Securing Windows Server (Network Infrastructure Security)

Vatsal Patel

8980484

INFO8046

Wareez Bashorun

July 30, 2024

Table of Contents

Lab 1 - Securing Windows Server (Network Infrastructure Security) Lab

Description

In this Securing Windows Server (Network Infrastructure Security) Lab, you will configure and secure the Windows Server environment practically. In this lab, you will learn how to secure a limited domain join account; revoke the domain join permissions in authenticated users, configure Active Directory attributes and service user accounts. Also, you will specify complex account policies including password requirements and account lockouts to enhance security. As a result of completing such procedures, you will gain practical knowledge and practical skills on methodologies in handling and protecting Windows Server infrastructure that will assist them in enhancing Network Security.

Observations

In this lab specifically, the description of creating a domain join account was strictly followed to strengthen the protection of the Windows Server. Delete authenticated users from the group policy and use the ms-DS-MachineAccountQuota attribute with zero value to block domain joins not authorized. Separation of duties through the creation of a universal service user account and its inclusion in a controlled group allowed the domain join process to be performed only by qualified people on the company's team. In addition to this, the delegation of domain joins permissions to the service account also strengthened the above security aspect. The account policies that were configured included setting strict passwords and were effective in enhancing the domain security. This test proved that these configurations were effective by confirming the successful implementation of the additional layers of protection with the use of standard and domain joiner accounts.

Screenshots

Exercise 1:

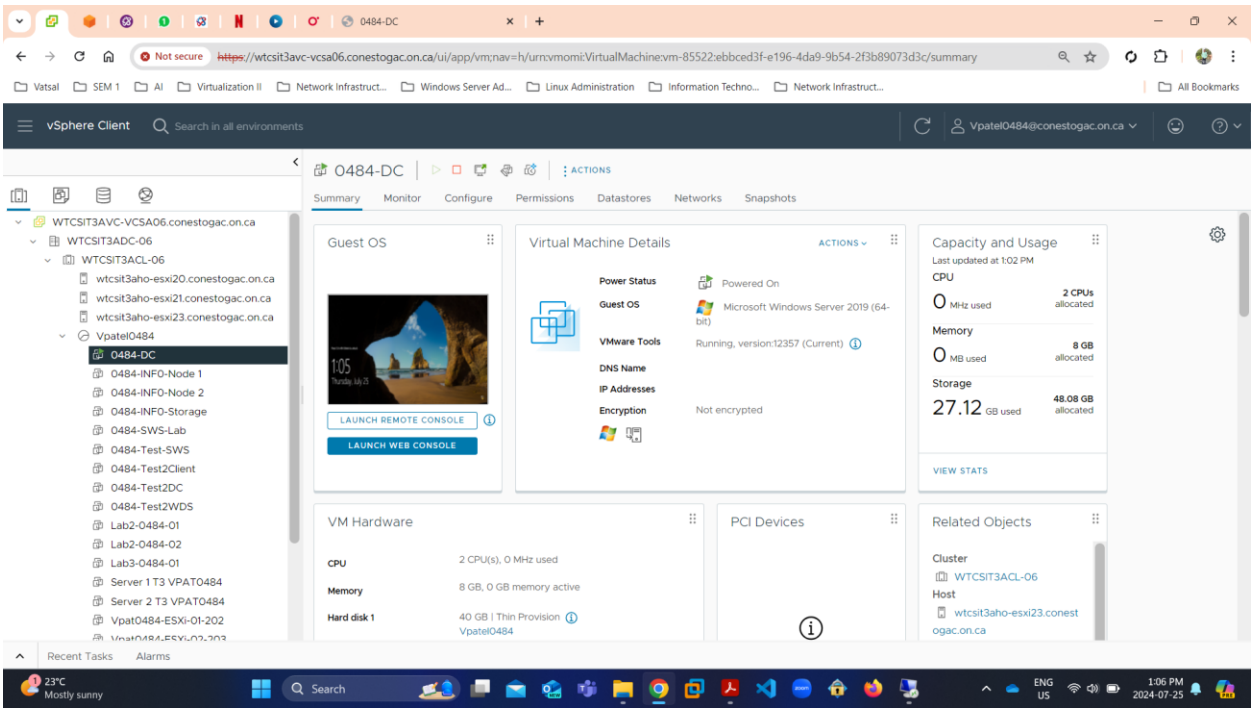

Fig 1: Picture shows that I am using 0484-DC virtual machine for this lab which is main DC.

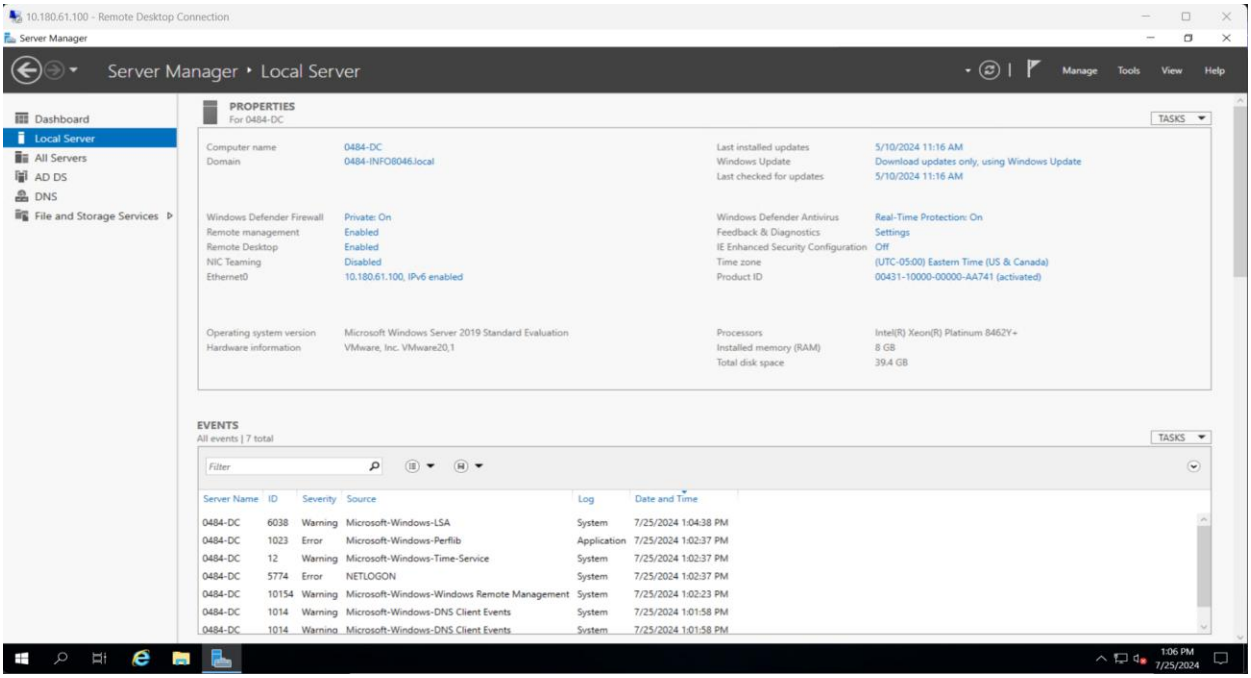

Fig 2: Picture shows we successfully adding the roles and features for the 0484-DC VM.

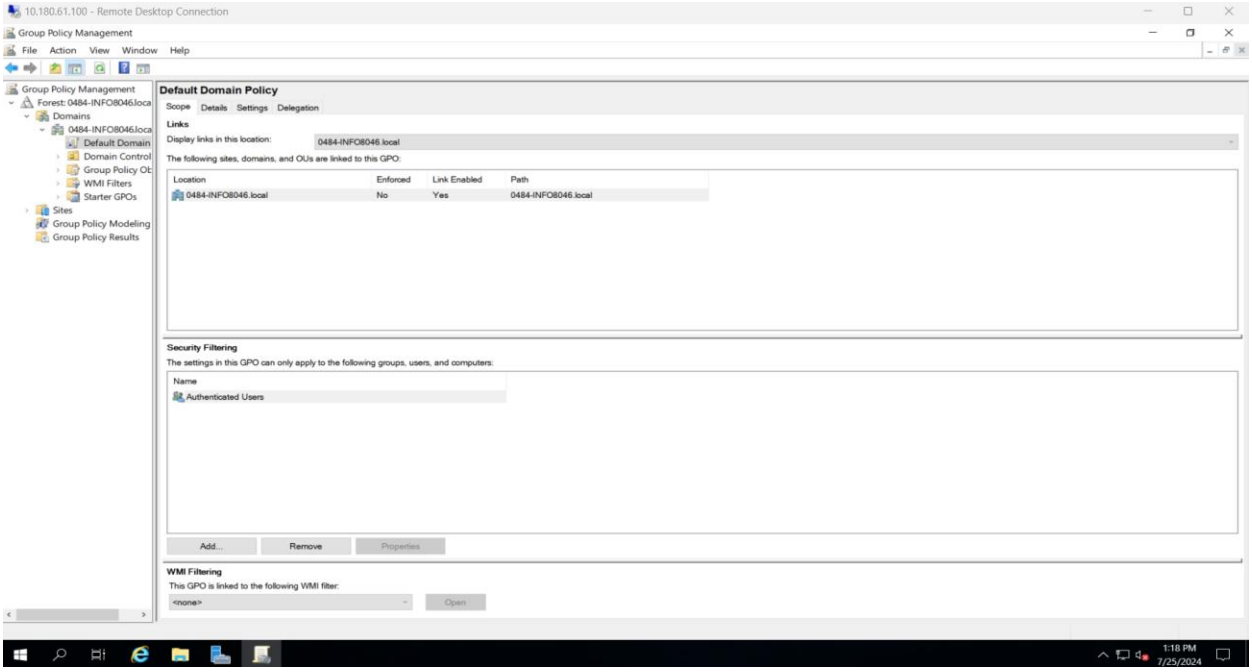

Fig 3: Picture shows open the panel of Group Policy Management Default Domain Policy.

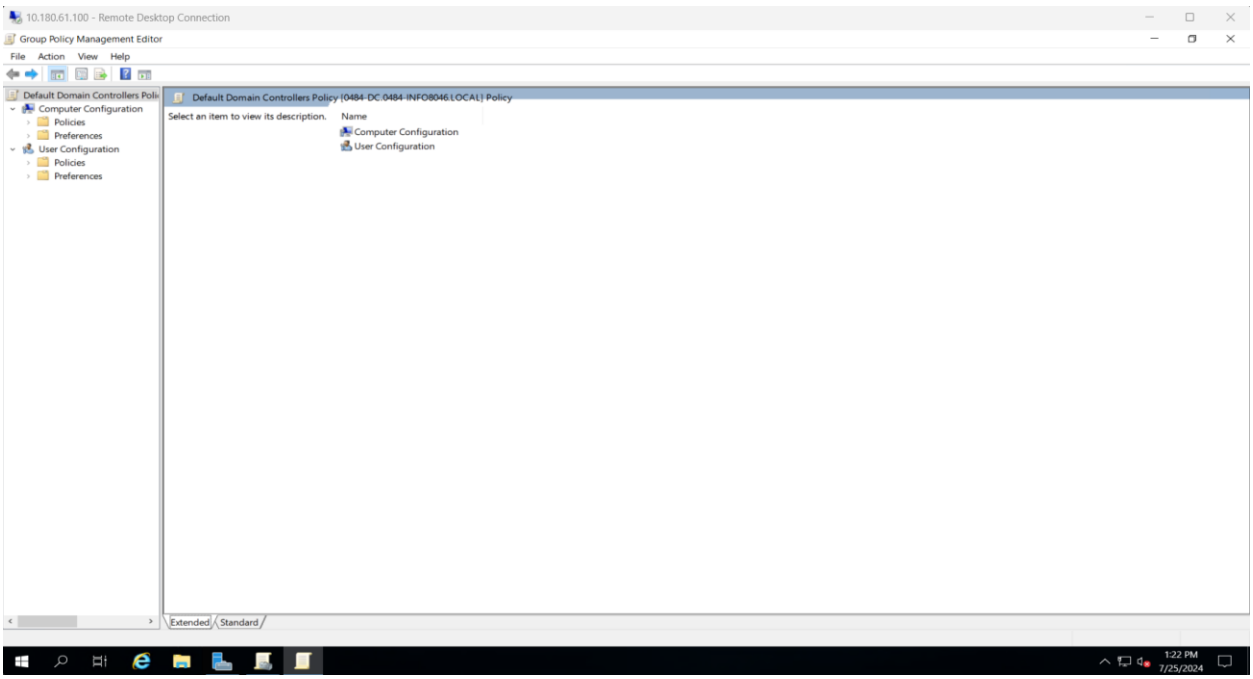

Fig 4: Picture shows navigating the Default Domain Policy tab in 0484-DC VM.

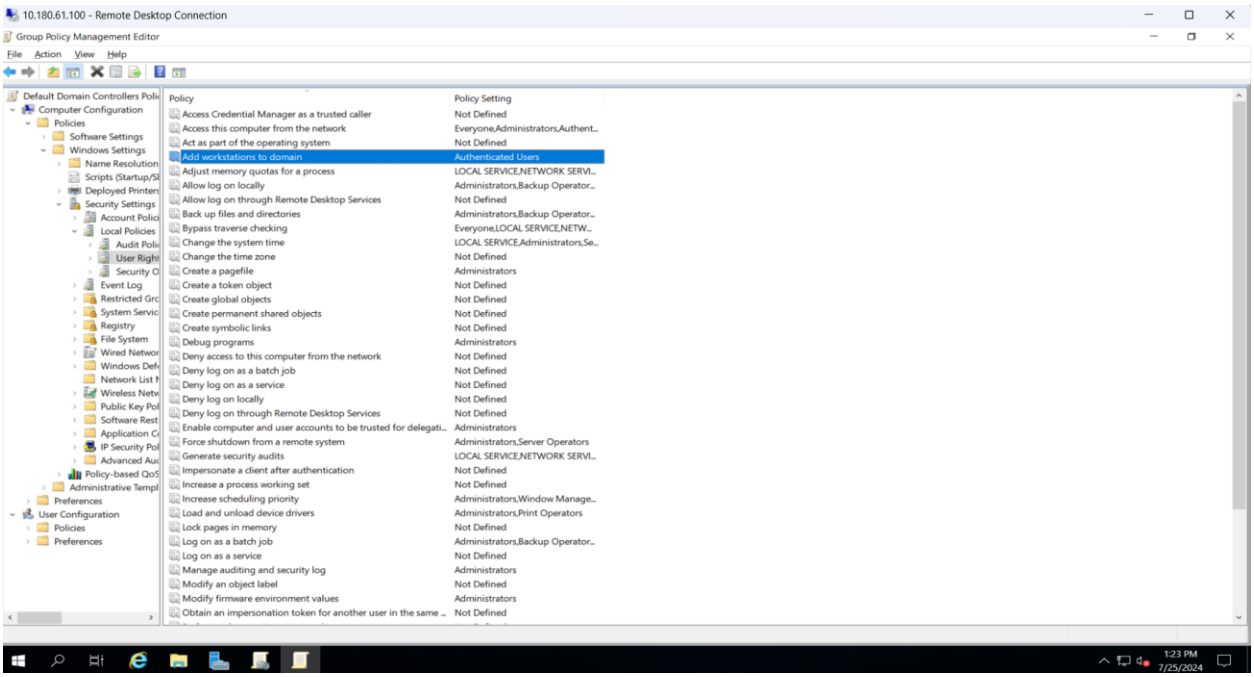

Fig 5: Picture shows modifying the User Rights Assignment of the 0484-DC VM.

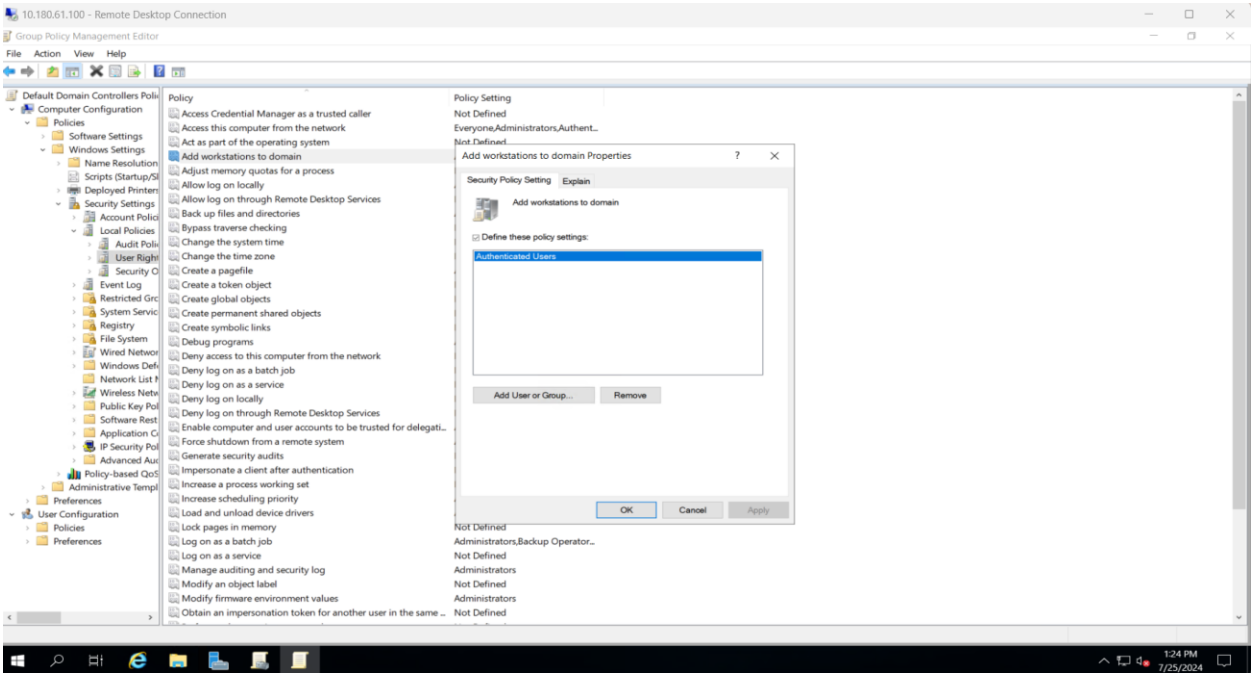

Fig 6: Picture shows Authenticated Users in the Domain properties tab, and we must remove them from the list.

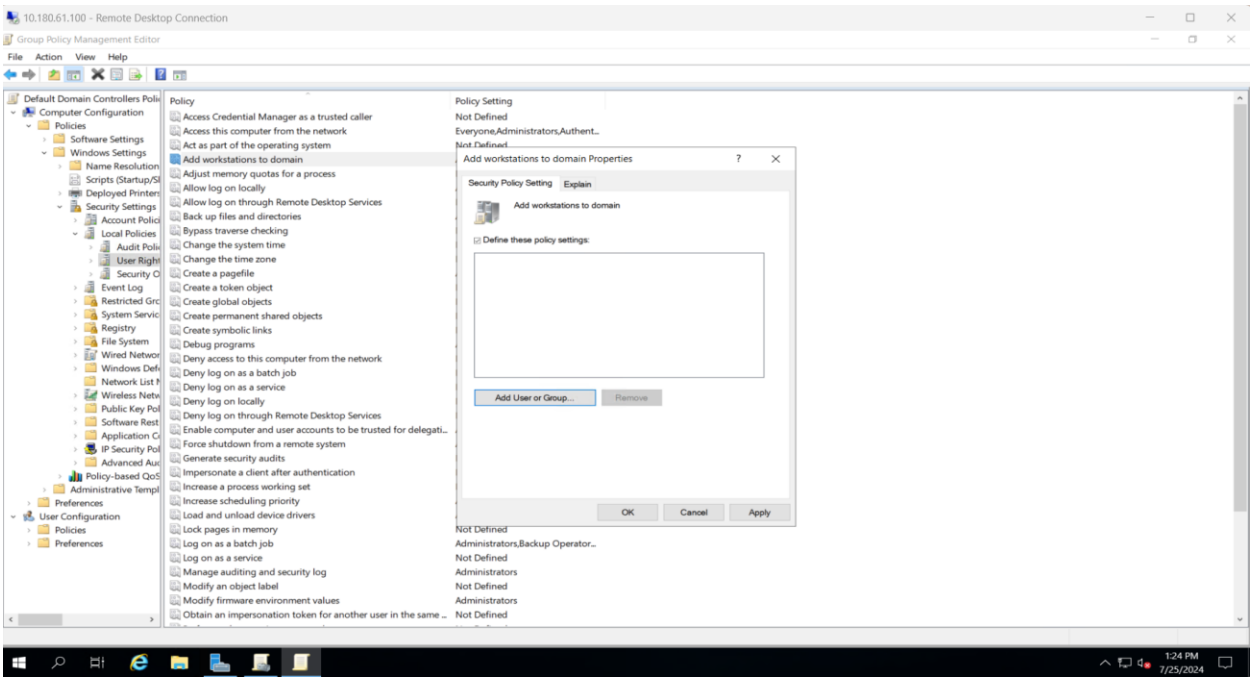

Fig 7: Picture shows successfully remove the Authenticated Users from the lists.

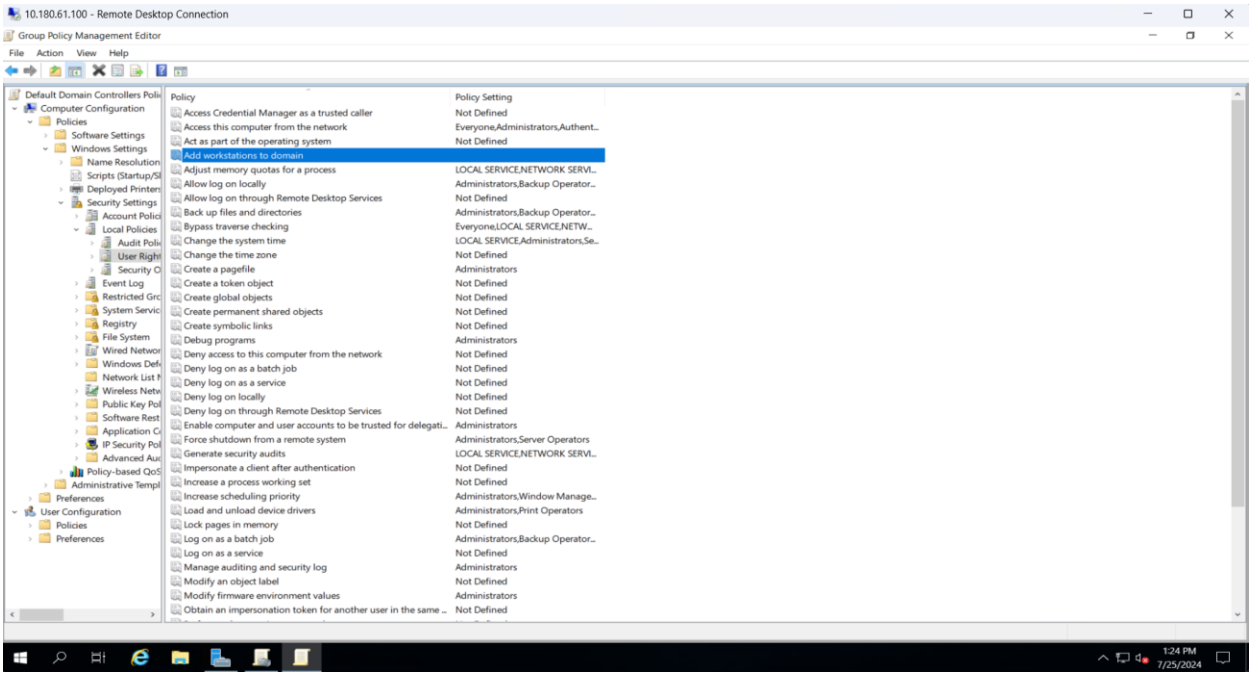

Fig 8: Picture shows after removing the Authentication Users from the lists the policy setting panel is empty.

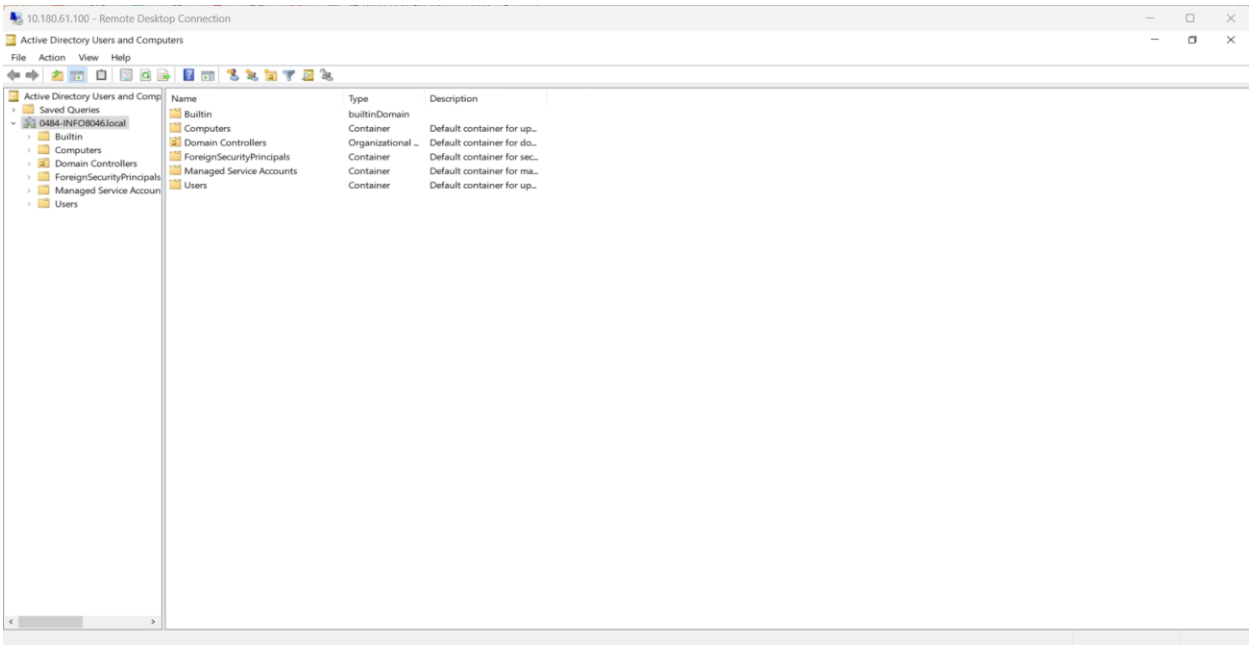

Fig 9: Picture shows open the Active Directory Users and Computers in the main DC.

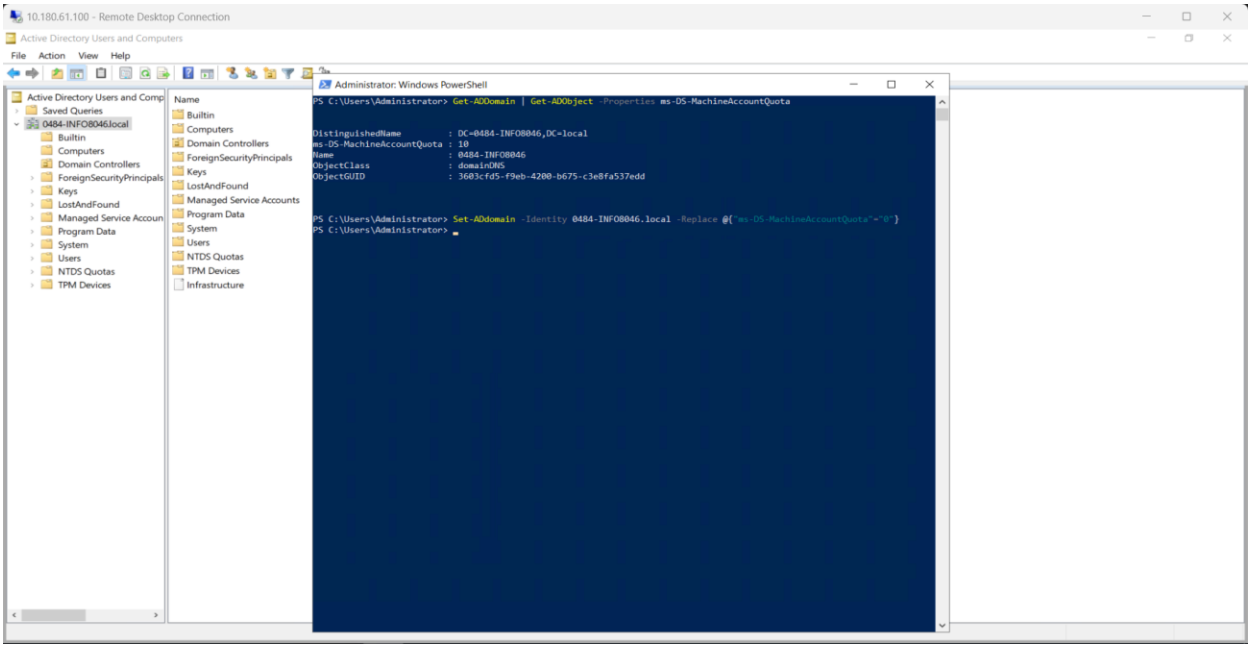

Fig 10: Picture shows set the value of an AD attribute to 0 using PowerShell.

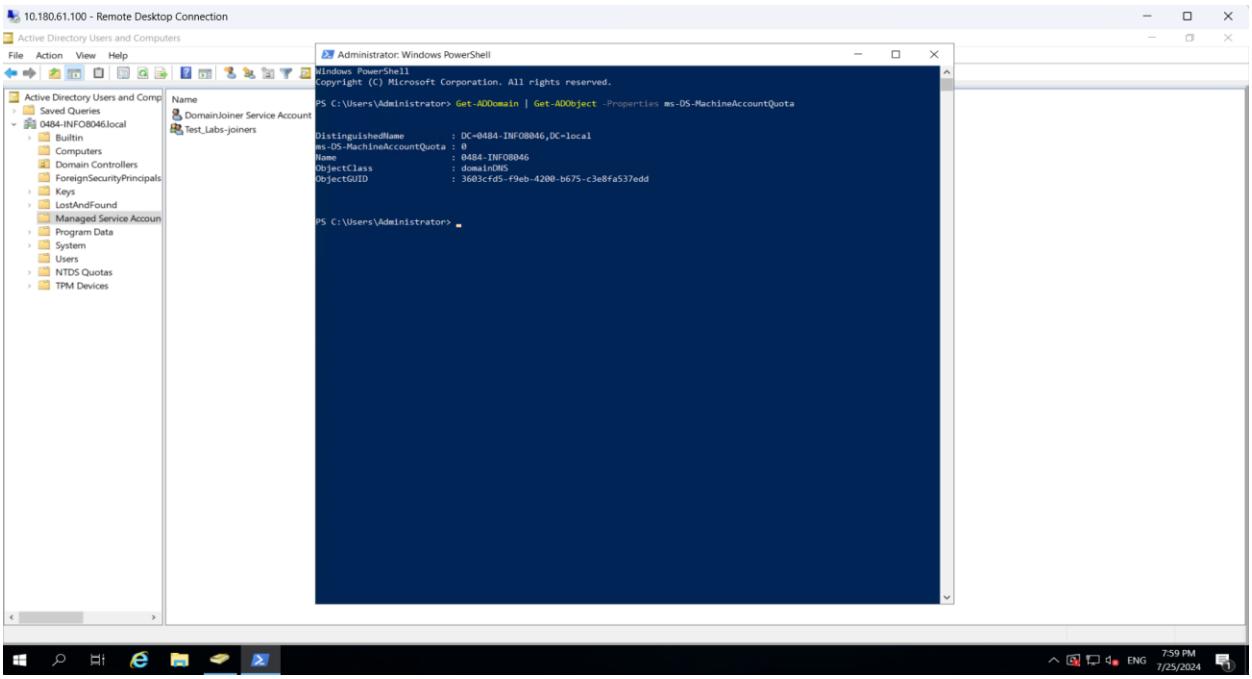

Fig 11: Picture shows set the value of an AD attribute to 0 using PowerShell is successful.

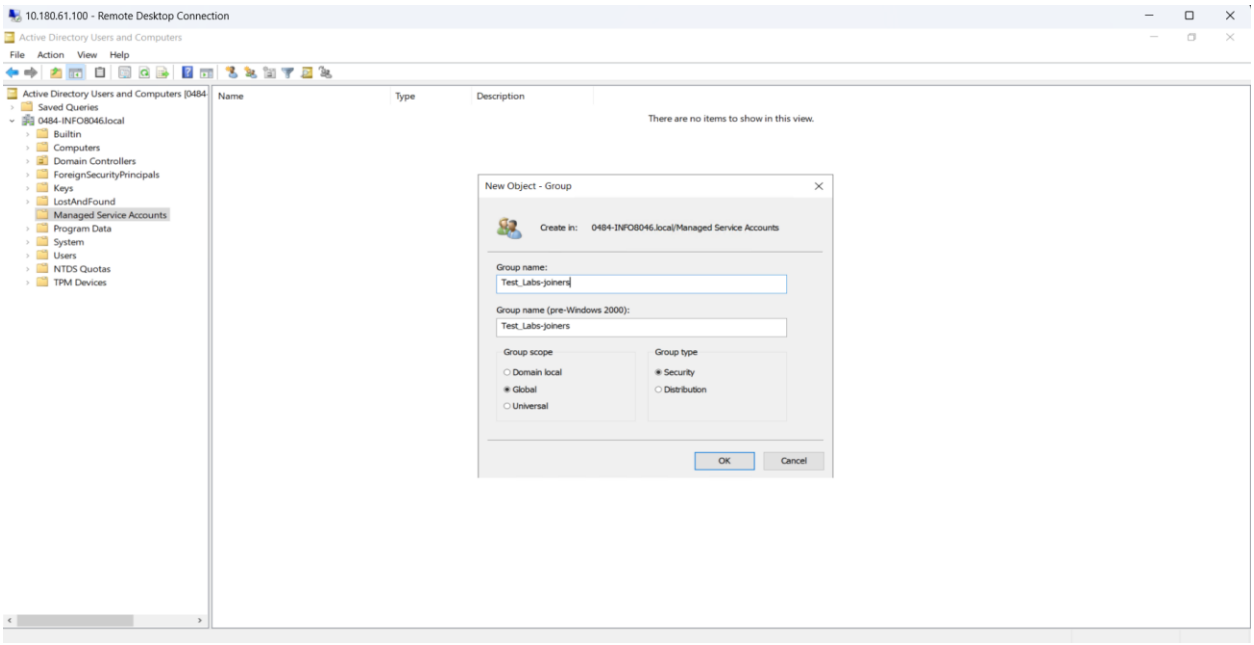

Fig 12: Picture shows creating a Security Group Test_Labs-joiners in the Service Accounts OU.

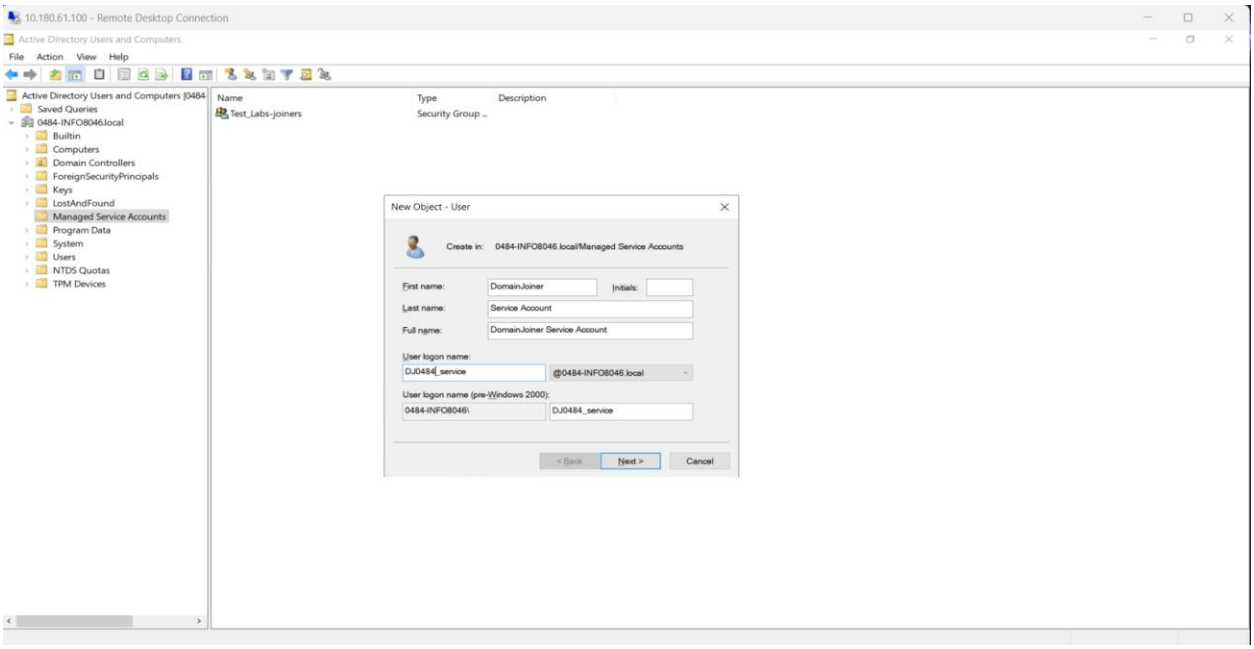

Fig 13: Picture shows creating a User DomainJoiner in the Service Accounts OU.

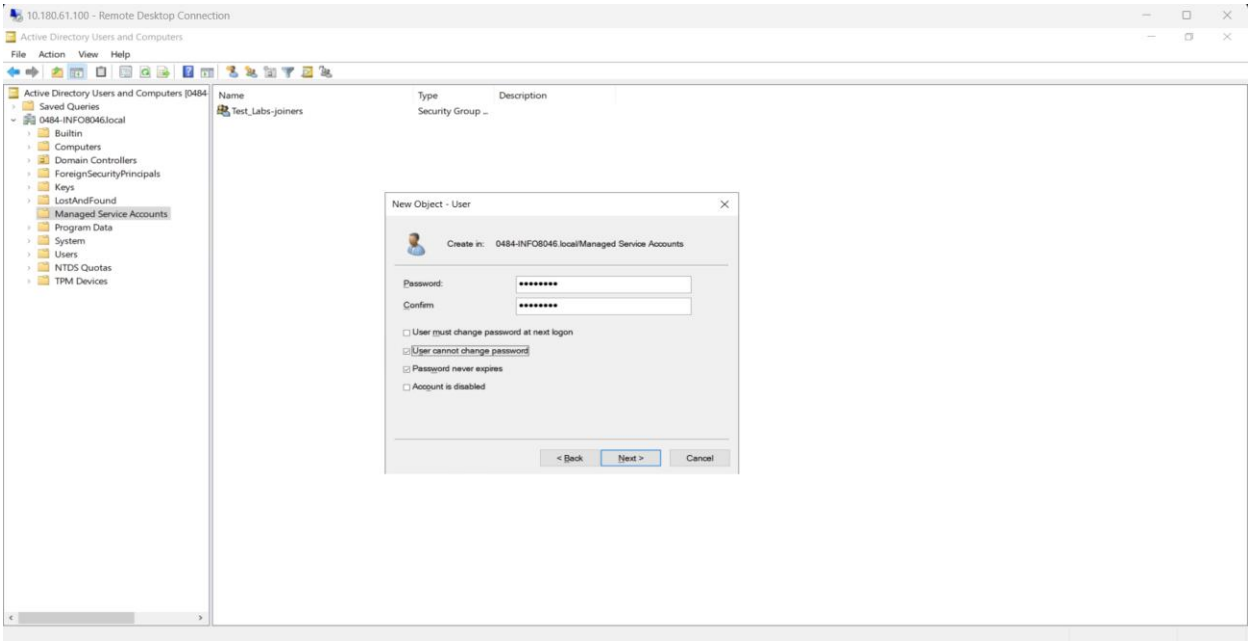

Fig 14: Picture shows giving the password of the DomainJoiner User.

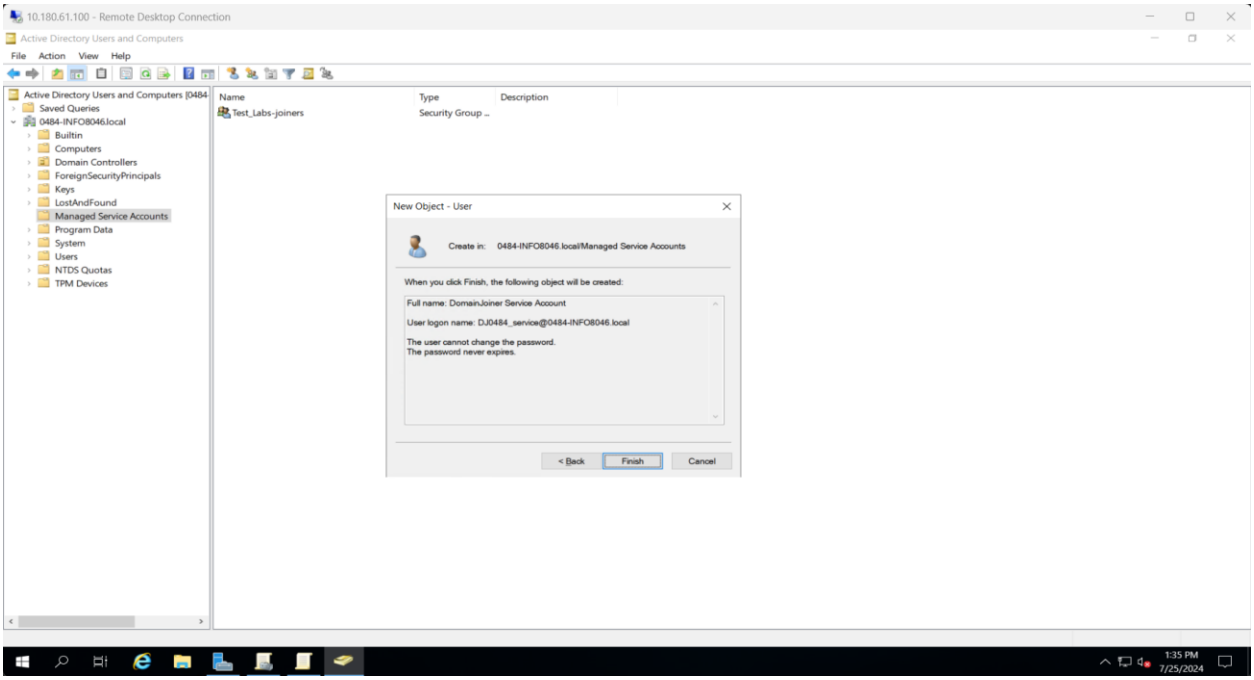

Fig 15: Picture shows User will successfully create in the Service Accounts OU.

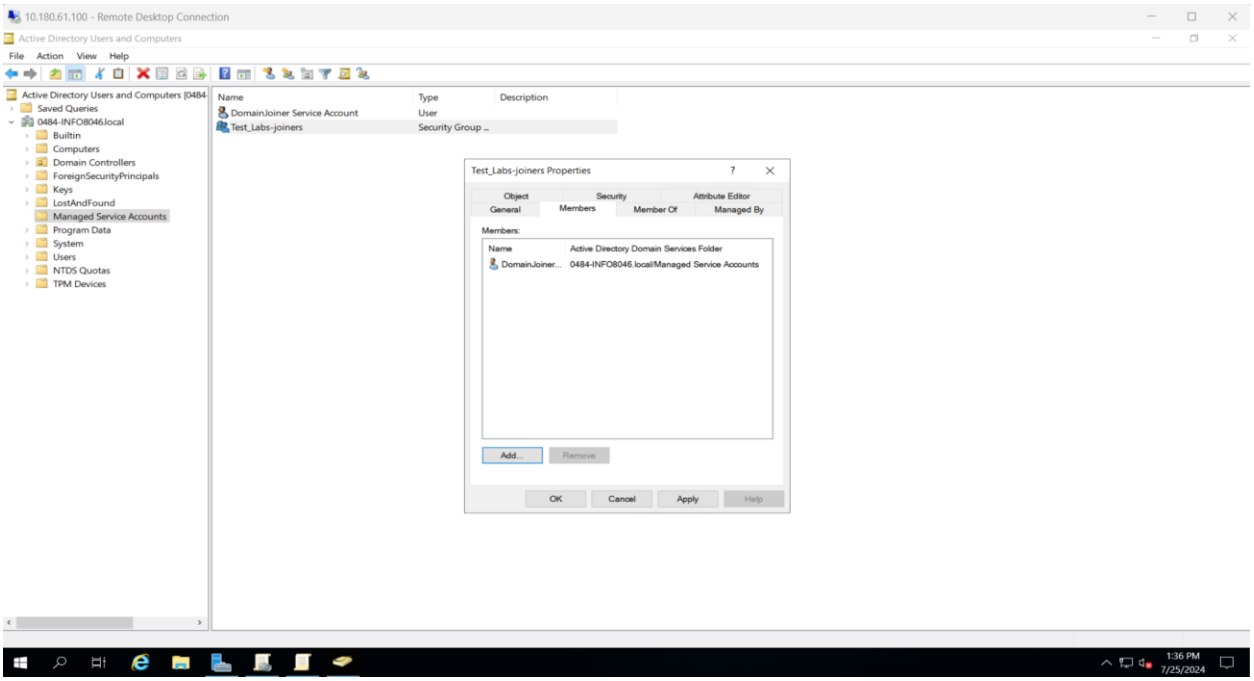

Fig 16: Picture shows adding the DomainJoiner User to the Test_Labs-joiner Group.

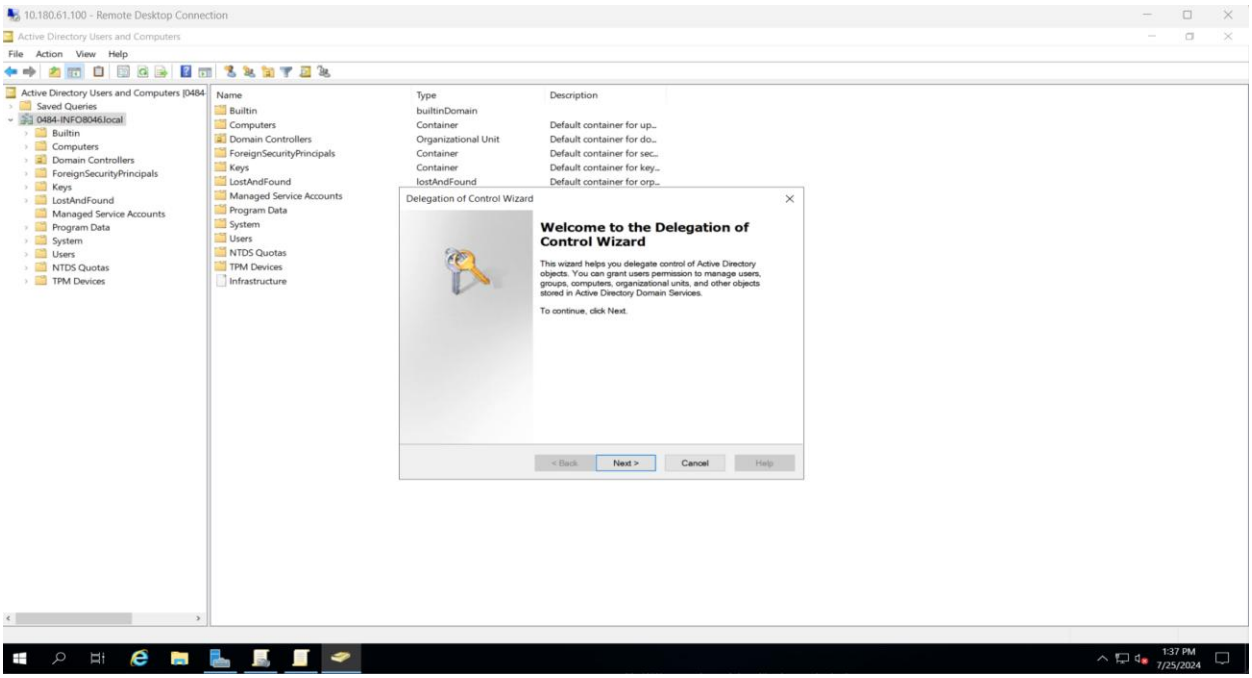

Fig 17: Picture shows the Delegation of control wizard in the Active Directory Users and Computers.

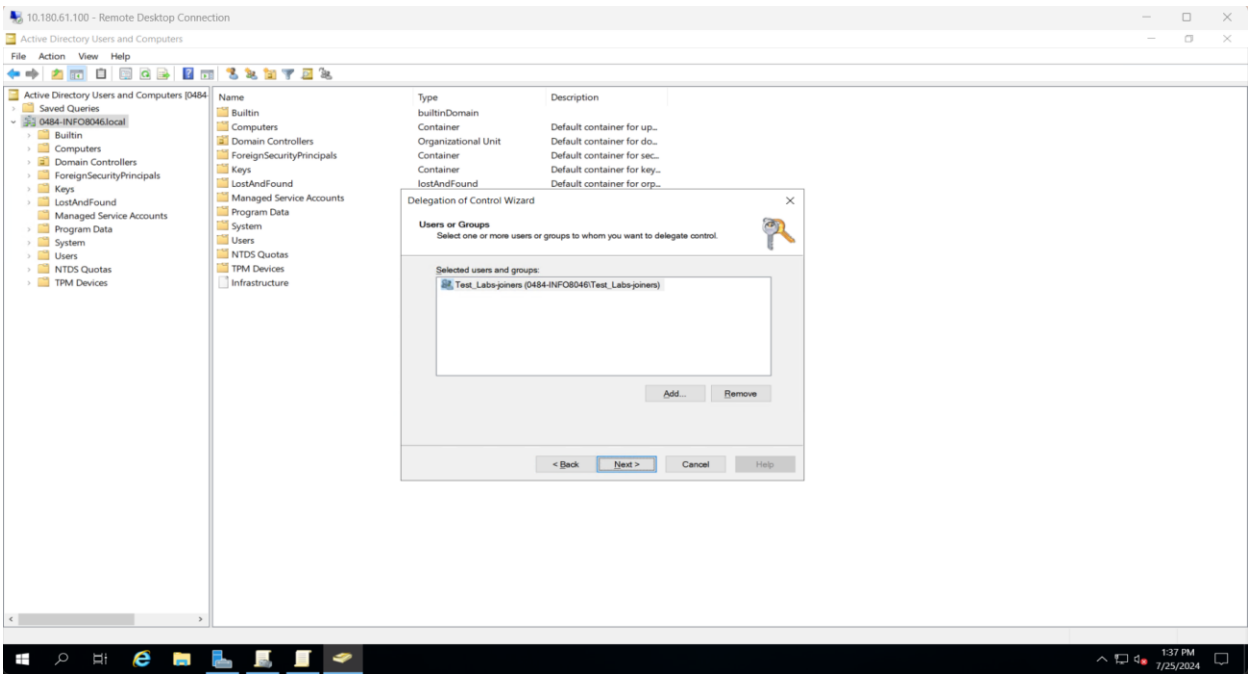

Fig 18: Picture shows successfully adding the Test_Labs-joiners group which has delegate control.

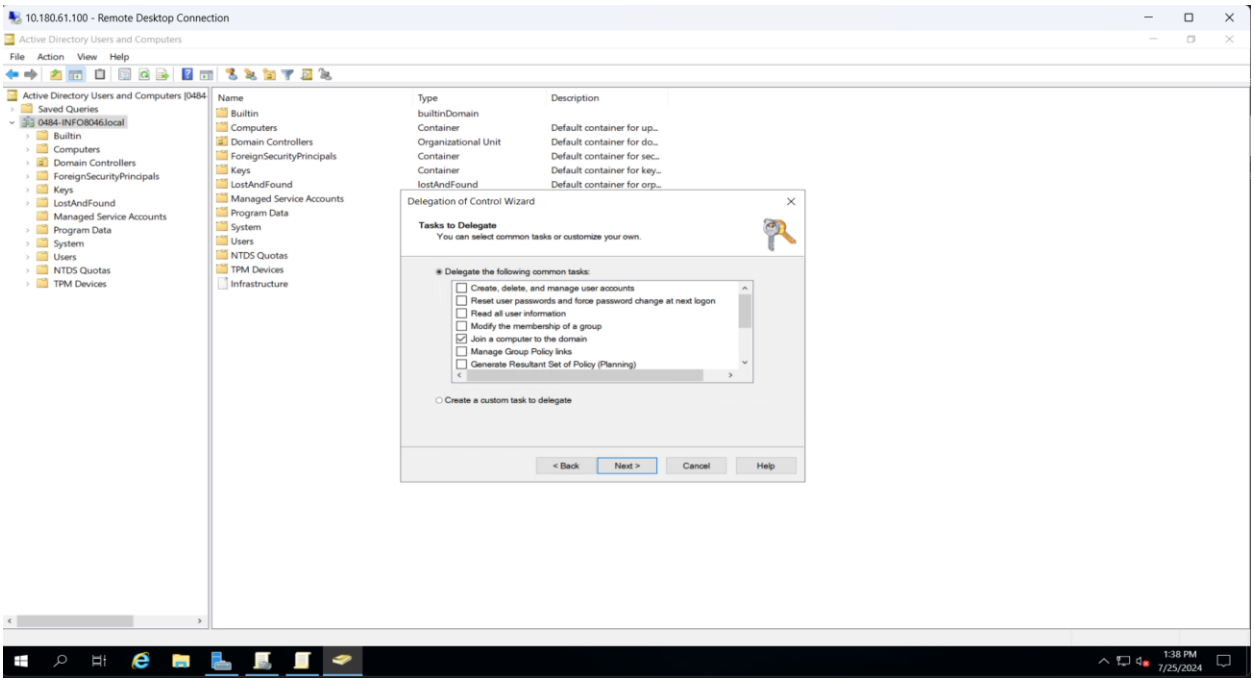

Fig 19: Picture shows selecting the Join a computer to the domain option in the tasks to delegate.

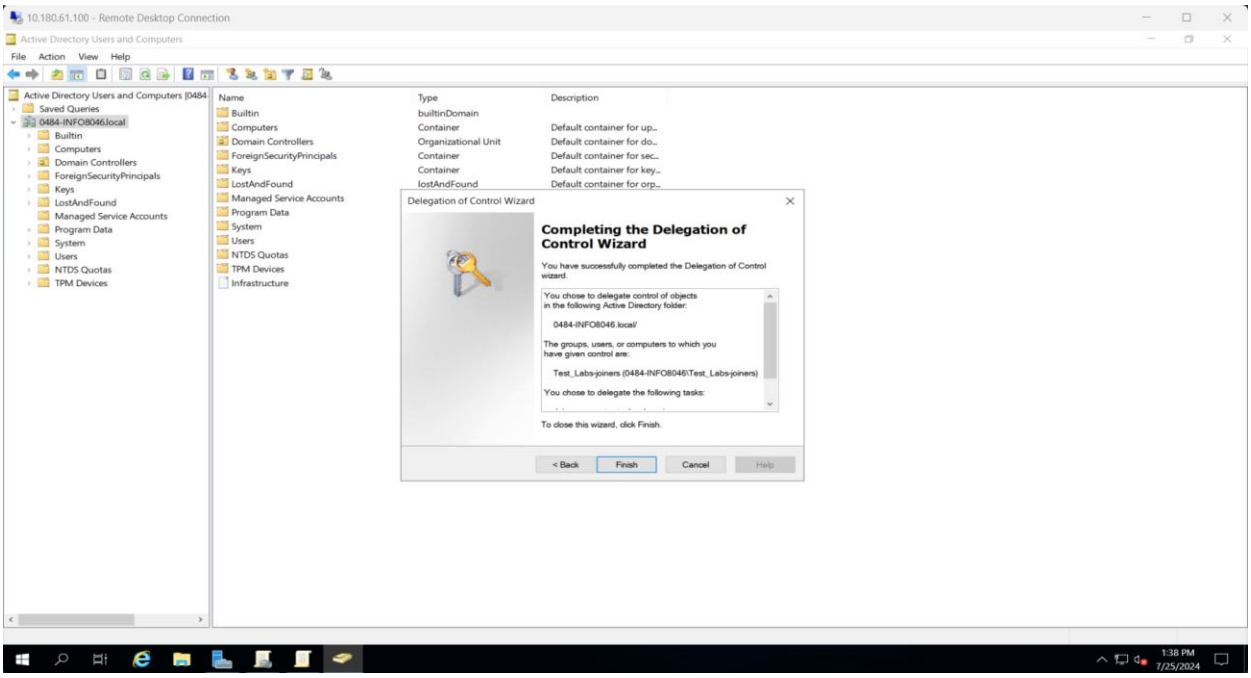

Fig 20: Picture shows successfully completing the Delegation of control wizard.

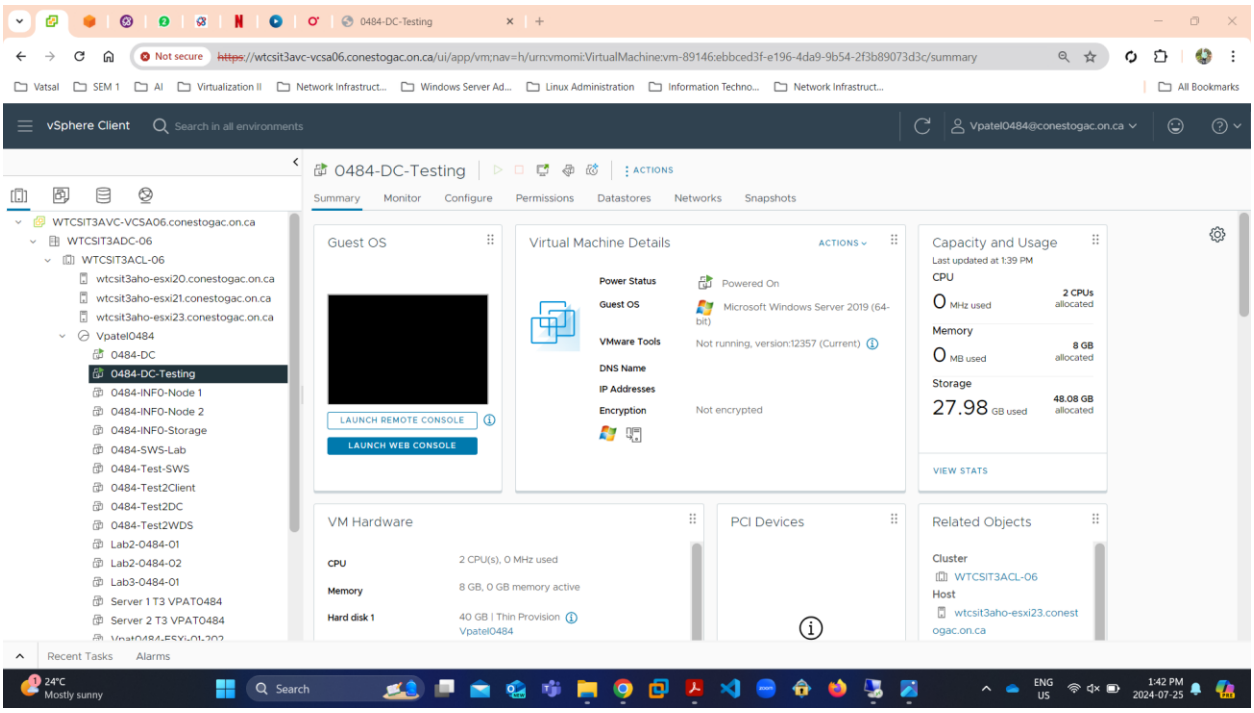

Fig 21: Picture shows We are creating the testing virtual machine which is 0484-DC-Testing.

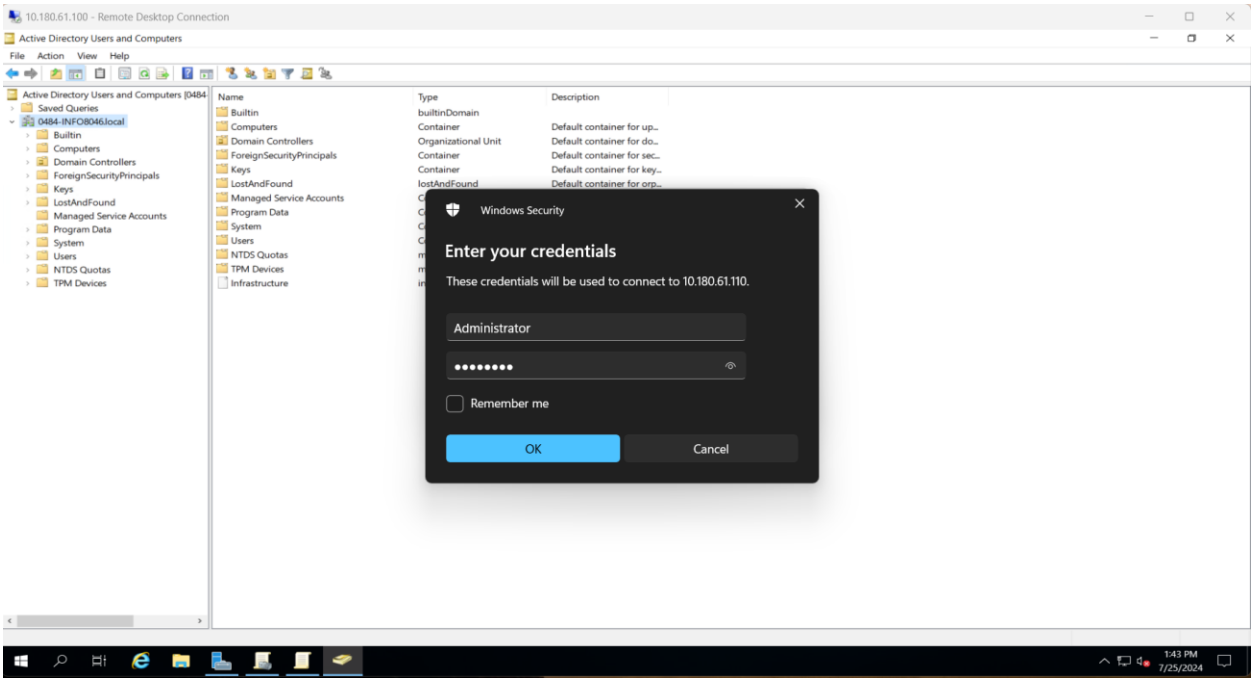

Fig 22: Picture shows normal login credential for the Testing Users.

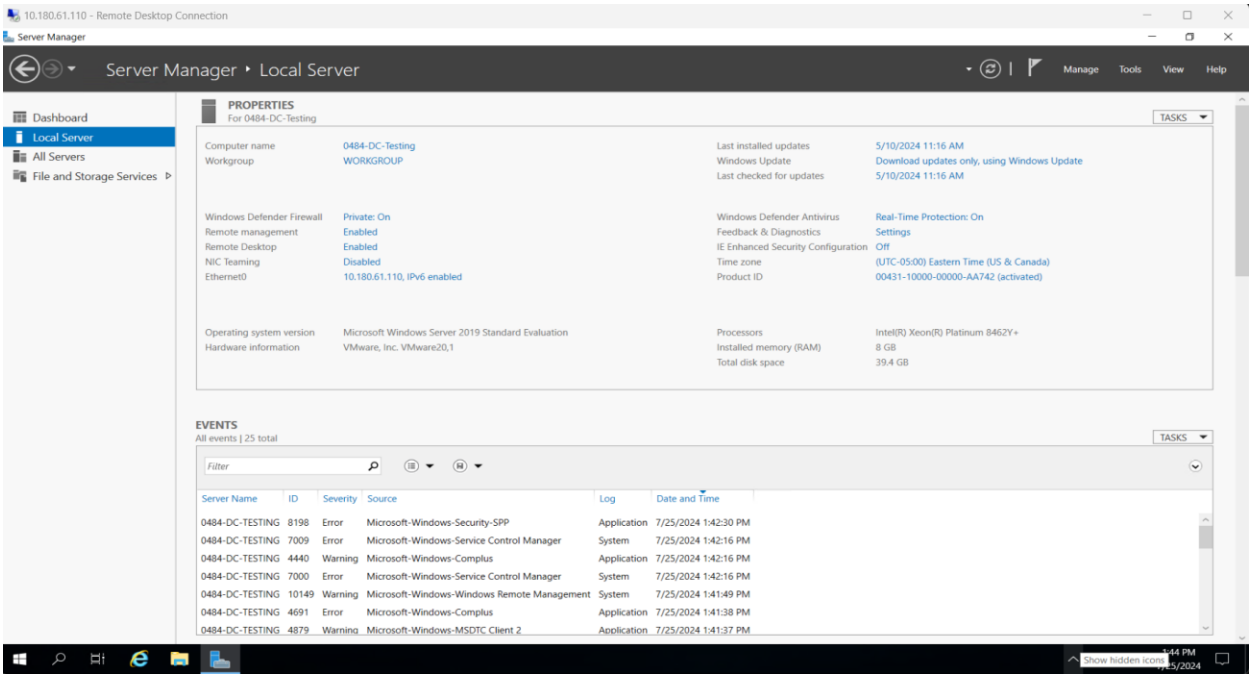

Fig 23: Picture shows successfully login into the VMs for normal Login.

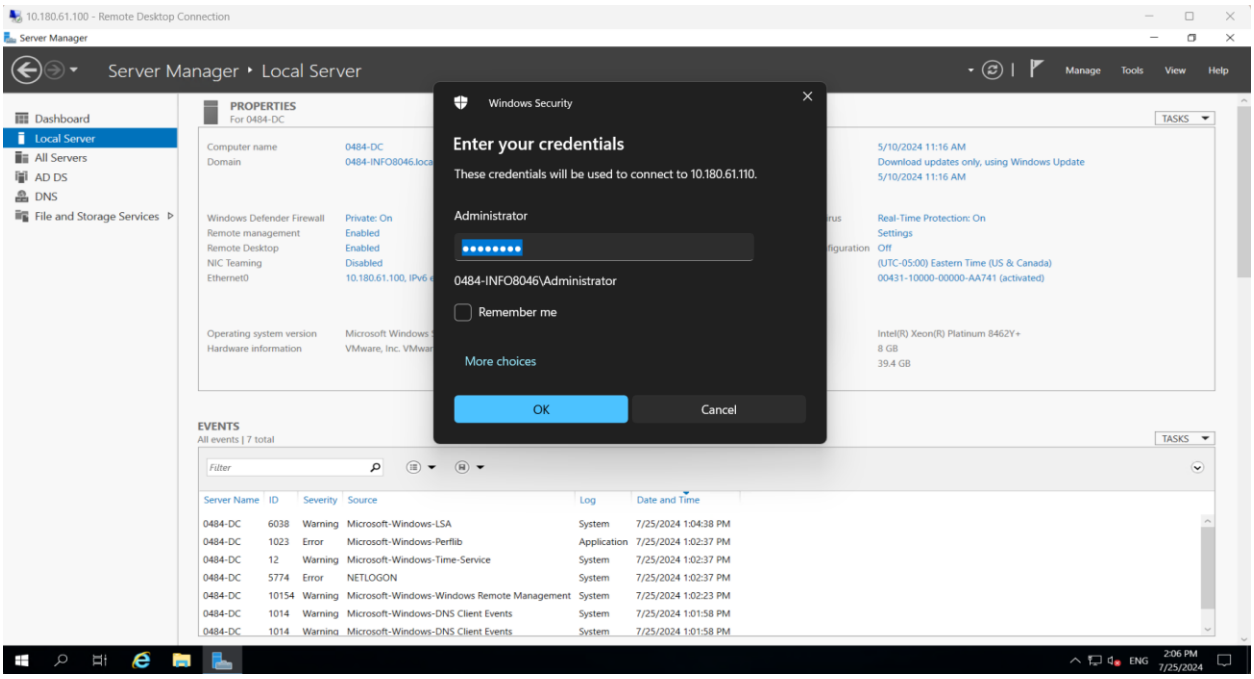

Fig 24: Picture shows Domain Login credential for the Testing virtual machine.

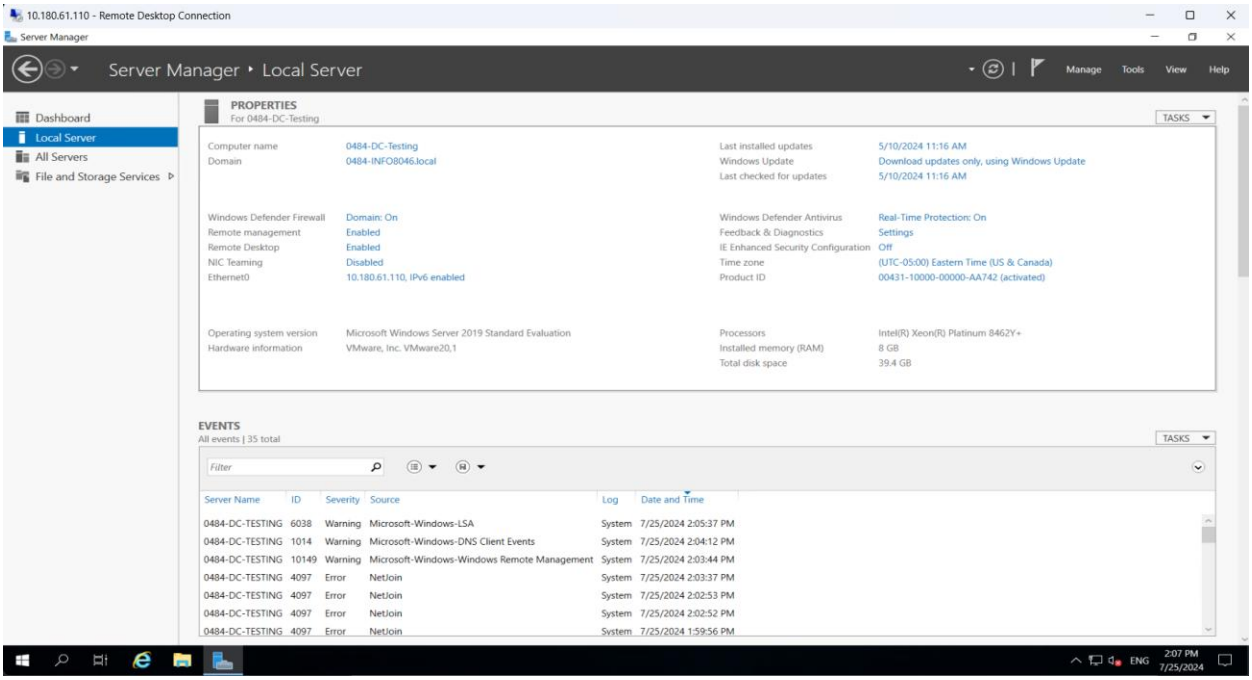

Fig 25: Picture shows successfully Login and Joining with the Main Domain Controller.

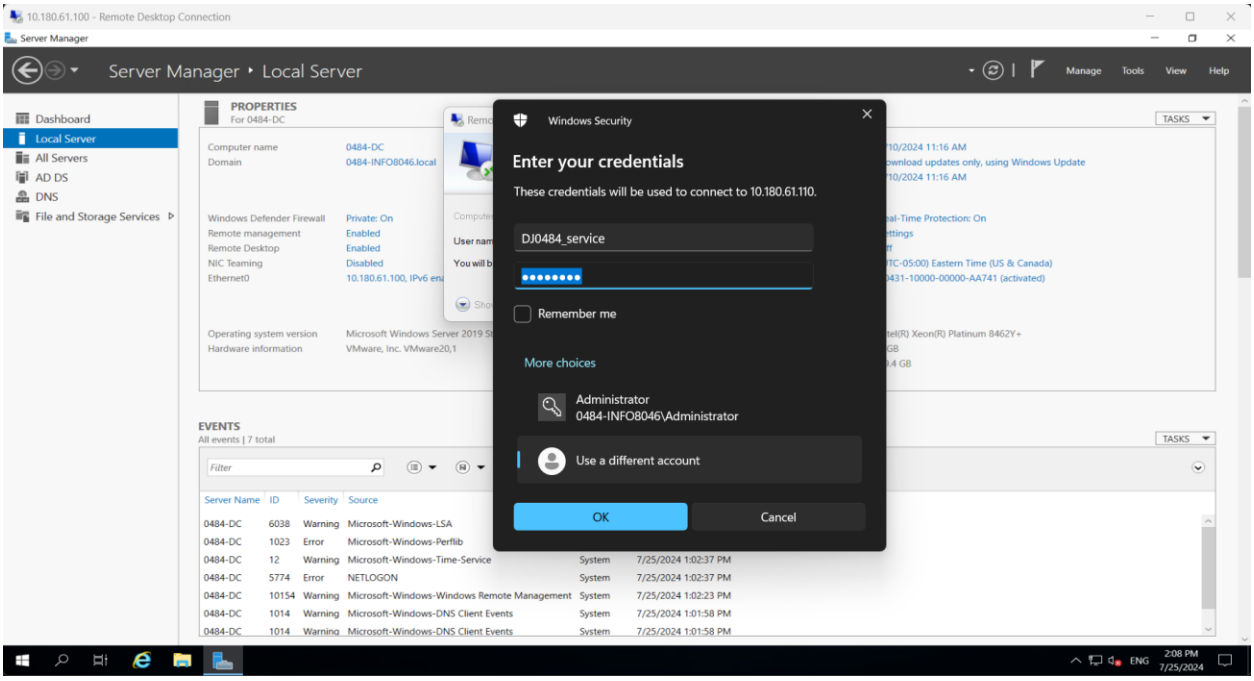

Fig 26: Picture shows DJ0484_service Login credential in the Remote desktop connection.

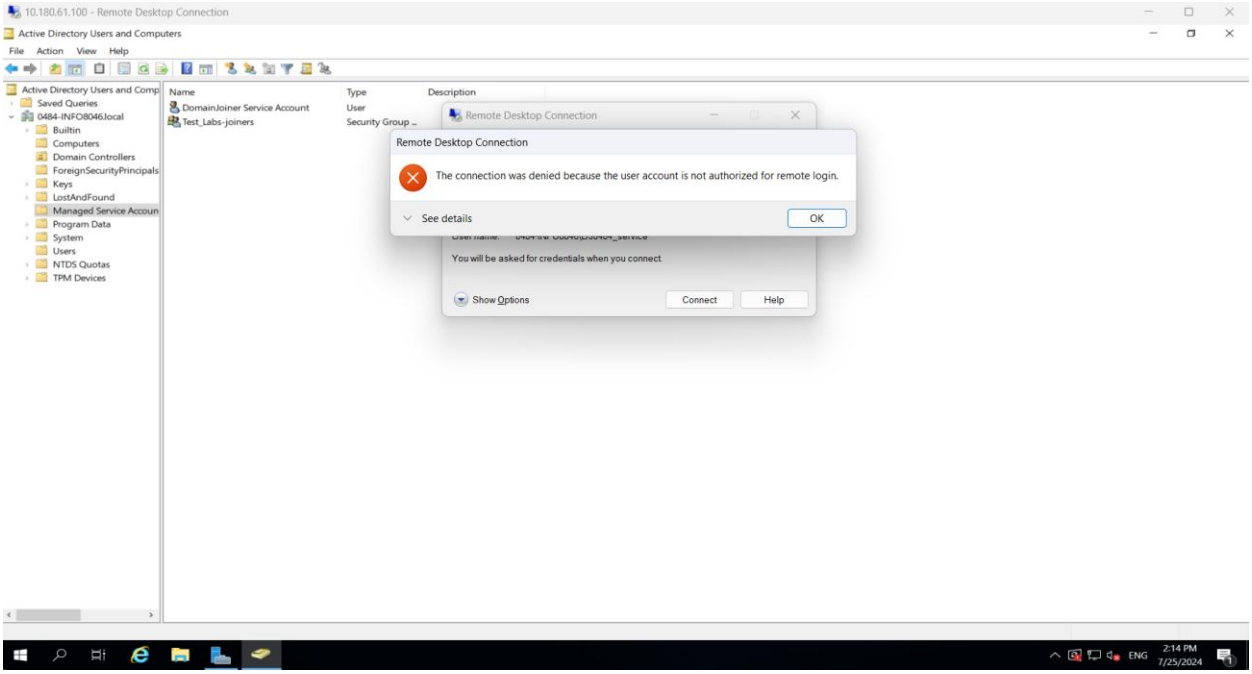

Fig 27: Picture shows the User cannot connect remotely because we are not giving permission for the Remotely Login.

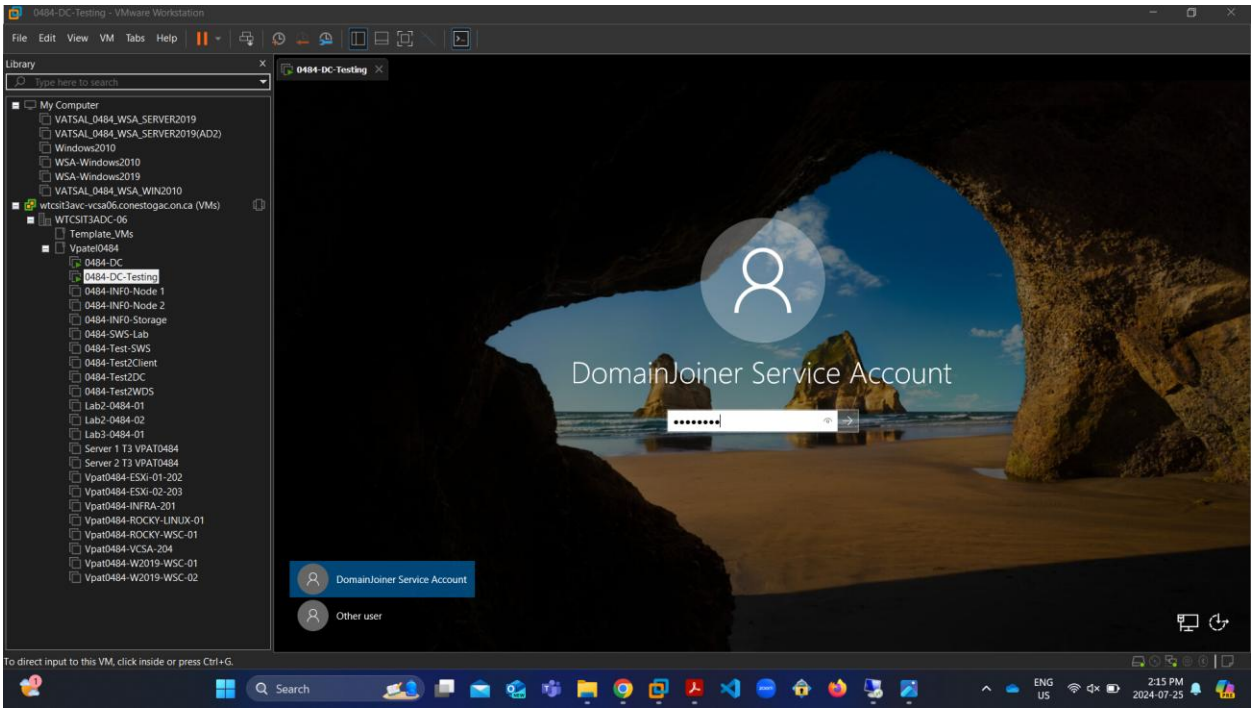

Fig 28: Picture shows Another Remote VMware Workstation that we are using for DomainJoiner Service Account Login User.

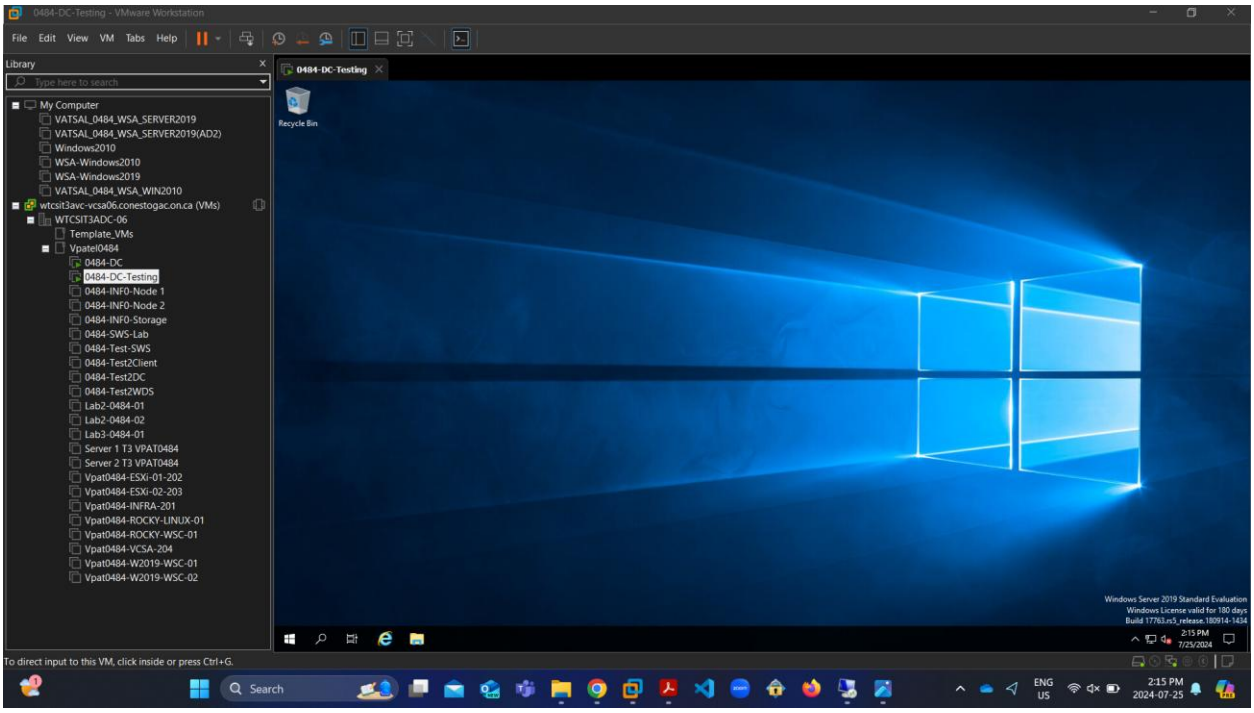

Fig 29: Picture shows successfully Login DomainJoiner Service Account User with the help of another remote desktop connection.

Exercise 2:

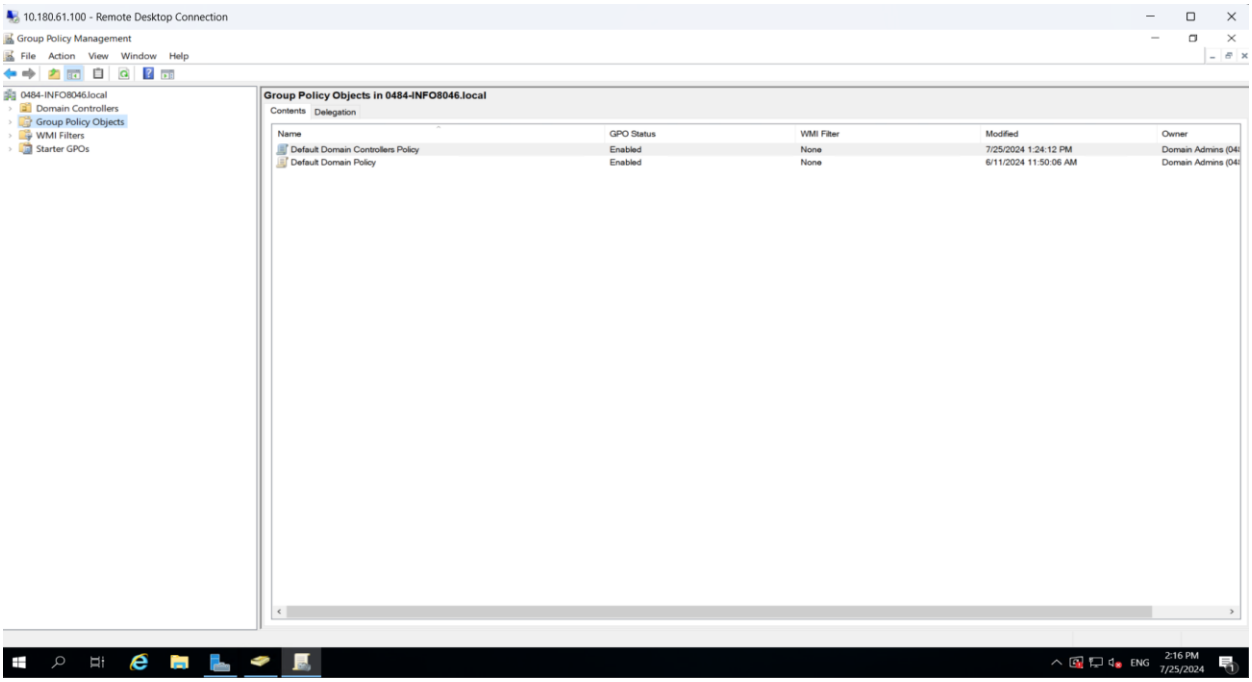

Fig 30: Picture shows opening the Group Policy Management for Exercise 2 into the main DC.

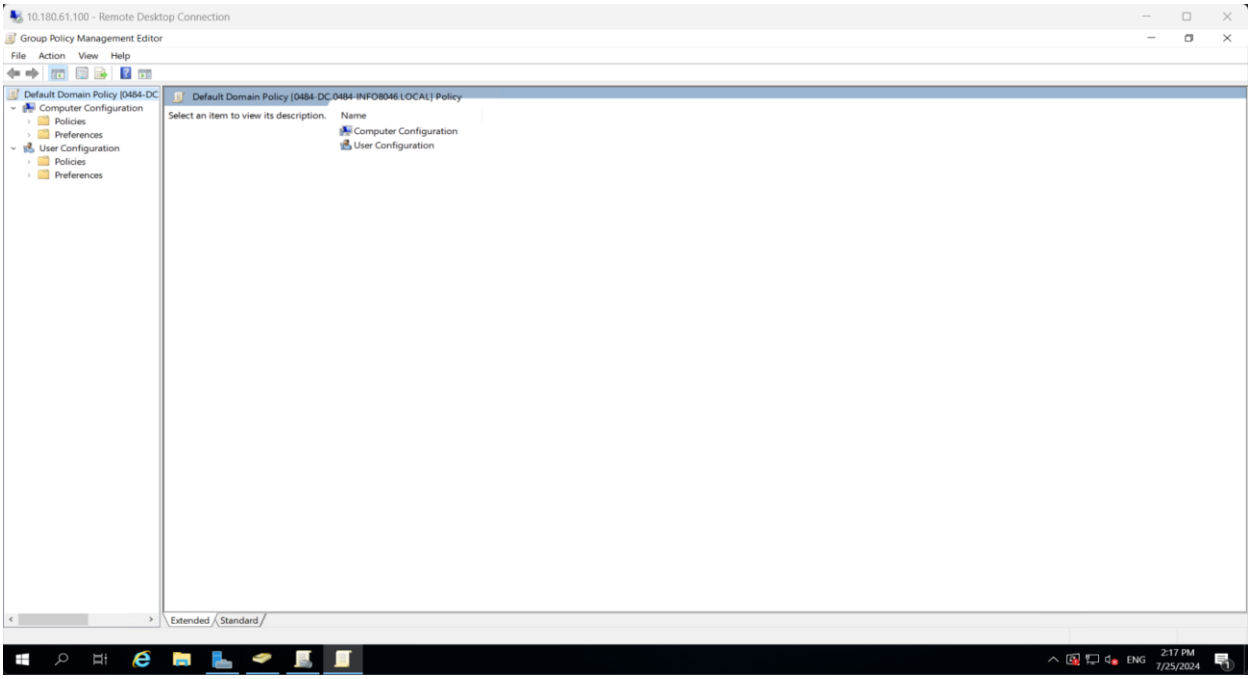

Fig 31: Picture shows navigating the Default Domain Policy into Group Policy Management.

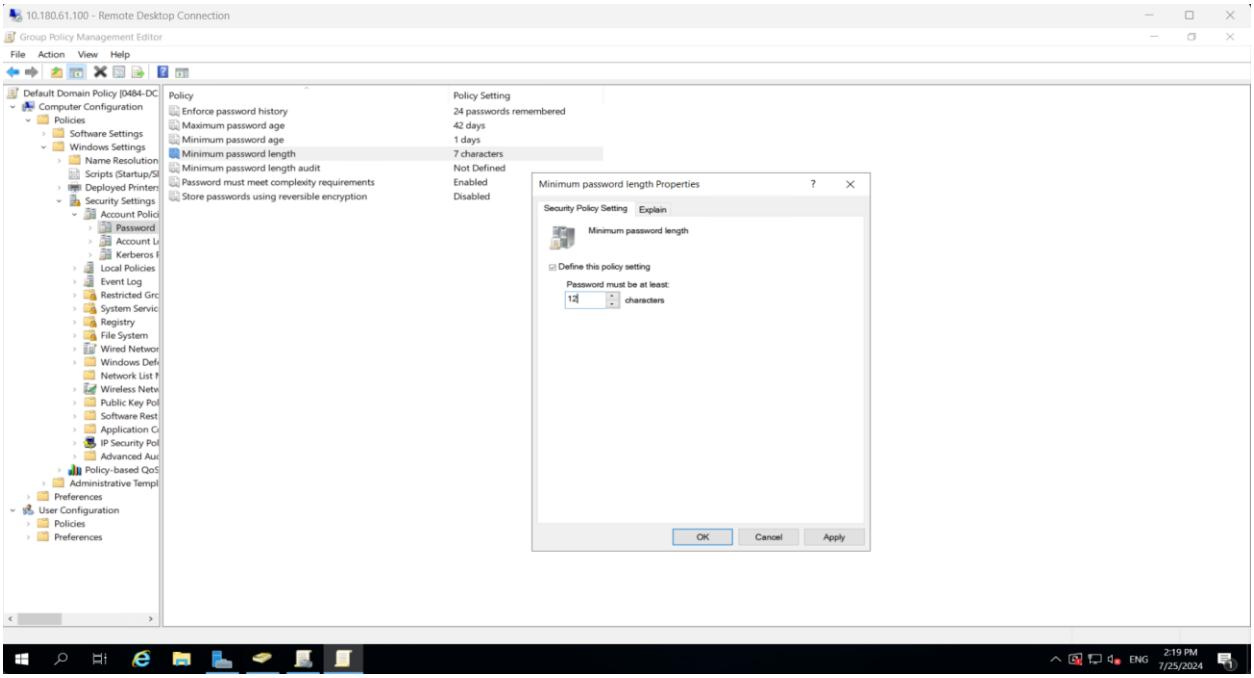

Fig 32: Picture shows Policy setting dialog box for the Minimum password length which we will set to 12 characters.

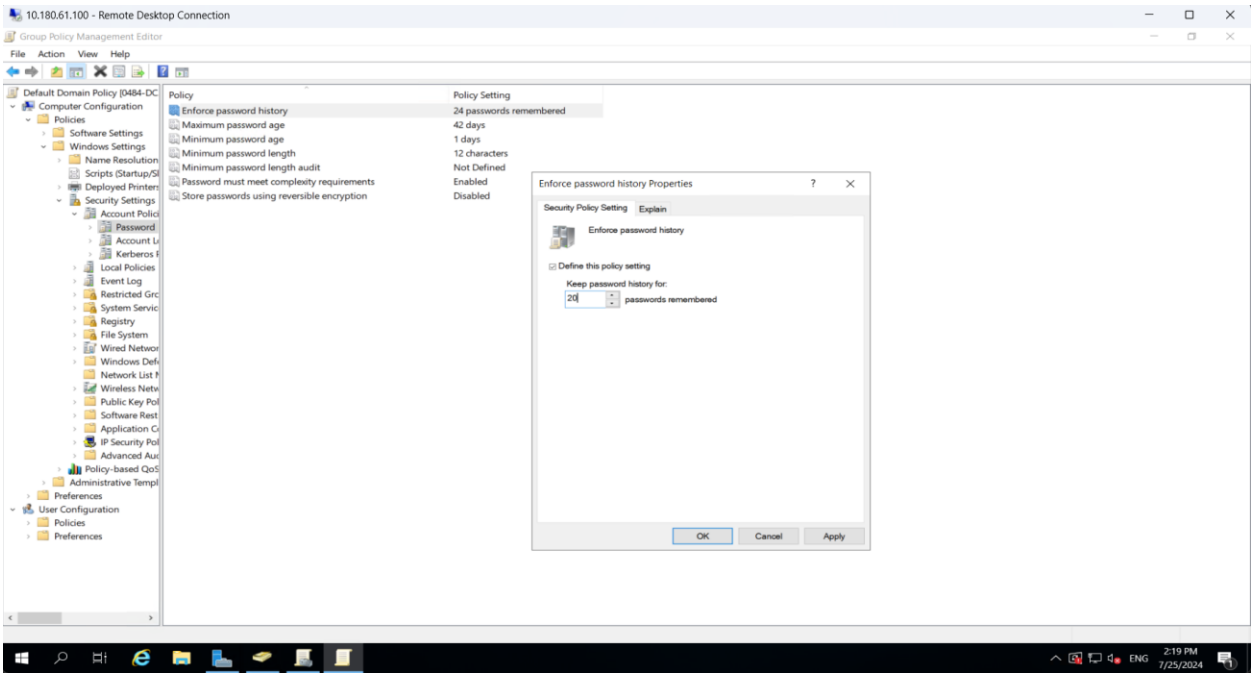

Fig 33: Picture shows Policy setting dialog box for the Enforce password history which we will set to 20 passwords remembered.

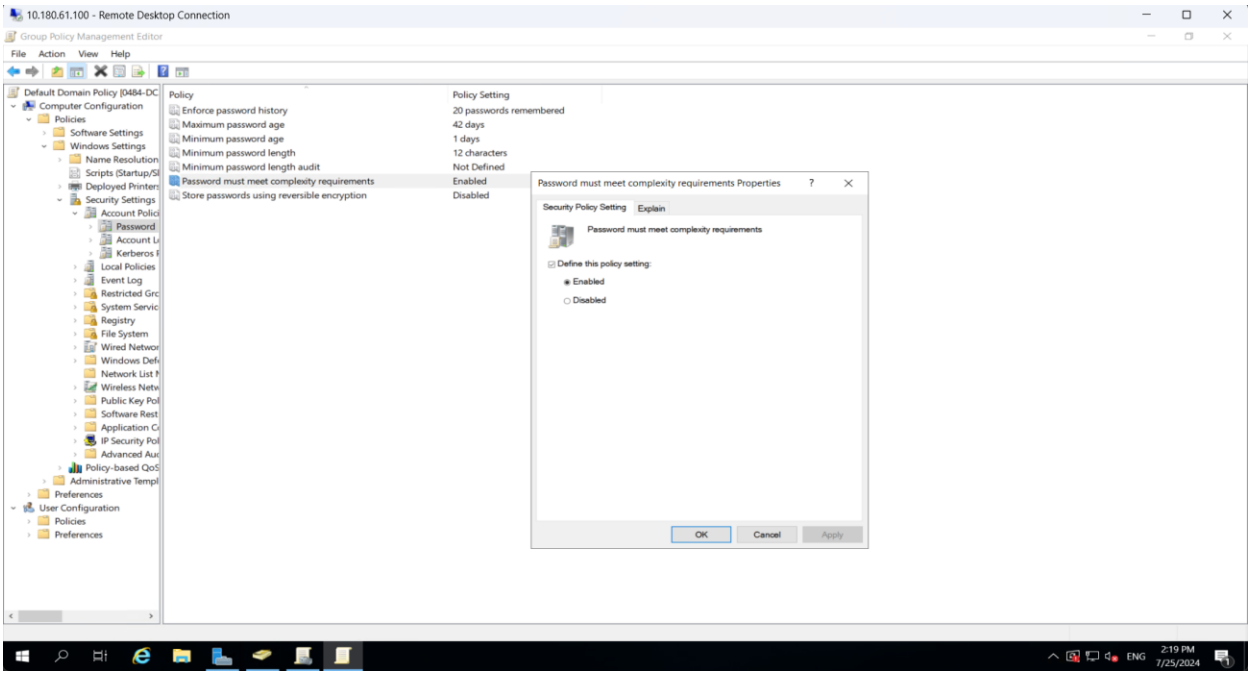

Fig 34: Picture shows Policy setting dialog box for the Password must meet complexity requirements which we will set to Enabled.

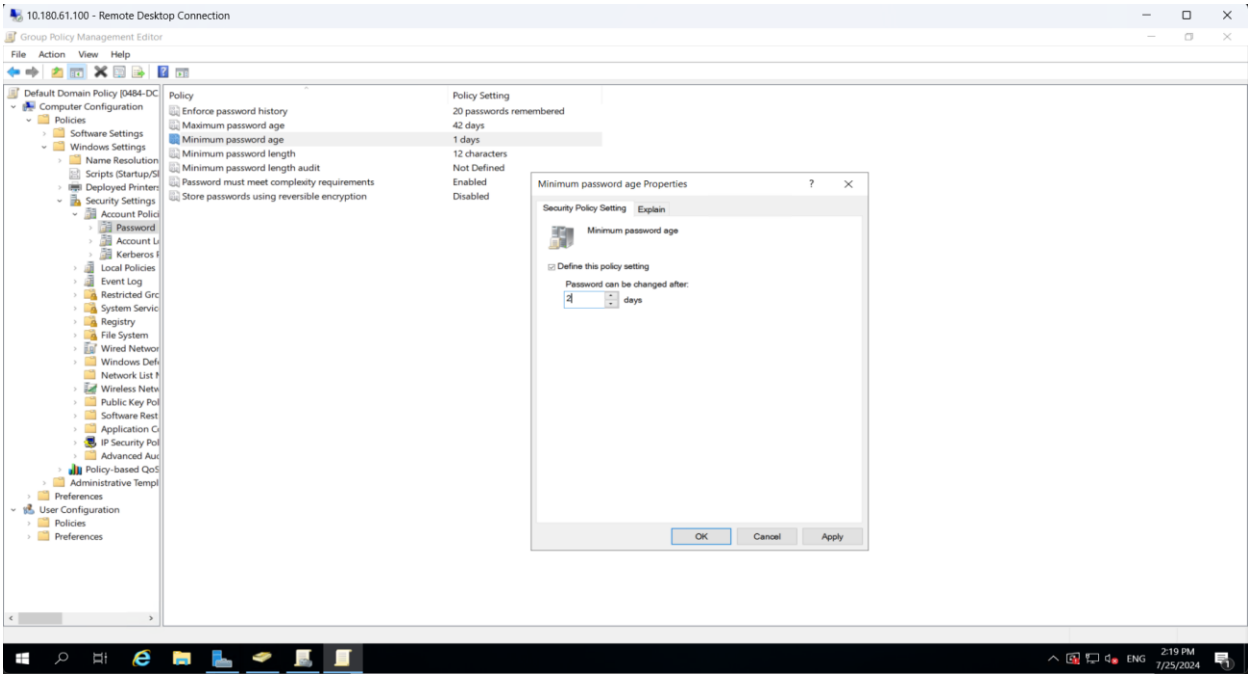

Fig 35: Picture shows Policy setting dialog box for the Minimum password age which we will set to 2 days.

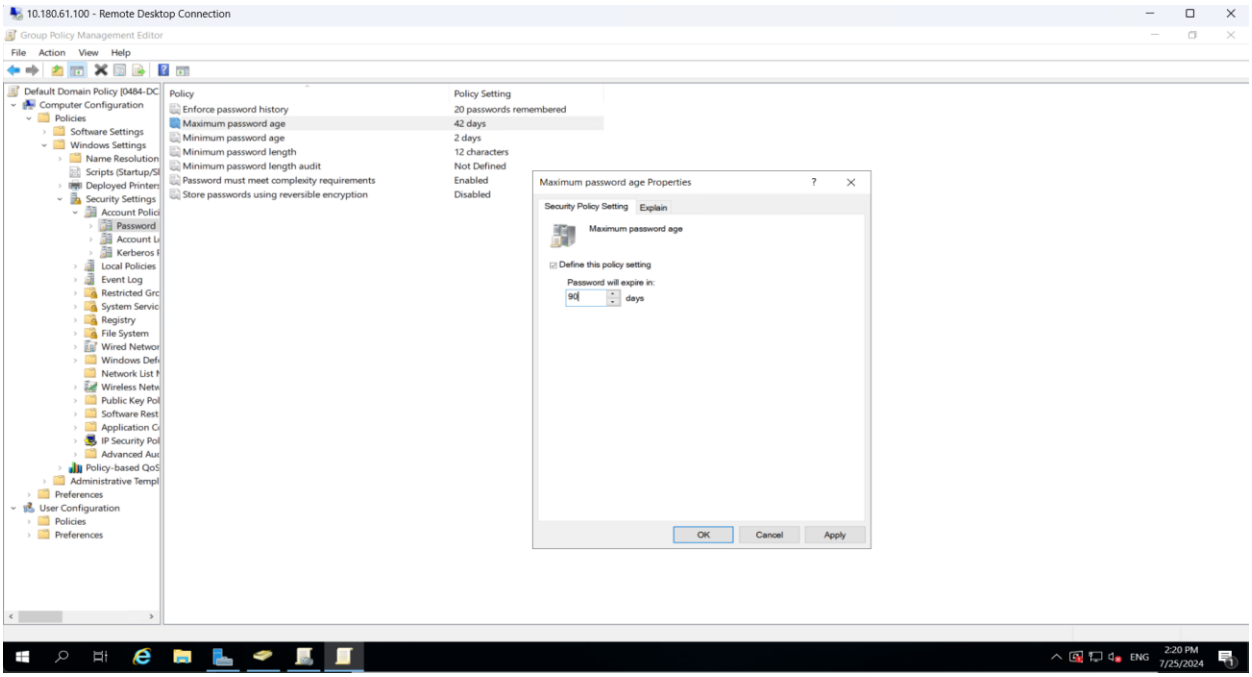

Fig 36: Picture shows Policy setting dialog box for the Maximum password age which we will set to 90 days.

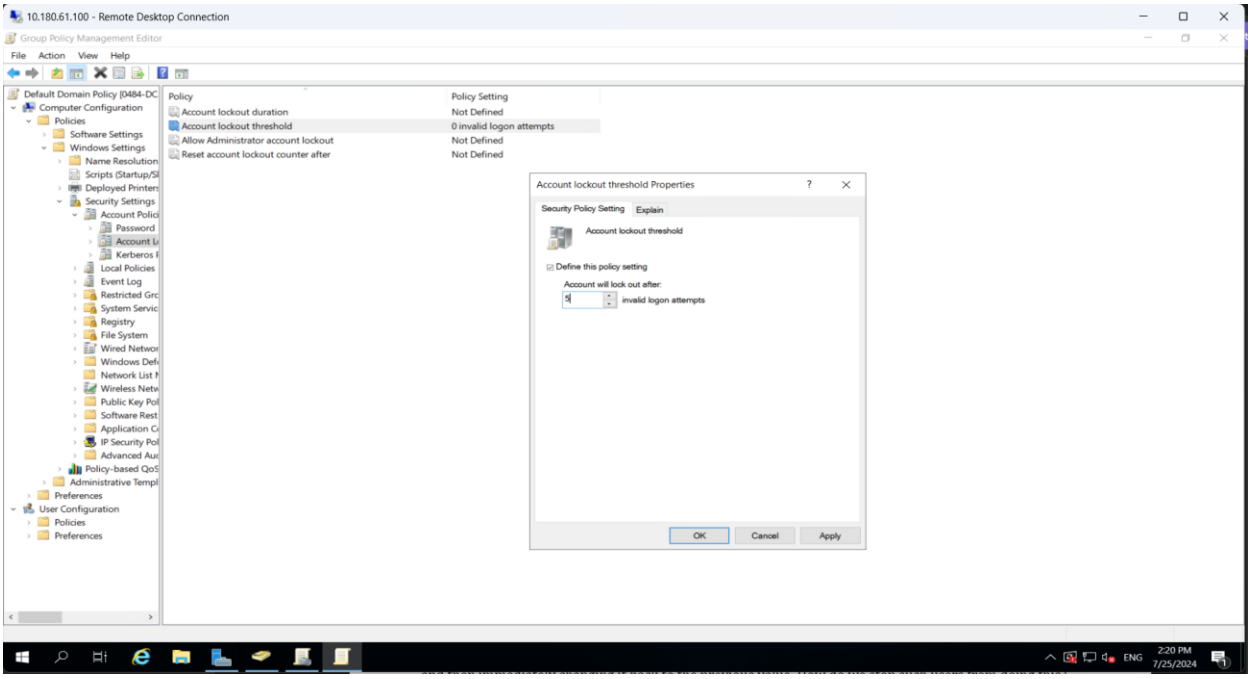

Fig 37: Picture shows Policy setting dialog box for the Number of failed Login attempts which we will set to 5 invalid login attempts.

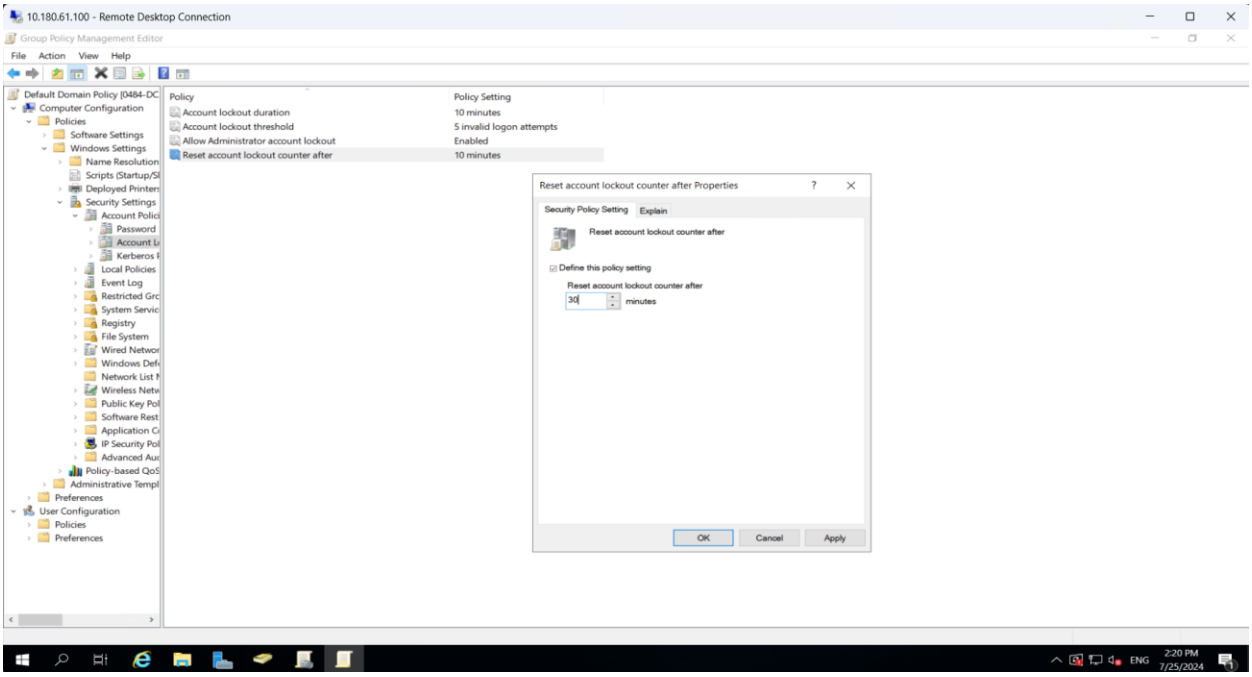

Fig 38: Picture shows Policy setting dialog box for the Reset failed logon which we will set to 30 Minutes.

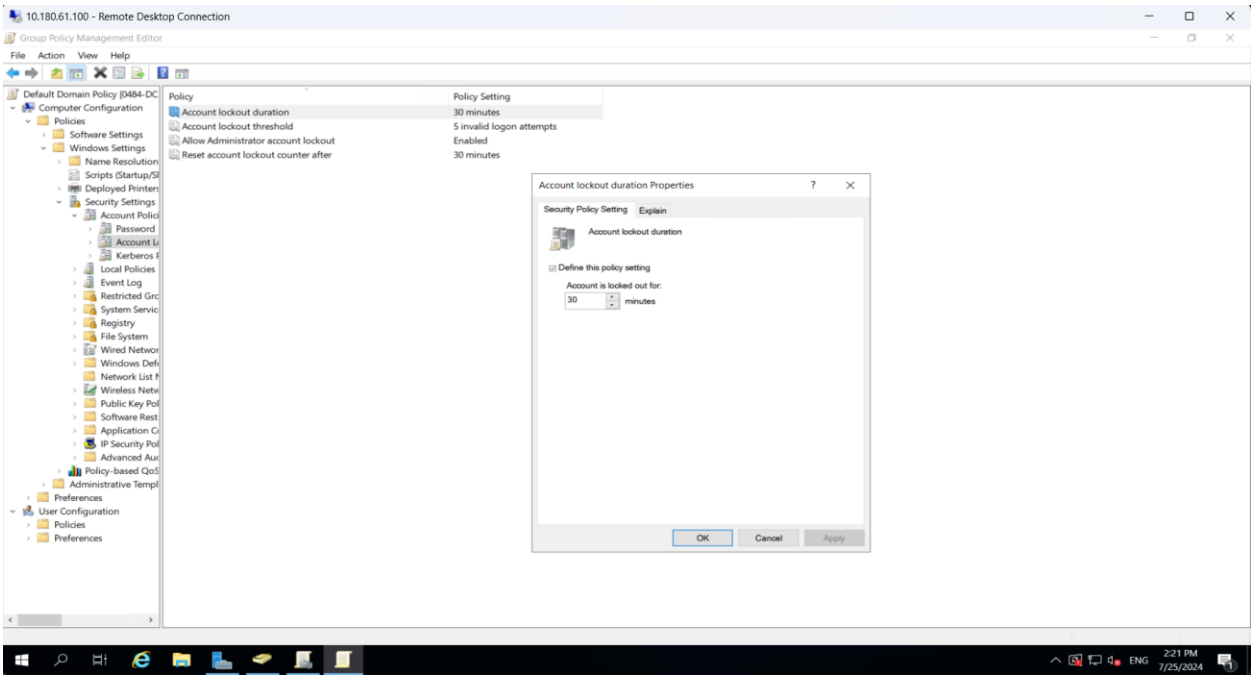

Fig 39: Picture shows Policy setting dialog box for the Account locked out duration which we will set to 30 minutes.

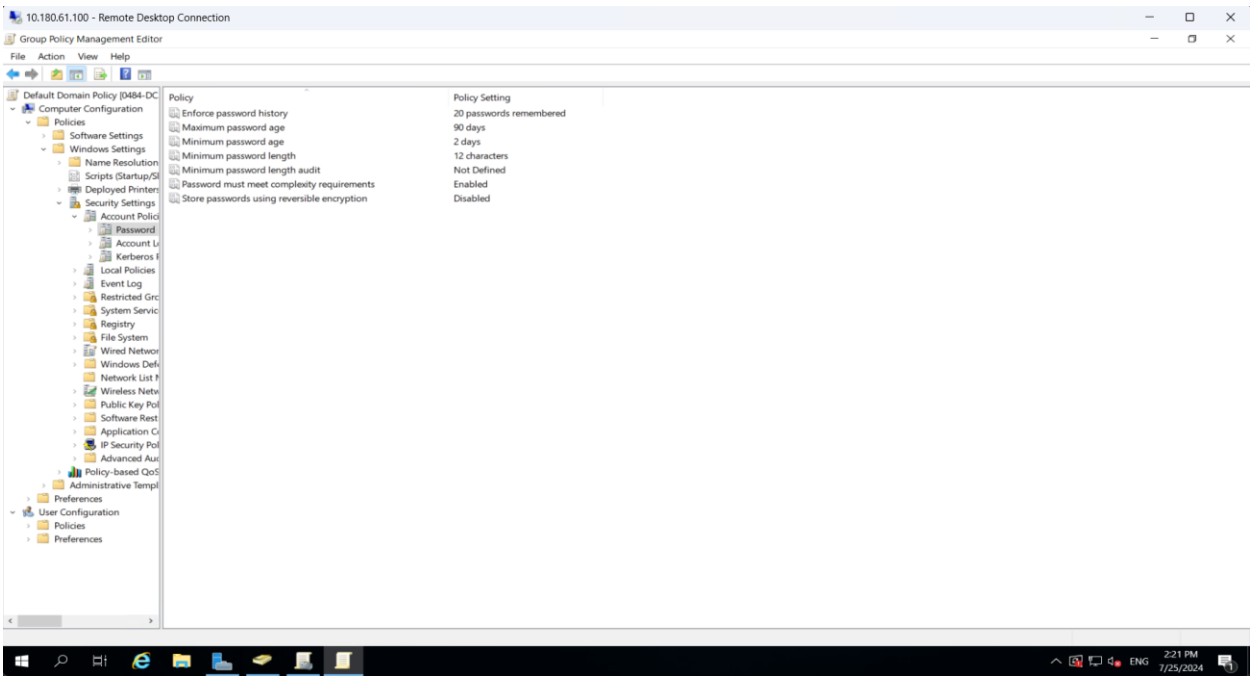

Fig 40: Picture shows successfully set all the account policies for the domain account.

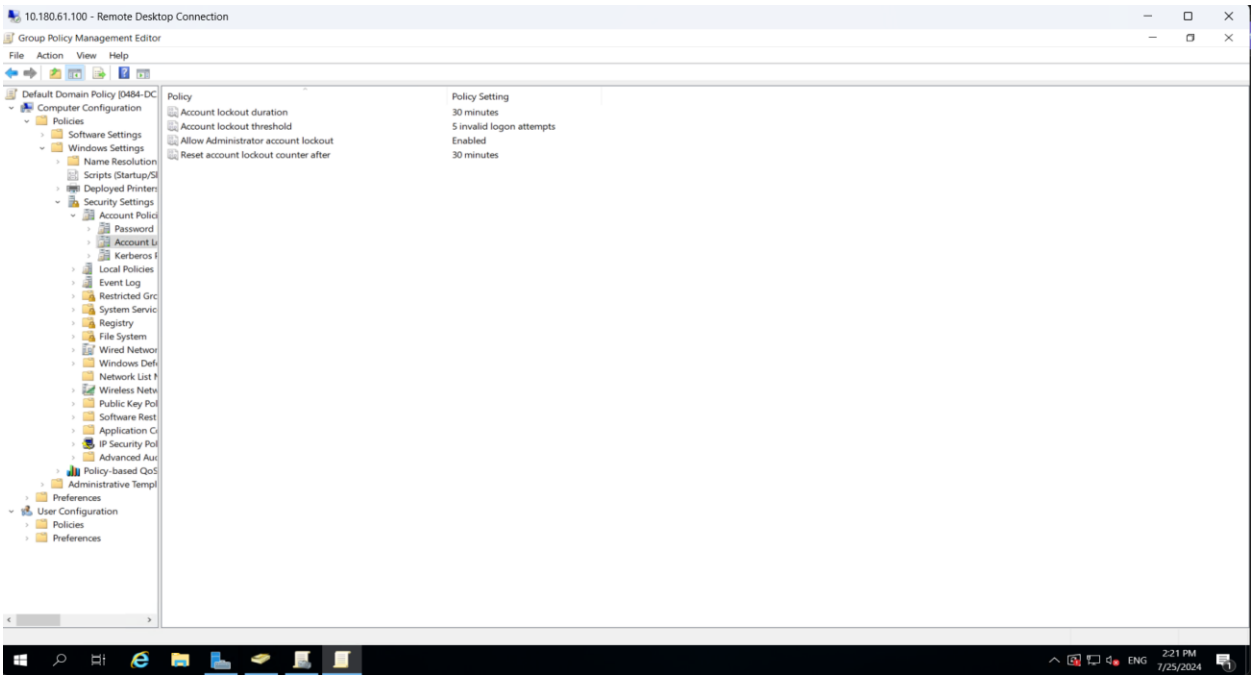

Fig 41: Picture shows successfully setting all the account policies for the domain account.

Reflection

We learned about functioning that is critical to securing a Windows Server environment, we touched on the domain join operations management as well as non-forgettable account security policies. In Exercise 1, you learned how to help limit domain join permissions to only those which you have configured; you removed the authenticated user's group from the default settings and set the ms-DS-MachineAccountQuota attribute to zero. This also upheld the role of principle of least privilege that holds that only the service accounts with limited rights can join computers in the domain. Hence, the practical aspect of performing the simulated creation of a service user account and the delegation of control provided a good understanding of how these security measures must be put into practice.

The second exercise concerned proper accounting policies & correctness of passwords to enhance password practices. Minimum password length, password history, and complexity requirements were put in place to increase the security of the users' accounts in the wake of possible breaches. The exercise also involved the use of account lockouts to avoid cases of brute force attacks. Managing and tweaking these options in the Group Policy Management console was insightful in understanding the solid defenses in an Active Directory environment. Combined, these exercises demonstrated the significance of the thorough configuration and adherence to policies in protecting the network infrastructure necessary for organizations' operations; none of the exercises were unrealistic or hypothetical, making the practical experience gained through these exercises highly beneficial.

Questions

1) To ensure that users cannot have just one password forever, which of these policies do we need to change?
Ans. Maximum password age.

2) Users sometimes attempt to bypass password change requirements by changing their password when it expires and then immediately changing it back to the previous value. How do we stop such users from doing this?
Ans. Enforce password history.

3) To make passwords complex and difficult to guess requires users to include different characters, such as uppercase characters, lowercase characters, digits, and symbols. Which policy would enable this?
Ans. Password must meet complexity requirements.