ThreatQuotient

A Securonix Company

iZoologic Operation

Version 1.0.0

February 17, 2026

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

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.

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	>= 5.9.0
Support Tier	ThreatQ Supported

Introduction

The iZoologic Operation enables analysts to take action on individual iZoologic cases directly from within the ThreatQ platform, streamlining case management and response workflows. By integrating with iZOOlabs, a global security laboratory and operations center specializing in cybercrime mitigation, this operation allows users to update and manage cases efficiently while maintaining visibility and coordination between ThreatQ and iZoologic systems.

The integration provides the following operation actions:

- **Send Case Message -** sends a communication message to the iZoologic team for the specified case.
- **Approve Case Takedown** - approves incident cases for takedown.
- **Mark as Reviewed -** marks a case as reviewed.
- **Move Case -** moves a case from one case type to another

The operation is compatible with the following object types:

- Events
- Identities

Prerequisites

The following is required to run the integration:

- Your iZoologic API Hostname.
- Your iZoologic API Key - located under the **Account** > **Profile** > **API Key**.
- Your iZoologic Secret Key - located under the **Account** > **Profile** > **API Key**.

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.

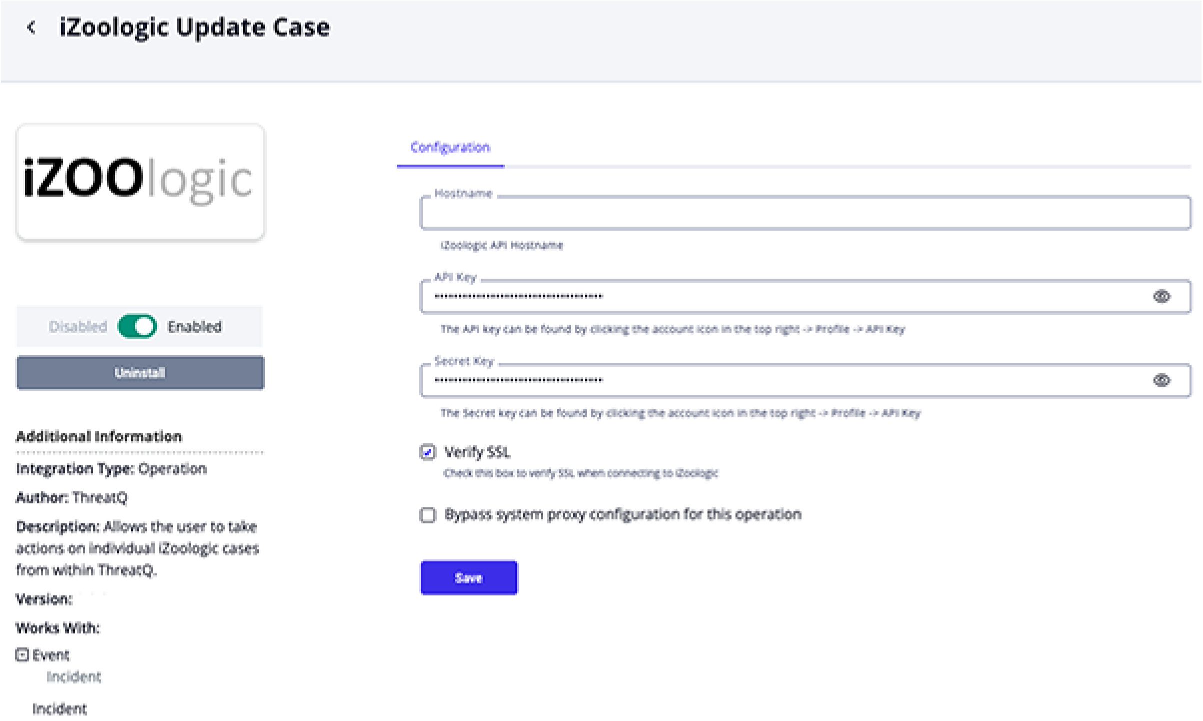
Configuration

> 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
Hostname	Enter the iZoologic API Hostname.
API Key	Enter your iZoologic API Key.
Secret Key	Enter your iZoologic Secret Key.
Verify SSL	Enable this parameter if the integration should validate the host-provided SSL certificate.



iZoologic Update Case

Hostname

iZoologic API Hostname

API Key: ••••••••••••••••••••••••••••••••••••

The API key can be found by clicking the account icon in the top right -> Profile -> API Key

Secret Key: ••••••••••••••••••••••••••••••••••••

The Secret key can be found by clicking the account icon in the top right -> Profile -> API Key

☑ Verify SSL

Check this box to verify SSL when connecting to iZoologic

☐ Bypass system proxy configuration for this operation

Additional Information

Integration Type: Operation

Author: ThreatQ

Description: Allows the user to take actions on individual iZoologic cases from within ThreatQ.

Version:

Works With:

⊟ Event
Incident

Incident

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
Send Case Message	Sends a communication message to the iZoologic team for the specified case.	Incident, Event	N/A
Approve Case Takedown	Approve incident cases for takedown. Changes status from "Pending" to "Open" and triggers email notifications.	Incident, Event	N/A
Mark As Reviewed	Mark a case as reviewed by updating its review status and logging the action.	Incident, Event	N/A
Move Case	Move a case from one case type to another.	Incident, Event	N/A

Send Case Message

The Send Case Message operation action sends a communication message to the iZoologic team for the specified case. Messages are sent via email to the iZOOlabs support team and automatically logged in the case communication history for tracking and follow-up.

```
POST https://client-api.izoolabs.com/api/ThreatManagement/SendCaseMessage?CaseID=CASE123456&Subject=Urgent%20Follow-up&Message=Please%20provide%20status%20update%20on%20this%20phishing%20case&ClientCode=ABC
```

Sample Response:

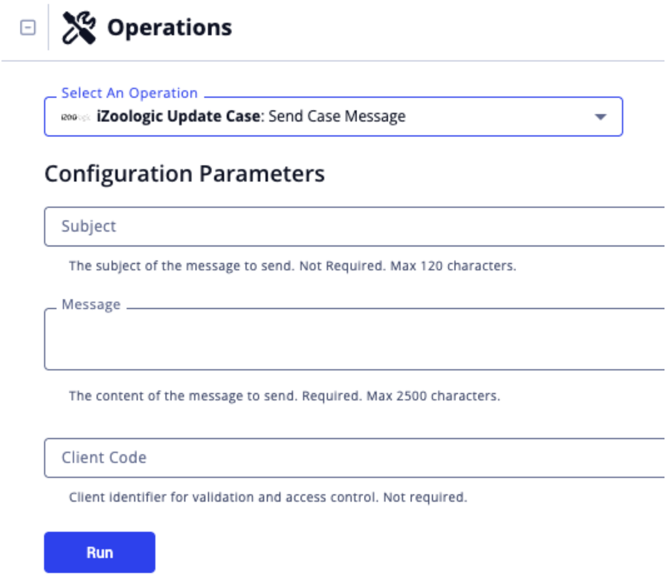
```
{
  "result": "Message sent successfully",
  "success": true,
  "message": null,
  "errorCode": null
}
```

Run Configuration Options

> These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is available after selecting the action:

RUN OPTION	DESCRIPTION
Subject	Enter the subject of the message to send. The character max for this option is 120.
Message	Enter the content of the message to send. The character max for this option is 2,500. This is required to run the operation action.
Client Code	Enter the client identifier for validation and access control.



Select An Operation: **iZoologic Update Case**: Send Case Message

Configuration Parameters

Subject

The subject of the message to send. Not Required. Max 120 characters.

Message

The content of the message to send. Required. Max 2500 characters.

Client Code

Client identifier for validation and access control. Not required.

Approve Case Takedown

The Approve Case Takedown operation action approves incident cases for takedown, changing the status from `Pending` to `Open`, and triggering email notifications.

`POST https://client-api.izoolabs.com/api/ThreatManagement/ApproveCaseTakedown`

Sample Body Example:

```
{
  "ids": "INC123456",
  "clientCode": "ABC",
  "remark": "Approved for immediate takedown - high priority threats"
}
```

Sample Response:

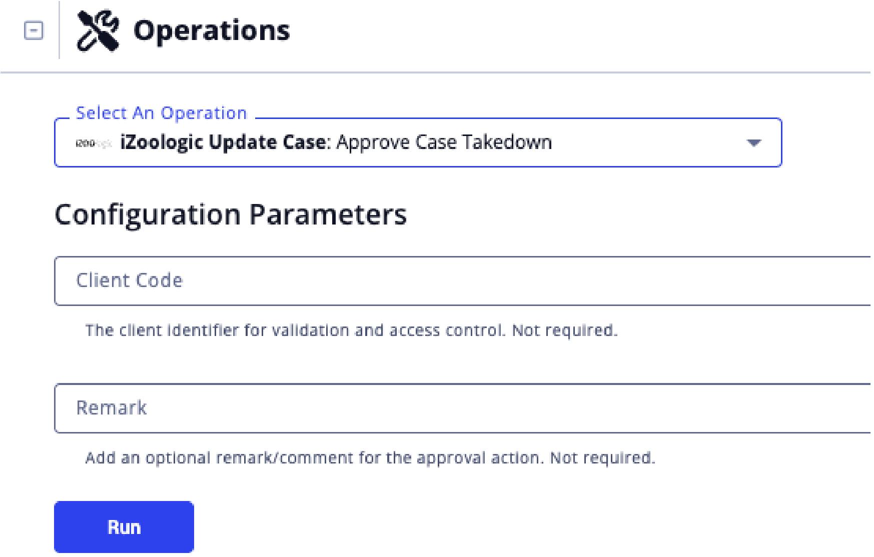
```
{
  "success": true,
  "message": "message": "Incidents approved for takedown",
  "errorCode": null
}
```

Run Configuration Options

> These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is available after selecting the action:

RUN OPTION	DESCRIPTION
Client Code	Enter the client identifier for validation and access control.
Remark	Enter optional remark to include with the takedown approval.



Select An Operation: **iZoologic Update Case**: Approve Case Takedown

Configuration Parameters

Client Code

The client identifier for validation and access control. Not required.

Remark

Add an optional remark/comment for the approval action. Not required.

Mark as Reviewed

The Mark as Reviewed operation action marks a case as reviewed by updating its review status and logging the action. It supports both incident cases and monitoring cases (Brand Abuse, Domain, Social Media, Mobile App, and Executive monitoring).

`POST https://client-api.izoolabs.com/api/ThreatManagement/MarkAsReviewed`

Sample Body:

```
{
  "ids": "INC123456",
  "clientCode": "CLIENT001",
  "remark": "Case reviewed and validated. No further action required."
}
```

Sample Response:

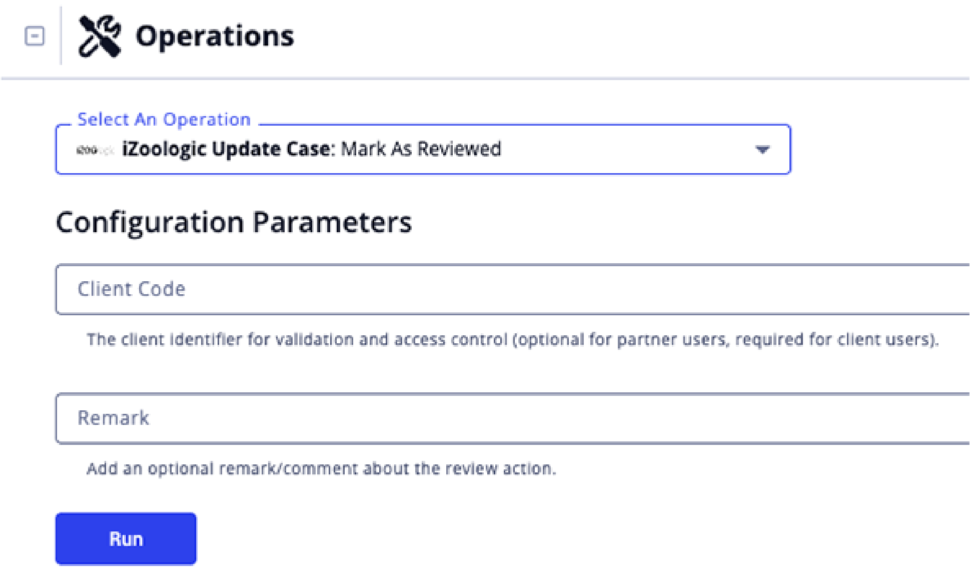
```
{
  "success": true,
  "message": "Cases Marked as Reviewed",
  "errorCode": null
}
```

Run Configuration Options

> These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is available after selecting the action:

RUN OPTION	DESCRIPTION
Client Code	Enter the client identifier for validation and access control. This is required for client users but optional for partner users.
Remark	Add an optional remark/comment about the review action.



Select An Operation
iZoologic Update Case: Mark As Reviewed

Configuration Parameters

Client Code

The client identifier for validation and access control (optional for partner users, required for client users).

Remark

Add an optional remark/comment about the review action.

Move Case

The Move Case operation action moves a case to a different status or queue within the iZoologic system.

```
POST https://client-api.izoolabs.com/api/ThreatManagement/SendCaseMessage?CaseID=CASE123456&Subject=Urgent%20Follow-up&Message=Please%20provide%20status%20update%20on%20this%20phishing%20case&ClientCode=ABC
```

Sample Body:

```
{
  "clientCode": "CLIENT001",
  "caseID": "CASE123456",
  "moveToCaseType": 6,
  "comment": "Moving case to incident for further investigation"
}
```

Sample Response:

```
{
  "result": {
    "Success": true,
    "Message": "Case moved successfully"
  },
  "success": true,
  "message": null,
  "errorCode": null
}
```

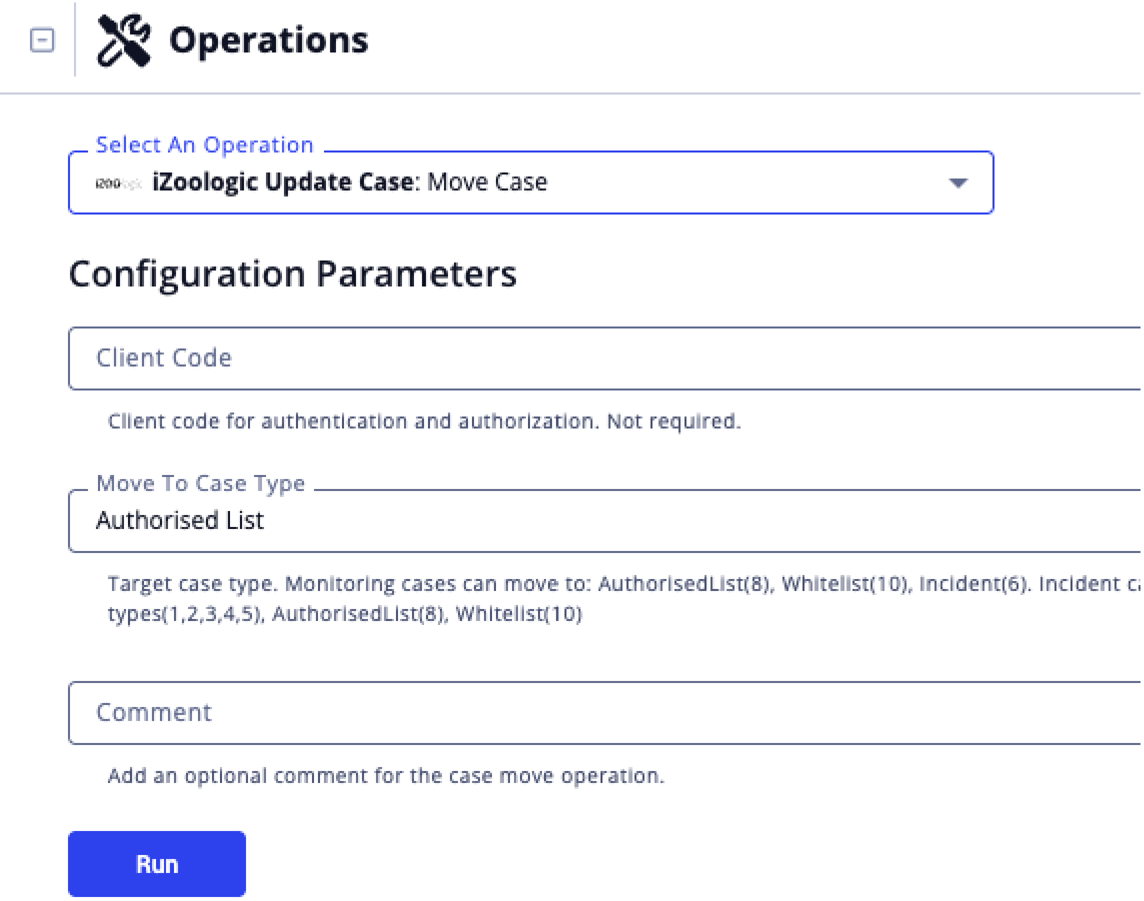
Run Configuration Options

> These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is available after selecting the action:

RUN OPTION	DESCRIPTION
Client Code	Enter the client code for authentication and authorization.
Move to Case Type	Select the Target case type. Monitoring cases can be moved to: • AuthorisedList(8) • Whitelist(10) • Incident(6) Incident cases can be moved to:

RUN OPTION	DESCRIPTION
	• All Monitoring types(1,2,3,4,5) • AuthorisedList(8) • Whitelist(10).
Comment	Enter an optional comment for the case move operation.



Operations

Select An Operation: **iZoologic Update Case:** Move Case

Configuration Parameters

Client Code

Client code for authentication and authorization. Not required.

Move To Case Type: Authorised List

Target case type. Monitoring cases can move to: AuthorisedList(8), Whitelist(10), Incident(6). Incident ca types(1,2,3,4,5), AuthorisedList(8), Whitelist(10)

Comment

Add an optional comment for the case move operation.

Known Issues / Limitations

- ThreatQ system egress IP Address may need to be whitelisted with iZoologic - contact iZoologic support for assistance.

Change Log

- **Version 1.0.0**
  - Initial release