

# ةياهن طاقن ىلע لزعلا فاقيإ/عدب ةتمتأ ةدعتم

## تاي وتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملما](#)

[ةيساسأتامولعم](#)

[ةلكشملا](#)

[لحلا](#)

[صين](#)

[تاميلعات](#)

[ةحصلات قرحتلما](#)

## ةمدقملا

ةدعتم ئياهن طاقن ىلע عدبلا/فاقيإ لزع ةيلمع ةتمتأ ئيفيك دنتسملا اذه فصي نم ئنمآل ئياهنلا ةطقنل (API) تاقيب طتلما ةجمرب ةهجاو مادختساب Cisco.

## ةيساسألا تابلطتملا

### تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت:

- نم ئنمآل ئياهن ةطقن Cisco
- نم ئنمآل ئياهنلا ةطقن مكحهت ةدحو Cisco
- Cisco Secure Endpoint API تاقيب طت ةجمرب ةهجاو
- نوثياب

### ةمدختسملا تانوكملما

ةيلاتلا جماربلأا تارادصإ لىإ دنتسملا اذه يف ةدراولأا تامولعملا دنتسست:

- Cisco Secure Endpoint 8.4.0.30201
- نوثياب ةئياب ةفاضتسال ئياهنلا ةطقن
- Python 3.11.7

ةصالخ ةيلمعم ةئياب يف ةدوچوملا ةزهجلأا نم دنتسملا اذه يف ةدراولأا تامولعملا عاشنام مت تناك اذا. (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجلأا عيمج تأدبو رمأ يأ لمحتملا ريثأتلل كمهف نم دكأتف ،ليغشتلما ديق كتكبش.

## ةياساس أ تامولع

- لزعلا عدبلا بـPUT مدخلتست.
- لزعلا فاقـيـالـ بـDELETE مـادـخـتـسـاـ متـيـ.
- تـامـوـلـعـلاـ نـمـ دـيـزـمـ ىـلـعـ لـوـصـحـلـلـ [تـاقـيـبـ طـتـلـاـ](#) قـجـمـرـبـ قـهـجـأـوـقـئـاثـوـ عـجـارـ.

## ةـلـكـشـمـلـاـ

ةـرمـ لـكـ يـفـ دـحـ اوـ زـاهـجـ ىـلـعـ فـاقـيـإـلـاـ/عـدـبـلـاـ لـزـعـ ةـيـنـاـكـمـ Ciscoـ نـمـ ةـنـمـآـلـاـ ةـيـاهـنـلـاـ ةـطـقـنـ حـيـتـتـ  
ةـيـاهـنـ طـاـقـنـ ىـلـعـ تـايـلـمـعـلـاـ هـذـهـ عـارـجـ!ـ يـرـوـرـضـلـاـ نـمـ نـوـكـيـ اـمـ ةـدـاعـ،ـ ةـيـنـمـآـلـاـ ثـداـوـحـلـاـ لـلـاخـ،ـ كـلـذـعـمـ وـ  
ةـتـمـتـأـ دـعـاسـتـ نـأـ نـكـمـيـوـ.ـ لـاعـفـ لـكـشـبـ ةـلـمـتـحـمـلـاـ تـادـيـدـهـتـلـاـ عـاوـتـحـاـلـ تـقـوـلـاـ سـفـنـ يـفـ ةـدـدـعـتـمـ  
ةـجـمـرـبـ قـهـجـأـوـ مـادـخـتـسـاـبـ ةـرـيـبـكـلـاـ ةـيـاهـنـلـاـ طـاـقـنـلـ لـيـغـشـتـلـاـ فـاقـيـإـاـ/عـدـبـ ةـصـاخـلـاـ لـزـعـلـاـ ةـيـلـمـعـ  
لـيـلـقـتـ نـعـ الـضـفـ،ـ رـيـبـكـ لـكـشـبـ ثـداـوـحـلـلـ ةـبـاجـتـسـاـلـاـ ةـعـافـكـ نـيـسـحـتـ ىـلـعـ (API)ـ تـاقـيـبـ طـتـلـاـ  
ةـكـبـشـلـاـ اـهـلـ ضـرـعـتـتـ يـتـلـاـ ةـيـلـكـلـاـ رـطـاـخـمـلـاـ.

## لحـلـاـ

- ىـلـعـ لـزـعـلـاـ ءـاهـنـاـ/عـدـبـلـاـ ةـلـاـقـمـلـاـ هـذـهـ يـفـ رـفـوـتـمـلـاـ يـصـنـلـاـ جـمـانـرـبـ مـادـخـتـسـاـ نـكـمـيـ
- ةـيـاهـنـلـاـ ةـطـقـنـلـ APIـ دـامـتـعـاـ تـانـاـيـبـ مـادـخـتـسـاـبـ كـتـسـسـفـمـ يـفـ ةـدـدـعـتـمـ ةـيـاهـنـ طـاـقـنـ  
ةـنـمـآـلـاـ.
- **لوـصـحـلـلـ Cisco AMP**ـ ىـلـعـ قـمـاـعـ قـرـظـنـ ىـلـاـ عـوـجـرـلـاـ يـجـرـيـ،ـ APIـAMPـ دـامـتـعـاـ تـانـاـيـبـ عـاشـنـإـلـ  
[ةـيـاهـنـلـاـ طـاـقـنـ تـاقـيـبـ طـتـلـاـ](#)ـ قـجـمـرـبـ قـهـجـأـوـ ىـلـعـ
- ةـيـاهـنـلـاـ طـاـقـنـ Pythononـ تـيـبـثـتـ ىـلـاـ جـاتـحـتـ،ـ رـفـوـتـمـلـاـ يـصـنـلـاـ جـمـانـرـبـلـاـ مـادـخـتـسـاـلـ  
كـبـ ةـصـاخـلـاـ.
- تـابـلـ طـلـلـ ةـيـطـمـنـلـاـ ةـدـحـوـلـاـ تـيـبـثـتـ يـجـرـيـ،ـ pythonـ تـيـبـثـتـ دـعـبـ

```
pip install requests
```



حیضوت ھب دصقیو طقف ۋە يىچيپوت ضارغألى يىصنللا جمانربلا رېفوت مەتى: رېذحت  
ال (API). تاقييىب طتللا ۋە جمرب ۋە جاڭ او مادختساب ۋە اهنىلا ۋە طقىن لىزىم ۋە تىممۇت ۋە يىفيك  
جمانربلا ادە ئاطخا فاش كىتسا يىف Cisco نم (TAC) ۋە يىن قىتللا ۋە دعاسىملا زىركەم كىراشى  
ۋە قىدب يىصنللا جمانربلا رابتىخا ورۇچىلا يىخوت نىمىدىختىسىملا يىلۇ بەجى. اەحالىسى او يىصنللا  
جاتىندا دادعا يىف ھەرشن لېبىق ۋە نەمآ ۋە يىب يىف.

## صن

يىف ۋە دىدەتمەن ۋە اهنى طاقىن يىلۇ لىزىلە عىدبىل رفوتىمىلا يىذىفەن تىلا صنللا مادختىسى كەنگەمىي  
كەتكەرش:

```
import requests

def read_config(file_path):
    """
    Reads the configuration file to get the API base URL, client ID, and API key.
    """
    # Your code here to read the config file and return the required values
```

```

config = {}
try:
    with open(file_path, 'r') as file:
        for line in file:
            # Split each line into key and value based on '='
            key, value = line.strip().split('=')
            config[key] = value
except FileNotFoundError:
    print(f"Error: Configuration file '{file_path}' not found.")
    exit(1) # Exit the script if the file is not found
except ValueError:
    print(f"Error: Configuration file '{file_path}' is incorrectly formatted.")
    exit(1) # Exit the script if the file format is invalid
return config

def read_guids(file_path):
    """
    Reads the file containing GUIDs for endpoints to be isolated.
    """
    try:
        with open(file_path, 'r') as file:
            # Read each line, strip whitespace, and ignore empty lines
            return [line.strip() for line in file if line.strip()]
    except FileNotFoundError:
        print(f"Error: GUIDs file '{file_path}' not found.")
        exit(1) # Exit the script if the file is not found
    except Exception as e:
        print(f"Error: An unexpected error occurred while reading the GUIDs file: {e}")
        exit(1) # Exit the script if an unexpected error occurs

def isolate_endpoint(base_url, client_id, api_key, connector_guid):
    """
    Sends a PUT request to isolate an endpoint identified by the connector GUID.
    Args:
        base_url (str): The base URL for the API.
        client_id (str): The API client ID for authentication.
        api_key (str): The API key for authentication.
        connector_guid (str): The GUID of the connector to be isolated.
    """
    url = f"{base_url}/{connector_guid}/isolation"
    try:
        # Send PUT request with authentication
        response = requests.put(url, auth=(client_id, api_key))
        response.raise_for_status() # Raise an HTTPError for bad responses (4xx and 5xx)

        if response.status_code == 200:
            print(f"Successfully isolated endpoint: {connector_guid}")
        else:
            print(f"Failed to isolate endpoint: {connector_guid}. Status Code: {response.status_code}")
    except requests.RequestException as e:
        print(f"Error: An error occurred while isolating the endpoint '{connector_guid}': {e}")

if __name__ == "__main__":
    # Read configuration values from the config file
    config = read_config('config.txt')

    # Read list of GUIDs from the GUIDs file
    connector_guids = read_guids('guids.txt')

    # Extract configuration values
    base_url = config.get('BASE_URL')
    api_client_id = config.get('API_CLIENT_ID')

```

```

api_key = config.get('API_KEY')

# Check if all required configuration values are present
if not base_url or not api_client_id or not api_key:
    print("Error: Missing required configuration values.")
    exit(1) # Exit the script if any configuration values are missing

# Process each GUID by isolating the endpoint
for guid in connector_guids:
    isolate_endpoint(base_url, api_client_id, api_key, guid)

```

## تاميلعن

- [لوضحل Cisco AMP API](#) دامتع اتان اي بعاشن ال [قياهنلا طاقن تاقيب طت قجمرب ٽهنج او ىلع](#)
- كتقطنم يف روکذمل ا BASE\_URL مادختسا:

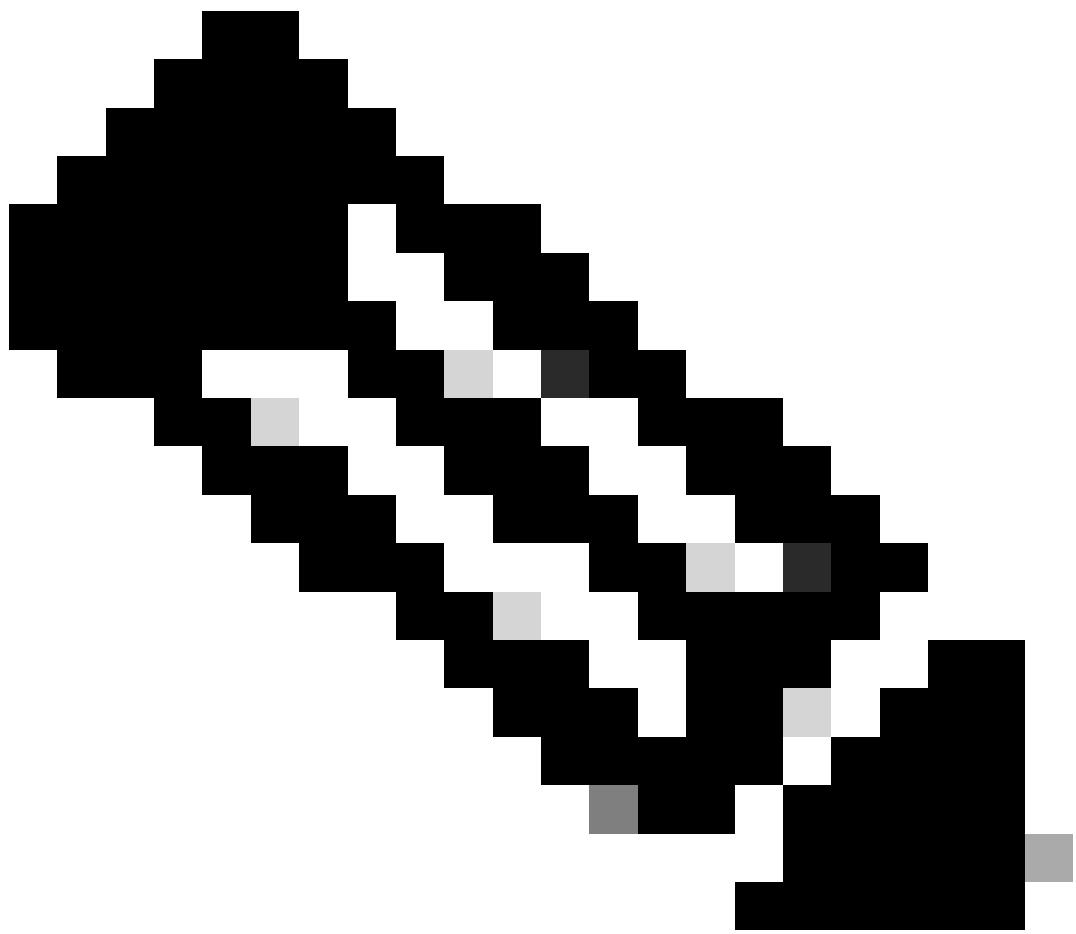
NAM - <https://api.amp.cisco.com/v1/computers/>  
EU - <https://api.eu.amp.cisco.com/v1/computers/>  
APJC - <https://api.apjc.amp.cisco.com/v1/computers/>

- ىوتحمل ا عم يذيفن تلا صنل ا لثم ليلدلا سفن يف config.txt فلم عاشناب مق فلم ىلع config.txt:

BASE\_URL=https://api.apjc.amp.cisco.com/v1/computers/  
API\_CLIENT\_ID=xxxxxxxxxxxxxxxxxxxx  
API\_KEY=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

- تافرعمب ةمئاق عم يصنل ا جمانرب ل ا لثم ليلدلا سفن يف config.txt فلم عاشناب مق GUID .ةجاحل ا بسح (GUID) ةيمومع تافرعم ةفاضاب مق .رطس ل كل دحاو ،لصوملل فلم ىلع config.txt:

abxxxxxxxxxxxxxxcd-XefX-XghX-X12X-xxxxxx567xxxxxxxx  
yzxxxxxxxxxxxxxxlm-XprX-XmnX-X34X-xxxxxx618xxxxxxxx



لالخ نم اما كب ڦصالا ٿياهنلا طاقنل ٿيمومع تافرعم عيمجت كنكمي :ٽحالم لاقتنا لالخ نم Cisco نم ڦنمآلا ٿياهنلا ٿطقون مكحت ڏدحو نم وأ [API](#) [GET /v1/computers](#) GUID خسنو، ڦنيعم ٿياهن ٿطقونل لاخدا لاعيسوت و، رتو وي بمکلا ڙهنجا > ڦرادإا ىلإ لصو مل ل.

- ۾ ب دجوي يذلا ليلدلا ىلإ لقتنا. ٿيفرط ٿطحم وأ رمأ ٥ جوم حتف:
- روک ذمل رمألا ليغشت بيصنلا جمانربلا ذيفنتب مق:

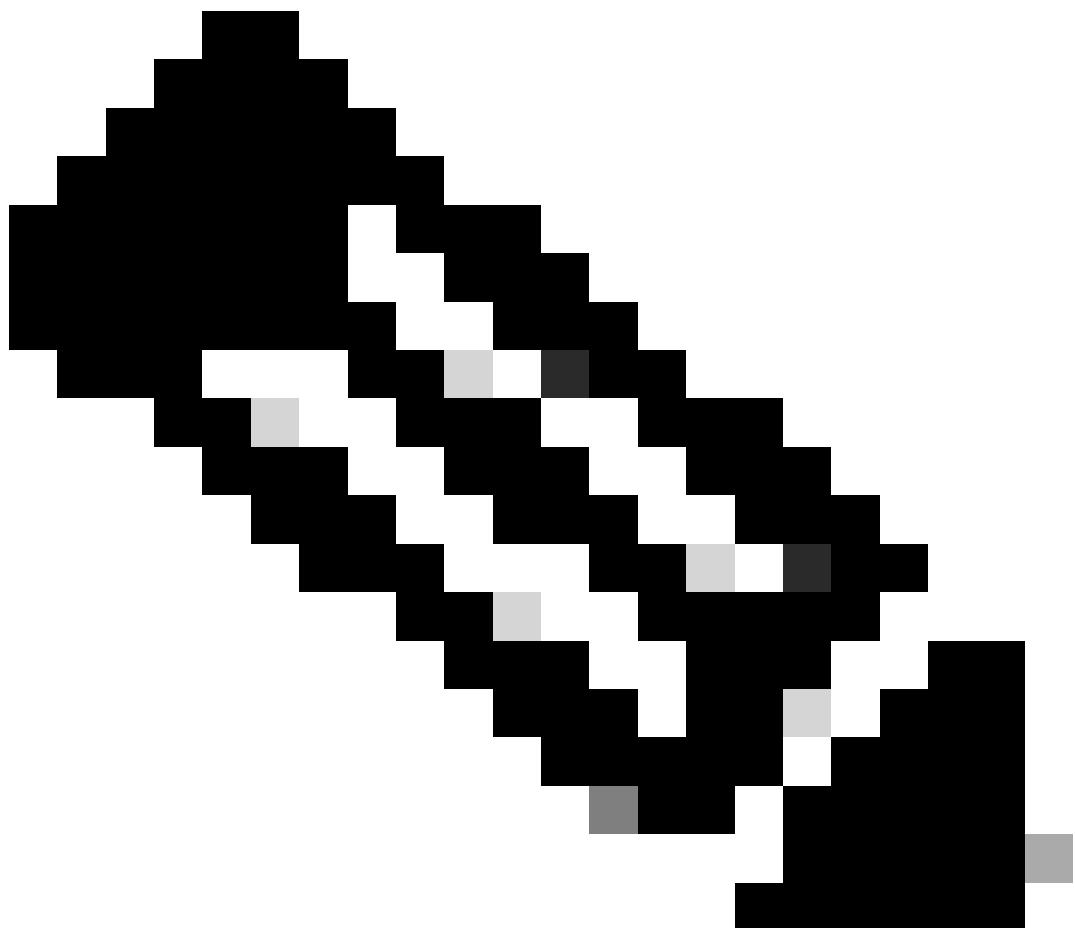
```
python start_isolation_script.py
```

## ڦحصلانم ٿققحتلا

- فلم يف ڏددم ٿياهن ٿطقون لك لزع يصنلا جمانربلا لواحي guid.txt.
- ٿطقون لك كل ٻڌخلا وأ حاجنلا لئاسرنع اثحب رمألا هجوم وأ ٿيفرطلا ڏدحولانم ٿققحت

ةياهن.

---



طاون ىلع لزعلا عدل قفروملا script start\_isolation.py رمألا مادختسا نكمي :ةظحالم  
لك .ةياهنلا طاقن ىلع لزعلا فاق毅إا stop\_isolation.py ميمصت مت امنيب ،ةياهنلا  
يه امك ىقبت يذيفنتلا صنلا ذيفنتول يغشتبا ةصالحا تاميلعتلا.

---

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).