

Tivoli Directory Configuration Guide

Introduction

Use this guide along with the [Data Tab Configuration](#) guide to configure a Tivoli Directory-integrated SecureAuth IdP realm.

Prerequisites

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

Tivoli Directory Configuration Steps

Membership Connection Settings

| | |
|--|--|
| Data Store: | <input type="text" value="Tivoli Directory"/> |
| Domain: | <input type="text" value="@ directory.domain"/> <input type="button" value="Generate LDAP Connection String"/> |
| Connection String: | <input type="text" value="LDAP://directory.domain/DC=directory,DC=domain"/> |
| Anonymous LookUp: | <input type="text" value="False"/> |
| Service Account: | <input type="text" value="Username"/> <input type="text" value="@ directory.domain"/> |
| Password: | <input type="password" value="*****"/> <input checked="" type="checkbox"/> Hidden |
| Connection Mode: | <input type="text" value="Secure"/> |
| Search Attribute: | <input type="text" value="uid"/> <input type="button" value="Generate Search Filter"/> |
| searchFilter: | <input type="text" value="(&(uid=%v)(objectclass=inetOrgPerson))"/> |
| Advanced AD User Check: | <input type="text" value="True"/> |
| Validate User Type: | <input type="text" value="Search"/> |
| User Group Check Type: | <input type="text" value="Allow Access"/> |
| User Groups: | <input type="text" value="Admins"/> <input checked="" type="checkbox"/> Include Nested Groups |
| Groups Field: | <input type="text" value="memberOf"/> |
| <input type="button" value="Test Connection"/> | |

1. In the **Membership Connection Settings**, select **Tivoli Directory** from the **Data Store** dropdown
2. Provide the **Domain** of the data store
3. Click **Generate LDAP Connection String**, and the **Connection String** will auto-populate
4. Select **True** from the **Anonymous LookUp** dropdown if the directory can be searched without supplying the username
Select **False** if the username must be supplied to search the directory
5. Provide the SecureAuth IdP **Service Account** username in the Distinguished Name (DN) format, e.g. **cn=svc-account,DC=directory,DC=domain**
6. Provide the **Password** that is associated with the **Service Account**
7. Select the type of **Connection Mode** to be used from the dropdown
8. Provide the **Search Attribute** to be used to search for the user's account in the directory, e.g. **uid**
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 **uid**, but end-users will log in with their email addresses (field=**mail**), the **searchFilter** would be **(&(mail=%v)(objectclass=inetOrgPerson))**
10. Select **Search** from the **Validate User Type** dropdown if SecureAuth IdP is to use the search function to find a username and password
Select **Bind** if SecureAuth IdP is to make a direct call to the directory to validate the username and password
11. Select **Allow Access** from the **User Group Check Type** to create a list of allowed user groups; select **Deny Access** to create a list of denied user groups
12. Provide the allowed or denied **User Groups** based on the selection in step 11, e.g. **Admins**
Leave this field blank if there is no access restriction
13. Check **Include Nested Groups** if the subgroups from the listed **User Groups** are to be allowed or denied access as well
14. Provide the **Groups Field** that contains users' groups, e.g. **memberOf**
15. 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