

ThreatQuotient

A Securonix Company



ANY.RUN Action

Version 1.0.0

November 25, 2025

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 ThreatQ Supported

Support

Email: tq-support@securonix.com

Web: <https://ts.securonix.com>

Phone: 703.574.9893

Contents

Warning and Disclaimer 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Configuration 8

Actions 10

 ANY.RUN Submit for Analysis..... 11

Enriched Data..... 12

Use Case Example..... 13

Change Log 14

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 © 2025 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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: tq-support@securonix.com

Support Web: <https://ts.securonix.com>

Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 6.7.3
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ANY.RUN Action enables users to submit a collection of URLs and FQDNs to ANY.RUN for sandbox analysis. The results of this analysis are later utilized by the ANY.RUN CDF to collect and enrich contextual information derived from the executed analysis.

The integration provides the following action:

- **ANY.RUN Submit for Analysis** - submits a collection of URL and FQDN type indicators to ANY.RUN sandbox for analysis.

The integration is compatible with the following indicator types:

- FQDN
- URL

The integration enriches the following indicator types:

- FQDN
- URL



This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- A valid ANY.RUN API Key.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the following indicator object types:
 - FQDN
 - URL

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:



The configurations set on this page will be used as the default settings when inserting this action into a new workflow. 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.

PARAMETER	DESCRIPTION
API Key	Enter your ANY.RUN API Key.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Environment	<p>Select which environment to sandbox this sample. Options include:</p> <ul style="list-style-type: none"> ◦ Windows 10 64 bit (default) ◦ Windows 8.1 64 bit ◦ Windows 8.1 32 bit ◦ Windows 7 64 bit ◦ Windows 7 32 bit ◦ Windows Vista 64 bit ◦ Windows Vista 32 bit
Offline Analysis	Enable this parameter analyze the file offline. This parameter is disabled by default.

PARAMETER	DESCRIPTION
Network Location	<p>Select the network location to sandbox the sample. Options include:</p> <ul style="list-style-type: none"> ◦ Fastest (<i>default</i>) ◦ Australia ◦ Brazil ◦ France ◦ Germany ◦ Italy ◦ Russia ◦ South Korea ◦ Switzerland ◦ United Kingdom ◦ United States

< ANY.RUN Submit for Analysis



Uninstall

Additional Information

Integration Type: Action

Version:

Action ID: 5

Accepted Data Types:

☒ Indicators

URL

FQDN

Configuration

Authentication and Connection

API Key

☒ Enable SSL Certificate Verification

When checked, validates the host-provided SSL certificate.

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

Sandbox Options

Environment

Windows 10 64 bit

Which environment would you like to sandbox this sample in?

☐ Offline Analysis

Do you want this file to be analyzed offline?

Network Location

Fastest

Select the network location you want to sandbox the sample in

Objects per run

100

Maximum number of objects to process per-run.

- Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
ANY.RUN Submit for Analysis	Submits a collection of indicators (URL, FQDN) to a ANY.RUN sandbox for Analysis.	Indicator	URL, FQDN

ANY.RUN Submit for Analysis

The ANY.RUN Submit for Analysis action submits a URL and FQDN type indicators to a user-designated ANY.RUN sandbox for Analysis.

POST <https://api.any.run/v1/analysis/>

Sample Request:

```
data={
  "obj_type": "url",
  "obj_url": "google.nl",
  "env_os": "windows",
  "env_bitness": "64",
  "env_version": "10",
  "opt_network_connect": "true",
  "opt_network_geo": "fastest"
}
```

Sample Response:

```
{
  "error": false,
  "data": {
    "taskid": "d2db3dc6-b86d-465f-b641-4f9fd924efd8"
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Indicator Attribute	ANY.RUN Analysis Time	N/A	2025-11-20 20:45:36+00:00	Updatable. The time that the Feed Run actually started.

Enriched Data



Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Indicators	10
Indicator Attributes	10

Use Case Example

1. A user submits a collection of indicators to ANY.RUN using the Submit for Analysis action.
2. ANY.RUN processes the submission, applying the specified environment configuration options and indicator values, and returns a unique task ID for the newly initiated analysis.
3. The action records the timestamp marking when the feed begins, allowing for accurate reference in future operations.
4. At a later stage, the user executes the CDF to retrieve the contextual information collected by ANY.RUN during the analysis.

Change Log

- Version 1.0.0
 - Initial release