mergerIT

ENABLING STABLE IT FOR BUSINESS GROWTH

Quest

Change Auditor

Change Auditor for Active Directory

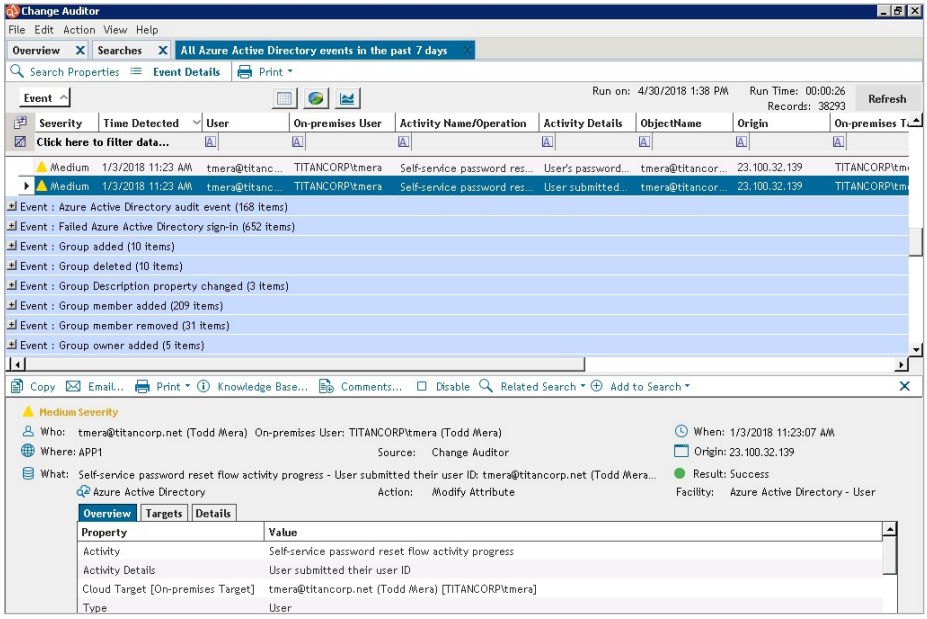
Real-time auditing for Active Directory and Azure Active Directory

Microsoft Active Directory (AD) is at the heart of your mission-critical network infrastructure. Issues with your AD can result in unplanned and costly service disruptions and business-crippling network downtime — not to mention hefty costs from harmful security data breaches and non-compliance with critical government regulations, such as SOX, PCI, HIPAA, GDPR and more. Organizations need to be notified — in real time — of critical changes to both AD and Azure AD.

Quest® Change Auditor for Active Directory drives the security and control of AD and Azure AD by tracking all key configuration changes and then consolidating them in a single console. 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 the who, what, when, where and originating workstation of 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 and Azure AD changes, including those made to Group Policy Objects (GPOs), your Domain Name System (DNS), server configurations, nested groups and much



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.

BENEFITS:

- Installs in minutes with fast event collection for immediate analysis into Windows environments
- Enables enterprise-wide, on-premises and cloud auditing and compliance from a single client
- Proactively detects threats based on user behavior patterns
- 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 in seconds with real-time alerts to any device for immediate response, in or out of the office
- 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, including GDPR, SOX, PCI DSS, HIPAA, FISMA, SAS 70 and more
- 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.

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 across your AD and Azure AD environments. 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.

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.

PROACTIVE THREAT DETECTION WITH CHANGE AUDITOR THREAT DETECTION

Simplify user threat detection by analyzing anomalous activity to rank the highest risk users in your organization, identify potential threats and reduce the noise from false positive alerts.

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, Micro Focus ArcSight or IBM QRadar. Additionally, Change Auditor integrates with Quest® InTrust® for long-term 20:1 compressed event storage and aggregation of native or third-party logs to reduce storage costs on SIEM forwarding and create a highly compressed log repository.

AUTOMATE REPORTING FOR CORPORATE AND GOVERNMENT REGULATIONS

Get clean, meaningful security and compliance reports on the fly using Microsoft SQL Server Reporting Services. With a built-in compliance library as well as customizable reports, proving compliance with government standards, like GDPR, SOX, HIPAA, PCI DSS, FISMA and SAS 70, is a breeze.

ABOUT MERGER IT

Merger IT helps customers with solutions to assisting their organisations, providing the innovation of products which will enhance M&A activities delivery, and provide outcomes, through tried and tested toolsets and processes.

This ensures customers' requirements and outcomes are expedited leveraging the experience provided by Merger IT.

merger IT

Phone: +44 (0)1480 877 188
Email: mergers@mergerit.net
Web: mergerIT.net

Quest