EC-Council

codered
FROM EC-COUNCIL

CHAPTER 5

NETWORK SECURITY CONTROLS - ADMINISTRATIVE CONTROLS

CERTIFIED CYBERSECURITY TECHNICIAN

Copyrights @ 2022 EC-Council International Ltd.

INDEX

Chapter 1:
Information Security Threats and Vulnerabilities

Copyrights @ 2022 EC-Council International Ltd.

SCENARIO

Compliance, policies, and governance are integral to the information security program of any organization. An organization needs to comply with certain regulatory standards to run its businesses. Simultaneously, it must also have strong security policies and governance in order to fulfil regulatory standards. The labs in this module will provide a real-time experience in designing and developing network security policies and procedures to ensure availability, confidentiality, and integrity across an organizational network.

OBJECTIVE

The objective of this lab is to provide expert knowledge in implementing network security policies including the following tasks:

- Implementation of password policies and auditing policies
- Designing Secure network and SSH server
- Implementation of policies for PowerShell security

OVERVIEW INTERRUPTED SESSIONS

A security policy is a well-documented set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status of an organization. Security policies are used to inform people on how to work in a safe and secure manner; they define and guide employee actions on how to deal with organization sensitive operation, data, or resources in an organization. The security policies are an integral part of the information security management program for any organization.
Security policy is a high-level document, or set of documents, describing the security controls that should be implemented to protect a company. It maintains confidentiality, availability, integrity, and asset values. Security policies form the foundation of a security infrastructure.

Copyrights @ 2022 EC-Council International Ltd.

LAB TASKS

A cyber security professional or security professional uses numerous tools and techniques to implement network security policies. The recommended labs that will assist you in learning the implementation of network security controls include:

01 **Implement Password Policies using Windows Group Policy**

02 **Implement Auditing Policies**

03 **Implement a Secure Network Policy**

04 **Implement a PowerShell Security Policy**

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

Copyrights @ 2022 EC-Council International Ltd.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

The Group Policy Management Console (GPMC) is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing group policy across the enterprise.

LAB SCENARIO

Security professionals can use the GPMC to manage group policies in the Active Directory (AD) across the enterprise. It can be used to protect user accounts and implement domain password policies to enable the use of complex and lengthy passwords. This prevents attackers from cracking the passwords of user accounts through brute-force attacks.
A security professional must configure group policy settings (group policy object, or GPO) in the AD domain to implement common password requirements.

OBJECTIVE

This lab demonstrates how to create a GPO from the GPMC; this group policy will implement a common password policy to enable the use of complex and lengthy passwords in the AD domain.

OVERVIEW OF GROUP POLICY

Group policies enable the cyber security professional to manage drive mappings, registry settings, local users and groups, services, files, and folders without the need to learn a scripting language. GPO can help in configuring the password history, password age, password length, and complexity and store user passwords using reversible encryption policies for users' passwords. The AD domain contains two default GPOs:

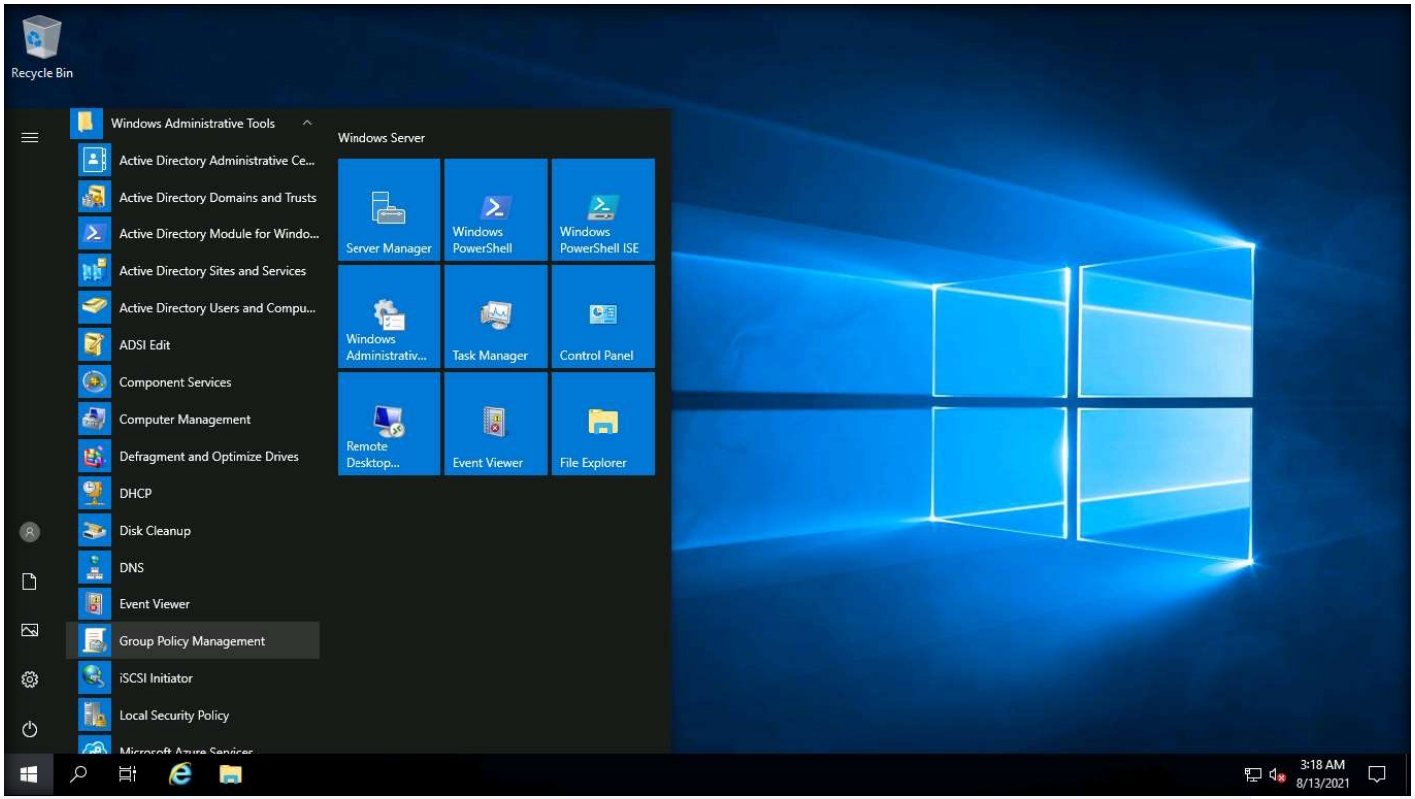
- Default domain policy, which is linked to the domain

- Default domain controllers policy, which is linked to the domain controller's organizational unit (OU).

Copyrights @ 2022 EC-Council International Ltd.

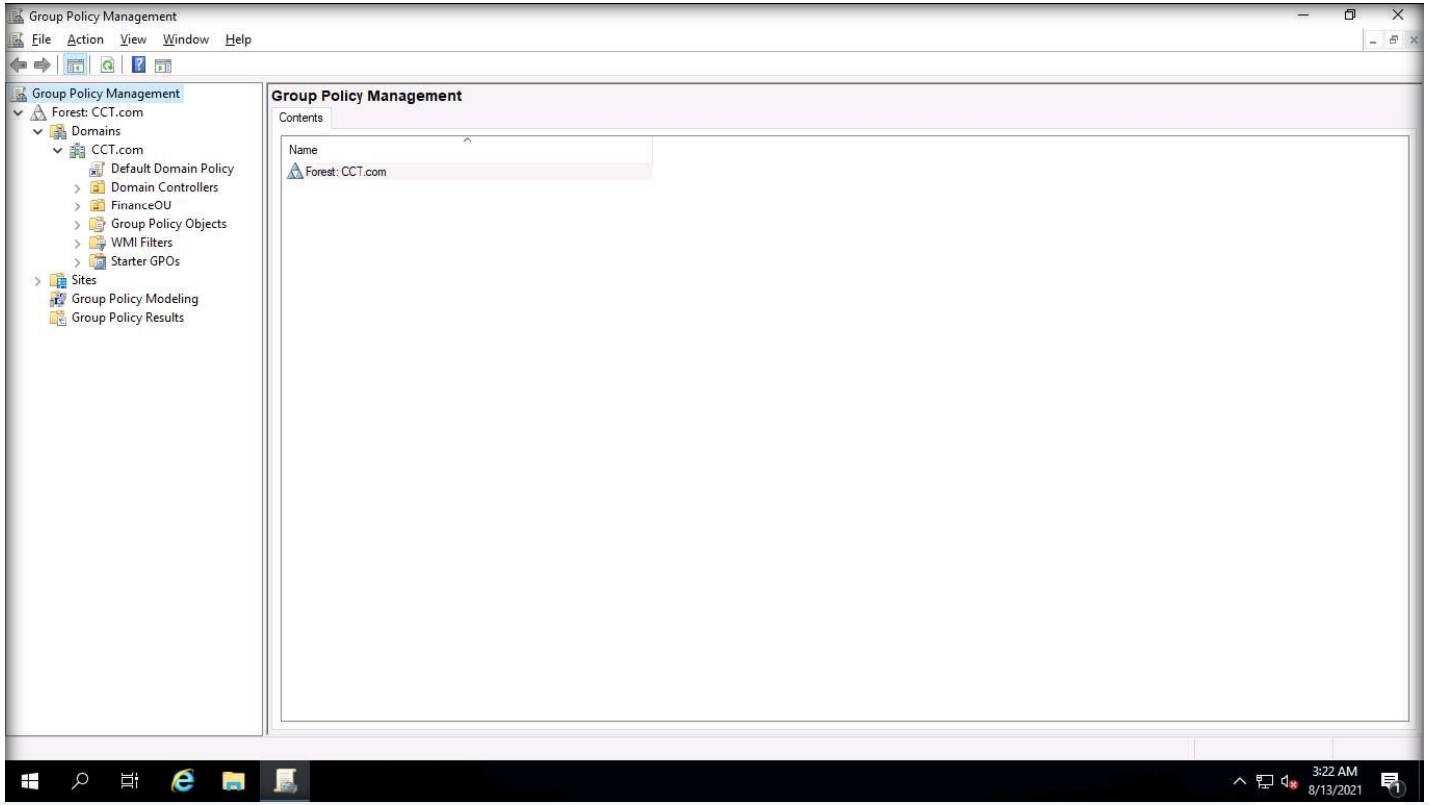
Note: If there are conflicting group policies, the last applied policy is implemented.
Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on AD Domain Controller and Web Server virtual machines.
2. In the AD Domain Controller virtual machine, log in with the credentials CCT\Administrator and admin@123.
Note: The network screen appears, click Yes.
3. Launch Group Policy Management to create a new password policy. To launch GPM, click Windows Start icon and navigate to Windows Administrative Tools → Group Policy Management.
Note: Alternatively, you can launch Group Policy Management by typing gpmc.msc in Run. To open Run, right-click on Start and click Run.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



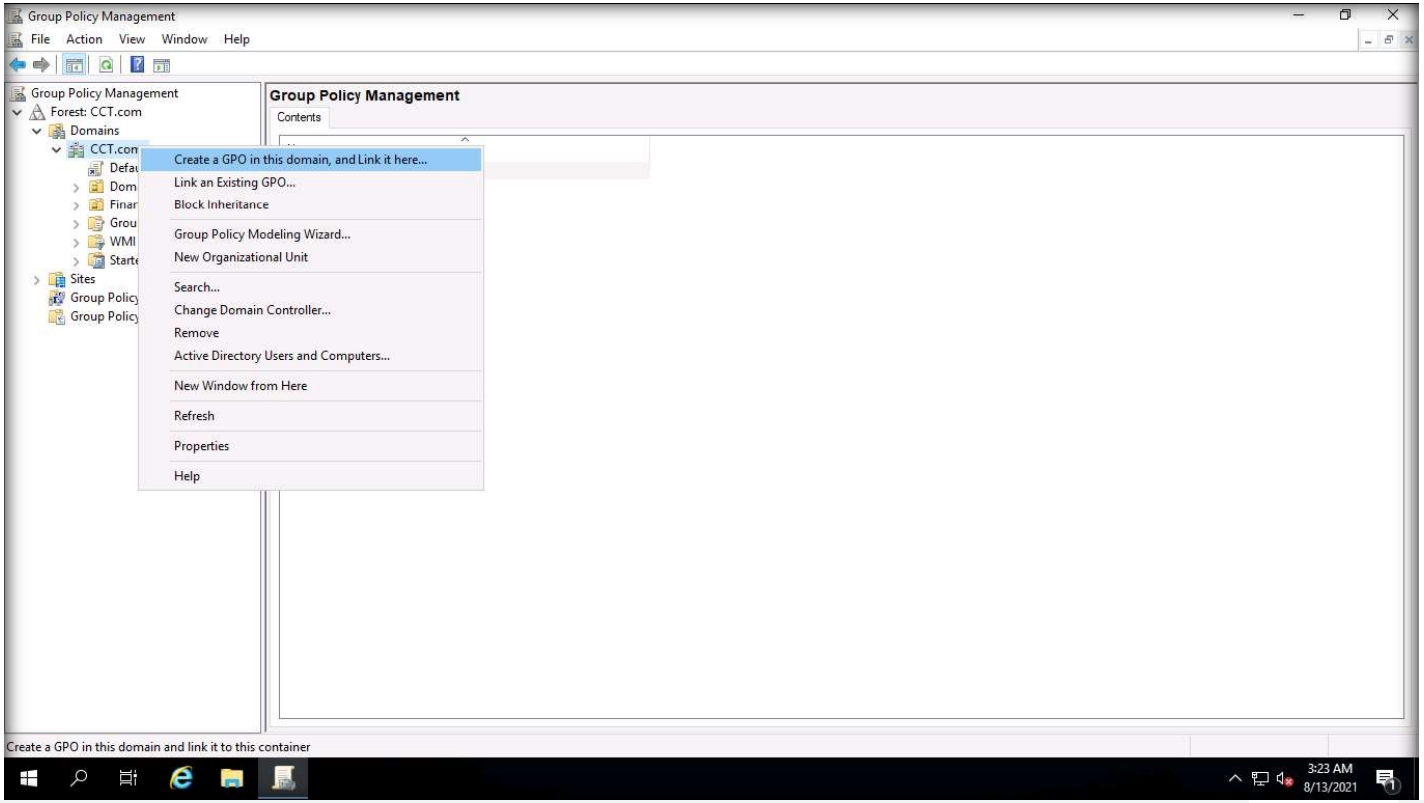
4. The Group Policy Management main window appears, as shown in the screenshot below. Expand the Forest: CCT.com domain tree.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



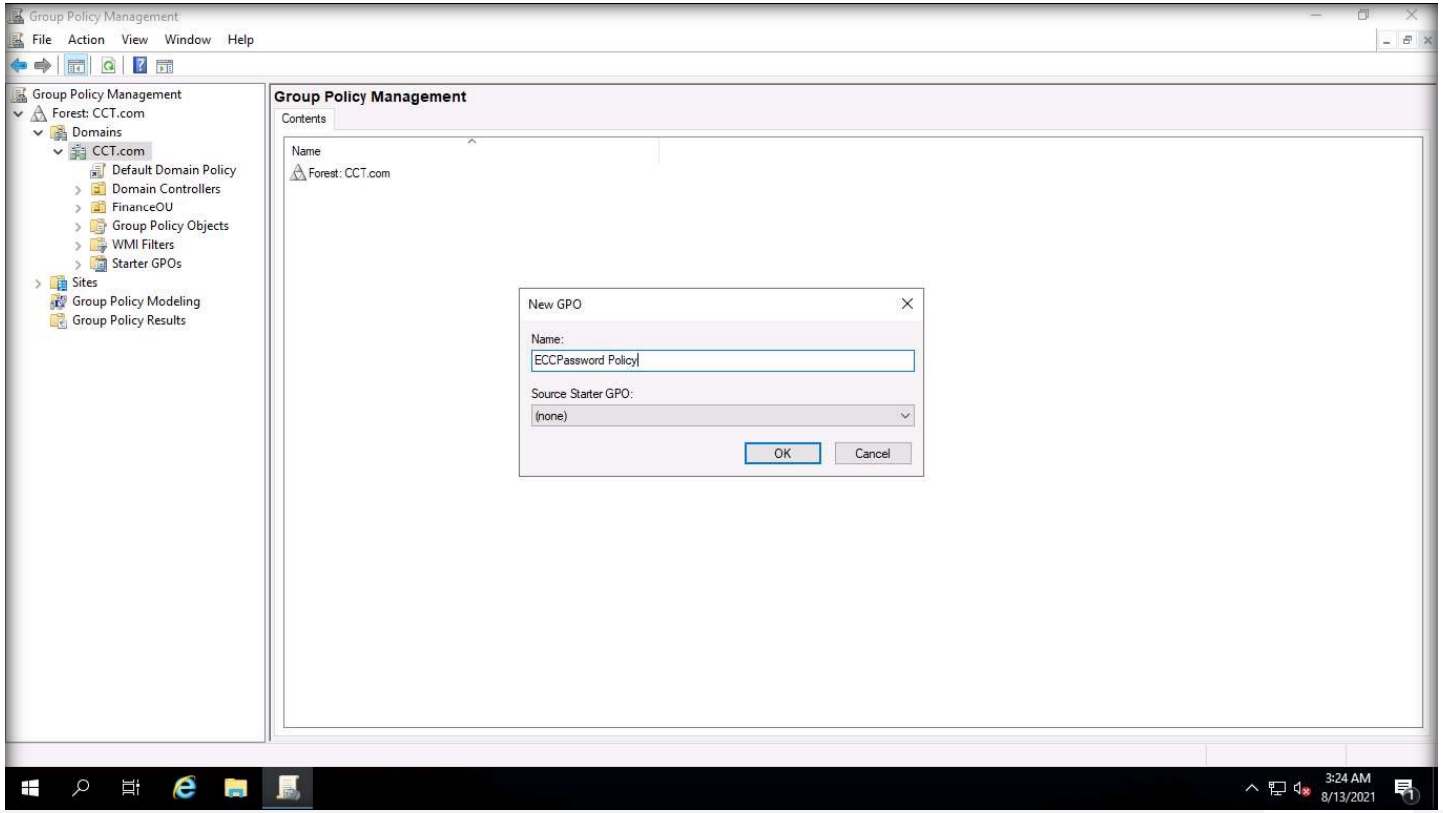
5. To create a new GPO to implement password policies across the domain (CCT.com), under the Domains tree, right-click on the CCT.com domain, and select Create a GPO in this domain, and Link it here....

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



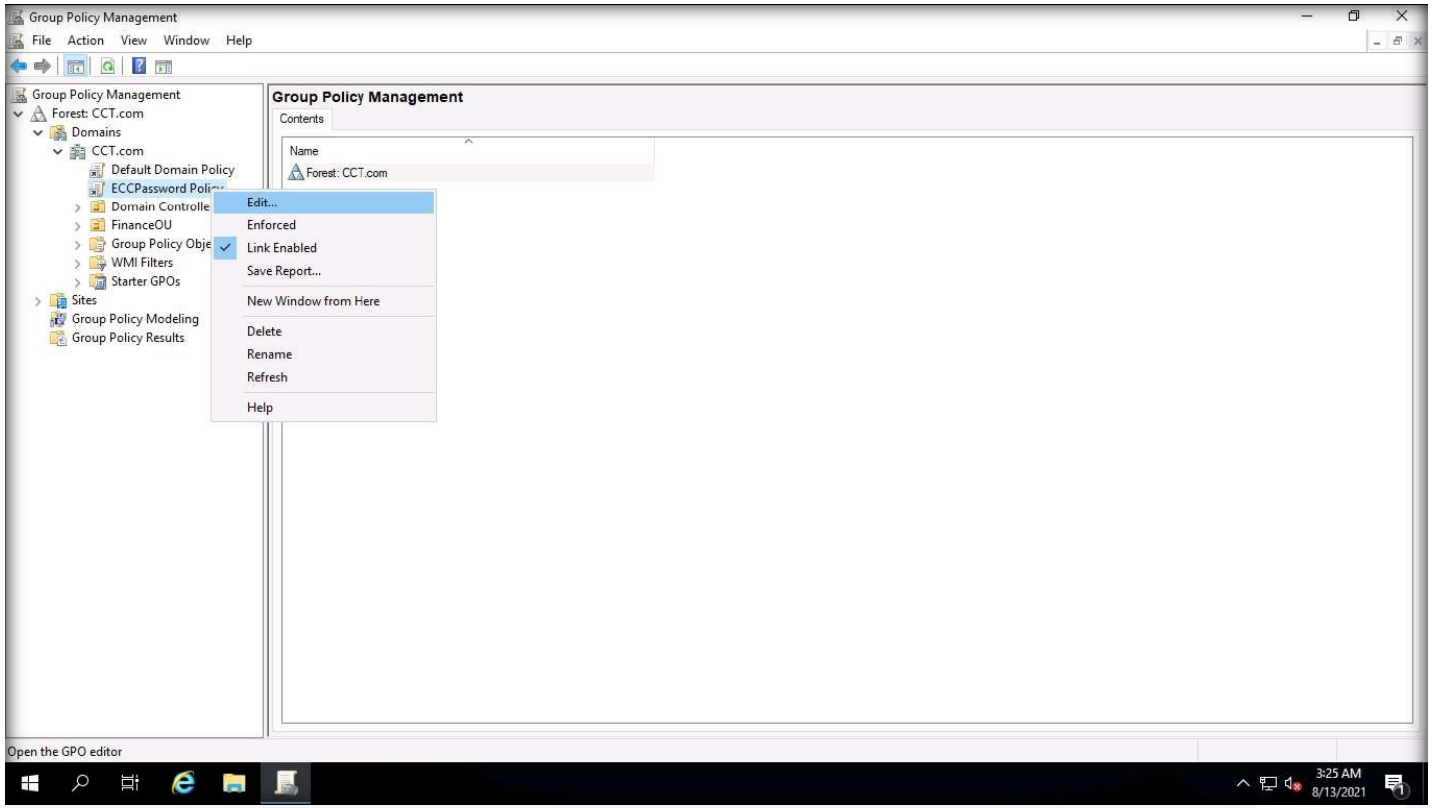
6. The New GPO window opens, type the name for the new GPO as “ECCPassword Policy” and click OK (use any name as per your requirement).

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



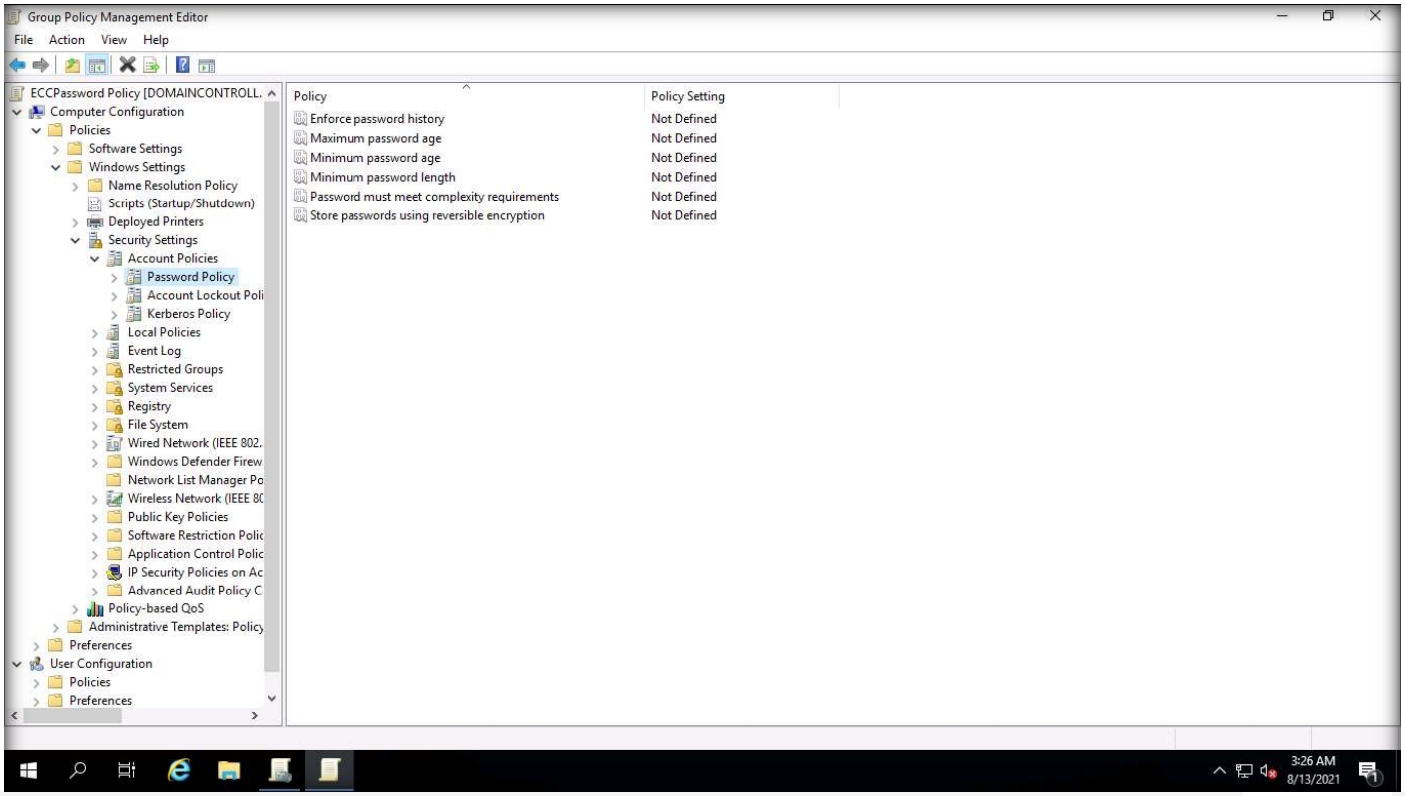
7. A new GPO ECCPassword Policy will be created. Expand CCT.com to view the created GPO (ECCPassword Policy). To configure the settings for ECCPassword Policy, right-click on ECCPassword Policy and select Edit....

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



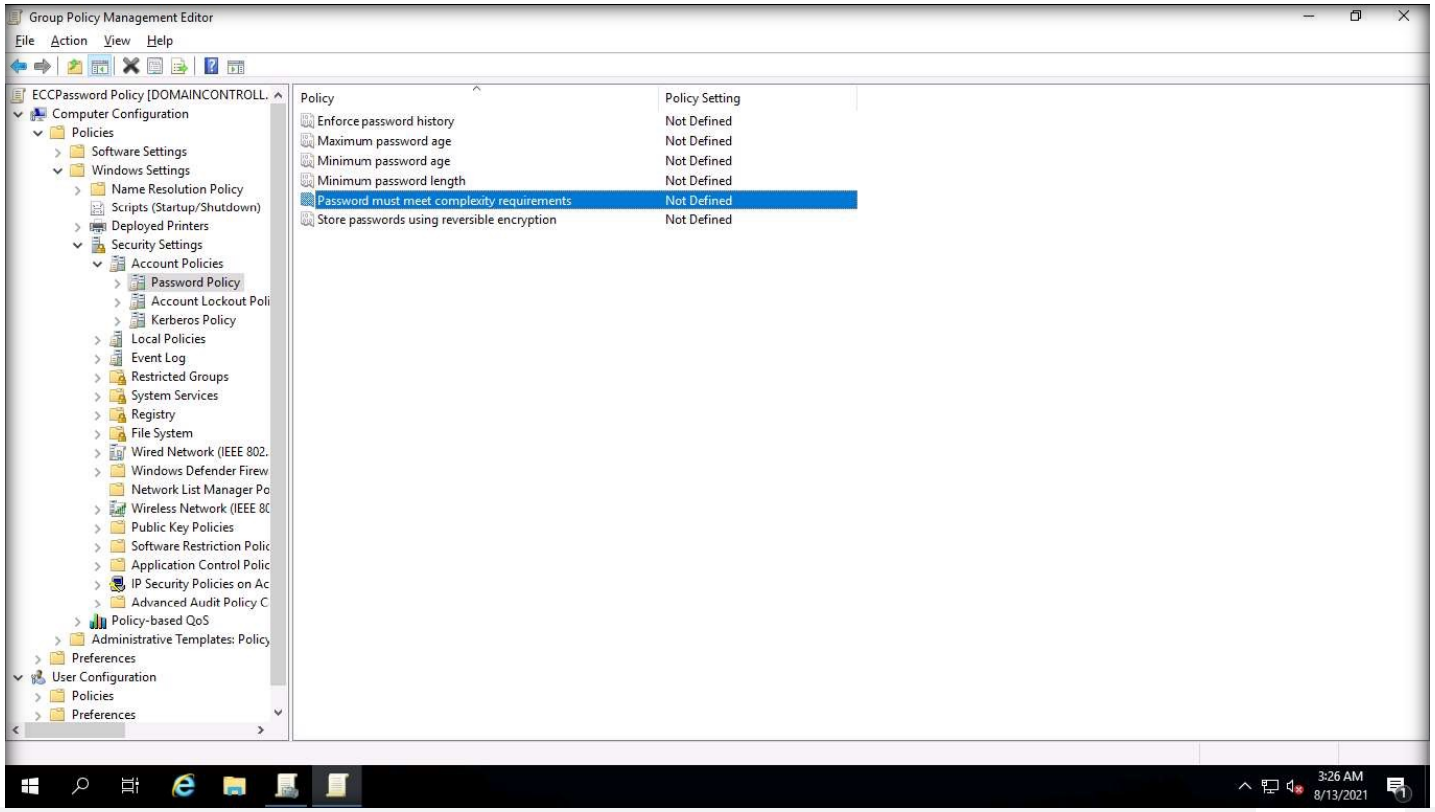
8. In the Group Policy Management Editor window, expand Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies. Click on Password Policy; the password policies will be listed in the right pane.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



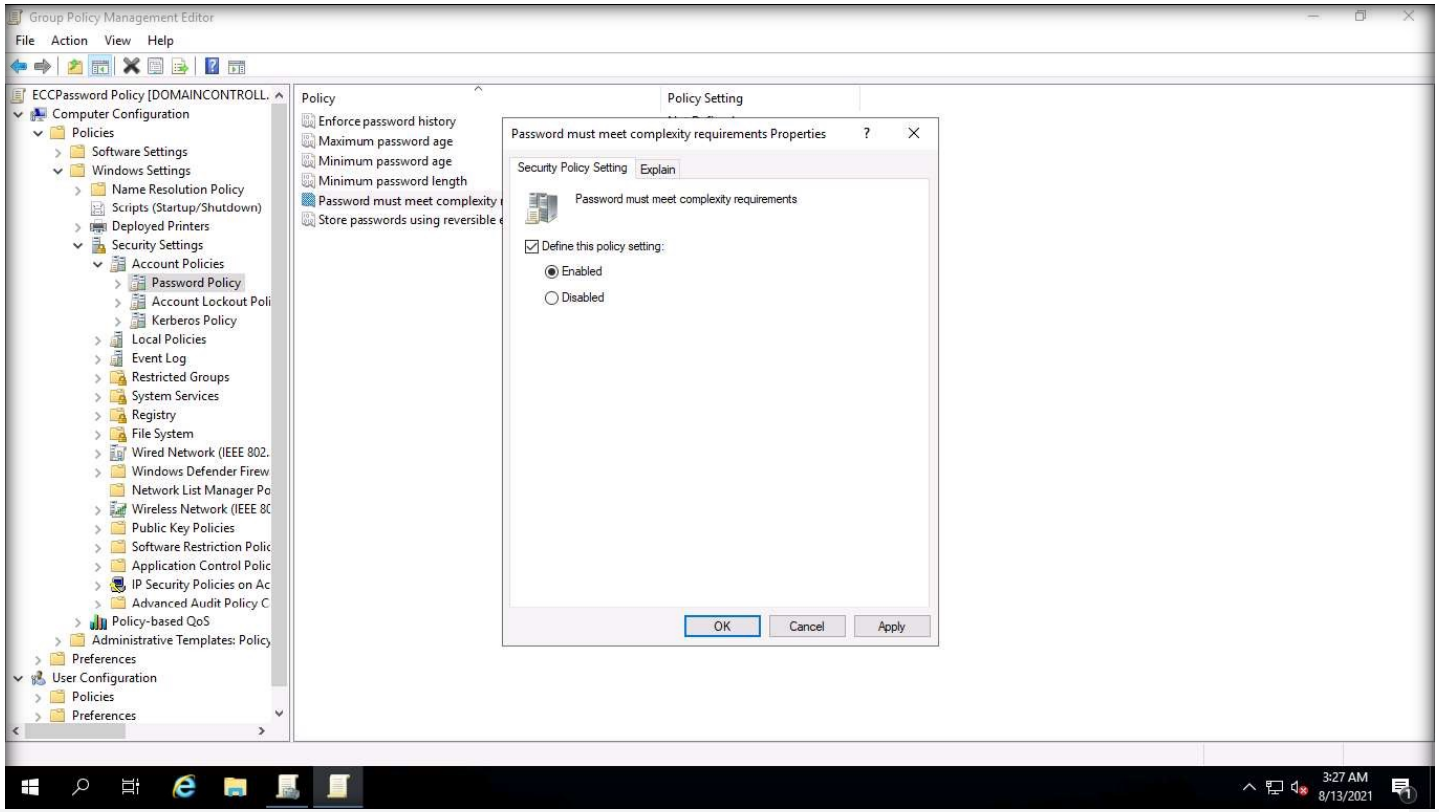
9. Ensure that the created, or modified, password does not contain the user account name or parts of the full name of the user, i.e., two consecutive characters in the name—and is at least six characters in length; it must also contain English uppercase characters (A through Z), English lowercase characters (a through z), numeric 10 digits (0 through 9), and non-alphabetic characters such as !, $, #, and %. The password must meet the complexity requirements policy setting. To ensure this, double-click on the Password must meet complexity requirements policy in the right pane

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



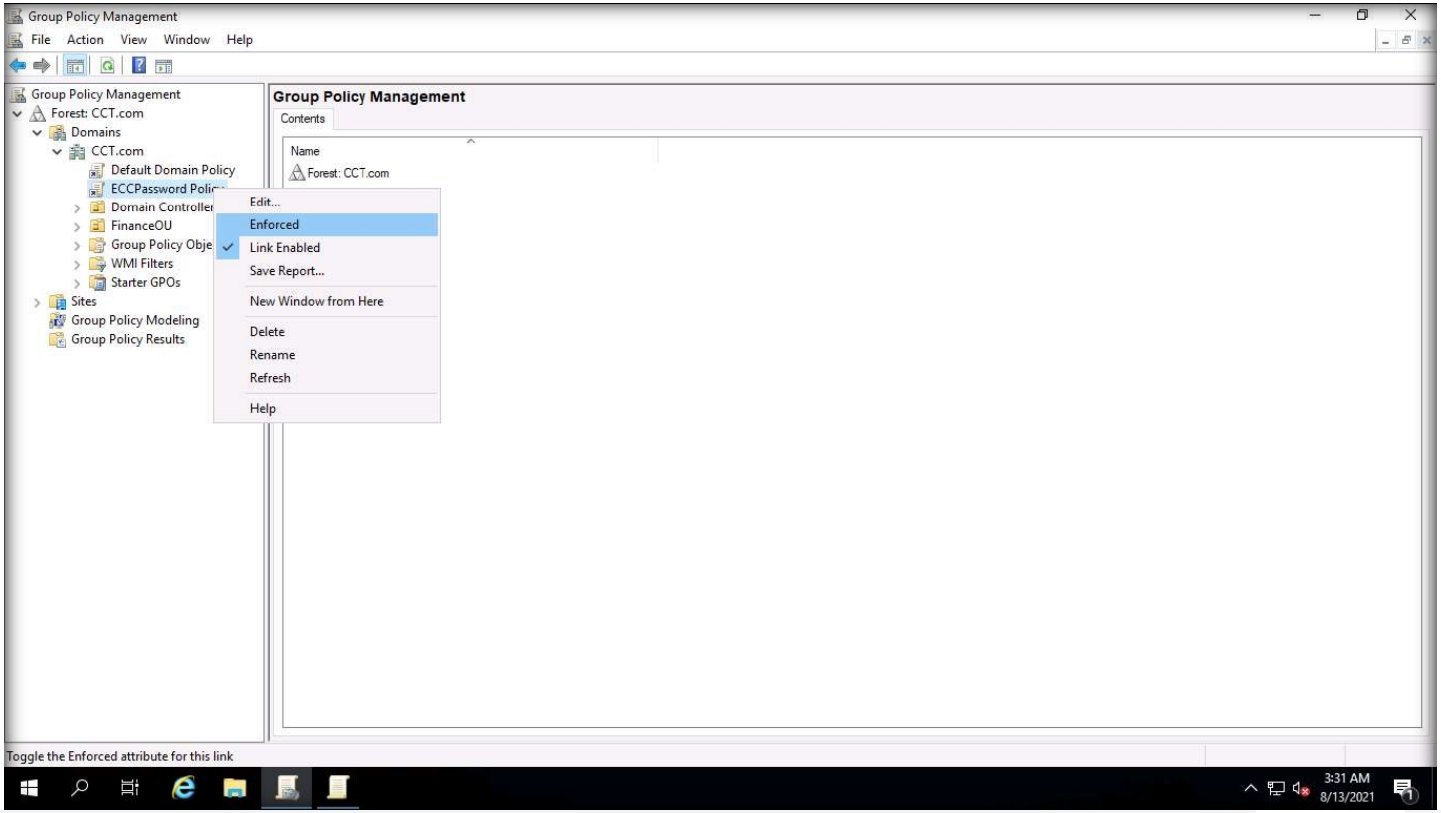
EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

10. In the Password must meet complexity requirements Properties window, check Define this policy setting and select the Enabled radio button to enable the password complexity policy. You can click the Explain tab to view the details of the policy. Click Apply and then click OK to close the policy properties window



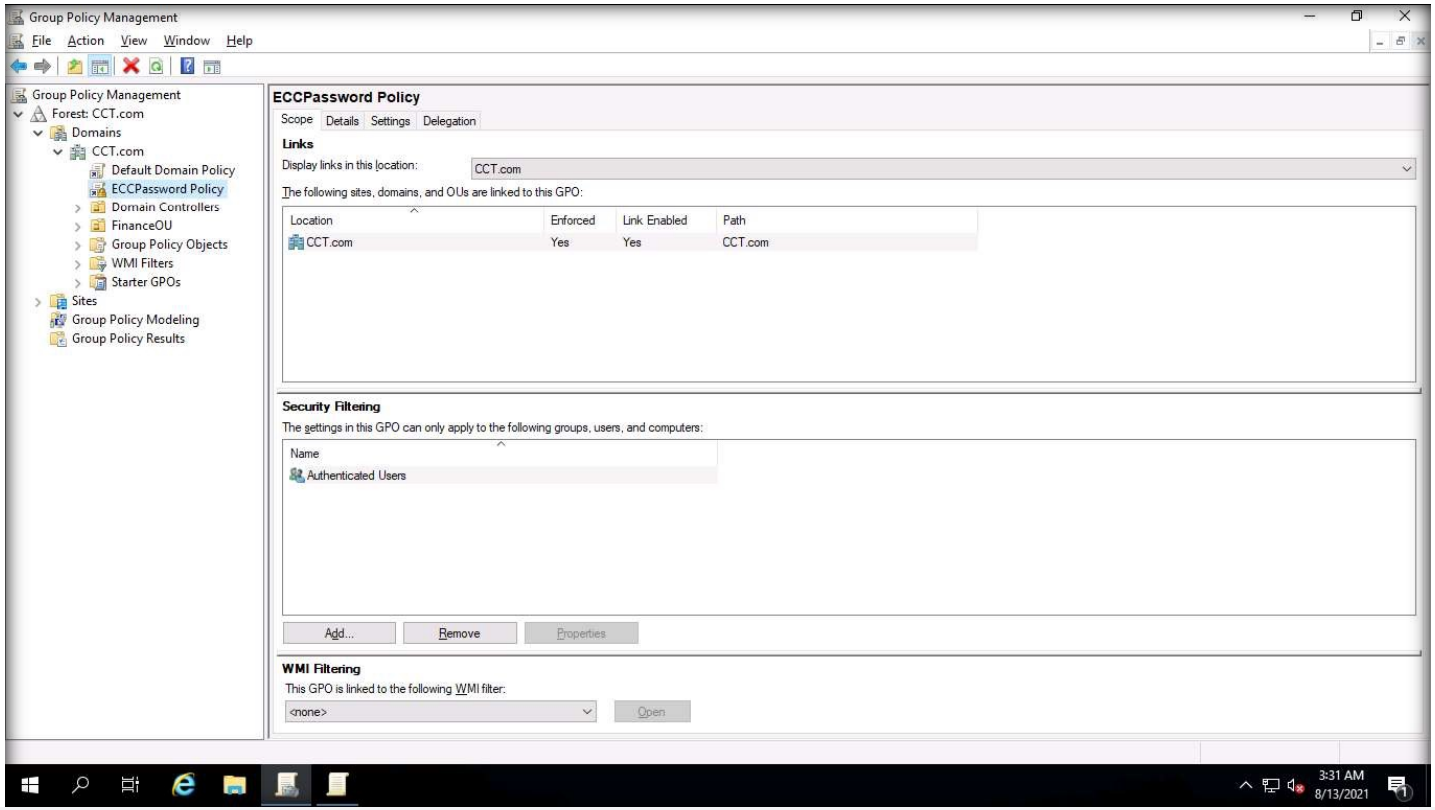
11. Switch to the Group Policy Management window. To ensure that the GPO is not overridden by other GPOs, and cannot be blocked from the parent container, enforce the created policy by right-clicking on ECCPassword Policy and selecting the Enforced option.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



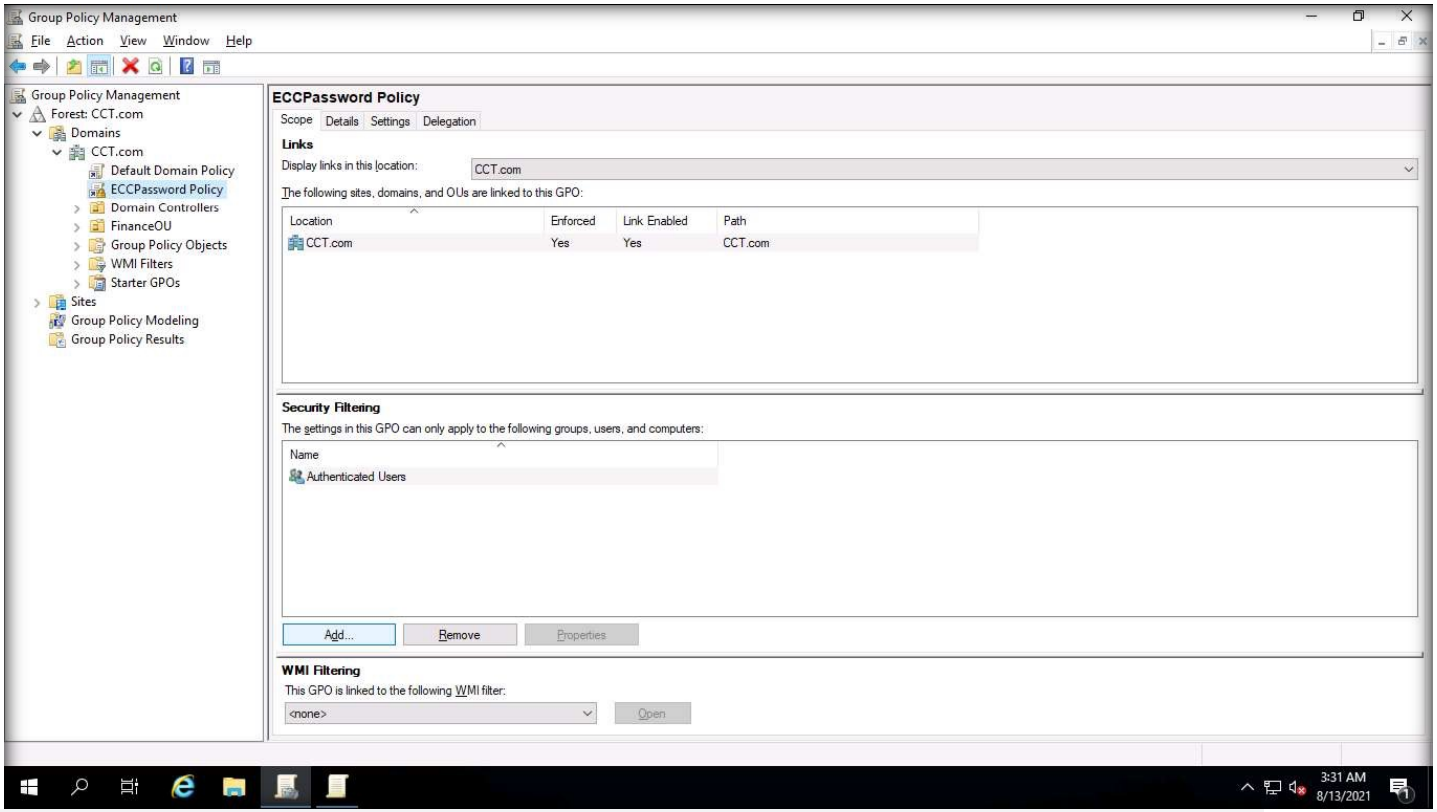
Note: If a Group Policy Management Console window appears click on OK.
Note: If the link is already enabled, then skip this step.
12. Click on ECCPassword Policy and you can see that the policy has been enforced and linked, as shown in the screenshot.
Note: If a Group Policy Management Console window appears click on OK.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



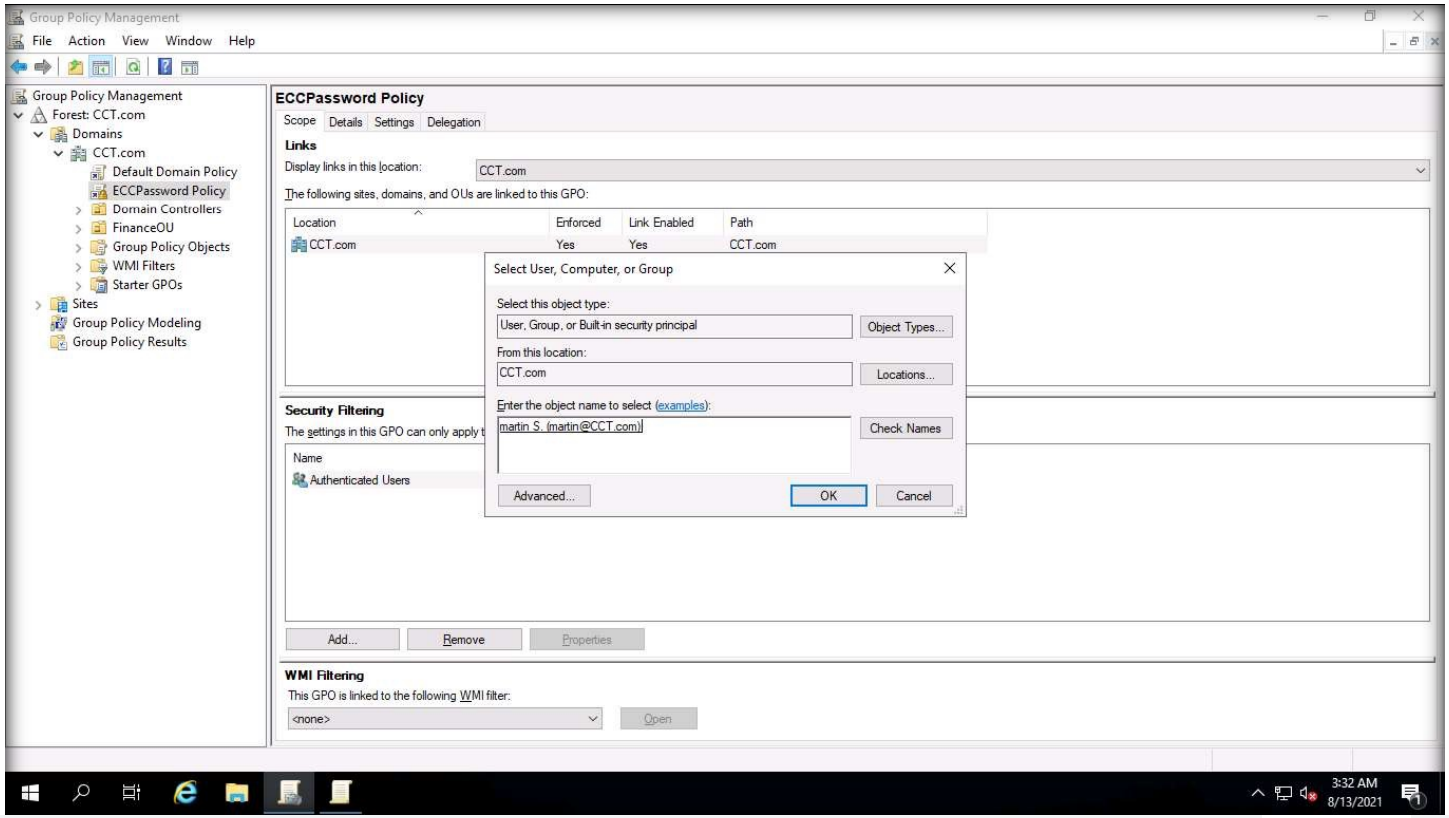
13. To select the users, groups, and computers to which the policy should be applied, click Add... under the Security Filtering section of ECCPassword Policy.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



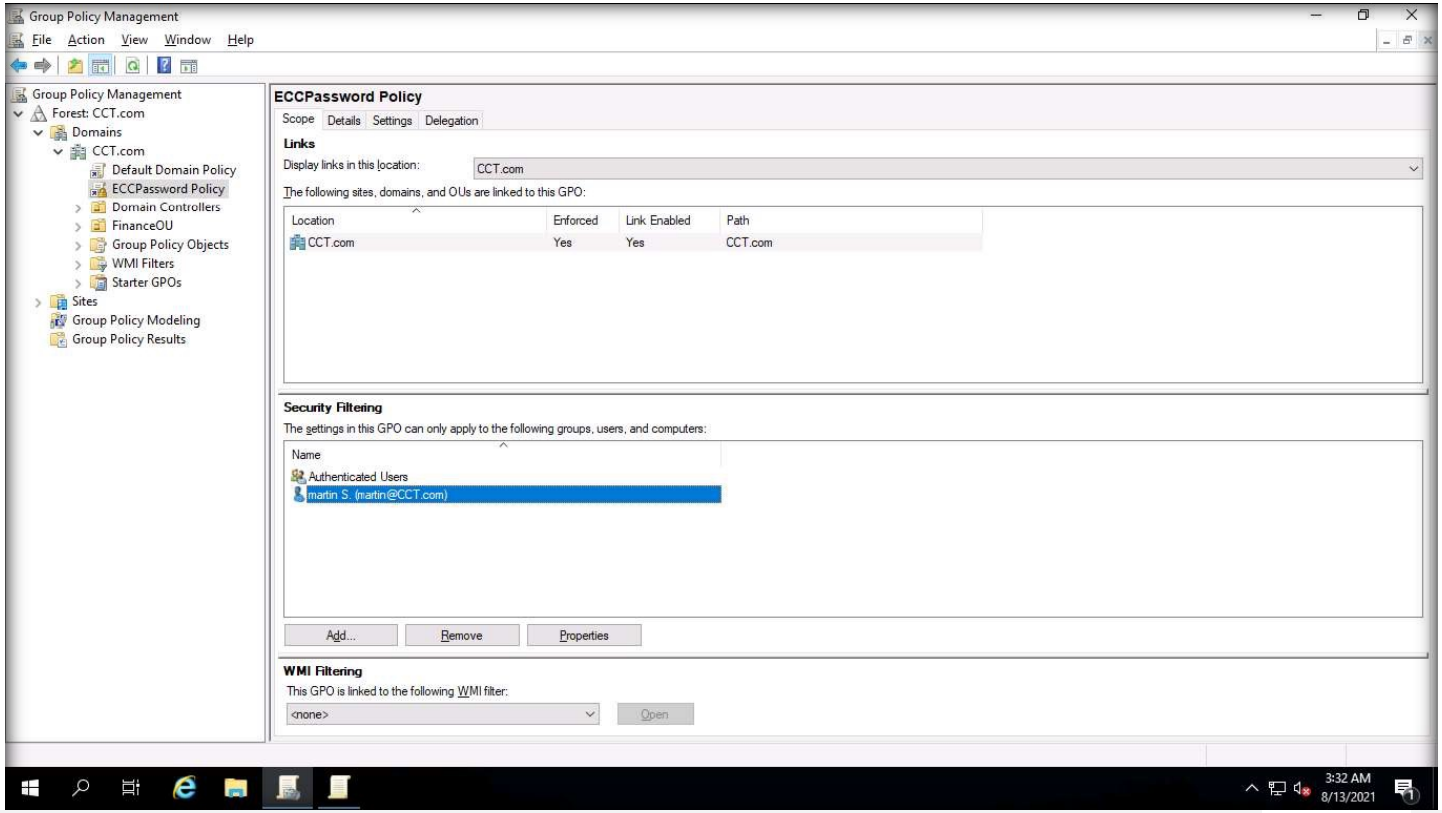
14. The Select User, Computer, or Group window opens; you can apply this policy to the selected users, computer, or groups. Type “Martin” in the Enter the object name to select (examples) field and click Check Names button. When the system displays the user details of Martin, click OK.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



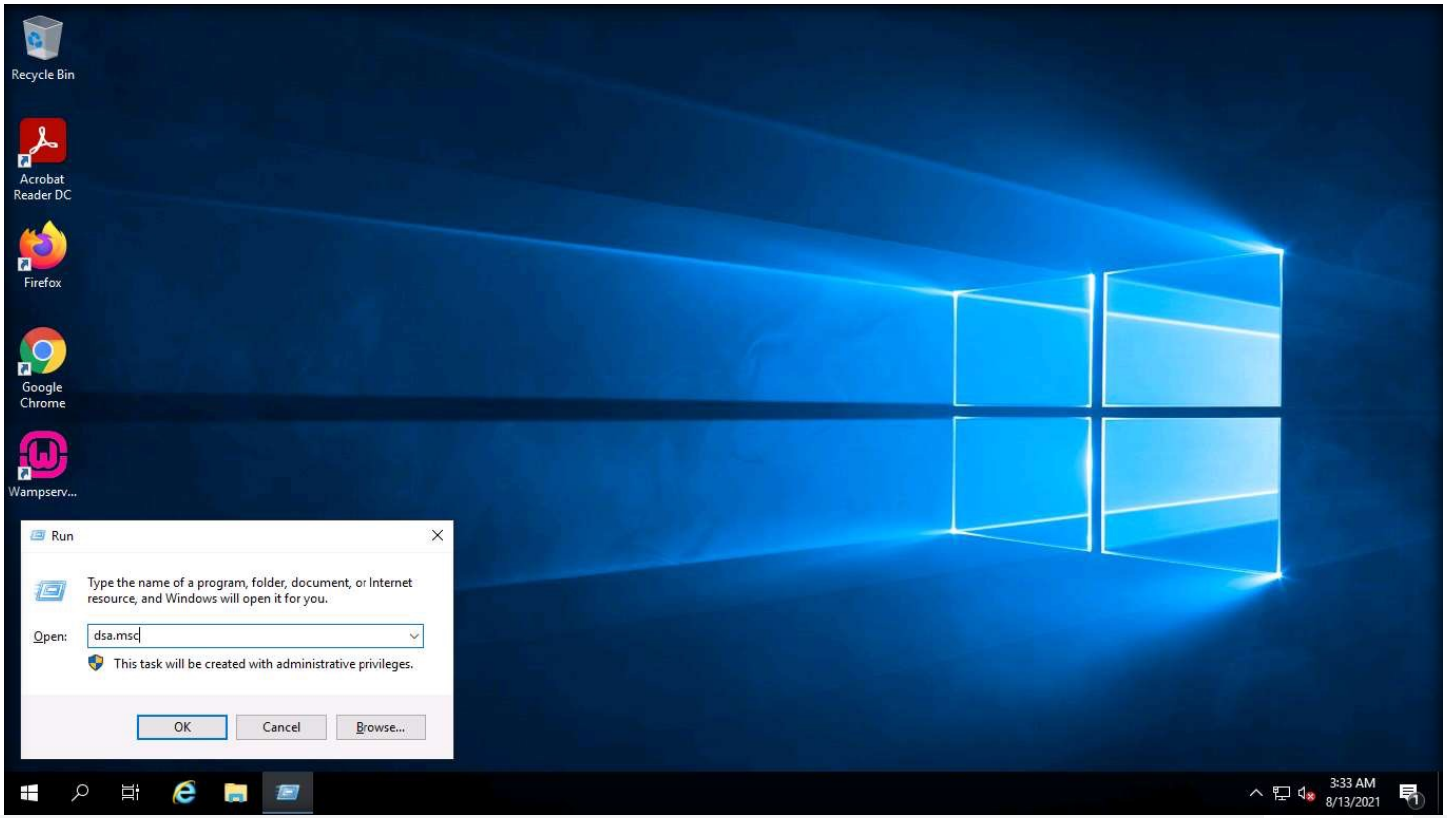
15. Once the GPO is applied to user Martin, you can view the user in the Security Filtering tab.

EXERCISE 1:
IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



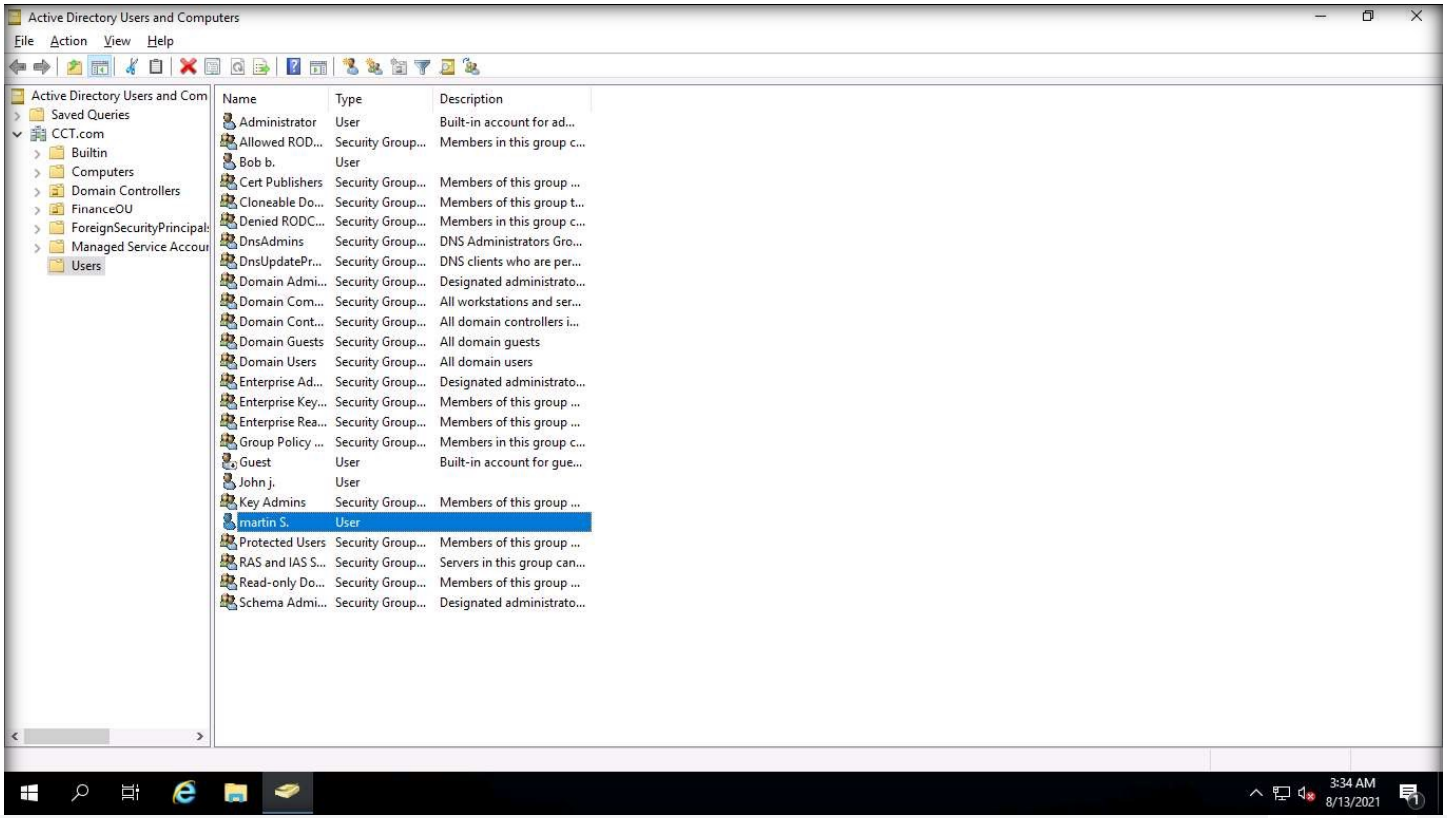
16. To demonstrate the effect of the GPO for enforcing Password must meet complexity requirements, ensure that user Martin is forced to change the password at the next login.
17. Close all open windows.
18. To change user the password settings of user Martin, right-click on Windows Start icon and select Run, type dsa.msc. Click OK. The Active Directory Users and Computers window will open.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



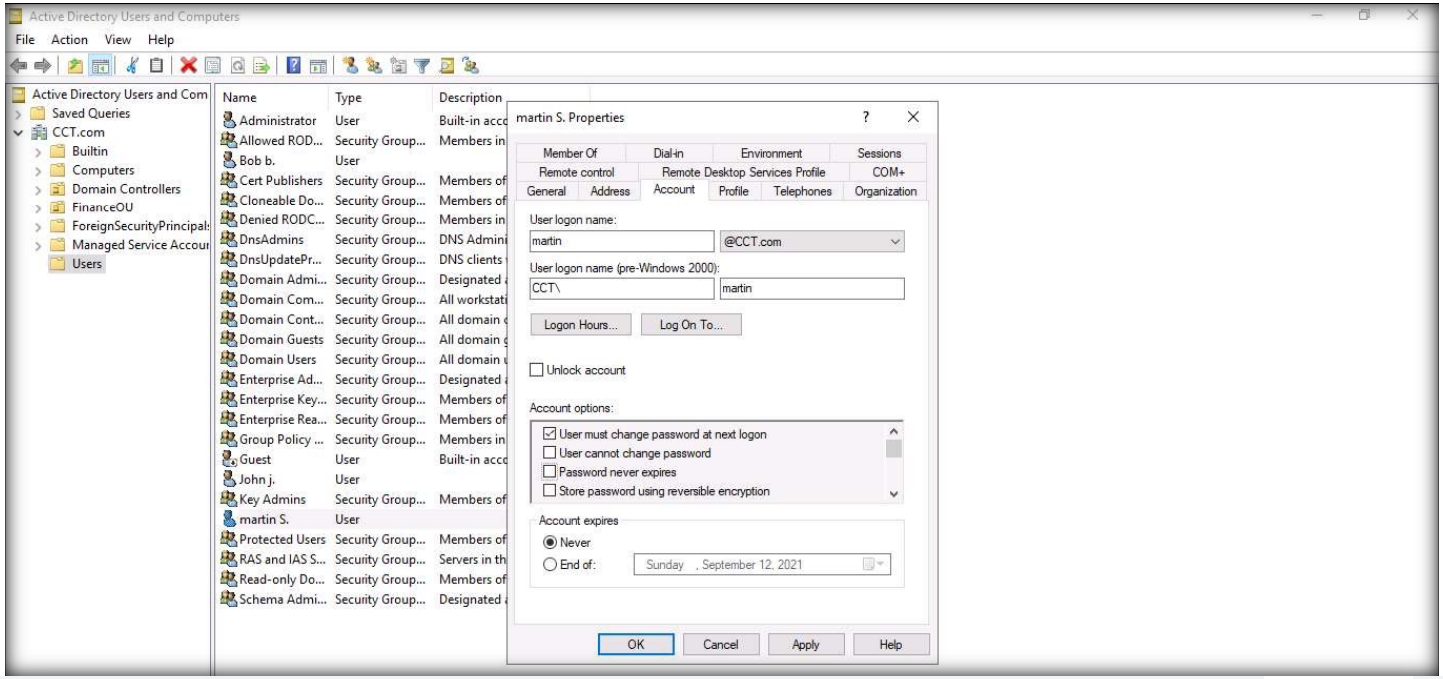
19. Expand CCT.com and select Users, which shows the list of AD users; double-click on martin S.

EXERCISE 1:
IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



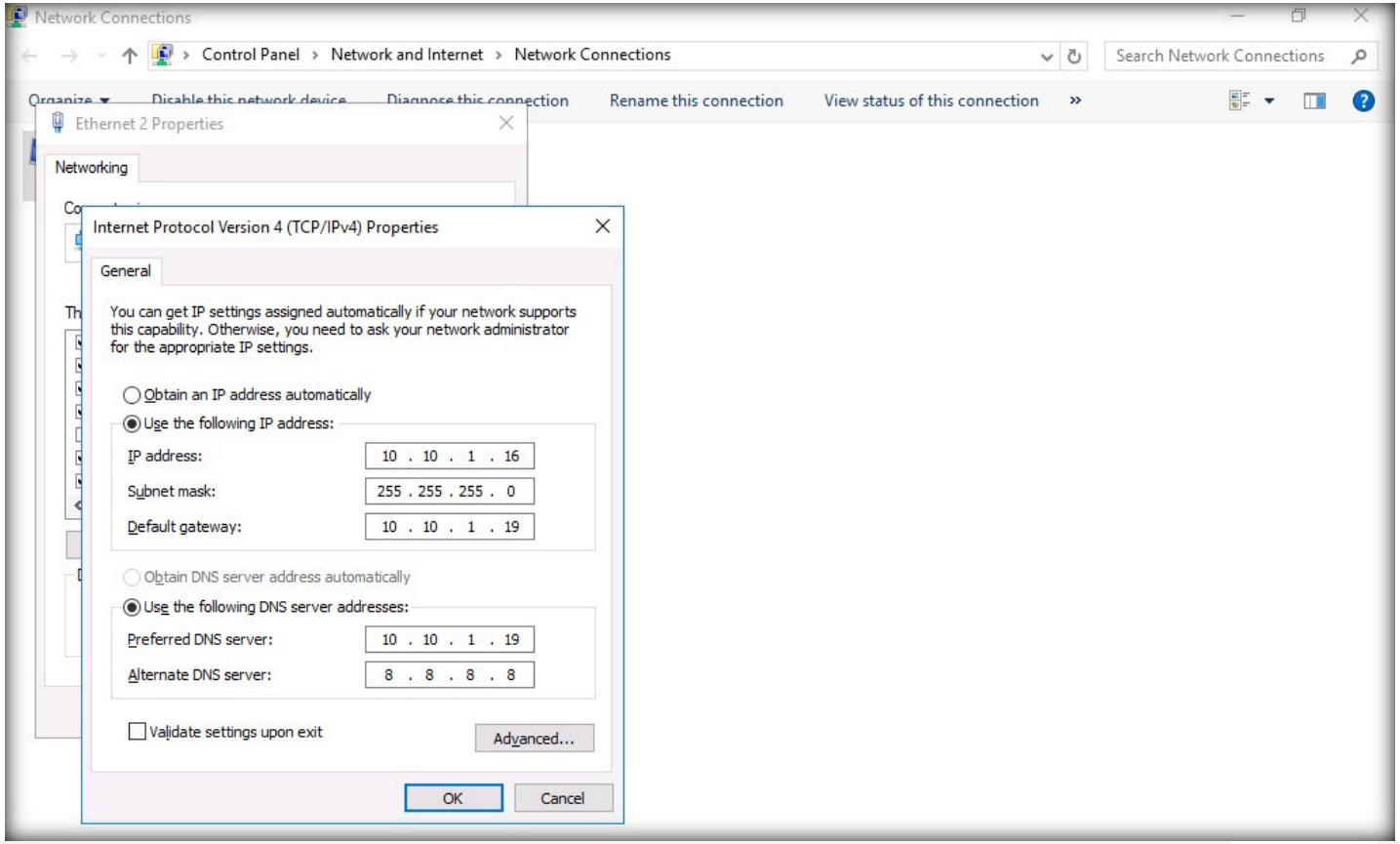
20. The martin S. Properties window opens; click the Account tab. In Account options, check User must change password at next logon and uncheck Password never expires if it is checked. Click Apply and OK.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



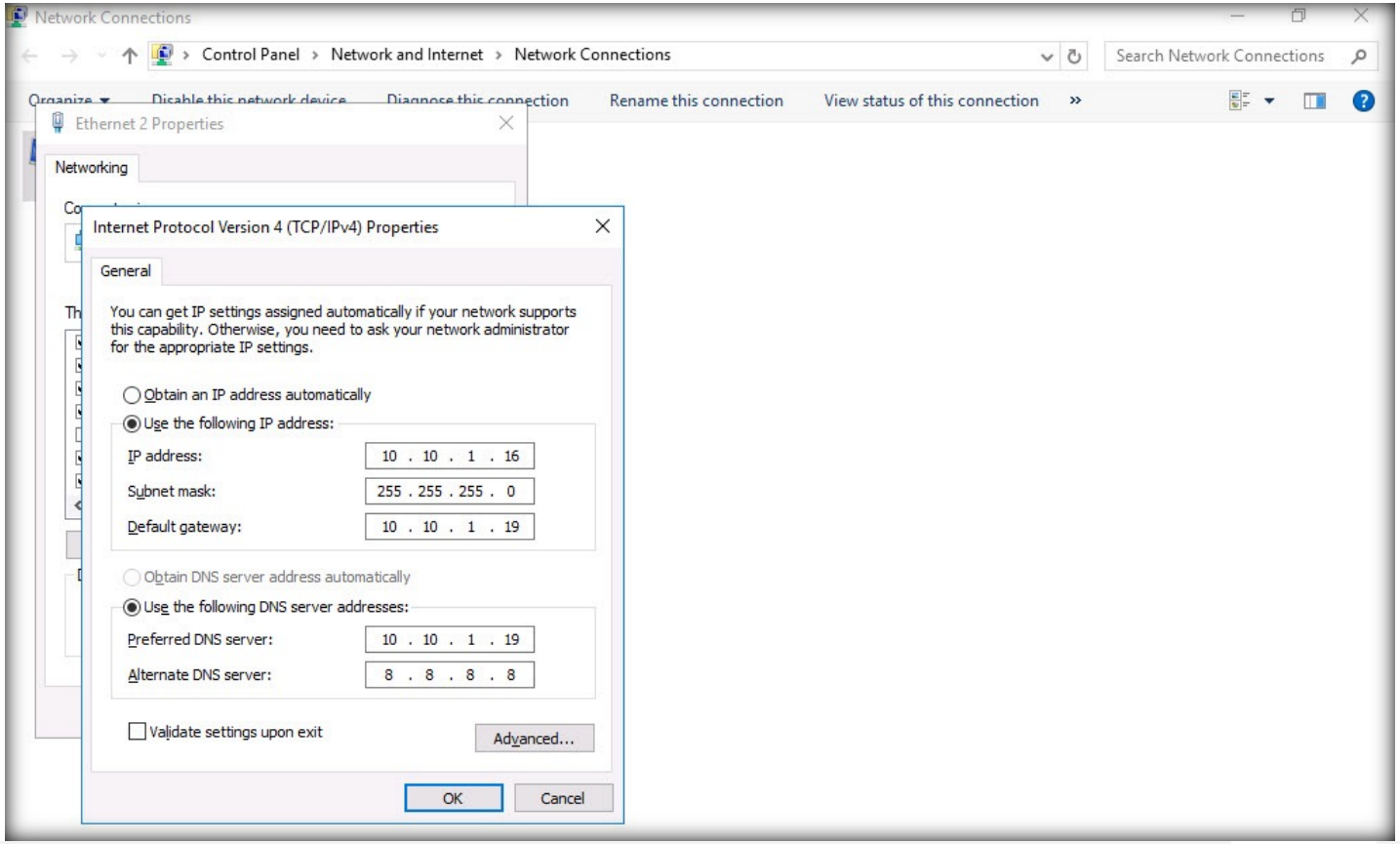
EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

21. Close all open windows.
22. Switch to the Web Server virtual machine.
23. Log in with the credentials Administrator and admin@123.
24. Open a Control Panel window and navigate to Network and Internet → Network and Sharing Center → Change adapter settings. In the Network Connections window, right-click the ethernet adapter (here, Ethernet 2) and select Properties from the drop-down options. Double-click Internet Protocol Version 4 (TCP/IPv4) and change the Default gateway address to 10.10.1.19. Click OK twice. Close the window.



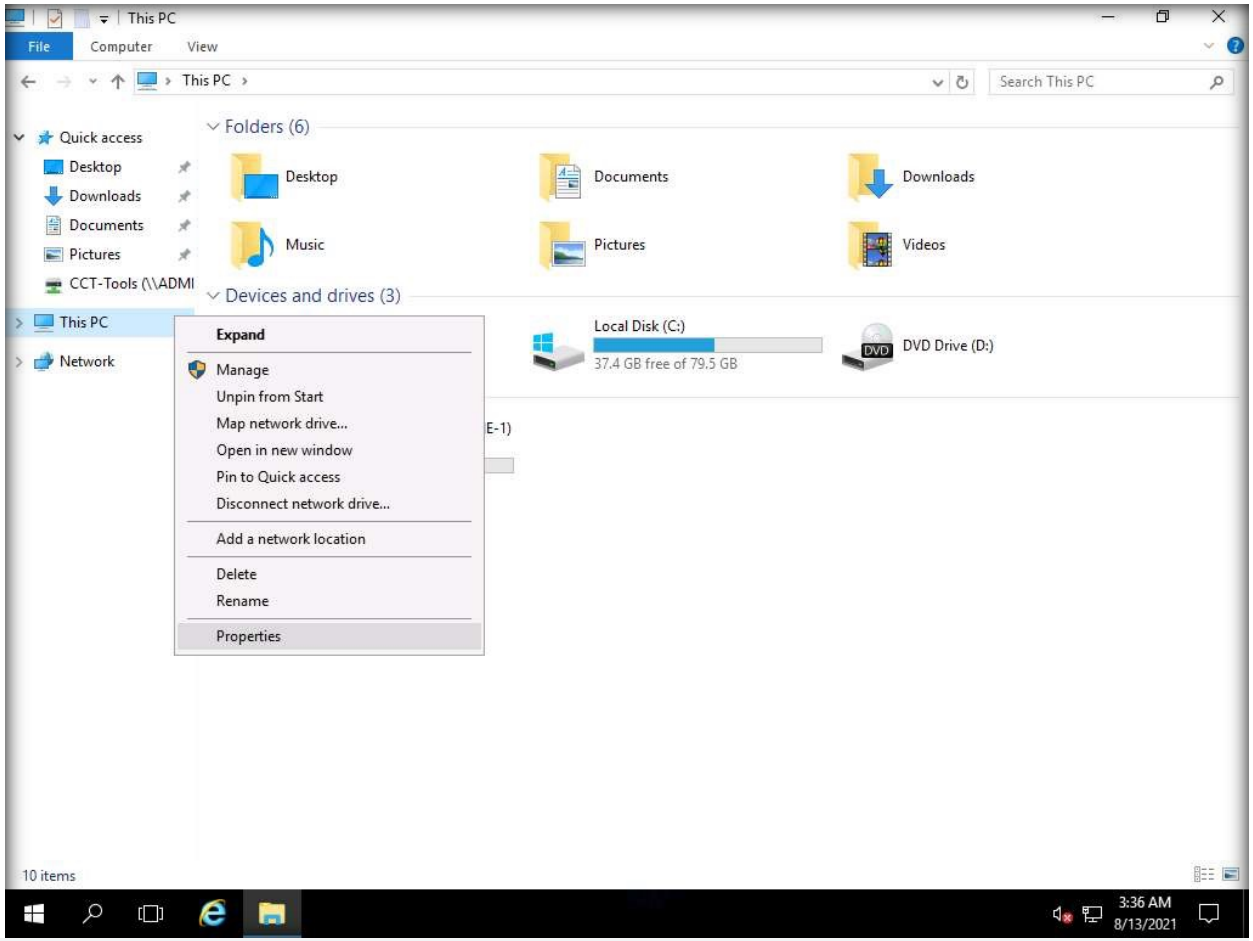
EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

21. Close all open windows.
22. Switch to the Web Server virtual machine.
23. Log in with the credentials Administrator and admin@123.
24. Open a Control Panel window and navigate to Network and Internet → Network and Sharing Center → Change adapter settings. In the Network Connections window, right-click the ethernet adapter (here, Ethernet 2) and select Properties from the drop-down options. Double-click Internet Protocol Version 4 (TCP/IPv4) and change the Default gateway address to 10.10.1.19. Click OK twice. Close the window.



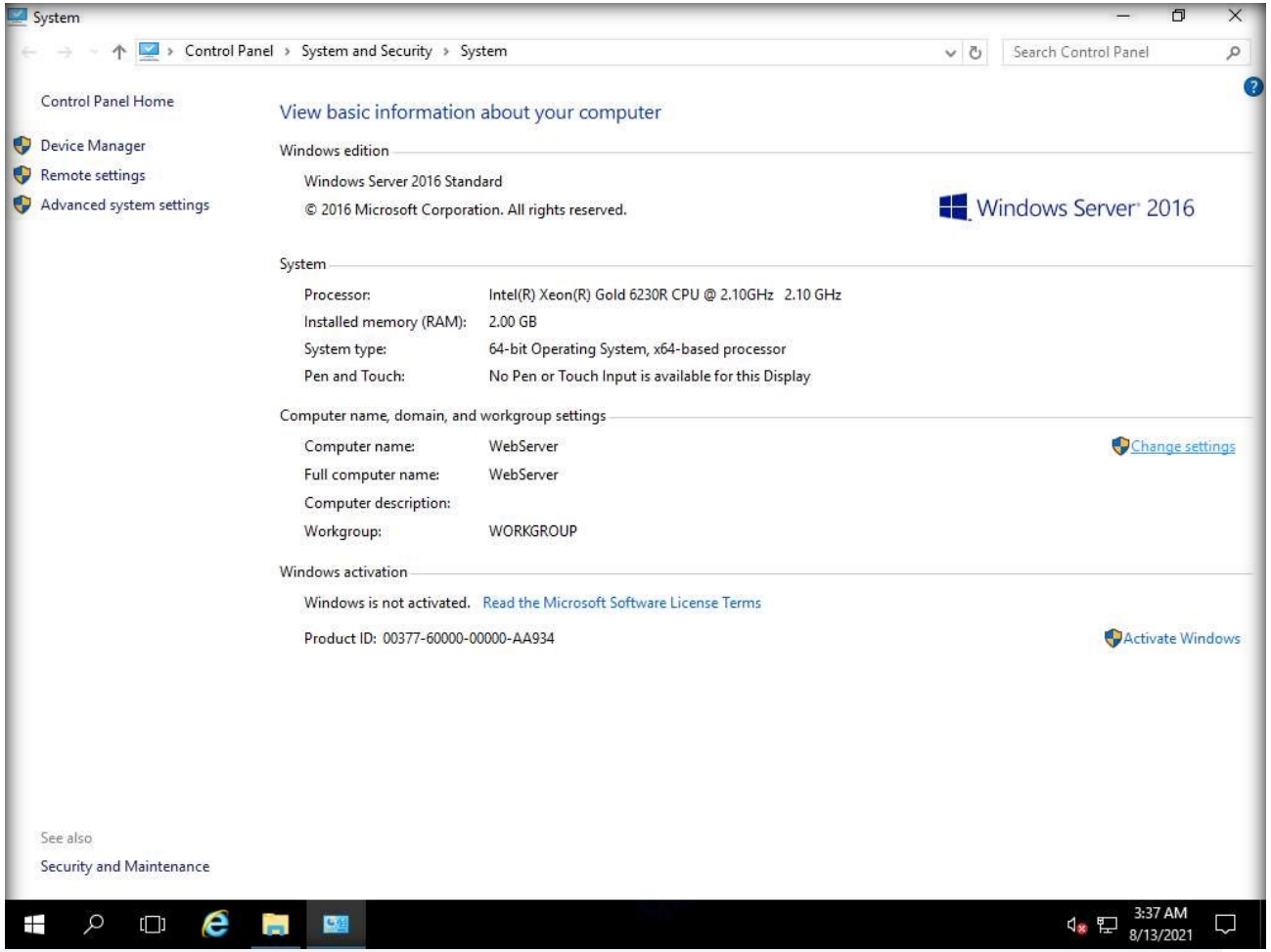
25. Open File Explorer and right-click on This PC, select Properties.
Note: If the Networks window appears, click on Yes.
Note: If the Shutdown Event Tracker pop-up appears, click Cancel.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



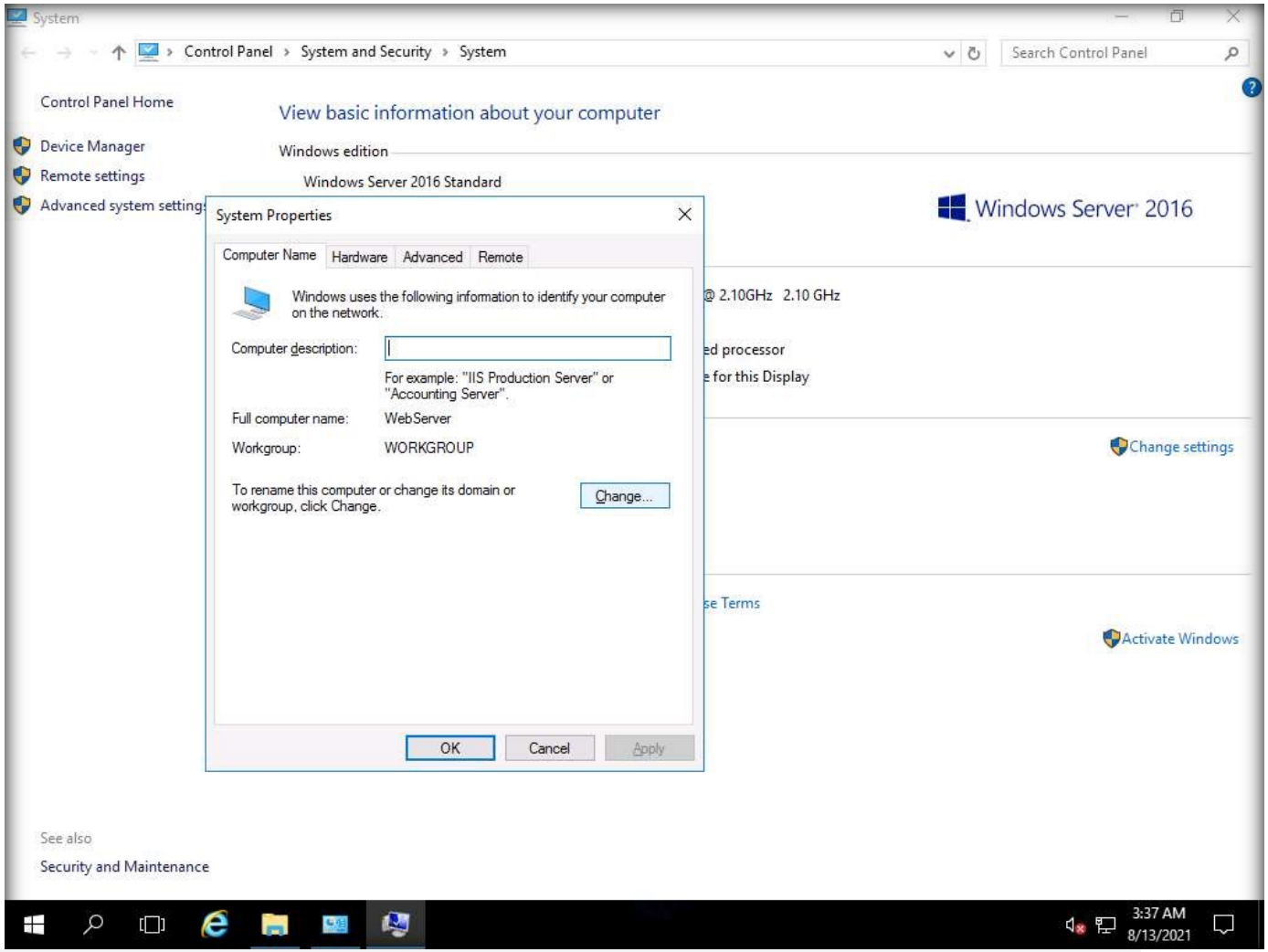
26. The System window opens, click Change settings.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



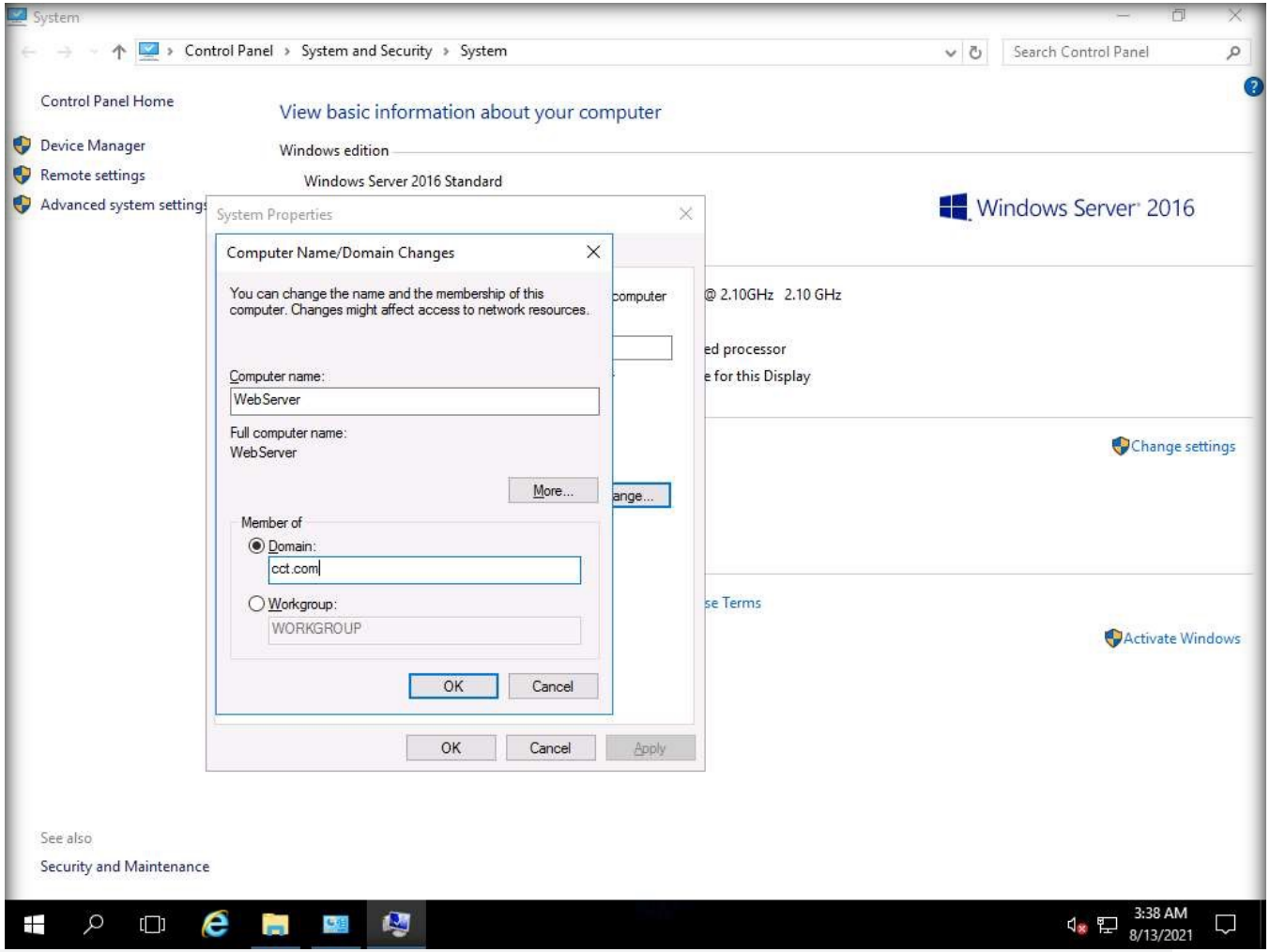
EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

27. The System Properties window opens click Change....



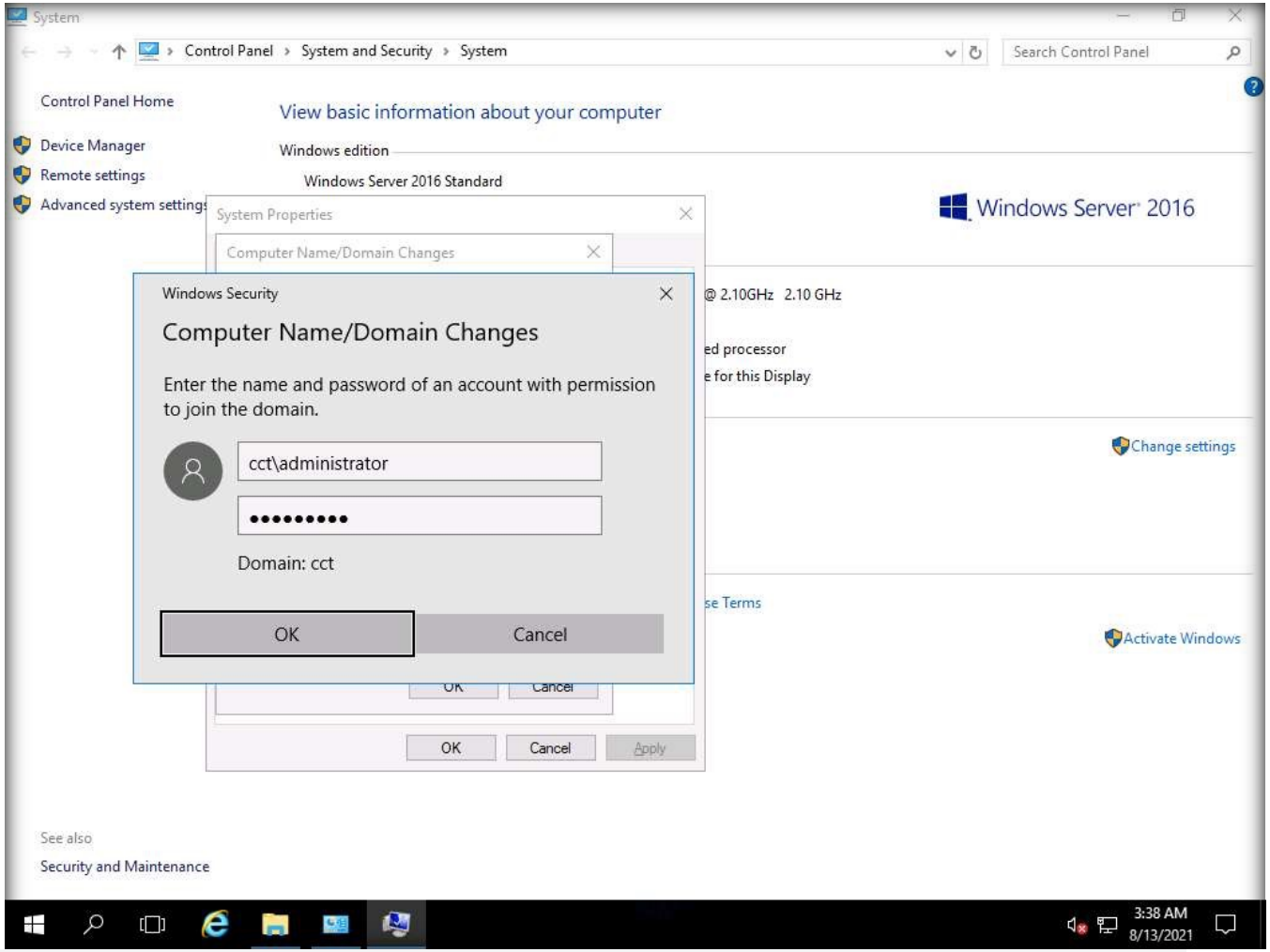
EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

28. The Computer Name/Domain Changes sub-window opens, select the Domain radio button, and type cct.com under the empty text box. Click OK.



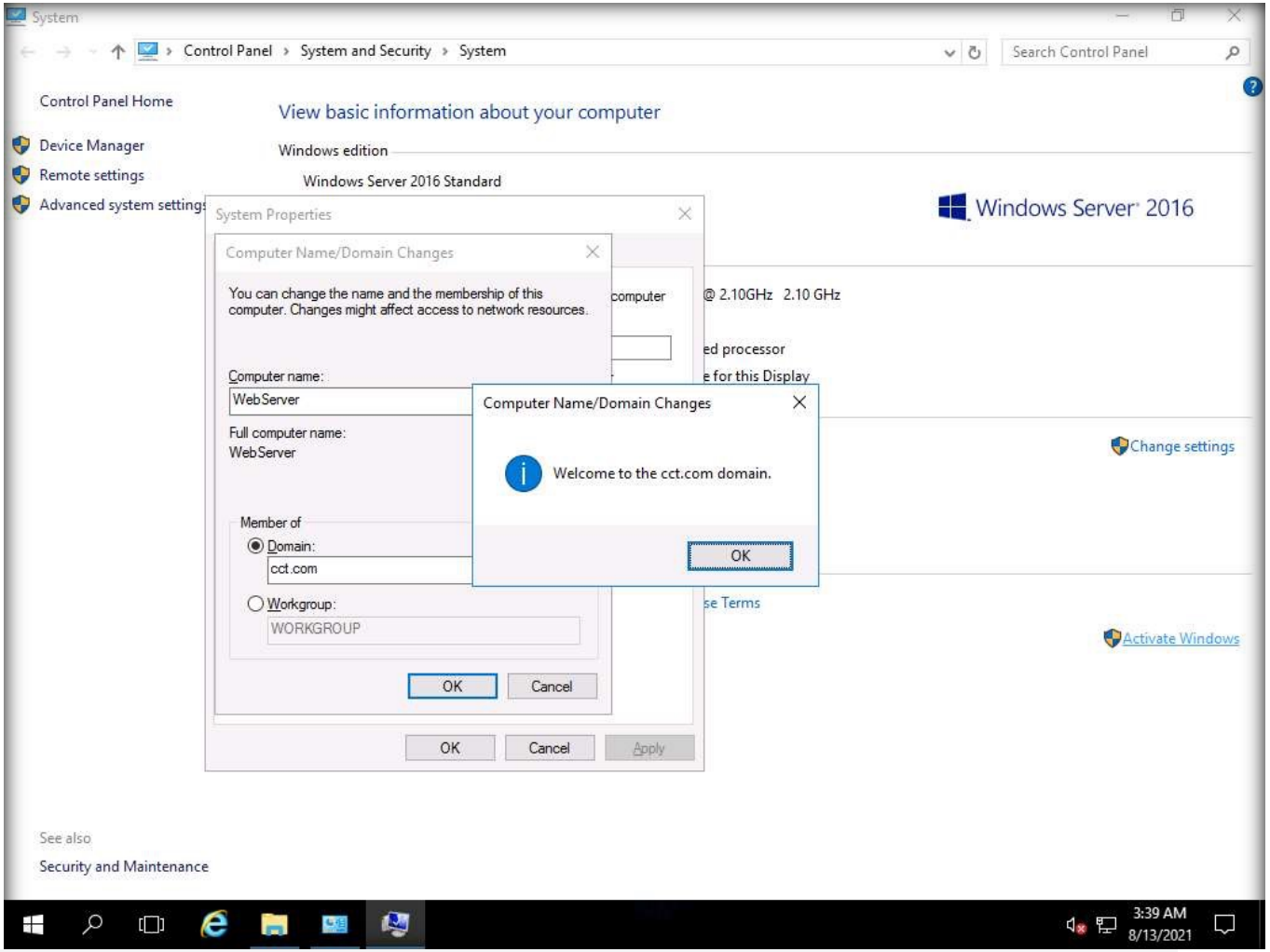
EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

29. The Window Security credential window opens, type the username as cct\administrator and type password as admin@123 respectively and click OK.



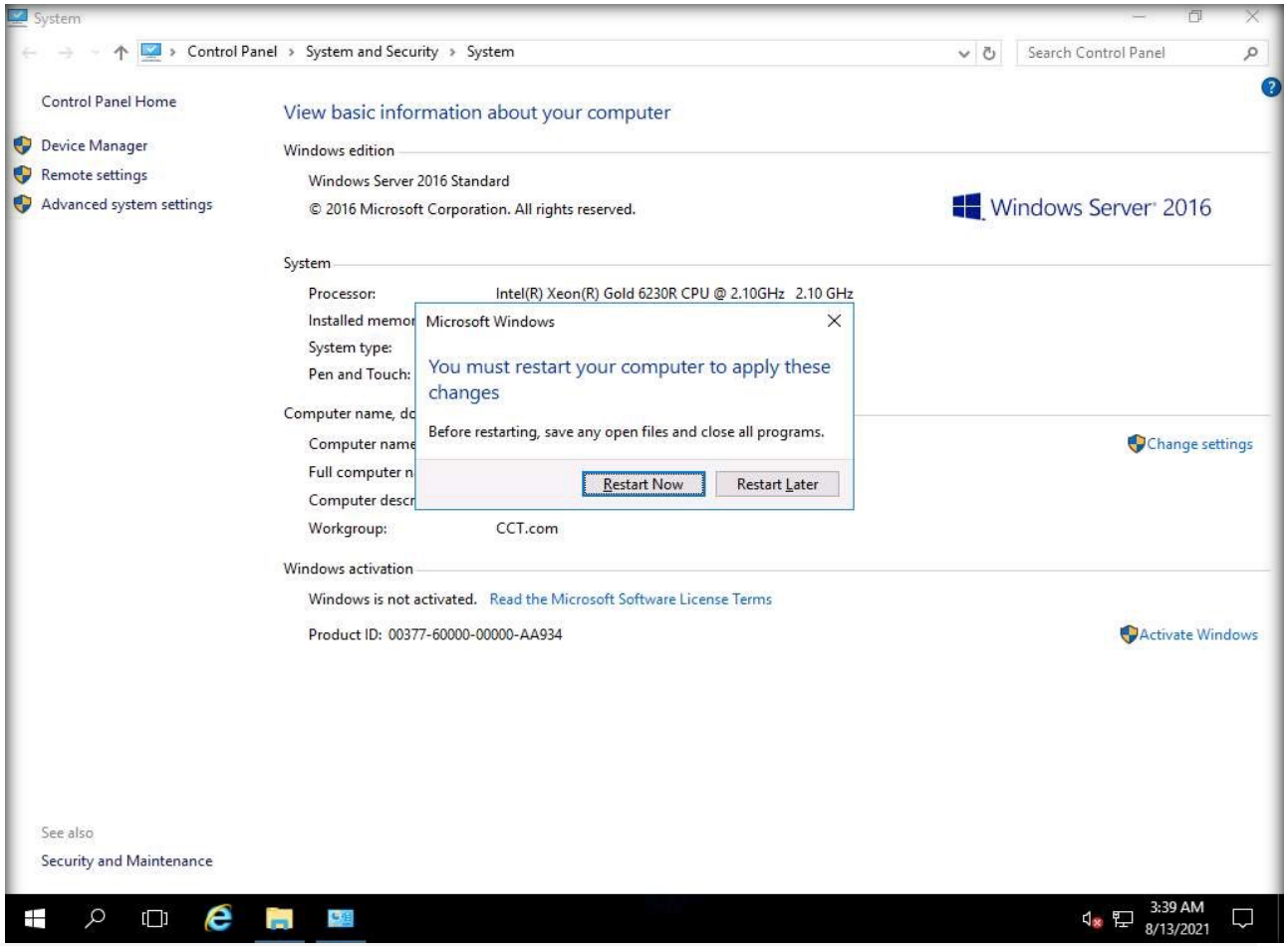
30. Wait for few seconds, the welcome to cct.com pop-up appears, then, click OK.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



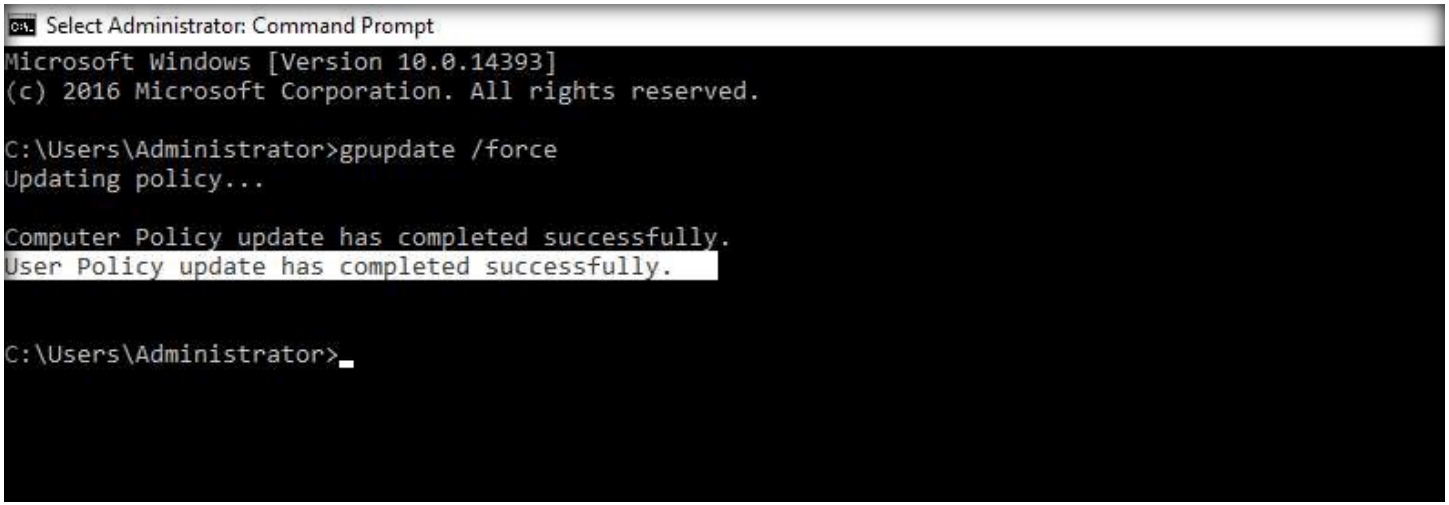
31. The restarting confirmation popup appears, Click OK.
32. You will be diverted back to the System Properties window. Click Close.
33. The Microsoft Windows message box opens, click Restart Now button to restart the system.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



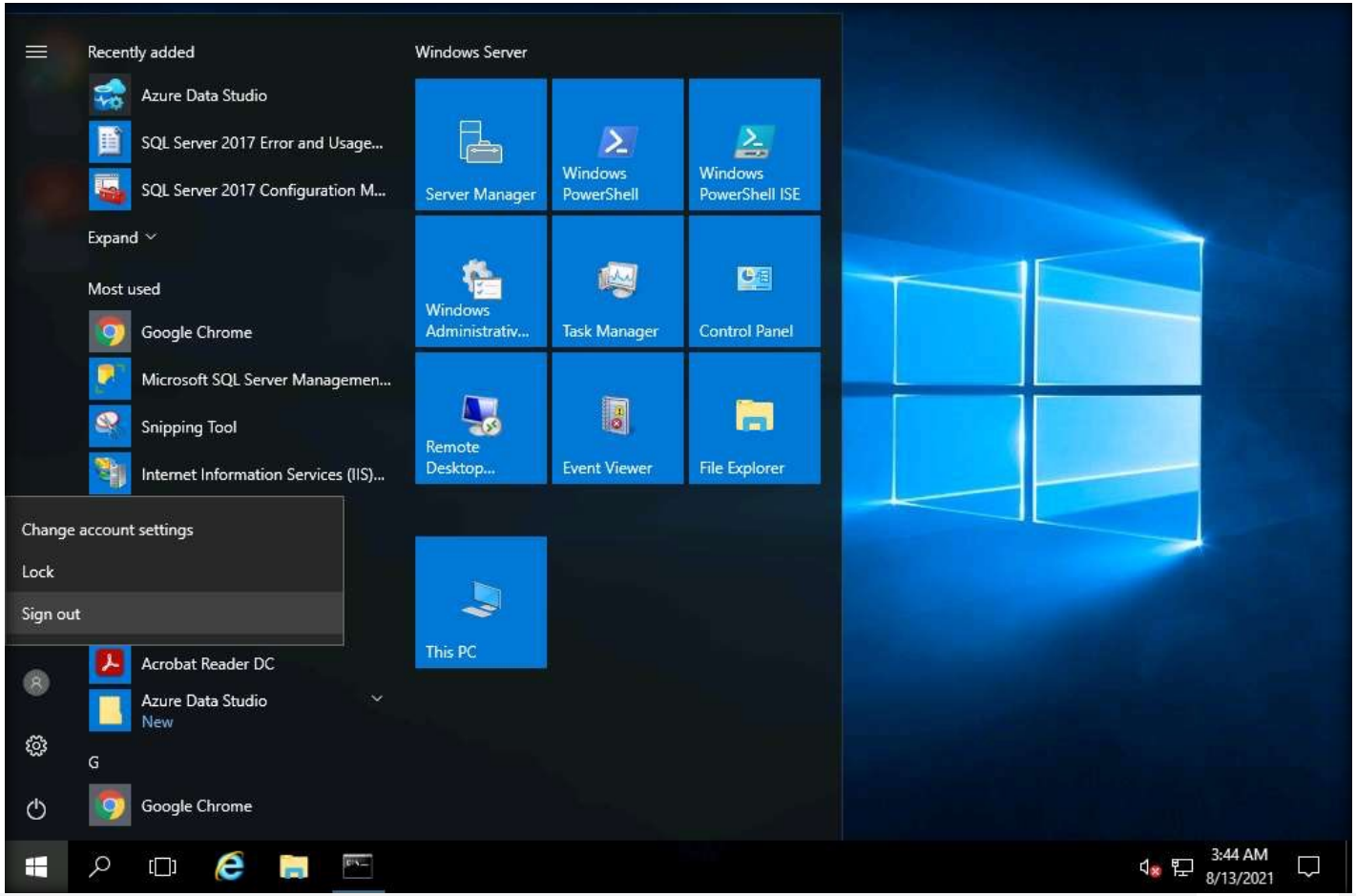
34. The system will restart, login with the credentials Administrator and admin@123.
35. Open Command Prompt and type the command gpupdate /force, press Enter to update the group policy settings.
Note: If you receive any errors while executing the command, then rerun the command.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



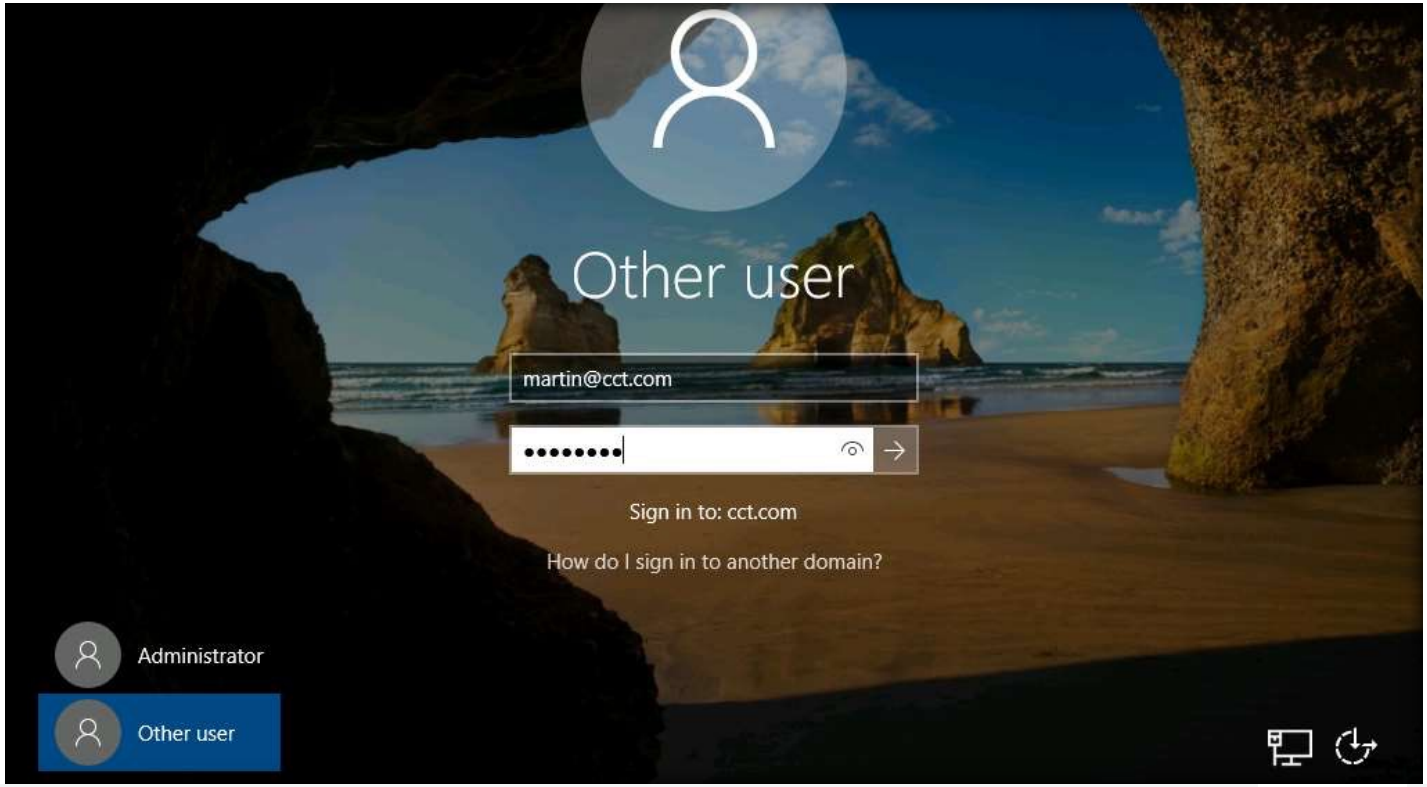
36. Thus, the group policy has been successfully updated; log out from the Administrator account.

EXERCISE 1:
IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



37. To observe the effect of the created GPO, observe user Martin while changing the password to make it more complex and lengthier.
38. Next, select Other user, type the username as martin@cct.com, password as user@123 respectively and press Enter.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

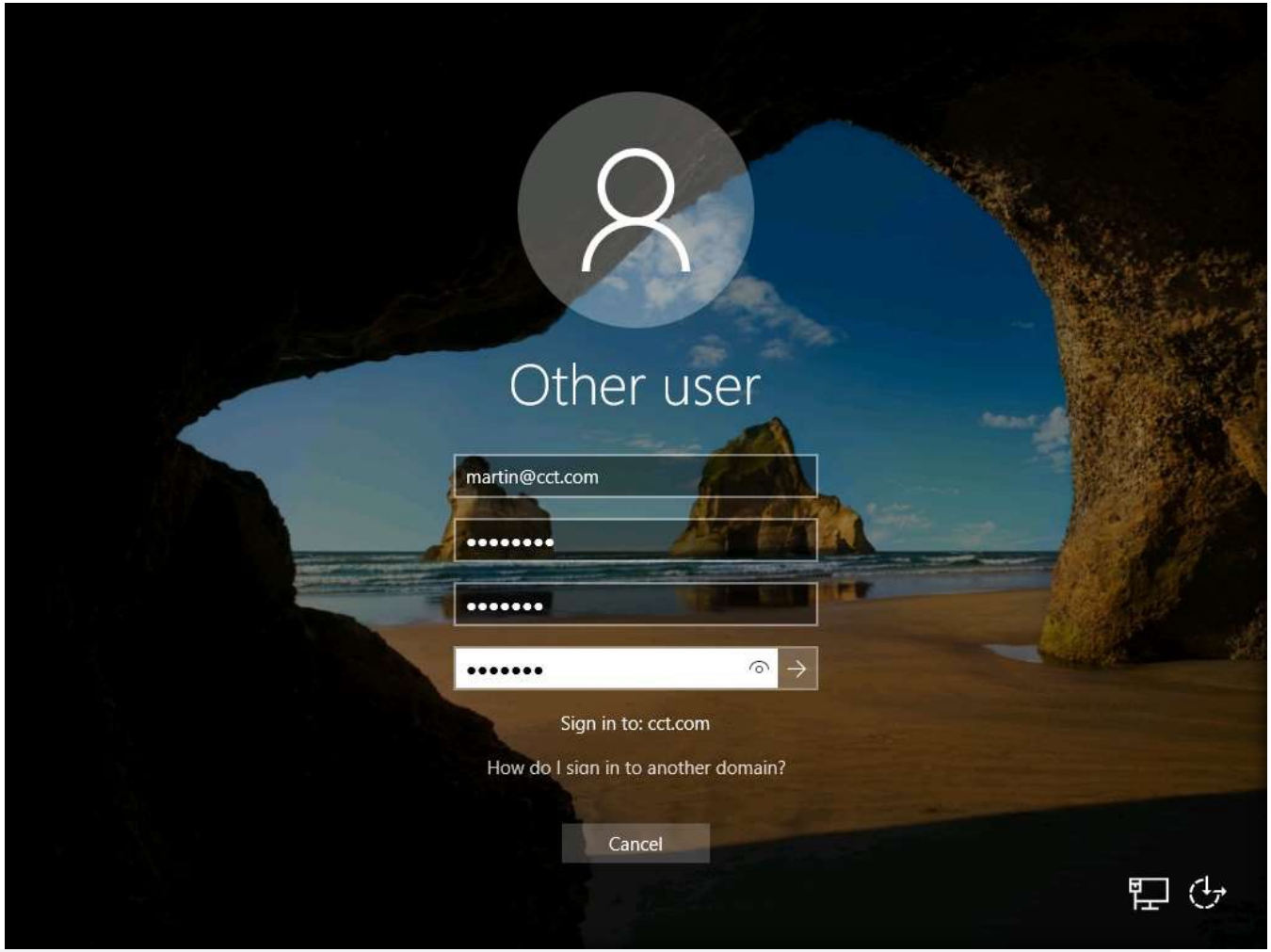


39. Because you have altered the settings of user Martin to change the password at the next login, you will be prompted to change the password as soon as you press Enter; click OK.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

EXERCISE 1:
IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY

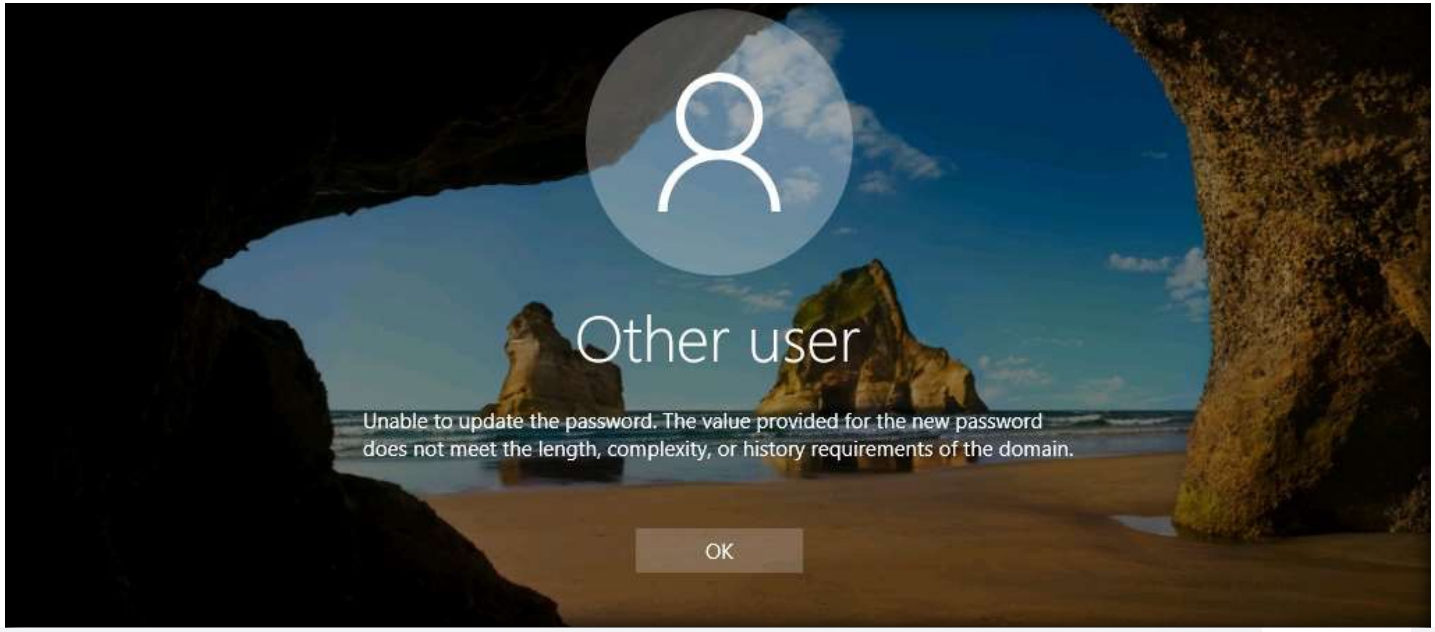
40. Type a simple password such as test123 without special characters as the new password and confirm password, then click the arrow button.



Copyrights @ 2022 EC-Council International Ltd.

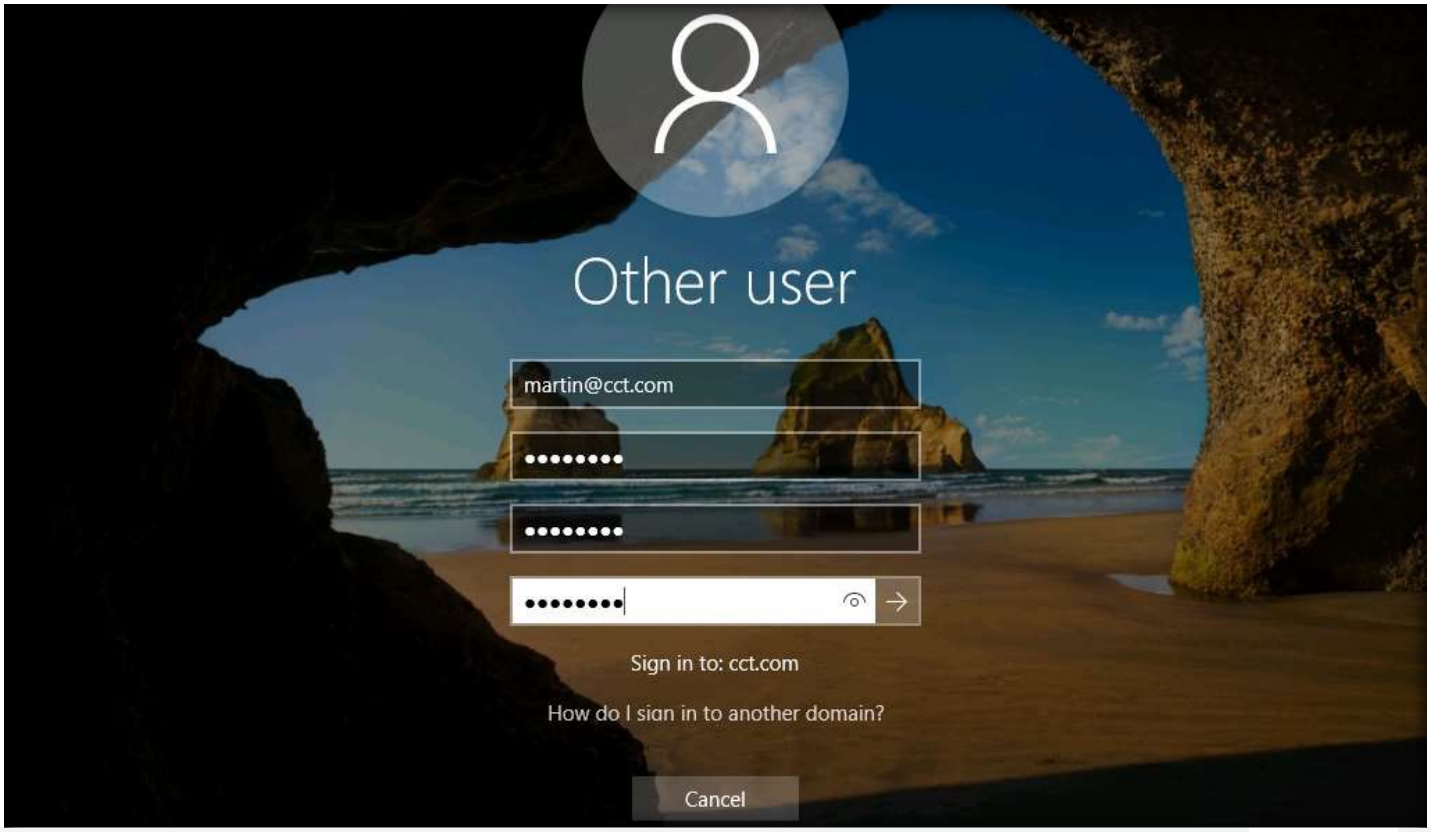
41. The system will prompt Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain. Click OK

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



42. Retype the new password as Test@123. This attempt will be successful because it meets the complexity requirements.
Note: In the Password field, enter user@123.
Note: Log out from Martin account if you are logged in with the new password.
43. Similarly, configure the other password policies according to the organization policies.
44. Close all open windows.
45. Turn off AD Domain Controller and Web Server virtual machines.

EXERCISE 1: IMPLEMENT PASSWORD POLICIES USING WINDOWS GROUP POLICY



EXERCISE 2: **IMPLEMENT AUDITING POLICIES**

The account audit policy defines the types of user actions or events to be recorded in the security logs.

LAB SCENARIO

A security professional must know how to audit system policies. In this exercise, we will find how to run processes and Group Policy Objects that are designed in the system and further configure auditing policies using GPOs.

OBJECTIVE

This lab demonstrates how to implement and configure auditing policies in a system.

OVERVIEW OF AUDIT POLICY

It is important for organizations to create an efficient and effective account audit policy to monitor and identify potential security issues beforehand, ensure accountability, and provide evidence in case of data breach. Each organization must take appropriate decision related to the threats they face, risk tolerance factor, and design relevant audit policy that best suits their security needs.

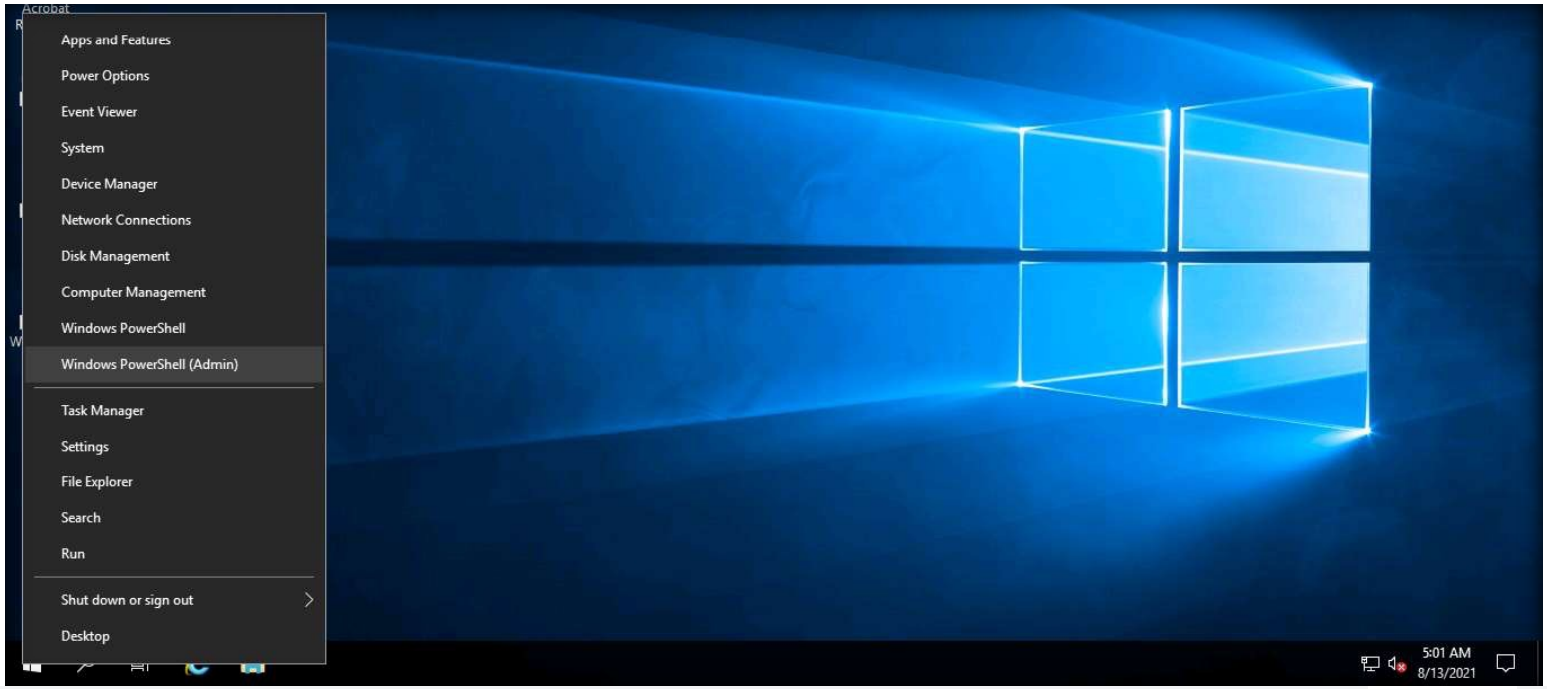
Design Considerations

- Decide how to collect, store, and analyze audit data.
- Test the audit policy before deploying it in the production environment
- Consider the amount of storage required to store the audit data
- Decide the types of events you want to audit such as account sign in, access to directory services, system changes and process tracking.

Copyrights @ 2022 EC-Council International Ltd.

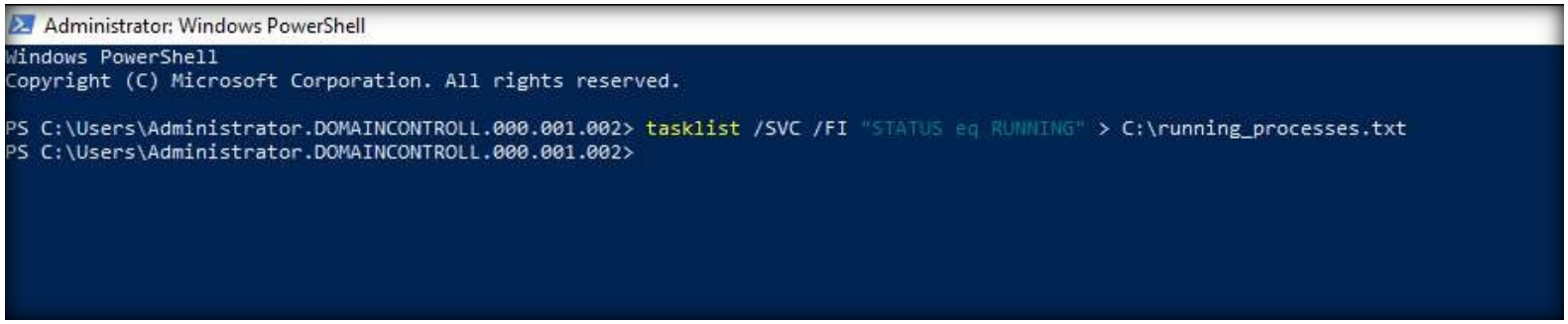
Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on the AD Domain Controller virtual machine.
2. Login with the credentials CCT\Administrator and admin@123.
Note: The network screen appears, click Yes.
3. Right-click the Start icon present at the left-bottom of the Desktop. Select Windows PowerShell (Admin) option.
Note: If User Account Control pop-up appears, click Yes.

EXERCISE 2: IMPLEMENT AUDITING POLICIES



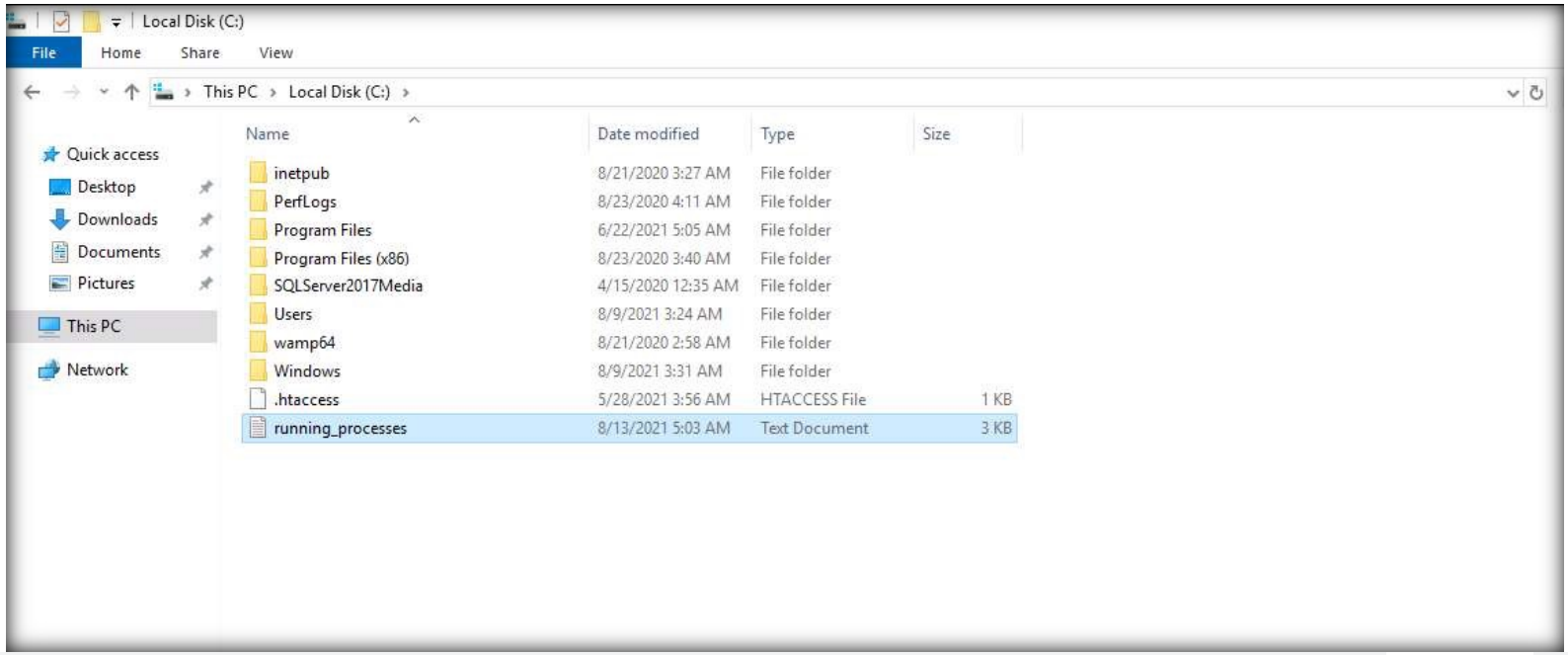
4. The Administrator: Windows PowerShell window appears, type tasklist /SVC /FI “STATUS eq RUNNING” > C:\running_processes.txt and press Enter. This command fetches a list of processes running in the system and writes the output to a file (running_processes.txt) saved in C: drive.

EXERCISE 2:
IMPLEMENT
AUDITING POLICIES



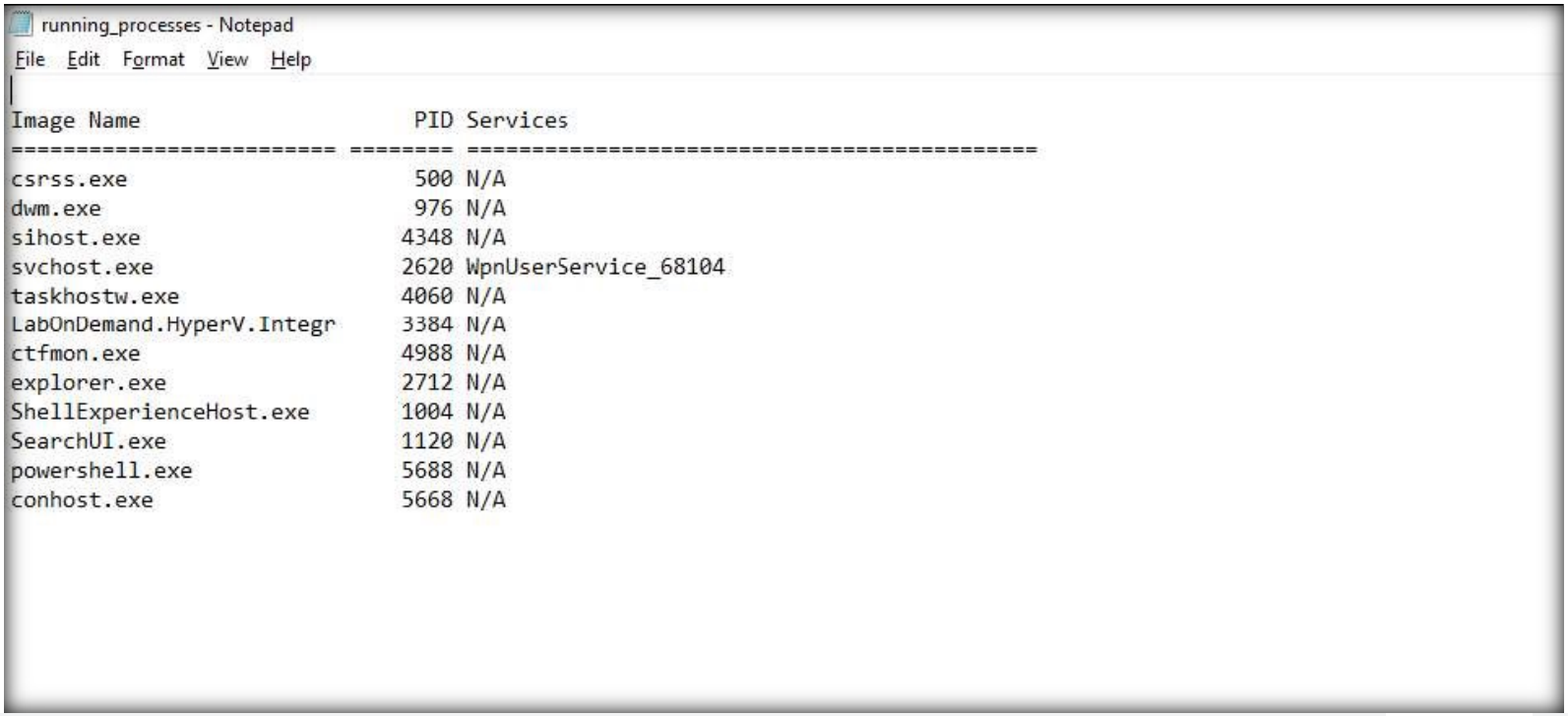
5. Open the File Explorer window, navigate to Local Disk (C:) and a text file (running_processes.txt) has been created here.

EXERCISE 2: IMPLEMENT AUDITING POLICIES



6. Double-click the running_processes.txt file to view its content.
7. A text file with a list of processes running in the system is displayed along with their values such as PID and Services, as shown in the screenshot.
Note: The list of running processes might differ while you are performing this lab task.

EXERCISE 2: IMPLEMENT AUDITING POLICIES

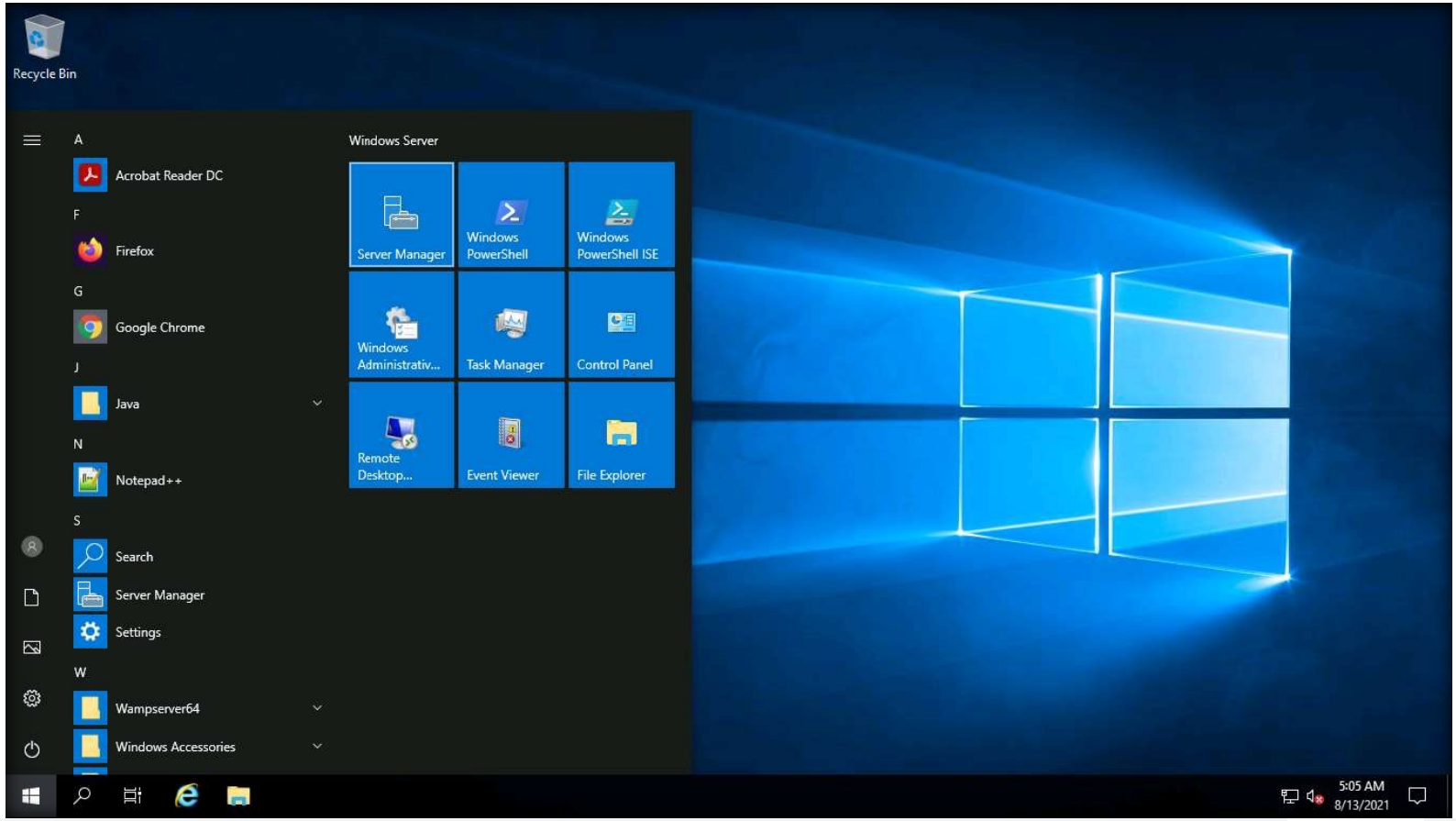



```
Image Name                     PID Services
========================= ======== ============================================
csrss.exe                      500 N/A
dwm.exe                        976 N/A
sihost.exe                    4348 N/A
svchost.exe                   2620 WpnUserService_68104
taskhostw.exe                 4060 N/A
LabOnDemand.HyperV.Integr     3384 N/A
ctfmon.exe                    4988 N/A
explorer.exe                  2712 N/A
ShellExperienceHost.exe       1004 N/A
SearchUI.exe                  1120 N/A
powershell.exe                5688 N/A
conhost.exe                   5668 N/A
```

Copyrights @ 2022 EC-Council International Ltd.

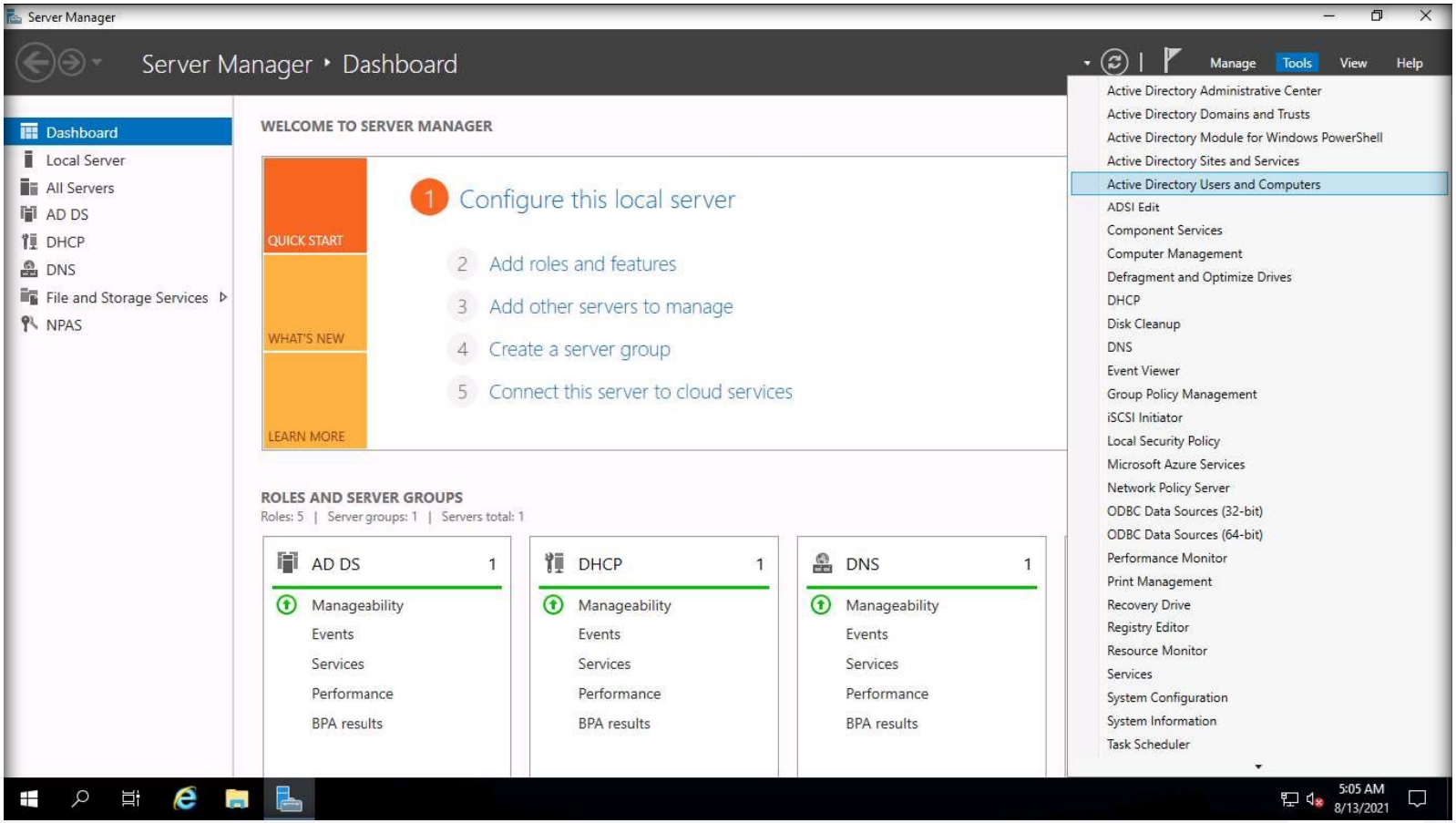
EXERCISE 2: IMPLEMENT AUDITING POLICIES

8. Close all open windows.
9. Now, we will configure NTFS permissions on a account named Bob.
Note: NTFS files and folder permissions allow users to access files stored on the local computer and those access files stored in a shared folder over the network. NTFS also enables sharing permissions in shared folders in accordance with file and folder permissions.
10. Click Start icon and select Server Manager.



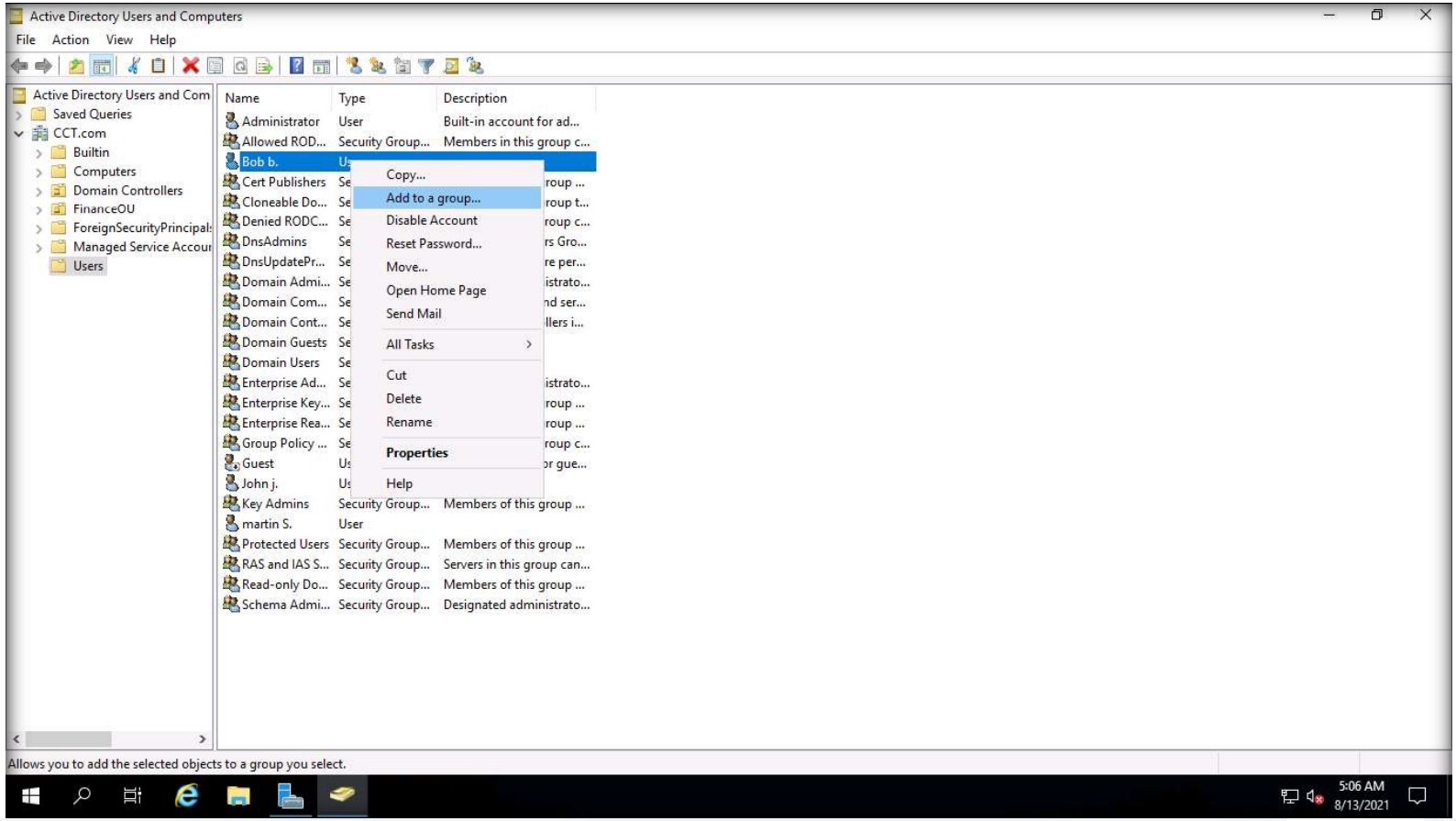
EXERCISE 2: IMPLEMENT AUDITING POLICIES

11. The Server Manager window appears. Click Tools and select the Active Directory Users and Computers option.



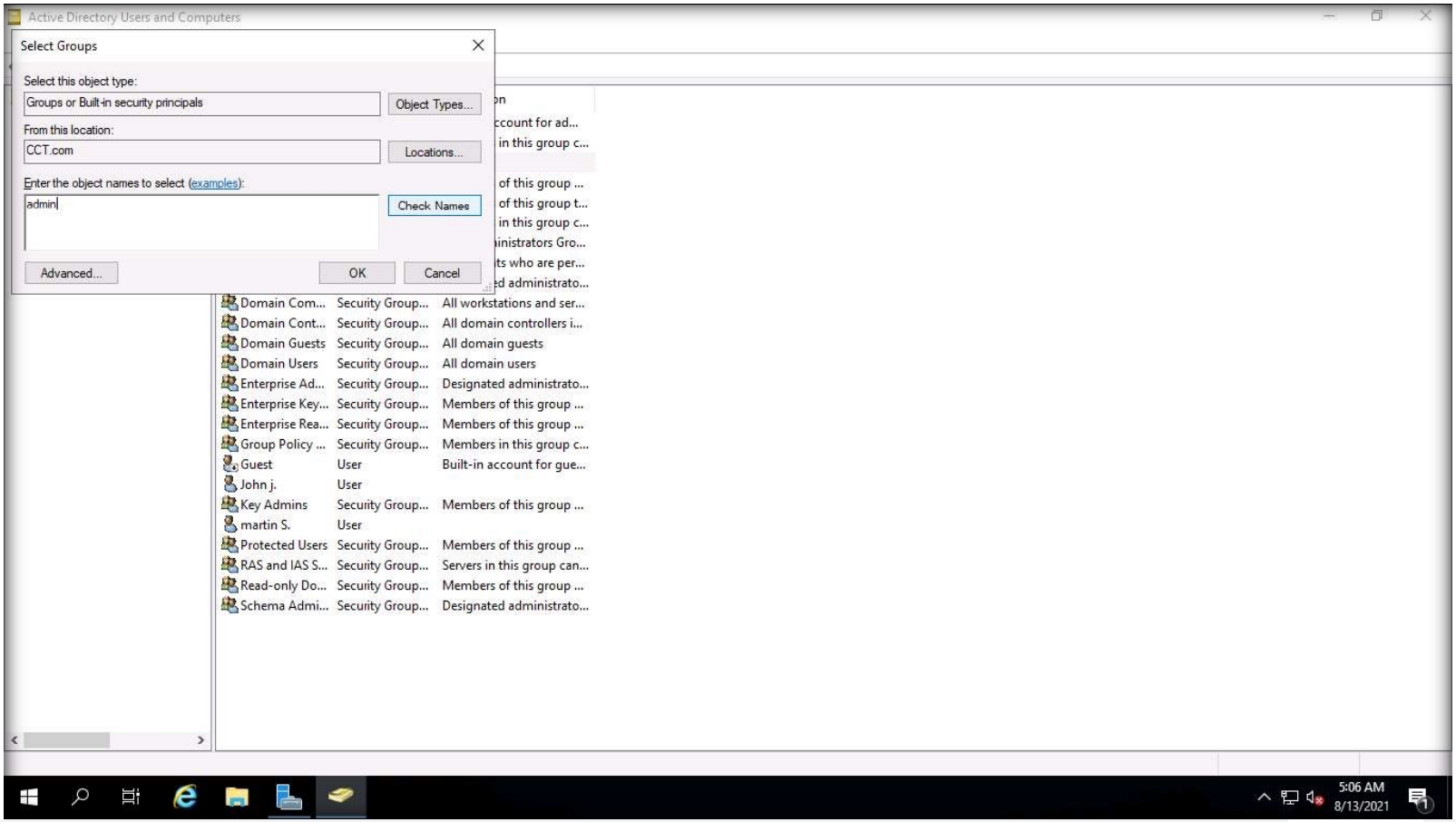
12. Click and select the Users node, right-click Bob b. user and select Add to a group....

EXERCISE 2:
IMPLEMENT
AUDITING POLICIES



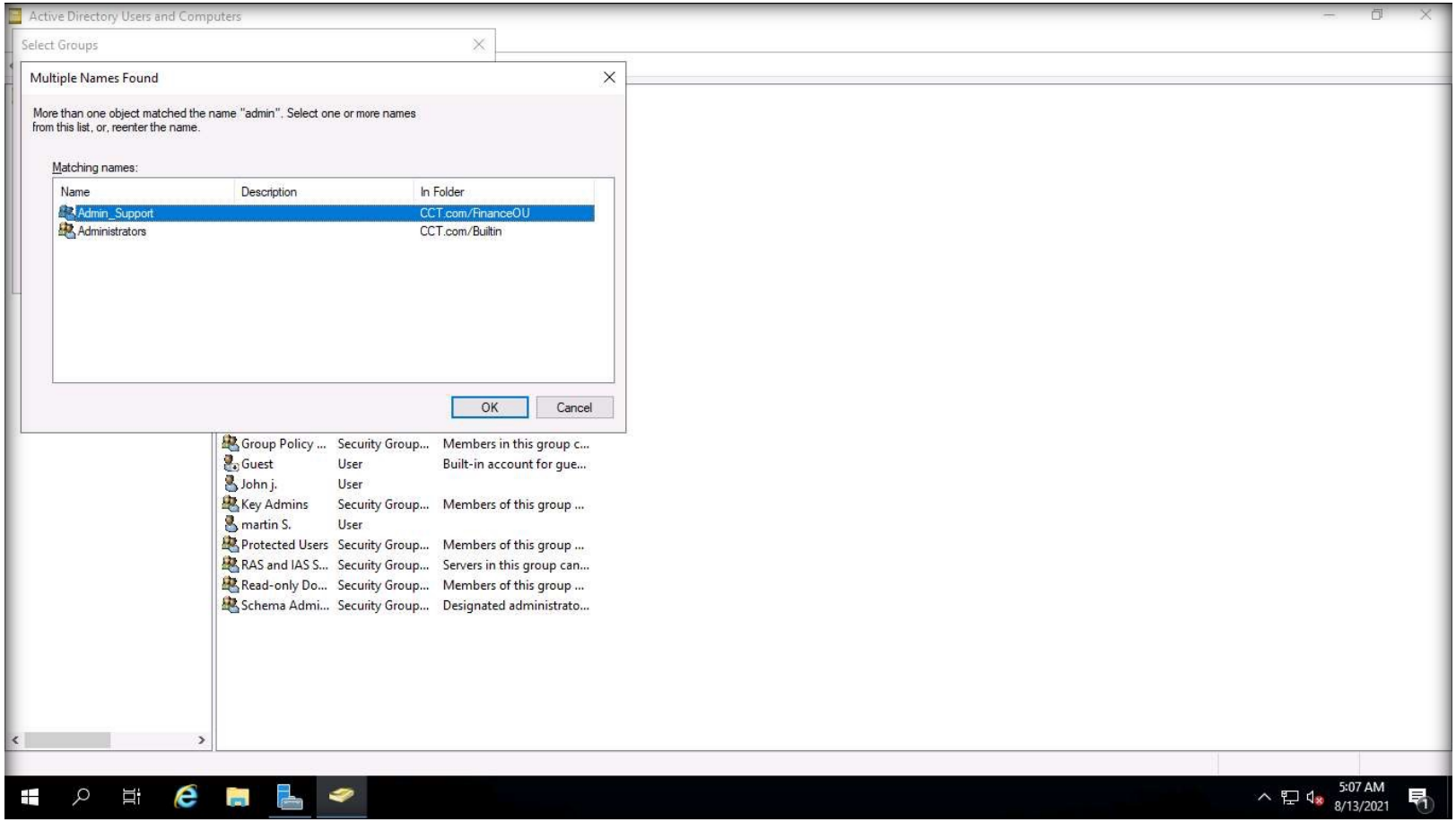
EXERCISE 2:
IMPLEMENT AUDITING POLICIES

13. A Select Groups window appears, in the Enter the object names to select field, type admin and click Check Names button.



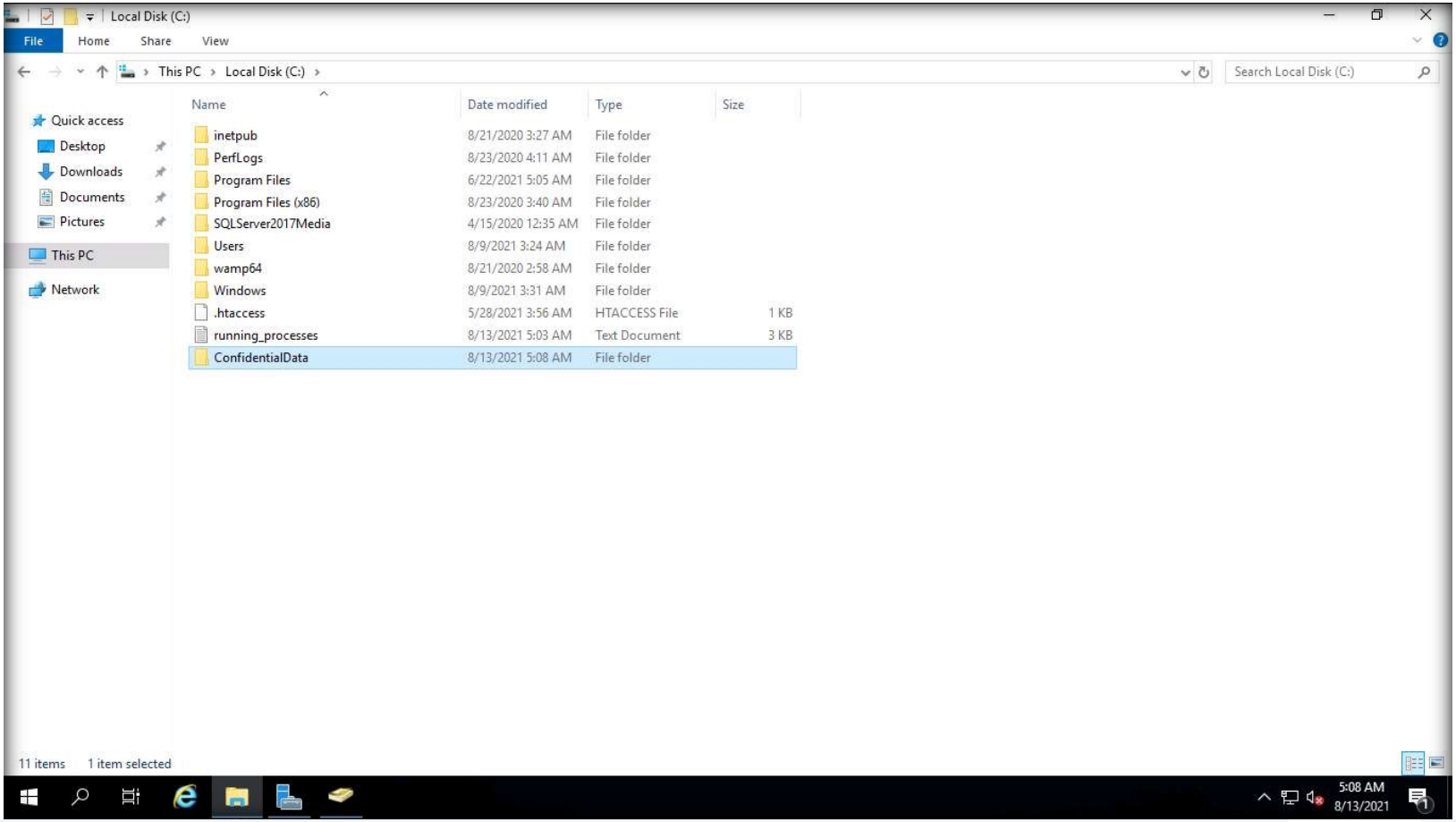
EXERCISE 2: IMPLEMENT AUDITING POLICIES

14. In the Multiple Names Found window, select the Admin_Support group and click OK.



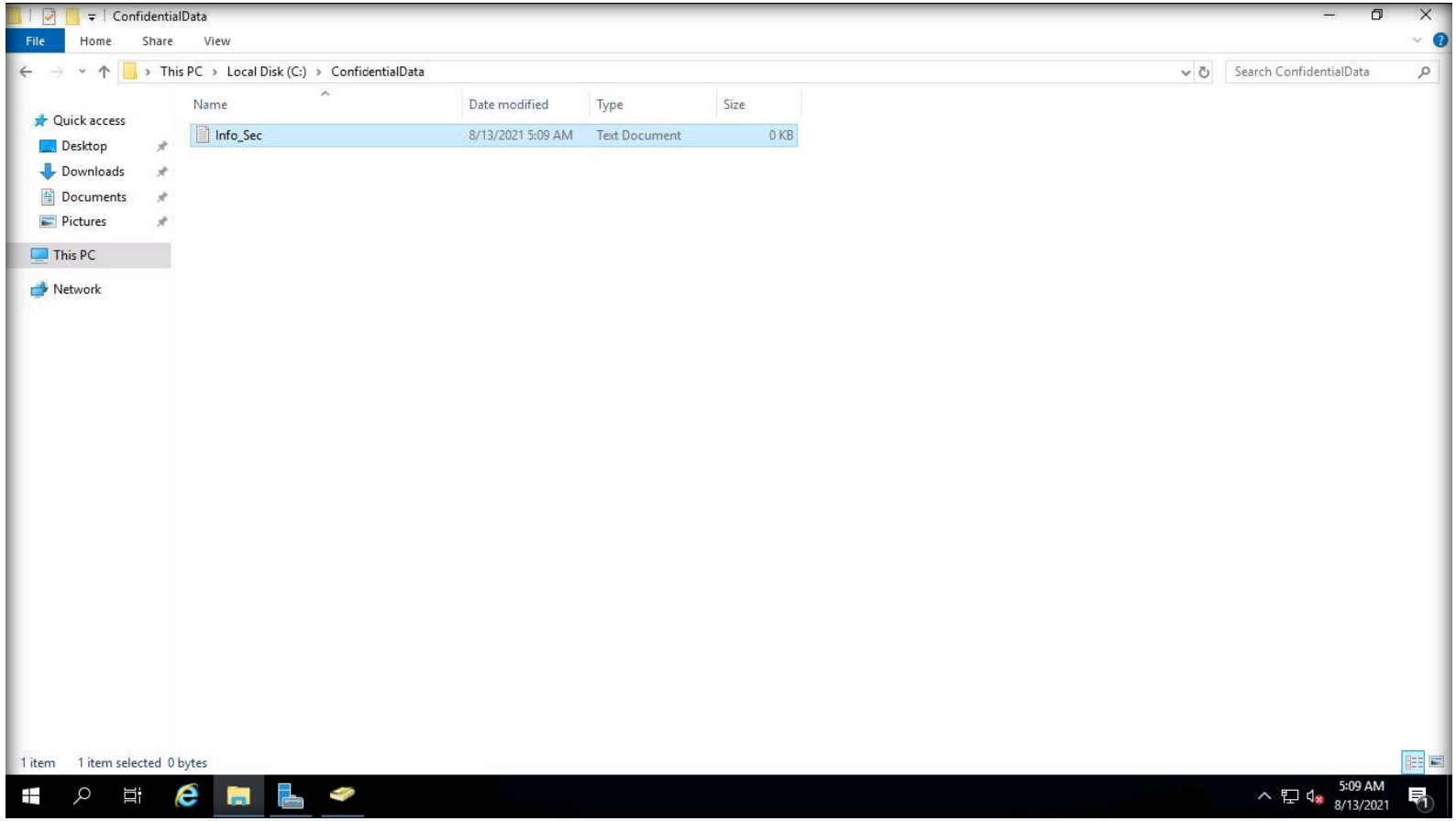
EXERCISE 2: IMPLEMENT AUDITING POLICIES

15. In the Select Groups window, click OK.
16. In the Active Directory Domain Services pop-up, click OK.
17. Minimize the Active Directory Users and Computers window
18. Open the File Explorer window, navigate to Local Disk (C:) and create a folder named ConfidentialData.



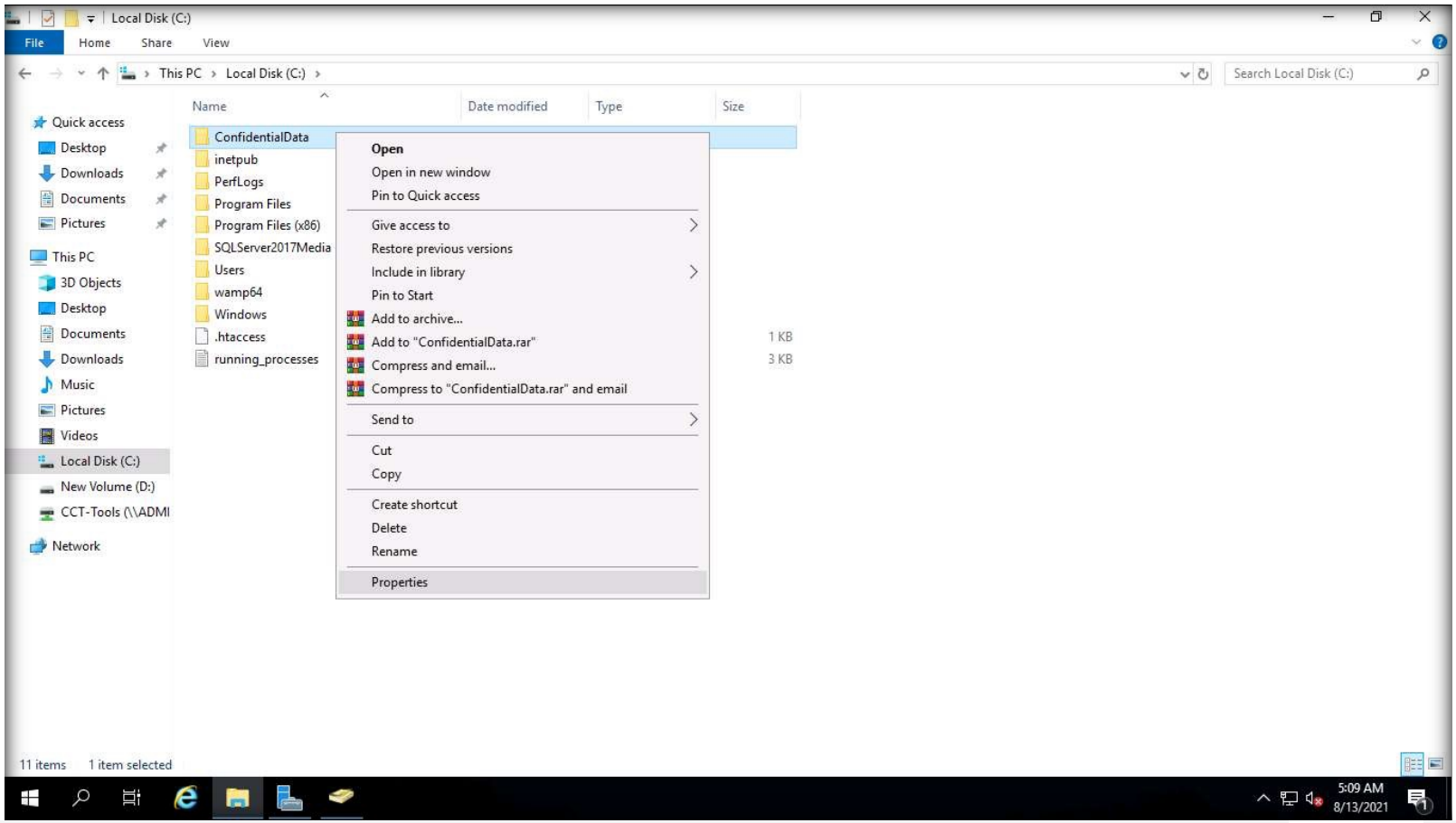
19. Double-click to open the ConfidentialData folder. Create a text file (Notepad file) and name it as Info_Sec and press Enter.
Note: To create a text file, right-click inside the folder and navigate to New → Text Document.

EXERCISE 2: IMPLEMENT AUDITING POLICIES



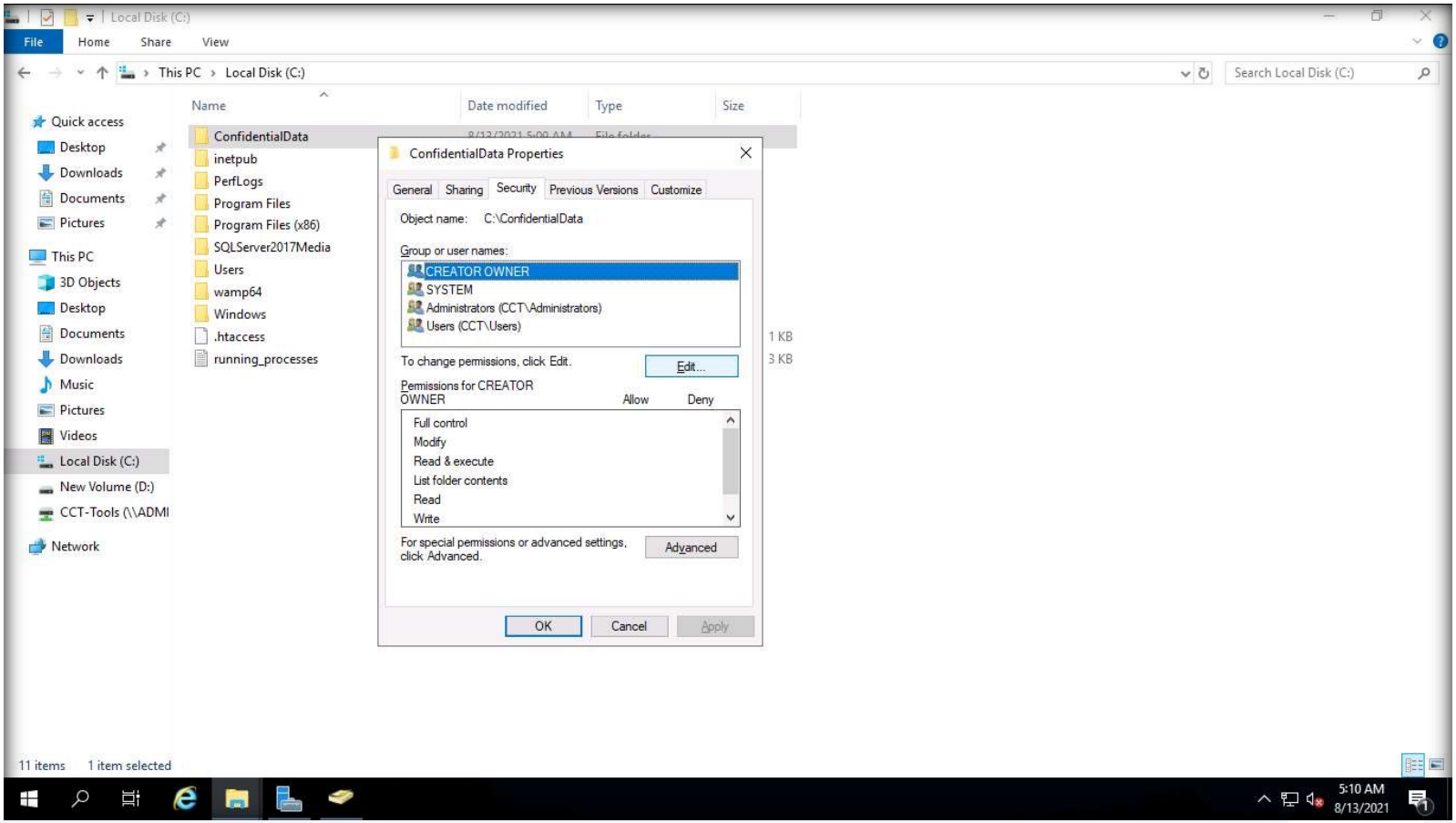
EXERCISE 2: IMPLEMENT AUDITING POLICIES

20. Now, navigate back to the ConfidentialData folder, and right-click on it and select Properties.



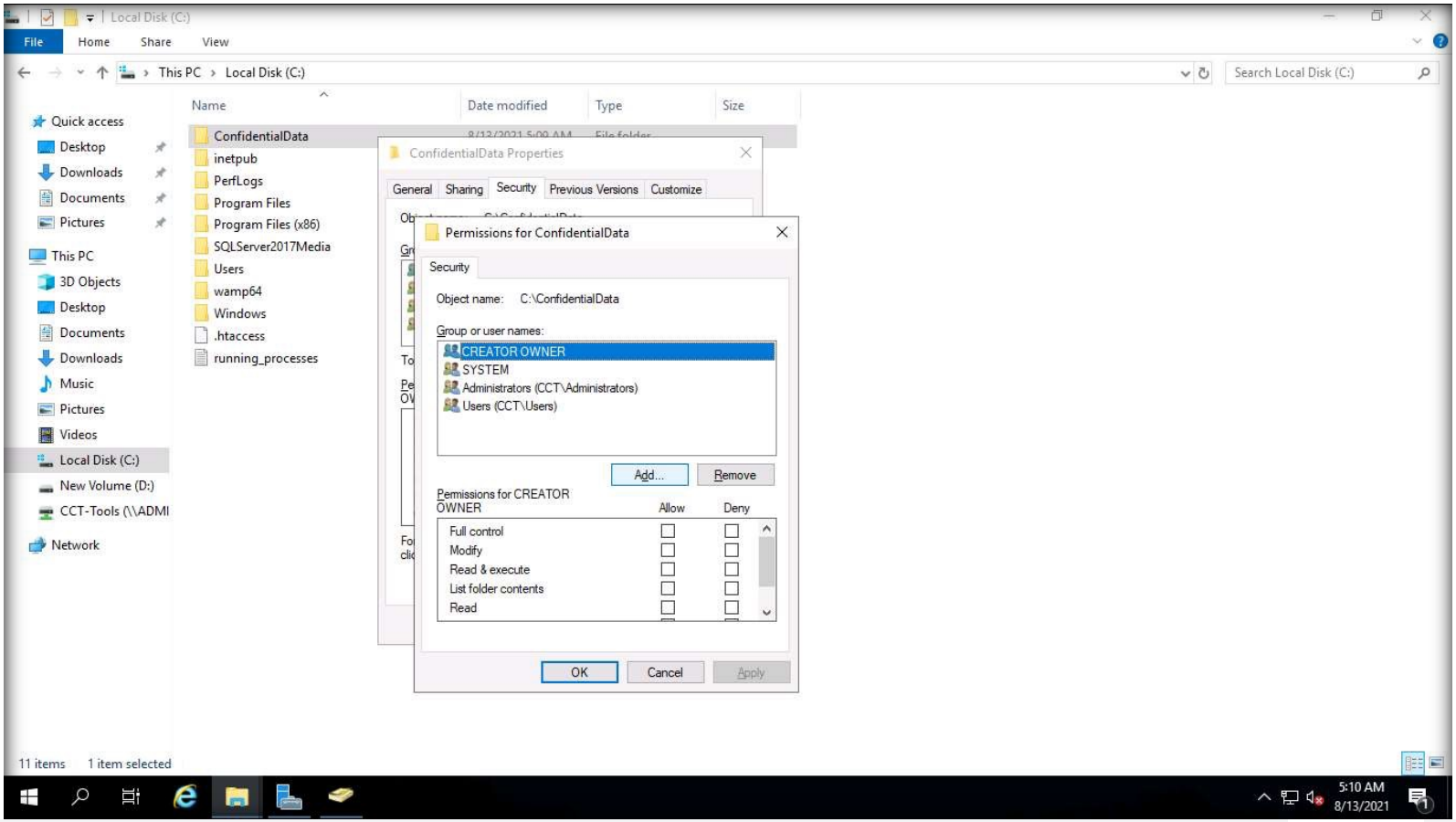
EXERCISE 2: IMPLEMENT AUDITING POLICIES

21. A ConfidentialData Properties window appears, navigate to the Security tab.
22. In the Security tab, click Edit button under to change folder permissions.



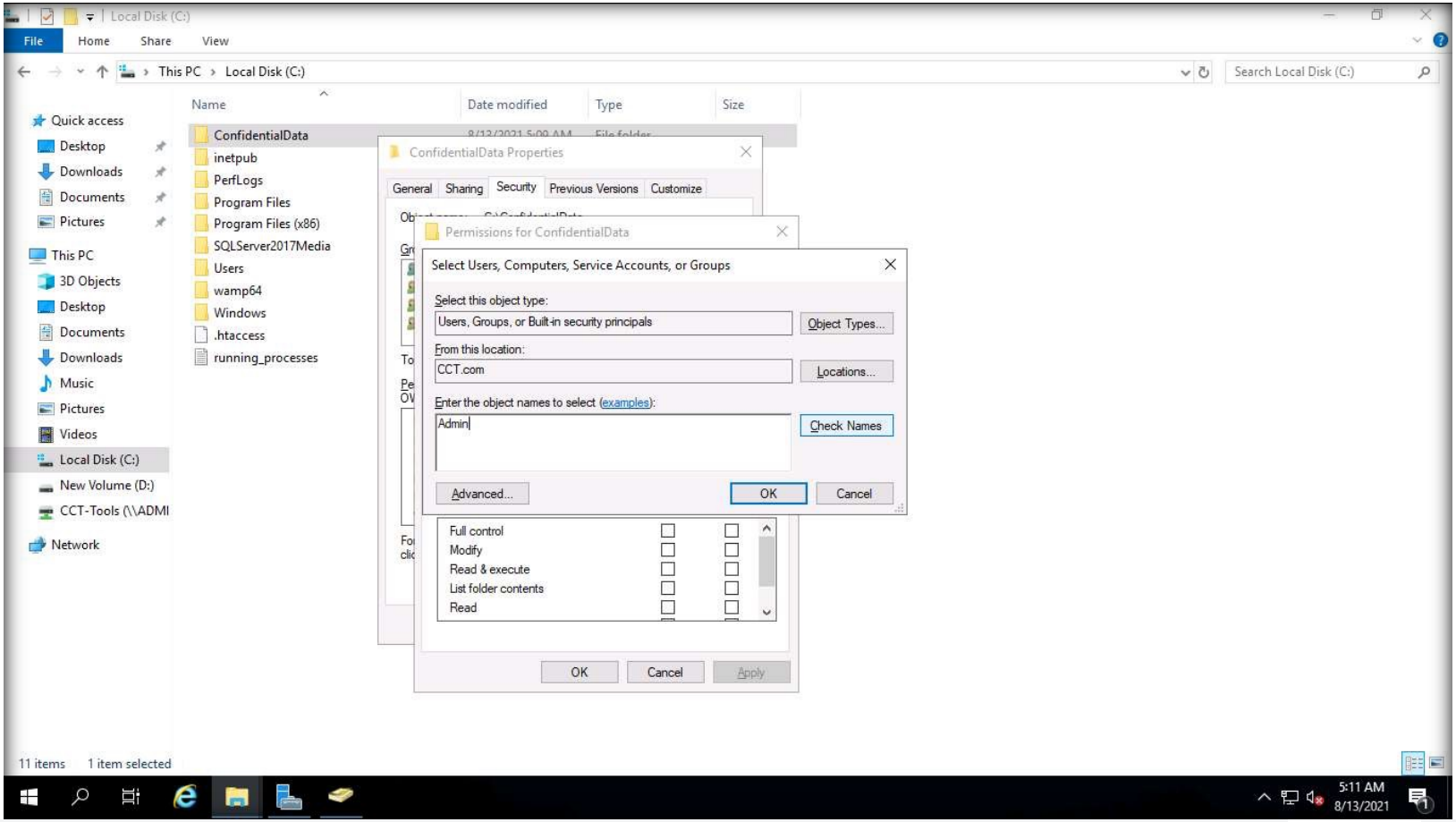
EXERCISE 2: IMPLEMENT AUDITING POLICIES

23. A Permissions for ConfidentialData window appears, click Add button.



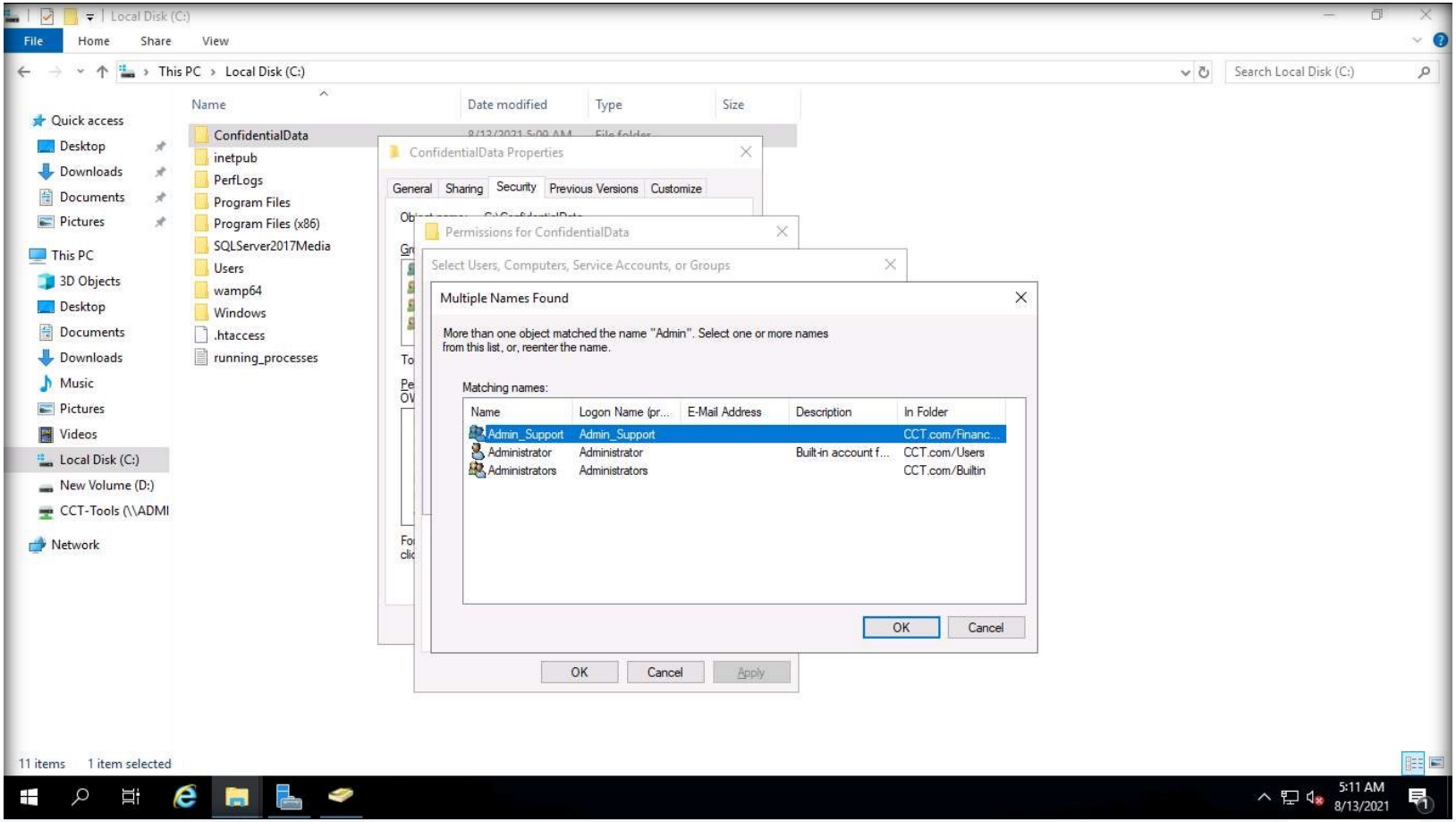
EXERCISE 2: IMPLEMENT AUDITING POLICIES

24. Select Users, Computers, Service Accounts, or Groups dialog box appears, in the Enter the object names to select field, type Admin and click Check Names button.



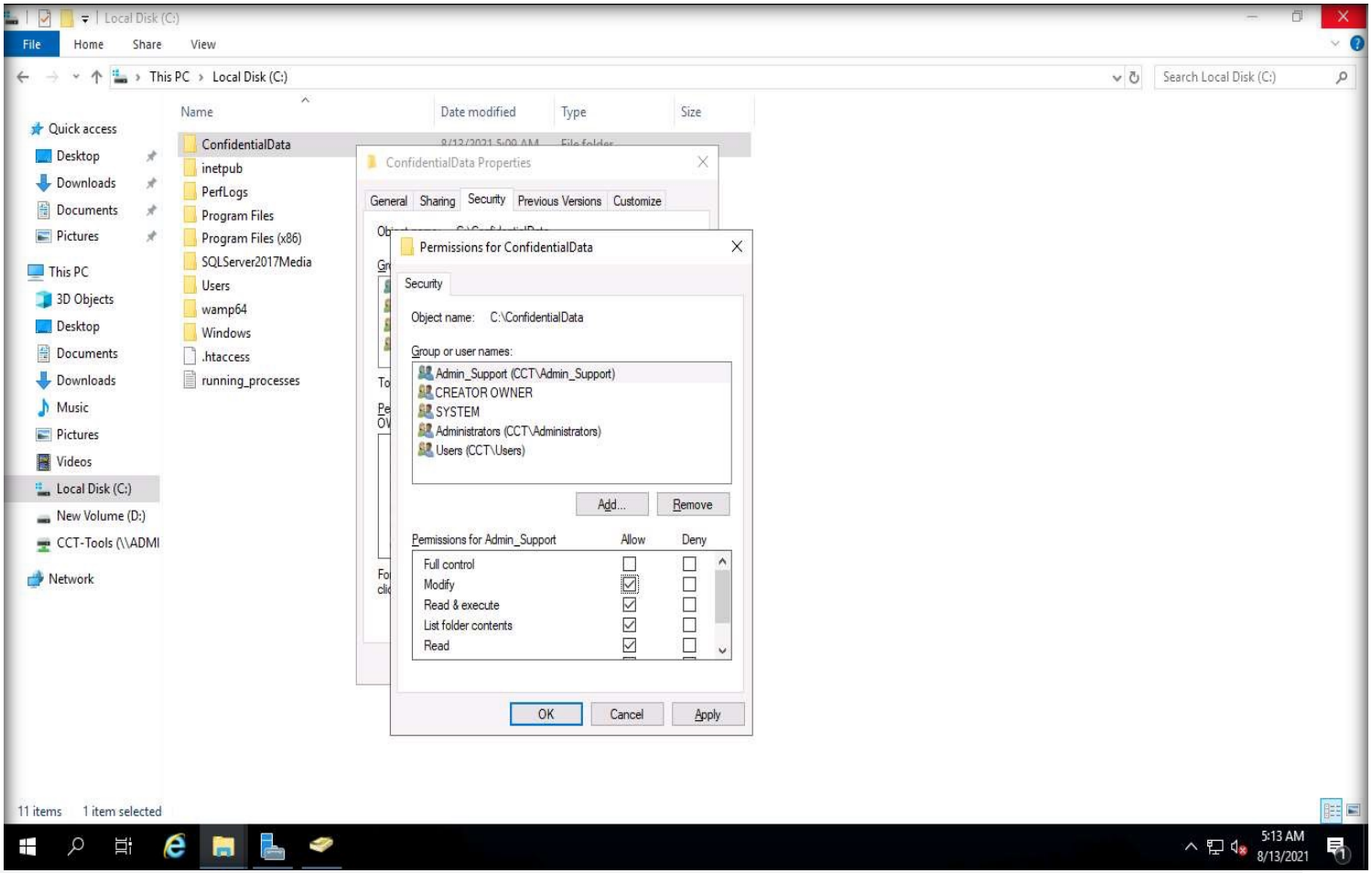
EXERCISE 2: IMPLEMENT AUDITING POLICIES

25. In the Multiple Names Found window, select the Admin_Support group and click OK.



EXERCISE 2: IMPLEMENT AUDITING POLICIES

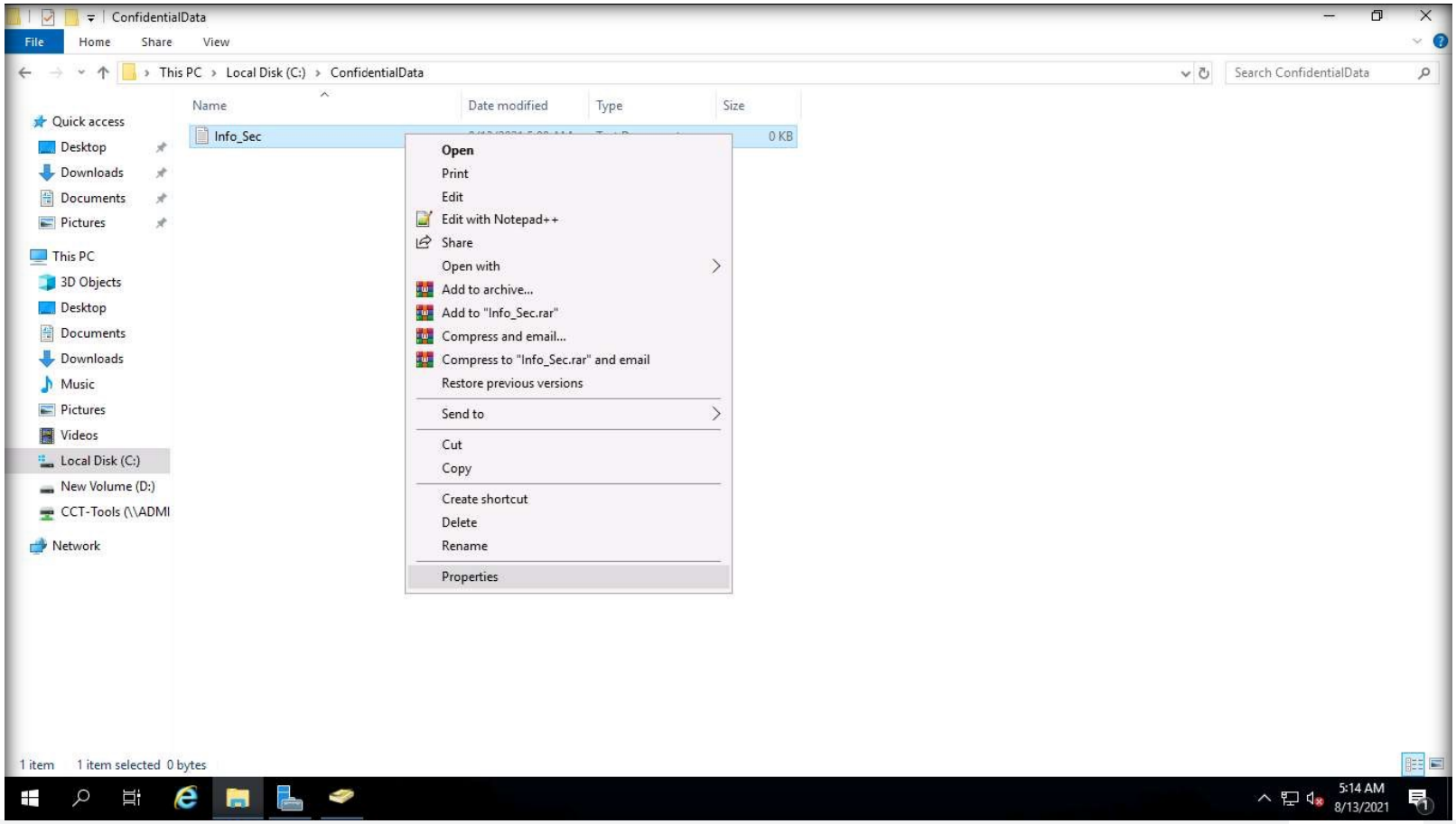
26. In the Select Users, Computer, Service Accounts, or Groups dialog box, click OK.
27. You can observe that the Admin_Support group is highlighted under the Group or user names section. Click on the Modify checkbox under the Allow column under Permissions for Admin_Support section.



EXERCISE 2: IMPLEMENT AUDITING POLICIES

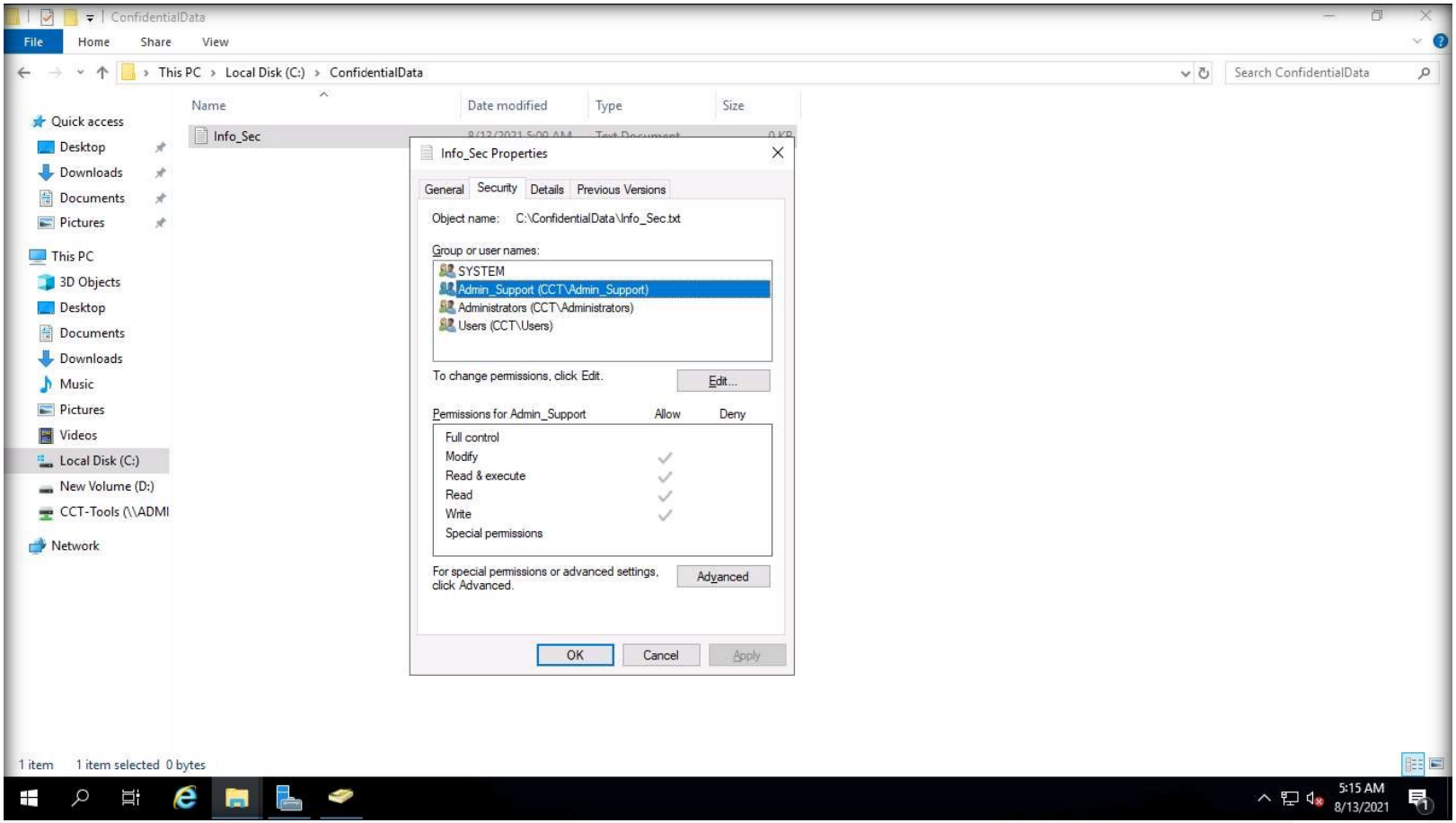
28. In the Permissions for ConfidentialData window and ConfidentialData Properties window, click OK.

29. Now, double-click to open ConfidentialData folder, click to select Info_Sec text file, right-click on it and select Properties.



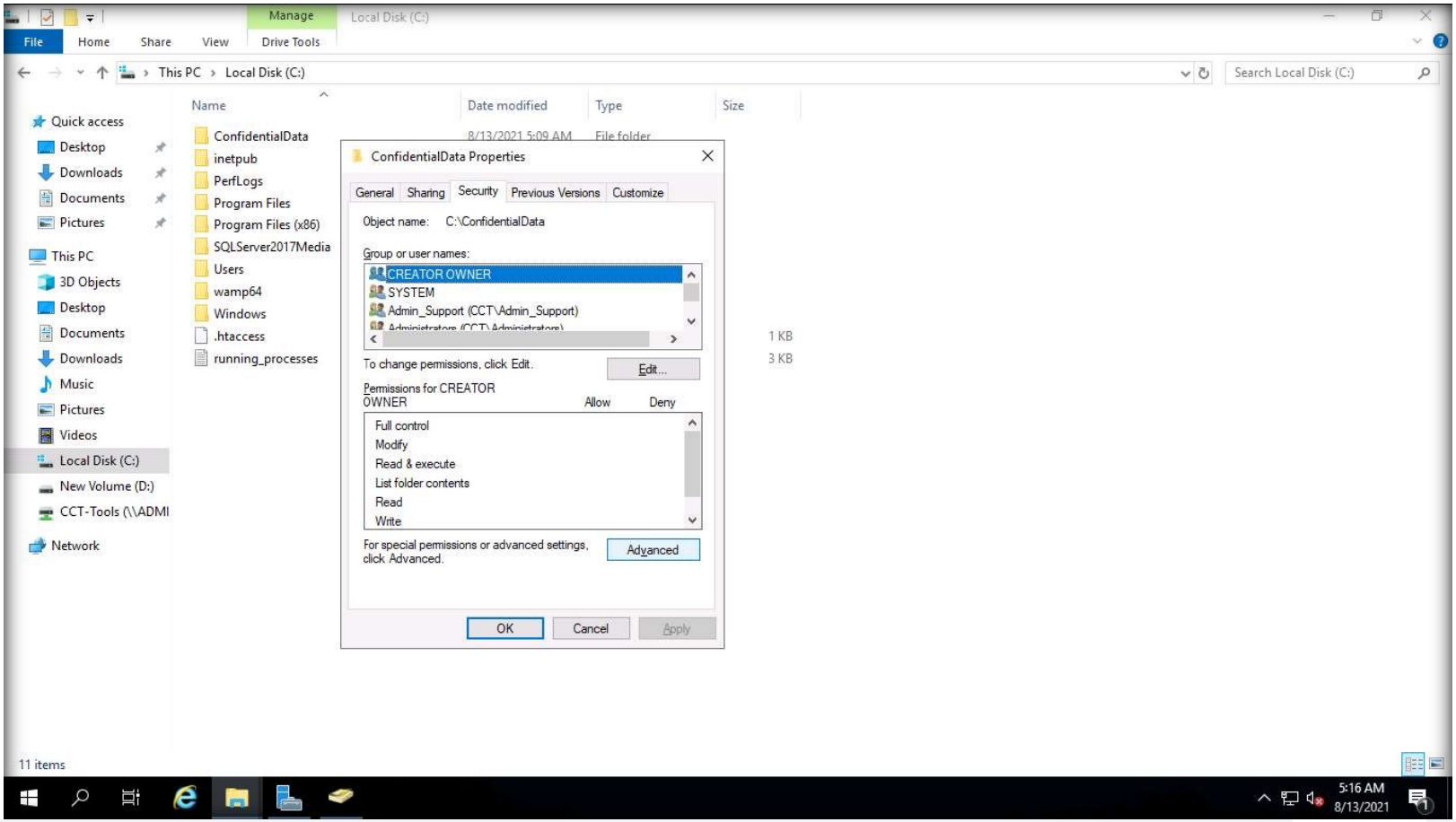
EXERCISE 2: IMPLEMENT AUDITING POLICIES

30. In the Info_Sec Properties dialog box, navigate to the Security tab and observe that the Admin_Support group is listed under Group or user names section, as shown in the screenshot.
Note: The folders and files inside the parent folder (here, ConfidentialData) inherit the same permissions as configured for the parent folder.



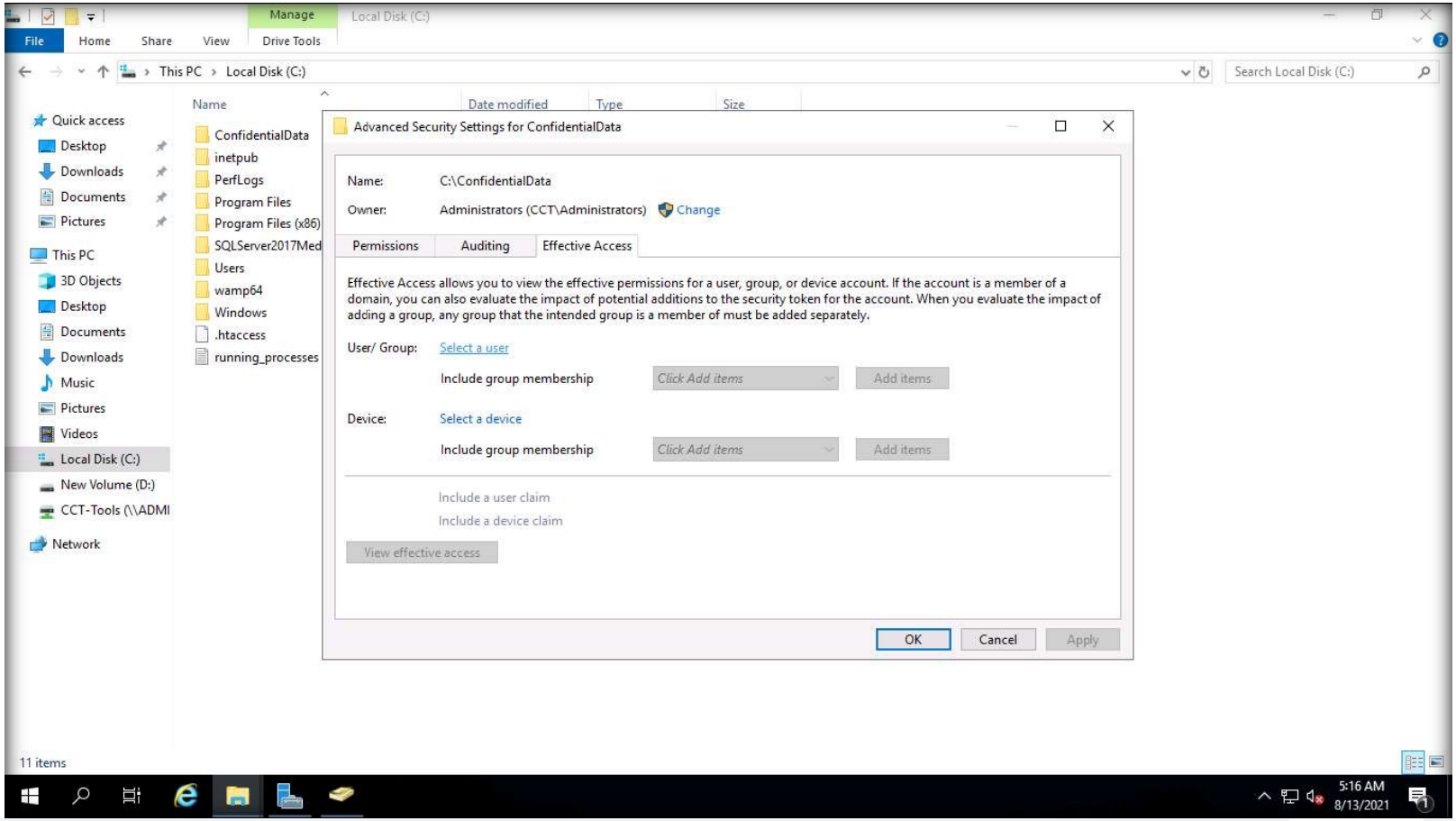
EXERCISE 2: IMPLEMENT AUDITING POLICIES

31. Click OK to close the Info_Sec Properties dialog box.
32. Navigate back to the Local Disk (C:) drive, right-click the ConfidentialData folder and select Properties.
33. A ConfidentialData Properties window appears. Navigate to the Security tab and click Advanced button.



EXERCISE 2: IMPLEMENT AUDITING POLICIES

34. A window appears, navigate to the Effective Access tab.
35. Under the Effective Access tab, click on Select a user link.

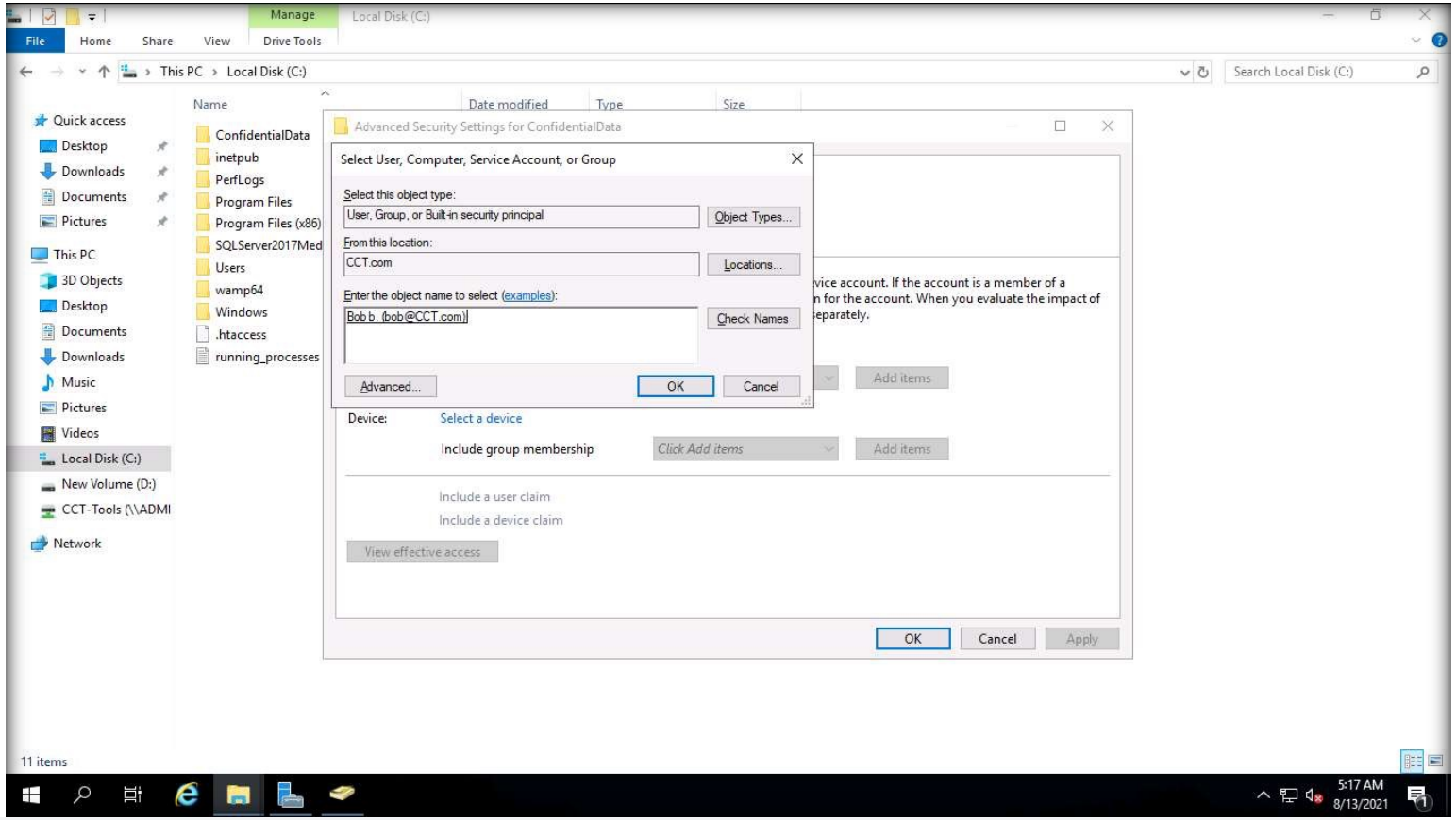


EXERCISE 2: IMPLEMENT AUDITING POLICIES

36. Next, the Select User, Computer, Service Account, or Group dialog box appears, in the Enter the object names to select field, type bob and click Check Names button.

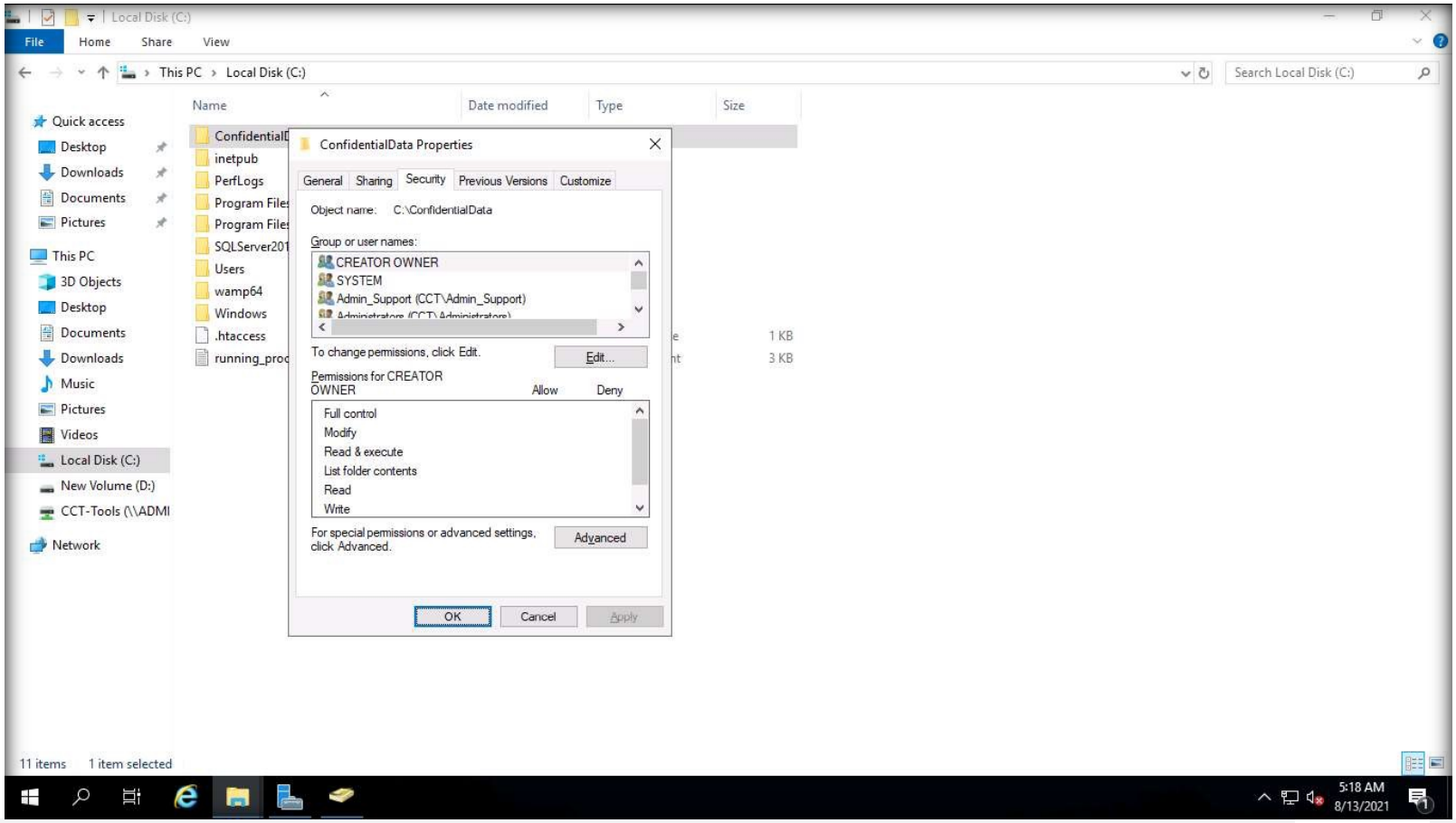
Note: Here, user account bob is a member of the Admin_Support group which does not have complete control over the folder; user accounts that are members of the Administrators group have complete control over the folder.

37. A complete user address appears, click OK.



38. Select OK in the dialog-box to close it. Similarly, click OK in the ConfidentialData Properties window.

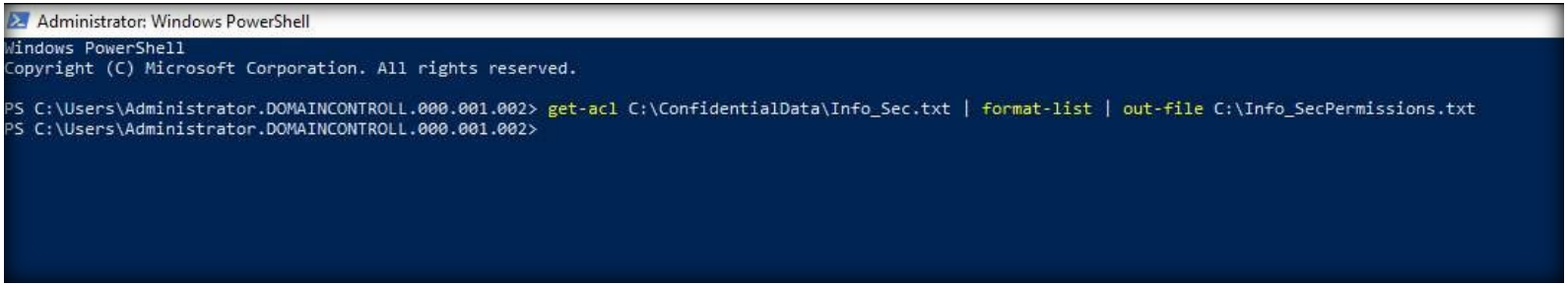
EXERCISE 2: IMPLEMENT AUDITING POLICIES



39. Now, right-click the Start icon at the bottom left of the Desktop. Select Windows PowerShell (Admin) option.

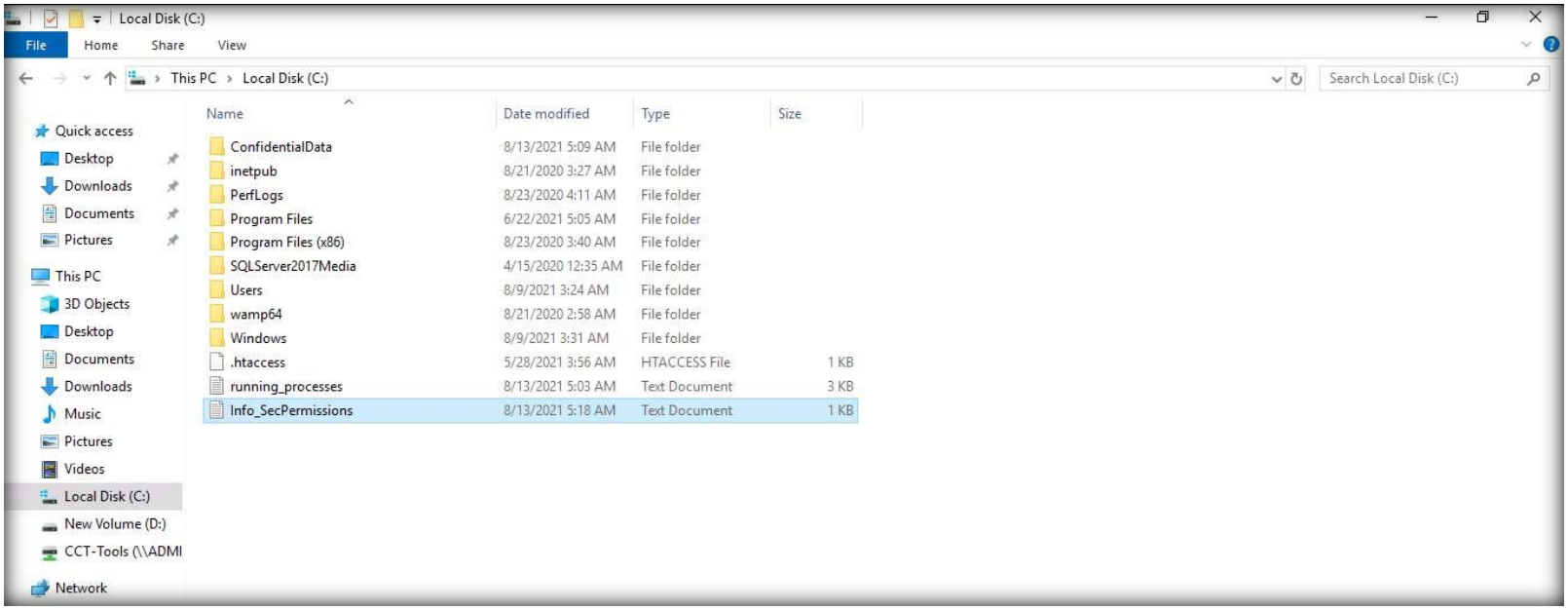
40. The Administrator: Windows PowerShell window appears, type get-acl C:\ConfidentialData\Info_Sec.txt | format-list | out-file C:\Info_SecPermissions.txt and press Enter.

EXERCISE 2:
IMPLEMENT
AUDITING POLICIES



41. Navigate to C:\ drive and observe that a text file Info_SecPermissions.txt has been created.

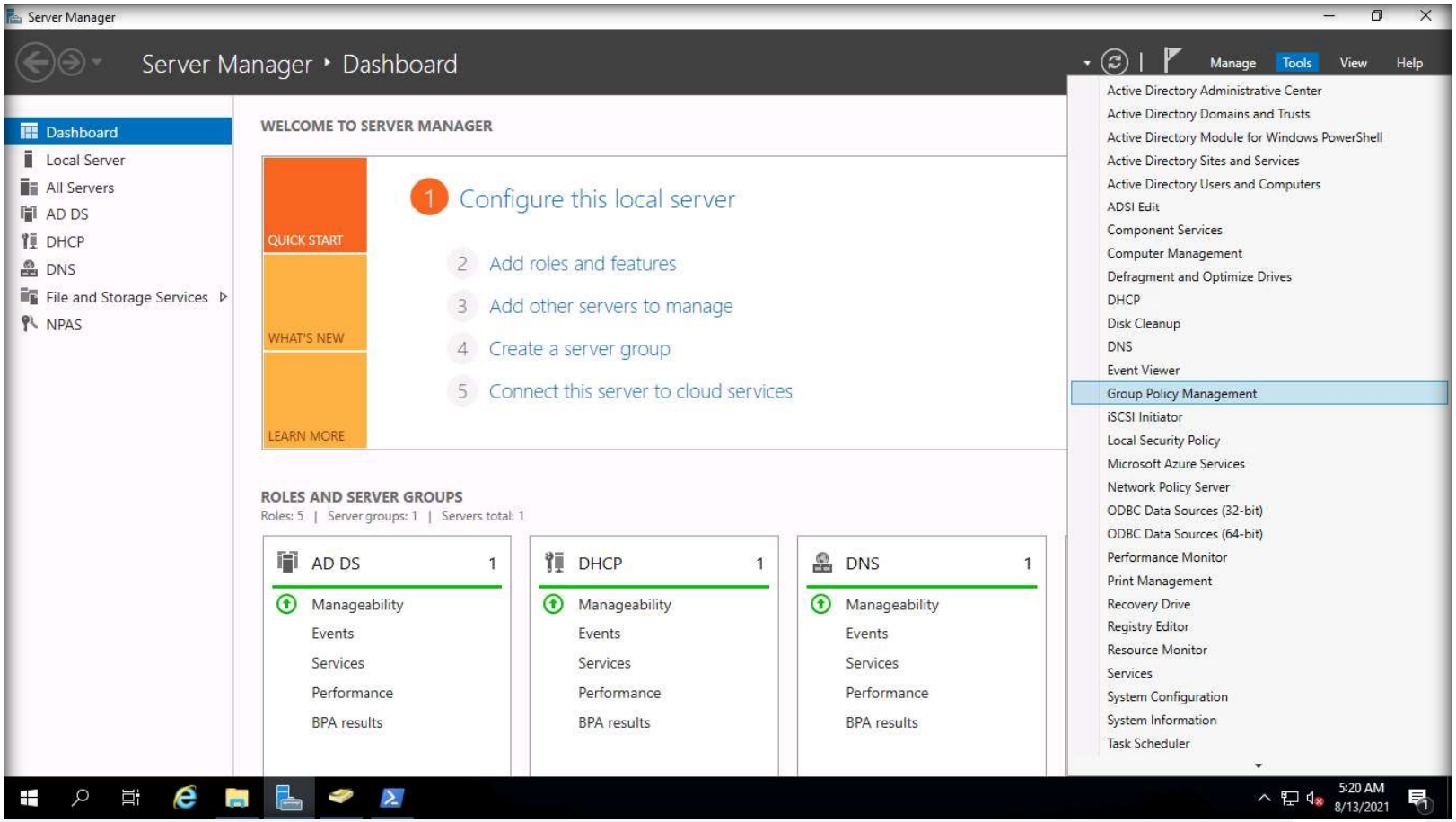
EXERCISE 2: IMPLEMENT AUDITING POLICIES



EXERCISE 2: IMPLEMENT AUDITING POLICIES

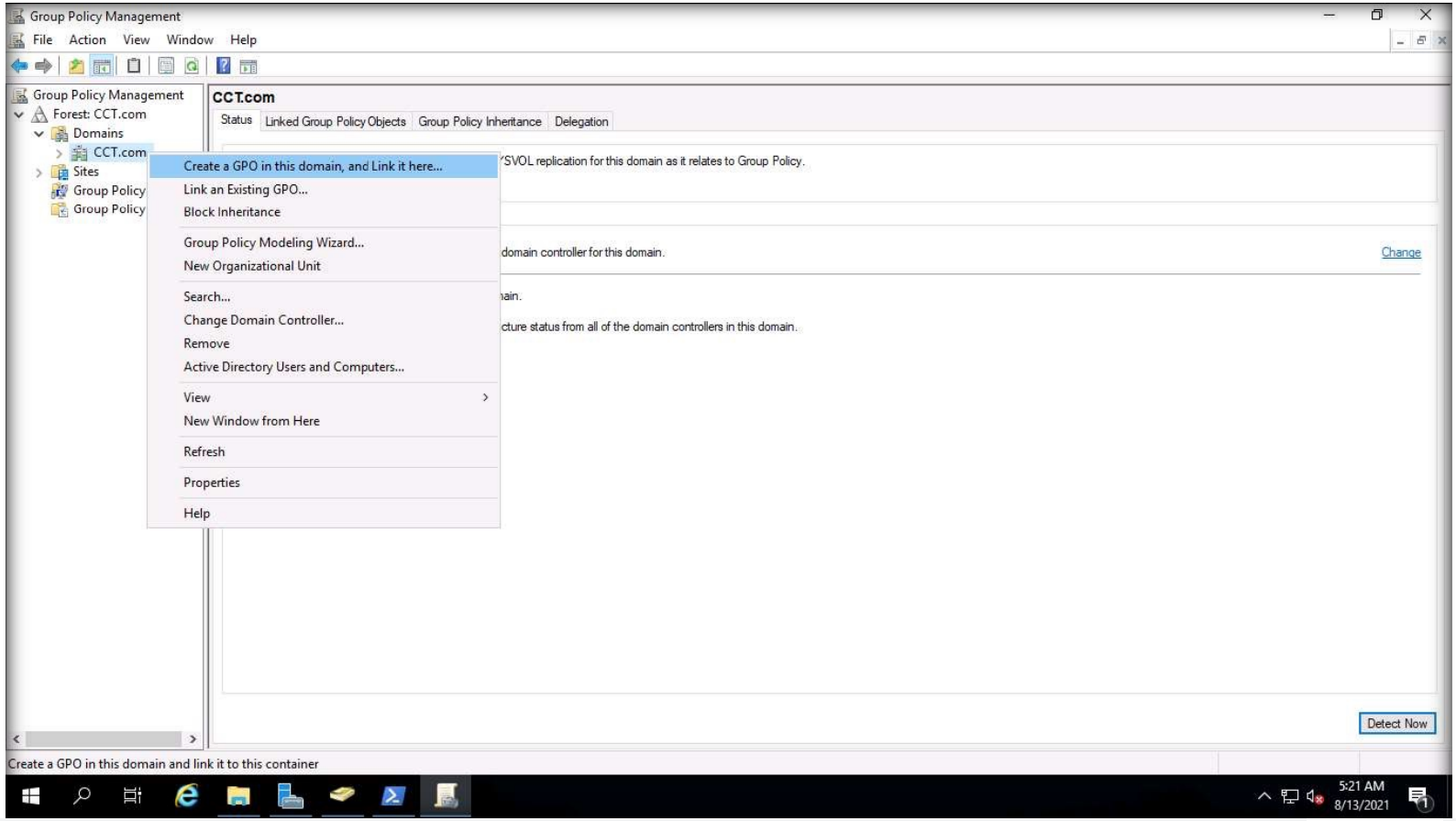
42. Next, we will configure an audit policy in GPO (Group Policy Object).

43. Maximize the Server Manager window and navigate to Tools → Group Policy Management.



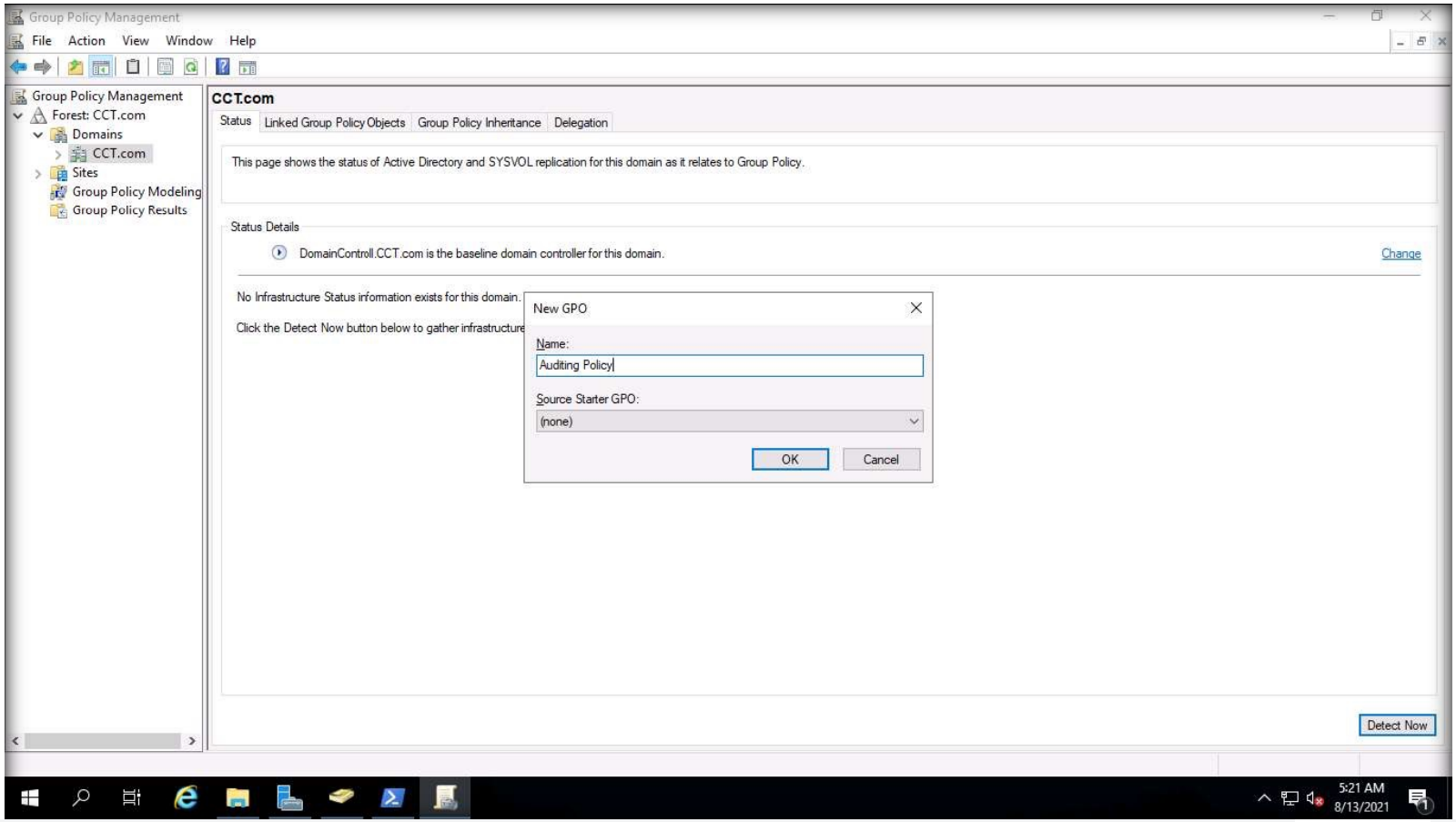
EXERCISE 2: IMPLEMENT AUDITING POLICIES

44. The Group Policy Management window appears. In the left-pane, expand Forest: CCT.com and the Domains node. Click to select CCT.com and right-click Create a GPO in this domain, and Link it here... option.



EXERCISE 2: IMPLEMENT AUDITING POLICIES

45. A New GPO dialog-box appears, in the Name field, enter Auditing Policy and click OK.



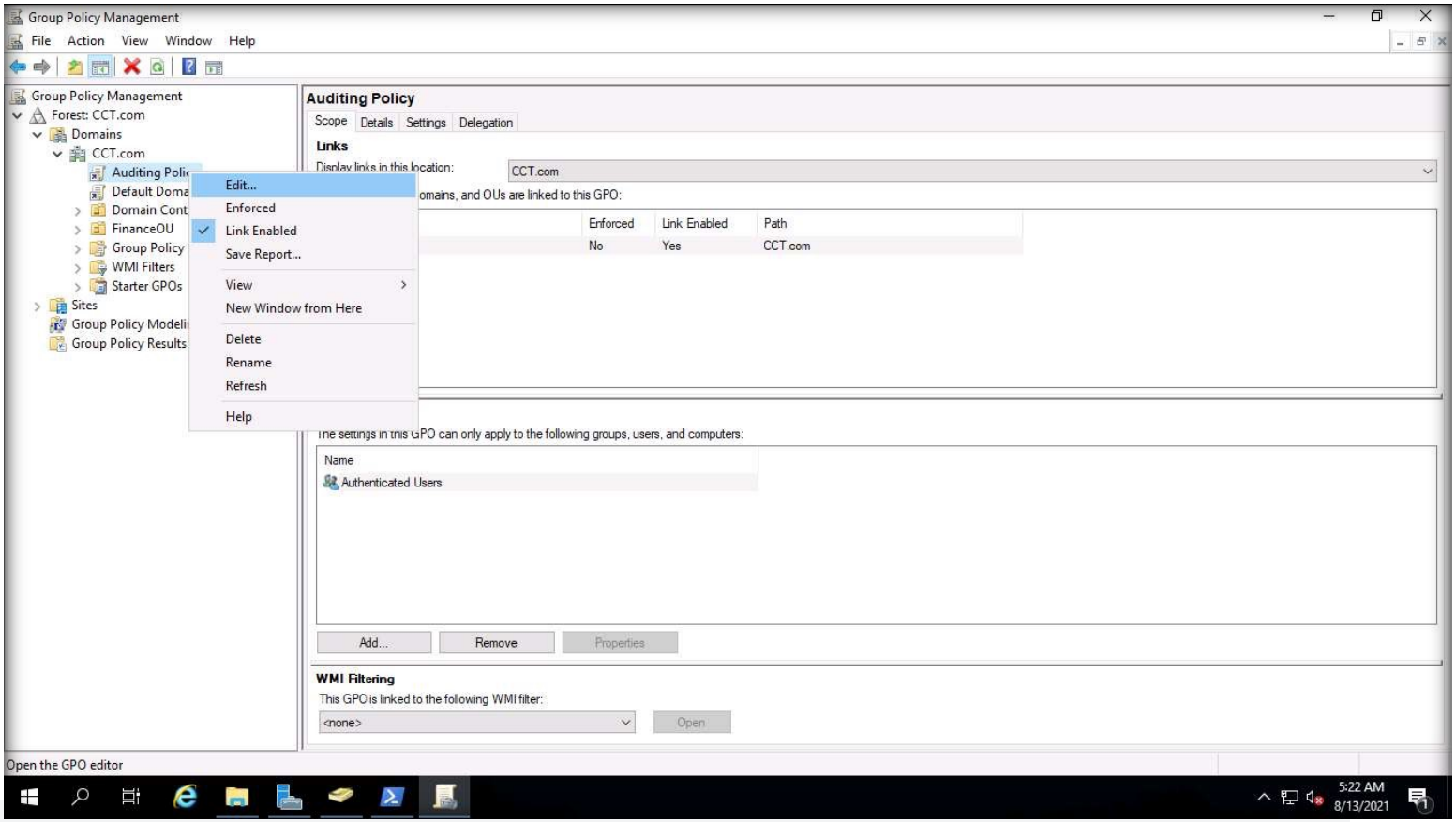
EXERCISE 2: IMPLEMENT AUDITING POLICIES

Note: Here, we will attach the Auditing Policy to the OU (Organizational Unit) of AD Domain Controller machine.

46. Click to expand the CCT.com node.

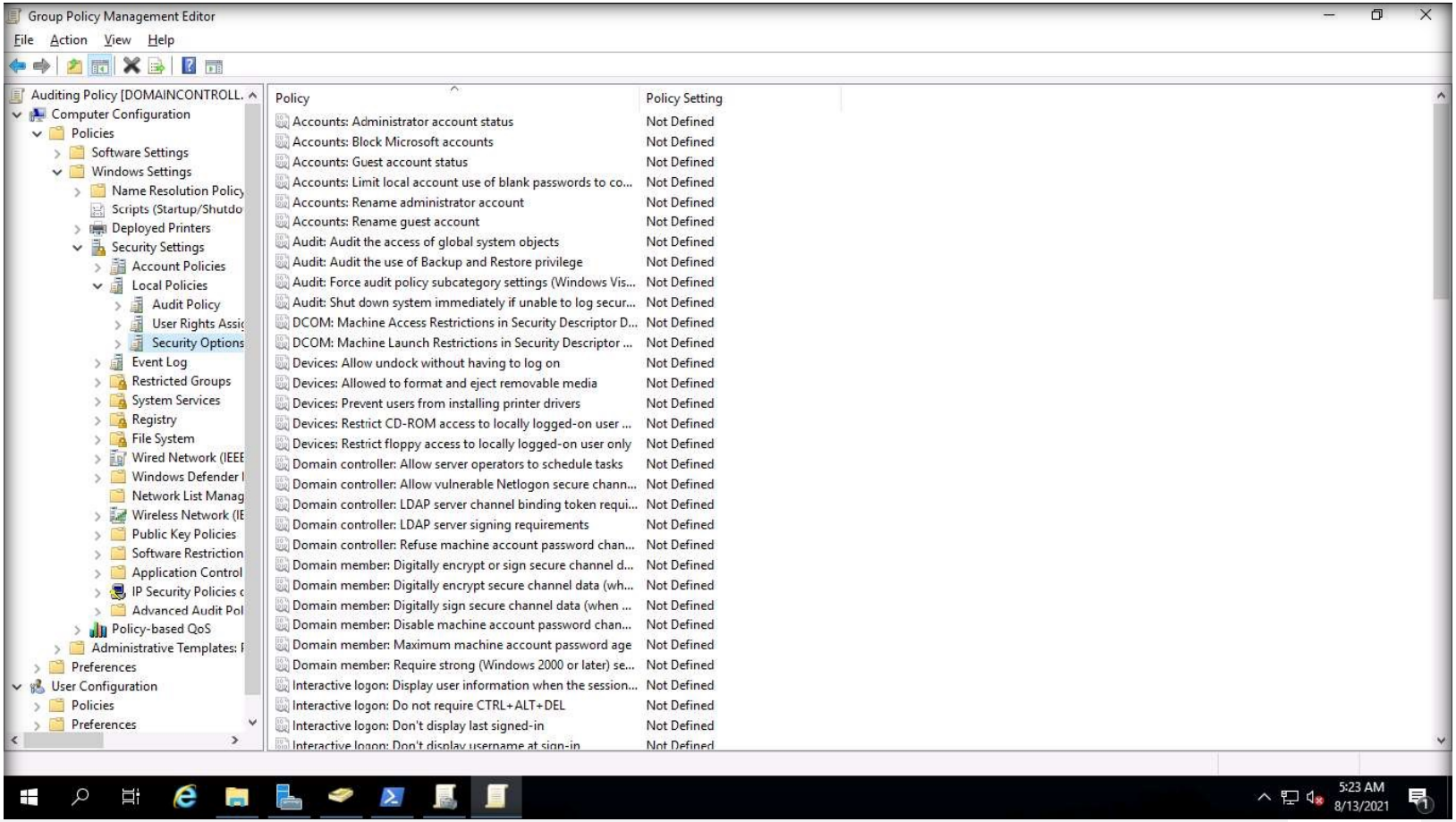
47. Click to select the Auditing Policy node, the Group Policy Management Console pop-up appears, click OK.

48. Right-click the Auditing Policy node and select Edit....



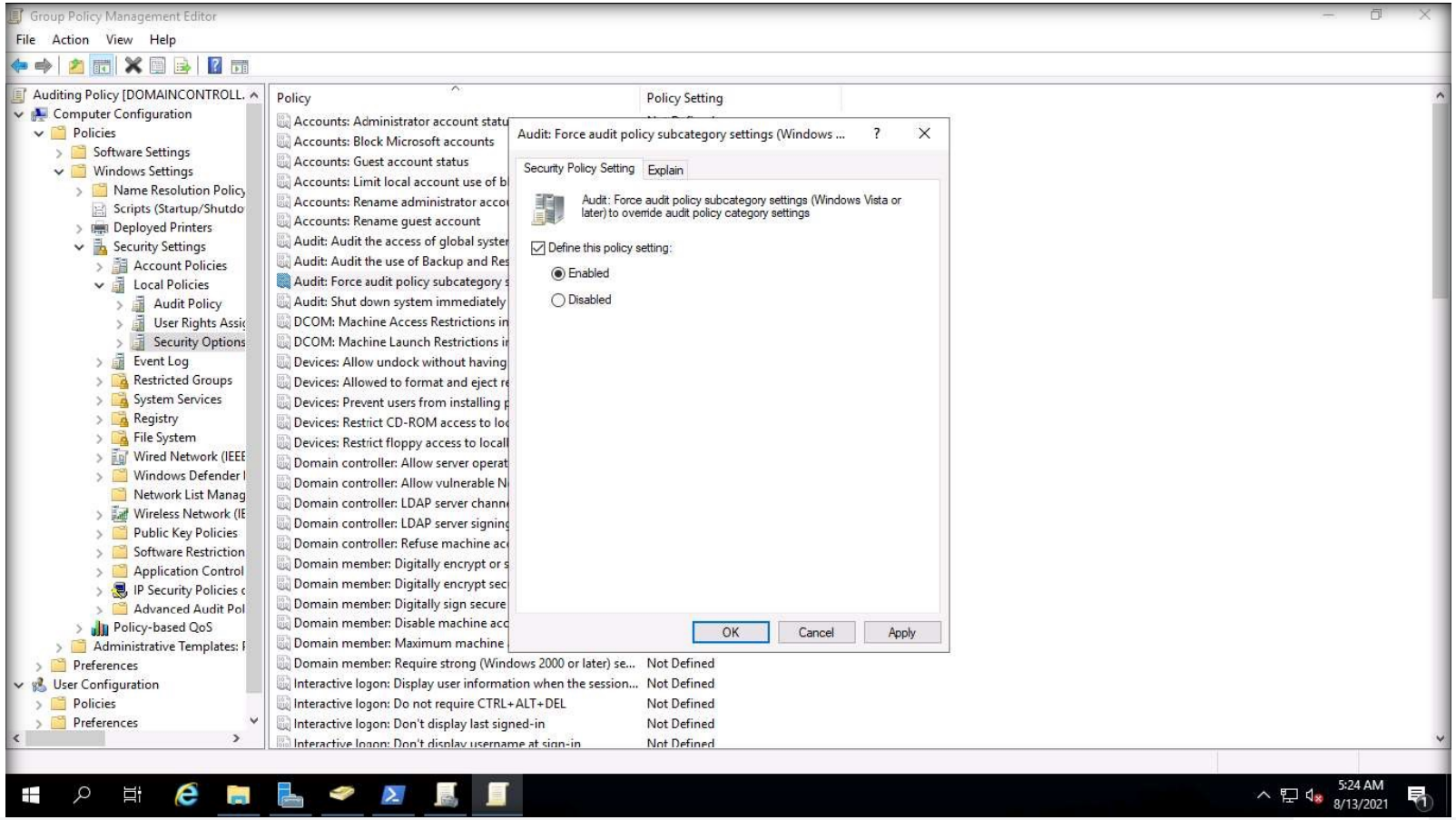
EXERCISE 2: IMPLEMENT AUDITING POLICIES

49. The Group Policy Management Editor window appears, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options.



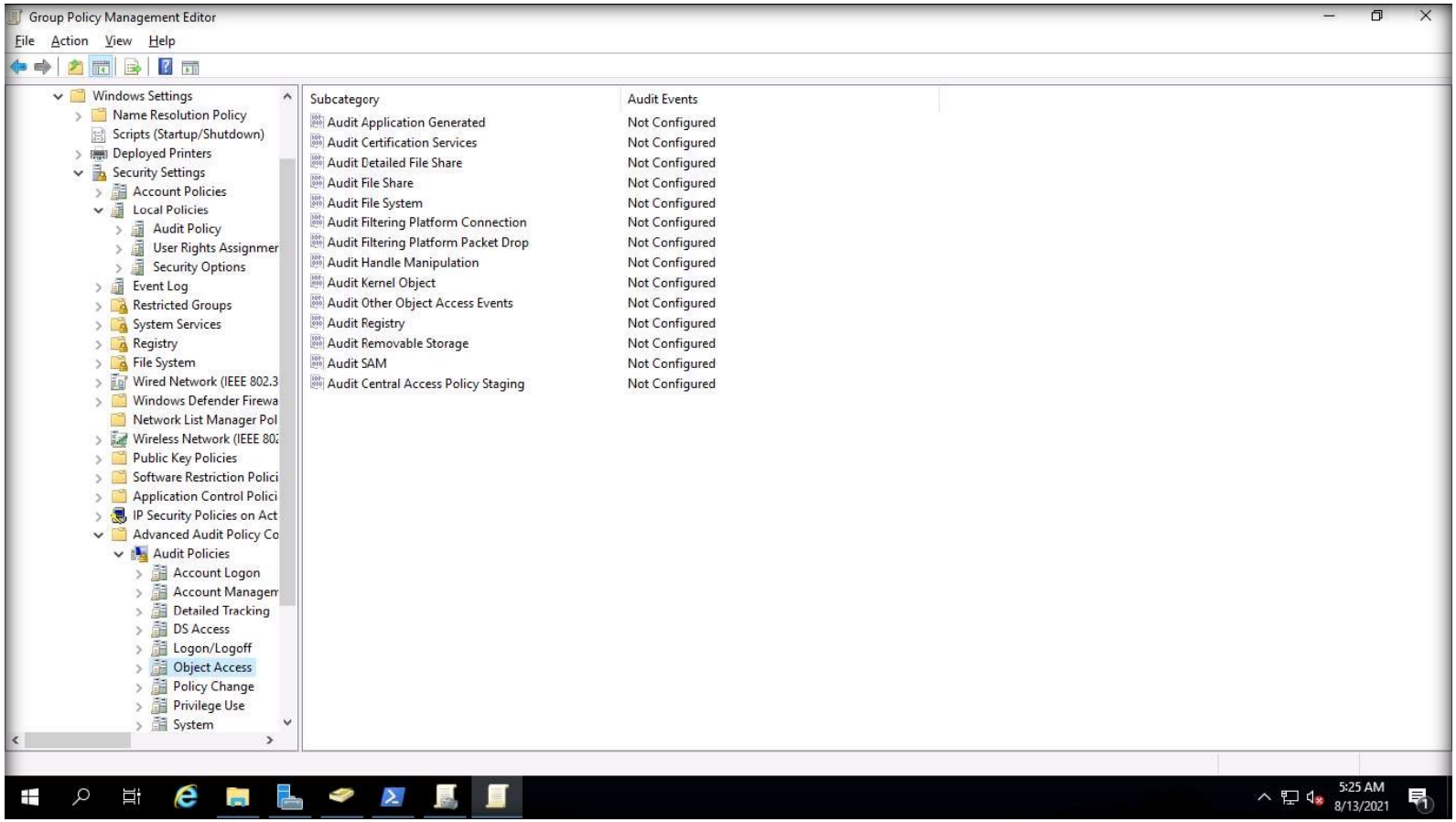
EXERCISE 2: IMPLEMENT AUDITING POLICIES

50. Double-click on the Audit: Force audit policy subcategory settings. Click on Define this policy setting checkbox and ensure that Enabled radio-button is selected. Click Apply and OK.



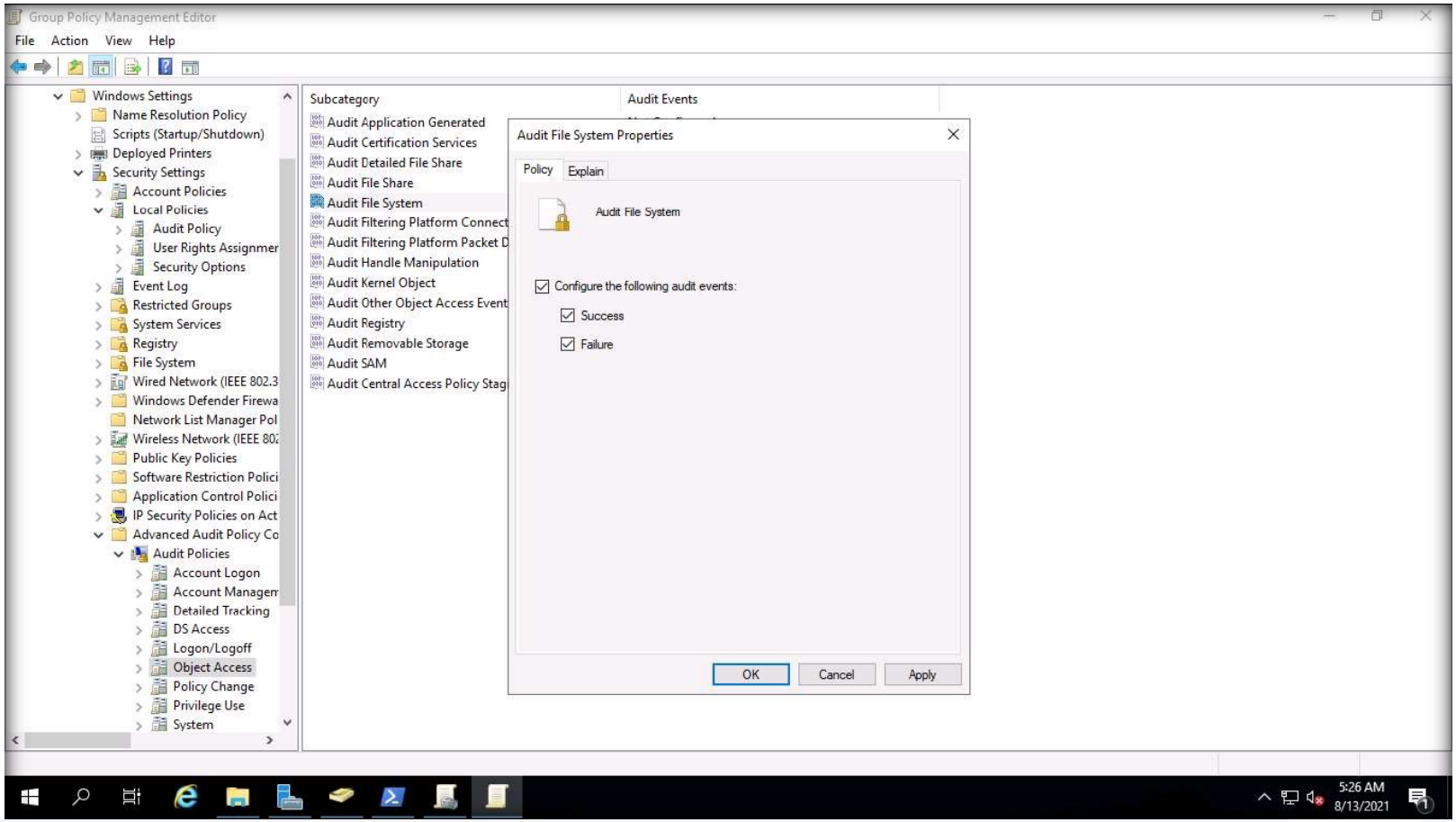
EXERCISE 2:
IMPLEMENT
AUDITING POLICIES

51. Now, navigate to Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Object Access.



EXERCISE 2: IMPLEMENT AUDITING POLICIES

52. Double-click Audit File System policy from the right-pane. Click on Configure the following audit events checkbox and select both Success and Failure checkboxes. Click OK.

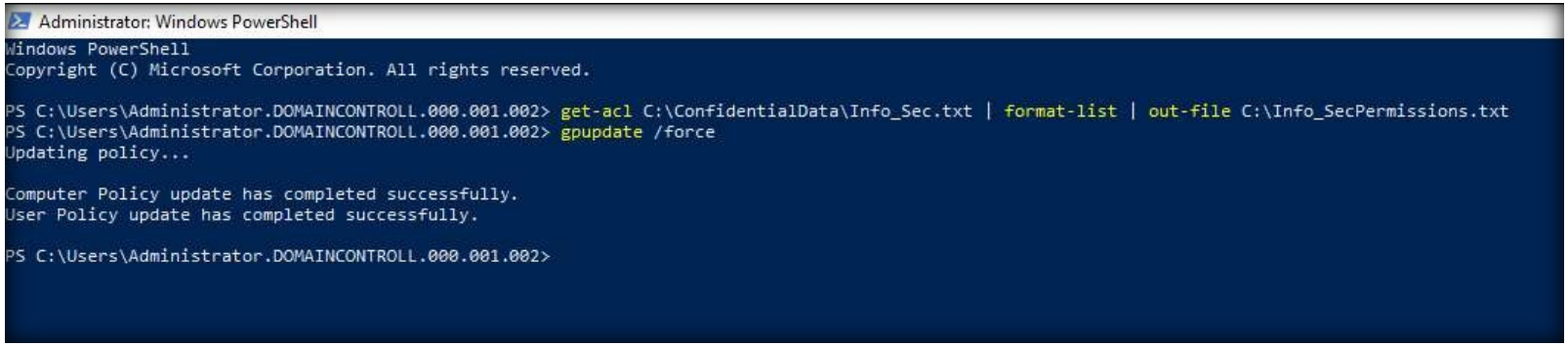


53. Now, maximize the Administrator: Windows PowerShell window, type gpupdate /force and press Enter to implement the policy settings used in the GPO to the OU of the AD Domain Controller machine.

54. Close all open windows.

55. Turn off the AD Domain Controller virtual machine.

EXERCISE 2: IMPLEMENT AUDITING POLICIES



EXERCISE 3: **IMPLEMENT A SECURE NETWORK POLICY**

A network connection policy is drafted to secure an organization's network.

LAB SCENARIO

A security professional must know how to configure an HTTPS connection to provide a secure connection to the internal website hosted in the web server.

OBJECTIVE

This lab demonstrates how to implement and configure security policy for an internal web application.

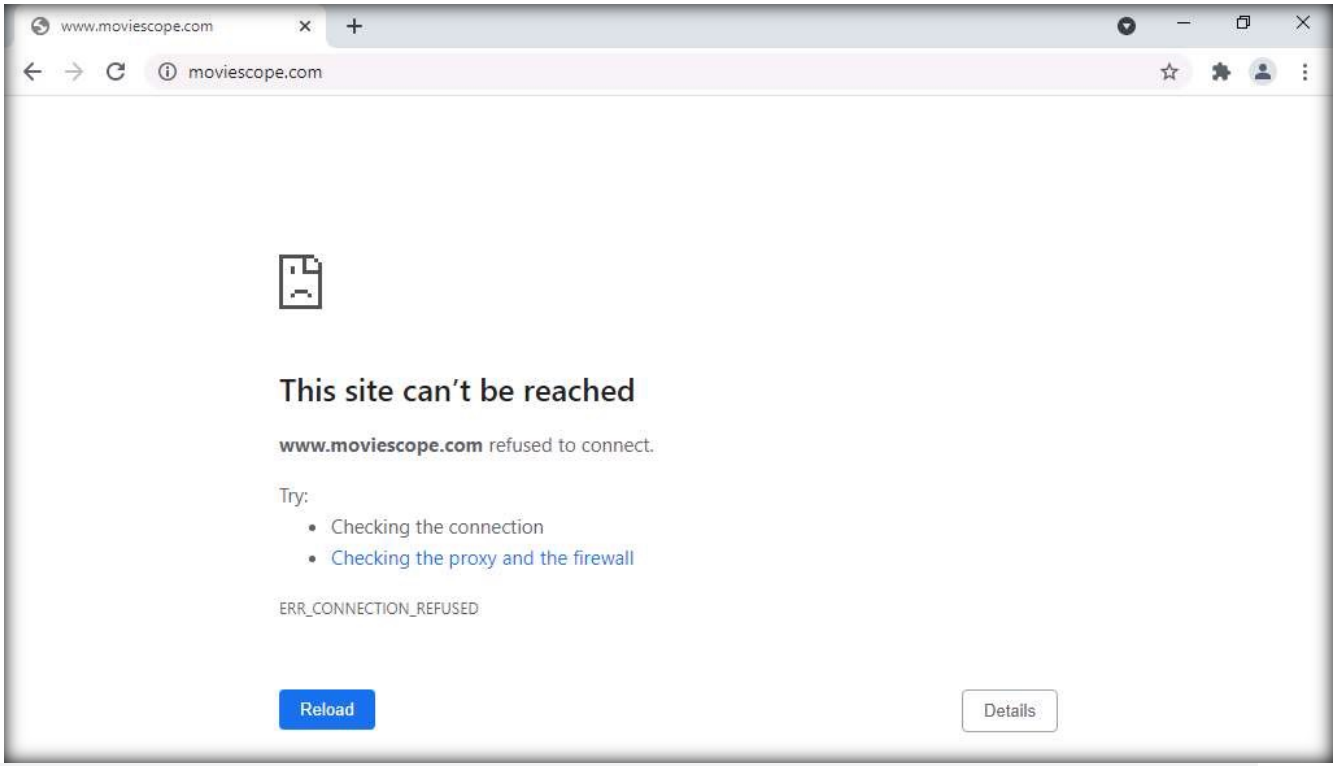
OVERVIEW OF NETWORK POLICY

A network connection policy defines regulations to be followed and implemented on the systems, servers, and other electronic devices used in an organization. An effective network connection policy involves securing the devices from potential intrusion that can be encountered by an organization.
Organizations implement policies based on their network, which enhances their data security. It facilitates protection when sharing information between other systems on a network. When security policies are implemented correctly and the network is monitored regularly, no unnecessary load is observed. The data transmission speed in the system increases, thereby ensuring an overall performance enhancement.

Copyrights @ 2022 EC-Council International Ltd.

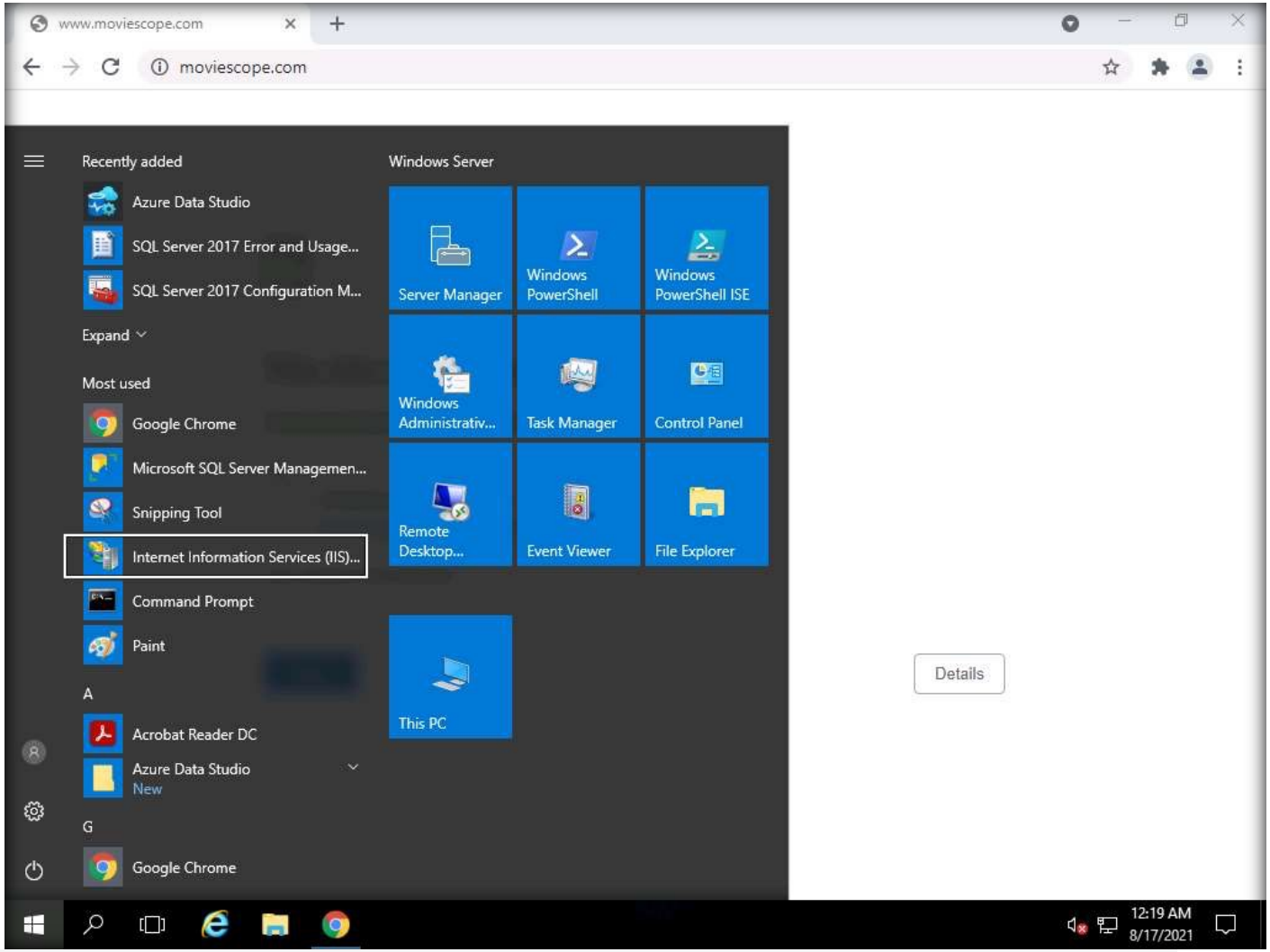
Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on the Web Server virtual machine.
2. Log in with the credentials Administrator and admin@123.
Note: If Martin username is selected by default, click on other user, and enter Administrator as username and click admin@123 and press Enter to login.
Note: The network screen appears, click Yes.
3. Launch any web browser (here, Google Chrome), place the cursor in the address bar and type on https://www.moviescope.com, and press Enter.
4. Because you are using an https channel to browse the website, it displays a page stating that This site can't be reached.
5. As the site does not have a self-signed certificate, it displays a connection refused message, as shown in the screenshot. Now, close the web browser.

EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY



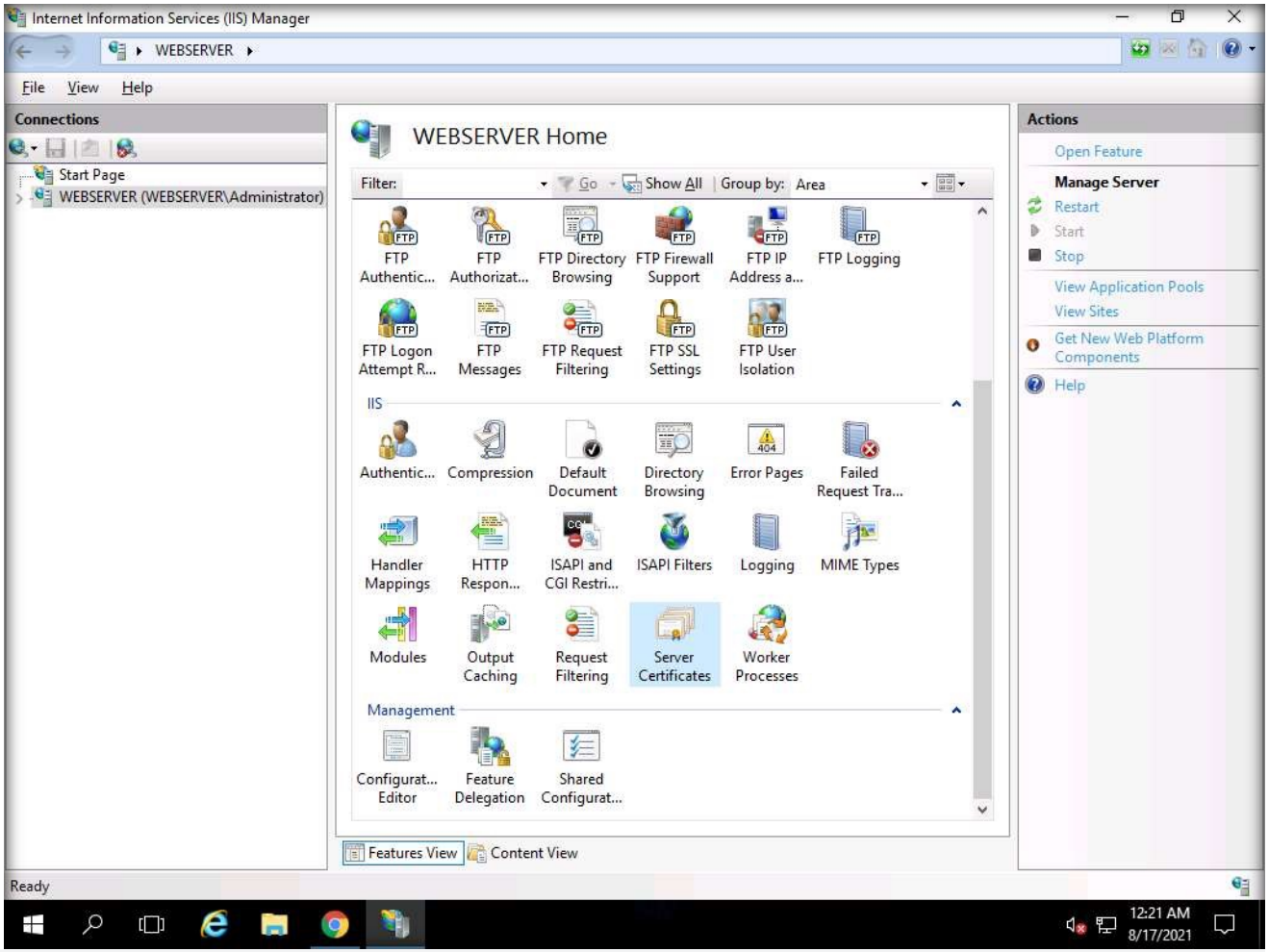
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

6. Click the Start icon in the bottom-left corner of Desktop and select Internet Information Services (IIS) Manager from the options.



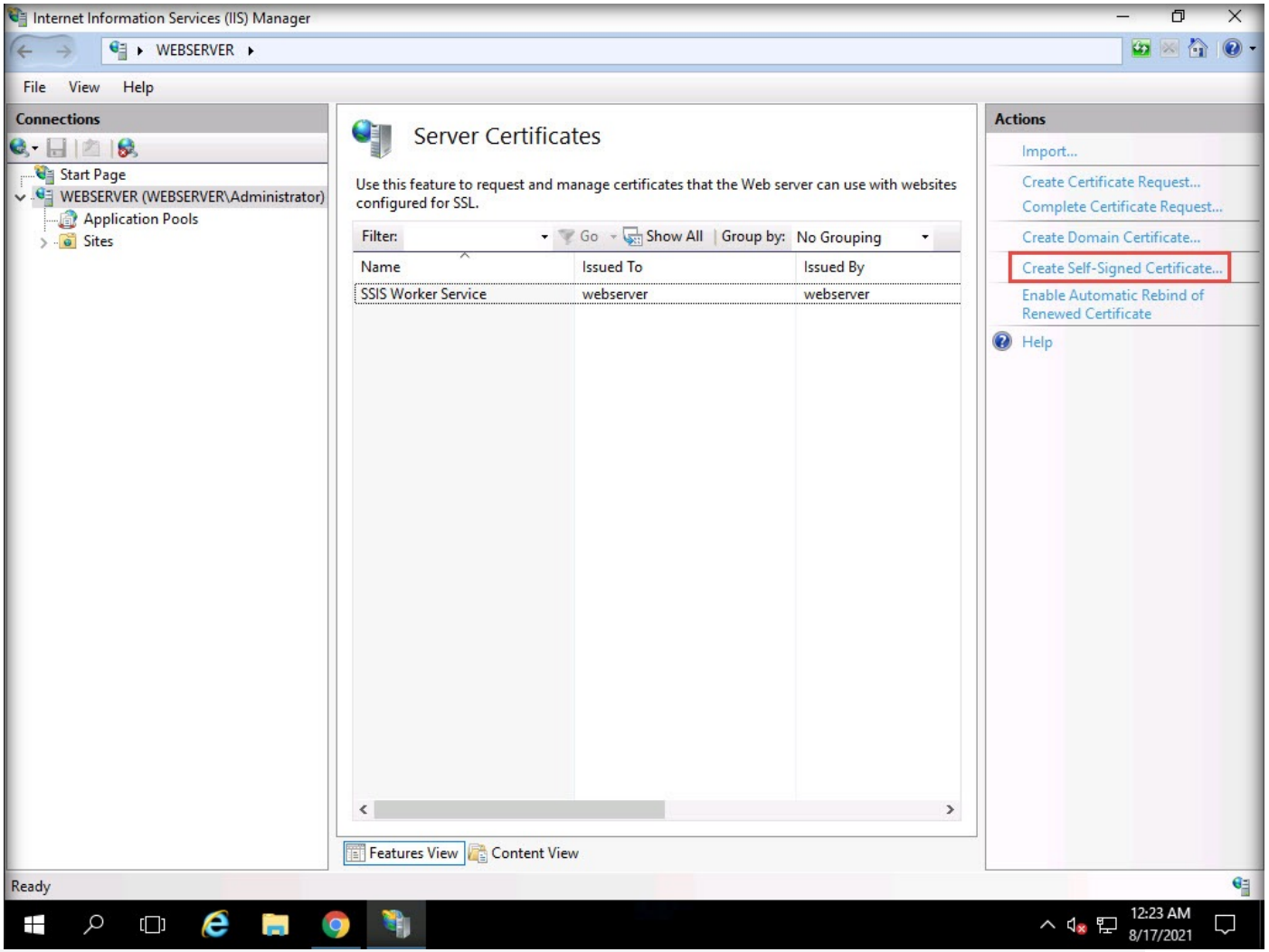
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

7. The Internet Information Services (IIS) Manager window appears; click the machine name (WEBSERVER (WEBSERVER\Administrator)) under the Connections section from the left-hand pane.
8. In WEBSERVER Home, double-click Server Certificates in the IIS section.



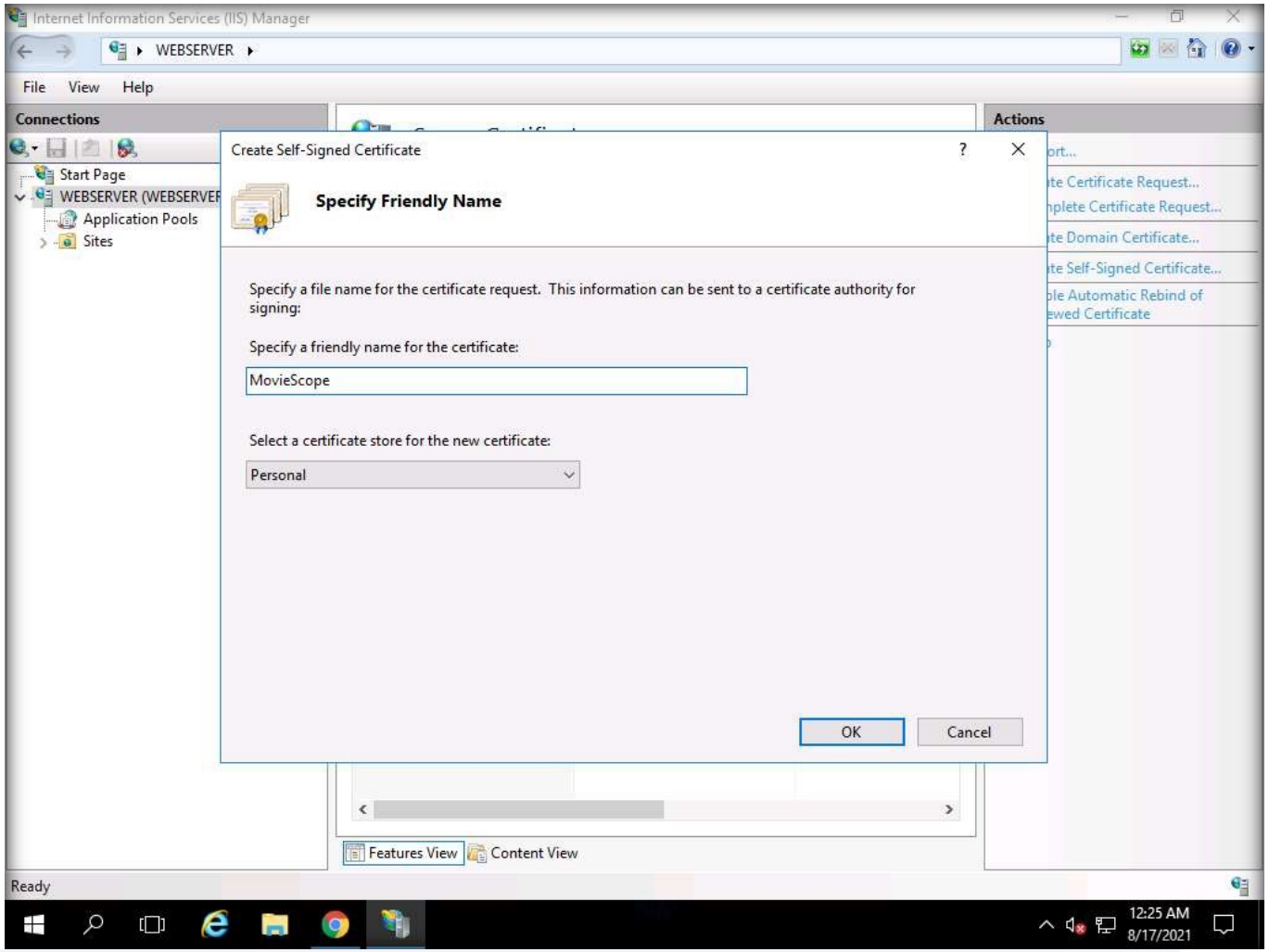
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

9. The Server Certificates wizard appears; click Create Self-Signed Certificate... from the right-hand pane in the Actions section.



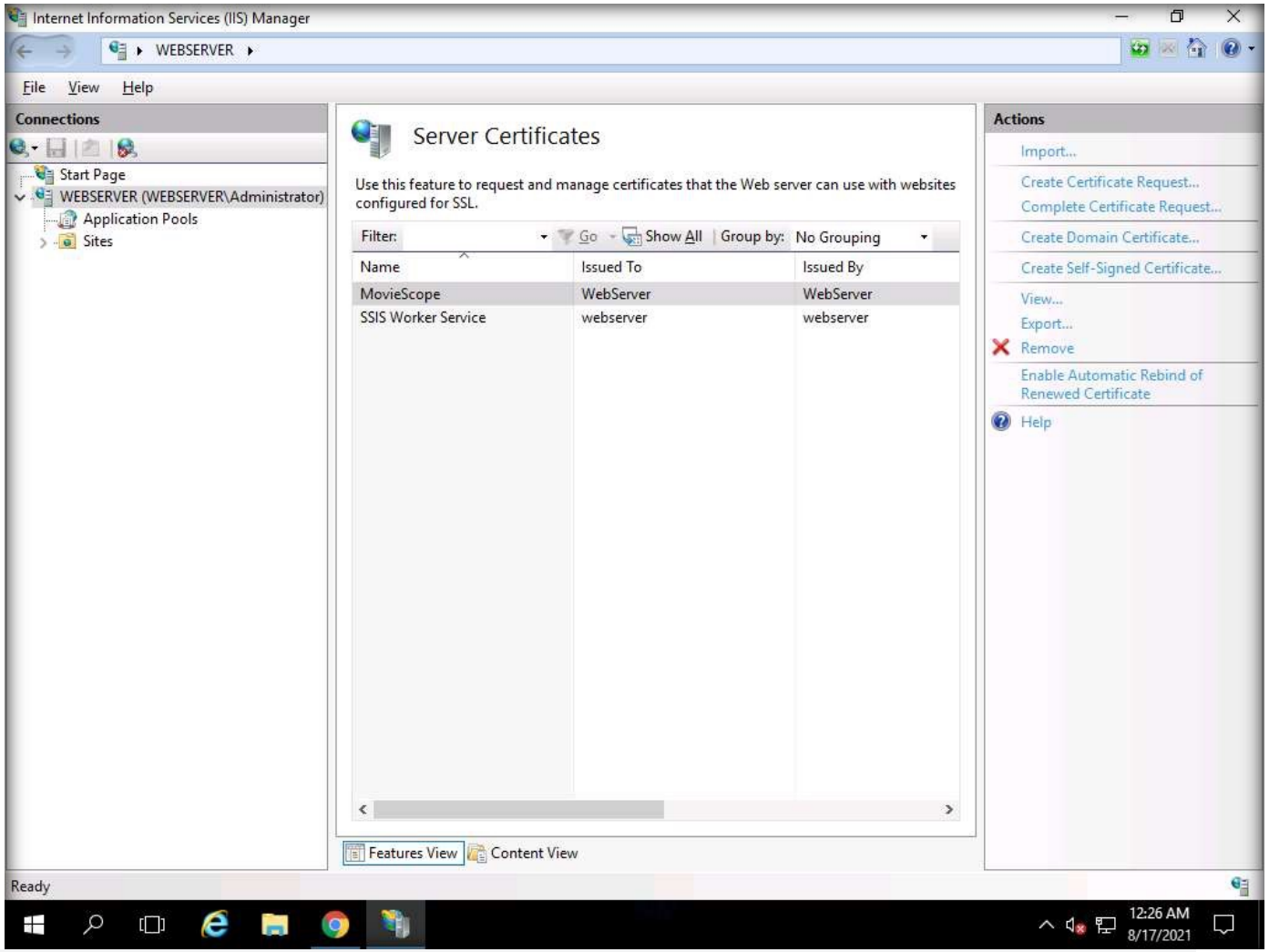
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

10. The Create Self-Signed Certificate window appears; type MovieScope in the Specify a friendly name for the certificate field. Ensure that the Personal option is selected in the Select a certificate store for the new certificate field; then, click OK.



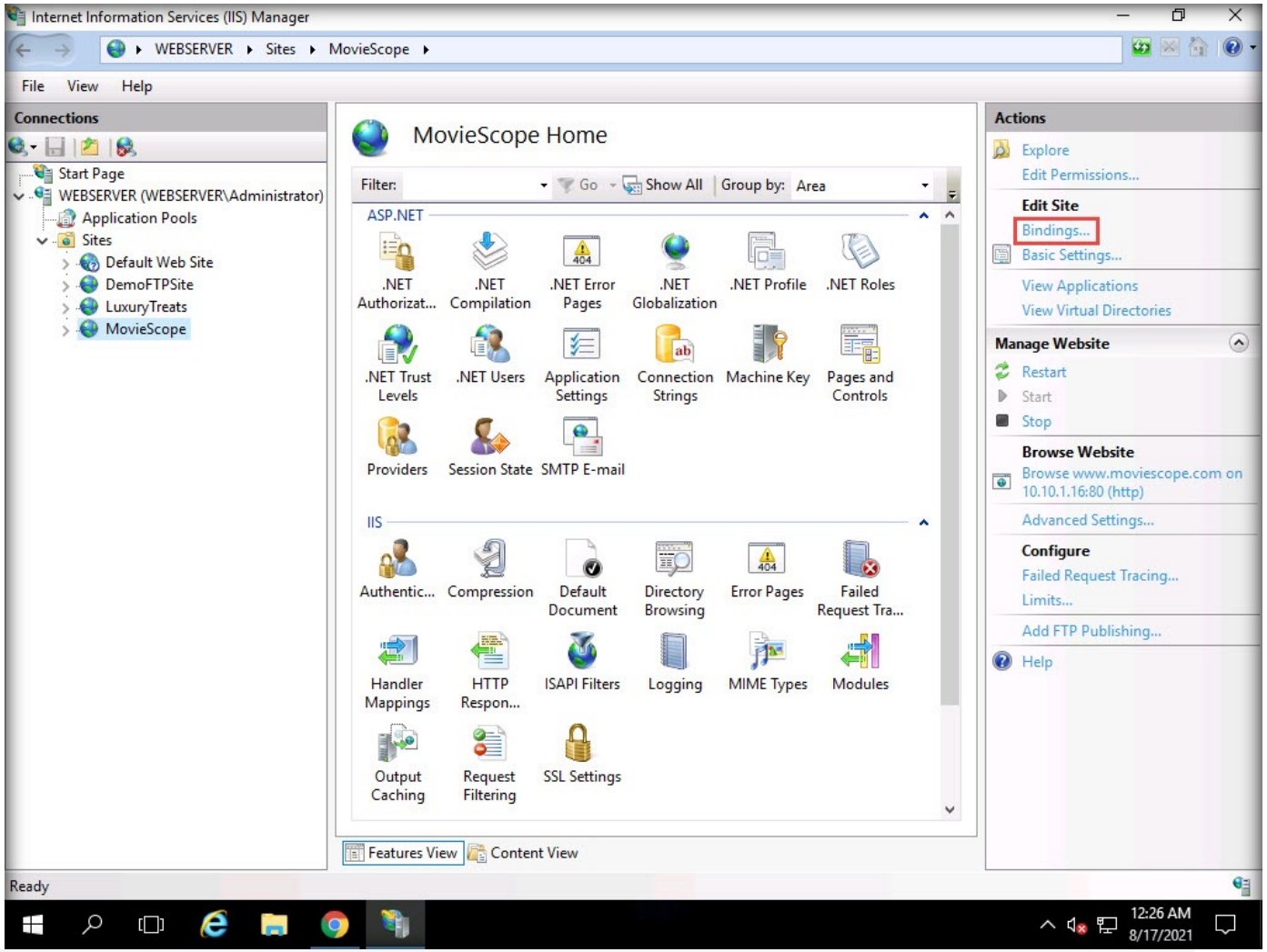
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

11. A newly created self-signed certificate will be displayed in the Server Certificates pane, as shown in the screenshot.



EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

12. Expand the Sites node from the left-hand pane and select MovieScope from the available sites. Click Bindings... from the right-hand pane in the Actions section.

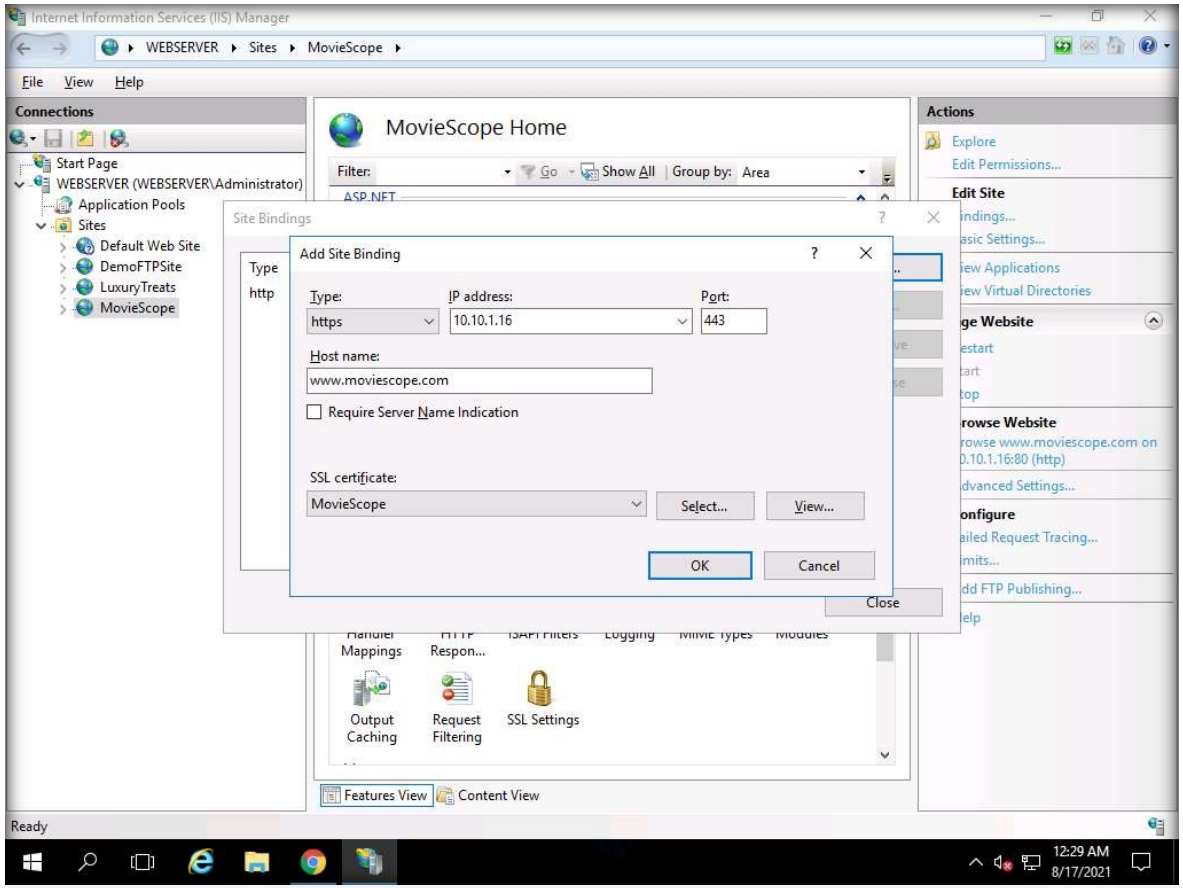


EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

14. The Add Site Binding window appears; select https from the Type field drop-down list. After selecting the https type, the port number in the Port field automatically changes to 443 (the channel on which HTTPS runs).

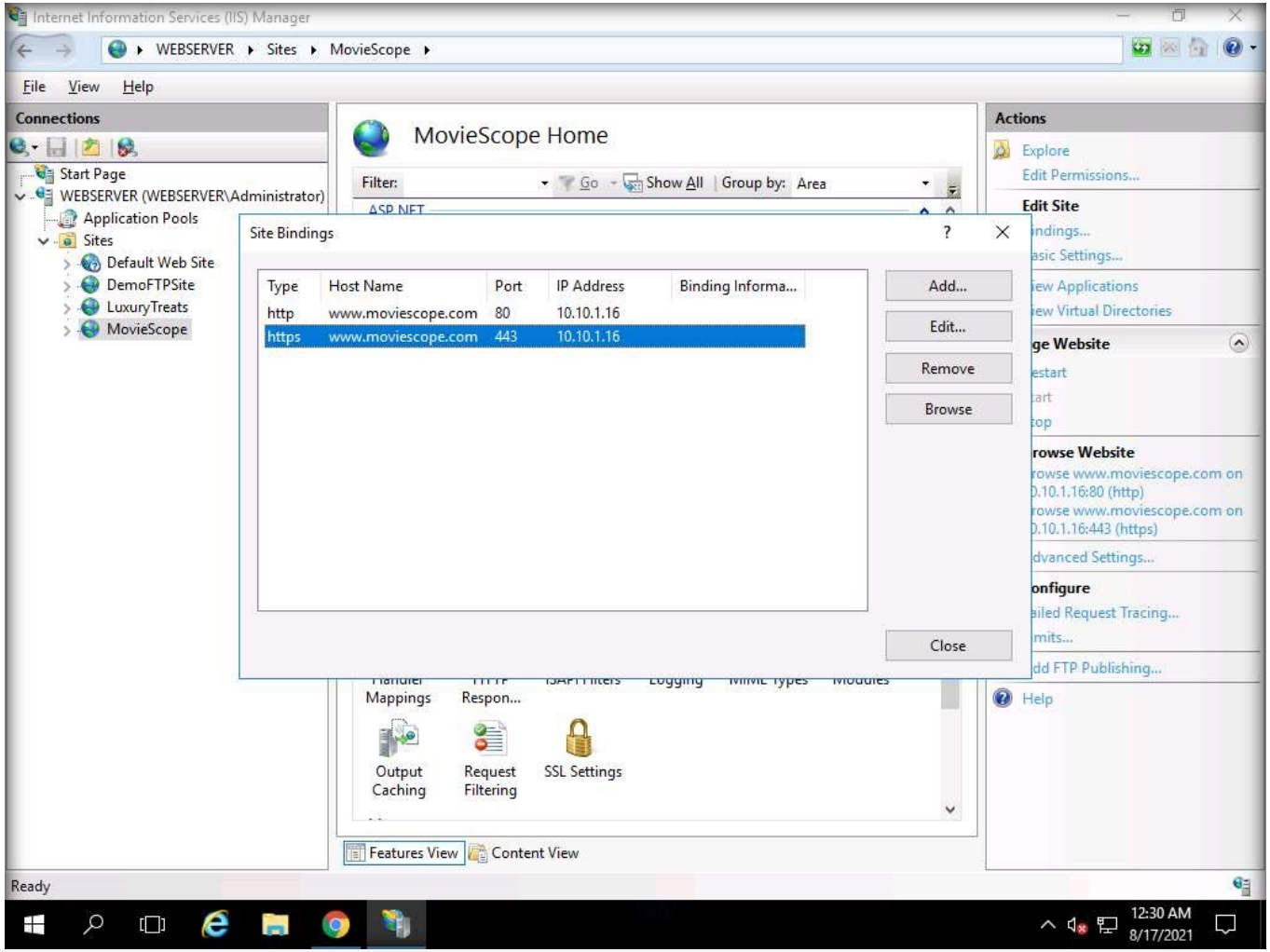
15. Select the IP address on which the site is hosted (here, 10.10.1.16).

16. Under the Host name field, type www.moviescope.com. Under the SSL certificate field, select MovieScope from the drop-down list, and click OK.



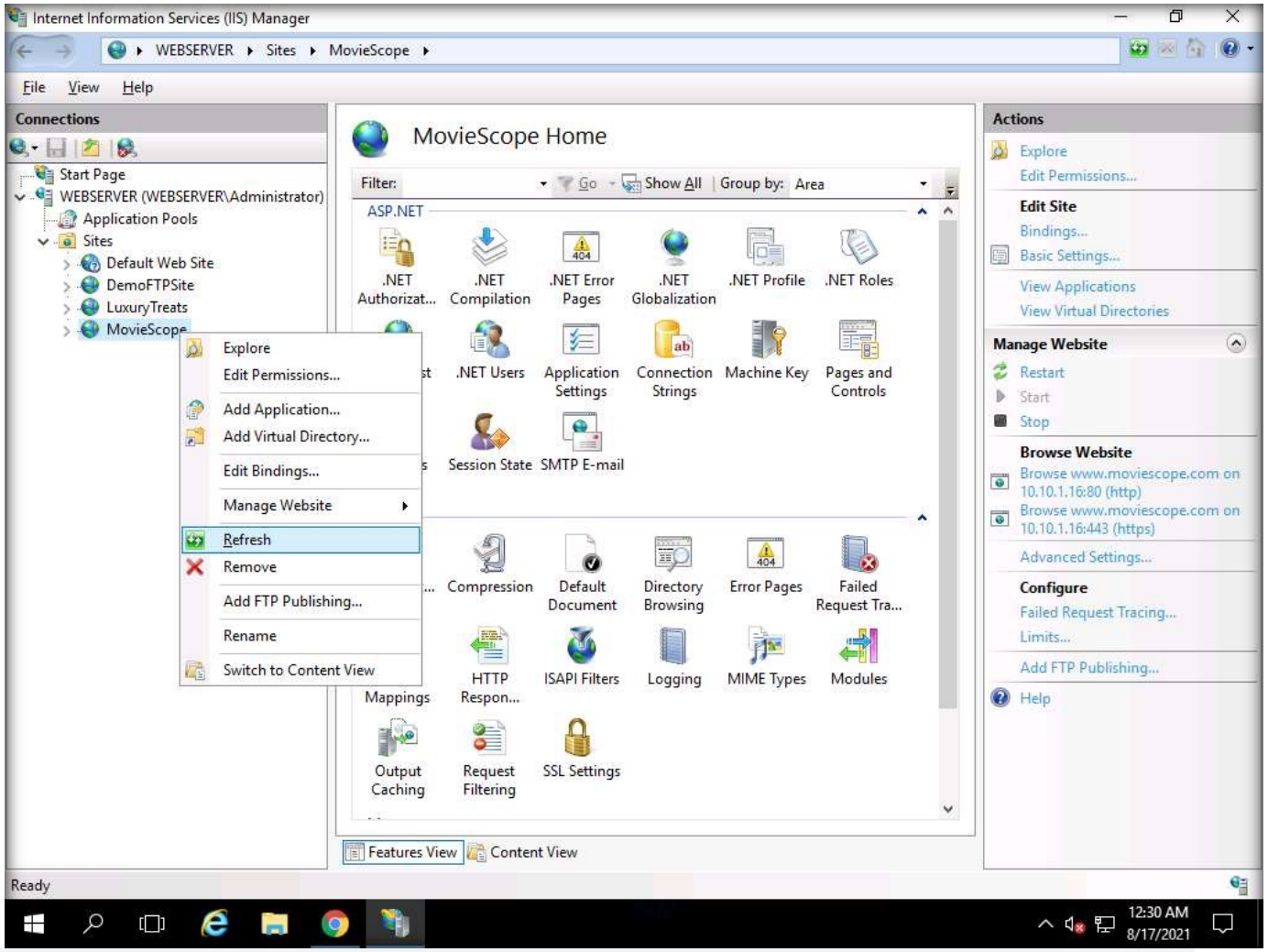
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

17. The newly created SSL certificate is added to the Site Bindings window; then, click Close.



EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

18. Now, right-click the name of the site for which you have created the self-signed certificate (here, MovieScope) and click Refresh from the context menu.

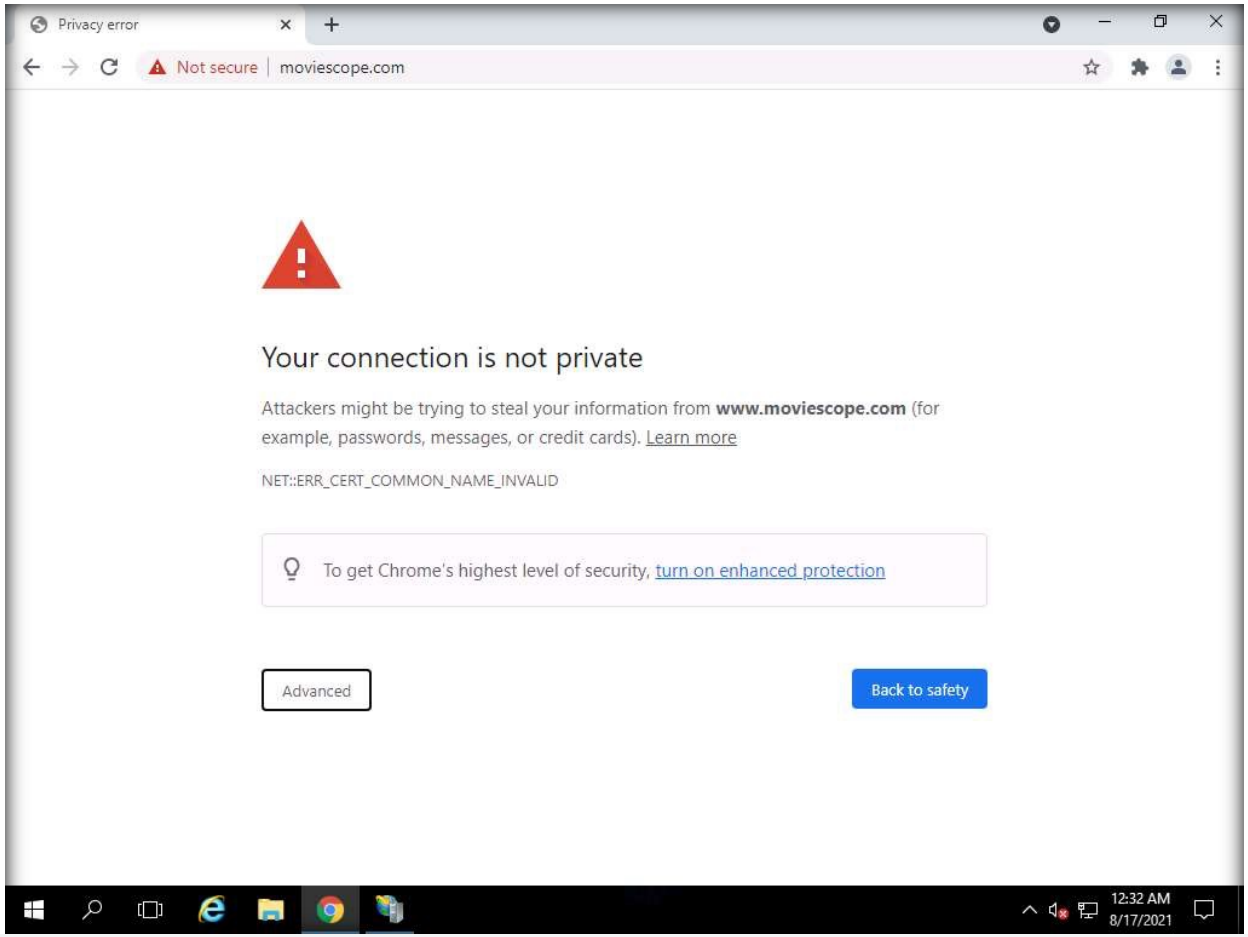


EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

19. Minimize the Internet Information Services (IIS) Manager window.

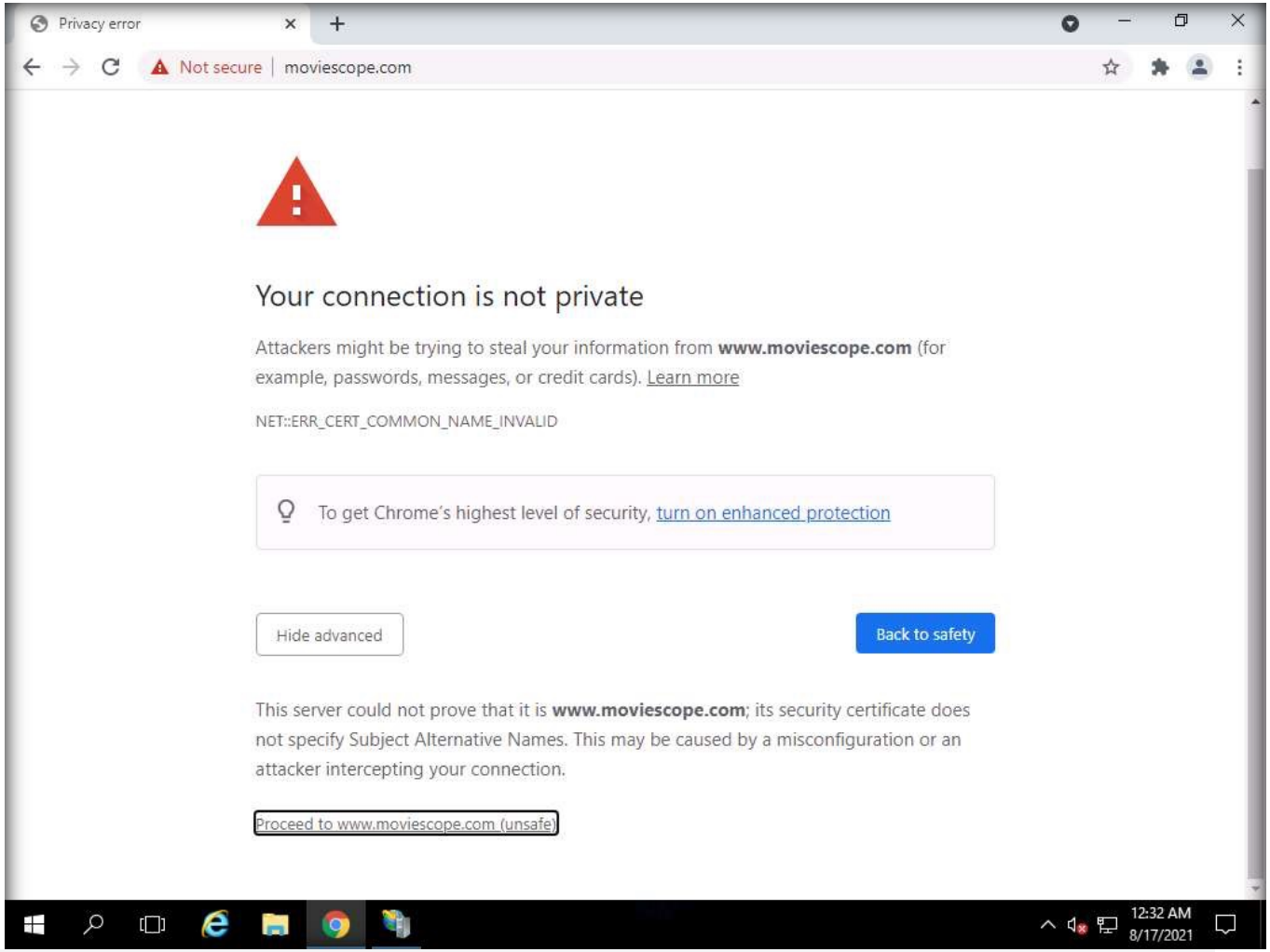
20. Open the Google Chrome browser, place the mouse cursor in the address bar and type on https://www.moviescope.com, and press Enter.

21. A message stating Your connection is not private is displayed, click ADVANCED to proceed.



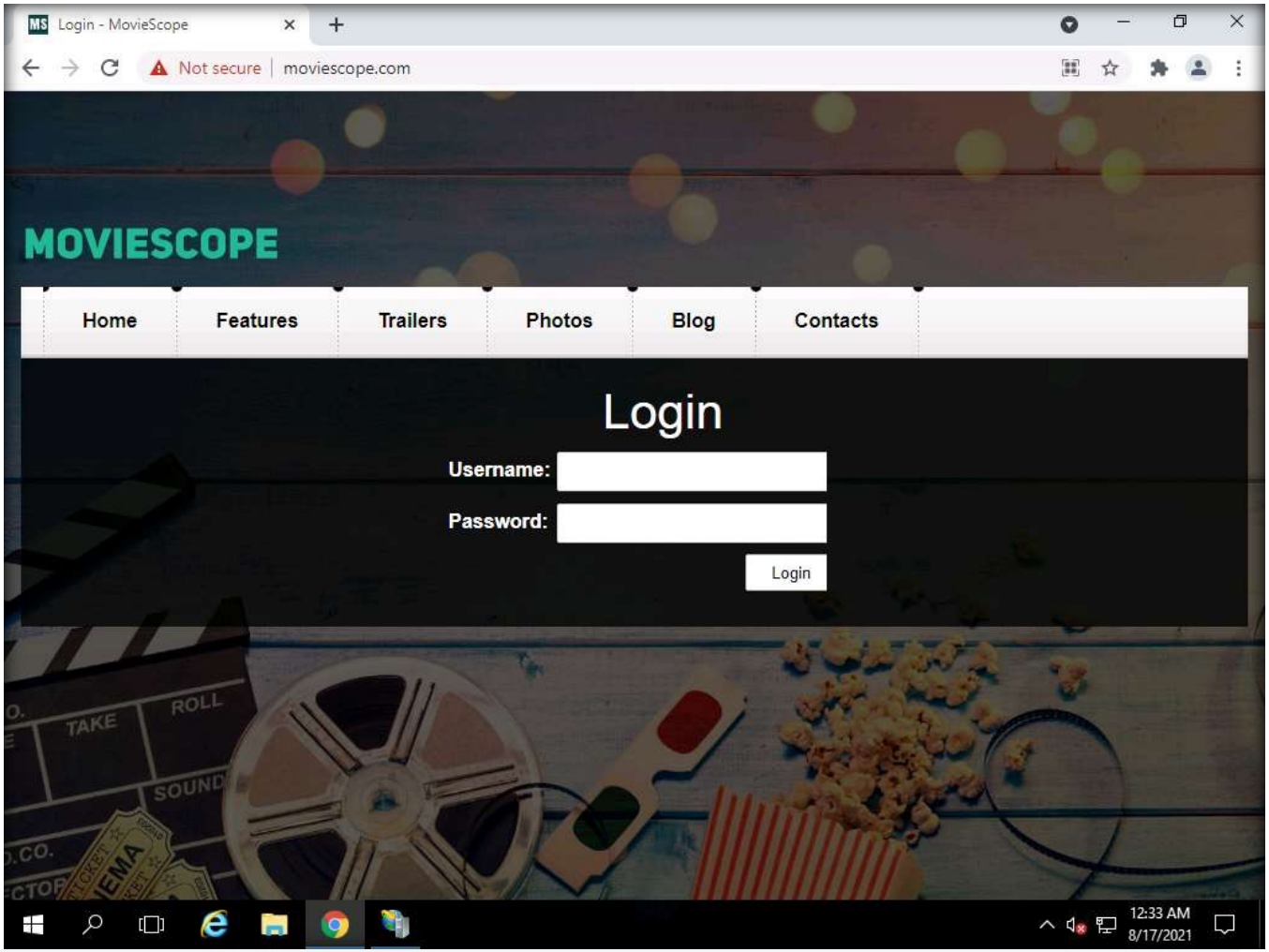
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

22. Click Proceed to www.moviescope.com (unsafe).



EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

23. You can see the Moviescope webpage with the ssl certificate assigned to it, as shown in the screenshot.



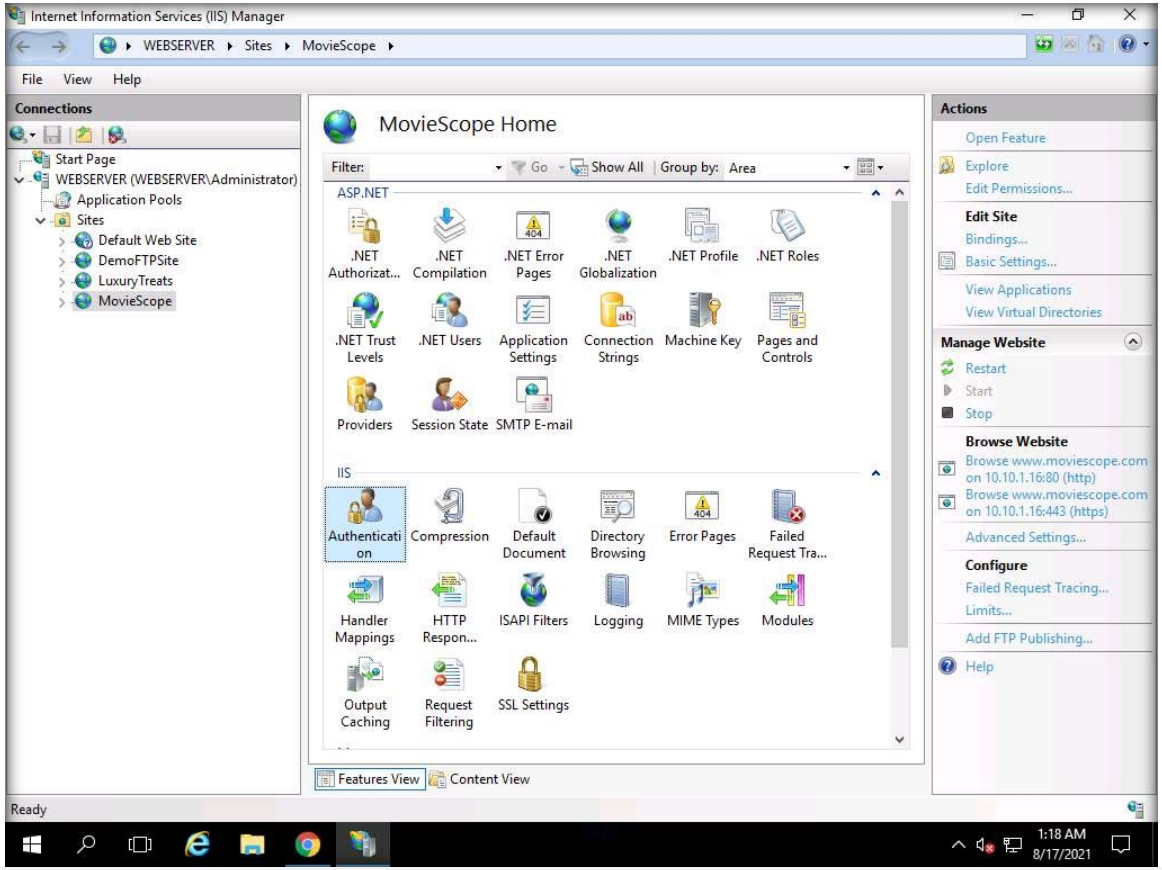
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

24. Minimize the browser window.

25. Now, we will configure an authentication policy to access the internal website.

26. Maximize the Internet Information Services (IIS) Manager window, ensure that MovieScope site is selected from the left-pane.

27. Double-click on Authentication applet under IIS section.

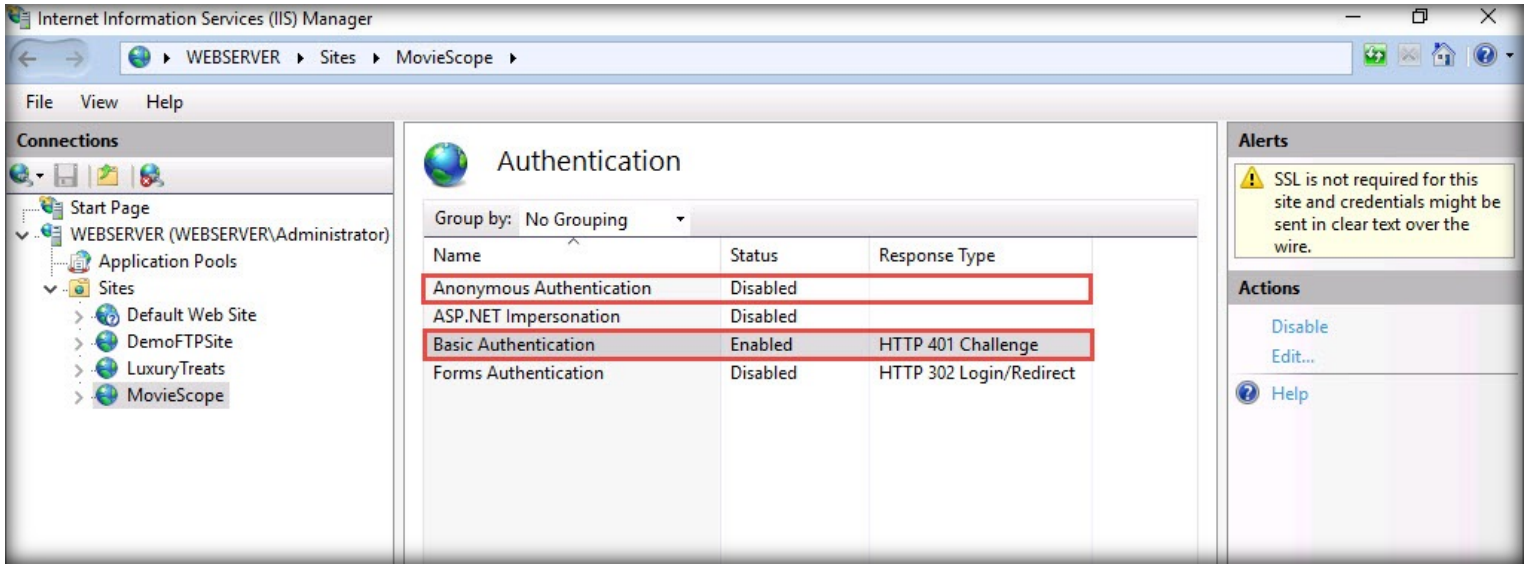


28. An Authentication wizard appears, select Anonymous Authentication and click Disable from the right-pane under Actions section.

29. Similarly, select Basic Authentication and click Enable from the right-pane under Actions section.

Note: For demonstration purpose, here, we are using Basic authentication mechanism where plaintext credentials are used to authenticate and access the website which is not a safe practice. In the real-time, it is advised to use Windows authentication which is significantly more secure than basic authentication.

EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

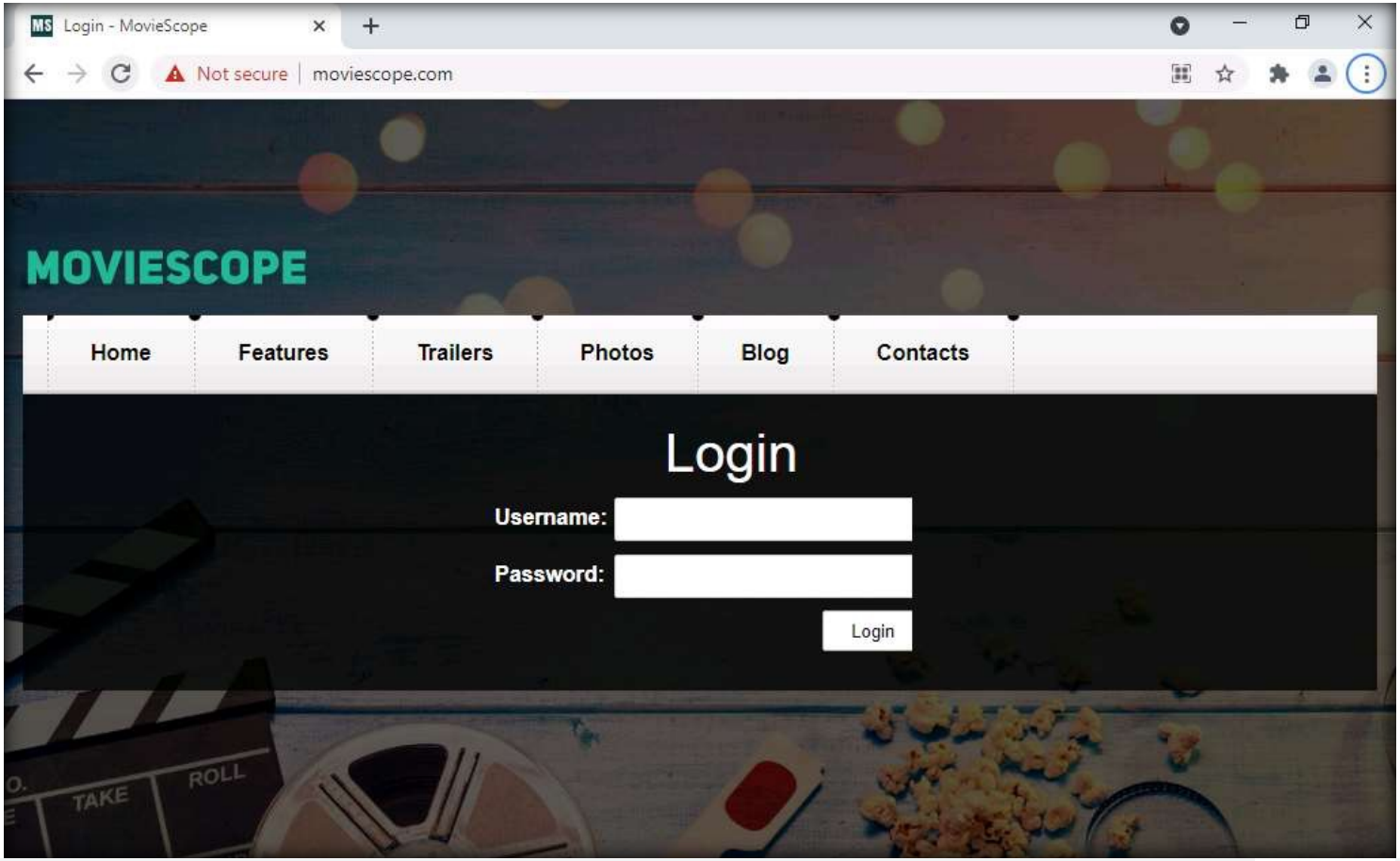


30. Now, we will browser the internal website and test the authentication policy that was implemented in the aforementioned steps.

31. Maximize the browser window.

32. Press F5 key or click the Reload this page icon to reload the web application.

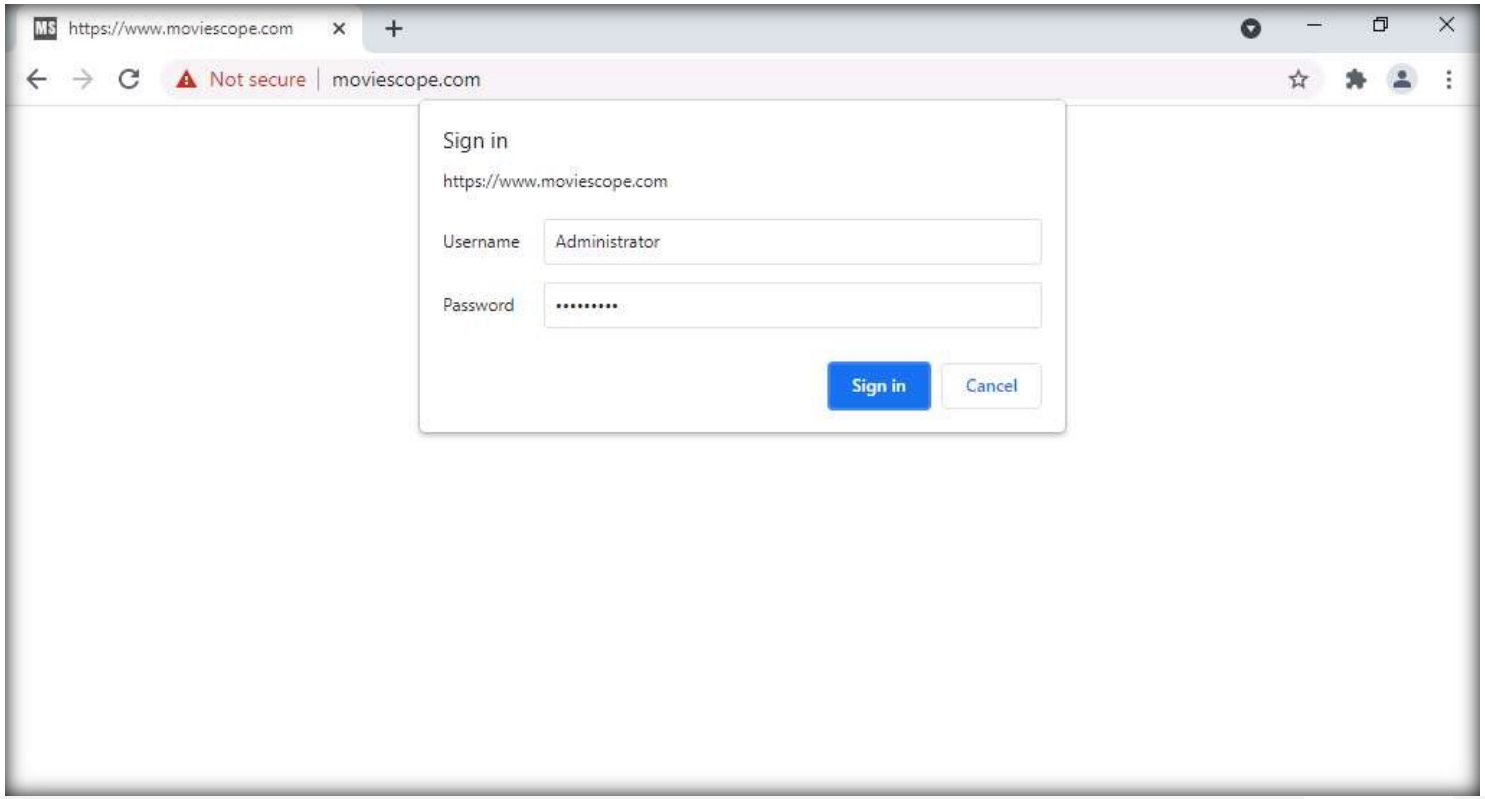
EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY



33. A Sign in pop-up appears, enter the Username and Password as Administrator and admin@123 respectively. Click Sign-in button.

Note: If prompted to save the login by Chrome appears, select Don't Save or Never Save.

EXERCISE 3: IMPLEMENT A SECURE NETWORK POLICY

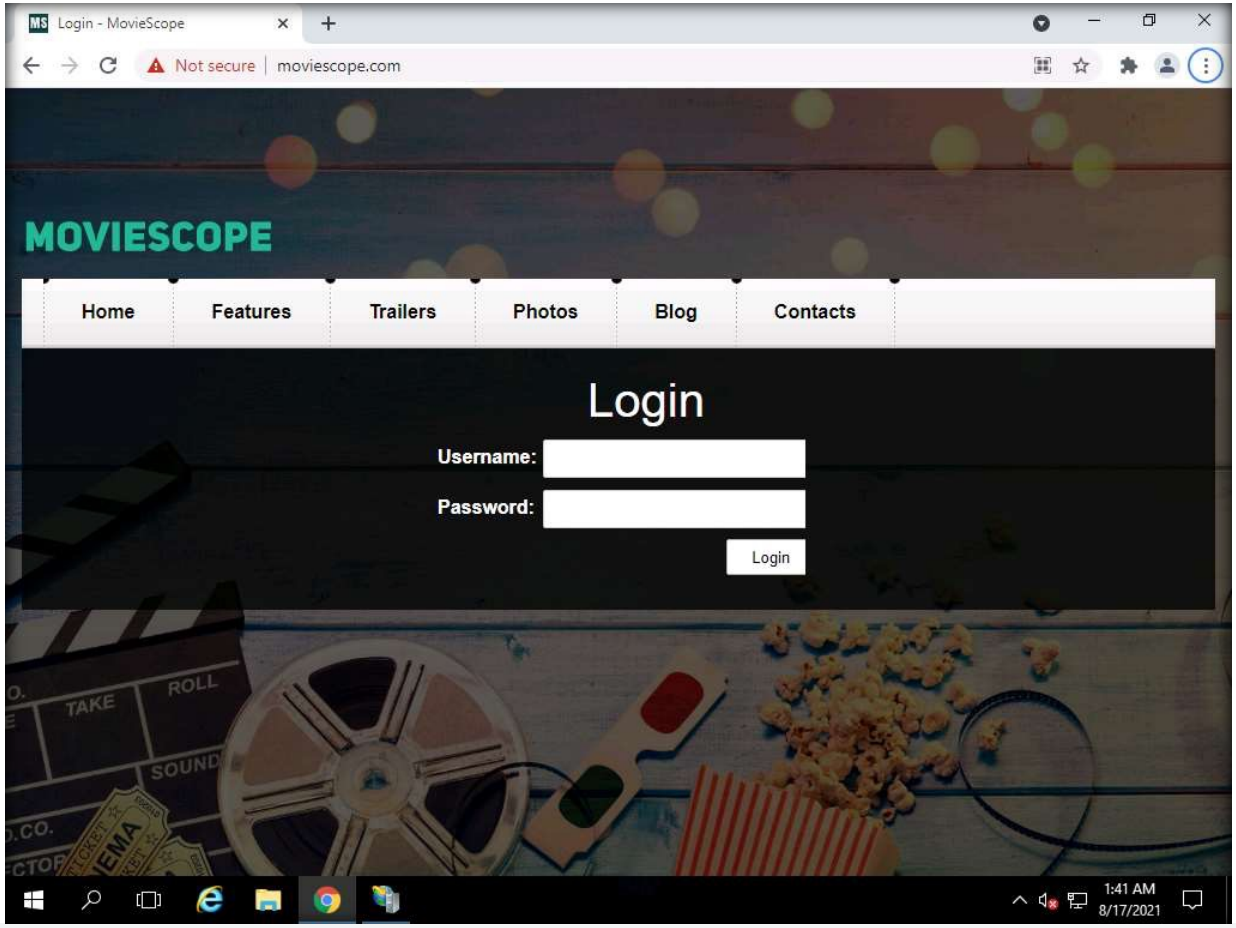


EXERCISE 3:
IMPLEMENT A
SECURE NETWORK
POLICY

34. The website appears, as shown in the screenshot.

35. Close all open windows.

36. Turn off the Web Server virtual machine.



EXERCISE 4: **IMPLEMENT A POWERSHELL SECURITY POLICY**

A security policy is a well-documented set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status of an organization

LAB SCENARIO

A security professional must know how to configure PowerShell policies for running scripts on Windows server and further create a script to determine the execution policies.

OBJECTIVE

This lab demonstrates how to implement and configure security policies for PowerShell using Group Policy.

OVERVIEW OF SECURITY POLICY

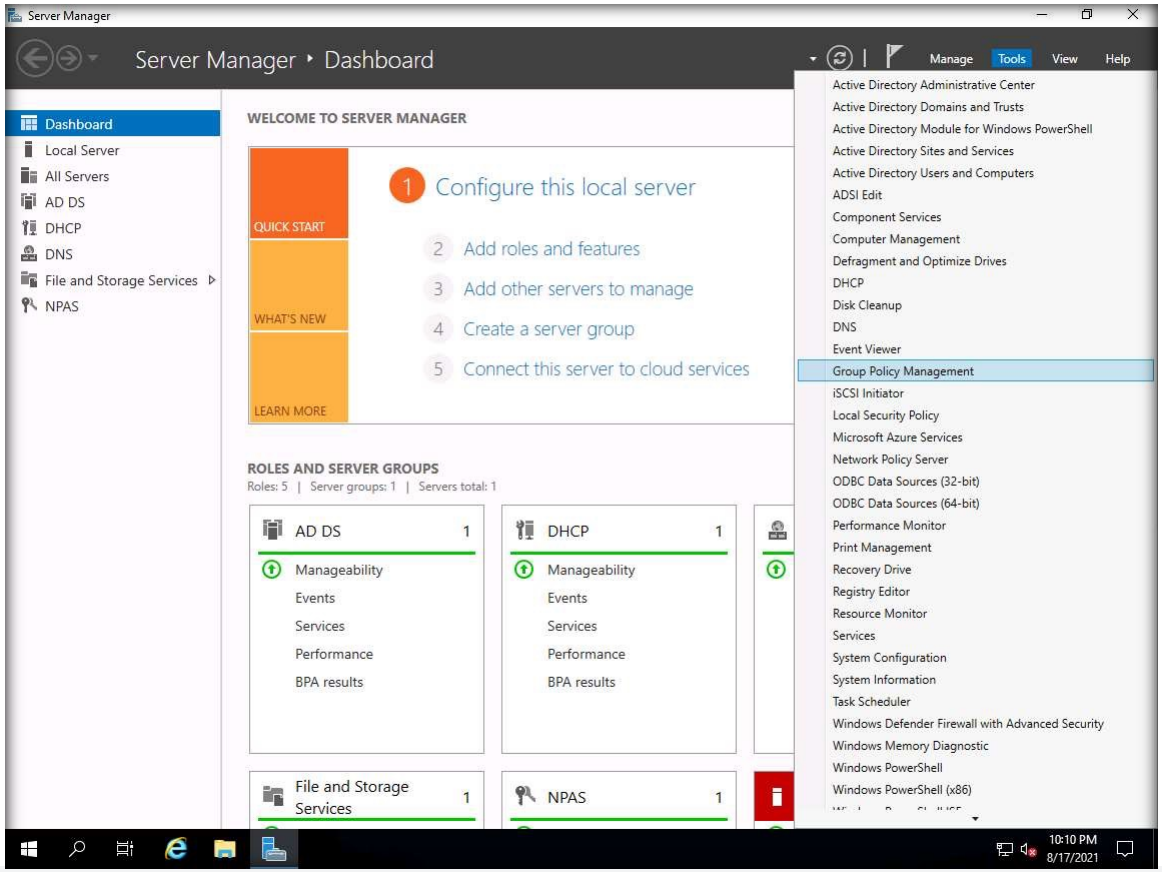
Security policies are used to inform people on how to work in a safe and secure manner; they define and guide employee actions on how to deal with sensitive operations, data, or resources in an organization. A security policy is an integral part of the information security management program in any organization

A security policy is a high-level document, or set of documents, describing the security controls that should be implemented to protect a company. It maintains confidentiality, availability, integrity, and asset values. Security policies form the foundation of a security infrastructure. Without them, it is impossible to protect any company from possible lawsuits, lost revenue, and bad publicity, or even basic security attacks.

Copyrights @ 2022 EC-Council International Ltd.

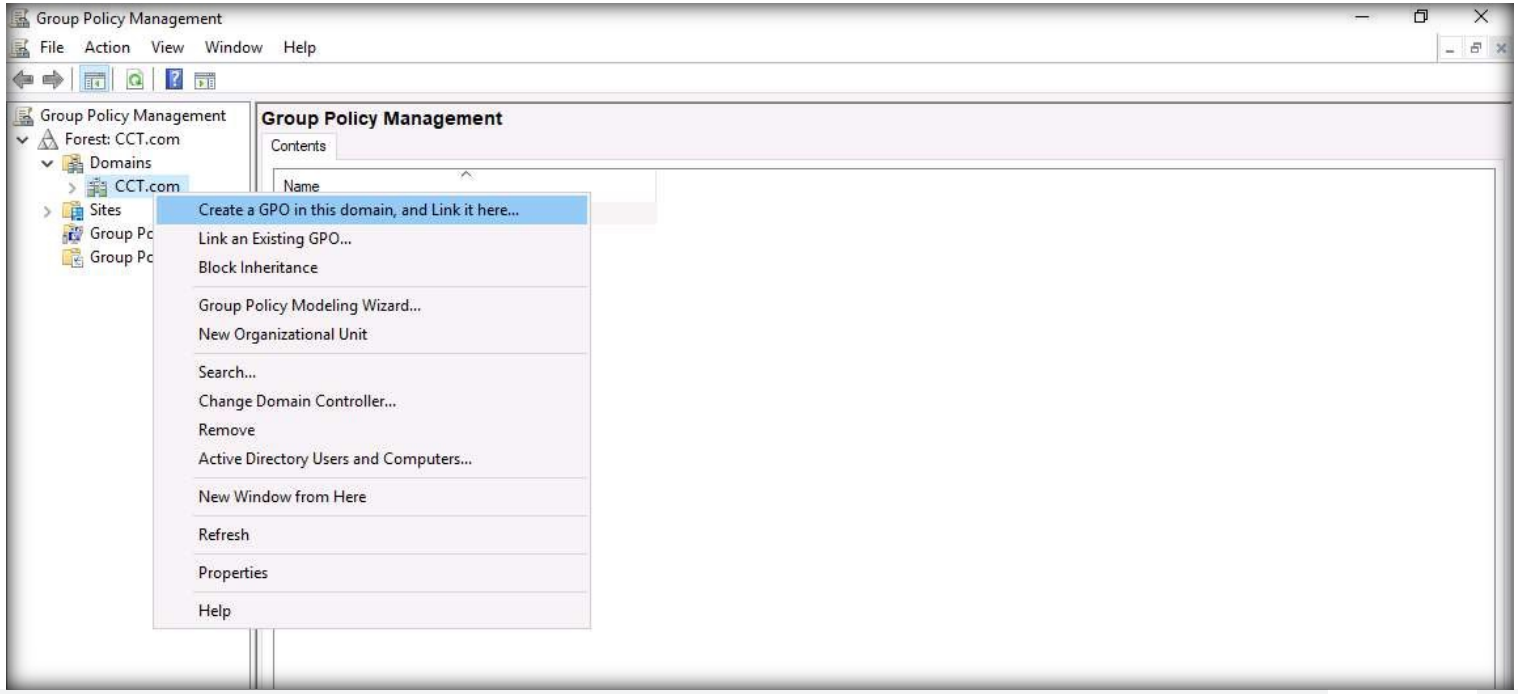
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

Note: First, we will enable logging by configuring Group Policy Object and link it to the CCT.com domain.
Note: Ensure that PfSense Firewall virtual machine is running.
1. Turn on the AD Domain Controller virtual machine.
2. Log in with the credentials CCT\Administrator and admin@123.
Note: The network screen appears, click Yes.
3. Click the Start icon and select Server Manager.
4. The Server Manager window appears. Click Tools and select the Group Policy Management option.



5. A Group Policy Management window appears, expand Forest: CCT.com node and Domains node. Right-click CCT.com node and select Create a GPO in this domain, and Link it here... option.

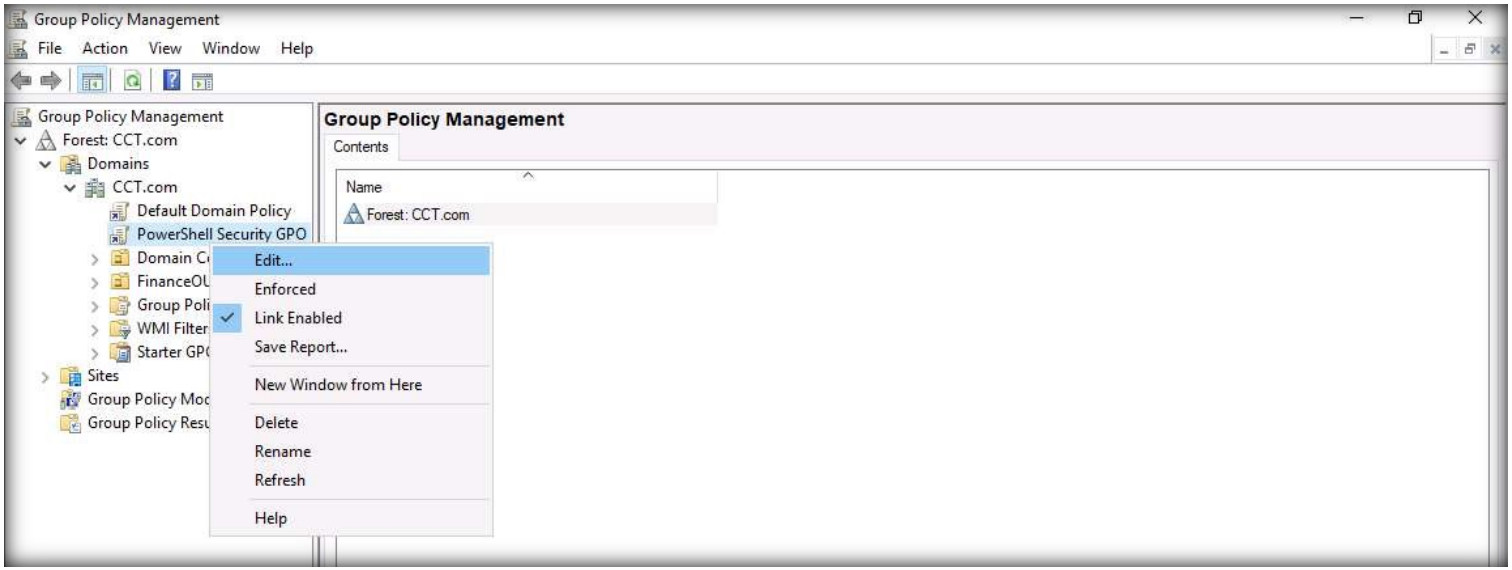
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



6. A New GPO dialog-box appears, in the Name field, type PowerShell Security GPO and click OK.

7. Now, expand the CCT.com node, right-click PowerShell Security GPO and select Edit... option.

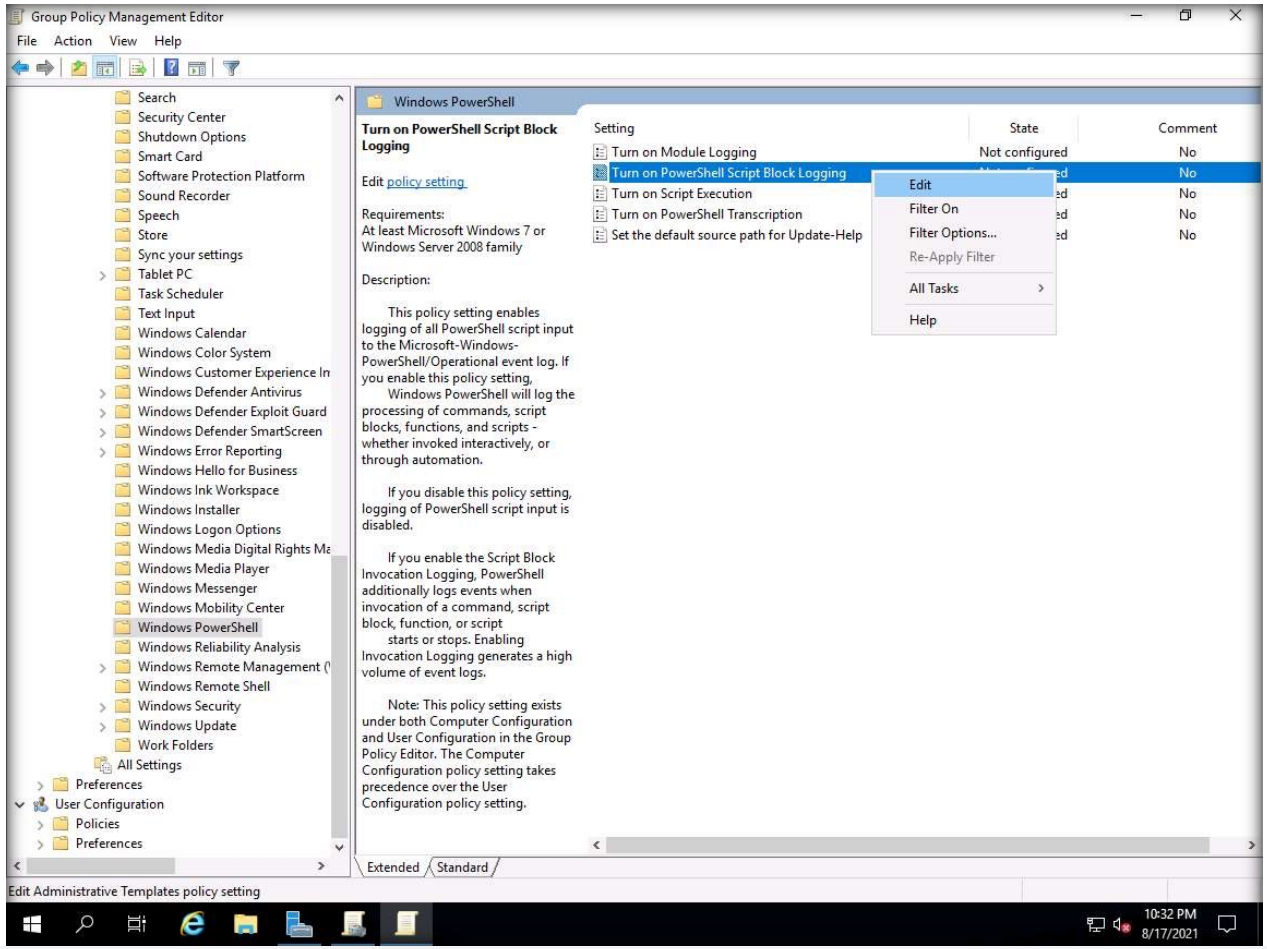
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

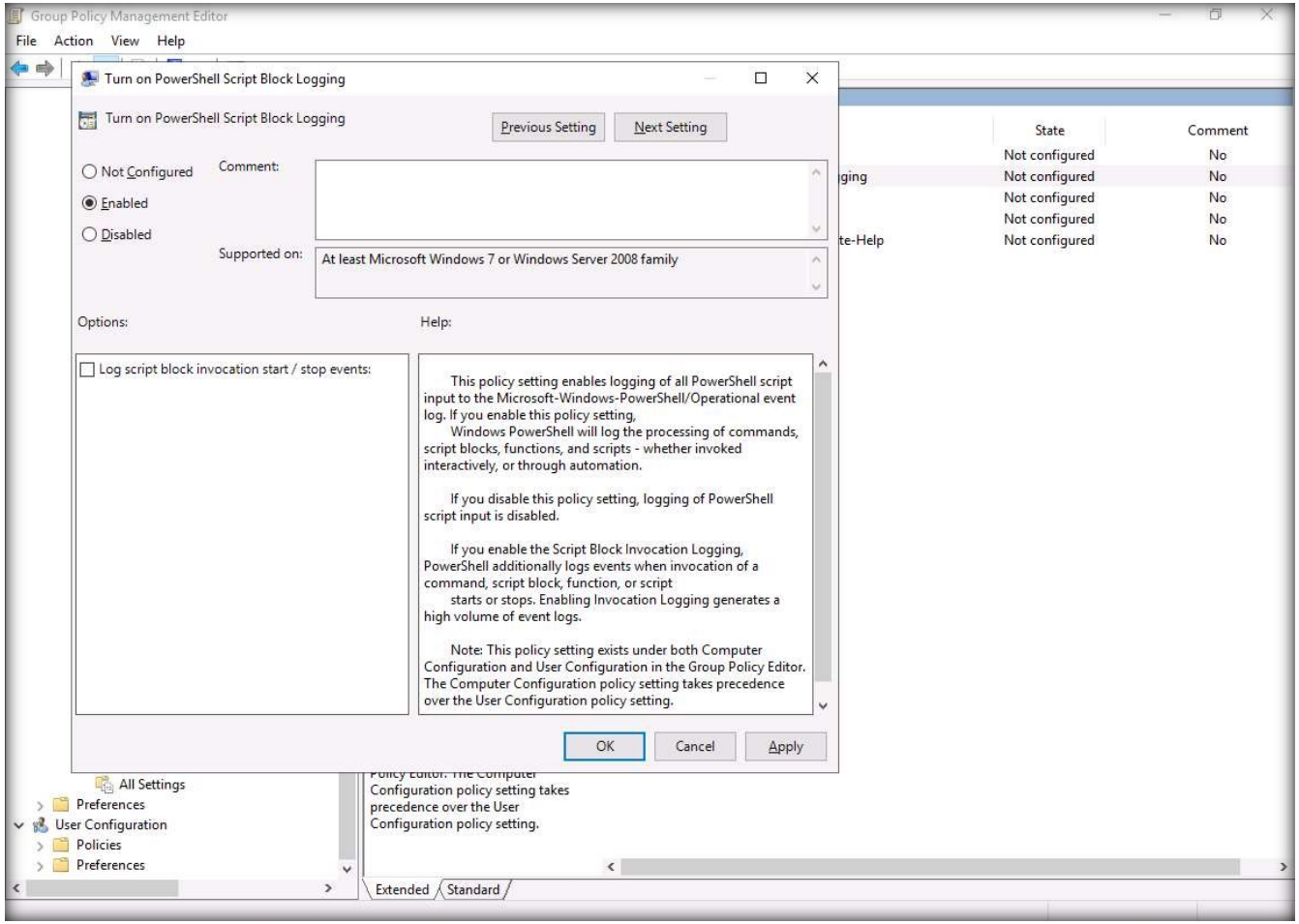
8. The Group Policy Management Editor window appears, in the left-pane navigate to Computer Configuration → Policies → Administrative Templates → Windows Components → Windows PowerShell.

9. In the PowerShell policies, right-click Turn on PowerShell Script Block Logging setting, and then click Edit.



10. A Turn on PowerShell Script Block Logging window appears, select the Enabled radio button and then click Apply. Then, click OK to close the window.

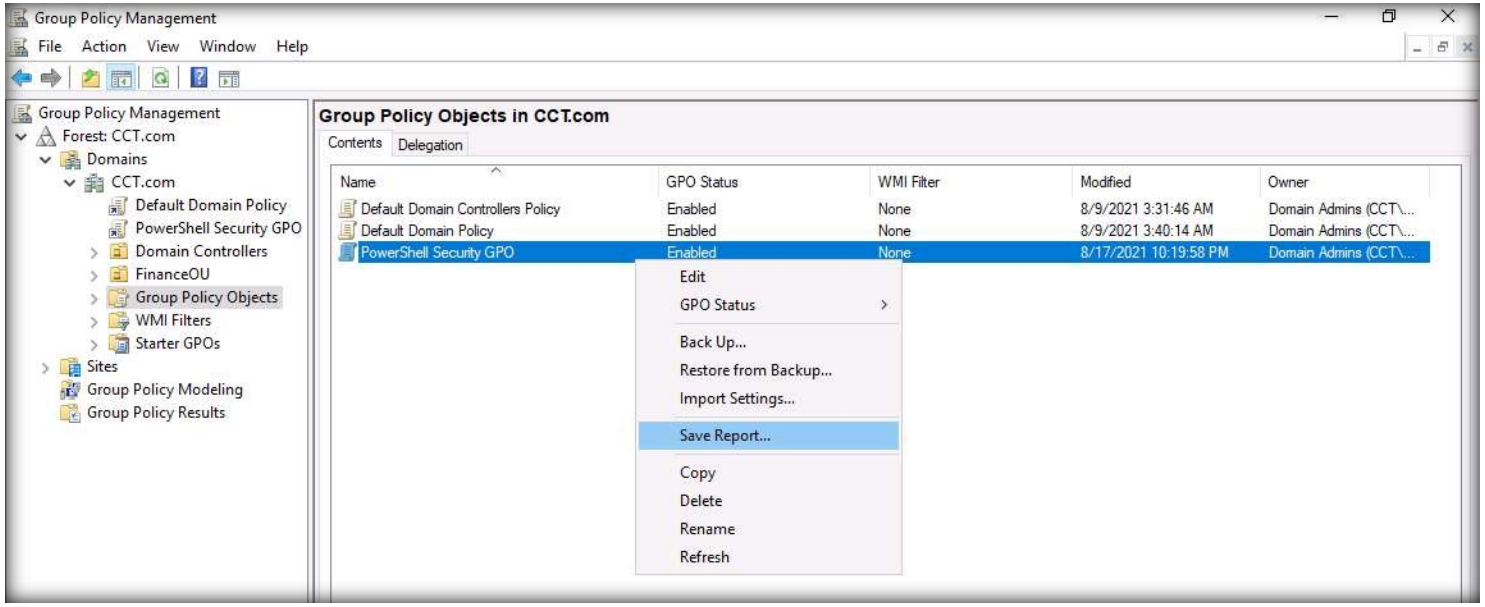
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



11. Close the Group Policy Management Editor window and switch to Group Policy Management window.

12. From the left-pane, click to select the Group Policy Objects node. In the right-pane, right-click the PowerShell Security GPO, and select Save Report....

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

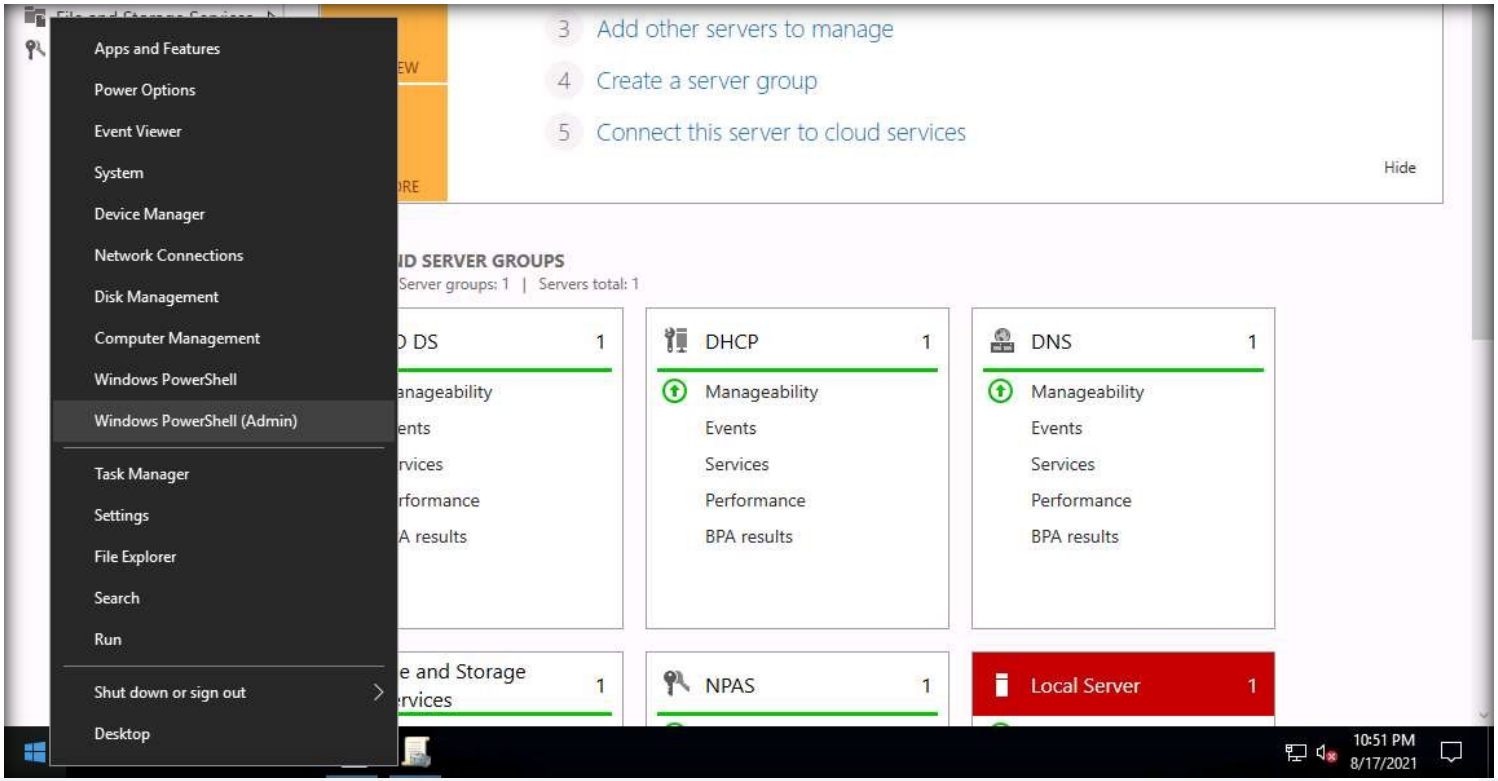


13. A Save GPO Report window appears, select the location as Desktop and click Save.

14. Minimize the Group Policy Management window.

15. Right-click Start icon and select the Windows PowerShell (Admin) option.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



16. An Administrator: Windows PowerShell window appears, type gpupdate /force and press Enter.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

17. Next, a message stating that the user policy has been updated successfully appears.

18. Minimize the PowerShell window.

19. Now, we will configure execution control policies for PowerShell in the AD Domain Controller machine.

Note: Execution policy table for PowerShell is given below:

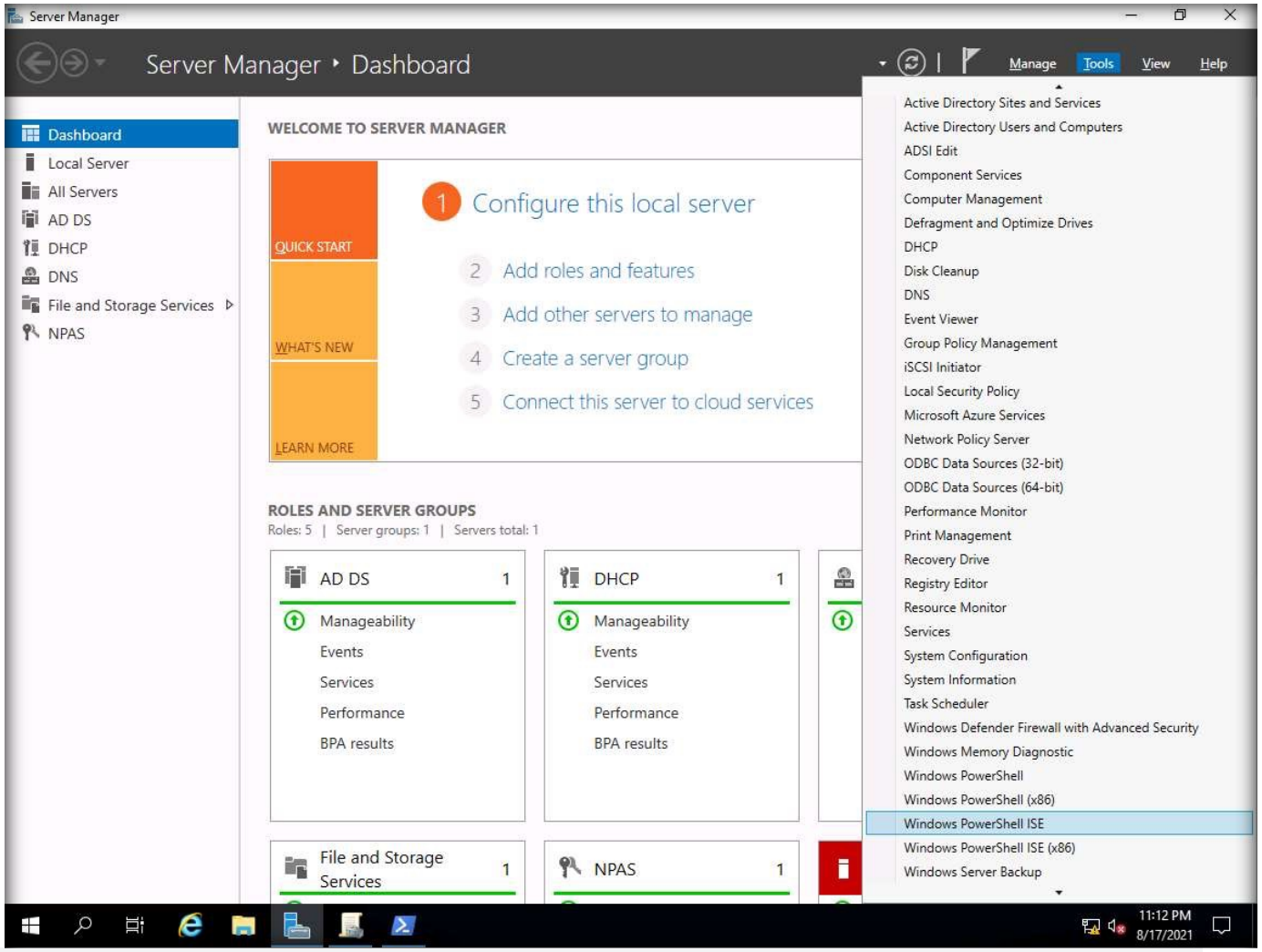
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

Setting	Description
Unrestricted	No requirements; all scripts allowed
RemoteSigned	Local scripts allowed; remote scripts must be signed
AllSigned	Local and remote scripts must be signed
Restricted	No scripts allowed

Copyrights @ 2022 EC-Council International Ltd.

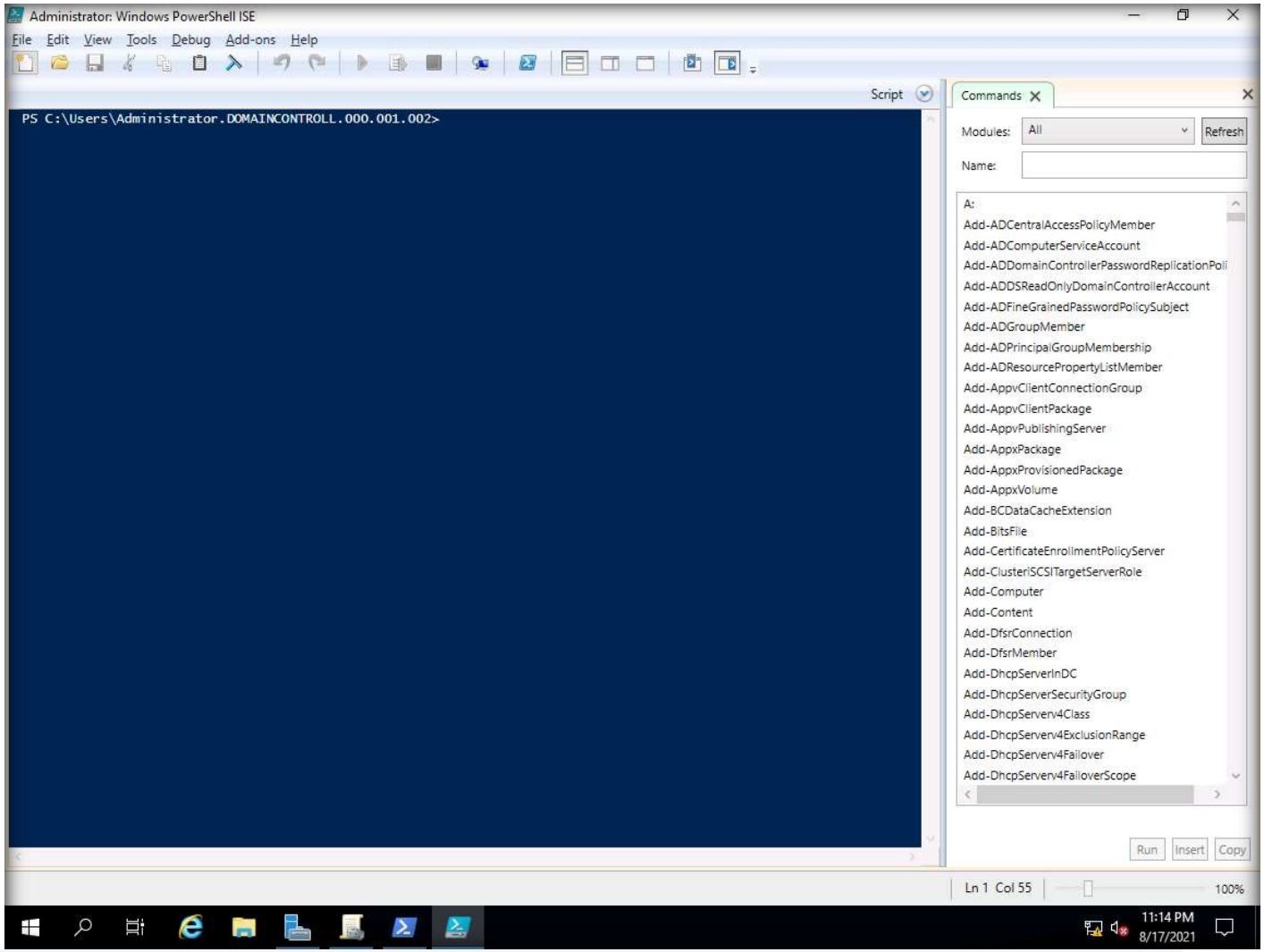
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

20. In the Server Manager window, Click Tools and select the Windows PowerShell ISE option.



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

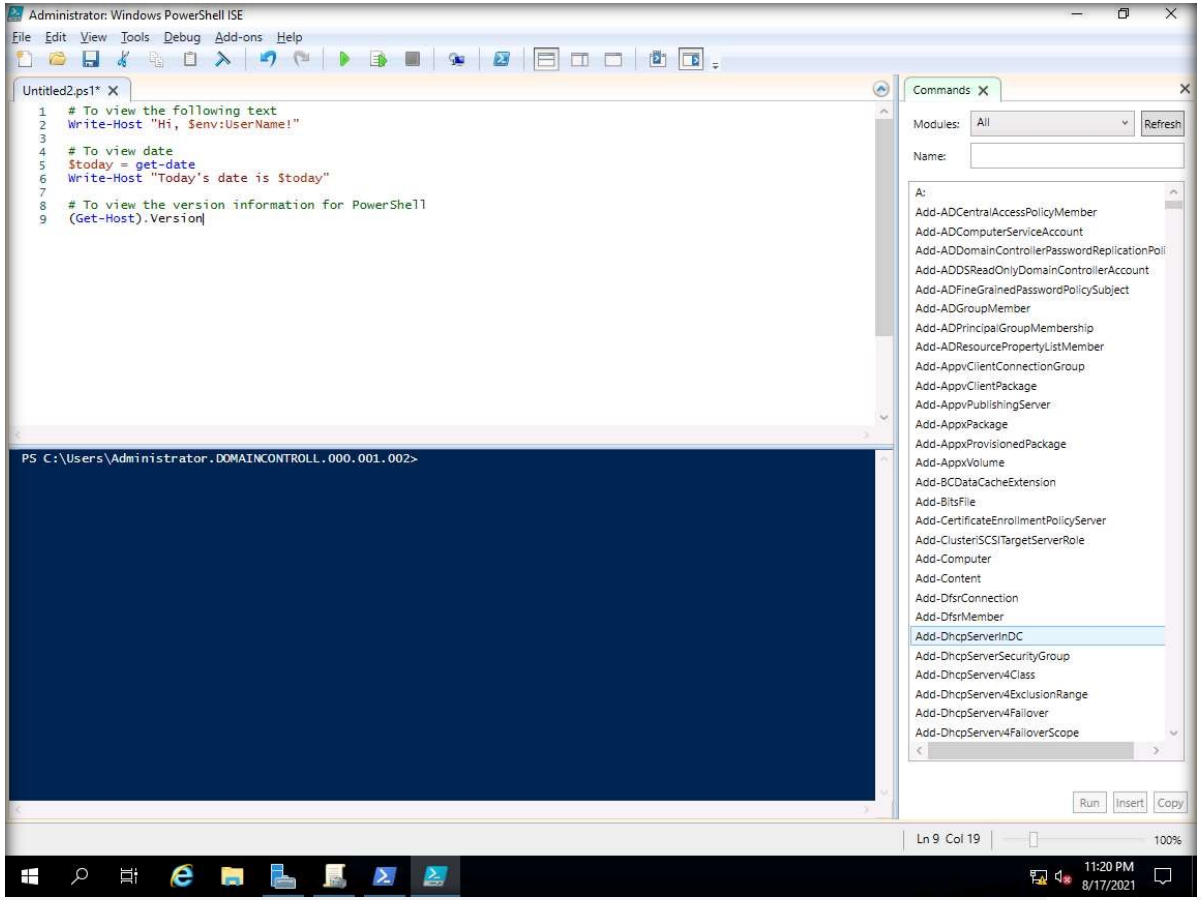
21. An Administrator: Windows PowerShell ISE window appears, click New Script icon ( ) from the tool bar to open a text editor.



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

22. An Untitled.ps1 script pane appears, type the following script:
Note: You can use the auto-type feature to type the following script automatically in the script pane.

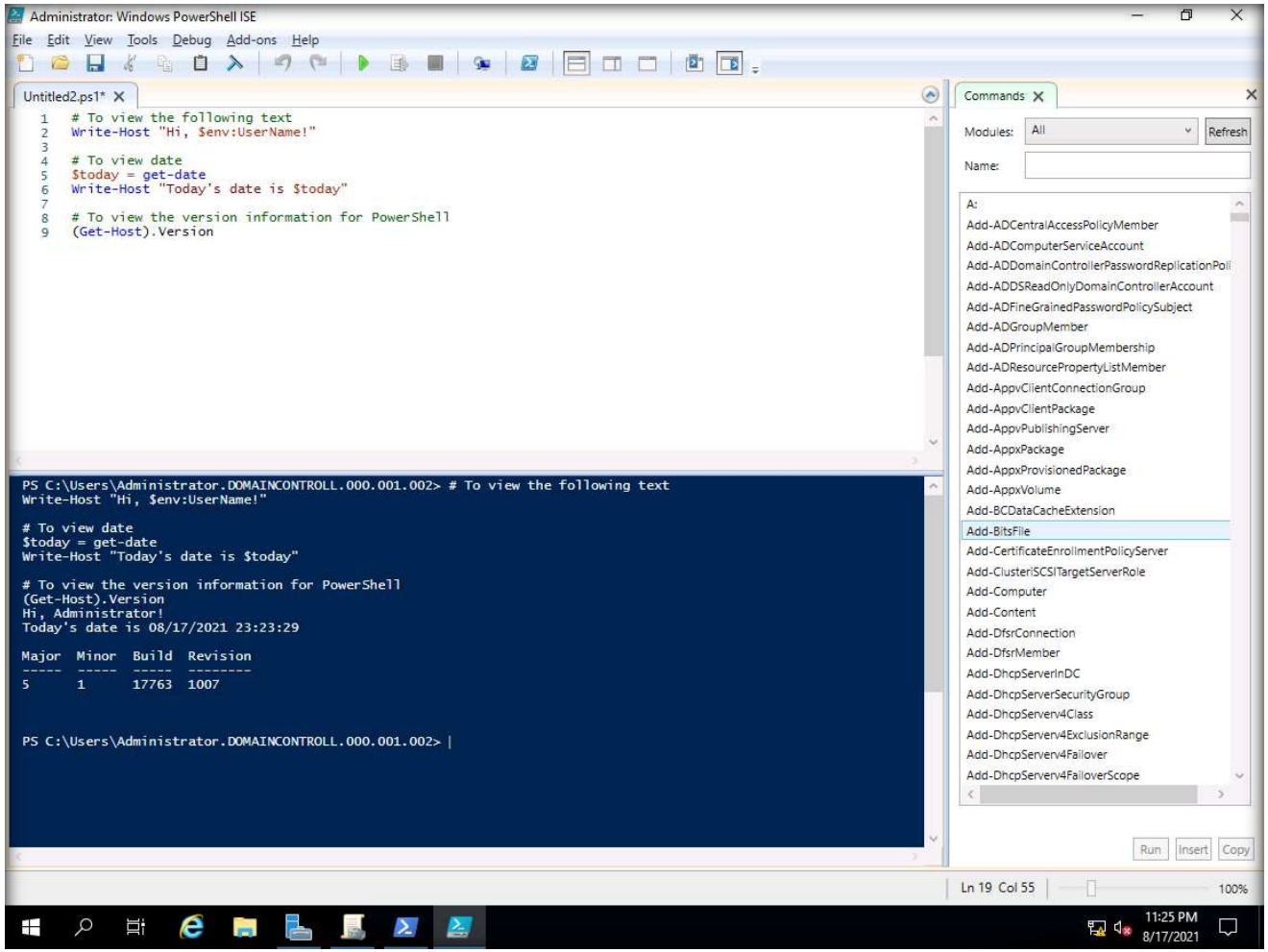
```
# To view the following text
Write-Host “Hi, $env:UserName!”

# To view date
$today = get-date
Write-Host “Today’s date is $today”
```



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

23. Now, from the toolbar, click Run Script (F5) icon ( ) to execute the script.

24. It can observed that the script has been executed and the script content is displayed in the lower-section of the window.



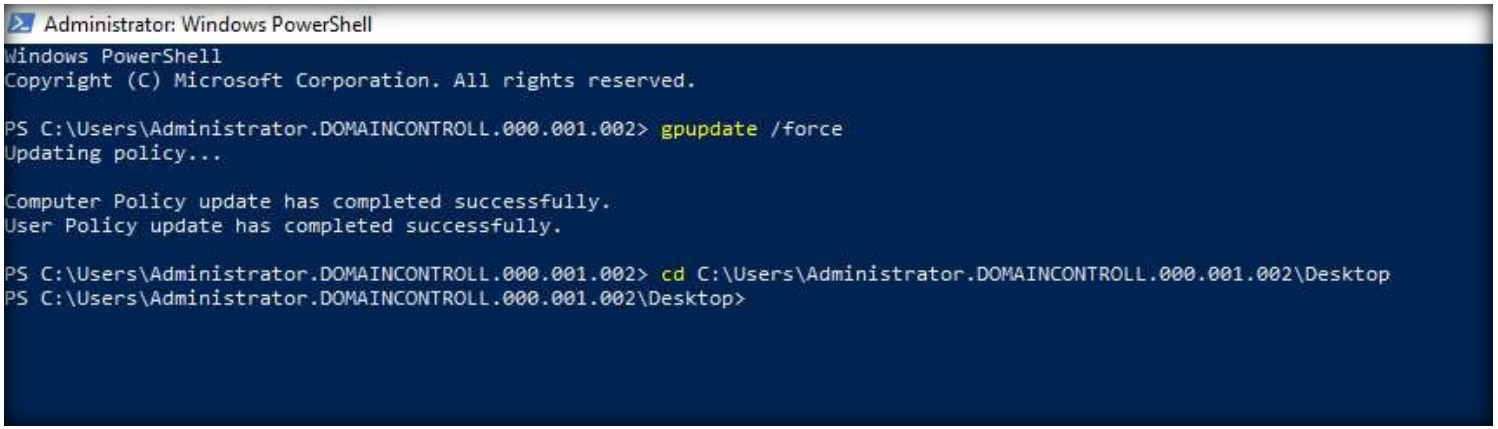
25. Press Ctrl+S to save the script.

26. A Save As window appears, name the file as PSTest.ps1 and select the location as Desktop. Click Save button.

27. Close the PowerShell ISE window.

28. Now, maximize the Administrator: Windows PowerShell window and type cd C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop; then, press Enter to change the working directory to Desktop.

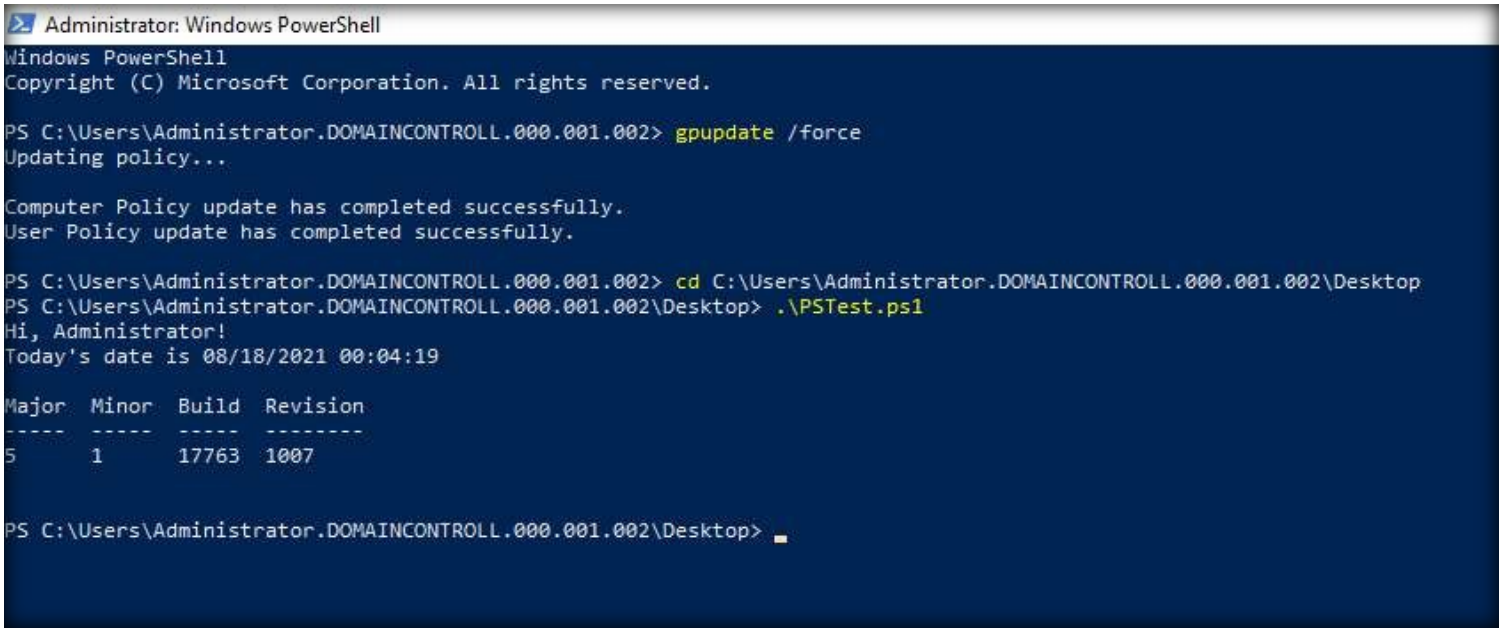
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



29. Type .\PSTest.ps1 and press Enter to execute the script.

30. It can be observed that the script is executed successfully and the username and date are displayed, as shown in the screenshot.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

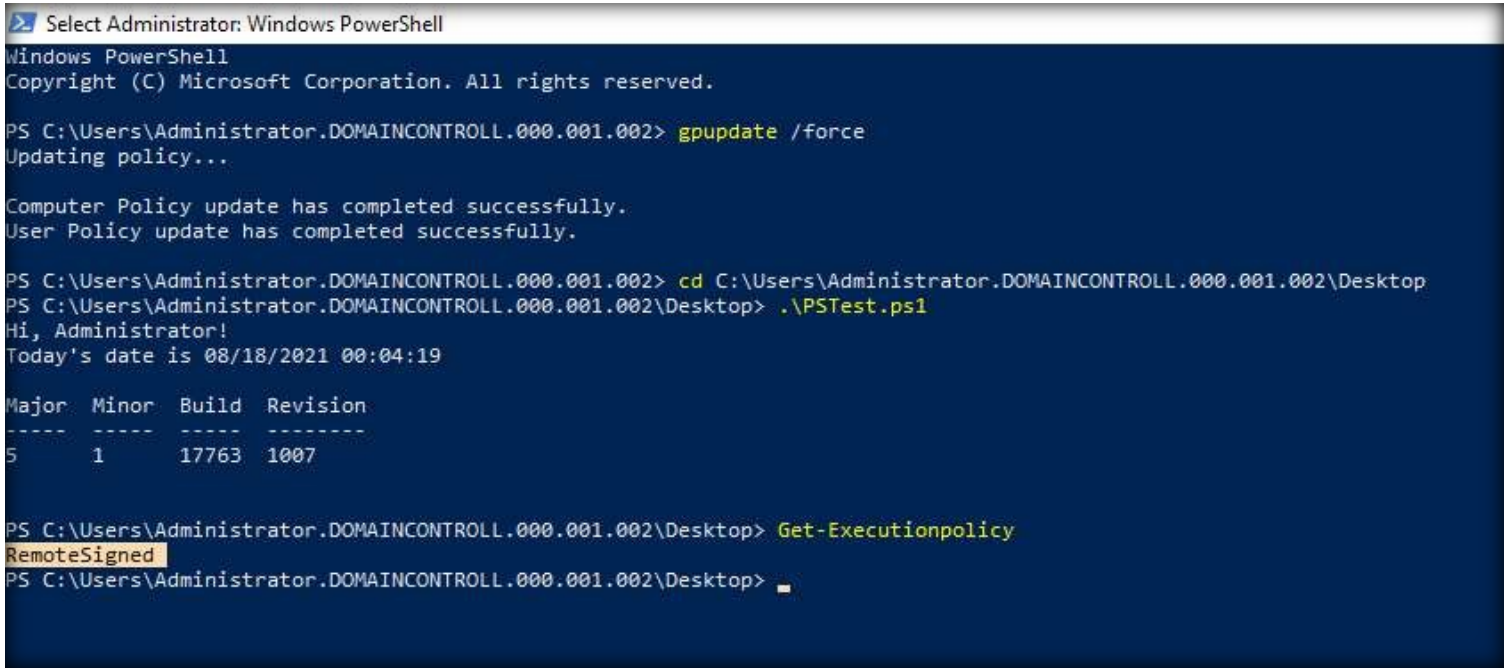


31. Now, type Get-Executionpolicy and press Enter to display the current execution control policy implemented on the system.

32. Here, the RemoteSigned execution control policy is used, as shown in the screenshot.

Note: The scripts which are created internally or on a personal system must be signed digitally or they can be signed with a self-signed certification. However, the scripts which are downloaded from the internet or from the online sources must be digitally signed by a source. Here, we will set the execution policy to AllSigned.

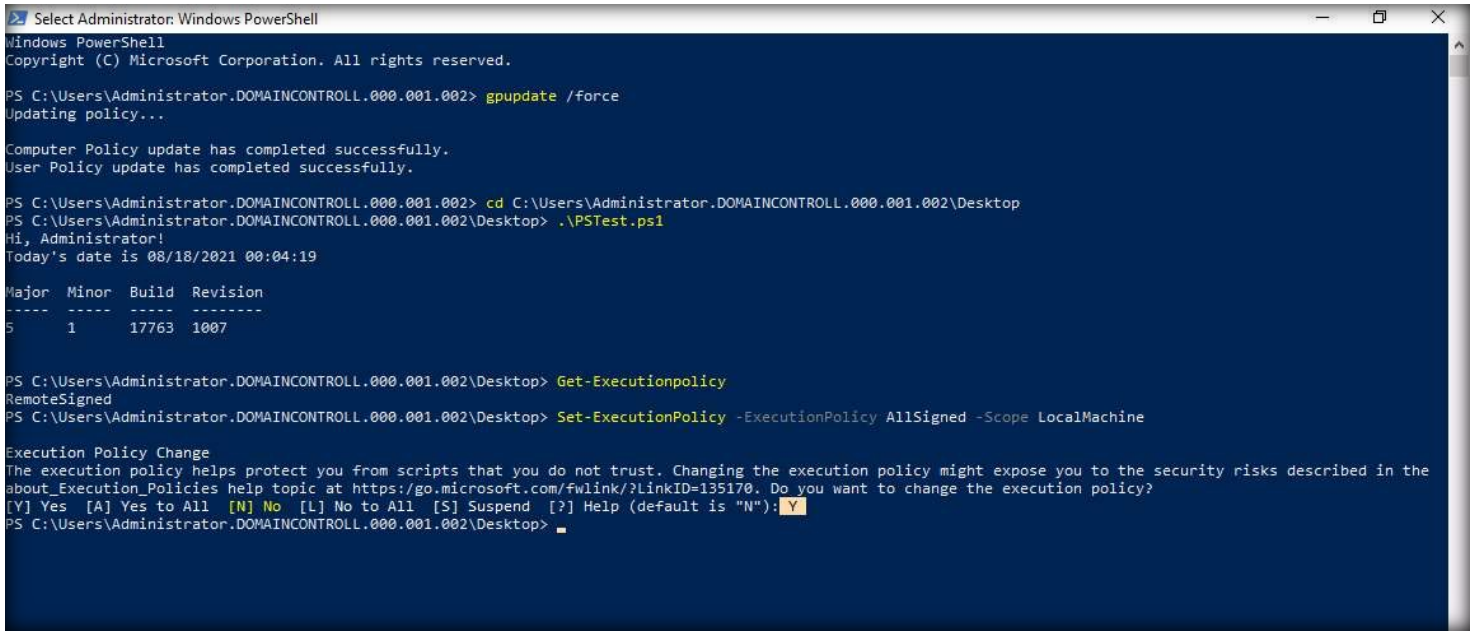
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



33. Type Set-ExecutionPolicy -ExecutionPolicy AllSigned -Scope LocalMachine and press Enter to configure the execution policy to AllSigned.

34. When prompted, type Y and press Enter for the confirmation.

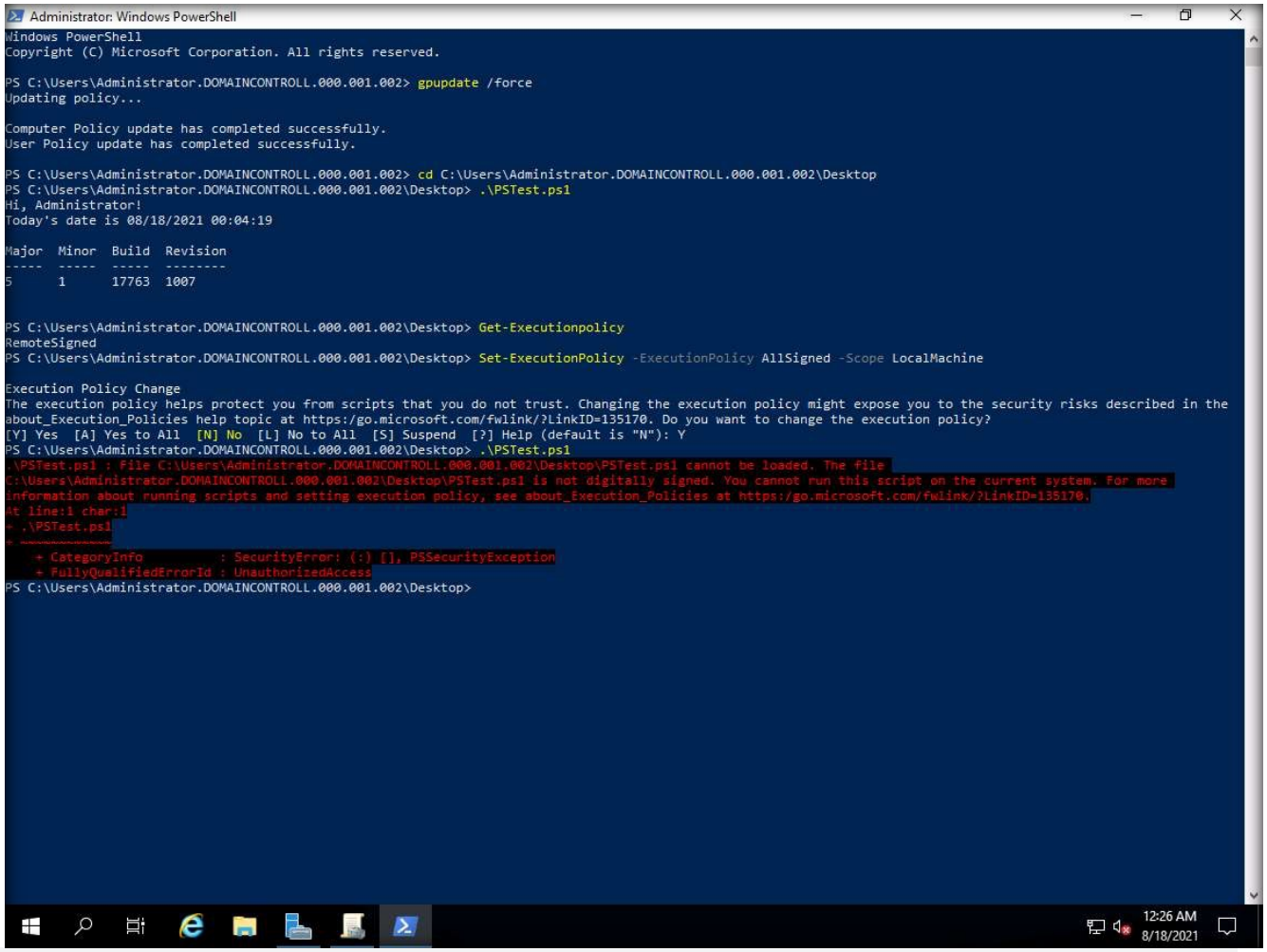
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

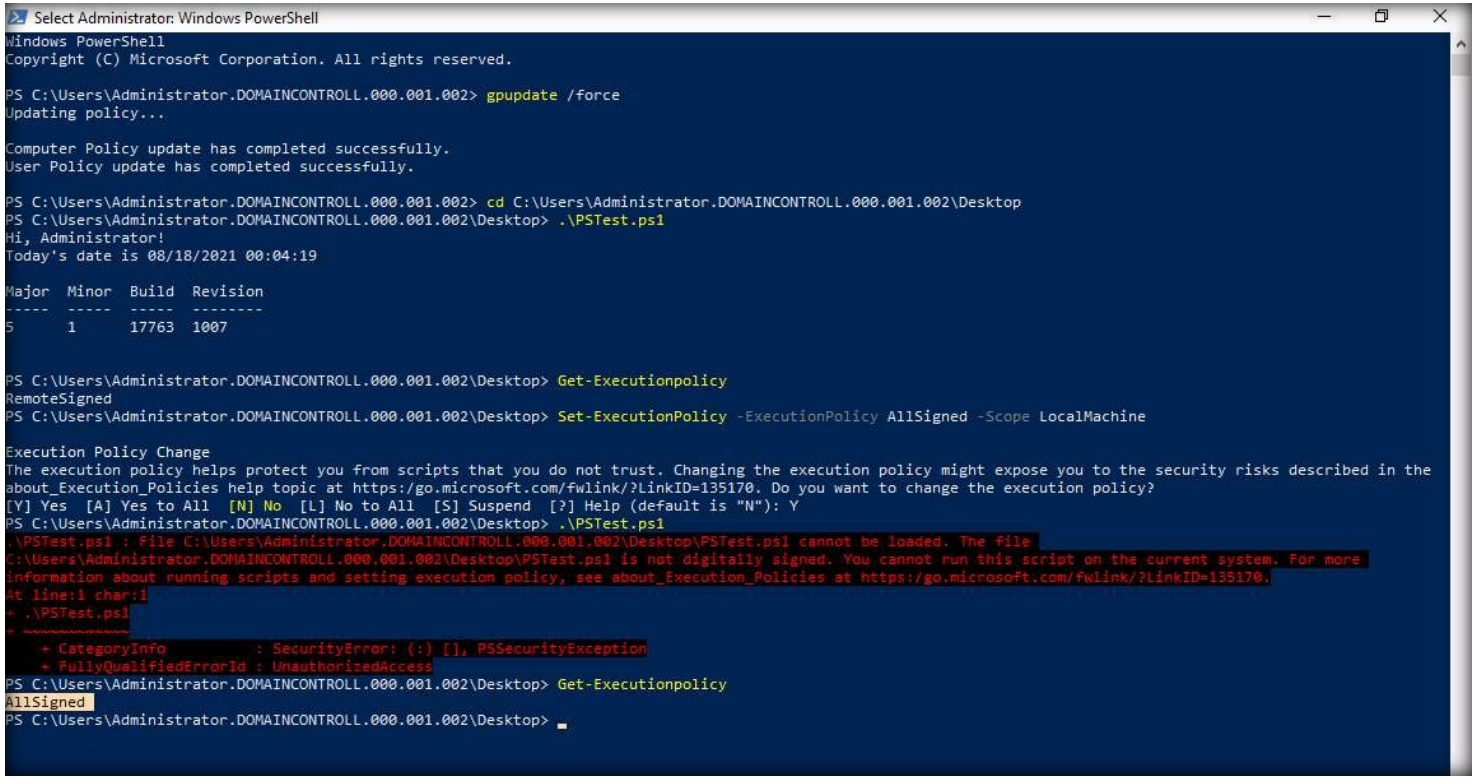
35. Now, type .\PSTest.ps1 and press Enter to execute the script again.

36. It can be observed that an error occurs and the script is not executed properly because it is not digitally signed.



37. Type Get-Executionpolicy and press Enter to confirm that the execution policy is set to AllSigned.

EXERCISE 4:
IMPLEMENT A
POWERSHELL
SECURITY POLICY



38. Type Get-AuthenticodeSignature -FilePath C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop\PSTest.ps1 and press Enter to display the Status of PSTest.ps1 script.

39. The Status was found to be NotSigned.

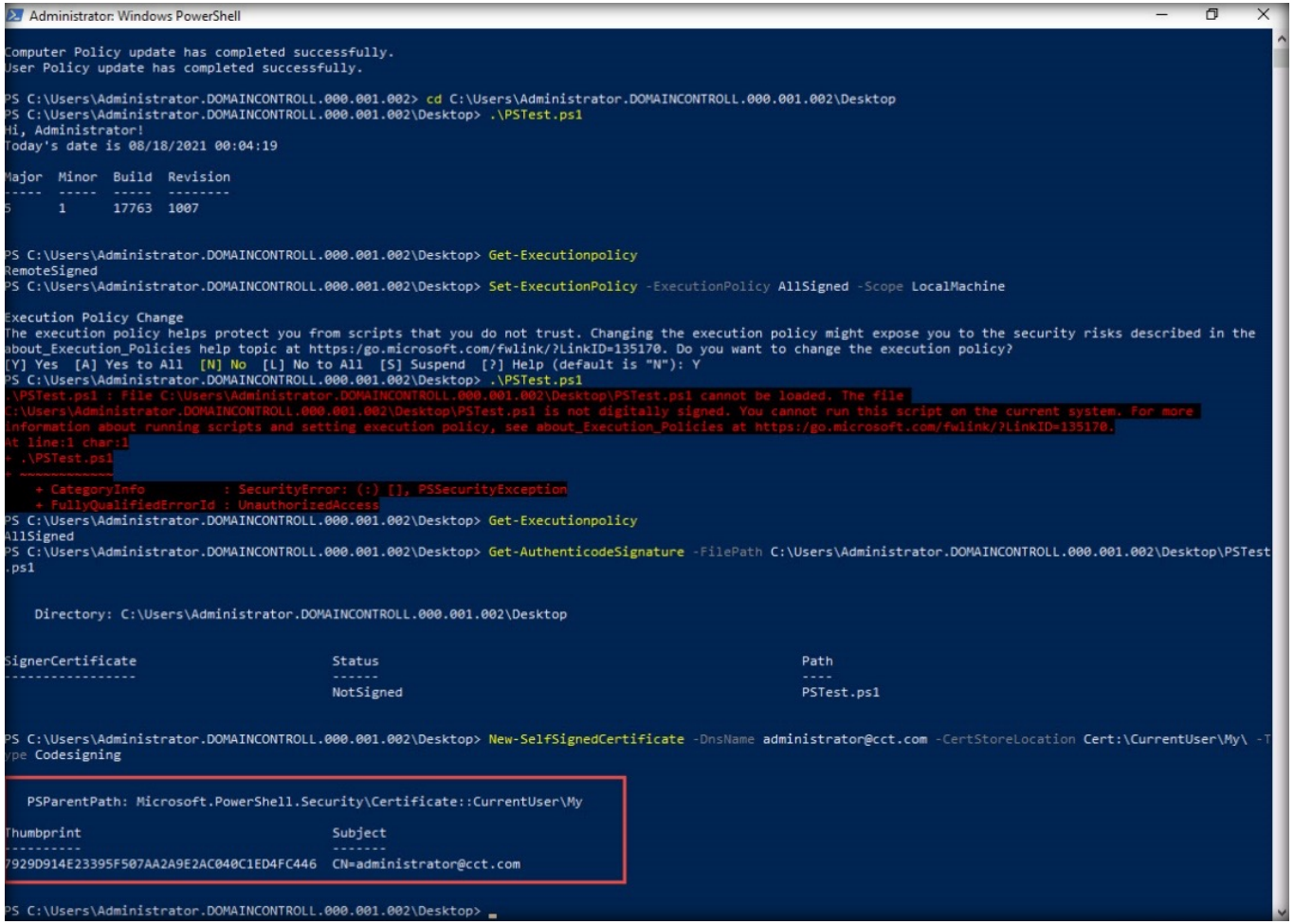
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

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

PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002> cd C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop> .\PSTest.ps1
Hi, Administrator!
Today's date is 08/18/2021 00:04:19

Major  Minor  Build  Revision
-----  -----  -----  --------
5      1      17763  1007


PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop> Get-Executionpolicy
RemoteSigned
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop> Set-ExecutionPolicy -ExecutionPolicy AllSigned -Scope LocalMachine

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the
about_Execution_Policies help topic at https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop> .\PSTest.ps1
.\PSTest.ps1 : File C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop\PSTest.ps1 cannot be loaded. The file
C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop\PSTest.ps1 is not digitally signed. You cannot run this script on the current system. For more
information about running scripts and setting execution policy, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\PSTest.ps1
+ ~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop> Get-Executionpolicy
AllSigned
PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop> Get-AuthenticodeSignature -FilePath C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop\PSTest
.ps1


    Directory: C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop


SignerCertificate                         Status                                                  Path
-----------------                         ------                                                  ----
                                          NotSigned                                               PSTest.ps1


PS C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop>
```

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

40. Now, we will digitally sign the PowerShell script for this, we will create a certificate and link it to the script.

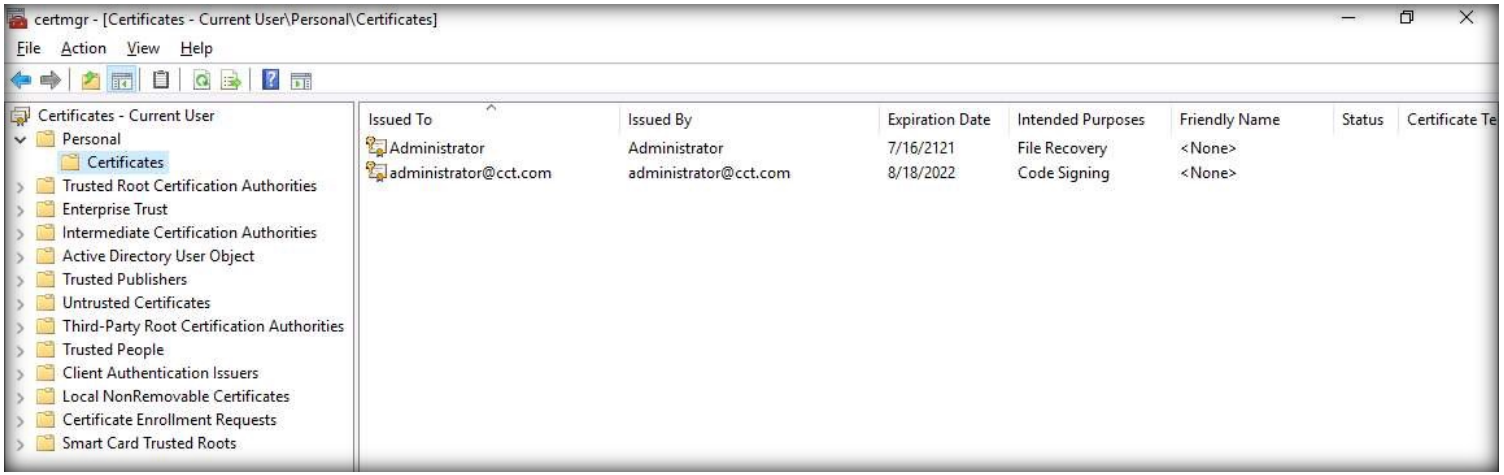
41. In the PowerShell window, type New-SelfSignedCertificate -DnsName administrator@cct.com -CertStoreLocation Cert:\CurrentUser\My\ -Type Codesigning and press Enter to generate the code signing certificate.



42. In the PowerShell window, type certmgr.msc and press Enter to open the certificate manager.

43. The certmgr window appears. In the left-pane expand Personal node and select Certificates node.

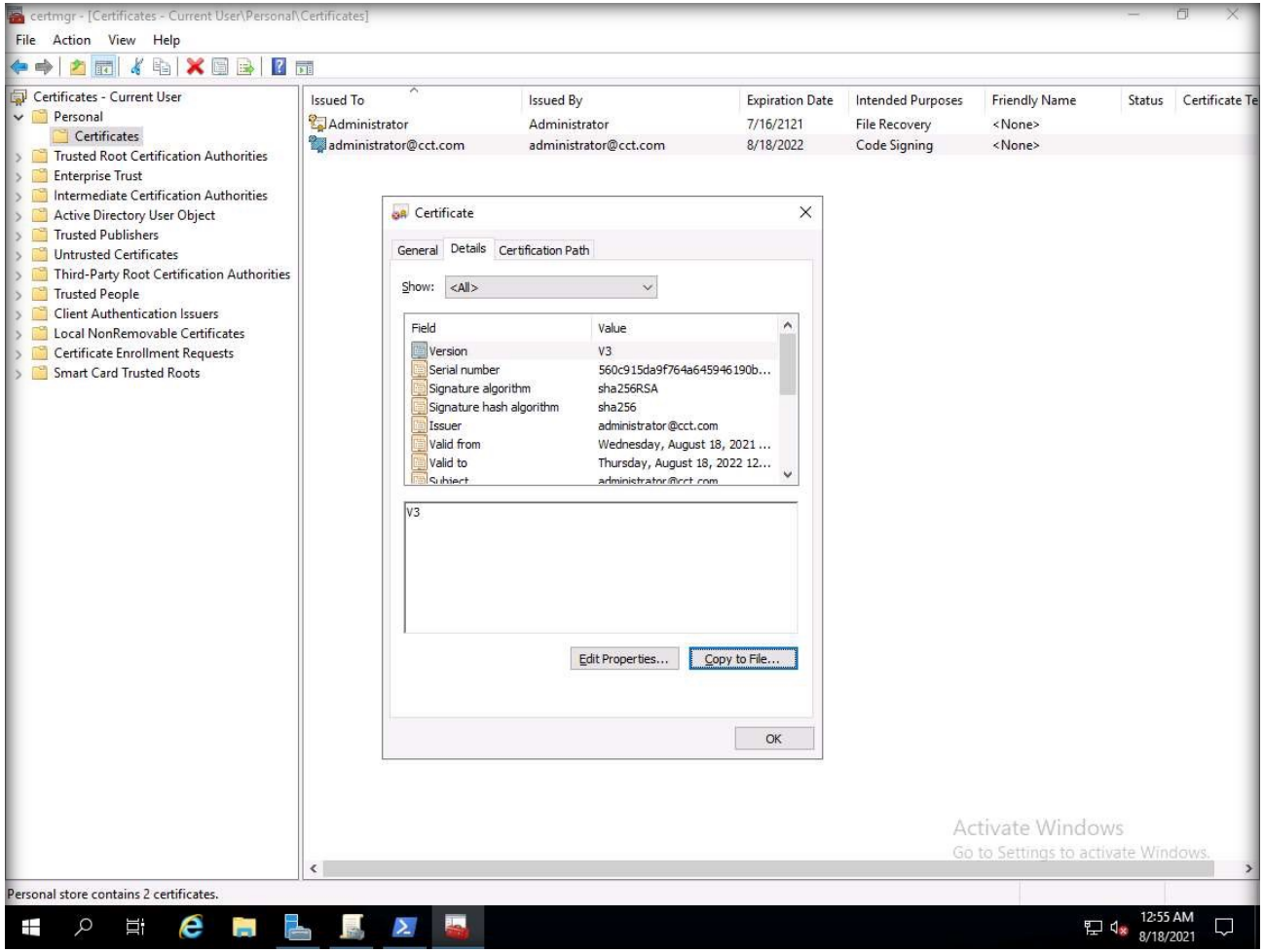
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

44. In the right-pane, two certificates can be observed. Double-click administrator@cct.com certificate.

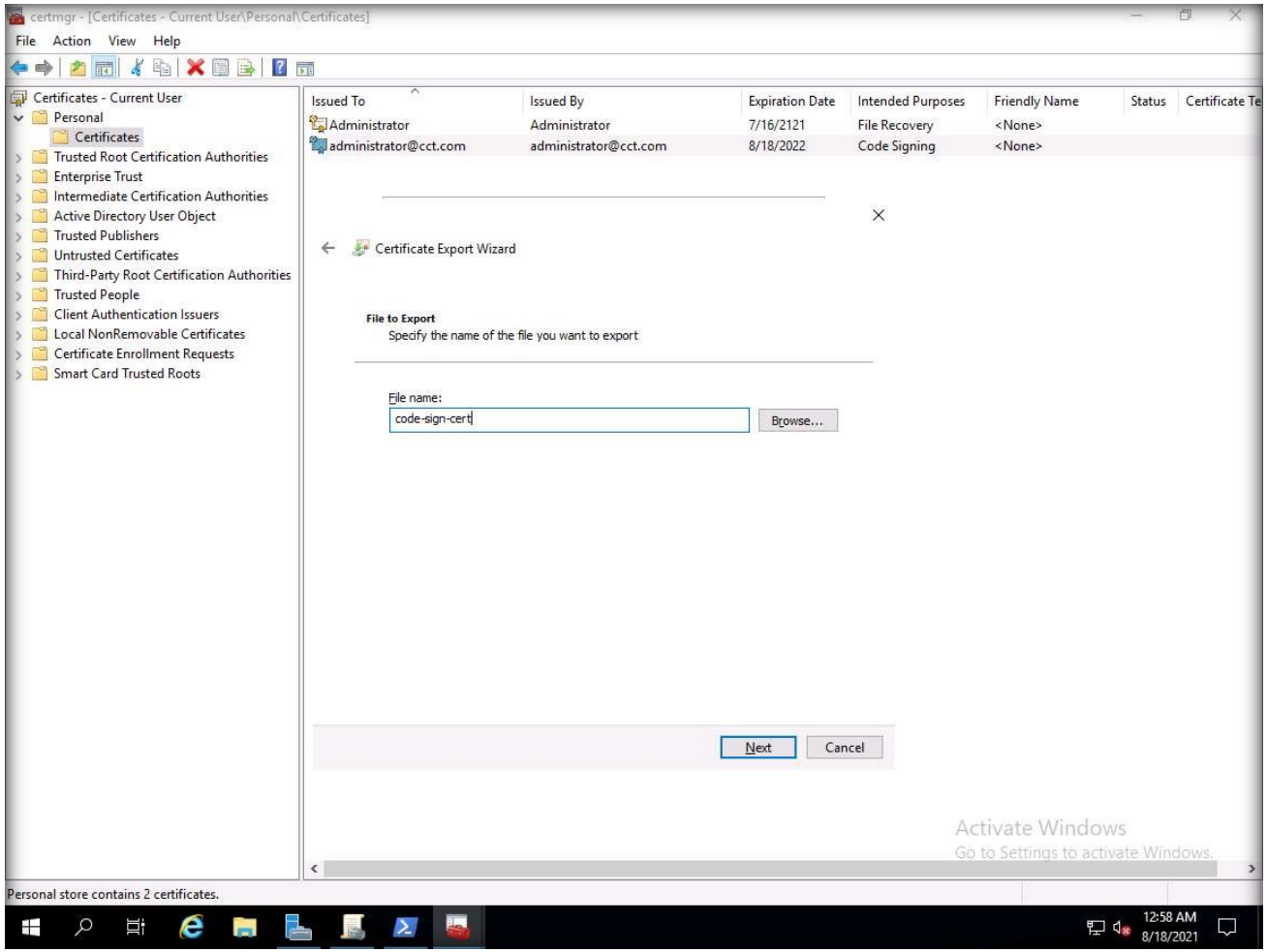
45. The Certificate window appears, navigate to the Details tab and click Copy to File... button.



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

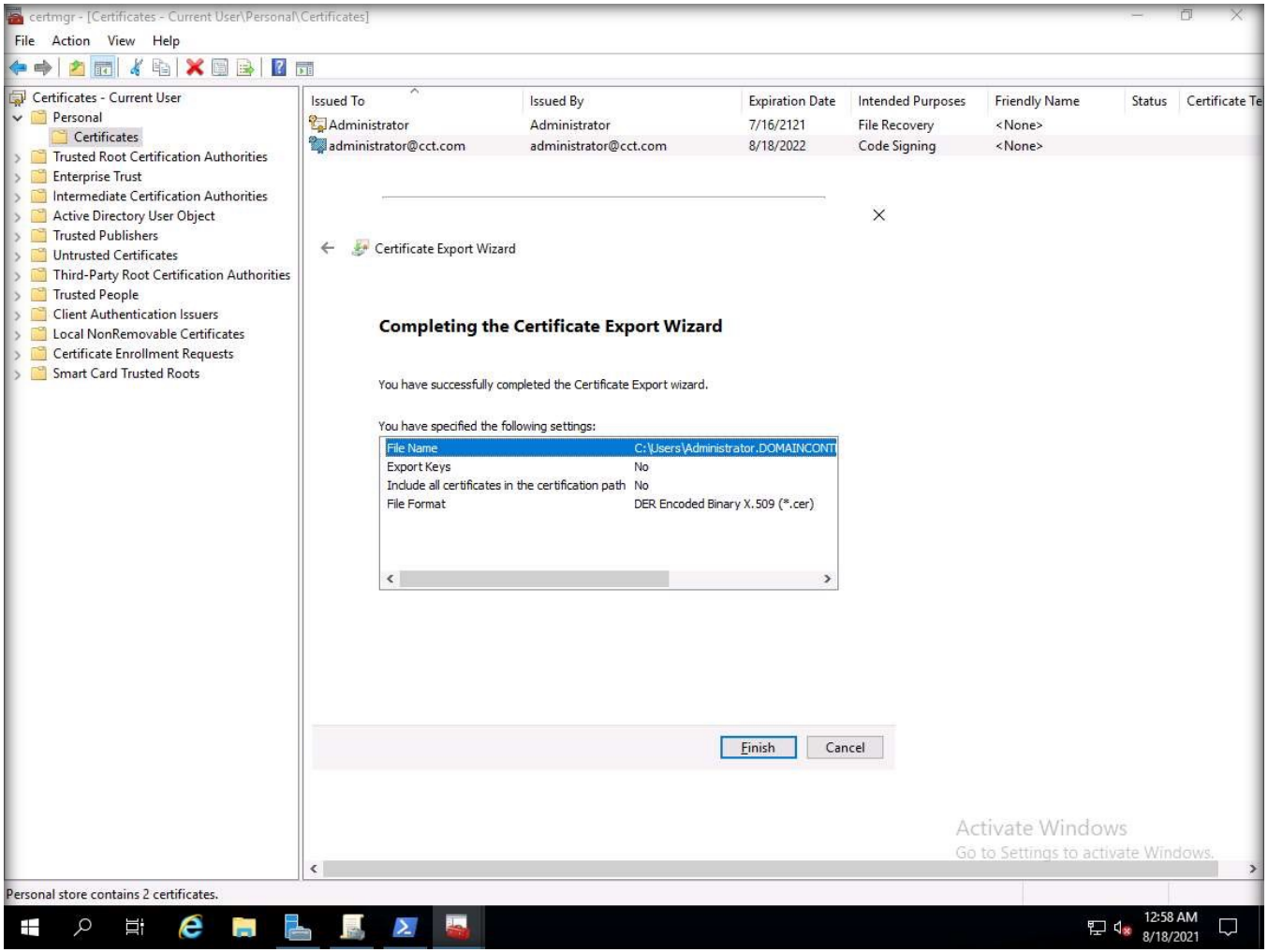
46. A Certificate Export Wizard window appears, click Next in all the wizards.

47. In the File to Export wizard, enter the File name as code-sign-cert and click Next button.



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

48. In the Completing the Certificate Export Wizard, click Finish button.

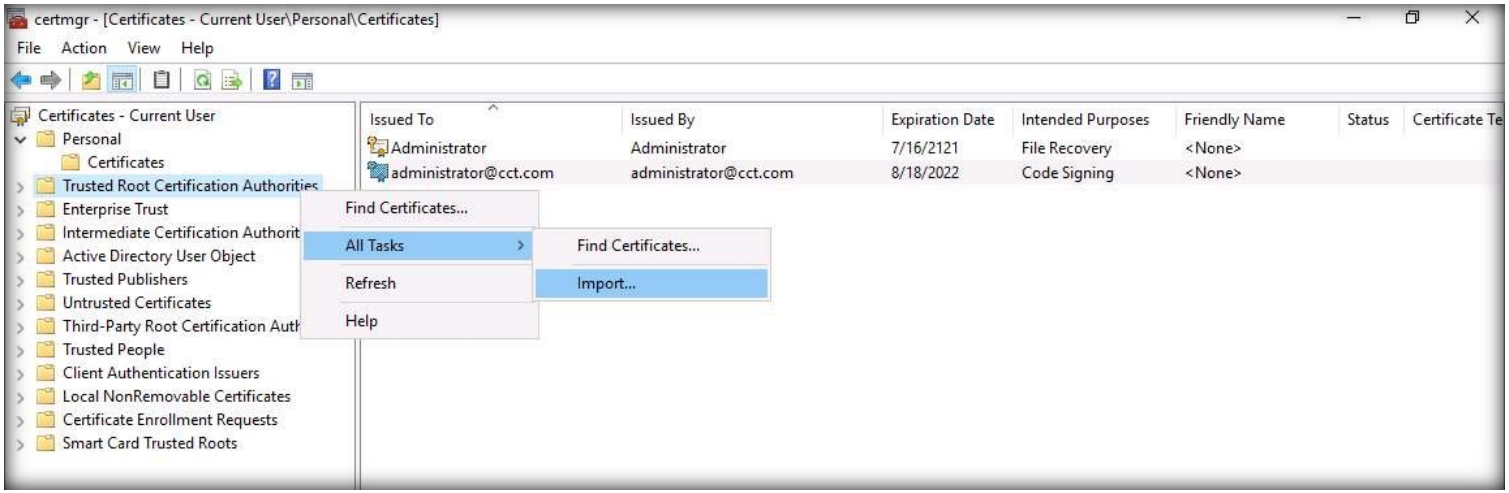


49. Now, a pop-up stating that the export was successful appears, click OK.

50. In the Certificate window, click OK to close it.

51. In the certmgr window, right-click Trusted Root Certification Authorities node from the left-pane and navigate to All Tasks → Import....

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

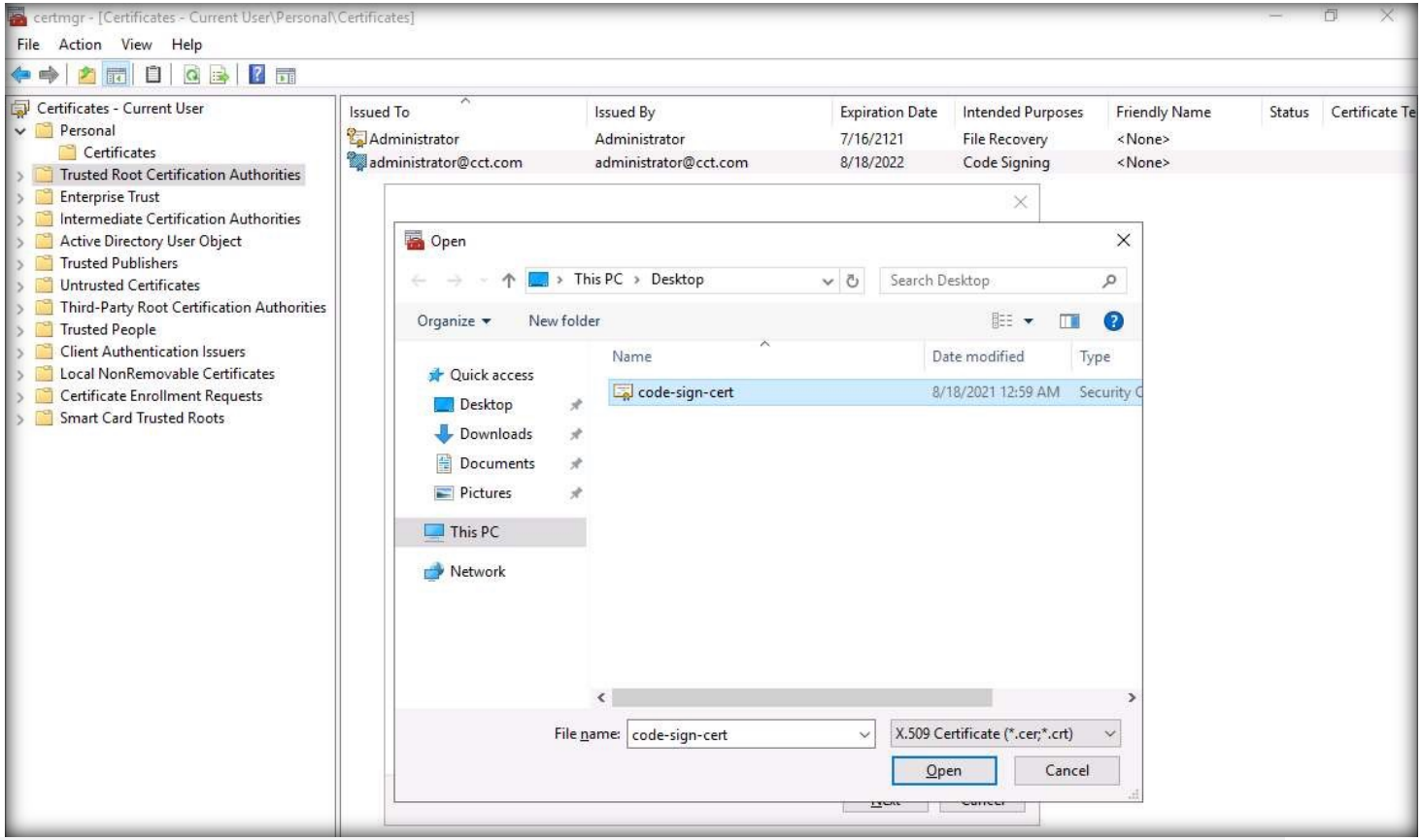


52. The Certificate Import Wizard appears, click Next.

53. Now, the File to Import wizard appears, click Browse... button under File name.

54. An Open window appears, select the code-sign-cert file on the Desktop and click Open.

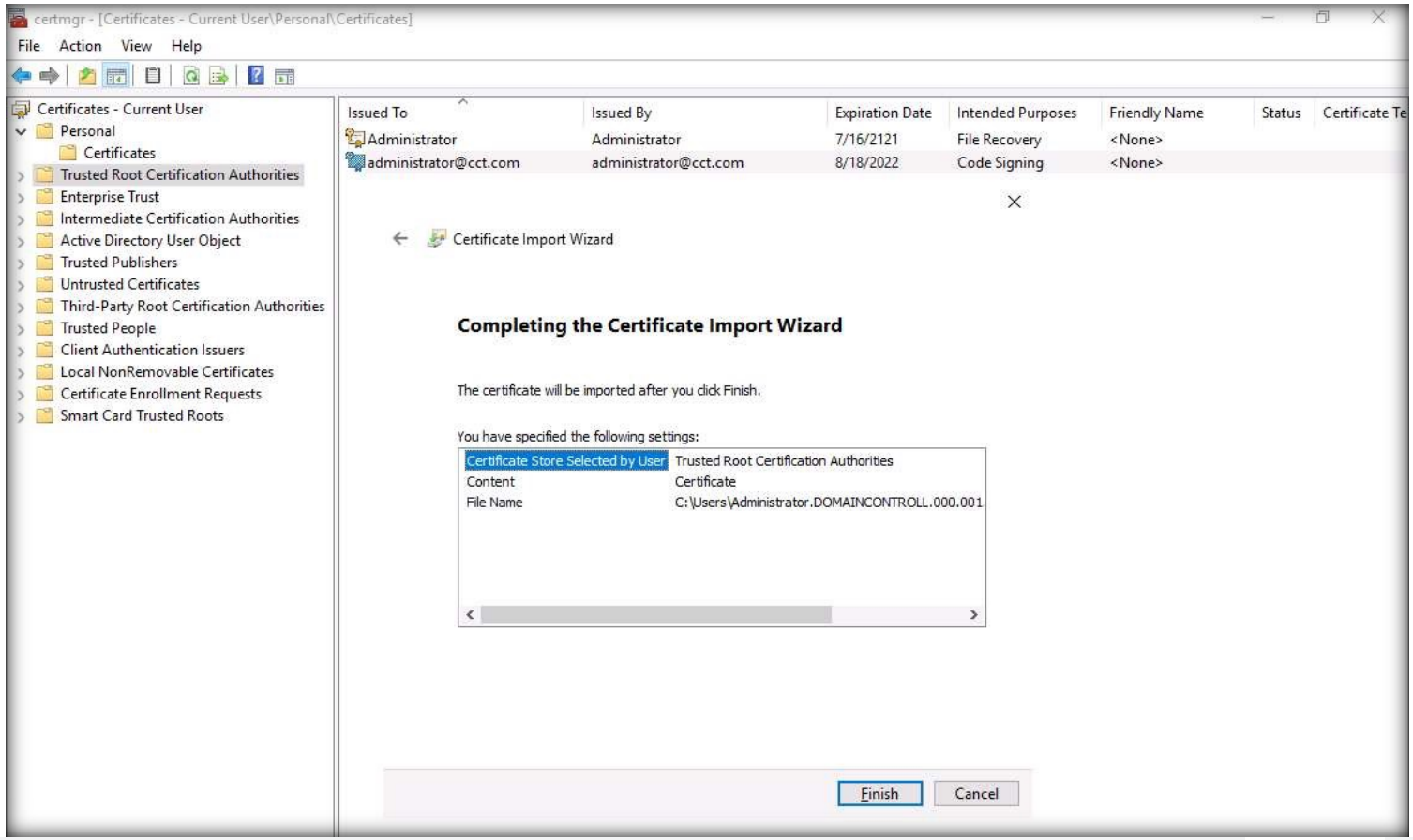
EXERCISE 4:
IMPLEMENT A
POWERSHELL
SECURITY POLICY



55. The file path appears in the File name field, click Next in all following wizards.

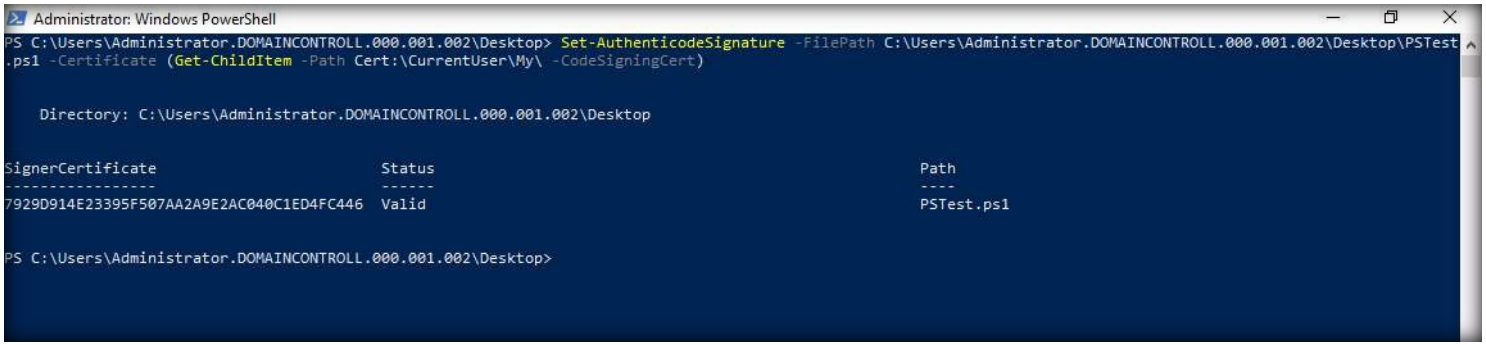
56. In the Completing the Certificate Import Wizard, click Finish.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



57. A Security Warning window appears, click Yes.
58. An import was successful pop-up appears, click OK.
59. In the certmgr window, right-click Trusted Publishers node from the left-pane and then perform Steps#51-58 to import the code-sign-cert certificate.
60. Close the certmgr window.
61. Maximize the PowerShell window, type Set-AuthenticodeSignature -FilePath C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop\PSTest.ps1 -Certificate (Get-ChildItem -Path Cert:\CurrentUser\My\ -CodeSigningCert) and press Enter to implement the execution policy as digitally signed on the PSTest.ps1 script.

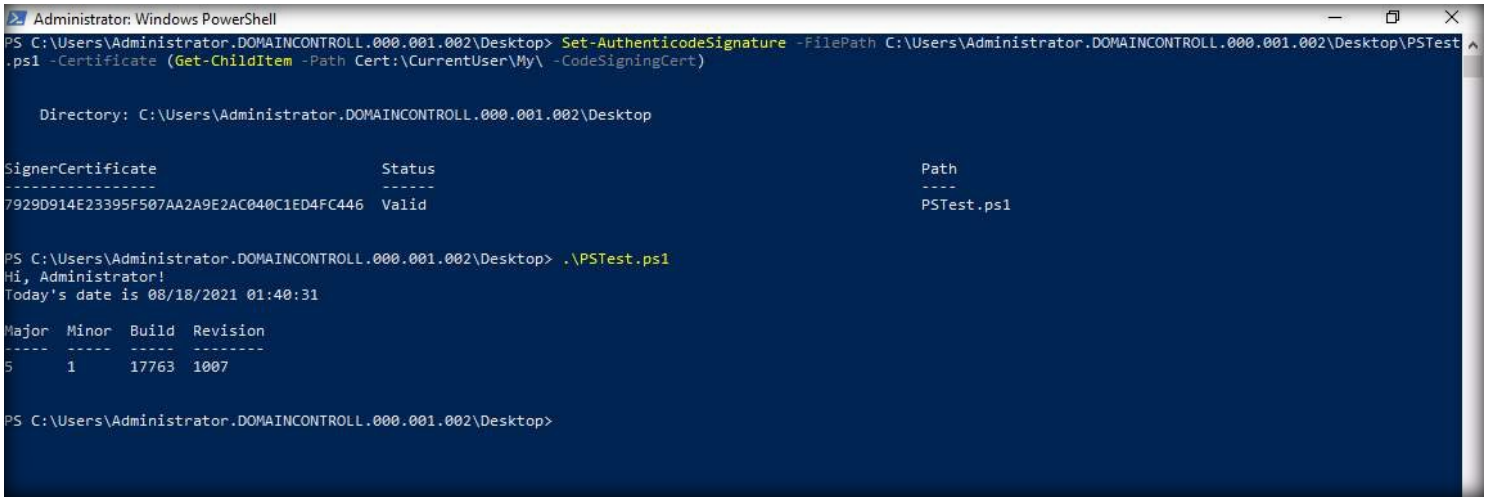
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



62. Type .\PSTest.ps1 and press Enter to execute the script.

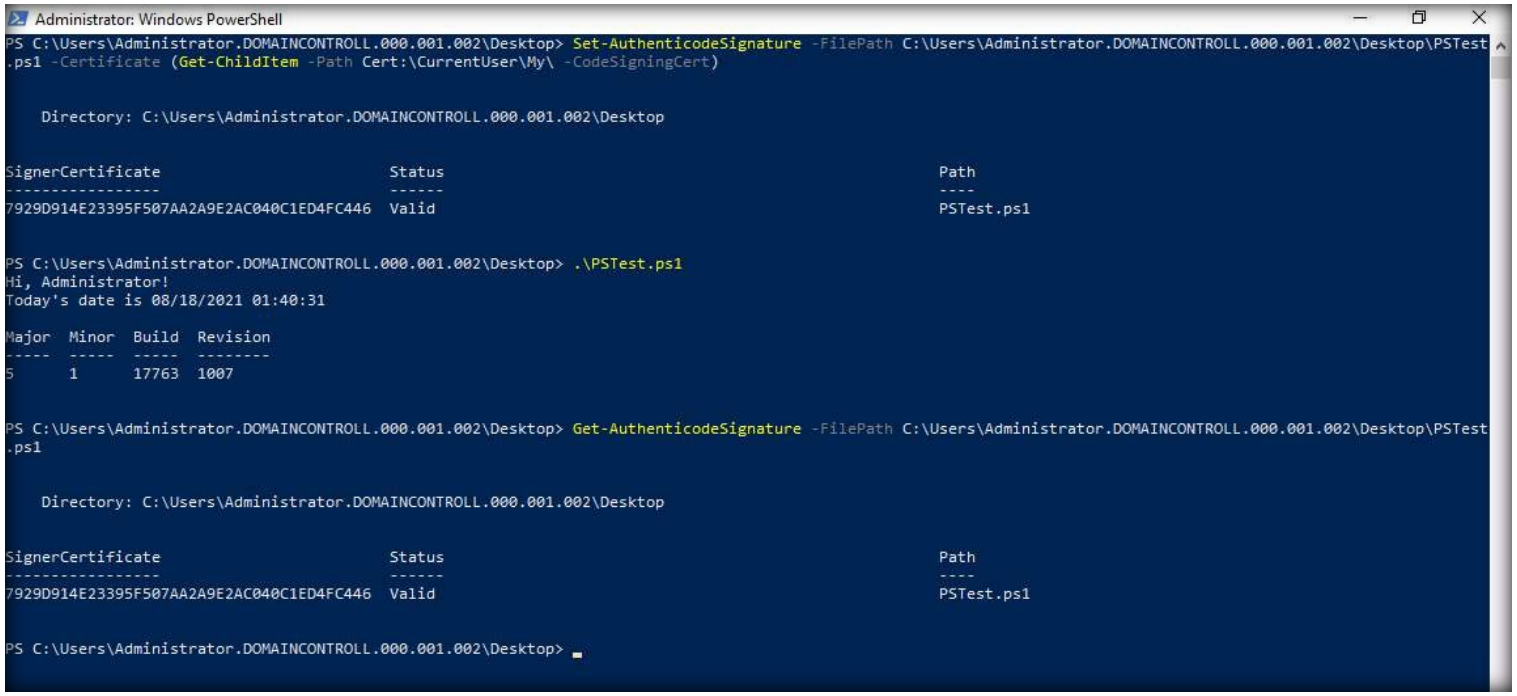
63. The script will be successfully executed because it now digitally signed.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

64. Type Get-AuthenticodeSignature -FilePath C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop\PSTest.ps1 and press Enter to confirm the Status of the script as Valid. Details regarding SignerCertificate can be viewed, as shown in the screenshot.



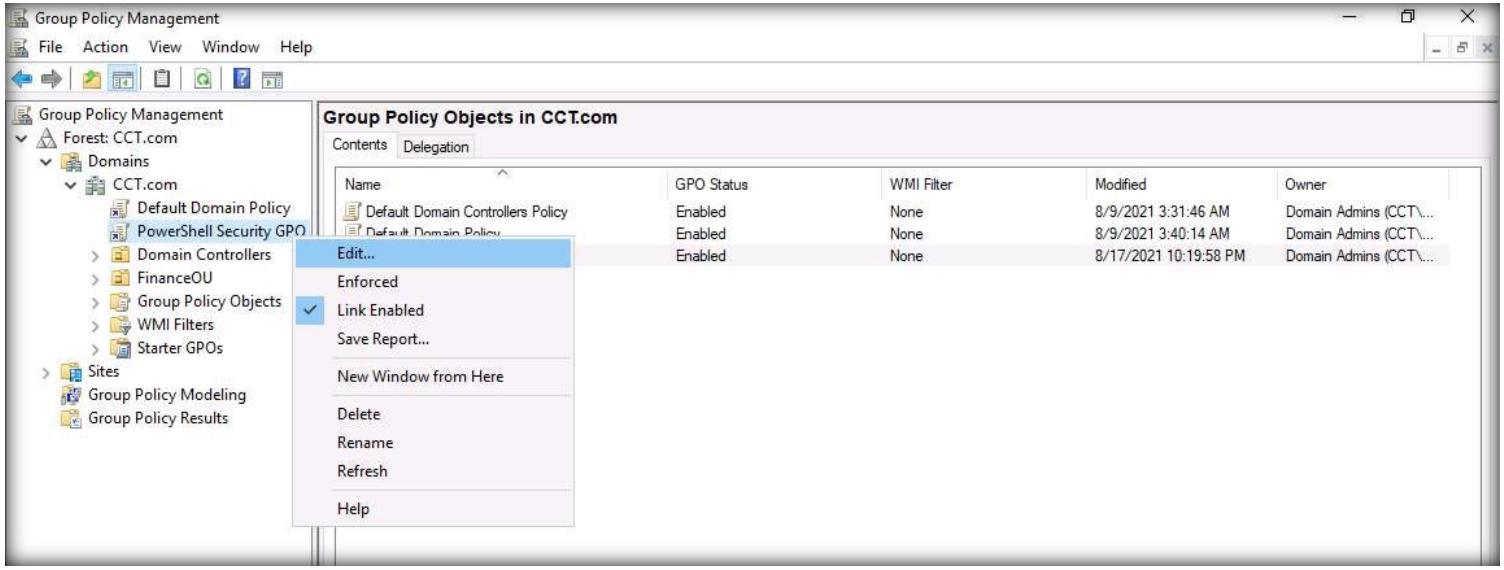
65. Close the PowerShell window.

66. Now, we shall enforce the execution control policy using GPO (Group Policy Object). Here, we will configure the execution policy as AllSigned.

67. Maximise Group Policy Management window.

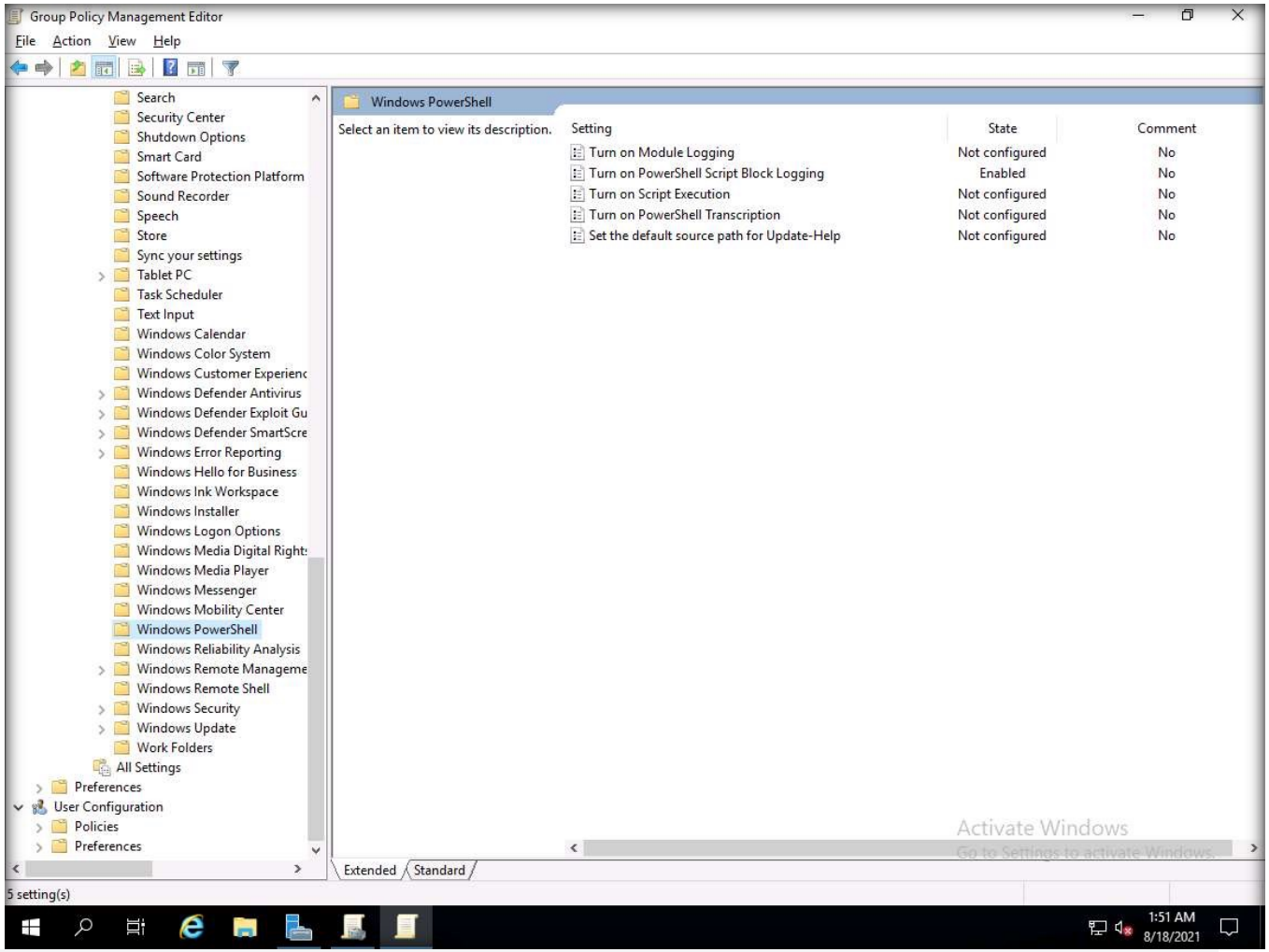
68. Right-click PowerShell Security GPO node under the CCT.com node and click Edit....

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



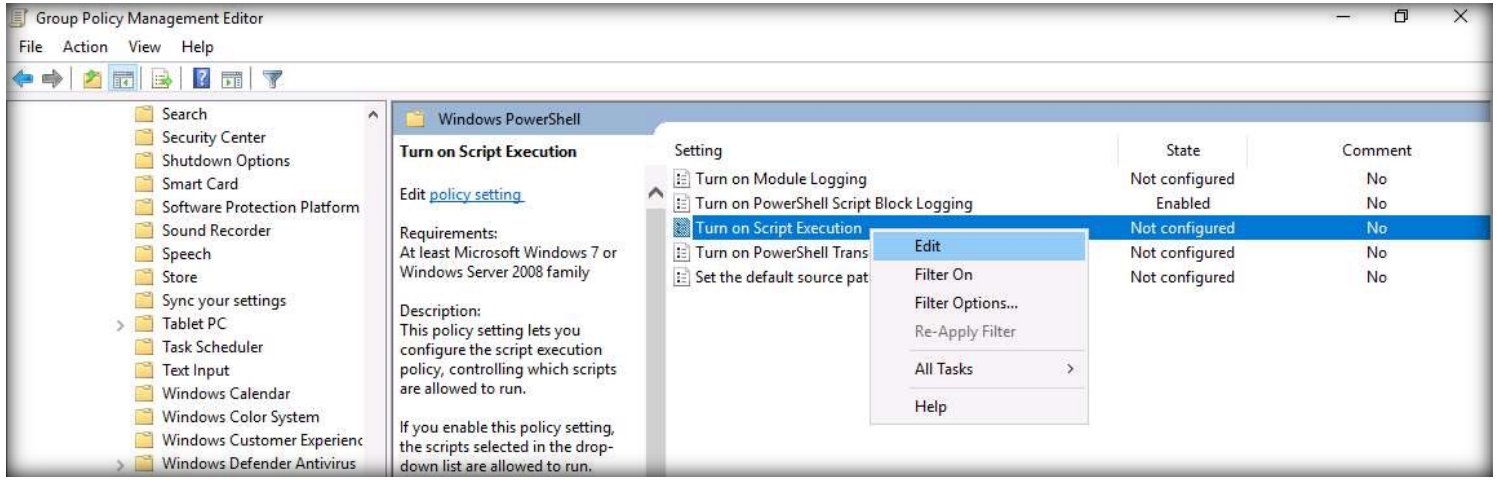
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

69. The Group Policy Management Editor window appears, navigate to Computer Configuration → Policies → Administrative Templates → Windows Components → Windows PowerShell.



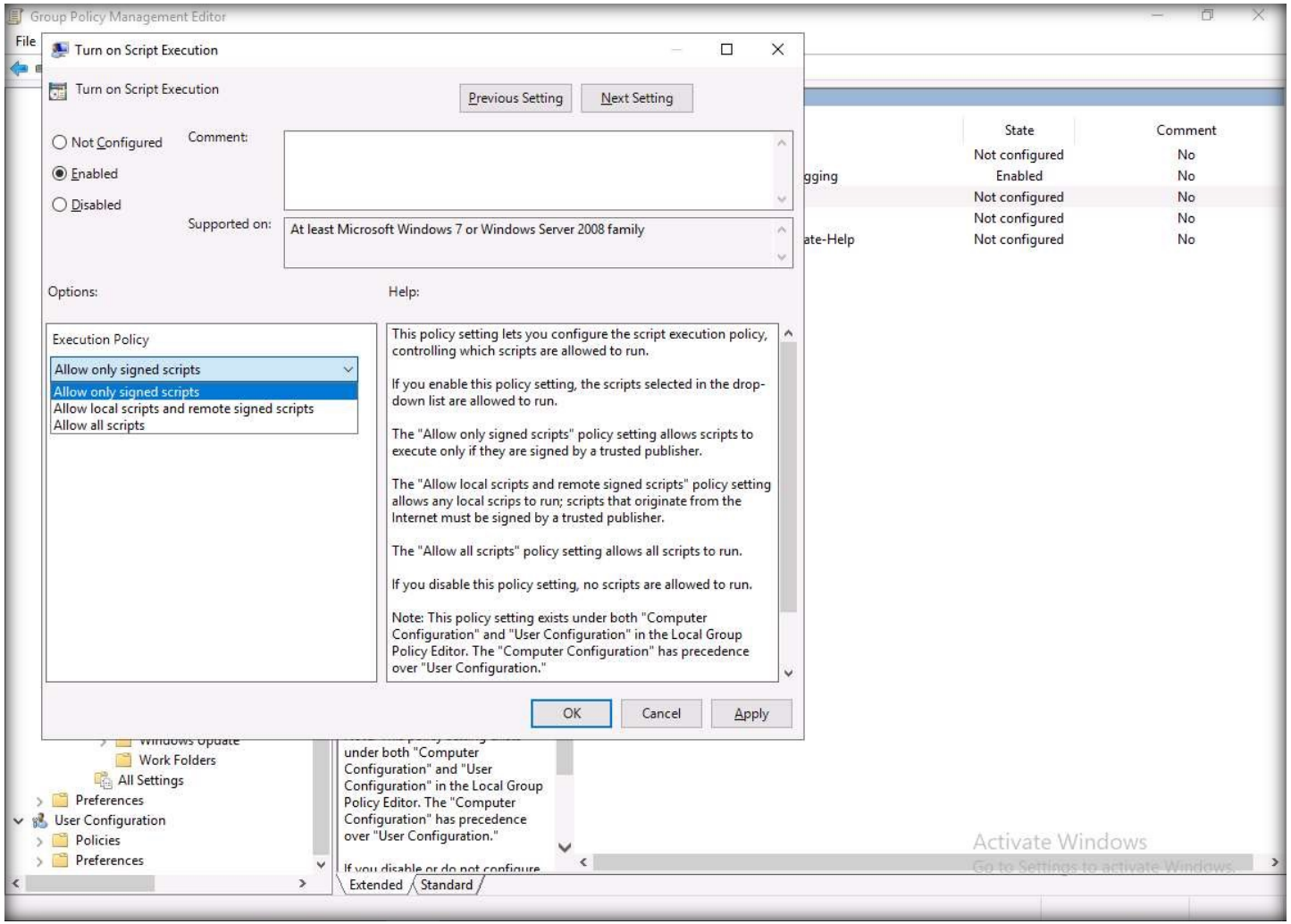
70. Right-click Turn on Script Execution, click Edit.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

71. The Turn on Script Execution window appears, select the Enabled radio button and then select the Allow only signed scripts option from the drop-down options under Execution Policy. Click Apply and click OK.



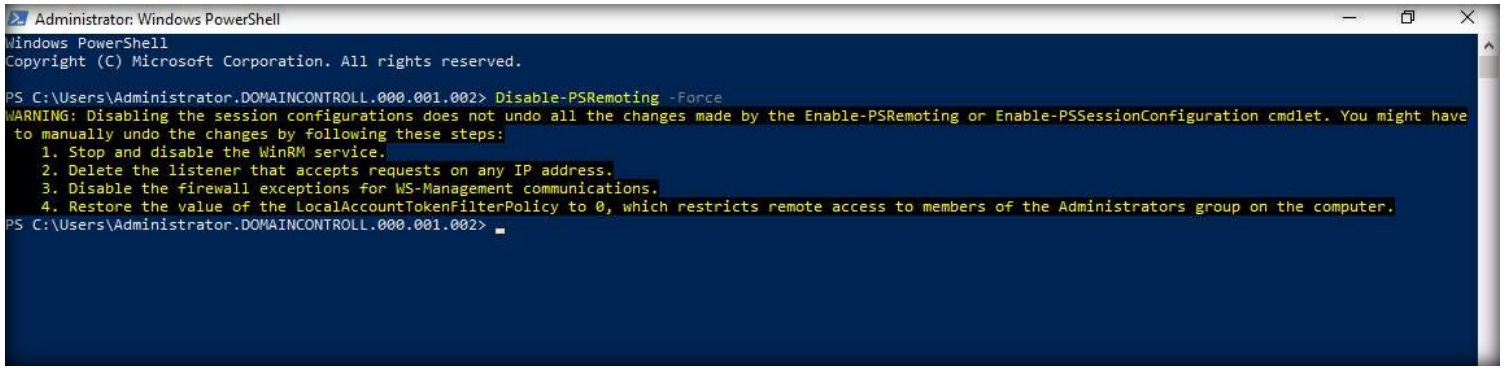
72. Close the Group Policy Management Editor window and Group Policy Management window.

73. Now, we will configure PowerShell security to ensure that the commands or scripts can only be run locally (here, the AD Domain Controller machine). For this, we will disable the remoting feature in PowerShell to prevent users from establishing a remote connection with PowerShell.

74. Right-click the Start icon present at the left-bottom of the Desktop. Select Windows PowerShell (Admin) option to launch PowerShell window.

75. In the PowerShell window, type Disable-PSremoting -Force and press Enter to disable the remoting feature in PowerShell.

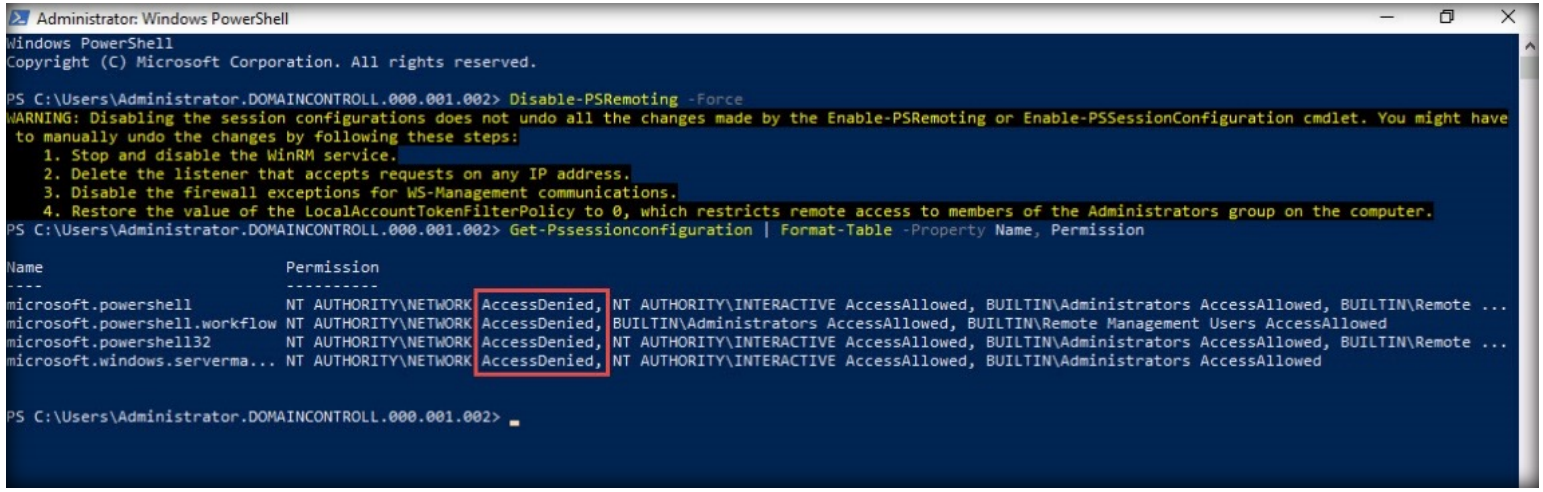
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



76. Type Get-Pssessionconfiguration | Format-Table -Property Name, Permission and press Enter to determine the status of PowerShell remoting.

77. An AccessDenied message can be observed under the Permission column indicating that the PowerShell remoting has been disabled.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

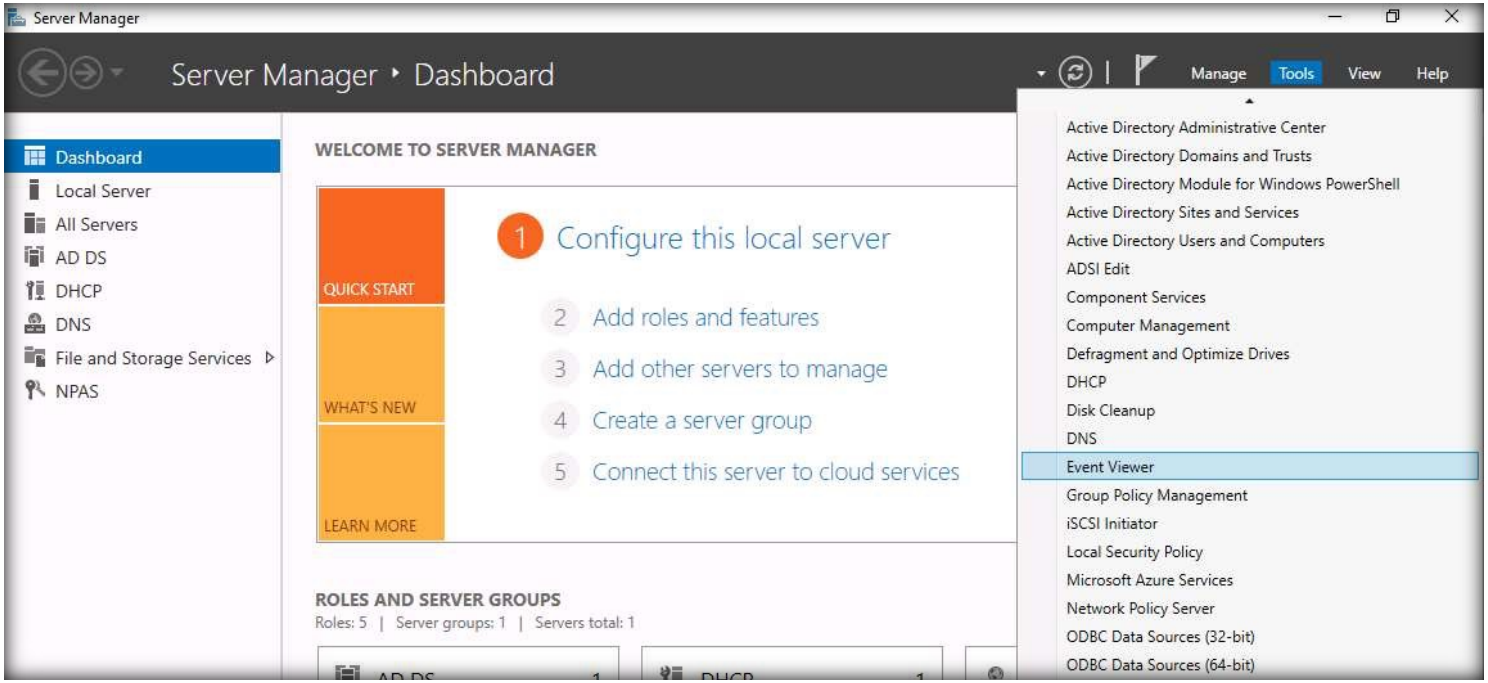


78. Close the PowerShell window.

79. Now, we will view the event log of suspicious entries that were captured when we tried to run an unsigned script.

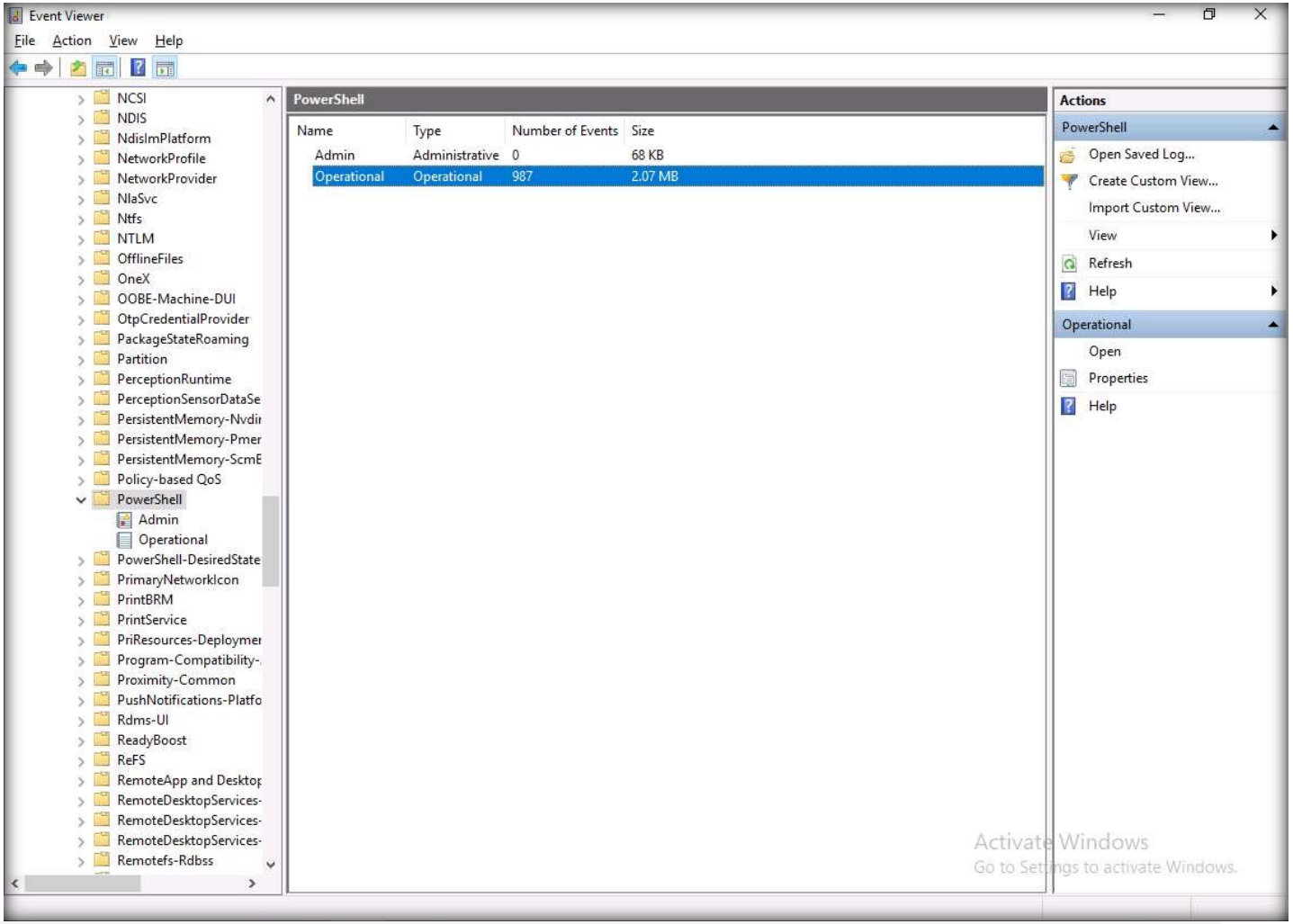
80. In the Server Manager window, click Tools and select the Event Viewer option.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



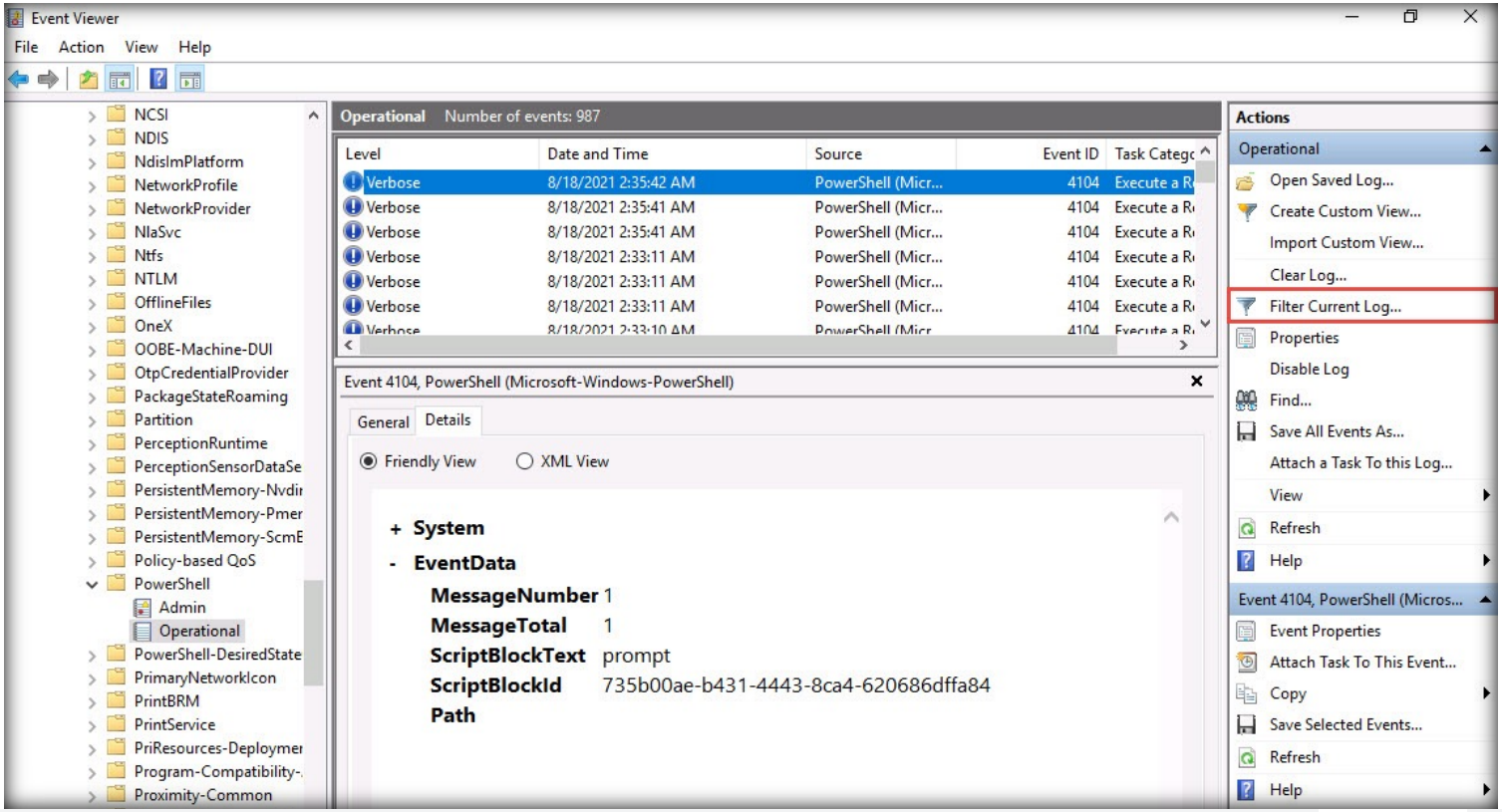
EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY

81. The Event Viewer window appears. In the left-pane, navigate to Applications and Services Logs Microsoft Windows PowerShell. In the right-pane, double-click the Operational log.



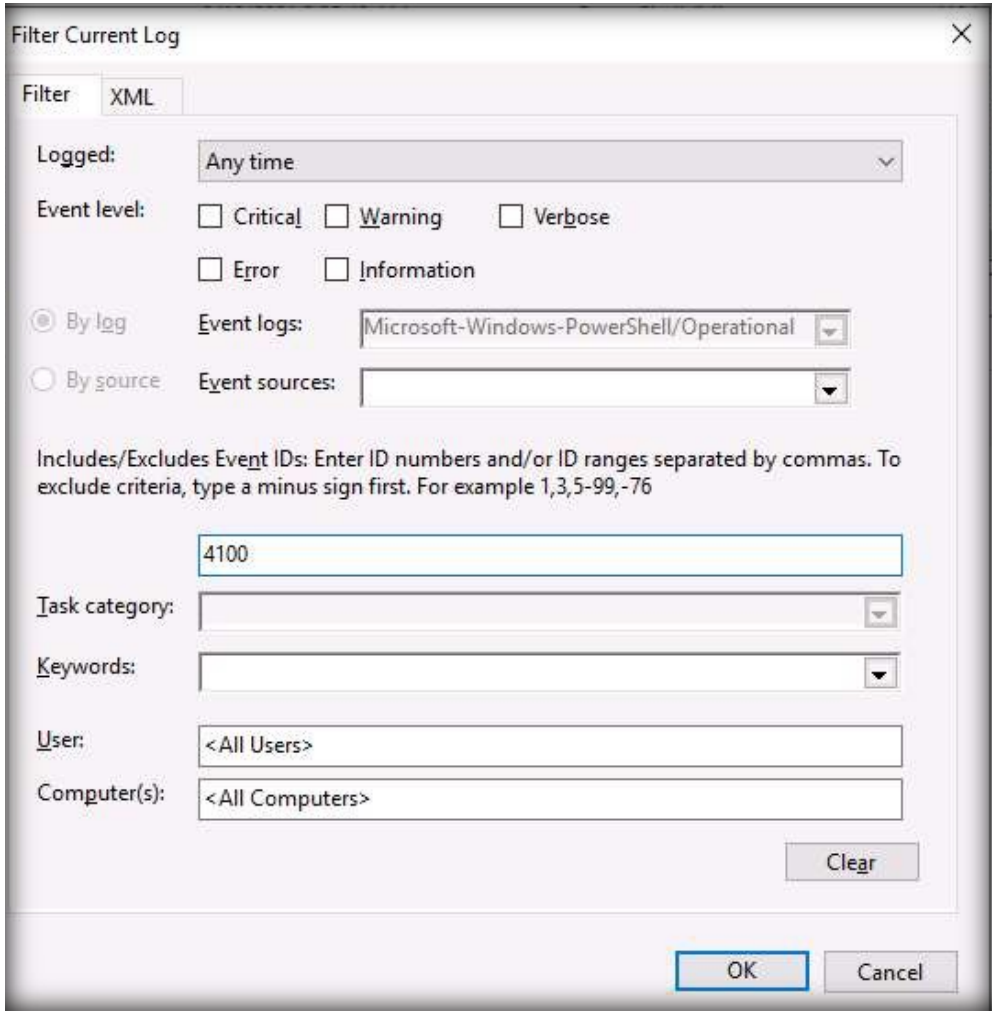
82. The Operational log appears, in the right-pane, under the Actions section, click Filter Current Log... option.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



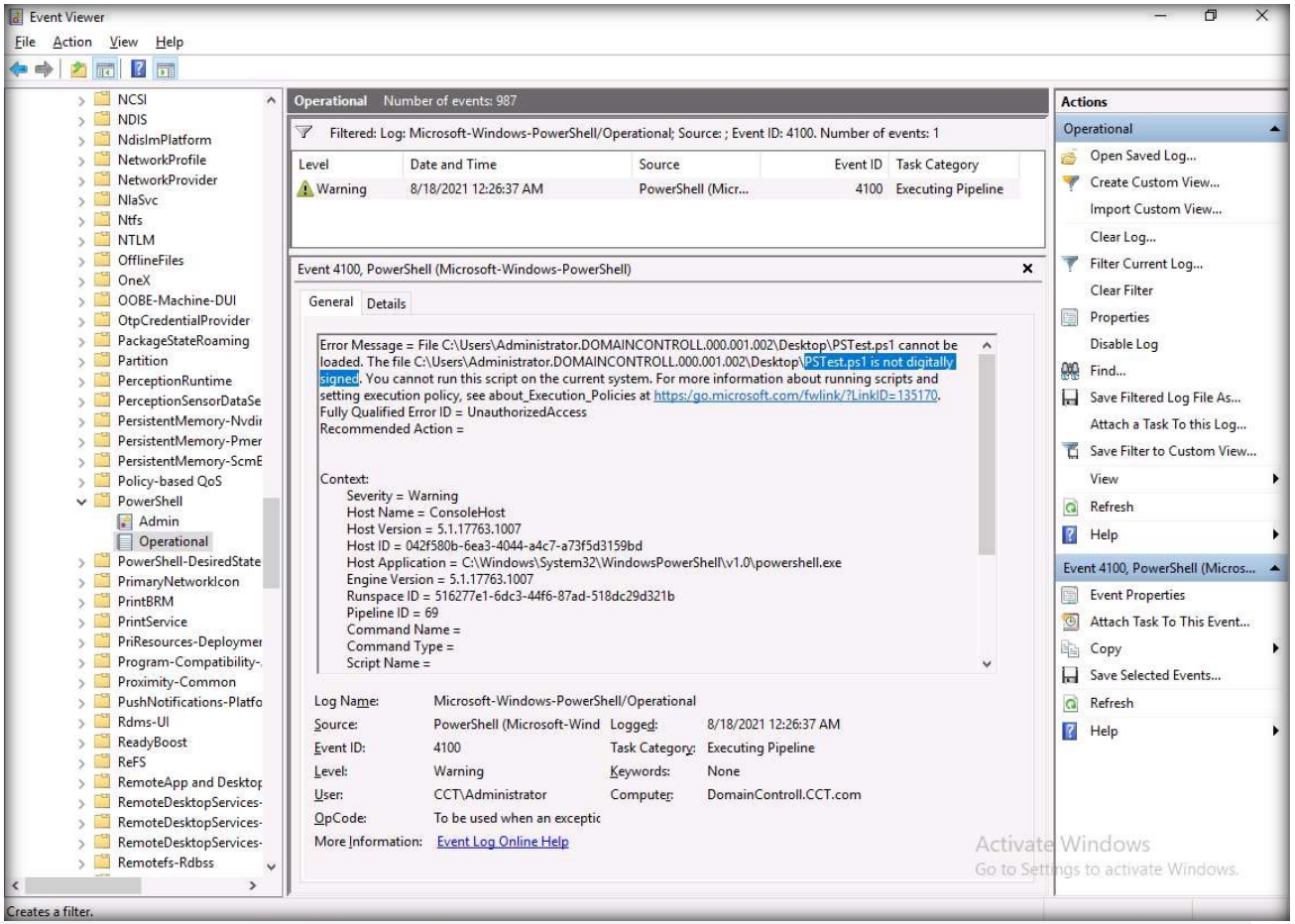
83. A Filter Current Log window appears, replace <All Event IDs> field with 4100 and click OK.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY



84. A Warning entry is displayed indicating that the PSTest.ps1 script could not be executed because it is not digitally signed.
85. Close all open windows.
86. This concludes the demonstration of implementing a PowerShell Security Policy.
87. Turn off AD Domain Controller and PfSense Firewall virtual machines.

EXERCISE 4: IMPLEMENT A POWERSHELL SECURITY POLICY




EC-Council