2024

sdmsoftware

The Configuration Experts

*Get Secure and Stay Secured*

Whitepaper

# The Importance of GPO and Intune Cyber Hygiene

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

## Enhancing Security, Control, and Compliance for Windows Environments

As organizations move to hybrid environments combining Group Policy Objects (GPO) and Microsoft Intune, the importance of maintaining rigorous cyber hygiene has never been greater. Poorly managed configurations can lead to vulnerabilities, while secure, compliant workflows ensure operational efficiency and defense against modern threats. This whitepaper explores how GPO and Intune hygiene practices are critical for mitigating risk, simplifying management, and driving efficiency.

## Executive Overview

Cyber hygiene encompasses security practices that reduce vulnerabilities by enforcing clean, consistent, and auditable policies. In a Windows environment:

1. **Group Policy** centralizes security controls across on-premises Active Directory.
2. **Intune** delivers modern management for cloud-joined Windows devices.

Both platforms must be securely managed, updated, and continuously monitored to prevent misconfigurations and unauthorized changes.

## Challenges in Maintaining GPO and Intune Cyber Hygiene

1. **Outdated or Orphaned GPOs**:
   - Stale or forgotten policies can cause configuration risks and increase attack surfaces.
2. **Inadequate Auditing and Attestation**:
   - Lack of real-time change control and attestation mechanisms hinders visibility into unauthorized changes and can result in GPO sprawl.
3. **Lack of Automation**:
   - Manual management of policies leads to inefficiencies, errors and higher operational costs.
4. **Hybrid Environment Complexity**:
   - Managing both Group Policy Object Policies and Intune Profiles  creates challenges for consistency and compliance.
5. **Risk of Unauthorized or Malicious Changes**:
   - Without proper approval workflows, attackers can leverage poorly designed or misconfigured policies to gain access, escalate privileges, and distribute malware.

## Core Principles and Tools for GPO and Intune Cyber Hygiene

Achieving robust GPO and Intune cyber hygiene requires a combination of foundational principles and modern tools to streamline management, enhance security, and maintain compliance in Windows environments.

### Core Principles of Cyber Hygiene with SDM Software Tools

1. **Regular Auditing and Attestation**
   - Ensure real-time monitoring, historical tracking, and periodic attestations of GPO changes using **GPAA (Group Policy Auditing and Attestation)**. This ensures policies remain current and compliant with standards.
2. **Change Control and Version Management**
   - Implement secure approval workflows, role-based access, and rollback capabilities with **CMGPI (Change Manager for Group Policy and Intune)** to manage changes effectively and securely.
3. **Policy Migration and Cleanup**
   - Use **GPO Migrator** to consolidate, streamline, and optimize GPO structures while reducing complexity and improving policy efficiency.
4. **Compliance and Reporting**
   - Leverage **GP Reporting Pak** for real-time insights into GPO health, optimization, and security, identifying stale, orphaned, or conflicting policies.
5. **Automation for Efficiency**
   - Automate routine policy deployment and management tasks using PowerShell-based tools like **GPAE (Group Policy Automation Engine)**, reducing manual intervention and improving efficiency.
6. **Role-Based Access and Least Privilege**
   - Enforce **Role-Based Access Control (RBAC)** to limit editing and approvals to authorized personnel, ensuring secure operations and adherence to least privilege principles.

By aligning these principles with SDM Software's modern tools, organizations can establish a secure, compliant, and streamlined approach to managing GPOs and Intune Profiles in their Windows environments.

## Benefits of a Strong GPO and Intune Cyber Hygiene Practice

1. **Improved Security Posture**:
   - Eliminate vulnerabilities caused by misconfigurations and stale policies.
2. **Operational Efficiency**:
   - Reduce manual overhead with automated workflows and reporting.
3. **Enhanced Compliance**:
   - Meet security and regulatory requirements with auditing, attestation, and change control.
4. **Centralized Management**:
   - Gain control over hybrid environments with tools that unify GPO and Intune workflows.
5. **Reduced Risk of Unauthorized Changes**:
   - Prevent malicious or accidental misconfigurations with role-based approvals and rollback features.

---

## Final Thoughts

Maintaining a strong GPO and Intune cyber hygiene is crucial for any organization looking to enhance security, streamline operations, and ensure compliance. Leveraging modern tools like SDM Software's Group Policy Auditing and Attestation (GPAA), Change Manager for Group Policy and Intune (CMGPI), Group Policy Object Migrator (GPOM), Group Policy Automation Engine (GPAE), and Group Policy Reporting Pak (GPRP) enables organizations to implement automated, secure, and scalable management frameworks. By adhering to best practices, organizations can mitigate risk, prevent unauthorized changes, and efficiently manage their Windows environments.

### About SDM Software

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