CISCO Secure Endpoint - Secure Endpoint API

Authentication

The Secure Endpoint API requires access via an authenticated and authorized account. Only authorized accounts are able to submit requests to API operations. All operations must communicate over a secure HTTPS connection.

To authenticate and access the Secure Endpoint API, perform the following:

1. Integrate Secure Endpoint with Cisco XDR or Secure Client Cloud Management.

- Navigate to the Secure Endpoint console.
- Click the Integrate Now button on the Secure Endpoint Dashboard.
- This enables the integration between Secure Endpoint and Cisco XDR or Secure Client Cloud Management.

Integrate xdr :

- Navigate to the Cisco XDR or Secure Client Cloud Management console and verify the integration.
- Enable the Integration (Cisco XDR only)
- Navigate to Administration -> Integrations, then click + Enable
- Enable Secure Endpoint

2. Register the API Client.

- From within either Cisco XDR or Secure Client Cloud Management
- Navigate to Administration -> API Clients.
- On the API Clients page, click the Generate API Client button to open the Add New Client form.
  - add new client form
- Enter a Client Name and select a Scope.
  - Note: The Secure Endpoint API will work with any of the selected Scopes.
  - The API Client will have the same permissions within Secure Endpoint as the creator of the API Client.
- Optionally, enter a Description and click Add New Client.

- The Client Id and Client Password are generated and will appear on the Add New Client form. api credential form
- Secure the Client ID and Client Password before closing the window. Copy and paste it properly.

3. Generate an API Access Token.

Method 1: Linux

Use the following OAuth2 token API to generate an API access token:

North America	https://visibility.amp.cisco.com/iroh/oauth2/token
Asia Pacific, Japan, and China	https://visibility.apjc.amp.cisco.com/iroh/oauth2/token
Europe	https://visibility.eu.amp.cisco.com/iroh/oauth2/token

The Client-Id and Client-Password (Client-Secret per OAuth2) generated in the previous step are required to call the token endpoint.

Get an Access Token via the Token API:

```
# Read in the client_id and client_secret if they are not already set.
[ -z "$client_id" ] && read -p "client_id: " client_id
[ -z "$client_secret" ] && read -p "client_secret: " client_secret

# Call the token endpoint and store the result in a variable.
result=$(curl -s 'https://visibility.eu.amp.cisco.com/iroh/oauth2/token' \
    --user "${client_id}:${client_secret}" \
    --header 'Content-Type: application/x-www-form-urlencoded' \
    --header 'Accept: application/json' \
    -d 'grant_type=client_credentials')

# Extract the access_token from the result.
export BEARER_TOKEN=$(echo "$result" | jq -r .access_token)

# Print the result.
[ -x "$(command -v jq)" ] && echo "$result" | jq . || echo "$result"
```

Response:

```
{
  "access_token": "eyJhbGciO...",
  "token_type": "bearer",
  "expires_in": 600,
  "scope": "enrich:read casebook inspect:read"
}
```

4. Generate Secure Endpoint API Access Token.

Use the following access token endpoint to generate a Secure Endpoint API access token:

North America	https://api.amp.cisco.com/v3/access_tokens
Asia Pacific, Japan, and China	https://api.apjc.amp.cisco.com/v3/access_tokens
Europe	https://api.eu.amp.cisco.com/v3/access_tokens

The API access token generated in previous step is required to call the token endpoint.

Get and Access Token from the Secure Endpoint Token API:

```
# Call the Secure Endpoint token endpoint and store the result in a variable.
result=$(curl -s 'https://api.amp.cisco.com/v3/access_tokens' \
    --header 'Content-Type: application/x-www-form-urlencoded' \
    --header 'Accept: application/json' \
    --header "Authorization: Bearer $BEARER_TOKEN" \
    -d 'grant_type=client_credentials')

# Extract the access_token from the result.
export BEARER_TOKEN=$(echo "$result" | jq -r .access_token)

# Print the result.
[ -x "$(command -v jq)" ] && echo "$result" | jq . || echo "$result"
```

Response:

```
{
  "access_token": "eyJhbGciO..."
}
```

5. Access Secure Endpoint API.

The token generated in previous step is used to access the Secure Endpoint APIs.

Request:

```
# Call the Secure Endpoint API and store the result in a variable.
result=$(curl -s 'https://api.amp.cisco.com/v3/organizations?size=10' \
              --header "Authorization: Bearer ${BEARER_TOKEN}")

# Print the result.
[ -x "$(command -v jq)" ] && echo "$result" | jq . || echo "$result"
```

Response:


```
{
  "meta": {
    "start": 0,
    "size": 10,
    "total": 2
  },
  "data": [
    {
      "name": "Example Organization #1",
      "organizationIdentifier": "4baascfeaofqpxidpinxtt5l"
    },
    {
      "name": "Example Organization #2",
      "organizationIdentifier": "nxtf3phj4w0z41pim3vqarzk"
    }
  ]
}
```


Method 2: Windows

1. Set Client ID and Client Secret

The script reads client_id and client_secret from the user if not set and uses them to request an OAuth2 token.

```
@echo off
REM Check if client_id and client_secret are set
if "%client_id%"=="" set /p client_id="Enter client_id: "
if "%client_secret%"=="" set /p client_secret="Enter client_secret: "

REM Call the OAuth2 token endpoint
curl -s -u "%client_id%:%client_secret%" ^
    -H "Content-Type: application/x-www-form-urlencoded" ^
    -H "Accept: application/json" ^
    -d "grant_type=client_credentials" ^
    https://visibility.amp.cisco.com/iroh/oauth2/token > token.json

REM Extract the access_token using jq (ensure jq is installed)
for /f "delims=" %%A in ('jq -r ".access_token" token.json') do set BEARER_TOKEN=%%A

REM Output the token
echo OAuth2 Access Token: %BEARER_TOKEN%
```

2. Generate Secure Endpoint API Access Token

Use the token from the previous step to generate an API access token for Secure Endpoint.

```
@echo off
REM Call the Secure Endpoint token endpoint
curl -s -X POST ^
    -H "Content-Type: application/x-www-form-urlencoded" ^
    -H "Accept: application/json" ^
    -H "Authorization: Bearer %BEARER_TOKEN%" ^
    -d "grant_type=client_credentials" ^
    https://api.amp.cisco.com/v3/access_tokens > endpoint_token.json

REM Extract the access_token using jq (ensure jq is installed)
for /f "delims=" %%A in ('jq -r ".access_token" endpoint_token.json') do set SECURE_ENDPOINT_TOKEN=%%A

REM Output the Secure Endpoint API token
echo Secure Endpoint API Access Token: %SECURE_ENDPOINT_TOKEN%
```

3. Access the Secure Endpoint API

```
@echo off
REM Call the Secure Endpoint API
curl -s -X GET ^
    -H "Authorization: Bearer %SECURE_ENDPOINT_TOKEN%" ^
    https://api.amp.cisco.com/v3/organizations?size=10 > organizations.json

REM Output the API response
echo Secure Endpoint API Response:
type organizations.json
```

Key Notes:

Prerequisites:

- Install curl (default on Windows 10/11 or available via Chocolatey).
- Install jq for JSON parsing (available via jq).
- Save and Run:
- Save the script as a .bat file (e.g., get_token.bat).
- Run the script in Command Prompt or PowerShell.
- Replace Region URLs:
- Use the appropriate region URL in the curl commands (e.g., North America, APJC, or Europe).

Source: https://developer.cisco.com/docs/secure-endpoint/authentication/#3-generate-an-api-access-token

---

Revision #6
Created 17 January 2025 05:42:55 by Richmond Abella
Updated 27 February 2025 09:31:16 by Richmond Abella