UBNetDef S25 Instructional Report Lab #4

Adi Czobel

Edwin Kairu

CSE 427

February 20th, 2025

Contents

1. General Content

1.1 Join Win10 Client and IIS Server VMs to your domain

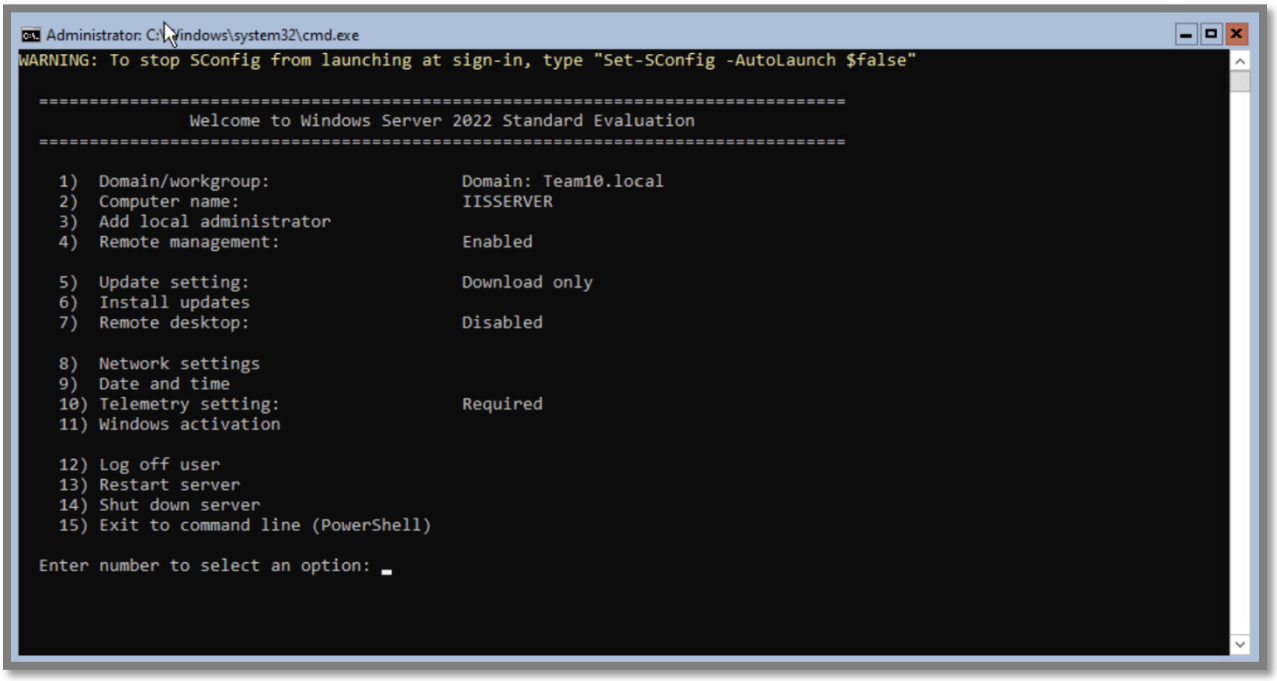


Figure 1: Change Domain on IISServer

After I updated the DNS server IP, it become possible to change the domain to **team10.local**, which has been set up earlier. With the DNS now being capable of resolving **team10.local**, the next step involves selecting option 1 (refer to Figure 2) and pressing Enter to access the domain

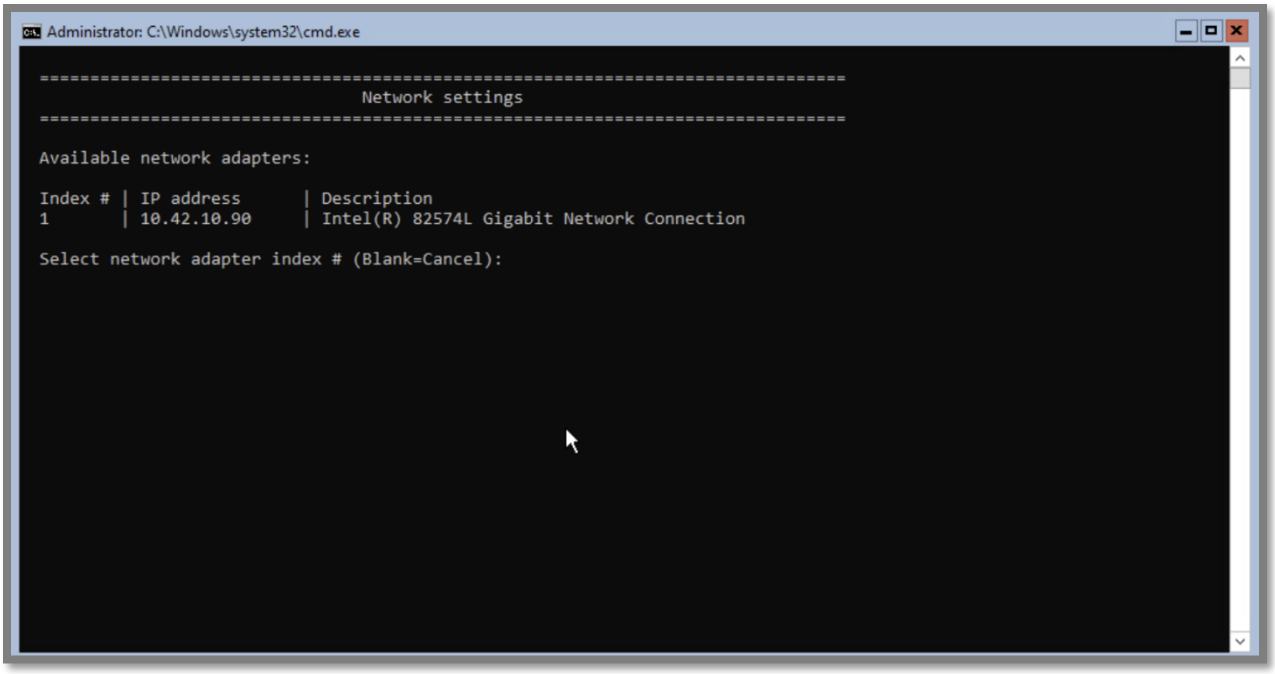


Figure 2: Joining the Domain **team10.local** with Authorized Credentials

In order to change the domain, refer to figure 2, select **d** for domain. The objective is to join the domain **team6.local**. Specify the authorized domain user as **Administrator** and follow that by entering your password **Change.me!** After you enter your password, the system successfully joins the domain **team10.local**.

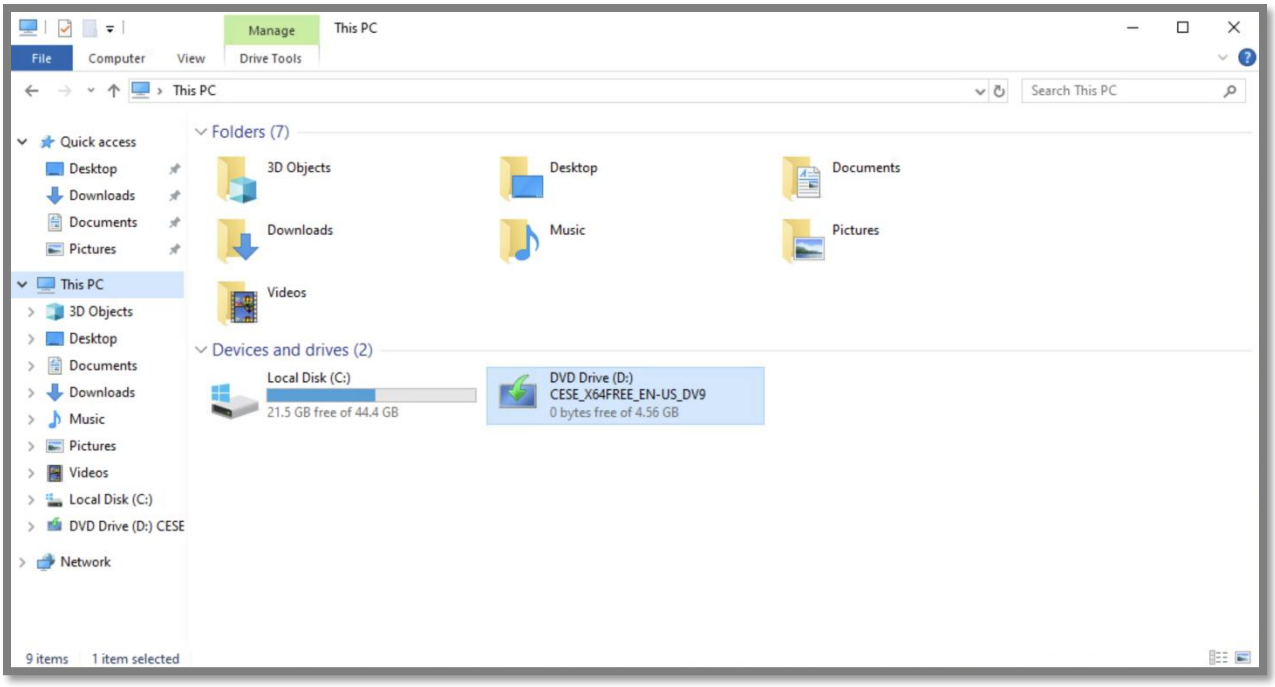


Figure 3: Selecting **This PC** and Accessing **Properties**

After I opened the File Explorer, I navigated to **This PC** refer to figure 3 in the left pane. Right-click on **This PC** and select **Properties** from the context menu to access system information and settings.

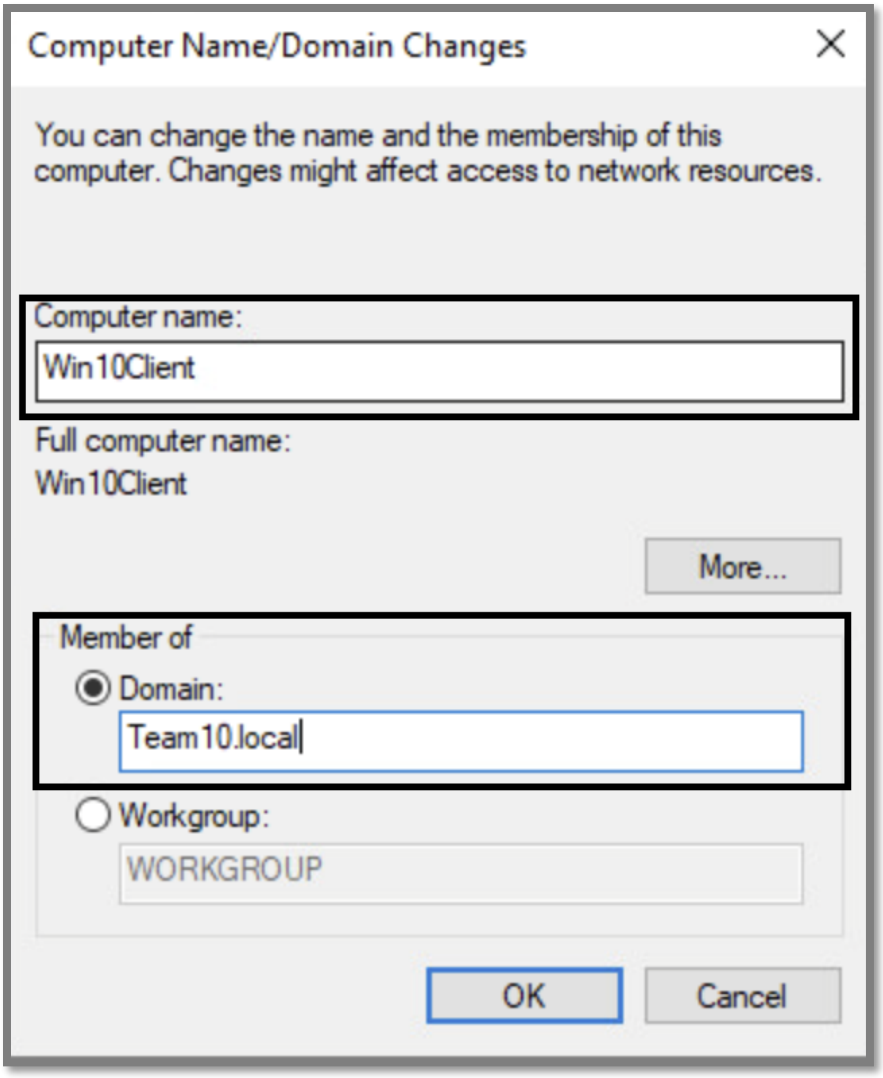


Figure 4: Configuring Computer Name and Domain Membership in System Properties

In the **Computer Name/Domain Changes** window, change the **Computer Name** to **Win10Client** and change the Workgroup setting to **Member of Domain: team10.local**. refer to figure 4 After making these adjustments, click **OK** to confirm the changes, and then select **Apply** to cement the changes.

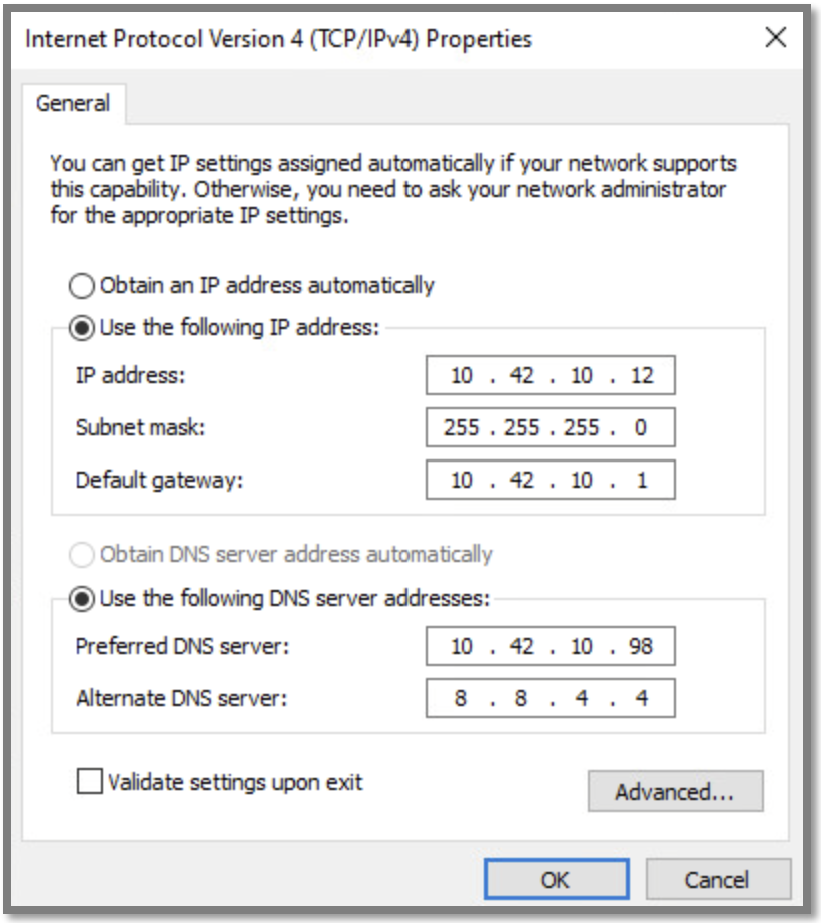


Figure 5: Configuring Preferred DNS on Win10 Client

Once you change your computers name and domain, search for **ncpa.cpl,** in the search bar. Once it opens make sure to click on ethernet and then properties (refer to figure 5). Once in properties make sure to change your preferred DNS server to the IP of your AD server which is **10.42.10.98.**

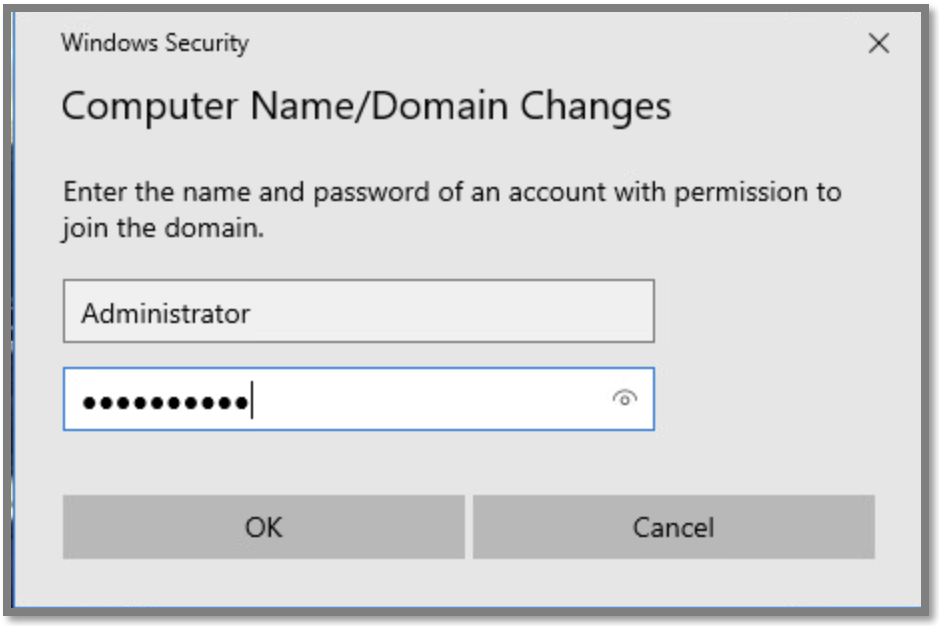


Figure 6: sign in to confirm DNS change

Once you input the correct DNS IP address and put In your team name and domain name, if you were successful you will get this pop up window (referred to in Figure 6). Then you sign in using your administrator's name and password to connect your win10 client to your AD server, and restart your VM.

2. Create two users on your domain

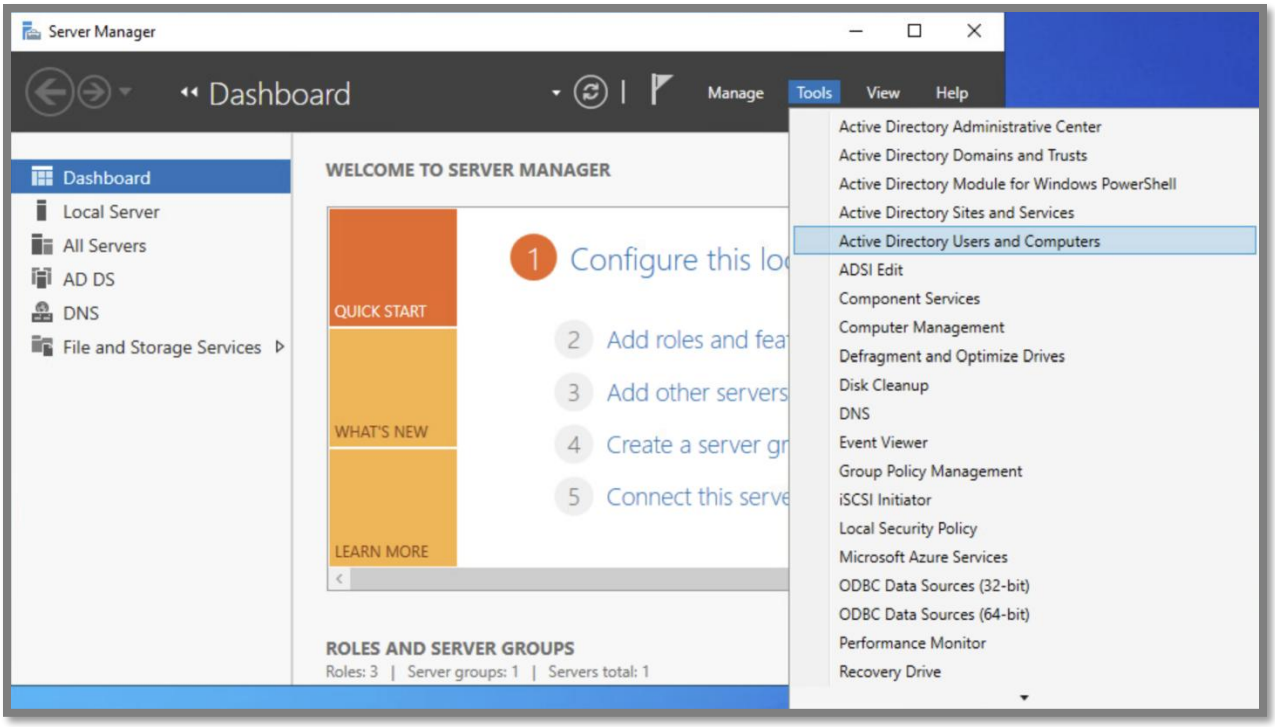


Figure 7: Accessing and Expanding Active Directory Users and Computers in Server Manager

Go to **Server Manager**, click on **Tools** and click on **Active Directory Users and Computers** (refer to figure 7). Once you click on it, expand the domain tree to view the organizational units and users within the domain.

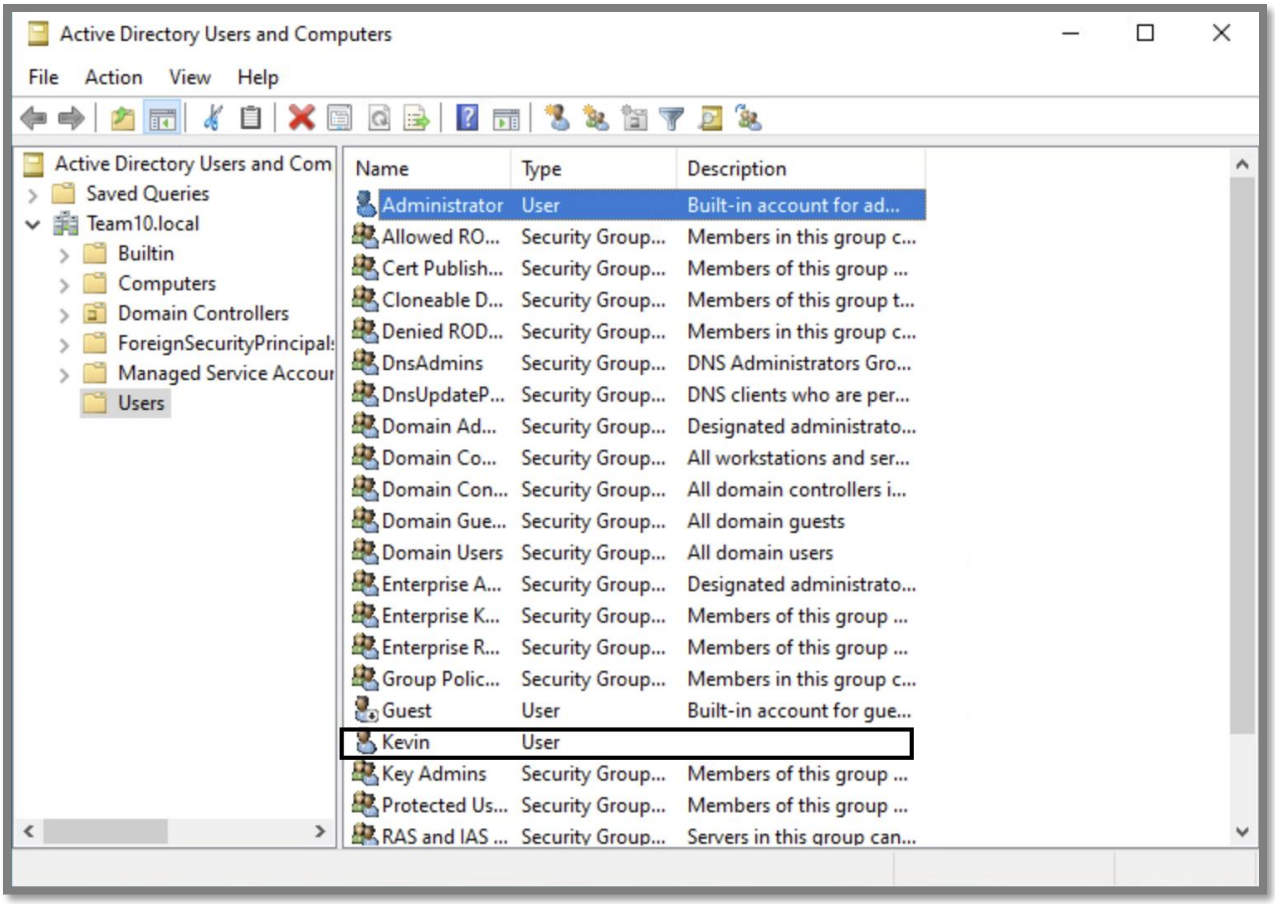


Figure 8: Adding a User in Active Directory Users and Computers

After you select **Active directory users and computers** (refer to figure 8). Go to the users section and click on the add user icon, to create a new user into your domain.

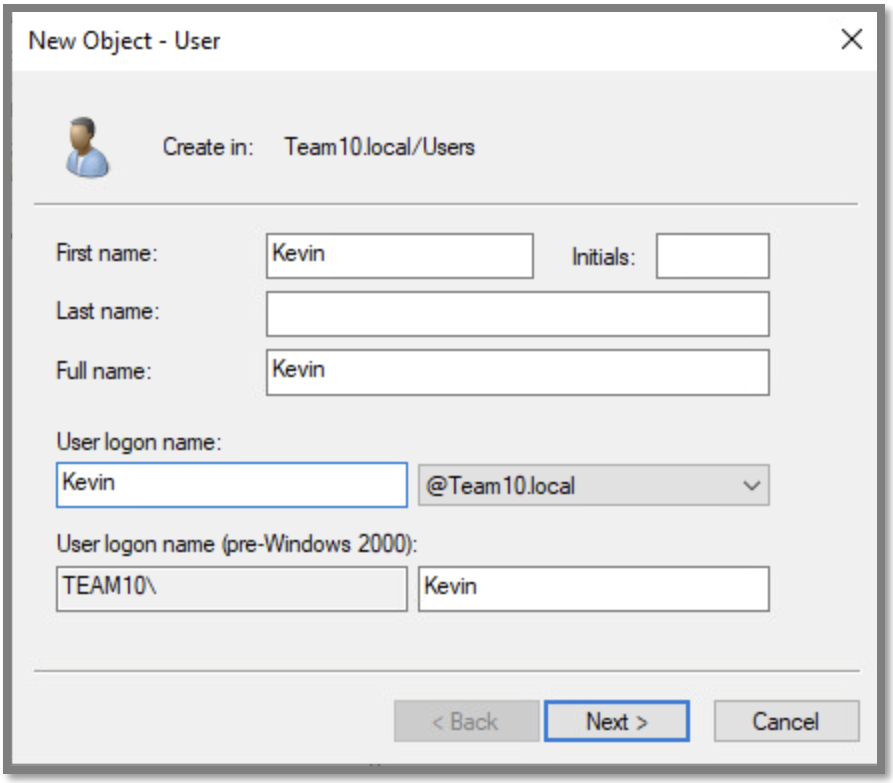


Figure 9: Creating a New User in Active Directory

Go to the **New Object - User** window (refer to Figure 9), enter the first name as Kevin and set the user logon name to Kevin also. Once you fill in information, click **Next** to proceed.

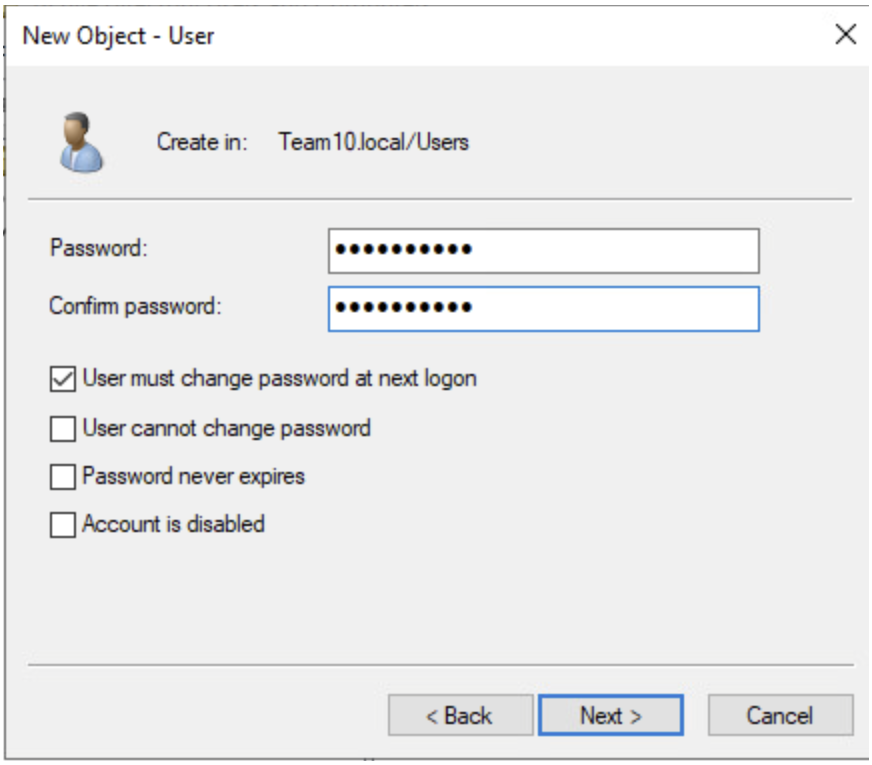


Figure 10: Setting Password and Finalizing User Creation in Active Directory I

When you get to the **Password** screen (refer to Figure 13), enter **Change.me!** as the password and confirm it. Uncheck the option **User must change password at next login**, then click **Next**, then **Apply** and **Close** to finalize the creation of the user.

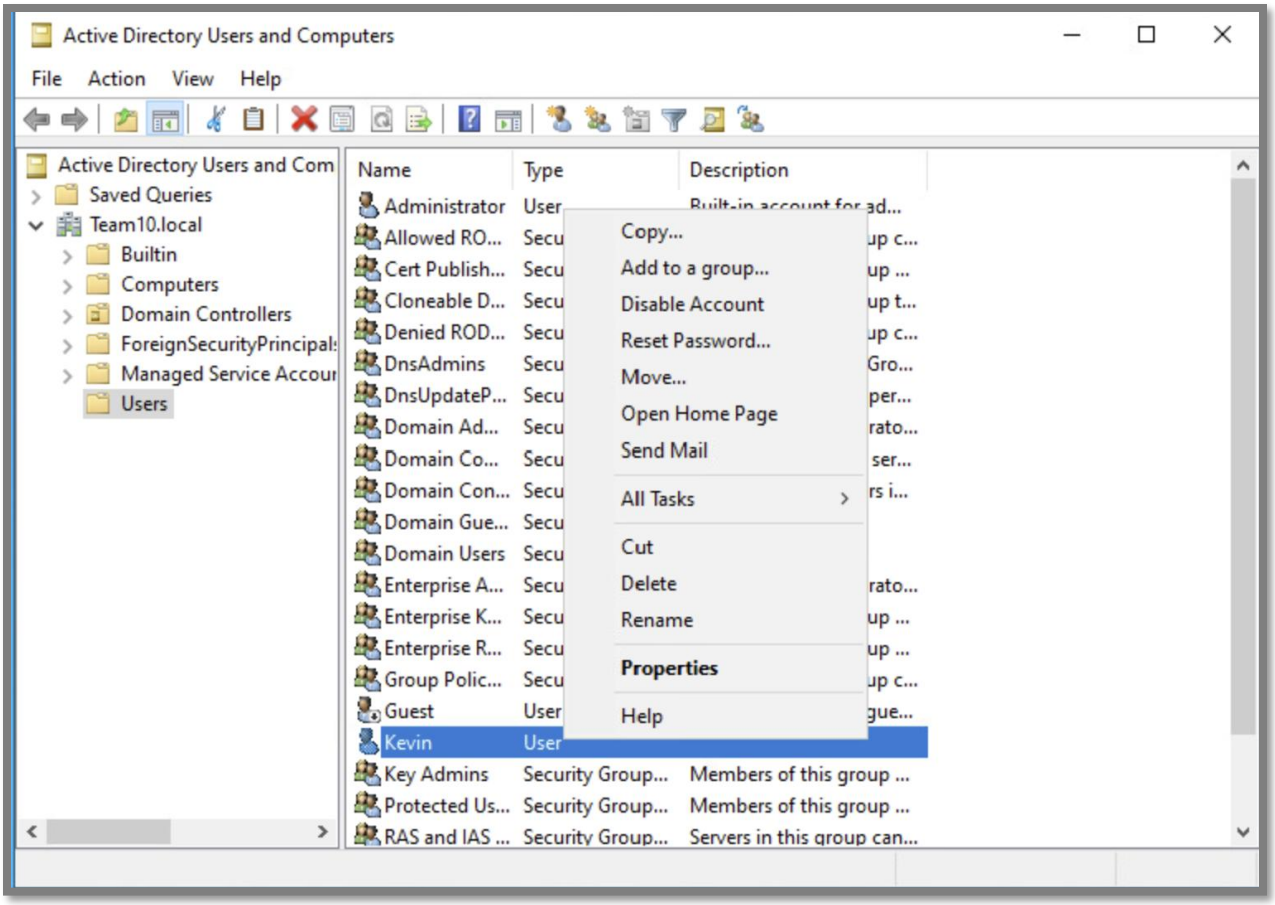


Figure 11: Adding User to Administrators Group

After going back to the **Users** screen (refer to Figure 11), right-click on the user **Kevin** and select **Properties** to begin the process of adding Kevin to the Administrators group

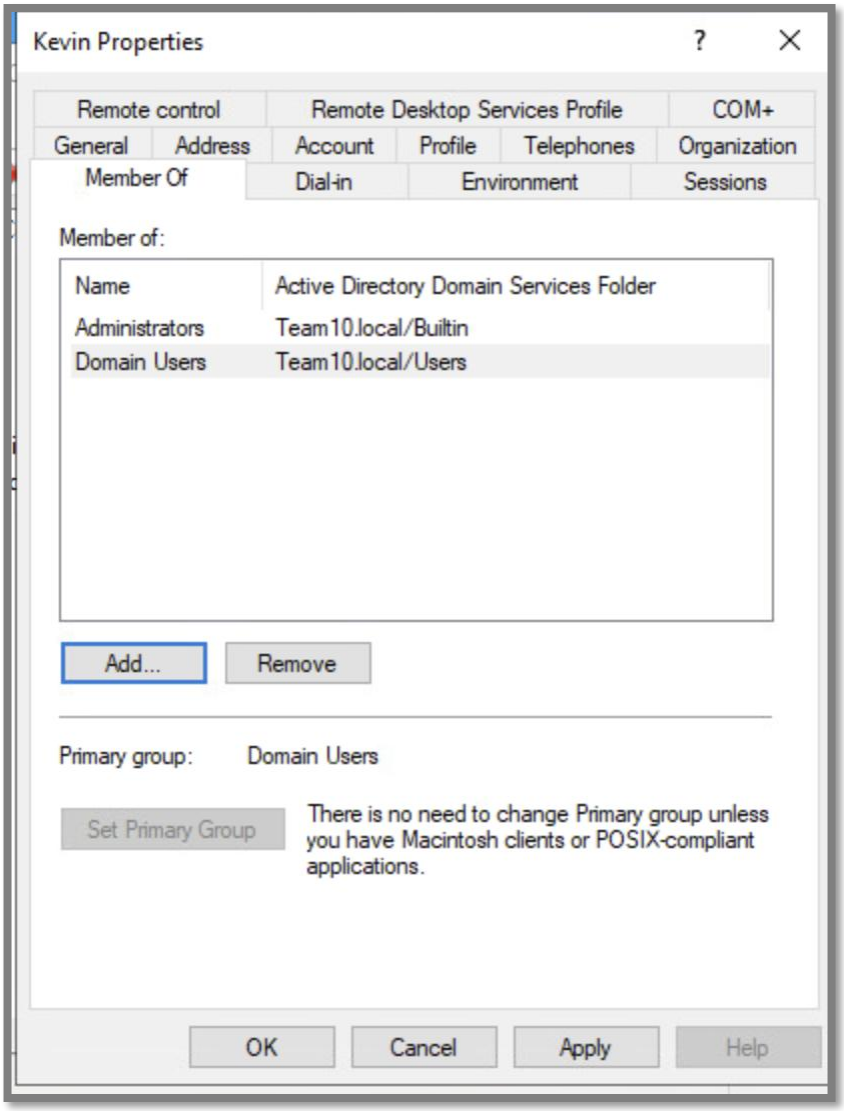


Figure 12: Adding Kevin to the Administrators' Group

While in Kevin's **Properties** window, click the **Add** button to include the user in the Administrators group.

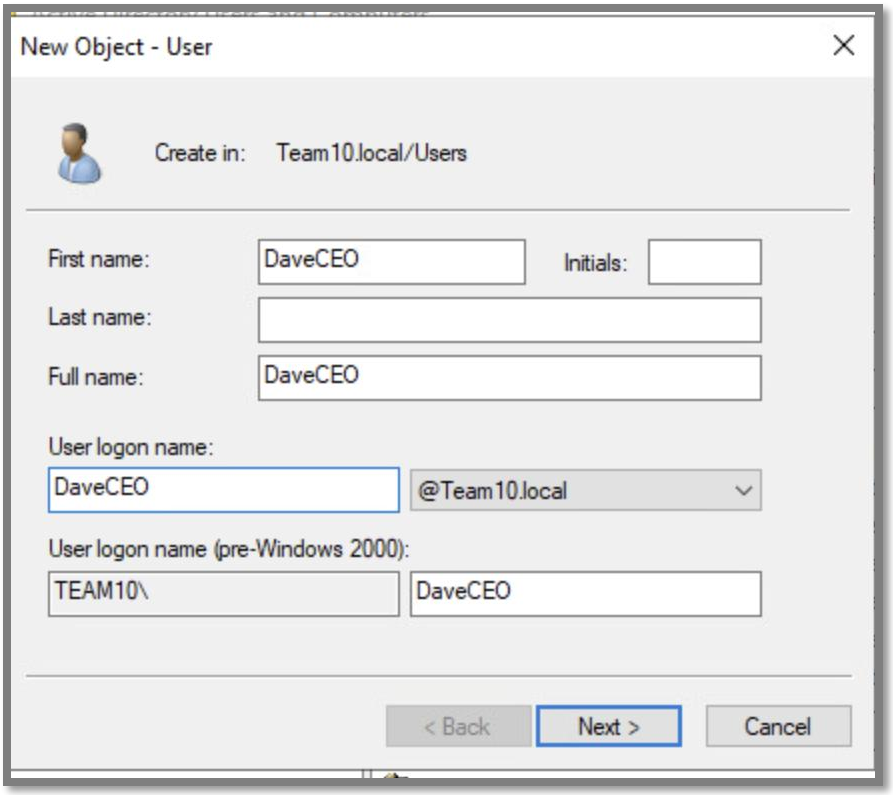


Figure 13: Creating a New User in Active Directory

In the **New Object - User** window (refer to Figure 13), enter the first name as DaveCEO and set the user logon name to DaveCEO as well. Once the information is filled in, click **Next** to proceed.

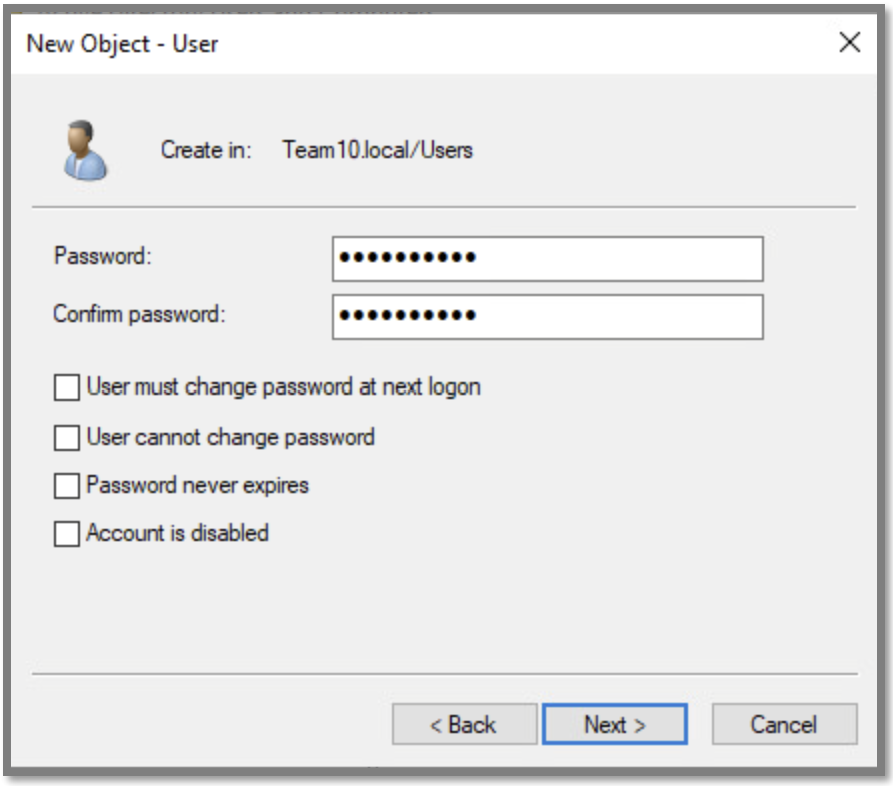


Figure 14: Setting Password and Finalizing User Creation in Active Directory II

When you reach the **Password** screen (refer to Figure 14), enter **Change.me!** as the password and confirm it. Uncheck the option **User must change password at next login**, then click **Next**, followed by **Apply** and **Close** to finalize the creation of the user.

3. Add IISserver to the ADServer Server Pool

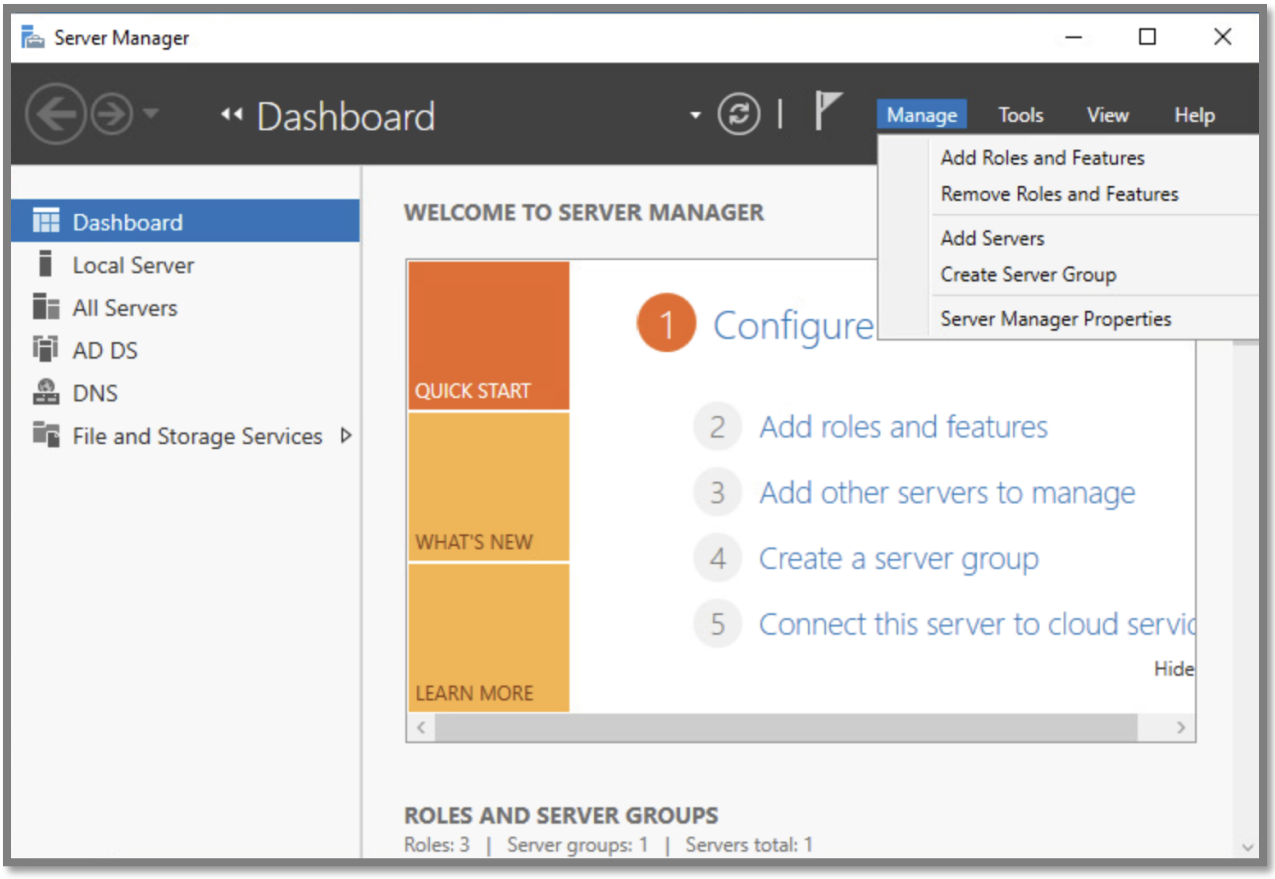


Figure 15: Adding Servers in Server Manager

You Navigate to **ADServer** in **Server Manager** (refer to Figure 15) and click on the **Add Servers** option to initiate the process of adding new servers.

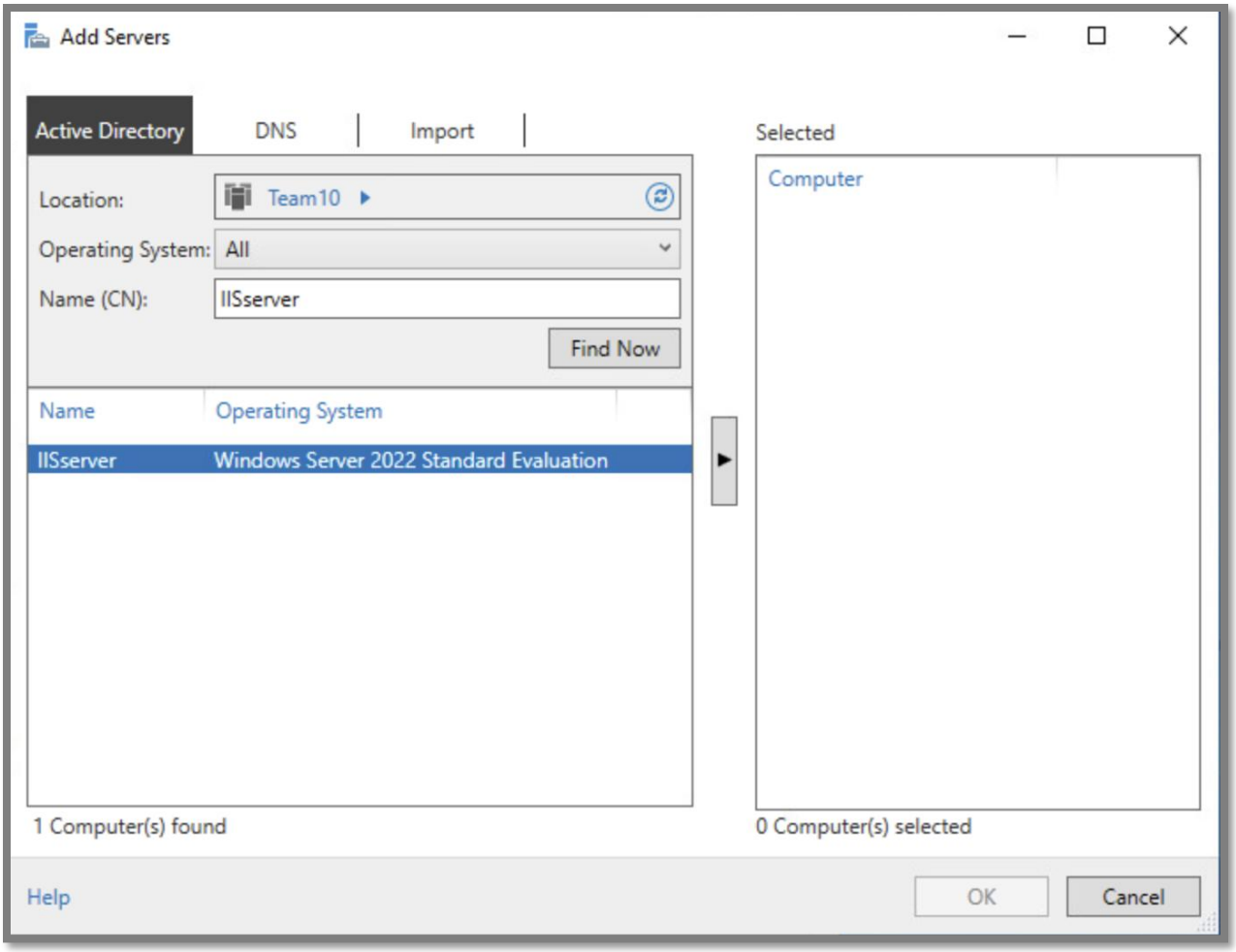
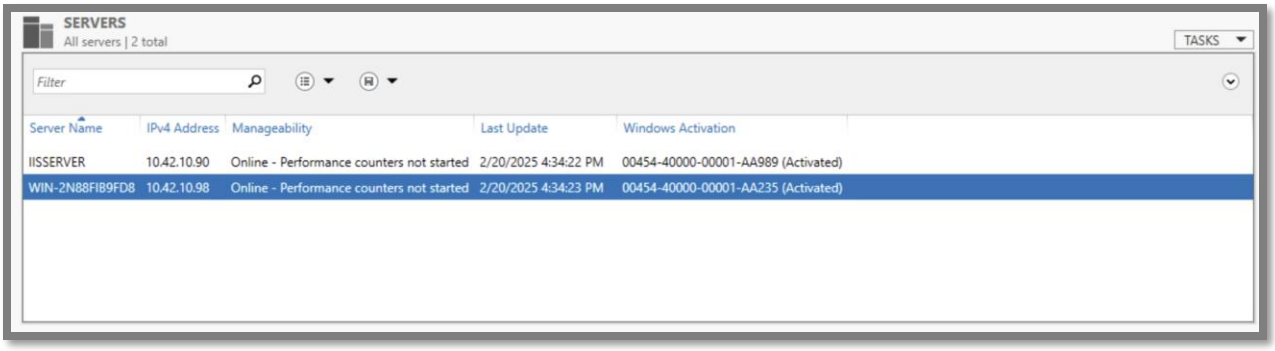


Figure 16: Adding a Server to Active Directory

In the **Add Server** window, under the **Active Directory** section, write **IISServer** and click **Find Now**. Once the server appears in the results, double-click on it and then click **OK** to add it.

Figure 17: Successfully Added IISServer to ADServer Server Pool



You can see the server **IISServer** has been successfully added to the ADServer server pool, indicated by its status showing as **Online**. This shows that the server is now manageable within the environment.

4. Install "Internet Information Services" Web Server on IISserver

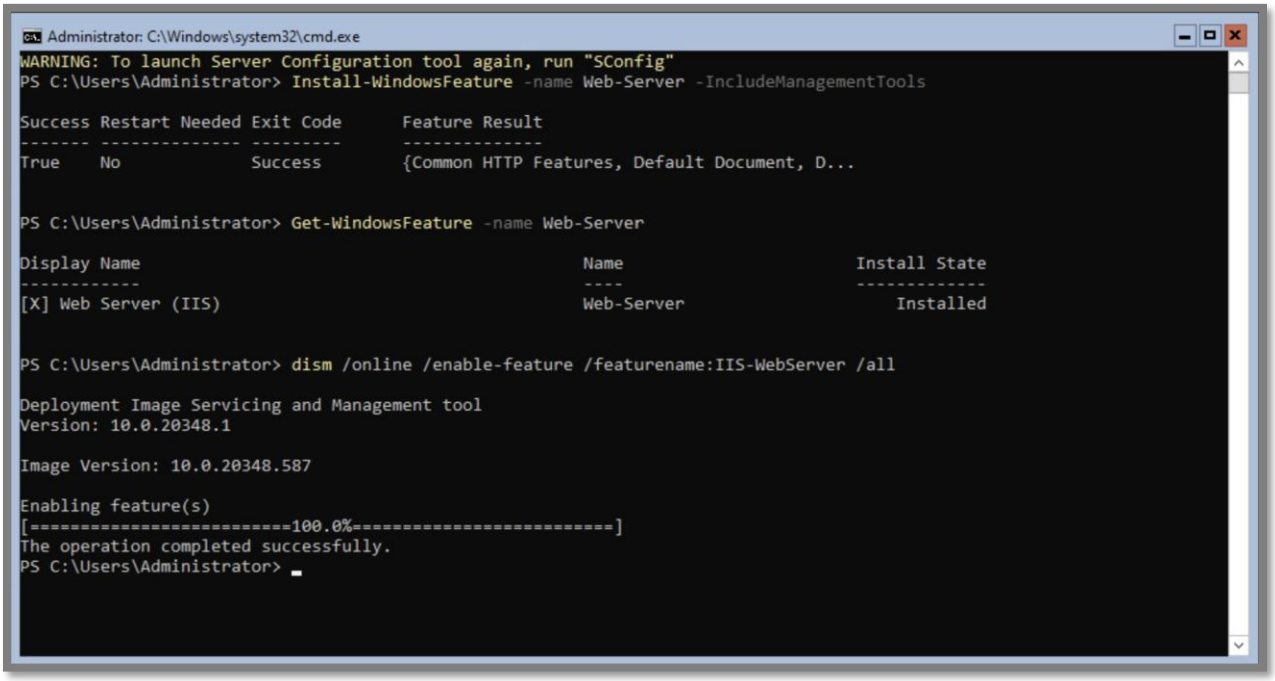


Figure 18: Set up IIS on IISServer

In order to install Internet Information Services (IIS) on an IISServer using the command line (refer to Figure 18), first, open PowerShell by typing in **15**. Then, input the command **Install- WindowsFeature -name Web-Server -IncludeManagementTools** to install with its management tools. Then inputthe command **dism /online /enable-feature/featurename:IIS-WebServer /all** to enable

the IIS feature. Once the installation is complete, you can verify it by running **Get-WindowsFeature -Name Web-Server** in PowerShell.

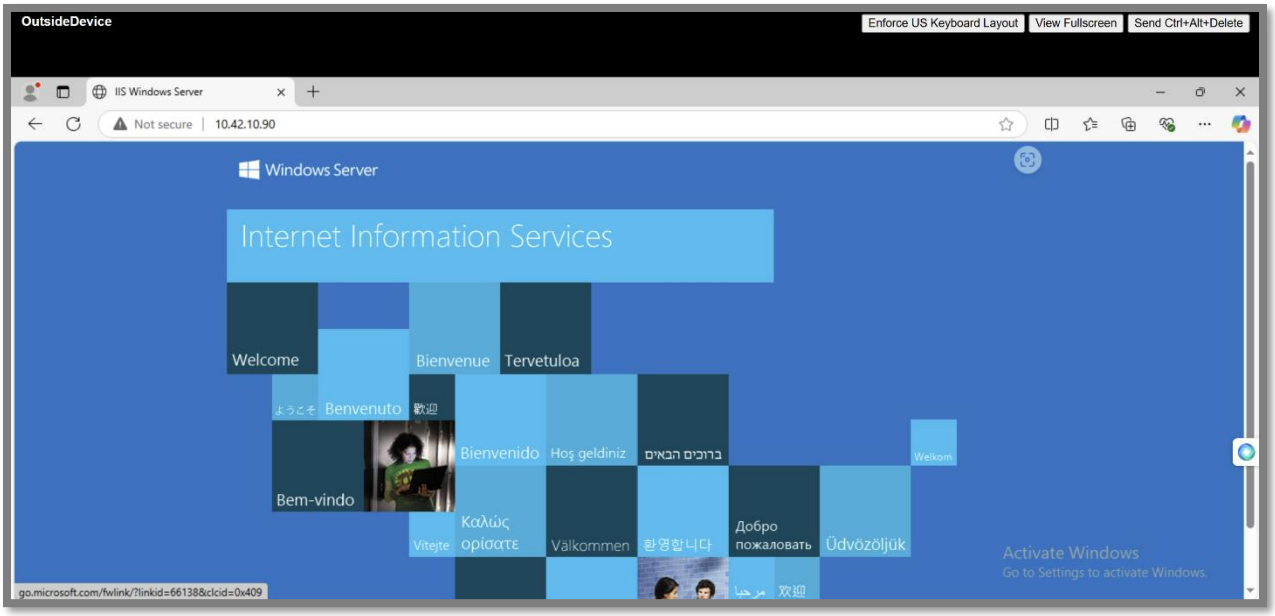


Figure 19: IISServer IP Loaded on OutsideDevice

Figure 19 shows the OutsideDevice successfully accessing a webpage hosted by the IIS server. This webpage, which is served from the IIS server, demonstrates that the connection has been established correctly and that the content is loading as intended. The successful interaction indicates that the IIS server is configured properly and can serve web requests from external devices, showcasing its functionality as a web hosting solution.

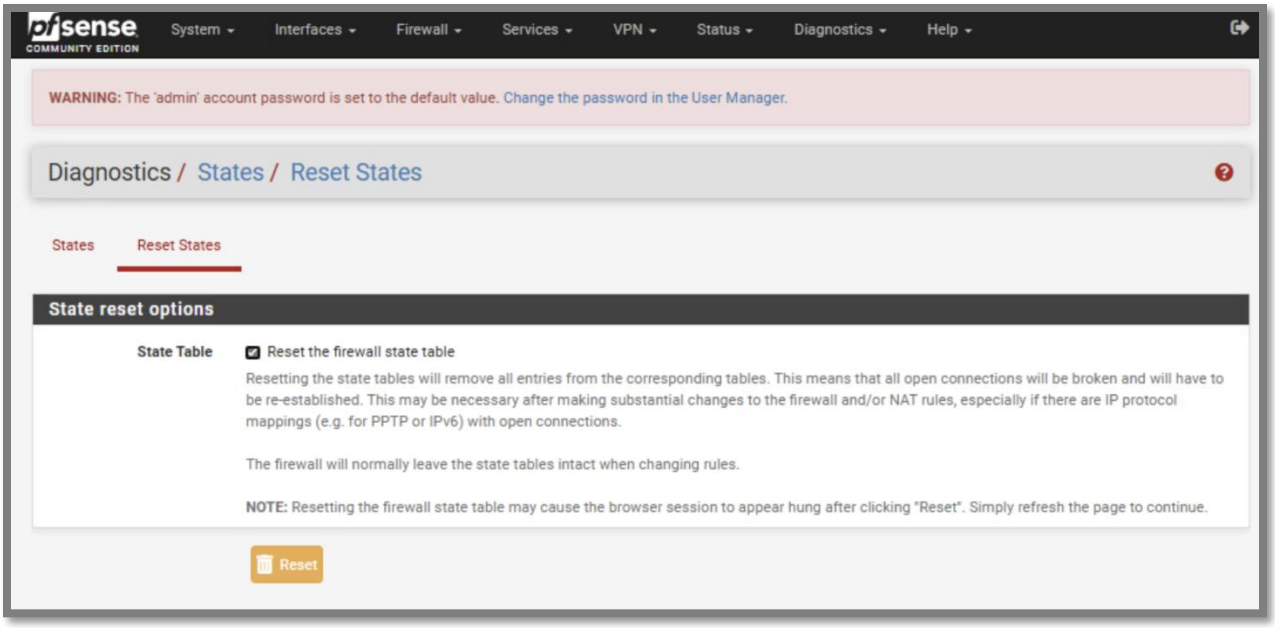
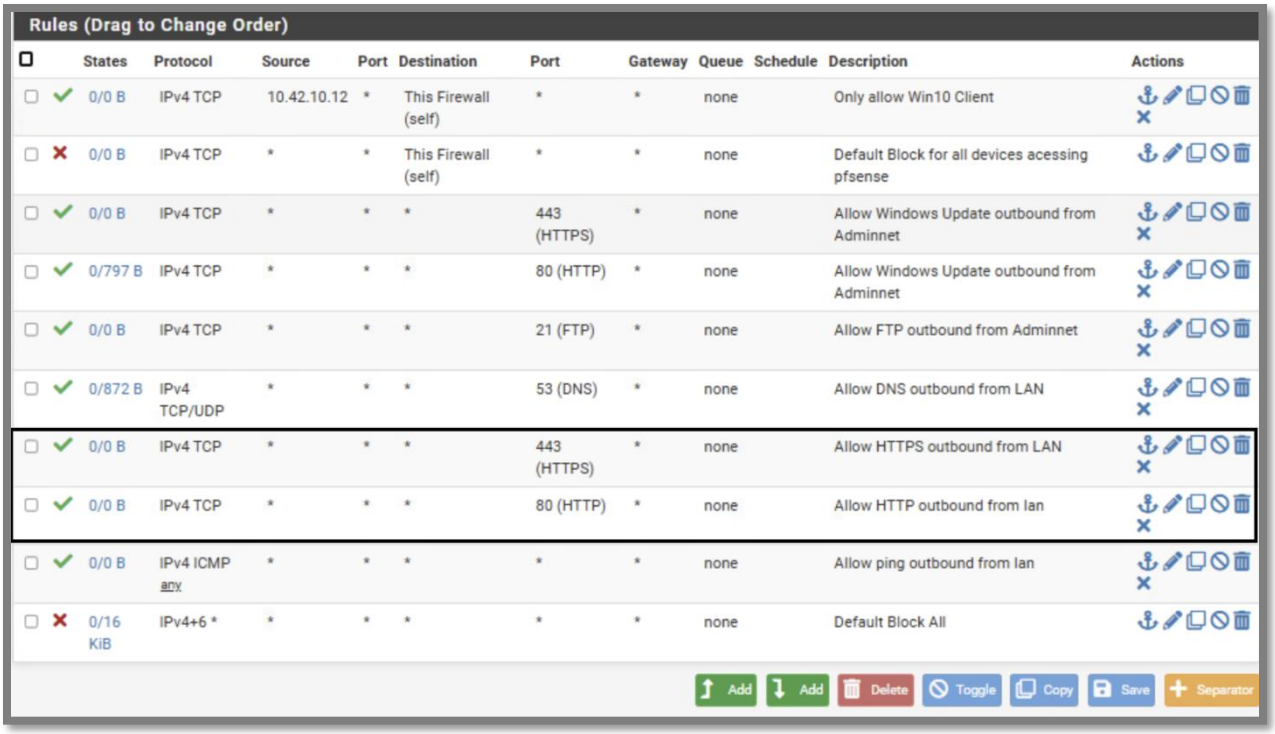


Figure 20: Resetting the State on the Firewall

In order to reset the firewall state table in pfSense, go to **Diagnostics**, click on **States**, and choose **Reset States**. This action clears all active connections in the state table, which tracks the status of ongoing connections through the firewall. Resetting the state table is often performed during troubleshooting or after significant changes to firewall rules, ensuring that new connections adhere to updated configurations. Simply click the **Reset** button to complete the process and clear the state table.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐ ✓	0/0 B	IPv4 TCP	10.42.10.12	*	This Firewall (self)	*	*	none		Only allow Win10 Client	
☐ ✗	0/0 B	IPv4 TCP	*	*	This Firewall (self)	*	*	none		Default Block for all devices acessing pfsense	
☐ ✓	0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Allow Windows Update outbound from Adminnet	
☐ ✓	0/797 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Allow Windows Update outbound from Adminnet	
☐ ✓	0/0 B	IPv4 TCP	*	*	*	21 (FTP)	*	none		Allow FTP outbound from Adminnet	
☐ ✓	0/872 B	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		Allow DNS outbound from LAN	
☐ ✓	0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Allow HTTPS outbound from LAN	
☐ ✓	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Allow HTTP outbound from lan	
☐ ✓	0/0 B	IPv4 ICMP any	*	*	*	*	*	none		Allow ping outbound from lan	
☐ ✗	0/16 KiB	IPv4+6 *	*	*	*	*	*	none		Default Block All	

Add | Add | Delete | Toggle | Copy | Save | Separator

Figure 21: Firewall Rules Used for This Task

The firewall rules configured in the webConfigurator GUI include those that facilitate HTTP and HTTPS traffic. These rules are essential for allowing web traffic through the firewall and ensure proper connectivity for the task. Specifically, rules permitting traffic on port 80 (HTTP) and port 443 (HTTPS) are highlighted, they enable access to web services required for the task at hand.

5. Create Groups

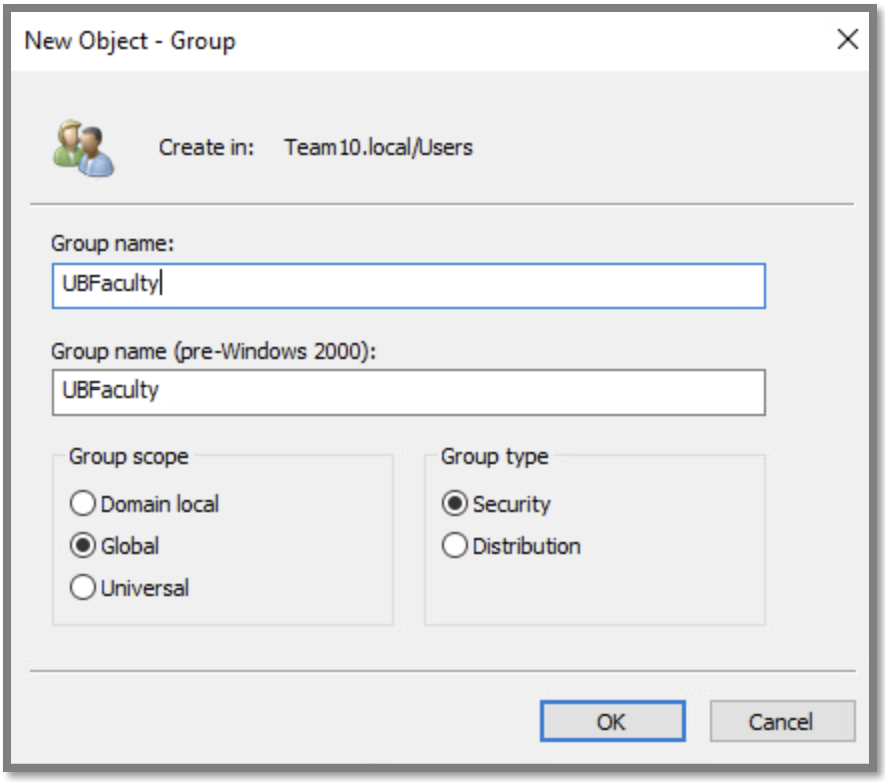


Figure 22: Creating the UBFaculty Group

In order to create the group **UBFaculty** (refer to Figure 26), begin by going to the appropriate management console for group creation. Select the option to create a new group, and input **UBFaculty** as the group name. Ensure that the group scope is set to **Global,** and the group type is designated as Security. Once these parameters are confirmed, click **OK** to finalize the creation of the group.

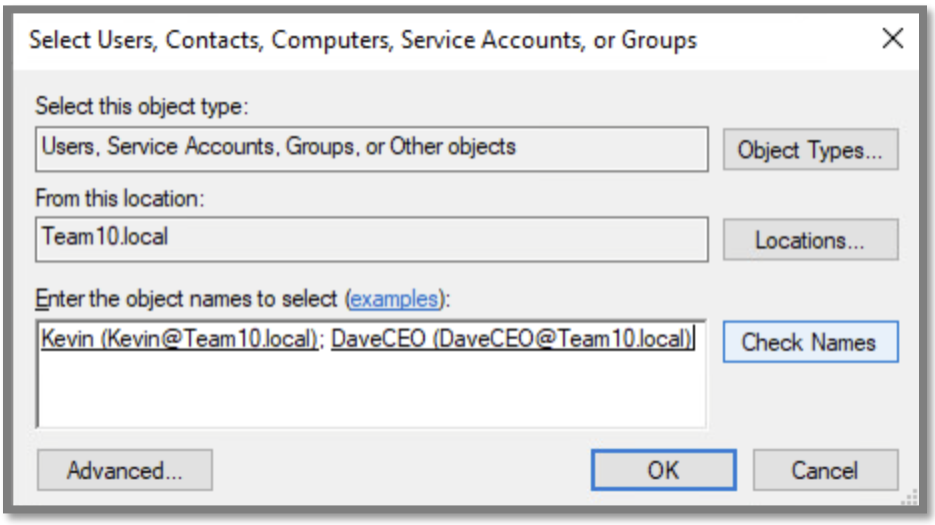


Figure 23: Adding Domain Users to the UBFaculty Group

In order to add users to the **UBFaculty** group (refer to Figure 23), right-click on the group and select **Properties**. In the properties window, locate the section for adding members. Search for domain users by finding **Kevin** and **DaveCEO** within the **team10.local** domain. Use the **Check Names** feature to ensure the correct object names are identified. After confirming the names, click **OK** to add these users to the UBFaculty group.

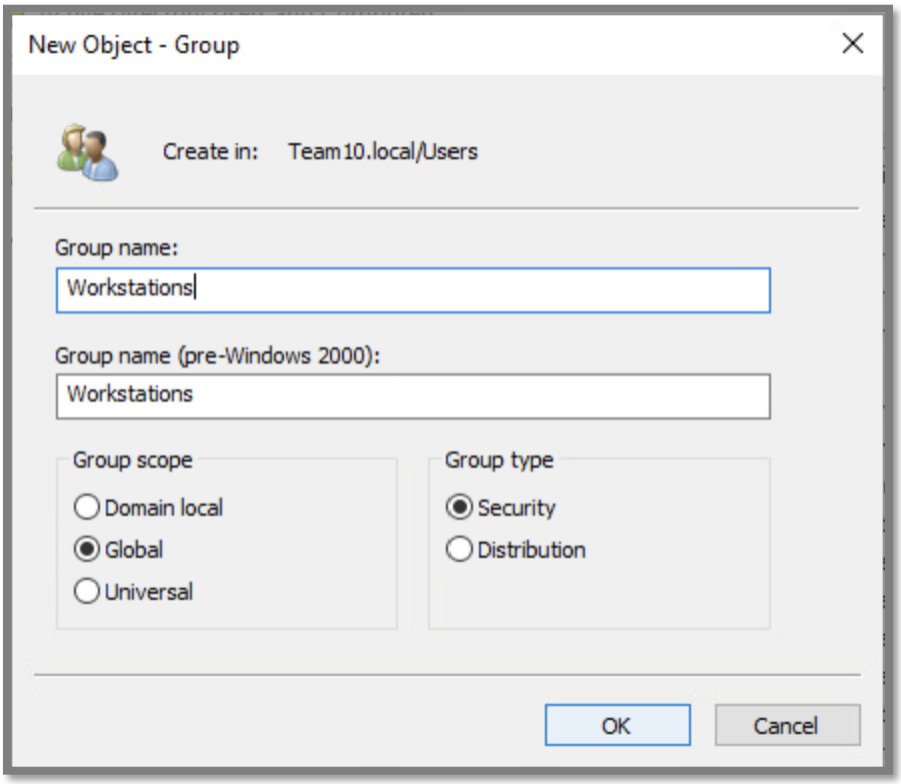


Figure 24: Creating the Workstations Group

In order to create the group **Workstations** (refer to Figure 24), begin by navigating to the appropriate management console for group creation. Click on the option to create a new group, and input **Workstations** as the group name. Ensure that the group scope is set to **Global,** and the group type is designated as Security. Once these parameters are confirmed, click **OK** to complete the creation of the group.

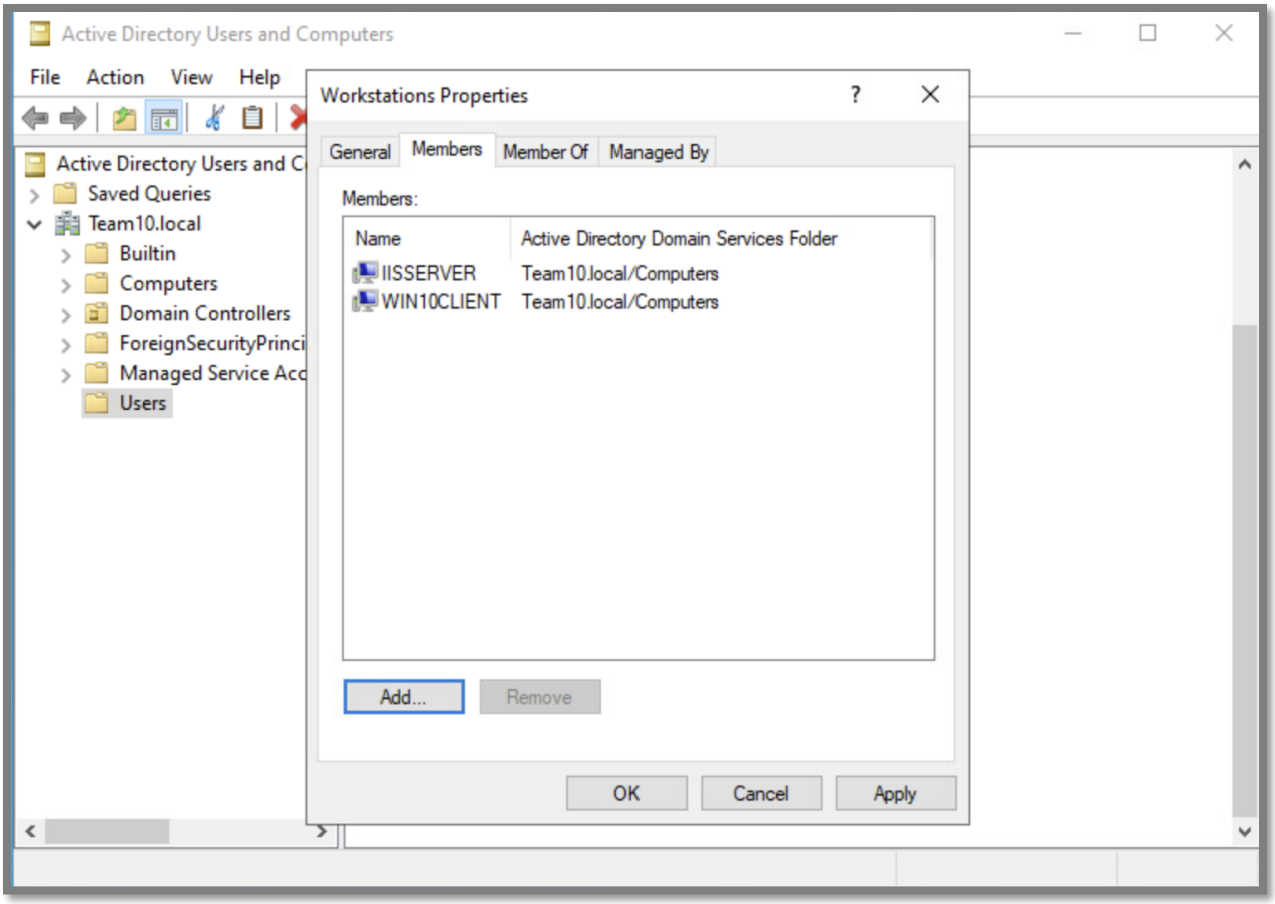


Figure 25: Adding Domain Devices to the Workstations Group

In order to add users to the **Workstations** group (refer to Figure 25), right-click on the group and select **Properties**. In the properties window, locate the section for adding members. Search for domain devices (in this case it was under computers) by finding **Win10Client** and **IISServer** within the **team10.local** domain. Use the **Check Names** feature to ensure the correct object names are identified. After confirming the names, click **OK** to add these users to the Workstations group.

6. Enforce Background Group Policy

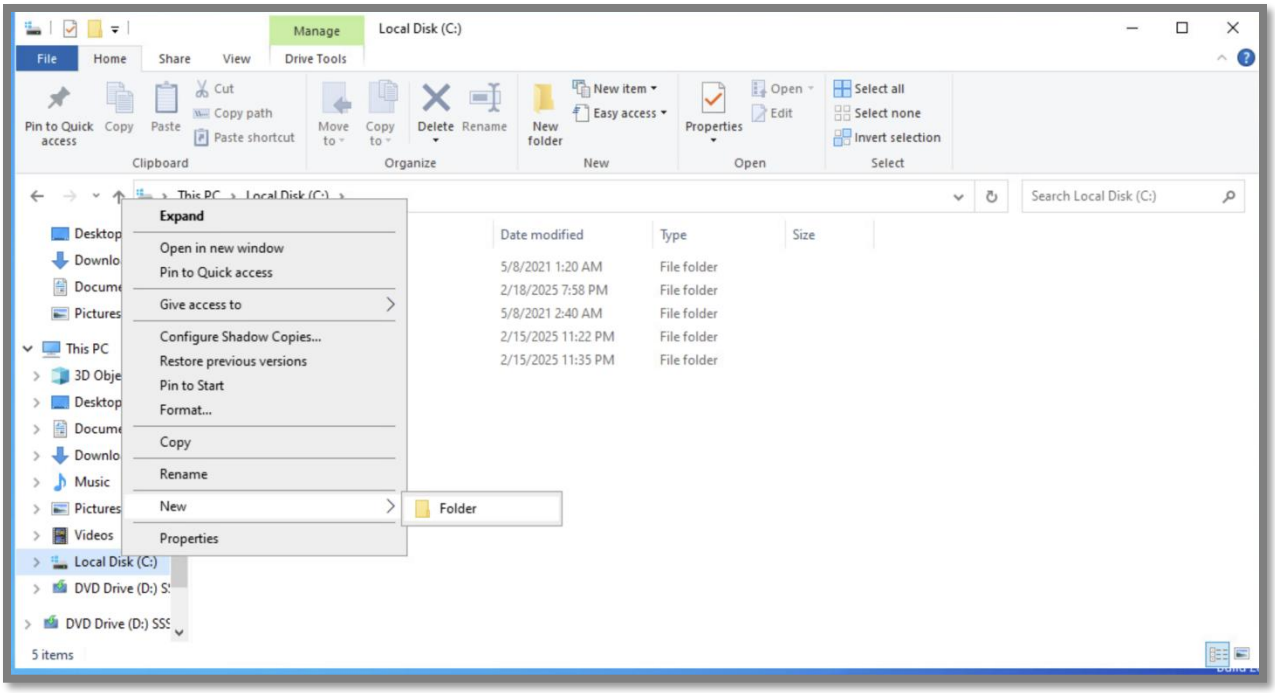


Figure 26: Creating a Shared Folder

In Figure 26 it outlines the process of creating a shared folder on a local machine. Start by navigating to **This PC** and selecting **Local Disk (C:)**. Once in the local disk, right-click in the file explorer window, choose **New**, and then select **Folder** from the dropdown menu.

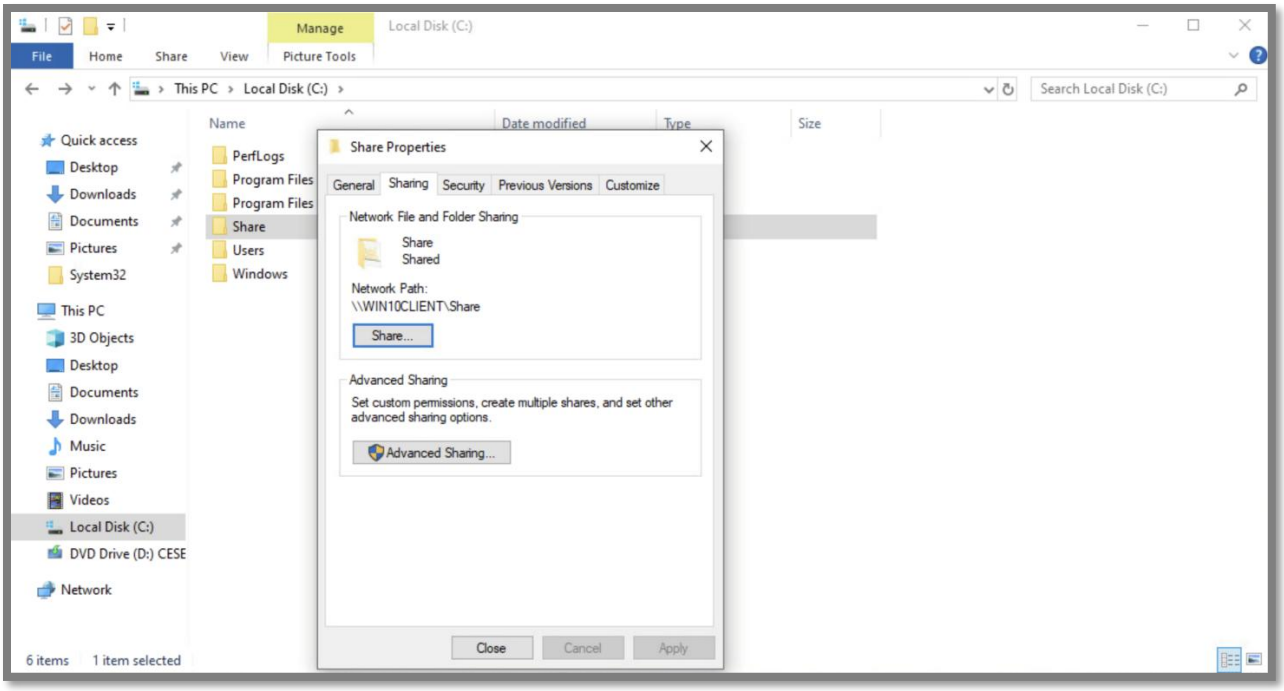


Figure 27: Configuring Advanced Sharing for a Folder

In Figure 27 I demonstrate how to configure advanced sharing settings for a folder. Begin by right-clicking on the folder named **Share** and selecting **Properties** from the context menu.

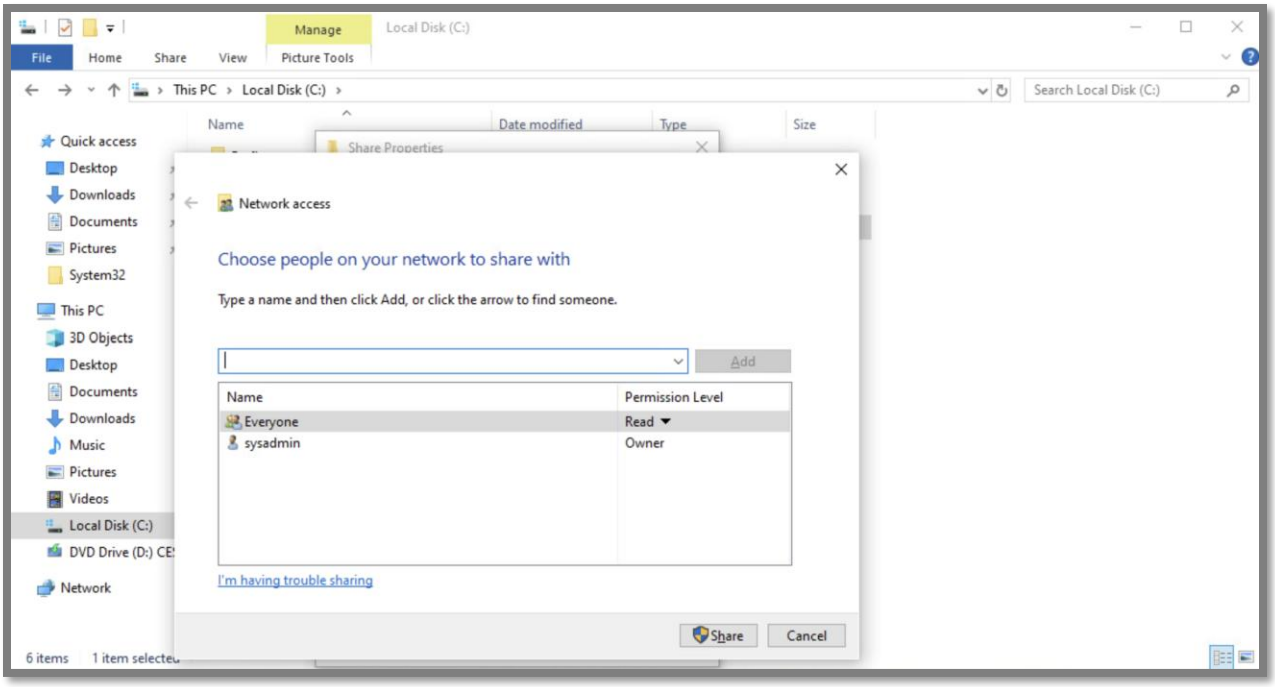


Figure 28: Sharing a Folder with Everyone with Read and Write Permissions

In Figure 28, the folder's sharing properties are configured to grant access to all users. After right clicking on the folder and selecting **Properties**, click on the **Sharing** tab and click **Sharing**. In the **Network access** section, select **Everyone** from the user list and check both **Read** and **Write** permissions.

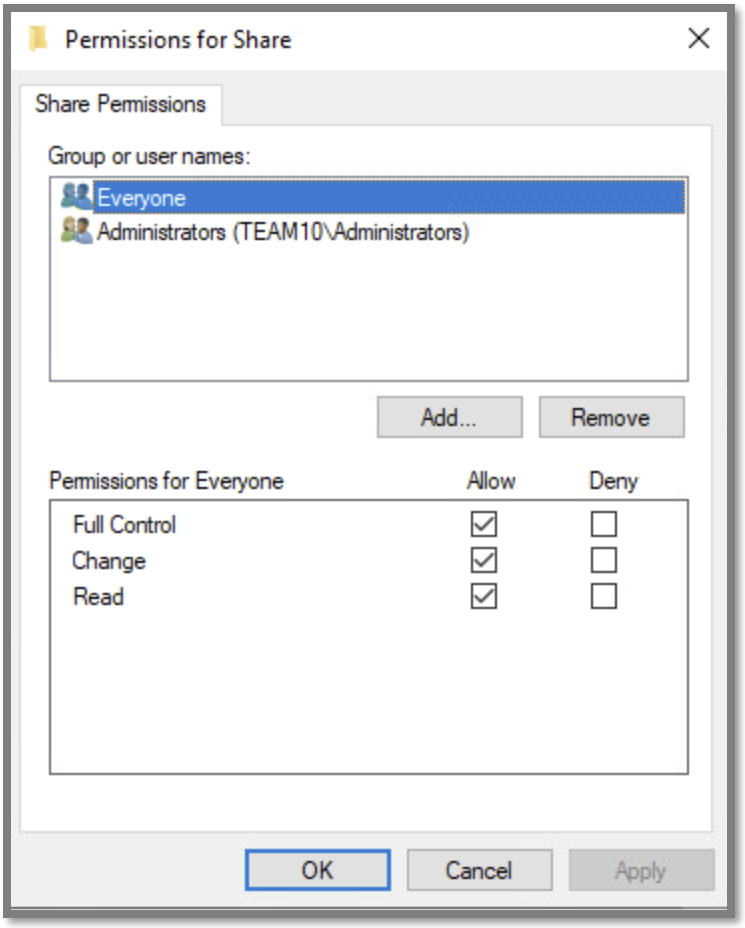


Figure 29: Advanced Sharing Permission

In the properties window, I navigated to the **Sharing** tab and click on **Advanced Sharing**. From there, I enabled **Share this folder**, and adjusted the permissions, allowing specific users or groups to access and modify the folder's contents. This step ensures the folder is properly shared across the network with the desired level of access control.

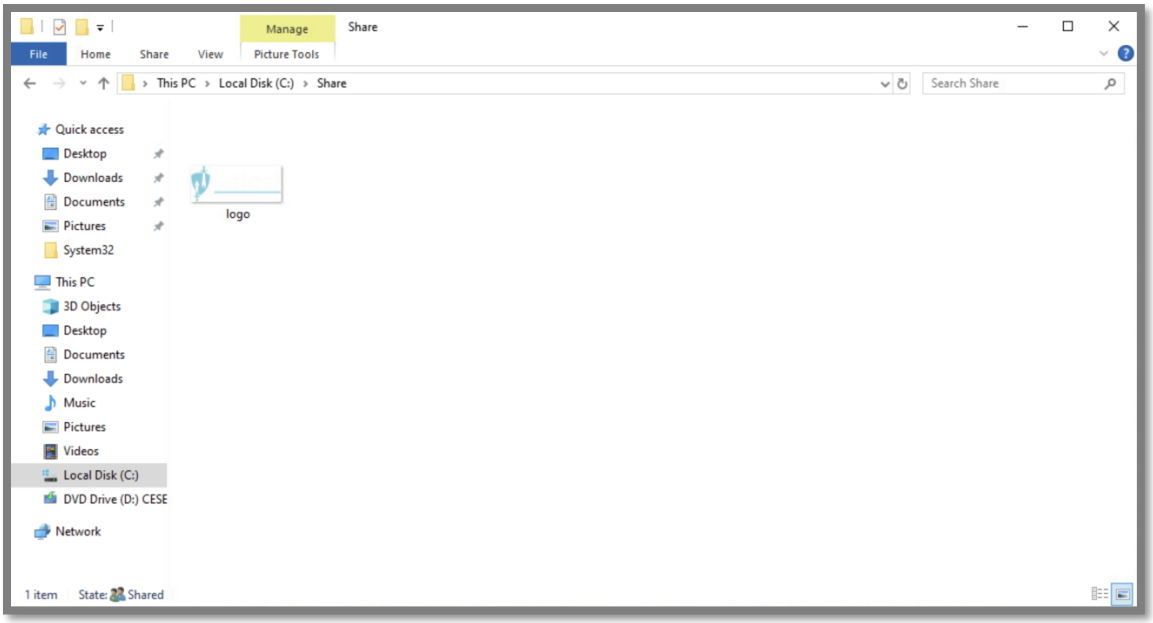


Figure 30: Uploading a Photo to the Shared Folder via WIN10CLIENT

In Figure 34, the process of navigating through **File Explorer** is shown, beginning with accessing the **Network** section. From there, the user navigates to **WIN10CLIENT**, then to the **share** folder. A photo, previously downloaded by typing the image's URL directly into the web browser (without logging into UBLearns), is then dragged and dropped into the shared folder. This method ensures the file is transferred correctly to the shared network location, bypassing any platform-specific restrictions.

Figure 31: Accessing Group Policy Management

Figure 31 shows the steps to navigate to **Group Policy Management**. Start by opening the **Tools** menu, typically found in the **Server Manager** or through the **Administrative Tools** section in Windows. From the list of available tools, select **Group Policy Management**.This utility allows administrators to configure and manage Group Policy Objects (GPOs), which control various settings and policies across the network or domain, ensuring centralized management of user and computer configurations.

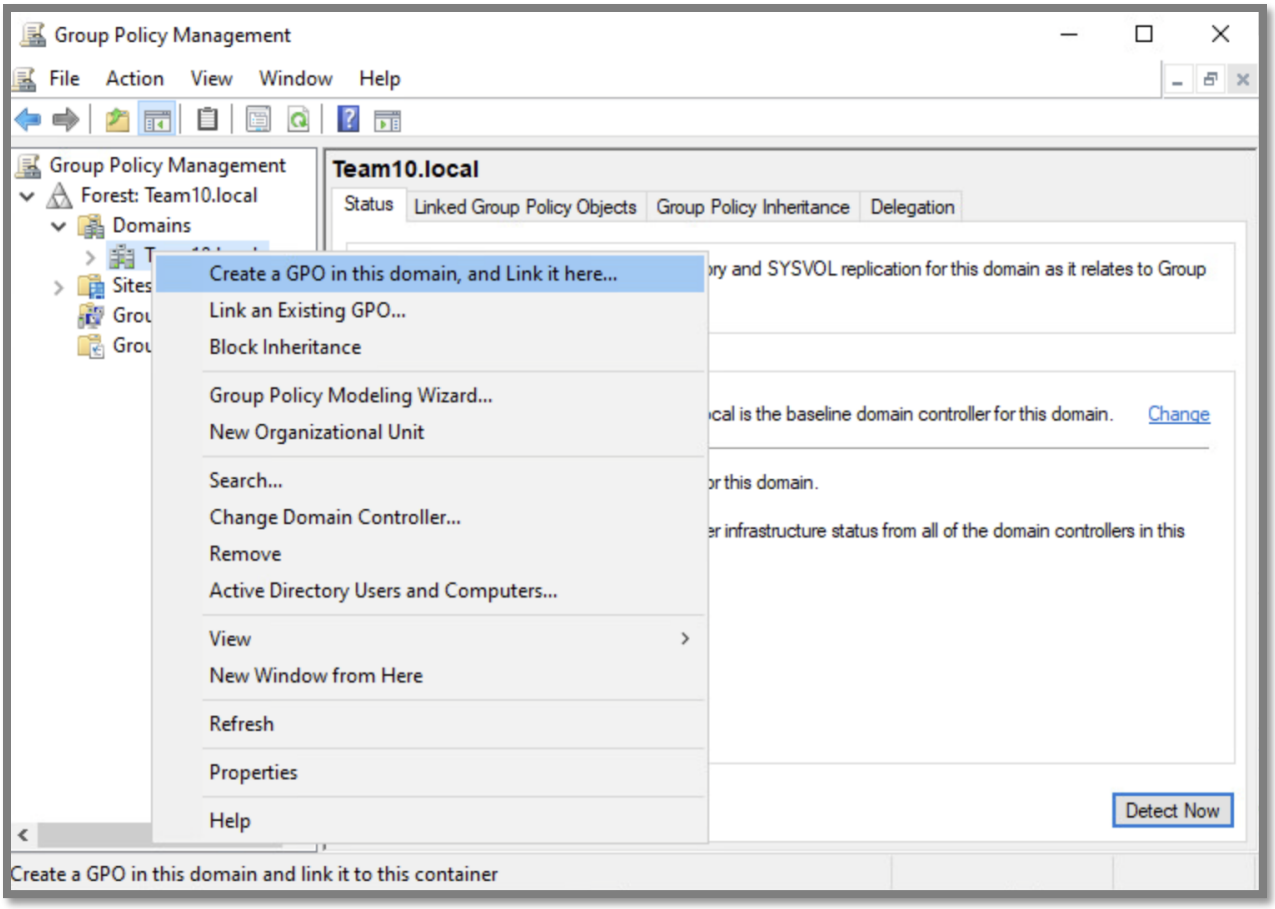


Figure 32: Creating and linking a GPO for Background Policy

Figure 32 demonstrates the process of creating a new Group Policy Object (GPO) and linking it to the domain. In **Group Policy Management**, right-click on the domain or organizational unit where you want to apply the policy, then select **Create a GPO in this domain, and link it here**. Name the GPO **Background Policy**. This newly created GPO can now be configured to manage specific settings, such as enforcing desktop background policies or other system configurations across the domain.

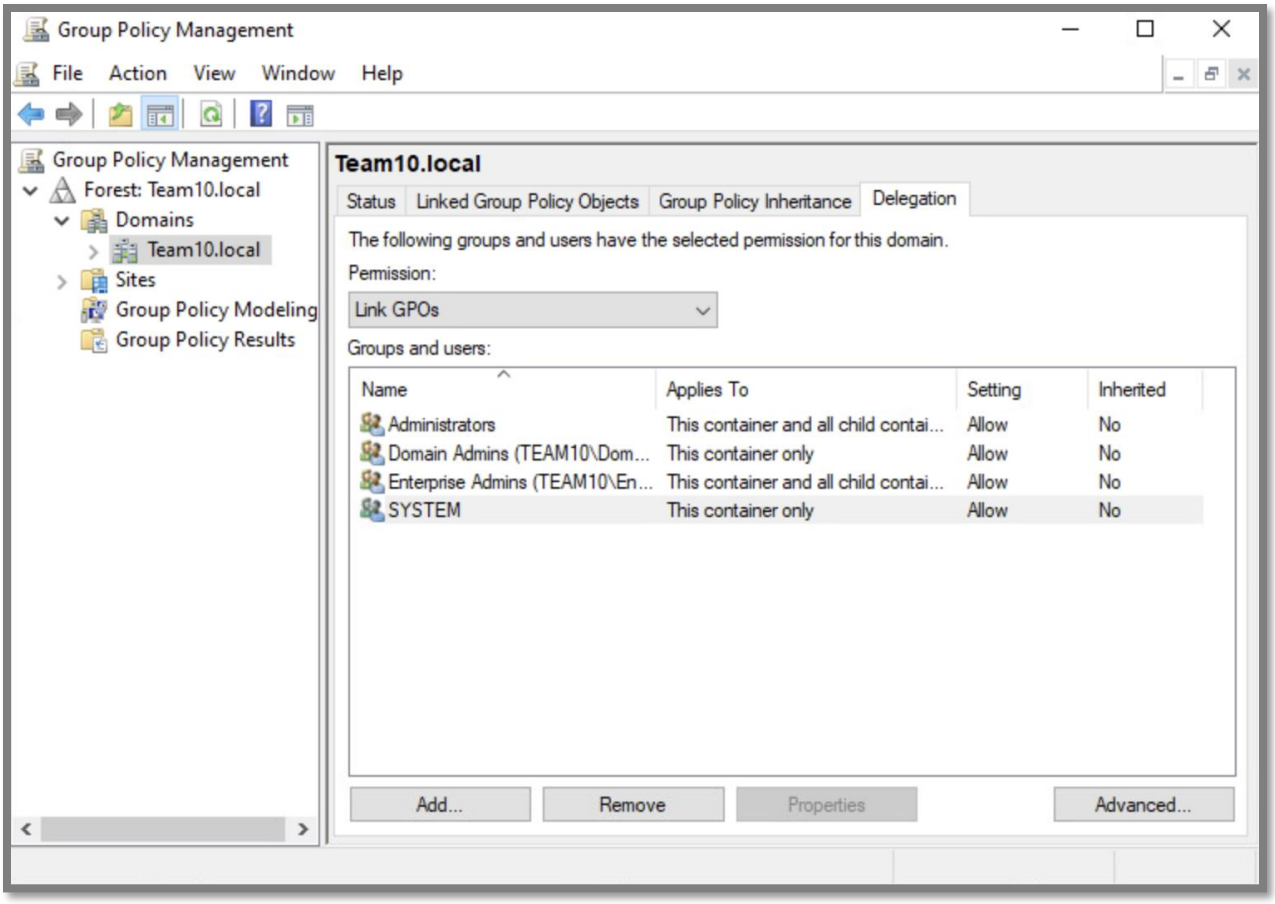


Figure 33: Adding “System” in Delegation

In Figure 33, the **Delegation** settings of the newly created **Background Policy** GPO are being configured. First, click on the **Delegation** tab within the Group Policy Management window. Next, click **Add**, and in the dialog box that appears, search for **System**. Once located, select **System** and add it to the list of delegated users or groups. This allows the system to apply and manage the GPO as needed, ensuring the policy is enforced properly across all relevant machines in the domain.

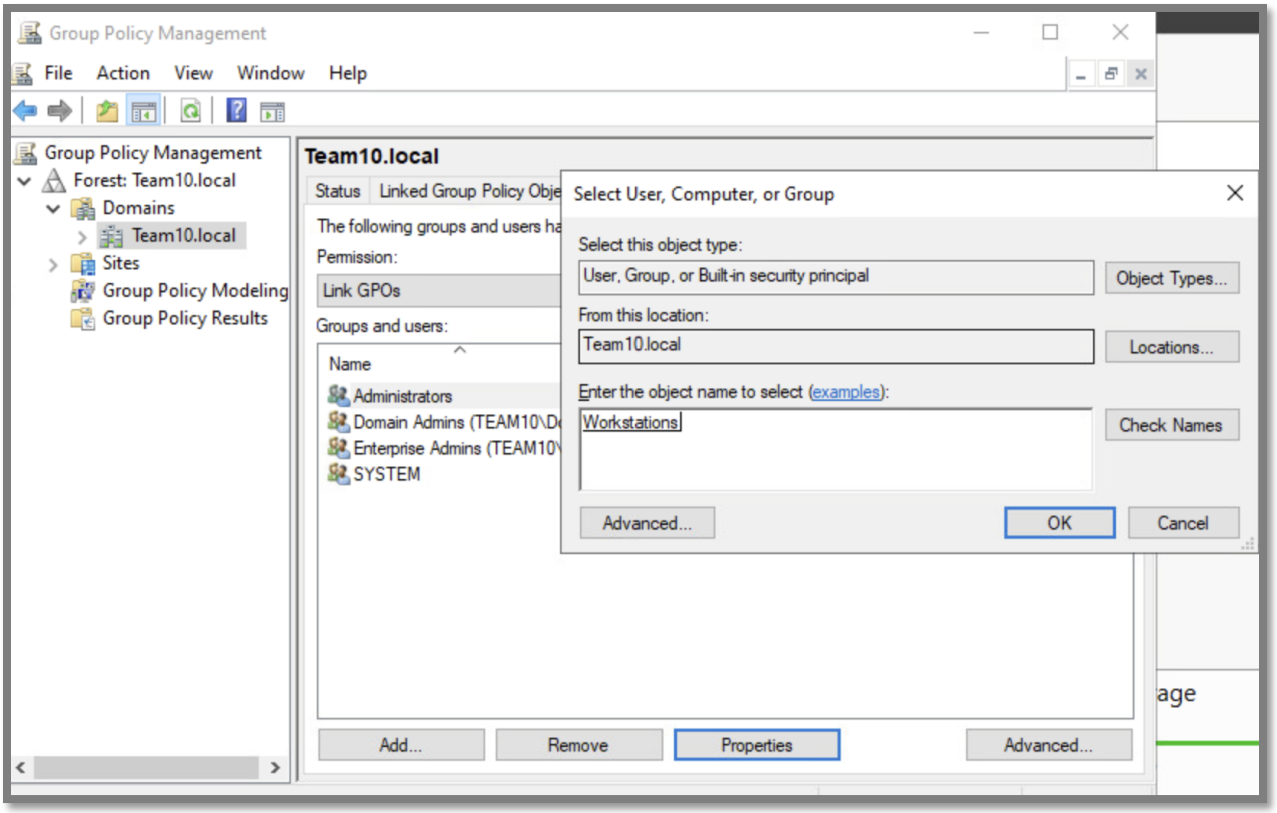


Figure 34: Adding “Workstation” in User, Computer, or Group and Applying Changes.

In Figure 34, the process involves adding a **Workstation** to the list of users, computers, or groups for the GPO. First, in the **Select User, Computer, or Group** dialog, type "Workstation" in the input box, and click **Check Names** to verify and resolve the name. Once confirmed, click **Apply** to save the changes. This ensures that the **Workstation** is correctly added, allowing the GPO to be applied to specific workstations within the network as needed.

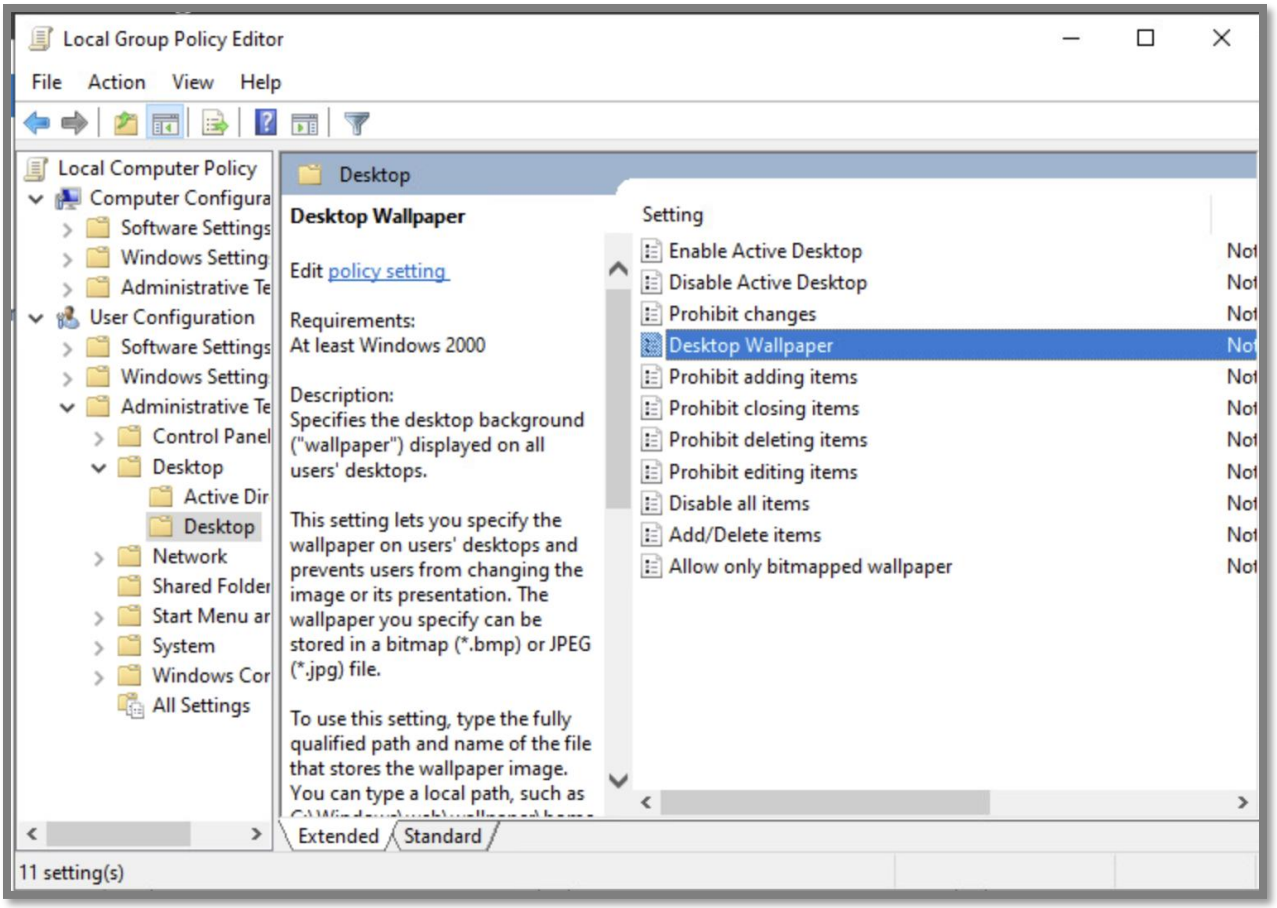


Figure 35: Configuring Desktop Wallpaper via Group Policy

In Figure 35, the steps to set a desktop wallpaper through Group Policy are demonstrated. Navigate to the **User Configuration** section within the **Group Policy Management Editor**. Under **Policies**, expand **Administrative Templates** and then navigate to **Desktop**. In this section, locate the **Desktop Wallpaper** setting. This allows administrators to configure a policy that enforces a specific wallpaper across all users governed by the GPO, ensuring uniformity in desktop appearance.

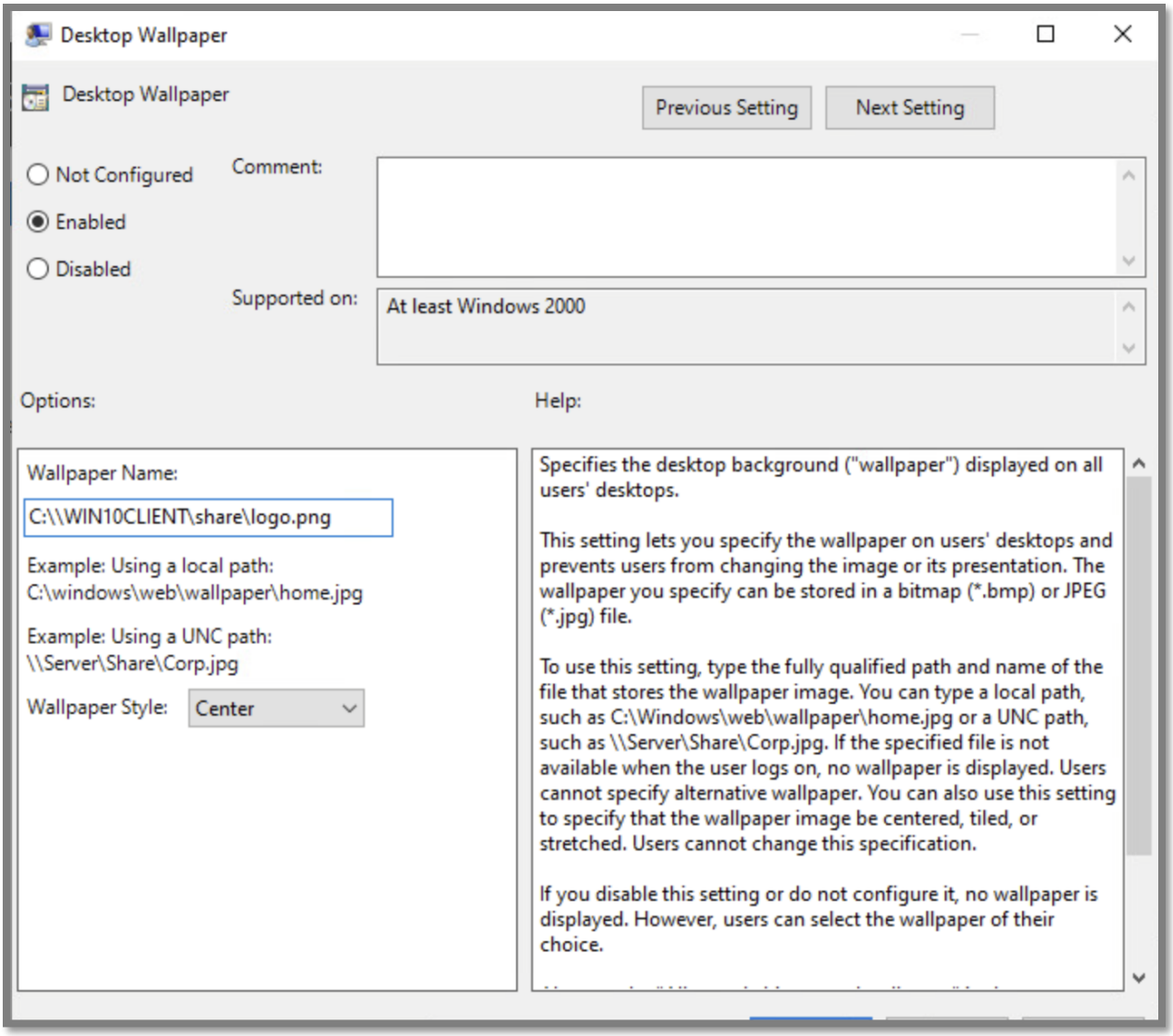


Figure 36: Enabling and Setting the Desktop Wallpaper

This figure shows the process of enabling the **Desktop Wallpaper** policy. Once the **Desktop Wallpaper** setting is located under **User Configuration > Policies >Administrative Templates > Desktop**, click to open it. Select **Enabled** and in the **Wallpaper Name** field, enter the path \\WIN10CLIENT\Share\logo.png to specify the network location of the wallpaper image. Finally, click **Apply** and then **OK** to save the changes. This ensures that all users affected by the GPO will have the specified wallpaper applied from the shared folder.

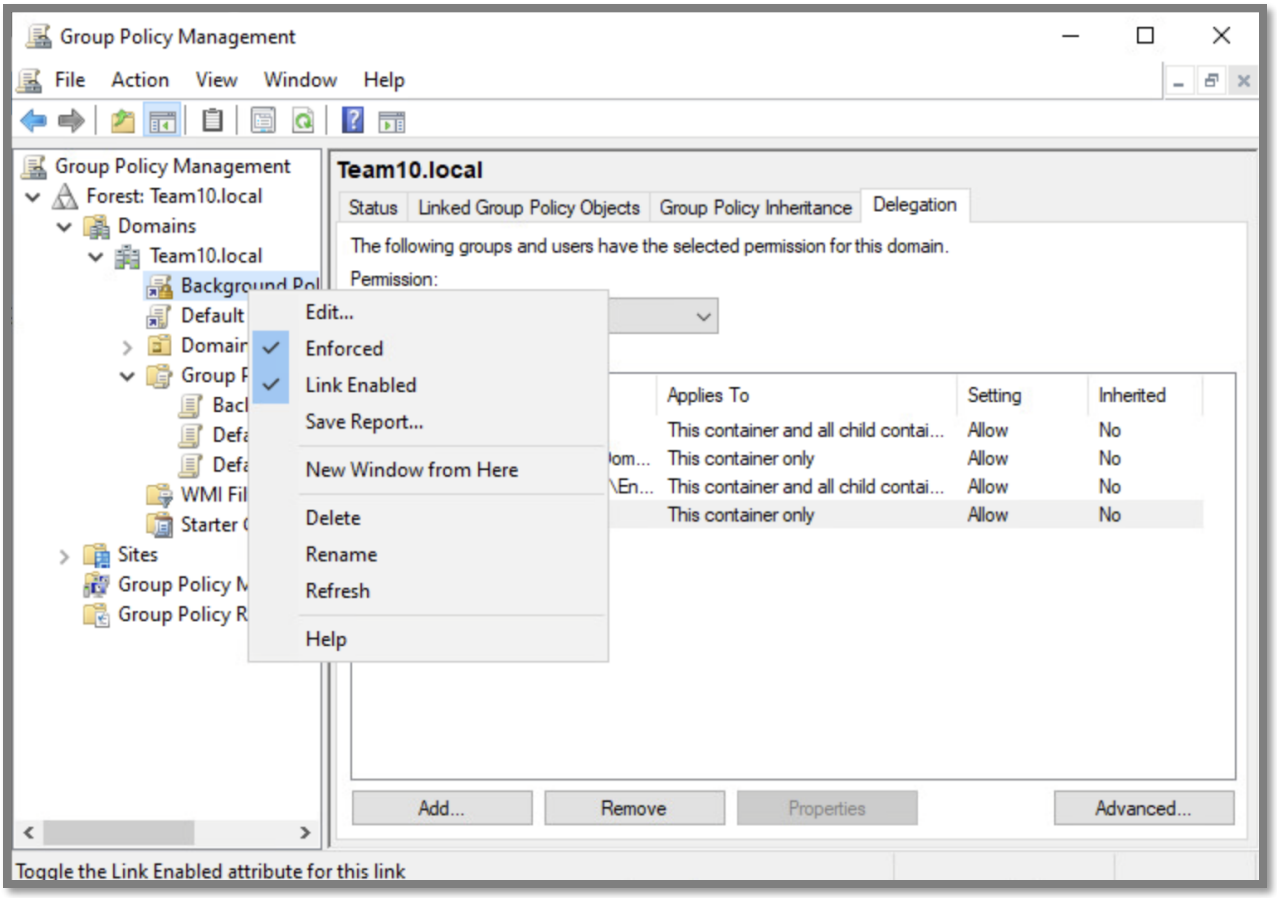


Figure 37: Enforcing and Enabling the Background Policy GPO

In Figure 37, the **Background Policy** GPO is being configured for enforcement. Locate the **Background Policy** in the Group Policy Management console. Right-click on the GPO and select **Enforced** from the context menu. This action ensures that the policy takes precedence over any conflicting policies within the hierarchy. Additionally, confirm that **Link Enabled** is checked, which allows the GPO to be actively applied to the designated organizational unit or domain. These settings are crucial for ensuring that the wallpaper policy is consistently enforced across all applicable user accounts.

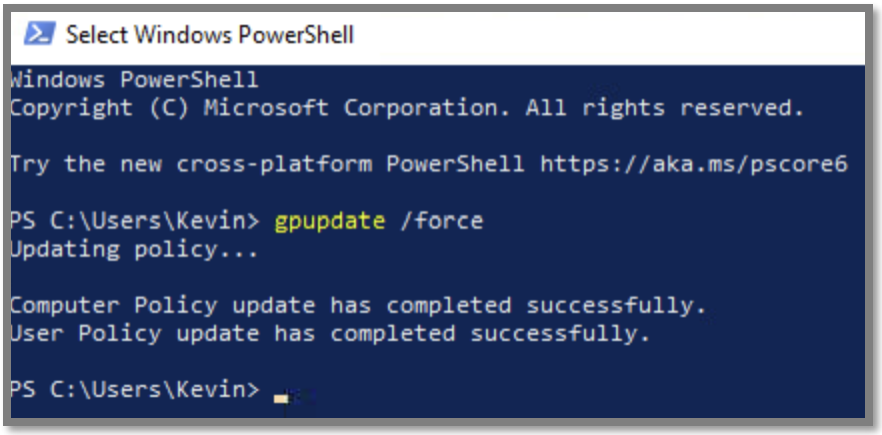


Figure 38: Updating Group Policy on Win10Client

In this figure, the process of logging into the **Win10Client** using the user account **Kevin** is demonstrated. After successfully logging in, open the Command Prompt with administrative privileges. Type the command gpupdate /force and press Enter to force an update of the Group Policy settings. This command ensures that any new policies, including the **Background Policy** GPO, are applied immediately to the user session. The execution of this command is essential for confirming that the desktop wallpaper settings take effect as configured.

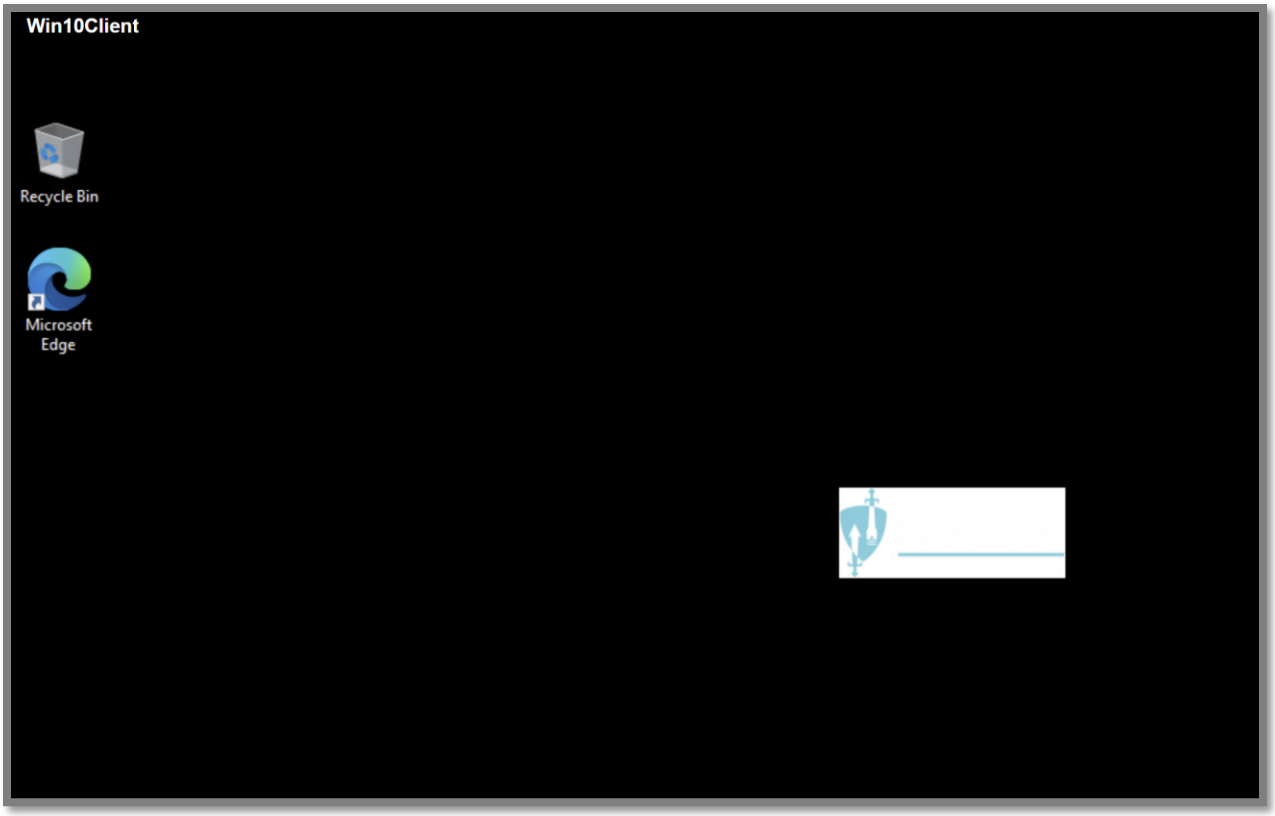


Figure 39: NetDef Background Successful

Figure 39 illustrates the successful application of the **NetDef Background** policy. After starting the **Win10Client** and signing in with the user account **Kevin**, the specified background image is displayed as the desktop wallpaper. This outcome confirms that the Group Policy Object (GPO) for the desktop wallpaper has been effectively applied, showcasing the successful implementation of network-wide configurations for user environments. The presence of the intended background image indicates that the policy settings were correctly enforced and updated during the user login process.

7. Setup Powershell Transcription using Group Policy

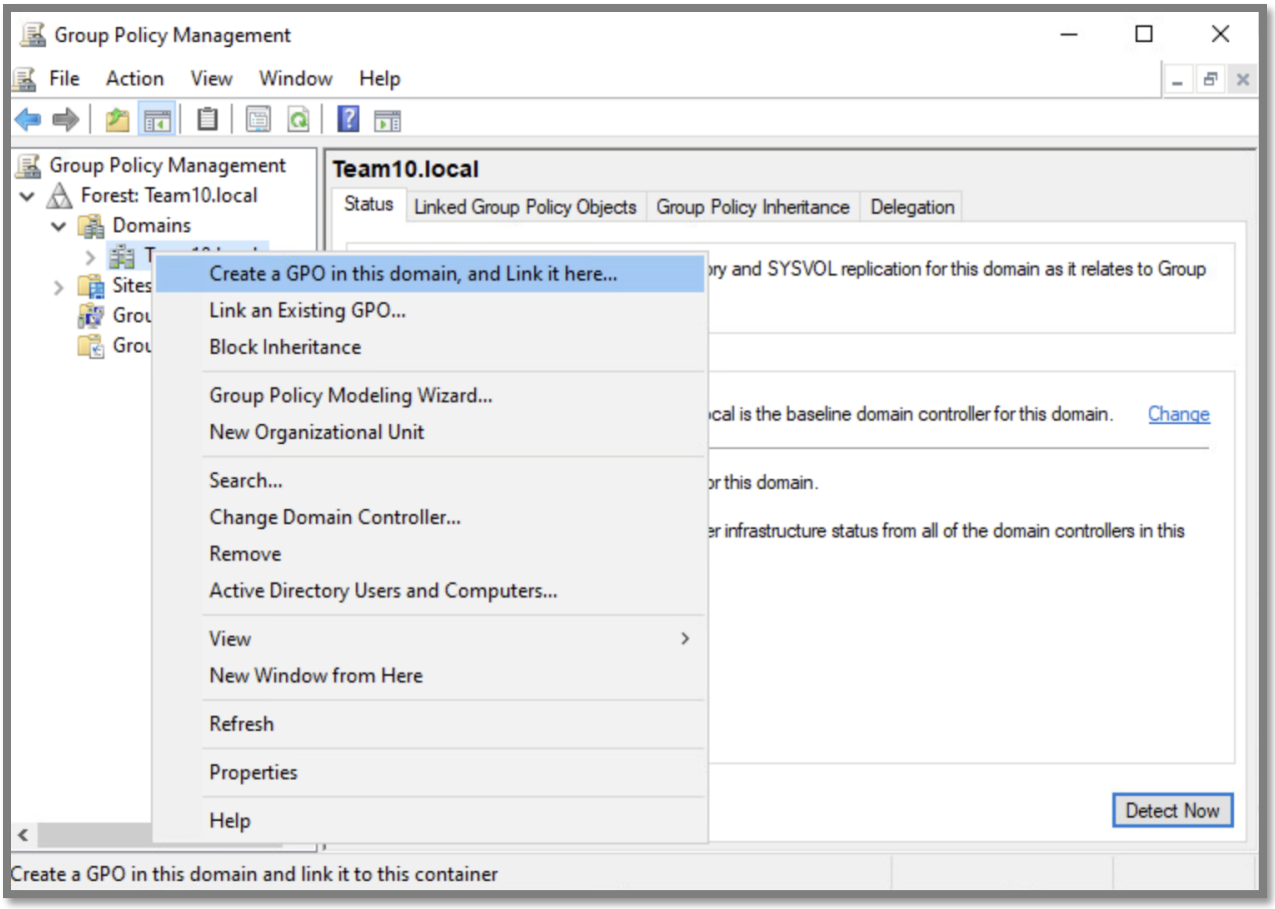


Figure 40: Creating and linking a GPO for Background Policy

Figure 40 shows the process of creating a new Group Policy Object (GPO) and linking it to a domain. In **Group Policy Management**, right-click on the domain where you want to apply the policy, then select **Create a GPO in this domain, and Link it here**. Name the GPO **PowerShell Transcript**. This newly created GPO can now be configured to manage specific settings, such as enforcing desktop background policies or other system configurations across the domain.

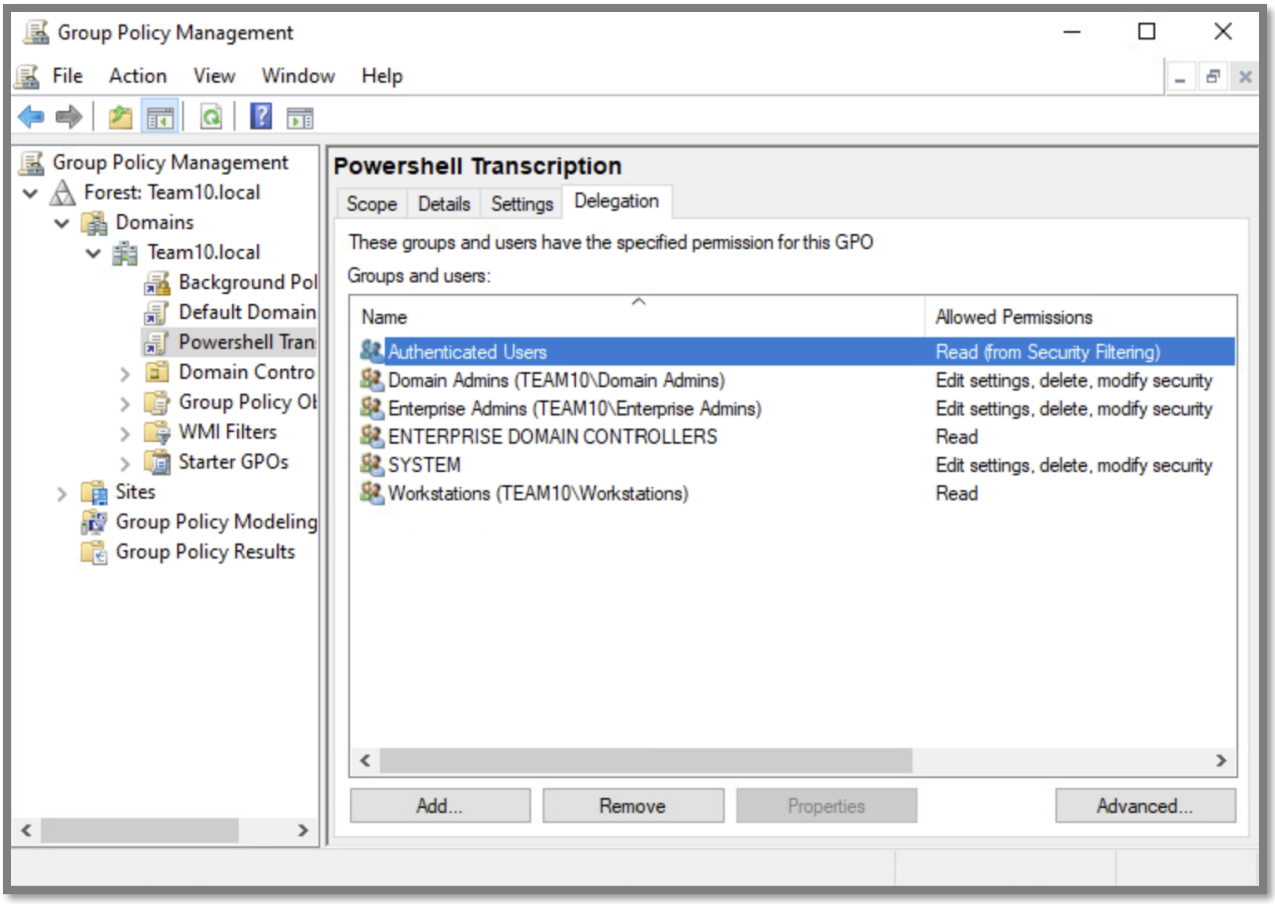


Figure 41: Adding “System” in Delegation

In Figure 41, the **Delegation** settings of the newly created **PowerShell Transcript** GPO are being configured. First, navigate the **Delegation** tab within the Group Policy Management window. The, click **Add**, and in the dialog box that appears, search for **Workstations**. Once located, select **Workstations** and add it to the list of delegated users or groups. This allows the system to apply and manage the GPO as needed, ensuring the policy is enforced properly across all relevant machines in the domain.

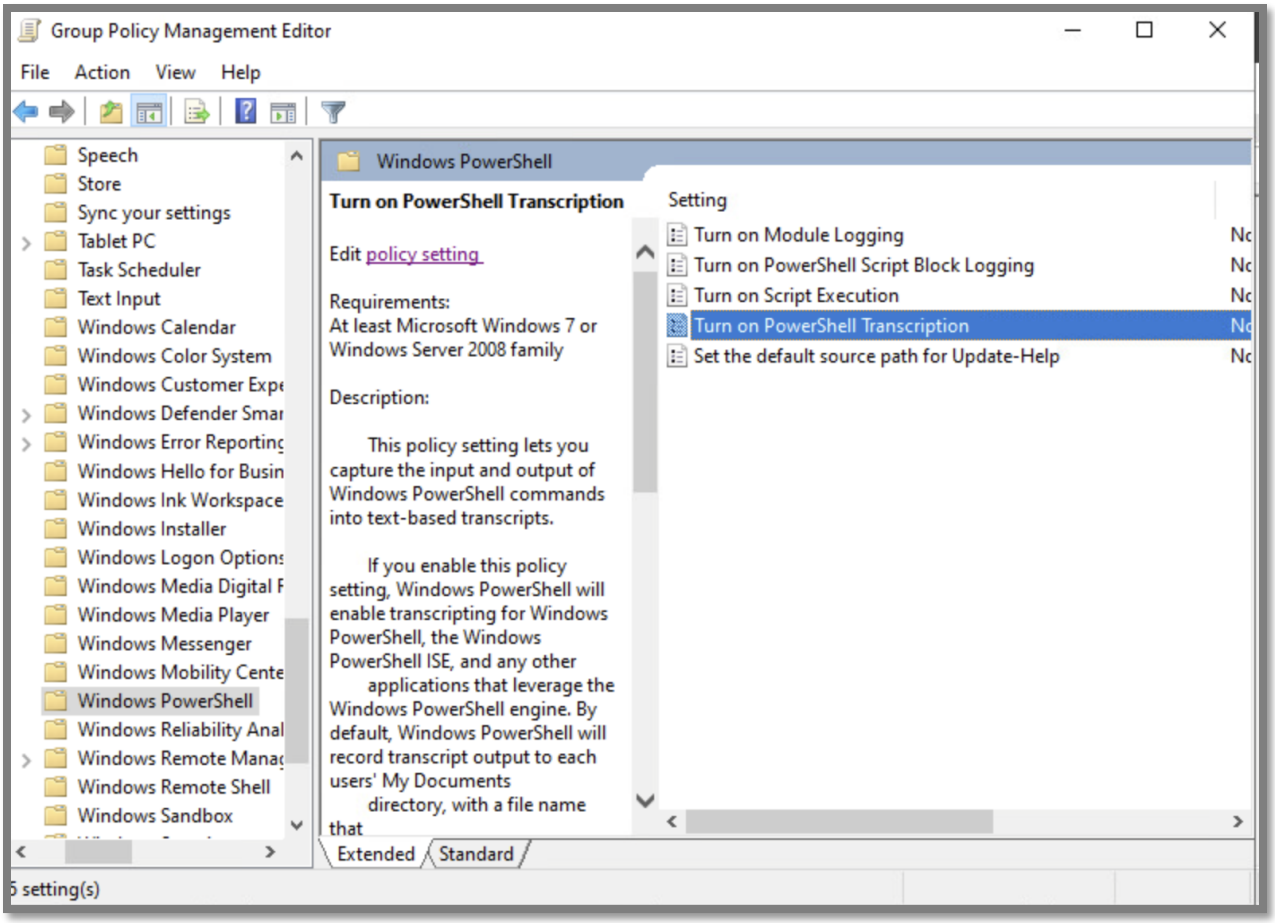


Figure 42 Enabling PowerShell Transcript

In Figure 42, the process of enabling PowerShell transcription is demonstrated. Navigate to **Computer Configuration** within the Group Policy Management Editor. Expand the **Administrative Templates** section, then go to **Windows Components** and select **Windows PowerShell**. Locate the setting labeled **Turn on PowerShell Transcription** and double-click it to open its properties.

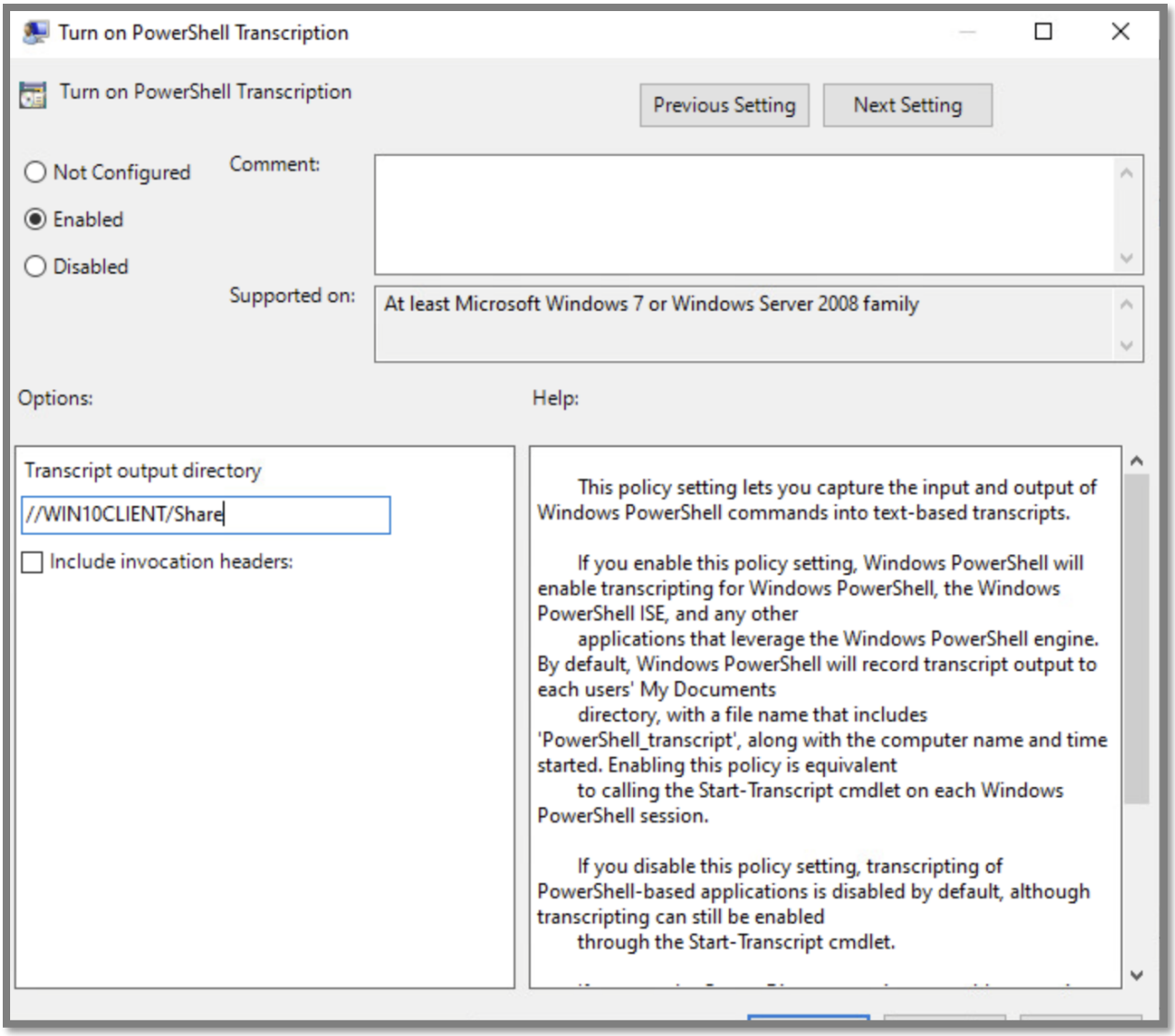


Figure 43: Configuring PowerShell Transcription Settings

In Figure 43, the process of enabling PowerShell transcription is continued. Then double- click on the **Turn on PowerShell Transcription** setting in the Group Policy Management Editor, click **Enabled** to activate the transcription feature. In the **Transcript output directory** field, enter the path **\\WIN10CLIENT\Share** to specify the network location where the transcription logs will be saved. This configuration ensures that all PowerShell session activities are recorded and stored in the designated directory, facilitating easy access and review for auditing purposes. After making these changes, click **Apply** and then **OK** to save the settings.

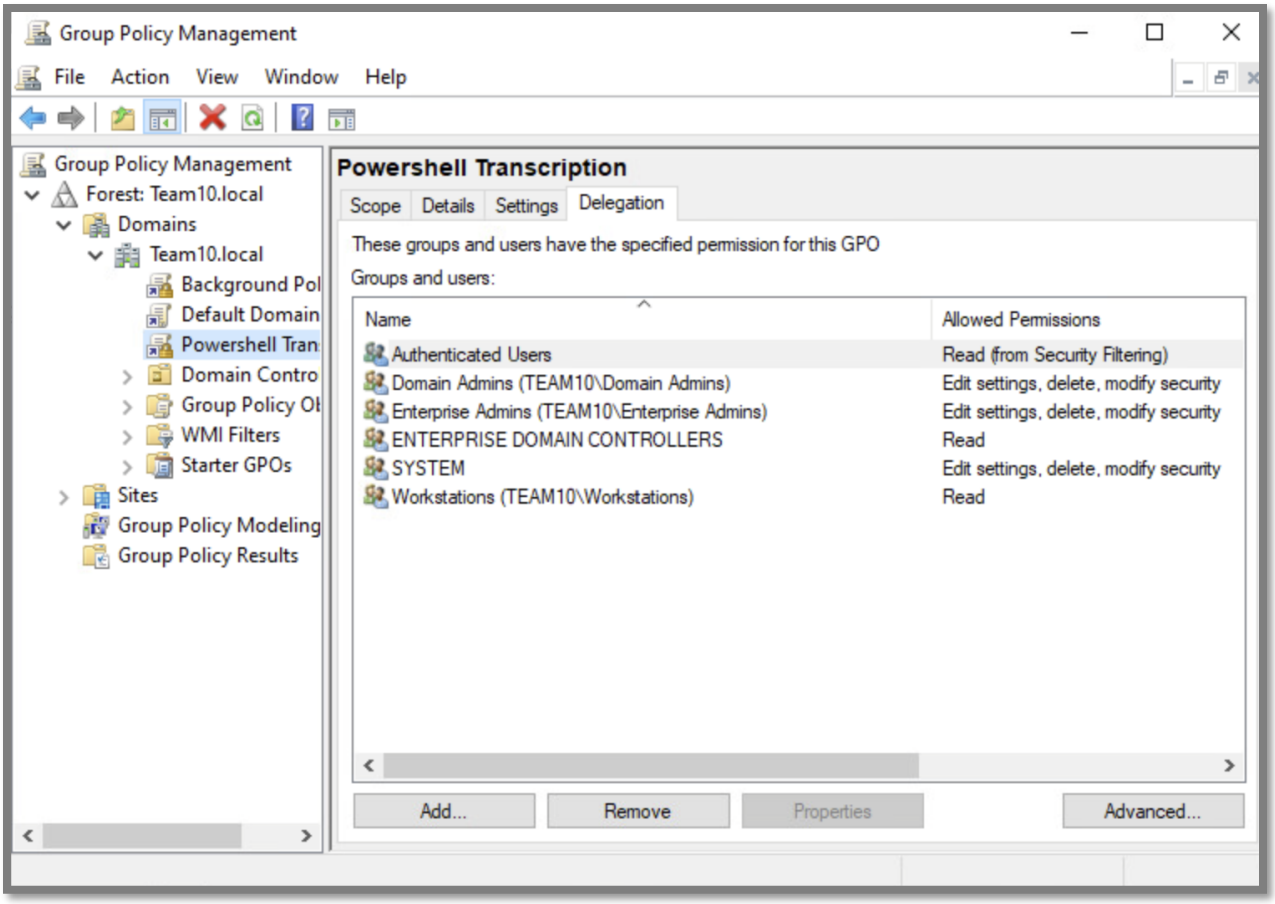


Figure 44: Enforcing and Enabling the Background Policy GPO

In Figure 44, the **PowerShell Transcript** GPO is being configured for enforcement. Locate the **PowerShell Transcript** in the Group Policy Management console. Right-click on the GPO and select **Enforced** from the context menu. This action ensures that the policy takes precedence over any conflicting policies within the hierarchy. Additionally, confirm that **Link Enabled** is checked, which allows the GPO to be actively applied to the designated organizational unit or domain.

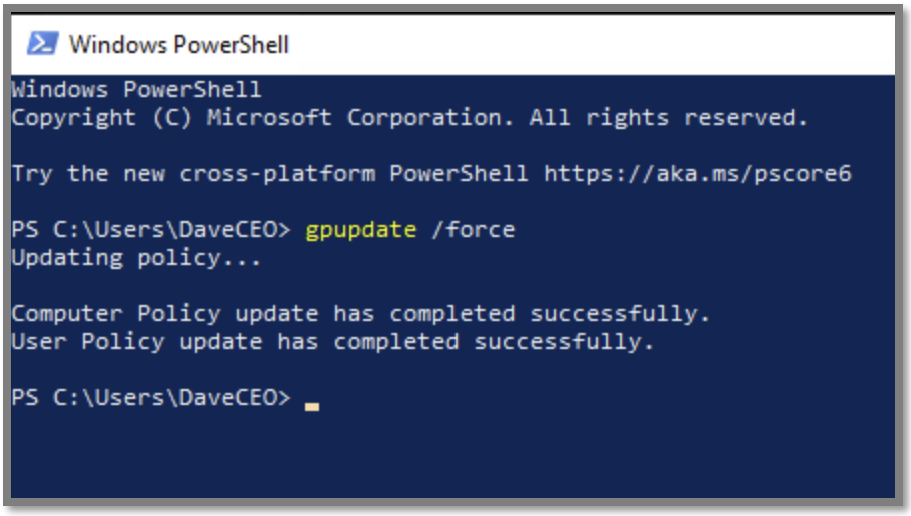


Figure 45: Updating Group Policy on Win10Client as DaveCEO

In this figure, the process of logging into the **Win10Client** with the user account **DaveCEO**is shown. After successfully logging in, open **PowerShell** with administrative privileges. Type the command gpupdate /force and press Enter to force an update of the Group Policy settings. This command ensures that any new policies, including the PowerShell transcription settings, are applied immediately to the user session. Running this command is crucial for confirming that the configured policies are effectively enforced for the user, enabling the transcription of all PowerShell commands executed during the session.

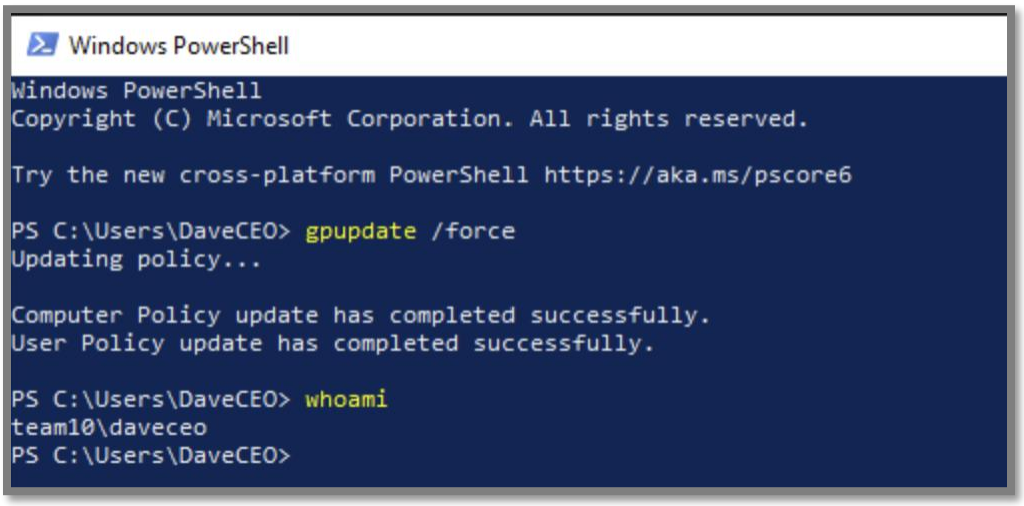


Figure 46: Verifying User Identity with the whoami Command

In Figure 46, the process of verifying the current user identity on **Win10Client** is demonstrated. After logging in as **DaveCEO**, type the command **whoami** in the PowerShell window and press Enter. The output will return the user account in the format

team10\Daveceo.

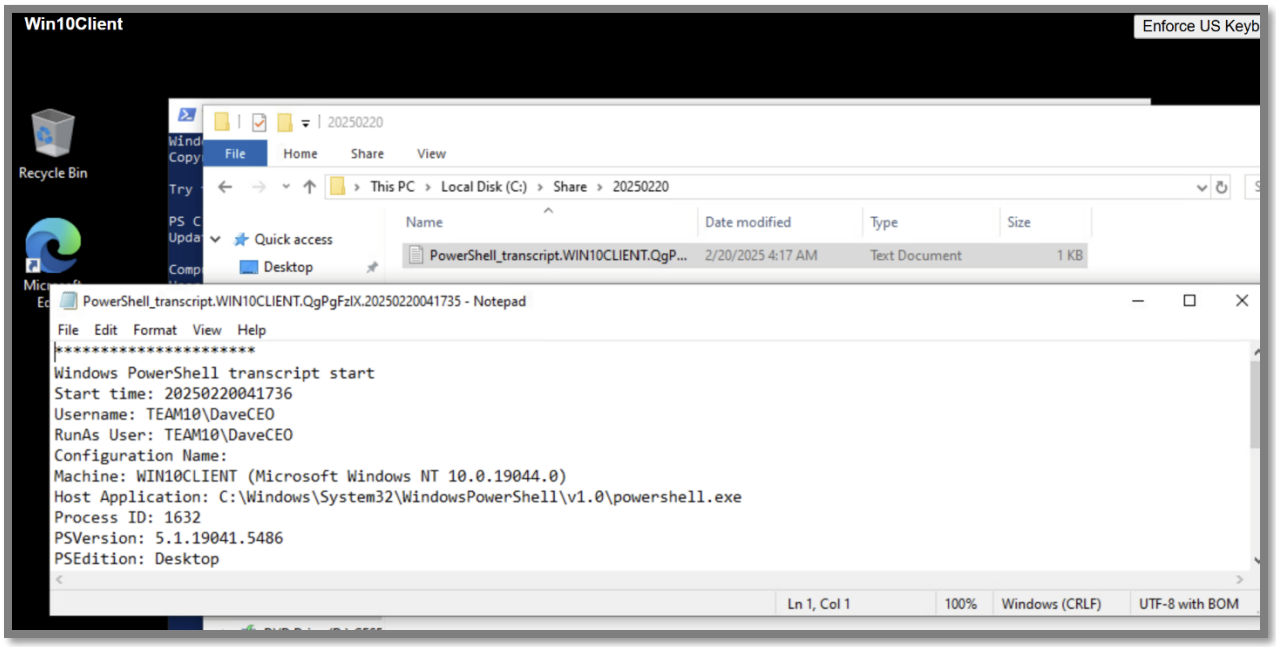
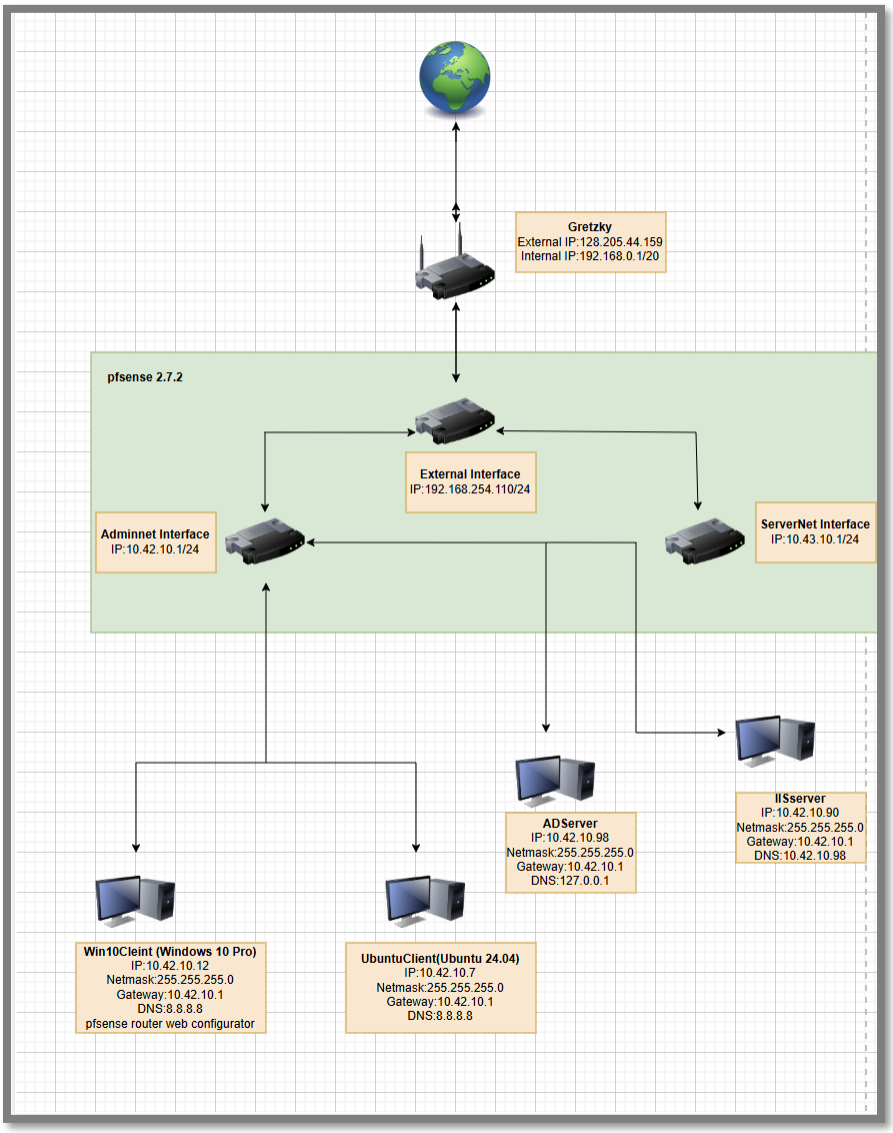


Figure 47: Verifying PowerShell Transcript in the Shared Folder

In Figure 47, I show the successful execution of PowerShell transcription. After logging in to **Win10Client** as **DaveCEO**, navigate to the shared folder at \\WIN10CLIENT\Share. Within this folder, there the PowerShell transcript files is visible, showing that the transcription feature is working as intended. The presence of these transcript files confirms that all PowerShell commands and their outputs executed during the session have been successfully recorded, providing an effective audit trail for review and analysis.

Appendix A.


Gretzky
External IP:128.205.44.159
Internal IP:192.168.0.1/20
pfsense 2.7.2
External Interface
IP:192.168.254.110/24
Adminnet Interface
IP:10.42.10.1/24
ServerNet Interface
IP:10.43.10.1/24
ADServer
IP:10.42.10.98
Netmask:255.255.255.0
Gateway:10.42.10.1
DNS:127.0.0.1
IISserver
IP:10.42.10.90
Netmask:255.255.255.0
Gateway:10.42.10.1
DNS:10.42.10.98
Win10Cleint (Windows 10 Pro)
IP:10.42.10.12
Netmask:255.255.255.0
Gateway:10.42.10.1
DNS:8.8.8.8
pfsense router web configurator
UbuntuClient(Ubuntu 24.04)
IP:10.42.10.7
Netmask:255.255.255.0
Gateway:10.42.10.1
DNS:8.8.8.8