

Group Policy troubleshooting

Find the applicable policy, the processing instance and the reason a setting differs.

Start in the affected context

Record the computer, affected user, domain/OU, expected setting and UTC time. Separate User Configuration from Computer Configuration. Compare a healthy machine or user. Confirm that the setting is managed by a domain GPO rather than MDM, a script or a local preference.

Capture the resultant policy

```
gpresult /scope user /r
```

Run in the affected user session to see a user-policy summary.

```
gpresult /scope computer /r
```

Inspect computer-policy results; an elevated prompt may be required.

```
gpresult /h .\gp-report.html
```

Write an HTML report in the current writable folder. Review applied and denied GPOs and the winning setting.

Check scope and precedence

Confirm the correct site, domain and OU links; link status; enabled user/computer sections; security filtering and permissions; WMI filter; and inheritance. Normal processing runs Local > Site > Domain > parent OU > child OU. Link order, Enforced and Block Inheritance can change which setting wins.

Check loopback when relevant

Loopback uses the computer location to influence user policy. Merge and Replace behave differently. Check this on shared workstations, kiosks and session hosts before assuming that user OU links alone determine the result.

Read the processing evidence

Start with Group Policy errors and warnings in Windows Logs > System. Then inspect Applications and Services Logs > Microsoft > Windows > GroupPolicy > Operational. Correlate the same processing instance using its ActivityID, user/computer context and timestamps.

Find the failing dependency

Read the full event text, error code and affected client-side extension. Check DNS/DC discovery, access to SYSVOL/NETLOGON, replication and connectivity when the evidence points there. Distinguish a denied GPO from a GPO that applied but did not configure the expected setting.

Refresh only after collecting evidence

```
gpupdate /target:user
```

Apply changed user policies in the current context.

```
gpupdate /target:computer
```

Apply changed computer policies.

This changes policy state. /force reapplies all settings; it is not a substitute for diagnosing scope or access. Some settings need sign-out or restart. Plan that separately; do not add /logoff or /boot casually. A refresh creates a new processing ActivityID.

Keep a useful handover

Save the report, affected setting, GPO name/GUID, ActivityID, full errors and a before/after comparison. Reports can contain internal names and user information. Share only the material needed for the investigation.