LDAP/AD Attribute Provider performs a lookup in an LDAP/AD and returns attributes from the AD. These attributes can be mapped to output attributes returned by the authority as a part of the policy assertion if the policy evaluates to a GRANT.

Configuring the LDAP/AD Attribute Provider

To configure the authority, complete the following steps.

1. Sign into the Administrative Console.
2. Click **Create New Authority**.
3. Select **LDAP/AD Attribute Provider** is selected in the **Authority Type** list box.
4. Type a name for the authority in the **Authority Name** box.
5. Type a name for the authority in the **Authority Display Name** box.
6. Type a description of the authority in the **Authority Description** box (optional).
7. Type the 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 Resilient and the Resilient Access Connector, type **https**.
   http[s]://*fully_qualified_domain_name*:*port_number*
8. Use the **Runtime Parameters** area to add and configure the parameters without literal values. The values of these parameters will be supplied by the end user at runtime. For each runtime parameter, specify the following:
   - Type the name of the parameter in the **Name** box. The parameter name gets paired with the value provided at runtime and sent to the custom REST authority.
   - Type the label of the box displayed to the end user in the **Display Name** box.
   - If the parameter will contain a sensitive value, such as personally identifiable information, select the **Obfuscate** check box. This instructs the Policy Workflow Engine to substitute an opaque token for the value as it transits the network, ensuring that the value never passes through the central Policy Workflow Engine component and does not get stored in the Trust History.
   - If the user will provide the value in the initial request form, select the **Initial Request** check box. NOTE: Resilient recommends leaving the **Initial Request** check box blank if the value is sensitive or contains personally identifiable information.
   - Select the **Mask Input** check box to mask the values with bullet characters as the user types them in. This protects against shoulder surfing.
9. 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 connection user **Distinguished Name (DN)** in the **Connection Name** box: e.g. ***cn=admin,dc=acme,dc=com***
   3. The password for the user account to connect to the LDAP/AD server in the **Connection Password** box.
10. 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**

    5. Select the runtime parameter that will match the **User Identity Attribute** for the LDAP/AD record lookup

11. Specify the attributes to retrieve from the LDAP/AD by entering the attribute names in the **LDAP/AD Attributes to retrieve** section
12. Configure the attributes to return using the steps below:
    1. Enter the name for the output attribute under the *Output Attribute Name* column
    2. Select the mapping type:
        - If **Mapped Type** is ***Runtime Parameter*** then **Mapped Value** will be populated with the runtime parameters defined. Select the one to use from the drop-down
        - If **Mapped Type** is ***Literal*** enter the value in the **Mapped Value** box
        - If **Mapped Type** is ***Query Result*** then **Mapped Value** will be populated with the attributes defined in the **LDAP/AD Attributes to retrieve** section. Select the one to use from the drop-down.
    3. Click the button with the + icon to add the attribute to return
    4. Repeat the above steps for adding more attributes to return. Click the button with the x icon to delete an attribute.
13. Once you have finished configuring the custom authority, click **Create** or **Save**.