ThreatQuotient

Exabeam IOC Exporter Action

Version 1.0.0

November 11, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

Email: support@threatq.com
Web: support.threatq.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: 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	1.0.0
Compatible with ThreatQ Versions	>= 5.25.0
Compatible with Exabeam API Versions	>= 1.0.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Exabeam IOC Exporter Action for ThreatQ enables the automatic dissemination of IOCs from a ThreatQ data collection to Exabeam Context Tables.

The integration provides the following action:

- **Exabeam IOC export -** exports IP Address and FQDN IOCs to Exabeam Context Tables in dedicated custom tables.

The action is compatible with the following indicator types:

- FQDN
- IP Address

As the action is designed to export ThreatQ objects to your Exabeam Context Tables, the action does not return enriched threat data back to the ThreatQ platform.

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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- An Exabeam Client ID and Client Secret. Permissions for Context Management are required for this account.
- A data collection containing at least one of the following indicator types:
    - FQDN
    - IP Address

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

> 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.

You will still need to configure the action.

Configuration

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

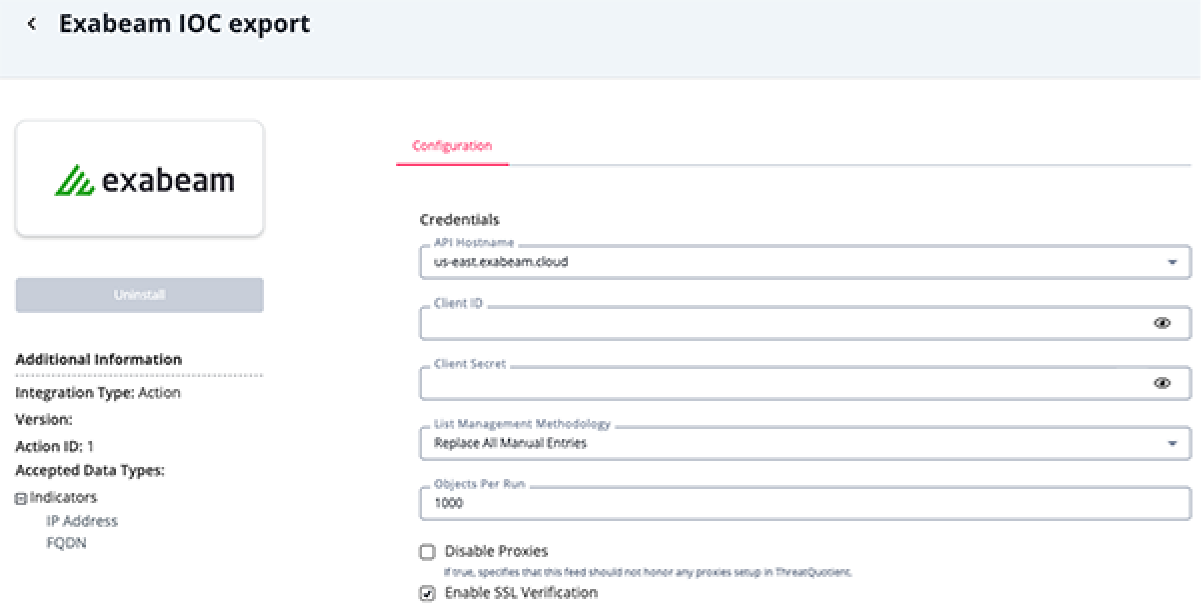
To configure the integration:

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 Hostname	Select your Exabeam API hostname from the dropdown. Options include: ◦ us-west.exabeam.cloud ◦ us-east.exabeam.cloud ◦ sg.exabeam.cloud ◦ jp.exabeam.cloud ◦ eu.exabeam.cloud ◦ au.exabeam.cloud ◦ ca.exabeam.cloud ◦ ch.exabeam.cloud
Client ID	Enter your Exabeam Client ID. ⚠ This account must have Context Management permissions on the specified hostname.
Client Secret	Enter your Exabeam Client Secret. ⚠ This account must have Context Management permissions on the specified hostname.

PARAMETER	DESCRIPTION
List Management Methodology	Select the operation mode to ingest indicators. Options include: ◦ Replace All Manual Entries ◦ Append New Entries
Objects Per Run	Enter the max number of objects per run to send to this action. The default value is 1000.
Enable SSL Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.



Exabeam IOC export

Additional Information

Integration Type: Action

Version:

Action ID: 1

Accepted Data Types:

⊟ Indicators
IP Address
FQDN

Credentials

API Hostname: us-east.exabeam.cloud

Client ID:

Client Secret:

List Management Methodology: Replace All Manual Entries

Objects Per Run: 1000

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

☑ Enable SSL Verification

5. 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
Exabeam IOC Export	Exports IP Addresses and FQDNs to Exabeam	Indicator	IP Address, FQDN

Exabeam IOC Export

The Exabeam IOC Export action takes a collection of Indicators (FQDN, IP Address) and exports it to Exabeam in dedicated tables based on indicator type.

- `tq_domain_table` table for FQDNs.
- `tq_ip_address_table` table for IP Addresses.

> If the custom tables do not exist, the action will create them.

Creating Custom Context Management Table

`POST https://{hostname}/context-management/v1/tables/`

Sample Request for Custom IP Addresses Table:

```
{
  "contextType": "Other",
  "source": "Custom",
  "name": "tq_ip_address_table",
  "attributes": [
    {
      "id": "ti_ip_address",
      "isKey": true
    }
  ]
}
```

Sample Request for Custom FQDNs Table:

```
{
  "contextType": "Other",
  "source": "Custom",
  "name": "tq_domain_table",
  "attributes": [
    {
      "id": "ti_domain",
      "isKey": true
    }
  ]
}
```

Sample Response:

```
{
    "table": {
        "attributeMapping": [],
        "attributes": [
            {
                "displayName": "Domain",
                "id": "ti_domain",
                "isKey": true,
                "type": "string"
            }
        ],
        "contextType": "Other",
        "id": "y1pXvWWRkb",
        "name": "test",
        "source": "Custom",
        "totalItems": 0
    },
    "url": "http://api.us-east.exabeam.cloud/context-management/v1/tables/
y1pXvWWRkb"
}
```

Add Records to Custom Context Management Table

`POST https://{hostname}/context-management/v1/tables/{table_id}/addRecords`

Sample Request

```
{
  "operation": "append",
  "data": [
    {
      "ti_domain": "download.uberlingen.com"
    }
  ]
}
```

Sample Response:

```
{
  "jsonEntries": 1,
  "totalDuplicates": 0,
  "totalIgnoredMissingKey": 0,
  "trackerId": "c9e72c9bd4944966af19e5d049c213ef"
}
```

Use Case Example

1. A user submits a collection of FQDN/ IP Address indicators using `Exabeam IOC Export` action to be appended or replaced to Exabeam context management tables.
2. The action first searches for `tq_domain_table` and `tq_ip_address_table` tables in Exabeam context management and creates them, if they do not exist.
3. The action sends the collection in batches of 50 indicators based on their type to Exabeam, where they are saved.

Known Issues / Limitations

- The Exabeam Add Context Records endpoint has a content length limitation. In response to this limitation, the action will send indicators in batches of 50 to Exabeam.

Change Log

- **Version 1.0.0**
    - Initial release