Group Policy Auditing in the Enterprise
# Table of Contents

1. What Is Group Policy Auditing?  
2. Why Is Group Policy Auditing Important?  
   2.1 Group Policy Auditing: A Real-World Example  
   2.2 Group Policy Auditing to Reduce Risk  
   2.3 Group Policy Auditing to Improve Security  
   2.4 Group Policy Auditing to Sustain Compliance  
   2.5 Group Policy Auditing to Improve Manageability  
3. Required Features for Group Policy Auditing  
   3.1 Compensation for Native Auditing Deficiencies  
   3.2 Automatic Data Collection  
   3.3 Efficient and Centralized Data Storage  
   3.4 Scalability  
   3.5 Advanced Reporting Capabilities  
   3.6 Additional Considerations  
   3.7 SIEM, IT Governance, Risk Management and Group Policy Auditing  
4. Netwrix Approach to Group Policy Auditing  
5. About Netwrix Corporation  
6. Additional Resources
Why Is Group Policy Auditing Important?

Group Policy Auditing: A Real-World Example

The importance of Group Policy auditing is best illustrated by a real-world example. Consider a company that uses Group Policy to establish both a minimum password length of 12 characters and time between required password changes set to 90-days. This use of Group Policy has been implemented to meet specific security standards as required by multiple regulations.

A junior administrator, while troubleshooting an account lockout problem for an OU containing accounting and finance staff decides to modify both of these password settings so as to reduce helpdesk calls and ease the burden on end users, shortening the required password length to 3 characters and extending password age to 360-days. This makes end users happy as they no longer need to remember a lengthy password and no longer need to worry about having to change it for nearly a year.

This modification to Group Policy for this OU has now introduced security risks and the environment is no longer compliant with regulations. To make matters worse, no change auditing procedure exists to review and archive these changes making it highly improbable for someone to recognize the changes and correct them. Four months later, a major accounting error is discovered.

During the investigation, IT determined who made the error, and when, however, the employee in question was on vacation and it is now believed that another staff member compromised the account from a different machine and made the change to make it look like another employee had caused the error. As a result, the IT department also learns through manual examination that the Group Policy used to secure the passwords had been changed and contributed to the breach causing embarrassment though uncovering the need to audit Group Policy changes such as these. This costs the organization numerous hours of troubleshooting and damage as a result of the accounting error.

Situations like this are both rare and completely avoidable. Without GPO auditing, there was no way for the company to protect itself. Errors can occur and that is to be expected, however, without a proper Group Policy auditing tool in place to confirm and track Group Policy changes in Active Directory, the company suffered serious harm. Monitoring Group Policy change is important because without it, an organization is subject to greater risks and cannot as easily maximize the potential of GPO policies.

Group Policy Auditing to Reduce Risk

Group Policy auditing provides accountability thereby reducing risk through detailed collection and analysis of GPO change information. A policy setting made today may not be appropriate at some point in the future. GPO auditing is the vehicle by which changes made to GPOs controlling users and computer environments today can be measured against predetermined risk factors and mitigated accordingly.

Establishing risk factors is the single most important step in securing any IT environment. Doing so will ensure that everyone involved from end users to senior management understands what is at risk. This creates a conscious awareness of all things critical to sustaining normal business operations. Regularly revisiting these risk factors will serve to adjust them as needs and conditions change.
Once the risk factors have been identified, the next step is to secure them. For Group Policy, rules and controls limit rights to environment variables and interactive behaviors for both users and computers. Effectively managing every aspect of user interaction with the environment reduces risk while granting the appropriate access needed to perform job responsibilities.

Change may sometimes have unpredictable results, one of which is unintentionally creating conditions that increase calls to the help desk. Group Policy auditing provides actionable and historical forensic information to ensure risk factors are managed appropriately while delivering consistent rights and controls to operationally diverse end-user populations.

**Group Policy Auditing to Improve Security**

Accountability will always keep the honest users and administrators honest, however, internal threats pose a more immediate danger than those external to the organization because of trust. Change auditing provides the ability to establish a robust check-and-balance record for all changes to Group Policy. Security improvements through the use of Group Policy are most often reactionary.

Flaws and holes are discovered after the fact and the reason for this is that without auditing Group Policy activity, there is no way to predict and react to how a change will impact the environment. Environments that rely on tickets, or other change approval processes may still experience security problems if the information submitted is later found to have been inaccurate or intentionally misleading. One of the easiest ways to improve security through Group Policy is to extract and review change information regularly.

**Group Policy Auditing to Sustain Compliance**

Regulations such as SOX, PCI, FISMA, HIPAA each have their own detailed explanations of security standard practices including what exactly needs to be tracked and recorded. These regulations exist to establish (IT) change auditing standards to protect both businesses and consumers. At the end of the day, these regulations and their enforcement strive to confirm the organization is securing, recording and monitoring change events that permit access to sensitive information such as banking information, social security numbers, and health records.

Additionally, regulations exist to establish a minimum set of security standards as they apply to user interaction with the environments in which they operate including numerous aspects that are controllable through Group Policy security settings. Some examples include: password length, complexity, reusability, permitted login times, installation of applications and access to removable media.

Demonstrating compliance is an exercise in presenting this information to auditors upon request and to the level of details as is interpreted by the law or standard and subject to the individual auditor’s discretion. Auditing Group Policy provides the Who, What, When, and Where information most frequently requested by auditors and almost equally important is the need to store this information for sometimes up to 7 years or more to be considered compliant. For Group Policy, this is extremely difficult and an entirely manual process with native functionality and
thus gives rise to the demand for additional tools, especially in large environments with multiple levels of IT administration.

**Group Policy Auditing to Improve Manageability**

Making changes to Group Policy is performed easily when provided sufficient access. The consequences of changes however require thought and planning to avoid problems. Even if a lab environment is used to test changes, unexpected results can still occur, making the need to monitor Group Policy change essential to effectively managing how Group Policy controls user and computer behaviors.

Group Policy auditing offers the opportunity to see changed setting names with before and new values that can greatly improve an administrator’s response times to recover from changes that result in harm or that introduce unnecessary risks.

Additionally, by maintaining a historical record of changes over time, further analysis can be used to uncover less obvious problems or inefficiencies. Being able to make changes is necessary to adjust to meet business and operational goals, however, the ability to look back at the impact those changes had is the difference between ensuring a consistent, stable and safe environment for users and loosing visibility and control over established policies for users and computers.

The ease with which changes are made can create a false sense of security with regards to the impacts those changes may bring and thus reinforces the need to have Group Policy auditing solution to improve overall enterprise IT manageability.

**Required Features for Group Policy Auditing**

Group Policy auditing is the process of gathering information, reporting the information, analyzing the information, taking action and evaluating the results of those actions, to ensure restrictions and controls established by Group Policy are consistently enforced. Windows natively has the ability to output audit information. This information however is stored local to each domain controller and is not centrally aggregated.

Reporting is also unavailable for audit data making the collection and reporting steps of change auditing for Group Policy changes difficult and time consuming. There is also a risk of losing audit data if event log settings are not set properly to handle the volume of information logged and running out of disk space on domain controllers if too much information is being captured and not cleared after it’s been archived properly.

Native events will lack object setting names as well as before and after values, even in Windows 2008 R2. Once the available native information is analyzed by an administrator experienced with system events and messages, the interpretation then would need to result in a decision to act or, accept the change and information as having met the intended goal and did not result in a deficiency or unacceptable compromise.
Evaluating using native Group Policy functionality requires the same activity as collecting the information and thus requires similar investments in time. Combine these factors and the result is native change auditing is not feasible except for small to mid-sized environments. The following information is a collection of must-have Group Policy auditing features. Additional deployment considerations are provided as well.

**Compensation for Native Auditing Deficiencies**

Native Windows auditing capabilities are only a starting point. Without them, auditing efforts will risk incompleteness and compliance. While built-in auditing capabilities provide an abundance of valuable information, it is deficient in two specific areas: Setting names and before/after values. To comply with regulations like HIPAA, SOX, PCI, and FISMA, before and after values should be captured as well as setting names to aid in overall compliance efforts. This information is unavailable through Windows and even Windows 2008 R2 audit information.

A clear picture of setting change activity must include those setting names as well as before and after values in order to sustain compliance. Furthermore, having this added information makes the data actionable, greatly increasing its value and thus are must-have attributes to Group Policy auditing.

**Automatic Data Collection**

In order to efficiently audit Group Policy changes, the process must be automated through scripting or a third-party tool. Without it, collecting the information in a timely manner is not feasible. This is especially true as the size of the organization will have a great impact on the raw volume of information collected making it even more challenging to track GPO changes.

Special steps must also be taken on servers and domain controllers throughout the environment to facilitate auditing of the information which is by default not enabled. Additional scripting and third-party tools may also be employed to pre-configure systems in preparation of collecting event data. Furthermore, if audit data is not collected regularly, there is a risk of losing this information due to event log automatic overwrites or disk space issues. This is an important required feature to change auditing because without it, timely auditing is not feasible.

**Efficient and Centralized Data Storage**

Automation of any kind typically requires additional resources and may negatively impact system performance which can lead to bigger problems. For this reason, it’s important that the impact of the method employed to automatically collect data is minimal. Furthermore, storage of data must also be a consideration during implementation.

While it is possible to store event and audit data exclusively on the local system where the events are taking place, the preferred method will be to centralize the information. This will lead to numerous additional benefits over time as the need to analyze and report on this information becomes part of daily routine for the IT administrator or group responsible.
Collection of information must also be reliable. Occasionally, each piece of the change auditing system should have a periodic check to ensure information is consistent when collected. The most advanced methods of reliably collecting this information will also have the ability to pre-screen data and filter for only essential data and the ability to compress this information to further add to overall efficiency.

During collection, preference should be given to methods that leverage the existing Windows Event Log and audit information as opposed to injected agents or modified core system code for event extraction. Doing so will eliminate any potential system stability issues or future incompatibility problems. Relying solely on event log data introduces problems because this information is frequently incomplete.

To completely understand an event, information from all sources involved must be aggregated and analyzed as a whole. Securing this information for short and long-term storage is also an important consideration and thus best-practices for securing audit data should be included pre-deployment such that no single power-user has access to or the ability to delete or tamper with information. Access to this information should be heavily restricted and monitored.

**Scalability**

Auditing Group Policy changes must be scalable to adjust to the environment without the need for dramatic or drastic steps. Implementation and ongoing use of GPO change auditing will be simplified when no additional software or extensive reconfigurations are required to accommodate changes within the organization.

GPO auditing should keep pace with all granular changes as the overall topology of the network, domain controllers and Active Directory changes to ensure consistent optimal Group Policy control to best serve end-users and be administered by IT and help desk staff.

**Advanced Reporting Capabilities**

Once data collection is automated, reliable and stored securely, change auditing for Group Policy can assume a proactive posture. Advanced reporting is necessary to provide IT administrators, management and auditors with summarized information on any aspect of the Group Policy Object implementation and for any time period. Without the ability to produce clear information on change history for day-to-day modifications to GPOs, such as, who changed Group Policy or if there has been a deleted GPO, sustaining compliance will be impossible and many opportunities will be lost to better secure the environment.

For Windows environments, using SQL to store data and leverage Advanced Reporting Services are obvious choices for storing and reporting on data. SQL Server with Advanced Reporting can be downloaded for free from Microsoft. The ability to customize ad-hoc and predefined third-party reports will accelerate an effective change auditing implementation by saving time and providing configuration options to suit the majority of needs.

Using reports on a daily basis ensures complete visibility over the entire IT infrastructure providing opportunities to improve security and sustain compliance. Additional reporting services including e-mail subscription capabilities
and will also add to the impact advanced reporting will have on overall systems management effectiveness. Once established, advanced reporting will be the main driver behind sustained Group Policy auditing success and will become an important part of day-to-day management of the IT environment.

Additional Considerations

Preferred solutions (and providers) should offer plug-in or add-on modules and software to help form a cohesive and comprehensive management suite to make the most of change auditing. Some additional types of systems may include firewalls, switches, database servers, SANs, storage appliances and of course Microsoft technologies such as Exchange and SharePoint and especially Active Directory.

SIEM, IT Governance, Risk Management and Group Policy Auditing

These common buzzwords appear frequently when discussing security and change auditing and represent a broader view of enterprise IT management methodologies.

SIEM, which stands for Security Information and Event Management is related to change auditing, however, with some important differentiators. SIEM encompasses real-time analysis of security alerts and events generated through the entire enterprise, extending to all applications and devices at all corners of the organization.

Change auditing is a critical information collection and reporting layer to overall SIEM objectives and must have a high level of interoperability with SIEM systems and services in order to achieve maximum effectiveness. SIEM implementations range from in-house, customized systems to massive modular deployments providing management capabilities for nearly all IT resources in an environment.

IT Governance is a term often used to describe the overall mission of an IT organization within the broader context of the organization as a whole. It’s meant to provide a means by which core activities and services provided by IT align with overall organizational directives and goals.

Risk Management is a term found more and more frequently in press and publications to challenge the status of security for appropriately describing how organizations approach keeping their resources stable and secure. More recently, the increased visibility of mobile devices and cloud computing as part of an organization’s IT strategy present new challenges to traditional models of thought on security and how best to provide that in an increasingly mobile world where borders to IT infrastructure have blurred greatly.

Keeping these new terms in mind while approaching Active Directory change auditing will help keep IT objectives in line with organizational objectives and needs as requirements change.
Netwrix Approach to Group Policy Auditing

The Netwrix approach incorporates all the necessary features for achieving effective Group Policy auditing in a software solution. The Group Policy Auditing feature within Netwrix Auditor for Active Directory provides tracking of changes made to the Group Policy Objects across the entire organization. Netwrix Auditor generates audit reports that include the four W’s: who, what, when, and where for every audited GPO change including created and deleted GPOs, GPO link changes, changes made to audit policy, password policies, software deployment, user desktops, and all other change activity.

In addition, it automatically provides changed setting names with before and after setting values for each GPO object change to improve security and Group Policy change control. The automatic collection and reporting on Group Policy changes not only surpasses native capabilities in Windows but expands upon them eliminating the time and effort spent collecting GPO change audit information manually or through complex scripting thereby making this information actionable.

Furthermore, it has the ability to sustain compliance through historical reporting for up to 7 years and more and extent GPO auditing into SIEM systems such as SCOM for improved IT control.

To learn more about Group Policy auditing with Netwrix Auditor, please read the overview of this feature or download a free 20-day trial of Netwrix Auditor for Active Directory.

About Netwrix Corporation

Netwrix Corporation is the leading provider of change auditing software, offering the most simple, efficient and affordable IT infrastructure auditing solution with the broadest coverage of audited systems and applications available today. Founded in 2006, Netwrix has grown to have thousands of customers worldwide. The company is headquartered in Irvine, California, with regional offices in New Jersey, Ohio, Georgia and the UK.
Additional Resources

Information security professionals and trends - http://www.infosecisland.com

Articles and commentary on a wide array of IT related topics - http://www.techrepublic.com

Community focused on Windows technologies - http://www.windowsitpro.com

Editorial resource for technology professionals - http://www.redmondmag.com

Innovative tool and active community of IT practitioners - http://www.spiceworks.com

Focused community on Windows security needs, trends, and information - http://www.windowssecurity.com


Excellent resource for Windows Administrators - http://www.petri.co.il

Netwrix Corporate Blog - http://blog.netwrix.com