EclecticIQ

EclecticIQ Platform

Incoming feed - Recorded Future Feeds

Table of contents

ⓘ This article describes how to configure Incoming feeds for a particular feed source.
To see how to configure incoming feeds in general, see Configure incoming feeds general options[1].

	Specifications
Transport types	• Recorded Future Analyst Note Feed • Recorded Future Domain Feed • Recorded Future Hash Feed • Recorded Future IP Feed • Recorded Future URL Feed
Content types	• Recorded Future JSON • Recorded Future CSV
Ingested data	Cleaned and processed Recorded Future JSON and CSV.
Processed data	IPs, domains, URLs, hashes, and reports.
Endpoints	• `https://api.recordedfuture.com/v2/analystnote/search` (Analyst Note) • `https://api.recordedfuture.com/v2/fusion/files/?path=/public/risklists/default_domain_risklist.csv` (Domain) • `https://api.recordedfuture.com/v2/fusion/files/?path=/public/risklists/default_hash_risklist.csv` (Hash) • `https://api.recordedfuture.com/v2/fusion/files/?path=/public/risklists/default_ip_risklist.csv` (IP) • `https://api.recordedfuture.com/v2/fusion/files/?path=/public/risklists/default_url_risklist.csv` (URL)
Description	The Recorded Future integration provides both a feed and enricher capabilities. With the feed, users have access to the Recorded Future Risk List which includes IP and file hashes, for example. The results are provided in standard STIX/TAXII protocols including TTPs and Indicators. The enricher allows users to query Domains, hashes, URLs and IP addresses.

Requirements

---

1 https://docs.eclecticiq.com/display/LAT/Configure+incoming+feeds+general+options

The Recorded Future feeds are compatible with EclecticIQ Platform release 2.3 and later. Users need an API key for their own configuration. Sign up and subscribe to the service to obtain the required API key credentials.

Configure the incoming feed

1. In the top navigation bar, click **Data configuration > Incoming feeds >** ➕ .
2. From the **Transport type** drop-down menu, select the preferred Recorded Future feed.
3. From the **Content type** drop-down menu, select preferred Recorded Future content type.
4. The **API URL** field is automatically filled in with the default domain for the endpoint, depending on the selected **Transport type**.
   You can add a proxy or set up ports according to your needs.
5. In the **API key** field, enter your API key.
6. The **SSL verification** checkbox is automatically selected.
7. In the **Path to SSL certificate** field, enter the path to your PEM file.
   To store your changes, click **Save**; to discard them, click **Cancel**.

Test the feed

1. In the top navigation bar, click **Data Configuration > Incoming feeds**.
2. Click the feed that you just created, using the steps above.
3. In the **Overview** view, click **Download now**.
4. Click **Ingested entities** and check that entities have been ingested into the platform.

Or:

1. In the top navigation bar, click **Intelligence > All intelligence > Browse**.
2. Click the **Entities** tab.
3. In the top-left corner, click ⟱ .
4. From the **Source** drop-down menu, select the incoming feed you have just created, using the steps.

5. You can also filter also by entity type: from the **Entity** drop-down menu, select the entity types you want to include in the filtered results.

See also

- Configure the general options[2]
- Set a schedule[3]
- About TLP overrides[4]
- Set half-life values[5]
- Start and stop incoming feeds[6]
- Purge incoming feeds[7]
- Delete incoming feeds[8]
- List of incoming feeds[9]

---

2 https://docs.eclecticiq.com/display/PINT/Configure+incoming+feeds+general+options
3 https://docs.eclecticiq.com/display/PINT/Set+a+schedule
4 https://docs.eclecticiq.com/display/PINT/About+TLP+overrides
5 https://docs.eclecticiq.com/display/PINT/Set+half-life+values
6 https://docs.eclecticiq.com/display/PINT/Start+and+stop+incoming+feeds
7 https://docs.eclecticiq.com/display/PINT/Purge+incoming+feeds
8 https://docs.eclecticiq.com/display/PINT/Delete+incoming+feeds
9 https://docs.eclecticiq.com/display/PINT/List+of+incoming+feeds