SQL Server Configuration Guide

Use this guide along with the Data tab configuration guide to configure a SQL Server-integrated SecureAuth IdP realm.

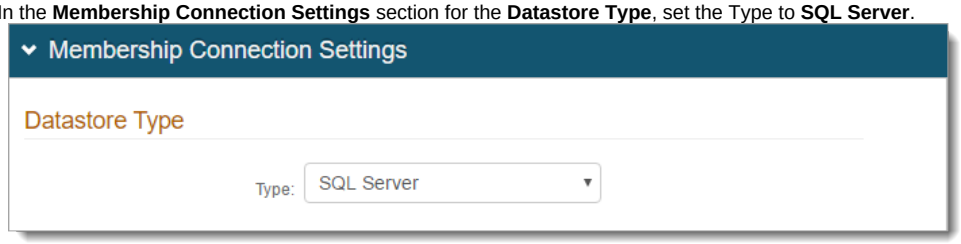
If connecting SecureAuth IdP to SQL Server User Data Store using Windows Authentication, see the SecureAuth SQL Server Windows ID Implementation PDF.

Prerequisites

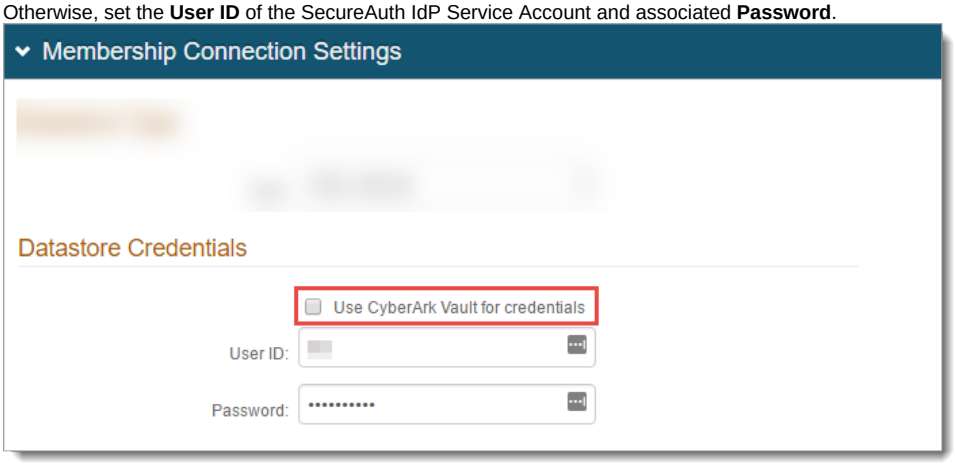
- SecureAuth IdP version 9.1 and later
- On-premises SQL Server data store
- A service account with read access (and optional write access) designated for use by SecureAuth IdP

SQL Server configuration steps

1. In the SecureAuth IdP Web Admin, select the **Data** tab.
2. In the **Membership Connection Settings** section for the **Datastore Type**, set the Type to **SQL Server**.



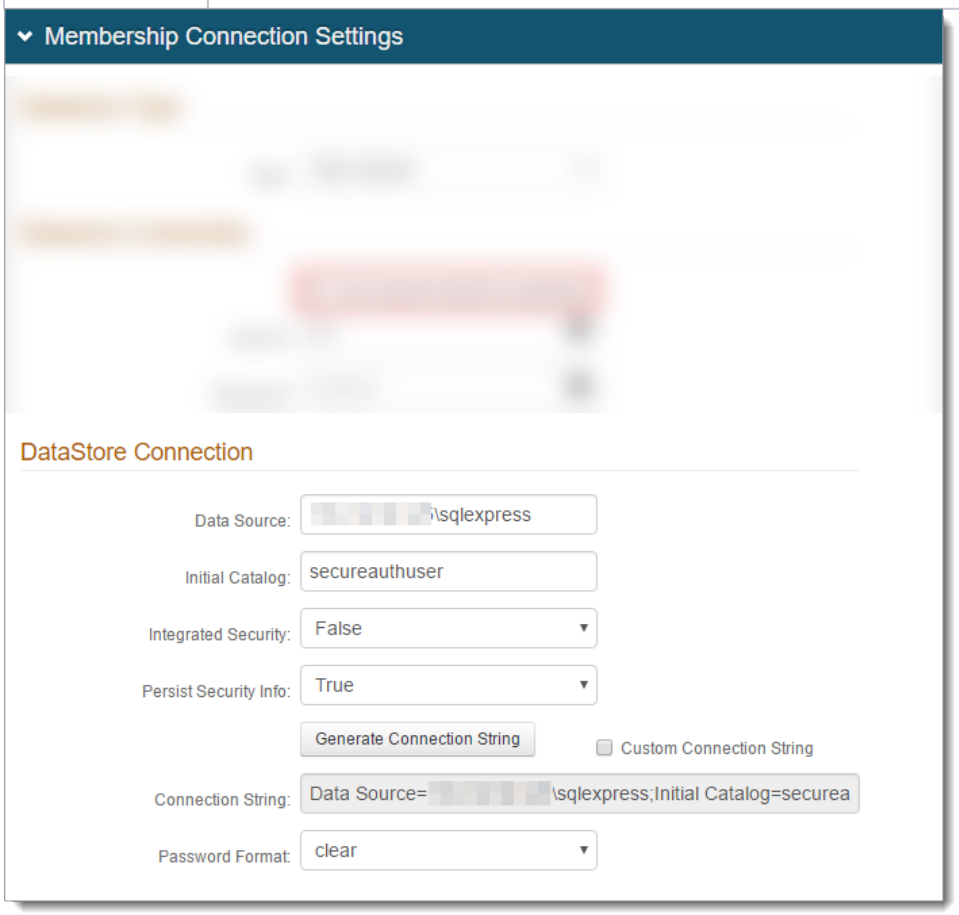
3. In the **Datastore Credentials** section, do one of the following:
   - To use **CyberArk Vault for credentials**, select this check box. Follow the steps in CyberArk Password Vault Server and AIM Integration with SecureAuth IdP.
   - Otherwise, set the **User ID** of the SecureAuth IdP Service Account and associated **Password**.



4. In the **Datastore Connection** section, set the following:

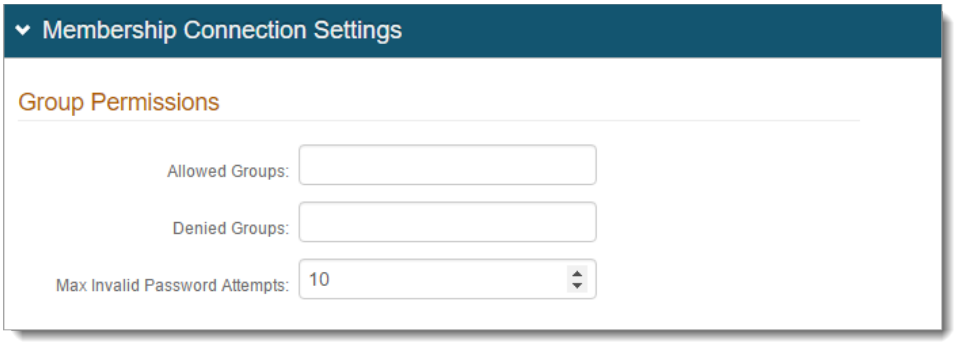
Data Source	Set to the **Fully Qualified Domain Name (FQDN)** or the **IP Address**.
Initial Catalog	Set to the database name.

Integrated Security	Set to one of the following: • **True** – Use the IIS app pool service account in the connection (see **Integrated Auth Requirements** below) Integrated Auth Requirements 1. Join the server to the domain to utilize a domain service account. 2. In IIS, set the application pool **Identity** for both the **.NET v4.5** and **SecureAuth0** app pools to use the preferred service account; and set **Load User Profile** to **True.** 3. Make the service account a member of the local administrators group of the SecureAuth IdP server(s). 4. Perform an **IIS reset** after making the changes. • **False** – Use a SQL service account
Persist Security Info	To allow access to the username and password information, set to **True**.
Generate Connection String	Click **Generate Connection String** and it autopopulates the **Connection String** field.
Password Format	Indicate how the service account password is stored in the directory.



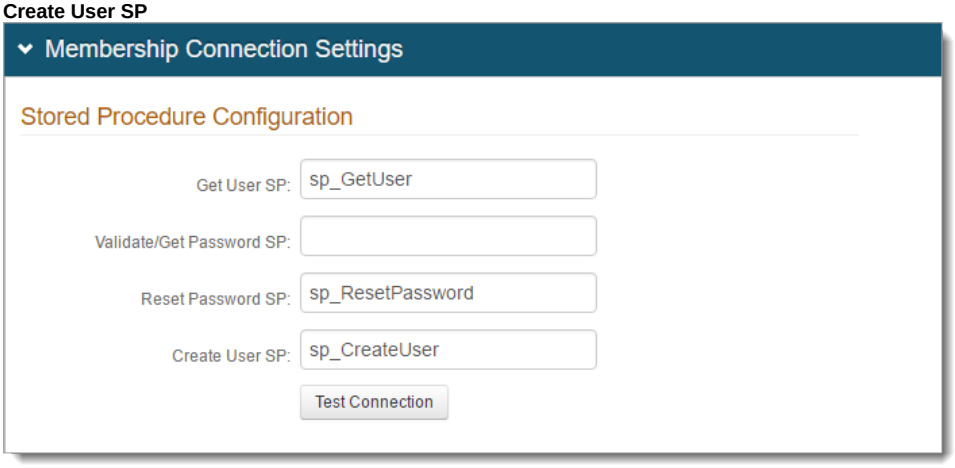
5. In the **Group Permissions** section, set the following:

Allowed Groups	Create a list of groups allowed access to the target resource of this realm. For example, **Admins**.
Denied Groups	Create a list of groups not allowed access to the target resource of this realm.
Max Invalid Password Attempts	Set the maximum number of password attempts before the user account is locked.



6. In the **Stored Procedure Configuration** section, provide the stored procedure names for the following fields:

    - **Get User SP**
    - **Validate/Get Password SP**
    - **Reset Password SP**
    - **Create User SP**

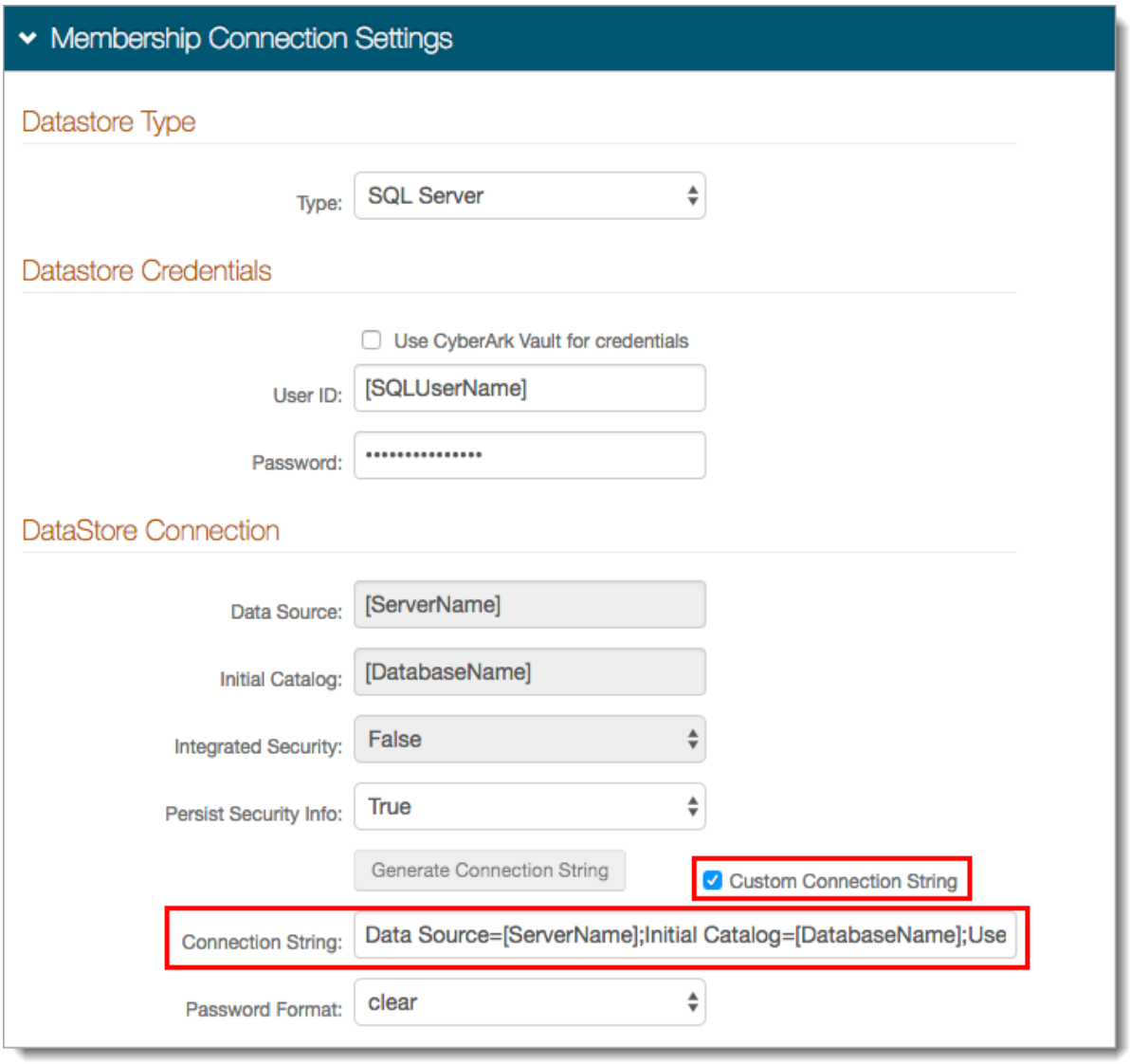
    

    For more stored procedures configuration information, see SQL User Data Store Tables and Stored Procedures Configuration Guide.
7. To test the connection, click **Test Connection**.
   If using a **Custom Connection String** and experience an error when testing the connection, see the **Custom Connection String Error** section for a workaround.

Custom Connection String Error

When a custom connection string is manually entered, an error might occur when testing the connection. This can prevent the SQL server from successfully integrating with SecureAuth IdP.

This error can occur when the **Custom Connection String** check box selected and the **Connection String** is manually entered into the field instead of being generated by the Web Admin.

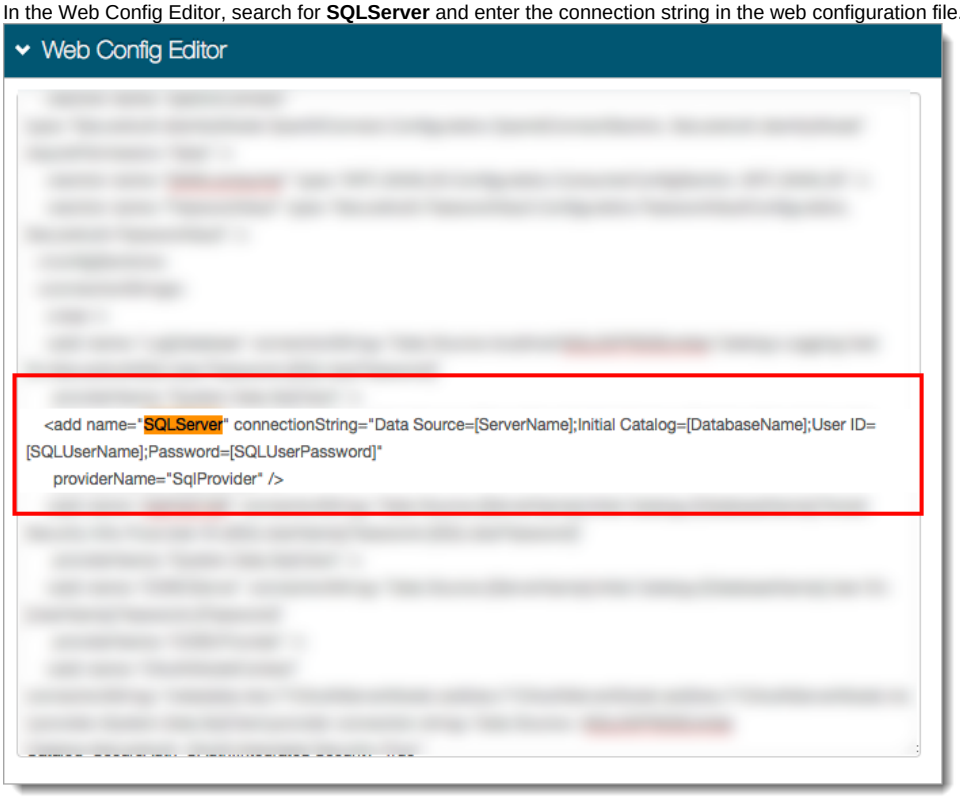


Workaround

See the following steps for a workaround to this issue.

1. Go to the **System Info** tab.
2. In the **Links** section, click the **Click to edit Web Config file** link.

3. In the Web Config Editor, search for **SQLServer** and enter the connection string in the web configuration file.



4. **Save** your changes.
   This enables a successful connection; however clicking **Test Connection** in the **Data** tab might still yield an error.