

Quest® GPOADmin® 5.17

Release Notes

August 2022

These release notes provide information about the Quest GPOADmin release.

- [About this release](#)
- [New features](#)
- [Resolved issues](#)
- [Known issues](#)
- [System requirements](#)
- [Product licensing](#)
- [Getting started with GPOADmin 5.17](#)
- [About us](#)

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:

- Container management enhancements

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

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

The following commands have also been added for this functionality

- Get-BlockKeywordInheritance
- Get-ContainerBlockKeywordInheritance
- Get-ContainerKeywords
- Set-BlockKeywordInheritance
- Set-ContainerKeywords

- Set-ContainerBlockKeywordInheritance
- Microsoft Azure GCC High supported for email for notifications and approvals.
- Improved security for Office 365 and Exchange Online

To improve security, GPOADmin now requires certificate authentication for Office 365 and Exchange Online.

- Additional Microsoft Intune support

GPOADmin now includes support for Microsoft Intune's compliance policies. The following workflow actions are supported:

- Register/ Unregister
- Check In/ Check Out/ Undo Check Out
- Migration Actions
- Modify Security
- Apply Workflow / Approval Workflow order
- Failed Deployment
- Get/ Import
- Roll Back/ Restore/ Delete
- Incorporate Live
- Deploy
- Check Compliance

The following PowerShell commands have also been added to help manage Intune support:

- Add-ConfigurationProfileAssignments has been renamed to Add-IntuneAssignments and functions for both configuration profiles and compliance policies.
 - Clear-ConfigurationProfileAssignments has been renamed to Clear-IntuneAssignments and functions for both configuration profiles and compliance policies.
 - Remove-ConfigurationProfileAssignments has been renamed to Remove-IntuneAssignments and functions for both configuration profiles and compliance policies.
 - Get-ConfigurationProfileAssignments has been renamed to Get-IntuneAssignments and functions for both configuration profiles and compliance policies.
 - Get-Unregistered and Get-SettingsReport now support compliance policies.
- GPO synchronization enhancements:
 - Ability to validate synchronization results. You can easily see the synchronization results and view which GPOs have been successfully (or unsuccessfully) synchronized on the selected target.
 - Synchronization status.
- Validation rule enhancements for protected settings

Ability to include the processing of added items when the validation rule is set to Value.
- Additional platform support
 - Windows Server 2022
 - Windows 11
 - Microsoft Edge WebView2 Evergreen Bootstrapper 97.0.1072.69
- Miscellaneous updates
 - Ability to configure SQL replication from within the client.

- Ability to include the contents of the Settings and Difference reports in the body of the notification email.
- New Modify Link Properties right.
- Ability to restrict which global catalogs are used within the forest to search for the GPOADmin server during connection.
- Ability to schedule the generation of RSoP reports to validate whether the desired Group Policy settings have been applied.
- Ability to use Microsoft Graph APIs when using Office 365 for notifications.
- Selected items are automatically refreshed on right-click.
- Default SPN set on install now uses server and port format.

Resolved issues

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

Table 1. Resolved issues

Issue	Issue ID
Importing into an OU from a backup does not function properly.	379848
Restore GPO with links not functioning properly.	379850
Upgrading with SQL replication issue has been resolved. Users are now prompted to allow GPOADmin to end replication pre upgrade and restore replication post upgrade. If they select not to go this route, they will need to manually end replication before you can continue with the upgrade process.	225119
Synchronization to locked objects is allowed.	225122
Opening the version control options dialog causes GPOADmin to become unresponsive if the OAuth 2.0 credentials used for authentication are expired.	224317
Importing a DSC script backup into a file that has existing content does not function properly.	224340
An exception error occurs when you perform a checkout and deploy after a rollback.	224322
PowerShell becomes unresponsive if you close the authorization window before authorization is granted while executing the Set-GmailOptions command. Workaround: Set the Gmail options through the GPOADmin console.	191287

Known issues

i | **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
Existing custom search folders will not function after an upgrade. NOTE: This is not an issue for an update from 5.16.	254617
Index out of range exception is generated in the even 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
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
After migrating the configuration store from Active Directory to SQL, backups are not removed when pressing the Apply Settings button on the Backup Retention page of the Service Options.	225272
Running GPOAdmin.ConfigMig.exe does not migrate all service options as expected.	225003
The context menu on the Linked Group Policy Objects page of the Group Policy Modeling Wizard results in the wizard losing 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 its original location.	458939
Using SQL as a backup store will not allow you to export historical versions of GPOs as Protected Settings Policies.	370605
When adding or removing account from the Access tab in the GPOAdmin Properties, the display may not function properly and hide accounts.	445238
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
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

Table 4. Version Control system

Known issue	Issue ID
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
Hide and show link is not functioning properly on the Group Policy Modeling report.	281016
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
The MMC snap-in may become unresponsive when running the Group Policy Object Consistency Report with 5000 or more GPOs.	108930
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
Information about new Group Policy preferences in Windows Server 2008.	http://support.microsoft.com/kb/943729
"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 5.17, 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 8.1 Windows 10 Windows 11 Windows Server 2012 Windows Server 2012 R2 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 2013
- Microsoft Exchange 2016
- Microsoft Exchange 2019

Configuration store requirements

- Active Directory (Not recommended)
- AD LDS
- SQL Server (Supported version include 2012, 2012R2, 2014, 2016, 2017 and 2019)

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

Backup store requirements

- Network Share (recommended)

- Active Directory (not recommended)
- AD LDS
- SQL Server (Supported version include 2012, 2012R2, 2014, 2016, 2017 and 2019)

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

Watcher service

Same system requirements as GPOAdmin.

Upgrade and compatibility

Note the following when upgrading GPOAdmin:

- During the upgrade a Files in Use dialog may open and reference the GPOAdmin Dashboard Service Host. You can safely ignore this and click **OK** to proceed with the default **Close the applications and attempt to restart them**.
- 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 5.15 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**.

Authentication Services integration

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

i 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\vgrp

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

HKEY_LOCAL_MACHINE\SOFTWARE\Quest\GPOAdmin\Extensions\vgrp

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\vgrp]

"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\vgrp]

"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 5.17 is compatible with the following software:

- Change Auditor 7.2

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 5.17

- [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 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.

© 2022 Quest Software Inc.

ALL RIGHTS RESERVED.

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

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

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

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

Legend

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

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