This type of authority authorizes access if the user is a member of a LDAP or AD group. This authority can be used for role based access control policies.

Configuring the LDAP/AD Group Membership Authority

To configure the authority, complete the following steps.

1. Sign into the Administrative Console
2. Click **Create New Authority.**
3. Select **LDAP/AD Group Membership** from the **Authority Type** drop down.
4. Type a name for the authority in the **Authority Name** box.
5. Type a description of the authority in the **Authority Description** box (optional).
6. Type he fully qualified URI location of the Resilient Access Authority Connector in the **Resilient Access Authority Connector Host** box, including the number of the port on the Resilient Access Authority Connector host that will accept incoming connections. To encrypt the communications between the Trust Network and the Resilient Access Authority Connector, type **https**.
   http[s]://*fully_qualified_domain_name*:*port_number*
7. Configure the connection to the LDAP/AD server by entering:
   1. The LDAP Protocol connection URL using the ldap:// or ldaps:// scheme in the **Connection URL** box: **ldap[s]://*fully_qualified_domain_name*:*port_number***
   2. The LDAP/AD server bind account **Distinguished Name (DN)** in the **Connection Name** box: e.g. ***cn=admin,dc=acme,dc=com***
   3. The password for the bind account to connect to the LDAP/AD server in the **Connection Password** box.
8. Configure how the user record for a member of the LDAP/AD will be found
   1. Enter the base path within the LDAP/AD where user records are stored in the **User Search Base** box. This field allows multiple base paths to be entered, by clicking the "+" icon to the right of the text box. If more than one base path is specified, all the specified base paths will be searched sequentially for the user record. e.g.
      (ou=employees,dc=acme,dc=com) OR (ou=contractors,dc=acme,dc=com)
   2. If sub-paths below the base path should be searched for the user record, then click on the **Search Subtree** checkbox
   3. If entries within the LDAP/AD references other locations where user records are stored, then those locations will also be searched if the **Follow Referrals** checkbox is checked
   4. Enter the name of the user record attribute in the LDAP/AD that will be the user identifier when searching for the user record in the **User Identity Attribute** box. For example if the authentication is performed based on email address as the identity attribute and the "**mail**" attribute hold the email address in the user record then ***mail*** should be entered for **User Identity Attribute**
9. Configure Group membership attributes as follows:
   1. Specify the Base DN for the LDAP/AD group the authority is verifying membership of.
   2. Specify the attribute that lists the members of the group within the Group DN. For AD this attribute is typically member while for LDAPs this attribute is typically uniqueMember
10. Once you have finished configuring the LDAP/AD Authentication authority, click **Create** or **Save**.