Active Administrator

Complete Active Directory management from a single console

Windows network administrators must increasingly manage critical Microsoft Active Directory environments more quickly and with fewer staff. Doing more with less increases the likelihood of accidental changes to Active Directory (AD) objects, configurations and Group Policy data that can raise your risk of hardware and software failure. The need to enforce internal policies and address compliance regulations only adds to the challenge. You need an all-inclusive, cost-efficient solution that can help you secure, manage, maintain, audit and prevent problems in AD and Group Policy environments.

Active Administrator is an extensive Active Directory management solution that allows you to control auditing, security, recovery and health for Active Directory from a single integrated console. By centralizing the management of the most important capabilities of AD and Group Policy, Active Administrator saves you time and delivers maximum control over your environment.

FEATURES AND BENEFITS

Auditing and change control — Use a single, consolidated audit record to track changes in AD, Group Policy and Active Administrator. Easily customizable with flexible reporting, alerting and event filtering, the audit record makes it quick and easy to troubleshoot problems and demonstrate that proper auditing and alerts occurred where appropriate. You can even automate proactive actions to take place when specified events occur.

Figure 1. Active Administrator delivers a complete solution for managing your Active Directory.

> "Active Directory is the biggest application we use. It controls security and directly affects how all employees do their job. Being able to back up/recover AD and Group Policy Objects is a huge timesaver and offers great peace of mind."
>
> *Derek Schauland, Microsoft MVP, MCTS, IT Manager, Briess Malt & Ingredients Co.*

BENEFITS:

- Improves regulatory compliance enforcement of internal policies with comprehensive audit trails, access controls and reporting
- Tightens security through simplified, standardized security management, elimination of overprivileged users and consistent delegation of AD administration
- Maintains business continuity by delivering alerts on AD and GPO changes to reduce network and user downtime, and by ensuring rapid recovery from accidental changes, deletions and administrative errors
- Increases IT efficiency by simplifying routine AD management tasks to give you more time for business-critical tasks
- Ensures AD health by monitoring replication and domain controller status and performance, and by automating database maintenance

SYSTEM REQUIREMENTS

PROCESSOR

1GHz Pentium

DISK SPACE

100MB

OPERATING SYSTEMS

Windows Server 2012

Windows Server 2012 R2

Windows Server 2016

Windows Server 2019

SERVER INSTALLATION

Group Policy Management Console

Microsoft SQL Server 2012, 2014, 2016, 2017 and 2019

Microsoft SQL Express 2012 and 2014

.NET Framework v.4.5.2 and 4.6

DETAILED REQUIREMENTS

See the Release Notes for the full list of system requirements.

Security management — Streamline processes for applying security policies and permissions to improve productivity. You can quickly identify overprivileged users and clean up their accounts. You can also delegate administrative control quickly and consistently with customizable, reusable and self-healing templates. A centralized audit trail of all changes helps you manage change control.

Group Policy management — Manage, report, compare, roll back and analyze changes in Group Policy easily from a single location. Modeling enables you to simulate changes and test what-if scenarios. The Offline Repository enables users without administrative rights to manage Group Policy Objects (GPOs) without the risk of editing them live. Undo changes using automated backups and version history.

Accounts — Perform universal searches that easily and efficiently locate any user, group, contact, computer or organizational unit (OU) in a selected domain. Quickly identify inactive users and computers to clean up these accounts, and simplify management in an automated, proactive manner. Configure daily email notifications of pending account expirations, as well as preview all accounts that will expire by a user-defined threshold. Send reminders to users with expiring or expired passwords to reduce user/password maintenance headaches. Enhance password security with fine-grained password policies for individual users or groups.

Backup and recovery — View essential Active Directory and Group Policy information in one place. Preview and quickly restore items, including users, security descriptors, OUs, objects, attributes, group memberships and individual Group Policy versions from your automated backups.

AD health assessments — Monitor and run health and performance assessment reports on AD configuration, replication and domain controllers to ensure availability of your Active Directory and ease administrative burden.

DNS management — Proactively manage, monitor and alert on DNS server health with free access to Active Administrator for DNS Management. Enable your IT administrators to proactively manage, monitor and alert on Domain Name Server health and availability from a single, easy-to-use console.

ABOUT QUEST SOFTWARE

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

DataSheet-ActiveAdmin-US-KS-55731