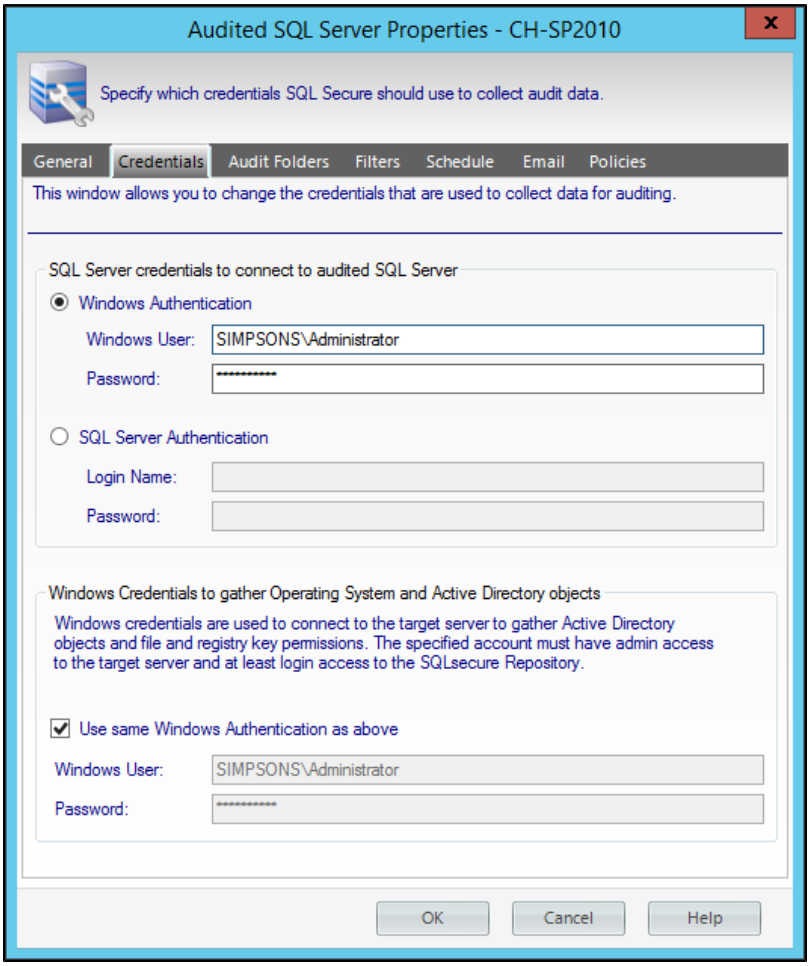
Change connection credentials

The **Credentials** tab displays the credentials that IDERA SQL Secure uses to access the databases on the selected SQL Server instance. If you need to make changes to your credentials, change the information in the fields provided.



There are two types of credentials you need to specify:

Option	Description
SQL Server credentials to connect to audited SQL Server	Choose one of the following options: • Select **Azure Active Directory** and enter the credentials for your Azure AD account. • Select **Windows Authentication** and enter the credentials in the fields provided. • Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.
Azure AD or 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.	Select 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.

If the login configuration for the SQL Server you want to audit is case-sensitive, you must enter your login credentials in a 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.