ANY.RUN
INTERACTIVE MALWARE ANALYSIS

ANY.RUN's TI Feeds:

Integration with Microsoft Sentinel

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 integrate 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.

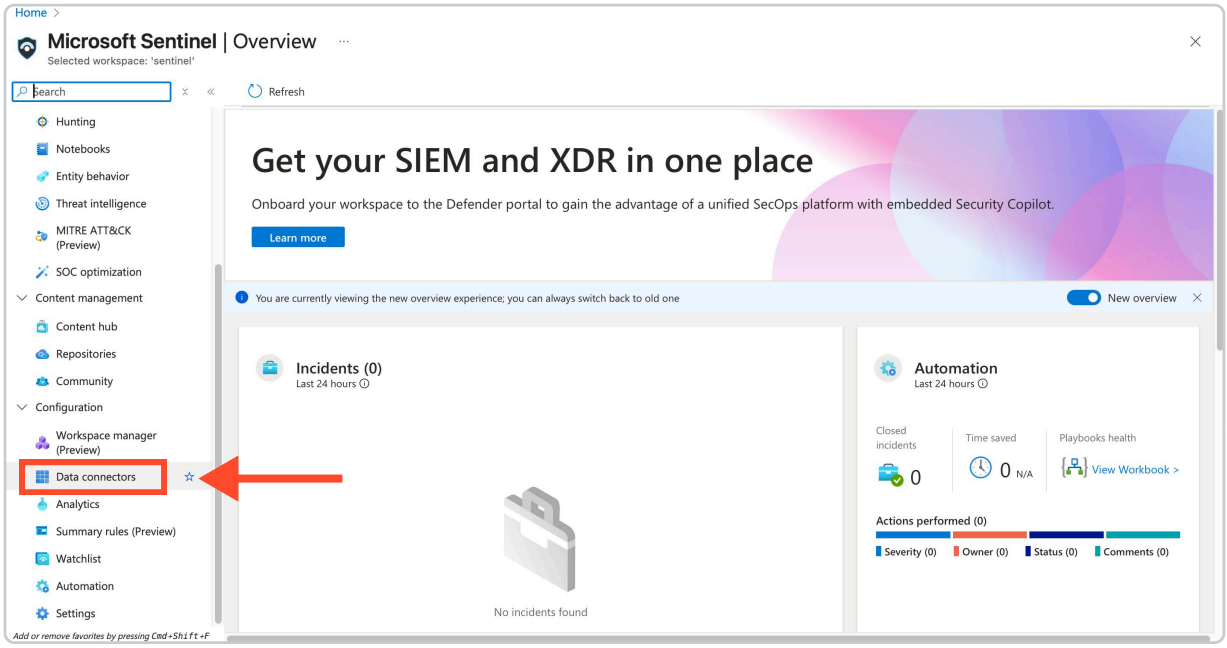
TI Feeds are available for integration using API or SDK and support TAXII protocol.

For more details, feel free to contact us.

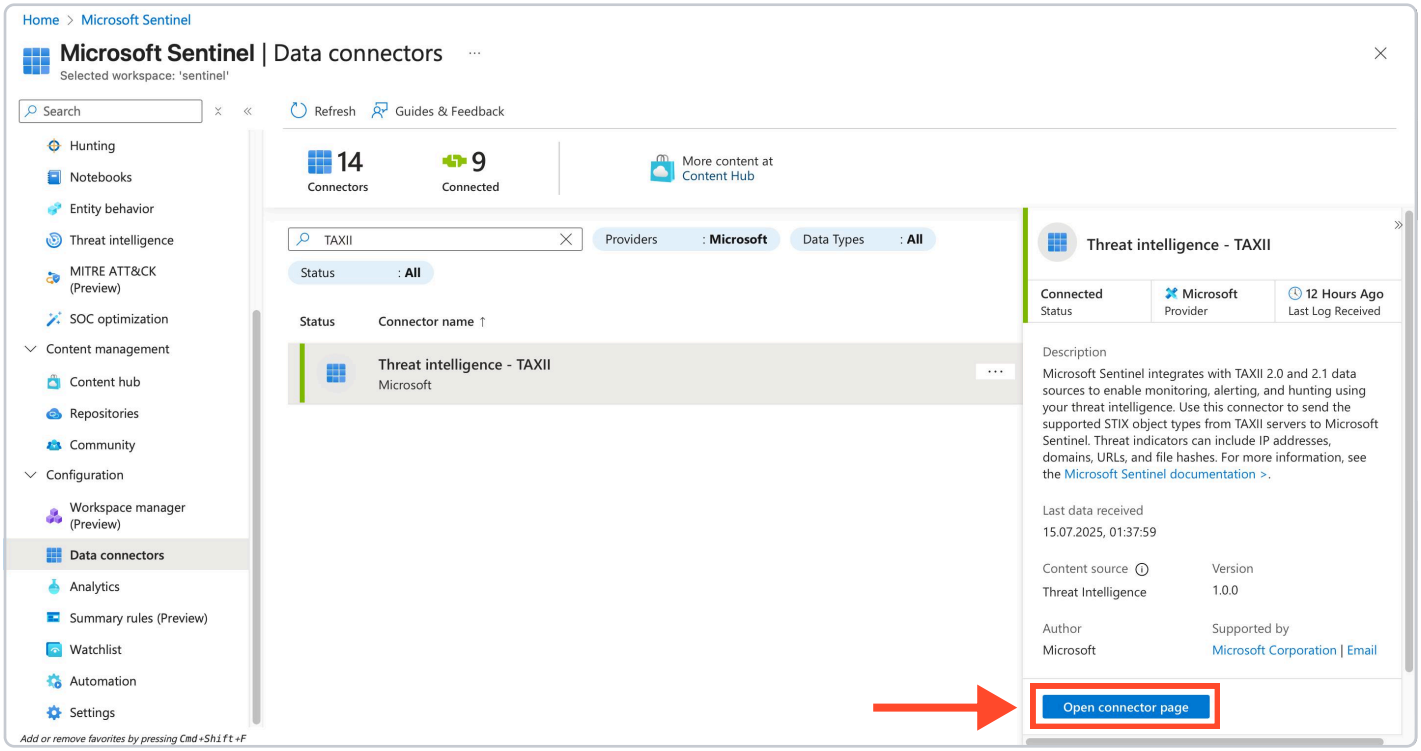
How to Connect TI Feeds to MS Sentinel

Connecting to TAXII server

1. Open MS Sentinel and go to the **Data connectors** tab in the **Configuration** section.

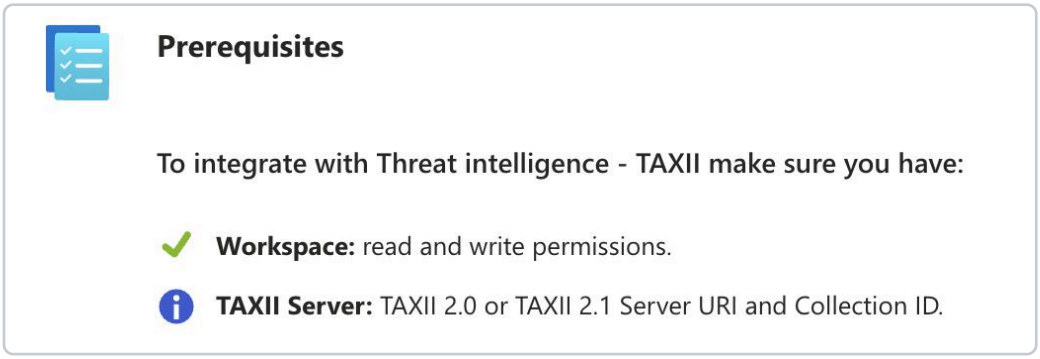


2. Search for the **Threat Intelligence TAXII** connector and click **Open connector page**.



3. You will see the list of prerequisites for the connector. If you lack any of them, see this documentation:

   https://learn.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-taxii



4. Fill out the **Configuration** form:

- Name the server via the **Friendly name** field.
- Insert **API root URL**: https://api.any.run/v1/feeds/taxii2/api1/
- Choose a **Collection ID**:

Name	Description	ID
All indicators	Contains IOCs of all formats (IPs, Domains, URLs)	3dce855a-c044-5d49-9334-533c24678c5a
IPs collection	Contains only IPs	55cda200-e261-5908-b910-f0e18909ef3d
Domains collection	Contains only Domains	2e0aa90a-5526-5a43-84ad-3db6f4549a09
URLs collection	Contains only URLs	05bfa343-e79f-57ec-8677-3122ca33d352

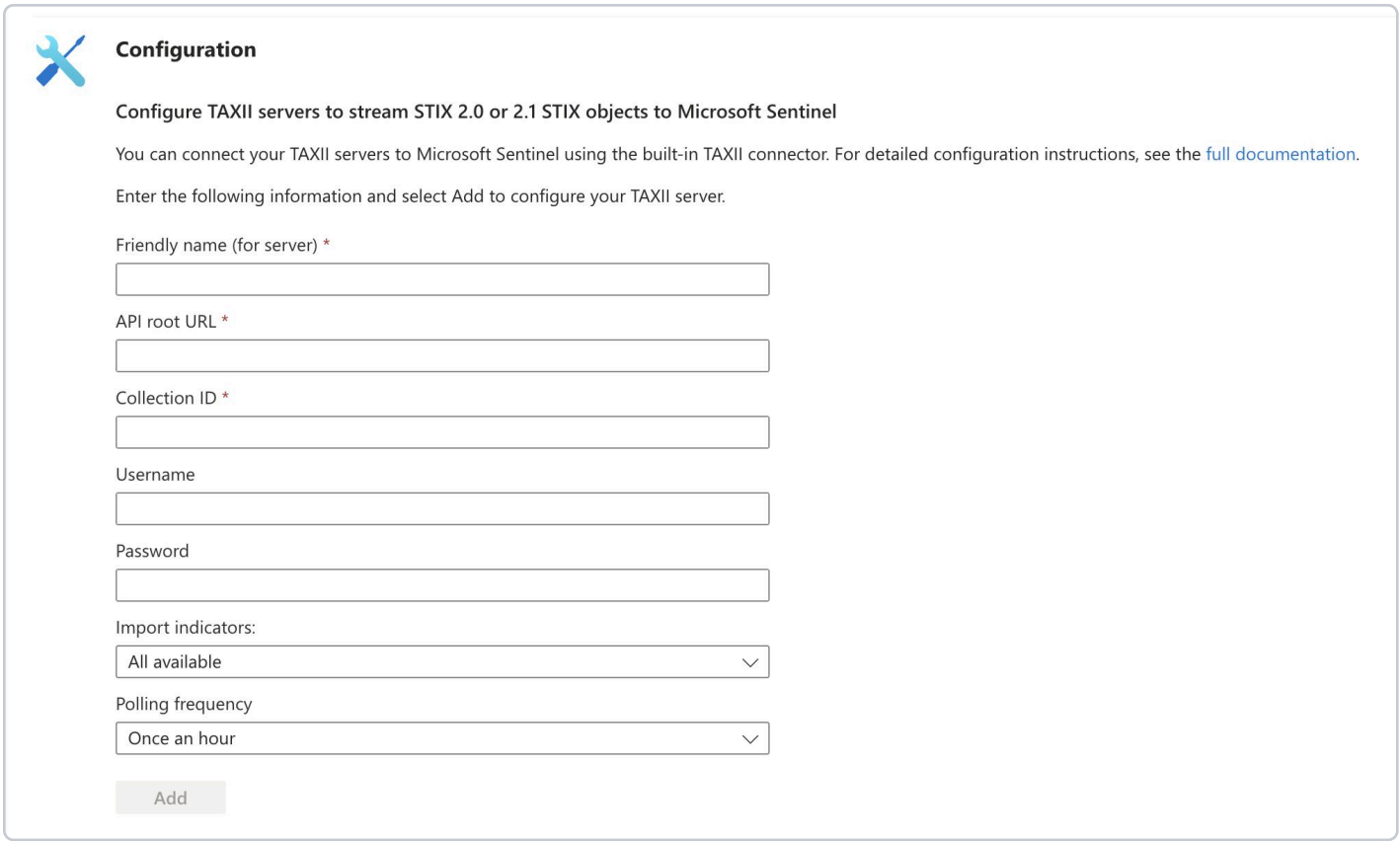
- Enter your **Username** and **Password**.

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

You can also choose to import all available indicators or those that are one day, week, or month old via the field **Import indicators**.

Another optional setting is **Polling frequency** that determines how often you'd like to connect to the TAXII server to retrieve new feeds: once a minute, once an hour, or once a day.

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



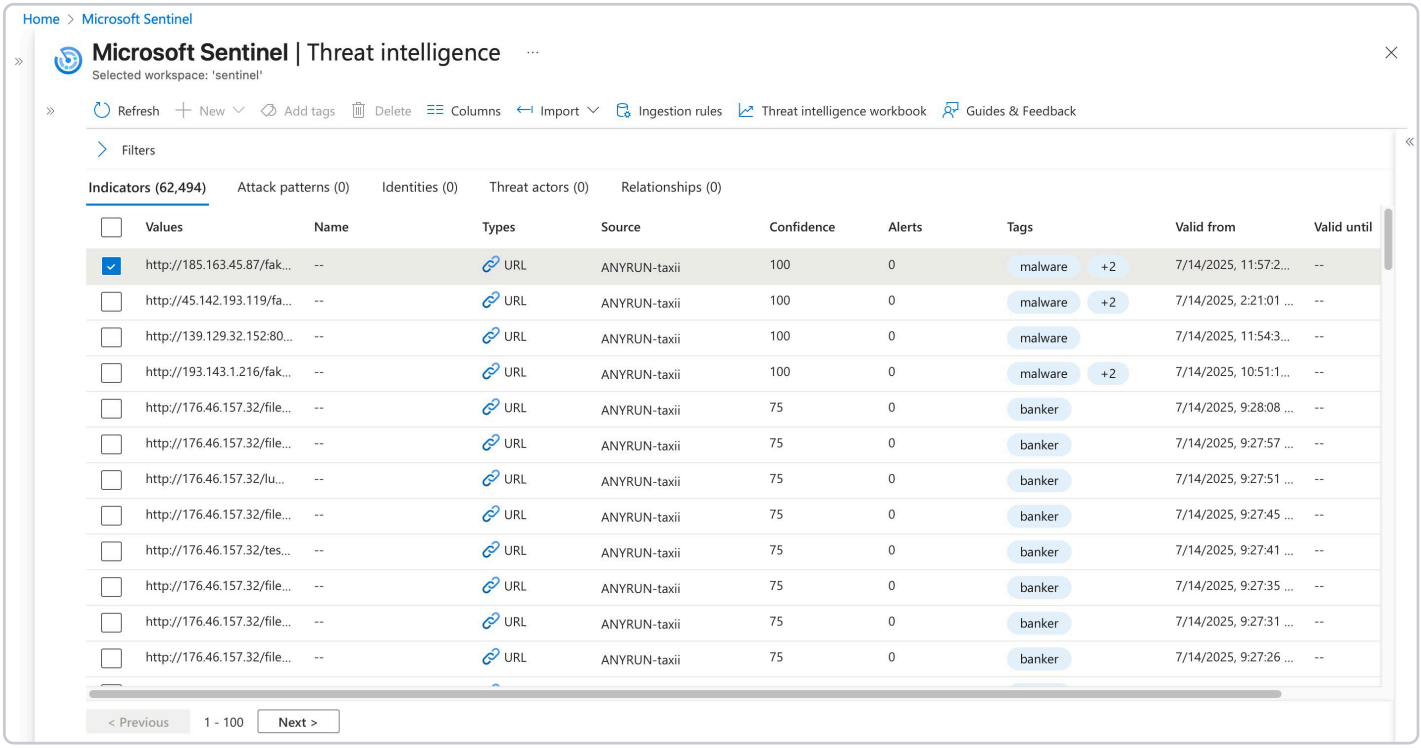
Finally, click **Add** and you're all set up.

Browsing indicators

To access the indicators you've retrieved, go to the **Threat intelligence** tab.

You'll find a table with fields describing each indicator:

- **Values** – indicator itself
- **Names** – name of an indicator
- **Types** – type of an indicator (IP, URL, or Domain)
- **Sources** – source of an indicator
- **Confidence** – this rate determines our level of certainty on whether an indicator is malicious (50 – suspicious, 75 – likely malicious, 100 – malicious).
- **Alerts** – number of alerts related to an indicator
- **Tags** – descriptors of an indicator
- **Valid from** and **Valid until** – time period during which an indicator is considered valid



If you have any questions,
contact us via this form or write to support@any.run