Mandiant

ELASTIC SIEM INTEGRATION

This feature is released as a Public Preview.
Pre-GA products and features are available "as is" and might have limited support. For more information, please contact your TSC, your CSM, or go to **Support.**
(https://docs.mandiant.com/home/mandiant-support-cases)

The Mandiant Advantage integration for Elastic SIEM lets you retrieve Indicators of Compromise (IOCs) from Mandiant Advantage Threat Intelligence (MATI). These indicators can be used for correlation in Elastic SIEM to help discover potential threats. MATI gives you access to unparalleled visibility and expertise to understand the threats that matter most to your business.

Prerequisites

- An Elasticsearch instance for storing and searching your data.
  - You can use Elasticsearch Service on Elastic Cloud (recommended), or self-manage the Elastic Stack on your own hardware.
- API access Key ID and Secret generated from the MATI platform to authenticate requests from Elastic.
- Network connectivity to **https://api.intelligence.mandiant.com** over port 443

Compatibility

- This integration has been tested against the MATI API v4.

Get API Key ID and Secret

To obtain a **Service API Key** (which is tied to an organization rather than an individual user) for use with third-party security technologies such as a SIEM, contact **Support** **(https://www.mandiant.com/support)**.

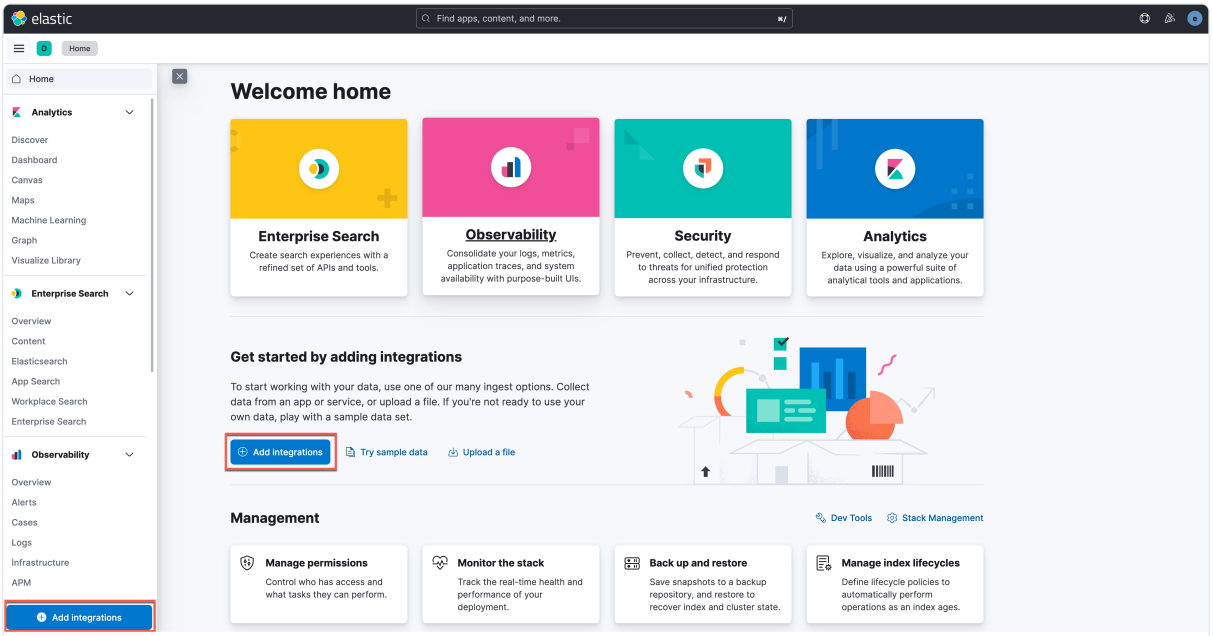
To obtain an API Key ID and Secret for an individual user account, perform the following:

1. Navigate to the Mandiant Threat Intelligence web console.
2. Click **Account Settings**.
3. Select **API Access and Keys** from the navigation menu.
4. Click **Get Key ID and Secret**.
5. Copy and store the displayed values in a secure location.

Installation

Complete the following workflow to set up and install the integration.

1. Log into the Elastic SIEM web console.
2. Click **Add Integration**.

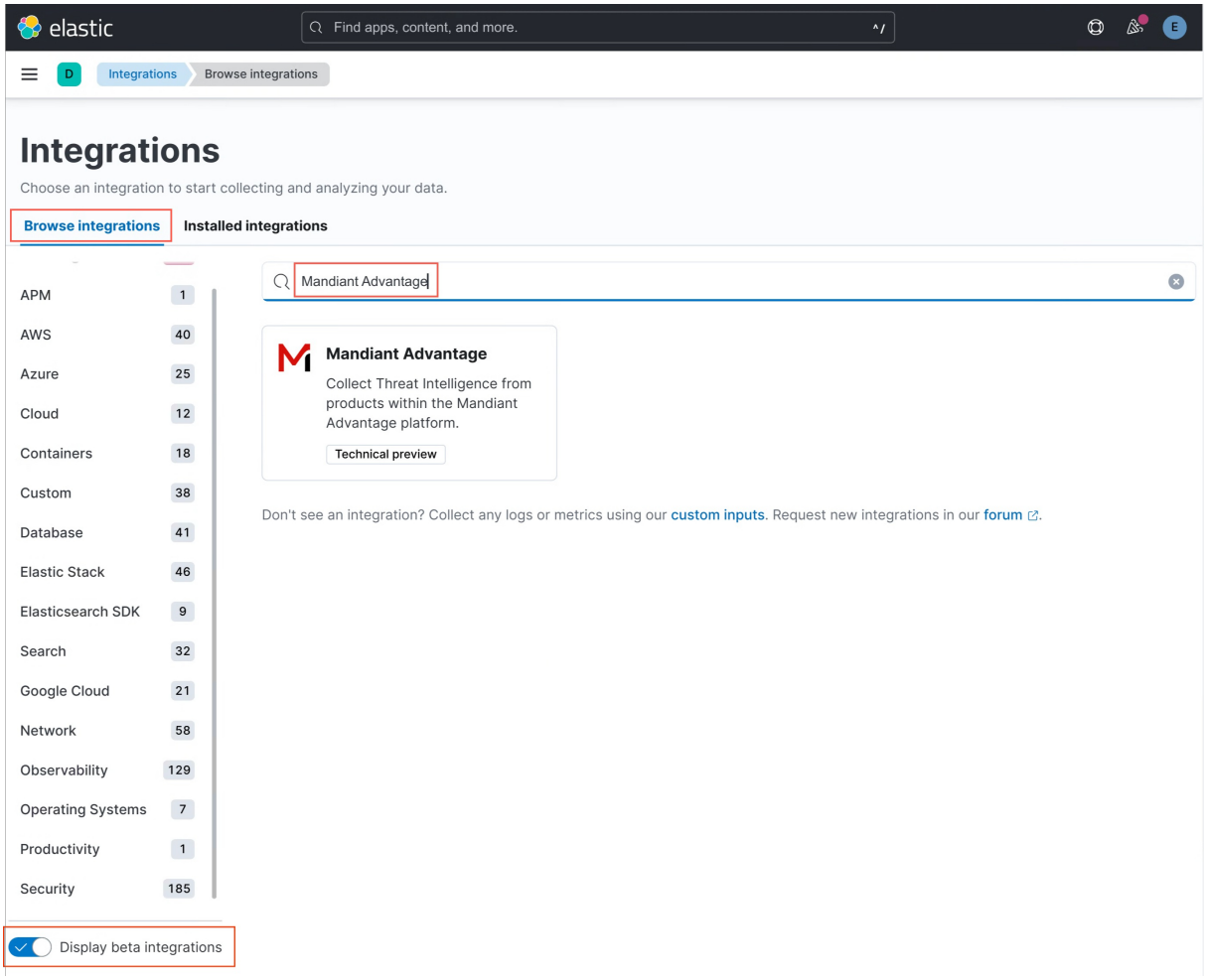


The Elastic Home page

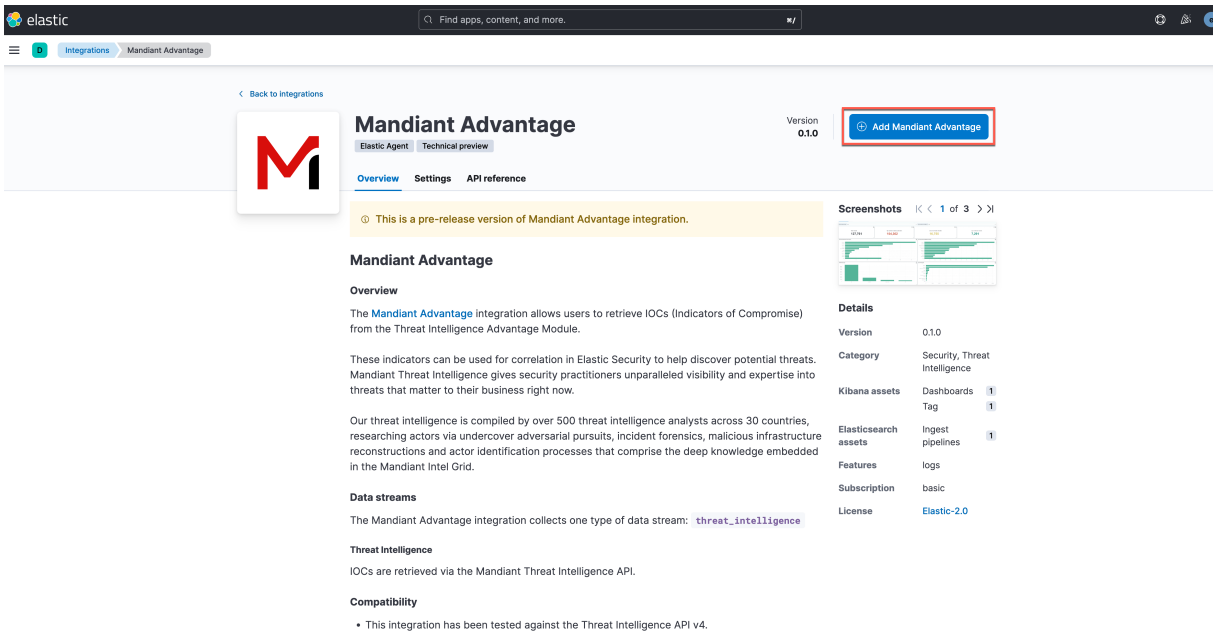
3. Navigate to the **Browse integrations** tab.
4. Enter "Mandiant Advantage" in the **Search** field.

> Be sure the option to **Display beta integrations** is enabled.

5. Click **Mandiant Advantage**.

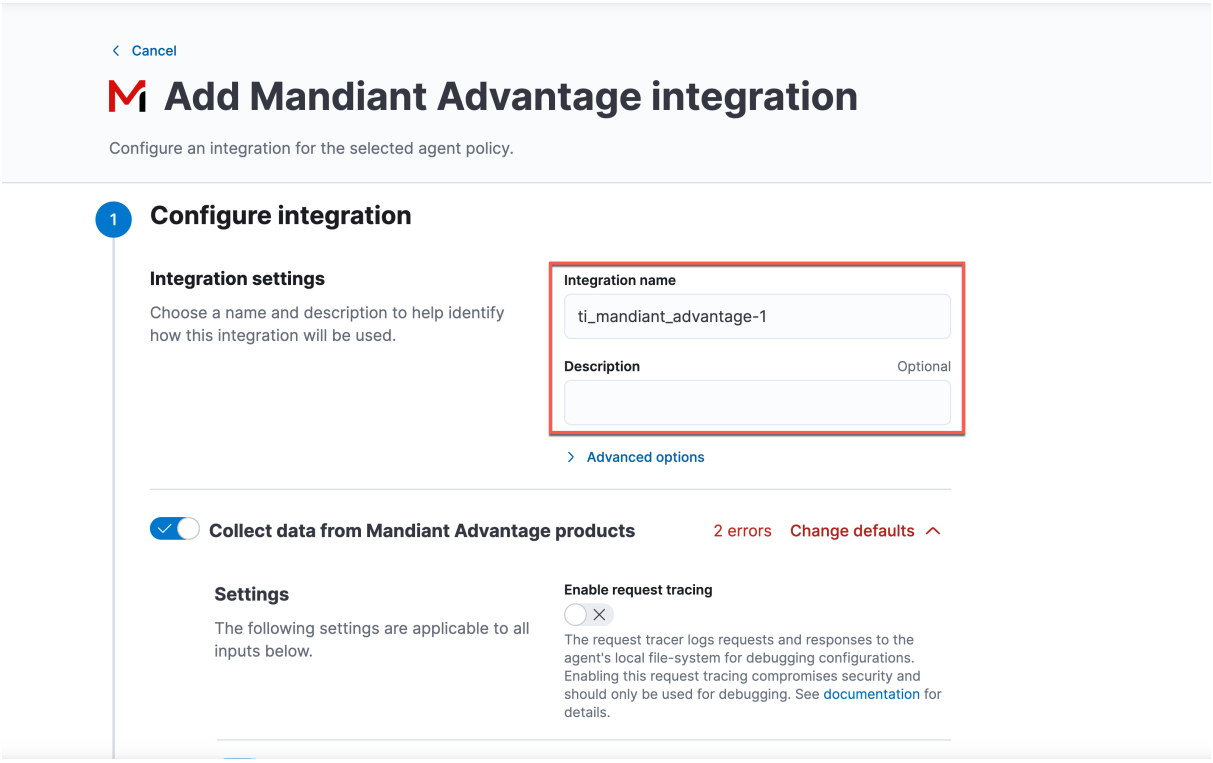


6. Click **Add Mandiant Advantage**.

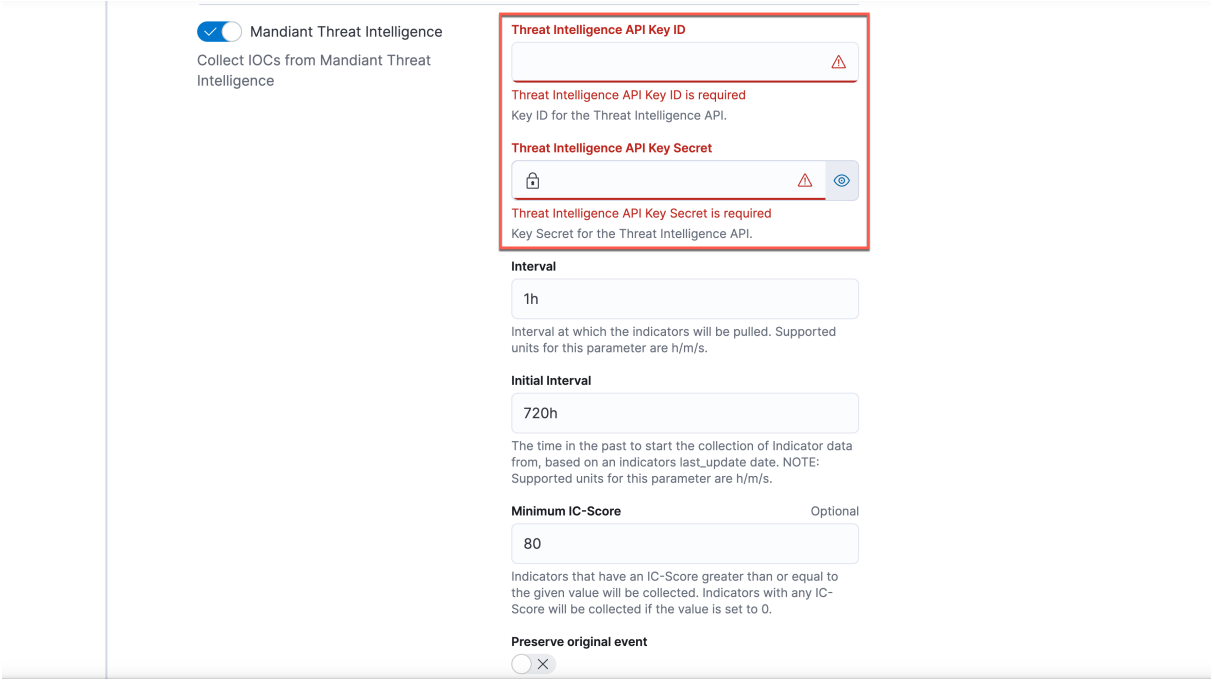


7. Enter an **Integration name.**

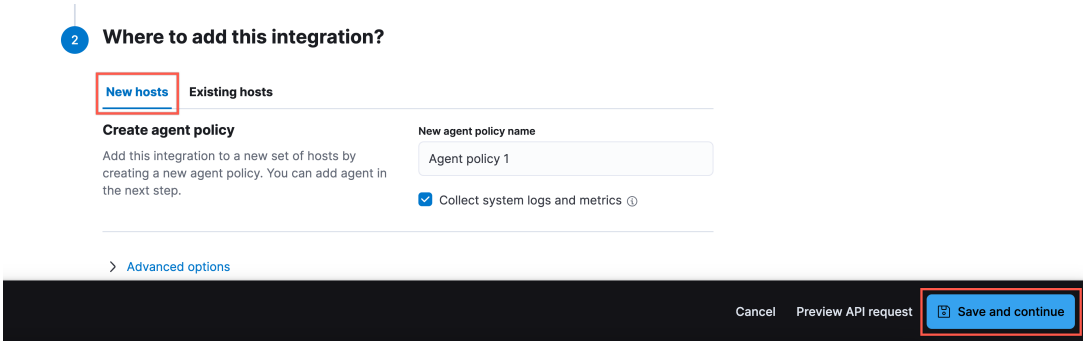
8. Optional: Enter a **Description** for the integration.



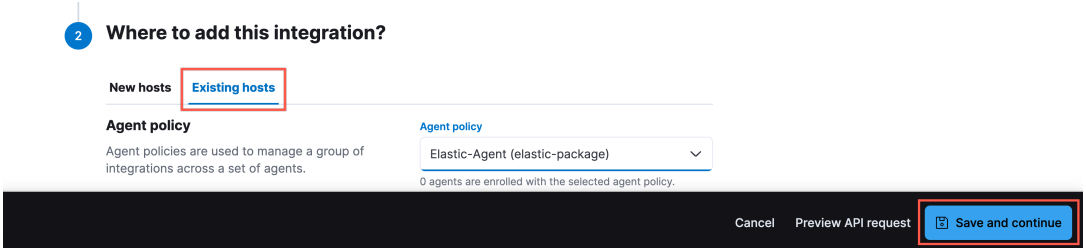
9. Enter your **Threat Intelligence API Key ID** and **Threat Intelligence API Key Secret** generated from the MATI platform.



10. Choose where to add the integration.
    - To add this integration to a new set of hosts, click the **New Hosts** tab.
        - Enter a **New agent policy name** to create an Agent policy for the new hosts.
        - Click **Save and continue** to complete the integration installation.



- To add this integration to an existing set of hosts, click the **Existing hosts** tab.
  - Select which **Agent policy** to apply.
  - Click **Save and continue** to complete the integration installation.



API details and usage

Elastic SIEM documentation defines data sources as Data Streams and data storage locations as Log References.

Data streams

- The Mandiant Advantage integration collects one type of data stream: `threat_intelligence`
  - IOCs are retrieved from the `threat_intelligence` for correlation and analysis in Elastic SIEM using the MATI API v4.

Log References

- IOCs retrieved using the MATI API v4 over time can be viewed in the `Threat Intelligence` logs.

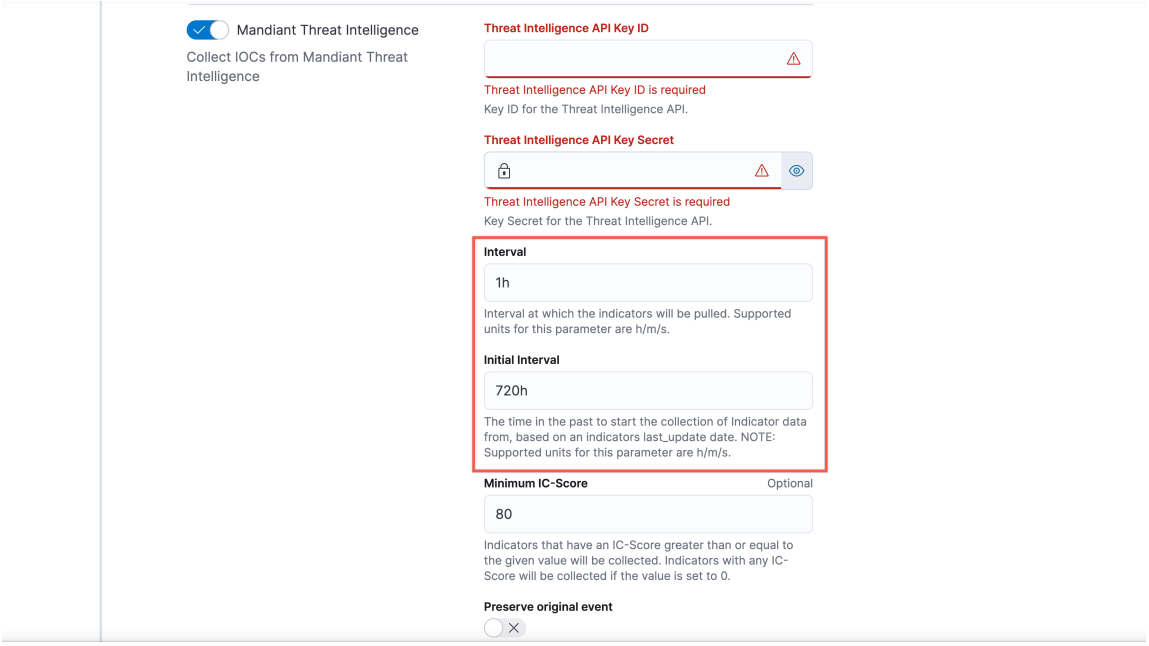
API usage parameters

The integration lets you control the timing of API queries and filter the number of IOCs that are ingested.

> Elastic SIEM does not support manual or ad hoc API calls.

- Update the **Initial interval** to modify the frequency of API calls.
  - The time in the past to start collecting Indicator data from MATI, based on an Indicator's `last_update` date.
  - Supported units for this parameter are hours, minutes, and seconds. The default value is 720 hours (equivalent to 30 days).

    > You may reduce this interval if you don't want as much historical data to be ingested when the integration first runs.



- Update the **Minimum IC-Score** filter to control the number Indicators pulled into Elastic SIEM.
  - Indicators that have an Indicator Confidence Score (IC-Score) greater than or equal to the given value will be collected.

    For more information, see **Understanding IC-Score (https://docs.mandiant.com/home/understanding-ic-score)**.

  - Indicators with any IC-Score will be collected when the value is set to 0.

    To ensure that only high-confidence Indicators are ingested, this value should be set to 80.