Quest® GPOADmin® 5.20
Release Notes

November 2024

These release notes provide information about the Quest GPOADmin release.

About this release

GPOADmin gives organizations control of Group Policy Objects (GPOs) across the enterprise. Built to augment the Microsoft GPMC, GPOADmin provides comprehensive GPO management with additional features such as offline editing, reporting, archival and restoration, version control, test framework, change notification and approval, and quick rollback in the event that an object change has unexpected results.

New features

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Quest GPOADmin:

Platform support updates

- The following support has been added:
    - Ability to select Strict Encryption for SQL Server 2022 for data sent between the client and server when using SQL as the data store.

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.

PowerShell updates

- Set-Configuration command updated for Strict Encryption for SQL Server 2022 for data sent between the client and server.

Additional rights

- Ability to assign attestation using the "Attest" right.

- Ability to assign keywords using the "Assign Keywords" right.

Miscellaneous updates

- Users are warned if they attempt to remove Authenticated Users from a GPO.

Resolved issues

The following is a list of resolved issues in this release.

Table 1. Resolved issues

Issue	Issue ID
Service accounts and GMSAs configured with the minimum permission script are unable to create working copies of starter Group Policy Objects (GPOs) because the accounts are not granted the required "take ownership" permission.	199151
Right-clicking on a saved report in the reports folder and selecting "New Report" causes MMC to close unexpectedly.	504735
New DevExpress reports do not work if GPOADmin is not installed on C:\.	513015
Viewing GPO history causes GPOADmin to close unexpectedly.	517578
Typo in MinimumPermissisons error message for incorrect permissions.	512170
New Link button is not enabled in the OU Editor for non-admin users.	511895
Error when a non-administrator user selects an OU name when linking from a GPO.	517584

Known issues

ⓘ | **NOTE:** Defects with leading zeros (0) are from the Clarify system.

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 2. Installation and upgrade

Known issue	Issue ID
Change Auditor integration is lost during upgrade in Active Directory and AD LDS configuration stores. Workaround: To resolve this issue, reset the Change Auditor integration in the Service options.	496278
Change Window restrictions will not apply after upgrade until the Change Window actions list settings are reapplied.	428460
Index out of range exception is generated in the event log for the Watcher Service after upgrading. This will be resolved once the database is upgraded.	217430

Table 3. Cross-forest support

Known issue	Issue ID
If you create a SOM backup in one forest and import it to another, the links will appear as deleted GPOs if those GPOs cannot be accessed from the second forest.	0228454

Table 4. Version Control system

Known issue	Issue ID
Unable to import a historical version from Version Control if the source object was exported with the Copy History option enabled. Recommended workaround: Export the desired historical version to to disk and then Import from the disk.	523130
Inherited keywords are not displayed in the Keywords column in the list view.	519682
GPOADmin help Table of Contents is not available in MMC on Windows Server 2019.	499296
Service accounts and GMSAs configured with the minimum permission script are unable to create working copies of starter Group Policy Objects (GPOs) because the accounts are not granted the required "take ownership" permission.	499151
GPOADmin does not support Certificate references for Intune Configuration profiles.	498612
GPOADmin does not support Settings Catalog for Intune Configuration profiles.	498233
GPOADmin does not support iOS/iPadOS Security Assessment (Education) template from Intune Configuration profiles.	497162
Over time when using GPOADmin, the number of available detailed views (right pane views) in MMC will be exceeded causing a UI error. To mitigate this, expand views using the chevron icon rather than clicking on the node name.	482110
Validation of the Service Connection Point for the GPOADmin service account does not function for Group Managed Service Accounts.	380823
Export As Desired State Configuration requires users to have the Write permission on the Desired State Configuration Root directory.	377548
Compliance checks on a configuration profile which has had an assignment deleted from it in Azure do not show noncompliant differences in the Difference report.	286622
The Applications Preference extension is not supported during Group Policy Object merging.	265012
When synchronizing GPOs with the Use Migration Table Exclusively and Migrate Security Filter options set, GPOADmin may shutdown unexpectedly if an error occurs and the message exceeds 1024 characters.	244657
The context menu on the Linked Group Policy Objects page of the Group Policy Modeling Wizard results in the wizard loosing focus when launched via Citrix XenDesktop.	611801
Backups will not be removed for unregistered objects when running the Remove-Backups PowerShell command.	591669
Rolling back a moved OU does not move the OU back to it original location.	458939
Each time that you change the Enable workflow approval through email option, you must restart the service for the change to take effect.	360005
Compliance actions may result in an unhandled exception in the GPMC Extension. Workaround: To avoid this issue, you can either perform the compliance actions in the client or by running the Check compliance wizard.	322839
If users do not have the User role assigned on the Version Control root, they may not have the required rights to successfully run the User Activity report.	238909
If an object is renamed or deleted within Active Directory, the Approvals tab does not reflect the change.	246579
Some GPO settings are not backwards compatible between operating systems.	122825
When you edit GPOs, you are notified of persistent registry values through a flashing icon on the Registry Cleanup button in the GPO Editor. For this notification to display, you must first close and then open the GPO Settings property page by selecting the Edit menu.	240689
The Watcher Service needs to be restarted after changing Configuration Stores.	65408
Deploying a GPO containing existing Software Installation packages may cause each of those packages to be reinstalled on target workstations.	0222515

Table 4. Version Control system

Known issue	Issue ID
When checking for compliance, GPOADmin will not perform a backup if the unauthorized changes result in an object in the same state as the currently stored version.	106505
After changing storage locations, the individual version information is not transferred from the old storage location to the new. You must keep the old storage server online if you want to still access those individual versions.	0229309
When using the SeizeVCRole.exe utility, if a port is specified with the new server name, the utility assumes that the new server is an AD LDS instance. When using an Active Directory Version Control server, the default port of 389 does not need to be specified.	0229311
When you are editing a GPO with both the GPOADmin console and the GPMC Extension open, closing the Group Policy Object Editor may not return you to the expected interface.	91914

Table 5. Reports

Known issue	Issue ID
Global Configuration Settings sub-headers do not display correctly in the Difference report.	445715
The Change Auditor Working Copies report displays a non-functional "placeholder" link instead of the "Show/Hide" link that is used to expand and collapse the report details.	428685
For GPO difference reports to run properly when they contain Authentication Services settings, Quest Authentication Services must be installed on the GPOADmin client and the GPOADmin server.	284883
In the Difference Report, filters are not supported for GPO Preference settings.	151065
In the Group Policy Settings and Resultant Set of Policies reports, some dates (for example, Created, Modified and Applied date) will display with the time zone of the GPOADmin Server.	102486
Pre-existing GPO settings are being displayed in the Change Auditor Working Copies report.	194922
When viewing Preference settings in the Difference Report, the values displayed for text entries may have a capital letter when the actual value is a lower-case letter. This may cause some date settings to be incorrect.	150634

Table 6. User Account Control

Known issue	Issue ID
When installing the GPOADmin service on a system with User Account Control turned on, the installer must be launched using elevated privileges. To do this, run the 'Quest GPOADmin.msi' file from an elevated command prompt.	41286

Table 7. Third Party

Known issue	Issue ID
"Object reference not set to an instance of an object" error message when you view the GPO backup settings in the Group Policy Management Console.	http://support.microsoft.com/kb/2379592

System requirements

Before installing GPOADmin 5.20, ensure that your system meets the following hardware and software requirements.

Table 8. Hardware 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

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 (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.

- 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.

- Azure SQL managed instance

Watcher service

Same system requirements as GPOADmin.

Upgrade and compatibility

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.

- 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 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 ensure the "Ensure service account has access prior to deployment" service option is checked in the Options dialog.

- When you upgrade the Server, you must also upgrade the Client, GPMC Extension, and Watcher 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.

- The supported upgrade paths are from versions 5.18 and later.

- 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.

Authentication Services integration

- To view Unix settings in GPOADmin, Authentication Services must be installed after GPOADmin is installed. See Support Knowledge Article 82383.

NOTE: Authentication Services and GPOADmin integration

Due to rebranding, changes are required in the registry setting for the integration to function correctly.

Authentication Services installs to the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Quest Software\Quest Group Policy Manager\Extensions\vgp

GPOADmin requires the settings to be installed under this registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\Extensions\vgp

To import the settings into the registry at the correct location:

1 Export the key to a file, and change the key path (the bolded line) to the new path.

   Old path:

   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Quest Software\Quest Group Policy Manager\Extensions\vgp]

   "CLSID"="{F0648064-537A-45AF-98A4-74D2AABE867C}"

   "ReportingDLL"="C:\\Program Files (x86)\\Quest Software\\Authentication Services\\x64\\SettingsProvider.dll"

   "DisplayName"="QAS Group Policy for Unix"

   "NamespaceUri"="urn:schemas-quest-com:vgp"

   The new path:

   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOADmin\Extensions\vgp]

   "CLSID"="{F0648064-537A-45AF-98A4-74D2AABE867C}"

   "ReportingDLL"="C:\\Program Files (x86)\\Quest Software\\Authentication Services\\x64\\SettingsProvider.dll"

   "DisplayName"="QAS Group Policy for Unix"

   "NamespaceUri"="urn:schemas-quest-com:vgp"

2 Save the file.

3 Right-click the file, and select Merge. (You can also double-click it and select Yes on the warning dialog.)

   This settings will now be in the correct location required for the integration to function.

Compatible Products

GPOADmin is compatible with the following software:

• Change Auditor 7.4

Product licensing

To activate a new installation

1 Launch the GPOADmin client.

2 Right-click the GPOADmin node and select Connect To.

3 Select an existing connection or create a new one using the "New" button.

4   Click Connect.

5   When the Invalid License dialog box displays, browse to and select your GPOADmin license file and click OK.

To update your existing license for a given server

1   Launch the GPOADmin client and connect to the server where you want to update the license.

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**.

Getting started with GPOADmin

- Installation and upgrade instructions
- Additional resources

Installation and upgrade instructions

Refer to the Quest GPOADmin Quick Start Guide for installation and upgrade procedures.

Consider the following before installing GPOAdmin:

> **i** | **NOTE: Group policy modeling report**
>
> The Group policy modeling report displays the resultant set of policies based on the selected simulation options within the modeling session. An application partition is created during the simulation to house the report. It contains a temporary staging container that will be deleted once the report has been generated. The service account must have permissions to create an Application Partition in Active Directory.
>
> If required, you can create or delete the staging application directory partition:
>
> 1 Open Command Prompt.
>
> 2 Type:
>
> **ntdsutil**
>
> 3 At the ntdsutil command prompt, type:
>
> **domain management or partition management**
>
> 4 At the domain management command prompt, type:
>
> **connection**
>
> 5 At the server connections command prompt, type:
>
> **connect to server ServerName**
>
> 6 At the server connections command prompt, type:
>
> **quit**
>
> 7 At the domain management command prompt, do one of the following:
>
>   ▪ To create an application directory partition, type:
>
>   **create nc dc=staging,dc=gpoadmin DomainController**
>
>   For every domain controller which might be used to run the Group policy modeling report on, type the following:
>
>   **add nc replica "dc=staging,dc=gpoadmin" DomainControllerName**
>
>   ▪ To delete an application directory partition, type:
>
>   **delete nc dc=staging,dc=gpoadmin**

Additional resources

Additional information is available from the following:

- Online product documentation https://support.quest.com/technical-documents.
- Quest community https://www.quest.com/Community#.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. It supports simultaneous operation with multilingual data. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

About us

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 https://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.