

Registered SQL Server Properties window - Advanced tab

The Advanced tab of the Registered SQL Server Properties window allows you to configure the following settings:

- Control the default permission settings on the databases that contain audit data for this SQL Server instance.
- Indicate whether collected SQL statements should be truncated if they pass the specified character limit. This option is only available if you are auditing SQL statements executed at the server level on this instance.

Registered SQL Server Properties

General Audited Activities Trusted Users Privileged User Auditing Auditing Thresholds **Advanced**

Default Database Permissions
Select the default level of access you want to grant users on the database containing audit data for this SQL Server instance.

- ☒ Grant right to read events and their associated SQL statements .
- ☐ Grant right to read events only - To allow users to view the associated SQL statements, you will need to explicitly grant users read access to the database.
- ☐ Deny read access by default - To allow users to view events and the associated SQL, you will need to explicitly grant users read access to the database.

SQL Statement Limit
In most cases, the high level event information gathered is sufficient for meeting audit requirements. However, some users may find that they need the extra details afforded by the collection of the actual SQL statement associated with each event.
Be aware that collecting SQL statements will significantly increase the amount of data gathered and should be used sparingly. Gathered SQL statements may also contain confidential information. The option to gather SQL statements is available on each audited database.
Use the following option to specify the maximum size of stored SQL statements. Statements exceeding this maximum are truncated.

- ☐ Store entire text of SQL statements
- ☒ Truncate stored SQL statements after characters
For Reports, SQL text will be truncated after characters.

☒ Add New Databases for auditing automatically

[Learn how to optimize performance with audit settings.](#)

OK Cancel

Available fields

Default Database Permissions

Allows you to set the default permissions on the databases that contain audit data for this instance. Keep in mind that login permissions specified at the database are applied along with the default permissions you set here. You can select one of the following default permissions:

- Grant right to read events and their associated SQL statements.
- Grant right to read events only - To allow users to view the associated SQL statements, you will need to explicitly grant users read access to the database.
- Deny read access by default - To allow users to view events and the associated SQL statements, you will need to explicitly grant users read access to the database.

SQL Statement Limit

Allows you to specify whether you want to truncate collected SQL statements associated with audited events. You can set the character limit for collected SQL statements. By default, this limit is 512 characters. The Collection Server truncates SQL statements that are longer than the specified character limit.

Add New Databases Automatically

Selecting this checkbox will automatically add newly created databases to your list of audited databases for the selected server. Database Default Audit Settings will be apply to the newly created databases, you can update the [Database Default Audit Settings](#) at any time.

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