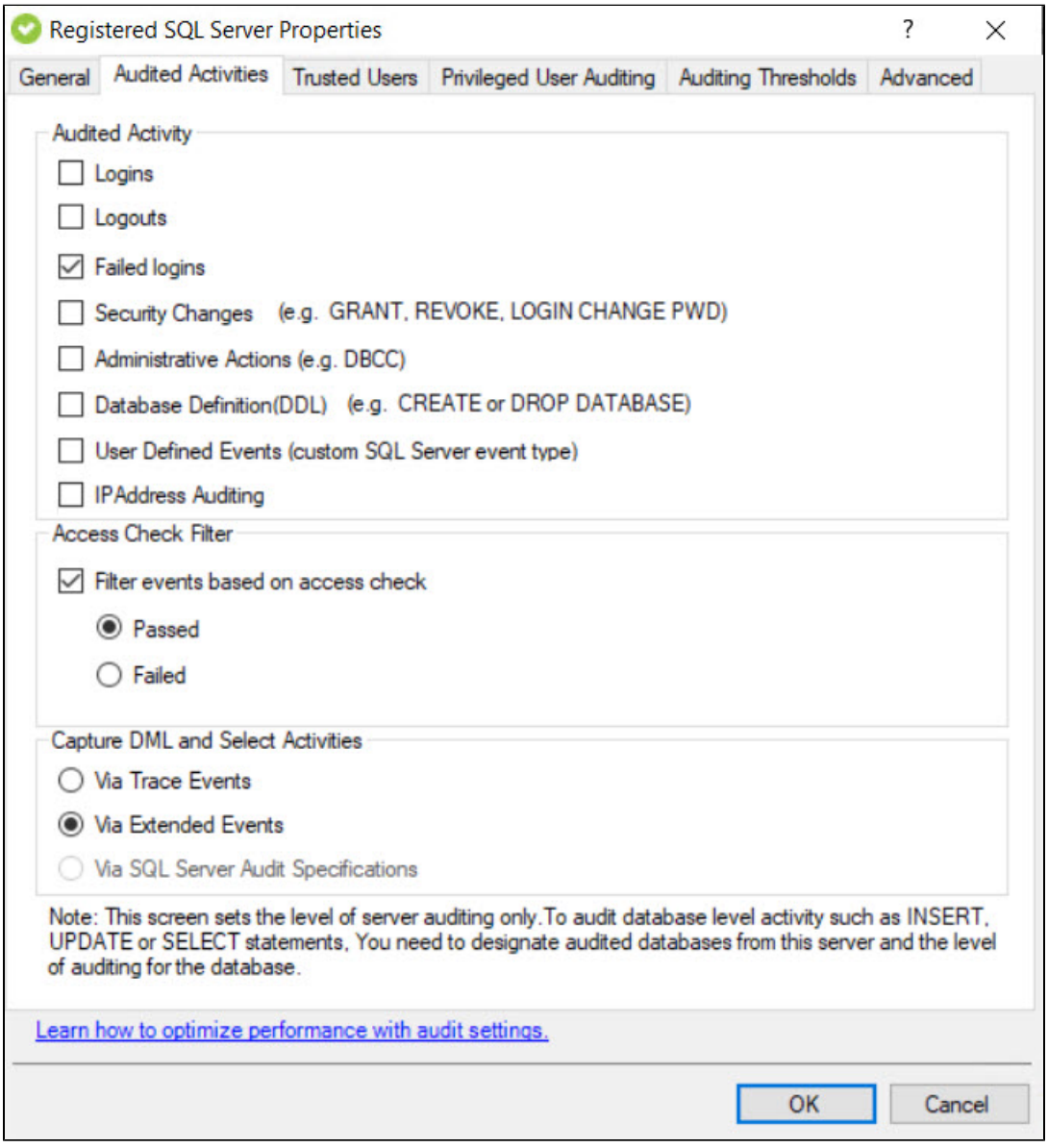
Registered SQL Server Properties window - Audited Activities tab

If you want to use SQL Extended Events as the event handling system for DML and SELECT events occurring on your SQL Server 2012 and later instances, you must enable/disable this feature in the SQL Compliance Manager Web Console. For more information about this feature, see Using SQL Server Extended Events.

The Audited Activities tab allows you to change which types of SQL Server events you want to audit on the selected instance. IDERA SQL Compliance Manager audits these events at the server level only.



Available fields

Audited Activity

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

You can choose to audit event categories and user-defined events. An event category includes related SQL Server events that occur at the server level. A user-defined event is a custom event you create and track using the `sp_trace_generateevent` stored procedure.

Available options include:

- Logins
- Logouts
- Failed logins
- Security changes
- Administrative actions
- Database definition (DDL)
- User-defined events
- IP Address Auditing

Audited Activities selected at Server-level are automatically pre-selected and disabled for selection for Privileged Users added at the Server-level Privileged User Auditing.

Note

Audited Activities selected at Server-level are no longer pre-selected at the audited activities for the Database auditing level.

Capture DML and Select Activities

For each instance registered, the option of Extended Events is selected by default to capture DML and Select activities. During the upgrade process, SQL Compliance Manager checks for the current saved value for the Capture DML and Select Activities options.

Via Trace Events - Allows you to select Trace Events as your event handling system for DML and SELECT activities. For more information about this feature, see Understanding Traces.

Via Extended Events - Allows you to select SQL Server Extended Events as your event handling system for DML and SELECT events for SQL Server 2012 and later versions. For more information about this feature, see Using SQL Server Extended Events.

SQL Compliance Manager does not support Extended Events functionality on SQL Server releases earlier than SQL Server 2012, therefore, for the registration of SQL Server instances with versions lower than SQL Server 2012, the Capture DML and Select Activities option is set to Via Trace Events.

Via SQL Server Audit Specifications - Allows you to select SQL Server Audit Logs as your event handling system for DML and SELECT events for SQL Server 2017 and later versions. For more information about this feature, see Using SQL Server Audit Logs.

SQL Server Audit Specifications is the default Event Collection Method.

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 registered instance*** , SQL Compliance Manager collects access check events at the server level.

Select this filter to help identify logins with 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