Configure AlienVault as an External Threat Feed for ESA

Contents

Introduction

This document describes the steps to configure External Threat Feeds from an AlienVault source and use it within the ESA.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Cisco Secure Email Gateway (SEG / ESA) AsyncOS 16.0.2

- Linux CLI
- Python3 pip
- AlienVault account

Components Used

The information in this document is based on these software and hardware versions:

- Email Security Appliance
- Python3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The External Threat Feeds (ETF) framework enables the email gateway to ingest external threat intelligence shared in STIX format via the TAXII protocol. By leveraging this capability, organizations can:

- Take a proactive stance against cyber threats such as malware, ransomware, phishing, and targeted attacks.
- Subscribe to both local and third-party threat intelligence sources.
- Enhance the overall effectiveness of the email gateway.

What is STIXX/TAXII?

STIX (Structured Threat Information Expression)

STIX is a standardized format used to describe cyber threat intelligence (CTI)—including indicators, tactics, techniques, malware, and threat actors—in a structured and machine-readable way. A STIX feed typically includes indicators—patterns that help detect suspicious or malicious cyber activity.

TAXII (Trusted Automated Exchange of Intelligence Information)

TAXII is a protocol used to exchange STIX data between systems securely and automatically. Defines how cyber threat intelligence is exchanged between systems, products, or organizations through dedicated services (TAXII servers).

Note: AsyncOS 16.0 release supports STIX/TAXII versions: STIX 1.1.1 and 1.2, with TAXII 1.1.

Feed Sources

Email Security Appliances can consume threat intelligence feeds from various sources, including public repositories, commercial providers, and their own private servers within your organization.

To ensure compatibility, all sources must use the STIX/TAXII standards, which enable structured, automated sharing of threat data.

Cabby library

The Cabby Python library is a useful tool for connecting to TAXII servers, discovering STIX collections, and polling threat data. It is a great way to test and validate that a feed source is working correctly and returning data as expected before integrating it into your Email Security Appliance.

Installing Cabby Library

To install the Cabby library, you need to make sure that your local machine have Python pip installed.

Once python pip is installed, you just need to run this command to install the cabby library.

```
 python3 -m pip install cabby
```

Once cabby library installation is finished, you can verify that the *taxii-collections* and *taxii-poll* commands are now available.

```
(cabby) bash-3.2$ taxii-collections -h
usage: taxii-collections [-h] [--host HOST] [--port PORT] [--discovery DISCOVERY] [--path URI] [--https
                         [--cert CERT] [--key KEY] [--key-password KEY_PASSWORD] [--username USERNAME]
                         [--proxy-url PROXY_URL] [--proxy-type {http,https}] [--header HEADERS] [-v] [-
```

```
(cabby) bash-3.2$ taxii-poll -h
usage: taxii-poll [-h] [--host HOST] [--port PORT] [--discovery DISCOVERY] [--path URI] [--https] [--ve
                  [--key KEY] [--key-password KEY_PASSWORD] [--username USERNAME] [--password PASSWORD]
                  [--proxy-type {http,https}] [--header HEADERS] [-v] [-x] [-t {1.0,1.1}] -c COLLECTION
                  [-b BINDINGS] [-s SUBSCRIPTION_ID] [--count-only]
```

AlienVault - Pulses and Feeds

To start discovering AlienVault information, first create an account on the AlienVault site, then start to search for the information you want.

In AlienVault, feeds and pulses are related but not the same:

Pulses

Pulses are curated threat intel with grouped indicators + context (human-readable).

- A Pulse is a collection of threat indicators (IOCs) grouped around a specific threat or campaign.
- Created by the community or providers to describe things like malware, phishing, ransomware.
- Each pulse includes context like threat description, associated indicators (IP, domain, file hash and so on), tags, and references.
- Pulses are human-readable and structured in a way that can be easily understood and shared.

Think of a pulse as a threat report with grouped IOCs and metadata.

Feeds

Feeds are automated stream of indicators from multiple pulses (machine-readable).

- Feeds are a stream of raw indicators (IOCs) pulled from one or more pulses, usually in an automated way.
- They are typically used by security tools to ingest indicators in bulk, via formats like STIX/TAXII, CSV, or JSON.
- Feeds are machine-focused and used for automation and integration with SIEMs, firewalls, and email gateways.

A feed is more about the delivery mechanism, while a pulse is the content and context of the threat.

You usually poll feeds, and those feeds are made up of indicators extracted from pulses.

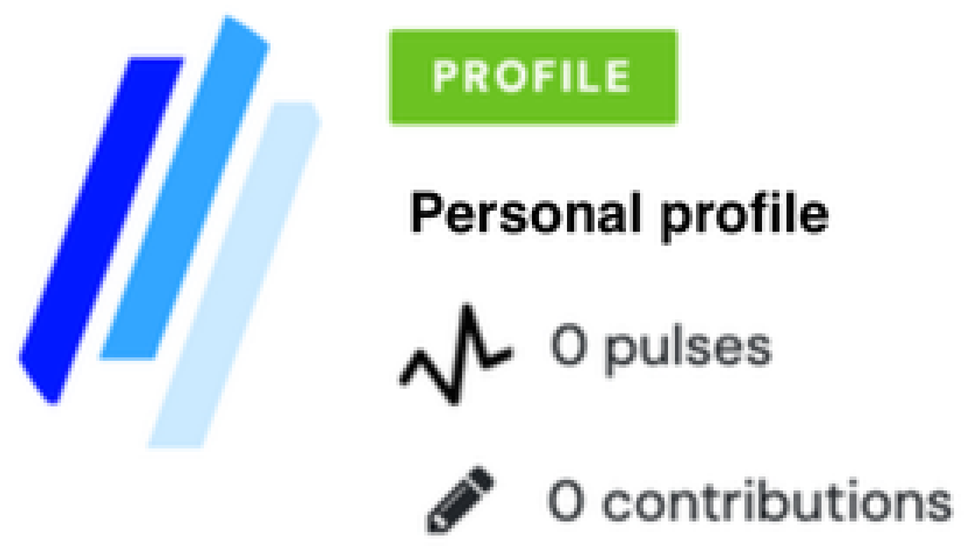
Start Polling Collections

Polling From Own Profile

Once you have your AlienVault account, you can start using the **taxii-collections** and **taxii-poll** commands.

This is how to use these commands for this use case:

In this case, within the AlienVault profile, there are no pulses available, but as a test, you can poll a collection from your profile using the **taxii-poll** command:



PROFILE

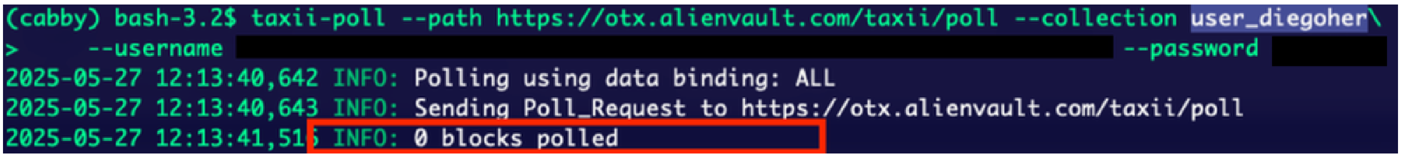
Personal profile

0 pulses

0 contributions

alienvault personal profile

```
taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_<your-alienvault-username> --
```



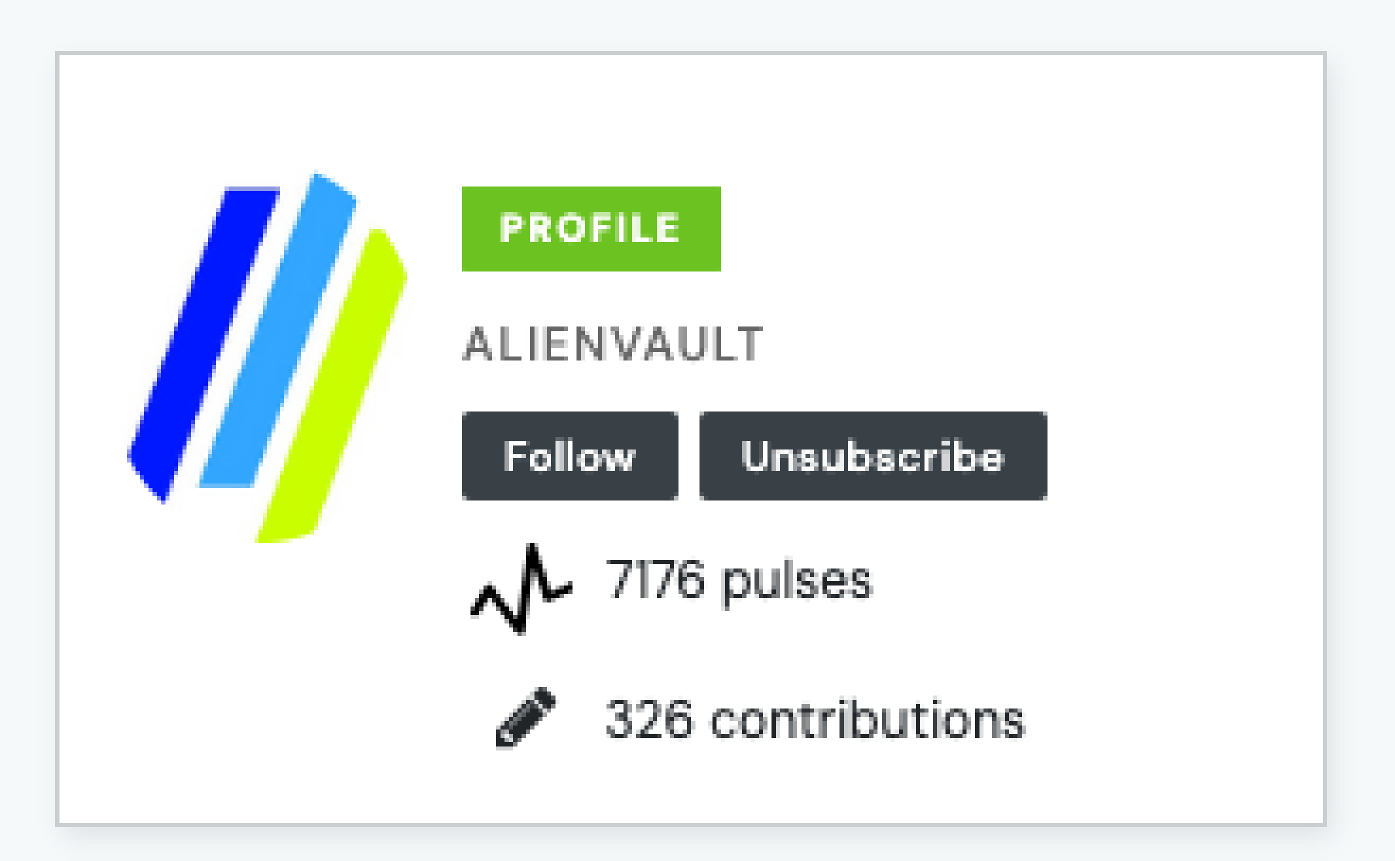
```
(cabby) bash-3.2$ taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_diegoher\
>      --username [redacted]   --password [redacted]
2025-05-27 12:13:40,642 INFO: Polling using data binding: ALL
2025-05-27 12:13:40,643 INFO: Sending Poll_Request to https://otx.alienvault.com/taxii/poll
2025-05-27 12:13:41,515 INFO: 0 blocks polled
```

poll personal profile

As you can see, there are no blocks polled because no information is available within the AlienVault profile.

Polling From AlienVault Profiles

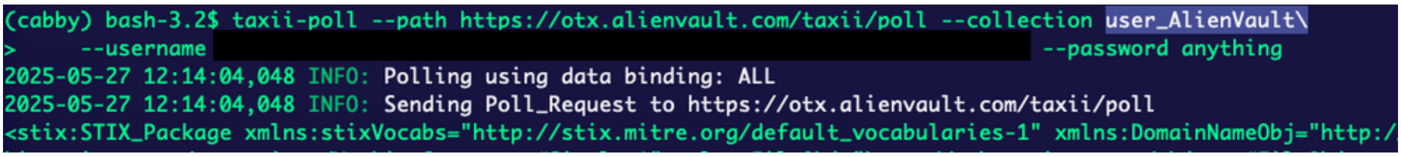
Once profiles inside AlienVault are discovered, some of them have pulses. In this example, the AlienVault profile is used.



alienvault profile

When running the poll with the **taxii-poll** command, it immediately starts fetching all the information from the profile.

```
taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_AlienVault --username abcdefg
```



```
(cabby) bash-3.2$ taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_AlienVault\
>      --username [redacted]   --password anything
2025-05-27 12:14:04,048 INFO: Polling using data binding: ALL
2025-05-27 12:14:04,048 INFO: Sending Poll_Request to https://otx.alienvault.com/taxii/poll
<stix:STIX_Package xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:DomainNameObj="http:/
```

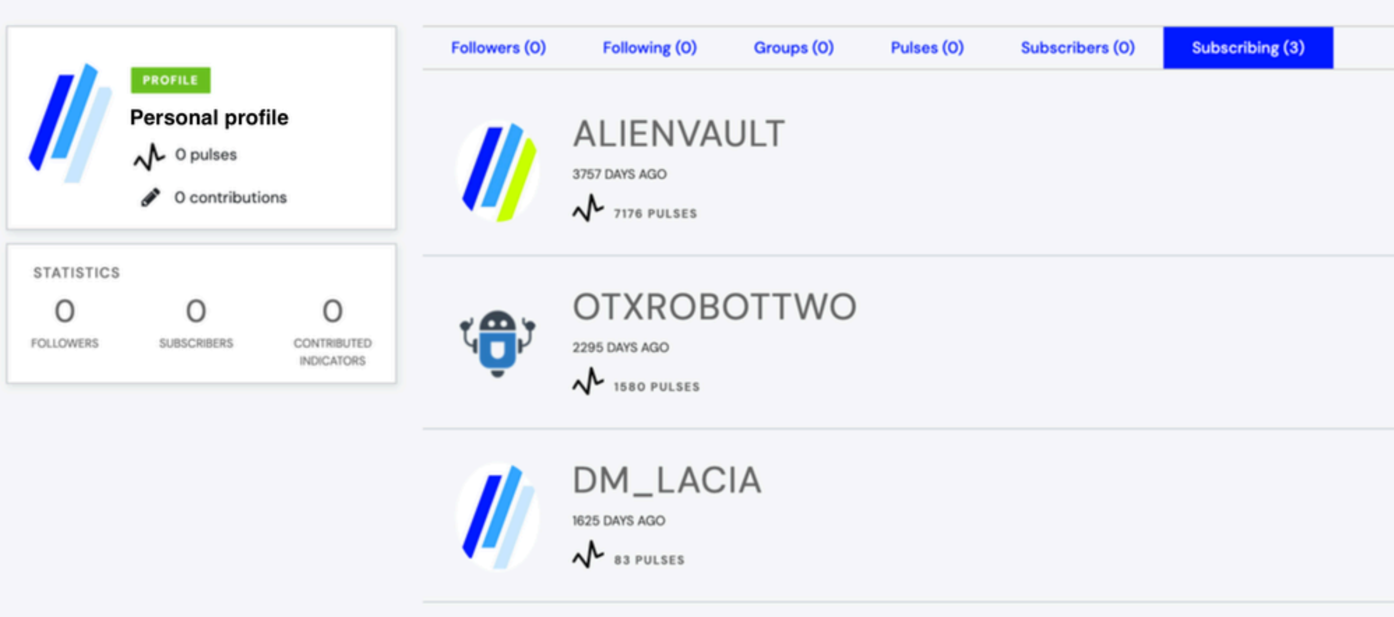
alienvault poll

As shown, the process begins fetching the information.

Note: To know which is your username and password, check this link https://otx.alienvault.com/api

AlienVault Profile Collection Subscriptions

As a test, this user subscribed to 3 profiles.



PROFILE

Personal profile

0 pulses

0 contributions

STATISTICS

0 FOLLOWERS

0 SUBSCRIBERS

0 CONTRIBUTED INDICATORS

ALIENVAULT
3757 DAYS AGO
7176 PULSES

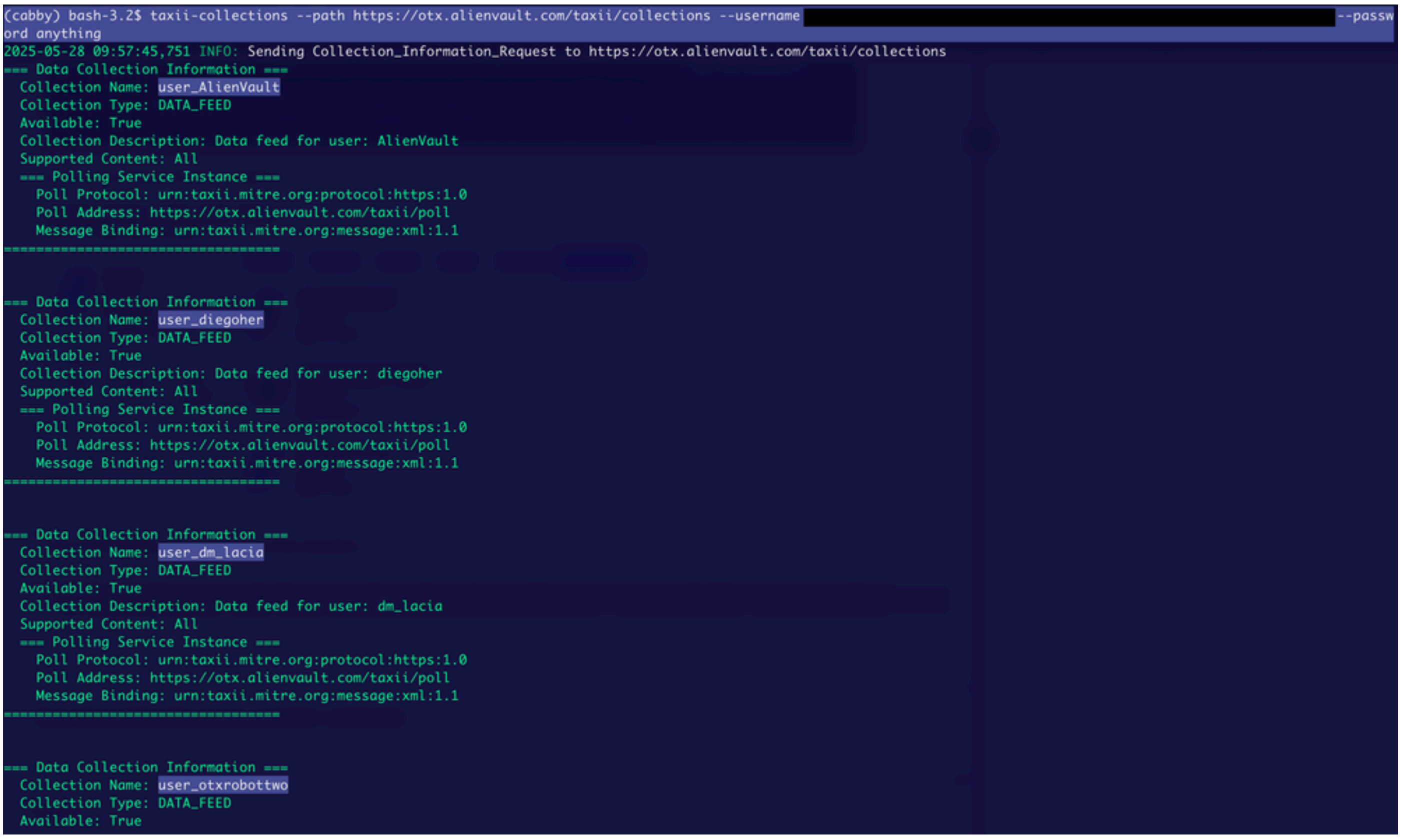
OTXROBOTTWO
2295 DAYS AGO
1580 PULSES

DM_LACIA
1625 DAYS AGO
83 PULSES

personal profile subscriptions

You can use the **taxii-collections** command to fetch those subscriptions.

```
taxii-collections --path https://otx.alienvault.com/taxii/collections --username abcdefg --password ***
```



```
(cabby) bash-3.2$ taxii-collections --path https://otx.alienvault.com/taxii/collections --username [redacted] --passw
ord anything
2025-05-28 09:57:45,751 INFO: Sending Collection_Information_Request to https://otx.alienvault.com/taxii/collections
=== Data Collection Information ===
  Collection Name: user_AlienVault
  Collection Type: DATA_FEED
  Available: True
  Collection Description: Data feed for user: AlienVault
  Supported Content: All
  === Polling Service Instance ===
    Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
    Poll Address: https://otx.alienvault.com/taxii/poll
    Message Binding: urn:taxii.mitre.org:message:xml:1.1
==================================


=== Data Collection Information ===
  Collection Name: user_diegoher
  Collection Type: DATA_FEED
  Available: True
  Collection Description: Data feed for user: diegoher
  Supported Content: All
  === Polling Service Instance ===
    Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
    Poll Address: https://otx.alienvault.com/taxii/poll
    Message Binding: urn:taxii.mitre.org:message:xml:1.1
==================================


=== Data Collection Information ===
  Collection Name: user_dm_lacia
  Collection Type: DATA_FEED
  Available: True
  Collection Description: Data feed for user: dm_lacia
  Supported Content: All
  === Polling Service Instance ===
    Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
    Poll Address: https://otx.alienvault.com/taxii/poll
    Message Binding: urn:taxii.mitre.org:message:xml:1.1
==================================


=== Data Collection Information ===
  Collection Name: user_otxrobottwo
  Collection Type: DATA_FEED
  Available: True
```

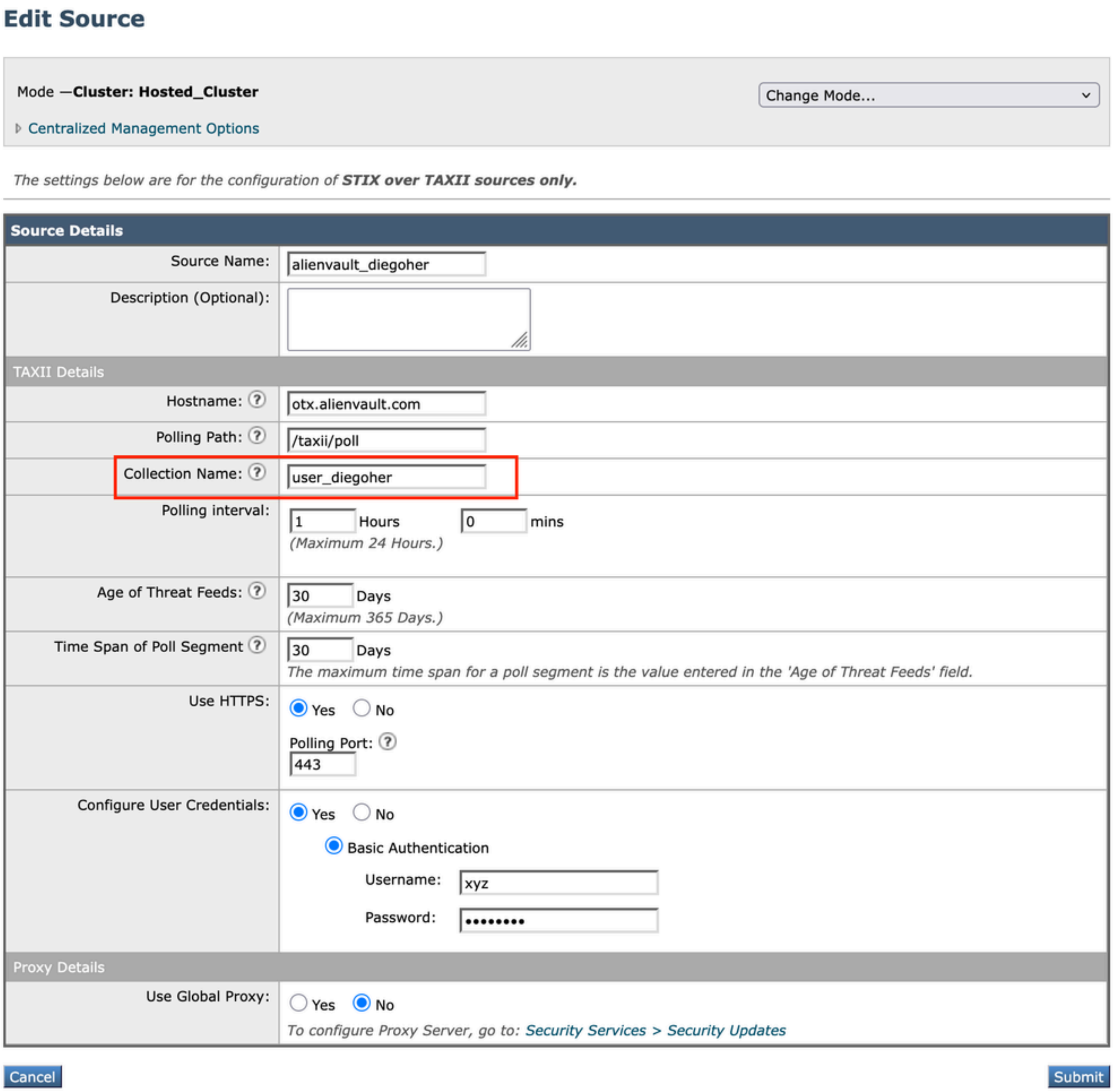
personal profile collections

You can confirm that the taxii-collections command works if the Collection Name is the same as the one you are subscribed to.

Adding Sources to ESA

Adding Source without Feeds

1. Navigate to **Mail Policies** > **External Threat Feeds Manager**.
2. Change to **Cluster Mode**.
3. Click **Add Source**.
4. Hostname: otx.alienvault.com
5. Polling Path: /taxi/poll
6. Collection Name: user_<your_AlienVault_username>
7. Port: 443
8. Configure User Credentials: The one that AlienVault provided to you.
9. Click **Submit** > **Commit Changes**.



Edit Source

Mode —**Cluster: Hosted_Cluster**

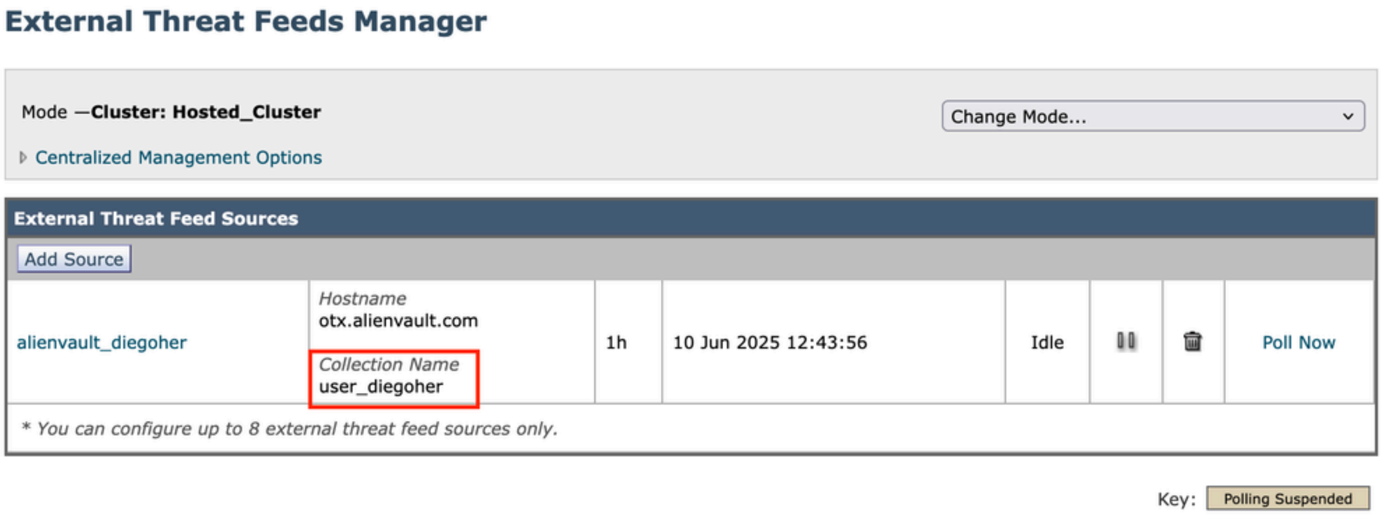
*The settings below are for the configuration of **STIX over TAXII sources only.***

Source Details	
Source Name:	alienvault_diegoher
Description (Optional):	
TAXII Details	
Hostname: ?	otx.alienvault.com
Polling Path: ?	/taxii/poll
Collection Name: ?	user_diegoher
Polling interval:	1 Hours 0 mins *(Maximum 24 Hours.)*
Age of Threat Feeds: ?	30 Days *(Maximum 365 Days.)*
Time Span of Poll Segment ?	30 Days *The maximum time span for a poll segment is the value entered in the 'Age of Threat Feeds' field.*
Use HTTPS:	● Yes ○ No Polling Port: ? 443
Configure User Credentials:	● Yes ○ No ● Basic Authentication Username: xyz Password: ••••••••
Proxy Details	
Use Global Proxy:	○ Yes ● No *To configure Proxy Server, go to: Security Services > Security Updates*

personal source

Polling Source without Feeds

In the External Threat Feeds Manager, after the source is added, the newly added source becomes visible.



External Threat Feeds Manager

Mode —**Cluster: Hosted_Cluster**

Change Mode...

Centralized Management Options

External Threat Feed Sources

Add Source

alienvault_diegoher	*Hostname* otx.alienvault.com *Collection Name* user_diegoher	1h	10 Jun 2025 12:43:56	Idle	⏸	🗑	Poll Now

** You can configure up to 8 external threat feed sources only.*

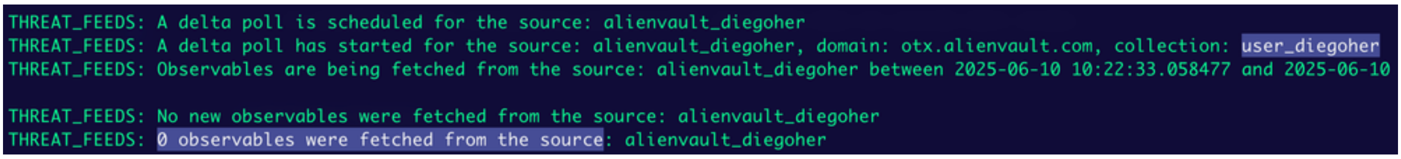
Key: Polling Suspended

personal feed

Once added, click **Poll Now.**

Verify

Log into the ESA via CLI and review the threatfeed logs to verify the information.



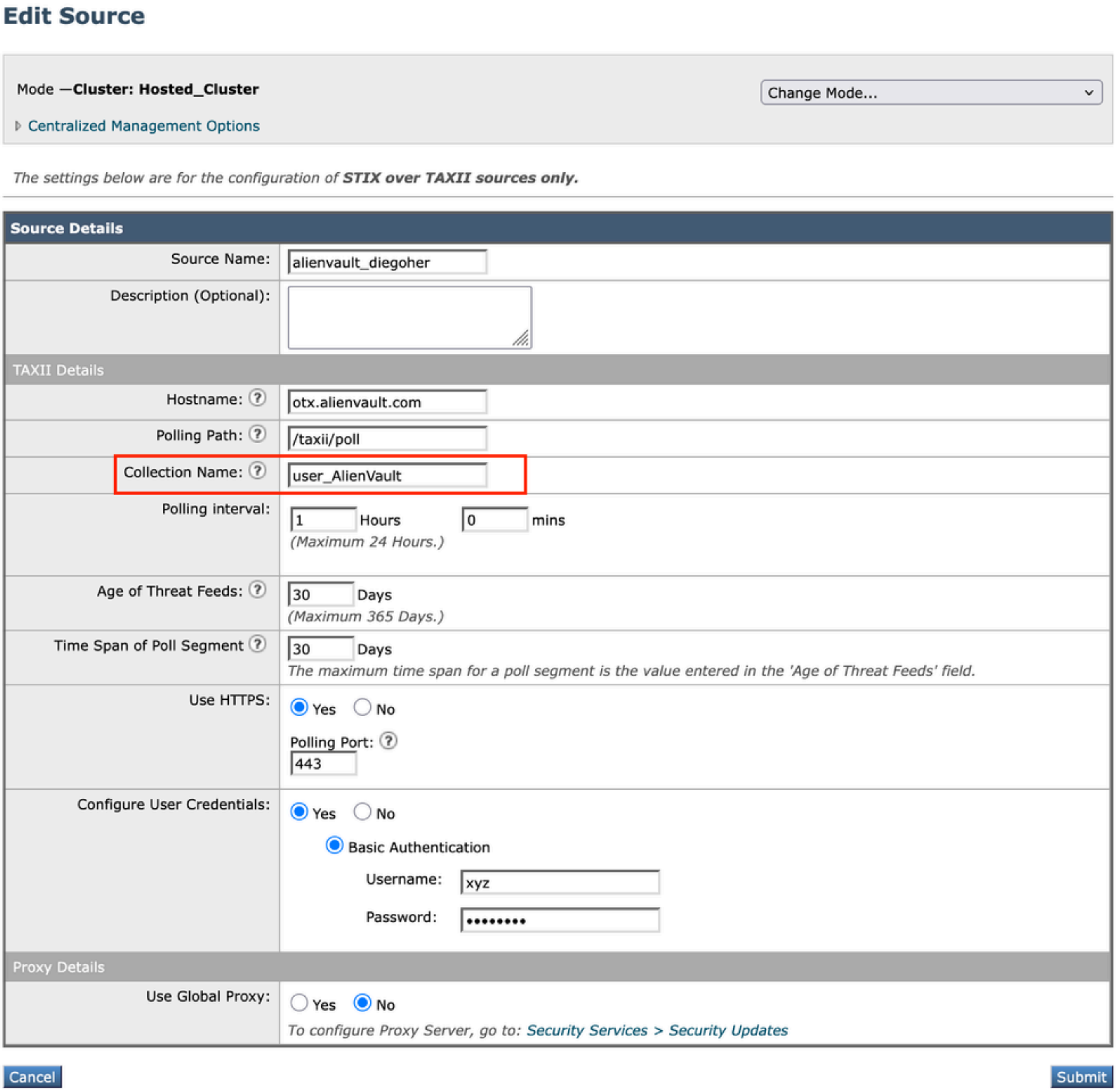
```
THREAT_FEEDS: A delta poll is scheduled for the source: alienvault_diegoher
THREAT_FEEDS: A delta poll has started for the source: alienvault_diegoher, domain: otx.alienvault.com, collection: user_diegoher
THREAT_FEEDS: Observables are being fetched from the source: alienvault_diegoher between 2025-06-10 10:22:33.058477 and 2025-06-10

THREAT_FEEDS: No new observables were fetched from the source: alienvault_diegoher
THREAT_FEEDS: 0 observables were fetched from the source: alienvault_diegoher
```

ETF personal poll

As shown in the image you can see that 0 observables were fetched and this is expected because there are no feeds in the profile shown.

Adding Source with Feeds

1. Navigate to **Mail Policies** > **External Threat Feeds Manager**.
2. Change to **Cluster Mode**.
3. Click **Add Source**.
4. Hostname: otx.alienvault.com
5. Polling Path: /taxi/poll
6. Collection Name: user_AlienVault
7. Port: 443
8. Configure User Credentials: The one that AlienVault provided to you.
9. Click **Submit** > **Commit Changes**.



Edit Source

Mode —**Cluster: Hosted_Cluster**

Change Mode...

Centralized Management Options

The settings below are for the configuration of ***STIX over TAXII sources only.***

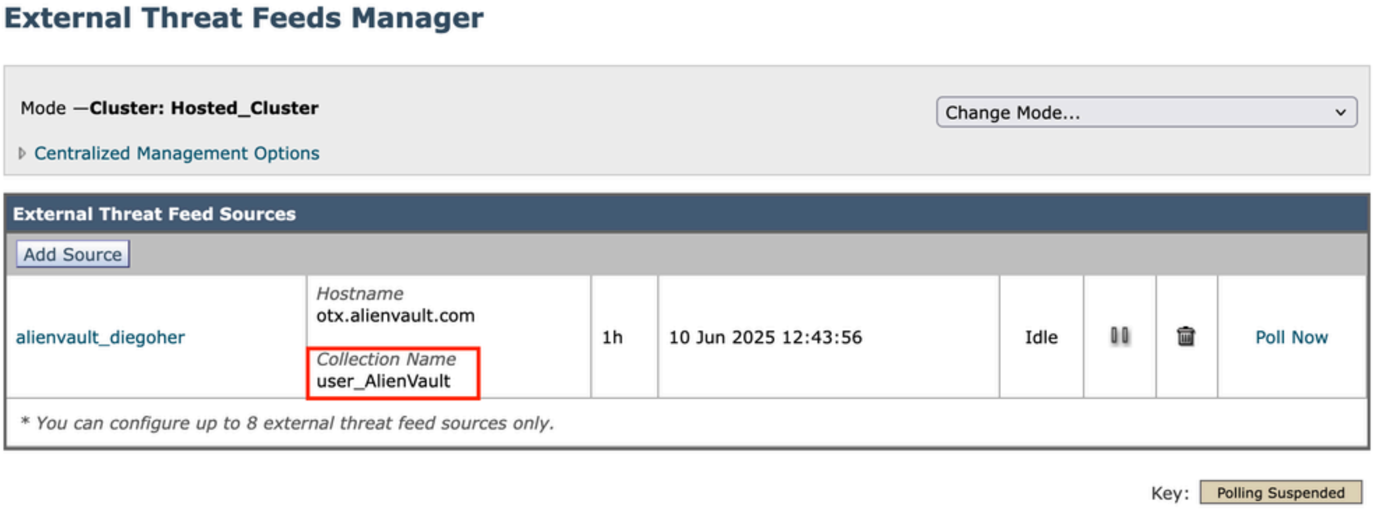
Source Details

Source Name:	alienvault_diegoher
Description (Optional):	
TAXII Details	
Hostname: ?	otx.alienvault.com
Polling Path: ?	/taxii/poll
Collection Name: ?	user_AlienVault
Polling interval:	1 Hours 0 mins *(Maximum 24 Hours.)*
Age of Threat Feeds: ?	30 Days *(Maximum 365 Days.)*
Time Span of Poll Segment ?	30 Days *The maximum time span for a poll segment is the value entered in the 'Age of Threat Feeds' field.*
Use HTTPS:	● Yes ○ No Polling Port: ? 443
Configure User Credentials:	● Yes ○ No ● Basic Authentication Username: xyz Password: ••••••••
Proxy Details	
Use Global Proxy:	○ Yes ● No *To configure Proxy Server, go to: Security Services > Security Updates*

alienvault source

Polling Source with Feeds

In the External Threat Feeds Manager, after the source is added, the newly added source becomes visible.



External Threat Feeds Manager

Mode —**Cluster: Hosted_Cluster**

Change Mode...

Centralized Management Options

External Threat Feed Sources

Add Source

alienvault_diegoher	*Hostname* otx.alienvault.com *Collection Name* user_AlienVault	1h	10 Jun 2025 12:43:56	Idle	⏸	🗑	Poll Now

* *You can configure up to 8 external threat feed sources only.*

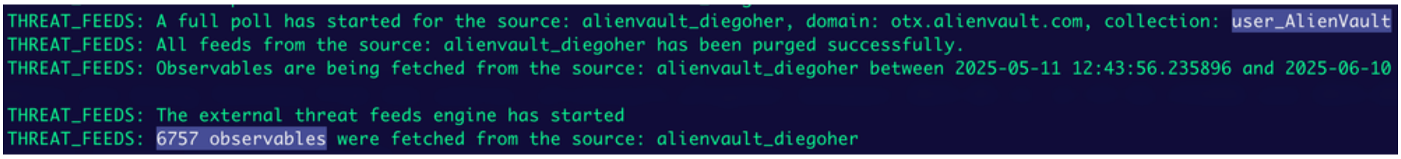
Key: Polling Suspended

alienvault feed

Once added, click Poll Now.

Verify

Log into the ESA via CLI and review the threatfeed logs to verify the information.



```
THREAT_FEEDS: A full poll has started for the source: alienvault_diegoher, domain: otx.alienvault.com, collection: user_AlienVault
THREAT_FEEDS: All feeds from the source: alienvault_diegoher has been purged successfully.
THREAT_FEEDS: Observables are being fetched from the source: alienvault_diegoher between 2025-05-11 12:43:56.235896 and 2025-06-10

THREAT_FEEDS: The external threat feeds engine has started
THREAT_FEEDS: 6757 observables were fetched from the source: alienvault_diegoher
```

polling alienvault feed

As shown in the image, you can see that several observables were fetched.

Note: If new feeds are added to the configured collection, the ESA automatically polls the source, and the new observables are fetched.