

ThreatQuotient



KELA Monitor CDF Guide

Version 1.0.0

March 21, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

 Developer Supported

Support

Email: support@ke-la.com

Web: <https://ke-la.com/contact-us/>

Phone: N/A

Contents

- Integration Details..... 5
- Introduction 6
- Prerequisites..... 7
 - KELA API Key 7
 - KELA Monitor ID 8
- Installation..... 9
- Configuration 10
- Known Issues / Limitations 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 © 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 **Developer Supported**.

Support Email: support@ke-la.com

Support Web: <https://ke-la.com/contact-us/>

Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration's download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient's determination, fulfilling reasonable obligations for support and maintenance.



Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Actively Supported.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
-----------------------------	-------

Compatible with ThreatQ Versions	>= 4.28.0
----------------------------------	-----------

Support Tier	Developer Supported
--------------	---------------------

ThreatQ Marketplace	https:// marketplace.threatq.com/ details/kela-monitor-cdf
---------------------	---

Introduction

The KELA Monitor integrations allows a user to automatically load new incidents from the KELA monitoring platform directly to the ThreatQ platform.

The monitor integrations are according to their matched KELA modules:

- KELA Monitor Leaked Credentials
- KELA Monitor Compromised Accounts
- KELA Monitor Instant Messaging
- KELA Monitor Hacking Discussions
- KELA Monitor Network Vulnerabilities

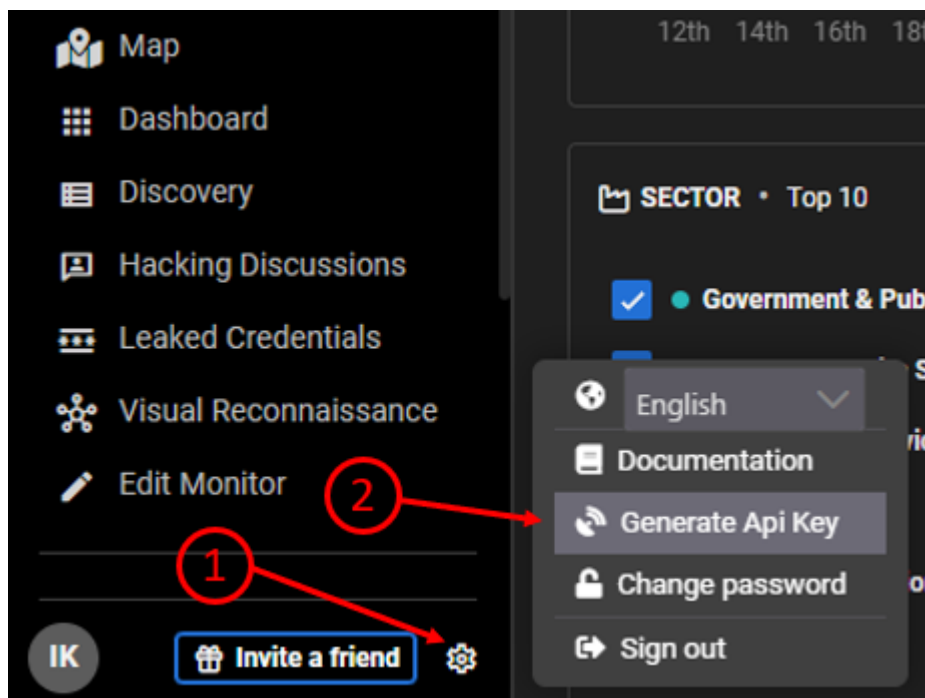
Each integration creates its own threat objects of type Incidents, together with other objects depending on the integration.

Prerequisites

Review the following requirements before attempting to install the integration.

KELA API Key

All integrations require the use of an API Key that can be obtained from within the KELA platform, by clicking on the gear icon on the left side bar, and then choosing the **Generate API key** option.

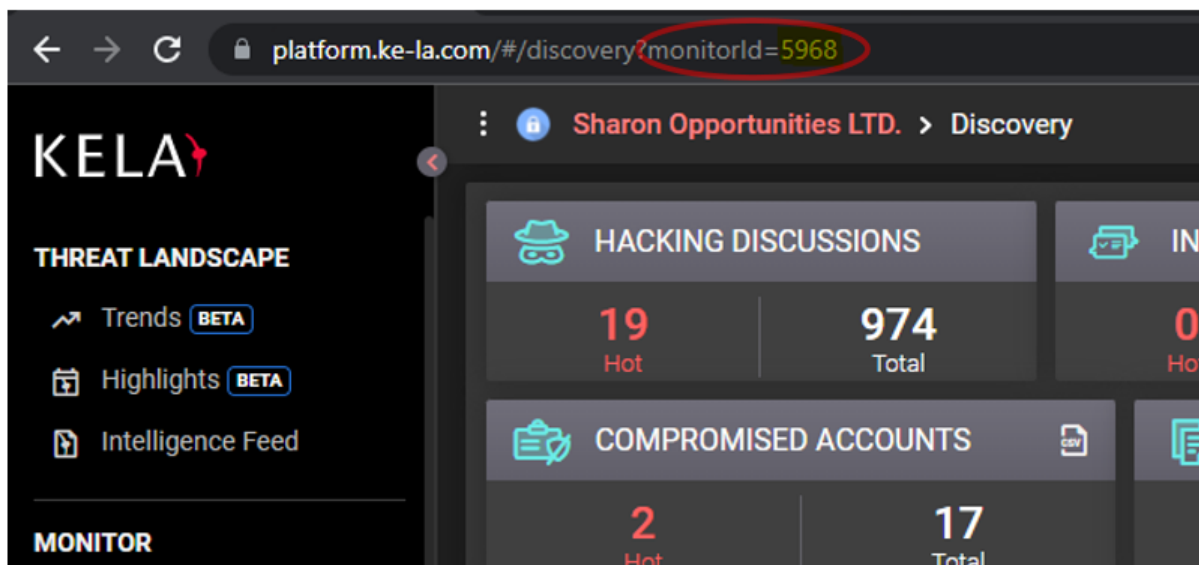


Key will be presented on the opened window.

KELA Monitor ID

For monitoring integrations, there is also a need for the getting the monitor ID from the KELA platform. This ID can be obtained from the URL when going into the monitor in the platform.

Example: The URL for monitor ID 5968 will look as follows:



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

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

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 **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key (All feeds)	Your KELA API Key. See the KELA API Key section for more information.
Workspace ID (All feeds)	Your Monitor ID. See the KELA Monitor ID section for more information.
Company/Organization Name (All feeds)	The company or organization name that the monitor is associated with. <div> This field is not required but may be useful in multi-tenant implementations for separation of alerts.</div>

PARAMETER	DESCRIPTION
Captured Passwords <i>(KELA Monitor Leaked Credentials, KELA Monitor Compromised Accounts, KELA Monitor Instant Messaging feeds only)</i>	When enabled, passwords will be captured from KELA if they are available.
Capture Dump Descriptions <i>(KELA Monitor Leaked Credentials feed only)</i>	Retrieved the detail description for leaked credentials coming from leaked dumps for each related dump. <div> Enabling this feature will slow down feed pull execution.</div>
Capture Identified Hostnames as Indicators <i>(KELA Monitor Leaked Credentials and KELA Monitor Compromised Accounts feeds only)</i>	Enable/disable the option to capture Identified Hostnames as Indicators.
Ingest CVEs as... <i>(KELA Monitor Network Vulnerabilities feed only)</i>	Configure how CVEs will be ingested. Options include: <ul style="list-style-type: none">◦ Indicators (default)◦ Vulnerability
Hostnames as Indicators <i>(KELA Monitor Network Vulnerabilities feed only)</i>	Enable/disable the ingestion of Hostnames as Indicators.
IPs as Indicators <i>(KELA Monitor Network Vulnerabilities feed only)</i>	Enable/disable the ingestion of IPs as Indicators.

< KELA Monitor Leaked Credentials



Disabled ☐ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

Configuration Activity Log

API Key 

Workspace ID

Company/Organization Name

The company or organization name that the monitor is associated with. Not required, but useful in multi-tenant implementations for separation of alerts.

☐ Capture Passwords

When checked, passwords will be captured from KELA if they are available.

☐ Capture Dump Descriptions

Get detailed descriptions - please note that this will slow down feed execution.

☐ Capture identified hostnames as indicators

Set indicator status to...

Active

Run Frequency

Every 24 Hours

☒ 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

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.

Known Issues / Limitations

- **KELA Monitor Leaked Credentials feed** - enabling the **Capture Dump Descriptions** configuration option will slow down feed pull execution.

Change Log

- Version 1.0.0
 - Initial release