This authority type is used for routing the policy evaluation to a particular branch based on a criteria on one of the runtime parameters that are among its inputs. We can think of this authority type functioning similar to a *switch* statement in a programming language or rules engine. A few pre-defined decision criterias based on common use cases such as domain in an email address or IP address/CIDR range are provided. A custom decision criteria can be created by defining a regular expression extraction rule from the value of the parameter.

The cases within the decision switch consists of key-value pairs where the *key* is the value extracted off the decision criteria runtime parameter and the *value* is an existing Authority that is online and in-scope for routing the policy evaluation to. The Authority needs to be online and have at-least one parameter in common with the runtime parameters configured for the Decision Authority in order for it be eligible for selection as the authority to forward the evaluation to. An e.g. is a Decision Authority that takes 2 parameters - a email address (parameter name *email*) as a user identifier parameter and an IP address (parameter name *ipAddress*) that is used as the decision criteria parameter. An eligible Authority that can be selected for routing the policy evaluation must have at-least one parameter in common (e.g the *email*). The parameters received by the Decision Authority is passed to the matching parameter inputs of the authority the policy evaluation routes to.

Configuring the Decision Authority

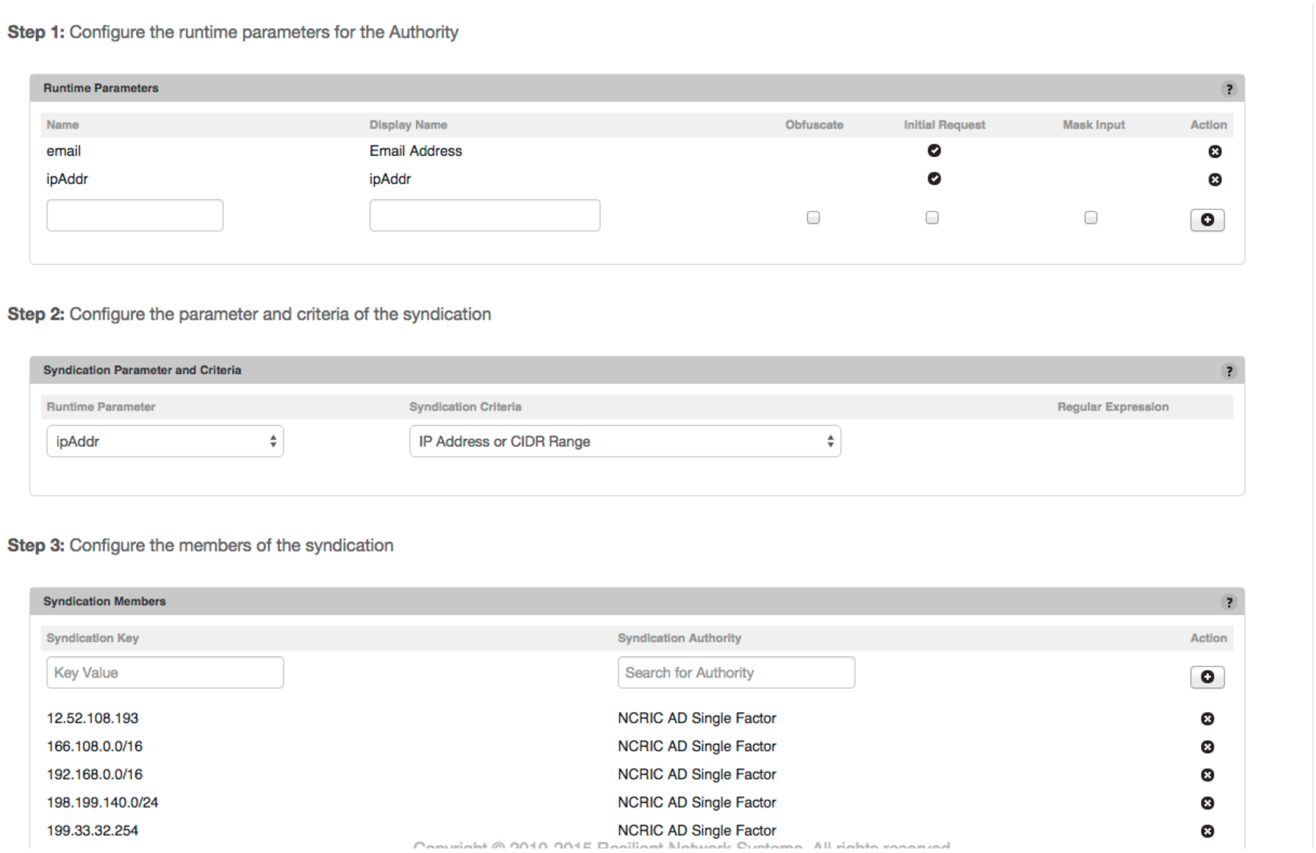
To configure the authority, complete the following steps.

1. Sign into the Administrative Console
2. Click **Create New Authority.**
3. Select **Decision Authority** 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. 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 Access 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.
7. Configure the decision runtime parameter and the decision criteria:
    1. Select the runtime parameter the decision will be based on in the **Runtime**

Parameter drop-down.

    2. Select the decision criteria to use in the **Decision Criteria** drop- down. Select between the following options:
        1. Select *Parameter Value* if the entire parameter value will be used as the decision criteria
        2. Select *Extract Domain from Email* if the decision criteria is based on the domain in an email address
        3. Select *Extract sub-domain from Hostname* if the decision criteria is based on the sub-domain in a hostname of a URL
        4. Select *IP Address or CIDR Range* if the decision criteria is based on a IPV4 IP address value e.g. 192.168.1.1 or within a CIDR Range such as 192.168.1.0/24 which includes all IP addresses between 192.168.1.0 - 192.168.1.255
        5. Select *Custom Regular expression to extract from Parameter Value* if the decision criteria is extracted from a runtime parameter based on the specified regular expression. In this case the regular expression must be specified in the **Regular Expression** box.

8. Configure the Key-Value pairs that make up the routing options for the Decision Authority
    1. For each routing option enter the key in the **Key Value** box and start typing the authority name in the **Search Authority** box and the Authorities that are eligible and match the partial name entered will appear. One of the eligible authorities must be selected and clicking the + button will add the authority.
    2. If you wish to route the evaluation to an authority if none of the key-value pairs match then check the **Has a no match case** box and select the default authority to route to by entering the partial name for the authority in the **Authority to invoke if no match** box
9. Once you have finished configuring the Decision authority, click **Create** or **Save**.



Step 1: Configure the runtime parameters for the Authority

Runtime Parameters ?

Name	Display Name	Obfuscate	Initial Request	Mask Input	Action
email	Email Address		✓		✖
ipAddr	ipAddr		✓		✖
		□	□	□	⊕

Step 2: Configure the parameter and criteria of the syndication

Syndication Parameter and Criteria ?

Runtime Parameter	Syndication Criteria	Regular Expression
ipAddr	IP Address or CIDR Range	

Step 3: Configure the members of the syndication

Syndication Members ?

Syndication Key	Syndication Authority	Action
Key Value	Search for Authority	⊕
12.52.108.193	NCRIC AD Single Factor	✖
166.108.0.0/16	NCRIC AD Single Factor	✖
192.168.0.0/16	NCRIC AD Single Factor	✖
198.199.140.0/24	NCRIC AD Single Factor	✖
199.33.32.254	NCRIC AD Single Factor	✖