Quest

Active Administrator® 8.3
What's New 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 (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, the Quest logo, Active Administrator, and Join the Innovation 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.

Active Administrator What's New Guide
Updated - October 2018
Software Version - 8.3

Contents

1

What’s New in Active Administrator

Quest® Active Administrator® 8.3 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.

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 8.3 User Guide*.

Additional supported platforms

- SQL Server® 2017
- Transport Layer Security (TLS) 1.2

Azure Active Directory Connect Health Monitoring

Once you install the Active Administrator® Azure® Active Directory® Connect Health Monitoring Agent on a computer where Microsoft® Azure Active Directory Connect is installed, you can view a summary of the output of the Synchronization Service Manager; manage the Azure Active Directory Connect Scheduler; view warnings, errors, and events that occurred over the last 24 hours; view a list of the installed connectors, properties, and partitions; and run profiles of selected connectors. Select **Active Directory Health | Active Directory Connect** and use the tabs to analyze Azure Active Directory Connect.

Network Operations Center

The Network Operations Center (NOC) in the Active Administrator Web Console provides a centralized location where you can monitor your forests, domains, sites, and domain controllers. You can view a summary of data points, view active alerts, and detailed information on each domain. You also can create topology diagrams for a visual representation of your network. To customize your view of the NOC, create unique profiles to view the specific data you need. Open the Web Console and click **NOC View**.

Web Console - new authentication method

Added the ability to log out of the Active Administrator Web Console. (**user name | Log Out**). Added options to manage session timeouts, and expiration and refresh of the authentication token (**Start** | **AA Server Manager** | **Configure**).

Trend report for all domain controllers

The Domain Controller Trend report (**Report | Active Directory Health**), displays the average performance values on a domain controller.

Values include:

- Cache copy read hits
- CPU processor time
- DFSRS % processor time, private bytes, USN records accepted, and working set
- LSASS % processor time, private bytes, and working set
- file replication (NTFRS) staging space free in kilobytes
- memory page faults a second
- NTDS DRA inbound properties filtered a second, LDAP searches a second, and LDAP writes a second
- Server sessions

Physical Memory Utilization report

Report	Description
Domain Controllers Memory Utilization	Displays the top domain controllers sorted by the average % of physical memory consumed over a specified period of time. **NOTE:** You can select only domain controllers that are monitored by Directory Analyzer agents and for which there is data about memory consumption. **Minimum required permission:** Domain User rights.

Encryption updated from 3DES to AES

Active Administrator® was updated from Triple Date Encryption Algorithm (3DES) to Advanced Encryption Standard (AES-256). During the configuration of the Active Administrator server for both new installations and upgrades, users are required to create a passphrase. This passphrase is used to generate part of the symmetric encryption key.

IMPORTANT: The passphrase can never be restored or changed. Therefore, the passphrase should be stored in a secure location.

PowerShell cmdlets

Active Administrator® PowerShell cmdlets mirror the included utilities in the AA Server Manager application (**Start | Quest | AA Server PowerShell Scripts**).

The cmdlets are located at C:\Program Files\Quest\Active Administrator\Server\PowerShell. You can run the cmdlets from the PowerShell console (right-click the cmdlet, and choose **Run with PowerShell**) or PowerShell ISE (open the cmdlet in ISE and click **Run**) or use the cmdlets manually. See the *Active Administrator User Guide*, appendix B for detailed instructions.

IMPORTANT: All command utilities should be run while logged on as an Administrator. Cmdlets marked with an asterisk must be run as an administrator with elevated privileges (if UAC is enabled). The cmdlets should be used only by those familiar with Windows PowerShell®.

These Active Administrator cmdlets display the current settings for the Active Administrator server.

Cmdlet	Description
Get-AAFeaturesLicenseStatus*	Get the status of Active Administrator licenses
Get-AAWebServerConfiguration	Get the configuration settings for the Web server
Get-ADSLoggingStatus	Get logging status for ADS
Get-ADSOperationStatus*	Get operation status for ADS
Get-ADSPort	Get the port number for ADS
Get-AFSLoggingStatus	Get logging status for AFS
Get-AFSOperationStatus*	Get operation status for AFS
Get-AFSPort	Get the port number for AFS
Get-AFSHTTPOperationStatus	Get operation status for the HTTP service
Get-FullTextSearchStatus	Get the status of Full-Text Search
Get-NotificationServiceOperationStatus*	Get operation status for the Active Administrator Notification Service

These Active Administrator cmdlets mirror the options provided in AA Server Manager.

Cmdlet	Description
Clear-AFSCache	Clear the AFS cache
Set-AALicense	Update the Active Administrator license
Set-AAWebServerConfiguration	Set configuration for the Active Administrator Web server
Set-ADSPort	Set the port for ADS
Set-AFSAndADSStartup Account	Set the startup account for AFS and ADS
Set-AFSPort	Set the port for AFS
Set-NotificationServiceStartupAccount	Set the startup account for the Active Administrator Notification Service
Switch-ADSLoggingStatus	Switch logging status of ADS
Switch-ADSOperationStatus	Switch operation status of ADS
Switch-AFSLoggingStatus	Switch logging status of AFS
Switch-AFSOperationStatus	Switch operation status of AFS
Switch-AFSHTTPOperationSatus	Switch operation status of the HTTP service
Switch-FullTextSearchStatus	Switch the setting of Full-Text Search
Switch-NotificationServiceOperationStatus	Switch operation status of the Active Administrator Notification Service

Email configuration

Throughout Active Administrator, you can set up notifications to notify email recipients of various alerts and situations. Each notification has its own list of email addresses. With this version of Active Administrator, you can now manage these email address lists in one place. Select **Settings | Email Configuration**, select the module, and select the email address list. Here you can also change the email address of the Active Administrator owner.

Table 1. Email address lists

Module	Email address list
Configuration	Service Monitoring Policy
Security & Delegation	Inactive Accounts
	Password Reminder Settings
	Account Expiration
	Active Templates
Active Directory Health	DA Agent Auto Deploy
	DA Agent Notification Settings
	All DA Notifications
Certificates	Certificate Settings
Auditing & Alerting	Agent Auto Deploy Configuration
	Auditing and Alerting Alerts

Miscellaneous enhancements

Change ownership of scheduled reports

When a user creates a scheduled audit report, that user owns the report schedule and only that user can see the schedule. In the event a user leaves the company, another user with Full Control permissions for Active Administrator can take over the ownership of the scheduled reports. Select **Auditing & Alerting | Audit Reports | Scheduling | Scheduled Reports**, select a report, select a schedule, click **Edit** if you own the schedule or **View** if you do not, and then click **Take Ownership** or **Transfer Ownership**. You also can create a new schedule from the schedule of another account by clicking **Add** and using the take ownership feature.

Exclude domain controllers from Active Directory Health tests

Exclude specified domain controllers when analyzing forests, domains, and sites, and from matching Active Directory Health Check tests. Excluded domain controllers will also be removed from the Agent Configuration wizard.

Edit the file **ExcludedDomainControllers.xml**, which is located in the **AAServer\DACache** folder. See the *Active Administrator 8.3 User Guide* for details.

Daily performance report sent to email recipients

A daily performance report contains the average values for CPU usage, memory usage, data points, errors, warnings, restarts, and work load; and indicates if an update is required for each Directory Analyzer agent. You can specify email recipients and set the start time for data collection (**Active Directory Health | Agents** | **Analyzer Agents** tab | **More | Agent Performance Settings**).

Monitor audit report updates

Capture the user account that modifies or deletes audit reports and alerts. Create a new report that captures the **Active Administrator Report Updated** and **Active Administrator Audit Report Deleted** events to see who updated or deleted any reports (**Auditing & Alerting | Audit Reports | New**).

Use ‘password does not expire’ as a criteria for determining inactive accounts

Exclude accounts with passwords set to never expire when creating a report of inactive users (**Security & Delegation | Inactive Accounts | Users & Computers | Identify Inactive Users Only | Exclude accounts that have passwords set to not expire**).

Active Directory Health agents have option to select all sites

When adding new or modifying existing Directory Analyzer Agent servers in an agent pool and selecting sites to monitor, the options to **Select all** or **Clear all** were added.

Browse button for preferred domain controller

Browse for the preferred domain controller (**Configuration | Preferred Domain Controllers**).

Change the path for Active Administrator Active Directory backups

Change the location of Active Directory backup files (**Configuration | Recovery Settings | Override AD Backup share path**). Only newly created backup files appear in the new location. Existing backup files must be moved manually.

Automatically configure Windows firewall

Automatic configuration of Windows® Firewall allows the Directory Analyzer and Azure Active Directory Connect agents to communicate with the Active Administrator Data Service (ADS). For the Directory Analyzer agent, you can select to configure the firewall during agent installation or after installation at **Active Directory Health |**

Agents | More | Configure Firewall Rules. For the Azure Active Directory Connect agent, use `/i /setFWRules` when installing the agent and `/setFWRules` after installation.

Graceful handling if the preferred domain controller is offline

Verify a preferred domain controller before use. If the preferred domain controller is off-line, you can choose to use the primary domain controller (PDC) in the domain or allow Active Directory to choose the domain controller (**Configuration | Preferred Domain Controllers**).

Agent deployment displays only unmonitored domain controllers from the selected site

During agent deployment, only the unmonitored domain controllers from the selected site display in the selection list.

Security | Domain | View All Users contains a column for 'Password Never Expires'

New **Password Never Expires** column when viewing all users (**Security & Delegation | Security | View | All users**). The column is included when filtering and exporting the list of users.

Select multiple objects to perform an action

Perform actions, such as deleting, unlocking accounts, and moving to another OU on multiple selected items, such as users, computers, and groups (**Security & Delegation | Security**). Actions that cannot be performed on multiple selected items are unavailable. If different types of items are selected, only actions that can be performed to all selected types are available.

Report containing all critical alerts for a specific alert for a specific time period

Filter Directory Analyzer alert history (**Active Directory Health | Alerts | Filter History**) and the Alert History Report (**Active Directory | Alerts | Alert History Report**) by the type of alerts and the severity of the alerts.

Ability to add a logo/image to the password reminder emails

Include a logo/graphic in password reminder emails (**Security & Delegation | Password Reminder | Message | Edit | Inline Picture**).

Anti-forgery added to the Active Administrator Web Server

Anti-forgery was added to the Web Server to prevent POST and DELETE requests to the Active Administrator API from sources unauthorized to perform such requests. All POST and DELETE requests are now equipped with anti-forgery cookies and anti-forgery headers.

Alert History filter added to the Active Administrator Web Console

Filter Directory Analyzer alert history (**Monitor | Active Directory Health | Alert History | Filter**) and the Alert History Report (**Monitor | Active Directory Health | Alert History | Report**) by the type of alerts and the severity of the alerts.

Ability for the SRV record test to use the netlogon.dns file on each domain controller to compare with the registered SRV records in DNS

New alert (SRV record is not registered in DNS) and general data collector (Compare SRV DNS records with netlogon.dns file) to identify missing SRV records in the netlogon.dns file on each domain controller.

Add a general setting within the Console to change the instance

Change the volume instance for the DFS Replication Service through the DFSRS USN Records Accepted data collector (**Active Directory Health | Agents | Monitored Domain Controllers |** select a domain controller **| Data Collectors | Domain Controllers | DFSRS USN Records Accepted**).

Prevent license file from modification and enhanced license compliance

The number of licensed users and enabled users in Active Directory® from the License Dashboard (**Settings | License Dashboard**) now display at the bottom of the console window. If you click the numbers, the License Dashboard opens.

Enhance GPO synchronization status time for large number of GPOs

Enhanced the GPO synchronization status time for a large number of GPOs, so the generation time for the GPO Consistency report is reduced (**Report | Active Directory Health | GPO Consistency**).

GPOs from domain controllers are cached. If you generate a GPO Consistency report and want to see changes when you run the report again, check the **Reload Cache** check box.

Add print button to Active Directory Health

Print the details of a selected data collector in the Active Directory Health Check report results (**Monitor | Active Directory Health Check**).

Password Reminder email customization

Customize the subject line of the Password Reminder email message (**Security & Delegation | Password Reminder | Message**). Use %FIRSTNAME%, %LASTNAME%, %DISPLAYNAME%, %DATE%, %LASTCHANGEDATE%, and %DAYSLEFT% in the subject line.

Refresh OU lists

Refresh the list of organizational units (OUs) when making selections. Clicking **Refresh** reloads the list of organizational units and clears any selections.

View backup files from single domain

Use the **Domain** drop-down list to manage the list of backup files when selecting a backup for recovery. By default all domains are listed, but now you can select a single domain to view only those backup files (**Recovery | Object Recovery**).

Suppress Active Directory Health alert notifications

Suppress notifications if an alert clears itself within a specified time frame. You can set it during the create notification wizard (**Active Directory Health | Agents | Notifications** in the Console or **Monitor | Active Directory Health |Notifications | Add Notification** in the Web Console) or while editing a selected notification.

New data collectors and alerts

New data collectors and corresponding alerts (see the *Alerts Appendix* in the *Active Administrator User Guide*):

- Active Directory Certificate Services
- Active Directory Web Services
- Detected NO_CLIENT_SITE record
- DNS Client
- File Replication Service
- Intersite Messaging

- Security Accounts Manager Service
- Workstation Service

Documentation updates

- Minimum permissions for the Diagnostic Console are in the Install Guide and the User Guide.
- Instructions for deploying workstation logon audit agent from a Group Policy Object (GPO) are in the *Active Administrator User Guide* and online help. See *Setting up workstation logon auditing* | *Deploying the workstation logon audit agent* | *Deploying the workstation logon agent from a GPO* in the *Configuration* chapter.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

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 www.quest.com/contact.

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.