

PRESS RELEASE

June 2004
For Immediate Release

QMessage Monitor V6 Offers Major New Real-Time Security Capabilities For iSeries Shops

Gillingham, Kent, UK, June 2004 – iSeries systems management software developer CCSS strikes fresh ground with the July release of QMessage Monitor Version 6 and its range of newly developed security focussed features that, in the age of numerous security threats, address the requirement for more stringent audit compliance.

The latest version now has the ability to monitor the audit journal (QAUDJRN) where **CRITICAL** messages and messages of security failures are sent. Additional filters can be set up to limit the number of audit journal entries converted into messages. Similarly, another **NEW** feature now ensures all QHST log entries are monitored in the same way, providing total monitoring coverage of important messages from the main system queues, securing your business data.

A distinct group of new features that target specific security breaches or threats to security protocols have also been introduced within QMessage Monitor giving users a staggering 426 new possibilities for auditing. These functions are especially useful for companies working to strict internal auditing standards or those set out by legal requirements such as the Sarbanes-Oxley Act. The security feature set includes monitoring for authority failures that may otherwise go undetected, due to MONMSG statements in CL programs, and can often be the cause of programs on the system not functioning correctly or even falling over. The FTP access feature ensures that any user attempting to access the

iSeries via FTP will be immediately identified in real-time and details of the attempt recorded in the audit journal. From here, all suspicious attempts can be validated to confirm if the access is legitimate or not. As with all messages, critical threats such as these can now be escalated to an appropriate contact, or group of contacts, according to severity, staff availability and preferred communication device to ensure that no intrusion attempt remains undetected by system and/or security managers.

Changes to critical system values will also be detected and for each change, will include details of the user responsible, the original value and the new changed value. User profile changes will also be identified; by clicking on the message details, managers can view details of the user instigating the change together with the original and new status. Two additional features are dedicated to objects that adopt QSECOFR authority. The first highlights in real-time, programs that are using this level of authority and will detect, for example, a program that adopts this level when it starts. The second highlights objects being restored to the system with QSECOFR authority.

All users entering an invalid password will also be acknowledged as will users without the proper authorisation who attempt to use service tools. A historical log of activities such as these can help security and system managers to build an accurate picture of the methods and trends adopted by individuals to access system data and will also help distinguish and resolve other instances where user errors and mistakes have occurred. Similarly, users who delete spool files or users who delete objects, either accidentally or deliberately, will also be identified in real-time. Features like this will prevent instances of critical reports that were scheduled to run, mysteriously 'disappearing' and will enforce a high degree of accountability and best practice procedures.

Finally, a new feature that detects when jobs have been submitted and started will keep a watchful eye on scheduling products and their activities. Previously, users would only be alerted to events that did not occur. Now no time is wasted in waiting for expected scheduled tasks to complete. For example, a critical scheduled job such as payroll or purchase ledger updates that may take several hours to complete can be monitored to ensure that managers have real-time confirmation of their submission and start times and dates, reducing the time it takes to resolve any problematic or unusual circumstances surrounding critical jobs that may need restarting.

The new security and history monitoring capabilities in this latest Version 6 of QMessage Monitor are only part of the new features and enhancements on offer. Additional changes to the activity log, escalation procedures and PC console interface will be announced separately.

QMessage Monitor is an award winning message management solution favoured by banks, pharmaceutical, manufacturing and facilities management companies across the world. The CCSS systems management suite includes QMessage Monitor, QSystem Monitor, a performance monitoring and reporting solution and QRemote Control, a remote systems management solution.

For more information about this press release please contact Greer Hahn: news@ccssltd.com

CCSS (Europe) Ltd 6 The Courtyard Gillingham Business Park Gillingham Kent ME8 0NZ England.
Tel: +44 (0) 1634 370 444 Fax: +44 (0) 1634 370 555
Email: info@ccssltd.com Web site: www.ccssltd.com

CCSS (USA) Corporation 3737 Glenwood Avenue Suite 100 Raleigh NC 27612 USA
Tel: +1 919.573.6126 Fax: +1 919.573.6026
Email: us.sales@ccssltd.com Web site: www.ccssltd.com

CCSS Deutschland GmbH Hinter Hoben 149 53129 Bonn Germany.
Tel: +49 (0)228 9168-207/-417 Fax: +49 (0) 228 9168-102
Email: Info@CCSSEurope.de Website: www.ccssltd.com