BEA AquaLogic® Enterprise Repository

LDAP/Active Directory Installation Guide

Version 3.0. RP1
Revised: February, 2008

LDAP/Active Directory Overview

When utilizing LDAP / Active Directory to authenticate users, some consideration must be given to the user's department and role configurations prior to the utilization of LDAP / Active Directory server. All users will be authenticated through LDAP/AD once the integration is enabled; it is essential to have at least one user created within the AquaLogic Enterprise Repository database that matches the username from LDAP/AD. This user account should also be assigned the appropriate roles ino order to that administrative functions within AquaLogic Enterprise Repository can still be performed when LDAP/AD is enabled.

If Role synchronization is enabled from LDAP, at least one user account should be assigned an administration-level role. When that user logs into AquaLogic Enterprise Repository, that person will have the ability to configure and administer the application properly.

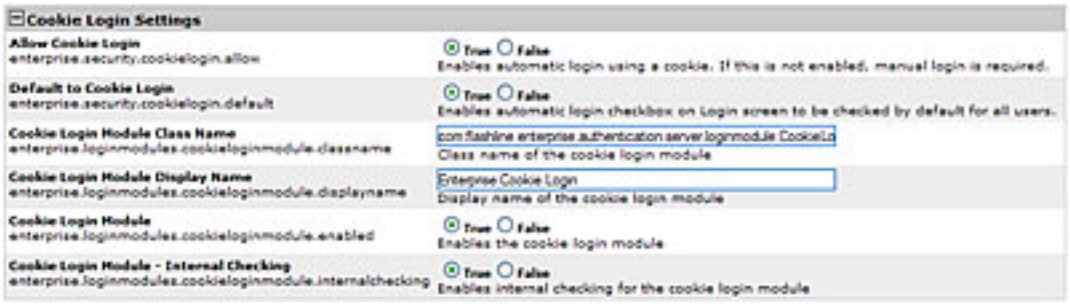
Enable LDAP Integration System Properties

This procedure is performed on the AquaLogic Enterprise Repository **Admin** screen.

1. Click **System Settings** in the left pane.

   The **System Settings** section opens in the main pane.

2. Locate the **Cookie Login Settings** group in the **Enterprise Authentication** section.



3. Make sure the **Allow Cookie Login** setting is set to **False**

4. Use the **System Settings Search** box to easily locate each of the following settings.

5. Enter **`enterprise.authentication.ldap.enabled`** into the Search box. Set the value to **True** and click Save.

Change the settings as indicated below. Pay particular attention to the **True \ False** settings for each.

- **Default to Cookie Login**
  - Set to **False**.
- **Unapproved User Login**
  - Set to **True**.
- **Cookie Login Module**
  - Set to **False**.
- **Cookie Login Module - Internal Checking**
  - Set to **False**.
- **Plug-in Login Module Class Name**
  - Enter **`com.flashline.enterprise.authentication.server.loginmodule.LDAPLogin`** in the text box.
    - **Note:** This property turns LDAP on/off. Once enabled, the application will use LDAP server for user authentication.
- **Plug-in Login Module Display Name**
  - Enter **`Enterprise LDAP Login`** in the text box.
- **Plug-in Login Module**
  - Set to **True**.
- **Plug-in Login Module - Internal Checking**
  - Set to **False**.

6. Click **Save** when finished.

Modify LDAP/Active Directory Properties

1. Click **System Settings** in the left pane.
2. Use the **System Settings Search** to easily locate each of the following settings. Enter the values as indicated below.

   Pay particular attention to the **True \ False** setting for each.

   - **LDAP Server Host Name**
     - In the text box, enter the Host name, or the directory server IP address.
   - **LDAP Server Port Number**
     - Enter **`389`** in the text box.
   - **LDAP Mask**
     - Enter **`uid\=^`** for LDAP
       or...
     - Enter **`samAccountName\=^`** for Active Directory

- **Creation of Unapproved User Accounts**
  - Set to **True**.

- **Assign default roles to users**
  - Set to **True**.
    - **Note:** This property will assign default roles on every user authentication.

- **Auto create missing roles**
  - Set to **True**.
    - **Note:** This property will create roles synchronized from the LDAP/AD server, but will **NOT** assign any permissions to those roles.

- **Auto create missing departments**
  - Set to **True**.
    - **Note:** This property will create departments synchronized from the LDAP/AD server, but will **NOT** assign any description to those departments. However, the user **WILL** be assigned to the new role.

- **LDAP Version**
  - Enter **3** in the text box. (Supported versions are 2 and 3)

- **Administrator Account Distinguished Name**
  - **Note:** This property is required with using Active Directory. This property must contain a DN of a user account with at least read-only directory look-up permissions.
    - Example: **CN=Some_User,CN=Users,DC=ad,DC=example,DC=com**

- **Administrator Account Password**
  - In the text box, enter the password for the administrator account identified in the **Administrator Account Distinguished Name** property, above.

- **Use SSL Connection**
  - Set to **True** to enable an SSL connection for LDAP. Default is false.

- **Follow referrals**
  - Set to **True**.

- **Retrieve data using the admin account**
  - Set to **False** for LDAP (if applicable) Or
  - Set to **True** for Active Directory or restricted LDAP environments.

- **Search Start Location**
  - **Note:** This property defines where in the directory tree the search for user records will begin.
  - Examples:
    - For LDAP:
      - OU=MemberGroupB, O=en_us
    - For Active Directory: CN=Users,DC=ad,DC=example,DC=com

- **Search Scope**
  - Select **subtree** in the drop-down.
    - **Note:** This property defines the depth (below the baseDN) of user record searches.

- **Attribute Name that Identifies a Found Entry**
  - **Note:** This property designates the attribute name that uniquely identifies the user account within the scope of the tree search.
  - For LDAP: **`uid`** Or
  - For Active Directory: **`samAccountName`**
- **Found Entry Email Attribute Name**
  - Enter **`mail`**
- **Found Entry First Name Attribute Name**
  - Enter **`givenName`**
- **Found Entry Middle Name Attribute Name**
  - Enter the middle name attribute from your LDAP or Active Directory (if applicable)
- **Found Entry Last Name Attribute Name**
  - Enter **`sn`**
- **Found Entry Telephone Number Attribute Name**
  - Enter **`telephoneNumber`**
- **Use LDAP Departments**
  - Set to **`True`**
    - **Note:** This property defines the user's department attribute value that will be synchronized within AquaLogic Enterprise Repository.
- **Department Attribute**
  - Enter **`department`**
- **Use LDAP Roles**
  - Set to **`False`**
- **Role Attribute**
  - Enter the LDAP / Active directory attribute that contains the role information for the user.
- **Second Level Lookup Attribute**
  - **Note:** This property defines the attribute that identifies a second-level lookup to retrieve user info; the value must be a DN. If you are using a redirect for second level lookups, define the base DN for this second lookup.

3. Click **Save** when finished.
4. Restart the AquaLogic Enterprise Repository application.

Security Considerations

Using the AquaLogic Enterprise Repository LDAP/Active Directory Connector allows LDAP to act as the single source of user identification for AquaLogic Enterprise Repository user authentication and role assignment. However, this does not prevent respective host repositories from managing user authentication for access to files via AquaLogic Enterprise Repository.

When using the AquaLogic Enterprise Repository LDAP/Active Directory Connector, AquaLogic Enterprise Repository depends on LDAP or Active Directory to authenticate users. The username/password combination is delegated to the LDAP system as a bind request. The user is authenticated only if the bind request is successful.

As an option, LDAP can be configured to store/retrieve AquaLogic Enterprise Repository user role assignments. In this configuration, at each user login AquaLogic Enterprise Repository synchronizes with the user's roles as stored in LDAP. Roles are added directly through LDAP, and are not managed by AquaLogic Enterprise Repository.

Use Case Sample Scenarios

The following scenarios illustrate a selection of LDAP setups and configurations in order to clarify property settings for user management.

Scenario 1

Prevent user access to AquaLogic Enterprise Repository despite LDAP authentication. Access is provided only to pre-existing users with active AquaLogic Enterprise Repository accounts.

- ***Rationale***
  - Non-enterprise license agreements where user base is predefined and number of users allowed into the application is limited.
- ***Property Settings***
  - **`ldap.allow-user-creation`**
    - Set to **False**
  - **`enterprise.security.unapproveduser.allowlogin`**
    - Set to **False**

Scenario 2

On LDAP authentication, create a default AquaLogic Enterprise Repository user account and assign the default role(s), but deny the user access to the AquaLogic Enterprise Repository.

- ***Rationale***
  - To deny AquaLogic Enterprise Repository access to a new user until the security administrator is notified that the new user account was created. Once approved by the security administrator, the user's status is changed to active, allowing AquaLogic Enterprise Repository login.
- ***Property Settings***
  - **`ldap.allow-user-creation`**
    - Set to **True**
  - **`ldap.assign-default-roles`**

        - Set to **True**
    - **`enterprise.security.unapproveduser.allowlogin`**
        - Set to **False**

Scenario 3

On LDAP authentication, a default AquaLogic Enterprise Repository user account is created with the default role(s), and the user is permitted to login to the AquaLogic Enterprise Repository.

- ***Rationale***
    - An enterprise license agreement in which LDAP authentication is the only restriction on new user creation. Typically, the default AquaLogic Enterprise Repository role would be set to User in order to limit access for new users whose roles are not predefined by an LDAP account.
- ***Property Settings***
    - **`ldap.allow-user-creation`**
        - Set to **True**
    - **`ldap.assign-default-roles`**
        - Set to **True**
    - **`enterprise.security.unapproveduser.allowlogin`**
        - Set to **True**

LDAP Property Examples

Since limitations in Active Directory prevent searches below the top level of the directory while anonymously bound (not authenticated) to the directory server, AquaLogic Enterprise Repository user information lookup requires the **Bind DN**, **Bind Password**, and **Retrieve Data As Admin** properties to be set with appropriate values.

Active Directory		**Traditional LDAP** (InetOrgPerson)	
ldap.host	ad.example.com	ldap.host	ldap.example.com
ldap.port	389	ldap.port	389
ldap.version	3	ldap.version	3
ldap.bindDN	**CN=Some_User, OU=Users,DC=ad, DC=example,DC=com**	ldap.bindDN	(required if Anonymous lookups are disabled)
ldap.bindPassword	**password**	ldap.bindPassword	(required if Anonymous lookups are disabled)
ldap.retrieve-data-as-admin	**true**	ldap.retrieve-data-as-admin	false (TRUE if anonymous lookups are disabled)
ldap.mask	sAMAccountName=^	ldap.mask	uid=^
ldap.baseDN	CN=Users,DC=ad, DC=example,DC=com	ldap.baseDN	OU=MemberGroupB, O=en_us
ldap.scope	subtree	ldap.scope	one

ldap.uniqueIDAttrib	samAccountName	ldap.uniqueUDAttrib	uid
ldap.emailAttrib	mail	ldap.emailAttrib	mail
ldap.givennameAttrib	givenname	ldap.givennameAttrib	givenName
ldap.surnameAttrib	sn	ldap.surnameAttrib	sn
ldap.telephoneAttrib	telephonenumber	ldap.telephoneAttrib	telephoneNumber
ldap.deptAttrib	department	ldap.deptAttrib	department

Custom and Common Properties Regardless of implementation	
ldap.rbac.mapperclass	com.flashline.enterprise.authentication.server.loginmodule.LDAPMapperImpl
ldap.deptAttrib	department
ldap.rbac.roleAttrib	roles
ldap.allow-user-creation	true
ldap.enable-synch-roles	true
ldap.enable-synch-depts	true