

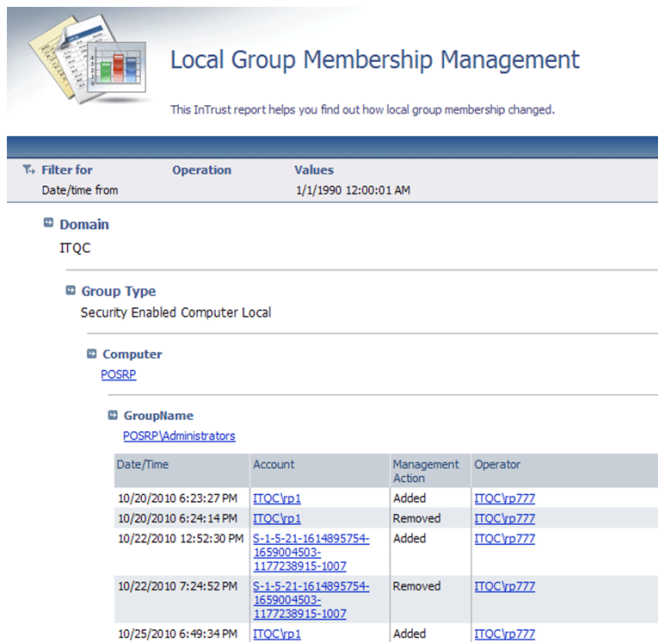
# InTrust for Workstations

## Endpoint Auditing and Monitoring for the Secure Enterprise

Knowing what your users do across the IT environment is critical to meeting compliance regulations and keeping your enterprise network secure. Traditionally this task meant establishing thorough auditing of user access to critical IT resources on all the various infrastructure servers – domain controllers, file and Exchange servers, SharePoint farms and so on. However, this approach incurs a high risk of security issues, from data leakage and spreading of viruses to unauthorized resource access – ruining all your efforts towards achieving compliance.

InTrust for Workstations from Quest Software can help. This endpoint auditing and monitoring solution extends market-proven InTrust technology to Windows workstations, helping you achieve compliance and improve the security posture of your entire enterprise network.

For example, InTrust for Workstations can show all changes to your local administrative groups:



**Local Group Membership Management**  
This InTrust report helps you find out how local group membership changed.

Filter for	Operation	Values	
Date/time from		1/1/1990 12:00:01 AM	
<b>Domain</b>			
ITQC			
<b>Group Type</b>			
Security Enabled Computer Local			
<b>Computer</b>			
POSRP			
<b>GroupName</b>			
POSRP\Administrators			
Date/Time	Account	Management Action	Operator
10/20/2010 6:23:27 PM	ITQC\vp1	Added	ITQC\vp777
10/20/2010 6:24:14 PM	ITQC\vp1	Removed	ITQC\vp777
10/22/2010 12:52:30 PM	S-1-5-21-161-4895754-1659004503-1177238915-1007	Added	ITQC\vp777
10/22/2010 7:24:52 PM	S-1-5-21-161-4895754-1659004503-1177238915-1007	Removed	ITQC\vp777
10/25/2010 6:49:34 PM	ITQC\vp1	Added	ITQC\vp777

*InTrust for Workstations tracks changes to local administrative groups and alerts you in real time when users attempt to elevate their own privileges.*

## Features

**Control of Local Administrator Privileges** – Track local group membership changes so you can control users with administrator access to workstations. Should any user attempt to elevate his or her own privileges in violation of access control policies defined in Active Directory, InTrust for Workstations will notify you in real time.

**User Activity Tracking** – Keep tabs on what end user activities are taking place on user workstations. Keep up to date on activities like logins and logoffs, workstation locks and unlocks, account lockouts, installation and removal of software, access to system registry and others. InTrust for Workstations comes with a set of pre-defined reports that can be automatically delivered to your inbox for periodic review of such activities.

**Monitoring of Removable Media** – Monitor use of removable media, including USB drives and CD/DVD drives, enabling you to detect and, in many cases, prevent loss of confidential data, as well as limit the risk of intentional or accidental attacks from insiders.

## BENEFITS

- **Achieve compliance** by monitoring user activity and detecting inappropriate or suspicious events on user workstations. InTrust for Workstations complements your compliance efforts by collecting, reporting and alerting on events that exist only on user workstations.
- **Improve system security** by identifying user accounts that are being used in violation of corporate policy and proactively alerting you in real time. The solution can even take immediate, automatic action in response to certain events, such as disabling the offending user or reversing the change.
- **Reduce costs** by automating the collection and compression of event data across thousands of user workstations.



**Removable media attached and detached**  
This InTrust report shows removable media attaches and detaches during selected time period. This report runs on InTrust Alerts database.

Filter for	Operation	Values
Date/Time from:	>=	1/1/1990 12:00:01 AM

Desktop POSRP

Date Wednesday, July 27, 2011

Date\Time	Action	Description
7/27/2011 7:30:14 PM	Copy of Removable medium inserted	Removable medium was inserted into logical drive E:. The device type is: "CD-ROM Disc". The medium has 0 free bytes of total 314150912 and is formatted as CDFS.
7/27/2011 7:31:10 PM	Copy of Removable medium ejected	Removable medium was ejected from logical drive E:. The device type was: "CD-ROM Disc". The media had 0 free bytes of total 314150912 and was formatted as CDFS.

Date Thursday, August 04, 2011

Date\Time	Action	Description
8/4/2011 5:44:33 PM	Removable device attached	Removable device was attached as logical volume "H:". The device type is: "Removable Disk". The drive has 1191936 free bytes of total 14684160 and is formatted as FAT.
8/4/2011 5:45:06 PM	Removable device detached	Removable device (logical volume "H:") was detached from the computer. The device type was: "Removable Disk". The drive had 1191936 free bytes of total 14684160 and was formatted as FAT.

Page 1  Date: 11/3/2011

InTrust for User Workstations tracks the use of removable media by end users

**Log Integrity** – Create a cached location on each workstation where logs are duplicated as they are created, preventing a rogue user or administrator from tampering with the audit log evidence. If the user’s laptop is disconnected from the enterprise network, the logs will be preserved in a secure location until the laptop comes back online.

**Centralized Archive** – Effectively deal with myriads of workstations across the entire enterprise. The solutions’ negligible agent footprint, high-performance event aggregators and efficient repository make it possible to store all workstation logs in a centralized archive for years to come.

**Forensic Analysis** – Get a complete, consolidated view of user activity across the enterprise: from users logging to their workstations, to resource access on the servers, to termination of the workstation sessions. You can pull out the entire trail of activity for any given user and any point in time by querying the indexed repository data in InTrust Repository Viewer.

**Flexible, Preconfigured Reports** – Easily create and distribute the information needed for your organization’s internal and external auditing efforts. InTrust for Workstations offers both predefined and custom reports that you can save in a variety of formats, ensuring that you can deliver precisely the information requestors need, in the format they require.

**Alerting on Abnormal User Activity** – Receive alerts in real time about unusual user, administrator and system activity, such as attempts to modify critical system files and multiple failed logon attempts followed by a successful logon. All alerts can be sent directly to you by email or integrated into the workflow of third-party monitoring applications.

**SYSTEM REQUIREMENTS**

**Supported Operating Systems**

- Microsoft Windows XP Professional (32-bit and x64 architectures)
- Microsoft Windows Vista (32-bit and x64 architectures)
- Microsoft Windows 7
- Microsoft Windows Embedded POSReady 2009

**Additional Software and Services**

- For data gathering without agents: Remote Registry Service
- For executing response action scripts:
  - Microsoft Windows Script Host 5.6 or later
  - ADSI 2.5 or later
- For valid descriptions in Windows Embedded POSReady events gathered with InTrust agents and real-time monitoring alerts: the Utilities Windows component.

**ABOUT QUEST SOFTWARE, INC.**

Quest Software (Nasdaq: QSFT) simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest solutions for **administration and automation, data protection, development and optimization, identity and access management, migration and consolidation,** and **performance monitoring,** go to [www.quest.com](http://www.quest.com).



5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB [www.quest.com](http://www.quest.com) | EMAIL [sales@quest.com](mailto:sales@quest.com)  
If you are located outside North America, you can find local office information on our Web site.

© 2012 Quest Software, Inc.  
ALL RIGHTS RESERVED.

Quest, Quest Software, the Quest Software logo, and InTrust are 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. DSW-InTrust4Workstations-US-SW-12282011