

Use filters to specify which data is collected

IDERA SQL Secure uses snapshot filters to control the data collected from your audited SQL Server instances. Each filter rule defines which data, such as permissions on user tables in a specific database, is collected and included in the snapshot.

By default, SQL Secure collects all available audit data. You can edit this default filter rule or delete it after you have defined your custom filter.



Filters applied per Instance

Custom filters are applied at the instance level and are unique to that instance. You can create a different filter for each instance. You can also create more than one filter, depending on your assessment needs. When multiple filters are defined, SQL Secure aggregates them, collecting all data identified by all the filters associated with this instance.

Go to [Add Filters](#) to view about specifying filter properties, databases, and objects.

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)