

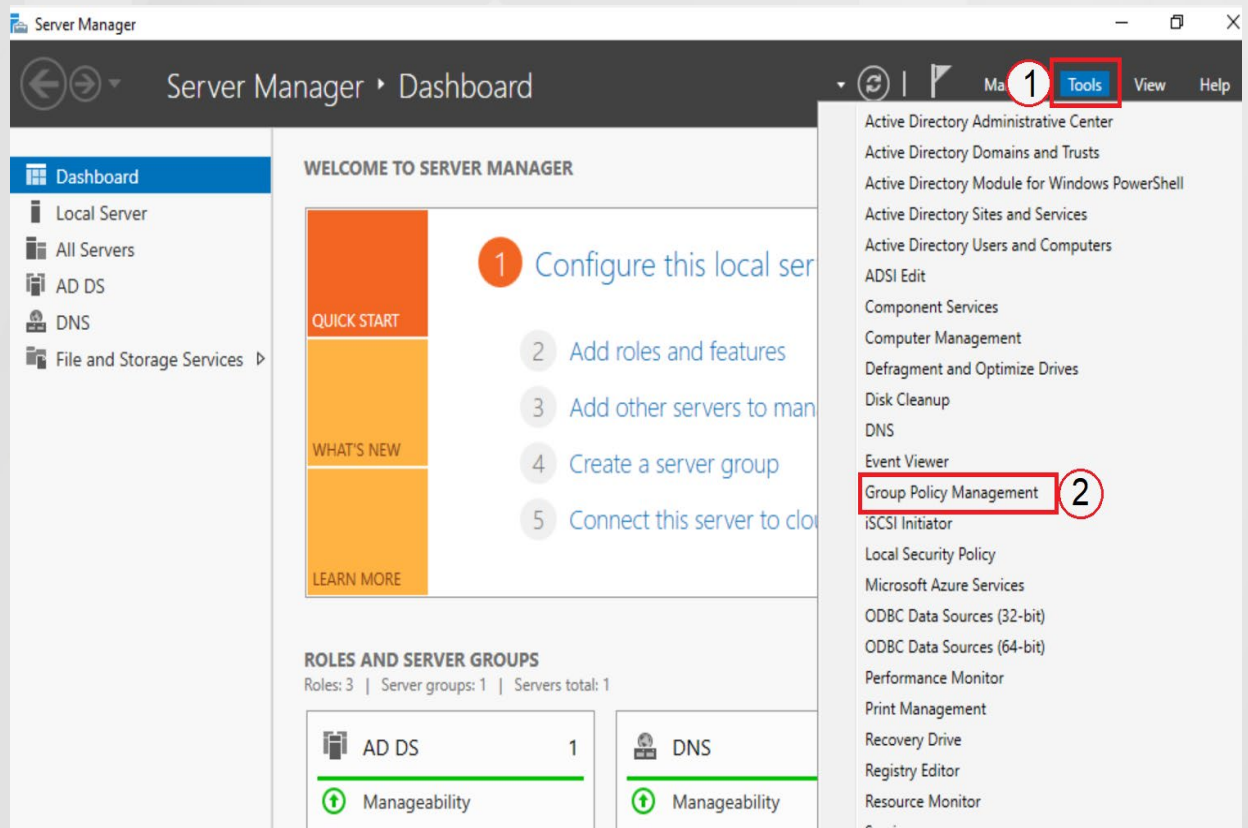
Active Directory Lab #5 Create GPOs in Active Directory

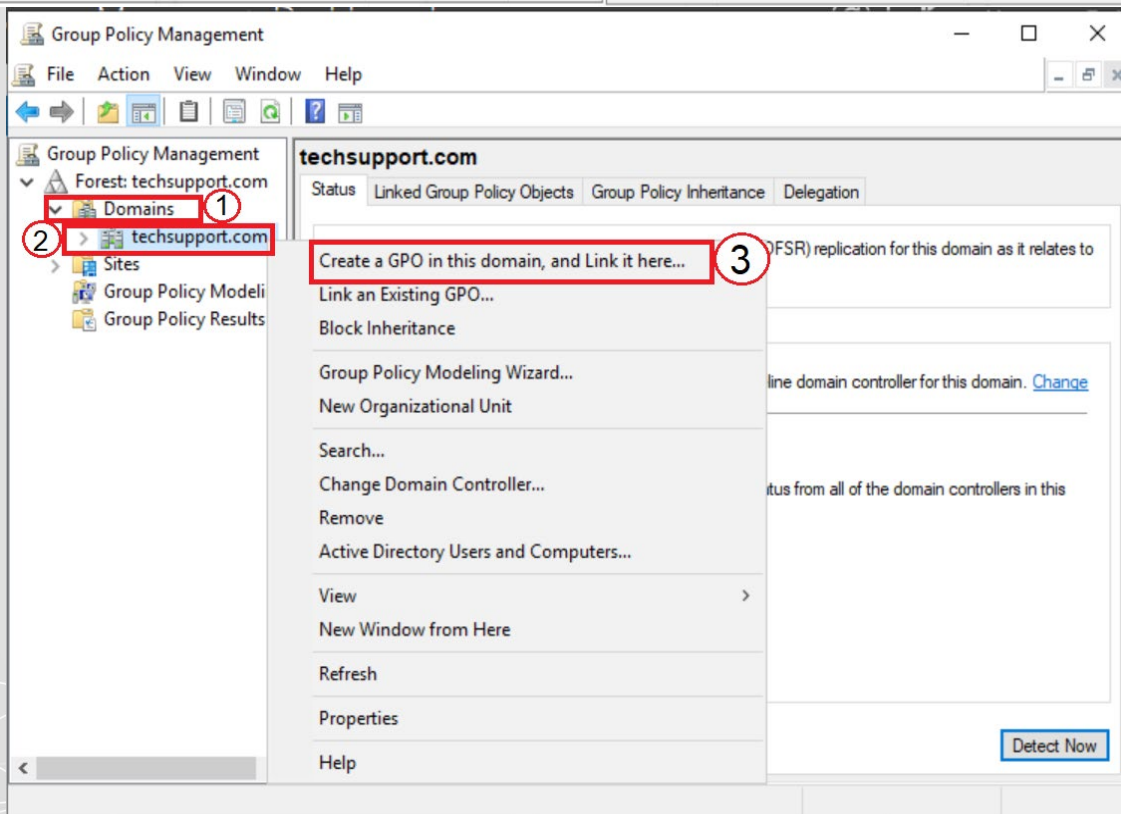
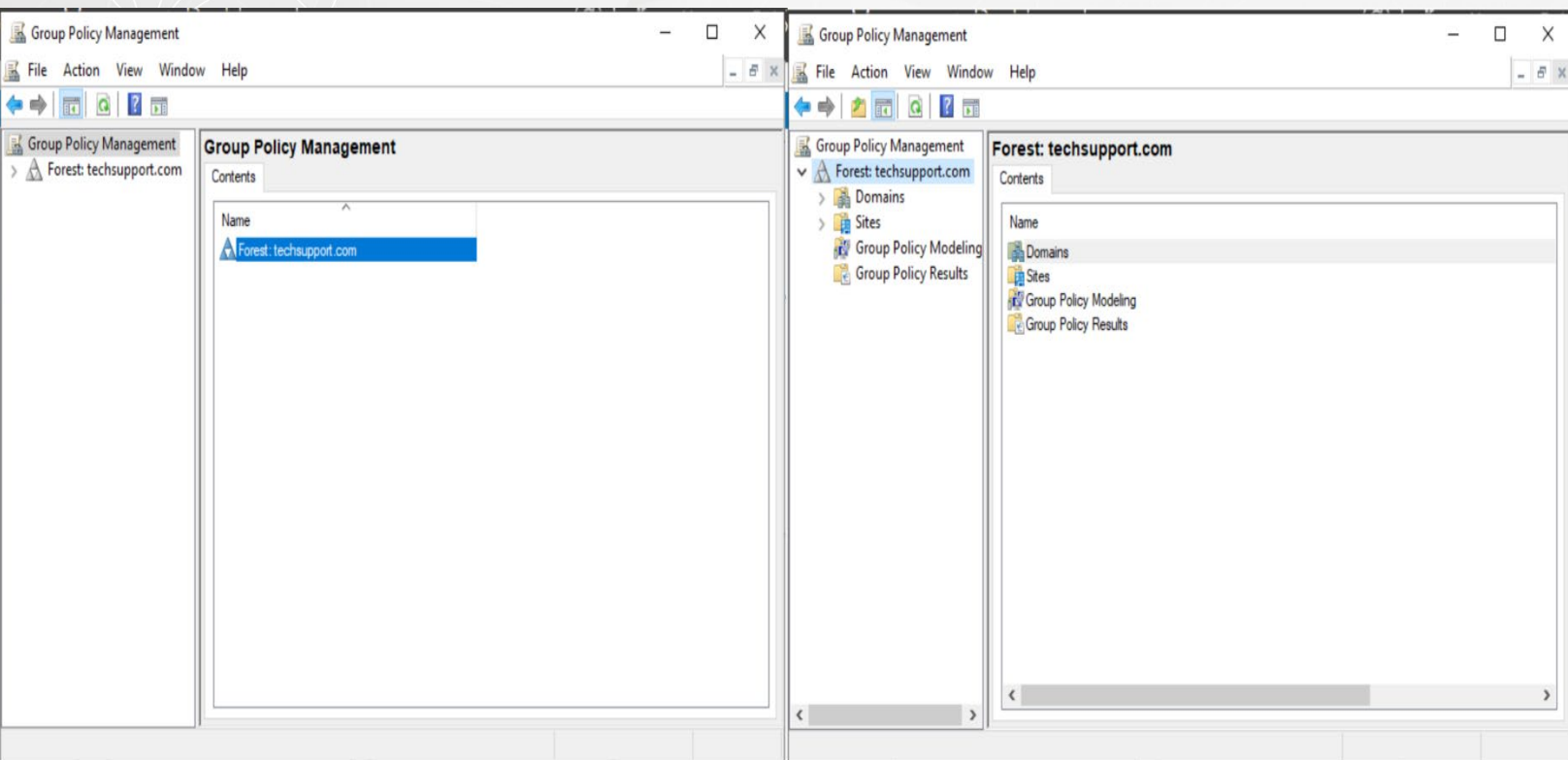
Objective:

The objective of this laboratory is to apply different levels of security on Active Directory objects through GPOs.

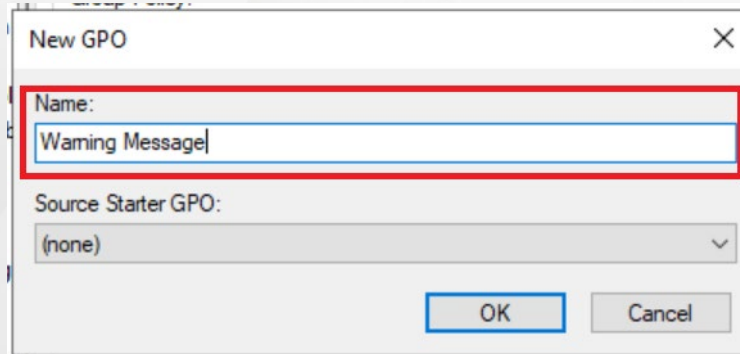
Task 1: Create a GPO

1. Enter the server manager, click on tools, look for the Group Policy management option and click
2. Look for the domain option and display it
3. Click on the domains option (1), left click on the **techsupport.com** (2) domain where we want to assign the GPO, right click, and select the option Create a GPO in this domain (3)

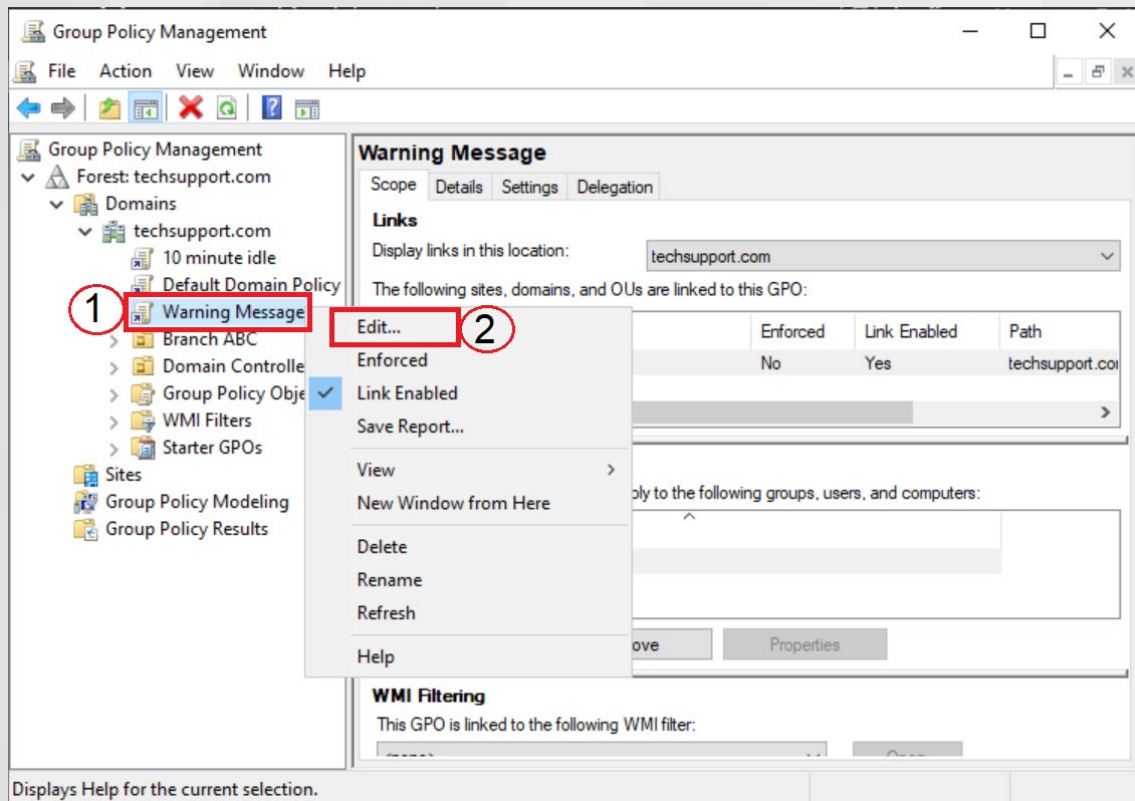




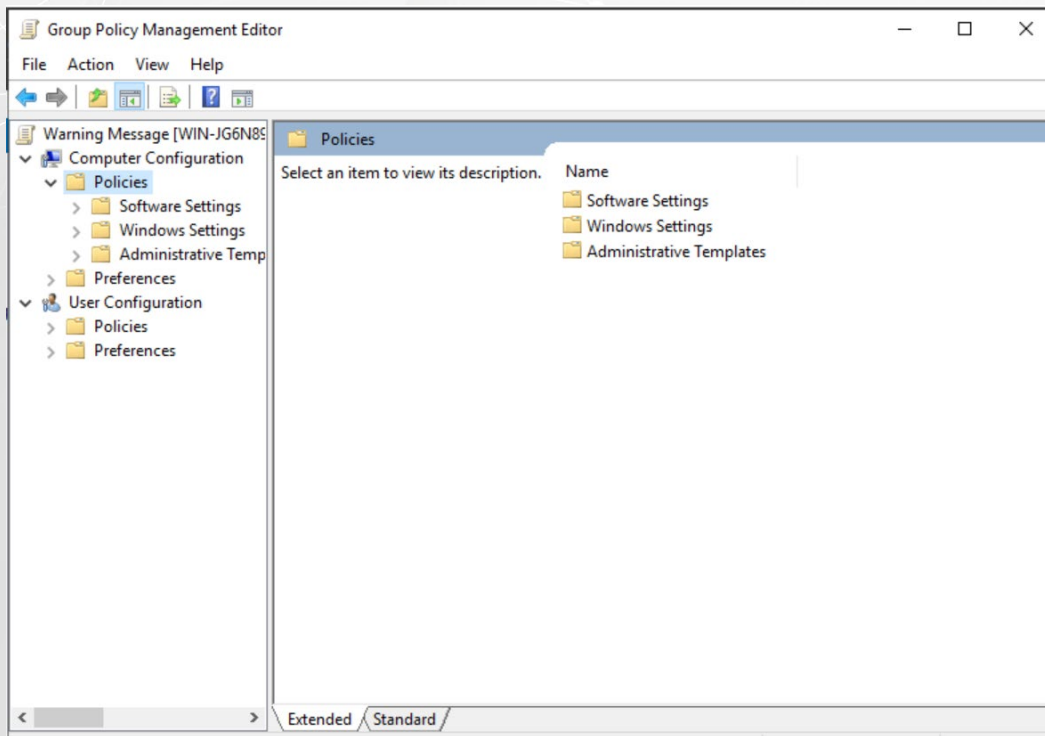
4. In order to identify the GPO, we call it **Warning Message**



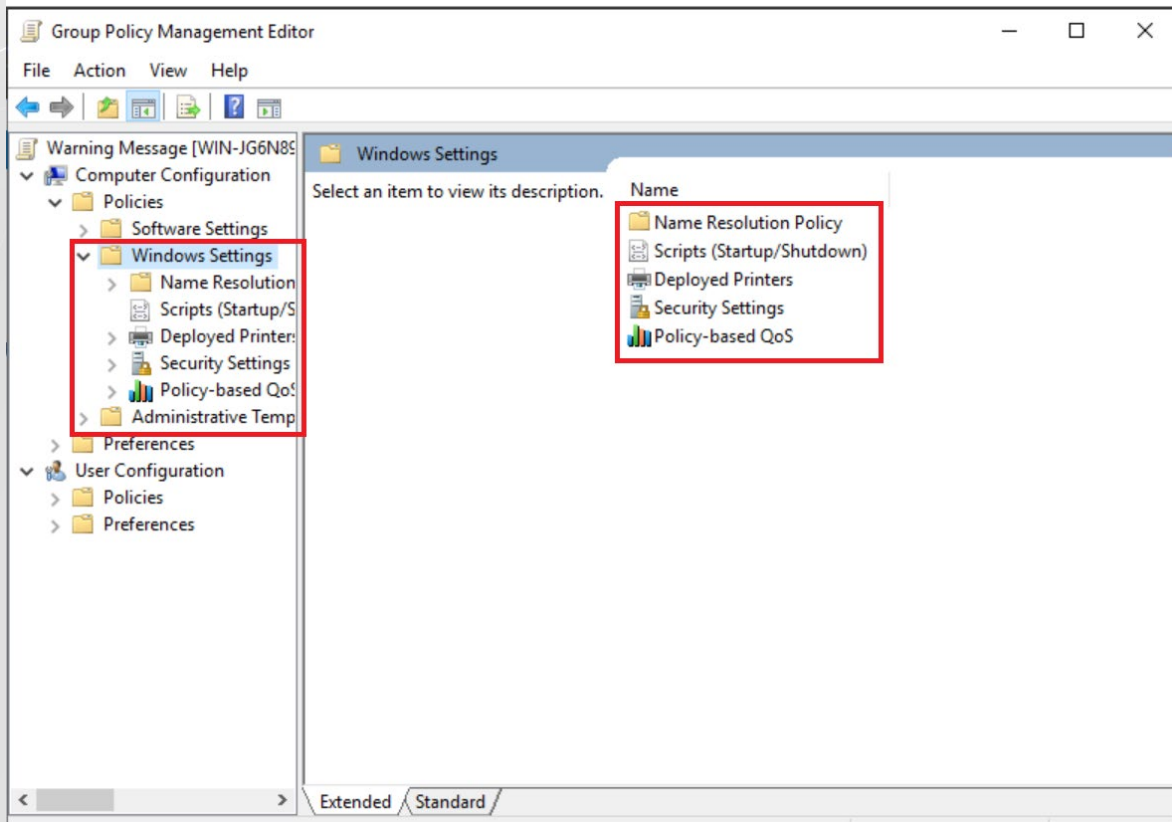
5. Now that the Warning Message GPO appears in the bar on the left side, we right click it



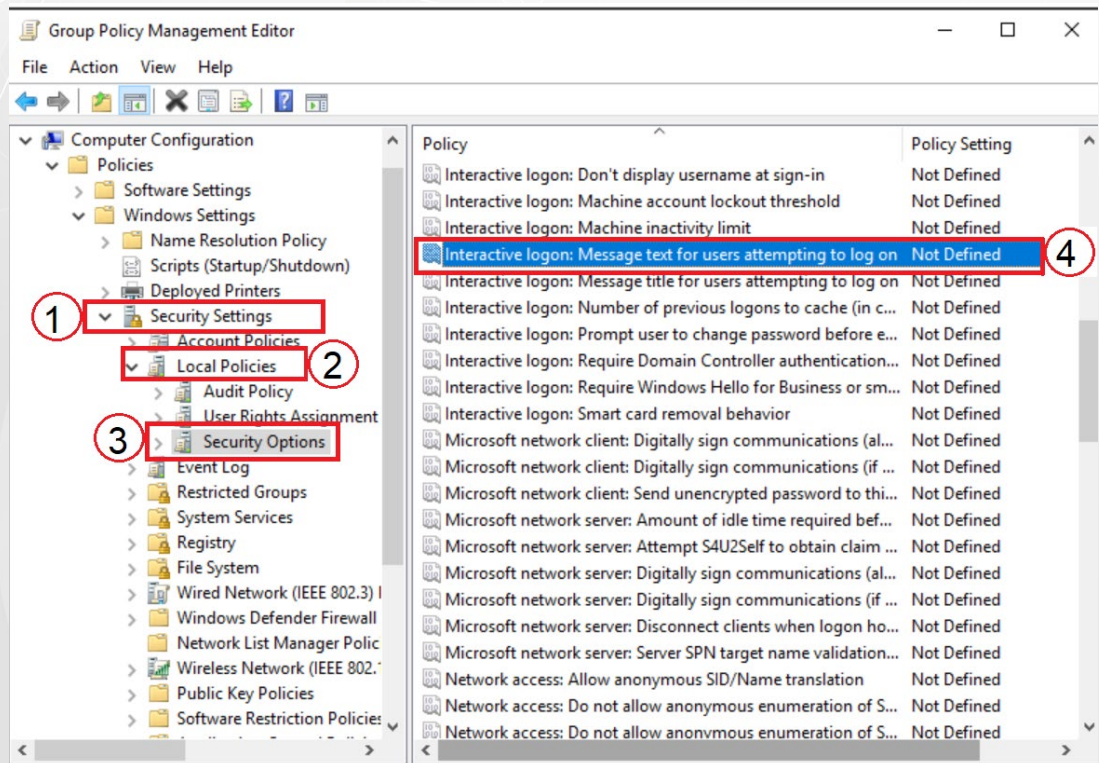
6. A pop-up window named Group Policy Management Editor will appear



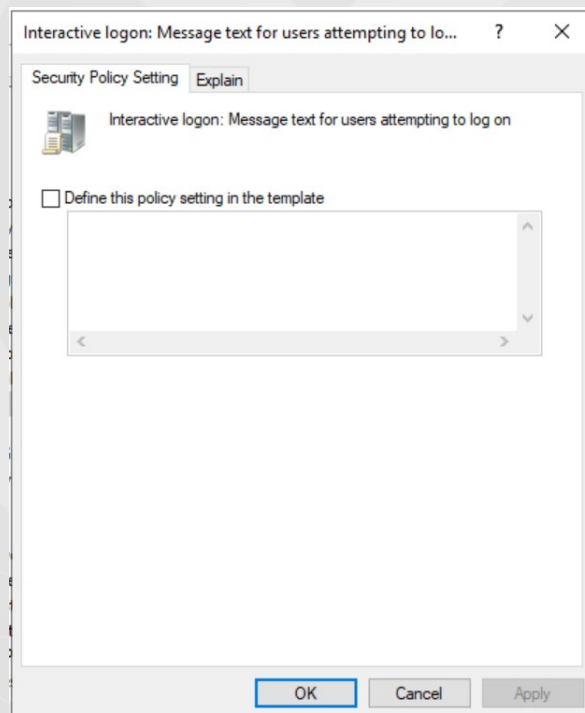
7. In the section on the left side, we select the Computer Configuration option and then click where the Policies folder is, to expand it, we display where it says Windows Settings
8. We click on Security Settings (1), then we display where it says Local Policies (2)



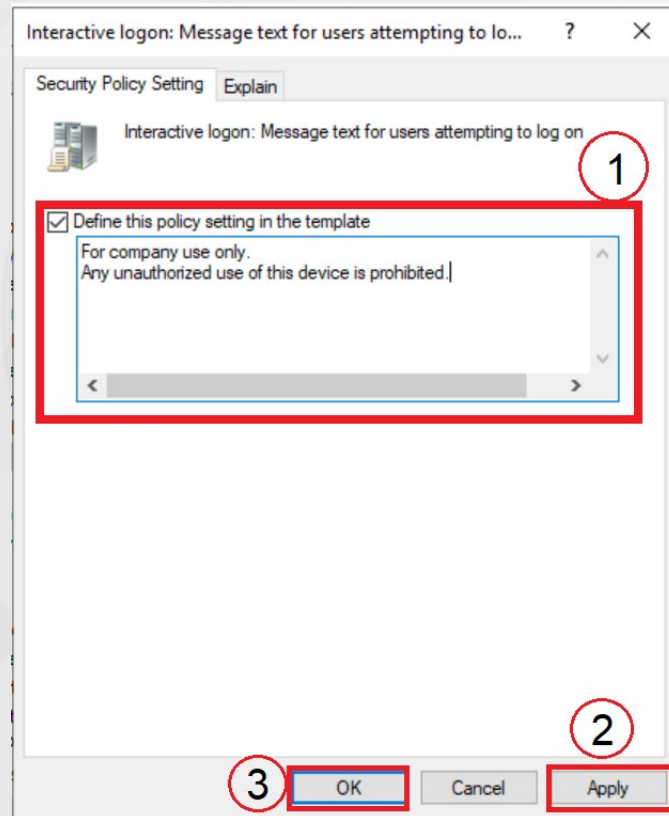
9. and we finish by clicking where it says Security Options (3), we look for the option that says, "Interactive login: Message text for users trying to log in" (4) and we double click it



10. A new pop-up window named "Interactive logon: Message text for users trying to log in" opens, we click on the dialog box that says Define these policy settings

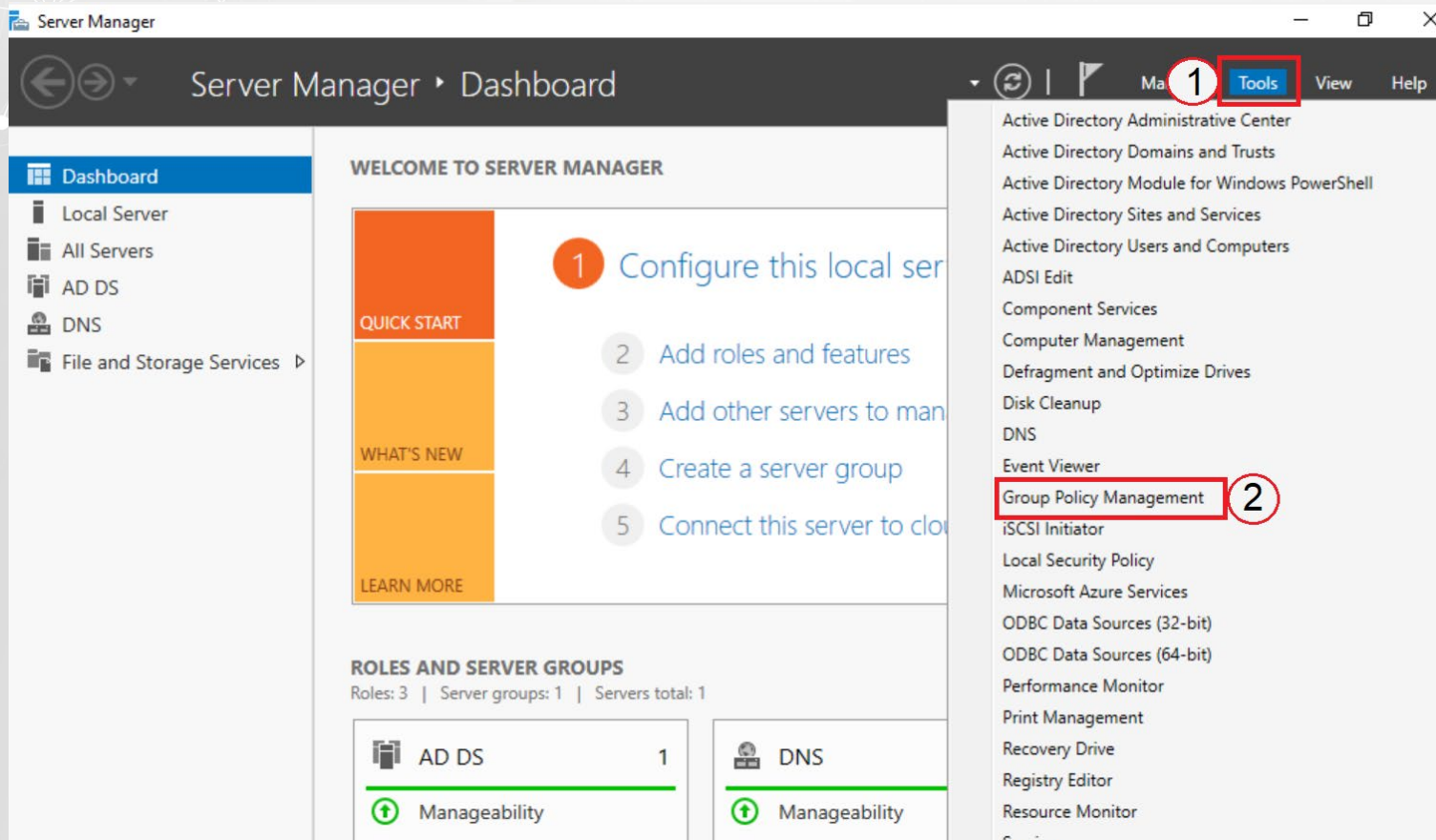


11. When the dialog box is activated. We write: **For company use only. Any unauthorized use of this device is prohibited** (1), at the end click Apply (2) and OK (3) and that's it.

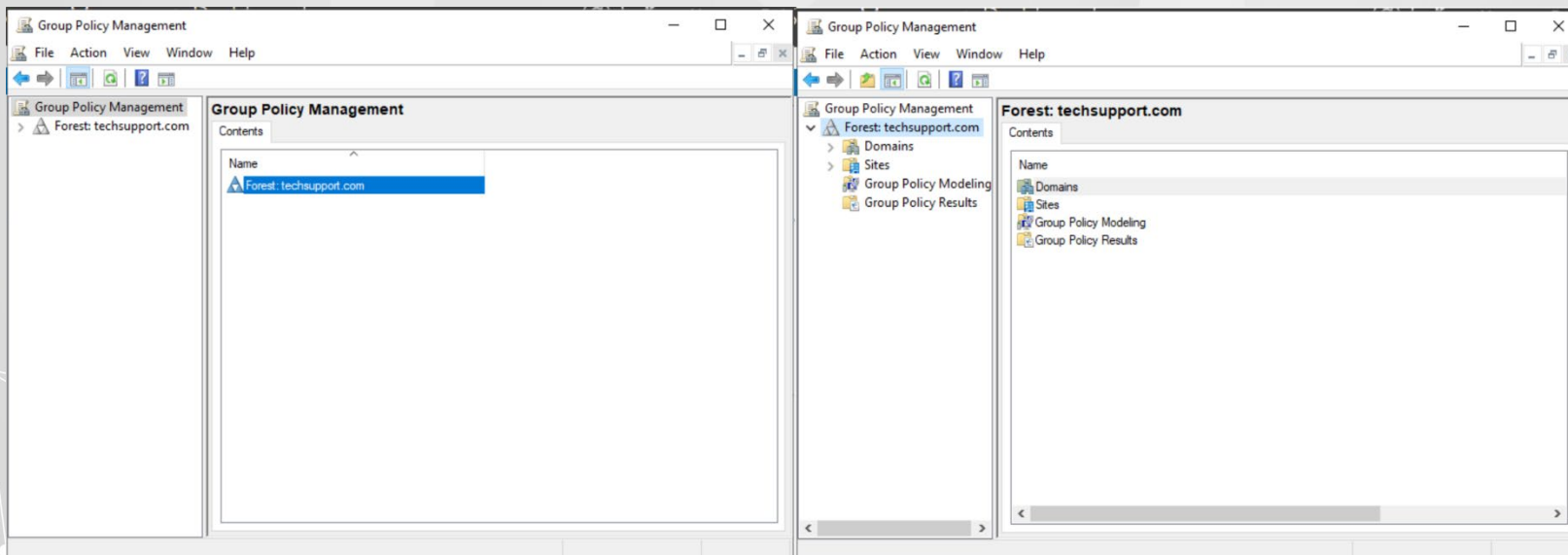


Task 2: Create a policy to lock the device after 10 minutes of inactivity

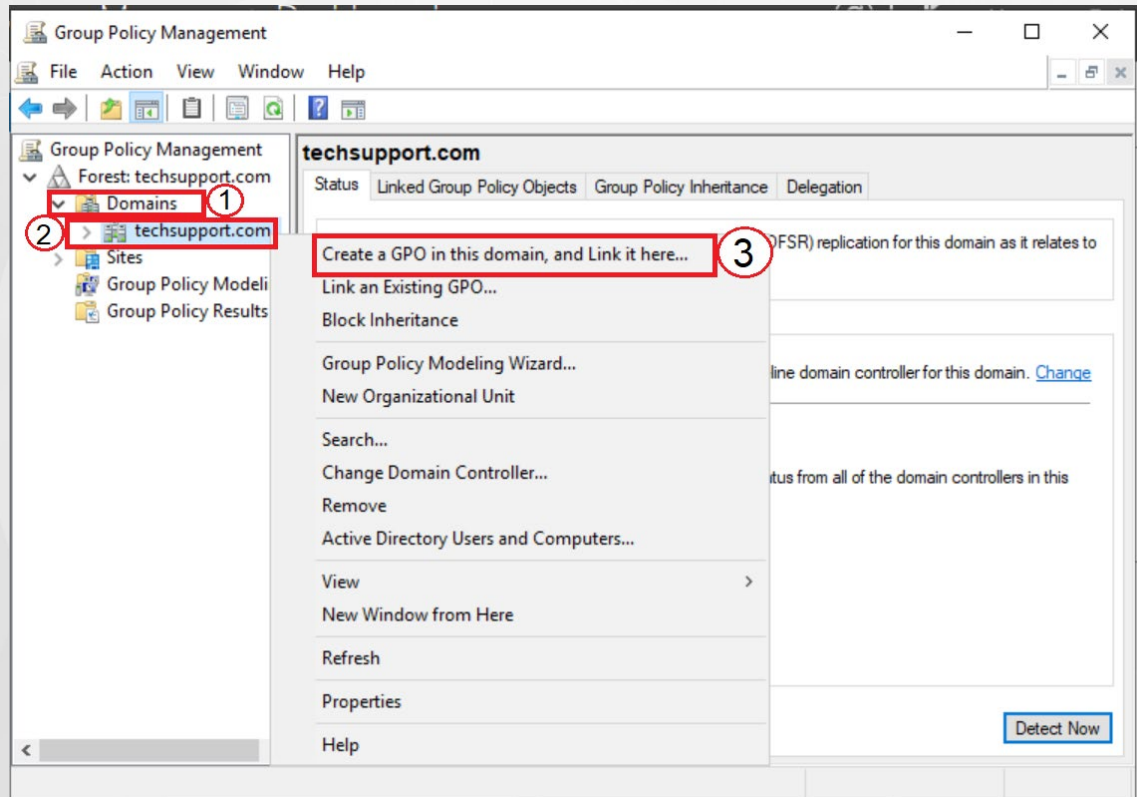
1. Enter the server manager, click on tools (1), look for the Group Policy management option (2) and click



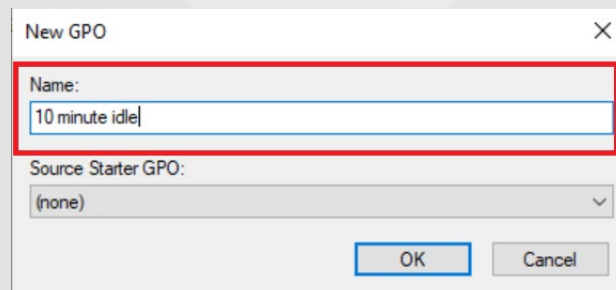
2. Look for the domains option and display it



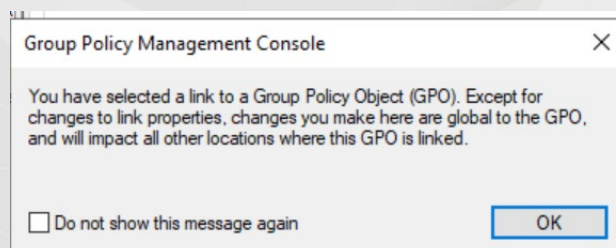
1. Left click domains (1) then on the **techsupport.com** domain (2) where we want to assign the GPO, we right click and select the option Create a GPO in this domain (3)



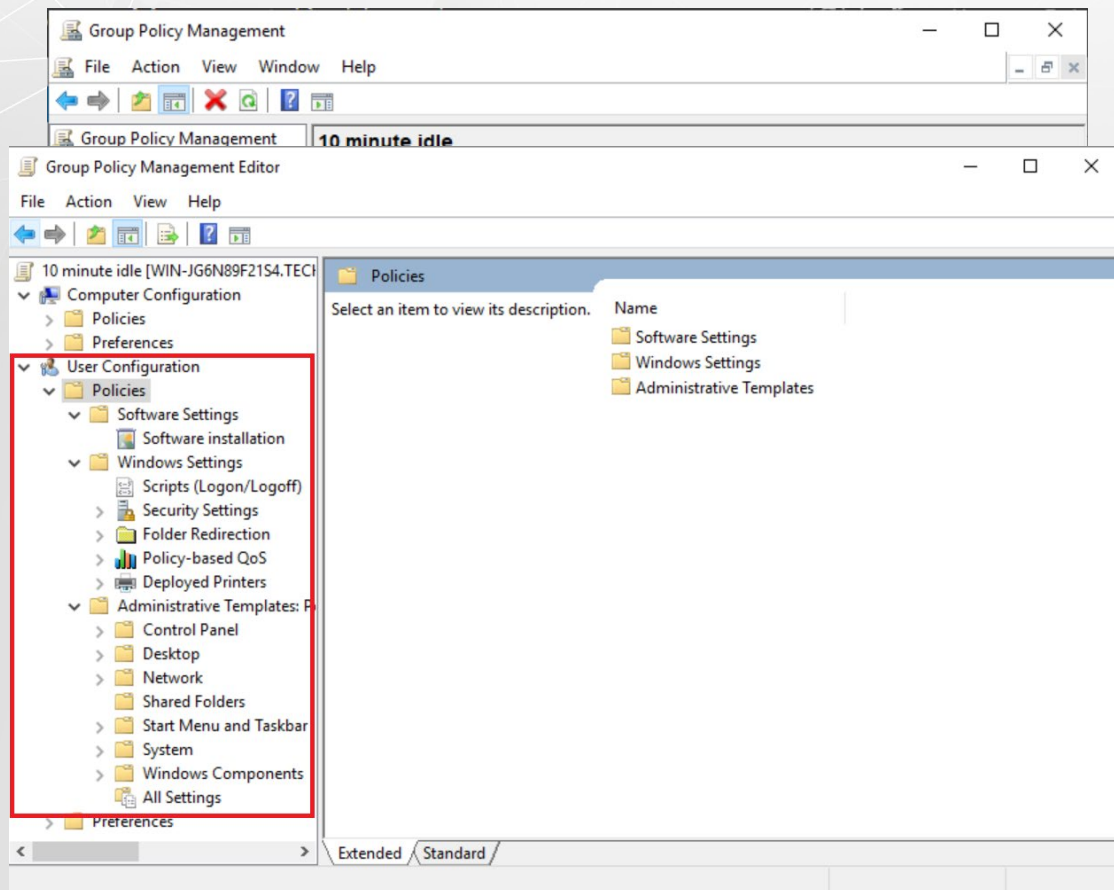
2. In order to identify the GPO, we call it **10 minutes idle**



3. Now if a warning message appears, we just click on ok

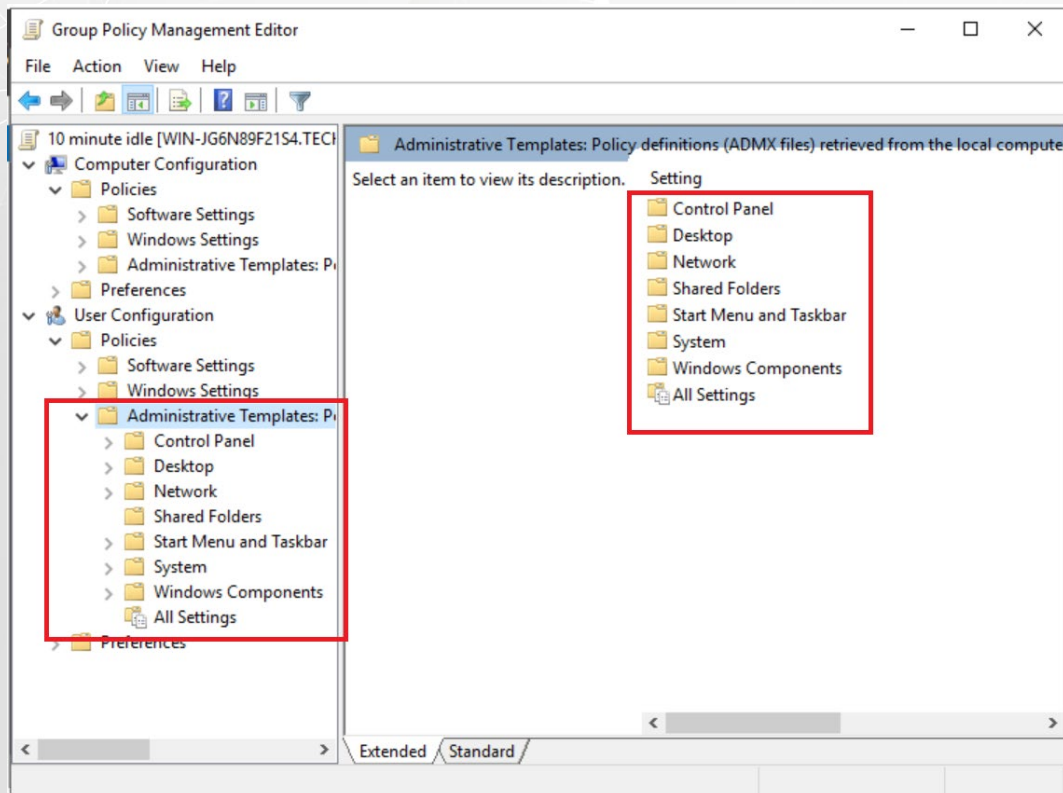


4. Once the GPO is created, right click on the name, and choose the edit option

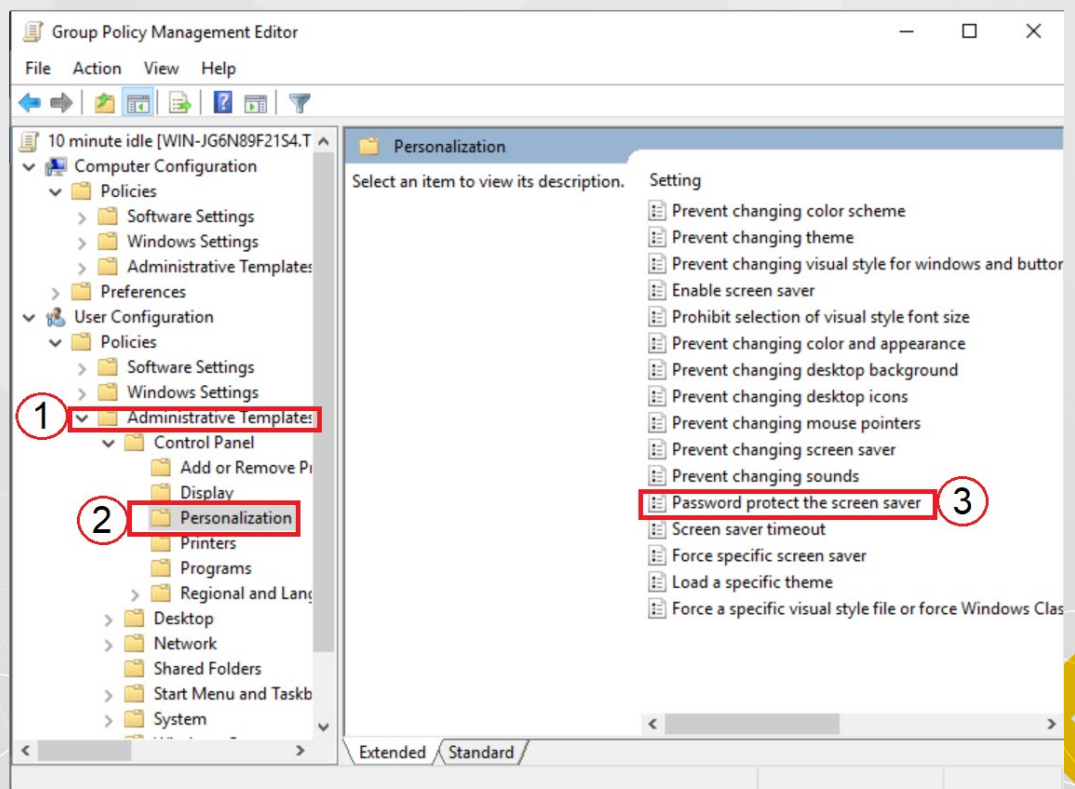


5. A pop-up window named Group Policy Management Editor will appear, In the section on the left side, we select the User Configuration option and then click where the policies folder is to expand it.

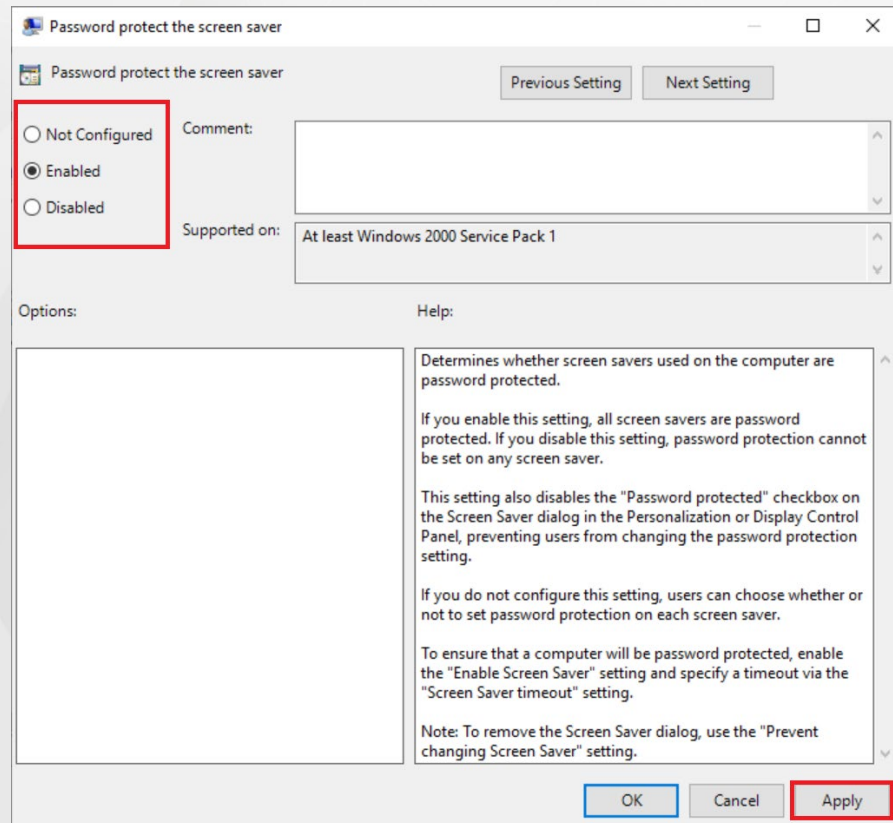
6. We look where it says Administrative Templates and expand it



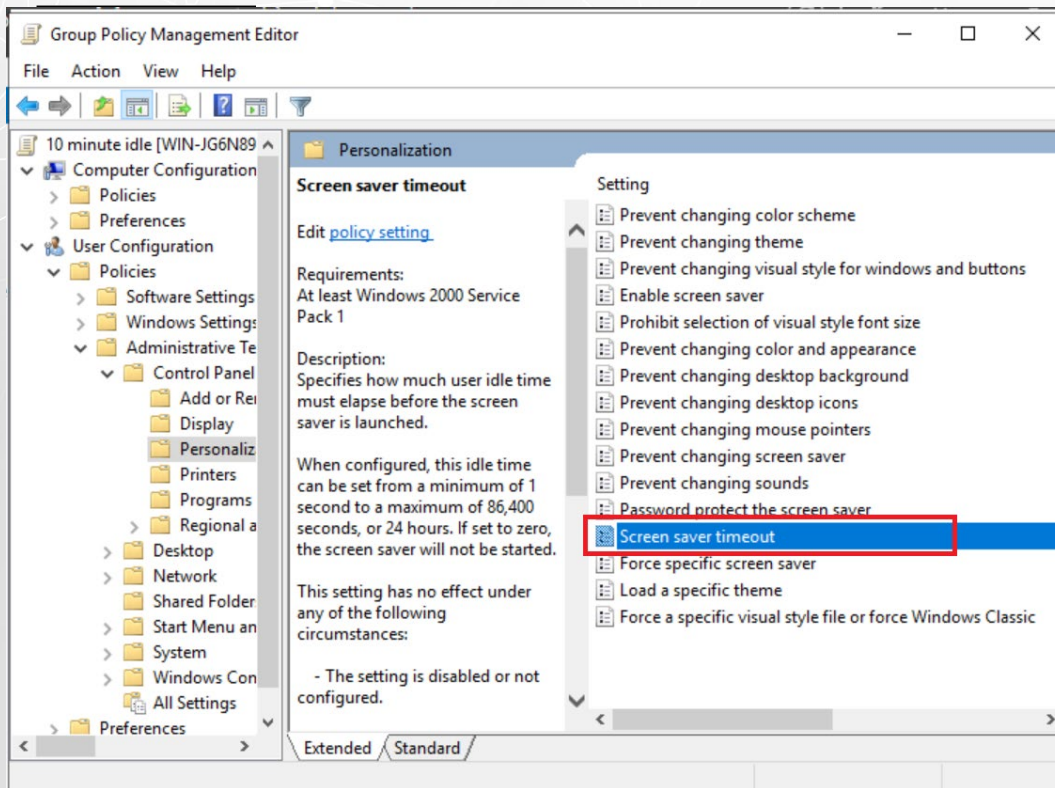
7. We choose the Control Panel option of the Administrative Templates (1) and display it, then we double click in the Personalization option (2), a list appears, we look for the option Password Protect the Screen Saver (3)



8. We double click Password Protect the Screen Saver option and select enable, then click apply and ok



9. Now to activate the timeout in the same window where we activated the password protection, we click on the option below that says screen saver timeout and double click on it.



10. We click on enabled (1) and below it says number of seconds to wait to enable the screen saver we write **600 seconds** (2) which is equivalent to 10 minutes. We click on apply (3) and ok (4), we can now close the editor window.

Screen saver timeout

Screen saver timeout

Previous Setting Next Setting

☐ Not Configured
☒ Enabled
☐ Disabled

Comment: 1

Supported on: At least Windows 2000 Service Pack 1

Options:

Number of seconds to wait to enable the screen saver

Seconds: 600 2

Help:

Specifies how much user idle time must elapse before the screen saver is launched.

When configured, this idle time can be set from a minimum of 1 second to a maximum of 86,400 seconds, or 24 hours. If set to zero, the screen saver will not be started.

This setting has no effect under any of the following circumstances:

- The setting is disabled or not configured.
- The wait time is set to zero.
- The "Enable Screen Saver" setting is disabled.
- Neither the "Screen saver executable name" setting nor the Screen Saver dialog of the client computer's Personalization or Display Control Panel specifies a valid existing screen saver program on the client.

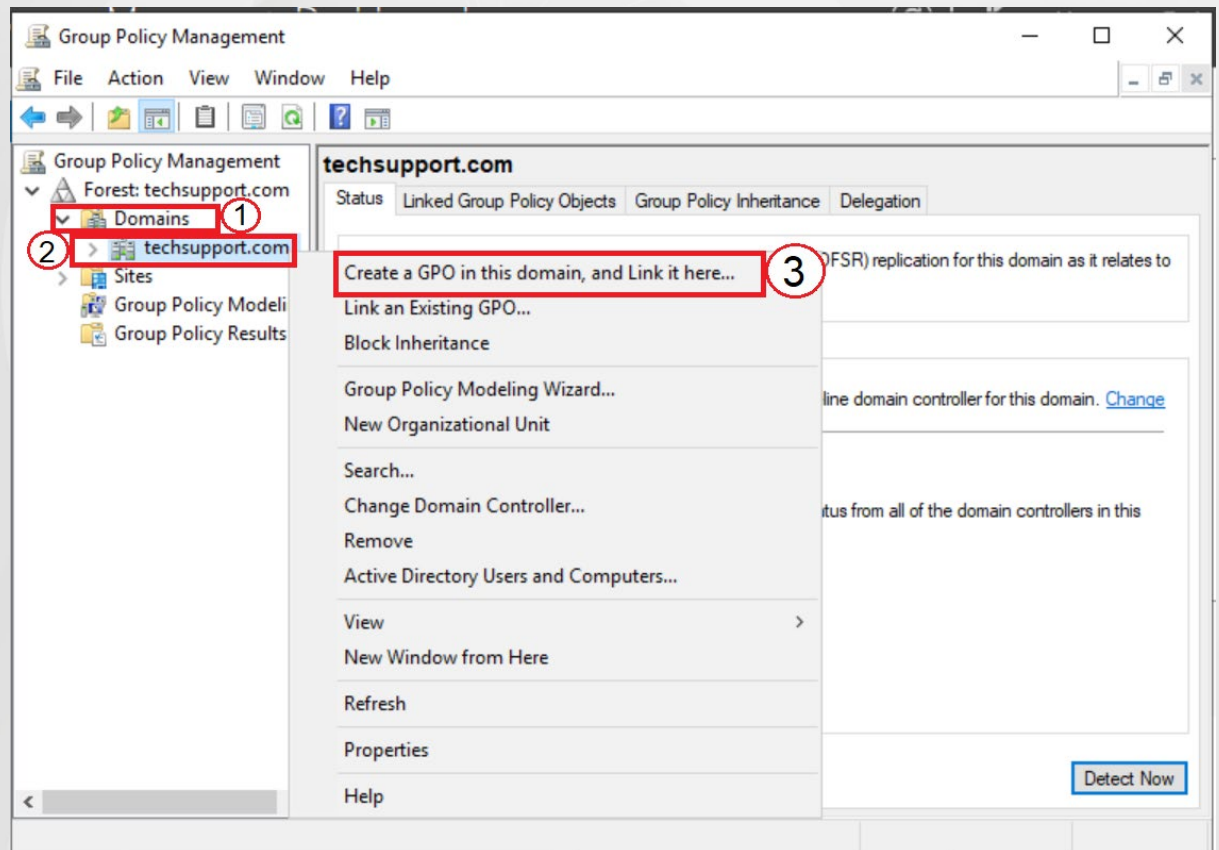
3

4 OK Cancel Apply

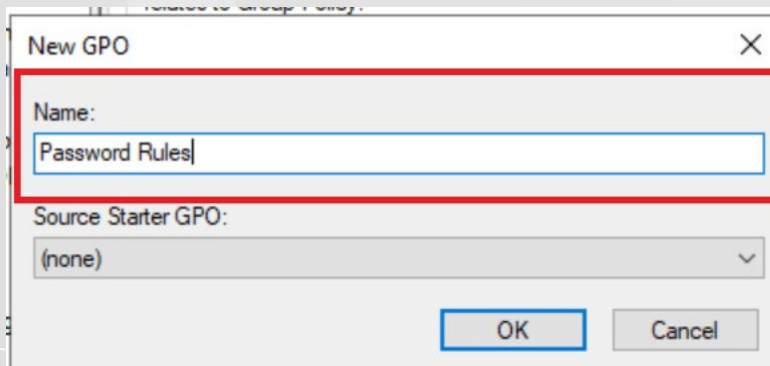
Task 3: Password GPOs

Now we are going to apply a very common Passwords GPO and that is applied in almost all companies:

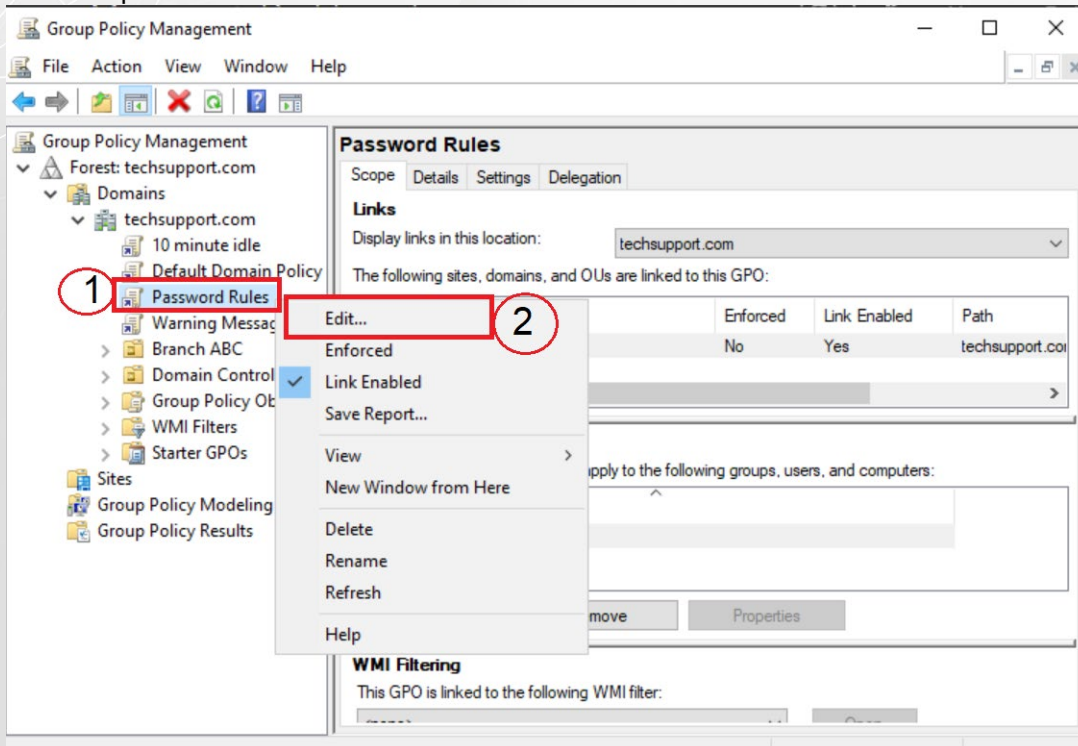
1. We are going to apply this policy at the domain level (1), so we select Techsupport.com (2) and right click, we select the option to Create a GPO (3)



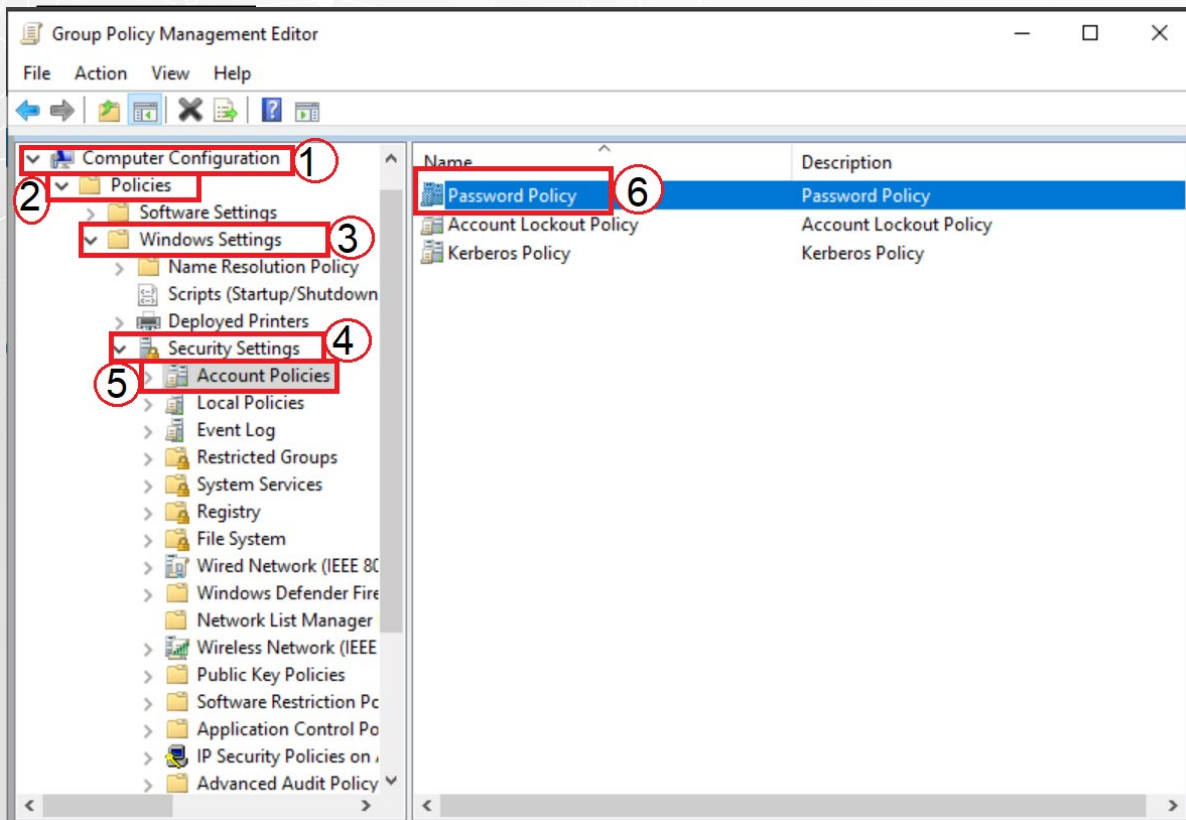
2. We are going to name the GPO **Password Rules** and click ok



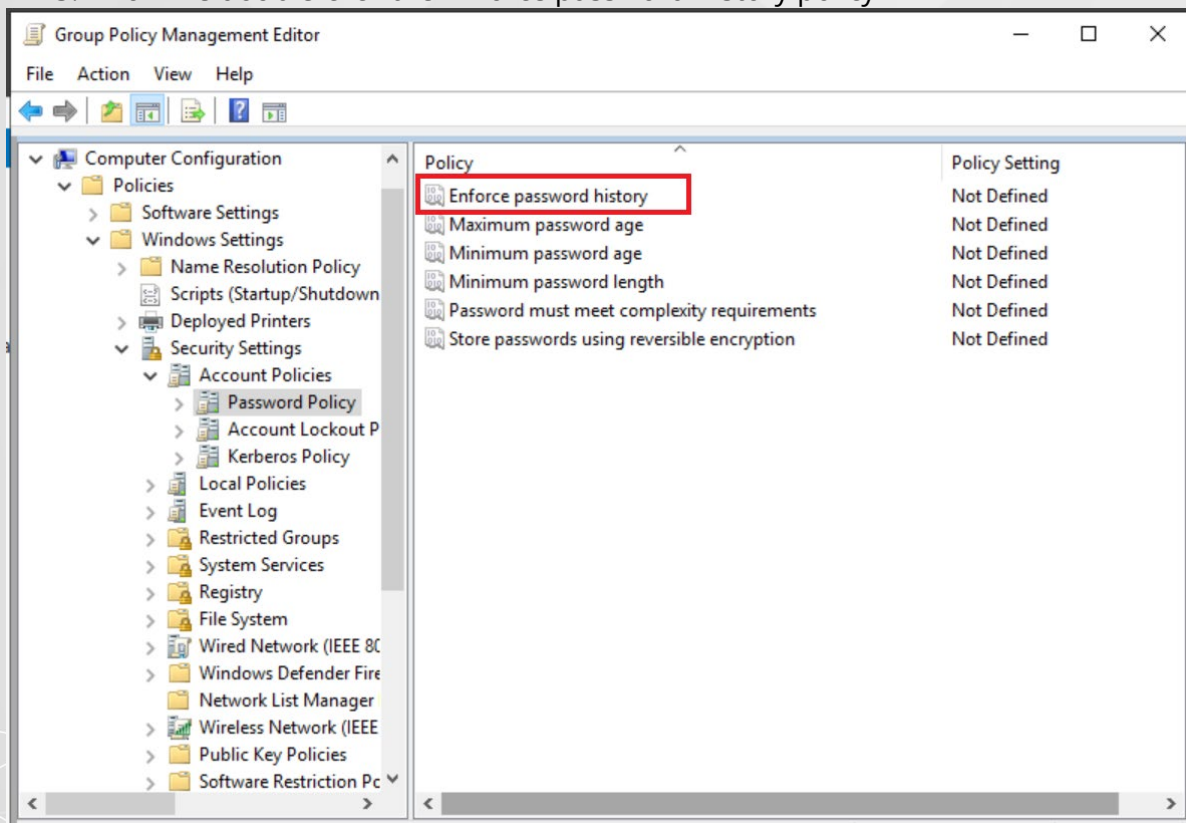
- Now we select password rules and right click on it and then select the edit option



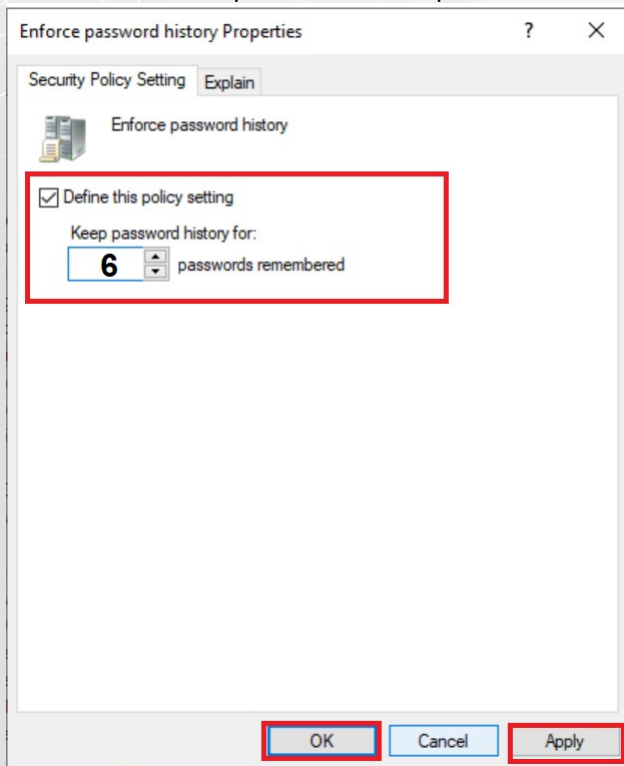
- In the new window we display the windows settings folder (2) in computer configuration (1), display the security settings (4) and select the Account policies (5), then click on the Password Policy (6)



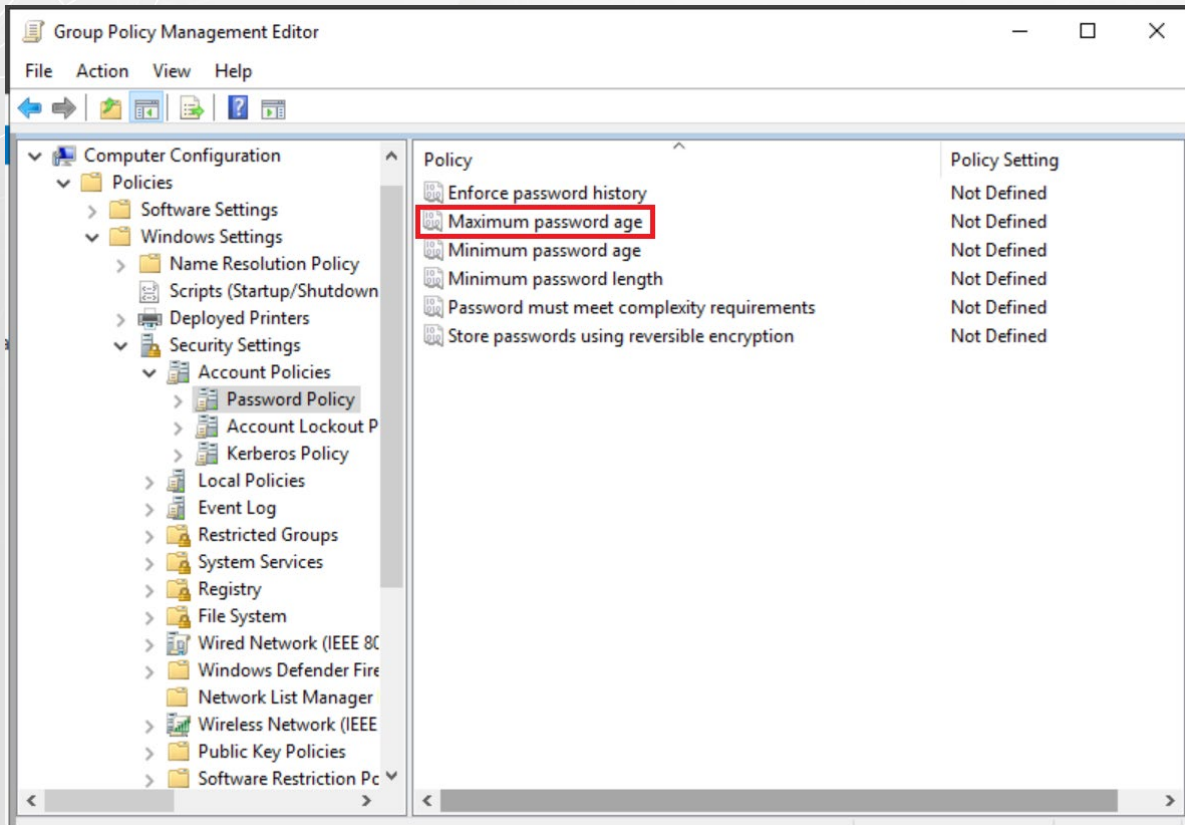
5. Now we double-click the Enforce password history policy



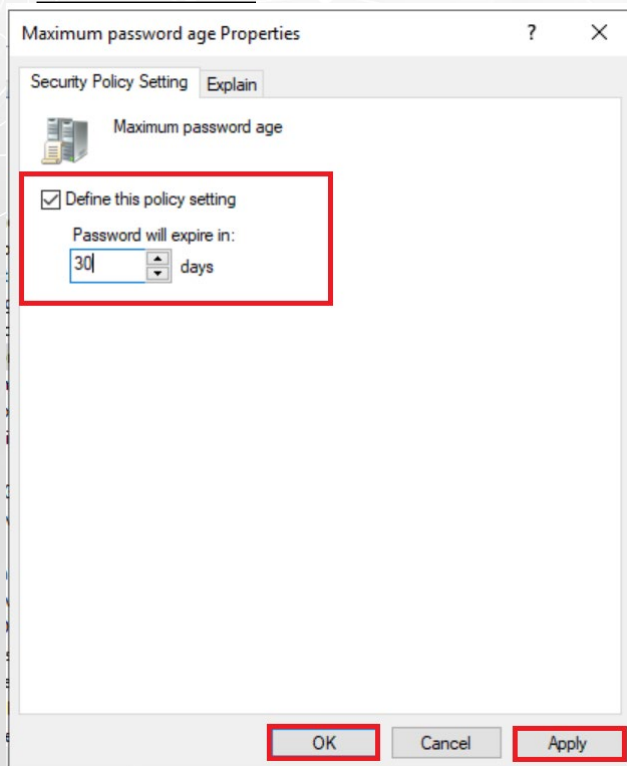
6. When the pop-up window appears mark the check that says define this policy setting and write a 6 where it says passwords remember. This means that we cannot repeat the same password until we have written 7 new ones



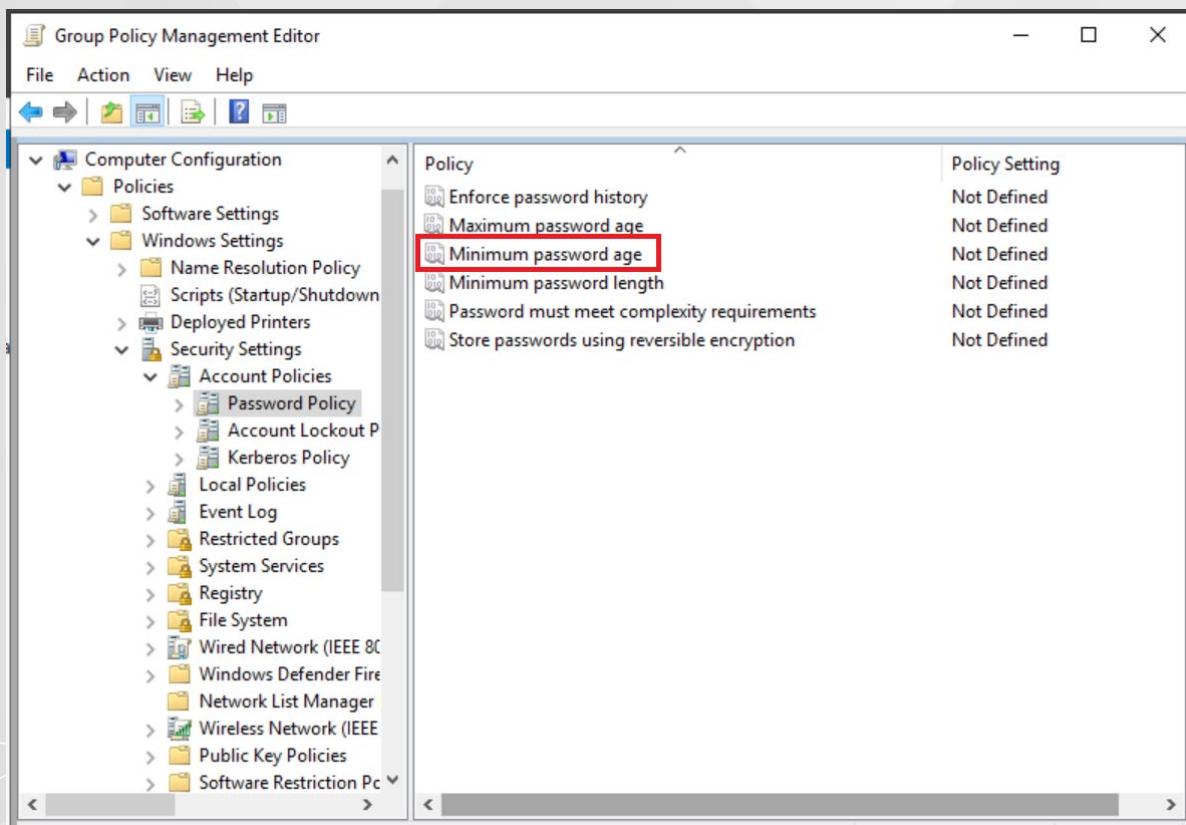
7. Now we double click on the maximum password age option



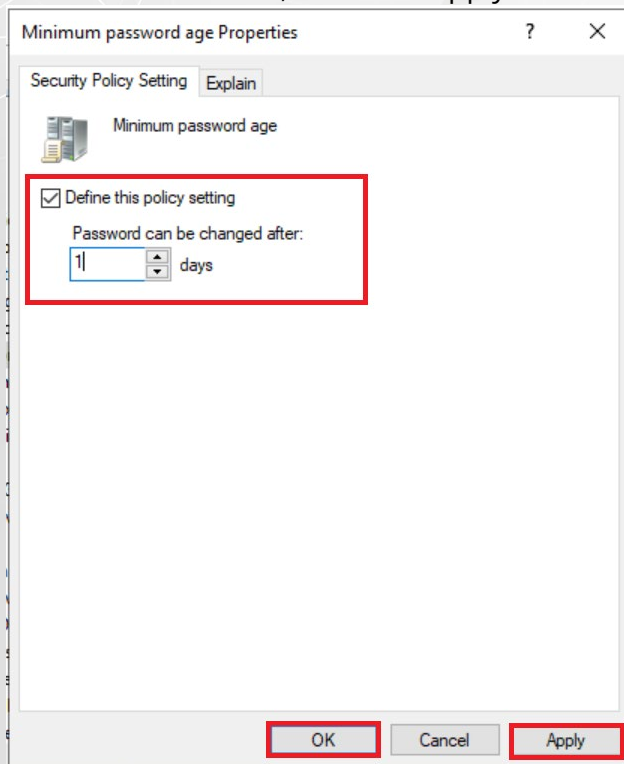
8. We click on the check box and put 30 as the maximum password age, the policy establishes that it must be changed every month, then click apply and ok



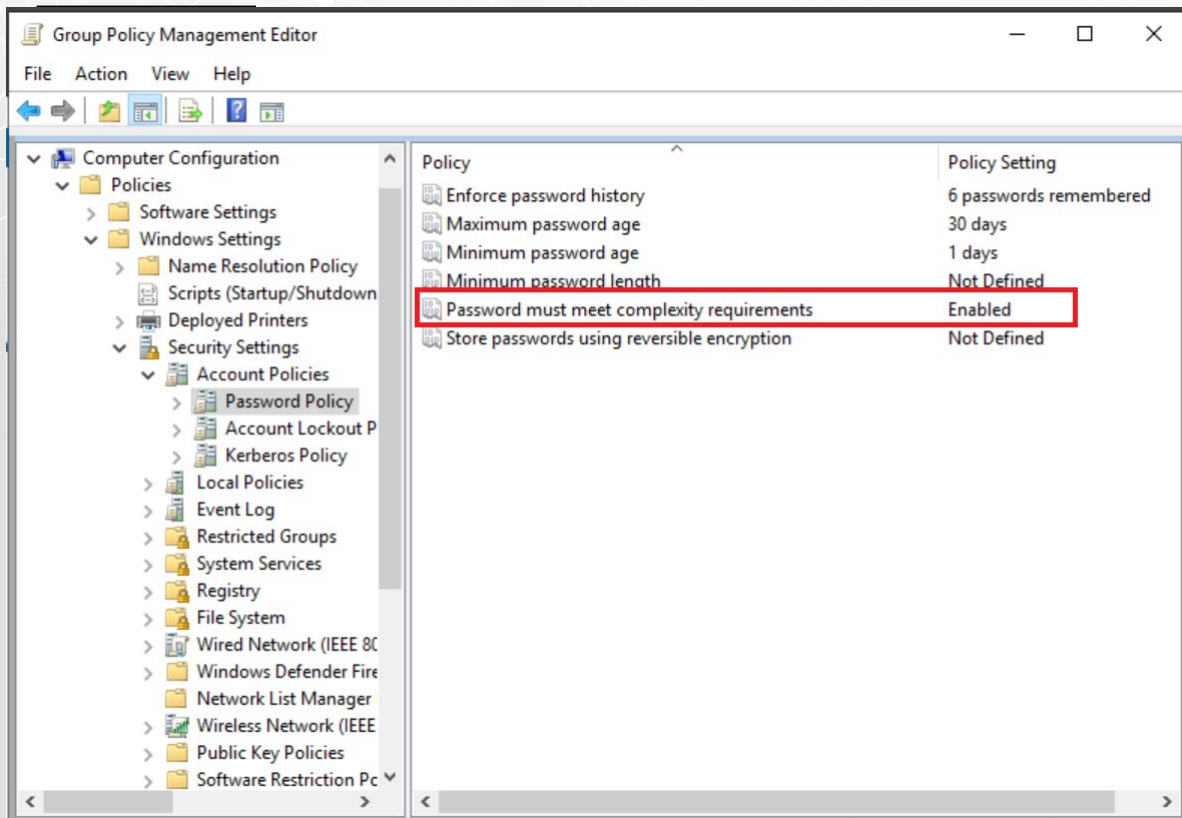
9. Now double click where it says minimum password age



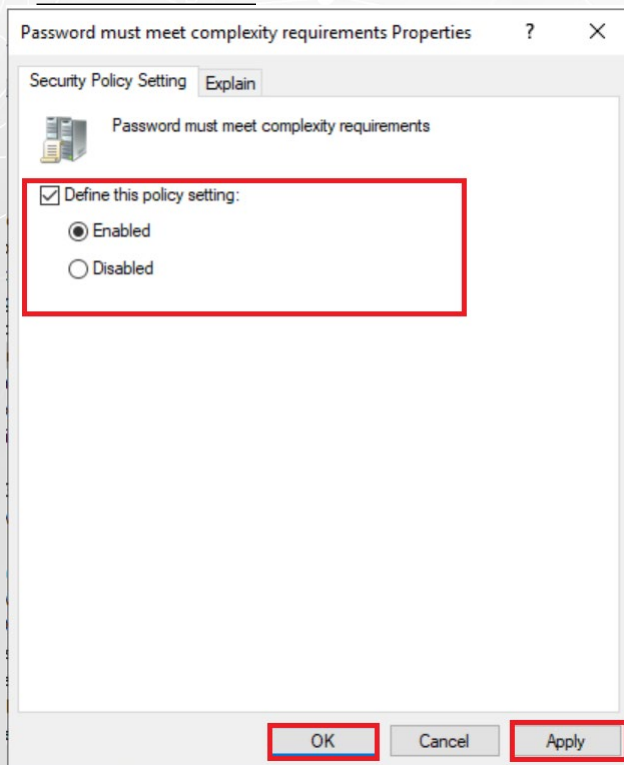
10. We mark the box and change the number to 1, this means that once the password has been changed, at least one day must pass to change it for a different one, then click apply and ok



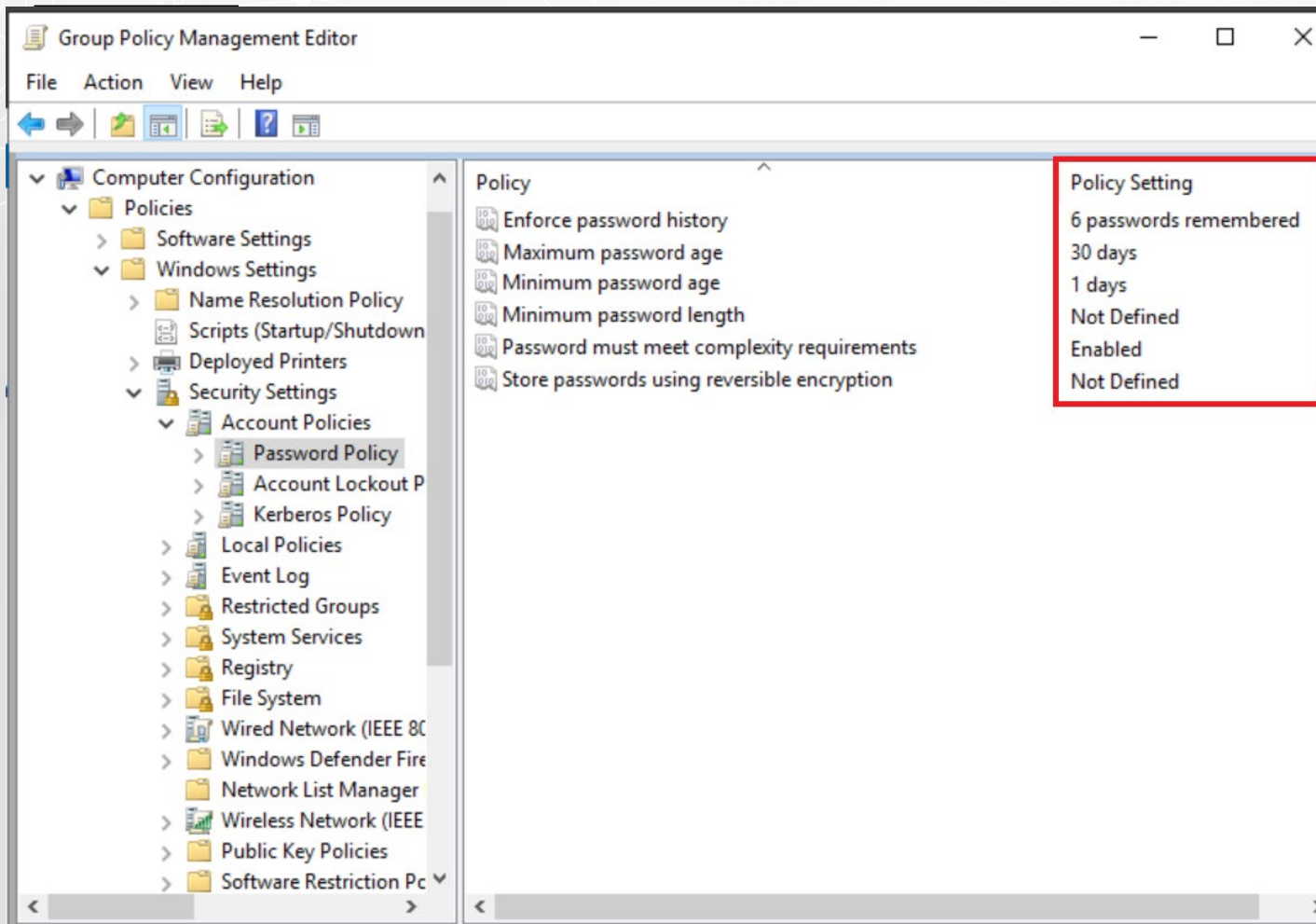
11. Finally, we double-click where it says the password must meet the complexity requirements.



12. We mark the check and then select the enabled option, this rule forces users to use uppercase, lowercase, numbers, and punctuation marks, we click on apply and ok, now we can close the window

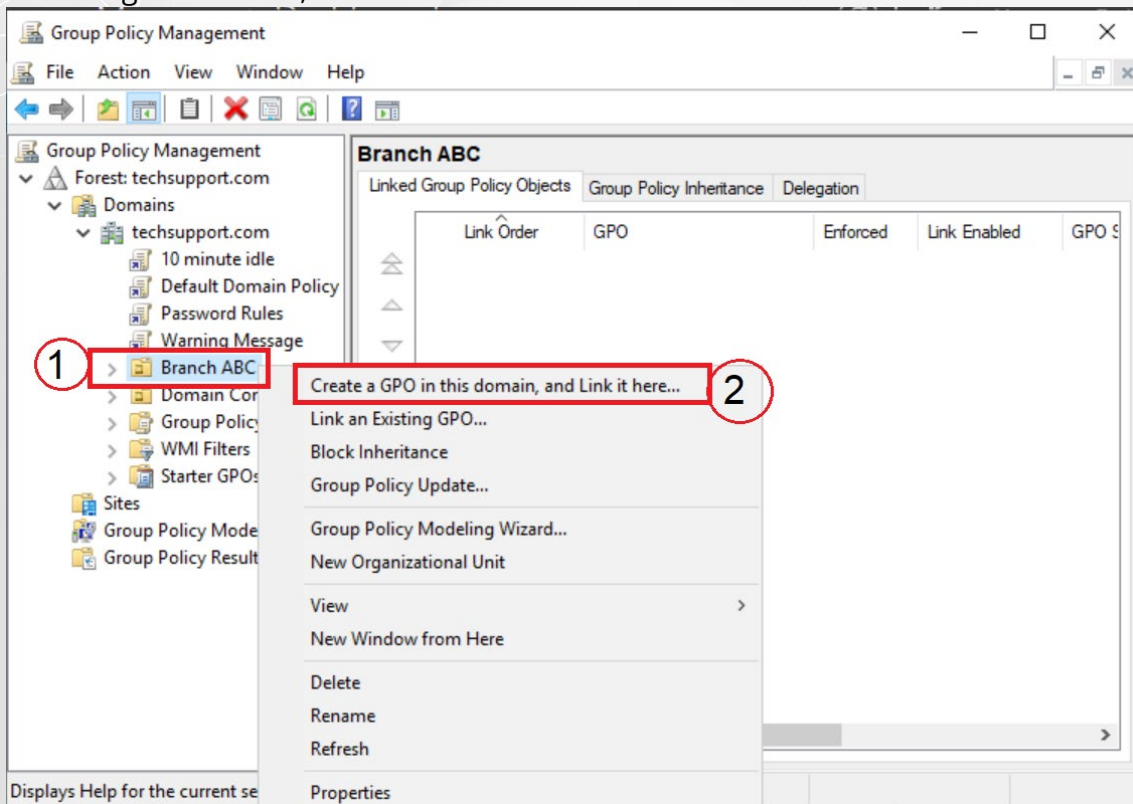


13. The policies are ready, it should look like the following image, if everything is correct, we can close the editor window.

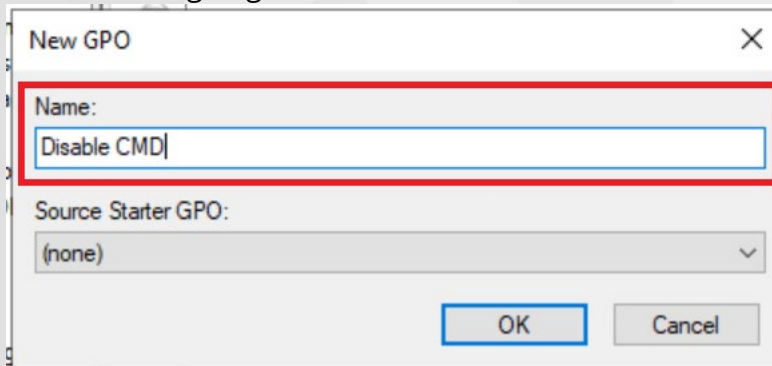


Task 4: OU GPOs

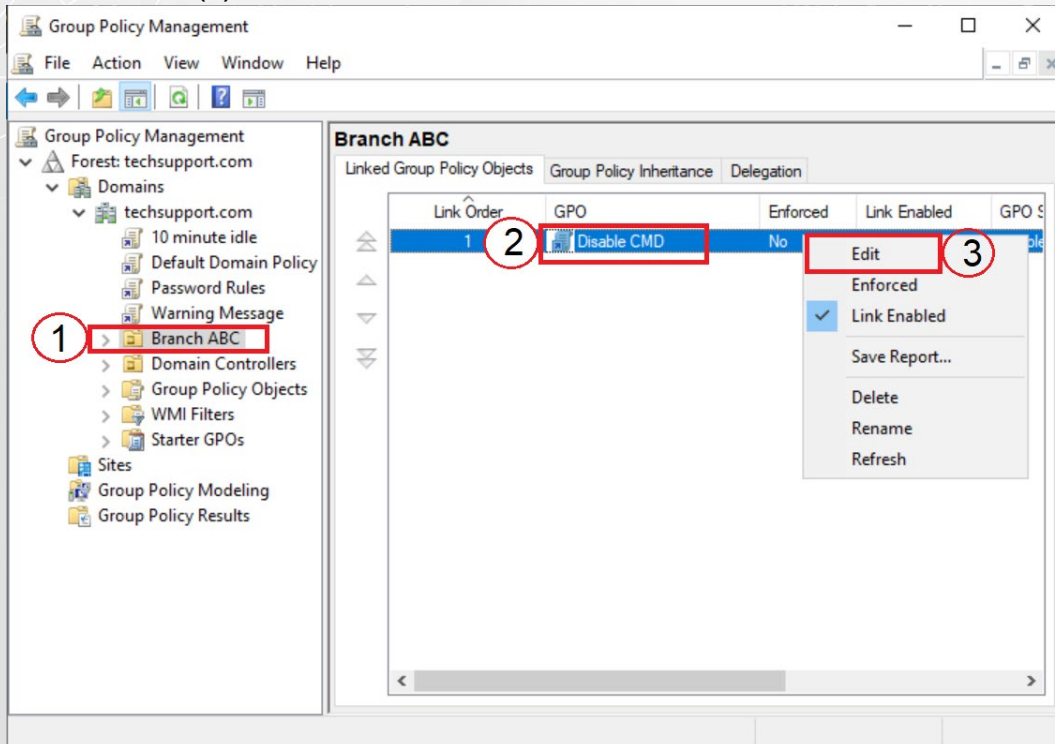
1. Now we are going to create a GPO directly in an OU, select Branch ABC and right click on it, then click on create a GPO



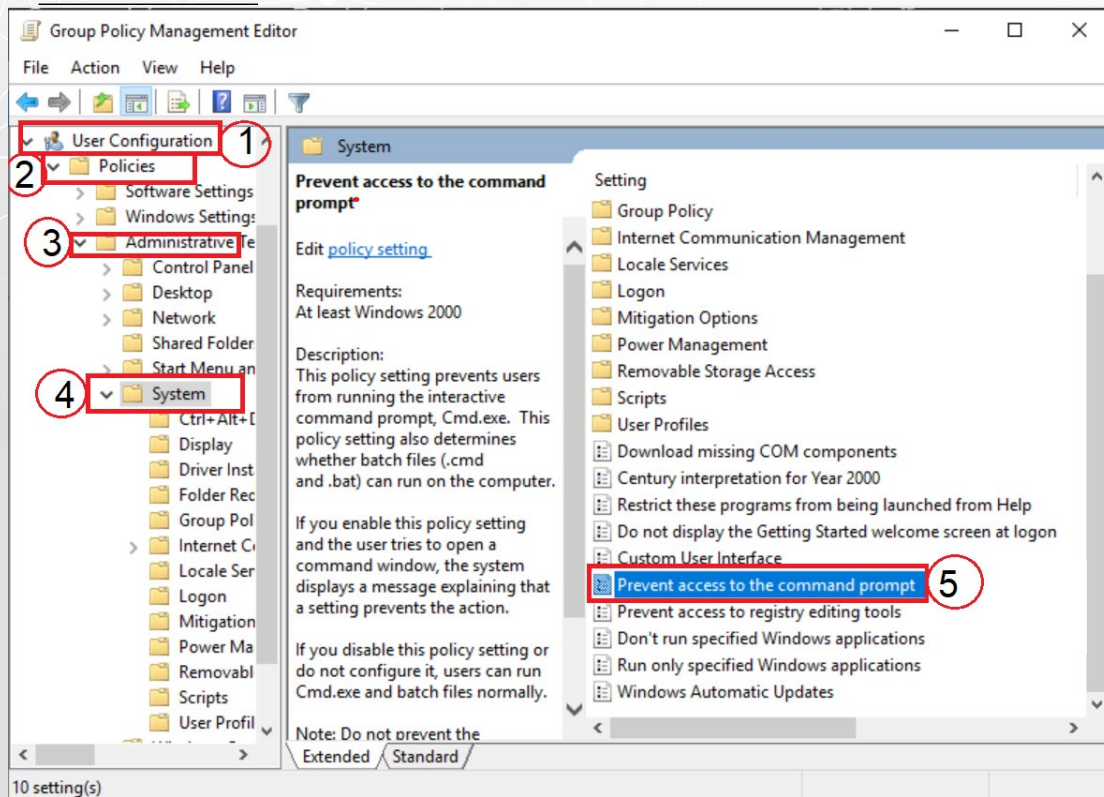
2. We're going to name this GPO "Disable CMD" and click ok



3. Now we are going to click on Branch ABC (1), select the GPO (2) and right click to Edit (3)



4. Let's go to User configuration and display the Policies option then we display where it says administrative template and click in System, look for the option "Prevent Access to the command prompt" and double click it



5. In the pop-up window we click on enabled (1), in comment we write **Hey you cannot use this tool** (2). Finally, in the box below on the left where it says disable the command prompt script, we change the option to yes (3), we do apply (4) and ok (5), and that's it, we can close the editor window.

Prevent access to the command prompt

Previous Setting Next Setting

☐ Not Configured
☒ Enabled **1**
☐ Disabled

Comment: Hey you cannot use this tool **2**

Supported on: At least Windows 2000

Options:

Disable the command prompt script processing also?
Yes **3**

Help:

This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

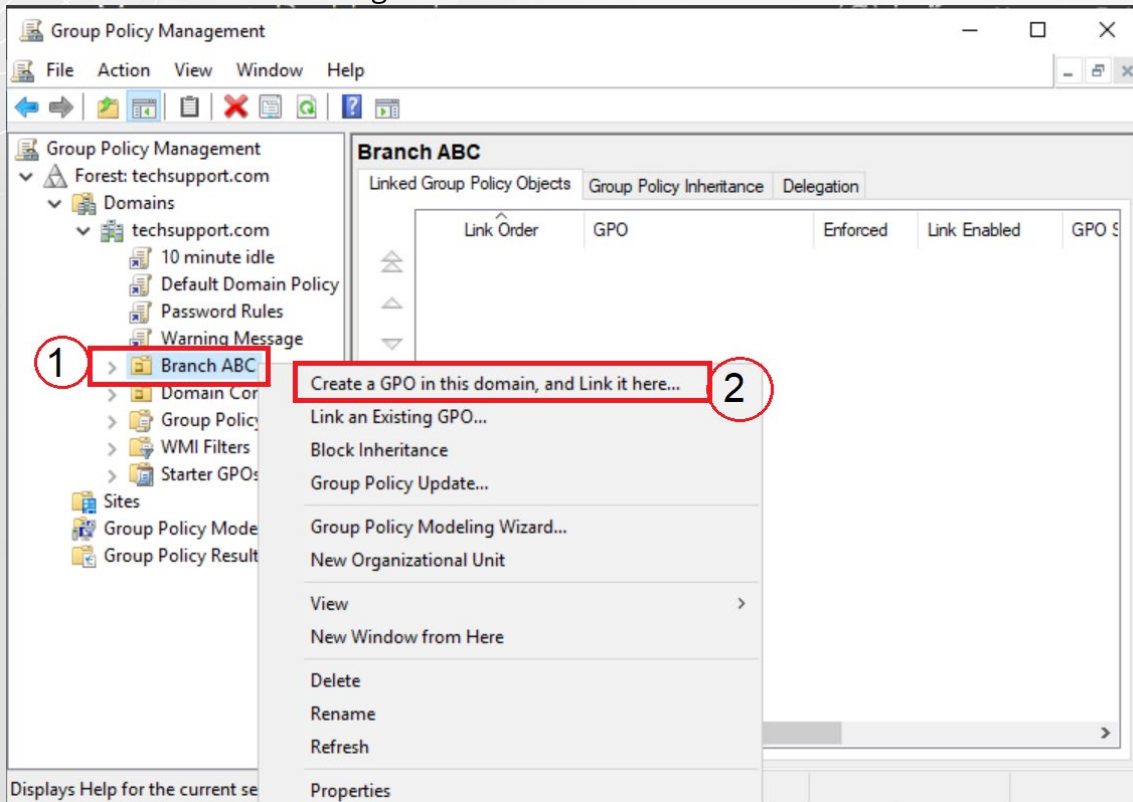
Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

4

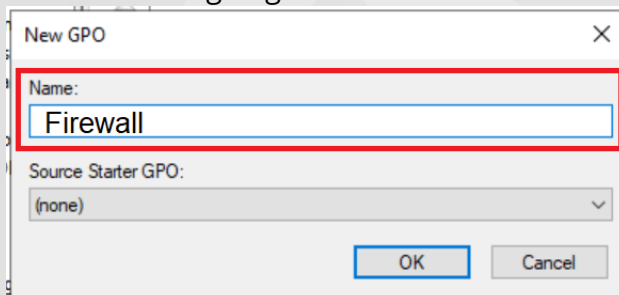
5 OK Cancel Apply

Task 5: Firewall

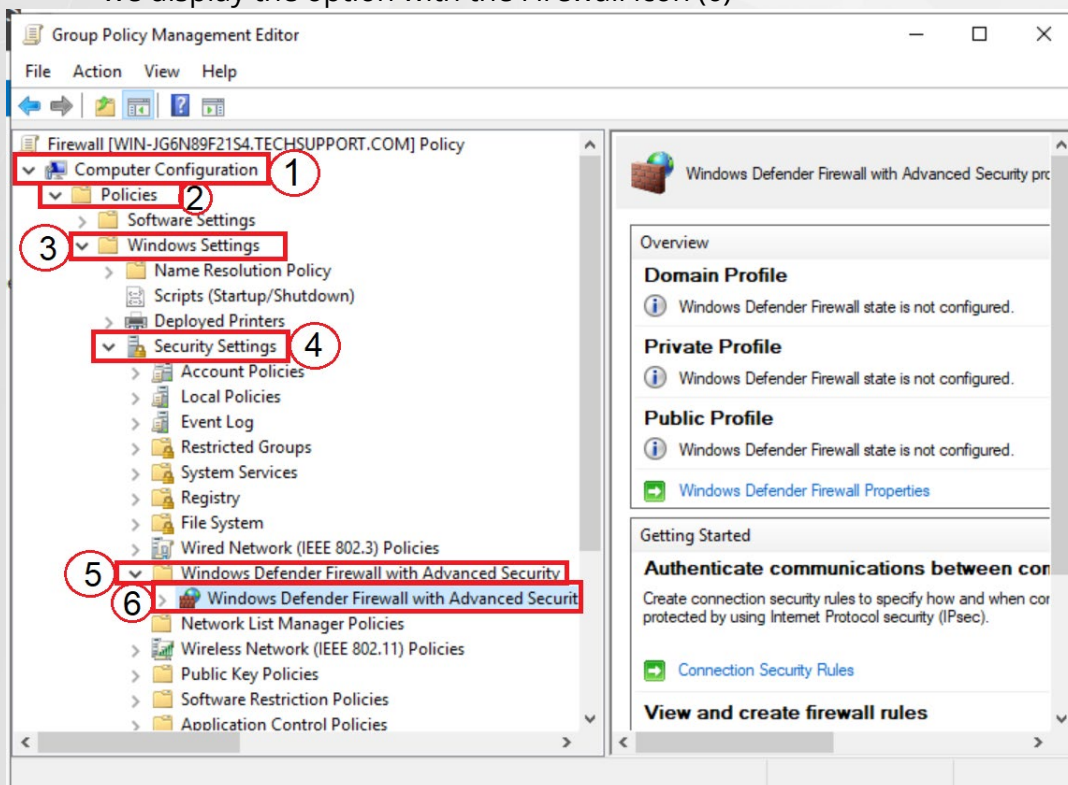
1. In ABC Branch we right click and click on Create a GPO



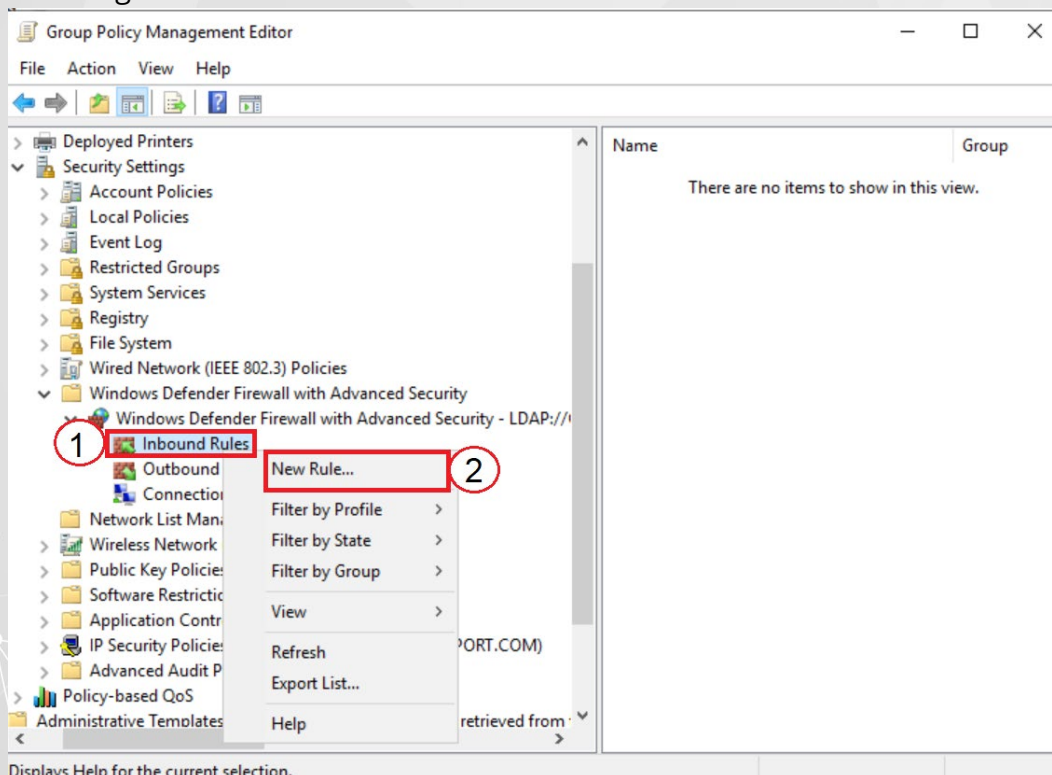
2. We are going to name the GPO **Firewall** and click ok



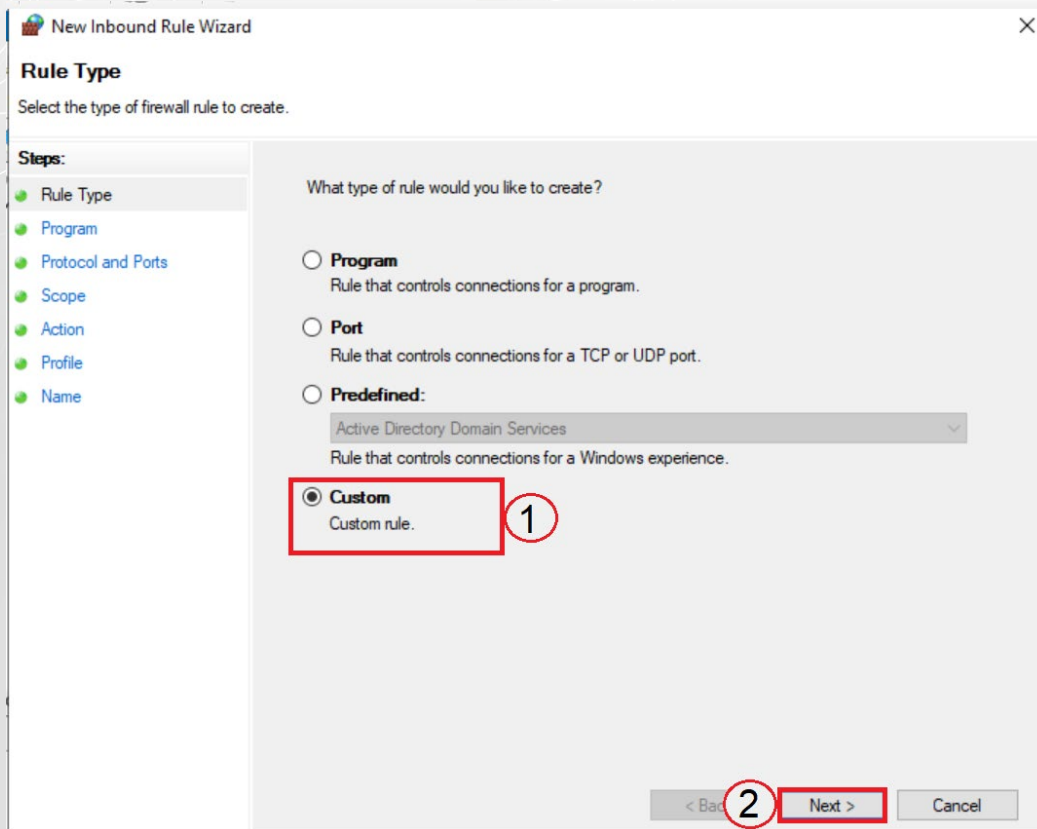
- The editor window will appear, and in the section on the left side, we select the Computer Configuration (1) option, display and click on the policies option (2) and then click and display the windows settings (3), select the security settings (4) then the Windows Defender Firewall with Advanced Security folder is, to expand it (5). Within Windows defender Firewall with Advanced Security folder, we display the option with the Firewall icon (6)



- We right click on inbound rules and click on new rule.



5. In the wizard we click on Custom (1) and then next (2)



6. In the next window we select all programs and then next

New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

☒ **All programs**
Rule applies to all connections on the computer that match other rule properties. **1**

☐ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services

Specify which services this rule applies to.

< Back **2** Cancel

7. In the next window we leave the option on any and then next

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: Any **1**

Protocol number: 0

Local port: All Ports

Example: 80, 443, 5000-5010

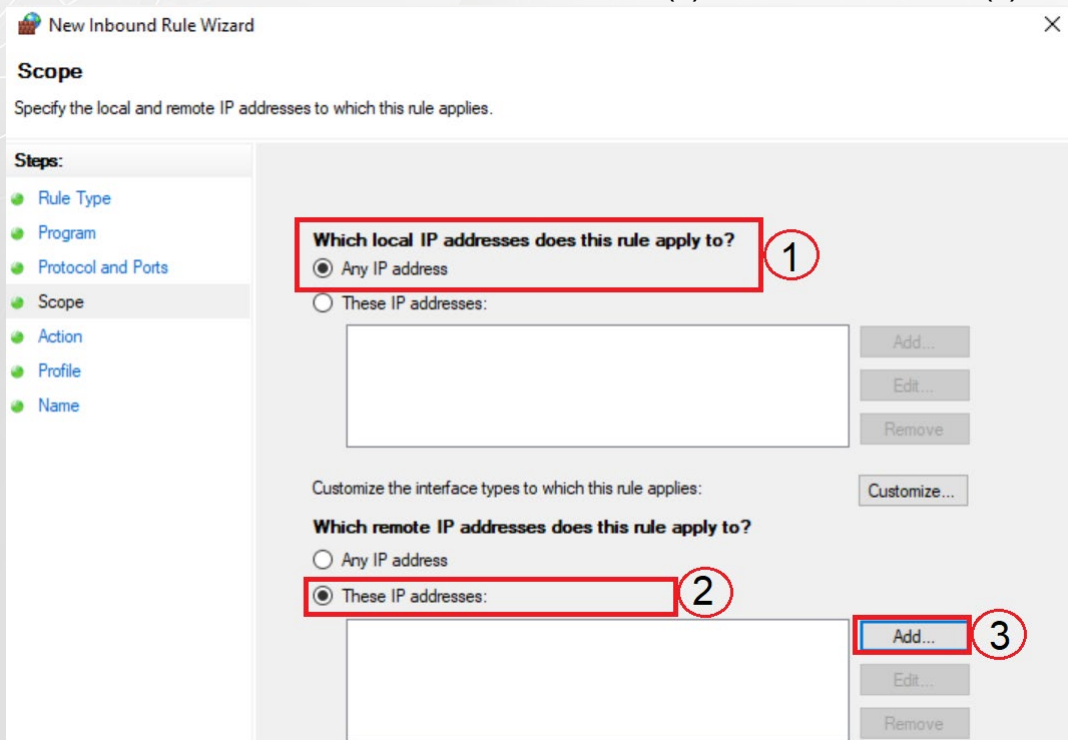
Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

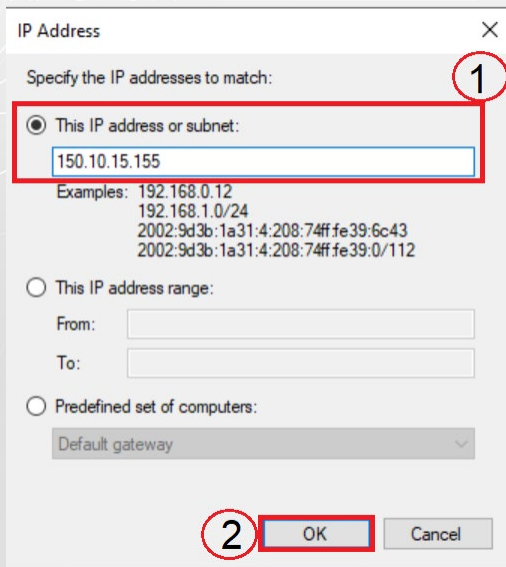
< Back **2** Cancel

8. In the next one selects “Any IP addresses” option (1), below where it says which remote IP we select “These IP addresses” (2) and we click on add (3)



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Scope' step. The window title is 'New Inbound Rule Wizard' with a close button. The section is titled 'Scope' with the instruction 'Specify the local and remote IP addresses to which this rule applies.' On the left, a 'Steps:' sidebar lists: Rule Type, Program, Protocol and Ports, Scope (highlighted), Action, Profile, and Name. The main area has two sections. The first, 'Which local IP addresses does this rule apply to?', has a red box around the 'Any IP address' radio button, which is also circled with a red '1'. Below it is a text box and buttons for 'Add...', 'Edit...', and 'Remove'. The second section, 'Which remote IP addresses does this rule apply to?', has a red box around the 'These IP addresses:' radio button, which is circled with a red '2'. Below it is a text box and buttons for 'Add...', 'Edit...', and 'Remove'. The 'Add...' button in the second section is circled with a red '3'. A 'Customize...' button is also present between the two sections.

9. In the pop-up window we write 150.10.15.155 (1) at the top and click ok (2)



IP Address

Specify the IP addresses to match:

☒ This IP address or subnet:

150.10.15.155

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

☐ This IP address range:

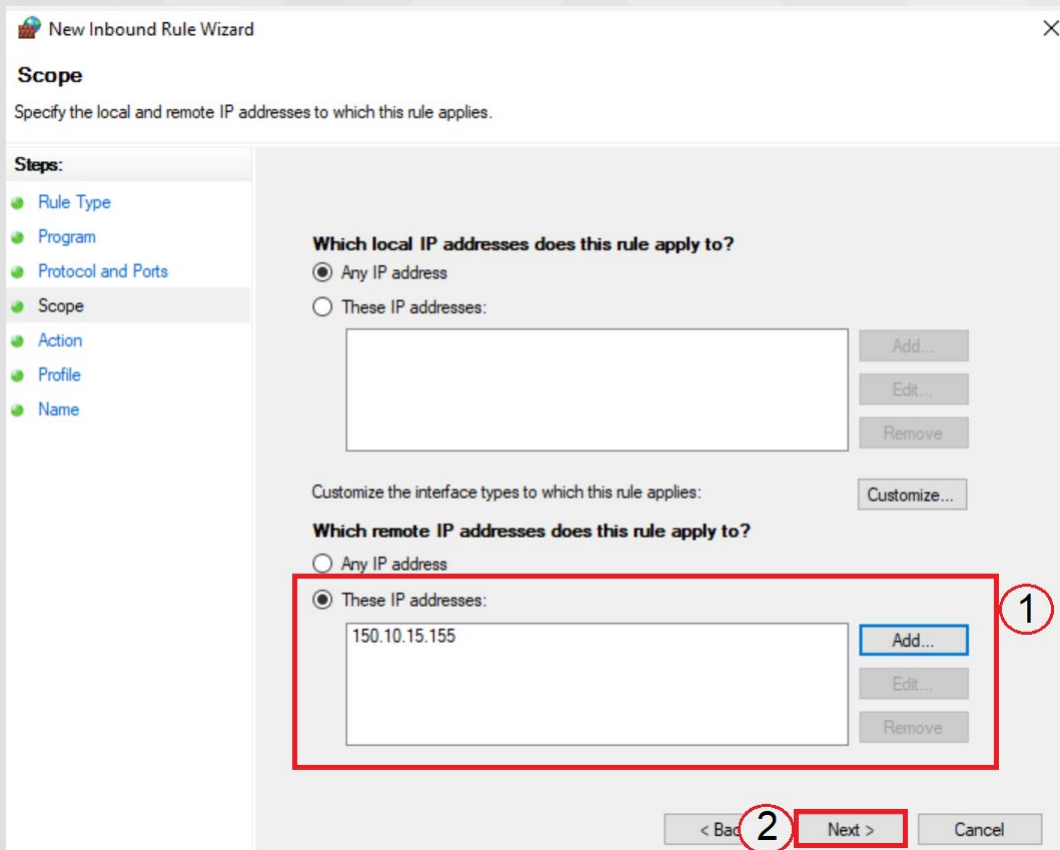
From:
To:

☐ Predefined set of computers:

Default gateway

2 OK Cancel

10. In the wizard click next to the other window (2)



New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

Which remote IP addresses does this rule apply to?

☐ Any IP address

☒ These IP addresses:

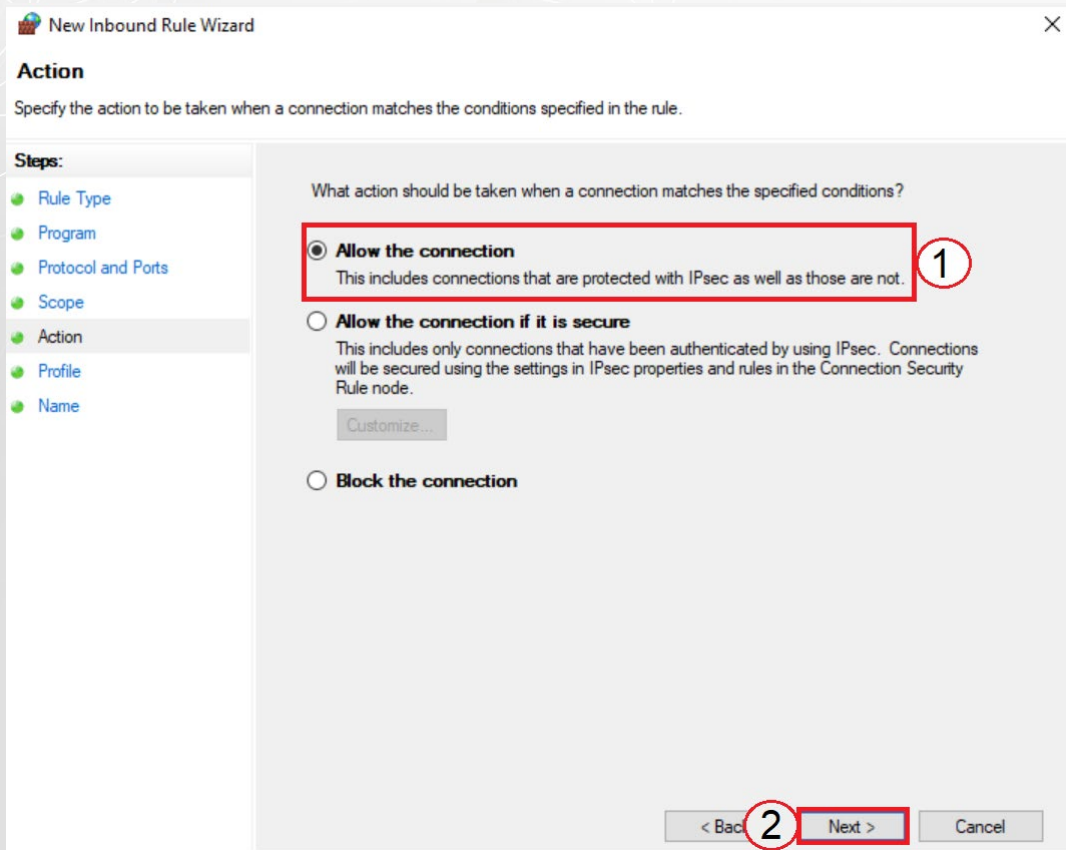
150.10.15.155

Add... Edit... Remove

1

2 < Back Next > Cancel

11. Select allow the connection and next



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

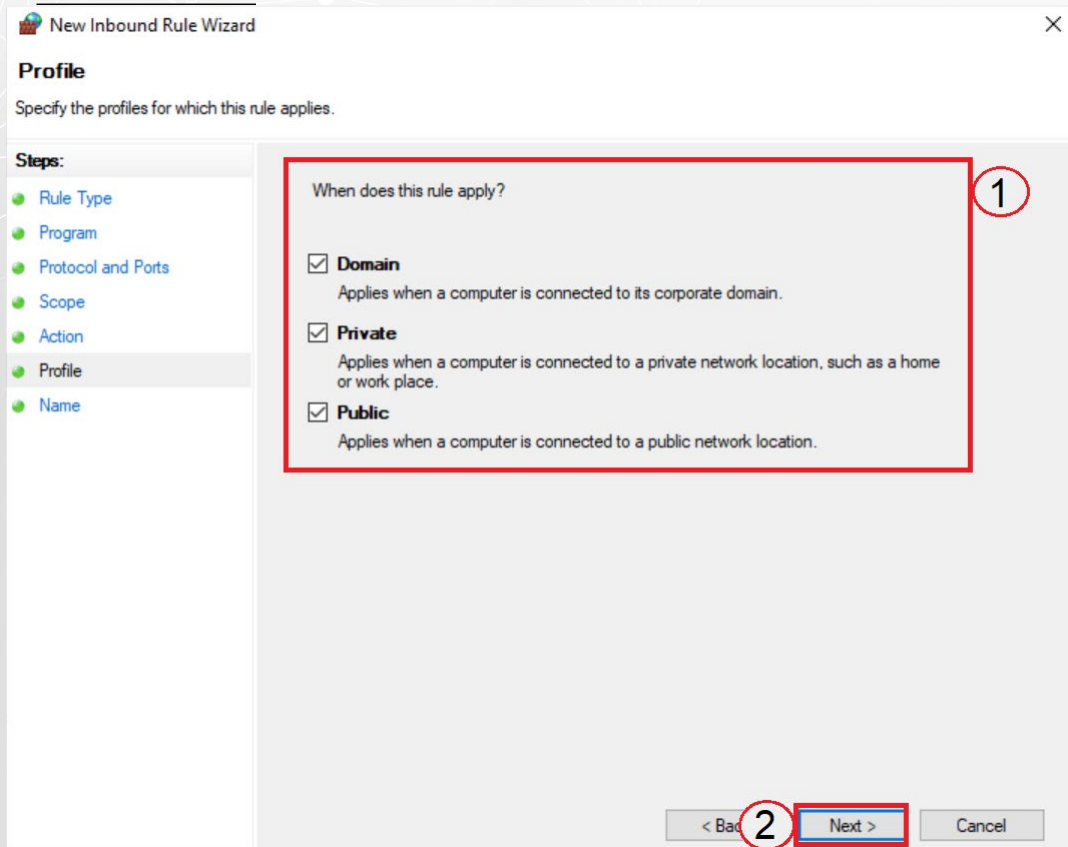
☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

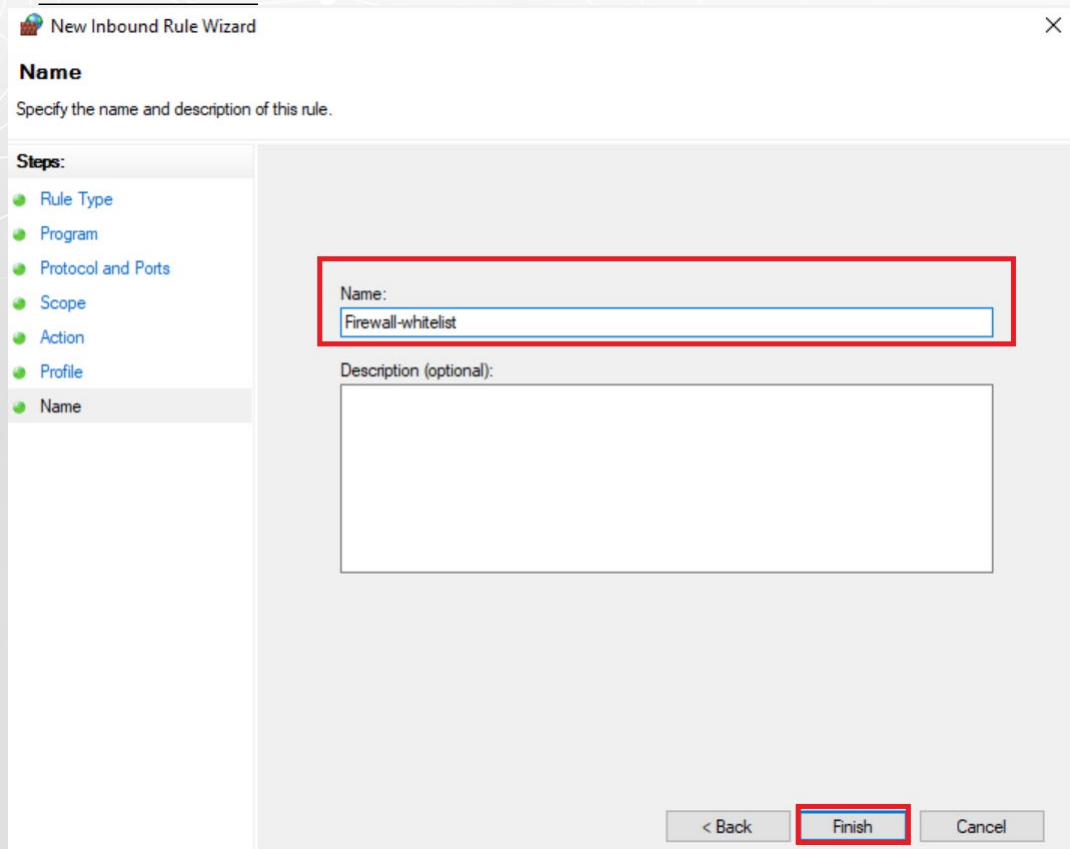
☐ **Block the connection**

< Back **2** Next > Cancel

12. In the window "When does this rule apply" we mark all and click next



13. In the following step we name it as Firewall-whitelist, Finish and close



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name**

Name:
Firewall-whitelist

Description (optional):

< Back Finish Cancel

14. It should look like this at the end