# Automatisering van start/stop-isolatie op meerdere endpoints

## Inhoud



## Inleiding

Dit document beschrijft hoe de stop/start-isolatie op meerdere endpoints kan worden geautomatiseerd met behulp van de API voor Cisco Secure Endpoint.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure-endpoint
- Cisco Secure Endpoint-console
- Cisco Secure Endpoint API
- Python

### Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco Secure Endpoint 8.4.0.30201
- Endpoint voor host python-omgeving
- Python 3.1.7.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

## Achtergrondinformatie

- U gebruikt een PUT aanvraag om de isolatie te starten.
- Een Delete-aanvraag wordt gebruikt om de isolatie te stoppen.
- Controleer de API-documentatie voor meer informatie.

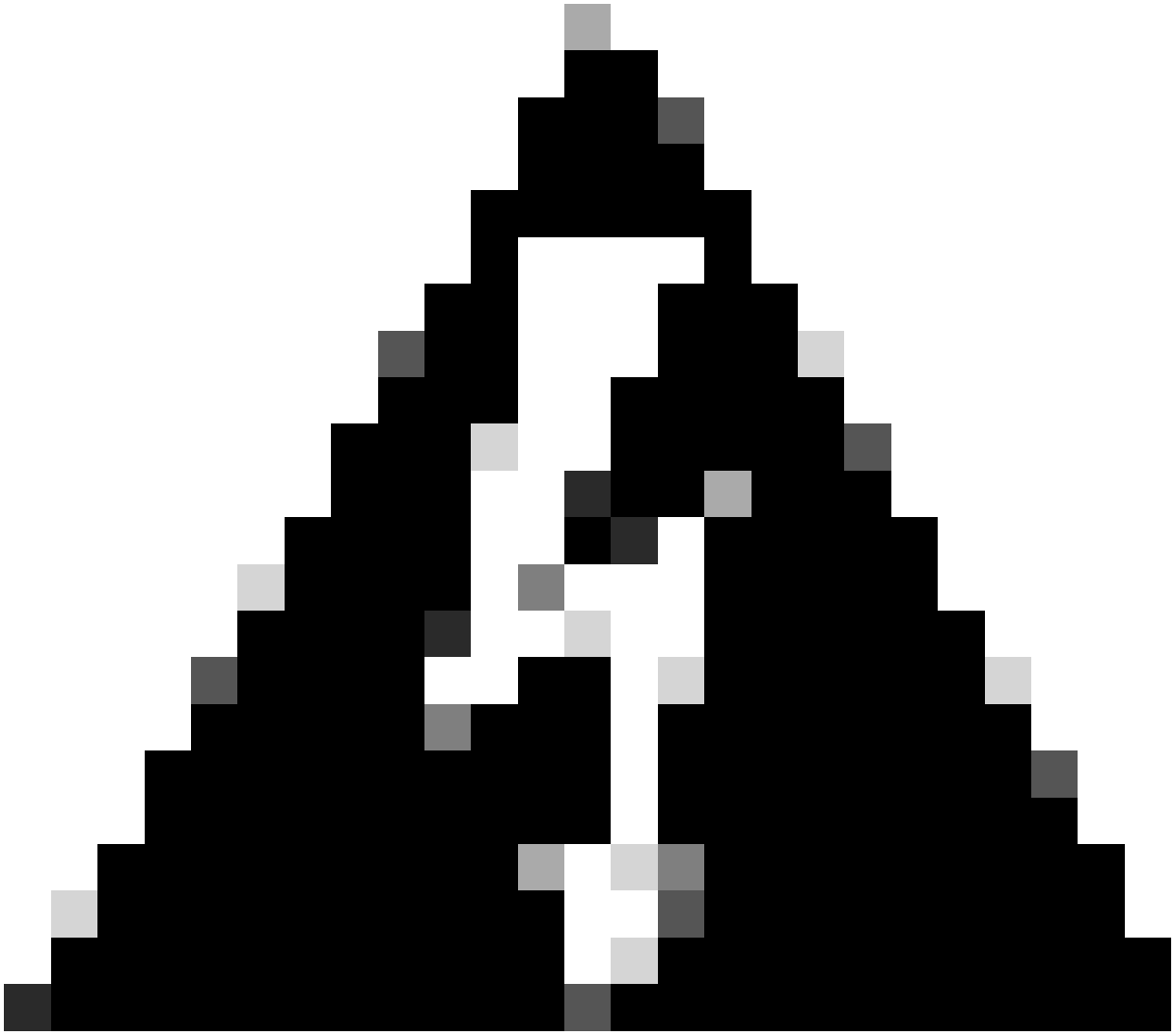
## Probleem

Cisco Secure Endpoint maakt start/stop-isolatie op één machine tegelijk mogelijk. Tijdens een beveiligingsincident is het echter vaak nodig om deze bewerkingen op meerdere endpoints tegelijkertijd uit te voeren om potentiële bedreigingen effectief te kunnen bevatten. Automatisering van het begin-/stop-isolatieproces voor bulk-endpoints met behulp van de API kan de responsefficiëntie van incidenten aanzienlijk verbeteren en het algemene risico voor het netwerk verminderen.

## Oplossing

- Het Python-script dat in dit artikel wordt geleverd, kan worden gebruikt om isolatie op meerdere endpoints in uw organisatie te starten of te beëindigen met behulp van Secure Endpoint API-referenties.
- Raadpleeg voor het genereren van de API-referenties voor Advanced Malware Protection Overzicht van Cisco Advanced Malware Protection voor Endpoints API
- Om het bijgeleverde script te kunnen gebruiken, moet u pythonon installeren op uw endpoints.
- Na het installeren van python, te installeren gelieve verzoeken module

```
pip install requests
```



Waarschuwing: het script wordt louter ter illustratie gegeven en is bedoeld om aan te tonen hoe de isolatiefunctie van het eindpunt moet worden geautomatiseerd met behulp van de API. Cisco Technical Assistance Center (TAC) is niet betrokken bij problemen met betrekking tot dit script. Gebruikers moeten voorzichtigheid betrachten en het script grondig testen in een veilige omgeving voordat ze het in een productie-instelling implementeren.

## Script

U kunt het verstrekte script gebruiken om isolatie te starten op meerdere endpoints in uw bedrijf:

```
import requests

def read_config(file_path):
    """
    Reads the configuration file to get the API base URL, client ID, and API key.
    """
```

```
    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)
```

## Instructies

- Raadpleeg voor het genereren van de API-referenties voor Advanced Malware Protection Overzicht van Cisco Advanced Malware Protection voor Endpoints API
- Gebruik BASE_URL vermeld voor uw regio:

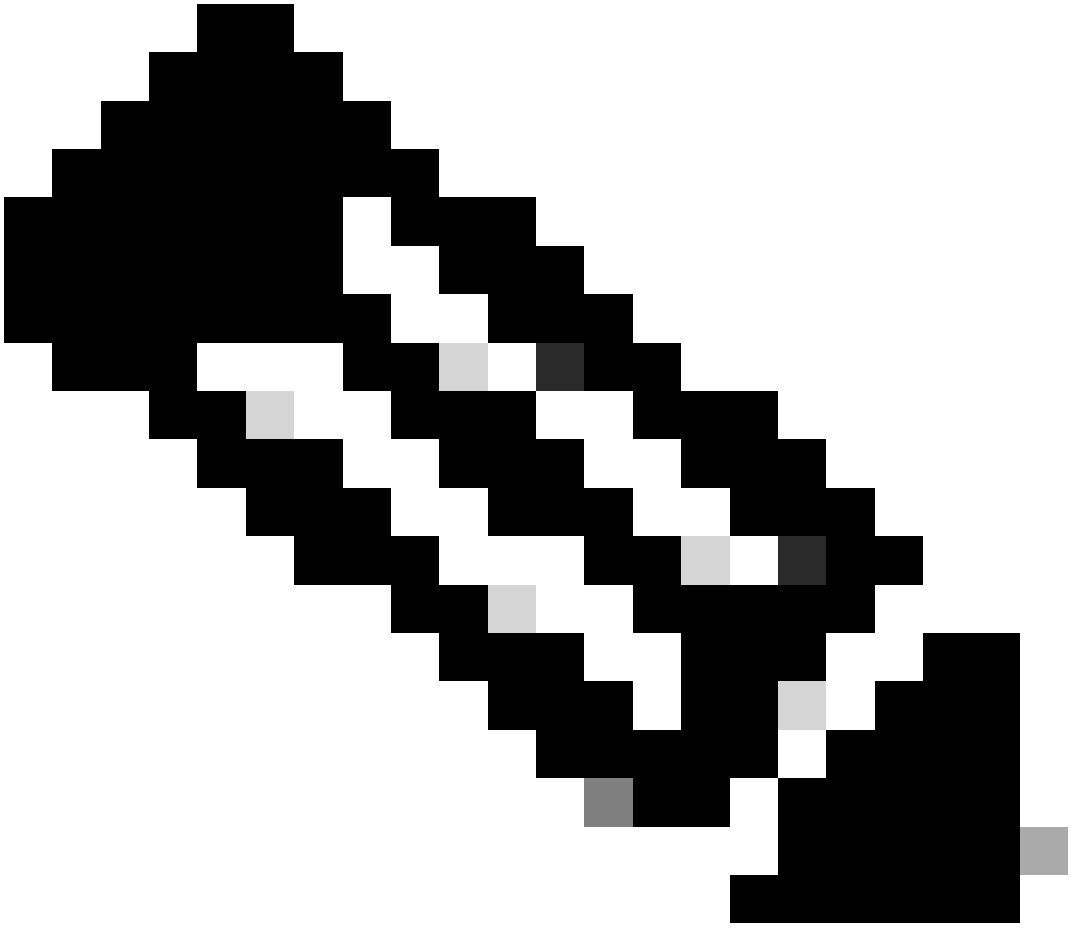
```
NAM - https://api.amp.cisco.com/v1/computers/
EU - https://api.eu.amp.cisco.com/v1/computers/
APJC - https://api.apjc.amp.cisco.com/v1/computers/
```

- Maak een config.txt bestand in dezelfde map als het script met de genoemde inhoud. Voorbeeld van config.txt bestand:

```
BASE_URL=https://api.apjc.amp.cisco.com/v1/computers/
API_CLIENT_ID=xxxxxxxxxxxxxxxxxxxx
API_KEY=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

- Maak een guids.txt-bestand in dezelfde map als het script met de lijst met connector-GUID's, een per lijn. Voeg zo veel GUID's toe als nodig is. Voorbeeld van guids.txt-bestand:

```
abXXXXXXXXXXXXcd-XefX-XghX-X12X-XXXXXX567XXXXXXX
yzXXXXXXXXXXXXlm-XprX-XmnX-X34X-XXXXXX618XXXXXXX
```



Opmerking: u kunt de GUID's van uw endpoints verzamelen via de API GET /v1/computers of via de Cisco Secure Endpoint Console door te navigeren naar Management > Computers, de vermelding voor een specifiek eindpunt uit te breiden en de Connector GUID te kopiëren.

---

- Open een terminal- of opdrachtprompt. Navigeer naar de directory waar start_isolation_script.py zich bevindt.
- Voer het script uit door de aangegeven opdracht uit te voeren:

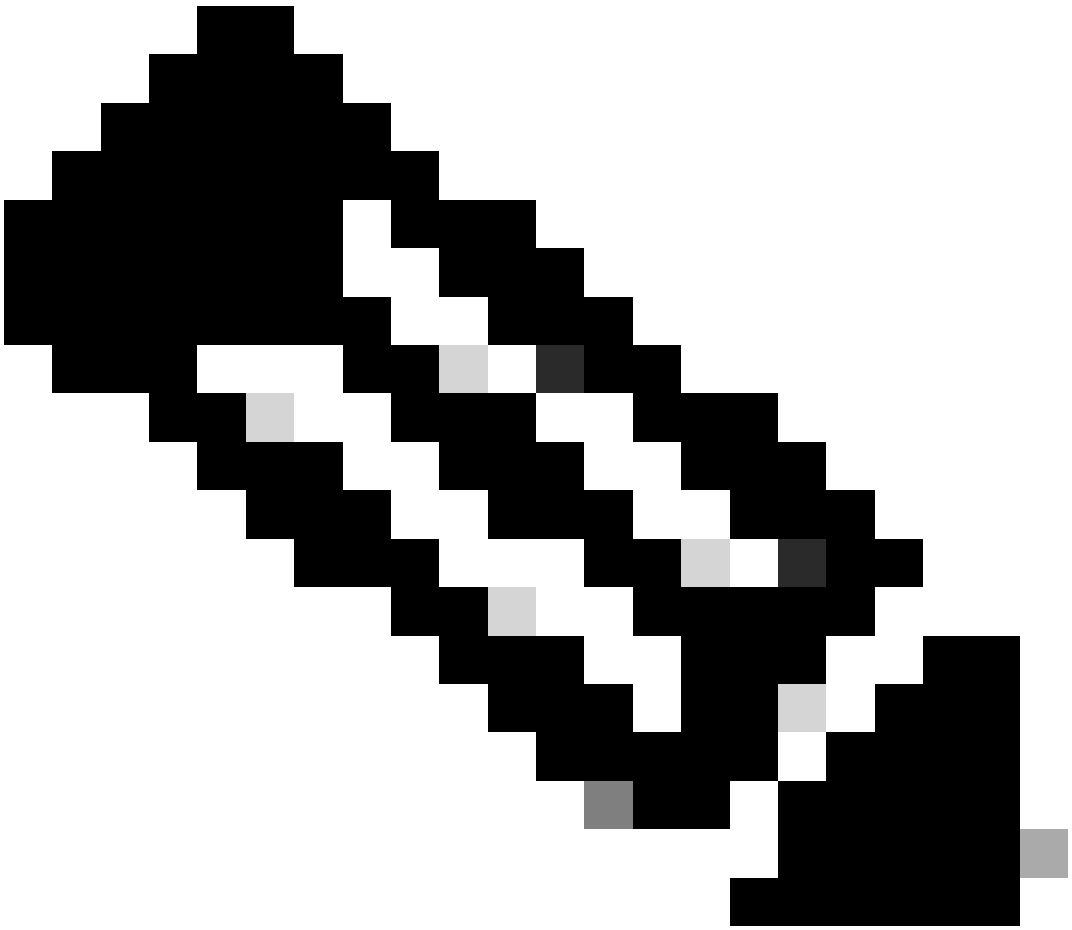
```
python start_isolation_script.py
```

## Verifiëren

- Het script probeert elk eindpunt dat in het guids.txt-bestand is opgegeven, te isoleren.

- Controleer de terminal- of opdrachtprompt op succes of foutmeldingen voor elk eindpunt.

---



Opmerking: het bijgevoegde script start_isolation.py kan worden gebruikt om de isolatie op endpoints te starten, terwijl stop_isolation.py is ontworpen om de isolatie op endpoints te stoppen. Alle instructies voor het uitvoeren van het script blijven hetzelfde.

---

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.