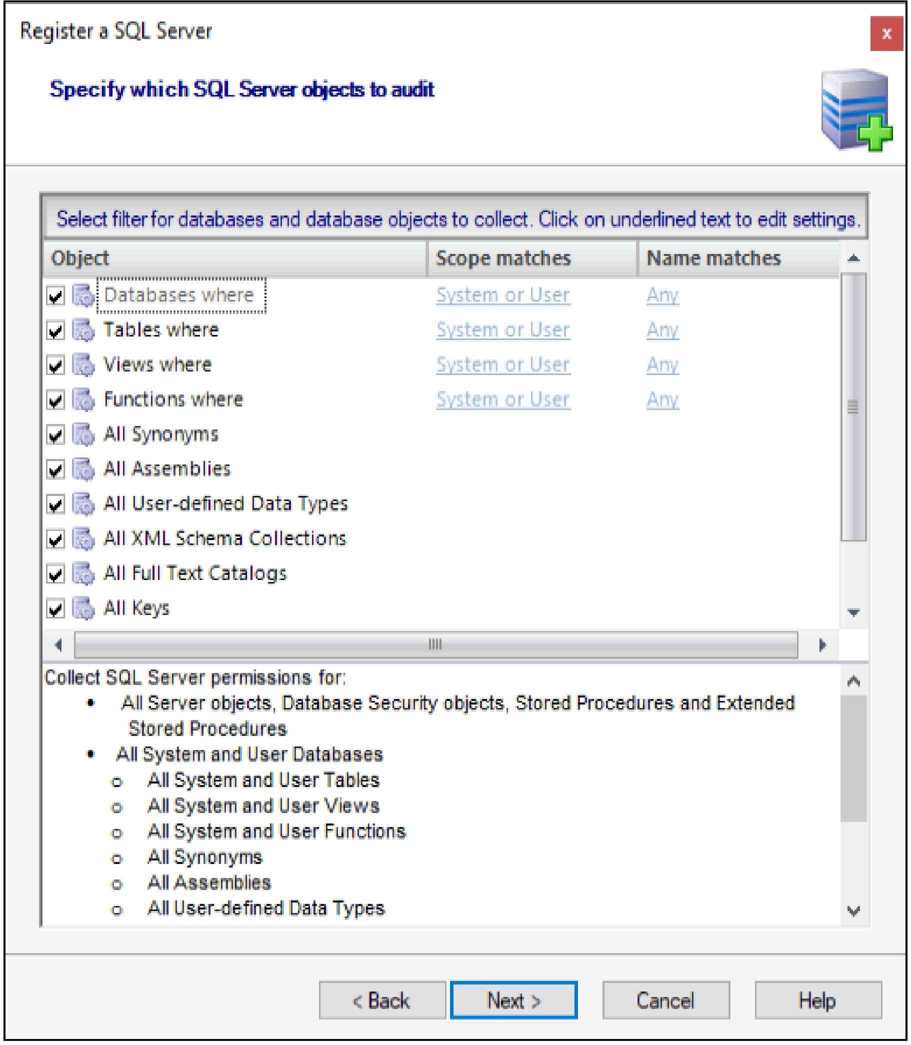
Select SQL Server objects to audit

In the **Select SQL Server Objects to Audit** section of this wizard, you can specify which database or server objects IDERA SQL Secure will audit to collect security information. By default, SQL Secure audits all SQL Server objects.

To select objects to audit:

1. Check the objects you want to audit in the list.



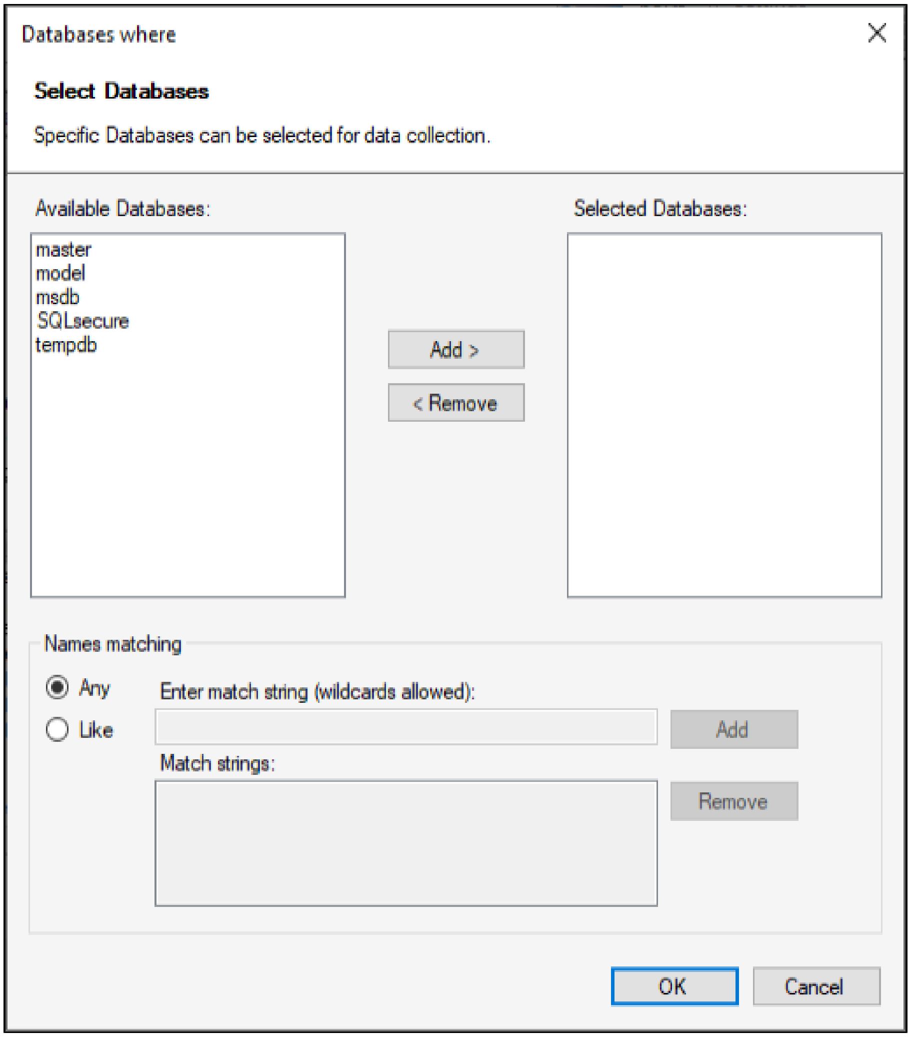
Select filter for databases and database objects to collect. Click on underlined text to edit settings.

Object	Scope matches	Name matches
☑ Databases where	System or User	Any
☑ Tables where	System or User	Any
☑ Views where	System or User	Any
☑ Functions where	System or User	Any
☑ All Synonyms		
☑ All Assemblies		
☑ All User-defined Data Types		
☑ All XML Schema Collections		
☑ All Full Text Catalogs		
☑ All Keys		

Collect SQL Server permissions for:

- All Server objects, Database Security objects, Stored Procedures and Extended Stored Procedures
- All System and User Databases
  - All System and User Tables
  - All System and User Views
  - All System and User Functions
  - All Synonyms
  - All Assemblies
  - All User-defined Data Types

2. For those objects that have scope options, click the text in the **Scope matches** column, and select the appropriate option (User, System, System or User).
3. For those objects that have naming options, click the text in the **Name matches** column, and a new window opens with the following options:
   - In the first part of the window, select the elements you want to move to the **Selected** list, and then click **Add.** You can remove the added elements from the list by selecting the element and clicking **Remove**.
   - On the Names matching box, select **Any** if you want to include all elements names in your snapshot.
   - If you want to specify strings that your filter will use to match the names of your databases, click **Like** to enable new options on the **Name matching** box. You can search for a specific element by typing a specific string in the **Enter match string** field (you can use wildcards), and then click **Add**. The **Match strings** field added strings. You can also remove strings from this box by selecting the string and clicking **Remove**.



Databases where

Select Databases

Specific Databases can be selected for data collection.

Available Databases:

master
model
msdb
SQLsecure
tempdb

Selected Databases:

Names matching

● Any

○ Like

Enter match string (wildcards allowed):

Match strings:

4. SQL Secure displays at the bottom section of this window a summary of all selected objects and their specified settings.
5. Click **Next** to go to Schedule Snapshots.

ⓘ For Amazon RDS and Azure SQL Databases the **Full Text Catalogs** objects are supported

⚠ When you are selecting objects to audit, be aware that you need to include all the objects your policies need to appropriately assess security risks.