Web Service (Multi-Data Store) 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 Web Service (Multi-Data Store) as an additional Profile Provider.

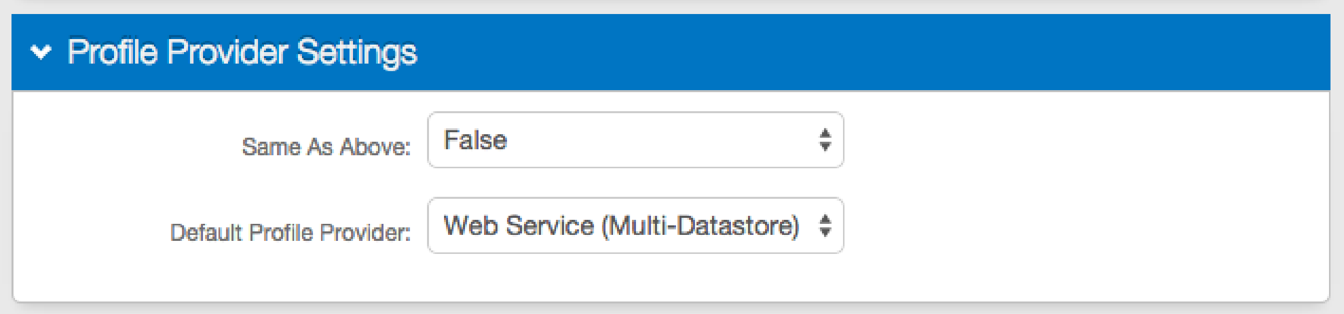
Web Service enables SecureAuth IdP to access multiple data stores to extract the appropriate user information for authentication and assertion.

Prerequisites

1. Have on-premises data stores (Active Directory, SQL Server, ODBC, etc.)

2. Service accounts with read access (and optional write access) for SecureAuth IdP for each data store

Web Service (Multi-Data Store) Configuration Steps



Profile Provider Settings

Same As Above: False

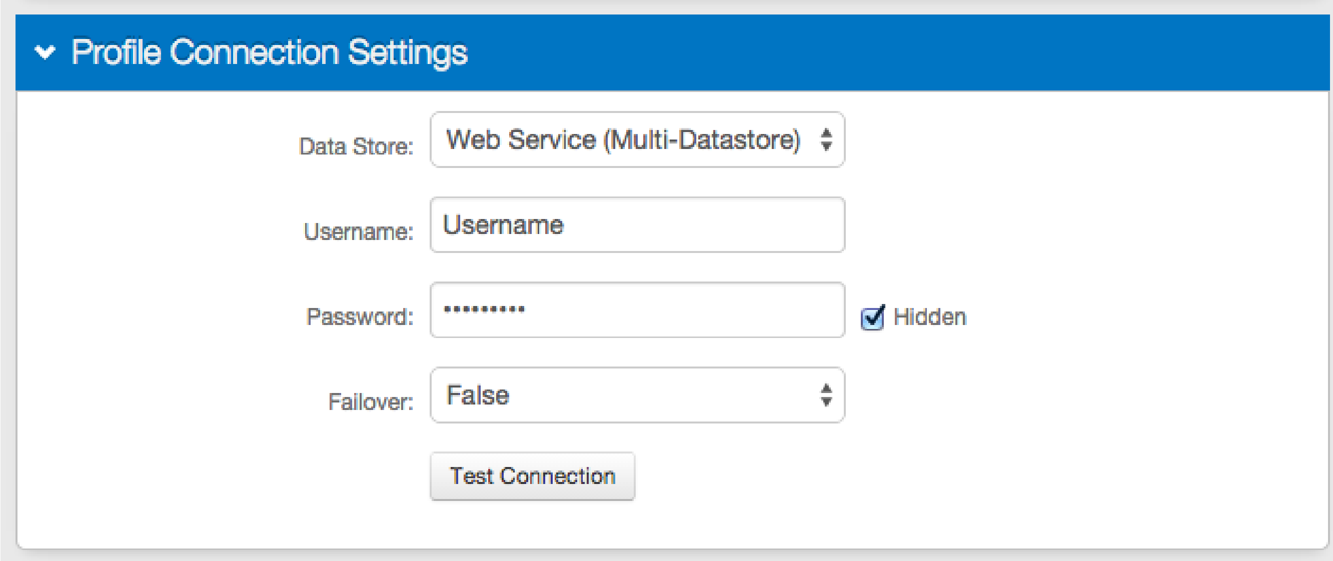
Default Profile Provider: Web Service (Multi-Datastore)

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 **Web Service (Multi-Datastore)** from the **Default Profile Provider** dropdown if Web Service is to be used as the default profile provider

- If another **Web Service** 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 Web Service configuration
- Only one **Web Service** configuration can be utilized for profile connection
- If another directory is selected from the **Default Profile Provider** dropdown, then **Web Service** must be selected from **Source** dropdown in the **Profile Fields** section for the SecureAuth IdP **Properties** that are mapped to Web Service configuration fields

Profile Connection Settings



Profile Connection Settings

Data Store: Web Service (Multi-Datastore)

Username: Username

Password: •••••••••• ☑ Hidden

Failover: False

3. Select **Web Service (Multi-Datastore)** from the **Data Store** dropdown

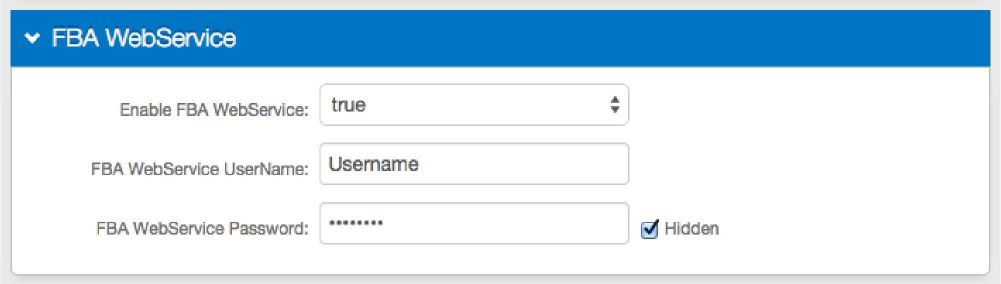
4. Set the **Webservice Username**

    It is recommended that this be changed from the default to ensure security

5. Set the **Webservice Password**

    It is recommended that this be changed from the default to ensure security

ⓘ



FBA WebService

Enable FBA WebService: true

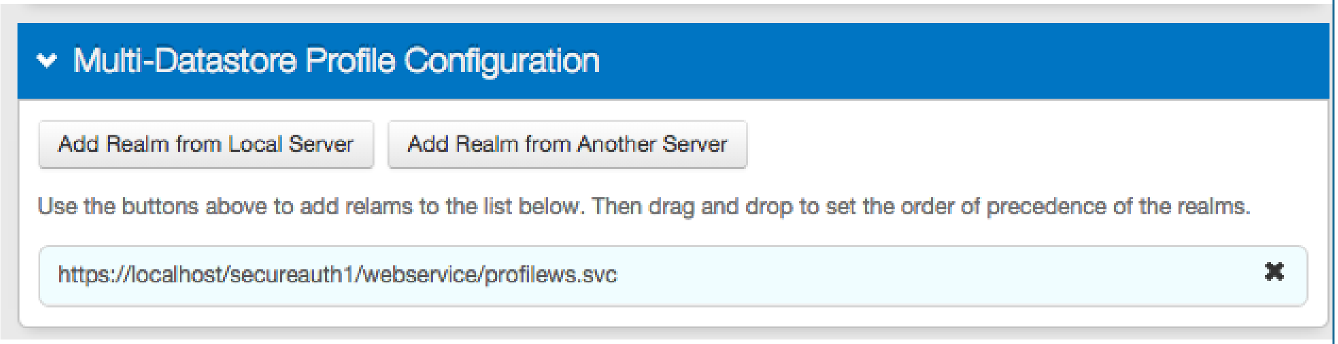
FBA WebService UserName: Username

FBA WebService Password: •••••••• ☑ Hidden

6. Select **True** from the **Failover** dropdown if SecureAuth IdP is to respond in the event of a failure

7. Click **Test Connection** to ensure that the connection is successful

Multi-Datastore Profile Configuration


Multi-Datastore Profile Configuration
Add Realm from Local Server
Add Realm from Another Server

Use the buttons above to add relams to the list below. Then drag and drop to set the order of precedence of the realms.

https://localhost/secureauth1/webservice/profilews.svc

8. Click **Add Realm from Local Server** to use the **Profile Connection Settings** data store integration information from a realm on the same SecureAuth IdP appliance

Click **Add Realm from Another Server** to use the data store integration information from a realm on a different SecureAuth IdP appliance

9. Select the realms in which the necessary **Profile Connection Settings** data store integration is configured to be used for this realm's workflow, and click **Add**

10. Once realms are added, **drag and drop** the realms to create the order in which SecureAuth IdP will check for user information

ⓘ Refer to **Data Tab Configuration** to complete the configuration steps in the **Data** tab of the Web Admin