TOPIC: IMPLEMENTING GROUP POLICY

Objective:

To learn how to:

- Create, configure, and link Group Policy Objects (GPOs)

- Manage the scope of GPOs, including inheritance and security filtering

- Employ advanced Group Policy features such as loopback processing

- Troubleshoot and verify Group Policy application in a Windows Server 2016 Active Directory environment

---

Pre-requisites:

- Functional domain controller (LON-DC1) running Windows Server 2016

- At least one member server (e.g., LON-SVR1) and a client (LON-CL1) joined to the domain (RPSLAB.COM)

- Active Directory Domain Services (AD DS) deployed and configured

- Users and Organizational Units (OUs) set up as per lab scenario

- Administrative privileges on the domain controller and client machines


Procedure:

Exercise 1: Creating and Configuring GPOs

Task 1: Create and Edit a GPO

1. Open **Server Manager** on LON-DC1.

2. Navigate to **Tools > Group Policy Management**.

3. In the Group Policy Objects container, **right-click** and select **New**. Name the GPO (e.g., RPSLAB Standards).

4. Right-click the new GPO and select **Edit**.

5. In the Group Policy Management Editor, expand **User Configuration > Policies > Administrative Templates > System**.

6. Double-click **Prevent access to registry editing tools** policy, set to **Enabled**, and click OK.

7. Expand **Control Panel > Personalization**.

8. Double-click **Screen saver timeout**, set to **Enabled**, set timeout (e.g., 600 seconds), and click OK.

9. Double-click **Password protect the screen saver**, set to **Enabled**, and click OK.

10. Close the editor.
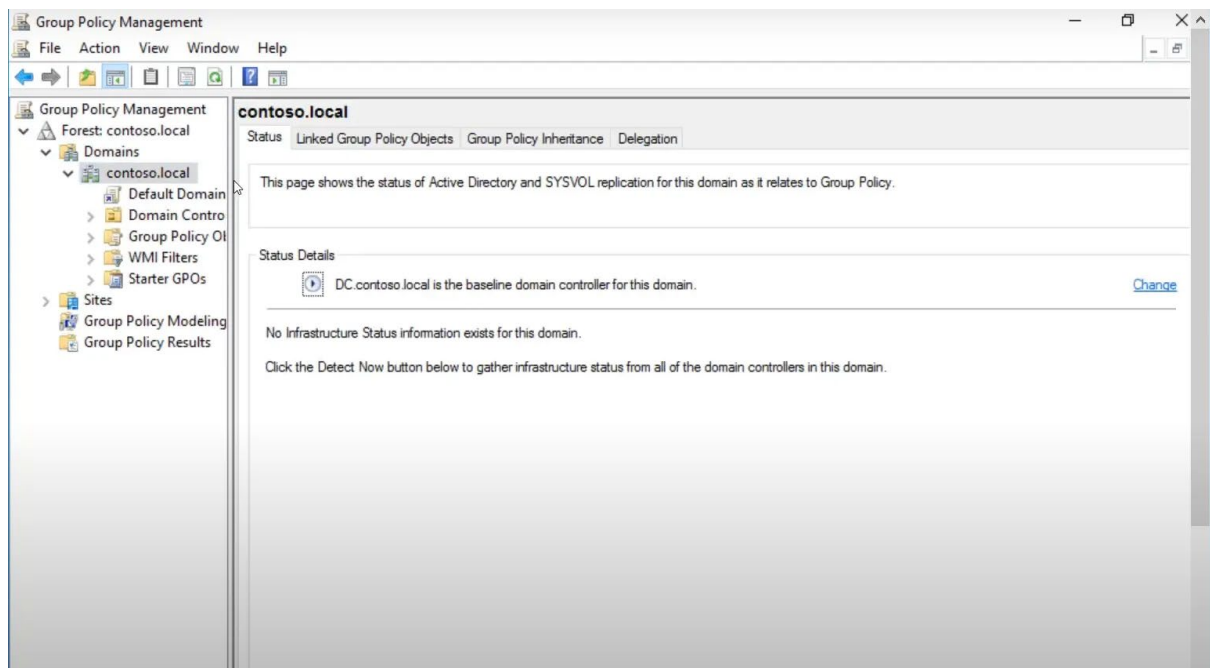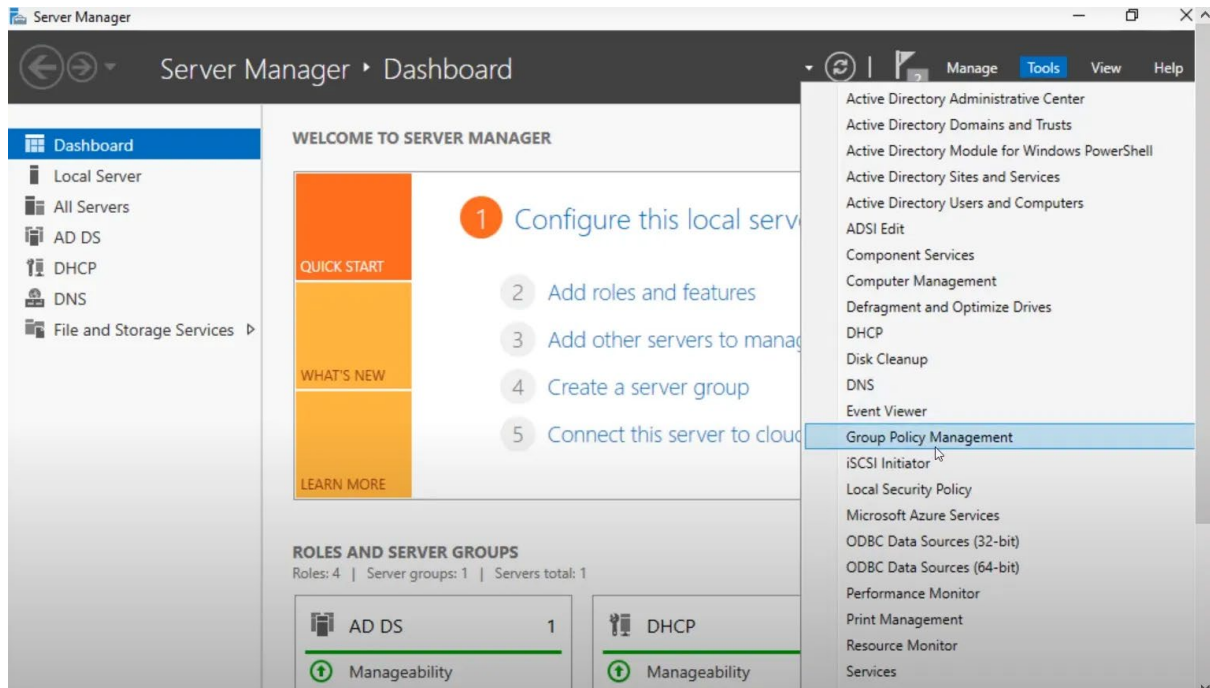
Task 2: Link the GPO

1. In Group Policy Management, **right-click** the domain (e.g., RPSLAB.COM) and select **Link an Existing GPO**.

2. Select the previously created GPO and click OK.

Task 3: View GPO Effects

1. Sign in to LON-CL1 as a domain user.

2. Access **Control Panel > Appearance and Personalization > Change screen saver**.

3. Verify screen saver settings are enforced and options are grayed out.

4. Run gpupdate /force in Command Prompt if changes aren't visible.

5. Attempt to run regedit—it should be blocked due to group policy.


Exercise 2: Managing GPO Scope

Task 1: Create and Link Required GPOs

1. In **Group Policy Management** on LON-DC1, right-click the target OU (e.g., Research).

2. Click **Create a GPO in this domain, and Link it here**. Name it Research Application Override.

3. Edit the new GPO. Set **User Configuration > Policies > Administrative Templates > Control Panel > Personalization > Screen saver timeout** to **Disabled**.

Task 2: Verify Precedence

1. In the **Research OU**, go to **Group Policy Inheritance** tab.

2. Confirm that Research Application Override GPO has higher precedence than the domain GPO.
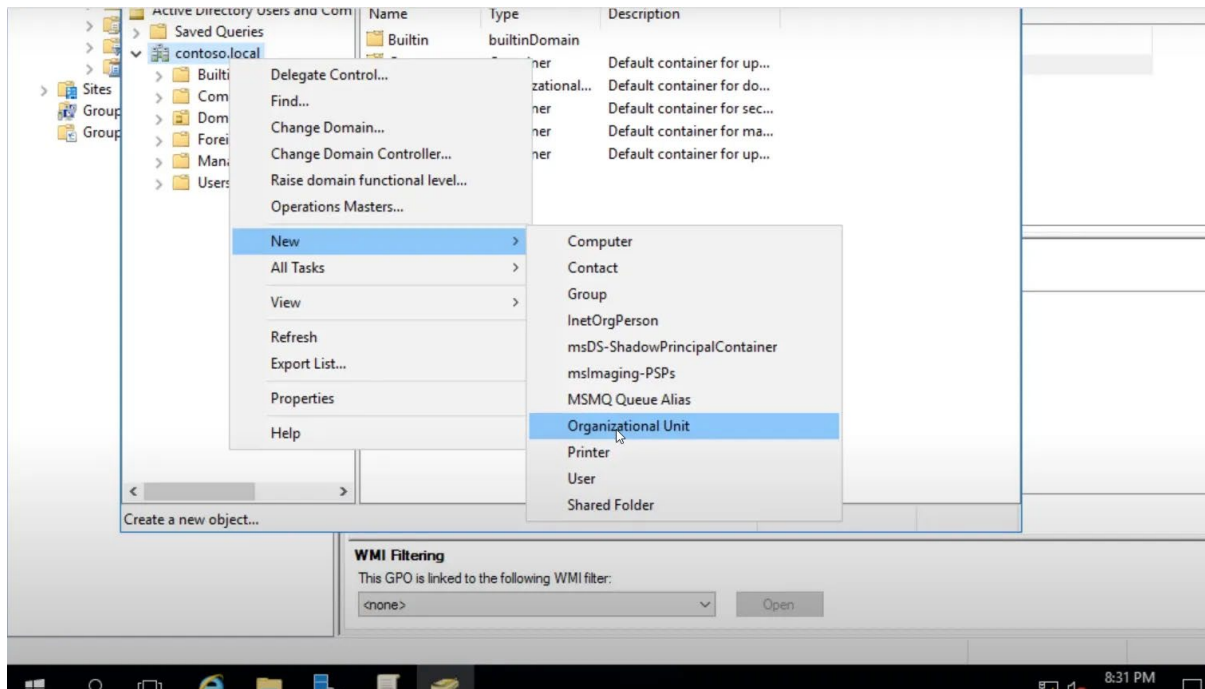
Task 3: Configure GPO Scope with Security Filtering

1. In the GPO properties, under **Security Filtering**, remove Authenticated Users.

2. Add the **Research** group so only its members are affected by the override policy.

Task 4: Configure Loopback Processing

1. Create a new OU for kiosks (e.g., **Kiosks**), then a sub-OU (e.g., **Conference Rooms**).

2. Within **Conference Rooms**, create and link a GPO (e.g., Conference Room Settings).

3. In this GPO, set **Screen saver timeout** to 7200 seconds.

4. In **Computer Configuration > Policies > Administrative Templates > System > Group Policy**, enable **Configure user Group Policy loopback processing mode** and choose **Merge**.

Exercise 3: Troubleshooting Group Policy

Task 1: Perform RSoP Analysis

1. On LON-CL1, update policies with gpupdate /force and note the system time.

2. Restart LON-CL1.

3. On LON-DC1, open **Group Policy Management Console**, run the **Group Policy Results Wizard** for LON-CL1 and the target user.

4. Review applied GPOs, settings, and winning policies.

Task 2: Analyze RSoP with GPResult

1. On LON-CL1, run gpresult /r (summary), /v (detailed), /z (most detailed), and /h:"%userprofile%\Desktop\RSOP.html" (HTML report).

2. Compare these results to the Group Policy Results Wizard output.

Task 3: Group Policy Modeling Wizard

1. On LON-DC1, use **Group Policy Modeling Wizard** to simulate effects of GPOs based on user and computer location.

Task 4: Review Policy Events

1. On LON-CL1, use **Event Viewer > Windows Logs > System**.

2. Filter for Group Policy events (IDs 1500–1503).

3. Use **Applications and Services Logs > Microsoft > Windows > Group Policy > Operational** for Group Policy refresh events.

4. Use GPMC **Status** tab to verify domain controller health and replication.
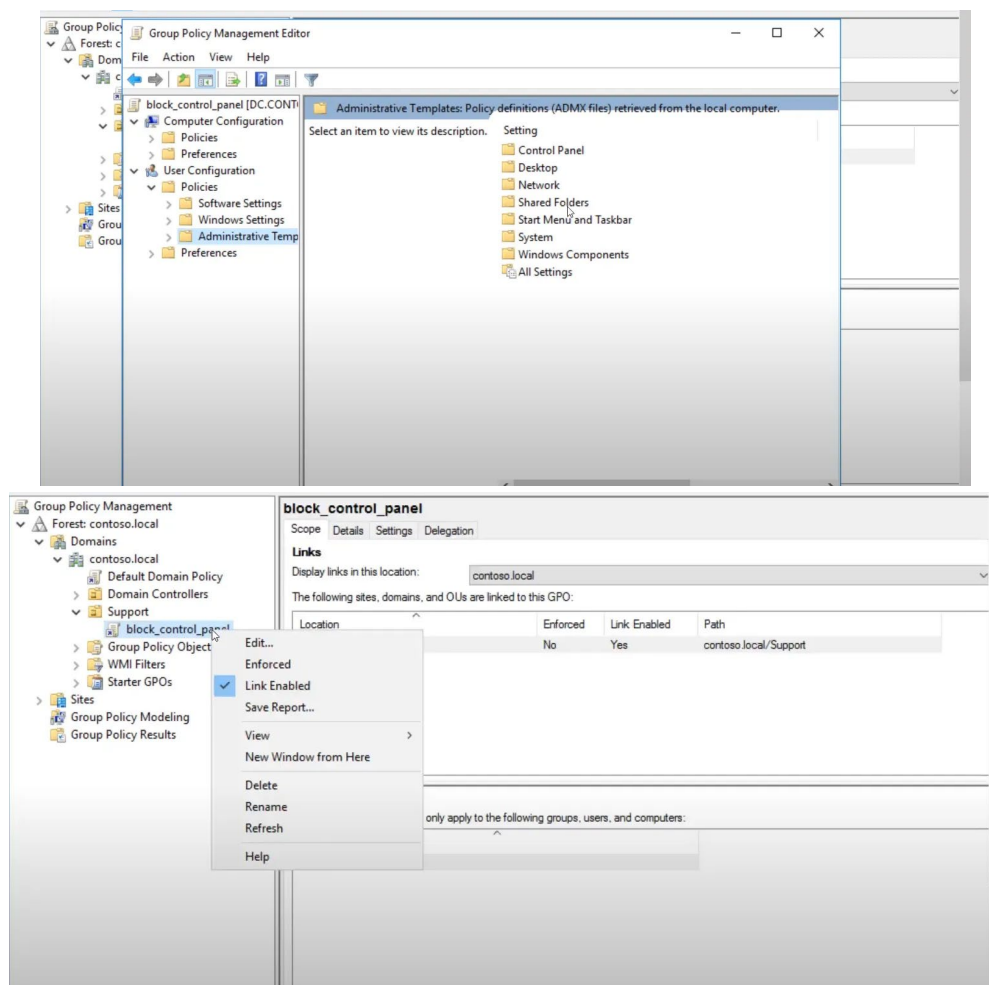
Exercise 4: Resolving GPO Application Problems

Scenario: User is not receiving correct GPO settings.

Steps:

1. Use **Group Policy Results Wizard** for affected user and computer.

2. Review denied GPOs and their reasons.

3. Confirm user is a member of the security group specified in the GPO's filtering.

4. Add the user to the correct group as needed.

5. Update policies and verify settings are applied.
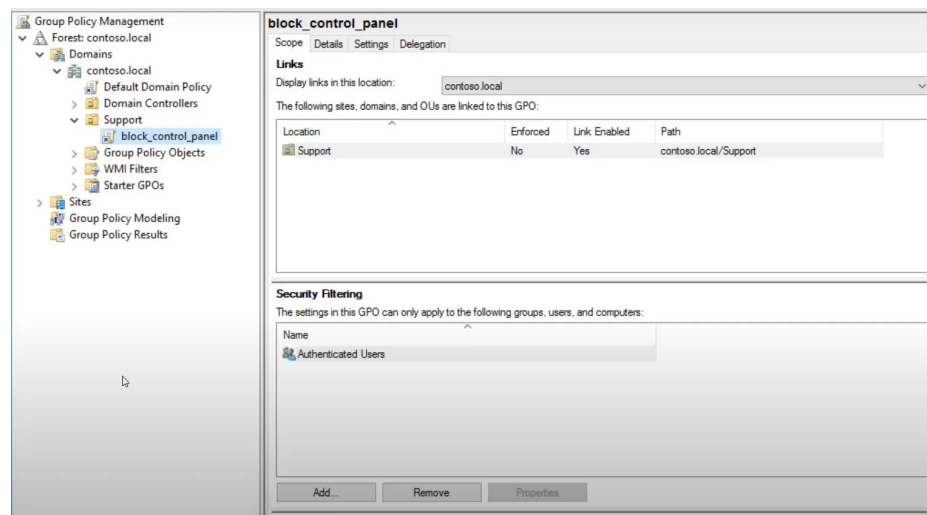
Conclusion:

In this lab, you learned to:

- **Create, configure, and link GPOs** for enforcing security and personalization settings.

- **Control GPO scope** through link order, inheritance, and security filtering, ensuring policies are accurately targeted.

- **Troubleshoot and verify policy application** using RSoP tools, GPResult, Event Viewer, and group membership checks.

- **Resolve common GPO issues**, such as misapplied policies due to security filtering or group membership.
  These skills are essential for centralized and secure management of Windows environments in an enterprise using Active Directory.