Audit reports view

The Audit reports view allows you to generate audit reports using the built-in Microsoft SQL Server Reporting Services Report Viewer (Report Viewer). Each report lets you view and track audited events stored in your event databases and archive files. Use these reports to confirm regulatory compliance, enforce security policies, and capture activity history.

Available actions

Generate a report now

Use the **Audit Reports** tree to navigate to the appropriate report, and then specify your criteria in the report view.

Deploy reports to Microsoft Reporting Services

In the **Reporting Services** pane, click **Deploy Reports**. Starts the Reports Installer, allowing you to deploy individual IDERA SQL Compliance Manager reports to your existing Reporting Services server and customize the report.

View which reports have been deployed

In the **Reporting Services** pane, click **View Deployed Reports**. Opens the Report Manager on the Reporting Services server, allowing you to see which SQL Compliance Manager reports you have deployed.

Available reports

Alert Reports

These reports list alert details, such as target object, affected SQL Server instance, the event, and time of the alert. Use these reports to audit Event and Status Alerts triggered over a specified time period.

- Alert Activity - Events
- Alert Activity - Status

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.

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

These reports list backup, restore, DBCC, DML, 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
- DML Activity (Before-After)
- 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.

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.

Policy Audit Reports

These reports list changes and updates applied to the SQLcompliance 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 SQLcompliance Agent service restarts.

- Agent History
- Alert Rules
- Audit Control Changes
- Integrity Check

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

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