Specify connection credentials

The **Specify Connection Credentials** wizard allows you to designate the credentials that IDERA SQL Secure will use to access the SQL Server instance you are adding whether the SQL Server instance is running private network or public cloud such as Azure VM, Azure SQL Databases, Amazon EC2 or Amazon RDS. You have to specify credentials according the type of server you want to register:
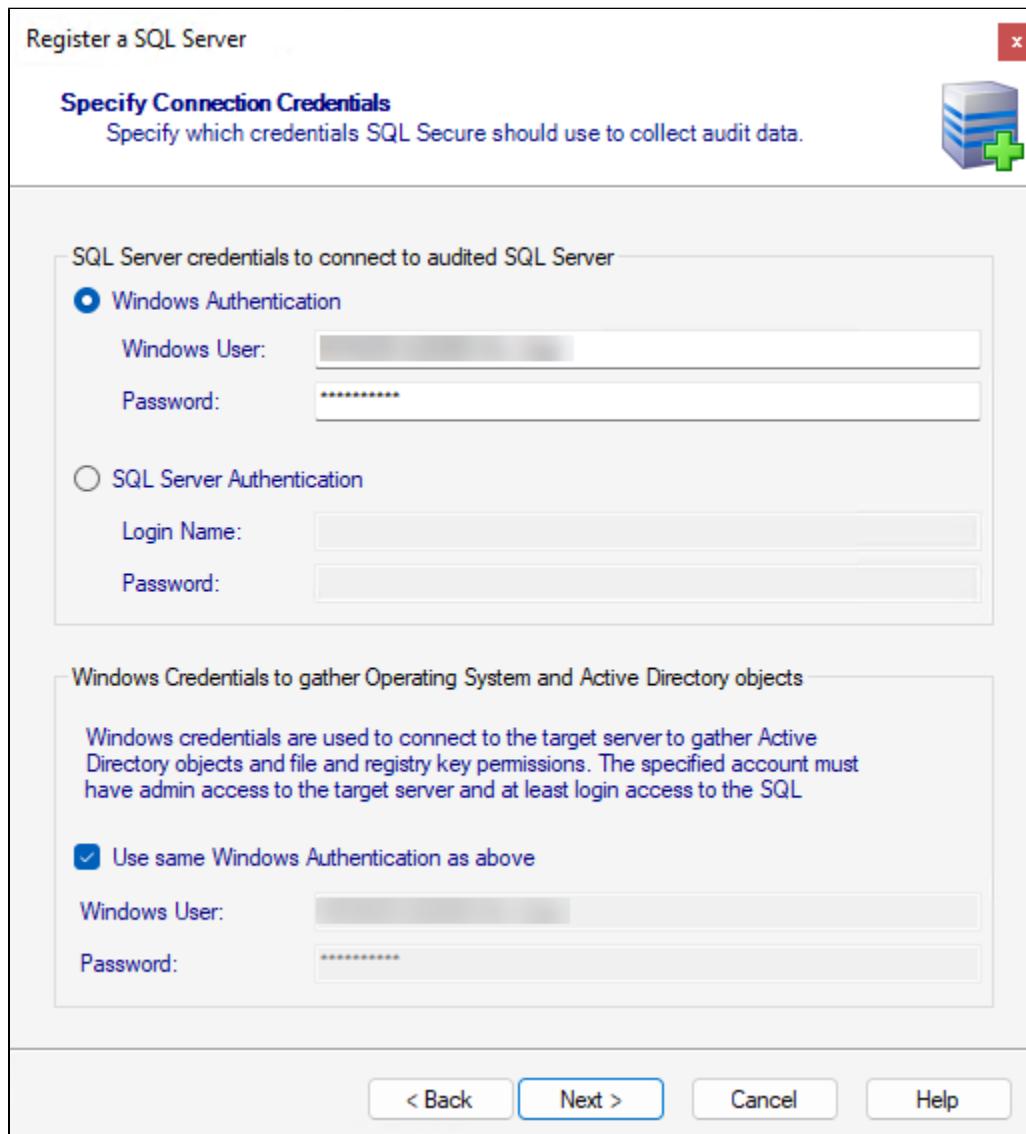
On-Premise SQL Server

For **On-Premise SQL Server** servers, you have to specify the following credentials:

On the first section you will see the **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.
- ○ Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

On the **Windows Credentials to gather Operating System and Active Directory objects** credentials section, you have 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.

SQL Server on Azure Virtual machine

For **SQL Servers on Azure Virtual machines**, you have to specify the following credentials:

On the **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.
- ○ Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

The **Azure Active Directory to gather Operating System and Active Directory objects** section, asks for credentials to connect the target server to gather Active Directory objects and key permissions.

The accounts need **Administrator** access to the target server.

SQL Server on Amazon EC2

For **SQL Servers on Azure Virtual machines**, you have to specify the following credentials:

On the **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.
- ○ Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

The **AWS Directory Service for Microsoft Active Directory to gather Operating System and Active Directory objects** section, asks for credentials to connect the target server to gather Active Directory objects and key permissions.

The accounts need **Administrator** access to the target server.

Azure SQL Database

On the SQL Server credentials to connect to audited SQL Server section, choose one of the following options:

- Select **Azure Active Directory** and enter the credentials in the fields provided.
- Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

⚠

Connection Error

Configure your Azure SQL Server Firewall if a Connection Error displays**.**

Amazon RDS for SQL Server

On the SQL Server credentials to connect to the audited SQL Server section, choose one of the following options:

- Select **AWS Directory Service for Micrsoft Active Directory** and enter the credentials in the fields provided.
- Click **SQL Server Authentication** to use the default credentials of your SQL Server Agent.

Register a SQL Server

Specify Connection Credentials
Specify which credentials SQL Secure should use to collect audit data.

SQL Server credentials to connect to audited SQL Server

○ AWS Directory Service for Microsoft Active Directory

Amazon AD Account:

Password:

● SQL Server Authentication

Login Name:

Password: ••••••••••

[< Back] [Next >] [Cancel] [Help]

⚠️

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.

6

IDERA | **Products** | **Purchase** | **Support** | **Community** | **Resources** | **About Us** | **Legal**