Active Directory (UPN) as Additional Profile Provider Configuration Guide

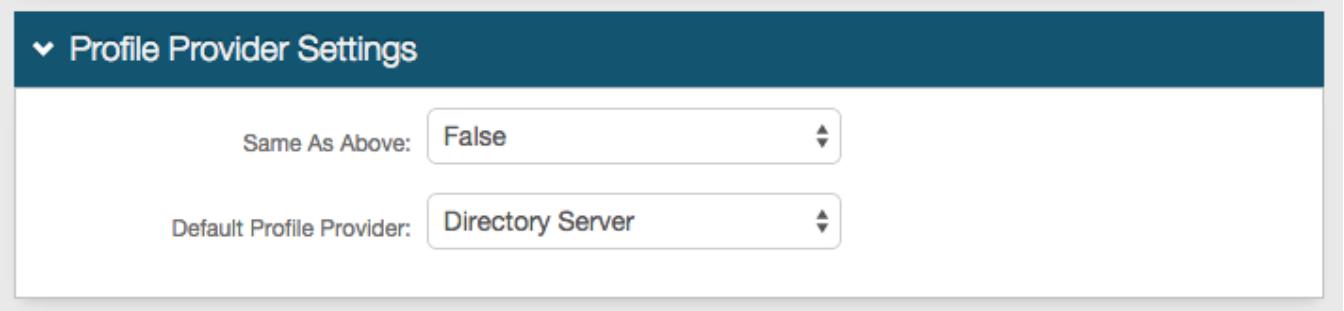
Introduction

Use this guide along with the **Data Tab Configuration** guide to configure a SecureAuth IdP realm that uses Active Directory (UPN) as an additional Profile Provider.

Prerequisites

- An on-premises **Active Directory** data store
- A service account with read access (and optional write access) for SecureAuth IdP

Active Directory (UPN) Configuration Steps

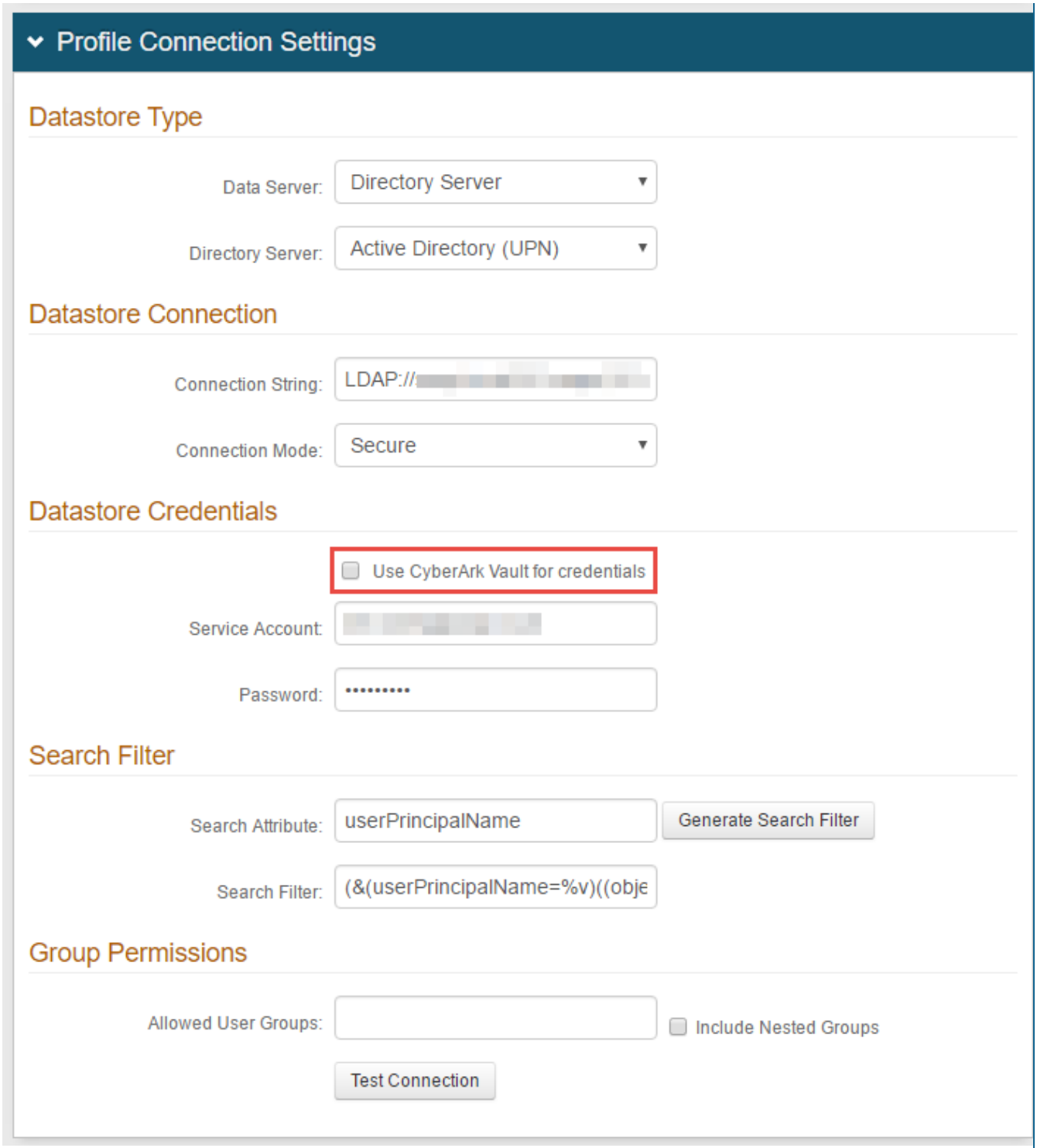


1. In the **Profile Provider Settings** section, select **True** from the **Same as Above** dropdown to copy the data store integration from the **Membership Connection Settings** section for use in profile connection; or select **False** if that directory is only used for the membership connection

2. Select **Directory Server** from the **Default Profile Provider** dropdown if Active Directory (UPN) is to be used as the default profile provider

- If another **Directory Server** data store (LDAP, AD, others) 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 Active Directory (UPN) data store
- Only one **Directory Server** can be utilized for profile connection
- If another directory is selected from the **Default Profile Provider** dropdown, then **Directory Server** must be selected from **Source** d ropdown in the **Profile Fields** section for the SecureAuth IdP **Properties** that are mapped to Active Directory (UPN) fields

Profile Connection Settings


Profile Connection Settings
Datastore Type
Data Server:
Directory Server
Directory Server:
Active Directory (UPN)
Datastore Connection
Connection String:
LDAP://
Connection Mode:
Secure
Datastore Credentials
Use CyberArk Vault for credentials
Service Account:
Password:
Search Filter
Search Attribute:
userPrincipalName
Generate Search Filter
Search Filter:
(&(userPrincipalName=%v)((obje
Group Permissions
Allowed User Groups:
Include Nested Groups
Test Connection

Datastore Type

3. Select **Directory Server** from the **Data Server** dropdown

4. Select **Active Directory (UPN)** from the **Directory Server** dropdown

Datastore Connection

5. Set the **Connection String** using the directory domain, e.g. **LDAP: <directory>.<domain>/DC=<directory>,DC=<domain>**

6. Select **Secure** from the **Connection Mode** dropdown

Datastore Credentials

If using CyberArk Vault for credentials, enable **Use CyberArk Vault for credentials** and follow the steps in **CyberArk Password Vault Server and AIM Integration with SecureAuth IdP**

With this feature, steps 7 and 8 are not required

7. Provide the SecureAuth IdP **Service Account** username, and it will be @ the directory domain

8. Provide the **Password** that is associated with the **Service Account** username

Search Filter

9. Provide the **Search Attribute** to be used to search for the user's account in the directory, e.g. **userPrincipalName**

10. Click **Generate Search Filter**, and the **Search Filter** will auto-populate

The value that equals **%v** is what the end-user will provide on the login page, so if it is different from the **Search Attribute**, change it here

For example, if the **Search Attribute** is **userPrincipalName**, but end-users will log in with their email addresses (field= **mail**), the **Search Filter** would be **(&(mail=%v)((objectclass=user)(objectcategory=person)))**

Group Permissions

11. Provide the **Allowed User Groups** for this realm

Leave this field blank if there is no access restriction

12. Check **Include Nested Groups** if the subgroups from the listed **User Groups** are to be allowed access as well

13. Click **Test Connection** to ensure that the integration is successful

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

Refer to **LDAP Attributes / SecureAuth IdP Profile Properties Data Mapping** for information on the **Profile Properties** section