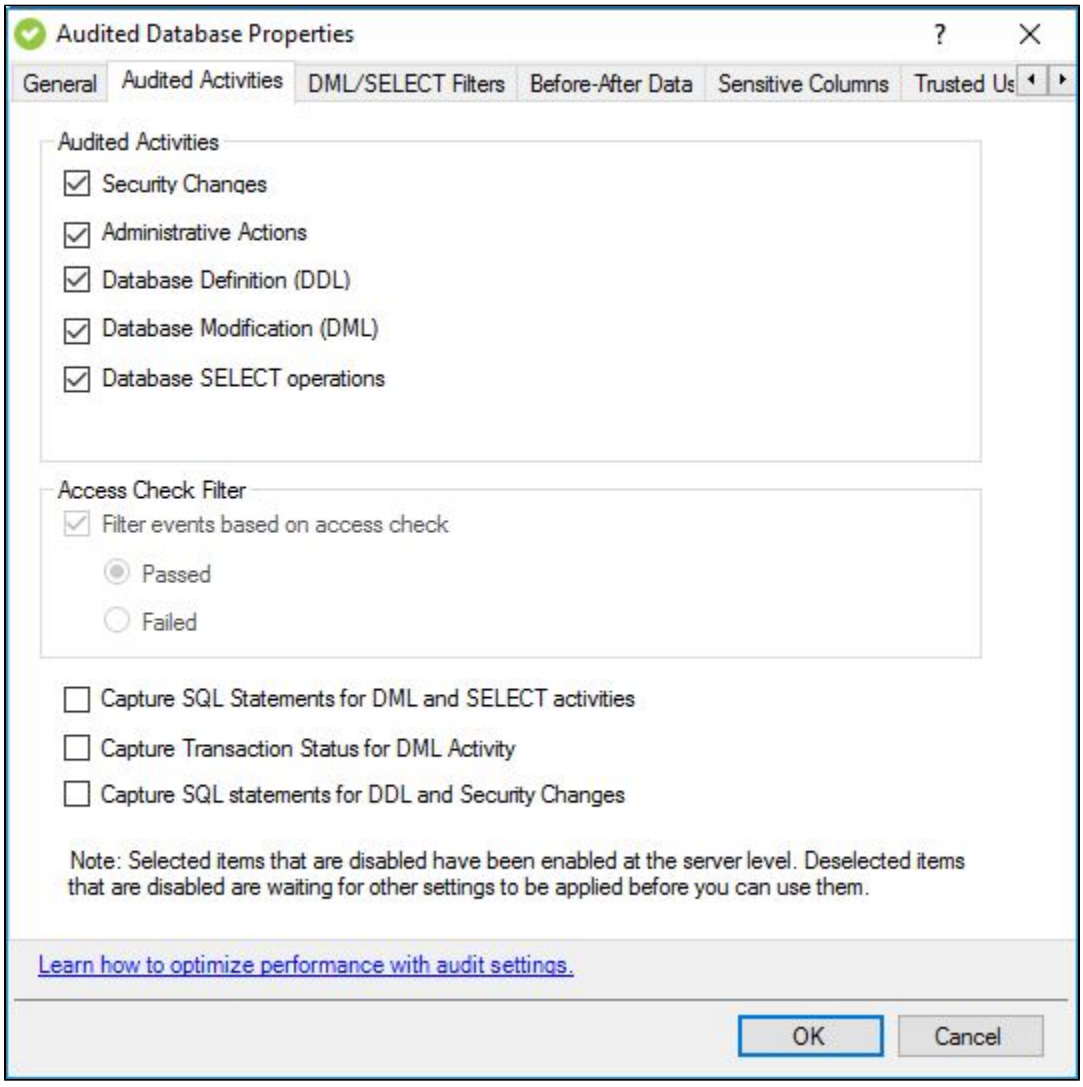
Audited Database Properties window - Audited Activities tab

The Audited Activities tab of the Audited Database Properties tab allows you to change which types of SQL Server events you want to audit on the selected databases. Use the Audit Events tab to see your collected data.



Available fields

Audited Activities

Allows you to select the type of activity you want to audit. IDERA SQL Compliance Manager collects and processes the corresponding SQL Server events based on your selections.

The following are the activities you can audit:

- Security changes
- Administrative Actions
- Database Definition (DDL)
- Database Modification (DML)
- Database SELECT operations

Note

Audited Activities selected at Database-level are automatically pre-selected and disabled for selection when adding new Privileged Users at the Database Privileged User auditing configurations.

Note

When deselecting an audited activity, choose between deselecting at Database-level auditing only or Database-level and Privileged Users auditing.

Access Check Filter

Allows you to refine your audit trail for SQL Server login data by collecting events that better reflect your auditing requirements for security and user processes.

SQL Server validates login permissions and access rights when a user attempts to execute an operation or SQL statement on the audited

SQL Server instance. ***If the access check filter is enabled for a database on a registered instance***, SQL Compliance Manager collects access check events at the database level.

Select this filter to help identify logins that may have inappropriate access rights or permissions. This filter may also help reduce the size of your audit data.

Type of Event Filter	Description
Audit only actions that passed access check	Omits events that track failed access checks performed by SQL server
Audit only actions that failed access check	Omits events that track passed access checks performed by SQL Server

Capture SQL statements for DML and SELECT activity

Allows you to specify whether you want to collect SQL statements associated with audited DML and SELECT activities. To capture these statements, you must also enable DML or SELECT auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.

Capture Transaction Status for DML Activity

Allows you to specify whether you want to collect the status of all DML transactions that are executed by T-SQL scripts run on your audited database. This setting captures begin, commit, rollback, and savepoint statuses. To capture these statuses, you must enable DML auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit transaction status, such as rollbacks.

Capture SQL statements for DDL and Security Changes

Allows you to specify whether you want to collect SQL statements associated with audited database definition (DDL) activities. To capture these statements, you must also enable DDL auditing.

Ensure the Collection Server and the target SQL Server computers have ample resources to handle the additional data collection, storage, and processing. Because this setting can significantly increase resource requirements and negatively impact performance, choose this setting only when your compliance policies require you to audit SQL statements.