An authority that authenticates a user in an LDAP or Active Directory. The Policy Workflow Engine privacy enhancing policy evaluation mechanism avoids the passing around of the password through the network by requesting for the password only when the LDAP/AD Authentication authority is invoked. The sensitive information is only exchanged between the user and the LDAP/AD Authentication authority over TLS.

Configuring the LDAP/AD Authentication Authority

To configure the authority, complete the following steps.

1. Sign into the Administrative Console
2. Click **Create New Authority.**
3. Select **LDAP/AD Authentication** 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 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.
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**
    5. Resilient Access has integrated with Intensity Analytics Behavioral Biometric Authentication to seamlessly provide strong second factor authentication to policies created in Resilient Access. Intensity Analytics has a patented technology of calibrating

the rhythm of a user's keystoke pattern and using that to create a unique user identity signature. This is then applied to detect if the person typing the password is the person being authenticated. As the user authenticates using their password the system calibrates and stores profiles of the keystroke rhythm until enough profiles have been created to accurately determine a user's keystroke rhythm. Subsequent authentication attempts will enforce the Intensity Analytics Behavioral Biometric Authentication as an additional authentication factor. To enable Intensity Analytics Behavioral Biometric Authentication click the **Include Intensity Analytics** checkbox.

9. Once you have finished configuring the LDAP/AD Authentication authority, click **Create** or **Save**.