ThreatQuotient

Cisco ESA Export IOC Action Bundle

Version 1.0.1

July 01, 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	1.0.1
Compatible with ThreatQ Versions	>= 5.20.0
Compatible with Cisco Async OS API	>=14.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Cisco ESA Export IOC Action Bundle uses AsyncOS API for Cisco Secure Email Gateway to enable users to add or delete Safelist and Blocklist entries. Cisco Secure Email Gateway is an email security solution that blocks spam and security threats from the internet and prevents the accidental or intentional leakage of customer data.

The integration provides the following actions:

- **Cisco ESA Add Recipients To Quarantine List -** adds recipients to Safelist/Blocklist
- **Cisco ESA Add Senders To Quarantine List -** adds senders to Safelist/Blocklist
- **Cisco ESA Delete Recipients From Quarantine List -** deletes recipients from Safelist/Blocklist
- **Cisco ESA Delete Senders From Quarantine List -** deletes senders from Safelist/Blocklist

The actions are compatible with following indicator types:

- Email Address
- FQDN
- IP Address

> 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.
- A data collection containing the following indicator types:
  - Email Address
  - FQDN (**Add Senders to Quarantine List** and **Delete Senders from Quarantine List** only)
  - IP Address (**Add Senders to Quarantine List** and **Delete Senders from Quarantine List** only)
- A Cisco ESA Username and Password.
- The Cisco AsyncOS API must be enabled according to this documentation: https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-0/api/b_ESA_API_Guide_14-0/b_ESA_API_Guide_chapter_01.html

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.

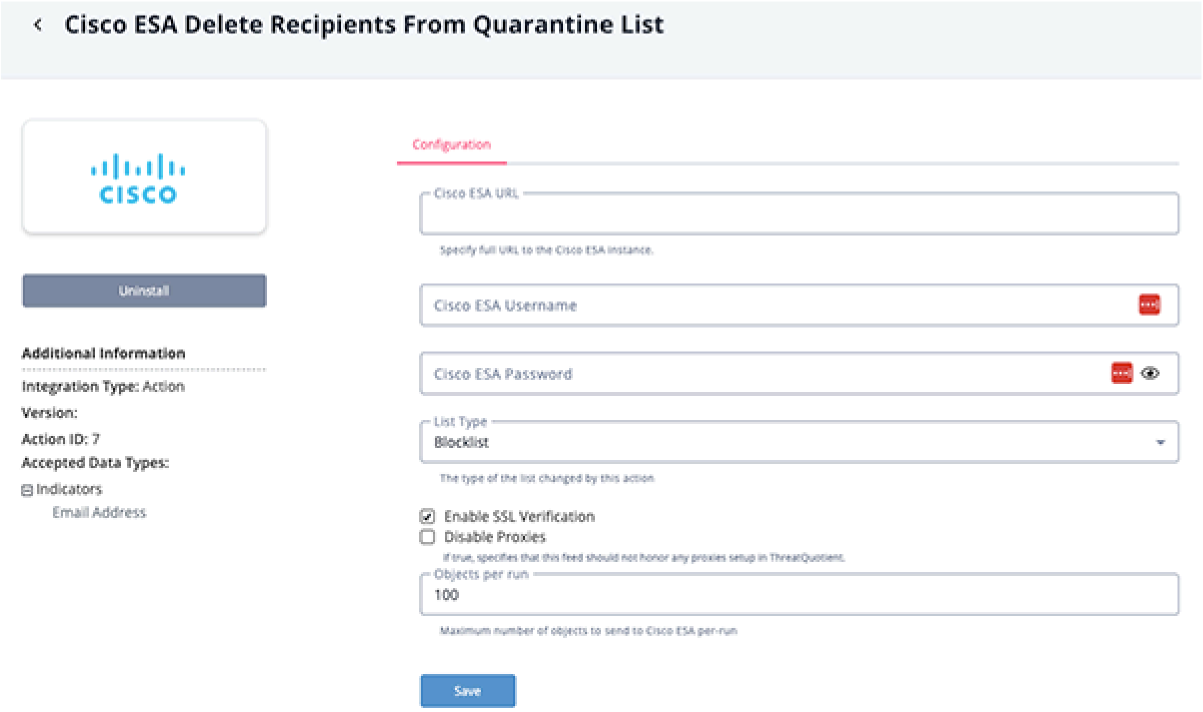
To configure the integration:

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
Cisco ESA URL	Enter the URL to your Cisco ESA instance (e.g https://cisco-esa.<domain>.com:<async-os-api-port>).
Cisco ESA Username	Enter your Cisco ESA Username.
Cisco ESA Password	Enter your Cisco ESA Password.
List Type	The type of the list changed by this action. Options: `Blocklist` or `Safelist`.
Recipient List *(Add Senders to Quarantine List only)*	A comma-separated list of valid Email Addresses. This list is set as recipient for the exported senders.
Sender List *(Add Recipients to*	Enter a comma-separated list of Email Addresses. This list is set as sender for the exported recipients. You can also add a domain to include all emails associated with it (example: threatq.com).

PARAMETER	DESCRIPTION
Quarantine List only)	
Enable SSL Verification	When checked, validates the host-provided SSL certificate. This parameter is enabled by default.
Disable Proxies	Enabling this option will have the action ignore proxy setting configured in ThreatQ.
Objects per run	Enter the maximum number of objects to send to Cisco ESA per-run.



Cisco ESA Delete Recipients From Quarantine List

Additional Information

Integration Type: Action

Version:

Action ID: 7

Accepted Data Types:

⊟ Indicators

Email Address

Cisco ESA URL

Specify full URL to the Cisco ESA instance.

Cisco ESA Username

Cisco ESA Password

List Type: Blocklist

The type of the list changed by this action

☑ Enable SSL Verification

☐ Disable Proxies

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

Objects per run: 100

Maximum number of objects to send to Cisco ESA per-run

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

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Cisco ESA Add Recipients To Quarantine List	Adds recipients to Safelist/Blocklist	Indicator	Email Address
Cisco ESA Add Senders To Quarantine List	Adds senders to Safelist/ Blocklist	Indicator	Email Address, FQDN, IP Address
Cisco ESA Delete Recipients From Quarantine List	Deletes recipients from Safelist/Blocklist	Indicator	Email Address
Cisco ESA Delete Senders From Quarantine List	Deletes senders from Safelist/Blocklist	Indicator	Email Address, FQDN, IP Address

Cisco ESA Add Recipients to Quarantine List

The Cisco Esa Add Recipients to Quarantine List action adds recipient entries to the Safelist or Blocklist - depending on action configuration.

`POST {{CISCO_ESA_URL}}/esa/api/v2.0/quarantine/blocklist?resource_attribute`

Sample Request Body:

```
{
  "action": "add",
  "quarantineType": "spam",
  "viewBy": "recipient",
  "recipientAddresses": [
    "user1@acme.com"
  ],
  "senderList": [
    "acme.com"
  ]
}
```

Sample Response:

```
{
  "data": {
    "action": "add",
    "recipientAddresses": [
      "user1@acme.com"
    ],
    "senderList": [
      "acme.com"
    ]
  }
}
```

Cisco ESA Add Senders to Quarantine List

The Cisco ESA Add Senders to Quarantine List action adds sender entries to either Safelist or Blocklist - depending on action configuration.

`POST {{CISCO_ESA_URL}}/esa/api/v2.0/quarantine/blocklist?resource_attribute`

Sample Request Body:

```
{
  "action": "append",
  "quarantineType": "spam",
  "viewBy": "sender",
  "senderAddresses": [
    "user1@acme.com"
  ],
  "recipientList": [
    "user2@acme.com"
  ]
}
```

Sample Response:

```
{
  "data": {
    "action": "append",
    "recipientList": [
      "user2@acme.com"
    ],
    "senderList": [
      "acme.com"
    ]
  }
}
```

Cisco ESA Delete Recipients from Quarantine List

The Cisco ESA Delete Recipients from Quarantine List action deletes recipient entries from the Safelist or Blocklist - depending on action configuration.

`DELETE {{CISCO_ESA_URL}}/esa/api/v2.0/quarantine/blocklist`

Sample Request Body:

```
{
  "quarantineType": "spam",
  "viewBy": "recipient",
  "recipientList": [
    "user1@acme.com"
  ]
}
```

Sample Request Body:

```
{
  "data": {
    "action": "delete",
    "totalCount": 1,
    "recipientList": [
      "user1@acme.com"
    ]
  }
}
```

Cisco ESA Delete Senders from Quarantine List

The Cisco ESA Delete Senders from Quarantine List action deletes sender entries from Safelist or Blocklist - depending on the action configuration.

`DELETE {{CISCO_ESA_URL}}/esa/api/v2.0/quarantine/blocklist`

Sample Request Body:

```
{
  "quarantineType": "spam",
  "viewBy": "sender",
  "senderList": [
    "user1@acme.com"
  ]
}
```

Sample Response:

```
{
  "data": {
    "action": "delete",
    "totalCount": 1,
    "senderList": [
      "user1@acme.com"
    ]
  }
}
```

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.

Cisco ESA Add Recipients To Quarantine List

METRIC	RESULT
Run Time	3 minutes
Indicators	50

Cisco ESA Add Senders To Quarantine List

METRIC	RESULT
Run Time	3 minutes
Indicators	50

Cisco ESA Delete Recipients From Quarantine List

METRIC	RESULT
Run Time	3 minutes
Indicators	50

Cisco ESA Delete Senders From Quarantine List

METRIC	RESULT
Run Time	3 minutes
Indicators	50

Known Issues / Limitations

- Adding already existing indicators to a Safelist/Blocklist returns a 409 error with possible connection closed errors. Due to security reasons, Pynoceros is not tolerant of network issues and the errors logged.
- The maximum number of entries that can be added to a list can be adjusted through the web interface of the Cisco ESA. The value must be in the range 1-500.

Change Log

- **Version 1.0.1**
  - Added a new configuration option for all actions: Disable Proxy. This allows users to determine whether or not the integration will honor ThreatQ proxy settings.
  - Added a new known limitation entry regarding the max number of entries that can be added to a list.
- **Version 1.0.0**
  - Initial release