

10 min

✓ **Video:** Group Policy: Group Policy Object (GPO)
4 min

✓ **Video:** Group Policy Creation and Editing
12 min

✓ **Video:** Group Policy Inheritance and Precedence
7 min

✓ **Video:** Group Policy Troubleshooting
5 min

✓ **Video:** Group Policy Troubleshooting: Common Issues
6 min

✓ **Reading:** Supplemental Reading for Group Policy Troubleshooting
10 min

✓ **Reading:** Supplement Reading

Supplement Reading for Group Policy Troubleshooting Examples

Group Policy Troubleshooting Example

As an IT Support professional, you may need to troubleshoot Group Policy issues in Windows. The following are a few examples of the most common problems encountered when working with Group Policies. Included are suggested tips on how to troubleshoot these issues using tools you've learned about previously.

Scenario 1: Group Policy settings are not being applied

Imagine that you are an IT Support Analyst for an organization. You recently made changes to several settings on a Group Policy Object (GPO). However, the group policy changes do not appear to be active for the target end users or computers. You must troubleshoot to uncover the root of the problem and to fix it.

1. **Check the GPO Scope.** In the Group Policy Management utility, select the GPO that you recently changed and go to the **Scope** tab. Check the **Links** section to see if the GPO that you changed is linked to the correct Organizational Units (OUs). The linked OUs should contain the target computers (for computer-side settings) or target users (for user-side settings) for the changed GPOs.
2. **Check Security Filtering.** Below the **Links** section on the **Scope** tab, check the **Security Filtering** section. Make sure the correct computers and/or users intended for the changed GPO settings are specified in the security filters.
3. **Check Read and Apply permissions.** If any items have been added to **Security Filtering**, check the **Delegation** > **Advanced** tab to ensure the **Allow** option is checked for the **Read** and **Apply** permissions.
4. **Check the Group Policy Delegation.** On the **Delegation** tab, check the **Groups and users** section for **Allowed Permissions** for the GPO. This list contains the groups and users that have the authority to edit, delete, and modify security for the GPO. Ensure that these settings are desired for your environment and no unauthorized users or groups can edit GPO settings.
5. **Enable/disable User or Computer configurations.** On the **Details** tab of the GPO, check the **GPO Status** to ensure the selection matches your intended setting. The options are:
 - **All settings disabled:** GPO will be inactive.
 - **Computer configuration settings disabled:** Any Computer configurations in the GPO will be inactive.
 - **User configuration settings disabled:** Any User configurations in the GPO will be inactive.
 - **Enabled:** All GPO configurations will be applied (default).
6. **Check the GPO Policy Process Order (LSDOU).** The GPO process order from first applied to last is **Local GPOs**, **Site GPOs**, **Domain GPOs**, then **OU GPOs**. Each GPO policy overrides the previous GPO setting in this **LSDOU** process order. To change the default order, select the affected OU in the Group Policy Manager and go to the **Linked Group Policy Objects** tab. The **Link Order** enumeration for the GPOs is listed in reverse order, meaning the GPO with the highest **Link Order** number is applied first and the GPO with the lowest number (1) is applied last. The number 1 indicates the GPO has the top-ranking priority, as it will override the previous GPO settings where the settings overlap. You can change the order that the GPOs are applied using the up and down arrows to the left of the list.
7. **Ensure target GPO to OU links are enabled.** GPO to OU links are technically shortcuts, which can easily be enabled or disabled. Check to ensure that the **Link Enabled** setting has not inadvertently been turned off.
8. **Check if an upstream GPO is set to Enforced.** An upstream GPO is a GPO linked to an OU that has a higher LSDOU priority than a downstream GPO. If an upstream order of applying settings is enforced, a lock will appear on the link icon. Evaluate if enforcement is overriding the desired GPO settings.
9. **Check if the affected OU is set to Block Inheritance.** The default Group Policy inheritance for OUs, which is applied hierarchically to nested objects, can be blocked. **Block Inheritance** is indicated in the Group Policy Manager as a blue exclamation point icon on the affected OU. If you believe this setting might be the cause of the GPO changes not propagating, right-click on the OU and select **Block Inheritance** from the menu to toggle it off/on. Note that **Block Inheritance** will not affect **Enforced** GPOs.
10. **Check if loopback is enabled.** If **loopback** is enabled, the user-side settings that belong to the computer's OU will override any computer-side settings in the same OU. If the OU's computer-side settings need to have priority over the user-side, set the **user Group Policy loopback processing mode** to **Disabled**.
11. **Check MI or WMI filters.** Check to see if Windows Management Infrastructure (MI) or Windows Management Instrumentation (WMI) filters are set on the changed GPO. MI or WMI filters might be used to apply a policy to a subset of objects. The MI or WMI query may need to be edited to ensure the target objects for the changed GPO are not excluded by the filter.
12. **Ensure your expectations for the GPO settings match its actual purpose.** If the troubleshooting steps listed

above do not solve the Group Policy problem, research the GPO settings you are using. It is possible that your expectation for a setting may not match what the setting actually does.

Scenario 2: GPO settings are not correct.

- **Edit incorrect GPO settings.** If there are any problems found with GPO settings, open the Group Policy Management interface and edit the GPO:
 - **Step 1:** Select the GPO with the incorrect settings.
 - **Step 2:** Right-click the GPO, and then click Edit.
 - **Step 3:** Edit the settings using the appropriate instructions listed in Scenario 1 of this article.

Scenario 3: The user can't authenticate into the Active Directory domain

- **Check Active Directory (AD) infrastructure.** Investigate if the user or computer cannot locate the domain controller. Domain controller and replication problems in AD can prevent GPOs from functioning correctly.



Key takeaways

Outline of troubleshooting steps for GPO settings that are not being applied:

1. Check the GPO Scope.
2. Check Security Filtering.
3. Check Read and Apply permissions.
4. Check the Group Policy Delegation.
5. Enable/disable User or Computer configurations.
6. Check the GPO Policy Process Order (LSDOU).
7. Ensure target GPO to OU links are enabled.
8. Check if an upstream GPO is set to Enforced.
9. Check if the affected OU is set to Block Inheritance.
10. Check if loopback is enabled
11. Check MI or WMI filters.
12. Ensure your expectations for the GPO setting match its actual purpose.

Resources for more information

For more information on Group Policy troubleshooting, please visit:

- [Working with Group Policy Objects using GPMC](#)  - Microsoft's guide to the Group Policy Management Console and managing GPOs.
- [Troubleshooting: Group Policy \(GPO\) Not Being Applied to Clients](#)  - Troubleshooting guide for GPOs. Includes screenshots of various settings in the Group Policy Management Console with descriptions of how each setting works.

✓ Completed

Go to next item

 Like  Dislike  Report an issue