

## Group Policy Management with Active Directory Home Lab

### **Objective:**

To design and implement a secure, scalable Active Directory (AD) environment using Windows Server 2022. This project demonstrates my core AD skills for Group policy creation and management.

### **Tools and Technologies Used:**

- Oracle VirtualBox – Virtualization platform
- Windows Server 2022 – Domain Controller and Active Directory Domain Services (ADDS)
- Microsoft Active Directory – Directory management and user provisioning
- PowerShell – Scripting for automation
- Draw.io –Diagramming

### **Project Scope:**

**Platform:** Oracle VirtualBox

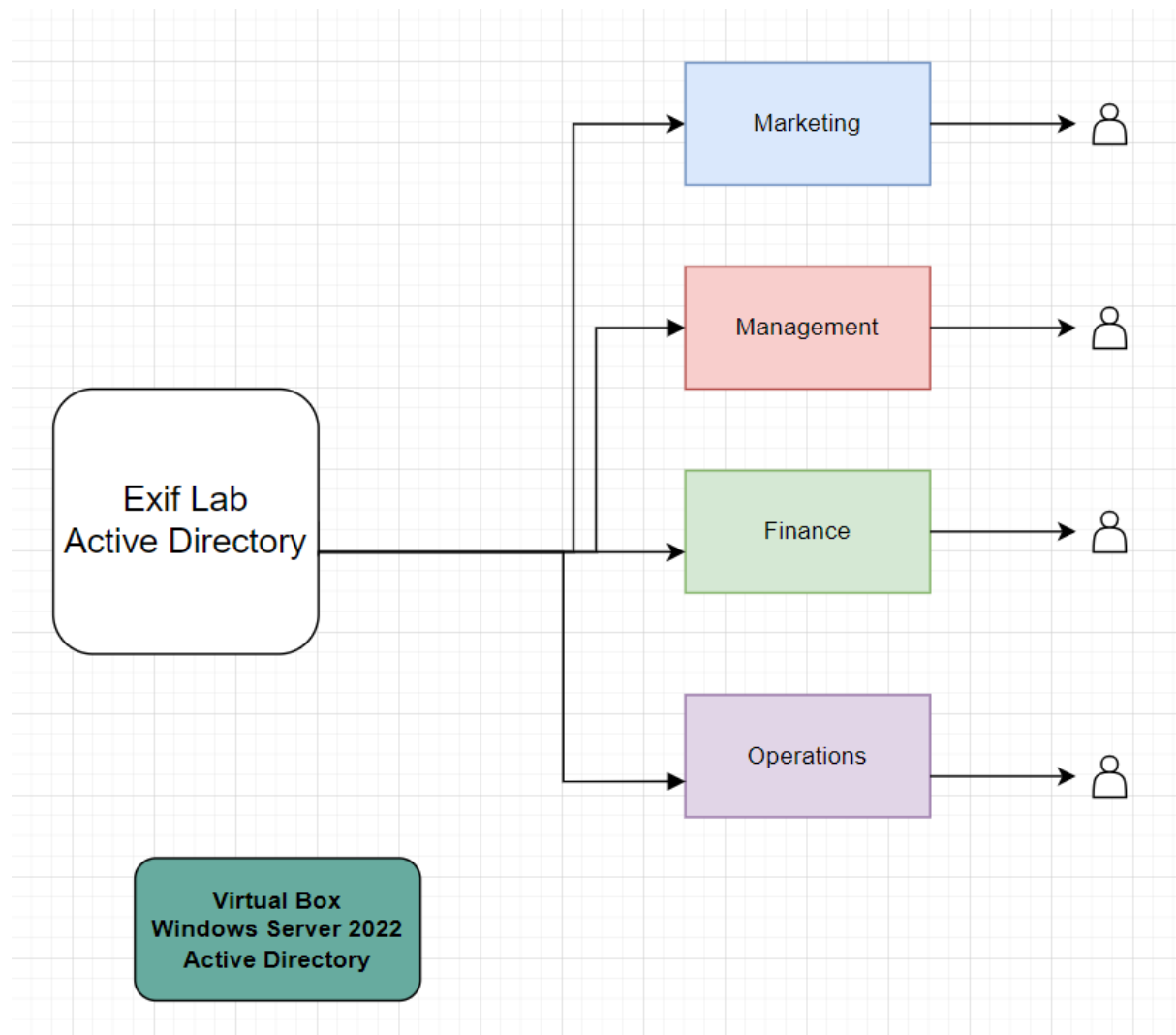
**Domain:** exiflab.com

**Operating System:** Windows Server 2022 (4GB RAM , 25GB Storage), Window 10 Pro (64bit)

## Environment Setup:

Deployed a virtualized Windows Server 2022 instance on Oracle VirtualBox with internal networking to enable inter-VM communication. Installed Active Directory Domain Services (ADDS) and promoted the server to a Domain Controller (DC) for the domain exiflab.com.

---

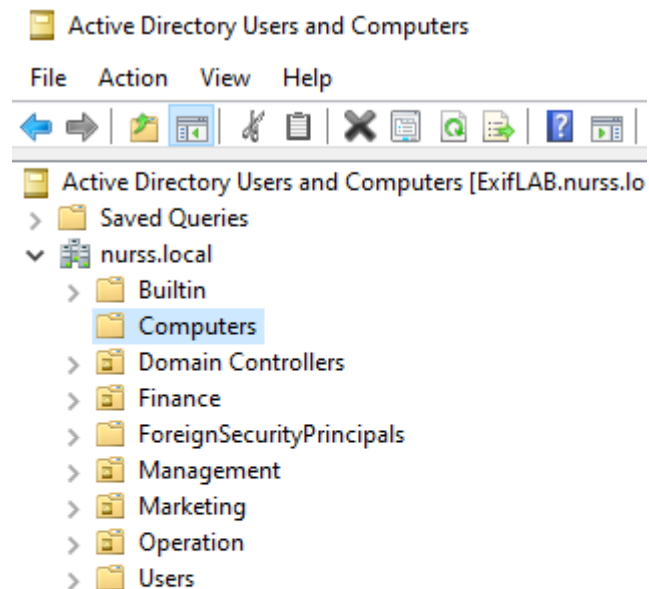


## Organizational Unit (OU) Structure:

Created a structured Organizational Unit (OU) hierarchy to reflect company departments:

- Finance
- Operations
- Management
- Marketing

I have assigned 3-5 users to simulate a real world.



To showcase automation skills, I created the computer OU in the PowerShell – find it my ps1 script file.

It has been used to automate the OU creation using PowerShell which enhances efficiency repeatability and accuracy.

## Connecting with Windows Client

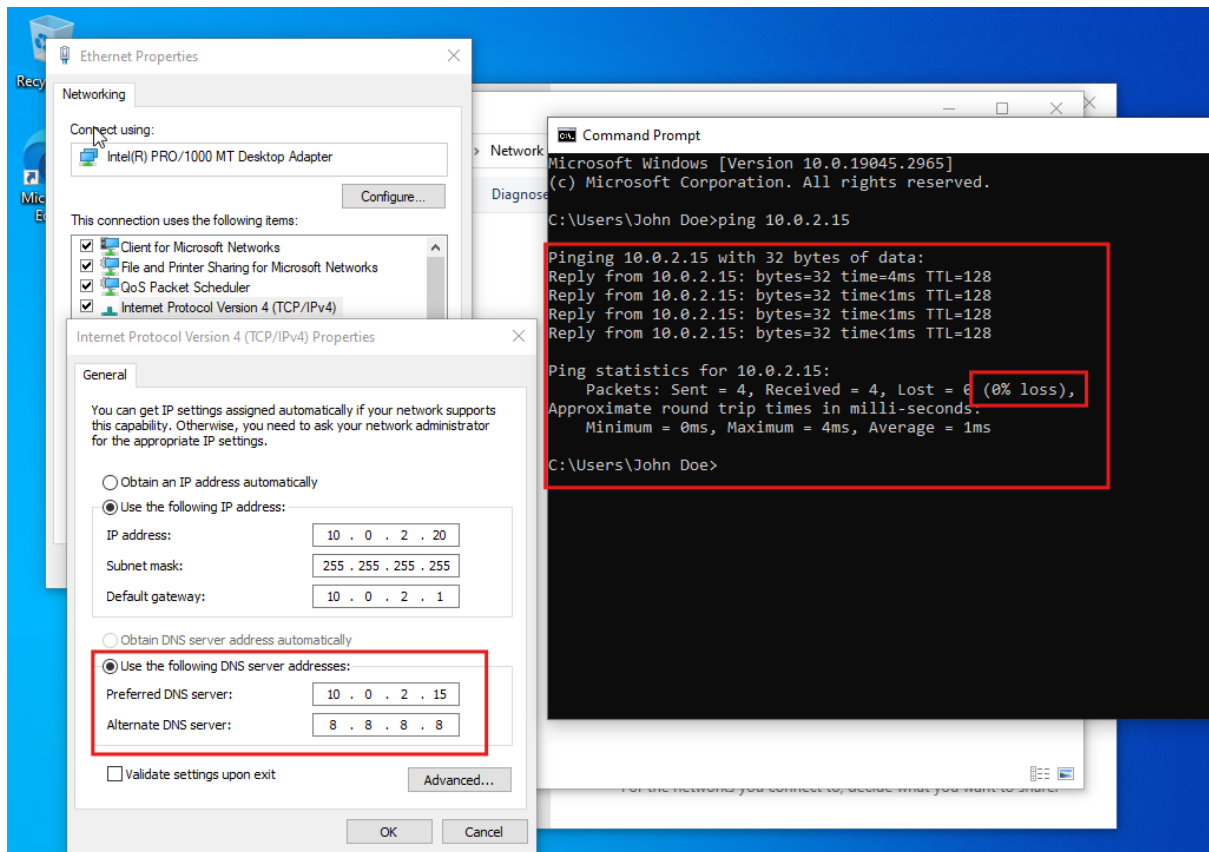
The project presented several challenges along the way, with one of the most significant being the installation of the Windows 10 Professional ISO on VirtualBox. I encountered an error related to the product key in the unattended answer file during the installation process.

After conducting some research on online forums, I discovered a solution. I decided to bypass the alert in the VirtualBox expert settings under storage, which resolved the issue and allowed the installation to proceed successfully.

Following the installation, I navigated to the **Network Adapter settings > Change Adapter Options> Properties > IPv4.**

Here, I configured a static IP address and entered the DNS address of the Active Directory domain.

To verify the connection, I used **Command Prompt** to ping the DNS address, which resulted in a successful connection with 0% packet loss.



## **Group Policy Configuration**

Group Policy in Active Directory allows administrators to define and manage policies for users and computers within the domain, ensuring consistent configurations across the network.

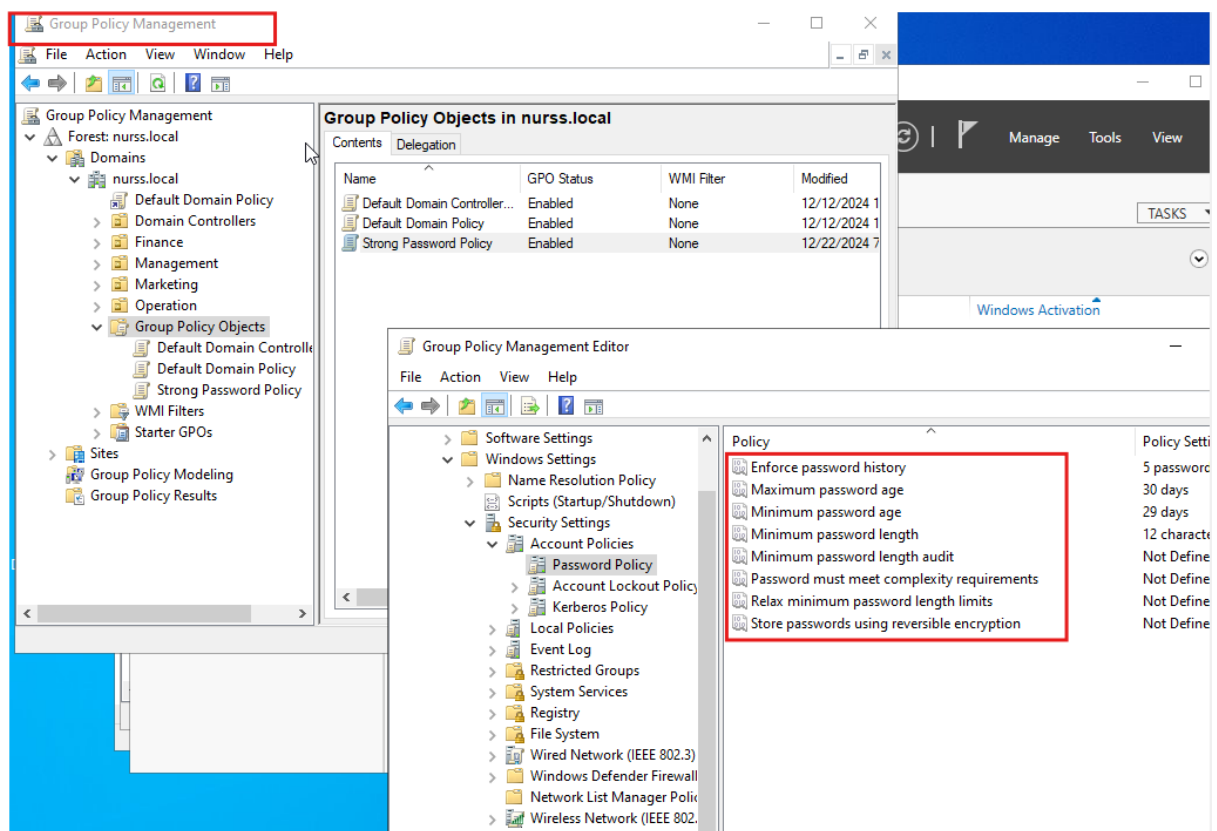
For this project, I configured cross-functional group policies that applied uniformly across all departments. These policies were designed to enforce security settings, software installations, and user configurations, ensuring that the same standards and practices were maintained, regardless of the department or location.

# 1. Password Hardening Policy (Security Compliance)

## Configuration:

### Tools> Group Policy Management > Create Group Policy Objects

- Enforce password history: 5 passwords remembered
- Minimum password length: 12 characters
- Maximum password age: 30 days
- Password complexity: Enabled

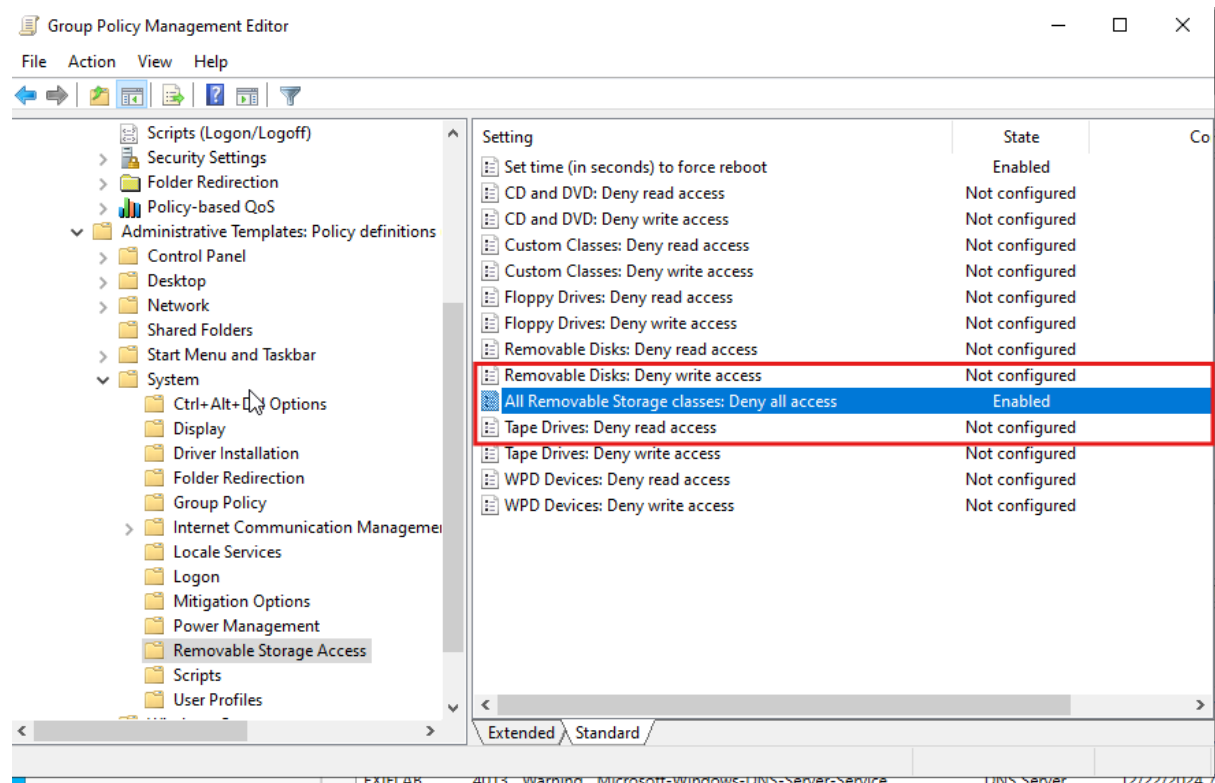


Enforcing strict password policies is fundamental to defend against brute-force attacks and credential theft. By requiring complex passwords and regular changes, this policy mitigates password reuse and ensures stronger authentication across departments. It aligns with compliance frameworks like NIST and ISO27001

## 2. Disable Removable Media

### Configuration:

Administrative Templates: Policy Definition > System > All Removable Storage Classes: Deny all access

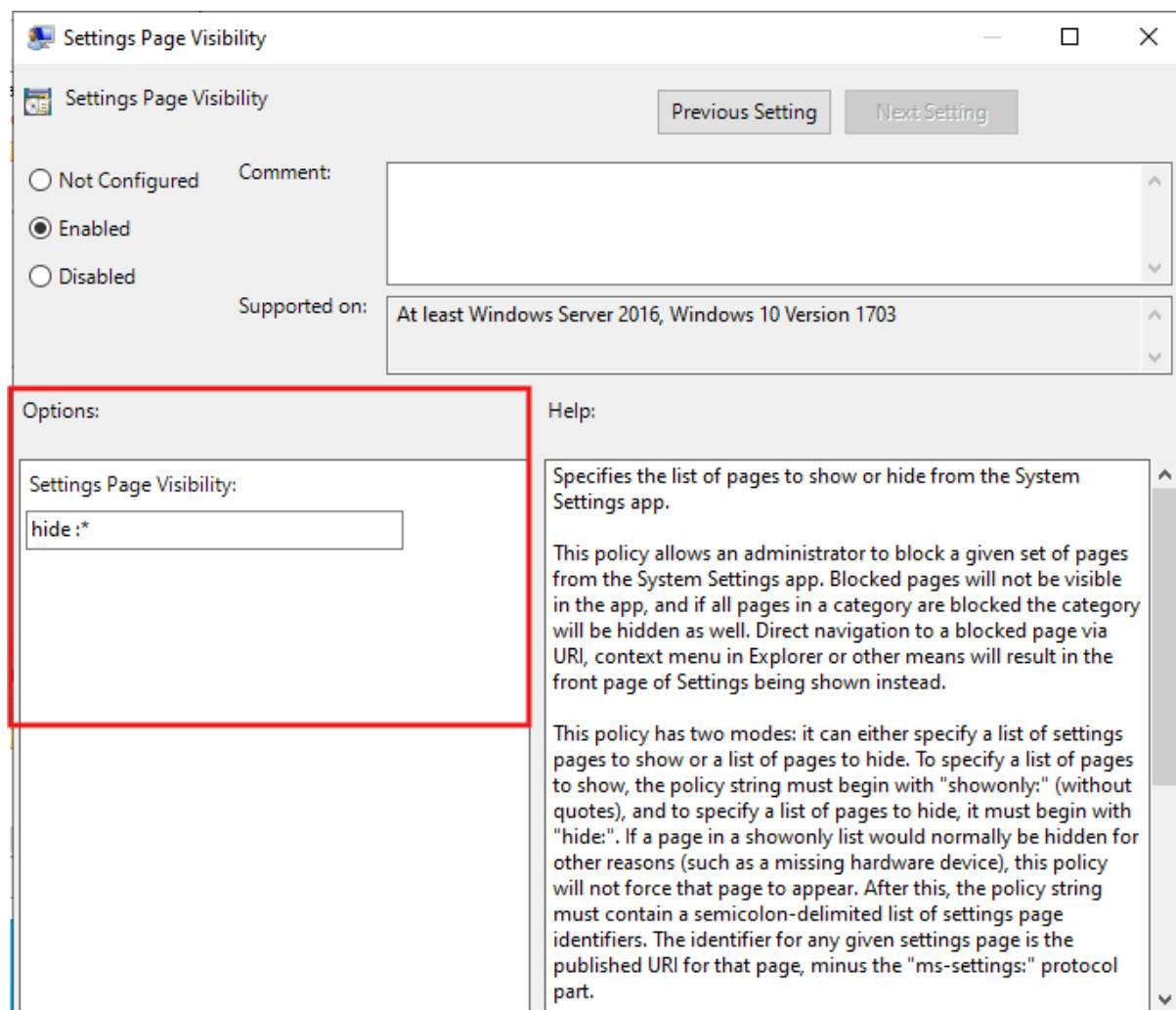


Blocking USB drives and external devices prevents data exfiltration, malware introduction, and insider threats. This proactive policy safeguards sensitive financial data and intellectual property by preventing unauthorized data transfers. It can be critical for industries that handle sensitive information (e.g., Finance, HR), ensuring data integrity and confidentiality.



### 3. Block Control Panel Access (Restrict System Changes)

**Configuration:** Administrative Templates > Control Panel > Settings Page Visibility.  
Here I enabled the option by using the command **hide\*** to hide all the all-control panel items



Settings Page Visibility

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Server 2016, Windows 10 Version 1703

Options:

Settings Page Visibility:

hide:\*

Help:

Specifies the list of pages to show or hide from the System Settings app.

This policy allows an administrator to block a given set of pages from the System Settings app. Blocked pages will not be visible in the app, and if all pages in a category are blocked the category will be hidden as well. Direct navigation to a blocked page via URL, context menu in Explorer or other means will result in the front page of Settings being shown instead.

This policy has two modes: it can either specify a list of settings pages to show or a list of pages to hide. To specify a list of pages to show, the policy string must begin with "showonly:" (without quotes), and to specify a list of pages to hide, it must begin with "hide:". If a page in a showonly list would normally be hidden for other reasons (such as a missing hardware device), this policy will not force that page to appear. After this, the policy string must contain a semicolon-delimited list of settings page identifiers. The identifier for any given settings page is the published URI for that page, minus the "ms-settings:" protocol part.

Limiting access to system settings reduces the risk of unauthorized system modifications or misconfigurations by end users. This policy enforces role-based access control by ensuring only administrators can alter critical system settings, preventing accidental or malicious changes.

It simplifies system administration by maintaining consistent configurations across user environments.

^ \_\_\_\_ ^

Lastly, I look forward to extending on this project with the principles learned from my CompTIA Security+ certification. Happy Holidays.

.