An Authority that calls a REST service that returns attributes if access is granted. These attributes are mapped to the input parameters of the output policy configured. The REST service must implement the Custom REST Authority API that provides a mechanism for developers to extend and enhance the access control capabilities of Resilient Access to meet their requirements.

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 **Custom REST Policy Authority - V2** 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 **Configuration Parameters** area to specify static name/value pairs to be sent with each evaluation request at runtime. Since the same value is sent every time, this type of parameter may be useful to send API credentials for web services the REST service authority is encapsulating. The config parameters can be sent either in the POST body or as HTTP header parameters
8. 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.
9. Type the fully qualified URL for the base address of the REST service in the **Custom REST Service URL** box including scheme and port (if applicable). The /token and /evaluate end-points must be implemented off this base address as per the Custom REST Authority API specifications.
10. Specify the names of the attributes that will be returned in the assertions object in the response to the /evaluate API if the "result"="GRANT".
11. Define the output policy and configure the policy parameters using the steps below:
    11. 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
    12. 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*** or a

Query Result.

- 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 the attributes defined in the **Custom REST Service Attributes** section. Select the one to use from the drop-down.

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

Retrieving API Credentials

From the Authorities list retrieve the API credentials for the JWT Bearer Token OAuth authentication that is required for the Custom REST service API. This includes:

- Client ID
- Client Secret
- Public Key of an RSA Key Pair in PEM format (the Private Key is stored in Resilient Access)
- Key ID