A Simple Policy Authority returns the output policy configured, mapping the runtime parameters passed to it to the parameters required by the output policy. This type of authority is well suited to define the top level policy when the policy consists of several lower level policies where each lower level policy performs a similar function. E.g. an isEmployee policy that checks against different identity sources to verify if an employee is a member of an organization.

Configuring the Simple Policy Authority

To configure the authority, complete the following steps.

1. Sign into the Administrative Console.
2. Click **Create New Authority**.
3. Ensure that **Simple Policy Authority** 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 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.
8. Define the output policy and configure the policy parameters using the steps below:
    1. Click the **Create Output Policy** button to define the output policy. The output policy is created in a popup window with a similar interface as the Create Policies page. Drag and drop authorities and define the output policy
    2. The **Configure Policy Parameters** table will list the parameters of the output policy. These can either be mapped to ***Runtime Parameter*** defined above or a ***Literal Value***. If selecting a ***Runtime Parameter*** then select the one to use from the **Mapped Value** drop-down, if **Mapped Type** is ***Literal Value*** then the value should be entered in the **Mapped Value** box.
9. Once you have finished configured the Simple Policy Authority, click **Create** or **Save**