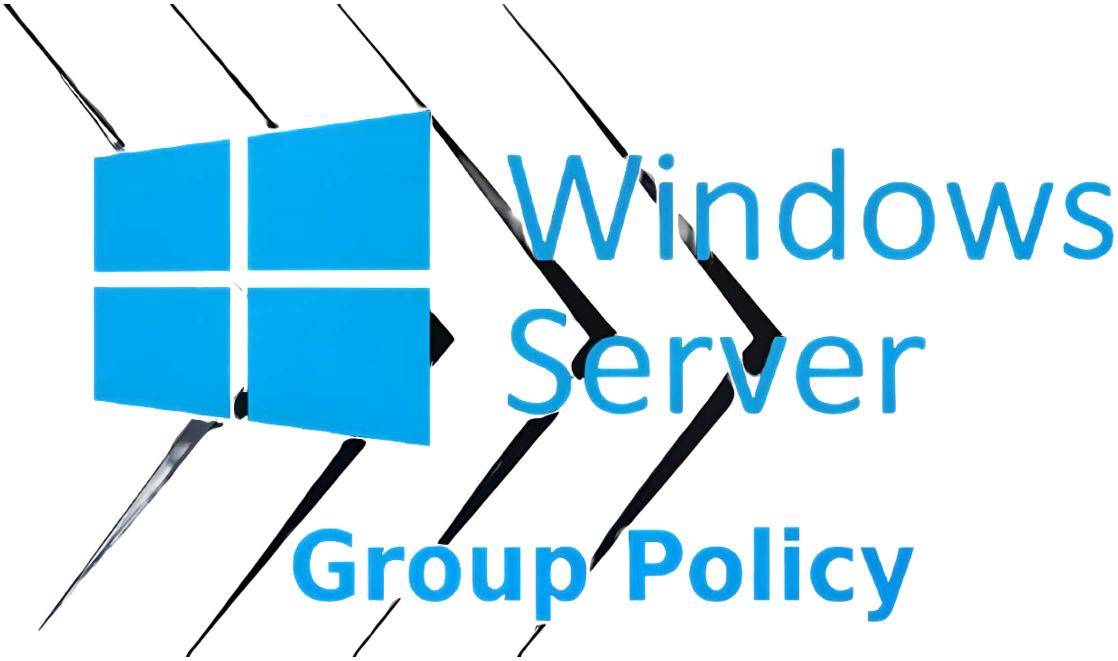
Active Directory Group Policy



For Educational Use Only

Isolated Lab Environment Hands-On Guide for IT Professionals & Students

Author: Silent Mucharira
Date: January 2026

Configurations shown here are for educational purposes only and require hardening for production use.

What is Group Policy in Active Directory?

In Active Directory, a **Group Policy Object (GPO)** is a set of configuration settings used for **centralized management**. Administrators use the Group Policy Management Console (GPMC) to link these policies to Domains or Organizational Units (OUs), allowing them to automatically deploy security rules, software updates, or desktop restrictions across the entire network at once. For example, a GPO can be used to force Microsoft Edge to launch automatically for every user in the domain without manually configuring each computer.

Imagine you are at a very big school with hundreds of classrooms. Instead of the Principal walking into every single room to tell every student the rules, they have a "Magic Rule Book" in their office. Whenever the Principal writes a new rule in this book, like "Everyone must have a blue background on their computer" or "The school website must open as soon as you turn your laptop on," the rule instantly flies and lands on every student's desk at the same time. This "Magic Rule Book" is what we call **Group Policy**. It helps the person in charge make sure everyone follows the same rules and has the same tools ready for work without having to talk to everyone one by one.

The Benefits of Group Policy in Active Directory

Using Group Policy Objects (GPOs) provides several key advantages for managing a network:

- **Single Sign-On:** Users only need to log in once to access all authorized network resources.
- **Centralized User Management:** Administrators can create, modify, or delete user accounts across the entire network from one central location.
- **Consistent Security:** Security settings and policies (like password requirements) can be applied instantly to every computer in the domain.
- **Efficient Resource Sharing:** It simplifies the process of sharing files, printers, and applications with specific groups.
- **Scalability:** The system is designed to grow easily, supporting everything from small offices to massive enterprise organizations.
- **Predictable Environments:** Settings like desktop backgrounds or mandatory applications (e.g., Microsoft Edge) are standardized, making troubleshooting and documentation much easier.

Key Components of Group Policy

For your project document, here is a concise breakdown of the main parts that make Group Policy work:

- **Group Policy Objects (GPOs):** These are the actual containers or "files" where all the specific rules and settings are stored.

- **Group Policy Management Console (GPMC):** The central tool (found in **Server Manager > Tools**) used by administrators to create, delete, and manage these policies across the domain.
- **Group Policy Management Editor:** The specific window where you go to "Edit" a policy to choose the exact rules, such as setting a wallpaper or starting an app like Edge.
- **Containers (OUs, Domains, Sites):** These are the locations in Active Directory where you "Link" a GPO. For example, linking a policy to your domain ensures it applies to everyone in that group.
- **Client-Side Extensions (CSEs):** These are small pieces of software on the user's computer (like your Windows 10 machine) that read the "Magic Rule Book" and apply the changes to the system.

Purpose and Uses of Group Policy

The primary purpose of **Group Policy** is to provide **centralized management** and automation across a network. Instead of manually configuring every computer, an administrator can use GPOs to perform the following tasks:

- **Security Enforcement:** Apply consistent security settings, such as password requirements and account lockouts, to all computers instantly.
- **Access Control:** Restrict or allow access to specific system tools, control panel items, or hardware like USB drives.
- **User Environment Customization:** Standardize the user experience by setting mandatory desktop backgrounds or branding.
- **Automation:** Automatically launch essential applications (like Microsoft Edge) or run scripts as soon as a user logs on.
- **Software Deployment:** Install or update software across the entire organization from one central location.
- **Resource Efficiency:** Easily share and manage access to network files, folders, and printers for specific groups.

Types of Group Policy in Active Directory

In an Active Directory environment, Group Policies are primarily categorized by how they are applied and where they are stored. The two main types you will work with in your project are:

- **Local Group Policy:** These are settings stored directly on an individual computer. They only affect that specific machine and are used when a computer is not part of the domain.
- **Domain-Based Group Policy:** These are the policies we are creating in this lab (like the "Auto-Start Edge" or "Wallpaper" policies). They are stored in Active Directory

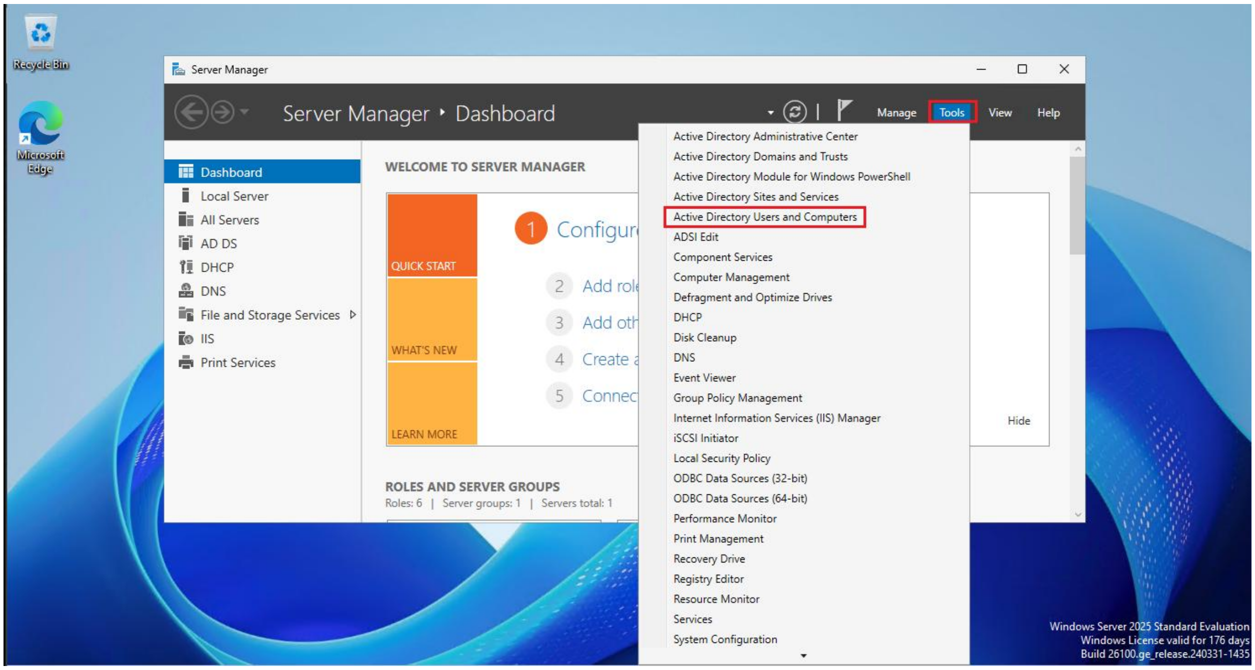
and can be applied to thousands of users or computers at once across the entire domain.

Within these GPOs, settings are further divided into two sections:

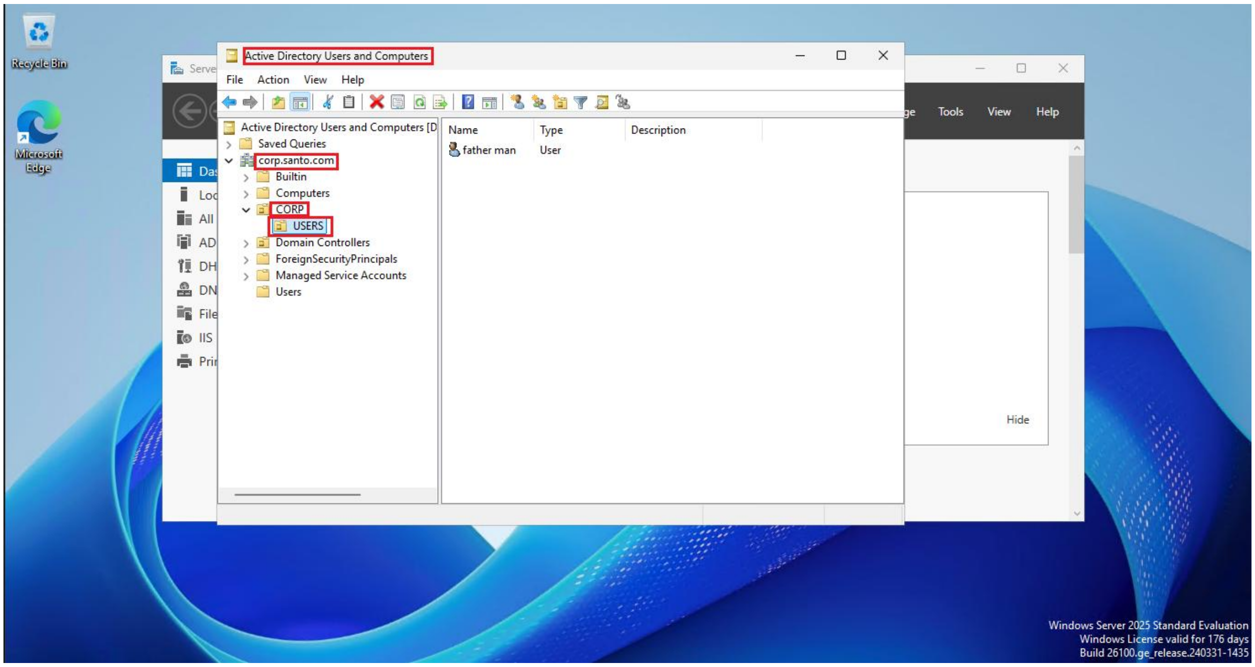
- **Computer Configuration:** Rules that apply to the machine itself, regardless of who logs in (e.g., system updates or security lockdowns).
- **User Configuration:** Rules that follow the person, no matter which computer they sit at (e.g., your specific desktop wallpaper or starting Microsoft Edge at logon).

Deploying GPO

- Go to Start >> Server Manager >> Tools >> Active Directory Users and Computers

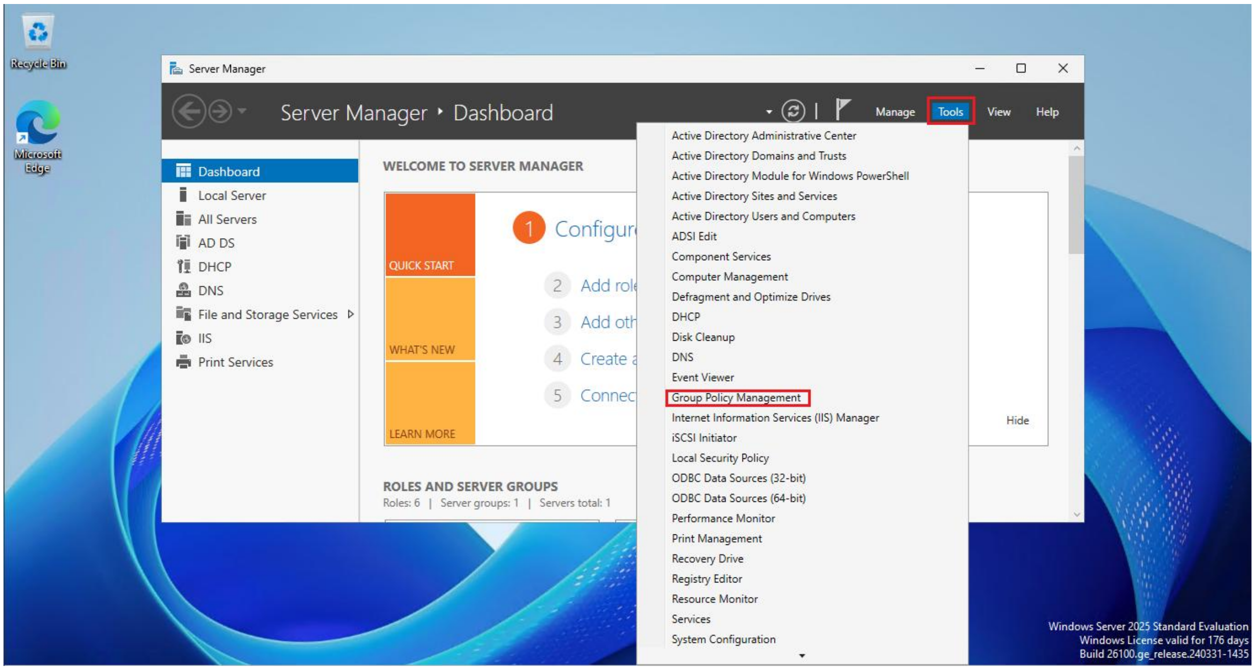

Recycle Bin
Microsoft Edge
Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
IIS
Print Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure
2 Add role
3 Add oth
4 Create a
5 Connec
Hide
ROLES AND SERVER GROUPS
Roles: 6 | Server groups: 1 | Servers total: 1
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Recovery Drive
Registry Editor
Resource Monitor
Services
System Configuration
Windows Server 2025 Standard Evaluation
Windows License valid for 176 days
Build 26100.ge_release.240331-1435

- Select the domain, select the OU (CORP), and select USERS; you will then see the users in the domain. These are the users on whom we are going to impose the GPO.



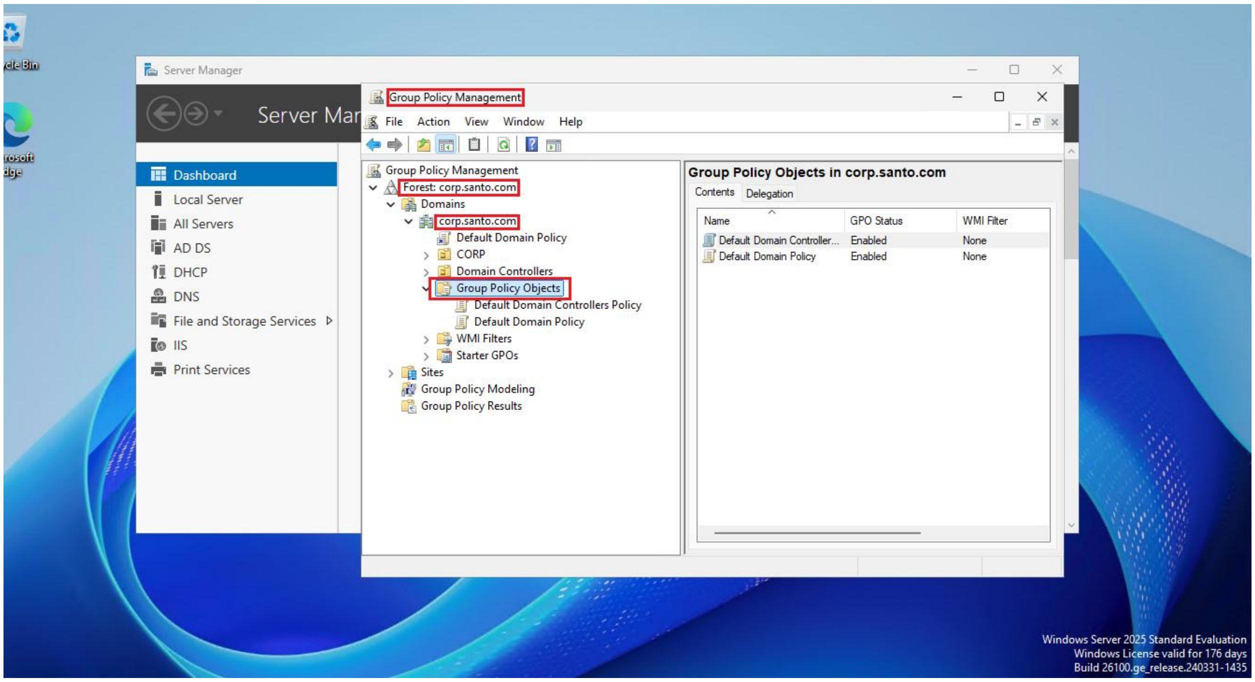
Recycle Bin
Microsoft Edge
Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [D
Saved Queries
corp.santo.com
Builtin
Computers
CORP
USERS
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name Type Description
father man User
Tools View Help
Hide
Windows Server 2025 Standard Evaluation
Windows License valid for 176 days
Build 26100.ge_release.240331-1435

- In Server Manager, select Tools, and then click Group Policy Management.



Recycle Bin
Microsoft Edge
Server Manager
Server Manager ▸ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
IIS
Print Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configur
2 Add rol
3 Add oth
4 Create
5 Connec
ROLES AND SERVER GROUPS
Roles: 6 | Server groups: 1 | Servers total: 1
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Recovery Drive
Registry Editor
Resource Monitor
Services
System Configuration
Hide
Windows Server 2025 Standard Evaluation
Windows License valid for 176 days
Build 26100.ge_release.240331-1435

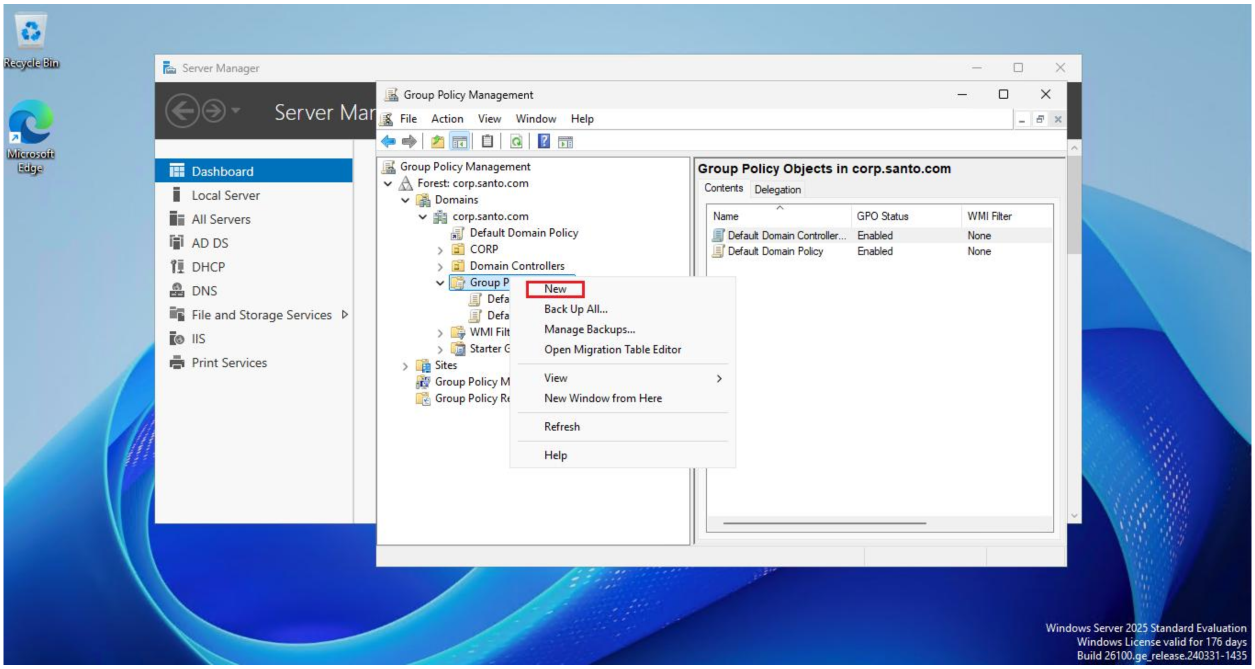
- Expand the **Forest**, select the **Domain**, and then click on **Group Policy Objects**.



Group Policy Objects in corp.santo.com

Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None

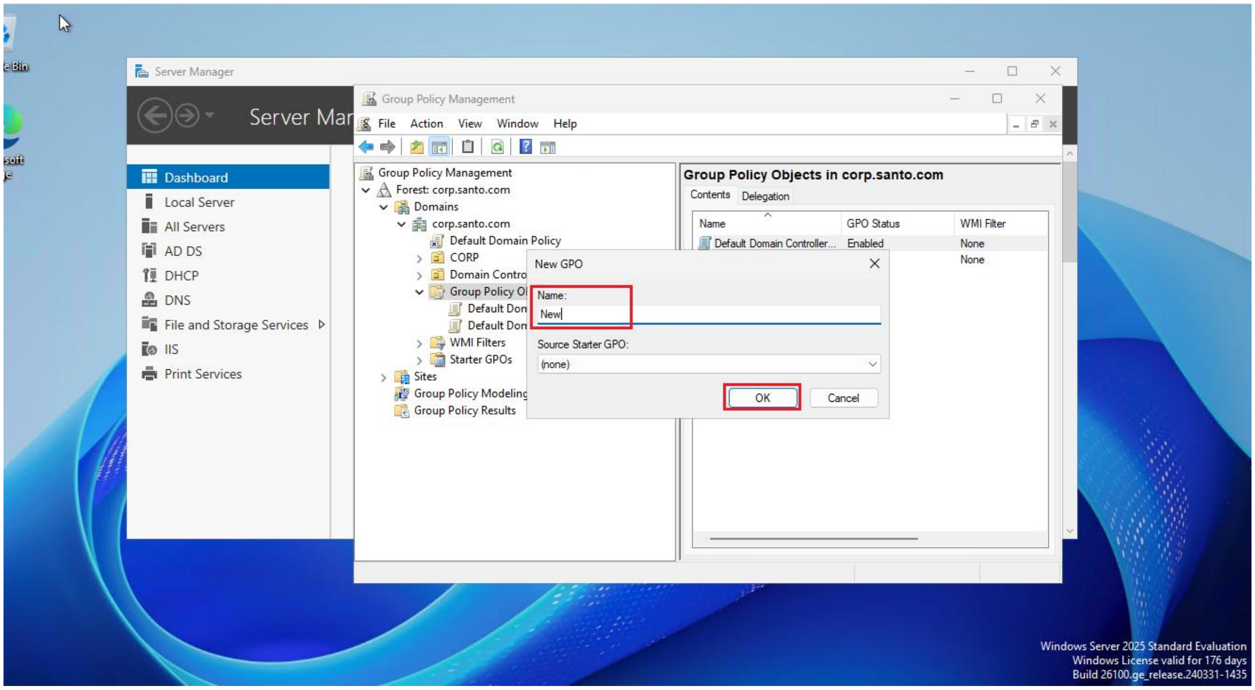
- Right-click **Group Policy Objects** and select **New** to create and name your new GPO.



Group Policy Objects in corp.santo.com

Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None

- Enter a name of your choice for the **new GPO and click OK.**



New GPO

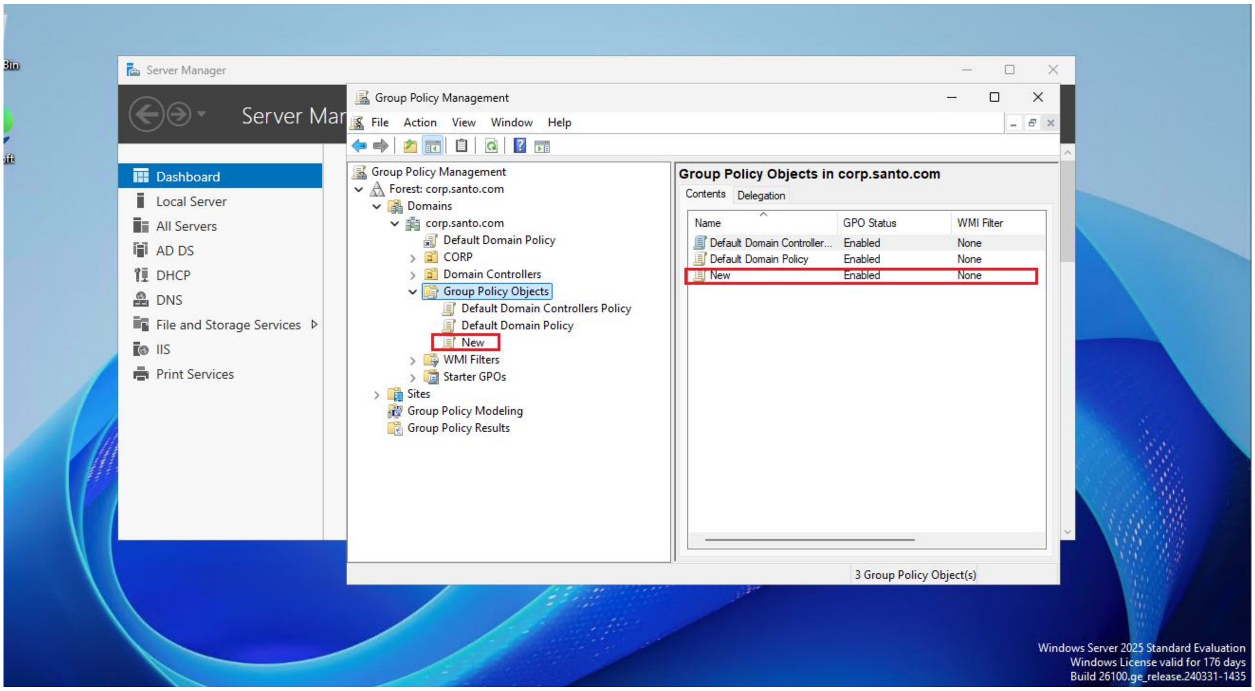
Name: New

Source Starter GPO: (none)

OK Cancel

Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
		None

- Once the new Group Policy Object is created, you can view its details in the right-hand panel.

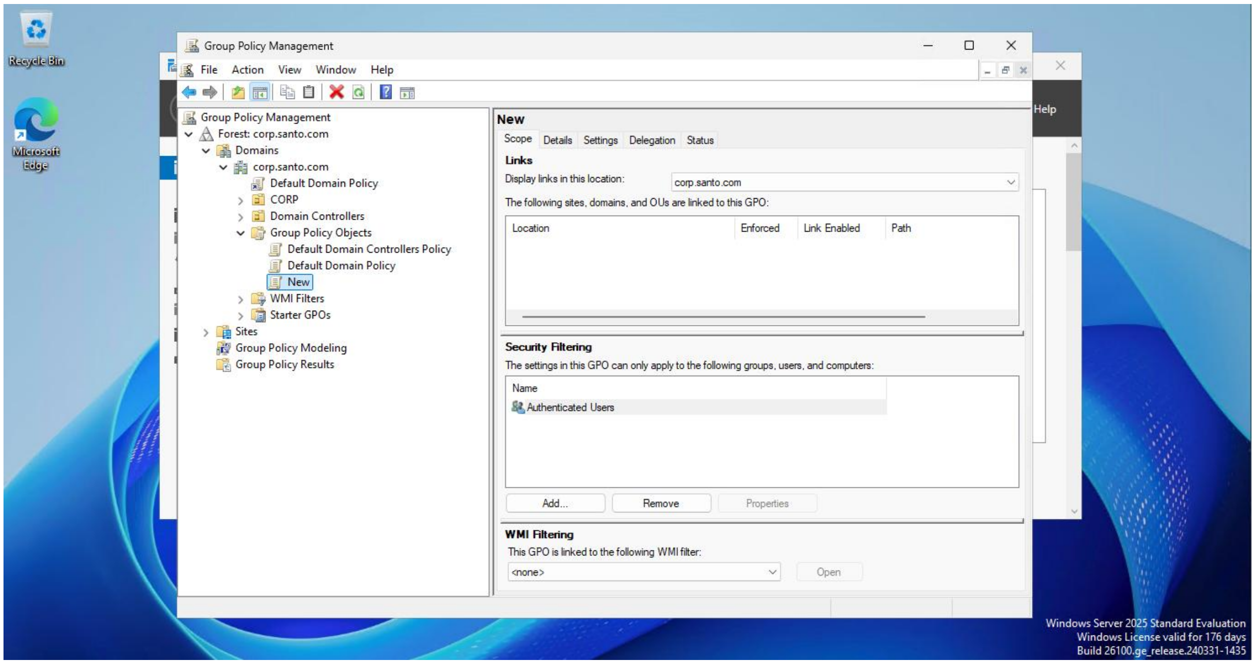


Group Policy Objects in corp.santo.com

Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None
New	Enabled	None

3 Group Policy Object(s)

- **Double-click the new GPO**; in the right-hand pane, you can see that the object is linked to the domain and that the settings apply to **'Authenticated Users' by default.**



New

Links

Display links in this location: corp.santo.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

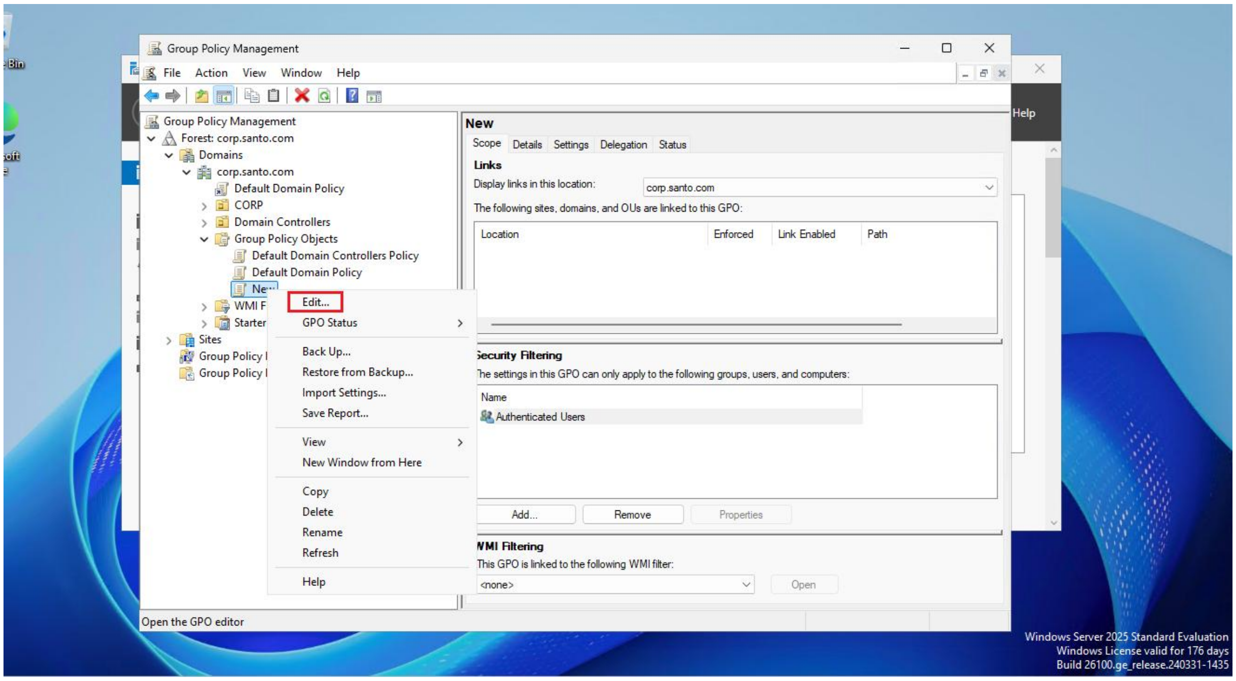
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

- To set a new rule on the GPO, right-click the **new GPO and select Edit;** you will then be prompted with the Group Policy Management Editor.



New

Links

Display links in this location: corp.santo.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

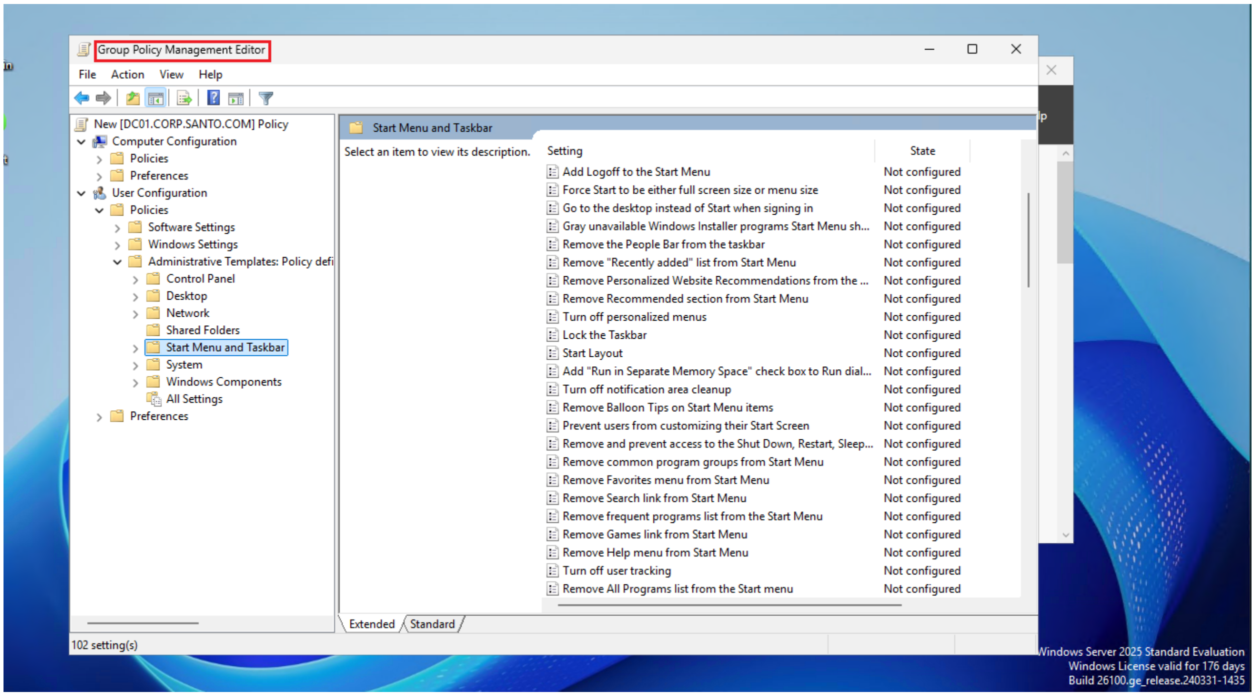
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

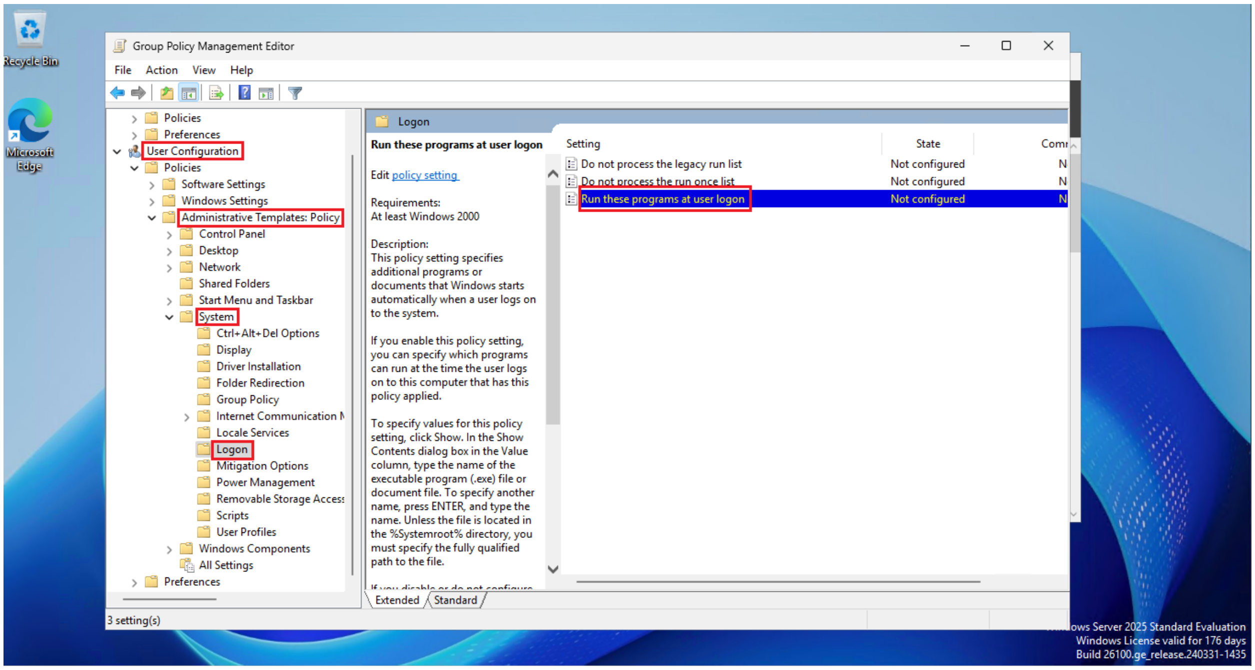
<none>

- Within the GPO Editor, there are numerous policies and configurations available to be set.



Setting	State
Add Logoff to the Start Menu	Not configured
Force Start to be either full screen size or menu size	Not configured
Go to the desktop instead of Start when signing in	Not configured
Gray unavailable Windows Installer programs Start Menu sh...	Not configured
Remove the People Bar from the taskbar	Not configured
Remove "Recently added" list from Start Menu	Not configured
Remove Personalized Website Recommendations from the ...	Not configured
Remove Recommended section from Start Menu	Not configured
Turn off personalized menus	Not configured
Lock the Taskbar	Not configured
Start Layout	Not configured
Add "Run in Separate Memory Space" check box to Run dial...	Not configured
Turn off notification area cleanup	Not configured
Remove Balloon Tips on Start Menu items	Not configured
Prevent users from customizing their Start Screen	Not configured
Remove and prevent access to the Shut Down, Restart, Sleep...	Not configured
Remove common program groups from Start Menu	Not configured
Remove Favorites menu from Start Menu	Not configured
Remove Search link from Start Menu	Not configured
Remove frequent programs list from the Start Menu	Not configured
Remove Games link from Start Menu	Not configured
Remove Help menu from Start Menu	Not configured
Turn off user tracking	Not configured
Remove All Programs list from the Start menu	Not configured

- For this project, we are focusing on Logon policies. This specific policy allows you to run programs automatically when a user logs on. Click on **'Run these programs at user logon'** to enable the setting and define the parameters.



Run these programs at user logon

Edit policy setting

Requirements:
At least Windows 2000

Description:
This policy setting specifies additional programs or documents that Windows starts automatically when a user logs on to the system.

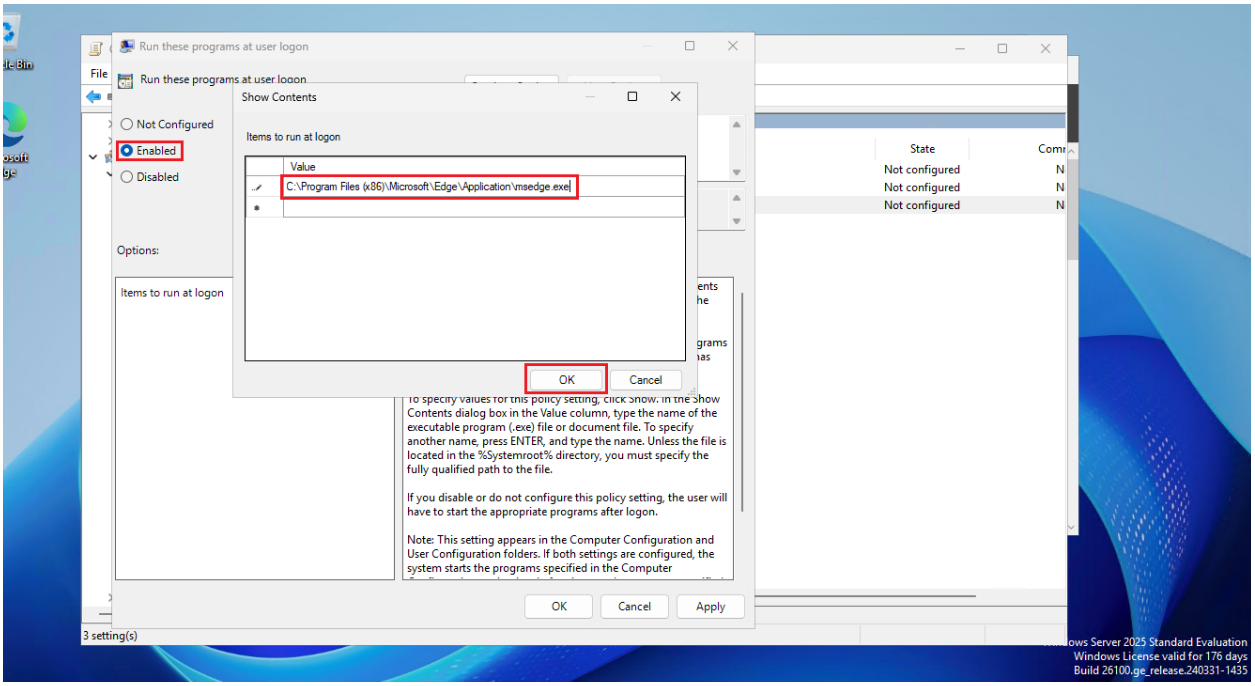
If you enable this policy setting, you can specify which programs can run at the time the user logs on to this computer that has this policy applied.

To specify values for this policy setting, click Show. In the Show Contents dialog box in the Value column, type the name of the executable program (.exe) file or document file. To specify another name, press ENTER, and type the name. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file.

If you disable or do not configure

Setting	State	Comm
Do not process the legacy run list	Not configured	N
Do not process the run once list	Not configured	N
Run these programs at user logon	Not configured	N

- After enabling the policy, add the executable path of the program you wish to run. For this example, I have chosen **Microsoft Edge;** click **'OK'** and then **'Apply**' to save the changes.


Run these programs at user logon
File
Show Contents
OK
Cancel
OK
Cancel
Apply
State
Not configured
Not configured
Not configured
3 setting(s)
Windows Server 2025 Standard Evaluation
Windows License valid for 176 days
Build 26100.ge_release.240331-1435

Run these programs at user logon

○ Not Configured
● Enabled
○ Disabled

Options:

Items to run at logon

Items to run at logon

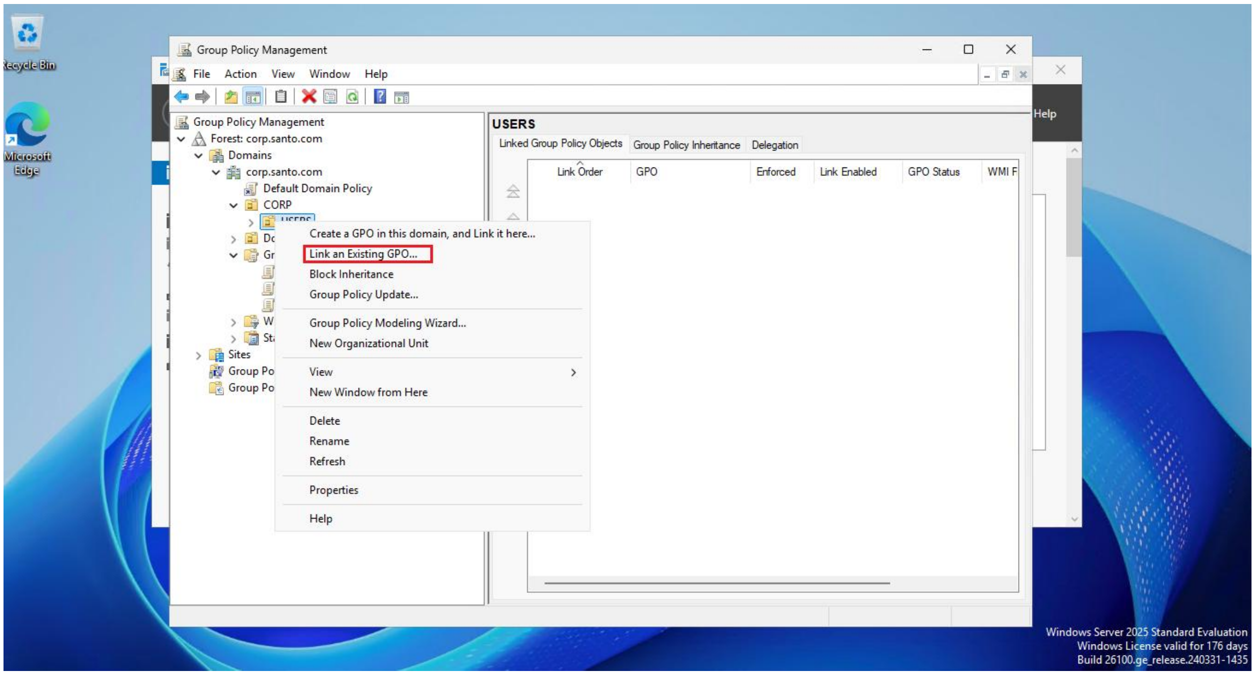
	Value
	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

To specify values for this policy setting, click Show. In the Show Contents dialog box in the Value column, type the name of the executable program (.exe) file or document file. To specify another name, press ENTER, and type the name. Unless the file is located in the %Systemroot% directory, you must specify the fully qualified path to the file.

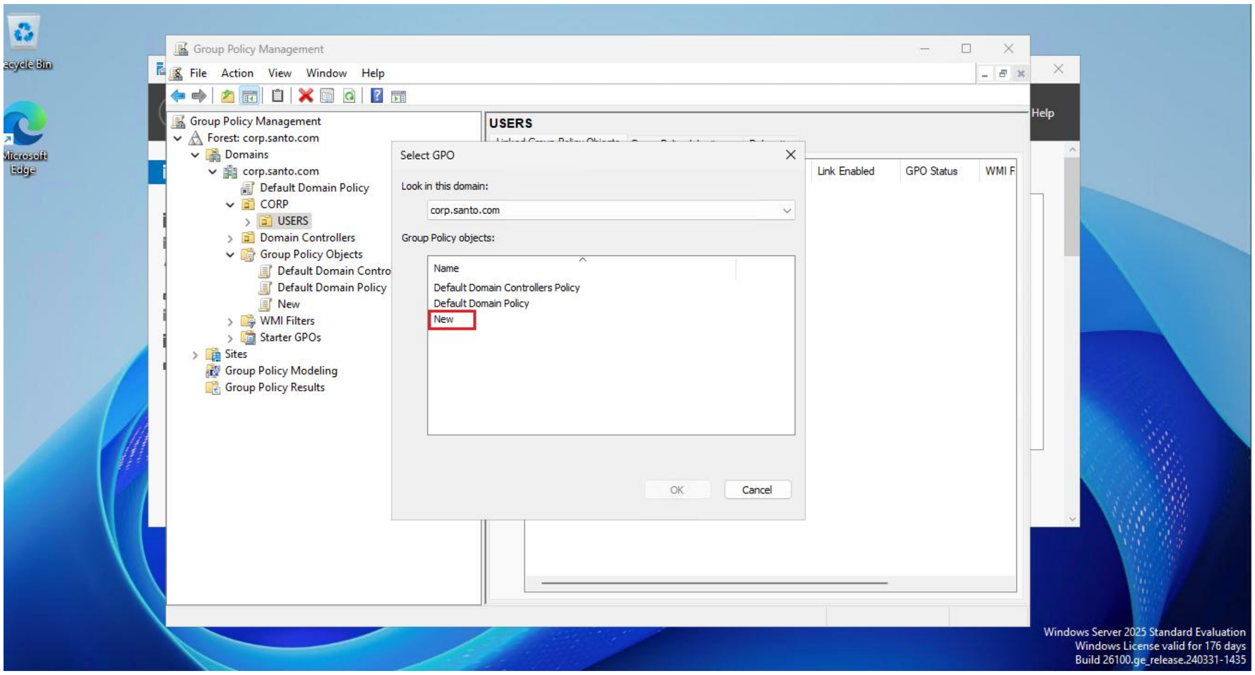
If you disable or do not configure this policy setting, the user will have to start the appropriate programs after logon.

Note: This setting appears in the Computer Configuration and User Configuration folders. If both settings are configured, the system starts the programs specified in the Computer

- To apply the GPO, right-click the **'USERS**' OU and select **'Link an Existing GPO…'**



- Select the name of the GPO; for this project, I am selecting the **'New GPO'** we just created.



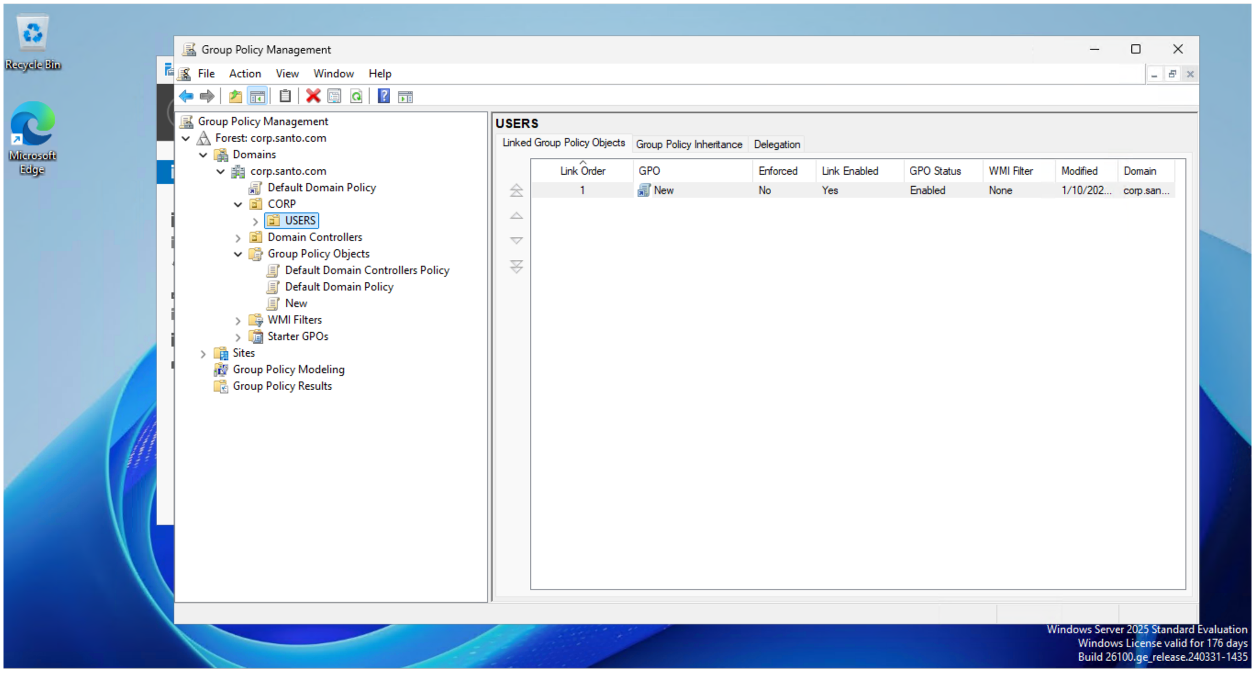
Select GPO

Look in this domain: corp.santo.com

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
New

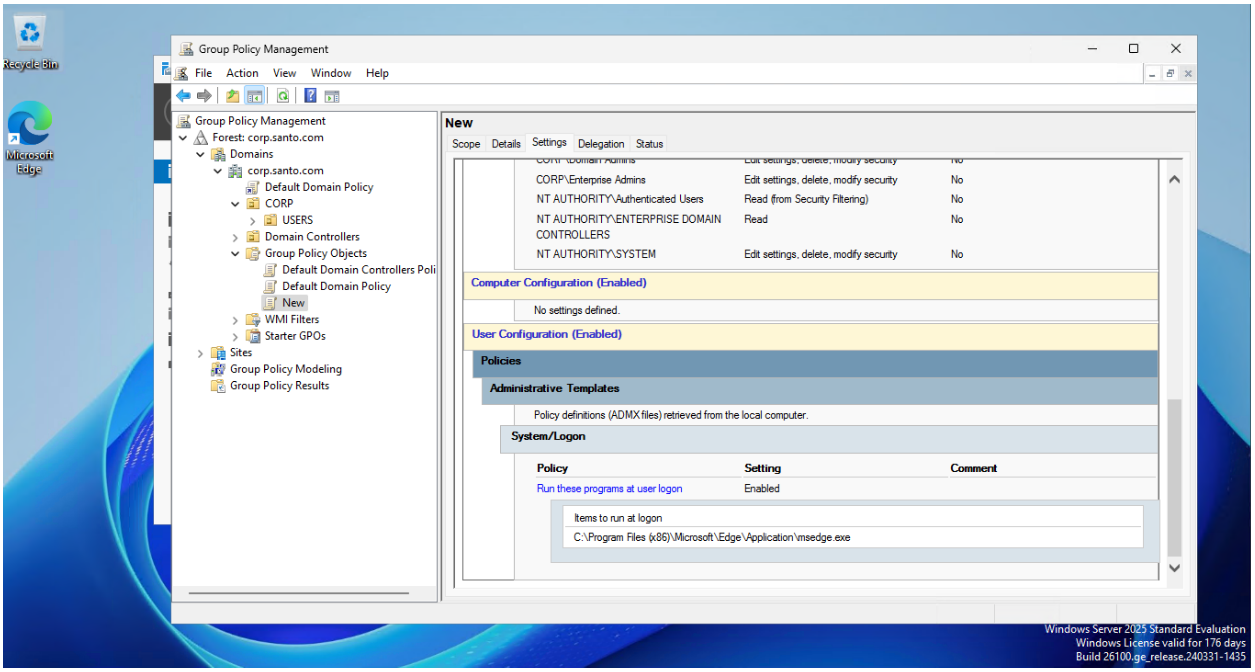
- Once the GPO is successfully linked, you will see it listed under the **'Linked Group Policy Objects'** tab in the right-hand pane.



USERS

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	New	No	Yes	Enabled	None	1/10/202...	corp.san...

- Click the new policy and select the **'Settings' tab;** this will confirm that the policy is enabled and display the configured rules.



New

CORP\Domain Admins	Edit settings, delete, modify security	No
CORP\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

No settings defined.

User Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

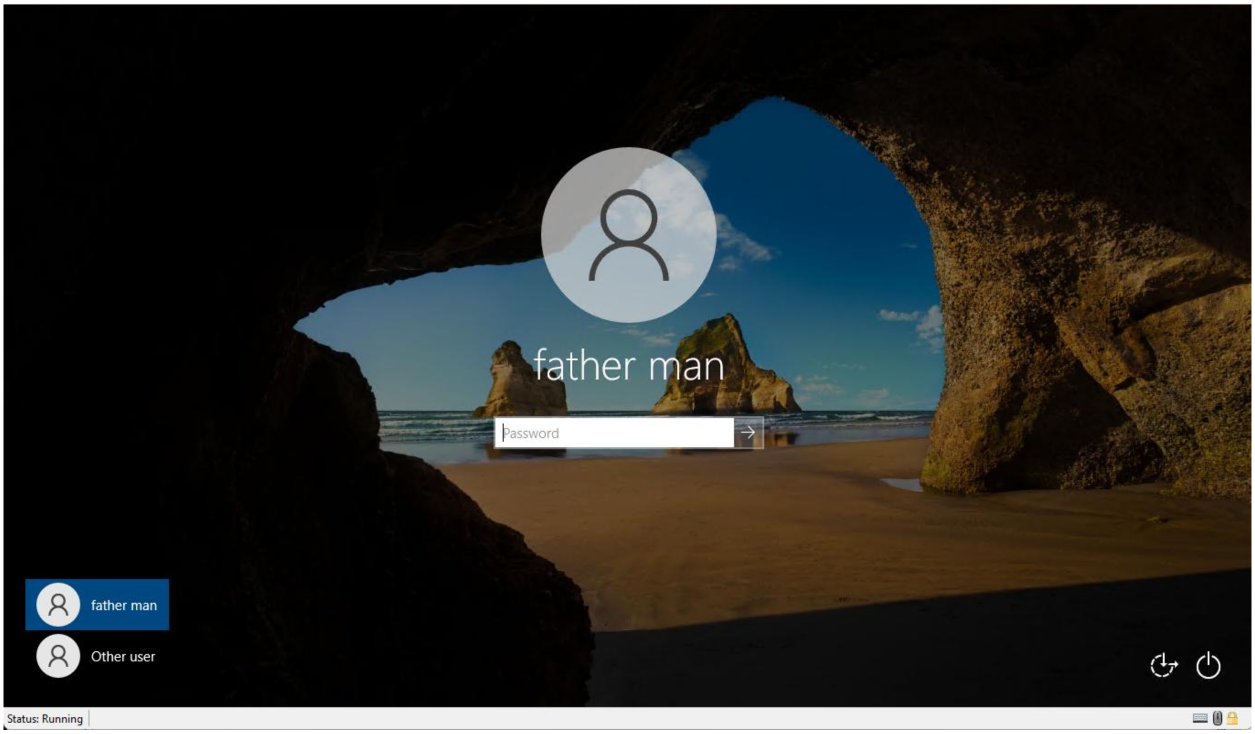
System/Logon

Policy	Setting	Comment
Run these programs at user logon	Enabled	

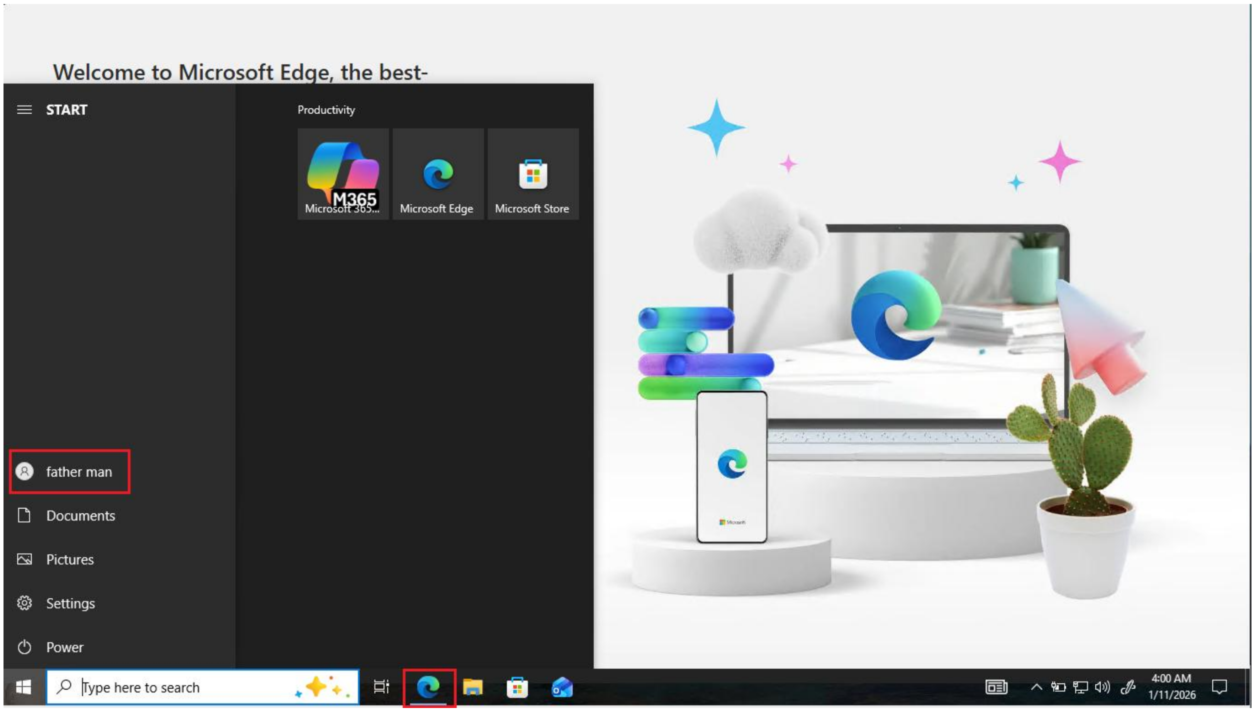
Items to run at logon

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

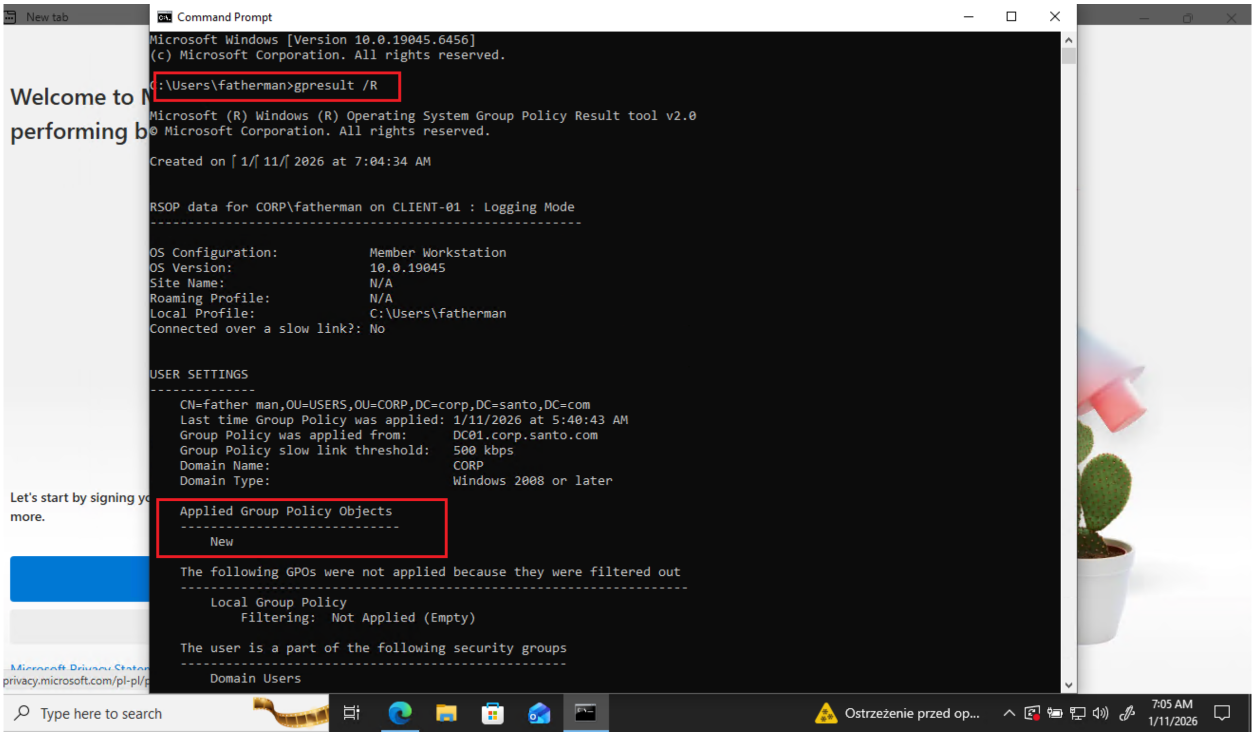
- To test if the GPO was successful, log on as the user **'father man,'** whom we previously located in **Active Directory Users and Computers**.



- After a successful logon, wait a few seconds and Microsoft Edge will start automatically.



- Running **gpresult /r** will show which GPOs have been applied.



```
Microsoft Windows [Version 10.0.19045.6456]
(c) Microsoft Corporation. All rights reserved.

C:\Users\fatherman>gpresult /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on ‎1/‎11/‎2026 at 7:04:34 AM


RSOP data for CORP\fatherman on CLIENT-01 : Logging Mode
---------------------------------------------------------

OS Configuration:            Member Workstation
OS Version:                  10.0.19045
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\fatherman
Connected over a slow link?: No


USER SETTINGS
-------------
    CN=father man,OU=USERS,OU=CORP,DC=corp,DC=santo,DC=com
    Last time Group Policy was applied: 1/11/2026 at 5:40:43 AM
    Group Policy was applied from:      DC01.corp.santo.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        CORP
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        New

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
```

Common Challenges and Troubleshooting Tips

Even with a "Magic Rule Book," sometimes things don't go as planned. Here are the most common challenges you might face and how to fix them quickly:

- **GPO Not Applying (The Rule Didn't Arrive):**
  - **The Fix:** Open the **Command Prompt** on the client machine and run gpupdate /force to manually pull the latest rules from the server.
- **Domain Connection Issues (The Client is Lost):**
  - **Symptoms:** You see errors like "The specified domain does not exist".
  - **The Fix:** Ensure the client's DNS is pointing exactly to the **Domain Controller's IP**.
- **Network Path Errors (The App is Missing):**
  - **The Fix:** Double-check that the file path for your application (like Microsoft Edge) is exactly correct and that the user has permission to "Read" files from that folder.
- **DHCP Failures (No Address):**
  - **Symptoms:** The client has a "169.x.x.x" address.
  - **The Fix:** Ensure the DHCP scope is **Activated** and the server is **Authorized** in the DHCP console.
- **Virtual Machine (VM) Lag or Boot Failures:**
  - **The Fix:** Check your computer's RAM levels and ensure you haven't assigned more memory to the VMs than your physical computer can handle.

Conclusion

In conclusion, Group Policy is a fundamental tool within Active Directory that empowers administrators to maintain a secure, organized, and efficient network through centralized control. By automating tasks like application deployment, such as our project's goal of auto-starting Microsoft Edge and enforcing consistent security standards, GPOs eliminate the need for repetitive manual configurations. Mastering these policies is essential for any IT professional, as they ensure that an entire organization can operate within a predictable and protected digital environment.