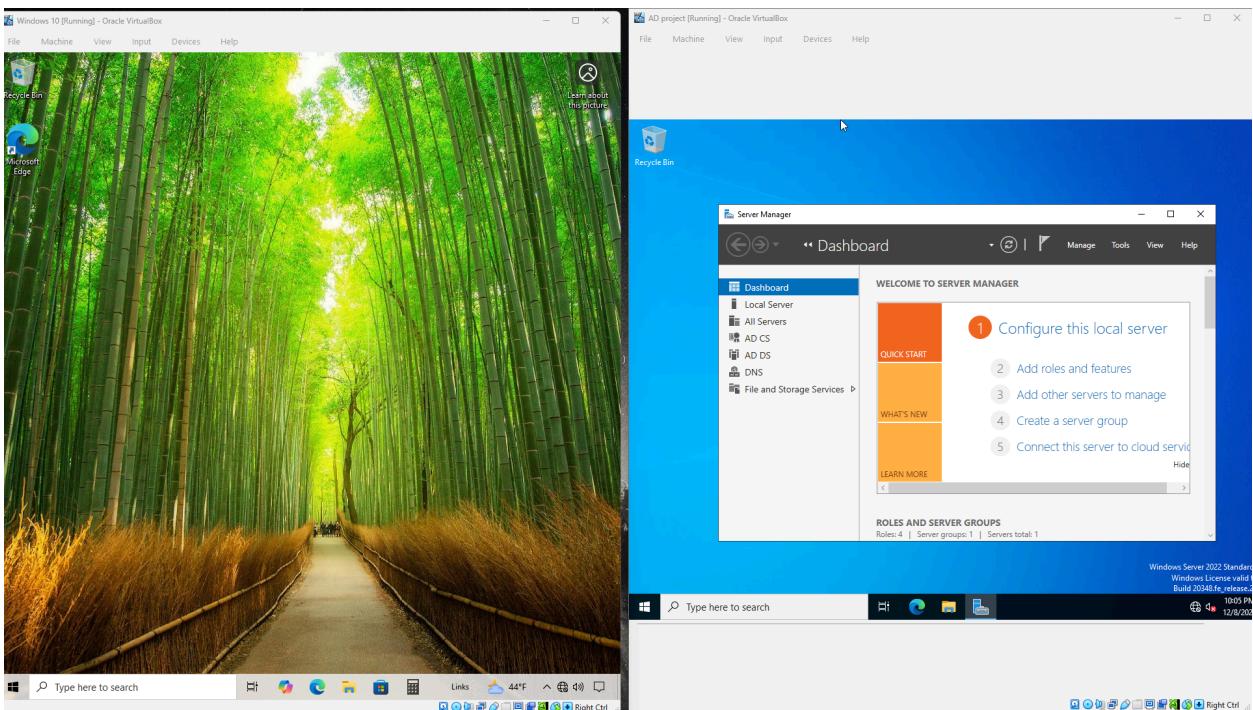
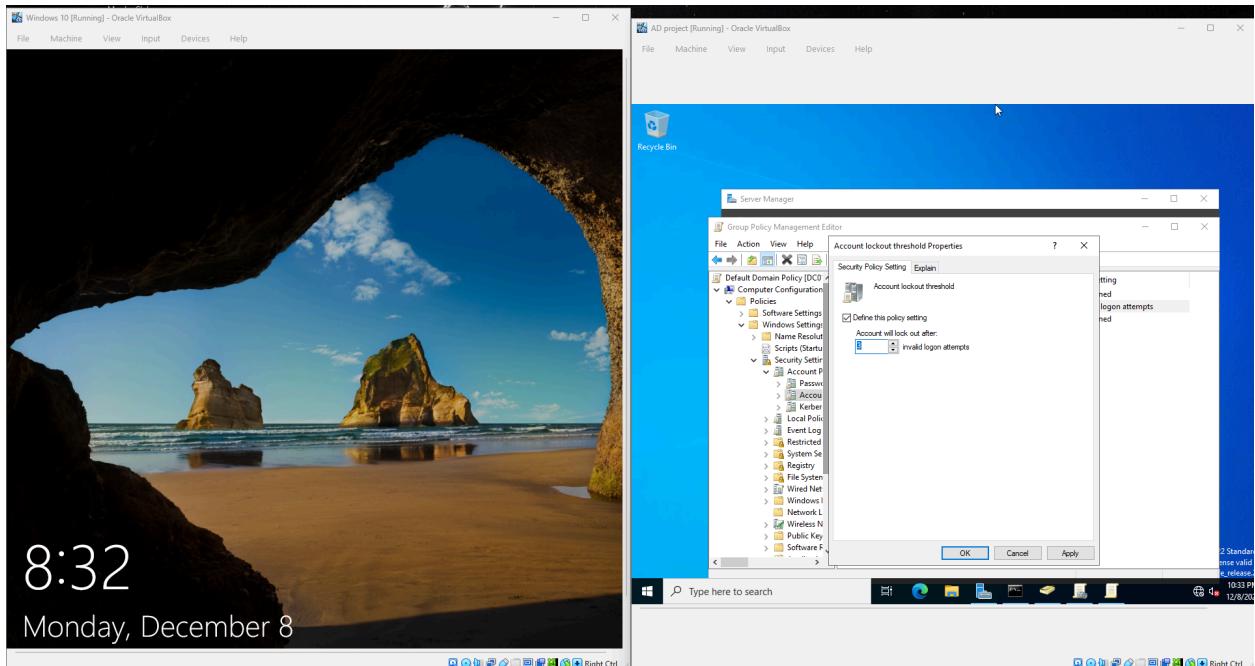


This lab demonstrates my ability to deploy and manage a Windows Server 2022 Active Directory environment using Oracle VirtualBox. I implemented common enterprise GPOs such as account lockout policy, USB device restrictions, and Control Panel access prevention. I also created OUs, security groups, and tested client-side enforcement.

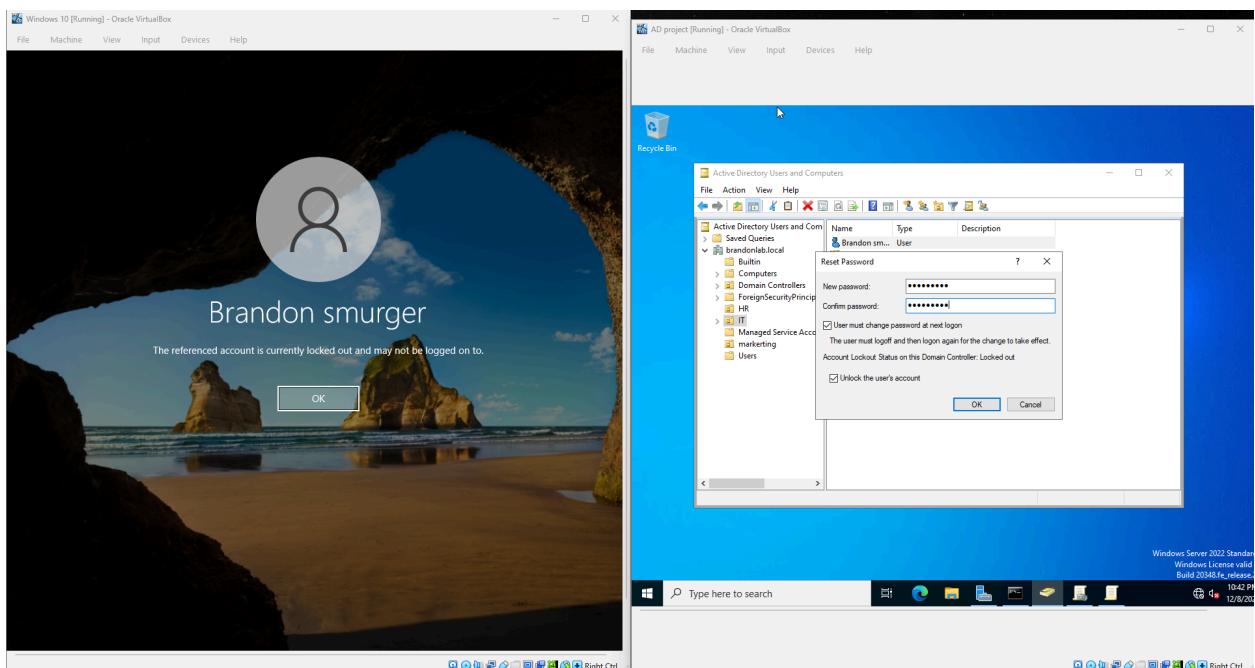
VM1 Windows Server 2022 Domain Controller (AD DS, DNS)
VM2 Windows 10 Domain-joined client



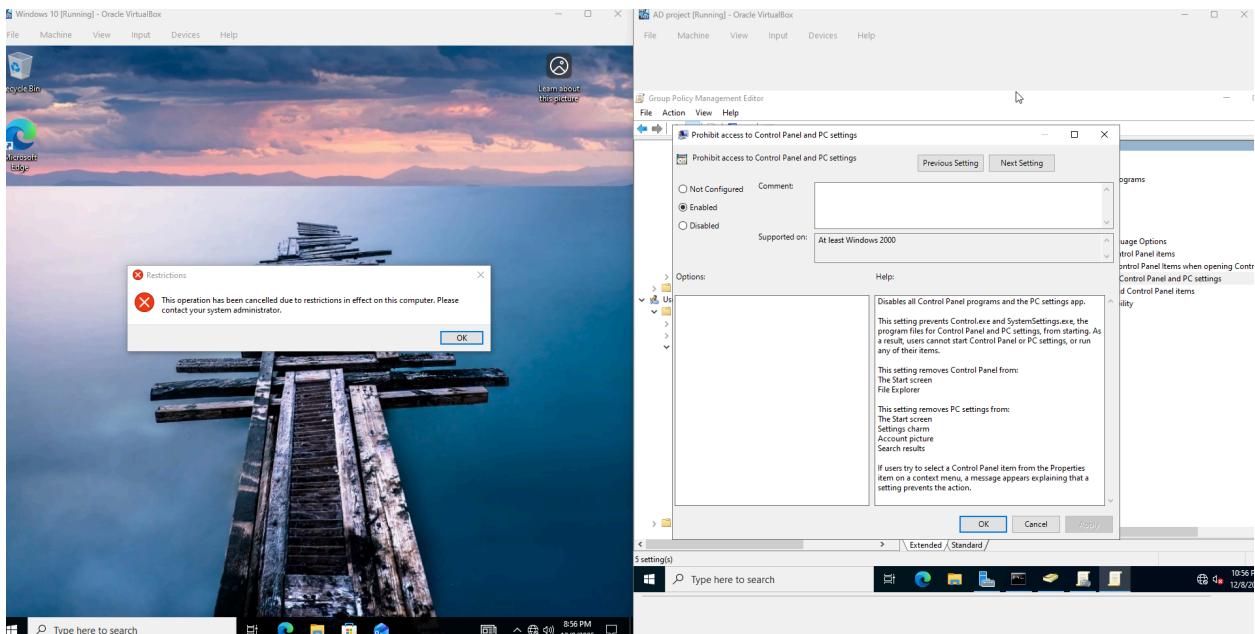
First I opened the group policy management to limit the number of attempts allowed before lockout (= Computer Config → Policies → Windows Settings → Security Settings → Account Lockout)



The user has locked themselves out so, I reset their password and unlocked the account.

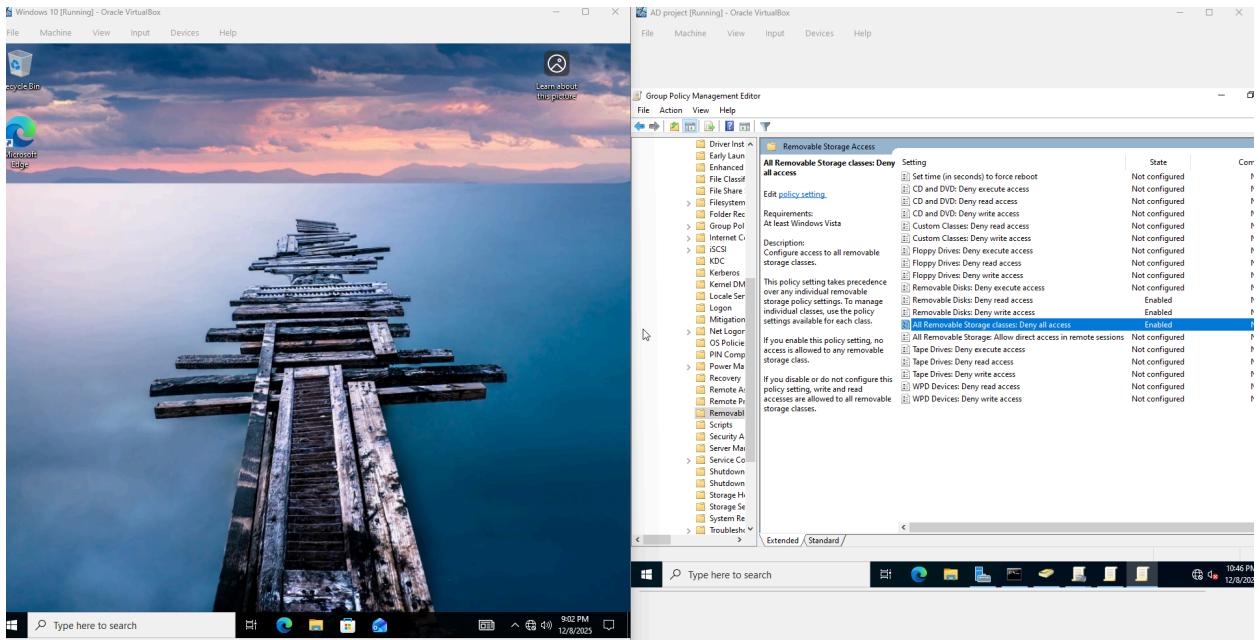


**I went back into the Group Policy Management Console to disable access to the Control Panel and Settings so the user wouldn't accidentally change system configurations
(User Config → Policies → Administrative Templates → Control Panel → Prohibit access to Control Panel and PC settings)**

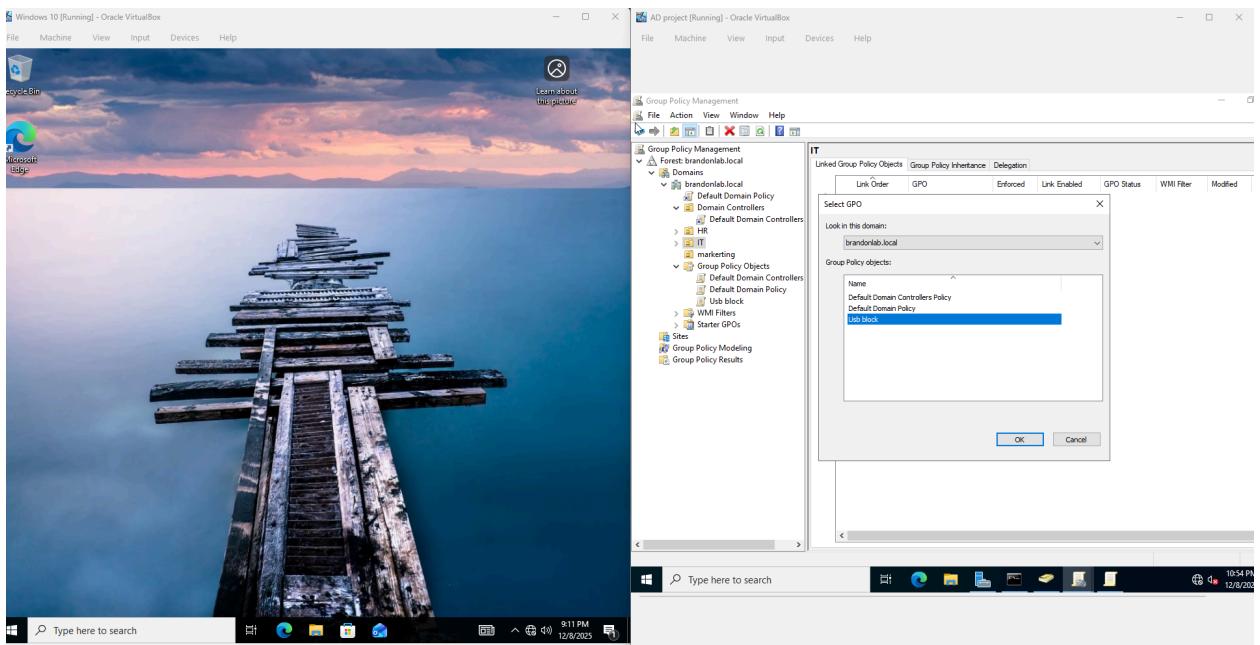


I created a new GPO To Block removable usb devices to prevent malware introduction & data theft(Computer Config → Policies →

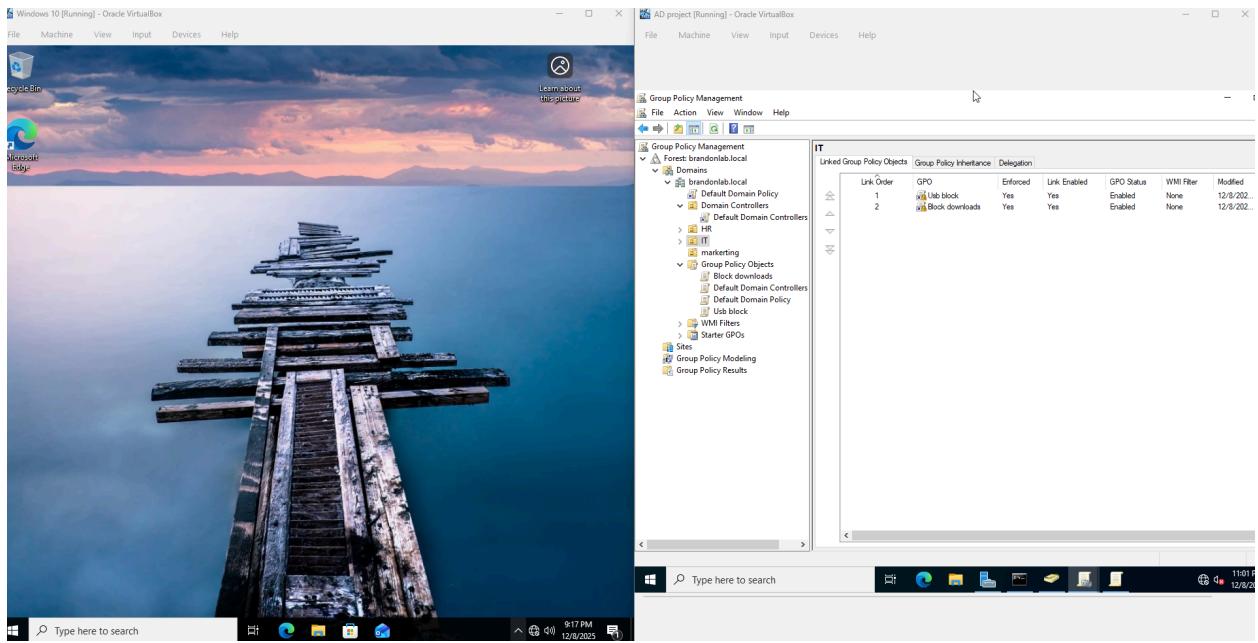
Administrative Templates → System → Removable Storage Access)



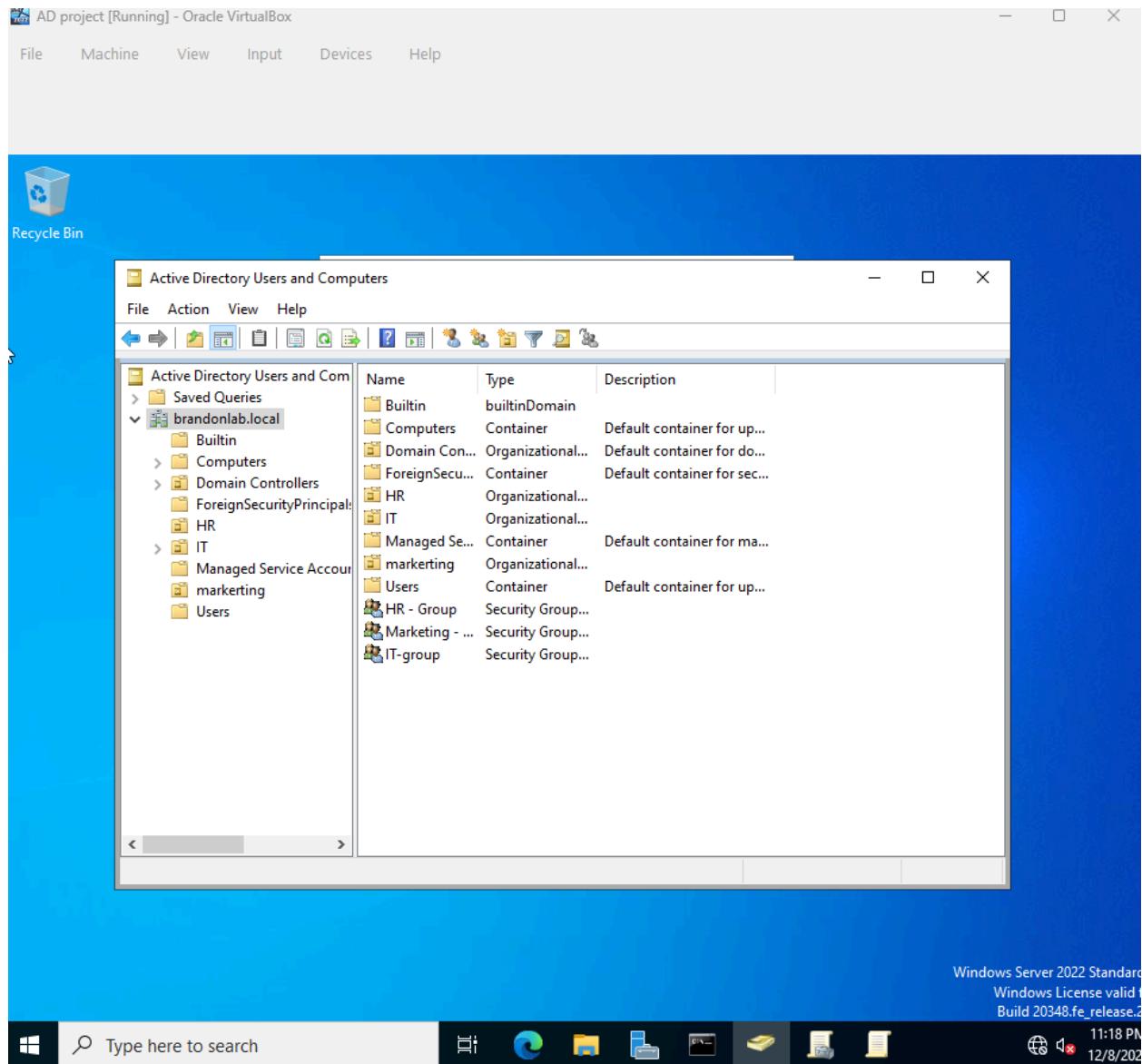
Linking the GPO and then enforcing it.



Repeated the process to block user downloads. (Computer Config → Policies → Administrative Templates → Windows Components → File Explorer → Do not allow file downloads)



Creating security groups for each OU. (ADUC → brandonlocal.net → (OU Name) → New → Group)



This lab demonstrates basic Active Directory administration skills including user management, OU design, Group Policy creation, and security hardening. These are the same tasks performed by Tier 1 Help desk techs.