Change Auditor for Active Directory

Real-time auditing for Active Directory and Azure Active Directory

Active Directory (AD) issues can result in unplanned and costly service disruptions as well as business-crippling network downtime. Harmful data breaches and non-compliance with GDPR, PCI, HIPAA, SOX and more can cause you to incur hefty costs as well. You need Active Directory security auditing that ensures you're notified in real time of critical changes to AD, Azure AD and ADFS configuration.

Quest® Change Auditor for Active Directory drives the security and control of your hybrid AD environment by providing real-time threat monitoring and proactive object protection to prevent unwanted changes. Change Auditor tracks, audits, reports and alerts on the changes that impact your on-premises and cloud environments — without the overhead of turning on native auditing. With Change Auditor for AD, you'll get a normalized view of all changes and any related event details, including before and after values, as well as the correlated on-premises and cloud identities. You can also add comments explaining why a specific change was made in order to fulfill audit requirements. With Change Auditor for AD, you'll be able to quickly and efficiently audit all critical changes to keep your valuable data and resources secure.

AUDIT ALL CRITICAL CHANGES

Get extensive, customizable auditing and reporting for all critical AD, Azure AD and ADFS changes, including those made to Group Policy Objects (GPOs), your Domain Name System (DNS), server configurations, nested groups, the NTDS.dit file itself, and much more. Unlike native auditing, you'll get a consolidated view of all on-premises, cloud and hybrid AD change activity with in-depth forensics on the relation to other events over the course of time in chronological order.And, with proactive alerts, you'll be able to maintain constant awareness and respond from anywhere — and on any device — to vital policy changes and security breaches as they occur, reducing the risks associated with day-to-day modifications.

With Change Auditor for Active Directory, you'll get the who, what, when, where and originating workstation of all changes, in chronological order, including correlated on-premises and cloud identities.

> "We've had pen testers come in and be very surprised that they could not get past the Change Auditor object protection."
>
> *Enterprise Administrator, Large Retail Chain*

BENEFITS:

- Installs in minutes with fast event collection for immediate analysis
- Enables enterprise-wide, on-prem & cloud auditing and compliance from a single client
- Eliminates unknown security concerns, ensuring continuous access to applications, systems and users by tracking all events and those changes related to specific incidents
- Reduces security risks with real-time alerts to any device for immediate response
- Strengthens internal controls with protection from unwanted changes and limits control of authorized users
- Drives availability by enabling proactive troubleshooting for account lockouts
- Reduces the performance drag on servers and saves storage resources by collecting events without the use of native auditing
- Streamlines compliance to corporate and government policies and regulations
- Turns information into intelligent, in-depth forensics for auditors and management

"Overall, Change Auditor has been very useful. No other product we evaluated offered the same level of real-time auditing and protection, without requiring Windows auditing be enabled for all Active Directory changes."

Patrick Rohe
Senior IT Architect
Towson University

SYSTEM REQUIREMENTS

For a detailed and current list of system requirements, please visit quest.com/products/change-auditor-for-active-directory.

TRACK USER ACTIVITY AND PREVENT UNWANTED CHANGES

Tighten enterprise-wide change and control policies by tracking user and administrator activity for account lockouts and access to critical registry settings. With proactive controls to prevent critical changes from happening in the first place, to 24x7 alerts, in-depth analysis, the ability to restore previous values and reporting capabilities, your AD and Azure AD environments are protected from exposure to suspicious behavior and unauthorized access, and it's always in compliance with corporate and government standards.

SECURITY THREAT MONITORING

Audit and block exploits such as AD database copies via NinjaCopy and credential theft via unauthorized domain replication using DCSync.

TURN IRRELEVANT DATA INTO MEANINGFUL INFORMATION TO DRIVE SECURITY AND COMPLIANCE

Track critical changes and then translate that raw data into meaningful, intelligent insights to help safeguard the security and compliance of your infrastructure. Change Auditor for AD helps you get the who, what, when, where and originating workstation of changes as well as any related event details, including before and after values, so you can make quick decisions where your security is concerned. You'll also be able to make auditing limitations a thing of the past with the Change Auditor high-performance auditing engine. And without the need for native audit logs, you'll see faster results and storage savings.

INTEGRATED EVENT FORWARDING

Easily integrate with SIEM solutions to forward Change Auditor events to Splunk, ArcSight, QRadar or any platform supporting Syslog. Additionally, Change Auditor integrates with Quest® InTrust® for 20:1 compressed event storage and centralized native or third-party log collection, parsing and analysis with alerting and automated response actions to suspicious events.

AUTOMATE REPORTING FOR CORPORATE AND GOVERNMENT REGULATIONS

With a built-in compliance library as well as customizable reports, proving compliance with government standards, like GDPR, PCI DSS, HIPAA, FISMA / NIST, SOX, and GLBA, is a breeze.

HOSTED AUDITING DASHBOARD WITH ON DEMAND AUDIT

Upgrade to the On Demand Audit Hybrid Suite for Office 365, which includes Change Auditor for Active Directory, Change Auditor for Logon Activity and On Demand Audit. Pair them easily in a few clicks to get a single, hosted view of all changes made across AD, Azure AD, Exchange Online, SharePoint Online, OneDrive for Business and Teams. Simplify investigations with responsive search and interactive data visualization, and retain audit history for up to 10 years.

ABOUT QUEST

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. Quest Software. Where next meets now.

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-ChangeAuditorAD-US-LR-64107