



**NOZOMI**  
NETWORKS

# **Threat Intelligence Feed Configuration Guide**

## Legal notices

*Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.*

### Copyright

Copyright © 2013-2024, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

### Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at <https://security.nozominetworks.com/licenses>.

# Contents

<b>Chapter 1. Introduction.....</b>	<b>5</b>
TAXII overview.....	7
<b>Chapter 2. Requirements.....</b>	<b>9</b>
Server information.....	11
<b>Chapter 3. Configuration.....</b>	<b>13</b>
taxii2client configuration.....	15
Configure Anomali STAXX.....	16
Configure Microsoft Sentinel.....	21
Configure ThreatQ.....	24
Configure QRadar.....	30
<b>Chapter 4. Troubleshooting.....</b>	<b>35</b>
Error message: HTTP 401 Unauthorized.....	37
Error message: HTTP 404 Not found.....	37
Error message: HTTP 406 Not Acceptable.....	38
Glossary.....	39



# Chapter 1. Introduction



## TAXII overview

*TAXII standardizes the exchange of cyber threat intelligence (CTI) over the internet, enabling organizations to share security threat information more efficiently and effectively. This improves threat detection, analysis, and response.*

*Trusted Automated Exchange of Indicator Information (TAXII)* is a protocol used for the exchange of *cyber threat intelligence (CTI)* over the internet. *TAXII* is designed to support the distribution of *CTI* using a standardized methodology, enabling organizations to share information about security threats more efficiently and effectively.

*TAXII* is often used in conjunction with *Structured Threat Information Expression (STIX)*, which is a language and serialization format used to exchange *CTI*. *STIX* enables organizations to convey the full range of potential threat information, from high-level attack patterns and technical indicators to detailed threat actor profiles and the *tactics, techniques, and procedures (TTPs)* that they use.

Together, *TAXII* and *STIX* facilitate the automated exchange, processing, and analysis of cyber threat information among various parties, including private sector organizations, government agencies, and other entities involved in cybersecurity defense. This leverages shared knowledge about existing and emerging threats to help improve the speed and accuracy of threat detection, analysis, and response.





# Chapter 2. Requirements



## Server information

Server information for Trusted Automated Exchange of Indicator Information (TAXII) services, highlighting uniform resource locators (URLs) for discovery and root access, server protocol and Structured Threat Information Expression (STIX) versions, along with collection IDs for threat types such as phishing and ransomware.

**Table 1. Server information**

Syntax	Description
TAXII Discovery <i>uniform resource locator (URL)</i>	<a href="https://ti-taxii.nws.nozominetworks.io/taxii/">https://ti-taxii.nws.nozominetworks.io/taxii/</a>
TAXII Root <i>URL</i>	<a href="https://ti-taxii.nws.nozominetworks.io/root/">https://ti-taxii.nws.nozominetworks.io/root/</a>
Server protocol	TAXII 2.0
STIX version	STIX 2.0

**Table 2. Collection IDs**

Operational Technology (OT)	thw2k6rf-w130-zaiv-i606-rsm42fk4dwms
Internet of Things (IoT)	aq6odbpq-5tzs-zonm-yr2p-3djab10n5t6k
Phishing	24m19vt0-vbi4-61td-a813-xhuxpwxeccha
Ransomware	sx76qzvj-bx02-vnrn-zsd7-k9fx4g8c2tqg
Hacking Frameworks	56a15872-9565-4f3a-9975-340416369a4d
General (includes indicators from all other collections)	y6bpc38c-bxvz-49ga-y96f-558drdq2x6s4



# Chapter 3. Configuration



## taxii2client configuration

Learn how to use the minimal Python library from OASIS to set up a **taxii2client** to interact with the TAXII server from Nozomi Networks. This includes integration for software that does not support the TAXII 2.0 protocol.

The **taxii2client** is a minimal Python [TAXII](#) client from OASIS, which can be used to interact with the Nozomi Networks [TAXII](#) server. This library is useful if you want to integrate indicators that are pulled from the Nozomi Networks [TAXII](#) server with software which does not support the [TAXII](#) 2.0 protocol. For more detailed installation instructions and library documentation, see the [OASIS TC Open Repository cti-taxii-client GitHub repository](#).

The code snippet below prints all indicator objects from the **Operational Technology (OT)** collection and calculates their total number:

```
from taxii2client.v20 import Collection, as_pages

COLLECTION_ID = 'thw2k6rf-wl30-zaiv-i606-rsm42fk4dwms' # OT collection
TAXII_USER = 'REPLACE_WITH_PROVIDED_USERNAME_HERE'
TAXII_PASSWORD = 'REPLACE_WITH_PROVIDED_PASSWORD_HERE'

collection =
    Collection(f"https://
ti-taxii.nws.nozominetworks.io/root/collections/{COLLECTION_ID}/",
    user=TAXII_USER, password=TAXII_PASSWORD)
total_indicators = 0
for page in as_pages(collection.get_objects, per_request=99):
    for o in page['objects']:
        if 'type' in o and o['type'] == 'indicator':
            total_indicators += 1
            print(o)
print(f"total indicators: {total_indicators}")
```

## Configure Anomali STAXX

Do this procedure to configure the Anomali STAXX, a free TAXII/STIX solution, for integration with the Nozomi Networks TAXII server, including setting descriptions, uniform resource locators (URLs), and authentication details.

### Procedure

1. Download Anomali STAXX from the [Anomali website](#).
2. To install the downloaded *open virtual appliance (OVA)* file, follow the [Anomali instructions](#).
3. Launch Anomali STAXX.
4. Select **Add New Site**.

**Result:** A dialog shows.

5. In the **Description** field, enter a description.

The screenshot shows a dialog box titled "ADD NEW SITE" with a close button in the top right corner. The dialog contains the following fields and options:

- Description \***: A text input field containing "Nozomi Networks TAXII". Below it, an example is provided: "Example: Anomali Limo".
- Discovery URL \***: A text input field containing "https://ti-taxii.nws.nozominetworks.io/taxii/". Below it, an example is provided: "Example: https://limo.anomali.com/taxii/".
- Basic Authentication**: A checked checkbox.
- Username \***: A text input field containing "secresearch@nozominetworks.com".
- Password \***: A password input field with masked characters (dots).
- SSL Two-Way Certificate**: An unchecked checkbox.
- A legend at the bottom indicates that "\*" is a required field.
- At the bottom right, there are two buttons: "Cancel" and "Add Site" (which is highlighted in blue).

6. In the **Discovery URL** field, enter the **Discovery URL**:  
`https://ti-taxii.nws.nozominetworks.io/taxii/`
7. Select the **Basic Authentication** checkbox.
8. In the **Username** field, enter your username.
9. In the **Password** field, enter your password.
10. Do not select the **SSL Two-Way Certificate** checkbox.



11. Select **Add Site**.

The site will be added.

12. In the section on the right, select **Discover**.

DETAILS:

Name: Nozomi Networks TAXII  
 Address: https://ti-taxii.nws.nozominetworks.io/taxii/  
 Username: secresearch@nozominetworks.com  
 Last Updated:  
 TAXII Version: Unknown

Task State: Pending

Discover

Poll Collections Available Collections Scheduled Pushes

25

Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
NO DATA AVAILABLE				

13. Select **Enable** for each item as necessary.

DETAILS:

Name: Nozomi Networks TAXII  
 Address: https://ti-taxii.nws.nozominetworks.io/taxii/  
 Username: secresearch@nozominetworks.com  
 Last Updated:  
 TAXII Version: 2.0

Task State: Completed  
 Feed discovery is successful

Discover

Poll Collections Available Collections Scheduled Pushes

25 1 - 5 of 5 items

Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
Operational Technology (OT)	N/A	N/A	<input type="checkbox"/>	Edit
Internet of Things (IoT)	N/A	N/A	<input type="checkbox"/>	Edit
Phishing	N/A	N/A	<input type="checkbox"/>	Edit
Ransomware	N/A	N/A	<input type="checkbox"/>	Edit
General	N/A	N/A	<input type="checkbox"/>	Edit

14. To select the time range to poll indicators from, select **Edit** for the applicable collection.

The screenshot shows the 'CONFIGURE FEED' dialog box. The 'Poll Time Range' is set to 7 days. The 'Confidence' section has 'Source Indicator Confidence' selected. The 'Schedule' section has 'Default' selected. The 'Confidence Score' field is empty. The 'Subscription ID' field is empty. The 'Discover' button is visible in the background.

Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
Operational Technology (OT)	N/A	N/A	<input type="checkbox"/>	Edit
Internet of Things (IoT)	N/A	N/A	<input type="checkbox"/>	Edit
Phishing	N/A	N/A	<input type="checkbox"/>	Edit
Ransomware	N/A	N/A	<input checked="" type="checkbox"/>	Edit Poll Now

In order to receive historical indicators, this value should be high for the initial poll. You can then decrease it based on how often the server will be polled. For example, if polling daily, only poll for indicators that have been added within the last 24 hours.

The screenshot shows the 'CONFIGURE FEED' dialog box. The 'Poll Time Range' is set to 1825 days. The 'Confidence' section has 'Source Indicator Confidence' selected. The 'Schedule' section has 'Default' selected. The 'Confidence Score' field is empty. The 'Subscription ID' field is empty. The 'Discover' button is visible in the background.

Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
Operational Technology (OT)	N/A	N/A	<input type="checkbox"/>	Edit
Internet of Things (IoT)	N/A	N/A	<input type="checkbox"/>	Edit

15. To poll indicators, select **Poll Now**.

**DETAILS:**

Name: Nozomi Networks TAXII  
 Address: https://ti-taxii.nws.nozominetworks.io/taxii/  
 Username: secresearch@nozominetworks.com  
 Last Updated:  
 TAXII Version: 2.0

Task State: Completed  
 Feed discovery is successful

Discover

Poll Collections Available Collections Scheduled Pushes

25 1 - 5 of 5 items

Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
Ransomware	N/A	N/A	<input checked="" type="checkbox"/>	Edit Poll Now
Operational Technology (OT)	N/A	N/A	<input type="checkbox"/>	Edit
Internet of Things (IoT)	N/A	N/A	<input type="checkbox"/>	Edit
Phishing	N/A	N/A	<input type="checkbox"/>	Edit
General	N/A	N/A	<input type="checkbox"/>	Edit

**Note:**  
 This can take some minutes depending on how large a collection is.

Once this process completes, the number of **Last Poll Observables** will show a value.

**DETAILS:**

Name: Nozomi Networks TAXII  
 Address: https://ti-taxii.nws.nozominetworks.io/taxii/  
 Username: secresearch@nozominetworks.com  
 Last Updated:  
 TAXII Version: 2.0

Task State: Completed

Discover

Poll Collections Available Collections Scheduled Pushes

25 1 - 5 of 5 items

API Root	Feed Name / Description	Last Poll	Last Poll Observables	Enabled	Actions
root	Ransomware	2023-8-18 14:26:56	1391	<input checked="" type="checkbox"/>	Edit Poll Now
root	Operational Technology (OT)	N/A	N/A	<input type="checkbox"/>	Edit
root	Internet of Things (IoT)	N/A	N/A	<input type="checkbox"/>	Edit
root	Phishing	N/A	N/A	<input type="checkbox"/>	Edit
root	General	N/A	N/A	<input type="checkbox"/>	Edit

### Results

The indicators can be accessed from the **Dashboard** menu.



# Configure Microsoft Sentinel

Once the Threat Intelligence - TAXII data connector is installed, you need to configure the TAXII server.

## About this task

Microsoft Sentinel is a cloud-native [security information and event management \(SIEM\)](#) solution that provides intelligent security analytics. Microsoft Sentinel can interact with TAXII servers using the Threat Intelligence - TAXII data connector. For more details on Microsoft TAXII configuration, see the [Microsoft documentation](#).

## Procedure

1. Open **Microsoft Sentinel**.
2. Select the **Threat Intelligence - TAXII** data connector for **Microsoft Sentinel**.
3. In the bottom right section, select **Open connector page**.

The screenshot displays the Microsoft Sentinel interface for configuring data connectors. The main area shows a list of connectors, with 'Threat intelligence - TAXII' selected. The right-hand pane provides detailed settings for this connector, including its status, description, and related content.

Status	Connector name	Content Source	Updates
Onboarded	Microsoft Defender Thr...	Microsoft	Threat Intelligence
Connected	Threat intelligence - TAXII	Microsoft	Threat Intelligence
Onboarded	Threat Intelligence Platf...	Microsoft	Solution Threat Intelligence
Onboarded	Threat Intelligence Uplo...	Microsoft	Solution Threat Intelligence

**Threat intelligence - TAXII**

Disconnected Status | Microsoft Provider | Last Log Received

Description: Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

Last data received: --

Content source: Threat Intelligence | Version: 1.0.0

Author: Microsoft | Supported by: Microsoft Corporation | Email


Related content: 0 Workbooks, 2 Queries, 35 Analytics rules templates

Data received: 0 (Graph showing 0 data points from 21 August to 18 August)

Open connector page

The connector settings for **Microsoft Sentinel** show.

#### 4. Use the `/root/` endpoint to add each collection individually for **Microsoft Sentinel**.

**Configuration**

Configure TAXII servers to stream STIX 2.0 or 2.1 threat indicators to Microsoft Sentinel

You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector. For detailed configuration instructions, see the [full documentation](#).

Enter the following information and select Add to configure your TAXII server.

Friendly name (for server) \*

API root URL \*

Collection ID \*

Username

Password

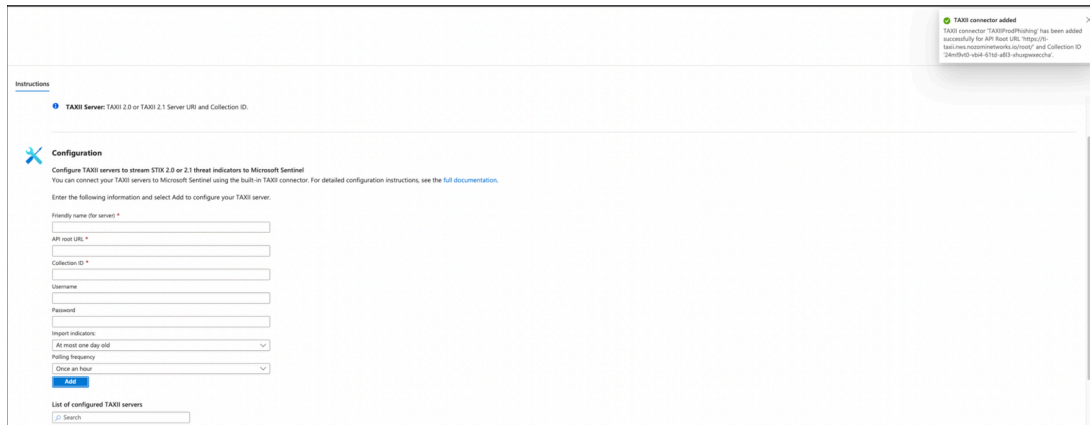
Import indicators:

Polling frequency

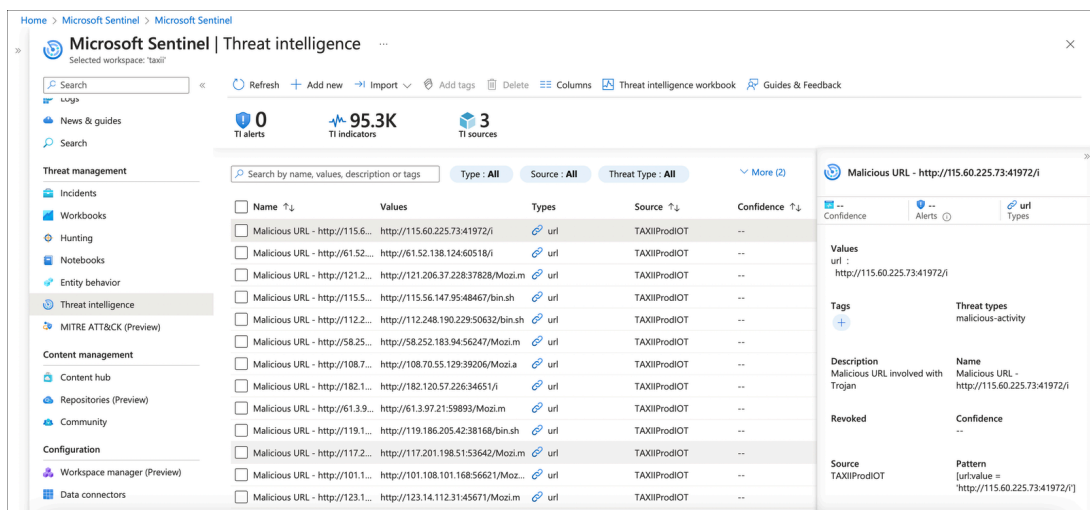
**Note:**

Make sure that you use the `/root/` endpoint instead of the discovery endpoint `/taxii/`.

5. To verify that the operation was successful, make sure that you can see a message on the right.



You can now access the indicators from the **Threat Intelligence** page.



## Results

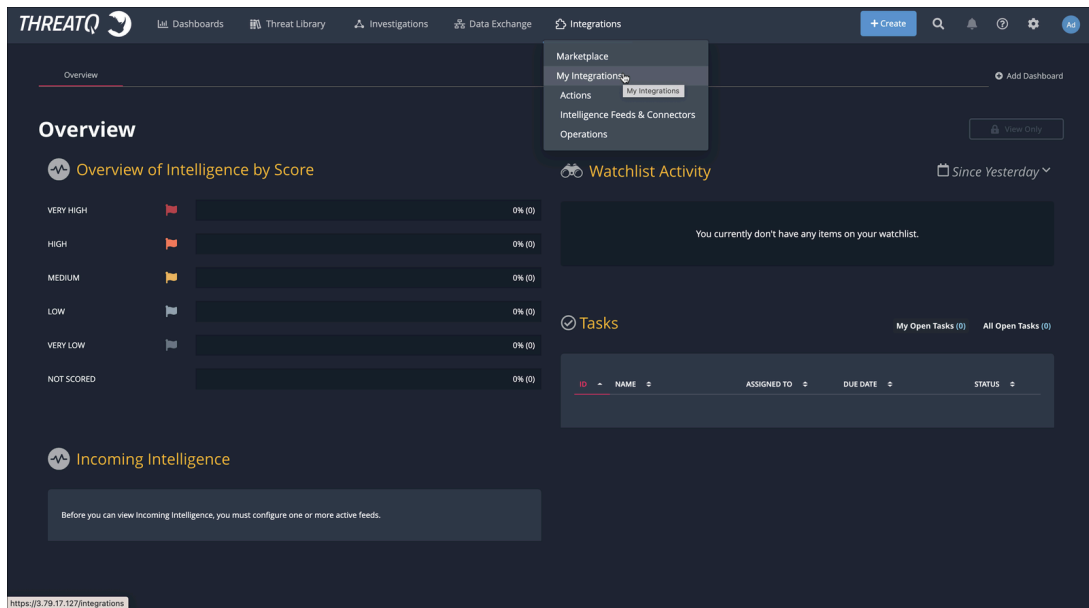
Microsoft Sentinel has now been configured.

## Configure ThreatQ

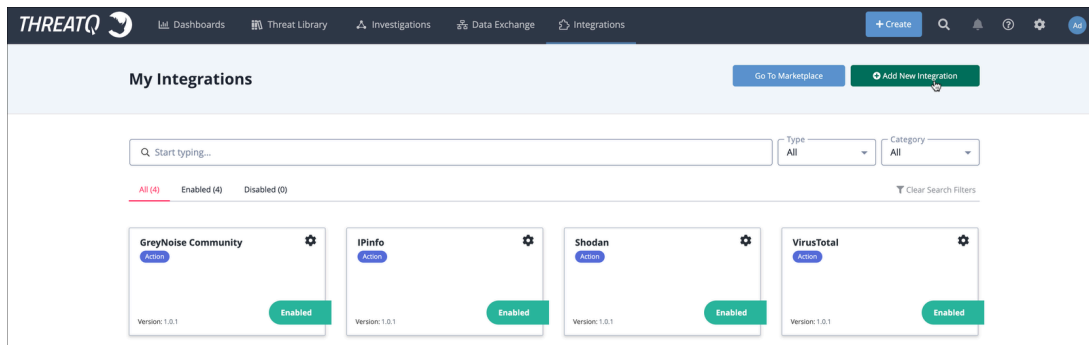
Follow these steps to add and enable a new TAXII feed integration in ThreatQ, verify indicator ingestion, and monitor the integration's status through the Activity Log.

### Procedure

1. Open ThreatQ.
2. Go to **Integrations > My Integrations**.



3. In the top right section, select **Add New Integration**.



**Result:** A dialog shows.



4. Select **Add New TAXII Feed**.

## Add New Integration ✕

Add New Integration Add New TAXII Feed

What would you like to name this feed?

How often would you like to pull new data from this feed?

### TAXII Connection Settings

TAXII Server Version

Discovery URL   
Path to the TAXII Server's Discovery Service

Poll URL (Optional)

Optional URL specifying a specific endpoint on the TAXII Server to poll for data. If not supplied, the TAXII Client will attempt to determine the appropriate path via the Collections Service.

Collection Name   
Name of the collection to poll data from

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

5. Enter the details in each field.

### Login Credentials (if applicable)

Username

Basic Authentication Username

Password

Basic Authentication Password

### Certificates/Keys (if applicable)

Certificate

Client Certificate for authentication with the TAXII Server.

Private Key

Private Key for authentication with the TAXII Server.

**Verify SSL**

Specifies whether the TAXII client should verify a provider's SSL certificate

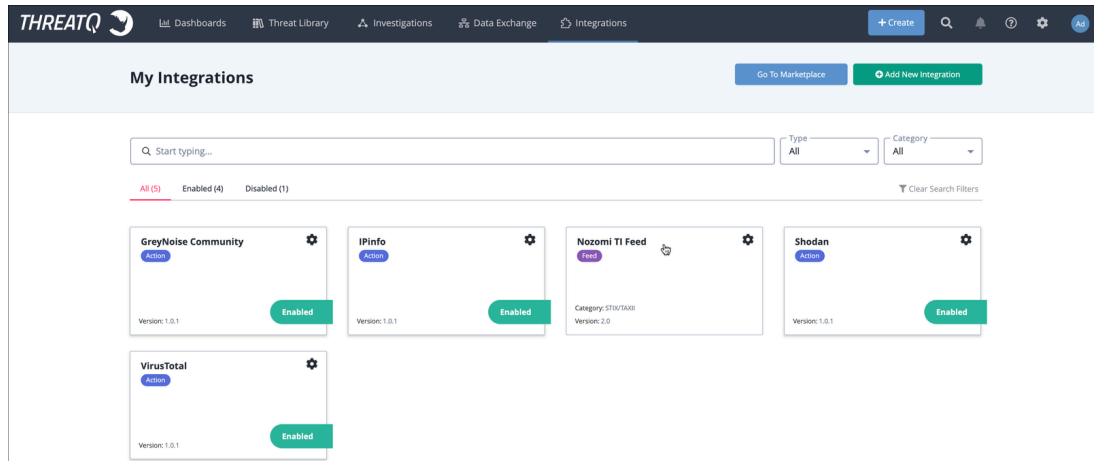
Host CA Certificate Bundle

Used to specify a provider's CA Certificate Bundle to verify SSL against. This denotes that Verify SSL is True.

Do not use Collection *identifier (ID)*s, use Collection names.

6. Select **Add TAXII Feed**.

7. In the **My Integrations** page, select the integration that you just created.



8. In the top left section, select the toggle to **Enabled**.

The screenshot displays the configuration page for a TAXII integration. On the left, there is a puzzle piece icon, a toggle switch set to 'Enabled', and buttons for 'Run Integration' and 'Uninstall'. Below this is an 'Additional Information' section listing 'Integration Type: Feed', 'Version: 2.0', and 'Accepted Data Types:'. The main configuration area is titled 'Configuration' and contains the following fields and options:

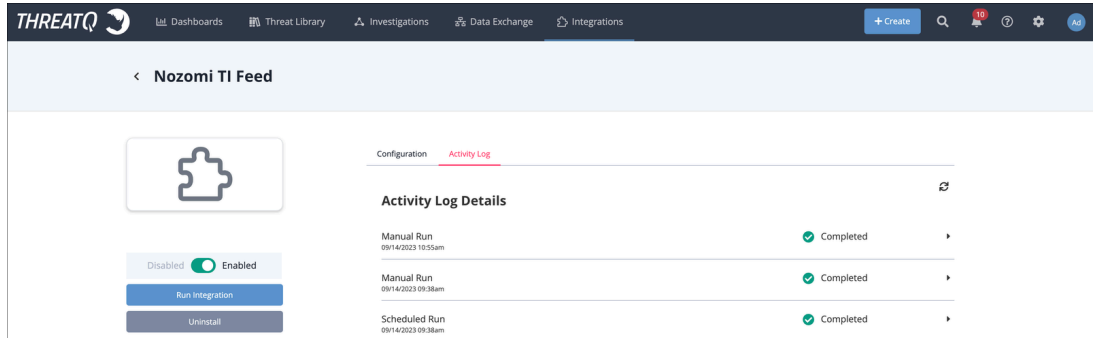
- TAXII Server Version:** A dropdown menu set to '2.0'. Below it, a note states: 'The version of the TAXII Server to poll for data.'
- Discovery Path URL:** A text input field containing 'https://ti-taxii.nws.nozominetworks.io/taxii/'. Below it, a note states: 'Path to the TAXII Server's Discovery Service.'
- Poll URL (Optional):** An empty text input field. Below it, a note states: 'Optional URL specifying a specific endpoint on the TAXII Server to poll for data. If not supplied, the TAXII Client will attempt to determine the appropriate path via the Collections Service.'
- Collection Name:** A text input field containing 'Hacking Frameworks'. Below it, a note states: 'Name of the collection to poll data from.'
- Disable Proxies:** An unchecked checkbox. Below it, a note states: 'If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.'
- Username:** A text input field containing 'nozominetworks'. Below it, a note states: 'Basic Authentication Username.'
- Password:** A password input field with masked characters and an eye icon. Below it, a note states: 'Basic Authentication Password.'
- Client Certificate:** A large text area for a certificate file. Below it, a note states: 'Client Certificate for authentication with the TAXII Server.'
- Client Key:** A large text area for a private key file. Below it, a note states: 'Private Key for authentication with the TAXII Server.'
- Verify SSL:** A checked checkbox. Below it, a note states: 'Specifies whether the TAXII client should verify a provider's SSL certificate.'
- Host CA Certificate Bundle:** A large text area for a CA certificate bundle. Below it, a note states: 'Used to specify a provider's CA Certificate Bundle to verify SSL against. This denotes that Verify SSL is True.'
- Set Indicator status to...:** A dropdown menu set to 'Active'.
- Run Frequency:** A dropdown menu set to 'Every 30 Days'. To its right, the text reads: 'Next scheduled run: 2023-10-20 11:12am (+02:00)'. This section is highlighted with a light blue background.
- Send a notification when this feed encounters issues:** A checked checkbox.
- Debug Option: Save the raw data response files:** An unchecked checkbox. Below it, a note states: 'We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.'

At the bottom of the configuration area is a blue 'Save' button.

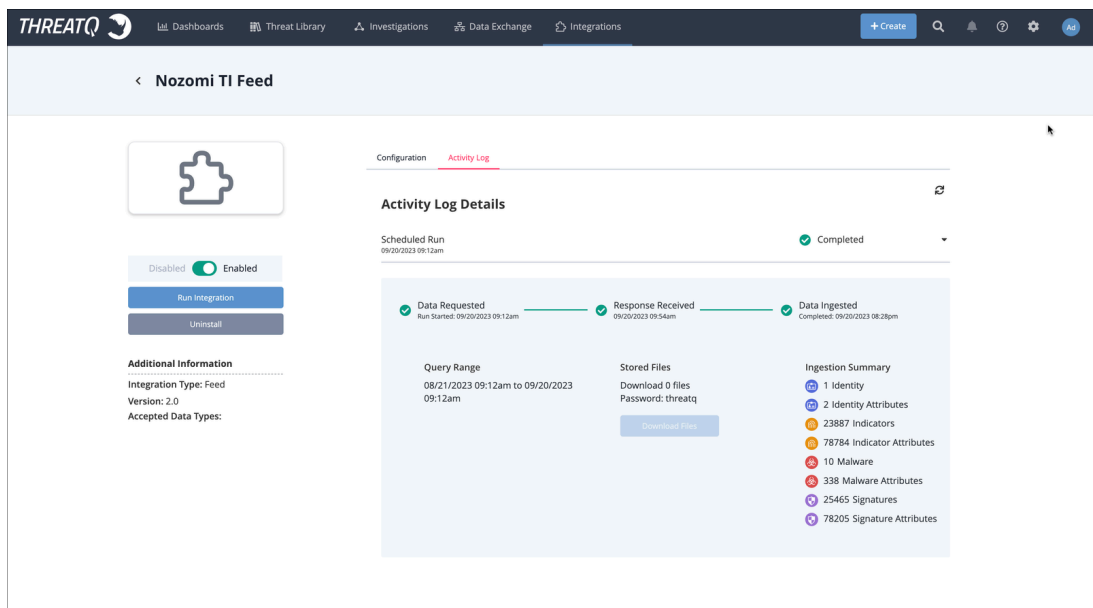
9. Select **Save**.

10. Select **Activity Log**.

11. In the **Activity Log Details** section, make sure that the first manual, or scheduled, run shows as **Completed**.



12. Make sure that the indicators have been ingested correctly.



## Results

ThreatQ has been configured.

## Configure QRadar

Do this procedure to integrate a new TAXII feed into QRadar to enhance threat intelligence capabilities. This procedure covers adding the feed, ensuring full indicator ingestion, and monitoring the integration via the Activity Log for optimal security posture.

### About this task

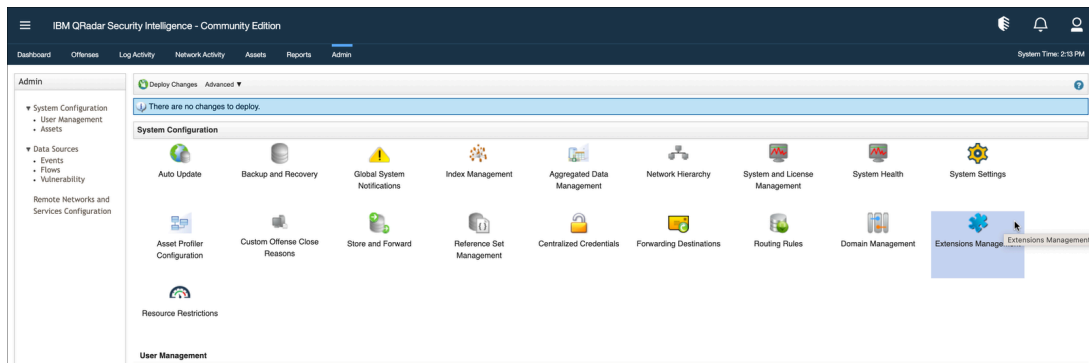


#### Note:

The Threat Intelligence application version 2.4.2, and earlier, has a bug that can lead to only partial ingestion of the [TAXII](#) data. IBM is aware of the bug.

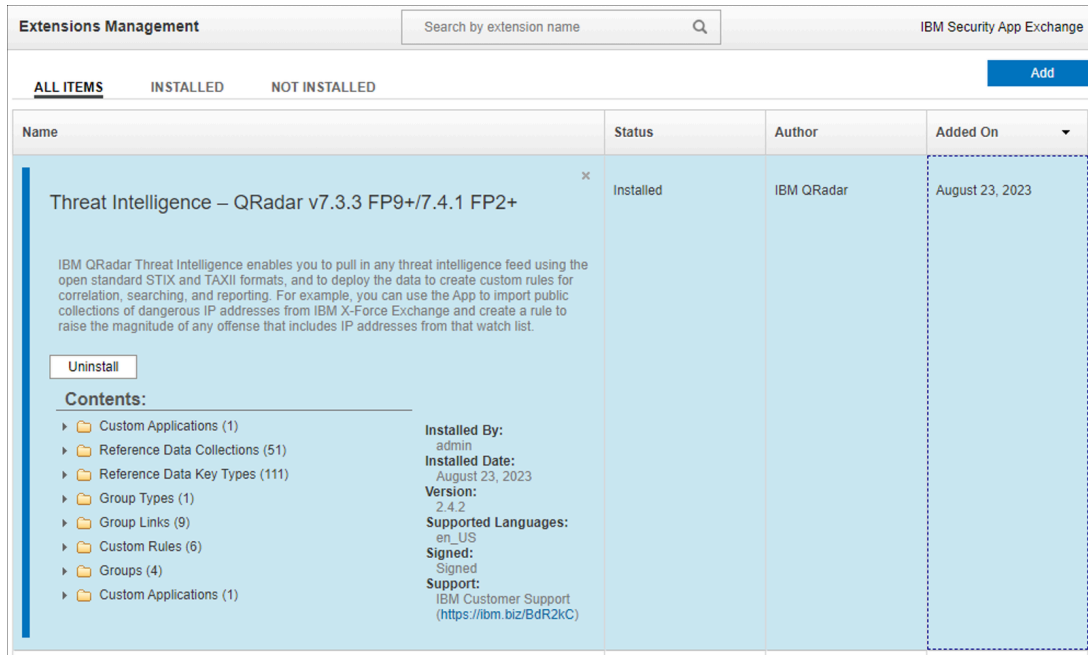
### Procedure

1. Download QRadar from the [IBM website](#).
2. Go to **Admin > Extensions Management**.

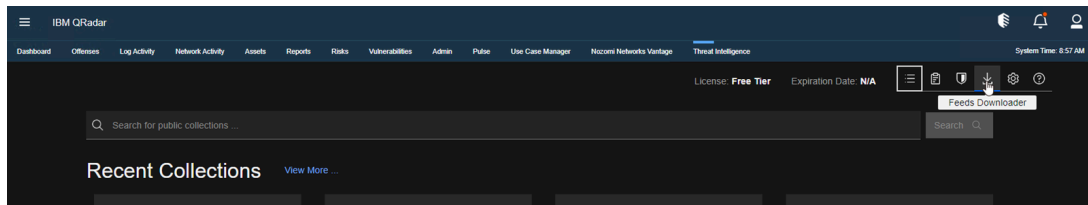


3. Select **All items**.

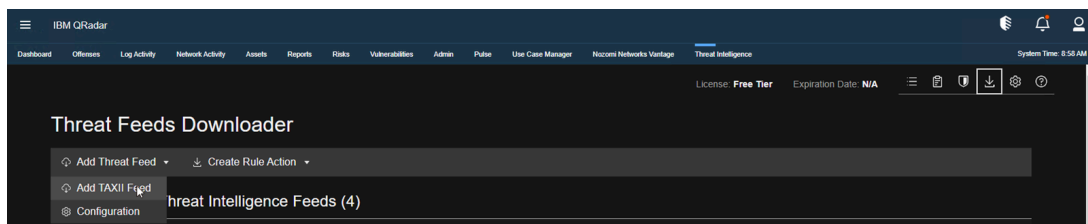
4. Make sure that you have the latest version of the Threat Intelligence app installed.



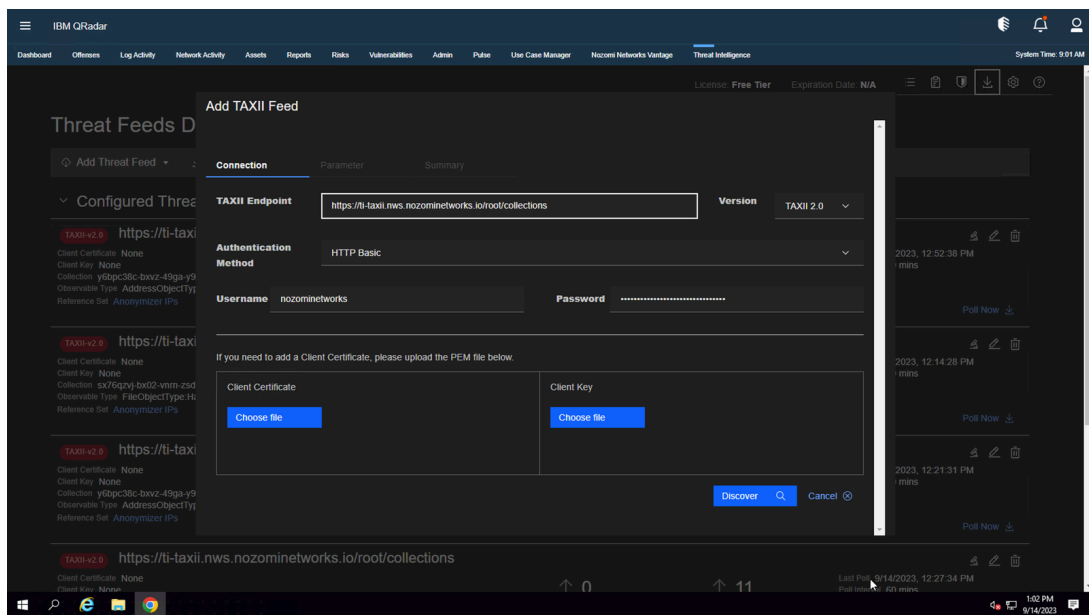
5. Select **Threat Intelligence**.



6. Select **Feeds Downloader**.
7. Select **Add Threat Feed > Add TAXII Feed**.



8. In the **Connection** page, in the **Version** dropdown, select **TAXII 2.0**.

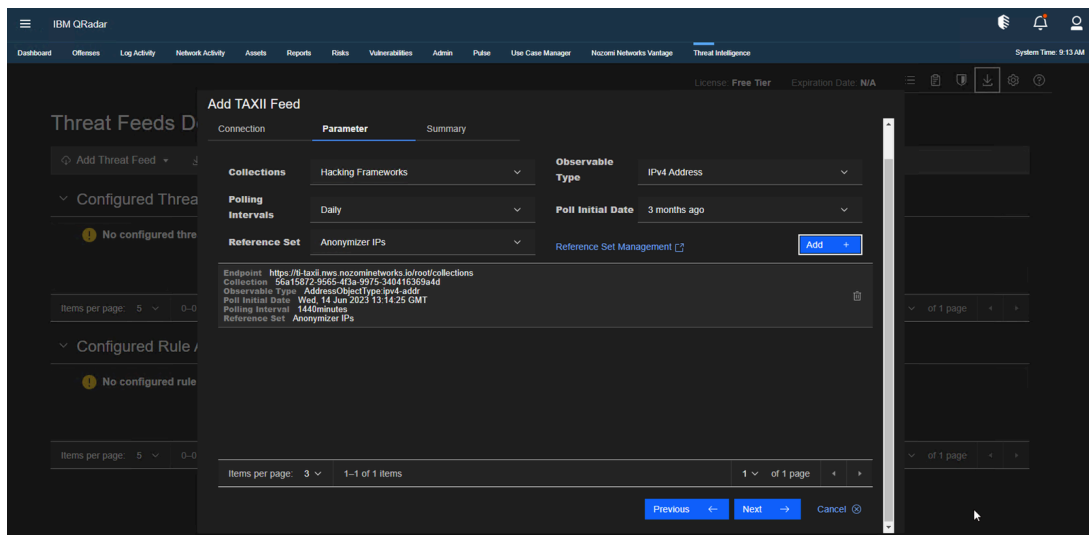


9. Enter the details as necessary in the other fields. Make sure the endpoint string has `/root/collections` at the end.

10. Select **Discover**.

11. Select **Parameter**.

12. From the **Collections** dropdown, select the applicable option.



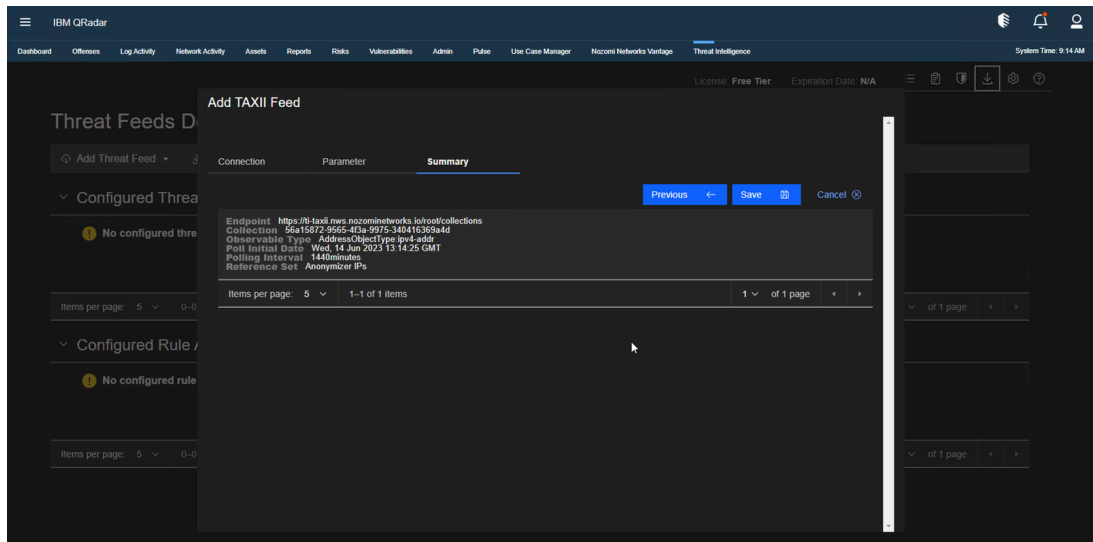
13. From the **Observable Type** dropdown, select the applicable indicator type.

14. To the right of **Reference Set Management**, select **Add**.

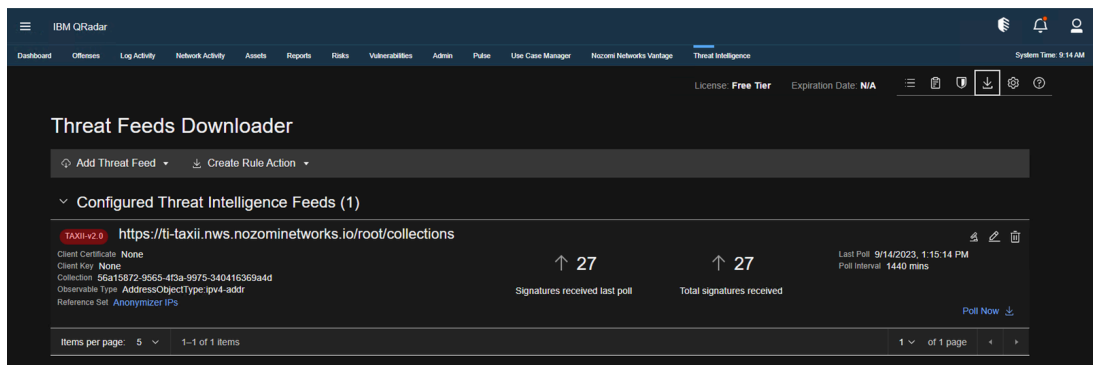
15. In the bottom right section, select **Next**.



16. In the **Summary** page, select **Save**.



17. You can now select **Poll Now** to force the indicator collection.



## Results

QRadar has been configured.



# Chapter 4. Troubleshooting



## Error message: HTTP 401 Unauthorized

### Possible cause

This error will show if the incorrect credentials were used.

### Procedure

Make sure that the user is using the correct credentials that were provided to them.

If none of the previous solutions work, please contact our [Customer Support](#) team.

## Error message: HTTP 404 Not found

### Possible cause

The incorrect discovery, or root, [URL](#) has been used.

### Procedure

Make sure that the discovery [URL](#) used in the configuration is correct.

### Procedure

Make sure that the root [URL](#) used in the configuration is correct.

If none of the previous solutions work, please contact our [Customer Support](#) team.

## Error message: HTTP 406 Not Acceptable

### Possible cause

This error will show if the client sent a *hypertext transfer protocol (HTTP)* header, which the server cannot accept. The expected header can be found in the official TAXII 2.0 [specification](#). This might happen if the client is not correctly configured to use TAXII 2.0 as its protocol, and instead uses TAXII 1.x or TAXII 2.1.

### Procedure

1. Make sure that you specify that the server is TAXII 2.0.
2. If this does not solve the problem, contact our [Customer Support](#) team with this information:
  - The name of the client
  - The version of the client
  - All logs that you can export
  - A timestamp of when the error occurred

**Note:**

This information will be extremely valuable for further debugging.

# Glossary





### **Cyber threat intelligence**

CTI collects and analyzes information on cyber threats and vulnerabilities, providing insights for organizations to proactively understand, prevent, and mitigate cyberattacks. To do this, it learns about the tactics, techniques, and procedures of attackers.

### **Hypertext Transfer Protocol**

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

### **Identifier**

A label that identifies the related item.

### **Internet of Things**

The IoT describes devices that connect and exchange information through the internet or other communication devices.

### **Open Virtual Appliance**

An OVA file is an open virtualization format (OVF) directory that is saved as an archive using the .tar archiving format. It contains files for distribution of software that runs on a virtual machine. An OVA package contains a .ovf descriptor file, certificate files, an optional .mf file along with other related files.

### **Operational Technology**

OT is the software and hardware that controls and/or monitors industrial assets, devices and processes.

### **Security Information and Event Management**

SIEM is a field within the computer security industry, where software products and services combine security event management (SEM) and security information management (SIM). SIEMs provide real-time analysis of security alerts.

### **Structured Threat Information Expression**

STIX™ is a language and serialization format for the exchange of cyber threat intelligence (CTI). STIX is free and open source.

### **Tactics, techniques, and procedures**

TTPs are the patterns of behavior that describe how cyber adversaries operate, encompassing their strategies (tactics), tools and methods (techniques), and specific procedures for executing attacks. Understanding TTPs aids in predicting and defending against future cyber threats.

### **Trusted Automated Exchange of Indicator Information**

TAXII is a protocol for the exchange of cyber threat intelligence (CTI) online. It is often used with Structured Threat Information Expression (STIX) to share detailed threat information.

### **Uniform Resource Locator**

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

