

**Access Accountability: QMessage Monitor V7 Highlights Real-Time Security Breaches with New Database Monitoring Capability**

**December, 6<sup>th</sup> 2011 – QMessage Monitor (QMM)**, the real-time message monitoring and escalation solution for IBM i environments, now offers a new database monitoring feature to identify real-time access issues on the system. Available now within the latest V7 release of QMM and developed by IBM i systems management experts CCSS, database monitoring will provide the system generated 'proof positive' accountability Auditors and IT Managers require to take action against malevolent system intruders.

QMM users already have the ability to monitor the Audit Journal for real-time security breaches but the new database monitoring capability gives them a more detailed level of insight. Now audit-friendly proof can be obtained showing not only who is accessing the system, but from where and crucially, what that person is doing with the files that have been accessed. Keeping database server activity under real-time scrutiny, IT Managers can be alerted to potential security violations relating to files on libraries that contain sensitive data. The new monitor will issue a real-time message for escalation at each instance of a sensitive file being opened (read, written, deleted or updated); instances of SQL access performed through the database server (DBS) and finally, instances of native access (such as creating, deleting and retrieving information).

"IT Managers and Auditors will appreciate the precision the new database monitor offers," says Paul Ratchford, Product Manager for CCSS, "there's tremendous value in being able to pin-point the exact files, libraries, users and IP addresses they are interested in – it's a very inclusive approach to monitoring and those environments that have visibility of these issues can better protect the types of sensitive files that are sometimes targeted causing great disruption – be it those containing payroll information or personal employee details. Suspicious activity has no place to hide on the system."

Database monitoring works by the user optionally setting up 'client lists' which specify either a single, or a range of IP addresses. A client list may relate to a particular group or certain individual within the IT department (for example, IP addresses in a defined range can be identified for a regional support team or helpdesk.) Database monitoring rules can then be applied. These rules determine the types of access behaviors that will be logged. In addition to the actions associated with a file being opened as mentioned already, a manager may choose to log any or all of the following actions: creation, deletion, overriding or retrieval of file information; the reading, adding, updating or deleting of records; the adding, clearing or

removal of file members and finally, when a library list is set. These rules can be applied to either specified or all users, files, libraries, library owners, programs or program libraries on the system. Database server parameters can be set using a command that allows the user to pause/restart database monitoring, either locally, if on a remote system, or for a remote system if running from the central system.

With database monitoring in place, any breach of the defined rules that occurs will be identified in real-time and escalated for immediate attention of the IT Manager or other authorized person. For example, if an unauthorized user were to select all the records in a payroll file, the alert message details include the user, action, file details and job details for an instant summary of the breach. Help text provides further details on the parameters and rules associated with the user and their client list including the top 3 programs in the call stack, and the SQL command actually run when SQL access is being used. This instant view not only provides confirmation of the breach but also saves investigation time in identifying vulnerable access points and the methods used to exploit those vulnerabilities.

For more information about QMessage Monitor please visit:

<http://www.ccssltd.com/products/qmessage-monitor/>

Note to Editors: Screenshot image of QMM v7 Database Monitoring is available for use with this release. Please download here: [http://www.ccssltd.com/images/Dbase\\_Example.jpg](http://www.ccssltd.com/images/Dbase_Example.jpg)

## **ENDS**

### **About CCSS**

CCSS develops, supports and markets IBM i (on Power Systems & System i servers) performance monitoring and reporting, message management and remote management solutions. An Advanced IBM Business Partner, CCSS develops powerful solutions to support some of the world's most demanding IBM i environments across many industries including insurance, banking, pharmaceutical and manufacturing. Existing customers that rely on CCSS's feature-rich solutions include leading organizations such as Volvo, Mattel, Newell-Rubbermaid, The Royal Bank of Scotland, and Siemens Healthcare.

CCSS is headquartered in Gillingham, Kent, UK with key regional headquarters in Raleigh, North Carolina, USA and Bonn, Germany together with a global agent network spanning Austria, Portugal, the Netherlands, Switzerland, Sweden and Africa.

**[www.ccssltd.com](http://www.ccssltd.com)**

IBM, Power Systems, System i, are trademarks of the International Business Machines Corporation in the United States and/or other countries.