

Quest® GPOADmin® 5.20
Quick Start Guide



© 2024 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. 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 right 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 right 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.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

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 Quick Start Guide
Updated - November 2024
Software Version - 5.20

Contents

Quest GPOAdmin Quick Start Guide	4
About this guide	5
Product overview	5
GPOAdmin architecture	6
GPOAdmin service	8
Backup repository (storage method)	8
GPOAdmin client	9
GPO management extension in GPMC	9
GPOAdmin watcher service	9
Port requirements	10
Configuring GPOAdmin to use a Group Managed Service Account (GMSA)	11
Minimum permissions required for the service accounts	12
Minimum permissions, rights, and roles required for Microsoft Intune	18
SQL storage method	19
AD LDS storage method	20
Network share storage method	20
Authentication	20
Managing client connections	20
Editing connection options	21
Connecting to GPOAdmin using NTLM authentication	21
Deploying with Multiple service accounts	21
Restricting search scope	22
System requirements	22
Getting started with Quest GPOAdmin	23
Downloading Quest GPOAdmin	23
Licensing GPOAdmin	23
Installing Quest GPOAdmin	24
Upgrading GPOAdmin	25
Configuring the GPOAdmin Server	28
Updating your license	30
Setting Permissions on AD LDS	30
Editing the Version Control server properties	30
Editing the Version Control server configuration store	37
Replacing the Version Control server configuration settings	38
Migrating from AD/AD LDS to a SQL configuration store	39
Step-by-step walkthrough	41
Connect to the Version Control system	41
Register a GPO	41
Check out and edit GPOs	42
Best practices	43
About us	45

Quest GPOADmin Quick Start Guide

- [About this guide](#)
- [Product overview](#)
- [GPOADmin architecture](#)
- [Authentication](#)
- [System requirements](#)
- [Getting started with Quest GPOADmin](#)
- [Step-by-step walkthrough](#)
- [Best practices](#)

About this guide

This document has been prepared to assist you in becoming familiar with Quest GPOADmin. The Quick Start Guide contains information required to install and use GPOADmin and is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

Product overview

Business problem

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 functional security. Core aspects such as password policies, logon 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 corrupt. Windows Group Policy is powerful but difficult to manage. Uncontrolled changes can have disastrous consequences. For example, unplanned effects of a GPO change could prohibit hundreds of users from logging on, exclude access to critical software applications, or expose system settings. The Group Policy Management Console (GPMC) from Microsoft is a useful tool for the individual administrator, but additional functionality—such as GPO check in/check out, change control, and rollback—is needed to effectively manage GPOs across the enterprise.

Business solution

GPOADmin offers a mechanism to control this highly important component of Active Directory. GPOs, Scope of Management links, and WMI filters are backed up in a secure, distributed manner and then placed under version control. When changes are made a backup of the object is made. Changes are then managed from the Version Control system, and approval for change is required. GPOADmin also offers two methods of ensuring GPO consistency. The stored object can be retrieved if the current object in the directory is not valid for any reason. This means that objects become managed and deployed with a sense of security. If issues do arise, recovery time is reduced between the discovery of an issue and the resolution by restoring to a previous version of the object. GPOADmin:

- Gives Active Directory managers and security officers control of GPO changes, to eliminate system outages and security exposures
- Allows administrators to edit and test GPOs offline and have them approved before they are implemented
- Provides a way to quickly roll back changes, in the event that a change has unexpected results
- Archives all GPO settings into a reliable, scalable data store
- Leverages and complements Microsoft technology, including Group Policy Management Console (GPMC), to strengthen infrastructure investments

GPOADmin architecture

GPOADmin is a directory-enabled application and all of its configuration information is stored in the configuration container of either Active Directory Domain Services (ADDS), Active Directory Lightweight Directory Services (AD/LDS).

Active Directory deployments

For all Active Directory deployments, the application information along with the GPOADmin Version Control System is stored in the configuration container of Active Directory in the following location:

CN=QGPM,CN=Quest,CN=Services,CN=Configuration,DC=Domain,DC=com

Where if you drilled down on the GPOADmin container you will find the following directories:

- CN=QGPM
 - CN=Wentworth
 - + CN=Roles (Custom Roles location)
 - + CN=Users (Where users' preferences are stored)
 - + CN=VCRoot (The root of the version control container hierarchy)
 - + CN=Version Control (Pointers to backups' locations (perhaps also backups themselves if 'Directory' is selected as the backup storage location) and controlled object history)
 - + CN=Scheduled Actions

Since this information is stored in the configuration container of Active Directory, it is replicated to all other DCs within your forest. However, the primary version control server is unique and the authoritative source for all version control actions. The primary version control server role is normally held by the DC specified during the initial run of the Server Configuration wizard shortly after the GPOADmin server and service have been installed.

Active Directory Lightweight Directory Services (AD/LDS) deployments

For all AD LDS deployments, the application information, along with the GPOADmin Version Control system, follows the same format as the Active Directory deployment with the exception that the application information and Version Control system is stored in the configuration of the AD LDS instance. The information is not replicated to other AD LDS servers (unless manually set up) like Active Directory replicates information with the configuration container.

SQL storage

During configuration of the Version Control server, you now have the option to select to store GPOADmin data in a SQL database. If you select this option, the data can be found in the following tables:

Table 1. Database Tables

Table	Description
AcITable	Contains access control list information when cloaking or locking GPOs.
ApprovalWorkflow	Contains approval workflow information.
BackupData	Contains backup information such as date, location, and storage type.
CustomSearchFolders	Contains custom search folder information.
Domains	Contains registered domain names, their Id, and whether or not they are visible in the live environment.
DomainSecurity	Contains a mapping of which rights a user has for a registered domain.
EmailTemplateAttachments	Contains a mapping of which attachments are to be include with what email template for a given notification type.
EmailTemplates	Contains email template information.
EmailTemplateSubjectLines	Contains custom email template subject line information.

Table 1. Database Tables

Table	Description
ExchangeSettings	Contains Exchange settings.
GmailSettings	Contains Gmail settings.
GPOLineage	Contains a mapping of GPO lineage for a given registered GPO, when the lineage was assigned, and by whom.
GPOLinks	Contains a mapping of GPO links between the GPO and the SOM.
History	Contains a historical list of actions for any registered object or container.
KeywordList	Contains a mapping of keywords to registered object.
LiveEnvironmentAccess	Contains a list of trustees who have access to the live environment.
MasterKeywordList	Contains a list of all keywords.
Notifications	Contains a mapping of which notifications are enabled for a given user on a given registered object or container.
ObjectData	Contains registered object information.
ProtectedSettingsAssignments	Contains a mapping of which protected settings policies are assigned to a specific container.
ProtectedSettingsExclusions	Contains a list of policies that are excluded from verification of a given protected settings policy.
Remediation	Contains remediation information for a given registered object or container.
Roles	Contains default and custom role information.
RootContainerAssignments	Contains a mapping between a trustee and their root container assignment.
ScheduledTasks	Contains a list of all scheduled deployment tasks.
Security	Contains a list of GPOAdmin permissions assignments for a given registered object or container.
ServiceIDs	Contains a list GPOAdmin service host names and UIDs.
ServiceOptions	Contains the list of service options and there current values.
SOMLinks	Contains the list of GPO links for a given SOM.
SynchronizationResults	Contains a list of the results for a given GPO synchronization.
SynchronizationTargets	Contains a mapping between a source GPO and it synchronization targets.
Trustees	Contains a list of trustees who have been granted access to GPOAdmin as either a user or administrator.
VersionControlContainers	Contains a mapping of child and parent version control containers.
WatcherData	Contains a temporary list of newly created or registered items for the watcher service to monitor.
WorkingCopy	Contains a mapping between a registered object and its working copy.

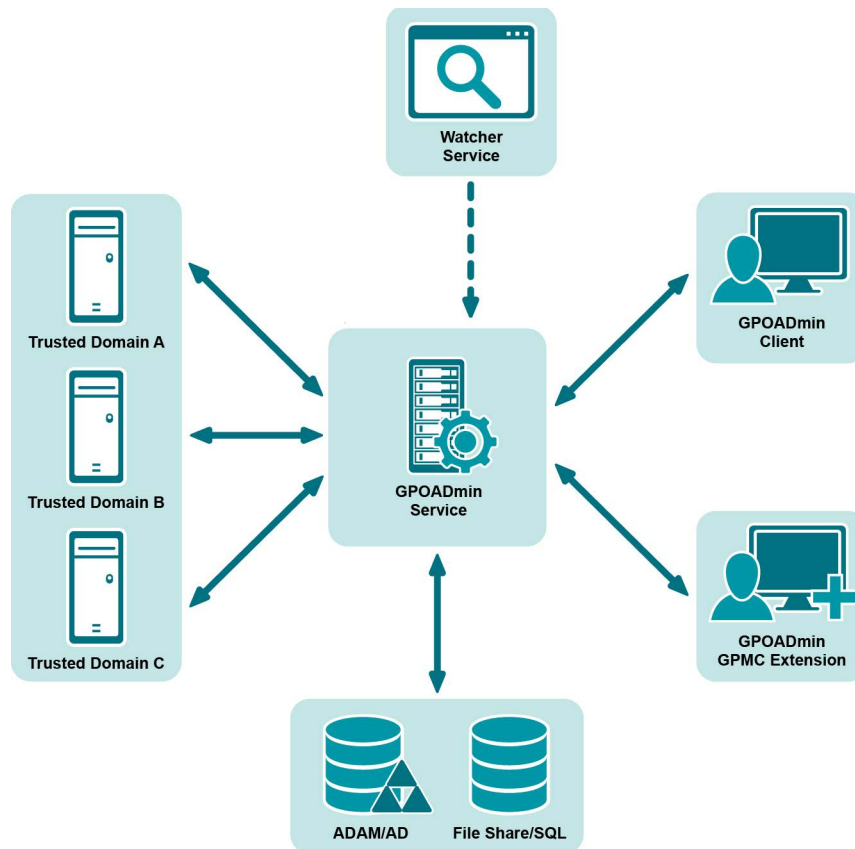


Figure 1. GPOAdmin architecture

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. 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.

GPOAdmin service

The GPOAdmin service can be hosted on a shared application server. Its purpose is to communicate with the Version Control system and implement change requests initiated by the authorized users of the GPOAdmin application. These requests would normally include:

- Check out of an object for editing
- Check in of an object after editing and request for approval
- Approval of the changes
- Implementation of the updated object into the production Active Directory

Backup repository (storage method)

You have the option of choosing one of the following for the location of the physical backup copy of the object versions:

- Configuration store location (Active Directory is not recommended for production deployments due to the volume of replication data)
- Active Directory Lightweight Directory Services (AD LDS)
- Microsoft SQL Server 2016, 2017, 2019, and 2022.
- A network share

i | **NOTE:** For the majority of deployments, network share is the recommended approach as it provides a high performance backup store with a minimum of configuration and maintenance overhead.

GPOADmin client

The GPOADmin client application is a MMC Snap-in that can be installed on the workstations of all administrators responsible for the management of GPOs. Through the client, administrators and users will connect to the appropriate GPOADmin server to perform the tasks described under GPOADmin service.

GPO management extension in GPMC

The Extended Group Policy Management Console allows users to work within a familiar interface that incorporates all the benefits of GPOADmin, rather than having them learn a new client interface. When the Group Policy Management Console is opened, the user will see an extra GPO Management tab that will allow them to perform GPOADmin actions on Group Policy Objects from within the Group Policy Management Console.

GPOADmin watcher service

The watcher service protects an organization from unauthorized changes by automatically detecting changes to GPOs, scripts, and Scopes of Management made outside of the Version Control system. An optional component of GPOADmin, the watcher service will monitor registered GPOs, scripts, configuration profiles, and Scopes of Management outside of the GPOADmin console for changes and display them as non compliant with an icon change. If the change is valid, an administrator can either incorporate the change into the version control system or roll back the change to the previous deployed version.

The GPOADmin watcher service must be run using credentials with sufficient network permissions.

i | **NOTE:** The watcher service requires the Replicating directory changes permission on the Default Naming Context and the Configuration Context for an object and all its descendants.

i | **TIP:**

- Quest recommends installing only one GPOADmin watcher service per forest. If multiple watcher services are used, the timing of changes made to objects could get out of sync.
- It is recommended that you do not install the Watcher Service on a domain controller.

For example, if you have a GPO checked out and it is flagged as non compliant by the Watcher Service, this indicates that the GPO settings in the live environment have changed since you checked out and started working on that GPO.

Once you have selected GPOs for check-in, the Non compliant Objects Detected dialog box shows you a list of the non-compliant objects, alerting you of any GPOs that have been modified outside of the version control system of GPOADmin, and providing you with the following options:

- Cancel pending check in for all objects.
- Cancel pending check in for non compliant objects and proceed with check in for compliant objects.
- Accept unauthorized modifications and discard local changes. (Checks in the unauthorized and discards the local changes made within GPOADmin.)

- Accept local changes and discard unauthorized modifications. (Checks in only the local changes made within GPOAdmin.)
- i** | **NOTE:** If the GPOs were in an Available state (not Checked out) and flagged as non compliant, you would not get this dialog box; you would see the regular compliance actions – Incorporate Live or Rollback.
- i** | **NOTE:** The Remote Registry service must be running on the targeted GPOAdmin service when installing the Watcher service standalone.

Watcher service polling interval

The default polling interval is 45000 milliseconds (45 seconds). If required, you can alter this to meet your needs.

To adjust the Watcher Service polling interval

- 1 Update the DWORD value named “Interval” under the following registry key:
HKLM\Software\Quest\GPOAdmin\WatcherConfig
- 2 Select **Decimal** as the Base when editing the value.
- 3 Enter the desired value under Value data. (The value is in milliseconds where there is 1000 milliseconds to a second.)

Excluding 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 system-provided security.

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.

To exclude security modifications on Scopes of Management from the watcher service

- 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

- i** | **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.

Port requirements

- i** | **CAUTION:** It is recommended to 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:

- Kerberos TCP/UDP port 88
- Kerberos Password TCP\UDP port 464
- Inbound: Port 40200 (default)
- Outbound: TCP ports within the following range (1024-65535) (For more details on default dynamic port range for TCP/IP see <https://support.microsoft.com/en-us/kb/929851>.)

i **NOTE:** To run the Version Control server on a custom port, you must set the following registry value:

Key: HKLM\Software\Quest\GPOAdmin\Remoting
 Value Name: Port
 Value Type: DWord
 Valid Values: 1-65536

If this value is not set, the default (port 40200) will be used.

From the GPOAdmin Server:

Configuration storage

- LDAP Service - TCP/UDP - 389 -or- AD LDS port (defaults to 389 or 50000)
- If you are using SQL Server for GPO backup storage, the appropriate ports will need to 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/or 445.
- If you are using SQL Server for GPO backup storage, the appropriate ports will need to 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 will default to port 389 if not coexisting with AD. If AD is already installed, AD LDS will default to port 50000.

Configuring GPOAdmin to use a Group Managed Service Account (GMSA)

To configure GPOAdmin to use a Group Managed Service Account

- 1 Create a Global security group and add the computers that will host the GPOAdmin service.
- 2 Create the Group Managed Service Account for GPOAdmin using the New-ADServiceAccount PowerShell command. For more details, see <https://docs.microsoft.com/en-us/powershell/module/activedirectory/new-adserviceaccount?view=windowsserver2019-ps>.

Set the `-PrincipalsAllowedToRetrieveManagedPassword` switch to specify the name of the global security group created in step 2.

Set the `-ServicePrincipalNames` switch for the default domain unique SPN to 'GPOADmin/server.domain.com:port#'. For example, GPOADmin/DC1.domain.com:40200. See [Managing client connections](#) for more information.

i | **NOTE:** The GMSA will not update the SPN automatically each time the service starts resulting in warnings in the GPOADmin event log. To prevent the service from updating the SPN, add the following to the registry of the GPOADmin service host if it does not exist:

Value name: UpdateSPN
 Value type: DWORD
 Value path: HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\ServerConfig
 Value: 0

- 3 Create a global security group and add the Group Managed Service Account. This security group will be used to grant permission to the service account.
- 4 For each computer that will host the GPOADmin service and that you added to the security group in step 2, do the following:
 - a Restart the computer.
 - b Run the following PowerShell command once the GPOADmin host computers have restarted to install the GMSA: `Install-ADServiceAccount -Identity <service_account_name>`.
 - c Run the following PowerShell command to verify that the GMSA was successfully installed. The command will return True if the GMSA was successfully installed: `Test-ADServiceAccount -Identity <service_account_name>`.
- 5 Follow the [Minimum permissions required for the service accounts](#) and replace the service account with the group the GMSA member of create in step 4.

i | **NOTE:** If configuring for SQL, enter the actual GMSA instead of the group when specifying a windows login.

Once the service is using a GMSA account, the password is retrieved from the LSA. This will disable the ability to stop the service or change the service account.

You can run the following command to switch back to a normal account:

`sc <server> managedaccount [service name] [type].` For example, `sc managedaccount "QGPMService" false.`

Minimum permissions required for the service accounts

To set up minimum permissions for the service accounts

- 1 Create a service account and add it as a member of the Local Administrators group where the GPOADmin service is installed.
- 2 Grant this account **Log on as a Service** on the computer where GPOADmin is installed.
- 3 Grant the service account **Full Control** to the installation directory.
- 4 Create the "Quest" container for the configuration store in either Active Directory or AD LDS (depending on where the configuration will be stored).

CONFIGURATION STORE	TO CREATE THE QUEST CONTAINER...
Active Directory	Using ADSIEdit.msc, create a "Quest" container under CN=Services,CN=Configuration,DC=Domain,DC=com within the GPOADmin servers domain.

CONFIGURATION STORE	TO CREATE THE QUEST CONTAINER...
AD LDS (Preferred option)	Using ADSIEdit.msc, connect to the AD LDS instance, expand CN=Services and create the Quest container.
SQL	Skip this step.

i | **NOTE:** ADSIEdit.msc is available from the Windows Support Tools or through Add Roles and Features.

5 Grant the service account access to the Quest container.

CONFIGURATION STORE	TO GRANT THE SERVICE ACCOUNT ACCESS...
Active Directory	<ol style="list-style-type: none"> 1 Go to the properties of the Quest container. 2 Select the Security tab and click Advanced. 3 Click Add and select the service account. The applies to option should be This object and all descendant objects. 4 Delegate the following permissions in the Advanced Security Settings: List Contents, Read all Properties, Write all Properties, Delete Subtree, Read Permissions, Modify Permissions, Modify Owner, All Validated Writes, Create All Child Objects, and Delete All Child Objects.
AD LDS (Preferred option)	<ol style="list-style-type: none"> 1 Connect to the AD LDS instance using ADSIedit.msc (for example "CN=Configuration,CN={AD LDS INSTANCE GUID}"). 2 Expand CN=Roles and go to the properties of CN=Administrators. 3 Browse to the Member attribute and click Edit. Add the GPOAdmin service account as a Windows Account. <p>NOTE: If adding the service account as a member of the AD LDS Administrators role is not possible, the AD LDS support tool dscls.exe can be used to fine-tune the rights given by this role or grant specific rights to user accounts.</p>

CONFIGURATION STORE	TO GRANT THE SERVICE ACCOUNT ACCESS...
SQL	<ol style="list-style-type: none"> 1 Run the database script GPOADmin.sql. <ol style="list-style-type: none"> 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 Execute the InitializeDatabase stored procedure on the newly created database. <ol style="list-style-type: none"> 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. <ol style="list-style-type: none"> 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. Click OK to close the properties page.

- 6 Grant the service account **Full Control** on each WMI Filter that will be managed by GPOAdmin.
Using ADSIEDIT.msc, expand the Default Naming Context partition, open 'CN=SOM,CN=WMIPolicy,CN=System,DC=domain,DC=com' and delegate **Full control for All descendant objects**.
- 7 Using GPMC, delegate **Link GPOs** to the service account on the Site and Domain level (or even on the OU level depending on where GPOAdmin is required to manage GPOs), for **This container and all child containers**, if child containers are needed.
- 8 For the service account to run RSoP reports, the Read Group Policy Results data right must be granted. Using GPMC, delegate **Read Group Policy Results Data** to the service account on the Domain level (or even on the OU level, depending on where GPOAdmin is required to perform the RSoP analysis), for **This container and all child containers**, if child containers are needed.

For each computer that will be targeted during the RSoP analysis, add the service account to that computer's local Administrators group.
- 9 Using GPMC, delegate **Create GPOs** to the service account on the Group Policy Objects Level.
- 10 Using GPMC, delegate **Edit settings, Delete, and Modify security** to the service account for each existing GPO that will be managed by GPOAdmin using GPMC.
- 11 For each GPO managed by GPOAdmin, verify that the service account has direct ownership of the GPO on the **Owner** tab of the Advanced Security Settings dialog box.
 - i** | **NOTE:** This step can be automated after GPOAdmin has been installed and configured using the GPOAdmin.AddServiceAccountToALLGPOs.ps1 PowerShell script located in the Scripts directory of the install directory.
- 12 Make the service account the owner of each existing starter GPO to be managed.
 - 1 Expand the StarterGPOs folder in SYSVOL.
 - 2 Click the Guid folder of the StarterGPO and select **Properties**.
 - 3 Click the **Advanced** button on the **Security** tab.
 - 4 Click **Change** at the top of the Advanced Security Settings page and select the service account.
 - 5 Click **OK** three times.
 - 6 Repeat this process for each starter GPO.
- 13 The service account must be granted Read and Write servicePrincipalName.
 - 1 Using ADSIEdit, navigate to the service account.
 - 2 Right-click and select **Properties**.
 - 3 Click the **Advanced** button on the **Security** tab and click **Add**.
 - 4 Click Select a principal and type **SELF**.
 - 5 Ensure **Read servicePrincipalName** and **Write servicePrincipalName** are selected.
 - 6 Click **OK** three times.
- 14 An application partition is created prior to running the Group Policy Modeling Report to simulate the live environment during the report execution. It contains a temporary staging container that is deleted once the report has been generated.

Add the GPOAdmin service account to the **Distributed COM Users** security group in each domain that will be reported onp

To have the GPOAdmin service create the application Partition:
 - a Open ADSI Edit and navigate to the Partitions container in the Configuration naming context.
 - b Right-click the **CN=Partitions** object and select **Properties**.
 - c Select the **Security** tab, click **Add**, and add the GPOAdmin service account.
 - d Under **Permissions for <Service Account>**, enable **Allow** for the following permissions:

- Read
 - Write
 - Create all child objects
 - Delete all child objects
- e Click **Advanced**, select the service account, and click **Edit**.
- f Set **Applies to** to **This object and all descendant objects** and enable the following permissions:
 - Delete
 - Delete subtree
 - Modify permissions
 - All extended rights
- g Click **OK** to close the Permission Entry for Partitions dialog.
- h Click **OK** to close the Advanced Security Settings for Partitions dialog.
- i Click **OK** to close the CN=Partitions Properties dialog.
- j Close ADSI Edit.

OR

To manually create the application partition:

- Create the partition by running the following PowerShell command:
`Add-DnsServerDirectoryPartition -ComputerName DomainController -Name Staging.GPOADmin`
 Where *DomainController* is the domain controller's FQDN where you want to create the partition. If you are using a preferred domain controller, this should be the same domain controller. Otherwise this should be the Primary domain controller.
- Assign access to the service account on the new application partition:
 - a Open ADSI Edit and navigate to the Partitions container in the Configuration naming context.
 - b Right-click the object with the Directory Partition Name "DC=Staging,DC=GPOADmin" and select **New Connection to Naming Context**.
 - c Select the **DC=Staging,DC=GPOADmin** context in the left pane.
 - d Right-click the **DC=Staging,DC=GPOADmin** domainDNS object in the right pane, and select **Properties**.
 - e Click the **Security** tab, click **Add**, and add the GPOADmin service account.
 - f Under **Permissions for <Service Account>**, enable **Allow** for the following permissions:
 - Read
 - Write
 - Create all child objects
 - Delete all child objects
 - g Click **Advanced**, select the service account, and click **Edit**.
 - h Set **Applies to** to **This object and all descendant objects**, and enable the following permissions:
 - Delete
 - Delete subtree
 - Generate resultant set of policy (planning)
 - i Click **OK** to close the Permission Entry for Staging dialog.
 - j Click **OK** to close the Advanced Security Settings for Staging dialog.

- k Click **OK** to close the DC=Staging,DC=GPOADmin Properties dialog.
 - l Close ADSI Edit.
- 15 To ensure that GPOs created in GPMC and then registered in GPOADmin can be deleted and are not missed during a check in, the Service Account must have the Delete Subtree right on the required GPOs.
 - 16 For each GPO managed by GPOADmin, the Service Account must have ownership of the GPO. This is required in all environments to ensure that modifications made to the delegation of a GPO can be properly applied. You can verify direct ownership of the GPO on the Owner tab of the Advanced Security Settings dialog box.
 - 17 Repeat steps 7 to 16 for every domain that will require GPOADmin to manage its GPOs.
 - 18 The service account requires rights to create a Service Connection Point on computers where GPOADmin is installed.
 To do so, open ADSIedit.msc or DSA.msc and connect to the Active Directory domain. Navigate to the computer where GPOADmin will be installed, the computer properties, and select the **Security** tab. Grant the service account the following permissions: **Create serviceConnectionPoint objects** and **Delete serviceConnectionPoint objects for This object and all descendant objects**.
 - 19 Install GPOADmin using the service account.
 For more information about the installation, see [Installing Quest GPOADmin](#) on page 24.
 - 20 Connect to GPOADmin as an Enterprise Admin or the service account.
 Only these accounts are granted access to change the configuration during the install of GPOADmin.
 - 21 Make sure the service account has access to the desired configuration and backup storage locations. Then, step through the Server Configuration Wizard.
 You can add GPOADmin trustees to connect to the system or change server properties.
 For more information about the configuration, see [Configuring the GPOADmin Server](#) on page 28.
 - 22 Once the product has been configured, connect to the GPOADmin console using the service account. Configure any additional administrators and users (trustees) that will connect to the product by right-clicking the connected domain and selecting **Options** and then **Access**. Delegate any roles required by these users through the Version Control Root properties, or any registered OU/GPO within the Version Control Root as necessary.
 - 23 Connect to GPOADmin as any account granted rights to connect during the Server configuration setup.
- i** | **NOTE:** The Watcher Service requires that the service account created in step 1 has the “Replicating directory changes” permission on the Default Naming Context (DC=domain, DC=com) and the Configuration Context (CN=Configuration, DC=domain, DC=com) for this object and all descendents.
- i** | **NOTE:** The service account must have List folder contents, Read, Write, and Modify on the Scripts folder in SYSVOL.
- 24 The service account requires the following registry access on the GPOADmin service host computer:

Registry Key	Required service account access
HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin	<ul style="list-style-type: none"> • Full Control

Registry Key	Required service account access
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Diagnostics	<ul style="list-style-type: none"> • Query Value • Set Value • Create Subkey • Enumerate Subkeys • Delete • Read Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog	<ul style="list-style-type: none"> • Query Value • Set Value • Create Subkey • Enumerate Subkeys • Delete • Read Control

25 Open GPMC and add the GPOAdmin service account to the **Delegations** tab for Starter GPOs.

To remove the application partition:

- 1 Run the following PowerShell command:
Remove-DnsServerDirectoryPartition -Name Staging.GPOAdmin

Minimum permissions, rights, and roles required for Microsoft Intune

To register an application with the required permissions:

- 1 Sign in to the Azure portal.
- 2 If you have access to more than one tenant, select your account in the top right corner, and set your portal session to the Microsoft Entra tenant that you are going to use.
- 3 Select **Microsoft Entra ID | App registrations | New registration**.
- 4 On the Register an application page:
 - a Enter your application's name. For example, GPOAdmin Intune App.
 - b Select the supported account type. For example, Accounts in this organizational directory only (gpoadmin only- single tenant.)
- 5 Click **Register**.
Microsoft Entra assigns a client ID to your app, and the application's Overview page opens where you can now enter additional required information.
- 6 Under **Manage**, select **Certificates & Secrets**.
- 7 Under **Certificates**, select **Upload certificate** and upload the .cer file. You will need the matching .pfx file for the certificate when configuring Intune support in the **Service Options**.
- 8 Under **Manage**, select **API permissions**, and click **Add a permission**.
 - a Under **Microsoft APIs**, select **Microsoft Graph**.
 - b Select **Application permissions**.

- c Under **All APIs**, select **Device Management Configuration**, and enable **DeviceManagementConfiguration.ReadWrite.All**.

i | **NOTE:** User.Read is also a required permission that is added by default.

- d Under **APIs my organization uses**, select **Microsoft Graph | Application permissions | Group** and enable **Group.ReadWrite.All**.

- 9 Under **Manage**, select **API permissions**, and click **Grant Admin consent for GPOADmin**.

Additional requirements to edit Intune objects

To edit Intune objects, you need to create a custom role with the required permissions and assign it to the required Intune user group.

To create a custom role

- 1 In the Microsoft Endpoint Manager admin center, select **Microsoft Entra ID | Manage | Roles and administrators**.
- 2 On the Roles and administrators - All roles blade, select **New custom role**.
- 3 On the Basic page, enter **Intune Object Editor** in the Name field, leave Baseline permissions **Start from scratch** selected, and click **Next**.
- 4 On the Permissions page, search for and add the following two permissions `microsoft.directory/deviceManagementPolicies/basic/update` and `microsoft.directory/deviceManagementPolicies/standard/read` permissions, and click **Next**.
- 5 On the Scope tags page, click **Next** to move to the Review + Create page.
- 6 Review your settings and click **Create**.

You are now ready to assign the role to the required users. For details on assigning roles, refer to the [Microsoft Intune documentation](#).

Additional required tenant permissions

Before you can perform workflow actions within GPOADmin on Intune objects associated to a tenant, you need to set the required permissions.

To enable the required rights

- 1 From the GPOADmin console, right-click the tenant node, select **Properties**.
- 2 Add the required users.
- 3 Enable **Read**, **Register**, and **Report**.
- 4 Apply the settings.

SQL storage method

Using SQL as the backup repository (storage method), the service account will need the following minimum requirements:

- Database Creator's rights in order to create the GPOADmin_Backups Database during the Server Configuration Wizard setup.

i | **NOTE:** Database Creator's right is only required for the initial creation of the GPOADmin_Backups database. If the database has been pre-created (see [Configuring the GPOADmin Server](#) on page 28) by your DB Administrators team then only the following database roles and permissions are required by the GPOADmin service account to access and update the Database:

db_datareader, db_datawriter: Permissions to Execute the following GPOADmin stored procedures:

```
quest_qgpm_add_group_to_role
quest_qgpm_domainid_pr
quest_qgpm_gpoid_pr
quest_qgpm_insbackup_p
```

AD LDS storage method

Using AD LDS as the backup repository (storage method) the service account will need the following minimum requirements:

Member of the Administrator Role in the AD LDS instance. If using the command line tool or the GUI (ldp.exe), the service account will require the same permissions in AD LDS that it would require in Active Directory.

For more information, see [Setting Permissions on AD LDS](#) on page 30.

Network share storage method

Using Network Share as the backup repository (storage method) the service account will need the following minimum requirements:

- At the Share level, Change & Read permissions.
- At the Directory level, all permissions except "Change Permissions" and "Take Ownership."

Authentication

GPOADmin supports both NTLM and Kerberos authentication by using Windows Communication Foundation (WCF) configuration elements. By default, GPOADmin will use Kerberos.

i | **NOTE:** If your environment is not configured to use Kerberos, GPOADmin will authenticate using NTLM.

Managing client connections

GPOADmin uses the Default.Client.Connection.config file when connecting to a GPOADmin service. This file is located in the Connections sub-directory of the install directory. It contains the basic parameters that you can manipulate along with a link to Microsoft's complete list of adjustable settings.

To change settings on a global scale, you simply edit this file. However, to adjust only a specific server connection, you need to copy the file, and rename it to the FQDN of the target server ensuring that you retain the .config file extension.

Editing connection options

An environment has multiple GPOADmin servers and one remote GPOADmin server called GPOADmin.Remote.MyDomain.com. The remote server is on the other side of a slow WAN link and users frequently receive connection timeout messages while connected. To solve this issue, the administrator can make a copy of the Default.Client.Connection.config file to target just the remote server and adjust the connection timeout parameters using the following process:

- 1 Copy the Default.Client.Connection.config and rename the copy to GPOADmin.Remote.MyDomain.com.config.
- 2 Edit this file and adjust the connection timeout parameters.

This file will only be used when connecting to the GPOADmin.Remote.MyDomain.com server. All other connections will use the Default.Client.Connection.config file unless there is a specific file matching the FQDN of the target server.

Connecting to GPOADmin using NTLM authentication

To override the default settings and use NTLM authentication, you can edit the configuration file by navigating to configuration/Settings/ForceNTLM and setting the value to "true".

Installing GPOADmin in a disjointed domain

When GPOADmin is installed in a disjointed domain environment, you may encounter errors with configuring, connecting, and in general usage. This is most likely due to the DNS name of the domain not matching the Active Directory name.

To resolve this, edit the Default.Client.Connection.config file in the Connections directory located in the install directory. Add the following to the <Settings> section below the <ForceNTLM value="false" /> entry:
<DomainName value="ACTIVE_DIRECTORY_FULLY_QUALIFIED_DOMAIN_NAME" />

Deploying with Multiple service accounts

By default, GPOADmin uses a domain unique SPN for connections which requires the use of a single service account in the domain, reducing the number of elevated accounts.

However, you can configure GPOADmin to use multiple service accounts in your domain.

To configure GPOADmin to use multiple service accounts:

- 1 On each GPOADmin service host, browse to HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\ServerConfig and set the registry value UseServerAndPortSPN to 1.
- 2 On each GPOADmin service host and client, browse to the UseServerAndPortSPN in the Default.Client.Connection.config file in the Connections subdirectory of the install directory, and set the configuration value to true.
- 3 Restart all GPOADmin services on each modified host.

The SPN format will change to GPOADmin/SERVICE_HOST_FQDN:PORT allowing for a separate service account per service host.

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.

System requirements

Before installing GPOADmin, ensure that your system meets the following hardware and software requirements.

Table 2. System Requirements

Requirement	Details
Processor	2Ghz CPU
Memory	8Gb RAM
Hard disk space	1 Gb (prefer 50Gb if backups and reports stored on the same drive) hard disk space
Operating systems	Windows 10 Windows 11 Windows Server 2016 Windows Server 2019 Windows Server 2022

NOTE: Nano Server is not supported.

GPOADmin requirements

- .NET Framework 4.8
- GPMC Extension compatible for the system where you are installing GPOADmin.
- Microsoft Edge WebView2 Evergreen Bootstrapper 97.0.1072.69

Microsoft Exchange requirements

- Microsoft Exchange 2016
- Microsoft Exchange 2019

Configuration store requirements

- Active Directory
- AD LDS
- SQL Server (Supported version include 2016, 2017, 2019, and 2022)

i | **NOTE:** GPOADmin supports SQL AlwaysOn Availability Groups and SQL Clusters for SQL data.

i | **NOTE:** GPOADmin supports TLS 1.3; however, TLS 1.2 is still required to be enabled on the SQL Server due to Microsoft SQL Server 2022 requirements.

- Azure SQL managed instance

Backup store requirements

- Network Share (recommended)
- Active Directory (not recommended)
- AD LDS
- SQL Server (Supported version include 2016, 2017, 2019 and 2022)

i | **NOTE:** GPOADmin supports SQL AlwaysOn Availability Groups and SQL Clusters for SQL data.

i | **NOTE:** GPOADmin supports TLS 1.3; however, TLS 1.2 is still required to be enabled on the SQL Server due to Microsoft SQL Server 2022 requirements.

Watcher service

Same system requirements as GPOADmin.

i | **NOTE:** The Remote Registry service must be running on the targeted GPOADmin service when installing the Watcher service standalone.

Getting started with Quest GPOADmin

Downloading Quest GPOADmin

To download Quest GPOADmin

- 1 Go to the Quest web site at <https://www.quest.com/products/gpoadmin/>
- 2 Follow the instructions provided for product downloads.

Licensing GPOADmin

Before you can connect to the Version Control system, you must license GPOADmin. Ensure that you have the license file before you begin an installation or upgrade. Copy the license file to the desktop of the computer where GPOADmin is installed, or to another convenient location. You will be prompted for this license file the first time

you run the Server Configuration wizard, or the first time you attempt to connect to the Version Control Server. For information on licensing the product at a later date, see [Updating your license](#) on page 30.

The following types of licenses are available for GPOADmin:

- Enterprise license: This grants full use of GPOADmin in all locations of an enterprise.
- Enterprise Term license: This grants full use of GPOADmin in all locations of an enterprise for up to a year.
- Perpetual license: This grants full use of GPOADmin.
- Term license: This grants full use of GPOADmin from a specified start date to a specific end date.
- Trial license: GPOADmin Evaluation - This grants full use of GPOADmin for up to a year (100,000 Users).
- Trial license: GPOADmin Trial Days Evaluation - This grants full use of GPOADmin for a specified period of time (usually 30 days - 100,000 Users).

Installing Quest GPOADmin

Prerequisites for installation

The install will place all of the roles of GPOADmin on one computer. Ensure that the computer meets the system requirements mentioned above. To prepare for the install, you must perform the following steps:

- 1 Create a service account for GPOADmin in the root of the domain.
- 2 Add the service account to the local administrators group on the console computer.
- 3 Log in to the console as the service account.
- 4 Ensure that .NET Framework 4.8 and any associated fixes are installed.
- 5 Ensure that AD LDS is installed.

i | **NOTE:** The service account created for GPOADmin should be the account used for AD LDS.

- 6 Ensure that Microsoft Group Policy Management Console with Service Pack 1 or Remote Server Administration Tools are installed.
- 7 Create a folder for the backup storage destination and share it on the network.

Ensure that the service account has full access to both the share and NTFS permissions.

i | **NOTE:** When you uninstall GPOADmin, registry keys with any connection specific values such as "UseSQL", "Servername", "UserID", and "Password" remain.

If you have no other Quest products installed, you can remove these by deleting the HKEY_LOCAL_MACHINE\SOFTWARE\Quest key. Otherwise, delete the KEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin key

To install Quest GPOADmin

- 1 Unzip the GPOADmin package, browse to the GPOADmin folder, and run the Quest GPOADmin.msi.
- 2 In the Welcome screen, click **Next**.
- 3 Click **View License Agreement**, scroll down to read the licensing information, select **I accept these terms**, click **OK**, then click **Next**.
- 4 In the Choose Setup Type dialog box, select **Complete**.
- 5 In the Destination Folder dialog box, accept the default location or enter a new location to install GPOADmin and click **Next**.
- 6 In the Service Credentials dialog box, enter the service account name and password that you created earlier for use by the GPOADmin Service and click **Next**.
- 7 Click **Install**.

- 8 After the software has been installed and the Completed dialog box is displayed, click **Finish**.

Installing GPOADmin with msixec.exe

If required, GPOADmin and its various components can be installed silently from the command line using the msixec.exe utility. Please see the GPOADmin User Guide Appendix: GPOADmin Silent Installation Commands for details on the commands and examples for the following types of installation options:

- All components (Complete GPOADmin installation)
- Client and components
- Watcher Service
- GPMC Extension

Upgrading GPOADmin

During an upgrade, the previous version will be uninstalled and the new version installed. Settings are retained except for those noted below.

i NOTE:

Once an upgrade has begun, you cannot rollback to a previous version. However, if an error occurs, you can manually restore the files from the installation backup folder.

During an upgrade, the installer creates an InstallationBackup folder in the install directory and copies the contents of the Connections folder, MigrationTables folder, and customworkflowactions.xml file into it. Once the existing version is removed and the new version installed, the installer then copies the contents of the InstallationBackup folder back to the correct locations.

Failed Upgrades

If the upgrade fails, and you want to go back to a previous version, you will need to manually install it and restore the files in the InstallationBackup folder to their correct locations:

- Copy the contents of Connections folder into the Connections folder in the install directory.
- Copy the contents of the MigrationTables folder into the MigrationTables folder in the install directory. (If this directory does not exist, you will need to create it.)
- Copy the customworkflowactions.xml file to the install directory.

If you want to restore previously set registry settings, browse to the GPOADminRegistrySettings.reg file located in the InstallationBackup folder in the install directory after re-installing the previous version, right-click and select **Merge**.

Upgrade requirements

- All registered objects must be in the available state prior to any upgrade.
- If you are running GPMC during an upgrade, you must close and re-open it before the GPO Management tab will display.
- If you set a custom report folder path in a previous version, you must change the reports folder path in the User Preferences to point to the existing folder.
- In a minimum permissions environment, Group Policy Objects with a version of 0.x may fail to deploy correctly. To solve this, make a copy of the GPO and deploy the copy. Once this has been verified as successful, delete the original.
- When you upgrade a GPOADmin service, you need to upgrade any GPOADmin client, watcher service, or GPMC extension that reference that service.
- If you have multiple servers to upgrade, the process must be done manually on each of the host computers.

- The live environment will only be visible for GPOADmin Administrators and users who have been explicitly granted access.

As a GPOADmin administrator, however, 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. 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 users who require access to the live environment.
 - 4 Click **OK**.
- Due to security improvements implemented in GPOADmin 5.16, the previous custom search folder format is no longer supported. To retain your existing custom search folders, they must be converted to the new format before you upgrade. To update the format, run the Export script found in the Utilities folder of the downloaded installation package, then upgrade to the latest version of GPOADmin. Once the upgrade is complete, run the Import script located in the same directory to convert your custom search folder to the currently supported format.
 - GPOADmin.CustomSearchFolderExport.ps1 Description: Exports each custom search folders to an xml file in the specified directory. Parameters: -SearchFilterPath : The location where custom search folder will be exported to.
 - GPOADmin.CustomSearchFolderImport.ps1 Description: Imports each custom search folder found in the specified directory. Parameters:-SearchFilterPath : The location where the exported custom search folder files are located.
 - Service account requirements:
 - Due to an upgraded encryption algorithm, the service account cannot decrypt previously encrypted passwords. If you are upgrading and using SQL as your configuration store, accessed with SQL authentication, you must re-enter the password for the connection account the first time you connect to the service. The following pre-configured passwords will also need to be re-entered: the SQL Server Backup Store account, the SMTP notifications account, and the Exchange notifications account.
 - In previous versions of GPOADmin ownership and delegation information was not collected as part of the backup process. Since this data is now included in the GPO backup, after upgrading the service account will be added as the owner during the deployment process. Until the GPO is deployed with the newly upgraded version of GPOADmin, GPO delegation may report incorrectly as compliant.
 - After upgrading, ensure that the “Ensure service account has access prior to deployment” service option is checked in the Options dialog.
 - GPOADmin runs under the security context of a privileged service account that must have full access to GPOs in the managed forest. If you plan to change this account, you must unlock all GPOs before making the change.
 - Configuration store requirements:
 - If multiple GPOADmin services share the same configuration store or backup store, they must all be upgraded to the same version.
 - If multiple GPOADmin services share the same configuration store or backup store, it is recommended that all of the services, including the watcher, be stopped before upgrading.
 - Rolling back to a previous configuration store is not supported.

To upgrade GPOADmin from a previous version:

- 1 Unzip the GPOADmin package, browse to the GPOADmin folder, and run the Quest GPOADmin.msi.

2 Complete the Installation Wizard.

i **NOTE:** The Quest GPOAdmin GPMC Extension.msi should only be used when you only have the GPMC Extension component installed. If you upgrade using this option with a full GPOAdmin installation, only the extension will be upgraded. All other components will be removed.

Using the database upgrade script

GPOAdmin upgrade scripts are located in the Database Scripts sub-directory in the install directory. The database upgrade script for each GPOAdmin version is in a sub-directory for that version.

The upgrade scripts are run based on the following:

- GPOAdmin determines if an upgrade is required by checking the internal database version to that of the current database in use.
- If an upgrade is required, GPOAdmin searches for all upgrade scripts with a version greater than the current database version using the pattern "GPOAdmin_*_Upgrade.sql".
- For every upgrade script found, the upgrade process executes the script and then requests the value of the property "GPOAdmin Version" from the current database.
- This process is repeated until the database version currently in use, matches the internal data version of the product. The scripts are processed sequentially from oldest to newest.

If required, you can manually upgrade the GPOAdmin database.

To manually upgrade the GPOAdmin database

- 1 Determine the version of the database currently in use by looking at the extended properties of the database in SQL Management Studio.
- 2 Expand the **Database Scripts** sub directory in the install directory.
- 3 Open the directory of the next higher version.
- 4 Change all instances of [GPOAdmin] to the name of the existing database.
- 5 Execute the upgrade script in the directory.
- 6 Repeat steps 1 to 4 until the database is fully upgraded.

For example:

To upgrade from GPOAdmin 5.19 RTM to 5.20

- 1 After installing GPOAdmin 5.20, expand the "Database Scripts" sub directory in the install directory.
- 2 Open the 5.20.0.0 directory and run the script.

To upgrade from GPOAdmin 5.18 RTM to 5.20

- 1 After installing GPOAdmin 5.20, expand the "Database Scripts" sub directory in the install directory.
- 2 Open the 5.18.1.0 directory and run the script.
- 3 Open the 5.18.2.0 directory and run the script.
- 4 Open the 5.19.0.0 directory and run the script.
- 5 Open the 5.20.0.0 directory and run the script.

To upgrade from GPOAdmin 5.18 Update 1 to 5.20

- 1 After installing GPOAdmin 5.20, expand the "Database Scripts" sub directory in the install directory.
- 2 Open the 5.18.2.0 directory and run the script.
- 3 Open the 5.19.0.0 directory and run the script.
- 4 Open the 5.20.0.0 directory and run the script.

To upgrade from GPOAdmin 5.18 Update 2 to 5.20

- 1 After installing GPOADmin 5.20, expand the “Database Scripts” sub directory in the install directory.
- 2 Open the 5.19.0.0 directory and run the script.
- 3 Open the 5.20.0.0 directory and run the script.

Configuring the GPOADmin Server

i | **NOTE:** To run the Server Configuration Wizard, you must logon with an account that is a member of the Enterprise Administrators group or the GPOADmin Service Account.

The Version Control server must be configured before users can connect to the Version Control system.

To configure the GPOADmin Server

- 1 Run **All Programs | Quest | GPOADmin** from the **Start** menu.
- 2 In the GPOADmin console, right-click the **GPOADmin** node and select **Connect**.
- 3 In the Connect to Server dialog box 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.
- 5 In the Select a Configuration Store dialog, select Active Directory, AD LDS, or SQL Server for your configuration storage location.

i | **NOTE: Configuration Store Selection**

The best practice is to use AD LDS as the configuration store. However, in large environments, SQL server is the recommended option. Quest uses the following criteria to define large environments:

- Domains with more than 500 registered objects that run searches on a regular basis.
- More than 500 registered containers.
- Containers with objects nested more than 3 levels deep.

These are guidelines and should not be considered as an exhaustive list.

i | **IMPORTANT:** Ensure that you are following the minimum permissions. 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`.

i | **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.

- i** | **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 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** (Default in GPOADmin): 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**

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.

- i** | **NOTE:** 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](#).

- 6 In the Select Storage Options dialog box, the Network Share is pre-selected (this is the best practice for backup storage). Select the backup storage destination that was created in the prerequisites procedure ([Installing Quest GPOADmin on page 24](#)) and click **Next**.

- i** | **NOTE:** To create the GPOADmin_Backups database during the Server Configuration Wizard setup, the Service account must have Database Creator role for the specific SQL Server.

- 7 In the Configure Server Access dialog box, add the accounts that will be Administrators and Users.

To add an Administrator, select the icon with the Plus sign (the icon with the arrowhead will expand or collapse the list). After the account is selected, it will appear in the Administrators list. The account can be removed by selecting the red X icon.

By default the Enterprise Admins and the Service Account are added to the trustees permitted to connect to the system and change server properties. We recommend that you create a Global Group for GPOADmin Admins (<Domain>-GPOADmin Admins), add it, and click Next.

- 8 In the Configure Server Access dialog box, after you have added all the accounts, click **Finish** to commit the changes.

Updating your license

If you want to upgrade your license (for example from a trial license) or you want to change your license for any reason, you can access the license information through the server properties.

- NOTE:** If your license expires, you will be prompted to update it the next time you attempt to connect to the service.

To update the GPOAdmin license through the Server Properties

- 1 Select the **GPOAdmin** node, right-click and select **Connect To**, and connect to the console.
- 2 Right-click the forest for that connection and select **Options**.
- 3 In the Options dialog expand **License | Current License**.
- 4 Check the **Update License** check box and browse to and select your updated license.
- 5 Click **OK**.

- NOTE:** If your license expires, you will be prompted for the DLV file when you try to connect to the Version Control System.

Setting Permissions on AD LDS

To use GPOAdmin with an AD LDS deployment, users must be assigned the Administrator role.

To set permissions on AD LDS

- 1 Open AD LDS ADSI-Edit (ADSI-Edit is installed as part of the AD LDS tools).
- 2 In the Select a well known Naming Context, select **Configuration**, then enter the console and port number in the Computer box, and click **OK**.
For example, GPOconsole:389.
- 3 Double-click **Configuration** to expand the configuration and browse to and select the **Roles** container.
- 4 To grant the users rights, right-click the **Administrators** role, and select **Properties**.
- 5 Browse to the member attribute and click **Edit**.
- 6 Add the service account and other accounts that will be administering GPOAdmin to the selected role.

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

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.
- 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, unregistered SOM linking, WMI filter display, and custom workflow actions.

- configure the domain controller that GPOAdmin will use for all Active Directory actions as well as 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 FIPS mode.

To edit the Version Control Server configuration

i | **NOTE:** You must use the GPOAdmin console to edit server configuration, not the GPMC Extension.

- 1 Right-click the forest, and select **Options**.
- 2 Select **Access** to add and remove users who can connect to and alter the Version Control server options.
Select **Administrators** and add/remove users who can connect to and alter the Version Control server-specific settings.
Select **Users** and add/remove users who can connect to the Version Control server, but can only perform those actions that have been assigned by an administrator.
- 3 Select **Storage** to select the location of the physical backup copy of the various versions of an object.

You can choose between:

Backup store location: This will store the backups in Active Directory if you selected it during the initial setup of GPOAdmin as the storage method for your configuration.

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

AD LDS: This will store the backups in Active Directory Lightweight Directory Services (AD LDS).

Enter the server name and port.

i | **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.

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

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

SQL Server: This will store the backups in SQL Server. Enter the database name and the required authentication.

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

- 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 will be used to delegate rights over the Version Control system.

The built in roles and descriptions are displayed. Add, edit, and delete roles as required.

i | **NOTE:** You cannot alter predefined roles.

For complete information on creating and delegating roles, see [Configuring role-based delegation in the User Guide](#).

- 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 Exchange Online, OAuth 2.0 authentication is required.
- When using Gmail a credential file is required.

Table 3. SMTP options

Option	Procedure
<p>Select SMTP to modify the global SMTP notification options.</p>	<ol style="list-style-type: none"> 1 Select Basic to use Exchange for notifications. <ol style="list-style-type: none"> 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 to use Office 365 Exchange Online for notifications. <ol style="list-style-type: none"> a Select to Enabled SMTP notifications via Exchange. b Enter the application ID, tenant ID, tenant name, certificate, certificate password, and <code>https://outlook.office365.com/ews/exchange.asmx</code> as the Exchange Server Url. <p>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 the User Guide appendix Registering GPOAdmin for Office 365 Exchange Online for details.</p> 3 Select Gmail to use Google mail for notifications. <ol style="list-style-type: none"> 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 the User Guide 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.
<p>NOTE:</p>	
<ul style="list-style-type: none"> • Users can alter the email address for their notification email through their personal settings, or through the Notification Manager. See the User Guide for details.) • 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. 	

Table 4. Workflow notification options

Option	Procedure
<p>Select Workflow to enable workflow approval through email, set the authentication method, and modify the mailbox and server information.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • The Exchange option supports a minimum Microsoft Exchange 2010 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. • Distribution lists should be used for approval groups. • 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. 	<ol style="list-style-type: none"> 1 Select Exchange to use Exchange or Exchange Online for notifications. <ol style="list-style-type: none"> a Select Enable Workflow Approval through email. b Set the required authentication. <p>To use Exchange for notifications, select Basic 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.</p> <p>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.</p> <p>To use Office 365 Exchange Online for notifications, select Exchange Online. Enter the mailbox application ID, tenant ID, tenant name, certificate, certificate password, and https://outlook.office365.com/ews/exchange.asmx as the Exchange Server Url.</p> <p>(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 the User Guide Appendix: Registering GPOADmin for Office 365 Exchange Online for details.)</p> 2 Select Gmail to use Google mail for notifications. <ol style="list-style-type: none"> 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 the User Guide 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.
<p>9 Select Logging Configuration to enter the log location and the type of information you want to track.</p>	<p>You can choose to log to the Event Log, to a specific directory where log files will be created, or not at all.</p>

You can also 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 personnel).

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

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

Table 5. 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.
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.
Enable Group Policy Object Synchronization	Synchronizing GPOs allows you to automatically push out predefined 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.
Allow the service account to synchronize Group Policy Objects during deployment	Provides the ability to control whether the service account can perform a GPO synchronization during deployment. <ul style="list-style-type: none"> • 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.
Enable Unique Role Names	This ensures that roles cannot be created with the same name as an existing role.

Table 5. General options

Option	Description
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. 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.
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 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.

i | **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.

Select **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.

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

11 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.

12 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 [Minimum permissions, rights, and roles required for Microsoft Intune](#).

13 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**.

- 14 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 ensure 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.

- 15 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 Active Directory, AD LDS, or SQL Server for your configuration storage location.

i NOTE: Configuration Store Selection

The best practice is to use AD LDS as the configuration store. However, in large environments, SQL server is the recommended option. Quest uses the following criteria to define large environments:

- Domains with more than 500 registered objects that run searches on a regular basis.
- More than 500 registered containers.
- Containers with objects nested more than 3 levels deep.

These are guidelines and should not be considered as an exhaustive list.

- 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`.

- i** | **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.

i | **NOTE:** See the Release Notes for supported SQL Server versions.

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 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** (Default in GPOAdmin): 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**

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 is available 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.

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

- i** | **IMPORTANT:** The configuration utility must be:
 - Run on the GPOAdmin 5.20 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 later 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.

- i** | **NOTE:** 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 properties](#) to change the storage from AD/AD LDS to SQL.

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.

- /G = Grant the specified service account access.

Step-by-step walkthrough

This step-by-step walkthrough takes you through a GPOAdmin scenario that includes the following:

- Connect to the Version Control system
- Register an object
- Check out and edit an object
- Check in the object and request approval

i | **NOTE:** GPOAdmin provides roles that enable users to perform actions within the Version Control system. The following scenario is created on the assumption that the administrator has already delegated the User and Moderator roles to the required users.

To view the roles applied to a specific container, right-click it, select Properties, and click the Security tab.

For complete information on how to create and delegate roles, see “Configuring Role-based Delegation” in the Quest GPOAdmin User Guide or Online Help.

Connect to the Version Control system

Because the application has been fully configured by the administrator, users connect to the Version Control system in the following manner:

To connect to the Version Control system

- 1 Right-click the **GPOAdmin** node and select **Connect To**.
- 2 Click **New** to create a new connection and enter the server name.
- 3 Select the Version Control server that you want to connect to and click **Connect** to connect with the current logged on user credentials or select **Connect As** to enter a new credentials (user name and password).
- 4 To save the credentials, select the **Remember my password** check box and click OK.

For more information about saving connections, see “Persisting Connections” in the GPOAdmin User Guide.

Register a GPO

Initially all GPOs are unregistered. To add GPOs to the Version Control system, they must be registered.

i | **NOTE:** When GPOs are registered they maintain their GPO status (User and Computer settings enabled or disabled), links, security, and WMI filters.

To register a GPO

i | **NOTE:** You must have the Register right and been granted access to the Live Environment node to register a GPO.

- 1 Expand **GPOAdmin**, the forest, **Live Environment**, and the **Domain Controller**. Select the **Group Policy Objects**, right-click a GPO in the right-hand pane, right-click and select **Register**.
- 2 Select the container where you want to place the registered object and click **OK**.

Once objects have been registered, they are located in the selected container under the Version Control Root with their initial version number set to 1.0. They are now available to be checked out and edited.

If you are migrating from an existing Version Control system, you can set the major version number to any number greater than 1.0 in the Initial major version list.

Check out and edit GPOs

i | **TIP:** The information in this section applies to workflow-enabled GPOs only. For more information on workflow enabling/disabling, see the Quest GPOAdmin User Guide or Online Help.

Before users can edit registered GPOs, the GPOs must be checked out.

The workflow is as follows:

- Check out the GPO from the system,
- make the required edits, and
- check in the changes to the system.

i | **NOTE:** The changes are only applied to the live environment after they are approved and deployed.

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

i | **NOTE:** If you have all required rights, you can approve a GPO from the checked out state and the necessary workflow steps happen automatically.

Checking out a GPO for the first time creates a copy of the original GPO. The copy is an exact duplicate of the original GPO until it passes through the approval process.

To check out a GPO

- 1 Expand the **Version Control Root** and select the available GPO.
- 2 Right-click a GPO and select **Check Out**.
- 3 Enter a comment and click **OK**.

Once you have a GPO checked out, you can edit the settings from the Group Policy Management Editor as well as edit the Security and WMI Filter settings. When you check out a GPO, the changes are made to a copy of the live GPO. Those changes do not affect the GPO settings on the network until the changes are approved and deployed.

To edit a GPO

- 1 Right-click a checked out GPO and select **Edit**.
- 2 Click **Launch Editor** and make the required changes.
- 3 If required, select the **Security** tab and click **Add** or **Remove** to modify the current security filter. Enter or search for the required user, computer, or group, and click **OK**.
- 4 Click the **Advanced** button to select advanced permissions.
- 5 To add or remove a WMI filter, select the **WMI Filter** tab and choose a filter from the list of available WMI filters. Click **OK**.

i | **NOTE:** You will only see the filters you have permission to access.

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.

To check in and request approval

- 1 Expand the **Version Control Root** node and select the checked out GPO.
- 2 Right-click and select **Check In**.
- 3 Enter a comment and click **OK**.
- 4 Right-click the GPO and select **Request Approval**.
- 5 Enter a comment and click **OK**.

The GPO status will be Pending Approval until the changes are approved or rejected by a user with the appropriate permissions. When the GPO has been approved it is ready to be deployed into the live environment.

Best practices

The following best practices exist within GPOAdmin:

- Deploying Cloaked GPOs

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 non-compliant.

- Forest Configuration

It is recommended that users who are members of the Enterprise Administrators group configure the forest for version control.

- Client Installation

Users should be a local administrator on the computer where the client is installed.

- Remote Forest Management

Although remote forest version control management options are available, it is recommended to manage a forest logged in as a user from the same forest to eliminate any additional trust and security-related considerations.

- Storage Repository Placement

If using AD LDS or SQL as storage options it is recommended that they are located in the same forest that is being managed to eliminate any additional trust and security-related considerations. It is recommended that AD LDS is used as the configuration store, and a network share as the backup store.

- Register/Unregister Actions

It is recommended that users who are members of the Enterprise Administrators group perform the register and unregister actions on GPOs within the Version Control system.

- Naming Conventions

When creating GPOs within the Version Control system, it is possible to enter names that have already been used. However, it is highly recommended to use unique names. You enable the option to use unique names in the Server Properties Options tab.

- Action Comments

Use descriptive comments to help others easily identify the reasons for performing actions within the Version Control system.

- Deploying Changes

Ensure each object has the desired settings before approving and deploying any pending modification actions. Once the modification has been approved and deployed, the changes will be applied to the live object.

- GPO Settings - Versions

When running in a mixed mode environment, newer GPO settings are not backwards compatible with older versions of GPMC. For example:

Preferences introduced in Windows Server 2008 are not backwards compatible.

- Watcher Service

It is recommended that only one GPOAdmin Watcher Service be installed per configuration store.

It is recommended that you not install the Watcher Service on a domain controller.

- Migration Utility

A configuration utility is available that allows you to migrate the configuration store to SQL from an AD/ AD LDS. 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.

- Configuration Store Selection

The best practice is to use AD LDS as the configuration store. However, in large environments, SQL server is the recommended option. Quest uses the following criteria to define large environments:

- Domains with more than 500 registered objects that run searches on a regular basis.
- More than 500 registered containers.
- Containers with objects nested more than 3 levels deep.

These are guidelines and should not be considered as an exhaustive list.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit <https://quest.com/company/contact-us.aspx> or call +1-949-754-8000.

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.