

This type of authority receives a number of attributes as run-time parameters. Typically these attributes are retrieved from identity stores like LDAP/AD or Databases and the attribute authorization authority is configured as an authority in the output policy of a LDAP/AD or Database policy authority. The authority provides an intuitive user interface for building a logical expression of any complexity using the run-time parameters and literals as shown in the example below.

## Configuring the authority

To configure the authority, complete the following steps.

1. Sign into the Administrative Console.
2. Click **Create New Authority**.
3. Ensure that **Attribute Authorization** 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. Use the **Runtime Parameters** area to add and configure the parameters that are used in the execution of the authority, e.g. email address or user ID. 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 Access to substitute an opaque token for the value as it transits the network, ensuring that the value is opaque to other authorities that may be part of the policy workflow.
  - 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** checkbox to mask the values with bullet characters as the user types them in. This protects against shoulder surfing.
8. The logical expression is built in the **Attributes Authorization Logical Expression** panel by creating sub-expressions that combine the run-time parameters. The sub-expressions are then joined through the AND and OR join operators. To create Attribute Authorization expression follow the steps below
  1. For each run-time parameter specify at-least one value, multiple values can be provided by either clicking the + button next to the parameter value box or by clicking the ENTER key. Values can be removed by clicking the X for an entry in the drop-down of the parameter value. When multiple values are specified for a run-time parameter the operator should be IN or NOT IN
  2. Specify the join operator for each run-time parameter expression. Typically the run-time parameters are joined using the same join operator.
  3. Click **Add Expression** to add the sub-expression to the overall Attribute Authorization expression
  4. Specify the join operator that joins the sub-expression when there are multiple sub-

expressions. Typically the same join operator is used to join all the sub-expressions.

5. When mouse hovers over an sub-expression the entire expression is displayed in a popup tooltip.

9. Once you have finished configuring the Attribute Authorization authority, click **Create** or **Save**.

**Step 2:** Configure the Attributes Authorization logical expression

The screenshot displays the 'Attributes Authorization Logical Expression' configuration window. At the top, there is a list of existing expressions, each with a preview and an 'OR' button. Below this, there is a form to create a new expression. The form consists of three rows, each representing a different attribute:

- Document Class:** A dropdown menu with an equals sign, followed by a search box labeled 'select or add a Document Class Values'.
- User AD Group:** A dropdown menu with an equals sign, followed by a search box labeled 'select or add a User AD Group Values'.
- Access Context:** A dropdown menu with an equals sign, followed by a search box labeled 'select or add a Access Context Values'.

Between the rows, there are blue buttons labeled 'AND' and 'OR' to combine the expressions. At the bottom right of the form, there is a blue button labeled 'Add Expression'.