Configure Webhooks

Contents:

- *Limitations*
- *Pre-requisites*
- *Enable*
- *Configure*
  - *Limit URLs*
  - *Configure retries*
  - *Add signature header to webhook requests*
  - *Disable test button*
- *Use*

A **webhook** is a notification sent from one application to another using HTTP requests. The Trifacta® platform can be configured to send webhook notifications to other applications based on the outcome of job executions. For example, you can configure the Trifacta platform to send a text message to a channel in your enterprise's messaging platform when jobs from a flow succeed or fail or both.

Limitations

- You cannot deploy an SSL certificate of a third-party application for use when sending webhook notifications from the Trifacta node.

Pre-requisites

For more information, see *Create Flow Webhook Task*.

Enable

Steps:

1. You apply this change through the *Workspace Settings Page*. For more information, see *Platform Configuration Methods*.
2. Locate the **Webhooks** settings.
3. Set this value to `true`.

See *Workspace Settings Page*.

Configure

Limit URLs

If necessary, you can restrict the IP address and URLs to which webhook requests can be sent.

> **NOTE:** If you are permitting webhook requests to be submitted back to the Trifacta platform, you must verify that the IP address for the Trifacta node is not forbidden. See Security considerations below.

Steps:

1. You can apply this change through the *Admin Settings Page* (recommended) or `trifacta-conf.json`. For more information, see *Platform Configuration Methods*.
2. Modify the following settings:

Setting	Description
`webapp.webhookSettings.forbiddenIPs`	This list contains the set of IP addresses that are not permitted to be sent webhook requests. **NOTE:** Do not remove the default values. These values prevent requests being sent to the Trifacta node. Addresses can be submitted in IPv4 or IPv6 format. Values are delimited by semi-colons.
`webapp.webhookSettings.allowedUrlRegexes`	As needed, you can create a regular expression to limit the permitted URLs to which webhooks can be sent.

3. Save your settings and restart the platform.

Security considerations when whitelisting the platform

Webhooks can be configured to submit requests back to the Trifacta platform. For example, you can configure a webhook request to run a job after completion of a job. However, since a webhook request could be any REST API request to a target platform, it is potentially risky to enable webhook requests from the Trifacta platform to itself. To limit security risks:

- Where possible, specify URLs instead of IPs, which are more likely to change.
- The allowed URL regexes are processed first. For security, you can restrict access to the Trifacta node to only the permitted endpoint version `v4`:

```
webapp.webhookSettings.allowedUrlRegexes: ['^http:\/\/my\.trifacta-instance\.com\/v4.*$']
```

- The Trifacta node must not be on the forbidden IP addresses.
- Webhooks should not be configured to use admin accounts.
- Accounts used for webhook requests should be limited in scope.

  Tip: You can create a `webhook` user account, with which flows are shared. Then, jobs can be executed under this account, which is limited in scope.

- Webhook accounts should always be authenticated. Use of access tokens for these accounts is recommended.

Configure retries

If a webhook request fails to be received by the target application, the Trifacta platform retries sending the request. You can configure the following parameters pertaining to these retries:

You can apply this change through the *Admin Settings Page* (recommended) or `trifacta-conf.json`. For more information, see *Platform Configuration Methods*.

Parameter	Description
webapp.webhookQueue.maxRetries	The maximum number of times that a failed webhook request is sent. Default is `1`.
webapp.webhookQueue.retryDelayMs	The number of milliseconds between a failure and retrying to send the request. Default is `1000` (one second).

webapp.webhookSettings. timeoutMs	Global timeout setting for webhooks in milliseconds.

Add signature header to webhook requests

As needed, you can sign the webhook requests that are submitted to a target platform.

> **NOTE:** For each target application that requires a signed request, you must deploy a secret key in the request, and the target application must be defined to expect this key.

> **NOTE:** Adding signatures may require custom coding or configuration in the target application.

For more information, see *Create Flow Webhook Task*.

Disable test button

When you create a new webhook task, you can optionally send a test webhook message to verify that the task is properly configured. As needed, this Test button can be disabled.

1. You can apply this change through the *Admin Settings Page* (recommended) or `trifacta-conf.json`. For more information, see *Platform Configuration Methods*.
2. Set the following parameter to `false`:

```
"webapp.webhookSettings.testWebhook": false,
```

3. Save your changes and restart the platform.

Use

Webhook notifications can be defined to be sent on the success or failure of executed jobs. These notifications are defined on a per-flow basis but can be restricted to individual outputs as needed. For more information, see *Create Flow Webhook Task*.