ANY.RUN's TI Feeds:

Integration with Rapid7

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 16,000+ organizations, TI Feeds integrate seamlessly with SIEMs/XDRs/firewalls and other security solutions to monitor and identify malware and phishing threats.

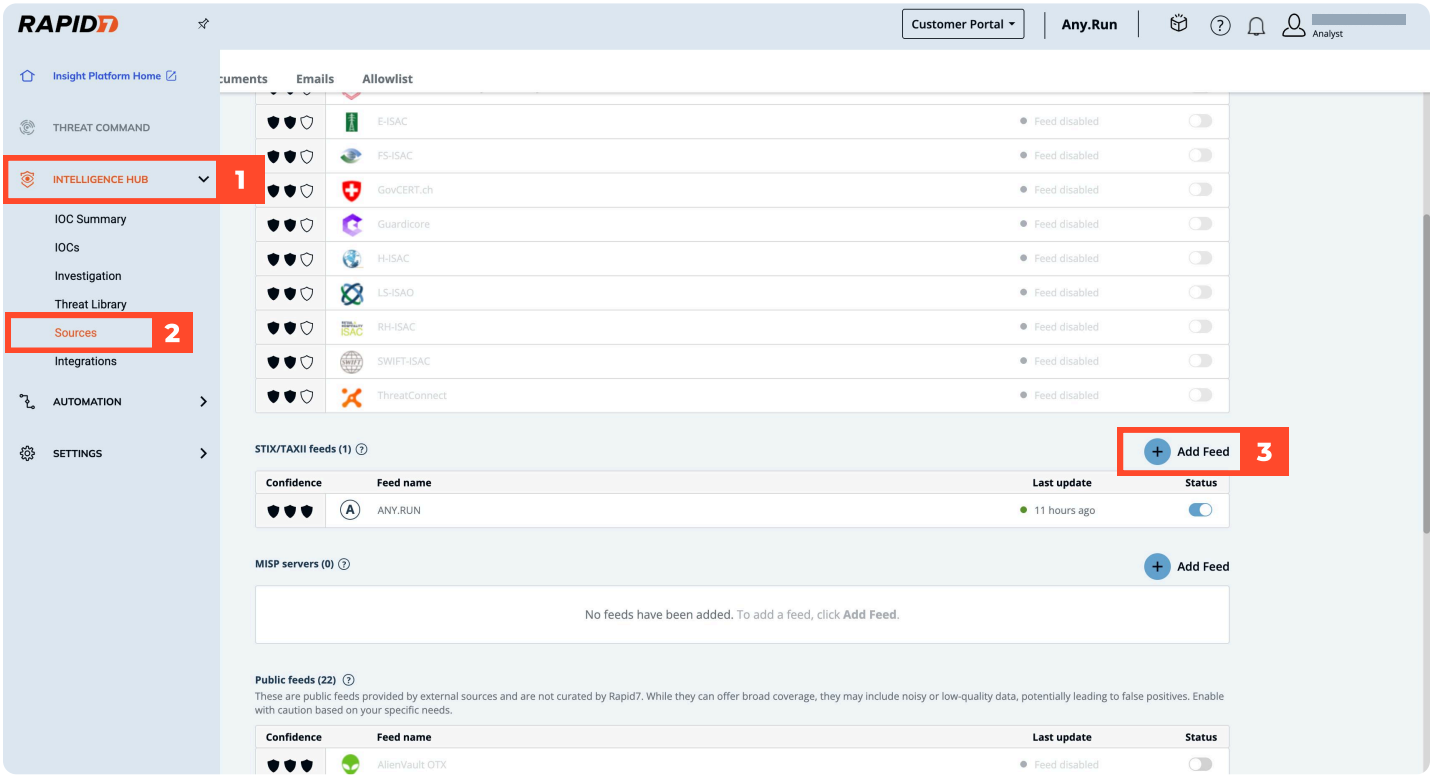
ANY.RUN's feeds are updated every two hours, allowing you to track threats as they emerge, develop, and spread to take critical security actions early.

- **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 Rapid7

1. Open your Rapid7 environment and go to the **Intelligence Hub** tab. In the **Sources** section, click **Add Feed**.

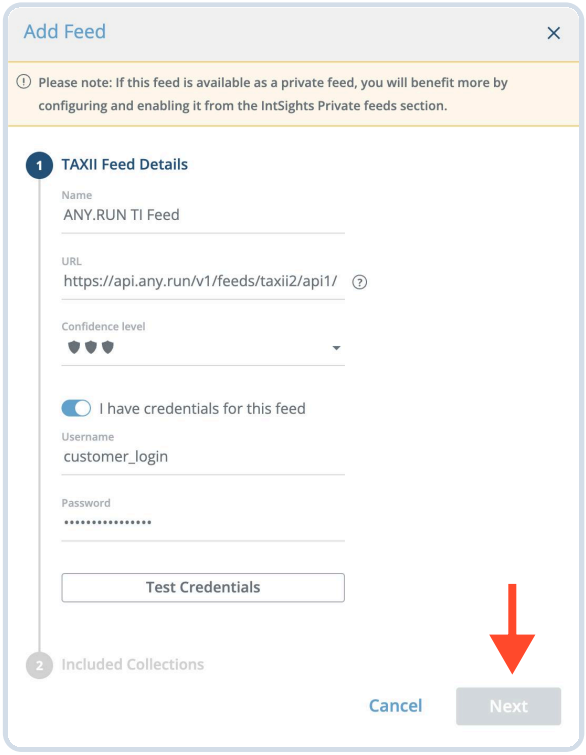


2. Configure the integration by filling in the required fields.

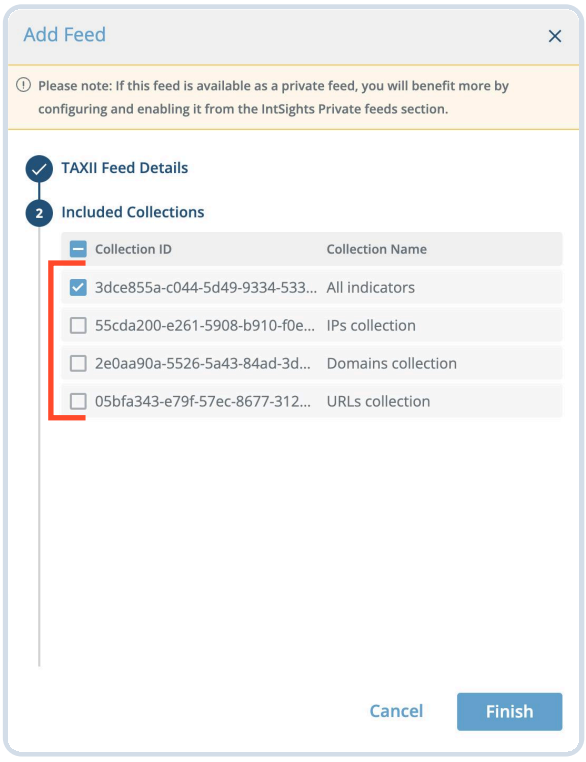
- Enter a **Name** for the feed and the following **URL**:

https://api.any. run/v1/feeds/taxii2

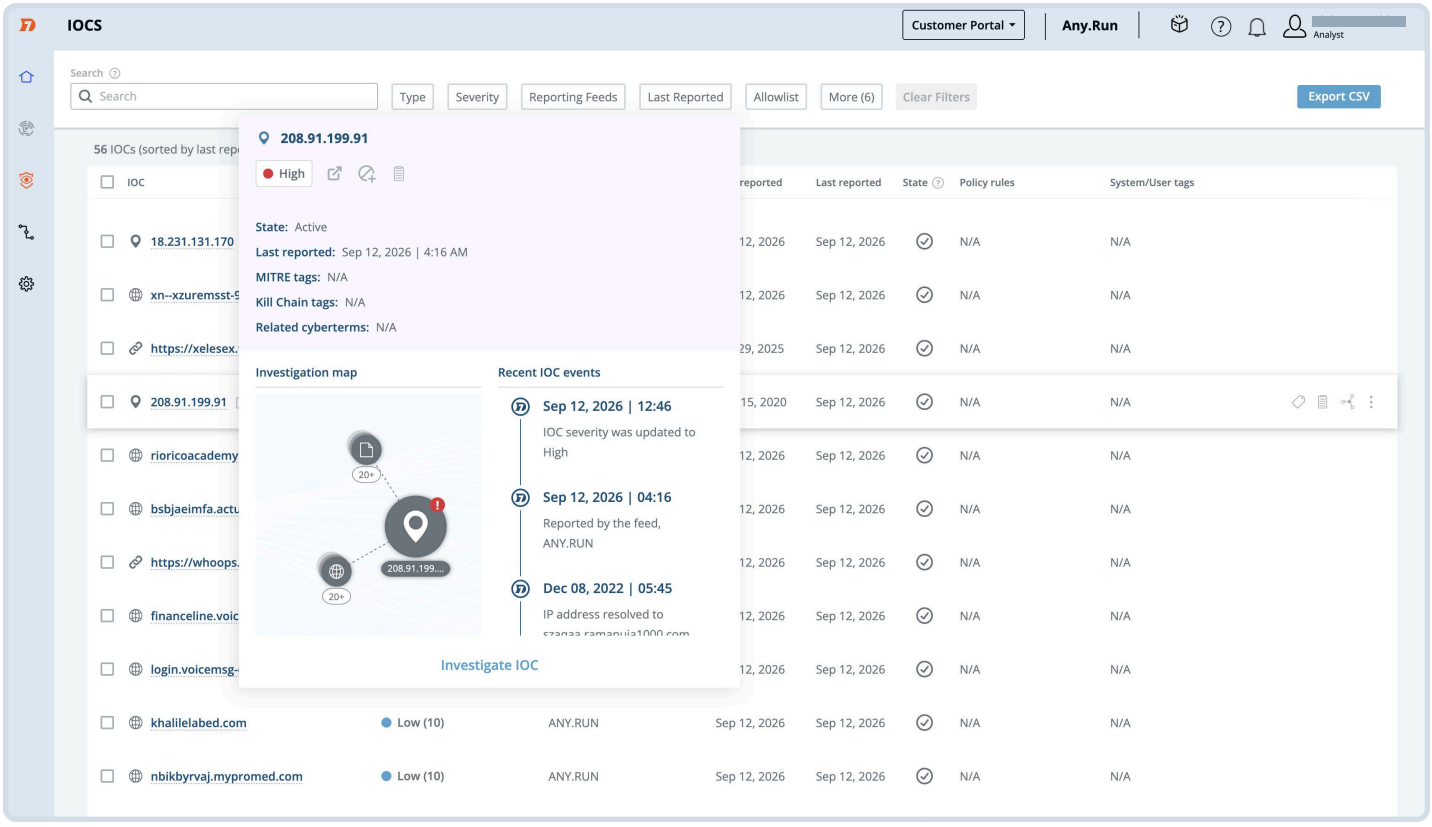
- Set the **Confidence level** to the maximum and enable **I have credentials to this feed**.
- Enter the **Username** and **Password** for your ANY.RUN account with access to TI Feeds.
- Click **Test Credentials**, then click **Next**.



3. Select the feed collections you want to include: All indicators, IPs, Domains, or URLs. We recommend choosing **All indicators**.



4. The setup is complete. Once the feed loads, indicators from ANY.RUN TI Feeds will appear in the **IOCS** section. You can now use them in your daily SOC workflows and detection rules.



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