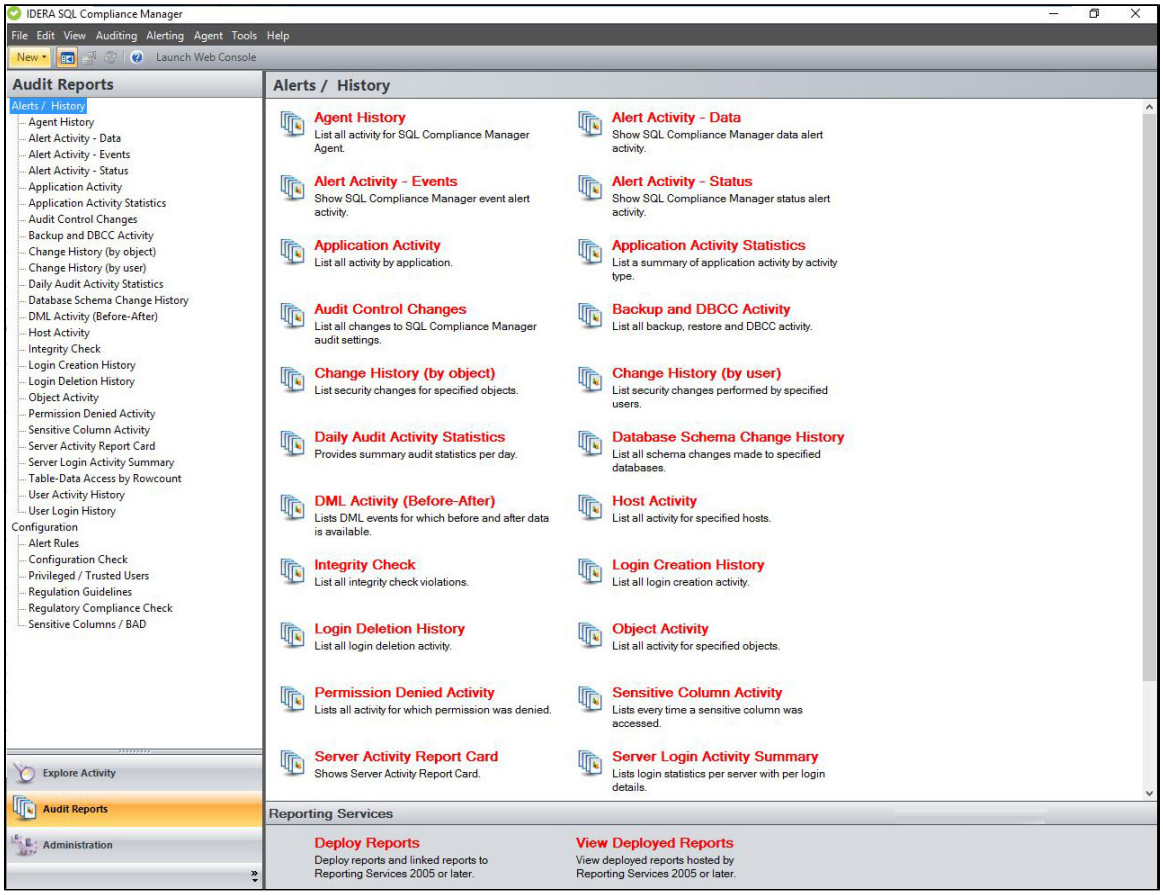
Available reports

The following report categories are included with IDERA SQL Compliance Manager. The activity, change, and history reports list events that passed the SQL Server access check. To audit events that failed the SQL Server access check, generate the Permission Denied Activity report for the appropriate SQL Server instance.



Alerts/History Reports

Audit Reports

The Daily Audit Activity Statistics report lists the amount of activity that occurred on the SQL Server instance or designated database, on an hourly basis, for the dates specified. Use this report to audit overall activity levels on your SQL Server instances and databases.

- Daily Audit Activity Statistics

Alerts Reports

The Alert Activity report lists alert details, such as target object, event, and time of the alert. Use this report to audit alerts triggered over a specified time period.

- Alert Activity - Data
- Alert Activity - Events
- Alert Activity - Status

Application Audit Reports

These reports list activity details, such as login, event, and time of activity, per application and database. Use these reports to audit activity across multiple applications and databases.

- Application Activity
- Application Activity Statistics

Database Object Audit Reports

The Backup and DBCC Activity report lists backup, restore, DBCC, and database object activities on specific databases. Use these reports to audit mass data movement or database object activity, such as SELECT or UPDATE, across multiple databases.

- Backup and DBCC Activity
- Object Activity

DDL Audit Reports

The Database Schema Change History report lists schema changes applied to audited databases. Use these reports to audit data definition language (DDL) statements, such as dropped tables, executed against one or more databases on a SQL Server instance.

- Database Schema Change History

DML Audit Reports

The DML Activity (Before-After) report lists DML events for which before and after data is available. Use this report to audit UPDATE, INSERT, and DELETE activity on critical or sensitive databases.

- DML Activity (Before-After)

Host Audit Reports

The Host Activity report lists all host computers from which specific logins executed an action. Use this report to audit user behavior from multiple client computers, identifying the host computer from which an activity request originated.

- Host Activity

Policy Audit Reports

These reports list changes and updates applied to the SQL Compliance Manager Agent deployed on a specific SQL Server, and any integrity violations in your audit data. Use these reports to diagnose audit data integrity issues and track agent configuration changes as well as agent activities, such as SQL Compliance Manager Agent service restarts.

- Agent History
- Audit Control Changes
- Integrity Check

Row Count Reports

The Row Count reports lists all information about data access. Use this report to audit the frequency in which data is accessed, identifying suspicious behavior.

- Table-Data Access by Rowcount

Security Audit Reports

These reports list permission changes by object type as well as unauthorized attempts to execute activities. Use these reports to audit your SQL Server security settings and identify misconduct.

- Change History (by object)
- Change History (by user)
- Permission Denied Activity
- User Login History

Server Activity Reports

The Server Activity Report Card report allows you to review the activity status and recent audit event history on your SQL Server instance. Use this report to display a particular server´s activity status.

- Server Activity Report Card

SELECT Audit Reports

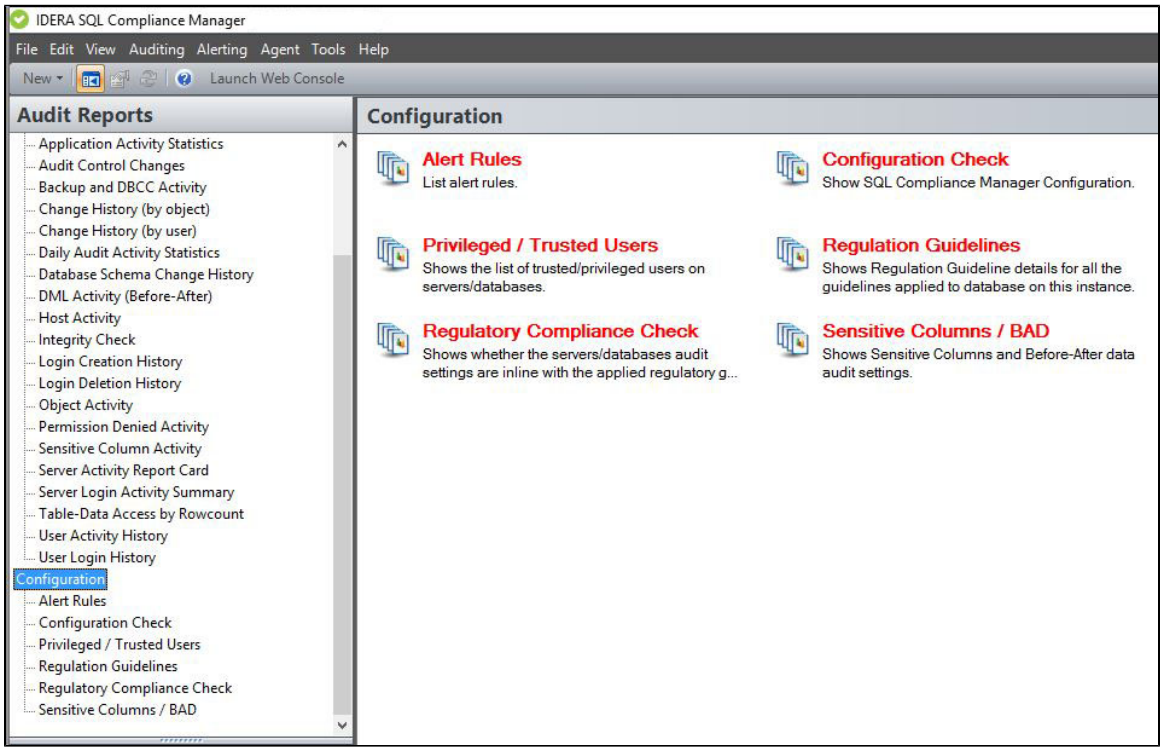
The Sensitive Column report lists all SELECT events that were initiated by applications to read specific columns that contain sensitive data. This report also includes the T-SQL statements that executed the corresponding commands. Use this report to audit columns that require high security, such as employee Social Security numbers (SSNs).

- Sensitive Column Activity

User Audit Reports

These reports list user activities performed on a specific SQL Server instance, and provide a history of login creations and deletions. Use these reports to audit user behavior and login management.

- Login Creation History
- Login Deletion History
- Server Login Activity Summary
- User Activity History



Configuration Reports

Alert Rules

The Alert Rules report lists the existing alert rules for your servers and databases. Use these reports to diagnose audit data integrity issues.

- Alert Rules

Configuration Check Reports

The configuration check report lists all the configurations selected on a Server or Database. Use these reports to reconcile the differences in regards to the configurations across different servers and databases.

- Configuration Check Report

Privileged/Trusted User Reports

The Privileged/Trusted Users report lists all trusted and privileged users set in each server instance and database. Use this report to monitor which Trusted and Privileged Users were set to during a snapshot in time.

- Privileged/Trusted Users

Regulation Audit Reports

These reports list all the regulations and their individual guidelines applied to your servers and databases. Use the Regulation Guideline report to audit the regulatory guidelines applied to your SQL Server instance, or use the Regulation Compliance Check report to ensure that your servers and databases continue to be in compliance with the selected regulatory guidelines.

- Regulation Guideline Report
- Regulation Compliance Check Report

Sensitive Column/BAD Reports

The Sensitive Column/BAD report lists Sensitive Column and Before-After data audit settings applied to your servers and databases. Use this report to monitor what Sensitive Columns and Before-After data auditing were set to during a snapshot in time.

- Sensitive Column/BAD