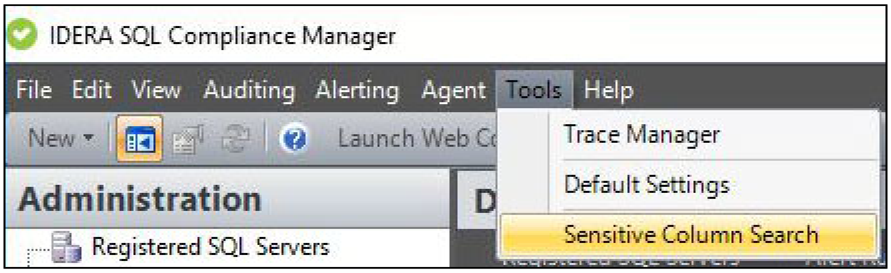
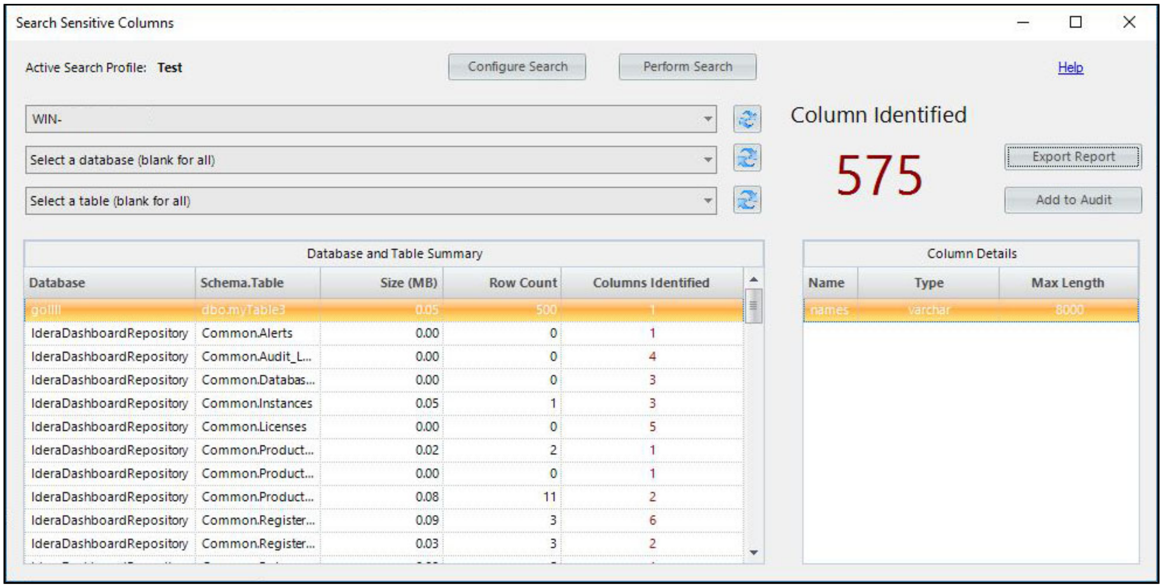
Sensitive Column Search

The Sensitive Column Search window allows you to search all of the tables and columns on a targeted database to discover the location of sensitive data that needs to be audited. The Sensitive Column Search feature includes pre-configured common sensitive data strings for you to select from, or you can define specific strings in order to customize your Search Profile exactly the way you want. Define your search to a specific table within a database or search an entire instance and export your successful search results to a CSV format to easily analyze results.



You can access this window from the Tools option of the SQL Compliance Manager Menu and select Sensitive Column Search from the drop-down list available, or by right clicking any registered Database or Instance and selecting the Sensitive Column Search option.



Active Search Profile: **Test**

WIN-

Select a database (blank for all)

Select a table (blank for all)

Column Identified

575

Database and Table Summary

Database	Schema.Table	Size (MB)	Row Count	Columns Identified
golll	dbo.myTable3	0.05	500	1
IderaDashboardRepository	Common.Alerts	0.00	0	1
IderaDashboardRepository	Common.Audit_L...	0.00	0	4
IderaDashboardRepository	Common.Databas...	0.00	0	3
IderaDashboardRepository	Common.Instances	0.05	1	3
IderaDashboardRepository	Common.Licenses	0.00	0	5
IderaDashboardRepository	Common.Product...	0.02	2	1
IderaDashboardRepository	Common.Product...	0.00	0	1
IderaDashboardRepository	Common.Product...	0.08	11	2
IderaDashboardRepository	Common.Register...	0.09	3	6
IderaDashboardRepository	Common.Register...	0.03	3	2

Column Details

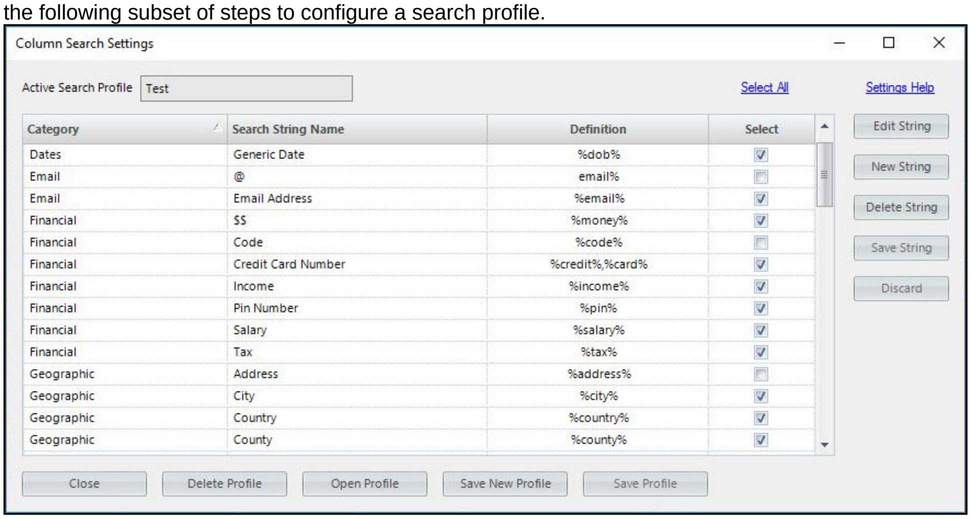
Name	Type	Max Length
names	varchar	8000

Performing a search

To search for Sensitive Columns within one or more databases:

1. Select the target server name from the available list. To search all databases, leave the list at the default **Select a database** option.
2. ***If you selected a specific database,*** select a target table name. Note that you cannot select a table if you did not select a target database.
3. Select a search profile, and then continue with the next step. ***If no profiles are configured or if you want to edit an existing profile,*** click **Configure Search**. SQL Compliance Manager displays the Column Search Settings window for you to configure a search profile. Use

the following subset of steps to configure a search profile.

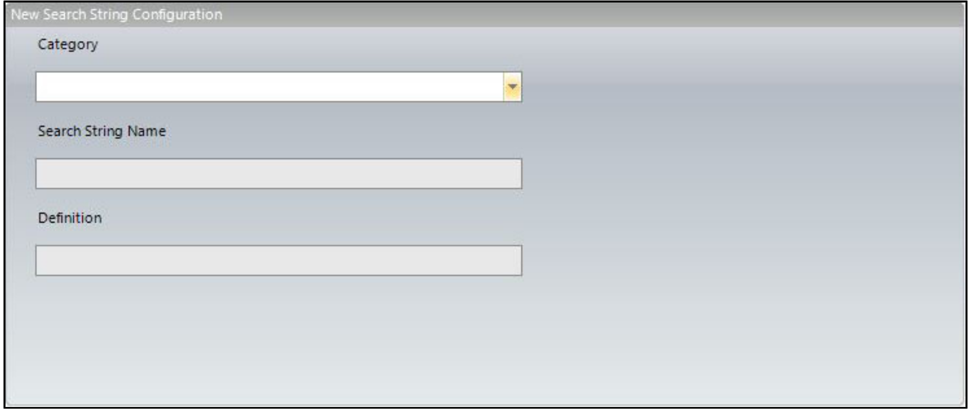


Active Search Profile: Test

Category	Search String Name	Definition	Select
Dates	Generic Date	%dob%	☑
Email	@	email%	☐
Email	Email Address	%email%	☑
Financial	$$	%money%	☑
Financial	Code	%code%	☐
Financial	Credit Card Number	%credit%,%card%	☑
Financial	Income	%income%	☑
Financial	Pin Number	%pin%	☑
Financial	Salary	%salary%	☑
Financial	Tax	%tax%	☑
Geographic	Address	%address%	☐
Geographic	City	%city%	☑
Geographic	Country	%country%	☑
Geographic	County	%county%	☑

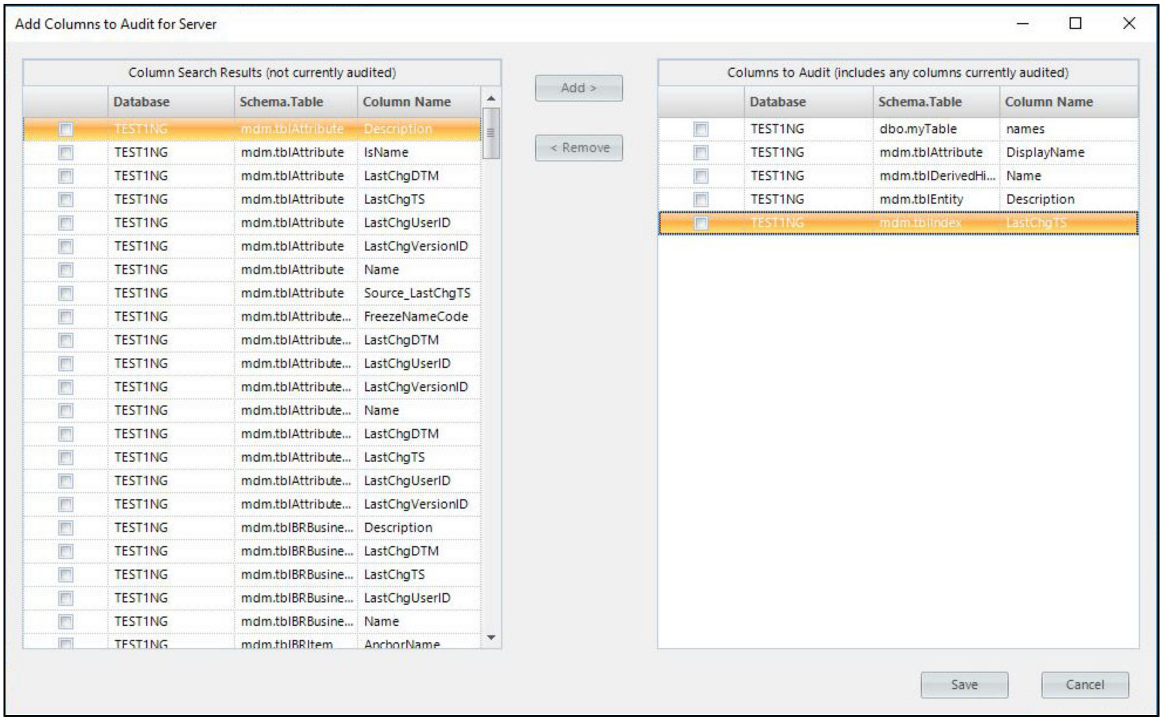
a. In the Column Search Settings window, select one or more search strings you want to include in the search profile. Click **Select All** to include all of the available search strings in this profile.

b. ***If the search string you want to use does not exist and you want to create a new search string,*** click **New**. This option allows you to select a category, type a name for the search string, and then include the string Definition. Click **Save** to retain the search string you just created.



c. Once you select all of the search string you want in the profile, click **Save Profile**. The profile is now available for you to select on the Sensitive Column Search window.

4. Click **Perform Search** to execute the search on the selected database(s) and table(s) based on the selected **Active Search Profile**. SQL Compliance Manager runs the Sensitive Column search and displays the results.
5. Click **Export Report** to export the results in .csv format. This function allows you to save the data in a format that is compatible with the Import Sensitive Columns feature.
6. Click **Add to Audit** to open the Add Columns to Audit for Server window where you can Add or Remove your Column Search Results to the Columns to Audit section.



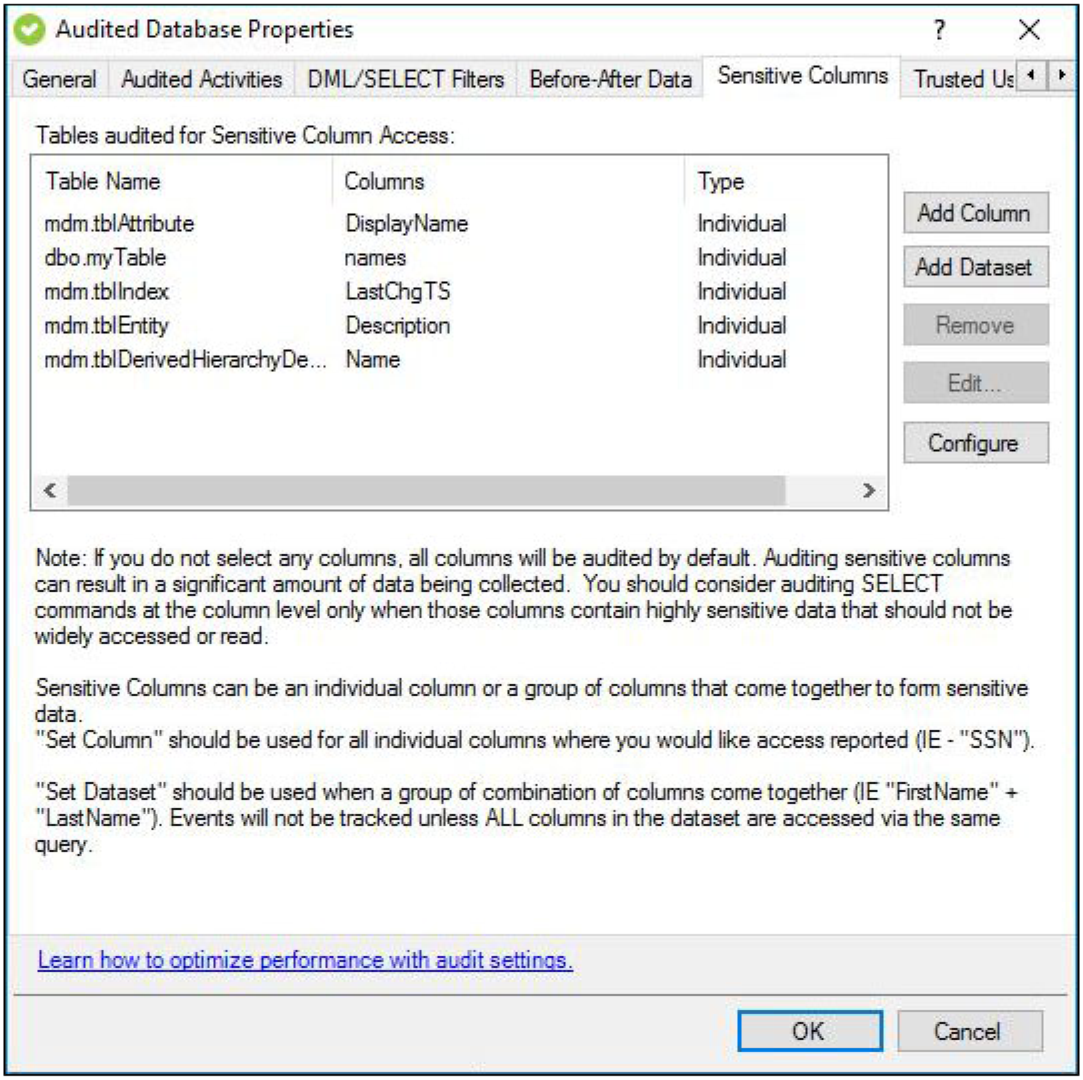
Add Columns to Audit for Server

Column Search Results (not currently audited)

	Database	Schema.Table	Column Name
□	TEST1NG	mdm.tblAttribute	Description
□	TEST1NG	mdm.tblAttribute	IsName
□	TEST1NG	mdm.tblAttribute	LastChgDTM
□	TEST1NG	mdm.tblAttribute	LastChgTS
□	TEST1NG	mdm.tblAttribute	LastChgUserID
□	TEST1NG	mdm.tblAttribute	LastChgVersionID
□	TEST1NG	mdm.tblAttribute	Name
□	TEST1NG	mdm.tblAttribute	Source_LastChgTS
□	TEST1NG	mdm.tblAttribute...	FreezeNameCode
□	TEST1NG	mdm.tblAttribute...	LastChgDTM
□	TEST1NG	mdm.tblAttribute...	LastChgUserID
□	TEST1NG	mdm.tblAttribute...	LastChgVersionID
□	TEST1NG	mdm.tblAttribute...	Name
□	TEST1NG	mdm.tblAttribute...	LastChgDTM
□	TEST1NG	mdm.tblAttribute...	LastChgTS
□	TEST1NG	mdm.tblAttribute...	LastChgUserID
□	TEST1NG	mdm.tblAttribute...	LastChgVersionID
□	TEST1NG	mdm.tblBRBusine...	Description
□	TEST1NG	mdm.tblBRBusine...	LastChgDTM
□	TEST1NG	mdm.tblBRBusine...	LastChgTS
□	TEST1NG	mdm.tblBRBusine...	LastChgUserID
□	TEST1NG	mdm.tblBRBusine...	Name
□	TEST1NG	mdm.tblBRItem	AnchorName

Columns to Audit (includes any columns currently audited)

	Database	Schema.Table	Column Name
□	TEST1NG	dbo.myTable	names
□	TEST1NG	mdm.tblAttribute	DisplayName
□	TEST1NG	mdm.tblDerivedHi...	Name
□	TEST1NG	mdm.tblEntity	Description
□	TEST1NG	mdm.tblIndex	LastChgTS



Tables audited for Sensitive Column Access:

Table Name	Columns	Type
mdm.tblAttribute	DisplayName	Individual
dbo.myTable	names	Individual
mdm.tblIndex	LastChgTS	Individual
mdm.tblEntity	Description	Individual
mdm.tblDerivedHierarchyDe...	Name	Individual

Note: If you do not select any columns, all columns will be audited by default. Auditing sensitive columns can result in a significant amount of data being collected. You should consider auditing SELECT commands at the column level only when those columns contain highly sensitive data that should not be widely accessed or read.

Sensitive Columns can be an individual column or a group of columns that come together to form sensitive data.
"Set Column" should be used for all individual columns where you would like access reported (IE - "SSN").

"Set Dataset" should be used when a group of combination of columns come together (IE "FirstName" + "LastName"). Events will not be tracked unless ALL columns in the dataset are accessed via the same query.

Learn how to optimize performance with audit settings.