|  |  |
| --- | --- |
| **AGPM_Logo.png** |  |

Planning Guide for Advanced Group Policy Management 3.0

Published December 2008

Abstract

Microsoft® Advanced Group Policy Management (AGPM) 3.0 is the latest version of Microsoft’s comprehensive change control and enhanced management for Group Policy objects (GPOs). AGPM extends the capabilities of the Group Policy Management Console (GPMC) to provide GPO change control workflow, GPO version control, and role-based delegation of GPO administration. This guide helps in planning the successful deployment of AGPM to ensure that an organization achieves its maximum benefits.



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.

© 2008 Microsoft Corporation. All rights reserved. Microsoft, Active Directory, BitLocker, Windows, Windows Server, Windows Vista, and the Windows logo and 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

Contents 2

Introduction 4

Using This Guide 4

Common Deployment Configurations 5

Centralized Configuration 5

Decentralized Configuration 6

Manage Group Policy in Extranets 8

Planning a Basic AGPM Deployment 9

Collect Necessary Information About the Existing AD DS Infrastructure and GPOs 9

Determine the Number of AGPM Servers Required 10

Determine the Number of AGPM Clients Required 10

Determine the User Accounts Required for Deployment 10

Determine the E-mail Infrastructure Requirements 11

Determine the AGPM Archive Location and Storage Requirements 11

Ensure That Computers Meet Installation Requirements 12

AGPM Server Installation Requirements 12

AGPM Client Installation Requirements 12

Plan an AGPM Server Backup Strategy 13

Planning AGPM Security 14

Assign the Appropriate Security Roles 14

Secure the AGPM Service Account 16

Secure the AGPM Archive 17

Secure AGPM Communication 17

Harden Computers Running AGPM Server 18

Planning for AGPM Scaling 21

Upgrading from Previous Versions of AGPM 22

Upgrade AGPM Server 22

Upgrade the AGPM Client 22

Summary 23

For More Information 24

# Introduction

Microsoft® Advanced Group Policy Management (AGPM) version 3.0 is the latest version of Microsoft’s comprehensive change control and enhanced management for Group Policy objects (GPOs). AGPM 3.0 improves on the functionality of previous versions, including:

* Support for multiple languages.
* Support for 64-bit operating systems.
* Support for Group Policy preferences, which is a new Group Policy feature in Windows Server® 2008.
* A simplified installation process.
* More detailed information about GPO revision history.
* The ability to limit the number of GPO versions stored in the GPO archive.
* Improved e-mail security.
* Updated role permissions security.

## Using This Guide

This guide provides an in-depth description the processes, procedures, and decisions for planning the deployment of AGPM 3.0 in your production environment. It also offers prescriptive guidance to help properly deploy AGPM in your organization so that you can obtain the maximum benefit from using AGPM to manage GPOs.

This guide is written such that if you make your planning decisions as you read this guide, your AGPM design will be complete when you finish the guide. The document is divided into the following sections, which cover the various aspects of your AGPM design:

* **Planning a basic AGPM deployment.** Learn how to plan an AGPM deployment using a single AGPM Server connected to a single domain. Advanced planning topics for security, high availability, fault tolerance, and scaling are included in the other sections.
* **Planning AGPM security.** This section discusses the security-related planning decisions in an AGPM deployment. Topics in this section include planning AGPM Server hardening, communications ports that AGPM uses, Windows® Firewall rules that AGPM enables, services that AGPM requires, files that AGPM installs, AGPM security roles, and AGPM Service Accounts and permissions.
* **Planning for AGPM high-availability and improved fault tolerance.** This section discusses the availability and performance aspects of the AGPM deployment planning process. Topics in this section include hardware fault tolerance, AGPM Server availability, and AGPM Client availability.
* **Planning for AGPM scaling.** Learn how to create AGPM solutions that can support the current and future size of your organization. Topics in this section include scaling up existing AGPM Servers by adding additional system resources.
* **Migrating from previous versions of AGPM.** Learn how to migrate from AGPM 2.5 to AGPM 3.0. Topics in this section include migrating AGPM Servers and AGPM Clients.

Planning is an iterative process, so as you complete the processes in this guide, you may need to revisit earlier planning decisions. For example, you may need to change security-related decisions based on scaling-related planning decisions. Perform the necessary iterative reviews of your plan until all aspects of the plan meet or exceed your requirements.

## Common Deployment Configurations

AGPM can be deployed to serve the needs of any size organization, any network infrastructure, and any security model. This planning guide presents common deployment configurations. Even though these scenarios are presented as discrete units, your implementation of AGPM may consist of a combination of these scenarios. For example, you might have data centers that use one configuration but branch offices that use a different one.

**Note:** The level of management centralization in AGPM can be influenced by your corporate structure and network performance issues between domains. The number of GPOs that AGPM manages is typically not a factor in the level of management centralization.

### Centralized Configuration

The centralized configuration assumes a single computer running AGPM Server and one or more client computers running the AGPM Client. Figure 1 provides an example of the centralized configuration, in which one AGPM Server is serving multiple domains.



Figure 1. Example of the centralized configuration

Select the centralized configuration when:

* The Active Directory® Domain Services (AD DS) infrastructure includes a single forest.
* Availability and scalability do not require more than one computer running AGPM Server.

**Note**   One AGPM Server can support large workloads and is sufficient for most scenarios if the other centralized configuration selection criteria are met. You are unlikely to need more than one AGPM Server to meet scaling requirements.

* High-speed and reliable network connectivity exists between domains, the AGPM Server, and the AGPM Clients.

### Decentralized Configuration

The decentralized configuration assumes that more than one computer is running AGPM Server. Figure 2 provides an example of the decentralized configuration, in which some AGPM Servers are serving multiple domains while other AGPM Servers each serve only one domain, respectively.

**Note**   Ensure that each domain is served by only one AGPM Server. Do not allow multiple AGPM Servers to serve the same domain.



Figure 2. Example of the decentralized configuration

Select the decentralized configuration when:

* The AD DS infrastructure includes multiple forests.

**Note**   An AGPM Server can only serve multiple domains within a forest. An AGPM Server cannot serve multiple domains in different forests.

* Availability and scalability require more than one computer running AGPM Server.

**Note**   One AGPM Server can support large workloads and is sufficient for most scenarios if the other centralized configuration selection criteria are met. You are unlikely to need more than one AGPM Server to meet scaling requirements.

* The network connectivity between sites is slow or erratic, which requires an AGPM Server to be placed in each site.

## Manage Group Policy in Extranets

Most organizations have extranets as a part of their network infrastructure. These extranets are also known as perimeter networks or demilitarized zones (DMZs). In some extranets, organizations deploy an AD DS forest dedicated to managing the identities and computers in the extranet. These domains also have the same Group Policy management issues.

These extranet forests are intentionally isolated from the private forests in the intranet for security reasons. Because the extranet forests are isolated, you must deploy at least one AGPM Server and AGPM Client to manage the Group Policy settings in the extranet forest.

You deploy AGPM Server on at least one member server or domain controller in the extranet. You deploy the AGPM Client on the computers that are currently used to manage the extranet forest, which can be in the extranet or within the intranet.

If you deploy the AGPM Client on a computer in the intranet, you must enable intermediary firewall ports for AGPM. By default, the AGPM Server and AGPM Client communicate by using TCP port 4600. You must enable TCP port 4600 on any intermediary firewalls between the AGPM Server and AGPM Client. The firewall rule should allow the traffic to originate in the internal network to the AGPM Server, and then allow the AGPM Server to reply to the return port based on a stateful rule.

**Note**   If you change the default TCP port that AGPM communications use during the installation process, enable that TCP port instead of the default TCP port 4600.

# Planning a Basic AGPM Deployment

Planning the basics of an AGPM deployment depends on the deployment scenario you selected earlier in the planning process. In the single-server scenario, the planning process for deploying AGPM is relatively uncomplicated: You identify the computer that will run AGPM Server and the client computers that will run AGPM Client. For the multiple-server scenario, the AGPM planning process is more complex.

**Note**   While the planning process for deploying AGPM for the single-server scenario is relatively uncomplicated, planning the Group Policy settings that AGPM will manage requires more extensive planning.

For either the single-server or multiple-server scenario, you need to plan the basics for your AGPM deployment. To plan a basic AGPM deployment, perform the following steps:

1. Collect necessary information about your existing AD DS infrastructure and GPOs.
2. Determine the number of AGPM Servers to deploy.
3. Determine the number of AGPM Clients to deploy.
4. Identify the user accounts required for deployment.
5. Select the Simple Mail Transfer Protocol (SMTP) server for e-mail notification.
6. Determine the location and storage requirements for the AGPM archive.
7. Ensure that target computers meet installation requirements.
8. Plan an AGPM Server backup strategy.

## Collect Necessary Information About the Existing AD DS Infrastructure and GPOs

As the first step in planning your AGPM deployment, collect all the pertinent information about your existing AD DS infrastructure and the GPOs. In some instances, this information already exists as a part of your documentation. If the information does not exist, gather this information for the planning process. The required information is listed in Table 1.

Table 1. Information to Collect About the Existing AD DS Infrastructure and GPOs

|  |  |
| --- | --- |
| Information collected | Helps you determine the: |
| Number of AD DS forests | Number of AGPM Servers. |
| Whether network connectivity issues exist between some domains | Number of AGPM Servers. |
| Level of centralization of administration | Number of AGPM Servers. |
| GPOs in each domain | Number of GPOs to manage using AGPM. |
| IT pros who:* Manage access to GPOs.
* Edit GPOs.
* Approve GPO creation, deployment, and deletion.
* Require Read-only access to information about GPOs.
 | AGPM roles to be assigned to each user and who requires AGPM Client. |

## Determine the Number of AGPM Servers Required

In the single-server scenario, only one AGPM Server is deployed, which means the one AGPM Server manages the GPOs for all the domains in a single forest. In the multiple-server scenario, you deploy two or more computers running AGPM Server in your environment.

You can deploy AGPM Server on a member server or a domain controller. Installing AGPM Server installs the AGPM Service on the computer. For information on the AGPM Server installation requirements, see “AGPM Server Installation Requirements,” later in this guide.

In the multiple-server scenario, deploy a separate AGPM Server for:

* Each forest in your AD DS infrastructure.
* Each site that is isolated by network connectivity issues.
* Each site that your organization’s structure requires to be managed separately.

**Note**   At this step in the planning process, you are concerned only with the number of AGPM Servers required to support your environment. Deploying additional AGPM Servers for availability and scalability is discussed later in this guide.

## Determine the Number of AGPM Clients Required

In either the single-server or multiple-server scenario, you deploy one or more AGPM Clients. Deploy the AGPM Client on every computer used to administer GPOs. For information on the AGPM Client installation requirements, see “AGPM Client Installation Requirements” later in this guide.

## Determine the User Accounts Required for Deployment

Before you begin the AGPM Server installation process, create the AGPM Service Account and determine which account will become the Archive Owner account, as listed in Table 2. These accounts must exist prior to deployment of the AGPM Server.

Table 2. Accounts to Create Prior to AGPM Server Deployment

| Account | Description |
| --- | --- |
| AGPM Service Account | This user account provides the identity for the AGPM Service. This account must also be a member of the local Administrators group on the computer on which AGPM is deployed, unless the computer is a domain controller. While you can make the account a member of the Domain Admins security group, the minimum privileges required for the AGPM Service Account include:* Membership in the Group Policy Creator Owners group in each domain the AGPM Server manages.
* Membership in the Backup Operators group in each domain the AGPM Server manages.

The AGPM Service Account also requires the following permissions* Full Control permission on the AGPM archive folder, which is automatically granted during the installation of AGPM Server if the folder is on a local drive.
* Full Control permission on the local system temp folder, which is typically %windir%\temp.
* Full Control permission on any existing GPOs that AGPM will manage.
 |
| Archive Owner | This user or group account is initially assigned the AGPM Administrator role. This account can subsequently assign other AGPM roles and permissions to other Group Policy administrators. |

In addition to the accounts listed in Table 2, you should create groups for each AGPM role and add users to those groups. Doing so reduces the complexity of AGPM role administration tasks. For more information on AGPM roles, see “Select the Appropriate Security Roles” later in this guide.

## Determine the E-mail Infrastructure Requirements

During configuration of the AGPM Server connection, you should specify the fully qualified domain name (FQDN) of a computer running SMTP. This computer can be the SMTP service running on the same computer as Microsoft Exchange Server, or it can be an SMTP relay that forwards e-mail messages to your messaging infrastructure.

Additional e-mail infrastructure planning considerations exist:

* If the SMTP servers restrict message relaying to a specific list of computers or IP addresses, you must add each AGPM Server to the list of approved computers or IP addresses.
* If there are intervening firewalls between the AGPM Servers and the SMTP servers, you may need to modify the firewall rules to allow SMTP traffic from the AGPM Servers.

## Determine the AGPM Archive Location and Storage Requirements

AGPM stores the current and previous versions of GPOs in the AGPM archive. The default path for the AGPM archive is %ProgramData%\Microsoft\AGPM on the AGPM Server. Beneath this folder is a subfolder for each GPO stored in the archive.

You can configure the AGPM Service to store the archive in a different path, even on another computer. For example, you may want to store the archive on a volume that is located on a Storage Area Network (SAN) logical unit (LUN) or on a local disk that has greater capacity than the system disk. To calculate the storage requirements for the AGPM archive, use the following calculation:

Storage\_Requrements=Avg\_GPO\_Size \* Num\_GPO \* Num\_Ver

Table 3 lists the variables in the equation listed above and provides a brief description of each. Perform this calculation for each AGPM Server in your plan.

Table 3. Variables for Calculating AGPM Archive Storage Requirements

|  |  |
| --- | --- |
| Variable | Description |
| Avg\_GPO\_Size | The average size of the GPOs in your environment; for most GPOs, you can use a value of 64 kilobytes (KB) for each GPO. |
| Num\_GPO | The number of GPOs in your current production environment that this AGPM Server will manage. |
| Num\_Ver | The number of GPO versions retained in the archive; you can configure the maximum number of versions to retain in the archive (by default, AGPM retains all GPO versions).  |

For most modern computers, the storage requirements for the AGPM archive are negligible. However, you can reduce the storage requirements by limiting the number of GPO versions retained. You can specify a range of 0–999 versions. If you specify a value of 0, only the current GPO version is retained in the archive. Although each organization will vary, retaining the last 10 versions in the AGPM archive is a recommended initial configuration value. Then, you can adjust the number of version retained in the archive based on your experience in your organization. For more information on how to limit the number of GPO versions stored, see “Limit the GPO Versions Stored” in Microsoft Advanced Group Policy Management Help.

## Ensure That Computers Meet Installation Requirements

As a part of the planning process for all AGPM deployments, ensure that the computers on which AGPM Server and AGPM Client are deployed meet or exceed the installation requirements.

### AGPM Server Installation Requirements

AGPM Server 3.0 can be installed on 32-bit or 64-bit versions of Windows Server 2008 or Windows Vista® with Service Pack 1 (SP1). However, it is a best practice recommendation to install AGPM Server 3.0 on Windows Server 2008. Install AGPM Server 3.0 when logged on as an account that is a member of the Domain Admins group. AGPM Server 3.0 has the following prerequisites:

* Group Policy Management Console (GPMC). For Windows Vista with SP1, the GPMC is included with Remote Server Administration Tools (RSAT). For Windows Server 2008, the GPMC is already installed.
* Microsoft .NET Framework version 3.5 or later, which is downloaded and installed separately.
* Windows Communication Foundation (WCF) non-HTTP activation.
* Windows Process Activation Service (WAS):
* Process model
* Microsoft .NET Environment
* Configuration application programming interfaces (APIs)

For more information on AGPM Server installation, see Step-by-Step Guide for AGPM 3.0.

### AGPM Client Installation Requirements

AGPM Client 3.0 is installed on each computer used to administer GPOs. You do not need to install AGPM Client on user computers. AGPM Client 3.0 can be installed on 32-bit or 64-bit versions of Windows Server 2008 or Windows Vista with SP1 and requires the following Windows features:

* **GPMC.** For Windows Vista with SP1, the GPMC is included with RSAT. For Windows Server 2008, the GPMC is already installed.
* **Microsoft .NET Framework version 3.0 or later.** This is automatically installed if not previously installed.

**Note**   AGPM Client can also be installed on the same computer as AGPM Server.

For more information on AGPM Client installation, see Step-by-Step Guide for AGPM 3.0.

## Plan an AGPM Server Backup Strategy

Performing regular and frequent backups of the AGPM Server and the AGPM archive is essential to the continued operation of AGPM in the event of a complete failure of an existing AGPM Server or the computer on which the AGPM archive resides. The AGPM information that needs to be protected includes the:

* **AGPM archive**. The AGPM archive contains the GPOs that the AGPM Server manages. The default path for the AGPM archive is %ProgramData%\Microsoft\AGPM on the AGPM Server.
* **AGPM Server configuration**. The configuration settings for AGPM Servers—such as the SMTP configuration and TCP port that the AGPM Server uses—are stored in the registry.

Backing up the AGPM Server helps ensure the continued operation of AGPM. Create a backup plan that includes the following:

* Back up the entire AGPM Server after initial installation, after applying any service pack or updates, or after assigning AGPM roles.
* If the AGPM archive is stored on a computer other than on which the AGPM Server is installed, back up the AGPM archive after initial installation, after applying any service pack or updates, or after assigning AGPM roles.
* Back up the AGPM archive after making updates to GPOs.

# Planning AGPM Security

From an installation perspective, AGPM is installed in as secure a configuration as possible by default. After the initial installation, you configure AGPM to meet the requirements of your organization. As you plan the configuration of your AGPM deployment, include the appropriate security decisions that will help ensure that your AGPM deployment stays secure.

To plan the security of your AGPM deployment, perform the following steps:

1. Assign the appropriate security roles to Group Policy administrators.
2. Secure the service account used by the AGPM Service running on each AGPM Server.
3. Secure the AGPM archive.
4. Secure the communication between AGPM Clients and AGPM Servers.
5. Harden computers running AGPM Server.

## Assign the Appropriate Security Roles

AGPM provides comprehensive, easy-to-use, role-based delegation. It includes domain-level permissions that allow you to provide access to all GPOs throughout a domain and GPO-level delegation that allows you to configure access to specific GPOs. Table 4 lists the roles in AGPM and provides a brief description of each.

Table 4. AGPM Roles and Descriptions

|  |  |
| --- | --- |
| Role | Description |
| AGPM Administrator (Full Control) | This role includes the permissions for all other roles and has full control of the AGPM environment. An AGPM Administrator can assign any role to other Group Policy administrators, including the AGPM Administrator role. By default, the archive owner (specified during the AGPM Server installation process) is assigned this role. |
| Approver | This role approves changes to the GPOs by users assigned the Editor role and deploys the GPOs to the production environment. |
| Editor | This role modifies the GPOs. Any modifications must be approved by a user assigned the Approver role before they are deployed into the production environment. |
| Reviewer | This role views the GPO settings in reports. All other roles include the permissions in this role. |

As a best practice, create security groups in AD DS, and assign the AGPM roles to the security groups. Then, make Group Policy administrators members of the appropriate groups to help reduce the complexity of AGPM administration. The roles listed in Table 4 are assigned a predefined set of individual permissions to perform each role. These permissions are listed in Table 5.

Table 5. AGPM Permissions and Descriptions

| Permission | Description |
| --- | --- |
| Full Control | Includes all the other permissions. |
| Create GPO | Create GPOs in the domain. |
| List Contents | List the GPOs in a domain. |
| Read Settings | Read the Group Policy settings within a GPO. |
| Edit Settings | Modify the Group Policy settings within a GPO. |
| Delete GPO | Delete a GPO. |
| Modify Security | Delegate domain-level access, access to an individual GPO, and access to the production environment. |
| Deploy GPO | Deploy a GPO from the AGPM archive to the production environment. |
| Create Template | Create an AGPM template. |
| Modify Options | Configure AGPM e-mail notification, and limit the GPO versions stored in the archive. |

Table 6 lists the AGPM roles and the individual AGPM permissions assigned to each role. The existing AGPM roles are sufficient for most environments. However, you can fully customize the security by allowing or denying the individual permission listed in Table 5 to a user or security group.

Table 6. AGPM Roles and Individual AGPM Permissions

| Role | Includes these AGPM permission |
| --- | --- |
| AGPM Administrator(Full Control) | List ContentsRead SettingsEdit SettingsCreate GPODeploy GPODelete GPOModify OptionsModify SecurityCreate Template |
| Approver | List ContentsRead SettingsCreate GPODeploy GPODelete GPO |
| Editor | List ContentsRead SettingsEdit SettingsCreate Template |
| Reviewer | List ContentsRead Settings |

You can assign AGPM roles and permissions at a domain level or to individual GPOs. AGPM roles or permissions assigned at the domain level are automatically inherited by all GPOs in the domain. AGPM roles or permissions assigned to individual GPOs override domain-level settings.

You assign:

* Domain-level AGPM roles and permissions on the **Domain Delegation** tab in the Change Control folder. For more information on how to do this, see “Delegate Doman-Level Access” in Microsoft Advanced Group Policy Management Help.
* GPO-level AGPM roles and permissions on the **Controlled** tab on the **Contents** tab in the Change Control folder. For more information on how to do this, see “Delegate Access to an Individual GPO” in Microsoft Advanced Group Policy Management Help.

Use the following recommendations when planning your security roles:

* **Use the principle of least privilege.** When planning which AGPM roles or permissions to assign to users, use the principle of least privilege. This principle means that you assign the lowest permission set possible required to perform a task. For example, if a user only needs to view GPOs, assign the user the Reviewer role. Although the other roles include the ability to view GPOs, they also include other permissions and may allow unintentional configuration changes.
* **Limit the number of users assigned the AGPM Administrator role.** Because the AGPM Administrator role is a highly privileged role, grant this role to only a few users.
* **Perform regular security audits of the AGPM roles.** Doing so helps ensure that only authorized users or groups are assigned these roles. Review the higher-privilege roles frequently to ensure that the assignment of these roles is tightly controlled.

## Secure the AGPM Service Account

The AGPM Service runs on any computer on which the AGPM Server is installed. During the installation process, you provide an account that is used as the identity for the AGPM Service. The account must have the permissions and rights listed in Table 2 for the each domain the AGPM Server manages.

Because of the elevated privileges of this account, include the following recommendations in your plan:

* **Use stronger passwords.** Users should never interactively log on using the AGPM Service account. To increase the security of the account, create a password that is stronger by:
* **Increasing the length of the password.** Increasing the length of the password helps make the password more resilient to brute force attack methods.
* **Increasing the complexity of the password.** Use a combination of all character types in the password, including uppercase letters, lowercase letters, special characters, and numbers. This also helps make the password more resistant to brute force attack methods.
* **Use fine-grained password policies.** In Windows Server 2008, you can specify a different set of password policies for accounts. Create a fine-grained password policy that you apply to the AGPM Service account. This policy will help protect the password from being compromised. For more information on fine-grained password policies, see “AD DS: Fine-Grained Password Policies” at <http://technet.microsoft.com/en-us/library/cc770394.aspx>.

**Note**   To use fine-grained password polices, the forest must be operating at the Windows Server 2008 functional level.

* **Restrict the account to log on only as a service.** The AGPM Service account should never be used to log on interactively. Change the rights for this account so that it can only log on as a service and not log on interactively. You can configure these user rights in a GPO in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment folder with the following respective Group Policy settings:
* Log on as a service
* Deny log on locally

## Secure the AGPM Archive

By default, the AGPM archive is stored on a local hard disk of the AGPM Server computer. However, the AGPM archive can be stored on a computer other than the AGPM Server. The default path for the AGPM archive is %ProgramData%\Microsoft\AGPM. Beneath this folder is a subfolder for each GPO stored in the archive. The default installation of AGPM allows file system access to the AGPM Service Account, SYSTEM account, and Administrators group. The AGPM administration interface allows you to control access to the archive. By default, the AGPM Administrator role is the only role that has full control of the archive.

Because of the sensitivity of the information stored in the AGPM archive, include the following recommendations in your plan:

* **Limit the number of users who are members of the Administrators group.** Because members of the Administrators group have full control of the archive, limit the membership of this group to a small number of trusted users. This membership will also include all members of the Domain Admins group.
* **Periodically audit the permissions of the archive and remove unauthorized permissions.** As a part of your ongoing security plan, periodically review the list of permissions on the archive to ensure that no unauthorized permissions have been added. If during your audit you discover an unauthorized set of permissions, remove the permissions immediately and report a potential security problem to the security director of your organization. Only the AGPM Service Account, SYSTEM account, and Administrators group should have permissions to the archive. You can configure the auditing by using Group Policy settings in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy folder and by enabling auditing on the AGPM archive. For more information on how to enable auditing on files for folders, see “Apply or Modify Auditing Policy Settings for a Local File or Folder” in Windows Server Help.

## Secure AGPM Communication

The AGPM Server communicates with the AGPM Clients, AD DS domain controllers, and the SMTP server that delivers e-mail notifications. To help prevent unauthorized users from viewing the communication, encrypt all communication among the AGPM Server, the AGPM Clients, domain controllers, and the SMTP server.

Encrypt AGPM communications by using:

* **Internet Protocol Security (IPsec).** Use IPsec to encrypt communication between the AGPM Server and all other computers. IPsec encrypts all traffic and is transparent to higher-level protocols.
* **Secure SMTP.** Use secure SMTP to secure the communication between the AGPM Server and the SMTP server. Secure SMTP only requires a certificate for the encryption, which can come from your organizations’ public key infrastructure (PKI) or from public certificate companies. For more information, see “Configure E-Mail Security for AGPM” in Microsoft Advanced Group Policy Management Help.

## Harden Computers Running AGPM Server

The default installation of Windows Server 2008 and AGPM Server installs AGPM Server in as secure a configuration as possible. Table 7 describes the security footprint for the AGPM Server, which helps you identify how Windows Server 2008 is modified after the installation of AGPM Server. You can use this information to identify unauthorized services, firewall rules, or files on the AGPM Server.

Table 7. AGPM Server Security Footprint

| Installation change | Description |
| --- | --- |
| Services | The AGPM Service is installed as a part of the AGPM Server installation process. By default, the AGPM Service has the following configuration:**Service name:** AGPM Service**Display name:** AGPM Service**Path to executable:** %ProgramFiles%\Microsoft\AGPM\Server\Agpm.exe**Startup:** Automatic (Delayed Start)**Log on as:** Account specified during installation |
| Windows Firewall | The AGPM Server installation process creates and enables an inbound Windows Firewall rule that allows the AGPM Client to communicate with the AGPM Server. By default, the Windows Firewall rule created has the following configuration:**Name:** AGPM Service**Action:** Allow the connection**Programs:** All programs that meet the specified conditions**Protocol type:** TCP**Local port:** 4600**Remote port:** All ports**Local IP address:** Any**Remote IP address:** Any |
| File system | The AGPM Server installation process creates folders and files on the local file system. The default installation folder for AGPM is %ProgramFiles%\Microsoft\AGPM. There is a subfolder beneath the AGPM folder for the AGPM Client and the AGPM Server. The folders and files created are as follows (where language is the language of AGPM installed:%ProgramFiles%\Microsoft\AGPM\Client\agpm.chmagpm.dllgpmctabs.dllMicrosoft.Agpm.Client.dllMicrosoft.Agpm.Client.Interop.dllMicrosoft.Agpm.Common.dll%ProgramFiles%\Microsoft\AGPM\Client\<*language*>agpm.dll.muigpmctabs.dll.muiMicrosoft.Agpm.Client.resources.dllMicrosoft.Agpm.Common.resources.dll%ProgramFiles%\Microsoft\AGPM\Server\agpm.exeagpm.exe.configAgpmPerfCounters.manMicrosoft.Agpm.Common.dllMicrosoft.Agpm.GroupPolicy.Interop.dllMicrosoft.Agpm.Server.dllMicrosoft.Agpm.Utils.dllUpgrade.exe%ProgramFiles%\Microsoft\AGPM\Server\<*language*>Upgrade.resources.dllMicrosoft.Agpm.Utils.dll.muiMicrosoft.Agpm.Server.resources.dllMicrosoft.Agpm.Common.resources.dllAgpm.resources.dll  |

You can harden the security of AGPM by following these recommendations when planning AGPM deployment:

* **Dedicate a computer to AGPM Server.** Doing so helps reduce the attack surface of the computer running AGPM Server. If you install additional Windows Server 2008 server roles, role services, or features not required by AGPM Server on the same computer as AGPM Server, you increase the attack surface of the computer. Ensure that you install only the required software on a computer dedicated to AGPM Server. For more information about the AGPM Server required software, see “Ensure That Computers Meet Installation Requirements” earlier in this guide.

**Note:** If the AGPM archive is stored on a computer other than the AGPM Server, consider dedicating that computer to only storing the AGPM archive.

* **Physically secure the AGPM Server.** If an unauthorized person has physical access to the AGPM Server, he or she can carry out many attacks that can compromise the AGPM Server. To prevent unauthorized access to the AGPM Server, perform one or more of the following tasks:
* Place the computer in a lockable server rack.
* Place the computer in a secured data center (larger organizations) or in a locked computer closet or wiring closet (smaller organizations).
* Disable the DVD or CD drive in the computer to prevent installation of unauthorized software.
* Disable any USB ports to prevent connection of removable devices.

**Note:** If the AGPM archive is stored on a computer other than the AGPM Server, use the same methods for physically securing the computer on which the AGPM archive is stored.

* **Enable Windows BitLocker™ Drive Encryption.** Encrypting the local disks on the AGPM Server prevents unauthorized access to AGPM information in the event that a hard disk or the entire computer is stolen. Windows BitLocker Drive Encryption keys are required to start the computer and to access the information on the local hard disks.

**Note:** If the AGPM archive is stored on a computer other than the AGPM Server, consider securing the computer on which the AGPM archive is stored by using Windows BitLocker Drive Encryption.

# Planning for AGPM Scaling

With the advances in today’s computer system resources, a single, dedicated AGPM Server could potentially serve any size organization. Typically, there is a need for additional AGPM Servers for other reasons, such as:

* Managing an isolated extranet forest.
* Decentralized management of AGPM.
* Slow or erratic connectivity between sites.

To help ensure that your AGPM Server can adequately serve your organization, include the following recommendations in your plan:

* **Dedicate a computer to running AGPM Server.** In this way, AGPM Server can fully use the computer’s system resources and not compete with other software. In addition, this helps reduce the attack surface of the AGPM Server.
* **Increase the system resources of the computer running AGPM Server.** This allows the AGPM Server to support more simultaneous Group Policy administrators and to manage more domains. Typical system resources to increase include the:
* Number and speed of processors.
* Capacity of physical memory.
* Number and speed of network adapters (including teamed network adapters).
* Capacity and speed of disk storage.

# Upgrading from Previous Versions of AGPM

You can upgrade existing AGPM 2.5 deployments to AGPM 3.0. As a part of the migration process, you must upgrade the operating system and software prior to upgrading to AGPM 3.0. In addition, you must upgrade both the AGPM Servers and AGPM Clients to AGPM 3.0. AGPM 2.5 Clients and Servers cannot work with AGPM 3.0 Clients and Servers. You can upgrade the AGPM Clients or AGPM Servers in any order.

For example, you can upgrade:

* All the AGPM Clients first, then upgrade all the AGPM Servers.
* All the AGPM Servers first, then upgrade all the AGPM Clients.
* AGPM Servers and Clients in logical groupings (upgrade an AGPM Server, then upgrade all the Clients that access that server).

## Upgrade AGPM Server

This process assumes that you are upgrading a computer running AGPM Server 2.5 on Windows Server 2003. To upgrade a computer running AGPM Server 2.5 to AGPM 3.0, follow this process:

1. Ensure that the existing AGPM 2.5 solution is functioning properly.
2. Upgrade Windows Server 2003 to Windows Server 2008. (For more information about upgrading to Windows Server 2008, see “Upgrading to Windows Server 2008” at <http://technet.microsoft.com/en-us/library/cc754728.aspx>.)
3. Ensure that the required software is installed. (For more information, see the section, “AGPM Server Installation Requirements,” earlier in this guide.)
4. Upgrade AGPM Server 2.5 to AGPM Server 3.0:
5. Install AGPM 3.0 on the computer.
6. Open a Command Prompt window with Administrator-level permissions.
7. Navigate to the %ProgramFiles%\Microsoft\AGPM\Server folder.
8. In a Command Prompt window, run:

upgrade.exe archive\_path

(where archive\_path is the fully qualified path to the AGPM 2.5 Extensible Markup Language (XML) archive index. The default path for the XML archive index is %ProgramData%\Microsoft\AGPM).

## Upgrade the AGPM Client

This process assumes that you are upgrading a computer running AGPM Client 2.5 on Windows Vista without SP1. To upgrade a computer running AGPM Client 2.5 to AGPM Client 3.0, follow this process:

1. Ensure that the existing AGPM 2.5 solution is functioning properly.
2. Install Windows Vista SP1.
3. Ensure that the required software is installed. (For more information, see the section, “AGPM Client Installation Requirements,” earlier in this guide.)
4. Install AGPM Client 3.0 on the computer.

# Summary

AGPM can help any size organization manage GPOs more securely and efficiently than by using only the GPMC. AGPM allows you to delegate Group Policy administration based on roles for the tasks that Group Policy administrators perform. AGPM also allows you to delegate Group Policy administration at a domain level and at a GPO level so that you can allow different administrators to manage different GPOs.

In addition, AGPM allows you to control the version of GPOs deployed from the GPO archive to your production environment. This level of control allows you to keep a record of changes to each GPO and to revert a current GPO to a previous GPO in the event of a problem with a change to a Group Policy setting.

With AGPM, you reduce the risks associated with deploying GPOs as well as the ongoing support costs for managing GPOs. This helps your organization focus on managing the mission-critical applications and services in your production environment instead of focusing on GPO change-management processes and security.

# For More Information

* **Microsoft Advanced Group Policy Management** at <http://www.microsoft.com/windows/products/windowsvista/enterprise/agpm.mspx>
* **Advanced Group Policy Management Overview** at <http://www.microsoft.com/downloads/details.aspx?FamilyID=993a34d0-c274-4b46-b9fc-568426b81c5e&DisplayLang=en>
* Microsoft TechNet’s **Advanced Group Policy Management** at <http://technet.microsoft.com/en-us/library/bb895887.aspx>