

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

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

Active Directory (UPN) 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 **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** dropdown in the **Profile Fields** section for the SecureAuth IdP **Properties** that are mapped to Active Directory (UPN) fields

▼ Profile Connection Settings

Data Store:

Directory Server:

Connection String:

Service Account:

Password: Hidden

Connection Mode:

Search Attribute:

Search Filter:

Allowed User Groups: Include Nested Groups

3. Select **Directory Server** from the **Data Store** dropdown
4. Select **Active Directory (UPN)** from the **Directory Server** dropdown
5. Set the **Connection String** using the directory domain, e.g. `LDAP:<directory>.<domain>/DC=<directory>,DC=<domain>`
6. Provide the **Username** of the SecureAuth IdP **Service Account**
7. Provide the **Password** associated with the **Username**
8. Provide the **Search Attribute** to be used to search for the user's account in the directory, e.g. `userPrincipalName`
9. Click **Generate Search Filter**, and the `searchFilter` 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 `searchFilter` would be `(&(mail=%v)((objectclass=user)(objectcategory=person)))`
10. Provide the **Allowed User Groups** for this realm

Leave this field blank if there is no access restriction
11. Check **Include Nested Groups** if the subgroups from the listed **User Groups** are to be allowed access as well
12. 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