SQL Logins tab

The SQL Logins tab allows you to manage the SQL Server login accounts associated with the Repository databases. Use this window to configure SQL Server security access and designate permissions within IDERA SQL Compliance Manager.

SQL Compliance Manager leverages the SQL Server security model, using SQL Server logins to authenticate access to the Repository databases and your audit data.

This tab does not list the following logins, which have read access to audit data stored in the Repository databases:

- SQL authentication logins, such as the sa account, who are members of the sysadmin fixed server role
- Windows authentication logins who are members of the local Administrators group

Available actions

New Login

Allows you to create a SQL Server login. SQL Compliance Manager creates this login at the SQL Server instance that hosts the Repository databases.

View Login Properties

Allows you to view details about permissions settings and database access.

Delete

Allows you to delete the selected SQL Server login. Deleting a login removes the login from the SQL Server instance that hosts the Repository databases. This login will no longer be able to view or report on audit data, and the Windows user account associated with this login will no longer be able to access the Management Console.

Refresh

Allows you to refresh the Logins list with current information.

Available columns

Name

Provides the logon name of the SQL Server login account.

Type

Indicates whether the login is a Windows user or group.

Server Access

Indicates whether security access is permitted or denied to the SQL Server instance that hosts the Repository databases.

Permissions in SQL Compliance Manager

Indicates which SQL Compliance Manager permission the selected login has on the Repository databases.

SQL Compliance Manager audits all activity on your server. Learn more > >

IDERA Website	Products	Purchase	Support	Community	About Us	Resources	Legal