

Quest InTrust Microsoft Windows Knowledge Pack

Benefits

- Saves time and improves efficiency by automating the collection of Windows-based .evf logs
- Ensures information security by collecting, storing, and reporting on local file and object access
- Enables organizations to address regulatory compliance requirements by reporting on access to information

Understanding user activity at every level and in every application is imperative to the security of all organizations. Whether supporting an internal security requirement or external regulatory compliance initiative, collecting, storing and reporting on this data must be a priority for any IT organization.

Most organizations have enabled auditing at the local file level, but soon realize that it is difficult to manage, and oftentimes end up turning it off. Large quantities of event log data can be costly to store. To see a return on investment, companies need a scalable solution with cost-effective long term storage.

Further, application and system logs have become increasingly important as Microsoft has increased the information held within them. However, these logs can be modified or deleted by users with sufficient enough rights, leading to theft, fraud and a failure to meet compliance requirements. Non-compliance can result from failure to collect all logs and the inability to assure the integrity of the logs collected.

The challenge is set: In order to meet external compliance objectives and internal security mandates, a company must audit and report on file access and permission changes, while securing and cost-effectively storing the event data in order to ensure its integrity.

The Quest InTrust® Windows Knowledge Pack can help. It automates the process of collecting, storing and reporting on Windows

events, helping to further strengthen a company's information security and address compliance requirements. Through agent-side caching, InTrust assures that the logs are in their native state and that no logs have been lost due to deletion or roll-over.

Having all this information available, and ensuring the integrity of the data, means an executive is now able to determine what user permissions have changed and which users are accessing business critical files and objects. For instance, if a change turns out to be invalid, permissions can be reversed. If the change was made by unauthorized personnel, their rights can be revoked and appropriate action taken against that employee.

Reports can be generated on a daily, weekly or quarterly basis depending on a company's needs. The figure below represents a detailed view of certain actions that a user took against business critical files.

Quest Reporting Console

User			
BGV2003VMWAdministrator			
Date/Time	Computer	File or Folder	Action
14.05.2005 18:35:30	BGV2003/VMW	C:\tsf\New Text Document.txt	Modify file
14.05.2005 18:37:15	BGV2003/VMW	C:\tsf\New Text Document.txt	Modify file
14.05.2005 18:37:18	BGV2003/VMW	C:\tsf\New Text Document.txt	Modify file
14.05.2005 18:38:00	BGV2003/VMW	C:\tsf\New Text Document.txt	Modify permissions
14.05.2005 18:47:16	BGV2003/VMW	C:\tsf\New Text Document.txt	Modify file
14.05.2005 18:53:33	BGV2003/VMW	C:\tsf\New Text Document.txt	Modify file
14.05.2005 18:58:42	BGV2003/VMW	C:\tsf\New Folder	Delete file/folder
14.05.2005 19:01:55	BGV2003/VMW	C:\tsf\SI_Trace.log	Delete file/folder
14.05.2005 19:02:06	BGV2003/VMW	C:\tsf\SI_Trace.log	Delete file/folder
14.05.2005 19:10:48	BGV2003/VMW	C:\tsf\I1New Text Document.txt	Delete file/folder
14.05.2005 19:10:48	BGV2003/VMW	C:\tsf\I1New Text Document.txt	Modify file

Figure 1: Windows Knowledge Pack Report Sample

Having this functionality means that companies can provide auditors and investigators with a complete view into file/object access, local logons, as well as application and system logging.

For more information on how InTrust can help your organization address internal security mandates and external compliance requirements, regardless of your environment, visit <http://wm.quest.com/products/intrust/>.