Plan View for HTTP Tasks

Feature Availability: This feature is available in the following editions:

- Trifacta® Enterprise Edition
- Trifacta Professional Edition
- Trifacta Premium

In Plan View, you can create HTTP tasks to send request to endpoints before or after the execution of other tasks. These tasks are specified in the right context panel.

Figure: HTTP task

> **Tip**: To rename the task, click the task name.

Fields:

Field	Description
Method	Select the HTTP method to use to deliver the message. The appropriate method depends on the receiving application. Most use cases require the POST method.

URL	URL where the HTTP request is received by the other application.
Headers	Insert HTTP content headers as key-value pairs. For example, if your body is in JSON format, you should include the following header: ``` key: Content-Type value: application/json ``` > **NOTE:** You may be required to submit an authentication token as the value for the `Authorization` key.
Body	(`POST` , `PUT` , or `PATCH` methods only) The body of the request submitted to the receiving application. Request body is structured as follows: ``` {"text":"My text message to the receiving application."} ``` > **Tip:** As part of the request body or header fields, you can insert metadata references to the plan definition, current run, tasks already executed in the run, and underlying flows, including column data and datasources. For more information on the available metadata, see *Plan Metadata References*. For examples of requests including metadata examples, see *Create HTTP Task*.
Secret Key	(Optional) A secret key can be used to verify the request payload. This secret value must be inserted in this location, and it must be included as part of the code used to process the requests in the receiving application. Insert the secret value here as a string without quotes. For more information on how this secret key is used to generate a signature, See *Create HTTP Task*.
Validate SSL Certificate	When set to `true`, HTTPS (SSL) communications are verified to be using a valid certificate before transmission. > **NOTE:** If you must send a request to an endpoint that has an expired/invalid certificate, you must disable SSL verification.
Retry	If the returned status code is outside of the 200-299 range, then the HTTP task is considered to have failed. When this option is enabled, the request is retried. If the request fails, this value defined the number of times that the request should be retried. If this number of retries is reached without success, the task fails.

Actions:

- To test if the specified endpoint is reachable, click **Test**.

  > **Tip:** A status code of `200` indicates that the test was successful.

  > **Tip:** You can use the GET method for testing purposes. A GET request does not change any data on the target platform but may permit you to specify elements in the request body.

- **Edit task name:** Change the name of the task.

  > **Tip:** Good naming may include the target platform endpoint and method, as well as the purposes of the task in your plan.

- **Delete:** Delete the task.

> **This step cannot be undone.**

For more information, see *Create HTTP Task*.