

ODBC as Additional Profile Provider Configuration Guide

Introduction

Use this guide along with the [Data Tab Configuration](#) guide to configure a SecureAuth IdP realm that uses ODBC as an additional Profile Provider.

Prerequisites

1. Have an on-premises **ODBC** data store
2. A service account with read access (and optional write access) for SecureAuth IdP

ODBC Configuration Steps

▼ Profile Provider Settings

Same As Above:

Default Profile Provider:

1. In the **Profile Provider Settings** section, select **True** from the **Same as Above** dropdown to copy the data store integration from the **Membership Connection Settings** section for use in profile connection; or select **False** if that directory is only used for the membership connection.
2. Select **ODBC** from the **Default Profile Provider** dropdown if ODBC is to be used as the default profile provider



- If another **ODBC** data store is configured in the **Membership Connection Settings** section, and **True** is selected from the **Same as Above** dropdown, then those settings appear in the **Profile Connection Settings** (below) and must be modified to reflect the settings of the new ODBC data store
- Only one **ODBC** can be utilized for profile connection
- If another directory is selected from the **Default Profile Provider** dropdown, then **ODBC** must be selected from **Source** dropdown in the **Profile Fields** section for the SecureAuth IdP **Properties** that are mapped to ODBC fields

Profile Connection Settings

▼ Profile Connection Settings

Data Store: ODBC

Data Source: FQDN

Initial Catalog: DatabaseName

Integrated Security: False

Persist Security Info: True

Username: Username

Password: Show Password

Custom Connection String

Connection String: Data Source=FQDN;Initial Catalo

Get Profile SP: FIELD

Update Profile SP: FIELD

3. Select **ODBC** from the **Data Store** dropdown
4. Provide the **Fully Qualified Domain Name (FQDN)** or the **IP Address** in the **Data Source** field
5. Provide the **Database Name** in the **Initial Catalog** field
6. Select **True** from the **Integrated Security** dropdown if the IIS app pool's service account is to be used in the connection
Select **False** to specify an ODBC service account instead
7. Select **True** from the **Persist Security Info** dropdown if access to the username and password information is allowed
8. Provide the **User ID** of the SecureAuth IdP Service Account (if **False** is selected in step 6)
9. Provide the **Password** associated to the **User ID** (if **False** is selected in step 6)
10. Click **Generate Connection String**, and the **Connection String** will auto-populate
11. Create a list of **Allowed Groups** that can access the target resource of this realm
12. Provide the **Stored Procedure Name** for **Get Profile SP**
13. Provide the **Stored Procedure Name** for **Update Profile SP**
14. Click **Test Connection** to ensure that the connection is successful



Refer to [Data Tab Configuration](#) to complete the configuration steps in the **Data** tab of the Web Admin