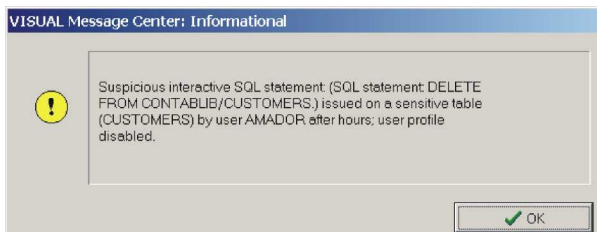


iSeries SQL Monitor

The VISUAL Message Center Interactive SQL Monitor and SQL Monitor Agents reinforce the protection of the critical data stored in your iSeries systems by auditing all SQL statements executed by users and programs.

Automate Auditing of SQL usage and Ensure Integrity of Data

The Tango/04 SQL Monitors enable system supervisors, database administrators, auditors and security officers to capture key data about every single SQL statement run against the database engine. If preferred, dynamic rules can be set to highlight only the most suspicious events. In conjunction with the VISUAL Message Center SmartConsole, they can execute unattended actions for maximum security.



Regulatory compliance... the smart way

- Sarbanes-Oxley Act
- California Security Breach Act
- U.S. Patriot Act
- HIPAA
- 21 CFR Part 11
- Basel II
- And others

Interactive SQL Monitor Features

- Record every single SQL statement executed through STRSQL.
- Automatically execute self-protecting actions: Hold a job, disable a user profile, remove authorization to tables, etc.
- Be alerted in real time of STRSQL statements being executed.
- Use advanced escalation rules to ensure notification of suspicious activity.
- Color-code suspicious activity.
- Filter out non-critical SQL statements by user, table name, date, time, calendar, system, job, subsystem, SQL completion code, etc.
- Schedule automated actions based on any event data, calendar, system, etc.
- Easily navigate audit trails by using the SmartConsole dynamic Event List, Business Views and Event Navigator.
- Create web-based reports of SQL activity to demonstrate regulatory and policy compliance.
- Export audit data into Excel and many other formats.
- Monitor SQL activity without journal files, triggers or application changes.
- Use real time dynamic subscriptions to grant or deny access to the data retrieved by the agent.

SQL Monitor Features

The iSeries SQL Monitor Agent extends the capabilities of the Interactive SQL Monitor to any kind of SQL statement. Major features, additional to those of the Interactive SQL Monitor, include:

- Obtain a comprehensive auditing coverage of any SQL statement, including Client/Server programs, ODBC applications, Java JDBC-based programs, and any kind of remote SQL statement.
- Capture internal SQL accesses in batch or interactive programs, or embedded SQL on RPG, COBOL, or any other language.
- Use time elapsed data to fine-tune Client/Server or Web applications.
- Identify CPU-abusive SQL statements to improve the quality of your software.
- Mask constant values on WHERE, SET and other clauses to preserve data confidentiality.
- Filter or execute actions based on the remote IP address.
- Filter out non-critical SQL statements job name, job user, real user, job type, group profile, user class, and/or accounting code).
- And more.

distributed by

iSeries SQL Monitor is part of VISUAL Message Center, a Tango/04 solution that enables companies to manage and control systems and applications, optimizing performance and reducing operating costs.

For more information about VISUAL Message Center and other Tango/04 iSeries solutions, visit www.tango04.com



Solutions for Advancing People

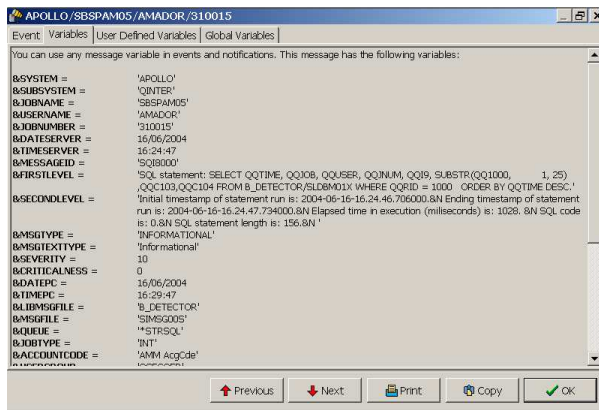
Demonstrate policy and regulation compliance

Use the Reporting System to generate reports that demonstrate compliance with company policies or legal requirements. SQL activity and suspicious actions can be sent to a corporate dashboard, be assigned a color-coded severity and status, or used to support Business Service Management (BSM) initiatives. Customizable Audit Reports can be obtained in a variety of formats, either on demand or automatically.



Optimize your applications

The SQL Monitors can measure database response time and help you understand, profile, and optimize your applications, either native, Client/Server or Web-based.



Two Agents. A Single Mission.

While the Interactive SQL Monitor Agent covers only the SQL statements entered by using the STRSQL (Start Interactive SQL) command, the SQL Monitor Agent may capture all the SQL statements regardless of their source, including: SQL transactions coming from embedded SQL statements on RPG and COBOL programs, ODBC/JDBC clients, Client/Server applications, and any kind of program using SQL statements to access the native database. Both monitors have been designed to address the security concerns of companies using structured queries to run their corporate applications. Both can be run simultaneously.

Benefits of the iSeries SQL Monitors

The iSeries SQL Monitor agents can contribute enormously to the safety, integrity, confidentiality and availability of your sensitive files. By keeping applications working your company will save the enormous cost of downtime.

- **Audit all STRSQL activity and data patches**
STRSQL statements are not recorded by the OS/400 operating system. Use the SQL Monitors to audit changes and accesses done through the STRSQL command.

- **Real Time alerting of suspicious activity and automated actions**
Send events automatically to the VISUAL Message Center SmartConsole to automate actions and get alerted in real time.

- **Flexible Reporting**
Use the Reporting System to generate detailed or summary reports on a variety of formats, including PDF and HTML.

- **Simplify and reduce the cost of operations**
Filter out non-critical events: Ignore statements that do not alter the database, or focus on the SQL statements that access sensitive files. Further save valuable time by automating actions such as event escalation, duplicate suppression, coloring, enrichment, transformation, and formatting.

- **Speed up ad-hoc changes after an application failure**
Since interactive SQL statements can not be audited, some security officers prohibit the usage of SQL to patch production databases. Developers and operators are forced to write ad-hoc RPG or COBOL programs for correcting tables after a failure or bug appears. With the Interactive SQL Monitor, SQL statements are much easier to audit (and require less technical knowledge) than RPG or COBOL programs.

- **Easier audits, no app changes required**
Compared to record-level auditing, SQL statement auditing requires less effort by making it unnecessary to track millions of record changes or implement any resource-consuming journal or trigger mechanism.

- **Comply with regulation and avoid fines**
Audit the date, time, user, real user (which can be different from the job user), and the full SQL statement performed to identify the record (or record set) accessed or modified. American and European privacy laws such as SOX, HIPAA and 21 CFR Part 11 require accesses to sensitive data to be recorded and stored for several years.

- **Prevent and investigate fraud**
By monitoring SQL activity, accesses, changes, deletions and inserts to the production databases and sensitive files can enormously help you preventing and investigating fraud cases.