Database Policy Authority performs a SQL Query in a Database and retrieves attributes from the database. 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. The query should only return one result row for the authority to correctly forward the evaluation to the output policy.

Configuring the Database Attribute Provider

To configure the authority, complete the following steps.

1. Sign into the Administrative Console.
2. Click **Create New Authority**.
3. Select **Database Attribute Provider** 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 Authority 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 Resilient 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 Database server by entering:
   1. The fully qualified hostname of the database server in the **Database Host** box:
   2. The name of the database containing the user records in the **Database Name** box
   3. The database user name in the **Database User Name** box
   4. The password for the user account to connect to the Database server in the **Database Password** box.
10. Build the SQL Expression to extract attributes through the SQL query builder.
    1. First select the table name and click on the + button to add the table to the expression
    2. After the first table is added the controls for adding columns to the SQL query will appear. Add each column by specifying the **Column Name** the type

whether *String* or *Numeric* and the table the column belongs to and then the + button to add the column to the SQL query

3. After adding a column the controls for adding WHERE clauses will appear. The left-hand side of the WHERE clause expression will be populated with the columns in the SELECT section, the right-hand side can either be *Runtime Parameter* a *SQL Column* or a *Literal*. The widget next to it will be appropriately populated to specify the right-hand side value. Click the + button to add the WHERE clause.

4. For either the SELECT column or the FROM table or the WHERE clause can be delete by clicking on the delete icon. The SQL expression will be updated as required to ensure it always remains a valid SQL query.

11. 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 columns in the SQL query defined in the Build the SQL Expression to extract attributes 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.

12. Once you have finished configuring the custom authority, click **Create** or **Save**.