2025

The Configuration Experts

Get Secure and Stay Secured

Whitepaper

Managing Domain-Joined Endpoints with Group Policy Objects (GPOs)

SDM SOFTWARE | 2100 4TH STREET, #132 SAN RAFAEL, CA 94901

Managing Domain-Joined Endpoints with Group Policy Objects (GPOs)

Group Policy is a feature of Windows that enables centralized configuration and management of operating systems, computer settings and user settings. Each policy, or Group Policy object (GPO), defines a set of Group Policy settings. Managing domain-joined endpoints are a critical task for IT administrators, as these devices are central to the security, compliance, and configuration management of an organization's IT infrastructure. Administrators can manage any GPO in Active Directory using the Group Policy Management Console (GPMC). It includes the Microsoft Management Console (MMC) snap-in, which provides a set of programmable interfaces for managing Group Policy and a scripting interface and has long been a primary tool for centrally managing security settings, system configurations, and user behaviors across Windows endpoints. However, as organizations evolve, additional tools are often required to ensure that GPOs are effectively implemented, audited, and kept compliant with both internal and external standards.

Group Policy is powerful and complex, with well over a thousand settings to choose from. As a result, managing Group Policy manually is a formidable task.

But getting Group Policy right is essential, since one errant GPO setting can put security, compliance and business continuity at risk. In fact, Group Policy is one of the most common targets of malicious actors; altering local GPOs on one computer can enable lateral movement across the network, and changing Active Directory GPOs can disable domain-wide security controls.

SDM Software offers a platform of six products that formulate a solution that can help, including the following:

SDM Software provides a suite of solutions that complement GPO management like compliance reporting capabilities - **Group Policy Compliance Manager (GPCM),** providing real-time auditing **- Group Policy Auditing & Attestation (GPAA),** and change control **- Change Manager for Group Policy and Intune (CMGPI)** that enhance the traditional Group Policy management workflow.

1. Domain-Joined Endpoints: Centralized Control and Security

When endpoints are domain-joined to an organization's Active Directory (AD), they become a part of a centralized management structure, where IT administrators can enforce uniform security policies and configurations. Domain-joining enables administrators to apply GPOs that define security configurations, application settings, and user permissions across the organization's devices.

Key Features of Domain-Joined Endpoints:

Centralized Authentication: Active Directory facilitates secure, centralized user authentication for all domain-joined devices, ensuring that only authorized users can access the network.

Security and Compliance: Through GPOs, administrators can apply consistent security settings across all endpoints, such as password policies, user rights assignments, and application restrictions, helping mitigate risks and maintain compliance.

Consistent Configuration: GPOs ensure that all endpoints receive the same configuration settings, reducing the likelihood of discrepancies and security vulnerabilities.

2. Group Policy Objects (GPOs) for Endpoint Configuration and Security

GPOs are a core feature in managing domain-joined endpoints within a Windows environment. Through GPOs, administrators can define and enforce a wide range of system settings, security policies, and user preferences on all endpoints.

Key GPO Management Features:

Security Configuration: GPOs allow for the enforcement of critical security settings, such as password complexity, account lockout policies, and encryption settings, ensuring all domain-joined endpoints adhere to organizational security standards.

Software Deployment: Administrators can use GPOs to automate the installation and maintenance of software applications on multiple devices, ensuring that all endpoints have the necessary software installed and up to date.

User Configuration: GPOs allow administrators to define user settings, such as desktop configurations, network drive mappings, and application access, ensuring a consistent experience across all endpoints.

While GPOs are powerful, they require robust management to ensure they are correctly applied, monitored, and kept compliant with organizational policies and regulatory standards.

3. Enhancing GPO Management with SDM Software Solutions

While GPOs offer centralized control over endpoints, SDM Software solutions such as GPCM, GPAA and CMGPI provide advanced capabilities for managing, auditing, and ensuring compliance with GPO settings. These Products help to ensure that GPOs are not only applied correctly but also maintained and monitored in real-time.

Change Manager for Group Policy and Intune (CMGPI):

CMGPI is a powerful solution that helps organizations streamline the Group Policy and Intune profile management process. It supports policy creation, modification, deployment, rollback and change management, making it easier for administrators to manage both on-premises GPOs and cloud-based Intune profiles in a unified platform.

GPO Management: CMGPI allows for the management of GPOs across a wide range of endpoints facilitating scheduled deployments of approved changes, saving time and reducing human error in policy applications.

Intune Profile Management: CMGPI extends its management capabilities to Intune profiles, allowing administrators to manage both traditional on-premises and modern cloud-based policies in a seamless manner. This is particularly useful in hybrid IT environments where endpoints are managed both on-premises and in-the-cloud. Features like versioning, rollback and scheduled deployments also apply to Intune profiles with CMGPI.

Streamlined Change Control: CMGPI provides change management features that help ensure GPOs and Intune profiles are deployed with proper approval workflows, reducing the risk of unauthorized or misconfigured changes.

Group Policy Compliance Manager (GPCM):

GPCM enables organizations to maintain compliance with GPO settings across all domain-joined endpoints. It offers powerful tools for auditing and tracking historical GPO changes and their impact on endpoint security and configuration.

Compliance Reporting: GPCM provides detailed compliance reports that enable administrators to quickly verify that GPO settings have been applied correctly across all endpoints. These reports can help demonstrate compliance with internal standards and external regulatory frameworks such as GDPR, HIPAA, and PCI DSS.

Change Tracking:

By scheduling collections, GPCM enables historical tracking of GPO settings applied to endpoints, allowing administrators to review past configurations and assess compliance trends over time. This helps in tracking setting changes and identifying deviations from intended policies.

Risk Mitigation: By ensuring that all GPOs are correctly applied and regularly checked for compliance, GPCM helps mitigate risks associated with misconfigurations, unauthorized changes, and security vulnerabilities.

Group Policy Auditing & Attestation (GPAA):

GPAA adds another layer of monitoring and security by enabling real-time auditing of GPO changes. This solution is particularly useful for organizations that need to maintain a high level of visibility over their GPO environment and respond quickly to unauthorized changes or security incidents.

Real-Time Auditing: GPAA continuously tracks GPO changes, capturing detailed information about who made the change, what was changed, and when it occurred. This real-time tracking helps to identify and respond to security threats or policy violations before they cause significant issues.

Attestation and Accountability: GPAA provides organizations with the ability to assign owners to group policies. Attestation campaigns ensure that owners are performing proper reviews of Group Policy Objects on a periodic basis ensuing applied settings are valid. By maintaining a clear record of all changes, GPAA supports internal auditing and regulatory compliance, making it easier to demonstrate accountability and adherence to security policies.

Key Compliance and Risk Management Features:

Audit-Ready Reports: Both GPCM and GPAA provide detailed, audit-ready reports that can be used during compliance audits. These reports include information about GPO configurations, changes, and who made them, making it easier to meet regulatory requirements. With GPCM, create reports to compare baseline Group Policies with what is being applied to ensure that settings applied meet corporate standards.

Continuous Monitoring: With continuous auditing and real-time alerts, SDM Software ensures that administrators are notified of any unauthorized changes to GPO settings, helping to detect and address potential security issues before they escalate.

5. Integrating GPO Management with Security and Compliance Frameworks

Managing GPOs and Intune profiles in a unified manner is essential in today's hybrid IT environments, where both on-premises and cloud-based endpoints must be managed securely and efficiently. SDM Software's solutions integrate seamlessly with security frameworks and compliance tools, that help organizations enforce consistent security policies across all devices, whether they are managed on-premises or in the cloud.

Key Integration Considerations:

SIEM Integration: SDM Software's Products can integrate with Security Information and Event Management (SIEM) platforms, ensuring that GPO and profile changes are logged, analyzed, and correlated with other security events.

Cloud and Hybrid Management: For organizations with a mix of on-premises and cloud-based devices, SDM Software solutions help manage both environments effectively, ensuring that GPOs and Intune profiles are applied consistently, no matter where the device is located.

Final Thought

GPOs remain a critical tool for managing domain-joined endpoints, ensuring consistent configuration, security, and compliance across an organization's IT infrastructure. However, to maximize the effectiveness of GPO management, organizations can leverage SDM Software solutions like CMGPI, GPCM, and GPAA to enhance auditing, monitoring, and compliance. These solutions provide real-time auditing, change tracking, rollback and compliance reporting, making it easier for IT teams to manage GPOs and Intune profiles across diverse environments while maintaining the highest standards of security and operational efficiency.

About SDM Software

Since 2006, **SDM Software** has been **the** leader in providing products for managing Windows configuration efficiently, and Group Policy technology (and now Intune®) specifically. With extensive knowledge of the real-world best practices and experience managing Windows environments ranging from 100 to 300,000+ systems and with over 700 customers worldwide, we built a platform of products that are designed with security and simplified management efficiency in mind. Our Group Policy and Intune products – commercial and freeware – are in use by thousands of administrators around the world.