

# Quest InTrust Microsoft Internet Security and Acceleration Server Knowledge Pack

## Benefits

- Saves time and improves efficiency by automating the collection of Windows based Microsoft Internet Security and Acceleration Server (ISAS) logs
- Provides valuable information about ISAS environments, ensuring the security and use of servers in accordance with company policy
- Correlates ISAS information with internal user activity

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.

However, sometimes addressing these mandates means understanding client activity as well. That's where ISAS comes in. Most organizations have scanned through their ISAS .txt log information, but have struggled to understand or trend it. The amount of data generated by users and clients can quickly become overwhelming and costly due to storage requirements. Companies must implement a scalable solution with cost effective long term storage.

Not understanding this critical information can lead to an unsecured infrastructure and its assets. The ability to understand and use this information can also help lead to discovering misuse by internal employees. Corporations must be able to monitor the activity on their ISA servers, their internal users' activity in relation to their Web use and the built-in intrusion detection functionality within an ISA server.

The challenge is set: In order to secure the network and provide a better ISAS environment, a company must audit, collect and report on ISAS log information such as:

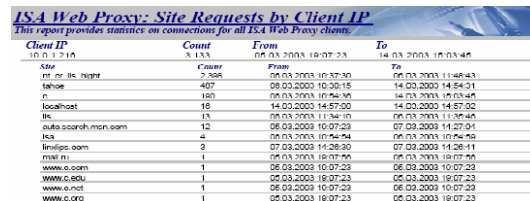
- Incoming and outgoing attacks

- Prohibited user activity
- All firewall and proxy connections
- Server management

The new Quest InTrust<sup>®</sup> Microsoft Internet Security and Acceleration Server Knowledge Pack can help. It automates the process of collecting, storing and reporting on ISA server events, helping to further strengthen a company's information security. InTrust assures the logs are in their native state, which means that you can be assured of their unimpeachability.

Having all this information available, and ensuring the integrity of the data, means an administrator and the organization are now able to determine how their ISAS environment is being used and how users and clients are behaving. Organizations can act in a proactive manner to make changes to security and configurations of their ISAS environment.

Reports can be generated on a daily, weekly or quarterly basis depending on a company's needs. The figure below represents a report on site requests by client IP.



**ISA Web Proxy Site Requests by Client IP**  
This report provides statistics on connections for all ISA Web Proxy clients.

Client IP	Count	From	To
(IP:PORT)	A:133	06.03.2003 18:07:23	14.03.2003 18:03:46
Actix	2	06.03.2003 18:07:30	06.03.2003 11:48:43
atc.nc.ibm.net	407	06.03.2003 18:00:15	14.03.2003 14:54:31
atc	163	06.03.2003 18:04:35	14.03.2003 18:03:45
localhost	18	14.03.2003 14:57:00	14.03.2003 14:57:02
its	13	06.03.2003 11:34:10	06.03.2003 11:38:45
quds.solaris.msn.com	12	06.03.2003 18:07:23	07.03.2003 14:27:31
ica	4	06.03.2003 18:04:54	06.03.2003 18:04:56
linifips.oam	3	07.03.2003 14:28:30	07.03.2003 14:28:11
msn.com	1	06.03.2003 18:07:05	06.03.2003 18:07:05
www.c.com	1	06.03.2003 18:07:23	06.03.2003 18:07:23
WWW.C.EDU	1	06.03.2003 18:07:23	06.03.2003 18:07:23
www.c.net	1	06.03.2003 18:07:23	06.03.2003 18:07:23
www.c.org	1	06.03.2003 18:07:23	06.03.2003 18:07:23

Figure 1: ISAS Knowledge Pack Report Sample

Having this functionality means that companies can provide a complete view into the ISAS infrastructure, thus providing a more secure network.

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/>.