

Microsoft®

# Advanced Group Policy Management

## Operations Guide for Microsoft Advanced Group Policy Management 4.0

---

Microsoft Corporation

Published: September 2009

### **Abstract**

This guide provides step-by-step instructions for performing tasks by using Microsoft Advanced Group Policy Management (AGPM) 4.0. It includes all of the information in the Help for AGPM.

***Microsoft***®

# Copyright

---

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

# Contents

---

Operations Guide for Microsoft Advanced Group Policy Management 4.0 .....	5
Overview of Advanced Group Policy Management .....	6
Best Practices for Version Control .....	7
Checklist: Administer the AGPM Server and Archive .....	8
Checklist: Create, Edit, and Deploy a GPO.....	8
Search and Filter the List of GPOs .....	9
Performing AGPM Administrator Tasks .....	11
Configuring Advanced Group Policy Management.....	12
Configure AGPM Server Connections.....	13
Configure E-Mail Notification.....	15
Configure E-Mail Security for AGPM.....	16
Delegate Access to the Production Environment.....	17
Configure Logging and Tracing.....	19
Managing the Archive .....	19
Delegate Domain-Level Access to the Archive .....	20
Delegate Access to an Individual GPO in the Archive.....	21
Limit the GPO Versions Stored .....	22
Import a GPO from a File.....	23
Back Up the Archive .....	24
Restore the Archive from a Backup.....	25
Managing the AGPM Service .....	26
Start and Stop the AGPM Service .....	26
Modify the AGPM Service .....	27
Move the AGPM Server and the Archive .....	28
Performing Editor Tasks .....	30
Creating or Controlling a GPO.....	31
Request Control of an Uncontrolled GPO.....	31
Request the Creation of a New Controlled GPO.....	32
Import a GPO from Production.....	32
Editing a GPO.....	33
Edit a GPO Offline .....	33
Label the Current Version of a GPO.....	35
Rename a GPO or Template .....	36
Using a Test Environment.....	37
Export a GPO to a File.....	37
Import a GPO from a File.....	38
Test a GPO in a Separate Organizational Unit .....	38
Request Deployment of a GPO .....	39
Creating a Template and Setting a Default Template.....	40

Create a Template.....	40
Set a Default Template.....	41
Deleting or Restoring a GPO.....	42
Request Deletion of a GPO .....	42
Request Restoration of a Deleted GPO.....	43
Performing Approver Tasks .....	44
Approve or Reject a Pending Action.....	45
Creating or Controlling a GPO.....	45
Control an Uncontrolled GPO .....	46
Create a New Controlled GPO.....	46
Delegate Management of a Controlled GPO .....	47
Import a GPO from Production.....	48
Check In a GPO.....	49
Deploy a GPO .....	49
Roll Back to an Earlier Version of a GPO .....	50
Deleting, Restoring, or Destroying a GPO .....	51
Delete a Controlled GPO .....	51
Restore a Deleted GPO.....	52
Destroy a GPO .....	53
Performing Reviewer Tasks .....	53
Configure an AGPM Server Connection .....	54
Review GPO Settings .....	54
Review GPO Links.....	55
Identify Differences Between GPOs, GPO Versions, or Templates.....	56
Troubleshooting AGPM.....	58
User Interface: Advanced Group Policy Management.....	61
Contents Tab .....	61
Contents Tab Features .....	62
History Window .....	64
Controlled GPO Commands .....	66
Uncontrolled GPO Commands.....	69
Pending GPO Commands .....	70
Template Commands .....	72
Recycle Bin Commands.....	73
Domain Delegation Tab .....	75
AGPM Server Tab .....	76
Production Delegation Tab.....	77
Administrative Templates Folder .....	77
Logging and Tracing Settings .....	78
AGPM Server Connection Settings.....	78
Feature Visibility Settings.....	79

# Operations Guide for Microsoft Advanced Group Policy Management 4.0

---

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

Using AGPM, you can do these tasks:

- Perform offline editing of GPOs so that you can create and test them before you deploy them to a production environment.
- Maintain multiple versions of a GPO in a central archive so that you can roll back if a problem occurs.
- Share the responsibility for editing, approving, and reviewing GPOs among multiple people by using role-based delegation.
- Eliminate the danger of multiple Group Policy administrators overwriting one another's work by using the check-in and check-out capability for GPOs.
- Analyze changes to a GPO, comparing it to another GPO or another version of the same GPO by using difference reporting.
- Simplify creating new GPOs by using GPO templates, storing common policy settings and preference settings to use as starting points for new GPOs.
- Delegate access to the production environment.
- Search for GPOs with specific attributes and filter the list of GPOs displayed.
- Export a GPO to a file so that you can copy it from a domain in a test forest to a domain in a production forest.

AGPM adds a **Change Control** folder under each domain displayed in the GPMC, in addition to a **History** tab for each GPO and Group Policy link displayed in the GPMC.

- [Overview of Advanced Group Policy Management](#)
- [Best Practices for Version Control](#)
- [Checklist: Administer the AGPM Server and Archive](#)
- [Checklist: Create, Edit, and Deploy a GPO](#)
- [Search and Filter the List of GPOs](#)
- [Performing AGPM Administrator Tasks](#)
- [Performing Editor Tasks](#)
- [Performing Approver Tasks](#)
- [Performing Reviewer Tasks](#)
- [Troubleshooting AGPM](#)
- [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) to provide comprehensive change control and improved 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 that Group Policy administrators can view and change it offline without immediately affecting 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 necessary.

The terms "check in" and "check out" are used just as in a library (or in applications that provide change control, version control, or source 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 you develop GPOs by using AGPM:

1. Create a new controlled GPO or control a previously uncontrolled GPO.
2. Check out the GPO, so that you and only you can change it.
3. Edit the GPO.
4. Check in the edited GPO, so that others can change it, or so that 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 for managing access to GPOs in the archive. Domain-level permissions enable AGPM Administrators to provide access to individual domains without providing access to other domains. GPO-based delegation enables AGPM Administrators to provide access to specific GPOs without providing domain-wide access.

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 of a domain, protecting the environment from 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 change 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

- **Operations Guide for Microsoft Advanced Group Policy Management 4.0**

## Best Practices for Version Control

Microsoft Advanced Group Policy Management (AGPM) provides version control for Group Policy objects (GPOs) much like Microsoft Visual SourceSafe® provides version control for source code. Developers can use Visual SourceSafe to manage multiple versions of each source file. Group Policy administrators can use AGPM to do the same for GPOs. When you use AGPM, Group Policy administrators should be aware of best practices that apply to any version control system:

- **Date and time:** AGPM stamps each version of a GPO with the date and time. To ensure that history is accurate, especially when you edit GPOs on more than one computer, make sure that each computer synchronizes its clock with one authoritative time source.
- **Check in GPOs when you are finished editing them:** It is common for Editors to check out GPOs and forget to check them back into the archive. However, this can prevent other Group Policy administrators from changing the GPO. Always check GPOs back in to AGPM immediately when you are finished editing.
- **Save changes frequently:** When you edit a GPO, save changes frequently. Most Editors check out a GPO, make many changes, and then check the GPO into the archive. Instead, check the GPO into the archive regularly, and then check it out again. The detail can be as small as checking in the GPO after you change every setting (not recommended) or checking in the GPO after you make groups of related changes. The result is a better-documented history for each GPO that can help when troubleshooting issues.
- **Deploy GPOs frequently:** Do not let new and edited GPOs that have not yet been deployed accumulate in large numbers in the archive. Instead, deploy new and edited GPOs as soon as possible so that they have a minimum effect on the production environment. Deploying many new and edited GPOs at one time can jeopardize the production environment.
- **Document the purpose of changes when you check in GPOs:** Any Reviewer can compare versions of a GPO to see specific changes between the two. Documenting those specific changes adds no value. Instead, document the intent and purpose of a change instead of documenting what Reviewers can see by viewing difference reports. Version comments should add value to the comparison report and help a Reviewer understand why the Editor changed the GPO.
- **Test GPOs in a test environment:** Deploying GPOs to the production environment without testing them is risky. Instead, test your GPOs in a domain in a test forest, and then export the GPOs to files and import them to a domain in a production forest. Also, you can link GPOs to an organizational unit that contains test computers and users. Verify that each GPO functions correctly in the test environment and then deploy the GPOs to the production environment.

#### Additional references

- **Operations Guide for Microsoft Advanced Group Policy Management 4.0**

## Checklist: Administer the AGPM Server and Archive

In Advanced Group Policy Management (AGPM), both the AGPM Service and the archive are managed by AGPM Administrators (Full Control). The following are typical tasks for an AGPM Administrator.

Frequent Task	Reference
Delegate access to Group Policy objects (GPOs) in the archive.	<a href="#">Delegate Domain-Level Access to the Archive</a> <a href="#">Delegate Access to an Individual GPO in the Archive</a>
Back up the archive to enable disaster recovery.	<a href="#">Back Up the Archive</a>

Infrequent Task	Reference
Restore the archive from a backup to recover from a disaster.	<a href="#">Restore the Archive from a Backup</a>
Move the AGPM Service, the archive, or both to a different server.	<a href="#">Move the AGPM Server and the Archive</a>
Change the archive path, the AGPM Service Account, or the port on which the AGPM Service listens.	<a href="#">Modify the AGPM Service</a>
Troubleshoot common problems with the AGPM Server.	<a href="#">Troubleshooting AGPM</a> <a href="#">Configure Logging and Tracing</a>

#### Additional references

- **Operations Guide for Microsoft Advanced Group Policy Management 4.0**

## Checklist: Create, Edit, and Deploy a GPO

In an environment where multiple people change Group Policy objects (GPOs) by using Advanced Group Policy Management (AGPM), 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 that a new GPO be created or an Approver creates a new GPO.	<a href="#">Request the Creation of a New Controlled GPO</a> <a href="#">Create a New Controlled GPO</a>
Approver approves the creation of the GPO if it was requested by an Editor.	<a href="#">Approve or Reject a Pending Action</a>
Editor checks out a copy of the GPO from the archive so that no one else can modify the GPO. Editor makes changes to the GPO, and then checks the modified GPO into the archive.	<a href="#">Edit a GPO Offline</a>
If developing in a test forest, Editor exports the GPO to a file, transfers the file to the production forest, and imports the file. Additionally, an Editor can link the GPO to an organizational unit that contains test computers and users.	<a href="#">Using a Test Environment</a>
Editor requests deployment of the GPO to the production environment of the domain.	<a href="#">Request Deployment of a GPO</a>
Reviewers, such as Approvers or Editors, analyze the GPO.	<a href="#">Performing Reviewer Tasks</a>
Approver approves and deploys the GPO to the production environment of the domain or rejects the GPO.	<a href="#">Approve or Reject a Pending Action</a>

### Additional references

Operations Guide for Microsoft Advanced Group Policy Management 4.0

## Search and Filter the List of GPOs

In Advanced Group Policy Management (AGPM), you can search the list of Group Policy objects (GPOs) and their attributes to filter the list of GPOs displayed. For example, you can search for GPOs with a particular name, state, or comment. You can also search for GPOs that were last changed by a particular Group Policy administrator or on a particular date.

### Performing a complex search

You can perform a complex search by using the format *GPO attribute 1: search string 1 GPO attribute 2: search string 2...all-column search strings*. The search is not case-sensitive.

- **GPO attribute:** Any column heading in the list of GPOs in AGPM other than **Computer Version** or **User Version**. GPO attributes include the GPO name, state, user who most

recently changed the GPO, date and time when the GPO was most recently changed, comment, GPO status, and WMI filter applied to the GPO.

- **Search string:** Text for which to search in the specified column. If a string includes spaces, you must enclose the string with quotation marks.
- **All-column search strings:** Text for which to search in all columns in the list of GPOs in AGPM other than **Computer Version** and **User Version**. You can include multiple strings separated by spaces. If a string includes spaces, you must enclose the string with quotation marks.

Each GPO attribute and search string pair and each all-column search string are combined by using a logical AND operation. The result is a list of all GPOs for which each specified attribute includes the specified search string and for which any all-column search strings appear in at least one column. The search returns any partial matches for strings so that you can enter part of a GPO name or user name and view a list of all GPOs that include that text in their name.

The following are examples of searches:

Description of search result	Search query
All GPOs with names that include the text <b>security</b> and <b>North America</b> .	<b>name: security name: "North America"</b>
All checked out GPOs.	<b>state: "checked out"</b>
All GPOs most recently changed by the user named <b>Administrator</b> and most recently changed within the previous month.	<b>changed by: Administrator change date: lastmonth</b>
All GPOs in which the word <b>firewall</b> is included in the most recent comment and in which the word <b>security</b> appears in any column.	<b>comment: firewall security</b>
All GPOs that have a status of <b>All Settings Disabled</b> .	<b>gpo status: all</b>
All GPOs that have a WMI filter named <b>My WMI Filter</b> applied and that have a status of <b>User Configuration Settings Disabled</b> .	<b>wmi filter: "My WMI Filter" gpo status: user</b>

## Specifying dates

You can search for GPOs changed on a specific date, at a specific time, or during a span of time by using the same special terms available when you search in Windows. If entering a specific date or time, you must use the format that is used in the **Change Date** column. The following are examples of searches of the **Change Date** column:

- **change date: 10/10/2009**

- **change date: 10/10/2009 9:00:00 AM**
- **change date: thisweek**

You can use the following special terms, which are not case-sensitive, when you search the **Change Date** column:

- Today
- Yesterday
- ThisWeek
- LastWeek
- ThisMonth
- LastMonth
- TwoMonths
- ThreeMonths
- ThisYear
- LastYear

#### **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** permission for the domain.
- For more information about GPO attributes, see [Contents Tab Features](#).

#### **Additional references**

- **Operations Guide for Microsoft Advanced Group Policy Management 4.0**

## **Performing AGPM Administrator Tasks**

Advanced Group Policy Management (AGPM) lets an AGPM Administrator (Full Control) configure domain-wide options and delegate permissions to Approvers, Editors, Reviewers, and AGPM Administrators. By default, an AGPM Administrator is someone who has Full Control— all AGPM permissions—and who therefore can perform tasks associated with any role.

In an environment in which multiple people develop Group Policy objects (GPOs), you can choose to let all Group Policy administrators perform the same tasks and have the same level of access. Or, you can choose to let AGPM Administrators delegate permissions to Editors who can change GPOs and to Approvers who deploy GPOs to the production environment. AGPM Administrators can configure permissions to meet the needs of your organization.

- [Configuring Advanced Group Policy Management](#): Configure the AGPM Server Connection and e-mail notification, delegate access to GPOs in the production environment, and configure logging and tracing for troubleshooting.

- [Managing the Archive](#): Delegate access to GPOs in the archive, limit the number of versions of each GPO stored, import a GPO from another domain, and back up and restore the archive.
- [Managing the AGPM Service](#): Stop and start the AGPM Service or change the archive path, the AGPM Service Account, or the port on which the AGPM Service listens.
- [Move the AGPM Server and the Archive](#): Move the AGPM Service, the archive, or both to a different server.



#### Notes

Because the AGPM Administrator role includes the permissions for all other roles, an AGPM Administrator can perform the tasks usually 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
- Export GPO
- Import GPO
- Create Template
- Modify Options
- Modify Security

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

## Configuring Advanced Group Policy Management

In Advanced Group Policy Management (AGPM), as an AGPM Administrator (Full Control), you can centrally configure AGPM Server connections for Group Policy administrators, configure e-mail notification for AGPM, configure optional e-mail security for AGPM, delegate access to Group Policy objects (GPOs) in the production environment of the domain, and configure logging and tracing for troubleshooting.

- [Configure AGPM Server Connections](#)

- [Configure E-Mail Notification](#)
- [Configure E-Mail Security for AGPM](#)
- [Delegate Access to the Production Environment](#)
- [Configure Logging and Tracing](#)

#### **Additional references**

- For information about delegating access to GPOs in the archive, see [Managing the Archive](#).
- For information about how to restrict the number of versions of each GPO stored in the archive, see [Limit the GPO Versions Stored](#).
- [Performing AGPM Administrator Tasks](#)

## **Configure AGPM Server Connections**

All versions of each controlled Group Policy object (GPO) are stored in a central archive so that 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 (AGPM) 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 AGPM Server connections**

As an AGPM Administrator, you can ensure that all Group Policy administrators connect to the same AGPM Server by centrally configuring the associated 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 connection for all Group Policy administrators](#)
- [Configure additional AGPM Server connections for all Group Policy administrators](#)
- [Manually configure an AGPM Server connection for your account](#)

#### **▶ To configure an AGPM Server connection 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 Management Editor** window, click **User Configuration, Policies, Administrative Templates, Windows Components, and AGPM**.
3. In the details pane, double-click **AGPM: Specify default AGPM Server (all domains)**.
4. In the **Properties** window, select the **Enabled** check box, and type the fully-qualified computer name and port (for example, server.contoso.com:4600).
5. Click **OK**. Unless you want to configure additional AGPM Server connections, close the

**Group Policy Management Editor** window 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 Server connections 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. In the **Group Policy Management Editor** window, click **User Configuration, Policies, Administrative Templates, Windows Components**, and then **AGPM**.
4. In the details pane, double-click **AGPM: Specify AGPM Servers**.
5. In the **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 AGPM Service](#).)
  - d. Repeat for each domain not using the default AGPM Server.
7. Click **OK** to close the **Show Contents** and **Properties** windows.
8. Close the **Group Policy Management Editor** window. (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 configure it is unavailable for all Group Policy administrators.

▶ **To manually configure which 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 selected AGPM Server 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 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

- [Configuring Advanced Group Policy Management](#)

## 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 (AGPM) 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 e-mail address** field, type the e-mail alias for AGPM from which notifications should be sent.
4. In the **To e-mail address** 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.
- By default, e-mail messages sent as a result of actions in Advanced Group Policy Management (AGPM) are not encrypted. However, you can configure e-mail security for AGPM using registry settings to specify whether to use Secure Sockets Layer (SSL) encryption and which SMTP port to use. For more information, see [Configure E-Mail Security for AGPM](#).

#### Additional references

- [Configuring Advanced Group Policy Management](#)

### Configure E-Mail Security for AGPM

By default, e-mail notifications sent because of actions in Advanced Group Policy Management (AGPM) are not encrypted and are sent through SMTP port 25. However, you can configure e-mail security for AGPM by using registry settings to specify whether to use Secure Sockets Layer (SSL) encryption and which SMTP port to use.

By encrypting AGPM e-mail notifications, you can better protect those that could reveal sensitive information about your organization's security. Encrypting e-mail notifications is recommended when they are being relayed through remote mail servers, and may be required by some compliance regulations.

#### Caution

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

A user account that has the AGPM Administrator (Full Control) role, the user account of the Approver who created the Group Policy object (GPO) used in these procedures, or a user account that has the necessary permissions in AGPM is required to complete these procedures. Review the details in "Additional considerations" in this topic.

#### To configure e-mail security for AGPM by using Group Policy preferences

1. In the **Group Policy Management Console** tree, edit a GPO that is applied to all AGPM Servers for which you want to configure e-mail security. (For more information, see [Editing a GPO](#).)
2. In the **Group Policy Management Editor** window, expand the **Computer Configuration, Preferences, Windows Settings**, and **Registry** folders.
3. In the console tree, right-click **Registry**, point to **New**, click **Collection Item**, and type **AGPM e-mail security**.
4. Create a Registry preference item to turn on encryption:
  - a. In the console tree, right-click **AGPM e-mail security**, point to **New**, and then click **Registry Item**.



- b. In the **New Registry Properties** dialog box, select the **Update** action.
  - c. For **Hive**, select **HKEY\_LOCAL\_MACHINE**.
  - d. For **Key Path**, type **SOFTWARE\Microsoft\AGPM**.
  - e. For **Value name**, type **EncryptSmtp**.
  - f. For **Value type**, select **REG\_DWORD**.
  - g. For **Base**, select **Decimal**, and for **Value data**, type **1** to use SSL encryption, or **0** to let e-mail to be sent without encryption. By default, e-mail is sent without encryption. Click **OK**.
5. Create a Registry preference item to specify the SMTP port:
    - a. In the console tree, right-click **AGPM E-mail security**, point to **New**, and then click **Registry Item**.
    - b. In the **New Registry Properties** dialog box, select the **Update** action.
    - c. For **Hive**, select **HKEY\_LOCAL\_MACHINE**.
    - d. For **Key Path** dialog box, type **SOFTWARE\Microsoft\AGPM**.
    - e. For **Value name**, type **SmtpPort**.
    - f. For **Value type**, select **REG\_DWORD**.
    - g. For **Base**, select **Decimal**, and for **Value data**, type a port number for the SMTP port. By default, the SMTP port is port 25 if encryption is not enabled or port 587 if SSL encryption is enabled. Click **OK**.
  6. Close the **Group Policy Management Editor** window, and then check in and deploy the GPO. For more information, see [Deploy a GPO](#).

#### **Additional considerations**

- You must be able to edit and deploy a GPO to configure registry settings by using Group Policy Preferences. See [Editing a GPO](#) and [Deploy a GPO](#) for additional detail.

#### **Additional references**

- [Configuring Advanced Group Policy Management](#)

## **Delegate Access to the Production Environment**

In Advanced Group Policy Management (AGPM), you can change access to Group Policy objects (GPOs) in the production environment of the domain, replacing any existing permissions on those GPOs. You can configure permissions at the domain level to either allow or prevent users from editing, deleting, or modifying the security of GPOs in the production environment when they are not using the **Change Control** folder in the Group Policy Management Console (GPMC).



#### **Notes**

- Changing how access to the production environment is delegated does not affect users' ability to link GPOs.
- When GPOs are controlled or deployed, access for any other accounts except those with **Read** and **Apply** permissions is removed.

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

► **To change access to GPOs in the production environment of the 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 **Production Delegation** tab.
3. To add permissions for a user or group that does not have access to the production environment, or to replace the permissions for a user or group that does have access:
  - a. Click **Add**, select a user or group, and then click **OK**.
  - b. Select permissions to delegate to that user or group for the production environment, and then click **OK**.
4. To remove all permissions to the production environment for a user or group, select the user or group, click **Remove**, and then 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.
- Permissions for the AGPM Service Account cannot be changed on the **Production Delegation** tab.
- By default, the following accounts have permissions for GPOs in the production environment:

Account	Default Permissions for GPOs
<AGPM Service Account>	Edit Settings, Delete, Modify Security
Authenticated Users	Read, Apply
Domain Admins	Edit Settings, Delete, Modify Security
Enterprise Admins	Edit Settings, Delete, Modify Security
Enterprise Domain Controllers	Read
System	Edit Settings, Delete, Modify Security

- Membership in the Group Policy Creator Owners group should be restricted, so 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**

- [Configuring Advanced Group Policy Management](#)

## Configure Logging and Tracing

You can centrally configure optional logging and tracing using Administrative templates. This may be helpful when diagnosing any problems related to Advanced Group Policy Management (AGPM).

A user account with the AGPM Administrator (Full Control) role, the user account of the Approver who created the Group Policy object (GPO) used in these procedures, or a user account with the necessary permissions in AGPM 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 Management Editor** window, click **Computer Configuration, Policies, Administrative Templates, Windows Components, and AGPM**.
3. In the details pane, double-click **AGPM: Configure logging**.
4. In the **Properties** window, click **Enabled**, and configure the level of detail to record in the logs.
5. Click **OK**.
6. Close the **Group Policy Management Editor** window. (For more information, see [Deploy a GPO](#).) After Group Policy is updated, you must restart the AGPM Service to start, modify, or stop logging on the AGPM Server. Group Policy administrators must close and restart the GPMC to start, modify, or stop logging on their computers.

#### Trace file locations:

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

#### Additional considerations

- You must be able to edit and deploy a GPO to configure AGPM logging and tracing. See [Editing a GPO](#) and [Deploy a GPO](#) for additional detail.

#### Additional references

- [Configuring Advanced Group Policy Management](#)

## Managing the Archive

In Advanced Group Policy Management (AGPM), as an AGPM Administrator (Full Control), you manage access to the archive and have the option to limit the number of versions of each Group Policy object (GPO) stored in the archive. You can delegate access to GPOs in the archive at the domain level or GPO level. Additionally, you can back up the archive so that you may be able to recover it if a disaster occurs.

As an AGPM Administrator, you can export a GPO to a file, copy the file to another forest, and then import the GPO into a domain in that forest. Unlike an Editor, you can import policy settings from a GPO backup directly into a new controlled GPO when you create it. For information about how to export a GPO, see [Export a GPO to a File](#).

- [Delegate Domain-Level Access to the Archive](#)
- [Delegate Access to an Individual GPO in the Archive](#)
- [Limit the GPO Versions Stored](#)
- [Import a GPO from a File](#)
- [Back Up the Archive](#)
- [Restore the Archive from a Backup](#)

#### **Additional references**

- For information about how to delegate access to GPOs in the production environment, see [Delegate Access to the Production Environment](#).
- For information about how to move the archive, see [Move the AGPM Server and the Archive](#).
- [Performing AGPM Administrator Tasks](#)

### **Delegate Domain-Level Access to the Archive**

Set up delegation for your environment so that Group Policy administrators have the appropriate access to and control over Group Policy objects (GPOs) in the archive. There are baseline permissions you can apply to make operation 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 (AGPM) is required to complete this procedure. Review the details in "Additional considerations" in this topic.

#### **▶ To delegate access so that 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, and configure access to all GPOs in the domain:
  - a. To add access for a user or group, click the **Add** button, select the user or group, and click **OK**. In the **Add Group or User** dialog box, select a role and click **OK**.
  - b. To remove access for a user or group, select the user or group, and click the **Remove** button.
  - c. To modify the roles and permissions delegated to a user or group, select click the **Advanced** button. In the **Permissions** dialog box, select the user or group, select the check box for each role to be assigned to that user or group, and then click **OK**.



Editor and Approver include Reviewer permissions.

### **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. 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 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**

- [Managing the Archive](#)

## **Delegate Access to an Individual GPO in the Archive**

As an AGPM Administrator (Full Control), you can delegate the management of a controlled Group Policy object (GPO) in the archive so that 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 (AGPM) 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:
  - a. To add access for a user or group, click the **Add** button, select the user or group, and click **OK**. In the **Add Group or User** dialog box, select a role and click **OK**.
  - b. To remove access for a user or group, select the user or group, and click the **Remove** button.



#### **Note**

If a user or group inherits domain-wide access, the **Remove** button is unavailable. You can modify domain-wide access on the **Domain Delegation** tab.

- c. To modify the roles and permissions delegated to a user or group, click the **Advanced** button. In the **Permissions** dialog box, select the user or group, select the check box for each role to be assigned to that user or group, and click **OK**.

**Note**

Editor and Approver include Reviewer permissions.

**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. 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 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**

- [Managing the Archive](#)

**Limit the GPO Versions Stored**

By default, all versions of every controlled Group Policy object (GPO) are retained in the archive on the AGPM Server. However, you can limit the number of versions retained for each GPO and delete older versions when that limit is exceeded. When GPO versions are deleted, a record of the version remains in the history of the GPO, but the GPO version itself is deleted from the archive.

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

**► To limit the number of GPO versions stored**

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. Select the **Delete old versions of each GPO from the archive** check box, and type the maximum number of GPO versions to store for each GPO, not including the current version. To retain only the current version, enter 0. The maximum must be no greater

than 999.

 **Important**

Only GPO versions displayed on the **Unique Versions** tab of the **History** window count toward the limit.

4. Click the **Apply** button.

#### **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.
- You can prevent a GPO version from being deleted by marking it in the history as ineligible for deletion. To do so, right-click the version in the history of the GPO and click **Do Not Delete**.

#### **Additional references**

- [Managing the Archive](#)

### **Import a GPO from a File**

In Advanced Group Policy Management (AGPM), if you are an AGPM Administrator (Full Control) and you have exported a Group Policy object (GPO) to a CAB file, you can import the policy settings from that GPO into a new GPO or an existing GPO in a domain in another forest. For information about exporting GPO settings to a CAB file, see [Export a GPO to a File](#).

A user account with the AGPM Administrator role or the necessary permissions in AGPM is required to import policy settings into a new controlled GPO. A user account with the Editor or AGPM Administrator role or necessary permissions in AGPM is required to import policy settings into an existing GPO. Review the details in "Additional considerations" in this topic.

#### **Importing policy settings from a file**

When you import policy settings from a file, you can import them into a new GPO or an existing GPO. However, if you import policy settings into an existing GPO, all policy settings within it are replaced.

- [Import policy settings into a new controlled GPO](#)
- [Import policy settings into an existing GPO](#)

#### **To import policy settings into a new controlled GPO**

1. In the **Group Policy Management Console** tree, click **Change Control** in the domain to which you want to import policy settings.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Create a new controlled GPO. In the **New Controlled GPO** dialog box, click **Import** and then click **Launch Wizard**. For more information about how to create a GPO, see [Create a New Controlled GPO](#).
4. Follow the instructions in the **Import Settings Wizard** to select a GPO backup, import

policy settings from it for the new GPO, and enter a comment for the audit trail of the new GPO.

#### ▶ **To import policy settings into an existing GPO**

1. In the **Group Policy Management Console** tree, click **Change Control** in the domain to which you want to import policy settings.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Check out the destination GPO to which you want to import policy settings.
4. Right-click the destination GPO, point to **Import from**, and then click **File**.
5. Follow the instructions in the **Import Settings Wizard** to select a GPO backup, import its policy settings to replace those in the destination GPO, and enter a comment for the audit trail of the destination GPO. By default, the destination GPO is checked in when the wizard is finished.

#### **Additional considerations**

- To import policy settings to a new controlled GPO, you must have **List Contents**, **Import GPO**, and **Create GPO** permissions for the domain. By default, you must be an AGPM Administrator to perform this procedure.
- To import policy settings to an existing GPO, you must have **List Contents**, **Edit Settings**, and **Import GPO** permissions for the domain, and the GPO must be checked out by you. By default, you must be an Editor or an AGPM Administrator (Full Control) to perform this procedure.

#### **Additional references**

- [Managing the Archive](#)

## **Back Up the Archive**

To help in the recovery of the archive for Advanced Group Policy Management (AGPM) if there is a disaster, an AGPM Administrator (Full Control) should back up the archive frequently. By default, the archive is created in %ProgramData%\Microsoft\AGPM. However, you can specify a different path during the setup of Microsoft Advanced Group Policy Management - Server.

A user account that has access to both the AGPM Server—the computer on which the AGPM Service is installed—and to the folder that contains the archive is required to complete this procedure.

#### ▶ **To back up the archive**

1. Stop the AGPM Service. For more information, see [Start and Stop the AGPM Service](#).
2. Back up the archive folder by using Windows Explorer, Xcopy, Windows Server® Backup, or another backup tool. Make sure that you back up hidden, system, and read-only files.
3. Store the archive backup in a secure location.



4. Restart the AGPM Service. For more information, see [Start and Stop the AGPM Service](#).



#### Note

If an AGPM Administrator backs up the archive infrequently, the Group Policy objects (GPOs) in the archive backup will not be current. To better ensure that the archive backup is current, back up the archive as part of your organization's daily backup strategy.

#### Additional references

- [Restore the Archive from a Backup](#)
- [Move the AGPM Server and the Archive](#)
- [Managing the Archive](#)

### Restore the Archive from a Backup

If a disaster occurs and the archive for Advanced Group Policy Management (AGPM) is damaged or destroyed, an AGPM Administrator (Full Control) can restore the archive from a backup copy prepared in advance and then import from the production environment of the domain any Group Policy objects (GPOs) that are not in the archive or for which the version in production is more current than that in the archive. For information about how to restore an archive backup to a different server, see [Move the AGPM Server and the Archive](#).

A user account that has access to the AGPM Server (the computer on which the AGPM Service is installed) and to the folder that contains the archive is required to complete this procedure.

#### ► To restore the archive from a backup

1. Stop the AGPM Service. For more information, see [Start and Stop the AGPM Service](#).
2. Remove the existing archive. By default, the archive folder is %ProgramData%\Microsoft\AGPM, however the AGPM Administrator who installed Microsoft Advanced Group Policy Management - Server may have entered a different location during setup.
3. Re-create the archive folder by configuring the archive path, AGPM Service Account, Archive Owner, and listening port. Using the same values as used during the original installation is not necessary. For more information, see [Modify the AGPM Service](#).
4. Copy the contents of the archive backup to the archive folder, copying the subfolders and files to make sure that each subfolder and file inherits the permissions of the archive folder. Be careful not to overwrite the archive folder.
5. If you not sure about whether a GPO in the archive backup is more current than the copy of that GPO in production, generate a difference report and compare their settings. For more information, see [Identify Differences Between GPOs, GPO Versions, or Templates](#).
6. Restart the AGPM Service. For more information, see [Start and Stop the AGPM Service](#).

#### Additional references

- [Back Up the Archive](#)

- [Move the AGPM Server and the Archive](#)
- [Managing the Archive](#)

## 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 of the domain. 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 AGPM Service](#)

### Additional references

- [Move the AGPM Server and the Archive](#)
- [Performing AGPM Administrator Tasks](#)

## 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.

### Additional references

- [Managing the AGPM Service](#)

## Modify 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 of the domain. If this service is stopped or disabled, AGPM Clients cannot perform operations through the server. You can modify the archive path, the AGPM Service Account, and the port on which the AGPM Service listens.

### 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. Additionally, you must provide credentials for the AGPM Service Account to complete this procedure.

### To modify the AGPM Service

1. On the computer on which Microsoft Advanced Group Policy Management - Server is installed, click **Start, Control Panel, Programs, and Programs and Features**.
2. Right-click **Microsoft Advanced Group Policy Management - Server**, and then click **Change**.
3. Click **Next**, and then click **Modify**.
4. Follow the instructions to configure the AGPM Service:
  - a. In the **Archive Path** dialog box, enter a new location for the archive relative to the AGPM Server, or confirm the current archive path, and then click **Next**.

#### Important

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. In the **AGPM Service Account** dialog box, enter credentials for a service account under which the AGPM Service will run, and click **Next**.

#### 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 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.

- c. In the **Archive Owner** dialog box, enter the user name of an AGPM Administrator (Full Control) or group of AGPM Administrators, and click **Next**.



#### **Note**

Modifying the installation clears the credentials for the Archive Owner. You must re-enter credentials, but they are not required to match the credentials used during the original installation.

- d. In the **Port Configuration** dialog box, type a new port on which the AGPM Service should listen or confirm the port currently selected, and click **Next**.



#### **Notes**

By default, the AGPM Service listens on port 4600.

If you manually configure port exceptions or have rules configuring port exceptions, you can clear the **Add port exception to firewall** check box.

5. Click **Change**, and when the installation is complete click **Finish**.
6. If you have changed the port on which the AGPM Service listens, modify the port in the AGPM Server connection for each Group Policy administrator. (For more information, see [Configure AGPM Server Connections](#).)
7. Repeat for each AGPM Server to which the configuration changes should be applied.

#### **Additional references**

- [Managing the AGPM Service](#)

## **Move the AGPM Server and the Archive**

If you are replacing the AGPM Server and the server on which the archive is hosted, you must move the AGPM Service and the archive. If you prefer, you can move the AGPM Service and the archive separately.



#### **Notes**

- The AGPM Server is the computer that hosts the AGPM Service and the computer on which Microsoft Advanced Group Policy Management – Server is installed.
- By default, the archive is hosted on the AGPM Server, but you can specify an archive path to host it on another server instead.

A user account that is a member of the Domain Admins group and has access to the previous and new AGPM Servers is required to complete this procedure. Additionally, you must provide credentials for the AGPM Service Account to be used by the new AGPM Server to complete this procedure.

► **To move the AGPM Service and the archive to a different server or servers**

1. Back up the archive. For more information, see [Back Up the Archive](#).
2. Move the AGPM Service:
  - a. Stop the AGPM Service. For more information, see [Start and Stop the AGPM Service](#).
  - b. Install Microsoft Advanced Group Policy Management - Server on the new server that will host the AGPM Service. During this process, you specify the new archive path, the location for the archive in relation to the AGPM Server. For more information, see [Step-by-Step Guide for Microsoft Advanced Group Policy Management 4.0](#) (<http://go.microsoft.com/fwlink/?LinkId=153505>) and [Planning Guide for Microsoft Advanced Group Policy Management](#) (<http://go.microsoft.com/fwlink/?LinkId=156883>).
  - c. Either an AGPM Administrator (Full Control) must configure the AGPM Server connection for all Group Policy administrators who will use the new AGPM Server and remove the connection for the old AGPM Server, or else each Group Policy administrator must manually configure the new AGPM Server connection and remove the old AGPM Server connection for the AGPM snap-in on their computer. For more information, see [Configure AGPM Server Connections](#).



**Note**

As a best practice, you should uninstall Microsoft Advanced Group Policy Management – Server from the previous AGPM Server. This will ensure that the AGPM Service cannot be unintentionally restarted on that server and potentially cause confusion if any AGPM Server connections to it remain.

3. Copy the archive from the backup to the new server that will host the archive. For more information, see [Restore the Archive from a Backup](#).



**Important**

If you moved the archive without moving the AGPM Service at the same time:

- a. You must change the archive path to point to the new location for the archive in relation to the AGPM Server. For more information, see [Modify the AGPM Service](#).
- b. You must re-enter and confirm the password on the **Domain Delegation** tab. For more information, see [Configure E-Mail Notification](#).

**Additional references**

- [Back Up the Archive](#)
- [Restore the Archive from a Backup](#)
- [Configure AGPM Server Connections](#)
- [Modify the AGPM Service](#)

- [Step-by-Step Guide for Microsoft Advanced Group Policy Management 4.0](http://go.microsoft.com/fwlink/?LinkId=153505)  
(<http://go.microsoft.com/fwlink/?LinkId=153505>)
- [Planning Guide for Microsoft Advanced Group Policy Management](http://go.microsoft.com/fwlink/?LinkId=156883)  
(<http://go.microsoft.com/fwlink/?LinkId=156883>)
- [Performing AGPM Administrator Tasks](#)

## Performing Editor Tasks

In Advanced Group Policy Management (AGPM), an Editor is a person authorized by an AGPM Administrator (Full Control) to change Group Policy objects (GPOs) and create GPO templates. Additionally, an Editor can request that a GPO be created, deleted, or restored. An Approver must approve the request for it to be implemented. An Editor can export a GPO to a file so that it can be copied to a domain in another forest, and import a GPO that was copied from another domain.



### Important

Make sure that you are connecting to the central archive for GPOs. For more information, see [Configure an AGPM Server Connection](#).

- [Creating or Controlling a GPO](#)
- [Editing a GPO](#)
- [Using a Test Environment](#)
- [Request Deployment of a GPO](#)
- [Creating a Template and Setting a Default Template](#)
- [Deleting or Restoring 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
- Export GPO
- Import GPO
- Create Template

## Creating or Controlling 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** folder 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 an Uncontrolled GPO](#)
- [Request the Creation of a New Controlled GPO](#)
- [Import a GPO from Production](#)

### Request Control of an Uncontrolled GPO

To provide change control for an existing Group Policy object (GPO), the GPO must be controlled. 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 (AGPM) is required to complete this procedure. Review the details in "Additional considerations" in this topic.

#### ► To control an 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 or Controlling 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).

A user account with the Editor or Reviewer role or necessary permissions in Advanced Group Policy Management (AGPM) 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 **Change Control**, 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 of the domain 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 or Controlling 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 of the domain 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 an Uncontrolled GPO](#).)



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

▶ **To import a GPO from the production environment of the 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. 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 or Controlling 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 or Controlling 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, test it, and request deployment of the GPO to the production environment.

- [Edit a GPO Offline](#)
- [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 that 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 (AGPM) 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 that it can be reviewed and deployed (or modified by other Editors).

- [Check out a GPO from the archive for editing](#)
- [Edit a GPO offline](#)
- [Check a GPO into the archive](#)

### ▶ 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, 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, and 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 Management Editor** window, make changes to an offline copy of the GPO.

#### **Note**

To disable all Computer Configuration settings or all User Configuration settings, right-click the GPO in the **Group Policy Management Editor** window and click **Properties**. Select **Disable Computer Configuration settings** or **Disable User Configuration settings** as appropriate.

3. When you have finished modifying the GPO, close the **Group Policy Management Editor** window.

### ▶ 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**, and 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, and 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](#)

### 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 (AGPM) 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 (AGPM) 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, and 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](#)

## Using a Test Environment

Before you request that a Group Policy object (GPO) be deployed to the production environment, you should test the GPO in a lab environment. If you develop the GPO in a domain in a test forest, you can export the GPO to a file and import the file to a domain in the production forest. You can then test the GPO by linking it to an organizational unit (OU) that contains test computers and users.

- [Export a GPO to a File](#)
- [Import a GPO from a File](#)
- [Test a GPO in a Separate Organizational Unit](#)



### Note

You can also import a GPO from the production environment of the domain. For more information, see [Import a GPO from Production](#).

## Export a GPO to a File

You can export a controlled Group Policy object (GPO) to a CAB file so that you can copy it to a domain in another forest and import the GPO into Advanced Group Policy Management (AGPM) in that domain. For information about how to import GPO settings into a new or existing GPO, see [Import a GPO from a File](#).

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

### ▶ To export a GPO to a file

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 **Export to**.
4. Enter a file name for the file to which you want to export the GPO, and then click **Export**. If the file does not exist, it is created. If it already exists, it is replaced.

### 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**, **Read Settings**, and **Export GPO** permissions for the GPO.

### Additional references

- [Using a Test Environment](#)

## Import a GPO from a File

In Advanced Group Policy Management (AGPM), if you have exported a Group Policy object (GPO) to a CAB file, you can import the policy settings from that GPO into an existing GPO in a domain in another forest. Importing policy settings into an existing GPO replaces all policy settings within that GPO. For information about exporting GPO settings to a CAB file, see [Export a GPO to a File](#).

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

### ► To import policy settings into an existing GPO

1. In the **Group Policy Management Console** tree, click **Change Control** in the domain to which you want to import policy settings.
2. On the **Contents** tab, click the **Controlled** tab to display the controlled GPOs.
3. Check out the destination GPO to which you want to import policy settings.
4. Right-click the destination GPO, point to **Import from**, and then click **File**.
5. Follow the instructions in the **Import Settings Wizard** to select a GPO backup, import its policy settings to replace those in the destination GPO, and enter a comment for the audit trail of the destination GPO. By default, the destination GPO is checked in when the wizard is finished.

### 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**, **Edit Settings**, and **Import GPO** permissions for the domain, and the GPO must be checked out by you.
- Although an Editor cannot import policy settings into a new GPO during its creation, an Editor can request the creation of a new GPO and then import policy settings into it after it is created.

### Additional references

- [Using a Test Environment](#)

## Test a GPO in a Separate Organizational Unit

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

### ► To use a test OU

1. Although 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 by **[AGPM]**. (If it is not listed, click **Action**, then **Refresh**. Sort the names alphabetically, and **[AGPM]** GPOs will typically appear at the top of the list.)
3. Drag the GPO to the test OU.
4. Click **OK** in the dialog box that asks 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**

- [Using a Test Environment](#)

## **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 (AGPM) 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 of the 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. 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. 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**

- [Performing Editor Tasks](#)

## Creating a Template and Setting a Default Template

Creating a template enables you to save all 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.

Some potential uses for a template include the following:

- Create a security baseline that your organization can reuse across domains.
- Create a template to manage folder redirection and offline files that your organization can customize for each department.
- Create a wireless networking template that your organization can use to configure wireless network connections for different geographical areas.
- Create regulatory compliance templates for local network administrators.
- Create a read-only snapshot of an existing GPO.



### Note

A template is a static version of a GPO that cannot be edited, yet can be used as a starting point for creating new, editable GPOs. Renaming or deleting a template does not affect 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 (AGPM) 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, and then click **Save as Template**.
4. Type a name for the template and a comment, and 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 (AGPM) 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](#)

## **Deleting or Restoring a GPO**

To use Advanced Group Policy Management (AGPM) to delete a Group Policy object (GPO) from the archive or restore a deleted GPO from the Recycle Bin, the GPO must be controlled by AGPM. As an Editor, you may not have permission to complete the deletion or restoration of a GPO, but you do have the permission necessary to begin the process and submit your request to an Approver.

- [Request Deletion of a GPO](#)
- [Request Restoration of a Deleted GPO](#)

## **Request Deletion of a GPO**

Unless you are an Approver or an AGPM Administrator (Full Control), you must request the deletion of a Group Policy object (GPO).

A user account with the Editor role or necessary permissions in Advanced Group Policy Management (AGPM) 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 you want 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**.
  - To delete the GPO from both the archive and production environment of the domain, click **Delete GPO from archive and production**.
4. 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**.
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 **Recycle Bin** tab, where it can be restored or destroyed.

#### **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.
- 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 or Restoring a GPO](#)

### **Request Restoration of a Deleted GPO**

Unless you are an Approver or an AGPM Administrator (Full Control), you must request the restoration of a deleted Group Policy object (GPO) from the Recycle Bin to return it to the archive.

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

#### **▶ To request the restoration of 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 you want to restore, and then click **Restore**.
4. Unless you have special permission to restore GPOs, you must submit a request for restoration of the deleted 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**.
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 [Request Deployment of a GPO](#).

#### **Additional considerations**

- By default, you must be an Editor to perform this procedure. Specifically, you must have **List Contents** and **Edit Settings** permission 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 **Recycle Bin** tab.

#### Additional references

- [Deleting or Restoring a GPO](#)

## 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

Make sure that you are connecting to the central archive for GPOs. For more information, see [Configure an AGPM Server Connection](#).

- [Approve or Reject a Pending Action](#)
- [Creating or Controlling a GPO](#)
- [Check In a GPO](#)
- [Deploy a GPO](#)
- [Roll Back to an Earlier Version of a GPO](#)
- [Deleting, Restoring, or Destroying a GPO](#)



#### Note

Before approving a GPO, an Approver should review the policy settings that it contains. The Approver role includes the permissions for the Reviewer role, so that an Approver can review policy 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. Reports 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 (AGPM) 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 an item 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 e-mail address** 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 or Controlling 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** folder will automatically be controlled.

- [Control an Uncontrolled GPO](#)
- [Create a New Controlled GPO](#)
- [Delegate Management of a Controlled GPO](#)
- [Import a GPO from Production](#)

## Control an Uncontrolled GPO

To provide change control for a Group Policy object (GPO), you must first control the GPO.

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

### ▶ To control an 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 or Controlling a GPO](#)

## Create a New Controlled GPO

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

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management (AGPM) 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 **Change Control**, 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 of the domain, 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, and then 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 or Controlling a GPO](#)

### **Delegate Management of a Controlled 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 that 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 (AGPM) 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:
  - a. To add access for a user or group, click the **Add** button, select the user or group, and click **OK**. In the **Add Group or User** dialog box, select a role and click **OK**.
  - b. To remove access for a user or group, select the user or group, and then click the **Remove** button.



If a user or group inherits domain-wide access, the **Remove** button is unavailable. You can modify domain-wide access on the **Domain Delegation** tab.

- c. To modify the roles and permissions delegated to a user or group, click the **Advanced** button. In the **Permissions** dialog box, select the user or group, select the check box for each role to be assigned to that user or group, and then click **OK**.



**Note**

Editor and Approver include Reviewer permissions.

**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. 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.

**Additional references**

- [Creating or Controlling 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 of the domain 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 an Uncontrolled GPO](#).)

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

**▶ To import a GPO from the production environment of the 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. 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 or Controlling 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 (AGPM) 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, 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

An Approver can deploy a new or edited Group Policy object (GPO) to the production environment. For information about redeploying an earlier version of a GPO, see [Roll Back to an Earlier Version of a GPO](#).

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management (AGPM) 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 an item 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 an Earlier Version of a GPO**

An Approver can 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 (AGPM) is required to complete this procedure. Review the details in "Additional considerations" in this topic.

### ▶ To deploy an earlier version of a GPO to the production environment of the 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. 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 Controlled GPO](#)
- [Restore a Deleted GPO](#)
- [Destroy a GPO](#)

### Delete a Controlled GPO

Approvers can 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 (AGPM) 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 you want 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**.
  - To delete the GPO from both the archive and production environment of the domain, 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 perform this procedure. Specifically, you must have **List Contents** and **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

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

A user account with the Approver or AGPM Administrator (Full Control) role or necessary permissions in Advanced Group Policy Management (AGPM) 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 Approver or an AGPM Administrator (Full Control) to perform this procedure. Specifically, you must have **List Contents** and either **Deploy GPO** or **Delete GPO** permissions for the GPO.

#### **Additional references**

- [Deleting, Restoring, or Destroying a GPO](#)

## **Destroy a GPO**

Approvers can 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 (AGPM) 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 an 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 an 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 an 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 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 (AGPM) 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 (AGPM) 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 (AGPM) 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 AGPM

This section lists common issues that you may encounter when you use Advanced Group Policy Management (AGPM) to manage Group Policy objects (GPOs). To diagnose issues not listed here, it may be helpful for an AGPM Administrator (Full Control) to use logging and tracing. For more information, see [Configure Logging and Tracing](#).



#### Notes

- For information about rolling back to an earlier version of a GPO if there are problems, see [Roll Back to an Earlier Version of a GPO](#).
- For information about how to recover from a disaster by restoring the complete archive from a backup, see [Restore the Archive from a Backup](#).

## 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](#)
- [An error occurred when I restored the archive to a new AGPM Server](#)

### **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 AGPM Server Connections](#).
  - If you are not an AGPM Administrator: Request connection details for the AGPM Server from an AGPM Administrator. See [Configure an AGPM Server Connection](#).
- **Cause:** The AGPM 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 AGPM Server Connections](#).
  - If you are not an AGPM Administrator: Request connection details for the AGPM Server from an AGPM Administrator. See [Configure an 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 AGPM Server Connections](#).
  - 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 to the Archive](#) and [Delegate Access to an Individual GPO in the Archive](#). AGPM permissions will cascade from the domain to all GPOs currently in the archive. For details about which roles can perform a task and which 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. Be aware 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 of the domain, 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 was deployed is renamed but not yet redeployed, it will be displayed under its old name in the production environment of the domain. Therefore, the old name is still being used. 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 the port configuration on the AGPM Server to use another port and then update the port in the AGPM Server connection for AGPM Clients. For more information, see [Modify the AGPM Service](#).

#### **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 **Programs and Features** in Control Panel. For more information, see [Modify the AGPM Service](#).

#### **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 in addition to cached client information are preserved. This is by design.
- **Solution:** When you edit 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.

#### **An error occurred when I restored the archive to a new AGPM Server**

- **Cause:** For security reasons, the encryption protecting the password entered on the **Domain Delegation** tab causes the password to fail if the archive is moved to another computer.
- **Solution:** Re-enter and confirm the password on the **Domain Delegation** tab. For more information, see [Configure E-Mail Notification](#).

## **User Interface: Advanced Group Policy Management**

Advanced Group Policy Management (AGPM) adds a **Change Control** folder 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** folder in the console tree. Each domain has a **Change Control** folder under it, and there is one archive of Group Policy objects (GPOs) per domain.

Within the details pane there are four primary tabs, providing access to both GPO-level settings and domain-level settings and commands for AGPM. Additionally, there are Administrative template settings specific to 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
- [Production Delegation Tab](#): Production environment delegation
- [Administrative Templates Folder](#): Central configuration of logging and tracking, archive locations, and the visibility of features

### **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 following secondary tabs filter the list of GPOs displayed:

- **Controlled:** GPOs managed by Advanced Group Policy Management (AGPM)
- **Uncontrolled:** GPOs not managed by AGPM
- **Pending:** GPO changes awaiting approval by an Approver

- **Templates:** GPO templates for creating new GPOs and comparing to existing GPOs
- **Recycle Bin:** Deleted GPOs

The **Contents** tab and its secondary tabs provide details about each GPO and access to the history of each GPO:

- [Contents Tab Features](#)
- [History Window](#)

When you right-click GPOs on any secondary tab, a shortcut menu unique to that tab is displayed, providing commands for managing the GPOs:

- [Controlled GPO Commands](#)
- [Uncontrolled GPO Commands](#)
- [Pending GPO Commands](#)
- [Template Commands](#)
- [Recycle Bin Commands](#)

#### Additional references

- [User Interface: Advanced Group Policy Management](#)

## Contents Tab Features

Each secondary tab within the **Contents** 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 attributes for each GPO. You can use the **Search** box to search for GPOs with specific attributes. For more information, see [Search and Filter the List of GPOs](#).

GPO attribute	Description
<b>Name</b>	Name of the GPO.
<b>State</b>	The state of the selected GPO
<b>Changed By</b>	The Editor who checked in or the Approver who deployed the selected GPO.
<b>Change Date</b>	For a controlled GPO, the most recent date it was checked in after being modified or checked out to be modified. For an uncontrolled GPO, the date when it was last modified.
<b>Comment</b>	A comment entered by the person who checked in or deployed a GPO at the time that it was modified. Useful for identifying the specifics of the version in case of the need to

GPO attribute	Description
	roll back to an earlier version.
<b>Computer Version</b>	Automatically generated version of the Computer Configuration part of the GPO.
<b>User Version</b>	Automatically generated version of the User Configuration part of the GPO.
<b>GPO Status</b>	The Computer Configuration and the User Configuration can be managed separately. The GPO Status indicates which portions of the GPO are enabled.
<b>WMI Filter</b>	Display any WMI filters that are applied to this GPO. WMI filters are managed under the <b>WMI Filters</b> folder for the domain in the console tree of the GPMC.

### 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, Reviewer, and AGPM Administrator) or a customized combination of permissions.

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

### 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 record of events in the lifetime of the selected GPO. From the **History** window, you can obtain a report of the settings in a version of the GPO, compare multiple versions of a GPO, or roll back to an earlier version of a GPO.

### Filtering events in the History window

The tabs within the **History** window filter the states in the history of the GPO.


Tabs	Filtering
<b>All States</b>	Display all states in the history of the GPO.
<b>Unique Versions</b>	Display only unique versions of the GPO checked into the archive. The version deployed to the production environment, shortcuts to unique versions, and informational states are omitted from this list.

### Event information

Information is provided for each state in the history of the GPO.

GPO attribute	Description
<b>Change Date</b>	Time stamp of when the action in the <b>State</b> column was performed.
<b>State</b>	A state in the history of the GPO.
<b>Changed By</b>	The person who checked in or deployed the GPO.
<b>Comment</b>	A comment entered by the person who checked in or deployed a GPO at the time that this version was changed, useful for identifying the specifics of the version in case of the need to roll back to an earlier version.
<b>Deletable</b>	Whether this version of the GPO can be deleted if the number of unique versions of



GPO attribute	Description
	<p>each GPO retained in the archive is limited.</p> <p> <b>Note</b>            You can change whether a version of a GPO can be deleted by right-clicking the GPO and then clicking <b>Do Not Allow Deletion</b> or <b>Allow Deletion</b>.</p>
<b>Computer Version</b>	Automatically generated version of the Computer Configuration part of the GPO.
<b>User Version</b>	Automatically generated version of the User Configuration part of the GPO.
<b>GPO Status</b>	The Computer Configuration and the User Configuration can be managed separately from each other. This status shows which portions of the GPO are enabled.
<b>Source GPO Information</b>	For a GPO that has been imported from another forest, the original GPO name, domain, and user and date associated with the last change.

## Reports

The **Settings** and **Differences** buttons display reports about GPO settings for the GPO version or versions selected. Also, right-clicking a GPO version or versions provides the option to display XML-based reports.

Button	Effect
<b>Settings</b>	Generate an HTML-based report displaying the settings within the selected version of the GPO.
<b>Differences</b>	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

Symbol	Meaning	Color
[#]	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 items (one present only in the first GPO, one present only in the second), instead of one item that has changed.

#### Additional references

- [Contents Tab](#)

## Controlled GPO Commands

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. This menu includes whichever of the following options are applicable.

#### Control and history

Command	Effect
<b>New Controlled GPO</b>	Create a new GPO with change control managed through AGPM and deploy it to the production environment of the domain. If you do not have permission to create a GPO, you are prompted to submit a request. (This option is displayed if no GPO is selected when right-clicking in the <b>Group Policy Objects</b> list.)
<b>History</b>	Open a window listing all versions of the selected GPO saved within the archive. From the history, you can obtain a report of the

Command	Effect
	settings within a GPO, compare two versions of a GPO, compare a GPO to a template, or roll back to an earlier version of a GPO.

## Reports

Command	Effect
<b>Settings</b>	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.
<b>Differences</b>	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
<b>Edit</b>	Open the <b>Group Policy Management Editor</b> window to change the selected GPO.
<b>Check Out</b>	Obtain a copy of the selected GPO from the archive for offline editing and prohibit anyone else from editing the GPO until it is checked back into the archive. Check Out can be overridden by an AGPM Administrator (Full Control).
<b>Check In</b>	Check the edited version of the selected GPO into the archive, so other authorized Editors can make changes or an Approver can deploy the GPO to the production environment of the domain.
<b>Undo Check Out</b>	Return a checked out GPO to the archive without any changes.

## Version management

Command	Effect
<b>Import from Production</b>	For the selected GPO, copy the version in the production environment of the domain to the archive.
<b>Import from File</b>	Replace the policy settings of the selected, checked-out GPO with those from a GPO backup file.
<b>Delete</b>	Move the selected GPO to the Recycle Bin and indicate whether to leave the deployed version (if one exists) in production or to delete the deployed version in addition to the version in the archive. If you do not have permission to delete a GPO, you are prompted to submit a request.
<b>Deploy</b>	Move the selected GPO that is checked into the archive to the production environment of the domain. 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.
<b>Export to</b>	Save the selected GPO to a backup file so that you can copy it to another domain.
<b>Label</b>	Mark the selected GPO with a descriptive label (such as "Known good") and comment for record keeping. Labels appear in the <b>State</b> column and comments in the <b>Comment</b> column of the <b>History</b> window. They help you identify earlier versions of a GPO so that you can roll back if a problem occurs.
<b>Rename</b>	Change the name of the selected GPO. If the GPO has already been deployed, the name will be updated in the production environment of the domain when the GPO is redeployed.
<b>Save as Template</b>	Create a new template based on the settings of the selected GPO.

## Miscellaneous

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

### Additional references

- [Contents Tab](#)
- [Performing Editor Tasks](#)
- [Performing Approver Tasks](#)
- [Performing Reviewer Tasks](#)

## Uncontrolled GPO Commands

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
<b>History</b>	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 an earlier version of a GPO.
<b>Control</b>	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
<b>Save as Template</b>	Create a new template based on the settings of the selected GPO.

## Reports

Command	Effect
<b>Settings</b>	Generate an HTML-based or XML-based report displaying the settings within the selected GPO.
<b>Differences</b>	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
<b>Refresh</b>	Update the display of the Group Policy Management Console (GPMC) to incorporate any changes. Some changes are not visible until the display is refreshed.
<b>Help</b>	Display help for AGPM.

## Additional references

- [Contents Tab](#)
- [Performing Editor Tasks](#)
- [Performing Approver Tasks](#)
- [Performing Reviewer Tasks](#)

## Pending GPO Commands

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
<b>History</b>	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 an earlier version of a GPO.
<b>Withdraw</b>	Withdraw your pending request to create, control, or delete the selected GPO before the request has been approved.
<b>Approve</b>	Complete a pending request from an Editor to create, control, or delete the selected GPO.
<b>Reject</b>	Deny a pending request from an Editor to create, control, or delete the selected GPO.

### Reports

Command	Effect
<b>Settings</b>	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.
<b>Differences</b>	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
<b>Refresh</b>	Update the display of the Group Policy

Command	Effect
	Management Console (GPMC) 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](#)

### Template Commands

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
<b>New Controlled GPO</b>	Create a new GPO based on the selected template. The option to deploy the new GPO to the production environment of the domain 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 <b>Group Policy Objects</b> list.)



## Reports

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

## Template management

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

## Miscellaneous

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

## Additional references

- [Contents Tab](#)
- [Performing Editor Tasks](#)
- [Performing Reviewer Tasks](#)

## Recycle Bin Commands

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
<b>Settings</b>	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.
<b>Differences</b>	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
<b>Destroy</b>	Remove the selected GPO from the <b>Recycle Bin</b> , so it can no longer be restored.
<b>Restore</b>	Move the selected GPO from the <b>Recycle Bin</b> to the <b>Controlled</b> tab. This does not restore the GPO to the production environment.

### Miscellaneous

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

### Additional references

- [Contents Tab](#)
- [Performing Approver Tasks](#)
- [Performing Reviewer Tasks](#)

## 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
<b>From e-mail address</b>	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.
<b>To e-mail address</b>	A comma-delimited list of e-mail addresses of Approvers to whom notification is to be sent
<b>SMTP server</b>	The name of the e-mail server, such as mail.contoso.com
<b>User name</b>	A user with access to the SMTP server
<b>Password</b>	User's password for authentication to the SMTP server
<b>Confirm password</b>	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
<b>Add</b>	Add a new entry to the security descriptor. Any users or groups in Active Directory can be added as Group Policy administrators.
<b>Remove</b>	Remove the selected Group Policy administrators from the Access Control List.
<b>Properties</b>	Display the properties for the selected Group Policy administrators.
<b>Advanced</b>	Open the <b>Access Control List Editor</b> .

#### 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, and to delete older versions of Group Policy objects (GPOs) from the archive to conserve disk space on the AGPM Server.

### Specifying the AGPM Server

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. The default port for Advanced Group Policy Management (AGPM) is port 4600.

If the AGPM Server connection is centrally configured using Administrative template settings, the options on this tab for configuring the connection are unavailable. For more information, see [Configure AGPM Server Connections](#).

### Deleting old GPO versions

By default, all versions of every controlled GPO are retained in the archive. However, you can configure the AGPM Service to limit the number of versions retained for each GPO and

automatically delete the oldest version when that limit is exceeded. Only GPO versions displayed on the **Unique Versions** tab of the **History** window count toward the limit.



#### Notes

The maximum number of unique versions to store for each GPO does not include the current version, so entering 0 retains only the current version. The limit must be no greater than 999 versions.

When a GPO version is deleted, a record of that version remains in the history of the GPO, but the GPO version itself is deleted from the archive. You can prevent a GPO version from being deleted by marking it in the history as not deletable.

#### Additional references

- [User Interface: Advanced Group Policy Management](#)
- [Performing AGPM Administrator Tasks](#)
- [Performing Reviewer Tasks](#)

## Production Delegation Tab

The **Production Delegation** tab on the **Change Control** pane provides a list of users and groups who have domain-level access to controlled Group Policy objects (GPOs) in the production environment and indicates the allowed permissions of each user or group.

This tab allows an AGPM Administrator (Full Control) to modify the default delegation of access to GPOs in the production environment of the domain, adding or removing users and groups, and modifying the allowed permissions for each user and group.

Button	Effect
<b>Add</b>	Add a new entry to the security descriptor.
<b>Remove</b>	Remove the selected users or groups from the Access Control List.
<b>Properties</b>	Display the properties for the selected user or group. The properties page is the same one displayed for an object in <b>Active Directory User and Computers</b> .

#### Additional references

- [User Interface: Advanced Group Policy Management](#)
- [Performing AGPM Administrator Tasks](#)

## Administrative Templates Folder

The Administrative template settings for Advanced Group Policy Management (AGPM) enable you to centrally configure logging and tracing options for AGPM Clients and AGPM 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** folder 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\Policies\Administrative Templates\Windows Components\AGPM when editing a GPO.

**Trace file locations:**

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

Setting	Effect
<b>AGPM: Configure logging</b>	This policy setting allows you to turn on and configure logging for AGPM. This setting affects both client and server components of AGPM.

**Additional references**

- [Administrative Templates Folder](#)

### 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\Policies\Administrative Templates\Windows Components\AGPM when editing a GPO.

Setting	Effect
<b>AGPM: Specify default AGPM Server (all</b>	This policy setting allows you to specify a

Setting	Effect
domains)	default AGPM Server for all domains. This is used only by AGPM Clients, and restricts Group Policy administrators from connecting to another archive. You can override this default for individual domains using the <b>AGPM: Specify AGPM Servers</b> setting.
<b>AGPM: Specify AGPM Servers</b>	This policy setting allows you to specify the AGPM Servers for individual domains. This is used only by AGPM Clients, and restricts Group Policy administrators from connecting to a different archive for the specified domain. To specify a default AGPM Server, use the <b>AGPM: Specify default AGPM Server (all domains)</b> setting and use this policy setting to override the default on a per domain basis.

#### Additional references

- [Administrative Templates Folder](#)
- [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** folder 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\Policies\Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted Snap-ins\Extension Snap-ins when editing a GPO.

Setting	Effect
<b>AGPM: Show Change Control tab</b>	This policy setting allows you to control the visibility of the <b>Change Control</b> folder in the Group Policy Management Console (GPMC).
<b>AGPM: Show History tab for linked GPOs</b>	This policy setting allows you to control the visibility of the <b>History</b> tab provided by AGPM when you view a linked GPO in the GPMC.
<b>AGPM: Show History tab for GPOs</b>	This policy setting allows you to control the visibility of the <b>History</b> tab provided by AGPM when you view a GPO in the GPMC.

**Additional references**

- [Administrative Templates Folder](#)