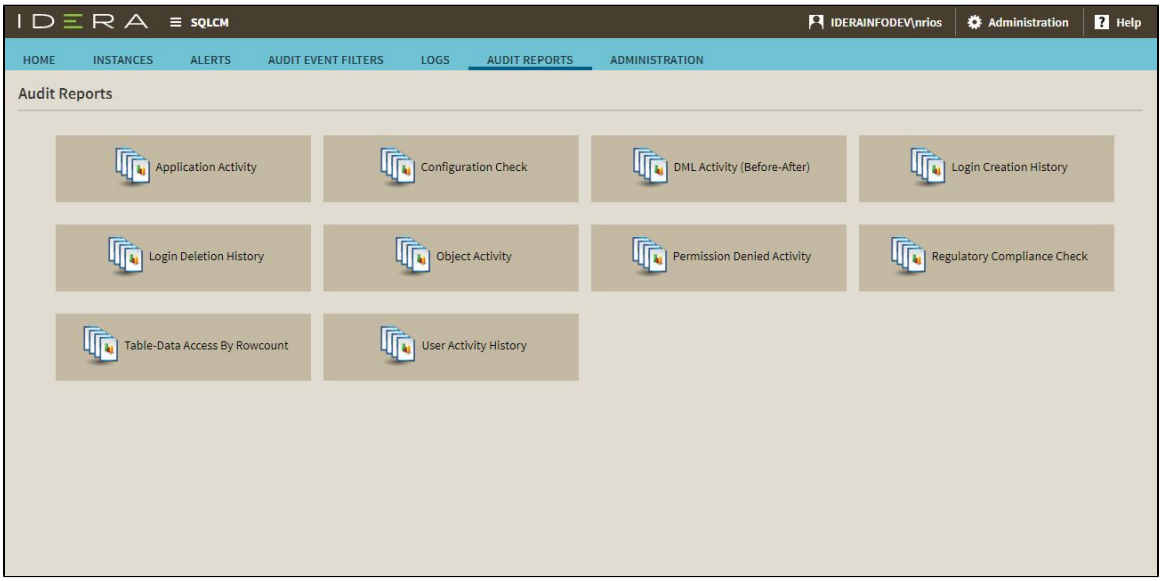
Generate audit reports

The IDERA SQL Compliance Manager Audit Reports view contains a simple interface that allows you to generate audit reports. Each report is based on a template file that is stored in the Reports folder in the SQLcompliance installation directory. When you generate a report, you are able to determine what is displayed by selecting from the options on each individual report. This allows you to generate reports tailored to your needs.

For additional information about SQL Compliance Manager reporting, see Report on Audit Data.



Available reports include:

- **Application Activity**. The Application Activity 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.
- **Configuration Check**. The Configuration Check report displays a list of all the configurations that are set up for your servers and databases.
- **DML Activity (Before-After)**. 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.
- **Login Creation History**. The Login Creation History report lists a history of login creation activities performed on a specific SQL Server instance. Use this report to audit user behavior and login management.
- **Login Deletion Histor**y. The Login Deletion History report lists a history of login deletion activities performed on a specific SQL Server instance. Use this report to audit user behavior and login management.
- **Object Activity**. The Object Activity report lists activities performed on a specific SQL Server instance. Use this report to audit object behavior and settings.
- **Permission Denied Activity**. The Permission Denied Activity report lists unauthorized attempts to execute activities. Use this report to audit your SQL Server security settings and identify misconduct.
- **Regulatory Compliance Check**. The Regulation Compliance Check report displays which servers or databases continue to be in compliance with the selected Regulation Guidelines.
- **Table/Data Access by Row Count.** The Row Count reports on the frequency data is accessed. Use this report to audit sensitive data access and identify suspicious behavior.
- **User Activity Histor**y. The User Activity History report lists activities performed by user account. Use this report to audit your user account settings and identify misconduct.