

ThreatQuotient



Infoblox Dossier Operation User Guide

Version 1.0.1

October 28, 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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

Actions 9

 Enrich Indicator 9

Change Log 10

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.

Support

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

Support Email: support@threatq.com

Support Web: <https://support.threatq.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	1.0.1
Compatible with ThreatQ Versions	>= 4.40.0
Support Tier	ThreatQ Supported

Introduction

The ThreatQuotient for Infoblox Dossier Operation enables a ThreatQ user to query Infoblox Dossier for enrichment metadata.

The operation provides the following action:

- **Enrich Indicator** - enriches indicators (IP Addresses, Emails, FQDNs, URLs, and MD5, SHA-1, and SHA-256 hashes) with research from Infoblox Dossier.

The operation is compatible with the following indicator types:

- Email Address
- FQDN
- IP Address
- MD5
- SHA-1
- SHA-256
- URL

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to [configure](#) and then [enable](#) the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your API key for connecting to Infoblox Dossier.
Hostname	The Hostname or IP address of Infoblox Dossier.
Port	The communication port (default is 8000).
Verify SSL	Check this box to verify SSL when connecting to the Infoblox Dossier instance.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

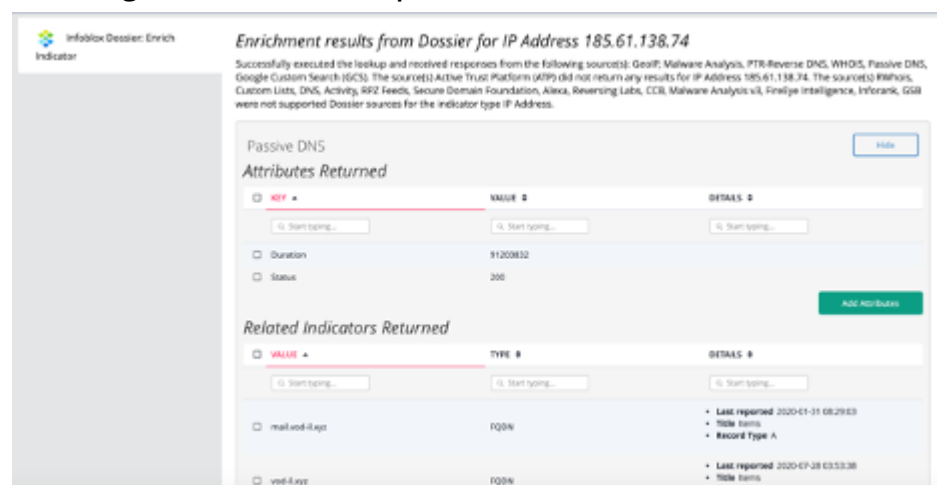
ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Enrich Indicator	Enriches indicators with research from Infoblox Dossier.	Indicator	IP Addresses, Emails, FQDNs, URLs, and MD5, SHA-1, SHA-256

Enrich Indicator

The Enrich Indicator action enriches indicators (IP Addresses, Emails, FQDNs, URLs, and MD5, SHA-1, and SHA-256 hashes) with research from Infoblox Dossier.

The action also supports the **Source** filter.

Enriching Data Results Example



Infoblox Dossier: Enrich Indicator

Enrichment results from Dossier for IP Address 185.61.138.74

Successfully executed the lookup and received responses from the following sources: GeotIP, Malware Analysis, PTR-Reverse DNS, WHOIS, Passive DNS, Google Custom Search (GCS). The source(s) Active Trust Platform (ATP) did not return any results for IP Address 185.61.138.74. The source(s) RMMHors, Custom Lists, DNS, Activity, RFP Feeds, Secure Domain Foundation, Alexa, Reversing Labs, CCR, Malware Analysis v3, Finalize Intelligence, Infoblox, GSI were not supported Dossier sources for the indicator type IP Address.

Passive DNS

Attributes Returned

KEY	VALUE	DETAILS
Start time	Start time	Start time
Duration	91209832	
Status	200	

Related Indicators Returned

VALUE	TYPE	DETAILS
Start time	Start time	Start time
mail.vod-4.jp	FQDN	<ul style="list-style-type: none"> Last reported: 2020-01-31 08:29:03 Title: mail Record Type: A
vod-4.jp	FQDN	<ul style="list-style-type: none"> Last reported: 2020-07-28 03:53:38 Title: vod-4.jp Record Type: A

Change Log

- **Version 1.0.1**
 - Updated Dossier URI - <https://csp.infoblox.com/tide/>
 - Accounted for empty responses from Activity, CCB, Custom Lists, zvelo
 - Parsed data from RPZ Feeds, Custom Lists, DNS
 - Added functionality for sources **zvelo** and **whitelist**
- **Version 1.0.0**
 - Initial Release