ANY.RUN
INTERACTIVE MALWARE ANALYSIS

ANY.RUN's TI Feeds:
Connector for ThreatQ TIP

Configuration guide

Threat Intelligence Feeds (TI Feeds)

TI Feeds help MSSPs and SOCs fortify their security with filtered, high-fidelity indicators of compromise (IPs, domains, URLs) enriched with threat context from ANY.RUN's Interactive Sandbox.

Sourced from real-time sandbox investigations of active attacks across 15,000+ organizations, TI Feeds connect seamlessly with SIEMs/XDRs/firewalls and other security solutions to monitor and identify malware and phishing threats.

ANY.RUN's feeds are updated every two hours, allowing you to track threats as they emerge, develop, and spread to take critical security actions early.

- **Unique data:** Fresh indicators from live detonations of attacks with links to sandbox sessions with full threat context, including TTPs.
- **No false alerts:** TI Feeds provide reliable IOCs with a near-zero false positive rate thanks to pre-processing.
- **Prioritization of incidents:** SOC teams use TI Feeds as part of alert triage, incident response, and proactive hunting to effectively handle urgent threats.

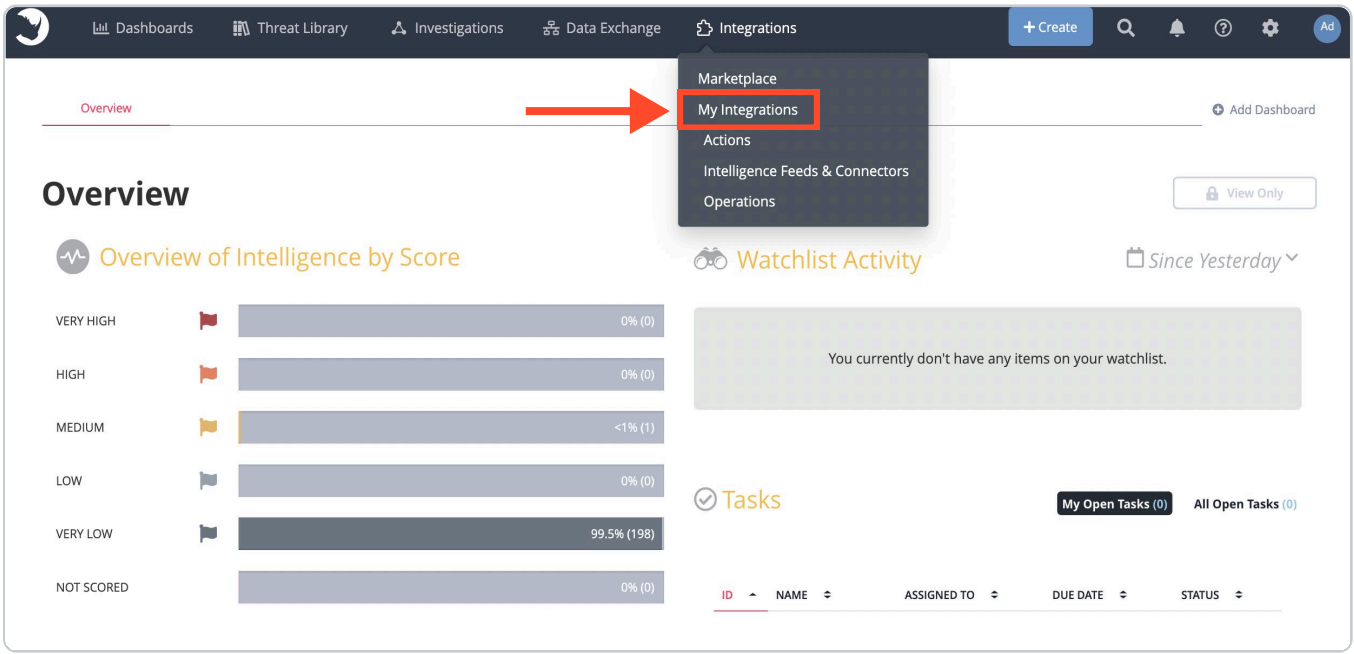
TI Feeds are available for integration using API or SDK and support TAXII protocol.

➡ For more details, feel free to **contact us**.

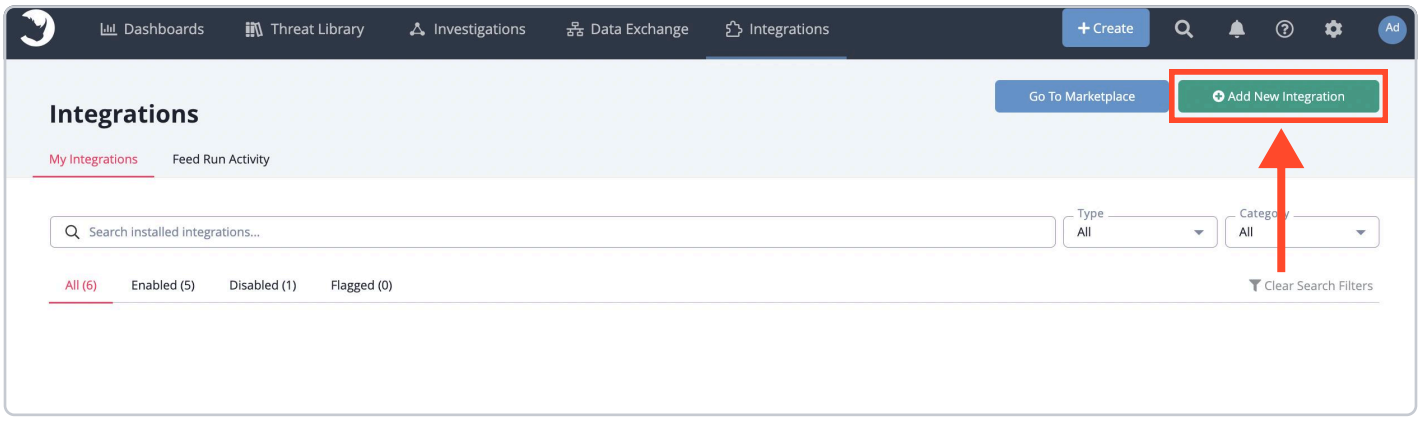
How to Connect TI Feeds with ThreatQ TIP

Connecting to TAXII server

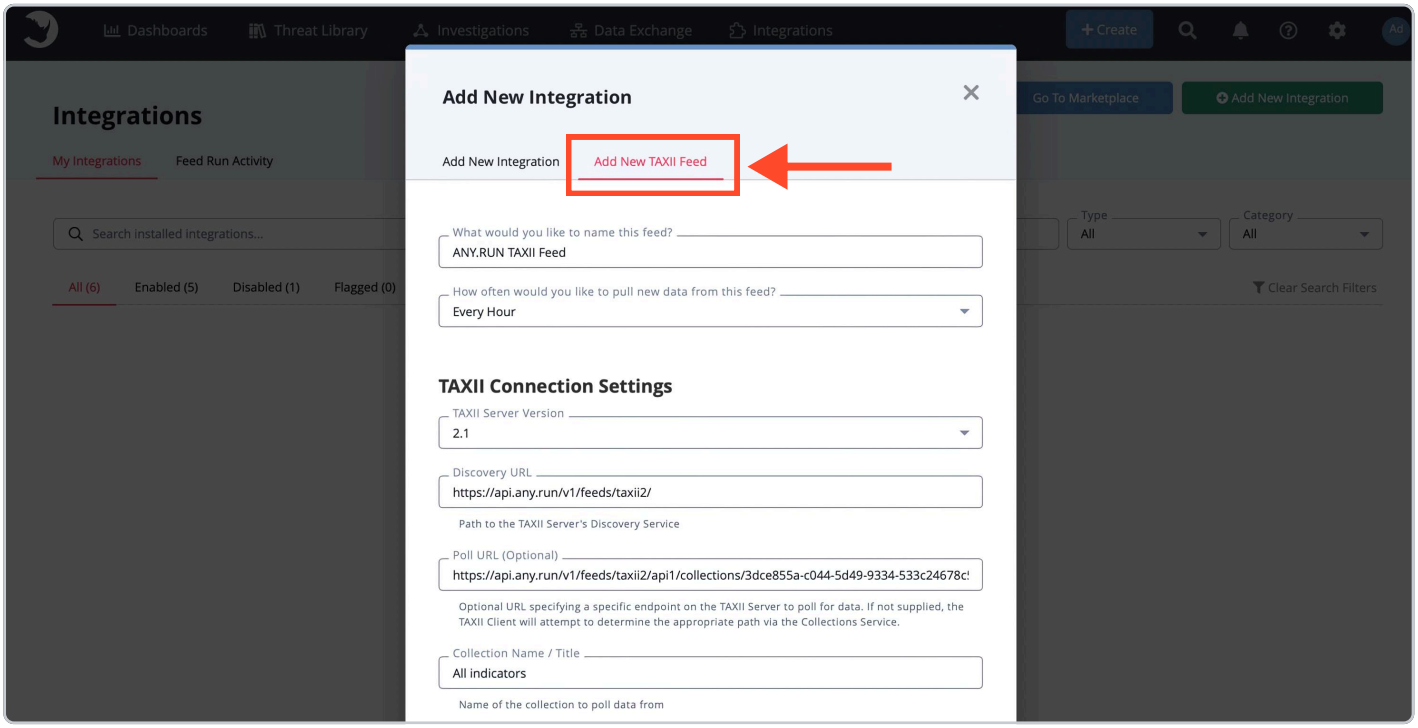
1. Open ThreatQ and click **My Integrations** in the **Integrations** tab.



2. Click **Add New Integration**.



3. Go to the tab **Add New TAXII Feed**:



4. Fill out the configuration form.

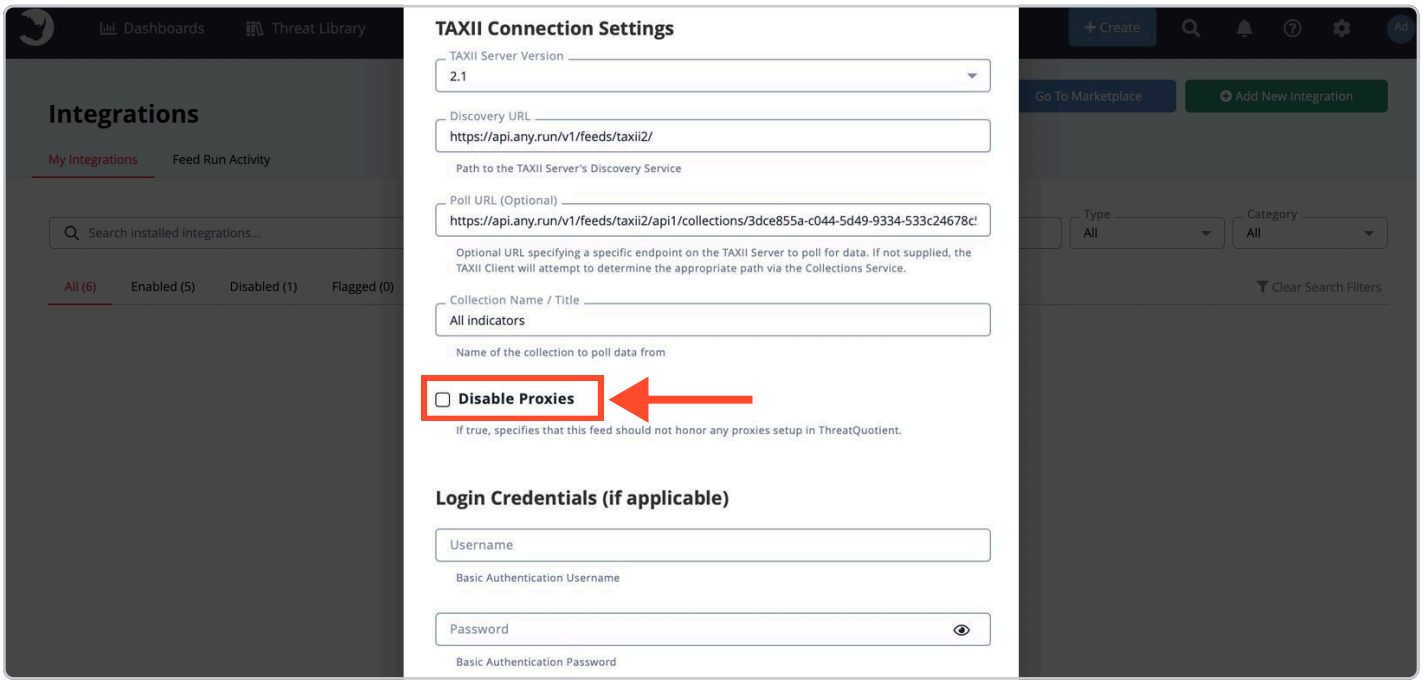
4.1 Name the feed and set the frequency for pulling new data from it in a range from every hour to every 30 days.

4.2 Configure TAXII connection settings:

- Set **TAXII Server Version** to 2.1
- Set **Discovery URL**: https://api.any.run/v1/feeds/taxii2
- To fill Poll URL and Connection Name / Title fields, choose a collection from the table below:

Name	Description	Poll URL
All indicators	Contains IOCs of all formats (IPs, Domains, URLs)	https://api.any.run/v1/feeds/taxii2/api1/collections/3dce855a-c044-5d49-9334-533c24678c5a
IPs collection	Contains only IPs	https://api.any.run/v1/feeds/taxii2/api1/collections/55cda200-e261-5908-b910-f0e18909ef3d
Domains collection	Contains only Domains	https://api.any.run/v1/feeds/taxii2/api1/collections/2e0aa90a-5526-5a43-84ad-3db6f4549a09
URLs collection	Contains only URLs	https://api.any.run/v1/feeds/taxii2/api1/collections/05bfa343-e79f-57ec-8677-3122ca33d352

- You can also **Disable Proxies** if needed.



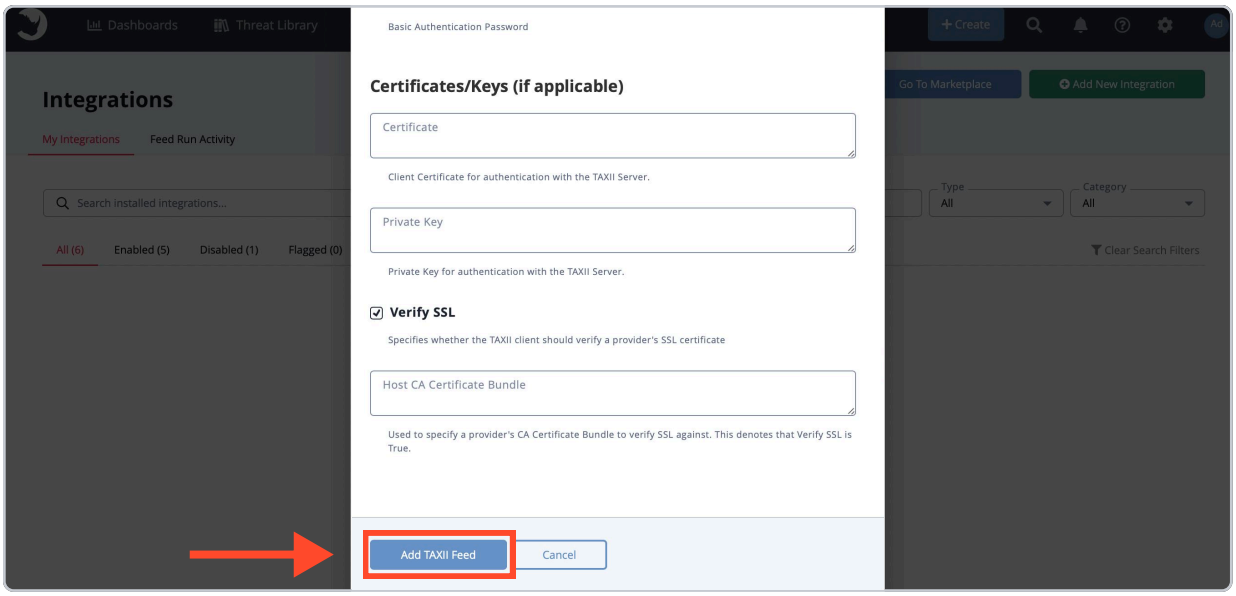
4.3 Fill out your **Login Credentials**.

- Enter your Username and Password.

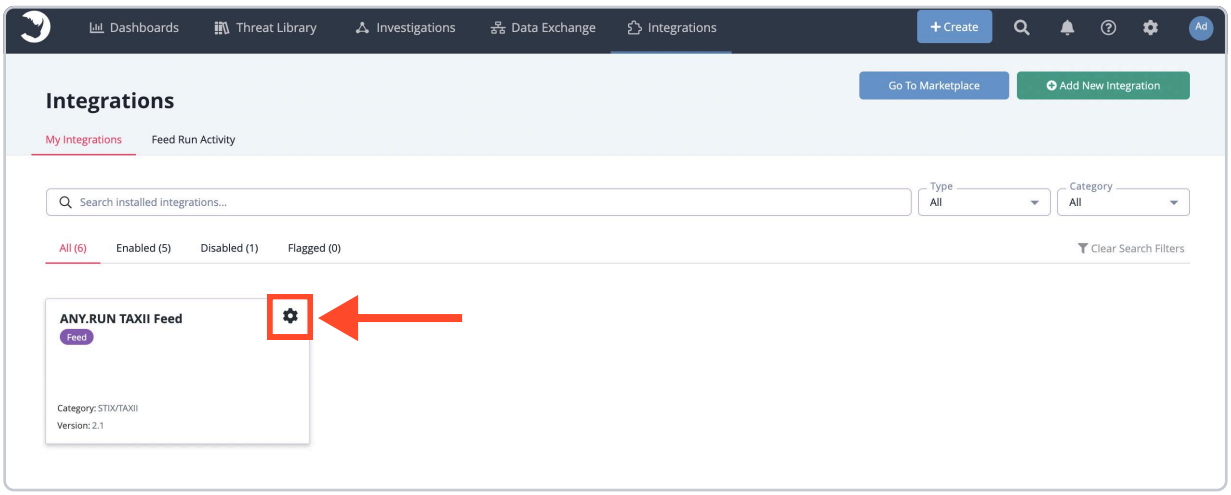
If you don't have these credentials, contact your account manager at ANY.RUN or fill out this form.

For more information, see TAXII documentation by ANY.RUN: https://intelligence.any.run/guide/

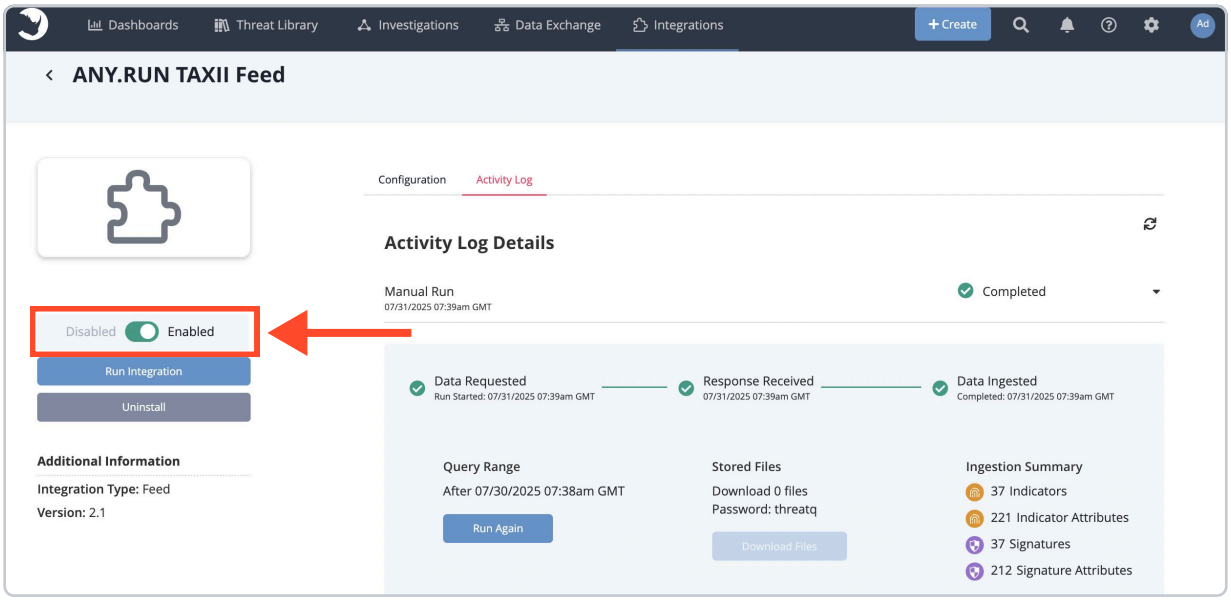
4.4 Once all fields are filled out, click **Add TAXII Feed**.



4.5 Click on the settings button in the created connector card:



4.6 Set switch to **Enabled** and you're all set up.



On this page you can also check the Activity Log to ensure everything was set up correctly.

How to Use TI Feeds with ThreatQ TIP

After finalizing the configuration, you can use the retrieved indicators to:

- Export them to SIEM/SOAR to automate detection and blocking of threats
- Prioritize high-risk threats to stay focused on the most critical incidents
- Combine them with data from other sources to gain full visibility into attacks
- Enrich and accelerate threat hunting and investigations with actionable intelligence
- Launch playbooks for automated response to threats