sdmsoftware
The Configuration Experts
Get Secure and Stay Secured

SDM Software - FAQs Sheet

Introduction to Policy Governance by SDM Software

Policy Governance in the context of Active Directory (AD) Group Policy Objects (GPOs) and Intune Profiles involves the management, oversight, and auditing of policies that control configurations and settings across an organization's IT infrastructure. It ensures that policies are consistently applied, updated, and compliant with regulatory and organizational standards. Today's Hybrid IT environments can make it challenging to enforce consistent Policy governance across the enterprise. Solutions from SDM Software enable a risk-aware, extensible governance across on-premises, Hybrid and Cloud Only environments.

Key Principles of Policy Governance:

1. **Creation and Management**: Establishing and maintaining policies that define how resources are configured and managed.
2. **Compliance and Security**: Ensuring that policies meet compliance requirements and safeguard the IT environment.
3. **Delegation and Role Management**: Assigning responsibilities and permissions to appropriate roles within the organization.
4. **Monitoring and Auditing**: Continuously tracking changes and actions related to policies to ensure accountability.
5. **Automation and Efficiency**: Implementing tools and workflows to automate policy management processes.

How SDM Software Implements Governance

SDM Software's solutions are designed to facilitate comprehensive governance of GPOs and Intune Profiles by addressing key governance principles.

SDM Software Products:

1. **Change Manager for Group Policy & Intune (CMGPI)**
2. **Group Policy Auditing & Attestation (GPAA)**

Key Governance Features and How SDM Products Address Them:

1. Creation/Deletion of GPO and Intune Profiles, with Rollback

- **CMGPI**: Enables the lifecycle management of GPO's and Intune Profiles. It facilitates the creation, modification, and deletion of GPOs and Intune profiles with the ability to rollback to previous version states in case of errors or issues. Compare versions to see what's changed. This ensures informed decisions when restoring and that changes can be undone safely, maintaining environmental stability and security.

2. Role-Based Delegation

- **CMGPI & GPAA**: Allows administrators to assign specific roles and permissions to users, ensuring that only authorized personnel can make changes to GPOs and Intune profiles. This role-based access control helps in minimizing unauthorized changes and enhances security.

3. Ensures Compliance through Comprehensive Alerting and Notification

- **GPAA**: Provides real-time alerting and notification mechanisms to inform administrators of any changes or non-compliant activities related to GPO changes in the environment. This feature helps organizations stay compliant with internal policies and external regulations.
- **CMGPI**: Provides real-time alerting and notification for change workflows. Notifications of GPO's/Intune Profiles being Checked out, checked-in, Approval requests and more, enable organizations to maintain the checks and balances of their policy and profile environments.

4. Automate Change Management Workflows

- **CMGPI**: Facilitates the automation of change management workflows, reducing the manual effort required to manage GPO and Intune profile changes. Automated workflows ensure consistency and reduce the risk of human error. This process is applied to ensure that GPO& Intune changes in the environment are controlled, coordinated and approved before their implementation.

5. Certification/Attestation

- **GPAA**: Offers tools for certification and attestation of GPOs, ensuring that policies are reviewed and approved periodically. This process helps in maintaining the integrity and compliance of policies over time.

6. Audit Logging

- **CMGPI:** All changes made to GPOs and Intune Profiles within the Product are logged. The log reports the date and time of the activity, the type of activity performed, the object on which it was performed, the domain where that object resides, the status of the activity and the user who performed it.
- **GPAA**: Maintains detailed logs of all changes and activities related to GPOs in the environment. GPAA captures changes done natively and by third party tools using proxy accounts. These logs are essential for forensic analysis, compliance audits, and tracking the history of changes.

7. Analytics & Reporting

- **GPAA**: Provides advanced analytics and reporting capabilities to give insights into policy compliance, change history, and overall governance status. These reports can be used to demonstrate compliance and inform strategic decisions.
- **CMGPI**: Offers the ability to view the difference report, showing difference between what's currently in production and what CMGPI knows is the last known good version deployed. CMGPI also analyzes and reports on out-of-band changes. If a change that is out of compliance is detected, the dialog allows you to roll-back the non-compliant version to the last compliant version. Or ignore the differences and absorb those changes to make it compliant.

8. Entitlement Management

- **GPAA**: Entitlements relate to anything an identity is the owner of. With GPAA, define primary and secondary owners of GPO's enabling them to certify the legitimacy of its settings. This helps in maintaining a secure and organized policy management system.

How CMGPI and GPAA Implement These Features:

- **Change Manager for Group Policy & Intune (CMGPI)**: Focuses on the lifecycle management of GPOs and Intune profiles, offering features such as creation, deletion, role-based delegation, change workflows, and rollback capabilities
- **Group Policy Auditing & Attestation (GPAA)**: Concentrates on the auditing, compliance, and reporting aspects, providing tools for real-time alerting, comprehensive audit logging, certification/attestation processes, and advanced analytics and reporting.

Frequently Asked Questions (FAQs)

General Questions

Q1: What is Policy Governance in the context of Active Directory Group Policy and Intune Profiles?

A1: Policy Governance involves the lifecycle management, oversight, and auditing of policies that control configurations and settings across an organization's IT infrastructure to ensure compliance, security, and efficiency.

Q2: Why is Policy Governance important for GPOs and Intune Profiles?

A2: It ensures that policies are consistently applied, updated, and compliant with regulatory and organizational standards, safeguarding the IT environment and enhancing operational efficiency.

Q3: Why is Change Management Critical for my GPOs and Intune Profiles?

A3: Change management in general is critical for an organization because:

- Every modification to a process, material or equipment needs to be properly recorded and authorized
- It ensures proper coordination across stakeholders through automated workflows and alerts
- It helps meet compliance with industry and government regulations and standards

It is no different for Group Policy and Intune Profiles. With an increase in modern hacking techniques and frequencies, it is imperative that every organization have processes that enforce a measure of auditing, compliance and security for unwanted changes to their Group Policies and Intune Profiles.

Product-Specific Questions

Q4: How does SDM Software help in creating and managing GPOs and Intune Profiles?

A4: Change Manager for Group Policy/Intune (CMGPI) brings modern change control to customers that rely on Group Policy and Intune day in and day out. Securely delegate access to GPO editing, container linking and Intune settings and assignments, with approval-based workflows. View differences and search for settings between versions of GPOs, containers and Intune profiles and rollback, undelete or schedule deployment of changes–all from a modern web interface. Whether you are new to GPO (and Intune) Change Control or looking for an alternative to the antiquated tools such as **Microsoft's AGPM** or **Quest's GPOAdmin** - CMGPI can meet your needs! Bring Security and Governance to your Windows configuration environments

Q5: Can SDM Software help in ensuring compliance and security?

A5: Yes, GPAA provides real-time alerting, notification, and comprehensive audit logging of both native and proxy-based changes to help ensure that policies meet compliance requirements and security standards.

A5b: CMGPI Offers the ability to view the difference report, showing difference between what's currently in production and what CMGPI knows is the last known good version deployed. CMGPI also analyzes and reports on out-of-band changes. If a change that is out of compliance is detected, the dialog allows you to roll-back the non-compliant version to the last compliant version. Or ignore the differences and absorb those changes to make it compliant.

Q6: How does SDM Software handle role-based delegation?

A6: CMGPI allows administrators to assign roles and permissions to users, ensuring only authorized personnel can make specific changes, which enhances security and minimizes unauthorized modifications. Furthermore, GPAA enables role-based delegation, defining who and what a user's has access to within the product.

Q7: What features does SDM Software offer for automated change management?

A7: CMGPI facilitates the automation of change management workflows, reducing manual effort and ensuring consistency and accuracy in policy changes. CMGPI also is equipped with a robust list of PowerShell cmdlets enabling organizations to integrate change management function by calling these cmdlets from a 3rd party or in a script.

Q8: How does SDM Software support certification and attestation?

A8: GPAA provides tools for the periodic review and approval of GPOs to maintain the integrity and compliance of policies over time. Schedule the Initial notification interval, Follow-up notification interval, Secondary notification interval and more!

Q9: What kind of audit logging capabilities does SDM Software provide?

A9: With CMGPI, all changes made to GPOs and Intune Profiles within the Product are logged. The log reports the date and time of the activity, the type of activity performed, the object on which it was performed, the domain where that object resides, the status of the activity and the user who performed it. Furthermore, GPAA maintains detailed logs of all changes and activities related to GPOs in the environment. GPAA captures changes done natively and by third party tools using proxy accounts. These logs are essential for forensic analysis, compliance audits, and tracking the history of changes.

Q10: What analytics and reporting tools does SDM Software offer?

A10: GPAA provides advanced analytics and reporting capabilities to give insights into policy compliance, change history, and overall governance status, supporting strategic decision-making.

A10b: CMGPI Offers the ability to view the difference report, showing difference between what's currently in production and what CMGPI knows is the last known good version deployed. CMGPI also analyzes and reports on out-of-band changes. If a change that is out of compliance is detected, the dialog allows you to roll-back the non-compliant version to the last compliant version. Or ignore the differences and absorb those changes to make it compliant.

Q11: How does SDM Software manage user entitlements?

A11: With GPAA, define primary and secondary owners of GPO's enabling them to certify the legitimacy of its settings. This helps in maintaining a secure and organized policy management system.

Q12: What if I only use Intune Profiles and do not have an on-premises Active Directory, Do I still need SDM Software Products?

A12: Yes, the basic principle of governance is important whether you have AD only, Hybrid or Cloud-Only environments! With CMGPI, organizations can benefit from the robust features previously mentioned. With CMGPI you get lifecycle management of Intune profiles, offering features such as creation, deletion, role-based delegation, change workflows, and rollback capabilities complete with auditing. CMGPI also analyzes and reports on out-of-band changes. If a change that is out of compliance is detected, the dialog allows you to roll-back the non-compliant version to the last compliant version. Or ignore the differences and absorb those changes to make it compliant.

Q13: Do I need to purchase both Products to benefit from governance?

A13: SDM Software's solutions are designed to facilitate comprehensive governance of GPOs and Intune Profiles by addressing key governance principles. Both CMGPI and GPAA can be purchased separately depending on your needs and have been designed to work independently of each other.

- **Change Manager for Group Policy & Intune (CMGPI)**: Focuses on the lifecycle management of GPOs and Intune profiles, offering features such as creation, deletion, role-based delegation, change workflows, and rollback capabilities
- **Group Policy Auditing & Attestation (GPAA)**: Concentrates on the auditing, compliance, and reporting aspects, providing tools for real-time alerting, comprehensive audit logging, certification/attestation processes, and advanced analytics and reporting.

However, if your organization requires full governance of Active Directory and Entra ID objects, the combined power of CMGPI and GPAA for Group Policy objects and Intune Profiles is the solution for you!