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:

- o Failed Logins
- o 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

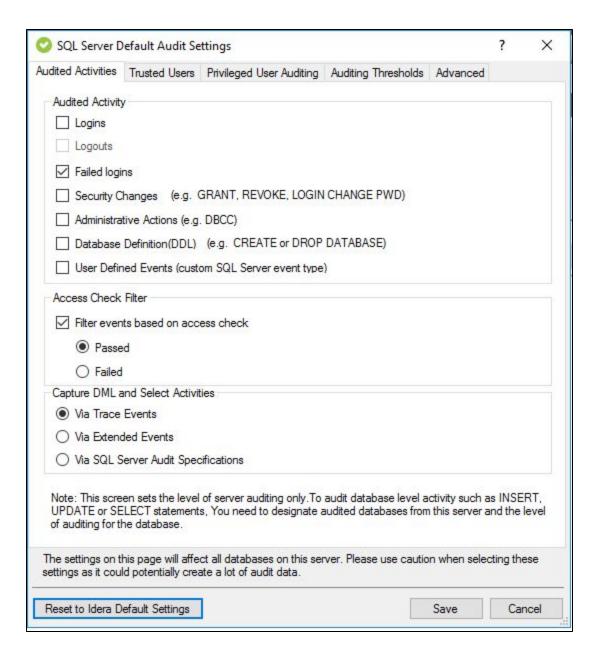
No users selected

Auditing Thresholds tab

No settings enabled

Advanced tab

- Default Database Permissions
 - $^{\circ}\,$ Grant right to read events and their associated SQL statements
- SQL Statement Limit
 - Truncate stored SQL statements after 512 characters



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)
- O Access Check Filter setting selected at server level.

Before-After Data

These settings must be set on the individual database level.

Sensitive Columns tab

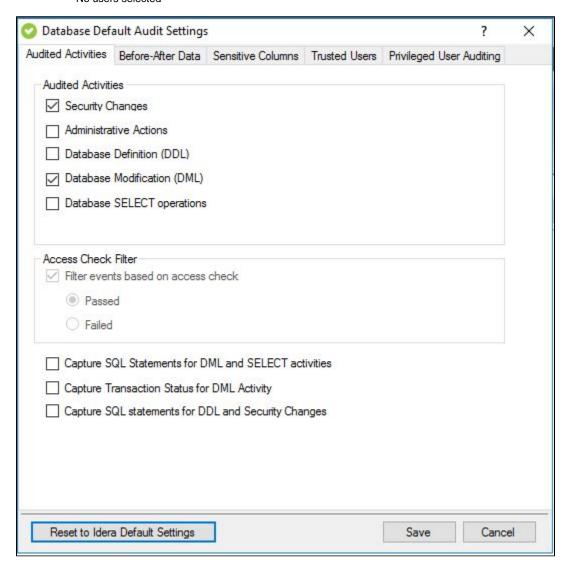
These settings must be set on the individual database level.

Trusted Users tab

No users selected

Privileged Users Auditing tab

No users selected



IDERA | Products | Purchase | Support | Community | Resources | About Us | Legal