|  |  |
| --- | --- |
|  |  |

By Jerry Honeycutt

Published

Abstract

Microsoft® Advanced Group Policy Management (AGPM) helps you better manage Group Policy objects (GPOs) in your environment by providing change control, offline editing, and role-based delegation. AGPM is a key component of the Microsoft Desktop Optimization Pack (MDOP). This white paper is an overview of AGPM, and describes its benefits, how it works, and the next steps for evaluating it.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2007 Microsoft Corporation. All rights reserved. Microsoft, MSDN, SharePoint, SoftGrid, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

[Overview 3](#_Toc179355401)

[Offline Editing 5](#_Toc179355402)

[GPMC Integration 6](#_Toc179355403)

[Change Control 7](#_Toc179355404)

[Role-Based Delegation 8](#_Toc179355405)

[Summary 9](#_Toc179355406)

# Overview

Imagine a tool that can help you take control of Group Policy. What would this tool do? It would help you better delegate who can review, edit, and deploy Group Policy objects (GPOs). It would help you prevent widespread failures that result from editing GPOs in production. You could use it to track each version of each GPO. Any tool that provided these capabilities, cost little, and was easy to deploy would certainly be worth a closer look.

Such a tool indeed exists, and it’s an integral part of the [Microsoft® Desktop Optimization Pack](http://www.microsoft.com/windows/products/windowsvista/enterprise/mdopoverview.mspx) (MDOP) for Software Assurance. MDOP helps organizations reduce the cost of deploying applications, deliver applications as services, and better manage desktop configurations. Together, the MDOP components shown in Figure 1 deliver to Software Assurance customers a highly cost-effective and flexible solution for managing desktop computers.

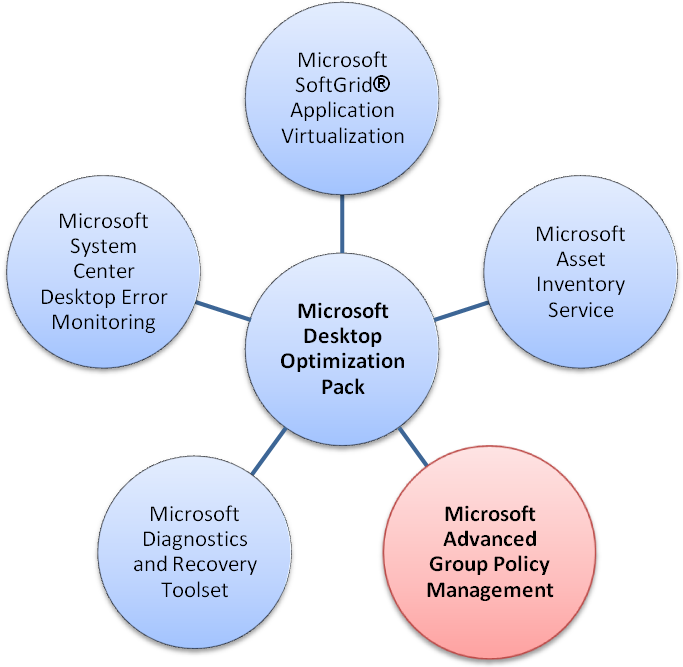


Figure 1. MDOP components

Microsoft Advanced Group Policy Management (AGPM) is a key MDOP component. It helps customers overcome challenges that affect Group Policy management in any organization, particularly those with complex information technology (IT) environments. A robust delegation model, role-based administration, and change-request approval provide granular administrative control. For example, you can delegate Reviewer, Editor, and Approver roles to other administrators — even administrators who do not have access to production GPOs. The Editor role can edit GPOs but not deploy them; the Approver role can deploy GPO changes. AGPM also helps reduce the risk of widespread failures. You can use AGPM to edit GPOs offline, outside of the production environment, and then audit changes and easily find differences between GPO versions. In addition, AGPM supports effective change control by providing version tracking, history capture, and quick rollback of deployed GPO changes. It also supports a management workflow by allowing you to create GPO template libraries and send GPO change e-mail notifications.

This white paper describes the key features of AGPM: change control, offline editing, and role-based delegation. It then describes how Software Assurance customers can begin evaluating AGPM today.

# Offline Editing

The AGPM archive provides offline storage for GPOs. As shown in Figure 2, changes made to GPOs in the archive don’t affect the production environment until you deploy the GPOs. By limiting changes to the archive, you can edit and test GPOs without affecting the production environment. After reviewing and approving the changes, you can then deploy them with the knowledge that you can quickly roll them back if they have an undesirable effect.



Figure 2. Offline editing

# GPMC Integration

AGPM has a server component and a client component, each of which you install separately. First, you install the Group Policy Management Console (GPMC) and the server component on a server system that has access to the policies you want to manage. Then, you install GPMC and the AGPM client on any computer from which administrators will review, edit, and deploy policies. You can run the client on Windows Vista® or Windows Server® 2003.

The AGPM client integrates completely with GPMC, as shown in Figure 3. Administrators review, edit, and deploy GPOs within each domain’s **Change Control** folder. The GPOs you see in the **Group Policy objects** list on the **Controlled** tab are stored in the AGPM server’s archive. Changes made to these GPOs don’t affect the production environment until administrators with the Approver role deploy the GPOs to production.



Figure 3. AGPM integration with GPMC

# Change Control

AGPM provides advanced change control features that help you manage and control GPOs. Many of the AGPM change control concepts are already familiar to administrators with experience using common version-control tools, such as the version control feature in Microsoft Windows® SharePoint® Services. The steps necessary to change and deploy a GPO are as follows:

1. Check out the GPO from the archive.
2. Edit the GPO as necessary.
3. Check in the GPO to the archive.
4. Deploy the GPO to production.

Change control is more than checking files in and out of the archive, though. AGPM keeps a history of changes for each GPO, as shown in Figure 4. You can deploy any version of a GPO to production, so you can quickly roll back a GPO to an earlier version if you need to. AGPM can compare different versions of a GPO, and show settings that were added, changed, or deleted. This way, you can easily review changes before approving and deploying them to the production environment.

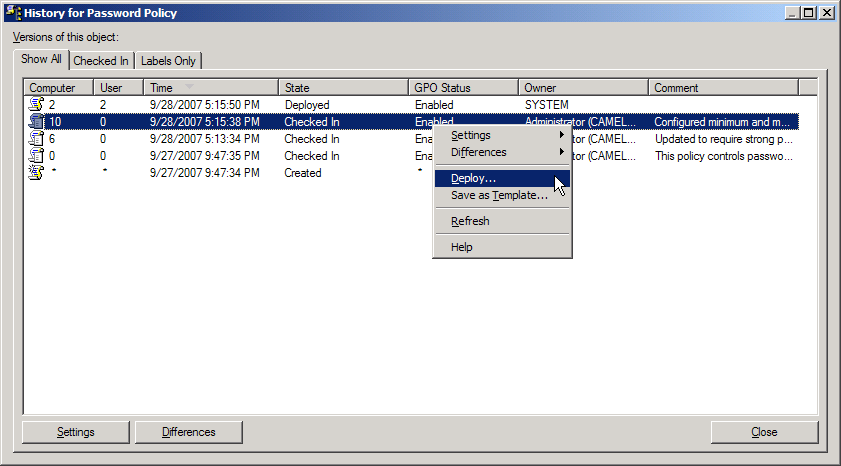


Figure 4. GPO History

# Role-Based Delegation

Group Policy already provides a rich delegation model. It allows you to delegate administration to regional and task-oriented administrators. It also, however, lets administrators approve their own changes. In contrast, AGPM provides a role-based delegation model that adds a review and approval step to the workflow, as shown in Figure 5.



Figure 5. Role-based delegation

To support this delegation model, AGPM defines three special roles:

* **Reviewer.** Administrators assigned to the Reviewer role can view and compare GPOs. They cannot edit or deploy them.
* **Editor.** Administrators assigned to the Editor role can view and compare GPOs. They can check out GPOs from the archive, edit them, and check them in to the archive. They can also request deployment of a GPO.
* **Approver.** Administrators assigned to the Approver role can approve the creation and deployment of GPOs. (When administrators assigned to the Approver role create or deploy a GPO, approval is automatic.)

You can assign administrators and groups to these roles for all controlled GPOs within the domain. For example, you can assign administrators globally to the Reviewer role, which allows them to review any controlled GPO in the domain. You can also assign administrators to these roles for individual controlled GPOs. Rather than allow administrators to edit any controlled GPO in the domain, for example, you can give them specific permission to edit individual controlled GPOs by assigning to them the Editor role for those GPOs only.

# Summary

Forsyth County covers the Winston-Salem, North Carolina, metropolitan area. Its population of nearly 325,000 is located in a 410–square mile area. The county’s IT department supports approximately 1,400 users and 1,650 desktop computers.

Forsyth County needed a solution for managing desktop computers that didn’t compromise server security, helped the County nimbly update desktop computer configurations, and provided a rich history of changes. Michael Wilcox, MIS Client Services Supervisor, says, “I attended a seminar on Group Policy and learned about Microsoft Advanced Group Policy Management. I was impressed with how it could enhance the delegation capabilities for administrators.” Forsyth County went on to implement AGPM.

After deploying AGPM, Forsyth County immediately began realizing benefits. “It’s amazing. Managing our desktop configurations is so much easier. We’d be floundering without it,” Wilcox said. Using AGPM the county can easily and safely build GPOs. They can create and change GPOs without affecting the production environment. Importantly, administrators at Forsyth County don’t have to manually document their changes, because AGPM keeps a rich history of changes. According to Wilcox, “Advanced Group Policy Management has been like a magic bullet for us. Its automated change management and workflow-enabled delegation capabilities are impressive. I wouldn’t be able to manage GPOs without it.”

AGPM is an add-on license available only to Software Assurance customers. Begin your evaluation today by taking the following steps:

* **Download and evaluate AGPM**

The AGPM evaluation is available to Volume Licensing customers and MSDN® subscribers. The evaluation includes a step-by-step guide that walks customers through most AGPM capabilities.

* **See the Windows Vista for the Enterprise, Microsoft Desktop Optimization Pack Web site**

To learn how AGPM and the MDOP for Software Assurance can help you, see <http://www.windowsvista.com/optimizeddesktop>. This Web site provides videos and datasheets that help you evaluate AGPM.