STIX-TAXII Connector for Cisco Umbrella and Secure Access

Installation & Configuration Guide (Ubuntu)

Version 1.0

A black background with white text

AI-generated content may be incorrect.

Table of Contents

[Prerequisites 3](#_Toc199714032)

[Recommended Minimum Hardware Specifications 3](#_Toc199714033)

[Step-by-Step Installation Guide 4](#_Toc199714034)

[1. Connect to the Ubuntu Server 4](#_Toc199714035)

[2. Switch to Root User 4](#_Toc199714036)

[3. Navigate to Working Directory 4](#_Toc199714037)

[4. Download the Python Connector Script 4](#_Toc199714038)

[5. Download the Installation Script 4](#_Toc199714039)

[6. Make the Scripts Executable 4](#_Toc199714040)

[7. Run the Installation Script 4](#_Toc199714041)

[8. Configure the configuration.cfg File 5](#_Toc199714042)

[9. Verify the Cron Job Is Active 6](#_Toc199714043)

[10. Manually Run the Connector for Verification 6](#_Toc199714044)

[11. Validate in Cisco Umbrella 7](#_Toc199714045)

[Summary 7](#_Toc199714046)

[Configuration File Guide: configuration.cfg 8](#_Toc199714047)

[File Structure Overview 8](#_Toc199714048)

[Section 1: [api\_umbrella] 8](#_Toc199714049)

[Section 2: [umbrella\_org1] 9](#_Toc199714050)

[Section 3: [otx] (or any TAXII server) 10](#_Toc199714051)

[Section 4: [namespace] 10](#_Toc199714052)

[Where to Place the File 11](#_Toc199714053)

[Validation Tips 11](#_Toc199714054)

[Tips 11](#_Toc199714055)

[Change History 12](#_Toc199714056)

[Copyright Information 13](#_Toc199714057)

This guide explains how to set up the STIX-TAXII Connector on a target Ubuntu machine. The connector pulls threat intelligence data from a TAXII server (like AlienVault OTX) and pushes observables (domains, IPs, URLs) into Cisco Umbrella or Secure Access destination lists.

# Prerequisites

* Ubuntu 20.04 or later
* Internet access on the server
* Cisco Umbrella API credentials
* TAXII server credentials

## Recommended Minimum Hardware Specifications

For a small to medium-scale deployment (e.g. polling 10–20 collections once every 60 minutes):

| **Resource** | **Recommended** | **Notes** |
| --- | --- | --- |
| **CPU** | 2 vCPU | Basic Python processing, no heavy computation |
| **RAM** | 2-4 GB | Python + libraries (lxml, requests, etc.) |
| **Disk** | 5-10 GB | Mainly for logs and Python environment |
| **Network** | Stable internet connection | Needed for TAXII polling and Umbrella API pushes |
| **OS** | Ubuntu Server 20.04+ | Python 3.8+ is required |

# Step-by-Step Installation Guide

## 1. Connect to the Ubuntu Server

Log into your Ubuntu machine via SSH or terminal:

# ssh user@your-server-ip

## 2. Switch to Root User

We need root privileges to install dependencies and schedule cron jobs.

# sudo su

## 3. Navigate to Working Directory

All files will be placed under /usr/local/bin:

# cd /usr/local/bin

## 4. Download the Python Connector Script

# curl -O https://raw.githubusercontent.com/pfiano/stix-taxii-connector/refs/heads/main/stix-taxii-connector-v1.0.py

## 5. Download the Installation Script

# curl -O https://raw.githubusercontent.com/pfiano/stix-taxii-connector/refs/heads/main/install\_stix\_taxii\_connector.sh

## 6. Make the Scripts Executable

# chmod +x install\_stix\_taxii\_connector.sh stix-taxii-connector-v1.0.py

## 7. Run the Installation Script

The install\_stix\_taxii\_connector.sh script will:

* Install Python 3.8 and dependencies
* Create a virtual environment
* Install Python packages (certifi, lxml, cabby, requests)
* Create a base configuration file
* Schedule the connector to run every minute via cron

Run the installation script:

# ./install\_stix\_taxii\_connector.sh

When complete, you should see:

✅ Installation complete. The connector will run every minute via cron.

## 8. Configure the configuration.cfg File

The configuration file is located at:

# /usr/local/bin/configuration.cfg

Edit it with:

# nano /usr/local/bin/configuration.cfg

Replace all TBA (To Be Added) values with your actual credentials:

[umbrella\_org1]

key = YOUR\_UMBRELLA\_API\_KEY

secret = YOUR\_UMBRELLA\_SECRET

org\_id = YOUR\_ORG\_ID

destination\_list\_name = THREAT\_LIST\_NAME

[otx]

username = YOUR\_USERNAME

password = YOUR\_PASSWORD

host = TAXII\_SERVER

use\_https = true/false

discovery\_path = DISCOVERY\_PATH

poll\_days = POLL\_DAYS

[namespace]

stix = http://stix.mitre.org/stix-1

cybox = http://cybox.mitre.org/cybox-2

URIObj = http://cybox.mitre.org/objects#URIObject-2

DomainNameObj = http://cybox.mitre.org/objects#DomainNameObject-1

AddressObj = http://cybox.mitre.org/objects#AddressObject-2

Save and close the configuration.cfg file (CTRL+O, ENTER, CTRL+X in nano).

## 9. Verify the Cron Job Is Active

Check your crontab with:

# crontab -l

You should see:

0 \* \* \* \* /usr/bin/env bash -c 'source /usr/local/bin/myenv/bin/activate && /usr/local/bin/myenv/bin/python /usr/local/bin/stix-taxii-connector-v1.0.py >> /var/log/stix\_taxii\_connector.log 2>&1'

This confirms the connector is scheduled to run every hour.

Log will eb saved in /var/log/stix\_taxii\_connector.log.

## 10. Manually Run the Connector for Verification

You can manually trigger the connector to ensure it runs properly:

/usr/bin/env bash -c 'source /usr/local/bin/myenv/bin/activate && /usr/local/bin/myenv/bin/python /usr/local/bin/stix-taxii-connector-v1.0.py'

If the setup is correct, you should see output like:

📥 Polling OTX collection: user\_AlienVault

🚀 Pushing 74 destinations to all configured Umbrella orgs...

🔐 Connecting to Umbrella Org 2502376 (umbrella\_org1)...

✅ Successfully added 74 destinations

If you see a KeyError or missing config values, check the contents of configuration.cfg file.

## 11. Validate in Cisco Umbrella

* Log into your Cisco Umbrella or Secure Access Dashboard
* Navigate to: **Policies** > **Destination Lists**
* Open the list you configured in **destination\_list\_name**
* Confirm that observables have been added (IPs, domains, URLs)

# Summary

| Step | Action |
| --- | --- |
| 1 | SSH into Ubuntu |
| 2 | Become root (sudo su) |
| 3 | Go to /usr/local/bin |
| 4 | Download Python script |
| 5 | Download installer |
| 6 | Make scripts executable |
| 7 | Run installer |
| 8 | Edit config file |
| 9 | Verify cron job |
| 10 | Run script manually |
| 11 | Check Umbrella dashboard |

# Configuration File Guide: configuration.cfg

The configuration.cfg file contains the settings needed by the connector to authenticate with:

1. Cisco Umbrella or Secure Access (to update Destination Lists)
2. A TAXII/STIX source (like AlienVault OTX)
3. STIX Namespaces for parsing threat intelligence data

## File Structure Overview

[api\_umbrella]

auth\_url = https://api.umbrella.com/auth/v2/token

list\_url = https://api.umbrella.com/policies/v2/destinationlists

push\_url\_template = https://api.umbrella.com/policies/v2/destinationlists/{destination\_list\_id}/destinations

[umbrella\_org1]

key = TBA

secret = TBA

org\_id = TBA

destination\_list\_name = TBA

[otx]

username = TBA

password = TBA

host = TBA

use\_https = false

discovery\_path = TBA

[namespace]

stix = http://stix.mitre.org/stix-1

cybox = http://cybox.mitre.org/cybox-2

URIObj = http://cybox.mitre.org/objects#URIObject-2

DomainNameObj = http://cybox.mitre.org/objects#DomainNameObject-1

AddressObj = http://cybox.mitre.org/objects#AddressObject-2

## **Section 1:** [api\_umbrella]

This section must remain untouched in case of Umbrella:

[api\_umbrella]

auth\_url = <https://api.umbrella.com/auth/v2/token>

list\_url = <https://api.umbrella.com/policies/v2/destinationlists>

push\_url\_template = [https://api.umbrella.com/policies/v2/destinationlists/{destination\_list\_id}/destinations](https://api.umbrella.com/policies/v2/destinationlists/%7bdestination_list_id%7d/destinations)

This section must be amended in case of Secure Access (please do not change the [api\_umbrella] key (just replace umbrella with sse):

[api\_umbrella]

auth\_url = <https://api.sse.com/auth/v2/token>

list\_url = [https://api.sse.com/policies/v2/destinationlists](https://api.umbrella.com/policies/v2/destinationlists)

push\_url\_template = [https://api.sse.com/policies/v2/destinationlists/{destination\_list\_id}/destinations](https://api.sse.com/policies/v2/destinationlists/%7bdestination_list_id%7d/destinations)

## **Section 2:** [umbrella\_org1]

This section defines the **Umbrella organization** you are updating with threat intelligence.

| **Key** | **Description** |
| --- | --- |
| key | Your **Cisco Umbrella API key** (from the API Key Generator in Umbrella) |
| secret | The **secret** tied to the above key |
| org\_id | Your **Umbrella organization ID** (numeric) |
| destination\_list\_name | The **name** of the destination list where observables (e.g. IPs, domains) will be pushed |

You can add **multiple organizations** by duplicating this block with different section names like [umbrella\_org2], [umbrella\_customerX], etc. as long as you keep the prefix “umbrella\_”

**Example:**

[umbrella\_org1]

key = abcd1234efgh5678

secret = s3cr3tK3yXyZ!

org\_id = 2502376

destination\_list\_name = threat\_intel\_auto

[umbrella\_org2]

key = cd14574efgh5678sd

secret = 453cr3tK3sdkahfjak

org\_id = 2404676

destination\_list\_name = threat\_intel\_MISP

[umbrella\_org3]

key = 145jfkgd74efghd3378sd

secret = cr3tK3sdka8347hfjak

org\_id = 2104576

destination\_list\_name = threat\_intel\_update

## **Section 3:** [otx] (or any TAXII server)

This section defines how to **connect to your TAXII server** (e.g., AlienVault OTX).

| **Key** | **Description** |
| --- | --- |
| username | TAXII authentication username (or API key if applicable) |
| password | Password for above user |
| host | TAXII server host name or IP (e.g. otx.alienvault.com) |
| use\_https | true or false – whether to connect over HTTPS |
| discovery\_path | Relative path to the server’s discovery endpoint (e.g. /taxii/discovery) |

If using **OTX TAXII 1.1**, you may need to register and generate TAXII credentials.

**Example:**

[otx]

username = mytaxiiuser

password = mytaxiipassword

host = otx.alienvault.com

use\_https = true

discovery\_path = /taxii/discovery

## **Section 4:** [namespace]

This section is used to define **STIX/Cybox XML namespaces**, required for parsing structured threat intelligence. You usually don’t need to modify these unless you're using custom STIX formats.

**Example (default values):**

stix = http://stix.mitre.org/stix-1

cybox = http://cybox.mitre.org/cybox-2

URIObj = http://cybox.mitre.org/objects#URIObject-2

DomainNameObj = http://cybox.mitre.org/objects#DomainNameObject-1

AddressObj = http://cybox.mitre.org/objects#AddressObject-2

## Where to Place the File

The configuration.cfg file should be placed in the **same directory** as the script stix-taxii-connector-v1.0.py:

/usr/local/bin/configuration.cfg

## Validation Tips

1. Make sure there are **no extra spaces** or invisible characters.
2. Confirm the key, secret, and org\_id are correct and active in Umbrella.
3. Try a **manual run**:

source /usr/local/bin/myenv/bin/activate

python /usr/local/bin/stix-taxii-connector-v1.0.py

If the config is correct, you should see:

📥 Polling OTX collection: user\_AlienVault

🚀 Pushing 74 destinations to all configured Umbrella orgs...

✅ Successfully added 74 destinations

## Tips

* Always **test manually** before relying on cron execution.
* Keep **backup copies** of the config file when modifying it.
* If using version control, **exclude** this file (contains secrets).

# Change History

|  |  |  |
| --- | --- | --- |
| **Document Version** | **Published Date** | **Description** |
| 1.0 | 02/06/2025 | Initial version |

# Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)