Quest

Quest® GPOADmin® 5.22

User Guide

© 2026 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copy. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
10801 N. Mopac Expressway
Building 3, Suite 400
Austin, TX 78759

Refer to our website (www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at www.quest.com/legal.

Trademarks

Quest Software, Quest, the Quest logo, GPOADmin, and Change Auditor are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

> **CAUTION:** **A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

> **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Quest GPOADmin User Guide
Updated - May 2026
Software Version - 5.22

Contents

Introducing Quest GPOADmin 7
GPOADmin overview 7
GPOADmin security overview 8
GPOADmin features 10
Client/server architecture 10
Multiforest support 11
Group Policy Management Console extension 12
Version control 12
Change approval process 12
Role-based delegation 13
Notification system 15
GPO ACL editor 15
Reporting options 15
Customized views 15
Offline GPO testing 16
Custom workflow actions 16

Configuring GPOADmin 17
Configuring the Version Control server 18
Setting permissions on AD LDS 21
Setting permissions when using SQL as the configuration store 21
Port requirements 22
Using a custom port 23
Editing the Version Control server properties 24
Editing the Version Control server configuration store 31
Replacing the Version Control server configuration settings 33
Migrating from AD/AD LDS to a SQL configuration store 33
Changing the Service Account 35
Root container assignment 36
Restricting GPO management for specific domains 36
Configuring role-based delegation 38
Creating roles 41
Editing roles 42
Delegating roles 42
Restricting access to objects 42
Adding notifications for users 43
Selecting events on which to be notified 44
Restricting inheritance on notifications 44
Creating email templates 44
Working with Protected Settings policies 46
Rights and role for Protected Settings for GPOs 47
Create a Protected Settings policy 48
Protecting policy settings based on extensions 49

Generating Protected Settings policies reports . . . 50
Using Protected Settings policies . . . 50
Checking a GPO against a Protected Settings policies and blocked extensions . . . 51
Validating a GPO against a Protected Settings policies and blocked extensions before a check-in . . . 51
Working with Protected Settings Policy Baselines . . . 52

Using GPOADmin . . . 53
Connecting to the Version Control system . . . 54
Restricting search scope . . . 54
Working with multiple connections . . . 54
Version Control data in the directory . . . 55
Navigating the GPOADmin console . . . 55
Search folders . . . 56
Creating custom search folders . . . 56
Accessing the GPMC extension . . . 57
Configuring user preferences . . . 58
Working with the live environment . . . 58
Registering objects . . . 58
Registered status . . . 60
Removing registered objects . . . 63
Viewing the live environment . . . 63
Working with controlled objects (version control root) . . . 64
Creating a custom container hierarchy . . . 64
Selecting security, levels of approval, and notification options . . . 65
Viewing the differences between objects . . . 65
Copying/pasting objects . . . 66
Proposing the creation of controlled objects . . . 67
Merging GPOs . . . 70
Restoring an object to a previous version . . . 70
Restoring links to a previous version . . . 72
Managing your links with search and replace . . . 73
Linking GPOs to multiple Scopes of Management . . . 74
Managing compliance issues automatically with remediation rules . . . 74
Validating GPOs . . . 75
Managing GPO revisions with lineage . . . 76
Setting the change window for specific actions . . . 76
Working with registered objects . . . 77
Working with available objects . . . 84
Working with checked out objects . . . 87
Working with objects pending approval and deployment . . . 88
Checking compliance . . . 93
Editing objects . . . 95
Editing GPOs . . . 95
Editing Intune objects (Configuration profiles and Compliance policies) . . . 96
Editing WMI filters . . . 97
Editing scripts . . . 97
Linking GPOs . . . 98

Synchronizing GPOs 99
Enabling synchronization 99
Working with GPO synchronizations 99
Generating Synchronized GPO report 103
Exporting and importing 103
Export objects 103
Exporting GPO registry settings as a Desired State Configuration resource file 105
Import objects 105

Creating Reports 107
Available reports 108
Controlled object reports 109
Diagnostic and troubleshooting reports 115
Live, working copy, latest version, and differences reports 124
Historical Settings Reports 124
Creating RSoP validation reports 125
Exporting registry settings 126
Working with report folders 127
Managing report folders 127
Exporting reports to CSV and importing into Excel 127

Appendix: Windows PowerShell Commands 129
Introduction 130
GPOADmin scripts 132
Available commands 134
GPOADmin PowerShell provider extensions 142
Using the GPOADmin PowerShell commands (Examples) 143
Loading the GPOADmin modules 144
Extracting help for GPOADmin commands 144
Managing objects 146
Gathering object and GPOADmin information 152
Utility commands 154
Administrative commands 156
Protected Settings commands 160

Appendix: GPOADmin Event Log 162
What is the GPOADmin event log? 163
Interpreting the GPOADmin event log 163
Example GPOADmin events 165

Appendix: GPOADmin Backup and Recovery Procedures 166
GPOADmin Backup Requirements 167
Restoring GPOADmin 167

Appendix: Customizing your workflow 168
What is a custom workflow action? 169
Working with custom workflow actions in the Version Control system 170

Working with the custom workflow actions xml file 171
Actions 171
Predefined Tags 173
Conditions 175
Example of a complete pre-action 177
Troubleshooting custom workflow actions 177

Appendix: GPOADmin Silent Installation Commands 178
Installing GPOADmin with msiexec.exe 179
All components (Complete GPOADmin installation) 179
Client and components 179
Watcher Service 180
GPMC Extension 181

Appendix: Configuring Gmail for Notifications 182
Using Gmail for Workflow Approvals 182
Creating a Gmail Credentials File 182

Appendix: Registering GPOADmin for Microsoft 365 Exchange Online 184

Appendix: GPOADmin with SQL Replication 185

Appendix: Feature Support 189

About Us 192

1

Introducing Quest GPOADmin

- GPOADmin overview
- GPOADmin security overview
- GPOADmin features

GPOADmin overview

Security issues are becoming paramount within organizations. Within Active Directory, Group Policy Objects (GPOs) are at the forefront of an organization's ability to roll out and maintain functional security. Core aspects such as password policies, log on hours, software distribution, and other crucial security settings are handled through GPOs. Organizations need methods to control the settings of these GPOs and to deploy GPOs in a meaningful and safe manner with confidence. Since GPOs are so important to the proper operating of the Active Directory, organizations also need methods to restore GPOs when they are either incorrectly updated or have become corrupt.

GPOADmin offers a mechanism to control this highly important component of Active Directory. First, GPOs are backed up in a secure manner, then placed under version control. When changes are made, a backup of the GPO is again made. Changes are managed from the Version Control system, and approvals for any changes are required. Stored GPOs can be retrieved if the current GPO in the directory is not valid for any reason. This means that GPOs are managed and deployed with a secure rollback capability. When an issue does arise, the time between the discovery of the issue and its resolution is kept to a minimum, because a previous version of the GPO can be restored.

GPO implementation is a key consideration when planning your organization’s Active Directory structure. GPOs streamline management of all user, computer, and configuration issues to ensure smooth day-to-day network operation.

You can use GPOs to control specific configurations applied to users and computers through policy settings. When grouped, the policy settings form a single GPO, which you can then apply to sites, domains, and OUs.

You can define settings for users and computers and then rely on the system to enforce the policies. GPOs provide the following types of policies:

- Computer configuration policies, such as security and application settings, which are applied when the operating system is initialized.
- User configuration policies, such as desktop settings, security settings, logon and log off scripts, which are applied when users log on to the computer.

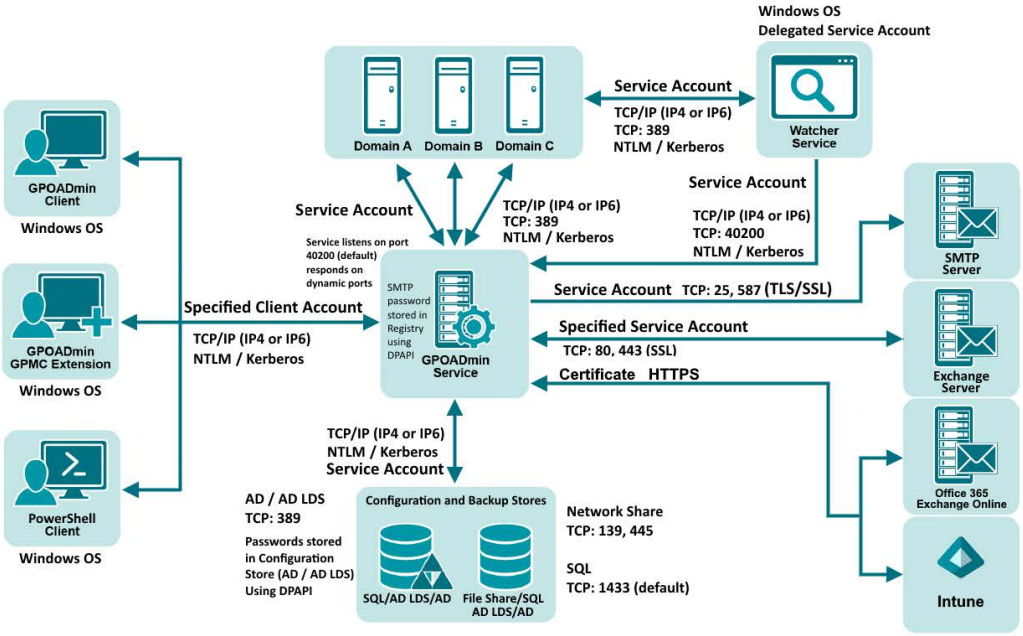
GPOADmin security overview

The following diagram provides an overview of the interactions and communication protocols between service accounts, client accounts, and servers within a Windows OS environment.

It illustrates how the GPOAdmin client, AD/ADS Server, SQL Server, network share, SMTP Service, and Exchange Service interact using various protocols like TCP/IP (IPv4 and IPv6), NTLM/Kerberos authentication, and HTTPS certificates.

It also shows the use of service accounts for accessing these services securely using different authentication methods such as NTLM/Kerberos and HTTPS certificates.

Figure 1. Communication Protocols Overview

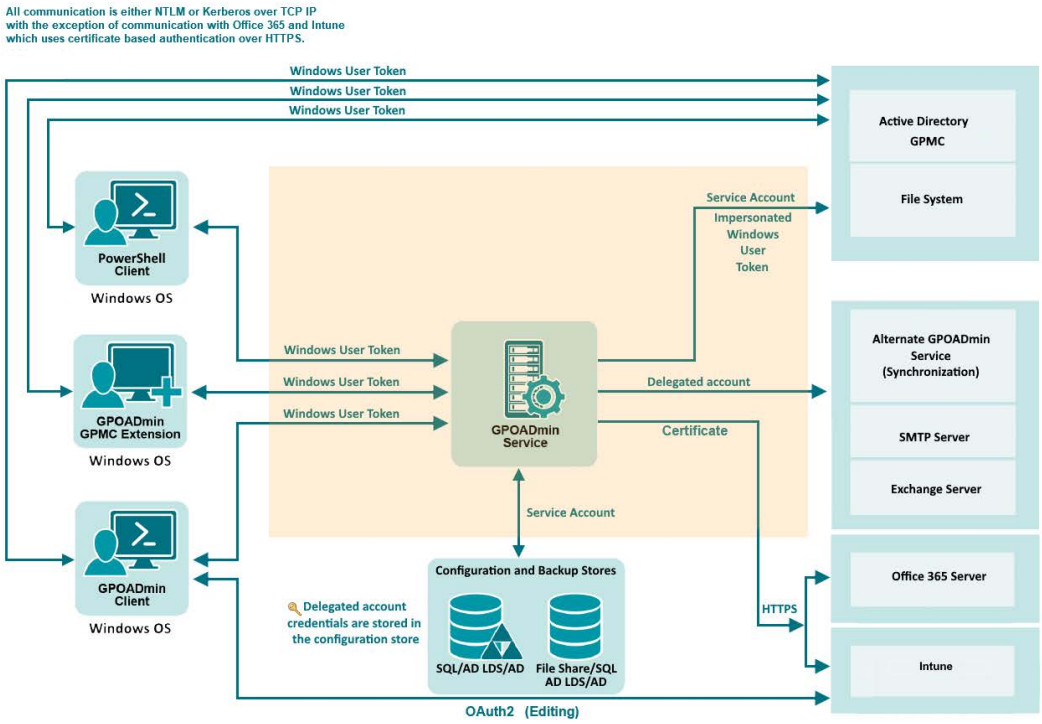


The following diagram illustrates the architecture and communication flow of a system involving the GPOADmin Service. The main components include:

- GPOADmin Service: Central service that manages registered Objects.
- Clients: Various clients such as PowerShell Client, GPMC Extension, and GPOADmin client on Windows OS.
- Configuration and Backup Stores: Stores configuration data and backups.
- Other components accessed by the service and users: Includes Active Directory, the file system, SMTP, Exchange Office365, and Intune.

The diagram shows how different clients communicate with the GPOADmin Service using Windows User Tokens or Delegated Accounts. The service uses certificates for secure communication over HTTPS.

Figure 2. Architecture and Communication Overview



GPOADmin features

Group policy version control is crucial to an organization's efforts to safeguard continual operation. GPOs can have a negative impact on users' ability to access the network and resources they need to work efficiently.

GPOADmin allows administrators to check the status of a GPO, back up changes into a common data repository, and report on that repository as required. If a GPO has become corrupt or is no longer in a working state, any previous iteration of a GPO can be retrieved.

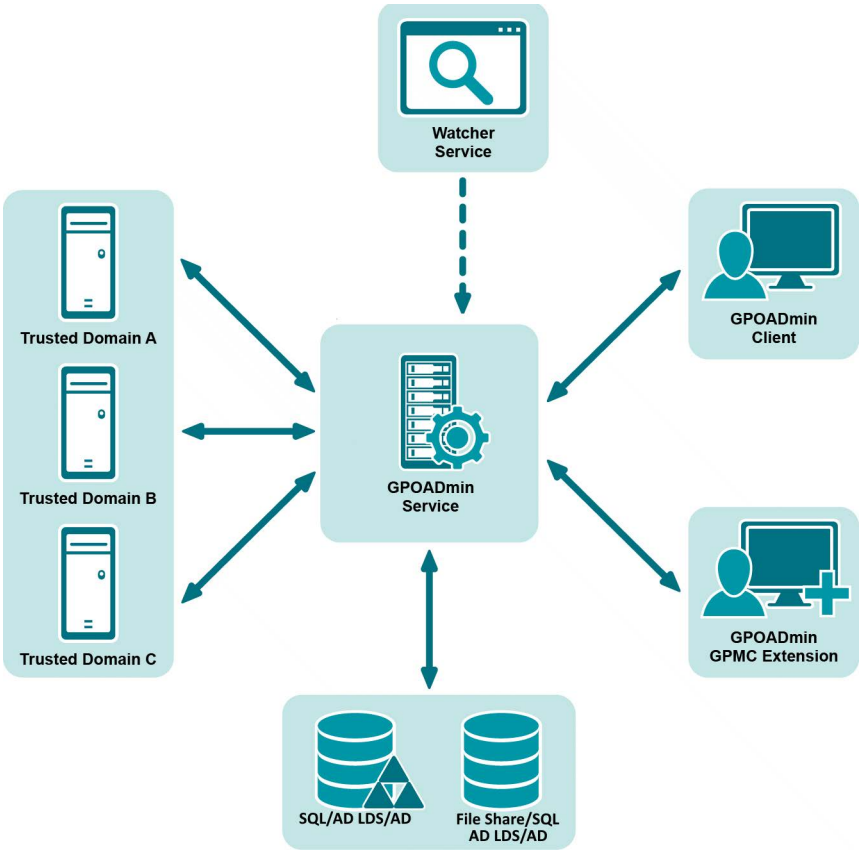


Figure 3. Group Policy Workflow

Client/server architecture

The client/server architecture facilitates granular security and delegation. GPOADmin runs under the security context of a privileged service account that must have full access to GPOs in the managed forest.

This architecture allows for multiple servers to be installed within the same forest, allowing you to manage domains independently. Clients can connect to any deployed server within any Active Directory forest. GPOADmin maintains a most recently used (MRU) list of servers to which the users have previously connected to facilitate quick subsequent server connections.

NOTE: For more information on permissions required for the Service Account, see the Quest GPOADmin Quick Start Guide.

Multiforest support

The GPOADmin management console allows you to connect to multiple GPOADmin Server Service instances within the same console. The GPOADmin Server Service could be from a trusted or non-trusted domain or forest. You can provide credentials for all non-trusted domains and forests while connecting to the nontrusted environments. By enumerating all GPOADmin Server Service instances, you can manage all Version Control systems from a single console, thus making it much easier to transition GPOs from a test environment to production.

Managing Multiple Forests with Bidirectional Trust

GPOADmin can manage GPOs in external forests or domains as long as every managed domain has a bidirectional trust relationship, whether transitive or non-transitive, with the domain hosting the GPOADmin server.

GPOADmin consoles used to connect to the GPOADmin server must also reside in domains that have bidirectional trust with:

- All domains managed by GPOADmin.
- The GPOADmin server's domain.

Adding Non-Visible Domains

If a domain that meets the required trust configuration does not appear in GPOADmin, it can be added manually by configuring the following registry settings:

1. Open the following registry path: HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\VCConfig
2. Add a new multi-string (REG_MULTI_SZ) value named: ExternalDomains
3. For each bidirectionally trusted domain, add its fully qualified domain name (FQDN) to this value, one FQDN per line.

NOTE: When working with multiple forests without bidirectional trust relationships, it is recommended to have a GPOADmin server per forest. This ensures a more secure configuration where only native security principals perform the actions against the specific forest.

NOTE: **Known Limitations of Managing objects in an untrusted domain**

Although not recommended, if you plan to manage GPOs in an untrusted domain from your local client console, the following limitations must be considered:

- File and directory browsing is performed locally on the client computer.
- Users and groups can only be selected from the client domain and trusted domains.
- Domain-specific information of workflow enabled Group Policy Objects cannot be set.
- Internet Protocol Security (IPSec) do not load in the Group Policy editor when editing a workflow enabled Group Policy Object.
- Workflow disabled Group Policy Objects cannot be edited.
- Workflow disabled Group Policy Objects cannot be copied.
- Workflow disabled Group Policy Objects cannot be renamed.
- Workflow enabled Group Policy Object cannot be edited.
- Workflow enabled Group Policy Objects can only be copied to an untrusted domain when the GPOADmin client and source Group Policy Object are in the same domain.
- Workflow enabled Group Policy Objects can only be moved to an untrusted domain when the GPOADmin client and source Group Policy Object are in the same domain.
- Objects cannot be exported to the Live Environment of an untrusted domain.
- Objects cannot be imported from the Live Environment of an untrusted domain.

Group Policy Management Console extension

You can work in the Group Policy Management Console (GPMC) to perform many GPO-related tasks. GPOADmin comes with two interfaces — the GPOADmin Console, and the GPMC Extension. The console provides full functionality, and is intended for administrators responsible for a wide variety of tasks. The GPMC Extension is a convenient tool for users who are already comfortable with the GPMC, or for GPO administrators who do not need the advanced features of the GPOADmin Console.

The following tasks can be performed using the GPMC Extension:

- Create GPOs
- Register and unregister GPOs
- Create labels
- Cloak and uncloak
- Lock and unlock
- View and edit properties
- View the history
- View the differences between versions
- Roll back a GPO to a previous version
- Check in and out
- Edit
- Request approval
- Approve or reject changes
- Deploy
- Generate Working Copy, Latest Version and Differences reports

For more information, see Using GPOADmin on page 53 and Accessing the GPMC extension on page 57.

Version control

GPOs, scripts, DSC scripts, WMI filters, Intune objects, and Scopes of Management (domains, sites, and OUs) links can be stored and backed up in a secure Active Directory, AD LDS, network share, or SQL repository. Objects that are stored within the Control system are labeled with a version number. You can view all changes made to the controlled object through the object history and through numerous reports.

For detailed information, see Registering objects on page 58, Proposing the creation of controlled objects on page 67 and Controlled object reports on page 109.

Change approval process

All changes made within the Version Control system are not rolled out into the online Active Directory environment until assigned users approve and deploy them.

You can enforce a multi-approval process at the container and object level so that all changes made to the live production environment are approved by all approvers. Ensuring the approval process uses the combined agreement of multiple approvers rather than just one provides better security.

Deploying changes within the system is a critical process that affects the live environment. To minimize the impact of disruption, perform this when the impact to users is minimal as the changes to the GPO might alter the behavior of particular systems.

To avoid any issues, you can schedule the deployment of the changes for a specific date and time that best suits your needs.

For detailed information, see Approving and rejecting edits on page 90 and Deploying objects (scheduling and associated items) on page 91.

Role-based delegation

GPOADmin users can create and define roles that consist of a set of roles to perform actions on the Version Control system. These roles can delegate users-specific access to resources within the system. GPOADmin includes predefined built-in roles (Moderator, System Administrator, and User), and granular roles users can define through a custom role. For a list of roles, see Configuring role-based delegation.

Table 1. Custom s

	Users with this can...
Version Controlled Objects	• Block Inheritance for SoM links • Cloak/Uncloak • Compliance Action • Create • Delegate Security • Delete • Delete links outside of workflow • Deploy • Edit • Edit Lineage • Enable and Disable Workflow • Export • Label • Link • Lock/Unlock • Modify Approval Workflow • Modify Keywords • Modify Managed By • Modify System-Provided Security • Modify Security Filter • Read • Register • Run Contextual Reports • Run Reports • Set Remediation Rules • Synchronize • Undo Check-out • Unregister • View Cloaked

	Users with this can...
Version Control Containers	• Create Subcontainers • Delegate Container Security • Delete Container • Rename Container
Protected Settings	• Block Protected Settings Inheritance • Export Group Policy Objects as Protected Settings Policies • Modify Protected Settings • Modify Protected Settings Assignments • Modify Protected Settings Baseline Assignments • Modify Protected Settings Exclusions

Notification system

GPOADmin contains a rich notification system that allows users to control a wide variety of Version Control events, sending details by email as the events occur.

Users can subscribe to the notification service, which is based on a granular defined event trigger such as Register, Check In, Create, and Delete for each object under the Version Control system. For approve and reject notifications, the email includes information on who was the last to approve any changes and the date of the last approved change.

Reports are included in notification emails when more details are required. For example, check-in notifications come with a settings report (to show the settings that were checked in) and a difference report (to show the differences between this version and the last version).

In addition, Administrators can delegate notifications to users who do not use GPOADmin, but who for business reasons, must be notified when an object is created, modified, or deleted.

For detailed information, see Selecting events on which to be notified, Adding notifications for users, and Configuring user preferences.

GPO ACL editor

A security group, user, or computer must have both Read and Apply Group Policy permissions for a policy to be applied. By default, all users and computers have these permissions for all new GPOs. They inherit these permissions from their membership in the group Authenticated Users. In GPOADmin, aside from changing the Security Filter, you can also manage the permissions of a particular group. For example, if you do not want a GPO applied to a group of users you can easily configure the permission on a particular GPO (“Deny Apply Group Policy”) so that it is not applied to the group of users.

For more information, see Selecting security, levels of approval, and notification options on page 65.

Reporting options

GPOADmin allows you to configure real time (for quick regeneration of live data) and historical snapshot report templates. All reports now run asynchronously; therefore, you no longer have to wait until one report has rendered before initiating a new report.

For detailed reporting options, see Creating Reports on page 107.

Customized views

You can organize controlled objects into a user-defined container hierarchy. Each container has its own security descriptor in which trustees can be granted (delegated) roles to define access to the container, subcontainer, or simply a specific GPO within these containers.

Version Control Root Hierarchy should be used for administrator management as a means to organize many objects into a logical view based on their enterprise structure.

The Search folders allow you to quickly view controlled objects based on their state within the Version Control system. Search folders are used as an easy way for users to view the status of objects within the Version Control system.

For more information, see Creating a custom container hierarchy on page 64.

Offline GPO testing

Using the Export Wizard, you can test GPOs offline before implementing them. For more information, see Exporting and importing on page 103.

Custom workflow actions

You can extend GPOADmin's version control system to incorporate customized actions based on your organizations existing workflow. This allows you to customize and control the deployment of controlled objects (such as GPOs, scripts, DSC scripts, SOMs, and WMI filters) to meet your individual needs. For details, see Appendix: Customizing your workflow on page 168.

2

Configuring GPOADmin

- Configuring the Version Control server
- Setting permissions on AD LDS
- Setting permissions when using SQL as the configuration store
- Port requirements
- Editing the Version Control server properties
- Editing the Version Control server configuration store
- Replacing the Version Control server configuration settings
- Migrating from AD/AD LDS to a SQL configuration store
- Changing the Service Account
- Root container assignment
- Restricting GPO management for specific domains
- Configuring role-based delegation
- Restricting access to objects
- Adding notifications for users
- Selecting events on which to be notified
- Restricting inheritance on notifications
- Creating email templates
- Working with Protected Settings policies
- Working with Protected Settings Policy Baselines

Configuring the Version Control server

You must configure the Version Control server the first time that you connect to it.

To configure the Version Control server

NOTE: Configure the server using the GPOADmin console, even if you intend to use the GPMC Extension.

1. Right-click the **GPOADmin** node and select **Connect To**.
2. Select the required Version Control server and click **Connect** to connect with the current logged on user credentials. Alternatively, select the down arrow in the Connect button and select Connect As to enter new credentials (domain\user and password).
3. To save the credentials, select the **Remember my password** check box and click **OK**.

   For information about saving connections, see Connecting to the Version Control system on page 54.
4. In the Select a Configuration Store dialog, select SQL Server, AD LDS, or Active Directory for your configuration storage location.

   NOTE: Configuration Store Selection

   The best practice is to use:

   - SQL Server for optimal performance.
   - AD LDS for small environments. Quest uses the following criteria to define small environments. (These are guidelines and should not be considered as an exhaustive list.)
     - Domains with less than 500 registered objects that run searches on a regular basis.
     - Less than 500 registered containers.
     - Containers with objects nested no more than 3 levels deep.
   - Active Directory for legacy deployments. It is not recommended for new installations.

   IMPORTANT: Ensure that you are following the minimum permissions detailed in the Quick Start guide. The listed permissions help to secure the database by limiting the access to only the required accounts.

   a. If you select Active Directory, select the Domain Controller (DC) to be the Version Control server, (optionally) select **Use Secure LDAP** to protect your directory data and credentials during communication with Active Directory, and click **Next**.

      Any DC in any domain of the selected forest can be specified as the primary version control server. This server can be thought of as another FSMO role in the Microsoft sense (such as Schema master, PDC Emulator, and RID master).

      GPOADmin is a directory-enabled application and all its application information is stored in the configuration container of Active Directory. Because of how the information is stored, all information is automatically replicated to all other DCs. However, the primary version control server is the authoritative source for all version control actions. If it goes offline, users cannot perform actions such as check-in a desired group policy object change until the problem has been rectified.

   b. If you select AD LDS, enter the NetBIOS name of the computer you are installing to and the port number in the format: `server_name:port`, (optionally) select **Use SSL** to protect your directory data and credentials during communication with AS LDS, and click **Next**.

      For example, gpoadmin_svr: 389.

      NOTE: The username/port/server (but not password) will be cached, so the next time you open the console you will not need to enter this information.

   c. If you select SQL Server, choose the required SQL server, enter a name for the database, select the authentication method to access the server.

To connect as the current user, select NT Authentication.

Select the level of encryption for the connection. When enabled, SQL Server uses TLS encryption for data sent between the client and server.

NOTE: When using SQL as the Configuration or Backup store with GPOADmin, TLS 1.2 remains a requirement since SQL Server satellite services require TLS 1.2 to be enabled. For more information on TLS support, see Microsoft documentation.

Choose between:

- **Strict (SQL Server 2022, 2025, and Azure SQL)**: Select this option for Azure SQL Database and Azure SQL Managed Instance or when the instance has **Force Strict Encryption** enabled.
- **Mandatory**: Select this option when the instance has **Force Encryption** enabled. It can also be used when no encryption is configured for the instance, but **Trust server certificate** is enabled. While this method is less secure than installing a trusted certificate, it does support an encrypted connection.
- **Optional** (Default in GPOADmin)

Enabling **Trust Server Certificate**, when 'Optional' or 'Mandatory' encryption is selected, or if the server enforces encryption, means that SQL Server will not validate the server certificate on the client computer when encryption is enabled for network communication between the client and server.

Under **Host name in the certificate**, you can provide an alternate, yet expected, Common Name (CN) or Subject Alternative Name (SAN) in the server certificate for the connection to SSMS. You would use this option when the server name does not match the CN or SAN, for example, when using DNS aliases.

Leaving this option blank allows certificate validation to confirm that the CN or SAN matches the server name.

To connect using SQL credentials, select SQL Authentication and enter the username and password.

Click **Next** to continue.

NOTE:

- SQL Server (See the Release Notes for supported versions.)
- See Appendix: GPOADmin with SQL Replication to configure database replication for an SQL configuration store.
- When configuring GPOADmin to use an Azure SQL managed instance, you must specify the public endpoint including the port number, in the Server Name field in GPOADmin. For details on configuring a public endpoint, see Microsoft documentation.

NOTE: When using SQL replication with a SQL configuration store, objects may be incorrectly flagged as non-compliant. This occurs when SQL replication and Active Directory replication are on different cycles. To resolve this, GPOADmin provides a HashStorageProperties.ini file that allows you to store the comparison hash on the Active Directory object. The file is located in the GPOADmin installation directory and contains the information on the settings to change. Ensure that objects are in the available state prior to changing the values in this file.

SQL Injection inserts malicious code into SQL statements which can lead to security vulnerabilities. To protect your environment from a SQL Injection attack, you can mark SQL statement inputs that are not permitted. See Editing the Version Control server properties. By default, we have marked the following

inputs as not permitted. If you allow these inputs, malicious code may be inserted in a SQL statement resulting in security vulnerabilities:

Table 2. SQL inputs

Input	Description
:	Denotes the end of a SQL query. Allowing this character can permit malicious queries to be included in user input.
--	All trailing input is interpreted as a comment until the new line character.
/*	The character combination used to denote the start of a block comment. All trailing input is interpreted as a comment until the comment end delimiter.
*/	The character combination used to denote the end of a block comment. Input between the comment start delimiter and the comment end delimiter is interpreted as a comment.
xp_	Extended procedures are routines residing in DLLs that function similarly to regular stored procedures. The extended stored procedure function is run under the security context of Microsoft SQL Server.
\AUX	Generally, the AUX port on a PC is computer port 1 (COM1), which is the first serial port with a preconfigured assignment for serial devices. File paths can be constructed using this input.
\CLOCK$	The system clock. File paths can be constructed using this input.
\COM1	The first Communications port. File paths can be constructed using this input.
\COM2	The second Communications port. File paths can be constructed using this input.
\COM3	The third Communications port. File paths can be constructed using this input.
\COM4	The forth Communications port. File paths can be constructed using this input.
\COM5	The fifth Communications port. File paths can be constructed using this input.
\COM6	The sixth Communications port. File paths can be constructed using this input.
\COM7	The seventh Communications port. File paths can be constructed using this input.
\COM8	The eighth Communications port. File paths can be constructed using this input.
\CON	A common device name for the keyboard and screen. File paths can be constructed using this input.
\CONFIG$	A configuration information file. File paths can be constructed using this input.
\LPT1	The first line print terminal. File paths can be constructed using this input.
\LPT2	The second line print terminal. File paths can be constructed using this input.
\LPT3	The third line print terminal. File paths can be constructed using this input.
\LPT4	The fourth line print terminal. File paths can be constructed using this input.
\LPT5	The fifth line print terminal. File paths can be constructed using this input.
\LPT6	The sixth line print terminal. File paths can be constructed using this input.
\LPT7	The seventh line print terminal. File paths can be constructed using this input.
\LPT8	The eighth line print terminal. File paths can be constructed using this input.
\NUL	The NUL port. File paths can be constructed using this input.
\PRN	The DOS name for the first connected parallel port. File paths can be constructed using this input.

5 Select where you want to store the historical backup information.

You have the option of choosing Configuration store location, a network share, SQL Server, AD LDS, or the Directory Configuration Location.

TIP: The best practice is to use a network share.

Table 3. Storage Options

Option	If you select this option
Network Share **NOTE:** Recommended method as it provides a high level of performance and a low level of configuration and maintenance overhead.	Browse to and select the required network share or directory, and click **Next**.
SQL Server	Enter the server name and the required authentication information, and click **Next**. **NOTE:** If the server is installed as a unique instance, it must be specified as servername\instancename rather than just the SQL Server name.
AD LDS	Enter the server and port name, and click **Next**. For more information about an AD LDS deployment, see Setting permissions on AD LDS on page 21.
Directory Configuration Location	This option is only available if you have selected to use Active Directory or AD LDS as your configuration store.

6 Select which users should have the right to connect to and administer the Version Control server, and click **Next**.

7 Click **Finish**.

Now that the system has been configured, users can connect to and use the version control features.

NOTE: Users with the appropriate rights can modify the server settings at anytime by right-clicking the GPOADmin node and selecting **Options**.

Setting permissions on AD LDS

To use GPOADmin with an AD LDS deployment, users must be assigned the Administrators role.

To set permissions on AD LDS

1 Open ADSI-Edit (ADSI-Edit is installed as part of the AD LDS tools.)

2 Connect to the configuration naming context and browse to the roles container.

3 To grant the user rights, right-click the **Administrators** role and select **Properties**.

4 Browse to the member attribute and click **Edit**.

5 Add the service account to the selected role.

NOTE: If necessary, you can use the AD LDS support tool dsacls.exe to fine-tune the rights given by these roles or to grant specific rights to users.

Setting permissions when using SQL as the configuration store

Perform the following after installing GPOADmin and before configuring the GPOADmin server.

1 Run the database script GPOADmin.sql.

a In Microsoft SQL Server Management Studio, select **File | Open | File** or press the control key and the O key (Ctrl + O).

b In the Open File dialog, select the GPOADmin.sql file and press **OK**. This file is located in the GPOADmin server install directory by default, but if your SQL server is on a different computer, the file can be copied.

c If you want to create the database with a different name other than the default name of GPOADmin, change the name from GPOADmin on line 4 and line 7 to the name you want to use.

d Click the **Execute** button or press **F5** to create the database.

2 Run the InitializeDatabase stored procedure on the newly created database.

a Create a new query by pressing the **New Query** button.

b Set the available database to the name of your GPOADmin database or type **USE [DATABASE_NAME]** where **DATABASE_NAME** is the name of your GPOADmin database.

c On the next line, type **EXEC InitializeDatabase.**

d When ready, click the **Execute** button or press **F5** to run the command.

3 Create a login for the GPOADmin service account.

a In Microsoft SQL Server Management Studio, navigate to **Security**, then **Logins**.

b Right-click **Logins** and select **New Login**.

c On the General page, enter the name of the service account in the **Login name** field.

d Select Windows authentication to connect as the GPOADmin service account or SQL Server Authentication to connect as a SQL account. SQL authentication is useful if you want to use this database as the configuration store for a GPOADmin installation in another untrusted domain.

e Set the **Default database** property to the name of your GPOADmin database.

f On the Server Roles page, check the **public** server role.

g On the User Mapping page, under **Users mapped to this login**, check the name of your GPOADmin database. Under Database role membership for the selected database, check **db_owner** and **public**.

h Click **OK** to close the properties page.

Port requirements

CAUTION: Conduct a thorough threat analysis before opening these services to an untrusted network.

The following ports must be open for the application to function correctly:

Name resolution can be achieved using DNS on port 53 or WINS (downlevel) on port 137.

Between the client and the GPOADmin Server:

- Inbound: Port 40200 (default)
- Outbound: TCP ports within the following range (1024 to 65535). For more details on default dynamic port range for TCP/IP see, https://support.microsoft.com/en-us/kb/929851.)

NOTE: To run the Version Control server on a custom port, see Using a custom port for details.

From the GPOADmin Server:

Configuration storage

- LDAP Service — TCP/UDP TCP/UDP — 389 -or- AD LDS port (defaults to 389 or 50000)

  GPOADmin leverages Microsoft GPMC (see [MS-GPOL]: Group Policy: Core Protocol (Protocol Revision 39.0) and supports secure LDAP for all other calls if specified. Calls made on port 389 use a SASL(sign and seal) bind when connecting to Active Directory (see 5.1.1.1.2 SASL Authentication).

- If you are using SQL Server for GPO backup storage, the appropriate ports must be open. SQL Server's default port is 1433.
- If you are using Named Pipes with SQL, arbitrary ports may be required. SQL Named Pipes is not a recommended configuration through firewalls.

GPO Archives

- If you are using a network share for GPO backup storage, you may require open ports on 135, 138, 139, and 445.
- If you are using SQL Server for GPO backup storage, the appropriate ports must be open. SQL Server's default port is 1433.
- If you are using Named Pipes with SQL, arbitrary ports may be required. SQL Named Pipes is not a recommended configuration through firewalls.
- If you are using AD LDS for GPO backup storage or configuration data, AD LDS defaults to port 389 if not coexisting with AD. If AD is already installed, AD LDS defaults to port 50000.

Using a custom port

If needed, you can set a custom port.

NOTE: Upgrading between versions will overwrite the GPOADmin.Service.exe.config file setting the port number back to the default value of 40200.

To change the port number

1. Replace the current port number with the custom port in the GPOADmin.Service.exe.config file found in the install directory. The default port number is 40200.
2. Replace the current port number with the custom port in the Default.Client.Connection.config file found in the Connections subdirectory of the install directory on all client instance that will connect to the modified service. The default port number is 40200. (See Managing client connections in the Quick Start Guide for details on server specific connections.)
3. Set the registry key HKLM\Software\Quest\GPOADmin\Remoting\Port to the custom port number.
4. GMPC Extension: Add a colon (if not already present) and the custom port number to the end of the server name in the following location:
   HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\GPMCExtension\ServerName
5. Watcher Service: Add a colon (in not already present) and the custom port number to the end of the server name in the following location:
6. HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\WatcherConfig\ServerName
7. If the service account is a GMSA, you will have to manually update the servicePrincipalName on GMSA in Active Directory. For a standard user account, the servicePrinciaplName will be updated automatically when the service starts with the port number from the registry provided the UpdateSPN registry key has not been added with a value of 0. See Configuring GPOADmin to use a Group Managed Service Account (GMSA) in the Quick Start Guide for details.
8. If the ServiceConnectionPoint for the modified service will need to be manually updated to include the desired port number.
9. Restart the GPOADmin service.

Editing the Version Control server properties

Users logged on with an account that is a member of the GPOADmin administrators group can edit the properties of the Version Control server when required. Specifically, they can:

- Add and remove users and administrators to your GPOADmin deployment.
- Select the backup repository for the historical copies of objects.
- Create and define roles used to delegate rights over the Version Control system.
- Configure email notifications on Version Controlled events.
- Delete data from SMTP and workflow notification settings.
- Select the type of information you want to track and the location for the log files.
- Configure various properties such as GPMC version checks, workflow options for GPOs, default link state, protected settings, GPO synchronization, unique names, unique role names, unregistered SOM linking, WMI filter display, custom workflow actions, prevent users from approving their own requests, and enable the identification of associated objects during a deployment and ensure that the service account has the required service account has the required rights to deploy associated items.
- Configure the domain controller that GPOADmin uses for all Active Directory actions and whether to enforce comments to all actions and naming conventions for newly created objects.
- View or update the current license.
- Select product integration options.
- Enable support for Microsoft Intune.
- Enable web proxy to enhance security and privacy.
- Enable FIPS mode.

To edit the Version Control Server configuration

NOTE: You must use the GPOADmin console to edit server configuration, not the GPMC Extension.

1. Right-click the forest, and select **Options**.
2. To add and remove users who can connect to and alter the Version Control server options, select **Access**.

   Select **Administrators** and add and remove users who can connect to and alter the Version Control server-specific settings.

   Select **Users** and add and remove users who can connect to the Version Control server, but can only perform those actions assigned by an administrator.
3. To select the location of the physical backup copy of the various versions of an object, select **Storage**. For complete details, see Configuring the Version Control server.

   You can choose between:

   Network Share: Enter or browse to a network share or directory.

   NOTE: This option is the recommended method as it provides a high level of performance and a low level of configuration and maintenance overhead.

   SQL Server: This option stores the backups in SQL Server. Enter the database name and the required authentication.

   NOTE: If the server is installed as a unique instance, it must be specified as servername\instancename rather than just the SQL Server name.

   You can also migrate from AD LDS to SQL. See Migrating from AD/AD LDS to a SQL configuration store.

AD LDS: This option stores the backups in Active Directory Lightweight Directory Services (AD LDS).

NOTE: To use the same **AD LDS** instance for both the configuration and backup store, select the "Configuration store location" option on the Backup location page.

Directory Configuration Location: This option stores the backups in Active Directory or AD LDS if you selected it during the initial setup of GPOADmin as the storage method for your configuration.

NOTE: Active Directory is not recommended for production deployments due to the amount of replication data.

4 To help optimize performance and secure your data by configuring accepted SQL input filters and timeout settings, select **SQL**.

   a To protect your environment from a SQL Injection attack, choose the **SQL Input Filters** option to specify which SQL statement inputs are not permitted within your deployment. By default, all of the inputs are marked as not permitted.

   If you allow these inputs, malicious code may be inserted in a SQL statement resulting in security vulnerability.

   b Choose the **SQL Timeouts** option to configure how long GPOADmin will wait to connect to the SQL server or to process a command.

   c Adjust the timeout values that best fit your deployment and click OK. The default for the connection timeout is 15 seconds and the default for the command timeout is 30 seconds.

5 Select **Desired State Configuration | Root directory** to specify a DSC root directory for each domain that supports DSC scripts. This root directory serves as the starting point for the DSC script enumeration and deployment location. DSC scripts cannot be registered until this option is enabled.

6 Select **Scripts** to set the file types that will be returned when enumerating Scripts in the live environment. Add and remove the file extensions as required and click **OK**.

7 Select **Delegation** | **Roles** to create and edit roles that are used to delegate rights over the Version Control system. The built-in roles and descriptions are displayed. Add, edit, and delete roles as required. For complete information about creating and delegating roles, see Configuring role-based delegation on page 38.

NOTE: You cannot alter predefined roles.

8 Select **Notifications** to configure email notifications on Version Controlled events. Notifications help you to stay informed of the latest changes to objects under version control and can be enabled for Exchange on-premises, Office 365 Exchange Online, and Gmail.

To use notifications, you must enable SMTP and set the method of authentication. The required method is dependent on the mechanism selected to send notifications.

- When using Exchange on-premises, basic authentication is required.
- When using Office 365 and Exchange Online, OAuth 2.0 authentication is required.
- When using Gmail a credential file is required.

Table 4. SMTP options - Attachments

Option	Procedure
Select **Attachments** to embed report content in the body of the email.	1 Select the report contents to include and click **OK**.

Table 5. SMTP options

Option	Procedure
Select **SMTP** to modify the global SMTP notification options. **NOTE:** • If required, select **Clear** to delete data from SMTP and workflow notification settings. • Users can alter the email address for their notification email through their personal settings, or through the Notification Manager. See Configuring user preferences on page 58 or Selecting events on which to be notified on page 44. • GPOADmin supports TLS/SSL connections. When connecting to Office 365 for standard SMTP notifications, the **From** account must be a valid email address and have access to the mailbox of the authentication account. • To ensure secure communication between GPOADmin and your Exchange server, it is recommended that your Exchange server be configured to support TLS 1.2. • If you select to use Gmail, a folder directory is created in the location of the credential file which contains a tokens.json response folder and a corresponding token response file. This file is no longer required once the activation has been processed and can be safely removed. • If you want to use Microsoft Azure GCC High email for notifications, select the **U.S Government GCC High** option. For information on using Exchange Online for US Government environments refer to Microsoft documentation. • GPOADmin is configured to use TLS 1.2 for communication with web services such as Microsoft Azure. To use a different security protocol, edit the following value in the registry: HKLM\SOFTWARE\Quest\GPOADmin\SecurityProtocol Valid values are: SystemDefault, Ssl3, Tls, Tls11, Tls12 (default), Tls13 (only available on Server 2022 and Windows 11).	1 Select **Basic** to use Exchange for notifications. a Select to **Enabled SMTP notifications**. b Enter the SMTP server. c Enter the port number. 25 for standard, unencrypted communication, 465 for older SSL communication, or 587 for TLS communications. d Enter a “From” address. If your SMTP server is not configured for anonymous connections, enter the associated credentials. e You can optionally select to attach read and/or delivery receipts with notifications. Once enabled, the email specified in the “From” address can confirm that notifications are received and/or read after they are sent. 2 Select **Exchange Online and Office 365** to use Office 365 Exchange Online for notifications. a Select to **Enabled SMTP notifications via Exchange.** b Enter the application ID, tenant ID, tenant name, certificate, certificate password, and https://outlook.office365.com/ews/exchange.asmx as the Exchange Server Url, and a valid certificate and password. The certificate must be previously uploaded to Microsoft Entra App certificates & secrets. The application ID, tenant ID, tenant name, certificate, and certificate password are set when you register GPOADmin to use Office 365 Exchange Online through Microsoft Entra. See Appendix: Registering GPOADmin for Microsoft 365 Exchange Online. 3 Select Gmail to use Google mail for notifications. a Select to **Enabled SMTP notifications via Gmail.** b Enter the Gmail account. c Enter the credential file location. (To use Gmail, users must generate this credentials file from Gmail. GPOADmin uses this file to connect to Gmail, verify the authorization, get access and refresh tokens to retrieve and send messages.) See Appendix: Configuring Gmail for Notifications for information on creating this file. d To navigate past the application verification warning, click **Advanced** and then click the **Go to GPOAdmin (unsafe)** link. e Grant GPOAdmin permissions to **View and modify but not delete your email**. f Click **Allow** to confirm your selection.

Table 6. Workflow notification options

Option	Procedure
Select **Workflow** to enable workflow approval through email, set the authentication method, and modify the mailbox and server information. **NOTE:** • If required, select **Clear** to delete data from SMTP and workflow notification settings. • The Exchange option supports at a minimum Microsoft Exchange 2019 for on-premises mailboxes and Office 365 Exchange Online. • All approvers and the service account must have a valid Exchange on-premises or Office 365 Exchange Online inbox. • Exchange Distribution Groups should be used for approval groups. Active Directory groups are not supported when using the Workflow Approval through email feature. • Proper Exchange certificates must be installed on the GPOADmin server if certificates are being used in your Exchange environment. • You must restart the GPOADmin service when you enable or disable this option. • If you select to use Gmail, a folder directory is created in the location of the credential file which contains a tokens.json response folder and a corresponding token response file. This file is no longer required once the activation has been processed and can be safely removed. • If you want to use Microsoft Azure GCC High email for approvals, select the **U.S Government GCC High** option. For information on using Exchange Online for US Government environments refer to Microsoft documentation. This option is only available for OAuth 2.0 Authentication.	1 Select **Exchange, Exchange Online, & Office 365** to use Exchange, Exchange Online, or Office 365 for notifications. a Select **Enable Workflow Approval through email**. b Set the required authentication. To use Exchange for notifications, select **Basic Authentication** and enter the account to use to connect to the mailbox and password. Enter the Exchange Server Url or select **Autodiscover Exchange Server Url** to locate the Exchange server that is hosting the specified mailbox. To ensure that approvals are processed only by users who have the rights to do so, check the **Enforce approver account validation** option. (This option will not function if you select to follow the Microsoft documentation that restricts access to a single mailbox.) By default, GPOADmin uses the mailbox associated with the service account. If necessary, you can specify a different mailbox for the service to use when processing approvals and rejections through email. To do so, uncheck the **Use the service accounts mailbox** option and enter the mailbox that you want to the service to monitor. To connect as the service, leave the account blank and password blank. To use Office 365 and Exchange Online for notifications, select **OAuth 2.0 Authentication**. Enter the mailbox. application Id, tenant Id, https://outlook.office365.com/ews/exchange.asmx as the Exchange Server Url. and a valid certificate and password. The certificate must be previously uploaded to Microsoft Entra App certificates & secrets. The application ID and tenant ID are set when you register GPOADmin to use Office 365 Exchange Online through Microsoft Entra. See Appendix: Registering GPOADmin for Microsoft 365 Exchange Online.)

Table 6. Workflow notification options

Option	Procedure
	2 Select Gmail to use Google mail for notifications. a Select to **Enabled SMTP notifications via Gmail.** b Enter the Gmail account. c Enter the credential file location. (To use Gmail, users must generate this credentials file from Gmail. GPOADmin uses this file to connect to Gmail, verify the authorization, get access and refresh tokens to retrieve and send messages.) See Appendix: Configuring Gmail for Notifications for information on creating this file. d To navigate past the application verification warning, click **Advanced** and then click the **Go to GPOAdmin (unsafe)** link. e Grant GPOAdmin permissions to **View and modify but not delete your email**. f Click **Allow** to confirm your selection.

2 Select **Logging | Configuration** to enter the log location and the type of information you want to track.

From here you can:

Choose to log to the Event Log, to a specific directory where log files will be created, or not at all.

Select which (if any) types of events to log. The types of events are as follows: Service Actions (such as service startup and shutdown), User Actions (such as check in, approve, edit), Errors, and Debug Information (used by Quest Support).

Enable Group Policy Management console logging and set the logging level to Normal or Verbose. The logs (GPmgmtManaged.log and the GPmgmt.log) are located in the service account's %temp% directory.

Enable Exchange logging for workflow approval through email. Restart the GPOAdmin service for this to take effect. The EWS.txt file can be found in the application install directory.

3 Select **Options** to configure various settings.

Select **General** to configure the following options:

Table 7. General options

Option	Description
Perform Group Policy Management version check	Check to ensure the version of GPMC on the client is compatible with the GPMC version used within GPOADmin.
Disable all workflow options for Group Policy Objects	Disable all workflow on GPOs. Keep in mind, if you disable the workflow, any changes made are immediately deployed in the live environment. To bring the GPO back under version control, enable the workflow.
Disable all workflow options for Scopes of Management	Disable all workflow on SOMs. Keep in mind, if you disable the workflow, any changes made are immediately deployed in the live environment. To bring the SOM back under version control, enable the workflow.
Disable all workflow options for WMI Filters	Disable all workflow on WMI filters. Keep in mind, if you disable the workflow, any changes made are immediately deployed in the live environment. To bring the WMI filter back under version control, enable the workflow.
Set default link state to enable when adding new links	This enables the default link state for any new links added to a SOM.

Table 7. General options

Option	Description
Enable Protected Settings for Group Policy Objects	This enables the ability to have Protected Settings policies that contain settings that you want to control. They are protected in the sense that they contain and identify the settings that cannot be altered by users. This provides an added level of security for the policies within your organization. If a user attempts to create, edit, or remove the flagged settings they are stopped. **NOTE:** If you have GPOADmin configured with SQL as the configuration store, you can select to **Enable Policy Baselines**. Selecting this option allows Protected Setting policies to be assigned to individual GPOs as policy baselines. See Working with Protected Settings Policy Baselines for details.
Enable Group Policy Object Synchronization	Synchronizing GPOs allows you to automatically push out predefined “primary GPO” settings to specified targets both within a forest and between two forests. This allows you to ensure specific GPOs, which are required in every domain, contain the same settings without having to link to a GPO outside of the domain. You are able to select one or more GPOs from various domains as synchronization targets for the source GPO. When the source GPO has been successfully deployed, the settings from the last major backup are imported into each synchronization target GPO.
Enable automatic synchronization of Group Policy Objects during deployment	Provides the ability to control whether the service account can perform a GPO synchronization during deployment. • If disabled, a GPO synchronization will only happen during deployment if the deploying account has the Synchronization right on the GPO. • If enabled, the service account will perform a GPO synchronization during deployment. (Default)
Enable Unique Name	This ensures that GPOs and WMI filters cannot be created with the same name as an existing GPOs or WMI filter in a domain, select the **Enforce Unique Names** option. If a non-deployed GPO indicates that a duplicate name exists, run a full compliance check to determine if any GPOs were modified outside of GPOADmin. For more info see, Checking compliance on page 93. **NOTE:** In order to reuse a unique name, you must select to delete the GPO and WMI filters and the associated backups.
Enable Unique Role Names	This ensures that roles cannot be created with the same name as an existing role.
Enable unregistered Scopes of Management linking	To allows users to link to unregistered Scopes of Management, select the **Enable unregistered Scope of Management linking** option. If this option is not selected, the policy and the SOM must be registered and the user linking the policy must have the Link right on both objects.
Display only the WMI Filters a user has Read access to when editing a GPO	Users are restricted to only the WMI Filters they have Read access.
Ensure service account access prior to deployment	This option must be enabled if you want users to be able to automatically deploy an object’s associated items. See Deploying objects (scheduling and associated items) on page 91. It ensures that the service account has the Edit settings, delete, modify security rights on the working copy before deployment.
Enable the identification of associated items during deployment	Provides users with the option to identify and deploy associated items in a pending deployment state.

Table 7. General options

Option	Description
Prevent approval requester from approving their own changes	Ensures that a user cannot approve their own changes, even if they are in the approver's list for the object.
Enable empty policy deploy warning	Enable a warning message when users are trying to deploy a GPO that does not include any policy settings.
Refresh objects on selection	When this option is enabled, the objects are refreshed when they are selected in the client.
Log service option changes	Enabling this option will log any changes made to the version control server configuration options. **IMPORTANT:** By default, this option is disabled as it may pose a security risk. If this option is enabled, Quest highly recommends that you review the security for the GPOADmin event log and the log file and ensure the access is altered as required.
Enable the processing of custom workflow actions	Clicking the Launch Editor button starts the Custom Workflow Editor.
OU display format	Set the display format for OUs.

Select **SQL Input Filters** to view the allowed strings and characters for SQL statements.

NOTE: To protect your environment from a SQL Injection attack, you can mark which SQL statement inputs are not permitted. If you allow these inputs, malicious code may be inserted in a SQL statement resulting in security vulnerabilities.

Select **Comments** to enforce comments to all actions and naming conventions for newly created objects. Set a minimum comment length greater than 0. Leaving the value at 0 means comments are optional for all actions. Any value greater than zero makes comments mandatory for all actions and all users.

Select **Deployment Failure** to enable an automatic retry on failed deployments. Enable the option and select the number of attempts (maximum of 10) and the interval in minutes (maximum of 1440). Re-deployment attempts are done as scheduled deployments.

Select **Preferred Domain Controllers** and click **Add** to configure the domain controller that GPOADmin will use for all Active Directory actions. By default, GPOADmin uses the Primary Domain Controller. Optionally, select **Use Secure LDAP** to protect your directory data and credentials during communication with Active Directory.

4 Select **Retention | Backups Retention** to configure a retention schedule for backups. You can select to limit the backups to keep based on a specified number, age, or date. Backup retention settings apply to SQL configuration stores only.

NOTE: All backups generated by the watcher service due to non-compliance are counted in the retention limit.

5 Select **Retention | Deleted Object Retention** to configure retention settings for deleted objects. You can choose to specify the retention to be based on a specific number of days to keep deleted objects or a date after which the object will no longer be retained. Deleted Object Retention settings apply to SQL configuration stores only.

6 Select **License | Current License** to view the current license information.

Select the **Update License** check box and then click **Browse** and go to the new license location.

7 Select **Intune | Configuration** to enable support for Intune and enter the information to connect to the required Microsoft Entra tenant. This includes the application ID, tenant ID, tenant name, certificate, and certificate password for the tenant where Intune is installed. See the GPOADmin Quick Start Guide for minimum permission requirements.

NOTE: GPOADmin is unable to support Intune Setting Catalog items that contain encrypted values.

If you want to use a Microsoft Azure GCC High Intune tenant, select the **U.S Government GCC High** option.

8 Select **Integration** to configure settings that apply to a Quest Change Auditor™ integration.

If you have multiple Change Auditor coordinators installed, you can select a specific coordinator to use for reports and auditing.

If necessary, you can also select to turn off Change Auditor, by selecting **Not Set**.

9 For increased security and privacy, select **Web Proxy** to configure GPOADmin to use a web proxy server for internet communication.

> **NOTE:** Web Proxy is not supported when using Gmail for notifications.

Select to **Enable Proxy**.

Enter proxy server address and the username and password for authentication.

Optionally, select **Bypass local addresses** if you want to exclude local network traffic from being routed through the proxy. Add and remove local addresses as required.

Click **OK** to save the proxy settings.

10 Select **Enable FIPS Mode.** The Federal Information Processing Standards (FIPS) are government set guidelines and standards published by the National Institute of Standards and Technology. To run a Windows environment in FIPS compliant mode, the Microsoft Policy “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” must be enabled.

Select **Enable FIPS mode** to ensures that GPOADmin uses cryptographic algorithms that are FIPS compliant.

Select **Allow self-signed certificates when communicating with Exchange servers** if required.

Both these options are enabled by default.

11 When you have made all the required selections, click **OK**.

Editing the Version Control server configuration store

Users logged on with an account that is a member of the GPOADmin administrators group can edit the type of configuration store.

To edit the configuration store

1 Right-click the forest, and select **Re-configure Version Control server.**

2 In the Select a Configuration Store dialog, select SQL Server, AD LDS, or Active Directory for your configuration storage location.

> **NOTE: Configuration Store Selection**
> The best practice is to use:
>
> - SQL Server for optimal performance.
> - AD LDS for small environments. Quest uses the following criteria to define small environments. (These are guidelines and should not be considered as an exhaustive list.)
>   - Domains with less than 500 registered objects that run searches on a regular basis.
>   - Less than 500 registered containers.
>   - Containers with objects nested no more than 3 levels deep.
> - Active Directory for legacy deployments. It is not recommended for new installations.

IMPORTANT: Ensure that you are following the minimum permissions detailed in the Quick Start guide. The listed permissions help to secure the database by limiting the access to only the required accounts.

a If you select Active Directory, select the Domain Controller (DC) to be the Version Control server, and click **Next**.

Any DC in any domain of the selected forest can be specified as the primary version control server. This server can be thought of as another FSMO role in the Microsoft sense (such as Schema master, PDC Emulator, and RID master).

GPOADmin is a directory-enabled application and all its application information is stored in the configuration container of Active Directory. Because of how the information is stored, all information is automatically replicated to all other DCs. However, the primary version control server is the authoritative source for all version control actions. If it goes offline, users cannot perform actions such as check-in a desired group policy object change until the problem has been rectified.

b If you select AD LDS, enter the NetBIOS name of the computer you are installing to and the port number in the format: `server_name:port`, and click **Next**.

For example, gpoadmin_svr: 389.

NOTE: The username/port/server (but not password) will be cached, so the next time you open the console you will not need to enter this information.

c If you select SQL Server, choose the required SQL server, enter a name for the database, select the authentication method to access the server, and click **Next**.

NOTE:

- See the Release Notes for supported SQL Server versions.
- To protect your environment from a SQL Injection attack, you can mark which SQL statement inputs are not permitted. See Editing the Version Control server properties. By default, all of the inputs are marked as not permitted. If you allow these inputs, malicious code may be inserted in a SQL statement resulting in security vulnerabilities.
- When configuring GPOADmin to use an Azure SQL managed instance, you must specify the public endpoint including the port number, in the Server Name field in GPOADmin. For details on configuring a public endpoint, see Microsoft documentation.

To connect as the current user, select NT Authentication.

Select the level of encryption for the connection. When enabled, SQL Server uses TLS encryption for data sent between the client and server.

Choose between:

- **Strict (SQL Server 2022, 2025, and Azure SQL)**: Select this option for Azure SQL Database and Azure SQL Managed Instance or when the instance has **Force Strict Encryption** enabled.
- **Mandatory**: Select this option when the instance has **Force Encryption** enabled. It can also be used when no encryption is configured for the instance, but **Trust server certificate** is enabled. While this method is less secure than installing a trusted certificate, it does support an encrypted connection.
- **Optional** (Default in GPOADmin)

Enabling **Trust Server Certificate**, when 'Optional' or 'Mandatory' encryption is selected, or if the server enforces encryption, means that SQL Server will not validate the server certificate on the client computer when encryption is enabled for network communication between the client and server.

Under **Host name in the certificate**, you can provide an alternate, yet expected, Common Name (CN) or Subject Alternative Name (SAN) in the server certificate for the connection to SSMS. You would use this option when the server name does not match the CN or SAN, for example, when using DNS aliases.

Leaving this option blank allows certificate validation to confirm that the CN or SAN matches the server name.

To connect using SQL credentials, select SQL Authentication and enter the user name and password.

3 Click **Next** to continue.

4 Click through the rest of the Service Configuration Wizard and click **Finish**.

Replacing the Version Control server configuration settings

In some cases, you may want to keep the majority of the Version Control server settings the same throughout the deployment and have only select settings unique for each server.

If this is the case, you can copy the settings from an existing sever and then update where required rather than having to enter all the settings required during a reconfiguration.

To edit the Version Control configuration using another servers settings

1 Right-click the forest, and select **Copy Server Configuration**.

2 Select the server configuration that you want to copy and click **OK**.

3 Right-click the forest, and select **Options** to update where required.

Migrating from AD/AD LDS to a SQL configuration store

A configuration utility (GPOADmin.ConfigMig.exe) is available in the GPOADmin install directory that allows you to migrate the configuration store to SQL from an AD/AD LDS. You can migrate all objects or specify users, custom folders, keywords, email templates, roles, domains, containers, version control items, scheduled deployments, synchronization targets and synchronization results data as required.

NOTE:

- The Migration utility migrates configuration store data; it does not migrate backups. To ensure the migration completes without issue, we recommend that you continue to use the same backup store.
- To ensure the configuration utility is running against the latest version of GPOADmin, login and configure for the existing AD/AD LDS configuration store prior to migrating to SQL. This also ensures that AD/AD LDS configuration store is up-to-date and reduces possible migration issues.

The output from the configuration utility is written to the screen as well as to a Migration.txt file located in the install directory.

IMPORTANT: The configuration utility must be:

- Run on the GPOADmin server host computer.
- Run as an account that has access to the AD/AD LDS configuration store and the new SQL database. In most cases this will be the service account.
- Pointed to a GPOADmin 5.16 or above configuration storage location. (Upgrade from versions older than 5.16 are not supported.)
- After the migration, you need to restart the Watcher Service so that it will use the correct configuration store.

Before running the configuration utility, you need to configure the version control server to use SQL as the configuration store. See Editing the Version Control server configuration store to change the storage from AD/AD LDS to SQL.

SQL Injection inserts malicious code into SQL statements which can lead to security vulnerabilities. To protect your environment from a SQL Injection attack, you can mark SQL statement inputs that are not permitted. See Editing the Version Control server properties. By default, we have marked the following inputs as not permitted. If you allow these inputs, malicious code may be inserted in a SQL statement resulting in security vulnerabilities:

Table 8. SQL inputs

Input	Description
:	Denotes the end of a SQL query. Allowing this character can permit malicious queries to be included in user input.
--	All trailing input is interpreted as a comment until the new line character.
/*	The character combination used to denote the start of a block comment. All trailing input is interpreted as a comment until the comment end delimiter.
*/	The character combination used to denote the end of a block comment. Input between the comment start delimiter and the comment end delimiter is interpreted as a comment.
xp_	Extended procedures are routines residing in DLLs that function similarly to regular stored procedures. The extended stored procedure function is run under the security context of Microsoft SQL Server.
\AUX	Generally, the AUX port on a PC is computer port 1 (COM1), which is the first serial port with a preconfigured assignment for serial devices. File paths can be constructed using this input.
\CLOCK$	The system clock. File paths can be constructed using this input.
\COM1	The first Communications port. File paths can be constructed using this input.
\COM2	The second Communications port. File paths can be constructed using this input.
\COM3	The third Communications port. File paths can be constructed using this input.
\COM4	The forth Communications port. File paths can be constructed using this input.
\COM5	The fifth Communications port. File paths can be constructed using this input.
\COM6	The sixth Communications port. File paths can be constructed using this input.
\COM7	The seventh Communications port. File paths can be constructed using this input.
\COM8	The eighth Communications port. File paths can be constructed using this input.
\CON	A common device name for the keyboard and screen. File paths can be constructed using this input.
\CONFIG$	A configuration information file. File paths can be constructed using this input.
\LPT1	The first line print terminal. File paths can be constructed using this input.
\LPT2	The second line print terminal. File paths can be constructed using this input.
\LPT3	The third line print terminal. File paths can be constructed using this input.
\LPT4	The fourth line print terminal. File paths can be constructed using this input.
\LPT5	The fifth line print terminal. File paths can be constructed using this input.
\LPT6	The sixth line print terminal. File paths can be constructed using this input.
\LPT7	The seventh line print terminal. File paths can be constructed using this input.
\LPT8	The eighth line print terminal. File paths can be constructed using this input.
\NUL	The NUL port. File paths can be constructed using this input.
\PRN	The DOS name for the first connected parallel port. File paths can be constructed using this input.

Before migrating the configuration store, Quest suggests that you test the migration to ensure that all objects migrate according to your specifications. To validate the migration, run the command with the /t option. This gathers all the information that will be committed to the SQL database but does not commit any changes.

To run the configuration utility:

- From a command prompt, browse to and run Program Files\Quest\GPOAdmin\GPOADmin.ConfigMig.exe "FQDN of the AD/AD LDS server hosting the source configuration store."

  The following switches and options are available: (If none are specified, all objects are migrated.)

  - O = Service Options
  - U = Users
  - F = Custom Search Folders
  - K = Keywords
  - E = Email Templates
  - R = Roles
  - D = Domains
  - C = Version Control Containers
  - I = Version Control Items
  - S = Scheduled Deployments
  - T = Synchronization Targets
  - Y = Synchronization Results
  - /T = Testing only. Validates the object data from the source configuration store. Nothing is written to the database.
  - /H:<GPOADmin Host>] = The FQDN of the source GPOADmin host (Used to migrate Service Options stored in the registry)
  - /S:<domain\account> = The GPOADmin service account name. If not specified, the current user account is used.
  - /R = Re-migrate items. Items are logged to their own log file in a timestamped directory based on when the migration was started. It is located in the Configuration Migration folder of the installation directory. The file name is a combination of the item name and its Version Control Id.
  - /G = Grant the specified service account access.

Changing the Service Account

To change the GPOADmin service account in an existing deployment, consider the following:

- Existing live GPOs

  Must have their ownership and delegation updated with the new service account. You can update the service account by running the GPOADmin.AddServiceAccountToAllGPOs PowerShell script found in the Scripts folder of the GPOADmin install directory.

- Existing registered GPO backups

  The Watcher service may detect and report GPOs as non-compliant because they contain the previous service account as the owner and as a delegate with the edit settings, delete, and modify security Group Policy Management Console permissions. To prevent this, stop the Watcher service monitoring the forest before changing the service account. Note: Running a manual compliance check by right-clicking the object and selecting to Check Compliance will also report GPOs as non-compliant.

To bring GPOs back into compliance complete the one of the following:

- GPOs with a major version less than 1.0 should be copied and deployed. This corrects the security and ownership to reflect the new service account. Once the copied GPO has been successfully deployed, delete the original.
- GPOs with any version greater than 1.0, when deployed, display a message indicating the policy is not compliant. This is expected behavior since the owner and delegation for the GPO have changed. The deployment can proceed; however, the security on the policy template in SYSVOL may become "out of sync". To address this, locate the policy in question in GPMC and select the service account from the Delegation tab. Right-click and select Edit settings and OK. Right-click again and select Edit settings, delete, modify security and OK.

  To ensure that service account has proper access to any registered policies, we recommend that you enable the "Ensure service account access prior to deployment" option within GPOADmin.

Root container assignment

If necessary, the GPOADmin administrator can assign a specific container as a user's or group's "Root Container". When the user or group member logs in they will only have access to the container they have been assigned, rather than the default "Version Control Root". This allows for the administration of containers and sub containers to be assigned to specific users or groups without those users being able to access or change managed objects in any other containers.

This assignment is also valid for the PowerShell commands and the GPOADmin snap-in for GPMC.

NOTE: A user or group can only be directly assigned one root container at a time, however, they may have access to multiple root containers through their group membership.

To assign a container to a user or group

1. Right-click the container to be the root, and select **Properties**.
2. Select the **Root Container Assignment** tab and assign the users or groups who are going to see this as their Root Container.

IMPORTANT: The security for the container must be set so the users or group members have the User, Moderator, Administrator, or some specially created role. If the security is not set for the assigned users of the Root Container, they will not be able to see, create, or manage any objects in the container and sub containers.

Restricting GPO management for specific domains

If necessary, you can restrict access to domains to ensure that only specified individuals or groups can view, register, create, and report on items in a domain. You can fine-tune the level of available management based on the level of security.

By default, the Domain Users group is assigned all domain rights to their corresponding domain. To take advantage of the new level of security, you must remove Domain Users and assign rights as appropriate.

IMPORTANT: These rights refer to domain access and work with the existing GPOADmin delegated user rights that are in place; they do not replace them.

To manage the security on a domain

1. Expand the **Live Environment**, right-click the required domain, and select **Properties**.
2. Add and remove the user or groups that you want to apply the restrictions to.
3. Select to allow (or remove previously applied) rights and click **Apply**.

Table 9. Available rights

Right	Description
Read	A base right that you must apply as it is used with other rights. This right works with, but does not replace, the delegated custom user Read right that controls whether users and groups can see a version control container's contents.
Register	Apply this right to users and groups that are assigned the Domain Read right to allow them to register/unregister objects from the selected domain. This right works with, but does not replace, the delegated custom user Register and Unregister rights that controls whether a user can register objects into a specific version control container or unregister objects.
Create Group Policy Objects	Apply this right to users and groups that are assigned the Domain Read right to allow them to create Group Policy Objects in the selected domain. This right works with, but does not replace, the delegated custom user Create right that controls whether a user can create an object in a specific version control container. The Edit right on the Version Control container is also required.
Create WMI Filters	Apply this right to users and groups that are assigned the Domain Read right to enable them to create WMI Filters in the selected domain. This right works with, but does not replace, the delegated custom user Create right that controls whether a user can create an object in a specific version control container. The Edit right on the Version Control container is also required.
Create Scripts (Logon/Logoff Startup/Shutdown)	Apply this right to users and groups that are assigned the Domain Read right to enable them to create a script in the selected domain. This right works with, but does not replace, the delegated custom user Create right that controls whether a user can create an object in a specific version control container. The Edit right on the Version Control container is also required.
Create Desired State Configuration Scripts	Apply this right to users and groups that are assigned the Domain Read right to enable them to create Desired State Configuration scripts in the selected domain. This right works with, but does not replace, the delegated custom user Create right that controls whether a user can create an object in a specific version control container. The Edit right on the Version Control container is also required.
Report	Apply this right to users and groups that are assigned the Domain Read right to enable them to report on objects within the selected domain. Once applied, they will only see the "Live" report option for objects which exist in the associated domain and only the domains for which the user has this right is displayed in the report wizard. This right works with, but does not replace, the delegated custom user Run Reports right that controls whether a user can run the "New Report" wizard, and the Run Contextual Reports right which controls whether a user can run the "Live", "Working Copy", "Latest", and "Difference" from the context menu.
Create Starter GPO	Apply this right to users and groups that are assigned the Domain Read right to allow them to create Starter GPOsin the selected domain. This right works with, but does not replace, the delegated custom user Create right that controls whether a user can create an object in a specific version control container. The Edit right on the Version Control container is also required.

Configuring role-based delegation

NOTE:

- The predefined roles cannot be altered.
- You must perform all role-related tasks in the GPOADmin console.
- When using the Link right, you must have Link right on the GPO and the SOM.

GPOADmin Administrators can create custom roles that can be applied to specific users to allow them to perform certain functions within the Version Control system. For more information about users with permissions to create roles see Configuring the Version Control server on page 18.

When building custom roles, keep in mind the rights must also have the dependent permissions assigned.

Table 10. Right dependencies

Right	Dependencies
Assign Keywords	Read
Attest	Read
Block Inheritance for SOM links	Read and Edit
Block Notification Inheritance	Read
Cloak / Uncloak	Read
Compliance Action	Read
Create	Read and Edit
Delegate Security	Read
Delete	Read
Delete links outside of workflow	Read, Edit, Link and Deploy (User must be the sole approver on linked Scopes of Management)
Deploy	Read
Edit	Read
Edit Linage	Read
Enable/Disable Approvals	Read
Enable / Disable Workflow	Read
Export	Read
Label	Read
List Folders	None
Link	Read and Edit (For managed Scopes of Management)
Lock / Unlock	Read
Modify Approval Workflow	Read
Modify Keywords	Read
Modify Change Window	Read
Modify Link Properties	Read and Edit (For managed Scopes of Management)
Modify Managed By	Read
Modify System-Provided Security Right	Read, Edit and Modify Security Filter
Modify Security Filter	Read and Edit
Move	Read
Read	None
Register	Read

Table 10. Right dependencies

Right	Dependencies
Reject Change	Read
Request Approval	Read
Run Contextual Reports	Read
Run Reports	Read
Set Notifications	Read
Set Remediation Rules	Read
Synchronize	Read
Undo Check-out	Read
Unregister	Read
Unregister and Remove History	Read
View Cloaked	Read
Create Subcontainers	Read
Delegate Container Security	Read
Delete Container	Read
Rename Container	Read
Block Protected Settings Inheritance	Read and Modify Protected Settings Assignments
Export Group Policy Objects as Protected Settings Policies	Read and Register (On the target Protected Settings Container)
Modify Protected Settings	Read
Modify Protected Settings Assignments	Read
Modify Protected Settings Exclusions	Read
Modify Protected Settings Baseline Assignments	Read
Modify Intune Assignments	Read

See also:

- Creating roles
- Editing roles
- Delegating roles

Table 11. Roles and rights

Role	Rights included in the role
System Administrator	System Administrators can perform any action in the Version Control system. Version Controlled Object Rights include: • Block Inheritance for SoM links • Block Notification Inheritance • Cloak/Uncloak • Compliance Action • Create • Delegate Security • Delete • Delete links outside of workflow • Deploy • Edit • Edit Lineage • Enable/Disable Workflow • Export • Label • Link • Lock/Unlock • Modify Approval Workflow • Modify Change Window • Modify Keywords • Modify Managed By • Modify System-Provided Security • Modify Security Filter • Move • Read • Register • Run Contextual Reports • Run Reports • Set Remediation Rules • Set Notifications • Synchronize • Undo Check-out • Unregister • Unregister and Remove History • View Cloaked

Role	Rights included in the role
System Administrator (continued)	Version Control Container Rights include: • Create Subcontainers • Delegate Container Security • Delete Container • Rename Container Protected Settings Rights include: • Block Protected Settings Inheritance • Export Group Policy Objects as Protected Settings Policies • Modify Protected Settings • Modify Protected Settings Assignments • Modify Protected Settings Baseline Assignments • Modify Protected Settings Exclusions
Moderator	Moderator (Moderators can perform every action a user can, plus undoing check outs from other users and running the compliance wizard.) They can also: • Create • Delete • Edit • Export • Label • Read • Run Contextual Reports • Run Reports • Undo Check Out
User	User (Users can perform all the basic actions of the Version Control system, such as check in, check out, edit.) They can also: • Create • Delete • Edit • Export • Label • Read • Run Contextual Reports • Run Reports • Set Notifications

Creating roles

You can easily create roles with any of the customized rights.

To create a role

NOTE: You must use the GPOADmin console to create roles, not the GPMC Extension.

1 Right-click the forest, and select **Options**.

2 Select **Delegation | Roles**.

3 Click **Add New Role**.

4 Enter a name and description for the role, and click **Next**.

You can create a role that is based on an existing role. (To see which rights are assigned to a particular role, hover the cursor over it.)

5 Select the role or roles you want to copy and click **Next**.

If you want to create the role from scratch, do not select an existing role before clicking **Next**.

6 Select the rights that you want included in the role, and click **Finish**.

Editing roles

To edit roles

NOTE: You must use the GPOADmin console to edit roles, not the GPMC Extension.

1 Right-click the forest node, and select **Options**.

2 Select **Delegation | Roles**.

3 Select the role that you want to edit and click **Edit Role**.

4 Make the required changes and click **OK**.

5 Click **OK** again to apply the changes.

Delegating roles

Once the required roles are in place, GPOADmin Administrators can begin to delegate the security over containers and GPOs to specific users and groups.

To delegate rights on the Version Control system through roles

NOTE: You must use the GPOADmin console to delegate roles, not the GPMC Extension.

1 Right-click the Version Control Root node, required container or object, and select **Properties**.

2 Select the **Security** tab.

3 Click **Add** to select the users and groups to which you want to apply the role.

4 Select the role to apply and click **OK**.

The specified users will now have the specified rights included in the assigned role over the selected container or object.

Restricting access to objects

By default, access to containers and objects is based on the security directly assigned to it and the security from its parent container.

If necessary, you can block inheritance to restrict access to the container or object.

NOTE: Inheritance cannot be blocked on root containers (Version Control Root, Lost & Found, and Protected Settings Root).

To block inheritance:

1. Right-click the required container and select **Properties**.
2. Select the **Security** tab and click to enable the **Block Inheritance** option.
3. Click **OK**.

   Once enabled, the security on the container or object is based on the access directly assigned to it. Any child container or objects inheritance stops at the first container where inheritance is blocked.

Adding notifications for users

An administrator can add notifications for multiple users. Such users may never log in to GPOADmin, but for business reasons, may need to be notified when an object is created, modified, or deleted.

Administrators can also copy notification settings from one user to other users or merge new notification settings with existing ones.

NOTE: Only users with the Set Notification right can manage GPOADmin notifications.

To add notifications

1. Right-click the **Forest** node and select **Notification Manager**.
2. Select the container you want to set notifications on.
3. Under the Notifications menu, select **Add Subscribers**.
4. If there are no users listed, you can add either an Administrator or a User by selecting **Add Administrator** or **Add User**.
5. Select the check box next to the user and click **OK**.
6. You can have the application attempt to discover the user's email address by clicking the **Autodiscover email address** button.

   If the application fails to discover the user's email, or you want to redirect it, type the email address in the Email box and click **Set**.
7. Click **OK**.
8. In the Notification Manager window, select the user and then under the Notifications menu, select **Set Notifications**.

NOTE: A newly added user will not be retained until you assign notifications for that user.

9. Select the actions for which you want to have the user notified and click **OK**.

To paste and merge notification settings

1. In the Notification Manager window, right-click the name of the user from which you want to copy notifications and select **Copy Notifications**.
2. Select the target user or group of users and do one of the following:

   To paste notifications, select **Paste Notifications**.

   Pasting overwrites the target user's existing notifications.

   To merge the copied notifications with the target user's existing notifications, select **Merge Notifications**.

Selecting events on which to be notified

Using the notification option you can set up to receive an email each time a specified action is performed within the Version Control system.

NOTE: Only users with the Set Notification right can manage GPOADmin notifications.

To set up notification

1. Navigate to the version-controlled object for which you want to be notified.
2. Right-click the object and select **Options**.
3. Select **Notifications**.
4. Select the events that you want to be notified about, and click **OK**.

   A notification email will now be sent when the specified events take place on (and beneath, in the case of a container) the selected object.

NOTE: To set up the email address for the notification messages, see Configuring user preferences on page 58 or Adding notifications for users on page 43.

Restricting inheritance on notifications

If required, you can select to restrict the inheritance on notification settings from the Version Control root to child containers and objects.

NOTE: Only users with the Block Notification Inheritance right can restrict notifications.

To block the notification settings on child containers and objects:

1. Right-click the Version Control Root node, required container or object, and select **Properties**.
2. Select the **Notifications** tab.
3. Click to enable the **Block inheritance** option.
4. Select the actions for the selected container or object that you want to be notified on.
5. Click **OK**.

   The notification settings will now follow the selected configuration rather than be inherited from the parent container,

Creating email templates

You can create a custom email template for notifications or email requests (if this option is enabled, see Configuring the Version Control server) and associate it with specific roles. This allows you to standardize the information that is presented to users based on their role within your organization.

You can choose to include attachments and custom subject lines for specified version control actions. For example, you can easily include forms used to track change requests in an external system, risk assessment checklist, or logs in the email.

NOTE:

- Administration accounts must be explicitly added to the GPOADmin Administrators group in order for the email template assigned to the System Administrator Role to be used when sending notification to an administrator. You can set this option through the Access tab in the Version Control Options.
- If notifications are not delivered, check the attachment filters on your mail server.

NOTE: If required, you can modify the information generated by the Watcher Service by creating a new role specifically for it and then customizing an existing template or creating a new template to associate with it.

For example, to ensure that the Watcher Service or server name does not display in the notification message, remove the following section from the template html file:

```
<tr>
      <td class="style3">
            Detected on:
      </td>
      <td>
            [MACHINENAME]
      </td>
</tr>
```

The keyword MACHINENAME specifies the computer where Watcher Service is running.

GPOADmin includes a sample template (DefaultNotificationTemplate.html) in the server installation directory. This file should not be moved or modified; however, you can use it as a basis for the creation of new templates.

To select an email template for an existing role

1. Right-click the forest node, and select **Options**.
2. Select **Delegation | Roles**, select the require role, and click **View Role**.
3. Select the **Email Template** tab.
4. Click **Browse** to select the template to use for the selected role.

   By default, the DefaultNotificationTemplate.html in the server install directory is used by the notification system if the specified custom template cannot be found.

   If there are no templates displayed, click **Add** and browse to where the templates are located. The default template is located at C:\Program Files\Quest\GPOADmin.
5. Select the template and click **OK**.
6. Select the cost for this template.

   If a user is a member of two or more roles which have subscribed to the same notification, the email template associated with the role with the lowest cost is the one used for that user.

   For example, User A has subscribed to all event on Version Control Root. They are a member of the Moderators role set on the Version Control Root container and a member of the Administrators Role set on a child container When a version-controlled object is Checked-Out in the child container a notification is sent to them. GPOADmin determines that user A is a member of two roles. The cost that you have applied to the role tells the system which template to use when sending the notification. If the Moderators role has a lowest cost then the cost associated with the Administrators role, then the template associated with the Moderators role is used.

7 To select an attachment to include in the email, select the **Attachments** tab, click **Add,** select the action that triggers the attachment inclusion from the list, select the attachment to include by entering its location or browsing to it, and apply the changes.

NOTE: You can optionally use any GPOADmin predefined tag in this field.

To further control the inclusion of attachments, you can use keywords. The attachment is only included if the specified keywords are present in the list of keywords on the version-controlled object.

Enter, enable, disable keywords as required. (Check an existing keyword to have it associated with this attachment and click to clear the keyword to exclude it.)

NOTE: Any attachment with an empty keyword list would always be included for the associated action.

8 To include a subject in the email, select the **Subject Lines** tab, click **Add**, select the required action, enter the text that you want included in the **Subject Line** field, and apply the changes.

To further customize the subject line, you can use tags and keywords.

Tags allow you to include a very specific subject line. For example, if you select Type, Name, and Trustee Name from the drop down list (The “[TYPE] '[NAME]' has been checked in by [TRUSTEENAME]”), the resulting email for a GPO named Sales would be "The GPO 'Sales" has been checked in by domain\user".

Keywords allow you to include a set subject line when the specified keywords are present in the list of keywords on the version-controlled object.

9 Click **OK**.

10 Click **Apply** to associate the template.

Working with Protected Settings policies

Protected Settings policies contain settings that you want to control. They are protected in the sense that they contain and identify the settings that may not be altered by users. This provides an added level of security for the policies within your organization. If a user attempts to create, edit, or remove the flagged settings they are stopped.

Protected Settings are identified by examining the difference report between the Protected Settings policies and the Group Policy Object being checked in. The difference is produced by using the Difference Engine in GPOADmin. Once this is completed, the protected setting function searches the difference report for matches based on the specified validation mode.

Protected Settings policies have a modified workflow and follow the typical check-out, edit, and check-in process. As with any other object, when you are ready to make the newly created Protected Settings policy active or edit an existing policy, a request approval action must be initiated.

Once the approval is granted, the Protected Settings policy is available for use.

NOTE: These policies differ from other GPOs in that they are not deployed to the environment.

If a protection issue is detected during check in, users with the Modify Protected Settings right on the GPO in question, have the option to continue with the check in and override the blocked setting or review a report and address the issue.

Protected settings must be:

- Enabled within the domain
- Created with the selected settings
- Applied to the required container within GPOADmin

To enable Protected Settings for Group Policy Objects

1. Right-click the domain and select **Options**.
2. Select **Options | General** and select **Enable Protected Settings for Group Policy Objects**.
3. Click **OK**.

   A new Protected Settings Root container is created to store and manage the Protected Settings policies deployed within your environment.

See also:

- Rights and role for Protected Settings for GPOs
- Create a Protected Settings policy
- Generating Protected Settings policies reports
- Using Protected Settings policies
- Checking a GPO against a Protected Settings policies and blocked extensions
- Validating a GPO against a Protected Settings policies and blocked extensions before a check-in

Rights and role for Protected Settings for GPOs

The Protected Settings for GPOs requires the following rights to control the actions of the Protected Settings tab on containers and provide the ability to export GPOs to create protected settings:

- Block Protected Settings Inheritance
- Export Group Policy Objects as Protected Settings Policies
- Modify Protected Settings Assignments
- Modify Protected Settings Exclusions

NOTE: These rights are not available until the Protected Settings for Group Policy Objects is enabled through the server properties. See Working with Protected Settings policies on page 46.

These rights are automatically assigned to the System Administrator role when Protected Settings are enabled. No other roles, built in or otherwise, are given the Protected Settings rights. They must be assigned.

IMPORTANT: Built-in roles cannot be modified, so if users require these rights then a new role must be created.

To create and assign the required role to the user responsible for managing containers and controlling the settings on the Protected Settings tab for containers

1. Create a role called **Prot_All** and assign rights listed above and the **Read** right to this role. No other rights are required for this role.
2. Right-click the **Protected Setting** container, and select the **Security** tab. Click **Add** and add the user who is going to manage the container. Give them the **Prot_All** role. Do not give them any other roles to the Protected Settings container. Select **OK** to apply the security changes.
3. Right-click the container that the user is to manage, and select **Properties**.
4. Select the **Security** tab, and click **Add** to add the user account. Give them the **User (built-in)** and the P**rot_All** roles. Click **Apply** and **OK**.

   The user account now has the necessary rights to make all the required changes to the container.

To review why the above roles were created and assigned consider the following:

- The Prot_All role gives the user the necessary rights to perform any of the Protected Settings functions and because they have the Read right, the user can see what is in the Protected Settings container but cannot change or add anything to the container. The ability to Read is needed so the user can assign a Protected Settings policy to a container or any sub containers being managed.

- The User role is also given so the user can do the normal actions such as create, check out, edit, and check in a GPO in the container. The role Prot_All has the right, Export Group Policy Objects as Protected Settings policies. The user also needs the Create right which is part of the built-in User role.

Securing protected settings

Protected Settings policies can be further controlled by delegating who has permission to modify protected settings. To secure the protected settings, you can assign a role (that contains the “Modify Protected Settings” right) to a user on the Protected Settings policy. If during the validation process, GPOADmin determines the current user possess this right, the associated Protected Settings policy is excluded from the validation allowing the modification of those protected settings to proceed.

Create a Protected Settings policy

Once the ability to use Protected Settings has been enabled, you can create the policies using one of the following methods:

- Create a policy directly from the Protected Settings container.
- Export a GPO to the Protected Settings container.
- Drag a GPO onto the Protected Settings container.

To create Protected Settings Policy from the Protected Settings container

1. Select the **Protected Settings** container in the tree view.
2. Right-click and select **New | New Protected Settings Policy**.
3. Enter a name for the policy. Quest recommends using a naming convention that sets these GPOs apart from other GPOs and make them easily identifiable as protected. For example, PROT_01.
4. Select the domain that the Protected Settings policy will be related to and click **Next**.
5. In the Settings page, edit the policy and configure the setting you want to protect.

   NOTE: You can elect to configure the settings later.

6. Click **Finish**.

   The policy is identified as a Protected Setting Policy type and has the same icon as the Protected Settings container.

   At this point, the Protected Settings policy is checked out and has a version of 0.0.

   Protected Settings policies have a modified workflow and therefore require workflow processing such as requesting approval during creation.

To export a GPO to the Protected Settings container

1. In the Version Control Root, right-click the GPO you want to export, and select **Protected Settings | Export as Protected Settings**.
2. Select the version of the GPO you want to make as a Protected Settings policy, and click **Next**.
3. Review and confirm the version and GPO to export, and click **Finish**.

   The selected GPO exports and then import into the Protected Settings container.
4. Refresh the **Protected Settings** container.

   The newly imported GPO has the same name as the exported GPO. Best practice is to rename it using a naming convention that identifies it as protected. For example, PROT_01.

To create a Protected Settings policy through drag and drop

1. In the **Version Control Root**, select the GPO you want to use for a Protected Settings policy.
2. Drag it on the Protected Settings container.

   The Export Wizard opens.
3. Select the version of the GPO you want to make as a Protected Settings policy, and click **Next**.
4. Review and confirm the version and GPO to export, and click **Finish**.

   The selected GPO exports and then import into the Protected Settings container.
5. Refresh the **Protected Settings** container.
6. The newly imported GPO has the same name as the exported GPO. Best practice is to rename it using a naming convention that identifies it as protected. For example, PROT_01.

Protecting policy settings based on extensions

If required, you can prevent users from editing policy settings based on one or more policy extensions. Once you have selected the extension to block, if a policy contains any settings from the extension, the policy will fail the validation test and will not be checked in.

NOTE: A blocked extension overrides allowed settings in a Protected Settings policy.

NOTE: The Modify Protected Settings right is required to block file extensions using a Protected Settings policy.

Available extensions include:

- All Computer Extensions
- All User Extensions
- Advanced Audit Configuration
- Application Control Policies
- Central Access Policy
- Data Sources
- Deployed Printer Connections Policy
- Devices
- Disk Quota
- Drive Maps
- Environment Variables
- Files
- Folder Options
- Folder Redirection
- Folders
- Ini Files
- Internet Explorer Maintenance
- Internet Settings
- IP security
- Wired Network Policies
- Local Users and Groups
- Name Resolution Policy
- Network Access Protection Client Management
- Network Options
- Network Shares
- Policy-based QoS
- Power Options
- Printers
- Public Key
- Regional Options
- Administrative Templates
- Remote Installation
- Scheduled Tasks
- Scripts
- Security
- Services
- Shortcuts
- Software Installation
- Software Restriction
- Start Menu
- Windows Firewall
- Windows Registry
- Wireless Network Policies

To block specific extensions

1. Right-click the required object or container and select **Properties**.
2. Select the **Protected Settings** tab and the **Blocked Extensions** tab.
3. Click to select the extensions that you want to block and click **Apply**.

Generating Protected Settings policies reports

The following reports are available for Protected Settings policies: Latest, Working Copy, and Differences reports.

To generate a report

1. Select the **Protected Settings Root** container in the tree view.
2. Right-click the Protected Settings Policy, and select **Reports**.
3. Select the type of report to run.

NOTE: When a Protected Settings policy is used in GPOADmin, a separate report is generated by the protection process and is generated when the comparison is made between a Protected Settings policy and a GPO.

Using Protected Settings policies

Once Protected Settings policies have been enabled through the Version Control properties and created they need to be applied to a container in GPOADmin.

This is done through new option on all containers that becomes available when the Enable Protected Settings for Group Policy Object is enabled.

To apply a Protected Settings policy

1. Right-click a container and select **Properties**.
2. Select the **Protected Settings** tab.
3. Select the **Add** button.
4. Select the policy to apply and click **OK**.

   The selected protected policy displays in the Assigned Protected Settings policy window with the default validation rule.

   NOTE: Inherited policies are displayed as disabled.

5. Select the validation rule that will be used to detect if a user is attempting to use or alter a protected setting, and choose to base it on **Settings** or a **Value**.

   If you selected **Value** from the drop-down list, you can now choose the items to check. Select from the following:

   None: Items that exist in the policy that do not exist in the Protected Settings Policy are ignored.

   User Rights Assignment: Items that exist under the User Rights Assignment in the policy that do not exist in the Protected Settings Policy are included in the validation process and are flagged as Invalid.

   All: Items that exist in the policy that do not exist in the Protected Settings Policy are included in the validation process and are flagged as Invalid

   A check is made for any similarities between the Protected Settings policy and the GPO being checked in. This can be either based on the settings name or value.

a **Settings defined in the Protected Settings policy are not allowed**: If a setting with the same name as a setting in the protected policy is detected in an active GPO, notification is generated. The value does not have to be the same for the setting, just the setting name.

b **Values other than those defined in the Protected Settings policy are not allowed**: If there is a setting used in the active GPO that has a value different than the protected value, then a notification is generated.

6 To block the Protected Settings from the parent container, select the **Block Protected Settings Inheritance** setting. You may want to do this as this container needs a unique protected setting and the setting from the parent would conflict with the new settings being applied.

7 Exclusions can be set for any GPO in the container which may contain protected settings. This allows specific GPOs to be excluded from any protected setting checking. Place a tick in the check box for any of the listed GPOs that you want to exclude from the Protected Settings policy.

8 If necessary, select **Include Group Policy Objects in all child containers** to allow the checking of all child containers against the assigned protected settings policy.

NOTE: Because there can be GPOs with the same name in GPOADmin, the path of the GPO is also listed to ensure that you select the correct GPO for exclusion.

9 Once you are satisfied with your selections, click **Apply** and then **OK**.

Checking a GPO against a Protected Settings policies and blocked extensions

A GPO that resides in a container with Protected Settings enabled will be checked against the protected settings policy when the GPO is checked in using Check-In.

During a check-in, the GPO is checked against the Protected Settings policy and any blocked extensions. Users that have the Modify Protected Settings right on the GPO in question, will have the option to continue with the check in and override the blocked setting or review a report and address the issue.

The report displays with the associated Protected Settings policies and blocked extensions, how many matches were found, and the Validation mode (either setting name or value).

NOTE: The GPO remains checked out until the issue with the Protected Settings policy is rectified and the GPO passes the check.

Validating a GPO against a Protected Settings policies and blocked extensions before a check-in

A GPO can be checked against the Protected Setting policy and blocked extensions before checking it in.

To check a GPO before a check-in

1 Right-click the GPO you want to check and select **Protected Settings | Verify Protected Settings**.

This checks the GPO against the Protected Settings policy and blocked setting. If the GPO includes secured settings, a dialog box displays with the associated Protected Settings policies, blocked extensions, how many matches were found, and the Validation mode (either setting name or value).

2 Select **View Report** to generate a report that displays the differences between the GPO and the Protected Settings policy. You can select to print or save the report. Once you have finished viewing the report click **Close**.

3 Click **OK** in the Protected Settings Modifications Detected dialog box to close it.

NOTE: The GPO remains checked out until the issue with the Protected Settings policy is rectified and the GPO passes the check.

Working with Protected Settings Policy Baselines

If you have GPOADmin configured with SQL as the configuration store, you can select to assign Protected Setting policies to individual GPOs as policy baselines.

When this option is enabled, the Watcher service will validate the settings against the policy baseline when a registered GPO is modified outside of GPOADmin. If a deviation is detected, a notification will be sent to all subscribers of the policy Deviation notification. The notification will include a difference report that is focused on only the settings that are in the baseline.

To enable Protected Settings policy baselines for Group Policy Objects

1 Ensure GPOADmin is configured with SQL as the configuration store.

2 Right-click the domain and select **Options**.

3 Select **Options | General** and select **Enable Protected Settings for Group Policy Objects** and select Enable Policy Baselines.

To receive deviation notifications

1 Expand the **Version Control Root** node, and the required container.

2 Right-click the required object and select **Properties**.

3 Select **Notifications**, and subscribe to the **Policy Deviation** notification.

To grant permission to assign a policy baseline

1 Edit or create a new role and assign the **Modify Protected Settings Baseline Assignment** right. See Configuring role-based delegation for details.

To assign policy baselines to a policy

1 As a user with the **Modify Protected Settings Baseline Assignments** right and the **Read** right on one or more Protected Settings Containers, right-click a policy and select **Properties.**

2 Click the **Policy Baseline** tab.

3 Click to enable to **Monitor this policy for deviations from the following Policy Baselines option.**

4 Click **Add** to open the Policy Browser dialog, select the baselines to add, and click **OK**.

5 Click **OK** again to save and apply your changes.

3

Using GPOADmin

- Connecting to the Version Control system
- Working with multiple connections
- Navigating the GPOADmin console
- Search folders
- Accessing the GPMC extension
- Configuring user preferences
- Working with the live environment
- Working with controlled objects (version control root)
- Checking compliance
- Editing objects
- Synchronizing GPOs
- Exporting and importing

Connecting to the Version Control system

When the GPOADmin console is closed, the GPOADmin servers you were connected to are persisted, so the next time you open GPOADmin the connections to those servers are initiated automatically.

If you selected the “Remember my password” check box during the initial connection, then you will not be prompted for credentials the next time you connect. Each connection to this server from here on will automatically use the specified credentials, which are stored in Windows Credentials Manager. To logon as a different user, you must remove the entry from the Windows Credentials Manager.

To connect to the Version Control system using the GPOADmin console

1. Right-click the **GPOADmin** node and select **Connect To**.
2. Click **New** to create a new connection and enter the server name.

   The connection dialog, is automatically populated with GPOADmin Services detected in the environment.
3. Select the required Version Control server and click **Connect** to connect with the current logged on user credentials or select the down arrow in the Connect button and select **Connect As** to enter new credentials (domain\user and password).
4. To save the credentials, select the **Remember my password** check box and click **OK**.

Restricting search scope

If required, you can restrict which global catalogs are used within the forest to search for the GPOADmin server during connection.

To restrict the search scope:

1. Create a file called PreferredGCs.txt.
2. List the fully qualified domain name of each Global Catalog server to include in the search on their own row in the file.
3. Save the file to the installation directory.

When you connect to GPOADmin, only the global catalog servers listed in the file will be searched as possible connection points. If this file is not included, GPOADmin will search all global catalog servers in the forest.

Working with multiple connections

If you have multiple connections, consider the following:

- Each connection display its own Lost and Found, Report, and Search Folder containers.
- When connecting to GPOADmin, the User Preferences menu option is disabled if you are not logged on to the client host computer. (This is because this option is stored in the registry of the connected user.)
- When connecting to GPOADmin, you are prompted to select a report location when first accessing the Reports container if you are not logged on to the client host computer. (This is because the users report folder is stored in the profile of the connected user.)
- If you connect to GPOADmin and have been assigned multiple root containers through group membership, you may have access to the same folders through each root container.

  For example, you have a container called PARENT which has a child container called CHILD and you are a member of Group A and Group B. Group A is assigned PARENT as their root container; Group B is assigned CHILD as their root container. When you log into GPOADmin you will see both PARENT and

CHILD as root containers instead of the Version Control Root container, allowing for two ways to access the CHILD container.

Version Control data in the directory

GPOADmin does not delete the information stored in the directory when it is uninstalled. The Version Control information may be deleted manually if it is no longer required.

GPOADmin uses "working copies" of objects for editing purposes. If the Version Control information is deleted from the server, while objects are still pending creation or in a minor version, these working copies may be seen as "Unregistered" if a new instance of the version control information is instantiated.

Navigating the GPOADmin console

The GPOADmin console consists of a window divided into two panes.

The left pane displays a hierarchical structure of the live enterprise objects and the Version Control systems that are available to you.

- Version Control Root enables administrators to organize many objects logically based on their enterprise structure.
- Lost and Found contains any deleted containers and the associated version controlled items and sub-containers.
- Reports which mirror the contents of My GPOADmin Reports folder in the Documents folder.
- Search Folders which allow you to view the status of objects within the Version Control system.
- Protected Settings Root is available to store and manage the Protected Settings policies deployed within your environment (if this option is enabled, see Working with Protected Settings policies on page 46).

The right pane displays the details that pertain to the selected item in the console tree. For version controlled objects this includes:

- name
- type
- version
- status
- pending action
- compliance status
- whether workflow is enabled
- deployment time
- managed by (who is responsible for it)
- the user who has it checked out
- the domain where it is applied
- when it was modified
- when it was last deployed
- associated keywords

Search folders

Search folders are an easy way to view the status of objects within the Version Control system. A complete list of default search folders is made available to cover most of your needs.

NOTE: If your deployment includes multiple servers, when you select a search folder (or refresh the page), you are presented with a dialog that allows you to narrow the search results by selecting one or more of the connected servers.

However, you can also create custom search folders to meet your specific requirements. See Creating custom search folders.

The default search folders include:

- All Managed objects: Displays all registered objects under version control within GPOADmin.
- Available: Displays all objects with an available status within the version control system.
- Checked out: Displays all objects not available due to being checked out for modification.
- Checked out to me: Displays all objects checked out to the user who is logged in to GPOADmin.
- Pending approval: Displays all objects awaiting specified approvals before being deployed.
- Pending deployment: Displays all objects awaiting deployment to the live environment.
- Failed deployment: Displays all failed deployments to the live environment.
- Containers: Displays container name, managed by, and full path information. From here you can search for specific containers based on previously applied keywords.
- Cloaked: Displays all cloaked GPOs.

NOTE: You must have the View Cloaked right to see these GPOs.

- Locked: Displays all locked GPOs.
- Unauthorized modifications: Displays all registered objects that were modified in the live environment outside of the GPOADmin version control system.
- Deleted objects: Displays all objects awaiting deletion.
- Unregistered: Displays all objects in the managed forest not registered within the version control system.
- Workflow enabled objects: Displays all objects registered within the version control system which are workflow enabled.
- Workflow disabled objects: Displays all GPOs registered within the version control system as workflow disabled.

NOTE: Any setting changes to these GPOs will be applied within version control as well as to the live environment.

- Linked scopes of management: Displays Scopes of Management that have linked GPOs.
- Unlinked scopes of management: Displays Scopes of Management that have no linked GPOs.
- Desired State Configuration Resources: Displays all the registered DSC scripts.

Creating custom search folders

Custom search folders allow you to combine many variations to augment the ability to view the status of the objects within your Version Control system deployment.

For example, because the “Name” and “Domain Name” support the use of wildcards (such as Name = *Accounting*), you can select to view all the unregistered objects that contain “Accounting” in their name to help pinpoint issues that require your attention.

You can also select to filter the search to return results based on specified GPO settings.

To create a custom folder

1. Right-click the **Search Folders** and select **New Custom Search**.
2. Right-click **New Custom Search** and select **Properties** to configure the type of objects that will be included in the search folder.
3. Begin by selecting the object attribute from the **Field**. These options allow you to create custom folders so that you can easily perform actions in bulk on objects that contain a specified value.

   You can select from cloaked, compliant, deleted, domain name, unique ID, locked, name, status, pending action, type, GPOADmin ID, workflow enabled, deployment results, keywords, managed by and attestation overdue.

   NOTE:
   - Search folders using the 'managed by' and 'attestation overdue' criteria can only be created when using SQL-based configuration stores.
   - Creating a filter with the Deleted field = True returns objects that have been deleted outside of the Version Control system; while a filter on Status = Deleted returns objects that have been deleted internally and have a deleted status.
4. Select the required **Value** for the selected object attribute. The available selection depends on the chosen field. (For example, the available keyword values reflect the primary list of keywords previously assigned to the object; the deployment results have a “Success” or “Fail” value with success returning items that were successfully deployed during the last deployment and fail returning items that failed their last deployment.)
5. Click **Add**.
6. Continue refining your query by adding attributes and values as required. You can also use {And} and {Or} operators to further refine the folder contents.

   To add a logical grouping, click on the whitespace to enable the {And} and {Or} buttons.

   To add a clause outside of a grouping, click on the white space to enable the Add button.

   To add a clause to a grouping, click on the open bracket of the clause.

   To delete a clause click on word 'And' or 'Or' and click the delete button.
7. For a a GPO search, you can select the **Apply settings to results option** and enter a value to filer the search results. For example, you easily search for and view all GPOs that contain the word "Enabled".
8. Select the run icon to run the query to see if it returns the expected result.
9. If you have more than one service installed, you need to select the service where the custom search will be saved and select **OK**.

   NOTE: While you are creating your filter, only objects from the service where you are saving the custom search will display. You can use this sample data to ensure the search meets your needs. Once the filter is applied, it will be applied to all connected services.
10. Once you are satisfied with the folder configuration, save it, and click **OK**.
11. Right-click the **New Custom Search** folder and select **Rename** to provide a meaningful name.

Accessing the GPMC extension

As part of its installation, GPOADmin appears as a tab in Microsoft Group Policy Management Console (GPMC). In the right pane, there are now two tabs: one for GPMC, and one for GPO Management. On the GPO Management tab, all GPOs are listed, regardless of whether they are under version control. The GPMC Extension has a toolbar for easy access to commonly used functions.

NOTE: Most tasks can be performed using either the toolbar or the context menu.

You are automatically connected to the Version Control server selected during the installation process, based on the credentials of the currently logged in user. You can connect to other Version Control servers if needed.

For a full list of tasks you can perform using the GPMC Extension, see Group Policy Management Console extension on page 12.

To access the GPMC Extension

1. In the GPMC, expand the forest, domain and domain node.
2. Click the **Group Policy Objects** node.
3. Click the **GPO Management** tab.

Configuring user preferences

Through user preferences, you can set where to store your reports, where to send notifications, and the default script editor.

To configure user preferences

NOTE: You must configure user preferences in the GPOADmin console.

1. Right-click the forest, and select **User Preferences**.
2. Select the **Preferences** tab.
   a. Choose a folder or disk where you want to store your reports.
   b. By default, Notepad is configured for editing scripts. To set an alternative editor, click **Add**, and enter the script extension, the application, and optional switches to use.
3. Select the **Notifications** tab and enter the email address where you want to have the notification messages sent.

   For more information on configuring the Notification system, see Selecting events on which to be notified.
4. To remove a notification, select the notification source and click the **Remove** button.
5. Click **OK**.

Working with the live environment

- Registering objects
- Registered status
- Removing registered objects
- Viewing the live environment

Registering objects

To start working with the Version Control system, the GPOs, starter GPOs, scripts, DSC scripts, WMI filters, and Scopes of Management (Sites, Domains, and Organizational Units) must be registered. You have the option to make GPOs workflow enabled at the time of registration and to maintain the version history of objects that were previously registered within GPOADmin.

Registering and unregistering are recursive for objects when they are selected from the treeview on the left of the console. All child objects are included unless you individually select lower-level objects to register.

You have the choice of registering all items in the selected container or domain, all GPOs, all scripts, all DSC scripts, or all WMI Filters when you use the Register menu. When you register objects at the domain level, you do not automatically register GPOs, scripts, DSC scripts, or WMI filters in the domain unless they are already linked to the Scopes of Management that are being registered. You can select WMI Filters, scripts, DSC scripts, and GPOs separately, using their respective folders.

NOTE: Only users with the Register and Unregister rights can register and unregister objects. For more information, see Configuring role-based delegation on page 38.

NOTE: Scripts contained in the SYSVOLS Scripts folder (and its subfolders) can be registered and will be detected by the Watcher Service and reported as non-compliant. DSC scripts are not monitored by the Watcher Service.

When an object is added to the system for the first time, it will be automatically backed up (stored) in the Version Control system history and labeled with a version of 1.0, unless another major version number is specified during the registration process. Each time a change is made (an object is checked in) a minor number is added. For example, v1.2, v1.3, and v1.4. When a change is deployed to the enterprise by a user with the appropriate role, the version number will change to the next major number, for example, v2.0 and v3.0.

NOTE: GPOADmin works with pre-existing GPOs, scripts, DSC scripts, WMI filters, and Scopes of Management, as well as any other objects created from within the system.

NOTE: If an object is not registered in version control, the modified date displayed is returned from the live object.

NOTE: You must have the Register right and access to the Live Environment to perform the following steps.

NOTE: Before you can register DSC scripts, you must enable DSC support in the Server options and specify a DSC root directory for each domain that will support DSC scripts. This root directory serves as the starting point for the DSC script enumeration and deployment location. See Editing the Version Control server properties on page 24.

NOTE: The Starter GPOs folder is not created by default. To create the Starter GPOs folder, open Group Policy Manager, expand the required **Domain | Starter GPOs**, and click **Create Starter GPOs Folder**.|

To register objects using the GPOADmin console

1. Expand **GPOADmin**, the **Live Environment**, and domain nodes, and select the object you want to register within the Version Control system.
2. Right-click and select one of the following: **Register - This Object Only, - All**, **- Group Policy Objects**, **- Scopes of Management,** or **- WMI Filters**.
3. Select the container in which you want to place the registered object, or create a new container, and click **OK**.

   Once the objects have been registered, they are located in the selected container under the Version Control Root with the initial version number set to 1.0. They are now available to be checked out and edited. You can set the major version number to any number greater than 1.0 (for example to maintain a version number if you are migrating from another Version Control system).

   Users with the delegated rights can link registered GPOs to Scopes of Management (Sites, Domains, and Organizational Units) and add WMI Filters. For more information about linking GPOs, see Linking GPOs on page 98. For information about adding WMI Filters, see Creating Group Policy Objects (GPOs) on page 67.

To register GPOs using the GPMC Extension

NOTE: You must use the GPOADmin console to register WMI filters and Scopes of Management.

Registering GPOs using the GPMC Extension is not recursive. If you want to register all child objects at once, use the GPOADmin console.

1. Expand the forest, domains, and domain nodes. Click the **Group Policy Objects** node, and select the GPO you want to register within the Version Control system.
2. Click **Register**.

3 Select the container in which you want to place the registered object and click **OK**.

OR

Click **New Container** and name the container then click **OK**.

Registered status

You can quickly see the status of registered GPOs, starter GPOs, scripts, DSC scripts, WMI filters, sites, domains, and OUs. The objects will either be available for check out, already checked out, or checked in and awaiting approval to be committed to the enterprise. The options available to you at each state will depend on your specific role and permission. Registered objects will be in one of the following states:

Table 12. Registered Status

Status	From this state, depending on your assigned role and enabled options, you may have the ability to:
Available	• link • search and replace • edit • check out • import and export settings • import Security Compliance Manager Backup in group policies • request approval (for objects that have minor versions greater than zero) • deploy (for objects that have minor versions greater than zero) • label • cloak/uncloak GPOs • lock/unlock GPOs • enable/disable workflow for GPOs, SOMs, and WMI Filters • managed by • check compliance • unregister objects • protected setting - export • create and save reports dealing with latest, and live objects, and the difference between them • show history • Synchronize – Synchronize Now, Set Synchronization Targets, and Validate Synchronization Results • edit object properties • refresh the object • cut • copy • mark objects for deletion • rename (This does not apply to SOMs.)

Table 13. Registered Status

Status	From this state, depending on your assigned role and enabled options, you may have the ability to:
Checked Out	• link • search and replace • edit objects • check in objects • undo any check out • import and export settings • import Security Compliance Manager Backup in group policies • request approval (for objects that have minor versions greater than zero) • deploy (for objects that have minor versions greater than zero) • label • managed by • protected setting - export and verify • create and save reports dealing with latest, live, and working copy objects, and the difference between them • show history • Synchronize – Synchronize Now, Set Synchronization Targets, and Validate Synchronization Results • edit object properties • refresh the object • cut • copy • rename (This does not apply to SOMs.)

Table 13. Registered Status

Status	From this state, depending on your assigned role and enabled options, you may have the ability to:
Pending Approval	• link • search and replace • export settings • withdraw approval request • approve changes • reject • deploy the changes to the environment • label • managed by • protected setting - export • create and save reports dealing with latest and live objects, and the difference between them • show history • Synchronize –Set Synchronization Targets, Validate Synchronization Results • edit object properties • refresh the object • cut • copy
Pending Deployment	• link • search and replace • export settings • reject • withdraw approval • deploy the changes to the environment • label • managed by • protected setting - export • create and save reports dealing with latest, and live objects, and the difference between them • show history • Synchronize –Set Synchronization Targets, Validate Synchronization Results • edit object properties • refresh the object • cut • copy

Removing registered objects

If you no longer want the object to be available for changes, you can remove it from the Version Control system, as long as you have been granted the Unregister right. Unregistering version-controlled objects is now recursive, unless you select the lower-level objects individually.

To remove objects from the Version Control system using the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click the object and select **Unregister**.

To remove GPOs from the Version Control system using the GPMC Extension

Unregistering GPOs using the GPMC Extension is not recursive. If you want to unregister all child objects, use the GPOADmin console.

1. Select the **Group Policy Objects** node and then select the GPO.
2. Click **Register** or right click and select **Unregister**.

NOTE: You can view a list of Unregistered objects in the Search Folders in the GPOADmin console. This includes GPOs, scripts, DSC scripts, WMI filters, and SOMs.

Viewing the live environment

As the administrator, you may want to allow users to see the live environment from within the GPOADmin console. This will, for example, enable you to delegate GPO, OU, or SOM object registration (and recursive registration) to specific users in your organization.

However, you may not want all domains within the live environment to be displayed to all users. Through the live environment properties you can also restrict which domains will display, be included in reports, and be available within the object creation wizard.

To permit a user to see the live environment

1. Login to GPOADmin as a GPOADmin administrator.
2. Right-click the **Live Environment** node and select **Properties**.
3. On the Security tab, add one or more user who require access to the live environment.
4. Click **OK**.

To exclude specific domains from being displayed in the live environment

1. Login to GPOADmin as a GPOADmin administrator.
2. Right-click the **Live Environment** node and select **Properties**.
3. On the Domains tab, select the domains to exclude and click **OK**.

Working with controlled objects (version control root)

- Creating a custom container hierarchy
- Selecting security, levels of approval, and notification options
- Viewing the differences between objects
- Copying/pasting objects
- Proposing the creation of controlled objects
- Merging GPOs
- Restoring an object to a previous version
- Restoring links to a previous version
- Managing your links with search and replace
- Managing compliance issues automatically with remediation rules
- Validating GPOs
- Working with registered objects
- Working with available objects
- Working with checked out objects
- Working with objects pending approval and deployment

Creating a custom container hierarchy

You can organize registered objects into a user-defined hierarchy under the Version Control Root container.

Each container has its own “security descriptor” in which trustees can be delegated roles to define their access to the contained objects. For more information see Configuring role-based delegation on page 38.

Once you have the containers created, you can easily move and copy objects to other containers within the same domain.

To create a new container

1. Expand the treeview and select the **Version Control Root** or subcontainer.
2. Right-click and select **New | Container**.
3. Enter the container name and click **OK**.

NOTE: If you are working in the GPMC Extension, you can only create a container when you are registering an object (for more information see Registering objects on page 58). You cannot delete or label containers in the GPMC Extension.

To delete a container

NOTE: You must use the GPOADmin console to delete a container.

1. Expand the treeview and locate the container under the Version Control Root node.
2. Right-click the container and select **Delete**.

   When you delete a container any associated version controlled items and sub-containers will be stored in the Lost and Found container.

To label a container

NOTE: You must use the GPOADmin console to label a container.

1. Expand the treeview and locate the container under the Version Control Root node.
2. Right-click, and select **Label**.
3. Enter the label for the container, and click **OK**.

Selecting security, levels of approval, and notification options

Through the container and object properties, you can delegate responsibilities over the container through the security options, implement safeguards by designating multi-level approvers, and set the events to be notified on. If the Protected Settings option has been enable, you can also assign protected setting and set exclusions.

NOTE:

- Configuring multi-level approvers will require that a change is approved by the designated number of approvers before it will become available for deployment in the live environment.

To set the security, approval level, and notification options on an object or container

1. Right-click the **Version Control Root** node, required container or object, and select **Properties**.
2. Select the appropriate option to configure the associated settings.

   For more information on delegating roles see Configuring role-based delegation on page 38. For more information on configuring the notification system, see Selecting events on which to be notified on page 44.

NOTE: If you are using the GPMC Extension, you can only set these options for GPOs.

Viewing the differences between objects

You can create a report that shows the differences between two or more objects.

To view the difference between settings using the GPOADmin console

1. Expand the **Version Control Root** node, and the required container.
2. Select two or more similar objects, right-click and select **Reports | Differences**.
3. In the **Base** column, select the Base object that you want to compare the other objects to.
4. In the **Version** column, select a version for each object to compare.
5. In the **Show** list, choose an option for which data to show in the report.
6. Click **OK**.
7. View the Report.

   If you choose to compare more than one object to the base, each comparison report is displayed in its own tab.
8. Click **Print** to print the report.

   Click **Save As** to save the report in HTML.
9. Click **Close**.

To view the difference between GPO settings using the GPMC Extension

1. Select the two or more GPOs to compare.

2 Click **Reports | Differences**. Select the version that you want to compare from the lists, and click **OK**.

3 In the **Base** column, select the Base object that you want to compare the other objects to.

4 In the **Version** column, select a version for each object to compare.

5 In the **Show** list, choose an option for which data to show in the report.

6 Click **OK**.

7 View the Report.

If you choose to compare more than one object to the base, each comparison report is displayed in its own tab.

8 Click **Print** to print the report.

9 Click **Save As** to save the report in HTML.

10 Click **Close**.

Copying/pasting objects

You can easily copy and paste objects within the hierarchy. When you copy and paste an object within the version control system, you have the option to preserve the object's history.

NOTE: Multiple objects can be cut and pasted, but you can only copy and paste one object at a time.

You can choose the version of the object to copy. When a single object is pasted, you have the option to select the live version (if available), the working copy (if the object is currently checked out to you) or any of the historical versions of the object.

When you paste the object, it becomes a new object with a version of 0.0 in the checked out state. This version number indicates that the version is not considered "live" until it goes through the approval process. If you copy and paste the GPO with the history, it becomes a GPO that is shared with the original GPO.

NOTE: If you copy and paste an object that is checked out, changes to the working copy will not be pasted. Only the history, up to the last checked out version, can be pasted.

When you drag and drop an object between containers on the same service, it will invoke the "move" operation. If dragging and dropping between containers on different services, it will invoke the "copy" operation.

When you right-click and drag and drop, you will be presented with two options: "Copy here" and "Move here". When dragging between containers on the same service, a copy means copy and a move means move. However, when dragging and dropping between containers on different services, regardless of which option is selected, the copy operation will be invoked.

NOTE: You cannot move objects between domains.

To copy and paste an object

NOTE: You cannot copy and paste objects in the GPMC Extension.

1 Expand the **Version Control Root** node and the required container.

2 Right-click an object and select **Copy**.

3 Right-click the target container, and select **Paste**.

4 From the Export wizard, select the version that you want to test and click **Next**.

5 Select the target Version Control domain for the object and click **Next**.

If you choose to copy the history from the source, when you view the history on the pasted object, the actions are clearly marked as having been actions on the source.

If an object with the same name already exists in the target container you will have the following options: cancel the paste, edit the name, or continue using the duplicate name.

6 Select a migration table (if required) and click **Next**.

7 Click **Finish**.

NOTE: If the Enable Unique Names option is selected, the copied object's name will be the same as the original with an auto-incremented numerical value appended. For example, Name (1), Name (2). etc.

Proposing the creation of controlled objects

- Creating Group Policy Objects (GPOs)
- Creating starter GPOs
- Creating WMI filters
- Creating scripts
- Creating Desired State Configuration (DSC) PowerShell scripts

Creating Group Policy Objects (GPOs)

Users with the appropriate permission can propose the creation of a GPO that does not currently exist in the enterprise environment and have it placed within the Version Control system. If you have starter GPOs within your version control system, you can select one to use as a basis for a new GPO.

When you create a GPO as Workflow Disabled, you are creating it in the context of the user you are logged in as. This GPO sits immediately in the live environment.

NOTE: To work with and edit workflow disabled GPOs, you must have the GPMC Edit, Delete, and Modify Security right as well as the DeleteSubtree right.

When you create a GPO as Workflow Enabled, you create it in the context of the GPOADmin Service Account and this GPO sits awaiting deployment. Once deployed, it sits in the live environment.

To propose the creation of a GPO in the GPOADmin console

1 Expand the **Version Control Root** node, right-click the required container, and select **New | Group Policy Object**.

2 Enter a name and select the location for the GPO and click **Next**.

3 If required, select the Starter GPOs to use as a basis for this new GPO.

4 Click **Launch Editor**.

5 Make the required edits to the new GPO and close the Group Policy Editor.

6 Modify any additional GPO settings if required and click **Next**.

7 If required, click **Add**, enter security filters, and click **Next**.

8 If required, select WMI filters to apply, and click **Finish**.

When you make edits and check the GPO in, the version will be updated to version 0.1. This number will increase by.1 until you select to Check In and Request Approval. At this point the GPO is not live.

Once you complete your edits, you can select Check In and Request Approval. If approved and deployed, the new GPO will become available with a version number of 1.0. For more information on the approval and deployment process, see Requesting approval on page 86 and Deploying objects (scheduling and associated items) on page 91.

Users with the delegated rights, can link registered GPOs to Scopes of Management (Sites, Domains, and Organizational Units) and add WMI Filters. For more information about linking GPOs, see Linking GPOs on page 98. For information about adding WMI Filters, see Creating WMI filters on page 68 and Creating Group Policy Objects (GPOs) on page 67.

To propose the creation of a GPO in the GPMC Extension

1. Right-click in any blank area of the GPO Management pane and choose **New | Group Policy Object**.
2. Enter a name and select the location for the GPO and click **Next**.
3. If required, select the Starter GPOs to use as a basis for this new GPO.
4. Click **Launch Editor**.
5. Make the required edits to the new GPO and close the Group Policy Editor.
6. Modify any additional GPO settings if required and click **Next**.
7. If required, click **Add**, enter security filters, and click **Next**.
8. If required, select WMI filters to apply, and click **Finish**.

Creating starter GPOs

Starter GPOs include a collection of Administrative Template policy settings in a single object. They are useful when you want to distribute a GPO with specific settings to other environments. When you create a new GPO from a starter GPO, it inherits all of the Administrative Template policy settings and values of the starter GPO.

There are 2 type of starter GPOs:

- User-defined starter GPOs which are editable.
- System starter GPOs which are read-only and provide a baseline of GPO settings.

NOTE:

- The Starter GPOs folder is not created by default. To create the Starter GPOs folder, open Group Policy Manager, expand the required **Domain | Starter GPOs**, and click **Create Starter GPOs Folder**.|
- Starter GPOs created within GPOADmin do not set the Initiator UserName and EventSource fields in Change Auditor.

To create a user-defined starter GPO

1. Expand the **Version Control Root** node, right-click the required container, and select **New | Starter GPO**.
2. Enter a name and location for the starter GPO, and click **Next**.
3. Click **Launch Editor**.
4. Make the required edits to the starter GPO and close the Group Policy Starter GPO Editor and click **Finish**.

   When you make edits and check the starter GPO in, the version will be updated to version 0.1. This number will increase by.1 until you select to Check In and Request Approval. At this point the starter GPO is not live.

   Once you complete your edits, you can select Check In and Request Approval. If approved and deployed, the new starter GPO will become available with a version number of 1.0. For more information on the approval and deployment process, see Requesting approval on page 86 and Deploying objects (scheduling and associated items) on page 91.

Creating WMI filters

Using Windows Management Instrumentation (WMI) filters, you can control where GPOs are applied based on the attributes of a target computer.

The WMI filter associated with the GPO is processed on the target computer. The query, in the WMI filter that is linked to a GPO, is evaluated on the target computer.

For example, your filter may be “Select computers that have a processor speed higher than 2 GHz”. If the target computer meets the criteria, the GPO is applied. If not, the GPO is not applied.

NOTE: The WMI filter and the GPO to which it is linked to must be in the same domain.

To propose the creation of a WMI filter

NOTE: WMI filters must be created using the GPOADmin console.

1. Expand the Version Control container where you want to place the new WMI filter.
2. Right-click and select **New | WMI Filter**.
3. Enter a name for the new WMI filter.
4. Select a domain in which the WMI filter will be created, add a description if required, and click **Next**.
5. Select a Root Namespace (default: root\CimV2) and enter a valid WQL (Windows Query Language) string in the Query field.

   You must have at least one query associated with a WMI Filter to continue.
6. To add an additional query to the filter, select **New Query**, and specify the Root Namespace and Query as described in Step 5.
7. To delete a query, click the “x” button next to the query in the list.
8. Click **Finish**.

   The WMI Filter must go through the approval and deployment process before it can be applied.For further information, see Requesting approval on page 86 and Deploying objects (scheduling and associated items) on page 91.

Creating scripts

Logon, logoff, Startup and Shutdown scripts contained in the SYSVOLS Scripts folder (and its subfolders) can be registered and will be detected by the Watcher Service and reported as non-compliant.

Users with the appropriate permission can propose the creation of a script that does not currently exist in the enterprise environment and have it placed within the Version Control system.

To propose the creation of a script:

1. Right-click the Version Control container and select **New | Script.**
2. Enter a descriptive name and domain where the script will be used.
3. Select where you want to deploy the script and click **Finish**.

Creating Desired State Configuration (DSC) PowerShell scripts

Desired State Configuration (DSC) extends Microsoft PowerShell to facilitate environment configuration – including your GPO deployment. Users with the appropriate permission can propose the creation of a script that does not currently exist in the enterprise environment and have it placed within the Version Control system.

NOTE: Only DSC PowerShell scripts are supported.

To propose the creation of a DSC PowerShell script:

1. Right-click the Version Control container and select **New |DSC Script.**
2. Enter a descriptive name and domain where the script will be used.
3. Select where you want to deploy the script and click **Finish**.

Merging GPOs

To reduce complexity and limit the number of GPOs in your organization, you can select to merge the settings of two GPOs into a single GPO or create a new GPO based on the merged settings. During the merge, any conflicts will be identified so that you can address them as required.

NOTE: Required Permissions

- To create a new GPO based on two existing GPOs:
  - Read, Create and Edit permissions
  - Read and Create Group Policy Object domain rights
- To merge GPO settings into an existing GPO:
  - Read and Edit permissions
  - Read domain right

To merge GPO settings into a new GPO

1. Expand the **Version Control Root** node, and select two GPOs.
2. Right-click and select **Merge | Merge To New Group Policy Object**.

   If conflicting settings are identified, the Merge Conflict Resolution dialog opens. To resolve the conflict, select the settings that you want applied. Once all conflicts are resolved click **OK**.
3. In the New Group Policy Object Wizard, enter a name and select the location for the GPO and click **Next**.
4. If required, select the WMI Filter to associate with the GPO and click **Finish**.

   The new GPO will be created based on the settings of the merged GPOs.

To merge settings into an existing GPO

1. Expand the **Version Control Root** node, and select two GPOs.
2. Right-click and select **Merge | Merge To Existing Group Policy Object**.

   If conflicting settings are identified, the Merge Conflict Resolution dialog opens. To resolve the conflict, select the settings that you want applied. Once all conflicts are resolved click **OK**.
3. Select the target GPO for the merged settings and click **OK**.

   The target GPO will now have the settings from both of the selected GPOs.
4. You now have the option to replace the Scope of Management links in the source GPO with the links in the target GPO. Click Yes, to replace the links, and Yes again in the Search and Replace Links wizard to complete the process.

   NOTE: This option is only available if the source GPO is currently liked to a SOM, the source and target GPO are in the same domain, and the user performing the merge has the Link right on the target GPO.

Restoring an object to a previous version

You can easily create a report that displays the historical settings for objects in the Version Control system or a comparison of versions to locate the differences. For more information, see Establishing Management for an Object on page 79 and Creating Reports on page 107.

You can also import settings from any version in the history of the Version Control System, as well as links between Group Policy Objects and Scopes of Management. This effectively creates a roll back to an earlier set of parameters. You must have the object checked out to perform this action. You must also have the Link right to restore links. For more information, see Configuring role-based delegation on page 38.

Rolling back to a particular version of a workflow enabled GPO does not affect the live enterprise environment until it has gone through the complete approval process. For a workflow disabled GPO, the effect is immediate.

From this point forward, the basic workflow of GPOADmin takes over once again. You must check in and approve the changes to have them go live in the enterprise environment.

For information about restoring inks, see Restoring links to a previous version on page 72.

To restore a previous version of an object using the GPOADmin console

1. Expand the **Version Control Root** node and select the required container.
2. In the right pane, select the required object, right-click and select **Show History**.

   You will see the name, type, version, action, account, date and comment pertaining to the history item.
3. Select the filtering options you want to apply.
4. To view the settings of a previous version, right-click the specific version you want, and click **View**.

   To view the difference in settings between two versions, select the versions using Ctrl + select, then right-click and click **Differences**.
5. Right-click the specific version you want to restore and click **Get**.

NOTE: When you Get a previous version of a workflow disabled GPO, the major version number will be increased by one.

The Get command replaces the settings in the working copy with those from the selected version. If the current object is not checked out, then the Get command will automatically perform a checkout, provided you have the required Edit right. If you do not have the Edit right then the Get option will not be available.

If you are rolling back the links of a GPO whose domain is different to that of the SOM to which it is linked, that SOM would not be available in the dialog box for management.

6. Enter a comment if required.

   You can choose to restore GPO Links. For more information, see Restoring links to a previous version on page 72.
7. Click **OK**.
8. Click **Close**.

To restore a previous version of a GPO using the GPMC Extension

1. Select the GPO and click **Show History**.

   The history displays in the bottom pane of the GPO Management tab. You will see the name, version, action, account, date and comment pertaining to the history item.
2. To view the settings of a previous version, select the version, right-click it and select **View**.

   To view the difference in settings between two versions, select the versions using Ctrl + select, then right-click and click **Differences**.
3. Right-click the version you want to restore and click **Get**.

NOTE: When you Get a previous version of a workflow disabled GPO, the major version number will be increased by one.

The Get command replaces the settings in the working copy with those from the selected version. If the current object is not checked out, then the Get command will automatically perform a checkout, provided you have the required Edit right. If you do not have the Edit right then the Get option will not be available.

4. Enter a comment if required.

   You can choose to restore GPO Links. For more information, see Restoring links to a previous version on page 72.
5. Click **OK**.

Restoring links to a previous version

You can restore the links between a GPO and its Scopes of Management, either to the last backup settings or to a specific history version that you select.

The affected Scopes of Management must be in the Available state, and the user must have rights to edit the SOMs, as well as the Link right, to restore the links. For more information, see Configuring role-based delegation.

To restore links to a previous version using the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click an object and select **Show History**.

   You will see the date, account, version, comment, and applicable action that generated the history item.
3. Select the version you would like to restore, right-click and select one of the following:

   To restore just the links, select **Restore Links**.

   To restore the object and the links together, select **Get** and then select the **Restore GPO Links** in the Comment box.
4. In the **Restore Links** box, you can review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.

   Hover over a link to get more information. If a link has an exclamation mark beside it, the Scope of Management Object is not Available.
5. Click **OK** and close the History box to complete the restore.

   At this point the modified SOMs, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

NOTE: You may need to right-click the object and select Refresh to ensure that you see its updated Status.

You can also restore Scope of Management links when rolling back a noncompliant GPO and when restoring a deleted GPO. For more information see, Checking compliance on page 93.

To restore links to a previous version using the GPMC Extension

1. Check out the Group Policy Object you want to restore.
2. Select the object and in the toolbar above, select **Show History**.

   You will see the date, account, version, comment, and applicable action that generated the history item in a list below the Group Policy Objects list on the right.
3. Select the version you would like to restore, right-click and select one of the following:

   To restore just the links, select **Restore Links**.

   To restore the object and the links together, select **Get** and then select the **Restore GPO Links** in the Comment box.
4. In the **Restore Links** dialog box, you can review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.
5. Click **OK** and close the History box to complete the restore.

   At this point the modified SOMs, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

Managing your links with search and replace

You can select a GPO that is currently linked to an OU and search for all occurrences of that link, then choose to replace, remove, or append anywhere that GPO is linked. This can also be done manually, but the Search and Replace is faster and it ensures all links are included.

NOTE: You must have the link right on each GPO and SOM you wish to manage.

To append links

1. Expand the node containing the GPO that you wish to manage and select it, then right-click the GPO and select **Search and Replace**.
2. To append the new links, leaving the original links intact, select **Append**.

   You will be asked to select the second GPO in the next step.
3. Click **Next**.
4. Expand the tree to select the GPO to append, then click **Next**.

   The **Review Links** panel now shows you the links with color coding. Red links are marked for deletion, green links are marked for addition and yellow links indicate that an attribute of the link has changed. If you notice at this point that you have made an error, click **Back** or **Cancel** to undo the proposed changes.
5. Right-click a link to change its link order, to remove it, or to set other properties.
6. Click **Finish**.

To replace links

1. Expand the node containing the GPO that you wish to manage and select it, then right-click the GPO and select **Search and Replace**.
2. To replace the links to the SOMs, select **Replace**.

   You will be asked to select the second GPO in the next step.
3. Click **Next**.
4. Expand the tree to select the replacement GPO, then click **Next**.

   The **Review Links** panel now shows you the links with color coding. Red links are marked for deletion, green links are marked for addition and yellow links indicate that an attribute of the link has changed.If you notice at this point that you have made an error, click **Back** or **Cancel** to undo the proposed changes.
5. **Right-click** a link to change its link order, to remove it, or to set other properties.
6. Click **Finish**.

To remove links

1. Expand the node containing the GPO that you wish to manage and select it, then right-click the GPO and select **Search and Replace**.
2. To remove the links, select **Remove**.
3. Click **Next**.

   The **Review Links** panel now shows you the links with color coding. Red links are marked for deletion, green links are marked for addition and yellow links indicate that an attribute of the link has changed. If you notice at this point that you have made an error, click **Back** or **Cancel** to undo the proposed changes.
4. **Right-click** a link to change its link order, to remove it, or to set other properties.
5. Click **Finish**.

Linking GPOs to multiple Scopes of Management

If required, you can easily take existing registered GPOs and link them to any number of SOMs within your deployment.

NOTE: GPOADmin does not support cross-domain GPO linking; these links will appear as deleted. To achieve similar functionality, we recommend using GPO synchronization.

To link GPOs to multiple SOMs

1. Select two or more registered SOMs, right-click and choose **Apply Link**.
2. Click the browse button to open the Choose a Group Policy Object dialog.
3. Select the required GPO and click **OK**.

   By default, the links will be applied to all selected Scopes of Management. You can, however, select to remove the application for specific SOMs by clearing the individual check box.

   The way in which the link is applied is set through the available options:

   If the GPO is not currently linked to a SOM, the default settings are enabled:

   - Enabled: This settings reflects the setting in the Version Control Server properties.
   - Enforced: Not enforced.
   - Link Order: Append link order.

   If the GPO is currently linked to one of the selected SOMs, the existing settings for that SOM are displayed.

6. If required, you can change the individual options or use the top level check box to set the options for all the selected SOMs.

   NOTE: To set the link as a specific link order, uncheck the check box for the specified SOM under the Link Order column, set the required link order using the up and down arrow. If the link order is set to a higher number than the current link count, the link will be appended.

7. Once you have all your settings in place, click **OK**.

   When the link action completes, the results are displayed in the Link Results dialog. If any of the links failed or an SOM was skipped, an error message displays the details so that you can take corrective action.

Managing compliance issues automatically with remediation rules

You have the option to setup an automatic way to deal with objects that have become non-complaint due to a modification or deletion performed outside of GPOADmin.

By default, the remediation option is set to None (no automatic resolution) at the Version Control Root level. Any remediation option set at this level will filter down to all child objects and containers unless you have specifically configured them to override their parents settings.

Watcher Service requirements

- The Watcher service is required to perform the compliance remediation actions. If the service is not running all remediation settings will be ignored.
- If the Watcher service account is not the same account as the GPOADmin service, it must be added to GPOADmin as and Administrative account.
- Remediation is not support on Protected Settings policies and WMI Filters as these objects are not monitored by the Watcher service.

To configure compliance remediation

NOTE: Only users with the Set Remediation Rule can set these options.

1. Right-click the required object or container and select **Properties**.
2. Select the **Remediation** tab and choose how you want to handle objects that have become non-compliant due to a modification or deletion.

If an object has become non-compliant due to:	Available options to resolve the compliance issue
Modification **NOTE:** Rollback with links and restore with links only apply to GPOs. All other objects will perform either a rollback or a restore remediation action.	• Rollback • Rollback with links • Incorporate live • Unregister
Deletion **NOTE:** Restore and Restore with links remediation is not supported on Scopes of Management.	• Restore • Restore with links • Unregister

3. Click **OK**. Once a rule has been set it will be applied when the object is flagged as non-compliant. If the object does not have a remediation rule applied then the first rule found on a parent container will be applied.

Validating GPOs

To ensure that the GPOs within your system are still required, you can setup an attestation process. If a GPO has not been deployed within the specified date range, an email will be sent to the account designated as its manager to attest to its validity. This option is supported for SQL and AD / AD LDS as a configuration store and all backup stores.

Administrators can also attest to the validity of a GPO without having to re-deploy it. An email, which includes a Settings report, is sent when the GPO is attested or when the attestation date has expired.

To configure GPO attestation

1. Right-click the required object or container and select **Properties**.
2. Select the **Attestation** tab.
3. Select **Enable Attestation**.
4. Set the date range (days, weeks, or months) for a GPO deployment that when exceeded will trigger a notification.
5. Enter the email notification subject and message.

   You can right-click and select **Insert Tag** to use any of the following pre-defined tags: Action, Comment, Domain Name, Full Path, ID, Last Backup ID, Name, Status, Sub status, Trustee Name, Trustee SID, Type, Version, Version Control ID, Last Deployed On. (See Predefined Tags for tag details.)
6. Click **OK**.

   The version control system is polled every 24 hours to identify GPOs that have not been deployed within the specified date range. Once identified, the attestaion email notification is sent to the account that is designated as its manager (Managed By property).

   NOTE: If you have GPOs that you do not want to validate, you can select to **Override Inherited Attesatation** and click to clear the **Enable Attestation** option.

To attest to the validity of GPOs without re-deploying it

NOTE: Only GPOADmin administrators and GPO managers (account specified in the Managed By field) can attest a GPO and only if attestation is enabled for that GPO.

1. Right-click the required object or container and select **Attest**.
2. Enter a comment and click **OK**.

   The attestation properties (Last attested date, Last attested by, and Attestation Due date) are found on the GPO General properties tab.

   The Attest action is also included in the GPO's history.

To attest GPOs through email

1. Ensure the **Enable Workflow Approval through email** or **Enable Workflow Approval through Gmail** option has been configured by the administrator. See Configuring the Version Control server.
2. Ensure the **Enable Attestation for Group Policy Objects** option has been configured either on the GPOs or on the container and that the **GPOs Managed By** property is set to either a mail-enabled account or a valid email address.

   Attesters will receive an email with the specified subject line and message. The email contains a Settings report that can be reviewed before making a decision.
3. Click the **Attest** button in the received email and enter a comment as the body of the new email message to perform the attestation for the GPO.

Managing GPO revisions with lineage

If required, you can manage GPO revisions through lineage by selecting a specific GPO to revert to when a rollback is performed. When this is configured, every SOM linked to the GPO will be updated the lineage GPO.

NOTE: Only users with the Set Lineage right can set the lineage.

To configure GPO lineage

1. Right-click the GPO that you want to manage and select **Properties**.
2. Select the **Lineage** tab and choose **Enable Lineage**.
3. Select the browse button and choose the GPO to revert to when a rollback is performed.
4. Click **OK**. Once this is set, a GPO rollback will unlink the GPO and re-link with the assigned lineage GPO.

Setting the change window for specific actions

If required, administrators can restrict specific actions during a specified day and time. For example, if a user checks out an object during the time period where changes are not permitted, all the management options will be unavailable.

NOTE: Only users with the Modify Change Window right can set the change window time frame.

NOTE: Administrators with the Modify Change Window right can override this option and make changes outside the allowable change window.

NOTE: PowerShell commands are not available for this feature.

To set the change window for specific actions:

1. Right-click the object that you want to manage and select **Properties**.
2. Select the **Change Window** tab.

If you are an administrator with the appropriate right, the **Override parent settings** option is enabled so that you can set the change window.

3 Select the **Time Setting** tab to set time frames individually (or select and drag to highlight the required time frame) and choose **Denied** or **Allowed** as required. Allowed hours display in blue, and denied hours display in white.

   Alternatively, you can:

   - Select to allow all, then deny specific days or a combination of days and hours.
   - Select to deny all, then allow specific days or a combination of days and hours.

4 Select the **Actions List** tab to select the actions to associate with this change window.

5 Click **Apply** to apply the settings and close the dialog.

   Once set, users will not be able to modify objects outside of the allowed change window.

Working with registered objects

Regardless of the status of the registered GPO, starter GPOS, scripts, DSC scripts, WMI filter, domain, site, or OU (Available, Checked Out, Pending Approval, and Pending Deployment), you can perform the following tasks if you have the appropriate role:

- Creating labels
- Cloaking a GPO (applies to available GPOs only)
- Locking a GPO (applies to available GPOs only)
- Establishing Management for an Object
- Viewing history
- Deleting version history
- Clearing account names in version history
- Viewing and editing object properties
- Applying keywords on containers
- Creating a report

NOTE: You can view a list of all registered objects in the All Managed Objects in the Search Folders in the GPOADmin console.

NOTE: The Starter GPOs folder is not created by default. To create the Starter GPOs folder, open Group Policy Manager, expand the required **Domain | Starter GPOs**, and click **Create Starter GPOs Folder**.|

Creating labels

You can include user-defined history comments (labels) on objects and containers in the Version Control system. This functionality allows users to rollback to an object identified by a specific label.

To create a label using the GPOADmin console

1 Expand the **Version Control Root** node, and select an object.

2 Right-click and select **Label**.

3 Enter the label in the Comment dialog box and click **OK**.

To create a label for a GPO using the GPMC Extension

1 Select the GPO and click **Workflow | Label**.

2 Enter the label in the Comment dialog box and click **OK**.

Cloaking a GPO

Cloaking allows you to hide Group Policy Objects (GPOs) from other users. The Cloaking role is not a default role installed with the product, and must be created with the Cloak/Uncloak and View Cloaked rights. By default, Domain Administrators can see all cloaked GPOs.

When a GPO is cloaked using GPOADmin, it is also cloaked in the live environment. Only users with the Cloak/Uncloak or View Cloaked right can see the GPO in the live environment. A cloaked GPO will only be applied to users who have the Cloak/Uncloak or View Cloaked right during group policy processing. All other users will no longer have the GPO applied.

Cloaked GPOs are indicated by a lighter GPO icon.

To cloak a GPO using the GPOADmin console

1 Select the GPO you want to cloak from the list of GPOs within the Version Control Root node.

2 Right-click and select **Cloak**.

Cloaked GPOs are displayed in the Cloaked search folder. Enter a comment and click **OK**.

NOTE: Users can also have the View Cloaked right only. This means that they can see cloaked GPOs but do not have permission to "uncloak" them. Cloaked GPOs can be viewed in the Search Folders in the GPOADmin console.

To cloak a GPO using the GPMC Extension

1 Select the GPO you want to cloak from the list of GPOs and click **Cloak**.

2 Enter a comment and click **OK**.

Locking a GPO

Locking allows you to lock a policy so other users cannot edit it. The Locking role has to be created and consists of the Lock/Unlock right. For example, you may choose to lock the Default Domain Policy and/or Default Domain Controller Policy as any modification to these settings would affect every GPO in the organization.

When a GPO is locked using GPOADmin, it is also locked in the live environment. All users can see the GPO, but no one can edit it.

By default, Domain Administrators can see all locked GPOs and unlock any locked GPO. Locked GPOs are indicated by a lock icon.

NOTE: Only GPOs can be locked. (You cannot lock WMI Filters or Scopes of Management).

To lock a GPO using the GPOADmin console

1 Select the GPO you want to lock from the list of GPOs within the Version Control Root node.

2 Right-click and select **Lock**.

Locked GPOs are displayed in the Locked search folder.

NOTE: When a user with the right to lock GPOs connects to the GPOADmin console, they will see all locked GPOs. A Locked GPO must be unlocked before any actions can be performed (even if you are a system administrator.) Locked GPOs can be viewed in the Search Folders in the GPOADmin console.

3 Enter a comment and click **OK**.

To lock a GPO using the GPMC Extension

1 Select the GPO you want to lock from the list of GPOs and click **Lock**.

2 Enter a comment and click **OK**.

Establishing Management for an Object

If you have the Modify Managed By right, you can set the user responsible for an object's management.

NOTE: The Managed By property is a textual field which can be used to sort objects by and as no affect on the objects security.

To set or change the user responsible for an object's management

1 Expand the **Version Control Root** node, and select an object.

2 Right-click and select **Managed By**.

3 Enter or browse for the required account and click **OK**.

You can also assign management on a container by right-clicking on it an selecting Properties and selecting the required account.

NOTE: Any child containers or objects below this container that do not have a managed assigned to them will automatically use this one.

Viewing history

You can easily create a report that displays the historical settings for objects in the Version Control system or a comparison of versions. When you view the history in the GPMC Extension, all events are shown. The GPOADmin console has a filter option that you can use to choose which events to display.

To view the history using the GPOADmin console

1 Expand the **Version Control Root** node, and the required container.

2 Right-click an object and select **Show History**.

3 Select a version in the list.

4 Select which, if any, filtering options you would like to apply, then right-click, and select **View** to view the historical information.

5 To view the difference between various check ins, select the required versions, right-click and select **Differences**.

6 Click **Print** to print the report.

Click **Save As** to save the report in HTML.

7 Click **Close**.

NOTE: You can also restore links between a GPO and its Scopes of Management from the history view. For more information, see Restoring links to a previous version on page 72.

To view the history using the GPMC Extension

1 Select the GPO and click **Show History**.

The history displays in the bottom pane of the GPO Management tab. You will see the name, version, action, account, date and comment pertaining to the history item.

2 To view the difference between various check ins, select the required versions, right-click and select **Differences**.

3 Click **Print** to print the report.

Click **Save As** to save the report in HTML.

4 Click **Close**.

For more information on the available reports, see Creating Reports on page 107.

Deleting version history

As you progress an object through the Version Control workflow, GPOADmin keeps an audit trail, as well as a history of all minor and major versions. If you no longer need to keep this history, you can selectively delete any of the versions except your last backup. Only the object settings are deleted; the audit trail is preserved, and you still see the entry in the object history. Deletions are permanent.

If required, you can select to remove the user account associated with the action from the view.

NOTE: When a new version is created, an internal record of the action that generated the version is kept—including the user that performed the action, the date and a label if one was created. You may wish to view this audit trail in a History report before deciding which versions you want to delete. For more information, see Historical Settings Reports on page 124.

To delete version history in the console

1. Expand the **Version Control Root** node, and the required container.
2. Right-click an object and select **Show History**.
3. In the **History** dialog box, select a version from the list. (Press **CTRL** and click to select multiple versions.)

   You can only delete major and minor versions. If you have Show All Events enabled, events that have occurred between versions cannot be deleted, as there are no settings associated with them.
4. Right-click and then select:

   Delete: This will delete the backup associated with the action.

   Delete and Clear Account: This deletes the backup and clears the account name associated with the action.
5. In the confirmation dialog box, click **OK**.

   After you delete a version history, it remains on the list, but is unavailable.

NOTE: Once you have deleted version history, it cannot be undone.

To delete version history of a GPO using the GPMC Extension

1. Select the GPO and click **Show History**.
2. In the bottom pane, select a version. (Press **CTRL** and click to select multiple versions.)

   You can only delete major and minor versions. Events that have occurred between versions cannot be deleted, as there are no settings associated with them.
3. **Select Delete to** remove the backup associated with the action.

   -OR-

   Delete and Clear Account to remove the backup and clear the account name associated with the action.
4. In the confirmation dialog box, click **OK**.

Clearing account names in version history

If required, you can remove the user account associated with a backup version from the historical view.

To clear the account name

1. Expand the **Version Control Root** node, and the required container.
2. Right-click an object and select **Show History**.
3. In the **History** dialog box, select a version from the list. (Press **CTRL** and click to select multiple versions.)

4 Right-click and then select **Clear Account**.

5 In the confirmation dialog box, click **OK**.

To clear the account name associated with an action using the GPMC Extension

1 Select the GPO and click **Show History**.

2 In the bottom pane, select a version. (Press **CTRL** and click to select multiple versions.)

3 Right-click and then select **Clear Account**.

4 In the confirmation dialog box, click **OK**.

Viewing and editing object properties

You can easily view and edit the details for the current version of an object in the Version Control system including the security, notification settings, keywords, approvals, lineage, remediation options, as well as the object's location within version control.

You can also view important information about changes made in the live environment on the Change Auditor tab, if you have a supported version of Change Auditor. See the Release Notes for a complete list of supported versions.

NOTE: Users with the appropriate permission can alter the security settings. For more information, see Configuring role-based delegation on page 38.

To view and edit the properties using the GPOADmin console

1 Expand the **Version Control Root** node, and the required container.

2 Right-click the required object and select **Properties**.

3 From the Properties dialog box, click the required tab to see the associated information.

Table 14. Options

Option	Description
General	View the domain, user, the creation and modification dates, the version, the unique ID, location in version control, and the GPO status. From here you can also see and, if required, change the user responsible for an object's management (Managed By property).
Links (From the GPO Properties page)	Edit the link to Scopes of Management. **NOTE:** You must have the Link permission to add or edit links.
Lineage	Manage GPO revisions by selecting a specific GPO to revert to when a rollback is performed.
Security	Delegate responsibilities over the object.
Policy Baseline	Assign a policy baseline to a policy and monitor the policy for deviations from the baseline.
Approvals	Approval workflows for object creation, deletion, or modification. **NOTE:** Users who have the Enable / Disable Approvals right can enable and disable approvals for containers or specific objects. **NOTE:** Approvals are inherited from the parent unless manually set on the object. (Explicitly applied settings take precedence over inheritance.) By default, approvals are processed in the order listed on the Approvals tab in the Container or Item Properties. **NOTE:** Click the **Override inherited work flow** check box if you want the approvals process for a container to be different from its top level container.
Link Source	Restrict linking by including only policies from specific containers.
Notifications	Select the actions to be notified on.

Table 14. Options

Option	Description
Remediation	Manage which action will occur automatically when an object becomes non-complaint due to an edit or deletion performed outside of GPOADmin.
Change Window	Set the day and time when users can make modifications to objects.
Attestation	Set the date range limit for a GPO deployment and configure the notification message that is sent when the limit is surpassed The version control system is polled every 24 hours to identify GPOs that have not been deployed within the specified date range. Once identified, the attestation email notification is sent to the account that is designated as its manager (Managed By property).
Keywords	View all the keywords for a given object. For here you can also, add and remove keywords as required. When a new keyword is entered it is saved into a primary list of keywords. This list is displayed for each object. The checkboxes indicate which keywords are applied to each object.
Group Policy Inheritance	View the group policy inheritance for the selected Scope of Management. including the location where they are linked and the order in which they will be applied.
Change Auditor	View changes made to objects in the live environment. You can move the columns and sort by columns. **NOTE:** You must have a supported version of Change Auditor installed. See the Release Notes for a complete list of supported versions. You can also view and save a report of changes. For information, see Change Auditor Report on page 113.
Naming Standards **NOTE:** Items with a backslash or forward slash in the name will not manageable in PowerShell. **NOTE:** Items with an astrix in the name must inclose the name in single quotes and escape the astrix using the backtick character (character below the tilde). For example: Item Name: Test * Escaped: 'Test `*'	Select to enforce naming conventions for GPOs and WMI filters. Enter the rule, a test name, and click **Verify** to ensure its accuracy. **NOTE:** Any existing naming conventions previously set, will be migrated to the Version Control root container during an upgrade. **Example rule:** ^[a-z]+[0-9]+_GPO$ • The caret character (^) means the start of the line. • The grouping [a-z]+ means at least one or more lower-case characters between a and z. • The grouping [0-9]+ means at least one or more numeric characters between 0 and 9. • The dollar sign character ($) means the end of the line. This rule states that from the start of the line there must be at least one or more lower-case characters immediately followed by at least one or more numeric characters immediately followed by the literal string “_GPO” and nothing after that. a1_GPO passes abc123_GPO passes _a1_GPO fails a1_GPO_ fails A1_GPO fails A1_gpo fails

To view the properties using the GPMC Extension

1 Right-click the GPO and select **Properties**.

2 From the Properties dialog box, click the required tab to see the associated information.

Table 15. Options

Option	Description
General	View the domain, user, the creation and modification dates, the version, the unique ID, location in version control, and the GPO status. From here you can also see and, if required, change the user responsible for an object's management (Managed By property).
Links (From the GPO Properties page)	Edit the link to Scopes of Management. **NOTE:** You must have the Link permission to add or edit links.
Lineage	Manage GPO revisions by selecting a specific GPO to revert to when a rollback is performed.
Security	Delegate responsibilities over the object.
Approvals	Number of required approvers for object creation, deletion, or modification. **NOTE:** Users who have the Enable / Disable Approvals right can enable and disable approvals for containers or specific objects. If approvals are enabled but the parents value is disabled, then inheritance stops at the parent. If approvals are disabled, then the workflow goes directly from check-in to deploy.
Notifications	Select the actions to be notified on.
Remediation	Manage which action will occur automatically when an object becomes non-complaint due to an edit or deletion performed outside of GPOADmin.
Keywords	View all the keywords for a given object. For here you can also, add and remove keywords as required. When a new keyword is entered it is saved into a primary list of keywords. This list is displayed for each object. The checkboxes indicate which keywords are applied to each object.
Change Auditor	View changes made to objects in the live environment. You can move the columns and sort by columns. **NOTE:** You must have a supported version of Change Auditor installed. See the Release Notes for a complete list of supported versions. **NOTE:** You can also view and save a report of changes. For information, see Change Auditor Report on page 113.

Applying keywords on containers

To ease the management of containers, you can now set keywords on them, locate them in the Search Folders based on those keywords, and edit their properties once they have been found.

NOTE: This option is only available for SQL configuration stores.

To set a keyword on a container:

1 Expand the **Version Control Root** node, and the required container.

2 Right-click the required object and select **Properties**.

3 From the Properties dialog box, click the **Keywords** tab.

4 Add and remove keywords as needed.

5 If required, you can block the inheritance on child containers and objects.

6 Click **Apply** to save the changes and close the dialog.

To search for containers based off applied keywords:

1. Expand **Search Folders** and open the **Containers** folder.
2. To filter the view, type the keywords to search or select the keywords from the drop down list, and click **Search**.
3. Right-click the required container and select **Properties** to view and edit the details for the current version of the container in the Version Control system.

Creating a report

You can create reports that show the details of controlled objects, as well as diagnostic and troubleshooting information. For more information on the available reports, see Creating Reports on page 107.

Working with available objects

With available objects, you can perform all the supported tasks of registered objects (Show history, view live reports, view properties, unregister, create labels, and import/export), as well as:

- Enabling/disabling workflow
- Checking out objects
- Requesting the deletion of an object
- Unregistering GPOs and removing history
- Requesting approval

NOTE: You can view a list of all Available objects in the Search Folders in the GPOADmin console.

Enabling/disabling workflow

If you have the Enable/Disable right, you can enable and disable the workflow for a deployed object. The object must be under version control and be a major version (for example, 2.0).

NOTE:

- To work with and edit workflow-disabled GPOs, you must have the GPMC Edit, Delete, and Modify Security right as well as the DeleteSubtree right.
- You can view a list of workflow-enabled or workflow-disabled objects in the Search Folders in the GPOADmin console.
- If you disable the workflow, any changes made are immediately deployed in the live environment. To bring the object back under version control, enable the workflow.
- When managing objects across forests, they must be workflow enabled.
- You can enable and disable workflow on objects through a remote console. However, once they are disabled, they cannot be managed through the remote console.

To enable/disable workflow in the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click a major version of an available object and select **Disable Workflow**.

   -OR-

   Right-click an object that is not workflow enabled and select **Enable Workflow**.
3. Enter a comment and click **OK**.

To enable/disable workflow in the GPMC Extension

1. Select a major version of an available object and click **Workflow | Disable Workflow**.

   -OR-

   Select an object that is not workflow enabled and click **Workflow | Enable Workflow**.

2. Enter a comment and click **OK**.

Checking out objects

Before users can edit registered objects, they must be checked out. The workflow is as follows: Check-out the object from the system, make the required edits, and check in the changes to the system.

Checking out an object for the first time creates a copy of the original live version.

NOTE: The changes are only applied to the live enterprise when they are approved by users included in the approval workflow and deployed by users with the Deploy permission.

NOTE: To edit the GPO working copy, users must have the GPMC edit right. If they do not have this right, it will be granted during checkout.

During check in, the edit right will be removed. This ensures that the user does not gain the edit right on the live GPO during the deployment process.

If you have the Modify System-Provided Security right, refrain from modifying the granted Edit right. Allow the system to remove it during the check-in process.

Version information is updated in the system's history when the object is checked back in. Only one person within the system can check out and work on any object at a given time.

NOTE: If you have all required rights, you can approve and deploy an object from the checked out state and all workflow steps happen automatically.

NOTE: You can view a list of checked out objects in the Checked Out or Checked Out to Me Search Folders in the GPOADmin console.

To check out an object using the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click an object in the Available state and select **Check Out**.
3. Enter a comment and click **OK**.

NOTE: When a GPO is checked out only the settings are maintained — not the GPO links. You can check out multiple GPOs at once.

To check out a GPO using the GPMC Extension

1. Select an available GPO and click **Workflow | Checkout**.
2. Enter a comment and click **OK**.

Requesting the deletion of an object

Users can propose the deletion of objects in the enterprise environment that are currently registered in the Version Control system and in the Available state. If the request is approved, the object will be removed from the system and deleted from the live environment.

NOTE:

- If you simply want to remove the object from the Version Control system (not the live environment), unregister it. For more information on unregistering objects, see Removing registered objects on page 63.
- You can view a list of Deleted objects in the Search Folders in the GPOADmin console.

To delete an object using the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click the required object and select **Delete**.
3. Enter a comment and click **OK**.

   The object is now in the Pending Approval state.

NOTE: Objects with a version number of 0.0 can be deleted by the user who created them.

To delete a GPO in the GPMC Extension

1. Right-click the GPO and select **Delete**.
2. Enter a comment and click **OK**.

Unregistering GPOs and removing history

You can select to permanently unregister a GPO and remove any associated metadata from the configuration store.

To unregister a GPO and remove history

1. Expand the **Version Control Root** node and the required container.
2. Right-click the required object and select **Unregister and remove history**.

Requesting approval

Once an object has been altered and checked in to the system, the update is ready to go through the approval process. (For more information on checking in objects, see Checking in controlled objects on page 87.)

To request approval using the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click the altered object and select **Request Approval.**
3. Enter a comment and click **OK**.

   The object will now be in the Pending Approval state.

To request approval using the GPMC Extension

1. Select the altered GPO and click **Workflow | Request Approval**.
2. Enter a comment and click **OK**.

Working with checked out objects

With checked out objects, you can perform all the tasks of registered objects (Show history, view live reports, view properties, unregister, create labels, and import/export), as well as:

- Undoing a check out
- Checking in controlled objects

NOTE: If you have all required rights, you can approve and deploy an object from the checked out state and all workflow steps happen automatically.

Undoing a check out

The user who checked out an object has the option of undoing the check out and reverting the state back to Available.

To undo a check out

1. Expand the **Version Control Root** node and the required container.
2. Right-click the object and select **Undo Check Out**.
3. Enter a comment and click **OK**.

To undo a checkout in the GPMC Extension

1. Select the checked out GPO and click **Workflow | Undo Check Out**.
2. Enter a comment and click **OK**.

NOTE: If you undo a check out of an object with a version 0.0, the working copy will be deleted and there will be no record of the object in the Version Control System.

Checking in controlled objects

Once you have checked out an object and edited its settings (for more information, see Editing objects on page 95), you have the option to:

- Check in objects in their temporary state for further updates
- Check in objects and notify Approvers that it is ready to be approved or rejected (For more information, see Requesting approval on page 86.)
- Undo the check out (For more information, see Undoing a check out on page 87.)

A check in updates the history of the object within the Version Control system with the changes made while it was checked out. Included with any check-in is a comment and a unique minor version number (such as 1.1).

A check in does not allow the offline changes to go live into the enterprise environment as it must first be approved. Once an object is marked as Pending Approval, it cannot be checked out by any other user of the system.

Multiple check in and check outs are allowed to occur within the system without requiring approval. When a user checks in an object so it is available to another system user, the next user to check out the same object will be working with the current offline version consisting of all changes made to date. After all the users have made their required changes to the offline object it is processed by the approval system to determine if the changes are accepted to go live into the enterprise or not.

To check in an object using the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click an object and select **Check In**.
3. Enter a comment if required and click **OK**.

If the GPO settings are flagged as being protected, users with the Modify Protected Settings right on the GPO in question, have the option to continue with the check in and override the blocked setting or review a report and address the issue. For details on protected settings, see Working with Protected Settings policies.

4 Right-click and select **Request Approval** if required. Enter a comment and click **OK**.

To check in a GPO using the GPMC Extension

1 Select the GPO and click **Workflow | Check In**.

2 Enter a comment if required and click **OK**.

3 Click **Workflow | Request Approval** if required. Enter a comment and click **OK**.

Working with objects pending approval and deployment

Only users with the Deploy permission can make the changes go live in the enterprise. The approval system safeguards the enterprise environment from any unauthorized live changes that could cause unwanted results. For more information on delegating permissions, see Configuring role-based delegation.

The types of requests from users that require approval are

- Changes to offline objects that are required to go live
- Creation of new objects
- Deletion of existing objects

NOTE: Using the Export Wizard, you can test GPOs offline before they are implemented in the live enterprise. For more information, see Exporting and importing on page 103.

NOTE: You can view a list of all objects Pending Deployment or Approval in the Search Folders in the GPOADmin console.

For more information, see:

- Enhanced workflow approval
- Changing the approval workflow
- Withdrawing an approval request
- Approving and rejecting edits
- Deploying objects (scheduling and associated items)

NOTE: User or groups added as an approver must have Read access on the object requiring approval. Validate and set the appropriate access through the Security tab.

Withdrawing an approval request

Any user who proposes a change to an object can withdraw their own request for approval while the change is in the Pending Approval state.

To withdraw an approval request in the GPOADmin console

1 Right-click an object in the Pending Approval state, and select **Withdraw Approval Request**.

2 Click **OK**.

The object is returned to the Available state.

3 Enter a comment and click **OK**.

To withdraw an approval request in the GPMC Extension

1. Select a GPO in the Pending Approval state, and click **Workflow | Withdraw Approval Request**.
2. Enter a comment and click **OK**.

Enhanced workflow approval

You have the option of implementing a further safeguard by designating and modifying multi-level approvers. With this option, the required approvals at all levels must be granted before an object becomes available for deployment in the live environment.

Not everyone in a named group has to approve, just the required number. For example there may be 10 members in Group B but we may require only 3 approvals from that group to satisfy our requirements.

When you create a role within GPOADmin, you now have the option of empowering that role with the **Modify Approval Workflow** permission.

To grant Modify Approval Workflow permission

1. Select the forest node, right-click and select **Properties.**
2. Open the **Roles** tab and select **Add New Role**.
3. Type the name of the new role and click **Next.**
4. Scroll down the list of permissions and select the **Modify Approval Workflow** check box.
5. Once you have granted all relevant permissions, click **Finish**, click **Apply** and then **OK**.

NOTE: You can view an existing role's rights by selecting the role, selecting **View Role**, opening the **Rights** tab, and noting the permissions that have been grated.

Use caution granting this permission. A user with this permission can add, modify or delete the approval workflow a requested change must follow before it modifies the live environment.

Changing the approval workflow

By default, approvals are processed in the order listed on the Approvals tab in the Container or Item Properties. Optionally, approvals can be performed base on count where the any approver can approve at any time. In this case, the item status will change to Pending Deployment once the total number of received approvals equals the total sum of the required approvals.

NOTE: You can select the **Override inherited work flow** check box if you want the approvals process for a container to be different from its top level container.

To change an approval workflow

1. Select a version control container or object, right-click and select **Properties.**
2. Open the **Approvals** tab and select the workflow type you want to manage.

   Approval workflows can be set for object creations, deletions, and modifications.

To add a level of approval

1. Click **Add** to select a user or group.
2. Use the arrow keys to the left of the dialog box to alter the order in which the approvals must take place.

   If a group is selected, you must specify how many members of that group must approve the item before it can proceed to the next stage.
3. Once you have all steps added to the new workflow, click **Apply**, then **OK**.

To delete a level of approval

1 Click the "**-**" button to the right of the level of approval you do not want.

NOTE: Be certain you want to remove the level as there is no step to ensure you have chosen the correct level - it is removed as soon as you click on the "-" button.

2 Use the arrow keys to the left of the dialog box to alter the order in which the approvals must take place.

3 Once you have all steps added to the new workflow, click **Apply**, then **OK**.

To modify a level of approval

1 Follow the steps above to add or delete steps in the workflow.

2 Where you have selected a group as part of the approval workflow, you can change the value in the Approval Count Window to modify the number of members of that group who must agree to the change before it proceeds to the next level of approval.

3 Use the arrow keys to the left of the dialog box to alter the order in which the approvals must take place.

The approvals will be handled from top to bottom of the displayed table.

4 Once you have modified the workflow, click **Apply**, then **OK**.

Withdrawing approval

Before the final approval has been made and the changes have been deployed, any approver has the right to withdraw their approval. When any approval is withdrawn, the process begins again from the start.

Approving and rejecting edits

Once an object has been checked in and the Approver has been notified that the offline changes are ready for approval, the changes are either approved or rejected.

NOTE: Before the approval of a change takes effect, the Version Control system detects if an object was changed unknowingly or outside the scope of the system and prompts the approver with the appropriate action to take. They can choose to overwrite the object or leave it as is.

Table 16. Approving Changes

If the changes are approved and deployed	If the changes are rejected
• The settings are applied to the live object and its major version number is incremented. (For example, v2.0) • The settings from the offline object are applied to the live object. • The next time a check out occurs, the process repeats of creating a new offline copy of the live group policy object.	• Nothing happens and the status is set back to an available state so it can be checked out again. **NOTE:** If the changes are only approved but not deployed, their status is changed to Pending Deployment and those GPOs can be seen in the Pending Deployment search folder.

To approve edits in the GPOADmin console

1 Expand the **Version Control Root** node, and the required container.

2 Right-click a controlled object in the Pending Approval state, and select **Approve**.

3 Enter a comment and click **OK**.

If you have the required permission, you can deploy the updates to the enterprise at this time. If not, the object will be set to the Pending Deployment state. For information on deploying objects, see Deploying objects (scheduling and associated items) on page 91.

To approve edits in the GPMC Extension

1. Click the GPO in the Pending Approval state, and click **Workflow | Approve**.
2. Enter a comment and click **OK**.

To approve or reject edits through email

1. If this option has been configured by the administrator (see Configuring the Version Control server), approvers will receive an email with the subject line “Approval Request Notification”.

   The email contains a Settings report that you can review before making your decision.
2. Click to **Approve** or **Reject** and enter a comment as the body of the new email message to perform the selected action for the requested changes.

To reject edits in the GPOADmin console

1. Expand the **Version Control Root** node, and the required container.
2. Right-click a controlled object in the Pending Approval state, and select **Reject**.
3. Enter a comment, and click **OK**.

To reject edits in the GPMC Extension

1. Right-click the GPO in the Pending Approval state, and click **Workflow | Reject**.
2. Enter a comment, and click **OK**.

Deploying objects (scheduling and associated items)

Deploying changes within the system is a critical process that affects the live environment. To minimize the impact of disruption, this process should be done during a time period when the impact to users is minimal as the changes may alter the behavior of particular systems.

To reduce any issues, you can schedule the deployment of the changes for a specific date and time that best suits your needs. You can also schedule a deployment based on a different time zone, for example if the client is not in the same time zone as the server and you want to deploy based on the client’s time zone.

If you have multiple approvers:

- Scheduling will only be available during the final approval and deployment.
- If the scheduled approval fails due to non-compliance or for any other reason, the Deployer will be notified.
- Only the Deployer can cancel the scheduled deployment.

NOTE: Before you deploy a GPO, ensure that it is not cloaked. If you deploy a cloaked GPO, and then later deploy it uncloaked, it will be flagged as noncompliant.

During the deployment of an object, you have the option to identify and deploy any associated items (in the pending deployment state). When the associated objects are deployed they are subject to all regular compliance checks (including security checks).

NOTE: This availability of the associated items option must be configured on the server by the administrator. For details, Configuring the Version Control server.

To deploy an approved object using the GPOADmin console

1. Expand the **Version Control Root** node, and the required container.
2. Right-click an object in the Approved state, and select **Deploy**.
3. Enter a comment.
4. Select the deployment time frame.

You have the option to deploy the changes immediately or at a specified time.

NOTE: To synchronize during an immediate deployment (a non-scheduled deployment), the user deploying the GPO must have the Synchronize right.

If you select Schedule deployment for a later date, set the date and time, select an appropriate time zone if required, enter a comment, and click **OK**.

After you have scheduled a time, a clock icon appears beside the object and the Deployment Time column reflects the scheduled deployment in UTC.

NOTE: If a scheduled deployment fails for any reason, the deployment is canceled and the object remains in the Pending Deployment state.

You now have the option to identify and deploy associated items.

5 Enable the **Identify associated items** option to see a list of all associated pending deployment items that you have Read access to.

Any items that you do not have access to and can therefore not deploy, will display in grayed out text.

6 Enable the **Deploy associated items** option to deploy the associated items.

NOTE: You must have been delegated the Deploy right on the associated items to deploy them.

NOTE: If this is a scheduled deployment, all associated objects in a pending deployment state will be deployed even if the scheduling user does not has the rights to deploy them. In this case, the service account will be doing the deployment and it will have the required rights to all objects.

To deploy an approved GPO using the GPMC Extension

You can only deploy GPOs using the GPMC Extension. To deploy SOMs or WMI filters, use the GPOADmin console.

1 Select the approved GPO and click **Workflow | Deploy**.

2 Enter a comment.

3 Select the deployment time frame, including a time zone if required, and click **OK**.

To reschedule a deployment using the GPOADmin console

1 Right-click the required controlled object and select **Deploy**.

2 Select the date and time, select an appropriate time zone if required, enter a comment, and click **OK**.

To reschedule a deployment using the GPMC Extension:

1 Select the GPO and click **Workflow | Deploy**.

2 Select the date and time, select an appropriate time zone if required, enter a comment, and click **OK**.

To cancel a deployment using the GPOADmin console

- Right-click an object in the Pending Deployment state and choose **Cancel Deployment.**

  Right-click an object in the Pending Deployment state and choose **Deploy**. Select **Cancel pending deployment**.

To cancel a deployment using the GPMC Extension

- Select the GPO in the Pending Deployment state and click **Workflow | Cancel Deployment.**

  Select the GPO in the Pending Deployment state and click **Workflow | Deploy,** then select **Cancel pending deployment**.

Checking compliance

GPOADmin provides two options to determine if an object has been changed outside the scope of the system in the live enterprise environment. You can manually check any object for compliance (GPOs, Scopes of Management, scripts, DSC scripts, Intune objects, and WMI filters), and you can let the GPOADmin Watcher Service detect unauthorized modifications to objects. For more information on configuring the Watcher service, see the GPOADmin Quick Start Guide.

If you are running the Watcher Service, non compliant objects are automatically flagged with a yellow exclamation point, regardless of their status.

NOTE: To ensure that you are notified immediately of non compliant objects, ensure that the Watcher Service is running.

NOTE: You can view a list of all objects that have been flagged as non compliant in the Unauthorized Modifications Search Folder in the GPOADmin console.

NOTE: When the Watcher Service detects a non compliant object under version control, it creates a backup of the change and increases the minor version number by one. If the non compliant object is workflow disabled, it creates a backup of the change and increases the major version number by one. For details on enabling or disabling workflow, see Enabling/disabling workflow on page 84.

NOTE: DSC scripts are not monitored by the Watcher Service.

If a delta is determined between the last historical backup and the live object, a user with the appropriate permissions will be able to either:

- Roll back: Restore the object in the live environment from the most current backup found in the system to overwrite the unauthorized live change.
- Roll back with Links: Restore a Group Policy Object in the live environment from the most current backup, including its links to Scopes of Management, and overwrite the unauthorized live change.

IMPORTANT: If the GPO has lineage enabled, during a rollback the GPO lineage takes precedence. To see if lineage has been enabled and a hierarchal overview of the applied lineage, view the GPO properties.

For more information see, Validating GPOs on page 75.

You can also roll back links from a different history version. For information, see Restoring links to a previous version on page 72.

- Incorporate Live: Accept the live changes as being authorized and more up-to-date than what is currently already in the system. This will automatically back up those changes into the system and increment the version number of the backup to the next major number.
- Leave the live object alone in its noncompliant state.

NOTE: If the change to the live environment occurs while the GPO is checked out, when you check it in you can choose which version of the GPO to accept.

If an object has been deleted in the live environment, a user with the appropriate permissions will be able to:

- Restore the object in the live environment
- Restore a Group Policy Object in the live environment and restore its links to Scopes of Management.
- Unregister the object from the Version Control system

NOTE: If a SOM has been deleted, you will only have the option to Unregister.

To check if any registered objects have been changed since their last backup

1. Right-click the required object in the Available state and select **Check Compliance**.
2. Right-click the **Version Control Root** node or subcontainer, and select **Check Compliance**.

NOTE: If you are using the GPMC Extension you can select the GPO and click Workflow | Check Compliance.

3 Click **Next** to run the compliance check.

The objects that are not compliant are displayed.

4 Select the required course of action by clicking in the Action field to open the list of options, and click **Next**.

5 If you are restoring GPO links, select the **More** (**...**) button to see the details of the links you will be restoring.

In the Restore Links box, you can review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.

6 Click **OK** save the Restore Links settings.

7 Click **Finish**.

At this point the modified SOMs affected by the restored links, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

NOTE: If you attempt to deploy a noncompliant compliant GPO, you have the option of running the Compliance Wizard or proceeding with the deployment.

To make a flagged GPO compliant

1 Right-click the noncompliant GPO and choose one of the following

- Incorporate Live
- Rollback

If you choose Incorporate Live, you cannot restore links.

2 Enter a comment and click **OK**.

3 Select the **Restore GPO Links** option in the Comment box.

4 In the **Restore Links** box, review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.

Hover over a link to get more information. If a link has an exclamation mark beside it, the Scope of Management Object is not Available.

5 Click **OK** save the Restore Links settings.

At this point the modified SOMs affected by the restored links, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

To restore a deleted GPO with links

When a Group Policy Object is deleted in the live environment, its status shows as Noncompliant - Deleted in GPOADmin.

1 Right-click the noncompliant GPO and select **Restore**.

2 Select the **Restore GPO Links** option in the Comment box.

3 In the Restore Links box, review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.

Hover over a link to get more information. If a link has an exclamation mark beside it, the Scope of Management Object is not Available.

4 Click **OK** save the Restore Links settings. At this point the modified SOMs affected by the restored links, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

To exclude security modifications on Scopes of Management from the watcher service

If needed, you can use a registry key to prevent the watcher service from flagging a Scope of Management as non-compliant when modifying the security outside of GPAODmin.

If you select to enable this, you need to redeploy all registered scopes of management to ensure that security is either included or excluded (depending on the value) in the latest backup used to perform the comparison. If you do not redeploy the SOMs, they will be flagged as non-compliant.

1. Set the **ExcludeSOMSecurityFromHash** registry value to 1. By default this is set to 0.
2. Set this to the same value on all GPOADmin service hosts and the watcher service host that share a common configuration store.

   GPOADmin service key location: HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\VCConfig

   Watcher service key location: HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\WatcherConfig

NOTE: You will see the following event in the GPOADmin event log if the ExcludeSOMSecurityFromHash is set to 1: The Scope of Management '<distinguished name of the scope of management>' has been brought back into compliance.

This is a standard message displayed by the Watcher service when a change is made to a registered object. In this case, the compliance is not affected because the metadata for the live and stored objects has not been changed.

Editing objects

- Editing GPOs
- Editing Intune objects (Configuration profiles and Compliance policies)
- Editing WMI filters
- Editing scripts
- Linking GPOs

Editing GPOs

Once you have a GPO checked out, you can edit its settings within the Group Policy Editor, create security and WMI filters, and enable/disable computer and user settings.

NOTE: The editor will first attempt to be launched as the user logged into GPOADmin. If that fails, you need to select to Run As and specify credentials of a user who has access to GPMC.

Because you can only link GPOs to sites, domains, and OUs, setting up security filters helps you to refine the application of GPO settings to a group, user, or computer.

NOTE: The users and computers that you select while setting up security filtering must have both Read and Apply Group Policy (AGP) permissions on the GPO.

When you check out a GPO, the changes you make are to a copy of the live GPO. The changes that you make do not affect the GPO settings in the enterprise until it is approved and deployed.

To edit GPO settings

1. Right-click a checked out GPO, and select **Edit**.
2. Click **Launch Editor**, make the required changes, and close the Group Policy Editor.

   When you register GPOs, the GPO status (Enabled/Disabled Computer and User settings) will be maintained. However, if required, you can also easily change these settings from within the Version Control system.
3. Select or clear the user and computer setting options as required.
4. If required, select the Security tab and click **Add**, enter or search for the required user, computer, or group, and click OK.

To change the current security filters, select the required entry, and click **Remove**.

5 Click the **Advanced** button to select advanced permissions.

> **NOTE:** This option will only be available to those with the Administrator role or users who have been assigned both the Modify Security Filter and Modify System-Provided Security rights.

6 To link the GPO to a pre-existing WMI filter in the domain, select the WMI Filter tab and choose the filter from the list.

> **NOTE:** You will only see the filters you have permission to access.

Upon approval the link will be added to the GPO.

To remove any existing WMI filtering select **None.**

If the GPO was previously linked to a WMI filter, the GPO will be unlinked from the filter upon approval.

7 Click **OK**.

You now have the option to check in the GPO to be stored for later use or check in and request approval of the changes. See Checking in controlled objects on page 87 and Requesting approval on page 86 for more information.

Removing persistent registry settings

Some GPO settings create registry entries when they are processed. When these settings are removed and the policy is processed, their corresponding registry entries may not be removed from client computers.

GPOADmin notifies you when potentially persistent registry values exist and allows you to remove them.

> **NOTE:** Because this option removes registry data when the policy is processed, you must take care to ensure that you do not remove settings set by other policies.

To remove these settings

1 Right-click a checked out GPO, and select **Edit**.

2 Click the **Registry Cleanup** button.

The registry settings that persist as a result of removing GPO settings will display. Settings that are unavailable will never persist as the Group Policy processing engine resets these settings before processing the GPO.

3 Select the registry settings that you want to remove when the policy is re-processed, and click **OK**.

Editing Intune objects (Configuration profiles and Compliance policies)

Once you have a Intune objects checked out, you can edit its settings and select the user or device group to receive the profile and policies.

> **NOTE:**
> - See the Quick Start Guide for the required minimum permissions, rights, and roles.
> - GPOADmin does not support:
>   - iOS/iPadOS Security Assessment (Education) template from Intune Configuration profiles.
>   - Certificate references for Intune Configuration profiles.

To edit Intune objects and assignments

1 Right-click a checked out Intune object, and select **Edit**.

2 From the **Settings** tab, click **Launch Editor.**

3 Update the settings and save your changes. For information on assigning groups, refer to Microsoft documentation.

4 Select the **Assignments** tab to include and exclude users and device groups from the selected Intune object.

NOTE:

- The Modify Intune Assignments right is required to edit the Intune object assignment. For more information see Configuring role-based delegation.
- Intune Assignments must be set using the Assignments tab in GPOADmin when editing.
- Assignments set in the Intune editor webpage will not be persisted.

5 Clicking **Add** or **Remove** allows you to select the required groups. You have the option of locating groups by entering their name in the search bar. Groups that have been previously added display as disabled. For information on assigning groups, refer to Microsoft documentation.

6 Click **OK**. You now have the option to check in the edited Intune object settings. See Checking in controlled objects for more information.

Editing WMI filters

NOTE: You must edit WMI filters using the GPOADmin console.

To edit a WMI filter

1 Expand the **Version Control Root** and the required container. Select the WMI filter you want to edit within the version control container node in which it exists.

2 Right-click the WMI filter and select **Edit**.

3 Edit the settings of the WMI filter.

4 Click **OK**.

You now have the option to check in the WMI filter to be stored for later use or check in and request approval of the changes.

For information on creating WMI filters, see Creating WMI filters on page 68.

Editing scripts

To edit a script

1 Expand the **Version Control Root** and the required container. Select the script you want to edit within the version control container node in which it exists.

2 Right-click the script and select **Edit**.

3 Edit the settings.

4 Click **OK**.

You now have the option to check in the script to be stored for later use or check in and request approval of the changes.

Linking GPOs

Once GPOs have been created and configured, they must be linked to the appropriate sites, domain, or OU. Before you can link a GPO, you must register and check out the site, domain, or OU. For information on registering Scopes of Management, see Registering objects on page 58.

Users with the Link right can link a single GPO with numerous sites, domains, or OUs and link multiple GPOs to a site, domain, or OU. (For more information on setting permissions, see Configuring role-based delegation.)

The Link right grants the user the right to add, modify, and remove links. This right must exist on the GPO and the scope of management being linked.

The Modify Link Properties right grants the right to modify the Enabled and Enforce properties of a GPO Link. This right must exist on the scope of management.

The Edit right, grants the user the right to modify the Link order. This right must exist on the scope of management.

If you link more than one GPO, you must pay attention to their order. The first GPO has the highest precedence because it is processed last. The Link Report and Group Policy Results Report can help you understand the inheritance structure of your group policies.

NOTE:

- The policies are applied according to the hierarchical structure of Active Directory. You can change the order in which the GPO is applied through the provided arrows.
- You must have the Link right on each GPO and SOM to which you wish to link.

By default, GPOs affect all users and computers contained within a linked site, domain, or OU. To refine the application of a GPO, see Editing GPOs on page 95.

You can also select to restrict the link source to include only policies from specific containers. To restrict linking, see Viewing and editing object properties.

To link GPOs to a single site, domain, or OU

1. Right-click a checked out site, domain, or OU and select **Edit**.
2. Click **New Link** to add another GPO.
3. Select the appropriate option to either Enable or Enforce the GPO link.
4. Enable **Block Inheritance** if required.

   You must have the Block Inheritance for SoM links right to enable this option.
5. Click **OK**.

To link multiple GPOs to multiple sites, domains, or OUs

1. Right-click one or more GPOs and select **Link**.

   Any SOMs that you want to link the GPOs to must be in the available state.
2. In the left pane of the Link dialog box, expand the domains and select the SOMs you want to link to.
3. In the right pane, ensure that the **Add** check box is selected for the GPOs you want to link.
4. Select the appropriate option to either Enable or Enforce the GPO link. You can use the arrows provided to modify the link order.
5. Click **OK**.

You can also rollback pre-existing links between GPOs and sites, domains, and OUs when restoring GPOs. For information, see Restoring links to a previous version on page 72 and Checking compliance on page 93.

Synchronizing GPOs

Synchronizing GPOs allows you to automatically push out pre-defined “primary GPO” settings to specified targets both within a forest and between two forests. This allows you to ensure specific GPOs, which are required in every domain, contain the same settings without having to link to a GPO outside of the domain.

You will be able to select one or more GPOs from various domains as synchronization targets for the source GPO. When the source GPO has been successfully deployed, the settings from the last major backup will be imported into each synchronization target GPO.

NOTE: If permissions between forests are not identical, a mapping table is also available to ensure that forest specific settings are covered.

- Enabling synchronization
- Working with GPO synchronizations
- Generating Synchronized GPO report

Enabling synchronization

The ability to synchronize GPOs requires that:

- It is enabled within the source domain.
- The source GPO must be workflow-enabled to ensure that any changes can be propagated to the targets. (The targets, however, can be workflow-disabled.)
- Targets are registered.
- The source GPO has been deployed at least once.
- Target synchronization settings are configured.
- Each domain has a GPOADmin server. Child domains of a parent domain will appear in the client by default. Trusted siblings however will not.
- The user performing a manual synchronization or setting the synchronization targets has the Synchronize right.

To enable GPO synchronization

1. Right-click the forest and select **Options**.
2. Select **Options| General**.
3. Select **Enable Group Policy Object Synchronization.**
4. Click **OK**.

   Once this has been enabled, you can access the synchronization options by right-clicking a GPO in the Version Control Root and selecting **Synchronize**.

Working with GPO synchronizations

Keep the following in mind when working with synchronizations:

- To synchronize during an immediate deployment (a non-scheduled deployment), the user deploying the GPO must have the Synchronize right.
- The target settings will be overwritten with the settings from the source.
- If a synchronization is attempted while a target GPO is checked out, the synchronization will fail.
- If a target is off line, the synchronization will fail.

- If the source GPO is out of compliance and either a ‘Rollback’ or ‘Incorporate Live’ compliance action will trigger a synchronization.
- Communicate synchronizations plans to those responsible for GPO administration in other domains.
- If GPO synchronization is enabled on a targeted GPOADmin server, ensure that the target GPO does not have the source GPO set as a synchronization target. Doing so will place the two GPOs in an endless synchronization loop.
- When changing the service account, any existing GPO synchronization configuration should be reconfigured to ensure the proper password is used to connect to the target GPOADmin server.
- All configuration options are available through menu options, right-click context menus, and the editor’s toolbar.
- Selecting File | Exit closes the Synchronization Editor.
- Select Edit | Select All allows you to select all the GPO targets listed in the editor.

Synchronization and custom actions

GPOADmin synchronization and custom actions are designed to trigger once per server for each synchronization event. This means that if the synchronization is occurring between two GPOs managed by the same GPOADmin server, or between two GPOs each managed by a different GPOADmin server, the synchronization custom action will function a little differently.

For example:

- Both GPOs are managed by the same GPOADmin server:
  - A synchronization action is initiated by either a user or during deployment.
  - The synchronization pre action takes place on the GPOADmin server.
  - The synchronization process occurs.
  - The synchronization post action is run on the GPOADmin server.
- GPOs are hosted on different GPOADmin servers. The source GPO is on server A, while the target GPO is on server B.
  - A synchronization action is initiated by either a user or during deployment.
  - The synchronization pre action is triggered on GPOADmin server A.
  - Synchronization begins on GPOADmin Server A.
  - The synchronization pre action is triggered on GPOADmin server B
  - Synchronization continues and is completed.
  - The synchronization post actions are run on both GPOADmin servers A and B.

To set up synchronization

1 In the **Version Control Root**, right-click the source GPO, and select **Synchronize | Set Synchronization Targets**.

This will open a dialog where you can add GPO targets and configure their synchronization settings. By default, the server that you are currently connected to will be displayed. It cannot be removed.

2 If required, select **Add Servers** to include other servers that contain the GPOs that you want to target. Select the server and click **Connect**. Enter the required credentials and click **OK**.

NOTE: The credential entered will be stored and used to connect to the associated server during the synchronization process.This allows for the synchronization of GPOs between untrusted domains.

You can also select to remove any servers that have been added. If you do however, any target GPOs setup from this server for synchronization will also be removed.

3 Select the required GPOs and choose **Synchronization | Add Synchronization Target** to select the required target GPOs. The list of all available GPOs will display.

4 Select the required targets and click **OK**.

5 If required, we provide the option to setup a migration table by selecting the target and choosing **Synchronization | Select Migration Table**. From here, you can add (or remove), create, modify the migration tables that are going to be used during the synchronization using the Microsoft Migration Table Editor.

The migration tables, which are xml files, contain the mapping between the source and the target accounts to ensure they have the same access. If permissions are not an issue, the migration table would not be required. It is stored in C:\Program Files\Quest\GPOADmin\MigrationTables.

You are now ready to set the synchronization options.

6 Select the target and choose **Synchronization** to set the synchronization options. You can choose between the following:

- **Clear Migration table**: Clear the tables when no longer required.
- **Use Migration Table Exclusively**: If enabled, the migration (import operation) will not proceed if any settings security principals or UNC paths configured within the source GPO do not exist in the migration table.
- **Migrate Security Filters**: Migrates any security principals from the security filter that are found in the migration table.
- **Set target WMI Filters**: Select this option to synchronize WMI filters between domains. You can choose between the following options:
  - **None**: When you select this option, the WMI filter in the target GPO will not be updated. Use this option to disable previously set WMI Filter synchronizations.
  - **Auto-map By Name**: When you select this option, if a WMI Filter in the target domain is found with the same name as the WMI Filter linked to the source GPO, it is assigned to the target GPO.
- **Select WMI Filter**: This opens a browser that lists all of the WMI Filters in the target domain where the connected account has access. From this list, select the WMI Filter to assign to the target GPO.
- **Target State**: Select the state that you want the target to be in after the synchronization completes. You can choose between **Available**, **Checked Out**, **Pending Approval**, or **Deployed**. The default is Checked Out.

  NOTE: If a target state of Deployed is to be used, it is recommended that this account is a member of the GPOADmin Administrators as they are the only ones who can Approve multiple times.

- **Set Target Workflow Delay**: Select this option to specify the amount of time to wait between workflow actions. By default, this is set to 0.
- **Synchronize Deletions**: Select to enable this option, if you want any deleted source GPOs to also be deleted in the target.

7 Once you have your targets set, it is recommended to validate the synchronization targets by selecting the target GPO and clicking **Tools | Validate Synchronization Targets**.

The synchronization targets are stored using their version control id and their display name. Over the course of time, the name may change or the object may be deleted. During the validation a connection to the target server is made and a check is performed to see if the synchronization target still exists or if the name has changed.

If there is an issue, the target will be displayed with warning icon and a tool-tip to inform you of the issue.

1 If you select to **Cancel the editor, t**he warning will not persist.

2 If you select **OK**, the warning will remain to alert you that the issues must be addressed. When ready to address the issue, simply select the **Correct** button at the top of the dialog or right-click and select **Correct.**

To change the service account used to synchronize GPOs

1 In the **Version Control Root**, select the source GPO, and choose **Synchronization | Set Synchronization Targets**.

This opens a dialog that displays the GPO targets and their synchronization settings.

2 Select any one of the target GPOs, choose **Tools | Update Credentials**, and enter the new credentials.

To perform a manual synchronization

1 Right-click the source GPO and choose **Synchronization | Synchronize Now**.

This opens the Synchronization Progress dialog and allows you to perform a synchronization without redeploying the source GPO.

2 Select the GPOs to synchronize (or select all using **Ctrl + A**) and click **Synchronize**.

NOTE: If nothing is selected, all items will be synchronized.

NOTE: You can also select a target and click the SynchSource header to select all the associated synchronization targets for that item.

The synchronization progress displays if the synchronization is pending, synchronizing, done, failed, or canceled.

NOTE: If the synchronization fails, you can view the error by hovering over the faulted item. You can retry by selecting the **Synchronize** button again.

3 If required, you can select **Export** to export the data to a .csv file.

To validate the synchronization results

1 Right-click a GPO that has synchronization targets set and select **Synchronize | Validate Synchronization Results**.

OR

Right-click a GPO that has synchronization targets set and select **Synchronize | Set Synchronization Targets**. Then select one or more synchronization targets and choose **Validate Synchronization Results**.

The Difference report will run comparing each target to the last major version of the source GPO. Settings that do not match the source GPO are displayed as Out-Of-Sync. The Out-Of-Sync status remains until the settings are synchronized.

To retry the synchronization, right-click the out-of-sync targets and choose **Synchronize Now**.

To validate syncronization results for all synchronization targets

- In the Version Control Root, select the source GPO, and choose **Synchronization | Validate Synchronization Results**.

This runs a comparison report comparing the last deployed version of the source GPO to each of the target GPOs. A warning icon is displayed on the tab of the targets that are out-of-sync.

To validate syncronization results for one ore more selected targets

1 In the Version Control Root, select the source GPO, and choose **Synchronization | Validate Synchronization Results**.

The Synchronization Target dialog displays the GPO targets and their synchronization settings.

2 Select one or more of the existing targets, and choose **Tools| Validate Synchronize Results**.

To synchronize to one or more individual targets from existing targets

1 In the **Version Control Root**, select the source GPO, and choose **Synchronization | Set Synchronization Targets**.

This opens the Synchronization Target dialog that displays the GPO targets and their synchronization settings.

2 Select one or more of the existing targets, and choose **Synchronization | Synchronize Now.**

Generating Synchronized GPO report

You can create a report that contains information on the GPO synchronizations that have been performed in your environment.

For details see the section Creating Diagnostic and Troubleshooting Reports on page 118.

Exporting and importing

- Export objects
- Exporting GPO registry settings as a Desired State Configuration resource file
- Import objects

Export objects

Using the Export Wizard, you can test objects offline before they are implemented in the live enterprise. A typical scenario would be to:

- Check-out an object and make the desired changes.

  Before you check in the change and request approval, you can test the edits.
- Export the object to another domain and test the updates.

  If you see an issue you can change it in the test domain.
- Import the object.
- Check in the new and improved changes for approval.

  NOTE: In the Pending Approval state, exporting the object provides an additional level of quality control before changes are made live in the enterprise.

The following built in roles can perform an export:

- Moderator
- System Administrator
- User

Alternatively, you can create a custom role that includes Read and Export rights.

NOTE: The exported objects must adhere to the naming conventions set on the destination container. Administrators can override this and move objects that do not comply; however, once moved the objects must adhere to the container naming conventions.

Migration table considerations

- When migrating to an untrusted domain, the source entries must be SIDs and the Source Type must be set to Free Test or SID.
- If migrating the Security Filter, the source entries (for the Security Filter only) must be in domain\account format. NT AUTHORITY accounts should have a Destination Name of <Same As Source>.
- If an account cannot be mapped, it is logged in the format that GPMC is looking for.

- If an entry is logged, change the source format to the format that is logged and try again.

To export objects to a test environment

1. Select the number of objects you want to export, either by using **Ctrl** + click to select multiple items, or **Shift** + click at the top and bottom of a contiguous series of items to select them all.
2. To export a single object, right-click the object.
3. Select **Export**.

   NOTE: If you are using the GPMC Extension, you can also select the GPO and click **Workflow|Export**.

4. Select the version that you want to export and click **Next**.
5. Select the target.

   You can select a local directory or network share, another version control system, or a test domain in the live network.

To select a local directory or network share:

- Select **A backup on disk** and click **Next**.
  - Select the backup directory and click **Next**.
  - Click **Finish**.

NOTE: Select **Compress to zip file** to compress one policy to one zip file in the backup location. The file name will be in the following format: {GPOName}_{PolicyVersion}_{PolicyVCID}.zip.

To select another Version Control system

- Select a Version Control Server and click **Next**.
  - Select a Target Folder and click **Next**.
  - Select a Version-Controlled Domain and click **Next**.
  - Select a migration table, if required, and click **Next**.

    NOTE: You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

To select a test domain in the live environment

- Select **The live environment** and click **Next**.
  - Select the target domain and click **Next**.
  - Select a migration table, if required, and click **Next**.

    NOTE: You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

Once you have reviewed the settings and the effects on the target domain, check in the object and request Approval. For more information, see Requesting approval on page 86.

Exporting GPO registry settings as a Desired State Configuration resource file

Desired State Configuration extends Microsoft PowerShell to facilitate environment configuration – including your GPO deployment. Through GPOADmin, you can export GPO's user and/or computer registry settings into a resource file to take advantage of this feature. See https://docs.microsoft.com/en-us/powershell/scripting/dsc/overview/overview?view=powershell-7.1 for more information.

To export GPO registry settings:

1. Right-click the required GPO and select **Export As Desired State Configuration Resource**.
2. Define the resource file and settings that you want to export.

   File Name - The full path to the DSC resource file to save.

   Configuration Name - The configuration used to "group" the registry settings.

   Node Name: The node (computer) the configuration will apply to.

   Select whether to export user, computer, or both registry settings.
3. Click **Next**.
4. To register the exported resources, enable the option, browse to select the target container, and click **Next**.
5. Review the summary information and click **Finish**.

NOTE: You can also uses the Select-ExportAsDSCResource PowerShell command to export the settings. You cannot register the resources using this command.

Import objects

Using the Import Wizard, you can import objects from a local directory or network share, a zip file, another version control system, or a version in the live network.

You can also import GPO backups created in Microsoft Security Compliance Manager version 3.0.

Migration table considerations

- When migrating to an untrusted domain, the source entries must be SIDs and the Source Type must be set to Free Test or SID.
- If an account cannot be mapped, it is logged in the format that GPMC is looking for.
- If an entry is logged, change the source format to the format that is logged and try again.
- You also have the option to use the migration table exclusively, overwrite an existing WMI filter, or to migrate the security filter.
- If migrating the Security Filter, the source entries (for the Security Filter only) must be in domain\account format. NT AUTHORITY accounts should have a Destination Name of <Same As Source>.

To update an object in the Version Control system

1. Right-click an object and select **Import**.

   NOTE: If you are using the GPMC Extension you can also select the GPO and click Workflow | Import.
2. Select the import source.

   If you select a local directory or network share:

   - Select **A backup on disk** and click **Next**.

- Select the backup directory and the backup that you want to import, and click **Next**.

NOTE: You also have the option to import from a zip file.

- Select to use the migration table if required, and click **Next**.

NOTE: You also have the option to use the migration table exclusively and to migrate the security filter.

- Click **Finish**.

If you select another version control system:

- Select **A version control system** and click **Next**.
  - Select the Version Control server and click **Next**.
  - Select the object that has the settings that you want to import and click **Next**.
  - Select the version of the controlled object that you want to import and click **Next**.
  - Select to use the migration table if required, and click **Next**.

NOTE: You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

If you select a version in the live environment:

- Select **The live environment** and click **Next**.
  - Select the domain and the object with the settings you want to import and click **Next**.
  - Select to use the migration table if required, and click **Next**.

NOTE: You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

To import a backup from Security Compliance Manager

1. Right-click an object and select **Import Security Compliance Backups.**
2. Browse to the location of the backup you want to import and click **Next**.
3. Review the import details and click **Finish** to complete the import.

NOTE: This is only supported when using the GPOADmin console. It is not supported when using the GPMC Extension.

4

Creating Reports

- Available reports
- Controlled object reports
- Diagnostic and troubleshooting reports
- Live, working copy, latest version, and differences reports
- Historical Settings Reports
- Creating RSoP validation reports
- Exporting registry settings
- Working with report folders
- Exporting reports to CSV and importing into Excel

Available reports

You can generate report templates for quick real-time reporting purposes, and simple point-in-time reports for historical reasons.

When creating reports, consider the following:

- Report templates are saved as XML files and historical reports are saved as HTML files.
- If you change regional options on your local compuer, restart the GPOADmin client to ensure that your changes are reflected in your reports.
- If you are using the GPMC Extension, you only have access to the History, Latest Version, Working Copy, Live, Differences, and Export Live Registry Settings To CVS reports.
- Times displayed in GPOADmin reports will be in the local time zone of the client computer. Any times displayed in the GPMC settings reports will appear in the time zone of the GPOADmin server.
- You must use the GPOADmin console to create report templates.
- Reporting is not supported when using the **Run as different user** option to open GPOADmin.

To create a report template

- Run the report wizard and select to save the report settings to a file.

  You can double-click the report template to generate a report or right-click the report from within the Reports folder, and select **Run**.

To create a historical report

- Run the report wizard and enter a unique filename in the "Save report settings to file" file.

  You can double-click the report to view the saved version or -click the report and select **Run**.

The available reports include:

- Controlled object reports
- Diagnostic and troubleshooting reports
- Live, working copy, latest version, and differences reports
- Historical Settings Reports

Controlled object reports

- Settings Report
- Difference Report
- Group Policy Comparison Report
- User Activity Report
- Group Policy Object Settings Search Report
- User Activity Report
- Role Assignment Report
- All Actions Report
- Compliance Report
- Change Auditor Report
- Change Auditor Working Copies Report
- Deployment Report
- Protected Settings Assignment Report
- Attestation Report
- Intune Readiness Report
- Internal Audit Report
- Creating Controlled Object Reports

Settings Report

This report generates a settings report for a controlled object. The settings retrieved for the selected object or objects are displayed in the report.

Difference Report

This report shows the difference between versions of one or more objects of the same type in the Version Control system. It allows you to compare a base object and version with one or multiple other objects. Each separate comparison appears in a different tab when the report is displayed.

Group Policy Comparison Report

This reports compares the settings of two or more policies in the Version Control system.

History Report

This report shows all historical actions performed on an object in the Version Control system.

Group Policy Object Settings Search Report

This report runs a text search against Group Policy Object settings for names and values. The most recent version of the GPO is searched for any details containing the text string you have submitted. This report also includes Authentication Services settings.

NOTE: If you want to include Authentication Services in the Settings, Difference, or Group Policy Settings Search reports, you must make a change in the registry settings due to product rebranding. For detailed instructions, see the Release Notes.

User Activity Report

This report shows all actions performed by specified users in the Version Control system.

Role Assignment Report

This report shows which rights and roles a user is assigned both directly and indirectly through group membership.

All Actions Report

This report shows all actions performed by specified users in the Version Control system.

Compliance Report

This report shows which items in the live environment are not compliant with the latest major version stored in the Version Control system. The categories of changes from the stored version are highlighted, to provide a quick compliance overview.

Change Auditor Report

This report shows Change Auditor events for a set of objects. Change Auditor is a comprehensive, low-level auditing tool that bypasses default Windows auditing mechanisms and provides a more robust audit trail. To run Change Auditor reports, you must have Change Auditor installed and the GPOADmin service account must be added to the Change Auditor Administrators group.

When a user logs in to GPOADmin and deploys a change to the live environment, those changes are made on their behalf by the GPOADmin service account. You can see more information about that user in the Initiator Username, Initiator SID (if the name cannot be resolved), and Comment columns of this report. This information is also available in the Change Auditor client.

NOTE: If the Change Auditor coordinator is installed after GPOADmin, you msut restart the GPOADmin service. The Change Auditor agent may take a few minutes to refresh its configuration or you can manually restart it.

NOTE: The Change Auditor report shows changes made in the live environment only.

Change Auditor Working Copies Report

This report shows Change Auditor events for any edits made to a checked-out working copy of a GPO. To run this report, you must have Change Auditor installed and the GPOADmin service account must be added to the Change Auditor Administrators group.

Deployment Report

This report displays the deployment details for all object types and gives you the option to view deployments within a specified date range.

Protected Settings Assignment Report

This report displays which Protected Settings Policies have been assigned to which containers, whether inheritance has been blocked, and the associated container settings. This report is useful when you have more than one Protected Settings Policy applied to a single container.

NOTE: To see this report, the Protected Settings for Group Policy Objects must be enabled through the server properties Options.

Attestation Report

This report displays the current attestation status of all GPOs with attestation enabled or only those where attestation will expire within a specified number of days.

Intune Readiness Report

This report details which GPO can be migrated to Intune. The report groups the results into the following categories:

- Ready To Migrate: 100% of the settings are supported (excluding deprecated settings).
- Attention Required: Not all settings are supported and should be reviewed.
- Not Migratable: 0% of the settings are supported.
- Not Applicable: The GPO has no settings.
- Errors: Errors encountered determining if a GPO can be migrated.

Internal Audit Report

The report captures changes made to internal GPOADmin settings, such as updates to container or object security permissions, modifications to Attestation configurations, and other related property changes.

Creating Controlled Object Reports

To create Controlled Object Reports

NOTE: You must use the GPOADmin console to create Controlled Object Reports.

1. Expand the **GPOADmin** node.
2. Right-click **Reports** and select **New | Report**.
3. Select the type of report to run.

If you select...	Procedure
Settings Report	1. Click **Next**. 2. Select the service that you want to report on and click **Next**. 3. Select the object you want to report on and click **Next**. 4. Select the version you want to report on and click **Next**. 5. Select to run the report or to save the report settings, and click **Finish**.

If you select...	Procedure
Difference Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the object, or objects you want to report on and click **Next**. 4 If you are comparing different versions of one object, select a Base version and then the Comparison versions. – OR – If you are comparing multiple objects, in the **Base** column, select the Base object that you want to compare the other objects to. In the **Version** column, select a version for each object to compare. 5 In the **Show** drop-down list, choose an option for which data to show in the report and click **Next**. 6 Select to run the report or to save the report settings, and click **Finish**. If you have chosen to compare more than two objects, click the tab corresponding to the object you are comparing to the base object to see those differences.
Group Policy Comparison Report	1 Click **Next**. 2 Select a connected service and click **Next**. 3 Select the objects you want to report on and click **Next**. 4 Select the version for comparison and click **Next**. 5 Select to run the report, save the report settings, save to CSV, and click **Finish**.
History Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the object you want to report on and click **Next**. 4 Select to run the report or to save the report settings and click **Finish**.
Group Policy Object Settings Search Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the object you want to report on and click **Next**. If you want to report on all the Group Policy Objects contained in this container and all subcontainers, select the **Include subcontainers** check box. 4 Enter the setting name or value you want to report on and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.
User Activity Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the user you want to report on and click **Next**. 4 Select to run the report or to save the report settings, and click **Finish**.

If you select...	Procedure
Role Assignment Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the user you want to report on and click **Next**. 4 Select to run the report or to save the report settings, and click **Finish**.
All Actions Report	1 Click **Next**. 2 Select the service to report on and click **Next**. 3 Select one or more objects to include in the report and click **Next**. 4 Select one or more actions to include in the report and click **Next**. 5 Select to run the report on all trustees or only select trustees and click **Next**. When using the Workflow Approval through email feature, select the Report on all trustees option to view Approve and Reject actions performed by approvers who are not GPOADmin users or administrators. 6 Select to include all the activity for the specified users and objects or only the activity during a specific time period and click **Next**. 7 Select how you want to group the report results and click **Next**. 8 Select to run the report or to save the report settings, and click **Finish**.
Compliance Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select to run the report or to save the report settings and click **Finish**.
Change Auditor Report	1 Select the service you want to report on and click **Next**. 2 Select the object you want to report on and click **Next**. 3 Select a time interval to report on, and click **Next**. 4 Choose the object you want to Group by, Sort by, and the Sort order, and click **Next**. 5 Select to run the report and/or to save the report settings and click **Finish**. 6 When you are finished with the report, click **Close**. You can also see Change Auditor information about objects on their Property pages, on the **Change Auditor™** tab (Viewing and editing object properties on page 81).
Change Auditor Working Copies Report	1 Select the service you want to report on and click **Next**. 2 Select the objects you want to report on and click **Next**. 3 Select a time interval to report on, and click **Next**. 4 Select to run the report and/or to save the report settings and click **Finish**. You can see the changes made to the working copies under the Check Out section of the report. 5 When you are finished with the report, click **Close**.

If you select...	Procedure
Deployment Report	1 Select the domain you want to report on and click **Next**. 2 Select the object types to display and an optional date range and click **Next**. 3 Select to run the report and/or to save the report settings and click **Finish**. 4 When you are finished with the report, click **Close**.
Protected Settings Assignment Report	1 Click **Next**. 2 Select the service that you want to report on and click **Next**. 3 Select the required Protected Settings Policy you want to report on and click **Next**. 4 Select to run the report or to save the report settings, and click **Finish**.
Attestation Report	1 Click **Next**. 2 Select the service that you want to report on and click **Next**. 3 Select to include all attestations or those about to expire within a specified number of days and click **Next**. 4 Select to run the report or to save the report settings, and click **Finish**.
Intune Readiness Report	1 Click **Next**. 2 Select the service that you want to report on and click **Next**. 3 Select the tenant that you want to report on and click **Next**. 4 Select the GPOs to include in the report. 5 Select the cleanup options. To retrieve the Intune readiness data, a migration report is generated on the selected Intune tenant. This report is required to perform the actual migration which must be done manually on the Intune web dashboard. You have the option to leave all of the migration reports, delete all of the migration reports, or delete all of the migration reports that have a supported settings percentage below a specified value. 6 Select to run the report or to save the report settings, and click **Finish**.
Internal Audit Report	1 Click **Next**. 2 Select the service that you want to report on and click **Next**. 3 Select the trustee on which you want to run the report and click **Next**. If you select to run the report on only select trustees, you will also need to specify the users that you want to report on. 4 Specify the time range for the report and click **Next**. 5 Select to run the report or to save the report settings, and click **Finish**.

Diagnostic and troubleshooting reports

NOTE: You must use the GPOADmin console to create Troubleshooting Reports.

- Group Policy Object Consistency Report
- Software Installation Package Report
- Linked/Unlinked Report
- Linked/Unlinked SOMs Report
- Inactive Policy Settings Report
- Group Policy Object Security Report
- Group Policy Permission Check Report
- Group Policy Size Validation Report
- Policy Analysis Report
- GPO Synchronization Report
- Group Policy Results
- Group Policy Results Difference Report
- Group Policy Modeling Report
- Group Policy Object Settings Priority Report
- WMI Filter Usage Report
- Creating Diagnostic and Troubleshooting Reports

Group Policy Object Consistency Report

This report tests all the domain controllers in a given domain to ensure the Active Directory and SYSVOL portions of all GPO's have replicated correctly and consistently.

Software Installation Package Report

This report shows a list of all GPOs that include software installation packages.

Linked/Unlinked Report

This report details GPOs that are linked to certain Scopes of Management and the GPOs that are not linked to anything.

Linked/Unlinked SOMs Report

This report shows a detailed view of SOM object (Domain, OU, Site) with linked GPOs and unlinked SOM objects.

Inactive Policy Settings Report

This report shows the registered GPOs that have settings defined within inactive user or computer sections.

Group Policy Object Security Report

This report details the security of GPOs, specifically where certain trustees are either present or not present.

Group Policy Permission Check Report

This report displays the group policy objects where:

- accounts other than those directly specified have the native GPMC Edit right
- the Active Directory and SYSVOL ACLs are not consistent
- the service account is not the owner

NOTE:

- The default accounts are:
  - GPOADmin service account, Enterprise Admins, Domain Admins, and SYSTEM.
- This report is only available for SQL configuration stores.

Group Policy Size Validation Report

This report displays policies that have a SYSVOL directory size greater than the specified value.

NOTE:

- The default size is 1MB.
- This report is only available for SQL configuration stores.

Policy Analysis Report

This report displays the registry settings for GPOs within a selected Scope of Management. You can use this report to help to manage your deployment by comparing GPOs to identify information such as duplicate settings, inconsistencies, or how many times a value has been changed.

You can select to export the entire report results as a .CSV file or select to only export only the settings that are different for the GPOs for the specified Scope of Management.

You can run the report by either:

- Right-clicking a registered Scope of Management and selecting **Reports | Policy Analysis**.
- Right-clicking an unregistered Scope of Management and selecting **Policy Analysis**.
- Using the Report Wizard.

The report details include:

- The registry key, the key name, and the value. (Hovering your mouse over any bold names or the information icon provides additional registry information.)
- The GPO name. (Hovering your mouse over the GPO name, displays the distinguished name for the SOM the policy is linked to.)
- A gray background signifies that the setting is not set in the GPO.
- A white background signifies that the setting is set in the GPO.
- A yellow background signifies that the setting has changed in the GPO.

NOTE:

- To run the report on the live environment, you must have the domain Read and domain Reports.
- To run the report by right-clicking an SOM, you must have the R**un Contextual Report.**
- To run the report from the report wizard, you must have the Run Reports, domain Read, and domain Reports.

GPOAnalyzer Utility

The Policy Analysis report does not check the security or validate the WMI filters. To analyze whether users have access to a GPO and how WMI filtering has been set to apply group policy objects, we have provided the GPOADmin.GPOAnalyzer.exe command-line utility.

To run the utility, start a command prompt and specify GPOADmin.GPOAnalyzer.exe with the appropriate parameters.

Table 17. Available parameters

Parameter	Required or optional	Description
/Domain	Required	Scope of Management fully qualified domain name.
/SOMDN	Required	Scope of Management distinguished name.
/Output	Required	File name for the saved report.
/x	Optional	Force the output to be in XML. (The default is HTML)
/DC	Optional	Domain controller to communicate with. (The default is the PDCe)
/E	Otional	Instructs the application to use LDAPs for communication with Active Directory. The default is LDAP.
/S	Optional	Process security filters. This checks to see if the current user can access the GPO. (The default is set to not check security.)
/F	Optional	Validate GPO WMI filters. (The default is set to not check WMI filters to see determine if a GPO should be processed.)
/L	Optional	Use the locally stored GPO definition. (The default is to use the central store, if configured. If not, the local policy definition will be used.)
/V	Optional	Log progress to the screen.
/U	Optional	Process only the user configuration. (The default is user and computer.)
/C	Optional	Process only the computer configuration. (The default is user and computer.)

GPO Synchronization Report

This report details the GPO synchronizations that have been performed in your environment.

Group Policy Results

This report shows the resultant set of policies (RSoP) for a given user or computer, or both.

Group Policy Results Difference Report

This report displays the resultant set of policies (RSoP) differences between the selected users or computers. The Group Policy Results Difference Report does not include the Remote Installation extension in the report settings.

Group Policy Modeling Report

This report displays the resultant set of policies based on the selected simulation options within the modeling session. You can use this report to simulate changes and validate that the results match the desired outcome before actually implementing any changes within your environment. Using this report, you can evaluate checked

out GPO working copies so that you can mitigate any unexpected effects once the changes are made to the live version.

IMPORTANT: An application partition is created during the simulation to house the report. It contains a temporary staging container that is deleted once the report has been generated.

If necessary, you can create or delete the staging application directory partition:

1. Open Command Prompt.
2. Type:

   ntdsutil
3. At the ntdsutil command prompt, type:

   domain management or partition management
4. At the domain management command prompt, type:

   connection
5. At the server connections command prompt, type:

   connect to server ServerName
6. At the server connections command prompt, type:

   quit
7. At the domain management command prompt, do one of the following:
   - To create an application directory partition, type:

     create nc dc=staging,dc=gpoadmin DomainController

     For every domain controller which might be used to run the Group policy modeling report on, type the following:

     add nc replica "dc=staging,dc=gpoadmin" DomainControllerName
   - To delete an application directory partition, type:

     delete nc dc=staging,dc=gpoadmin

Group Policy Object Settings Priority Report

This report can help to determine if a particular policy is having its settings overwritten based on its position in the link order.

WMI Filter Usage Report

This report can help to determine which GPOs are using WMI filters and which filters are in use.

Creating Diagnostic and Troubleshooting Reports

To create troubleshooting reports

NOTE: You must use the GPOADmin console to create Troubleshooting Reports.

1. Expand the **GPOADmin** node.
2. Right-click **Reports** and select **New| Report**.
3. Select the type of report to run under Diagnostic and Troubleshooting Reports:

If you select...	Procedure
Group Policy Object Consistency Report You can also check the consistency between selected group policy objects on a domain controller, by right-clicking the required GPOs and selecting **Reports | GPO Consistency.**	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select to include the GPO ACL, SYSVOL, or SYSVOL Scripts folder in the report and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.
Software Installation Package Report Linked/Unlinked Report Linked/Unlinked SOMs Report Inactive Policy Settings Report	1 Click **Next**. 2 Select the service you want to report on, and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select to run the report or to save the report settings, and click **Finish**.
Group Policy Object Security Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Specify accounts to include or exclude in the report and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.
Group Policy Permission Check Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Specify accounts that are allowed to have the native GPMC Edit right, click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.
Group Policy Size Validation Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Specify the size threshold for the report, and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.

If you select...	Procedure
Policy Analysis Report	1 Click **Next**. 2 Select the domain you want to report on and click **Next**. 3 Select the Scope of Management that you want to analyze, and click **Next**. 4 Select to run the report, save the report so that you can compare it to another report, or save the report settings. 5 If required, you can select **Export** to export the all the results to a .csv file or **Export Differences Only** to export only the settings that are different for the GPOs for the specified Scope of Management. 6 Click **Finish**.
GPO Synchronization Report	1 Select the service on which to run the report and click **Next**. 2 Select the GPO on which to run the report and click **Next**. 3 Select to run the report or to save the report settings and click **Finish.**
Group Policy Results	1 Click **Next**. 2 If you are connected to more than one service, you are asked "Which service do you want to run the report on?". Select a service and click **Next.** 3 Select the domain you want to report on and click **Next**. 4 Browse to locate the required computers or enter the computer name and click **Next**. **NOTE:** Multiple computers must be separated with a semicolon. 5 Select the user whose policy settings you would like to view and click **Next**. 6 Select to run the report or save the report settings, and click **Finish**.

If you select...	Procedure
Group Policy Results Difference Report	1 Click **Next**. 2 If you are connected to more than one service, you are asked "Which service do you want to run the report on?". Select a service and click **Next.** 3 Select the domain you want to report on and click **Next**. 4 Choose initial report to use in the comparison and click **Next**. You can choose between a new report, a dynamic report, or a previously saved report. If you choose to create a new report, you need to click through the wizard to select the required user and computer. 5 Choose the second report to use in the comparison and click **Next**. You can choose between a new report, a dynamic report, or a previously saved report. If you choose to create a new report, you need to click through the wizard to select the required user and computer. 6 Select the required display options and click **Next**. *You can choose to see all settings, differences only, or similarities only.* 7 Select to run the report or to save the report settings and click **Finish**.

If you select...	Procedure
Group Policy Modeling Report	1 Click **Next**. 2 Select the domain and the domain controller where the RSoP report will be run, (optionally) select **Use Secure LDAP** to protect your directory data and credentials during communication with Active Directory, and click **Next**. You can select any domain controller or a specific domain controller within the domain with the supported operating system. 3 Browse to and select the required user or computer (or container that contains the user or computer), and click **Next**. 4 If necessary, you can select to: ▪ Simulate a slow network connection. ▪ Enable loopback processing. This option is only available if a computer has been selected. You can use this to narrow down the settings to be considered in the simulation and focus on only those of interest to you. If **Replace** is selected, ONLY computer GPOs and WMI filters are considered for the simulation. If **Merge** is selected, all GPOs and WMI filters (user and computer) are included. When being evaluated for the simulation, the computer GPOs are placed with a higher precedence than the user GPOs. ▪ Select to use a site other than the default site. Click **Next** when satisfied with your selections. 5 If necessary, browse to and select an alternate network location for the user or computer. This option is only available for users or computers — you cannot select this for containers. **Note**: You can select the **Restore to Default** option to return to the initial state. Click **Next** when satisfied with your selections. 6 The top-level groups where the user or computer is a member displays. Select to see the effect of adding or removing users from groups as required. **Note**: You can only select to add immediate groups. Any group can be removed except for the Authenticated Users and Everyone groups. Click **Next** when satisfied with your selections. 7 If necessary, select to see the effects of removing WMI filters. You can select to see all linked filters or choose specific filters. ▪ **All linked filters**: This option assumes that the user meets the criteria and all filters are applied. ▪ **Only these filters**: This option enables you to list all available filters and remove as required.

If you select...	Procedure
Group Policy Modeling Report	**Note**: If you plan to alter GPO link properties, you should select the default **All linked filters**. If you select to include only select filters some changes may not be reflected in the simulation. Click **Next** when satisfied with your selections. 8 If necessary, select to simulate link modifications to a Scope of Management. ▪ Right-click a GPO and select whether to have the GPO link enforced or link enabled), alter their link order, and simply remove them. ▪ Right-click a parent OU to block inheritance or add GPOs as required. **Note**: You can only choose checked out working copy or deployed GPOs. **Note**: GPOs are added as unenforced, link enabled or disabled depending on the Default link state server option, and at the bottom of the list. Select **Restore** to undo any changes. This only affects the immediate OU. Child OUs will not be undone. Select **Restore All Defaults**, to undo all changes. Click **Next** when satisfied with your selections. 9 Review the summary page and click **Next** to proceed. 10 Select to run the report or save the report settings, and click **Finish**.
Group Policy Object Settings Priority Report	1 Click **Next**. 2 Select the domain you want to report on and click **Next**. 3 Select the GPO that you want to report on and click **Next**. 4 Select the computers whose policy settings you want to view and click **Next**. You can optionally select to view only the user policy settings in the report. 5 Select the users whose policy settings you want to view and click **Next**. You can optionally select to view only the computer policy settings in the report. 6 Select to run the report or save the report settings, and click **Finish**.
WMI Filter Usage Report	1 Click **Next**. 2 Select a connected service and click Next. 3 Select the domain you want to report on and click **Next**. 4 Select to report on either all WMI Filters or a selected range of WMI Filters and whether to group by WMI Filter or GPO and click **Next**. 5 Select to run the report or save the report settings, and click **Finish**.

Live, working copy, latest version, and differences reports

You can create a report that shows information about the live, working copy, or latest versions of an object, or that compares two or more versions of the same object.

- Creating live, working copy, latest version, and differences reports

Creating live, working copy, latest version, and differences reports

To create a report in the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click the required controlled object and select **Reports**.
   - To create a report of the live controlled object's settings, select **Live**.
   - To create a report on the checked out and working copy settings, click **Working Copy**.
   - To create a report on the latest version of the controlled object in Version Control, click **Latest**.
   - To create a report to show the differences between two or more object's settings, click **Differences**.
3. View the report.

   Click **Print** to print the report.

   Click **Save As** to save the report as an HTML file.

   To view the report in the Reports node, save it in the My GPOADmin Reports folder in the Documents folder.

NOTE: By default, GPOADmin looks to the My GPOADmin Reports folder (C:\Users\gpoadmin\Documents\My GPOADmin Reports) for saved reports. To point to a different folder, change your User Preferences. For more detail, see Configuring user preferences on page 58.

4. Click **Close**.

   To view the report later, double-click the required report and click to expand the section you want to view.

To create a report in the GPMC Extension

1. Select the GPO and click **Reports**.
   - To create a report of the live GPO's settings, select **Live**.
   - To create a report on the checked out and working copy settings, click **Working Copy**.
   - To create a report on the latest version of the GPO in Version Control, click **Latest**.
   - To create a report to show the differences between two or more GPO's settings, click **Differences**.
2. View the report.

   Click **Print** to print the report.

   Click **Save As** to save the report as an HTML file.
3. Click **Close**.

Historical Settings Reports

You can create a report that shows information about the historical settings.

- Creating historical settings reports

Creating historical settings reports

To create a Historical Settings Report

1. Expand the **Version Control Root** node and the required container.
2. Right-click the required controlled object and select **Show History**.
3. To view the settings of a previous version, -click the version and select **View**.
4. View the report. Click **show** or **hide** to expand or collapse each section.

   Click **Print** to print the report.

   Click **Save As** to save the report as an HTML file.
5. Click **Close**.

   To view the report later, double-click the required report and click to expand the section you want to view.

To create a Historical Settings Report in the GPMC Extension

1. Click **Show History**.
2. In the bottom pane, -click the version of the GPO and select **View**.
3. View the report. Click **show** or **hide** to expand or collapse each section.

   Click **Print** to print the report.

   Click **Save As** to save the report as an HTML file.

   Files saved in the GPMC Extension are visible in the Reports node of the GPOADmin console.
4. Click **Close**.

Creating RSoP validation reports

You can schedule the generation of RSoP difference reports on one or more computers every 24 hours to validate whether the desired Group Policy settings have been applied.

NOTE: This feature is available for SQL configuration stores only.

To create an RSoP validation report

1. Expand **GPOADmin**, the **Live Environment**, right-click a domain or OU, and choose **RSoP Validations**.
2. From the RSoP Validation Scheduler dialog, click **New**.
3. Use the default RSoP comparison source, use the ellipse button to select an existing source, or click **New RSoP** to create a new source.
4. Select which computers to compare against the specified RSoP report.

   Container: Select this option to include all computers in a given organizational unit.

   Computers: Select this option to add and remove specific computers.
5. Select the output directory for the generated reports. You can use the ellipse button to select an existing directory.

   The following subdirectories are created:

   - A subdirectory named "RSoP validation".

- A subdirectory with the name of the RSoP validation.
- A subdirectory with the long version of the execution date.

The report will be saved in the subdirectory with the name "RSoP on [COMPUTER_NAME].html"

6 Select **Show differences only** if you want the generated reports to only display differences; otherwise differences and similarities are displayed.

7 Select the start date, time and time zone to run the reports. After the initial run they will be repeated every 24 hours.

To edit an RSoP validation report

1 Expand **GPOADmin**, the **Live Environment**, right-click a domain or OU, and choose **RSoP Validations**.

2 From the RSoP Validation Scheduler dialog, select the validation report, and click **Edit**.

3 Click **New RSoP** to create a new source or use the ellipse button to select an existing source.

4 Select which computers to compare against the specified RSoP report.

Container: Select this option to include all computers in a given organizational unit.

Computers: Select this option to add and remove specific computers.

5 Select the output directory for the generated reports. You can use the ellipse button to select an existing directory.

The following subdirectories are created:

- A subdirectory named "RSoP validation".
- A subdirectory with the name of the RSoP validation.
- A subdirectory with the long version of the execution date.

The report will be saved in the subdirectory with the name "RSoP on [COMPUTER_NAME].html"

6 Select **Show differences only** if you want the generated reports to only display differences; otherwise differences and similarities are displayed.

7 Select the start date, time and time zone to run the reports. After the initial run they will be repeated every 24 hours.

To remove an RSoP validation report

1 Expand **GPOADmin**, the **Live Environment**, right-click a domain or OU, and choose **RSoP Validations**.

2 From the RSoP Validation Scheduler dialog, select the validation report, and click **Delete**.

Exporting registry settings

If you want to create custom GPO reports, you can export GPO settings to a spreadsheet and format the data to suit your needs.

To export GPO settings

1 Select one or more GPOs, right-click and select **Export Policy RegistrySettings to CSV**.

2 Select whether to export all settings, user settings only, or computer settings only.

Working with report folders

Reports in GPOADmin mirror the contents of My GPOADmin Reports folder in the Documents folder.

NOTE: Report Folders are only available in the GPOADmin console.

- Managing report folders

Managing report folders

To create a folder

- Right-click **Reports** or any subfolder, and select **New | Folder**.

To rename a folder

- Right-click any subfolder under Reports, select **Rename** and enter the new name.

NOTE: The name must be a valid Windows® folder and must not conflict with any other folder names of the same parent.

To delete a folder

- Right-click any subfolder under Reports and select **Delete**.

To manage reports using Windows ***Explorer***

1. Right-click **Reports** and select **Open Folder in Explorer**.

   From here, you can manage your files in the typical manner.

2. Once you return to GPOADmin, right-click **Reports**, and select **Refresh** to ensure that your view is updated.

Exporting reports to CSV and importing into Excel

You can export the following reports as CSV files for easy viewing and analysis in Microsoft Excel:

- All Actions Report
- Attestation Report
- Group Policy Object Settings Priority Report
- GPO Synchronization Report
- History Report
- Internal Audit Report
- Intune Readiness Report
- Group Policy Object Consistency Report
- Group Policy Permission Check Report
- Group Policy Size Validation Report

When saving a report as a CSV file, you will be prompted to choose a delimiter (the same options available in Excel).

To import a CSV file into Excel:

1. Open Excel and select **Blank workbook**.
2. Go to the **Data** tab and click **From Text/CSV.**
3. Browse and select the CSV file you want to import.
4. In the **Delimiter** drop down, choose the delimiter you selected when saving the report.
5. Click **Load**.

   Your report data will now be imported into Excel.

5

Appendix: Windows PowerShell Commands

- Introduction
- GPOADmin scripts
- Available commands
- Using the GPOADmin PowerShell commands (Examples)

Introduction

The GPOADmin PowerShell commands are installed during a complete or custom installation. (Asssuming that you have Windows PowerShell currently installed.)

The GPOADmin provider and commands allow you to perform virtually all available functionality through a command line.

For detailed examples on using the commands, see Using the GPOADmin PowerShell commands (Examples).

Registering the GPOADmin PowerShell commands

Before you can use the commands, you must register them on the system where GPOADmin is installed.

To register the GPOADmin commands

1. Open a PowerShell window and type the following in the command prompt:

   import-module 'C:\Program Files\Quest\GPOADmin\GPOADmin.psd1'

2. Type the following in the PowerShell command prompt to verify that the snap-in was added:

   get-command -module GPOADmin

   All registered PowerShell commands display.

Loading the PowerShell provider

To load the GPOADmin PowerShell provider

1. Open PowerShell and run the following command:

   `Import-Module -Name <GPOADmin Install Directory>\GPOADmin.psd1.`
   Once the GPOADmin provider is loaded, it creates two default drives called "VCRoot" and "PSRoot".

   PSRoot is the virtual directory created when Protected Settings policies are enabled for the specified server. All Protected Settings policy management and workflow actions are performed from here.

2. To access the drive, enter the following command: `CD VCRoot: or CD PSRoot:`

NOTE: You must include the colon.

If you are running only the GPOADmin client, you must create a PSDrive mapped to the version control root to use the available PowerShell capabilities.

We recommend that all commands be run from the created PSDrive.

NOTE: The account used in the credentials parameter must have permission to connect to the specified GPOADmin server. Permission is granted by adding the user as either a GPOADmin user or administrator on the Access tab of the targeted GPOADmin Server Properties dialog.

Table 18. Connection options

Connection requirement	Command
Connect to the Version Control Root of GPOADmin on this computer as the current user	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root"`
Connect to the Protected Settings Root of GPOADmin on this computer as the current user	`New-PSDrive -Name "PSRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -DriveType PSROOT`
Connect to the Version Control Root of GPOADmin on this computer as a different user (a dialog appears prompting for the user password)	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Credential "domain\user"`
Connect to the Protected Settings Root of GPOADmin on this computer as a different user (a dialog appears prompting for the user password)	`New-PSDrive -Name "PSRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -DriveType PSROOT -Credential "domain\user"`
Connect to the Version Control Root of GPOADmin on a different computer using the default port number as the current user	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Server"server.domain.com"`
Connect to the Protected Settings Root of GPOADmin on a different computer using the default port number as the current user	`New-PSDrive -Name "PSRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -DriveType PSROOT -Server"server.domain.com"`
Connect to the Version Control Root of GPOADmin on a different computer using the default port number as a different user (a dialog appears prompting for the user password)	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Server "server.domain.com" -Credential "domain\user"`
Connect to the Protected Settings Root of GPOADmin on a different computer using the default port number as a different user (a dialog appears prompting for the user password)	`New-PSDrive -Name "PSRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -DriveType PSROOT -Server"server.domain.com" -Credential "domain\user"`
Connect to the Version Control Root of a GPOADmin server on a different computer using a custom port number of 40201 as the current user	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Server "server.domain.com" -Port 40201`
Connect to the Protected Settings l Root of a GPOADmin server on a different computer using a custom port number of 40201 as the current user	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -Server "server.domain.com" -Port 40201`

Connection requirement	Command
Connect to the Version Control Root of a GPOADmin server on a different computer using a custom port number of 40201 as a different user (a dialog appears prompting for the user password)	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Server "server.domain.com" -Port 40201 -Credential "domain\user"`
Connect to the Protected Settings Root of a GPOADmin server on a different computer using a custom port number of 40201 as a different user (a dialog appears prompting for the user password)	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -Server "server.domain.com" -Port 40201 -Credential "domain\user"`

GPOADmin scripts

GPOADmin installs the following PowerShell scripts to c:\Program Files\Quest\GPOADmin\Scripts:

- GPOADmin.AddServiceAccountToAllGPOs.ps1
- GPOADmin.RunDynamicReport.ps1
- GPOADmin.MinimumPermissions.ps1

GPOADmin.AddServiceAccountToAllGPOs.ps1

Grants the specified service account Edit settings, Delete, and Modify Security privileges and assigns ownership to all the GPOs in the specified domain.

Parameters

- Domain: Specifies the DNS name of the domain in which to modify the GPOs.
- ServiceAccount: Specifies the account, in domain\user format, that will be granted access to and made the owner of all the GPOs.

Syntax

```
GPOADmin.AddServiceAccountToAllGPOs -Domain <string> -ServiceAccount <string>
```

Example

```
GPOADmin.AddServiceAccountToAllGPOs -Domain "MyDomain.com" -ServiceAccount
"mydomain\Service Account"
```

GPOADmin.RunDynamicReport.ps1

Runs a specified GPOADmin dynamic report and emails the results to a list of recipients.

Parameters

- gpmServer: Specifies the GPOADmin server to connect to. (Optional)
- gpmPort: Specifies the port number of the GPOADmin server. Default is 40200. (Optional)
- DynamicReportFile: Specifies the path to the dynamic report file to run.

- Recipients: Specifies the list of e-mail recipients.

Syntax

```
GPOADmin.RunDynamicReport.ps1 -Server <string> -Port <int> -DynamicReportFile
<string> -Recipients <stringArray>
```

Example

```
GPOADmin.RunDynamicReport.ps1 -Server "localhost" -Port 40200 -DynamicReportFile
"DynamicReport.xml" -Recipients ("recepient@company.com")
```

GPOADmin.MinimumPermissions.ps1

Sets, revokes, and reports on environment permissions for the service account.

Parameters

- ServiceAccount: The service account in either domain\user or user@domain.com format.
- Domain: The FQDN of the managed domain.
- LDAPServer: The FQDN of the domain controller to be used.
- Permissions: A comma delimited string of the permissions to be set, revoked, or reported on.
  - Delete: Grants "Delete Subtree”.
  - GPO: Grants "Create GPOs".
  - GPOEdit: Grants "Edit settings, Modify security, and Delete"
  - GPOOwner: Assigns the service account as the GPO owner.
  - GPOModel: Grants the ability for the service account to create the application directory for GPO Modeling Report and adds the service account to the Distributed COM users group.
  - Install: Grants "Full Control" to the install directory.
  - Link: Grants "Link GPOs".
  - Registry: Grants "Full Control" to HKLM\SOFTWARE\Quest\GPOADmin, grants "Query Value, Set Value, Create SubKey, Enumerate Subkeys, Delete, and Read Control" to HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Diagnostics and to HKLM\SYSTEM\CurrentControlSet\Service\EventLog.
  - Replication: Grants “Replicating directory changes" on the Default and Configuration naming contexts (for the Watcher Service).
  - RSoP: Grants "Read Group Policy Results Data" and "Perform Group Policy analysis".
  - SCP: Grants "Create and Delete serviceConnectionPoint objects".
  - Script: Grants "List folder contents, Read, and Write" to the Scripts container in SYSVOL.
  - SPN: Grants "Read and Write servicePrincipalName".
  - StarterGPO: Grants "Create Starter GPOs".
  - StarterGPOOwner: Assigns the service account as the Starter GPO owner.
  - WMI: Grants "Full Control" on all WMI Filters.
  - All: All of the above.
- Confirm: Prompts for confirmation before granting or revoking permissions.
- Revoke: Revokes the specified permissions.

- Report: Reports whether the supplied service account as the specified permissions.

Syntax

```
GPOADmin.MinimumPermissions -ServiceAccount <string> -Domain <string> -LDAPServer
<string> -Permissions <string> -Report <switch> -Revoke <switch> -Confirm <switch>
```

Example

```
GPOADmin.MinimumPermissions.ps1 -ServiceAccount "MyDomain\serviceaccount" -Domain
"MyDomain.com" -LDAPServer "MyDC.MyDomain.com" -Permissions "All" -Report
```

Available commands

The following section lists all available GPOADmin commands. To see examples on how to use some of these commands, see Using the GPOADmin PowerShell commands (Examples) on page 143.

NOTE:

- Items with a backslash or forward slash in the name will not manageable in PowerShell.
- Items with an astrix in the name must inclose the name in single quotes and escape the astrix using the backtick character (character below the tilde).

  For example:

  Item Name: Test *

  Escaped: 'Test `*'

To see a list of all available commands

- Open PowerShell, load the GPOADmin provider, and run the following command:

  get-command -module GPOADmin

  To see command details including the required parameters, run the PowerShell `get-help` command. To see more detailed help, see Extracting help for GPOADmin commands on page 144.

Table 19. Available commands

Type	Available commands
Add	• Add-Administrator • Add-IntuneAssignments • Add-DomainSecurity • Add-EmailTemplates • Add-Keywords • Add-LiveEnvironmentSecurity • Add-ProtectedSettingsExclusions • Add-ProtectedSettingsPolicies • Add-RootContainerAssignment • Add-Role • Add-User
Clear	• Clear-AssignedProtectedSettingsPolicies • Clear-ActionAccounts • Clear-BackupsByRetention • Clear-IntuneAssignments • Clear-DomainSecurity • Clear-ExchangeOptions -WorkflowOrSMTP • Clear-EmailTemplate • Clear-GmailOptions -WorkflowOrSMTP • Clear-IntuneOptions -TenantId • Clear-KeywordsList • Clear-LiveEnvironmentSecurity • Clear-Notifications • Clear-ProcessLock • Clear-ProtectedSettingsExclusions • Clear-RootContainerAssignment • Clear-SMTPOptions -WorkflowOrSMTP • Clear-SynchronizationTargets
Copy	• Copy-ServerConfiguration

Table 19. Available commands

Type	Available commands
Get	• Get-Administrators • Get-AllManagedObjects • Get-ApprovalWorkflow • Get-AssignedProtectedSettingsPolicies • Get-AssociatedItems • Get-Available • Get-BlockKeywordInheritance • Get-BlockProtectedSettingsInheritance • Get-ChangeAuditorDateRange • Get-ChangeAuditorService • Get-CheckedOut • Get-ChecktedOutToMe • Get-CloakedGPOs • Get-CommentMaximumLength • Get-CommentMinimumLength • Get-Compliance • Get-IntuneAssignments • Get-ContainerBlockKeywordInheritance • Get-ContainerKeywords • Get-CurrentUser • Get-DefaultLinkStateIsEnabled • Get-DeletedObjects • Get-Diagnostics • Get-DifferenceReport • Get-DisableAllGPOWorkflow • Get-DomainSecurity • Get-DSCRootPath • Get-DynamicReport • Get-EmailTemplates • Get-EnableApprovals • Get-EnableAssociatedItemIdentification • Get-EnableAutomaticDeploymentSynchronization • Get-EnableCustomWorkflowActions • Get-EnableDeploymentFailureAutomation • Get-EnableDSCSupport • Get-EnableGPOSynchronization • Get-EnableProtectedSettings • Get-EnableWMIFilterReadRestriction • Get-EnforceNamingStandards • Get-EnforceUniqueNames • Get-EnforceUniqueRoleNames • Get-EnsureServiceAccountAccess • Get-ExchangeOptions • Get-EnableFIPSMode • Get-FailedDeployment • Get-GmailOptions

Table 19. Available commands

Type	Available commands
	• Get-GPMCVersionCheck • Get-GPOLineage • Get-GPOLinks • Get-GPOLiveRegistrySettings • Get-GPOs • Get-ItemByID • Get-IntuneOptions • Get-KeywordsList • Get-LicenseInfo • Get-LinkedSOMs • Get-LiveEnvironmentSecurity • Get-LockedGPOs • Get-LoggingOptions • Get-NotificationEmailAddress • Get-NotificationList • Get-Notifications • Get-OrphanedWorkingCopies • Get-OuDisplayFormat • Get-OULinkContainers • Get-PendingApproval • Get-PendingDeployment • Get-Permissions • Get-PreferredDomainController • Get-Properties • Get-ProtectedSettingsBlockedExtensions • Get-ProtectedSettingsExclusions • Get-ProtectedSettingsExclusionsRecursion • Get-ProtectedSettingsPolicies • Get-RemediationRule • Get-Roles • Get-RootContainerAssignment • Get-Security • Get-SecurityFilter • Get-ServerConfiguration • Get-ServerDomain • Get-ServerVersion • Get-ServiceAccount • Get-SettingsReport • Get-SMTPOptions • Get-SQLTimeouts • Get-StarterGPOs • Get-StorageOptions • Get-SynchronizationTargets • Get-UnauthorizedModifications • Get-UnlinkedSOMs • Get-Unregistered

Table 19. Available commands

Type	Available commands
Get	• Get-Users • Get-ValidScriptExtensions • Get-VCItemHistory • Get-WorkflowDisabledGPOs • Get-WorkflowDisabledSOMs • Get-WorkflowDisabledWMIFilters • Get-WorkflowEnabledGPOs • Get-WorkflowEnabledSOMs • Get-WorkflowEnabledWMIFilters
New	• New -BackupServerUseSSL • New-ConfigServerUseSSL • New-Container • New-DomainACE • New-EmailTemplate • New-EmailTemplateAttachment • New-GPOLink • New-IntuneAssignment • New-ProtectedSettingsPolicyAssignment • New-ServiceInstance • New-SyncTargetData • New-Trustee • New-VCAce
Push	• Push-Notification
Remove	• Remove-Administrator • Remove-Backups • Remove-IntuneAssignments • Remove-DomainAndObjects • Remove-DomainSecurity • Remove-EmailTemplates • Remove-GPOLink • Remove-Keywords • Remove-LiveEnvironmentSecurity • Remove-Role • Remove-RootContainerAssignment • Remove-User • Remove-ValidScriptExtensions
Reset	• Reset-SynchronizationTargetCredentials

Table 19. Available commands

Type	Available commands
Select	• Select-Approve • Select-Attest • Select-CancelDeployment • Select-CheckIn • Select-Checkout • Select-Cloak • Select-Deploy • Select-Delete • Select-Export • Select-ExportAsDSCResource • Select-ExportAsProtectedSettingsPolicy • Select-Import • Select-ImportSCMBackup • Select-Label • Select-Lock • Select-RecursiveRegistration • Select-RecursiveUnregistration • Select-Register • Select-Reject • Select-RequestApproval • Select-Restore • Select-ScheduledDeploy • Select-SearchAndReplaceGPO • Select-SynchronizeNow • Select-Uncloak • Select-UndoCheckout • Select-Unlock • Select-Unregister • Select-UnregisterAndRemoveHistory • Select-VerifyProtectedSettings • Select-WithdrawApproval • Select-WithdrawApprovalRequest • Select-WorkflowDisabled • Select-WorkflowEnabled

Table 19. Available commands

Type	Available commands
Set	• Set-ApprovalWorkflow • Set-BackupsRetention • Set-BlockKeywordInheritance • Set-BlockProtectedSettingsInheritance • Set-ChangeAuditorDateRange • Set-ChangeAuditorService • Set-CommentMaximumLength • Set-CommentMinimumLength • Set-Compliance • Set-Configuration • Set-ContainerKeywords • Set-ContainerBlockKeywordInheritance • Set-DefaultLinkStateIsEnabled • Set-DSCRootPath • Set-DisableAllGPOWorkflow • Set-EmailTemplate • Set-EnableAssociatedItemIdentification • Set-EnableApprovals • Set-EnableAutomaticDeploymentSynchronization • Set-EnableCustomWorkflowActions • Set-EnableDeploymentFailureAutomation • Set-EnableDSCSupport • Set-EnableGPOSynchronization • Set-EnableProtectedSettings • Set-EnableUnregisteredSOMLinking • Set-EnableWMIFilterReadRestriction • Set-EnforceNamingStandards • Set-EnforceUniqueNames • Set-EnforceUniqueRoleNames • Set-EnsureServiceAccountAccess • Set-ExchangeOptions • Set-EnableFIPSMode • Set-GmailOptions • Set-GPMCVersionCheck • Set-GPOLineage • Set-IntuneOptions • Set-Keywords • Set-License • Set-LoggingOptions • Set-ManagedBy • Set-NotificationEmailAddress • Set-Notifications • Set-OuDisplayFormat • Set-OULinkContainers • Set-PreferredDomainController • Set-ProtectedSettingsBlockedExtensions

Table 19. Available commands

Type	Available commands
Set	• Set-ProtectedSettingsExclusionsRecursion • Set-RemediationRule • Set-Role • Set-Security • Set-SecurityFilter • Set-SMTPOptions • Set-SQLTimeouts • Set-SynchronizationTargets • Set-ValidScriptExtensions
Switch	• Switch-WatcherHashLocation

GPOADmin PowerShell provider extensions

GPOADmin has extended the following standard PowerShell commands:

- New-Item and Remove-Item
- Get-ChildItem and the New-PSDrive

New-Item and Remove-Item

GPOADmin has extended Microsoft's New-Item and Remove-Item PowerShell commands to add the ability to create and delete items from the GPOADmin version control.

Example: Create a container name HR

```
new-item -Path VCRoot:\ -Name HR -ItemType Container
```

Example: Create a GPO name HR_GPO in the HR container

```
new-item -Path VCRoot:\HR -Name HR_GPO -ItemType GPO -Comment "Set the minimum
password length  to 8 characters"
```

Example: Remove the GPO name HR_GPO in the HR container

```
remove-item -Path vcroot:\HR\HR_GPO
```

Example: Remove a container name HR

```
remove-item -Path VCRoot:\HR
```

Get-ChildItem and the New-PSDrive

The GPOADmin PowerShell provider has extended the Get-ChildItem and the New-PSDrive command to include the following parameters:

Table 20. Commands

command	parameters
Get-ChildItem extensions	**NOTE:** If no parameters are specified, then all objects are enumerated and returned. • Container: Returns Version Control containers. • Domain: Returns domain scopes of management. • GPO: Returns Group Policy Objects. • OrganizationalUnit: Returns Organizational Units. • Site: Returns site scopes of management. • SOM: Returns all scopes of management (domain, Organizational Units, and sites). • WMIFilter: Returns WMIFilters. • Count: Instructs the provider to return only the number of specified objects.
New-PSDrive extensions	• Server: Specifies the GPOADmin server service to connect to. • Port: Specifies the port to use when connecting to the specified server.

Table 20. Commands

command	parameters
New-Item	• Path: The fully qualified path to the new item. • ItemTypeName: The type of item to create. Valid values are: ▪ Version Control Root: CONTAINER, GPO, STARTERGPO, WMIFILTER, SCRIPT, and POWERSHELLSCRIPT. ▪ Protected Settings Root: CONTAINER and PROTECTEDSETTINGSPOLICY. • Domain: The domain in which the new item belongs. • Comment: A comment to associate with the creation of this item. • WorkflowDisabled: Creates the item as Workflow Disabled. Valid only with an ItemTypeName of GPO. • StarterGPO: The StarterGPOData representing the StarterGPO to use when creating a new GPO. Valid only with an ItemTypeName of GPO. • WMIFilter: The VersionControlledData representing the WMIFilter to be linked to this item. Valid only with an ItemTypeName of GPO. • Queries: The queries to be associated with this item. Valid only with an ItemTypeName of WMIFILTER • Description: The description for this item. Valid only with an ItemTypeName of WMIFILTER.
Remove-Item	• Comment: A comment to associate with this item.

Using the GPOADmin PowerShell commands (Examples)

The following examples show how to apply PowerShell commands to perform many of the GPOADmin functions. The commands are especially beneficial in environments where repetitive processes are required.

NOTE: All the example commands can be copied word for word and run in the PowerShell window.

NOTE: Some commands may appear more than once in these examples and not all GPOADmin commands are included in the examples in this guide.

NOTE: The examples are based on the commands available in GPOADmin version 5.11 and later. While most of these examples are valid for GPOADmin 5.x, the command names may have changed.

Example commands are included for the following:

- Loading the GPOADmin modules
- Extracting help for GPOADmin commands
- Managing objects
- Gathering object and GPOADmin information
- Utility commands
- Administrative commands
- Protected Settings commands

The ability to use a command is related to the role and user running it. For example, if the user has the User role then the commands they can run are limited to the actions associated with the s assigned to this role. This ensures that workflow, security, and protection are maintained with the commands.

For details on what is available for each role, see Configuring role-based delegation.

Before you can use the examples, you must ensure that you have registered the commands. See Registering the GPOADmin PowerShell commands on page 130.

Loading the GPOADmin modules

Rather than having to remember the module names each time you want to run a command, you can use the following simplify the process.

To load the GPOADmin module

1. On the system where GPOADmin is installed, open PowerShell.
2. To ensure the PowerShell scripts can be run, set the registry value using the following command:

   ```
   Set-Executionpolicy RemoteSigned
   ```
3. Next create a PowerShell profile file, with the following command:

   ```
   New-Item –path $profile -type file –force
   ```
4. Now you are going to put something into the profile file. Enter:

   ```
   notepad $profile
   ```

   This opens the profile file in Notepad so you can enter the following commands:

   ```
   import-module 'C:\Program Files\Quest\GPOADmin\GPOADmin.psd1'
   CD VCRoot:
   get-command -module GPOADmin
   ```

   The first line adds the module, the second changes to the Version Control Root drive used by GPOADmin, and the last one give you a list of all available GPOADmin commands.
5. Save the profile by selecting to save and exit Notepad.
6. Exit or close PowerShell, then open it again.

   The profile loads and displays a list of commands.

Extracting help for GPOADmin commands

The following code first gets all the GPOADmin commands, then creates an output file. The Get-Help command is run for each command with the –Full parameter set to return all help information. Finally, the help is written into the file along with a line used to separate the help for each command. This process continues until all the help is read for the commands.

NOTE: You can run this in a script or in the PowerShell window.

To extract the help for the GPOADmin commands

1. On the system where GPOADmin is installed, open a PowerShell window.
2. Copy the following code and paste it into Notepad to remove any hidden characters.

   Ensure that you copy everything from the $ (dollar sign) to the last } (closing bracket).

   ```
   $x = get-command -Module GPOADmin
   $file = "c:\PowerShell-Help-GPOADmin.txt"
   foreach ($y in $x)
   {
   ```

```
$y.Name.ToUpperInvariant() >> $file
"" >> $file
get-help -Full $y.Name >> $file
"" >> $file

"********************************************************************************
**********" >> $file
"" >> $file
}
```

3 Copy the code from Notepad and paste it into the PowerShell command line, and press Enter.

If you see >>, press Enter again.

Managing objects

The examples in this section include GPOADmin commands used for the day-to-day operations required to manage objects.

- Get information on all GPOs
- Get information for all managed objects
- Get unregistered objects
- Register an object
- Check out an object
- Check in an object
- Undo the check out of an object
- Request approval for changes
- Withdraw an approval request
- Approve changes
- Reject changes
- Withdraw approval on an object
- Deploy an object
- Deploy an object at a future time and date
- Check for pending deployments
- Cancel pending deployment

Get information on all GPOs

This command returns list of GPOs for the specified domain. It includes data for any and all GPOs such as whether it is registered, its name, and other data. The main use of this command to populate an array so that the data can be redirected to another command or used in some other way.

Syntax

```
Get-GPOs [[-Domain] <String>] [-PipelineVariable <String>]
```

Examples

```
Get-GPOs
```

Returns information about GPOs in the current domain.

```
Get-GPOs -Domain AMER.sitraka.com
```

Returns information about GPOs in the domain specified.

Get information for all managed objects

This command returns a list of all the version controlled objects. You can specify different object types, the domain, and get the number of objects for a type.

Syntax

```
Get-AllManagedObjects [-GPOs] [-ProtectedSettings] [-WMIFilters] [-SOMs] [-OUs] [-Domains] [-Sites] [-Scripts] [-SortBy <SortField>] [-Descending] [-Count] [-PipelineVariable <String>]
```

Examples

```
Get-AllManagedObjects
```
Returns a list of all managed objects.

```
Get-AllManagedObjects –GPOs
```

Returns a list of all managed GPO objects.

```
Get-AllManagedObjects –GPOs -Count
```

Returns only the number (count) of all managed GPO objects.

Get unregistered objects

This command returns information on any objects that are not registered in GPOADmin for a specified domain. You can use this information, to now register the objects if necessary. See Register an object.

Syntax

```
Get-Unregistered [-Domain <String>] [-GPOs] [-ProtectedSettings] [-WMIFilters] [-SOMs] [-OUs] [-Domains] [-Sites] [-Scripts] [-SortBy <SortField>] [-Descending] [-Count] [-PipelineVariable <String>]
```

Examples

```
Get-Unregistered
```

Returns information about all unregistered objects in the current domain.

```
Get-Unregistered -Domain AMER.sitraka.com -OUs
```

Returns information about OUs in the domain specified.

Register an object

Before you can control an object in GPOADmin, you must register it. To simplify the process, you can pipe values into this command to register a group of selected objects.

Syntax

```
Select-Register [-VCData] <VersionControllableData> [[-Container] <String>] [[-Comment] <String>] [[-MajorVersion] <Int32>] [[-WorkflowDisabled]] [-PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Examples

```
$unregisteredWMI = Get-Unregistered –WMI
```

```
$registeredWMI = $unregisteredWMI | Select-Register -Container "VCRoot:"
```

The Get-Unregistered places the data about the WMI filters into an array, then this data in used to register all of the WMI filters and puts them into a specific container. The container must be created before using this command.

```
Get-Unregisterd -WMI | Select-Register -Container "VCRoot:\WMI Filters"
```

In this example, the operation is the same as above but it does not place the unregistered objects into a variable first instead it pipes the unregistered WMI filters directly into the Select-Register command.

```
$unregisteredWMI = Get-Unregistered –WMI
$registeredWMI = $unregisteredWMI[4] | Select-Register -Container "VCRoot:"
```

In this example, the unregistered objects are placed into an array of objects. If you enter the array name, it lists all the items in the array. From there you can select a specific object in the array and register it.

NOTE: The number in an array starts at zero so if you want to register the fifth item then you need the offset to be four [4] as seen above.

Check out an object

Use this command to check out an object so you can work on it. A check out is required on any workflow enabled object before you can edit it.

Syntax

```
Select-Checkout [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example

```
$GPO = Get-Item "IE Settings"
Select-CheckOut $GPO
```

The Get-Item command identifies the object to check out. In this case, IE Settings is the GPO that is checked out and available to work on.

Check in an object

Once an object has been checked and worked on, it can be checked back in to the version control system.

Syntax

```
Select-CheckIn [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example:

```
$GPO = Get-Item "IE Settings"
Select-CheckIn $GPO
```

The Get-Item command identifies the object to check in. In this case, IE Settings is the GPO to check back in after having worked on it.

Undo the check out of an object

If you have an object checked out and realize that you do not need to work on it, do not want to save your changes, or have checked out the wrong object, you can undo the checkout. This checks the object back into the Version Controlled Root and disregard any changes.

Syntax

```
Select-UndoCheckout [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example

```
$GPO = Get-Item "IE Settings"

Select-UndoCheckout $GPO
```

The Get-Item command identifies which object to undo the check out for. In this case, IE Settings is the GPO you want to check back in and set back to its original condition without any changes.

Request approval for changes

When an object has workflow enabled it may require approvals to commit the changes and eventually deploy the object. To get this approval for changes, a request needs to be made to the approval authority.

Syntax

```
Select-RequestApproval [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example

```
$GPO = Get-Item "IE Settings"

Select-RequestApproval $GPO
```

The Get-Item command identifies the object for which the approval is requested. In this case, IE Settings is the GPO you want to get approval for because of the changes that have been made.

Withdraw an approval request

If you realize there is an issue with changes you have you made to an object, you can withdraw the request for approval on the changes. This is a straight forward process and easy to accomplish.

Syntax

```
Select-WithdrawApprovalRequest [-VCData] <VersionControlledData> [[-Comment]
<String>] [-PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example

$GPO = Get-Item "IE Settings"

Select-WithdrawApprovalRequest $GPO

The Get-Item command identifies the object for which to withdraw the request. In this case, IE Settings is the GPO you want to withdraw the request for.

NOTE: You can use the comments in the object history to explain the reason for the withdraw of the request.

Approve changes

After the changes have been checked and the approver is satisfied with the changes, they can approve the changes which will move it along in the workflow process to deployment.

Syntax

```
Select-Approve [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example

```
$GPO = Get-Item "IE Settings"
```

```
Select-Approve $GPO
```

The Get-Item command identifies the object to approve. In this case, IE Settings is the GPO to approve because the changes are correct.

Reject changes

Along with approving the changes to an object there may be situations where you want to reject the change. This could be due to numerous reasons such as the changes made to the object conflict with another object or a company policy.

Syntax

```
Select-Reject [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example:

```
$GPO = Get-Item "IE Settings"
```

```
Select-Reject $GPO
```

The Get-Item command identifies the object to reject. In this case, IE Settings is the GPO you want to reject because the changes are not correct.

You can use the comment to explain the reason for the rejection.

Withdraw approval on an object

Even at the point just before deployment of the object, you can stop the process by withdrawing the previous approval for an object.

Syntax

```
Select-WithdrawApproval [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example

```
$GPO = Get-Item "IE Settings"
```

```
Select-WithdrawApproval $GPO
```

The Get-Item command identifies the object for which to withdraw approval. In this case, IE Settings is the GPO you want to withdraw the approval for because the changes are not correct. The object reverts to the Pending Approval state.

NOTE: The comment can be used to explain the reason for withdrawing the approval.

Deploy an object

Once changes have been approved, the next step in the process is to deploy the object to the live environment for use.

Syntax

```
Select-Deploy [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example

```
$GPO = Get-Item "IE Settings"
```

```
Select-Deploy $GPO
```

The Get-Item command identifies the object to deploy. In this case, IE Settings is the GPO to deploy to the live environment.

Deploy an object at a future time and date

Deploying an object to the live environment can also be done at a future time and date.

Syntax

```
Select-ScheduledDeploy [-DeploymentTime] <DateTime> [-TimeZoneId] <String> [-VCData]
<VersionControlledData> [[-Comment] <String>] [-PipelineVariable <String>] [-WhatIf]
[-Confirm]
```

Example

```
$item = Get-Item "IE Settings"
```

```
Select-ScheduledDeploy -VCData $item -DeploymentTime "11/30/2016 12:00AM" -
TimeZoneId "GMT Standard Time" -Comment "Scheduled for Nov 30th, 2016 GMT"
```

The Get-Item command identifies the object to deploy. In this case, IE Settings is the GPO you want to the live environment at a future time and date.

Check for pending deployments

If you are unsure whether you have any pending deployments, you can use this command to return all pending deployments or just return any deployments related to specific object such as GPOs or WMI Filters.

Syntax

```
Get-PendingDeployment [-GPOs] [-ProtectedSettings] [-WMIFilters] [-SOMs] [-OUs] [-
Domains] [-Sites] [-Scripts] [-SortBy <SortField>] [-Descending] [-Count] [-
PipelineVariable <String>]
```

Examples:

```
Get-PendingDeployment
```

Returns a list of all of the pending deployments awaiting execution.

```
Get-PendingDeployment -GPOs
```

Returns a list of all of the pending GPO deployments awaiting execution.

Cancel pending deployment

If there is an issue with a pending deployment, you can easily cancel it. .

You need to know the object that is to be deployed

Syntax

```
Select-CancelDeployment [-VCData] <VersionControlledData> [[-Comment] <String>] [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Example

```
$GPO = Get-Item "IE Settings"
```

```
Select-CancelDeployment $GPO
```

The Get-Item command identifies the object for which you want to cancel the deployment. In this case, IE Settings is the GPO you want to cancel the deployment of to the live environment.

Gathering object and GPOADmin information

The examples in this section provide addition information on objects you are working with or GPOADmin in general.

- Identify which objects are checked out
- Identify which objects are checked out to me
- What are the properties of an object
- What objects are available
- What objects are checked out

Identify which objects are checked out

You may want to know which objects in the Version Control are checked out. You can specify the type of object such as OU and SOMs. This command provides a list of check out objects.

Syntax

```
Get-CheckedOut [-GPOs] [-ProtectedSettings] [-WMIFilters] [-SOMs] [-OUs] [-Domains] [-Sites] [-Scripts] [-SortBy <SortField>] [-Descending] [-Count] [-PipelineVariable <String>]
```

Examples

```
Get-CheckedOut
```

Returns a list of all objects giving the type and version of the object.

```
Get-CheckedOut -GPOs
```

Returns a list of all GPOs which are checked out.

Identify which objects are checked out to me

You may want to know which objects in the Version Control are checked out specifically by you. You can specify the type of object such as GPOs and WMI Filter. This command provides a list of check out objects.

Syntax

```
Get-CheckedOutToMe [-GPOs] [-ProtectedSettings] [-WMIFilters] [-SOMs] [-OUs] [-Domains] [-Sites] [-Scripts] [-SortBy <SortField>] [-Descending] [-Count] [-PipelineVariable <String>]
```

Examples:

```
Get-CheckedOutToMe
```

Returns a list of all objects giving the type and version of the object that are specifically checked out by you.

```
Get-CheckedOutToMe -GPOs
```

Returns a list of all GPOs which are specifically checked out by you.

What are the properties of an object

The Get-Properties command returns the properties for a specified object. This can be useful when you want to know specific information on an object.

Syntax

```
Get-Properties [-VCData] <VersionControlledData> [-PipelineVariable <String>]
```

Examples

```
Get-Item "IE Settings" | Get-Properties
```

The Get-Item command identifies the object for which to get the properties. The object data is then piped into the Get-Properties command and the properties for that object are displayed.

The piping works the same as the following command. It is just a quicker way of executing the command by taking advantage of the piping feature in PowerShell.

```
$GPO = Get-Item "IE Settings"
```

```
Get-Properties $GPO
```

The Get-Item command identifies the object and is stored in a variable. The Get-Properties command is called with the variable and the properties for that object are displayed.

What objects are available

The Get-Available command returns the objects that are available. This can be useful when you want to know which objects are available to edit.

Syntax

```
Get-Available [-GPOs] [-ProtectedSettings] [-WMIFilters] [-SOMs] [-OUs] [-Domains]
[-Sites] [-Scripts] [-SortBy <SortField>] [-Descending] [-Count] [-PipelineVariable
<String>]
```

Examples

```
Get-Available
```

Returns a listing of all the objects that are available for edit.

```
Get-Available -GPOs
```

Returns a listing of all the GPOs that are available for edit.

What objects are checked out

The Get-CheckedOut command returns the objects which are checked out. This can be useful when you want to know which objects are being edited.

Syntax

```
Get-CheckedOut [-GPOs] [-ProtectedSettings] [-WMIFilters] [-SOMs] [-OUs] [-Domains]
[-Sites] [-Scripts] [-SortBy <SortField>] [-Descending] [-Count] [-PipelineVariable
<String>]
```

Examples

```
Get-Available
```

Returns a listing of all the objects with a status of checked out and are being edited.

```
Get-Available -GPOs
```

Returns a listing of all the GPOs that are checked out.

Utility commands

The examples in this section demonstrate basic GPOADmin utility commands. Administrative actions usually require administrative privileges.

- Gather GPOADmin license information
- Install a GPOADmin license
- Get logging options
- Set logging options
- Get notifications
- Set notifications on objects

Gather GPOADmin license information

This command returns the license used by GPOADmin.

Syntax

```
Get-LicenseInfo [-PipelineVariable <String>]
```

Examples

```
Get-LicenseInfo
```

Return information about the license currently installed in GPOADmin.

Install a GPOADmin license

This command allows the installation or update of the license for GPOADmin.

Syntax

```
Set-License [-LicenseFile] <String> [-PipelineVariable <String>] [-WhatIf] [-
Confirm]
```

Example

```
Set-License c:\Licenses\GPOADmin_5.x.dlv
```

Installs the license specified and returns the info about the license.

Get logging options

This command returns the logging info currently used for GPOADmin.

Syntax

```
Get-LoggingOptions [-PipelineVariable <String>]
```

Example

```
Get-LoggingOptions
```

Returns the logging information.

Set logging options

This command sets the current logging options. Only a GPOADmin administrator can run this command.

Syntax

```
Set-LoggingOptions [-Location] <LogLocation> [-CategoriesToWrite] <EventCategories>
[[-Path] <String>] [-PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Examples

```
Set-LoggingOptions -Location None -CategoriesToWrite None
```

Disables the logging.

```
Set-LoggingOptions -Location EventLog -CategoriesToWrite UserAction, ServiceAction,
Error
```

Logs user actions, service actions, and errors to the event log.

```
Set-LoggingOptions -Location EventLog, File -CategoriesToWrite UserAction,
ServiceAction, Error -Path c:\Logs
```

Logs user actions, service actions, and errors to the event log and a file in c:\logs directory.

Get notifications

This command returns the notification list enabled on an object, user, or container. The list also displays if the notification was inherited and where the inheritance is from.

Syntax

```
Get-Notifications [[-VCData] <VersionControlledData>] [[-Account] <String>] [[-
Container] <String>] [-PipelineVariable <String>]
```

Examples

```
Get-Notifications
```

Returns the notifications for the current container where the command is run.

```
Get-Notifications -Account AMER\Administrator
```

Returns the notifications for the user specified.

```
$gpo = Get-Item "IE Settings"
Get-Notifications -VCData $gpo -Account AMER\Administrator
```

Returns all the notifications the AMER\Administrator has subscribed to for the version controlled object "IE Settings”.

```
Get-Notifications -Container "VCRoot:\Accounting" -Account domain\jdoe
```

Returns all the notifications that domain\jdoe has subscribed to for the container "VCRoot:\Accounting".

Set notifications on objects

This command sets the notification list enabled on an object, user, or container.

Syntax

```
Set-Notifications [[-VCData] <VersionControlledData>] [[-Account] <String>] [[-
Container] <String>] [-Notifications] <String[]> [-PipelineVariable <String>] [-
WhatIf] [-Confirm]
```

Examples

```
Set-Notifications -Notifications "Register", "Unregister"
```

Subscribes the currently connected user to the "Register" and "Unregister" notifications for the current container. In this case "VCRoot".

```
Set-Notifications -Account AMER\Administrator -Notifications "Register",
"Unregister"
```

Subscribes AMER\Administrator to the "Register" and "Unregister" notifications for the version controlled object "IE Settings"

```
$gpo = Get-Item "IE Settings"
Set-Notifications -VCData $gpo -Account AMER\Administrator -Notifications
"Register", "Unregister"
```

Subscribes AMER\Administrator to the "Register" and "Unregister" notifications for the version controlled object "IE Settings"

```
Set-Notifications -Container "VCRoot:\Accounting"  -Account AMER\jdoe -Notifications
"Register", "Unregister"
```

Subscribes AMER\jdoe to the "Register" and "Unregister" notifications for the container "VCRoot:\Accounting".

Administrative commands

The examples in this section deal with some of the basic GPOADmin administrative commands.

- Approval workflow information
- Set the approval workflow
- Identify user accounts
- Identify user roles
- Modify a role
- Add a role
- Get an object's security
- Set an object's security
- Overwrite a GPOs security filter

Approval workflow information

This command gets the approval workflow for the specified object. This is used to confirm who has the responsibility to approve actions for create, modify, and delete. This is usually applied to a container.

Syntax

```
Get-ApprovalWorkflow [-Path] <String> [-Action] <ActionType> [[-Raw]] [-
PipelineVariable <String>]
```

Examples

```
Get-ApprovalWorkflow VCRoot:\IE_Settings Create
```

Retrieves the create approval workflow for the IE_Settings container.

```
Get-ApprovalWorkflow VCRoot:\IE_Settings Create -Raw
```

Retrieves the create approval workflow for the IE_Settings container in its raw format.

Set the approval workflow

Sets the approval workflow for the specified container.

Syntax

```
Set-ApprovalWorkflow [-Path] <String> [-Action] <ActionType[]> [[-ApprovalWorkflow]
<String>] [-PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Examples

```
Set-ApprovalWorkflow VCRoot:\IE_Settings Create
"AMER\CreateReviewers,1|AMER\CreateApprover,0"
```

Sets the create approval workflow for the IE_Settings container. The group AMER\CreateReviewers requires one approver and the group AMER\CreateApprover requires no approvers.

```
Set-ApprovalWorkflow -Path "VCRoot:\IE_Settings" -Action "Create", "Delete", "Edit"
-ApprovalWorkflow "AMER\CreateReviewers,1|AMER\CreateApprover,0"
```

Sets the create, delete, and edit approval workflow for the IE_Settings container. The group AMER\CreateReviewers requires one approver and the group AMER\CreateApprover requires no approvers.

Identify user accounts

Gets the list of available s for the logged on user.

Syntax

```
Get-s [-PipelineVariable <String>]
```

Example

```
Get-s
```

Gets the list of available s.

Identify user roles

Gets a list of the currently defined roles within GPOADmin. There are three default roles which cannot be changed.

Syntax

```
Get-Roles [-PipelineVariable <String>]
```

Example

```
Get-Roles
```

Gets a list of all the currently defined roles within GPOADmin.

Modify a role

Modifies the properties of the specified user-defined role. The three default roles, System Administrator, Moderator and User cannot be changed.

Syntax

```
Set-Role [-Role] <RoleData> [[-DisplayName] <String>] [[-Description] <String>] [[-
s] <[]>] [-PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Examples

```
$roles = Get-Roles
```

```
Set-Role -Role $roles[3] -DisplayName Linkers
```

The Get-Roles stores the roles into an array. The Set-Role command updates the display name of the role in role[3] to Linkers. The array counts from zero and not from one. The first role is zero, the second is one.

```
$roles = Get-Roles
```

```
Set-Role -Role $roles[3] -Description "Users of this role can link Group Policy
Objects to Scopes of Management"
```

Updates the description of the role "Linkers".

```
$roles = Get-Roles
```

```
Set-Role -Role $roles[3] -s "Read, Link"
```

Updates the s of the role "Linkers".

Add a role

Adds a role to GPOADmin with the specified name, description, and s. Only a GPOADmin administrator can run this command.

Syntax

```
Add-Role [-Name] <String> [[-Description] <String>] [-s] <String[]> [-
PipelineVariable <String>] [-WhatIf] [-Confirm]
```

Examples

```
$s = "BlockInheritance", "Link"
```

```
Add-Role "Linker" "Can link GPOs to SOMs" $s
```

This first creates an array of s. You can use the Get-s command to retrieve a list of available s. Next the Linker role is defined, created, and the s are applied.

```
Add-Role -Name "Register Role" -Description "Can register objects" -s "Register",
"Unregister"
```

List of s can be added in-line instead of using a variable.

Get an object's security

Gets the security on the specified version controlled object. Security is set either to a container or directly on an object.

Syntax

```
Get-Security [-Path] <String> [[-IncludeInheritedAce]] [-Raw] [-PipelineVariable
<String>]
```

Examples

```
Get-Security -Path "VCRoot:\IE Settings"
```

Gets the security set on the "VCRoot:\IE Settings" object.

```
Get-Security -Path "VCRoot:\IE Settings" -IncludeInheritedAce
```

Gets the security set on the "VCRoot:\IE Settings" object including inheritance.

```
Get-Security -Path "VCRoot:\IE Settings" -IncludeInheritedAce -Raw
```

Gets the security set on the "VCRoot:\IE Settings" object including inheritance in its raw format.

Set an object's security

Sets the security on the specified version controlled object.

NOTE: This overwrites the existing security set on the object.

Syntax

```
Set-Security [-Path] <String> [-Acl] <VersionControlAce[]> [-PipelineVariable
<String>] [-WhatIf] [-Confirm]
```

Examples

```
$roles = get-roles
```

```
$ace1 = New-VCAce AMER\Administrator $roles[3]
```

```
$ace2 = New-VCAce AMER\jdoe $roles[3]
```

```
Set-Security -Path "VCRoot:\IE Settings" -Acl $ace1, $ace2
```

Sets the security on the specified version controlled object.

Overwrite a GPOs security filter

Overrides the security filter of the specified GPO.

Examples

To add a user or group:

- Use the Get-SecurityFilter command to store the result in a variable.
- Use the New-Trustee command to create a trustee object from the account name specified in the domain\account format and store this in a variable.
- Add the trustee variable to the existing security filter.
- Use the Set-SecurityFilter command and pass the new security filter.

```
$gpo = Get-Item VCRoot:\SOME_GPO
```

```
$filter = Get-SecurityFilter $gpo
```

```
$trustee = New-Trustee domain\user

$filter.Add($trustee)

Set-SecurityFilter $gpo $filter
```

To remove a specific trustee from the security filter, use the Get-SecurityFilter command and store the result in a variable. The result is a zero based list. If you know the index of the trustee you want to remove, use the RemoveAt command on the list.

```
$gpo = Get-Item VCRoot:\SOME_GPO

$filter = Get-SecurityFilter $gpo

$filter.RemoveAt(1)

Set-SecurityFilter $gpo $filter
```

If you know the name, you can first search for the trustee and store the account in a variable then user the Remove command.

```
$gpo = Get-Item VCRoot:\SOME_GPO

$filter = Get-SecurityFilter $gpo

$trustee = $filter | where{$_.Name -eq 'domain\user'}

$filter.Remove($trustee)

Set-SecurityFilter $gpo $filter
```

Protected Settings commands

The examples in this section deal with some of the basic GPOADmin Protected Settings commands. Protected Settings policies contain settings that you want to control. They are protected in the sense that they contain and identify the settings that may not be altered by users. This provides an added level of security for the policies within your organization. If a user attempts to create, edit, or remove the flagged settings they are stopped.

- Gather Protected Settings information
- Enable and disable Protected Settings
- Get a list of Protected Settings
- Add Protected Settings

Gather Protected Settings information

Returns the status of the "Enable Protected Settings for Group Policy Objects." option. The command informs you if the Protected Settings are enabled.

Syntax

```
Get-EnableProtectedSettings [-PipelineVariable <String>]
```

Example

```
Get-EnableProtectedSettings
```

Returns the status of the "Enable Protected Settings for Group Policy Objects." option.

Enable and disable Protected Settings

This command sets the status of the "Enable Protected Settings for Group Policy Objects." option. If true, then GPO settings are verified against Protected Settings policies during check-in. Only a GPOADmin administrator can run this command.

Syntax

```
Set-EnableProtectedSettings [[-EnableProtectedSettings]] [-PipelineVariable
<String>] [-WhatIf] [-Confirm]
```

Examples

```
Set-EnableProtectedSettings
```

Disables the Protected Settings for GPOs.

```
Set-EnableProtectedSettings –EnableProtectedSettings
```

Enables the Protected Settings for GPOs

Get a list of Protected Settings

Use this command to get a list of all Protected Settings policies assigned to the specified container. The 'Enable Protected Settings for Group Policy Objects' must be enabled for this command to return the list. Otherwise a warning stating the Protected Settings feature is not enabled is displayed.

Syntax

```
Get-AssignedProtectedSettingsPolicies [-Container] <VersionControlContainerData> [-
PipelineVariable <String>]
```

Examples

```
Get-Item . | Get-AssignedProtectedSettingsPolicies
```

Gets a list of all Protected Settings Policies assigned to the current container.

```
Get-Item "VCRoot:\Locations" | Get-AssignedProtectedSettingsPolicies
```

Gets a list of all Protected Settings Policies assigned to the "Locations" container.

Add Protected Settings

You can add the Protected Settings policy to a container. This command requires the "Modify Protected Settings Assignments" . First you need to have a Protected Setting object configured with the setting you want to check against, then set up the assignment information, and apply it to a container.

Syntax

```
Add-ProtectedSettingsPolicies [-Container] <VersionControlContainerData> [-
ProtectedSettingsPolicies] <ProtectedSettingsPolicyAssignment> [-PipelineVariable
<String>] [-WhatIf] [-Confirm]
```

Examples

```
$PSP = Get-ProtectedSettingsPolicies | ? {$_.Name -eq "PROT_01"}

$assignment = New-ProtectedSettingsPolicyAssignment -ProtectedSettingsPolicy $PSP -
ValidationRule Value

get-item .\locations | Add-ProtectedSettingsPolicies -ProtectedSettingsPolicies
$assignment
```

Adds the "PROT_01" Protected Settings object to the container "Locations" with a Validation Rule of "Value".

6

Appendix: GPOADmin Event Log

- What is the GPOADmin event log?
- Interpreting the GPOADmin event log
- Example GPOADmin events

What is the GPOADmin event log?

You can configure GPOADmin's event notification system to notify you of actions such as register, check in and check out. You can find details on configuring the event notification system in the section titled Selecting events on which to be notified.

The GPOADmin event log can be searched and filtered.

See also Event ID types.

Interpreting the GPOADmin event log

GPOADmin logs events in the following format:

Table 21. Log Format

Information Item	Purpose
Level	The event severity levels are: • Information • Warning • Error
Source	Indicates the GPOADmin application or associated GPOADmin service generating the event: • GPOADmin • Quest GPOADmin Watcher Service • Quest GPOADmin Service
Event ID	A code you can use to look up the type of event. See Event ID types on page 163 for a list of event IDs.
Task Category	Provides additional information about the event ID. • 0 – None • 1 – User action – check in, check out, and so on. • 2 – Service Action – startup, shutdown, and so on. • 4 – Error – an error has occurred. • 8 – Troubleshooting
Description	Provides detailed information about the event. It may include an object's name, the action performed on the object (such as check in or deployed) and by whom, as well as any other information relating to the event.

Event ID types

The Event IDs generated by GPOADmin are broken into the following types:

Event ID	Description
0	Associated with the GPOADmin Server Service
1000	Request
1001	Deploy
1002	Approve
1003	Reject
1004	Create

Event ID	Description
1005	Check Out
1006	Check In
1007	Move
1008	Undo check out
1009	Register
1010	Unregister
1011	Modify Security
1012	Withdraw Approval
1013	Withdraw Approval Request
1014	Compliance Action
1015	Create Container
1016	Delete Container
1017	Edit Container
1018	Modify Container Security
1019	Disable Workflow
1020	Enable Workflow
1050	The Watcher Service
1100	Email Message: "SMTP Host is undefined"
1150	Email Message: Exceptions
2001	Error importing settings to object
2002	Various generic exception messages
2004	Various generic exception messages
2005	Various generic exception messages
2006	Various generic exception messages
2007	Various generic exception messages
2010	Problem with Access Control List (ACL) attribute.
2013	GPOADmin server process – Information
2014	GPOADmin server process – Errors
2015	Custom Workflow Action process – Standard Output stream
2016	Custom Workflow Actions process – Error stream
2245	Problem with Read Only domains or a problem with the version control containers.
3060	Connect to and disconnect from GPOADmin.
5000	Problem with the license – error code and error message
5000-2086928381	Invalid license – wrong product
5000-2086928382	Invalid license – demo expired
5000-2086928383	Invalid license – license expired
5000-2147467259	Invalid license
6010	Collector initialization
6015	Polling interval set
6040	Failed to load configuration file
6045	Problem loading configuration file
6046	Configuration file corrupt

Event ID	Description
6047	Configuration file missing
6050	Error adding items to collection
6060	Configuration file deleted
6065	Configuration file renamed
6066	Configuration file name restored
6070	Configuration file restored
6100	Error during search
6101	Error during collection of object for GPO Statistics
6102	Error during parsing of objects for GPO Statistics

Example GPOADmin events

The following table illustrates how events display in your log.

Table 22. Log Events

LEVEL	SOURCE	EVENT ID	TASK CATEGORY	DESCRIPTION
Information	GPOADmin	1050	2	The change is an authorized change made by GPOADmin on a working copy.
Warning	GPOADmin	1050	2	Unable to locate any domain controllers to monitor.

7

Appendix: GPOADmin Backup and Recovery Procedures

- GPOADmin Backup Requirements
- Restoring GPOADmin

GPOADmin Backup Requirements

As part of your normal disaster procedures or requirements, GPOADmin should be considered for inclusion. In the event of a computer or network failure, the GPOADmin deployment and its data can be restored if you have performed regular and distributed backups of the following:

- The GPOADmin configuration store.
- The GPO backups store.

During the initial installation of GPOADmin, you must specify where to place these two items within your environment. The configuration store can reside in either Active Directory or AD LDS. The GPO backup store can be in Active Directory, AD LDS, a network share, or on a SQL server. The recommended location is on a network share.

Each of these options has its own backup strategies and requirements and should be included in your regular backup schedule.

NOTE: While GPOADmin is inaccessible, you can manage GPOs through the Group Policy Management Console (GPMC).

Restoring GPOADmin

Once you have performed the required recovery procedures listed below, simply reinstall GPOADmin, configure the services to use the recovered stores and resume the management of GPOs. For configuration details, see Configuring the Version Control server.

Any policies that were checked out, checked in, or pending approval up to the time of the last backup will be not be affected by the failure.

To restore the ADLDS instance

- For information on how to backup Microsoft AD LDS see: https://technet.microsoft.com/en-us/library/cc794761(v=ws.10).aspx or Microsoft TechNet.

To restore the file share

- Follow your internal procedure for recovering files and folders.

  If you plan to use a new host computer for the GPOADmin backup store, or the host computer has been renamed, please contact Quest Customer Support for assistance.

8

Appendix: Customizing your workflow

- What is a custom workflow action?
- Working with custom workflow actions in the Version Control system
- Working with the custom workflow actions xml file
- Troubleshooting custom workflow actions

What is a custom workflow action?

You can extend GPOADmin's version control system to incorporate customized actions based on your organizations existing workflow. This allows you to customize and control the deployment of controlled objects (such as GPOS, SOMs, and WMI filters) to meet your individual needs. For example, you can configure a pre-action to send the help desk distribution list an email each time a GPO change is requested.

Also, if you have a workflow tool in place that encompasses many different organizational tools you no longer need to use the workflow in both applications. With pre and post actions, a GPO check out, modification, and request for approval can be configured to create a ticket in an existing workflow system. Subsequent approval in the external workflow system can be configured to approve and deploy that same policy in GPOADmin. A post action can be configured to add additional ticket information about the deployment of the GPO into the customers external workflow application.

Custom actions are available on the following Version Control actions:

Action	Runs when...
Approve	A change to a version controlled object is approved.
CancelScheduledApproval	A version controlled object's scheduled deployment has been canceled.
CheckIn	A version controlled object is checked in.
CheckOut	A version controlled object is checked out.
Cloak	A version controlled object has been cloaked.
ComplianceAction	Either a "Rollback" or "IncoporateLive" compliance action is performed.
Create	A version controlled object has been created.
Delete	A version controlled object has been deleted.
Deploy	A version controlled object has been deployed into the live environment.
DisableWorkflow	A version controlled object has been workflow disabled.
Edit	A version controlled object has been modified.
EnableWorkflow	A version controlled object has been workflow enabled.
Label	A label has been applied to one or more version controlled objects.
Lock	A version controlled object has been locked.
ModifySecurity	The security has been modified on a version controlled object.
Move	A version controlled object is moved.
Register	An object is registered with the version control system.
Reject	A change to a version controlled object is rejected.
Rename	A version controlled object is renamed.
RequestApproval	An approval for a version controlled object is requested.
Restore	A version controlled object has been restored.
SubmitScheduledApproval	A version controlled object has been scheduled for deployment.
Synchronization	A version controlled Group Policy Object has been synchronized with another Group Policy Object.
ToggleApprovalWorkflow	Toggles a version controlled object between workflow enabled and disabled.
Uncloak	A version controlled object has been uncloaked.
UndoCheckOut	A version controlled object's checkout is undone.
Unlock	A version controlled object has been unlocked.
Unregister	A version controlled object is unregistered.
WithdrawApproval	An approval on a version controlled object is withdrawn.
WithdrawApprovalRequest	A request for approval has been withdrawn.

Working with custom workflow actions in the Version Control system

GPOADmin provides an easy to use editor to help you set up and configure your custom actions.

Each custom workflow action has two phases; pre-actions (processed prior to the version control action being run), and post-actions (processed after the version control action has run.

Whether or not an action is processed can be controlled by the use of conditions. This must be set through the editing the xml file directly. For details see, Conditions on page 175.

GPOADmin includes a sample custom workflow to get you started that shows how to incorporate the creation of Help desk ticket with each approval request generated from the Version Control system.

To access the sample custom workflow template

1. Right-click the forest, and select **Properties**.
2. Select **Options | General | Enable the processing of custom workflow actions**, and select **Launch Editor.**
3. In the editor, select File \ Open and select the CustomWorkflowActions.xml file located in the installation directory. (C:\Program Files\Quest\GPOADmin\Examples)
4. Select the **Request approval | Pre-Action** to view the sample.

To create a new custom workflow action

1. Right-click the forest, and select **Properties**.
2. Select **Options | General | Enable the processing of custom workflow actions**, and select **Launch Editor.**
3. Select the required action and click the **Pre-Actions** option.
4. Enter a name and comment for the action.
5. If desired, select the **Stop on error** option, and optionally add a custom error message. This will instruct the service to stop all processing for the current object when an error occurs.
6. Enter the location or browse to the required application to run.
7. Enter the required parameters in the Parameters window. To insert a tag, right-click in the Parameters window, select **Insert Tag**, and choose the required tag. For details on the available options, see Predefined Tags on page 173.
8. If required, select the **Post-Actions** tab and configure its options.
9. Click **Add**.
10. Once you have entered all the required pre and post actions, save your workflow.

NOTE: Because custom workflow actions are performed in the background by the GPOADmin service, they will not be visible from the interface and depending on the number and complexity of scripts defined for a given action, there may be a delay as the custom actions are being processed by the server.

When required, you can suspended custom workflow actions through the Server options.

11. When you are ready to deploy the workflow, select **Enable the processing of custom workflow actions**.

To edit a custom workflow action

1. Right-click the forest, and select **Options**.
2. Select **Options | General | Enable the processing of custom workflow actions**, and select **Launch Editor.**

3 Select the required action and pre or post action.

4 Edit the action as required. You can:

   a Change the name, comment, executable, and parameters.

   b Right-click and add or remove actions.

   c Right-click and adjust the order in which they are performed.

   d Copy and past actions.

5 When you have made all your changes, click **Update**.

To pause or stop the custom workflow action

1 Right-click the forest, and select **Options**.

2 Select **Options | General | Enable the processing of custom workflow actions**, and select **Launch Editor.**

3 Click to disable the custom workflow actions option.

Working with the custom workflow actions xml file

Custom workflow actions are defined in an XML file (CustomWorkflowActions.xml) which must be located in the same directory as the GPOADmin Service executable.

- Actions
- Predefined Tags
- Conditions
- Example of a complete pre-action

Actions

For a list of available actions, see What is a custom workflow action? on page 169. Custom workflow actions are defined in the CustomWorkflowActions.xml file as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
  </CheckIn>
</CustomWorkflowActions>
```

NOTE: Actions names are case sensitive.

PreActions and PostActions

The PreActions and PostActions are defined as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
    <PreActions/>
```

```
    <PostActions/>
  </CheckIn>
</CustomWorkflowActions>
```

Each phase may contain one or more actions with the following properties:

Table 23. Properties

Property	Description
Name	Identifies the action.
Comment	Describes the action.
StopOnErrors	Instructs the service to stop all processing for the current object when an error occurs.

The properties are defined as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
    <PreActions>
      <Action Name="CheckIn pre-action" Comment="A custom action."
StopOnError="false">
      </Action>
    </PreActions>
    <PostActions>
    </PostActions>
  </CheckIn>
</CustomWorkflowActions>
```

Each action also contains the following nodes:

Table 24. Nodes

Action	Description
Executable	The full path to the executable.
Parameters	The list of parameters to pass to the executable.
Conditions	A list of conditions which determine whether or not to process the action.

The nodes are defined as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
    <PreActions>
      <Action Name="CheckIn pre-action" Comment="A custom action."
StopOnError="false">
        <Executable>c:\windows\system32\cmd.exe</Executable>
        <Parameters>/C mkdir "c:\GPOSettingsReports\CheckIn"</Parameters>
        <Conditions>
        </Conditions>
      </Action>
    </PreActions>
    <PostActions>
    </PostActions>
  </CheckIn>
</CustomWorkflowActions>
```

Predefined Tags

Tags are typically replaced with their corresponding values by the service. However, there are cases where the tags will not be converted. For example, if a comment is not specified during the version control action then the [COMMENT] tag will be empty; or if the object is not checked out then the [TRUSTEENAME] and [TRUSTEESID] will be empty.

Keep in mind that in some cases the tags will always be empty as is the case of a pre-action for the Register version control action. At the time the pre-action is processed, the corresponding version control information would not exist.

NOTE: Tags must be uppercase and enclosed in square brackets.

Parameters and conditions support the following predefined tags:

Table 25. Available tags

Tag	Description
[ACTION]	The currently executing version control action.
[VCID]	The version control identifier of the current object.
[DOMAINNAME]	The name of the domain for the current object.
[FULLPATH]	The full path of the current object in the version control system.
[ID]	The identifier for the current object.
[LASTBACKUPID]	The identifier of the last backup for the current object.
[NAME]	The name of the current object.
[STATUS]	The version control status for the current object. See Status values for more information.
[SUBSTATUS]	The version control sub status for the current object.See Sub status values for more information.
[TRUSTEENAME]	The name of the user the current object is checked out to.
[TRUSTEESID]	The SID of the user the current object is checked out to.
[TYPE]	The version control type of the current object.
[VERSION]	The version of the current object.
[COMMENT]	The comment associated with the version control action.

Sub status values

The possible values of a registered object's sub status include the following:

Table 26. Substatus values

Value	Description
None	Default.
Register	Registers objects with the version control system.
Unregister	Unregisters objects from the version control system.
CheckIn	Save edits made to an object in the version control system.
CheckOut	Prepares an object in the version control system for editing.
UndoCheckOut	Discards change made to an object in the version control system.
RollBack	Restores an object in the version control system to a previous known state.
Restore	Restores an object in the version control system to a previous known state.
Get	Overwrites the current settings of an object in the version control system with settings from a previous known sate.

Table 26. Substatus values

Value	Description
Import	Overwrites the current settings of an object in the version control system with settings from a previous backup.
IncorporateLive	Overwrites the current settings of an object in the version control system with those from the live environment.
Create	Creates a new object in the version control system.
Branch	Branch on object.
Edit	Edits an object in the version control system.
Delete	Marks an object in the version control system as deleted.
Approve	Approves changes made to an object in the version control system.
Reject	Rejects changes made to an object in the version control system.
RequestApproval	Request approval for changes made to an object in the version control system.
ApplyPolicyTemplate	Applies a template to a policy in the version control system.
Label	Labels objects in the version control system.
Lock	Locks an object in the version control system.
Unlock	Unlocks an object in the version control system.
Cloak	Cloaks an object in the version control system.
Uncloak	Uncloaks an object in the version control system.
EnableWorkflow	Forces the object to follow version control workflow.
DisableWorkflow	Allows the object to not follow version control workflow.
Move	Moves an object from one container to another in the version control system.
WithdrawApproval	Withdraws approval of changes for an object in the version control system.
WithdrawApprovalRequest	Withdraws an approval request for changes to an object in the version control system.
Rename	Renames an object in the version control system.
SubmitScheduledApproval	Submits approval for scheduled deployment of an object in the version control system.
CancelScheduledApproval	Cancels a scheduled deployment of an object in the version control system.
Deploy	Deploys an object in the version control system to the live environment.
Link	Links a policy object to a scope of management in the version control system.
LinkUpdate	Updates the links on a scope of management.
ComplianceAction	An action which affects the compliance of an object in the version control system.
ModifySecurity	Modifies the security of an object in the version control system.
UnauthorizedModifications	A backup of a noncompliant object. This is intended to be done by the Watcher Service.
MigrationAction	Indicates an import from NetPro GPOADmin. This is intended to be done by the Migration Wizard.
Synchronization	Synchronizes a source object to one or more targets of the same type.
ToggleApprovalWorkflow	Toggles the order of approval workflow processing.
FailedDeployment	A deployment has failed.

Status values

The possible values of a version controlled object's status include the following:

Table 27.

Status Value	Description
Unregistered	The object is unregistered.
Available	The version controlled object is available.
CheckedOut	The version controlled object is checked out.
Pending	The version controlled object is in a pending state. Check the substatus for more information.
PendingDeployment	The version controlled object is pending deployment.
Deleted	The version controlled object is flagged as deleted.
Error	The version controlled object is in error.
ErrorNoWorkingCopy	The version controlled object does not have an associated working copy.
Cloaked	The version controlled object is cloaked
Locked	The version controlled object is locked.
Noncompliant	The version controlled object is noncompliant.
Noncompliant_Deleted	The version controlled object is noncompliant because it was deleted.
Noncompliant_Moved	The version controlled object is noncompliant because it was moved.
Moved	The version controlled object has been moved. This status only applies to OUs.
Unknown	The version controlled objects status is unknown.

Conditions

Whether or not an action is processed can be controlled by the use of conditions. A condition must evaluate to true in order for the action to be processed. If the condition evaluates to false then a log entry stating such is created and the current custom workflow action is not processed.

Each condition node has the following properties:

Table 28. Condition properties

Property	Description
DataType	The data type of the property being compared.
Value1	The left side of the comparison.
Value2	The right side of the comparison.
Operator	The operation to perform. Options depend on the DataType.
IgnoreCase	This is only valid for the string DataType. This property instructs the service to perform any string operations case insensitively.

The type of operations available depends on the DataType property.

The following DataTypes are available:

Table 29. DataTypes

DataType	Description
String	This condition is performed on a string.
Guid	This condition is performed on a Guid.
Version	The condition is performed on a version.

The following operations are available for a String DataType:

Table 30.

String operator	Description
equal	Determines whether or not Value1 and Value2 have the same value.
not equal	Determines whether or not Value1 and Value2 are different.
contains	Determines whether or not Value2 is present in Value1
not contains	Determines whether or not Value2 is missing from Value1.
starts with	Determines whether or not Value1 starts with Value2.
not starts with	Determines whether or not Value1 does not start with Value2.
ends with	Determines whether or not Value1 ends with Value2.
not ends with	Determines whether or not Value1 does not end with Value2.

The following operations are available for a Guid DataType:

Table 31. Guid operators

Guid operator	Description
equal	Determines whether or not Value1 and Value2 have the same value.
not equal	Determines whether or not Value1 and Value2 are different.

The following operations are available for a Version DataType:

Table 32. Version operators

Version operator	Description
equal	Determines whether or not Value1 and Value2 have the same value.
not equal	Determines whether or not Value1 and Value2 are different.
greater than	Determines whether or not Value1 is greater than Value2.
greater than or equals	Determines whether or not Value1 is greater than or equal to Value2.
less than	Determines whether or not Value1 is lesser than Value2.
less than or equals	Determines whether or not Value1 is lesser than or equal to Value2.

The available logical operators include:

Table 33. Operators

Operator	Description
And	Logically ANDs to conditions.
Or	Logically ORs to conditions.

The logical operators ‘And’ and ‘Or’ function sequentially and grouping is not supported. For example:

```
Condition1 And Condition2 Or Condition3
```

would be processed as:

```
(Condition1 And Condition2) Or Condition3
```

not as:

```
Condition1 And (Condition2 Or Condition3)
```

To use a logical “And” or “Or” operator, specify a new Condition with only the Operator property.

For example:

```
<Condition Operator="And"/>
<Condition Operator="Or"/>
```

Example of a complete pre-action

The following example demonstrates a pre-action that creates a CheckIn directory below the GPOSettingsReports directory provided that the name of the version controlled object contains an underscore and the version is less than 4.5 or the comment ends with “_AMER”.

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
    <PreActions>
      <Action Name="CheckIn pre-action" Comment="A custom action."
StopOnError="false">
        <Executable>c:\windows\system32\cmd.exe</Executable>
        <Parameters>/C mkdir "c:\GPOSettingsReports\CheckIn"</Parameters>
        <Conditions>
        <Condition DataType="String" Value1="[NAME]" Operator="contains" Value2="_"
IgnoreCase='true'/>
        <Condition Operator="And"/>
        <Condition DataType="Version" Value1="[VERSION]" Operator="less than"
Value2="4.5"/>
        <Condition Operator="Or"/>
        <Condition DataType="String" Value1="[COMMENT]" Operator="ends with"
Value2="_AMER"/>
        </Conditions>
      </Action>
    </PreActions>
    <PostActions>
    </PostActions>
  </CheckIn>
</CustomWorkflowActions>
```

Troubleshooting custom workflow actions

Because custom workflow actions are performed in the background by the GPOADmin service, they will not be visible from the interface. However, you can use the logs to assess any issues. When a custom workflow action is processed, the Standard Output and Error streams are redirected and logged as part of the server actions provided the Debug logging option is enabled.

NOTE: Depending on the custom workflow action, there can be a large amount of data written to the logs. It is strongly recommended that all custom workflow actions be thoroughly tested by a user who has access to the GPOADmin server logs.

Table 34. Event IDs and corresponding source

Event ID	Source
2013	GPOADmin server process – Information
2014	GPOADmin server process – Errors
2015	Custom Workflow Action process – Standard Output stream
2016	Custom Workflow Actions process – Error stream

9

Appendix: GPOADmin Silent Installation Commands

- Installing GPOADmin with msiexec.exe

Installing GPOADmin with msiexec.exe

If required, GPOADmin and its various components can be installed silently from the command line using the msiexec.exe utility. This section details the commands and provides examples for the following types of installation options:

- All components (Complete GPOADmin installation)
- Client and components
- Watcher Service
- GPMC Extension

All components (Complete GPOADmin installation)

This command installs all GPOADmin components.

```
msiexec /quiet /l* install.log /i "Quest gpoadmin" SERVICEACCOUNT="domain\account"
SERVICEPASSWORD="password" LICENSEACCEPTED=1 INSTALLLEVEL="1000"
```

NOTE:

- The parameters "domain\account" and "password" are the service account and its associated password used for GPOADmin.
- If doing a silent install using a GMSA for the GPOADmin service, the SERVICEPASSWORD must be specified as an empty string. e.g. SERVICEPASSWORD="".

Client and components

You can alternatively select to install the GPOADmin client and specific components on select computers. You can choose from the following:

- Server and client
- Client only
- Client and PowerShell provider (Client Only button on Installation dialog)
- PowerShell provider only

Server and client

This command installs both the server (QGPMService) and client.

```
msiexec /quiet /l* install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=ClientComponentFeature,ServerComponentFeature,ServerFeature
SERVICEACCOUNT="domain\account" SERVICEPASSWORD="password"
```

NOTE:

- The parameters "domain\account" and "password" are the service account and its associated password used for GPOADmin.
- If doing a silent install using a GMSA for the GPOADmin service, the SERVICEPASSWORD must be specified as an empty string. e.g. SERVICEPASSWORD="".

Client only

This command installs the client only.

```
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=ClientFeature
```

Client and PowerShell provider (Client Only button on Installation dialog)

These commands install the client only and PowerShell provider.

```
msiexec /quiet /l* install.log /i "Quest gpoadmin" LICENSEACCEPTED=1
INSTALLLEVEL="3"
```

OR

```
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=ClientFeature,PowerShellFeature
```

PowerShell provider only

This command installs the PowerShell only.

```
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=PowerShellFeature
```

Watcher Service

You can easily install the Watcher Service (QGPOADminWatcherService) on select computers. The following installation options are available:

- Watcher Service on localhost
- Watcher Service on another computer
- Watcher Service and GPMC Extension on another computer
- Watcher Service and Client only on another computer
- Watcher Service, Client, and GPMC Extension on another computer

NOTE: For each of these commands:

- The parameter "server_name" is the name of the computer where the GPOADmin service is installed.
- The parameters "domain\account" and "password" are the service account and its associated password used for GPOADmin.
- If doing a silent install using a GMSA for the GPOADmin service, the SERVICEPASSWORD must be specified as an empty string. e.g. SERVICEPASSWORD="".

NOTE: The Remote Registry service must be running on the targeted GPOADmin service when installing the Watcher service standalone.

Watcher Service on localhost

This command installs the Watcher Service on a computer where the GPOADmin components are installed (localhost).

```
msiexec /quiet /l* install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature SERVICEACCOUNT="domain\account" SERVICEPASSWORD="password"
```

Watcher Service on another computer

This command installs the Watcher Service on a computer that does not have other GPOADmin components installed.

```
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature SERVICEACCOUNT=domain\account SERVICEPASSWORD="password"
SERVERNAME="server_name"
```

Watcher Service and GPMC Extension on another computer

This command installs the Watcher Service and the GPMC Extension on a computer that does not have other GPOADmin components installed.

```
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature,GPMCExtensionFeature SERVICEACCOUNT=domain\account
SERVICEPASSWORD="password" SERVERNAME="server_name"
```

Watcher Service and Client only on another computer

This command installs the Watcher Service and Client only on a computer that does not have other GPOADmin components installed.

```
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature,ClientFeature SERVICEACCOUNT="domain\account"
SERVICEPASSWORD="password" SERVERNAME="server_name"
```

Watcher Service, Client, and GPMC Extension on another computer

This command installs the Watcher Service, Client, and GPMC Extension on a computer that does not have other GPOADmin components installed.

```
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature,ClientFeature,GPMCExtensionFeature
SERVICEACCOUNT=domain\account SERVICEPASSWORD="password" SERVERNAME="server_name"
```

GPMC Extension

You can select to install the GPMC Extension computers where GPMC is installed. The following options are available:

- GPMC Extension on a localhost
- GPMC Extension on another computer

GPMC Extension on a localhost

This command installs the GPMC Extension on a computer where the GPOADmin components are installed (localhost).

```
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=GPMCExtensionFeature
```

GPMC Extension on another computer

This command installs the GPMC Extension on a computer that does not have GPOADmin components installed.

```
Silent install of GPMC Extension (specified server):
msiexec /quiet /l* Install.log /i "Quest gpoadmin" LICENSEACCEPTED=1 /q
ADDLOCAL=GPMCExtensionFeature SERVERNAME="server_name"
```

NOTE:

- The parameter "server_name" is the name of the computer where the GPOADmin service is installed.
- If doing a silent install using a GMSA for the GPOADmin service, the SERVICEPASSWORD must be specified as an empty string. e.g. SERVICEPASSWORD="".

10

Appendix: Configuring Gmail for Notifications

- Using Gmail for Workflow Approvals
- Creating a Gmail Credentials File

Using Gmail for Workflow Approvals

To enable the ability to approve or reject changes through Gmail, you need to:

- Create a gmail account. This account is responsible for the application activities, settings, and API credentials. See https://www.google.com/intl/en-GB/gmail/about/# for details on creating an account.
- Create the required API credential file.
- Enable the Enable Workflow Approval through Gmail option under the Version Control properties. See Editing the Version Control server properties.

Creating a Gmail Credentials File

IMPORTANT: To ensure that access to the Gmail account remains secured, Quest suggests that you store the configuration file in a location that is only accessible by the required administrators or delete it after activation.

The API credentials file allows GPOADmin to connect to Gmail, verify the authorization, get access and refresh tokens to retrieve and send messages.

For best practice information on securely using API keys see the Google Support documentation (https://support.google.com/googleapi/answer/6310037?hl=en&ref_topic=7013279).

To create the required credentials file:

1. Sign in to your Gmail account.
2. Open https://console.cloud.google.com/apis/credentials. Review the Terms of Service and click Agree and Continue.
3. Select a project and click **New Project**.
4. Enter GPOADmin as the project name. Leave the default Location, and click Create.
5. Click **Create Credentials | OAuth client ID**.
6. Click **CONFIGURE CONSENT SCREEN**.
7. Select the user type and click **CREATE**.

   You can choose between Internal and External.

   NOTE: Internal requires a Google Workspace subscription; external allows any test user with a Google Account.

8 Enter the application name on the OAuth consent screen and click **SAVE AND CONTINUE**. Although some fields are optional, the following information is required:

- App name
- User support email
- Developer contact information

9 To add the GMAIL API from the library, select **ADD OR REMOVE SCOPES**, click Google API Library link, enter **GMAIL API** in the Filter field, choose **Gmail API**, and click **Enable**.

After the gmail api is added, you can close the secondary Overview Gmail API tab.

10 Back on the original tab, scroll to the bottom and click **UPDATE**.

11 Check the **Read, compose, send, and permanently delete all your email from Gmail** checkbox, then click **UPDATE**.

12 Click **SAVE AND CONTINUE** to select your test users.

13 Click **ADD USERS**.

14 Enter the required account's email and click **ADD**. (At a minimum, the account used to connect must be assigned as the test user.)

15 Click **SAVE AND CONTINUE** to review your settings.

16 Click **BACK TO DASHBOARD**.

17 Select **Credentials** under **APIs & Services**.

18 Click **CREATE CREDENTIALS**.

19 Select **Desktop app** for the **Application type** and optionally give it a name and click **Create**.

20 Click **OK** to close the **OAuth client created** dialog.

21 Click **Download** to download the credential information in JSON format.

This file location will be entered under the Version Control server properties when you select the **Enable Workflow Approval through Gmail** option.

11

Appendix: Registering GPOADmin for Microsoft 365 Exchange Online

To use email notifications using Microsoft 365 Exchange Online, you need to register GPOADmin with Microsoft Entra ID. During the registration process, the following variables are generated. These variables are used when you configure OAuth authentication.

- Application ID: Required to authenticate to your Microsoft Entra tenant.
- Tenant ID: The tenant associated with the client.

To register an application for Microsoft 365 Exchange Online through Microsoft Entra ID:

1. Log into the Azure portal (https://portal.azure.com/) with your global administrator user account.
2. In the Microsoft Azure dashboard, go to **Microsoft Entra ID | App registrations**, and click **New Registration**.
3. Enter a name for the application.
4. Under Supported account types, select **Accounts in this organizational directory only (Single tenant)** for the accounts that can access the application API.
5. Leave the **Redirect URI (optional)** field empty.
6. Click **Register**.
7. On the **Overview** tab, go to View API Permissions. Click **Add a permission**, click **Microsoft Graph | Application Permissions** and add the **Mail.ReadWrite and Mail.Send** permissions. See Microsoft documentation for details on limiting permissions to specific Exchange Online mailboxes. (Note: The **Enforce approver account validation** option found when configuring email notifications will not function if you select to follow the Microsoft article to restrict access to a single mailbox.)
8. Click **Add Permission**.
9. On the **API Permissions** tab, under **Grant consent**, click **Grant admin consent** for tenant name.
10. Click **Yes** to confirm.
11. On the preview screen, click **Overview**, and note the application ID and the directory ID. (You will need these values when setting up OAuth authentication.)
12. Go to **Manage | Certificates & secrets**, select **Upload certificate** and upload the required .cer file.

12

Appendix: GPOADmin with SQL Replication

The following information details how to setup SQL replication to allow multiple GPOADmin servers in the same domain to run concurrently sharing a configuration store and a backup store.

Before setting up SQL replication, ensure the following is in place:

- All SQL servers included in this configuration have the Replication SQL feature installed.
- Each GPOADmin server has a local Domain Controller and local SQL server.
- The Replication role is installed on all servers that will host a backup store share. (DFS replication is located under File and Folder Storage Services.)
- The SQL Server agent must run as the GPOADmin service account and have the startup type set to Automatic (Delayed Start).
- If this is an in place upgrade, ensure that the server used as the primary SQL server has a copy of the existing GPOADmin database. A separate copy should be kept as a backup.

To configure replication within GPOADmin

1. Right-click the required server and select **Configure Database Replication** (or **Remove Replication** if it is no longer required.)
2. If configuring replication, select the subscribers to replicate the database with using the **Add** or **Remove** buttons, and click **OK**.

   Once subscribers have been selected, GPOADmin verifies that the service account has access to the subscriber and if a database with the same name as the current database exists on the subscriber.

   - If the service account does not have access, the subscriber will not be added.
   - If the service account does have access but the database does not exist, a database with the same name as the current database is created on the subscriber.

   GPOADmin generates the following files in the install directory:

   - ReplicationConfiguration.sql: The SQL script used to configure replication.

- StartReplication.bat: The batch file that can start replication if it does not start automatically after the snapshot has been generated. This batch file must be run on the publisher SQL server.

NOTE: Upgrade considerations

During an upgrade, GPOADmin checks to see if the current database is configured for replication. If the database setup for replication, you have two options:

- Have GPOADmin attempt to end replication, perform the database upgrade, and restore the replication after the upgrade. With this option, GPOADmin generate the following files in the install directory:
  - ReplicationRestoration.sql: The SQL script used to restore replication.
  - RestartReplication.bat: The batch file to start replication if it does not start after the snapshot has been generated. This batch file must be run on the publisher SQL server.
  - ReplicationSubscribers.xml: A list of the replication subscribers recorded before replication was ended.
- Manually upgrade the replicated database:
  - When upgrading a configuration store which is using SQL replication, we recommend that a DBA be involved to oversee the process in case of replication issues.
  - Replication should be ended manually before upgrading any databases.
  - The GPOADmin database on each server used in replication should be upgraded using the manual database upgrade process outlined in the **Using the database upgrade script** section in the Quick Start guide.
  - Once all GPOADmin databases have been upgraded, replication can be restored by following the instructions for replicating Microsoft databases. This will be a new replication on the upgraded databases.
  - Re-enabling replication before all databases have been upgraded could lead to replication conflicts and partially upgraded GPOADmin databases. It is important to ensure all databases are upgraded prior to re-enabling replication.

To manually configure SQL replication for GPOADmin

1 Set up Distributed File System (DFS) for the backup store. (This creates a replicated DFS share on each GPOADmin server or a local file server to each GPOADmin server with a single Active Directory share name.)

NOTE: These instructions are derived from Microsoft documentation.

- Create a folder on each server to be a replicate backup store host. (All folders should have the same name.)
- On the primary server for the backup store, open the DFS Management tool.
- Create a new domain-based namespace in Windows Server 2008 mode.
- Create a new replication group.
- Add all servers hosting replicated backup stores to the group as members.
- Choose **Full Mesh** topology.
- Set to replicate constantly using the specified bandwidth.
- Select the current server as the primary member.
- Add the path to the folders created above.
- Complete the replication group creation.
- Publish the replication group to the Namespace created above.

  The path to the share will now be //domain.fqdn/Namespace/ReplicationGroup.

2 Install GPOADmin on all computers that will be used as GPOADmin servers.

3 On the primary GPOADmin server open the GPOADmin console and configure GPOADmin.

Ensure that all SQL configuration store upgrades have completed. (This may require multiple log out and log in cycles in GPOADmin.)

4 Stop all GPOADmin services on all GPOADmin servers.

5 Log into the SQL server to be used as the primary SQL server.

NOTE: The account used to login must have administrator privileges to all SQL servers to be added.

Ensure that a SQL Server agent is installed and running, and the distributor is set for the primary SQL server.

- Right-click the **Replication** node and Configure Distribution -> This machine should be its own Distributor.
- For the Snapshot folder, choose a network share that is visible to all other SQL servers in replication.

6 Create a new local publication by completing the wizard.

- Publication Database page: Choose the GPOADmin database for replication.
- Publication Type page: Choose **Merge publication**.
- Subscriber Types page: Choose **SQL Server 2008 or later**.
- Articles page: Choose to publish all articles.
- Article Issues page: Read the information and click **Next**.
- Filtered Table Rows page: Do not add any filters.
- Snapshot Agent page: Choose to create immediately and set a schedule. (These scheduled snapshots are essentially rollback points.)
- Agent Security page: Add a login for the agent. Quest recommends that this is a privileged account as it will run the agent for all replicated databases.
- Wizard actions: Select **Create the publication**.
- Name the publication.

7 Refresh the **Local Publications** node, then expand and select the new publication.

8 Right-click the publication and choose **View Snapshot Agent Status**.

The agent should start automatically. If not, you can start it from this dialog. Watch for the status message to become: **[100%] A snapshot of x article(s) was generated**.

9 Right-click the publication and choose **New Subscriptions**. (All subscriptions can be created from here.)

- Publication page: Choose the publisher (may be already set) and the previously created publication.
- Merge Agent Location page: Choose **Run all agents at the Distributor** to create a similar replication path as the peer-to-peer setup.
- Subscribers page: Click **Add SQL Server Subscriber** once for each SQL server in the replication. Choose the database on the target server for replication.

  Add the following values to the extended properties for any replication target databases: ProductName =GPOADmin, Version= 5.21.0.0.
- Merge Agent Security page: Set the accounts to communicate between nodes for the replication.
- Synchronization Schedule page: Set the **Agent Schedule** to **Run continuously** for each subscription.
- Initialize Subscriptions page: Select **Initialize** and set **Initialize When** to **Immediately**.

- Subscription Type page: The **Subscription Type** should be **Server**. Set the **Priority for Conflict Resolution** to a different number for each subscription.

  The publisher is 99.99 by default. Higher numbers will win in an exact timing conflict over lower numbers. Choose which servers have priority and ensure this number is different for each subscription.

- Finish the wizard,

  The subscription will be created and a script saved that can be used to recreate the subscription if needed.

10 Monitor each subscription until there are no more messages other than 'Waiting 60 seconds(s) before polling for further changes.' within 60 seconds.

11 Start all GPOADmin server services.

12 On each GPOADmin server:

- Set the backup store on one of the consoles to the DFS share from using the //domain.fqdn/Namespace/ReplicationGroup format.
- Set any other desired options required for each server.

13

Appendix: Feature Support

Following identifies GPOADmin feature support for GPOs and Intune policies.

Feature	Description	Supports
Version Control	Tracks changes and maintains historical versions for rollback and auditing.	GPOs and Intune Policies
Check-in/Check-out Workflow	Prevents simultaneous edits and enforces change control.	GPOs and Intune Policies
Approval Workflows	Requires multi-level approval before changes are applied.	GPOs and Intune Policies
Role-Based Delegation	Assigns permissions based on roles for secure policy management.	GPOs and Intune Policies
Reporting & Compliance	Generates detailed reports for auditing and compliance tracking.	GPOs and Intune Policies
Version Comparison	Verify setting consistency quickly and easily with advanced, side-by-side version comparisons at various intervals	GPOs and Intune Policies
Rapid Rollback	Quickly revert back to a working state in the event that a settings change has an undesired effect.	GPOs and Intune Policies
Custom Email Templates	Enable customization of e-mail notifications with specific text and/or attachments by role (e.g., help desk).	GPOs and Intune Policies
Custom Pre and Post Actions	Run custom actions before or after a GPOADmin change to facilitate integration with internal processes and systems.	GPOs and Intune Policies
Intuitive Scheduling	Immediately implement or schedule approved changes.	GPOs and Intune Policies
Offline Policy Management	Allows editing and staging of policies before deployment.	GPOs only
Multiforest Support	Manages GPOs across multiple AD forests.	GPOs only
Integration with Change Auditor	Tracks and logs changes for security and compliance.	GPOs only
Hybrid Migration Planning	Assists in transitioning GPOs to Intune equivalents.	GPOs only
GPO Consolidation	Merge reduncant Group Policy settings into a single GPO or create a new GPO baesed on the merged settings.	GPOs only

Feature	Description	Supports
Automated Attestation	Continually validate GPOs through automated attestation	GPOs only
GPO Syncing	Automate settings synchronization from master GPO to selected target GPOs.	GPOs only
Group Policy Lineage	Test pre-production GPO clones before rolling them out to ensure their impact on the live environment.	GPOs only
Protected Settings Policies	Improve Active Directory Group Policy management with the ability to define a list of GPO settings with predetermined values that must exist and cannot be modified.	GPOs only
Automatic Remediation	Choose whether to Rollback, incorporate Unregister, or Restore when a GPO becomes non-compliant.	GPOs only
Multitenant Support	Manages Intune Policies across multiple Azure Tenants	Intune Policies

Report	Description	Support
Settings Report	Generates a settings report for a controlled object.	GPOs and Intune Policies
Difference Report	Shows the difference between versions of one or more objects of the same type in the Version Control system.	
Group Policy Comparison Report	Compares the settings of two or more policies in the Version Control system.	GPOs and Intune Policies
Group Policy Object Settings Search Report	Runs a text search against Group Policy Object settings for names and values.	GPOs only
Group Policy Object Consistency Report	Tests all the domain controllers in a domain to make sure the Active Directory and the SYSVOL portions of GPOs have replicated properly and consistently.	GPOs only
Linked/Unlinked Report	Details which GPOs are linked to which scopes of management and which GPOs are not linked to anything (and could possibly be removed.).	GPOs only
Inactive Policy Settings Report	Shows which registered GPOs have settings defined within disabled user or computer sections.	GPOs only
Group Policy Object Security Report	Reports on the security of GPOs, specifically where certain trustees are either present or not present.	GPOs only

Report	Description	Support
Group Policy Permission Check Report	Shows policies where the service account is not the owner, Active Directory and SYSVOL security is out-of-sync, and accounts other than those specified have the GPMC Edit right.	GPOs only
Group Policy Size Validation Report	Shows policies that have a SYSVOL directory size greater than the specified value.	GPOs only
Policy Analysis Report	Compares the registry settings for each linked policy in processing order.	GPOs only
GPO Synchronization Report	Shows all the synchronization results for the synchronization source.	GPOs only
Group Policy Results	Shows the resultant set of policy for a given user or computer or both.	GPOs only
Group Policy Results Difference Report	Displays the resultant set of policy differences between the specified users or computers.	GPOs only
Group Policy Modeling Report	Shows the resultant set of policy based on the options selected during the modeling session.	GPOs only
Group Policy Object Settings Priority Report	Shows which settings were applied from a specific policy.	GPOs only

About Us

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

Third-party contributions

This product contains the following third-party components. For third-party license information, go to https://www.quest.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at https://opensource.quest.com.

Table 35. List of third-party contributions

Component	License or acknowledgement
Azure.Core 1.38.0	MIT License 2020
Azure.Identity 1.11.4	MIT License 2020

Table 35. List of third-party contributions

Component	License or acknowledgement
BouncyCastle.Crypto 1.8.10	Copyright (c) 2000 - 2017 The Legion of the Bouncy Castle Inc. (http://www.bouncycastle.org) Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
DevExpress.Reporting.Core 22.2.5	Developer Express - DevExpress .Net Controls & Frameworks 2000-2023
DevExpress.WinForms 22.2.5	Developer Express - DevExpress .Net Controls & Frameworks 2000-2023
DiffPlex 1.4.4	Apache 2.0
Google APIs Client Library for working with Oauth2 1.60	Apache 2.0
Google.Apis (Google API) 1.60	Apache 2.0
Google.Apis.Auth (Google API) 1.60	Apache 2.0
Google.Apis.Core (Google API) 1.60	Apache 2.0
Google.Apis.Gmail.v1 (Google API) 1.60	Apache 2.0
Microsoft.Bcl.AsyncInterfaces 6.0.0	The MIT License (MIT) Copyright (c) .NET Foundation and Contributors
Microsoft.Data.SqlClient 5.2.0	MIT License 2020
Microsoft.Data.SqlClient.SNI 5.2.0	MIT License 2020
Microsoft.Graph 4.15	The MIT License (MIT) Copyright (c) .NET Foundation and Contributors
Microsoft.Graph.Core.dll 2.0.7.0	MIT License Copyright 2019 Microsoft Graph
Microsoft.Identity.Client 4.61.3	The MIT License (MIT) Copyright (c) .NET Foundation and Contributors
Microsoft.Identity.Client.Extensions.Msal 4.61.3	MIT License Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.IdentityModel.Abstractions 6.35.0	The MIT License (MIT) Copyright (c) Microsoft Corporation
Microsoft.IdentityModel.JsonWebTokens 6.35.0	The MIT License (MIT) Copyright (c) Microsoft Corporation

Table 35. List of third-party contributions

Component	License or acknowledgement
Microsoft.IdentityModel.Logging 6.35.0	The MIT License (MIT) Copyright (c) Microsoft Corporation
Microsoft.IdentityModel.Protocols 6.35.0	The MIT License (MIT) Copyright (c) Microsoft Corporation
Microsoft.IdentityModel.Protocols .OpenIdConnect 6.35.0	The MIT License (MIT) Copyright (c) Microsoft Corporation
Microsoft.IdentityModel.Tokens 6.35.0	The MIT License (MIT) Copyright (c) Microsoft Corporation
Microsoft.NETCore.Targets 1.1.3	The MIT License (MIT) Copyright (c) Microsoft Corporation
Microsoft.Web.WebView2 1.0.818.41	Microsoft.Web.WebView2 1.0
MimeKit 2.11	The MIT License (MIT) Copyright (c) Microsoft Corporation
MSTest.TestAdapter 3.6.4	The MIT Template 2020 Copyright (c) Microsoft Corporation
MSTest.TestFramework 3.6.4	The MIT Template 2020 Copyright (c) Microsoft Corporation
Newtonsoft.Json 13.0.2	The MIT License (MIT) Copyright (c) .NET Foundation and Contributors
SharpZipLib 1.3.0.8	The MIT License (MIT) Copyright (c) .NET Foundation and Contributors
SpecFlow 1.9.0	SpecFlow Licence (New BSD License) 2.1 Copyright 2009 TechTalk
System.Buffers 4.5.1	The MIT License (MIT) Copyright (c) .NET Foundation and Contributors
System.ClientModel 1.0.0	MIT Template 2020
System.Configuration.ConfigurationManager 6.0.1	MIT Template 2020
System.Diagnostics.DiagnosticSource 6.0.1	MIT Template 2020
System.IdentityModel.Tokens.Jwt 6.35.0	The MIT License (MIT) Copyright (c) Microsoft Corporation
System.IO.FileSystem.AccessControl 5.0.0	The MIT License (MIT) Copyright Notice - System.IO.FileSystem.AccessControl 6.0.0 Copyright (c) .NET Foundation and Contributors
System.Memory 4.5.4	MIT 1.0 Copyright Notice - System.Memory 4.5.4 Copyright (c) .NET Foundation and Contributors
System.Memory.Data 1.0.2	MIT 1.0 Copyright Notice - System.Memory.Data 1.0.2 Copyright (c) 2015 Microsoft
System.Numerics.Vectors 4.5.0	MIT 1.0 Copyright Notice - System.Numerics.Vectors 4.5.0 Copyright (c) .NET Foundation and Contributors

Table 35. List of third-party contributions

Component	License or acknowledgement
System.Runtime.CompilerServices.Unsafe 6.0.0	MIT License Copyright Notice - System.Runtime.CompilerServices.Unsafe 6.0.0
System.Security.AccessControl 6.0.0	The MIT License (MIT) Copyright (c) .NET Foundation and Contributors
System.Security.Cryptography.ProtectedData 4.7.0	MIT Template 2020 Copyright Notice - System.Security.Cryptography.ProtectedData 4.7.0
System.Security.Permissions 6.0.0	MIT Template 2020 Copyright Notice - System.Security.Permissions 6.0.0
System.Security.Principal.Windows 5.0.0	MIT Template 2020 Copyright Notice - System.Security.Principal.Windows 5.0.0
System.Text.Encodings.Web 6.0.0	MIT Template 2020 Copyright Notice - System.Text.Encodings.Web 6.0.0
System.Text.Json 6.0.10	MIT Template 2020 Copyright Notice - System.Text.Json 6.0.10
System.Threading.Tasks.Extensions 4.5.4	MIT 1.0 Copyright Notice - System.Threading.Tasks.Extensions 4.5.4 Microsoft Corporation
System.ValueTuple 4.5.0	MIT 1.0 Copyright Notice - System.ValueTuple 4.5.0 Copyright (c) .NET Foundation and Contributors
WixToolset.Netfx.wixext 5.0.2	Microsoft Reciprocal License (MS-RL) Users can find the source at http://opensource.quest.com.
WixToolset.UI.wixext 5.0.2	Microsoft Reciprocal License (MS-RL) Users can find the source at http://opensource.quest.com.