Data Tab Configuration

Introduction

Use this guide to configure the Data tab in the Web Admin for each SecureAuth IdP realm.

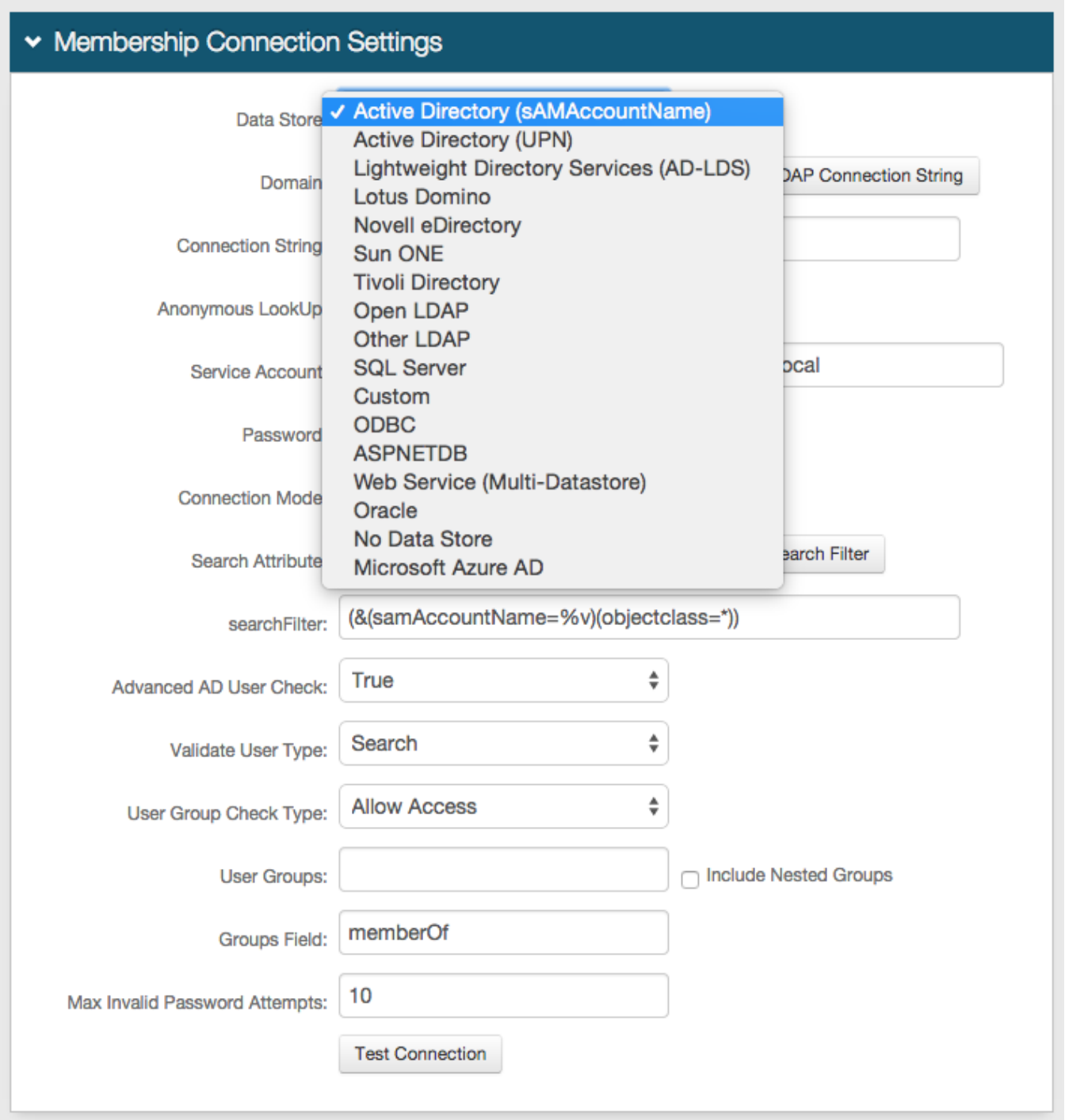
This includes directory integration and user profile field mapping.

Prerequisites

- An on-premises directory must be established and ready to integrate with SecureAuth IdP
- A Service Account must be created for SecureAuth IdP with read privileges to access the data store, and write privileges (optional) to update user information
- Create a **New Realm** for the target resource for which the configuration settings will apply, or open an *existing realm* for which configurations have already been started
- Configure the **Overview** tab in the Web Admin before configuring the **Data** tab

Data Configuration Steps

Version 9.0.0



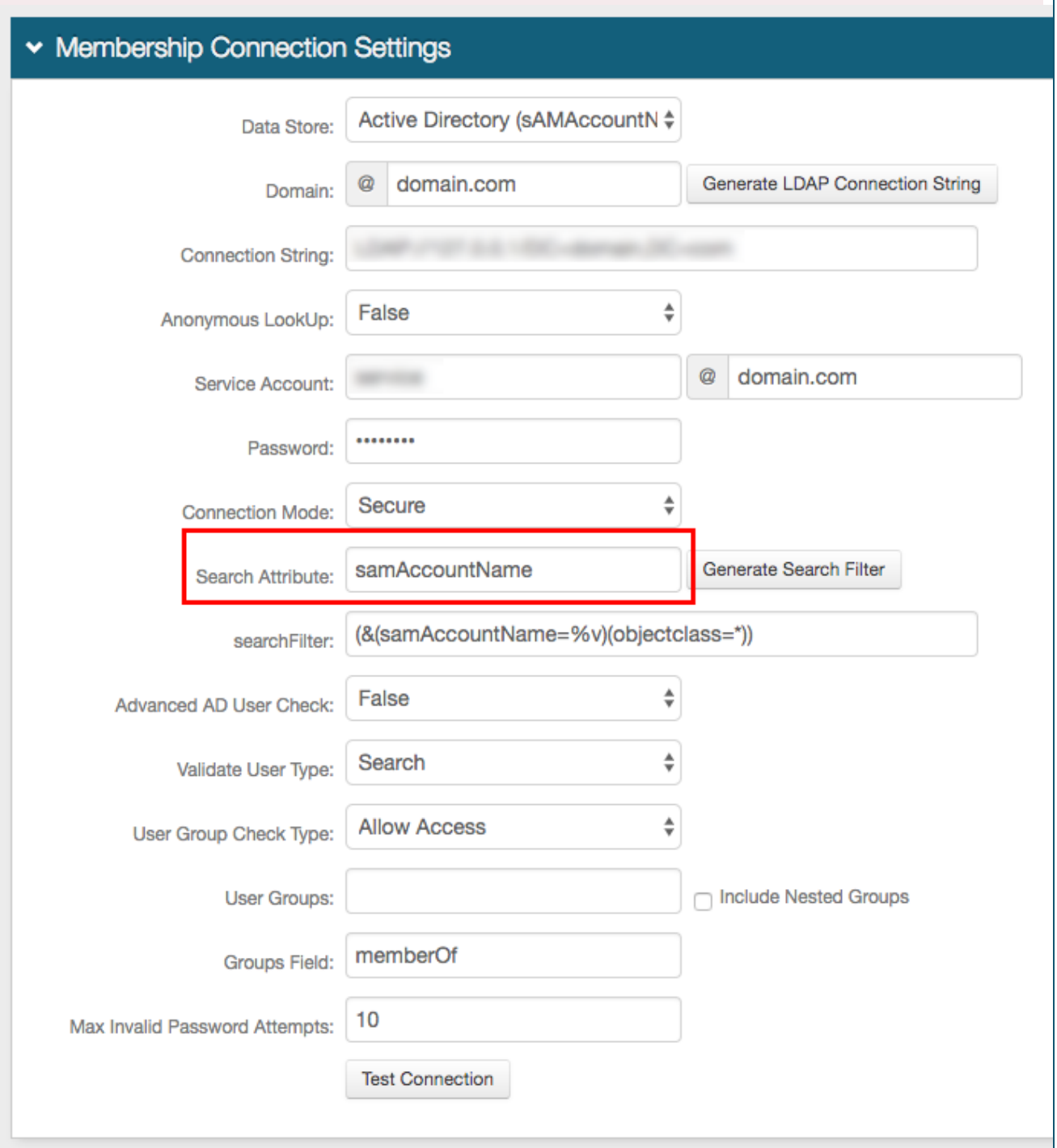
1. In the **Membership Connection Settings** section, select the directory with which SecureAuth IdP will integrate for Multi-Factor Authentication and assertion from the **Data Store** dropdown

2. Follow the distinct configuration steps for the specific data store in addition to the configuration steps on this page

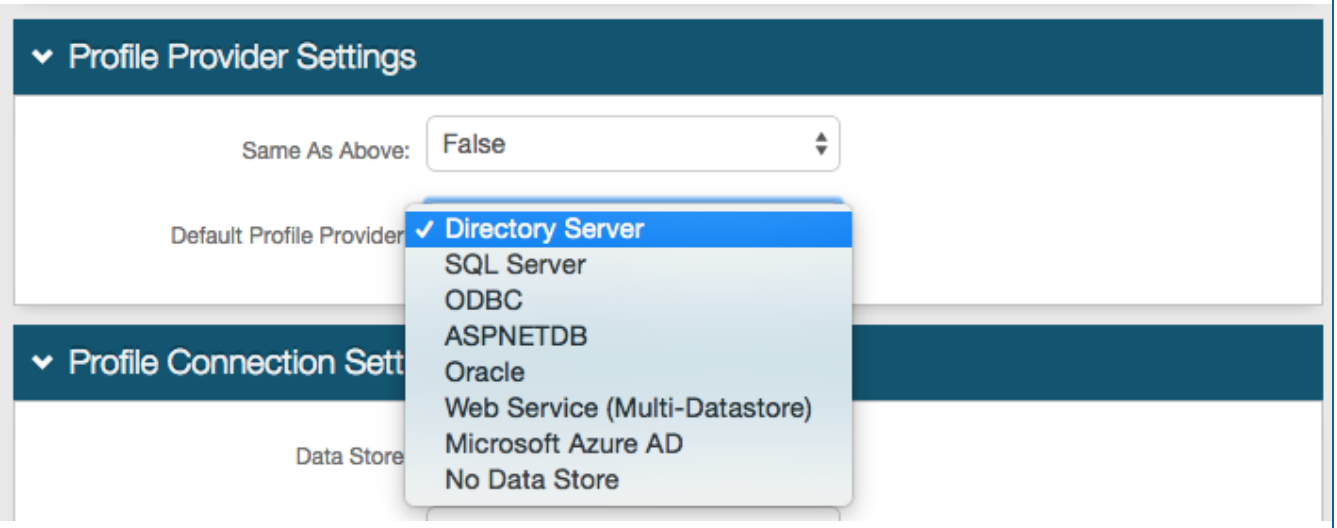
- **Active Directory (sAMAccountName)**
- **Active Directory (UPN)**
- **Lightweight Directory Services (AD-LDS)**
- **Lotus Domino**
- **Novell eDirectory**
- **Sun ONE**
- **Tivoli Directory**
- **Open LDAP**
- **Other LDAP**
- **SQL Server**
- **Custom** – for directories not listed. This would require custom coding – contact SecureAuth for configuration steps / requirements
- **ODBC**
- **ASPNETDB**
- **Web Service (Multi-Datastore)**
- **Oracle**
- **WebAdmin** (*for SecureAuth0 Admin Realm only*)
- **Microsoft Azure AD**

For **Active Directory** and other **LDAP** data stores, note the **Search Attribute** directory field value, e.g. sAMAccountName.

To use OATH OTPs for Multi-Factor Authentication, the **Search Attribute** directory field *must be* the *same* in the **OATH Provisioning Realm** and *all realms* using OATH OTPs for Multi-Factor Authentication.



Profile Provider Settings

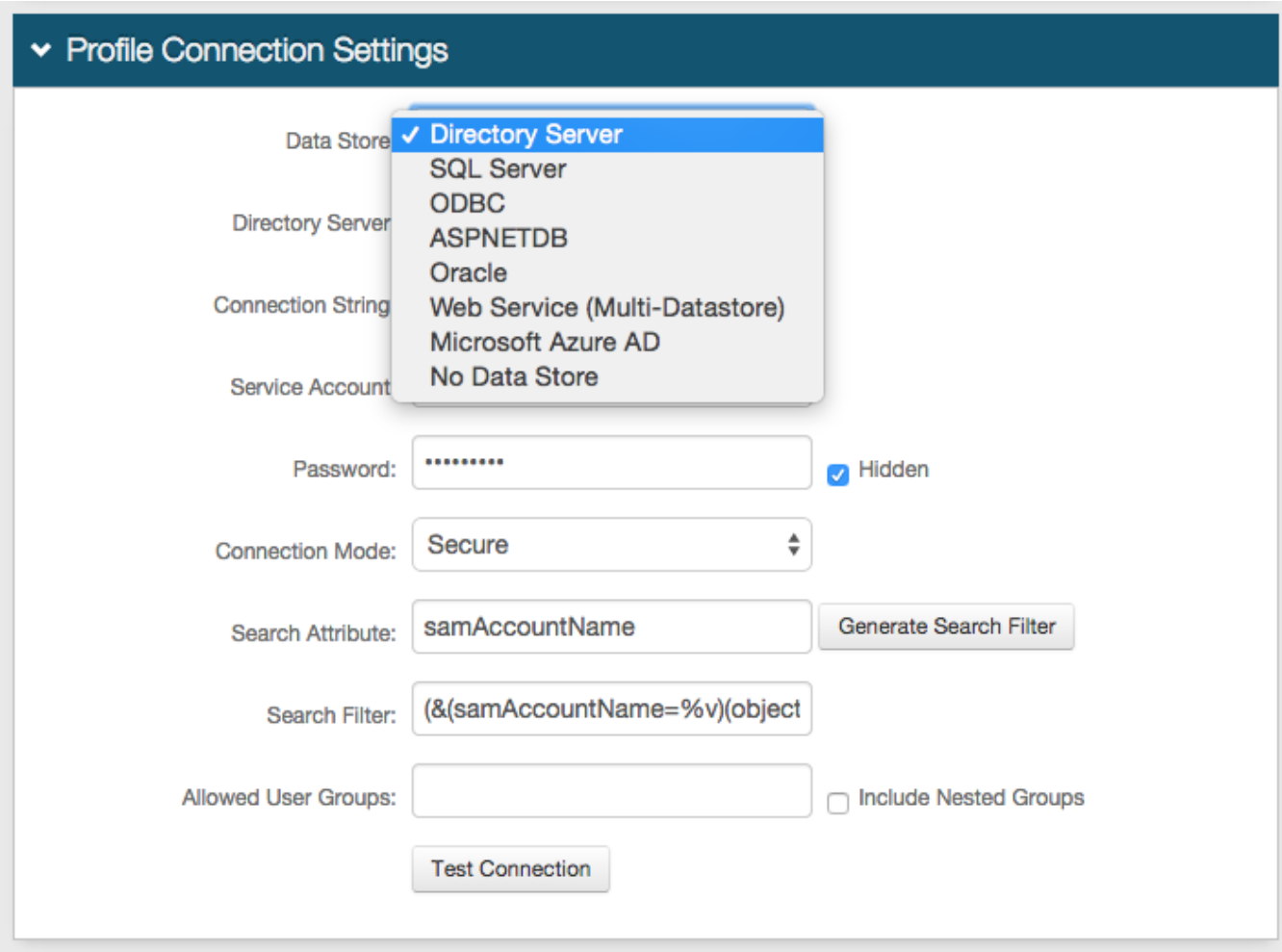


3. Select **True** from the **Same As Above** dropdown if the profile fields used for authentication (telephone number, email address, knowledge-based questions) are all contained in the data stored selected in step 1

Select **False** if a different data store will be used to contain the profile fields, and select the data store type from the **Default Profile Provider** dropdown

Profile Connection Settings

No configuration is required in this section if **True** is selected from the **Same As Above** dropdown (step 3)



4. If **False** is selected from the **Same As Above** dropdown (step 3), select the data store type from the **Data Store** dropdown; this selection will appear in the **Default Profile Provider** dropdown from which user profile information will be pulled (e.g. **Directory Server**)

5. Follow the distinct configuration steps for the specific data store in addition to the configuration steps on this page

- **Active Directory (sAMAccountName)**
- **Active Directory (UPN)**
- **Lightweight Directory Services (AD-LDS)**
- **Lotus Domino**
- **Novell eDirectory**
- **Sun ONE**
- **Tivoli Directory**
- **Open LDAP**
- **Other LDAP**
- **SQL Server**
- **ODBC**
- **ASPNETDB**
- **Web Service (Multi-Datastore)**
- **Oracle**
- **Microsoft Azure AD**

Version 9.0.1+

Membership Connection Settings

Datastore Type

Type: Active Directory (sAMAccoun

- Active Directory (sAMAccountName)
- Active Directory (UPN)
- Lightweight Directory Services (AD-LDS)
- Lotus Domino
- Novell eDirectory
- Sun ONE
- Tivoli Directory
- Open LDAP
- Other LDAP
- SQL Server
- Custom
- ODBC
- ASPNETDB
- Web Service (Multi-Datastore)
- Microsoft Azure AD
- Oracle
- No Data Store

Datastore Connection

Domain:

ate LDAP Connection String

Connection String:

Anonymous LookUp:

Connection Mode:

Datastore Credentials

Service Account: @

Password: ••••••••••

Search Filter

Search Attribute: samAccountName

Generate Search Filter

searchFilter: (&(samAccountName=%v)(objectclass=*))

Group Permissions

Advanced AD User Check: True

Validate User Type: Search

User Group Check Type: Allow Access

User Groups:

Include Nested Groups

Groups Field: memberOf

Max Invalid Password Attempts: 10

Datastore Type

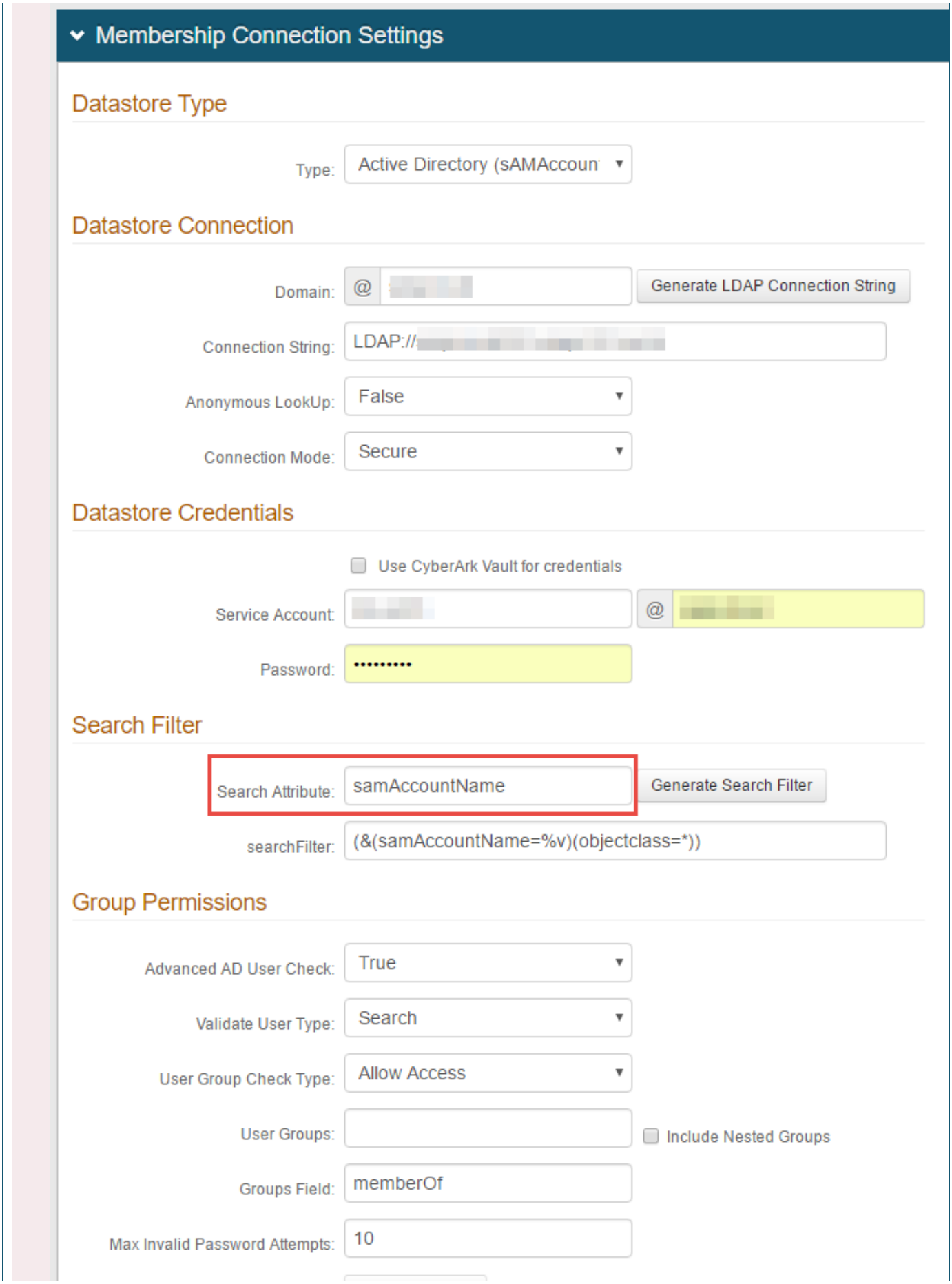
1. Select the directory with which SecureAuth IdP will integrate for Multi-Factor Authentication and assertion from the **Type** dropdown

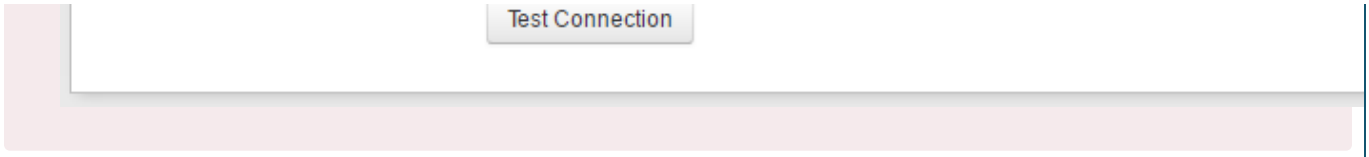
2. Follow the distinct configuration steps for the specific data store in addition to the configuration steps on this page

- **Active Directory (sAMAccountName)**
- **Active Directory (UPN)**
- **Lightweight Directory Services (AD-LDS)**
- **Lotus Domino**
- **Novell eDirectory**
- **Sun ONE**
- **Tivoli Directory**
- **Open LDAP**
- **Other LDAP**
- **SQL Server**
- **Custom** – for directories not listed. This would require custom coding – contact SecureAuth for configuration steps / requirements
- **ODBC**
- **ASPNETDB**
- **Web Service (Multi-Datastore)**
- **Microsoft Azure AD**
- **Oracle**
- **WebAdmin** (*for SecureAuth0 Admin Realm only*)

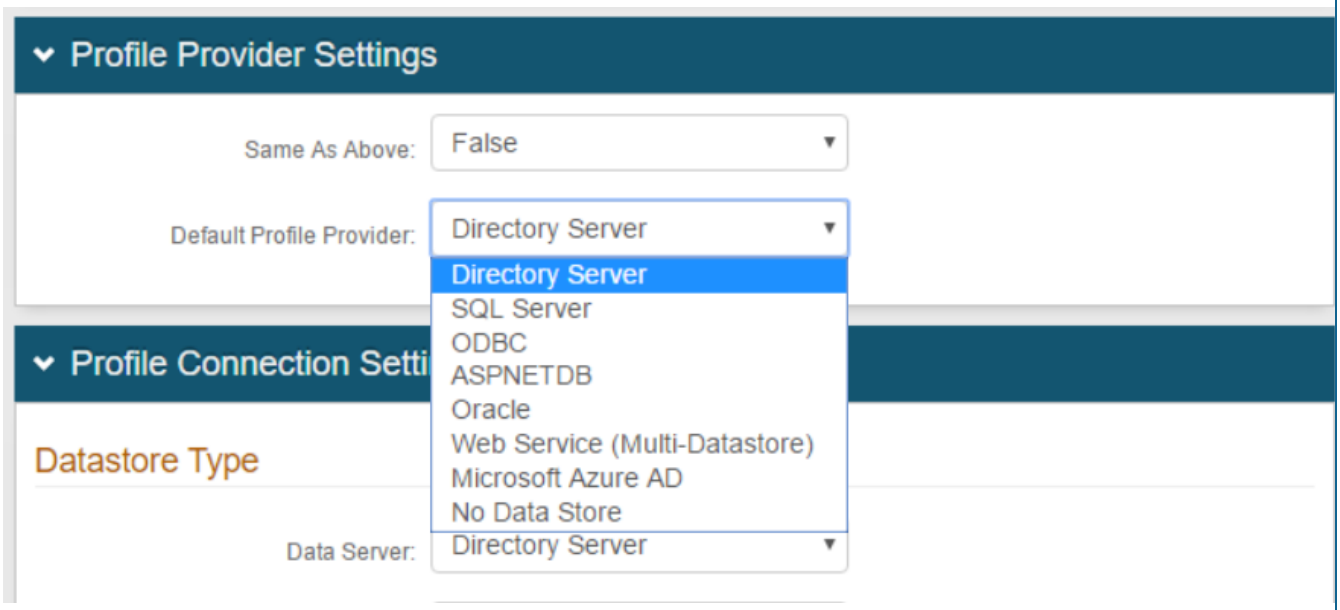
For **Active Directory** and other **LDAP** data stores, note the **Search Attribute** directory field value, e.g. sAMAccountName.

To use OATH OTPs for Multi-Factor Authentication, the **Search Attribute** directory field *must be* the *same* in the **OATH Provisioning Realm** and *all realms* using OATH OTPs for Multi-Factor Authentication.


Membership Connection Settings
Datastore Type
Type:
Active Directory (sAMAccoun
Datastore Connection
Domain:
@
Generate LDAP Connection String
Connection String:
LDAP://
Anonymous LookUp:
False
Connection Mode:
Secure
Datastore Credentials
Use CyberArk Vault for credentials
Service Account:
@
Password:
Search Filter
Search Attribute:
samAccountName
Generate Search Filter
searchFilter:
(&(samAccountName=%v)(objectclass=*))
Group Permissions
Advanced AD User Check:
True
Validate User Type:
Search
User Group Check Type:
Allow Access
User Groups:
Include Nested Groups
Groups Field:
memberOf
Max Invalid Password Attempts:
10



Profile Provider Settings

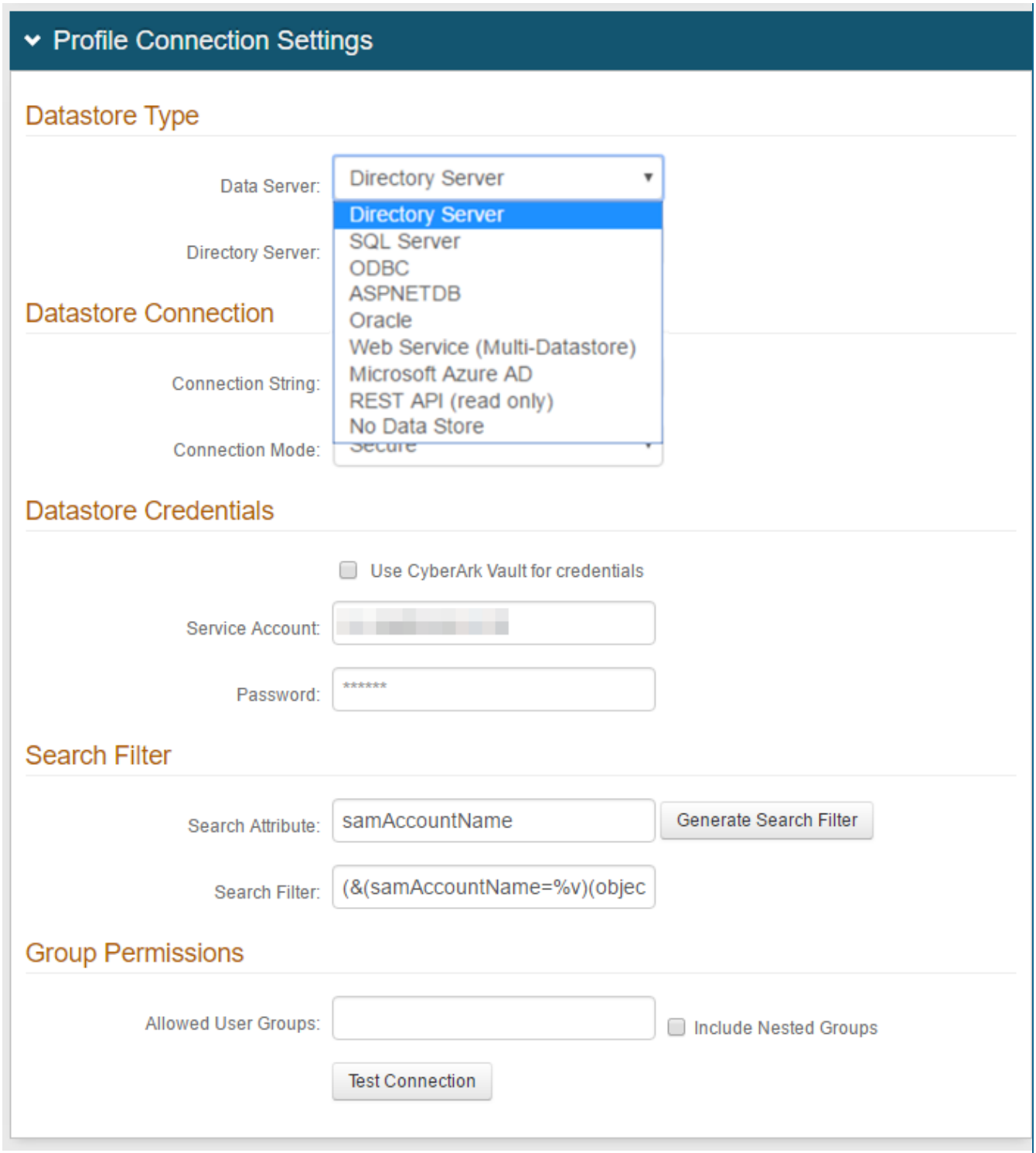


3. Select **True** from the **Same As Above** dropdown if the profile fields used for authentication (telephone number, email address, knowledge-based questions) are all contained in the data stored selected in step 1

Select **False** if a different data store will be used to contain the profile fields, and select the data store type from the **Default Profile Provider** dropdown

Profile Connection Settings

No configuration is required in this section if **True** is selected from the **Same As Above** dropdown (step 3)


Profile Connection Settings
Datastore Type
Data Server:
Directory Server
Directory Server:
Directory Server
SQL Server
ODBC
ASPNETDB
Oracle
Web Service (Multi-Datastore)
Microsoft Azure AD
REST API (read only)
No Data Store
Datastore Connection
Connection String:
Connection Mode:
Datastore Credentials
Use CyberArk Vault for credentials
Service Account:
Password:
******
Search Filter
Search Attribute:
samAccountName
Generate Search Filter
Search Filter:
(&(samAccountName=%v)(objec
Group Permissions
Allowed User Groups:
Include Nested Groups
Test Connection

Datastore Type

4. If **False** is selected from the **Same As Above** dropdown (step 3), select the data store type from the **Data Server** dropdown; this selection will appear in the **Default Profile Provider** dropdown from which user profile information will be pulled (e.g. **Directory Server**)

5. Follow the distinct configuration steps for the specific data store in addition to the configuration steps on this page

- **Active Directory (sAMAccountName)**
- **Active Directory (UPN)**
- **Lightweight Directory Services (AD-LDS)**
- **Lotus Domino**
- **Novell eDirectory**
- **Sun ONE**
- **Tivoli Directory**
- **Open LDAP**
- **Other LDAP**
- **SQL Server**
- **ODBC**
- **ASPNETDB**
- **Web Service (Multi-Datastore)**
- **Oracle**
- **Microsoft Azure AD**
- **REST API (read only)**

Profile Fields

Profile Fields

Property	Source	Field	Data Format	Writable
Groups	Default Provider	memberOf		☐
First Name	Default Provider	givenName		☐
Last Name	Default Provider	sn		☐
Phone 1	Default Provider	telephoneNumber		☑
Phone 2	Default Provider	mobile		☑
Phone 3	Default Provider	homePhone		☑
Phone 4	Default Provider	Pager		☑
Email 1	Default Provider	mail		☑
Email 2	Default Provider	wWWHomePage		☐
Email 3	Default Provider	ipPhone		☐
Email 4	Default Provider	extensionName		☐

6. Map the SecureAuth IdP **Property** to the appropriate data store **Field**

    For example, **Groups** is located in the **memberOf** data store **Field**

7. Change the **Source** from **Default Provider** if another directory is enabled in the **Profile Connection Settings** section and contains the **Property**

8. Check **Writeable** for a **Property** that will be changed in the data store by SecureAuth IdP

    For example, user account information (telephone number) or authentication mechanisms (knowledge-based questions, fingerprints)

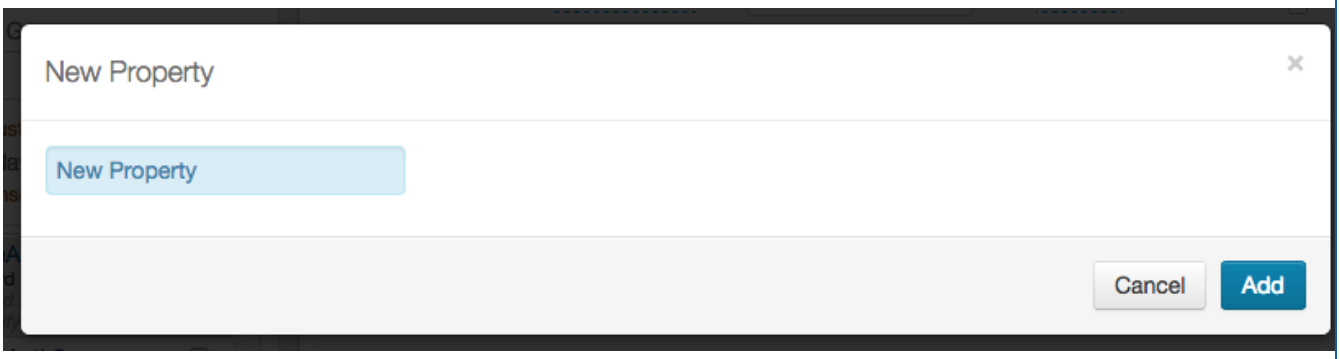
The **Data Format** section states how the information is stored in the directory (not available for all **Profile Properties**):

- **Plain Text**: Stored as regular text, readable (default)
- **Standard Encryption**: Stored and encrypted using RSA encryption
- **Advanced Encryption**: Stored and encrypted using AES encryption
- **Standard Hash**: Stored and encrypted using SHA 256 hash
- **Plain Binary**: Stored as a binary representation of the data (uses a .NET library to make it binary – may not be readable by all applications)
- **JSON**: Stored in a universal format, readable by all applications (similar to Plain Text)
- **Encrypted JSON**: Stored as JSON, with values inside encrypted using AES encryption

If using a SQL directory, then **JSON** or **Encrypted JSON** is not supported

For the **Fingerprints**, **Push Notification Tokens**, **OATH Tokens**, and **Access Histories** Properties, only **Plain Binary** can be utilized as the **Data Format**

The **Fields** listed are only *examples* as each data store is organized differently and may have different values for each **Property**



9. Click **Add Property** if a required **Property** is not listed

10. **Enter property name** and click **Add**

11. The new **Property** will appear at the bottom of the list and can then be mapped to the appropriate data store **Field**

Global Aux Fields

12. Add any additional identities or user information that is not stored in the on-premises data store but will be used in assertion (optional)

Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes