Microsoft®
Advanced Group Policy Management

Operations Guide for Microsoft Advanced Group Policy Management 2.5

Microsoft Corporation

Published: May 2007

Abstract

This guide provides step-by-step instructions for performing tasks using Microsoft Advanced Group Policy Management 2.5. This information is also provided in the AGPM Help included with the product.

Microsoft

Copyright

Contents

Operations Guide for Microsoft Advanced Group Policy Management 2.5 5
Overview of Advanced Group Policy Management 5
Checklist: Create, Edit, and Deploy a GPO 7
Performing AGPM Administrator Tasks 7
Configure the AGPM Server Connection 8
Configure E-Mail Notification 11
Delegate Domain-Level Access 12
Delegate Access to an Individual GPO 13
Configure Logging and Tracing 14
Managing the AGPM Service 15
Start and Stop the AGPM Service 15
Modify the Archive Path 16
Modify the AGPM Service Account 17
Modify the Port on Which the AGPM Service Listens 18
Performing Editor Tasks 18
Creating, Controlling, or Importing a GPO 19
Request Control of a Previously Uncontrolled GPO 19
Request the Creation of a New Controlled GPO 20
Import a GPO from Production 21
Editing a GPO 22
Edit a GPO Offline 22
Use a Test Environment 24
Request Deployment of a GPO 24
Label the Current Version of a GPO 25
Rename a GPO or Template 25
Creating a Template and Setting a Default Template 26
Create a Template 27
Set a Default Template 27
Delete a GPO 28
Performing Approver Tasks 29
Approve or Reject a Pending Action 30
Creating, Controlling, or Importing a GPO 31
Control a Previously Uncontrolled GPO 31
Create a New Controlled GPO 32
Delegate Access to a GPO 33
Import a GPO from Production 33
Check In a GPO 34
Deploy a GPO 35
Roll Back to a Previous Version of a GPO 36

Deleting, Restoring, or Destroying a GPO 36
Delete a GPO 37
Restore a Deleted GPO 38
Destroy a GPO 38
Performing Reviewer Tasks 39
Configure the AGPM Server Connection 39
Review GPO Settings 40
Review GPO Links 41
Identify Differences Between GPOs, GPO Versions, or Templates 42
Troubleshooting Advanced Group Policy Management 44
User Interface: Advanced Group Policy Management 46
Contents Tab 47
Controlled Tab 47
Uncontrolled Tab 50
Pending Tab 51
Templates Tab 53
Recycle Bin Tab 54
Common Secondary Tab Features 56
History Window 58
Domain Delegation Tab 60
AGPM Server Tab 62
Administrative Template Settings 62
Logging and Tracing Settings 62
AGPM Server Connection Settings 63
Feature Visibility Settings 64
Other Enhancements to the GPMC 65

Operations Guide for Microsoft Advanced Group Policy Management 2.5

You can use Microsoft Advanced Group Policy Management (AGPM) to extend the capabilities of the Group Policy Management Console (GPMC), providing comprehensive change control and enhanced management for Group Policy objects (GPOs).

With AGPM you can:

- Perform offline editing of GPOs, so you can create and test them before deploying to a production environment.
- Retain multiple versions of a GPO in a central archive, so you can roll back if a problem occurs.
- Share the responsibility for editing, approving, and reviewing GPOs among multiple people using role-based delegation.
- Eliminate the danger of multiple Group Policy administrators overwriting each other's work by using a check-in/check-out capability for GPOs.
- Analyze changes to a GPO, comparing it to another GPO or another version of the same GPO using difference reporting.
- Simplify the creation of new GPOs by using GPO templates, storing standard settings to use as starting points for new GPOs.

AGPM adds a **Change Control** node under each domain displayed in the GPMC, as well as **History** and **Extensions** tabs for each GPO and Group Policy link displayed in the GPMC.

- Overview of Advanced Group Policy Management
- Checklist: Create, Edit, and Deploy a GPO
- Performing AGPM Administrator Tasks
- Performing Editor Tasks
- Performing Approver Tasks
- Performing Reviewer Tasks
- Troubleshooting Advanced Group Policy Management
- User Interface: Advanced Group Policy Management

Overview of Advanced Group Policy Management

You can use Advanced Group Policy Management (AGPM) to extend the capabilities of the Group Policy Management Console (GPMC), providing comprehensive change control and enhanced management for Group Policy objects (GPOs).

Group Policy object development with change control

With AGPM, you can store a copy of each GPO in a central archive, so Group Policy administrators can view and modify it offline without immediately impacting the deployed version of the GPO. Additionally, AGPM stores a copy of each version of each controlled GPO in the archive so that you can roll back to an earlier version if needed.

The terms "check in" and "check out" are used in much the same way as in a library (or in applications that provide change control, version control, or source code control for programming development). To use a book that is in a library, you check it out from the library. No one else can use it while you have it checked out. When you are finished with the book, you check it back into the library, so others can use it.

When developing GPOs using AGPM:

1. Create a new controlled GPO or control a previously uncontrolled GPO.
2. Check out the GPO, so you and only you can modify it.
3. Edit the GPO.
4. Check in the edited GPO, so others can modify it, or so it can be deployed.
5. Review the changes.
6. Deploy the GPO to the production environment.

Role-based delegation

AGPM provides comprehensive, easy-to-use role-based delegation. Domain-level permissions allow AGPM Administrators to provide access to individual domains without providing access to other domains. GPO-based delegation enables AGPM Administrators to allow access only to specific GPOs.

Within AGPM, there are specifically defined roles: AGPM Administrator (Full Control), Approver, Editor, and Reviewer. The AGPM Administrator role includes the permissions for all other roles. By default, only Approvers have the power to deploy GPOs to the production environment, protecting the environment from inadvertent mistakes by less experienced Editors. Also by default, all roles include the Reviewer role and therefore the ability to view GPO settings in reports. However, AGPM provides an AGPM Administrator with the flexibility to customize GPO access to fit the needs of your organization.

Delegation in a multiple Group Policy administrator environment

In an environment where multiple people make changes to GPOs, an AGPM Administrator delegates permission to Editors, Approvers, and Reviewers, either as groups or as individuals. For a typical GPO development process for an Editor and an Approver, see Checklist: Create, Edit, and Deploy a GPO.

Additional references

- Checklist: Create, Edit, and Deploy a GPO
- Performing AGPM Administrator Tasks

- Performing Editor Tasks
- Performing Approver Tasks
- Performing Reviewer Tasks
- Troubleshooting Advanced Group Policy Management
- User Interface: Advanced Group Policy Management

Checklist: Create, Edit, and Deploy a GPO

In an environment where multiple people make changes to Group Policy objects (GPOs), an AGPM Administrator (Full Control) delegates permission to Editors, Approvers, and Reviewers, either as groups or as individuals. The following is a typical GPO development process for an Editor and an Approver.

Task	Reference
Editor requests the creation of a new GPO or an Approver creates a new GPO.	Request the Creation of a New Controlled GPO Create a New Controlled GPO
Approver approves the creation of the GPO if it was requested by an Editor.	Approve or Reject a Pending Action
Editor checks out a copy of the GPO from the archive, so no one else can modify the GPO. Editor makes changes to the GPO, and then checks the modified GPO into the archive.	Edit a GPO Offline
Editor requests deployment of the GPO to the production environment.	Request Deployment of a GPO
Reviewers, such as Approvers or Editors, analyze the GPO.	Performing Reviewer Tasks
Approver approves and deploys the GPO to the production environment or rejects the GPO.	Approve or Reject a Pending Action

Performing AGPM Administrator Tasks

An AGPM Administrator (Full Control) configures domain-wide options and delegates permissions to Approvers, Editors, Reviewers, and other AGPM Administrators. By default, an AGPM Administrator is an individual with Full Control (all Advanced Group Policy Management [AGPM] permissions) and therefore can also perform tasks associated with any role.

In an environment in which multiple people develop Group Policy objects (GPOs), you can choose whether all Advanced Group Policy Management (AGPM) users perform the same tasks and have the same level of access or whether AGPM Administrators delegate permissions to

Editors who make changes to GPOs and to Approvers who deploy GPOs to the production environment. AGPM Administrators can configure permissions to meet the needs of your organization.

- Configure the AGPM Server Connection
- Configure E-Mail Notification
- Delegate Domain-Level Access
- Delegate Access to an Individual GPO
- Configure Logging and Tracing
- Managing the AGPM Service
  - Start and Stop the AGPM Service
  - Modify the Archive Path
  - Modify the AGPM Service Account
  - Modify the Port on Which the AGPM Service Listens

Also, because the AGPM Administrator role includes the permissions for all other roles, an AGPM Administrator can perform the tasks normally associated with any other role.

- Performing Approver Tasks, such as creating, deploying, or deleting GPOs
- Performing Editor Tasks, such as editing, renaming, labeling, or importing GPOs, creating templates, or setting a default template
- Performing Reviewer Tasks, such as reviewing settings and comparing GPOs

Additional considerations

By default, the AGPM Administrator role has Full Control—all AGPM permissions:

- List Contents
- Read Settings
- Edit Settings
- Create GPO
- Deploy GPO
- Delete GPO
- Modify Options
- Modify Security
- Create Template

The **Modify Options** and **Modify Security** permissions are unique to the role of AGPM Administrator.

Configure the AGPM Server Connection

Advanced Group Policy Management (AGPM) stores all versions of each controlled Group Policy object (GPO) in a central archive, so Group Policy administrators can view and modify GPOs offline without immediately impacting the deployed version of each GPO.

A user account with the AGPM Administrator (Full Control) role, the user account of the Approver who created the GPO used in these procedures, or a user account with the necessary permissions in Advanced Group Policy Management is required to complete these procedures for centrally configuring archive locations for all Group Policy administrators. Review the details in "Additional considerations" in this topic.

Configuring the AGPM Server connection

As an AGPM Administrator (Full Control), you can ensure that all Group Policy administrators connect to the same AGPM Server by centrally configuring the setting. If your environment requires separate AGPM Servers for some or all domains, configure those additional AGPM Servers as exceptions to the default. If you do not centrally configure AGPM Server connections, each Group Policy administrator must manually configure the AGPM Server to be displayed for each domain.

- Configure an AGPM Server for all Group Policy administrators
- Configure additional AGPM Servers for all Group Policy administrators
- Manually configure an AGPM Server for your account

To configure an AGPM Server for all Group Policy administrators

1. In the **Group Policy Management Console** tree, edit a GPO that is applied to all Group Policy administrators. (For more information, see Editing a GPO.)
2. In the **Group Policy Object Editor**, click **User Configuration**, **Administrative Templates**, and **Windows Components**.
3. If **AGPM** is not listed under **Windows Components**:
   a. Right-click **Administrative Templates** and click **Add/Remove Templates**.
   b. Click **Add**, select **agpm.admx** or **agpm.adm**, click **Open**, and then click **Close**.
4. Under **Windows Components**, double-click **AGPM**.
5. In the details pane, double-click **AGPM Server (all domains)**.
6. In the **AGPM Server (all domains) Properties** window, select the **Enabled** check box, and type the fully-qualified computer name and port (for example, server.contoso.com:4600).
7. Click **OK**. Unless you want to configure additional AGPM Server connections, close the **Group Policy Object Editor** and deploy the GPO. (For more information, see Deploy a GPO.) When Group Policy is updated, the AGPM Server connection is configured for all Group Policy administrators.

To configure additional AGPM Servers for all Group Policy administrators

1. If no AGPM Server connection has been configured, follow the preceding procedure to configure a default AGPM Server for all domains.
2. To configure separate AGPM Servers for some or all domains (overriding the default

AGPM Server), in the **Group Policy Management Console** tree, edit a GPO that is applied to all Group Policy administrators. (For more information, see Editing a GPO.)

3. Under **User Configuration** in the **Group Policy Object Editor**, double-click **Administrative Templates**, **Windows Components**, and then **AGPM**.
4. In the details pane, double-click **AGPM Server**.
5. In the **AGPM Server Properties** window, select the **Enabled** check box, and click **Show**.
6. In the **Show Contents** window:
   a. Click **Add**.
   b. For **Value Name**, type the domain name (for example, server1.contoso.com).
   c. For **Value**, type the AGPM Server name and port to use for this domain (for example, server2.contoso.com:4600), and then click **OK**. (By default, the AGPM Service listens on port 4600. To use a different port, see Modify the Port on Which the AGPM Service Listens.)
   d. Repeat for each domain not using the default AGPM Server.
7. Click **OK** to close the **Show Contents** and **AGPM Server Properties** windows.
8. Close the **Group Policy Object Editor**. (For more information, see Deploy a GPO.) When Group Policy is updated, the new AGPM Server connections are configured for all Group Policy administrators.

If you have centrally configured the AGPM Server connection, the option to manually it is unavailable for all Group Policy administrators.

To manually configure the AGPM Server to display for your account

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. In the details pane, click the **AGPM Server** tab.
3. Enter the fully-qualified computer name for the AGPM Server that manages the archive used for this domain (for example, server.contoso.com) and the port on which the AGPM Service listens (by default, port 4600).
4. Click **Apply**, then click **Yes** to confirm.

Additional considerations

- You must be able to edit and deploy a GPO to perform the procedures for centrally configuring AGPM Server connections for all Group Policy administrators. See Editing a GPO and Deploy a GPO for additional detail.
- The AGPM Server selected determines which GPOs are displayed on the **Contents** tab and to what location the **Domain Delegation** tab settings are applied. If not centrally managed through the Administrative Template, each Group Policy administrator must configure this setting to point to the AGPM Server for the domain.

- Membership in the Group Policy Creator Owners group should be restricted so that it is not used to circumvent the management of access to GPOs by AGPM. (In the **Group Policy Management Console**, click **Group Policy Objects** in the forest and domain in which you want to manage GPOs, click **Delegation**, and then configure the settings to meet the needs of your organization.)

Additional references

- Performing AGPM Administrator Tasks

Configure E-Mail Notification

When an Editor or a Reviewer attempts to create, deploy, or delete a Group Policy object (GPO), a request for this action is sent to a designated e-mail address or addresses so that an Approver can evaluate the request and implement or deny it. You determine the e-mail address or addresses to which notifications are sent, as well as the alias from which notifications are sent.

A user account with the AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To configure e-mail notification for AGPM

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. In the details pane, click the **Domain Delegation** tab.
3. In the **From** field, type the e-mail alias for AGPM from which notifications should be sent.
4. In the **To** field, type a comma-delimited list of e-mail addresses of Approvers who should receive requests for approval.
5. In the **SMTP server** field, type a valid SMTP mail server.
6. In the **User name** and **Password** fields, type the credentials of a user with access to the SMTP service.
7. Click **Apply**.

Additional considerations

- By default, you must be an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Modify Options** permissions for the domain.
- E-mail notification for AGPM is a domain-level setting. You can provide different Approver e-mail addresses or AGPM e-mail aliases on each domain's **Domain Delegation** tab, or use the same e-mail addresses throughout your environment.

Additional references

- Performing AGPM Administrator Tasks

Delegate Domain-Level Access

Set up delegation for your environment so Group Policy administrators have the appropriate access to and control over Group Policy objects (GPOs). There are baseline permissions you can apply to make the operation of Advanced Group Policy Management (AGPM) more efficient. You can grant permissions in any manner that meets the needs of your organization.

A user account with the AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To delegate access so users and groups have appropriate permissions to all GPOs throughout a domain

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. Click the **Domain Delegation** tab, then click the **Advanced** button.
3. In the **Permissions** dialog box, click the check box for each role to be assigned to an individual, and then click the **Advanced** button.

   Note

   Editor and Approver include Reviewer permissions.
4. In the **Advanced Security Settings** dialog box, select a Group Policy administrator, and then click **Edit**.
5. For **Apply onto**, select **This object and nested objects**, configure any special permissions beyond the standard AGPM roles, then click **OK** in the **Permission Entry** dialog box.
6. In the **Advanced Security Settings** dialog box, click **OK**.
7. In the **Permissions** dialog box, click **OK**.

Additional considerations

- By default, you must be an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **Modify Security** permission for the domain.
- To delegate read access to Group Policy administrators who use AGPM, you must grant them **List Contents** as well as **Read Settings** permissions. This enables them to view GPOs on the **Contents** tab of AGPM. Set the permission to apply to **This object and nested objects**. Other permissions must be explicitly delegated.
- Editors must be granted **Read** permission for the deployed copy of a GPO to make full use of Group Policy Software Installation.
- Membership in the Group Policy Creator Owners group should be restricted so that it is not used to circumvent AGPM management of access to GPOs. (In the **Group Policy Management Console**, click **Group Policy Objects** in the forest and domain in which you want to manage GPOs, click **Delegation**, and then configure the settings to meet the needs of your organization.)

Additional references

- Performing AGPM Administrator Tasks

Delegate Access to an Individual GPO

As an AGPM Administrator (Full Control), you can delegate the management of a controlled Group Policy object (GPO), so selected groups and Editors can edit it, Reviewers can review it, and Approvers can approve it.

A user account with the AGPM Administrator (Full Control) role, the user account of the Approver who created the GPO, or a user account with the necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To delegate the management of a controlled GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Controlled** tab to display controlled GPOs, and then click the GPO to delegate.
3. Click the **Add** button, select the users or groups to be permitted access, and then click **OK**.
4. To customize the permissions for each user or group, click the **Advanced** button on the **Contents** tab and check role permissions to allow or deny. (For more detailed control, click **Advanced** in the **Permissions** dialog box.)
5. Click **Apply**, and then click **OK** in the **Permissions** dialog box.

Additional considerations

- By default, you must be the Approver who created or controlled the GPO or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** permission for the domain and **Modify Security** permission for the GPO.
- To delegate read access to Group Policy administrators who use AGPM, you must grant them **List Contents** as well as **Read Settings** permissions. This enables them to view GPOs on the **Contents** tab of AGPM. Set the permission to apply to **This object and nested objects**. Other permissions must be explicitly delegated.
- Editors must have **Read** permission for the deployed copy of a GPO to make full use of Group Policy Software Installation.
- Membership in the Group Policy Creator Owners group should be restricted so that it is not used to circumvent AGPM management of access to GPOs. (In the **Group Policy Management Console**, click **Group Policy Objects** in the forest and domain in which you want to manage GPOs, click **Delegation**, and then configure the settings to meet the needs of your organization.)

Additional references

- Performing AGPM Administrator Tasks

Configure Logging and Tracing

You can centrally configure optional logging and tracing for Advanced Group Policy Management (AGPM) using Administrative templates.

A user account with the AGPM Administrator (Full Control) role, the user account of the Approver who created the GPO used in these procedures, or a user account with the necessary permissions in Advanced Group Policy Management is required to complete these procedures. Additionally, a user account with access to the AGPM Server is required to initiate logging on the AGPM Server. Review the details in "Additional considerations" in this topic.

To configure logging and tracing for AGPM

1. In the **Group Policy Management Console** tree, edit a GPO that is applied to all Group Policy administrators for which you want to turn on logging and tracing. (For more information, see Editing a GPO.)
2. In the **Group Policy Object Editor**, click **Computer Configuration**, **Administrative Templates**, and **Windows Components**.
3. If **AGPM** is not listed under **Windows Components**:
   a. Right-click **Administrative Templates** and click **Add/Remove Templates**.
   b. Click **Add**, select **agpm.admx** or **agpm.adm**, click **Open**, and then click **Close**.
4. Under **Windows Components**, double-click **AGPM**.
5. In the details pane, double-click **AGPM Logging**.
6. In the **AGPM Logging Properties** window, click **Enabled**, and configure the level of detail to record in the logs.
7. Click **OK**.
8. Close the **Group Policy Object Editor**. (For more information, see Deploy a GPO.) After Group Policy is updated, you must restart the AGPM Service to begin logging on the AGPM Server. Group Policy administrators must close and restart the GPMC to begin logging on their computers.

   Trace file locations:

   - Client: %LocalAppData%\Microsoft\AGPM\agpm.log
   - Server: %CommonAppData%\Microsoft\AGPM\agpmserv.log

Additional considerations

- You must be able to edit and deploy a GPO to confige AGPM logging and tracing. See Editing a GPO and Deploy a GPO for additional detail.

Additional references

- Performing AGPM Administrator Tasks

Managing the AGPM Service

The AGPM Service is a Windows service that acts as a security proxy, managing client access to Group Policy objects (GPOs) in the archive and production environment. It enforces Advanced Group Policy Management (AGPM) delegation and provides an enhanced level of security. The AGPM Service is hosted on the server on which the Microsoft Advanced Group Policy Management - Server is installed.

Caution

Do not modify settings for the AGPM Service through **Administrative Tools** and **Services** in the operating system. Doing so can prevent the AGPM Service from starting.

- Start and Stop the AGPM Service
- Modify the Archive Path
- Modify the AGPM Service Account
- Modify the Port on Which the AGPM Service Listens

Start and Stop the AGPM Service

The AGPM Service is a Windows service that acts as a security proxy, managing client access to Group Policy objects (GPOs) in the archive and production environment.

Important

Stopping or disabling the AGPM Service will prevent AGPM clients from performing any operations (such as listing or editing GPOs) through the server.

A user account with access to the AGPM Server (the computer on which the AGPM Service is installed) is required to complete this procedure.

To start or stop the AGPM Service

1. On the computer on which Microsoft Advanced Group Policy Management - Server (and therefore the AGPM Service) is installed, click **Start**, click **Control Panel**, click **Administrative Tools**, and then click **Services**.
2. In the list of services, right-click **AGPM Service** and select **Start**, **Restart**, or **Stop**.

   Caution

   Do not modify settings for the AGPM Service through **Administrative Tools** and **Services** in the operating system. Doing so can prevent the AGPM Service from starting. To modify settings for the service, see Managing the AGPM Service.

Additional references

- Managing the AGPM Service

Modify the Archive Path

The archive path is the location of the archive relative to the AGPM Server. The archive path can point to a folder on the AGPM Server or on another server in the same forest.

The archive path and AGPM Service Account are configured during the installation of AGPM Server and can be changed afterward through **Add or Remove Programs** on the AGPM Server.

A user account that is a member of the Domain Admins group and has access to the AGPM Server (the computer on which Microsoft Advanced Group Policy Management - Server is installed) is required to complete this procedure.

To modify the archive path

1. On the computer on which Microsoft Advanced Group Policy Management - Server is installed, click **Start**, click **Control Panel**, click **Add or Remove Programs**.
2. Click **Microsoft Advanced Group Policy Management - Server**, and then click **Change**.
3. Click **Next**, and then click **Modify**.
4. Follow the instructions on screen to configure settings for the AGPM Service:
   a. For the archive path, enter a new location for the archive relative to the AGPM Server. The archive path can point to a folder on the AGPM Server or elsewhere, but the location should have sufficient space to store all GPOs and history data managed by this AGPM Server.
   b. Enter credentials for the AGPM Service Account.

      Important
      Modifying the installation clears the credentials for the AGPM Service Account. You must re-enter credentials, but they are not required to match the credentials used during the original installation.

      The AGPM Service Account must have full access to the GPOs that it will manage. If you will be managing GPOs on a single domain, you can make the Local System account for the primary domain controller the AGPM Service Account.

      If you will be managing GPOs on multiple domains or if a member server will be the AGPM Server, you should configure a different account as the AGPM Service Account because the Local System account for one domain controller cannot access GPOs on other domains.

   c. For the archive owner, enter the credentials of an AGPM Administrator (Full Control).
5. Click **Change**, and when the installation is complete click **Finish**.

Additional references

- Managing the AGPM Service

Modify the AGPM Service Account

The AGPM Service is a Windows service that acts as a security proxy, managing client access to Group Policy objects (GPOs) in the archive and production environment. If this service is stopped or disabled, AGPM clients cannot perform operations through the server.

The archive path and AGPM Service Account are configured during the installation of AGPM Server and can be changed afterward through **Add or Remove Programs** on the AGPM Server.

Caution

Do not modify settings for the AGPM Service through **Administrative Tools** and **Services** in the operating system. Doing so can prevent the AGPM Service from starting.

A user account that is a member of the Domain Admins group and has access to the AGPM Server (the computer on which Microsoft Advanced Group Policy Management - Server is installed) is required to complete this procedure.

Important

The AGPM Service Account must have full access to the GPOs that it will manage and will be granted **Log On As A Service** permission. If you will be managing GPOs on a single domain, you can make the Local System account for the primary domain controller the AGPM Service Account.

If you will be managing GPOs on multiple domains or if a member server will be the AGPM Server, you should configure a different account as the AGPM Service Account because the Local System account for one domain controller cannot access GPOs on other domains.

To modify the AGPM Service Account

1. On the computer on which Microsoft Advanced Group Policy Management - Server is installed, click **Start**, click **Control Panel**, click **Add or Remove Programs**.
2. Click **Microsoft Advanced Group Policy Management - Server**, and then click **Change**.
3. Click **Next**, and then click **Modify**.
4. Follow the instructions on screen to configure settings for the AGPM Service:
    a. For the archive path, confirm or change the location for the archive relative to the AGPM Server. The archive path can point to a folder on the AGPM Server or elsewhere, but the location should have sufficient space to store all GPOs and history data managed by this AGPM Server.
    b. Enter new credentials for the AGPM Service Account.
    c. For the archive owner, enter the credentials of an AGPM Administrator (Full Control).
5. Click **Change**, and when the installation is complete click **Finish**.

Additional references

- Managing the AGPM Service

Modify the Port on Which the AGPM Service Listens

The AGPM Service is a Windows service that acts as a security proxy, managing client access to Group Policy objects (GPOs) in the archive and production environment. By default, the AGPM Service listens on port 4600. You can change this port by modifying the Advanced Group Policy Management (AGPM) archive index file for each archive.

Note

Before modifying the port on which the AGPM Service listens, it is recommended that you back up the AGPM archive index file (gpostate.xml). This file is located in the folder entered as the archive path during the installation of Advanced Group Policy Management - Server. By default, this location of this file is %CommonAppData%\Microsoft\AGPM\gpostate.xml on the AGPM Server. If you do not know which computer hosts the archive, you can follow the procedure for modifying the archive path to display the current archive path. For more information, see Modify the Archive Path.

A user account with access to the AGPM Server (the computer on which the AGPM Service is installed) and the archive index file is required to complete this procedure.

To modify the port on which the AGPM Service listens

1. On the computer hosting the archive, open the archive index file (gpostate.xml) in a text editor.
2. In the file, search for **agpm:port="4600"**.
3. Replace **4600** with the port on which the AGPM Service should listen; then, save and close the file.
4. On the AGPM Server, restart the AGPM Service. (For more information, see Start and Stop the AGPM Service.)
5. Modify the port in the AGPM Server connection for each Group Policy administrator. (For more information, see Configure the AGPM Server Connection.)
6. Repeat for each archive and AGPM Server.

Additional references

- Managing the AGPM Service

Performing Editor Tasks

An Editor is a person authorized by an AGPM Administrator (Full Control) to make changes to Group Policy objects (GPOs) and create GPO templates. Additionally, an Editor can initiate the process of creating or deleting a GPO, but by default must request approval from an Approver.

Important

Ensure that you are connecting to the central archive for GPOs. For more information, see Configure the AGPM Server Connection.

- Creating, Controlling, or Importing a GPO
- Editing a GPO
- Creating a Template and Setting a Default Template
- Delete a GPO

Note
Because the Editor role includes the permissions for the Reviewer role, an Editor can also review settings and compare GPOs. See Performing Reviewer Tasks for more information.

Additional considerations

By default, the following permissions are provided for the Editor role:

- List Contents
- Read Settings
- Edit Settings
- Create Template

Creating, Controlling, or Importing a GPO

To use Advanced Group Policy Management (AGPM) to provide change control for a Group Policy object (GPO), the GPO must first be controlled by AGPM. New GPOs created through the **Change Control** node will automatically be controlled. As an Editor, you may not have permission to complete the control, creation, or deletion of a GPO, but you do have the permission necessary to begin the process and submit your request to an Approver.

- Request Control of a Previously Uncontrolled GPO
- Request the Creation of a New Controlled GPO
- Import a GPO from Production

Request Control of a Previously Uncontrolled GPO

To use Advanced Group Policy Management (AGPM) to provide change control for an existing Group Policy object (GPO), the GPO must be controlled with AGPM. Unless you are an Approver or an AGPM Administrator (Full Control), you must request that the GPO be controlled.

A user account with the Editor or Reviewer role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To control a previously uncontrolled GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.

2. On the **Contents** tab in the details pane, click the **Uncontrolled** tab to display the uncontrolled GPOs.
3. Right-click the GPO to be controlled with AGPM, and then click **Control**.
4. Unless you have special permission to control GPOs, you must submit a request for control. To receive a copy of the request, type your e-mail address in the **Cc** field. Type a comment to be displayed in the **History** of the GPO, and then click **Submit**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The GPO is removed from the list on the **Uncontrolled** tab and added to the **Pending** tab. When an Approver has approved your request, the GPO will be moved to the **Controlled** tab.

Additional considerations

- By default, you must be an Editor or a Reviewer to perform this procedure. Specifically, you must have **List Contents** and **Read Settings** permissions for the domain.
- To withdraw your request before it has been approved, click the **Pending** tab. Right-click the GPO, and then click **Withdraw**. The GPO will be returned to the **Uncontrolled** tab.

Additional references

- Creating, Controlling, or Importing a GPO

Request the Creation of a New Controlled GPO

Unless you are an Approver or an AGPM Administrator (Full Control), you must request the creation of a new Group Policy object (GPO) if it is to be managed using Advanced Group Policy Management (AGPM).

A user account with the Editor or Reviewer role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To create a new GPO with change control managed through AGPM

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. Right-click the **Change Control** node, and then click **New Controlled GPO**.
3. Unless you have special permission to create GPOs, you must submit a request for creation. In the **New Controlled GPO** dialog box:
   a. To receive a copy of the request, enter your e-mail address in the **Cc** field.
   b. Type a name for the new GPO.
   c. Optional: Type a comment for the new GPO.
   d. To deploy the new GPO to the production environment immediately upon approval, click **Create live**. To create the new GPO offline without immediately deploying it upon approval, click **Create offline**.

e. Select the GPO template to use as a starting point for the new GPO.

f. Click **Submit**.

4. When the **Progress** window indicates that overall progress is complete, click **Close**. The new GPO is displayed in the list of GPOs on the **Pending** tab. When an Approver has approved your request, the GPO will be moved to the **Controlled** tab.

Additional considerations

- By default, you must be an Editor or a Reviewer to perform this procedure. Specifically, you must have **List Contents** permission for the domain.
- To withdraw your request before it has been approved, click the **Pending** tab. Right-click the GPO, then click **Withdraw**. The GPO will be destroyed.

Additional references

- Creating, Controlling, or Importing a GPO

Import a GPO from Production

If changes are made to a controlled Group Policy object (GPO) outside of Advanced Group Policy Management (AGPM), you can import a copy of the GPO from the production environment and save it to the archive to bring the archive and the production environment to a consistent state. (To import an uncontrolled GPO, control the GPO. See Request Control of a Previously Uncontrolled GPO.)

A user account with the Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To import a GPO from the production environment

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Right-click the GPO, and then click **Import from Production**.
4. Type a comment for the audit trail of the GPO, then click **OK**.

Additional considerations

- By default, you must be an Editor, Approver, or AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and either **Edit Settings**, **Deploy GPO**, or **Delete GPO** permissions for the GPO.

Additional references

- Creating, Controlling, or Importing a GPO

Editing a GPO

A Group Policy object (GPO) must be controlled by Advanced Group Policy Management (AGPM) before you can edit it. See Creating, Controlling, or Importing a GPO for more information about controlling a GPO.

To make changes to a GPO offline without immediately impacting the deployed copy of the GPO in the production environment, check out a copy of the GPO from the archive. When changes are complete, check the GPO back into the archive and request deployment of the GPO to the production environment.

- Edit a GPO Offline
- Use a Test Environment
- Request Deployment of a GPO
- Label the Current Version of a GPO
- Rename a GPO or Template

Edit a GPO Offline

To make changes to a controlled Group Policy object (GPO), you must first check out a copy of the GPO from the archive. No one else will be able to modify the GPO until it is checked in again, preventing the introduction of conflicting changes by multiple Group Policy administrators. When you have finished modifying the GPO, you check it into the archive, so it can be reviewed and deployed to the production environment.

A user account with the Editor or AGPM Administrator (Full Control) role, the user account of the Approver who created the GPO, or a user account with the necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

Editing a GPO offline

To edit a GPO, you check out the GPO from the archive, edit the GPO offline, and then check the GPO into the archive, so it can be reviewed and deployed (or modified by other Editors).

- Check out a GPO
- Edit a GPO
- Check in a GPO

To check out a GPO from the archive for editing

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Controlled** tab to display the controlled GPOs.
3. Right-click the GPO to be edited, and then click **Check Out**.
4. Type a comment to be displayed in the History of the GPO while it is checked out, then

click **OK**.

5. When the **Progress** window indicates that overall progress is complete, click **Close**. On the **Controlled** tab, the state of the GPO is now identified as **Checked Out**.

To edit a GPO offline

1. On the **Controlled** tab, right-click the GPO to be edited, and then click **Edit**.
2. In the **Group Policy Object Editor**, make changes to an offline copy of the GPO.
3. When you have finished modifying the GPO, close the **Group Policy Object Editor**.

To check a GPO into the archive

1. On the **Controlled** tab:
   - If you have made no changes to the GPO, right-click the GPO and click **Undo Check Out**, then click **Yes** to confirm.
   - If you have made changes to the GPO, right-click the GPO and click **Check In**.
2. Type a comment to be displayed in the audit trail of the GPO, and then click **OK**.
3. When the **Progress** window indicates that overall progress is complete, click **Close**. On the **Controlled** tab, the state of the GPO is identified as **Checked In**.

Additional considerations

- To check out and edit a GPO, by default, you must be the Approver who created or controlled the GPO, an Editor, or an AGPM Administrator (Full Control). Specifically, you must have **List Contents** and **Edit Settings** permissions for the GPO. Additionally, to edit the GPO you must be the individual who has checked out the GPO.
- To check in a GPO, by default, you must be an Editor, an Approver, or an AGPM Administrator (Full Control). Specifically, you must have **List Contents** and either **Edit Settings** or **Deploy GPO** permissions for the GPO. If you are not an Approver or AGPM Administrator (or other Group Policy administrator with **Deploy GPO** permission), you must be the Editor who has checked out the GPO.
- When editing a GPO, any Group Policy Software Installation upgrade of a package in another GPO should reference the deployed GPO, not the checked-out copy.

Additional references

- Editing a GPO
- Reviewing a GPO
  - Review GPO Settings
  - Review GPO Links
  - Identify Differences Between GPOs, GPO Versions, or Templates
- Deploying a GPO
  - Request Deployment of a GPO
  - Deploy a GPO

Use a Test Environment

If you use a testing organizational unit (OU) to test Group Policy objects (GPOs) before deployment to the production environment, you must have the necessary permissions to access the test OU. The use of a test OU is optional.

To use a test OU

1. While you have the GPO checked out for editing, in the **Group Policy Management Console**, click **Group Policy Objects** in the forest and domain in which you are managing GPOs.
2. Click the checked out copy of the GPO to be tested. The name will be preceded with **[Checked Out]**. (If it is not listed, click **Action**, then **Refresh**. Sort the names alphabetically, and **[Checked Out]** GPOs will typically appear at the top of the list.)
3. Drag and drop the GPO to the test OU.
4. Click **OK** in the dialog box asking whether to create a link to the GPO in the test OU.

Additional considerations

- When testing is complete, checking in the GPO automatically deletes the link to the checked-out copy of the GPO.

Additional references

- Editing a GPO

Request Deployment of a GPO

After you have modified and checked in a Group Policy object (GPO), deploy the GPO, so it will take effect in the production environment.

A user account with the Editor role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To request the deployment of a GPO to the production environment

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Controlled** tab to display the controlled GPOs.
3. Right-click the GPO to be deployed, and then click **Deploy**.
4. Unless you are an Approver or AGPM Administrator or have special permission to deploy GPOs, you must submit a request for deployment. To receive a copy of the request, type your e-mail address in the **Cc** field. Type a comment to be displayed in the **History** for the GPO, and then click **Submit**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The GPO is displayed on the list of GPOs on the **Pending** tab. When an Approver has

approved your request, the GPO will be moved from the **Pending** tab to the **Controlled** tab and be deployed.

Additional considerations

- By default, you must be an Editor to perform this procedure. Specifically, you must have **List Contents** and **Edit Settings** permissions for the GPO.
- To withdraw your request before it has been approved, click the **Pending** tab. Right-click the GPO, and then click **Withdraw**. The GPO will be returned to the **Controlled** tab.

Additional references

- Editing a GPO

Label the Current Version of a GPO

You can label the current version of a Group Policy object (GPO) for easy identification in its history. You can use a label to identify a known good version to which you could roll back if a problem occurs. Also, by labeling multiple GPOs with the same label at one time, you can mark related GPOs that should be rolled back to the same point if rollback should later be necessary.

A user account with the Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To label the current version of GPOs in their histories

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Click a GPO for which to label the current version. To select multiple GPOs, press SHIFT and click the last GPO in a contiguous group of GPOs, or press CTRL and click individual GPOs. Right-click a selected GPO, and then click **Label**.
4. Type a label and a comment to be displayed in the history of each GPO selected, and then click **OK**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**.

Additional considerations

- By default, you must be an Editor, an Approver, or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and either **Edit Settings** or **Deploy GPO** permissions for the GPO.

Additional references

- Editing a GPO

Rename a GPO or Template

You can rename a controlled Group Policy object (GPO) or a template.

A user account with the Editor or AGPM Administrator (Full Control) role, the user account of the Approver who created the GPO, or a user account with the necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To rename a GPO or template

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Controlled** or **Templates** tab to display the item to rename.
3. Right-click the GPO or template to rename and click **Rename**.
4. Type the new name for the GPO or template and a comment, then click **OK**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The GPO or template appears under the new name on the **Contents** tab.

Additional considerations

- By default, you must be the Approver who created or controlled the GPO, an Editor, or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Edit Settings** permission for the GPO.
- When you rename a GPO that has been deployed, the name is immediately changed in the archive. The name is changed in the production environment only when the GPO is redeployed.

  Until the GPO is redeployed (or the production copy is deleted), the old name is still in use in the production environment and therefore cannot be used for another GPO. Likewise, the GPO in the archive cannot be renamed back to its original name until the GPO has been deployed (changing the name of the production copy) or the production copy has been deleted.

Additional references

- Editing a GPO

Creating a Template and Setting a Default Template

Creating a template enables you to save all of the settings of a particular version of a Group Policy object (GPO) to use as a starting point for creating new GPOs. As an Editor, you can also specify which of the available templates will be the default template for all Group Policy administrators creating new GPOs.

Note

A template is an uneditable, static version of a GPO for use as a starting point for creating new, editable GPOs. Renaming or deleting a template does not impact GPOs created from that template.

- Create a Template

- Set a Default Template

Create a Template

Creating a template enables you to save all of the settings of a particular version of a Group Policy object (GPO) to use as a starting point for creating new GPOs.

Note
A template is an uneditable, static version of a GPO for use as a starting point for creating new, editable GPOs.

A user account with the Editor or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To create a template based on an existing GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Controlled** or **Uncontrolled** tab to display available GPOs.
3. Right-click the GPO from which you want to create a template, then click **Save as Template**.
4. Type a name for the template and a comment, then click **OK**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The new template appears on the **Templates** tab.

Additional considerations

- By default, you must be an Editor or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Create Template** permissions for the domain.
- Renaming or deleting a template does not impact GPOs created from that template.
- Because it cannot be altered, a template does not have a history.

Additional references

- Creating a Template and Setting a Default Template
- Request the Creation of a New Controlled GPO

Set a Default Template

As an Editor, you can specify which of the available templates will be the default template suggested for all Group Policy administrators creating new Group Policy objects (GPOs).

Note

A template is an uneditable, static version of a GPO for use as a starting point for creating new, editable GPOs.

A user account with the Editor or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To set the default template for use when creating new GPOs

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Templates** tab to display available templates.
3. Right-click the template that you want to set as the default, and then click **Set as Default**.
4. Click **Yes** to confirm.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The default template has a blue icon and the state is identified as **Template (default)** on the **Templates** tab.

Additional considerations

- By default, you must be an Editor or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Create Template** permissions for the domain.
- After you set a template as the default, that template will be the one initially selected in the **New Controlled GPO** dialog box when Group Policy administrators create new GPOs. However, they will have the option to select any other GPO template, including **<Empty GPO>**, which does not include any settings.
- Renaming or deleting a template does not impact GPOs created from that template.
- Because it cannot be altered, a template does not have a history.

Additional references

- Creating a Template and Setting a Default Template
- Request the Creation of a New Controlled GPO

Delete a GPO

As an Editor, you may not have permission to complete the deletion of a Group Policy object (GPO), but you do have the permission necessary to begin the process and submit your request to an Approver.

A user account with the Editor role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To request the deletion of a controlled GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Right-click the GPO to delete, and then click **Delete**.
   - To delete the GPO from the archive while leaving the deployed version of the GPO untouched in the production environment, click **Delete GPO from archive only (uncontrol)**.
   - To delete the GPO from both the archive and production environment, click **Delete GPO from archive and production**.

     Unless you have special permission to delete GPOs, you must submit a request for deletion of the deployed GPO. To receive a copy of the request, type your e-mail address in the **Cc** field. Type a comment to be displayed in the audit trail for the GPO, and then click **Submit**.
4. When the **Progress** window indicates that overall progress is complete, click **Close**. The GPO is displayed on the list of GPOs on the **Pending** tab. When an Approver has approved your request, the GPO will be moved from the **Pending** tab to the **Recycle Bin** tab, where it can be restored or destroyed.

Additional considerations

- By default, you must be an Editor to request the deletion of a deployed GPO. Specifically, you must have **List Contents** and **Edit Settings** permissions for the GPO.
- By default, you must be an Editor, an Approver, or an AGPM Administrator (Full Control) to delete a GPO from the archive. Specifically, you must have **List Contents** and either **Edit Settings** or **Delete GPO** permissions for the GPO.
- To withdraw your request before it has been approved, click the **Pending** tab. Right-click the GPO, and then click **Withdraw**. The GPO will be returned to the **Controlled** tab.
- To delete an uncontrolled GPO from the production environment without first controlling it, in the **Group Policy Management Console**, click **Forest**, click **Domains**, click **<MyDomain>**, and then click **Group Policy Objects**. Right-click the uncontrolled GPO, and then click **Delete**.

Additional references

- Performing Editor Tasks

Performing Approver Tasks

An Approver is a person authorized by an AGPM Administrator (Full Control) to create, deploy, and delete Group Policy objects (GPOs) and to approve or reject requests (typically from Editors) to create, deploy, or delete GPOs.

Important

Ensure that you are connecting to the central archive for GPOs. For more information, see Configure the AGPM Server Connection.

- Approve or Reject a Pending Action
- Creating, Controlling, or Importing a GPO
- Check In a GPO
- Deploy a GPO
- Roll Back to a Previous Version of a GPO
- Deleting, Restoring, or Destroying a GPO

Note
Because the Approver role includes the permissions for the Reviewer role, an Approver can also review settings and compare GPOs. See Performing Reviewer Tasks for more information.

Additional considerations

By default, the following permissions are provided for the Approver role:

- List Contents
- Read Settings
- Create GPO
- Deploy GPO
- Delete GPO

Also, an Approver has full control over GPOs that he created or controlled.

Approve or Reject a Pending Action

The core responsibility of an Approver is to evaluate and then approve or reject requests for Group Policy object (GPO) creation, deployment, and deletion from Editors or Reviewers who do not have permission to complete those actions. The report capabilities of Advanced Group Policy Management (AGPM) can assist an Approver with evaluating a new version of a GPO.

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To approve or reject a pending request

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Pending** tab to display the pending GPOs.
3. Right-click a pending GPO, and then click either **Approve** or **Reject**.
4. If approving deployment, click **Advanced** in the **Approve Pending Operation** dialog box

to review links to the GPO. Pause the mouse pointer on a node in the tree to display details.

- By default, all links to the GPO will be restored.
- To prevent a link from being restored, clear the check box for that link.
- To prevent all links from being restored, clear the **Restore Links** check box in the **Deploy GPO** dialog box.

5. Click **Yes** or **OK** to confirm approval or rejection of the pending action. If you have approved the request, the GPO is moved to the appropriate tab for the action performed.

Note

If an Approver's e-mail address is included in the **To** field on the **Domain Delegation** tab, the Approver will receive e-mail from the AGPM alias when an Editor or Reviewer submits a request.

Additional considerations

- By default, you must be an Approver or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have the permissions required to perform the request that you are approving.

Additional references

- Performing Approver Tasks

Creating, Controlling, or Importing a GPO

To use Advanced Group Policy Management (AGPM) to provide change control for a Group Policy object (GPO), you must first control the GPO with AGPM. New GPOs created through the **Change Control** node will automatically be controlled.

- Control a Previously Uncontrolled GPO
- Create a New Controlled GPO
- Delegate Access to a GPO
- Import a GPO from Production

Control a Previously Uncontrolled GPO

To use Advanced Group Policy Management (AGPM) to provide change control for a Group Policy object (GPO), you must first control the GPO with AGPM.

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To control a previously uncontrolled GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.

2. On the **Contents** tab in the details pane, click the **Uncontrolled** tab to display the uncontrolled GPOs.
3. Right-click the GPO to be controlled with AGPM, and then click **Control**.
4. Type a comment to be displayed in the history of the GPO, and then click **OK**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The GPO is removed from the list on the **Uncontrolled** tab and added to the **Controlled** tab.

Additional considerations

- By default, you must be an Approver or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Create GPO** permissions for the domain.

Additional references

- Creating, Controlling, or Importing a GPO

Create a New Controlled GPO

New Group Policy objects (GPOs) created through the **Change Control** node will automatically be controlled, enabling you to manage them with Advanced Group Policy Management (AGPM).

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To create a new GPO with change control managed through AGPM

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. Right-click the **Change Control** node, and then click **New Controlled GPO**.
3. In the **New Controlled GPO** dialog box:
   a. Type a name for the new GPO.
   b. Optional: Type a comment for the new GPO to be displayed in the **History** for the GPO.
   c. To immediately deploy the new GPO to the production environment, click **Create live**. To create the new GPO offline without immediately deploying it, click **Create offline**.
   d. Select the GPO template to use as a starting point for the new GPO.
   e. Click **OK**.
4. When the **Progress** window indicates that overall progress is complete, click **Close**. The new GPO is displayed in the list of GPOs on the **Controlled** tab.

Additional considerations

- By default, you must be an Approver or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Create GPO** permissions for the domain.

Additional references

- Creating, Controlling, or Importing a GPO

Delegate Access to a GPO

An Approver can delegate the management of a controlled Group Policy object (GPO) that was **created by that Approver**. Like an AGPM Administrator (Full Control), the Approver can delegate access to such a GPO, so selected Editors can edit it, Reviewers can review it, and other Approvers can approve it. By default, an Approver cannot delegate access to GPOs created by another Group Policy administrator.

A user account with the AGPM Administrator (Full Control) role, the user account of the Approver who created the GPO, or a user account with the necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To delegate the management of a controlled GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Controlled** tab to display controlled GPOs, and then click the GPO to delegate.
3. Click the **Add** button, select the users or groups to be permitted access, and then click **OK**.
4. To customize the permissions for each, click the **Advanced** button on the **Contents** tab and check role permissions to allow or deny. (For more detailed control, click **Advanced** in the **Permissions** dialog box.)
5. Click **Apply**, and then click **OK** in the **Permissions** dialog box.

Additional considerations

- By default, you must be the Approver who created or controlled the GPO or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** permission for the domain and **Modify Security** permission for the GPO.

Additional references

- Creating, Controlling, or Importing a GPO

Import a GPO from Production

If changes are made to a controlled Group Policy object (GPO) outside of Advanced Group Policy Management (AGPM), you can import a copy of the GPO from the production environment and

save it to the archive to bring the archive and the production environment to a consistent state. (To import an uncontrolled GPO, control the GPO. See Control a Previously Uncontrolled GPO.)

A user account with the Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To import a GPO from the production environment

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Right-click the GPO, and then click **Import from Production**.
4. Type a comment for the audit trail of the GPO, and then click **OK**.

Additional considerations

- By default, you must be an Editor, Approver, or AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and either **Edit Settings**, **Deploy GPO**, or **Delete GPO** permissions for the GPO.

Additional references

- Creating, Controlling, or Importing a GPO

Check In a GPO

Ordinarily, Editors should check in Group Policy objects (GPOs) that they have edited when their modifications are complete. (For details, see Edit a GPO Offline.) However, if the Editor is unavailable, an Approver can also check in a GPO.

A user account with the Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To check in a GPO that has been checked out by an Editor

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Controlled** tab to display the controlled GPOs.
   - To discard any changes made by the Editor, right-click the GPO, click **Undo Check Out**, and then click **Yes** to confirm.
   - To retain changes made by the Editor, right-click the GPO and then click **Check In**.
3. Type a comment to be displayed in the audit trail of the GPO, and then click **OK**.
4. When the **Progress** window indicates that overall progress is complete, click **Close**. On the **Controlled** tab, the state of the GPO is identified as **Checked In**.

Additional considerations

- By default, you must be an Editor, an Approver, or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and either **Edit Settings** or **Deploy GPO** permissions for the GPO. If you are not an Approver or AGPM Administrator (or other Group Policy administrator with **Deploy GPO** permission), you must be the Editor who has checked out the GPO.

Additional references

- Performing Approver Tasks
- Edit a GPO Offline

Deploy a GPO

Advanced Group Policy Management (AGPM) enables an Approver to deploy a new or edited Group Policy object (GPO) to the production environment. For information about redeploying a previous version of a GPO, see Roll Back to a Previous Version of a GPO.

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To deploy a GPO to the production environment

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Right-click the GPO to be deployed and then click **Deploy**.
4. To review links to the GPO, click **Advanced**. Pause the mouse pointer on a node in the tree to display details.
   - By default, all links to the GPO will be restored.
   - To prevent a link from being restored, clear the check box for that link.
   - To prevent all links from being restored, clear the **Restore Links** check box in the **Deploy GPO** dialog box.
5. Click **Yes**. When the **Progress** window indicates that overall progress is complete, click **Close**.

Note
To verify whether the most recent version of a GPO has been deployed, on the **Controlled** tab, double-click the GPO to display its **History**. In the **History** for the GPO, the **State** column indicates whether a GPO has been deployed.

Additional considerations

- By default, you must be an Approver or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Deploy GPO** permissions for the GPO.

Additional references

- Performing Approver Tasks

Roll Back to a Previous Version of a GPO

Advanced Group Policy Management (AGPM) enables an Approver to roll back changes to a Group Policy object (GPO) by redeploying an earlier version of the GPO from its history. Deploying an earlier version of a GPO overwrites the version of the GPO currently in production.

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To deploy a previous version of a GPO to the production environment

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Double-click the GPO to be deployed to display its **History**.
4. Right-click the version to be deployed, click **Deploy**, and then click **Yes**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. In the **History** window, click **Close**.

Note
To verify that the version that has been redeployed matches the version intended, examine a difference report for the two versions. In the **History** window for the GPO, highlight the two versions, and then right-click and select **Difference** and either **HTML Report** or **XML Report**.

Additional considerations

- By default, you must be an Approver or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Deploy GPO** permissions for the GPO.

Additional references

- Performing Approver Tasks

Deleting, Restoring, or Destroying a GPO

As an Approver, you can delete a Group Policy object (GPO) (moving it to the Recycle Bin), restore a GPO from the Recycle Bin (returning it to the archive), or destroy a GPO (permanently deleting it so that it can no longer be restored).

- Delete a GPO
- Restore a Deleted GPO
- Destroy a GPO

Delete a GPO

Advanced Group Policy Management (AGPM) enables Approvers to delete a controlled Group Policy object (GPO), moving it to the Recycle Bin.

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To delete a controlled GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Right-click the GPO to delete, and then click **Delete**.
   - To delete the GPO from the archive while leaving the deployed version of the GPO untouched in the production environment, click **Delete GPO from archive only (uncontrol)**.
   - To delete the GPO from both the archive and production environment, click **Delete GPO from archive and production**.
4. Type a comment to be displayed in the audit trail for the GPO, and then click **OK**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The GPO is removed from the **Controlled** tab and is displayed on the **Recycle Bin** tab, where it can be restored or destroyed. If the GPO was deleted only from the archive, it is also displayed on the **Uncontrolled** tab.

Additional considerations

- By default, you must be an Approver or an AGPM Administrator (Full Control) to delete a deployed GPO. Specifically, you must have **List Contents** and **Delete GPO** permissions for the GPO.
- By default, you must be an Editor, an Approver, or an AGPM Administrator (Full Control) to delete a GPO from the archive. Specifically, you must have **List Contents** and either **Edit Settings** or **Delete GPO** permissions for the GPO.
- To delete an uncontrolled GPO from the production environment without first controlling it, in the **Group Policy Management Console**, click **Forest**, click **Domains**, click **<MyDomain>**, and then click **Group Policy Objects**. Right-click the uncontrolled GPO, and then click **Delete**.

Additional references

- Deleting, Restoring, or Destroying a GPO

Restore a Deleted GPO

Advanced Group Policy Management (AGPM) enables Approvers to restore a deleted Group Policy object (GPO) from the Recycle Bin, returning it to the archive.

A user account with the Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To restore a deleted GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Recycle Bin** tab to display the deleted GPOs.
3. Right-click the GPO to restore, and then click **Restore**.
4. Type a comment to be displayed in the history of the GPO, and then click **OK**.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The GPO is removed from the **Recycle Bin** tab and is displayed on the **Controlled** tab.

Note
If a GPO was deleted from the production environment, restoring it to the archive will not automatically redeploy it to the production environment. To return the GPO to the production environment, deploy the GPO. For information, see Deploy a GPO.

Additional considerations

- By default, you must be an Editor, an Approver, or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and either **Edit Settings**, **Deploy GPO**, or **Delete GPO** permissions for the GPO.

Additional references

- Deleting, Restoring, or Destroying a GPO

Destroy a GPO

Advanced Group Policy Management (AGPM) enables Approvers to destroy a Group Policy object (GPO), removing it from the Recycle Bin and permanently deleting it so that it can no longer be restored.

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To permanently delete a GPO so it can no longer be restored

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab, click the **Recycle Bin** tab to display the deleted GPOs.

3. Right-click the GPO to destroy, and then click **Destroy**.
4. Click **Yes** to confirm that you want to permanently delete the selected GPO and all backups from the archive.
5. When the **Progress** window indicates that overall progress is complete, click **Close**. The GPO is removed from the **Recycle Bin** tab and is permanently deleted.

Additional considerations

- By default, you must be an Approver or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Delete GPO** permissions for the GPO.

Additional references

- Deleting, Restoring, or Destroying a GPO

Performing Reviewer Tasks

A Reviewer is a person authorized by an AGPM Administrator (Full Control) to review or audit Group Policy objects (GPOs). An individual with only the Reviewer role cannot modify GPOs; however, all other roles include the Reviewer role.

- Configure the AGPM Server Connection
- Review GPO Settings
- Review GPO Links
- Identify Differences Between GPOs, GPO Versions, or Templates

Additional considerations

By default, the following permissions are provided for the Reviewer role:

- List Contents
- Read Settings

Configure the AGPM Server Connection

To ensure that you are connected to the correct central archive, review the configuration of the AGPM Server connection. If an AGPM Administrator (Full Control) has not configured the AGPM Server connection for you, then you must manually configure it.

To select an AGPM Server

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. In the details pane, click the **AGPM Server** tab:
   - If the options on the **AGPM Server** tab are unavailable, they have been centrally configured by an AGPM Administrator.
   - If the options on the **AGPM Server** tab are available, type the fully-qualified computer

name for the AGPM Server (for example, server.contoso.com) and the port on which the AGPM Service listens (by default, port 4600). Click **Apply**, then click **Yes** to confirm.

Additional considerations

- The AGPM Servers selected determine which GPOs are displayed on the **Contents** tab and to what location the **Domain Delegation** tab settings are applied. If not centrally managed through the Administrative template, each Group Policy administrator must configure this setting to point to the AGPM Server for the domain.

Additional references

- Performing Editor Tasks
- Performing Approver Tasks
- Performing Reviewer Tasks

Review GPO Settings

You can generate HTML-based and XML-based reports for reviewing settings within any version of a Group Policy object (GPO).

A user account with the Reviewer, Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

To review settings in any version of a GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click a tab to display GPOs.
3. Double-click the GPO to display its history.
4. Right-click the GPO version for which to review the settings, click **Settings**, and then click **HTML Report** or **XML Report** to display a summary of the GPO's settings.

Additional considerations

- By default, you must be a Reviewer, an Editor, an Approver, or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Read Settings** permissions for the GPO. Also, to display the list of GPOs, you must have **List Contents** permission for the domain.

Additional references

- Performing Reviewer Tasks

Review GPO Links

You can display a diagram showing where a Group Policy object (GPO) or GPOs that you select are linked to organizational units. GPO link diagrams are updated each time the GPO is controlled, imported, or checked in.

A user account with the Reviewer, Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

Reviewing GPO links

- For one or more GPOs
- For one or more versions of a GPO

To display GPO links for one or more GPOs

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Controlled**, **Pending**, or **Recycle Bin** tab to display GPOs.
3. Select one or more GPOs for which to display links, right-click a selected GPO, click **Settings**, and then click **GPO Links** to display a diagram of domains and organizational units with links to the selected GPO(s).

To display GPO links for one or more versions of a GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click the **Controlled** or **Recycle Bin** tab to display GPOs.
3. Double-click the GPO to display its history.
4. Right-click the GPO version for which to review the settings, click **Settings**, and then click **HTML Report** or **XML Report** to display a summary of the GPO's settings.

Additional considerations

- By default, you must be a Reviewer, an Editor, an Approver, or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Read Settings** permissions for the GPO. Also, to display the list of GPOs, you must have **List Contents** permission for the domain.

Additional references

- Performing Reviewer Tasks

Identify Differences Between GPOs, GPO Versions, or Templates

You can generate HTML-based or XML-based difference reports to analyze the differences between Group Policy objects (GPOs), templates, or different versions of a GPO.

A user account with the Reviewer, Editor, Approver, or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management is required to complete this procedure. Review the details in "Additional considerations" in this topic.

Identifying differences between GPOs, GPO versions, or templates

- Between two GPOs or templates
- Between a GPO and a template
- Between two versions of one GPO
- Between a GPO version and a template

To identify differences between two GPOs or templates

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click a tab to display GPOs (or templates, if comparing two templates).
3. Select the two GPOs or templates.
4. Right-click one of the GPOs or templates, click **Differences**, and then click **HTML Report** or **XML Report** to display a difference report summarizing the settings of the GPOs or templates.

To identify differences between a GPO and a template

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click a tab to display GPOs (or templates, if comparing two templates).
3. Right-click the GPO, click **Differences**, and then click **Template**.
4. Select the template and type of report, and then click **OK** to display a difference report summarizing the settings of the GPO and template.

To identify differences between two versions of one GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click a tab to display GPOs (or templates, if comparing two templates).
3. Double-click the GPO to display its history, and then highlight the versions to be

compared.

4. Right-click one of the versions, click **Differences**, and then click **HTML Report** or **XML Report** to display a difference report summarizing the settings of the GPOs.

To identify differences between a GPO version and a template

1. In the **Group Policy Management Console** tree, click **Change Control** in the forest and domain in which you want to manage GPOs.
2. On the **Contents** tab in the details pane, click a tab to display GPOs (or templates, if comparing two templates).
3. Double-click the GPO to display its history.
4. Right-click the GPO version of interest, click **Differences**, and then click **Template**.
5. Select the template and type of report, and then click **OK** to display a difference report summarizing the settings of the GPO version and template.

Key to difference reports

Symbol	Meaning	Color
None	Item exists with identical settings in both GPOs	Varies with level
[#]	Item exists in both GPOs, but with changed settings	Blue
[-]	Item exists only in the first GPO	Red
[+]	Item exists only in the second GPO	Green

- For items with changed settings, the changed settings are identified when the item is expanded. The value for the attribute in each GPO is displayed in the same order that the GPOs are displayed in the report.
- Some changes to settings may cause an item to be reported as two different items (one present only in the first GPO, one present only in the second) rather than as one item that has changed.

Additional considerations

- By default, you must be a Reviewer, an Editor, an Approver, or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and **Read Settings** permissions for the GPO. Also, to display the list of GPOs, you must have **List Contents** permission for the domain.

Additional references

- Performing Reviewer Tasks

Troubleshooting Advanced Group Policy Management

This section lists a few common issues you may encounter when using Advanced Group Policy Management (AGPM) to manage Group Policy objects (GPOs).

What problems are you having?

- I am unable to access an archive
- The GPO state varies for different Group Policy administrators
- I am unable to modify the AGPM Server connection
- I am unable to change the default template or view, create, edit, rename, deploy, or delete GPOs
- I am unable to use a particular GPO name
- I am not receiving AGPM e-mail notifications
- I cannot use port 4600 for the AGPM Service
- The AGPM Service will not start
- Group Policy Software Installation fails to install software

I am unable to access an archive

- **Cause**: You have not selected the correct server and port for the archive.
- **Solution**:
  - If you are an AGPM Administrator: See Configure the AGPM Server Connection.
  - If you are not an AGPM Administrator: Request connection details for the AGPM Server from an AGPM Administrator. See Configure the AGPM Server Connection.
- **Cause**: The Advanced Group Policy Management Service is not running.
- **Solution**:
  - If you are an AGPM Administrator: Start the AGPM Service. For more information, see Start and Stop the AGPM Service.
  - If you are not an AGPM Administrator: Contact an AGPM Administrator for assistance.

The GPO state varies for different Group Policy administrators

- **Cause**: Different Group Policy administrators have selected different AGPM Servers for the same archive.
- **Solution**:
  - If you are an AGPM Administrator: See Configure the AGPM Server Connection.
  - If you are not an AGPM Administrator: Request connection details for the AGPM Server from an AGPM Administrator. See Configure the AGPM Server Connection.

I am unable to modify the AGPM Server connection

- **Cause**: If the settings on the **AGPM Server** tab are unavailable, the AGPM Server has been centrally configured using an Administrative template.
- **Solution**:
  - If you are an AGPM Administrator: If the settings on the **AGPM Server** tab are unavailable, see Configure the AGPM Server Connection.
  - If you are not an AGPM Administrator: If the settings on the **AGPM Server** tab are unavailable, you do not need to modify the AGPM Server.

I am unable to change the default template or view, create, edit, rename, deploy, or delete GPOs

- **Cause**: You have not been assigned a role with the permissions required to perform the task or tasks.
- **Solution**:
  - If you are an AGPM Administrator: See Delegate Domain-Level Access and Delegate Access to an Individual GPO. AGPM permissions will cascade from the domain to all GPOs currently in the archive. As new Group Policy administrators are added at the domain level, their permissions must be set to apply to **This object and nested objects**. For details about which roles can perform a task and what permissions are necessary to perform a task, refer to the help for that task.
  - If you are not an AGPM Administrator and you require additional roles or permissions: Contact an AGPM Administrator for assistance. Note that if you are an Editor, you can begin the process of creating a GPO, deploying a GPO, or deleting a GPO from the production environment, but an Approver or AGPM Administrator must approve your request.

I am unable to use a particular GPO name

- **Cause**: Either the GPO name is already in use or you lack permission to list the GPO.
- **Solution**:
  - If the GPO name appears on the **Controlled**, **Uncontrolled**, or **Pending** tab, choose another name. If a GPO that has been deployed is renamed but not yet redeployed, it will be displayed under its old name in the production environment—therefore, the old name is still in use. Redeploy the GPO to update its name in the production environment and release that name for use by another GPO.
  - If the GPO name does not appear on the **Controlled**, **Uncontrolled**, or **Pending** tab, you may lack permission to list the GPO. To request permission, contact an AGPM Administrator.

I am not receiving AGPM e-mail notifications

- **Cause**: A valid SMTP e-mail server and e-mail address has not been provided, or no action has been taken that generates an e-mail notification.
- **Solution**:
  - If you are an AGPM Administrator: For e-mail notifications about pending actions to be sent by AGPM, an AGPM Administrator must provide a valid SMTP e-mail server and e-

mail addresses for Approvers on the **Domain Delegation** tab. For more information, see Configure E-Mail Notification.

- E-mail notifications are generated only when an Editor, Reviewer, or other Group Policy administrator who lacks the permission necessary to create, deploy, or delete a GPO submits a request for one of those actions to occur. There is no automatic notification of approval or rejection of a request.

I cannot use port 4600 for the AGPM Service

- **Cause**: By default, the port on which the AGPM Service listens is port 4600.
- **Solution**: If port 4600 is not available for the AGPM Service, modify each archive index file to use another port and then update the AGPM Server for all Group Policy administrators. For more information, see Modify the Port on Which the AGPM Service Listens.

The AGPM Service will not start

- **Cause**: You have modified settings for the AGPM Service in the operating system under **Administrative Tools** and **Services**.
- **Solution**: Modify the settings for **Microsoft Advanced Group Policy Management - Server** under **Add or Remove Programs**. For more information, see Modify the AGPM Service Account.

Group Policy Software Installation fails to install software

- **Cause**: AGPM preserves the integrity of Group Policy Software Installation packages. Although GPOs are edited offline, links between packages as well as cached client information are preserved. This is by design.
- **Solution**: When editing a GPO offline with AGPM, configure any Group Policy Software Installation upgrade of a package in another GPO to reference the deployed GPO, not the checked-out copy. The Editor must have **Read** permission for the deployed GPO.

User Interface: Advanced Group Policy Management

Advanced Group Policy Management (AGPM) adds a **Change Control** node to each domain displayed in the **Group Policy Management Console** (GPMC). In an environment where multiple domains are managed with the GPMC, each domain is listed under the **Domains** node in the console tree. Each domain has a **Change Control** node under it, and there is one archive of Group Policy objects (GPOs) per domain.

Within the details pane there are three primary tabs, providing access to both GPO-level settings and domain-level settings and commands for AGPM.

- Contents Tab: GPO settings and commands and GPO-level delegation
- Domain Delegation Tab: AGPM e-mail notification settings and domain-level delegation
- AGPM Server Tab: Domain-level archive connection settings

Other enhancements and settings:

- Administrative Template Settings: Central configuration of logging and tracing, archive locations, and the visibility of features
- Other Enhancements to the GPMC: AGPM adds a **History** tab and an **Extensions** tab for each GPO and Group Policy link

Contents Tab

The **Contents** tab on the **Change Control** pane provides access to Group Policy objects (GPOs) and a shortcut menu for managing GPOs. The options displayed when right-clicking items are dependent on your role, your permissions, and your ownership stake in the GPO being managed. Additionally, these shortcut menus differ with the state of the GPO being managed.

The secondary tabs filter the list of GPOs displayed.

- Controlled Tab: GPOs managed by AGPM
- Uncontrolled Tab: GPOs not managed by AGPM
- Pending Tab: GPO changes awaiting approval by an Approver
- Templates Tab: GPO templates for creating new GPOs and comparing to existing GPOs
- Recycle Bin Tab: Deleted GPOs

Additionally, the secondary tabs provide access to the History of each GPO and to other features:

- Common Secondary Tab Features
- History Window

Additional references

- User Interface: Advanced Group Policy Management

Controlled Tab

The **Controlled** tab:

- Displays a list of Group Policy objects (GPOs) managed by Advanced Group Policy Management (AGPM).
- Provides a shortcut menu with commands for managing GPOs and for displaying the history and reports for GPOs.
- Displays a list of the groups and users who have permission to access a selected GPO.

Right-clicking the **Group Policy Objects** list on this tab displays a shortcut menu, including whichever of the following options are applicable.

Control and history

Command	Effect
New Controlled GPO	Create a new GPO with change control managed through AGPM and deploy it to the production environment. If you do not have

Command	Effect
	permission to create a GPO, you will be prompted to submit a request. (This option is displayed if no GPO is selected when right-clicking in the **Group Policy Objects** list.)
History	Open a window listing all versions of the selected GPO saved within the archive. From the history, you can obtain a report of the settings within a GPO, compare two versions of a GPO, compare a GPO to a template, or roll back to a previous version of a GPO.

Reports

Command	Effect
Settings	Generate an HTML-based or XML-based report displaying the settings within the selected GPO or display links to the selected GPO(s) from organizational units as of when the GPO(s) was most recently controlled, imported, or checked in.
Differences	Generate an HTML-based or XML-based report comparing the settings within two selected GPOs or within the selected GPO and a template.

Editing

Command	Effect
Edit	Open the **Group Policy Object Editor** to make changes to the selected GPO.
Check Out	Obtain a copy of the selected GPO from the archive for offline editing and prohibit anyone else from editing it until it is checked back into the archive. (Check Out can be overridden by an AGPM Administrator (Full Control).)
Check In	Check the edited version of the selected GPO into the archive, so other authorized Editors

Command	Effect
	can make changes or an Approver can deploy it to the production environment.
Undo Check Out	Return a checked out GPO to the archive without any changes.

Version management

Command	Effect
Import from Production	For the selected GPO, copy the version in the production environment to the archive.
Delete	Move the selected GPO to the Recycle Bin and indicate whether to leave the deployed version (if one exists) in production or to delete it as well as the version in the archive. If you do not have permission to delete a GPO, you will be prompted to submit a request.
Deploy	Move the selected GPO that is checked into the archive to the production environment. This action makes it active on the network and overwrites the previously active version of the GPO if one existed. If you do not have permission to deploy a GPO, you will be prompted to submit a request.
Label	Mark the selected GPO with a descriptive label (such as "Known good") and comment for record keeping. Labels appear in the **State** column and comments in the **Comment** column of the **History** window, enabling you to easily identify previous versions of a GPO identified with a particular label, so you can roll back if a problem occurs.
Rename	Change the name of the selected GPO. If the GPO has already been deployed, the name will be updated in the production environment when the GPO is redeployed.
Save as Template	Create a new template based on the settings of the selected GPO.

Miscellaneous

Command	Effect
Refresh	Update the display of the Group Policy Management Console to incorporate any changes. Some changes are not visible until the display is refreshed.
Help	Display help for AGPM.

Additional references

- Contents Tab
- Performing Editor Tasks
- Performing Approver Tasks
- Performing Reviewer Tasks

Uncontrolled Tab

The **Uncontrolled** tab:

- Displays a list of Group Policy objects (GPOs) not managed by Advanced Group Policy Management (AGPM).
- Provides a shortcut menu with commands for bringing uncontrolled GPOs under the management of AGPM and for displaying the history and reports for GPOs.
- Displays a list of the groups and users who have permission to access a selected GPO.

Right-clicking the **Group Policy Objects** list on this tab displays a shortcut menu, including whichever of the following options are applicable.

Control and history

Command	Effect
History	Open a window listing all versions of the selected GPO saved within the archive. From the history, you can obtain a report of the settings within a GPO, compare two versions of a GPO, compare a GPO to a template, or roll back to a previous version of a GPO.
Control	Bring the selected uncontrolled GPO under the change control management of AGPM. If you do not have permission to control a GPO, you will be prompted to submit a request.

Command	Effect
Save as Template	Create a new template based on the settings of the selected GPO.

Reports

Command	Effect
Settings	Generate an HTML-based or XML-based report displaying the settings within the selected GPO.
Differences	Generate an HTML-based or XML-based report comparing the settings within two selected GPOs or within the selected GPO and a template.

Miscellaneous

Command	Effect
Refresh	Update the display of the Group Policy Management Console to incorporate any changes. Some changes are not visible until the display is refreshed.
Help	Display help for AGPM.

Additional references

- Contents Tab
- Performing Editor Tasks
- Performing Approver Tasks
- Performing Reviewer Tasks

Pending Tab

The **Pending** tab:

- Displays a list of Group Policy objects (GPOs) with pending requests for GPO management actions (such as creation, control, deployment, or deletion).
- Provides a shortcut menu with commands for responding to pending requests and for displaying the history and reports for GPOs.
- Displays a list of the groups and users who have permission to access a selected GPO.

Right-clicking the **Group Policy Objects** list on this tab displays a shortcut menu, including whichever of the following options are applicable.

Control and history

Command	Effect
History	Open a window listing all versions of the selected GPO saved within the archive. From the history, you can obtain a report of the settings within a GPO, compare two versions of a GPO, compare a GPO to a template, or roll back to a previous version of a GPO.
Withdraw	Withdraw your pending request to create, control, or delete the selected GPO before the request has been approved.
Approve	Complete a pending request from an Editor to create, control, or delete the selected GPO.
Reject	Deny a pending request from an Editor to create, control, or delete the selected GPO.

Reports

Command	Effect
Settings	Generate an HTML-based or XML-based report displaying the settings within the selected GPO or display links to the selected GPOs from organizational units as of when the GPOs are most recently controlled, imported, or checked in.
Differences	Generate an HTML-based or XML-based report comparing the settings within two selected GPOs or within the selected GPO and a template.

Miscellaneous

Command	Effect
Refresh	Update the display of the Group Policy

Command	Effect
	Management Console to incorporate any changes. Some changes are not visible until the display is refreshed.
Help	Display help for AGPM.

Additional references

- Contents Tab
- Performing Approver Tasks
- Performing Reviewer Tasks

Templates Tab

The **Templates** tab:

- Displays a list of available templates that you can use to create new Group Policy objects (GPOs).
- Provides a shortcut menu with commands for creating a GPO based on a selected template, managing templates, and displaying reports for templates.
- Displays a list of the groups and users who have permission to access a selected template.

Because a template cannot be altered, templates have no history. However, like any GPO version, the settings of a template can be displayed with a settings report or compared to another GPO with a difference report.

Note

A template is an uneditable, static version of a GPO for use as a starting point for creating new, editable GPOs.

Right-clicking the **Group Policy Objects** list on this tab displays a shortcut menu, including whichever of the following options are applicable.

Control

Command	Effect
New Controlled GPO	Create a new GPO based on the selected template. The option to deploy the new GPO to the production environment is provided. If you do not have permission to create a GPO, you will be prompted to submit a request. (This option is displayed if no GPO is selected when right-clicking in the **Group Policy Objects** list.)

Reports

Command	Effect
Settings	Generate an HTML-based or XML-based report displaying the settings within the selected GPO.
Differences	Generate an HTML-based or XML-based report comparing the settings within two selected GPO templates.

Template management

Command	Effect
Set as Default	Set the selected template as the default to be used automatically when creating a new GPO.
Delete	Move the selected template to the **Recycle Bin**. If you do not have permission to delete a GPO, you will be prompted to submit a request.
Rename	Change the name of the selected template.

Miscellaneous

Command	Effect
Refresh	Update the display of the Group Policy Management Console to incorporate any changes. Some changes are not visible until the display is refreshed.
Help	Display help for Advanced Group Policy Management (AGPM).

Additional references

- Contents Tab
- Performing Editor Tasks
- Performing Reviewer Tasks

Recycle Bin Tab

The **Recycle Bin** tab:

- Displays a list of Group Policy objects (GPOs) that have been deleted from the archive.

- Provides a shortcut menu with commands for managing GPOs and for displaying reports for GPOs.
- Displays a list of the groups and users who have permission to access a selected GPO.

Right-clicking the **Group Policy Objects** list on this tab displays a shortcut menu, including whichever of the following options are applicable:

Reports

Command	Effect
Settings	Generate an HTML-based or XML-based report displaying the settings within the selected GPO or display links to the selected GPOs from organizational units as of when the GPOs were most recently controlled, imported, or checked in.
Differences	Generate an HTML-based or XML-based report comparing the settings within two selected GPOs or within the selected GPO and a template.

Version management

Command	Effect
Destroy	Remove the selected GPO from the **Recycle Bin**, so it can no longer be restored.
Restore	Move the selected GPO from the **Recycle Bin** to the **Controlled** tab. This does not restore the GPO to the production environment.

Miscellaneous

Command	Effect
Refresh	Update the display of the Group Policy Management Console to incorporate any changes. Some changes are not visible until the display is refreshed.
Help	Display help for AGPM.

Additional references

- Contents Tab
- Performing Approver Tasks
- Performing Reviewer Tasks

Common Secondary Tab Features

Each secondary tab has two sections—**Group Policy objects** and **Groups and Users**.

Group Policy objects section

The **Group Policy objects** section displays a filtered list of Group Policy objects (GPOs) and identifies the following characteristics for each GPO:

GPO Characteristic	Description
Name	Name of the Group Policy object.
Computer (Comp.)	Automatically generated version of the Computer Configuration portion of the GPO.
User	Automatically generated version of the User Configuration portion of the GPO.
State	The state of the selected GPO:  **Uncontrolled:** Not managed by AGPM.  **Checked In:** Available for authorized Editors to check out for editing or for a Group Policy administrator to deploy.  **Checked Out:** Currently being edited. Unavailable for other Editors to check out until the Editor who checked it out or an AGPM Administrator checks it in.  **Pending:** Awaiting approval from a Group Policy administrator before being created, controlled, deployed, or deleted.  **Deleted:** Deleted from the archive, but still able to be restored.  **Template:** A static version of a GPO for use as a starting point when creating new GPOs.  **Template (default):** By default, this template is the starting point used when creating a new GPO.

GPO Characteristic	Description
GPO Status	The Computer Configuration and the User Configuration can be managed separately. The GPO Status indicates which portions of the GPO are enabled.
WMI Filter	Display any WMI filters that are applied to this GPO. WMI filters are managed under the **WMI Filters** node for the domain in the console tree of the GPMC.
Modified	For a controlled GPO, the most recent date when it was checked in after being modified or checked out to be modified. For an uncontrolled GPO, the date when it was last modified.
Owner	The Editor who checked in or the Approver who deployed the selected GPO.

Groups and Users section

When a GPO is selected, the **Groups and Users** section displays a list of the groups and users with access to that GPO. The allowed permissions and inheritance are displayed for each group or user. An AGPM Administrator can configure permissions using either standard AGPM roles (Editor, Approver, and Reviewer) or a customized combination of permissions.

Button	Effect
Add	Add a new entry to the security descriptor. Any user or group in Active Directory can be added.
Remove	Remove the selected entry from the Access Control List.
Properties	Display the properties for the selected object. The properties page is the same one displayed for an object in **Active Directory Users and Computers**.
Advanced	Open the **Access Control List Editor**.

Additional considerations

- For information about roles and permissions related to specific tasks, see the tasks under Performing AGPM Administrator Tasks, Performing Editor Tasks, Performing Approver Tasks, and Performing Reviewer Tasks.

Additional references

- Contents Tab

History Window

The history of a Group Policy object (GPO) can be displayed by double-clicking a GPO or by right-clicking a GPO and then clicking **History**. It is also displayed in the **Group Policy Management Console** (GPMC) as a tab for each GPO.

The history provides a list of all versions of the selected GPO saved within the archive. From the **History** window, you can obtain a report of the settings within a GPO, compare multiple versions of a GPO, or roll back to a previous version of a GPO.

Filtering events in the History window

The tabs within the **History** window filter the events displayed.

Tabs	Filtering
Show All	Display all versions of the GPO.
Checked In	Display only checked-in versions of the GPO. The deployed version is omitted from this list.
Labels Only	Display only GPOs that have labels associated with them.

Event information

Information is provided for each event in the history of the selected GPO.

GPO Characteristic	Description
Computer	Automatically generated version of the Computer Configuration portion of the GPO.
User	Automatically generated version of the User Configuration portion of the GPO.
Time	Timestamp of the version of the GPO when the action in the status field was performed.
State	The state of the selected version of the GPO:  **Deployed**: This version of the GPO is currently live in the production environment.  **Checked In**: This version of the GPO is available for authorized Editors to check out for editing or for a Group Policy administrator to

GPO Characteristic	Description
	deploy.  **Checked Out**: This version of the GPO is currently checked out by an Editor and is unavailable for other Editors. (The checked out state is not recorded in the **History** except to indicate if a GPO is currently checked out.)  **Created**: Identifies the date and time of the initial creation of the GPO.  **Labeled**: Identifies a labeled version of the GPO.
GPO Status	The Computer Configuration and the User Configuration can be managed separately from each other. This status shows which portions of the GPO are enabled.
Owner	The person who checked in or deployed the GPO.
Comment	A comment entered by the owner of a GPO at the time that this version was modified. Useful for identifying the specifics of the version in case of the need to roll back to a previous version.

Reports

Depending on whether a single GPO version or multiple GPO versions are selected, the **Settings** and **Differences** buttons display reports on GPO settings. Right-clicking GPO versions provides the option to display XML-based reports as well.

Button	Effect
Settings	Generate an HTML-based report displaying the settings within the selected version of the GPO.
Differences	Generate an HTML-based report comparing the settings within multiple selected versions of the GPO.

Key to difference reports

Symbol	Meaning	Color
None	Item exists with identical settings in both GPOs	Varies with level
[#]	Item exists in both GPOs, but with changed settings	Blue
[-]	Item exists only in the first GPO	Red
[+]	Item exists only in the second GPO	Green

- For items with changed settings, the changed settings are identified when the item is expanded. The value for the attribute in each GPO is displayed in the same order that the GPOs are displayed in the report.
- Some changes to settings may cause an item to be reported as two different items (one present only in the first GPO, one present only in the second), rather than as one item that has changed.

Additional references

- Contents Tab

Domain Delegation Tab

The **Domain Delegation** tab on the **Change Control** pane provides a list of Group Policy administrators who have domain-level access to the archive and indicates the roles of each. Additionally, this tab enables AGPM Administrators (Full Control) to configure domain-level permissions for Editors, Approvers, Reviewers, and other AGPM Administrators. There are two sections on the **Domain Delegation** tab—configuration of e-mail notification and role-based delegation for Advanced Group Policy Management (AGPM) at the domain level.

Configuration of e-mail notification

The e-mail notification section of this tab identifies the Approvers that will receive notification when operations are pending in AGPM.

Setting	Description
From	The AGPM alias from which notification is sent to Approvers. In an environment with multiple domains, this can be the same alias throughout the environment or a different alias for each domain.
To	A comma-delimited list of e-mail addresses of Approvers to whom notification is to be sent

Setting	Description
SMTP server	The name of the e-mail server, such as mail.contoso.com
User name	A user with access to the SMTP server
Password	User's password for authentication to the SMTP server
Confirm password	Confirm user's password

Domain-level role-based delegation

The role-based delegation section of this tab displays and enables an AGPM Administrator to delegate allowed, denied, and inherited permissions for each group and user on the domain with access to the archive. An AGPM Administrator can configure domain-wide permissions using either standard AGPM roles (Editor, Approver, Reviewer, and AGPM Administrator) or a customized combination of permissions for each Group Policy administrator.

Button	Effect
Add	Add a new entry to the security descriptor. Any users or groups in Active Directory can be added as Group Policy administrators.
Remove	Remove the selected Group Policy administrators from the Access Control List.
Properties	Display the properties for the selected Group Policy administrators. The properties page is the same one displayed for an object in **Active Directory User and Computers**.
Advanced	Open the **Access Control List Editor**.

Additional considerations

- For information about roles and permissions related to specific tasks, see the tasks under Performing AGPM Administrator Tasks, Performing Editor Tasks, Performing Approver Tasks, and Performing Reviewer Tasks.

Additional references

- User Interface: Advanced Group Policy Management
- Performing AGPM Administrator Tasks

AGPM Server Tab

The **AGPM Server** tab on the **Change Control** pane enables you to select an AGPM Server by entering a fully-qualified computer name and port. The default port for Advanced Group Policy Management (AGPM) is port 4600.

The AGPM Server selected determines which archive is displayed for you on the **Contents** tab and to which location the **Domain Delegation** settings are applied.

If the AGPM Server connection is centrally configured using Administrative template settings, the options on this tab are unavailable. For more information, see Configure the AGPM Server Connection.

Additional references

- User Interface: Advanced Group Policy Management
- Performing AGPM Administrator Tasks
- Performing Reviewer Tasks

Administrative Template Settings

The Administrative template settings for Advanced Group Policy Management (AGPM) enable you to centrally configure logging and tracing options for AGPM clients and servers to which a Group Policy object (GPO) with these settings is applied. Similarly, these settings enable you to centrally configure archive locations and the visibility of the **Change Control** node and **History** tab for Group Policy administrators to whom a GPO with these settings is applied.

- Logging and Tracing Settings
- AGPM Server Connection Settings
- Feature Visibility Settings

Additional references

- User Interface: Advanced Group Policy Management
- Performing AGPM Administrator Tasks

Logging and Tracing Settings

The Administrative Template settings for Advanced Group Policy Management (AGPM) enable you to centrally configure logging and tracing options for AGPM Servers and clients to which a Group Policy object (GPO) with these settings is applied.

The following setting is available under Computer Configuration\Administrative Templates\Windows Components\AGPM in the **Group Policy Object Editor** when editing a GPO in the Group Policy Management Console (GPMC). If this path is not visible, right-click **Administrative Templates**, and add the agpm.admx or agpm.adm template.

Trace file locations:

- Client: %LocalAppData%\Microsoft\AGPM\agpm.log
- Server: %CommonAppData%\Microsoft\AGPM\agpmserv.log

Setting	Effect
AGPM Logging	If enabled, this setting configures whether tracing is turned on and the level of detail. This setting affects both client and server components of AGPM. If disabled or not configured, this setting has no effect.

Additional references

- Administrative Template Settings

AGPM Server Connection Settings

You can use Administrative template settings for Advanced Group Policy Management (AGPM) to centrally configure AGPM Server connections for Group Policy administrators to whom a Group Policy object (GPO) with these settings is applied.

The following settings are available under User Configuration\Administrative Templates\Windows Components\AGPM when editing a GPO. If this path is not visible, right-click **Administrative Templates**, and add the agpm.admx or agpm.adm template.

Setting	Effect
AGPM Server (all domains)	If enabled, this setting centrally configures one AGPM Server connection for use by all domains and disables the settings on the **AGPM Server** tab for Group Policy administrators. For multiple AGPM Servers, configure this setting with a default server and then configure the **AGPM Server** setting in the Administrative template to override this server for other domains. If disabled or not configured, each Group Policy administrator must select the AGPM Server to display for each domain on the **AGPM Server** tab in AGPM.
AGPM Server	If enabled, this setting centrally configures multiple domain-specific AGPM Servers, overriding the **AGPM Server (all domains)** setting in the Administrative template. If your environment requires only a single AGPM Server, use only the **AGPM Server (all domains)** setting in the Administrative

Setting	Effect
	template. If disabled or not configured, the **AGPM Server (all domains)** setting in the Administrative template configures the AGPM Server connection.

Additional references

- Administrative Template Settings
- Performing AGPM Administrator Tasks

Feature Visibility Settings

The Administrative template settings for Advanced Group Policy Management (AGPM) enable you to centrally configure the visibility of the **Change Control** node and **History** tab for Group Policy administrators to whom a Group Policy object (GPO) with these settings is applied.

The following settings are available under User Configuration\Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted Snap-ins\Extension Snap-ins in the **Group Policy Object Editor** when editing a GPO in the Group Policy Management Console (GPMC). If this path is not visible, right-click **Administrative Templates**, and add the agpm.admx or agpm.adm template.

Setting	Effect
AGPM Change Control	If enabled or not configured, the **Change Control** node is visible in the GPMC. If disabled, the **Change Control** node is not visible in the GPMC.
AGPM Link Extension	If enabled or not configured, a **History** tab appears in the GPMC for each linked GPO. If disabled, the **History** tab is not visible for linked GPOs.
AGPM GPO Extension	If enabled or not configured, a **History** tab appears in the GPMC for each GPO. If disabled, the **History** tab is not visible for GPOs.

Additional references

- Administrative Template Settings

Other Enhancements to the GPMC

Advanced Group Policy Management (AGPM) adds a **History** tab and an **Extensions** tab to extend the functionality of the **Group Policy Management Console** (GPMC).

History tab

AGPM adds a **History** tab to all Group Policy objects (GPOs) and Group Policy links displayed in the GPMC. The features of the **History** tab in the details pane of a GPO are the same as those of the **History** window displayed through the **Change Control** tab. For information about these features, see History Window.

Extensions tab

In the Microsoft Windows Server® 2003 operating system, AGPM adds an **Extensions** tab to all GPOs and Group Policy links displayed in the GPMC. This tab lists all extensions that have settings in the GPO (or all registered extensions if **Show all registered extensions** is checked) and identifies them as part of the user or computer context.

Additional references

- User Interface: Advanced Group Policy Management