



Quest® ChangeAuditor for Active Directory

Real-Time Auditing for Active Directory

The Challenge

Microsoft Active Directory is at the heart of your mission-critical network infrastructure. Don't leave Active Directory management, support and administration to chance. Issues with your directory can result in unplanned and costly service disruptions and business-crippling network downtime, as well as harmful security breaches and non-compliance with critical government regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI) and the Health Insurance Portability and Accountability Act (HIPAA). Organizations need to be notified—in real-time—of critical changes to Active Directory.

The Solution

Our award-winning ChangeAuditor software drives the security and control of Active Directory by tracking all key Active Directory configuration changes in real-time. From Group Policy Objects (GPO) and Schema changes to critical nested group and operational changes, ChangeAuditor tracks, audits, reports and alerts on the changes that impact your directory—without the overhead of turning on native auditing. With ChangeAuditor for Active Directory, you'll get the "Who, What, When and Where" of change, including details on previous and new change values. You can also add comments explaining why a specific change was made in order to fulfill your audit requirements.

Severity	Time	Source	Destination	Operation	Account	Where	When	Scope
Medium	3/19/2008 6:23 AM	Active Directory	FEDERAL\ldominguez	group changed	FEDDC01	Delete Object	FEDERAL	
Medium	3/19/2008 6:23 AM	Active Directory	FEDERAL\ldominguez	group changed	FEDDC01	Delete Object	FEDERAL	
Medium	3/19/2008 6:23 AM	Active Directory	FEDERAL\ldominguez	Group object removed	FEDDC01	Delete Object	FEDERAL	
Medium	3/19/2008 6:23 AM	Active Directory	FEDERAL\ldominguez	user changed	FEDDC01	Delete Object	FEDERAL	
Medium	3/19/2008 6:23 AM	Active Directory	FEDERAL\ldominguez	User object removed	FEDDC01	Delete Object	FEDERAL	
High	3/18/2008 10:15 PM	Active Directory	FEDERAL\ldominguez	DAEL changed on DU object	FEDDC01	Modify Attribute	FEDERAL	
High	3/18/2008 12:18 PM	Active Directory	FEDERAL\WPAccessManager	DAEL changed on group policy object	FEDDC02	Modify Attribute	FEDERAL	
High	3/18/2008 12:17 PM	Active Directory	FEDERAL\WPAccessManager	DAEL changed on group policy object	FEDDC02	Modify Attribute	FEDERAL	
High	3/18/2008 11:44 AM	Active Directory	FEDERAL\WPAccessManager	DAEL changed on group policy object	FEDDC02	Modify Attribute	FEDERAL	
High	3/18/2008 11:44 AM	Active Directory	FEDERAL\WPAccessManager	DAEL changed on group policy object	FEDDC02	Modify Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	Group object added	FEDDC01	Add Object	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	group changed	FEDDC01	Add Object	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	User Must Change Password At Next Logon option	FEDDC01	Modify Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	User userPrincipalName changed	FEDDC01	Add Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	Last name changed on user object	FEDDC01	Add Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	User account enabled	FEDDC01	Modify Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	First name changed on user object	FEDDC01	Add Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	Display name changed on user object	FEDDC01	Add Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	User object added	FEDDC01	Add Object	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	user changed	FEDDC01	Add Object	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	User Must Change Password At Next Logon option	FEDDC01	Modify Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	User userPrincipalName changed	FEDDC01	Add Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	User Must Change Password At Next Logon option	FEDDC01	Modify Attribute	FEDERAL	
Medium	3/18/2008 9:32 AM	Active Directory	FEDERAL\billton	User account enabled	FEDDC01	Modify Attribute	FEDERAL	

Operation	Type	Account	Permission	Scope
Permission Removed	Allow	FEDERAL\Domain Admins	Read/Write All Properties + Create/Delete All objects + List Contents + List Contents + Delete Ch...	This object only
Permission Added	Deny	Everyone	Write All Properties + Create/Delete All objects + Delete Children + Delete + All Validated Writes	This object and all child object.

With ChangeAuditor for Active Directory, you'll get the "Who, What, When and Where" of change, plus comments on why a specific change was made in order to fulfill your audit requirements.

Audit All Critical Changes

ChangeAuditor provides extensive, customizable auditing and reporting for all critical Active Directory and File System changes, including GPO, Domain Name System (DNS), server configurations and nested

KEY BENEFITS

- Simple installation enables rapid deployment in days versus weeks
- Enables enterprise-wide change management from a single client
- Ensures a secure and compliant networking environment by tracking all critical changes in real-time
- Automates procedures to continually track and report on compliance initiatives
- Strengthens internal controls through real-time insight into both authorized and unauthorized changes
- Drives availability by enabling proactive troubleshooting
- Enables streamlined Windows management through integration with SCOM and other platforms
- Streamlines compliance to corporate and government policies and regulations, including SOX, PCI DSS, HIPAA, FISMA, SAS 70 and more
- Turns information into intelligent, in-depth forensics for auditors and management



KEY FEATURES

- Detailed “Who, What, When, Where and Why,” plus original and current values for all changes
- Audit visibility beyond native logs with coverage for GPO and nested groups
- Comprehensive audit library, including built in alerts, reports and powerful searches based on Microsoft and security best practices and regulations
- Extensive reporting library for compliance, security and operations
- Dispatch instant change alerts, as well as “Smart Alerts” based on event patterns
- Integrates with SQL Reporting Services for subscription based and scheduled report delivery
- Management Pack for Microsoft Systems Center Operations Manager (SCOM) enables you to leverage the power of System Center for more detailed analysis of your Active Directory environment

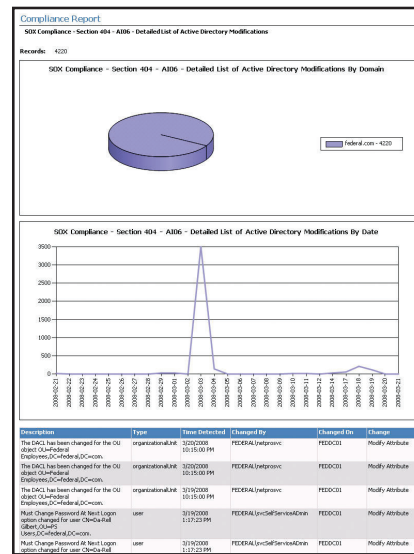
groups. You'll get complete visibility into all changes with in-depth forensics on Who, What, When, Where and Why, plus the original and current values for all changes. And, with real-time alerts, you'll maintain constant awareness of vital policy changes as they occur, reducing the risks associated with day-to-day modifications.

Track User Activity

ChangeAuditor for Active Directory helps tighten enterprise-wide change and control policies by tracking user and administrator activity for account lockouts, failed logins and access to critical registry settings. With 24x7 real-time alerts, in-depth analysis and reporting capabilities, your Active Directory is protected from exposure to suspicious behavior or unauthorized access, and is always in compliance with corporate and government standards.

Turn Irrelevant Data into Meaningful Information to Drive Security and Compliance

ChangeAuditor for Active Directory tracks critical configuration changes to your Windows environment, then translates raw data into meaningful intelligent data to help safeguard the security and compliance of your infrastructure. This comprehensive solution offers real-time alerts, Smart Alert technology for intelligent event correlation and in-depth reports on the activities taking place in your infrastructure.



With a built-in Compliance Library and the ability to build your own reports, proving compliance for standards such as Sarbanes-Oxley (SOX) is a breeze.

Automate Reporting for Corporate and Government Regulations

Utilizing Microsoft's SQL Reporting Services (SRS), ChangeAuditor for Active Directory provides clean, meaningful security and compliance reports on the fly. With a built-in Compliance Library and the ability to build your own reports, proving compliance for standards such as SOX, HIPAA, Payment Card Industry Data Security Standards (PCI DSS), Federal Information Security Management Act (FISMA) and SAS 70 is a breeze.

About Quest Software, Inc.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 90,000 customers worldwide meet higher expectations for enterprise IT. Quest provides customers with client management as well as server and desktop virtualization solutions through its subsidiaries, ScriptLogic and Vizioncore. Quest Software can be found in offices around the globe and at www.quest.com.



2007 GLOBAL ISV PARTNER OF THE YEAR



Quest Software Incorporated. • To learn more about our solutions, contact your local sales representative or visit www.quest.com • Headquarters: 5 Polaris Way, Aliso Viejo, CA 92656, USA

© 2008 Quest Software Incorporated. ALL RIGHTS RESERVED. Quest Software and Change Auditor for Active Directory are trademarks and registered trademarks of Quest Software, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.