ThreatQuotient

Netskope Action Bundle

Version 1.0.0

June 17, 2025

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	>= 6.1.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Netskope Action Bundle integration allow users to export data from the ThreatQ Threat Library to Netskope policies.

The integration bundle provides the following actions:

- **Netskope - Export File Profile Hashes** - exports hashes from ThreatQ to a Netskope File Profile.
- **Netskope - Manage URL List** - exports URLs or FQDNs from ThreatQ to a Netskope URL List.
- **Netskope - Fetch User Confidence Index Score** - ingest User Confidence Index (UCI) Score.
- **Netskope - Create User Confidence Index Impact** - creates a User Confidence Index (UCI) Impact.

The actions are compatible with the following object types:

- Identities
- Indicators
  - Email Address
  - FQDN
  - MD5
  - SHA-256
  - URL

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 at least one of the following object types:
  - Identity (Fetch User Confidence Index Score, Create User Confidence Index Impact)
  - Indicator
    - Email Address (Fetch User Confidence Index Score, Create User Confidence Index Impact)
    - FQDN (Manage URL List)
    - MD5 (Export File Profile Hashes)
    - SHA-256 (Export File Profile Hashes)
    - URL (Manage URL List)
- A Netskope instance.
- Action-specific requirements such as API tokens and permissions. See the entries below for each action's specific requirements.

Netskope - Export File Profile Hashes

The Export File Profile Hashes action requires the following:

- Netskope API v1 token. See https://docs.netskope.com/en/rest-api-v1-overview/ for more information.
- An existing Netskope File Profile with no pending changes. Be sure to apply all the pending changes otherwise the action will not run successful. See https://docs.netskope.com/en/adding-a-file-profile/ for instructions on how to create a Netskope File Profile.

Netskope - Manage URL List

The Manage URL List action requires the following:

- Neskope API V2 token.
  - The API token must have Read + Write Permissions for the following endpoints:
    - `/api/v2/policy/urllist`
    - `/api/v2/policy/urllist/deploy`

    See https://docs.netskope.com/en/rest-api-v2-overview for more information.

- An existing Netskope URL List. The URL List can have pending changes. See https://docs.netskope.com/en/url-lists for steps on how to create a Netskope URL List.

Netskope - Fetch User Confidence Index Score

The Fetch User Confidence Index Score action requires the following:

- Neskope API V2 token. See https://docs.netskope.com/en/rest-api-v2-overview for more information.
  - The API token must have Read Permissions for the following endpoints:
    - `/api/v2/incidents/uba/getuci`

Netskope - Create User Confidence Index Impact

The Create User Confidence Index Impact action requires the following:

- Neskope API V2 token. See https://docs.netskope.com/en/rest-api-v2-overview for more information.
  - The API token must have Read + Write Permissions for the following endpoints:
    - `/api/v2/incidents/user/uciimpact`

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:

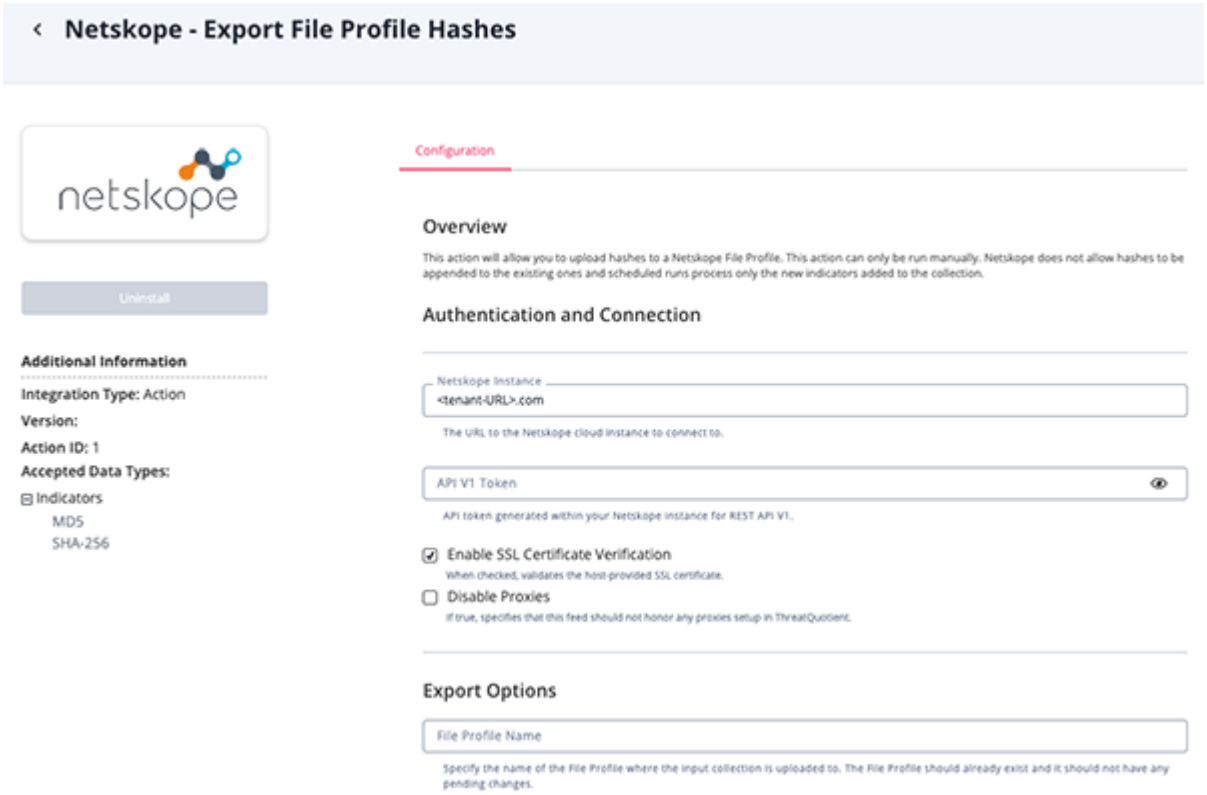
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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.

Export File Profile Hashes Parameters

PARAMETER	DESCRIPTION
Netskope Instance	The URL to the Netskope cloud instance.
API V1 Token	The API token generated within your Netskope instance for REST API V1.
Enable SSL Certificate 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.
File Profile Name	Specify the name of the File Profile where the input collection is uploaded to. The File Profile should already exist and it should not have any pending changes.

PARAMETER	DESCRIPTION
Objects per run	The maximum number of objects to process per-run. The default value is 1000.

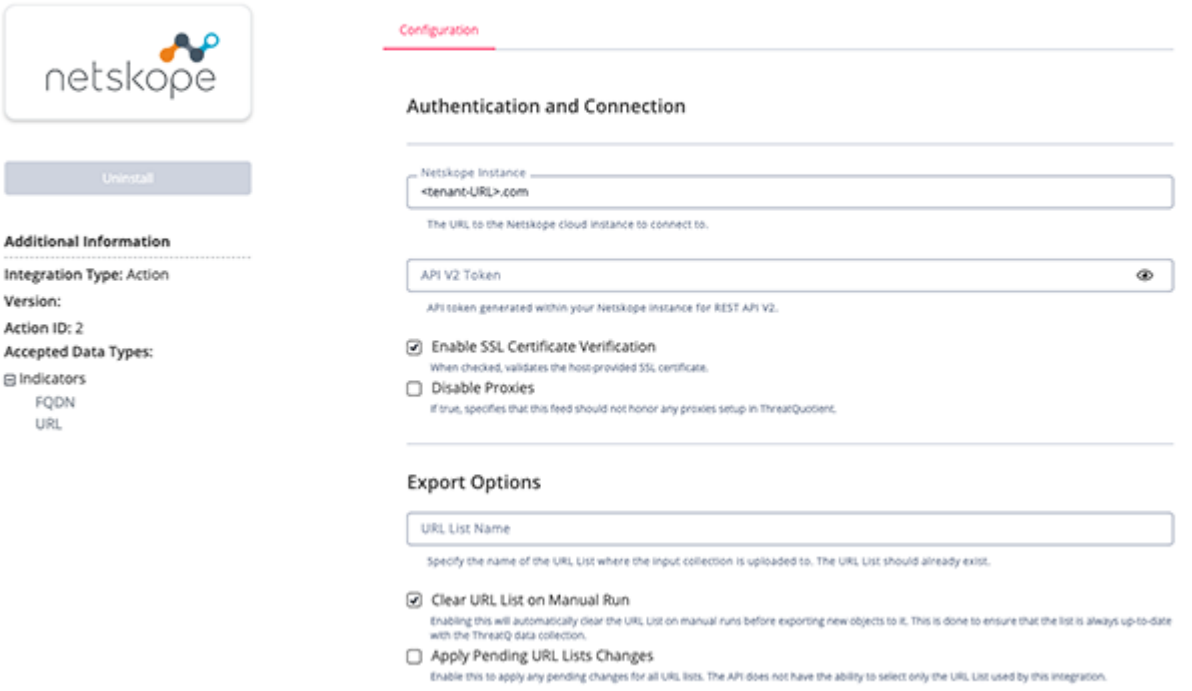


Manage URL List Parameters

PARAMETER	DESCRIPTION
Netskope Instance	The URL to the Netskope cloud instance.
API V2 Token	The API token generated within your Netskope instance for REST API V2.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.

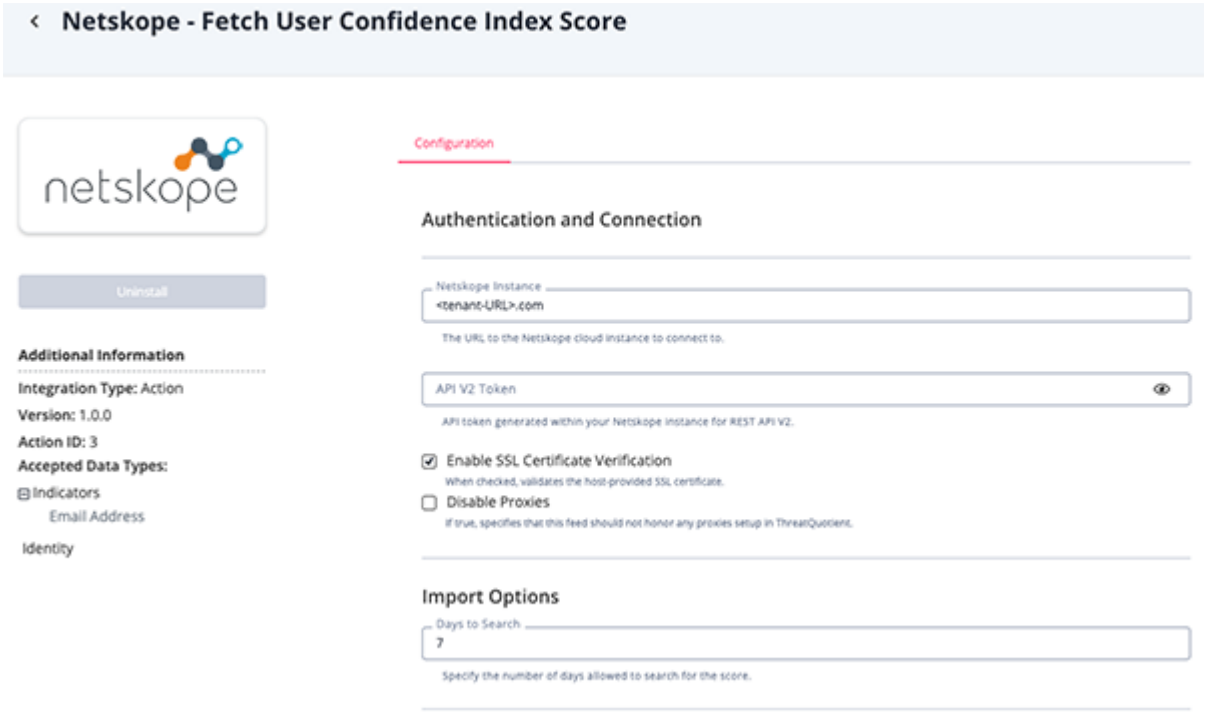
PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
URL List Name	Specify the name of the URL List where the input collection is uploaded to. The URL List should already exist.
Clear URL List on Manual Run	Enabling this will automatically clear the URL List on manual runs before exporting new objects to it. This is done to ensure that the list is always up-to-date with the ThreatQ data collection. This parameter is enabled by default.
Apply Pending URL Lists Changes	Enable this to apply any pending changes for all URL lists. The API does not have the ability to select only the URL List used by this integration.
Objects per run	The maximum number of objects to process per-run. The default value is 1000.

Netskope - Manage URL List



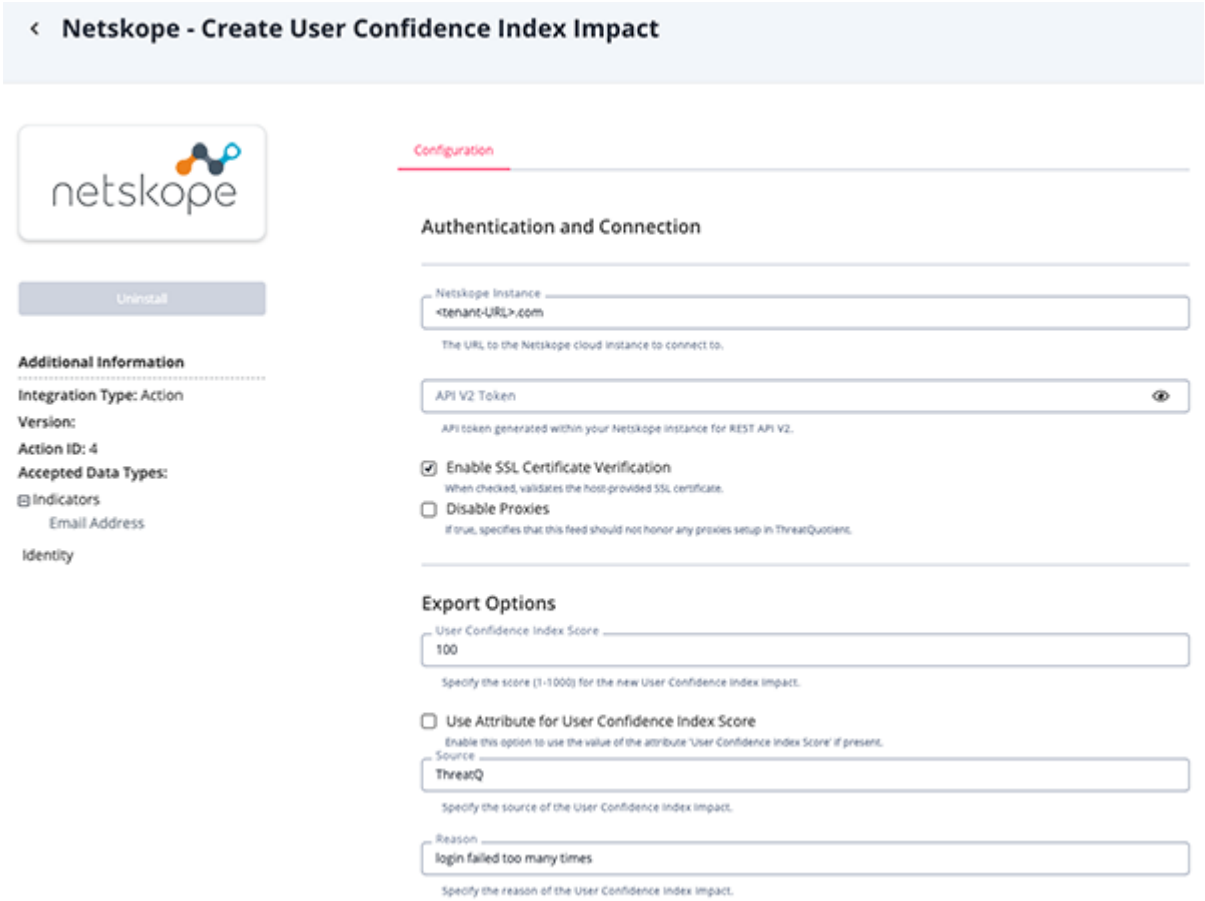
Fetch User Confidence Index Score Parameters

PARAMETER	DESCRIPTION
Netskope Instance	The URL to the Netskope cloud instance.
API V2 Token	The API token generated within your Netskope instance for REST API V2.
Enable SSL Certificate 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.
Days to Search	Specify the number of days allowed to search for the score. The default value is 7.
Objects per run	The maximum number of objects to process per-run. The default value is 1000.



Create User Confidence Index Impact Parameters

PARAMETER	DESCRIPTION
Netskope Instance	The URL to the Netskope cloud instance.
API V2 Token	The API token generated within your Netskope instance for REST API V2.
Enable SSL Certificate 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.
User Confidence Index Score	Specify the score (1-1000) for the new User Confidence Index Impact. The default value is 100.
Use Attribute for User Confidence Index Score	Enable this option to use the value of the attribute 'User Confidence Index Score' if present. This is disabled by default.
Source	Specify the source of the User Confidence Index Impact. The default value is `ThreatQ`).
Reason	Specify the reason of the User Confidence Index Impact. The default value is `login failed too many times.`
Objects per run	The maximum number of objects to process per-run. The default value is 1000.



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
Netskope - Export File Profile Hashes	Exports hashes from ThreatQ to a Netskope File Profile	Indicator	MD5, SHA-256
Netskope - Manage URL List	Exports URLs or FQDNs from ThreatQ to a Netskope URL List	Indicator	FQDN, URL
Netskope - Fetch User Confidence Index Score	Ingest User Confidence Index (UCI) Score	Indicator/ Identity	Email Address
Netskope - Create User Confidence Index Impact	Creates a User Confidence Index (UCI) Impact	Indicator/ Identity	Email Address

Netskop - Export File Profile Hashes

The Netskope - Export File Profile Hashes action exports indicators of type MD5 or SHA-256 to a Netskope File Profile. This action can only be run manually. Netskope does not allow hashes to be appended to the existing ones and scheduled runs process only the new indicators added to the collection. A scheduled run would only override the existing hashes in Netskope with the new ones that were added to the collection, this is why only manual runs are allowed.

> Netskope hash list maximum size is 8MB, the collection in truncated in case the size is exceeded.

`POST https://{NETSKOPE_TENANT}.com/api/v1/updateFileHashList`

Request Parameters:

```
{
  "name": "ThreatQ File Profile"
}
```

Request Body:

```
{
  "list":
"e28eb9739b6e84d0f796e3acc0f5b714,e28eb9739b6e84d0f697e3acc0f5b71a,e28eb9839b6e
74d0f696e3acc0f6b710"
}
```

Sample Response:

```
{
  "status": "success",
  "msg": "File Filter Profile updated successfully"
}
```

Netskope - Manage URL List

The Netskope - Manage URL List action uploads URLs and FQDNs from Threat Library to a Netskope URL List. The list must exist in Netskope and it can have pending changes. On manual run the integration can completely override the list from Netskope, or the new values are appended.

Request to Get the ID of the List

The action, at first, makes a call to get all the lists from Netskope. It searches in the result for the list having the name specified in the user configuration URL List Name.

`GET https://{NETSKOPE_TENANT}.com/api/v1/api/v2/policy/urllist`

Sample Response:

```
[
  {
    "id": 5,
    "name": "ThreatQ",
    "data": {
      "type": "exact",
      "urls": [
        "hello.threatq.com"
      ],
      "json_version": 2
    },
    "modify_by": "threatq",
    "modify_time": "2025-05-21T07:25:11.000Z",
    "modify_type": "Edited",
    "pending": 1
  }
]
```

Request to Update the URL List Content

The list ID (in this case 5) is taken from the previous request.

Append new indicators`PATCH https://{NETSKOPE_TENANT}.com/api/v1/api/v2/policy/urllist/5/append`

Delete existing indicators and add the new ones`PATCH https://{NETSKOPE_TENANT}.com/api/v1/api/v2/policy/urllist/5/replace`

Request Body:

```
{
  "data": {
    "type": "exact",
    "urls": [
      "hello2.threatq.com",
      "hello2.threatq.com/dashboard"
```

```
    ]
  }
}
```

Sample Response:

```
{
  "id": 5,
  "name": "ThreatQ",
  "data": {
    "type": "exact",
    "urls": [
      "hello.threatq.com",
      "hello2.threatq.com",
      "hello2.threatq.com/dashboard"
    ],
    "json_version": 2
  },
  "modify_by": "threatq",
  "modify_time": "2025-05-21T12:49:40.000Z",
  "modify_type": "Edited",
  "pending": 1
}
```

Netskope - Fetch User Confidence Index Score

The Netskope - Fetch User Confidence Index Score action ingests the User Confidence Index (UCI) Score for each value from the input ThreatQ collection. The score is ingested only if it is more recent then the number of days specified in the user configuration `Days to Search`.

`POST https://{NETSKOPE_TENANT}.com/api/v1/api/v2/incidents/uba/getuci`

Request Body:

```
{
  "fromTime": 1717372800000,
  "users": [
    "user1@silverfort.com",
    "user2@silverfort.com"
  ]
}
```

Sample Response:

```
{
  "usersUci": [
    {
      "userId": "user1@silverfort.com",
      "confidences": []
    },
    {
      "userId": "user2@silverfort.com",
      "confidences": [
        {
          "start": 1748995200000,
          "confidenceScore": 650
        },
        {
          "start": 1749081600000,
          "confidenceScore": 103
        }
      ]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this action based on each item within the `usersUci list`:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.userId`	Identity/Indicator	Identity/Email Address	N/A	`user2@silverfort.com`	Preserves the object type from the input collection.
`.confidences[].confidenceScore`	Identity/ Indicator.Attribute	User Confidence Index Score	N/A	`650`	The maximum value is selected. Updatable.

Netskope - Create User Confidence Index Impact

The Netskope - Create User Confidence Index Impact action creates a User Confidence Index (UCI) Impact. The timestamp of the impact is the moment when the integration is run.

If the user configuration `Use Attribute for User Confidence Index Score` is set to `False` then the score of the impact is taken from the user configuration `User Confidence Index Score`. Otherwise, the score is the value of the attribute `User Confidence Index Score` in case it exists. In case the attribute `User Confidence Index Score` has multiple values the maximum value is selected.

`POST https://{NETSKOPE_TENANT}.com/api/v1/api/v2/incidents/user/uciimpact`

Request Body:

```
{
  "user": "user1@silverfort.com",
  "score": 200,
  "timestamp": 1717372800000,
  "source": "ThreatQ",
  "reason": "login failed too many times"
}
```

Sample Response:

```
{
  "activity": "ActivityForUciImpactAPI",
  "anomalyCreatedTime": "2025-06-05T13:00:20Z",
  "anomalyId": "54cde79c419867912de0c342",
  "eventId": "54cde79c419867912de0c342",
  "reason": "login failed too many times",
  "score": 200,
  "source": "ThreatQ",
  "time": 1717372800000,
  "user": "user1@silverfort.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.

Netskope - Fetch User Confidence Index Score

METRIC	RESULT
Run Time	2 minutes
Identities	100
Identity Attributes	70

Known Issues / Limitations

- The Maximum size of the File Profile Hash List is 8 MB. List larger than 8 MB will be truncated.

Change Log

- **Version 1.0.0**
  - Initial release