AGPM Deprecation: What You Need to Know

Advanced Group Policy Management (AGPM), part of the **Microsoft Desktop Optimization Pack (MDOP)**, has long been a critical tool for IT administrators managing large-scale Group Policy deployments. AGPM enhances the capabilities of native **Group Policy Object (GPO)** management by adding features such as version control, change tracking, role-based administration, and approval workflows. However, since the release of **AGPM 4.0 SP3** in 2016, there have been no subsequent updates, signaling its deprecation. As organizations continue to move towards modern server environments, the viability of AGPM has come under scrutiny.

AGPM Overview

AGPM has provided several key features that have helped organizations maintain secure and efficient Group Policy environments:

1. **GPO Change Management**: It allows administrators to control changes to GPOs with approval workflows, ensuring that only authorized changes are implemented.
2. **Version Control**: AGPM offers historical tracking of GPO changes, enabling rollback to previous versions when necessary.
3. **Role-Based Access**: By defining roles for specific administrative tasks, AGPM improves security by limiting who can create, edit, or approve GPO changes.
4. **Audit Trail**: AGPM provides detailed logging, which is crucial for tracking and compliance purposes, showing who made changes to GPOs and when.

While these features are still relevant, AGPM has not kept pace with modern IT infrastructure needs, especially in hybrid and cloud environments.

AGPM 4.0 SP3: The Current Release

The current release, **AGPM 4.0 SP3**, came out in 2016. It was designed to work primarily with **Windows Server 2016**. The release featured minor bug fixes and performance improvements, but no major updates or new features were introduced. Since then, Microsoft has not released any newer versions or patches specifically designed for AGPM, making it incompatible with some modern server features and Group Policy advancements.

For more details on AGPM's features and deployment scenarios, refer to the official Microsoft documentation here.

Compatibility with Newer Windows Server Versions

Since the release of AGPM 4.0 SP3, Microsoft has introduced new server versions, such as:

- **Windows Server 2019**
- **Windows Server 2022**

One of the key concerns for organizations still using AGPM is its limitations in fully supporting newer server platforms like Windows Server 2019 and 2022. Despite AGPM's ability to technically function on these systems, several challenges arise:

- **Absence of Recent Updates or Enhancements:** Since the release of AGPM 4.0 SP3 in 2016, no new patches or updates have been issued to address potential compatibility issues or improve performance on newer servers. This means that any emerging problems, particularly those associated with modern server features, will need to be handled internally by organizations, adding complexity and risk to IT operations.
- **Ongoing Security Risks:** Although AGPM 4.0 SP3 is still supported on newer server versions like Windows Server 2019 and 2022, the lack of significant feature updates since 2016 may lead to security vulnerabilities in rapidly evolving IT infrastructures. While Microsoft will likely release patches for known security issues, relying on outdated software like AGPM in dynamic, complex environments could expose organizations to security threats. Organizations must continually assess whether AGPM aligns with their security and operational needs as technology advances.

In summary, while AGPM 4.0 SP3 remains functional on newer server platforms, its outdated nature presents challenges in terms of compatibility, operational efficiency, and security.

The Need for Modern Solutions

As organizations transition to newer server environments and hybrid infrastructures, the limitations of AGPM become more apparent. Microsoft has not provided a replacement or a modern version of AGPM that integrates with tools like **Microsoft Intune** or **Entra ID**. This leaves organizations that need advanced Group Policy management features without a clear path forward.

Latest Microsoft Alternatives

Microsoft itself now promotes tools such as **Microsoft** Intune (previously **Microsoft Endpoint Manager)** and **Microsoft** Entra ID for policy & identity management in hybrid environments, but these tools do not offer all the capabilities that AGPM provides. As a result, many organizations are looking for third-party solutions to fill this gap.

AGPM Deprecation and Alternatives

While AGPM is technically still usable in environments with **Windows Server 2016 2019 and 2022**, it is clear that its long-term utility is limited. For organizations looking to modernize their policy management, alternatives like **SDM Software's Change Manager for Group Policy and Intune (CMGPI)** offer a path forward. CMGPI provides:

- **An actively updated product with ongoing support for Group Policy and its current capabilities**
- **Integration with Microsoft Intune and cloud-based policy management**
- **Enhanced approval-based workflows and delegation features**
- **Advanced reporting and automation capabilities**

These modern features make CMGPI a more sustainable solution for organizations managing Group Policies in both on-premises and cloud environments.

Additionally, **SDM Software** offers a companion real-time detection solution called Group Policy Auditing and Attestation (GPAA), which identifies system administrators not conforming to organizational standards or detects unwanted changes due to security intrusions targeting Group Policy permissions. Together, **CMGPI** and **GPAA** provide comprehensive **governance, risk management, and compliance (GRC)** capabilities, offering more advanced control over Group Policy processes than AGPM ever did.

Key features of **CMGPI and GPAA** include:

- **Real-time GPO auditing**, automatic backup, and rollback capabilities
- **Detailed event tracking** for "Who, What, When, and Where" of changes
- **Critical GPO attestation** to meet compliance needs

These features make **CMGPI** a sustainable solution for organizations managing both on-premises and cloud-based Group Policy environments.

Future of Group Policy Management

Given that AGPM 4.0 SP3 (Released 2016) was the last release and that Microsoft has not signaled any future updates or patches, organizations should carefully evaluate the exposure to risks of continuing to rely on AGPM with all the cybersecurity issues that have surface in the last 10 years since it release. Modern IT environments require tools that support hybrid cloud infrastructure, real-time monitoring, and advanced automation—capabilities that AGPM, in its current state, cannot deliver.

Organizations should consider transitioning to more modern solutions that provide:

- **Real-time compliance monitoring**
- **Support for hybrid environments using both GPO and Intune**
- **Cloud-based policy management integration**

Solutions like SDM Software's CMGPI offer the flexibility and features needed for modern Group Policy management, including enhanced security, automation, and scalability.

Conclusion

The deprecation of **AGPM** signals the end of an era for organizations that relied on its Group Policy management features. While it still provides value for organizations running **Windows Server 2016**, the lack of updates for newer server versions such as **Windows Server 2019** and **Windows Server 2022** presents both security and operational challenges. Organizations should strongly consider migrating to alternative tools like **CMGPI**, which provide modern Group Policy management capabilities to meet the demands of hybrid and cloud-based IT environments.

For organizations still using AGPM, now is the time to assess the risks, evaluate alternatives, and plan for the future of Group Policy management in a rapidly evolving IT landscape.

Advanced Group Policy Management 4.0 - Microsoft Desktop Optimization Pack | Microsoft Learn

Advanced Group Policy Management 4.0