Idera Default Audit Settings

IDERA SQL Compliance Manager provides users with a default basic set of settings to begin auditing. These are just the Idera default settings, and users can modify these settings on individual servers and databases to accommodate their auditing needs. These settings will apply to newly added servers and databases. Users can reset back to the Idera default settings at any time by clicking the **Reset to Idera Default Settings** button.

Idera Default Server Audit Settings

Audited Activities tab

Allows you to select the type of activity you want to audit. The following are the Idera Default Database Audit Settings:

- Failed Logins
- **Access Check Filter** - Filter events based on access check
  - Audit only actions that passed access check
- **Capture DML and Select Activities**
  - Via Trace Events

Trusted Users tab

No users selected

Privileged Users Auditing tab

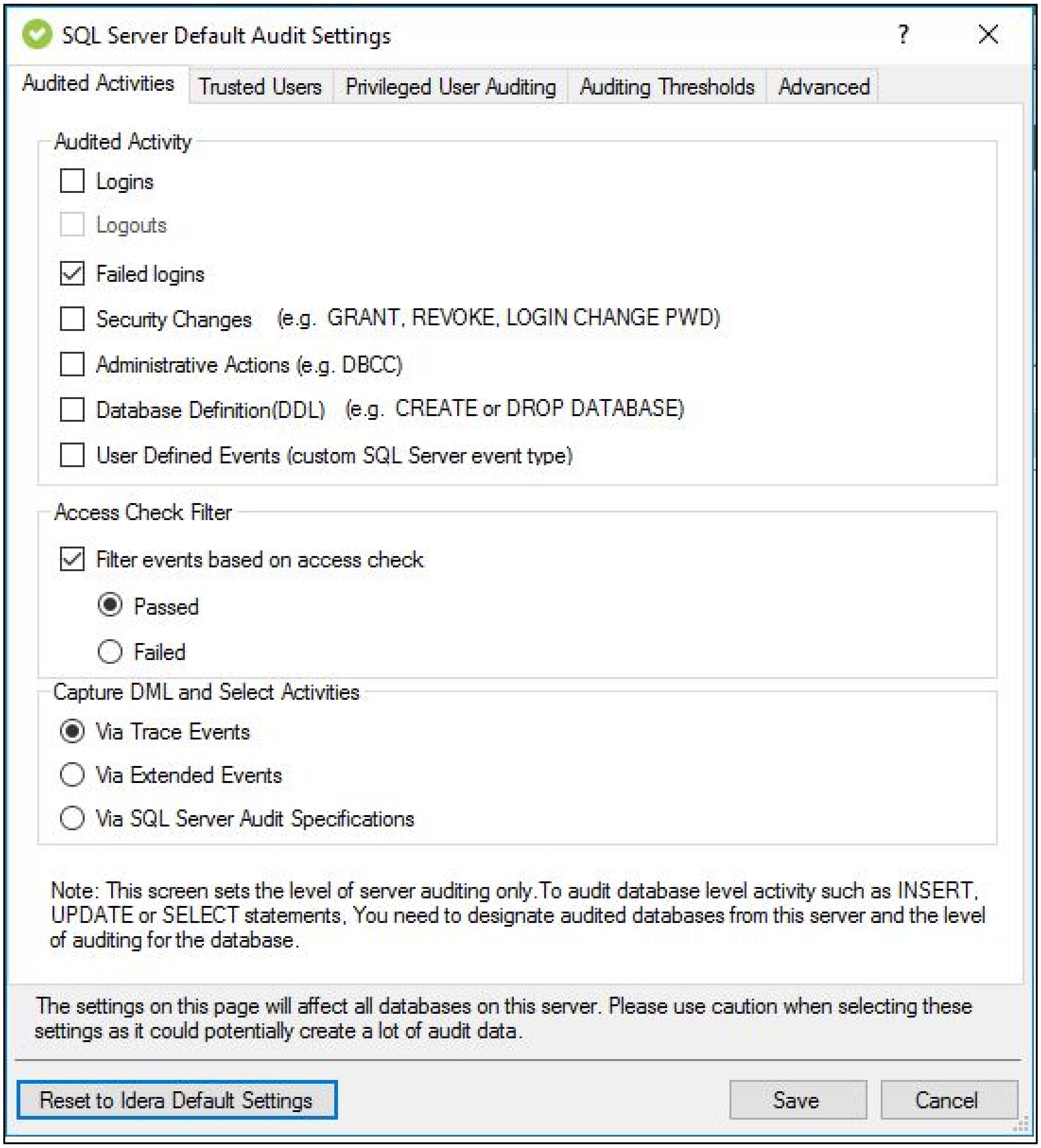
No users selected

Auditing Thresholds tab

No settings enabled

Advanced tab

- **Default Database Permissions**
  - Grant right to read events and their associated SQL statements
- **SQL Statement Limit**
  - Truncate stored SQL statements after 512 characters



SQL Server Default Audit Settings

Audited Activity

- □ Logins
- □ Logouts
- ☑ Failed logins
- □ Security Changes (e.g. GRANT, REVOKE, LOGIN CHANGE PWD)
- □ Administrative Actions (e.g. DBCC)
- □ Database Definition(DDL) (e.g. CREATE or DROP DATABASE)
- □ User Defined Events (custom SQL Server event type)

Access Check Filter

- ☑ Filter events based on access check
  - ● Passed
  - ○ Failed

Capture DML and Select Activities

- ● Via Trace Events
- ○ Via Extended Events
- ○ Via SQL Server Audit Specifications

Note: This screen sets the level of server auditing only.To audit database level activity such as INSERT, UPDATE or SELECT statements, You need to designate audited databases from this server and the level of auditing for the database.

The settings on this page will affect all databases on this server. Please use caution when selecting these settings as it could potentially create a lot of audit data.

Idera Default Database Audit settings

Audited Activities tab

Allows you to select the type of activity you want to audit. The following are the Idera Default Database Audit Settings:

- Security changes
- Database Modification (DML)
- Access Check Filter - setting selected at server level.

Before-After Data

These settings must be set on the individual database level.

Sensitive Columns tab

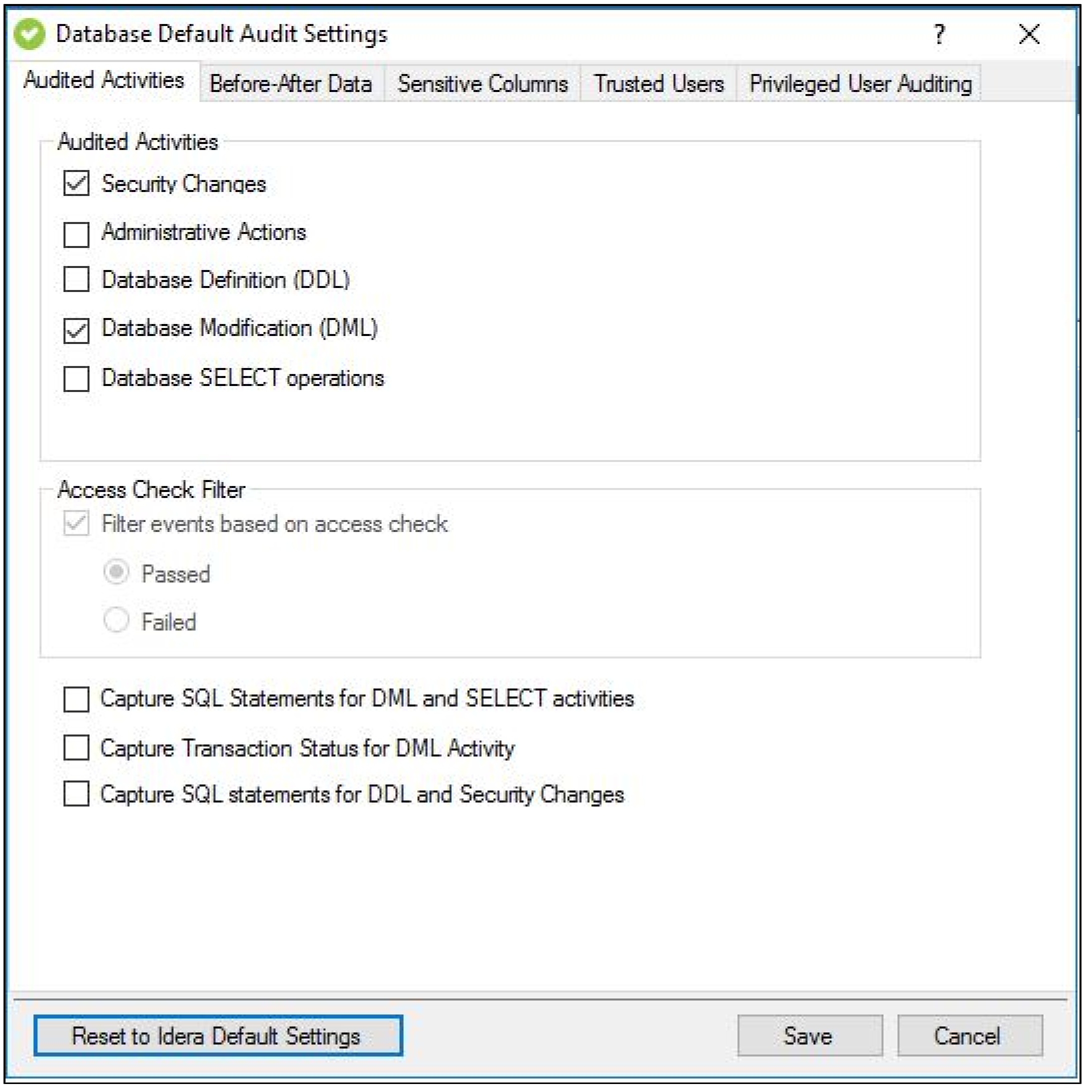
These settings must be set on the individual database level.

Trusted Users tab

No users selected

Privileged Users Auditing tab

No users selected



Audited Activities

☑ Security Changes

□ Administrative Actions

□ Database Definition (DDL)

☑ Database Modification (DML)

□ Database SELECT operations

Access Check Filter

☑ Filter events based on access check

● Passed

○ Failed

□ Capture SQL Statements for DML and SELECT activities

□ Capture Transaction Status for DML Activity

□ Capture SQL statements for DDL and Security Changes