SQL Compliance Manager

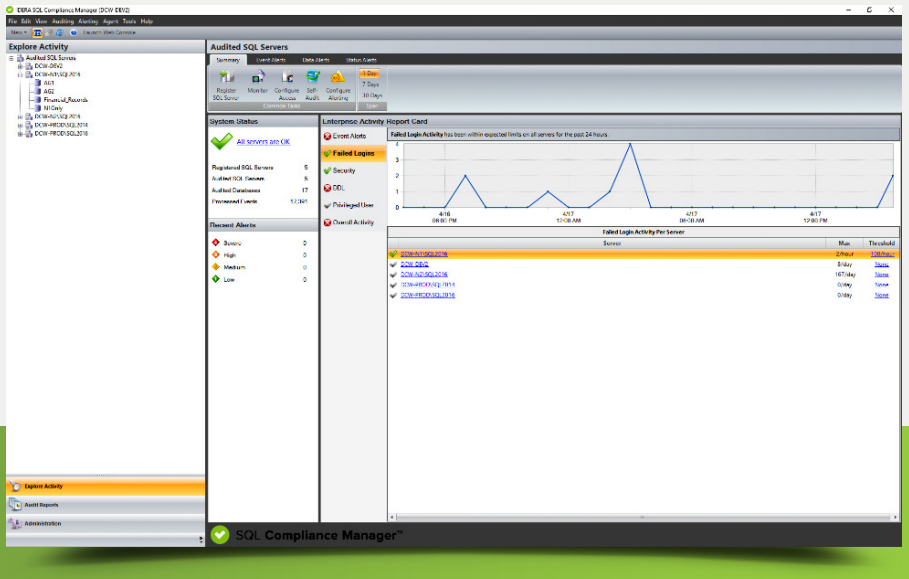
MONITOR, AUDIT, AND ALERT ON SQL SERVER USER ACTIVITY & DATA CHANGES

SQL Compliance Manager is a comprehensive auditing solution that monitors and tracks changes to SQL Server objects and data, and sends alerts on suspicious activity. SQL Compliance Manager gives you detailed visibility to determine who did “what”, “when”, “where”, and “how”, whether the event is initiated by privileged users or hackers. SQL Compliance Manager also helps ensure compliance with industry regulatory and data security requirements. SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring, alerting, and auditing of all data access, selects, updates, schema modifications and permission changes to SQL Server databases.

WHY SQL COMPLIANCE MANAGER?

Data security and regulatory compliance requirements have become increasingly stringent. As a result, DBAs are tasked with the monumental job of providing an accurate audit trail of SQL Server activities such as database access, update actions, schema changes, and security changes. Unfortunately, auditing and reporting this information can often require weeks or months of custom development or in some cases the employment of a full-time DBA staff to provide scheduled or on-demand reports to auditors.

SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring, alerting, and auditing of of all data access, SELECT statements (including column level granularity), DML, schema changes, permissions, and logins to SQL Server databases, giving quick, easy, accurate, and trusted answers to what has transpired on your servers. Furthermore, to ease the research and configuration required to comply with industry regulatory guidelines, SQL Compliance Manager delivers reporting templates with pre-configured audit settings that align with regulatory citations. SQL Compliance Manager provides the best SQL Server auditing, alerting, and reporting solution which ensures all server access and exceptions are tracked to comply with internal and external audits.



Start for FREE!

SQL Compliance Manager tremendously exceeded our expectations providing ease of setup, very granular configuration options, excellent real time activity monitoring and a great variety of reporting options.

PRODUCT HIGHLIGHTS

- **Audit Sensitive Data** Get detailed visibility of who did what, when, where and how
- **Improve Visibility** Web-based dashboard simplifies access from any browser
- **Track and Detect Changes** Monitor and audit all data access, failed logins, and schema and permission changes
- **Uncover Security Threats** Customize alerts and be notified of suspect activity by privileged users or hackers
- **Quickly Satisfy Audits** Demonstrate compliance with built-in multiple industry regulatory templates
- **Easily Generate Reports** Deliver over 25 out-of-the-box reports to validate SQL Server audit trails
- **Minimize Overhead** Reduce impact on audited servers via a lightweight data collection mechanism

KEY BENEFITS

Continuous, Flexible Auditing SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring and auditing of all data access, updates, data structure modifications and changes to security permissions. The type and detail of audit data collected is highly configurable and may be defined at the server, database and object level. No changes to applications or production databases are required.

Immediate Notification of Suspect Activity SQL Compliance Manager can be configured to alert DBAs of suspect server activity, either via e-mail or the event log. The alerting engine includes powerful features such as flexible alert definition, alert templates, custom messaging, and alert reporting, and alerts can be applied across the board, or to specific servers, databases, or tables, for more fine-grained control.

Minimal Performance Impact SQL Compliance Manager employs a very efficient, low-overhead data collection mechanism to minimize impact on audited servers. A lightweight agent monitors the SQL Server extended events files, collects the audit data and sends it back to the repository. SQL Compliance Manager does not use high-overhead approaches that can impact server performance such as profiling, 'heavy' tracing options or log scraping.

Powerful Reporting and Analytics SQL Compliance Manager provides out-of-the-box reports to address a broad range of auditing and security reporting needs and demonstrate compliance to multiple industry regulations. These reports were developed in conjunction with industry experts in security, compliance and auditing policies, such as Ernst and Young and Information Shield Inc. All reports may be easily customized, plus the user-friendly schema of the audit data repository enables rapid development of ad-hoc queries andreports for detailed forensic analysis.

KEY FEATURES

Customizable Regulatory Guideline Templates Easily apply the right auditing settings to your servers and databases for PCI DSS, DISA STIG, NERC, CIS, SOX, HIPAA, and FERPA regulations. Extensive research is no longer required as you can simply define the objects and apply customizations to the included regulatory guideline templates.

Low-Overhead Data Collection A lightweight agent captures data from the SQL Server trace events, extended events, and audit log files and extracts the selected events for auditing. The data collected can be streamed to the repository in real time or in scheduled batches.

Row Count Information Capture and filter on row count information for all event types (both traces and extended events, for SQL Server 2008 and later). Provide a consolidated row count for the event type for joined query statements. Provide alerts based on optional time interval thresholds that are set for row counts, users, sensitive data and specific queries.

Customized Alerting Provides customized alerting for over 200 specific SQL Server event types, allowing you to define rules to receive immediate notification when critical SQL Server events occur. These events are stored in the audit repository, can be emailed directly to a user and/or written to an event log that feeds an in-house operations monitor system (e.g. SCOM).

Before and After Data Capture Audit data changes on any table so you can compare before and after data values resulting from inserts, updates and deletions.

Data-Specific Alerting Define rules to issue alerts based on events, status, or data for sensitive columns or BAD (before/after data) changes.

Tamper-Proof Audit Data Repository Guarantees the integrity of audit data by providing an immutable repository – any attempts at changing or tampering with the audit data can be detected. In addition, powerful self-auditing features capture and alert on all changes to auditing policies and data collection parameters.

IDERA

IDERA.com

877 GO IDERA 464.3372
TWITTER twitter.com/Idera_Software
FACEBOOK facebook.com/IderaSoftware
LINKEDIN linkedin.com/company/idera-software

EMEA +44 1628 684 400
APAC +61 1300 307 211
MEXICO +52 (55) 8421-7980
BRAZIL +55 (11) 3280-1159