



DevNet & Programmability テクニカルセッション

第6回 Cisco Security 製品APIご紹介

Satoshi Katayama

セキュリティ事業 コンサルティングシステムズエンジニア

2018/03/20

SBG supports API as of March 2018

Product	API	CRUD	Use Case
AMP4E	✓	✓	エンドポイントの一括グループ移動やイベントの取得など
Threat Grid	✓	✓	複数の検体を一括解析など
Cloud lock	-	-	N/A
Umbrella	✓	✓	複数ドメインリストの一括削除など
ESA	✓	✓	メール関連レポートを取得
CES	-	-	N/A
Firepower	✓	✓	ルールの設定やイベントログの抽出など
Meraki MX	✓	✓	ルールの設定など
ASA	✓	✓	ルールの設定など
ISE	✓	✓	人事システムと連携したID管理など
SWATCH	✓	-	Flow情報の長期保管、必要な情報のみの抽出、独自検索UIなど
WSA	-	-	N/A
CTA	✓	-	外部SIEMへTAXIIでの情報提供
PSIRT	✓	-	保有製品及びバージョンでCVE確認、OVAL取得など

AMP4E

Item

Documents	https://api-docs.amp.cisco.com/api_versions?api_host=api.amp.cisco.com
Self Study Contents	n/a

Cisco AMP for Endpoints APIの使い方について – Cisco Support Community

<https://supportforums.cisco.com/t5/%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3-%E3%83%89%E3%82%AD%E3%83%A5%E3%83%A1%E3%83%B3%E3%83%88/cisco-amp-for-endpoints-api%E3%81%AE%E4%BD%BF%E3%81%84%E6%96%B9%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6/ta-p/3220035>

Threat Grid

Item

Documents	https://panacea.threatgrid.com/doc/main/api-getting-started.html
-----------	---

Self Study Contents	DEVNET Learning Labs(Cisco Threat Grid – Introduction to the Threat Grid API) https://learninglabs.cisco.com/labs/tags/Security,Threat+Grid+API
---------------------	---

Cloudlock

Item

Documents	n/a
Self Study Contents	n/a

Umbrella

Item

Documents	https://docs.umbrella.com/developer
-----------	---

Self Study Contents	DEVNET Learning Labs
---------------------	----------------------

ESA

Item

Documents	https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-programming-reference-guides-list.html
Self Study Contents	n/a

https://www.cisco.com/c/en/us/td/docs/security/esa/esa_all/esa_api/b_ESA_API_Getting_Started_Guide/b_ESA_API_Getting_Started_Guide_chapter_00.html#con_1092467

情報の取得は可能だが、アップデート等に関しては基本的にサポートしておらず

CES (API not provided for customer)

Item

Documents	https://www.cisco.com/c/ja_jp/support/docs/security/cloud-email-security/209696-CES-How-can-I-use-AsyncOS-API.html
Self Study Contents	n/a

Firepower

Item

Documents	https://www.cisco.com/c/en/us/support/security/defense-center/products-programming-reference-guides-list.html
Self Study Contents	DEVNET Learning Labs

Meraki MX

Item

Documents	https://dashboard.meraki.com/api_docs#mx-l3-firewall
Self Study Contents	n/a

ASA

Item

Documents	https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html#id_44480
Self Study Contents	n/a

ISE

Item

Documents	https://communities.cisco.com/docs/DOC-66297
-----------	---

Self Study Contents	<a href="https://<ise ip address>:9060/ers/sdk">https://<ise ip address>:9060/ers/sdk
---------------------	---

下記にはほとんど情報なく、筐体のsdk参照。

https://www.cisco.com/c/en/us/td/docs/security/ise/2-3/api_ref_guide/api_ref_book.html

SWATCH

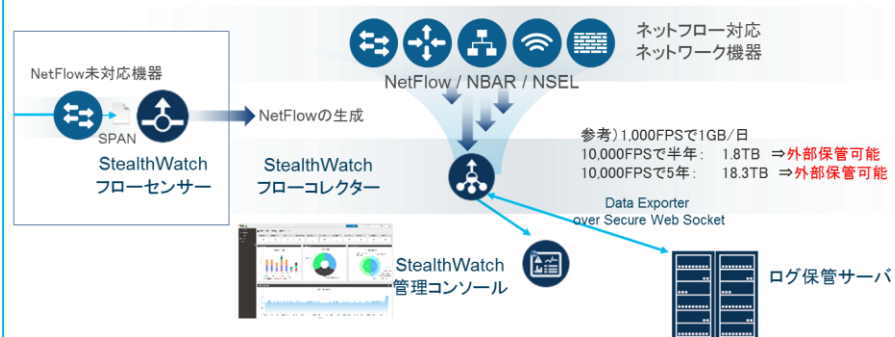
Item

Documents	https://www.cisco.com/c/ja_jp/support/security/stealthwatch/products-programming-reference-guides-list.html
Self Study Contents	https://developer.cisco.com/docs/stealthwatch/

Flow Collectorにたまっていくフローログそのものをパースしてライブストリームで取得可能。

<https://github.com/CiscoDevNet/stealthwatch-data-exporter>

Cisco Stealthwatch: システム概要 (ログオプション)



WSA

Item

Documents	–
-----------	---

Self Study Contents	–
---------------------	---

Anti-Malware and Reputationの設定のみで、WSA本体に対するAPIは無い。

https://www.cisco.com/c/ja_jp/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01110.html#task_2260707

CTA

Item

Documents	https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_0100011.html
-----------	---

Self Study Contents	n/a
---------------------	-----

Splunk等のSIEMに脅威情報をTAXIIで連携する仕組み

<https://github.com/CiscoCTA/taxii-log-adapter/wiki/Integration-with-Splunk>

PSIRT

Item

Documents	https://developer.cisco.com/site/PSIRT/discover/overview/
-----------	---

Self Study Contents	https://developer.cisco.com/site/PSIRT/get-started/getting-started.html
---------------------	---

DEVNET Learning Labs

Firepowerラボを触ってみましょう

DevNet Learning Labs

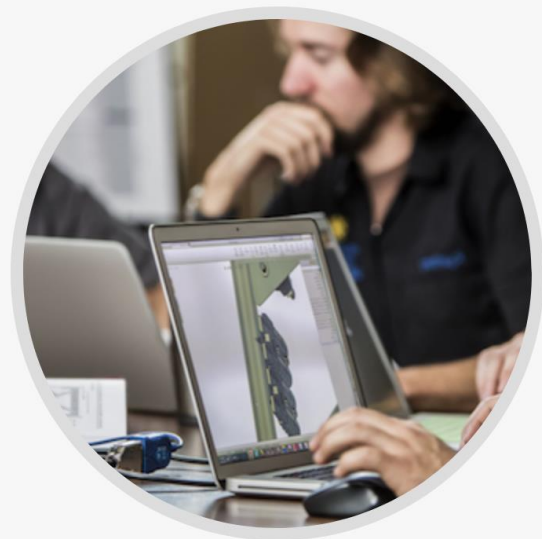
The DevNet Learning Labs will help you dive into Partner technologies, including Enterprise Mobility, Cloud, SDN, and IoT. If you're just getting started or a refresher, the Learning Labs will help you get up to speed on APIs, Python, JavaScript, and other programming languages.


Springboards are now Tracks.







DevNet [Tracks](#) and [Modules](#) now make it easier to learn. Modules are designed to guide you through related concepts.

... Cisco
... collaboration,
... ing
... ering REST
... ncepts.

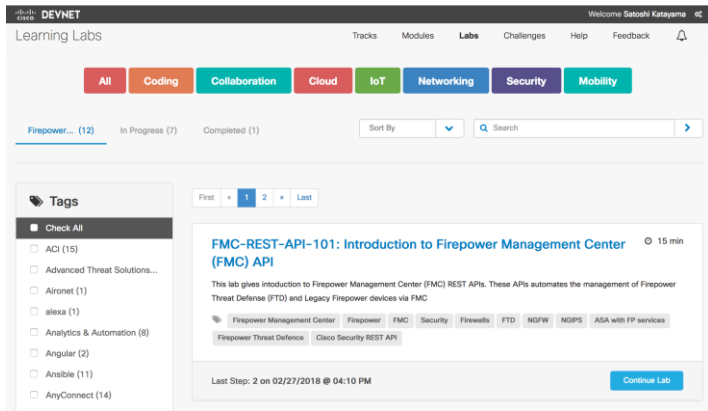
... s and
... ceptually



 DEVNET ×

-  Login with Github
-  Login with Google
-  Login with Facebook
-  Login with a Cisco ID
-  Login with Cisco NetAcad
-  Login with Cisco Spark

[Get Started →](#)

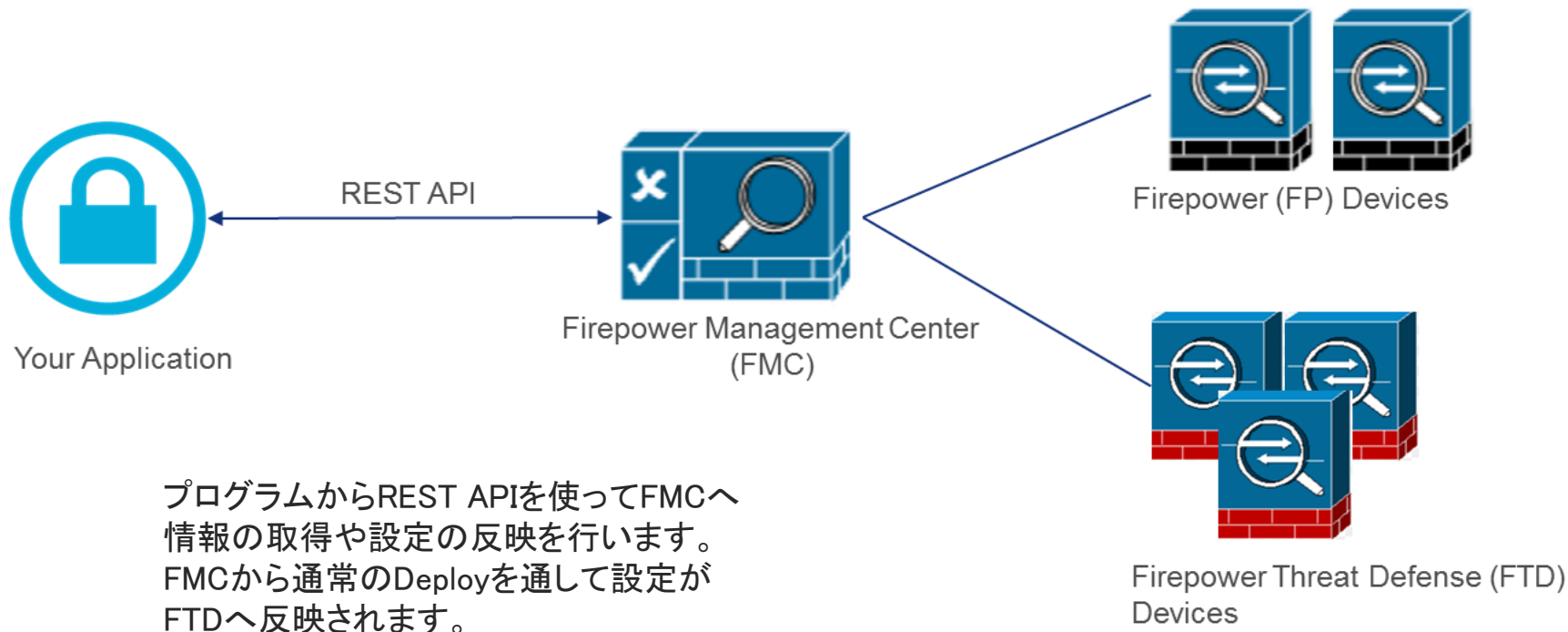


TagsからFirepowerをチェックしてフィルタします

FMC-REST-APIラボも充実しています

- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**
- **FMC-REST-API-102: FMC REST api authentication and access**
- **FMC-REST-API-103: Add/register a device to Firepower Management Center (FMC)**
- **FMC-REST-API-104: FMC REST api REQUEST AND RESPONSE structures and error codes**
- **FMC-REST-API-105: Debugging the FMC REST API errors**
- **FMC-REST-API-106: FMC object(s) and CRUD operations using REST API**
- **FMC-REST-API-107: Firewall Policy fundamentals and Policy CRUD**
- **FMC-REST-API-109: Creating a Threat Centric AC Policy using the FMC REST API**
- **FMC-REST-API-110: Using evenstreamer API to identify a potentially compromised host**
- **FMC-REST-API-111: Cisco Threat Intelligence Director (TID) APIs and their usage via API Explorer and Postman**
- **FMC-REST-API-112: Introduction to Firepower Management Center (FMC) API CRUD operations**
- **Firepower eStreamer and Splunk: Learn to create custom Splunk App that visualize threat data using Firepower Management Center (FMC) eStreamer API**

- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**



FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API

FMCサンドボックスが用意されていますのでそちらを使うこともできます。
サンドボックスを利用するには予め予約が必要です。

<https://developer.cisco.com/site/devnet/sandbox/docs/index.gsp#security/overview>

The screenshot displays the Cisco DevNet interface for the Firepower Management Center REST API sandbox. The main content area shows an overview of the sandbox environment, which includes Firepower Management Center (FMC) version 6.1, a Virtual Firepower Next Generation Firewall (NGFW), and Firepower Threat Defense (FTD) version 6.1. A diagram illustrates the connectivity between these three components. The interface also provides a link to the API Explorer and a quick start guide for the REST API.

サンドボックス予約が完了するとID/PWがメールで送付されます

Good News! Your user account for the DevNet Sandbox "Firepower Management Center" is setup, and the lab is ready for your use.

Here are your FMC user credentials, which will be active for the duration of your reservation:

- FMC Address: <https://fmcrestapisandbox.cisco.com/api/api-explorer/>
- FMC Username: skatayam
- FMC Password: w!x4HMGW

our Sandbox Lab

- Go directly to your [Firepower Management Center Lab](#) (You need to be logged into DevNet to navigate to your lab)
- You must establish a VPN connection (see above) in order to interact with the devices in your lab

We hope you find the FMC Lab useful, and your reservation time productive.

If you have questions or issues, we encourage you to engage with us in the [DevNet Sandbox Developer Community Forum](#).

Regards,

FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API

予約することで送付されたメールに記載あるID/PWにてAPIエクスプローラーにログイン

The screenshot displays the Cisco Firepower Management Center - API Explorer interface. The top navigation bar includes the Cisco logo, the title "Cisco Firepower Management Center - API Explorer", and a "logout" button. The main content area is divided into several sections:

- API INFO:** Shows "FMC Version: 6.1.0".
- Policy Services:** Includes a "Domains" dropdown set to "Global".
- API CONSOLE:** The active section, showing the endpoint `/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies`. It features a search input field containing "objectId", a "GET" button, and a "Success!" message. Below this, there are tabs for "Response Text", "Response Info", and "Request Info". The "Response Text" tab is selected, displaying a JSON response:

```
{  "links": {    "self": "https://fmcrestapisandbox.cisco.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies?offset=0&limit=25"  },  "items": [    {      "type": "AccessPolicy",      "links": {        "self": "https://fmcrestapisandbox.cisco.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/objectId"      }    }  ]}
```
- Implementation Notes:** Provides a description: "Retrieves, deletes, creates, or modifies the access control policy associated with the specified ID. Also, retrieves list of all access control policies." and includes an "Examples" link.
- Parameters:** A table listing query parameters for the API call.
- Response:** Shows the "Response Content Type" as "application/json" and the "Response Object" as "AccessPolicy".
- AccessPolicy Model:** A table showing the structure of the response object.

Parameter	Required	Description	Type	Data Type
objectId	true	Identifier for access control policy.	path	string
limit	false	Number of items to return	query	integer
offset	false	Index of first item to return	query	integer

Field	Value	Description	Constraints
metadata	object		None
metadata.lastUser	object		None

- **FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API**

APIコンソールからACPをGETした結果と実際のFMC上のACP

API CONSOLE

/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies

Identifier for access control policy.

+ query parameter

Content-Type Header

Accept Header

GET Success!

Response Text Response Info Request Info

```
{
  "type": "AccessPolicy",
  "links": {
    "self":
      "https://fmcrestapisandbox.cisco.com/api/fmc_config/v1/domain/e276abec-
      e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/005056BB-0B24-0ed3-
      0000-266287972781"
  },
  "name": "AC-TEST-BP",
  "id": "005056BB-0B24-0ed3-0000-266287972781"
},
```

Analysis **Policies** Devices Objects

Access Control ▶ Access Control Network Discovery

Access Control Policy

- AC-TEST-BP**
Enterprise Policy to Detect and Prevent Threats
- Access_Test_Nov13
- AccessPolicy-veer-test-1
- AccessPolicy_Marvin
- AccessPolicyHUEHUEBR

• FMC-REST-API-101: Introduction to Firepower Management Center (FMC) API

APIコンソールの実行サンプルスクリプトを入手も可能

Cisco Firepower Management Center - API Explorer

API INFO
FMC Version: 6.1.0

Audit
Deployment
Device Groups
Devices
Object
Policy
Policy Assignments
Status
System Information

Export operation in python language

Cut & paste below script in the appropriately typed file or download [GET__api_fmc_config_v1_domain_e276abec-e0f2-11e3-8169-6d9ed49b625f_policy_accesspolicies.py](#):

To execute the script type in following in a terminal by passing in FMC username and password as parameters:
python script.py <username> <password>

```
#  
# Generated FMC REST API sample script  
#  
import json  
import sys  
import requests  
  
server = "https://fmc-rest-api-sandbox.cisco.com"  
  
username = "admin"  
if len(sys.argv) > 1:  
    username = sys.argv[1]  
password = "sf"  
if len(sys.argv) > 2:  
    password = sys.argv[2]  
  
r = None  
headers = {'Content-Type': 'application/json'}  
api_auth_path = "/api/fmc_platform/v1/auth/generatetoken"  
auth_url = server + api_auth_path  
try:  
    # 2 ways of making a REST call are provided:  
    # One with "SSL verification turned off" and the other with "SSL verification"  
    # The one with "SSL verification turned off" is commented out. If you like to  
    # uncomment the line where verify=False and comment the line with =verify='/p  
    # REST call with SSL verification turned off:  
    # r = requests.post(auth_url, headers=headers, auth=requests.auth.HTTPBasicAuth(username, password), verify=False)  
    # REST call with SSL verification turned on: Download SSL certificates from y  
    r = requests.post(auth_url, headers=headers, auth=requests.auth.HTTPBasicAuth(username, password), verify=True)
```

Domains Global

API CONSOLE

[/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies](#)

objectId

Identifier for access control policy.

+ query parameter

Content-Type Header application/json

Accept Header application/json

GET Success!

Response Text Response Info Request Info

date: Tue, 13 Mar 2018 01:47:33 GMT
content-encoding: gzip
vary: Accept-Charset,Accept-Encoding,Accept-Language,Accept-Range
server: Apache
x-frame-options: SAMEORIGIN
content-type: application/json
cache-control: no-cache, no-store, must-revalidate, max-age=0
connection: Keep-Alive
accept-ranges: bytes
keep-alive: timeout=5, max=100

Export operation in...
Python script
Perl script

まとめ

- 多くのシスコセキュリティ製品がAPIを公開しております。
- セルフスタディにはDEVNET Learning Labsがオススメです。
- サンプルスクリプトをカスタムして自分なりに使い勝手のいいものを作り上げることが近道です。
- 標準機能だけでは満たせない要件をAPI利用することで実現できた時のエンジニアとして達成感もあります（本来メーカーが対応すべきという意見はさておき。。。）
- APIを駆使して考えも見なかった新しい価値を創造できればエンジニアとしての価値はプライスレス。

