Integrate a Microsoft Azure Sentinel Cloud Device

Configure a Microsoft Azure Sentinel cloud SIEM to pull IOCs from the IntSights ETP Suite. The Azure Sentinel connector supports TAXII v2.0.

You must first add the device to the ETP Suite and then configure the device to pull IOCs from the ETP Suite.

When IOCs are pulled to the device, all IOCs are pulled, every time.

IOCs are pulled, together with the following IntSights enrichment data:

- Source name (reporting feed)
- System and user tags
- First seen and last seen
- Severity
- Related threat actors, campaigns, or malware
- Related alert

IOC groups for this device can consist of domains, URLs, IP addresses, file hashes, and email addresses.

Add an Azure Sentinel cloud device

Add a cloud device to the ETP Suite.

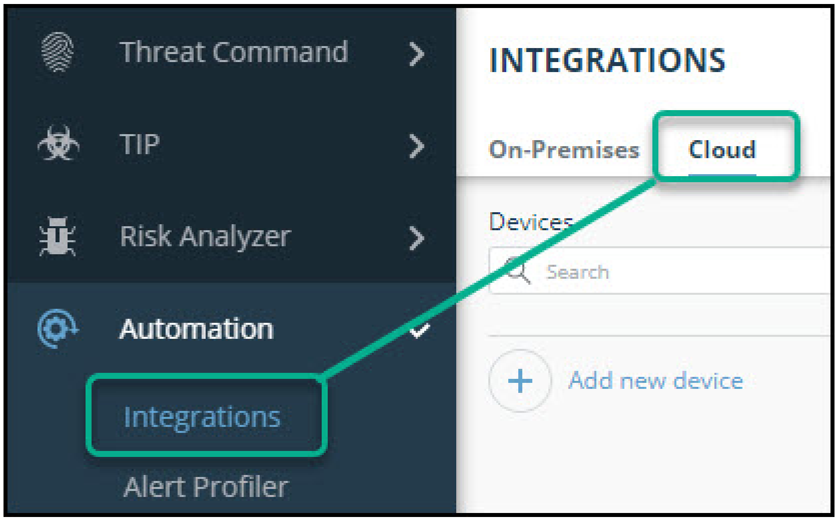
Prerequisites:

- You have the credentials to access the device.
- You have administrative credentials to access the IntSights ETP Suite with a subscription to the Automation and TIP modules.

To add a cloud device to the ETP Suite:

1. Log in to the IntSights ETP Suite at **dashboard.intsights.com**

2. From the main menu, select **Automation -> Integrations**.



3. From the **Integrations** page, click **Cloud**.

4. Click **Add new device**.

5. In the **Add New Cloud Device** dialog, type a user-defined name for the device.
   The name can contain a maximum of 50 letters, spaces, numbers, and underscores.

6. Select the **Device type**.
   The default device IOCs limit is displayed.
7. (Optional) You can change the IOCs limit.
8. Click **Add**.
9. To verify that the new device is added, refresh the **Automation > Integrations** page.

The new device is added to the cloud integrations device list. Next to the device name, there is a red dot, indicating that communication has not yet been established. The dot will change to green when the device is synchronized. If the device cannot synchronize for more than 48 hours, an email warning is sent to the account administrator.

Configure a Microsoft Azure Sentinel cloud device to pull IOCs

After a device has been added, you must enable the pulling of IOCs from the ETP Suite.

Prerequisites:

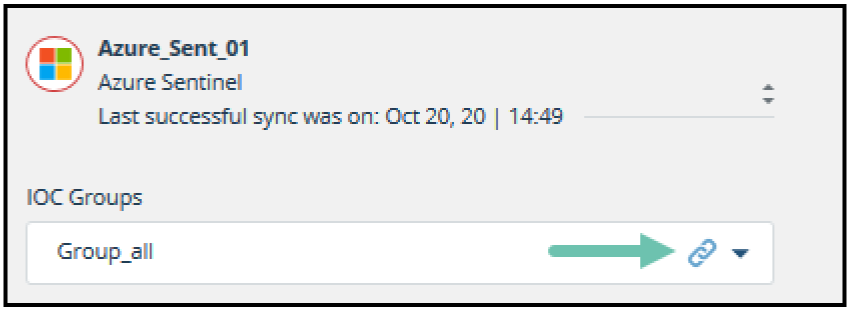
- You have the IntSights ETP Suite account ID and appliance API key. For more information, see API key, account ID, and appliance key.

- You have the device login credentials.
- The device has been integrated in the IntSights virtual appliance (if necessary) and the ETP Suite.

- You have administrative credentials to access the IntSights ETP Suite with a subscription to the Automation and TIP modules.
- An IOC group for this device exists in the IntSights ETP Suite.
  Creating IOC groups is described in Create an IOC group.

To configure an Azure Sentinel cloud device:

1. From the **Microsoft Azure** portal, open **Azure Sentinel**.
2. Select a workspace, then search for **Data connectors**.
   Picture
3. In the **Connector** list, search for **TAXII**, then click **Open connector page**.
   Picture.
4. In the Configuration section, type the following:

Field	**Description**
Friendly name	Type a user-defined name. Imported IOCs will be marked with this name.
API root URL	Copy/paste from the ETP Suite **Device Details** dialog. a. From the ETP Suite, select **Automation > Integrations**. b. From the **Cloud** device list, select the **Azure Sentinel device**. c. On the line of the desired IOC group, click the link symbol.  Azure_Sent_01 Azure Sentinel Last successful sync was on: Oct 20, 20 | 14:49 IOC Groups Group_all d. From the **IOC Group URL** dialog, use the **Copy** button to copy the **API Root URL**. e. Paste that URL in this field.
Collection ID	Copy/paste from the ETP Suite **Device Details** dialog. Follow the same instructions for API Root URL, but copy the **Collection ID**. The Collection ID is different for each IOC group.

Field	Description
Username	Paste the IntSights account ID. For more information, see API key, account ID, and appliance key.
Password	Paste the IntSights API appliance key. For more information, see API key, account ID, and appliance key.

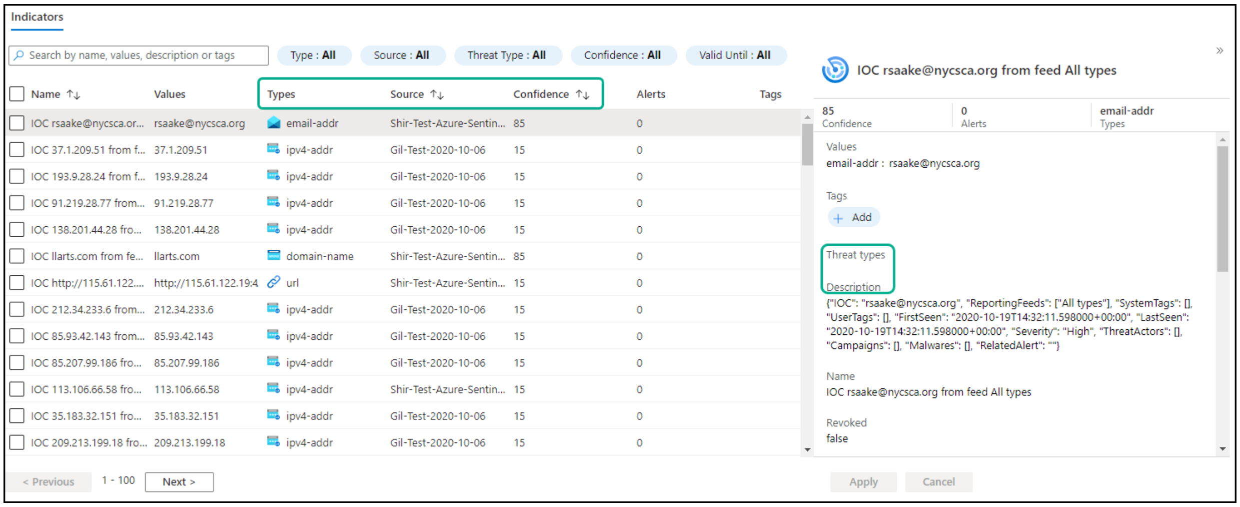
5. Click **Add**.
   The IntSights connector is added to the **Connectors** list.
   Picture

Viewing IOCs in Microsoft Azure Sentinel

You can view IOCs that are pulled in from the ETP Suite in the Azure Sentinel **Threat intelligence** page. This page shows summary data on imported IOCs as well as details per IOC.

To view IOCs:

1. From the **Microsoft Azure** portal, open **Azure Sentinel**.
2. Select a workspace, then search for **Threat intelligence**.
   The **Indicators** area displays a summary of all IOCs. To the right is more details on the selected IOC:



□	Name ↑↓	Values	Types	Source ↑↓	Confidence ↑↓	Alerts	Tags
□	IOC rsaake@nycsca.or...	rsaake@nycsca.org	email-addr	Shir-Test-Azure-Sentin...	85	0	
□	IOC 37.1.209.51 from f...	37.1.209.51	ipv4-addr	Gil-Test-2020-10-06	15	0	
□	IOC 193.9.28.24 from f...	193.9.28.24	ipv4-addr	Gil-Test-2020-10-06	15	0	
□	IOC 91.219.28.77 from...	91.219.28.77	ipv4-addr	Gil-Test-2020-10-06	15	0	
□	IOC 138.201.44.28 fro...	138.201.44.28	ipv4-addr	Gil-Test-2020-10-06	15	0	
□	IOC llarts.com from fe...	llarts.com	domain-name	Shir-Test-Azure-Sentin...	85	0	
□	IOC http://115.61.122....	http://115.61.122.19:4	url	Shir-Test-Azure-Sentin...	15	0	
□	IOC 212.34.233.6 from...	212.34.233.6	ipv4-addr	Gil-Test-2020-10-06	15	0	
□	IOC 85.93.42.143 from...	85.93.42.143	ipv4-addr	Gil-Test-2020-10-06	15	0	
□	IOC 85.207.99.186 fro...	85.207.99.186	ipv4-addr	Gil-Test-2020-10-06	15	0	
□	IOC 113.106.66.58 fro...	113.106.66.58	ipv4-addr	Shir-Test-Azure-Sentin...	15	0	
□	IOC 35.183.32.151 fro...	35.183.32.151	ipv4-addr	Gil-Test-2020-10-06	15	0	
□	IOC 209.213.199.18 fro...	209.213.199.18	ipv4-addr	Gil-Test-2020-10-06	15	0	

IOC rsaake@nycsca.org from feed All types

85	0	email-addr
Confidence	Alerts	Types

Values
email-addr : rsaake@nycsca.org

Tags
+ Add

Threat types

Description
{"IOC": "rsaake@nycsca.org", "ReportingFeeds": ["All types"], "SystemTags": [], "UserTags": [], "FirstSeen": "2020-10-19T14:32:11.598000+00:00", "LastSeen": "2020-10-19T14:32:11.598000+00:00", "Severity": "High", "ThreatActors": [], "Campaigns": [], "Malwares": [], "RelatedAlert": ""}

Name
IOC rsaake@nycsca.org from feed All types

Revoked
false

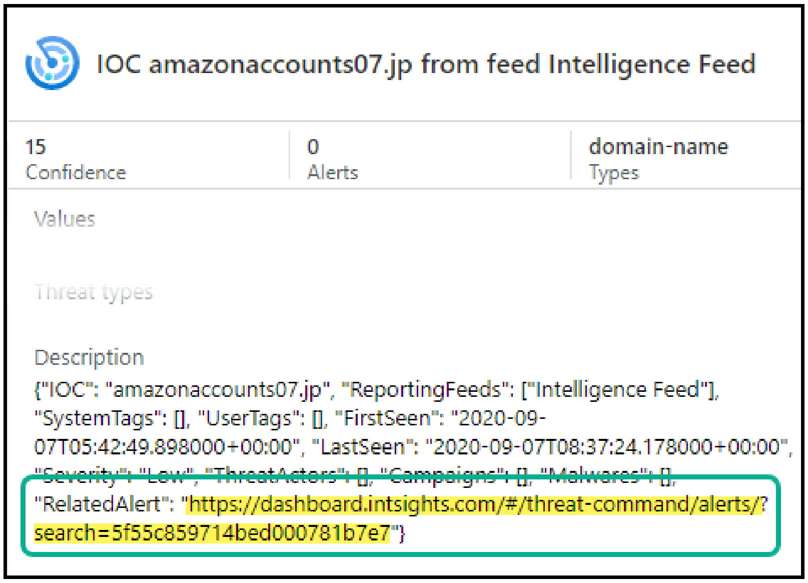
In the summary table, you can see the following data:

- **IOC type**
  IP address, URL, etc.
- **Source**
  The name that was assigned to the Azure connector.
- **Confidence**
  This is mapped from the IntSights severity. IntSights Low = 15, Medium = 50, and High = 85

- **Alerts** and **tags** are not relevant.

In the detail per IOC, you can see additional data:

- **Threat types**
  The IntSights system or user tags, if any.
- **Description**
  The IOC enrichment data. If an IntSights alert was created, you can copy the URL to the ETP Suite to see the alert:



IOC amazonaccounts07.jp from feed Intelligence Feed

15
Confidence

0
Alerts

domain-name
Types

Values

Threat types

Description

```
{"IOC": "amazonaccounts07.jp", "ReportingFeeds": ["Intelligence Feed"],
"SystemTags": [], "UserTags": [], "FirstSeen": "2020-09-
07T05:42:49.898000+00:00", "LastSeen": "2020-09-07T08:37:24.178000+00:00",
"Severity": "Low", "ThreatActors": [], "Campaigns": [], "Malwares": [],
"RelatedAlert": "https://dashboard.intsights.com/#/threat-command/alerts/?
search=5f55c859714bed000781b7e7"}
```

Searching for IOCs in Microsoft Azure Sentinel

You can search for IOCs that match criteria in the name, value, description, or tags. For example:

To search for IOCs:

- In the Indicators search bar, type a term to search for.

IOCs that match the term are displayed.

The **Description** field contains the IOC enrichment data, and you can search for matches in that field, also. This table summarizes some of the more common uses:

To find this	Enter this in the search bar
IOCs of a specific severity	Type the severity (high, medium, or low)
IOCs from a specific IntSights feed	Type the name of the feed (e.g., intelligence feed)

To find this	Enter this in the search bar
IOCs from a specific malware or threat actor	Type the name of the malware or threat actor

Was this helpful? Yes No Send feedback

Previous | Next