



"We chose Quest because this product will give our global systems administrators a proactive way to maintain control over Active Directory. This product will allow us to further promote and apply standard security policies and processes across the company."

—Arun DeSouza
Chief Information Security Officer
Inergy Automotive Systems

- Provides detailed, real-time auditing of all changes to Active Directory and Group Policy Objects
- Provides protection against unwanted changes to the most critical Active Directory objects
- Collects and correlates all unusual user and suspicious administrator activity
- Audits when users and administrators are granted additional permissions in Active Directory
- Provides notification when security best practices and internal policies are violated
- Provides real-time response to the most critical events and changes to Active Directory
- Audits changes out of the box, without any additional application configuration

InTrust®

for Active Directory

Comprehensive Activity Tracking and Change Auditing for Active Directory

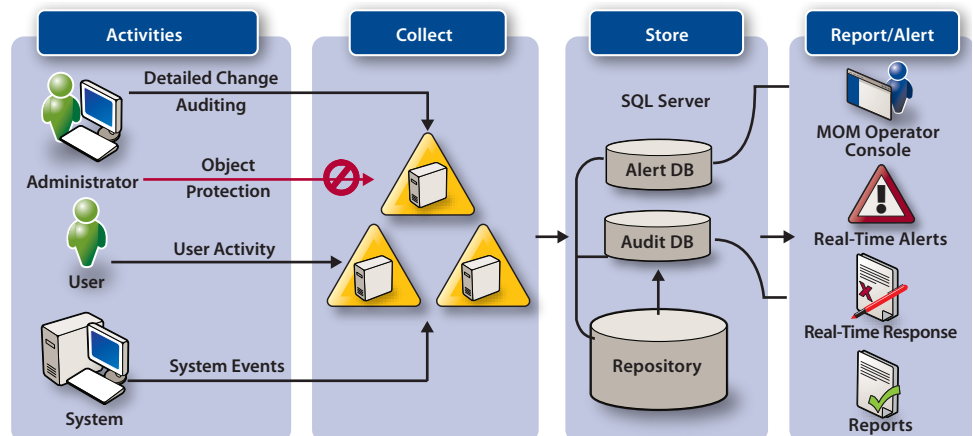
A great deal of important activity takes place on domain controllers. These activities include successful logons to Active Directory (AD), repeated failed logon attempts, the granting of additional privileges to users and modifications to account, domain and audit policies - all of which are logged on a domain controller. However, organizations find it difficult to centrally track this activity because the data is distributed across multiple servers throughout the enterprise. In turn, this affects an organization's ability to ensure compliance with external regulations and internal policies.

The volume of this audit data is difficult to analyze, trend and correlate, and makes it challenging to quickly react to security policy violations. In addition, administrators must be attentive to changes to critical objects in AD (i.e. AD configuration and Group Policy Object (GPO) settings) in order to quickly correct unwanted changes and avoid lost productivity or system downtime. Without an awareness of the necessary details behind these changes, organizations cannot efficiently detect and react to unwanted change.

InTrust® for Active Directory allows organizations to audit, report and alert on all domain controller activity, as well as track all detailed changes to AD and Group Policy. By providing efficient collection and storage of audit data, InTrust for Active Directory enables organizations to effectively react to, and even prevent, policy violations and unwanted changes to critical objects.

InTrust for Active Directory enables you to:

- Capture all Active Directory and Group Policy changes by providing detailed, real-time tracking of all changes to AD and GPOs, including changes to AD configuration and GPO settings.
- Track all activity in Active Directory, such as user logons and granted permissions, and ensure continued adherence to external compliance regulations, such as the Sarbanes-Oxley Act of 2002, as well as internal policies.
- Prevent unwanted changes to the most critical AD objects, such as the accidental deletion of organizational units (OUs) and modification of GPO settings.
- Receive real-time notification and respond to the most critical events and changes to AD. InTrust for Active Directory also takes immediate, automatic action in response to certain events, such as disabling the offending user or reversing the change.



System Requirements:

Operating Systems:

- Microsoft Windows 2000 Server SP4 or Advanced Server
- Microsoft Windows Server 2003 with or without SP1
- Server must be a domain controller

Platform

- 233 MHz Intel Pentium-compatible CPU

Memory

- 128 MB of RAM

Hard Disk Space

- 20 MB plus sufficient space to backup all Group Policy template files

Audit Detailed Active Directory Changes: InTrust for Active Directory provides comprehensive, detailed, real-time auditing of all changes to AD and GPOs, including changes to AD configuration, mailbox permissions and GPO settings. InTrust for Active Directory provides all information behind important changes, including who made the change, where the change was made and the before and after values. This provides operational value by allowing an administrator to troubleshoot AD problems and reverse any changes if necessary. It also adds security and compliance value by allowing organizations to track changes to AD security and policy and by showing how the changes have strayed from the approved configuration.

Protect Active Directory Objects: In addition to tracking all changes to AD and GPOs, InTrust for Active Directory provides protection against changes to the most critical AD objects, such as the accidental deletion of organizational units (OUs) and modification of GPO settings. InTrust for Active Directory can immediately notify you of unwanted changes via e-mail or SNMP, take automatic action against undesired changes and even prevent those changes to the most vulnerable objects.

Audit Unusual User Activity: InTrust for Active Directory collects and correlates all unusual user and suspicious administrator activity. For example, InTrust for Active Directory reports on logon anomalies, such as multiple failed logons and user logon after regular hours, as well as unauthorized usage of built-in administrator accounts.

Audit Active Directory Security Changes: InTrust for Active Directory audits when users and administrators are granted additional permissions in AD, either through addition to security groups, assignment of user rights or delegated rights to AD. InTrust for Active Directory also tracks policy changes, such as modified account, domain, Kerberos and IPSec policies.

Real-Time Response: InTrust for Active Directory provides real-time response to the most critical events and changes to AD. Administrators can be notified immediately by e-mail when possible violations and changes to critical objects occur. In addition to providing these notifications, InTrust for Active Directory also takes immediate, automatic action in response to certain events, such as disabling the offending user or reversing the change.

Management Pack for MOM 2005: InTrust for Active Directory enhances the monitoring and diagnostic value of MOM 2005 by providing valuable information about critical changes to AD and GPOs. The InTrust for Active Directory Management Pack for MOM ensures that important configuration changes are raised in the MOM Operator Console, with all the details behind the change including who made the change, and the before and after values. This empowers administrators with a single console with access to both performance and availability alerts as well as critical changes to AD.

Quick Installation and Deployment: InTrust for Active Directory features a Quick Start wizard which reduces the amount of time it takes to get results and further simplifies the user experience. The Configuration wizard guides you through a complete deployment of your activity tracking and change auditing solution, including site creations, associated policies and tasks, and real-time rules.

About Quest Software, Inc.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at www.quest.com.



www.quest.com/microsoft
e-mail: info@quest.com
Please refer to our Web site for international office information.



©2006 Quest Software, Inc. All rights reserved. Quest and inTrust for Active Directory are registered trademarks of Quest Software. All other brand or product names are trademarks or registered trademarks of their respective companies.