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

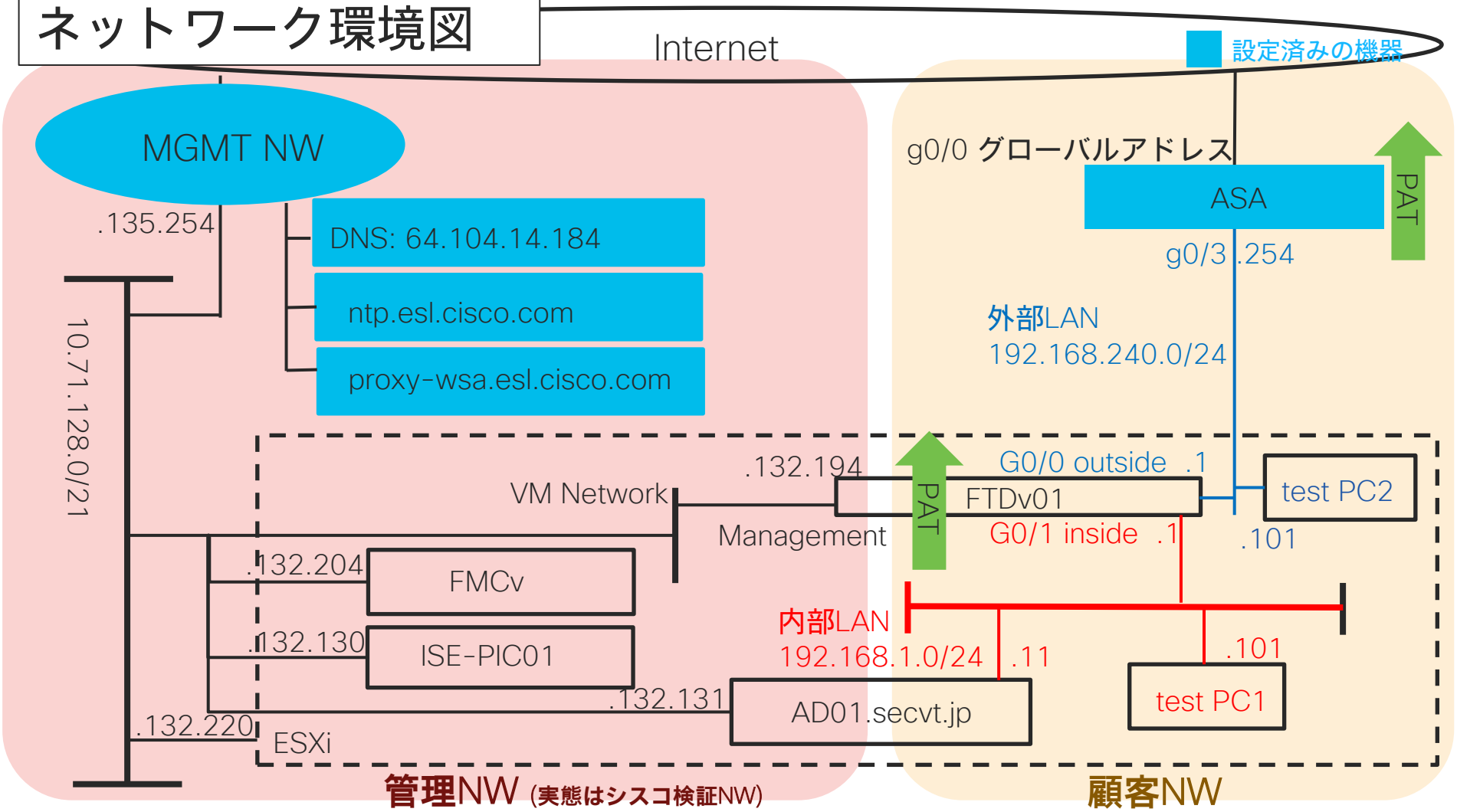
はじめに

- 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
10.71.128.0/21
DNS: 64.104.14.184
ntp.esl.cisco.com
proxy-wsa.esl.cisco.com
g0/0 グローバルアドレス
ASA
PAT
g0/3 .254
外部LAN
192.168.240.0/24
.132.194
VM Network
Management
PAT
FTDv01
G0/0 outside .1
G0/1 inside .1
test PC2
.101
.132.204
FMCv
.132.130
ISE-PIC01
内部LAN
192.168.1.0/24
.11
.101
test PC1
.132.131
AD01.secvt.jp
.132.220
ESXi
管理NW (実態はシスコ検証NW)
顧客NW

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

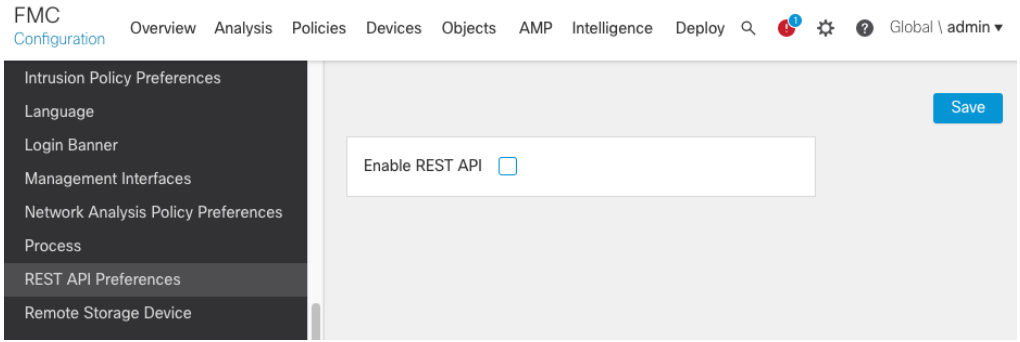
FMC API について

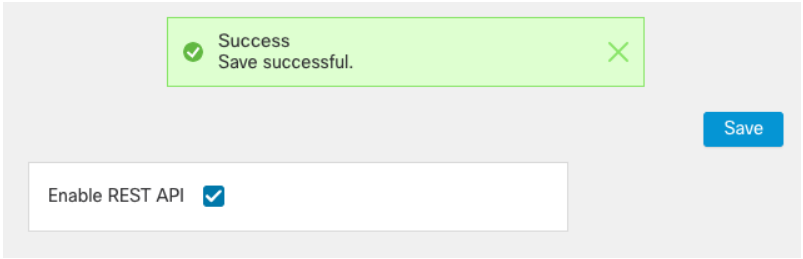
- REST API にて API を提供
- API に関するガイドは FMC 内部にある API Explorer にまとまっている
- API Explorer の UI は FMC の内部に存在するため、詳細を確認するには FMC が必要
- Python3 であれば “fmcapi” パッケージも用意されていてより簡単に構築可能

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. クレデンシャル (User/Pass) のエンコード

- FMC のクレデンシャルを 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ャルを入力
>>> 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

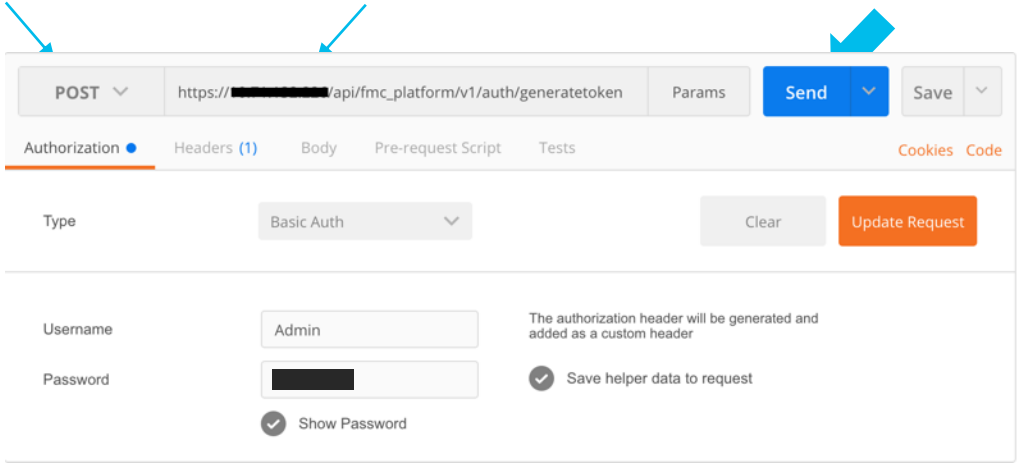
https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken

※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

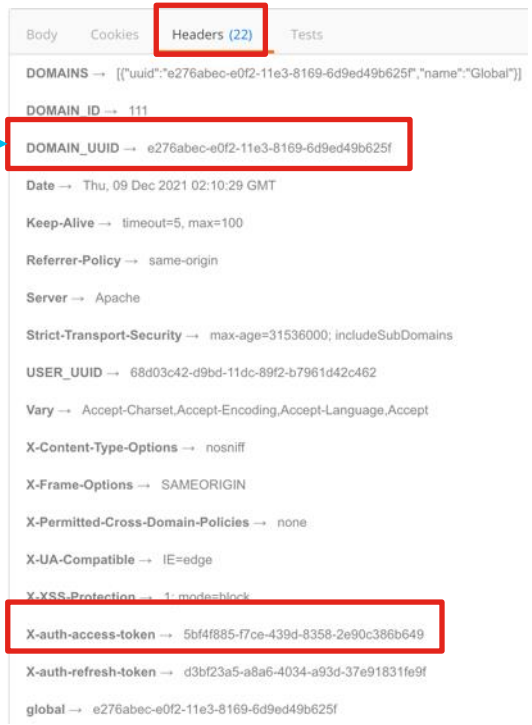
https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken



FMC にログインする Username/Password を入力

Send をクリック

ドメイン UUID



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

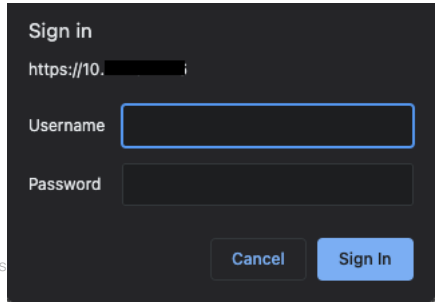
API Explorer

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：

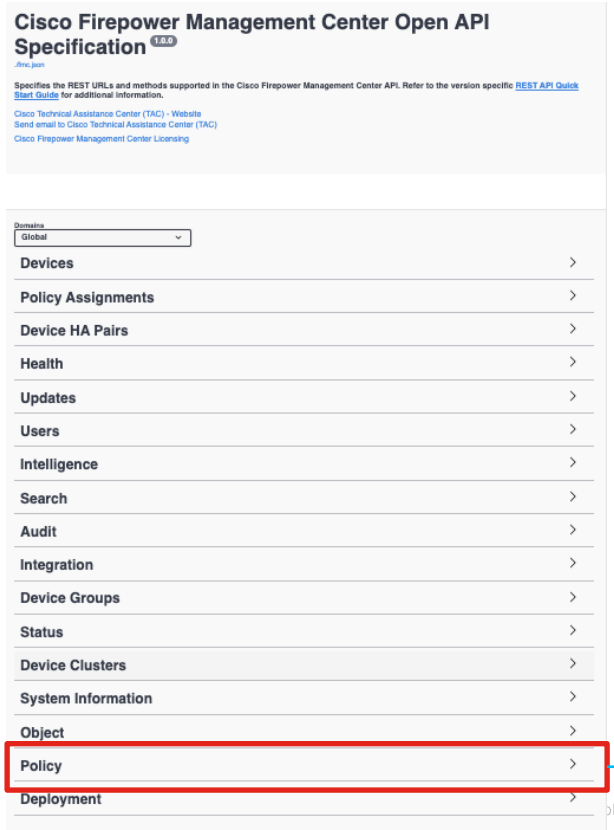
https://<firepower_management_center_IP_or_name>/api/api-explorer

(例：https://10.0.0.1/api/api-explorer)

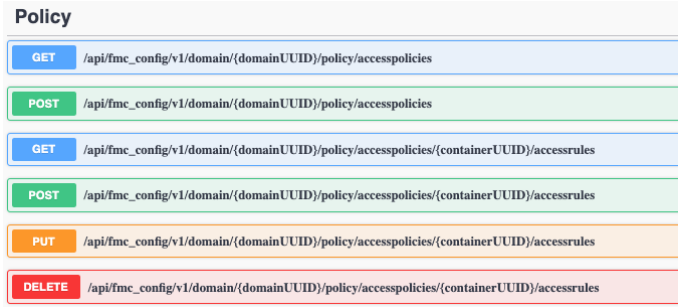


アクセスするとログインを求められるので
FMC の GUI へログインする時と同じ ID/PW で
ログイン

API Explorer の見方



OpenAPI フォーマットでカテゴリ毎に表示



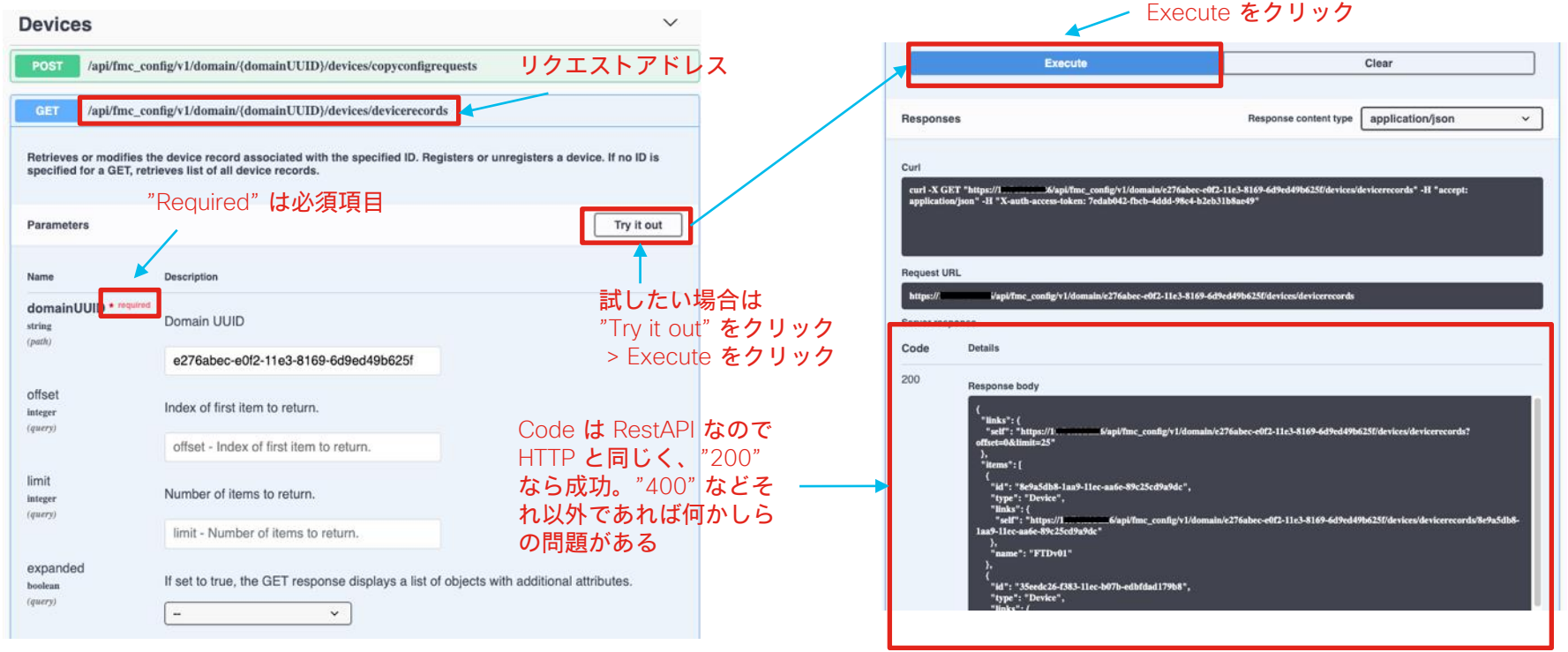
目的に応じて
GET/POST/PUT/DELETE
を使った操作が可能

※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)

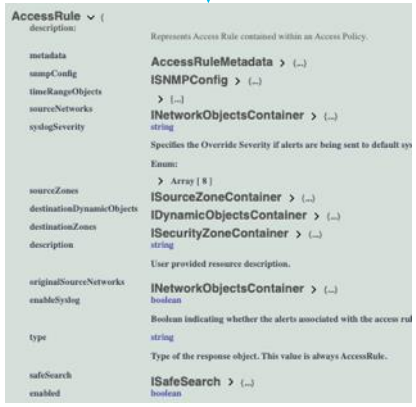
例） Devices > [GET] devices/devicerecords



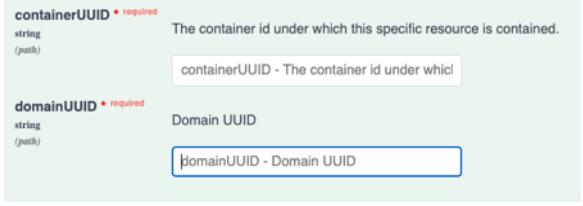
API Explorer の使い方 (POST)

← リクエスト先 URL (本例では access rule 追加)

サンプルの入力方法



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



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

ページ下部には具体的な入力例を表示

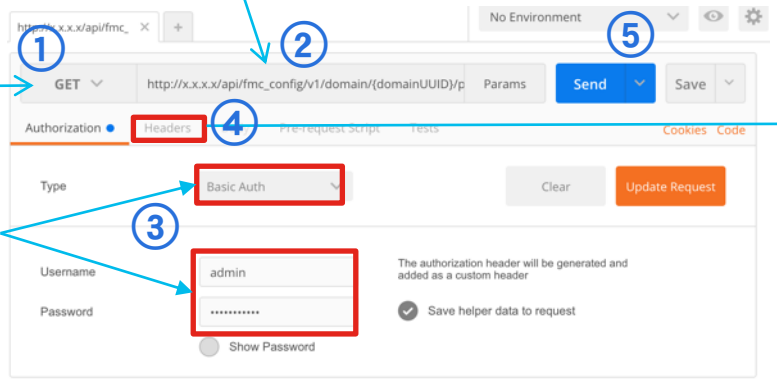
API 試行の例

Postman

Policy 情報 (ACP) を取得 (GET) する例

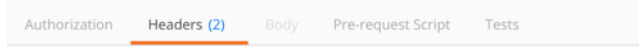
メソッドは GET を指定

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)

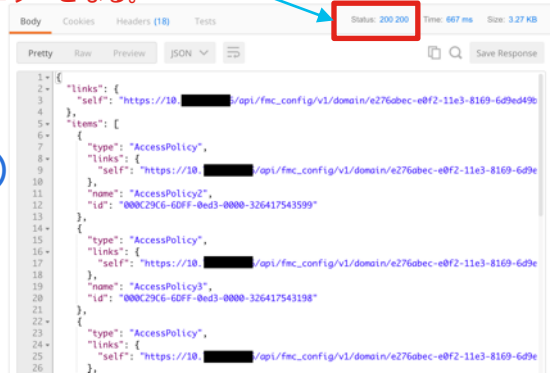


Type: は Basic Auth を選択し、FMC ログイン ID/PW をその下に入力

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



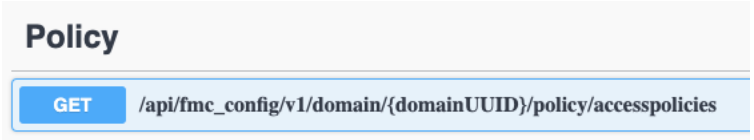
Status は HTTP と同じ 200/201 なら OK。400, 500 などはエラーとなる。



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トのタイプを入力
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




```
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}
>>>
>>> access_policy_api = "/api/fmc_config/v1/domain/" + DOMAIN_UUID +  "/policy/accesspolicies"
>>> 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)
{'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

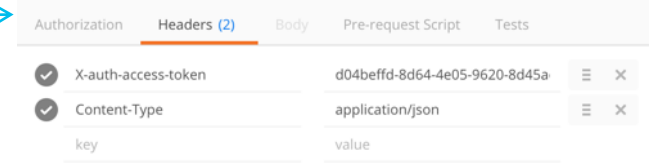
ACP 情報を取得し、返り値を json フォーマットにして変数として定義

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

Postman

Host object を追加 (POST) する例

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

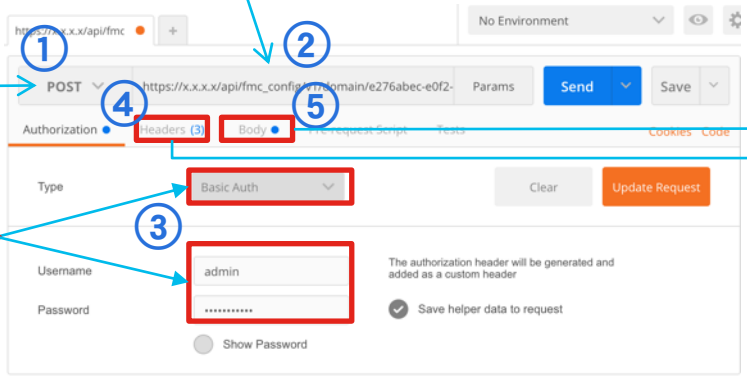


Body は "raw" と" Json(application/json)" を選択し
Host Object 追加に必要な情報を Json フォーマットで入力
(下記は必要最低限の情報のみを記載)

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)



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

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トのタイプを入力
⑤ "Send" をクリック
⑥ 取得結果は "Body" に表示

Python3

Host object を追加 (POST) する例

POST /api/fmc_config/v1/domain/{domainUUID}/object/hosts

```
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)
~省略~
```

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

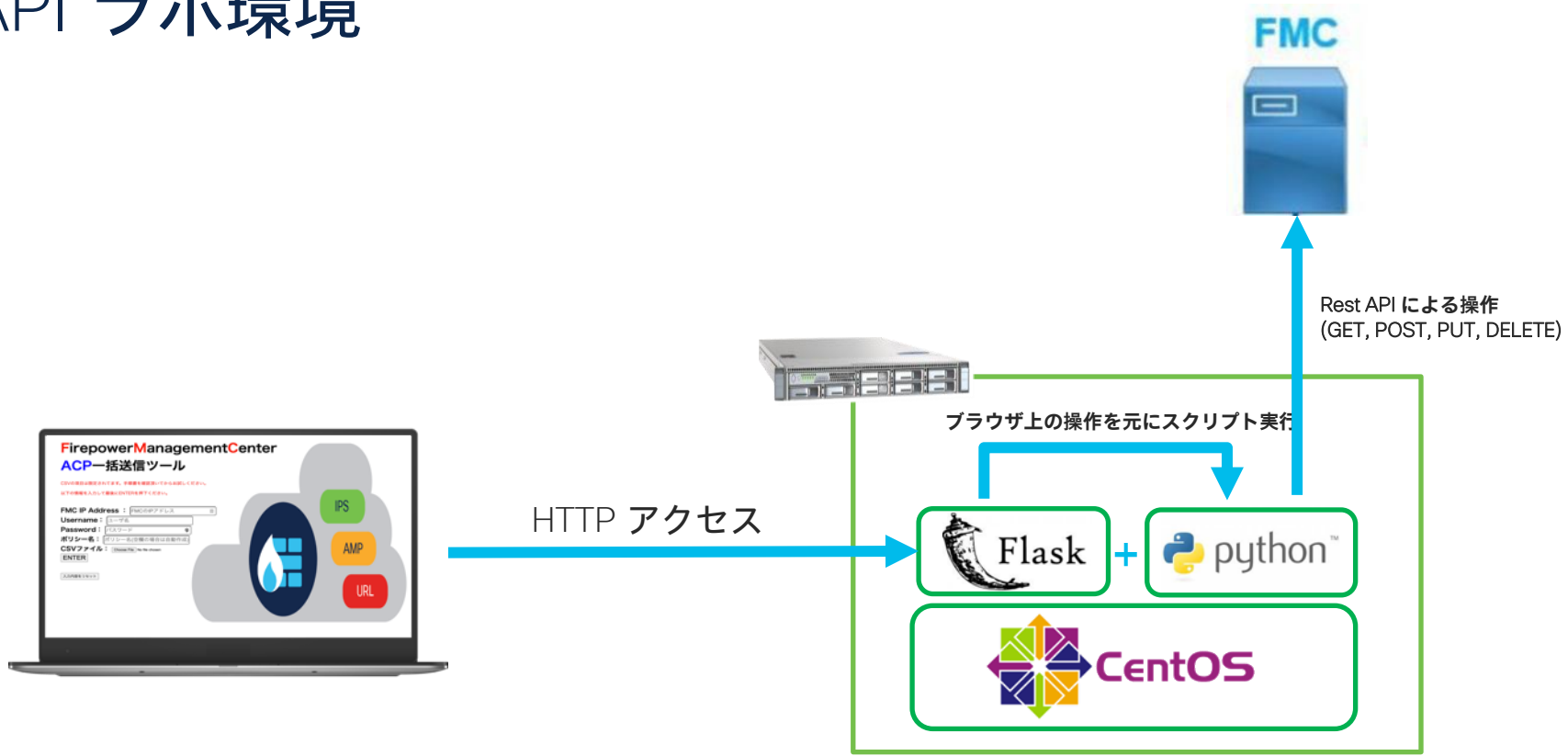
HOST object 追加用の URL を定義

HOST object を追加 (POST)

追加した結果を表示 (GUI でも確認可能)

API 活用例

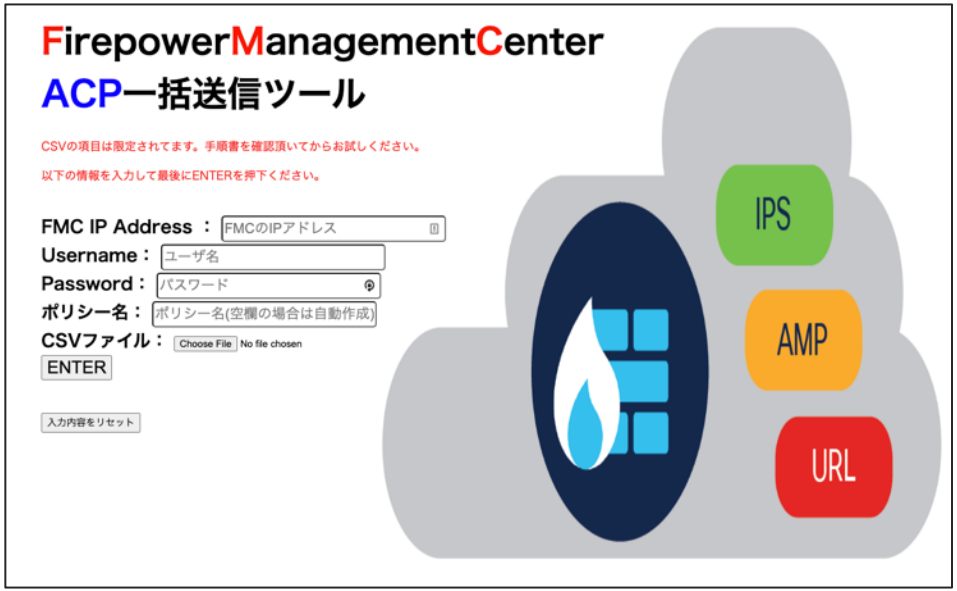
API ラボ環境



※Flask = ウェブアプリケーションフレームワーク

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



【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)

```python
import requests
import csv
import json
from requests.auth import HTTPBasicAuth
from getpass import getpass
import os
from flask import Flask, render_template, request, redirect, url_for, send_from_directory, session
from werkzeug.utils import secure_filename

app = Flask(__name__)

UPLOAD_FOLDER = './uploads'
ALLOWED_EXTENSIONS = set(['csv'])
app.config['UPLOAD_FOLDER'] = UPLOAD_FOLDER

@app.route('/', methods=['GET'])
def login():
    return render_template("index2.html")

def allowed_file(filename):
    return '.' in filename and \
        filename.rsplit('.', 1)[1] in ALLOWED_EXTENSIONS


@app.route('/send', methods=['GET', 'POST'])
def send():
    if request.method == 'POST':
        csv_file = request.files['csv_file']
        if csv_file and allowed_file(csv_file.filename):
            filename = secure_filename(csv_file.filename)
            csv_file.save(os.path.join(app.config['UPLOAD_FOLDER'], filename))
            csv_url = app.config['UPLOAD_FOLDER'] + '/' + filename
            abspath  = os.path.abspath(filename)

            fmc_ip = request.form.get('fmc_ip')
            fmc_username = request.form.get('fmc_username')
            fmc_password = request.form.get('fmc_password')
            fmc_policy_name = request.form.get('fmc_policy_name')

            address = fmc_ip
            username = fmc_username
            password = fmc_password
            policyname = fmc_policy_name

            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つずつ順番に読み取り

↓

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

↓

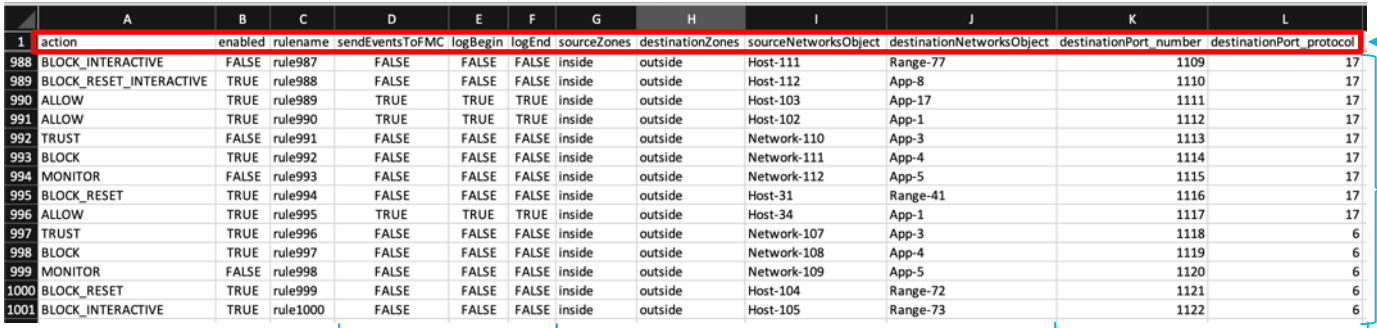
1行1ルールとしてすべての情報が揃ったら Access Rule として
RestAPI の POST を使って設定追加

↓

あとは CSV の最後の行までそれの繰り返し

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

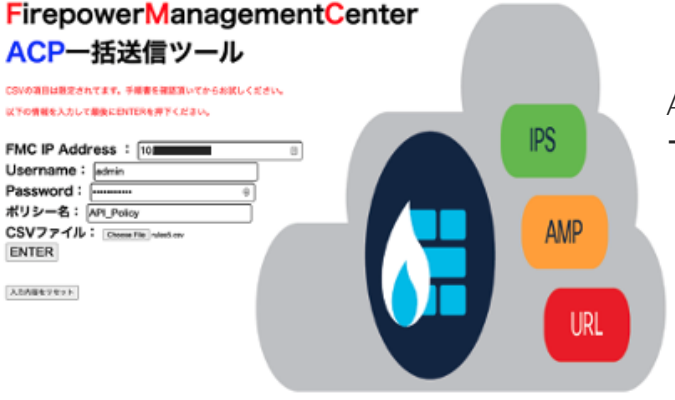
ルール名は任意の文字列を入力

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

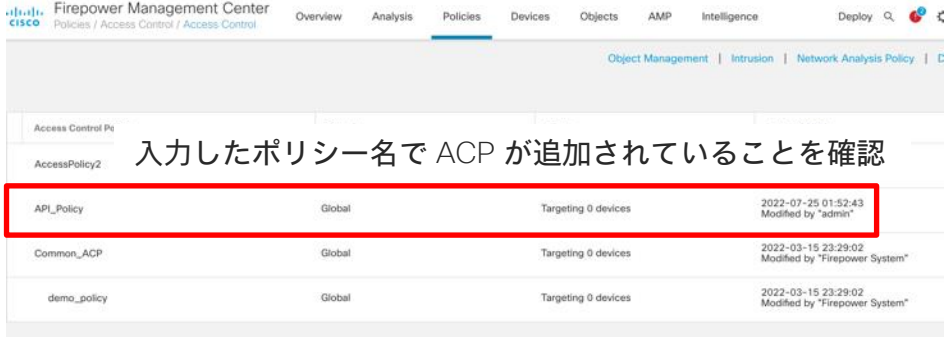
これらの項目は事前に作成済みのオブジェクト名を入力

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

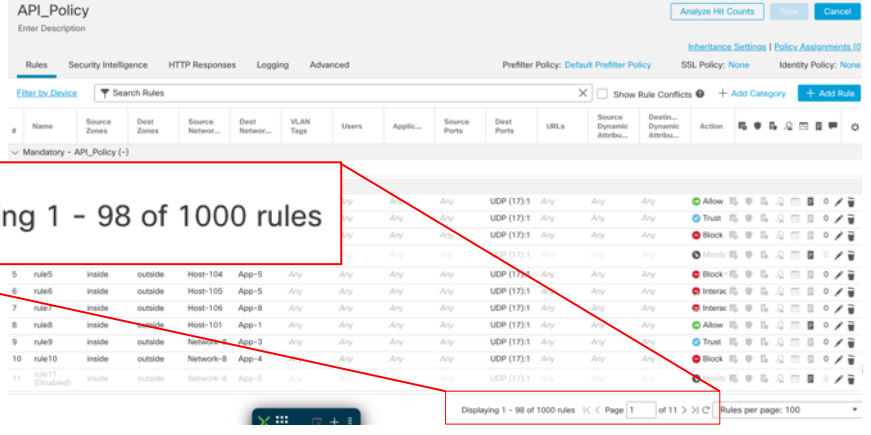


API で ACP とルールを一括設定



入力したポリシー名で ACP が追加されていることを確認

ACP 内のルールを確認

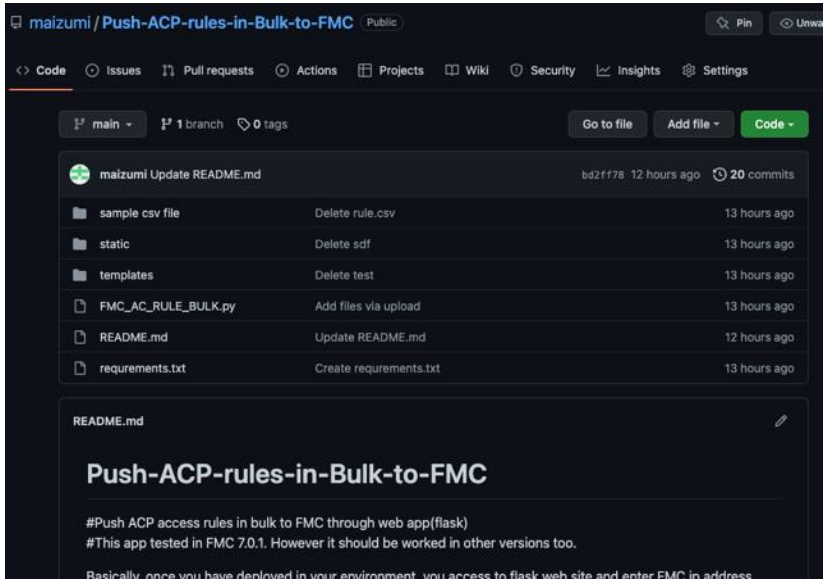


合計 1000行のルールが CSV ファイル通り設定されていることを確認

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

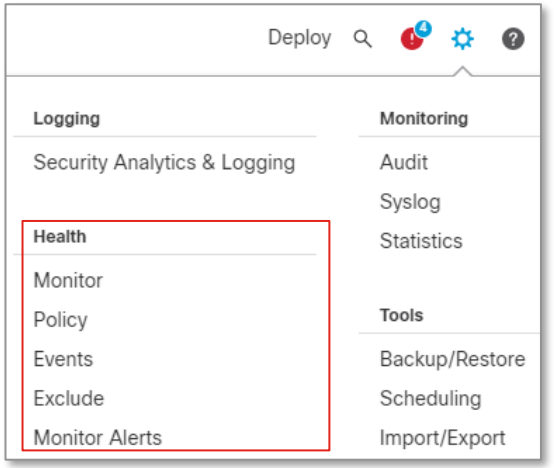
【Push Objects in Bulk to FMC using REST-API】
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215972-push-objects-in-bulk-to-fmc-using-rest-a.html

【fmcapi】
https://developer.cisco.com/codeexchange/github/repo/daxm/fmcapi/

16. システム監視

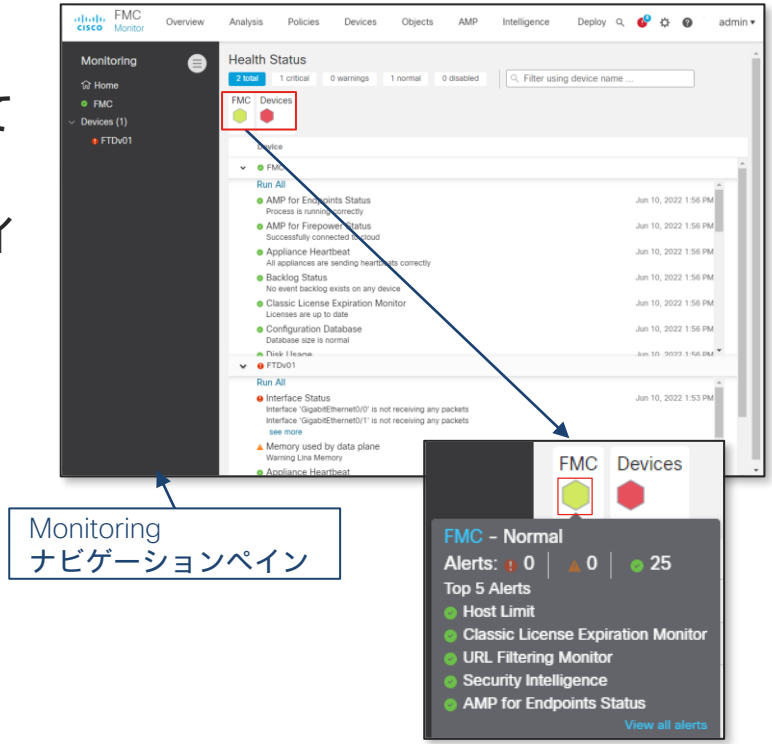
システム監視概要

- 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: ヘルスモ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

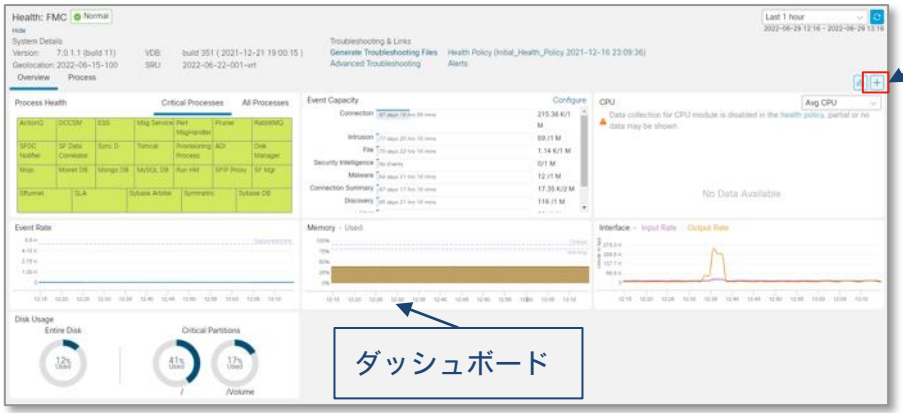
- モニターホーム画面
  - Health Status サマリページ: FMC とすべての管理デバイスのヘルス状況を確認
    - にマウスオーバーすると、FMC/管理デバイスのそれぞれのヘルス概要が表示。または、› マークにてヘルス詳細を確認。
      - 正常。アラームはなし
      - 注意。一つ以上のアラームが表示
      - 重大。一つ以上のアラームが表示
  - Monitoring ナビゲーションペインでは個々のデバイスのヘルス状況を確認



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



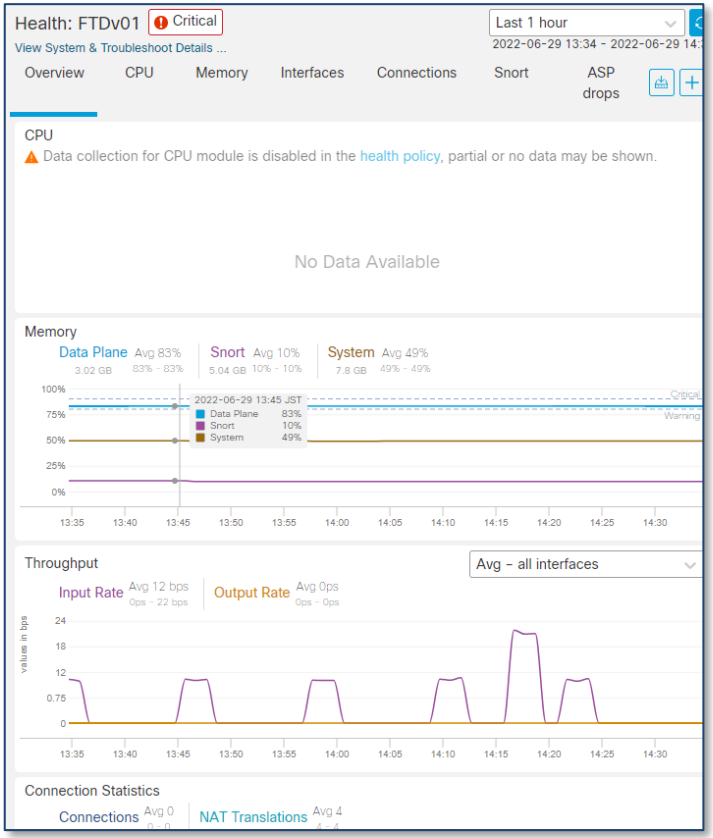
Add Dashboard
ダッシュボードの追加ができる

- 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

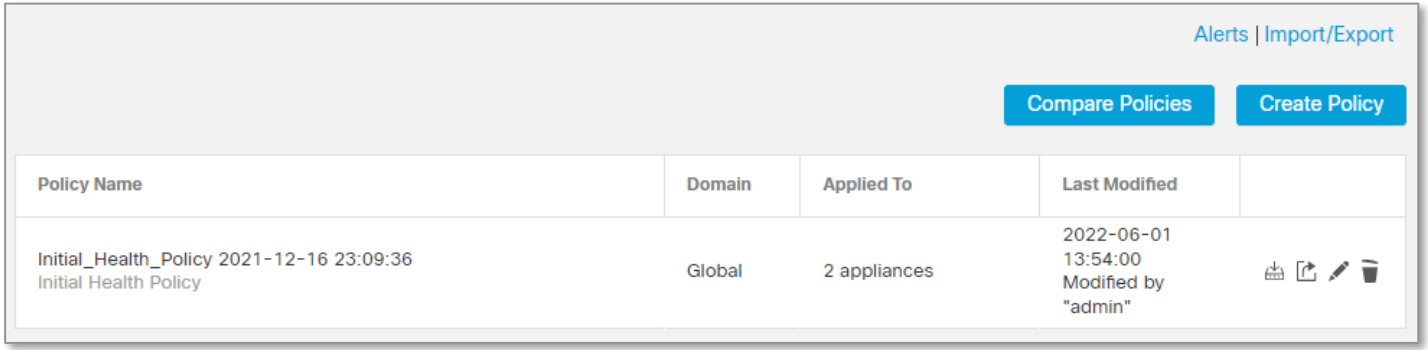
- FMC 各プロセスの状況を表示
  - Memory Usage
  - CPU Utilization
  - Restart count
  - Swap Memory

Monitoring: 管理デバイスヘルスモニター

- 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

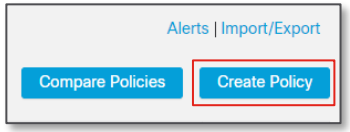


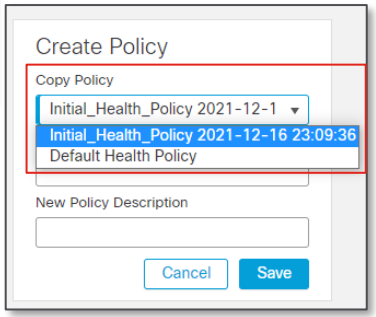
Health Policy 概要

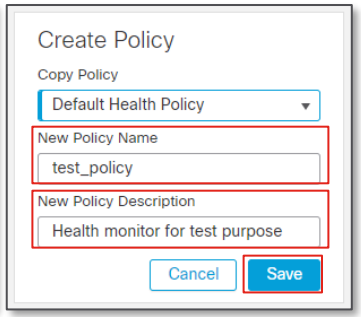


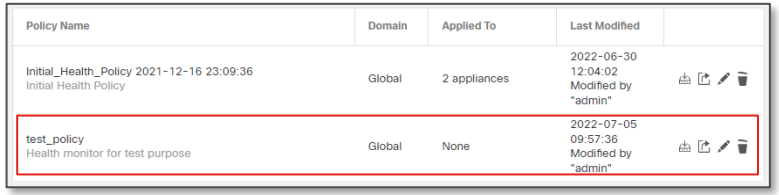
- ヘルスモジュール (監視機能) の有効/無効化や閾値のポリシーの設定ができる
- FMC セットアップ時に “Initial_Health_policy年月日時間” の初期ポリシーが作成され、FMC および管理デバイスに適用される
- 初期ポリシーはデフォルトポリシーを基に作成される
- デフォルトポリシーは、閲覧/編集は出来ないが、ポリシー作成の際、デフォルトポリシーの複製は可能
- FMC のアップグレードにてヘルスポリシーのモジュールに変更/追加があった場合は、最新のポリシーがデフォルトポリシー、初期ポリシー、カスタムポリシー (作成した場合) へ適用される

Health Policy 作成



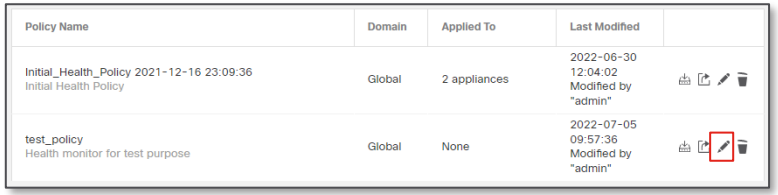


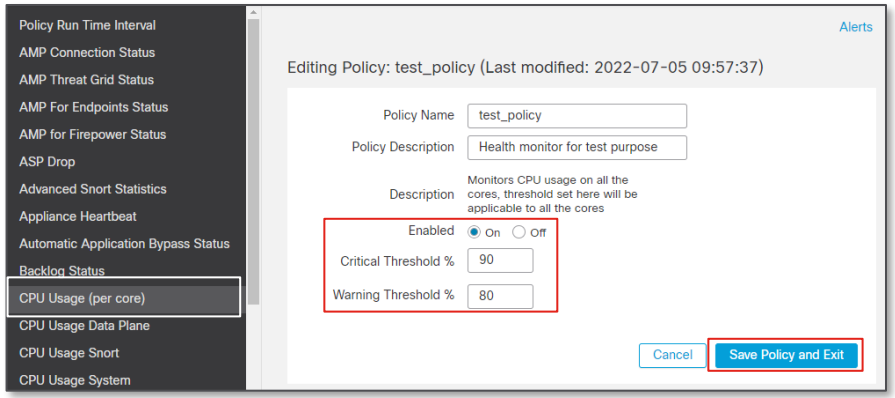




- Health Policy の作成は以下の手順で行う
  - System > Health > Policy > Create Policy を選択
    - 引用するポリシーの選択
    - New Policy Name: ポリシー名
    - New Policy Description: ポリシー説明
    - Save

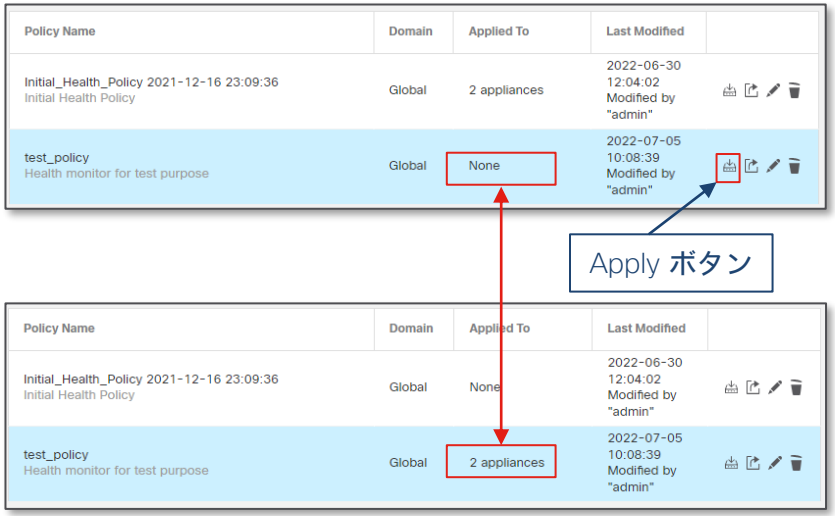
Health Policy 更新または修正

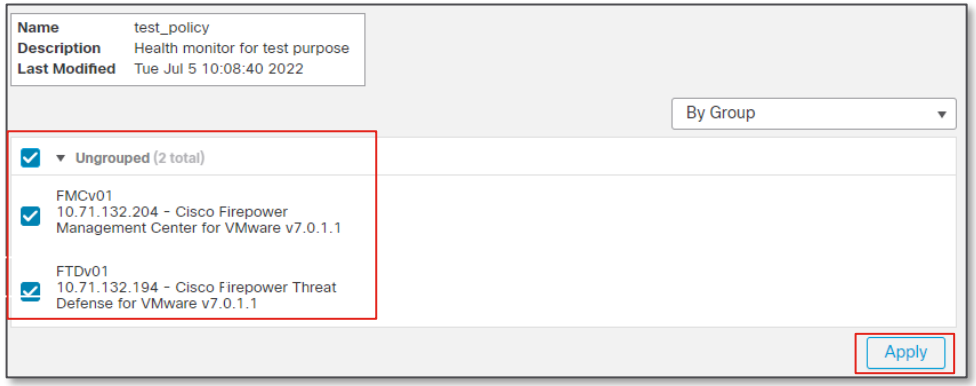




- Health Policy の更新または修正は以下の手順で行う
  - 更新/修正をするポリシーを選択し、鉛筆マーク (Edit) ボタンを押す
  - 修正を加えるポリシーを選択
    - 有効/無効の選択
    - 閾値の設定
    - Save Policy and Exit (他にも修正があれば上記内容を繰り返す)

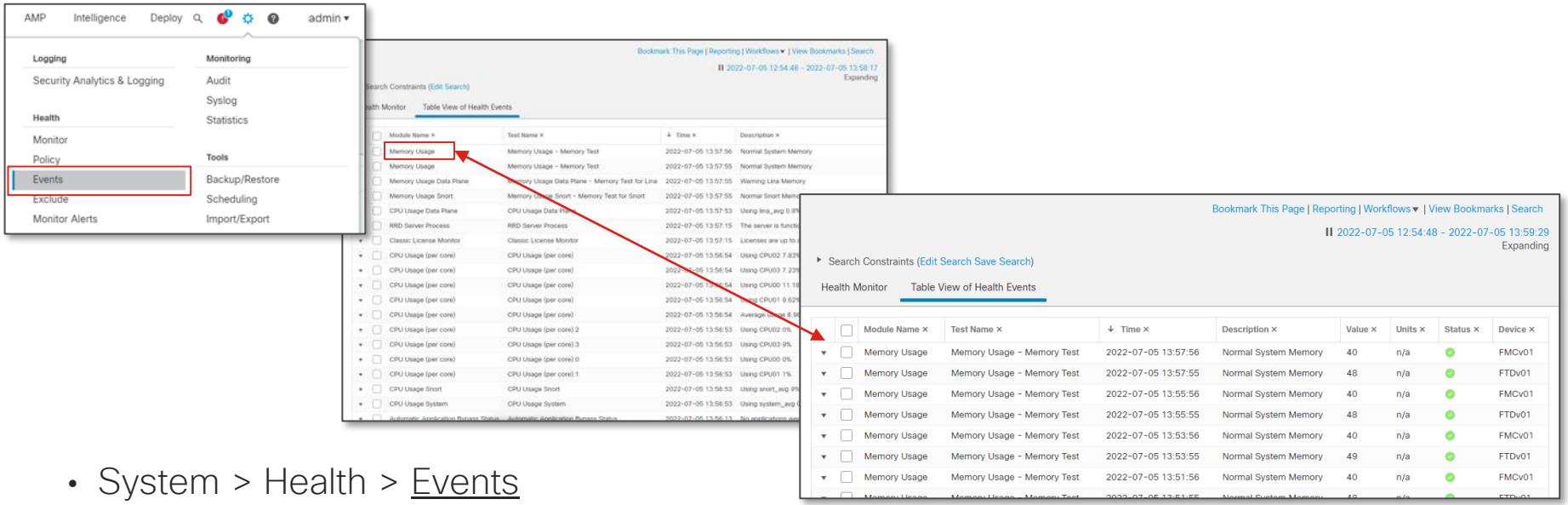
Health Policy をアプライアンスに適用





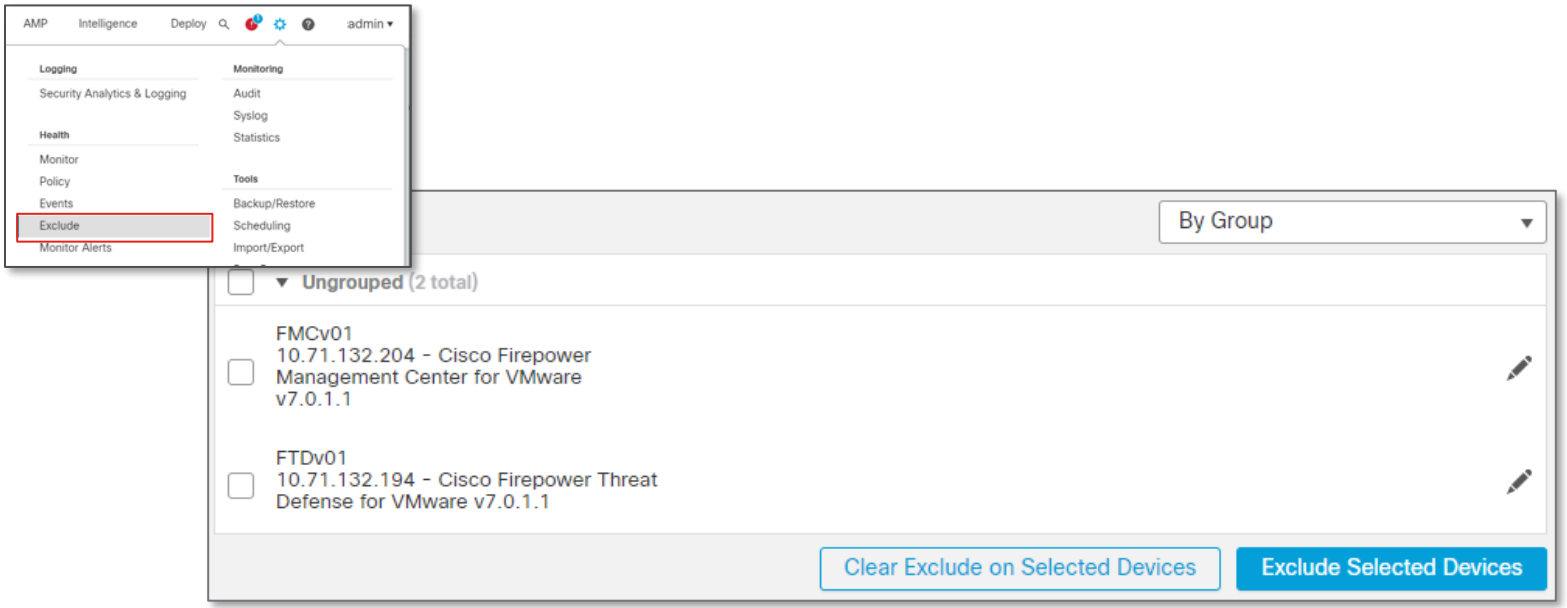
- Health Policy のアプライアンスへの適用は以下の手順で行う
  - アプライアンスに適用するポリシーを選択し Apply ボタンを押す
  - 適用するアプライアンスにチェックを入れる
    - Apply にてポリシーの適用完了

Health Event 概要



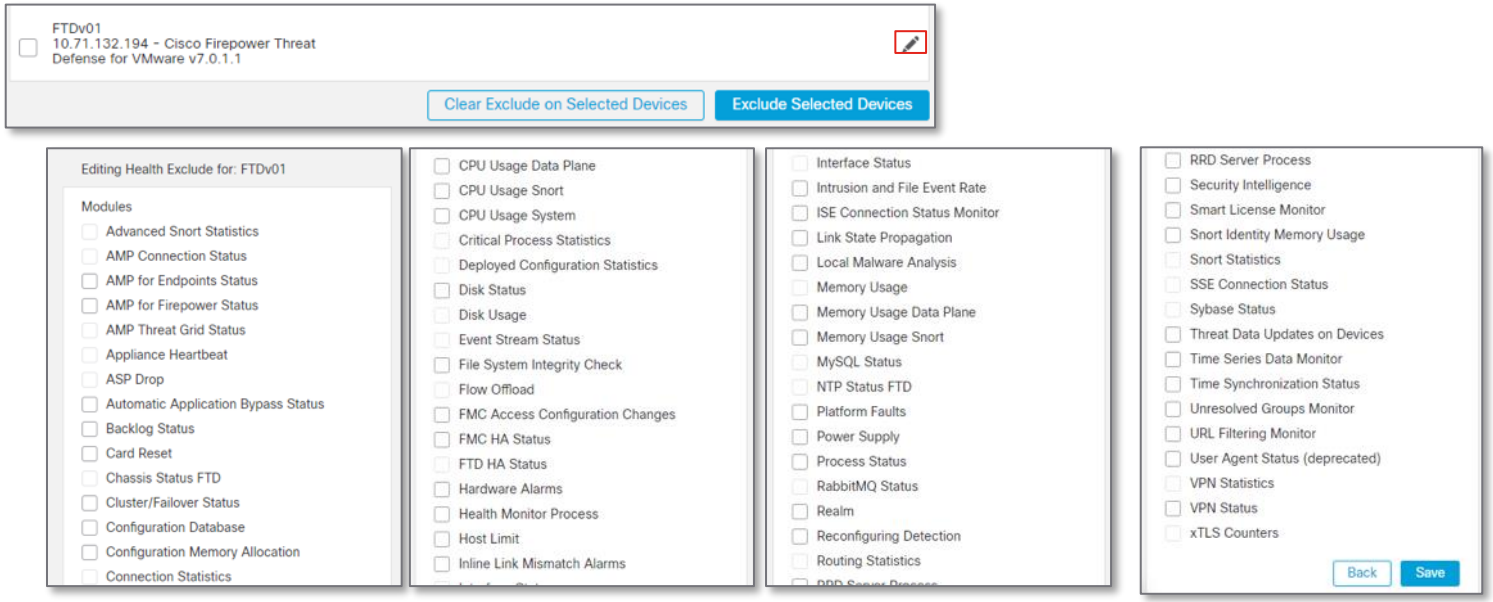
- System > Health > Events
- FMC のヘルスモニターにてログに記録されたヘルスイベントを表示
- イベントはカスタマイズ可能となり、目的により見易さを調整できる
- テーブルのイベントの一つを選択すると、そのイベントに関するログを確認できる

Health Exclude 概要



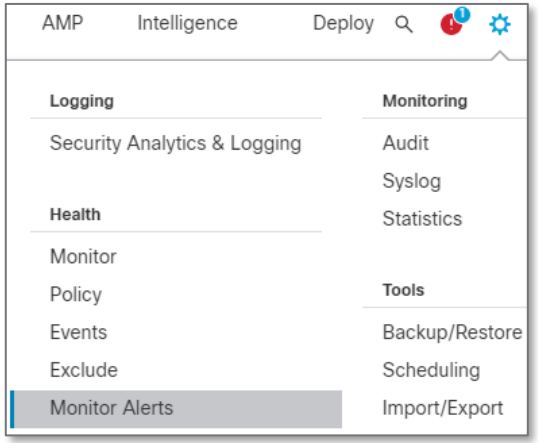
- System > Health > Exclude
- ヘルス監視の対象から除外するための設定
- デバイス毎での除外、ヘルスモジュール毎での除外リストの作成が可能

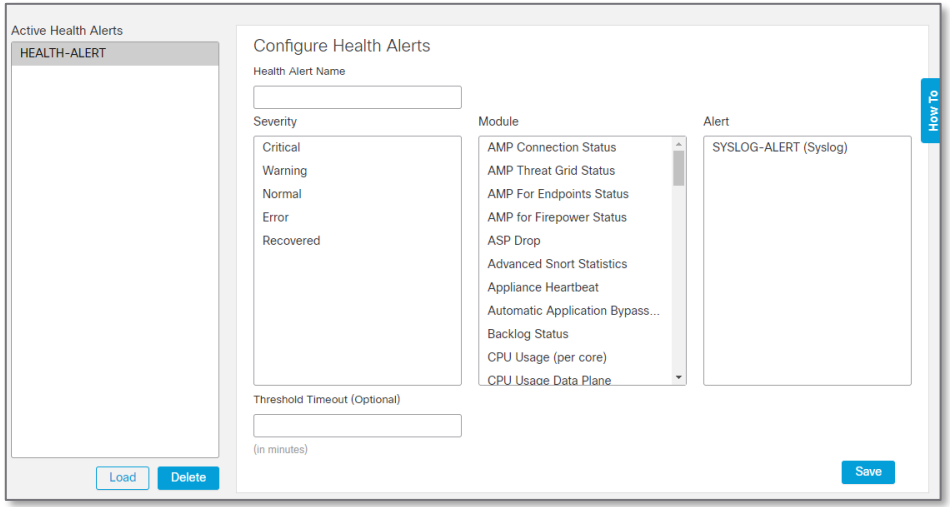
Health Exclude - ヘルスモジュール単位での除外



- Edit ボタンにて監視対象外のヘルスモジュールを選択
- 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

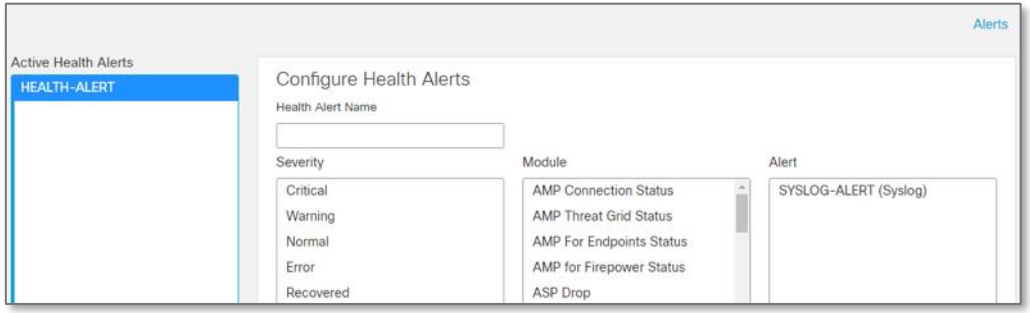
Health Monitor Alerts 概要①





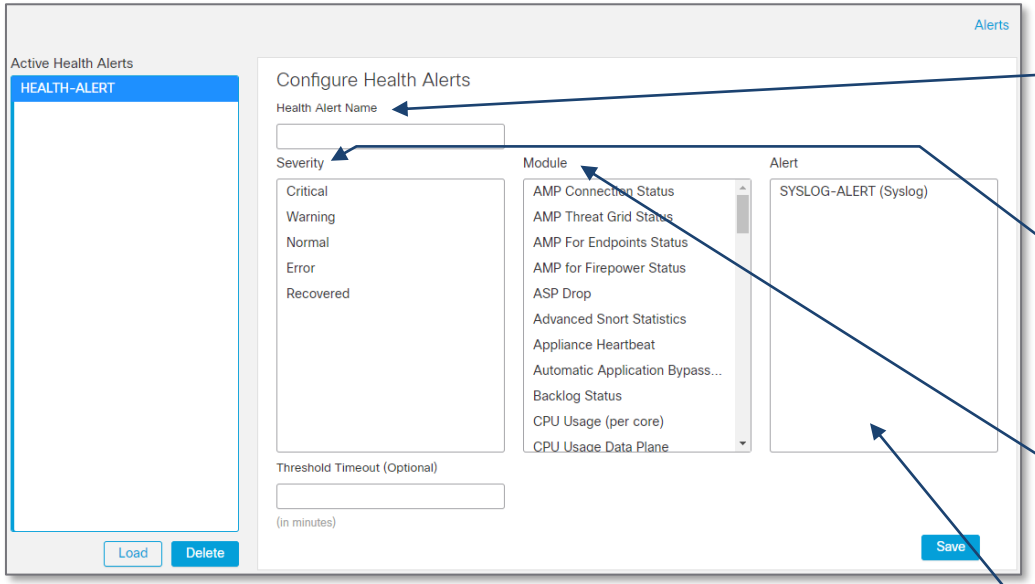
- System > Health > Monitor Alerts
- ヘルスポリシーのモジュールステータスが変更された際、Email、SNMP、またはシステムログを介して通知するアラートの設定
- Default では HEALTH-ALERT が作成され、それぞれのモジュールに対して、Syslog にて Alert を送信するよう設定されている

Health Monitor Alerts 概要②



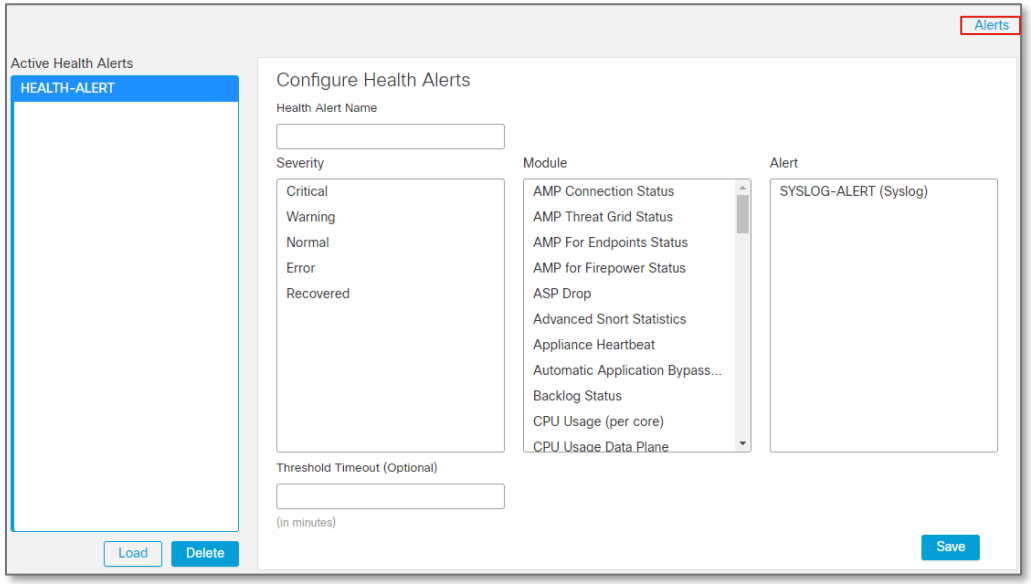
- ヘルスモニターによって生成されるアラートには、以下の情報を含む
  - Severity: アラートの重大度レベル。それぞれの重大度レベルに達した場合のアクションを次項で選択
  - Module: 監視結果のアラートをトリガーするヘルスモジュールの指定
  - Alert: 指定した重大度レベルに達した際の通知方法を選択

Health Monitor Alerts – 設定方法



- 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: 必要なヘルスモジュールを選択(複数選択可)
- Alert: 通知方法を選択

Health Monitor Alerts – Alerts 追加設定方法



- 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	• ヘルスチェック間隔の設定 • 7.0 以降のデバイスには Run Time Interval の値が適用される • 7.0 以前のデバイスには Legacy Run Time Interval の値が適用される	• 1分 (Run Time Interval) • 5分
2	AMP Connection Status	• 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	無効
3	AMP Threat Grid Status	• 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	有効
4	AMP for Endpoints Status	• 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	有効

5	AMP for Firepower Status	• 以下の条件にマッチした場合にアラートを通知
		  • 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
		  • 接続時の暗号化キーが無効の場合
		  • Threat Grid への動的分析によるファイル転送が失敗した場合
			有効

6	ASP Drop	• 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	有効
7	Advanced Snort Statistics	• Advanced Snort の統計情報を監視	

Appendix: Health Policy モジュール

No.	カテゴリ	説明	デフォルト値
8	Appliance Heartbeat	• 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	有効
9	Automatic Application Bypass Status	• 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	有効
10	Backlog Status	• 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	有効
11	CPU Usage (per core)	• 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	• 無効 • Critical Threshold 90% • Warning Threshold 80%
12	CPU Usage Data Plane	• 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	• Critical Threshold 90% • Warning Threshold 80%
13	CPU Usage Snort	• 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	• Critical Threshold 90% • Warning Threshold 80%

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	• 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	• Critical Threshold 90% • Warning Threshold 80%
15	Card Reset	• 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	無効
16	Chassis Status FTD	• Firepower2100/1000シリーズ 用 • シャーシパラメータ (ファン速度や温度など) を監視 • 設定した閾値を超えた場合にアラートを通知	• 有効 • Critical Chassis Temperature 85% • Warning Chassis Temperature 75%
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 • 新しい Primary デバイスが導入された際 • 新しい Secondary デバイスが Failover にジョインした際 • Primary/Secondary のどちらかが Failover から外れた場合	有効
18	Configuration Database	• 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	• Critical Threshold 50% • Warning Threshold 15%

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% • 2HD 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	• 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	• 有効 • Critical number Hosts 10 • Warning number Hosts 50
34	ISE Connection Status Monitor	• FMC と ISE 間の接続状況を監視	有効
35	Inline Link Mismatch Alarms	• 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	有効
36	Interface Status	• 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	有効
37	Intrusion and File Event Rate	• 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。	• 有効 • Events per second (Critical) 50 • Events per second (Warning)

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	• 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	• 有効 • Critical number Hosts 10 • Warning number Hosts 50
39	Local Malware Analysis	• ローカルマルウェア解析の動作の監視	有効
40	Memory Usage	• 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	• 有効 • Critical Threshold 90% • Warning Threshold 80%
41	Memory Usage Dataplane	• 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	• Critical Threshold 90% • Warning Threshold 80%
42	Memory Usage Snort	• 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	• Critical Threshold 90% • Warning Threshold 80%

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	• 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	無効
54	Security Intelligence	• 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	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 • Product Instance Registration Token の有効期限が切れた場合 • Smart License の使用が準拠していない場合 • 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	有効
56	Snort Identity Memory Usage	• 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	• 有効 • Critical Threshold 80%
57	Snort Statistics	• FTD にてイベント、フロー、パケットの Snort 統計情報を監視	有効
58	Sybase Status	• FMC にて Sybase のデータベースを監視	有効
59	Threat Data Updates on Devices	• 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	• 有効 • Send critical alert after (hours) 24 • Send warning alert after (hours) 1

Appendix: Health Policy モジュール

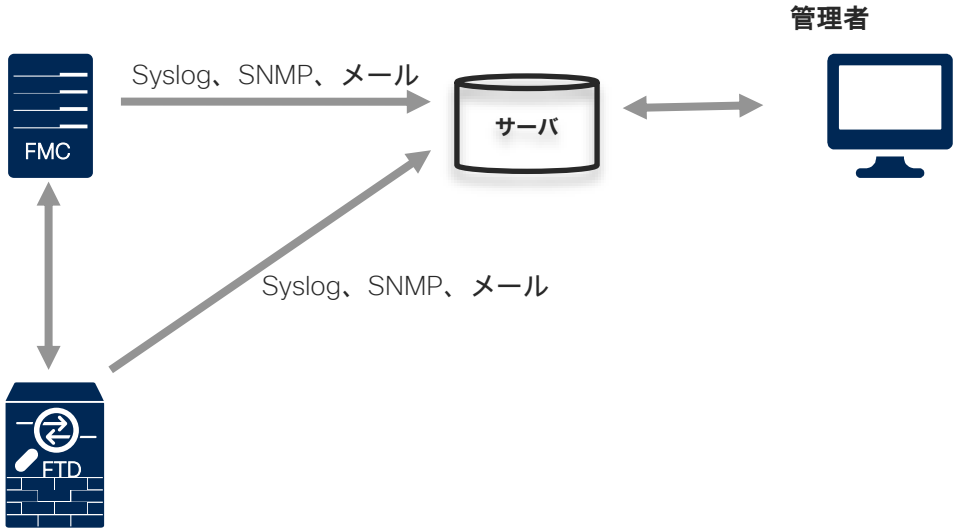
No.	カテゴリ	説明	デフォルト値
60	Time Series Data Monitor	• FMC の時系列データ (相関イベントカウントなど) が保存されているディレクトリ内にて、破損したファイルの存在をトラキングし、ファイルに破損フラグが付けられて削除された場合にアラートを通知	有効
61	Time Synchronization Status	• NTP を使用して時刻を取得するデバイスクロックと NTP サーバのクロックとの同期を追跡し、クロックの差が10秒を超える場合にアラートを通知	有効
62	URL Filtering Monitor	FMC が以下の条件にマッチした場合、アラートを通知 • Cisco クラウドへの登録に失敗 • 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 • URL ルックアップが出来ない	• 有効 • Send critical alert after (hours) 24 • Send warning alert after (hours) 1
63	Unresolved Groups Monitor	• ポリシー適用外のグループを監視	有効
64	User Agent Status (deprecated)	• ユーザエージェントの監視 • ただし、FMC 6.7 以前の機能であり、7.x では使用されない	有効
65	VPN Statistics	• Site to Site VPN や Remote Access VPN のトンネル統計情報を監視	有効
66	VPN Status	• Site to Site VPN や Remote Access VPN のトンネルの状態を監視 • トンネルダウンを検知した場合アラートを通知	有効
67	xTLS Counters	• xTLS/SSL フロー、メモリー、キャッシュの有効性を監視	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



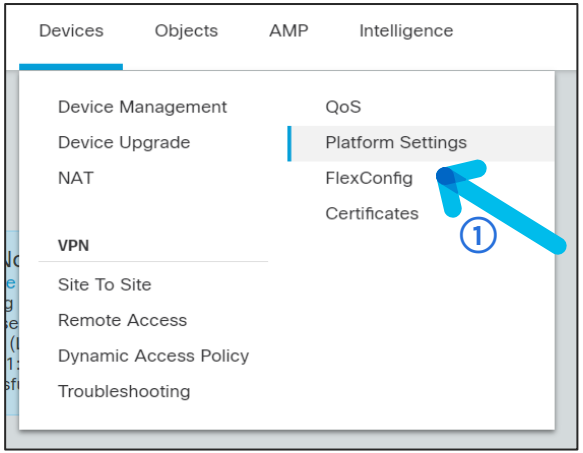
設定の流れ

- 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

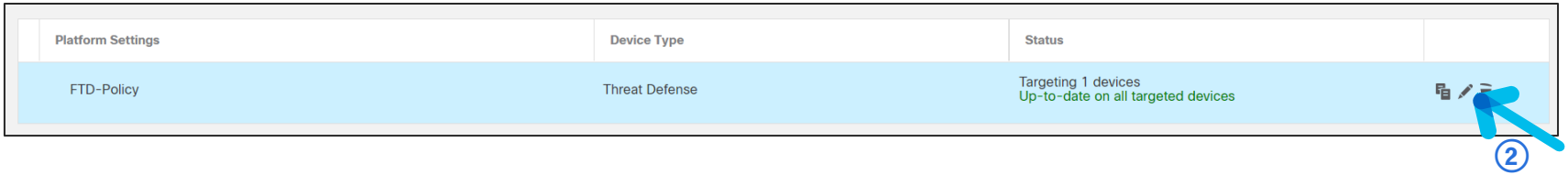
Syslog サーバが、FMC より疎通の取れるネットワークセグメントに構築してある前提とする

Logging Setup 設定

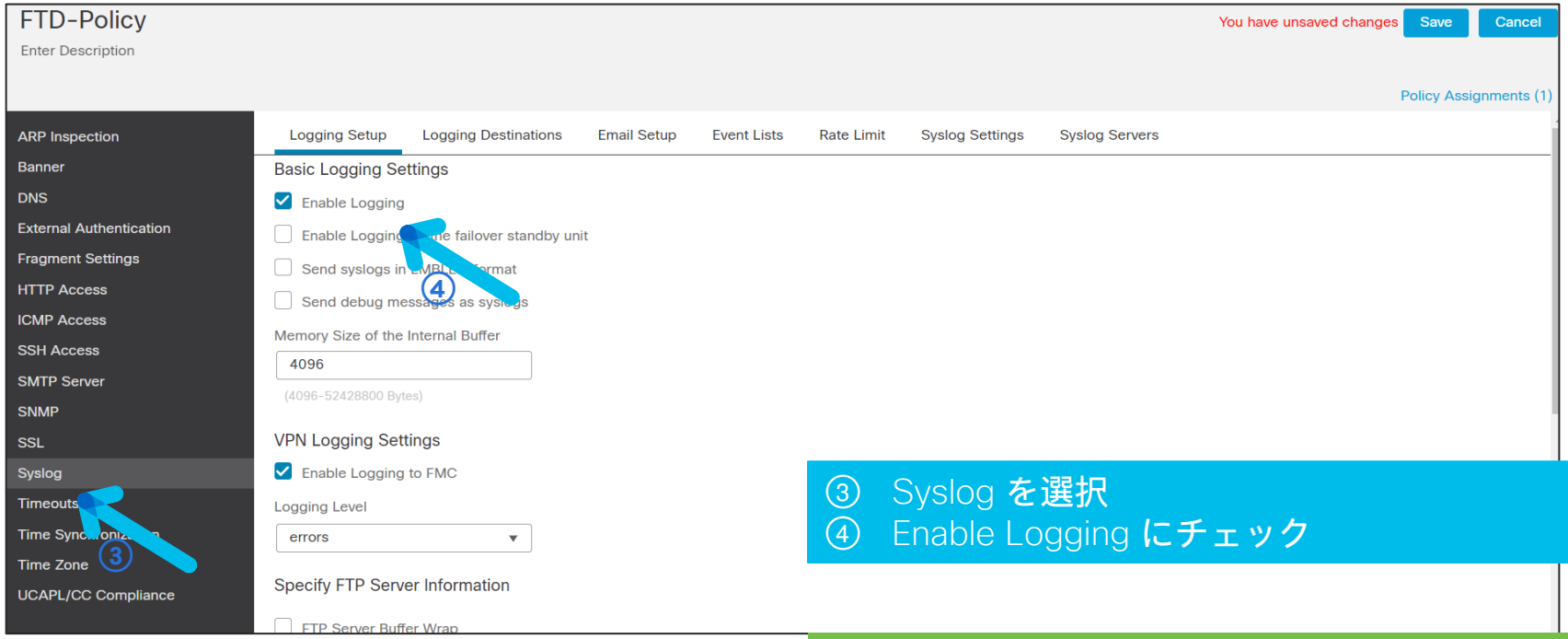
- ロギングの設定



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



Logging Setup 設定（続き）

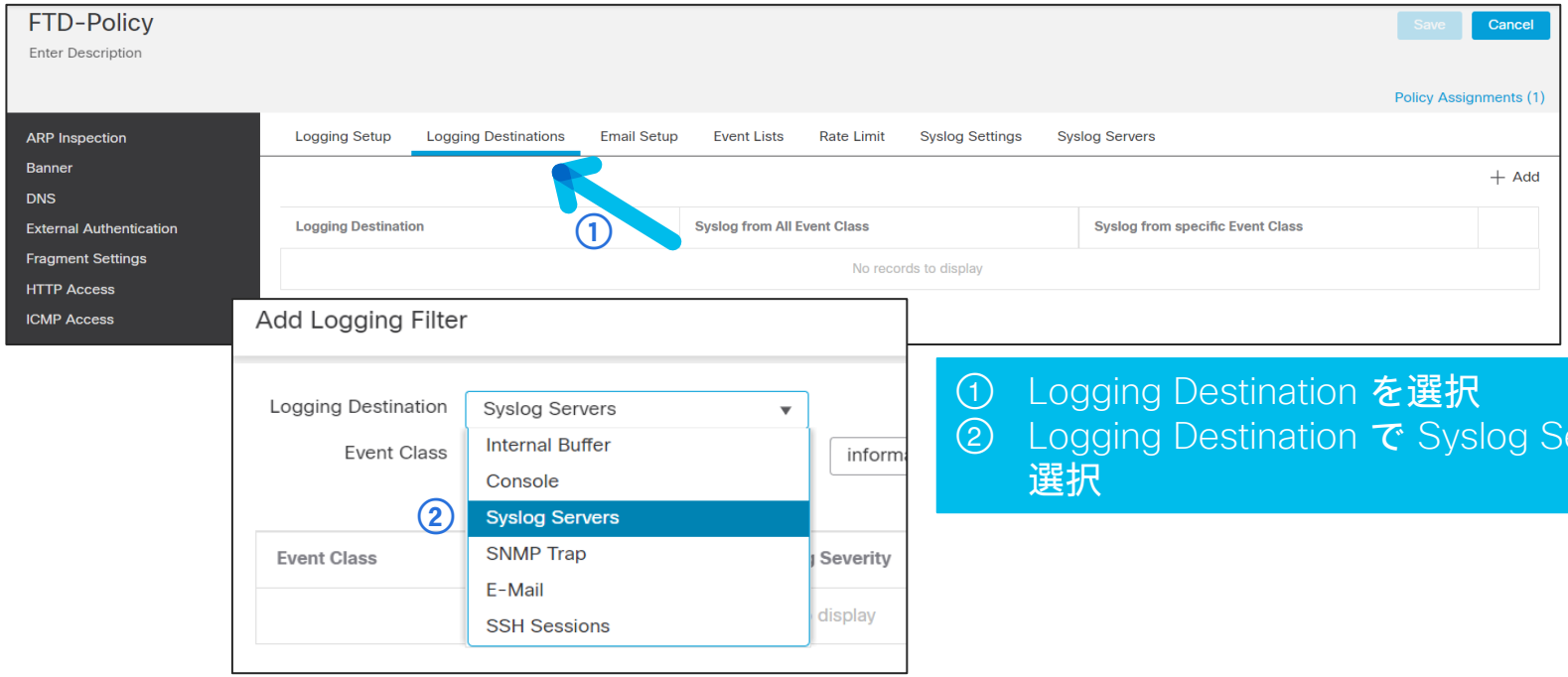


③ Syslog を選択
④ Enable Logging にチェック

- 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

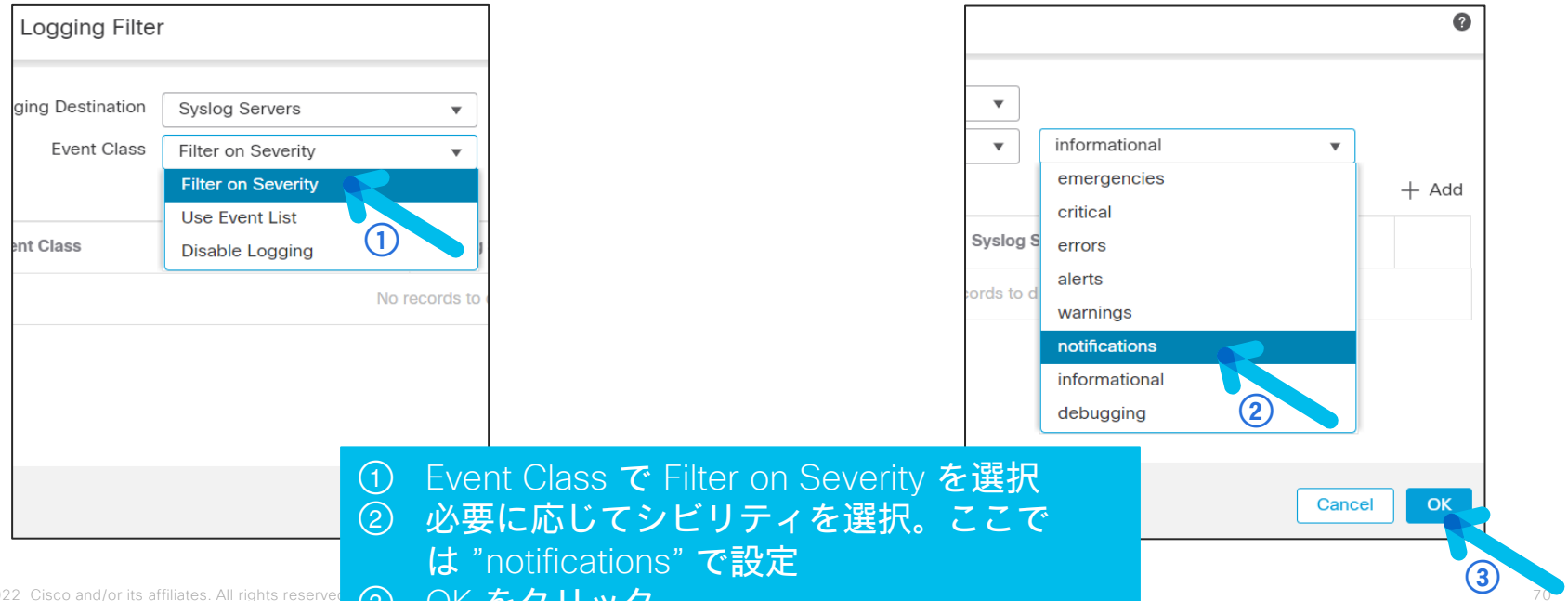
- ログの送付先を指定



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

Logging Destination 設定 (続き)

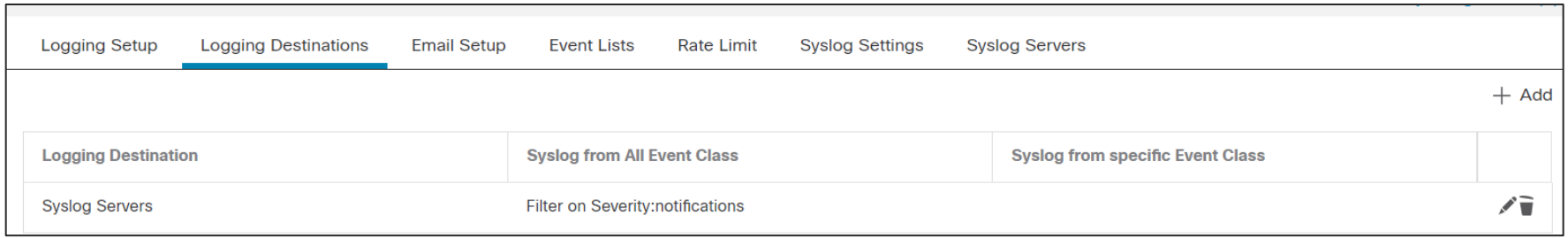
- 送付するログの種別を指定



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

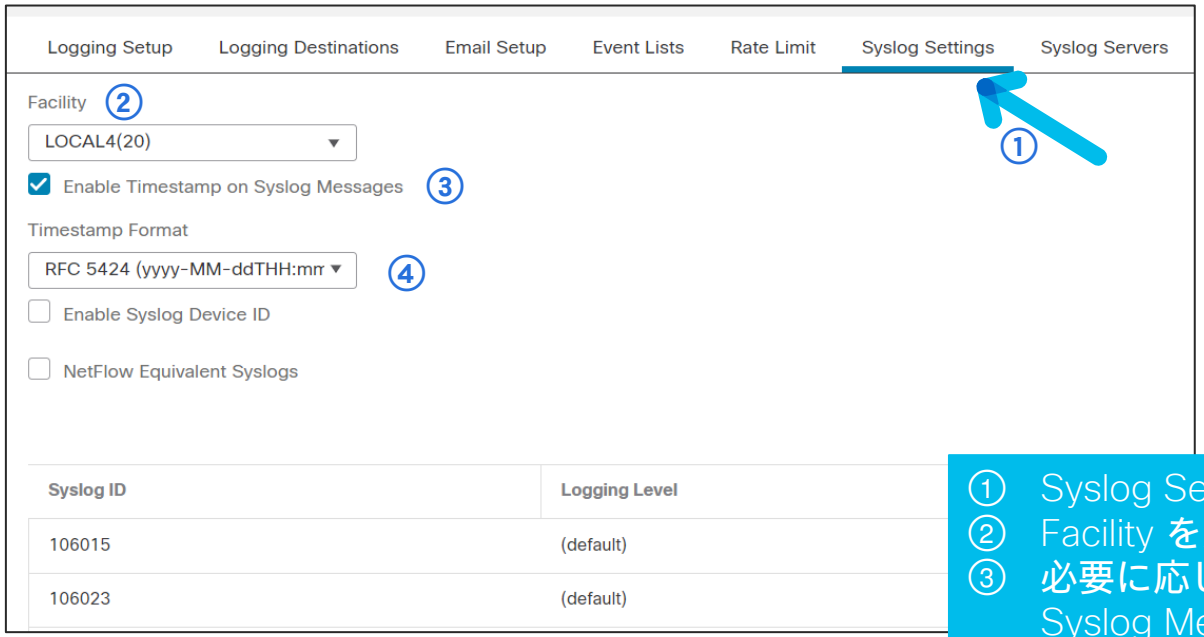
Logging Destination 設定 (続き)

- OK をクリック後、以下のような行が表示



Syslog Settings 設定

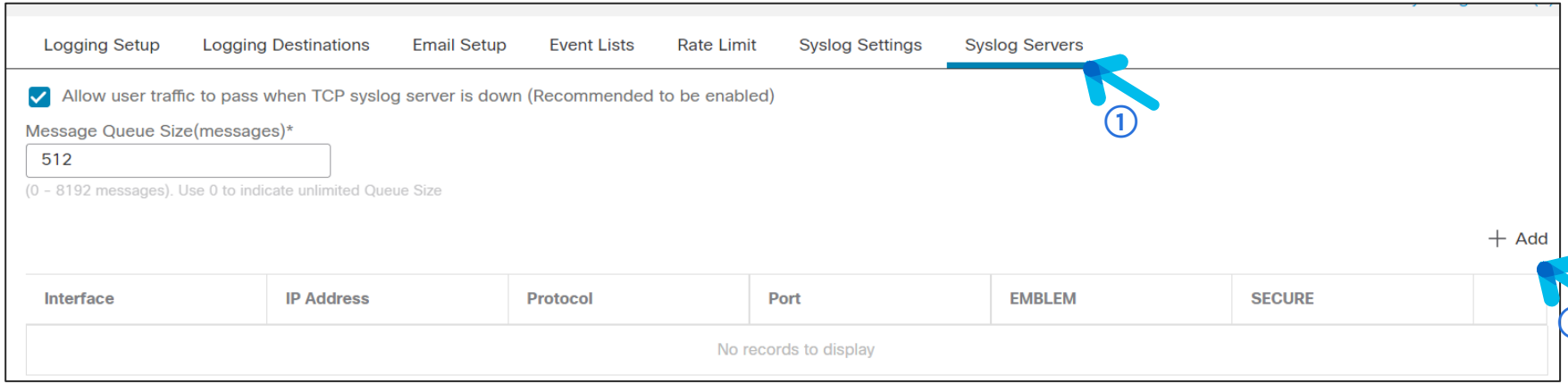
- Syslog メッセージの出力設定を実施



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

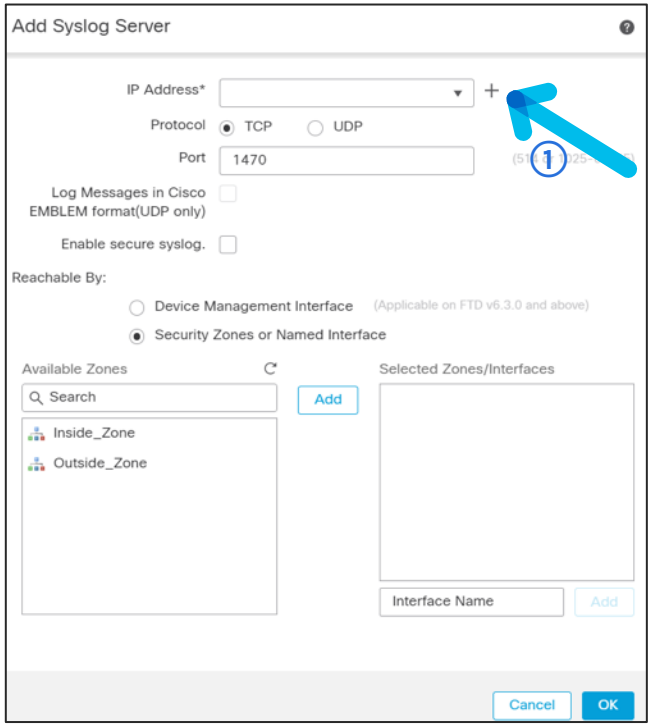
- Syslog メッセージを出力する先の Syslog サーバ設定を実施

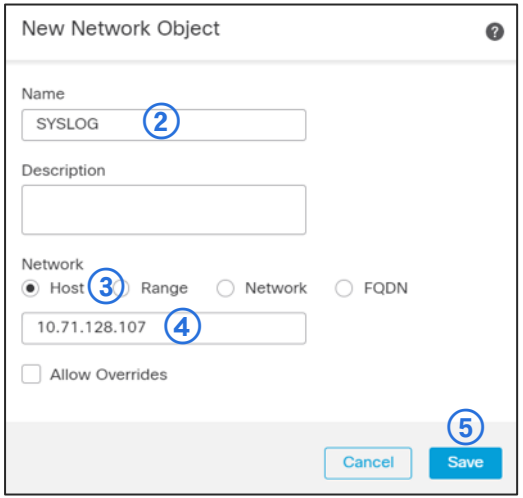


① Syslog Servers を選択
② Add をクリック

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



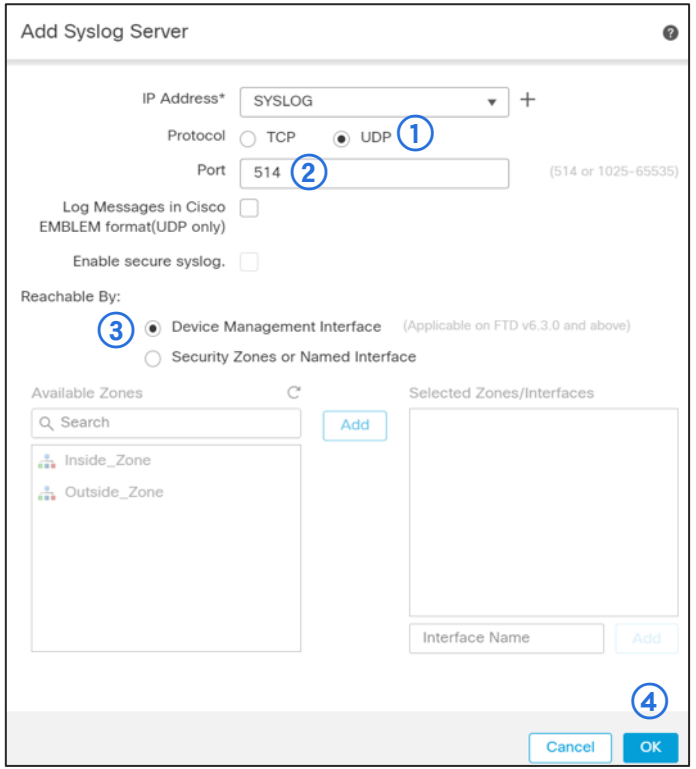


① “+” の追加アイコンをクリック。Network Object 作成画面が表示
② Name を入力。ここでは ”SYSLOG” と設定
③ Network 種別の Host をチェック
④ Syslog サーバの IP アドレスを入力
⑤ Save をクリック

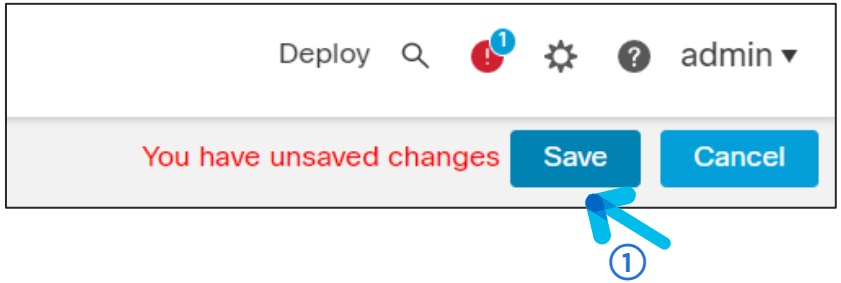
Syslog Servers 設定（続き）

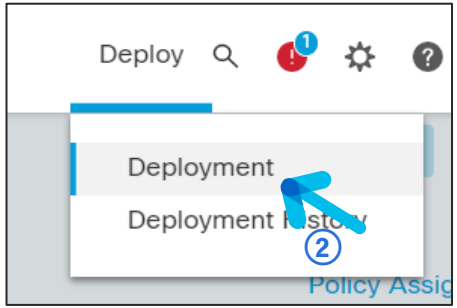
- Syslog メッセージを出力する先の Syslog サーバを設定

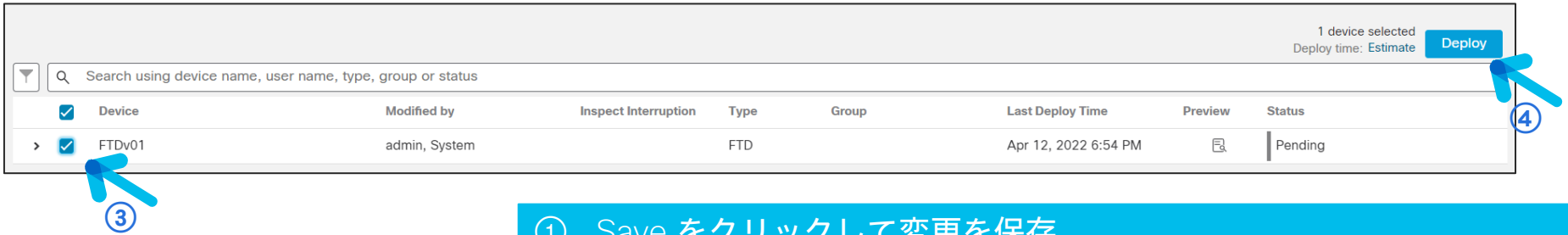
① Syslog メッセージ送信プロトコルを選択する。ここでは UDP を選択
② 同様にポートを指定する。ここでは 514 を選択
③ Reachable By で Syslog メッセージの送信元とするインターフェイスを選択する。ここでは ”Device Management Interface” を選択
④ OK をクリック



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

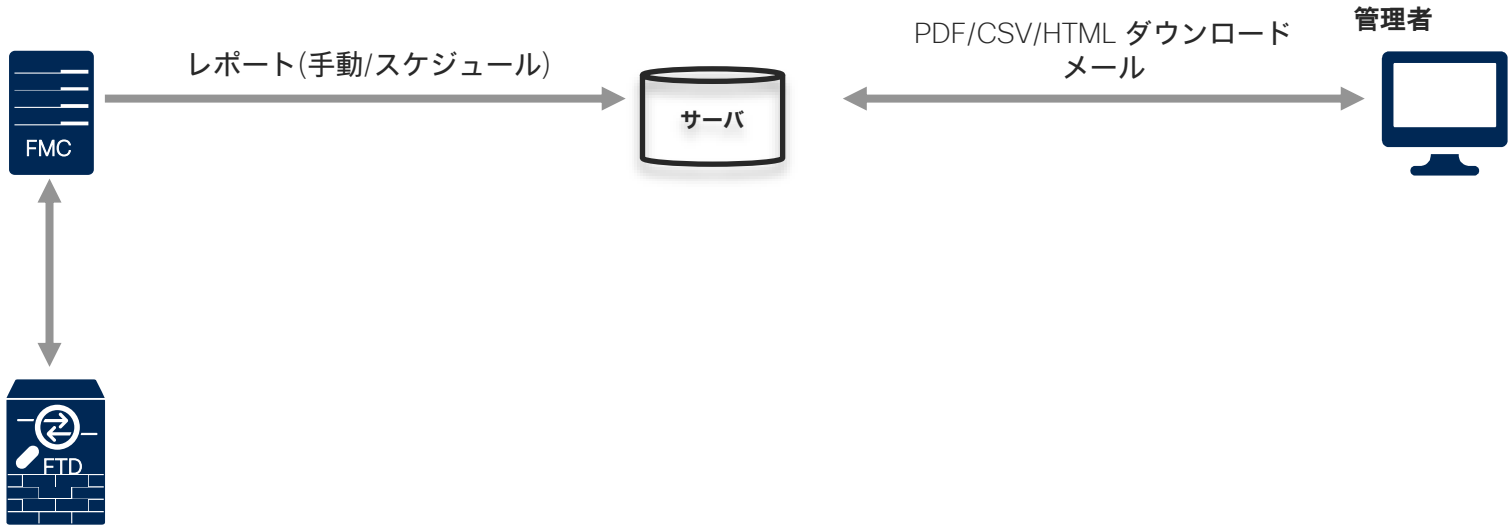
- 例えば FTD のインターフェイス GigaEthernet0/0、0/1 の Down と Up を行った場合、Syslog サーバへは下記のようにメッセージが出力

```
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

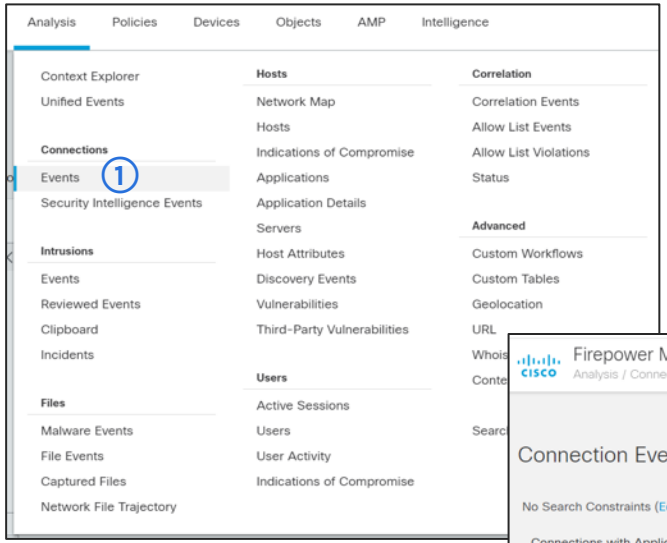
レポート機能

- 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



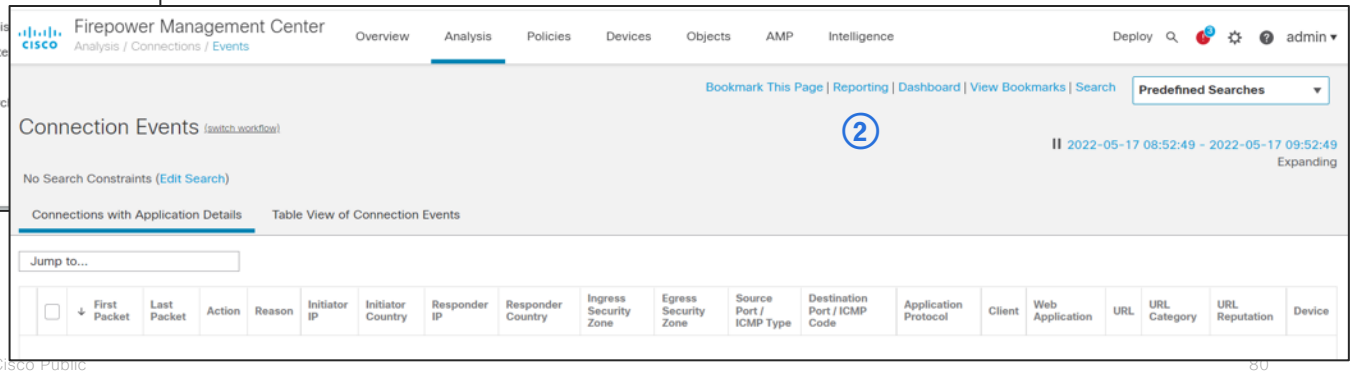
手動レポート作成

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



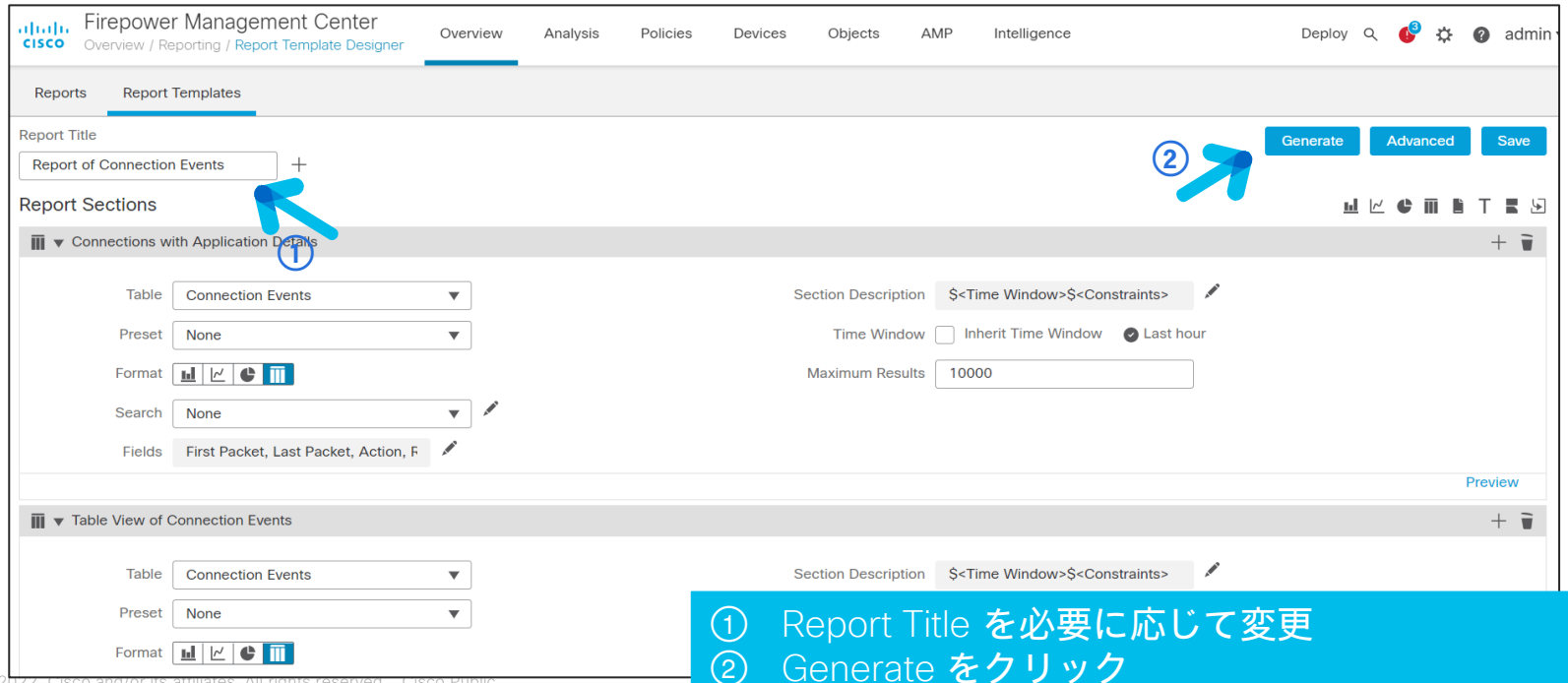
① Analytics – Connection – Events を選択
② Reporting をクリック

- 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



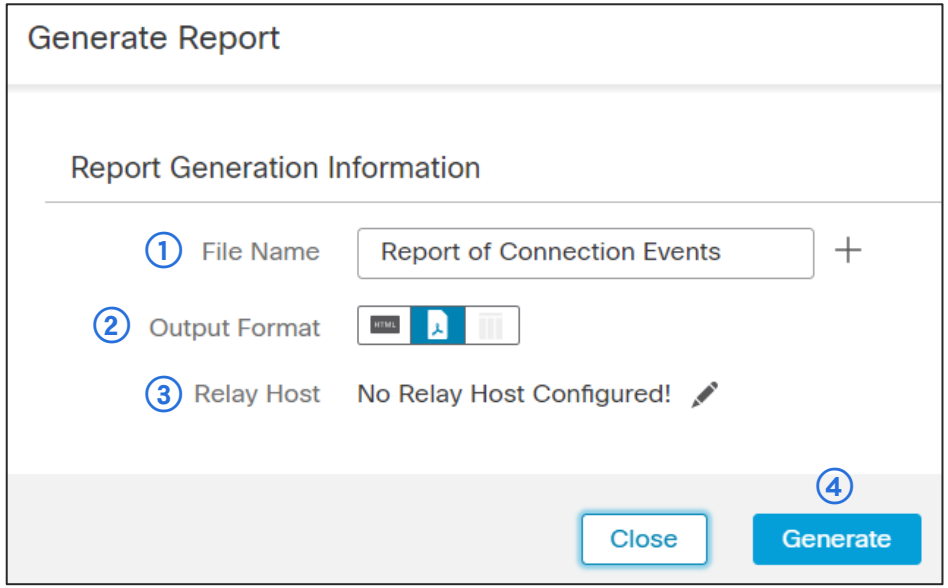
手動レポート作成 (続き)

手動生成レポートのパラメータを指定



手動レポート作成 (続き)

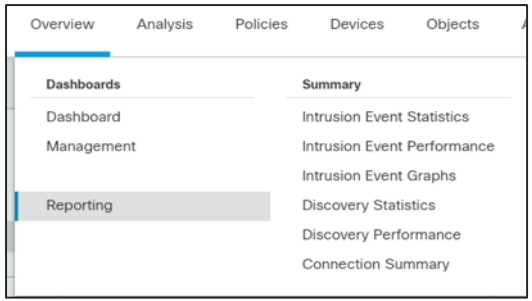
手動生成レポートの出力形式を指定



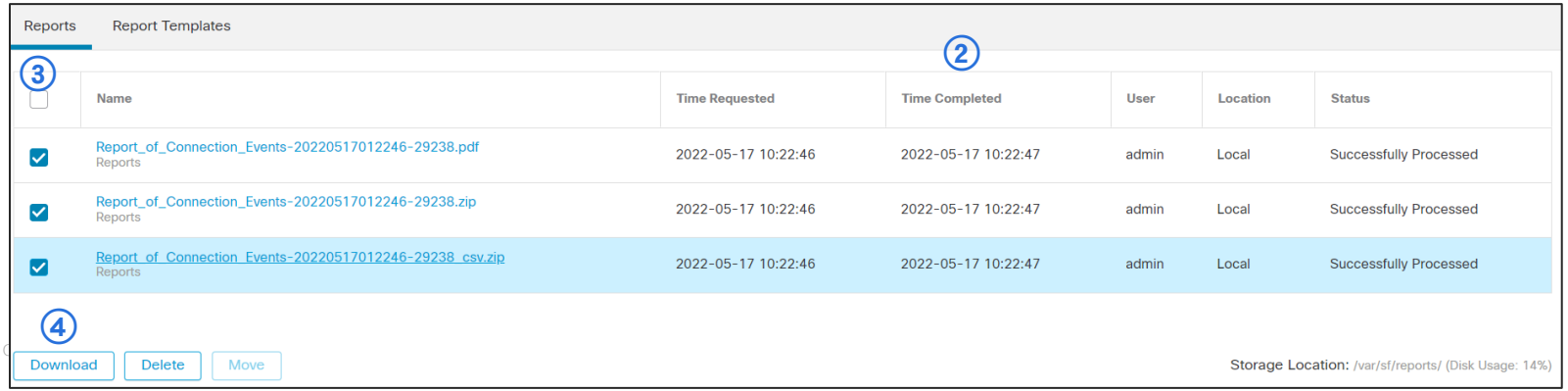
① File Name は Report Title が引き継がれる。変更することも可能
② Output Format を選択。左から HTML、PDF、CSV フォーマット（複数選択可能）
③ 必要に応じて Relay Host にてレポートを送信する Mail Relay Host を指定
④ Generate をクリック

レポートの確認

生成したレポートの確認

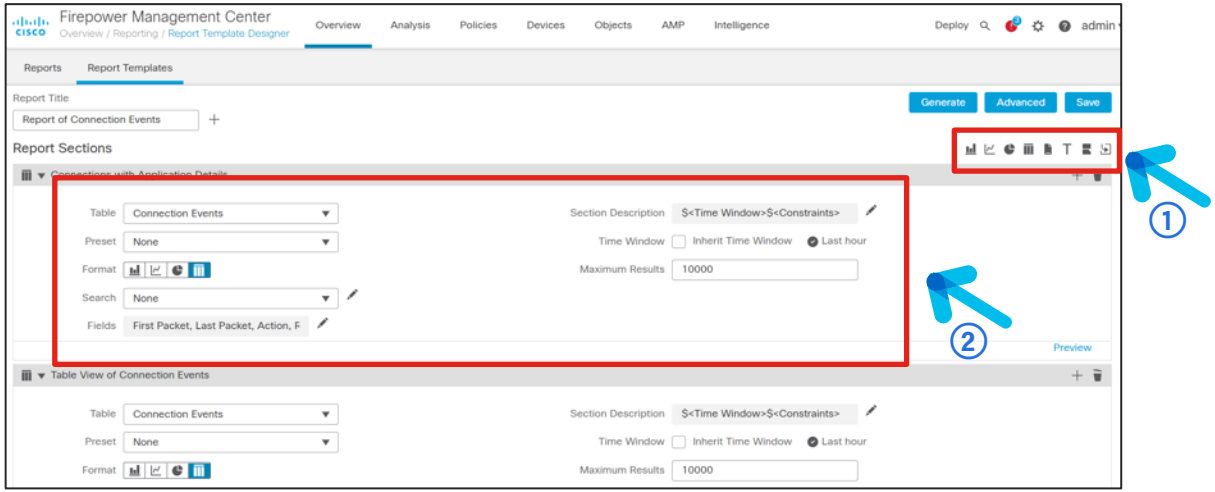


① Overview – Reporting を選択。生成済みレポートの一覧を表示
② 確認する対象のレポートの Time Completed の欄に日時が表示されていることを確認。日時が表示されていれば、レポートの生成処理が完了済み
③ 確認対象のレポートにチェックを入れる
④ Download をクリック



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

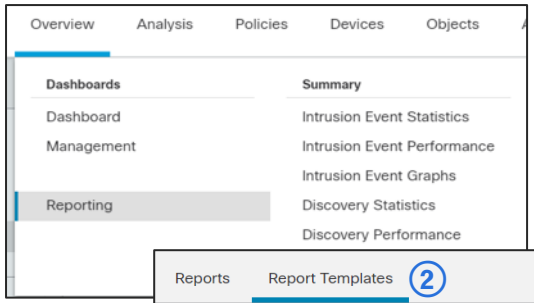


① **追加するセクション種別の選択。**Bar Chart / Line Chart / Pie Chart / Table View / Detail View / Text Section / Page Break / Import Sections from Dashboard, Summaries, and Workflows **より指定**

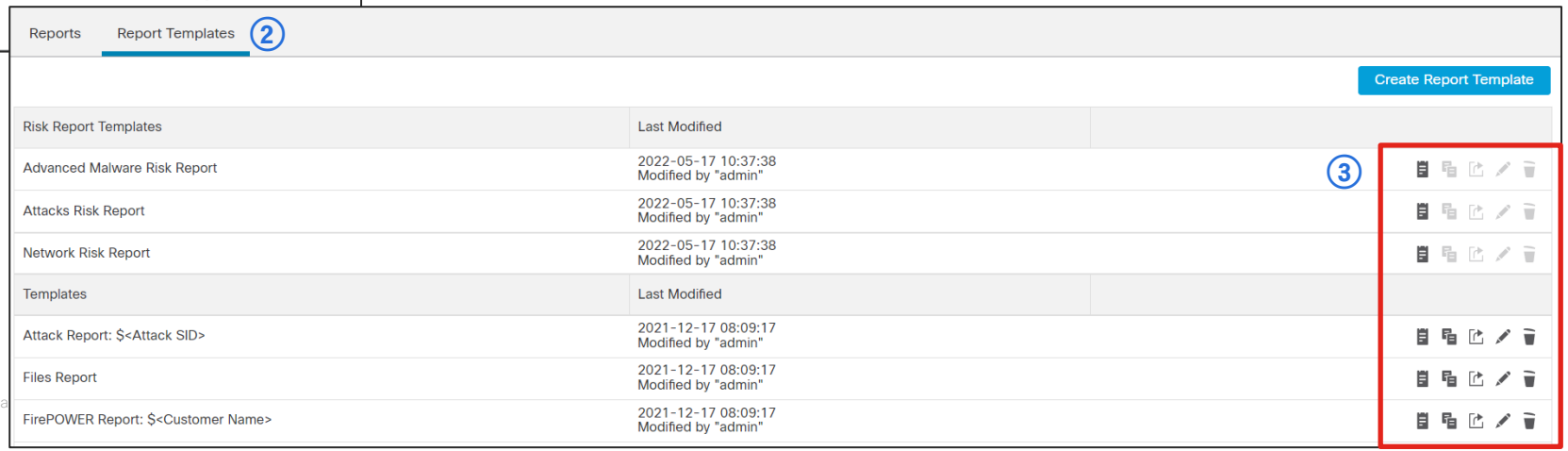
② **セクションごとのカスタマイズも可能。**Table**種別（**Table**）、レポートに含める検索条件（**Search**）、レポート対象の期間（**Time Window**）、表示するフィールド（**Fields**）等**

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

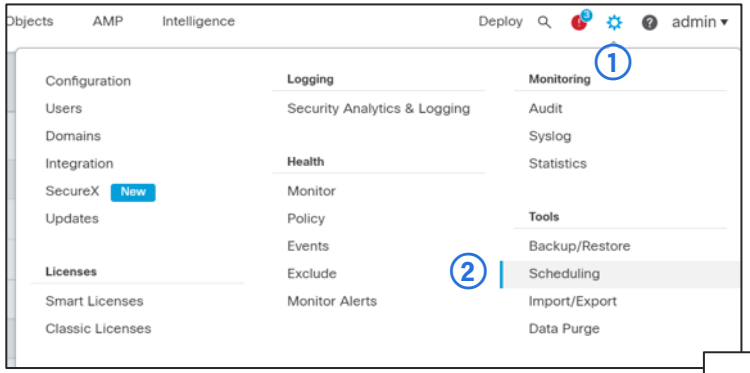


① Overview - Reporting を選択
② Report Templates を選択
③ 各種操作を実行可能。Generate / Copy / Export / Edit / Delete
※ただし Risk Report Templets 下のものは Generate のみ

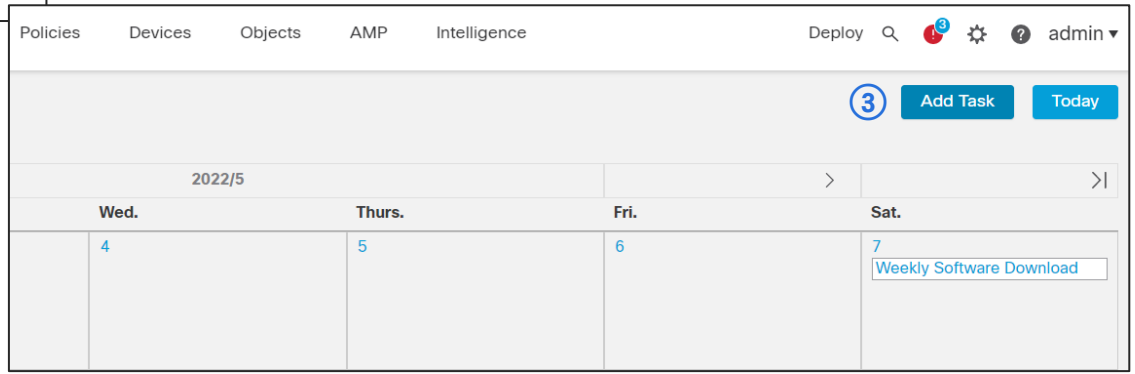


スケジュール レポート生成

スケジュールタスクにて、レポート生成タスクを定義

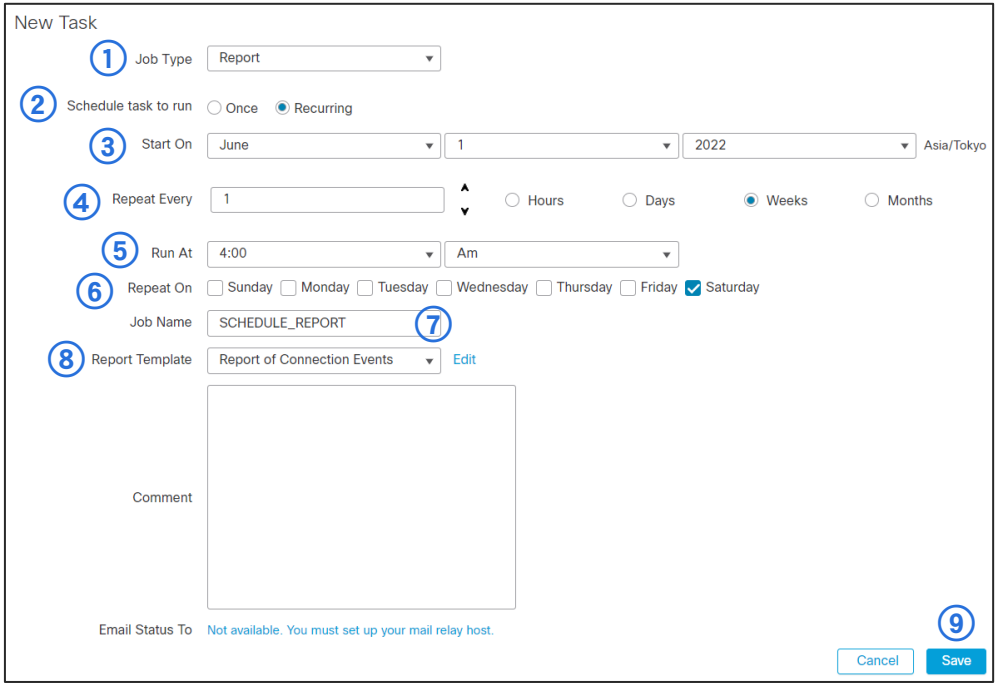


① 歯車マークをクリック
② Tools 下の Scheduling をクリック
③ Add Task をクリック



スケジュール レポート生成 (続き)

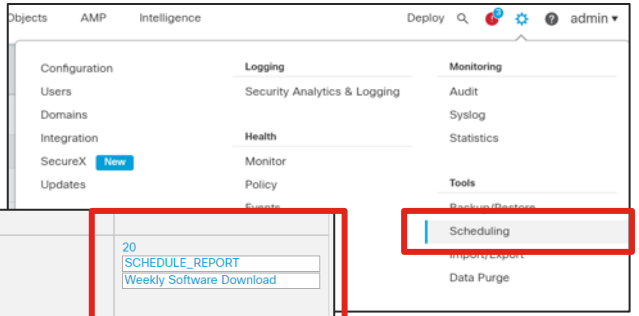
レポートの生成対象とする画面を開く。ここでは事前に作成した Connection Event を週次でスケジュール化

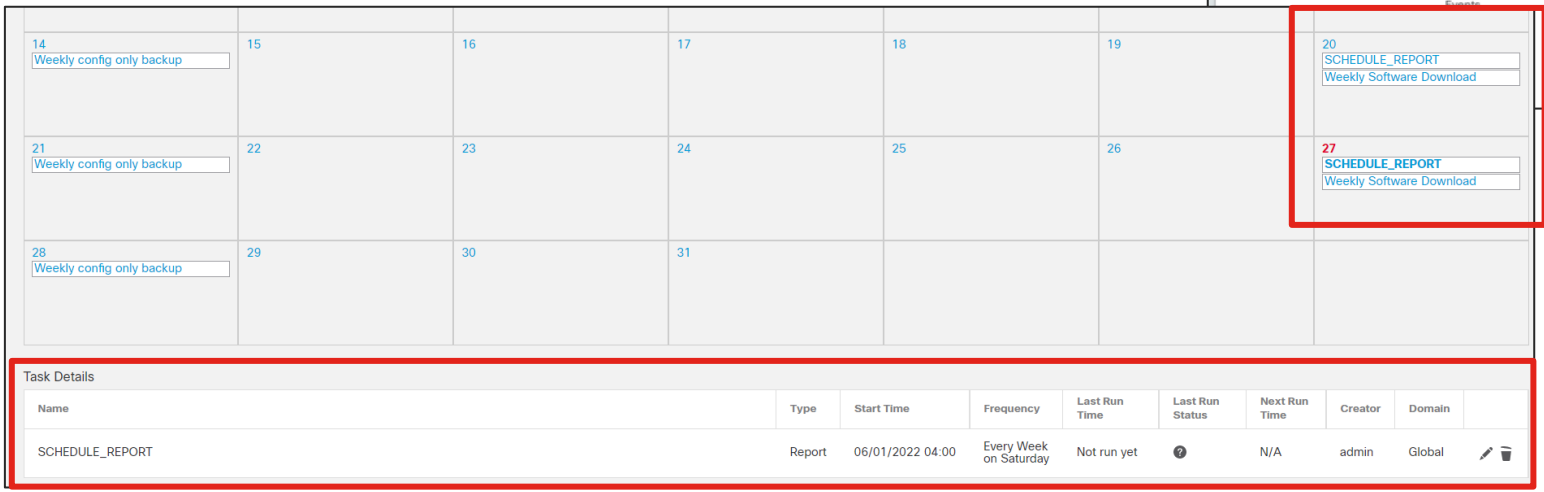


① Report を選択
② 繰り返しの作業として Recurring へチェックを入れる
③ レポート生成タスクの開始年月日を指定。ここでは 2022年6月1日と設定
④ レポート生成タスクの頻度を指定。ここでは週次で設定
⑤ 実行時間を指定。ここでは午前 4:00に処理を開始
⑥ 実行曜日を指定。ここでは日曜に処理を開始
⑦ Job Name を入力。ここでは ”SCHEDULE_REPORT” と入力
⑧ 生成する Report Template を指定する前のスライドで作成した Report of Connection Events を指定
⑨ Save をクリック

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

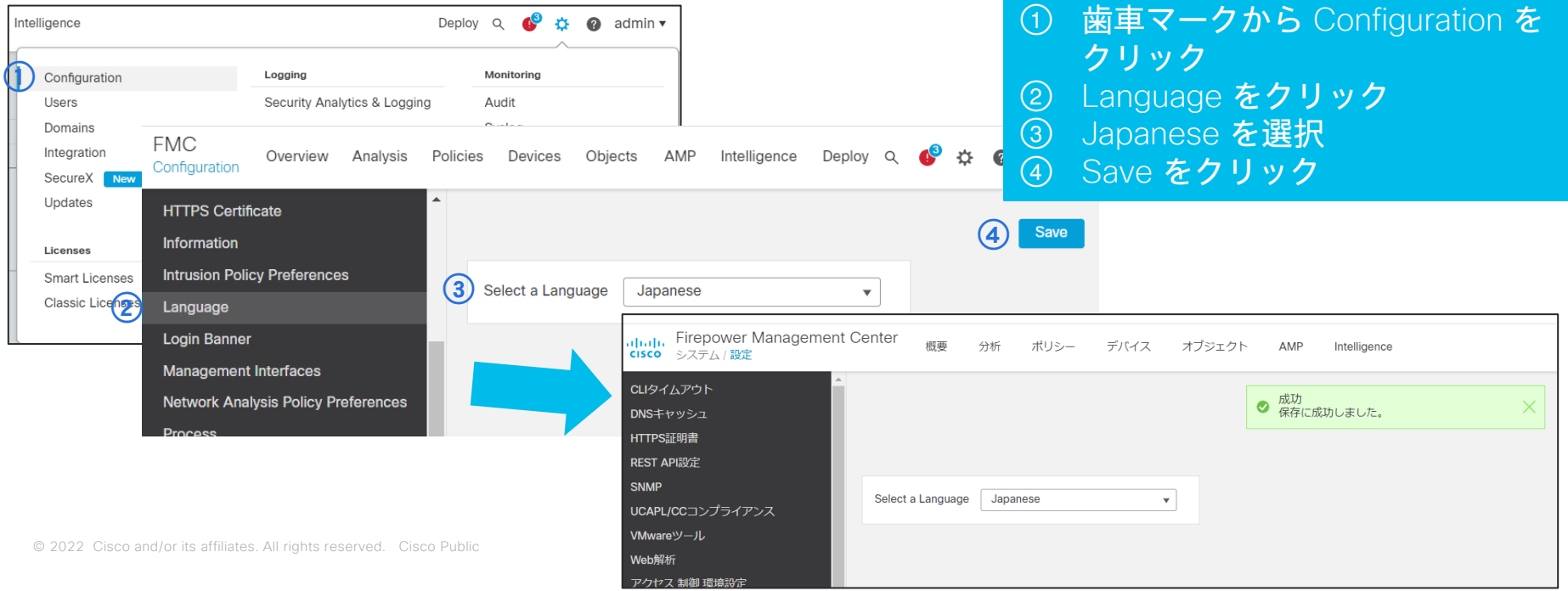




- 設定した通りにタスクが保存されていることを確認。毎週日曜日と設定したため、赤枠部分のようになっている
- 各タスクをクリックすると Task Details が下段に表示される。ここからタスクの実行状況や、編集/削除の操作が可能
- 生成されたレポートは手動生成レポートと同様に、Overview > Reporting > Reports より確認が可能

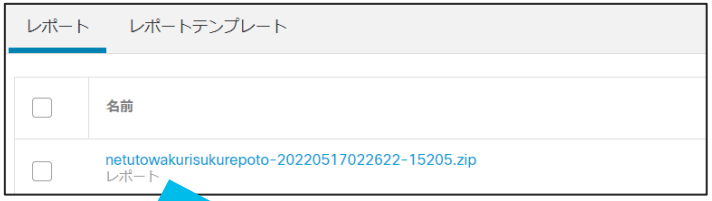
参考: レポートを日本語で生成

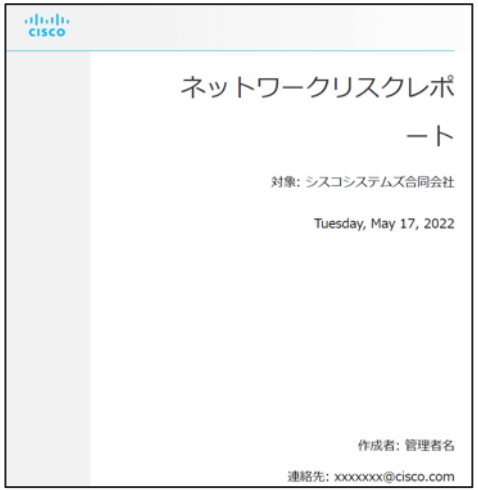
テンプレート定義済みのレポートは即時生成が可能。また、UIを日本語化していれば日本語でのレポート生成が可能。UI 日本語化の方法は以下の通り

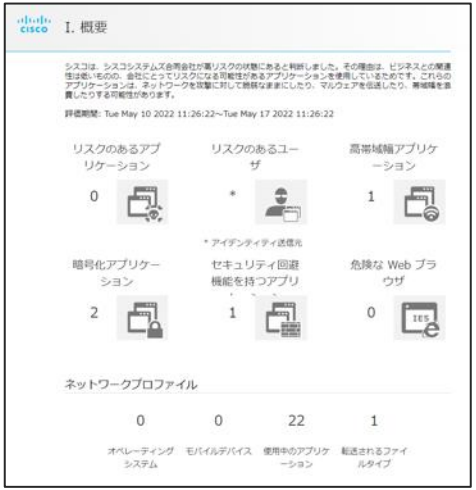


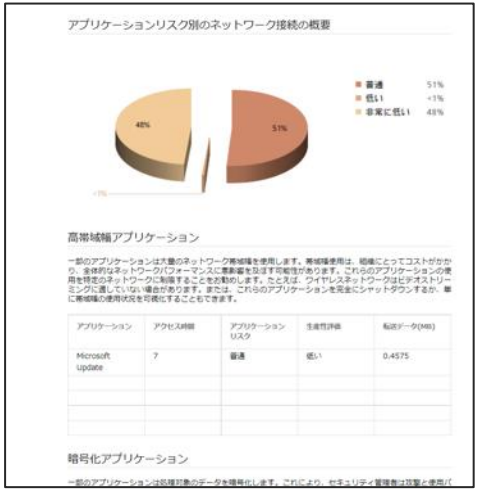
参考: レポートを日本語で生成 (続き)

参考: レポートを日本語で生成 (続き)









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
Health Monitor Event	機器自体のステータスに関するアラート
Audit Log Event	監査ログのアラート
Connection Event	Access Control Policy によるコネクションイベントのアラート
Discovery Event	Network Discovery のアラート
Impact Alert	Intrusion Policy イベントのうち、Impact Flag に応じたアラート
Intrusion Event	Intrusion Policy のアラート
Correlation Event	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
Network Malware Event	Network AMP のアラート

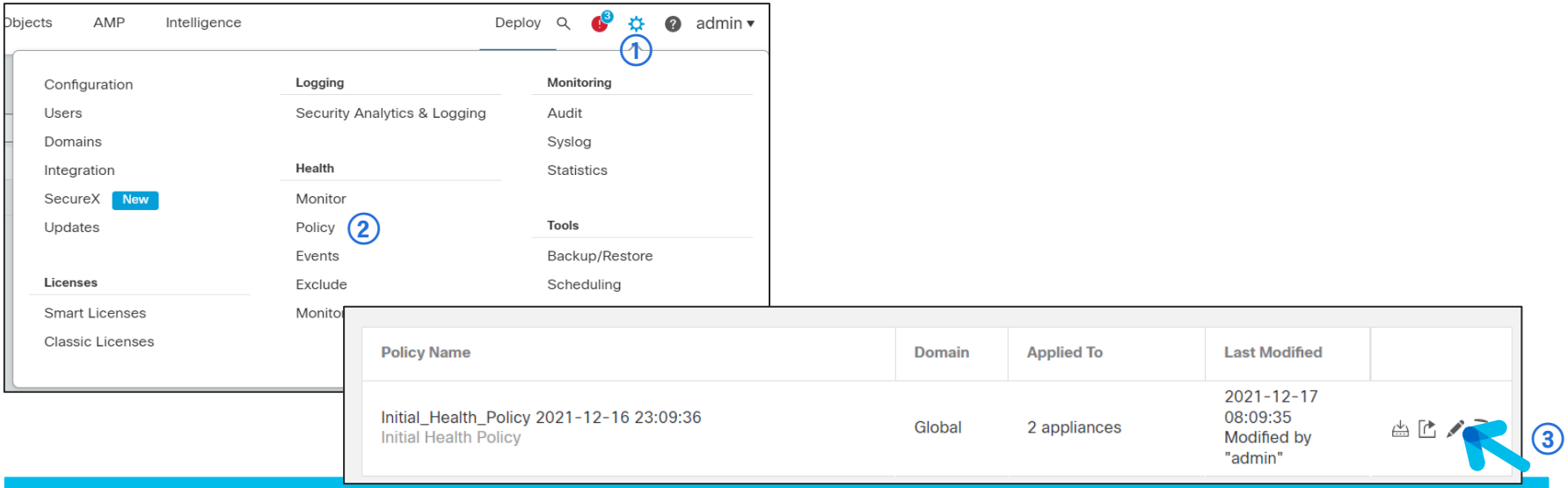
設定の流れ

- 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

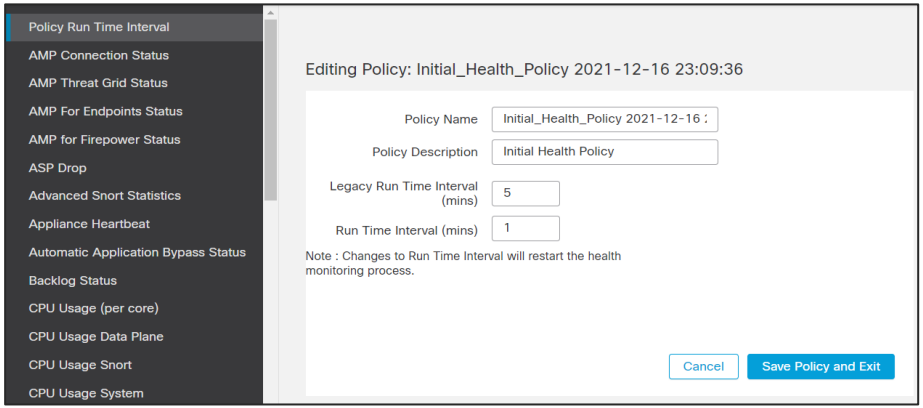


① 歯車マークを選択
② Health 下の Policy を選択
③ デフォルトで定義されている Health Policy 横の鉛筆アイコンをクリック

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)

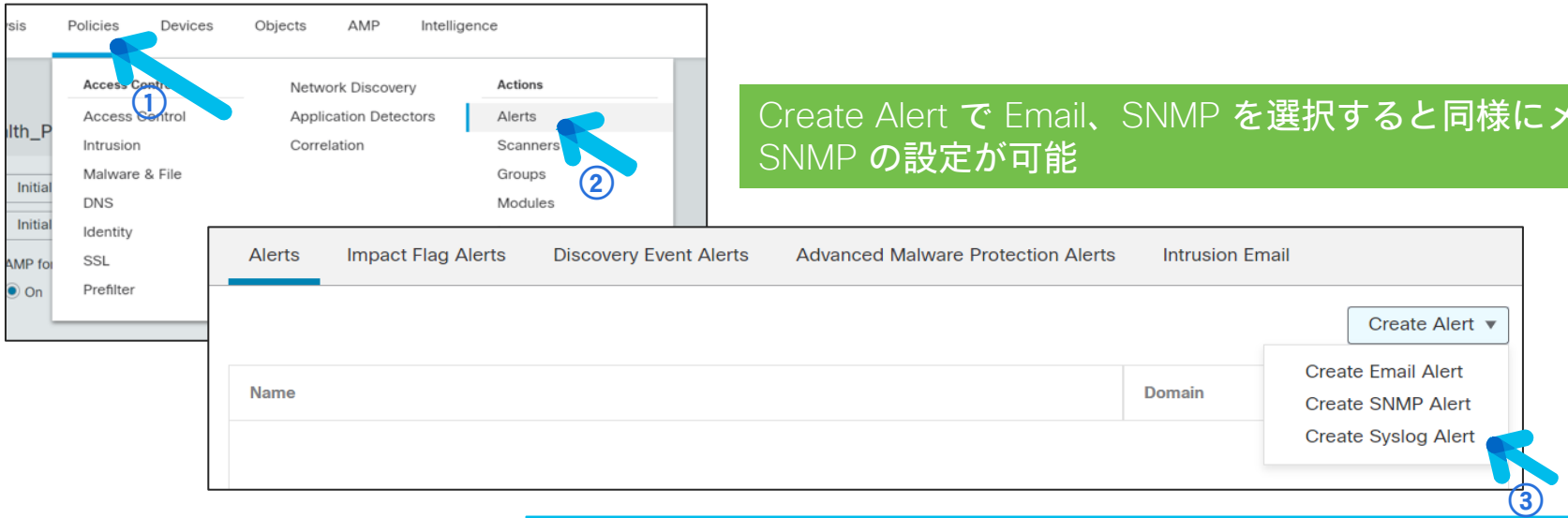
- デフォルトで定義されている Health Policy を確認



- 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

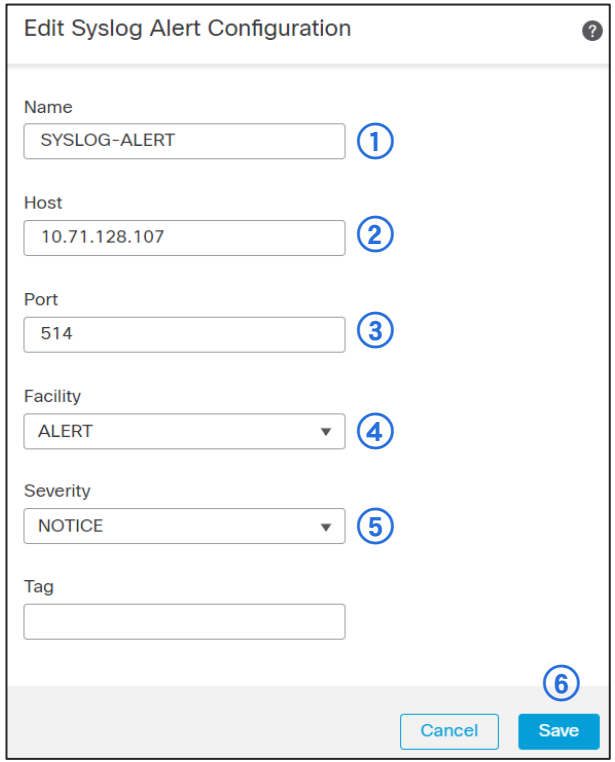
- Syslog Alert を作成



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

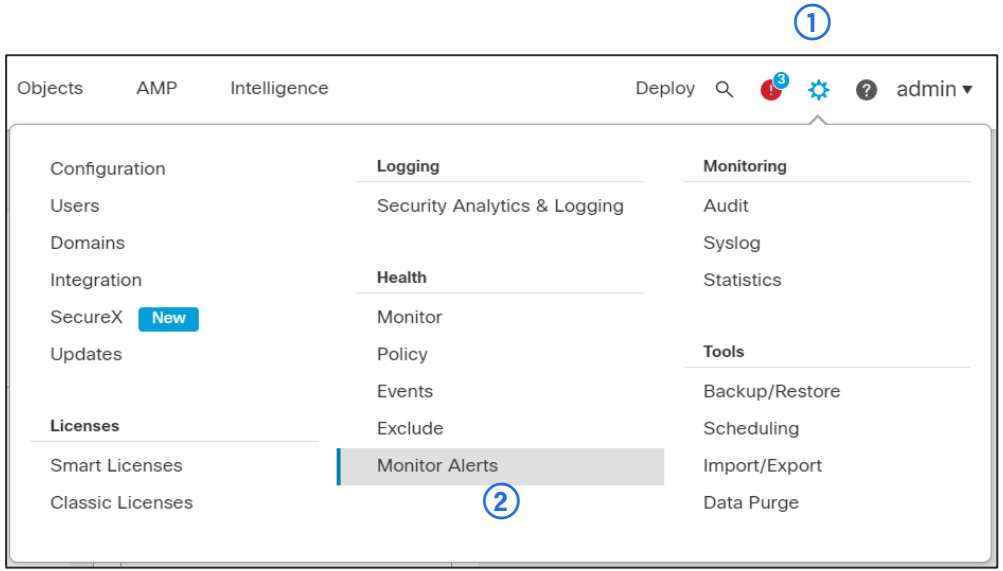
Syslog Alert 作成 (続き)



- Syslog Alert を作成

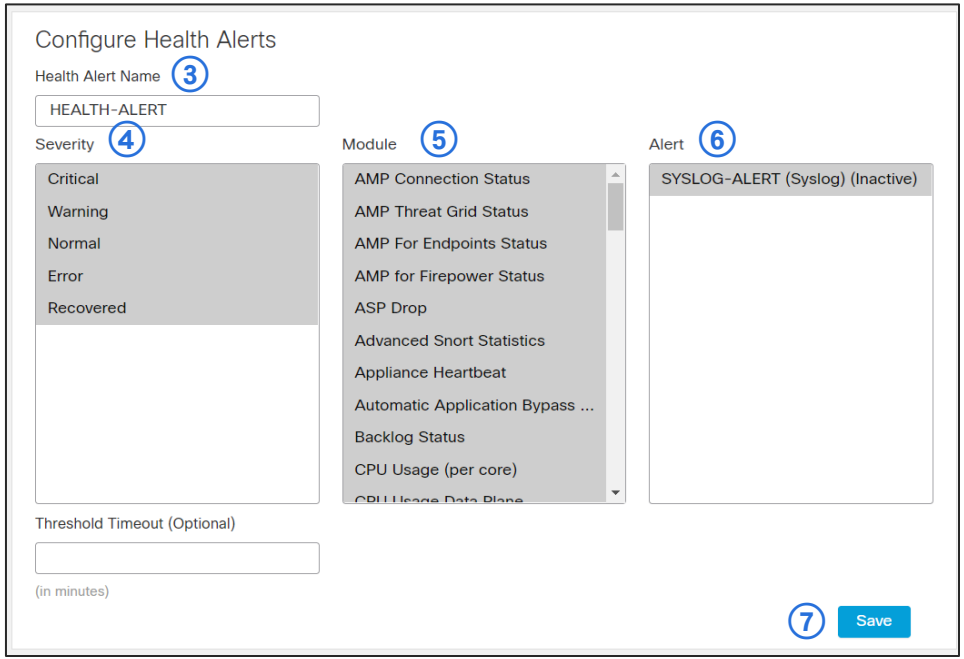
① Name を入力。ここでは ”SYSLOG-ALERT” とする
② Host に Syslog サーバのIPアドレスを入力
③ Port に Syslog サーバのポート番号を入力。デフォルトは 514
④ Facility を選択
⑤ Severity を選択。ここでは ”NOTICE” とする
⑥ Save をクリック

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)



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 によるコネクション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

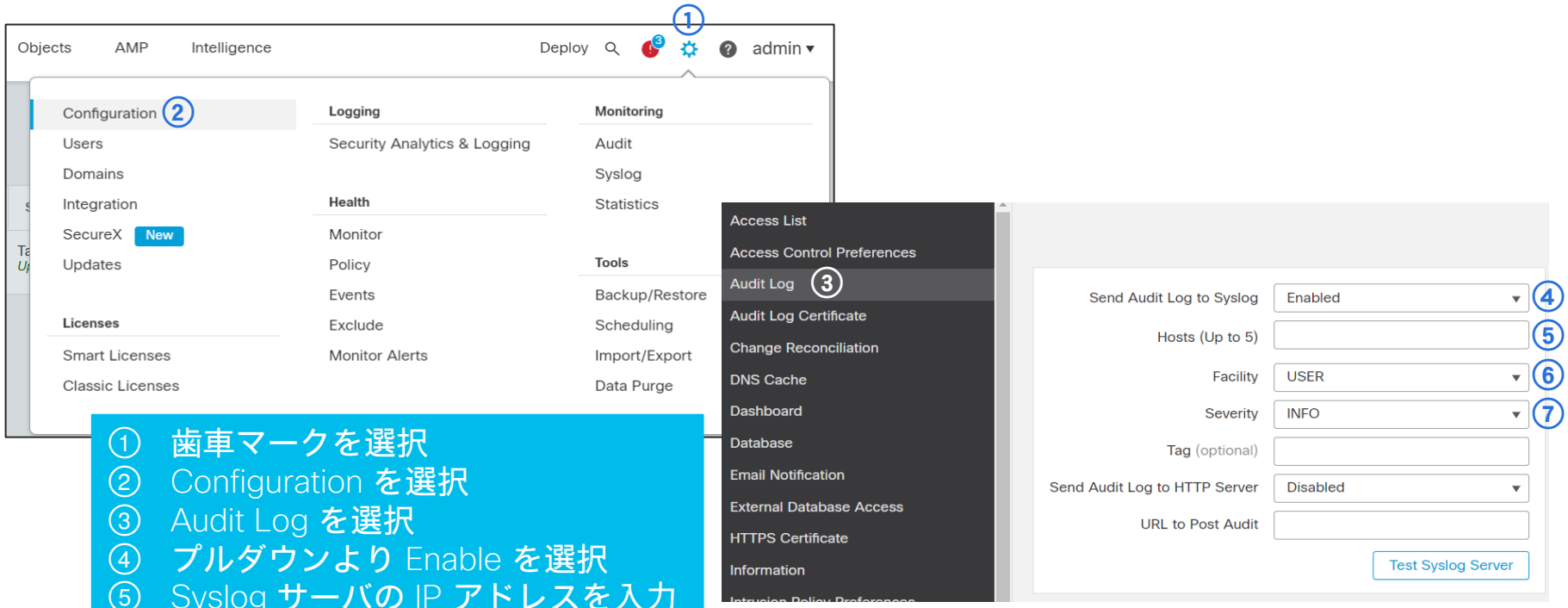
項目	説明	画面メニュー
Impact Flag Alert	Intrusion Policy イベントのうち、Impact Flag に応じたアラート	Alert ①Policies > Actions > Alerts Impact Flag Alerts ①Policies > Actions > Alerts > Impact Flag Alerts ②使用する Alert をプルダウンより指定
Intrusion Event	Intrusion Policy のアラート	Intrusion Event ①Policies > Access Control > Intrusion ②ア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

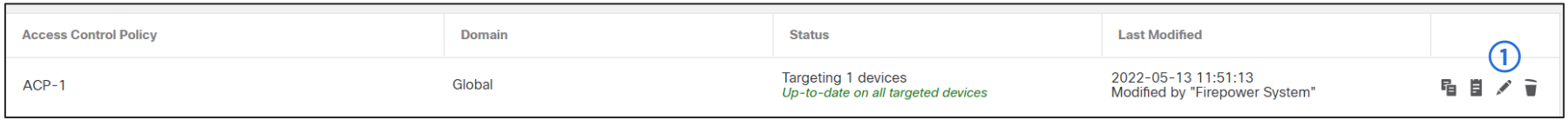
項目	説明	画面メニュー
Correlation Event	Correlation Policy のアラート	Alert ①Policies > Actions > Alerts Correlation Policy ①Policies > Correlation ②アラート有効にするルールの含まれる Correlation Policy を選択 ③アラート有効にする Correlation Rule を選択 ④使用する Responses を Alert 一覧より指定
Network Malware Evert	Network AMPのアラート	Alert ①Policies > Actions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

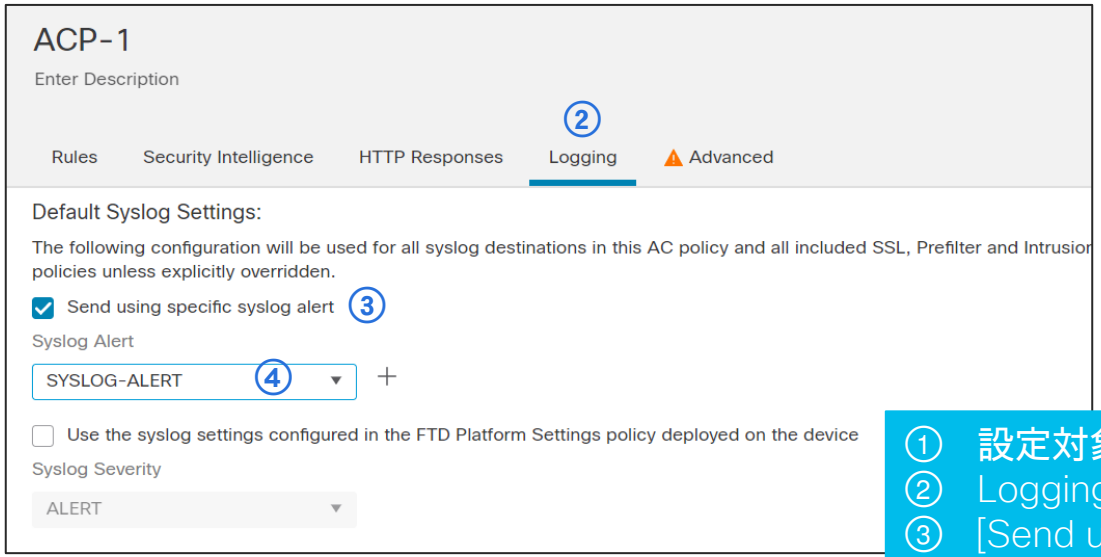
参考: Audit Log Event 設定画面



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

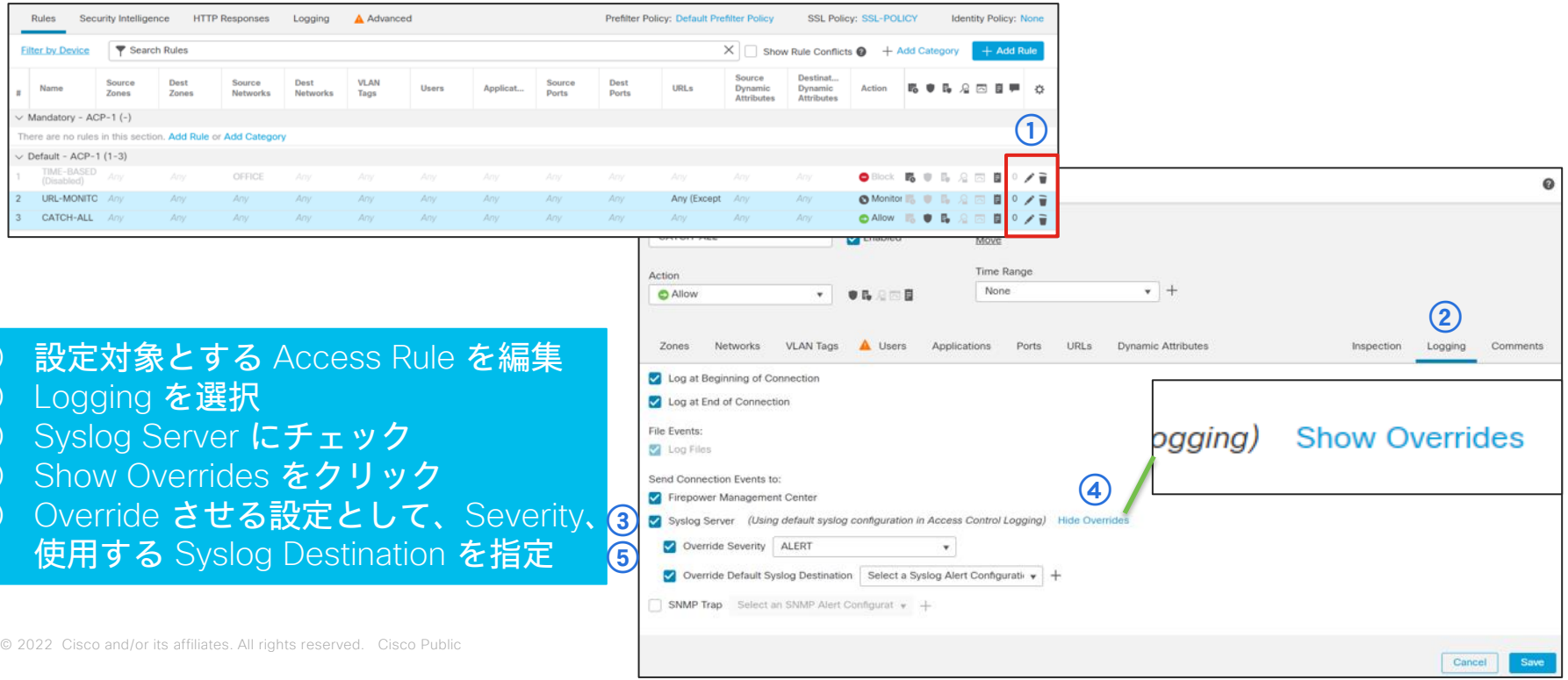
参考: Connection Event 設定画面





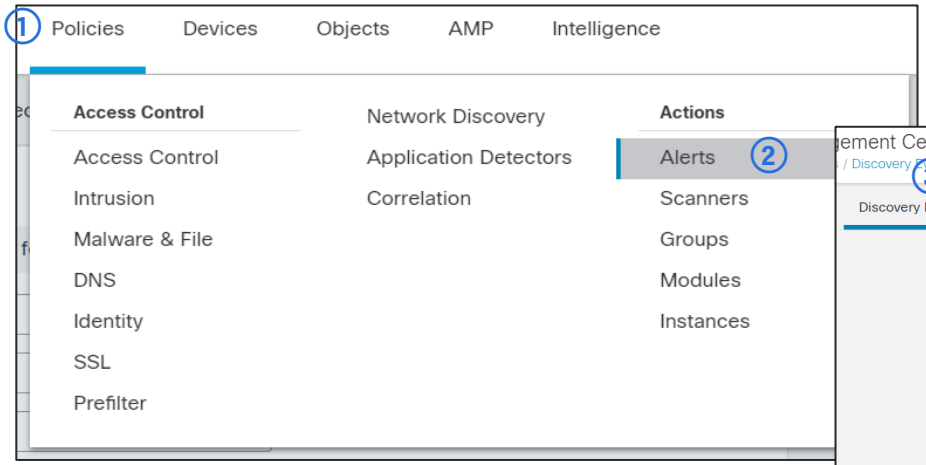
① 設定対象とする Access policy を開く
② Logging タブを選択
③ [Send using specific syslog alert] にチェック
④ 使用する Syslog Alert をプルダウンより選択

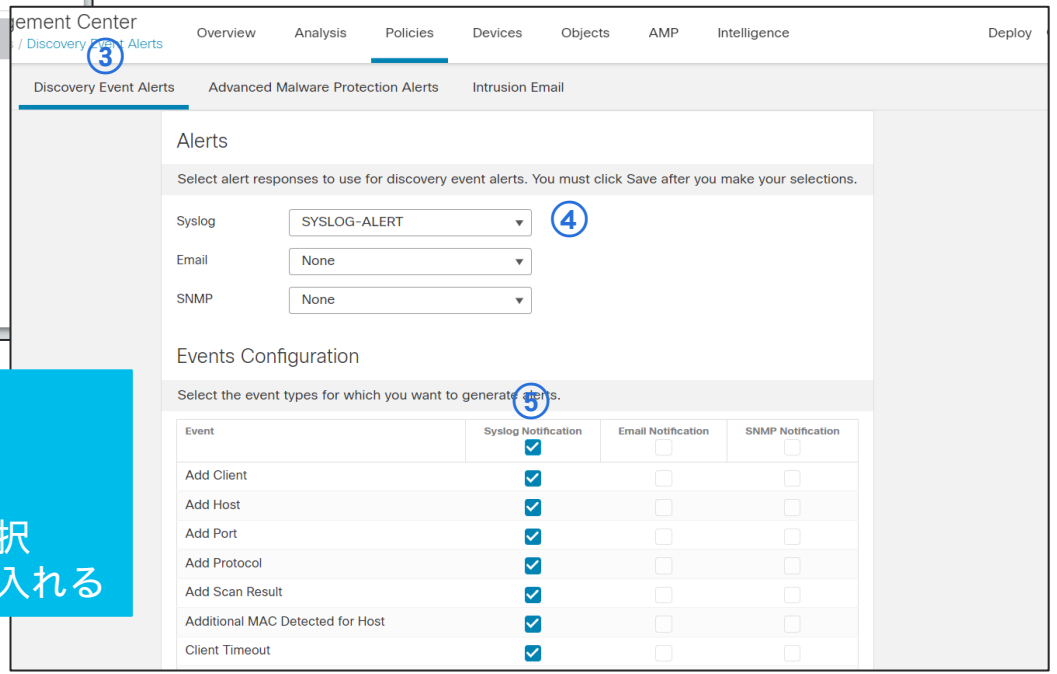
参考: Connection Event 設定画面 (続き)



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

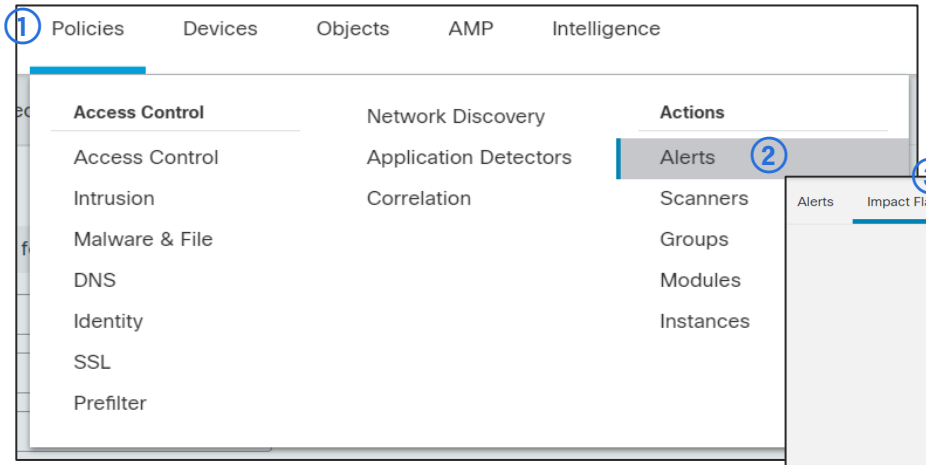
参考: Discovery Event 設定画面

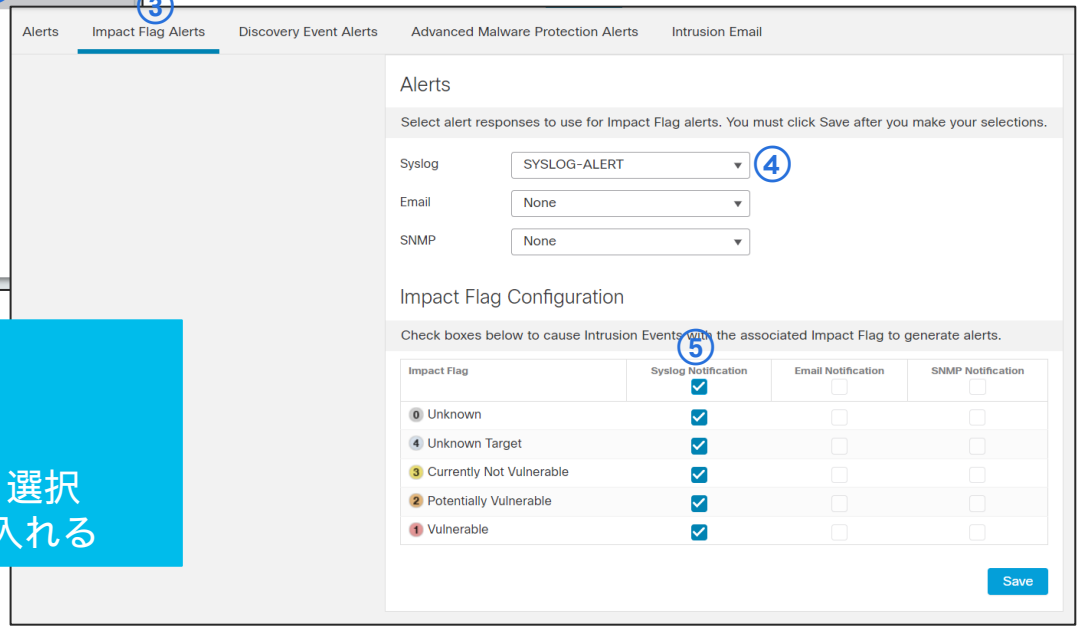




① Policies を選択
② Actions 下の Alerts を選択
③ Discovery Event Alerts を選択
④ 使用する Syslog Alert をプルダウンより選択
⑤ アラート対象とするイベントへチェックを入れる

参考: Impact Flag 設定画面





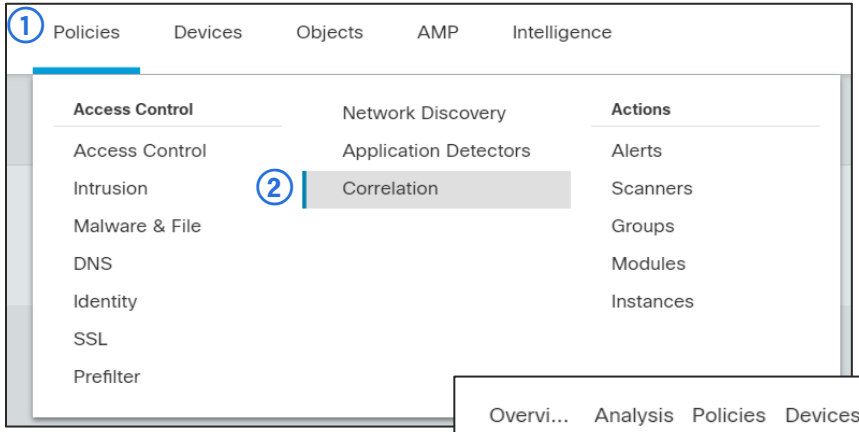
① Policies を選択
② Actions 下の Alerts を選択
③ Impact Flag Alerts を選択
④ 使用する Syslog Alert をプルダウンより選択
⑤ アラート対象とする Flag へチェックを入れる

参考: Intrusion Event 設定画面

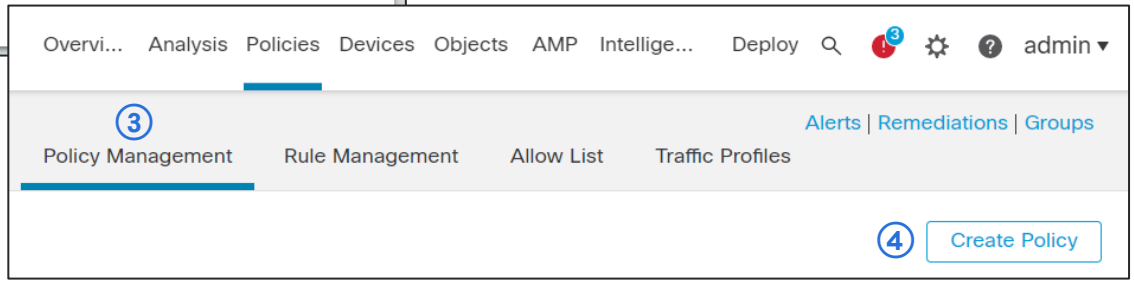
① 設定対象とする Access policy を開く
② Logging タブを選択
③ IPS Settings 以下にある [Send using specific syslog alert] にチェック
④ Show Overrides をクリックし展開
⑤ Overrides Severity 、Overrides Syslog Destination を必要に応じて選択

参考: Correlation Event 設定画面

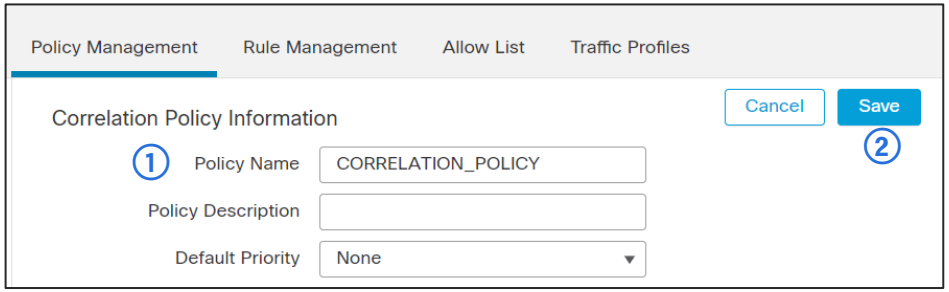
- Correlation Policy を設定することで、詳細な条件に基づくアラート通知が可能



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

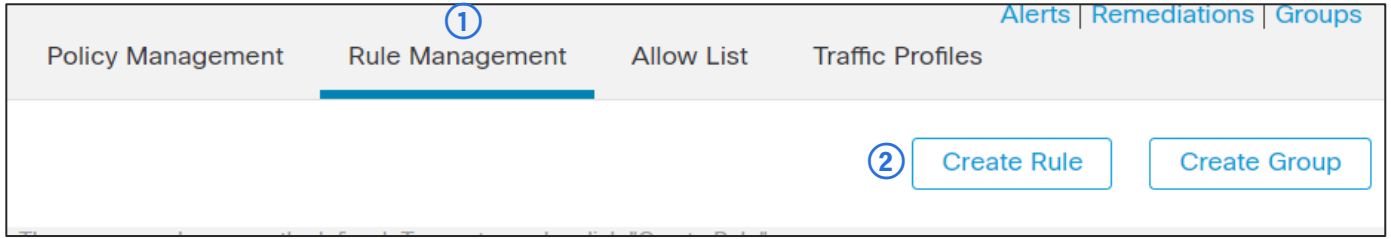


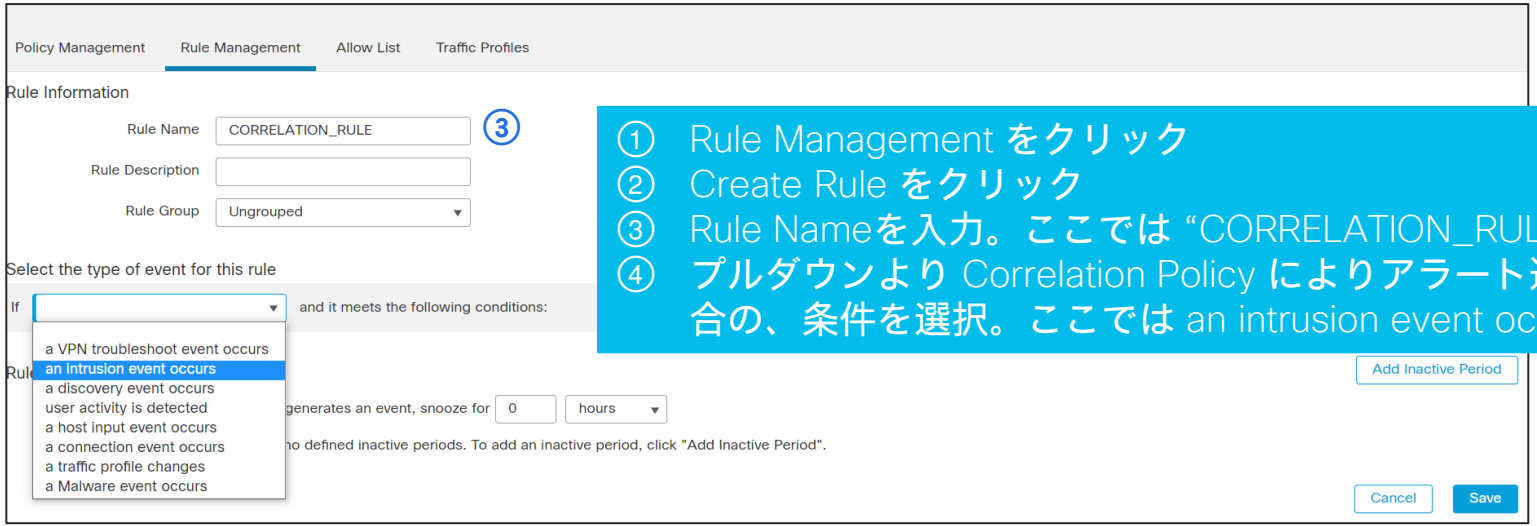
参考: Correlation Event 設定画面 (続き)



① Policy Name を入力
② Save をクリックし、一旦保存

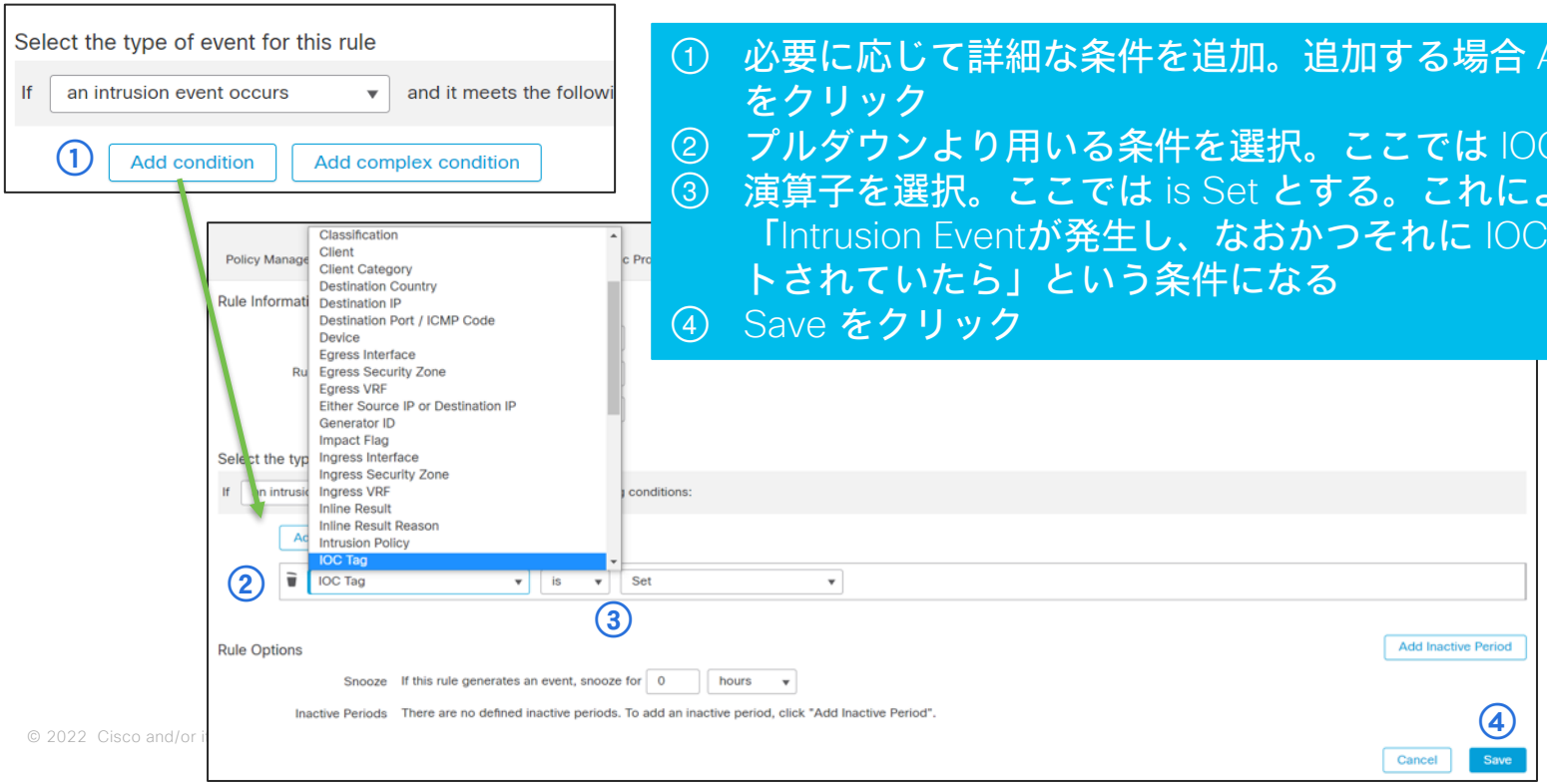
参考: Correlation Event 設定画面 (続き)





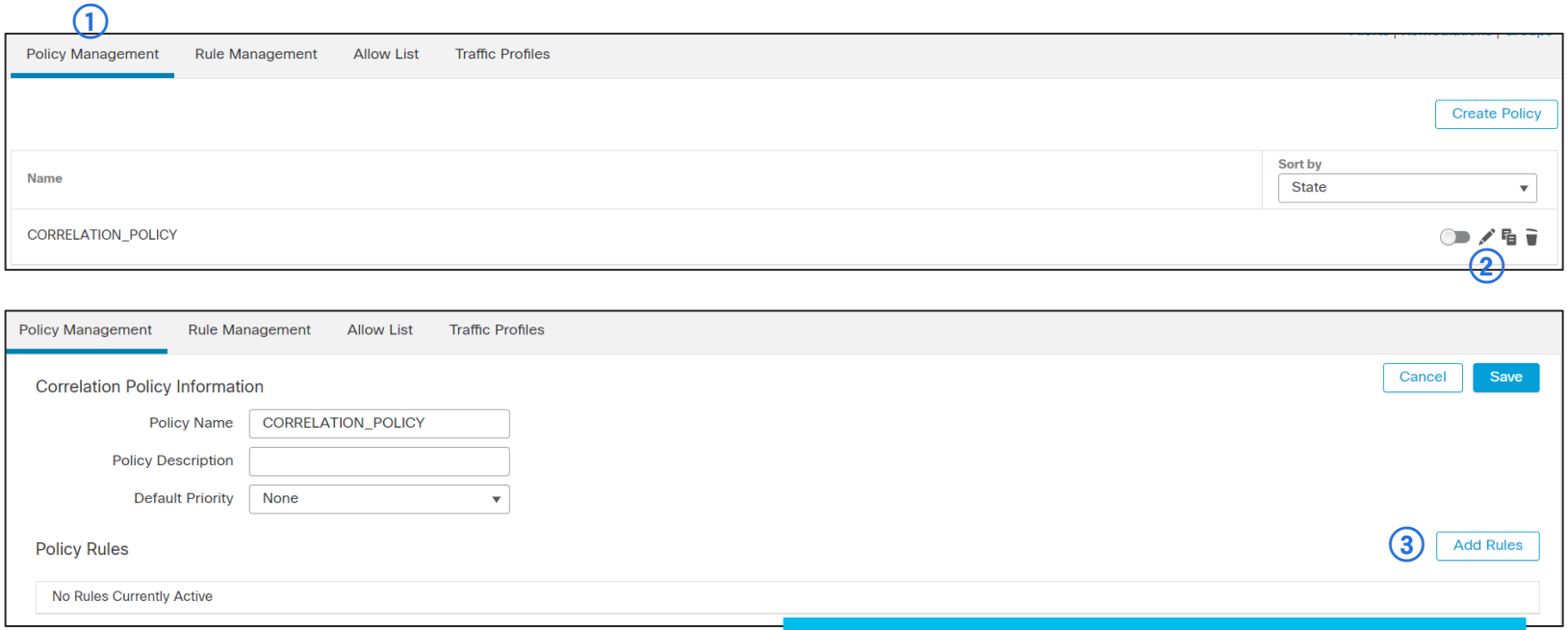
① Rule Management をクリック
② Create Rule をクリック
③ Rule Nameを入力。ここでは “CORRELATION_RULE” とする
④ プルダウンより Correlation Policy によりアラート通知させる場合の、条件を選択。ここでは an intrusion event occurs とする

参考: Correlation Event 設定画面 (続き)



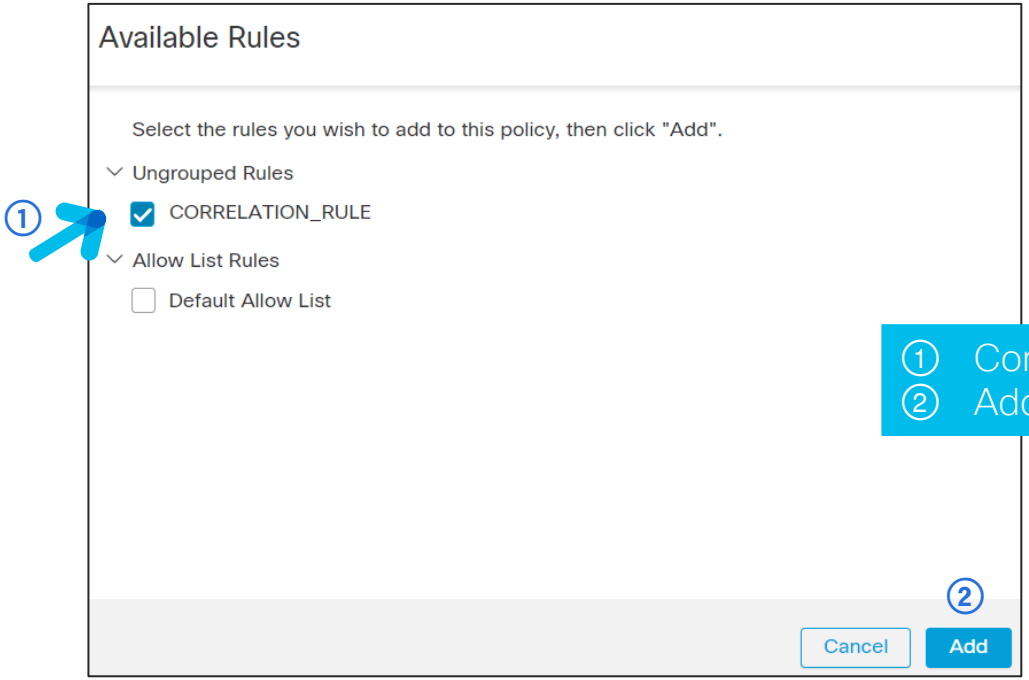
① 必要に応じて詳細な条件を追加。追加する場合 Add condition をクリック
② プルダウンより用いる条件を選択。ここでは IOC Tag とする
③ 演算子を選択。ここでは is Set とする。これにより「Intrusion Eventが発生し、なおかつそれに IOC Tag がセットされていたら」という条件になる
④ Save をクリック

参考: Correlation Event 設定画面 (続き)



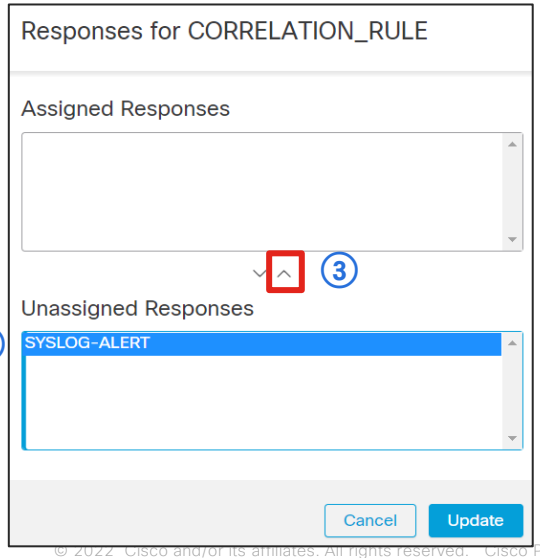
① Policy Management を選択
② 鉛筆マークをクリック
③ Add Rule をクリック

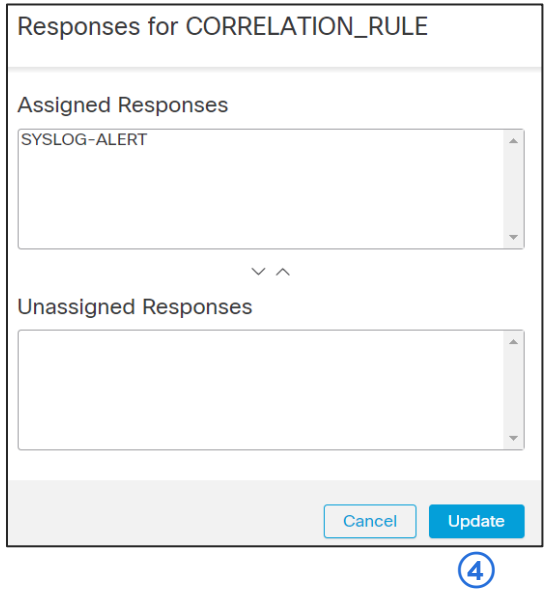
参考: Correlation Event 設定画面 (続き)



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

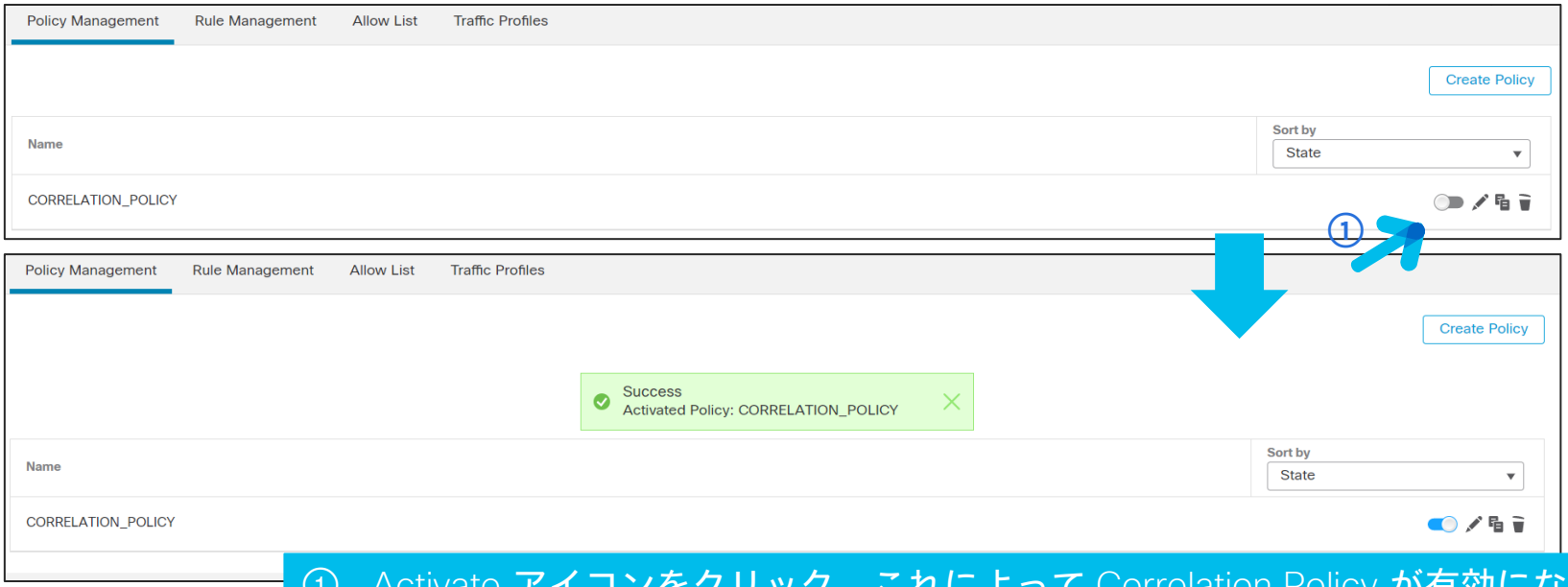
参考: Correlation Event 設定画面 (続き)





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

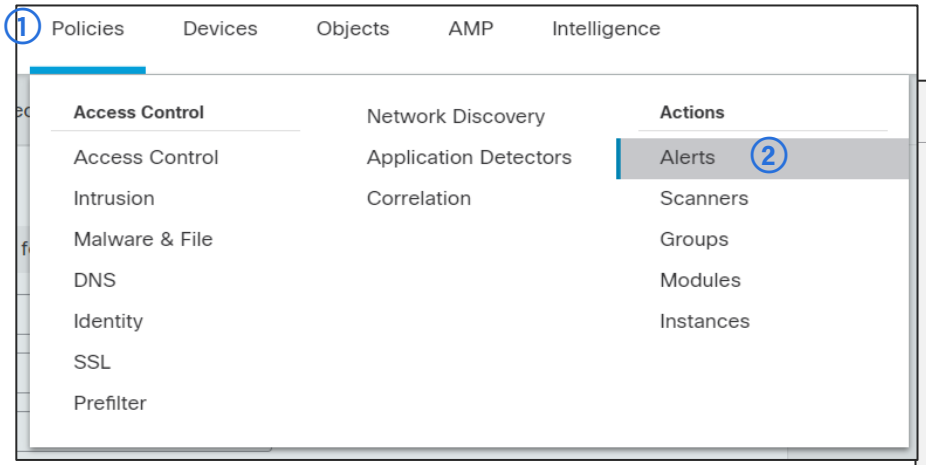
参考: Correlation Event 設定画面 (続き)

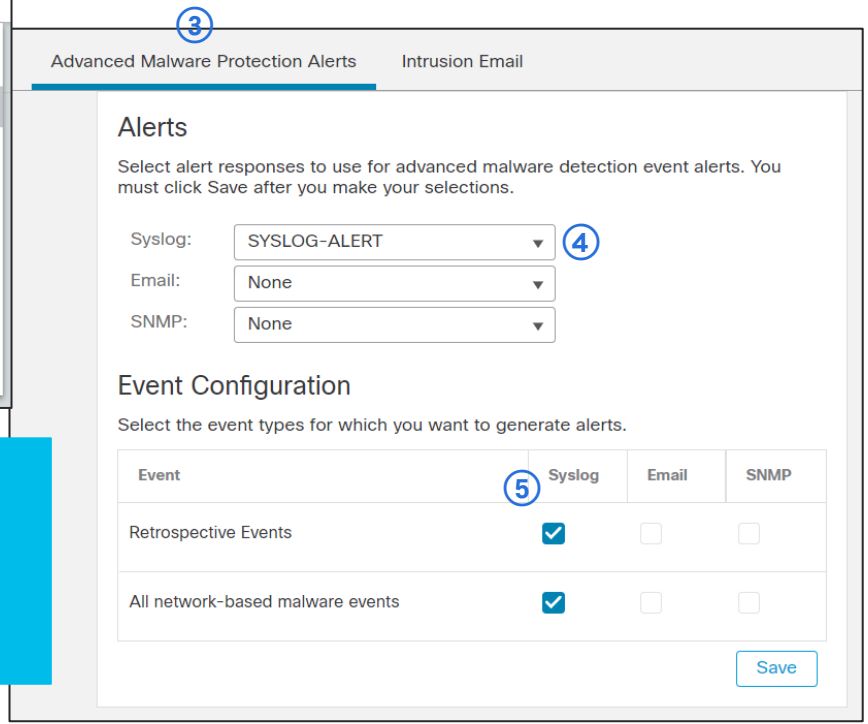


① Activate アイコンをクリック。これによって Correlation Policy が有効になり、Correlation Rule の条件を満たすイベントが発生した場合にアラートが送信される

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

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

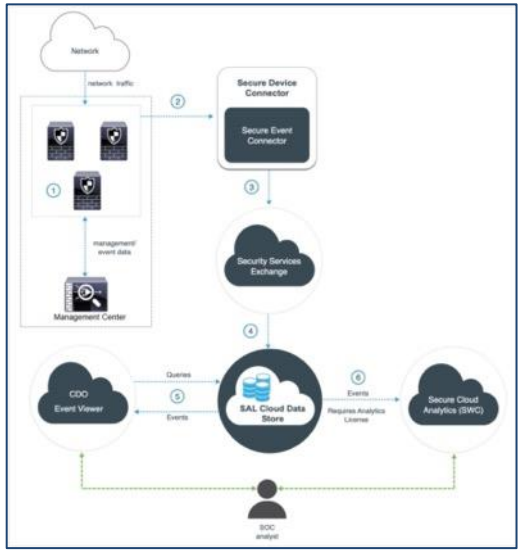
- さまざまな Cisco デバイスからのログを集約して分析することができるクラウドサービス
- セキュリティ分析とログは利用者の裁量で拡張できるため、長期間の保存が可能
- SAL SaaS に出力したログ情報は、CDO (Cisco Defense Orchestrator) もしくは SCA (Secure Cloud Analytics) で分析が可能
- 本セットアップガイドでは FMC と SAL SaaS の連携部分のみにフォーカスし、CDO と SCA の連携部分は解説の対象外とする
- SAL には On Premise 版の製品もあるが、本セットアップガイドでは SAL SaaS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

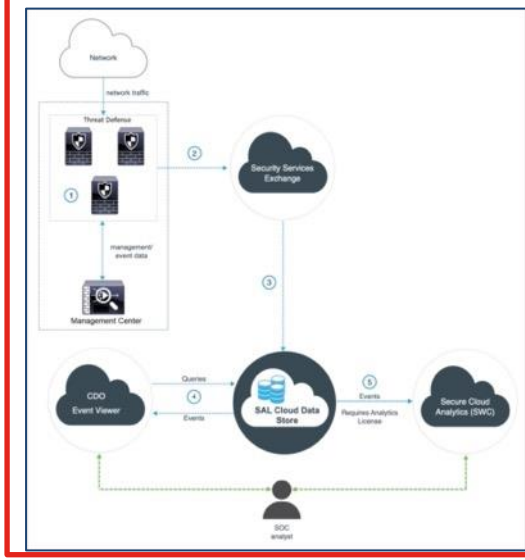
- FMC と SAL の接続方法は Syslog Connection と Direct Connection の 2パターン存在するが、本セットアップガイドでは Direct Connection にフォーカスして解説する。

本ガイドの解説対象

Syslog Connection

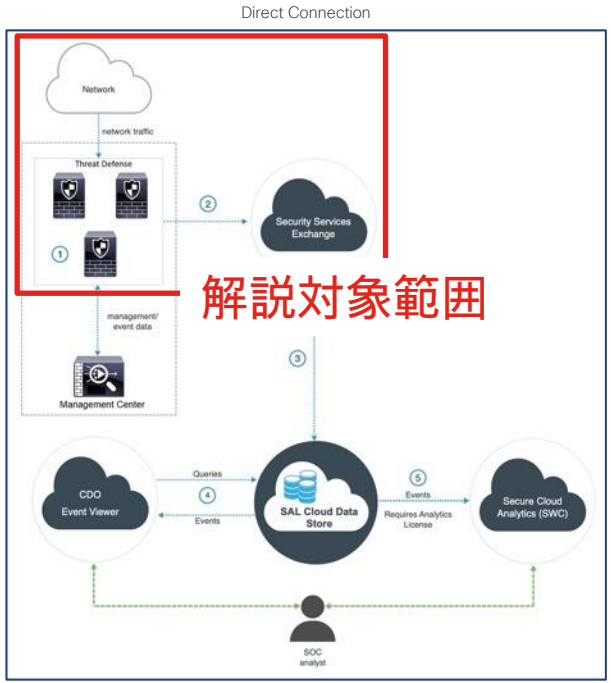


Direct Connection



本セットアップガイドでのシナリオ

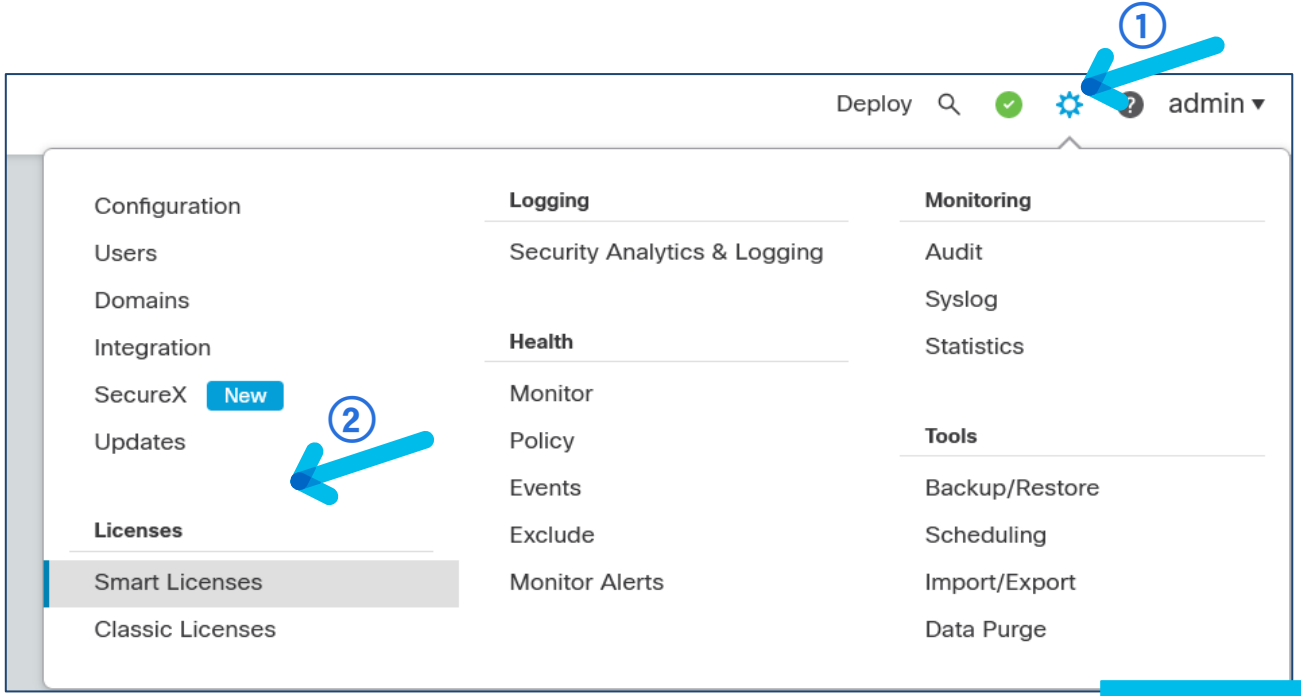
- Direct Connection パターンにおいて Security Services Exchange (SSE) との接続までの手順を解説する。



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

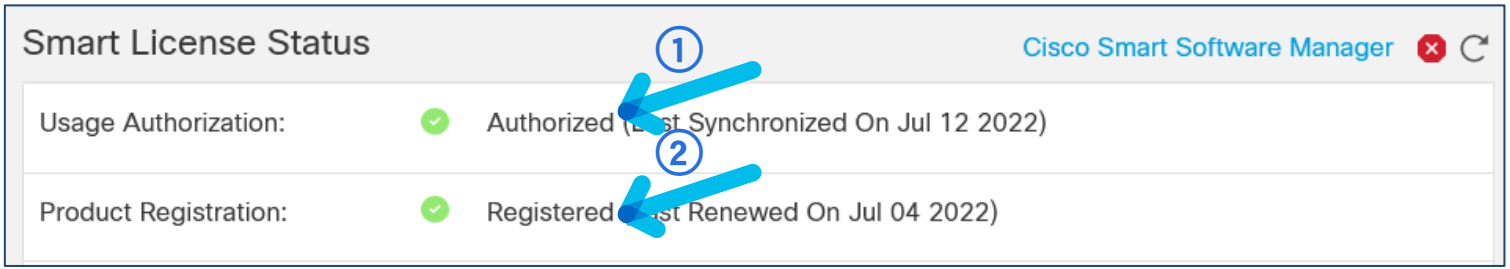


SSE への接続には FMC に登録している Smart Account / Virtual Account が必要

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

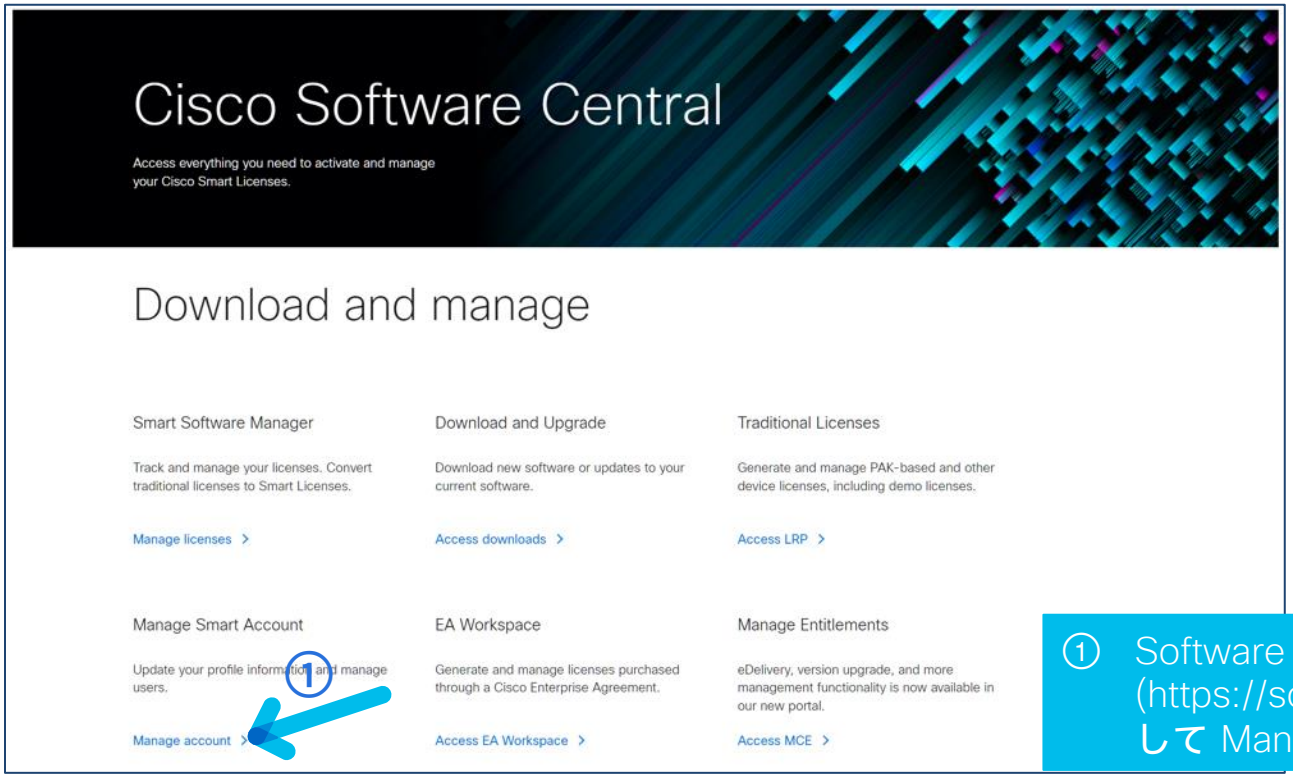
① FMC の System を選択
② Smart Licenses を選択

ステップ1：Smart License 状態確認



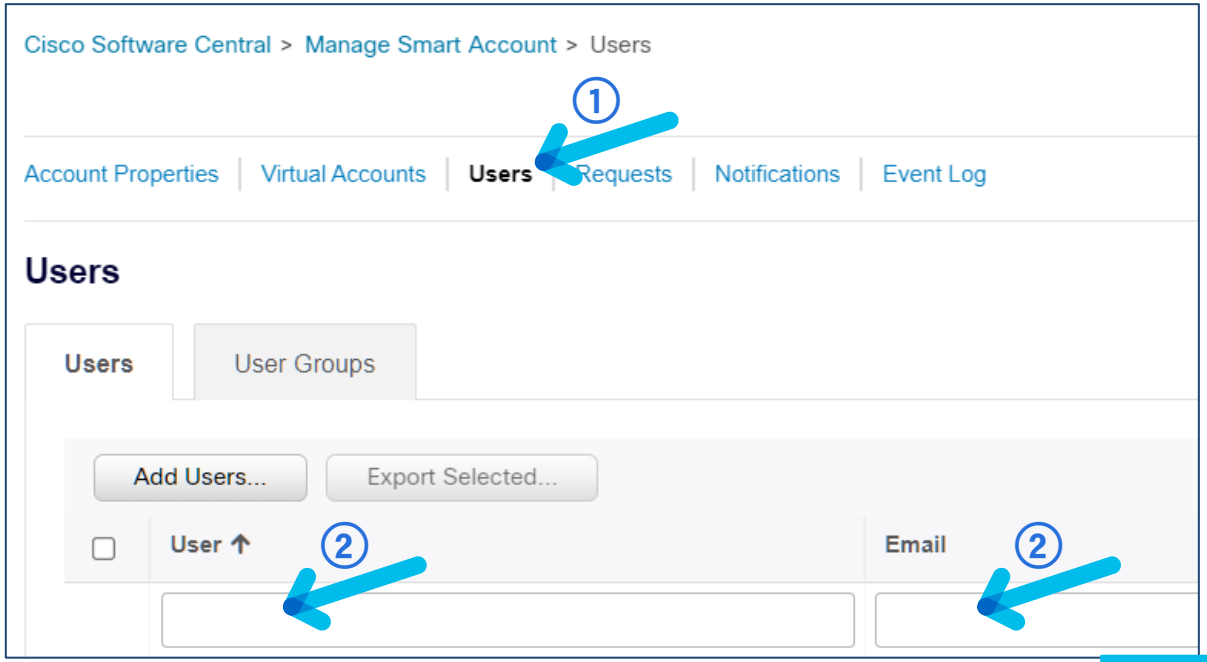
① Usage Authorization Status が Authorized であることを確認
② Product Registration Status が Registered であることを確認

ステップ2：Smart Account 権限確認



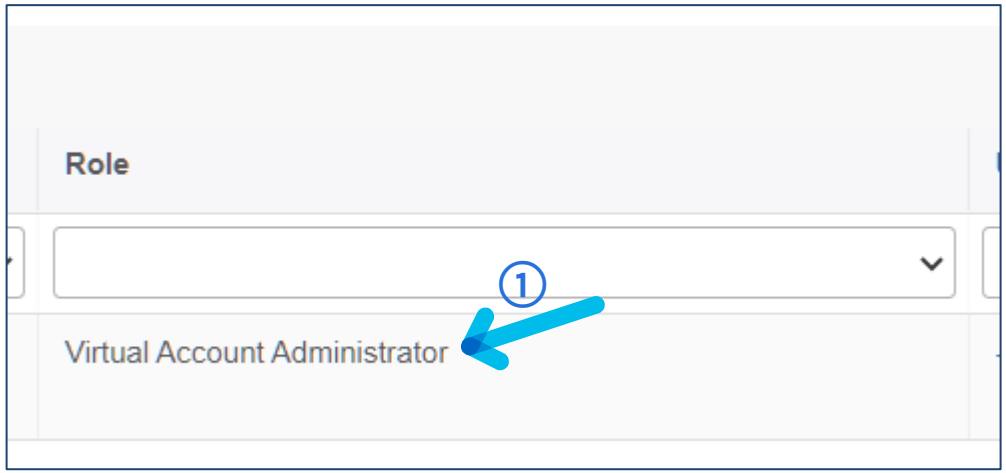
① Software Central (https://software.cisco.com) にアクセスして Manage Smart Account を選択

ステップ2：Smart Account 権限確認



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

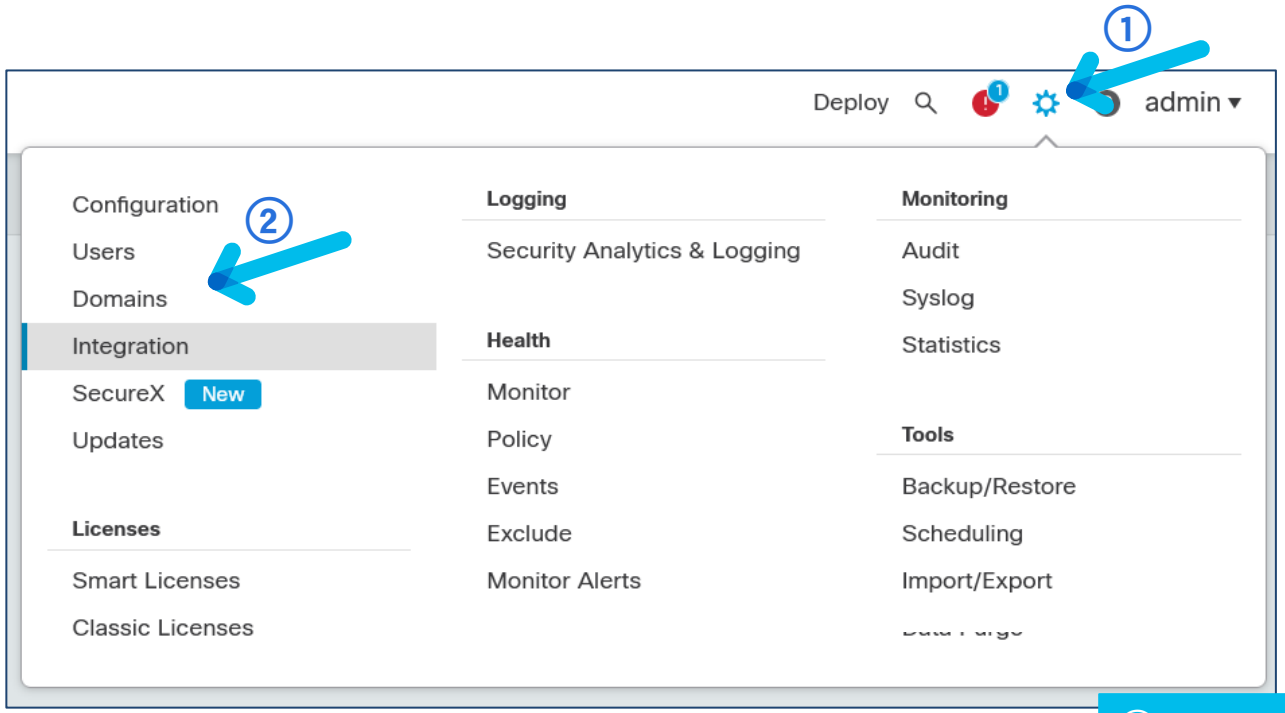
ステップ2：Smart Account 権限確認



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

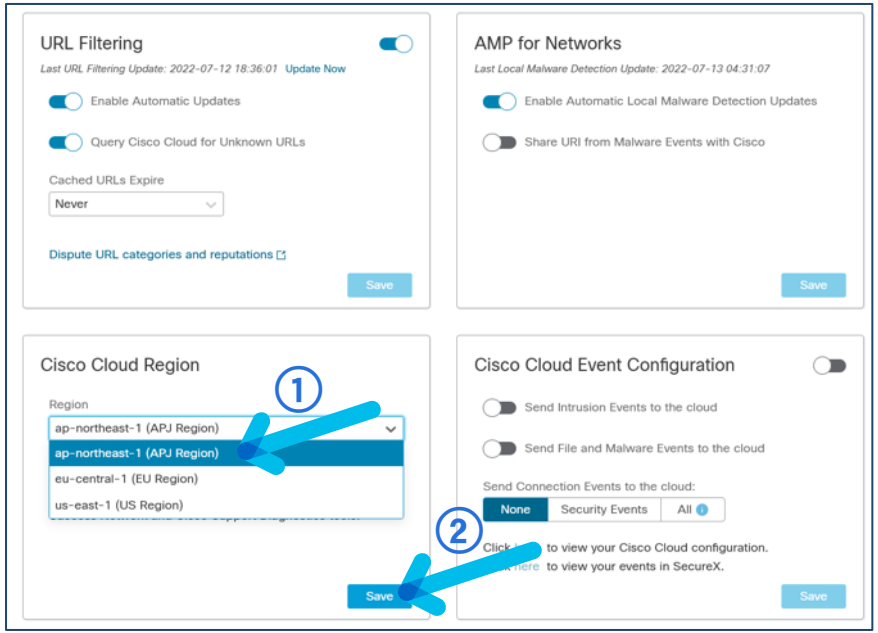
① 表示された User の Role を確認して以下のいずれかの権限を持っていることを確認
Admin
Access Admin
Network Admin
Security Approver

ステップ3：FMC から SSE に出力する Event の選択



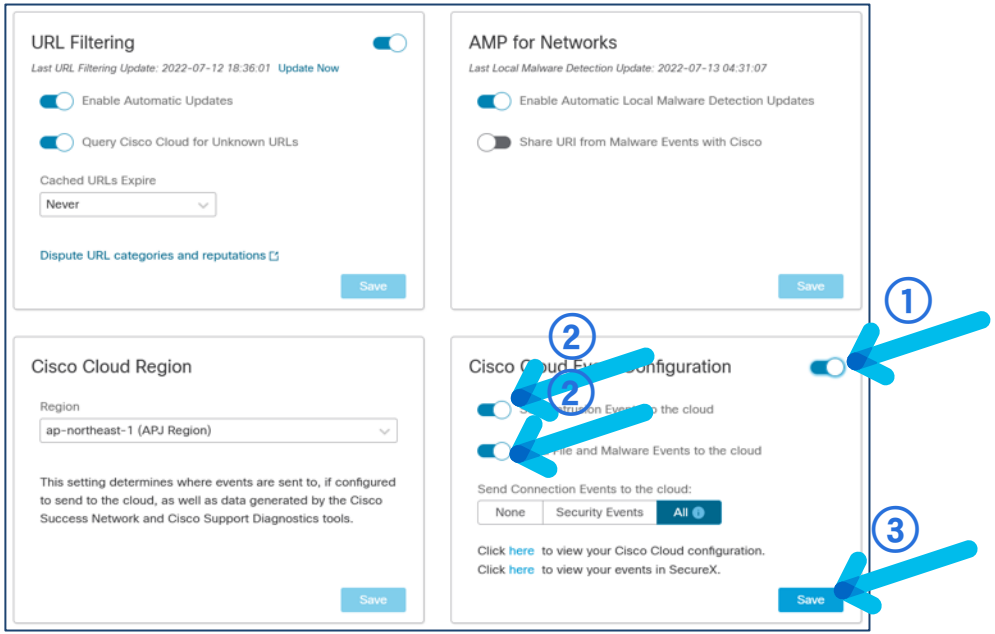
① FMC の System を選択
② Integration を選択

ステップ3：FMC から SSE に出力する Event の選択



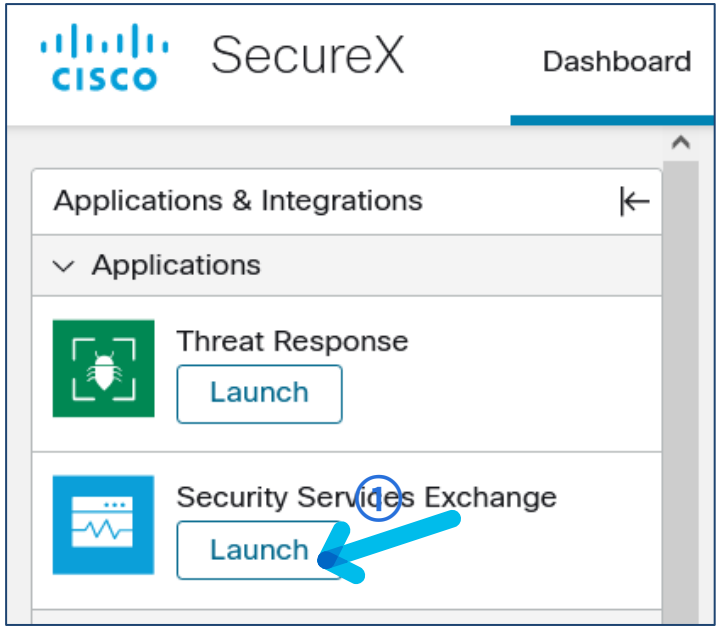
① Cisco Cloud Region から APJ Region を選択
② Save を選択

ステップ3：FMC から SSE に出力する Event の選択



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

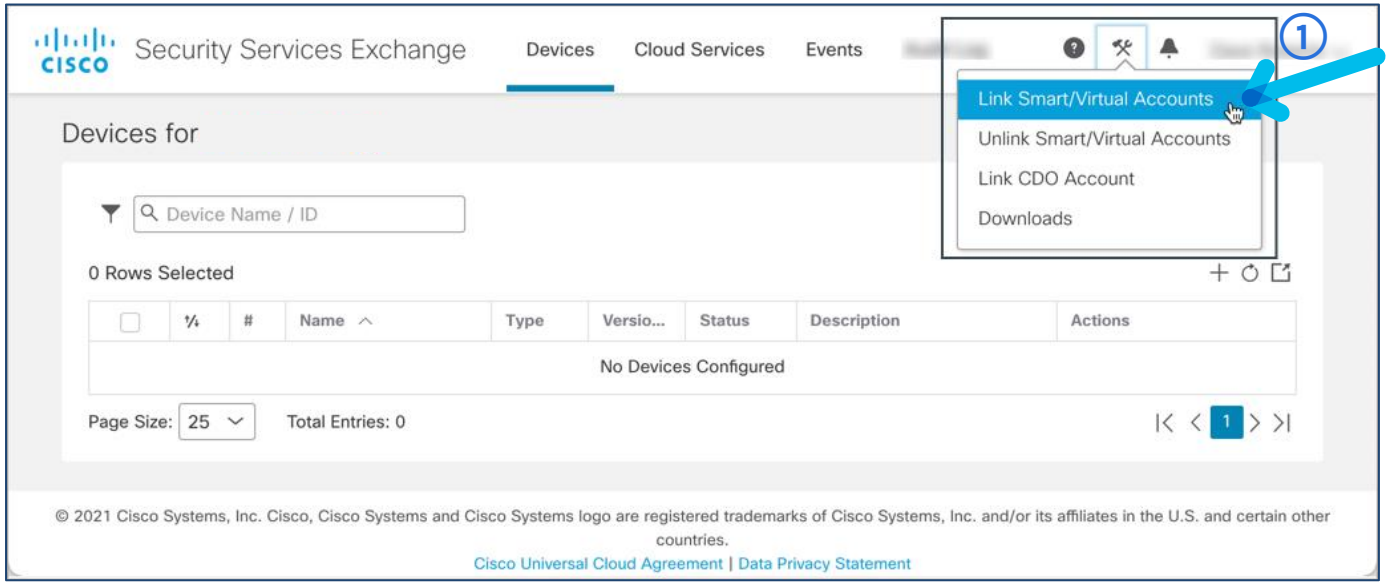
ステップ4：SSE と Smart Account との同期



① SecureX Dashboard*1 で SSE の Launch を選択

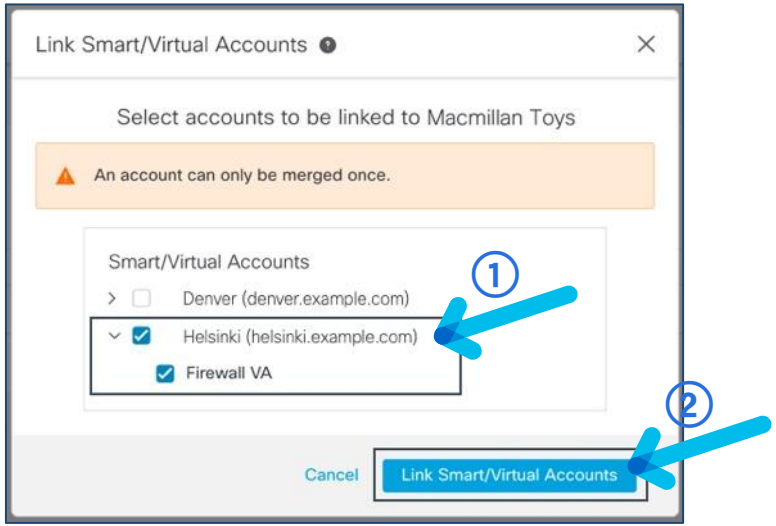
*1 FMC と同期する SecureX Accounts にログインすること

ステップ4：SSE と Smart Account との同期



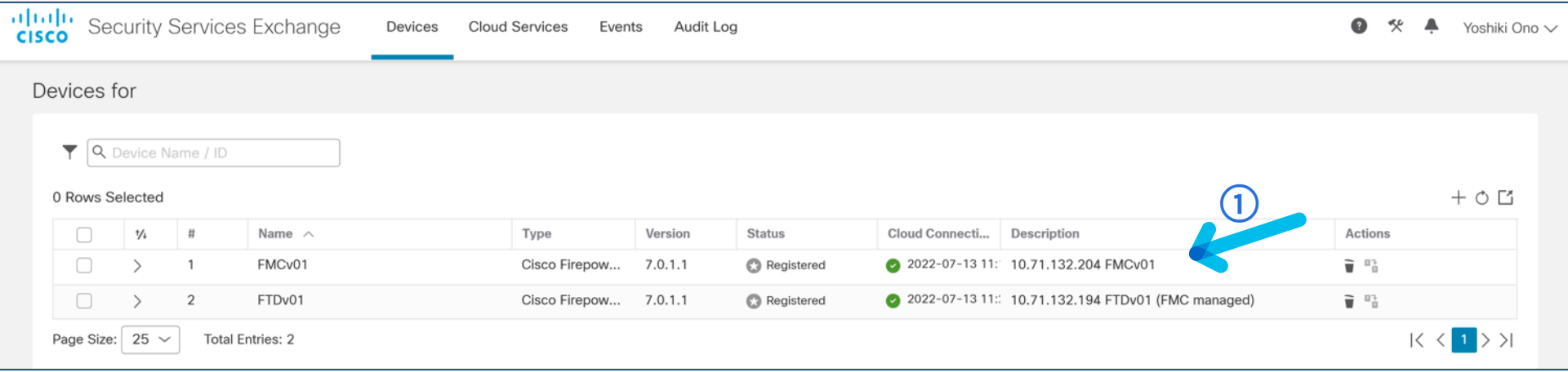
① Link Smart/Virtual Accounts を選択

ステップ4：SSE と Smart Account との同期



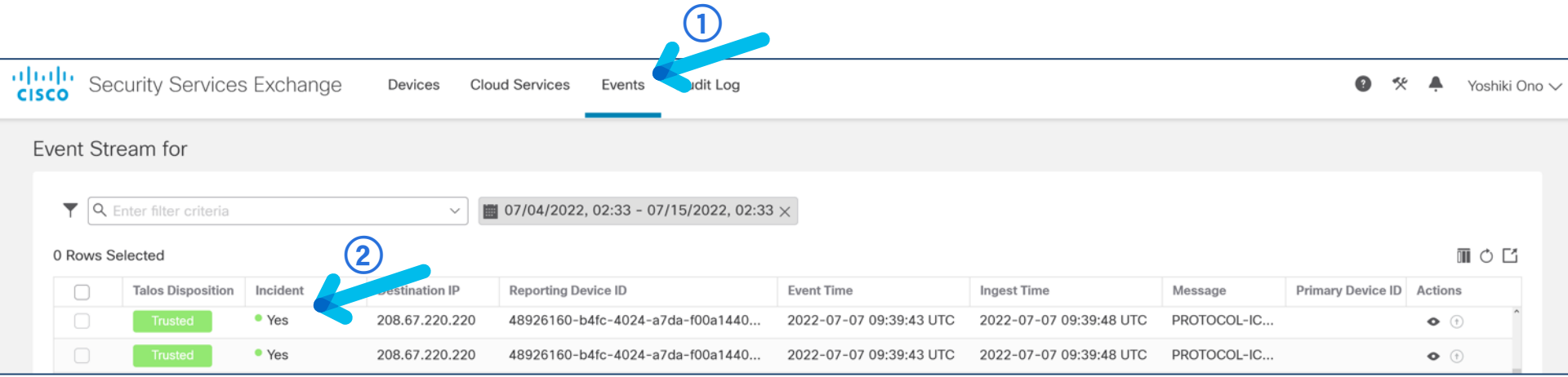
① 同期する Smart Accounts を選択
② Link Smart/Virtual Accounts を選択

ステップ4：SSE と Smart Account との同期



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



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

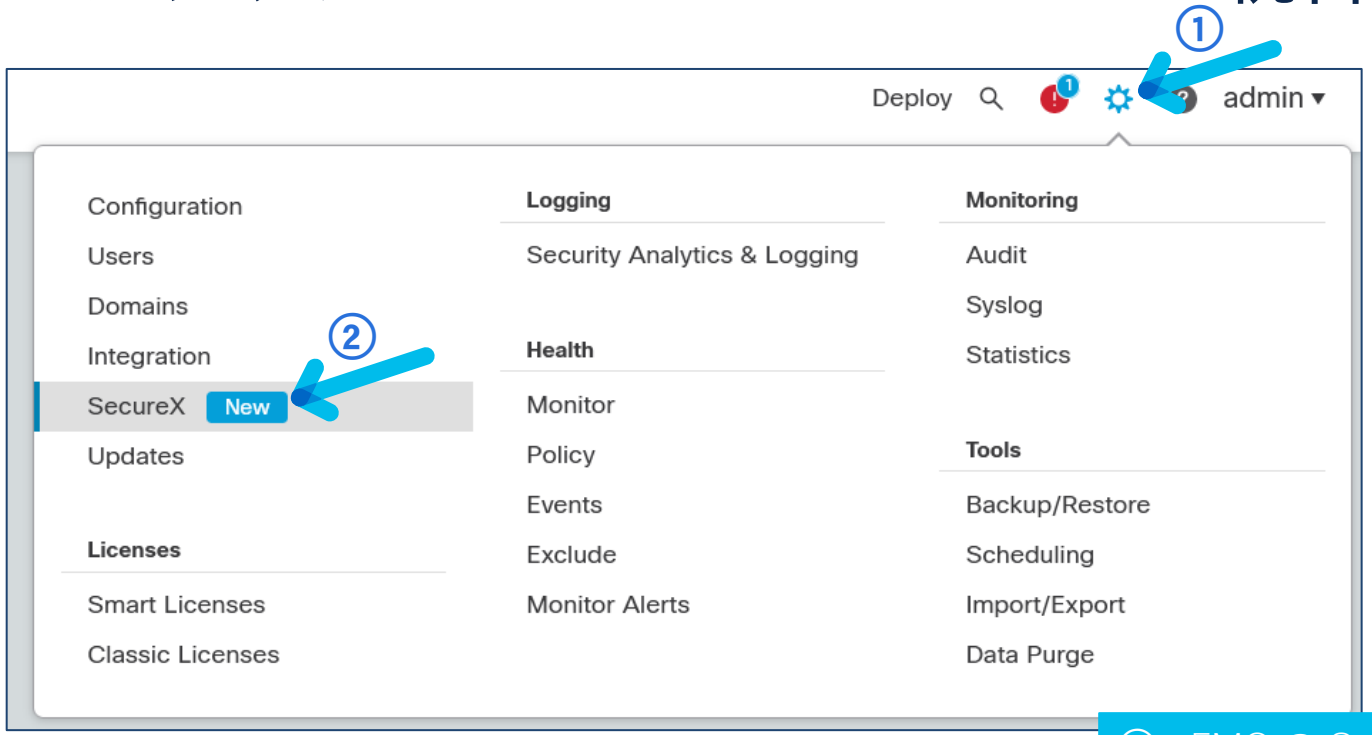
1. Smart License 状態確認
2. Smart Account 権限確認
3. FMC から SSEに出力する Event の選択
4. SSE と Smart Account との同期

---

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

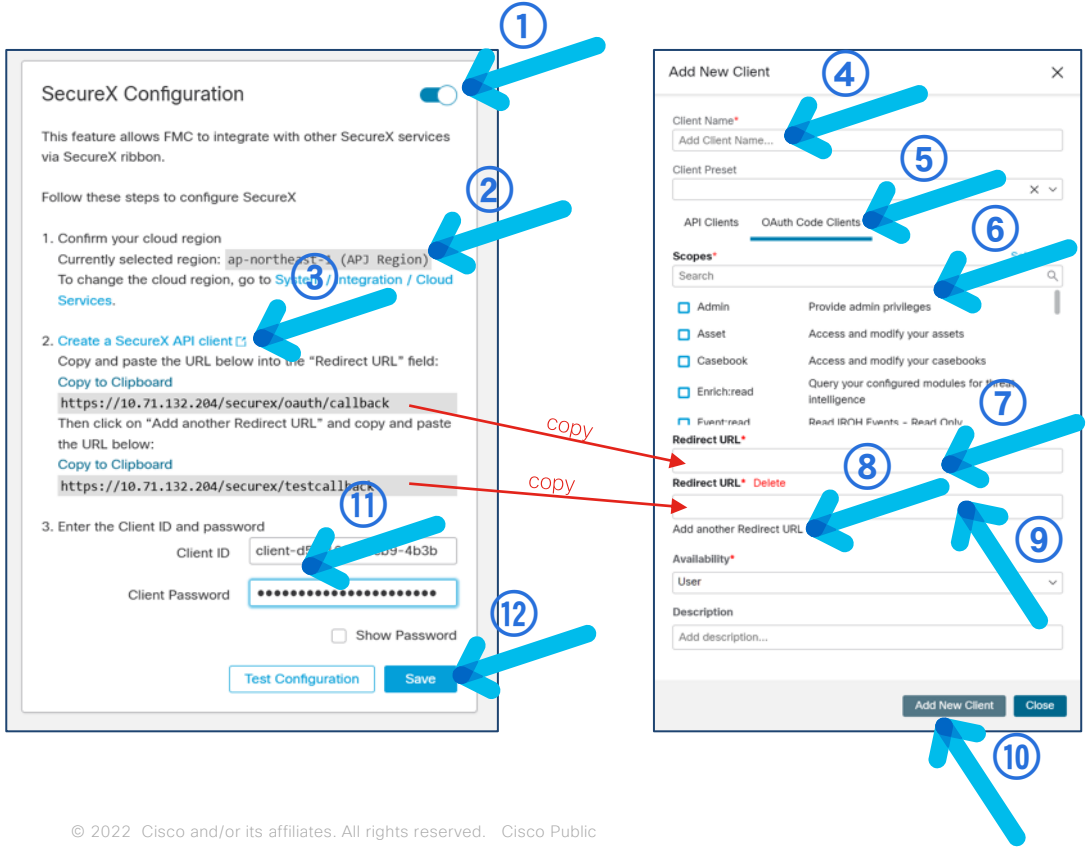
ここまで SSE 連携編のステップ4までと全く同じ手順なので、説明は割愛

ステップ5：FMC と SecureX との統合



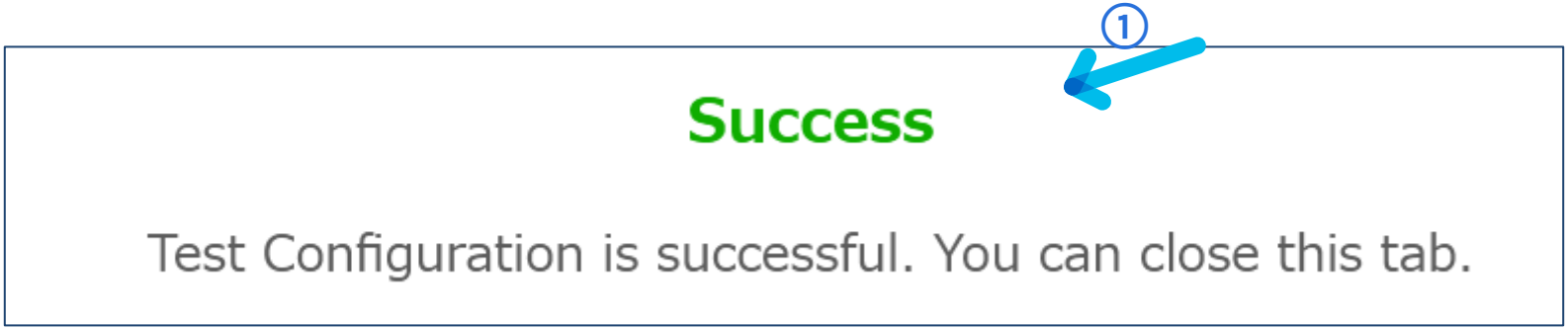
① FMC の System を選択
② SecureX を選択

ステップ5：FMC と SecureX との統合



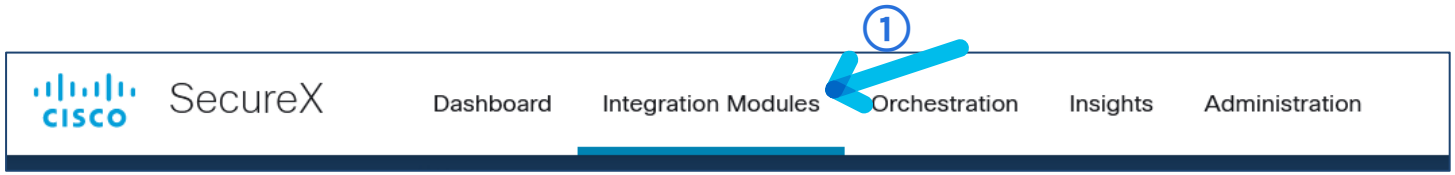
① SecureX Configuration を有効化
② APJ Region が選択されていることを確認
③ Create a SecureX API client を選択
④ 任意の API Client 名を入力
⑤ Oauth Code Clients を選択
⑥ Scopes は 事前設定されているためスキップ
⑦ Redirect URL に FMC からコピーした URL を入力
⑧ Add another Redirect URL を選択
⑨ もう一つの Redirect URL に FMC からコピーしたもう一つの URL を入力
⑩ Add New Client を選択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

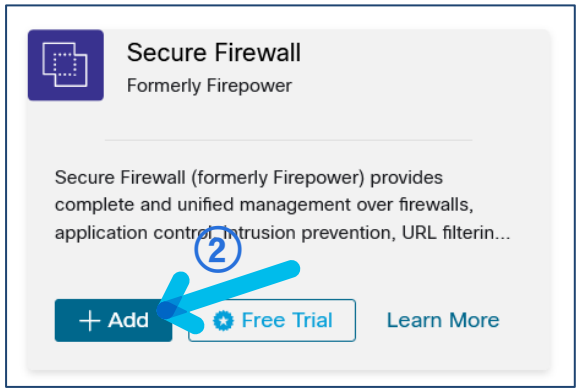
ステップ5：FMC と SecureX との統合



① Success と表示されることを確認

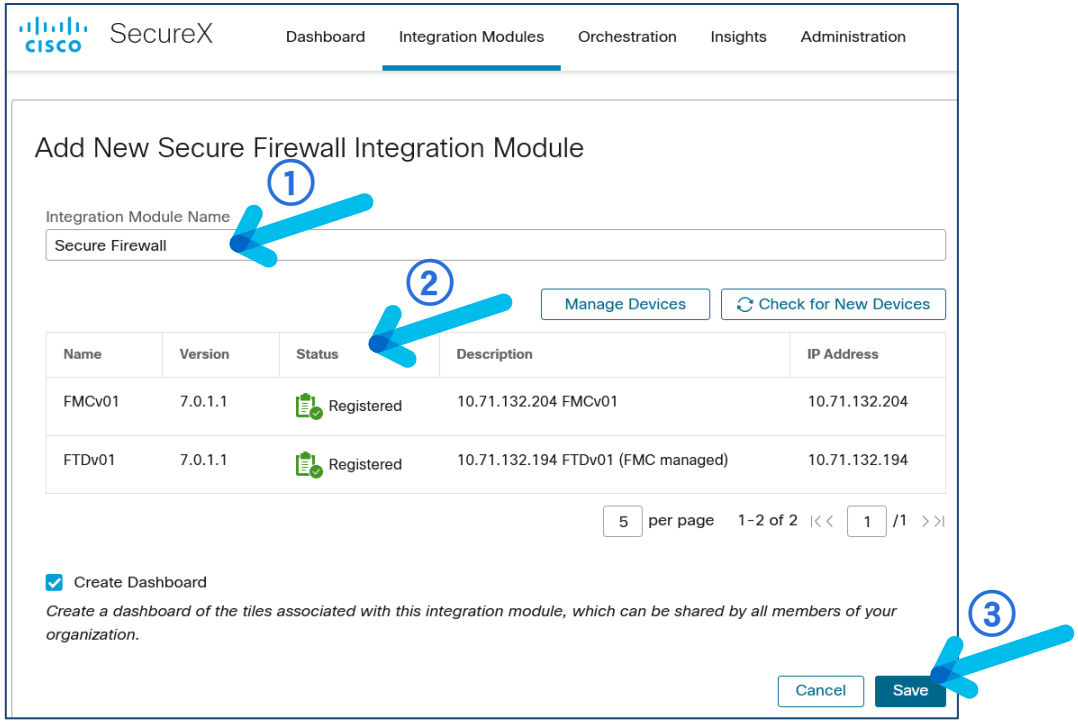
ステップ6：SecureX での Module 追加





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

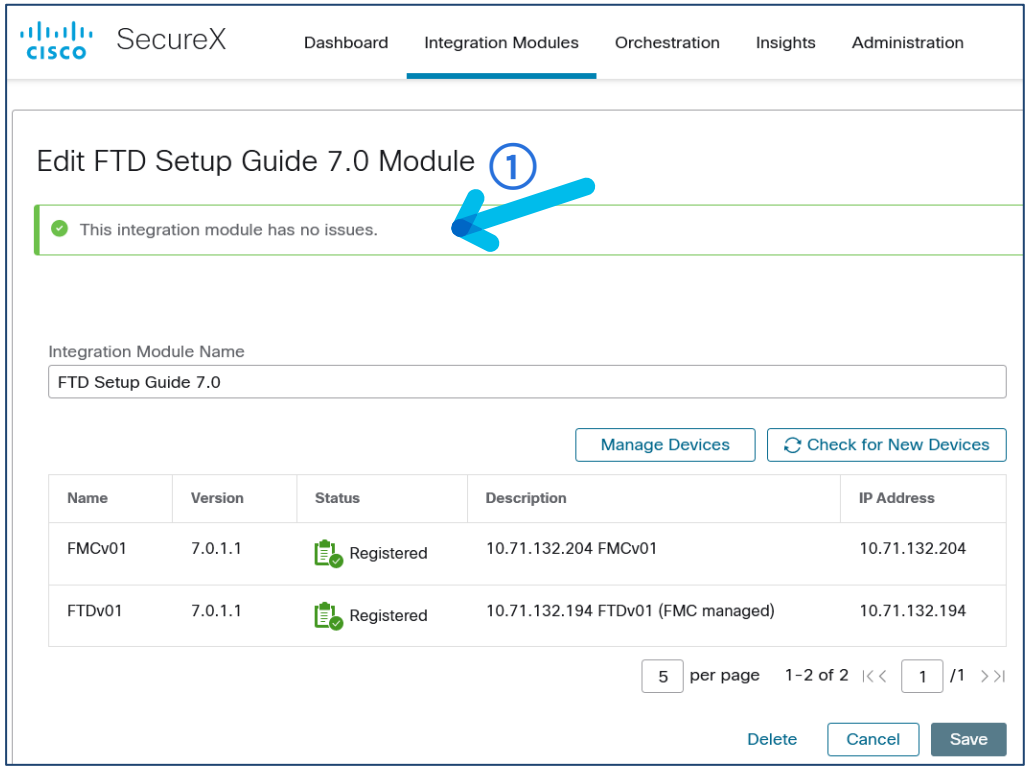
ステップ6：SecureX での Module 追加



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

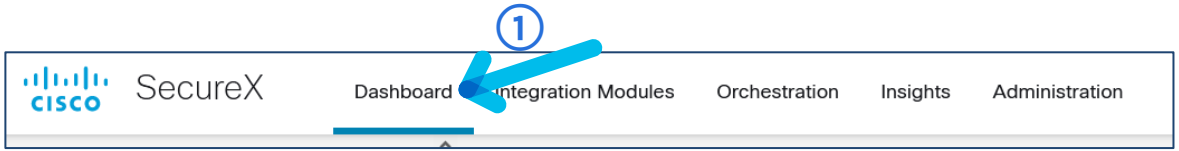
*1 登録できる Device は Administration > Devices で確認可能

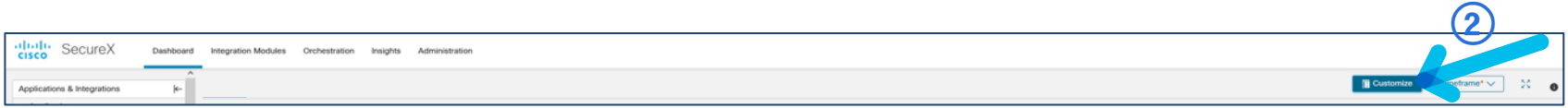
ステップ6：SecureX での Module 追加

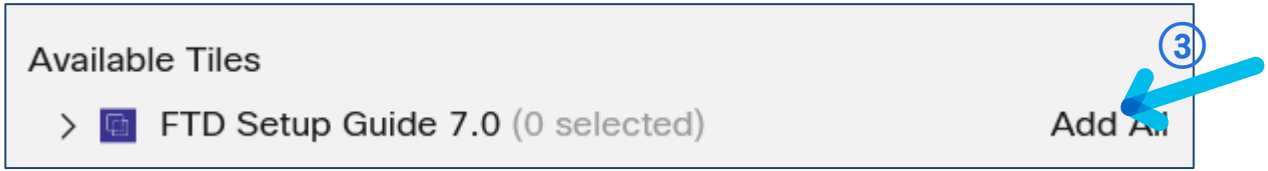


① 正常に登録できたことを確認

ステップ7：SecureX での Tile 追加

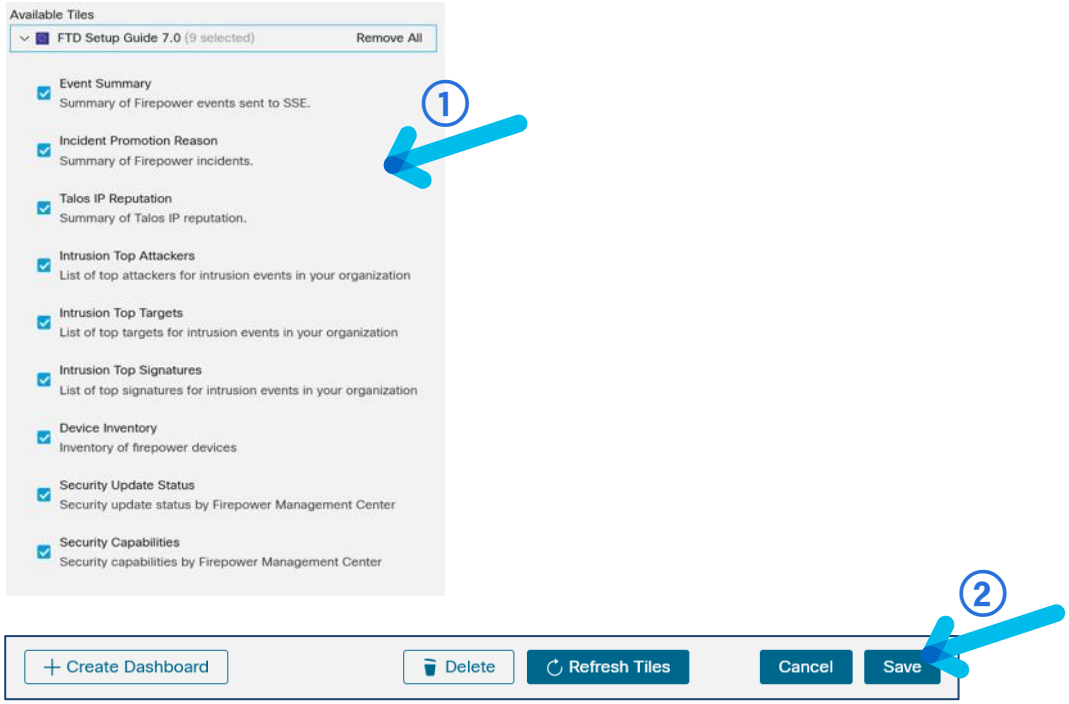






① SecureX の Dashboard を選択
② Customize を選択
③ ステップ5 で入力した Integration Module Name を確認し Add を選択

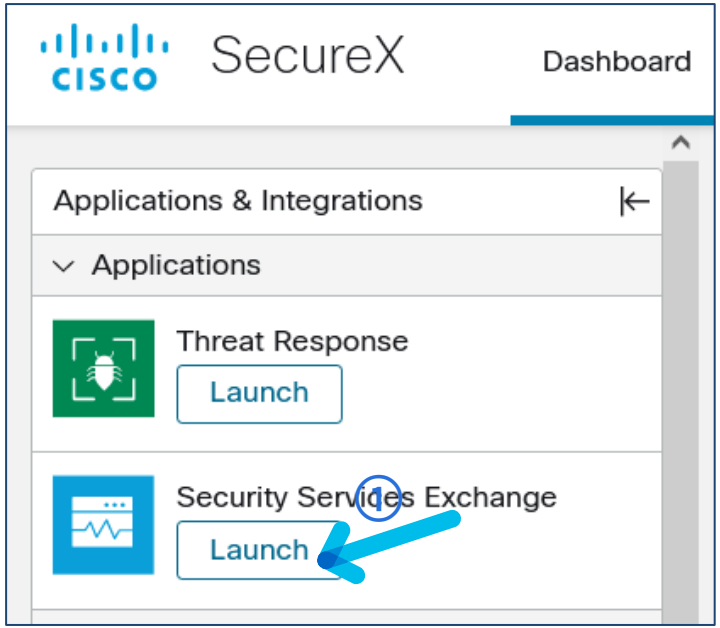
ステップ7：SecureX での Tile 追加



① 追加したい Tile を選択*1
② Save を選択

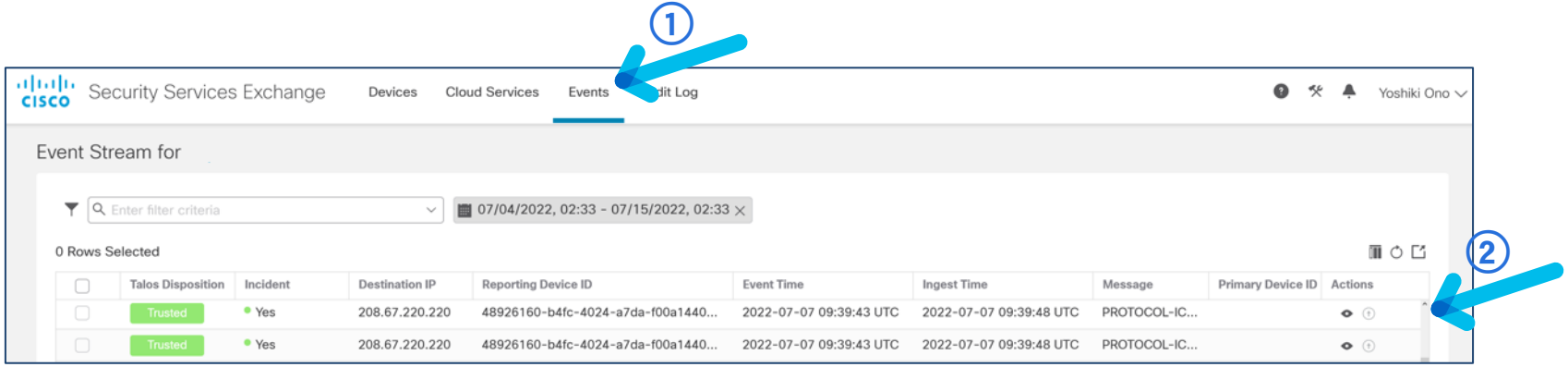
*1 必要に応じて Dashboard を 作成

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

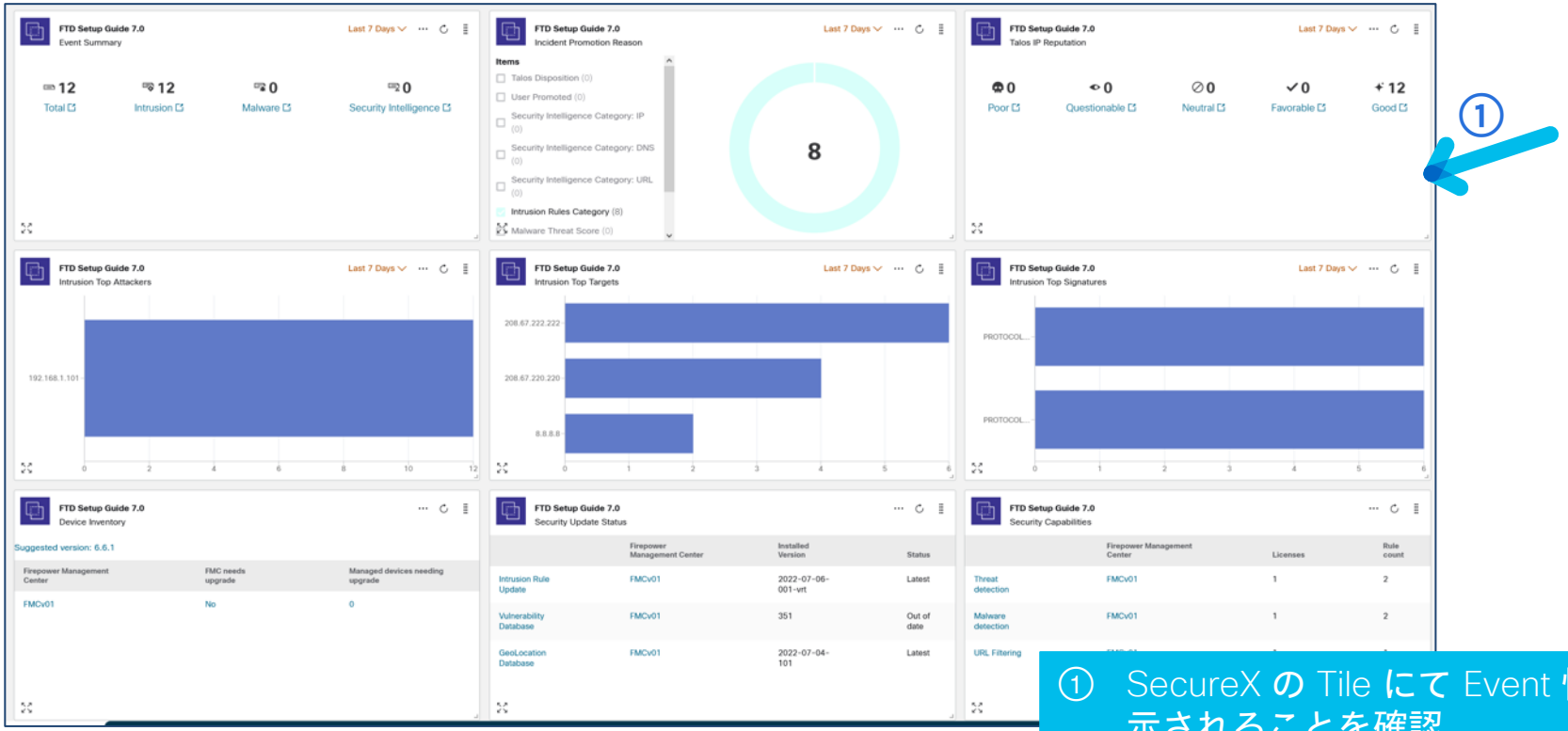


まずは SSE に Event が送られていることを確認

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

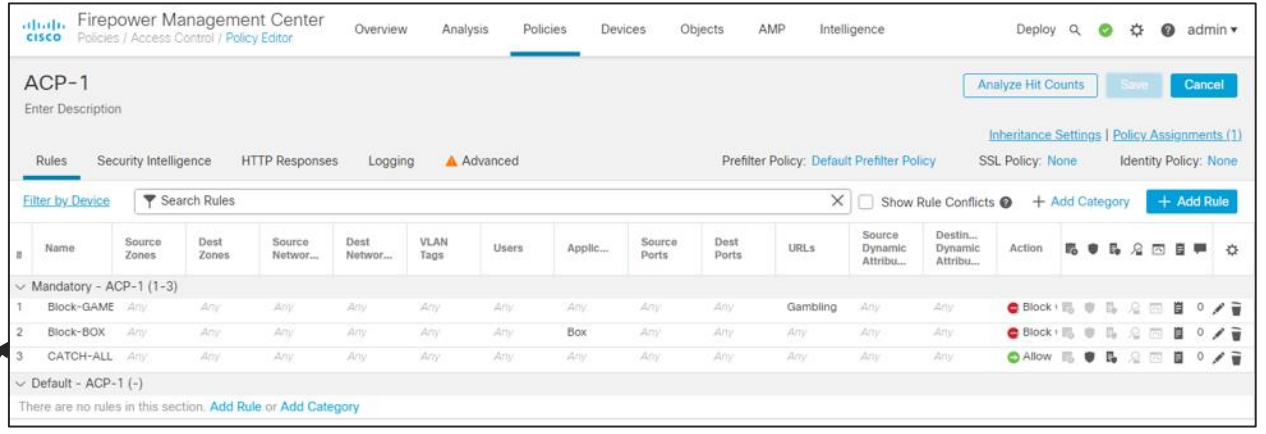
- FMC から FTD に設定変更内容をデプロイした後に、以前の FTD に戻す機能
- 間違った設定、ふさわしくない設定をデプロイしてしまった後に、まずは以前の正しく動いていた設定に戻すことができる
- 10世代前までの設定に戻すことが可能
- FMC から FTD へのデプロイ後に互い管理インターフェイス間の通信が途絶えてしまうような間違った設定により、FMC から FTD への設定変更ができないような場合には、FTD の CLI から1世代前の設定に戻すことが可能
  - (参考) バージョン 7.2 では SFTunnel の断を自動的に検知して自動的にロールバックすることも可能

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てデプロイしてしまったため、すぐにデプロイ前の FTD の設定に戻したい



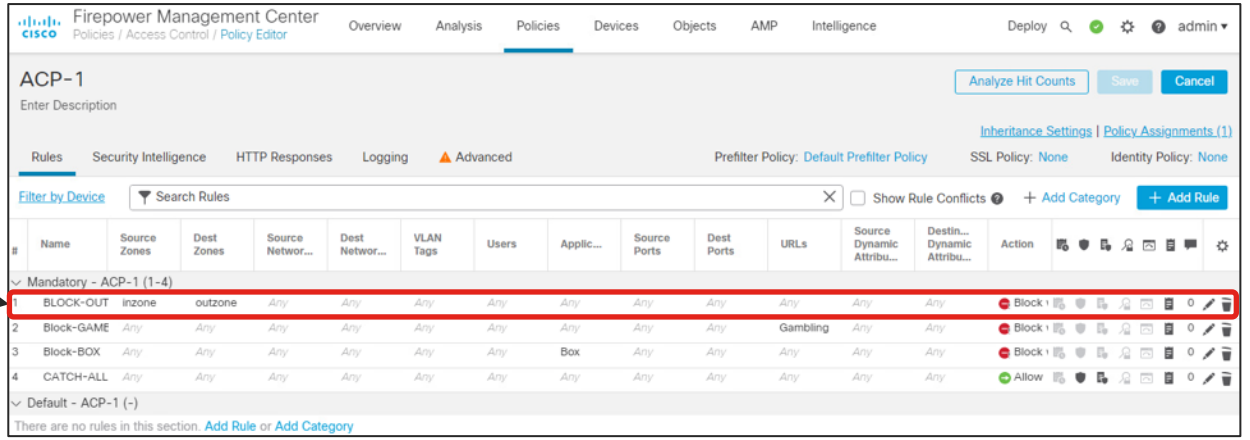
デプロイ前の正しい FTD の設定 (FMC)

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
```

ロ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)

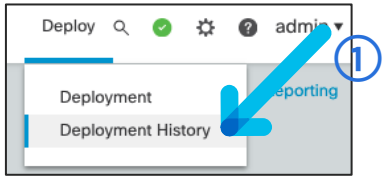


間違えて入れたルールが FTD にデプロイされてしまっている状態

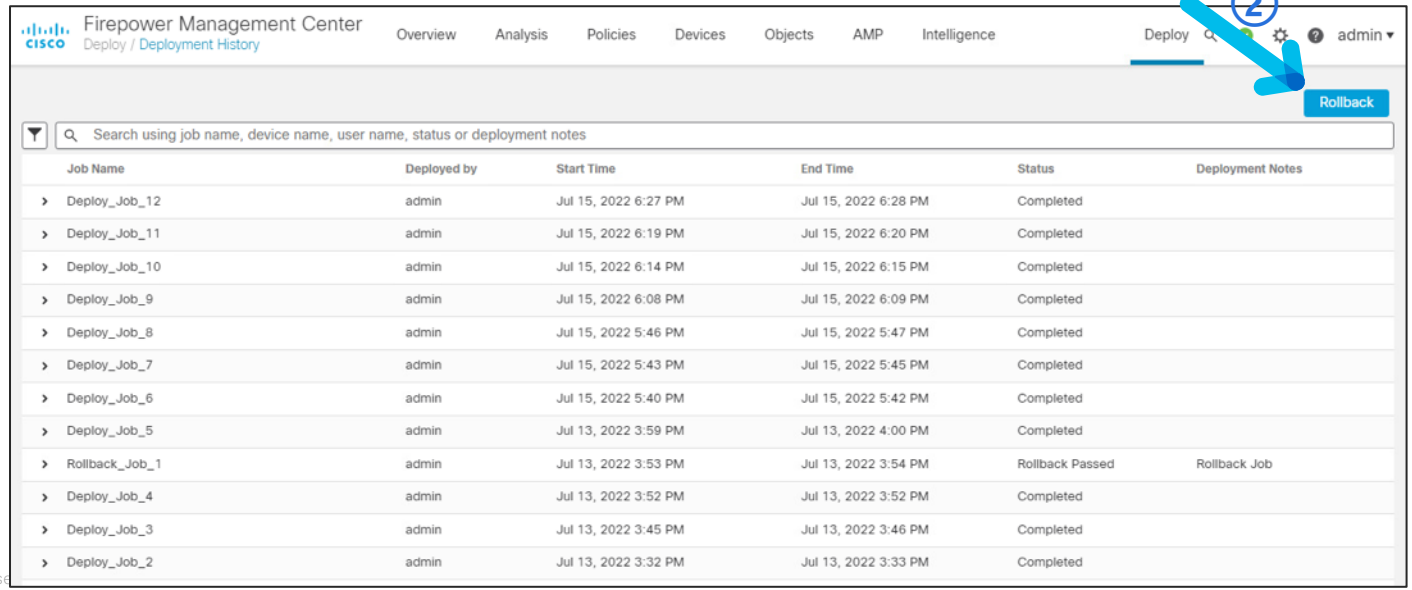
```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list CSM_FW_ACL_; 8 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit 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 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) 0xa1d3780e
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



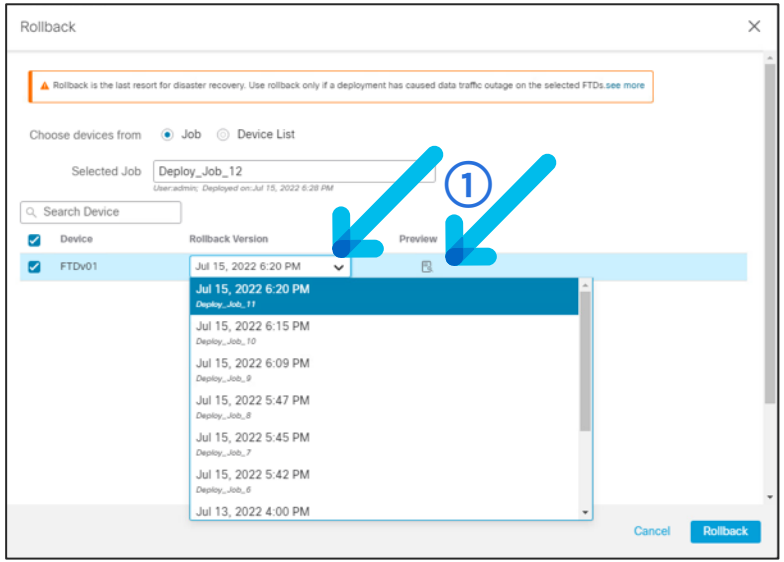
① Deploy → Deployment をクリック
② Rollback をクリック

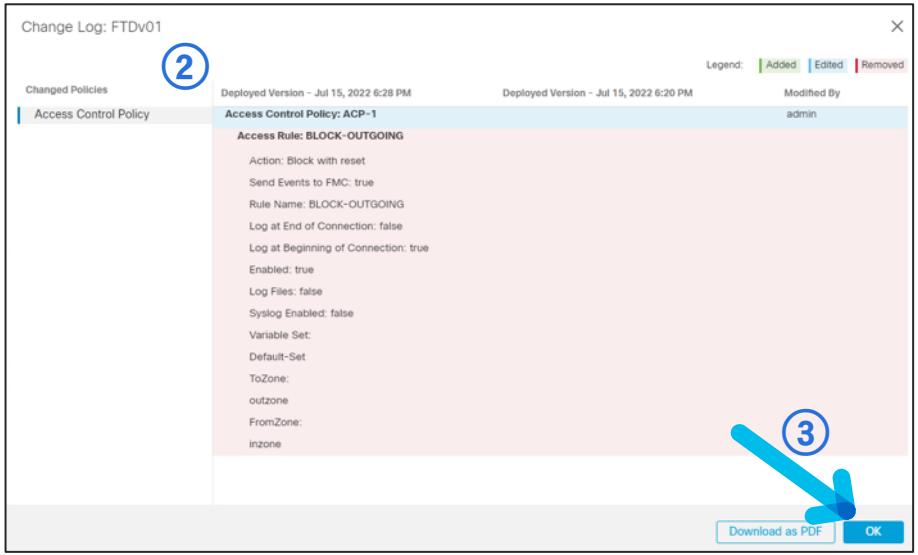


Job Name	Deployed by	Start Time	End Time	Status	Deployment Notes
Deploy_Job_12	admin	Jul 15, 2022 6:27 PM	Jul 15, 2022 6:28 PM	Completed	
Deploy_Job_11	admin	Jul 15, 2022 6:19 PM	Jul 15, 2022 6:20 PM	Completed	
Deploy_Job_10	admin	Jul 15, 2022 6:14 PM	Jul 15, 2022 6:15 PM	Completed	
Deploy_Job_9	admin	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

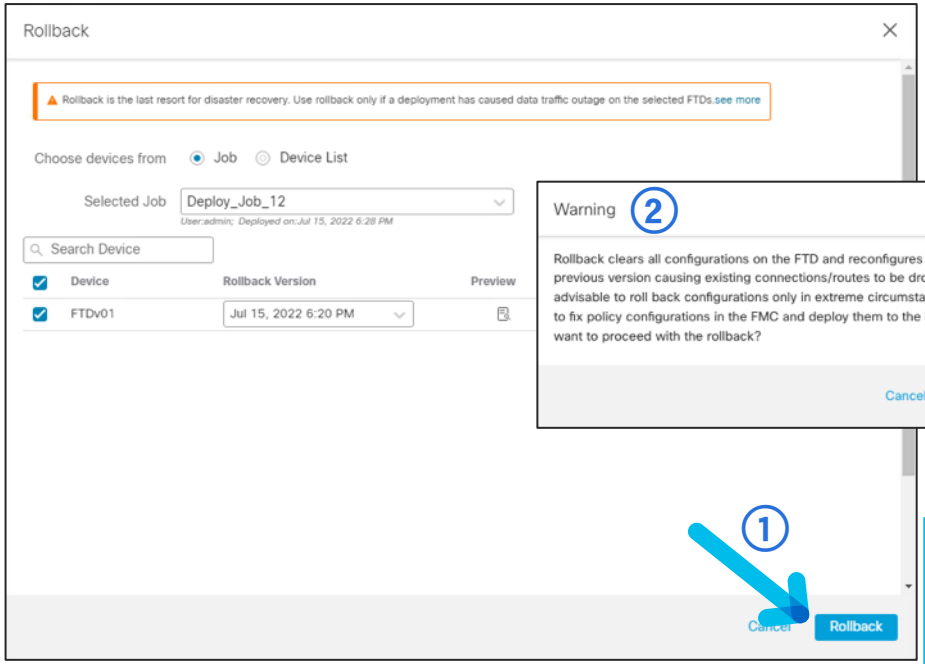


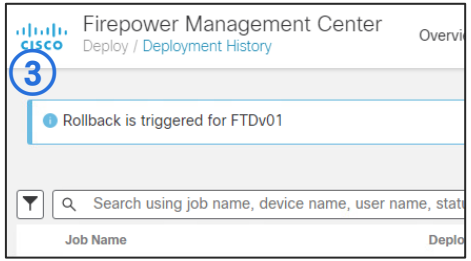


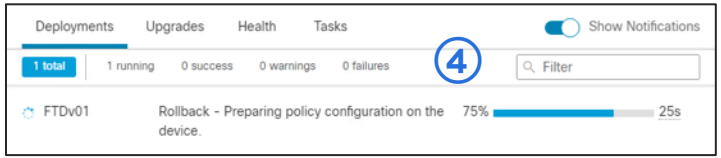
① 戻したい設定をデプロイした Job を選択し、Preview をクリック
② この Job にロールバックすると変更される差分のプレビューが表示される
③ 差分に問題がなければ OK をクリック

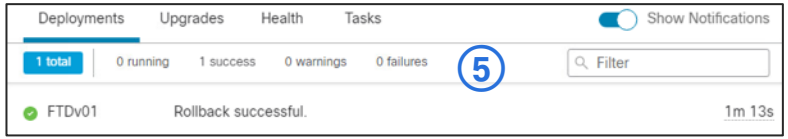
FMC での設定ロールバック実施 ③

- FTD への設定ロールバックを実施





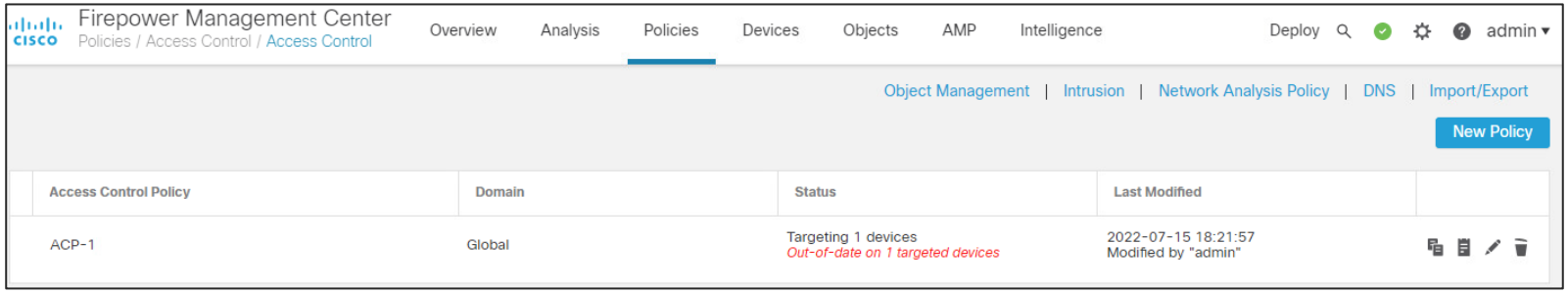




① Rollback をクリック
② ロールバック時の警告が表示される。問題なければ Proceed をクリック
③ 指定した FTD デバイスに対してロールバックが開始される
④ Task 画面よりロールバックの進捗状況を確認できる
⑤ ロールバックが無事に完了した旨が Task 画面に表示される

FMC での設定ロールバック実施 ④

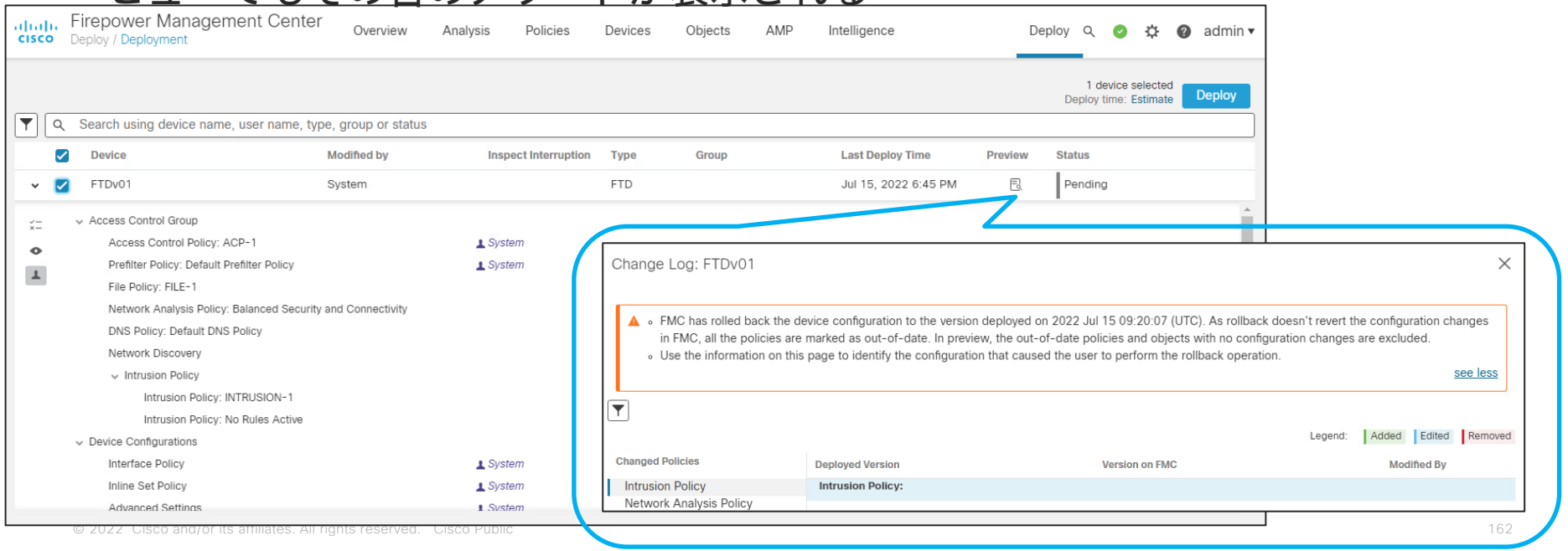
- FTD の実際の設定は戻っていることが確認できる。FMC 側の設定はそのままであり、デプロイした内容が out-of-date になっていることがわかる




```
> 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



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

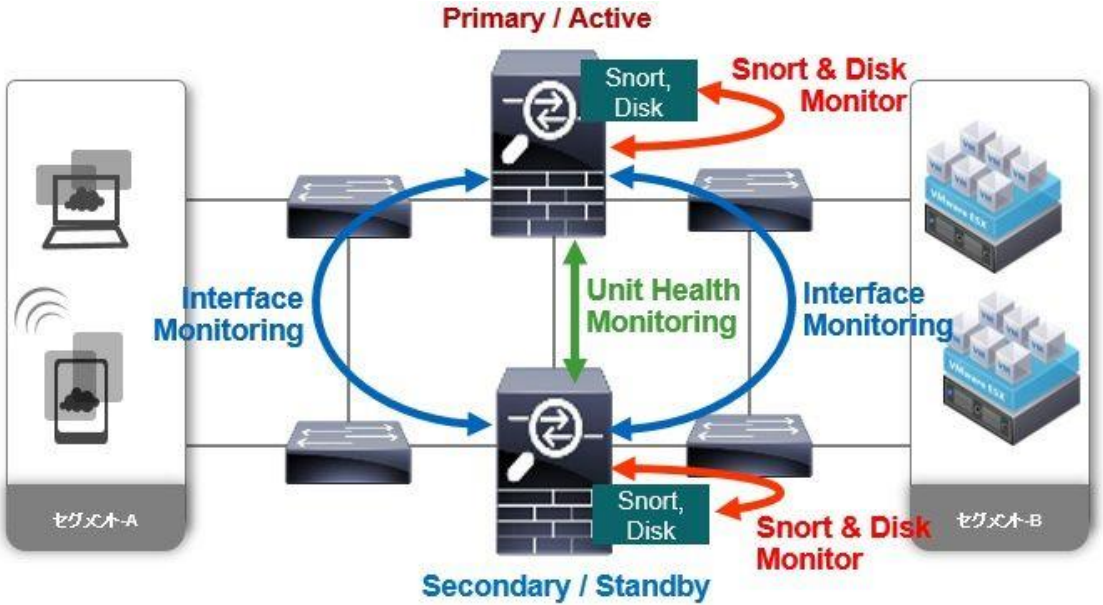
> configure policy rollback

```
> 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 deploy
ment 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

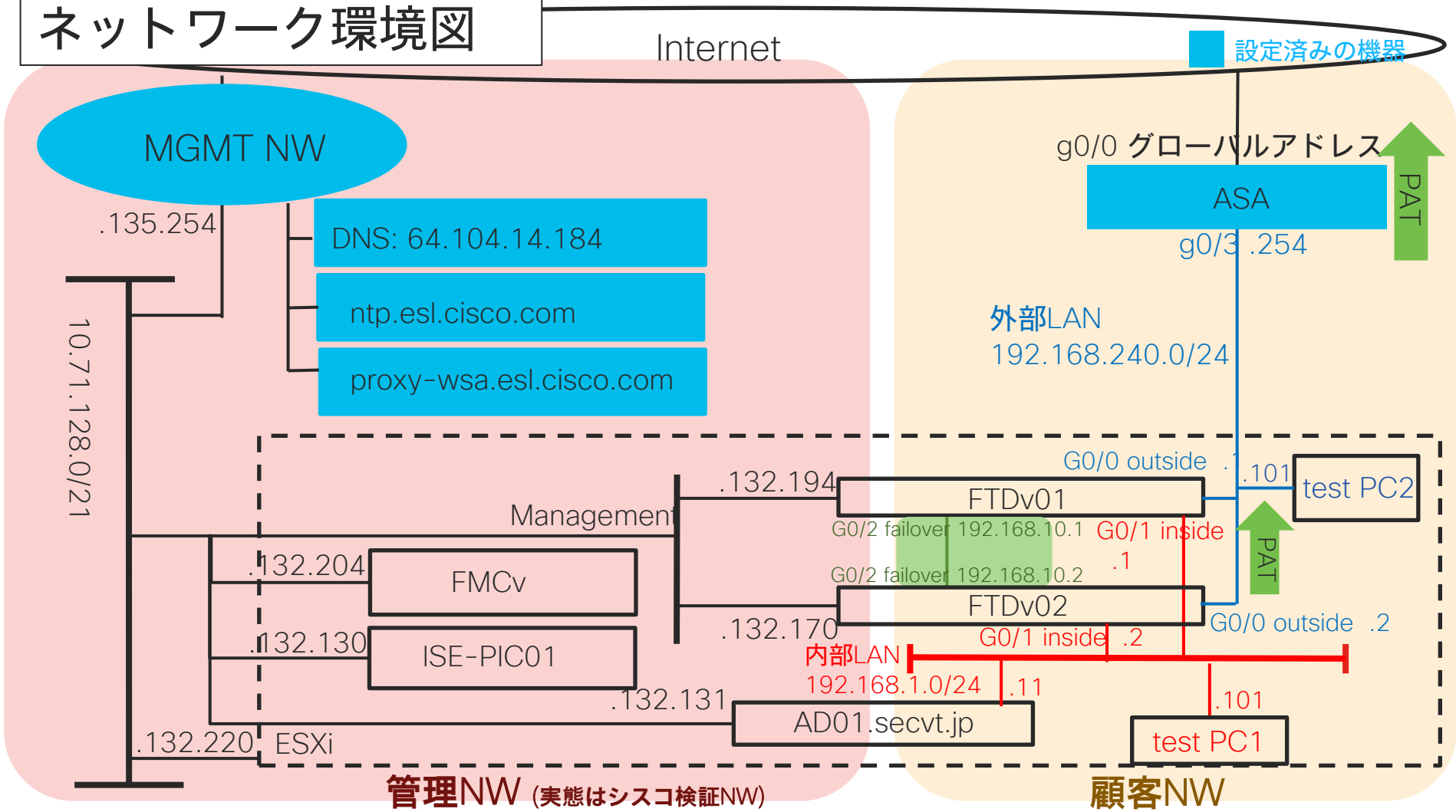


- 設定・動作イメージは ASA HA と同様
- FTD ではヘルスモニタリングとしてインタフェース以外に、Snort プロセスや Disk の障害監視も実施
- AWS 等パブリッククラウド上にデプロイされた FTDv は HA 非サポート

HA 設定における事前確認事項

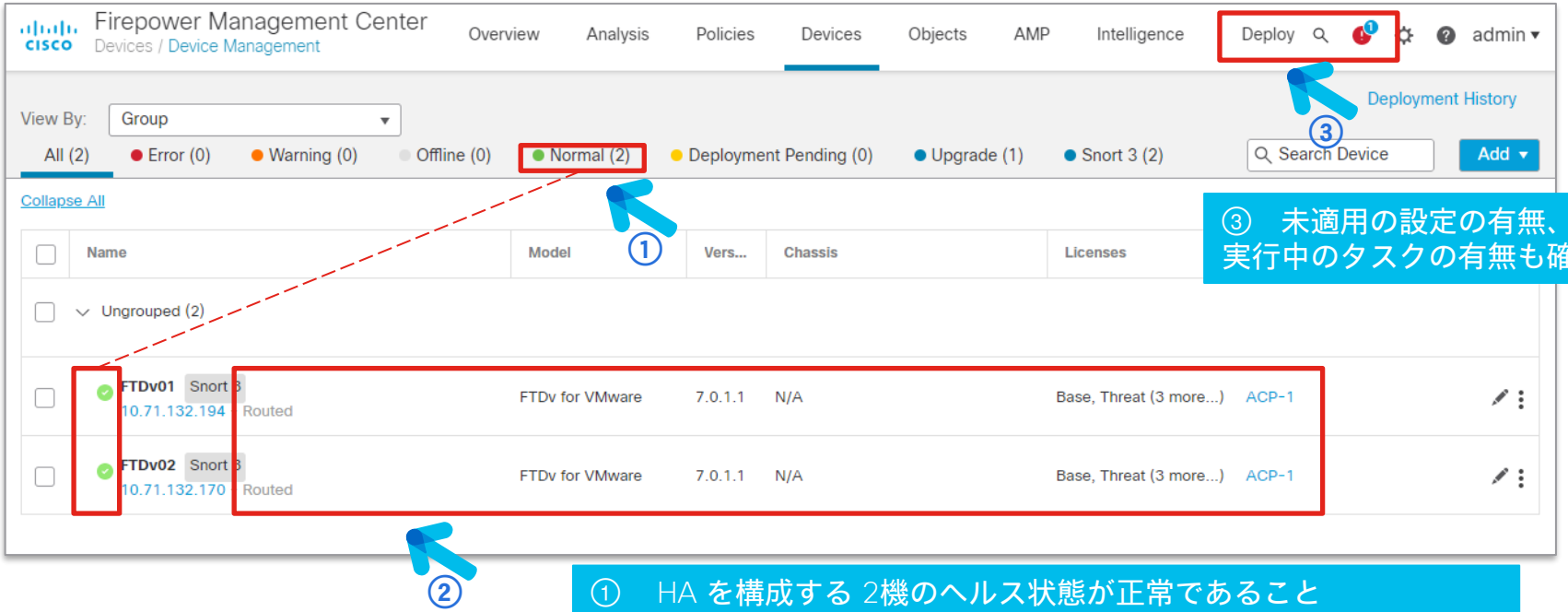
- 同じモデルあること
- 同じインターフェイス数とインターフェイスタイプであること。モジュール利用時は、同じモジュールを各デバイスに装着すること
- 同じソフトウェアバージョンを利用していること
- 同じ firewall モードであること。 Routed (default)、もしくは Transparent
- DHCP や PPPoE 設定をインターフェイスにしていないこと。DHCP のアドレス割当てや PPPoE 接続情報は、同期非サポートのため
- ヘルスモニターのステータスが各デバイスで Normal (正常) であること
- すべての設定変更が各デバイスでデプロイ済みであること
- 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 (スタンドアローン) 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
10.71.128.0/21
DNS: 64.104.14.184
ntp.esl.cisco.com
proxy-wsa.esl.cisco.com
g0/0 グローバルアドレス
ASA
g0/3 .254
PAT
外部LAN
192.168.240.0/24
G0/0 outside .1
.101
test PC2
.132.194
FTDv01
Management
G0/2 failover 192.168.10.1
G0/1 inside
.1
PAT
.132.204
FMCv
G0/2 failover 192.168.10.2
FTDv02
G0/0 outside .2
.132.170
.132.130
ISE-PIC01
G0/1 inside .2
内部LAN
192.168.1.0/24
.11
.101
.132.131
AD01.secvt.jp
test PC1
.132.220
ESXi
管理NW (実態はシスコ検証NW)
顧客NW

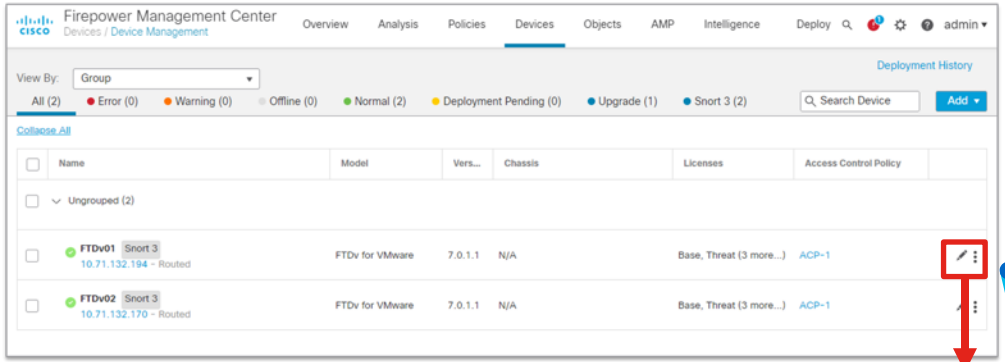
ステップ1-1: HA 設定 – 事前準備・確認

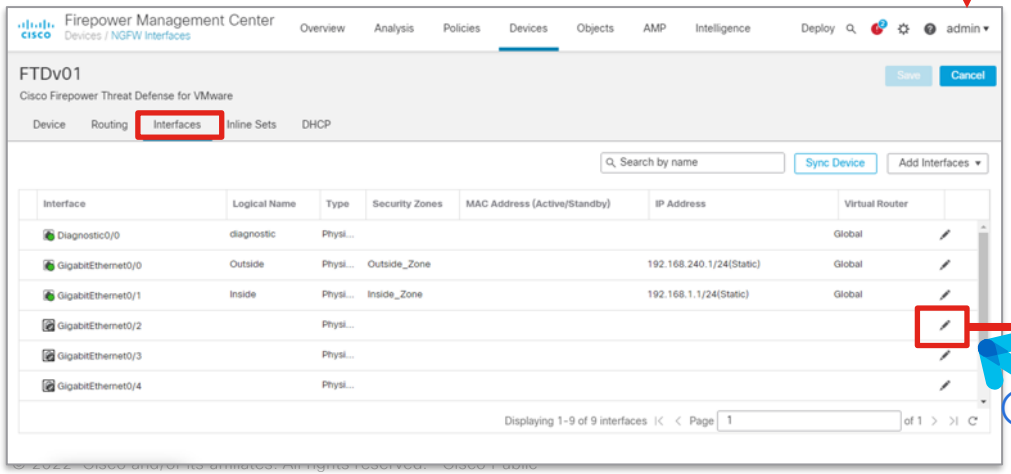
- HA 構成のために FTDv02 を新たにインストールし、初期セットアップおよび FMC への管理登録を実施（手順は FTDv01 と同様）
- HA を構成する FTD の状態が問題ないことを確認

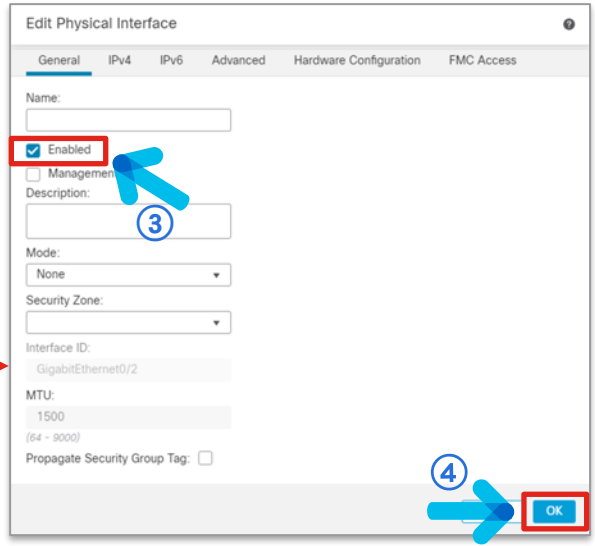


ステップ2-1: HA 設定 – FTDv01 の HA リンクのための IF 有効化

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

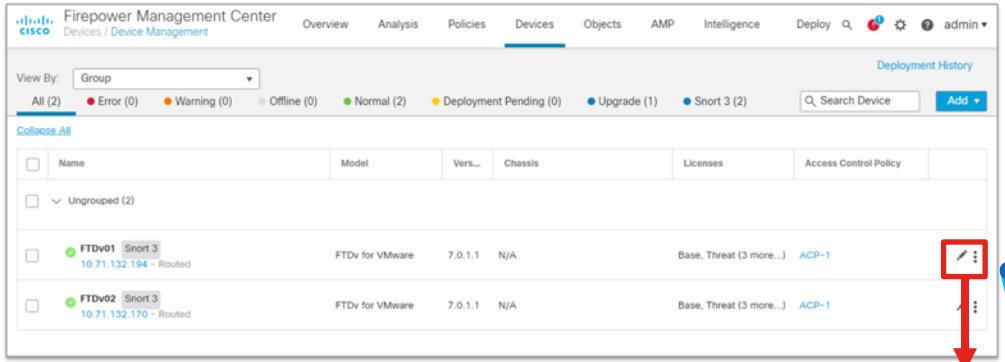


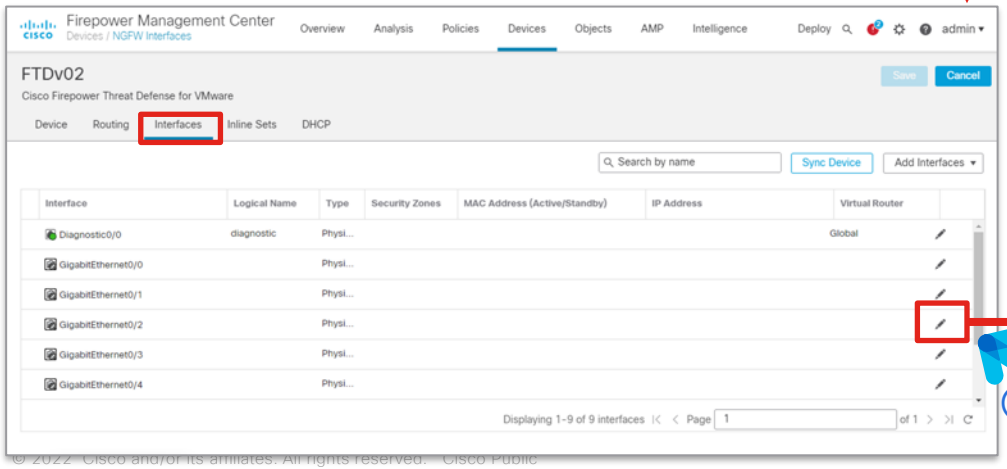


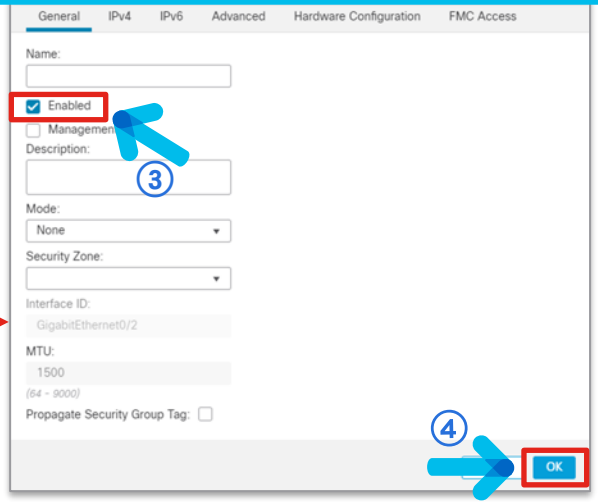


注：ESXi で HA リンク接続用の仮想スイッチを別途作成必要

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



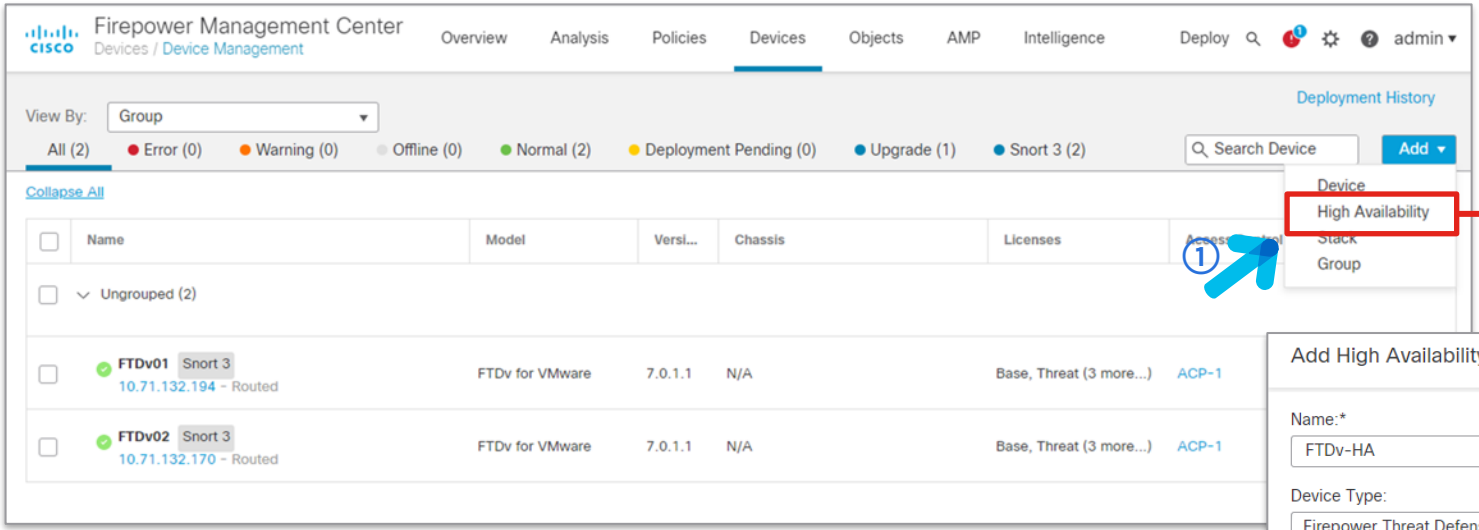


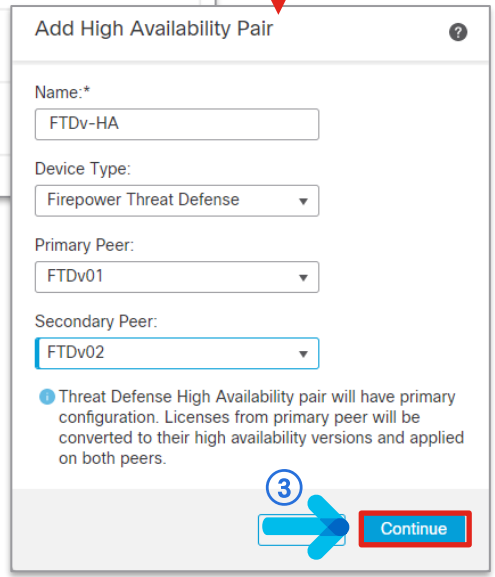


① Device Management より FTDv02 の鉛筆マークをクリック
② Interface タブをクリックし、Gig0/2 の鉛筆マークをクリック
※他の IF は HA に成功すれば自動で Enable となるため事前設定不要
③ General の Enable にチェック
④ OK をクリック
⑤ Save をクリックして設定を保存
⑥ Deploy をクリックして FTD に適用

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



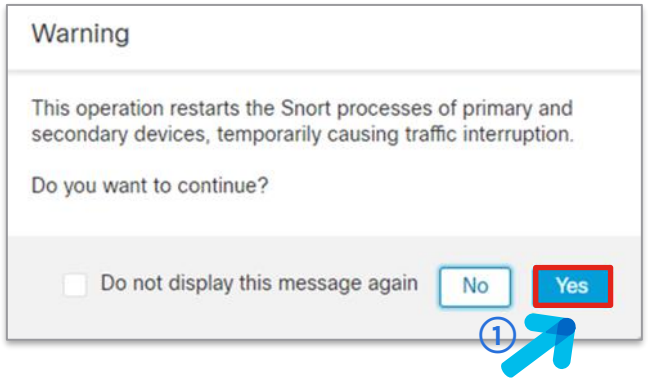


① Device Management > Add > High Availability をクリック
② 以下を設定
- Name： FTDv-HA ※任意の名前を記入
- Device Type： Firepower Threat Defense を選択
- Primary Peer： FTDv01 を選択
- Secondary Peer： FTDv02 を選択

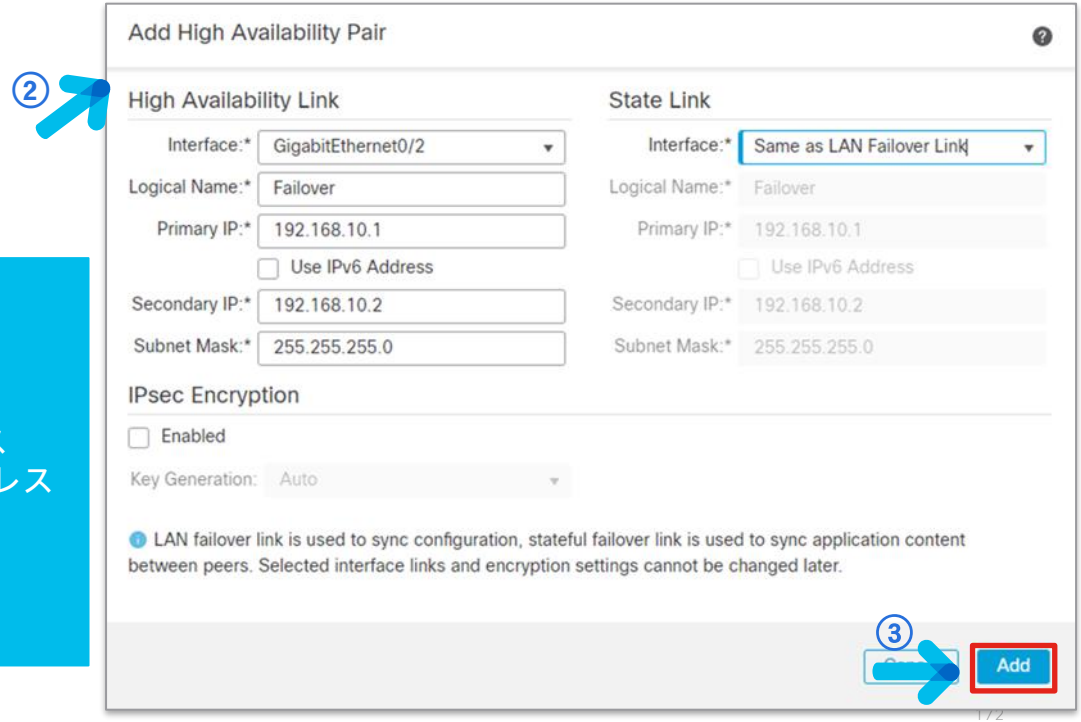
③ Continue をクリック

②

ステップ3-1: HA 設定 – HA ペアの作成 (続き)



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



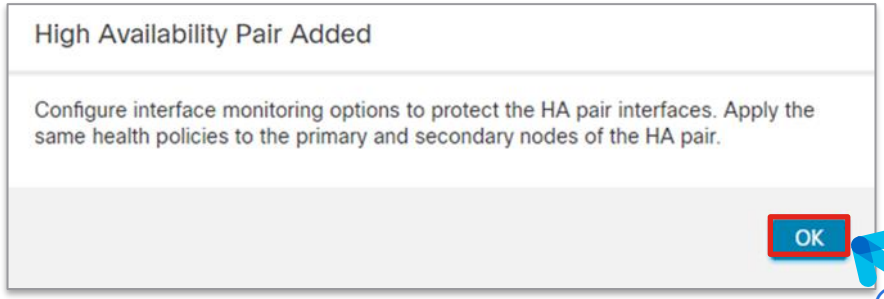
② HA リンク、State リンクで以下を入力・設定
HA リンク
- Interface : Gig0/2
- Logical Name: 任意の名前を入力
- Primary IP: FTDv01 の HA リンクの IP アドレス
- Secondary IP: FTDv02 の HA リンクの IP アドレス
- Subnet Mask: HA リンクのサブネットマスク

State Link
- Interface: Same as LAN Failover…を選択

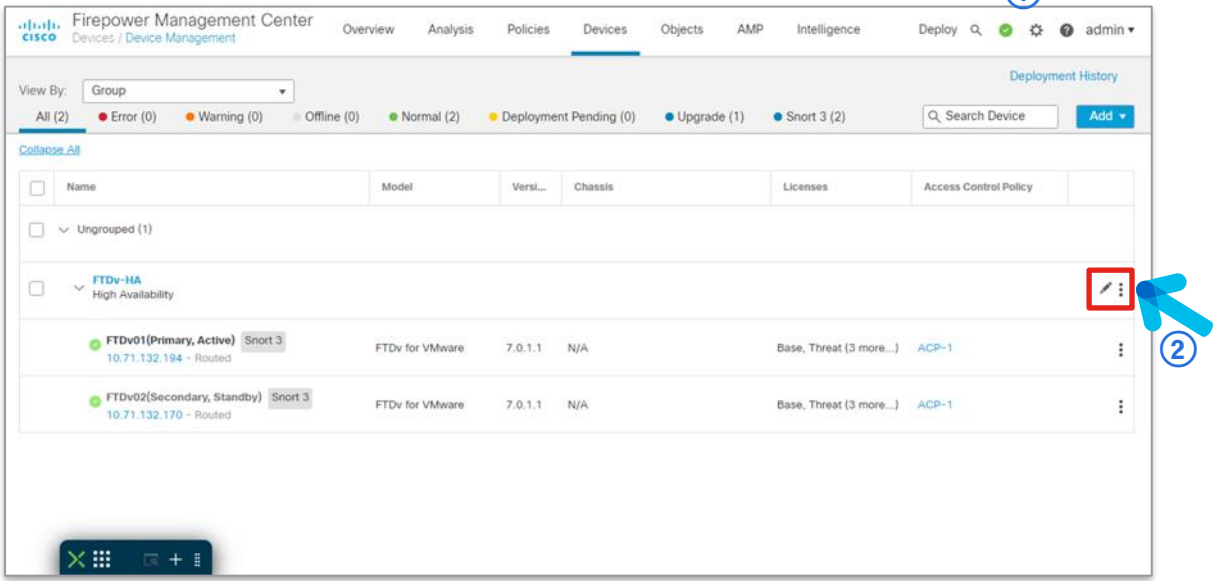
③ Add をクリック (クリック後、HA構成開始)

※ HA 構成完了までに 10分以上要する場合もある

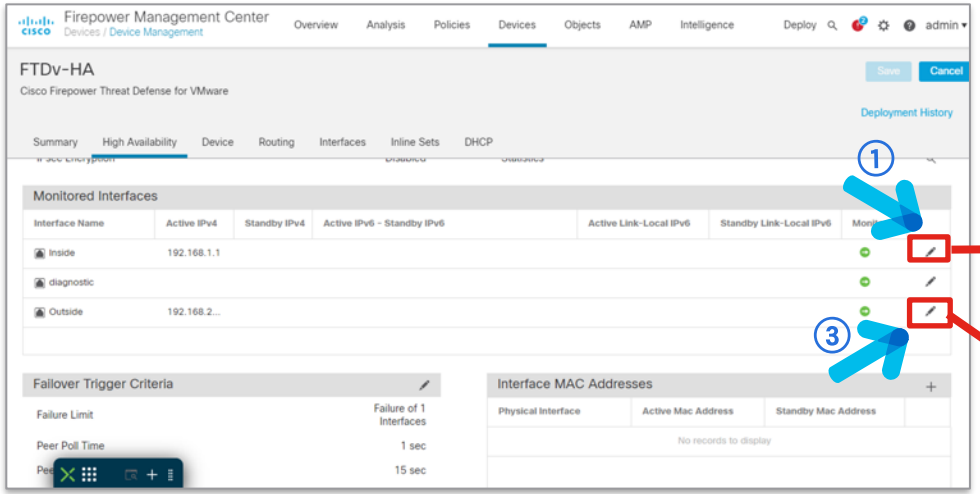
ステップ4-1: HA 設定 – HA の構成とインタフェースモニター設定

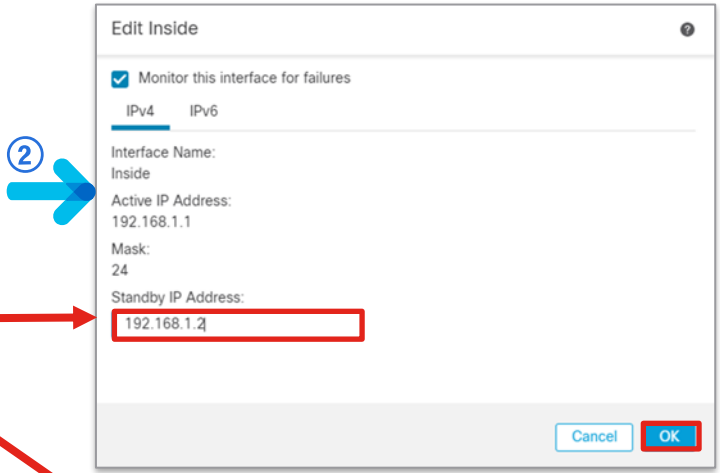


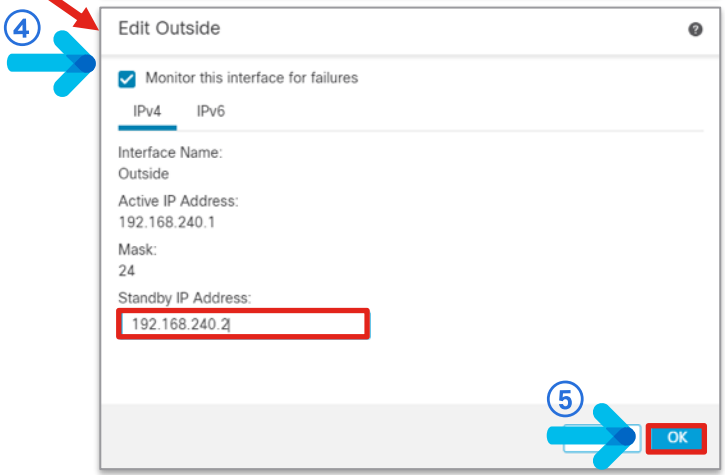
① FTD HA ペア登録後のインターフェイスモニター設定や、ヘルスポリシー設定の適用を忘れないように、という情報のポップアップがあるため、OK をクリック
② FTDv-HA の鉛筆マークをクリック



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)

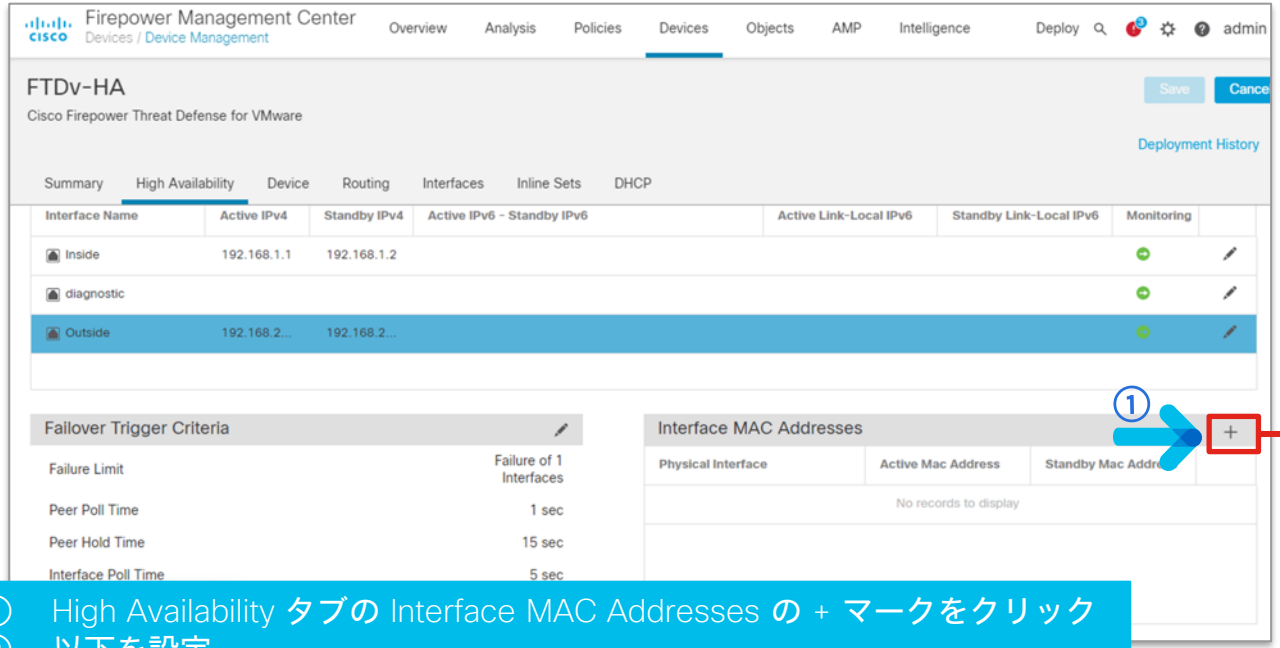






① High Availability タブの Monitoring Interfaces > inside の鉛筆マークをクリック
② Secondary IP Address に FTDv2 の inside IF モニタ用の IP アドレスを設定し、OK をクリック
③ Outside の鉛筆マークをクリック
④ Secondary IP Address に FTDv2 の Outside IF モニタ用の IP アドレスを設定し、OK をクリック
⑤ Save をクリック

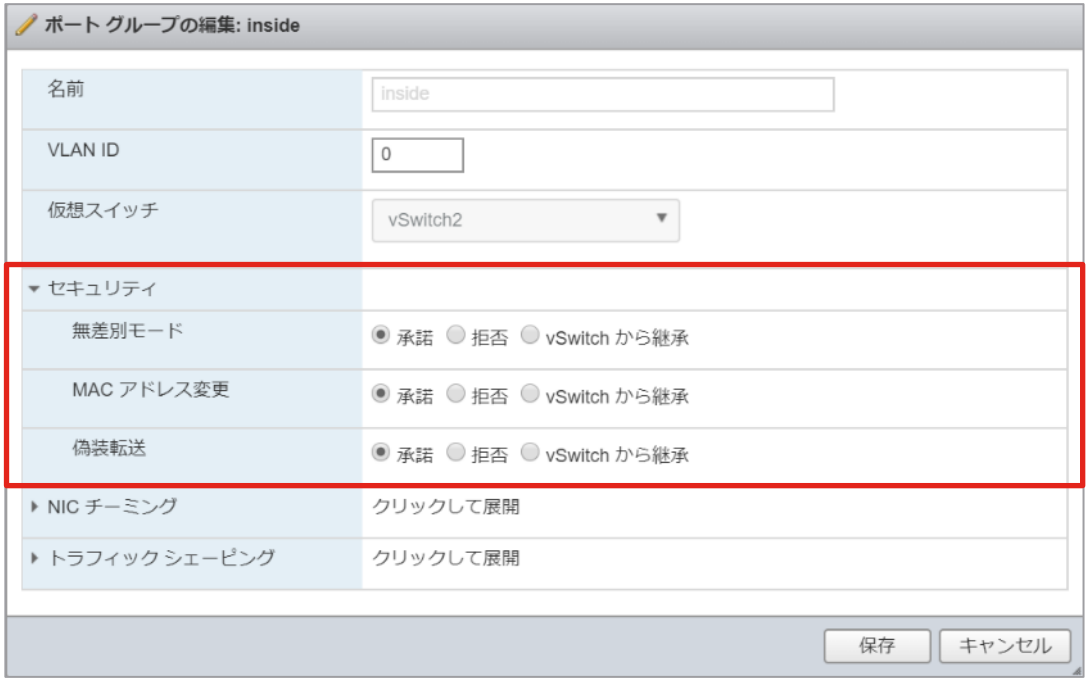
ステップ5-1: HA 設定 – 仮想 MAC アドレス設定



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



すべて承諾をチェック

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html#24182

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)
        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--------
```

HA リンクが UP 状態

Primary 機の状態

Secondary 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)

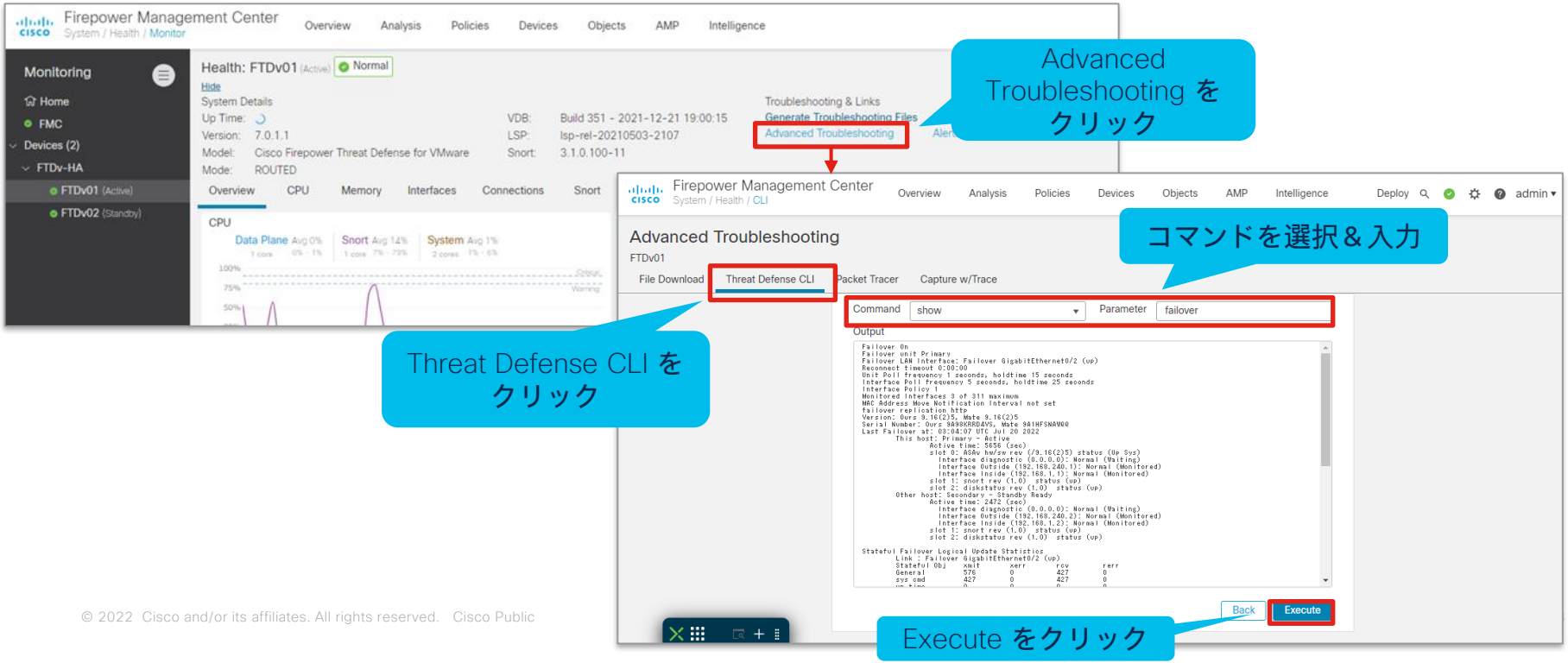
State リンクが UP 状態

モニタ対象の IF の状態 (Normal)

モニタ対象のSnortとDiskの状態 (Up)

参考: FMC での HA ステータス確認

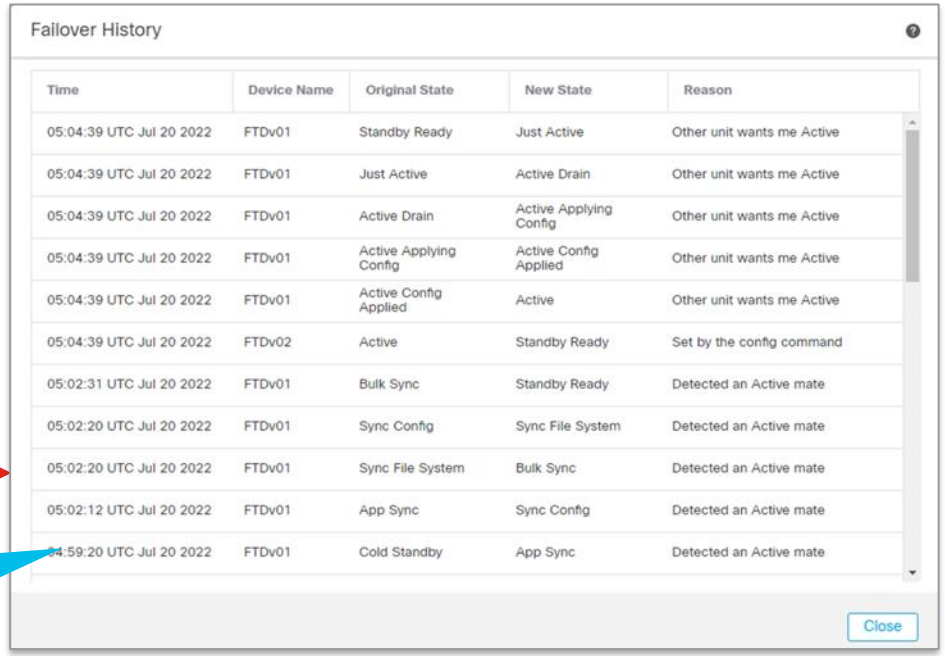
- show failover を FMC から確認する方法
- ⚙ より Health > Monitor > 対象の FTD デバイスをクリック



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

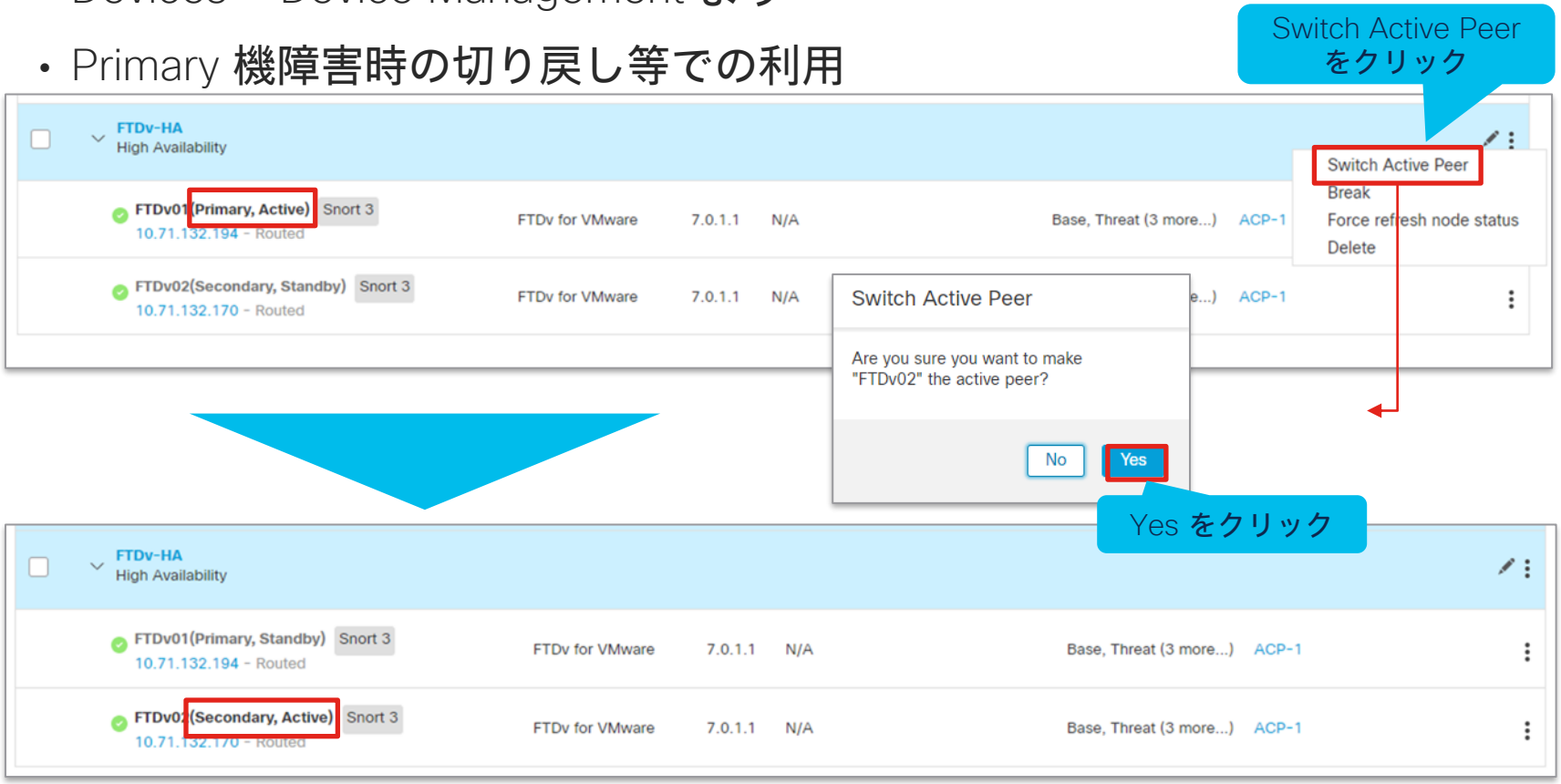
虫眼鏡アイコンを
クリック



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

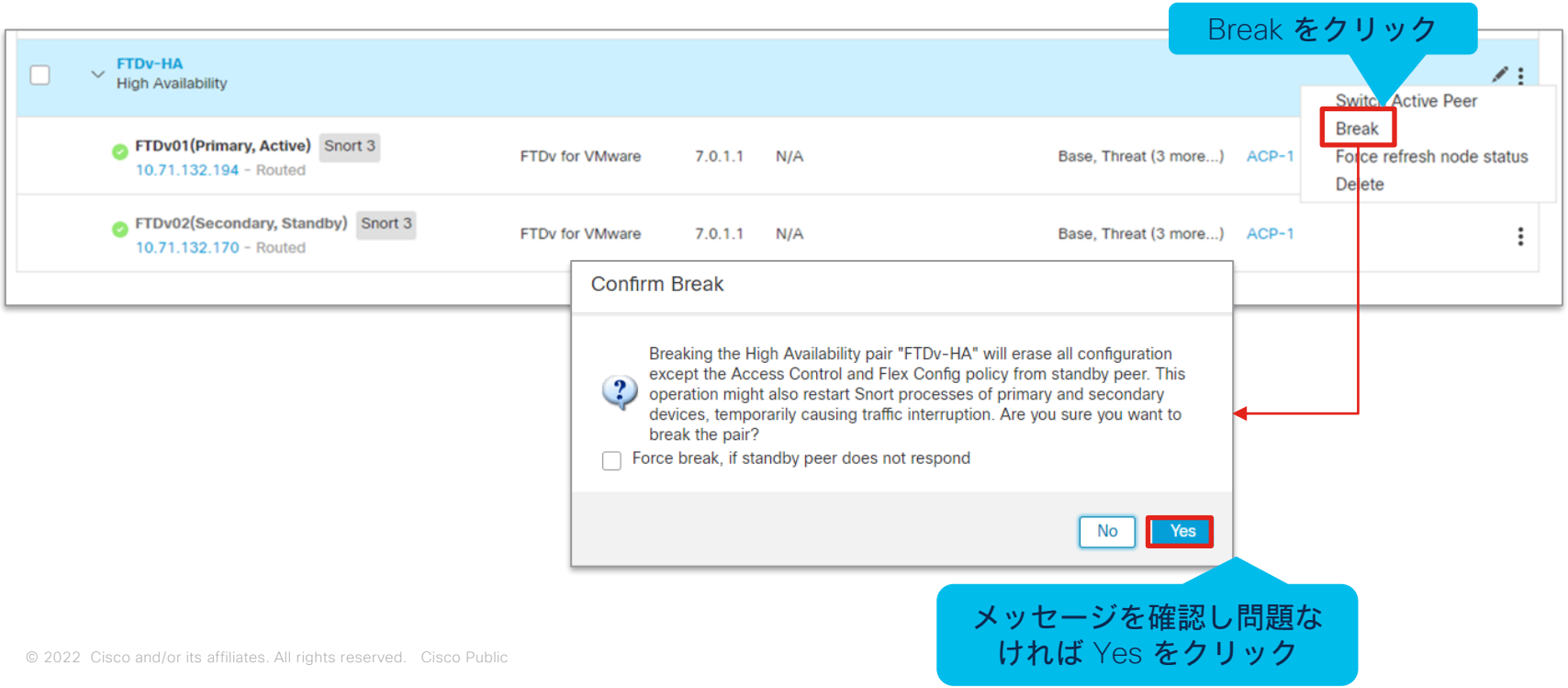
HA Active 機の切り替え

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



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



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。

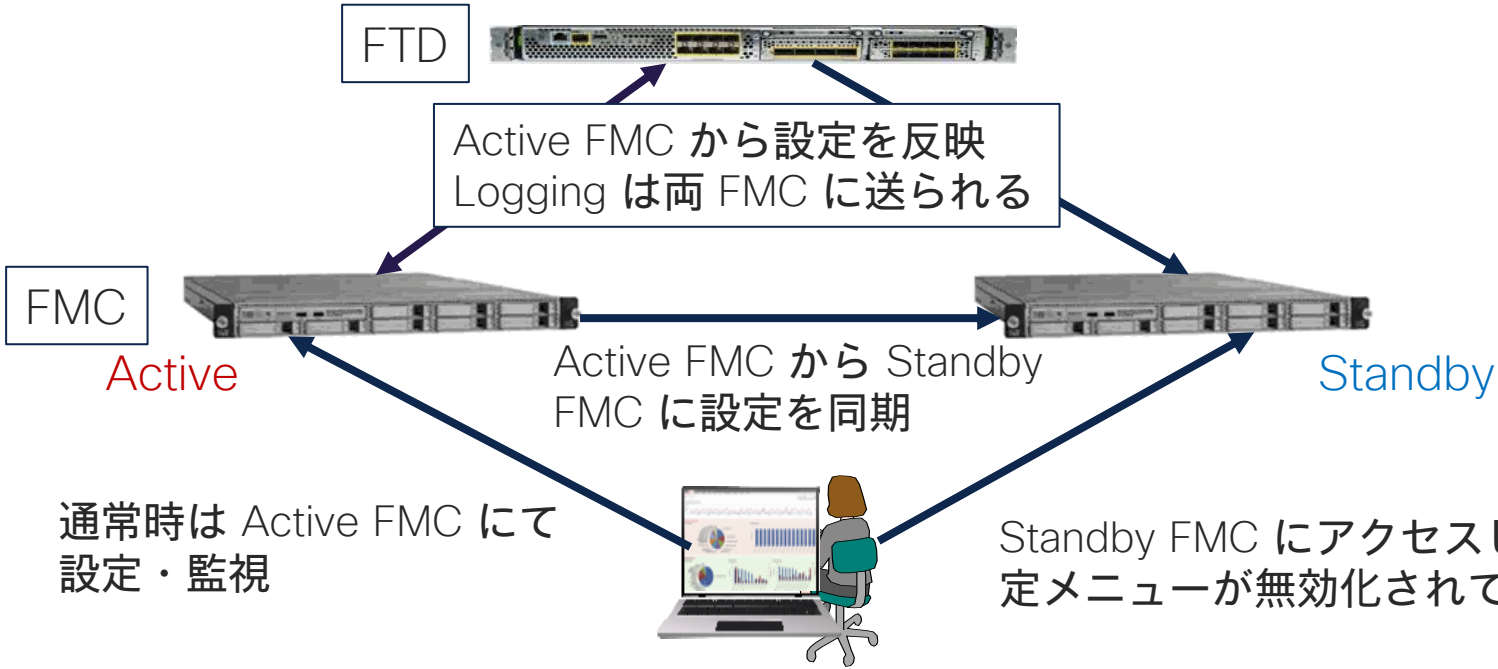
Firepower System: FTD HA: FTD 冗長構成の組み方とトラブルシューティング (FMC 利用時)
¥https://community.cisco.com/t5/-/-/ta-p/3952716

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 間通信で必要な帯域は最低 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



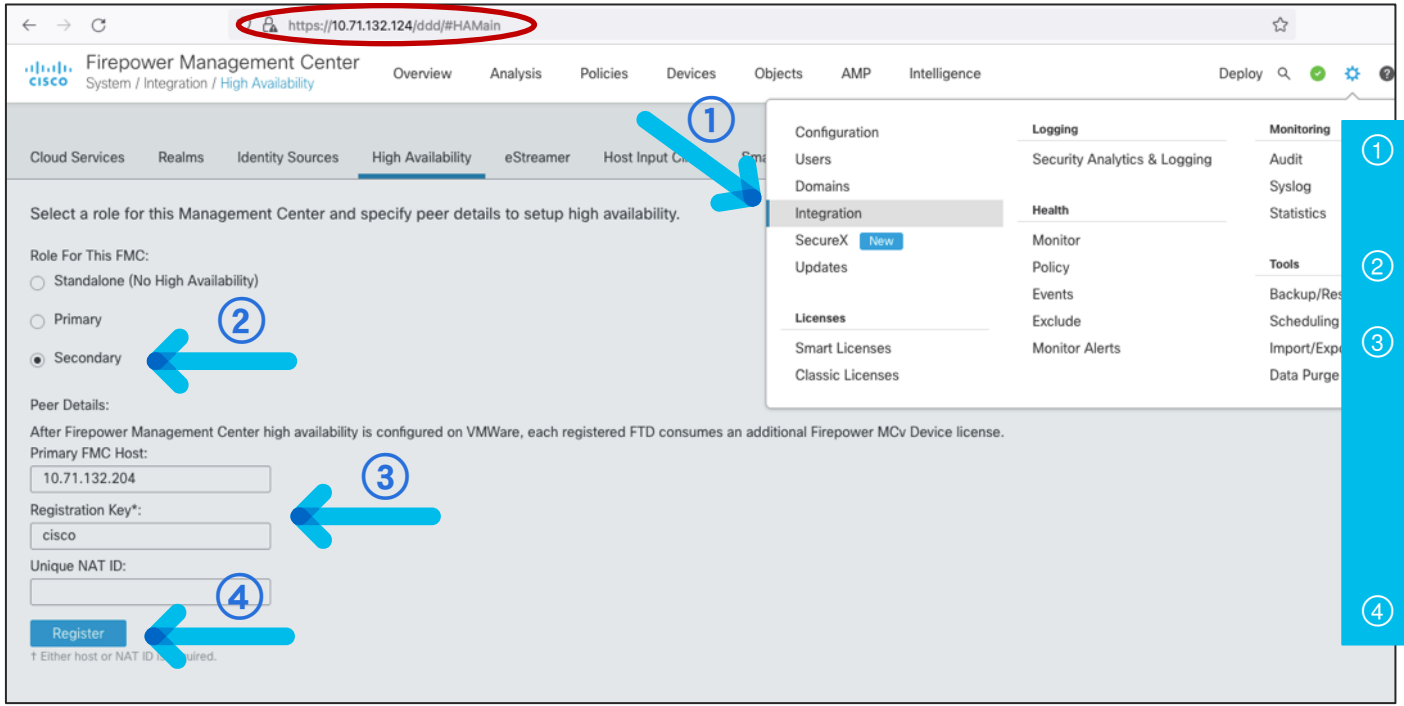
本章での手順

- 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

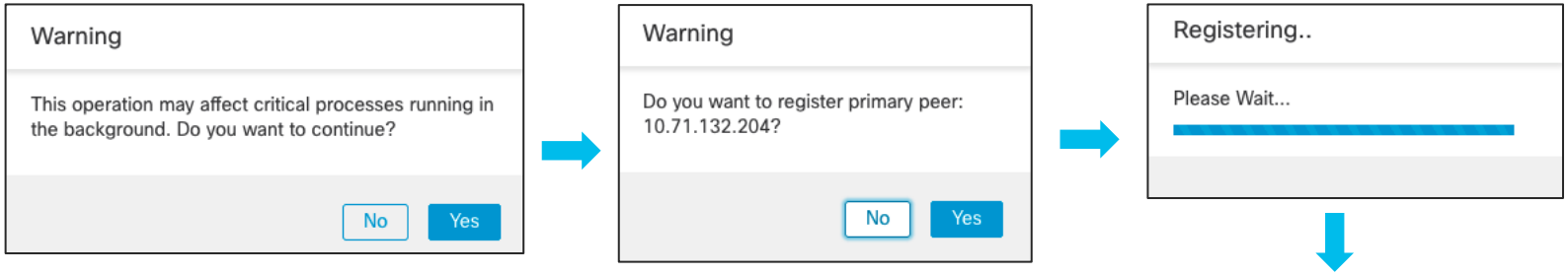
セカンダリ FMC とする予定の FMCv を新規作成、各種バージョンを揃えた後にその FMC で HA の構築を開始する。このとき、セカンダリとなる FMC には FTD デバイスが登録されていないこと

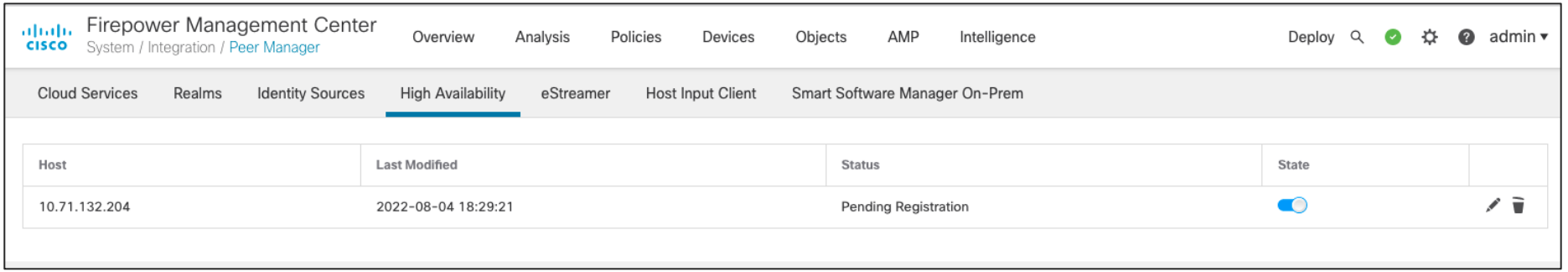


① セカンダリとする予定の FMC で System → Integration をクリック
② FMC ロールとして Secondary をクリック
③ Peer Details の Primary FMC Host にプライマリとする予定の FMC の IP アドレス (10.71.132.204) を、Registration Key として任意の文字列 (この例では cisco) を入力
④ Register をクリック

セカンダリ FMC での HA セットアップ②

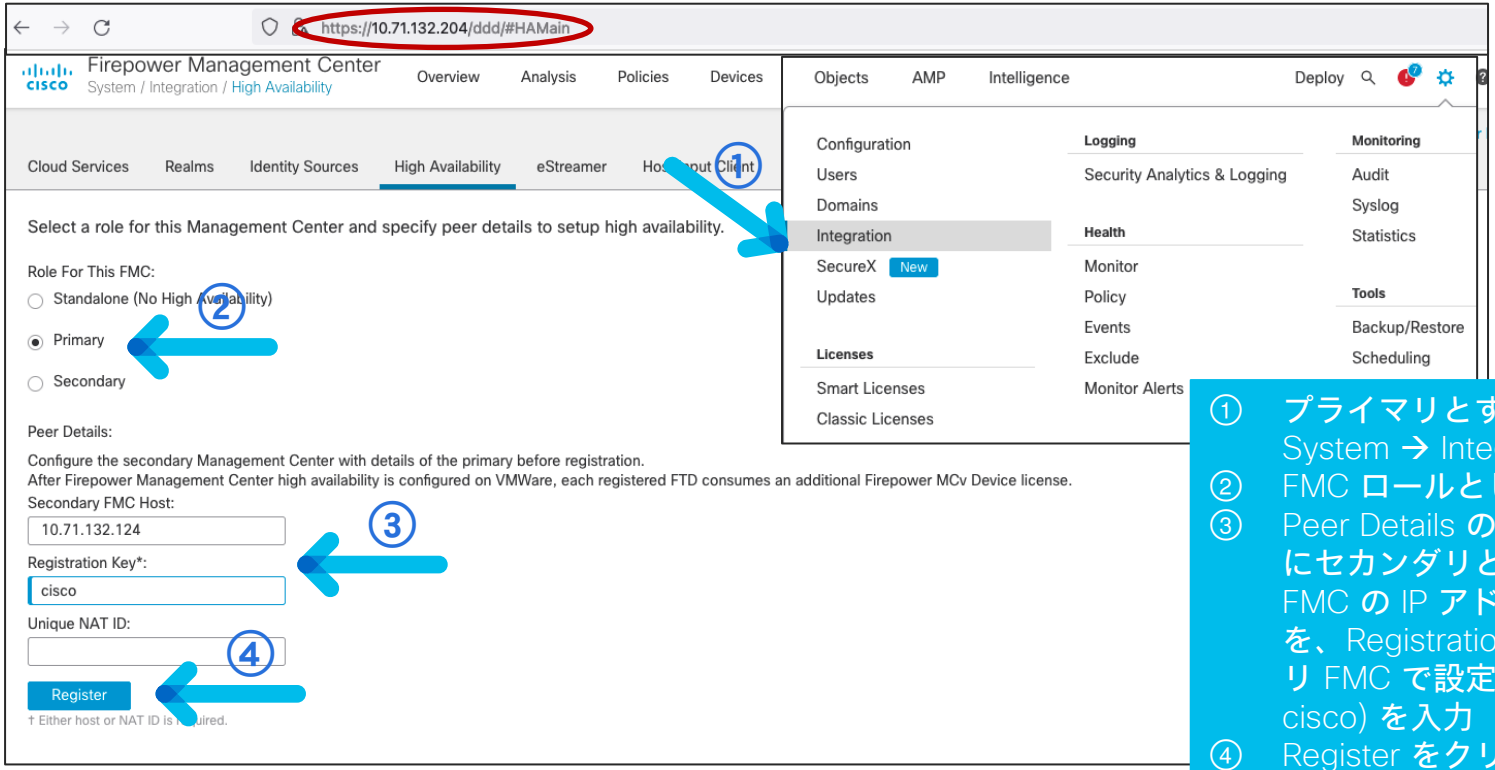
設定内容の確認のためのワーニングが何度か出てくるので、問題が無いことを確認して Yes をクリックして進める。セカンダリ FMC としての設定が終わると Status が Pending Registration となり、プライマリ FMC からの HA 設定リクエスト待ちとなる





プライマリ FMC での HA セットアップ①

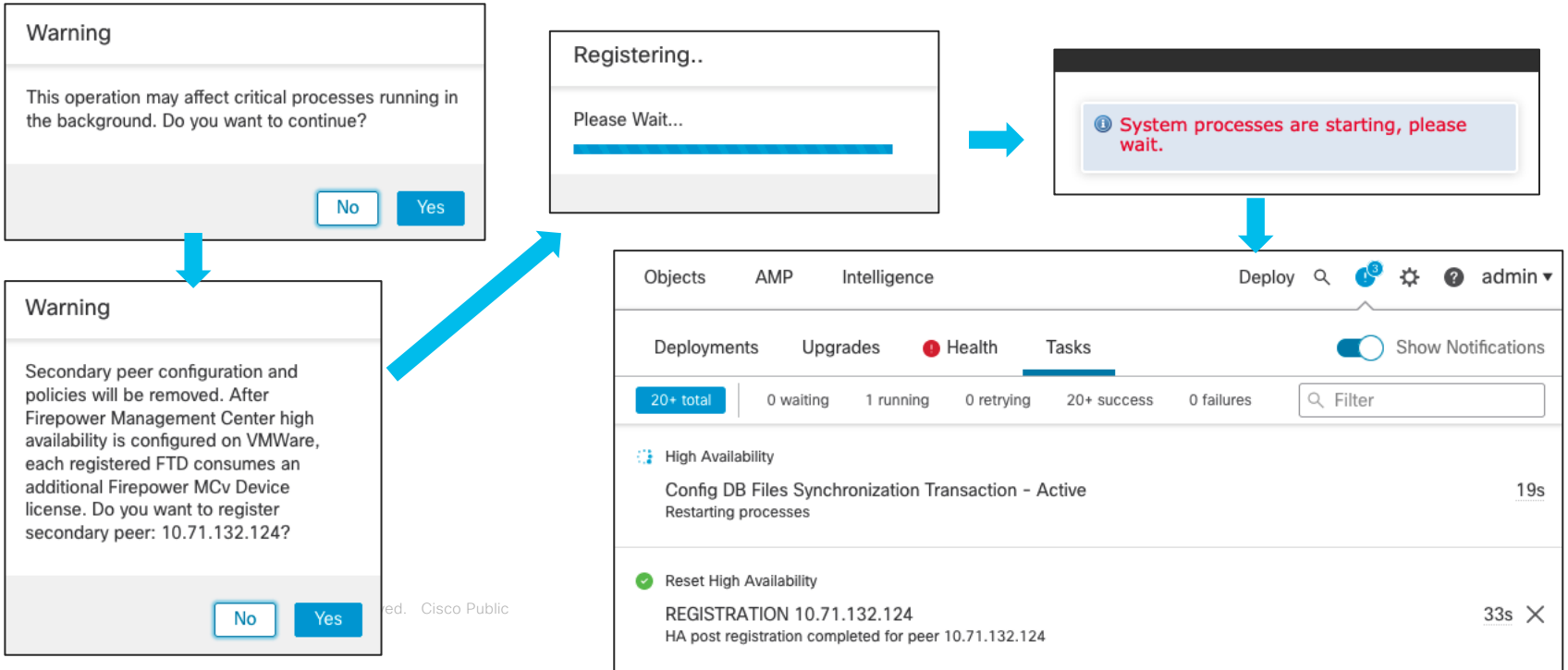
プライマリ FMC とする予定の FMC にて同様の手順で FMC HA の設定を開始する



① プライマリとする予定の FMC で System → 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

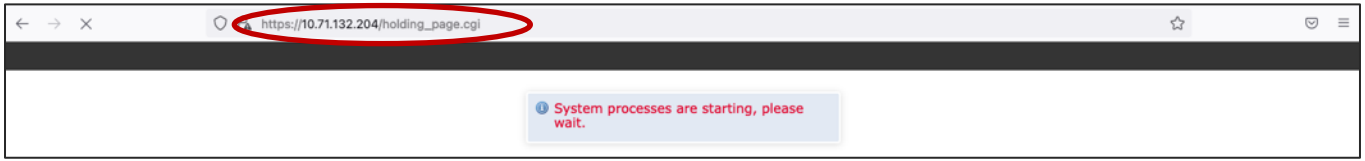
プライマリ FMC での HA セットアップ②

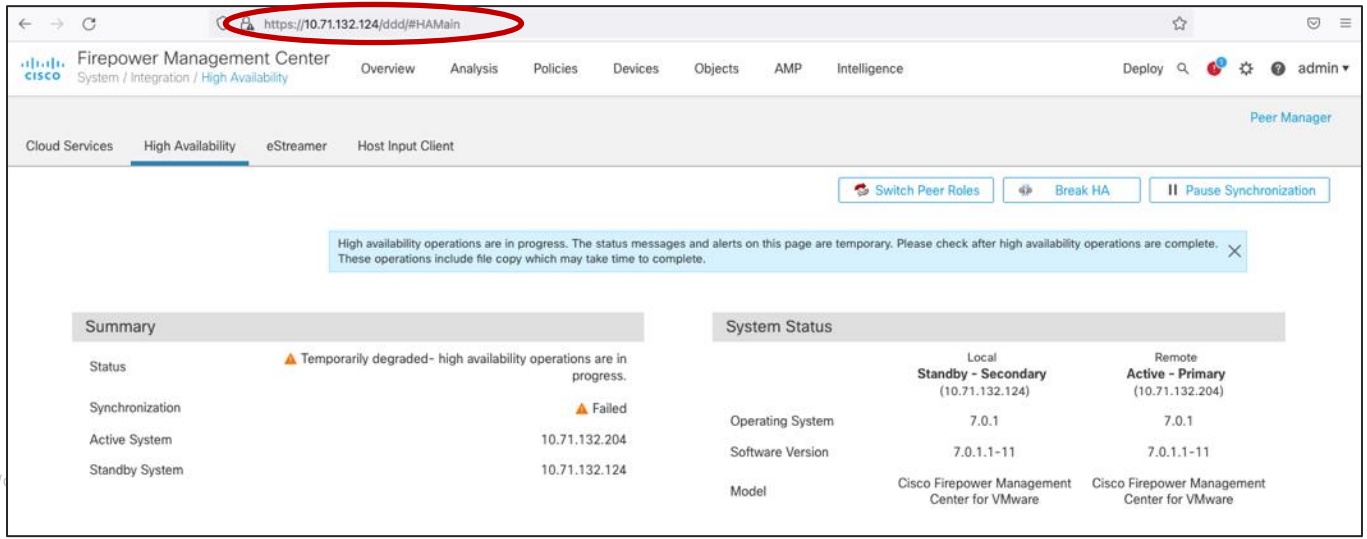
設定内容の確認のためのワーニングが何度か出てくるので、問題が無いことを確認して Yes をクリックして進める。プライマリ FMC としての設定が始まり、DB の同期等のタスクが進んでいく



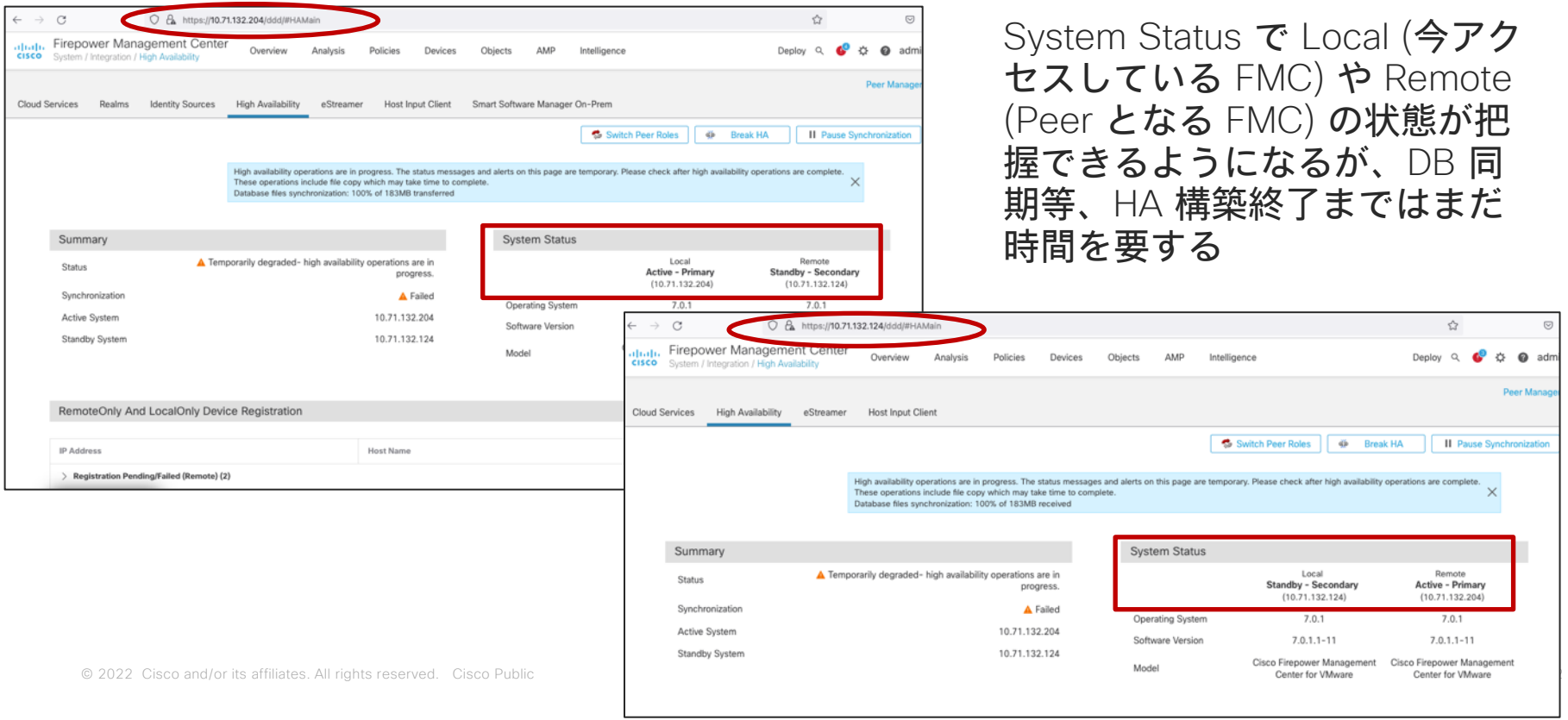
FMC HA 構築中のステータス確認①

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



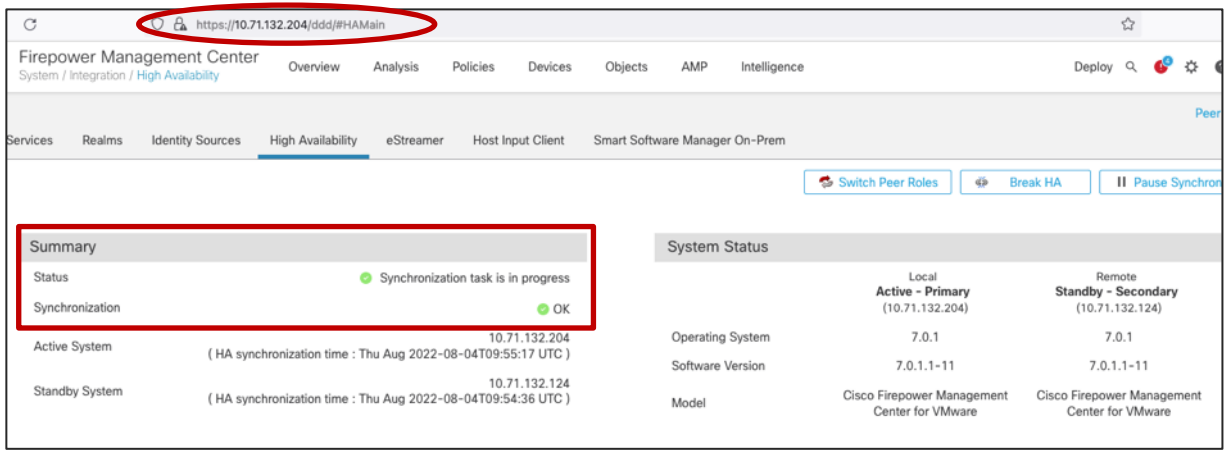


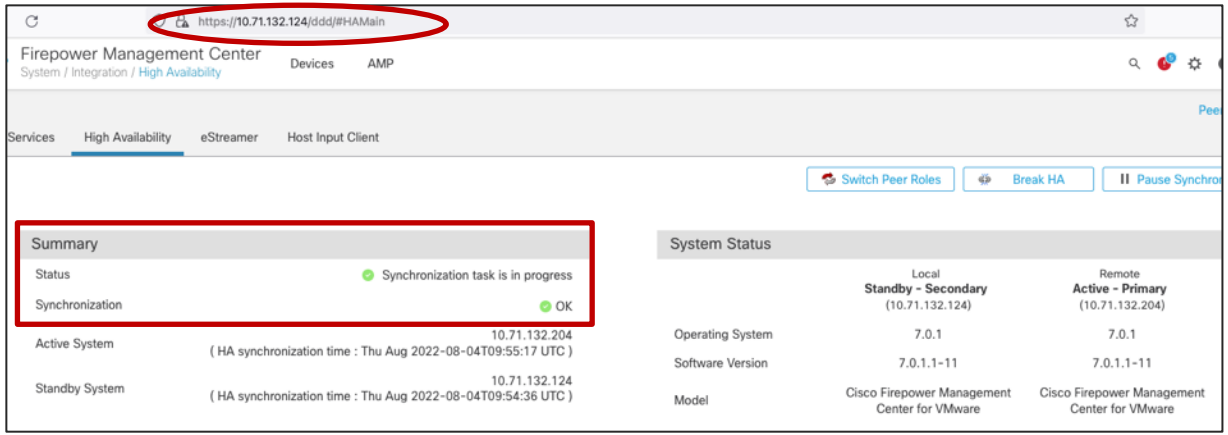
FMC HA 構築中のステータス確認②



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

FMC HA 構築完成を確認





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

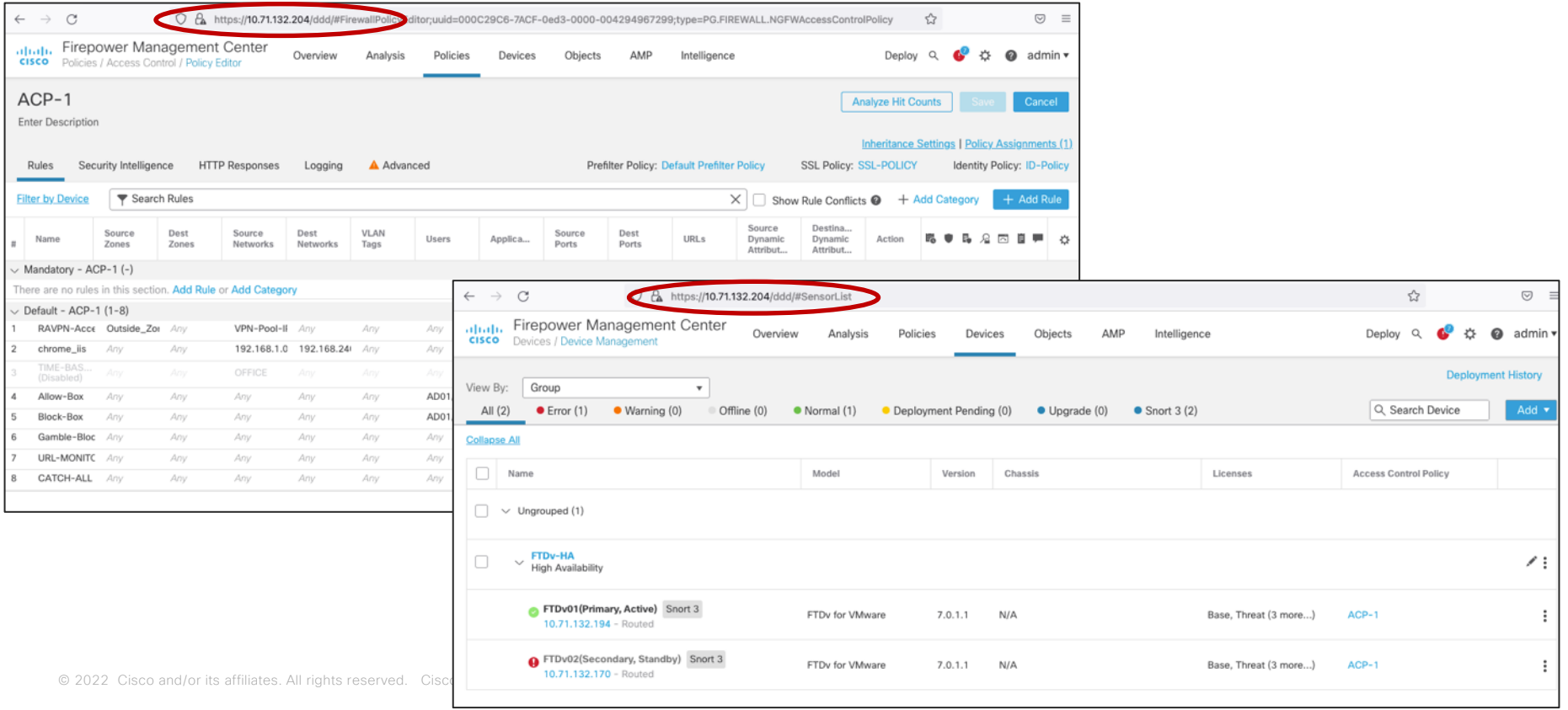
FTD と FMC の間の SFTunnel は、FTD から 2台の FMC に自動的に張り直される (次ページ参照)

(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

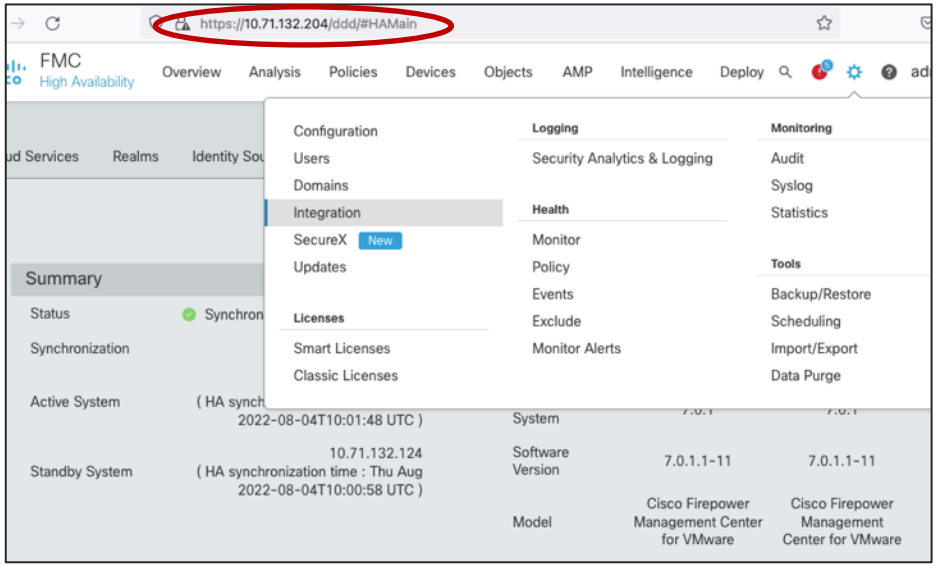
各種設定が Active FMC に残っていることを確認



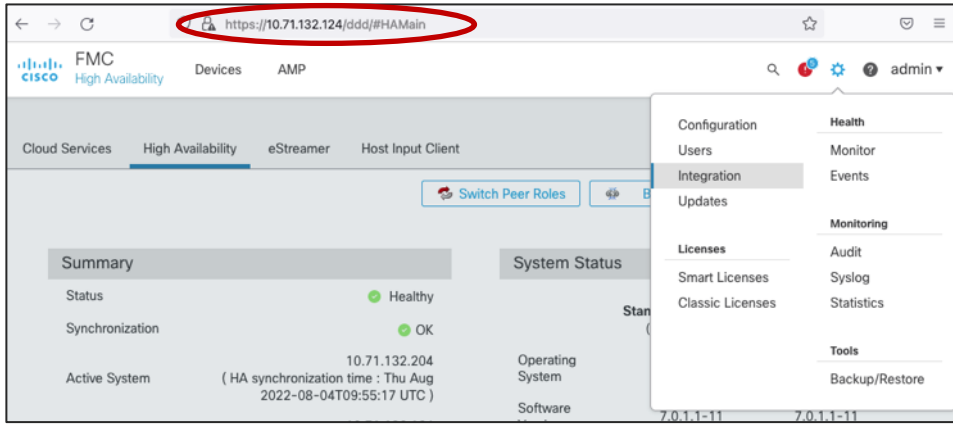
Standby FMC でのメニュー無効化の確認

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



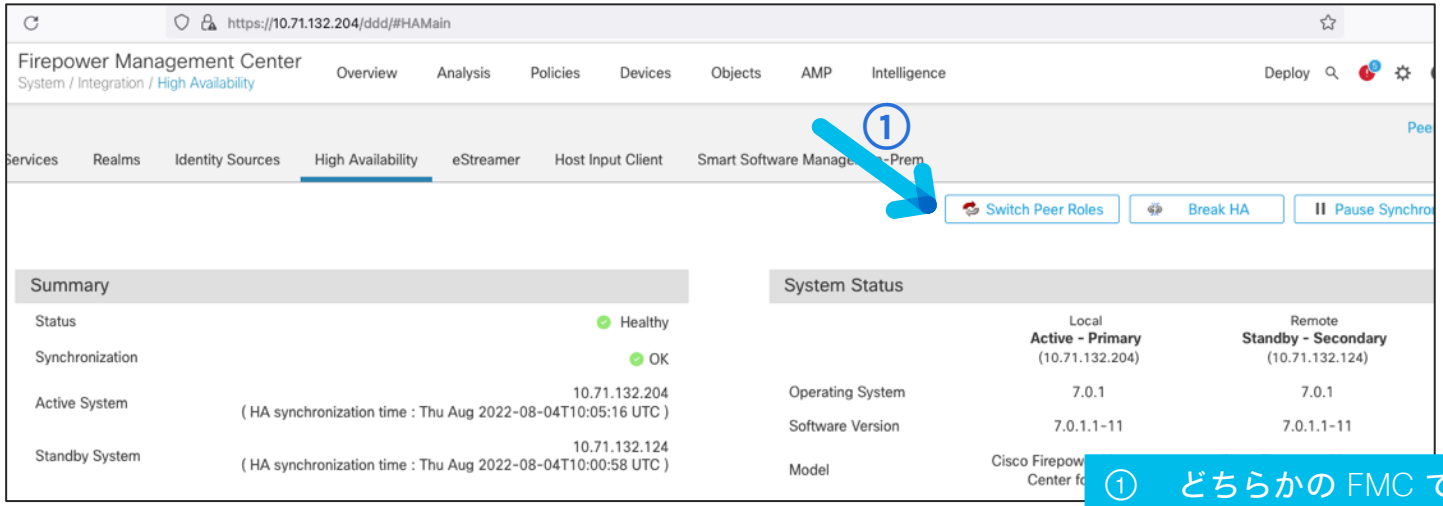
Standby FMC

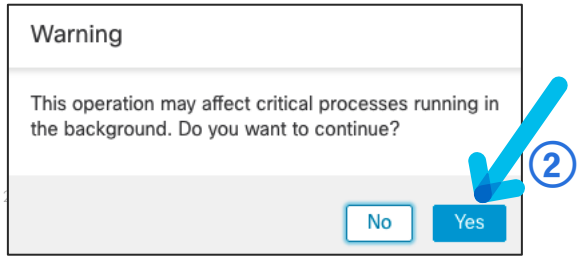


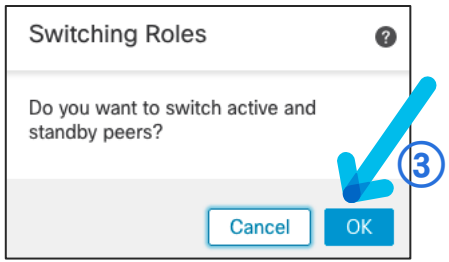
Standby FMC の方がクリックできるメニューが少ないことがわかる

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

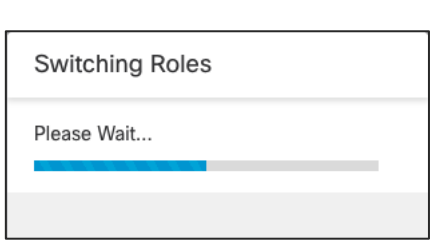


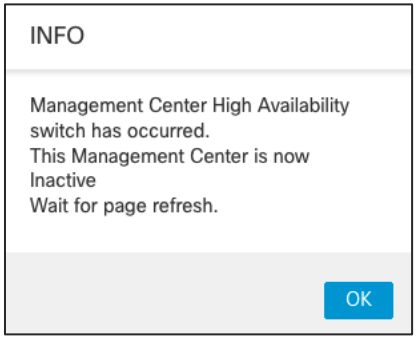




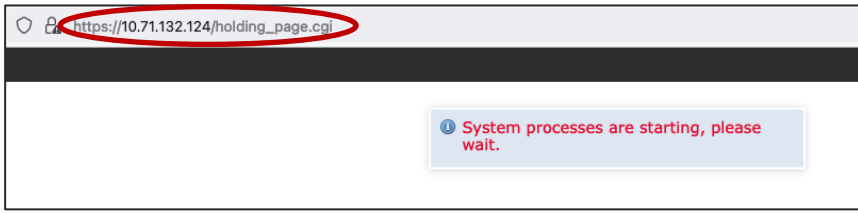
① どちらかの FMC で System → Integration → High Availability にある Switch Peer Roles をクリック
② Warning の内容を確認、問題なければ Yes をクリック
③ Switching Roles が始まる旨のメッセージを確認、問題なければ OK をクリック

FMC HA の Active / Standby 切り替え②

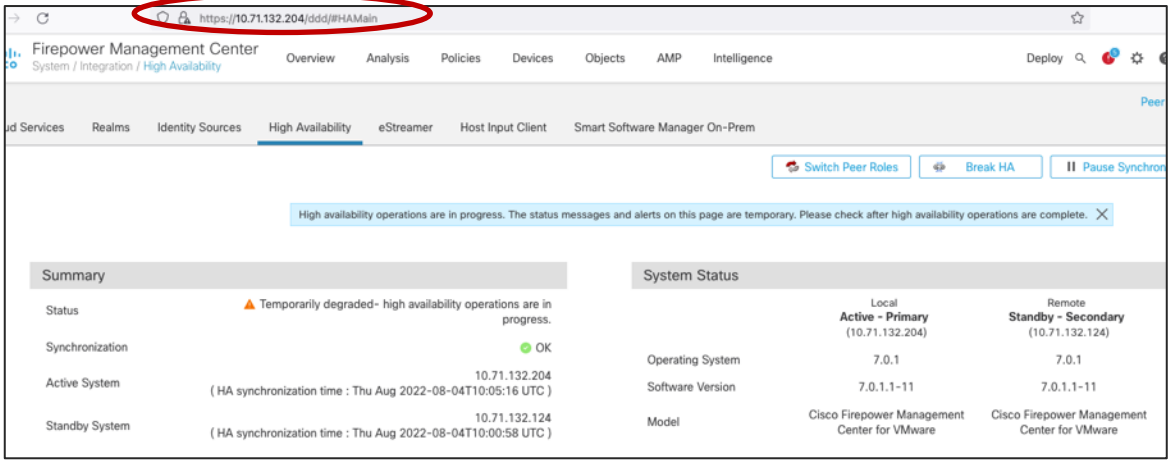




新 Active FMC



新 Standby FMC

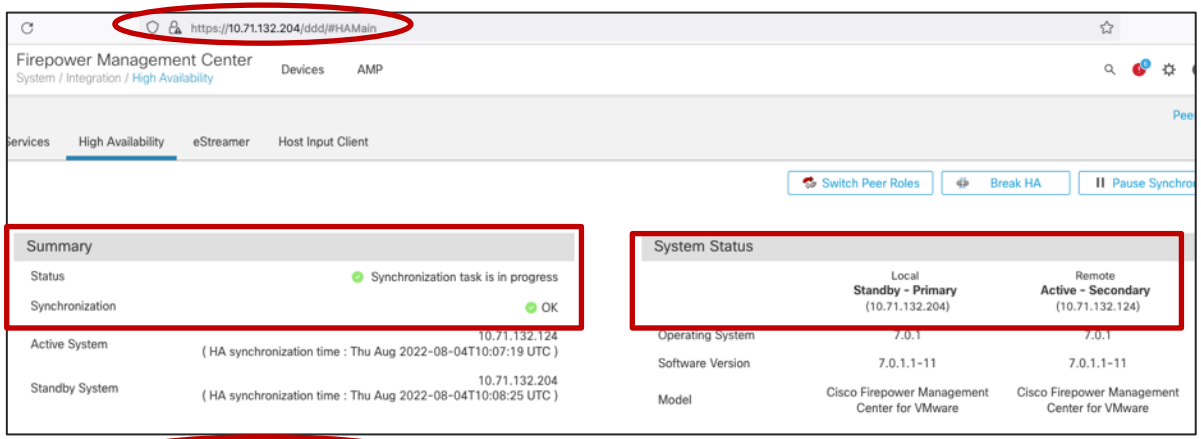


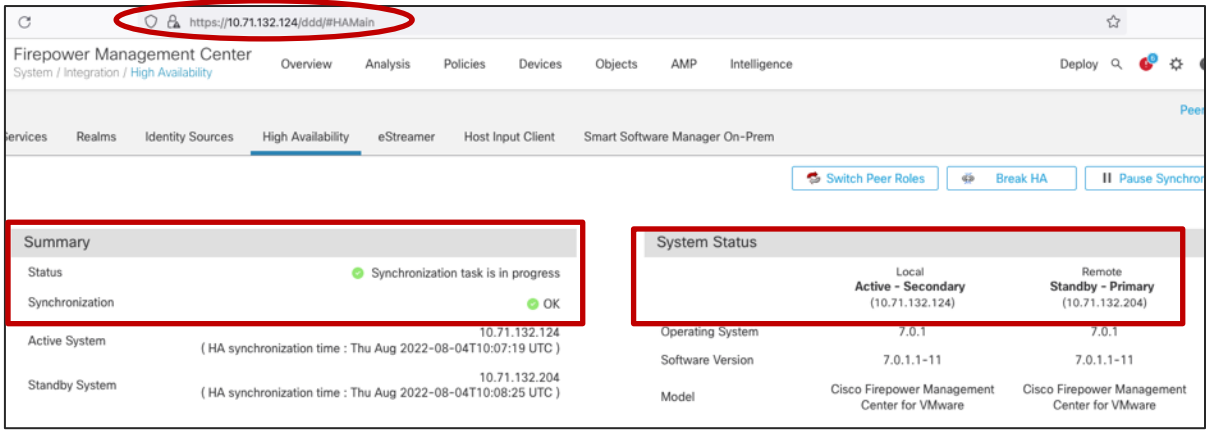
FMC の Active / Standby 切り替わりが開始され、旧 Standby FMC は Active に昇格するタスクが発生、旧 Active FMC はその後に Standby への移行が始まる

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 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

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

The bridge to possible