ThreatQuotient

A Securonix Company

Infoblox Threat Intelligence Data Exchange (TIDE) CDF

Version 2.0.1

August 12, 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	2.0.0
Compatible with ThreatQ Versions	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Infoblox Threat Intelligence Data Exchange (TIDE) CDF allows ThreatQ to ingest several dozen threat intelligence feeds from Infoblox (i.e. SURBL, Exploit Kits, EECN, DHS AIS NCCIC, TOR, DoT/DoH, etc.), as well as numerous optional 3rd party threat indicator feeds.

> Additional open source, public, or private feeds can also be integrated through the Infoblox TIDE feature to further enhance ThreatQ capabilities.

The integration ingests Indicator system object types and offers the following feeds:

- **Infoblox TIDE** - allows a user to ingest lookalike FQDN indicators from the Infoblox TIDE database.
- **Infoblox TIDE Lookalike Domains -** allows a user to ingest FQDNs that have similar spelling as popular FQDNs.

The integration ingests indicator and indicator attribute object types.

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
6. Select the individual feeds to install, when prompted, and click **Install**.

    > 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.

7. 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:

Infoblox TIDE Configuration Parameters

PARAMETER	DESCRIPTION
Infoblox TIDE Hostname	The Infoblox TIDE Hostname.
API Key	The Infoblox TIDE API key.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Threat Classes Filter	Enter a line-separated list of TIDE class names to filter the data by the threat class. Common properties include: Malicious, Phishing, APT, Bot, MalwareC2, MalwareDownload, Proxy, Sinkhole, Scam, and InternetInfrastructure.

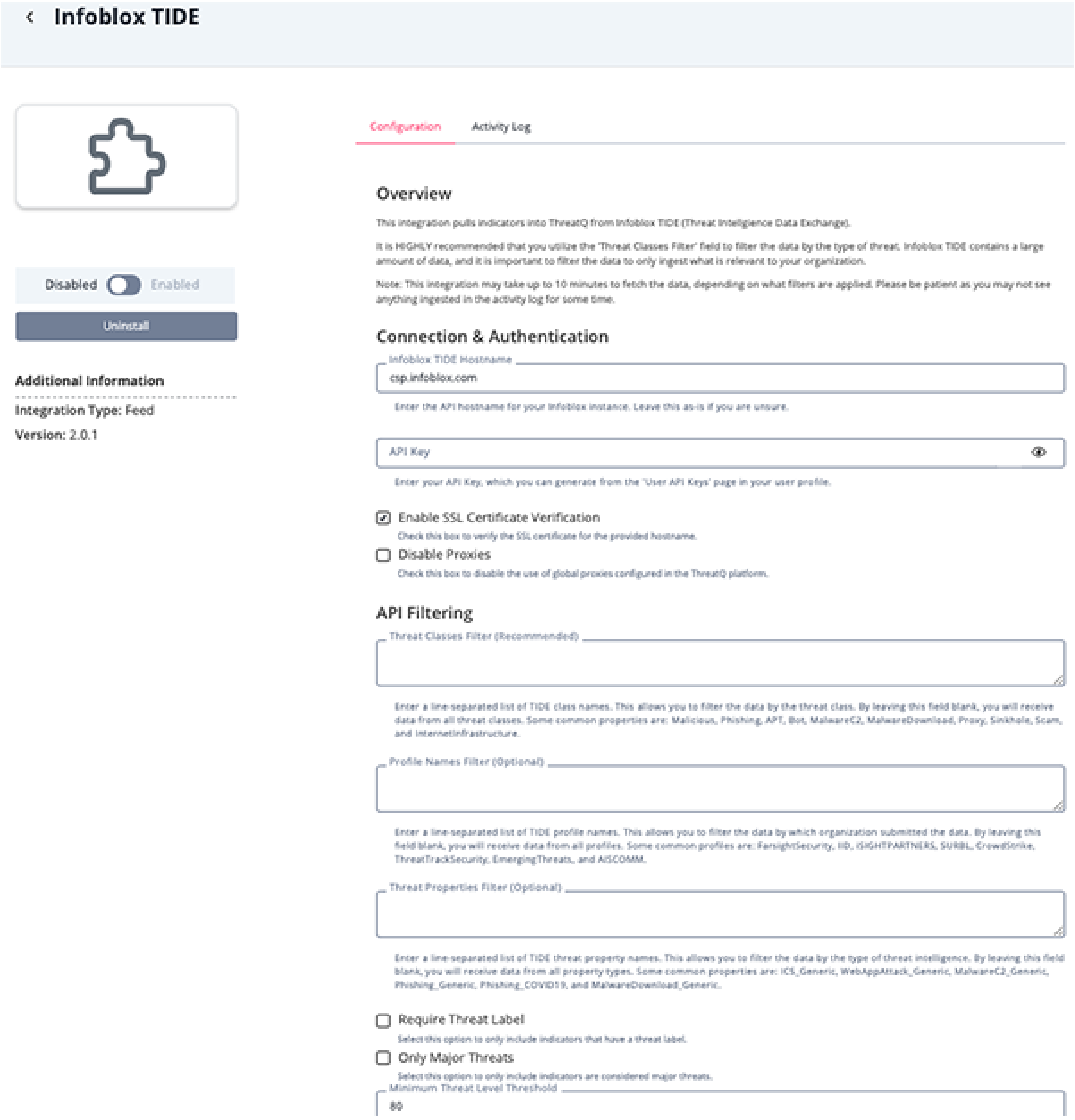
PARAMETER	DESCRIPTION
	ThreatQuotient recommends utilizing this parameter. Leaving this field blank will result in ingesting data from all threat classes.
Profile Names Filter	Optional - Enter a line-separated list of TIDE profile names to filter the data by which organization submitted the data. Common profiles include FarsightSecurity, IID, iSIGHTPARTNERS, SURBL, CrowdStrike, ThreatTrackSecurity, EmergingThreats, and AISCOMM. Leaving this field blank will result in ingesting data from all profiles.
Threat Properties Filter	Optional - Enter a line-separated list of TIDE threat property names to filter the data by the type of threat intelligence. Common properties are MalwareC2_Generic, Phishing_Generic, Phishing_COVID19, and MalwareDownload_Generic. Leaving this field blank will result in ingesting data from all property types.
Require Threat Label	Enable this parameter to only include indicators that have a threat label.
Only Major Threats	Enable this parameter to only include indicators that are considered major threats.
Minimum Threat Level Threshold	Enter a numeric value to represent the minimum threat level required to ingest an indicator. ThreatQuotient recommends using the default value of `80` to only ingest indicators that are considered high or critical threats. Setting this value to `0` will result in the ingestion of all reported indicators.
Minimum Confidence Threshold	Enter a numeric value to represent the minimum confidence score required to ingest an indicator. ThreatQuotient recommends using the default value of `100` to only ingest indicators with a confirmed

PARAMETER	DESCRIPTION
	confidence level. Setting this value to `0` will result in the ingestion of all reported indicators.
Only Ingest Indicators That Are Up	Enable this parameter to filter out indicators that are detected as down and only ingest indicators that are currently up. This parameter is enabled by default.
Ingested Indicator Types	Select which types of indicators to ingest into ThreatQ. This allows you to customize what is brought into ThreatQ based on what is relevant and important to your organization. Options include: ◦ FQDNs *(default)* ◦ IP Addresses *(default)* ◦ URLs *(default)*
Attribute Selection	Select which pieces of context to ingest into ThreatQ. This allows you customize what is brought into ThreatQ based on what is relevant and important to your organization. Options include: ◦ Target *(default)* ◦ Confidence Score *(default)* ◦ Threat Score *(default)* ◦ Threat Type *(default)* ◦ Threat Property ◦ Profile ◦ TLD ◦ Detected At ◦ Received At ◦ Expires At *(default)* ◦ Is DGA *(default)*
Normalize Confidence Scores	Enable this parameter to normalize the Confidence Score and Threat Score from the default 0-100 range to a human readable value. The normalization will be based on the mapping field below. This is useful for developing a ThreatQ Scoring Policy that is based on these normalized values.

Confidence Score Normalization Mapping	Enter line-separated mapping, in csv format, to normalize the numeric confidence score values to the scorable attribute: **Normalized Confidence Score**. The raw Confidence Score value will always be ingested. This mapping should contain the following: Minimum, Maximum, Normalized values. The default mapping is:
	`0,39,Low`
	`40,79,Medium`
	`0,99,High`
	`100,100,Confirmed`

PARAMETER	DESCRIPTION
	This parameter is only accessible if the **Normalize Confidence Scores** parameter is enabled.
Normalize Threat Scores	Enable this parameter to normalize the Threat Score from the default 0-100 range to a human readable value. The normalization will be based on the mapping table provided in the **Threat Score Normalization Mapping** parameter. This parameter is useful for developing a ThreatQ Scoring Policy that is based on these normalized values.

Threat Score Normalization Mapping	Enter your line-separated mapping, in csv format, to the scorable attribute: **Normalized Threat Score**. The raw Threat Score value will always be ingested. This mapping should contain a line-separated CSV formatted string with the following: Minimum, Maximum, Normalized values. The default mapping is:
	`0,39,Low`
	`40,79,Medium`
	`80,94,High`
	`95,100,Critical`
	This parameter is only accessible if the **Normalize Threat Scores** parameter is enabled.



Additional Information

Integration Type: Feed

Version: 2.0.1

Overview

This integration pulls indicators into ThreatQ from Infoblox TIDE (Threat Intelligence Data Exchange).

It is HIGHLY recommended that you utilize the 'Threat Classes Filter' field to filter the data by the type of threat. Infoblox TIDE contains a large amount of data, and it is important to filter the data to only ingest what is relevant to your organization.

Note: This integration may take up to 10 minutes to fetch the data, depending on what filters are applied. Please be patient as you may not see anything ingested in the activity log for some time.

Connection & Authentication

Infoblox TIDE Hostname: csp.infoblox.com

Enter the API hostname for your Infoblox instance. Leave this as-is if you are unsure.

API Key

Enter your API Key, which you can generate from the 'User API Keys' page in your user profile.

☑ Enable SSL Certificate Verification

Check this box to verify the SSL certificate for the provided hostname.

☐ Disable Proxies

Check this box to disable the use of global proxies configured in the ThreatQ platform.

API Filtering

Threat Classes Filter (Recommended)

Enter a line-separated list of TIDE class names. This allows you to filter the data by the threat class. By leaving this field blank, you will receive data from all threat classes. Some common properties are: Malicious, Phishing, APT, Bot, MalwareC2, MalwareDownload, Proxy, Sinkhole, Scam, and InternetInfrastructure.

Profile Names Filter (Optional)

Enter a line-separated list of TIDE profile names. This allows you to filter the data by which organization submitted the data. By leaving this field blank, you will receive data from all profiles. Some common profiles are: FarsightSecurity, IID, iSIGHTPARTNERS, SURBL, CrowdStrike, ThreatTrackSecurity, EmergingThreats, and AISCOMM.

Threat Properties Filter (Optional)

Enter a line-separated list of TIDE threat property names. This allows you to filter the data by the type of threat intelligence. By leaving this field blank, you will receive data from all property types. Some common properties are: ICS_Generic, WebAppAttack_Generic, MalwareC2_Generic, Phishing_Generic, Phishing_COVID19, and MalwareDownload_Generic.

☐ Require Threat Label

Select this option to only include indicators that have a threat label.

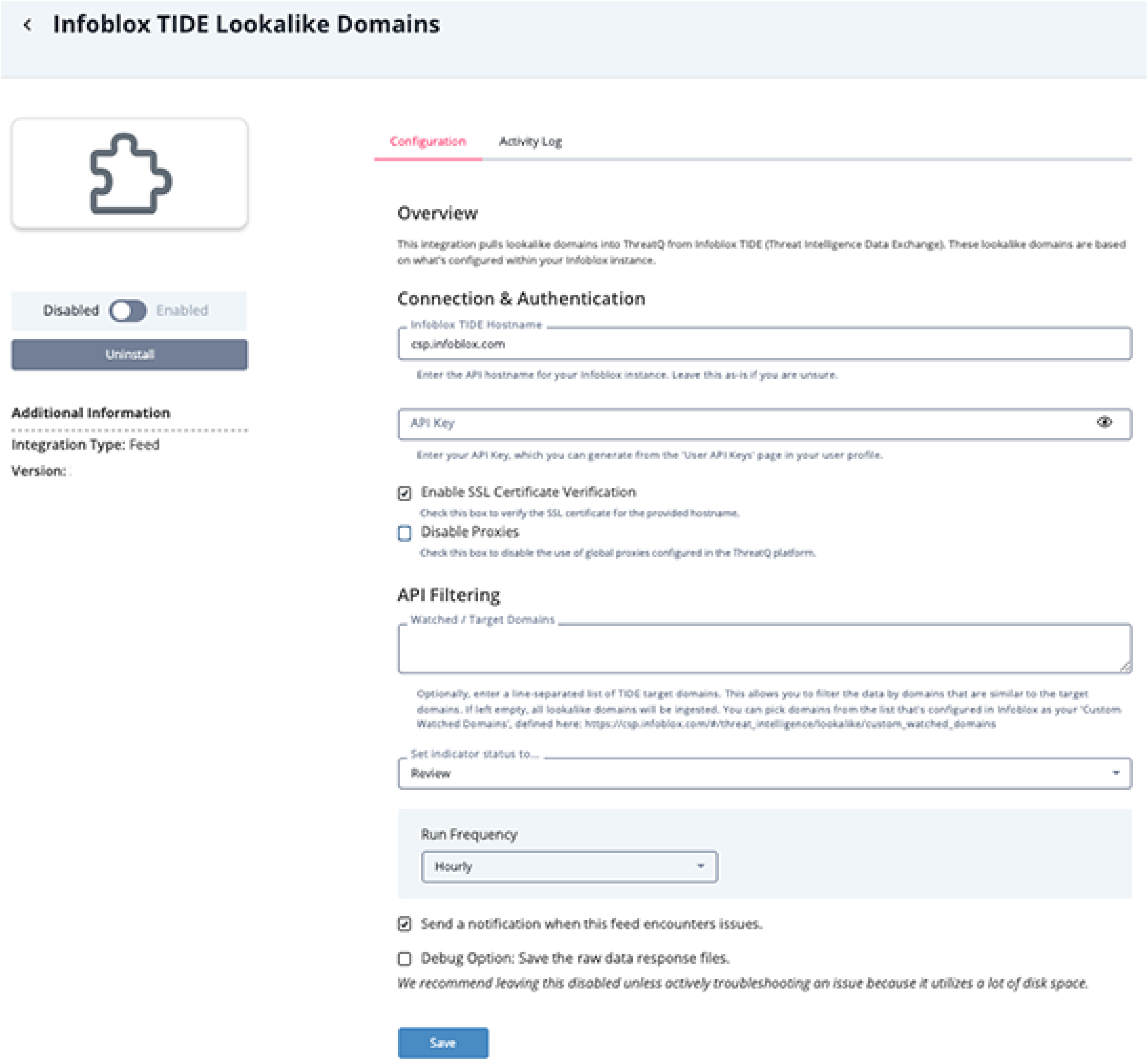
☐ Only Major Threats

Select this option to only include indicators are considered major threats.

Minimum Threat Level Threshold: 80

Infoblox TIDE Lookalike Domains Configuration Parameters

PARAMETER	DESCRIPTION
Infoblox TIDE Hostname	The Infoblox TIDE Hostname.
API Key	The Infoblox TIDE API key.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Watched / Target Domains	Enter a line-separated list TIDE target domains to specify the domain(s) to search for and return data on the lookalike domains. You can pick domains from the list that are configured in Infoblox as your 'Custom Watched Domains', defined at: https://csp.infoblox.com/#/threat_intelligence/lookalike/custom_watched_domains. Multiple Domain names should be entered in a comma-delimited format.



Additional Information

Integration Type: Feed

Version:

Overview

This integration pulls lookalike domains into ThreatQ from Infoblox TIDE (Threat Intelligence Data Exchange). These lookalike domains are based on what's configured within your Infoblox instance.

Connection & Authentication

Infoblox TIDE Hostname: csp.infoblox.com

Enter the API hostname for your Infoblox instance. Leave this as-is if you are unsure.

API Key

Enter your API Key, which you can generate from the 'User API Keys' page in your user profile.

☑ Enable SSL Certificate Verification

Check this box to verify the SSL certificate for the provided hostname.

□ Disable Proxies

Check this box to disable the use of global proxies configured in the ThreatQ platform.

API Filtering

Watched / Target Domains

Optionally, enter a line-separated list of TIDE target domains. This allows you to filter the data by domains that are similar to the target domains. If left empty, all lookalike domains will be ingested. You can pick domains from the list that's configured in Infoblox as your 'Custom Watched Domains', defined here: https://csp.infoblox.com/#/threat_intelligence/lookalike/custom_watched_domains

Set indicator status to...: Review

Run Frequency: Hourly

☑ 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.

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.

ThreatQ Mapping

Infoblox TIDE

The Infoblox TIDE and TIDE Lookalike Domains feed ingest lookalike FQDN indicators from the Infoblox TIDE database.

`GET https://csp.infoblox.com/tide/api/data/threats`

Sample JSON Response:

```
{
  "record_count": 3,
  "threat": [
    {
      "batch_id": "7d1d6343-eeaf-11ef-9ad1-5b0ed9e4cc77",
      "class": "Scam",
      "confidence": 100,
      "detected": "2025-02-19T10:50:49.813Z",
      "dga": false,
      "domain": "sdcne.com",
      "expiration": "2025-06-19T10:50:49.813Z",
      "extended": {
        "cyberint_guid": "4e1efcb72dcf46322085bffbd8a6023b",
        "notes": "Scam advertised via SMS. Lures victims to put their money
into fake investments."
      },
      "full_profile": "IID:ANALYST",
      "host": "sdcne.com",
      "id": "7d21d01c-eeaf-11ef-9ad1-5b0ed9e4cc77",
      "imported": "2025-02-19T10:51:35.776Z",
      "profile": "IID",
      "property": "Scam_Generic",
      "received": "2025-02-19T10:51:35.776Z",
      "threat_level": 100,
      "tld": "com",
      "type": "HOST",
      "up": true
    },
    {
      "batch_id": "e1f37c79-eeb0-11ef-b3ff-7bc3b35e5bcf",
      "class": "Scam",
      "confidence": 100,
      "detected": "2025-02-19T11:00:31.608Z",
      "dga": false,
      "domain": "usdcuu.com",
      "expiration": "2025-06-19T11:00:31.608Z",
      "extended": {
        "cyberint_guid": "36ff41945ab9068f082464bb424fb989",
        "notes": "Scam advertised via SMS. Lures victims to put their money
into fake investments."
      },
      "full_profile": "IID:ANALYST",
      "host": "usdcuu.com",
      "id": "e1f48dfe-eeb0-11ef-b3ff-7bc3b35e5bcf",
      "imported": "2025-02-19T11:01:34.428Z",
      "profile": "IID",
      "property": "Scam_Generic",
      "received": "2025-02-19T11:01:34.428Z",
      "threat_level": 100,
      "tld": "com",
      "type": "HOST",
      "up": true
    },
    {
      "batch_id": "e1f37c79-eeb0-11ef-b3ff-7bc3b35e5bcf",
      "class": "Scam",
      "confidence": 100,
      "detected": "2025-02-19T11:00:31.608Z",
      "dga": false,
      "domain": "btouqw.com",
      "expiration": "2025-06-19T11:00:31.608Z",
      "extended": {
        "cyberint_guid": "be10d82503db516bfa271a710baefd72",
        "notes": "Scam advertised via SMS. Lures victims to put their money
into fake investments."
      },
      "full_profile": "IID:ANALYST",
      "host": "btouqw.com",
      "id": "e1f48e0f-eeb0-11ef-b3ff-7bc3b35e5bcf",
      "imported": "2025-02-19T11:01:34.428Z",
      "profile": "IID",
      "property": "Scam_Generic",
      "received": "2025-02-19T11:01:34.428Z",
      "threat_level": 100,
      "tld": "com",
      "type": "HOST",
      "up": true
    }
  ]
}
```

ThreatQuotient provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.threat[].host,.threat[].ip, .threat[].url	Indicator. Value	FQDN, IP Address, URL	.threat[].imported	facebookforamericans.com	User-Configurable
.threat[].target	Indicator. Attribute	Target	.threat[].imported	facebook.com	User-Configurable
.threat[].confidence	Indicator. Attribute	Confidence Score	.threat[].imported	7.8	Updatable
.threat[].confidence	Indicator. Attribute	Normalized Confidence	.threat[].imported	Confirmed	Normalized based on user-field mapping. User-Configurable. Updatable
.threat[].threat_level	Indicator. Attribute	Threat Score	.threat[].imported	3.5	User-Configurable. Updatable
.threat[].threat_level	Indicator. Attribute	Normalized Threat Score	.threat[].imported	High	Normalized based on user-field mapping. User-Configurable. Updatable
.threat[].class	Indicator. Attribute	Threat Type	.threat[].imported	Policy	User-Configurable
.threat[].property	Indicator. Attribute	Threat Property	.threat[].imported	Policy_LookalikeDomains	User-Configurable
.threat[].profile	Indicator. Attribute	Profile	.threat[].imported	IID	User-Configurable
.threat[].tld	Indicator. Attribute	TLD	.threat[].imported	pl	User-Configurable
.threat[].detected	Indicator. Attribute	Detected At	.threat[].imported	2020-06-08 08:27:50-00:00	User-Configurable. Updatable
.threat[].received	Indicator. Attribute	Received At	.threat[].imported	2020-06-09 11:07:24-00:00	User-Configurable. Updatable
.threat[].expiration	Indicator. Attribute	Expires At	.threat[].imported	2020-06-09 08:10:33-00:00	User-Configurable. Updatable
.threat[].dga	Indicator. Attribute	Is DGA	.threat[].imported	false	User-Configurable
.threat[].extended.reason, .threat[].extended.notes	Indicator. Description	N/A	N/A	N/A	If `.threat[].extended` key is in ['protocol', 'references', 'attack_chain', 'registration_date']

Infoblox TIDE Lookalike Domains

The Infoblox TIDE Lookalike Domains feed ingest FQDNs that have similar spelling as popular FQDNs.

`GET https://csp.infoblox.com/api/tdlad/v1/lookalike_domains`

Sample JSON Response:

```
{
    "results": [
        {
            "detected_at": "2025-07-23T18:39:55Z",
            "lookalike_domain": "adamsapplesupport.com.au",
            "lookalike_host": "adamsapplesupport.com.au",
            "reason": "Domain is a lookalike to apple.com. The creation or first seen date is 2013-10-15.",
            "target_domain": "apple.com"
        },
        {
            "detected_at": "2025-07-23T18:39:55Z",
            "lookalike_domain": "aiappletools.com",
            "lookalike_host": "aiappletools.com",
            "reason": "Domain is a lookalike to apple.com. The creation or first seen date is 2024-08-18.",
            "target_domain": "apple.com"
        },
        {
            "detected_at": "2025-07-23T18:39:55Z",
            "lookalike_domain": "applers.ch",
            "lookalike_host": "applers.ch",
            "reason": "Domain is a lookalike to apple.com. The creation or first seen date is 2021-02-16.",
            "target_domain": "apple.com"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.lookalike_domain`	Indicator.Value	FQDN	`.detected_at`	facebookforamericans.com	N/A
`.lookalike_host`	Indicator.Value	FQDN	`.detected_at`	facebookforamericans.com	Only ingested if different from the domain
`.reason`	Indicator.Description	N/A	N/A	`Domain is a lookalike to apple.com. The creation or first seen date is 2013-10-15.`	Only ingested if different from the domain
`.target_domain`	Indicator.Attribute	Target Domain	`.detected_at`	`apple.com`	N/A
`.detected_at`	Indicator.Attribute	Detected At	`.detected_at`	`2025-07-23 18:39:55`	Updatable; UTC

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

With Target Domains: google.com

METRIC	RESULT
Run Time	5 minutes
Indicators	1,164
Indicator Attributes	17,564

With Target Domains: google.com,bing.com

METRIC	RESULT
Run Time	6 minutes
Indicators	1,241
Indicator Attributes	18,862

With Target Domains: google.com,bing.com,yahoo.com

METRIC	RESULT
Run Time	10 minutes
Indicators	3,062
Indicator Attributes	46,436

Lookalike Domains

METRIC	RESULT
Run Time	2 minutes
Indicators	1,402
Indicator Attributes	2,904

Known Issues / Limitations

- Occasionally during a feed run, the connector is unable to connect to the Infoblox server, resulting in the feed run completing without ingesting any indicators.

Change Log

- **Version 2.0.1**
    - Performed the following updates on the TIDE Lookalike Domains feed:
        - Resolved a pulling issue.
        - The feed now pulls from its own endpoint, `GET https://csp.infoblox.com/api/tdlad/v1/lookalike_domains`, opposed to using the TIDE endpoint.
        - Removed the following configuration parameters:
            - Threat Classes Filter
            - Profile Names Filter
            - Only Major Threats
            - Minimum Threat Level Threshold
            - Minimum Confidence Threshold
            - Only Ingest Indicators that are Up
            - Attribute Selection
            - Normalize Confidence Scores
            - Confidence Score Normalization Mapping
            - Normalize Threat Scores
            - Threat Score Normalization Mapping
- **Version 2.0.0**
    - Added ingestion rules that allow for certain attributes to be updated.
    - Added ability to normalize the confidence score and the threat score to a scorable attribute. This is useful for utilizing the Threat Score or Confidence Score in your ThreatQ Scoring Policy.
    - Added ability to select the pieces of context to ingest with each indicator.
    - Added ability to select which indicator types to ingest.
    - Increased the feed timeout to 10 minutes to prevent timeouts.
    - Indicator descriptions are now rich text that includes any notes or reasons, as well as any "extended" fields that are returned from the API.
    - Replaced the Confidence Rating and Threat Rating dropdowns for threshold fields as the Infoblox API no longer supports filtering on these fields.
    - Infoblox TIDE feed configuration updates:
        - added the following new configuration parameters:
            - **Verify SSL** - determine if the feed should verify the SSL certificate.
            - **Disable Proxies** - determine if the feed should ignore proxies set in the ThreatQ UI.
            - **Threat Classes Filter** - filter incoming data by the threat class.
            - **Require Threat Label** - configure the feed to only include indicators that have a threat label.
            - **Only Major Threats** - configure the feed to only include indicators are considered major threats.
            - **Minimum Threat Level Threshold** - enter a numeric value to represent the minimum threat level required to ingest an indicator.

        - **Minimum Confidence Threshold** - enter a numeric value to represent the minimum confidence score required to ingest an indicator. Set this to 0 to ingest all reported indicators.
        - **Only Ingest Indicators that are Up** - configure the feed to only ingest indicators that are currently up.
        - **Ingested Indicator Types** - select the indicator types to ingest.
        - **Attribute Selection** - select which pieces of context to ingest into ThreatQ.
        - **Normalize Confidence Scores** - normalize the Confidence Score and Threat Score from the default 0-100 range to a human readable value.
        - **Confidence Score Normalization Mapping** - enter the values to use to normalize the numeric confidence score values to the scorable attribute, **Normalized Confidence Score**.
        - **Normalize Threat Scores** - normalize the Threat Score from the default 0-100 range to a human readable value.
        - **Threat Score Normalization Mapping** - enter the values to use to normalize the numeric confidence score values to the scorable attribute, **Normalize Threat Scores**.
    - Removed the following configuration parameters as that type of filtering is no longer supported by the Infoblox API:

    > Threshold filtering is now done within the feed when processing the results.

        - Threat Score Rating
        - Risk Score Rating
        - Confidence Score Rating
- Infoblox TIDE Lookalike Domains feed configuration updates:
    - added the following new configuration parameters:
        - **Verify SSL** - determine if the feed should verify the SSL certificate.
        - **Disable Proxies** - determine if the feed should ignore proxies set in the ThreatQ UI.
        - **Threat Classes Filter** - filter incoming data by the threat class.
        - **Only Major Threats** - configure the feed to only include indicators are considered major threats.
        - **Minimum Threat Level Threshold** - enter a numeric value to represent the minimum threat level required to ingest an indicator.
        - **Minimum Confidence Threshold** - enter a numeric value to represent the minimum confidence score required to ingest an indicator. Set this to 0 to ingest all reported indicators.
        - **Only Ingest Indicators that are Up** - configure the feed to only ingest indicators that are currently up.
        - **Attribute Selection** - select which pieces of context to ingest into ThreatQ.
        - **Normalize Confidence Scores** - normalize the Confidence Score and Threat Score from the default 0-100 range to a human readable value.
        - **Confidence Score Normalization Mapping** - enter the values to use to normalize the numeric confidence score values to the scorable attribute, **Normalized Confidence Score**.

            - **Normalize Threat Scores -** normalize the Threat Score from the default 0-100 range to a human readable value.
            - **Threat Score Normalization Mapping -** enter the values to use to normalize the numeric confidence score values to the scorable attribute, **Normalize Threat Scores**.
    - Updated the minimum ThreatQ version to 5.5.0.
- **Version 1.1.0**
    - Added new threat feed: Infoblox TIDE
    - Added additional parameters for new threat feed.
- **Version 1.0.0**
    - Document rebuilt to reflect product naming update
    - Initial Release (06/16/2020