Quest

Quest® GPOADmin® 5.13.5

Quick Start Guide

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

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
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, 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.

GPOADmin Quick Start Guide
Updated - June 2019
Software Version - 5.13.5

Contents

1

Quest GPOADmin Quick Start Guide

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 native 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 Master Version Control is unique and the authoritative source for all version control actions. The Master Version Control 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.

Table	Description
AclTable	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.
GPOLineage	Contains a mapping of GPO lineage for a given registered GPO, when the lineage was assigned, and by whom.

Table 1.

Table	Description
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 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.

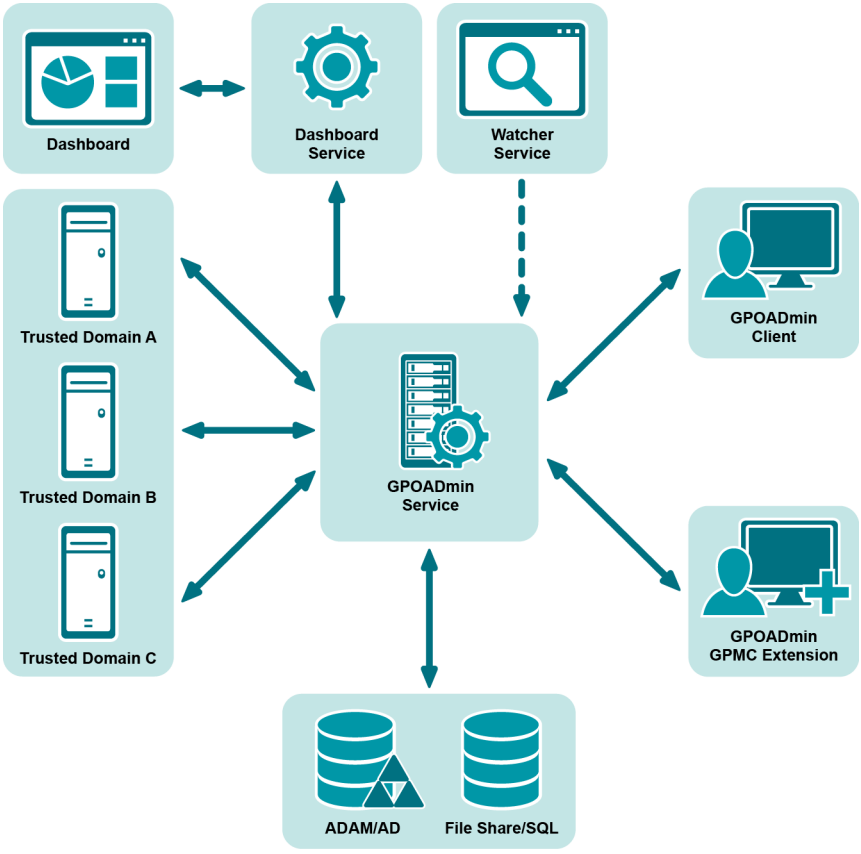

Figure 1. GPOADmin architecture

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) for Windows Server 2008
- Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016, and 2017
- A network share

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.

GPOADmin Dashboard

GPO implementation is a key consideration when planning your organization's Active Directory structure, because it streamlines management of all user, computer, and configuration issues, ensuring the smooth day-to-day operation of the network.

The GPOADmin Dashboard offers a quick overview of the state of your GPO deployment and enables you to affect changes where required.

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, and Scopes of Management outside of the GPOADmin console for changes and display them as noncompliant 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 of the GPO or Scopes of Management.

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

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 descendents.

TIP: It is recommended that only one GPOADmin watcher service is installed per forest. If multiple watcher services are used, the timing of changes made to GPOs, scripts, and Scopes of Management could get out of synch.

TIP: 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 noncompliant 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 Noncompliant 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 object(s).
- Cancel pending check in for noncompliant object(s) and proceed with check in for compliant object(s).
- 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.)

NOTE: If the GPOs were in an Available state (not Checked out) and flagged as noncompliant, you would not get this dialog box; you would see the regular compliance actions – Incorporate Live or Rollback.

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 desired, 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. Note: 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 security natively.

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

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

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.)

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.

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. Ensure the service account is a member of the **Group Policy Creator Owners** group.
3. Grant this account **Log on as a Service** on the computer where GPOADmin is installed.

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.
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.

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	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 child objects (in Windows Server 2003)** or **This object and all descendant objects (in Windows Server 2008)**. 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)	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. **NOTE:** If adding the service account as a member of the AD LDS Administrators role is not possible, the AD LDS support tool dsacls.exe can be used to fine-tune the rights given by this role or grant specific rights to user accounts.

CONFIGURATION STORE	TO GRANT THE SERVICE ACCOUNT ACCESS...
SQL	1 Run the database script GPOADmin.sql. a In Microsoft SQL Server Management Studio, select **File | Open | File** or press the control key and the O key (Ctrl + O). b In the Open File dialog, select the GPOADmin.sql file and press **OK**. This file is located in the GPOADmin server install directory by default, but if your SQL server is on a different computer, the file can be copied. c If you want to create the database with a different name other than the default name of GPOADmin, change the name from GPOADmin on line 4 and line 7 to the name you want to use. d Click the **Execute** button or press **F5** to create the database. 2 Execute the InitializeDatabase stored procedure on the newly created database. a Create a new query by pressing the **New Query** button. b Set the available database to the name of your GPOADmin database or type **USE [DATABASE_NAME]** where **DATABASE_NAME** is the name of your GPOADmin database. c On the next line, type **EXEC InitializeDatabase.** d When ready, click the **Execute** button or press **F5** to run the command. 3 Create a login for the GPOADmin service account. a In Microsoft SQL Server Management Studio, navigate to **Security**, then **Logins**. b Right-click **Logins** and select **New Login**. c On the General page, enter the name of the service account in the **Login name** field. d Select Windows authentication to connect as the GPOADmin service account or SQL Server Authentication to connect as a SQL account. SQL authentication is useful if you want to use this database as the configuration store for a GPOADmin installation in another untrusted domain. e Set the **Default database** property to the name of your GPOADmin database. f On the Server Roles page, check the **public** server role. g On the User Mapping page, under **Users mapped to this login**, check the name of your GPOADmin database. Under Database role membership for the selected database, check **db_owner** and **public**. h Click **OK** to close the properties page.

4 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**.

5 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.

6 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.

7 Using GPMC, delegate **Create GPOs** to the service account on the Group Policy Objects Level.

8 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.

9 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.

   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.

10 Repeat steps 5 to 9 for every domain that will require GPOADmin to manage its GPOs.

11 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 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**.

12 Install GPOADmin using the service account.

   For more information about the installation, see Installing Quest GPOADmin on page 21.

13 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.

14 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 24.

15 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.

16 Connect to GPOADmin as any account granted rights to connect during the Server configuration setup.

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.

NOTE: The service account must have List folder contents, Read, and Write on the Scripts folder in SYSVOL.

17 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	• Full Control
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Diagnostics	• Query Value • Set Value • Create Subkey • Enumerate Subkeys • Delete • Read Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog	• Query Value • Set Value • Create Subkey • Enumerate Subkeys • Delete • Read Control

18 Open GPMC and add the GPOADmin service account to the **Delegations** tab for Starter GPOs.

19 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.

20 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 on.

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:

a Open Command Prompt and type: `ntdsutil.`

b At the ntdsutil command prompt, type: `partition management.`

c At the partition management command prompt, type: `connection.`

d At the server connections command prompt, type: `connect to server ServerName.`

e At the server connections command prompt, type: `quit.`

f At the partition management command prompt, type the following: `create nc dc=staging,dc=gpoadmin DomainController.`

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.

Additional Service Account requirements

Consider the following additional Service Account requirements:

- 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.
- 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.

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.

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 24) 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 25.

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.

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 forces the use of a single service account in the domain, reducing the number of elevated accounts.

However, if required, 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.

System requirements

Before installing GPOADmin 5.13.5, 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 7 Windows 8 Windows 8.1 Windows 10 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 **NOTE:** Nano Server is not supported. **NOTE:** For Windows 7 or Windows Sever 2008 R2 see https://support.microsoft.com/en-us/kb/3033929. Quest provides the SHA-2 certificate with the understanding that even with this update, there may still be situations where certificate cannot be verified.

GPOADmin requirements

- .NET Framework 4.5 and 4.6
- GPMC Extension compatible for the system where you are installing GPOADmin.
- Microsoft Group Policy Management Console with Service Pack 1 or Remote Server Administration Tools

Configuration store requirements

- Active Directory
- AD LDS
- SQL Server (Supported version include 2012, 2012R2, 2014, 2016, 2016 Express, 2017 and 2017 Express)

Backup store requirements

- Network Share (recommended)
- Active Directory (not recommended)
- AD LDS
- SQL Server (Supported version include 2008, 2008R2, 2012, 2012R2, 2014, 2016, and 2017)

Watcher service

Same system requirements as GPOADmin.

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

GPOADmin Dashboard

For the best performance when using the dashboard, we recommend that you install the GPOADmin service on a computer with at least two CPUs.

When you install GPOADmin, by default the GPOADmin service and the Dashboard service are installed on the same computer with the Dashboard service configured to communicate with GPOADmin service “localhost”. However, to improve performance you can install the Dashboard service as a standalone option or change the default GPOADmin service the Dashboard service communicates with.

Additional dashboard requirements

If you are installing a standalone dashboard client, you must enable the following settings:

1. In the Local Security Policy on the GPOADmin Dashboard Service host:
    a. Open Local Policies.
    b. Select **User Right Assignment.**
    c. Double-click **Impersonate a client after authentication**.
    d. Click **Add User or Group**.
    e. Add the GPOADmin Dashboard service account.
2. Using Active Directory Users and Computers:
    a. Open the Properties of the GPOADmin Dashboard Service service account.
    b. Select the **Delegation** tab.
    c. Ensure **Trust this user for delegation to specified service only** is selected.
    d. Ensure Use Kerberos only is selected.
    e. Add the GPOADmin Dashboard Service service account.
    f. Select the **GPOADmin Service Type**.

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 24.

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 4.5 and any associated fixes are installed.
5. Ensure that AD LDS (Windows 2008 or 2012) is installed.

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.

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. Run the **autorun.exe** and select **Install**.
2. Select **Quest GPOADmin** and click **Install**.
3. In the Welcome screen, click **Next**.
4. Click **View License Agreement,** scroll down to read the licensing information, select **I accept these terms**, click **OK**, then click **Next**.
5. In the Choose Setup Type dialog box, select **Complete**.
6. In the Destination Folder dialog box, accept the default location or enter a new location to install GPOADmin and click **Next**.
7. 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**.
8. Click **Install**.
9. After the software has been installed and the Completed dialog box is displayed, click **Finish**.

Installing GPOADmin with msiexec.exe

If required, GPOADmin and its various components can be installed silently from the command line using the msiexec.exe utility. 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
- GPOADmin Dashboard

Upgrading GPOADmin

Consider the following when upgrading GPOADmin:

- Due to an upgraded encryption algorithm, the service account cannot decrypt previously encrypted passwords. If you are upgrading from 5.12.x and are 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 5.13.5 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 to version 5.13.5 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.

- 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.
- After upgrading to ensure that the “Ensure service account has access prior to deployment” service option is checked in the Options dialog.
- When you upgrade a GPOADmin service, you need to upgrade any GPOADmin client, watcher service, or GPMC extension that reference that service.
- 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.
- If multiple GPOADmin services share the same configuration store or backup store, they must all be upgraded to the same version.
- If you have multiple servers to upgrade, the process must be done manually on each of the host computers.
- 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.
- During an upgrade, the previous version will be uninstalled and the new version installed. Settings are retained except for the ones noted above.
- 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**.

To upgrade GPOADmin from an existing x64 version:

1 Run the **autorun.exe** and select **Install**.

2 Select **Quest GPOADmin** and click **Install**.

3 Complete the Installation Wizard.

To upgrade GPOADmin from an x86 to an x64 version:

1 Open Regedit.exe and navigate to HKLM\SOFTWARE\WOW6432Node\Quest\GPOADmin.

2 Right-click **GPOADmin** and select **Export**.

3 Select a location and name for the export file.

4 Run the **autorun.exe** and select **Install**.

5 Select **Quest GPOADmin** and click **Install**.

6 Complete the Installation Wizard.

7 Once the upgrade is completed, edit the exported file from step 3 in Notepad.exe.

8 Remove all references to WOW6432Node and ensure there is only one \ between SOFTWARE and Quest.

9 If your export file contains data for "ChangeAuditorService" remove any carriage returns for the XML data. Failure to do so will result in the import failing to set the value.

10 Save the file.

11 Double-click the file or right-click and select **Merge** to import the file back into the registry.

12 Once the import finishes, restart all GPOADmin services.

Configuring the GPOADmin Server

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 box, select AD LDS, Active Directory, or SQL for your configuration storage location.

TIP: The recommended best practice is to use AD LDS.

If you select AD LDS, enter the NetBIOS name of the computer you are installing to followed by the port number, in the format: `server_name:port`, and click **Next**. For example, gpoadmin_svr:389.

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

If you select SQL Server, enter the name of the server and database and the type of authentication.

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 21) and click **Next**.

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 dsacls 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.

To edit the Version Control Server configuration

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

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

2 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.

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.

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.

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.

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 **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.

NOTE: You cannot alter predefined roles.

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

7 Select **Notifications** to configure email notifications on Version Controlled events. These notifications help you to stay informed of the latest changes to objects under version control.

Select **SMTP** to modify the global SMTP notification options.

Select to **Enabled SMTP notifications**.

Enter the server, port, “From” address and credentials.

NOTE: Users can alter the email address for their notification email through their personal settings, or through the Notification Manager.

Select **Exchange** to modify the mailbox and Exchange server information.

By default, GPOADmin will use the service accounts mailbox. If required, you can specify the mailbox and Exchange Server that you want to use to process the approvals/rejections through email.

To do so, uncheck the **Use the service accounts mailbox** option. Enter the mailbox that you want to connect to, the account to use to connect to it, and the password for the account.

NOTE: To connect as the service, leave the account blank and password blank.

NOTE: To ensure secure communication between GPOADmin and your Exchange server, it is recommended that your Exchange server be configured to support TLS 1.2.

Select **Enable workflow approval through email** if you would like the ability to have changes approved and rejected through email.

NOTE:

- This option requires at a minimum Microsoft Exchange 2010 and all approvers and the service account must have a valid Exchange Inbox. Distribution lists should be used for approval groups.
- Ensure that the proper Exchange certificates are 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.

Enter the Exchange Server Url or select **Autodiscover Exchange Server Url** to locate the Exchange server that is hosting the specified mailbox.

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

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

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).

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

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

Table 3. 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.

Table 3. General options

Option	Description
Enable Protected Settings for Group Policy Objects	This enables the ability to have Protected Settings policies that contain settings that you want to control. They are protected in the sense that they contain and identify the settings that may not be altered by users. This provides an added level of security for the policies within your organization. If a user attempts to create, edit, or remove the flagged settings they will be stopped.
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 Group Policy Object Synchronization	Synchronizing GPOs allows you to automatically push out pre-defined “master GPO” settings to specified targets both within a forest and between two forests. This allows you to ensure specific GPOs, which are required in every domain, contain the same settings without having to link to a GPO outside of the domain. You will be able to select one or more GPOs from various domains as synchronization targets for the source GPO. When the source GPO has been successfully deployed, the settings from the last major backup will be imported into each synchronization target GPO.
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 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.
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 prior to 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.
Display only the WMI Filters a user has Read access to when editing a GPO	Users will be restricted to only the WMI Filters they have Read access.
Enable the processing of custom workflow actions	Clicking on the Launch Editor button launches the Custom Workflow Editor.

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

NOTE: To protect your environment from a SQL Injection attack, you can mark which SQL statement inputs are not permitted. By default, all of the inputs are marked as not permitted.

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

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 **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 **Naming Standards** to enforce naming conventions for newly created objects. Select to apply the conventions to GPOs and/or WMI filters, and enter the pattern that you want to use.

You can test your rule, by entering a name that conforms to your desired naming standard and selecting **Verify**. If you validate the rule here, users will see both the rule and your sample text if they try to use a non-conforming name.

If you receive a green check, then the name you entered is allowed and your rule is running as desired. If you receive a red X, then the name you entered failed the verification. You should adjust the rule to allow the name to pass or adjust the name to match the rule.

Users will now be forced to use names that adhere to your organization's standards. If they enter a name that does not comply, they will see the rule details that they must comply with.

NOTE: Example rule

^[a-z]+[0-9]+_GPO$

The caret character (^) means the start of the line.
The grouping [a-z]+ means at least one or more lower-case characters between a and z.
The grouping [0-9]+ means at least one or more numeric characters between 0 and 9.
The dollar sign character ($) means the end of the line.

This rule states that from the start of the line there must be at least one or more lower-case characters immediately followed by at least one or more numeric characters immediately followed by the literal string "_GPO" and nothing after that.

a1_GPO passes
abc123_GPO passes
_a1_GPO fails
a1_GPO_ fails
A1_GPO fails
A1_gpo fails

10 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.

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

12 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.

TIP: The best practice is to use AD LDS as the configuration store.

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 version control master. The version control master 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 version control master is the authoritative source for all version control actions. If it goes offline, users cannot perform actions such as check-in a desired group policy object change until the problem has been rectified.

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

For example, gpoadmin_svr: 389.

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

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

NOTE: SQL Server versions 2012, 2012R2, and 2016 are supported.

To connect as the current user, select NT Authentication.

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

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

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.

IMPORTANT: The configuration utility must be:

- Run on the GPOADmin 5.13.5 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 5.11, 5.11.1, 5.12,or 5.13 configuration storage location. (Upgrade from versions older than 5.11 are not supported.)
- After the migration, you need to restart the Watcher Service so that it will use the correct configuration store.

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>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.

Using the GPOADmin Dashboard

The Dashboard allows you to view GPO deployment summary and detailed information, configure the interval at which the dashboard data is updated, and perform actions that are available from within the GPOADmin client. For complete details on the available actions, see the GPOADmin User Guide.

To access the dashboard

- Select **Start | GPOADmin Dashboard**.

  The Dashboard opens with the overview view. From here you can get a quick summary of any issues that need to be addressed through the GPO Statistics or any actions that require your attention.

To configure the view

1. To have a full view of an individual tile, select it from the menu option on the left side or select **Show All**.
2. To move the position of a particular tile, select it and drag and drop it to the desired position. Keep in mind, you can only place it in a tile of similar size.
3. To sort information, select the desired column header and click it to sort in ascending and descending order.
4. To re-order the columns, select it and drag and drop it to the desired location.

NOTE: If you make changes to the column order or sorting, it is not maintained once you close the Dashboard or move between the tile view and the full page view.

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

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.

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

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

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.

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.

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**.

   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.

  If you backup a GPO on Windows Server 2012 and then attempt to import that backup into a GPO on Windows Server 2008, GPMC will indicate that there is a version mismatch and not allow the import.

- Resultant Set of Policies Reports

When running the Group Policy Results or Group Policy Results Difference reports against Windows Server 2008 R2 or Windows 7, the Quest GPOADmin Service should be running on an operating system that has the ability to read all policy settings.

- 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.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. 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.