

ThreatQuotient



ThreatQ TDR Orchestrator User Guide

Version 2.1.0

July 20, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	4
About ThreatQ Orchestrator	5
Data-Driven Triggers	5
Configuration-Driven Workflows (CDWs)	5
Capture Enriched Data	6
Requirements	7
Components	8
About the Orchestrator Page	12
Accessing the Orchestrator Page	13
Actions	14
About Actions	14
Quick Notes	16
Installing an Action	17
Configuring an Action	20
Deleting an Action	23
Workflows	25
About Workflows	25
About Manually Triggered Workflows	26
Running a Manually Triggered Workflow - Threat Library Results Page	26
Running a Manually Triggered Workflow - Object Details Page	27
Building a Workflow	29
Modifying a Workflow	35
Changing the Data Collection	35
Updating a Workflow's Run Frequency	37
Enabling Debug Option	38
Changing an Action in a Workflow	40
Updating an Action's Configuration for a Specific Workflow	41
Updating an Action's Default Configuration from the Workflow Builder	43
Performing Manual Workflow Runs	46
Viewing the Activity Log	47
Activity Log Details	48
Deleting a Workflow	50
Deleting a Workflow from the Workflow Builder	50
Deleting a Workflow from the Orchestrator Landing Page	51
Advanced Workflows	52
About Advanced Workflows	52
Important Notes	53
Installing an Advanced Workflow	54
Configuring an Advanced Workflow	56
Performing Manual Workflow Runs	59
Viewing the Activity Log	63
Activity Log Details	64

Deleting an Advanced Workflow.....	67
Deleting from the Orchestrator Page.....	67
Deleting from the Advanced Workflow Details Page.	67
Workflow Notifications.....	69
Tips and Tricks.....	70
Change Log	71

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.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

About ThreatQ Orchestrator

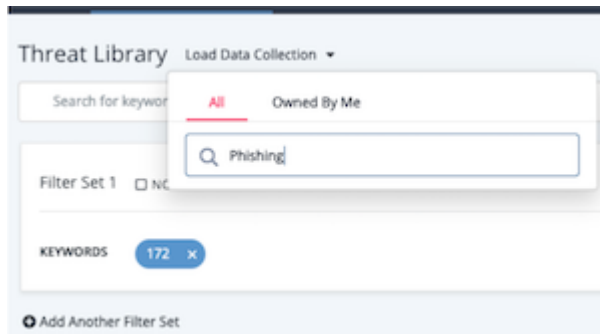
ThreatQ TDR Orchestrator includes enhanced automation, analysis and reporting capabilities that accelerate threat detection and response across disparate systems.

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 what 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.



Configuration-Driven Workflows (CDWs)

CDWs, 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.

< GreyNoise Enrichment



Disabled ☒ Enabled

Workflow ID: 11

Configuration

Collection: Hash from Threat Collection

Download: Download

GreyNoise API Key:

GreyNoise API Key:

Get indicator status to: Active

Run Frequency: Every 24 Hours

Send a notification when this feed encounters issues.

Setting Option: Save the raw data response files. We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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

Add Workflow

Create Upload

Name

The following characters are not permitted in the workflow name: # , ! , [

Description (optional)

Provide the data that you'd like to process with this workflow


Select a data collection

Create Cancel

Capture Enriched Data

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

< GreyNoise Enrichment



Disabled ☒ Enabled

Workflow ID: 11

Configuration

Activity Log

Activity Log Details

Scheduled Run: Completed

Query Range: After 04/12/2022 00:00pm

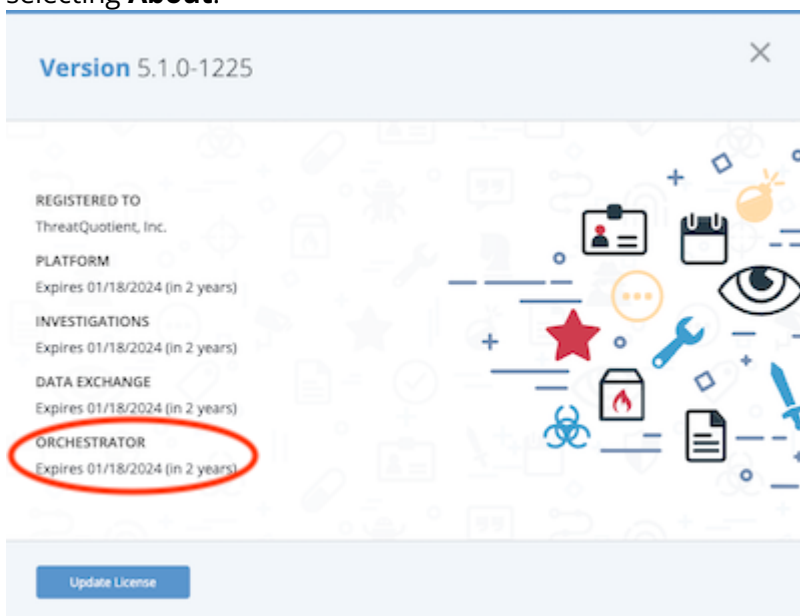
Download: Download

Workflow Summary: 11 Indicators, 48 Indicator Attributes

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
- An admin or maintenance user login

Components

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

COMPONENT/ TERM

DEFINITION

Action

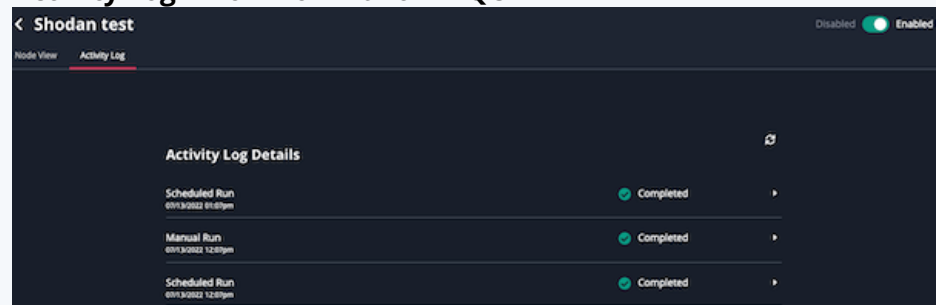
Actions are YAML snippets you can use to enrich the data specified by your workflow's data collection. TQO includes pre-seeded actions and allows you to install additional ones. See the [About Actions](#) topic for more information about actions.

Activity Log

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:

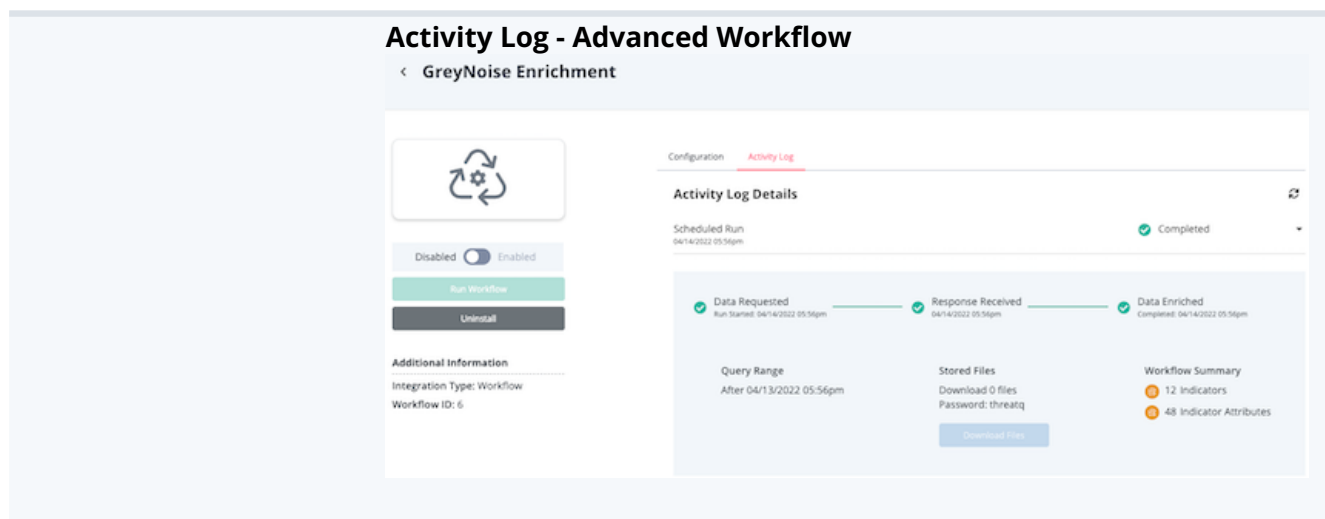
- Date/time of the run
- Run status at completion
- Data requested
- Response received
- Data enriched

Activity Log - Workflow Built in TQO



COMPONENT/ TERM

DEFINITION



Configuration Driven Workflow (CDW)/Workflow

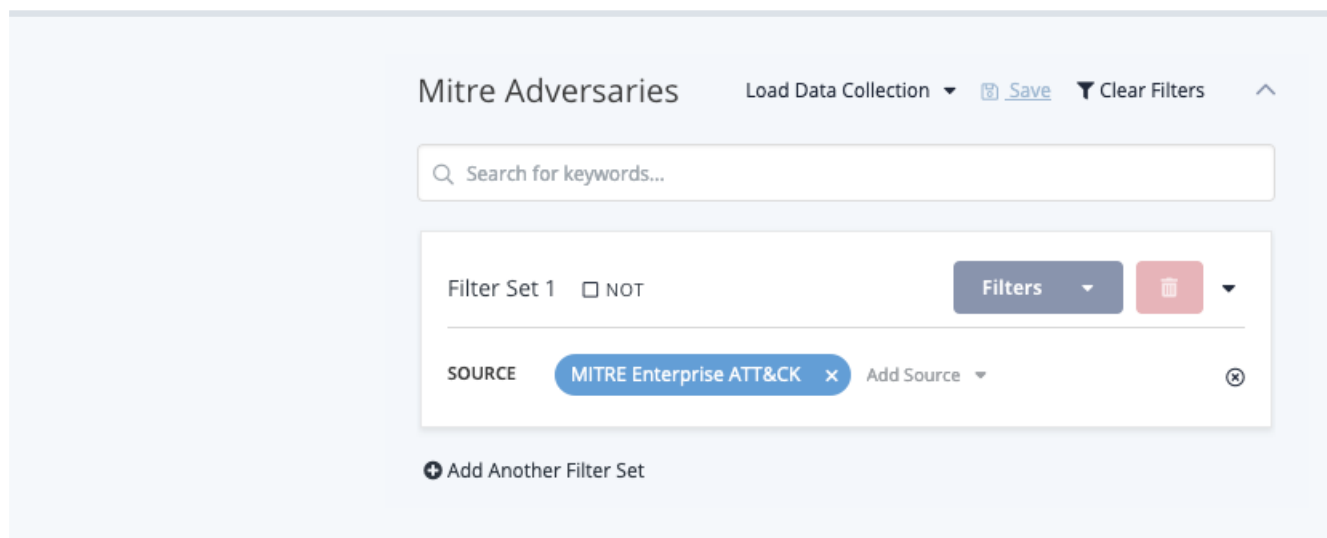
Configuration Driven Workflows (CDWs), also known as Data-Driven Playbooks, take your identified triggers, in the form of Data Collections, and enrich your selected threat intelligence data using third-party providers such as Rapid7, to curate further detailed threat information.

There are two types of workflows:

- **Standard Workflows** - workflows built within the Workflow Builder using installed Actions. These workflows can also be [run from the Threat Library and an object's details page](#).
- **Advanced Workflows** - preconfigured workflows, developed by ThreatQ Professional Services, that have been written to include all required actions and the data enrichment processes. Advanced Workflows are designed to be installed (required actions and workflow) via a single YAML file in the ThreatQ UI installer.

Data Collection

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

**COMPONENT/
TERM****DEFINITION****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 click on a node to view and/or update its configuration details.

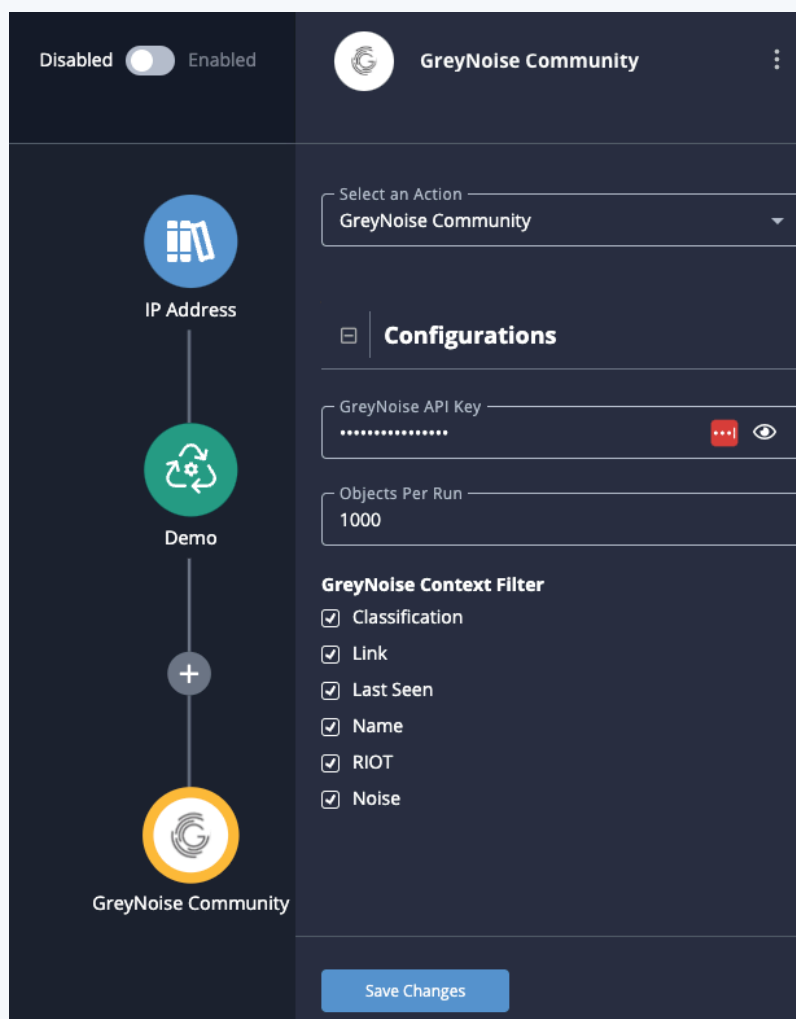
**Node View**

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.

COMPONENT/ TERM

DEFINITION

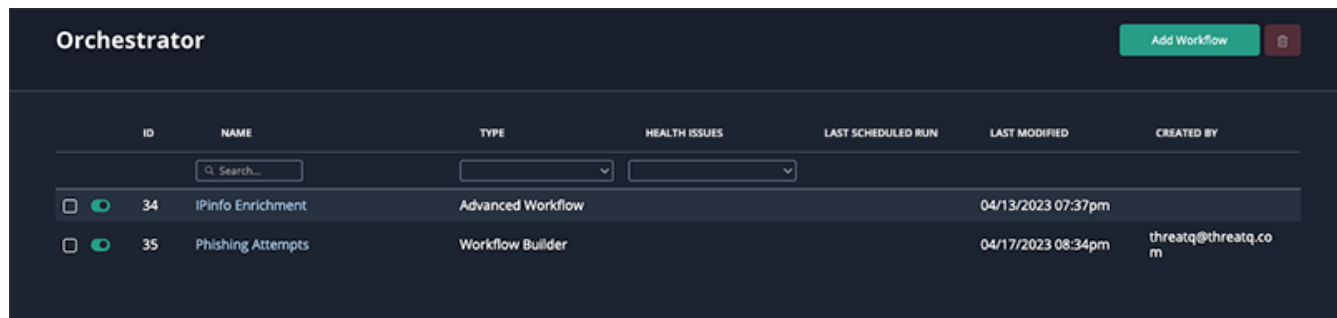
From the Node View you can click the various workflow nodes, such as data collection, workflow, or action nodes, and view or update each node's settings.





About 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.

Your workflows, both built within TQO and installed Advanced workflows, are displayed in an information table on the landing page.



The screenshot shows the 'Orchestrator' page with a dark theme. At the top right is a green 'Add Workflow' button and a trash icon. Below the header is a table with columns: ID, NAME, TYPE, HEALTH ISSUES, LAST SCHEDULED RUN, LAST MODIFIED, and CREATED BY. There are search and filter dropdowns for the NAME and TYPE columns. Two workflows are listed: ID 34, 'IPInfo Enrichment' (Advanced Workflow, last run 04/13/2023 07:37pm) and ID 35, 'Phishing Attempts' (Workflow Builder, last run 04/17/2023 08:34pm, created by threatq@threatq.com).

ID	NAME	TYPE	HEALTH ISSUES	LAST SCHEDULED RUN	LAST MODIFIED	CREATED BY
<input type="checkbox"/> 	34 IPInfo Enrichment	Advanced Workflow		04/13/2023 07:37pm		
<input type="checkbox"/> 	35 Phishing Attempts	Workflow Builder		04/17/2023 08:34pm		threatq@threatq.com

COLUMN

DESCRIPTION

ID The unique ID associated with the workflow.

Name The name of the workflow. You can use the search provided below the header to filter your workflow list by the workflow name.

Type The type of workflow. You can filter the workflow list use the column's dropdown list. Options include:

- Workflow Builder
- Advanced Workflow

Health Issues This column displays the current health of a workflow. You can filter the workflow list using the dropdown provided. Filter options include:

- Healthy
- Unhealthy

Last Scheduled Run The date stamp when the scheduled workflow was last run.

COLUMN

DESCRIPTION

Last Modified

The date stamp of when the workflow was last modified.

Created By

The user that created the workflow. This column will only be populated for workflows built within the workflow builder.



Accessing the Orchestrator Page

1. Click the **Orchestrator** icon in the top navigation bar.

The Orchestrator page will load.

Orchestrator

Add Workflow

ID	NAME	TYPE	HEALTH ISSUES	LAST SCHEDULED RUN	LAST MODIFIED	CREATED BY
	<input type="text" value="Search..."/>	<input type="text" value=""/>	<input type="text" value=""/>			
<input type="checkbox"/> 	34 IPInfo Enrichment	Advanced Workflow			04/13/2023 07:37pm	
<input type="checkbox"/> 	35 Phishing Attempts	Workflow Builder			04/17/2023 08:34pm	threatq@threatq.com

2. Click the **Add Workflow** button to begin your [building workflows](#) in workflow builder or [installing Advanced Workflows](#).

Actions

About Actions

Actions are YAML snippets you can use to enrich the data specified by your workflow's data collection. Actions are not designed to run by themselves but instead be inserted into your enrichment workflows.

< IPinfo



Uninstall

Additional Information

Integration Type: Action

Version: 1.0.1

Action ID: 2

Accepted Data Types:

Configuration

IPinfo API Key



Enter your IPinfo API Key.

IPinfo Objects Per Run

10000

IPinfo Objects Per Run

Context Filter

Select which pieces of context you want to bring into ThreatQ

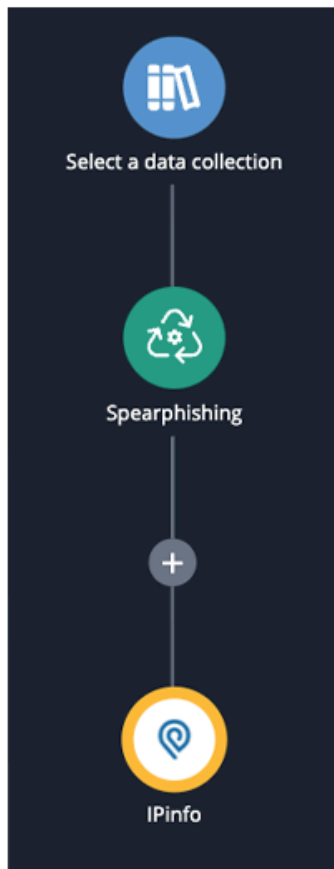
☒ Location coordinates

☒ City

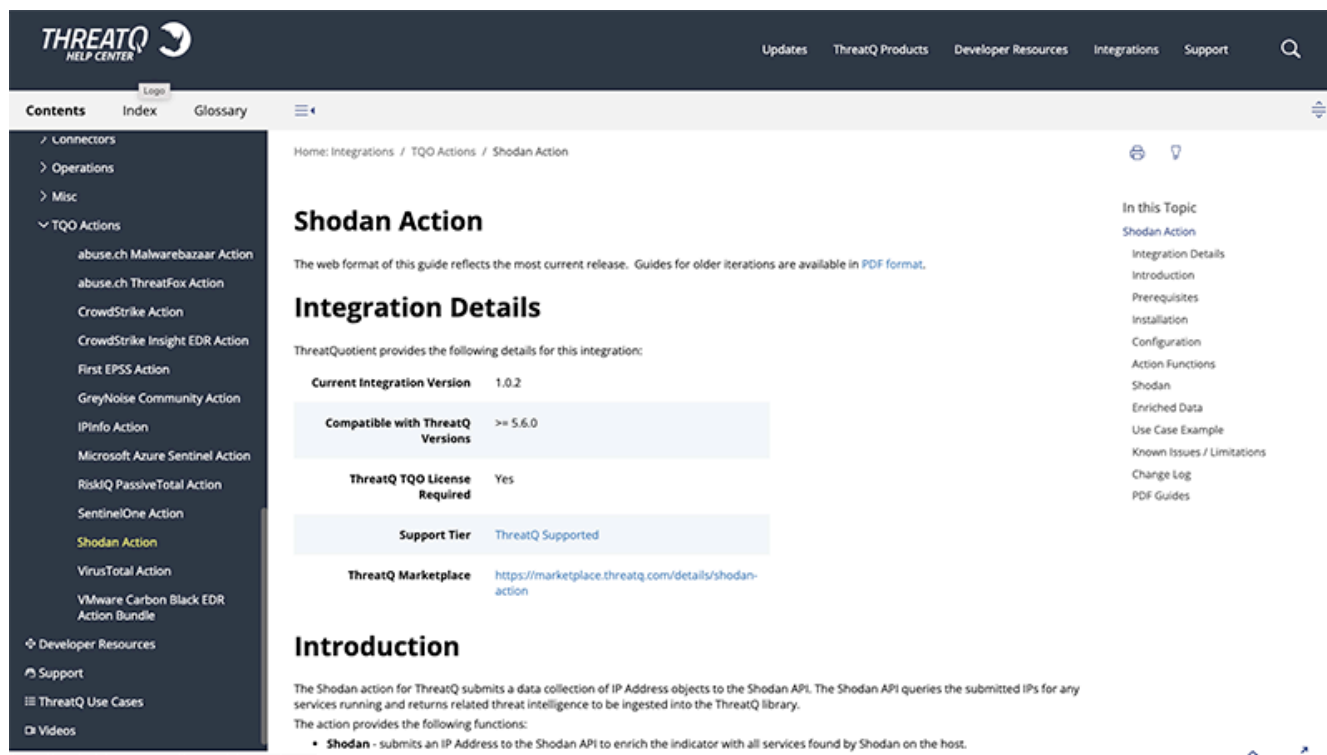
☒ Country

☒ Region

Save



ThreatQuotient highly recommends reviewing an action's user guide before downloading and installing the action. See the Integrations section for those guides - both in web and PDF format.



THREATQ HELP CENTER

Updates ThreatQ Products Developer Resources Integrations Support

Contents Index Glossary

Log in

Home: Integrations / TQO Actions / Shodan Action

Shodan Action

The web format of this guide reflects the most current release. Guides for older iterations are available in [PDF format](#).

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.2
Compatible with ThreatQ Versions	>= 5.6.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/shodan-action

Introduction

The Shodan action for ThreatQ submits a data collection of IP Address objects to the Shodan API. The Shodan API queries the submitted IPs for any services running and returns related threat intelligence to be ingested into the ThreatQ library.

The action provides the following functions:

- Shodan** - submits an IP Address to the Shodan API to enrich the indicator with all services found by Shodan on the host.

In this Topic

- Shodan Action
- Integration Details
- Introduction
- Prerequisites
- Installation
- Configuration
- Action Functions
- Shodan
- Enriched Data
- Use Case Example
- Known Issues / Limitations
- Change Log
- PDF Guides

Quick Notes

- Actions can be download from the ThreatQ Marketplace - <https://marketplace.threatq.com> .
- Actions with the term "bundle" in the name contain multiple actions.
- Actions can be installed by uploading the zip file itself to the ThreatQ platform.



Refer to the action's user guide for details. Some action zip files contain custom objects that are required to run the action. Those custom objects cannot be installed using the ThreatQ UI installer.

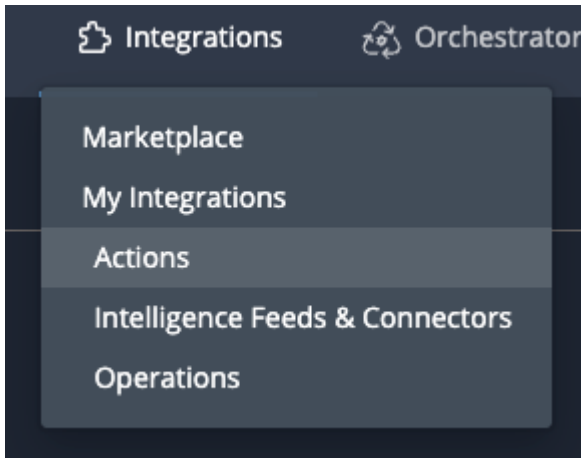
- Actions are automatically enabled upon installation and cannot be disabled.
- The configuration settings set for an action will be applied when inserting it into a workflow. You can [change an action's configuration settings for a specific workflow](#) or the [default configuration settings](#).



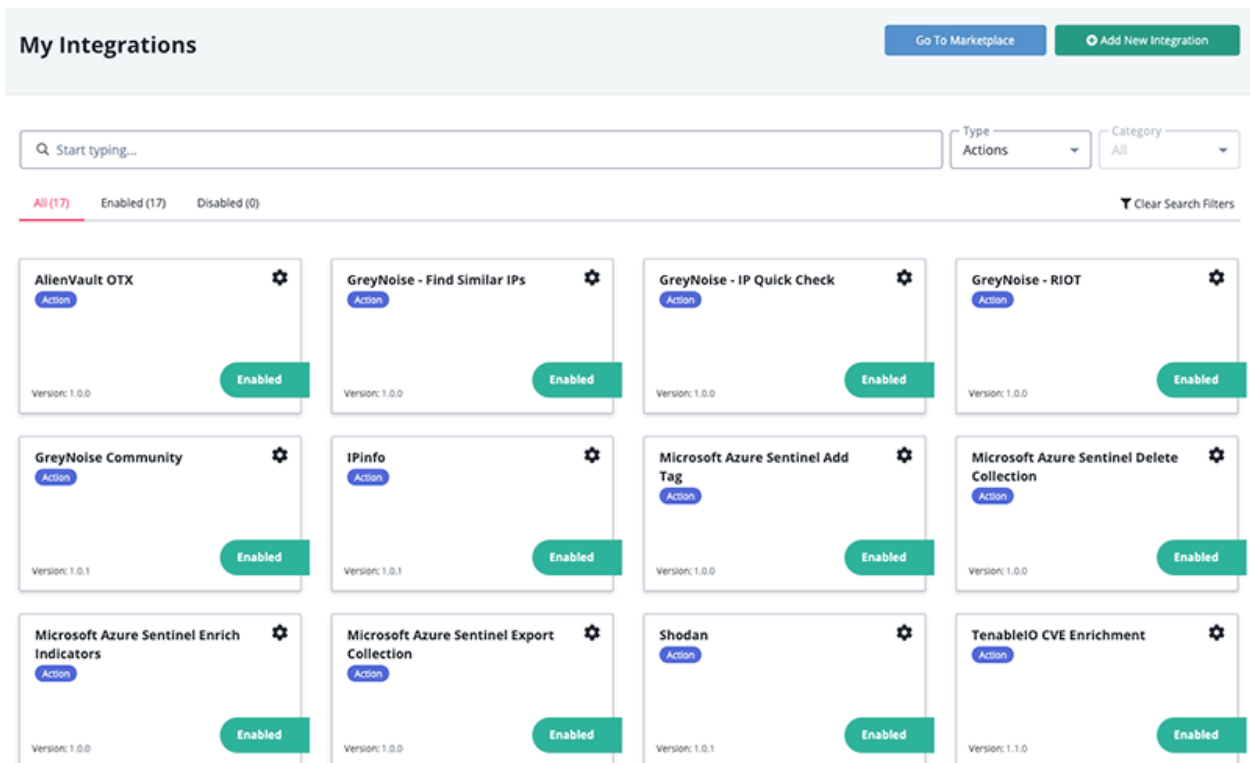
Updating the default configurations for an action will not update any instances of the action that has already been deployed in a workflow.

Installing an Action

1. Download the action zip file from the ThreatQ Marketplace.
2. Click on the Integrations navigation heading and select **Actions**.

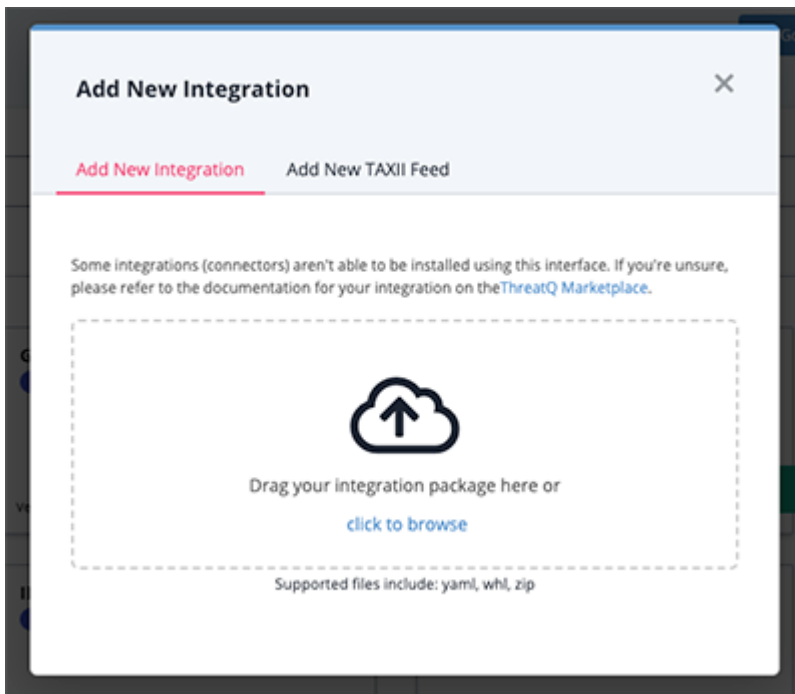


The My Integrations page will load with the list filtered down to actions.

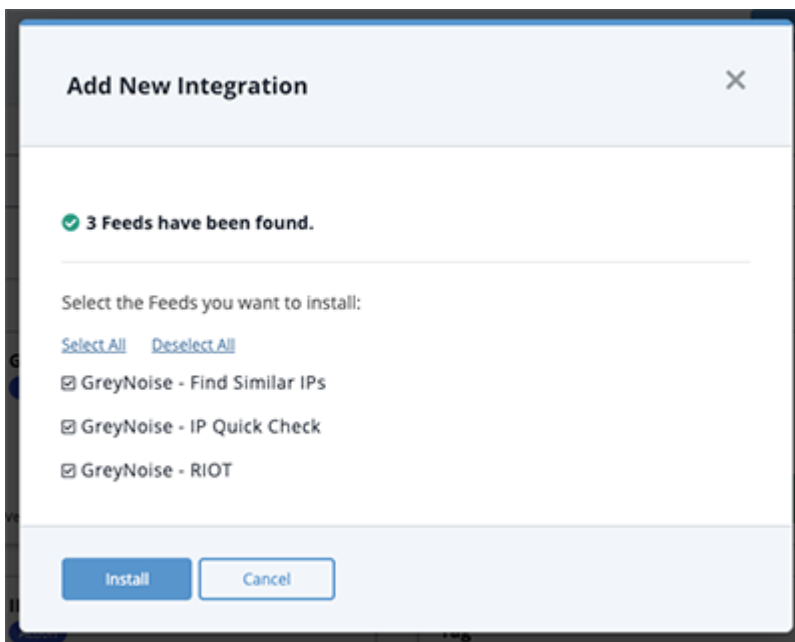


3. Click on the **Add New Integration**.

The Add New Integration dialog box will open.



4. Upload the action zip file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the action zip file on your local machine
5. Select which actions to install, if prompted, and click on **Install**.




ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

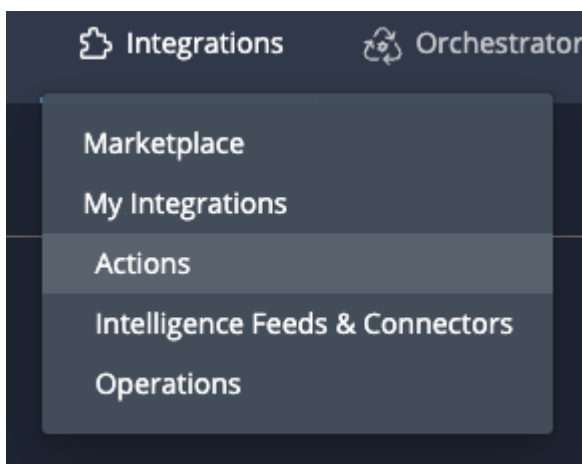
The action(s) will now be installed on your instance. While actions are automatically enabled by default, you will still need to [configure the action's default settings](#).

Configuring an Action

You can configure an action's default settings from its details page under the My Integrations page. This allows you to set common parameters, such as API Keys, that will be used within any workflow you insert the action into.

 Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must [update the action's configurations within the workflow itself](#).

1. Click on the Integrations navigation heading and select **Actions**.



The My Integrations page will load with the list filtered down to actions.

My Integrations

Type
Actions

Category
All

All (17) Enabled (17) Disabled (0)

Clear Search Filters

<div> AllenVault OTX </div> <div> Version: 1.0.0 </div> <div> Enabled </div>	<div> GreyNoise - Find Similar IPs </div> <div> Version: 1.0.0 </div> <div> Enabled </div>	<div> GreyNoise - IP Quick Check </div> <div> Version: 1.0.0 </div> <div> Enabled </div>	<div> GreyNoise - RIOT </div> <div> Version: 1.0.0 </div> <div> Enabled </div>
<div> GreyNoise Community </div> <div> Version: 1.0.1 </div> <div> Enabled </div>	<div> IPinfo </div> <div> Version: 1.0.1 </div> <div> Enabled </div>	<div> Microsoft Azure Sentinel Add Tag </div> <div> Version: 1.0.0 </div> <div> Enabled </div>	<div> Microsoft Azure Sentinel Delete Collection </div> <div> Version: 1.0.0 </div> <div> Enabled </div>
<div> Microsoft Azure Sentinel Enrich Indicators </div> <div> Version: 1.0.0 </div> <div> Enabled </div>	<div> Microsoft Azure Sentinel Export Collection </div> <div> Version: 1.0.0 </div> <div> Enabled </div>	<div> Shodan </div> <div> Version: 1.0.1 </div> <div> Enabled </div>	<div> TenableIO CVE Enrichment </div> <div> Version: 1.1.0 </div> <div> Enabled </div>

2. Click the action to configure to open its details page.

The Action Details page will load.

GREYNOISE

Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 20

Accepted Data Types:

Configuration

API Key

GreyNoise API Key.

Context Filter

The pieces of Context to ingest back into ThreatIQ.

☒ RiOT

☒ Category

☒ Service Name

☒ Trust Level

☐ External Reference

☐ Last Updated

RiOT IP Status

Whitelisted

The status of the IPs that are within the RiOT dataset.

Non-RiOT IP Status

Review

The status of the IPs that are NOT within the RiOT dataset.

Objects Per Run

10000

The max number of objects to send to this action, per run. This number should scale with your API rate limit.

3. Enter your configuration settings and click on **Save**.

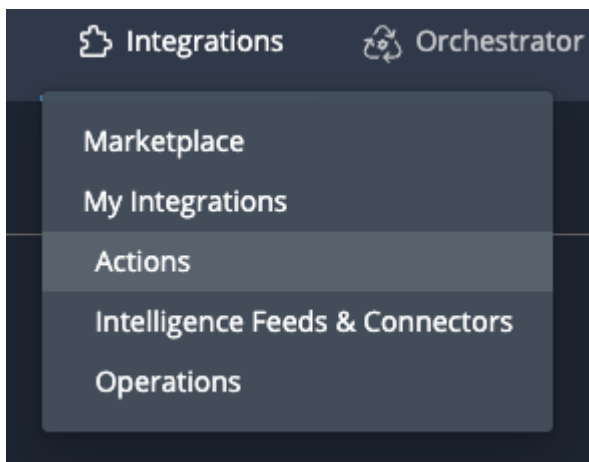


Specific configurations will differ based on the action used. See the action's individual user guide for more information.

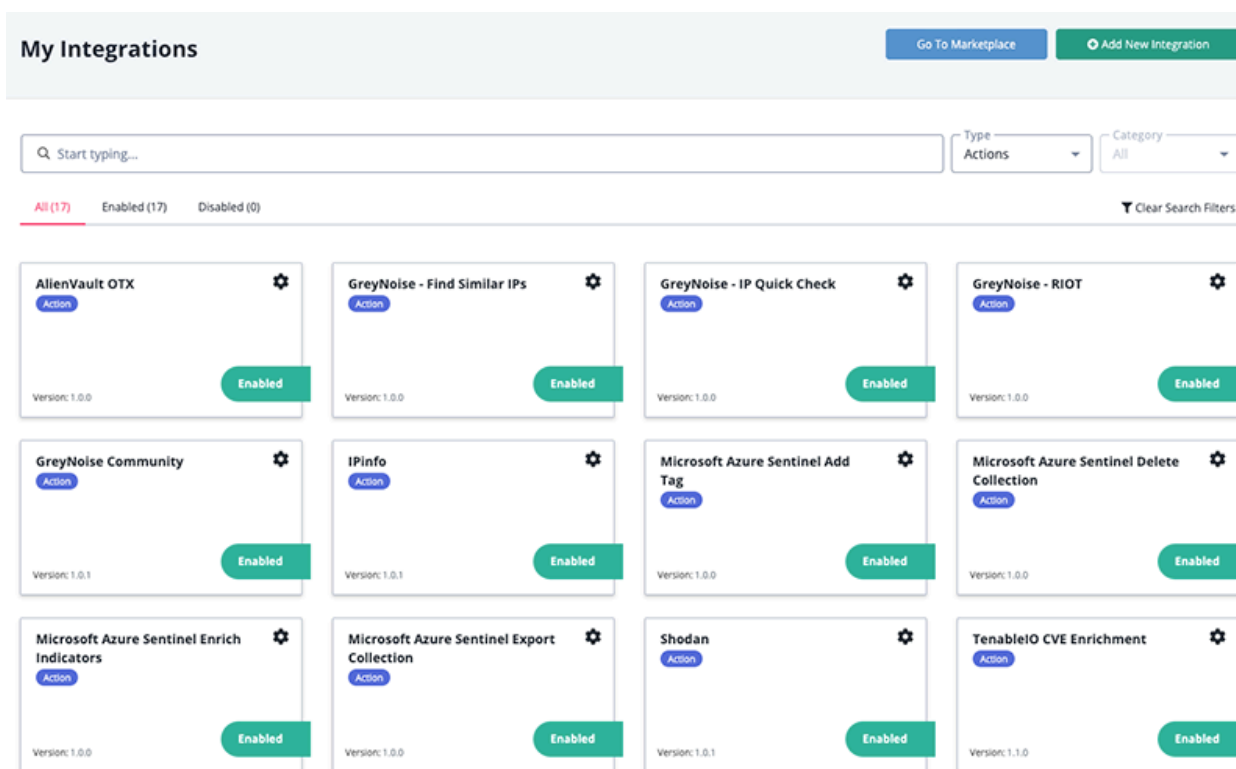
Deleting an Action

You can delete an action from its details page if it is not currently associated with a workflow. Deleting an action will not delete the data that has already been ingested by the ThreatQ platform.

1. Click on the Integrations navigation heading and select **Actions**.



The My Integrations page will load with the list filtered down to actions.



2. Click the action to configure to open its details page.

The Action Details page will load.

GREYNOISE

Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 20

Accepted Data Types:

Configuration

API Key

GreyNoise API Key.

Context Filter

The pieces of Context to ingest back into ThreatQ.

☒ RIOT

☒ Category

☒ Service Name

☒ Trust Level

☐ External Reference

☐ Last Updated

RIOT IP Status

Whitelisted

The status of the IPs that are within the RIOT datasets.

Non-RIOT IP Status

Review

The status of the IPs that are NOT within the RIOT dataset.

Objects Per Run

10000

The max number of objects to send to this action, per run. This number should scale with your API rate limit.

3. Click on the **Uninstall** button located below the action's logo.



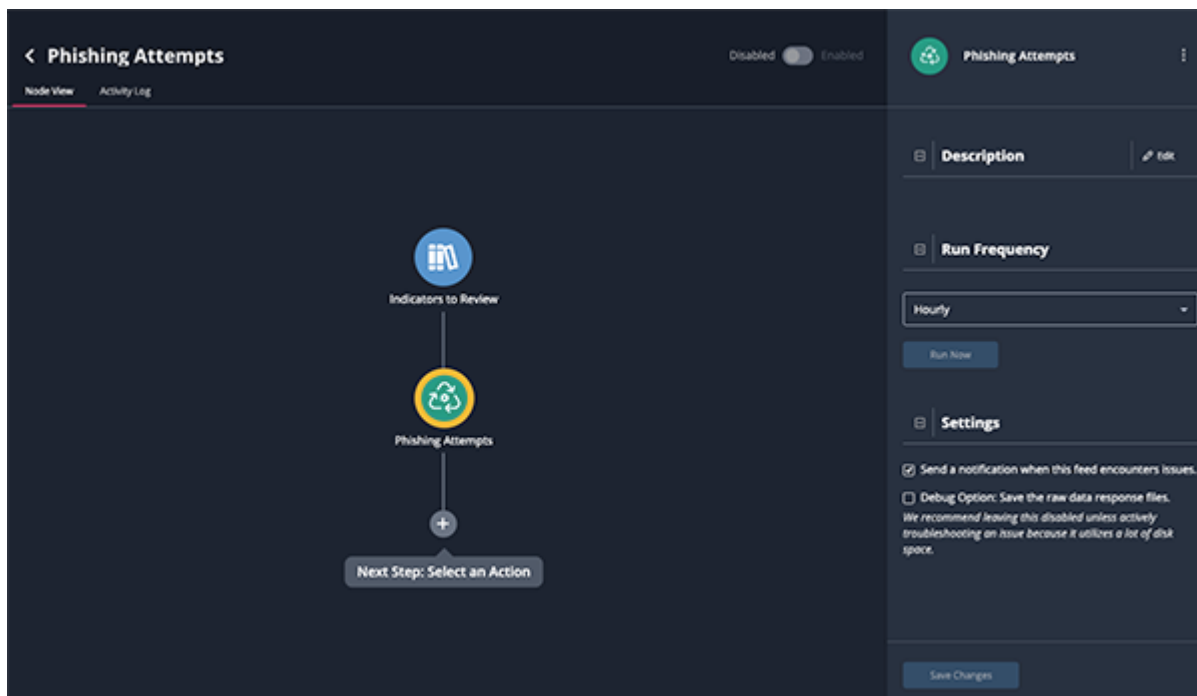
If the Uninstall button is grey out, the action is currently being used by a workflow. Locate the workflow using this action and remove the action.

4. Click on **Uninstall Action**, when prompted, to remove the action from your instance.

Workflows

About Workflows

Workflows take your identified triggers, in the form of Data Collections, and enrich your selected threat intelligence data using Actions, third-party providers such as Rapid7, to curate further detailed threat information.



Workflows can be triggered by the following:

- Workflow's Run Schedule.
- [Manually Running the workflow](#) from the builder page via the **Run Now** button.
- Performing a [Manually Triggered Workflow](#) run from the Threat Library or object details page.

The TQO workflow builder provides you with a visual representation of how your Threat Library data collection and action are utilized. The interface allows you to configure how an action is run, including what enriched context the action will ingest, the frequency of runs, and summaries of each run.

The following is required to build a workflow:

- A TQO License.
- A ThreatQ Data Collection.
- A [TQO Action](#) installed on your ThreatQ instance. TQO Actions can be downloaded from the [ThreatQ Marketplace](#).

About Manually Triggered Workflows

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



Running a workflow from the Threat Library or object details page will ignore any data collection set in the workflow's configuration for the object(s) you have selected.

Important Notes:

- 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. You can further customize by checking the checkbox next to each object you want to include.

- Click the (start workflow) button.

VALUE	TYPE	DATE CREATED	LAST MODIFIED	STATUS	SCORE	EXPIRATION
118.195.198.108	IP Address	07/05/2023 12:03pm	07/05/2023 01:00pm	Whitelisted	0	
xidekubitavepo.foaptoa.com	FQDN	07/05/2023 11:31am	07/05/2023 01:00pm	Whitelisted	0	
djezoxafupib.yubit.co.za	FQDN	07/05/2023 11:31am	07/05/2023 01:00pm	Whitelisted	0	
gufnegagarudin.yoyep.co.za	FQDN	07/05/2023 11:31am	07/05/2023 11:31am	Whitelisted	0	
kuzojogikeratel.joopsoa.com	FQDN	07/05/2023 11:31am	07/05/2023 11:31am	Whitelisted	0	

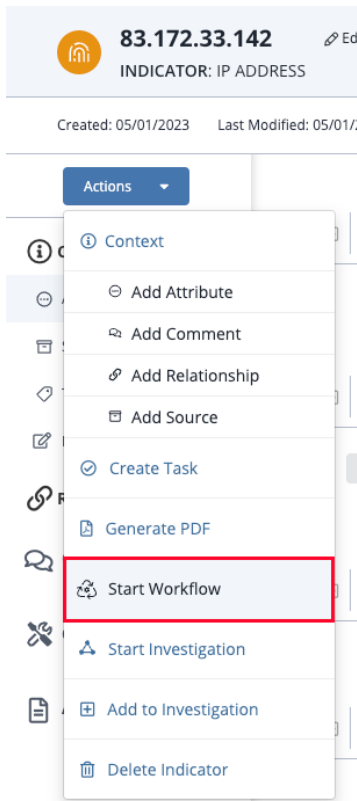
- Select the object type you want to work with.
- From the Select Workflow window locate and check the box next to each workflow you want to apply to your list of system objects. You can select up to three workflows.

- Click the **Run Now** button.
You can access each workflow's [Activity Log](#) to view the results of the manual run.

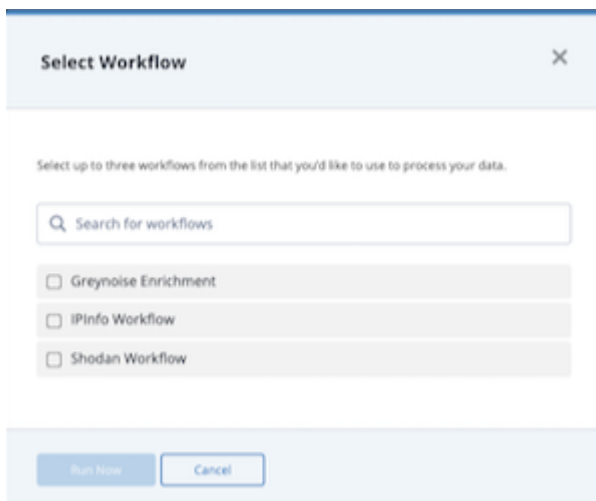
Running a Manually Triggered Workflow - Object Details Page

- Navigate to the system object's object details page.

- Click the **Actions** button and select the **Start Workflow** option.



- 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.



- Click the **Run Now** button.

You can access each workflow's [Activity Log](#) to view the results of the manual run.

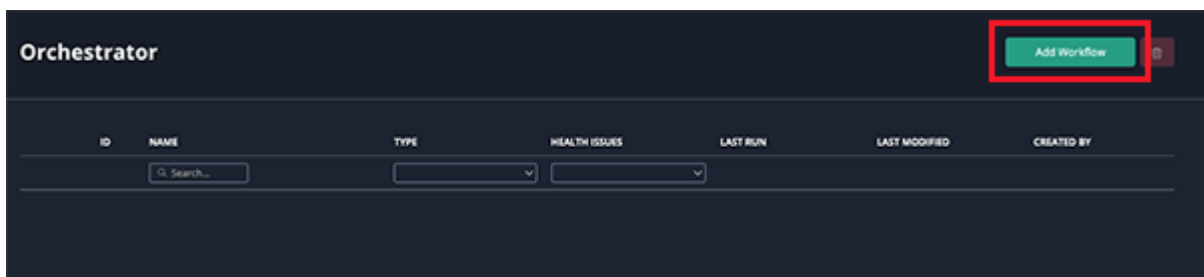
Building a Workflow

The workflow builder allows you to create your own workflows using data collections and installed TQO Actions, which are available on the [ThreatQ Marketplace](#).



Manually Triggered Workflows do not require a set data collection as the data is selected from the Threat Library. In the event that a workflow with a set data collection is selected as the Manually Triggered Workflow, the object or Threat Library selection will be used instead of the set data collection.

1. Navigate to the ThreatQ Orchestrator page.
2. Click on the **Add Workflow** button.



The Add Workflow dialog window will open.

Add Workflow [X]

Create Upload

Name


Description (optional)

Provide the data that you'd like to process with this workflow

Select a data collection

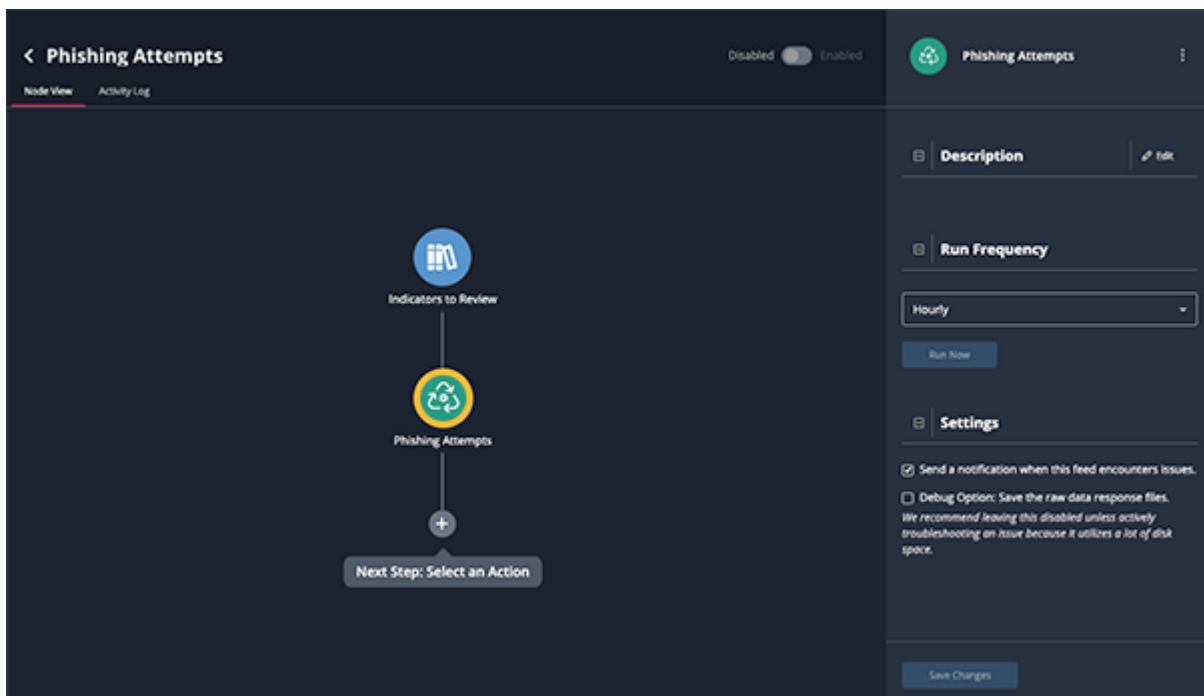
Create Cancel

- Complete the following fields:

FIELD	DESCRIPTION
Name	The name to give this workflow.
Description	Optional - A description of what this workflow does.
Data Collection	<p>The data collection that will be used in the workflow.</p> <div>  <p>A data collection is required if you intend to run the workflow by schedule. Workflows built to be used as Manually Triggered Workflows do not require a set data collection.</p> </div>

- Click on **Create**.

The Workflow Builder will load.



- Set how often the workflow will run using the dropdown provided under Run Frequency. You can select periodic or scheduled runs.

Periodic Run Options

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.

Schedule Run Options

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.

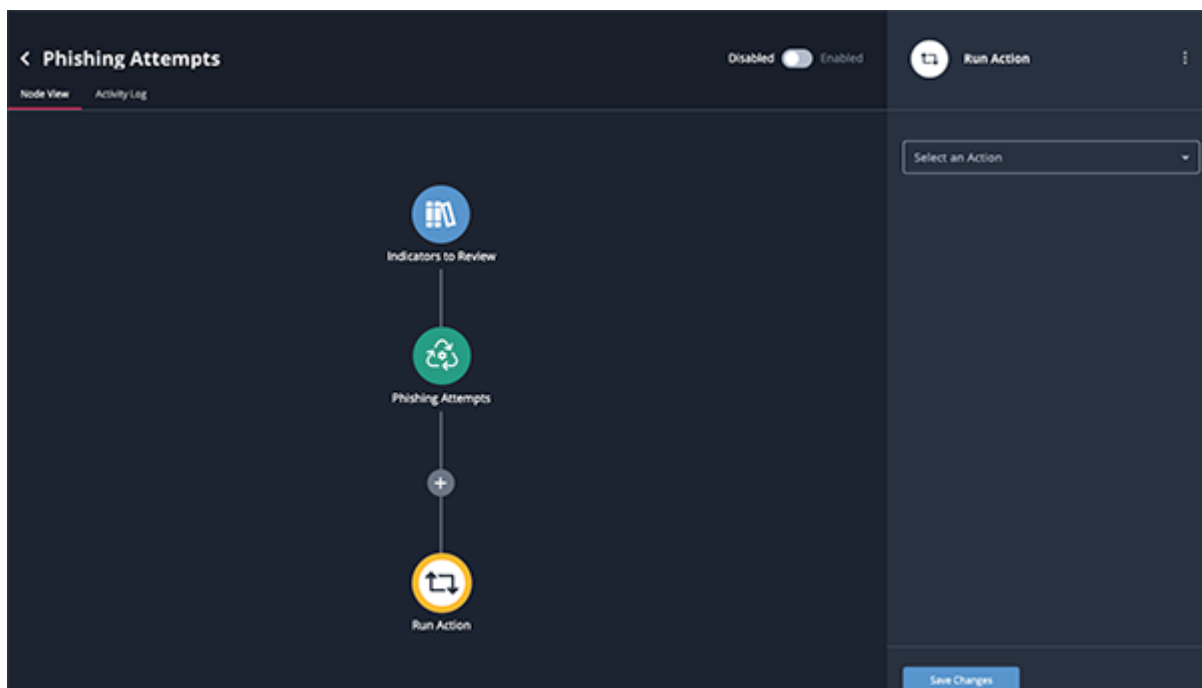


You can also select **No Schedule**. This will result in the workflow only running when you click on the **Run Now** button or initiate a **Manually Trigger Workflow** run from the Threat Library or an object's details page.

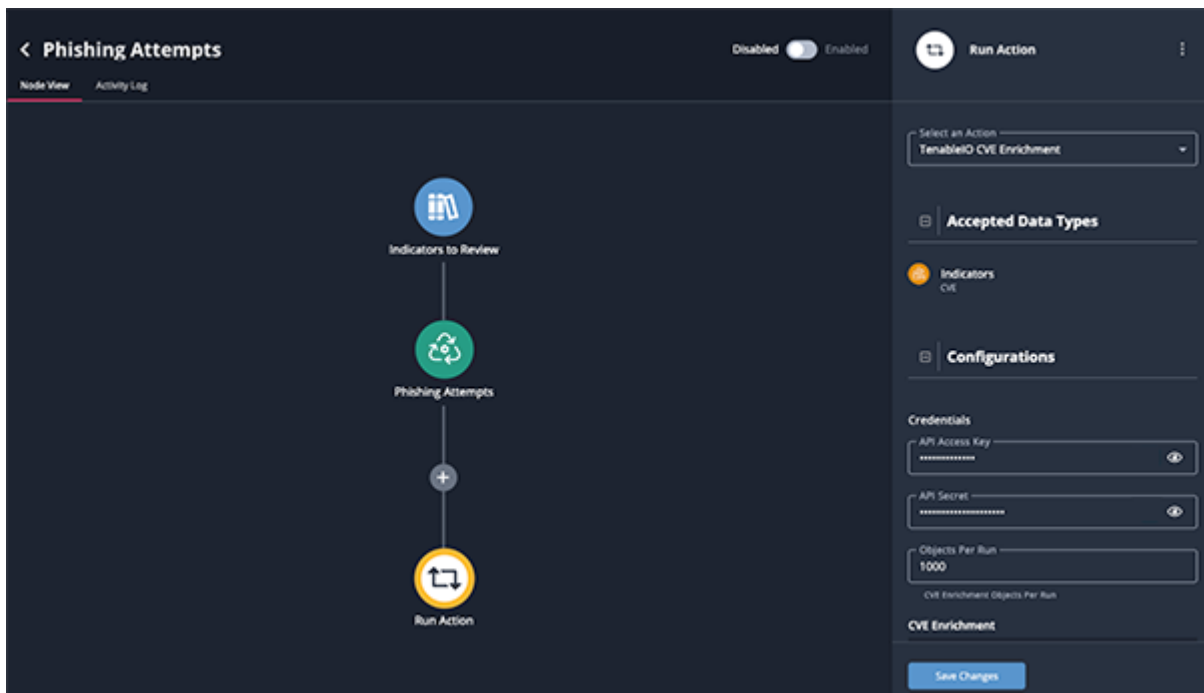
6. Review the workflow settings under the Settings option. Options include:

SETTING	DESCRIPTION
Send a Notification	Enabled by default. 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. See the Workflow Notifications topic for more information.
Debug Options	Disabled by default. 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. ThreatQuotient recommends temporarily enabling the option when you are troubleshooting a workflow issue.

- Click on the + icon, located beneath the workflow node, to select an action.
- Select an installed action from the dropdown menu provided in the right pane.



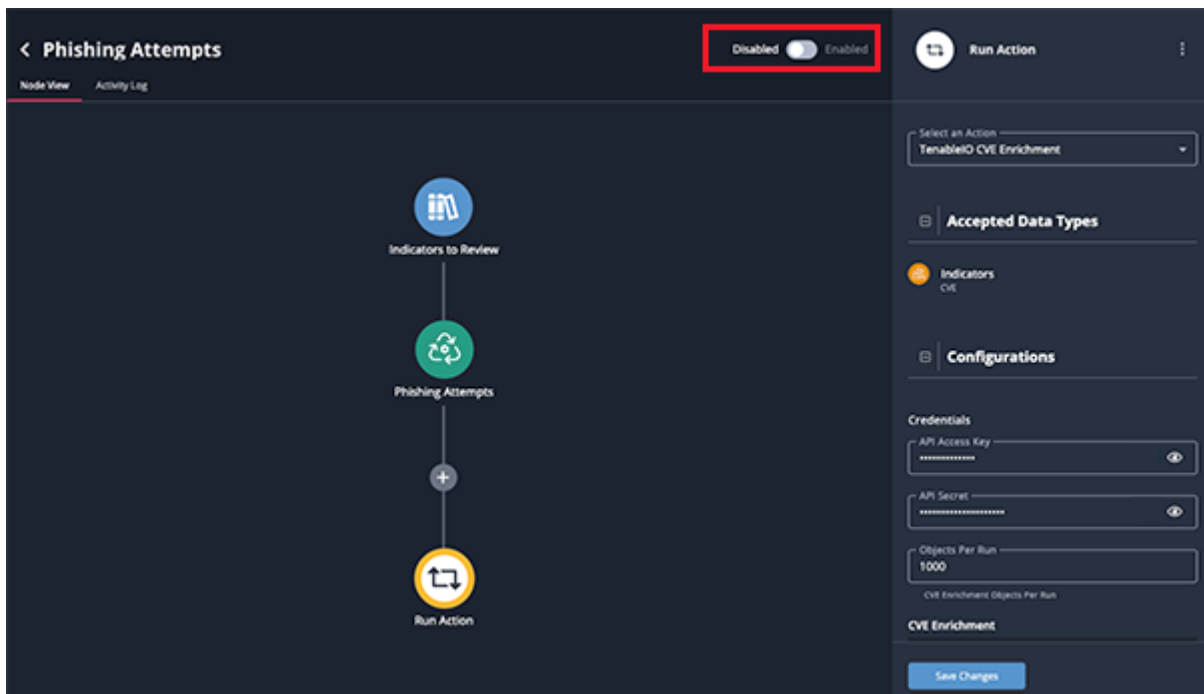
- The action node will appear in the builder view and the action's details will load in the right pane.



Actions will load with the default settings that have been saved in the action's details, such as API Keys, under the My Integrations page. This allows you to use an action in multiple workflows without having to enter credentials each time you add it. You can modify the action's configuration in the workflow itself in the right pane. Any configuration changes to an action made in the workflow itself will only apply to the action's instance in that particular workflow and will not change the default settings. Additionally, any modifications to the action's default configuration from the My Integrations page will not affect actions already deployed in a workflow.

10. Review the configuration options for the action, make any changes if needed, and click on **Save Changes**.
11. Repeat steps 7-10 to add additional actions.

12. Click on the **Disable/Enable** toggle switch to enable the workflow.



Upon enabling the workflow, it will initiate a run and then follow your set schedule. The workflow will not automatically initiate a run if you have **No Schedule** set as the frequency.

Modifying a Workflow

You can update an existing workflow from the workflow builder page.

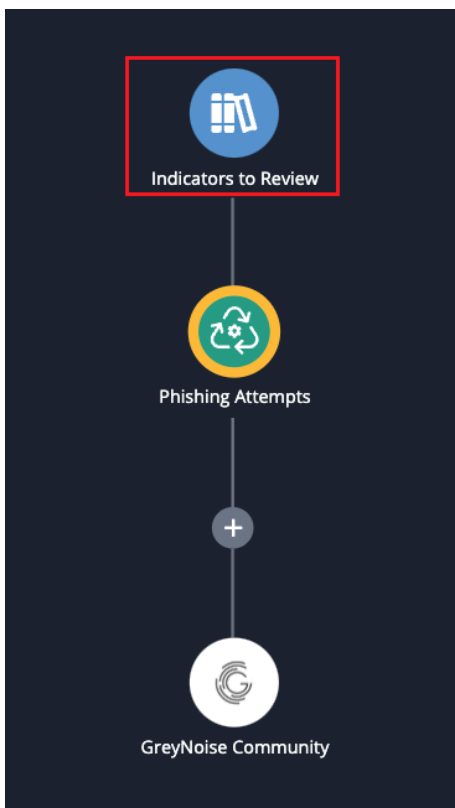


This steps covered in this section are for workflow built using the workflow builder. See the [Configuring Advanced Workflows](#) topic for steps on modifying Advanced Workflows.

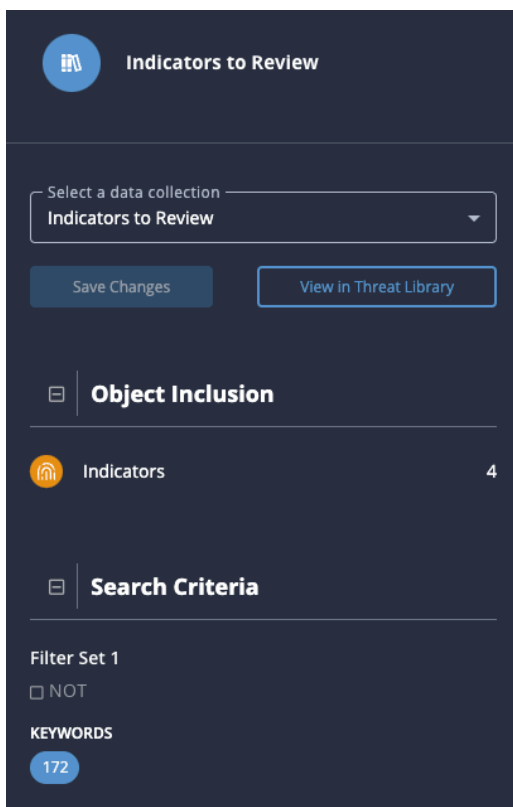
Changing the Data Collection

You can change the data collection used in the workflow.

1. Click on the data collection's node on the builder page.



The workflow's details will load in the right pane. You will see the current data collection selected and the objects included.



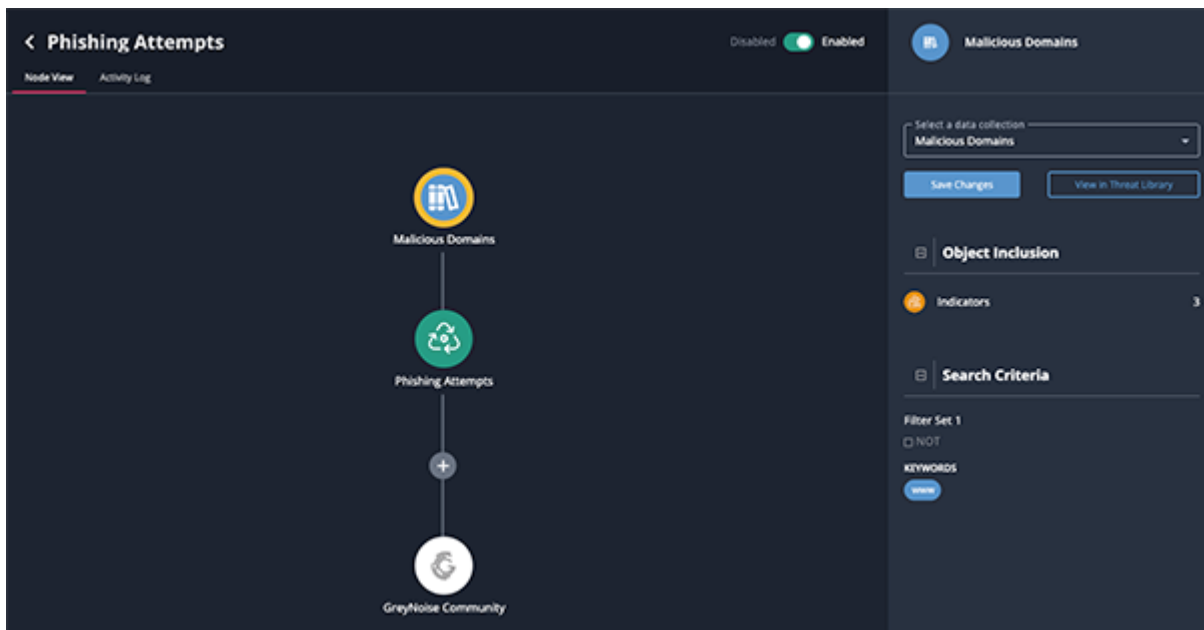
2. Use the dropdown provided to select a new data collection.



You can also click on the **View in Threat Library** option to open the data collection in the Threat Library to make changes to the data collection's filters.

3. Click on **Save Changes**.

The workflow will reload and the details pane will update with the new data collection.

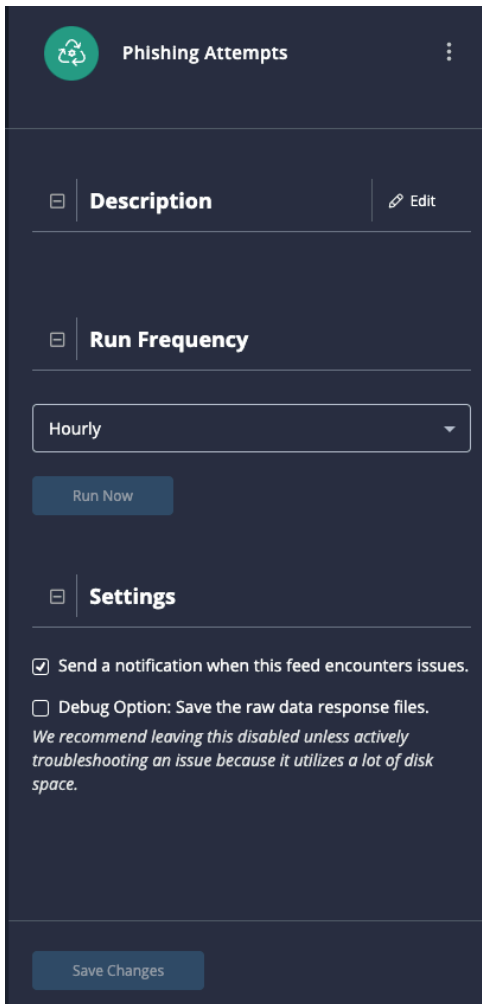


Updating a Workflow's Run Frequency

1. Click workflow's green node in the workflow builder.



The workflow's details will load in the right pane. You will see the current run frequency selected along with other details regarding the workflow.



Phishing Attempts

Description [Edit](#)

Run Frequency

Hourly

Run Now

Settings

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.
We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save Changes

2. Select a new run frequency using the dropdown provided.
3. Click on **Save Changes**.

Enabling Debug Option

You can enable the debug option to capture raw data response files for troubleshooting.

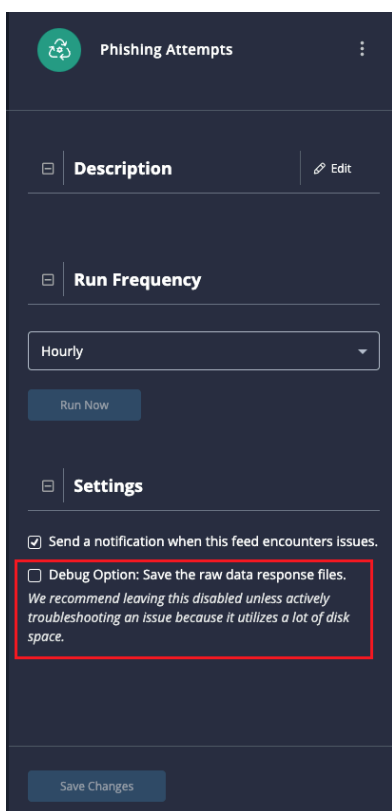


The Debug Option should only be enabled temporarily to troubleshoot a workflow as it uses a large amount of disk space.

1. Click workflow's green node in the workflow builder.



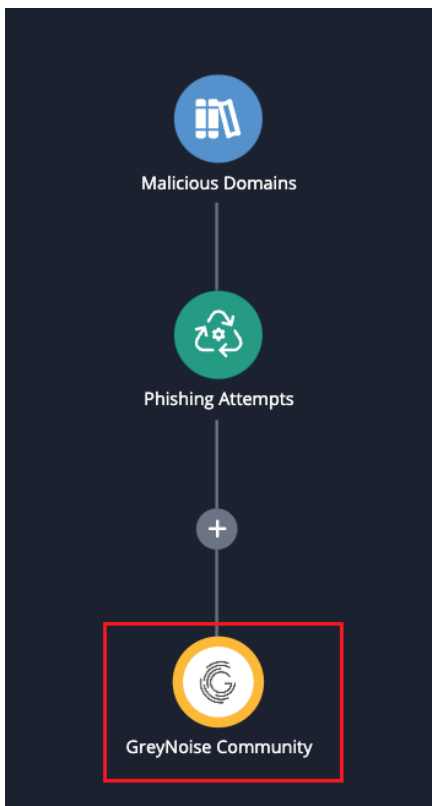
The workflow's details will load in the right pane.



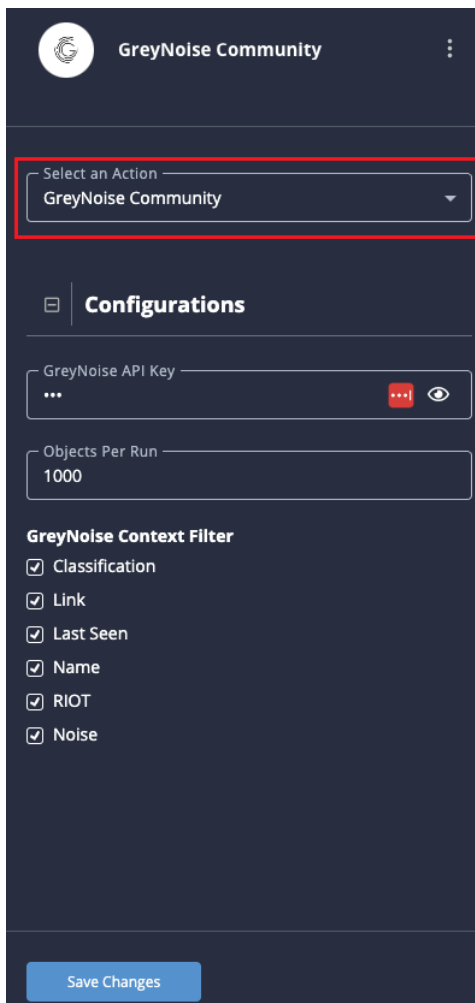
2. Check the **Debug Option** to enable it.
3. Click on **Save Changes**.

Changing an Action in a Workflow

1. Click on the action's node in the workflow builder.



2. Use the dropdown provided to select a new action for the workflow.



3. Click on **Save Changes**.

Updating an Action's Configuration for a Specific Workflow

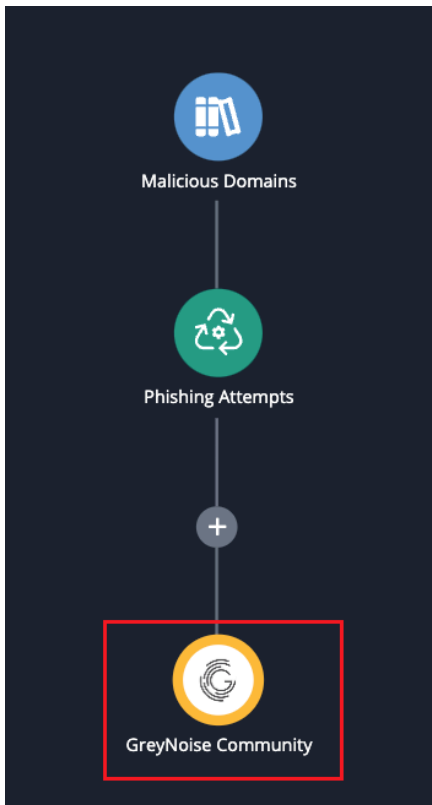
When an action is inserted into a workflow, the default configuration for the action, set in the action's details page, are included. This can include API credentials as well as specific settings how what is done with the data. You can edit the configuration settings for an action in a specific workflow in the right pane of the workflow builder.



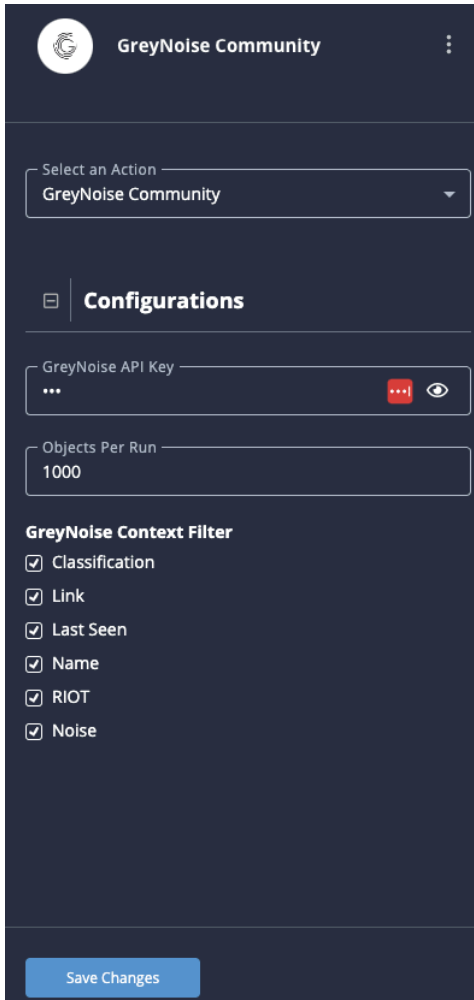
This will only effect the action's instance in that specific workflow and will not change the action's default configuration setting or other workflows that use the action.

Example: The default context filter for an action is designed to capture Name, Link, and Classification by default. When you insert the action into a workflow, you can update the configuration settings for that specific workflow to only capture the Name and Link without change the default for the action itself.

1. Click on the action's node in the workflow builder.



2. Make your required edits to the configuration options available under the **Configurations** heading.



3. Click on **Save Changes**.

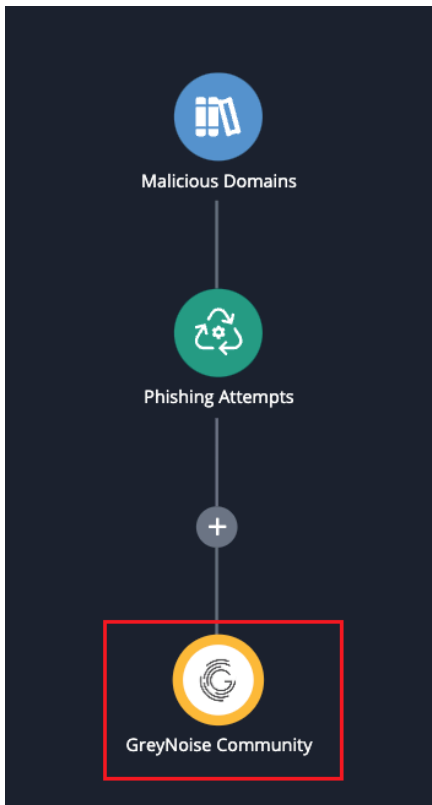
Updating an Action's Default Configuration from the Workflow Builder

You can access and edit an action's default configuration settings from the workflow builder.

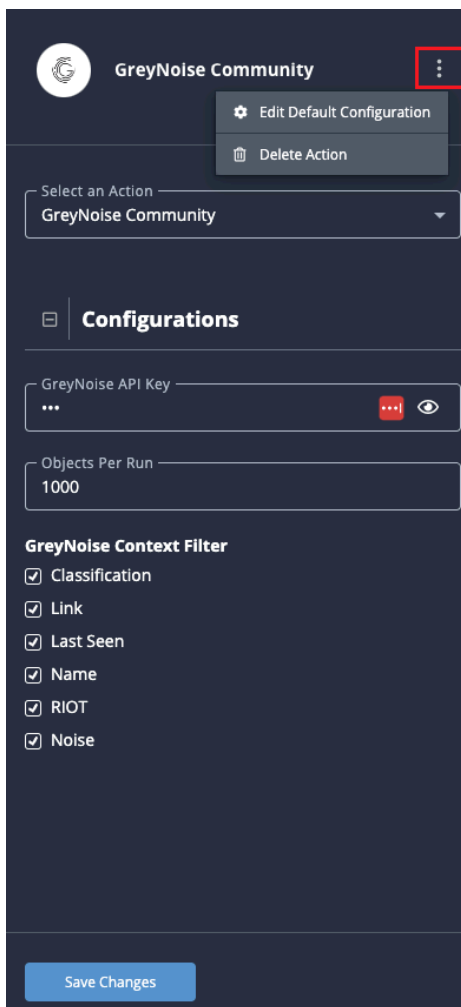


Updating the default configuration settings for an action will not update any instances of this action that have already been deployed to a workflow. This includes any workflow that you may be actively editing if you have already inserted the action.

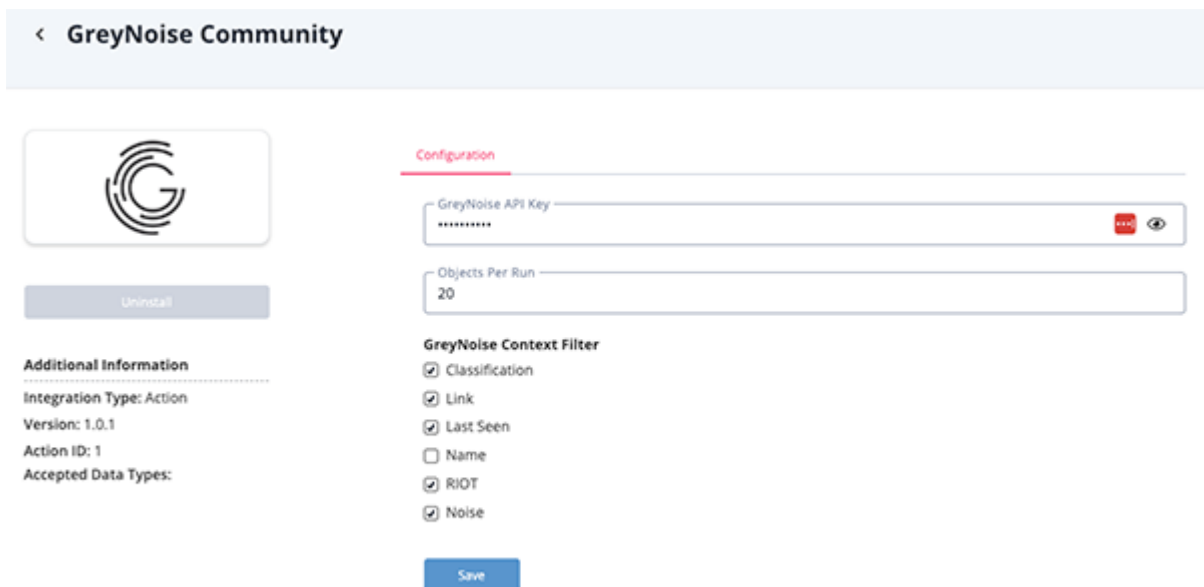
1. Click on the action's node in the workflow builder.



2. Click on the **vertical ellipsis** next to the action's name and select **Edit Default Configuration**.



The action's details page will load.

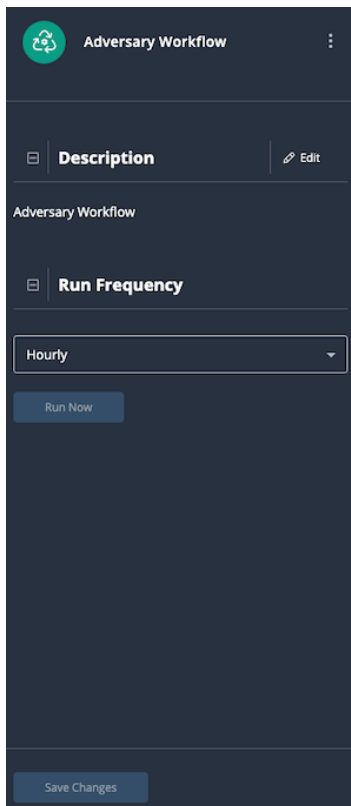


3. Make your required configuration settings and click **Save**.

Performing Manual Workflow Runs

You can perform manual workflow runs if the action utilized by workflow allows it.

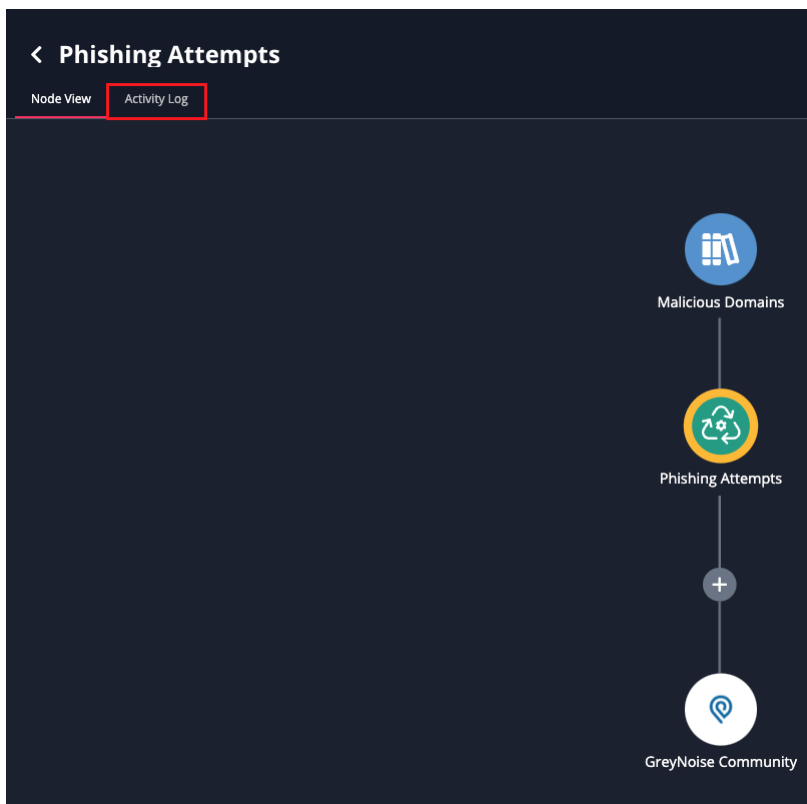
1. Open the workflow in the workflow builder.
2. Click on the **green workflow node** to load its details in the right panel.
3. Click on the **Run Now** button located under the **Run Frequency** heading.



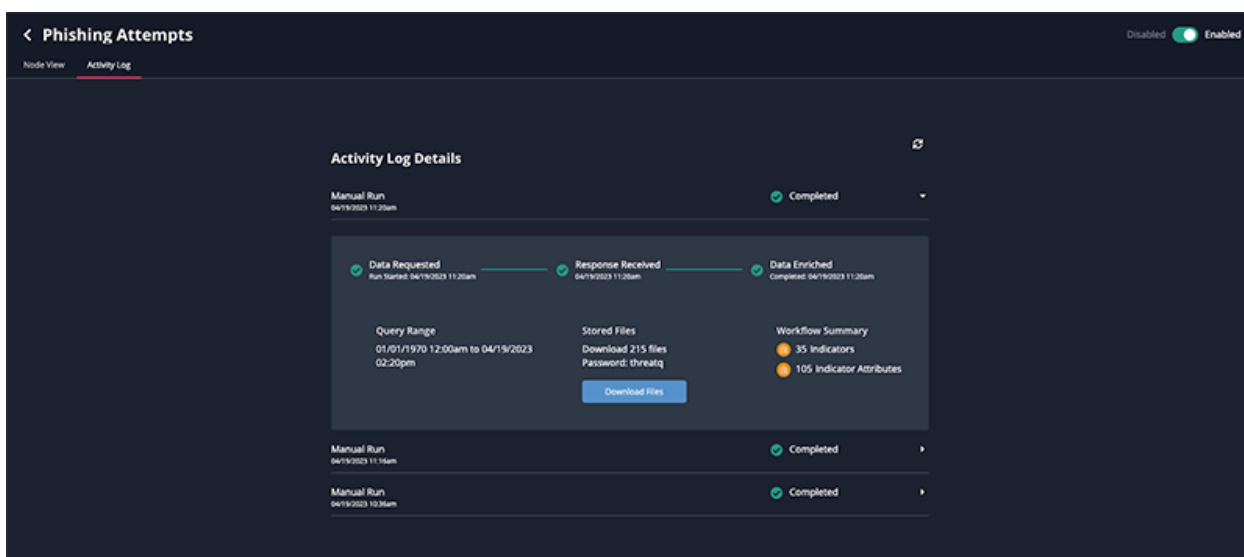
Viewing the Activity Log

You can review the activity log for workflow in the workflow builder page.

1. Open the workflow within the builder.
2. Click on the **Activity Log** tab located above the node graph.



The Activity Log will load.



Activity Log Details

The Activity Log provides the following run information:

FIELD	DESCRIPTION
Type of Run	Whether the run was a scheduled or manual run.
Data Requested	The timestamp of when the data was requested.
Response Received	The timestamp of when a response from the provider was received.
Data Enriched	The timestamp of when the action enrichment was completed.
Query Range	The dataset range for the information.
Stored Files	Files downloaded during the run and the password to open the files. If the workflow encountered errors, you can click the Download Files button to download a zip file(s) containing the error log(s). When you open the zip file(s) you are prompted to enter the Password displayed above the Download Files button.
Workflow Summary	A breakdown of the specific types of system objects were ingested during the run.

Activity Log Details

Manual Run

04/19/2023 11:20am

Completed

Data Requested

Run Started: 04/19/2023 11:20am

Response Received

04/19/2023 11:20am

Data Enriched

Completed: 04/19/2023 11:20am

Query Range

01/01/1970 12:00am to 04/19/2023 02:20pm

Stored Files

Download 215 files

Password: threatq

Download Files

Workflow Summary

35 Indicators

105 Indicator Attributes

Manual Run

04/19/2023 11:16am

Completed

Manual Run

04/19/2023 10:36am

Completed

Deleting a Workflow

There are two ways to delete a workflow: from the Workflow Builder page and from the Orchestrator landing page.



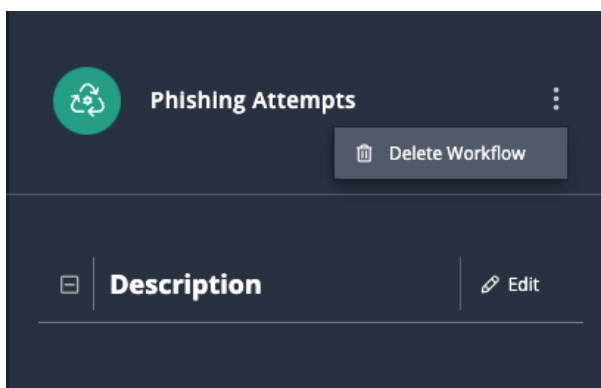
Deleting a workflow will not delete the system objects that have already been ingested into the ThreatQ platform.

Deleting a Workflow from the Workflow Builder

1. Click on green workflow node in the workflow builder page.



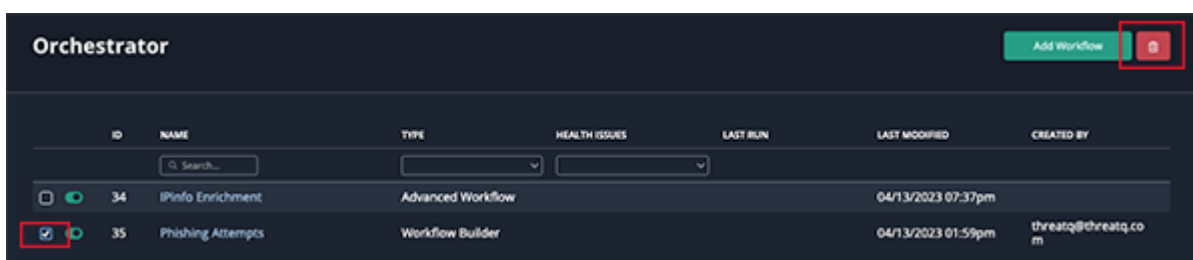
2. Click on the vertical ellipsis to the right of the workflow name and select **Delete Workflow**.



3. Click on the **Delete Workflow** button, when prompted, to confirm deletion.

Deleting a Workflow from the Orchestrator Landing Page

1. Select the checkbox next to the workflow to delete and then click on the red trashcan icon.



2. Click on the **Delete Workflow** button, when prompted, to confirm deletion.




Advanced Workflows

About Advanced Workflows

Advanced Workflows are preconfigured workflows, developed by ThreatQ Professional Services, that have been written to include all required actions and the data enrichment processes. Advanced Workflows are designed to be installed (required actions and workflow) via a single YAML file in the ThreatQ UI installer. Once installed, you will only need to add your third-party credentials and select your default configuration settings.



Contact [ThreatQuotient Customer Success](#) to request an Advanced Workflow.

Orchestrator							Add Workflow 	
ID	NAME	TYPE	HEALTH ISSUES	LAST RUN	LAST MODIFIED	CREATED BY		
	<input type="text" value="Q Search..."/>	<input type="text" value=""/>	<input type="text" value=""/>					
<input type="checkbox"/> 	34 IPinfo Enrichment	Advanced Workflow			04/13/2023 05:53pm			
<input type="checkbox"/> 	35 Phishing Attempts	Workflow Builder			04/13/2023 01:59pm	threatq@threatq.com		

< IPinfo Enrichment

Disabled ☒ Enabled

Uninstall

Additional Information

Integration Type: Workflow

Version: 1.0.0

Workflow ID: 34

Accepted Data Types:

Configuration

Activity Log

Select a data collection

Indicators to Review

Select the data collection you want to send for enrichment.

IPinfo API Key

Enter your IPinfo API Key.

Context Filter

Select which pieces of context you want to bring into ThreatIQ

☒ Location coordinates

☒ City

☒ Country

☒ Region

☐ Timezone

IPinfo Source

IPinfo

Objects reported by IPinfo will receive this source

Set indicator status to...

Review

Run Frequency

Every 24 Hours

Important Notes

The following is a list of important differences between workflows built in the Workflow Builder UI and Advanced Workflows:

- Advanced Workflows cannot be opened in the Workflow Builder. All configuration settings and workflow scheduling configurations are set from the workflow details page.
- All Advanced Workflow run details can be viewed on the Activity Log tab for the workflow details page.
- Advanced Workflow details can only be accessed from the Orchestrator page. You cannot view installed advanced workflows on the My Integrations page.
- Advanced Workflows cannot be used as Manually Triggered Workflows in the Threat Library nor an object's details page.

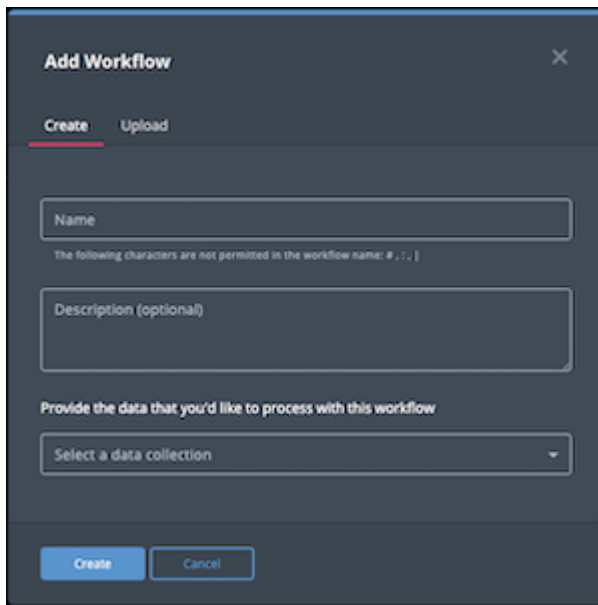
Installing an Advanced Workflow



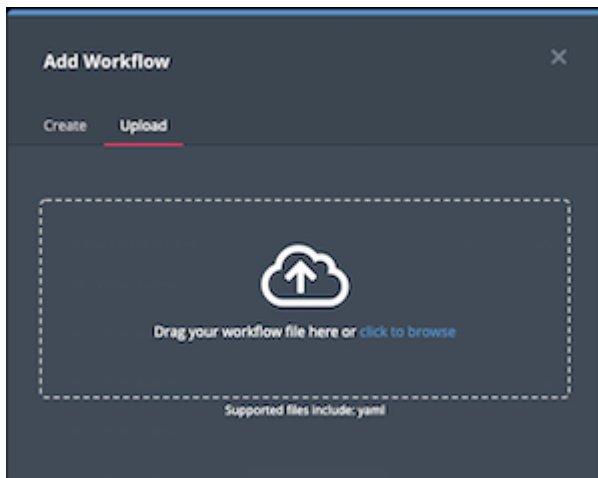
TQO only supports the uploading and use of workflow YAML files developed by ThreatQuotient. Contact [ThreatQuotient Customer Success](#) for more information.

1. Click the **Orchestrator** option in the main navigation.
2. Click the **Add Workflow** button.

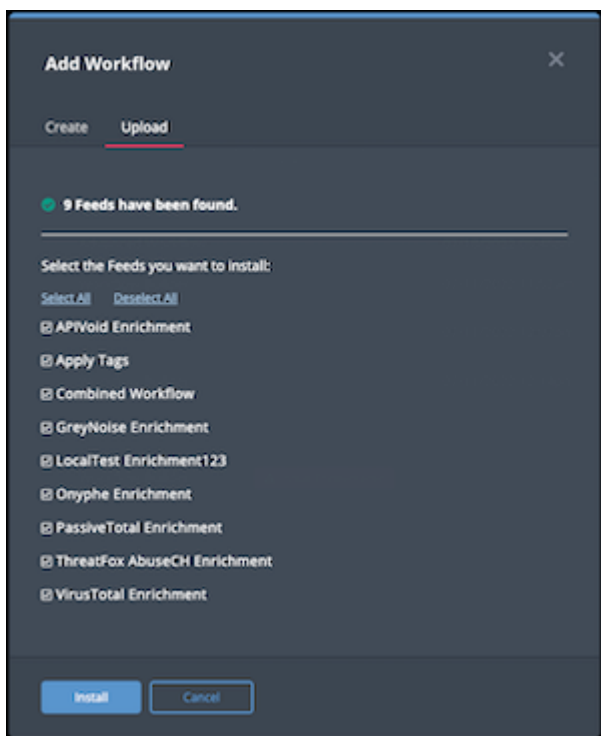
The Add Workflow window is displayed with the Create tab selected.



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.

Configuring an Advanced Workflow

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 both workflows built with the workflow builder and installed workflows (Advanced Workflows). Advanced Workflows will be marked as such in the **Type** column.

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

Disabled

Enabled

Uninstall

Additional Information

Integration Type: Workflow

Version: 1.0.0

Workflow ID: 34

Accepted Data Types:

Configuration

Activity Log

Select a data collection

Indicators to Review

Select the data collection you want to send for enrichment.

IPinfo API Key

.....

Enter your IPinfo API Key.

Context Filter

Select which pieces of context you want to bring into ThreatQ

☒ Location coordinates

☒ City

☒ Country

☒ Region

☐ Timezone

IPinfo Source

IPinfo

Objects reported by IPinfo will receive this source

Set indicator status to...

Review

Run Frequency

Every 24 Hours

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. You can 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.

4. Select a default status that the workflow will assign to system objects that are ingested by the workflow.
5. Select a **Run Frequency**. Options include:

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.

Schedule

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.

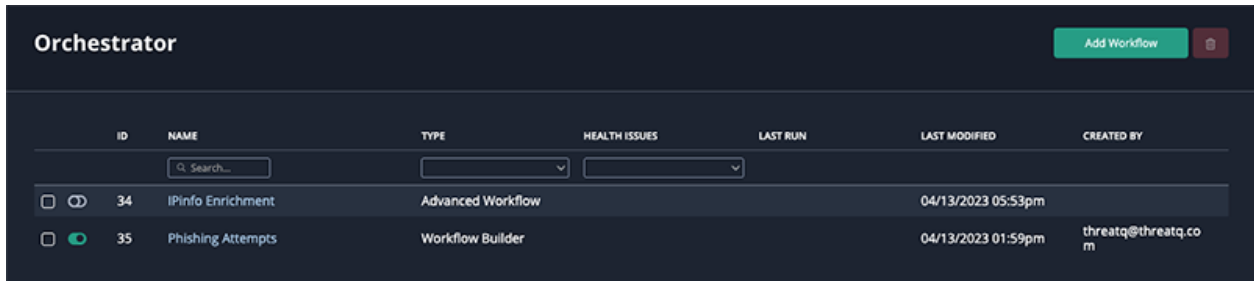
6. Select whether or not to receive **Feed Health Notifications** - See the [Workflow Health Notifications](#) section for more information.
7. **Debug Option** - The Debug Option checkbox gives you the option to save raw data response files for troubleshooting purposes. Since this option uses a large amount of disk space, it defaults to unchecked. We recommend temporarily enabling the option when you are troubleshooting a workflow issue.
8. Click **Save**.
9. Click the **Enable/Disable** toggle to enable the workflow.

Performing Manual Workflow Runs

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.

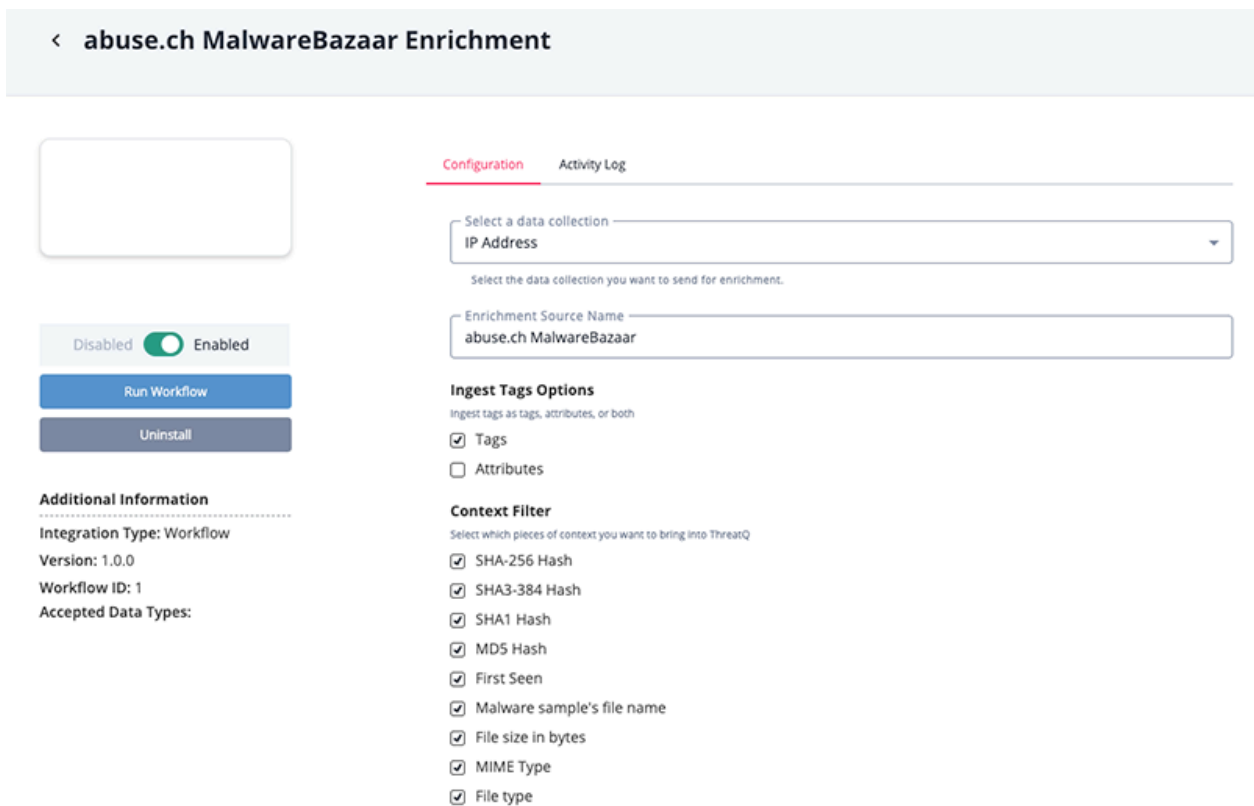
The Orchestrator page lists installed workflows.



Orchestrator							Add Workflow	
ID	NAME	TYPE	HEALTH ISSUES	LAST RUN	LAST MODIFIED	CREATED BY		
<input type="checkbox"/>	<input type="text" value="Search..."/>							
<input type="checkbox"/>	34	IPInfo Enrichment	Advanced Workflow		04/13/2023 05:53pm			
<input type="checkbox"/>	35	Phishing Attempts	Workflow Builder		04/13/2023 01:59pm	threatq@threatq.com		

2. Locate and click the workflow you want to run.

The workflow's details page is displayed.



< abuse.ch MalwareBazaar Enrichment

Disabled ☒ Enabled

Run Workflow

Uninstall

Additional Information
Integration Type: Workflow
Version: 1.0.0
Workflow ID: 1
Accepted Data Types:

Configuration Activity Log

Select a data collection
IP Address
Select the data collection you want to send for enrichment.

Enrichment Source Name
abuse.ch MalwareBazaar

Ingest Tags Options
Ingest tags as tags, attributes, or both
☒ Tags
☐ Attributes

Context Filter
Select which pieces of context you want to bring into ThreatQ
☒ SHA-256 Hash
☒ SHA3-384 Hash
☒ SHA1 Hash
☒ MD5 Hash
☒ First Seen
☒ Malware sample's file name
☒ File size in bytes
☒ MIME Type
☒ File type

3. Click the **Run Workflow** button.

Disabled

Enabled

Run Workflow

Uninstall

Additional Information

Integration Type: Workflow

Version: 1.0.0

Workflow ID: 1

Accepted Data Types:

Configuration

Activity Log

Select a data collection

IP Address

Select the data collection you want to send for enrichment.

Enrichment Source Name

abuse.ch MalwareBazaar

Ingest Tags Options

Ingest tags as tags, attributes, or both

☒ Tags

☐ Attributes

Context Filter

Select which pieces of context you want to bring into ThreatQ

☒ SHA-256 Hash

☒ SHA3-384 Hash

☒ SHA1 Hash

☒ MD5 Hash

☒ First Seen

☒ Malware sample's file name

☒ File size in bytes

☒ MIME Type

☒ File type

4. Review and/or update the Start and End (if supported) dates and Time as well as the 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.

Trigger Manual Run

Start Date

April

▼

18

▼

2023

▼

Time

05:38 PM

⌚

Time Zone

UTC

▼

End Date

April

▼

19

▼

2023

▼

Time

05:38 PM

⌚

Time Zone

UTC

▼

Queue Run

Cancel



Not all advanced workflows support the End Dates. If that case, you will only be able to select a Start Date.

Trigger Manual Run

Start Date

March

15

2022

Time

03:33 PM

Time Zone

UTC

NOTE:

This feed only supports a Start Date for manual runs and will use the current time as the End Date.

Queue Run

Cancel

5. Click the **Queue Run** button.

The workflow's Activity Log will load. See the [Viewing the Activity Log](#) for more information regarding the Activity Log.

abuse.ch MalwareBazaar Enrichment

Configuration

Activity Log

Disabled

Enabled

Run Workflow

Uninstall

Additional Information

Integration Type: Workflow

Version: 1.0.0

Workflow ID: 1

Accepted Data Types:

Configuration

Activity Log

Activity Log Details

Manual Run

04/19/2023 05:35pm

In Progress

✓ Data Requested

Run Started: 04/19/2023 05:35pm

⌄ Response Received

No response received for this feed run

⌄ Data Enriched

In Progress:

Query Range

04/18/2023 05:35pm to 04/19/2023 05:35pm

Stored Files

Download 36 files

Password: threatq

Download Files


Workflow Summary

1326 Indicators

Scheduled Run

04/19/2023 05:30pm

Completed




If the workflow encountered errors, you can click the **Download Files** button to download a zip file(s) containing the error log(s). When you open the zip file(s) you are prompted to enter the Password displayed above the Download Files button.

ThreatQ TDR Orchestrator User Guide
Version 2.1.0

61

[← HTTPError](#)



Disabled ☒ Enabled

[Run Workflow](#)
[Uninstall](#)

Additional Information

Integration Type: Workflow

Workflow ID: 11

Configuration
Activity Log

Activity Log Details

⚠️ Completed with errors

✔️ Data Requested
Run Started: 03/22/2022 01:16pm

—

—

✔️ Response Received
03/22/2022 01:17pm

—

⚠️ Data Enriched
Completed with errors: 03/22/2022 01:17pm

Query Range
 After 03/21/2022 01:15pm

Stored Files
 Download 2 files
 Password: threatq

Download Files

Workflow Summary
Error fetching data from provider: TimeoutError()
 Download files (left) to view the full error log.

Manual Run <small>03/22/2022 01:15pm</small>	⚠️ Completed with errors
Manual Run <small>03/22/2022 01:14pm</small>	⚠️ Completed with errors
Manual Run <small>03/22/2022 12:44pm</small>	✔️ Completed
Scheduled Run <small>03/22/2022 12:43pm</small>	✔️ Completed

Viewing the Activity Log

You can view the Activity Log for an Advanced Workflow from its details page.

1. Navigate to the Orchestrator landing page.
2. Click on the name of the Advanced Workflow to open its details page.
3. Click on the **Activity Log** tab to view run details.

← IPinfo Enrichment

Disabled

Enabled

Uninstall

Additional Information

Integration Type: Workflow

Version: 1.0.0

Workflow ID: 34

Accepted Data Types:

Configuration

Activity Log

Select a data collection

Indicators to Review

Select the data collection you want to send for enrichment.

IPinfo API Key

Enter your IPinfo API Key.

Context Filter

Select which pieces of context you want to bring into ThreatQ

☒ Location coordinates

☒ City

☒ Country

☒ Region

☐ Timezone

IPinfo Source

IPinfo

Objects reported by IPinfo will receive this source

Set indicator status to...

Review

The Activity log will load.

◀ IPinfo Enrichment

Disabled Enabled

Uninstall

Additional Information

Integration Type: Workflow

Version: 1.0.0

Workflow ID: 34

Accepted Data Types:

Configuration

Activity Log

Activity Log Details

Manual Run
04/19/2023 05:35pm

 In Progress



Query Range

04/18/2023 05:35pm to 04/19/2023
05:35pm

Stored Files

Download 36 files
Password: threatq

[Download Files](#)

Workflow Summary

1326 Indicators

Scheduled Run
04/19/2023 05:30pm

Completed

Activity Log Details

You can view the following information from the Activity Log:

FIELD	DESCRIPTION
Type of Run	Whether the run was a scheduled or manual run.
Data Requested	The timestamp of when the data was requested.
Response Received	The timestamp of when a response from the provider was received.
Data Enriched	The timestamp of when the action enrichment was completed.
Query Range	The dataset range for the information.
Stored Files	Files downloaded during the run and the password to open the files. If the workflow encountered errors, you can click the Download Files button to download a zip file(s) containing the error log(s). When you open the zip file(s) you are prompted to enter the Password displayed above the Download Files button.
Workflow Summary	A breakdown of the specific types of system objects were ingested during the run.

Activity Log Details



Manual Run
04/19/2023 05:35pm

✔ Completed ▾

✔ Data Requested
Run Started: 04/19/2023 06:12pm


✔ Response Received
04/19/2023 06:13pm

✔ Data Enriched
Completed: 04/19/2023 06:13pm

Query Range
04/18/2023 06:12pm to 04/19/2023 06:12pm

Stored Files
Download 48 files
Password: threatq

Download Files

Workflow Summary
 3368 Indicators

Scheduled Run
04/19/2023 05:30pm

✔ Completed ▶

Deleting an Advanced Workflow

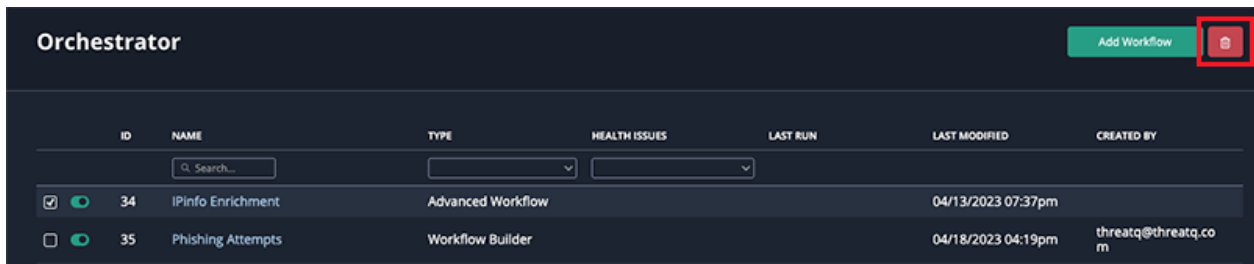
There are two ways to delete an Advanced Workflow.



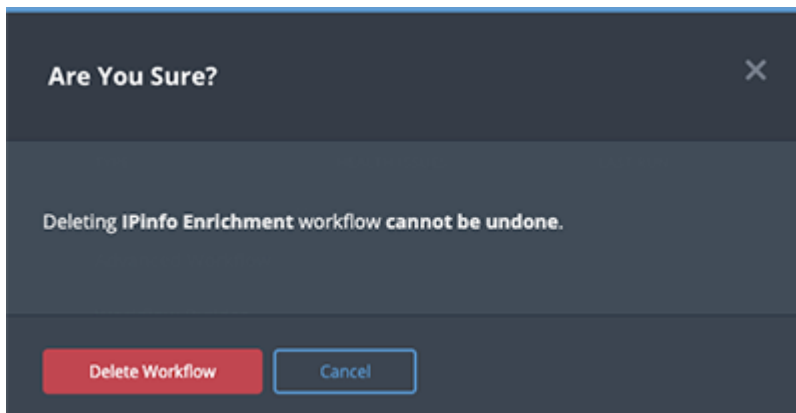
Deleting an Advanced Workflow will not delete the data already ingested into the ThreatQ platform.

Deleting from the Orchestrator Page

1. Navigate to the Orchestrator landing page.
2. Select the checkbox next to advanced workflow to delete.
3. Click on the **red trashcan icon** located to the top right of the page.



4. Click on **Delete Workflow**, when prompted, to confirm deletion.



Deleting from the Advanced Workflow Details Page.

1. Navigate to the Orchestrator landing page.
2. Click on the advanced workflow's name to load its details page.
3. Click on the **Uninstall** option.

< **IPinfo Enrichment**

Disabled
☒ Enabled

Uninstall

Additional Information

Integration Type: Workflow

Version: 1.0.0

Workflow ID: 34

Accepted Data Types:

Configuration
Activity Log

Select a data collection
Indicators to Review

Select the data collection you want to send for enrichment.

IPinfo API Key
.....

Enter your IPinfo API Key.

Context Filter

Select which pieces of context you want to bring into ThreatQ

☒ Location coordinates

☒ City

☒ Country

☒ Region

☐ Timezone

IPinfo Source
IPinfo

Objects reported by IPinfo will receive this source

Set indicator status to...
Review

4. Click on **Delete Workflow**, when prompted, to confirm deletion.

Are You Sure?
✕

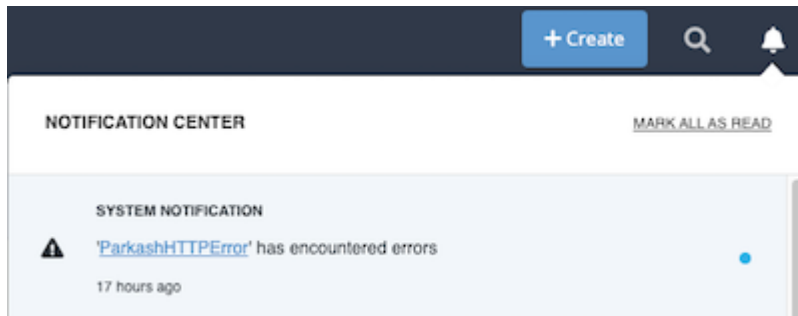
Deleting IPinfo Enrichment workflow cannot be undone.

Delete Workflow

Cancel

Workflow Notifications

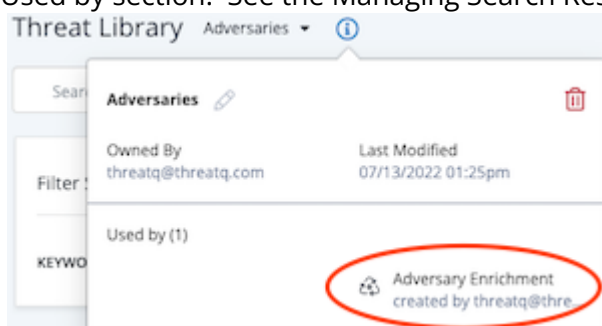
Workflow Health Notifications allow the ThreatQ application to send you, and other designated users, email and in-app notifications when a workflow encounters an issue. The in-app notifications appear in Notification Center for users with an administrator or maintenance account. These notifications include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

Tips and Tricks

- You can move the node graph to a new position on the screen by clicking and dragging any node.
- Workflows require a data collection and at least one action in order to run. The exception to this is when using a [manually triggered workflow](#). In that scenario, the workflow does not require a set data collection.
- 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.



Change Log

• Version 2.1.0



The following updates were included with ThreatQ version 5.17.0

- The Threat Library results list allows you to select multiple objects of the same type for workflows.
- Resolved the following issues:
 - The data collection pane included Filter Set fields in the Search Criteria section even though the data collection did not include a filter set. Now, the data collection pane displays the following message for a data collection that does not include a filter set: `No search criteria to display.`
 - ThreatQ allowed you to install TWO actions in instances that did not have the required ThreatQ version or a later version. For instance, you could install an action with a required ThreatQ version of 5.13.0 or later in a ThreatQ v5.12.1 instance.

• Version 2.0.0

- Reformatted Guide and contents.

• Version 1.4.0



The following updates were included with ThreatQ version 5.15.0

- TQO now supports the enrichment of all system object types.
- The **Last Run** column on the Orchestrator landing page has been updated to **Last Scheduled Run**.
- Resolved the following issues:
 - The workflow node view truncated the bottom of workflow names that included a letter with a descender, such as p or q.
 - When you uploaded a new version of an action that included a change to the action's name, the name change was reflected in the action configuration panel for existing TQO workflows but not in the node view. Now, action name changes are reflected in the configuration panel and node view.
 - In the workflow node view, we updated the Search Criteria display in the data collection details panel to be consistent with ThreatQ styles and formatting.

• Version 1.3.0



The following updates were included with ThreatQ version 5.14.0

- You can now perform manually triggered actions from the Threat Library and Object Details page.
- Resolved the following issues:
 - When you installed a group of actions from a single YAML file, any action with a namespace value that included a capital letter failed to install.

- When you uninstalled an action, the **Are You Sure?** confirmation window listed the action name as undefined.
- When you created a workflow without selecting a run schedule, TQO ran the workflow as soon as you enabled it.
- In the Orchestrator page, the display of workflows with IDs of two or more digits was wrapped so that the digits displayed on separate lines.

• Version 1.2.0



The following updates were included with ThreatQ version 5.12.0

- TQO actions can now be installed with provider icons.
- You can now change the name of a workflow created in TQO for the workflow node view.
- Resolved the following issues:
 - The Light mode version of the workflow Node View did not display the Virus Total action's logo. In addition, the display of the action node connector lines was not consistent with ThreatQ standards.
 - We resolved the following issues with the display of workflow names:
 - When you viewed a workflow created in TQO, the browser page title displayed the unique workflow ID (stored in the name field).
 - When you upgraded to ThreatQ 5.9, the system populated the new display_name field with the unique workflow ID instead of populating that value in the name field. As a result, the display names for your existing workflows were changed to the corresponding unique workflow IDs.



This issue only affected workflows created in TQO. It did not affect advanced workflows.

• Version 1.1.0

- Updates for version 5.8.0

• Version 1.0.0

- Initial Release