ThreatQuotient

ThreatQ TDR Orchestrator Guide

Version 1.3.0

April 27, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Contents

Overview

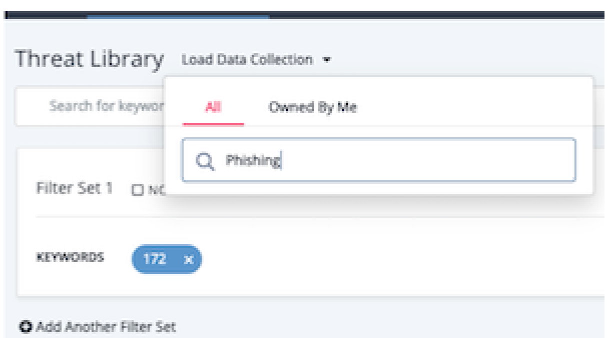
ThreatQ TDR Orchestrator includes enhanced automation, analysis, and reporting capabilities that accelerate threat detection and response across disparate systems.

Using Configuration-Driven Workflows (CDWs), applying Smart Collections, and Custom Scoring, ThreatQ prioritizes the threats that are important for remediation. That could be simple automation to quarantine the device or more complicated workflows to remediate the threat by shutting down a service, removing malware, restoring the system, submitting an alert, creating a ticket or initiating an investigation.

ThreatQ TDR Orchestrator can involve any number of tools and should provide cross team visibility for a more complete XDR security solution.

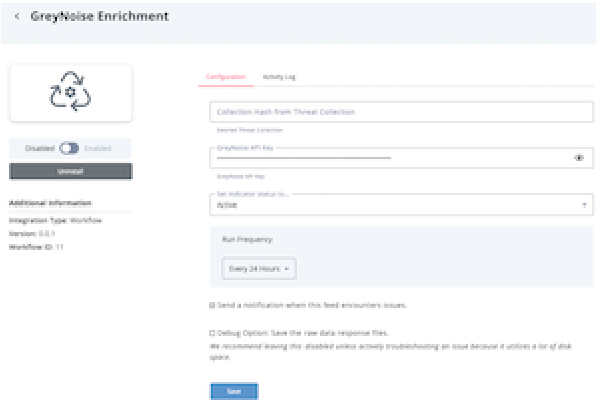
Data-Driven Triggers

Define the type of data to enrich using the ThreatQ Threat Library. Save your Threat Library queries as Data Collections to be used as Data-Driven Triggers in the orchestration workflow.

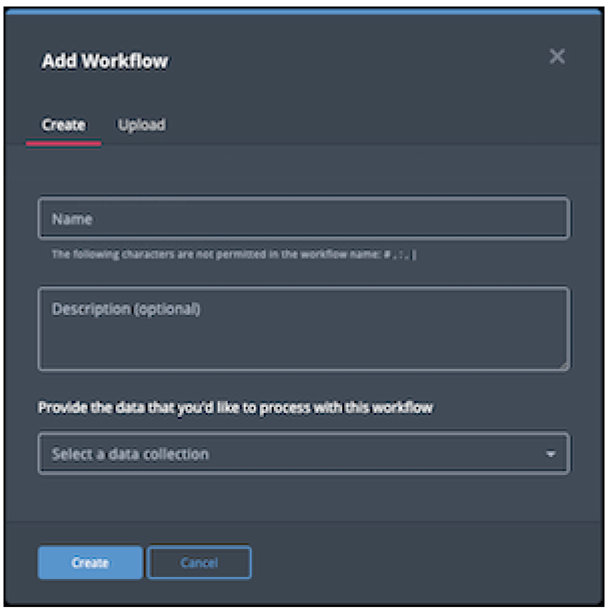


Workflows

Workflows, also known as Data-Driven Playbooks, take your identified triggers, in the form of Data Collections, and enrich your selected threat intelligence data using third-party providers such as Shodan, to curate further detailed threat information.



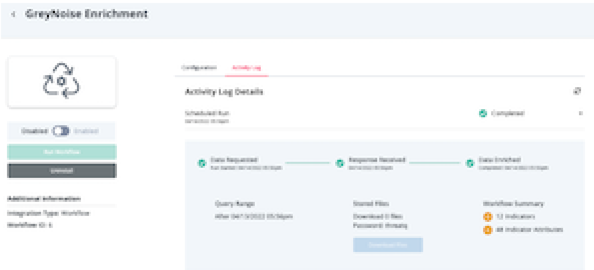
TQO gives you the option to import advanced workflows from predefined YAML files or create your own workflows in the TQO workflow builder.



These workflows can be configured to run at specific intervals or run manually from the Threat Library results or object details pages.

Capture Enriched Data

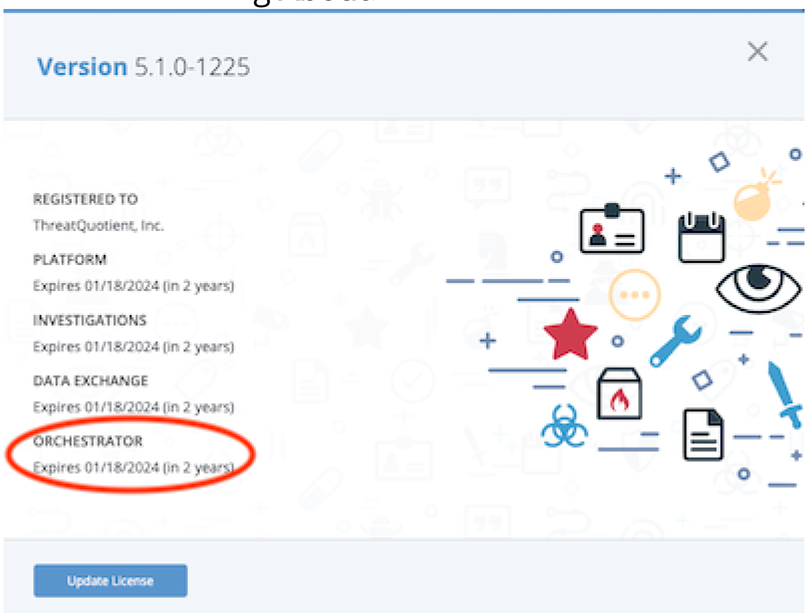
The enriched information captured by the workflow is then ingested back into the ThreatQ platform for further analysis and refinement.


GreyNoise Enrichment
Activity Log Details

Requirements

Confirm that you have the following:

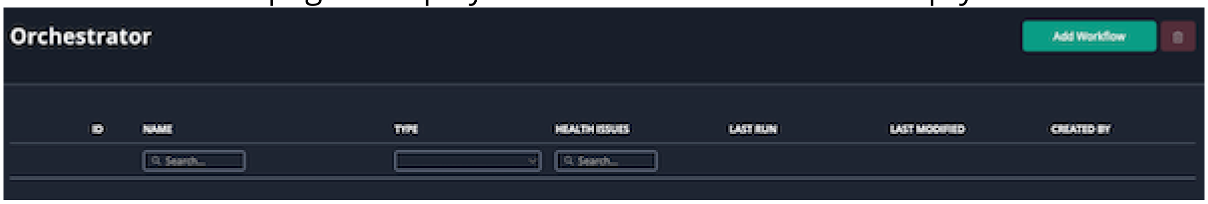
- ThreatQ version 5.4.0 or greater
- A ThreatQ Orchestrator license. This can be confirmed by clicking on the **Settings** gear icon and selecting **About**.



- A saved data collection is required for scheduled/periodic workflow runs
- An admin or maintenance user login

Accessing the Orchestrator Page

The Orchestrator page is the hub of TQO. It provides an overview of your existing workflows, allows you to manage these workflows, and create or import new ones.

1. Click the **Orchestrator** icon in the top navigation bar.
   The Orchestrator page is displayed and the workflow list is empty.
   

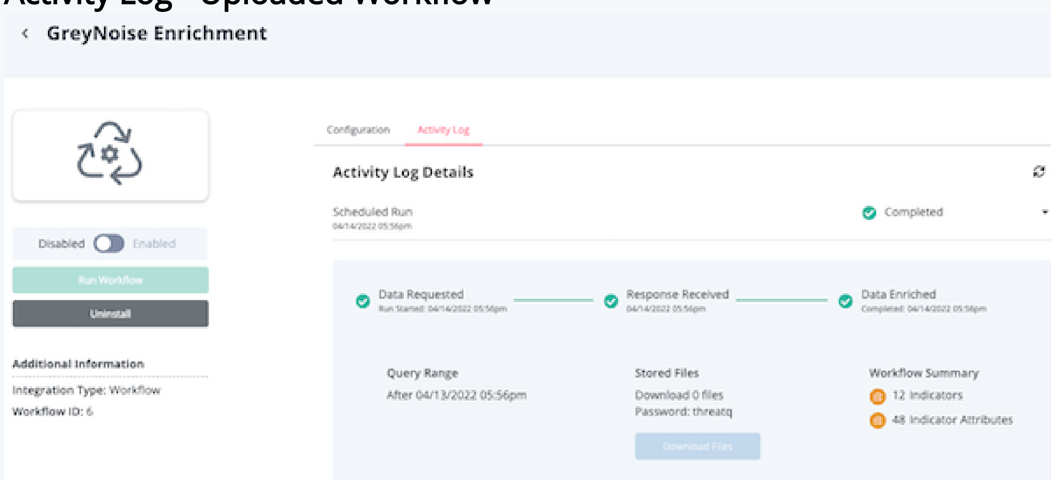
2. Click the **Add Workflow** button to begin adding workflows to your instance.

Components

The following table contains key components, terms, and definitions regarding ThreatQ TDR Orchestrator (TQO) .

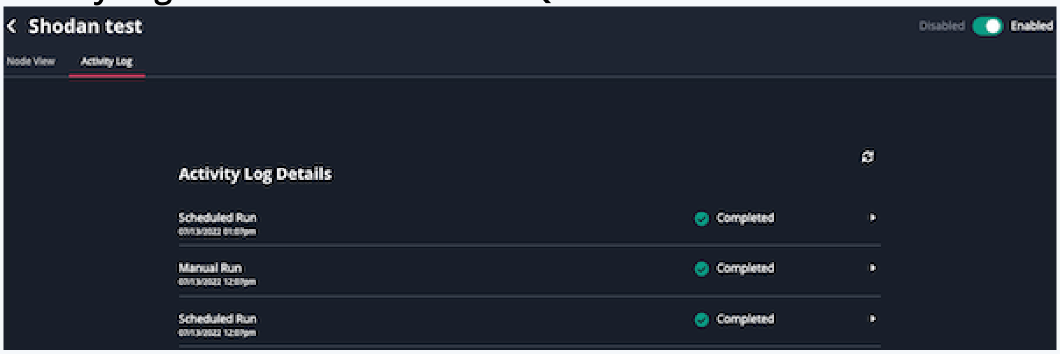
<table>
<tr><th>COMPONENT/ TERM</th><th>DEFINITION</th></tr>
<tr><td>Action</td><td>Actions are YAML snippets you can use to enrich the data specified by your workflow's data collection. TQO includes pre-seeded actions and allows you to install additional ones. See the Adding an Integration topic for more information on installing actions.</td></tr>
<tr><td>Activity Log</td><td>TQO provides activity logs for workflows uploaded into TQO as well as those created in TQO. A workflow's activity log provides you with a summary of each manual or scheduled run of the workflow. This includes:

Date/time of the run
Run status at completion
Data requested
Response received
Data enriched

Activity Log - Uploaded Workflow

</td></tr>
</table>

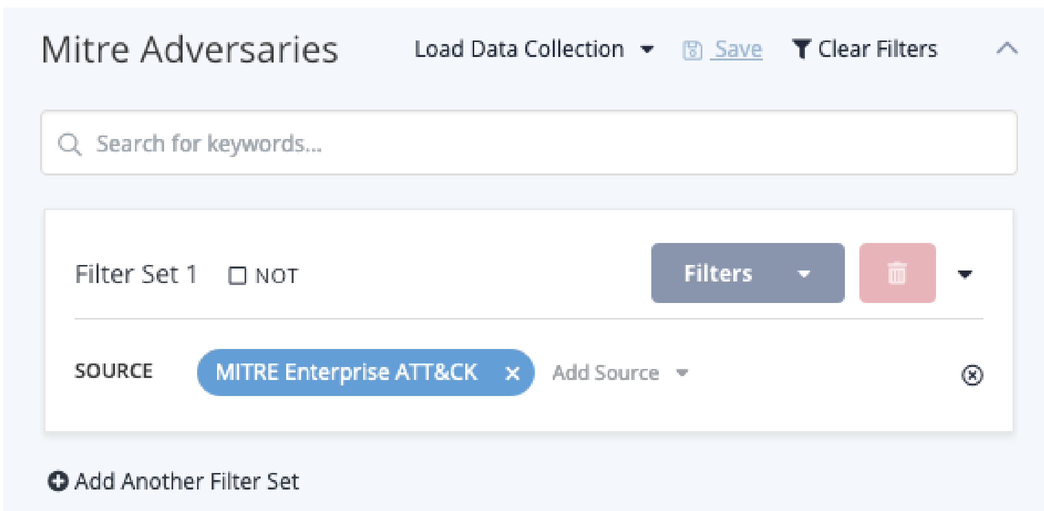
COMPONENT/ TERM	DEFINITION

Activity Log - Workflow Created in TQO



Data Collection

A data collection is a saved ThreatQ Threat Library query that identifies the information to be enriched by a workflow.



Nodes

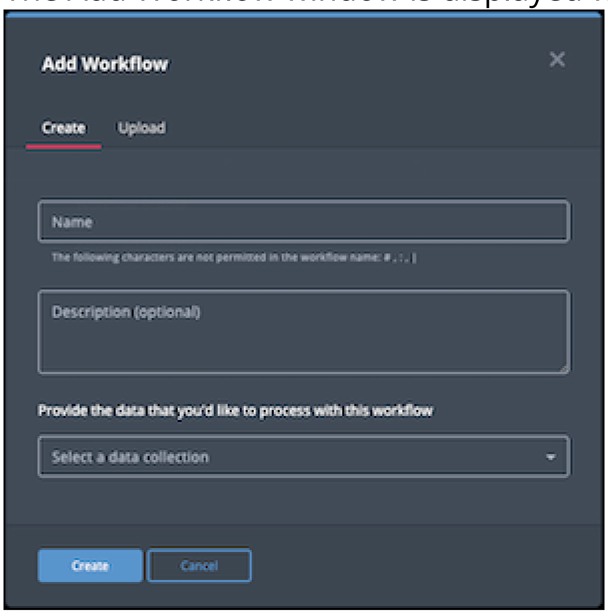
A node is a basic unit of a data structure within TQO, such as a data collection, workflow, or action, displayed in the Node View. You can

COMPONENT/ TERM	DEFINITION
	click on a node to view and/or update its configuration details. 
Node View	A workflow's Node View provides you with a visual representation of its basic components, the data collection, the workflow, and its action(s). You can access the Node View by clicking a workflow created in TQO in the Orchestrator page. These workflows have a type listed as Workflow Builder. From the Node View you can click the various workflow nodes, such as data collection, workflow, or action nodes, and view or update each node's settings.
Workflows	Workflows take your identified triggers, in the form of Data Collections, and enrich your selected threat intelligence data using third-party providers such as Rapid7, to curate further detailed threat information. You can add a workflow to TQO by uploading an Advanced Workflow YAML file or use the TQO workflow builder to create a workflow.

Adding Workflows

TQO allows you to create a new workflow using the TQO workflow builder or upload an advanced workflow from a YAML file.

Creating a Workflow

1. Click the **Orchestrator** option in the main navigation.
2. Click the **Add Workflow** button.
   The Add Workflow window is displayed with the Create tab selected.
   

3. Populate the following fields:
   - **Name** - Enter the name of the workflow.

     > The workflow name cannot include the # (pound), : (colon), or | (pipe) characters.

   - **Description** - Optional field. Enter a brief description of the workflow.
   - **Select a data collection** - Click this field to access a dropdown list of data collections. By default, this list displays **All** data collections you have permissions for. Click the **Owned By Me** tab to narrow your view to the data collections to which you have owner permissions. You can also use the search field to locate a data collection.

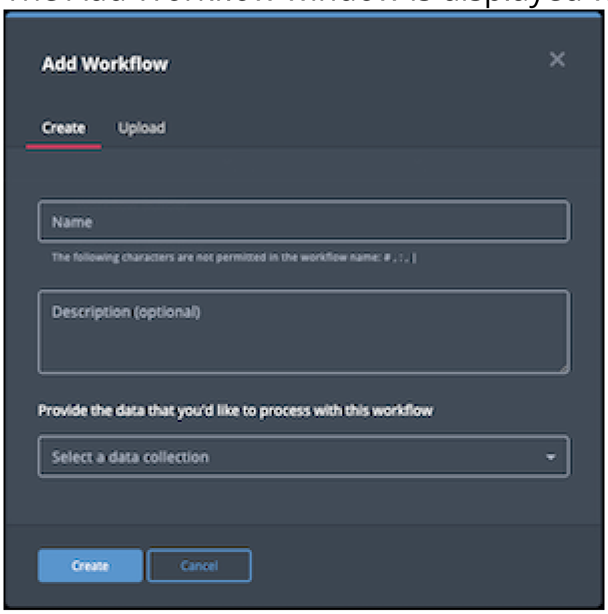
> You can leave this field blank and select the data collection from the workflow's Node View.

4. Click the **Create** button.
   The Node View of your new workflow is displayed. You must configure and enable the workflow before you can run it.

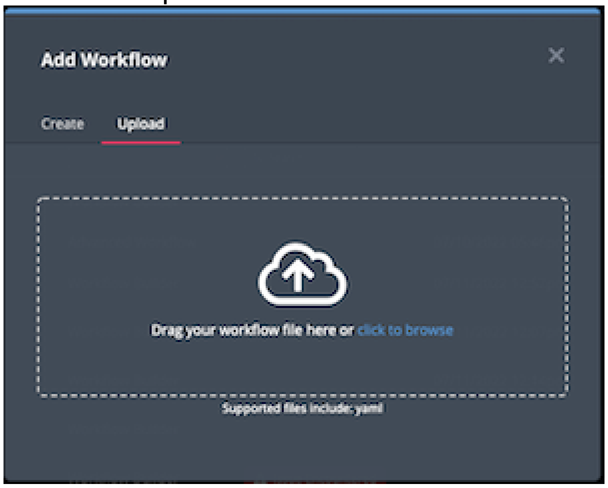
Uploading an Advanced Workflow

TQO only supports the uploading and use of workflow YAML files developed by ThreatQuotient. Contact ThreatQuotient Customer Success for more information.

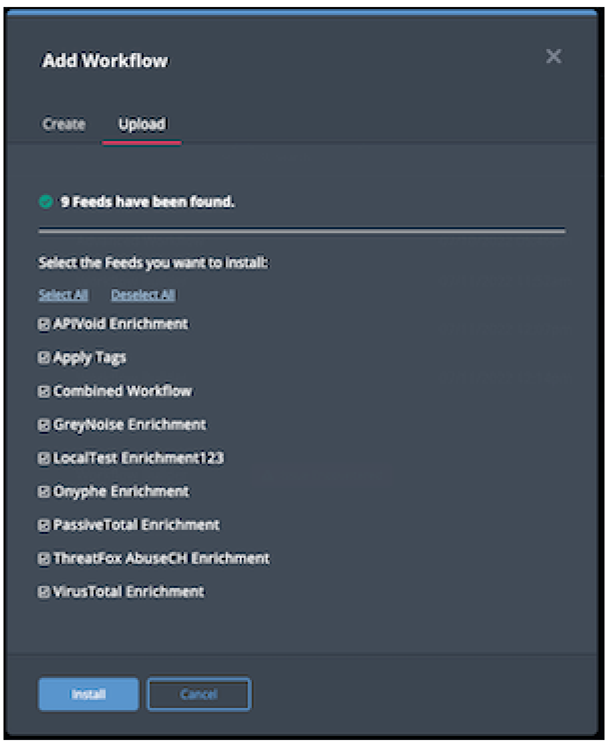
1. Click the **Orchestrator** option in the main navigation.
2. Click the **Add Workflow** button.
   The Add Workflow window is displayed with the Create tab selected.



3. Click the Upload tab.



4. Upload the advanced workflow file using one of the following methods:
   - Drag and drop the workflow file into the dialog box
   - Select the **click to browse** link to locate the workflow file.
5. If the workflow file contains multiple feeds, you are prompted to select which feeds to install. Select the feeds to include and click **Install**.

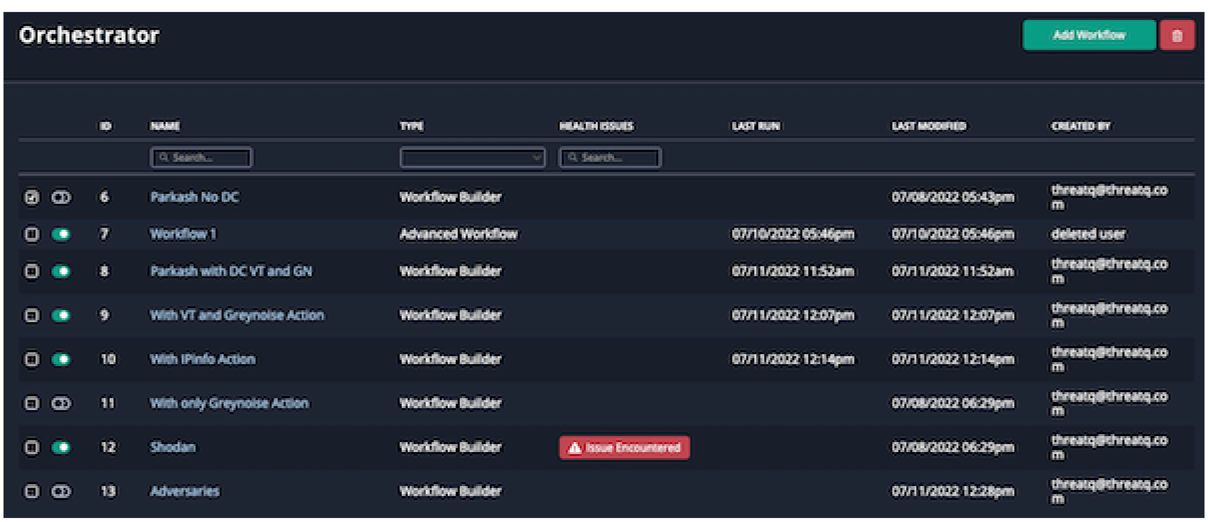


6. When the install is complete, you must configure and enable the advanced workflow before you can run it.

Managing Workflows

The Orchestrator page provides you with a list of your existing workflows as well as key information on each such as:

- **Name** - The workflow name. This name is extracted from the workflow file itself if you imported it.
- **Type** - Identifies the workflow as an **Advanced Workflow** uploaded from a YAML file or a workflow created within TQ0's **Workflow Builder**.
- **Health Issues** - If this column is blank, the last workflow run did not encounter an issue. If this column displays **Issue Encountered**, the last workflow run encountered one of the following error statuses:
    - Error Occurred
    - Error during run
    - Incomplete
    - Failed to Complete
- **Last Run** - The date/time of the last workflow run.
- **Last Modified** - The date/time of the most recent changes to the workflow. For a newly imported workflow, this column lists the date/time you imported it.
- **Created By** - For workflows created in TQO, this column lists the login of the user who created the workflow. For advanced workflows this column is blank.



You can use the **Name, Health Issues,** and **Type** fields to locate workflows as well as customize the list displayed in the Orchestrator page. For instance, you can filter your view to display only workflows created in TQO by selecting a type of Workflow Builder.

Workflow management options and pages vary by workflow type. The following sections provide instructions on:

- Managing Workflows Created in TQO
- Managing Advanced Workflows

Managing Workflows Created in TQO

Workflows created in TQO allow greater flexibility in terms of which indicators are processed and when they are processed. When you create a workflow in TQO, you can:

- Configure it to apply the workflow actions at periodic or scheduled intervals to the workflow's data collection.
- From the workflow node view, run it manually to apply the workflow actions to workflow's data collection
- From the Threat Library results page, run it manually to apply the workflow actions to a list of system objects/data collection displayed in the Threat Library results page
- From the Threat Library object details page, use the Actions menu to run it manually and apply the workflow actions to a single system object.

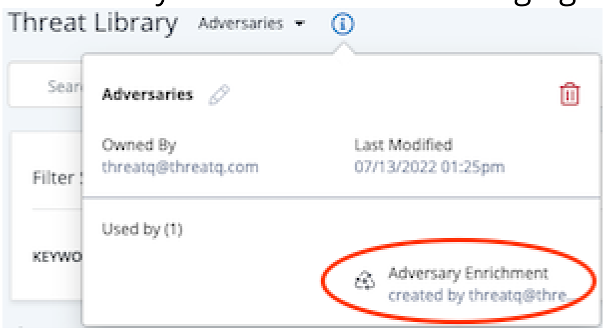
The workflow Node View allows you to complete the setup of a new workflow as well as update and run an existing workflow. From this page, you can:

- Configure a workflow
- Review a workflow’s activity log
- Enable or disable a workflow
- Delete a workflow
- Run a workflow

Tips and Tricks

- You can move the node graph to a new position on the screen by clicking and dragging any node.
- If you select a run schedule for a workflow, it must include a data collection and at least one action.
- If you do not select a run schedule for a workflow, it must include at least one action.
- A workflow that does not contain a data collection can only be used for manual workflow runs from the Threat Library results or object details pages.

- The info menu for any data collection included in a workflow, lists the workflow name in the Used by section. See the Managing Search Results topic for more information.



- If you delete a data collection associated with a workflow, the workflow is automatically disabled. You must select a new data collection for the workflow and enable the workflow before it can be run again.

Configuring a Workflow Created in TQO

After you create a workflow, you can use the workflow's Node View to further customize it by:

- Adding an action
- Updating an action
- Deleting an action
- Updating a workflow name
- Updating a workflow description
- Updating the workflow run schedule
- Selecting a data collection
- Viewing a data collection's details
- Updating workflow notification and debug options

Adding an Action

You can add up to ten actions to each workflow.

1. From the workflow's Node View tab, click the plus sign (+) below the workflow node. The Node View displays a new Run Action Node.
2. From the Run Action panel located to the right of the Node View, click the Select an Action field.
3. Use one of the following methods to select an action:
    - Type the action name in the Search field and click the action when it is displayed in the dropdown list.

- Locate and select the action from the dropdown list.

The action configuration panel displays the accepted data types and default configuration options for the action. These values are defined via the action's integration configuration page.

4. If needed, update the configuration options for the action. These options vary based on the action you select but usually include:
   - API key
   - Context filter(s)
   - Objects per run - The number of objects to be processed during a single run, regardless of the number of objects in the source data collection.

> Changes made to an action's configuration at the workflow level do not affect the action's default configuration. In addition, changes to an action's default configuration do not change existing workflow-level configurations.

5. Click the **Save Changes** button to save the action's configuration parameters. The new action node is displayed in the Node View.

Updating an Action

TQO allows you to update an action's configuration on a specific workflow as well as update an action's default configuration. You can access an action's default configuration from a workflow's action configuration panel and from the My Integrations page.

> Changes made to an action's configuration at the workflow level do not affect the action's default configuration. In addition, changes to an action's default configuration do not change existing workflow-level configurations.

To update an action's configuration options on a workflow:

1. From the workflow's Node View, click the action's node.
2. Enter your changes in the action configuration panel located to the right of the workflow's Node View.
3. Click the **Save Changes** button.

To update an action's default configuration:

1. From the workflow's Node View, click the action's node.
2. In the action configuration panel, click the ellipsis next to the action name and select the Edit Default Configuration option.

3. Enter you changes in the action's default configuration screen.
4. Click the **Save** button.
5. Click the arrow located to the left of the action name to return to your original workflow.

> Changes made to an action's default configuration are displayed when you add new instances of the action. These changes do not change existing workflow-level configurations.

Deleting an Action

If you delete all of the actions assigned to a workflow, the workflow is automatically disabled. You must add at least one action to the workflow to re-enable it.

1. From the workflow's Node View tab, click the action you want to delete.
2. From the Action panel located to the right of the Node View, click the ellipsis button next to the action name.
3. Select the **Delete Action** option
   The **Are You Sure?** window prompts you to confirm the deletion.
4. Click the **Delete Action** button.

Updating a Workflow Name

1. From the workflow's Node View tab, click the workflow node.
2. From the workflow panel located to the right of the Node View, click the workflow name field and enter your changes.
3. Click the checkmark next to the updated workflow name.
4. Click the **Save Changes** button.

Updating a Workflow Description

1. From the workflow's Node View tab, click the workflow node.
2. From the workflow panel located to the right of the Node View, click the **Edit** option next to the Description section and enter your changes.
3. Click the **Done** button below the description field.
4. Click the **Save Changes** button.

Updating the Workflow Run Schedule

When you create a workflow it defaults to a run frequency of No Schedule. Workflows set to No Schedule can be manually run from the workflow panel or the Threat Library. To automate workflow runs, you must select a data collection and a run frequency.

1. From the workflow's Node View tab, click the workflow node.
2. From the workflow panel located to the right of the Node View, click the run frequency field to select a periodic or scheduled run frequency from the dropdown list.

Periodic

SELECTION	DESCRIPTION
No Schedule	The workflow runs only when you click the Run Now button below the frequency field or when you manually trigger the workflow from the Threat Library.
Hourly	Run the workflow every hour.
Every 6 Hours	Run the workflow every six hours.
Every 24 Hours	Run the workflow every day.
Every 2 Days	Run the workflow every two days.
Every 14 Days	Run the workflow every two weeks.
Every 30 Days	Run the workflow every month.

Scheduled

SELECTION	DESCRIPTION
Daily	Allows you to run the workflow at a specific time every day.
Weekly	Allows you to run the workflow at a specific time, on a specific day, every week.

3. Click the **Save Changes** button.

Selecting a Data Collection

1. From the workflow's Node View tab, click the workflow node.
2. From the workflow panel located to the right of the Node View, click the Select a data collection field to locate and select a data collection.
3. Click the **Save Changes** button.

Viewing a Data Collection's Details

1. From the workflow's Node View tab, click the data collection node.
2. The data collection panel located to the right of the Node View lists the objects included in the data collection as well as object counts and the search parameters specified by the data collection.

> You can click the **View in Threat Library** button to view the data collection details in a new tab. If you update the data collection, you must refresh the Node View to see the changes.

Updating Workflow Notification and Debug Options

1. From the workflow's Node View tab, click the workflow node.
2. From the workflow panel located to the right of the Node View, the Settings section allows you to configure:
   - **Feed Health Notifications** - You can also enable feed health notifications for the workflow. See the Workflow Health Notifications section for more information.
   - **Debug Option** - The Debug Option checkbox gives you the option to save raw data response files for troubleshooting purposes. Since this option uses a large amount of disk space, it defaults to unchecked. We recommend temporarily enabling the option when you are troubleshooting a workflow issue.

Reviewing the Activity Log for a Workflow Created in TQO

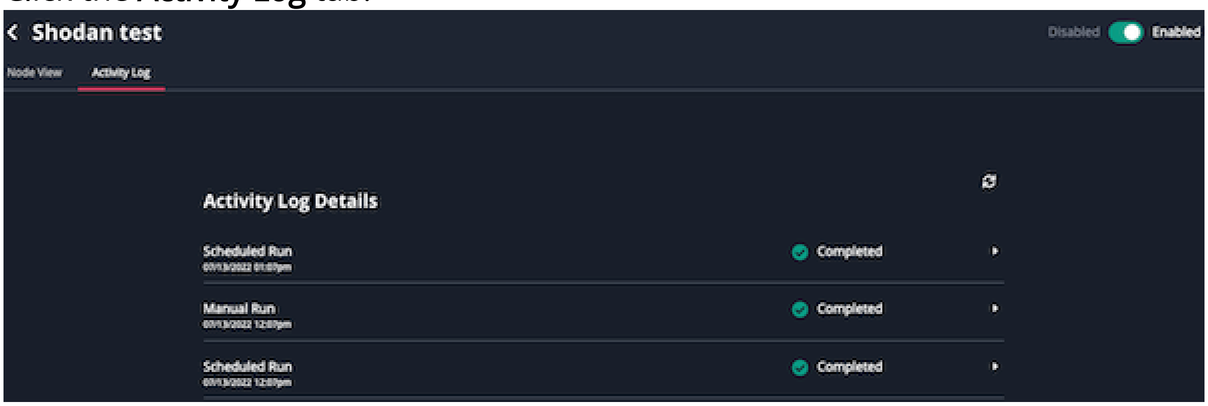
A workflow's Activity Log tab provides you with a summary of each manual or scheduled run of the workflow. This includes:

- Date/time of the run
- Run status at completion

- Data requested
- Response received
- Data enriched

In addition, the **Download Files** button allows you to download and review the error logs for any run that encountered issues.

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Locate and click the workflow to load its Node View.
3. Click the **Activity Log** tab.



4. Click the right arrow next to the run to view run details.

Enabling/Disabling a Workflow Created in TQO

You can enable and disable installed workflows from the Orchestrator page or the workflow's Node View. You cannot perform a manual or scheduled run until you enable the workflow. Disabling a workflow allows you to deactivate it without completely removing it from your instance.

> If you select a run schedule for a workflow, it must include a data collection and at least one action. If you do not select a run schedule for a workflow, it must include at least one action. A workflow configuration that does not contain a data collection can only be used for manual workflow runs from the Threat Library results or object details pages.

> When you disable a workflow during a run, the Workflow Run In Progress window warns you that you will lose any data that has not been fully ingested and prompts you to confirm your choice by clicking the **Terminate and Disable** button.

Enable/Disable Workflows - Orchestrator Page

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Click the toggle next to the workflow you want to enable/disable.
   On the Orchestrator page, Enabled workflows have a toggle with a green background. Disabled workflows have a toggle with a clear background.

Enable/Disable Workflows - Workflow Node View

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Locate and click the workflow you want to enable/disable.
   The workflow's Node View is displayed.
3. Click the **Disabled/Enabled** toggle.

Removing a Workflow Created in TQO

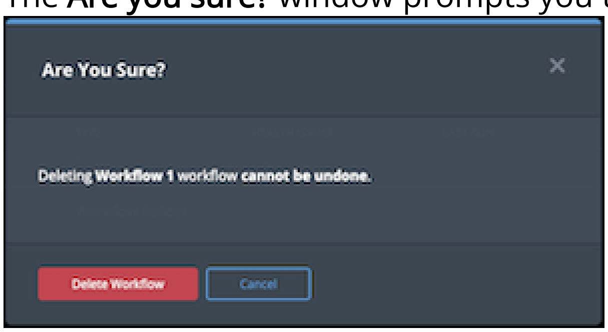
You can remove a workflow from the Orchestrator page or the workflow's Node View. Removing a workflow uninstalls it from your instance. You can also disable a workflow to deactivate it without completely removing it from your instance.

Remove Workflows - Orchestrator Page

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Click the checkbox next to the workflow you want to delete.

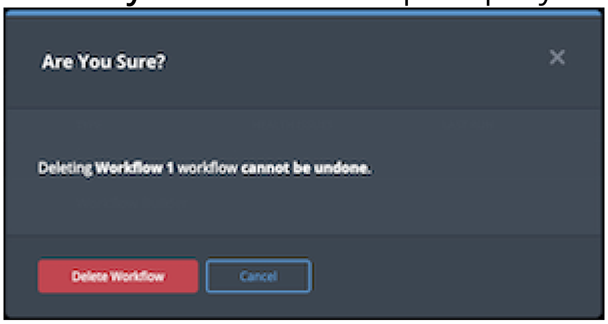
   > You can only delete one workflow at a time.

3. Click the delete button.
   The **Are you sure?** window prompts you to confirm the workflow removal.

4. Click the **Delete Workflow** button to confirm and remove the workflow.

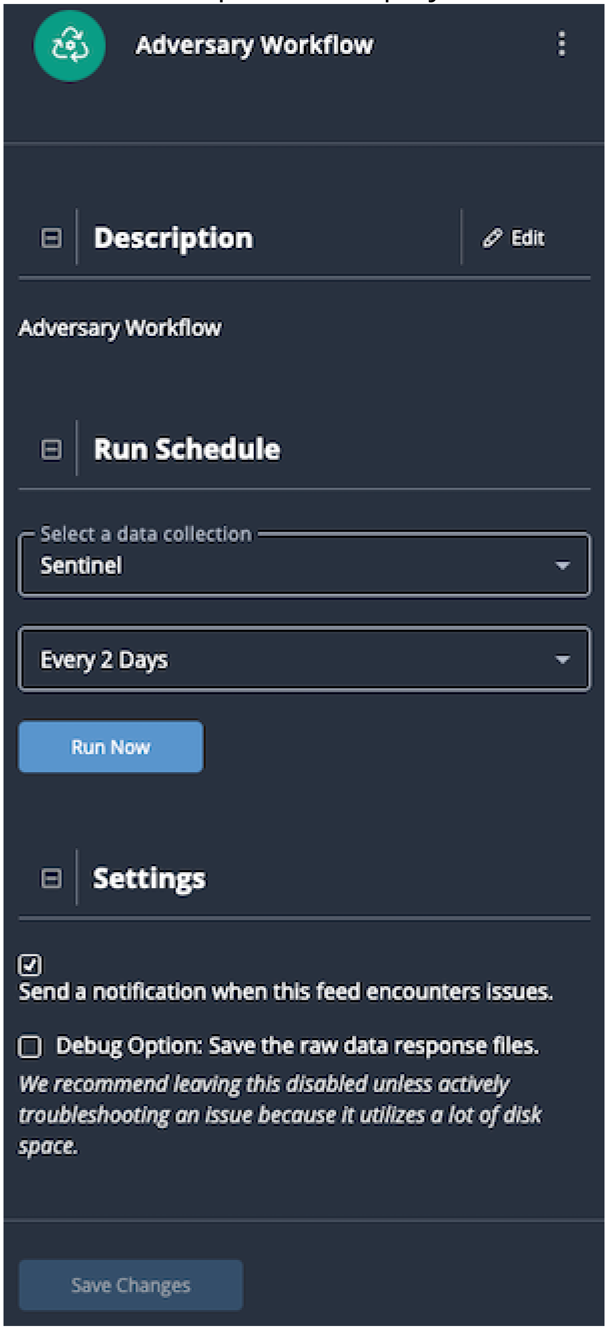
Remove Workflows - Workflow Node View

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Locate and click the workflow you want to remove.
   The workflow’s Node View is displayed.
3. Click the ellipsis button to the right of the workflow's name.
4. Select the Delete Workflow option.
   The **Are you sure?** window prompts you to confirm the workflow removal.
   

5. Click the **Delete Workflow** button to confirm and remove the workflow.

Performing a Manual Workflow Run for a Workflow Created in TQO

You must select a data collection and enable the workflow before you can perform a manual run. If the workflow already has a run in progress, the **Run Now** button is greyed out and you cannot launch a manual run.

1. From the workflow's Node View, click the workflow node.
   The Workflow panel is displayed on the right side of the page.
   

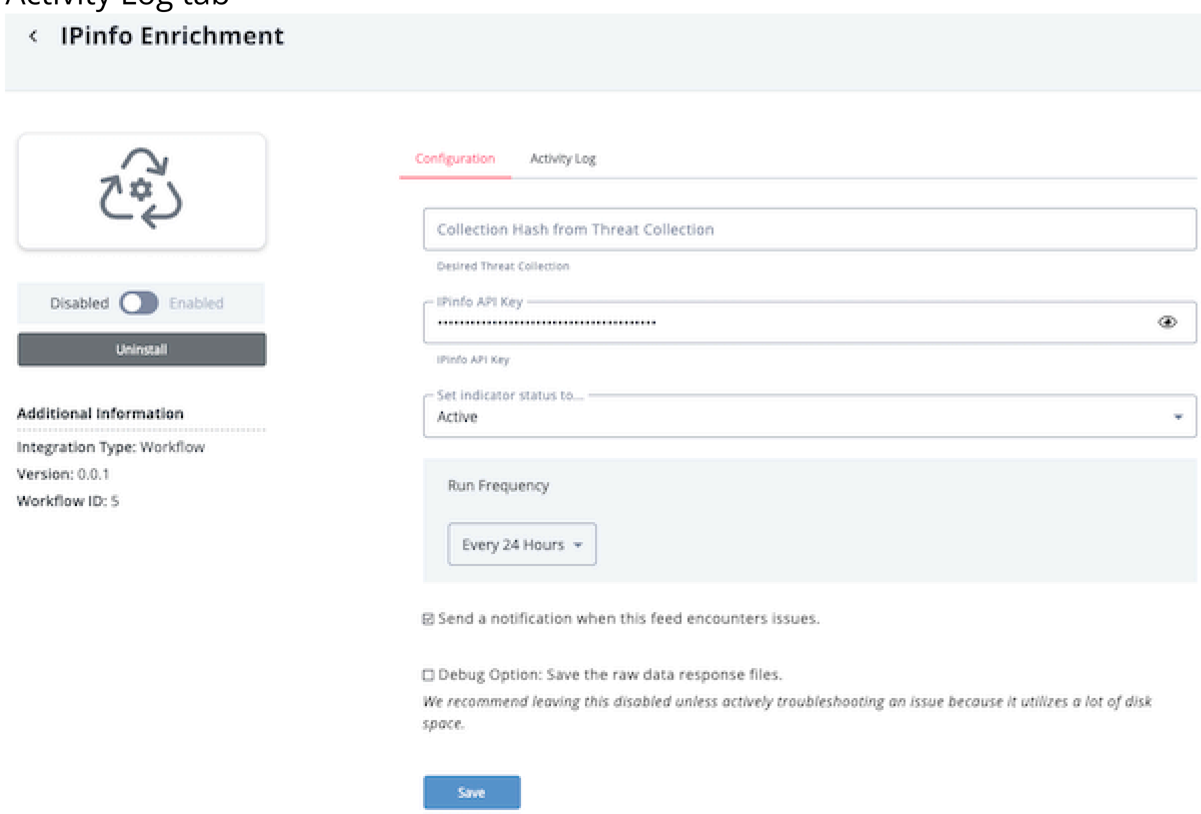
2. Click the **Run Now** button.

Managing Advanced Workflows

After you upload the YAML file for an advanced workflow, the workflow details page allows you to configure, enable, and run the workflow. In addition, the Activity Log tab in this page provides you with details for each workflow run.

> The workflow details page is available only for advanced workflows. Use the workflow node view to configure and manage workflows created in TQO.

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Locate and click the advanced workflow to load its details page.
   The workflow details page displays and lists the following:
   - Workflow details, such as the workflow version and workflow ID.
   - Configuration tab
   - Activity Log tab



3. Workflow configuration options can vary. However, most advanced workflows require the following configuration parameters:

- **Data Collection** - Click the Select a data collection field to access a drop-down list of saved data collections. This list displays all data collections you have been granted permissions for by default. You can click the **Owned by Me** tab to display only the data collections for which you have owner permissions. Use one of the following methods to select a data collection from either tab:
  - Select the data collection from the dropdown list.
  - Narrow the list by entering all or part of the data collection name. As you type, the dropdown list displays matches for your entry.

  > Adding a Data Collection to a Workflow will give all admin users read-only access to it.

- **Frequency and Default Status** - You can configure the workflow run frequency and default status the workflow assigns to system objects.

  Periodic

SELECTION	DESCRIPTION
Hourly	Run the workflow every hour.
Every 6 Hours	Run the workflow every six hours.
Every 24 Hours	Run the workflow every day.
Every 2 Days	Run the workflow every two days.
Every 14 Days	Run the workflow every two weeks.
Every 30 Days	Run the workflow every month.

  Scheduled

SELECTION	DESCRIPTION
Daily	Allows you to run the workflow at a specific time every day.

Weekly	Allows you to run the workflow at a specific time, on a specific day, every week.

- **Feed Health Notifications** - You can also enable feed health notifications for the workflow. See the Workflow Health Notifications section for more information.
- **Debug Option** - The Debug Option checkbox gives you the option to save raw data response files for troubleshooting purposes. Since this option uses a large amount of disk space, it defaults to unchecked. We recommend temporarily enabling the option when you are troubleshooting a workflow issue.

4. Click **Save**.
5. Click the **Enable/Disable** toggle to enable the workflow.

Reviewing an Advanced Workflow's Activity Log

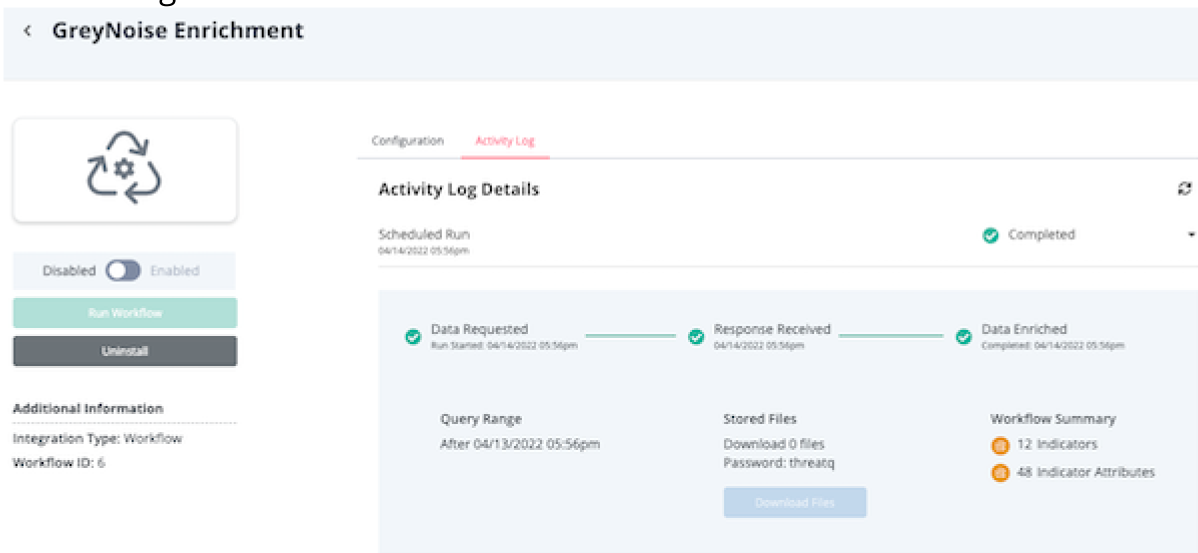
A workflow's Activity Log tab provides you with a summary of each manual or scheduled run of the workflow. This includes:

- Date/time of the run
- Run status at completion
- Data requested
- Response received
- Data enriched

In addition, the **Download Files** button allows you to download and review the error logs for any run that encountered issues.

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Locate and click the workflow to load its details page.
3. Click the Activity Log tab.

4. Click the right arrow next to the run to view run details.



Enabling/Disabling Advanced Workflows

You can enable and disable installed workflows from the Orchestrator page or the workflow's details page. Disabling a workflow allows you to deactivate it without completely removing it from your instance.

> When you disable a workflow during a run, the Workflow Run In Progress window warns you that you will lose any data that has not been fully ingested and prompts you to confirm your choice by clicking the **Terminate and Disable** button.

Enable/Disable Workflows - Orchestrator Page

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Click the toggle next to the workflow you want to enable/disable.
   On the Orchestrator page, Enabled workflows have a toggle with a green background. Disabled workflows have a toggle with a clear background.

Enable/Disable Workflows - Workflow Details Page

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Locate and click the workflow you want to enable/disable.
   The workflow's details page is displayed.
3. Click the **Disabled/Enabled** toggle.

Removing an Advanced Workflow

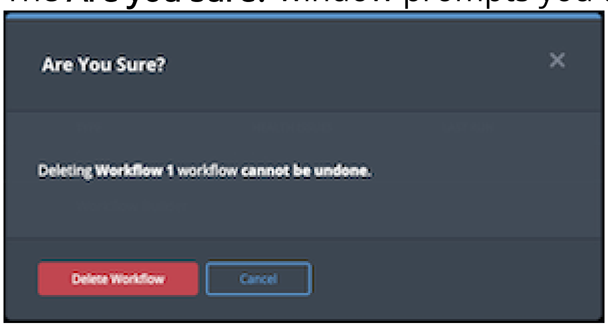
You can remove a workflow from the Orchestrator page or the workflow's details page. Removing a workflow uninstalls it from your instance. You can also disable a workflow to deactivate it without completely removing it from your instance.

Remove Workflows - Orchestrator Page

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Click the checkbox next to the workflow you want to delete.

   > You can only delete one workflow at a time.

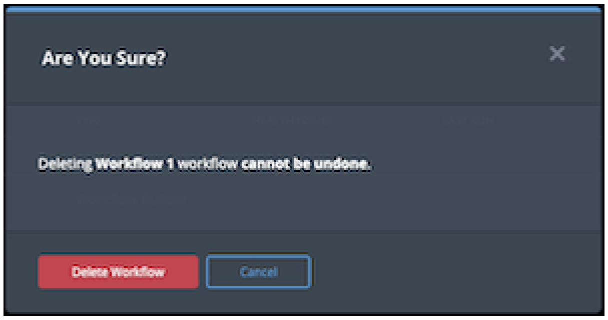
3. Click the delete button.
   The **Are you sure?** window prompts you to confirm the workflow removal.

4. Click the **Delete Workflow** button to confirm and remove the workflow.

Remove Workflows - Workflow Details Page

1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Locate and click the workflow you want to remove.
   The workflow's details page is displayed.
3. Click the Uninstall button.
   The **Are you sure?** window prompts you to confirm the workflow removal.

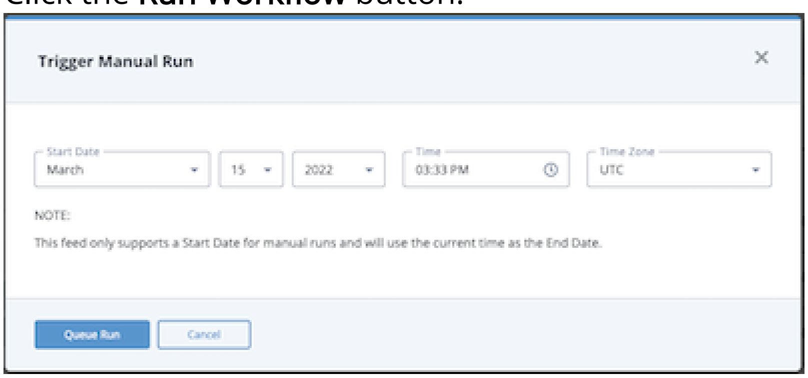


Click the **Delete Workflow** button to confirm and remove the workflow.

Performing Manual Workflow Runs for an Advanced Workflow

The **Run Workflow** button in a workflow's configuration screen gives you the option to initiate a manual run between scheduled runs.

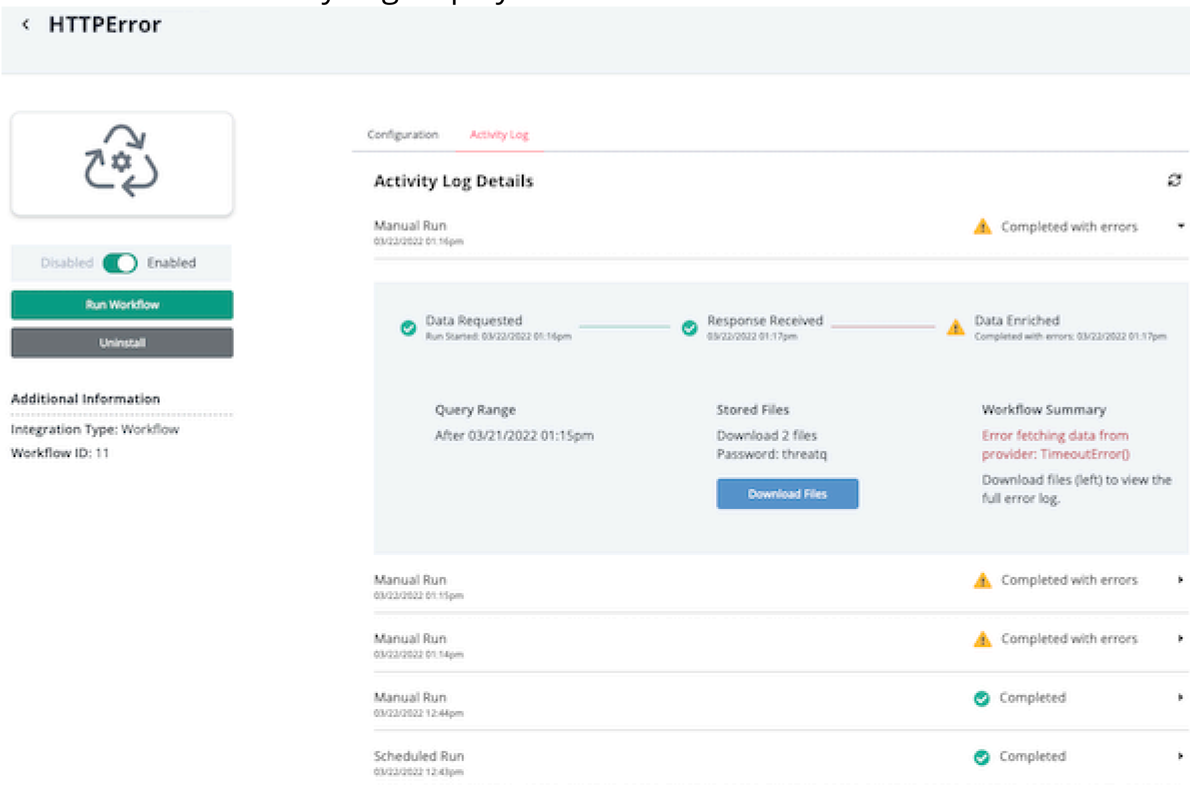
1. Click the **Orchestrator** option in the main navigation.
   The Orchestrator page lists installed workflows.
2. Locate and click the workflow you want to run.
   The workflow's details page is displayed.
3. Click the **Run Workflow** button.



4. Review and/or update the Start Date, Time and Time Zone fields. These fields default to the current date and time. When referencing a Data Collection, the Start Date value will reflect the Last Modified fields for threat objects.

> Some workflows only support a Start Date.

5. Click the **Queue Run** button.
   The workflow's Activity Log displays.



6. If the workflow encountered errors, you can click the **Download Files** button to download a zip file(s) containing the error log(s).

7. When you open the zip file(s) you are prompted to enter the Password displayed above the Download Files button.

Manually Triggered Workflows

Maintenance Account and Administrative Access users can apply a workflow created in TQO to a group of indicators from the Threat Library results page or to a single indicator from the object details page.

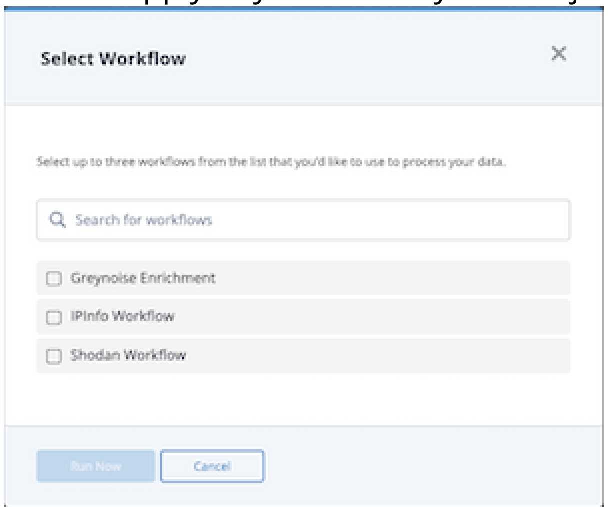
Tips and Tricks

- Only workflows created in TQO can be manually triggered from the Threat Library.
- Only Maintenance Account and Administrative Access users can access the Start Workflow button.
- The Start Workflow button is only displayed for indicator results lists and indicator object details pages.
- If you manually trigger a workflow that includes a data collection from the Threat Library, the workflow actions are applied only to the selected Threat Library object(s), not the workflow's configured data collection.

Running a Manually Triggered Workflow - Threat Library Results Page

1. Navigate to the Threat Library page.
2. Select the system objects to which you want to apply the workflows by searching or filtering the Threat Library or by selecting a Data Collection.
3. Click the  (start workflow) button.
4. Click the object type you want to work with.

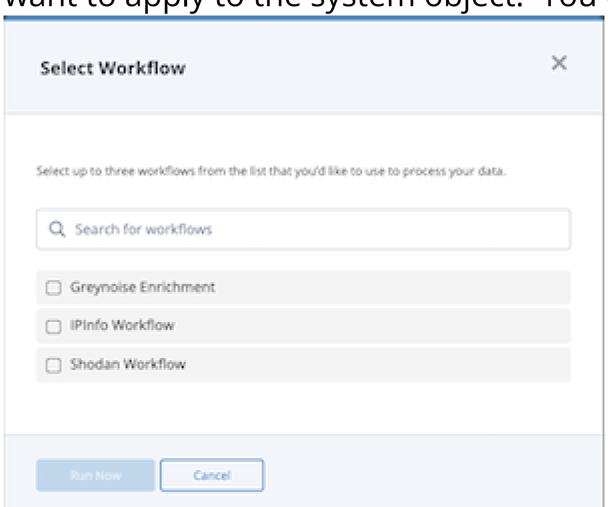
5. From the Select Workflow window locate and check the box next to each workflow you want to apply to your list of system objects. You can select up to three workflows.



6. Click the **Run Now** button.
   You can access each workflow's Activity Log to view the results of the manual run.

Running a Manually Triggered Workflow - Object Details Page

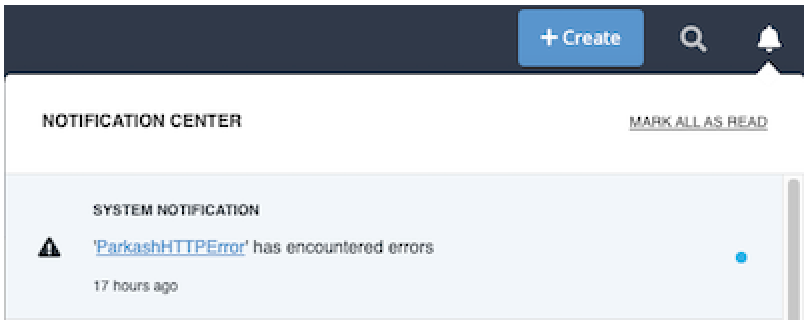
1. Navigate to the system object's object details page.
2. Click the Actions button.
3. Click the  (start workflow) button.
4. From the Select Workflow window locate and check the box next to each workflow you want to apply to the system object. You can select up to three workflows.



5. Click the **Run Now** button.
   You can access each workflow's Activity Log to view the results of the manual run.

Workflow Health Notifications

Workflow Health Notifications allow the ThreatQ application to send you, and other designated users, email and in-app notifications when a workflow encounters an issue. The in-app notifications appear in Notification Center for users with an administrator or maintenance account. These notifications include a link that redirects you to the Activity Log tab for the workflow.



The emails contain useful information such as connection information, data ingested, and an ingestion summary. See the Notifications topic for more information.

Change Log

- **Version 1.3.0**
  - Updates for version 5.14.0. Added information on manually triggered workflows.
- **Version 1.2.0**
  - Updates for version 5.12.0
- **Version 1.1.0**
  - Updates for version 5.8.0
- **Version 1.0.0**
  - Initial Release