SLASHNEXT

USER GUIDE V1.0.0

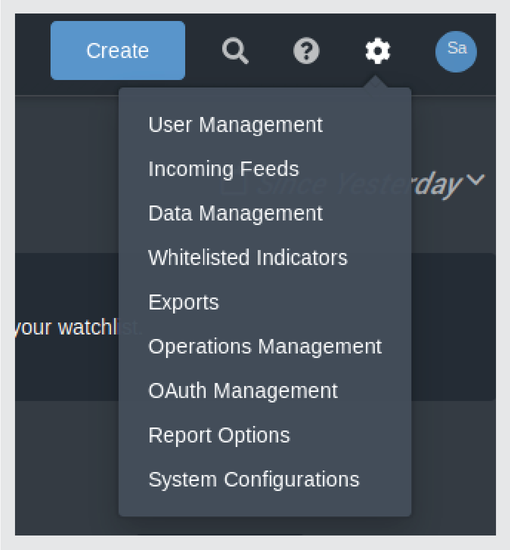
# SlashNext Threat Intelligence Integration Guide ThreatQ TIP

## TABLE OF CONTENTS

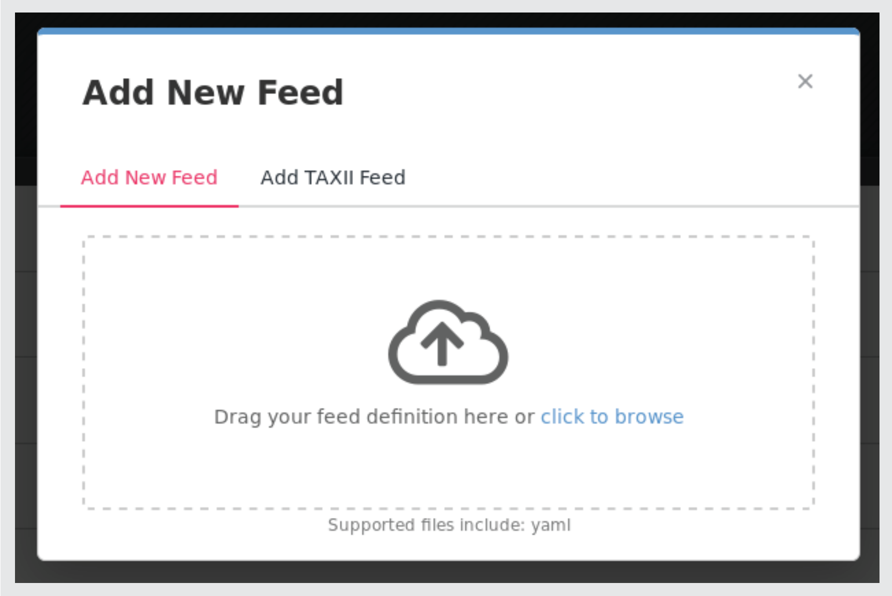
# 1 | FEED INSTALLATION

Follow the steps listed below to install the SlashNext threat feeds into ThreatQ threat intelligence platform.

1. Login to the ThreatQ platform.
2. Go to ThreatQ settings by clicking on the ⚙ icon on top right corner of the ThreatQ UI.
3. Select Incoming Feeds from the drop-down menu as shown following snapshot.

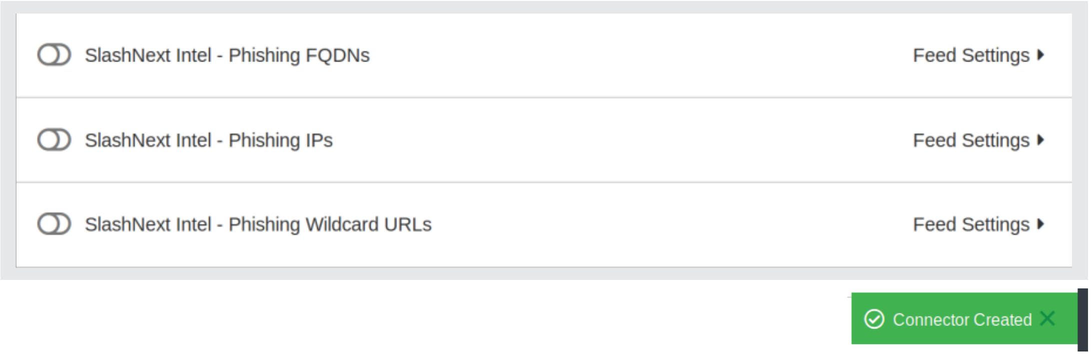


4. On **Incoming Feeds** page click on Add New Feed button on top of the page then a pop-up window will appear as shown in following snapshot.


Add New Feed
×
Add New Feed
Add TAXII Feed
Drag your feed definition here or click to browse
Supported files include: yaml

5. Click on **click to browse** under **Add New Feed** tab to input the feed definition from provided SlashNext .yaml file.

6. On successful installation of SlashNext feeds, a notification (Connector Created) will be displayed on bottom right corner as shown indicating success status and SlashNext feeds will be listed under **Commercial** tab as shown in following snapshot.



○ SlashNext Intel - Phishing FQDNs — Feed Settings ▸

○ SlashNext Intel - Phishing IPs — Feed Settings ▸

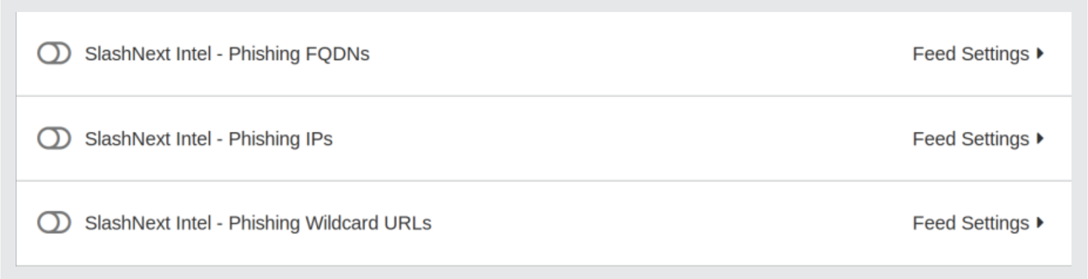
○ SlashNext Intel - Phishing Wildcard URLs — Feed Settings ▸

✓ Connector Created ✕

## 2 | FEED CONFIGURATION

Follow the steps listed below to update the SlashNext threat feeds configurations like update interval and API key.

1. Click on the **Feed Settings** which appears on the right side of the respective feed tab in ThreatQ as shown in the following snapshot.

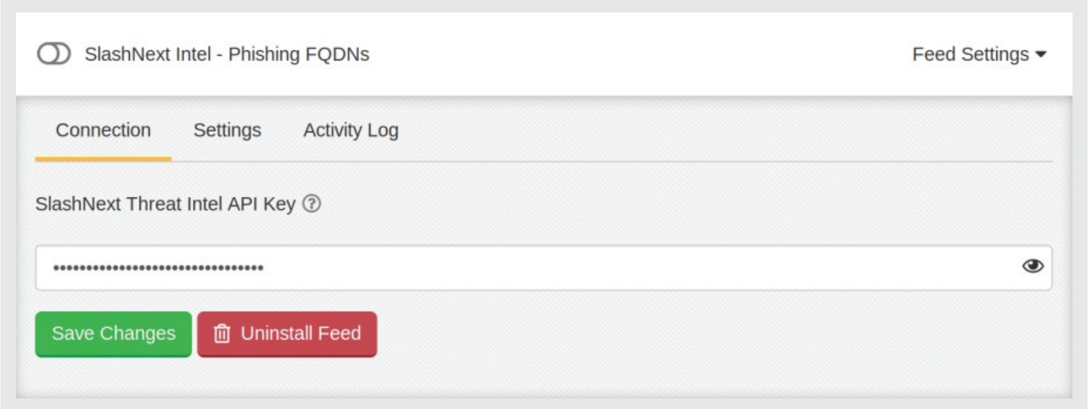


○ SlashNext Intel - Phishing FQDNs — Feed Settings ▸

○ SlashNext Intel - Phishing IPs — Feed Settings ▸

○ SlashNext Intel - Phishing Wildcard URLs — Feed Settings ▸

2. Select the **Connection** tab and input the API Key provisioned by SlashNext in the text input field and click on **Save Changes** button as shown in following snapshot.



○ SlashNext Intel - Phishing FQDNs — Feed Settings ▾

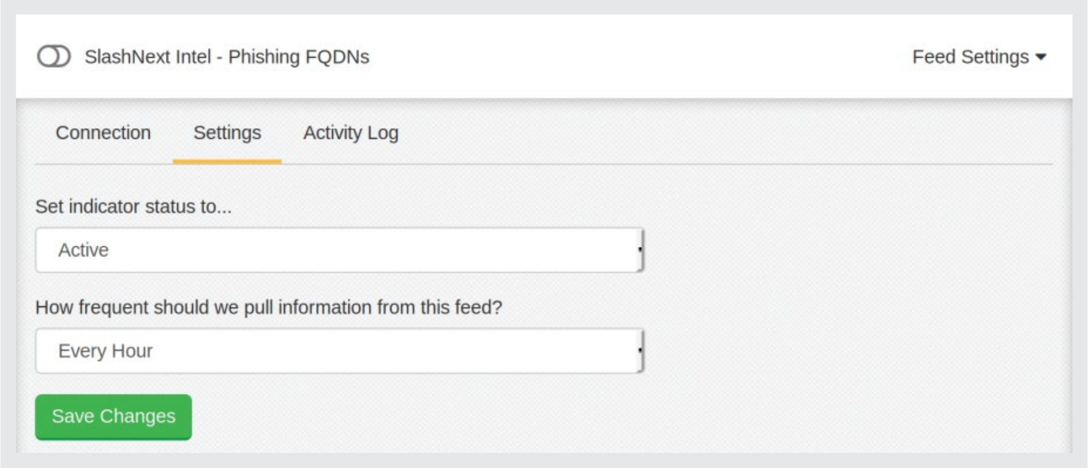
Connection | Settings | Activity Log

SlashNext Threat Intel API Key ⓘ

••••••••••••••••••••••••••••••••

Save Changes | Uninstall Feed

3. Select the **Settings** tab and click on the **How frequent should we pull information from this feed?** drop-down and select **Every Hour** and click on **Save Changes** button as shown in the following snapshot.



SlashNext Intel - Phishing FQDNs

Set indicator status to...

Active

How frequent should we pull information from this feed?

Every Hour

4. To enable the feed click on switch ○ next to feed name which will turn green like this ●.
5. On successful configurations of SlashNext feed, a notification (Connector Updated) will be displayed on bottom right corner.

ⓘ **Important Note**

Refresh rate of **Every Hour** is strongly recommended by SlashNext considering the dynamic nature to SlashNext threat feeds.

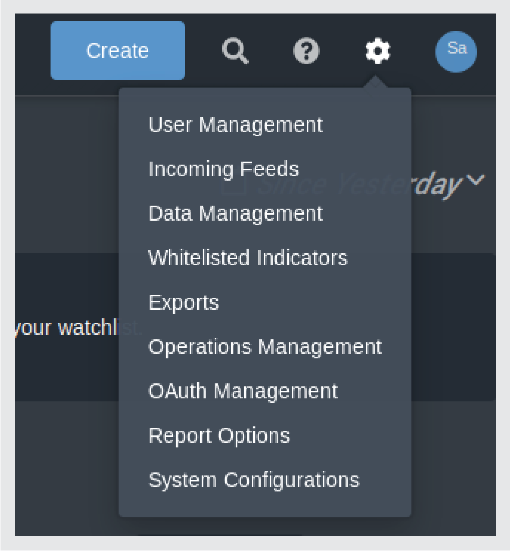
ⓘ **Important Note**

There are **three** type of threat feeds provided by SlashNext, you will need to repeat above step for each feed type individually.

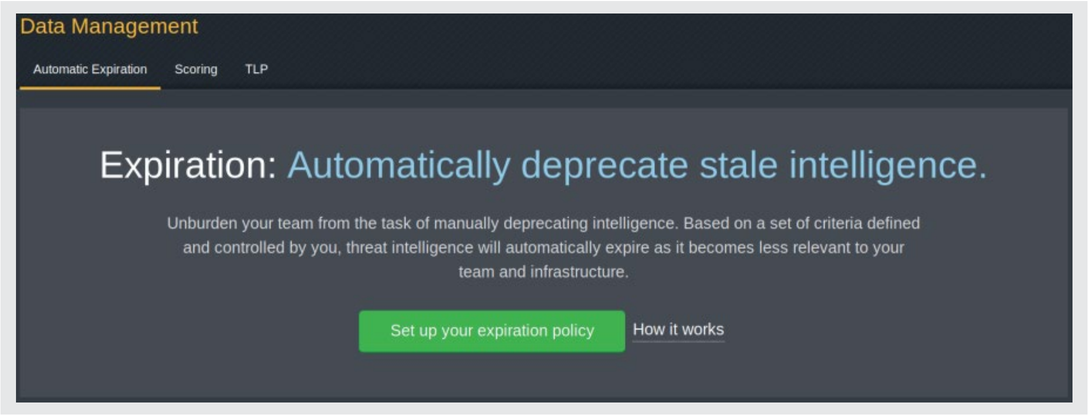
## 3 | FEED EXPIRATION POLICY

Considering the highly dynamic nature of SlashNext feeds, it is strongly recommended to set a threat feed expiration policy within ThreatQ platform. Follow the steps listed below to set expiration policy of SlashNext threat feeds.

1. Go to ThreatQ settings by clicking on the ⚙ icon on top right corner of the ThreatQ UI.
2. Select **Data Management** from the drop-down menu as shown following snapshot.



3. On the **Data Management** page, select **Automatic Expiration** tab and click on the **Set up your expiration policy** as shown in the snapshot below.



Data Management

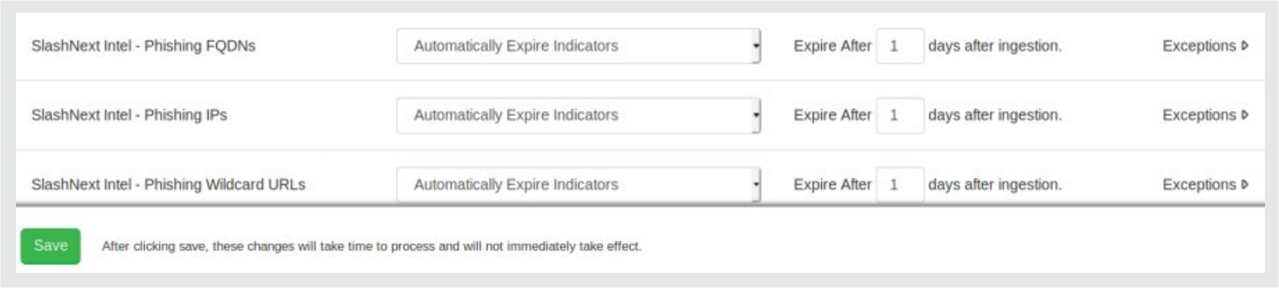
Automatic Expiration Scoring TLP

Expiration: Automatically deprecate stale intelligence.

Unburden your team from the task of manually deprecating intelligence. Based on a set of criteria defined and controlled by you, threat intelligence will automatically expire as it becomes less relevant to your team and infrastructure.

Set up your expiration policy | How it works

4. Go to the SlashNext feeds and select **Automatically Expire Indicators** from drop-down menu and set 1 day after ingestion for each feed and click on the **Save button** as shown in the snapshot below.



| | | | | | |
|---|---|---|---|---|---|
| SlashNext Intel - Phishing FQDNs | Automatically Expire Indicators | Expire After | 1 | days after ingestion. | Exceptions ▸ |
| SlashNext Intel - Phishing IPs | Automatically Expire Indicators | Expire After | 1 | days after ingestion. | Exceptions ▸ |
| SlashNext Intel - Phishing Wildcard URLs | Automatically Expire Indicators | Expire After | 1 | days after ingestion. | Exceptions ▸ |

Save After clicking save, these changes will take time to process and will not immediately take effect.

## 4 | LIST SPECIFIC IoCs

All the indicators within SlashNext feeds have 4 custom attributes to facilitate the filtering of feed to get a list of more desired indicators as per threat nature or as per usage.

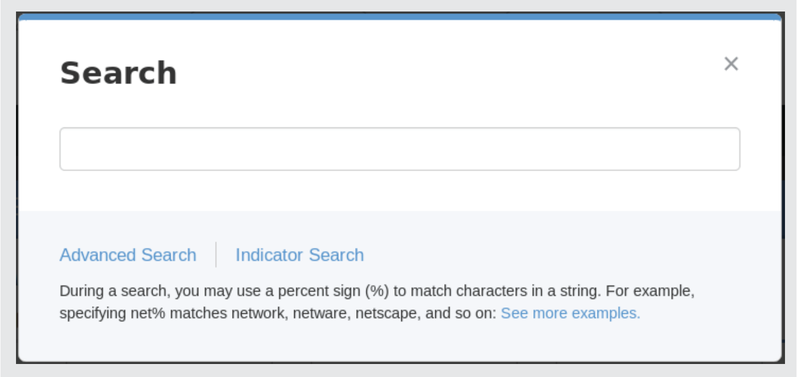
### 4.1 | FILTER FEED TYPES

SlashNext intel consists of following three types of feeds:

1. SlashNext Intel – Phishing FQDNs
2. SlashNext Intel – Phishing IPs
3. SlashNext Intel – Phishing Wildcard URLs

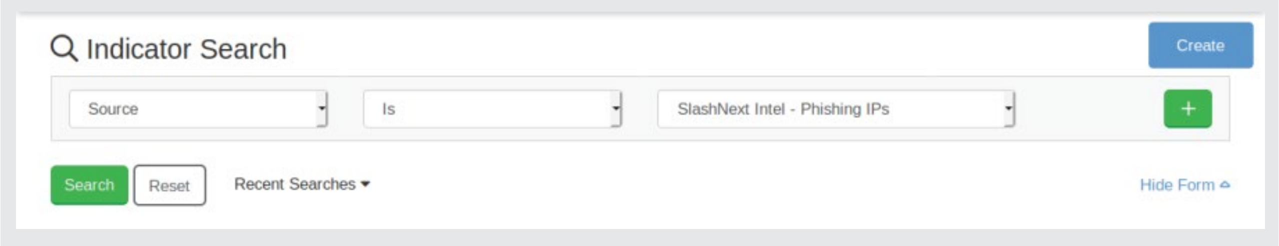
In order to get the list of indicators only from SlashNext IP feed, please follow the steps below.

1. Go to ThreatQ search by clicking on the 🔍 icon on top right corner of the ThreatQ UI.
2. Select **Indicator Search** from the pop-up window as can be seen in the snapshot below.



During a search, you may use a percent sign (%) to match characters in a string. For example, specifying net% matches network, netware, netscape, and so on: See more examples.

4. In the **Indicator Search** window select **Source** in the **Search Filter** drop-down menu, in the second drop-down select **Is** and the third drop-down menu select **SlashNext Intel – Phishing IPs** as shown in the following snapshot.



Source | Is | SlashNext Intel - Phishing IPs

Similarly for domains select **SlashNext Intel – Phishing FQDNs** in the third drop-down menu, for wildcard urls select **SlashNext Intel – Phishing Wildcard URLs** in the third drop-down menu and so on.

## 4.2 | FILTER FEED TYPES

Each indicator in the above feeds have following four custom attributes:

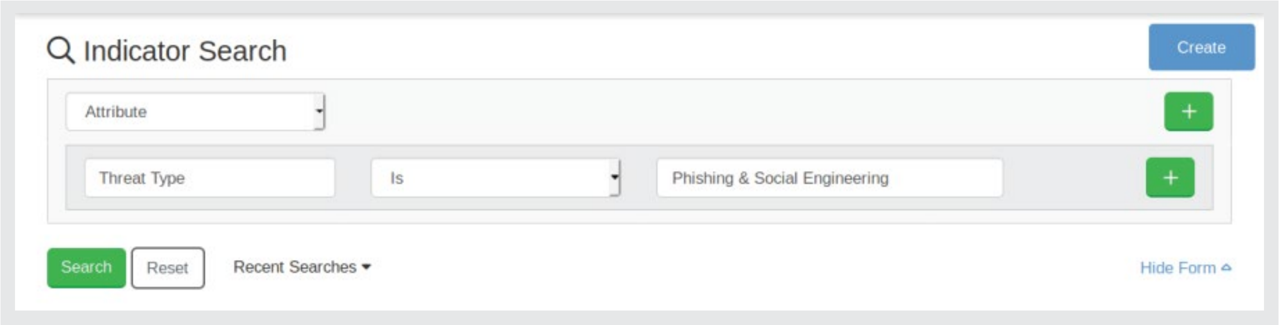
1. Threat Type (e.g. Phishing & Social Engineering, Callback/C2 etc)
2. Threat Name (e.g. Fake Login Page, Scareware, Rogue Software etc)
3. First Seen (first seen time UTC)
4. Last Seen (last seen time UTC)

**Threat Type** attribute can have one of the following value:

1. Phishing & Social Engineering
2. Malware & Exploit
3. Callback/C2

In order to get the list of indicators based upon a specific attribute value, please follow the steps below.

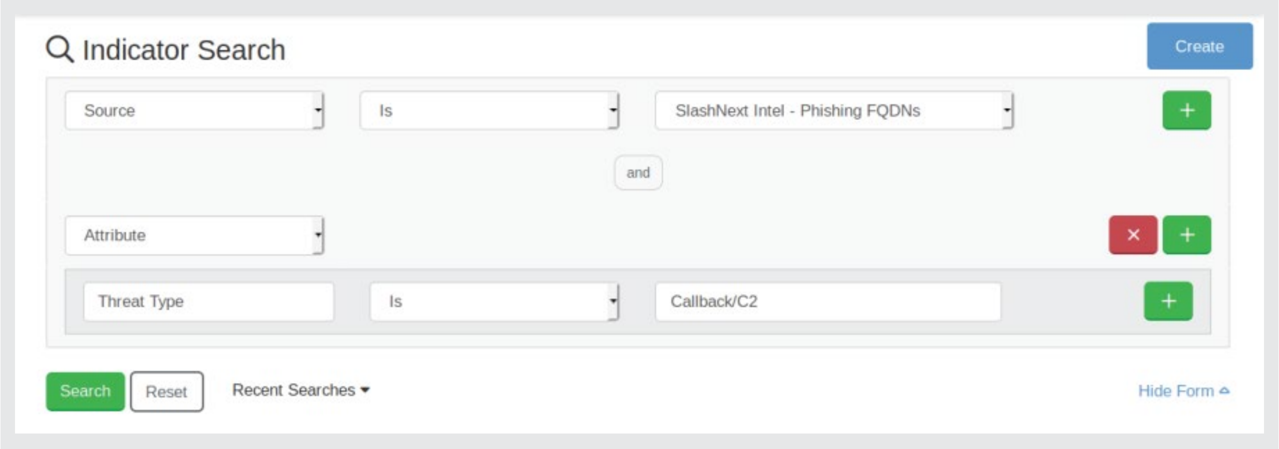
1. Go to ThreatQ search by clicking on the  icon on top right corner of the ThreatQ UI.
2. Select **Indicator Search** from the pop-up window as can be seen in the snapshot below.
3. In the **Indicator Search** window select **Attribute** in the **Search Filter** drop-down menu, in the **Attribute Type** drop-down select **Threat Type** or **Threat Name** depending upon the intended search, then select **Is** and in the **Attribute value** drop-down menu enter **Phishing & Social Engineering** or the value you want to search as shown in the following snapshot.


Indicator Search

Attribute

Threat Type | Is | Phishing & Social Engineering

Similarly user can combine different filters to get the list of desired indicators like in case a list of indicators from **SlashNext Intel – Phishing FQDNs** feed is need where attribute **Threat Type** has **Callback/C2** value. Please see the filter snapshot below.


Indicator Search

Source | Is | SlashNext Intel - Phishing FQDNs

and

Attribute

Threat Type | Is | Callback/C2