Audited Database Properties window - Sensitive Columns tab

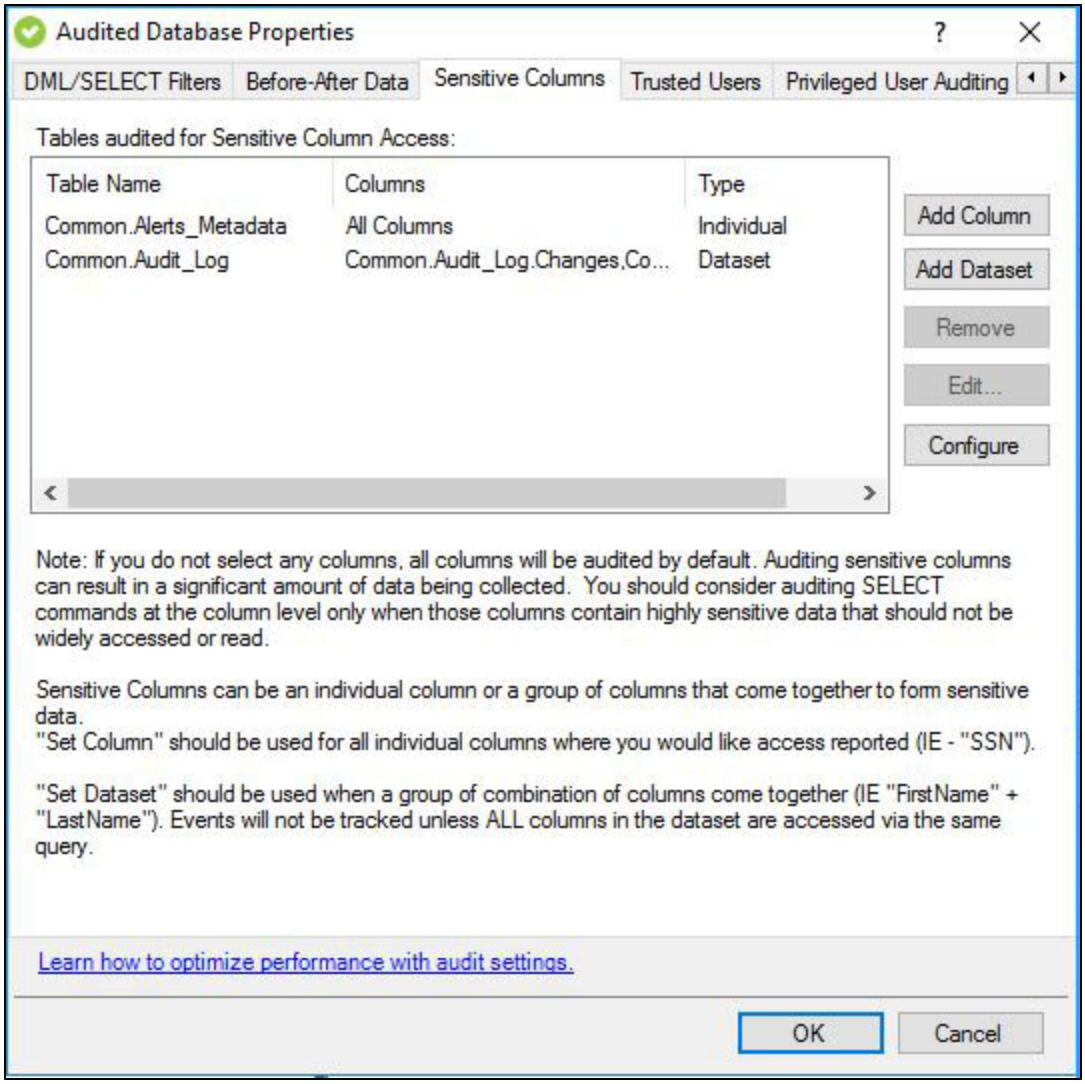
The Sensitive Columns tab of the Audited Database Properties window allows you to select the individual table columns or datasets you want IDERA SQL Compliance Manager to audit for sensitive column access. Configure the type of activity you want to collect data for, choose between Selects, Selects and DML or All Activity. This data tells you which third-party application or database user accessed and read the specified columns. Sensitive Columns can be an individual column or a group of columns that come together to form sensitive data. If no individual columns are selected, by default all columns from the selected table will be audited.

Audit access to sensitive columns when it is critical to capture whether someone read the data in a specific table column. When this feature is enabled, you can review the SELECT events in the Audit Events view. Enabling this feature can impact your Collection Server and Management Console performance. You can audit sensitive columns on specific tables without enabling SELECT statement auditing at the database level.

IDERA SQL Compliance Manager does not capture sensitive column data for trusted user accounts. For more information about trusted users, see Audited Database Properties window - Trusted Users tab.

To successfully audit specific columns on a table, ensure the table name does not contain the following special characters: \ / : * ? "

Sensitive Column auditing is supported by SQL Compliance Manager Agent 3.5 or later. To use this feature, please ensure you upgrade your agent to at least version 3.5.



Available actions

Specify tables for before and after data collection

Use **Add** and **Remove** to specify the tables for which you want to access to specific sensitive columns.

Specify which columns to audit

Use **Edit** to specify which columns you want to audit. You can audit all columns or individual columns.

Specify which columns to audit as a group

Use **AddDataSet** to specify a group of columns to audit as a set of sensitive information.

Configure

Allows you to choose which type of activity you want Sensitive Columns to collect data for. You can choose one of the following types of activity to collect data for your Sensitive Columns:

- Select Only
- All Activity
- SELECT and DML

Available fields

Table Name

Provides the name of the table you are auditing on this database.

Columns

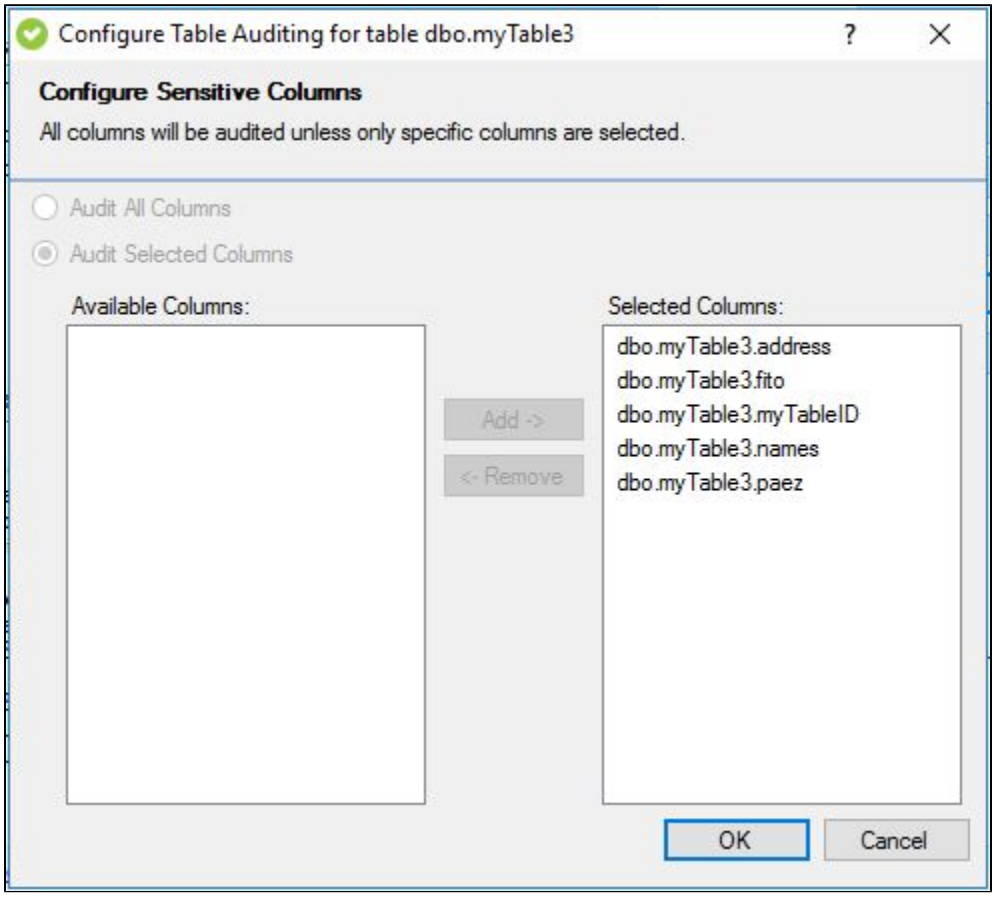
Indicates the status of the columns associated with the audited tables. Typically, this field will display **All Columns** or list the individual columns that are audited for SELECT events.

Type

Indicates whether the column is being audited as an 'Individual' or as part of a 'Dataset'.

Set up auditing sensitive columns

Sensitive column auditing occurs independently from your other database-level audit settings.

To set up auditing sensitive columns:

1. On the Sensitive Columns tab, click **Add** to choose which audited tables should also be audited at the column level when a user attempts to access this column.
2. Choose the appropriate tables, and then click **OK**. By default, all columns are audited.
3. ***If you want to audit specific columns***, select the table, and then click **Edit**.
4. ***if you want to audit a group of columns***, click **AddDataSet.**