

Quest® Active Administrator® 8.5
What's New Guide



© 2020 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 (<https://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 <https://www.quest.com/legal>.

Trademarks

Quest, Active Administrator, and the Quest logo 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.

Contents

What's New in Active Administrator	2
Additional Supported Platforms	2
License adjustments	2
Active Directory Health enhancements	2
Web console enhancements	4
Other enhancements	7
About us	10

What's New in Active Administrator

Active Administrator® 8.5 is the latest release of Quest Software's complete solution for managing Microsoft® Active Directory® health, delegation, accounts, GPOs, recovery and security auditing, and certificate and DNS management. This document provides a highlight of these improvements.

i | **NOTE:** The Certificate Management, Azure Active Directory, DNS Management, and Active Directory Health modules each require a license in addition to the license for Active Administrator.

This document highlights key features new in this release. For more information about these or any features, see the *Quest Active Administrator 8.5 User Guide*.

Topics

- [Additional Supported Platforms](#)
- [New Required Software](#)
- [Active Directory Health enhancements](#)
- [Web console enhancements](#)
- [Other enhancements](#)

Additional Supported Platforms

The following platforms are now supported in Active Administrator.

- Windows Defender Credential Guard

i | **NOTE:** Active Administrator can run in environments that have Windows Defender Credential Guard enabled. Due to compatibility issues with the Autorun utility, Active Administrator must be installed manually using the Active Administrator 8.5 Server.MSI file found with the installation CD or download package.

New Required Software

The following software is required for Active Administrator 8.5.

- Microsoft® .NET Framework 4.7.2

Active Directory Health enhancements

New Options

- **Create Notification**
Create a notification in which the selected alert should be included. Select **Active Directory Health | Alerts | Create Notification**.
- **Add to Notification**
Set the notifications in which the selected alert should be included. Select **Active Directory Health | Alerts | Add to Notification**.
- **Add Windows Event Log Alerts**
Select the event logs for which an alert should be generated. Select **Active Directory Health | Agents | Monitored Domain Controllers | Settings | Domain Controller | Event Log**.
- **Manually install Active Directory Health Analyzer agents**
Install the Active Directory Health Analyzer agents into a pool or onto domain controllers manually. Copy **C:\Program Files\Quest\ActivAdministrator\Server\SLAgent\DAAgent** to **C:\Windows** and use **Setup.exe -help** to see the usage details of the available parameters.

Web console enhancements

New Options

- **Display Active Alert Details**
Selecting an active alert now displays the details of that alert below the list of alerts. Select **Active Directory Health Dashboard | Active Alerts**.
- **Purge Health Check History**
Added the ability to purge Active Directory Health Check history that is older than a specified number of days. Select **Monitor | Active Directory Health Check | Purge Health Check History**.

New Reports

- **Authentications - Average Number of Kerberos and NTLM Requests for Authentication by DC Hourly or Daily**
This report displays the average number of Kerberos and Windows NT LAN Manager (NTLM) authentication requests being processed per test for a given domain controller and time period. All dates are in Coordinated Universal Time (UTC). **Report | Active Directory Health | Authentications - Average Number of Kerberos and NTLM Requests for Authentication by DC Hourly or Daily**.
- **Directory Changes Report**
This report displays the average number of directory change requests being processed for a given domain controller and time period. All dates are in Coordinated Universal Time (UTC). Select **Report | Active Directory Health | Directory Changes Report**.
- **DNS Query Time Report**

This report displays the responsiveness of the DNS servers used by the domain controllers. Select **Report | Active Directory Health | DNS Query Time Report**.

- **Object Type Summary**

This report shows the count of the objects by type in specified Active Directory path. Select **Report | Security | Object Type Summary**.

- **Page Faults - Top N DCs**

This report displays the Top N domain controllers that have the biggest average number of pages faulted per second in the specified period of time. Select **Report | Active Directory Health | Page Faults - Top N DCs**.

- **Top N Lowest free disk space on the selected DC In Last Week, Month**

This report displays the Top N domain controllers that are running out of disk space on the drive that hosts the directory service database. Select **Report | Active Directory Health | Top N Lowest free disk space on the selected DC In Last Week, Month**.

Other enhancements

PowerShell

ActiveAdministrator Module

You can now manage Active Administrator active templates and delegations using the Windows PowerShell interface. To open the PowerShell Console with the ActiveAdministrator module imported, select **Settings | AA PowerShell Console**. To display all cmdlets in the module, use **Get-Command -Module ActiveAdministrator**.

Auditing and Alerting

Excluding accounts from auditing

You can now select the accounts for which events will be excluded from auditing. Select **Auditing & Alerting | Event Definitions | Exclude Accounts**.

Certificates

Group Support

When managing certificates, there is now an option to select a group containing the computers to be monitored. You can include nested groups or monitor groups for added or removed computers. Select **Certificates | Certificate Management | Computers | Add | Select Group**.

The option to view Monitored Organizational Units has been changed to Monitored Objects and now includes Groups. Select **Certificates | Certificate Management | More | Monitored Objects**.

Purging Certificate Authority Backups

When managing certificates, there are new options related to purging Certificate Authority Backups.

- **Clear History** - facilitates clearing the history of the Certificate Authority Backups that have been purged. Select **Certificates | Certificate Authority | Clear History**

- Schedule Certificate Authority Backup Purge - facilitates scheduling the purge of Certificate Authority Backups. Select **Certificates | Certificate Authority | Schedule**
- Purge Certificate Authority Backup Now - facilitates the immediate purge of Certificate Authority Backups. Select **Certificates | Certificate Authority | Schedule | Purge Now**

Group Policy

Schedule GPO Backup Purge

You can now schedule the purge of GPO backups. Select **Group Policy | GPO Backup | Schedule Purge**.

Security and Delegation

Smart Card Logon Required

The All Users view now contains the option to display a column indicating when Smart Card Logon Required is set. This column is displayed by default. Select **Security & Delegation | Security | View | All Users | Columns | Smart Card Logon Required**.

The All Users view now contains the option to filter the results based on whether or not Smart Card Logon Required is set. Select **Security & Delegation | Security | View | All Users | Filters | Time | Smart Card Logon Required**.

Copy an Active Template

You can now make a copy of the selected active template and choose the category to which the copy should belong. Select **Security & Delegation | Active Templates | Copy**.

Add Exclusions for Change Your Password Reminders

You can now exclude password reminders by domain with the following options.

- Exclude Organization Unit
- Exclude Users and Groups
- Exclude user account if it is enabled/disabled
- Starts with <condition> (applies to user and computer objects only)
- Ends with <condition> (applies to user and computer objects only)
- Exclude user accounts with less than X days before their password expires
- Exclude user accounts with more than X days before their password expires

Select **Security & Delegation | Password Reminder | Exclusions**.

Server Manager

Security Manager

The Server Manager now contains a Security Manager where you can manage the passphrase, file security, and database security. Open **AA Server Manager** and select **Security Manager | Manage**.

SQL Full-Text Search Status Indicator

When SQL Full-Text Search is enabled, it now shows the current index status. Clicking on the index status will update it. Open **AA Server Manager** and see **SQL Full-Text Search**.

Support Windows Authentication

Web Server Configuration now contains an option to Enable Windows Authentication for the web login. To support Smart Card Authentication, you must enable Windows Authentication and use the Microsoft Edge browser when logging into the Active Administrator Web Console. Open **AA Server Manager** and select **Web Server Configuration | Enable Windows Authentication**.

Installation and Upgrade

The Active Administrator for Azure Active Directory module has been removed from the Active Administrator Console and the Active Administrator Web Console.

The default TCPConnectionPoolingEnabled value for deployed AD Health agents is now maintained during upgrades. The default value is now True.

The Active Administrator share is now created with Authenticated Users permissions instead of Everyone - Full Control permissions. You can modify the permissions of the share to only allow access to the service accounts used by Active Administrator services and by the users who run the Active Administrator console.

Configuration Wizard

When creating a new archive database, the default database and log size will now be based on the size of the SQL Server System Database model. Previously, the default database and log size was 50MB.

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.

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.