Group Policy

Our Group Policy auditing solution can help you monitor every change made to your Group Policy objects in real time. You can easily track any changes made to security setting policies, password policies, software restriction policies and much more with their before and after values.



Group Policy auditing.

Get detailed information on the changes taking place to Group Policy Objects with who, what, when and where values.



Configuration reporting.

Report on the current state of Group Policy Objects and their settings to quickly spot deviations from the norm.



Real time alerting.

Respond to Group Policy changes as they happen with either real time or threshold based alerts.



Pre-Defined reporting.

Pre-defined reports for common security and compliance concerns, including PCI, HIPAA, GDPR, CCPA, SOX and more.



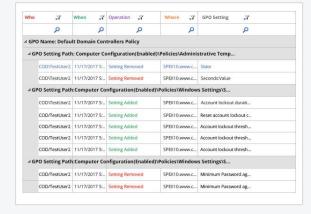
Filter, search and sort.

Overcome the limitations of native auditing and get the information you need quickly and easily.



Automate response.

Automate the execution of custom scripts to take action when a specific alert is generated.

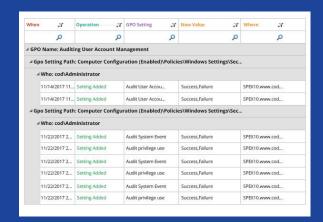


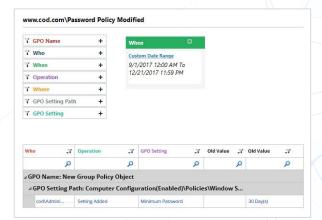
Track all modifications made to Group Policy objects.

Our solution enables you to track all modifications made to Group Policies such as created, deleted, modified, renamed, linked and more. Whether a group policy is applicable only an organizational unit or entire domain, we help you audit it. The audit data is displayed in the predefined audit reports, which you can create a long-trail of the changes to identify the anomalies in the modification trend.

See changes made in security setting policies.

Security group policies include the policies for IP security, network settings, auditing, registry, wireless networking, event log and more. These policies come in handy to ensure the security settings in the IT environment. Any unwanted or unplanned change can damage the IT security of the organization.



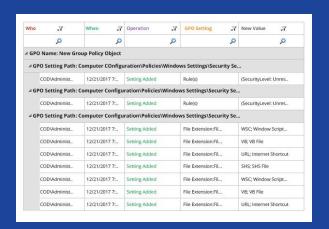


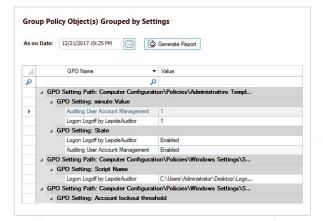
See all changes in password policies.

Numerous password policies are enabled and configured to maintain IT security. Any unwanted changes in such policies can lead to a security breach. Lepide Group Policy Auditor tracks such changes, records them, shows them in audit reports and generates real-time alerts to notify you before it is too late.

Audit changes in software restriction policies.

Software restriction policies are used to block users from installing unwanted software applications; including ransomware or malware. If any such policy is modified, the chances for installation of unwanted applications, especially a malware, are increased greatly. Our Group Policy Auditor tracks all changes made to software restriction policies and notifies you in real time.



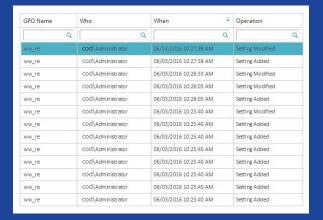


See the state of Group Policy objects on any selected date.

Lepide GPO Auditor periodically captures backup snapshots to save the state of Group Policy Objects. In addition to restoring entire Group Policy Objects, our solution also generates reports to show the state of Group Policies on selected dates. It shows a historical view of common settings, delegation settings, values, link status and other information regarding the group policies.

Securely delegate the viewing of audit reports.

To allow for separation of duties, we also enable IT teams to determine which reports could be delegated to which users. The administrator can create accounts for different users, who will then be able to logon at a secured based Web Console to view their authorized set of reports. No reports other than delegated ones will be displayed.



Start your 20-day free trial of Lepide today!

Start free trial