
      - 192.168.40.0/29
      - 192.168.50.0/30
      - 192.168.60.0/28

New List

Name

Internal Network - Infrastructure

IPv4 Address, Subnet or Range [Add](#)

[Add Multiple](#)

Address [Edit](#)

192.168.10.0/29

192.168.20.0/29

192.168.30.0/29

192.168.40.0/29

192.168.50.0/30

192.168.60.0/28 [Remove](#)

[Clear](#)

[Cancel](#) [Create](#)

- Port List: **Any**
- Advanced: **Auto**
- Click “Add Rule”

Rule Type

Simple Advanced

Type LAN In

Name Block Guest to Internal

Action Accept Reject Drop

Protocol All Before Predefined

Source

Source Type Network

Network Guest 0 Devices

Network Type IPv4 Subnet

MAC Address Enter MAC Address

Destination

Destination Type List

Address Group Internal Network - Infrastructure New

Port List Any

Advanced Auto Manual

Match State New Invalid Established Related

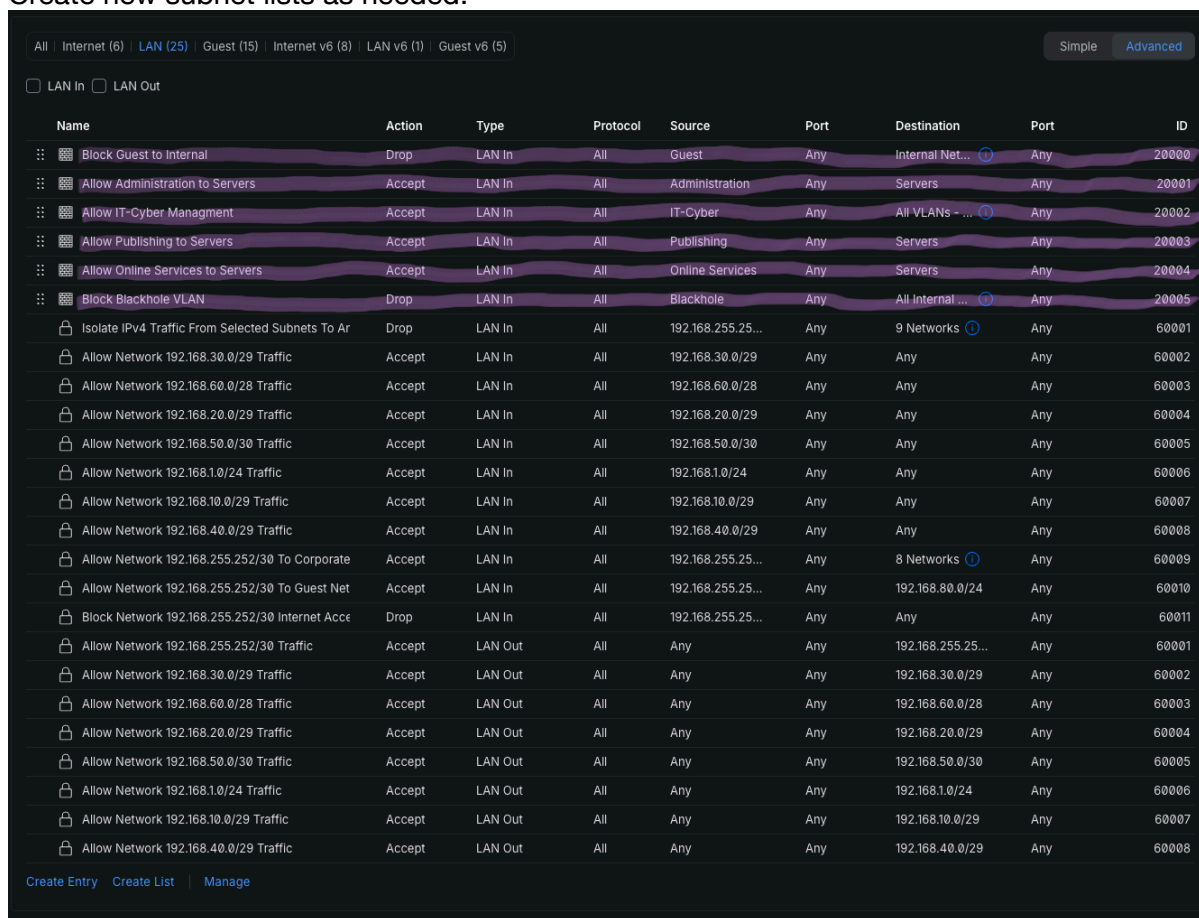
Match IPsec Do not match IPsec Non-IPsec

Logging

[Add Rule](#) [Cancel](#)

## Part 3: Network Fundamentals & Administration

5. Repeat step 4 to configure the rest of the firewall rules based on the table at the beginning of this section. Create new subnet lists as needed.



| Name                                             | Action | Type    | Protocol | Source            | Port | Destination       | Port | ID    |
|--------------------------------------------------|--------|---------|----------|-------------------|------|-------------------|------|-------|
| Block Guest to Internal                          | Drop   | LAN In  | All      | Guest             | Any  | Internal Net...   | Any  | 20000 |
| Allow Administration to Servers                  | Accept | LAN In  | All      | Administration    | Any  | Servers           | Any  | 20001 |
| Allow IT-Cyber Management                        | Accept | LAN In  | All      | IT-Cyber          | Any  | All VLANs - ...   | Any  | 20002 |
| Allow Publishing to Servers                      | Accept | LAN In  | All      | Publishing        | Any  | Servers           | Any  | 20003 |
| Allow Online Services to Servers                 | Accept | LAN In  | All      | Online Services   | Any  | Servers           | Any  | 20004 |
| Block Blackhole VLAN                             | Drop   | LAN In  | All      | Blackhole         | Any  | All Internal ...  | Any  | 20005 |
| Isolate IPv4 Traffic From Selected Subnets To Ar | Drop   | LAN In  | All      | 192.168.255.25... | Any  | 9 Networks        | Any  | 60001 |
| Allow Network 192.168.30.0/29 Traffic            | Accept | LAN In  | All      | 192.168.30.0/29   | Any  | Any               | Any  | 60002 |
| Allow Network 192.168.60.0/28 Traffic            | Accept | LAN In  | All      | 192.168.60.0/28   | Any  | Any               | Any  | 60003 |
| Allow Network 192.168.20.0/29 Traffic            | Accept | LAN In  | All      | 192.168.20.0/29   | Any  | Any               | Any  | 60004 |
| Allow Network 192.168.50.0/30 Traffic            | Accept | LAN In  | All      | 192.168.50.0/30   | Any  | Any               | Any  | 60005 |
| Allow Network 192.168.10.0/24 Traffic            | Accept | LAN In  | All      | 192.168.10.0/24   | Any  | Any               | Any  | 60006 |
| Allow Network 192.168.10.0/29 Traffic            | Accept | LAN In  | All      | 192.168.10.0/29   | Any  | Any               | Any  | 60007 |
| Allow Network 192.168.40.0/29 Traffic            | Accept | LAN In  | All      | 192.168.40.0/29   | Any  | Any               | Any  | 60008 |
| Allow Network 192.168.255.252/30 To Corporate    | Accept | LAN In  | All      | 192.168.255.25... | Any  | 8 Networks        | Any  | 60009 |
| Allow Network 192.168.255.252/30 To Guest Net    | Accept | LAN In  | All      | 192.168.255.25... | Any  | 192.168.80.0/24   | Any  | 60010 |
| Block Network 192.168.255.252/30 Internet Acce   | Drop   | LAN In  | All      | 192.168.255.25... | Any  | Any               | Any  | 60011 |
| Allow Network 192.168.255.252/30 Traffic         | Accept | LAN Out | All      | Any               | Any  | 192.168.255.25... | Any  | 60001 |
| Allow Network 192.168.30.0/29 Traffic            | Accept | LAN Out | All      | Any               | Any  | 192.168.30.0/29   | Any  | 60002 |
| Allow Network 192.168.60.0/28 Traffic            | Accept | LAN Out | All      | Any               | Any  | 192.168.60.0/28   | Any  | 60003 |
| Allow Network 192.168.20.0/29 Traffic            | Accept | LAN Out | All      | Any               | Any  | 192.168.20.0/29   | Any  | 60004 |
| Allow Network 192.168.50.0/30 Traffic            | Accept | LAN Out | All      | Any               | Any  | 192.168.50.0/30   | Any  | 60005 |
| Allow Network 192.168.10.0/24 Traffic            | Accept | LAN Out | All      | Any               | Any  | 192.168.10.0/24   | Any  | 60006 |
| Allow Network 192.168.10.0/29 Traffic            | Accept | LAN Out | All      | Any               | Any  | 192.168.10.0/29   | Any  | 60007 |
| Allow Network 192.168.40.0/29 Traffic            | Accept | LAN Out | All      | Any               | Any  | 192.168.40.0/29   | Any  | 60008 |

### Configuring Quality of Service (QoS)

Quality of Service policies will be configured to prioritize business-critical traffic while reducing the impact of guest network usage on organizational resources.

#### QoS Policies

| Name                          | QoS Behavior | Interface | Limits           | Source                                           | Destination       | Port                                     | Schedule | Purpose                                      |
|-------------------------------|--------------|-----------|------------------|--------------------------------------------------|-------------------|------------------------------------------|----------|----------------------------------------------|
| MSPUB-Critical-Infrastructure | Prioritize   | All WAN   | ↑ None<br>↓ None | Network VLAN 20<br>VLAN 60                       | Any               | Any                                      | Always   | Server traffic, IT management traffic        |
| MSPUB-VoIP-Calling            | Prioritize   | All WAN   | ↑ None<br>↓ None | Network VLAN 30<br>VLAN 40<br>VLAN 50<br>VLAN 60 | App:<br>Category: | VoIP Services                            | Always   | Voice Over Internet Protocol Calling traffic |
| MSPUB-Video-Calling           | Prioritize   | All WAN   | ↑ None<br>↓ None | Network VLAN 30<br>VLAN 40<br>VLAN 50<br>VLAN 60 | App:              | Zoom<br>MS Teams<br>Webex<br>Google Meet | Always   | Video conferencing traffic                   |
| MSPUB-Business-Traffic        | Prioritize   | All WAN   | ↑ None<br>↓ None | Network VLAN 40<br>VLAN 50                       | Any               | Any                                      | Always   | Publishing traffic, Online Services traffic  |

| Name                | QoS Behavior | Interface | Limits                  | Source          | Destination | Port | Schedule | Purpose                                                      |
|---------------------|--------------|-----------|-------------------------|-----------------|-------------|------|----------|--------------------------------------------------------------|
| MSPUB-Guest-Network | Limit        | All WAN   | ↑ 25 Mbps<br>↓ 100 Mbps | Network VLAN 80 | Any         | Any  | Always   | Guest network traffic, lower priority with limited bandwidth |

1. On the left toolbar click “Settings,” then click “Policy Table.”

The screenshot shows the UniFi Network Settings interface. The left sidebar has a 'Policy Table' option highlighted with a red arrow. The main content area displays a table of existing policies and two other sections: 'Internet' and 'Network Lists'.

| Name            | VLAN ID | Router     | Subnet             | IPv6 Subnet | DHCP   |
|-----------------|---------|------------|--------------------|-------------|--------|
| Default         | 1       | MSPUB-UDMP | 192.168.1.0/24     | -           | Server |
| Infrastructure  | 10      | MSPUB-UDMP | 192.168.10.0/29    | -           | Server |
| Servers         | 20      | MSPUB-UDMP | 192.168.20.0/29    | -           | Server |
| Administration  | 30      | MSPUB-UDMP | 192.168.30.0/29    | -           | Server |
| Publishing      | 40      | MSPUB-UDMP | 192.168.40.0/29    | -           | Server |
| Online Services | 50      | MSPUB-UDMP | 192.168.50.0/30    | -           | Server |
| IT-Cyber        | 60      | MSPUB-UDMP | 192.168.60.0/28    | -           | Server |
| Guest           | 80      | MSPUB-UDMP | 192.168.80.0/24    | -           | Server |
| Blackhole       | 255     | MSPUB-UDMP | 192.168.255.252/30 | -           | None   |

| Name         | Interface | ISP         | IPv4 Address   | IPv6 Address | Port | Uptime |
|--------------|-----------|-------------|----------------|--------------|------|--------|
| Primary WAN  | WAN1      | Zipty Fiber | 10.206.20.7    | -            | 10   | 100%   |
| Fallover WAN | WAN2      | Zipty Fiber | 172.16.216.133 | -            | 9    | 100%   |

| Name                              | Type | Values                                                      | Count |
|-----------------------------------|------|-------------------------------------------------------------|-------|
| Internal Network - Infrastruct... | IPv4 | 192.168.... 192.168.... 192.168.... 192.168.... 192.168.... | 6     |

2. Click “Create New Policy” towards the upper-left and configure the following:

- Policy Type: **QoS**
- Name: **MSPUB-Critical-Infrastructure**
- QoS Behavior: **Prioritize**
- Interface: **All WAN**
- Download Limit: **None**
- Upload Limit: **None**
- Source: **Network**
  - **Servers (20)**
  - **IT-Cyber (60)**
- Destination: **Any**
- Port: **Any**
- Schedule: **Always**
- Click: **Add**

## Part 3: Network Fundamentals & Administration

The image displays five screenshots of the QoS Policies configuration interface, arranged in two rows. Each screenshot shows a different policy configuration, with red arrows highlighting specific settings.

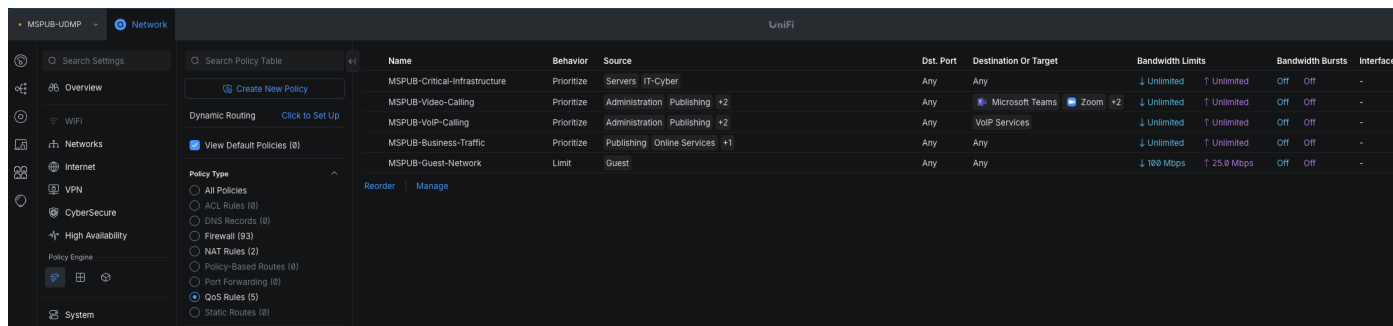
**Top Row:**

- MSPUB-Critical-Infrastructure:** The Name field is highlighted with a red arrow. The QoS Behavior section shows 'Prioritize' selected. The Source section shows 'Network' selected, and the Source list includes 'Servers (20)' and 'IT-Cyber (60)'. The Destination section shows 'Any' selected. The Schedule section shows 'Always' selected.
- MSPUB-VoIP-Calling:** The Name field is highlighted with a red arrow. The QoS Behavior section shows 'Prioritize' selected. The Source section shows 'Network' selected, and the Source list includes 'Administration (30)', 'Publishing (40)', 'Online Services (50)', and 'IT-Cyber (60)'. The Destination section shows 'App' selected. The Schedule section shows 'Always' selected.
- MSPUB-VoIP-Video-Calling:** The Name field is highlighted with a red arrow. The QoS Behavior section shows 'Prioritize' selected. The Source section shows 'Any' selected. The Destination section shows 'App' selected, and the Destination list includes 'Microsoft Teams', 'Zoom', 'Webex', and 'Google Meet'. The Schedule section shows 'Always' selected.

**Bottom Row:**

- MSPUB-Business-Traffic:** The Name field is highlighted with a red arrow. The QoS Behavior section shows 'Prioritize' selected. The Source section shows 'Network' selected, and the Source list includes 'Publishing (40)', 'Online Services (50)', and 'Administration (30)'. The Destination section shows 'Any' selected. The Schedule section shows 'Always' selected.
- MSPUB-Guest-Network:** The Name field is highlighted with a red arrow. The QoS Behavior section shows 'Limit' selected. The Interface section shows 'All WANs' selected. The Download Limit section shows '100 Mbps' selected. The Upload Limit section shows '25 Mbps' selected. The Source section shows 'Network' selected, and the Source list includes 'Guest (80)'. The Destination section shows 'Any' selected. The Schedule section shows 'Always' selected.

3. Repeat step 2 to create the remaining policies in the QoS Policies Table above.



## Configuring UniFi Wireless Access Points (WAPs)

### Scenario

Master Sword Publishing requires a secure wireless infrastructure to provide connectivity for employees, contractors, and guest. The wireless solution must support multiple departments while ensuring guest traffic remains isolated from internal business resources. The MSPUB IT Department will deploy UniFi Access Points utilizing WPA3 security, VLAN segmentation, and guest network controls.

### Objective

Deploy and configure wireless access points that provide secure employee wireless access and isolated guest connectivity while integrating with the MSPUB segmented network architecture.

### Equipment Being Used

- 2 UniFi WiFi 6 Pro PoE+ Access Points
  - Connected to MSPUB-USW24P-SW01
  - Powered by PoE+

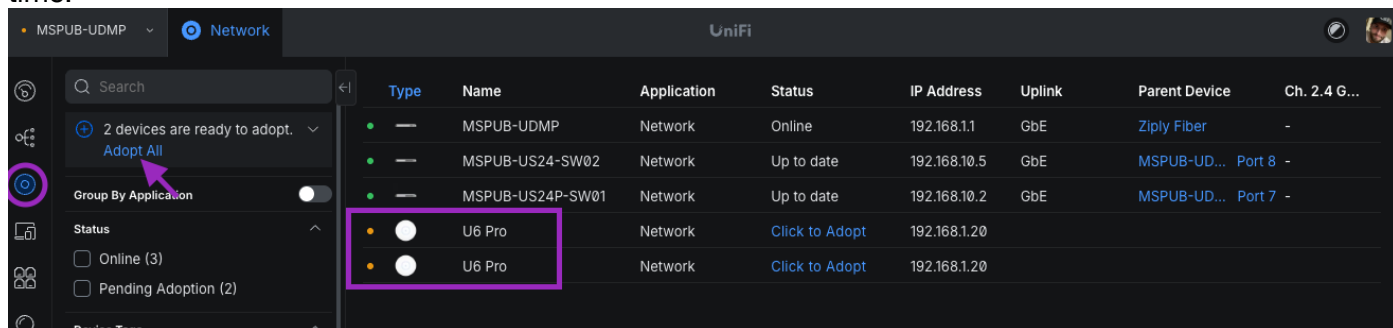
### Wireless Networks

| SSID        | Encryption Method    | Password        | Supported VLANs |
|-------------|----------------------|-----------------|-----------------|
| MSPUB-HQ    | WPA2/WPA3 - Personal | Hyrul3W@rr10r\$ | 30, 40, 50, 60  |
| MSPUB-Guest | Captive Portal       | M4\$t3r_5w0rd   | 80              |

### Adopting UniFi Wireless Access Points

Adopting the UniFi Access Points has to be done first before the wireless networks can be configured.

1. On the UniFi OS Console, click “UniFi Devices” on the left toolbar. There are two U6 Pro access points pending adoption. Click the the “Adopt All” hyperlink towards the upper-left to adopt both at the same time.

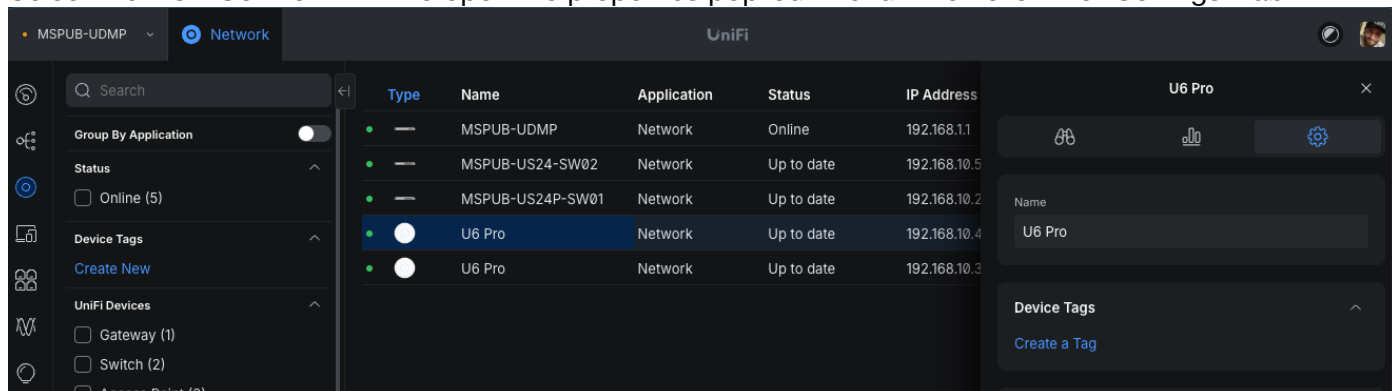


## Part 3: Network Fundamentals & Administration

2. The Access Points will begin adopting to the network.

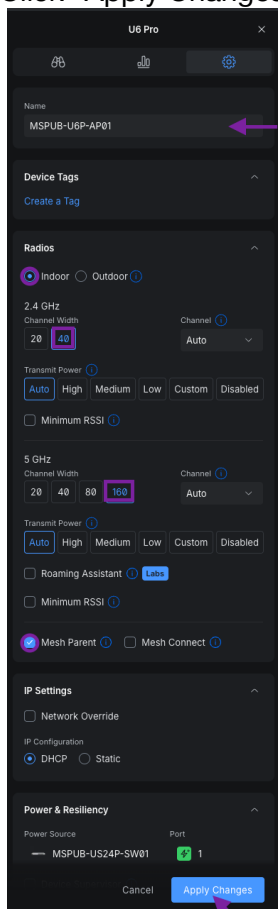
|                                                                                   |                                                                                   |        |         |               |              |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------|---------|---------------|--------------|
|  |  | U6 Pro | Network | Getting Ready | 192.168.10.4 |
|  |  | U6 Pro | Network | Getting Ready | 192.168.10.3 |

3. Select the first “U6 Pro” WAP to open the properties pop-out menu. Then click the “Settings” tab.



| Type    | Name             | Application | Status     | IP Address   |
|---------|------------------|-------------|------------|--------------|
| Network | MSPUB-UDMP       | Network     | Online     | 192.168.1.1  |
| Network | MSPUB-US24-SW02  | Network     | Up to date | 192.168.10.5 |
| Network | MSPUB-US24P-SW01 | Network     | Up to date | 192.168.10.2 |
| Network | U6 Pro           | Network     | Up to date | 192.168.10.4 |
| Network | U6 Pro           | Network     | Up to date | 192.168.10.3 |

4. Configure this AP with the following settings:
- Name: **MSPUB-U6P-AP01**
  - Radios: **Indoor**
  - 2.4 GHz Channel Width: **40**
  - 5 GHz Channel Width: **160**
  - Enable: **Mesh Parent**
  - Leave the remaining defaults selected.
  - Click “Apply Changes” once configured.



U6 Pro

Name: MSPUB-U6P-AP01

Device Tags: Create a Tag

Radios: Indoor (selected), Outdoor

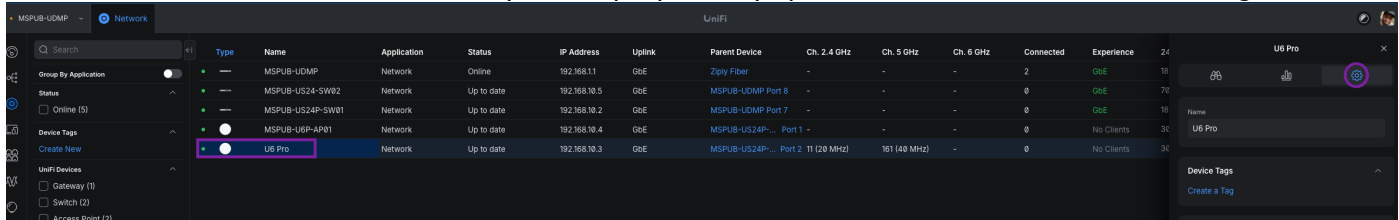
2.4 GHz Channel Width: 40 (selected), 20, 80, 160

5 GHz Channel Width: 160 (selected), 20, 40, 80

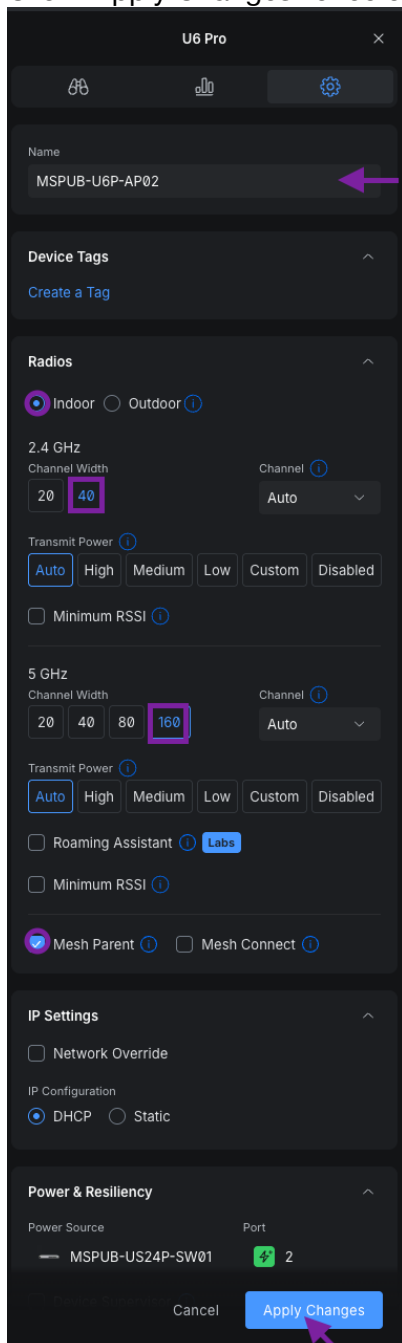
Mesh Parent: (selected), Mesh Connect

Apply Changes

5. Select the second “U6 Pro” WAP to open the properties pop-out menu. Then click the “Settings” tab.



6. Configure this AP with the following settings:
- Name: **MSPUB-U6P-AP02**
  - Radios: **Indoor**
  - 2.4 GHz Channel Width: **40**
  - 5 GHz Channel Width: **160**
  - Enable: **Mesh Parent**
  - Leave the remaining defaults selected.
  - Click “Apply Changes” once configured.



- The physical UniFi Wireless Access Points have been successfully adopted and configured. Wireless networks can now be created.

| Type | Name             | Application | Status     | IP Address   | Uplink | Parent Device                      | Ch. 2.4 GHz | Ch. 5 GHz    | Ch. 6 GHz | Connected | Experience | 24h Usage | Download    | Upload     |
|------|------------------|-------------|------------|--------------|--------|------------------------------------|-------------|--------------|-----------|-----------|------------|-----------|-------------|------------|
| ●    | MSPUB-UDMP       | Network     | Online     | 192.168.1.1  | GbE    | Ziply Fiber                        | -           | -            | -         | 2         | GBE        | 179 MB    | ↓ 19.5 Kbps | ↑ 319 Kbps |
| ●    | MSPUB-US24-SW02  | Network     | Up to date | 192.168.10.5 | GbE    | MSPUB-UDMP Port 8                  | -           | -            | -         | 0         | GBE        | 68.6 MB   | ↓ 0 bps     | ↑ 0 bps    |
| ●    | MSPUB-US24P-SW01 | Network     | Up to date | 192.168.10.2 | GbE    | MSPUB-UDMP Port 7                  | -           | -            | -         | 0         | GBE        | 184 MB    | ↓ 186 Kbps  | ↑ 114 Kbps |
| ●    | MSPUB-U6P-AP01   | Network     | Up to date | 192.168.10.4 | GbE    | MSPUB-US24P-... Port 1 6 (40 MHz)  | -           | 64 (160 MHz) | -         | 0         | No Clients | 304 B     | ↓ 172 Kbps  | ↑ 600 Kbps |
| ●    | MSPUB-U6P-AP02   | Network     | Up to date | 192.168.10.3 | GbE    | MSPUB-US24P-... Port 2 11 (40 MHz) | -           | 64 (160 MHz) | -         | 0         | No Clients | 304 B     | ↓ 173 Kbps  | ↑ 601 Kbps |

## Configuring Wireless Networks in UniFi OS

The MSPUB Wireless Network will consist of two SSIDs. One for MSPUB Employees and another for Guests. Both will be secured by a password. MSPUB-HQ will use WPA3 security encryption standards and MSPUB-Guest will require the password to be entered on a captive portal.

### MSPUB-HQ Configuration

- In the UniFi OS console click “Settings” on the left toolbar and select WiFi. Then click “Create New.”

The screenshot shows the UniFi OS console interface. On the left sidebar, the 'WiFi' option is highlighted with a purple box. The main content area displays the 'Create New' button for a new WiFi network. Below this, the 'Channel Plan' section shows the configuration for 2.4 GHz and 5 GHz bands. The 2.4 GHz band is set to 20 MHz channels, and the 5 GHz band is set to 40 MHz channels. The 'Default WiFi Speeds' are set to 'Conservative'. The 'Channel Width (MHz)' section shows the configuration for 2.4 GHz, 5 GHz, and 6 GHz bands. The 5 GHz band is set to 40 MHz channels. The '5 GHz Roaming Assistant' section shows the configuration for the roaming assistant, with the threshold set to -75 dBm.

- In the Create New WiFi properties pop-out menu configure the following:

- Name: **MSPUB-HQ**
- Password: **Hyrul3W@rr10r\$**
- Network: **Native Network**
- Broadcasting APs: **All**
- Application: **Standard**
- Radio Band: **2.4 GHz, 5 GHz**
- Enable: **Multicast to Unicast**
- Security Protocol: **WPA2/WPA3**
- Enable: **Band Steering**



## Part 3: Network Fundamentals & Administration

- Enable: **BBS Transition**
- Enable: **MAC address Filter**
  - Add a clients MAC address to allow them to connect
- Click “Create”

**Create New WiFi**

Name: MSPUB-HQ

Password: [Redacted]

Network: Native Network

Broadcasting APs: All

Application: Standard

Radio Band: 2.4 GHz, 5 GHz

Advanced: Auto Manual

Roaming Assistance: Fast Roaming (802.11r)

**Security**

Security Protocol: WPA3

PMF: Required

WPA3 enforces PMF, which may disconnect legacy or IoT clients. To avoid this, we strongly recommend a separate WPA2 broadcast with PMF disabled.

Private Pre-Shared Keys: [Off]

Hide WiFi Name: [Off]

Client Device Isolation: [Off]

SAE Anti-clogging: 5

SAE Sync Time: 5

**Behavior Controls**

Band Steering: [On]

BSS Transition: [On]

UAPSD: [Off]

MAC Address Filter: [On]

Filter Type: Allow

e.g. ab:cd:ef:12:34:56 Add

Add Multiple Add Client

MAC Address: a6:f5: [Redacted] Edit

Clear

RADIUS MAC Authentication: [Off]

WiFi Speed Limit: [Off]

Auto 802.11 DTIM Period: [On]

Group Rekey Interval: [Off]

Show Access Point Name in Beacon: [Off]

WiFi Blackout Schedule: Off On

### MSPUB-Guest Configuration

1. Click “Create New” under WiFi.

| Name     | Network        | Broadcasting APs | Radio Band    | Clients | Security |
|----------|----------------|------------------|---------------|---------|----------|
| MSPUB-HQ | Native Network | All APs          | 2.4 GHz 5 GHz | -       | WPA3     |

Create New Manage

3. In the Create New WiFi properties pop-out menu configure the following:

- Name: **MSPUB-Guest**
- Network: **Guest 80**
- Broadcasting APs: **All**
- Application: **Hotspot**
- Radio Band: **2.4GHz**
- Hotspot Type: **Captive Portal**
- Advanced: **Manual**
- Security Protocol: **Open**
- Security Mode: **Enhanced Open (OWE)**
- **Enable**: Client Device Isolation
- **Enable**: BBS Transition
- Click “Create”

**Create New WiFi**

Name: MSPUB-Guest

Password: [Redacted]

Network: Guest

Broadcasting APs: All

Application: Hotspot

Radio Band: 2.4 GHz

Hotspot Type: Captive Portal

Advanced: Auto Manual

**Security**

Security Protocol: Open

Security Mode: Enhanced Open (OWE)

PMF: Required

Private Pre-Shared Keys: [Off]

Hide WiFi Name: [Off]

Client Device Isolation: [On]

**Behavior Controls**

Band Steering: [On]

BSS Transition: [On]

UAPSD: [Off]

MAC Address Filter: [On]

RADIUS MAC Authentication: [Off]

WiFi Speed Limit: [Off]

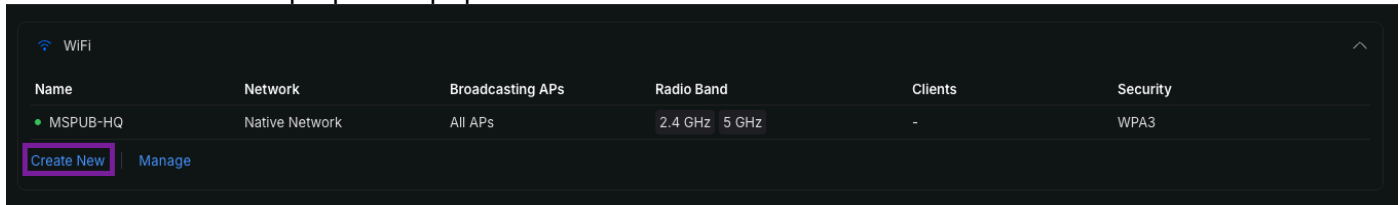
Auto 802.11 DTIM Period: [On]

Show Access Point Name in Beacon: [Off]

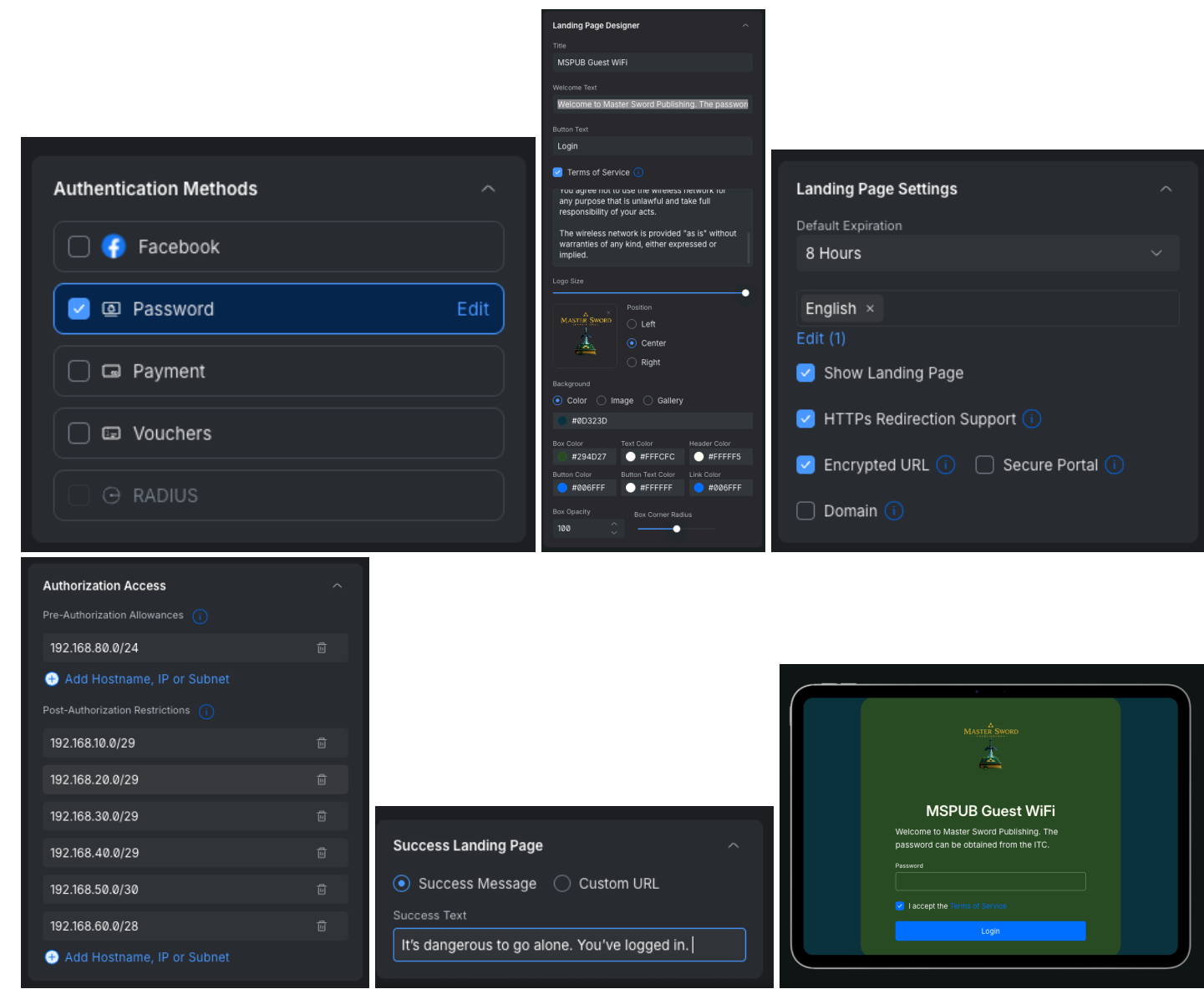
WiFi Blackout Schedule: Off On

Cancel Create

4. To create the Captive Portal select “MSPUB-Guest” WiFi network and click the hyperlink “Hotspot Portal” in the MSPUB-Guest properties pop-out menu.



5. On the Captive Portal configuration page configure the following:
- Authentication Methods: **Password**
    - Set password to: **M4\$t3r\_5w0rd**
  - Landing Page:
    - Title: **MSPUB Guest WiFi Login**
    - Welcome text: **Welcome to Master Sword Publishing. The password can be obtained from the ITC.**
    - **Enable:** Terms of Service
    - Upload the MSPUB logo by click the blue U and navigating the where the logo is located in your files.
    - Background Color: #0D323D
    - Box Color: #294D27
    - Text Color: #FFFCFC
    - Header Color: #FFFFFF5
    - Button Color: #006FFF
    - Button Text Color: #FFFFFFF
    - Link Color: #006FFF
  - Landing Page Settings:
    - Default Expiration: **8 Hours**
    - **Enable:** Show Landing Page
    - **Enable:** HTTPs Redirection Support
    - **Enable:** Encrypted URL
  - Authorization Access:
    - Pre-Authorization Allowances:
      - 192.168.20.0/24
    - Post-Authorization Restrictions:
      - 192.168.10.0/29
      - 192.168.20.0/29
      - 192.168.30.0/29
      - 192.168.40.0/29
      - 192.168.50.0/30
      - 192.168.60.0/28
  - Success Landing Page:
    - Select: **Success Message**
    - Success Message: **It's dangerous to go alone. You've logged in.**



Testing Network Elements

Device List

The device list shows that all VLANs are being connected to whether a device is connected via Ethernet or WiFi. And DHCP is assigning them to the correct VLAN IP address.

| Name                | Vendor          | Connection               | Network         | WiFi        | Experience | Technology  | Channel              | IP Address      |
|---------------------|-----------------|--------------------------|-----------------|-------------|------------|-------------|----------------------|-----------------|
| 7e:fe:0c:ea:33:23   | -               | -                        | -               | -           | -          | -           | -                    | -               |
| Apple MacBook 69:90 | Apple, Inc.     | MSPUB-U6P-AP01           | Guest           | MSPUB-Guest | Excellent  | WiFi 6, 2x2 | 11 (2.4 GHz, 20 MHz) | 192.168.80.78   |
| iPad 43:8c          | -               | MSPUB-U6P-AP01           | Default         | MSPUB-HQ    | Excellent  | WiFi 6, 2x2 | 11 (2.4 GHz, 20 MHz) | 169.254.225.201 |
| MSPUB-GLEEOK-DC01   | Microsoft Corp. | MSPUB-US24P-SW01 Port 17 | Servers         | -           | Excellent  | GbE         | -                    | 192.168.20.4    |
| MSPUB-MAC-ITC-WS    | Apple, Inc.     | MSPUB-US24-SW02 Port 11  | IT-Cyber        | -           | Excellent  | GbE         | -                    | 192.168.60.2    |
| MSPUB-UBT-OLS-WS    | Apple, Inc.     | MSPUB-US24-SW02 Port 1   | Online Services | -           | Excellent  | GbE         | -                    | 192.168.50.2    |
| MSPUB-WIN-ADM-WS    | Microsoft Corp. | MSPUB-U6P-AP01           | Administration  | MSPUB-HQ    | Excellent  | WiFi 5, 3x3 | 64 (5 GHz, 80 MHz)   | 192.168.30.2    |
| MSPUB-WIN-PUB-WS    | Microsoft Corp. | MSPUB-U6P-AP01           | Publishing      | MSPUB-HQ    | Excellent  | WiFi 6, 2x2 | 64 (5 GHz, 160 MHz)  | 192.168.40.3    |

## Part 3: Network Fundamentals & Administration

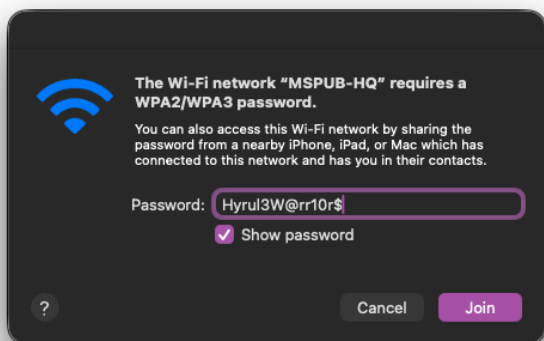
Trying to ping a device on the guest network fails, as expected.

```
jmanum -- -zsh -- 80x24
jmanum@00INRAAL ~ % ping -c 5 192.168.80.78
PING 192.168.80.78 (192.168.80.78): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3

--- 192.168.80.78 ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
jmanum@00INRAAL ~ %
```

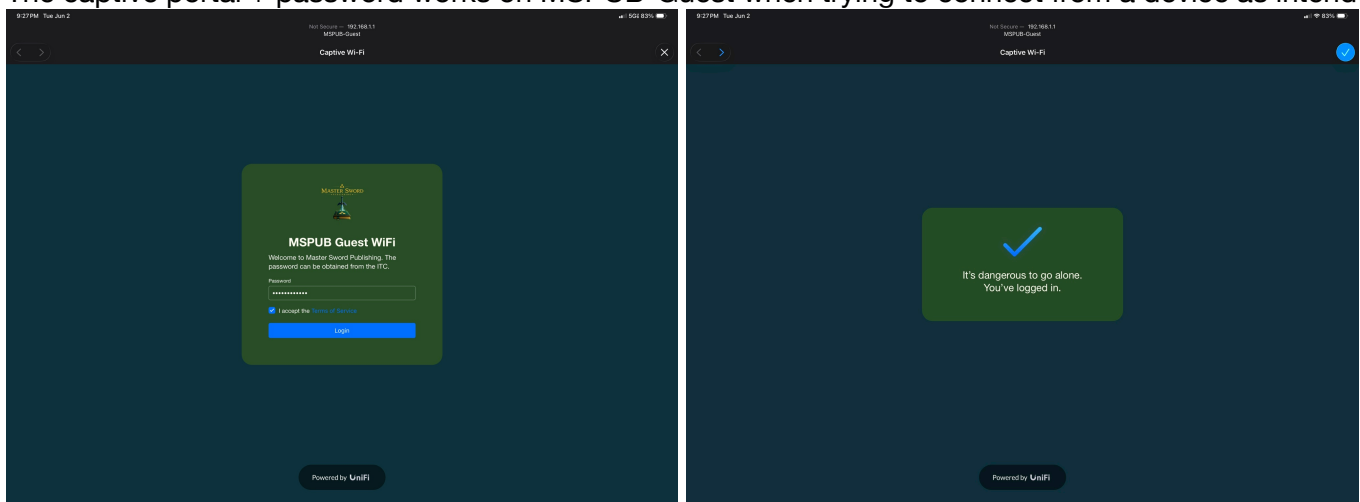
### MSPUB-HQ

Connecting to MSPUB-HQ it is connecting using the correct WPA2/WPA3 encryption method.



### MSPUB-Guest

The captive portal + password works on MSPUB-Guest when trying to connect from a device as intended.



### Download the Config File

UniFi doesn't allow for downloading of individual profiles per device. The entire UniFi OS Backup is the alternative which will include switches, routers, and WAP configurations. Download Link: [MSPUB-UniFiOS-Config.unifi](#)

# Master Sword Publishing's Security Awareness Campaign & Incident Response Plan

## Overview

*\*FILL OUT LATER\**

## Security Awareness Campaign

### Scenario

Link Hero, MSPUB's Cybersecurity Administrator, has identified phishing as one of the organization's greatest security risks. Because employees routinely communicate with authors, editors, vendors, and customers through email, phishing attacks represent a significant threat to the company's systems and data. To evaluate employee awareness and improve organizational security, MSPUB will conduct a simulated phishing campaign and provide additional security awareness training.

### Objective

Develop and implement a security awareness initiative that educates employees on phishing attacks, social engineering techniques, password security, and safe computing practices.

### Phishing Email Campaign Details

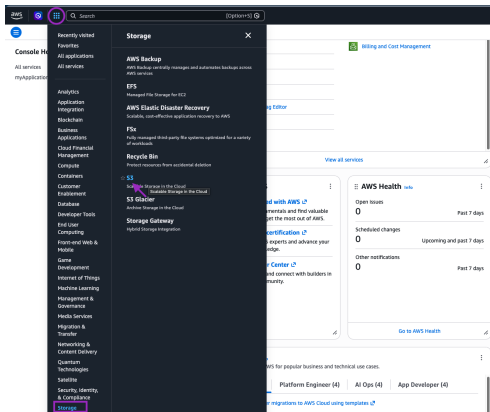
- URGENT: Microsoft 365 Password Expiration Notice
  - From: **micr0soft365-administrator@masterswordpublishing.jaycemangum.com**
- Fake Malicious Link
  - Fake Login Page
  - Employee Training Page after login
    - Phishing Test
    - Password Management
    - MFA
    - Safe Browsing Habits
    - What to look out for
- Results Tracking Table

### Configuring AWS Resources for Fake Login

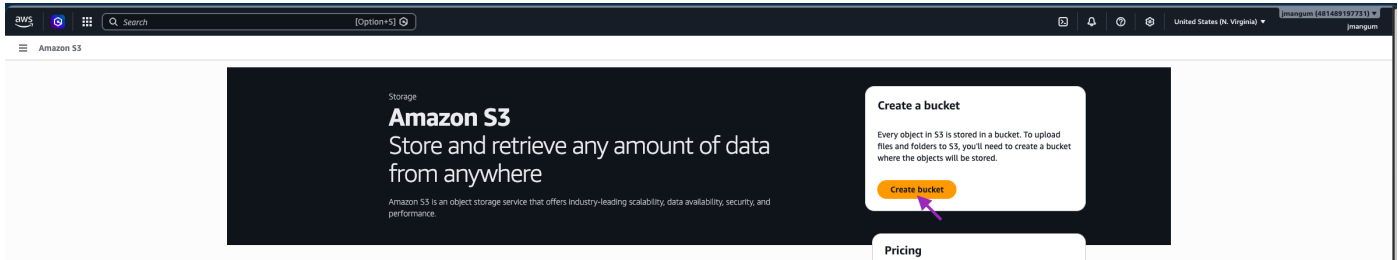
The phishing landing page as well as the employee training material will be hosted using an Amazon Web Services S3 Static Website. To configure the static site do the following:

1. In the AWS Console click the "Resources menu" to the left of search field. Select "Storage" on the left pane then click "S3."

## Part 4: Network Security and Encryption & Server Administration



### 2. Under “Create a bucket” click the “Create bucket” button.



### 3. Configure the following on the Create bucket page:

- Bucket Type: **General purpose**
- Bucket namespace: **Global namespace**
- Bucket name: **mspub-security-awareness-training**
- Object Ownership: **ACLs disabled**
- **Deselect:** Block all public access
  - **Select:** I acknowledge that the current settings might result in this bucket and the objects within becoming public.
- Leave the remaining settings as their defaults
- Click the “Create Bucket” button

Create bucket [help](#)

Buckets are containers for data stored in S3.

**General configuration**

**AWS Region**  
US West (Oregon) us-west-2

**Bucket type** [help](#)

☒ **General purpose**  
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**  
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

**Bucket namespace**  
Choose the namespace where you want to create your bucket. [Learn more](#)

☒ **Global namespace**  
By default, S3 stores general purpose buckets in the global namespace.

☐ **Account Regional namespace (recommended)**  
General purpose buckets created in your account Regional namespace are unique to your account. These buckets can never be created by another AWS account.

**Bucket name** [help](#)

mspub-security-awareness-training

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn more](#)

**Copy settings from existing bucket - optional**  
Copy the bucket settings on the following configuration are copied.

[Choose bucket](#)

Format: s3://bucketname

**Object Ownership** [help](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

**Object Ownership**  
Bucket owner enforced

## Part 4: Network Security and Encryption & Server Administration

**Block Public Access settings for this bucket**

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

**Bucket Versioning**

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

**Bucket Versioning**

☒ Disable  
☐ Enable

**Tags - optional**

You can use bucket tags to analyze, manage and specify permissions for a bucket. [Learn more](#)

**You can use s3:ListTagsForResource, s3:TagResource, and s3:UntagResource APIs to manage tags on S3 general purpose buckets for access control in addition to cost allocation and resource organization. To ensure a seamless transition, please provide permissions to s3:ListTagsForResource, s3:TagResource, and s3:UntagResource actions. [Learn more](#)**

No tags associated with this bucket.

[Add new tag](#)

You can add up to 50 tags.

**Default encryption** [info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

**Encryption type** [info](#)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)  
☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)  
☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

**Bucket Key**  
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable  
☒ Enable

▼ **Advanced settings**

**Object Lock**  
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

☒ Disable  
☐ Enable  
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

**Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.**

**After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.**

[Cancel](#) [Create bucket](#)

- Click the “Properties” tab on the mspub-securty-awareness-training page. Scroll down to the bottom to the Static website hosting card and click the “Edit” button.

### mspub-securty-awareness-training [info](#)

Objects | Metadata | **Properties** | Permissions | Metrics | Management | File systems - new | Access Points

#### Bucket overview

**AWS Region**  
US West (Oregon) us-west-2

**Amazon Resource Name (ARN)**  
[arn:aws:s3::mspub-securty-awareness-training](#)

**Creation date**  
June 4, 2026, 15:23:56 (UTC-07:00)

#### Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

**Requester pays**  
Disabled

[Edit](#)

#### Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

**We recommend using AWS Amplify Hosting for static website hosting**  
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [view your existing Amplify apps](#)

[Create Amplify app](#)

[Edit](#)

**S3 static website hosting**  
Disabled



## Part 4: Network Security and Encryption & Server Administration

5. On the Edit static website hosting page configure the following:

- Static website hosting: **Enable**
- Hosting Type: **Host a static website**
- Index document: **index.html**
- Click “Save Changes”

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

☐ Disable

☒ Enable

Hosting type

☒ Host a static website

Hosts the bucket endpoint as the web address. [Learn more](#)

☐ Redirect requests for an object

Redirects requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoints, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [using Amazon S3 Block Public Access](#).

Index document

Specify the name or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

JSON | List 1, Col 1 | Errors: 0 | Warnings: 0

Save changes

6. In the “Objects” tab, upload the “msup\_index.html” file created for the web server previously, and rename it to “index.html.” Also upload the login.html, user-failed-phishing-test.html, heart-container.html, and style.css files to the S3 Bucket.

mspub-security-awareness-training [Info](#)

Objects (5)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

| <input type="checkbox"/> | Name                                           | Type | Last modified                      | Size   | Storage class |
|--------------------------|------------------------------------------------|------|------------------------------------|--------|---------------|
| <input type="checkbox"/> | <a href="#">heart-container.html</a>           | html | June 4, 2026, 22:49:56 (UTC-07:00) | 1.4 KB | Standard      |
| <input type="checkbox"/> | <a href="#">index.html</a>                     | html | June 4, 2026, 17:47:08 (UTC-07:00) | 6.1 KB | Standard      |
| <input type="checkbox"/> | <a href="#">login.html</a>                     | html | June 4, 2026, 23:23:01 (UTC-07:00) | 1.2 KB | Standard      |
| <input type="checkbox"/> | <a href="#">style.css</a>                      | css  | June 4, 2026, 22:49:56 (UTC-07:00) | 4.1 KB | Standard      |
| <input type="checkbox"/> | <a href="#">user-failed-phishing-test.html</a> | html | June 4, 2026, 23:05:19 (UTC-07:00) | 2.5 KB | Standard      |

1

Upload

## Part 4: Network Security and Encryption & Server Administration

### 7. Click the “Permissions” tab and click “Edit” under “Bucket policy.”

**msspub-securirty-awareness-training** [Info](#)

Objects | Metadata | Properties | **Permissions** | Metrics | Management | File systems - new | Access Points

**Permissions overview**

**Access finding**  
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#). [View analyzer for us-west-2](#)

**Block public access (bucket settings)** [Edit](#)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

**Block all public access**  
 Off

► Individual Block Public Access settings for this bucket

**Bucket policy** [Edit](#) [Delete](#)

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

No policy to display. [Copy](#)

### 8. On the Edit bucket policy page under Policy enter the following:

```
{
 "Version": "2008-10-17",
 "Id": "PolicyForCloudFrontPrivateContent",
 "Statement": [
 {
 "Sid": "AllowCloudFrontServicePrincipal",
 "Effect": "Allow",
 "Principal": {
 "Service": "cloudfront.amazonaws.com"
 },
 "Action": "s3:GetObject",
 "Resource": "arn:aws:s3:::msspub-securirty-awareness-training/*",
 "Condition": {
 "StringEquals": {
 "AWS:SourceArn": "arn:aws:cloudfront::481489197731:distribution/E1BX3OEWAKNW7L"
 }
 }
 }
]
}
```

## Part 4: Network Security and Encryption & Server Administration

Click “Save changes”

Edit bucket policy [Info](#)

**Bucket policy**[Policy examples](#)

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

**Bucket ARN**  
 arn:aws:s3:::mspub-security-awareness-training

**Policy**

```
1 {
2 "Version": "2008-10-17",
3 "Id": "PolicyForCloudFrontPrivateContent",
4 "Statement": [
5 {
6 "Sid": "AllowCloudFrontServicePrincipal",
7 "Effect": "Allow",
8 "Principal": {
9 "Service": "cloudfront.amazonaws.com"
10 },
11 "Action": "s3:GetObject",
12 "Resource": "arn:aws:s3:::mspub-security-awareness-training/*",
13 "Condition": {
14 "StringEquals": {
15 "AWS:SourceArn": "arn:aws:cloudfront::481489197731:distribution/E1BX3OENAKNW7L"
16 }
17 }
18 }
19]
20 }
```

**Edit statement**

**Select a statement**

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

[+ Add new statement](#)

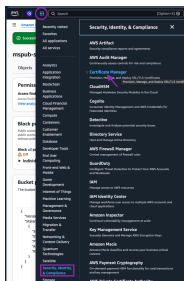
JSON Ln 20, Col 1

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0 [Preview external access](#)

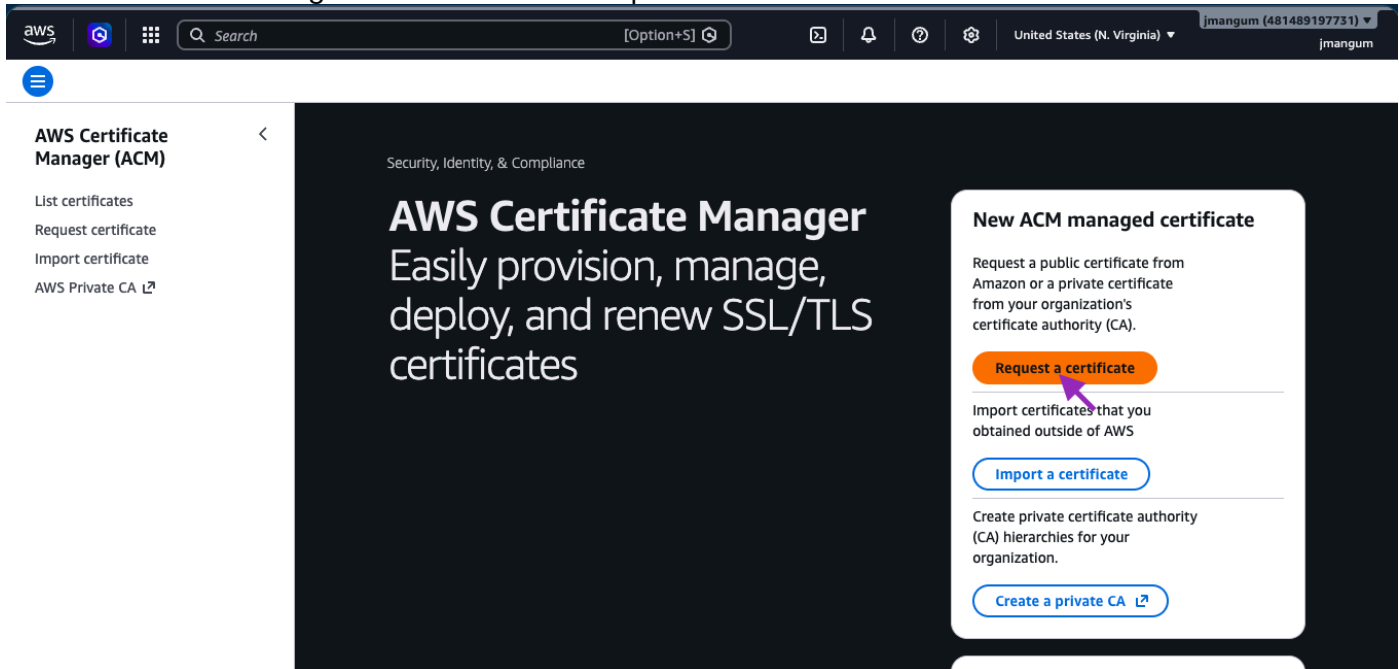
[Cancel](#) [Save changes](#)

A certificate will need to be created in Amazon Certificate Manger (ACM) to make the website look secured.

- Click the “Resources menu” next to the search field. Select “Security, Identity, & Compliance” then click “Certificate Manager.”



### 10. Under New ACM managed certificate click “Request a certificate.”



### 11. Select “Request a public certificate” then click “Next.”

#### Request certificate

**Certificate type** [Info](#)

ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for ACM to provide.

☒ **Request a public certificate**  
Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.

☐ Request a private certificate  
No private CAs available for issuance.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit [AWS Private Certificate Authority](#)

[Cancel](#) [Next](#)

### 12. On the Request public certificate page configure the following:

- Fully qualified domain name: **masterswordpub-net.jaycemangum.com**
- Allow export: **Disable export**
- Validation method: **DNS validation**
- Key algorithm: **RSA 2048**
- Click “Request”

**Request public certificate**

**Domain names** [Info](#)

Provide one or more domain names for your certificate.

**Fully qualified domain name** [Info](#)

masterswordpub-net.jaycemangum.com

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

**Allow export** [Info](#)

☒ **Disable export**  
Use this certificate only with integrated AWS services. The private key for this certificate will be distributed for exporting from AWS.

☐ Enable export  
Export this certificate and private key for use with any TLS workflow. ACM will charge your account based on the requested domains when the certificate is issued for the first time and for each renewal.

**Validation method** [Info](#)

Select a method for validating domain ownership.

☒ **DNS validation - recommended**  
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

☐ Email validation  
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

**Key algorithm** [Info](#)

Select an encryption algorithm. Some algorithms may not be supported by all AWS services.

☒ **RSA 2048**  
RSA is the most widely used key type.

☐ ECDSA P 256  
Equivalent in cryptographic strength to RSA 3072.

☐ ECDSA P 384  
Equivalent in cryptographic strength to RSA 7680.

**Tags** [Info](#)

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 tags.

[Cancel](#) [Previous](#) [Request](#)

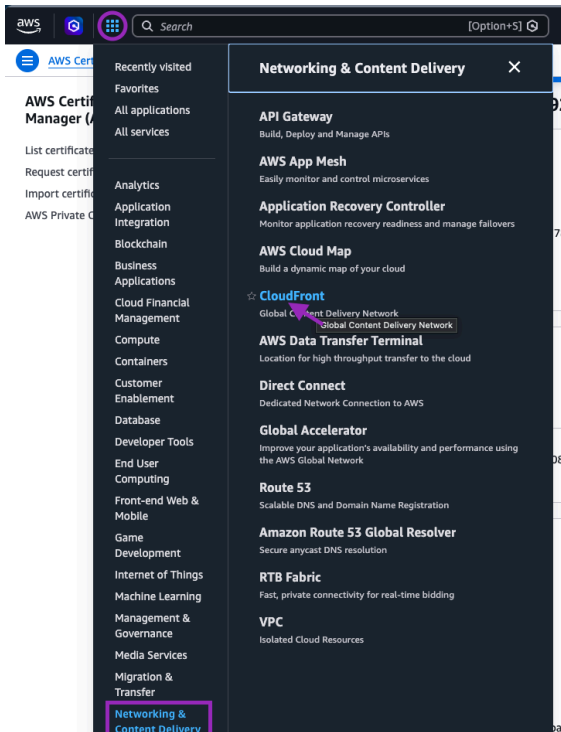
## Part 4: Network Security and Encryption & Server Administration

13. Take note of the information of the CNAME record in Domains tile.

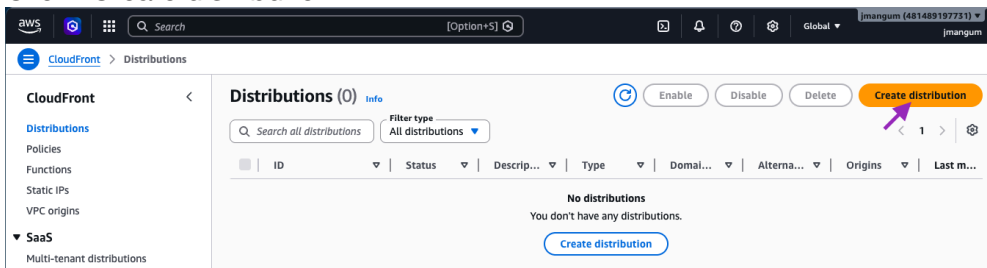
| Domains (1) |                                                                      |                                                                  | Create records in Route 53 | Export to CSV |
|-------------|----------------------------------------------------------------------|------------------------------------------------------------------|----------------------------|---------------|
| Type        | CNAME name                                                           | CNAME value                                                      |                            |               |
| CNAME       | _41bc09f33f4e6b9a158cdf9a48808bf.masterswordpub-net.jaycemangum.com. | _62c0154be4d4a7a78e5dbb7565558667.jkddztszm.acm-validations.aws. |                            |               |

To monitor metrics from the phishing site, CloudFront will be configured:

14. Click the “Resources menu” and click on “Networking & Content Delivery.” Then select “CloudFront.”



15. Click “Create distribution.”



16. On the Get started page configure the following:

- Distribution name: **MSPUB Security Awareness Training**
- **Select:** Single website or app

## Part 4: Network Security and Encryption & Server Administration

- Click “Skip domain setup”

Step 1: Get started (selected)  
Step 2: Specify origin  
Step 3: Enable security  
Step 4: Get TLS certificate  
Step 5: Review and create

### Get started

Connect your websites, apps, files, video streams, and other content to CloudFront. We optimize the performance, reliability, and security for your web traffic.

#### Distribution options

**Distribution name**  
Name will be stored as a tag on the resource. You can change the name, or more tags, later.  
MSPUB Security Awareness

**Description - optional**

**Distribution type**

☒ Single website or app  
Choose if each website or application will have a unique configuration.

☐ Multi-tenant architecture - New  
Choose when you have multiple domains that need to share configurations. This is a common architecture for SaaS providers.

#### Domain

**Route 53 managed domain - optional**  
Enter a domain that's already registered with Route 53 in your AWS account. CloudFront will provision a TLS certificate for you. If you have a domain from a different DNS provider, skip this step and configure your domain later.  
masterswordpub-net.jaycemangum.com [Check domain](#)

**You need to add this domain later**  
You can still create a distribution, but CloudFront can't automatically configure this domain. It might be registered in Route 53 in another AWS account, or with another domain registrar. [View our onboarding guide](#)

**Tags - optional**

[Cancel](#) [Skip domain setup](#)

### 17. Configure the following on Specify origin:

- Origin type: **Amazon S3**
- S3 origin: **mSPUB-security-awareness-training.s3.us-west-2.amazonaws.com**
- Origin path: index.html
- Leave the Settings as the defaults
- Click “Next”

### Specify origin

Your origin is where your content (such as a website or app) lives. CloudFront works with AWS-based origins and origins hosted on other cloud providers.

#### Origin type

☒ Amazon S3  
Deliver static assets like files and images, statically generated websites or single page applications (SPA).

☐ Elastic Load Balancing  
Deliver applications hosted behind ELB such as dynamic websites, web services, and APIs.

☐ API Gateway  
Deliver API endpoints for REST APIs hosted on API Gateway.

☐ Elemental MediaPackage  
Deliver end-to-end live events or video on demand (VOD).

☐ VPC origin  
Deliver applications and content hosted within private VPCs, such as EC2 instances and Application Load Balancers.

☐ Other  
Refer to any AWS or non-AWS origin through its publicly resolvable URL.

#### Origin

**S3 origin**  
Choose an AWS origin, or enter your origin's domain name. [Learn more](#)  
mSPUB-security-awareness-training.s3.us-west-2.amazonaws.com [Browse S3](#)

**This S3 bucket has static web hosting enabled.** If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint. [Use website endpoint](#)

**Origin path - optional**  
The directory path within your origin where your content is stored. [Learn more](#)  
/path

#### Settings

CloudFront provides default origin and cache settings based on what origin you selected. [View default settings for S3](#)

**Allow private S3 bucket access to CloudFront**  
CloudFront will update your S3 bucket policy to allow CloudFront to access your S3 bucket. The policy allows CloudFront to access the bucket only when the request is on behalf of the CloudFront distribution that contains the S3 origin.  
☒ Allow private S3 bucket access to CloudFront - Recommended

**Origin settings**  
Origin settings control how CloudFront connects to the specified origin.  
☒ Use recommended origin settings ☐ Customize origin settings

**Cache settings**  
Cache settings determine when CloudFront serves cached content and when it fetches new content from the origin.  
☒ Use recommended cache settings tailored to serving S3 content ☐ Customize cache settings

[Cancel](#) [Previous](#) [Next](#)

### 18. On the Enable security page select “Do not enable security protections” then click “Next.”

### Web Application Firewall (WAF)

☐ Enable security protections  
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

☒ Do not enable security protections  
Select this option if your application does not need security protections from AWS WAF.

[Cancel](#) [Previous](#) [Next](#)

### 19. On the Review and create page click “Create distribution.”

#### Review and create

#### General configuration

Distribution name

MSPUB Security Awareness

Description

-

Billing

Pay-as-you-go (\$0/month)

Edit

#### Origin

ⓘ

Because you granted CloudFront access to your origin, CloudFront can write and update S3 bucket policies that restrict access to your S3 origin to CloudFront.

S3 origin

msspub-security-awareness-training.s3.us-west-2.amazonaws.com

Origin path

-

Grant CloudFront access to origin

Yes

Enable Origin Shield

No

Connection attempts

3

Connection timeout

10

Edit

#### Cache settings

CloudFront will apply default cache settings tailored to serving content from a S3 origin. You can customize settings after you create your distribution.

Edit

#### Security

Security protections

None

Use monitor mode

No

Use existing WAF configuration

No

Edit

Cancel

Preview

Create distribution

### 20. Take note of the Distribution domain name

MSPUB Security Awareness

Standard

View metrics

#### Details

Distribution domain name

d3gvlgnv61nqv1.cloudfront.net

Billing

Pay-as-you-go

Switch to a plan

ARN

arn:aws:cloudfront::481489197731:distribution/E1BX3OEWAQNW7L

Last modified

Deploying

## Add the DNS Records from AWS to GoDaddy

### 1. Add a new CNAME record for the ACM certificate to the Domain DNS records.

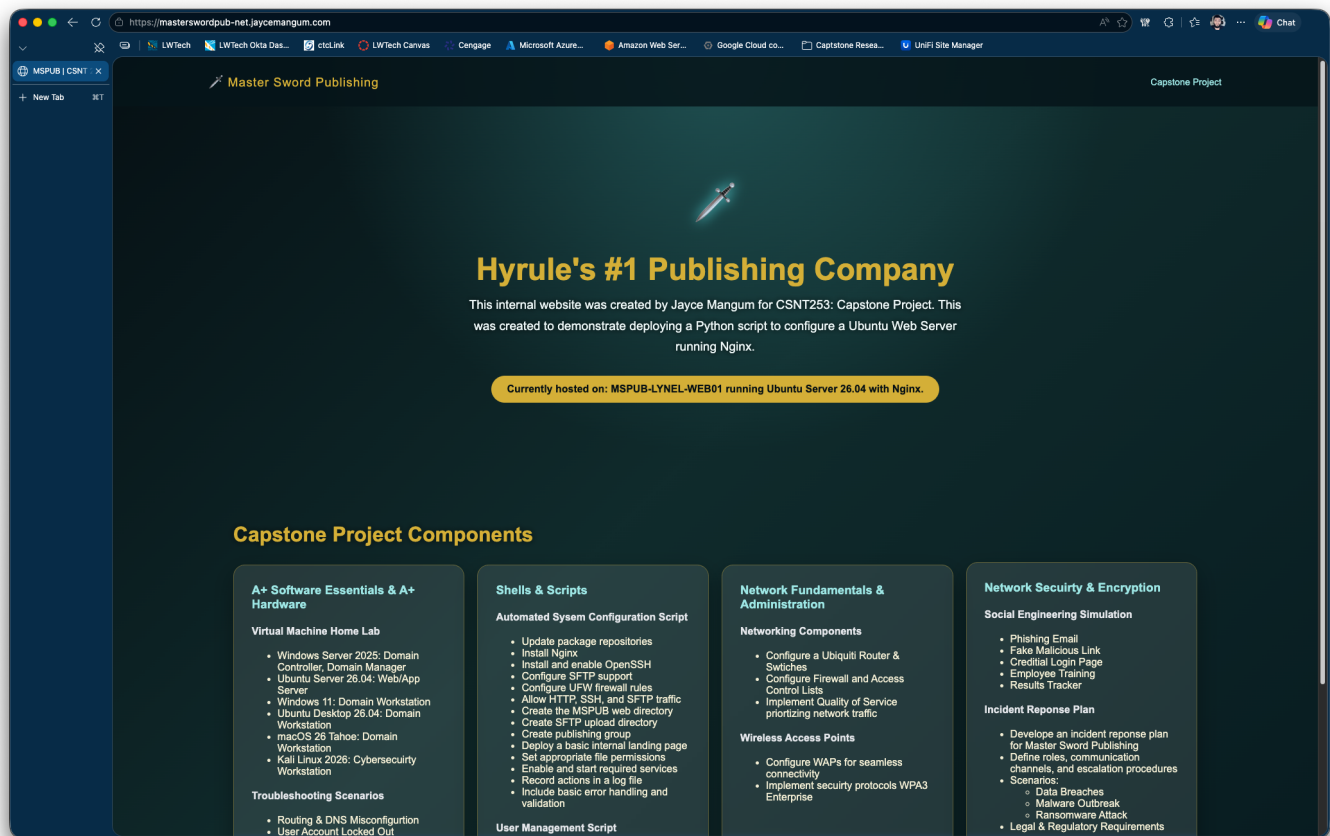
|                          |       |                                                         |                                                                      |        |  |  |
|--------------------------|-------|---------------------------------------------------------|----------------------------------------------------------------------|--------|--|--|
| <input type="checkbox"/> | CNAME | _41bc09f33f4e6b9a158cdf9a48<br>808bf.masterswordpub-net | _62c0154be4d4a7a78e5dbb756555866<br>7.jkddztszm.acm-validations.aws. | 1 Hour |  |  |
|--------------------------|-------|---------------------------------------------------------|----------------------------------------------------------------------|--------|--|--|

### 2. Add a new CNAME record with the following information from CloudWatch:

- Type: CNAME
- Name: masterswordpub-net
- Value: [CloudWatch Distribution domain name]

## Part 4: Network Security and Encryption & Server Administration

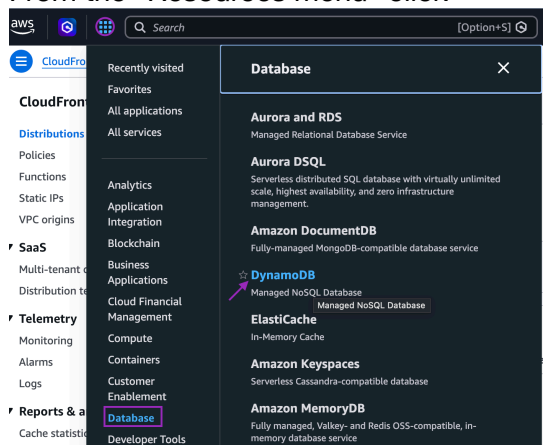
### 3. Test that the website resolves in a web browser.



## Logging Clicks with AWS Lambda

For metric cases click the button links will be recorded from users. No other information will be recorded from the login page.

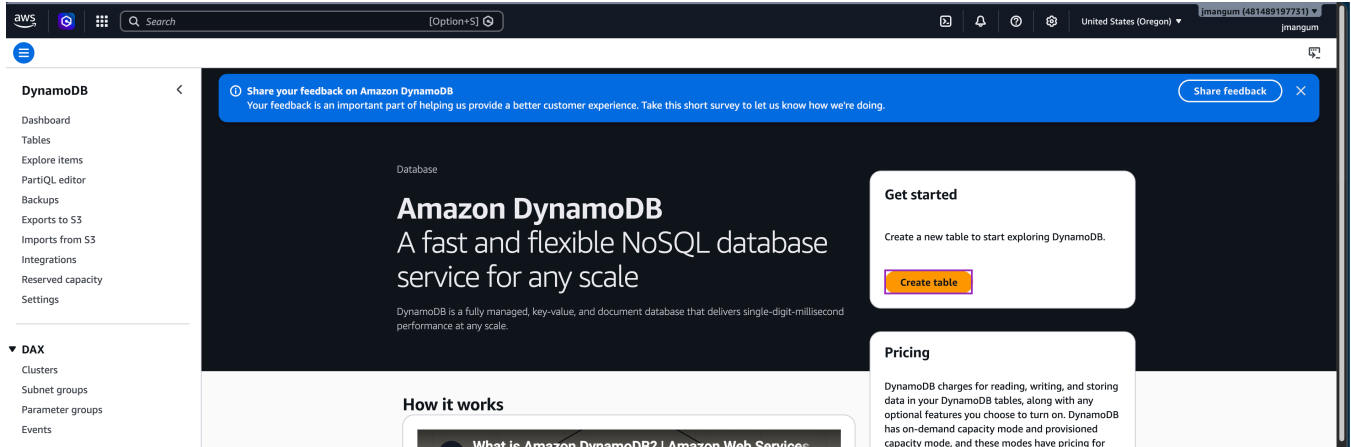
1. Create a DynamoDB Table within AWS:
  1. From the “Resources menu” click





## Part 4: Network Security and Encryption & Server Administration

### 2. Click “Create table.”



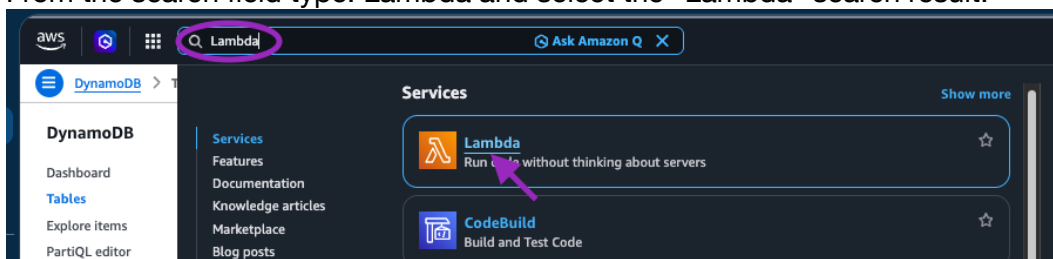
### 3. In the Create table page, configure the following:

- Table Name: MSPUB-SAT-2026-001-Results
- Partition key: event\_id
- Type: String
- Leave the remain settings as their defaults
- Click “Create table”

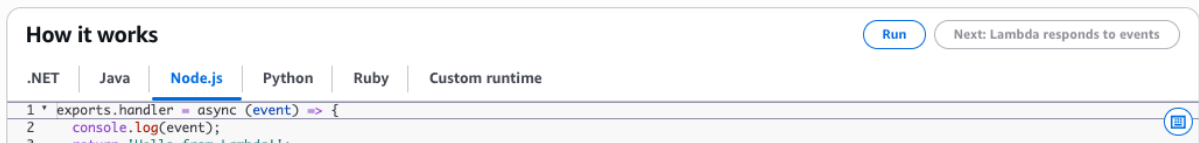
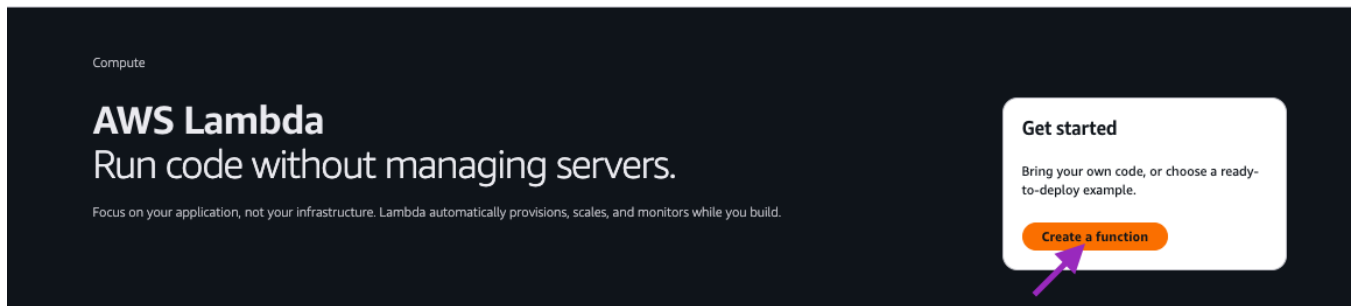
The screenshot shows the "Create table" configuration page. It has three main sections: "Table details", "Table settings", and "Tags". In the "Table details" section, the "Table name" is "MSPUB-SAT-2026-001-Results" and the "Partition key" is "event\_id" with a type of "String". The "Sort key - optional" is left empty. In the "Table settings" section, "Default settings" are selected. Below this is a table of default settings. In the "Tags" section, there is an "Add new tag" button. At the bottom right, there are "Cancel" and "Create table" buttons.

| Setting                      | Value             | Editable after creation |
|------------------------------|-------------------|-------------------------|
| Table class                  | DynamoDB Standard | Yes                     |
| Capacity mode                | On-demand         | Yes                     |
| Maximum read capacity units  | -                 | Yes                     |
| Maximum write capacity units | -                 | Yes                     |
| Local secondary indexes      | -                 | No                      |
| Global secondary indexes     | -                 | Yes                     |
| Encryption key management    | AWS owned key     | Yes                     |
| Deletion protection          | Off               | Yes                     |
| Resource-based policy        | Not active        | Yes                     |

### 4. From the search field type: Lambda and select the “Lambda” search result.



### 5. Click “Create a function.”

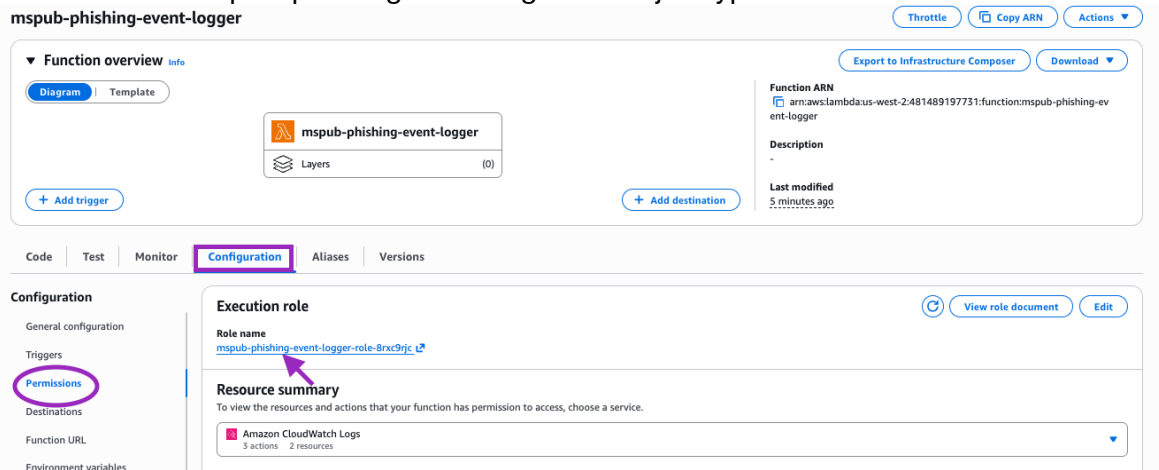


### 6. On the Create function page configure the following:

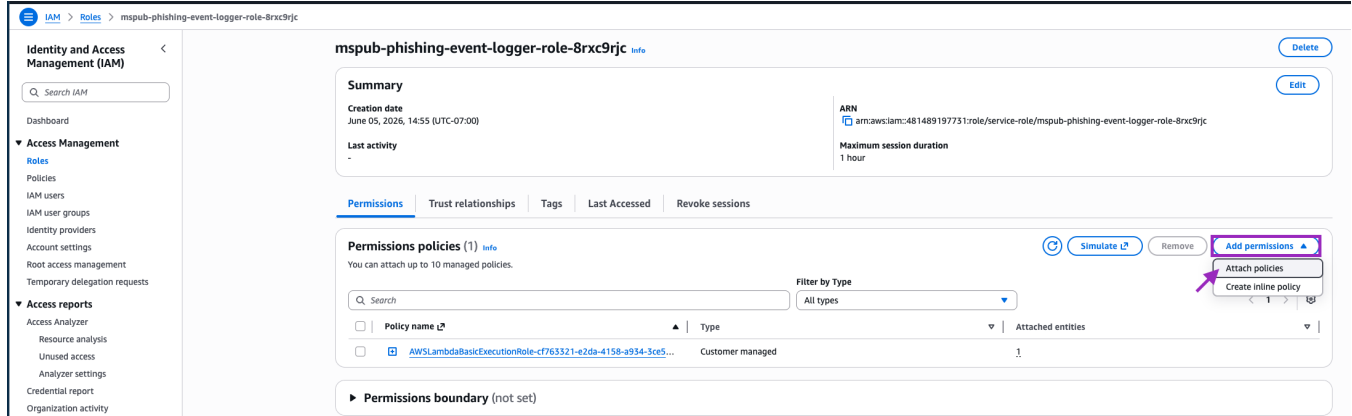
- **Select:** Author from scratch
- Function name: **msspub-phishing-event-logger**
- Partition key: **event\_id**
- Runtime: **Python 3.13**
- Click “Create function”

The image shows the 'Create function' page in the AWS Lambda console. It has a 'Choose one of the following options to create your function.' section with three radio buttons: 'Author from scratch' (selected), 'Use a blueprint', and 'Container image'. Below this is the 'Basic information' section with a 'Function name' field containing 'msspub-phishing-event-logger' and a 'Runtime' dropdown set to 'Python 3.13'. The 'Permissions' section has a note about the default execution role. The 'Custom settings' section has two toggle switches: 'Durable execution' and 'EC2 capacity provider'. At the bottom right are 'Cancel' and 'Create function' buttons.

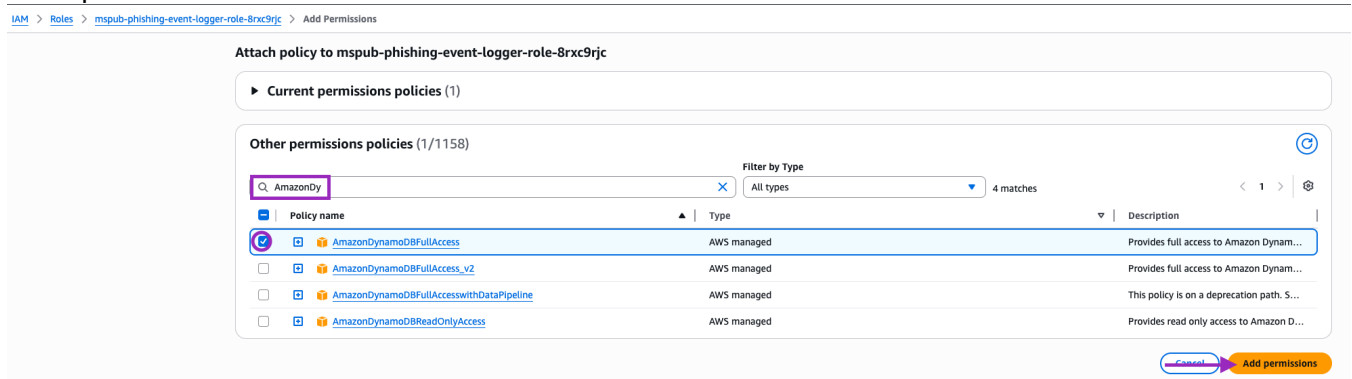
### 7. On the msspub-phishing-event-logger page click the “Configuration” tab, select “Permissions” on the left. Click the “msspub-phishing-event-logger-8rxc9rjc” hyper link under Role name.



- On the Identity and Access Management (IAM) page click “Add permissions,” then select “Attach policies.”



- In the search field type: “AmazonDynamo” and select “AmazonDynamoDBFullAccess.” Then click “Add permissions.”



- Back in the mspub-phishing-event-logger Lambda function click on Code and enter the following code into the “lambda\_fuction.py” text editor:

```
import json
import boto3
import uuid
from datetime import datetime, timezone
```

```
dynamodb = boto3.resource("dynamodb")
table = dynamodb.Table("MSPUB-SAT-2026-001-Results")
```

```
ALLOWED_ORIGIN = "https://masterswordpub-net.jaycemangum.com"
```

```
def response(status_code, body):
 return {
 "statusCode": status_code,
 "headers": {
 "Access-Control-Allow-Origin": ALLOWED_ORIGIN,
 "Access-Control-Allow-Headers": "content-type",
 "Access-Control-Allow-Methods": "OPTIONS,POST",
 "Content-Type": "application/json"
 },
 "body": json.dumps(body)
 }
```

```
def lambda_handler(event, context):
 try:
 method = event.get("requestContext", {}).get("http",
 {}).get("method", "")

 if method == "OPTIONS":
 return response(200, {"status": "cors_ok"})

 body = event.get("body") or "{}"

 if isinstance(body, str):
 body = json.loads(body)

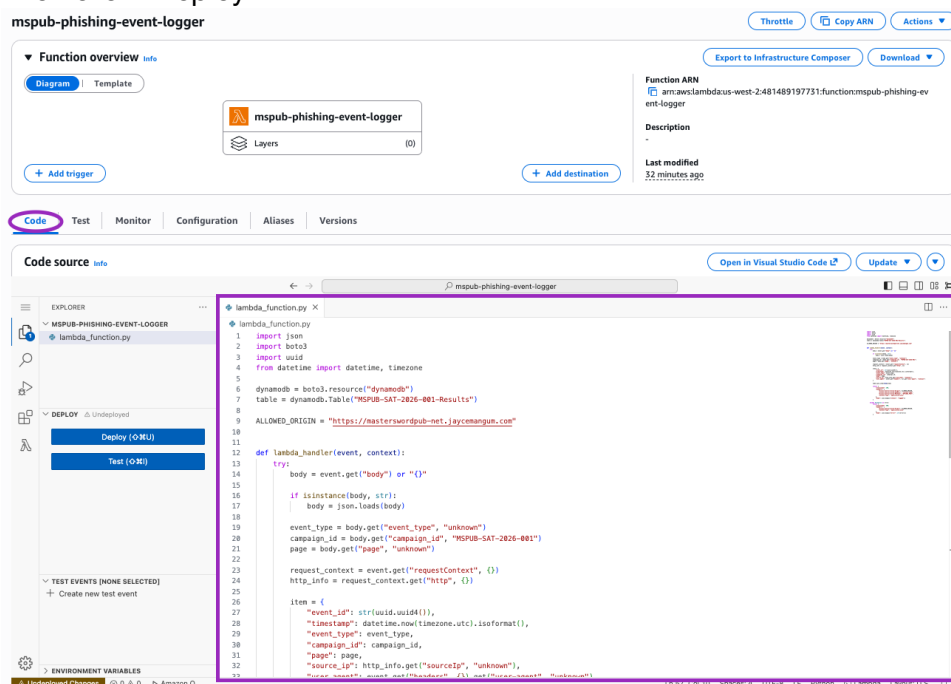
 item = {
 "event_id": str(uuid.uuid4()),
 "timestamp": datetime.now(timezone.utc).isoformat(),
 "campaign_id": body.get("campaign_id", "MSPUB-SAT-2026-001"),
 "participant_id": body.get("participant_id", "unknown"),
 "event_type": body.get("event_type", "unknown"),
 "page": body.get("page", "unknown")
 }

 table.put_item(Item=item)

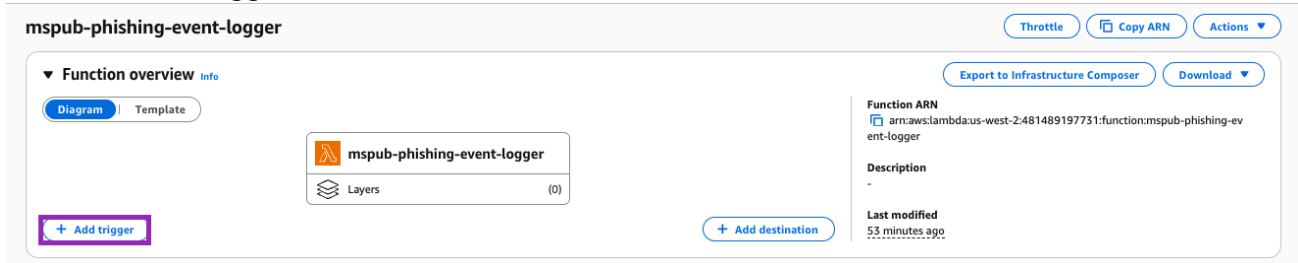
 return response(200, {"status": "logged", "event_id":
 item["event_id"]})

 except Exception as error:
 return response(500, {"error": str(error)})
```

Then click “Deploy.”

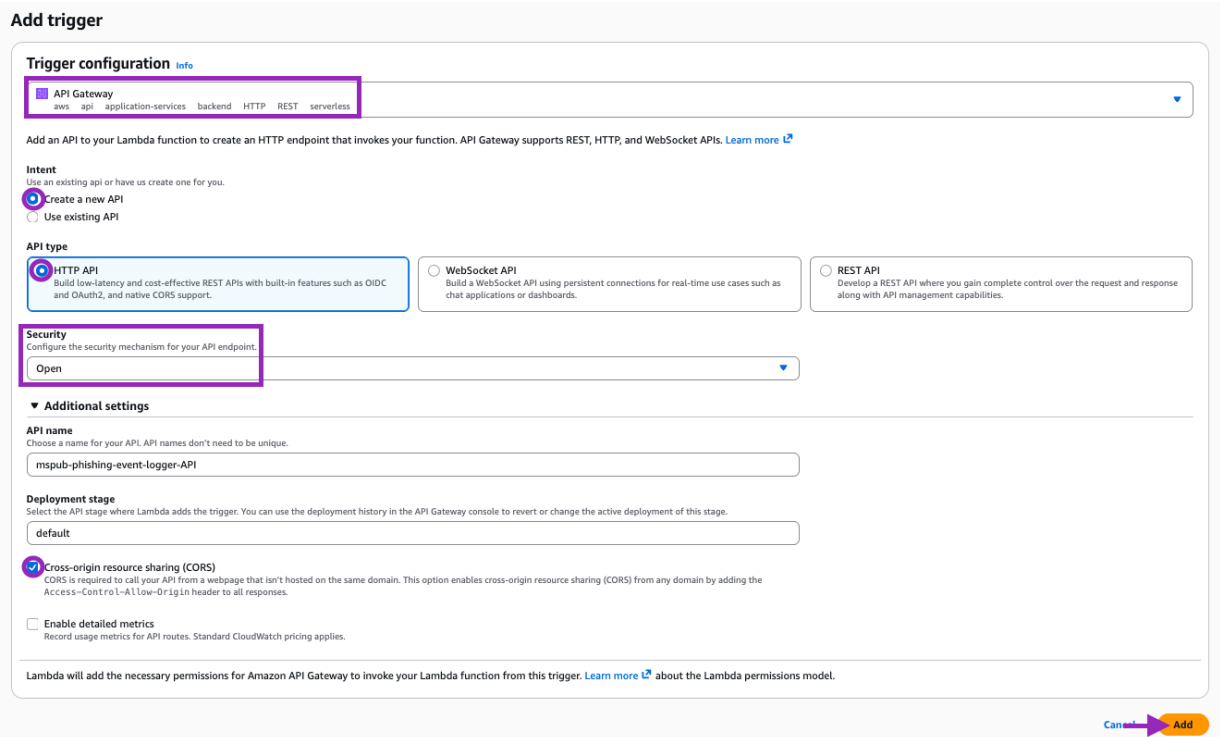


11. Click the “Add trigger” button in the Function overview.

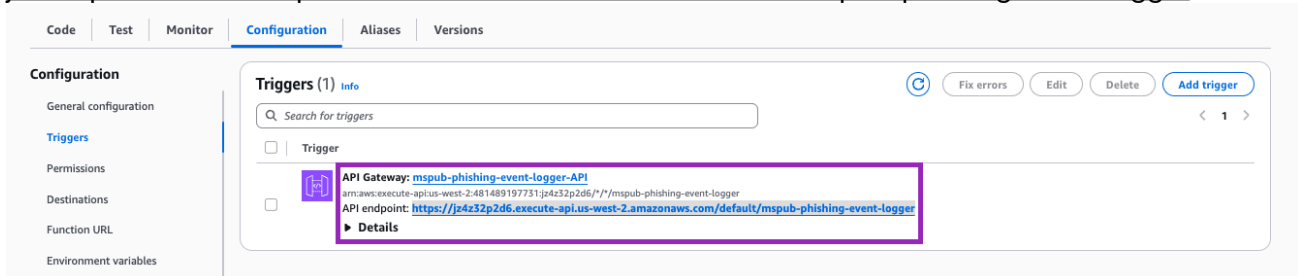


12. On the Add trigger page configure the following:

- **Select:** API Gateway from the drop-down menu
- **Select:** Create a new API
- **Select:** HTTP API
- Security: **Select:** Open
- Additional settings:
  - **Enable:** Cross-origin resource sharing (CORS)
- Click “Add”



13. Take note of the mispub-phishing-event-logger-API API endpoint. In this case it's <https://jz4z32p2d6.execute-api.us-west-2.amazonaws.com/default/mispub-phishing-event-logger>



14. Add the following script to the bottom of the login.html file (re-upload to the S3 Bucket):

```
<script>
const API_URL = "https://jz4z32p2d6.execute-api.us-west-2.amazonaws.com/
default/mispub-phishing-event-logger";
const params = new URLSearchParams(window.location.search);
```

```

const participantId = params.get("p") || "unknown";
function logEvent(eventType, pageName) {
 return fetch(API_URL, {
 method: "POST",
 headers: {
 "Content-Type": "application/json"
 },
 body: JSON.stringify({
 campaign_id: "MSPUB-SAT-2026-001",
 participant_id: participantId,
 event_type: eventType,
 page: pageName
 })
 });
}
logEvent("email_link_clicked", "login.html");
document.getElementById("loginForm").addEventListener("submit",
function(event) {
 event.preventDefault();
 logEvent("login_attempt", "login.html").finally(function() {
 window.location.href = "user-failed-phishing-test.html?p=" +
encodeURIComponent(participantId);
 });
});
</script>

```

15. Add the following script to the bottom of the user-failed-phishing-test.html file (re-upload to the S3 Bucket):

```

<script>
const API_URL = "https://jz4z32p2d6.execute-api.us-west-2.amazonaws.com/
default/mspub-phishing-event-logger";
const params = new URLSearchParams(window.location.search);
const participantId = params.get("p") || "unknown";

fetch(API_URL, {
 method: "POST",
 headers: {
 "Content-Type": "application/json"
 },
 body: JSON.stringify({
 campaign_id: "MSPUB-SAT-2026-001",
 participant_id: participantId,
 event_type: "training_page_view",
 page: "user-failed-phishing-test.html"
 })
});

document.getElementById("completeTraining").href =
 "heart-container.html?p=" + encodeURIComponent(participantId);
</script>
</body>

```

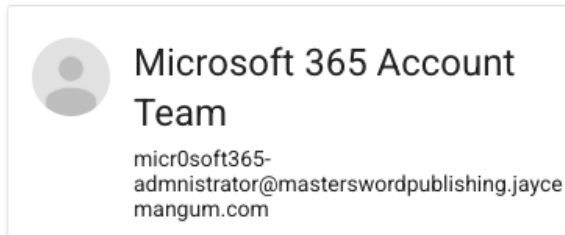
## Creating the Phishing Email

The initial email will be sent from a Google Workspace domain. With the email account name IT Administrator with the email address **micr0soft365-administrator@masterswordpublishing.jaycemangum.com**.

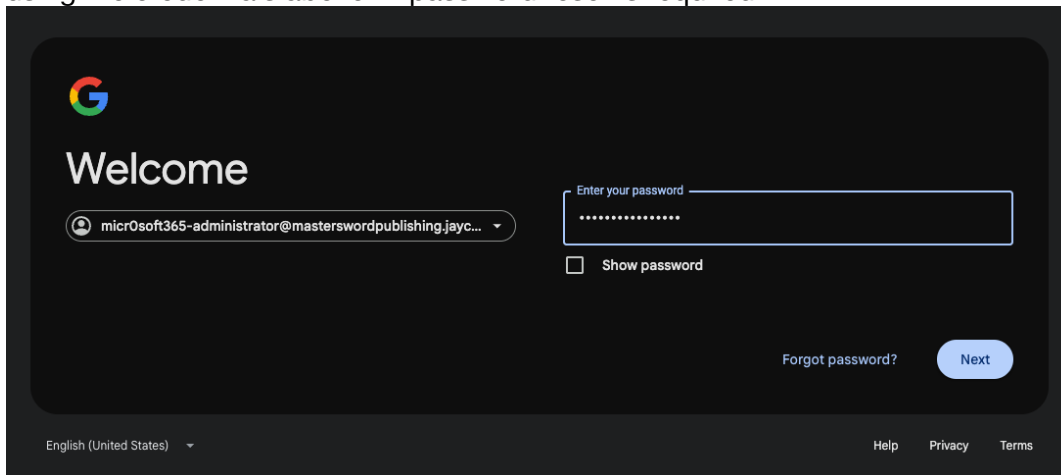
1. The subdomain will need to be added to GoDaddy DNS records, which will be provided by Google when adding a new domain. An MX record for sending emails and a TXT record which provides a DKIM string.

|                          |     |                                         |                                                                                                                                                                                                                                                                                                                                                                                                                           |        |  |  |
|--------------------------|-----|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--|--|
| <input type="checkbox"/> | MX  | masterswordpublishing                   | smtp.google.com. (Priority: 1)                                                                                                                                                                                                                                                                                                                                                                                            | 1 Hour |  |  |
| <input type="checkbox"/> | TXT | google._domainkey.masterswordpublishing | v=DKIM1;k=rsa;p=MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqc1i626A/RghKuDq6RN/UI0Hj/fHPC71MfOq6LjsABgO/K8fMETC35rCtvca8yTIYfX70babkY8KI2m9mIHj8ysWI7z/jPb3/fuMUCKzPQUIfv25AZm2ItN7LkpJOBgYOL+nyOJ2lgV+SoW7qAWcVnhdhYSldtJPVX3ulYij5Od6IEg0Rz9cIU+LI/+4vBDZ5B3tE59pJ+TuBino/embJqLTRd9KYsBNFQarPyWuhluPd8z9xKyxUQWTi39qL7Gc7opq5ZrfKf0BT1FAq9VcBowPKgD9FyJQKilSxOMOhqy5yAdyMLYrr636nwzPaRys7coS1LHQWJWan/FOa54HAWIDAQAB | 1 Hour |  |  |

2. Create a new User in Google Workspace with the following details:
  - First Name: **Microsoft 365**
  - Last Name: **accounts team**
  - Primary email: **micr0soft365-administrator@masterswordpublishing.jaycemangum.com**
  - Click “Add New User”

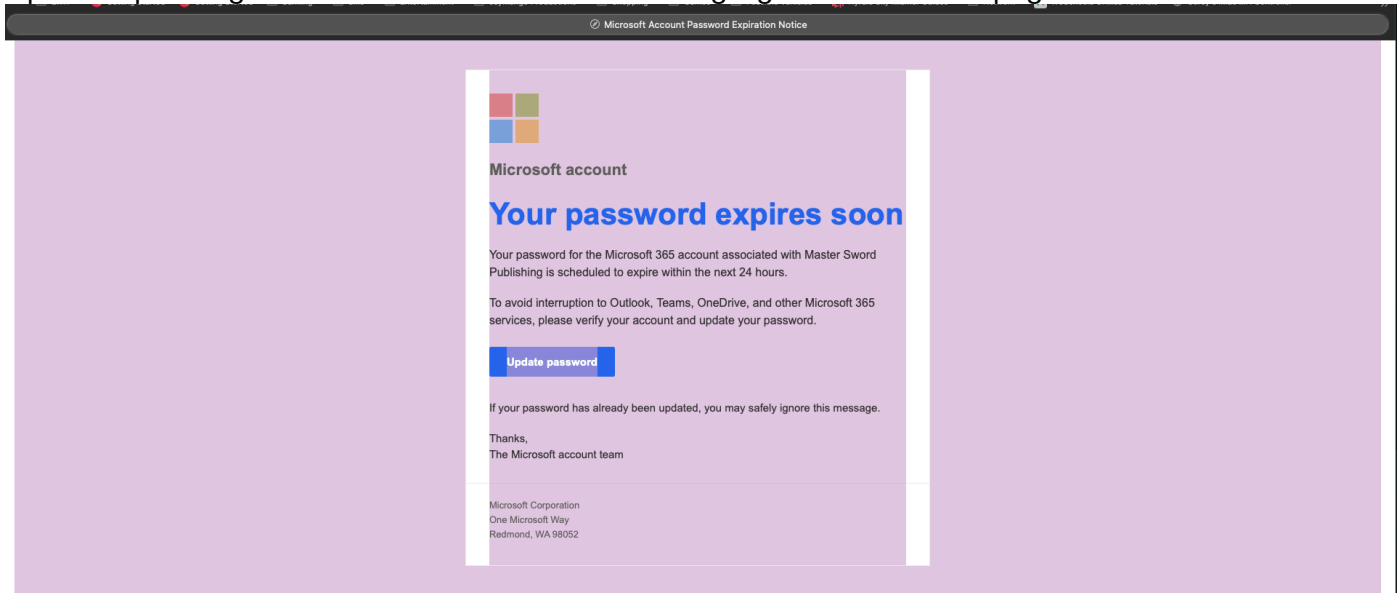


3. Login into new account from a private browser or another web browser by going to **mail.google.com** using the credentials above. A password reset is required.

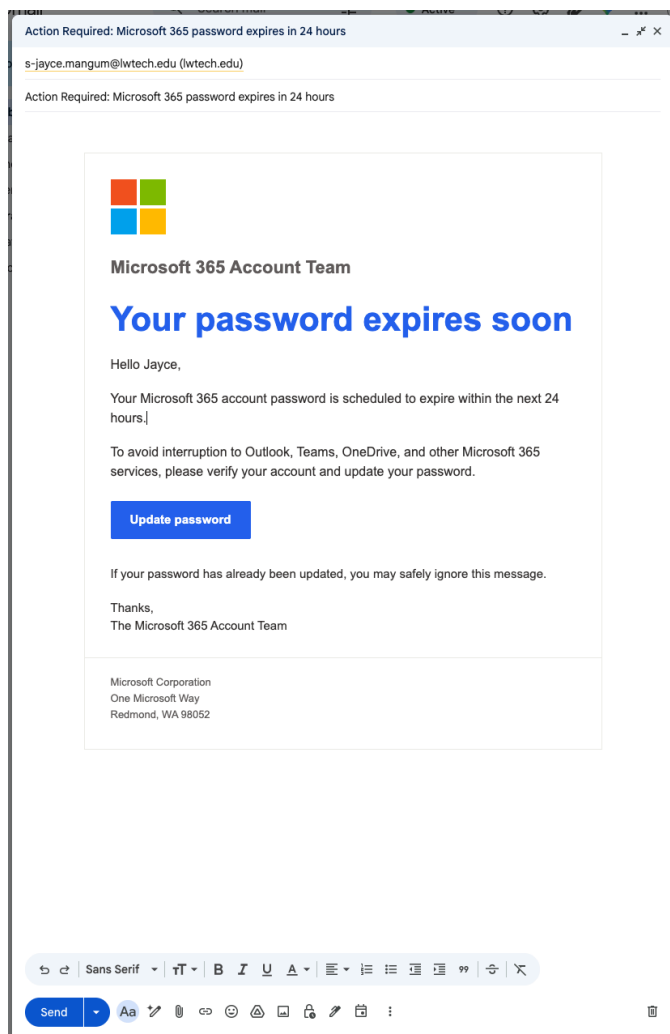


## Part 4: Network Security and Encryption & Server Administration

4. Open the phishing-email.html file in a web browser. Highlight the entire webpage.



5. Compose a new email to each participant individually. In the subject line type: "Action Required: Microsoft 365 password expires in 24 hours." Customize the email template with the person's name and updated the "Update Password" link with the participants ID number. Paste the copied webpage into the email body. Send the email message.





## Part 4: Network Security and Encryption & Server Administration

This Phishing Email was sent to 11 individuals. A randomizer was used to select 5 students and 5 friends to send it to. I also sent it to Professor Epps. Highlighted names below are the recipients, the email column has been blanked out, for privacy.

Participant Tracker

| Participant ID | Person              | Email address                             | Email Name | Custom Email Button Link ID                                           | Email Sent | Email Sent Date |
|----------------|---------------------|-------------------------------------------|------------|-----------------------------------------------------------------------|------------|-----------------|
| participant00  | Link H.             | l.hero@masterswordpub-net.jaycemangum.com | Link       | https://masterswordpub-net.jaycemangum.com/login.html?p=participant00 | ✓          | 6/6/26 7:06 PM  |
| participant01  | Linda E.            |                                           | Linda      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant01 | ✓          | 6/6/26 10:25 AM |
| participant02  | Bob H.              |                                           | Bob        | https://masterswordpub-net.jaycemangum.com/login.html?p=participant02 | N/A        | N/A             |
| participant03  | Brent B.            |                                           | Brent      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant03 | N/A        | N/A             |
| participant04  | Alyx B.             |                                           | Alyx       | https://masterswordpub-net.jaycemangum.com/login.html?p=participant04 | N/A        | N/A             |
| participant05  | Mihail B.           |                                           | Mihail     | https://masterswordpub-net.jaycemangum.com/login.html?p=participant05 | ✓          | 6/6/26 10:15 AM |
| participant06  | Joshua B.           |                                           | Joshua     | https://masterswordpub-net.jaycemangum.com/login.html?p=participant06 | N/A        | N/A             |
| participant07  | Tim C.              |                                           | Tim        | https://masterswordpub-net.jaycemangum.com/login.html?p=participant07 | N/A        | N/A             |
| participant08  | Keith C.            |                                           | Keith      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant08 | N/A        | N/A             |
| participant09  | Iftu I.             |                                           | Iftu       | https://masterswordpub-net.jaycemangum.com/login.html?p=participant09 | ✓          | 6/6/26 10:17 AM |
| participant10  | Mateen K.           |                                           | Mateen     | https://masterswordpub-net.jaycemangum.com/login.html?p=participant10 | N/A        | N/A             |
| participant11  | Akshatha K.         |                                           | Akshatha   | https://masterswordpub-net.jaycemangum.com/login.html?p=participant11 | N/A        | N/A             |
| participant12  | Brandon M.          |                                           | Brandon    | https://masterswordpub-net.jaycemangum.com/login.html?p=participant12 | N/A        | N/A             |
| participant13  | Maksim M.           |                                           | Maksim     | https://masterswordpub-net.jaycemangum.com/login.html?p=participant13 | ✓          | 6/6/26 10:18 AM |
| participant14  | Dylan R.            |                                           | Dylan      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant14 | N/A        | N/A             |
| participant15  | Zach S.             |                                           | Zach       | https://masterswordpub-net.jaycemangum.com/login.html?p=participant15 | N/A        | N/A             |
| participant16  | Hutton S.           |                                           | Hutton     | https://masterswordpub-net.jaycemangum.com/login.html?p=participant16 | N/A        | N/A             |
| participant17  | Mamadou S.          |                                           | Mamadou    | https://masterswordpub-net.jaycemangum.com/login.html?p=participant17 | ✓          | 6/6/26 10:20 AM |
| participant18  | Caden T.            |                                           | Caden      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant18 | ✓          | 6/6/26 10:21 AM |
| participant19  | Gilbert W.          |                                           | Gilber     | https://masterswordpub-net.jaycemangum.com/login.html?p=participant19 | N/A        | N/A             |
| participant37  | Taylor M.           |                                           | Taylor     | https://masterswordpub-net.jaycemangum.com/login.html?p=participant20 | ✓          | 6/6/26 10:09 AM |
| participant38  | Kali T.             |                                           | Kali       | https://masterswordpub-net.jaycemangum.com/login.html?p=participant21 | ✓          | 6/6/26 9:30 AM  |
| participant39  | David M.            |                                           | David      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant22 | ✓          | 6/6/26 9:26 AM  |
| participant40  | Anna J.             |                                           | Anna       | https://masterswordpub-net.jaycemangum.com/login.html?p=participant23 | ✓          | 6/6/26 9:55 AM  |
| participant41  | Mason H.            |                                           | Mason      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant24 | ✓          | 6/6/26 9:38 AM  |
| participant42  | Stacey M.           |                                           | Stacey     | https://masterswordpub-net.jaycemangum.com/login.html?p=participant25 | N/A        | N/A             |
| participant43  | Corey M.            |                                           | Corey      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant26 | N/A        | N/A             |
| participant44  | Kyrah B.            |                                           | Kyrah      | https://masterswordpub-net.jaycemangum.com/login.html?p=participant27 | N/A        | N/A             |
| participant45  | Tristan B.          |                                           | Tristan    | https://masterswordpub-net.jaycemangum.com/login.html?p=participant28 | N/A        | N/A             |
| tester01       | Jayce M. (LWTech)   |                                           | Jayce      | https://masterswordpub-net.jaycemangum.com/login.html?p=tester01      | ✓          | 6/5/26 11:01 PM |
| tester02       | Jayce M. (Personal) |                                           | Jayce      | https://masterswordpub-net.jaycemangum.com/login.html?p=tester02      | ✓          | 6/5/26 11:48 PM |

## Phishing Email Results

To track participant's progress each person was assigned a Participant ID to be able to track their link clicks within the simulation. The Participant ID was then translated from AWS DynamoDB to the person's name in a standard spreadsheet, that automatically calculates the statistics based on if a cell gets checked.

These were the statistics as of Tuesday, 09 June 2026.

## Part 4: Network Security and Encryption & Server Administration

| Participant Tracker |            |               |            |                                                                                                                                                           |            |                 |                                     |                                     |                                     |                                     |                                                                                                                                                   |  |
|---------------------|------------|---------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Participant ID      | Person     | Email address | Email Name | Custom Email Button Link ID                                                                                                                               | Email Sent | Email Sent Date | Initial Link Clicked                | Login Attempt Clicked               | Training Viewed                     | Training Completed                  | Note                                                                                                                                              |  |
| participant01       | Linda E.   | [REDACTED]    | Linda      | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant01">https://masterswordpub-net.jaycemangum.com/login.html?p=participant01</a> | ✓          | 6/6/26 10:25 AM | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link. |  |
| participant05       | Mihail B.  |               | Mihail     | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant05">https://masterswordpub-net.jaycemangum.com/login.html?p=participant05</a> | ✓          | 6/6/26 10:15 AM | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link. |  |
| participant09       | Ifu I.     |               | Ifu I.     | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant09">https://masterswordpub-net.jaycemangum.com/login.html?p=participant09</a> | ✓          | 6/6/26 10:17 AM | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link. |  |
| participant13       | Makaim M.  |               | Makaim     | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant13">https://masterswordpub-net.jaycemangum.com/login.html?p=participant13</a> | ✓          | 6/6/26 10:18 AM | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link. |  |
| participant17       | Mamadou B. |               | Mamadou    | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant17">https://masterswordpub-net.jaycemangum.com/login.html?p=participant17</a> | ✓          | 6/6/26 10:20 AM | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link. |  |
| participant18       | Caden T.   |               | Caden      | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant18">https://masterswordpub-net.jaycemangum.com/login.html?p=participant18</a> | ✓          | 6/6/26 10:21 AM | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link. |  |
| participant37       | Taylor M.  |               | Taylor     | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant20">https://masterswordpub-net.jaycemangum.com/login.html?p=participant20</a> | ✓          | 6/6/26 10:09 AM | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Opened link twice, then filled out the form, and proceeded through the exercise.                                                                  |  |
| participant38       | Kali T.    |               | Kali       | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant21">https://masterswordpub-net.jaycemangum.com/login.html?p=participant21</a> | ✓          | 6/6/26 9:30 AM  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Ignored email or didn't click the link in the email.                                                                                              |  |
| participant39       | David M.   |               | David      | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant22">https://masterswordpub-net.jaycemangum.com/login.html?p=participant22</a> | ✓          | 6/6/26 9:26 AM  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Opened link twice, then filled out the form, and proceeded through the exercise.                                                                  |  |
| participant40       | Anna J.    |               | Anna       | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant23">https://masterswordpub-net.jaycemangum.com/login.html?p=participant23</a> | ✓          | 6/6/26 9:55 AM  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                                                                                                                   |  |
| participant41       | Mason H.   |               | Mason      | <a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant24">https://masterswordpub-net.jaycemangum.com/login.html?p=participant24</a> | ✓          | 6/6/26 9:38 AM  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                                                                                                                                   |  |

| Statistics         |       |            |
|--------------------|-------|------------|
| Metric             | Count | Percentage |
| Emails Sent        | 11    | 100.00%    |
| Links Clicked      | 5     | 41.67%     |
| Login Attempts     | 5     | 41.67%     |
| Training Viewed    | 5     | 41.67%     |
| Training Completed | 4     | 33.33%     |
| Did Not Respond    | 6     | 50.00%     |

Figure SISAT-6: SAT Statistics Tracker Final Results, Campaign ended on 6/9/26

No classmates clicked on the email link. All five friends clicked the link entered credentials but only four completed the training.

## Source Code

### Phishing Email Template

Download [phishing-email-template.html](#)

```
<!-- This phishing site is for educational purposes only.
This simulation has been developed for a CSNT Capstone Project -->
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>Microsoft Account Password Expiration Notice</title>
</head>
<!-- Microsoft Logo, as a table -->
<body style="margin:0;padding:0;background:#ffffff;font-family:'Segoe
UI',Arial,sans-serif;">
<table width="100%" border="0" cellspacing="0" cellpadding="0"
style="background:#ffffff;">
<tr>
<td align="center" style="padding:40px 20px;">
<table width="640" border="0" cellspacing="0" cellpadding="0" style="border:1px
solid #edebe9;background:#ffffff;">
<tr>
<td style="padding:32px 32px 24px 32px;">
<div style="font-size:22px;font-weight:600;color:#605e5c;">
<table cellpadding="0" cellspacing="0" border="0" style="margin-bottom:24px;">
<tr>
<td style="width:32px;height:32px;background:#f25022;"></td>
<td style="width:4px;"></td>
<td style="width:32px;height:32px;background:#7fba00;"></td>
</tr>

<tr>
<td style="height:4px;"></td>
<td></td>
<td></td>
</tr>
<tr>
<td style="width:32px;height:32px;background:#00a4ef;"></td>
<td style="width:4px;"></td>
<td style="width:32px;height:32px;background:#ffb900;"></td>
</tr>
<!-- Email Body -->
</table>
Microsoft 365 Account Team
</div>
</td>
</tr>

<tr>
<td style="padding:0 32px 20px 32px;">
```

```
<div style="
font-size:42px;
line-height:48px;
font-weight:600;
color:#2563eb;">
```

Your password expires soon

```
</div>
```

```
</td>
```

```
</tr>
```

```
<tr>
```

```
<td style="
```

```
padding:0 32px 18px 32px;
```

```
font-size:16px;
```

```
line-height:24px;
```

```
color:#323130;">
```

Hello [participants name],

```
</td>
```

```
</tr>
```

```
<tr>
```

```
<td style="
```

```
padding:0 32px 18px 32px;
```

```
font-size:16px;
```

```
line-height:24px;
```

```
color:#323130;">
```

Your Microsoft 365 account password is scheduled to expire within the next 24 hours.

```
</td>
```

```
</tr>
```

```
<tr>
```

```
<td style="
```

```
padding:0 32px 24px 32px;
```

```
font-size:16px;
```

```
line-height:24px;
```

```
color:#323130;">
```

To avoid interruption to Outlook, Teams, OneDrive, and other Microsoft 365 services, please verify your account and update your password.

```
</td>
```

```
</tr>
```

```
<!-- Button with clickable click tracking -->
```

```
<tr>
```

```
<td style="padding:0 32px 32px 32px;">
```

```
<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=[ParticipantID]"
style="
```

```
background:#2563eb;
```

```
color:#ffffff;
text-decoration:none;
padding:12px 24px;
display:inline-block;
font-size:15px;
font-weight:600;
border-radius:2px;">
```

Update password

```

</td>
</tr>
```

```
<tr>
<td style="
padding:0 32px 20px 32px;
font-size:15px;
line-height:22px;
color:#323130;">
```

If your password has already been updated, you may safely ignore this message.

```
</td>
</tr>
```

```
<tr>
<td style="
padding:0 32px 28px 32px;
font-size:15px;
line-height:22px;
color:#323130;">
```

Thanks,<br>  
The Microsoft 365 Account Team  
</td>  
</tr>

```
<tr>
<td style="
padding:20px 32px 32px 32px;
font-size:13px;
line-height:20px;
color:#605e5c;
border-top:1px solid #edebe9;">
```

Microsoft Corporation<br>  
One Microsoft Way<br>  
Redmond, WA 98052  
</td>  
</tr>  
</table>  
</td>

```

</tr>

</table>
</body>
</html>

```

### **Suspicious Microsoft 365 Login Page**

Download [login.html](#)

```

<!-- This phishing site is for educational purposes only.
This simulation has been developed for a CSNT Capstone Project -->

<!DOCTYPE html>
<html>
<head>
 <meta charset="UTF-8">
 <title>Microsoft account | Sign In</title>
 <link rel="stylesheet" href="style.css">
</head>
<body class="login-body">
<!-- Microsoft Logo as table -->
 <main class="login-card">
 <div class="ms-logo">

 </div>

 <h1>Sign in</h1>
 <p class="subtitle">to continue to Microsoft 365</p>
<!-- Fake Login Credential Form, this information does not get recorded -->
 <form id="loginForm">
 <input type="text" placeholder="Email, phone, or Skype"
autocomplete="off">
 <input type="password" placeholder="Password" autocomplete="off">

 <div class="links">
 No account? Create one!
 Can't access your account?
 </div>
<!-- Fake Sign In button -->
 <button type="submit"> Sign in</button>
 </form>
 </main>

 <footer>
 Terms of use
 Privacy & cookies
 </footer>
<!-- AWS Lambda API to track link clicks in AWS DynamoDB -->

```

```
<script>
const API_URL = "https://jz4z32p2d6.execute-api.us-west-2.amazonaws.com/default/
mspub-phishing-event-logger";
const params = new URLSearchParams(window.location.search);
const participantId = params.get("p") || "unknown";
function logEvent(eventType, pageName) {
 return fetch(API_URL, {
 method: "POST",
 headers: {
 "Content-Type": "application/json"
 },
 body: JSON.stringify({
 campaign_id: "MSPUB-SAT-2026-001",
 participant_id: participantId,
 event_type: eventType,
 page: pageName
 })
 });
}
logEvent("email_link_clicked", "login.html");
document.getElementById("loginForm").addEventListener("submit", function(event) {
 event.preventDefault();
 logEvent("login_attempt", "login.html").finally(function() {
 window.location.href = "user-failed-phishing-test.html?p=" +
 encodeURIComponent(participantId);
 });
});
</script>
</body>
</html>
```

### **Phishing Email Training Page**

Download [user-failed-phishing-test.html](#)

```
<!-- This phishing site is for educational purposes only.
This simulation has been developed for a CSNT Capstone Project -->
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>MSPUB Security Awareness Training</title>
 <link rel="stylesheet" href="style.css">
</head>
<body class="training-body">

 <main class="training-card">
 <h1>Secuirty Awareness Training Report</h1>
 <h2>Hyahhh! You just interacted with a simulated phishing attack!</h2>
 <h3>This was a simulated phishing exercise on behalf of your IT &
Cybersecurity team!</h3>
```

## Part 4: Network Security and Encryption & Server Administration

<p>This exercise was created as part of the Master Sword Publishing Security Awareness Campaign. Luckily, this simulation did not collect or store your usernames, passwords, or other personal information.</p>

### <h3>What happened?</h3>

<p>

You clicked a link in a simulated Microsoft 365 password expiration notice and were directed to a fake login page. In a real phishing attack, entering credentials could allow an attacker access to email, files, cloud services, and company systems.

</p>

### <h3>Warning signs to watch for</h3>

<ul>

<li>An unexpected password expiration message </li>

<li>Urgent language pressuring for immediate action</li>

<li>Embedded login links in email</li>

<ul>

<li>The URL for this simulation is <a href="https://masterswordpub-net.jaycemangum.com/login">https://masterswordpub-net.jaycemangum.com/login.html</a>, but the actual Microsoft login page is, <a href="https://login.microsoftonline.com">https://login.microsoftonline.com/</a>.</li>

</ul>

<li>Sender addresses that do not match the official service.</li>

<ul>

<li>The email address for this exercise was, <u>micr0soft365-administrator@masterswordpublishing.jaycemangum.com</u>, which is not a Microsoft domain or email address.</li>

</ul>

<li>Web addresses that are close to, but not exactly the real website.</li>

</ul>

### <h3>Best practices</h3>

<ul>

<li>Go directly to the Microsoft 365 website instead of clicking email login links.</li>

<li>Verify the sender before responding.</li>

<li>Hover over links and buttons before clicking them, to check if the URL is legitimate.</li>

<li>Report suspicious message to your IT department.</li>

<li>Use Multi Factor Authentication (MFA) whenever available.</li>

</ul>

<li>Use a password manager like 1Password, Bitwarden, or LastPass.</li>

</ul>

### <h3>Questions or Concerns?</h3>

<p>



## Part 4: Network Security and Encryption & Server Administration

Please contact the MSPUB IT & Cybersecurity Department if you believe you have received a suspicious email, text messages or security-related communication.

</p>

```
I
Understand
</main>
<!-- AWS Lambda API to track link clicks in AWS DynamoDB -->
<script>
const API_URL = "https://jz4z32p2d6.execute-api.us-west-2.amazonaws.com/default/
mspub-phishing-event-logger";
const params = new URLSearchParams(window.location.search);
const participantId = params.get("p") || "unknown";

fetch(API_URL, {
 method: "POST",
 headers: {
 "Content-Type": "application/json"
 },
 body: JSON.stringify({
 campaign_id: "MSPUB-SAT-2026-001",
 participant_id: participantId,
 event_type: "training_page_view",
 page: "user-failed-phishing-test.html"
 })
});

document.getElementById("completeTraining").href =
 "heart-container.html?p=" + encodeURIComponent(participantId);
</script>
</body>
</html>
```

### **Training Completed Page**

Download [heart-container.html](#)

```
<!-- This phishing site is for educational purposes only.
This simulation has been developed for a CSNT Capstone Project -->
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <title>Training Completed</title>
 <link rel="stylesheet" href="style.css">
</head>
<body class="heart-body">

 <main class="heart-card">
<div class="pixel-heart">
 <div class="heart-row row1">■ ■</div>
```

```

 <div class="heart-row row2">██████████</div>
 <div class="heart-row row3">██████████</div>
 <div class="heart-row row4">██████████</div>
 <div class="heart-row row5">██████████</div>
</div>

<h1>Heart Container obtained!</h1>
<h2>+1 Security Awareness</h2>
<p>
 Congratulations, hero. You completed the MSPUB Security Awareness Training.
</p>

<p>
 You gained resistance against phishing attacks by learning how to verify
 sender email addresses, inspect links, recognize fake login pages, and report
 suspicious messages to the IT & Cyberseucirty Department.
</p>

<div class="reward-box">
 <p>Campaign: MSPUB-SAT-2026-001</p>
 <p>Stratus: Completed</p>
 <p>New Skill: Phisihing Detection</p>
 <p>Issued By: MSPUB IT & & Cybersecurity Department</p>
</div>

<h3>Please close this tab, when completed viewing or click the button to go
to the MSPUB Portal.</h3>
Return to MSPUB Portal
</main>
<!-- AWS Lambda API to track link clicks in AWS DynamoDB -->
<script>
 const API_URL = "https://jz4z32p2d6.execute-api.us-west-2.amazonaws.com/
default/mspub-phishing-event-logger";
 const params = new URLSearchParams(window.location.search);
 const participantId = params.get("p") || "unknown";
 fetch(API_URL, {
 method: "POST",
 headers: {
 "Content-Type": "application/json"
 },
 body: JSON.stringify({
 campaign_id: "MSPUB-SAT-2026-001",
 participant_id: participantId,
 event_type: "training_completed",
 page: "heart-container.html"
 })
 });
</script>
</body>
</html>

```

### **Stylesheet for the 3 Webpages**

Download [style.css](#)

```
/* This phishing site is for educational purposes only. */
/* This simulation has been developed for a CSNT Capstone Project */
/* Fake MS Login Page */
* {
 box-sizing: border-box;
}
body {
 margin: 0;
 font-family: "Segoe UI", Arial, sans-serif;
}
/* Login Page */
.login-body {
 min-height: 100vh;
 background:
 linear-gradient(rgba(255,255,255,0.85), rgba(255,255,255,0.85)),
 radial-gradient(circle at top left, #dbeafe, transparent 30%),
 radial-gradient(circle at bottom right, #e0e7ff, transparent 35%);
 display: flex;
 justify-content: center;
 align-items: center;
 color: #1f1f1f;
}
.login-card {
 width: 440px;
 min-height: 390px;
 background: #fff;
 padding: 44px;
 box-shadow: 0 2px 8px rgba(0,0,0,0.18);
}
.ms-logo {
 display: grid;
 grid-template-columns: repeat(2, 14px);
 grid-template-rows: repeat(2, 14px);
 gap: 3px;
 width: 34px;
 margin-bottom: 28px;
}
.sq {
 display: block;
 width: 14px;
 height: 14px;
}
.red { background: #f25022; }
.green { background: #7fba00; }
.blue { background: #00a4ef; }
.yellow { background: #ffb900; }
.login-card h1 {
```

```
 font-size: 28px;
 font-weight: 600;
 margin: 0 0 8px;
}
.subtitle {
 margin: 0 0 24px;
 color: #444;
}
input {
 width: 100%;
 border: none;
 border-bottom: 1px solid #666;
 padding: 10px 2px;
 margin-bottom: 20px;
 font-size: 15px;
 outline: none;
}
input:focus {
 border-bottom: 2px solid #0067b8;
}
.links {
 display: flex;
 flex-direction: column;
 gap: 8px;
 margin: 4px 0 28px;
}
.links a,
footer a {
 color: #0067b8;
 font-size: 13px;
 text-decoration: none;
}
button {
 float: right;
 background: #0067b8;
 color: white;
 border: none;
 padding: 10px 34px;
 font-size: 15px;
 cursor: pointer;
}
button:hover {
 background: #005a9e;
}
footer {
 position: fixed;
 bottom: 18px;
 right: 30px;
 display: flex;
 gap: 20px;
}
```

```
/* MSPUB Training Page */
.training-body {
 min-height: 100vh;
 background:
 radial-gradient(circle at top center, rgba(212, 175, 55, 0.18), transparent
35%),
 linear-gradient(135deg, #051f1f, #0b2f2f, #071515);
 color: #f5f5f5;
 padding: 50px 20px;
}
.training-card {
 max-width: 900px;
 margin: auto;
 background: rgba(15, 45, 45, 0.92);
 padding: 44px;
 border-radius: 14px;
 border: 1px solid rgba(212, 175, 55, 0.45);
 box-shadow: 0 8px 28px rgba(0,0,0,0.45);
}
.training-card h1 {
 color: #d4af37;
 margin-top: 0;
 font-size: 32px;
}
.training-card h2 {
 color: #ffffff;
}
.training-card h3 {
 color: #d4af37;
 margin-top: 28px;
}
.training-card p,
.training-card li {
 color: #e8eeee;
 line-height: 1.6;
}
.training-card li {
 margin-bottom: 8px;
}
.complete-btn {
 display: inline-block;
 margin-top: 24px;
 background: #d4af37;
 color: #071515;
 font-weight: 700;
 padding: 12px 22px;
 text-decoration: none;
 border-radius: 999px;
}
.complete-btn:hover {
```

```
background: #f1d36b;
}

/* Heart Container Completion Page */
.heart-body {
 min-height: 100vh;
 background:
 radial-gradient(circle at top center, rgba(212, 175, 55, 0.22), transparent
35%),
 linear-gradient(135deg, #031818, #0b2f2f, #020909);
 color: #f8fafc;
 padding: 50px 20px;
 font-family: "Segoe UI", Arial, sans-serif;
}
.heart-card {
 max-width: 820px;
 margin: auto;
 text-align: center;
 background: rgba(15, 45, 45, 0.94);
 padding: 46px;
 border-radius: 16px;
 border: 1px solid rgba(212, 175, 55, 0.5);
 box-shadow: 0 8px 30px rgba(0,0,0,0.5);
}
.pixel-heart {
 font-family: monospace;
 font-size: 34px;
 line-height: 0.82;
 color: #ef4444;
 text-shadow:
 0 0 6px rgba(239, 68, 68, 0.8),
 0 0 14px rgba(212, 175, 55, 0.45);
 margin-bottom: 28px;
}
.heart-row {
 letter-spacing: 2px;
}
.heart-card h1 {
 color: #d4af37;
 font-size: 34px;
 margin-bottom: 8px;
}
.heart-card h2 {
 color: #ffffff;
 font-size: 24px;
 margin-bottom: 24px;
}
.heart-card p {
 color: #e8eeee;
 line-height: 1.6;
}
```

```
.reward-box {
 margin: 28px auto;
 padding: 20px;
 max-width: 540px;
 text-align: left;
 background: rgba(5, 31, 31, 0.8);
 border-left: 4px solid #d4af37;
 border-radius: 8px;
}
.reward-box p {
 margin: 8px 0;
}
```

## Incident Response Plan

### Scenario

Following a successful phishing simulation, Link, the Cybersecurity Manager, brought the data to MSPUB leadership to help them recognize the importance of having a formal incident response plan. The organization requires documented procedures to respond to security incidents involving malware infections, phishing attacks, unauthorized access, and data breaches.

### Objective

Develop a formal incident response plan that outlines procedures for identifying, containing, eradicating, recovering from, and documenting cybersecurity incidents.

## Master Sword Publishing Incident Response Plan

### Executive Summary

Master Sword Publishing (MSPUB) will maintain an Incident Response Plan to identify, contain, eradicate, and recover from cybersecurity incidents. This plan provides a structured approach for responding to security events while minimizing business disruption and protecting company systems, data, and users.

### Purpose

This document outlines the plan for responding to cybersecurity incidents at Master Sword Publishing (MSPUB). It defines the roles and responsibilities of the participants involved in the incident response. It also characterizes the overall incident response process and establishes relationships with other relevant policies and procedures. Additionally, it provides guidelines for reporting requirements.

The purpose of this Incident Response Plan is to:

- Detect cybersecurity incidents quickly
- Define the roles associated with the individuals involved in an incident
- Limit damage to company systems
- Protect sensitive information
- Restore normal business operations
- Document lessons learned
- Meet organizational security requirements

### Standards Alignment

The Master Sword Publications (MSPUB) Incident Response Plan is aligned with the principles of ISO/IEC 27001 Information Security Management Systems (ISMS) and ISO/IEC 27035 Information Security Incident Management. These standards provide guidance for establishing, implementing, maintaining, and continually improving information security processes and incident response capabilities.

This plan incorporated industry best practices for incident preparation, detection, reporting, assessment, containment, eradication, recovery, post-incident review, and continuous improvement. The procedures outlined in this document are intended to support MSPUB's commitment to protecting the confidentiality, integrity, and availability of organization information assets while maintaining business continuity during security incidents.



### Scope

This plan applies to all information systems, company data, and networks of MSPUB, as well as any person or device that accesses system data. This plan applies to the following:

- Windows Server Domain Controllers
- Ubuntu Linux Web Server
- Windows Workstations
- macOS Workstations
- Ubuntu Linux Workstations
- Kali Linux Security Workstations
- Microsoft 365 Services
- Google Workspace Services
- Apple iCloud Services
- Network Infrastructure
- Company Web Applications

### Incident Response Team

In the event of a cybersecurity incident, these are the assigned roles of the individuals apart of the Incident Response Team. These roles should be reviewed and updated on a quarterly basis.

Role	Responsiiply	Point of Contact
IT Administrator	Incident coordinator	Purah Sheikah <a href="mailto:p.sheikah@masterswordpub.net">p.sheikah@masterswordpub.net</a>
Security Analyst	Investigation and analysis	Link Hero <a href="mailto:l.hero@masterswordpub.net">l.hero@masterswordpub.net</a>
System Administrator	Server remediation	Robbie Sheikah <a href="mailto:r.sheikah@masterswordpub.net">r.sheikah@masterswordpub.net</a>
Network Administrator	Network containment	Jayce Mangum <a href="mailto:j.mangum@masterswordpub.net">j.mangum@masterswordpub.net</a>
Management	Business decisions and communications	Impa Sheikah <a href="mailto:i.sheikah@masterswordpub.net">i.sheikah@masterswordpub.net</a>

### Incident Response Lifecycle

This section defines the lifecycle of an Incident.

#### Phase 1: Preparation

This phase prepares employees, critical systems, and data prior to a cybersecurity incident and defines what activities and actions are to be taken.

- **Security Awareness Training:** Master Sword Publishing employees will be required to participate in security awareness trainings on a monthly basis. These trainings may include users watching security awareness videos, taking a short quiz that tests their knowledge on various cyber attacks, and participating in controlled simulations developed by the Master Sword Publishing IT & Cybersecurity department.
- **Multi-Factor Authentication (MFA) implementation:** All Master Sword Publishing employees will be required to protect their company user accounts using MFA protection with a company-approved authentication app. They will be required to enter a verification code before accessing company resources.

## Part 4: Network Security and Encryption & Server Administration

- **Regular System Backups:** Backups of critical systems will be backed up using the 3-2-1 backup rule. Three total copies of all company data will be stored on 2 different media types, and one copy kept off-premise. A full backup will be run monthly of critical systems and stored onsite. An incremental backup will be run biweekly and stored through a cloud service provider as well as onsite. Differential Backups will be run weekly and stored through a cloud service provider. All backups of critical systems will be performed quarterly to ensure Master Sword Publishing can recover from a cybersecurity incident.
- **Endpoint Protection:** All Master Sword Publishing workstations and servers will use endpoint protection tools to detect malware, suspicious activity, and unauthorized changes. Security scans will be scheduled regularly, and alerts will be reviewed by the IT & Cybersecurity department. Any affected endpoints will be isolated from the network until it can be investigated and cleared for use.
- **Log Monitoring:** Master Sword Publishing will review system, authentication, firewall, web server, and cloud service logs to identify suspicious activity. Logs from Windows Server, Ubuntu Server, Microsoft 365, Google Workspace, AWS, and network devices will be used to support incident detection and investigation. Logs should be retained long enough to support incident review and post-incident analysis.
- **User Account Management:** User accounts will follow the principle of least privilege access. Employees will only receive access required for their job role. Account activity will be monitored for failed login attempts, unusual access patterns, and privilege changes. When an incident involves a user account, IT may disable the account, reset the password, revoke active sessions, and verify MFA enrollment before restoring access.

### Phase 2: Detection and Reporting

Users report an incident to the IT & Cybersecurity team. The IT & Cybersecurity department investigates the incident by reviewing system logs to determine what systems may be infected, and analyzes elements of what the user is reporting.

#### Example Incident:

An employee receives an email claiming that their Microsoft 365 password is about to expire. The employee clicks the link provided in the message and enters their credentials into a fraudulent login page. Shortly afterward, security logs show multiple failed login attempts and authentication activity originating from locations or systems that the user would not normally access. Review of the email headers reveals authentication failures and other indicators commonly associated with phishing campaigns. The incident is reported to the MSPUB IT & Cybersecurity department for investigation. Review phishing simulation results and user behavior metrics.

### Phase 3: Assessment and Analysis

Answer the following questions about the incident:

- **What happened?**
  - A MSPUB employee received an email reporting their password was about to expire not sent from the proper MSPUB IT channels.
  - The user entered their credentials into a suspicious web form.
  - Reviewing the logs, there have been multiple failed login attempts from the user's account and the account appears to be accessing critical IT systems.
- **Which systems are affected?**
  - Microsoft 365 user account
  - Windows Server Active Directory environment
  - Windows workstations used by the employee
  - Microsoft 365 cloud services including Outlook, OneDrive, and Teams
  - MSPUB web applications used during the phishing simulation

## Part 4: Network Security and Encryption & Server Administration

- Network authentication and logging systems
- **What data is involved?**
  - User account credentials
  - Company email communications
  - Authentication and security logs
  - Employee information stored within company systems
  - Files accessible through Microsoft 365 services
  - Potentially any data accessible through the compromised user account
- **What severity level applies?**
  - High:
    - Evidence indicates a user account may have been compromised, and unauthorized access attempts have been observed against company systems.
    - Multiple business systems may be affected, and immediate containment actions are required.

### Phase 4: Containment

#### Objective

Prevent further damage, stop unauthorized access, and limit the spread of the incident while preserving evidence for investigation.

#### Short-Term Containment:

- Disable affected user accounts
- Revoke active user sessions
- Block unauthorized IP addresses when applicable
- Isolate affected endpoints from the network
- Preserve relevant logs and evidence

#### Long-Term Containment:

- Increase monitoring of affected systems and network logs
- Apply temporary access restrictions to affected accounts
- Verify MFA enrollment and enforcement
- Monitor for additional indicators of compromise
- Review related systems for similar activity

### Phase 5: Eradication

#### Eradication Activities:

- Remove phishing emails from company mailboxes
- Reset affected user credentials
- Revoke unauthorized sessions and tokens
- Verify that no malware or malicious software is present
- Review and correct account permissions
- Scan affected systems for indicators of compromise
- Apply required security patches and updates
- Remove unauthorized persistence mechanisms, if discovered

### Phase 6: Recovery

#### Objective

Restore all affected systems and services to normal operation, verify that unauthorized access has been removed, ensure user credentials are secured, and implement corrective actions to reduce the likelihood of

future incidents.

### Recovery Procedure

In the event a user falls for a phishing email and evidence indicates that an account has been compromised, the user's account will be disabled immediately. The user will be required to reset their password through the IT department, and MFA will be enabled if it is not already configured. Affected devices will be removed from service and investigated for signs of compromise. Logs will be reviewed and malware or antivirus scans will be performed on affected systems. If necessary, backups will be restored to recover impacted data or services. Any identified vulnerabilities will be remediated before systems are returned to production. Once the incident has been confirmed as contained and eradicated, the user account and affected systems will be restored to normal operations. Additional security awareness training may be provided based on the severity and root cause of the incident to help prevent similar events in the future.

### **Phase 7: Post-Incident Review**

#### Objective

Identify lessons learned, improve security controls, and reduce the likelihood of similar incidents occurring in the future.

#### Activities:

- Conduct root cause analysis
- Review the incident timeline and response actions
- Evaluate the effectiveness of containment and recovery efforts
- Identify gaps in policies, procedures, or security controls
- Develop corrective actions
- Develop preventive actions
- Update incident response documentation as needed
- Determine whether additional user awareness training is required

## Roles and Responsibilities

### Employees

Master Sword Publishing Employees are responsible for following company security policies, participating in security awareness trainings, and reporting suspicious emails, security incidents, or unusual system behavior to the Master Sword Publishing IT & Cybersecurity Department as soon as possible. Employees should not attempt to investigate or remediate security incidents on their own.

### Information Technology & Cybersecurity Department

The Master Sword Publishing IT & Cybersecurity department is responsible for coordinating all incident response activities. Responsibilities include:

- Incident detection
- Investigation
- Containment
- Eradication
- Recovery
- Evidence collection
- Documentation
- Post-incident review

The department will also provide guidance and communication to affected users throughout the incident response process.

### System Administrators

## Part 4: Network Security and Encryption & Server Administration

System Administrators are responsible for maintaining servers, network infrastructure, user accounts, backups, and system security configurations. During an incident, administrators assist with account management, system isolation, log collection, vulnerability remediation, and restoration of affected services.

Management

Management is responsible for providing oversight and support during security incidents. Responsibilities include:

- Approving major response actions
- Allocating resources
- Coordinating business communications
- Ensuring compliance with organizational policies and regulatory requirements

### Third-Party Service Providers

Third-party service providers may assist with incidents involving cloud services, hosted applications, internet service providers, or other external systems. Providers may supply technical support, incident-related information, and recovery assistance when required.

### Responsibility Matrix

Role	Detection	Containment	Recovery	Documentation
Employees	Report	Assist	Assist	N/A
IT & Cybersecurity	Lead	Lead	Lead	Lead
System Administrators	Support	Support	Support	Support
Management	Oversight	Approve	Oversight	Review
Third-Party Providers	Support	Support	Support	N/A

## Incident Severity Classification

Master Sword Publishing will classify information security incidents based on their impact to business operations, systems, users, and data. Severity levels help determine response priorities, escalation requirements, and resource allocation.

### Low Severity

Definition: Suspicious activity with no confirmed compromise and minimal impact to business operations.

Examples:

- Spam email reported by a user
- Blocked phishing attempt
- Antivirus detection with no system impact
- Failed login attempts without account compromise

Response: Handled by IT & Cybersecurity department through normal operational procedures.

### Medium Severity

Definition: Potential compromise affecting a single user, device, or non-critical business system.

## Part 4: Network Security and Encryption & Server Administration

Examples:

- Employee clicks a phishing link but no credentials are entered
- Malware detected on a single workstation
- Unauthorized access attempt to a non-critical system
- Repeated suspicious login activity

Response: Investigation and containment actions initiated by IT & Cybersecurity staff.

### High Severity

Definition: Confirmed compromise involving user accounts, critical business systems, or sensitive company information.

Examples:

- Employee enters credentials into a phishing website
- Unauthorized access to Microsoft 365 services
- Malware affecting multiple devices
- Data exposure involving company information

Response: Immediate containment and escalation to management. Recovery activities prioritized to minimize business impact.

### Critical Severity

Definition: Major security incident resulting in significant business disruption, widespread compromise, ransomware activity, or substantial data loss.

Examples:

- Ransomware outbreak
- Multiple compromised user accounts
- Widespread network compromise
- Extended outage of critical business systems
- Large-scale data breach

Response: Immediate activation of the Incident Response Plan. Executive management and external service providers may be engaged as required.

### Severity Matrix

Severity Level	Color Code	Business Impact	Example
Low	Yellow	Minimal	Spam email or blocked phishing attempts
Medium	Orange	Limited	Suspicious activity affecting one user
High	Red	Significant	Confirmed account compromise
Critical	Dark Red	Severe	Widespread compromise or ransomware
Resolved	Green	Normal Operation	Systems have been restored

### MSPUB Phishing Campaign Example

- If an employee receives a phishing email and reports it without interacting with the message, the incident would be classified as Low Severity.

## Part 4: Network Security and Encryption & Server Administration

- If an employee clicks the phishing link but does not enter credentials, the incident would be classified as Medium Severity.
- If an employee enters credentials into a fraudulent login page, the incident would be classified as High Severity and immediate containment actions would be required.

### Incident Scenario

Master Sword Publishing just completed a successful phishing email campaign to get a general scope of how employees are at recognizing a phishing attack.

Incident ID: MSPUB-SAT-2026-001

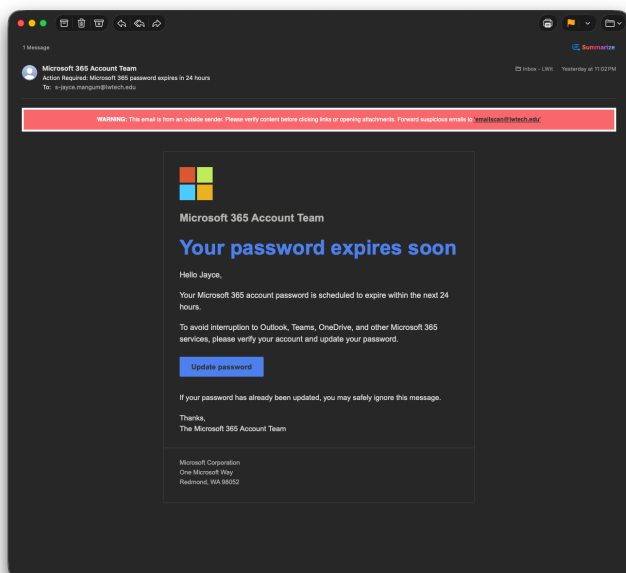
Campaign Start Date: 06 June 2026 9:00 AM

Campaign End Date: 10 June 2026 9:00 PM

### Phishing Simulation Outcomes Severity Levels

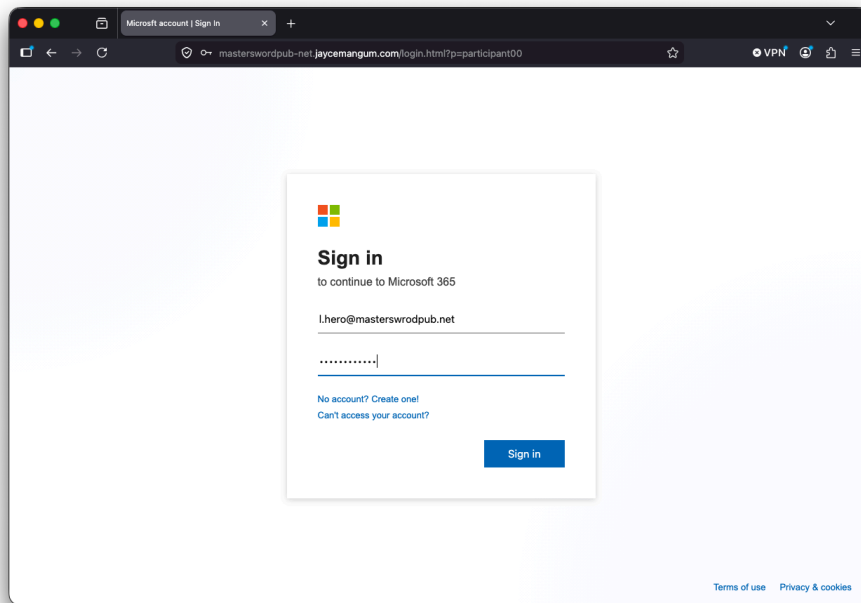
Scenario	Severity Level
User reports email without clicking	Low
User opens email but takes no action	Low
User clicks phishing link only	Medium
User reaches login page but enters nothing	Medium
User enters credentials into phishing page	High
Multiple users enter credentials	High
Evidence of account compromise after credential entry	High
Multiple compromised accounts affecting business operations	Critical
Malware/ransomware delivered through phishing campaign	Critical

MSPUB employees received an email from what appears to be from Microsoft 365 Account Team requiring immediate action to reset their Microsoft 365 account password.

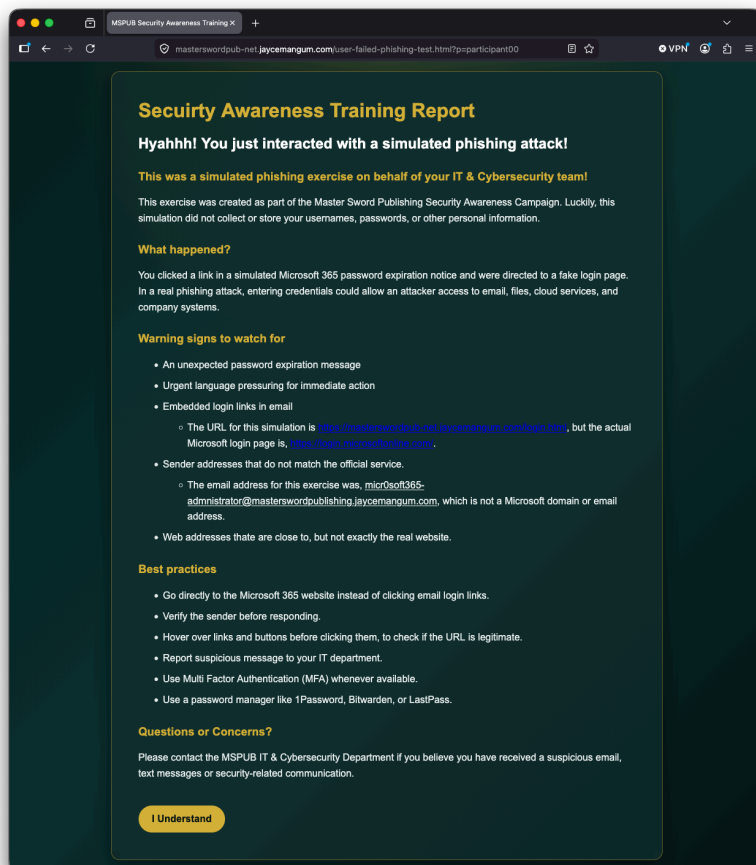


## Part 4: Network Security and Encryption & Server Administration

Clicking the “Update Password” button takes users to a suspicious sign-in page asking them to enter their account name and password. In an actual phishing attack, the credential form could record the user’s username and password.



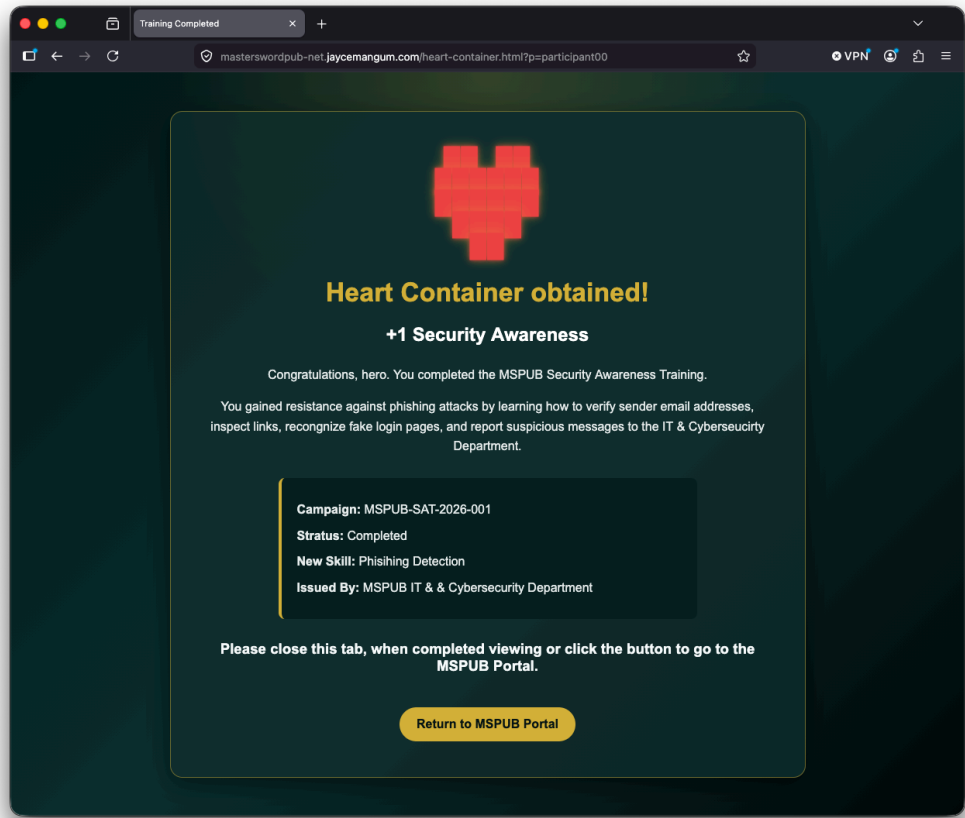
In this controlled simulation attack, the user’s credentials were not recorded; however, clicking any links or buttons was logged. Clicking the “Sign in” button took users to a “Security Awareness Training” page where users learned about how to spot a phishing email and to immediately report them to the IT department.





Part 4: Network Security and Encryption & Server Administration

Once users completed the training material, they clicked the “I Understand” button, and it took them to a certification page, congratulating them on completing the training. They were instructed to close this tab.



Each employee was given a ParticipantID to track their progress in an Amazon Web Services DynamoDB, which can then be recorded into an employee progress tracker.

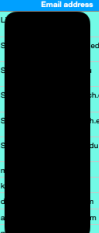
Table: MSPUB-SAT-2026-001-Results - Items returned (50)

Scan started on June 06, 2026, 17:30:39

 Actions 

<input type="checkbox"/>	event_id (String)	campaign_id	event_type	page	participa...	timestamp
<input type="checkbox"/>	<a href="#">7117e50c-dd76-4bc2-9874-0cc865dc3156</a>	MSPUB-SAT-2026-001	training_completed	heart-container.html	participant00	2026-06-06T22:40:54.333222+00:00
<input type="checkbox"/>	<a href="#">8978e452-a242-4c8d-a3c9-9c34cf4c58c7</a>	MSPUB-SAT-2026-001	training_page_view	user-failed-phishing-test.html	participant00	2026-06-06T22:40:22.062894+00:00
<input type="checkbox"/>	<a href="#">a079343a-c841-407b-9aad-4f970fe7435b</a>	MSPUB-SAT-2026-001	login_attempt	login.html	participant00	2026-06-06T22:40:21.929175+00:00
<input type="checkbox"/>	<a href="#">daf649d0-987d-48fa-97a7-4bd7120d0fc4</a>	MSPUB-SAT-2026-001	email_link_clicked	login.html	participant00	2026-06-06T22:39:22.327141+00:00

The IT & Cybersecurity department logs this in a separate spreadsheet to track which employees either ignored or reported the email, or if the employee clicked the link, entered their credentials in the form, and went through the training.

Participant Tracker											
Participant ID	Person	Email address	Email Name	Custom Email Button Link ID	Email Sent	Email Sent Date	Initial Link Clicked	Login Attempt Clicked	Training Viewed	Training Completed	Notes
participant01	Linda E.		Linda	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant01">https://masterswordpub-net.jaycemangum.com/login.html?p=participant01</a>	✓	6/6/26 10:25 AM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link.
participant05	Mihail B.		Mihail	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant05">https://masterswordpub-net.jaycemangum.com/login.html?p=participant05</a>	✓	6/6/26 10:15 AM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link.
participant09	Iltu I.		Iltu	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant09">https://masterswordpub-net.jaycemangum.com/login.html?p=participant09</a>	✓	6/6/26 10:17 AM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link.
participant13	Maksim M.		Maksim	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant13">https://masterswordpub-net.jaycemangum.com/login.html?p=participant13</a>	✓	6/6/26 10:18 AM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link.
participant17	Mamadou S.		Mamadou	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant17">https://masterswordpub-net.jaycemangum.com/login.html?p=participant17</a>	✓	6/6/26 10:20 AM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link.
participant18	Caden T.		Caden	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant18">https://masterswordpub-net.jaycemangum.com/login.html?p=participant18</a>	✓	6/6/26 10:21 AM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	College's email filter system appears to have tried verifying the email link. Participant has either ignored the email, or didn't click the link.
participant37	Taylor M.		Taylor	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant37">https://masterswordpub-net.jaycemangum.com/login.html?p=participant37</a>	✓	6/6/26 10:09 AM	✓	✓	✓	✓	Opened link twice, then filled out the form, and proceeded through the exercise.
participant38	Karl T.		Karl	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant38">https://masterswordpub-net.jaycemangum.com/login.html?p=participant38</a>	✓	6/6/26 9:30 AM	✓	✓	✓	<input type="checkbox"/>	Ignored email or didn't click the link in the email.
participant39	David M.		David	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant39">https://masterswordpub-net.jaycemangum.com/login.html?p=participant39</a>	✓	6/6/26 9:26 AM	✓	✓	✓	✓	Opened link twice, then filled out the form, and proceeded through the exercise.
participant40	Anna J.		Anna	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant40">https://masterswordpub-net.jaycemangum.com/login.html?p=participant40</a>	✓	6/6/26 9:16 AM	✓	✓	✓	✓	
participant41	Mason H.		Mason	<a href="https://masterswordpub-net.jaycemangum.com/login.html?p=participant41">https://masterswordpub-net.jaycemangum.com/login.html?p=participant41</a>	✓	6/6/26 9:38 AM	✓	✓	✓	✓	
Statistics											
Metric	Count	Percentage									
Emails Sent	11	100.00%									
Links Clicked	5	45.45%									
Login Attempts	5	45.45%									
Training Viewed	5	45.45%									
Training Completed	4	36.36%									
Did Not Respond	6	54.55%									

### AWS DynamoDB Event Types Severity Levels

event_type ID	Severity Level	Reason
email_link_clicked	Medium	User(s) accessed a phishing link
login_attempt	High	User entered their credentials into a credential capture form
training_page_view	High	User submitted their credentials to a capture form and reached remediation
training_completed	Resolved	User completed the Security Awareness Training

Looking at participant00's data on the AWS DynamoDB table, the user first clicked the email link and was brought to the credential capture form. This would be classified as Medium Severity. The user then entered their credentials into the credentials capture form and clicked the fake "sign in" button, which submitted the form. These events escalated the severity level to High. Once the user read through the training material and clicked "I Understand," the user completed their training on phishing emails and moved the incident into the Resolved level.

### Security Awareness Campaign Exception

Incidents generated during authorized Master Sword Publishing Security Awareness Training campaigns are simulated events and do not represent actual compromises. Severity classifications may still be assigned for training and reporting purposes to measure employee susceptibility and improve future awareness efforts.

## Communication & Escalation Procedures

### Purpose

The purpose of communication and escalation procedures is to ensure that security incidents are reported, communicated, and escalated in a timely manner. Effective communication helps Master Sword Publishing coordinate response activities, reduce business impact, and maintain accurate documentation throughout the incident lifecycle.

### Incident Reporting

All Master Sword Publishing employees are responsible for reporting suspected security incidents immediately to the IT & Cybersecurity department. Reports may include suspicious emails, phishing attempts, malware alerts, unauthorized access attempts, unusual system behavior, or any activity that could affect the confidentiality, integrity, or availability of company information systems.

Employees should provide as much information as possible, including screenshots, email messages, timestamps, and descriptions of observed activity.

### Escalation Requirements

**Low Severity** incidents will be handled by the IT & Cybersecurity Department through normal operational procedures. Management notification is not typically required unless the incident becomes recurring or indicates a larger security issue.

**Medium Severity** incidents will be investigated by the IT & Cybersecurity Department. System Administrators may be notified when technical assistance is required. Management may be informed if business operations could be affected.

**High Severity** incidents require immediate notification of Management, the IT & Cybersecurity Department, and System Administrators. Containment and recovery efforts should begin immediately to minimize business impact.

## Part 4: Network Security and Encryption & Server Administration

**Critical Severity** incidents require immediate escalation to executive management and all appropriate response personnel. External service providers, cloud providers, legal counsel, law enforcement, or regulatory agencies may be contacted when required by law, contractual obligations, or the severity of the incident.

### Communication Methods

Audience	Communication Method
Employees	Email, Microsoft Teams, Phone
IT & Cybersecurity Department	Email, Microsoft Teams, Phone
System Administrators	Email, Microsoft Teams, Phone
Management	Email, Phone, Scheduled Briefings
Third-Party Providers	Vendor Support Portals, Email, Phone

### Incident Documentation

All communications related to an incident must be documented. Documentation should include incident reports, notifications, response actions, decisions made during the investigation, recovery activities, and post-incident review findings. Incident documentation will be retained in accordance with MSPUB record retention policies and may be used to support future investigations, audits, security awareness training, and continuous improvement activities.

During the phishing simulations and security awareness campaigns, participant interactions, training completion records, and incident metrics may be collected and reviewed by the IT & Cybersecurity department to evaluate employee awareness and improve future training initiatives.

## Evidence Collection & Preservation

### Purpose

Evidence collection and preservation are to ensure that relevant information is identified, collected, protected, and retained throughout the incident response process. Proper evidence handling supports investigations, recovery efforts, root cause analysis, audits, and potential legal or regulatory requirements.

### Evidence Collection

During a security incident, Master Sword Publishing personnel will collect relevant evidence to support investigation and response activities. Evidence should be gathered as soon as possible while minimizing disruption to business operations and preserving data integrity.

### Examples of Evidence

Evidence collected during an incident may include:

- System and server logs
- Authentication and login records
- Firewall and network logs
- Email messages and email headers
- Screenshots of suspicious activity
- Malware detection and antivirus reports
- User statements and incident reports
- Security alerts and monitoring records
- AWS CloudWatch logs
- AWS Lambda execution logs
- DynamoDB event records

## Part 4: Network Security and Encryption & Server Administration

- Microsoft 365 audit logs
- Backup and recovery records

### Evidence Preservation

Collected evidence must be protected from unauthorized modification, deletion, or disclosure. Evidence should be stored in secure locations and access should be limited to personnel directly involved in the incident. Whenever possible, original evidence should be preserved and copies should be used for analysis to maintain data integrity.

### Chain of Custody

Master Sword Publishing will maintain documentation identifying who collected evidence, when the evidence was collected, where it was stored, and who has accessed it. Maintaining a chain of custody helps preserve the integrity and reliability of evidence throughout the investigation process.

### Evidence Retention

Incident-related evidence will be retained in accordance with Master Sword Publishing's record retention requirements and organizational policies. Evidence may be used for incident investigations, post-incident reviews, compliance audits, security awareness training, and future security improvements.

### Phishing Simulation Example

For phishing awareness campaigns, evidence may include participant interaction records, phishing email delivery records, login attempt logs, training page views, training completion events, and AWS DynamoDB records collected throughout the Master Sword Publishing Security Awareness Training platform. These records may be analyzed to measure employee awareness and improve future training initiatives.

## Continuous Improvement

### Purpose

Continuous improvements ensure that Master Sword Publishing learns from security incidents and continuously strengthens its security posture. Following each incident, the organization will review response activities, identify areas for improvement, and implement corrective actions to reduce the likelihood and impact of future incidents.

### Post-Incident Review

Following the resolution of an incident, Master Sword Publishing will conduct a Post-Incident Review to evaluate the effectiveness of the response process. This review should occur as soon as recovery activities have been completed.

The review will focus on:

- Incident timeline and sequence of events
- Effectiveness of detection and reporting
- Containment and eradication activities
- Recovery efforts
- Communication and escalation procedures
- Impact of business operations
- Opportunities for improvement

### Root Cause Analysis

Master Sword Publishing will perform a Root Cause Analysis to identify the underlying factors that contributed to the incident. Understanding the root cause helps prevent similar incidents from occurring in the future.

## Part 4: Network Security and Encryption & Server Administration

Examples may include:

- Successful phishing attacks
- Weak passwords
- Lack of user awareness
- Misconfigured systems
- Delayed detection of suspicious activity
- Unpatched software vulnerabilities
- Inadequate security controls

### Corrective Actions

Corrective actions will be developed and implemented to address weaknesses identified during the Post-Incident Review.

Examples may include:

- Updating security policies and procedures
- Improving monitoring and alerting capabilities
- Enhancing access control measures
- Implementing additional security controls
- Updating incident response documentation
- Strengthening authentication requirements

### Security Awareness and Training (SAT)

Master Sword Publishing recognizes that employees play a critical role in information security. Security awareness training will be reviewed and updated regularly based on incident trends and lessons learned.

Activities may include:

- Additional phishing awareness training
- Simulated phishing campaigns
- Security awareness reminders
- User education on reporting suspicious activity
- Review of common social engineering techniques

### Future Testing and Exercises

To ensure continued readiness, Master Sword Publishing will periodically test its Incident Response Plan through tabletop exercises, phishing simulations, and other security awareness activities. Results from these exercises will be reviewed and used to improve response procedures, training materials, and organizational preparedness.

### Continuous Improvement Objectives

Master Sword Publishing will strive to:

- Improve incident detection capabilities
- Reduce response and recovery times
- Increase employee security awareness
- Strengthen security controls
- Improve documentation and record-keeping
- Reduce the likelihood of future incidents

Results from the MSPUB Security Awareness Training (SAT) phishing simulation program will be reviewed to identify trends in employee behavior, measure training effectiveness, and support future security awareness initiatives. Findings may be incorporated into future training campaigns, incident response procedures, and security improvement efforts.

### Legal & Regulatory Considerations

Master Sword Publishing will comply with applicable legal, contractual, and regulatory requirements when responding to security incidents. Depending on the nature and severity of an incident, MSPUB may be required to preserve evidence, notify affected parties, coordinate with third-party service providers, or comply with reporting obligations.

All incident investigations will be conducted in accordance with organizational policies and applicable laws. Sensitive information collected during investigations will be protected from unauthorized disclosure, and access will be limited to authorized personnel.

### Document Control

The purpose of Document Control and Maintenance is to ensure that the Master Sword Publishing Incident Repose Plan remains current, accurate, and effective. This document will be reviewed regularly and updated as necessary to reflect changes in technology, business operations, security requirements, and lessons learned from incidents and exercises.

Item	Value
Document Name	MSPUB Incident Response Plan
Version	1.0
Owner	MSPUB IT & Cybersecurity Department
Approved By	MSPUB Management
Effective Date	June 2026
Review Cycle	Annually or following a major security incident

#### Review & Update Process

The MSPUB IT & Cybersecurity department is responsible for reviewing and maintaining this Incident Response Plan. Reviews will be conducted annually and after significant security incidents, organizational changes, technology changes, or regulatory updates.

#### Distribution

The Incident Repose Plan will be made available to authorized Master Sword Publishing personnel for incident repose activities. Employees may be provided with relevant portions of the plan based on their roles and responsibilities as part of their onboarding documentation and in the employee handbook.

#### Plan Testing

To ensure effectiveness, Master Sword Publishing will periodically test the Incident Response Plan through tabletop exercises, phishing simulations, security awareness training activities, and incident response drills. Results from testing activities will be documented and used to support continuous improvement efforts.

# References

Amazon Web Services. (n.d.). Amazon CloudWatch: What is Amazon CloudWatch?  
<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html>

Amazon Web Services. (n.d.). Amazon DynamoDB developer guide: Introduction to Amazon DynamoDB.  
<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html>

Amazon Web Services. (n.d.). Amazon Lambda developer guide: What is AWS Lambda?  
<https://docs.aws.amazon.com/lambda/latest/dg/welcome.html>

Amazon Web Services. (n.d.). Amazon S3 user guide.  
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html>

Apple Inc. (n.d.). *Mac User Guide*.  
<https://support.apple.com/guide/mac-help/welcome/mac>

Canonical Ubuntu. (n.d.). *Download Ubuntu Desktop*.  
<https://ubuntu.com/download/desktop>

Canonical Ubuntu. (n.d.). *Get Ubuntu Server*.  
<https://ubuntu.com/download/server#system-requirements-tab-lts>

Hyperproof. (n.d.). *The ultimate guide to ISO 27001: the complete guide*.  
<https://hyperproof.io/iso-27001/>

Kali Linux. (n.d.). *Installing Kali Linux*.  
<https://www.kali.org/docs/installation/hard-disk-install/>

Microsoft. (n.d.). *Hardware requirements for Windows Server*.  
<https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements?tabs=cpu&pivots=windows-server-2025>

Microsoft. (n.d.). *Windows 11 System Requirements*.  
<https://support.microsoft.com/en-us/windows/windows-11-system-requirements-86c11283-ea52-4782-9efd-7674389a7ba3>

National Institute of Standards and Technology. (2025 July 18). *NIST Cybersecurity Frame and ISO/IEC 27001 mappings*.  
<https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=154#/olir/home>

NSF. (n.d.). *ISO/IEC 27001 information security management systems*.  
<https://www.nsf.org/management-systems/iso-iec-27001>

Parallels International GmbH. (n.d.). *Parallels desktop for Mac 26 user's guide*.  
<https://docs.parallels.com/landing/pdfm-ug>

Reddit. (2022, December 3). *Ubuntu on a Windows domain with Active Directory* [Online forum discussion].  
Reddit.  
[https://www.reddit.com/r/linuxadmin/comments/zbcmt9/ubuntu\\_on\\_a\\_windows\\_domain\\_with\\_active\\_directory/](https://www.reddit.com/r/linuxadmin/comments/zbcmt9/ubuntu_on_a_windows_domain_with_active_directory/)

Tech With Emilio. (2021, July 7). *How to bind a Mac to Active Directory (join macOS to AD)* [Video]. YouTube.  
<https://www.youtube.com/watch?v=jHqY2txtQ0k>

Ubiquiti Inc. (n.d.). *UniFi Network documentation*.

<https://help.ui.com/hc/en-us/sections/6582310816535-Network>

W3Schools. (n.d.). *HTML tutorial*.

<https://www.w3schools.com/html/default.asp>

W3Schools. (n.d.). *CSS tutorial*.

<https://www.w3schools.com/css/default.asp>