



The bridge to possible

# Firewall Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 4 管理・監視・冗長構成編 Rev 2.0

August 2022

シスコシステムズ合同会社

# はじめに

- 本ガイドは、Version 7.0 の Firewall Management Center (以下、FMC) 管理の Firewall Threat Defense (以下、FTD) の初期セットアップ方法を解説しております。
- 本ガイドは、FTD と FMC の仮想版を使って、評価作業を開始できることをゴールとしております。
- 本ガイドは、4部作の Vol. 4 に相当します。

## 内容に関する保証について

- 本ガイドは、2022年8月現在の情報に基づいており、FTD & FMC のソフトウェアは 7.0.x を、ハイパーバイザは VMware ESXi 6.5 を利用しております。
- 本ガイドに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。
- シスコは、本ガイドに関して、その正確性又は完全性について一切の責任を負わないこととします。
- シスコは、本ガイドが十分な品質を有すること、特定の目的に対する適合性を有すること、又は第三者の知的財産権、プライバシー権等その他の一切の権利に対する侵害がないことを、明示にも黙示にも表明又は保証しません。

# ネットワーク環境図

Internet

■ 設定済みの機器

MGMT NW

.135.254

DNS: 64.104.14.184

ntp.esl.cisco.com

proxy-wsa.esl.cisco.com

10.71.128.0/21

VM Network

.132.194

G0/0 outside .1

FTDv01

test PC2

Management

G0/1 inside .1

.101

.132.204

FMCv

.132.130

ISE-PIC01

.132.220

ESXi

.132.131

内部LAN

192.168.1.0/24

.11

.101

AD01.secvt.jp

test PC1

管理NW (実態はシスコ検証NW)

顧客NW

g0/0 グローバルアドレス

ASA

g0/3 .254

外部LAN

192.168.240.0/24

PAT

PAT

# 当ガイド (Vol. 4) のシナリオ

- FMC を RestAPI を使って設定してみる
- FMC と FTD のデバイス監視方法を理解し、ヘルスポリシーを設定する
- FMC と FTD から外部への syslog 出力や、FMC でのレポート作成を実施してみる。また、問題が発生した際に外部にアラートが送られるように設定する
- FMC と FTD が SAL SaaS や SecureX と連携するように設定する
- FMC にて間違った設定をしてしまった際に、その設定を戻すロールバックを試してみる
- FTDv を 1 台追加し、High Availability の構成にする
- FMCv を 1 台追加し、High Availability の構成にする

# 注意事項

- 製品名称が更新されているが、ソフトウェア名称は旧製品のままで公開されている
- 新名称 ↔ 旧名称
  - Firewall Management Center ↔ Firepower Management Center
  - Firewall Threat Defense ↔ Firepower Threat Defense

# Vol.1 (初期インストール編) の目次

1. FMC と FTD のインストール
  - 1-1. FMCv の初期インストール
  - 1-2. FTDv の初期インストール
  - 1-3. (Option) FPR4100/9300 シリーズの初期インストール
  - 1-4. (Option) FPR1000/2100 シリーズの初期インストール
2. FTD と FMC その他初期設定
3. シグネチャ及び各種 DB の更新
4. スマートライセンスの適用
5. FMC と FTD の Upgrade / Patch インストール

# Vol. 2 (基本セキュリティポリシー設定編) の目次

6. Routed Firewall, NAT および Network Discovery の設定
7. Prefilter の設定
8. Intrusion Policy の設定 (Snort3)
9. Malware & File Policy の設定
10. Access Control Policy の設定

# Vol. 3 (応用設定編) の目次

11. TLS Decryptionの設定
12. IDFW の設定
13. AnyConnect VPN 接続の設定
14. バックアップの設定とリストアの方法

# Vol. 4 (管理・監視・冗長構成編:当ガイド) の目次

15. FMC API の利用例
16. システム監視
17. Syslog・レポート・アラートの設定
18. SAL SaaS, SecureX 連携の設定
19. 設定ロールバック
20. FTD High Availability の設定
21. FMC High Availability の設定

## 15. FMC API の利用例

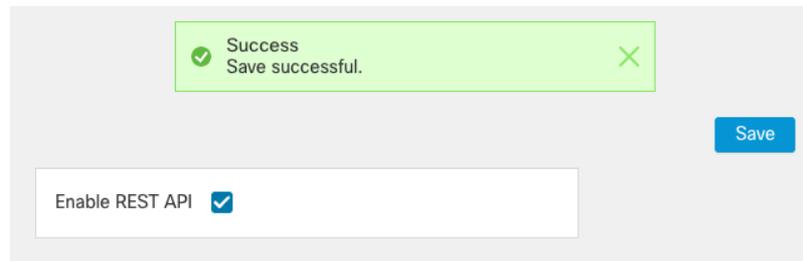
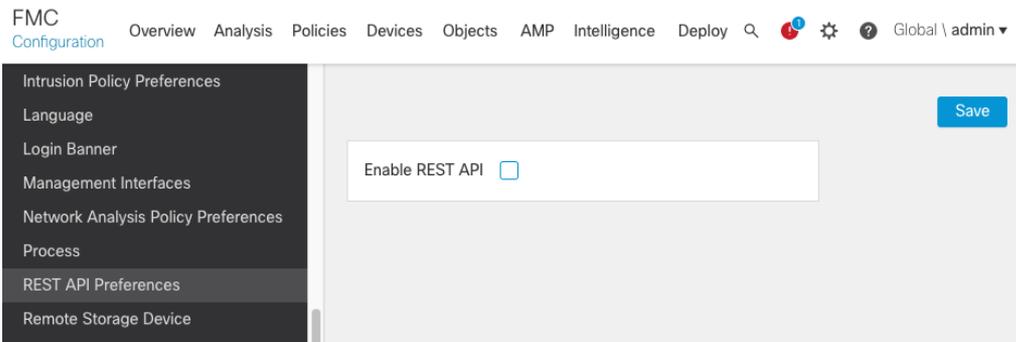
# FMC API について

- REST API にて API を提供
- API に関するガイドは FMC 内部にある API Explorer にまとまっている
- API Explorer の UI は FMC の内部に存在するため、詳細を確認するには FMC が必要
- Python3 であれば “fmccapi” パッケージも用意されていてより簡単に構築可能

# 事前準備

# 事前準備 – 1. REST APIの有効化

- [System] > [Configuration] > [REST API Preferences] > [Enable REST API]



# 事前準備 – 2. クレデンシヤル (User/Pass) のエンコード

- FMC のクレデンシヤルを ASCII でそのまま送ることは許可されないため Base64 に変換
- 「Username:Password」の形でエンコード
  - Username と password 間に「:」コロンを付けてエンコード
    - 例) username が "Admin" password が "Admin123" の場合「Admin:Admin123」の形で Base64 にエンコード
- エンコード方法
  - ネットで [base64エンコード] と検索すればウェブ上で変換できるツールが簡単に見つかる。
  - Python でも可能 >>

```
>>> import base64 <---base64 のライブラリをインポート
>>>
>>> credential = b"Admin:Admin123" <---" の前に「b」を付けてクレデンシヤルを入力
>>> base64ed = base64.b64encode(credential)<---base64 にエンコード
>>> print(base64ed)
b'QWRtaW46QWRtaW4xMjM=' <---エンコードされた文字列は'の間
```

# 事前準備 – 3. Authentication Token (認証トークン) 取得

FMC REST API ではユーザ名、パスワードの代わりにトークンを利用する。様々な取得方法が存在しているが、本資料では 2パターンを紹介

- a. POSTMAN でのトークン取得方法
- b. Python でのトークン取得方法

どちらのパターンでも基本的には以下の URL に対して「POST」で投げることでトークンを取得可能

[https://<management\\_center\\_IP\\_or\\_name>/api/fmc\\_platform/v1/auth/generatetoken](https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken)

※留意点：取得したトークンは 30分間有効で、最大 3回更新可能。それ以上の時間が必要であれば再度トークンを取得という流れになる

# 事前準備 - 3a. POSTMAN でのトークン取得方法

POST を選択

https://<management\_center\_IP\_or\_name>/api/fmc\_platform/v1/auth/generatetoken

POST

https://[redacted]/api/fmc\_platform/v1/auth/generatetoken

Send

Save

Authorization

Headers (1)

Body

Pre-request Script

Tests

Cookies

Code

Type: Basic Auth

Clear

Update Request

Username: Admin

Password: [redacted]

Show Password

The authorization header will be generated and added as a custom header

Save helper data to request

FMC にログインする Username/Password を入力

ドメイン UUID

Send をクリック

Body	Cookies	Headers (22)	Tests
DOMAINS → [{"uid":"e276abec-e0f2-11e3-8169-6d9ed49b625f","name":"Global"}]			
DOMAIN ID → 111			
DOMAIN_UUID → e276abec-e0f2-11e3-8169-6d9ed49b625f			
Date → Thu, 09 Dec 2021 02:10:29 GMT			
Keep-Alive → timeout=5, max=100			
Referrer-Policy → same-origin			
Server → Apache			
Strict-Transport-Security → max-age=31536000; includeSubDomains			
USER_UUID → 68d03c42-d9bd-11dc-89f2-b7961d42c462			
Vary → Accept-Charset,Accept-Encoding,Accept-Language,Accept			
X-Content-Type-Options → nosniff			
X-Frame-Options → SAMEORIGIN			
X-Permitted-Cross-Domain-Policies → none			
X-UA-Compatible → IE=edge			
X-XSS-Protection → 1; mode=block			
X-auth-access-token → 5bf4f885-f7ce-439d-8358-2e90c386b649			
X-auth-refresh-token → d3bf23a5-a8a6-4034-a93d-37e91831fe9f			
global → e276abec-e0f2-11e3-8169-6d9ed49b625f			

Headers 配下に "アクセストークン" が表示される

# 事前準備 - 3b. Python3.x でのトークン取得方法

```
import requests
url = "https://x.x.x.x/api/fmc_platform/v1/auth/generatetoken"

payload = {}
headers = {
    'Authorization': 'Basic YWRtaW46QzFzY28xMjM0NSE='
}
response = requests.request("POST", url, headers=headers, data = payload, verify=False)

print(response.headers)
{'date': 'Thu, 09 Dec 2021 02:11:05 GMT', 'server': 'Apache', 'strict-transport-security':
'max-age=31536000; includeSubDomains', 'cache-control': 'no-store', 'accept-ranges':
'bytes', 'vary': 'Accept-Charset,Accept-Encoding,Accept-Language,Accept', 'x-auth-
access-token': '9c9a207e-f8ac-4a67-9d69-60190500c24e', 'x-auth-refresh-token':
'59dfa9fb-fed5-46a4-b7de-a439920d751f', 'user_uuid': '68d03c42-d9bd-11dc-89f2-
b7961d42c462', 'domain_id': '111', 'domain_uuid': 'e276abec-e0f2-11e3-8169-
6d9ed49b625f', 'global': 'e276abec-e0f2-11e3-8169-6d9ed49b625f', 'domains':
[{"name": "Global", "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"}], 'x-frame-
options': 'SAMEORIGIN', 'x-ua-compatible': 'IE=edge', 'x-permitted-cross-domain-
policies': 'none', 'x-xss-protection': '1; mode=block', 'referrer-policy': 'same-origin',
'content-security-policy': "base-uri 'self'", 'x-content-type-options': 'nosniff', 'keep-
alive': 'timeout=5, max=100', 'connection': 'Keep-Alive'}
```

接続先のURL

header に Basic 認証用に  
Post として 上記URL へ送信

返り値の headers を Print  
コマンドで表示

token が表示される

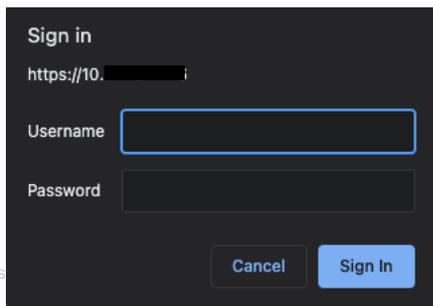
# API Explorer

# API Explorer について

- API Explorer は FMC で API を有効後に使える FMC 内部で保持している API ガイド
- API Explorer は OpenAPI Spec (OAS) 形式のインタフェースを提供
- API Explorer へのアクセス方法 :

`https://<firepower_management_center_IP_or_name>/api/api-explorer`

(例 : `https://10.0.0.1/api/api-explorer`)



Sign in

`https://10.0.0.1`

Username

Password

Cancel Sign In

アクセスするとログインを求められるので  
FMC の GUI へログインする時と同じ ID/PW で  
ログイン

# API Explorer の見方

## Cisco Firepower Management Center Open API Specification 1.0.0

[View JSON](#)

Specifies the REST URLs and methods supported in the Cisco Firepower Management Center API. Refer to the version specific [REST API Quick Start Guide](#) for additional information.

[Cisco Technical Assistance Center \(TAC\) - Website](#)  
[Send email to Cisco Technical Assistance Center \(TAC\)](#)  
[Cisco Firepower Management Center Licensing](#)

Domains

Global

Devices	>
Policy Assignments	>
Device HA Pairs	>
Health	>
Updates	>
Users	>
Intelligence	>
Search	>
Audit	>
Integration	>
Device Groups	>
Status	>
Device Clusters	>
System Information	>
Object	>
<b>Policy</b>	>
Deployment	>

## OpenAPI フォーマットでカテゴリ毎に表示

Policy	
GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies
POST	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies
GET	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules
POST	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules
PUT	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules
DELETE	/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules

目的に応じて  
GET/POST/PUT/DELETE  
を使った操作が可能  
※設定項目によっては一部の操作しかできないものもある

GET = 情報を取得  
POST = 情報を入力  
PUT = 情報を変更  
DELETE = 情報を削除

# API Explorer の使い方 (GET)

例) Devices > [GET] devices/devicerecords

**POST** /api/fmc\_config/v1/domain/{domainUUID}/devices/copyconfigrequests **リクエストアドレス**

**GET** /api/fmc\_config/v1/domain/{domainUUID}/devices/devicerecords

Retrieves or modifies the device record associated with the specified ID. Registers or unregisters a device. If no ID is specified for a GET, retrieves list of all device records.

**Parameters**

**Name** **Description**

domainUUID **required** Domain UUID  
string (path)  
e276abec-e0f2-11e3-8169-6d9ed49b625f

offset Index of first item to return.  
integer (query)  
offset - Index of first item to return.

limit Number of items to return.  
integer (query)  
limit - Number of items to return.

expanded If set to true, the GET response displays a list of objects with additional attributes.  
boolean (query)  
--

**Try it out**

**Execute をクリック**

Responses **Execute** Clear  
Response content type application/json

Curl  
curl -X GET "https://[redacted]/api/fmc\_config/v1/domain/c276abec-e0f2-11e3-8169-6d9ed49b625f/devices/devicerecords" -H "accept: application/json" -H "X-auth-access-token: 7edab042-fbcb-4dd3-98c4-b2eb31b8ae49"

Request URL  
https://[redacted]/api/fmc\_config/v1/domain/c276abec-e0f2-11e3-8169-6d9ed49b625f/devices/devicerecords

Code **Details**

200

Response body

```
{
  "links": {
    "self": "https://[redacted]/api/fmc_config/v1/domain/c276abec-e0f2-11e3-8169-6d9ed49b625f/devices/devicerecords?offset=0&limit=25"
  },
  "items": [
    {
      "id": "8e9a5db8-1aa9-11ec-aaf6-89c25c09a9dc",
      "type": "Device",
      "links": {
        "self": "https://[redacted]/api/fmc_config/v1/domain/c276abec-e0f2-11e3-8169-6d9ed49b625f/devices/devicerecords/8e9a5db8-1aa9-11ec-aaf6-89c25c09a9dc"
      },
      "name": "FTDv01"
    },
    {
      "id": "35eedc26-f383-11ec-b07b-edbfdad179b8",
      "type": "Device",
      "links": {
```

"Required" は必須項目

試したい場合は  
"Try it out" をクリック  
> Execute をクリック

Code は RestAPI なので  
HTTP と同じく、"200"  
なら成功。"400" などそ  
れ以外であれば何かしら  
の問題がある

# API Explorer の使い方 (POST)

POST /api/fmc\_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/accessrules

← リクエスト先 URL (本例では access rule 追加)

Name Description

**body** \* required  
object  
(body)

The input access control rule model.

Example Value	Model
---------------	-------

```
{
  "metadata": {
    "lastUser": {
      "name": "string",
      "links": {
        "parent": "string",
        "self": "string"
      },
      "id": "string",
      "type": "string"
    },
    "ruleIndex": 0,
    "domain": {
      "name": "string",
      "links": {
        "parent": "string",
        "self": "string"
      },
      "id": "string",
      "type": "string",
      "uuid": "string"
    },
    "readOnly": {
      "reason": "RBAC",
      "state": true
    },
    "section": "string",
    "accessPolicy": {
      "name": "string",
      "links": {
        "parent": "string",

```

サンプルの入力方法

AccessRule {

description: Represents Access Rule contained within an Access Policy.

metadata: AccessRuleMetadata > (...)

umpConfig: ISNMPConfig > (...)

timeRangeObjects: > [...]

sourceNetworks: INetworkObjectsContainer > (...)

cydlogSeverity: string

Specifies the Override Severity if alerts are being sent to default sys

Enum:

> Array [ # ]

sourceZones: ISourceZoneContainer > (...)

destinationDynamicObjects: IDynamicObjectsContainer > (...)

destinationZones: ISecurityZoneContainer > (...)

description: string

User provided resource description.

originalSourceNetworks: INetworkObjectsContainer > (...)

enableSyslog: boolean

Boolean indicating whether the alerts associated with the access rule

type: string

Type of the response object. This value is always AccessRule.

safeSearch: ISafeSearch > (...)

enabled: boolean

どのような階層構造で、どのような情報を入力できるのかが確認可能

**containerUUID** \* required  
string  
(path)

The container id under which this specific resource is contained.

containerUUID - The container id under which!

**domainUUID** \* required  
string  
(path)

Domain UUID

domainUUID - Domain UUID

access rule 追加の例では Body に加えて「containerUUID」「domainUUID」が必須項目  
※domainUUID は API Explorer では自動的に入力される

Request example 1 : POST /mc\_config/v1/domain/DomainUUID/policy/accesspolicies/containerUUID/accessrules (Test POST of Access rule)

```
{
  "action": "ALLOW",
  "actionType": "rule",
  "type": "AccessRule",
  "name": "Test1",
  "accessPolicy": {
    "name": "Test1",
    "links": {
      "parent": "string",
      "self": "string"
    },
    "id": "string",
    "type": "string",
    "uuid": "string"
  },
  "readOnly": {
    "reason": "RBAC",
    "state": true
  },
  "section": "string",
  "accessPolicy": {
    "name": "string",
    "links": {
      "parent": "string",

```

ページ下部には具体的な入力例を表示

# API 試行の例

# Postman

Policy 情報 (ACP) を取得 (GET) する例

## Policy

GET /api/fmc\_config/v1/domain/{domainUUID}/policy/accesspolicies

メソッドは GET を指定

FMC の IP アドレス + GET 横の URL を追加して入力  
(domainUUID はアクセストークン取得時に同時に取得)

Type: は Basic Auth を  
選択し、FMC ログイン  
ID/PW をその下に入力

① GET  
② http://x.x.x.x/api/fmc\_config/v1/domain/{domainUUID}/p  
③ Basic Auth  
④ Headers  
⑤ Send

Headers に必要な項目は以下の 2 点

1. x-auth-access-token < -- 本資料 "事前準備 - 2a" で取得したアクセストークン
2. Content-Type < -- application/json を選択

key	value
X-auth-access-token	d04beffd-8d64-4e05-9620-8d45a
Content-Type	application/json

Status は HTTP と同じ 200/201 なら OK。400, 500 などはエラーとなる。

⑥ Status: 200 OK

```
1- {
2-   "links": {
3-     "self": "https://10.10.10.10/api/fmc_config/v1/domain/e276bec-e0f2-11e3-8169-6d9ed49b
4-   },
5-   "items": [
6-     {
7-       "type": "AccessPolicy",
8-       "links": {
9-         "self": "https://10.10.10.10/api/fmc_config/v1/domain/e276bec-e0f2-11e3-8169-6d9e
10-      },
11-       "name": "AccessPolicy2",
12-       "id": "000C29C6-GDFF-0ed3-0000-326417543599"
13-     },
14-     {
15-       "type": "AccessPolicy",
16-       "links": {
17-         "self": "https://10.10.10.10/api/fmc_config/v1/domain/e276bec-e0f2-11e3-8169-6d9e
18-      },
19-       "name": "AccessPolicy3",
20-       "id": "000C29C6-GDFF-0ed3-0000-326417543198"
21-     },
22-     {
23-       "type": "AccessPolicy",
24-       "links": {
25-         "self": "https://10.10.10.10/api/fmc_config/v1/domain/e276bec-e0f2-11e3-8169-6d9e
26-      },
27-       "name": "AccessPolicy4",
28-       "id": "000C29C6-GDFF-0ed3-0000-326417543198"
29-     }
30-   ]
31- }
```

- ① メソッドは "GET" を選択
- ② URL を記入
- ③ Authentication のタイプは "Basic Auth" を選択し、FMC ログイン ID/PW をその下に入力
- ④ Headers の欄にアクセストークンとコンテンツのタイプを入力
- ⑤ "Send" をクリック
- ⑥ 取得結果は "Body" に表示

# Python3

## Policy 情報 (ACP) を取得 (GET) する例

### Policy

GET

/api/fmc\_config/v1/domain/{domainUUID}/policy/accesspolicies

```
bash-3.2$ python3 ← Python3 起動
```

```
Python 3.7.3 (v3.7.3:ef4ec6ed12, Mar 25 2019, 16:52:21)
```

```
[Clang 6.0 (clang-600.0.57)] on darwin
```

```
Type "help", "copyright", "credits" or "license" for more information.
```

```
>>>
```

```
>>> import requests
```

```
>>> import json
```

```
>>> from requests.auth import HTTPBasicAuth
```

```
>>>
```

```
>>> address = "10.1.1.1"
```

```
>>> username = "admin"
```

```
>>> password = "Admin123"
```

```
>>>
```

```
>>> api_uri = "/api/fmc_platform/v1/auth/generatetoken" } トークン発行用の URL を定義
```

```
>>> url = "https://" + address + api_uri
```

```
>>>
```

```
>>> response = requests.request("POST", url, verify=False, auth=HTTPBasicAuth(username, password))
```

```
>>> accesstoken = response.headers["X-auth-access-token"]
```

```
>>> DOMAIN_UUID = response.headers["DOMAIN_UUID"]
```

```
>>> headers = {'Content-Type': 'application/json', 'x-auth-access-token': accesstoken}
```

```
>>>
```

```
>>> access_policy_api = "/api/fmc_config/v1/domain/" + DOMAIN_UUID + "/policy/accesspolicies" } ACP 取得用の URL を定義
```

```
>>> access_policy_url = "https://" + address + access_policy_api
```

```
>>>
```

```
>>> response_acp = requests.get(access_policy_url, headers=headers, verify=False)
```

```
>>> responsemessage_acp = response_acp.json()
```

```
>>>
```

```
>>> print(responsemessage_acp) } ACP 情報 (responsemessage_acp) を print を使い表示し確認
```

```
{'links': {'self': 'https:// 10.1.1.1 /api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies?offset=0&limit=25'}, 'items': [{'type': 'AccessPolicy', 'links': {'self': 'https:// 10.1.1.1 /api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/000C29C6-6DFF-0ed3-0000-326417543599'}, 'name': 'AccessPolicy2', 'id': '000C29C6-6DFF-0ed3-0000-326417543599'}, {'type': 'AccessPolicy', 'links': {'self': 'https:// 10.1.1.1 /api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies/000C29C6-6DFF-0ed3-0000-326417543198'}, 'name': 'AccessPolicy3', 'id': '000C29C6-6DFF-0ed3-0000-326417543198'}], 'paging': {'offset': 0, 'limit': 25, 'count': 10, 'pages': 1}}
```

} ライブラリ、モジュール等を import

} FMC の IP アドレスやクレデンシャルの変数を定義

} トークン発行用の URL を定義

} トークンをリクエストして、返ってきた値からトークンや DomainUUID を変数として定義

} ACP 取得用の URL を定義

} ACP 情報を取得し、戻り値を json フォーマットにして変数として定義

# Postman

Host object を追加 (POST) する例

**POST** /api/fmc\_config/v1/domain/{domainUUID}/object/hosts

メソッドは POST を指定

FMC の IP アドレス + POST 横の URL を追加して入力  
(domainUUID はアクセストークン取得時に同時に取得)

① POST  
② URL  
③ Basic Auth  
④ Headers  
⑤ Body

Type: は Basic Auth を  
選択し、FMC ログイン  
ID/PWをその下に入力

Headers に必要な項目は以下の 2 点

1. X-auth-access-token < -- 本資料 "事前準備 - 2a" で取得したアクセストークン
2. Content-Type < -- application/json を選択

Authorization	Headers (2)	Body	Pre-request Script	Tests
✓	X-auth-access-token	d04beffd-8d64-4e05-9620-8d45a		
✓	Content-Type	application/json		
	key	value		

Body は "raw" と "Json(application/json)" を選択し  
Host Object 追加に必要な情報を Json フォーマットで入力  
(下記は必要最低限の情報のみを記載)

```
1- {
2  "name": "TestHost",
3  "type": "Host",
4  "value": "10.5.3.20",
5  "description": "Test Description"
6 }
```

- ① メソッドは "GET" を選択
- ② URL を記入
- ③ Authentication のタイプは "Basic Auth" を選択し、  
FMC ログイン ID/PW をその下に入力
- ④ Headers の欄にアクセストークンとコンテンツの  
タイプを入力
- ⑤ "Send" をクリック
- ⑥ 取得結果は "Body" に表示

# Python3

POST

/api/fmc\_config/v1/domain/{domainUUID}/object/hosts

## Host object を追加 (POST) する例

```
bash-3.2$ python3 ← Python3 起動
Python 3.7.3 (v3.7.3:ef4ec6ed12, Mar 25 2019, 16:52:21)
[Clang 6.0 (clang-600.0.57)] on darwin
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> import requests
>>> import json
>>> from requests.auth import HTTPBasicAuth
>>>
>>> address = "10.1.1.1"
>>> username = "admin"
>>> password = "Admin123"
>>>
>>> api_uri = "/api/fmc_platform/v1/auth/generatetoken"
>>> url = "https://" + address + api_uri
>>>
>>> response = requests.request("POST", url, verify=False, auth=HTTPBasicAuth(username, password))
>>> accesstoken = response.headers["X-auth-access-token"]
>>> DOMAIN_UUID = response.headers["DOMAIN_UUID"]
>>> headers = {'Content-Type': 'application/json', 'x-auth-access-token': accesstoken}
>>>
>>> host_payload1="""
... {
...   "name": "TestHost1",
...   "type": "Host",
...   "value": "10.5.3.21",
...   "description": "Test Description"
... }
... """
>>> host_api_uri = "/api/fmc_config/v1/domain/" + DOMAIN_UUID + "/object/hosts?bulk=false"
>>> host_url = "https://" + address + host_api_uri
>>>
>>> response = requests.request("POST", host_url, headers=headers, data = host_payload, verify = False)
>>> print(response.text)
```

ライブラリ、モジュール等を import

FMC の IP アドレスやクレデンシャルの変数を定義

トークン発行用の URL を定義

トークンをリクエストして、返ってきた値からトークンや DomainUUID を変数として定義

追加する Host 情報を定義

HOST object 追加用の URL を定義

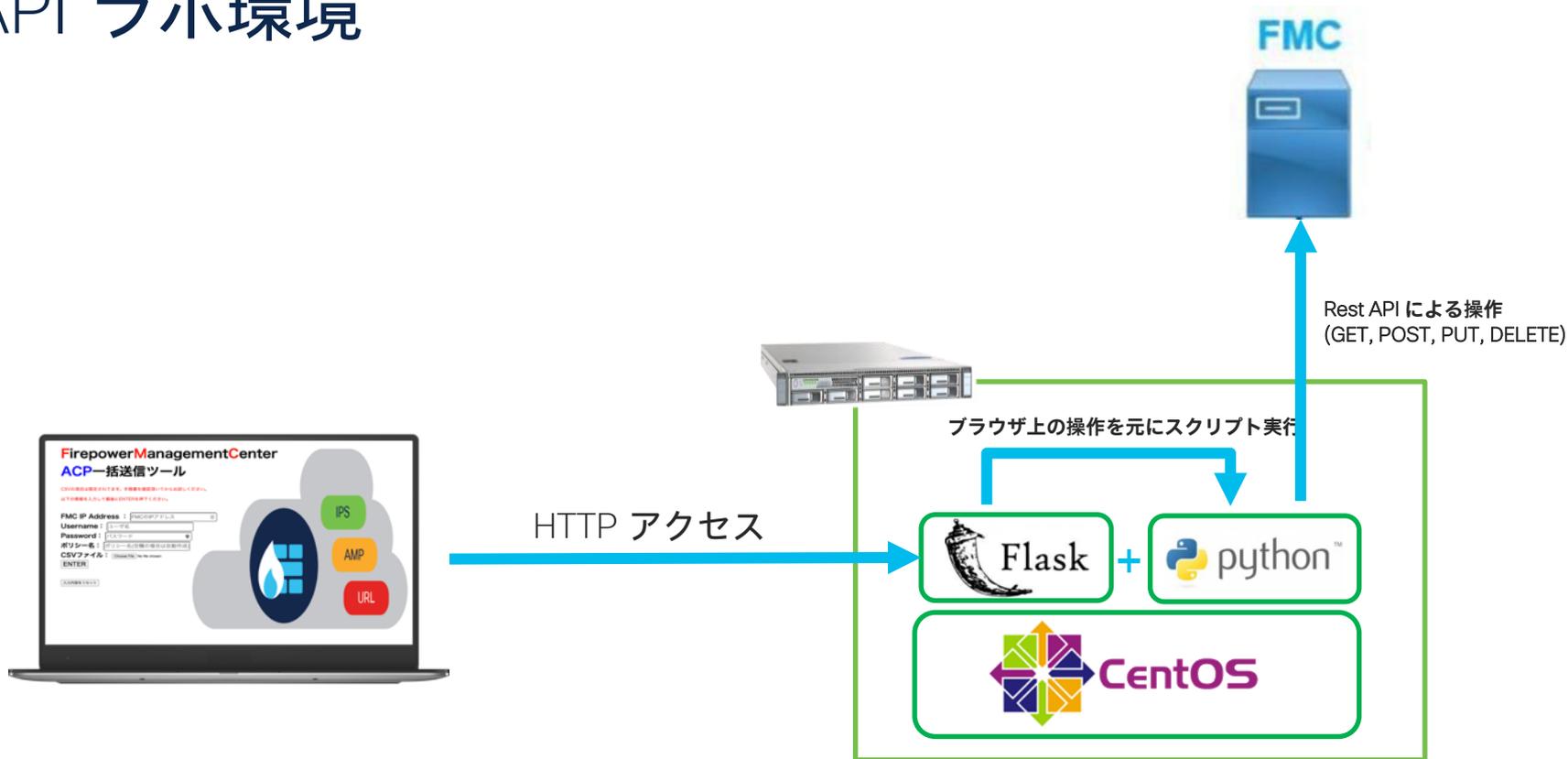
HOST object を追加 (POST)

追加した結果を表示 (GUI でも確認可能)

～省略～

# API 活用例

# API ラボ環境



# Python で ACP 一括送信ツールを作成

- FMC では ACP のルールを作成するのに GUI で1個ずつ設定するため時間が掛かる。そのため CSV ファイルを元に一括で作成できたら楽なのでは? という思いから作成

## FirepowerManagementCenter

### ACP一括送信ツール

CSVの項目は限定されています。手順書を確認頂いてからお試ください。

以下の情報を入力して最後にENTERを押下ください。

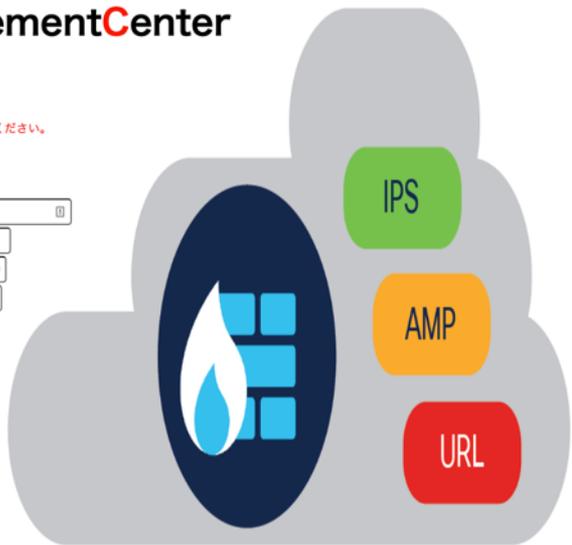
FMC IP Address :

Username :

Password :

ポリシー名 :

CSVファイル :  No file chosen



## 【ACP 一括送信ツール概要】

- ウェブアプリは Flask で作成
- 以下の情報はウェブページで手動入力
  - FMC IP
  - FMC ログインクレデンシャル
  - ACP 名
- 新規 ACP を入力した ACP 名で作成
- ACP 内のアクセスルールは CSV ファイルを使って一括設定

# Python スクリプト概要

Python スクリプト (Flask も同時実行)

```
1 import requests
2 import csv
3 import json
4 from requests.auth import HTTPBasicAuth
5 from getpass import getpass
6 import os
7 from flask import Flask, render_template, request, redirect, url_for, send_from_directory, session
8 from werkzeug.utils import secure_filename
9
10 app = Flask(__name__)
11
12 UPLOAD_FOLDER = './uploads'
13 ALLOWED_EXTENSIONS = set(['csv'])
14 app.config['UPLOAD_FOLDER'] = UPLOAD_FOLDER
15
16 @app.route('/', methods=['GET'])
17 def login():
18     return render_template("index2.html")
19
20 def allowed_file(filename):
21     return '.' in filename and \
22         filename.rsplit('.', 1)[1].in ALLOWED_EXTENSIONS
23
24
25 @app.route('/send', methods=['GET', 'POST'])
26 def send():
27     if request.method == 'POST':
28         csv_file = request.files['csv_file']
29         if csv_file and allowed_file(csv_file.filename):
30             filename = secure_filename(csv_file.filename)
31             csv_file.save(os.path.join(app.config['UPLOAD_FOLDER'], filename))
32             csv_url = app.config['UPLOAD_FOLDER'] + '/' + filename
33             abspath = os.path.abspath(filename)
34
35             fmc_ip = request.form.get('fmc_ip')
36             fmc_username = request.form.get('fmc_username')
37             fmc_password = request.form.get('fmc_password')
38             fmc_policy_name = request.form.get('fmc_policy_name')
39
40             address = fmc_ip
41             username = fmc_username
42             password = fmc_password
43             policyname = fmc_policy_name
44
45             api_url = "/api/fmc_platform/v1/auth/generatetoken"
```

Python スクリプト実行

Flask が起動するのでウェブページへアクセス

ウェブページで必要事項を入力し CSV ファイルを選択

Enter を押すと、クレデンシャル等の必要事項を変数に置き換え

CSV ファイルを左上から 1つずつ順番に取り

オブジェクトなどは読み込んだ文字列を元に UUID を検索して  
変数へ置き換え

1行1ルールとしてすべての情報が揃ったら Access Rule として  
RestAPI の POST を使って設定追加

あとは CSV の最後の行までその繰り返し

# CSV ファイル

- API を通して設定出来るルール内容に制限は特に無いが、今回作成したコードでは以下の項目に絞って設定される形とした。

	A	B	C	D	E	F	G	H	I	J	K	L
1	action	enabled	ruleName	sendEventsToFMC	logBegin	logEnd	sourceZones	destinationZones	sourceNetworksObject	destinationNetworksObject	destinationPort_number	destinationPort_protocol
988	BLOCK_INTERACTIVE	FALSE	rule987	FALSE	FALSE	FALSE	inside	outside	Host-111	Range-77	1109	17
989	BLOCK_RESET_INTERACTIVE	TRUE	rule988	FALSE	FALSE	FALSE	inside	outside	Host-112	App-8	1110	17
990	ALLOW	TRUE	rule989	TRUE	TRUE	TRUE	inside	outside	Host-103	App-17	1111	17
991	ALLOW	TRUE	rule990	TRUE	TRUE	TRUE	inside	outside	Host-102	App-1	1112	17
992	TRUST	FALSE	rule991	FALSE	FALSE	FALSE	inside	outside	Network-110	App-3	1113	17
993	BLOCK	TRUE	rule992	FALSE	FALSE	FALSE	inside	outside	Network-111	App-4	1114	17
994	MONITOR	FALSE	rule993	FALSE	FALSE	FALSE	inside	outside	Network-112	App-5	1115	17
995	BLOCK_RESET	TRUE	rule994	FALSE	FALSE	FALSE	inside	outside	Host-31	Range-41	1116	17
996	ALLOW	TRUE	rule995	TRUE	TRUE	TRUE	inside	outside	Host-34	App-1	1117	17
997	TRUST	TRUE	rule996	FALSE	FALSE	FALSE	inside	outside	Network-107	App-3	1118	6
998	BLOCK	TRUE	rule997	FALSE	FALSE	FALSE	inside	outside	Network-108	App-4	1119	6
999	MONITOR	FALSE	rule998	FALSE	FALSE	FALSE	inside	outside	Network-109	App-5	1120	6
1000	BLOCK_RESET	TRUE	rule999	FALSE	FALSE	FALSE	inside	outside	Host-104	Range-72	1121	6
1001	BLOCK_INTERACTIVE	TRUE	rule1000	FALSE	FALSE	FALSE	inside	outside	Host-105	Range-73	1122	6

設定項目

合計 1000個のルールを一括作成

ALLOW  
TRUST  
BLOCK  
など  
計7種類

ルール名は任意の文字列を入力

Enabled  
SendEventsToFMC  
LogBegin  
などは "TRUE" と "FALSE" の 2 択

これらの項目は事前に作成済みのオブジェクト名を入力

送信先ポート番号とプロトコルを入力。プロトコルは "17 = UDP", "6 = TCP" となっている。

# API を使った ACP ルール追加実行例

## FirepowerManagementCenter ACP一括送信ツール

CSVの項目は既定されています。手帳書きを確認してからお試しください。  
以下の情報を入力して最後にENTERを押してください。

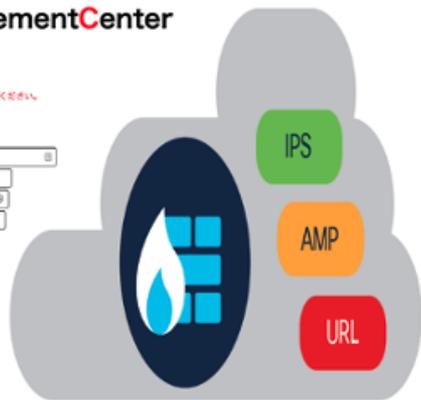
FMC IP Address :

Username :

Password :

ポリシー名 :

CSVファイル :



APIでACPとル  
ールを一括設定



Access Control Policy	Global	Targeting 0 devices	2022-07-25 01:52:43 Modified by "admin"
API_Policy	Global	Targeting 0 devices	2022-07-25 01:52:43 Modified by "admin"
Common_ACP	Global	Targeting 0 devices	2022-03-15 23:29:02 Modified by "Firepower System"
demo_policy	Global	Targeting 0 devices	2022-03-15 23:29:02 Modified by "Firepower System"



ACP 内のルールを確認

合計 1000行のルールが CSV ファイル  
通り設定されていることを確認

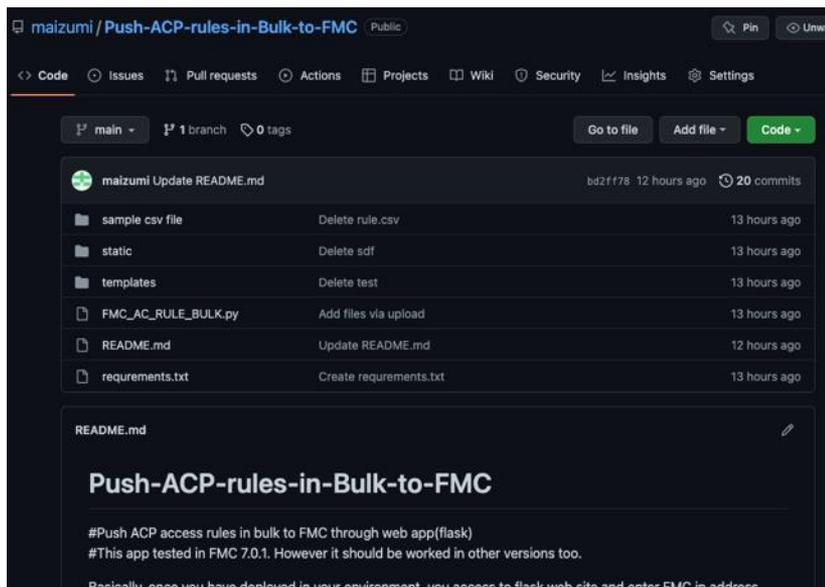


#	Name	Source Zones	Dest Zones	Source Network...	Dest Network...	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source Dynamic Attrib...	Destin... Dynamic Attrib...	Action
1	Mandatory - API_Policy (-)													
5	rule5	inside	outside	Host-104	App-5	Any	Any	Any	Any	UDP (17:1)	Any	Any	Any	Allow
6	rule6	inside	outside	Host-105	App-5	Any	Any	Any	Any	UDP (17:1)	Any	Any	Any	Trust
7	rule7	inside	outside	Host-106	App-8	Any	Any	Any	Any	UDP (17:1)	Any	Any	Any	Block
8	rule8	inside	outside	Host-101	App-1	Any	Any	Any	Any	UDP (17:1)	Any	Any	Any	Deny
9	rule9	inside	outside	Network-8	App-3	Any	Any	Any	Any	UDP (17:1)	Any	Any	Any	Block
10	rule10	inside	outside	Network-8	App-4	Any	Any	Any	Any	UDP (17:1)	Any	Any	Any	Deny
11	rule11 (Download)	inside	outside	Network-8	App-5	Any	Any	Any	Any	UDP (17:1)	Any	Any	Any	Deny

# GitHub

コードは Github の以下のリンクからダウンロード可能

<https://github.com/maizumi/Push-ACP-rules-in-Bulk-to-FMC>



# FMC API 参考資料

## 【[FMC] API Explorer の利用方法のご紹介】

<https://community.cisco.com/t5/-/-/ta-p/4386563>

## 【Firepower Management Center Programming Guides】

<https://www.cisco.com/c/en/us/support/security/defense-center/products-programming-reference-guides-list.html>

## 【FMC REST API インタラクションの認証トークンの生成方法】

[https://www.cisco.com/c/ja\\_jp/support/docs/security/firepower-management-center/215918-how-to-generate-authentication-token-for.html](https://www.cisco.com/c/ja_jp/support/docs/security/firepower-management-center/215918-how-to-generate-authentication-token-for.html)

## 【Push Objects in Bulk to FMC using REST-API】

<https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215972-push-objects-in-bulk-to-fmc-using-rest-a.html>

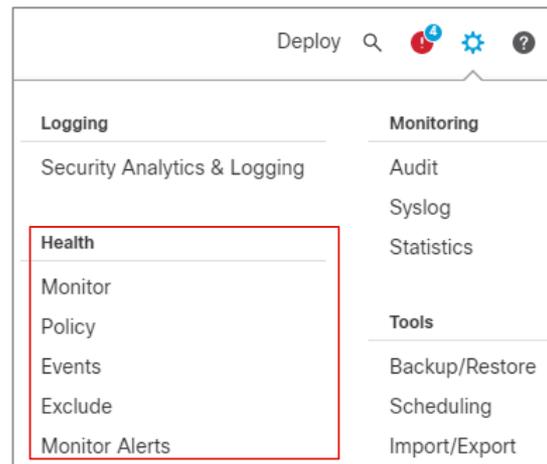
## 【fmcapi】

<https://developer.cisco.com/codeexchange/github/repo/daxm/fmcapi/>

# 16. システム監視

# システム監視概要

- System > Health: システム監視へのアクセス
- システム監視は、FMC にて管理されるすべてのデバイス、および FMC 自身のヘルスステータスを提供
- システム監視構成要素
  - Monitor: ヘルスステータスの監視
  - Policy: ヘルスポリシーの作成/カスタマイズ
  - Events: ヘルスイベントの表示
  - Exclude: ヘルスマニター監視対象から外す
  - Monitor Alerts: 設定されたヘルスイベントの閾値に合致した場合のアラート方法の作成/カスタマイズ



# Health Monitor 概要

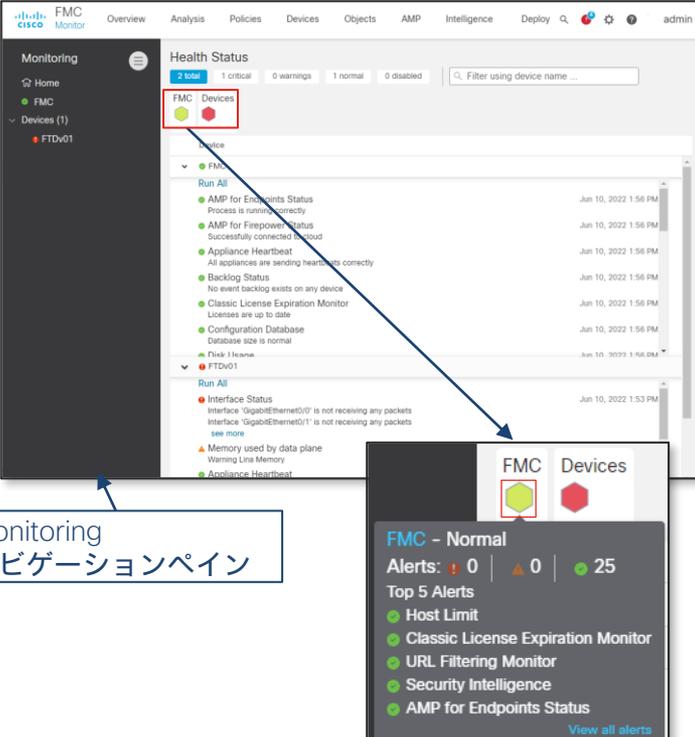
## ・ モニターホーム画面

- ・ Health Status サマリページ: FMC とすべての管理デバイスのヘルス状況を確認

- ・  にマウスオーバーすると、FMC/管理デバイスのそれぞれのヘルス概要が表示。または、> マークにてヘルス詳細を確認。

- ・  正常。アラームはなし
- ・  注意。一つ以上のアラームが表示
- ・  重大。一つ以上のアラームが表示

- ・ Monitoring ナビゲーションペインでは個々のデバイスのヘルス状況を確認



The screenshot displays the Cisco FMC Monitor interface. The 'Health Status' section shows a summary of health indicators for FMC and Devices. A red box highlights the 'FMC Devices' status indicator. A blue arrow points from this indicator to a detailed view of the FMC status, which shows 'FMC - Normal' and lists the top 5 alerts: Host Limit, Classic License Expiration Monitor, URL Filtering Monitor, Security Intelligence, and AMP for Endpoints Status.

Monitoring ナビゲーションペイン

FMC Devices

FMC - Normal  
Alerts: 0 0 25  
Top 5 Alerts  
● Host Limit  
● Classic License Expiration Monitor  
● URL Filtering Monitor  
● Security Intelligence  
● AMP for Endpoints Status  
[View all alerts](#)

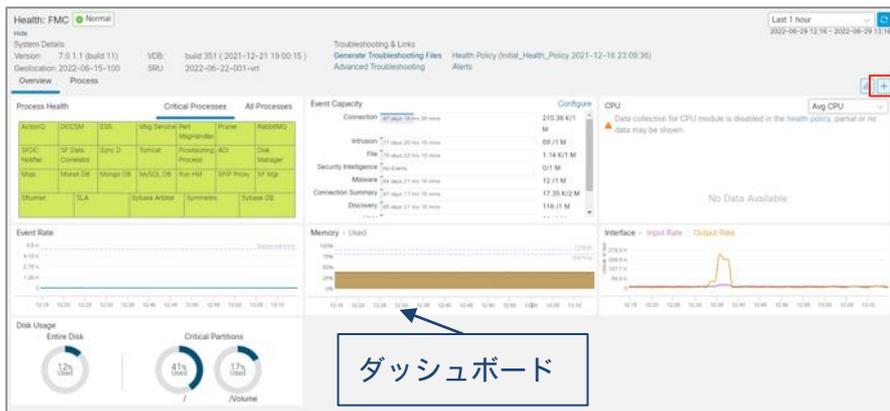
# Monitoring ナビゲーションペイン

- System > Health > Monitor > Home
  - アクセス時に表示される FMC/FTD のサマリページ
- System > Health > Monitor > FMC
  - FMC のヘルス状況のサマリページ
- System > Health > Monitor > Devices
  - 管理デバイス個々のヘルス状況のサマリページ
- それぞれのサマリページに表示されるダッシュボードは利用状況に合わせ、追加削除が可能



# Monitoring: FMC ヘルスモニター

Add Dashboard  
ダッシュボードの追加ができる

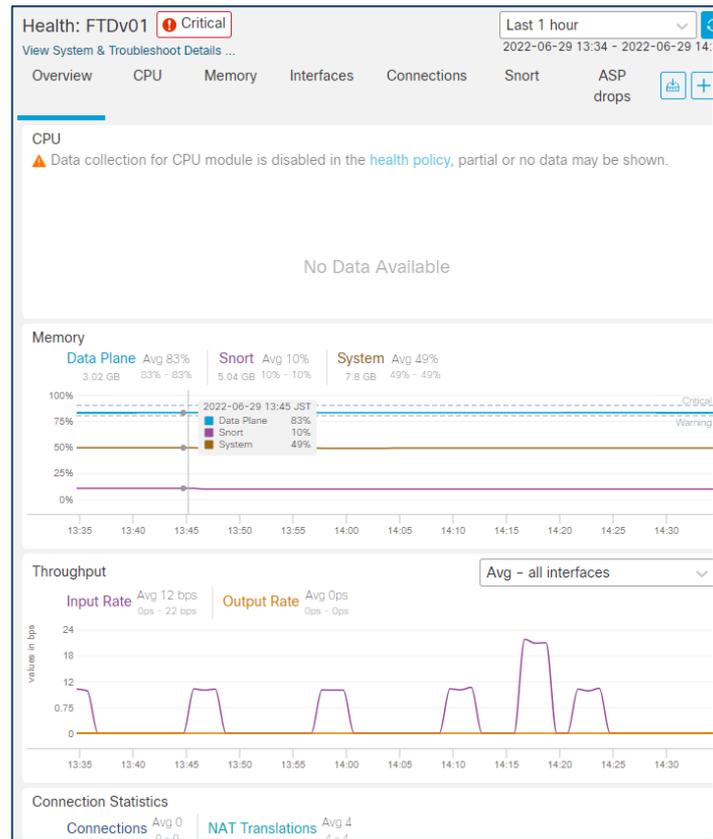


- System > Health > Monitor > FMC (デフォルトのダッシュボード)
  - Process Health: FMC 内で使用しているプロセスのヘルス状況
  - Event Capacity: FMC の Database 使用状況 (System > Configuration > Database にて変更可)
  - CPU: CPU 使用率
  - Event Rate: 時間軸に対する Event 数
  - Memory: メモリ使用率
  - Interface: Input/Output パケット状況
  - Disk Usage: ディスク使用率

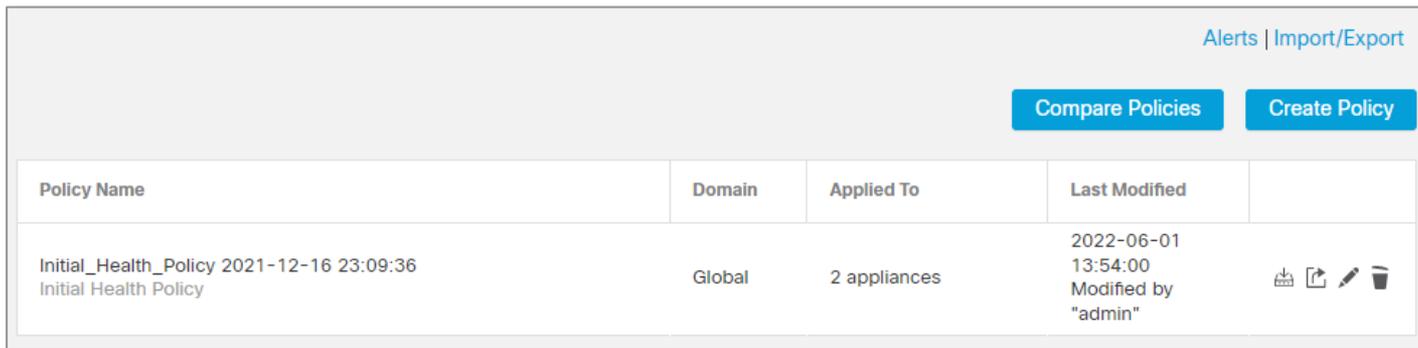
- FMC 各プロセスの状況を表示
  - Memory Usage
  - CPU Utilization
  - Restart count
  - Swap Memory

# Monitoring: 管理デバイスヘルスマニター

- Overview: CPU/Memory/Throughput などの概要を表示
- CPU: CPU 使用率 (Control Point、snort などの CPU 使用率)
- Memory: メモリ使用率 (Dataplane、snort などのメモリ使用率)
- Interfaces: インターフェースに関する使用率やエラーなど
- Connections: ピーク時のコネクション数や、TCP/UDP のコネクションス
- snort: snort フローに関する情報やパケット数など
- ASP drops: ASP 機能にてドロップされたパケット情報



# Health Policy 概要



The screenshot shows a web interface for managing Health Policies. At the top right, there are links for "Alerts" and "Import/Export". Below these are two blue buttons: "Compare Policies" and "Create Policy". The main content is a table with the following data:

Policy Name	Domain	Applied To	Last Modified	
Initial_Health_Policy 2021-12-16 23:09:36 Initial Health Policy	Global	2 appliances	2022-06-01 13:54:00 Modified by "admin"	   

- ヘルスモジュール (監視機能) の有効/無効化や閾値のポリシーの設定ができる
- FMC セットアップ時に “Initial\_Health\_policy年月日時間” の初期ポリシーが作成され、FMC および管理デバイスに適用される
- 初期ポリシーはデフォルトポリシーを基に作成される
- デフォルトポリシーは、閲覧/編集は出来ないが、ポリシー作成の際、デフォルトポリシーの複製は可能
- FMC のアップグレードにてヘルスポリシーのモジュールに変更/追加があった場合は、最新のポリシーがデフォルトポリシー、初期ポリシー、カスタムポリシー (作成した場合) へ適用される

# Health Policy 作成

Alerts | Import/Export

Compare Policies Create Policy

Create Policy

Copy Policy

Initial\_Health\_Policy 2021-12-1

Initial\_Health\_Policy 2021-12-16 23:09:36

Default Health Policy

New Policy Description

Cancel Save

Create Policy

Copy Policy

Default Health Policy

New Policy Name

test\_policy

New Policy Description

Health monitor for test purpose

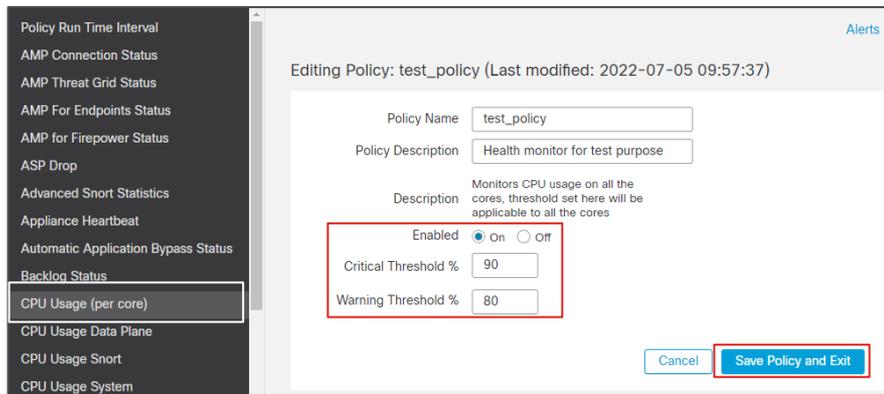
Cancel Save

Policy Name	Domain	Applied To	Last Modified	
Initial_Health_Policy 2021-12-16 23:09:36 Initial Health Policy	Global	2 appliances	2022-06-30 12:04:02 Modified by "admin"	📄 📄 🗑️
test_policy Health monitor for test purpose	Global	None	2022-07-05 09:57:36 Modified by "admin"	📄 📄 🗑️

- Health Policy の作成は以下の手順で行う
  - System > Health > Policy > Create Policy を選択
    - 引用するポリシーの選択
    - New Policy Name: ポリシー名
    - New Policy Description: ポリシー説明
    - Save

# Health Policy 更新または修正

Policy Name	Domain	Applied To	Last Modified	
Initial_Health_Policy Initial Health Policy	Global	2 appliances	2022-06-30 12:04:02 Modified by "admin"	   
test_policy Health monitor for test purpose	Global	None	2022-07-05 09:57:36 Modified by "admin"	   



Policy Run Time Interval

AMP Connection Status

AMP Threat Grid Status

AMP For Endpoints Status

AMP for Firepower Status

ASP Drop

Advanced Snort Statistics

Appliance Heartbeat

Automatic Application Bypass Status

Backlog Status

CPU Usage (per core)

CPU Usage Data Plane

CPU Usage Snort

CPU Usage System

Alerts

Editing Policy: test\_policy (Last modified: 2022-07-05 09:57:37)

Policy Name

Policy Description

Description

Enabled  On  Off

Critical Threshold %

Warning Threshold %

- Health Policy の更新または修正は以下の手順で行う
  - 更新/修正をするポリシーを選択し、鉛筆マーク (Edit) ボタンを押す
  - 修正を加えるポリシーを選択
    - 有効/無効の選択
    - 閾値の設定
  - Save Policy and Exit (他にも修正があれば上記内容を繰り返す)

# Health Policy をアプライアンスに適用

Policy Name	Domain	Applied To	Last Modified	
Initial_Health_Policy 2021-12-16 23:09:36 Initial Health Policy	Global	2 appliances	2022-06-30 12:04:02 Modified by "admin"	  
test_policy Health monitor for test purpose	Global	None	2022-07-05 10:08:39 Modified by "admin"	  

Apply ボタン

Policy Name	Domain	Applied To	Last Modified	
Initial_Health_Policy 2021-12-16 23:09:36 Initial Health Policy	Global	None	2022-06-30 12:04:02 Modified by "admin"	  
test_policy Health monitor for test purpose	Global	2 appliances	2022-07-05 10:08:39 Modified by "admin"	  

Name test\_policy  
Description Health monitor for test purpose  
Last Modified Tue Jul 5 10:08:40 2022

By Group

▼ Ungrouped (2 total)

FMCv01  
10.71.132.204 - Cisco Firepower Management Center for VMware v7.0.1.1

FTDv01  
10.71.132.194 - Cisco Firepower Threat Defense for VMware v7.0.1.1

Apply

- Health Policy のアプライアンスへの適用は以下の手順で行う
  - アプライアンスに適用するポリシーを選択し Apply ボタンを押す
  - 適用するアプライアンスにチェックを入れる
    - Apply にてポリシーの適用完了

# Health Event 概要

The screenshot shows the AMP Health Monitor interface. On the left is a navigation menu with categories: Logging, Security Analytics & Logging, Health, Monitor, Policy, Events (highlighted with a red box), Exclude, and Monitor Alerts. The main area displays a 'Table View of Health Events' for the period 2022-07-05 12:54:48 - 2022-07-05 13:58:17. A red arrow points from the 'Events' menu item to a specific row in the table. A second screenshot on the right shows a zoomed-in view of the selected event row, with another red arrow pointing to the 'Module Name' column header.

Module Name	Test Name	Time	Description	Value	Units	Status	Device
Memory Usage	Memory Usage - Memory Test	2022-07-05 13:57:56	Normal System Memory	40	n/a	✓	FMCv01
Memory Usage	Memory Usage - Memory Test	2022-07-05 13:57:55	Normal System Memory	48	n/a	✓	FTDv01
Memory Usage	Memory Usage - Memory Test	2022-07-05 13:55:55	Normal System Memory	40	n/a	✓	FMCv01
Memory Usage	Memory Usage - Memory Test	2022-07-05 13:55:55	Normal System Memory	48	n/a	✓	FTDv01
Memory Usage	Memory Usage - Memory Test	2022-07-05 13:53:56	Normal System Memory	40	n/a	✓	FMCv01
Memory Usage	Memory Usage - Memory Test	2022-07-05 13:53:55	Normal System Memory	49	n/a	✓	FTDv01
Memory Usage	Memory Usage - Memory Test	2022-07-05 13:51:56	Normal System Memory	40	n/a	✓	FMCv01

- System > Health > Events
- FMC のヘルスマニターにてログに記録されたヘルスイベントを表示
- イベントはカスタマイズ可能となり、目的により見易さを調整できる
- テーブルのイベントの一つを選択すると、そのイベントに関するログを確認できる

# Health Exclude 概要

The screenshot displays the Cisco AMP interface for configuring health exclusions. The left sidebar shows the navigation menu with 'Exclude' highlighted. The main content area shows a list of ungrouped devices with checkboxes and edit icons. At the bottom, there are buttons for 'Clear Exclude on Selected Devices' and 'Exclude Selected Devices'.

Device Name	IP Address	Device Type
<input type="checkbox"/> FMCv01	10.71.132.204	Cisco Firepower Management Center for VMware v7.0.1.1
<input type="checkbox"/> FTDv01	10.71.132.194	Cisco Firepower Threat Defense for VMware v7.0.1.1

- System > Health > Exclude
- ヘルス監視の対象から除外するための設定
- デバイス毎での除外、ヘルスマジュール毎での除外リストの作成が可能

# Health Exclude - ヘルスモジュール単位での除外

FTDv01  
10.71.132.194 - Cisco Firepower Threat  
Defense for VMware v7.0.1.1

Clear Exclude on Selected Devices Exclude Selected Devices

Editing Health Exclude for: FTDv01

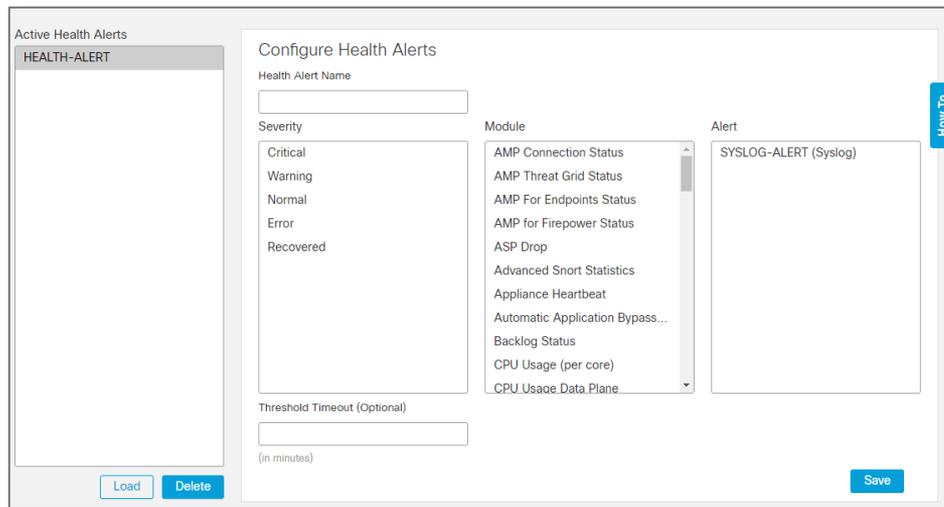
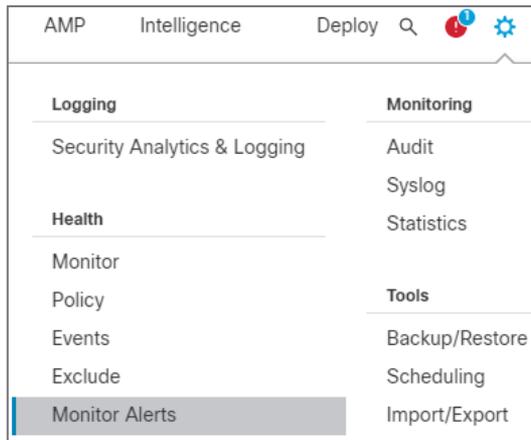
Modules

- Advanced Snort Statistics
- AMP Connection Status
- AMP for Endpoints Status
- AMP for Firepower Status
- AMP Threat Grid Status
- Appliance Heartbeat
- ASP Drop
- Automatic Application Bypass Status
- Backlog Status
- Card Reset
- Chassis Status FTD
- Cluster/Failover Status
- Configuration Database
- Configuration Memory Allocation
- Connection Statistics
- CPU Usage Data Plane
- CPU Usage Snort
- CPU Usage System
- Critical Process Statistics
- Deployed Configuration Statistics
- Disk Status
- Disk Usage
- Event Stream Status
- File System Integrity Check
- Flow Offload
- FMC Access Configuration Changes
- FMC HA Status
- FTD HA Status
- Hardware Alarms
- Health Monitor Process
- Host Limit
- Inline Link Mismatch Alarms
- Interface Status
- Intrusion and File Event Rate
- ISE Connection Status Monitor
- Link State Propagation
- Local Malware Analysis
- Memory Usage
- Memory Usage Data Plane
- Memory Usage Snort
- MySQL Status
- NTP Status FTD
- Platform Faults
- Power Supply
- Process Status
- RabbitMQ Status
- Realm
- Reconfiguring Detection
- Routing Statistics
- RRD Server Process
- Security Intelligence
- Smart License Monitor
- Snort Identity Memory Usage
- Snort Statistics
- SSE Connection Status
- Sybase Status
- Threat Data Updates on Devices
- Time Series Data Monitor
- Time Synchronization Status
- Unresolved Groups Monitor
- URL Filtering Monitor
- User Agent Status (deprecated)
- VPN Statistics
- VPN Status
- xTLS Counters

Back Save

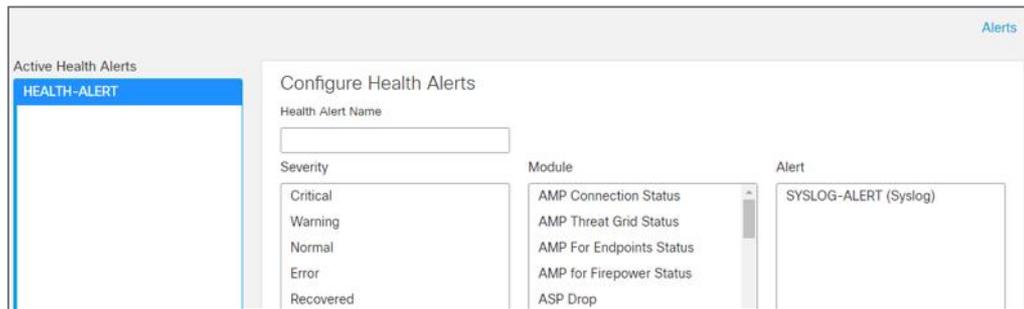
- Edit ボタンにて監視対象外のヘルスマジュールを選択
- Save ボタンにて除外リストの保存
- 各モジュールの詳細については Appendix 参照

# Health Monitor Alerts 概要①



- System > Health > Monitor Alerts
- ヘルスポリシーのモジュールステータスが変更された際、Email、SNMP、またはシステムログを介して通知するアラートの設定
- Default では HEALTH-ALERT が作成され、それぞれのモジュールに対して、Syslog にて Alert を送信するよう設定されている

# Health Monitor Alerts 概要②



- ヘルスモニターによって生成されるアラートには、以下の情報を含む
  - Severity: アラートの重大度レベル。それぞれの重大度レベルに達した場合のアクションを次項で選択
  - Module: 監視結果のアラートをトリガーするヘルスマジュールの指定
  - Alert: 指定した重大度レベルに達した際の通知方法を選択

# Health Monitor Alerts – 設定方法

Active Health Alerts

HEALTH-ALERT

Configure Health Alerts

Health Alert Name

Severity

- Critical
- Warning
- Normal
- Error
- Recovered

Module

- AMP Connection Status
- AMP Threat Grid Status
- AMP For Endpoints Status
- AMP for Firepower Status
- ASP Drop
- Advanced Snort Statistics
- Appliance Heartbeat
- Automatic Application Bypass...
- Backlog Status
- CPU Usage (per core)
- CPU Usage Data Plane

Alert

- SYSLOG-ALERT (Syslog)

Threshold Timeout (Optional)

(in minutes)

Load Delete Save

Health Alert Name: 通知定義を新たに作成する際に入力

Severity: 通知を行う際の重大度の選択(複数選択可)

Module: 必要なヘルスマジュールを選択(複数選択可)

Alert: 通知方法を選択

# Health Monitor Alerts – Alerts 追加設定方法

Active Health Alerts

HEALTH-ALERT

Alerts

### Configure Health Alerts

Health Alert Name

Severity

Critical  
Warning  
Normal  
Error  
Recovered

Module

AMP Connection Status  
AMP Threat Grid Status  
AMP For Endpoints Status  
AMP for Firepower Status  
ASP Drop  
Advanced Snort Statistics  
Appliance Heartbeat  
Automatic Application Bypass...  
Backlog Status  
CPU Usage (per core)  
CPU Usage Data Plane

Alert

SYSLOG-ALERT (Syslog)

Threshold Timeout (Optional)

(in minutes)

Load Delete Save

- 通知方法を追加する場合は、Alerts を選択し設定
- 設定方法は 17章「アラート設定」を参照

# Appendix: Health Policy モジュール

- Health Policy では以下のモジュールが用意され、カスタマイズが可能

No.	カテゴリ	説明	デフォルト値
1	Policy Run Time Interval	<ul style="list-style-type: none"><li>• ヘルスチェック間隔の設定</li><li>• 7.0 以降のデバイスには Run Time Interval の値が適用される</li><li>• 7.0 以前のデバイスには Legacy Run Time Interval の値が適用される</li></ul>	<ul style="list-style-type: none"><li>• 1分 (Run Time Interval)</li><li>• 5分</li></ul>
2	AMP Connection Status	<ul style="list-style-type: none"><li>• FTD から AMP クラウドへの接続が失敗した際にアラートを通知</li></ul>	無効
3	AMP Threat Grid Status	<ul style="list-style-type: none"><li>• FTD から AMP Threat Grid クラウドへの接続が失敗した際にアラートを通知</li></ul>	有効
4	AMP for Endpoints Status	<ul style="list-style-type: none"><li>• FMC から AMP クラウドへの接続が失敗した際にアラートを通知</li></ul>	有効
5	AMP for Firepower Status	<ul style="list-style-type: none"><li>• 以下の条件にマッチした場合にアラートを通知<ul style="list-style-type: none"><li>• FMC から AMP クラウドおよび AMP Threat Grid クラウドへの接続が失敗した場合</li><li>• 接続時の暗号化キーが無効の場合</li><li>• Threat Grid への動的分析によるファイル転送が失敗した場合</li></ul></li></ul>	有効
6	ASP Drop	<ul style="list-style-type: none"><li>• ASP (accelerated security path) にてコネクションがドロップした場合にアラートを通知</li></ul>	有効
7	Advanced Snort Statistics	<ul style="list-style-type: none"><li>• Advanced Snort の統計情報を監視</li></ul>	

# Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
8	Appliance Heartbeat	<ul style="list-style-type: none"><li>デバイスからのハートビートの受信をチェックし、ハートビートのステータスに基づいてアラートを通知</li></ul>	有効
9	Automatic Application Bypass Status	<ul style="list-style-type: none"><li>アプリケーションバイパス機能が実行されたかどうかを監視</li></ul>	有効
10	Backlog Status	<ul style="list-style-type: none"><li>管理デバイスから FMC へイベント送信の際、データのバックログが 30分以上連続して増加している場合にアラートを通知</li></ul>	有効
11	CPU Usage (per core)	<ul style="list-style-type: none"><li>FTD のすべてのコアの CPU 使用率の負荷を監視し、CPU 使用率の閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>無効</li><li>Critical Threshold 90%</li><li>Warning Threshold 80%</li></ul>
12	CPU Usage Data Plane	<ul style="list-style-type: none"><li>FTD のすべてのデータプレーンプロセスの平均 CPU 使用率の負荷を監視し、CPU 使用率の閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>Critical Threshold 90%</li><li>Warning Threshold 80%</li></ul>
13	CPU Usage Snort	<ul style="list-style-type: none"><li>FTD の Snort プロセスの平均 CPU 使用率の負荷を監視し、CPU 使用率の閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>Critical Threshold 90%</li><li>Warning Threshold 80%</li></ul>

# Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
14	CPU Usage System	<ul style="list-style-type: none"><li>FTD のシステムプロセスの平均 CPU 使用率の負荷を監視し、CPU 使用率の閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>Critical Threshold 90%</li><li>Warning Threshold 80%</li></ul>
15	Card Reset	<ul style="list-style-type: none"><li>ネットワークカードがハード故障などにより再起動し、リセットした場合にアラートを通知</li></ul>	無効
16	Chassis Status FTD	<ul style="list-style-type: none"><li>Firepower2100/1000シリーズ 用</li><li>シャーシパラメータ (ファン速度や温度など) を監視</li><li>設定した閾値を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>有効</li><li>Critical Chassis Temperature 85%</li><li>Warning Chassis Temperature 75%</li></ul>
17	Cluster/Failover Status	FTD にて以下のイベントが発生した場合にアラートを通知 <ul style="list-style-type: none"><li>新しい Primary デバイスが導入された際</li><li>新しい Secondary デバイスが Failover にジョインした際</li><li>Primary/Secondary のどちらかが Failover から外れた場合</li></ul>	有効
18	Configuration Database	<ul style="list-style-type: none"><li>FMC の設定データベースのサイズを監視し、データベースサイズが閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>Critical Threshold 50%</li><li>Warning Threshold 15%</li></ul>

# Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
19	Configuration Memory Allocation	• FTD において、デプロイされた設定サイズによってデバイスがメモリ不足になるリスクがある場合にアラートを通知	有効
20	Connection Statistics	• FTD のコネクション統計情報および NAT 変換の数を監視	有効
21	Critical Process Statistics	• FTD の重要なプロセスの状態、それらのリソース消費および再起動の数を監視	有効
22	Deployed Configuration Statistics	• FTD がにデプロイされた ACE の数や IPS ルールなどの統計情報を監視	有効
23	Disk Status	• アプライアンス上のハードディスクとマルウェアストレージパック (インストールされている場合) のパフォーマンスを監視	有効
24	Disk Usage	• アプライアンス上のハードディスクとマルウェアストレージパック (インストールされている場合) の使用率が閾値 (%) を超えた場合にアラートを通知	• 有効 • Critical Threshold 90% • Warning Threshold 85% • 2HD Critical Threshold 99% • 2 HD Warning Threshold 97%

# Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
25	Event Stream Status	• FMC にて登録した外部の Event ログサーバのステータスを監視	有効
26	FMC Access Configuration Changes	• FMC にアクセスを行い configure network management-data-interface コマンドでの設定変更を監視	有効
27	FMC HA Status	• FMC の HA ステータスおよび同期状況を監視	有効
28	FTD HA Status	• FTD の HA ステータスを監視	無効
29	File System Integrity Check	• ファイルシステムの整合性を確認し、またシステムが CC モード/UCAPL モードが有効、またはシステムが DEV キーにて署名されたイメージを実行する場合に監視	有効
30	Flow Offload	• firepower 4100/9300 に対してオフロードの統計情報を監視	有効
31	Hardware Alarms	• FTD (物理デバイス) のハードウェア交換が必要かの判断およびハードウェアのステータスに基づいてアラートを通知。また、ハードウェア関連のデーモンステータスについても報告。	有効
32	Health Monitor Process	• ヘルスモニター自体のステータスを監視し、FMC が最後に受信したヘルスイベントからの分数が警告またはクリティカルの制限を超えた場合にアラートを通知	• 無効 • Critical Minutes since last event 60 • Warning Minutes since last event 30

# Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
33	Host Limit	<ul style="list-style-type: none"><li>FMC が監視可能なホスト数の制限に近づいているかどうかを判断し、閾値に基づいてアラートを通知</li></ul>	<ul style="list-style-type: none"><li>有効</li><li>Critical number Hosts 10</li><li>Warning number Hosts 50</li></ul>
34	ISE Connection Status Monitor	<ul style="list-style-type: none"><li>FMC と ISE 間の接続状況を監視</li></ul>	有効
35	Inline Link Mismatch Alarms	<ul style="list-style-type: none"><li>インラインセットに関連付けられたポートを監視し、インラインペア2つのインターフェースが異なる速度にてネゴシエーションが発生した場合にアラートを通知</li></ul>	有効
36	Interface Status	<ul style="list-style-type: none"><li>物理インターフェイスと集約インターフェイスのトラフィックステータスに基づき、トラフィックとアラートを収集出来ているか監視</li></ul>	有効
37	Intrusion and File Event Rate	<ul style="list-style-type: none"><li>1秒あたりの IPS イベントの数が閾値と比較し、閾値を超えた場合にアラートを通知。</li></ul>	<ul style="list-style-type: none"><li>有効</li><li>Events per second (Critical) 50</li><li>Events per second (Warning)</li></ul>

# Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
38	Link State Propagation	<ul style="list-style-type: none"><li>FTD モジュールを付けた ASA5500/ISA 3000 シリーズにおいて、インラインセットのリンクがフェイルした場合や、リンクプロパゲーションモードがトリガーした際にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>有効</li><li>Critical number Hosts 10</li><li>Warning number Hosts 50</li></ul>
39	Local Malware Analysis	<ul style="list-style-type: none"><li>ローカルマルウェア解析の動作の監視</li></ul>	有効
40	Memory Usage	<ul style="list-style-type: none"><li>メモリ使用量を監視し、メモリ使用率の閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>有効</li><li>Critical Threshold 90%</li><li>Warning Threshold 80%</li></ul>
41	Memory Usage Dataplane	<ul style="list-style-type: none"><li>Dataplane にて使用されるメモリ使用率が閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>Critical Threshold 90%</li><li>Warning Threshold 80%</li></ul>
42	Memory Usage Snort	<ul style="list-style-type: none"><li>Snort にて使用されるメモリ使用率が閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>Critical Threshold 90%</li><li>Warning Threshold 80%</li></ul>

# Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
43	MySQL Status	• MySQL データベースの監視	有効
44	NTP Status FTD	• FTD の NTP 時刻の同期を監視	無効
45	Platform Faults	• Firepower1000/2100 にて障害が発生した場合にアラートを通知	無効
46	Power Supply	• FMC の電源を監視しステータスに基づいてアラートを通知	有効
47	Process Status	• プロセスを監視しステータスに基づいてアラートを通知	有効
48	RRD Server Process	• FMC 内部で稼働している RRDtools の状態を監視し、設定した閾値に該当するプロセスの再起動が確認された場合にアラートを通知	• 有効 • Critical Number of restarts 3 • Warning Number of restarts 2
49	RabbitMQ Status	• FMC にて RabbitMQ ステータスの監視	有効
50	Realm	• レルムまたはユーザの不一致が閾値 (%) を超えた場合にアラートを通知	• 無効 • Warning Users mismatch Threshold % 50
51	Reconfiguring Detection	• 管理デバイスにて再設定がフェイルした場合にアラートを通知	• 有効
52	Routing Statistics	• FMC にて既存のルーティングテーブルの監視	• 有効

# Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
53	SSE Connection Status	<ul style="list-style-type: none"><li>管理デバイスが SSE クラウドへ初期の接続が成功した後、その後クラウドへ接続できない場合にアラートを通知</li></ul>	無効
54	Security Intelligence	<ul style="list-style-type: none"><li>セキュリティインテリジェンスを使用し、かつ FMC がフィードを更新できない、フィードデータが破損している、または認識可能な IP アドレスが含まれていない場合にアラートを通知</li></ul>	有効
55	Smart License Monitor	FMC の Smart Licensing Agent と Smart Software Manager 間にて以下のエラーが発生した場合にアラートを通知 <ul style="list-style-type: none"><li>Product Instance Registration Token の有効期限が切れた場合</li><li>Smart License の使用が準拠していない場合</li><li>Smart License の認証または評価ライセンスの有効期限が切れた場合</li></ul>	有効
56	Snort Identity Memory Usage	<ul style="list-style-type: none"><li>Snort ID 処理のメモリ使用率の閾値 (%) を超えた場合にアラートを通知</li></ul>	<ul style="list-style-type: none"><li>有効</li><li>Critical Threshold 80%</li></ul>
57	Snort Statistics	<ul style="list-style-type: none"><li>FTD にてイベント、フロー、パケットの Snort 統計情報を監視</li></ul>	有効
58	Sybase Status	<ul style="list-style-type: none"><li>FMC にて Sybase のデータベースを監視</li></ul>	有効
59	Threat Data Updates on Devices	<ul style="list-style-type: none"><li>脅威データの更新がクラウドから FMC へ 30分毎に更新される。もし、指定した期間内に本情報が更新されなかった場合、アラートを通知</li></ul>	<ul style="list-style-type: none"><li>有効</li><li>Send critical alert after (hours) 24</li><li>Send warning alert after (hours) 1</li></ul>

# Appendix: Health Policy モジュール

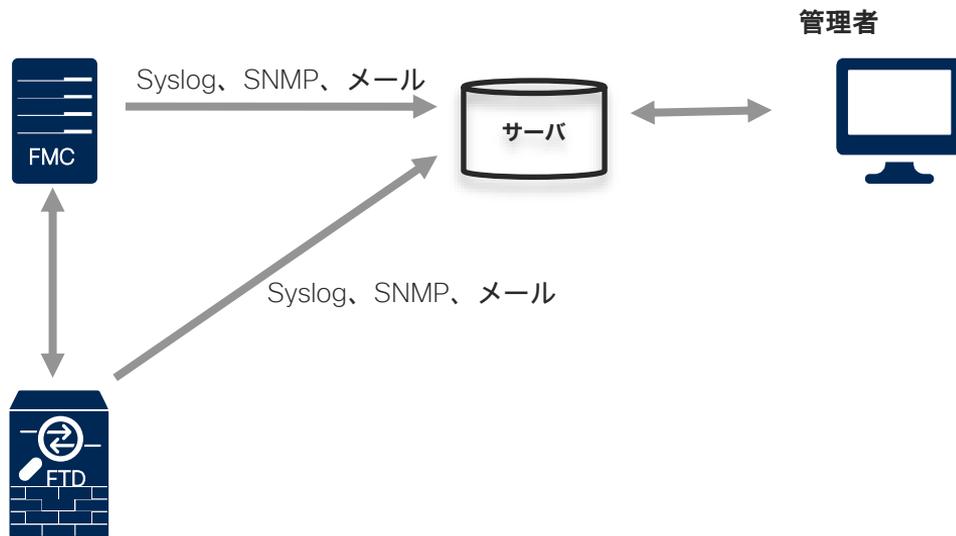
No.	カテゴリ	説明	デフォルト値
60	Time Series Data Monitor	<ul style="list-style-type: none"><li>• FMC の時系列データ (相関イベントカウントなど) が保存されているディレクトリ内にて、破損したファイルの存在をトラッキングし、ファイルに破損フラグが付けられて削除された場合にアラートを通知</li></ul>	有効
61	Time Synchronization Status	<ul style="list-style-type: none"><li>• NTP を使用して時刻を取得するデバイスクロックと NTP サーバのクロックとの同期を追跡し、クロックの差が10秒を超える場合にアラートを通知</li></ul>	有効
62	URL Filtering Monitor	<p>FMC が以下の条件にマッチした場合、アラートを通知</p> <ul style="list-style-type: none"><li>• Cisco クラウドへの登録に失敗</li><li>• URL 脅威データの更新をクラウドからダウンロードできない</li><li>• URL ルックアップが出来ない</li></ul>	<ul style="list-style-type: none"><li>• 有効</li><li>• Send critical alert after (hours) 24</li><li>• Send warning alert after (hours) 1</li></ul>
63	Unresolved Groups Monitor	<ul style="list-style-type: none"><li>• ポリシー適用外のグループを監視</li></ul>	有効
64	User Agent Status (deprecated)	<ul style="list-style-type: none"><li>• ユーザエージェントの監視</li><li>• ただし、FMC 6.7 以前の機能であり、7.x では使用されない</li></ul>	有効
65	VPN Statistics	<ul style="list-style-type: none"><li>• Site to Site VPN や Remote Access VPN のトンネル統計情報を監視</li></ul>	有効
66	VPN Status	<ul style="list-style-type: none"><li>• Site to Site VPN や Remote Access VPN のトンネルの状態を監視</li><li>• トンネルダウンを検知した場合アラートを通知</li></ul>	有効
67	xTLS Counters	<ul style="list-style-type: none"><li>• xTLS/SSL フロー、メモリー、キャッシュの有効性を監視</li></ul>	無効

# 17. Syslog ・ レポート ・ アラートの設定

# Syslog 設定

# ロギング概要

- 各種アラート、イベントは FMC 内部へ保存し、FMC GUI で表示するほかに、外部サーバへ通知を送ることが可能
- 本資料では Syslog サーバへのロギングを中心に記載



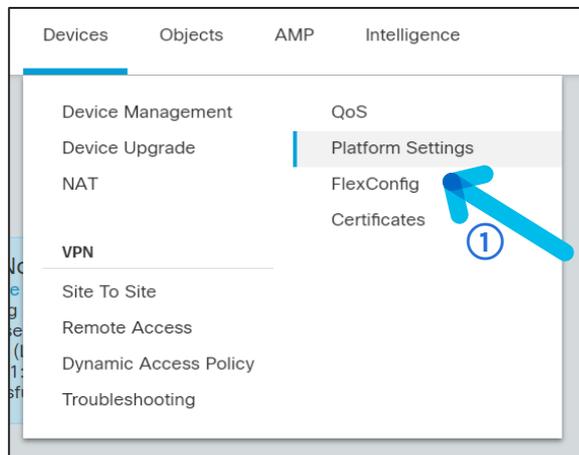
# 設定の流れ

- ステップ1 : Logging Setup 設定
- ステップ2 : Logging Destination 設定
- ステップ3 : Syslog Settings 設定
- ステップ4 : Syslog Servers 設定

Syslog サーバが、FMC より疎通の取れるネットワークセグメントに構築してある前提とする

# Logging Setup 設定

## ・ロギングの設定



- ① Device > Platform Settings をクリック
- ② 作成済みの FTD-Policy の鉛筆マークをクリック

Platform Settings	Device Type	Status	
FTD-Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices	

②

# Logging Setup 設定 (続き)

FTD-Policy You have unsaved changes [Save](#) [Cancel](#)

Enter Description Policy Assignments (1)

Logging Setup | Logging Destinations | Email Setup | Event Lists | Rate Limit | Syslog Settings | Syslog Servers

### Basic Logging Settings

- Enable Logging
- Enable Logging on the failover standby unit
- Send syslogs in EMML format
- Send debug messages as syslogs

Memory Size of the Internal Buffer

(4096-52428800 Bytes)

### VPN Logging Settings

- Enable Logging to FMC

Logging Level

### Specify FTP Server Information

- FTP Server Buffer Wrap

③ Syslog を選択

④ Enable Logging にチェック

- 左側メニューで SMTP Server、SNMP をクリックすることでメール、SNMP 設定が可能

# Logging Destination 設定

- ログの送付先を指定

FTD-Policy  
Enter Description

Save Cancel

Policy Assignments (1)

Logging Setup **Logging Destinations** Email Setup Event Lists Rate Limit Syslog Settings Syslog Servers

Logging Destination	Syslog from All Event Class	Syslog from specific Event Class

No records to display

+ Add

Add Logging Filter

Logging Destination Syslog Servers

Event Class Internal Buffer

Console

**Syslog Servers**

SNMP Trap

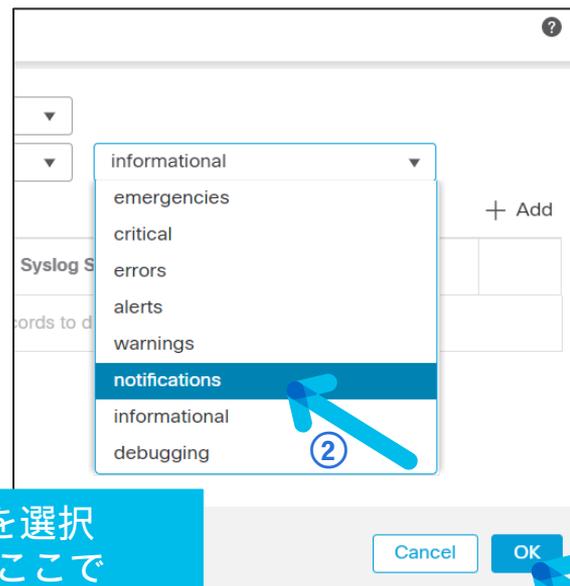
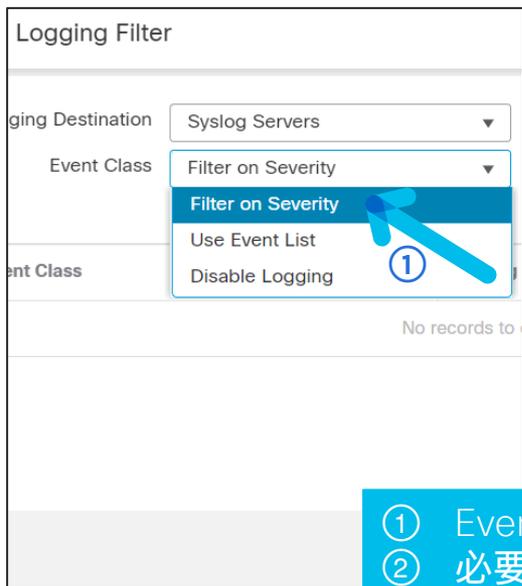
E-Mail

SSH Sessions

- ① Logging Destination を選択
- ② Logging Destination で Syslog Servers を選択

# Logging Destination 設定 (続き)

- 送付するログの種別を指定



- ① Event Class で Filter on Severity を選択
- ② 必要に応じてシビリティを選択。ここでは "notifications" で設定
- ③ OK をクリック

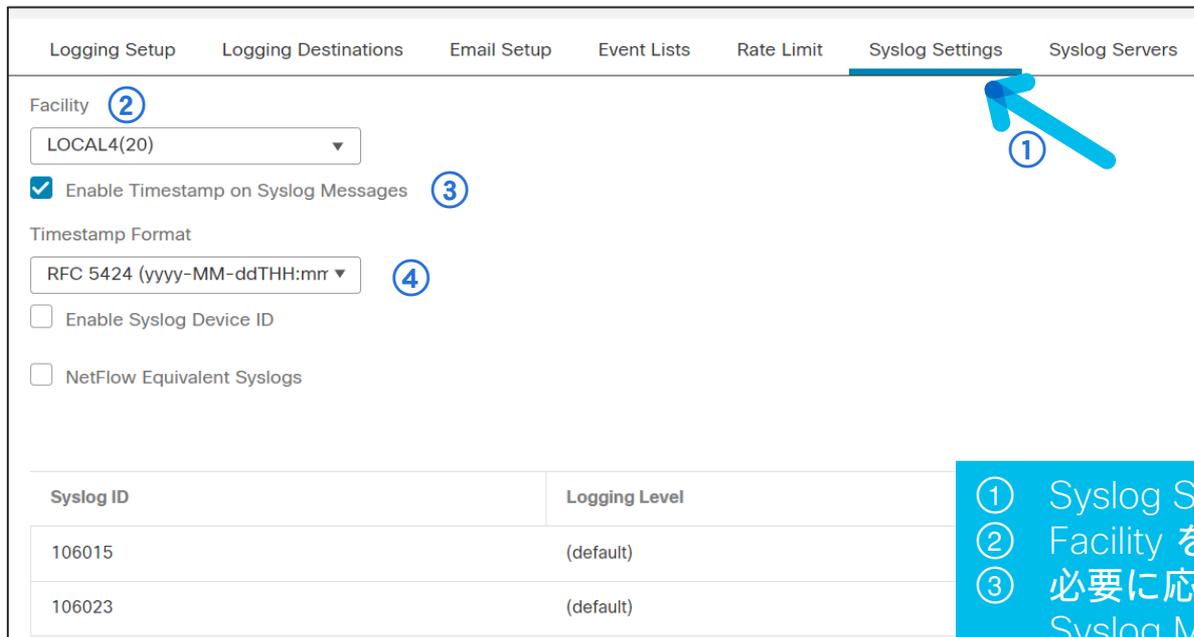
# Logging Destination 設定 (続き)

- OK をクリック後、以下のような行が表示

Logging Setup	Logging Destinations	Email Setup	Event Lists	Rate Limit	Syslog Settings	Syslog Servers
						+ Add
Logging Destination	Syslog from All Event Class	Syslog from specific Event Class				
Syslog Servers	Filter on Severity:notifications					 

# Syslog Settings 設定

- Syslog メッセージの出力設定を実施



Logging Setup   Logging Destinations   Email Setup   Event Lists   Rate Limit   **Syslog Settings**   Syslog Servers

Facility **②**  
LOCAL4(20) ▼

Enable Timestamp on Syslog Messages **③**

Timestamp Format  
RFC 5424 (yyyy-MM-ddTHH:mm) **④**

Enable Syslog Device ID

NetFlow Equivalent Syslogs

Syslog ID	Logging Level
106015	(default)
106023	(default)

- ① Syslog Settings を選択
- ② Facility を選択
- ③ 必要に応じて Enable Timestamp on Syslog Messages にチェック
- ④ Timestamp Format を選択

# Syslog Servers 設定

- Syslog メッセージを出力する先の Syslog サーバ設定を実施

Logging Setup   Logging Destinations   Email Setup   Event Lists   Rate Limit   Syslog Settings   **Syslog Servers**

Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)

Message Queue Size(messages)\*

512

(0 - 8192 messages). Use 0 to indicate unlimited Queue Size

+ Add

Interface	IP Address	Protocol	Port	EMBLEM	SECURE
No records to display					

- ① Syslog Servers を選択
- ② Add をクリック

# Syslog Servers 設定 (続き)

- Syslog メッセージを出力する先の Syslogサーバ設定を行う

Add Syslog Server

IP Address\*  +

Protocol  TCP  UDP

Port  (5104) (25-25)

Log Messages in Cisco EMBLEM format(UDP only)

Enable secure syslog.

Reachable By:

Device Management Interface (Applicable on FTD v6.3.0 and above)

Security Zones or Named Interface

Available Zones

Selected Zones/Interfaces

Interface Name

New Network Object

Name  ②

Description

Network  Host ③  Range  Network  FQDN

④

Allow Overrides

⑤

- ① “+” の追加アイコンをクリック。Network Object 作成画面が表示
- ② Name を入力。ここでは “SYSLOG” と設定
- ③ Network 種別の Host をチェック
- ④ Syslog サーバの IP アドレスを入力
- ⑤ Save をクリック

# Syslog Servers 設定 (続き)

- Syslog メッセージを出力する先の Syslog サーバを設定

- ① Syslog メッセージ送信プロトコルを選択する。ここでは UDP を選択
- ② 同様にポートを指定する。ここでは 514 を選択
- ③ Reachable By で Syslog メッセージの送信元とするインターフェイスを選択する。ここでは "Device Management Interface" を選択
- ④ OK をクリック

Add Syslog Server

IP Address\*  +

Protocol  TCP  UDP ①

Port  ② (514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only)

Enable secure syslog.

Reachable By:

③  Device Management Interface (Applicable on FTD v6.3.0 and above)

Security Zones or Named Interface

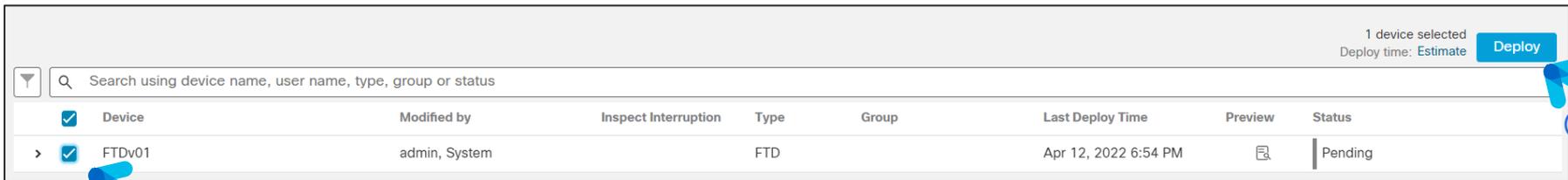
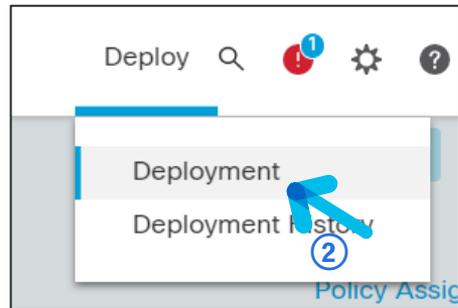
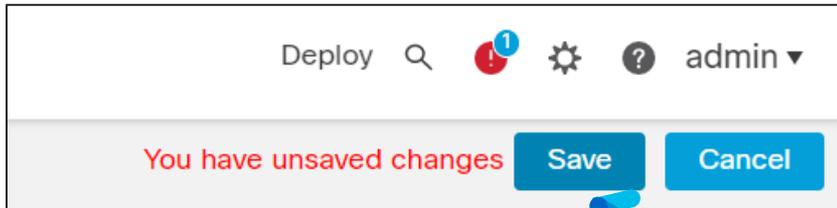
Available Zones

Selected Zones/Interfaces

Interface Name

④

# Deploy



- ① Save をクリックして変更を保存
- ② Deploy – Deployment をクリック
- ③ 変更された設定を確認の上、Deploy 対象機器にチェックを入れる
- ④ Deploy をクリック

# 参考: Syslog メッセージの出力例

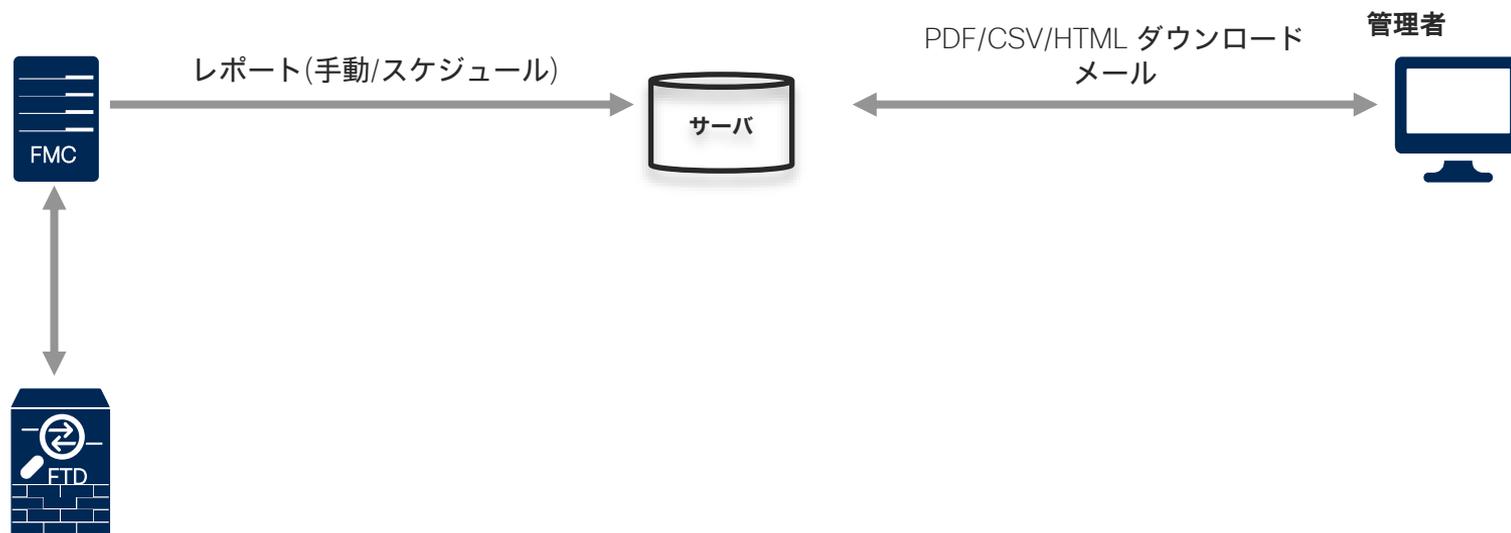
- 例えば FTD のインターフェイス GigabitEthernet0/0、0/1 の Down と Up を行った場合、Syslog サーバへは下記のようにメッセージが出力

```
Apr  8 08:10:26 FTDv01 %FTD-4-411002: Line protocol on Interface GigabitEthernet0/0, changed state to down
Apr  8 08:10:26 FTDv01 %FTD-4-411002: Line protocol on Interface GigabitEthernet0/1, changed state to down
Apr  8 08:12:06 FTDv01 %FTD-4-411001: Line protocol on Interface GigabitEthernet0/0, changed state to up
Apr  8 08:12:06 FTDv01 %FTD-4-411001: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

# レポート設定

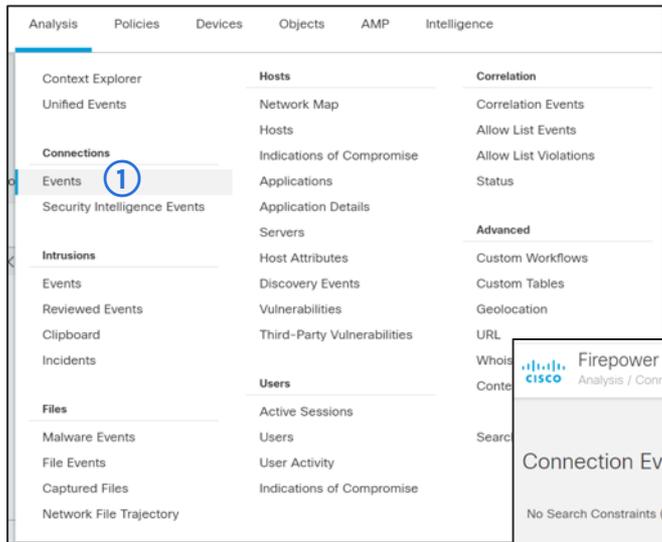
# レポート機能

- FMC より手動、もしくはスケジュールでレポートを生成できる
- レポートに含める内容はカスタマイズすることも可能



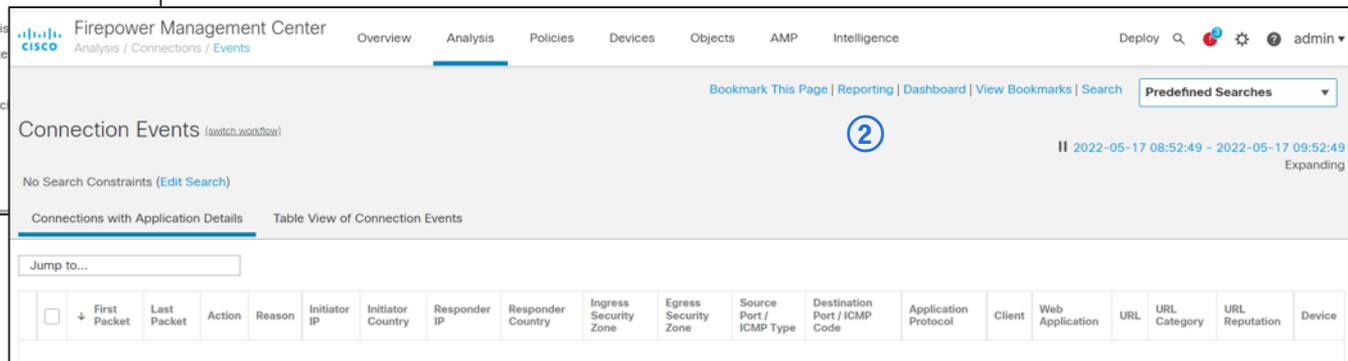
# 手動レポート作成

レポートの生成対象とする画面にアクセス。ここでは Connection Event を例にする



- ① Analytics - Connection - Events を選択
- ② Reporting をクリック

- その他のイベントも同様に、Reporting をクリックすることでレポートを手動で生成できる



# 手動レポート作成 (続き)

## 手動生成レポートのパラメータを指定

Firepower Management Center  
Overview / Reporting / Report Template Designer

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ ? admin

Reports Report Templates

Report Title  
Report of Connection Events +

Report Sections

Connections with Application Details

Table: Connection Events  
Preset: None  
Format: [Table] [Line] [Pie] [Bar]  
Search: None  
Fields: First Packet, Last Packet, Action, F

Section Description: \$<Time Window>\$<Constraints>  
Time Window:  Inherit Time Window  Last hour  
Maximum Results: 10000

Generate Advanced Save

Table View of Connection Events

Table: Connection Events  
Preset: None  
Format: [Table] [Line] [Pie] [Bar]

Section Description: \$<Time Window>\$<Constraints>

1 Report Title を必要に応じて変更  
2 Generate をクリック

# 手動レポート作成 (続き)

手動生成レポートの出力形式を指定

## Generate Report

---

### Report Generation Information

① File Name  +

② Output Format  HTML  PDF  CSV

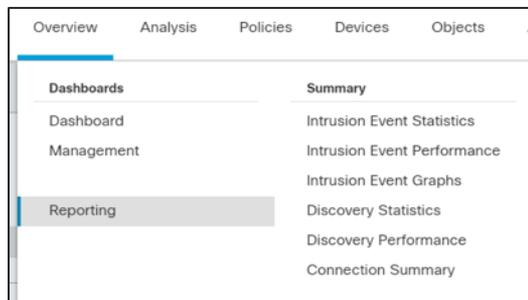
③ Relay Host No Relay Host Configured! 

④

- ① File Name は Report Title が引き継がれる。変更することも可能
- ② Output Format を選択。左から HTML、PDF、CSV フォーマット（複数選択可能）
- ③ 必要に応じて Relay Host にてレポートを送信する Mail Relay Host を指定
- ④ Generate をクリック

# レポートの確認

## 生成したレポートの確認



①

- ① Overview – Reporting を選択。生成済みレポートの一覧を表示
- ② 確認する対象のレポートの Time Completed の欄に日時が表示されていることを確認。日時が表示されていれば、レポートの生成処理が完了済み
- ③ 確認対象のレポートにチェックを入れる
- ④ Download をクリック

A screenshot of the 'Reports' section in a web application. The table has columns for Name, Time Requested, Time Completed, User, Location, and Status. Three rows of reports are listed, each with a checked checkbox in the first column. The third row is highlighted in blue. Below the table, there are buttons for 'Download', 'Delete', and 'Move'. A 'Storage Location' note is visible at the bottom right.

	Name	Time Requested	Time Completed	User	Location	Status
<input checked="" type="checkbox"/>	<a href="#">Report_of_Connection_Events-20220517012246-29238.pdf</a> Reports	2022-05-17 10:22:46	2022-05-17 10:22:47	admin	Local	Successfully Processed
<input checked="" type="checkbox"/>	<a href="#">Report_of_Connection_Events-20220517012246-29238.zip</a> Reports	2022-05-17 10:22:46	2022-05-17 10:22:47	admin	Local	Successfully Processed
<input checked="" type="checkbox"/>	<a href="#">Report_of_Connection_Events-20220517012246-29238_csv.zip</a> Reports	2022-05-17 10:22:46	2022-05-17 10:22:47	admin	Local	Successfully Processed

Storage Location: /var/st/reports/ (Disk Usage: 14%)

# 参考:レポートのカスタマイズ

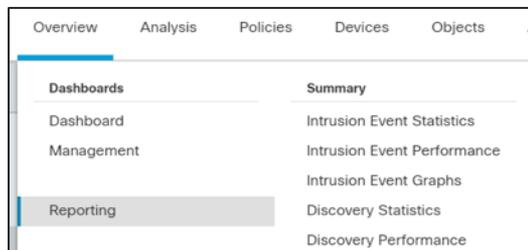
レポートはセクションの追加や変更といったカスタマイズが可能

The screenshot displays the 'Report Template Designer' interface in the Cisco Firepower Management Center. The main area is titled 'Report Sections' and shows a configuration for a section named 'Connections with Application Details'. This section is currently set to 'Table View'. The configuration includes a dropdown for 'Table' (set to 'Connection Events'), a 'Preset' dropdown (set to 'None'), a 'Format' dropdown (with icons for Table, Line Chart, Bar Chart, Pie Chart, and Text), a 'Search' dropdown (set to 'None'), and a 'Fields' field (set to 'First Packet, Last Packet, Action, F'). To the right of these options are fields for 'Section Description' (set to '\$<Time Window>\$<Constraints>'), 'Time Window' (with 'Inherit Time Window' and 'Last hour' options), and 'Maximum Results' (set to '10000'). A toolbar at the top right of the section configuration area contains icons for different section types: Table, Line Chart, Bar Chart, Pie Chart, Text, Page Break, and Import Sections. A blue arrow labeled '1' points to this toolbar. A red box highlights the configuration area for the selected 'Table' section, and a blue arrow labeled '2' points to this area.

- ① 追加するセクション種別の選択。Bar Chart / Line Chart / Pie Chart / Table View / Detail View / Text Section / Page Break / Import Sections from Dashboard, Summaries, and Workflows より指定
- ② セクションごとのカスタマイズも可能。Table種別 (Table)、レポートに含める検索条件 (Search)、レポート対象の期間 (Time Window)、表示するフィールド (Fields) 等

# 参考: レポートテンプレートの管理

デフォルト定義やカスタム定義したものをテンプレート一覧より管理可能



- ① Overview - Reporting を選択
- ② Report Templates を選択
- ③ 各種操作を実行可能。Generate / Copy / Export / Edit / Delete  
※ただし Risk Report Templates 下のは Generate のみ

② Report Templates を選択

③ 各種操作を実行可能。Generate / Copy / Export / Edit / Delete

※ただし Risk Report Templates 下のは Generate のみ

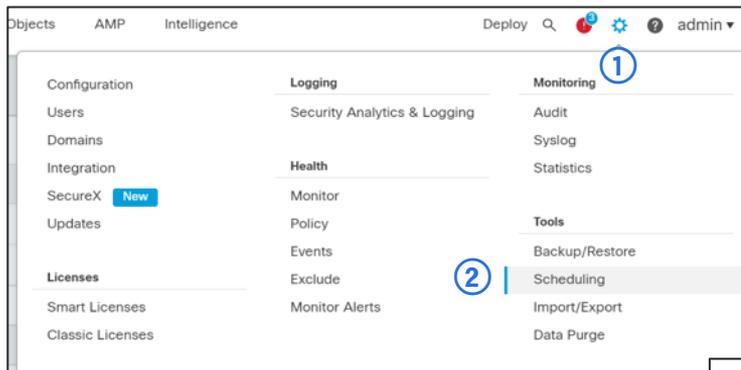
Risk Report Templates	Last Modified	
Advanced Malware Risk Report	2022-05-17 10:37:38 Modified by "admin"	③
Attacks Risk Report	2022-05-17 10:37:38 Modified by "admin"	
Network Risk Report	2022-05-17 10:37:38 Modified by "admin"	
Templates	Last Modified	
Attack Report: \$<Attack SID>	2021-12-17 08:09:17 Modified by "admin"	
Files Report	2021-12-17 08:09:17 Modified by "admin"	
FirePOWER Report: \$<Customer Name>	2021-12-17 08:09:17 Modified by "admin"	

③

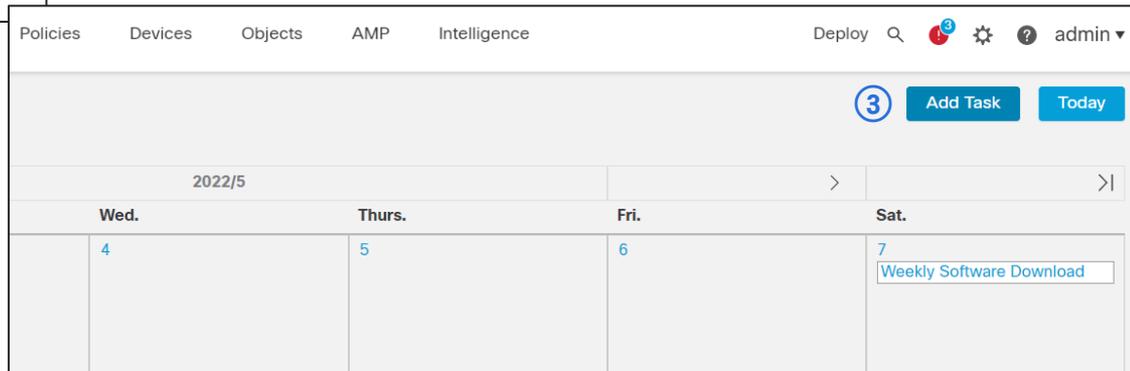
The screenshot shows the 'Report Templates' page. It has a 'Create Report Template' button in the top right. The table lists various templates, including 'Risk Report Templates' and 'Templates'. A red box highlights the action icons (Generate, Copy, Export, Edit, Delete) for each row. A circled '3' is next to the first row's icons.

# スケジュール レポート生成

スケジュールタスクにて、レポート生成タスクを定義



- ① 歯車マークをクリック
- ② Tools 下の Scheduling をクリック
- ③ Add Task をクリック



# スケジュール レポート生成 (続き)

レポートの生成対象とする画面を開く。ここでは事前に作成した Connection Event を週次でスケジュール化

New Task

① Job Type

② Schedule task to run  Once  Recurring

③ Start On    Asia/Tokyo

④ Repeat Every   Hours  Days  Weeks  Months

⑤ Run At

⑥ Repeat On  Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday

Job Name  ⑦

⑧ Report Template  [Edit](#)

Comment

Email Status To Not available. You must set up your mail relay host.

⑨

- ① Report を選択
- ② 繰り返しの作業として Recurring ヘチェックを入れる
- ③ レポート生成タスクの開始年月日を指定。ここでは 2022年6月1日と設定
- ④ レポート生成タスクの頻度を指定。ここでは週次で設定
- ⑤ 実行時間を指定。ここでは午前 4:00に処理を開始
- ⑥ 実行曜日を指定。ここでは日曜に処理を開始
- ⑦ Job Name を入力。ここでは "SCHEDULE\_REPORT" と入力
- ⑧ 生成する Report Template を指定する前のスライドで作成した Report of Connection Events を指定
- ⑨ Save をクリック

# スケジュール レポート確認

スケジュールタスクにて、レポート生成タスクが確認可能

The screenshot displays the Splunk interface for managing tasks. A grid shows a schedule of tasks from day 14 to 31. The 'SCHEDULE\_REPORT' task is highlighted in red in the grid. To the right, a sidebar menu shows 'Scheduling' selected. Below the grid, a 'Task Details' table provides information for the 'SCHEDULE\_REPORT' task.

Name	Type	Start Time	Frequency	Last Run Time	Last Run Status	Next Run Time	Creator	Domain	
SCHEDULE_REPORT	Report	06/01/2022 04:00	Every Week on Saturday	Not run yet	🚫	N/A	admin	Global	🗑️

- 設定した通りにタスクが保存されていることを確認。毎週日曜日と設定したため、赤枠部分のようにになっている
- 各タスクをクリックすると Task Details が下段に表示される。ここからタスクの実行状況や、編集/削除の操作が可能
- 生成されたレポートは手動生成レポートと同様に、Overview > Reporting > Reports より確認が可能

# 参考: レポートを日本語で生成

テンプレート定義済みのレポートは即時生成が可能。また、UIを日本語化していれば日本語でのレポート生成が可能。UI 日本語化の方法は以下の通り

① 歯車マークから Configuration をクリック

② Language をクリック

③ Japanese を選択

④ Save をクリック

成功 保存に成功しました。

# 参考: レポートを日本語で生成 (続き)

レポート レポートテンプレート

レポートテンプレートの作成

リスクレポートテンプレート	最終変更日	
ネットワークリスクレポート	2022-05-17 11:24:27 変更者: admin	   
攻撃リスクレポート	2022-05-17 11:24:27 変更者: admin	   
高度なマルウェアリスクレポート	2022-05-17 11:24:27 変更者: admin	   
テンプレート	最終変更日	
Attack Report: \$<Attack SID>	2021-12-17 08:09:17 変更者: admin	   

### レポート生成

レポート生成情報

ファイル名  +

タイムウィンドウ  Last week

リレーホスト  

空のセクション  除外

入力パラメータ

Company Name

Author

Contact

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

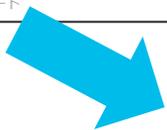
90

# 参考: レポートを日本語で生成 (続き)

レポート レポートテンプレート

名前

netutowakurisukurepoto-20220517022622-15205.zip  
レポート



**ネットワークリスクレポート**

対象: シスコシステムズ合同会社

Tuesday, May 17, 2022

作成者: 管理者名  
連絡先: xxxxxxx@cisco.com

**I. 概要**

シスコは、シスコシステムズ合同会社が属するリスクの状態にあると判断しました。その理由は、ビジネスとの関連性は低いものの、会社にとってリスクになる可能性のあるアプリケーションを使用しているためです。これらのアプリケーションは、ネットワークを攻撃に対して脆弱なままにしたり、マルウェアを伝送したり、弊組織を暴露したりする可能性があります。

評価期間: Tue May 10 2022 11:26:22~Tue May 17 2022 11:26:22

リスクのあるアプリケーション 0	リスクのあるユーザー *	高帯域幅アプリケーション 1
暗号化アプリケーション 2	セキュリティ回避機能を持つアプリ 1	危険な Web ブラウザ 0

ネットワークプロファイル

0	0	22	1
オペレーティングシステム	モバイルデバイス	使用中心アプリケーション	転送されるファイルタイプ

**アプリケーションリスク別のネットワーク接続の概要**

■ 普通	51%
■ 低い	1%
■ 非常に低い	48%

**高帯域幅アプリケーション**

一部のアプリケーションは大規模なネットワーク帯域幅を使用します。帯域幅使用は、組織によってコストがかかります。全体的なネットワークパフォーマンスに悪影響を及ぼす可能性があります。これらのアプリケーションの使用を特定のネットワークに制限することを検討します。たとえば、ワイヤレスネットワークはビストロドメインに属してはいない場合があります。または、これらのアプリケーションを完全にシャットダウンするか、帯域幅の使用状況を可視化することもできます。

アプリケーション	アクセル時間	アプリケーションリスク	生産性評価	転送データ(MB)
Microsoft Update	7	普通	低い	0.4575

**暗号化アプリケーション**

一部のアプリケーションは暗号化されたデータを転送します。これにより、セキュリティ監査は難しくなります。

# アラート設定

# アラート概要

- FMC、FTD が生成するアラートは外部サーバへロギングすることが可能
- 対象となるアラートは下記

項目	説明
<b>Health Monitor Event</b>	機器自体のステータスに関するアラート
<b>Audit Log Event</b>	監査ログのアラート
<b>Connection Event</b>	Access Control Policy によるコネクションイベントのアラート
<b>Discovery Event</b>	Network Discovery のアラート
<b>Impact Alert</b>	Intrusion Policy イベントのうち、Impact Flag に応じたアラート
<b>Intrusion Event</b>	Intrusion Policy のアラート
<b>Correlation Event</b>	Correlation Policy のアラート。詳細な条件を指定し、アラート通知を実行
<b>Network Malware Event</b>	Network AMP のアラート

# 設定の流れ

- ステップ1 : Health Policy 確認
- ステップ2 : Syslog Alert 作成
- ステップ3 : Health Alert 作成と Syslog Alert 関連付け

Syslog サーバが、FMC より疎通の取れるネットワークセグメントに構築してある前提とする

# Health Policy 確認

- ・ デフォルトで定義されているHealth Policyを確認

Objects AMP Intelligence Deploy Q admin ▼

Configuration Logging Monitoring

Users Security Analytics & Logging Audit

Domains Syslog

Integration Statistics

SecureX **New** Health

Updates Policy **2** Tools

Licenses Events Backup/Restore

Smart Licenses Exclude Scheduling

Classic Licenses Monitor

Policy Name	Domain	Applied To	Last Modified	
Initial_Health_Policy 2021-12-16 23:09:36 Initial Health Policy	Global	2 appliances	2021-12-17 08:09:35 Modified by "admin"	<b>3</b>

- ① 歯車マークを選択
- ② Health 下の Policy を選択
- ③ デフォルトで定義されている Health Policy 横の鉛筆アイコンをクリック

デフォルト定義の Health Policy は Description 欄に " Initial Health Policy" と記載がある

# Health Policy 確認 (続き)

- デフォルトで定義されている Health Policy を確認

Policy Run Time Interval

AMP Connection Status

AMP Threat Grid Status

AMP For Endpoints Status

AMP for Firepower Status

ASP Drop

Advanced Snort Statistics

Appliance Heartbeat

Automatic Application Bypass Status

Backlog Status

CPU Usage (per core)

CPU Usage Data Plane

CPU Usage Snort

CPU Usage System

Editing Policy: Initial\_Health\_Policy 2021-12-16 23:09:36

Policy Name: Initial\_Health\_Policy 2021-12-16 :

Policy Description: Initial Health Policy

Legacy Run Time Interval (mins): 5

Run Time Interval (mins): 1

Note : Changes to Run Time Interval will restart the health monitoring process.

Cancel Save Policy and Exit

Policy Run Time Interval

AMP Connection Status

AMP Threat Grid Status

AMP For Endpoints Status

AMP for Firepower Status

ASP Drop

Advanced Short Statistics

Appliance Heartbeat

Automatic Application Bypass Status

Backlog Status

CPU Usage (per core)

CPU Usage Data Plane

CPU Usage Snort

CPU Usage System

Editing Policy: Initial\_Health\_Policy 2021-12-16 23:09:36

Policy Name: Initial\_Health\_Policy 2021-12-16 :

Policy Description: Initial Health Policy

Description: AMP for Endpoints Status

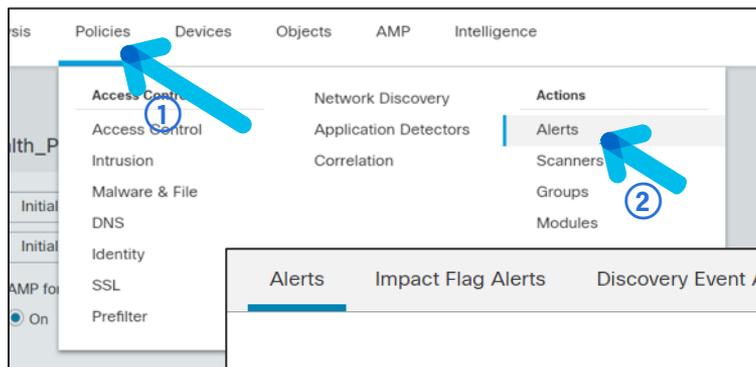
Enabled  On  Off

Cancel Save Policy and Exit

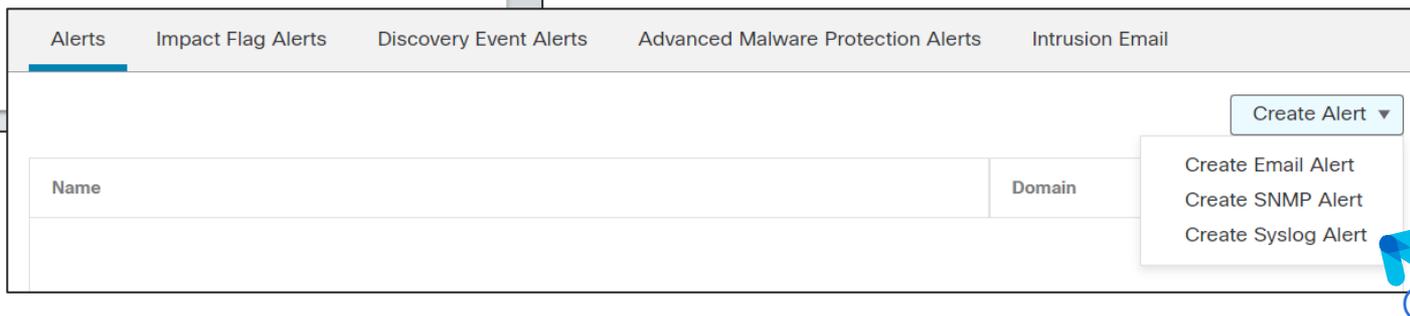
- 各種アラートの設定を確認
- 例えば AMP for Endpoints Status の Enabled の On にチェックが入っているため、このアラートは有効であることが確認可能

# Syslog Alert 作成

- Syslog Alert を作成



Create Alert で Email、SNMP を選択すると同様にメール、SNMP の設定が可能



- ① Policies を選択
- ② Actions 下の Alerts を選択
- ③ Create Alert のプルダウンより Create Syslog Alert をクリック

# Syslog Alert 作成 (続き)

Edit Syslog Alert Configuration

Name  
SYSLOG-ALERT ①

Host  
10.71.128.107 ②

Port  
514 ③

Facility  
ALERT ④

Severity  
NOTICE ⑤

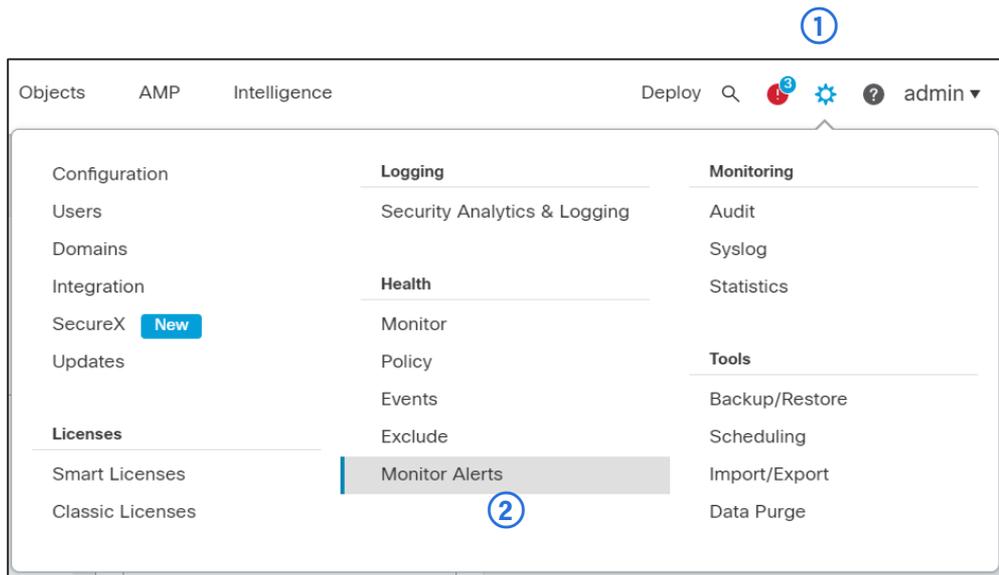
Tag  
⑥

Cancel Save

- Syslog Alert を作成

- ① Name を入力。ここでは "SYSLOG-ALERT" とする
- ② Host に Syslog サーバのIPアドレスを入力
- ③ Port に Syslog サーバのポート番号を入力。デフォルトは 514
- ④ Facility を選択
- ⑤ Severity を選択。ここでは "NOTICE" とする
- ⑥ Save をクリック

# Health Alert 作成と Syslog Alert 関連付け



- ① 歯車マークを選択
- ② Health 下の Monitor Alerts を選択

# Health Alert 作成と Syslog Alert 関連付け (続き)

Configure Health Alerts

Health Alert Name **③**

Severity **④**  
 Critical  
 Warning  
 Normal  
 Error  
 Recovered

Module **⑤**  
 AMP Connection Status  
 AMP Threat Grid Status  
 AMP For Endpoints Status  
 AMP for Firepower Status  
 ASP Drop  
 Advanced Snort Statistics  
 Appliance Heartbeat  
 Automatic Application Bypass ...  
 Backlog Status  
 CPU Usage (per core)  
 CPU Usage Data Plane

Alert **⑥**  
 SYSLOG-ALERT (Syslog) (Inactive)

Threshold Timeout (Optional)  
  
(in minutes)

**⑦** Save

- ③ Health Alert Name に Name を入力、ここでは "HEALTH-ALERT" とする
- ④ Severity を選択。ここでは全てを選択
- ⑤ Module を選択。ここでは全てを選択
- ⑥ Alert で作成済みの "SYSLOG-ALERT" を選択
- ⑦ Save をクリック

# 参考: Syslog メッセージの出力例

- 例えば FMC からのメッセージとして、Syslog サーバへは下記のように出力される

```
Apr 13 01:34:18 FMCv : HMNOTIFY: Threat Data Updates on Devices (Sensor fmc.cs.example.jp): Severity: normal: Process is running correctly
Apr 13 01:34:19 FMCv : HMNOTIFY: AMP for Firepower Status (Sensor fmc.cs.example.jp): Severity: normal: Successfully connected to cloud
Apr 13 01:34:20 FMCv : HMNOTIFY: RRD Server Process (Sensor fmc.cs.example.jp): Severity: normal: The server is functioning normally.
Apr 13 01:34:21 FMCv : HMNOTIFY: Interface Status (Sensor fmc.cs.example.jp): Severity: normal: All interfaces are working correctly
```

# 参考: その他のアラート設定について

## 各アラートの設定を行うメニュー

項目	説明	画面メニュー
Health Monitor Event	機器自体のステータスに関するアラート	Health Policy ①歯車マーク > Health > Policy Alert ①Policies > Actions > Alerts Health Alert ①歯車マーク > Health > Monitor Alert ②使用する Alert を一覧より指定
Audit Log Event	監査ログのアラート	Audit Log ①歯車マーク > Configuration > Audit Log
Connection Event	Access Control Policy による接続イベントのアラート	Connection Event ①Policies > Access Control ②アラート有効にするルールの含まれる Access Control Policy を選択 ③Logging タブで Default Syslog Settings を設定
Discovery Event	Network Discovery のアラート	Alert ①Policies > Actions > Alerts Discovery Event Alert ①Policies > Actions > Alerts > Discovery Event Alerts ②使用する Alert をプルダウンより指定

# 参考: その他のアラート設定について②

## 各アラートの設定を行うメニュー

項目	説明	画面メニュー
<b>Impact Flag Alert</b>	Intrusion Policy イベントのうち、Impact Flag に応じたアラート	Alert ①Policies > Actions > Alerts Impact Flag Alerts ①Policies > Actions > Alerts > Impact Flag Alerts ②使用する Alert をプルダウンより指定
<b>Intrusion Event</b>	Intrusion Policy のアラート	Intrusion Event ①Policies > Access Control > Intrusion ②アラート有効にする Intrusion Policy を選択 ③Advanced Settings > External Responses

# 参考: その他のアラート設定について③

## 各アラートの設定を行うメニュー

項目	説明	画面メニュー
<b>Correlation Event</b>	Correlation Policy のアラート	Alert ①Policies > Actions > Alerts Correlation Policy ①Policies > Correlation ②アラート有効にするルールの含まれる Correlation Policy を選択 ③アラート有効にする Correlation Rule を選択 ④使用する Responses を Alert 一覧より指定
<b>Network Malware Evert</b>	Network AMPのアラート	Alert ①Policies > Actions > Alerts Advanced Malware Protection Alert ①Policies > Actions > Alerts > Advanced Malware Protection Alerts ②使用する Alert をプルダウンより指定

# 参考: Audit Log Event 設定画面

The screenshot shows the configuration interface for Audit Log Events. The top navigation bar includes 'Objects', 'AMP', 'Intelligence', 'Deploy', a search icon, a notification icon with '3', a settings gear icon (1), a help icon, and the user 'admin'. The left sidebar has 'Configuration' (2) selected. The main content area is divided into 'Logging', 'Monitoring', and 'Tools' sections. The 'Audit Log' option (3) is selected in the 'Tools' section. A dark overlay menu is open, showing 'Audit Log' (3) as the selected item. The right panel shows the configuration for 'Send Audit Log to Syslog', with 'Enabled' (4) selected in the dropdown, an empty 'Hosts (Up to 5)' field (5), 'USER' (6) selected in the 'Facility' dropdown, and 'INFO' (7) selected in the 'Severity' dropdown. A 'Test Syslog Server' button is at the bottom right.

- ① 歯車マークを選択
- ② Configuration を選択
- ③ Audit Log を選択
- ④ プルダウンより Enable を選択
- ⑤ Syslog サーバの IP アドレスを入力
- ⑥ Facility を選択
- ⑦ Severity を選択

# 参考: Connection Event 設定画面

Access Control Policy	Domain	Status	Last Modified	
ACP-1	Global	Targeting 1 devices <i>Up-to-date on all targeted devices</i>	2022-05-13 11:51:13 Modified by "Firepower System"	 ①

## ACP-1

Enter Description

Rules Security Intelligence HTTP Responses **Logging** ▲ Advanced

Default Syslog Settings:

The following configuration will be used for all syslog destinations in this AC policy and all included SSL, Prefilter and Intrusion policies unless explicitly overridden.

Send using specific syslog alert ③

Syslog Alert

④ +

Use the syslog settings configured in the FTD Platform Settings policy deployed on the device

Syslog Severity

- ① 設定対象とする Access policy を開く
- ② Logging タブを選択
- ③ [Send using specific syslog alert] にチェック
- ④ 使用する Syslog Alert をプルダウンより選択

# 参考: Connection Event 設定画面 (続き)

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action	Icons
Mandatory - ACP-1 (-)															
There are no rules in this section. <a href="#">Add Rule</a> or <a href="#">Add Category</a>															
Default - ACP-1 (1-3)															
1	TIME-BASED (Disabled)	Any	Any	OFFICE	Any	Any	Any	Any	Any	Any	Any	Any	Any	Block	Icons
2	URL-MONITO	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any (Except	Any	Any	Monitor	Icons
3	CATCH-ALL	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	Icons

- ① 設定対象とする Access Rule を編集
- ② Logging を選択
- ③ Syslog Server にチェック
- ④ Show Overrides をクリック
- ⑤ Override させる設定として、Severity、使用する Syslog Destination を指定

Action: Allow

Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes

Log at Beginning of Connection

Log at End of Connection

File Events:

Log Files

Send Connection Events to:

Firepower Management Center

Syslog Server (Using default syslog configuration in Access Control Logging) [Hide Overrides](#)

Override Severity: ALERT

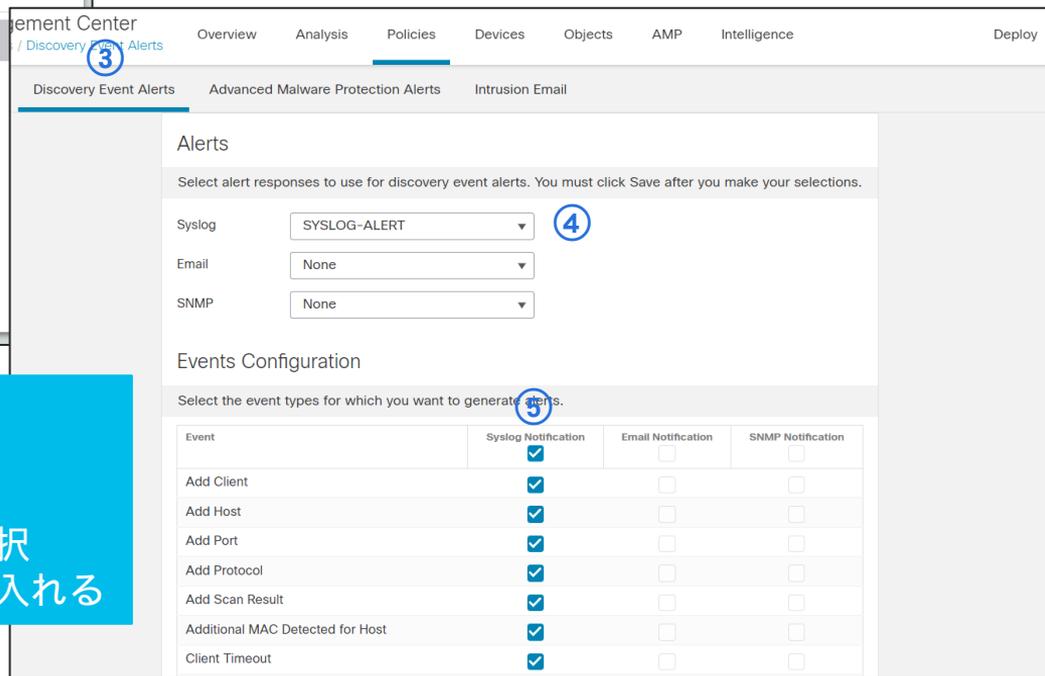
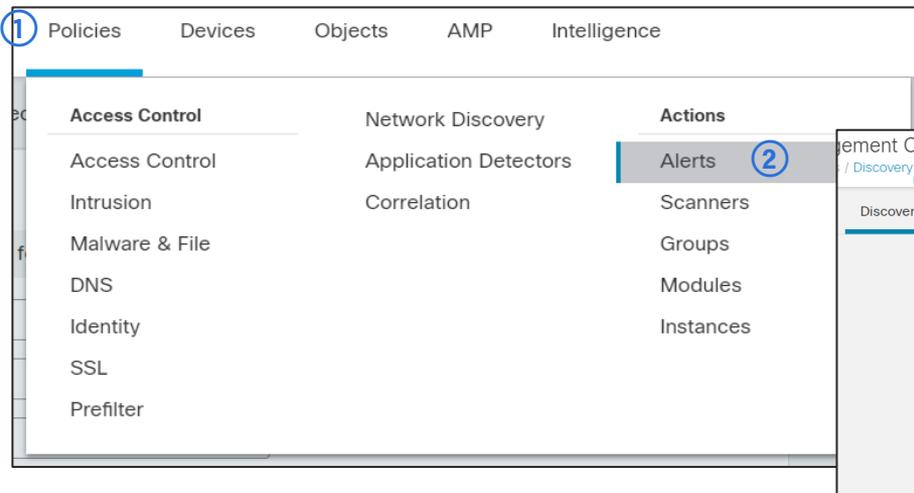
Override Default Syslog Destination: Select a Syslog Alert Configurati

SNMP Trap: Select an SNMP Alert Configurati

[Logging](#) [Show Overrides](#)

Cancel Save

# 参考: Discovery Event 設定画面



- ① Policies を選択
- ② Actions 下の Alerts を選択
- ③ Discovery Event Alerts を選択
- ④ 使用する Syslog Alert をプルダウンより選択
- ⑤ アラート対象とするイベントへチェックを入れる

# 参考: Impact Flag 設定画面

① Policies を選択

② Actions 下の Alerts を選択

③ Impact Flag Alerts を選択

④ 使用する Syslog Alert をプルダウンより選択

⑤ アラート対象とする Flag へチェックを入れる

Impact Flag	Syslog Notification	Email Notification	SNMP Notification
① Unknown	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
④ Unknown Target	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
③ Currently Not Vulnerable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
② Potentially Vulnerable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
① Vulnerable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

# 参考: Intrusion Event 設定画面

Access Control Policy	Domain	Status	Last Modified	
ACP-1	Global	Targeting 1 devices <i>Up-to-date on all targeted devices</i>	2022-05-13 11:51:13 Modified by "Firepower System"	

ACP-1  
Enter Description

Rules Security Intelligence HTTP Responses **Logging** Advance

ALERT

▲ At least one of the options in Default Syslog Settings must be selected if syslog is

IPS Settings

Send Syslog messages for IPS events

Default syslog settings configured above are used for syslog destinations for IPS events

Hide Overrides

Override Severity

ALERT

Override Syslog Destination

SYSLOG-ALERT

File and Malware Settings

Send Syslog messages for File and Malware events

Default syslog settings configured above are used for syslog destinations for File and Malware events

IPS Settings

Send Syslog messages for IPS events

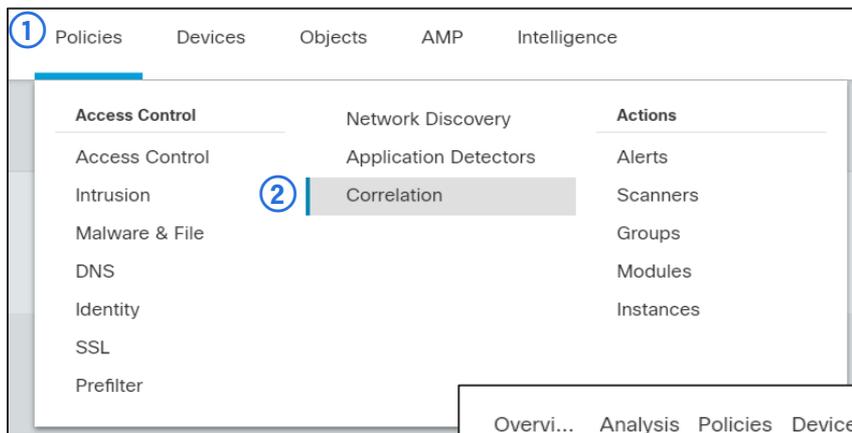
Default syslog settings configured above are used

Show Overrides

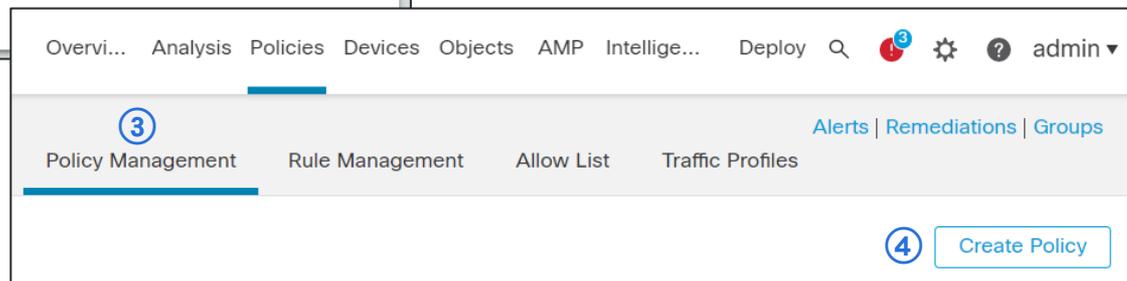
- ① 設定対象とする Access policy を開く
- ② Logging タブを選択
- ③ IPS Settings 以下にある [Send using specific syslog alert] にチェック
- ④ Show Overrides をクリックし展開
- ⑤ Overrides Severity、Overrides Syslog Destination を必要に応じて選択

# 参考: Correlation Event 設定画面

- Correlation Policy を設定することで、詳細な条件に基づくアラート通知が可能



- ① Policies を選択
- ② Access Control 下の Correlation を選択
- ③ Policy Management を選択
- ④ Create Policy をクリック

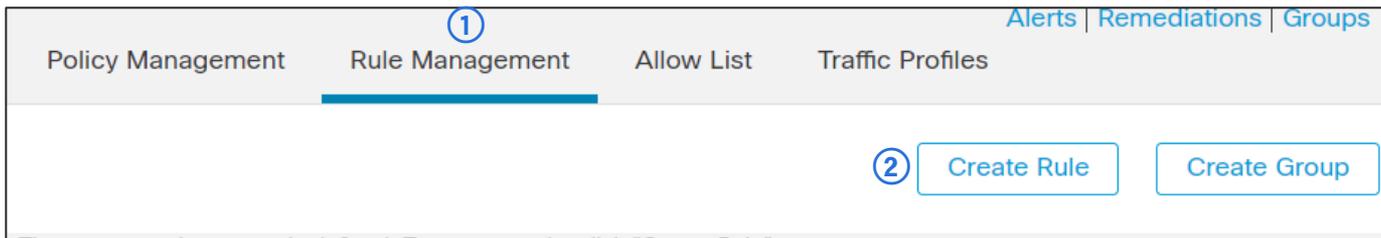


# 参考: Correlation Event 設定画面 (続き)

The screenshot shows a web interface for configuring a Correlation Policy. At the top, there are navigation tabs: "Policy Management" (selected), "Rule Management", "Allow List", and "Traffic Profiles". Below the tabs, the page title is "Correlation Policy Information". To the right of the title are two buttons: "Cancel" and "Save". The main form contains three fields: "Policy Name" with the value "CORRELATION\_POLICY", "Policy Description" (empty), and "Default Priority" with a dropdown menu set to "None". A circled "1" is placed to the left of the "Policy Name" field, and a circled "2" is placed to the right of the "Save" button.

- ① Policy Name を入力
- ② Save をクリックし、一旦保存

# 参考: Correlation Event 設定画面 (続き)



Policy Management Rule Management Allow List Traffic Profiles

Rule Information

Rule Name: CORRELATION\_RULE ③

Rule Description: [Empty]

Rule Group: Ungrouped

Select the type of event for this rule

If [Dropdown] and it meets the following conditions:

④ [Dropdown] (Options: a VPN troubleshoot event occurs, an intrusion event occurs, a discovery event occurs, user activity is detected, a host input event occurs, a connection event occurs, a traffic profile changes, a Malware event occurs)

generates an event, snooze for 0 hours

no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Add Inactive Period

Cancel Save

① Rule Management をクリック  
② Create Rule をクリック  
③ Rule Nameを入力。ここでは“CORRELATION\_RULE”とする  
④ プルダウンより Correlation Policy によりアラート通知させる場合の、条件を選択。ここでは an intrusion event occurs とする

# 参考: Correlation Event 設定画面 (続き)

Select the type of event for this rule

If  and it meets the following conditions:

①

Classification  
Client  
Client Category  
Destination Country  
Destination IP  
Destination Port / ICMP Code  
Device  
Egress Interface  
Egress Security Zone  
Egress VRF  
Either Source IP or Destination IP  
Generator ID  
Impact Flag  
Ingress Interface  
Ingress Security Zone  
Ingress VRF  
Inline Result  
Inline Result Reason  
Intrusion Policy  
IOC Tag

②

③  is

Rule Options

Snooze If this rule generates an event, snooze for

Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

④

- ① 必要に応じて詳細な条件を追加。追加する場合 Add condition をクリック
- ② プルダウンより用いる条件を選択。ここでは IOC Tag とする
- ③ 演算子を選択。ここでは is Set とする。これにより「Intrusion Eventが発生し、なおかつそれに IOC Tag がセットされていたら」という条件になる
- ④ Save をクリック

# 参考: Correlation Event 設定画面 (続き)

The screenshot displays the configuration interface for Correlation Events. The top navigation bar includes 'Policy Management', 'Rule Management', 'Allow List', and 'Traffic Profiles'. The 'Policy Management' tab is selected, indicated by a circled '1'. Below the navigation bar, there is a 'Create Policy' button. A table lists the policy 'CORRELATION\_POLICY'. To the right of the table, there is a 'Sort by' dropdown menu set to 'State' and a set of action icons (toggle, edit, copy, delete), with the edit icon (pencil) circled as '2'. Below this is a form titled 'Correlation Policy Information' with fields for 'Policy Name' (CORRELATION\_POLICY), 'Policy Description', and 'Default Priority' (None). There are 'Cancel' and 'Save' buttons. Below the form is a section for 'Policy Rules' with an 'Add Rules' button circled as '3' and a message 'No Rules Currently Active'.

- ① Policy Management を選択
- ② 鉛筆マークをクリック
- ③ Add Rule をクリック

# 参考: Correlation Event 設定画面 (続き)

Available Rules

Select the rules you wish to add to this policy, then click "Add".

▼ Ungrouped Rules

- CORRELATION\_RULE

▼ Allow List Rules

- Default Allow List

Cancel Add

- ① Correlation Policy へ含める Rule にチェック
- ② Add をクリック

# 参考: Correlation Event 設定画面 (続き)

Policy Rules Add Rules

Rule	Responses	Priority
<a href="#">CORRELATION_RULE</a>	This rule does not have any responses.	Default <span style="float: right;">①</span>

Responses for CORRELATION\_RULE

Assigned Responses

Unassigned Responses

^ 3

2 SYSLOG-ALERT

Cancel Update

Responses for CORRELATION\_RULE

Assigned Responses

SYSLOG-ALERT

Unassigned Responses

Cancel Update

- ① Responses アイコンをクリック
- ② Correlation Rule で使用する Syslog Alert を選択
- ③ 追加アイコンをクリック
- ④ Update をクリック

# 参考: Correlation Event 設定画面 (続き)

Policy Management Rule Management Allow List Traffic Profiles

Create Policy

Name

CORRELATION\_POLICY

Sort by State

①

Policy Management Rule Management Allow List Traffic Profiles

Create Policy

Success  
Activated Policy: CORRELATION\_POLICY

Name

CORRELATION\_POLICY

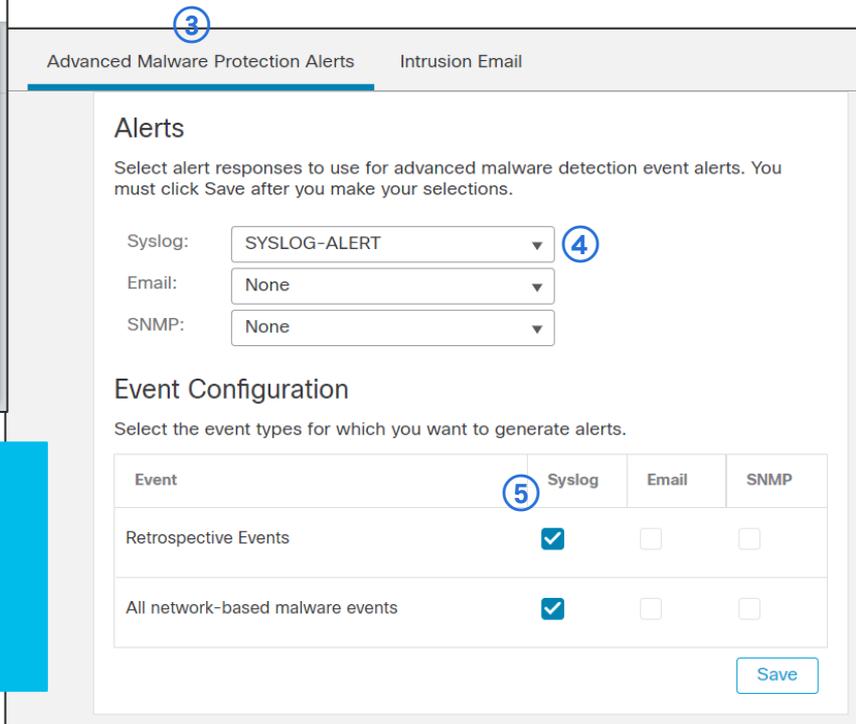
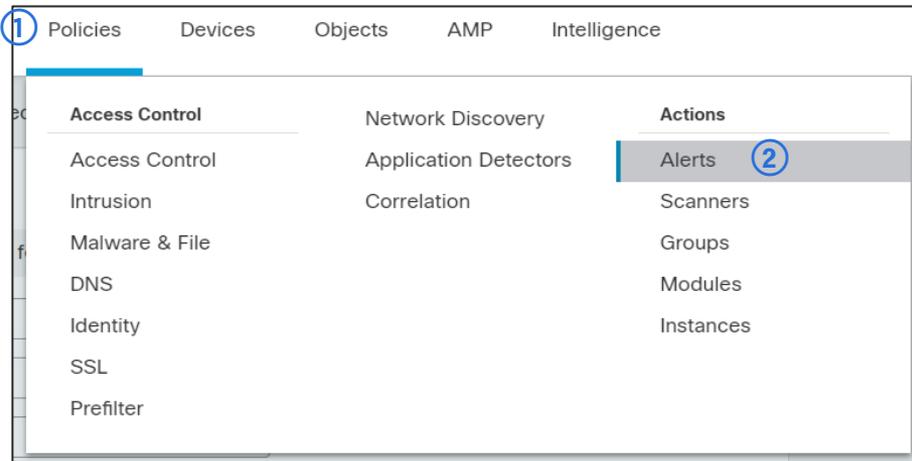
Sort by State

- ① Activate アイコンをクリック。これによって Correlation Policy が有効になり、Correlation Rule の条件を満たすイベントが発生した場合にアラートが送信される

Correlation Ruleの条件文については下記を参照のこと

[https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/correlation\\_policies.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/correlation_policies.html)

# 参考: Advanced Malware Protection Alerts 設定画面



- ① Policies を選択
- ② Actions 下の Alerts を選択
- ③ Advanced Malware Protection Alerts を選択
- ④ 使用する Syslog Alert をプルダウンより選択
- ⑤ アラート対象とする Event へチェックを入れる

# 18. SAL SaaS, SecureX 連携の設定

SAL SaaS 連携編

# Cisco SAL ( Security Analytics and Logging ) SaaS とは

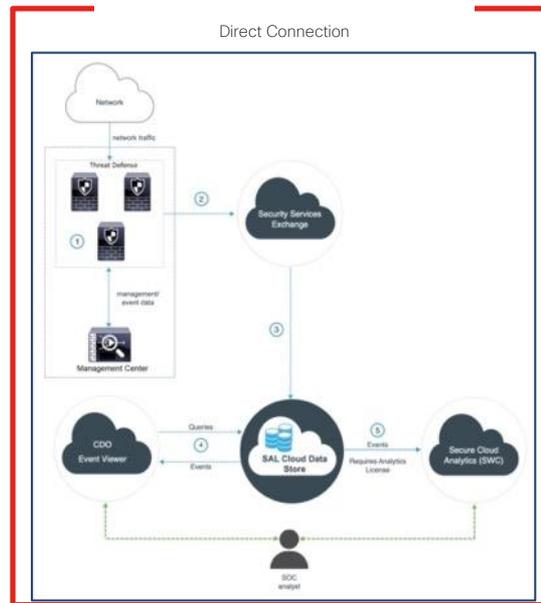
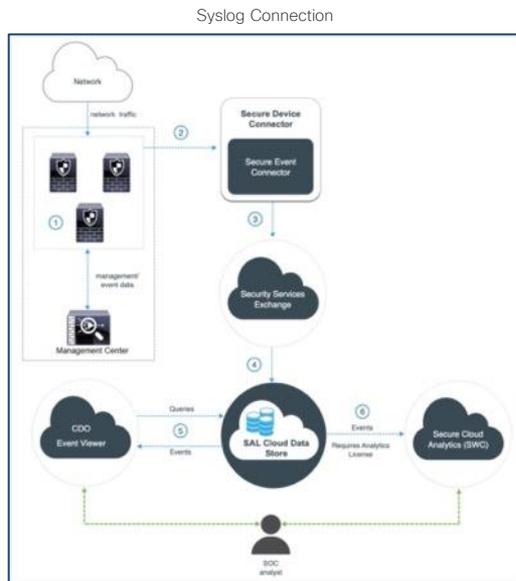
- さまざまな Cisco デバイスからのログを集約して分析することができるクラウドサービス
- セキュリティ分析とログは利用者の裁量で拡張できるため、長期間の保存が可能
- SAL SaaS に出力したログ情報は、CDO (Cisco Defense Orchestrator) もしくは SCA (Secure Cloud Analytics) で分析が可能
- 本セットアップガイドでは FMC と SAL SaaS の連携部分のみにフォーカスし、CDO と SCA の連携部分は解説の対象外とする
- SAL には On Premise 版の製品もあるが、本セットアップガイドでは SAL SaaS にフォーカスし、以降、SAL と言えば SAL SaaS を意味するものとする



# コネクションパターン

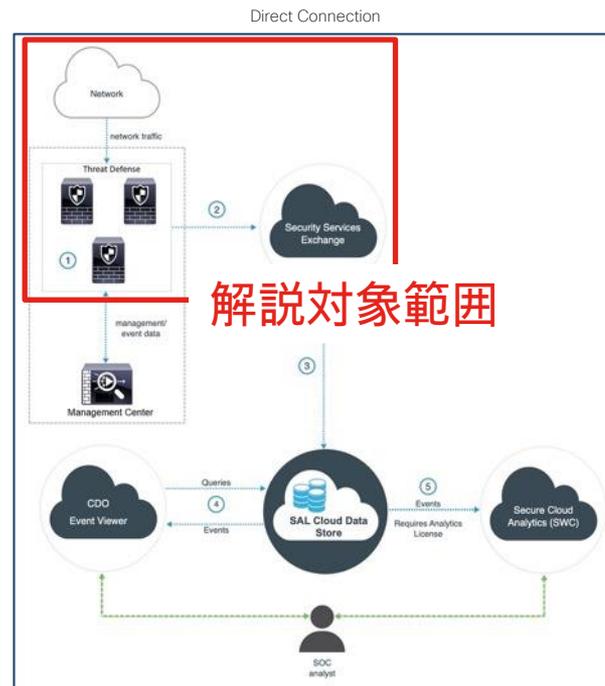
- FMC と SAL の接続方法は Syslog Connection と Direct Connection の 2パターン存在するが、本セットアップガイドでは Direct Connection にフォーカスして解説する。

## 本ガイドの解説対象



# 本セットアップガイドでのシナリオ

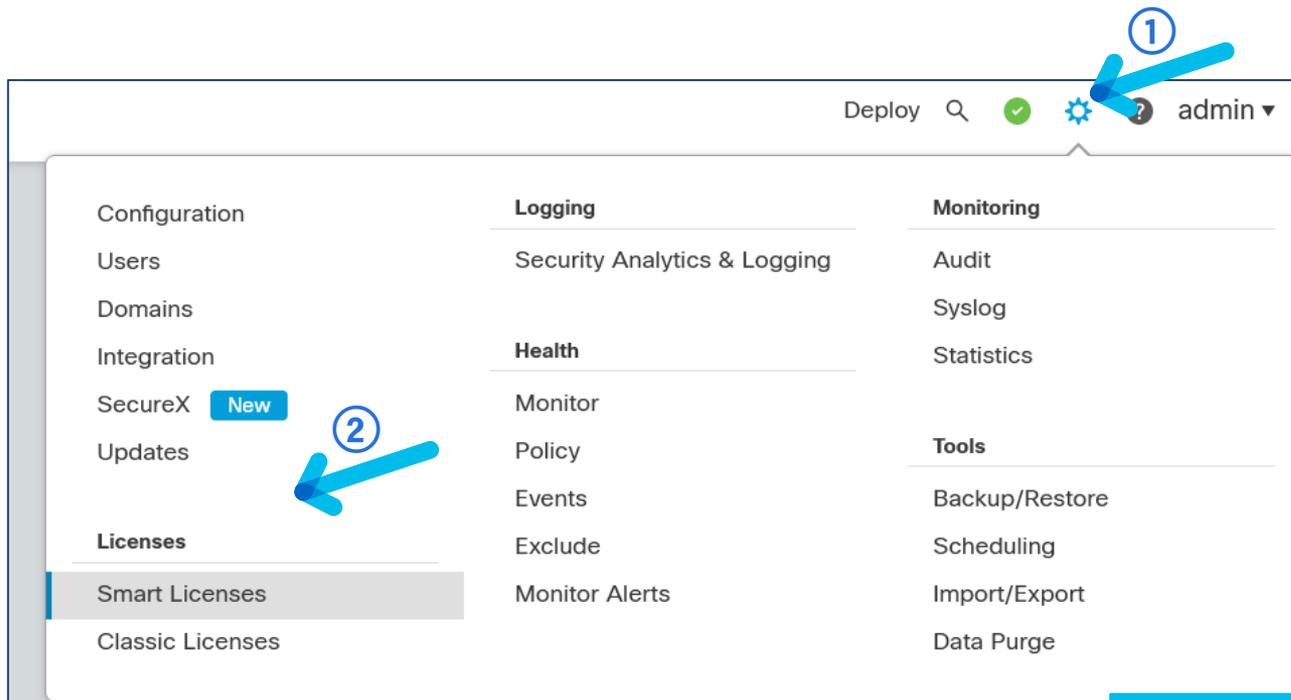
- Direct Connection パターンにおいて Security Services Exchange (SSE) との接続までの手順を解説する。



# 設定手順

1. Smart License 状態確認
2. Smart Account 権限確認
3. FMC から SSEに出力する Event の選択
4. SSE と Smart Account との同期
5. SSE から SAL への Event 出力確認

# ステップ1 : Smart License 状態確認



SSE への接続には FMC に登録している Smart Account / Virtual Account が必要

まずはその Smart Account / Virtual Account に正しく License が認識されているかを確認する

- ① FMC の System を選択
- ② Smart Licenses を選択

# ステップ1 : Smart License 状態確認

Smart License Status Cisco Smart Software Manager ✖ ↻

Usage Authorization:	✓	Authorized (Last Synchronized On Jul 12 2022)
Product Registration:	✓	Registered (Last Renewed On Jul 04 2022)

- ① Usage Authorization Status が Authorized であることを確認
- ② Product Registration Status が Registered であることを確認

# ステップ2 : Smart Account 権限確認

Cisco Software Central

Access everything you need to activate and manage your Cisco Smart Licenses.

## Download and manage

<b>Smart Software Manager</b> Track and manage your licenses. Convert traditional licenses to Smart Licenses. <a href="#">Manage licenses &gt;</a>	<b>Download and Upgrade</b> Download new software or updates to your current software. <a href="#">Access downloads &gt;</a>	<b>Traditional Licenses</b> Generate and manage PAK-based and other device licenses, including demo licenses. <a href="#">Access LRP &gt;</a>
<b>Manage Smart Account</b> Update your profile information and manage users. <a href="#">Manage account &gt;</a>	<b>EA Workspace</b> Generate and manage licenses purchased through a Cisco Enterprise Agreement. <a href="#">Access EA Workspace &gt;</a>	<b>Manage Entitlements</b> eDelivery, version upgrade, and more management functionality is now available in our new portal. <a href="#">Access MCE &gt;</a>

① Software Central  
(<https://software.cisco.com>) にアクセス  
して Manage Smart Account を選択

# ステップ2 : Smart Account 権限確認

Cisco Software Central > Manage Smart Account > Users

Account Properties | Virtual Accounts | **Users** | Requests | Notifications | Event Log

## Users

Users | User Groups

Add Users... | Export Selected...

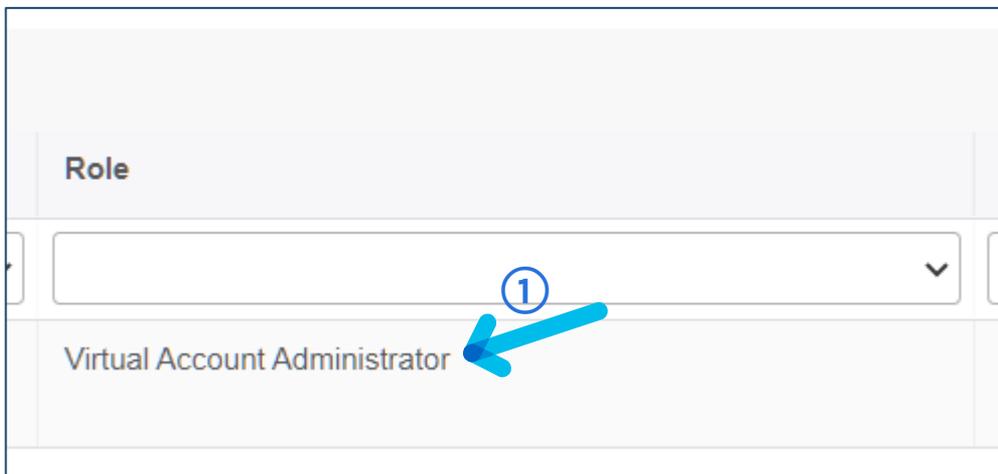
<input type="checkbox"/>	User ↑	Email

Annotation 1: A blue arrow points to the 'Users' tab in the navigation bar.

Annotation 2: Two blue arrows point to the 'User ↑' and 'Email' columns in the table header.

- ① Users を選択
- ② FMC に登録する User ID もしくは Email Address を検索

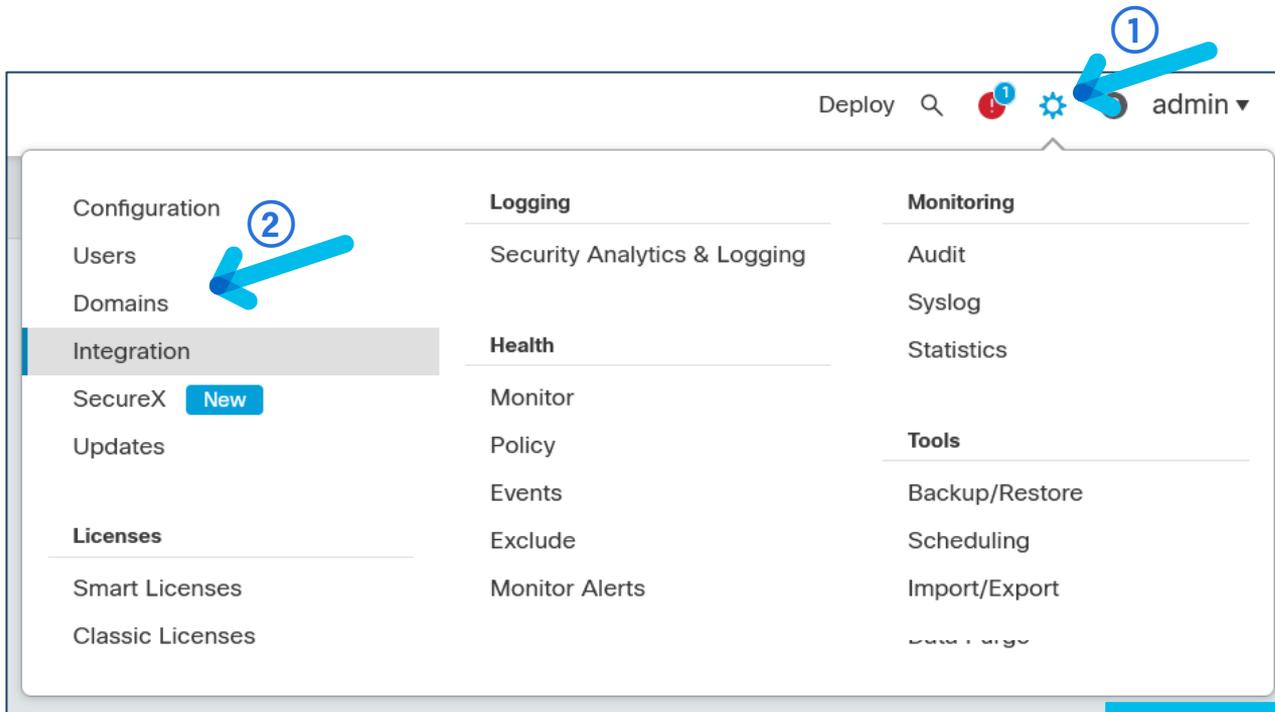
## ステップ2 : Smart Account 権限確認



FMC で登録している Smart Account の Virtual Account には、以下のいずれかの権限が無いと、SSE との接続設定ができない

- ① 表示された User の Role を確認して以下のいずれかの権限を持っていることを確認
  - Admin
  - Access Admin
  - Network Admin
  - Security Approver

# ステップ3 : FMC から SSE に出力する Event の選択



- ① FMC の System を選択
- ② Integration を選択

# ステップ3 : FMC から SSE に出力する Event の選択

The screenshot displays four configuration panels in a 2x2 grid:

- URL Filtering:** Includes a toggle for 'Enable Automatic Updates' (checked), a toggle for 'Query Cisco Cloud for Unknown URLs' (unchecked), a 'Cached URLs Expire' dropdown set to 'Never', and a 'Dispute URL categories and reputations' link.
- AMP for Networks:** Includes a toggle for 'Enable Automatic Local Malware Detection Updates' (checked) and a toggle for 'Share URI from Malware Events with Cisco' (unchecked).
- Cisco Cloud Region:** Features a 'Region' dropdown menu with a list of options: 'ap-northeast-1 (APJ Region)', 'eu-central-1 (EU Region)', and 'us-east-1 (US Region)'. A blue arrow labeled '1' points to the selected 'ap-northeast-1 (APJ Region)' option.
- Cisco Cloud Event Configuration:** Includes a toggle for 'Send Intrusion Events to the cloud' (unchecked), a toggle for 'Send File and Malware Events to the cloud' (unchecked), and a 'Send Connection Events to the cloud:' section with three buttons: 'None', 'Security Events', and 'All'. The 'All' button is selected. A blue arrow labeled '2' points to the 'All' button.

Each panel has a 'Save' button at the bottom right.

- ① Cisco Cloud Region から APJ Region を選択
- ② Save を選択

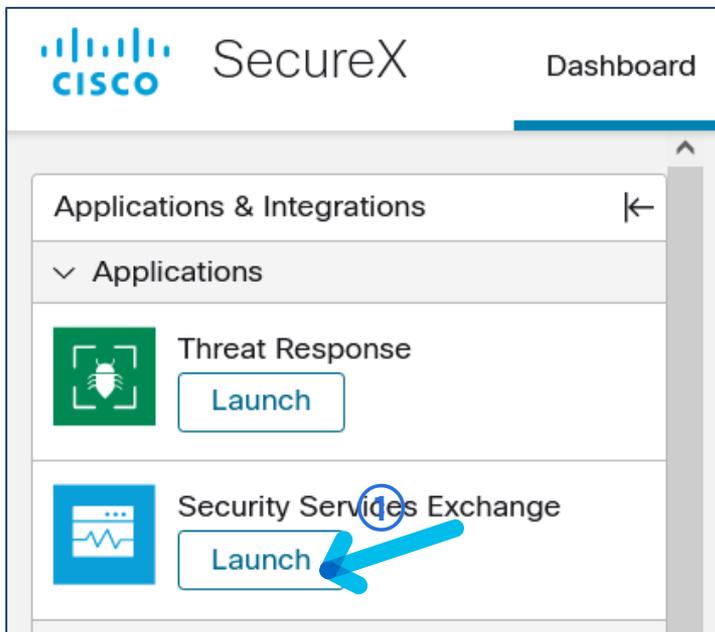
# ステップ3 : FMC から SSE に出力する Event の選択

The screenshot displays the configuration interface for Cisco FMC, divided into four main sections:

- URL Filtering:** Includes a toggle for 'Enable Automatic Updates' (checked), 'Query Cisco Cloud for Unknown URLs' (checked), and a 'Cached URLs Expire' dropdown set to 'Never'. A 'Save' button is at the bottom right.
- AMP for Networks:** Includes a toggle for 'Enable Automatic Local Malware Detection Updates' (checked) and a 'Share URI from Malware Events with Cisco' toggle (unchecked). A 'Save' button is at the bottom right.
- Cisco Cloud Region:** Features a 'Region' dropdown menu currently set to 'ap-northeast-1 (APJ Region)'. A 'Save' button is at the bottom right.
- Cisco Cloud Event Configuration:** This section is highlighted with a red arrow and the number '1'. It contains a main toggle for 'Cisco Cloud Event Configuration' (checked). Below it, there are two sub-toggles: 'Send Connection Events to the cloud' (checked, highlighted with a red arrow and '2') and 'Send Malware and Malware Events to the cloud' (checked). Underneath, there are radio buttons for 'Send Connection Events to the cloud': 'None', 'Security Events', and 'All' (selected, highlighted with a red arrow and '3'). A 'Save' button is at the bottom right.

- ① Cisco Cloud Event Configuration を有効化
- ② SSE に送信する Event を有効化
- ③ Save を選択

# ステップ4 : SSE と Smart Account との同期



① SecureX Dashboard\*1 で SSE の Launch を選択

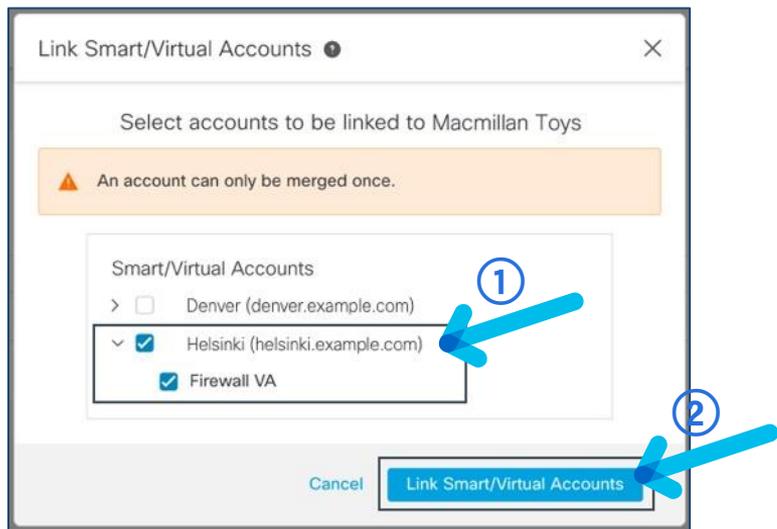
\*1 FMC と同期する SecureX Accounts にログインすること

# ステップ4 : SSE と Smart Account との同期

The screenshot displays the Cisco Security Services Exchange (SSE) interface. At the top, there are navigation tabs for 'Devices', 'Cloud Services', and 'Events'. The 'Devices' tab is active. Below the navigation, there is a search bar labeled 'Device Name / ID' and a table with columns: Name, Type, Versio..., Status, Description, and Actions. The table is currently empty, showing '0 Rows Selected' and 'No Devices Configured'. A context menu is open over the 'Actions' column, with the 'Link Smart/Virtual Accounts' option highlighted. A blue arrow points to this option, and a circled '1' is next to it. The footer contains copyright information and links to the Cisco Universal Cloud Agreement and Data Privacy Statement.

① Link Smart/Virtual Accounts を選択

# ステップ4 : SSE と Smart Account との同期



- ① 同期する Smart Accounts を選択
- ② Link Smart/Virtual Accounts を選択

# ステップ4 : SSE と Smart Account との同期

Security Services Exchange

Devices Cloud Services Events Audit Log

Yoshiki Ono

Devices for

Device Name / ID

0 Rows Selected

	¼	#	Name ^	Type	Version	Status	Cloud Connect...	Description	Actions
<input type="checkbox"/>	>	1	FMCv01	Cisco Firepow...	7.0.1.1	★ Registered	✓ 2022-07-13 11:	10.71.132.204 FMCv01	 
<input type="checkbox"/>	>	2	FTDv01	Cisco Firepow...	7.0.1.1	★ Registered	✓ 2022-07-13 11:	10.71.132.194 FTDv01 (FMC managed)	 

Page Size: 25 Total Entries: 2

1



① Smart Accounts に関連付いた FMC/FTD が表示されることを確認

# ステップ5 : SSE から SAL への Event 出力確認

The screenshot shows the Cisco Security Services Exchange (SSE) interface. The top navigation bar includes the Cisco logo, "Security Services Exchange", and tabs for "Devices", "Cloud Services", "Events", and "Audit Log". The "Events" tab is selected and highlighted with a blue arrow and a circled "1". Below the navigation bar, the "Event Stream for" section is visible, featuring a search filter "Enter filter criteria" and a date range "07/04/2022, 02:33 - 07/15/2022, 02:33". Below the filter, it indicates "0 Rows Selected". A table displays event data with columns: Talos Disposition, Incident, Destination IP, Reporting Device ID, Event Time, Ingest Time, Message, Primary Device ID, and Actions. The first two rows show "Trusted" Talos Disposition and "Yes" Incident status. A blue arrow and a circled "2" point to the "Incident" column.

	Talos Disposition	Incident	Destination IP	Reporting Device ID	Event Time	Ingest Time	Message	Primary Device ID	Actions
<input type="checkbox"/>	Trusted	Yes	208.67.220.220	48926160-b4fc-4024-a7da-f00a1440...	2022-07-07 09:39:43 UTC	2022-07-07 09:39:48 UTC	PROTOCOL-IC...		
<input type="checkbox"/>	Trusted	Yes	208.67.220.220	48926160-b4fc-4024-a7da-f00a1440...	2022-07-07 09:39:43 UTC	2022-07-07 09:39:48 UTC	PROTOCOL-IC...		

FMC と SSE で同じ Smart Account / Virtual Account が紐付いているため、FMC で設定した Cloud Event 設定により、FTD が処理を行った通信イベントのログが SSE にも表示される

- ① SSE の Events を選択
- ② Event が出力されていることを確認\*1

\*1 事前に FTD を経由する ICMP 等で Event を発生させること

SecureX 連携編

# SecureX とは

- Cisco のセキュリティポートフォリオだけでなく、サードパーティのポートフォリオとも統合可能な XDR ソリューション
- 複数ソリューションのイベント情報を一つのダッシュボードで集約することができ、相関分析により運用効率が向上
- 脅威ハンティング機能も備えており、最新の脅威情報（マルウェアのハッシュ値等）から組織内にその脅威情報が含まれるかどうかを調査可能
- オーケストレーション機能により、マニュアル作業の自動化が可能



# 設定手順

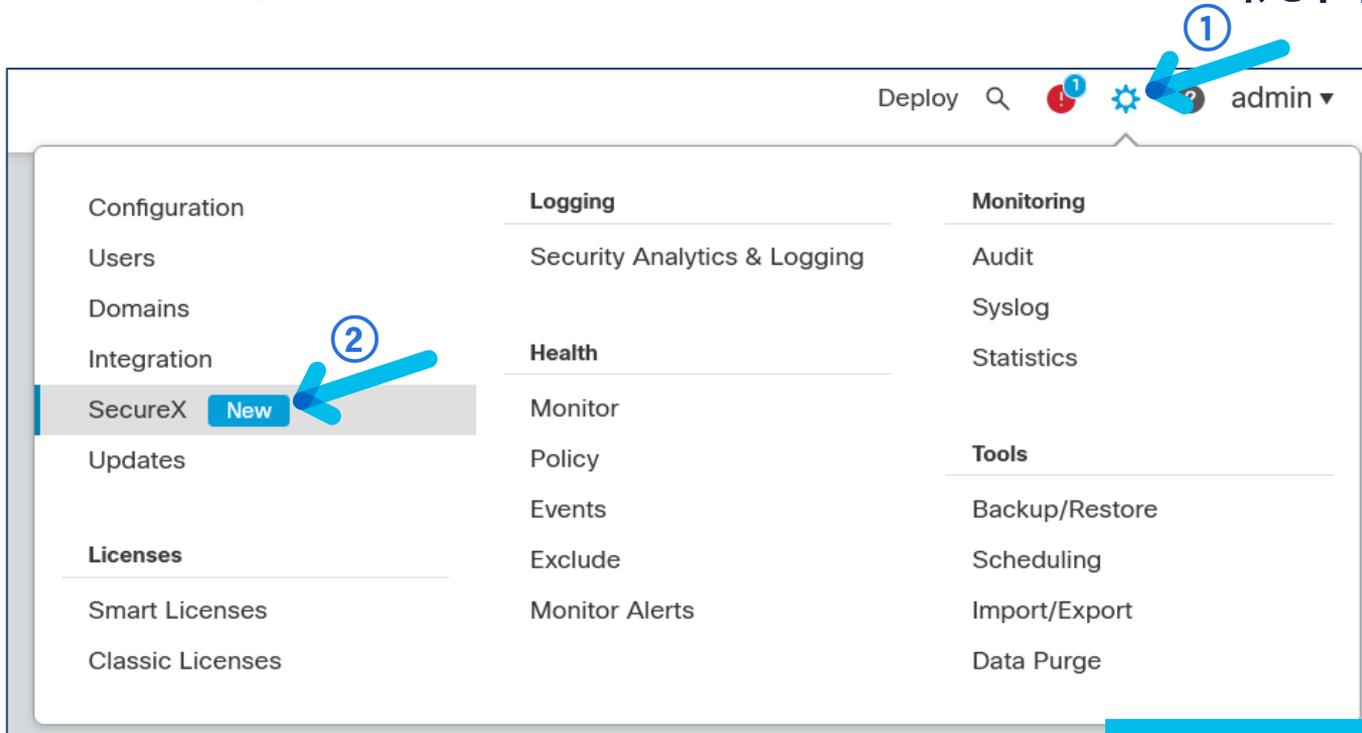
1. Smart License 状態確認
2. Smart Account 権限確認
3. FMC から SSEに出力する Event の選択
4. SSE と Smart Account との同期

---

5. FMC と SecureX との統合
6. SecureX での Module 追加
7. SecureX での Tile 追加
8. FMC から SecureX への Event 出力確認

ここまで SSE 連携編のステップ4までと  
全く同じ手順なので、説明は割愛

# ステップ5 : FMC と SecureX との統合



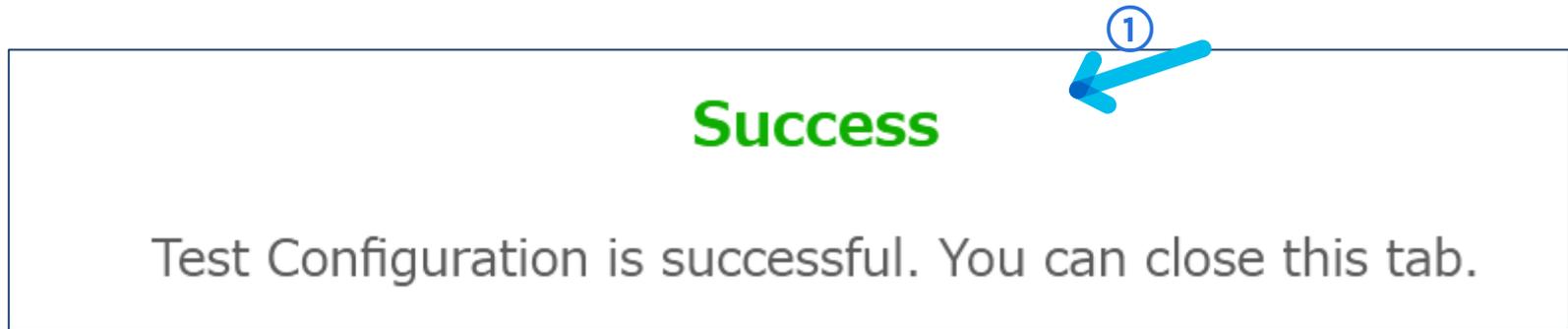
- ① FMC の System を選択
- ② SecureX を選択

# ステップ5 : FMC と SecureX との統合

The image shows two side-by-side screenshots from the Cisco SecureX interface. The left screenshot is titled "SecureX Configuration" and contains a toggle switch (1), a list of steps (2), and input fields for "Client ID" (11) and "Client Password" (12). The right screenshot is titled "Add New Client" and shows a form with fields for "Client Name" (4), "Client Preset" (5), "Scopes" (6), "Redirect URL" (7), "Add another Redirect URL" (8), "Availability" (9), and "Description" (10). Red arrows labeled "copy" point from the URLs in the left screenshot to the "Redirect URL" field in the right screenshot.

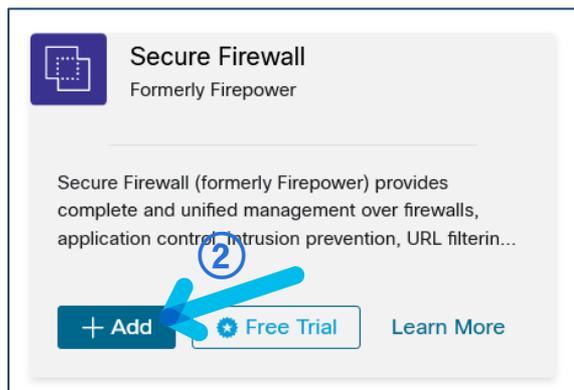
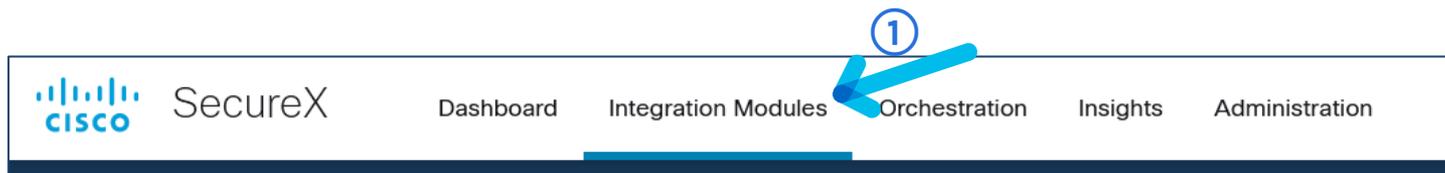
- ① SecureX Configuration を有効化
- ② APJ Region が選択されていることを確認
- ③ Create a SecureX API client を選択
- ④ 任意の API Client 名を入力
- ⑤ OAuth Code Clients を選択
- ⑥ Scopes は 事前設定されているためスキップ
- ⑦ Redirect URL に FMC からコピーした URL を入力
- ⑧ Add another Redirect URL を選択
- ⑨ もう一つの Redirect URL に FMC からコピーしたもう一つの URL を入力
- ⑩ Add New Client を選択
- ⑪ 表示される Client ID と Client Password を FMC に入力
- ⑫ Save を選択

## ステップ5 : FMC と SecureX との統合



① Success と表示されることを確認

# ステップ6 : SecureX での Module 追加



- ① SecureX のメニュー画面から Integration Modules を選択
- ② Secure Firewall の Module を選択して Add をクリック

# ステップ6 : SecureX での Module 追加

SecureX Dashboard Integration Modules Orchestration Insights Administration

## Add New Secure Firewall Integration Module

Integration Module Name  
Secure Firewall

Manage Devices Check for New Devices

Name	Version	Status	Description	IP Address
FMCv01	7.0.1.1	Registered	10.71.132.204 FMCv01	10.71.132.204
FTDv01	7.0.1.1	Registered	10.71.132.194 FTDv01 (FMC managed)	10.71.132.194

5 per page 1-2 of 2 << 1 /1 >>

Create Dashboard  
Create a dashboard of the tiles associated with this integration module, which can be shared by all members of your organization.

Cancel Save

- ① Integration Module Name に適切な名前を入力する
- ② 登録する Device が表示されていることを確認する \*1
- ③ Save を選択

\*1 登録できる Device は Administration > Devices で確認可能

# ステップ6 : SecureX での Module 追加

SecureX Dashboard Integration Modules Orchestration Insights Administration

## Edit FTD Setup Guide 7.0 Module ①

✔ This integration module has no issues.

Integration Module Name  
FTD Setup Guide 7.0

Manage Devices Check for New Devices

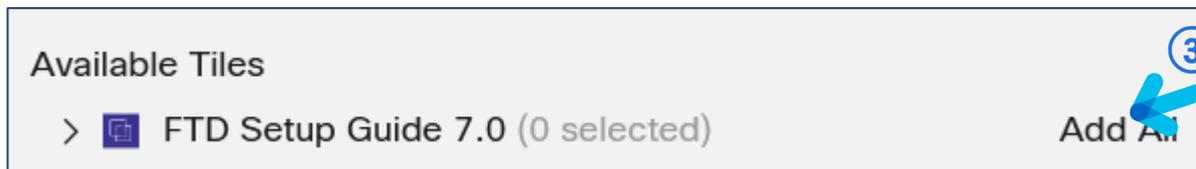
Name	Version	Status	Description	IP Address
FMCv01	7.0.1.1	Registered	10.71.132.204 FMCv01	10.71.132.204
FTDv01	7.0.1.1	Registered	10.71.132.194 FTDv01 (FMC managed)	10.71.132.194

5 per page 1-2 of 2 << 1 /1 >>

Delete Cancel Save

① 正常に登録できたことを確認

# ステップ7 : SecureX での Tile 追加



- ① SecureX の Dashboard を選択
- ② Customize を選択
- ③ ステップ5 で入力した Integration Module Name を確認し Add を選択

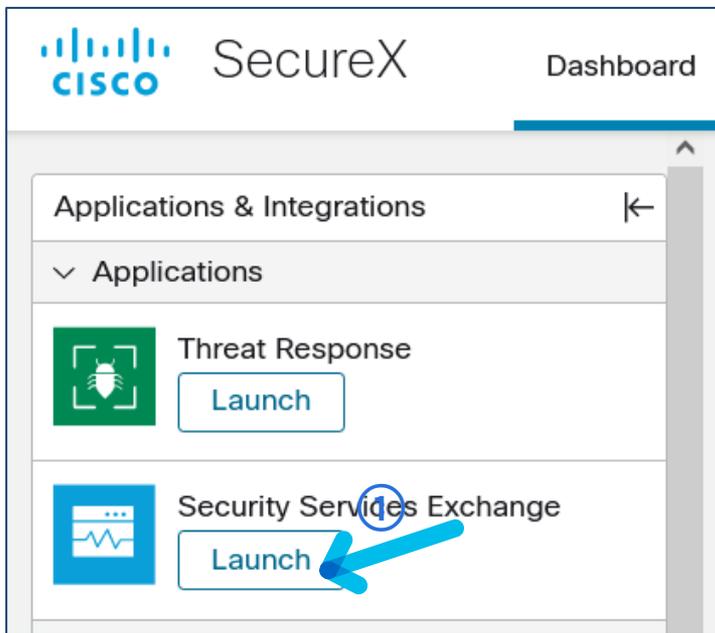
# ステップ7 : SecureX での Tile 追加



- ① 追加したい Tile を選択\*1
- ② Save を選択

\*1 必要に応じて Dashboard を作成

## ステップ8 : FMC から SecureX への Event 出力確認



- ① SecureX Dashboard で SSE の Launch を選択

# ステップ8 : FMC から SecureX への Event 出力確認

Event Stream for

07/04/2022, 02:33 - 07/15/2022, 02:33

0 Rows Selected

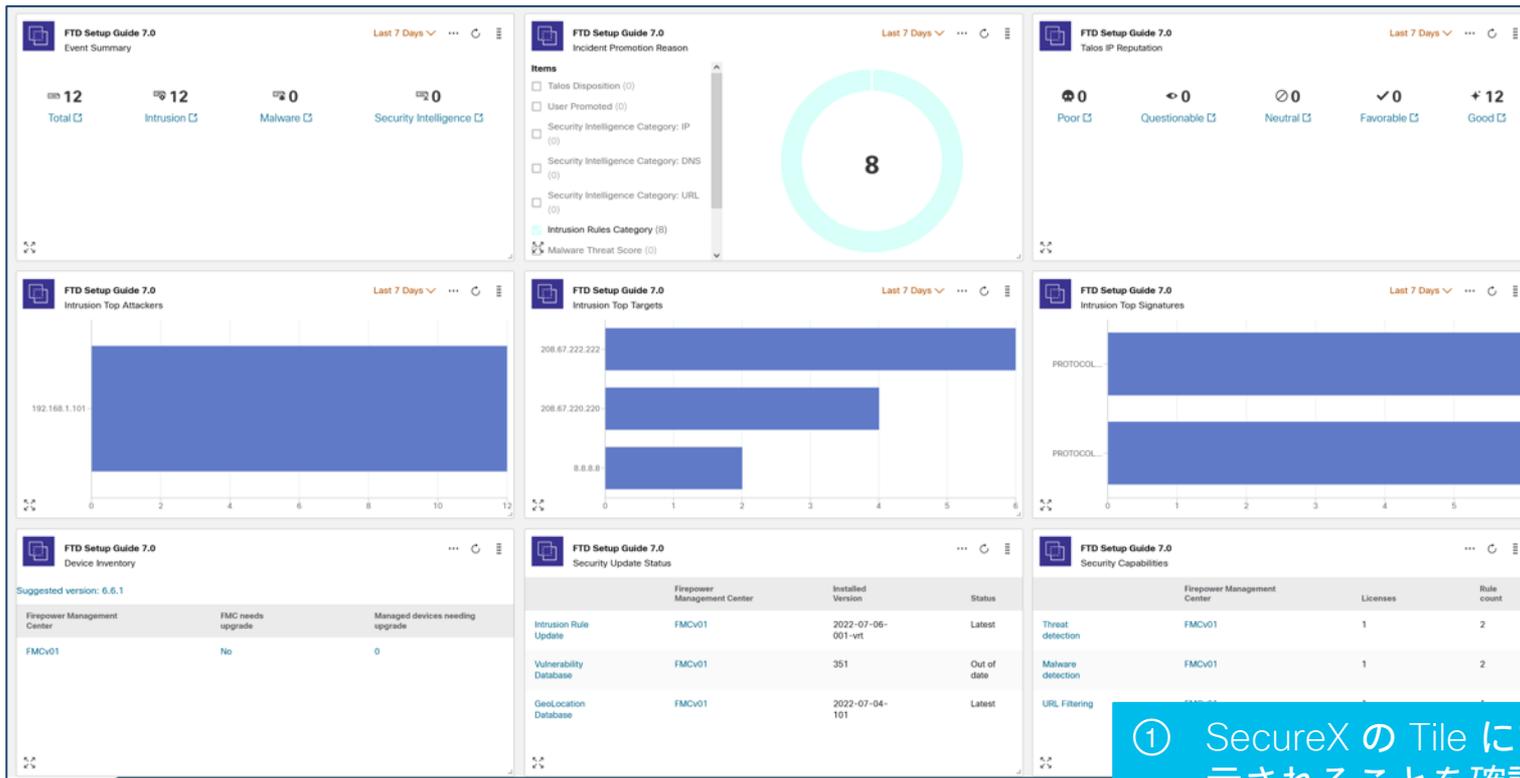
<input type="checkbox"/>	Talos Disposition	Incident	Destination IP	Reporting Device ID	Event Time	Ingest Time	Message	Primary Device ID	Actions
<input type="checkbox"/>	Trusted	Yes	208.67.220.220	48926160-b4fc-4024-a7da-f00a1440...	2022-07-07 09:39:43 UTC	2022-07-07 09:39:48 UTC	PROTOCOL-IC...		
<input type="checkbox"/>	Trusted	Yes	208.67.220.220	48926160-b4fc-4024-a7da-f00a1440...	2022-07-07 09:39:43 UTC	2022-07-07 09:39:48 UTC	PROTOCOL-IC...		

まずは SSE に Event が送られていることを確認

- ① Events を選択
- ② FMC から送信された Event 情報が表示されることを確認\*1

\*1 事前に FTD を経由する ICMP 等で Event を発生させること

# ステップ8 : FMC から SecureX への Event 出力確認



① SecureX の Tile にて Event 情報が表示されることを確認

## 19. 設定のロールバック

# 設定ロールバックとは

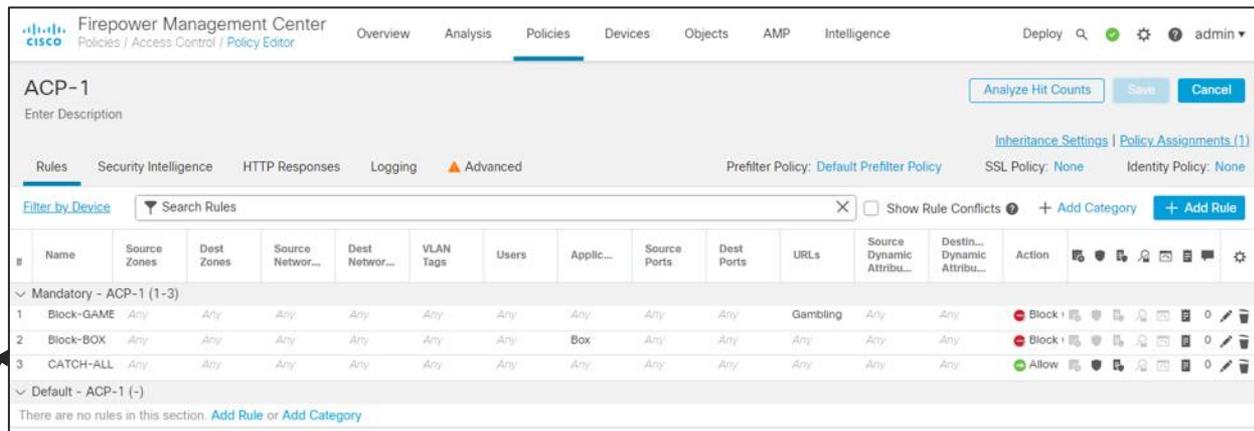
- FMC から FTD に設定変更内容をデプロイした後に、以前の FTD に戻す機能
- 間違った設定、ふさわしくない設定をデプロイしてしまった後に、まずは以前の正しく動いていた設定に戻すことができる
- 10世代前までの設定に戻すことが可能
- FMC から FTD へのデプロイ後に互い管理インターフェイス間の通信が途絶えてしまうような間違った設定により、FMC から FTD への設定変更ができないような場合には、FTD の CLI から1世代前の設定に戻すことが可能
  - (参考) バージョン 7.2 では SFTunnel の断を自動的に検知して自動的にロールバックすることも可能

# 設定ロールバックの注意点

- VDB や SRU / LSP 等のコンテンツアップデートはロールバックできない (関連の設定はロールバックされる)
- ソフトウェア更新を行う以前にはロールバックできない
- ロールバック中、一時的にコネクションテーブルや経路情報が消えるため、通信が途絶える
- 当該機能は FTD のためのものであり、ロールバック後は FTD の設定だけが指定したものに戻るが、FMC の設定は戻らず、FTD の設定は全て out-of-date となる。次の FMC からのデプロイ実施時は、全ての設定が上書きされてのデプロイとなる
- 設定ロールバックは緊急時に利用するものと理解しておく

# ロールバックのユースケース

Access Control Policy  
に間違ったルールを入  
れてしまったため、す  
ぐにデプロイ前の FTD  
の設定に戻したい



#	Name	Source Zones	Dest Zones	Source Network...	Dest Network...	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source Dynamic Attribu...	Destin... Dynamic Attribu...	Action
Mandatory - ACP-1 (1-3)														
1	Block-GAME	Any	Any	Any	Any	Any	Any	Any	Any	Any	Gambling	Any	Any	Block
2	Block-BOX	Any	Any	Any	Any	Any	Any	Box	Any	Any	Any	Any	Any	Block
3	CATCH-ALL	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
Default - ACP-1 (-)														

デプロイ前の正しい  
FTD の設定 (FMC)

デプロイ前の正しい  
FTD の ACL

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list CSM_FW_ACL_ ; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 8 remark rule-id 268434434: ACCESS POLICY: ACP-1 - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268434434: L7 RULE: Block-GAMBLE
access-list CSM_FW_ACL_ line 10 advanced permit ip any any rule-id 268434434 (hitcnt=699) 0xa1d3780e
access-list CSM_FW_ACL_ line 11 remark rule-id 268434432: ACCESS POLICY: ACP-1 - Default
access-list CSM_FW_ACL_ line 12 remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 13 advanced deny ip any any rule-id 268434432 (hitcnt=0) 0x97aa021a
```

# ルールバックのユースケース (続き)

間違えて ACP 1 行目に outgoing の通信をブロックする設定を入れてデプロイを実施 (FMC)

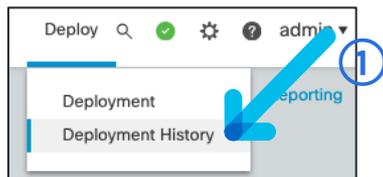
#	Name	Source Zones	Dest Zones	Source Network	Dest Network	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source Dynamic Attrib...	Destin... Dynamic Attrib...	Action
1	Mandatory - ACP-1 (1-4)													Block +
2	Block-GAME	Any	Any	Any	Any	Any	Any	Any	Any	Any	Gambling	Any	Any	Block +
3	Block-BOX	Any	Any	Any	Any	Any	Any	Box	Any	Any	Any	Any	Any	Block +
4	CATCH-ALL	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow

間違えて入れたルールが FTD にデプロイされてしまっている状態

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list CSM_FW_ACL; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL line 3 advanced permit ip ip ip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL line 8 remark rule-id 268434439: ACCESS POLICY: ACP-1 - Mandatory
access-list CSM_FW_ACL line 9 remark rule-id 268434439: L7 RULE: BLOCK-OUTGOING
access-list CSM_FW_ACL line 10 advanced permit ip ifc inside any ifc outside any rule-id 268434439 (hitcnt=1) 0xeebe6992
access-list CSM_FW_ACL line 11 remark rule-id 268434434: ACCESS POLICY: ACP-1 - Mandatory
access-list CSM_FW_ACL line 12 remark rule-id 268434434: L7 RULE: Block-GAMBLE
access-list CSM_FW_ACL line 13 advanced permit ip any any rule-id 268434434 (hitcnt=409) 0x1d3780e
access-list CSM_FW_ACL line 14 remark rule-id 268434432: ACCESS POLICY: ACP-1 - Default
access-list CSM_FW_ACL line 15 remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL line 16 advanced deny ip any any rule-id 268434432 (hitcnt=0) 0x97aa021a
```

# FMC での設定ロールバック実施 ①

- FTD に間違った設定や、意図しない設定をデプロイしてしまったために、とりあえず FTD の設定を以前のものに戻したい場合に、ロールバックを開始



- ① Deploy → Deployment をクリック
- ② Rollback をクリック

Firepower Management Center  
Deploy / Deployment History

Overview Analysis Policies Devices Objects AMP Intelligence Deploy Q [status] [gear] [help] admin

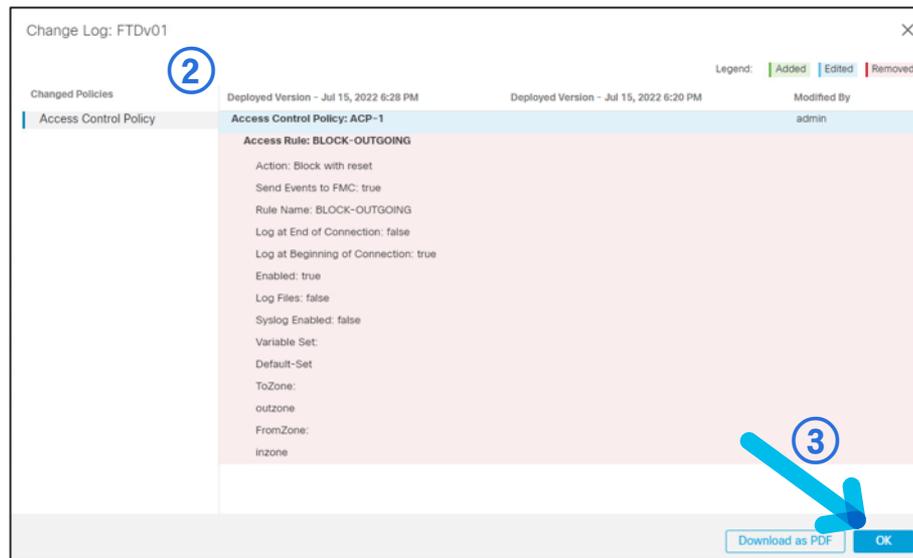
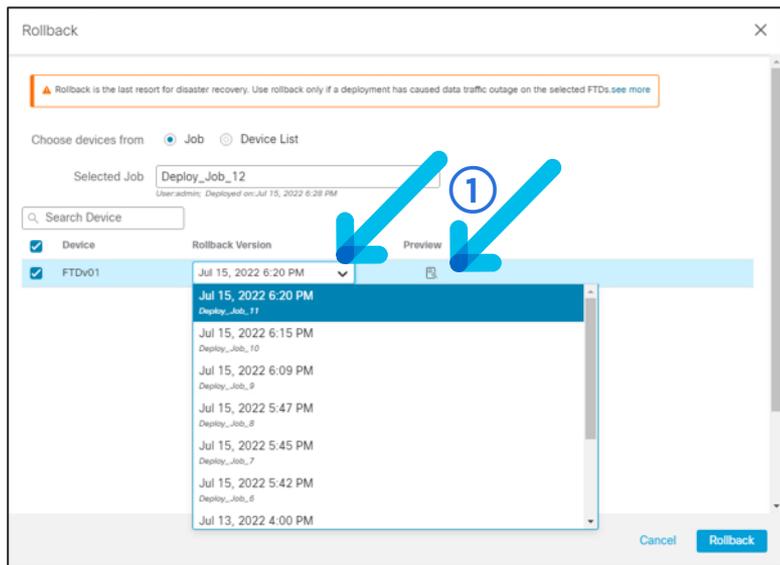
Rollback

Search using job name, device name, user name, status or deployment notes

Job Name	Deployed by	Start Time	End Time	Status	Deployment Notes
Deploy_Job_12	admin	Jul 15, 2022 6:27 PM	Jul 15, 2022 6:28 PM	Completed	
Deploy_Job_11	admin	Jul 15, 2022 6:19 PM	Jul 15, 2022 6:20 PM	Completed	
Deploy_Job_10	admin	Jul 15, 2022 6:14 PM	Jul 15, 2022 6:15 PM	Completed	
Deploy_Job_9	admin	Jul 15, 2022 6:08 PM	Jul 15, 2022 6:09 PM	Completed	
Deploy_Job_8	admin	Jul 15, 2022 5:46 PM	Jul 15, 2022 5:47 PM	Completed	
Deploy_Job_7	admin	Jul 15, 2022 5:43 PM	Jul 15, 2022 5:45 PM	Completed	
Deploy_Job_6	admin	Jul 15, 2022 5:40 PM	Jul 15, 2022 5:42 PM	Completed	
Deploy_Job_5	admin	Jul 13, 2022 3:59 PM	Jul 13, 2022 4:00 PM	Completed	
Rollback_Job_1	admin	Jul 13, 2022 3:53 PM	Jul 13, 2022 3:54 PM	Rollback Passed	Rollback Job
Deploy_Job_4	admin	Jul 13, 2022 3:52 PM	Jul 13, 2022 3:52 PM	Completed	
Deploy_Job_3	admin	Jul 13, 2022 3:45 PM	Jul 13, 2022 3:46 PM	Completed	
Deploy_Job_2	admin	Jul 13, 2022 3:32 PM	Jul 13, 2022 3:33 PM	Completed	

# FMC での設定ロールバック実施 ②

- ・ 戻したい設定をデプロイした時間の Job を選択し、プレビューを確認



- ① 戻したい設定をデプロイした Job を選択し、Preview をクリック
- ② この Job にロールバックすると変更される差分のプレビューが表示される
- ③ 差分に問題がなければ OK をクリック

# FMC での設定ロールバック実施 ③

- FTD への設定ロールバックを実施

Rollback

Rollback is the last resort for disaster recovery. Use rollback only if a deployment has caused data traffic outage on the selected FTDs. see more

Choose devices from  Job  Device List

Selected Job

User:admin; Deployed on: Jul 15, 2022 6:28 PM

Search Device

Device	Rollback Version	Preview
<input checked="" type="checkbox"/> FTDv01	<input type="text" value="Jul 15, 2022 6:20 PM"/>	<input type="text"/>

Cancel Rollback

Firepower Management Center

Deploy / Deployment History

Rollback is triggered for FTDv01

Search using job name, device name, user name, state

Job Name	Deployment
----------	------------

Warning

Rollback clears all configurations on the FTD and reconfigures the FTD with the previous version causing existing connections/routes to be dropped. It is advisable to roll back configurations only in extreme circumstances. It is better to fix policy configurations in the FMC and deploy them to the FTD. Do you still want to proceed with the rollback?

Cancel Proceed

Deployments Upgrades Health Tasks

1 total 1 running 0 success 0 warnings 0 failures

FTDv01 Rollback - Preparing policy configuration on the device. 75% 25s

Deployments Upgrades Health Tasks

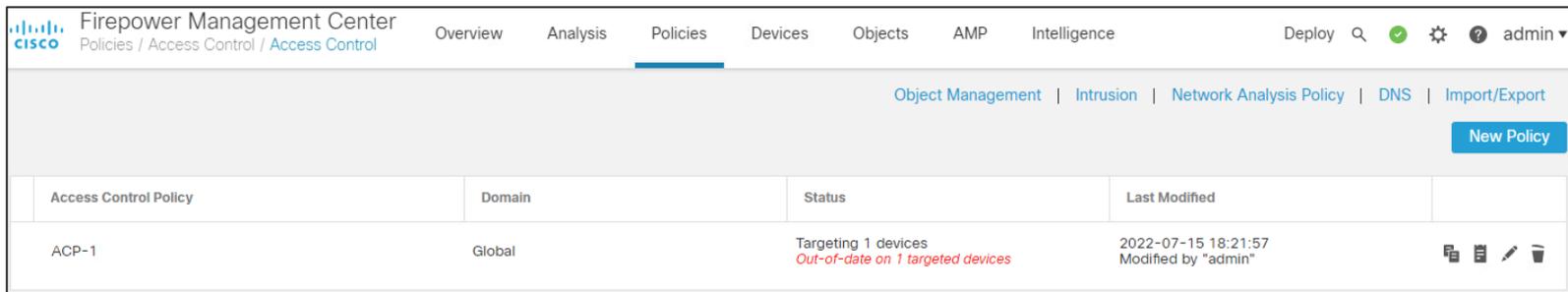
1 total 0 running 1 success 0 warnings 0 failures

FTDv01 Rollback successful. 1m 13s

- ① Rollback をクリック
- ② ロールバック時の警告が表示される。問題なければ Proceed をクリック
- ③ 指定した FTD デバイスに対してロールバックが開始される
- ④ Task 画面よりロールバックの進捗状況を確認できる
- ⑤ ロールバックが無事に完了した旨が Task 画面に表示される

# FMC での設定ロールバック実施 ④

- FTD の実際の設定は戻っていることが確認できる。FMC 側の設定はそのままであり、デプロイした内容が out-of-date になっていることがわかる



Access Control Policy	Domain	Status	Last Modified	
ACP-1	Global	Targeting 1 devices <i>Out-of-date on 1 targeted devices</i>	2022-07-15 18:21:57 Modified by "admin"	  

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list CSM_FW_ACL_ ; 7 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 8 remark rule-id 268434434: ACCESS POLICY: ACP-1 - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268434434: L7 RULE: Block-GAMBLE
access-list CSM_FW_ACL_ line 10 advanced permit ip any any rule-id 268434434 (hitcnt=146) 0xa1d3780e
access-list CSM_FW_ACL_ line 11 remark rule-id 268434432: ACCESS POLICY: ACP-1 - Default
access-list CSM_FW_ACL_ line 12 remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 13 advanced deny ip any any rule-id 268434432 (hitcnt=0) 0x97aa021a
```

# FMC での設定ロールバック実施 ⑤

- FMC 側で間違っていた設定を直し、再度 deploy を実施する。このとき、FTD 側への設定変更は差分ではなく、全ての設定が上書きされる。プレビューでもその旨のアラートが表示される

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Deploy' and 'admin'. A table lists devices, with 'FTDv01' selected. A 'Change Log' dialog box is open, showing a warning message: 'FMC has rolled back the device configuration to the version deployed on 2022 Jul 15 09:20:07 (UTC). As rollback doesn't revert the configuration changes in FMC, all the policies are marked as out-of-date. In preview, the out-of-date policies and objects with no configuration changes are excluded. Use the information on this page to identify the configuration that caused the user to perform the rollback operation.' Below the message is a table of 'Changed Policies'.

Changed Policies	Deployed Version	Version on FMC	Modified By
Intrusion Policy	Intrusion Policy:		
Network Analysis Policy			

# FTD CLI での設定ロールバック実施 ⑤

- FTD の CLI で1世代前の設定にロールバックすることも可能。FMC と FTD を接続する管理通信 (SFTunnel) がダウンしてしまった場合の緊急避難として有益

> configure policy rollback

```
> configure policy rollback
-----
[Warning] Perform a policy rollback if the FTD communicates with the FMC on a data interface, and it has lost connectivity due to a policy deployment from the FMC. If the FTD still has connectivity to the FMC, and you want to perform a policy rollback for other purposes, then you should do the rollback on the FMC and not with this command. Note that there will be a traffic drop when you rollback the policy.

===== DEVICE DETAILS =====
Device Version: 7.0.1
Device Type: FTD
Device Mode: Offbox
Device in HA: false
Device in Cluster: false
Device Upgrade InProgress: false
=====

Checking Eligibility ...
Device is eligible for rollback

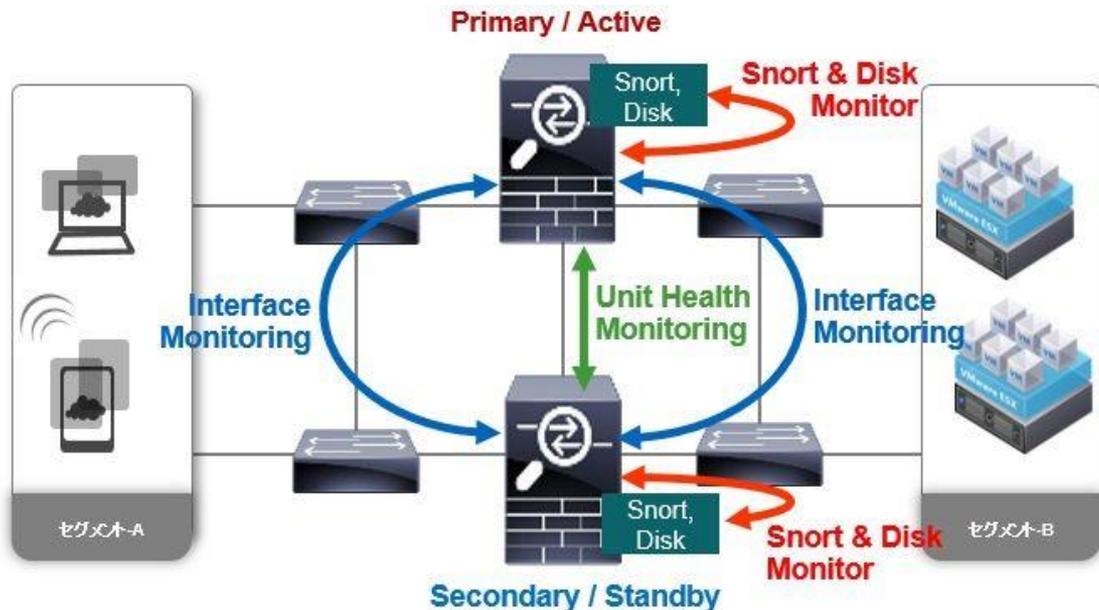
This command will rollback the policy to the last deployment done on Jul 15 09:46.
[Warning] The rollback operation will revert the convergence mode.
Do you want to continue (YES/NO)? yes

Starting rollback...
Deployment of Platform Settings to device.           Status: success
Preparing policy configuration on the device.        Status: success
Applying updated policy configuration on the device. Status: success
Applying Lina File Configuration on the device.      Status: success
Applying Lina Configuration on the device.          Status: success
Commit Lina Configuration.                          Status: success
Commit Lina File Configuration.                     Status: success
Finalizing policy configuration on the device.       Status: success
=====
POLICY ROLLBACK STATUS: SUCCESS
=====
>
```

## 20. FTD High Availability の設定

# FTD High Availability (HA) について

- FTD では高可用性の実現のためにアクティブ/スタンバイフェイルオーバーをサポート



- 設定・動作イメージは ASA HA と同様
- FTD ではヘルスマonitoringとしてインタフェース以外に、Snort プロセスや Disk の障害監視も実施
- AWS 等パブリッククラウド上にデプロイされた FTDv は HA 非サポート

# HA 設定における事前確認事項

- 同じモデルあること
- 同じインターフェイス数とインターフェイスタイプであること。モジュール利用時は、同じモジュールを各デバイスに装着すること
- 同じソフトウェアバージョンを利用していること
- 同じ firewall モードであること。Routed (default)、もしくは Transparent
- DHCP や PPPoE 設定をインターフェイスにしていないこと。DHCP のアドレス割当てや PPPoE 接続情報は、同期非サポートのため
- ヘルスモニターの状態が各デバイスで Normal (正常) であること
- すべての設定変更が各デバイスでデプロイ済みであること
- 2台分のライセンスを用意すること。FTD HA では、各デバイスに同じライセンス割当が必要のため、例えば IPS 機能を使う場合は、Threat ライセンスが 2つ必要。HA 構成での購入時にディスカウントされたバンドル型番有り。なお、物理アプライアンスの Base ライセンスは各 FTD デバイス内に同梱されており自動使用されるため準備は不要
- 既に稼働中の FTD デバイス (スタンドアロン) に、新規 FTD デバイスを追加し冗長ペアを組む場合、通信影響の少ない時間帯や メンテナンスタイムに実施すること。FTD HA を組む際、Snort 自動再起動が発生し、通信影響が発生するため

# ネットワーク環境図

Internet

■ 設定済みの機器

MGMT NW

.135.254

DNS: 64.104.14.184

ntp.esl.cisco.com

proxy-wsa.esl.cisco.com

10.71.128.0/21

Management

.132.194

G0/0 outside .101

test PC2

G0/2 failover 192.168.10.1

G0/1 inside .1

G0/2 failover 192.168.10.2

G0/0 outside .2

.132.204

FMCv

.132.170

G0/1 inside .2

G0/0 outside .2

.132.130

ISE-PIC01

内部LAN  
192.168.1.0/24

.11

.101

.132.220

ESXi

.132.131

AD01.secvt.jp

test PC1

g0/0 グローバルアドレス

ASA

g0/3 .254

外部LAN

192.168.240.0/24

管理NW (実態はシスコ検証NW)

顧客NW

PAT

PAT

# ステップ1-1: HA 設定 - 事前準備・確認

- HA 構成のために FTDv02 を新たにインストールし、初期セットアップおよび FMC への管理登録を実施（手順は FTDv01 と同様）
- HA を構成する FTD の状態が問題ないことを確認

Firepower Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 🔍 1 ⚙️ ? admin ▾

View By: Group

All (2) ● Error (0) ● Warning (0) ● Offline (0) ● **Normal (2)** ● Deployment Pending (0) ● Upgrade (1) ● Snort 3 (2)

Q Search Device Add ▾

Collapse All

<input type="checkbox"/>	Name	Model	Vers...	Chassis	Licenses	
<input type="checkbox"/>	▼ Ungrouped (2)					
<input type="checkbox"/>	FTDv01 Snort 3 10.71.132.194 Routed	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...) ACP-1	✎ ⋮
<input type="checkbox"/>	FTDv02 Snort 3 10.71.132.170 Routed	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...) ACP-1	✎ ⋮

③ 未適用の設定の有無、  
実行中のタスクの有無も確認

②

- HA を構成する 2機のヘルス状態が正常であること
- モデル、モード、バージョン、ライセンス等が同じであること

# ステップ2-1: HA 設定 - FTDv01 の HA リンクのための IF 有効化

Firepower Management Center  
Devices / Device Management

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (1) Snort (3 (2))

Name	Model	Vers...	Chassis	Licenses	Access Control Policy
FTDv01 10.71.132.194 - Routed	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...)	ACP-1
FTDv02 10.71.132.170 - Routed	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...)	ACP-1

- ① Device Management より FTDv01 の鉛筆マークをクリック
- ② Interface タブをクリックし、Gig0/2 の鉛筆マークをクリック
- ③ General の Enable にチェック
- ④ OK をクリック
- ⑤ Save をクリックして設定を保存

Firepower Management Center  
Devices / NGFW Interfaces

FTDv01  
Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP

Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Virtual Router
Diagnostic0/0	diagnostic	Physi...				Global
GigabitEthernet0/0	Outside	Physi...	Outside_Zone		192.168.240.1/24(Static)	Global
GigabitEthernet0/1	Inside	Physi...	Inside_Zone		192.168.1.1/24(Static)	Global
GigabitEthernet0/2		Physi...				
GigabitEthernet0/3		Physi...				
GigabitEthernet0/4		Physi...				

Displaying 1-9 of 9 interfaces Page 1 of 1

Edit Physical Interface

General IPv4 IPv6 Advanced Hardware Configuration FMC Access

Name:

Enabled

Management

Description:

Mode: None

Security Zone:

Interface ID: GigabitEthernet0/2

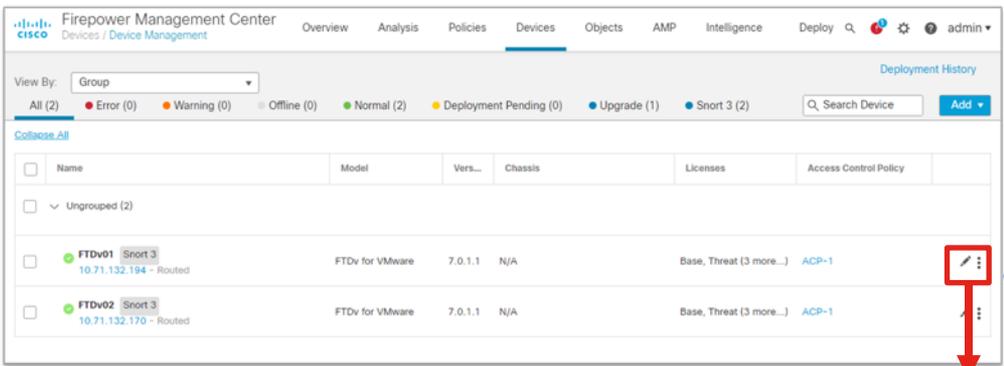
MTU: 1500 (64 - 9000)

Propagate Security Group Tag:

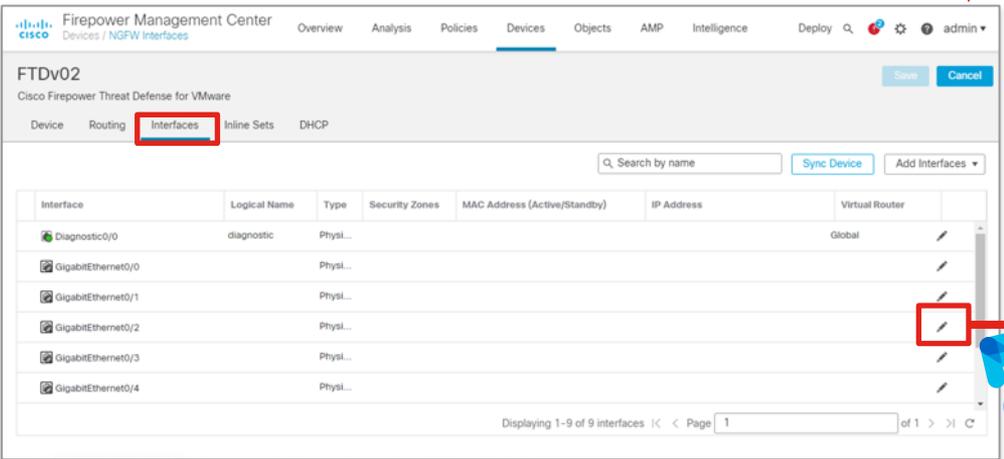
OK

注: ESXi で HA リンク接続用の仮想スイッチを別途作成必要

# ステップ2-2: HA 設定 - FTDv02 の HA リンクのための IF 有効化

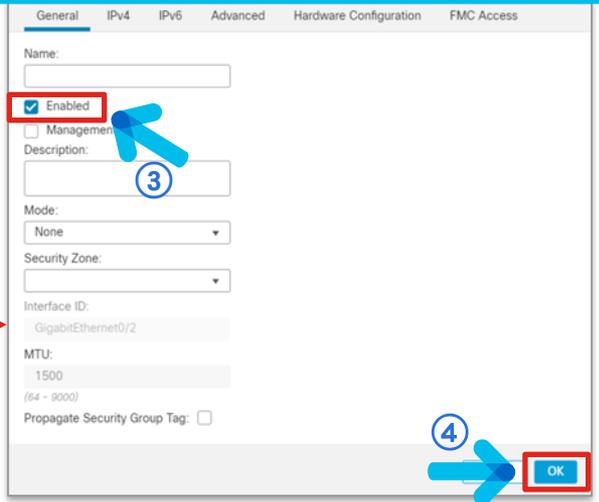


①



②

- ① Device Management より FTDv02 の鉛筆マークをクリック
- ② Interface タブをクリックし、Gig0/2 の鉛筆マークをクリック
- ※他の IF は HA に成功すれば自動で Enable となるため事前設定不要
- ③ General の Enable にチェック
- ④ OK をクリック
- ⑤ Save をクリックして設定を保存
- ⑥ Deploy をクリックして FTD に適用



④

注: ESXi で HA リンク接続用の仮想スイッチを別途作成必要

# ステップ3-1: HA 設定 - HA ペアの作成

Firepower Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy Search Admin

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (1) Snort 3 (2)

Search Device Add

Deployment History

Collaps All

<input type="checkbox"/>	Name	Model	Vers...	Chassis	Licenses	Access...
<input type="checkbox"/>	▼ Ungrouped (2)					
<input type="checkbox"/>	FTDv01 Snort 3 10.71.132.194 - Routed	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...)	ACP-1
<input type="checkbox"/>	FTDv02 Snort 3 10.71.132.170 - Routed	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...)	ACP-1

- ① Device Management > Add > High Availability をクリック
- ② 以下を設定
  - Name : FTDv-HA ※任意の名前を記入
  - Device Type : Firepower Threat Defense を選択
  - Primary Peer : FTDv01 を選択
  - Secondary Peer : FTDv02 を選択
- ③ Continue をクリック



Add High Availability Pair

Name:\*  
FTDv-HA

Device Type:  
Firepower Threat Defense

Primary Peer:  
FTDv01

Secondary Peer:  
FTDv02

① Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

③ Continue

# ステップ3-1: HA 設定 - HA ペアの作成 (続き)

Warning

This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.

Do you want to continue?

Do not display this message again

- ① HA 構成により Snort プロセスの Restart が発生する警告メッセージが表示。問題なければ Yes をクリック



Add High Availability Pair

High Availability Link

Interface:\* GigabitEthernet0/2

Logical Name:\* Failover

Primary IP:\* 192.168.10.1

Use IPv6 Address

Secondary IP:\* 192.168.10.2

Subnet Mask:\* 255.255.255.0

State Link

Interface:\* Same as LAN Failover Link

Logical Name:\* Failover

Primary IP:\* 192.168.10.1

Use IPv6 Address

Secondary IP:\* 192.168.10.2

Subnet Mask:\* 255.255.255.0

IPsec Encryption

Enabled

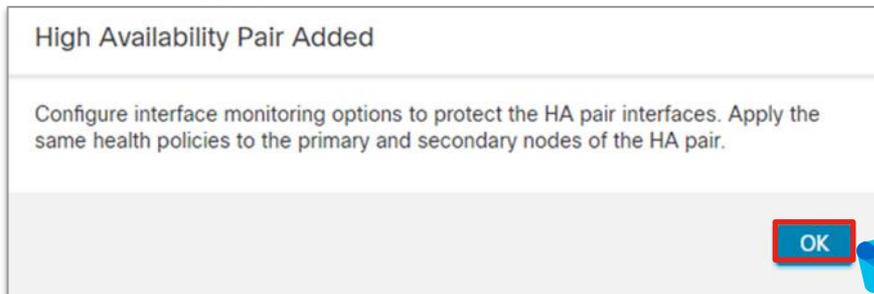
Key Generation: Auto

① LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

- ② HA リンク、State リンクで以下を入力・設定  
HA リンク
  - Interface : Gig0/2
  - Logical Name: 任意の名前を入力
  - Primary IP: FTDv01 の HA リンクの IP アドレス
  - Secondary IP: FTDv02 の HA リンクの IP アドレス
  - Subnet Mask: HA リンクのサブネットマスクState Link
  - Interface: Same as LAN Failover... を選択
- ③ Add をクリック (クリック後、HA構成開始)

※ HA 構成完了までに 10分以上要する場合もある

# ステップ4-1: HA 設定 - HA の構成とインタフェース モニター設定



- ① FTD HA ペア登録後のインターフェイスモニター設定や、ヘルスポリシー設定の適用を忘れないように、という情報のポップアップがあるため、OK をクリック
- ② FTDv-HA の鉛筆マークをクリック

Firepower Management Center  
Devices / Device Management

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (1) Snort 3 (2)

Name	Model	Vers...	Chassis	Licenses	Access Control Policy
Ungrouped (1)					
FTDv-HA High Availability					
FTDv01(Primary, Active) 10.71.132.194 - Routed	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...)	ACP-1
FTDv02(Secondary, Standby) 10.71.132.170 - Routed	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...)	ACP-1

# ステップ4-1: HA 設定 - HA の構成とインタフェース モニター設定 (続き)

Firepower Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy

FTDv-HA  
Cisco Firepower Threat Defense for VMware

Summary High Availability Device Routing Interfaces Inline Sets DHCP

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitor
Inside	192.168.1.1					
diagnostic						
Outside	192.168.2...					

Failover Trigger Criteria

Failure Limit	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer	15 sec

Interface MAC Addresses

Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

- ① High Availability タブの Monitoring Interfaces > inside の鉛筆マークをクリック
- ② Secondary IP Address に FTDv2 の inside IF モニタ用の IP アドレスを設定し、OK をクリック
- ③ Outside の鉛筆マークをクリック
- ④ Secondary IP Address に FTDv2 の Outside IF モニタ用の IP アドレスを設定し、OK をクリック
- ⑤ Save をクリック

Edit Inside

Monitor this interface for failures

IPv4 IPv6

Interface Name: Inside

Active IP Address: 192.168.1.1

Mask: 24

Standby IP Address:

Cancel OK

Edit Outside

Monitor this interface for failures

IPv4 IPv6

Interface Name: Outside

Active IP Address: 192.168.240.1

Mask: 24

Standby IP Address:

Cancel OK



# ステップ5-1: HA 設定 - 仮想 MAC アドレス設定

Firepower Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy

FTDv-HA  
Cisco Firepower Threat Defense for VMware

Save Cancel

Deployment History

Summary **High Availability** Device Routing Interfaces Inline Sets DHCP

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
Inside	192.168.1.1	192.168.1.2				🟢
diagnostic						🟢
Outside	192.168.2...	192.168.2...				🟢

Fallover Trigger Criteria

Failure Limit	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer Hold Time	15 sec
Interface Poll Time	5 sec

Interface MAC Addresses

Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

Add Interface Mac Address

Physical Interface:\*  
GigabitEthernet0/0

Active Interface Mac Address:\*  
a200.0a00.00fe

Standby Interface Mac Address:\*  
a200.0a00.00fd

Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab

OK

- ① High Availability タブの Interface MAC Addresses の + マークをクリック
- ② 以下を設定
  - Physical Interface : Gig0/0 を選択
  - Active Interface Mac Address : 任意の仮想 MAC アドレスを設定
  - Standby Interface Mac Address : 任意の仮想 MAC アドレスを設定
- ③ OK をクリック
- ④ 同様に Gig0/1 でも設定を行い、Save にて保存
- ⑤ Deploy をクリックして展開

# 参考: 仮想 MAC アドレス設定における vSwitch セキュリティポリシーの設定変更

- VM 環境で HA に仮想 MAC アドレスを登録する場合、vSwitch のセキュリティーポリシーの変更が必要となるため注意

ポートグループの編集: inside

名前	inside
VLAN ID	0
仮想スイッチ	vSwitch2
▼ セキュリティ	
無差別モード	<input checked="" type="radio"/> 承諾 <input type="radio"/> 拒否 <input type="radio"/> vSwitch から継承
MAC アドレス変更	<input checked="" type="radio"/> 承諾 <input type="radio"/> 拒否 <input type="radio"/> vSwitch から継承
偽装転送	<input checked="" type="radio"/> 承諾 <input type="radio"/> 拒否 <input type="radio"/> vSwitch から継承
▶ NIC チーミング	クリックして展開
▶ トラフィック シェーピング	クリックして展開

保存 キャンセル

すべて承諾を  
チェック

# CLI での確認 – FTDv01 への SSH

```
> show failover
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: Failover GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
```

```
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 3 of 311 maximum
```

```
MAC Address Move Notification Interval not set
```

```
failover replication http
```

```
Version: Ours 9.16(2)5, Mate 9.16(2)5
```

```
Serial Number: Ours 9A98KRRD4VS, Mate 9A1HFSNAWQQ
```

```
Last Failover at: 03:04:07 UTC Jul 20 2022
```

```
This host: Primary - Active
```

```
Active time: 3477 (sec)
```

```
slot 0: ASAv hw/sw rev (/9.16(2)5) status (Up Sys)
```

```
Interface diagnostic (0.0.0.0): Normal (Waiting)
```

```
Interface Outside (192.168.240.1): Normal (Monitored)
```

```
Interface Inside (192.168.1.1): Normal (Monitored)
```

```
slot 1: snort rev (1.0) status (up)
```

```
slot 2: diskstatus rev (1.0) status (up)
```

HA リンクが  
UP 状態

Primary 機の状態

モニタ対象の IF の状態 (Normal)

モニタ対象の Snort と Disk の状態 (Up)

```
Other host: Secondary - Standby Ready
```

```
Active time: 2472 (sec)
```

```
Interface diagnostic (0.0.0.0): Normal (Waiting)
```

```
Interface Outside (192.168.240.2): Normal (Monitored)
```

```
Interface Inside (192.168.1.2): Normal (Monitored)
```

```
slot 1: snort rev (1.0) status (up)
```

```
slot 2: diskstatus rev (1.0) status (up)
```

```
Stateful Failover Logical Update Statistics
```

```
Link : Failover GigabitEthernet0/2 (up)
```

```
Stateful Obj xmit xerr rcv rerr
```

```
General 216 0 133 0
```

```
sys cmd 133 0 133 0
```

```
up time 0 0 0 0
```

```
----- 以下省略 -----
```

Secondary 機の状態

モニタ対象 IF の  
状態 (Normal)

モニタ対象の Snort  
と Disk の状態 (Up)

State リンクが  
UP 状態

# 参考: FMC での HA ステータス確認

- show failover を FMC から確認する方法
- ⚙️ より Health > Monitor > 対象の FTD デバイスをクリック

Advanced Troubleshooting をクリック

Threat Defense CLI をクリック

コマンドを選択&入力

Execute をクリック

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

# 参考：FMC での HA ステータス確認

- failover history も FMC より確認可能
- Device > Device Management > HA の鉛筆マーク > Summary タブ

FTDv-HA  
Cisco Firepower Threat Defense for VMware

Summary High Availability Device Routing Interfaces Inline Sets DHCP

General

Name: FTDv-HA

Status: ●

Primary Peer: FTDv01(Active)

Secondary Peer: FTDv02(Standby)

Failover History:

虫眼鏡アイコンを  
クリック

Time	Device Name	Original State	New State	Reason
05:04:39 UTC Jul 20 2022	FTDv01	Standby Ready	Just Active	Other unit wants me Active
05:04:39 UTC Jul 20 2022	FTDv01	Just Active	Active Drain	Other unit wants me Active
05:04:39 UTC Jul 20 2022	FTDv01	Active Drain	Active Applying Config	Other unit wants me Active
05:04:39 UTC Jul 20 2022	FTDv01	Active Applying Config	Active Config Applied	Other unit wants me Active
05:04:39 UTC Jul 20 2022	FTDv01	Active Config Applied	Active	Other unit wants me Active
05:04:39 UTC Jul 20 2022	FTDv02	Active	Standby Ready	Set by the config command
05:02:31 UTC Jul 20 2022	FTDv01	Bulk Sync	Standby Ready	Detected an Active mate
05:02:20 UTC Jul 20 2022	FTDv01	Sync Config	Sync File System	Detected an Active mate
05:02:20 UTC Jul 20 2022	FTDv01	Sync File System	Bulk Sync	Detected an Active mate
05:02:12 UTC Jul 20 2022	FTDv01	App Sync	Sync Config	Detected an Active mate
04:59:20 UTC Jul 20 2022	FTDv01	Cold Standby	App Sync	Detected an Active mate

Close

show failover history コマンドで、障害検知などによる  
Active 機と Standby 機の切り替え (failover) 理由の確認可能

# HA Active 機の切り替え

- Devices > Device Management より
- Primary 機障害時の切り戻し等での利用

The screenshot illustrates the process of switching the active peer in a High Availability (HA) configuration. It is divided into two parts: the initial state and the state after the switch.

**Initial State (Top):** The interface shows two devices under the 'FTDv-HA High Availability' group. FTDv01 (10.71.132.194) is the 'Primary, Active' peer, and FTDv02 (10.71.132.170) is the 'Secondary, Standby' peer. A red box highlights 'Primary, Active' for FTDv01. A context menu is open over FTDv01, with 'Switch Active Peer' highlighted by a red box. A blue callout bubble points to this menu item with the text 'Switch Active Peer をクリック'.

**Confirmation Dialog (Middle):** A dialog box asks: 'Are you sure you want to make "FTDv02" the active peer?'. The 'Yes' button is highlighted with a red box. A blue callout bubble points to it with the text 'Yes をクリック'.

**Final State (Bottom):** After the switch, FTDv01 is now 'Primary, Standby' and FTDv02 is 'Secondary, Active'. A red box highlights 'Secondary, Active' for FTDv02. A large blue arrow points from the initial state to the final state.

Device	Status	IP	Role	Model	Version	Config	Group
FTDv01	Primary, Active	10.71.132.194	Primary, Active	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...) ACP-1
FTDv02	Secondary, Standby	10.71.132.170	Secondary, Standby	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...) ACP-1

Device	Status	IP	Role	Model	Version	Config	Group
FTDv01	Primary, Standby	10.71.132.194	Primary, Standby	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...) ACP-1
FTDv02	Secondary, Active	10.71.132.170	Secondary, Active	FTDv for VMware	7.0.1.1	N/A	Base, Threat (3 more...) ACP-1

# HA の解除

- Devices > Device Management より
- HA 構成を解除して単体の FTD に戻す場合に利用

The screenshot shows the Cisco FTDv configuration interface for a High Availability (HA) pair named "FTDv-HA". The interface lists two nodes: "FTDv01(Primary, Active)" and "FTDv02(Secondary, Standby)". A context menu is open over the "FTDv01" node, with the "Break" option highlighted. A blue callout bubble points to this menu with the text "Break をクリック". Below the main interface, a "Confirm Break" dialog box is displayed. The dialog contains the following text: "Breaking the High Availability pair 'FTDv-HA' will erase all configuration except the Access Control and Flex Config policy from standby peer. This operation might also restart Snort processes of primary and secondary devices, temporarily causing traffic interruption. Are you sure you want to break the pair?". There is an unchecked checkbox labeled "Force break, if standby peer does not respond". At the bottom of the dialog are "No" and "Yes" buttons, with the "Yes" button highlighted by a red box. A red arrow points from the "Break" option in the context menu to the "Yes" button. A blue callout bubble at the bottom right contains the text "メッセージを確認し問題なければ Yes をクリック".

Break をクリック

Confirm Break

Breaking the High Availability pair "FTDv-HA" will erase all configuration except the Access Control and Flex Config policy from standby peer. This operation might also restart Snort processes of primary and secondary devices, temporarily causing traffic interruption. Are you sure you want to break the pair?

Force break, if standby peer does not respond

No Yes

メッセージを確認し問題なければ Yes をクリック

# HAのベストプラクティス

- 以下の FTD HA ベストプラクティスにそって導入することで、トラブル発生リスクを抑えることが可能
  - FTD HA のデータインターフェイスは、スイッチもしくは HUB での収容が推奨。
  - スイッチを利用時は、Portfast もしくは同等の設定を スイッチ側ポートで有効化すること。冗長構成障害時の素早い通信再開や、インターフェイスアップ後の GARP 送付に必要
  - FTD HA の High Availability Link (=Failover Link) と State Link は、FTD デバイス間で直結、もしくは EtherChannel を利用。特に通信量の多い環境の場合、多量の同期情報が当 Link内を流れるため、広帯域のインターフェイスを利用すること
  - データインターフェイスには、Active IP アドレスと Standby IP アドレスを両方設定することが推奨。2つの IP アドレスを設定することで、両ポート間の動的監視が可能に
  - (特に NAT 利用時は) データインターフェイスには、Active 仮想 MAC アドレスと Standby 仮想 MAC アドレスの設定が推奨。仮想 MAC アドレスを設定することで、保守交換時の MAC アドレス変動や それに伴う通信影響を抑えることができる。
  - Interface 監視のための Polltime や Holdtime は デフォルト値利用が推奨。短すぎる Polltime や Holdtime は、過剰な通信や負荷が発生時の短時間の Hello パケットのドロップによる、予期せぬ切り替えの発生原因に。

Firepower System: FTD HA: FTD 冗長構成の組み方とトラブルシューティング (FMC 利用時)

© 2022, Cisco and/or its affiliates. All rights reserved. Cisco Public

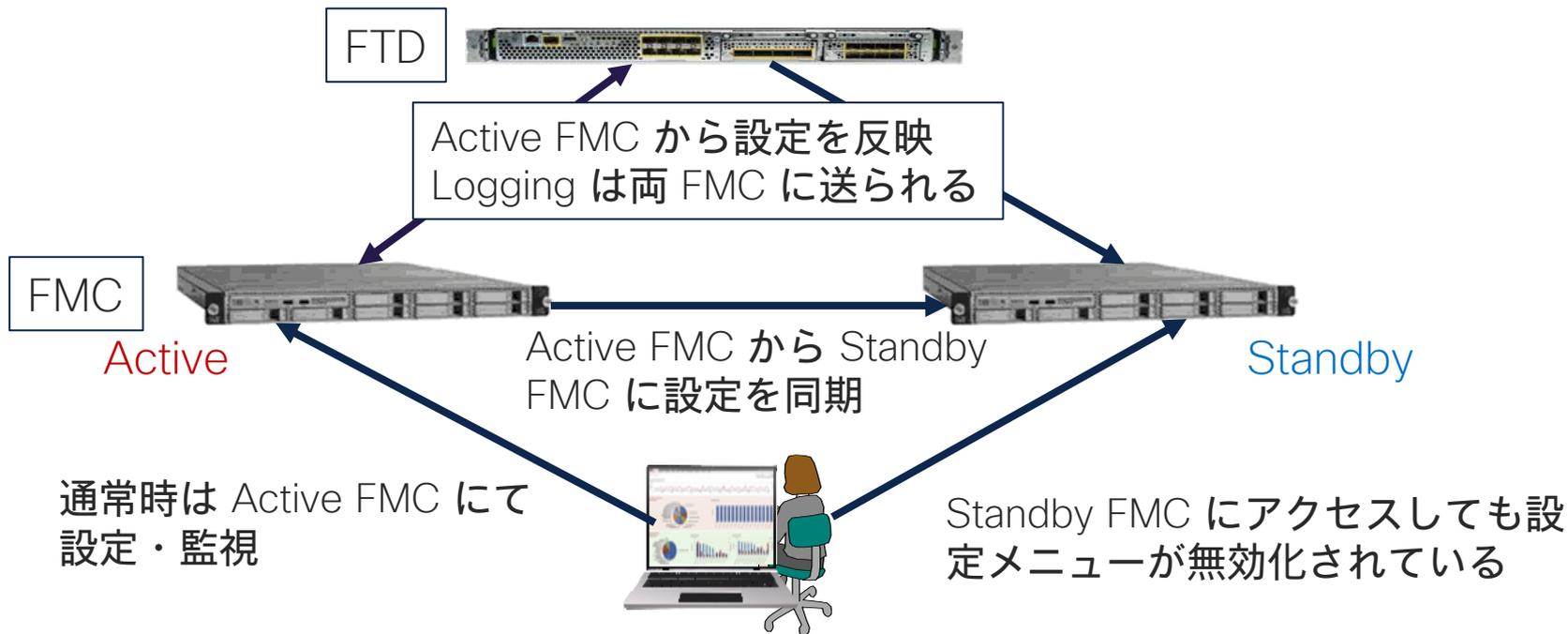
<https://community.cisco.com/t5/-/-/ta-p/3952716>

## 21. FMC High Availability の設定

# FMC の High Availability (HA) 概要

- FMC は Active / Standby の冗長構成を取ることが可能
- 同一モデルの FMC ハードウェアアプライアンスで HA を組む
- FMCv も HA を組むことが可能だが以下の条件がある
  - VMware ESXi で動作
  - FMCv10, FMCv25, FMCv300 の同じモデルでの HA 構成のみサポート
  - FMCv2 は未サポート
- それぞれの FMC の管理 IP アドレス間で IP レベルの疎通があれば良い (同一サブネットである必要は無い)。FMC 間通信に必要な帯域は最低 5Mbps
- FMC HA 構築時は先にセカンダリとなる FMC で設定、プライマリとなる FMC を指定し、プライマリ FMC から設定が同期される
- FMC HA は自動的に Active / Standby が切り替わることが無い。切り替えには手動での対応が必要

# FMC の HA 構成概要図



# 本章での手順

- 10.71.132.124 の管理 IP アドレスを持った FMCv を作成、パッチや SRU / LSP / VDB のバージョンを 10.71.132.204 の FMC と合わせておく。プライマリとなる FMC とこれらのバージョンを合わせておかないと FMC HA を構築できない (本章では手順は割愛)
- 10.71.132.124 の FMC をセカンダリ FMC としてセットアップ、プライマリ FMC を 10.71.132.204 として指定
- 10.71.132.204 の FMC で設定済のセキュリティポリシーや FTD レジスト情報をキープしたまま、FMC HA が構築されたことを確認
- Active / Standby FMC の手動切り替え試験を実施

**セカンダリとなる FMC にて作業を開始することがポイント**

# セカンダリ FMC での HA セットアップ①

セカンダリ FMC とする予定の FMCv を新規作成、各種バージョンを揃えた後にその FMC で HA の構築を開始する。このとき、セカンダリとなる FMC には FTD デバイスが登録されていないこと

← → ↻ https://10.71.132.124/ddd/#HAMain ☆

Firepower Management Center  
System / Integration / High Availability

Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🔍 ⚙️ ⓘ

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Input C...

Select a role for this Management Center and specify peer details to setup high availability.

Role For This FMC:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

After Firepower Management Center high availability is configured on VMWare, each registered FTD consumes an additional Firepower MCv Device license.

Primary FMC Host:

Registration Key\*:

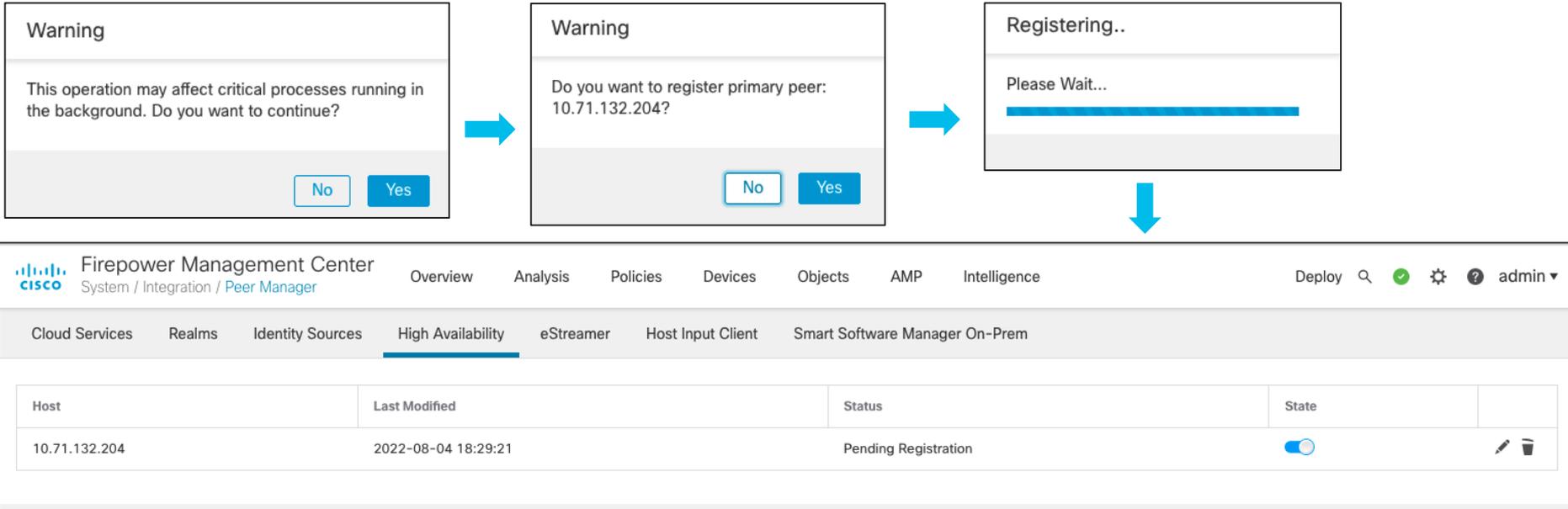
Unique NAT ID:

† Either host or NAT ID required.

- ① セカンダリとする予定の FMC で System → Integration をクリック
- ② FMC ロールとして Secondary をクリック
- ③ Peer Details の Primary FMC Host にプライマリとする予定の FMC の IP アドレス (10.71.132.204) を、Registration Key として任意の文字列 (この例では cisco) を入力
- ④ Register をクリック

# セカンダリ FMC での HA セットアップ②

設定内容の確認のためのワーニングが何度か出てくるので、問題が無いことを確認して Yes をクリックして進める。セカンダリ FMC としての設定が終わると Status が Pending Registration となり、プライマリ FMC からの HA 設定リクエスト待ちとなる



# プライマリ FMC での HA セットアップ①

プライマリ FMC とする予定の FMC にて同様の手順で FMC HA の設定を開始する

① <https://10.71.132.204/ddd/#HAMain>

Firepower Management Center  
System / Integration / High Availability

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Output Client

Select a role for this Management Center and specify peer details to setup high availability.

Role For This FMC:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.  
After Firepower Management Center high availability is configured on VMWare, each registered FTD consumes an additional Firepower MCv Device license.

Secondary FMC Host:

10.71.132.124

Registration Key\*:  
cisco

Unique NAT ID:

Register

† Either host or NAT ID is required.

②

③

④

① Integration をクリック

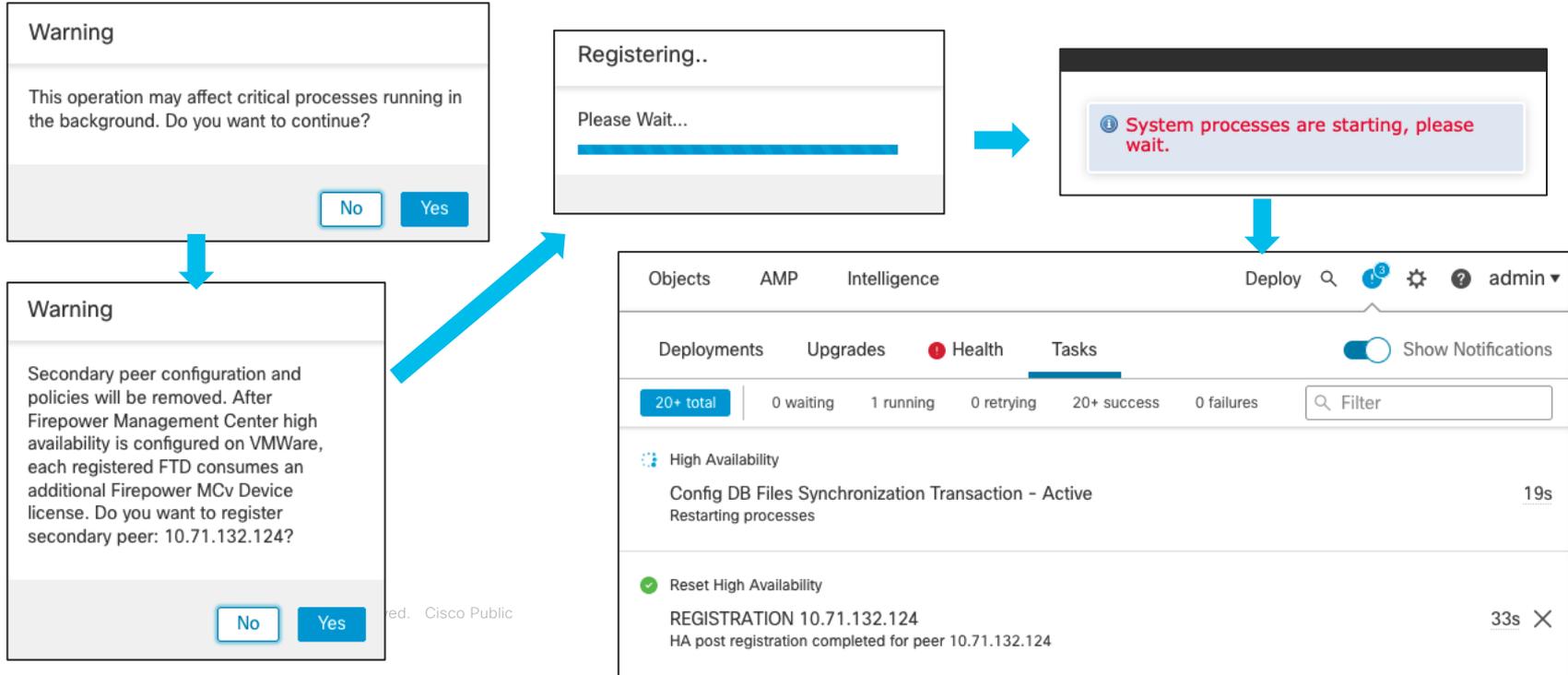
② FMC ロールとして Primary をクリック

③ Peer Details の Secondary FMC Host にセカンダリとしてセットアップした FMC の IP アドレス (10.71.132.124) を、Registration Key としてセカンダリ FMC で設定した文字列 (この例では cisco) を入力

④ Register をクリック

# プライマリ FMC での HA セットアップ②

設定内容の確認のためのワーニングが何度か出てくるので、問題が無いことを確認して Yes をクリックして進める。プライマリ FMC としての設定が始まり、DB の同期等のタスクが進んでいく



# FMC HA 構築中のステータス確認①

HA 構築中は、以下のようにプライマリ FMC とセカンダリ FMC で状態が目まぐるしく推移していく。構築完了までの時間は、データベースのサイズに大きく依存する



Summary	
Status	Temporarily degraded- high availability operations are in progress.
Synchronization	Failed
Active System	10.71.132.204
Standby System	10.71.132.124

System Status		
	Local Standby - Secondary (10.71.132.124)	Remote Active - Primary (10.71.132.204)
Operating System	7.0.1	7.0.1
Software Version	7.0.1.1-11	7.0.1.1-11
Model	Cisco Firepower Management Center for VMware	Cisco Firepower Management Center for VMware

# FMC HA 構築中のステータス確認②

https://10.71.132.204/ddid/#HAMain

Firepower Management Center  
System / Integration / High Availability

High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete. These operations include file copy which may take time to complete. Database files synchronization: 100% of 183MB transferred

System Status		
	Local	Remote
Status	Active - Primary (10.71.132.204)	Standby - Secondary (10.71.132.124)
Operating System	7.0.1	7.0.1
Software Version		
Model		

RemoteOnly And LocalOnly Device Registration

IP Address	Host Name
Registration Pending/Failed (Remote) (2)	

System Status で Local (今アクセスしている FMC) や Remote (Peer となる FMC) の状態が把握できるようになるが、DB 同期等、HA 構築終了まではまだ時間を要する

https://10.71.132.124/ddid/#HAMain

Firepower Management Center  
System / Integration / High Availability

High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete. These operations include file copy which may take time to complete. Database files synchronization: 100% of 183MB received

System Status		
	Local	Remote
Status	Standby - Secondary (10.71.132.124)	Active - Primary (10.71.132.204)
Operating System	7.0.1	7.0.1
Software Version	7.0.1.1-11	7.0.1.1-11
Model	Cisco Firepower Management Center for VMware	Cisco Firepower Management Center for VMware

# FMC HA 構築完成を確認

Firepower Management Center  
System / Integration / High Availability

Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Manager On-Prem

Switch Peer Roles Break HA Pause Synchron

**Summary**

Status ● Synchronization task is in progress

Synchronization ● OK

Active System 10.71.132.204  
( HA synchronization time : Thu Aug 2022-08-04T09:55:17 UTC )

Standby System 10.71.132.124  
( HA synchronization time : Thu Aug 2022-08-04T09:54:36 UTC )

	Local Active - Primary (10.71.132.204)	Remote Standby - Secondary (10.71.132.124)
Operating System	7.0.1	7.0.1
Software Version	7.0.1.1-11	7.0.1.1-11
Model	Cisco Firepower Management Center for VMware	Cisco Firepower Management Center for VMware

Summary で Status や Synchronization がグリーンになれば、FMC HA の構築が完了となる

FTD と FMC の間の SFTunnel は、FTD から 2 台の FMC に自動的に張り直される (次ページ参照)

Firepower Management Center  
System / Integration / High Availability

Services **High Availability** eStreamer Host Input Client

Switch Peer Roles Break HA Pause Synchron

**Summary**

Status ● Synchronization task is in progress

Synchronization ● OK

Active System 10.71.132.204  
( HA synchronization time : Thu Aug 2022-08-04T09:55:17 UTC )

Standby System 10.71.132.124  
( HA synchronization time : Thu Aug 2022-08-04T09:54:36 UTC )

	Local Standby - Secondary (10.71.132.124)	Remote Active - Primary (10.71.132.204)
Operating System	7.0.1	7.0.1
Software Version	7.0.1.1-11	7.0.1.1-11
Model	Cisco Firepower Management Center for VMware	Cisco Firepower Management Center for VMware

## (参考) FTD CLI での FMC 登録状況の確認

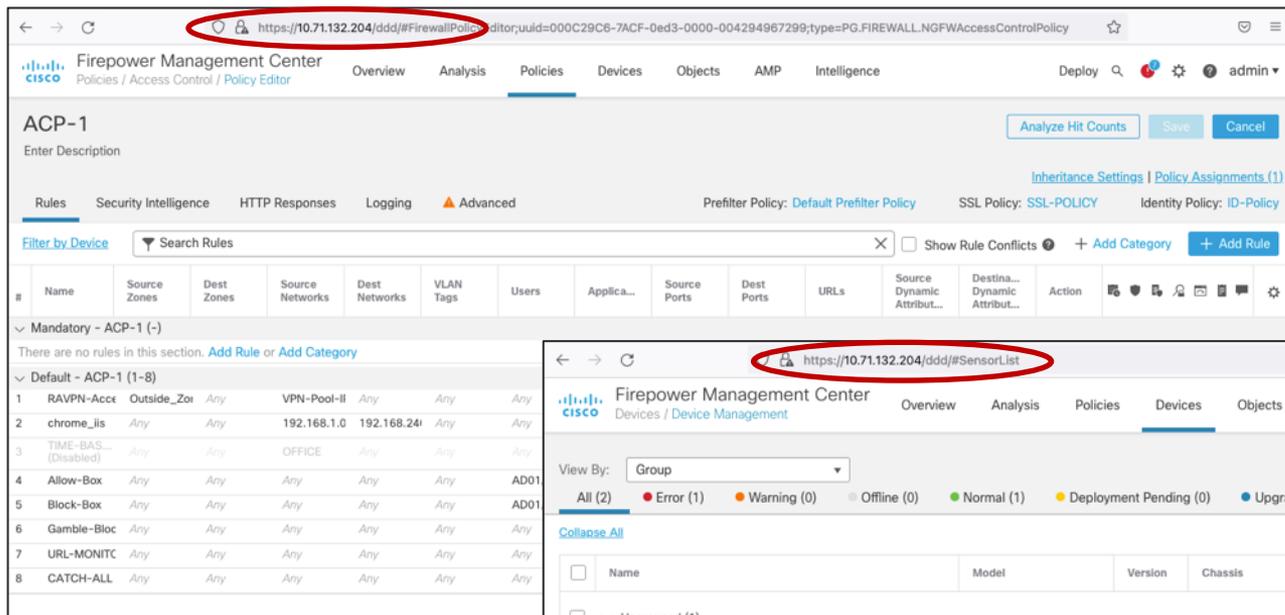
```
> show managers
Type           : Manager
Host           : 10.71.132.204
Registration    : Completed
```

```
Type           : Manager
Host           : 10.71.132.124
Registration    : Completed
```

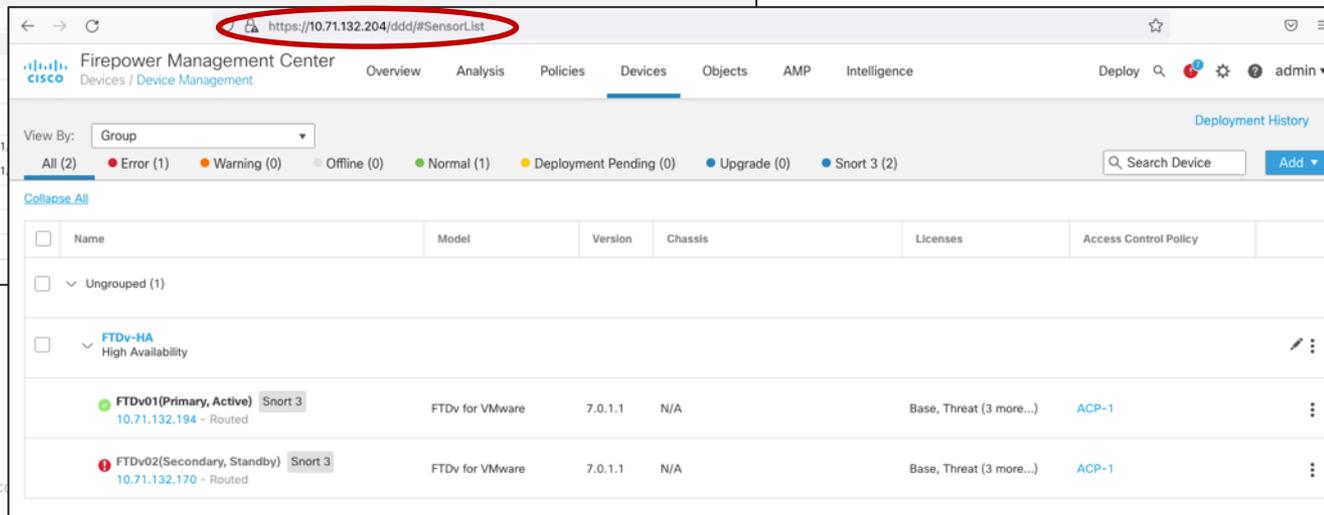
```
>
```

FTD の CLI で show managers  
コマンドで SFTunnel の状態を確認すると、2台の FMC に張られていることがわかる

# 各種設定が Active FMC に残っていることを確認



The screenshot shows the Firepower Management Center interface. The browser address bar contains the URL <https://10.71.132.204/ddd/#FirewallPolicyEditor;uid=000C29C6-7ACF-0ed3-0000-004294967299;type=PG.FIREWALL.NGFWAccessControlPolicy>, which is circled in red. The page title is "Firepower Management Center" and the breadcrumb is "Policies / Access Control / Policy Editor". The main heading is "ACP-1". Below the heading, there are tabs for "Rules", "Security Intelligence", "HTTP Responses", "Logging", and "Advanced". The "Rules" tab is selected. A search bar for rules is present. Below the search bar, there is a table of rules. The table has columns for Name, Source Zones, Dest Zones, Source Networks, Dest Networks, VLAN Tags, Users, Applica..., Source Ports, Dest Ports, URLs, Source Dynamic Attrib..., Destina... Dynamic Attrib..., and Action. The table is currently empty, with a message "Mandatory - ACP-1 (-) There are no rules in this section. Add Rule or Add Category".



The screenshot shows the Firepower Management Center interface. The browser address bar contains the URL <https://10.71.132.204/ddd/#SensorList>, which is circled in red. The page title is "Firepower Management Center" and the breadcrumb is "Devices / Device Management". The main heading is "Devices". Below the heading, there is a "View By:" dropdown menu set to "Group". Below the dropdown, there is a summary bar showing "All (2)", "Error (1)", "Warning (0)", "Offline (0)", "Normal (1)", "Deployment Pending (0)", "Upgrade (0)", and "Snort 3 (2)". Below the summary bar, there is a "Collapse All" link. Below the collapse link, there is a table of devices. The table has columns for Name, Model, Version, Chassis, Licenses, and Access Control Policy. The table is currently empty, with a message "Ungrouped (1)". Below the ungrouped message, there is a section for "FTDv-HA High Availability". Below the section, there are two rows of device information. The first row is "FTDv01(Primary, Active) Snort 3" with IP address "10.71.132.194 - Routed", Model "FTDv for VMware", Version "7.0.1.1", Chassis "N/A", Licenses "Base, Threat (3 more...)", and Access Control Policy "ACP-1". The second row is "FTDv02(Secondary, Standby) Snort 3" with IP address "10.71.132.170 - Routed", Model "FTDv for VMware", Version "7.0.1.1", Chassis "N/A", Licenses "Base, Threat (3 more...)", and Access Control Policy "ACP-1".

# Standby FMC でのメニュー無効化の確認

Standby となった FMC では、様々なメニューが無効化され、アクセスできないようになっている。設定、モニタリング、解析等は Active FMC で行う

Active FMC

Standby FMC

The screenshot shows the Active FMC web interface. The URL bar is circled in red, showing <https://10.71.132.204/ddd/#HAMain>. The navigation menu is open, displaying a comprehensive list of options including Configuration, Logging, Monitoring, Users, Domains, Integration, SecureX, Updates, Licenses, Smart Licenses, and Classic Licenses. The main content area shows system status and synchronization details.

System	HA synchronization time	Software Version	Model
Active System	( HA synchron 2022-08-04T10:01:48 UTC )	System	7.0.1-11
Standby System	( HA synchronization time : Thu Aug 2022-08-04T10:00:58 UTC )	Software Version	7.0.1-11

The screenshot shows the Standby FMC web interface. The URL bar is circled in red, showing <https://10.71.132.124/ddd/#HAMain>. The navigation menu is open, but many options are disabled (grayed out). Only a few options like Integration, Updates, Licenses, and Classic Licenses are visible. The main content area shows system status and synchronization details.

System	HA synchronization time	Software Version	Model
Active System	( HA synchronization time : Thu Aug 2022-08-04T09:55:17 UTC )	System	7.0.1-11
Standby System	( HA synchronization time : Thu Aug 2022-08-04T09:55:17 UTC )	Software Version	7.0.1-11

Standby FMC の方がクリックできるメニューが少ないことがわかる

# FMC HA の Active / Standby 切り替え①

FMC HA の Active / Standby の切り替えは手動で行う必要がある。どちらの FMC から  
も実施可能

The screenshot shows the FMC web interface for High Availability configuration. The 'Switch Peer Roles' button is highlighted with a blue arrow and a circled '1'. Below the button, there are two panels: 'Summary' and 'System Status'.

Summary	
Status	Healthy
Synchronization	OK
Active System	10.71.132.204 ( HA synchronization time : Thu Aug 2022-08-04T10:05:16 UTC )
Standby System	10.71.132.124 ( HA synchronization time : Thu Aug 2022-08-04T10:00:58 UTC )

System Status		
	Local Active - Primary (10.71.132.204)	Remote Standby - Secondary (10.71.132.124)
Operating System	7.0.1	7.0.1
Software Version	7.0.1.1-11	7.0.1.1-11
Model	Cisco Firepower Center for	

**Warning**

This operation may affect critical processes running in the background. Do you want to continue?

No Yes

**Switching Roles**

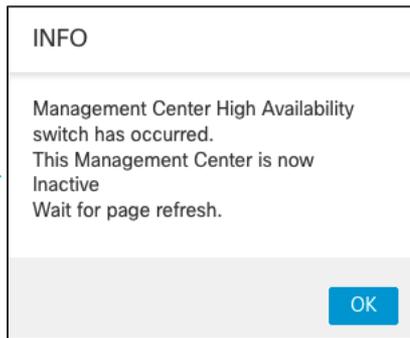
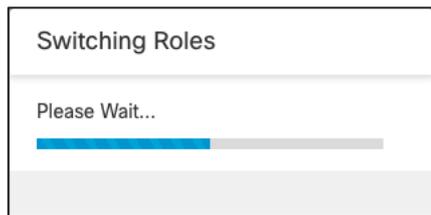
Do you want to switch active and standby peers?

Cancel OK

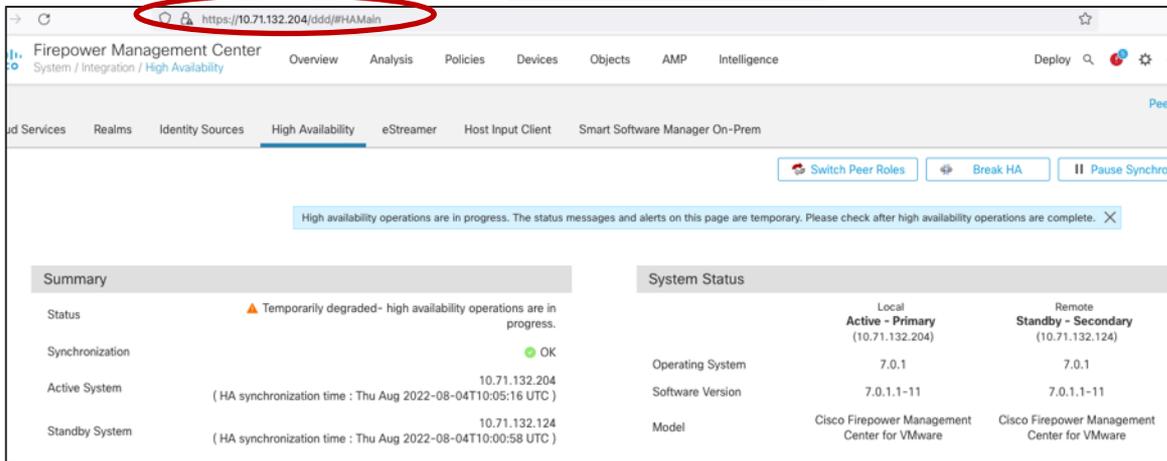
- ① どちらかの FMC で System → Integration → High Availability にある Switch Peer Roles をクリック
- ② Warning の内容を確認、問題なければ Yes をクリック
- ③ Switching Roles が始まる旨のメッセージを確認、問題なければ OK をクリック

# FMC HA の Active / Standby 切り替え②

新 Active FMC



新 Standby FMC



Summary		System Status	
Status	Temporarily degraded- high availability operations are in progress.	Local Active - Primary (10.71.132.204)	Remote Standby - Secondary (10.71.132.124)
Synchronization	OK	Operating System	7.0.1
Active System	10.71.132.204 ( HA synchronization time : Thu Aug 2022-08-04T10:05:16 UTC )	Software Version	7.0.1.1-11
Standby System	10.71.132.124 ( HA synchronization time : Thu Aug 2022-08-04T10:00:58 UTC )	Model	Cisco Firepower Management Center for VMware

FMC の Active / Standby 切り替わりが開始され、旧 Standby FMC は Active に昇格するタスクが発生、旧 Active FMC はその後、Standby への移行が始まる

従って、切り替わりタスク開始直後はこのように旧 Active FMC は Status が Active のままである

自動的に全タスクが終わるので、それまで待つ

# FMC HA の Active / Standby 切り替え③

Summary

Status	● Synchronization task is in progress
Synchronization	● OK

Active System (10.71.132.124)  
( HA synchronization time : Thu Aug 2022-08-04T10:07:19 UTC )

Standby System (10.71.132.204)  
( HA synchronization time : Thu Aug 2022-08-04T10:08:25 UTC )

System Status

	Local Standby - Primary (10.71.132.204)	Remote Active - Secondary (10.71.132.124)
Operating System	7.0.1	7.0.1
Software Version	7.0.1.1-11	7.0.1.1-11
Model	Cisco Firepower Management Center for VMware	Cisco Firepower Management Center for VMware

Summary で Status や Synchronization がグリーンになれば、FMC HA の Active / Standby の切り替えが無事完了となる

Summary

Status	● Synchronization task is in progress
Synchronization	● OK

Active System (10.71.132.124)  
( HA synchronization time : Thu Aug 2022-08-04T10:07:19 UTC )

Standby System (10.71.132.204)  
( HA synchronization time : Thu Aug 2022-08-04T10:08:25 UTC )

System Status

	Local Active - Secondary (10.71.132.124)	Remote Standby - Primary (10.71.132.204)
Operating System	7.0.1	7.0.1
Software Version	7.0.1.1-11	7.0.1.1-11
Model	Cisco Firepower Management Center for VMware	Cisco Firepower Management Center for VMware

System Status で Active / Standby が入れ替わっていることを確認



The bridge to possible