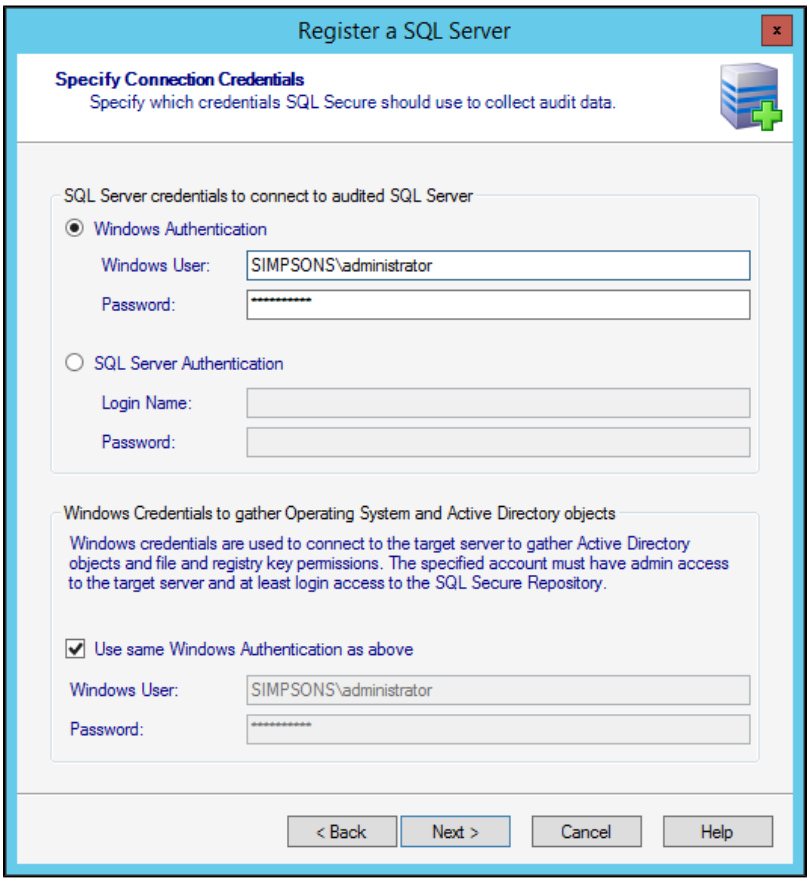
Specify connection credentials

The **Specify Connection Credentials** section of this wizard allows you to designate the credentials that IDERA SQL Secure will use to access the instance containing the SQL Server or Azure SQL databases you are adding. When adding a SQL Server instance, you can specify either SQL Server login or Windows account credentials. When adding an Azure SQL database, specify either the SQL Server login or Azure Active Directory credentials.



In this section you have to specify the following credentials:

Item	Description
SQL Server credentials to connect to audited SQL Server	Choose one of the following options: • Select **Windows Authentication** and enter the credentials in the fields provided. • Select **Azure Active Directory** and enter the credentials for the Azure AD account. • Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.
Windows Credentials to gather Operating System and Active Directory objects - These credentials are used to connect to the target server to gather Active Directory objects, file, and registry key permissions.	Choose one of the following options: • Check the **Use same Windows Authentication as above** box to use the Windows credentials specified above. • Specify a different Windows account that SQL Secure will use use to gather information about OS and AD objects.

Azure Active Directory credentials to gather Active Directory objects	Choose one of the following options: • Check the **Use same Azure AD Authentication as above** box to use the Azure Active Directory credentials specified above. • Specify a different Azure AD account that SQL Secure will use to gather information about Active Directory objects.

Case Sensitive accounts

Take into account that if the login configuration for the SQL Server you want to audit is case-sensitive, you must enter your login credentials in the case-sensitive format.

Permissions and Privileges

You should keep in mind the following permissions for the accounts specified in this section:

- The SQL Server login must belong to the sysadmin fixed role on the target instance.
- The Windows account must have Windows Administrator privileges on the target instance to collect group membership information.
- The account specified for gathering information about OS and AD objects must have admin access to the target server and at least login access to the SQL Secure Repository.

After you specify your connection credentials, click **Next** to go to Add server group tags.