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. 1 初期インストール編

Rev 2.0

August 2022

シスコシステムズ合同会社

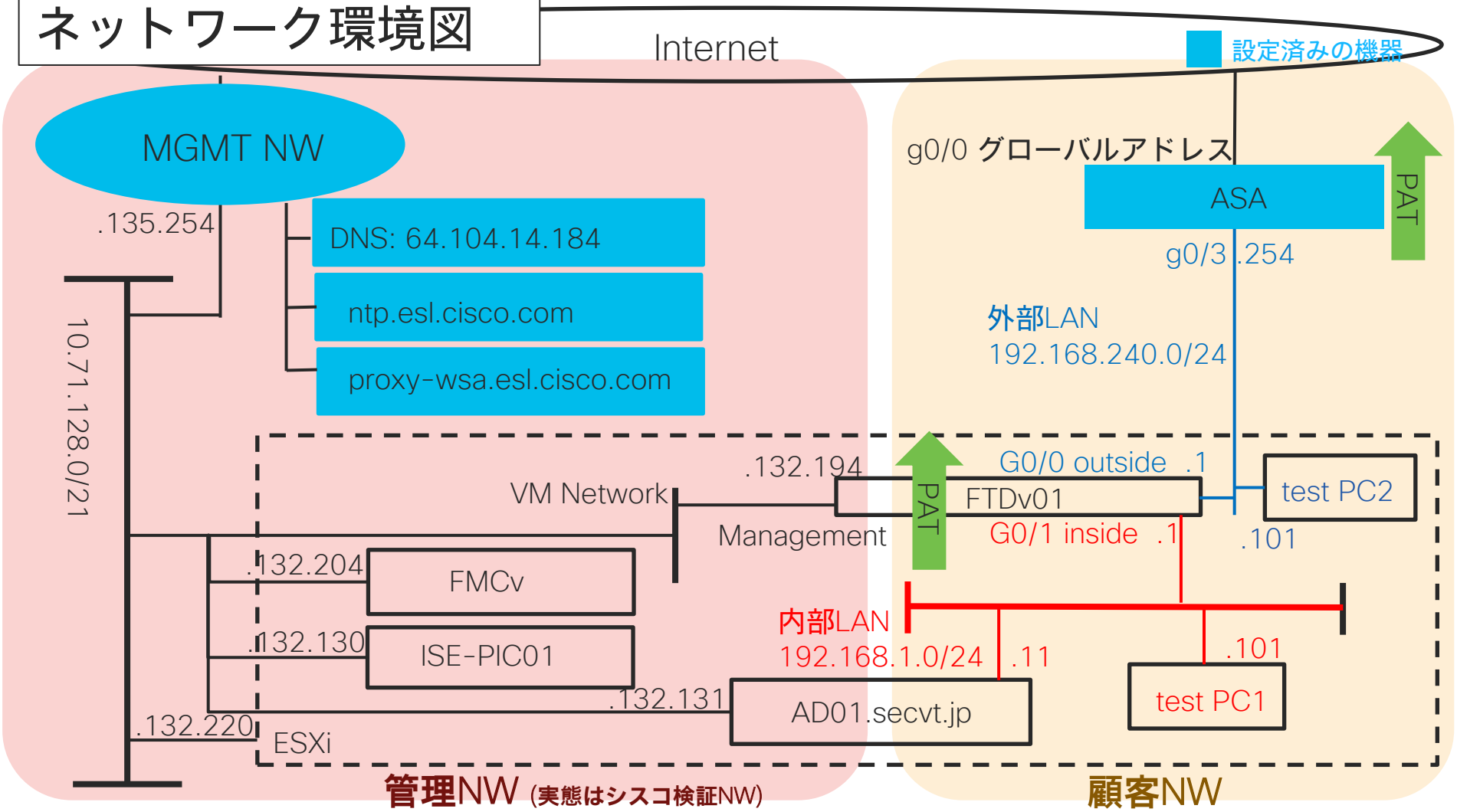
はじめに

- 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. 1 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. 1) のシナリオ

- FMCv と FTDv をインストールし、FTDv を Routed Firewall として設定する。
- (Option) FTDv ではなく Firepower アプライアンスを FTD として使う場合には、その設定をする。
- FMC と FTD の基本の設定を行う。
- シグニチャ (Snort ルール) や各種 DB の更新を設定する。
- スマートライセンスを適用する。
- FMC と FTD に適切な Upgrade / Patch をインストールする。

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:当ガイド) 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

Vol. 4 (管理・監視・冗長構成編) 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

1. FMC と FTD の初期インストール

FMC, FTD のインストールからデバイス登録までの流れ

設定の順序

Firewall Management Center

① OVF のデプロイ (FMCv の場合)
② CLI での初期設定
③ Web GUI での初期設定

Firewall Threat Defense

① OVF デプロイ (FTDv の場合) or FXOS での FTD インストール (FP4k/9k の場合0
② CLI での初期設定
③ FMC への登録キーの設定

Firewall Management Center

① FTD の登録

1-1. FMCv の初期インストール

FMCv の OVF デプロイ

https://software.cisco.com/ から”Software Download”に進む。

Select a Product のテキストフィールドで Firepower Management Center と入力する。結果表示される選択肢の中からここでは Firepower Management Center Virtual Appliance を選択。Firepower Management Center Software を選択し FMC の tar ファイルを取得し展開する。

ソフトウェアはその時適切なものを選択すること。

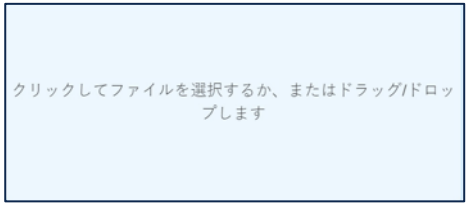
vSphere Client で展開した OVF をデプロイしていく

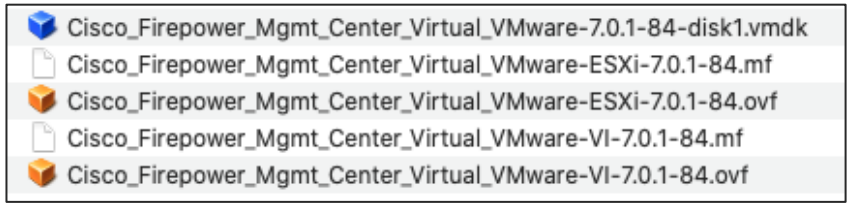
仮想マシンの作成/登録から OVF ファイル.... を選んで「次へ」をクリック

FMCv の OVF デプロイ

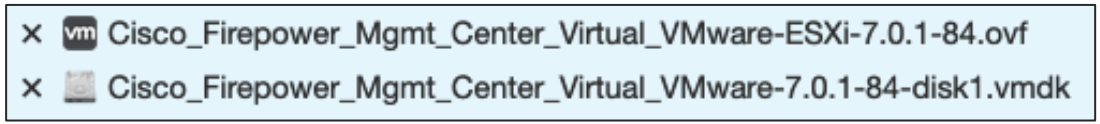
FMCv に名前をつける

同じ画面で以下をクリックし先ほど展開した OVF と VMDK を選択し Next をクリック





ファイル名に VI と入っているものは今回は使わない
(Day0 config 設定時に利用)

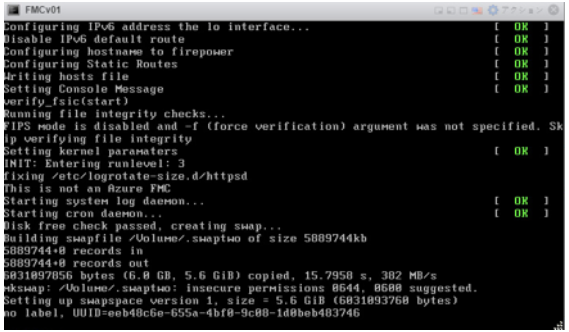


FMCv の OVF デプロイ

FMC は管理用に仮想 NIC を1つ持つため、管理ネットワークに所属

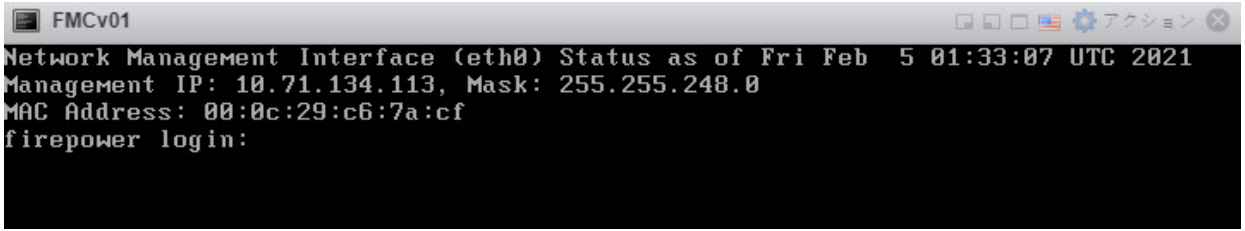
その他デフォルトの設定値でデプロイ (ディスクプロビジョニングは「シン」で良い)

CLI でインストール状況を確認



FMC の CLI での初期設定

FMC のインストールが完了すると CLI にログインプロンプトが出る。IP アドレスは DHCP クライアントで取得されるか 192.168.45.45 が割り当てられるが、初期の CLI で変更可能。



Login: admin　Password: Admin123 でログイン。EULA の表示の後に強制パスワード変更が実施される。以前のバージョンに比べて、パスワード強度の条件が厳しくなっているので注意

FMC の CLI での初期設定

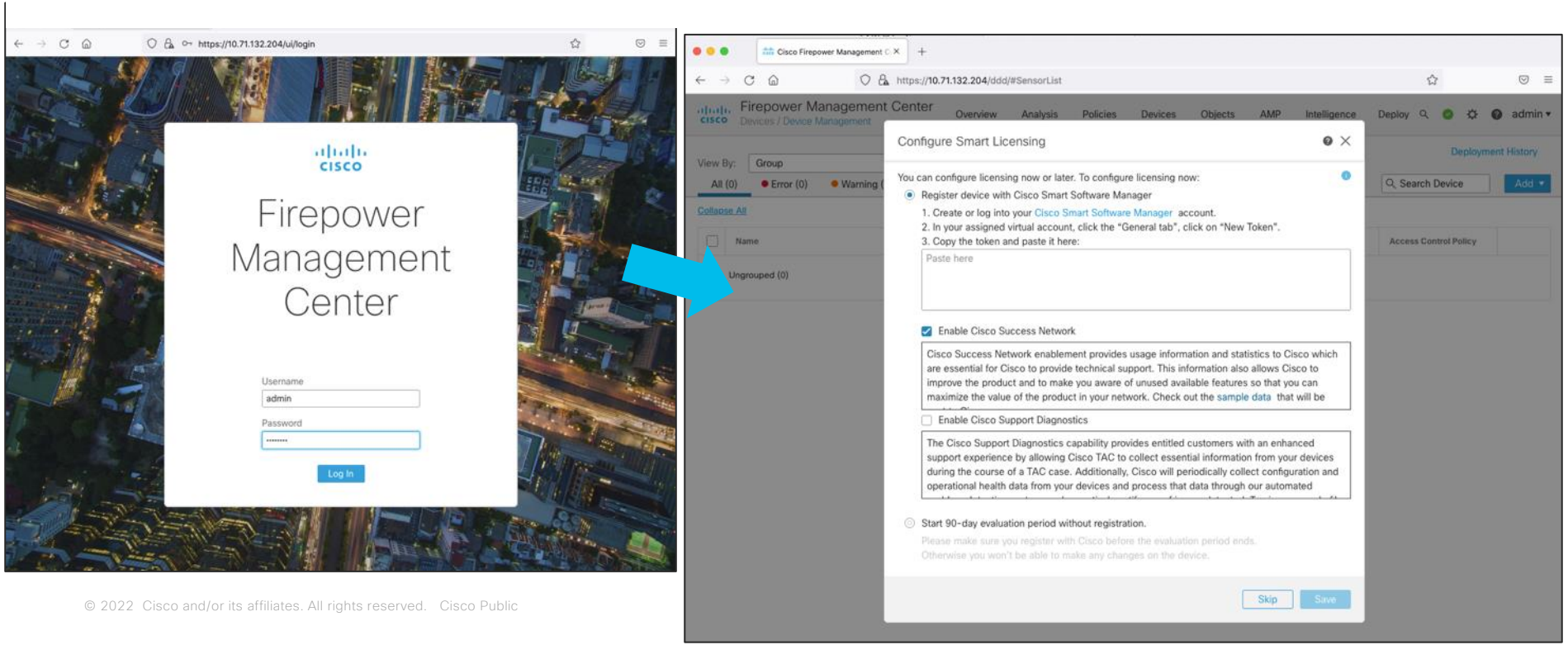
パスワード変更後、会話式セットアップが始まる。DHCP にて取得した情報の一部 (ネットマスクやデフォルトゲートウェイ等) をそのまま利用することも可能

```
Enter a hostname or fully qualified domain name for this system [firepower]: FMC
v01
Configure IPv4 via DHCP or manually? (dhcp/manual) [dhcp]: manual
Enter an IPv4 address for the management interface [10.71.134.113]: 10.71.132.20
4
Enter an IPv4 netmask for the management interface [255.255.248.0]:
Enter the IPv4 default gateway for the management interface [10.71.135.254]:
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220
.220]: 10.71.132.131
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.source
fire.pool.ntp.org]: ntp.esl.cisco.com

Hostname:                               FMCv01
IPv4 configured via:                    manual configuration
Management interface IPv4 address:      10.71.132.204
Management interface IPv4 netmask:      255.255.248.0
Management interface IPv4 gateway:      10.71.135.254
DNS servers:                            10.71.132.131
NTP servers:                            ntp.esl.cisco.com

Are these settings correct? (y/n) _
```

セットアップが終わったら、設定した IP アドレスにブラウザでアクセス。
今回は https://10.71.132.204 にアクセス

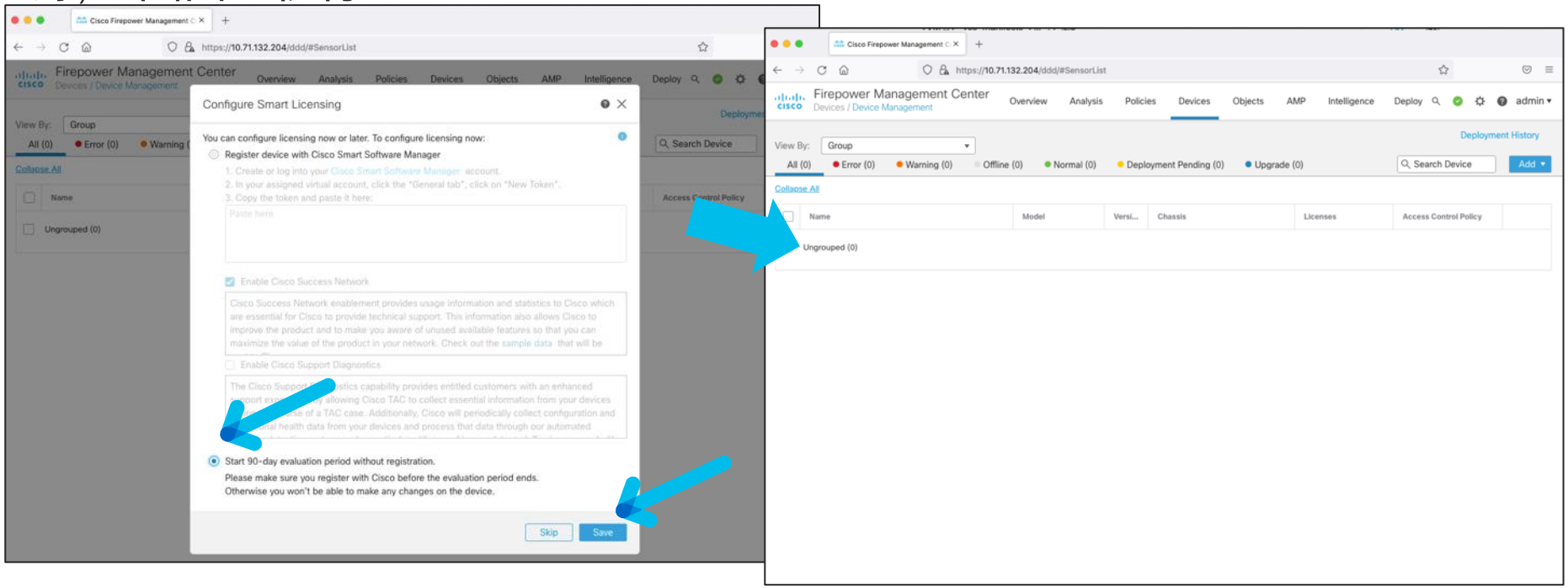
FMC の Web GUI 初期設定

変更した admin のパスワードでログインすると Web GUI にアクセスできる



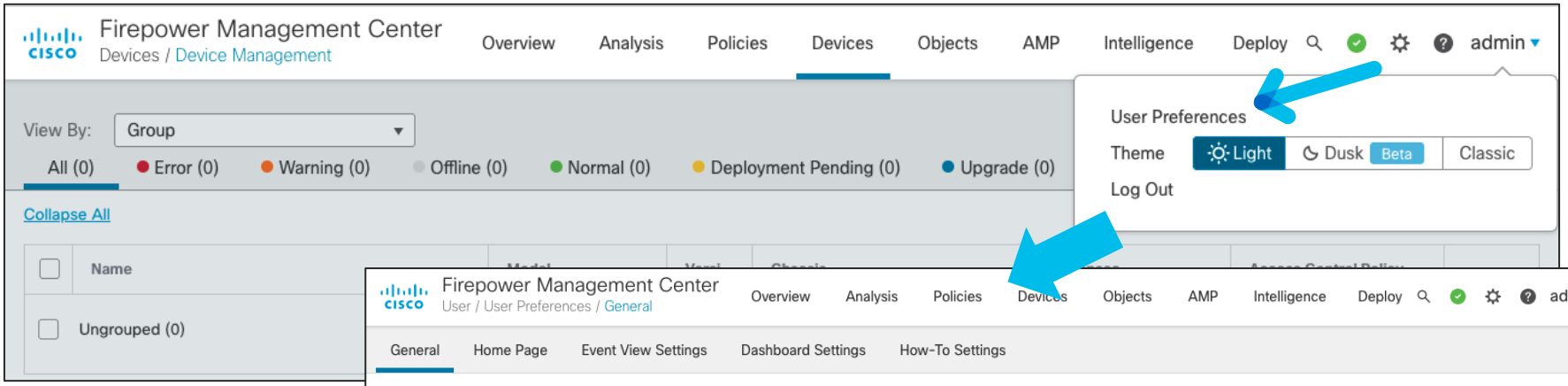
FMC の Web GUI 初期設定

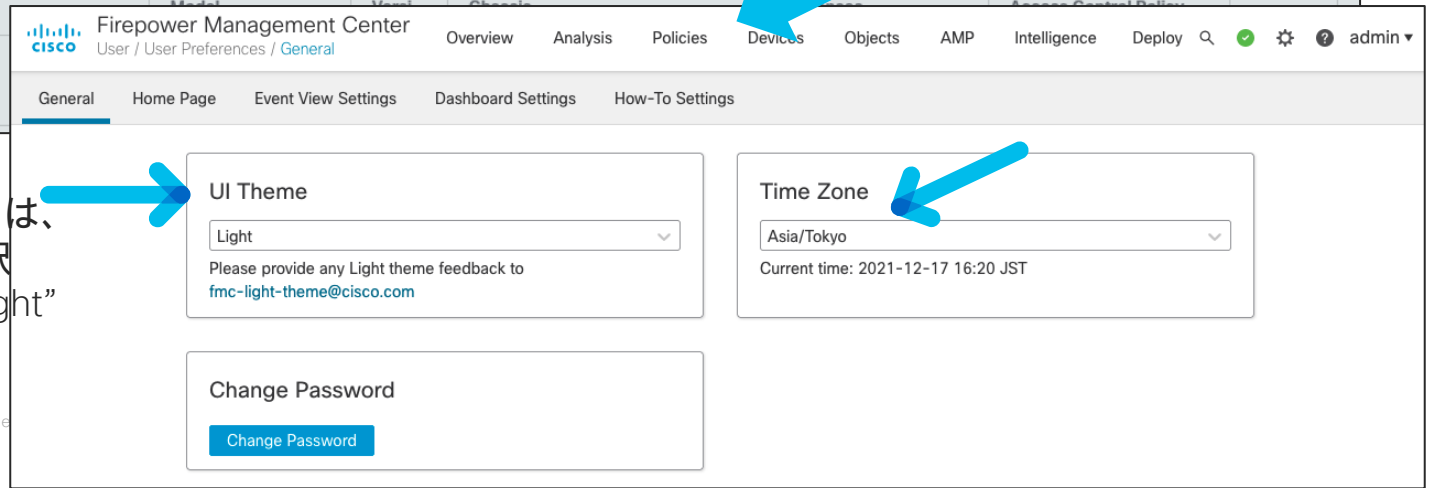
FMC インストール後から 90日間はライセンス登録無しで評価が可能なため、そちらを選択し、Save をクリックすると、デバイス一覧(未登録)の画面に移行する



FMC の Web GUI 初期設定

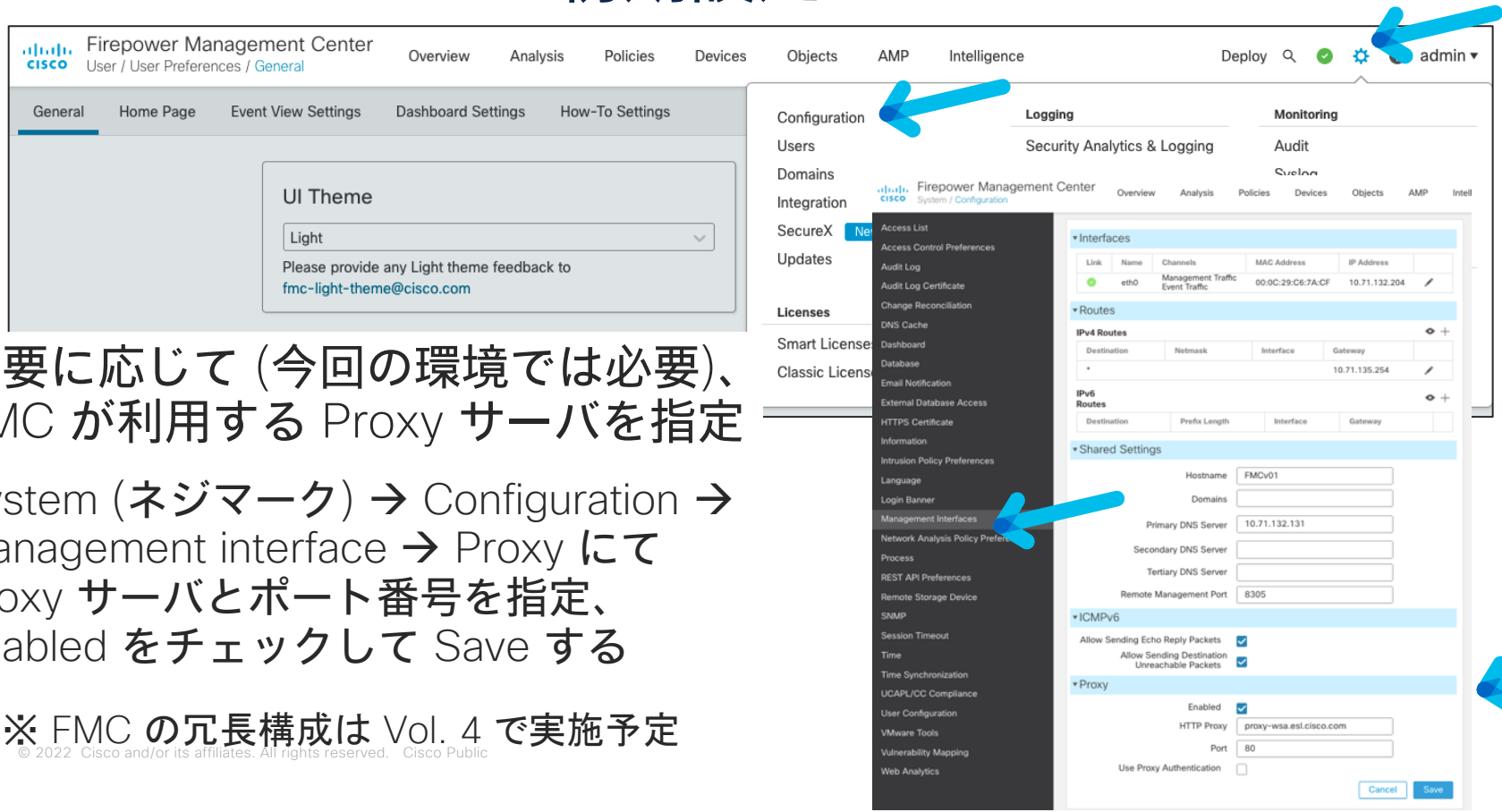
admin → User Preferences から、admin ユーザのタイムゾーンを設定





Version6.4 以前の FMC の Web GUI を使いたい場合には、こちらから ”Classic” を選択
当ガイドは新 UI である ”Light” を利用

FMC の Web GUI 初期設定



必要に応じて (今回の環境では必要)、
FMC が利用する Proxy サーバを指定

System (ネジマーク) → Configuration → Management interface → Proxy にて Proxy サーバとポート番号を指定、Enabled をチェックして Save する

※ FMC の冗長構成は Vol. 4 で実施予定

1-2. FTDv の初期インストール

FTDv の OVF デプロイ

https://software.cisco.com/ から ”Software Download” に進む。

Select a Product のテキストフィールドで Firepower Threat DefenseやNGFW と入力する。結果表示される選択肢の中からここでは Firepower NGFW Virtual を選択。Firepower Threat Defense (FTD) Software を選択し FTD の tar ファイルを取得し展開する。

- ソフトウェアバージョンはその時適切なものを選択すること。

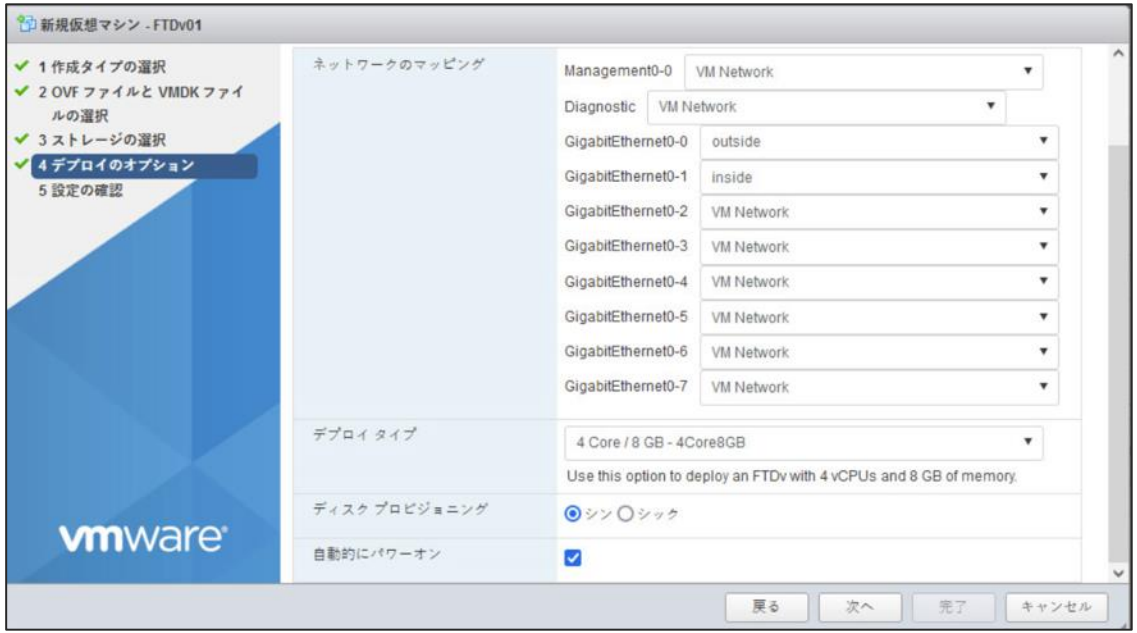
FMC と同じ要領で OVF と VMDK ファイルを選んでデプロイを進める

FTDv の OVF デプロイ

Management0-0 と Diagnostic インタフェースを管理ネットワークに所属させ、Gi0-0 は outside ネットワークに、Gi0-1 は inside ネットワークに所属させる (ESXi 上のネットワークは作成済とする)。

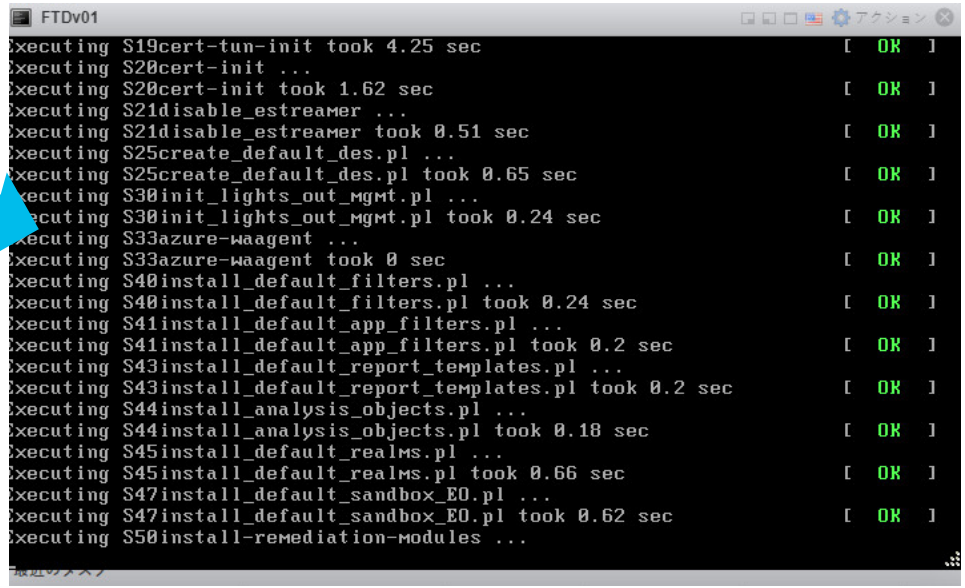
その他のインターフェイスは、現時点では使わないので適当なネットワークに割り当てる。

デプロイタイプで必要な Core とメモリを割り当てる。ディスクプロビジョニングはシンのままで良い。自動的にパワーオンの設定は任意。



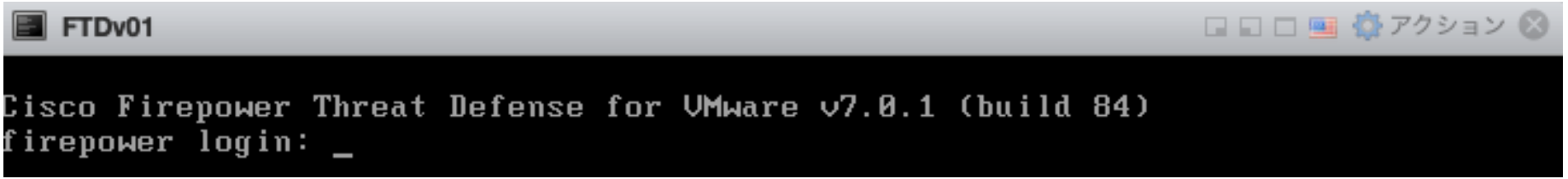
FTDv の OVF デプロイ

内容を確認し、問題なければ「完了」をクリックしてデプロイを開始。電源を入れ、CLI でインストール状況を確認。

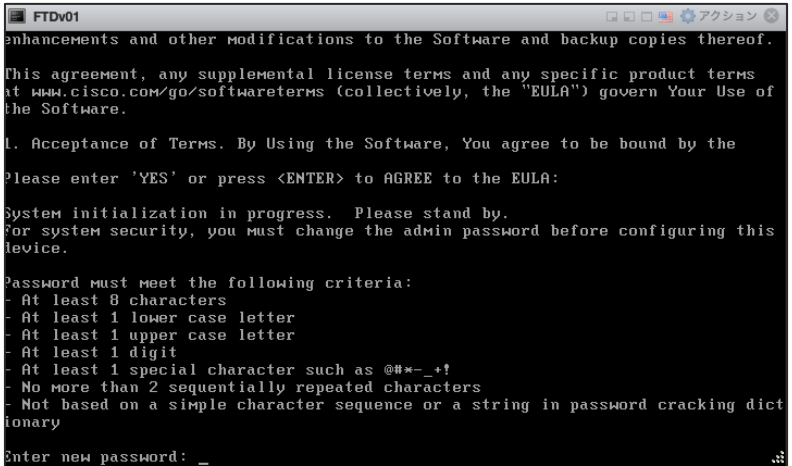


FTD の CLI での初期設定

FTD のインストールが完了すると CLI にログインプロンプトが出る。



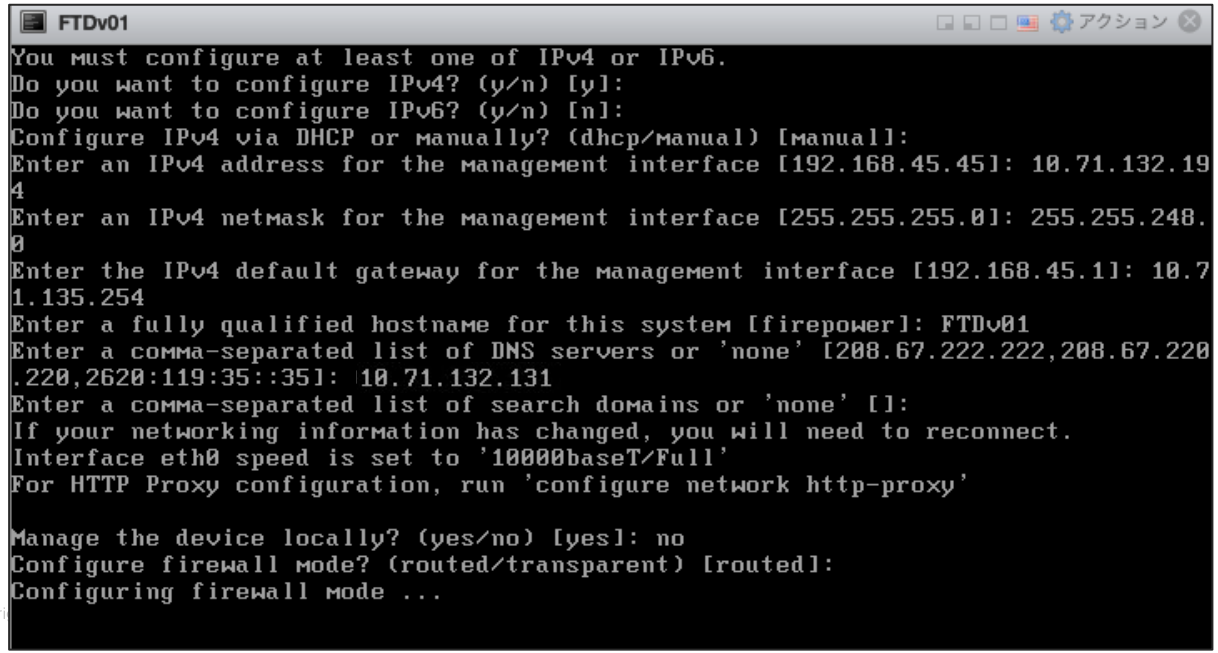
Login: admin　Password: Admin123 でログイン。EULA の表示の後に強制パスワード変更が実施される。以前のバージョンに比べて、パスワード強度の条件が厳しくなっているので注意。



FTD の CLI での初期設定

パスワード変更後、会話式セットアップが始まる。IP アドレスはデフォルトで 192.168.45.45 が付与されているので、これを変更する。

Manage the device locally は No とすることで FMC 管理となる。Firewall Mode は今回は routed とする。



FTD での FMC レジスト設定と Proxy 指定

FTD の CLI から以下のコマンドを使い、FMC へのデバイス登録の設定を行う
後述の FMC から FTD をデバイス登録する際に、この登録キー（この例では “cisco”）が一致している必要あり

> configure manager add <ip address> <key>

```
> configure manager add 10.71.132.204 cisco
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

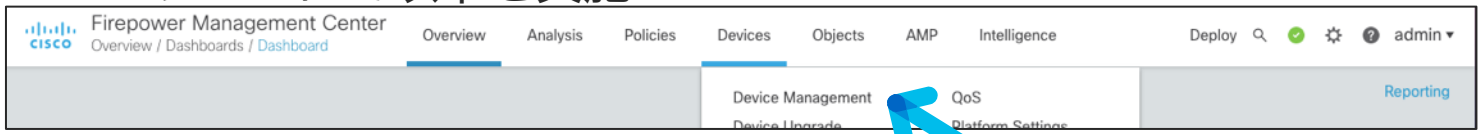
FTD の Proxy 指定は CLI で実施する必要あり。Proxy サーバの IP アドレスとポート番号を指定する

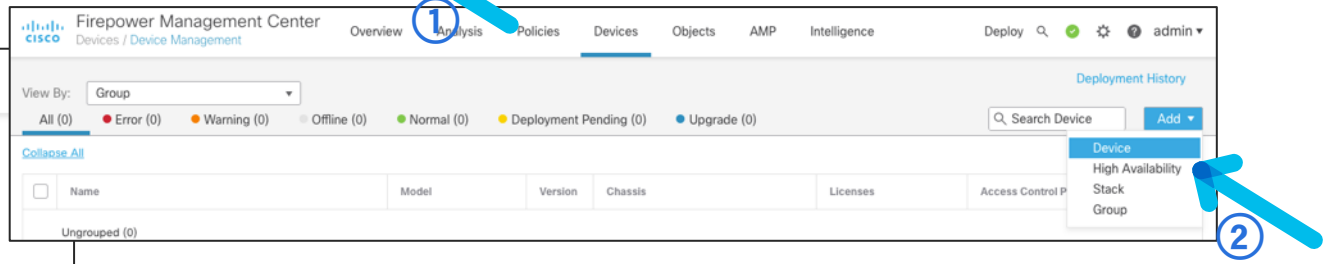
> configure network http-proxy

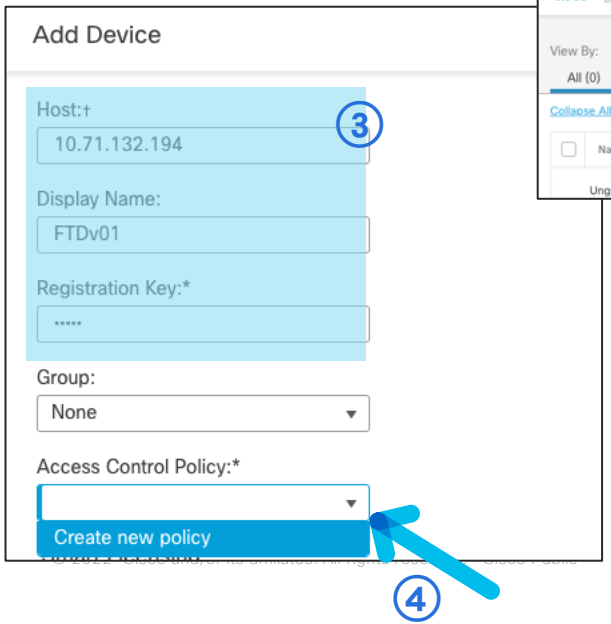
```
> configure network http-proxy

Manual proxy configuration
Enter HTTP Proxy address: 64.104.59.6
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]:


Configuration successfully saved.
```

FMC での FTD デバイス登録

FMC の GUI にて以下を実施

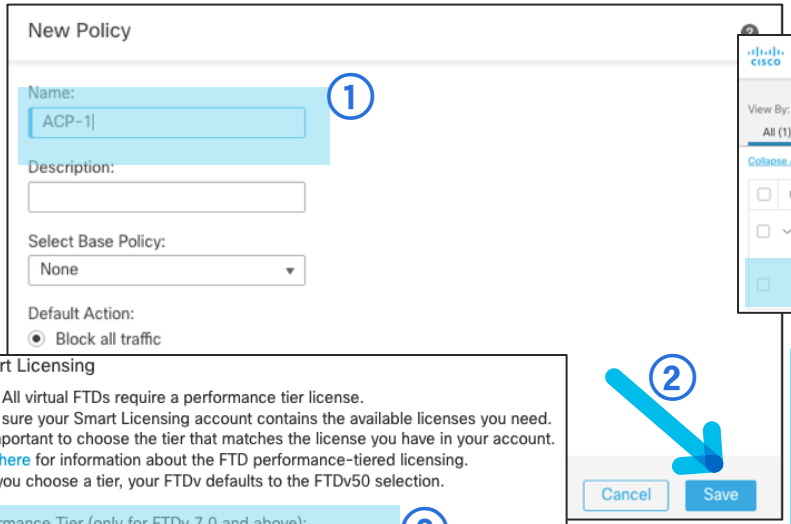


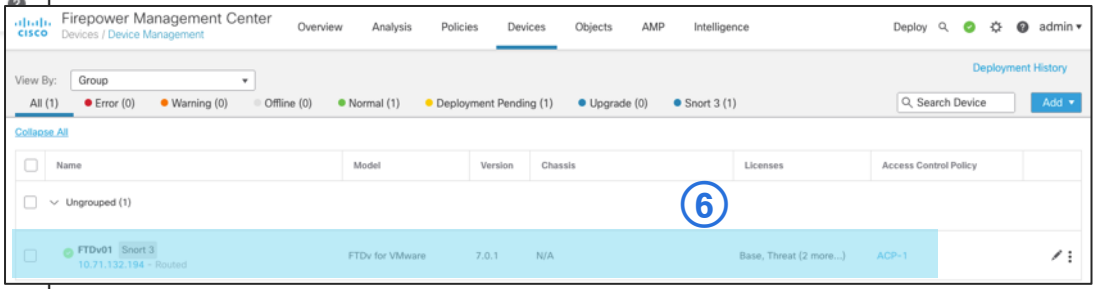




① Devices → Device Management を選択
② Add → Device を選択
③ FTD の IP アドレスと表示名、登録キー (今回の例では “cisco” を入力。入力時にデータはマスクされる)
④ “Create new Policy” を選択
引き続き、次のスライドを参照

FMC での FTD デバイス登録





① この FTD デバイスに適用する Access Control Policy を新規に作成するための名前を指定。他パラメータは現時点ではデフォルトで良い
② “Save” を選択
③ FTDv のサイジングを決定 (Ver 7.0 からの新機能)
④ この FTD デバイスで利用するライセンスを指定、今回はすべてにチェック
⑤ Register を選択し、FTD デバイス登録を実行
⑥ 上記のようになれば、デバイスの登録完了(所要時間:数分)

以上で、インストール と FTD を FMC で管理するための初期設定は完了
以降の設定はすべて FMC の画面から実施 (例外を除く)

※ FTD の冗長構成は Vol. 4 で実施予定

FTD – FMC 間のトンネル (sftunnel) が張れない場合

- 登録キーは正しいですか? 再度入力してみましょう
- お互いの機器から Ping は飛びますか? 飛ばない場合は IP アドレスの確認や経路上の機器の確認、または Mgmt ポートに正しく接続されてるかケーブルの確認もしてみましょう
- ポート番号への通信は制限されて無いですか? Ping は飛ぶけどトンネルが張れない場合はトンネルを貼るためのポート番号への通信が制限されてる可能性があるので、経路上の機器で制限されていないかチェックしてみましょう
  - sftunnel のデフォルトポートは ”8305”
  - 非推奨だが、変更することも可能
    - FTD > ”configure network manage-port [port#]”
    - FMC > “Configure > Management Interfaces > Shared Settings” 配下で変更可能。ただし FMC での場合はすべての FTD に影響するため注意が必要

1-3. (Option) FPR4100/9300シリーズの初期インストール

*FTD を FPR4100/9300 シリーズで設定する場合の参考情報

FMC, FTD(FPR4k,9k) のインストールからデバイス登録までの流れ

設定の順序

Firewall Management Center

① OVF のデプロイ (FMCv の場合)
② CLI での初期設定
③ Web GUI での初期設定

Firewall Threat Defense

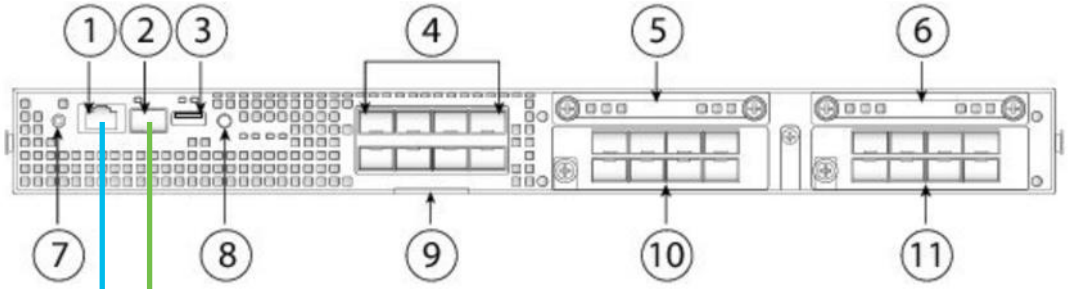
① FXOS を CLI で初期設定
② FXOS アップグレード ※
③ FTD インストール ※
④ FMC への登録キーの設定

※ FXOS, FTD のイメージは購入時にシャーシ内に格納されており、FTD のインストールは必須ですが、FXOS の方は FTDバージョンを変更した際に互換性に応じて適宜確認・アップグレードが必要です。

Firewall Management Center

① FTD の登録

HW (FPR4100 シリーズ)



管理ネットワーク

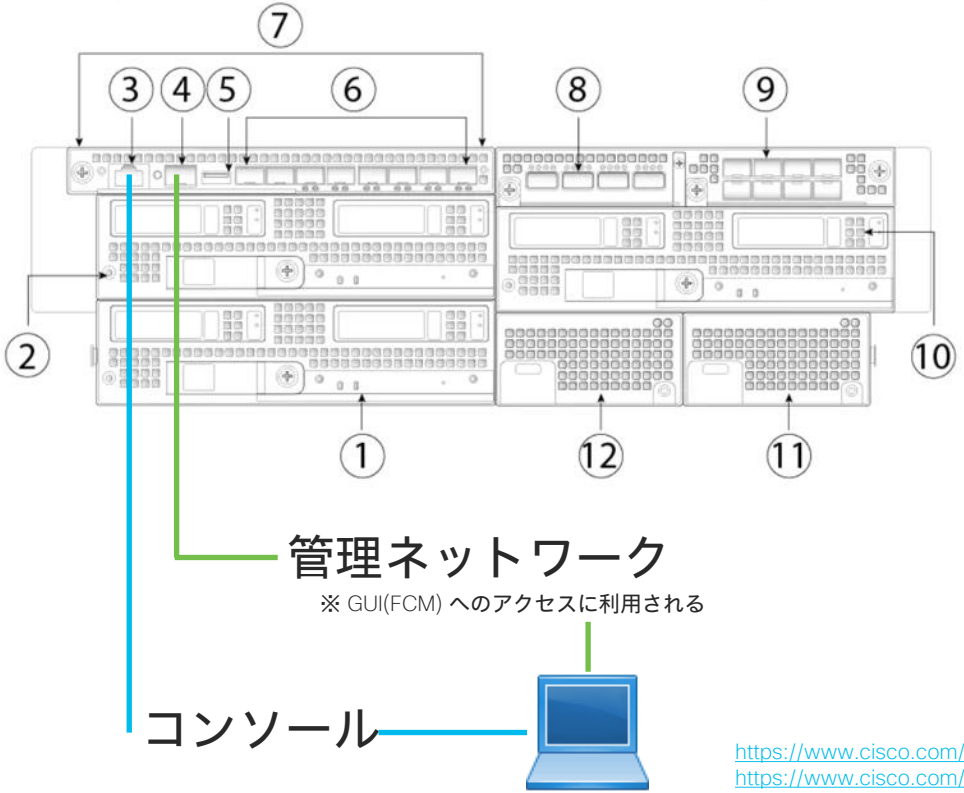
※ GUI (FCM) へのアクセスに利用される

コンソール

①RJ45 コンソールポート
②管理ポート (SFP)
③USB 2.0 タイプ A ポート
④8つの固定 SFP+ ポート
⑤SSD1 (必須)
⑥SSD2 (MSP 用)
⑦電源 LED
⑧ロケータ LED
⑨アセットカード
⑩ネットワークモジュール
⑪ネットワークモジュール

https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5.html
https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100.html
https://www.cisco.com/c/ja_jp/td/docs/security/firepower/41x5/hw/guide/install-41x5.htmll
https://www.cisco.com/c/ja_jp/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100.html

HW (FPR9300 シリーズ)



①セキュリティモジュール 3
②セキュリティモジュール 1
③RJ45 コンソールポート
④管理ポート (SFP)
⑤2.0 USB ポート
⑥10G データポート
⑦スーパバイザ
⑧ネットワークモジュール 1
⑨ネットワークモジュール 2
⑩セキュリティモジュール 2
⑪電源モジュール (PSU2)
⑫電源モジュール (PSU1)

https://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300.html
https://www.cisco.com/c/ja_jp/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300.html

FXOS を CLI で初期設定

FPR4100/9300 共通
デフォルト ユーザ名/パスワード : admin/cisco123

```
---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.


-----省略------

  Switch Fabric=A
  System Name=FPR41 4 5                          ← システム名
  Enforced Strong Password=yes                   ← 強力なパスワード (yes/no)
  Supervisor Mgmt IP Address=10.71.132.193       ← 管理用ポートに設定する管理用 IP
  Supervisor Mgmt IP Netmask=255.255.248.0       ← 管理用 IP マスク
  Default Gateway=10.71.135.254                  ← 管理用 IP のデフォゲ
  SSH Mgmt Access Configured=yes                 ← 管理用 IP への SSH アクセス許可の有無
    SSH Mgmt Access IP Address=0.0.0.0           ← SSH アクセスを許可するサブネットを指定 ※0.0.0.0=any
    SSH Mgmt Access IPv4 Netmask=0.0.0.0         ← SSH アクセス向け IP マスク
  HTTPS Mgmt Access Configured=yes               ← 管理用 IP への HTTPS アクセス許可の有無
    HTTPS Mgmt Access IP Address=0.0.0.0         ← HTTPS アクセスするサブネットを指定※0.0.0.0=any
    HTTPS Mgmt Access IPv4 Netmask=0.0.0.0       ← HTTPS アクセス向け IP マスク

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

.....  Configuration file - Ok
```

【参考】FXOS アップグレード

FTD をバージョンアップする場合は、その下で動いている FXOS のバージョンとの互換性が必要なため、まずは互換性ガイドをチェック（下記ガイドの table2）

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html

インストールされている FXOS バージョンが利用する FTD バージョンと互換性がない場合はアップグレードないしダウングレードが必要。

Table 2. ASA or FTD, and Firepower 4100/9300 Compatibility

FXOS Version	Firepower Model	ASA Version	FTD Version
2.11(1.154)+ **Note** FXOS 2.11(1.154)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.11(1.154)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	**9.17(x)** (recommended) 9.16(x) 9.15(1) 9.14(x)	**7.1.0** (recommended) 7.0.0 6.7.0 6.6.x
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17(x)** (recommended) 9.16(x) 9.15(1) 9.14(x) 9.13(1) 9.12(x)	**7.1.0** (recommended) 7.0.0 6.7.0 6.6.x 6.5.0 6.4.0
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17(x)** (recommended) 9.16(x) 9.15(1) 9.14(x) 9.13(x) 9.12(x) 9.10(x) 9.9(x) 9.8(x)	**7.1.0** (recommended) 7.0.0 6.7.0 6.6.x 6.5.0 6.4.0 6.3.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

互換性があっても基本的には”recommended” の組合せを推奨。
左記の例でいうと ”Firepower4112” で FTD 7.1.0 を使いたい場合は FXOS2.11(1.154) 以降のバージョンを使用。
注）2.11(1.154)+ の ”+” 表記は 2.11(1.154) 以降という意味

【参考】FXOS アップグレード

【手順】

1. 「fxos-k9.{fxos version}.SPA」を cisco.com からダウンロード
2. FPR4k/FPR9k へ FXOS イメージをアップロード
3. FXOS のアップグレード

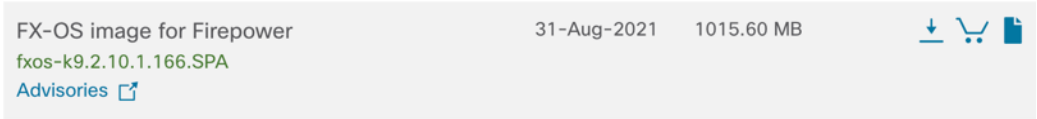
【参考】FXOS アップグレード

【FXOS イメージのダウンロード】

https://software.cisco.com/ から ”Software Download” に進む。

Select a Product のテキストフィールドで Firepower 4100 or Firepower 9300 と入力する。結果表示される選択肢の中からここでは購入した型番を選択。Firepower Extensible Operating System を選択し FXOS の SPA ファイルを取得し展開する。

ソフトウェアは互換性ガイドにある適切なものを選択すること。



【参考】FXOS アップグレード (CLI)

FPR4k/FPR9k へ FXOS イメージをアップロード (3パターン)

1. USB ドライブを使用
   - Firepower-chassis # scope firmware
   - Firepower-chassis /firmware # download image usbA:*image_name*
2. FTP, SCP, SFTP, TFTP を使用
   - Firepower-chassis # scope firmware
   - Firepower-chassis # download image tftp/ftp/scp/sftp://path to the image, including the server root /image name

例:

```
Firepower-chassis# scope firmware
Firepower-chassis /firmware # download image tftp://10.10.10.1/fxos-k9-fpr9k-firmware.1.0.10.SPA
Firepower-chassis /firmware # show download-task fxos-k9-fpr9k-firmware.1.0.10.SPA detail
```

```
FP4K-A /firmware # download image
  ftp:   Location of the image file
  scp:   Location of the image file
  sftp:  Location of the image file
  tftp:  Location of the image file
  usbA:  Location of the image file
  usbB:  Location of the image file
```

【参考】FXOS アップデート

・ダウンロード状況の確認方法 (show download-task detail)

```
FPR4145 /firmware # show download-task detail

Download task:
    File Name: fxos-k9.2.10.1.166.SPA
    Protocol: Tftp
    Server: 10.48.35.1
    Port: 0
    Userid:
    Path: /maizumi
    Downloaded Image Size (KB): 682786
    Time stamp: 2022-02-25T05:04:08.707
    State: Downloading
    Status: Downloading the image
    Transfer Rate (KB/s): 3483.602051
    Current Task: downloading image or file fxos-k9.2.10.1.166.SPA
```

DL してるファイル名

プロトコル

DL サーバ

DL したイメージサイズ

DL 速度

現在の状態
(左記は DL 中の記載)

・ダウンロード完了後の状態 (show download-task)

```
FPR4145 /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid         State
    --------- -------- --------------- ---------- -------------- -----
    fxos-k9.2.10.1.166.SPA
              Tftp     10.48.35.1      0          Downloaded
```

DL 完了

【参考】FXOS アップデート

・DL したパッケージ（イメージ）を確認し、”scope” で ”auto-install” に移動し、インストール

```
FPR4145 /firmware # show package
Name                                       Version
------------------------------------------ -------
fxos-k9.2.10.1.166.SPA                     2.10(1.166)
fxos-k9.2.8.1.143.SPA                      2.8(1.143)
FPR4145 /firmware # scope auto-install
FPR4145 /firmware/auto-install # install platform platform-vers 2.10(1.166)
This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
Do you want to proceed? (yes/no):yes
```

ここの例では DL した 2.10(1.166) をインストール

”scope firmware” で system に移動してから show firmware monitor でアップグレード状況の確認

```
FPR4145 /system # show firmware monitor
FPRM:
    Package-Vers: 2.10(1.166)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.6(1.224)
    Upgrade-Status: Upgrading

Chassis 1:
    Server 1:
        Package-Vers: 2.6(1.224)
        Upgrade-Status: Ready
```

Fabric, FPRM, Chassis の3つが順番にアップグレード

【参考】FXOS アップグレード (GUI)

FPR4k/FPR9k へ FXOSイメージをアップロード (3パターン)

3. GUI(FCM) を使用

FCM へログイン > システム > 更新

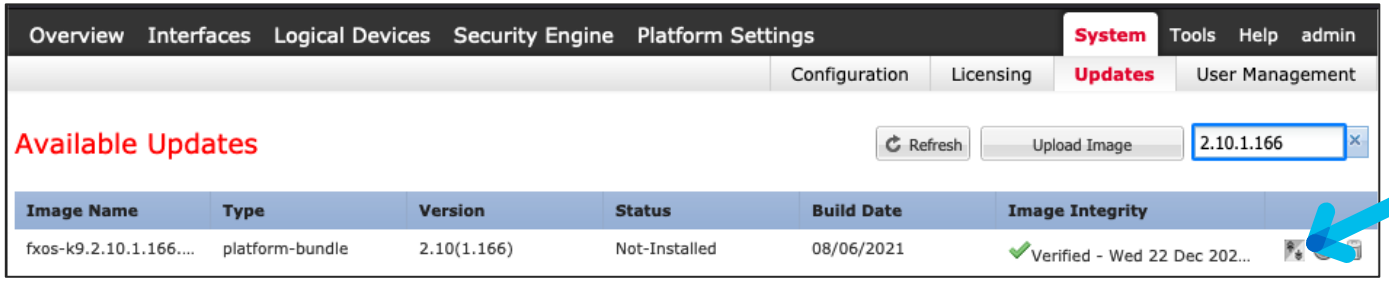
イメージのアップロードをクリック

イメージを選択してアップロードをクリック

アップロード完了

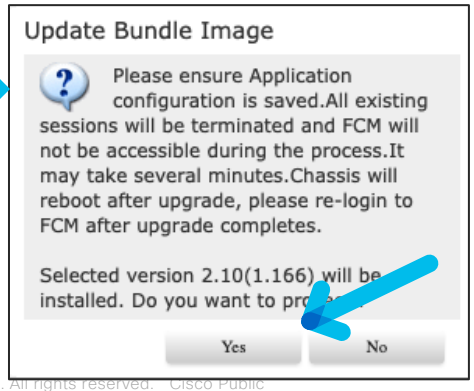
【参考】FXOS アップグレード (GUI)

FXOS アップグレード（システム > 更新）



アップグレードアイコン

をクリック



Yes を選択
その後はバックグラウンドでプロセスが実施され、
自動的に再起動。指定のバージョンで立ち上がってくる

【参考】FXOS バージョンと管理 IP の確認コマンド(CLI)

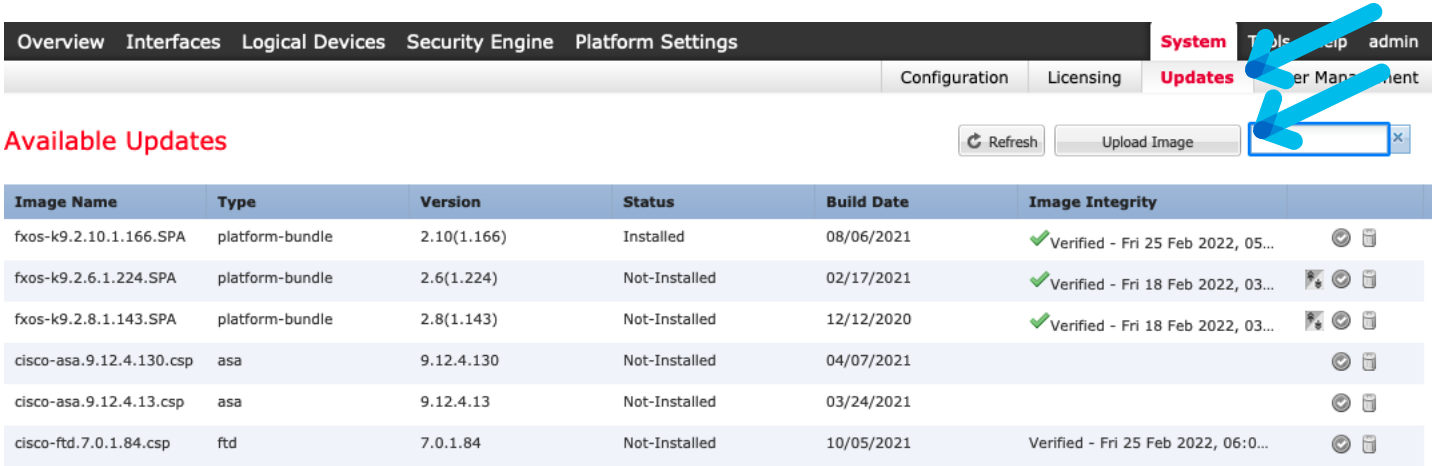
```
Firepower-chassis#
Firepower-chassis # scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show version
Fabric Interconnect A:
    Running-Kern-Vers: 5.0(3)N2(4.101.99)
    Running-Sys-Vers: 5.0(3)N2(4.101.99)
    Package-Vers: 2.10(1.166)
    Startup-Kern-Vers: 5.0(3)N2(4.101.99)
    Startup-Sys-Vers: 5.0(3)N2(4.101.99)
    Act-Kern-Status: Ready
    Act-Sys-Status: Ready
    Bootloader-Vers:
```

```
Firepower-chassis#
Firepower-chassis # scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show
Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB
IPv6 Address OOB IPv6 Gateway Prefix Operability Ingress
VLAN Group Entry Count (Current/Max) Switch Forwarding Path
Entry Count (Current/Max)

    ---- --------------- --------------- ---------------
---------------- ---------------- ------ ---------- --
---------------------------------------- ----------
----------------------------------

    A    10.10.10.1    10.10.10.254    255.255.255.0    ::
::            64     Operable    0/500                          0/
1021
```

FTD イメージアップロード (GUI)

・GUI の場合、FTD イメージのアップロード方法は FXOS と同じ手順で可能

System > Updates > Upload Image



【参考】FTD イメージのアップロード (CLI)

アップロードコマンド、確認コマンドは FXOS と一緒だが、階層が異なる

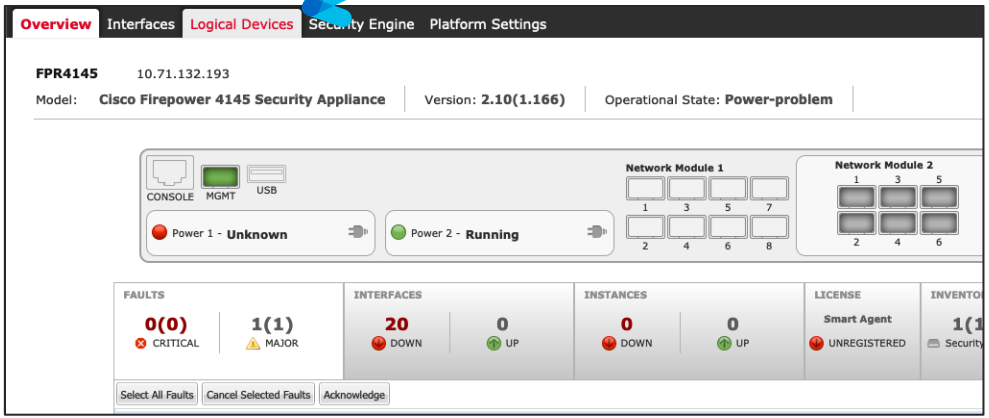
```
FPR4145# scope ssa
FPR4145 /ssa # scope app-software
FPR4145 /ssa/app-software # download image tftp://10.71.136.1/cisco-ftd.7.0.1.84.SPA.csp
FPR4145 /ssa/app-software # show download-task detail

Downloads for Application Software:
    File Name: cisco-ftd.7.0.1.84.SPA.csp
    Protocol: Tftp
    Server: 10.71.136.1
    Port: 0
    Userid:
    Path: /maizumi
    Downloaded Image Size (KB): 89169
    Time stamp: 2022-02-25T06:03:19.193
    State: Downloading
    Status: Downloading the image
    Transfer Rate (KB/s): 3429.576904
    Current Task: downloading image cisco-ftd.7.0.1.84.SPA.csp
```

“show download-task fsm status expand” で詳細を確認可能

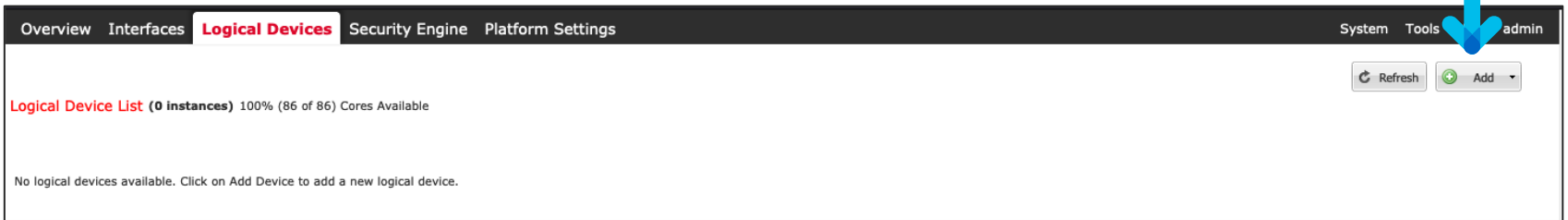
FTD インストール / FMC への登録キーの設定 (GUI)

- FCM (Firepower Chassis Manager) に GUI でログイン

Logical Devices をクリック

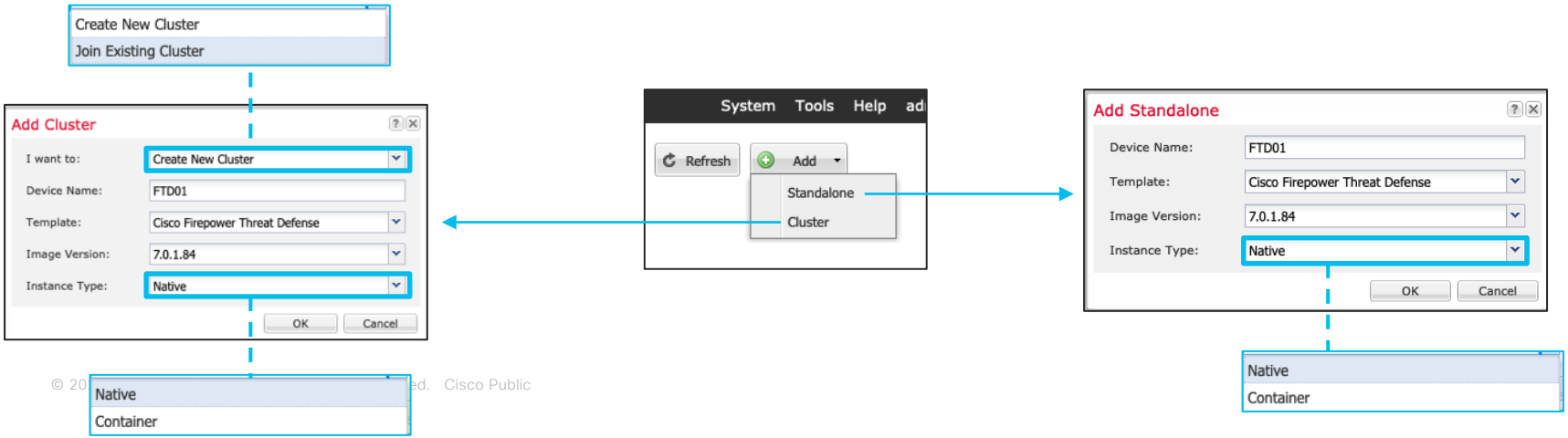


“Add” をクリック



FTD インストール / FMC への登録キーの設定 (GUI)

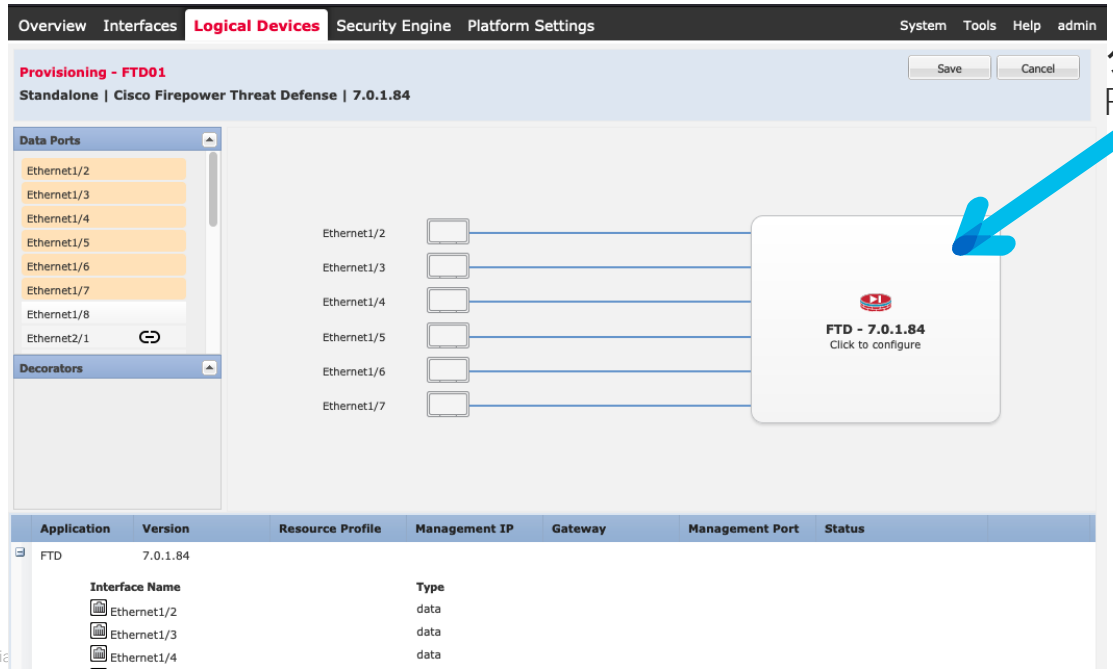
Device types	Instance Type	Description
Standalone	Native	FPR4k, 9k の上に1台の FTD のみを構築
	Container	FPR4k, 9k の上に複数の FTD を構築 (Multi-instance)
Cluster	Native	FPR4k, 9k の上に1台の Cluster 用 FTD を構築
	Container	FPR4k, 9k の上に複数の Cluster 用 FTD を構築 (Multi-instance)



FTD インストール / FMC への登録キーの設定 (GUI)

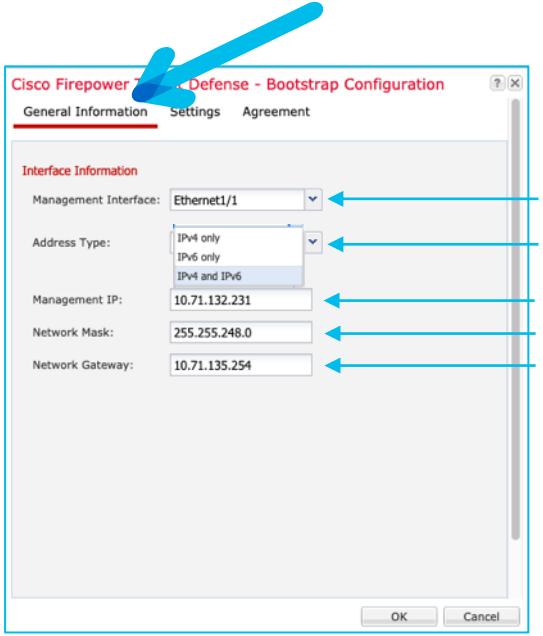
※本資料では Standalone+Native での設定について記載

FTD のデータ通信用インタフェースを
クリックして選択



クリックすると
FTD の初期設定画面に飛ぶ

FTD インストール / FMC への登録キーの設定 (GUI)



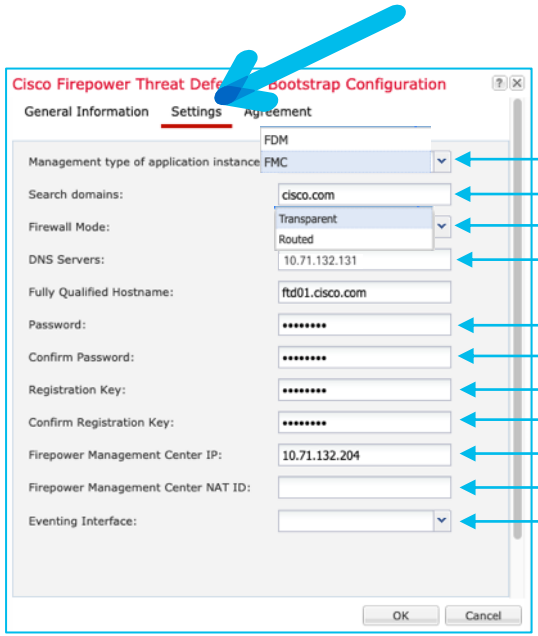
Mgmt インタフェース

アドレスタイプ

Mgmt アドレス

ネットマスク

デフォルトゲートウェイ



※FDM (Firepower Device Manager) = FTD をローカル管理

管理方式 (FDM or FMC)

検索ドメイン

Firewall モード (Transparent or Routed)

DNS サーバ

FTD ログインパスワード

FTD ログインパスワード (確認)

登録キー

登録キー (確認)

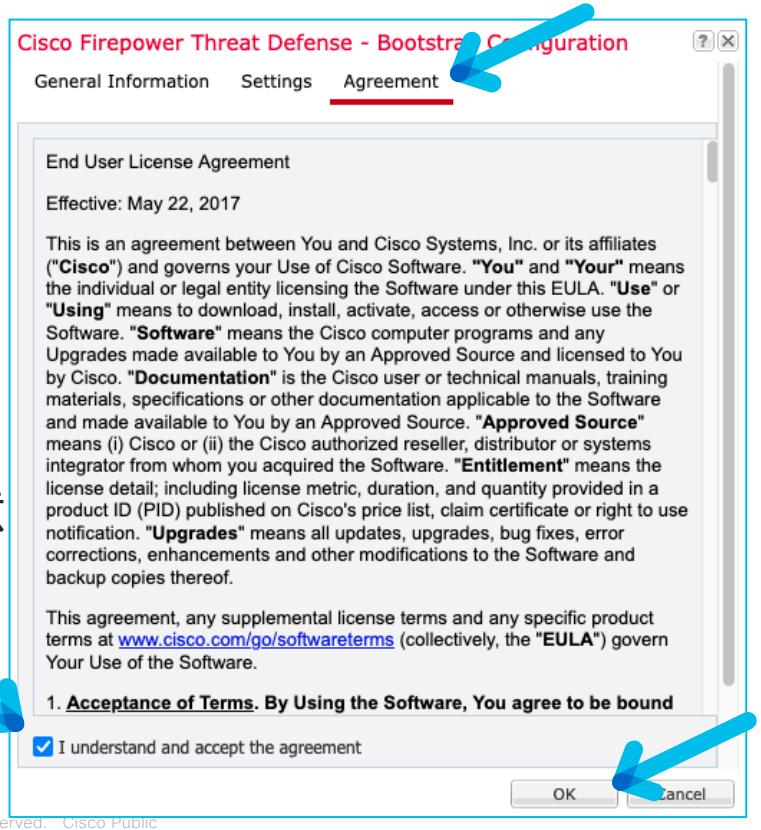
FMC の管理用 IP

FMC NAT ID

イベント専用インタフェースがあれば

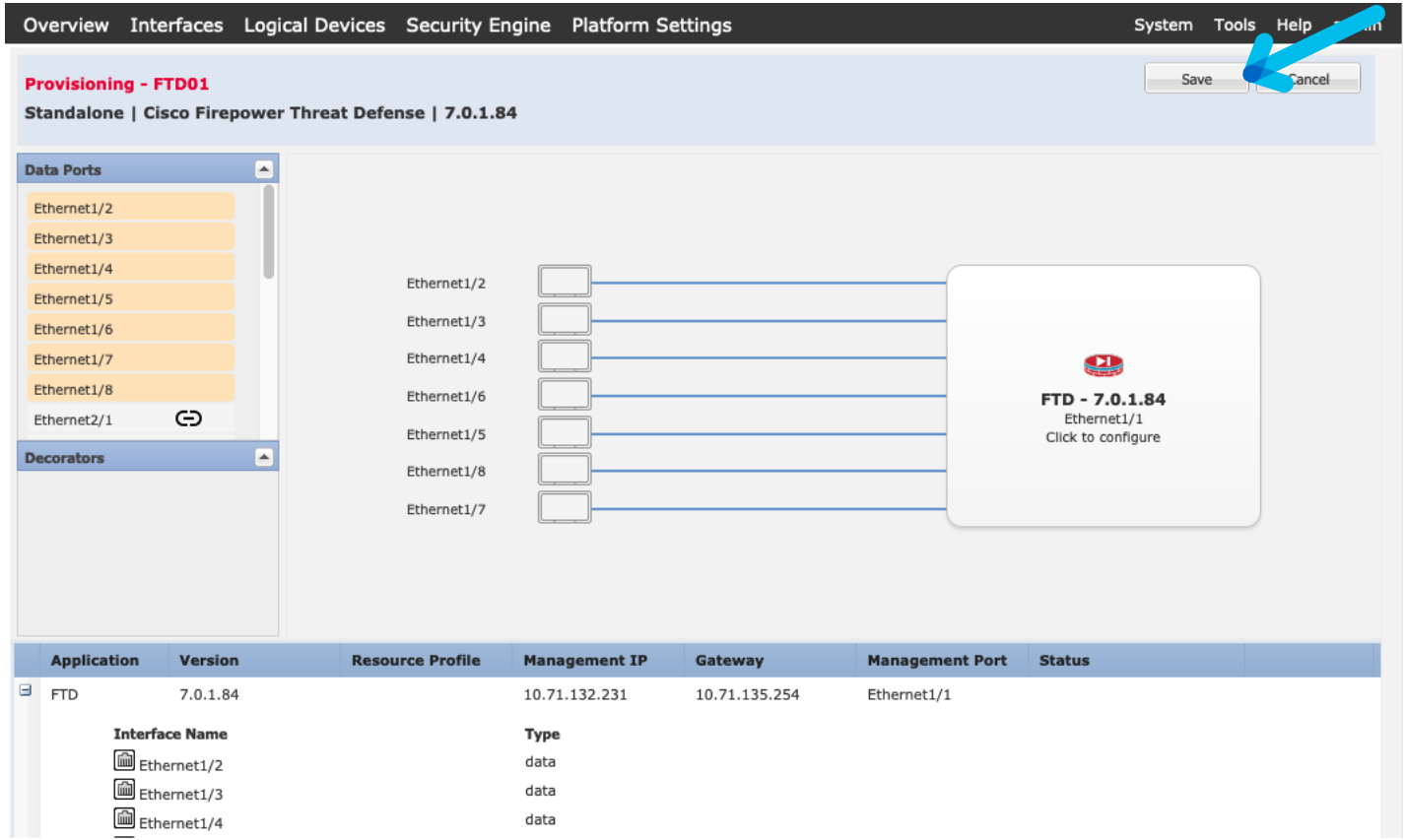
FTD インストール / FMC への登録キーの設定 (GUI)

EULA に対する同意チェック



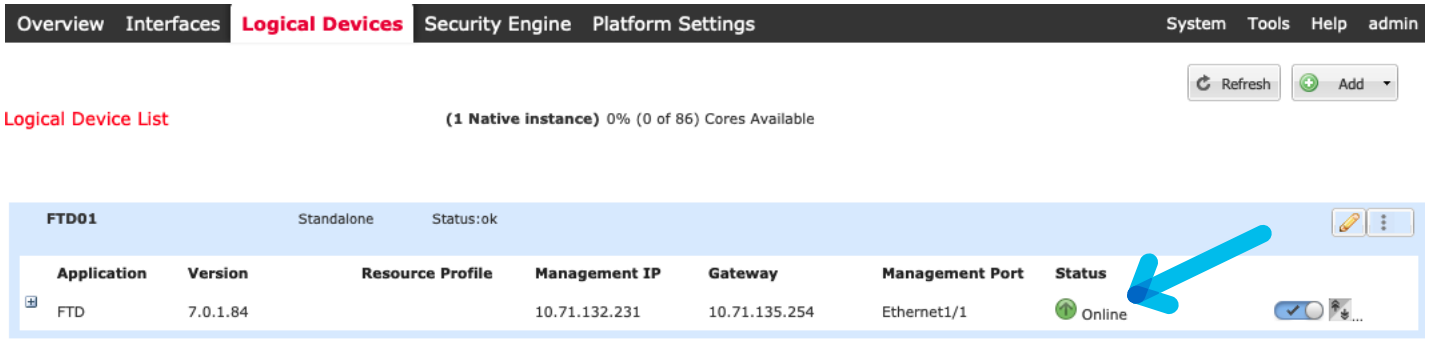
最後に ”OK” をクリック

FTD インストール / FMC への登録キーの設定 (GUI)



FTD インストール / FMC への登録キーの設定 (GUI)

しばらく時間が経って ”Status” が ”Online ”になれば FTD のインストール完了。



あとは “FMC での FTD デバイス登録” のページを参考に
FMC 側で FTD デバイスの登録作業を行えばポリシー等の設定が可能となる。

※FTD のインストールは CLI でも可能だが、かなり複雑なため本資料では割愛

1-4. (Option) FPR1000/2100 シリーズの初期設定

*FTD を FPR1000/2100 シリーズで設定する場合の参考情報

FMC, FTD のインストールからデバイス登録までの流れ

設定の順序

Firewall Management Center

① OVF のデプロイ (FMCv の場合)
② CLI での初期設定
③ Web GUI での初期設定

Firewall Threat Defense

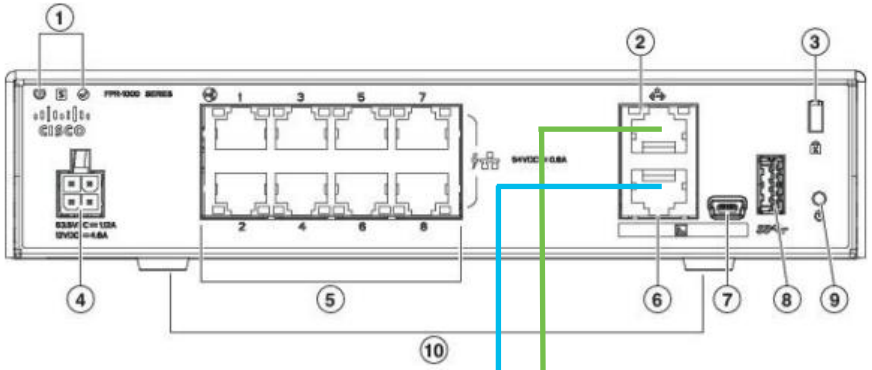
① FXOS を CLI で初期設定
② FXOS/FTD インストール ※
③ FMC への登録キーの設定

※ FXOS, FTD のイメージは購入時にシャーシ内に格納されており、また FPR1k,2k の場合は FXOS と FTD が 1 つのイメージとなっているため互換性の心配も不要です。また FPR4k, 9k と違い FTD のインストールも基本的には必要ありません。

Firewall Management Center

① FTD の登録

HW (FPR1010 シリーズ)



管理ネットワーク

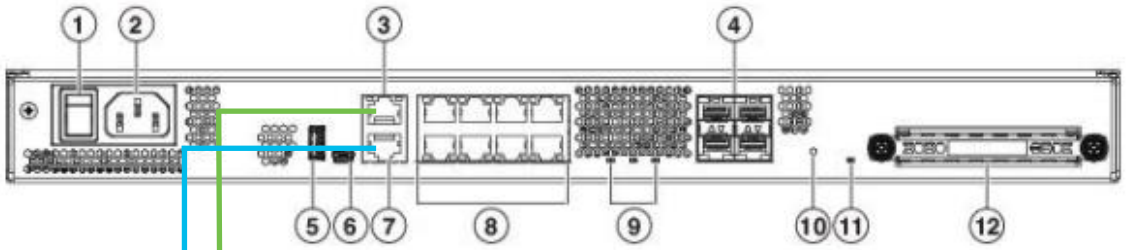
※デフォルトでは FMC との通信に利用される

コンソール

①ステータス LED
②管理ポート
③ロックスロット
④電源コードソケット
⑤ネットワークデータポート
⑥コンソールポート
⑦USB ミニBコンソールポート
⑧USB タイプAポート
⑨リセットボタン
⑩ゴム製の脚

https://www.cisco.com/c/en/us/td/docs/security/firepower/1010/hw/guide/hw-install-1010.html
https://www.cisco.com/c/ja_jp/td/docs/security/firepower/1010/hw/guide/hw-install-1010.html

HW (FPR1100 シリーズ)



管理ネットワーク

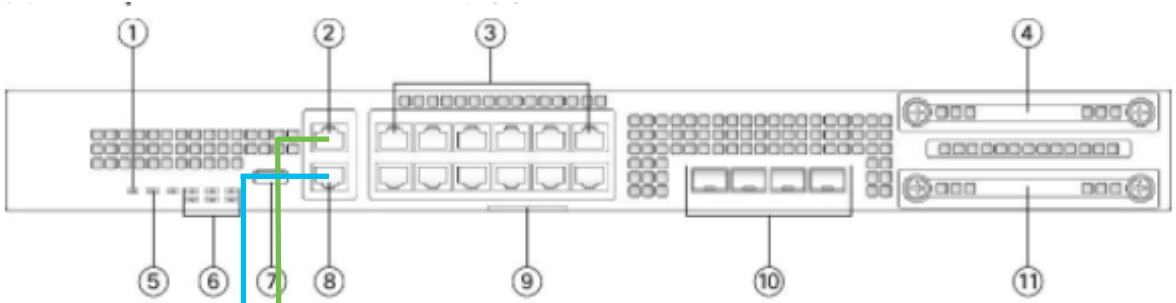
※デフォルトでは FMC との通信に利用される

コンソール

①電源スイッチ
②管理ソケット
③管理ポート
④SFP ポート
⑤USB タイプA ポート
⑥USB ミニBコンソールポート
⑦RJ-45 コンソール
⑧データポート
⑨ステータス LED
⑩リセットボタン
⑪SSD LED
⑫SSD ベイ

https://www.cisco.com/c/en/us/td/docs/security/firepower/1100/hw/guide/hw-install-1100.html
https://www.cisco.com/c/ja_jp/td/docs/security/firepower/1100/hw/guide/hw-install-1100.html

HW (FPR2100 シリーズ)



管理ネットワーク

※デフォルトでは FMC との通信に利用される

コンソール

①電源 LED
②管理ポート
③10/100/1000
イーサネットポート x 12
④SSD1
⑤ロケータ LED
⑥システム LED
⑦タイプA USB 2.0
⑧RJ-45 コンソール
⑨アセットカード
⑩SFP(1G) ポート x 4
⑪SSD2

https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100.html
https://www.cisco.com/c/ja_jp/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100.html

CLI で初期設定

Firepower1000, 2100 シリーズの場合、発注時に選択した FTD のイメージがインストールされた状態で手元に届く

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1
[...]
Hello admin. You must change your password. Enter
new password: ********
Confirm new password: ********
Your password was updated successfully.
firepower#
firepower# connect ftd
>
```

FPR1000/2100 共通
デフォルト ユーザ名/パスワード : admin/Admin123

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp1100/firepower-1100-gsg/ftd-fmc.html

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp2100/firepower-2100-gsg/ftd-fmc-remote.html

もし「connect ftd」コマンドを打ってエラーが返ってくる場合、何かしらの理由で FTD がインストールされていない状態となるため、FTD のインストール作業が必要。

【参考】 FPR1000, 2100 シリーズ:フォーマット ～FXOS インストール

フォーマット　※フォーマットは格納してるすべてのイメージを消去するため注意

```
fpr2130# connect local-mgmt
fpr2130(local-mgmt)#
fpr2130(local-mgmt)#
fpr2130(local-mgmt)#
fpr2130(local-mgmt)#
fpr2130(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
100+0 records in
100+0 records out
51200 bytes (51 kB, 50 KiB) copied, 0.00174817 s, 29.3 MB/s
4+0 records in
4+0 records out
2048 bytes (2.0 kB, 2.0 KiB) copied, 4.531e-05 s, 45.2 MB/s
100+0 records in
100+0 records out
51200 bytes (51 kB, 50 KiB) copied, 0.00272699 s, 18.8 MB/s

Broadcast message from root@fpr2130 (Thu Jan 20 07:53:33 2022):
All shells being terminated due to system /sbin/reboot
Broadcast message from root@fpr2130 (Thu Jan 20 07:53:34 2022):
```

rommon でイメージをダウンロード (tftp boot)

```
autoboot: All boot attempts have failed, will retry three times !
autoboot: retry count: 4 is over the limit, system will stop autoboot


rommon 1 > address 10.10.10.2
rommon 2 > netmask 255.255.255.0
rommon 3 > gateway 10.10.10.254
rommon 4 > file cisco-ftd-fp2k.7.0.1-84.SPA
rommon 5 > server 2.2.2.2
rommon 6 > set
   ADDRESS=10.10.10.2
   NETMASK=255.255.255.0
   GATEWAY=10.10.10.254
   SERVER=2.2.2.2
   IMAGE=cisco-ftd-fp2k.7.0.1-84.SPA
   CONFIG=
   PS1="rommon ! > "


rommon 7 > sync
rommon 8 > tftp -b
Enable boot bundle: tftp_reqsize = 268435456
```

【参考】 FPR1000, 2100 シリーズ:フォーマット～FXOS インストール

ダウンロードが完了すると自動的に FXOS が起動

```
link up
Receiving cisco-ftd-fp2k.7.0.1-84.SPA from
10.71.136.1!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot buffer bigbuf=7e13e3d8
Boot image size = 190962368 (0xb61dac0) bytes
[image size]      190962368
[MD5 signature]    4d087b0c53c25ff7b45b0e0e367fc348
```

```
+-----------------------------------------------------------------------------
+
+---------------------------- SUCCESS -------------------------------------
+
+-----------------------------------------------------------------------------
+
|                                                                            |
|          LFBFF signature authentication passed !!!             |
|                                                                            |
+-----------------------------------------------------------------------------
+
LFBFF signature verified.
+-----------------------------------------------------------------------------
+
+---------------------------- SUCCESS -------------------------------------
+
+-----------------------------------------------------------------------------
+
|                                                                            |
|          LFBFF controller type check passed !!!                |
|                                                                            |
+-----------------------------------------------------------------------------
+
```

【参考】 FPR1000, 2100 シリーズ:フォーマット ～FXOS インストール

再起動後、デフォルトのクレデンシャルでログインし、PW 変更

```
firepower-2130 login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1
Hello admin. You must change your password.
Enter new password: 新しいパスワードを入力
Confirm new password:  新しいパスワードを入力
Your password was updated successfully.
------省略------

firepower-2130#
```

フォーマットしたのでパッケージ (FTD のイメージ) は存在しない

```
firepower-2130# scope firmware
firepower-2130 /firmware # show package
firepower-2130 /firmware #
```

【参考】 FPR1000, 2100 シリーズ:フォーマット ～FXOS インストール

rommon で設定した IP は一時的な用途のため、起動後の FXOS では
管理 IP はデフォルトの ”192.168.45.45” が設定されており、必要に応じて変更。

```
firepower-2130# scope fabric-interconnect a
firepower-2130 /fabric-interconnect # show


Fire Power:
    ID   OOB IP Addr     OOB Netmask     OOB Gateway     OOB IPv6 Address Prefix OOB IPv6 Gateway Operability
    ---- ---------------  ---------------  ---------------  ----------------  ---------------  -----------
    A    192.168.45.45   255.255.255.0       0.0.0.0           ::                  64     ::                  Operable

firepower-2130 /fabric-interconnect # set out-of-band static ip 10.10.10.2 netmask 255.255.255.0 gw 10.10.10.254 ←― こちらの例では 10.10.10.2/24 を設定
firepower-2130 /fabric-interconnect* # commit-buffer      ←― commit-buffer で保存・適用
```

【参考】 FPR1000, 2100 シリーズ:FTD インストール

FTD のためのイメージ (FXOSと同じイメージ) をダウンロード

```
firepower-2130 /firmware # download image tftp://10.71.136.1/cisco-ftd-fp2k.7.0.1-84.SPA
Please use the command 'show download-task' or 'show download-task detail' to check download progress.
% Download-task cisco-ftd-fp2k.7.0.1-84.SPA : transferring 57019 KB          |

firepower-2130 /firmware #
firepower-2130 /firmware # show download-task detail
Download task:
    File Name: cisco-ftd-fp2k.7.0.1-84.SPA
    Protocol: Tftp
    Server: 10.71.136.1
    Port: 0
    Userid:
    Path:
    Downloaded Image Size (KB): 99780
    Time stamp: 2022-01-20T08:16:14.145
    State: Downloading
    Status: Downloading the image
    Transfer Rate (KB/s): 4338.260742
    Current Task: downloading image cisco-ftd-fp2k.7.0.1-84.SPA from 10.71.136.1
(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
% Download-task cisco-ftd-fp2k.7.0.1-84.SPA : completed successfully.

firepower-2130 /firmware #
firepower-2130 /firmware # show package
Name                                     Package-Vers
---------------------------------------- ------------
cisco-ftd-fp2k.7.0.1-84.SPA                 7.0.1-84
```

【参考】 FPR1000, 2100 シリーズ:FTD インストール

アップロード済みのパッケージ（イメージ）を確認

```
firepower# scope firmware
firepower /firmware # show package
Name                                      Package-Vers
------------------------------------------ ------------
cisco-ftd-fp2k.7.0.1-84.SPA               7.0.1-84
```

パッケージを指定して FTD をインストール (インストール後、自動的に再起動)

```
firepower /firmware # scope auto-install
firepower /firmware/auto-install # install security-pack version 7.0.1-84

The system is currently installed with security software package not set, which has:
   - The platform version: not set
If you proceed with the upgrade 7.0.1-84, it will do the following:
   - upgrade to the new platform version 2.10.1.175
   - install with CSP ftd version 7.0.1.84
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,
   and the default configuration applied.
Do you want to proceed? (yes/no):yes
Triggered the install of software package version 7.0.1-84
```

【参考】 FPR1000, 2100 シリーズ: FTD 初期設定

※選択項目では何も入力しないと[ ]内の値が設定される

```
firepower# connect ftd
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
-----省略------
Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES   ← EULA (利用許諾契約) に同意するか
-----省略------
Do you want to configure IPv4? (y/n) [y]: y   ← IPv4 の設定有無
Do you want to configure IPv6? (y/n) [y]: n   ← IPv6 の設定有無
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [10.71.134.51]: 10.71.132.192   ← IPv4 の管理用 IP
Enter an IPv4 netmask for the management interface [255.255.248.0]: 255.255.248.0   ← ネットマスク
Enter the IPv4 default gateway for the management interface [data-interfaces]:   ← どのインタフェースを管理用に設定するか
Enter a fully qualified hostname for this system [firepower]: fpr2130   ← ホスト名
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:   ← DNS サーバ
Enter a comma-separated list of search domains or 'none' []: cisco.com   ← 検索ドメイン
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222 208.67.220.220 2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as fpr2130
Setting static IPv4: 10.71.132.192 netmask: 255.255.248.0 gateway: data on management0
Updating routing tables, please wait...                                  ← 設定した内容の確認
-----省略------
Manage the device locally? (yes/no) [yes]: no   ← FTD 管理方法の設定。”no” は FMC 管理。”yes” はローカル管理 (FDM)
Not managing the device locally with a data-interface gateway will only allow
access through the management port. Do you want to continue? (yes/no): yes   ← 管理ポート経由で管理するかどうか
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:   ← FTD のモードを設定
Configuring firewall mode ...
-----省略------
> configure manager add [FMCのホスト名 | FMCのIPアドレス] [登録キー ]   ← 管理する FMC のアドレスと登録キーの設定
```

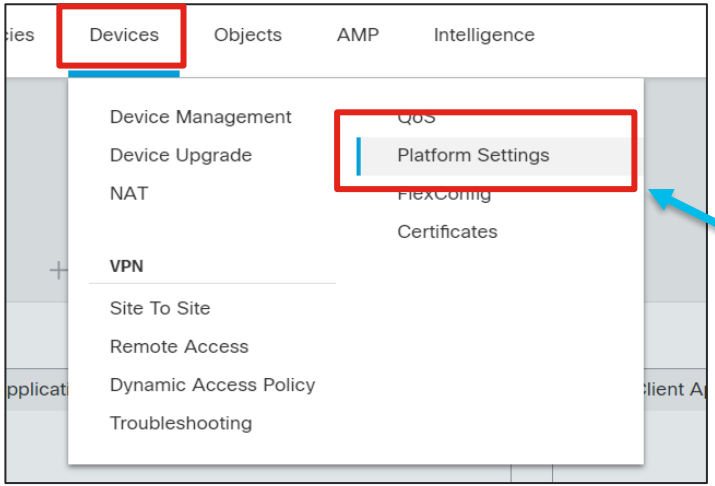
2. FTD と FMC その他初期設定

FTD と FMC その他初期設定に関して

- FTD のネットワーク周りで行うべき最低限の設定を行う
  - Time Synchronization
  - Interface
  - *Routing*
  - *NAT*
  - *Access Control Policy*
  - *Network Discovery Policy*
  - *Pre-filter*

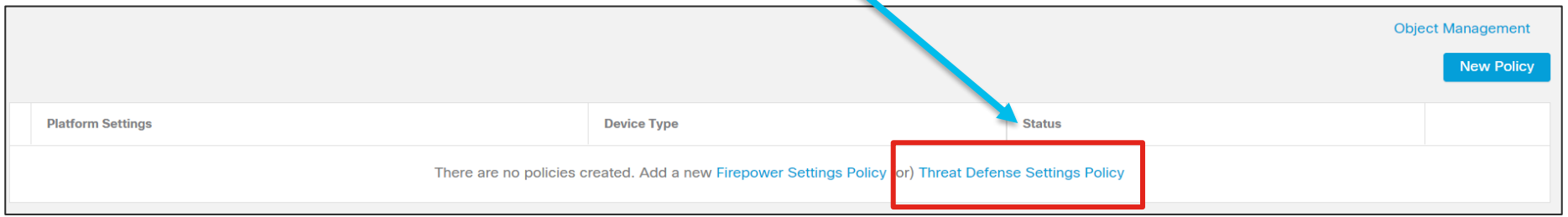
Vol. 2 基本設定編にて実施予定

Time Synchronization - 1

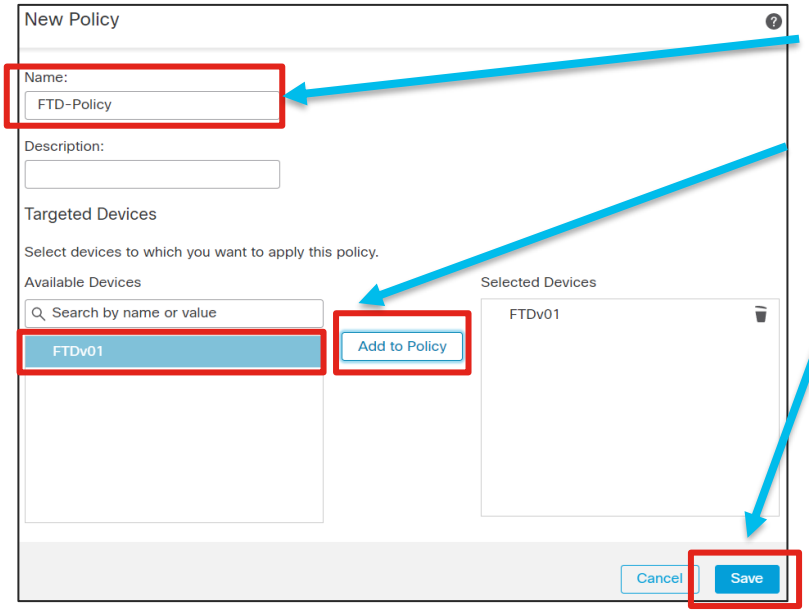


FTD の時刻同期の設定
※本手順書では FMC と同期

1. Devices メニューから Platform Settings をクリック
2. 表示された画面で Threat Defense Setting Policy をクリック

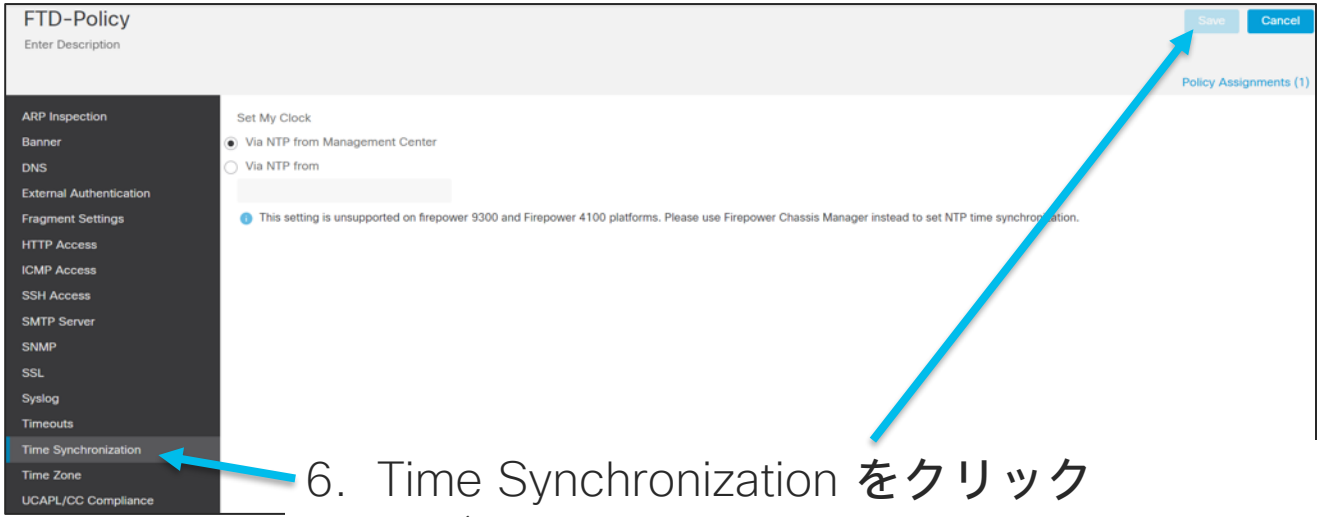


Time Synchronization - 2



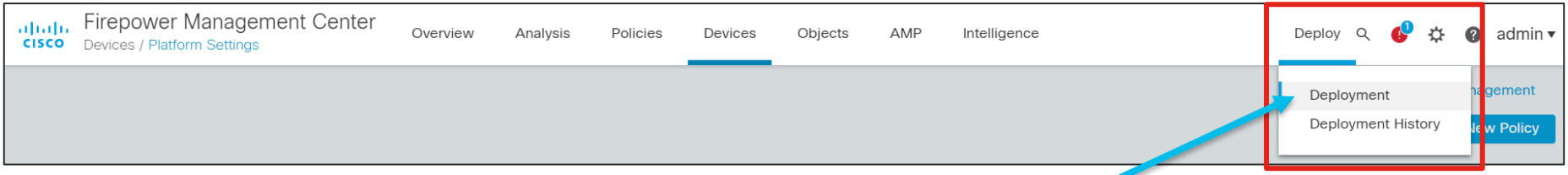
3. Name 欄に任意のポリシー名を入力 (今回は FTD-Policy として入力)
4. Available Devices から適用する FTD を選択し、Add to Policy をクリック
5. Save をクリック

Time Synchronization - 3

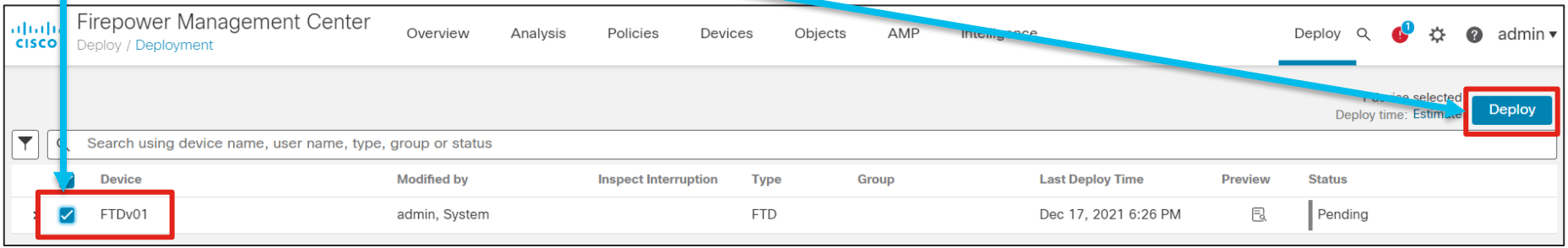


6. Time Synchronization をクリック
   ※デフォルトは Via NTP from Management Center になっている。
   今回の手順書の設定はこのままで問題なし
7. 変更した場合は、右上の Save ボタンをクリック（設定変更がない場合はボタンがグレーアウトされる）

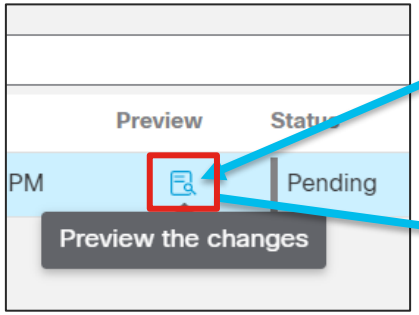
Time Synchronization – 4



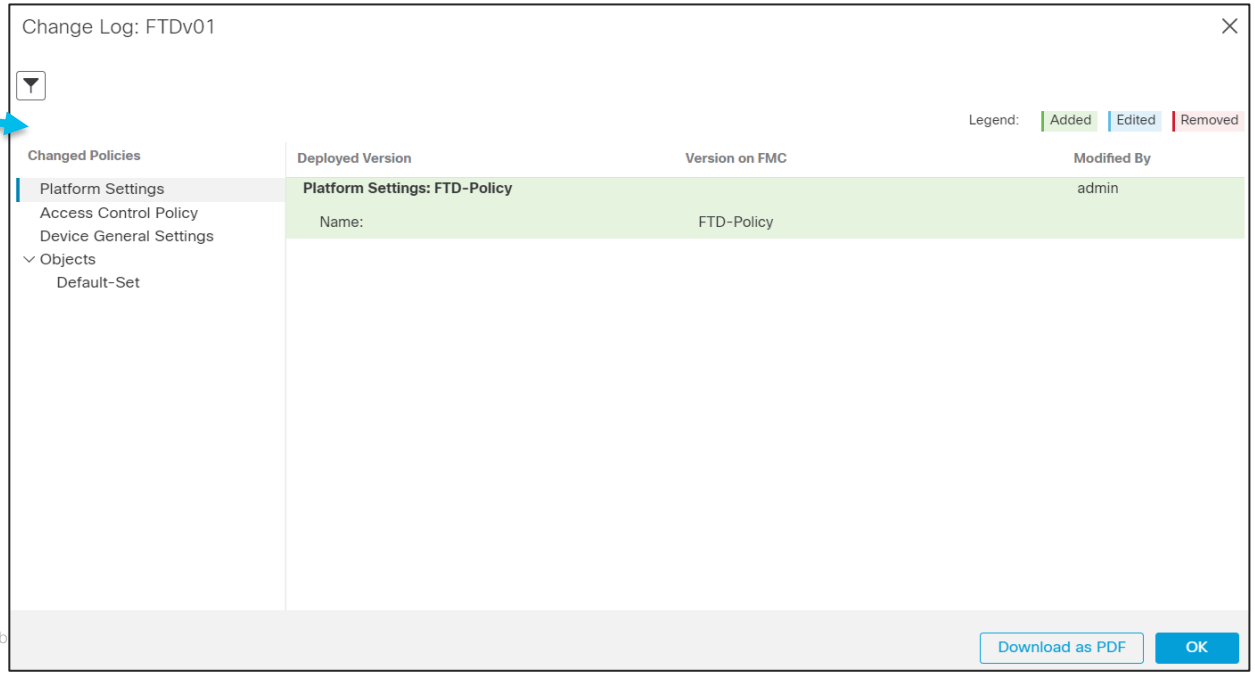
8. 設定を FTD に反映させるため、Deploy – Deployment をクリック
9. 反映させる FTD を選択 (今回のデバイス名は FTDv01)
10. Deploy ボタンをクリック



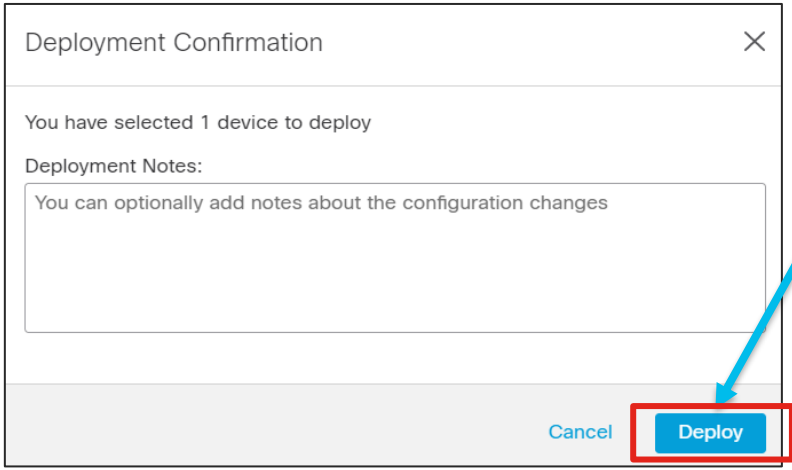
Time Synchronization - 5



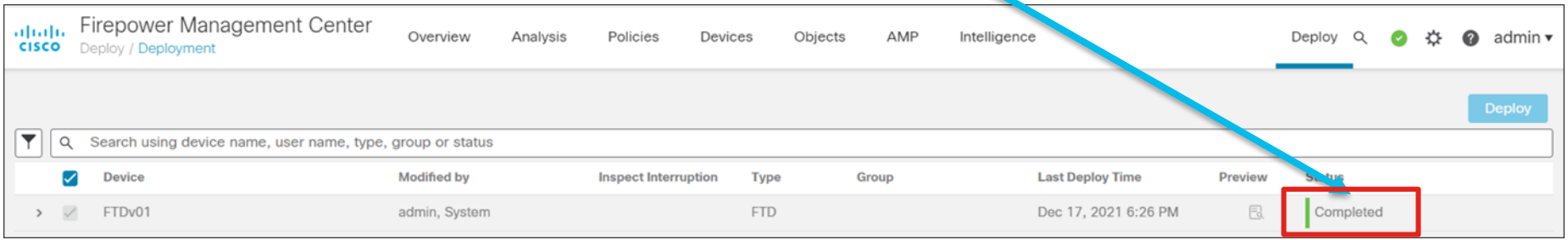
Deploy 前に Preview をクリックすると変更内容の確認が可能



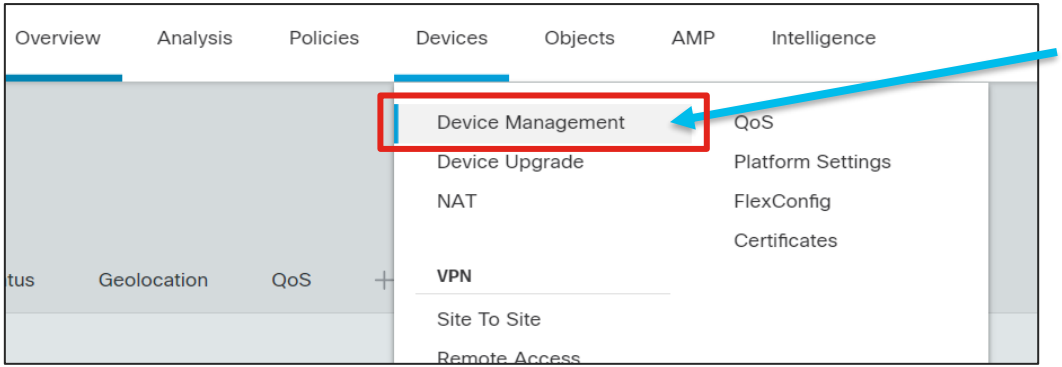
Time Synchronization - 6



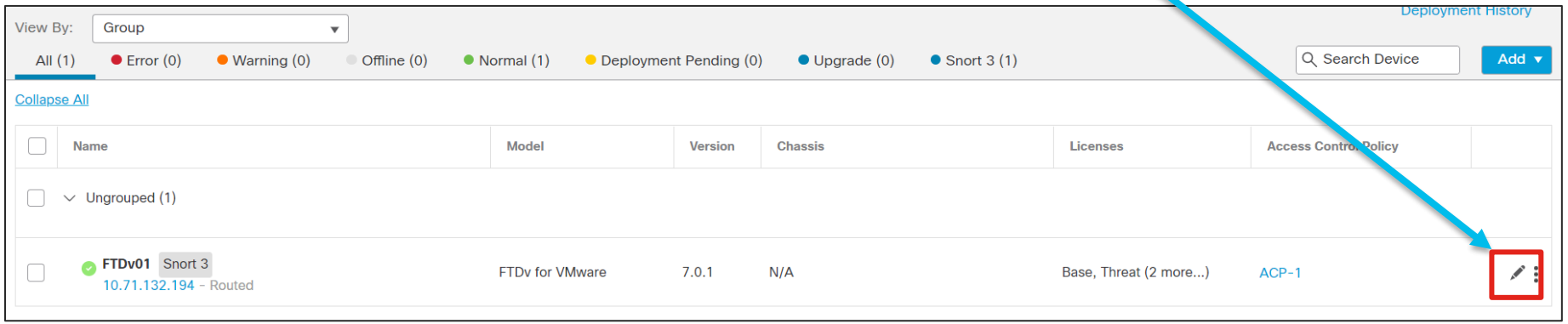
11. 確認画面が表示、Deploy をクリック
12. ポリシーの配布が行われ、Completed になったら完了



FTD Interface 設定 - 1

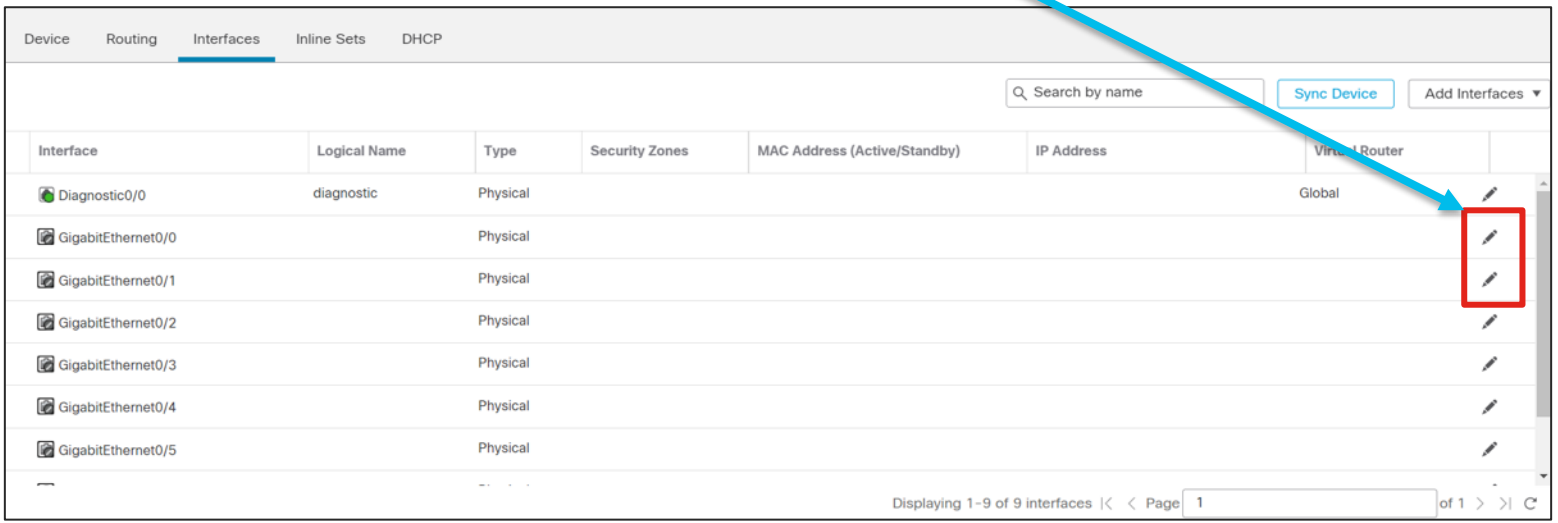


1. Device – Device Management をクリック
2. 編集する FTD の右側にある鉛筆マークをクリック

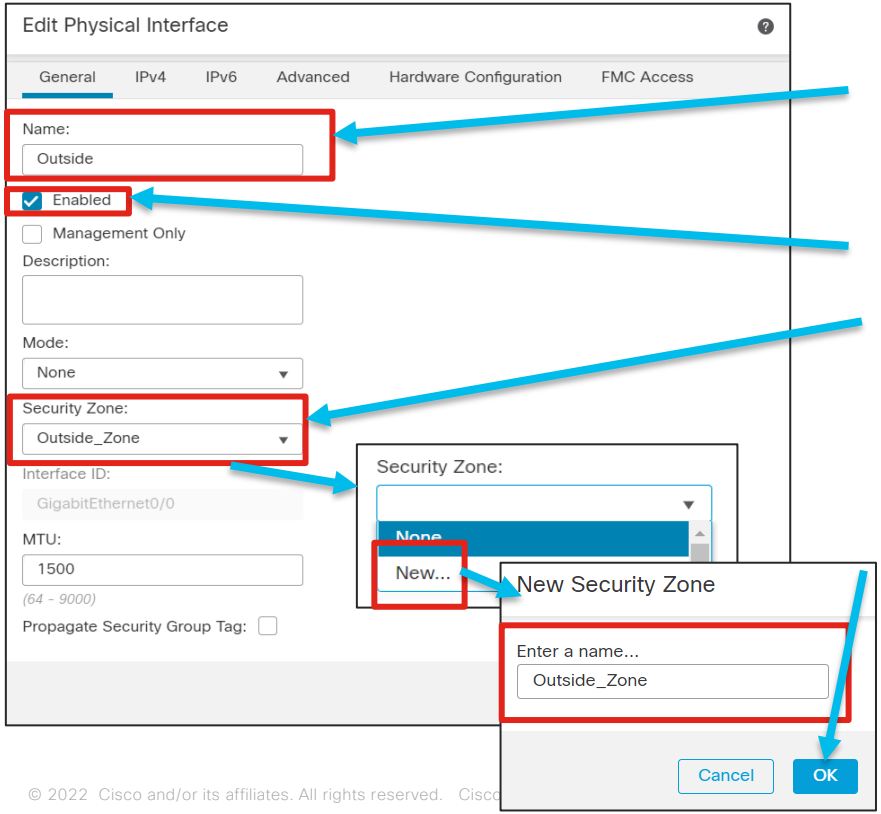


FTD Interface 設定 - 2

3. 編集するインタフェースの右にある鉛筆マークをクリック
   ※今回の環境では GigabitEthernet0/0 と 0/1 を編集

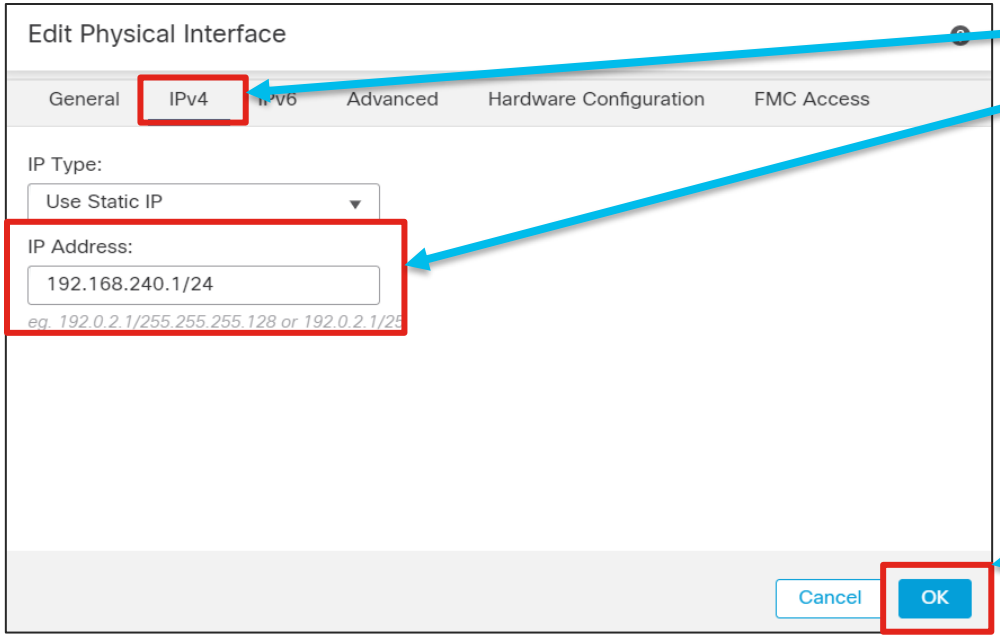


FTD Interface 設定 - 2



4. Name 欄に名前を入力
   ※今回の例では Outside 側の Interface 編集なので Outside と入力
5. Enabled をチェック
6. Security Zone もリストをクリックし、New をクリック
   ※すでに Zone を作成済みの場合は任意の Zone を選択
7. New Security Zone の画面で Zone 名を入力し、OK をクリック
   ※今回の例では Outside 側の Zone として Outside_Zone と記載

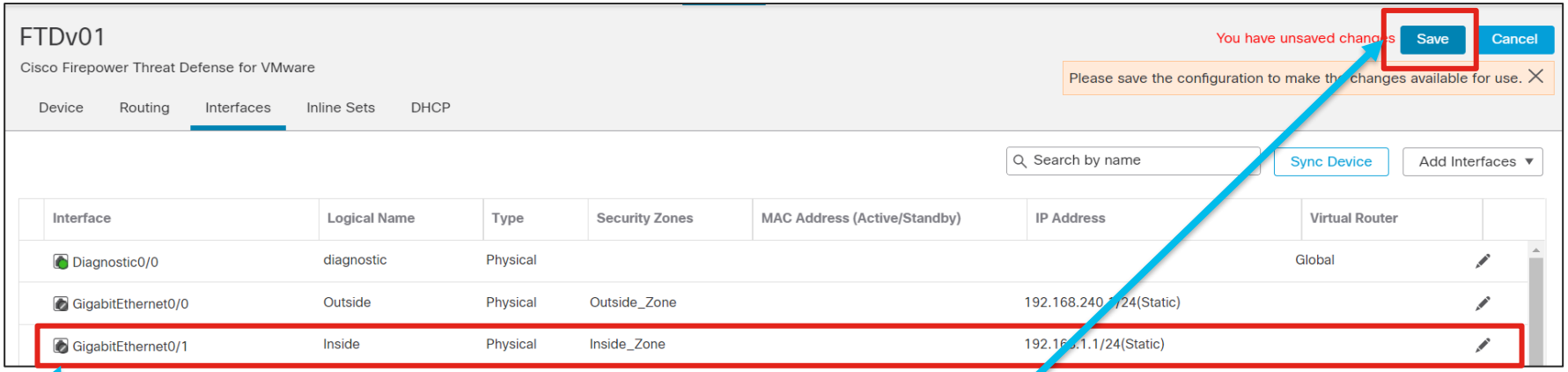
FTD Interface 設定 - 3



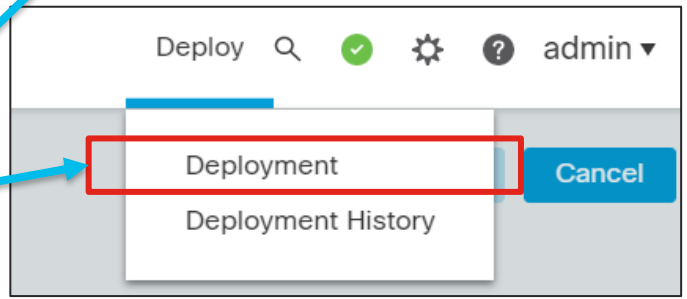
8. IPv4 のタブをクリック
9. IP Address の欄に IP アドレスを入力
   ※IP アドレスと / の後にサブネットを記載
   今回の例では、Outside 側の IP アドレスとなる 192.168.240.1 としサブネットマスクを 24bit として設定
10. OK をクリック

※環境に応じて IPv6 等も設定

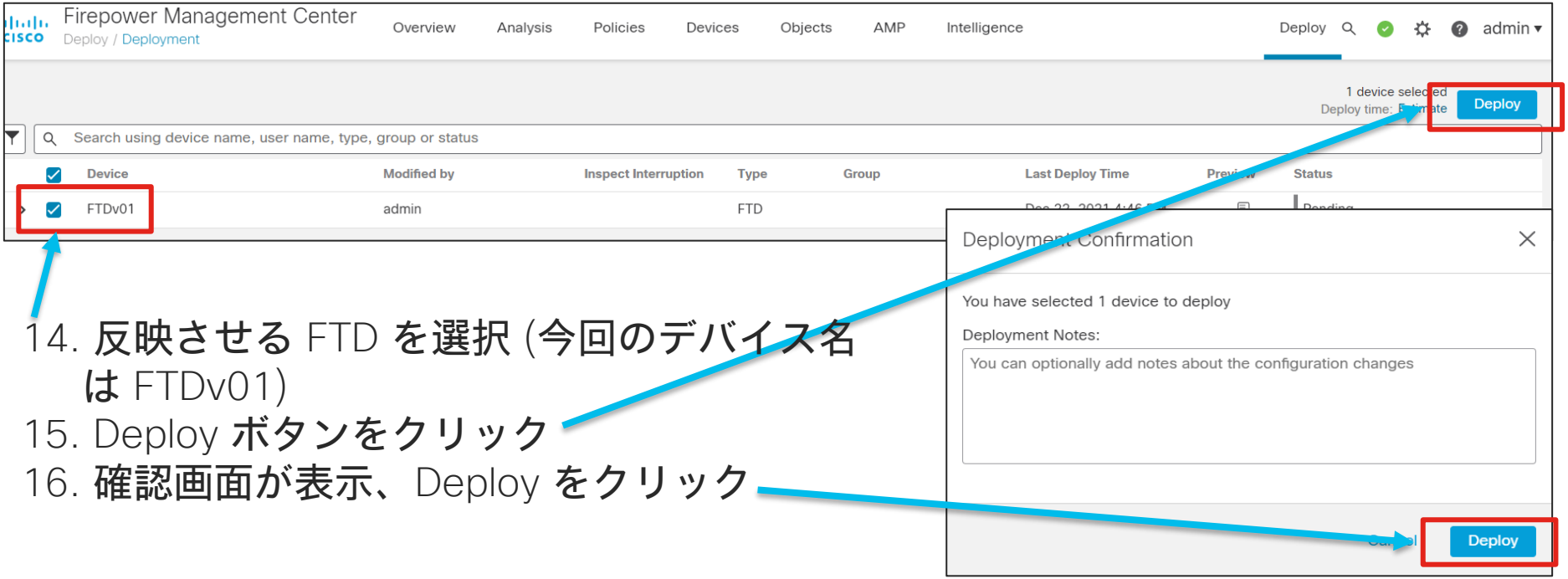
FTD Interface 設定 - 4



11. 同様に GigabitEthernet0/1 に Inside の情報を入力
12. 右上の Save をクリックして、設定を保存
13. 設定を FTD に反映させるため、Deploy – Deployment をクリック

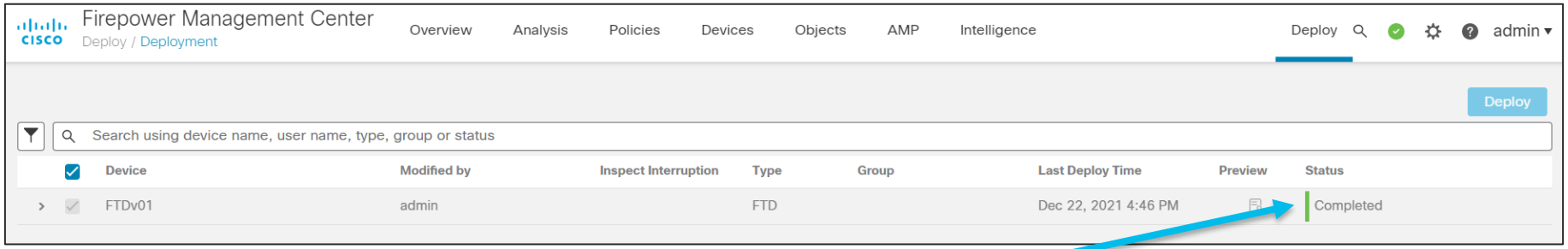


FTD Interface 設定 - 5



14. 反映させる FTD を選択 (今回のデバイス名は FTDv01)
15. Deploy ボタンをクリック
16. 確認画面が表示、Deploy をクリック

FTD Interface 設定 - 6

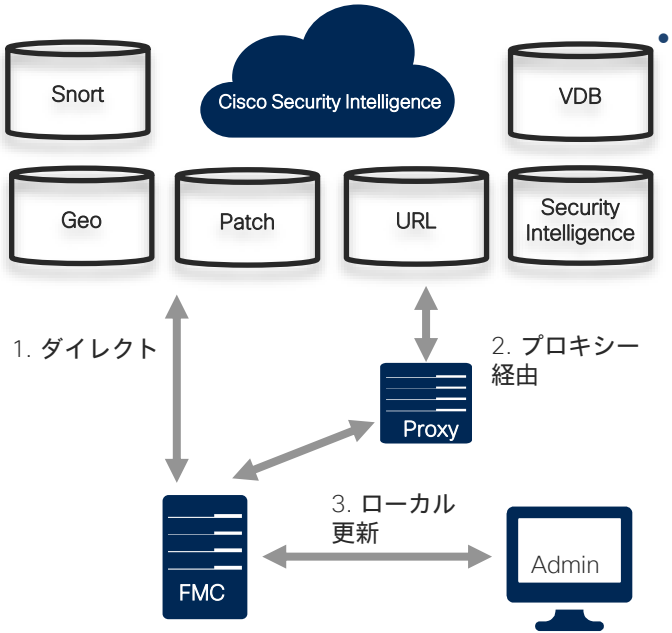


17. 設定の配布が行われ、Completed になったら完了
18. 必要に応じてテスト端末から inside interface への Ping 等で疎通を確認

```
C:\Users\cisco>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=10ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

3.　シグネチャ及び各種 DB の更新

FMC シグネチャ / DB 更新の概要



- FMC は3つの方法によって、情報を更新可能

1.クラウド更新 (ダイレクト)

利用条件：FMC が直接インターネットへ接続可能

2. クラウド更新 (プロキシー経由)

利用条件：Proxy サーバーがインターネットへ接続可能

3.ローカル更新

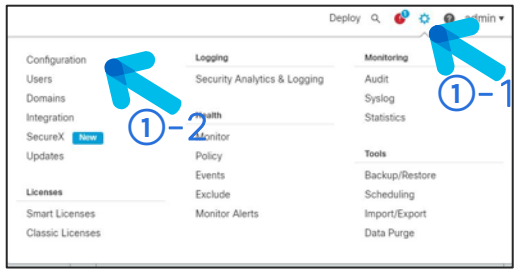
利用条件：FMC マネージメント IP がインターネット接続不可能

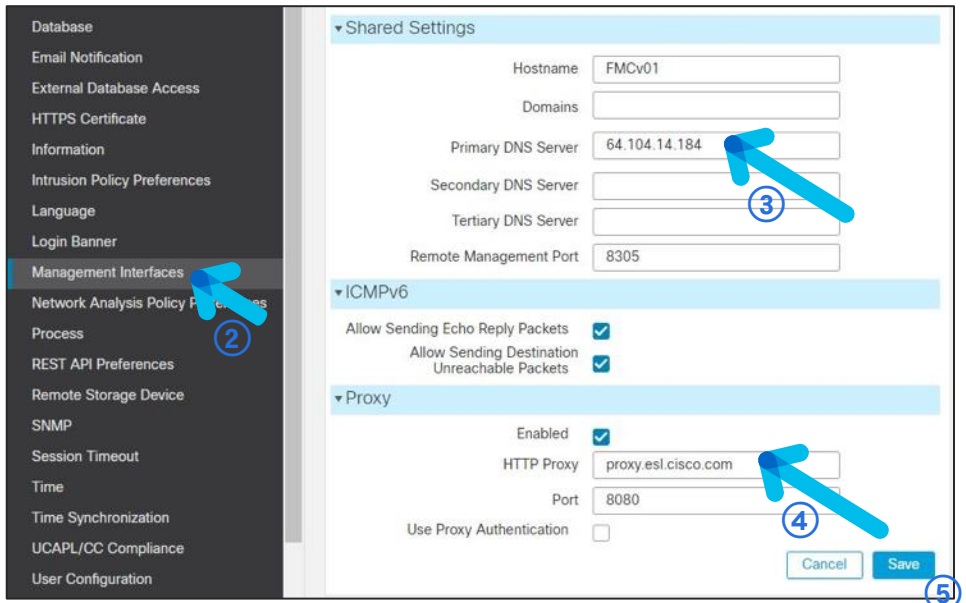
制限事項：URL, Security Intelligence 以外はローカル更新可能

更新パッケージ一覧

	内容	ファイル例	ワンタイム更新	定期更新	更新方法
Patch	新機能追加、既知 Bug 修正 (FMC/ FTD 両方にパッチが存在)	Cisco_Firepower_Mgmt_Center_Patch-7.0.0.1-15.sh.REL.tar	可能	可能 (別途スケジューリング必要)	クラウド・ローカル
Snort Rules	Snort IPS ルールアップデート	Cisco_Firepower_SRU-2020-04-24-001-vrt.sh.REL.tar (Snort 2 用) lsp-rel-20220314-1407.tar.xz.REL.tar (Snort 3 用)	可能	可能 (別途スケジューリング必要)	クラウド・ローカル
GeoDB	地理情報と紐づくグローバル IP アップデート	Cisco_Firepower_SRU-2022-01-18-001-vrt.sh.REL.tar.tar	可能	可能	クラウド・ローカル
VDB	OS / アプリケーションの脆弱性、検出、フィンガープリント情報	Cisco_VDB_Fingerprint_Database-4.5.0-351.sh.REL.tar	可能	可能	クラウド・ローカル
URL	URL フィルタリングに用いる URL 情報		可能	可能	クラウド
Security Intelligence	ブラックリスト IP / URL / Domain 情報		不可	可能	クラウド

クラウド接続方法の確認

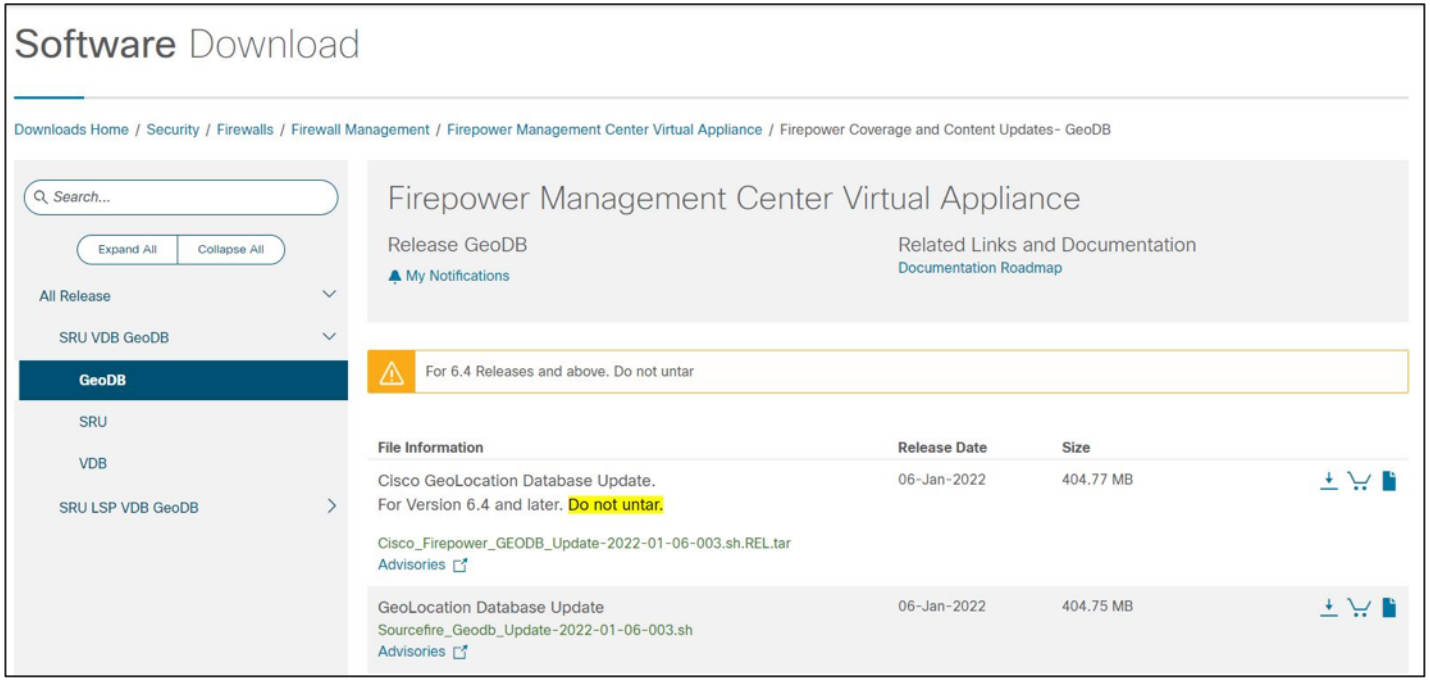




① System → Configuration を選択
② Management Interface を選択
③ Shared Settings 配下の Primary / Secondary / Tertiary DNS Server を参照し、Cisco クラウドの名前解決が可能な DNS が設定されていることを確認
④ プロキシを使用している環境の場合は Proxy を参照し、Enabled がチェックされ、HTTP proxy、Port、Use Proxy Authentication に使用しているプロキシの情報が入力されていることを確認
⑤ 設定を変更した場合は Save をクリック

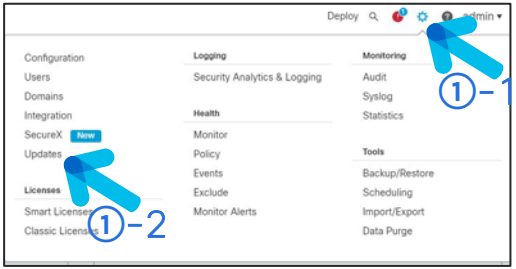
- 通信要件は Firepower Management Center Configuration Guide, Version 7.0 の Security Requirements に記載 (※使用しているソフトウェアバージョンのドキュメントを参照すること)

ローカル更新用パッケージ準備

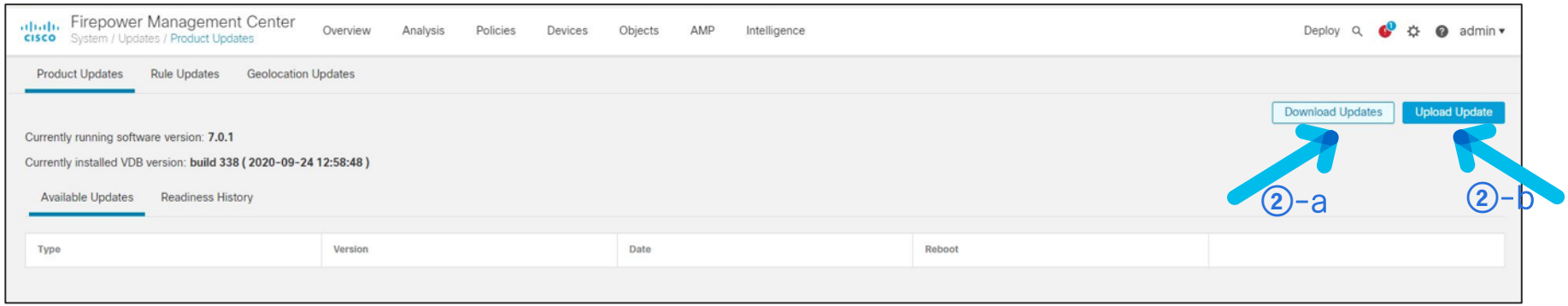


① Cisco Software Download ページへ、ファイルのダウンロード権限のあるアカウントでアクセス
② 使用している FMC モデルを選択
③ ローカル更新に使用する更新ファイルをダウンロード

VDB / Patch ワンタイム更新

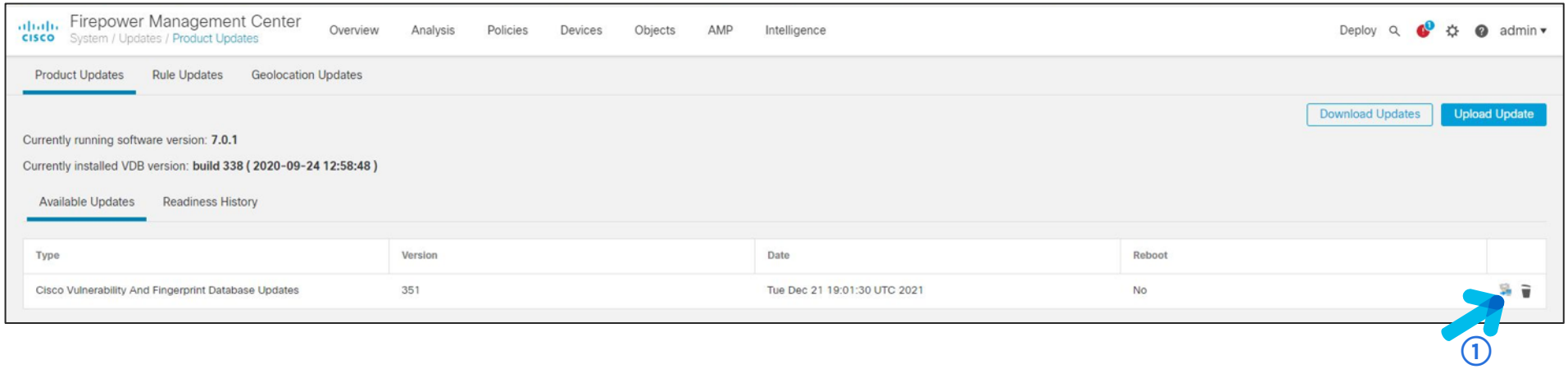


※ Patch 適用の詳細は 5章を参照



① System → Updates を選択
② いずれかを実施
   a. ダイレクト / Proxy 経由のクラウド更新：Downloaded Updates を選択。Patch, VDB に更新がある場合、更新可能なファイルがダウンロードされ、完了後に Available Updates へ表示される (タスクが進行している間、ブラウザの画面を閉じないこと)
   b. ローカル更新：Upload Update を選択。VDB もしくは FMC / FTD Patch をアップロード

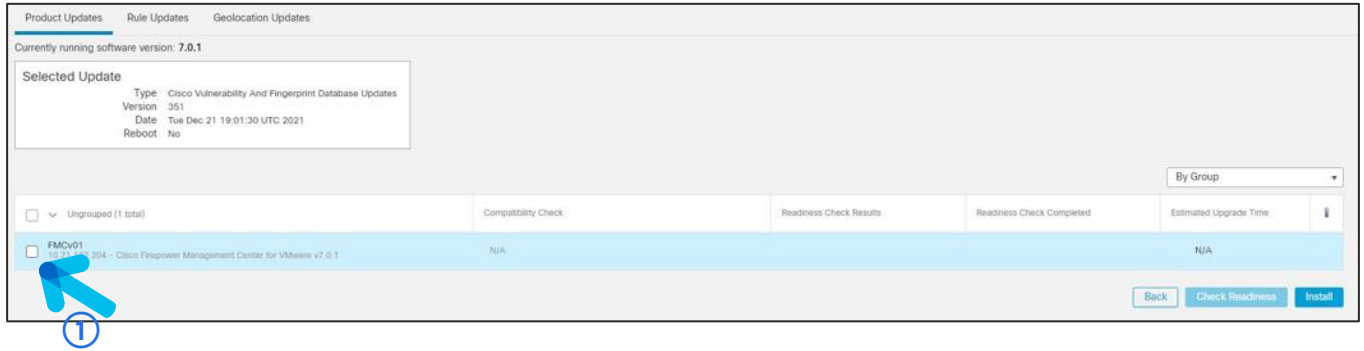
VDB / Patch ワンタイム更新～インストール

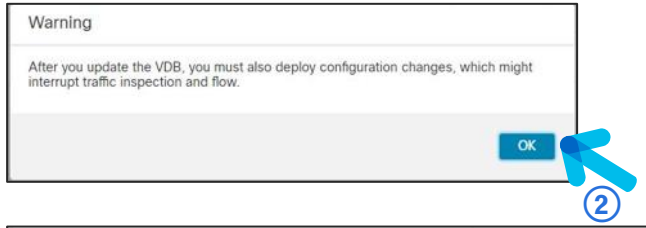


① インストールする更新ファイル列の右側にある Install をクリック

- VDB / Patch 更新は、FTD データ通信トラフィックへ影響があるため計画適用を推奨

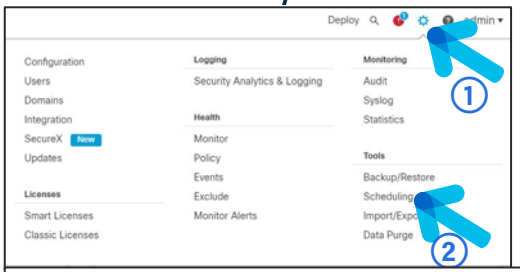
VDB / Patch ワンタイム更新～インストール

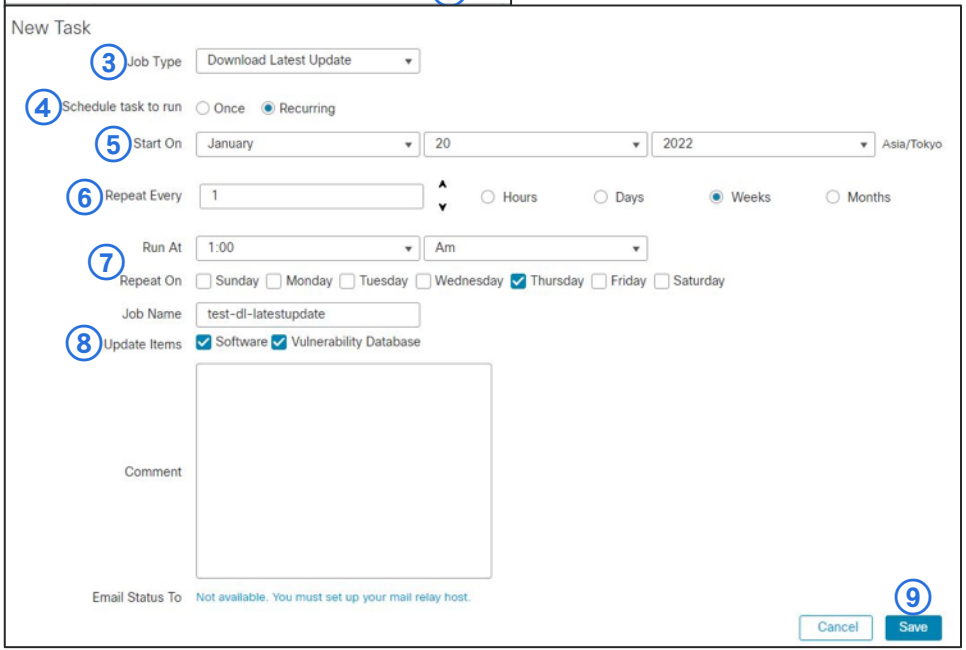




① 更新ファイルをインストールする対象デバイスへチェックを付ける
② ポップアップで Warning が表示される。内容を確認し、OK をクリック
③ Install をクリック

VDB / Patch 定期更新 ダウンロード

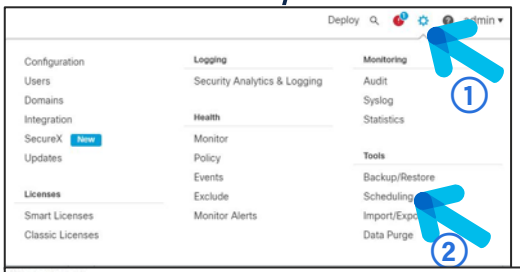


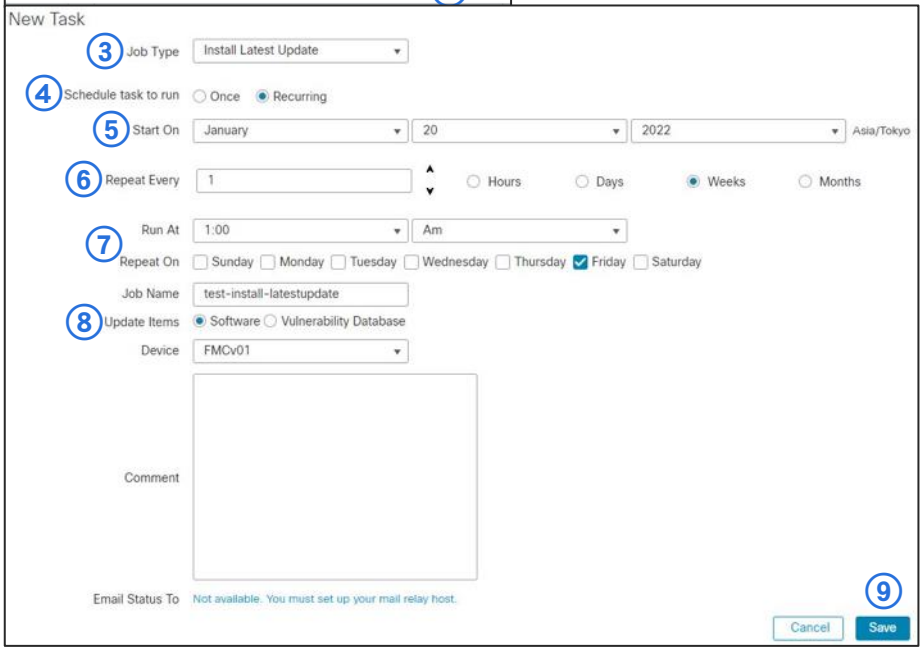


① System → Tools → Scheduling を選択
② Add Task をクリック
③ New Task より [Download Latest Update] を選択
④ Schedule task to run: Recurring へチェックを入れる
⑤ 定期更新を開始する日付を選択
⑥ 更新頻度を指定。Hours / Days / Weeks / Months より選択可能
⑦ 定期更新を実施するタイミングを指定
⑧ [Software]、[Vulnerability Database] より必要なパッケージへチェックを入れる
⑨ Save をクリック

- VDB / Patch の更新パッケージを定期チェックするためには、スケジューリング機能が必要
- バージョン7.0.x を新規インストールした場合は、Software の週次ダウンロード [Weekly Software Download] がデフォルトで設定されている

VDB / Patch 定期更新 インストール

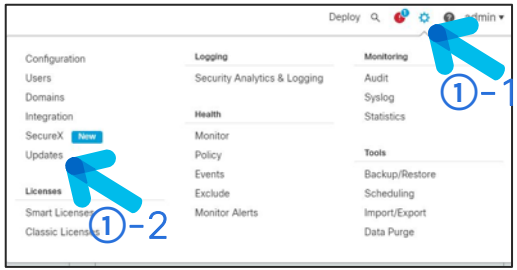


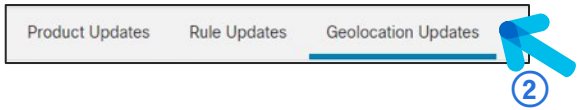


① System → Tools → Scheduling を選択
② Add Task をクリック
③ New Task より [Install Latest Update] を選択
④ Schedule task to run: Recurring へチェックを入れる
⑤ 定期更新を開始する日付を選択
⑥ 更新頻度を指定。Hours / Days / Weeks / Months より選択可能
⑦ 定期更新を実施するタイミングを指定
⑧ [Software]、[Vulnerability Database] より必要なパッケージへチェックを入れる
⑨ Save をクリック

- VDB / Patchインストールは、FTD データ通信トラフィック影響があるため実施時間 (Run At、Repeat On の設定)に注意

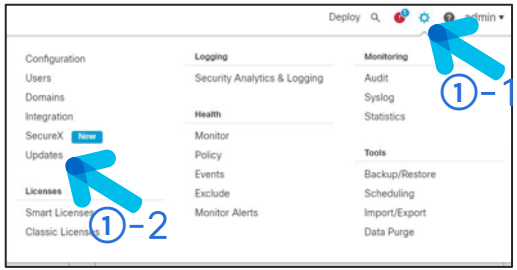
GeoDB ワンタイム更新

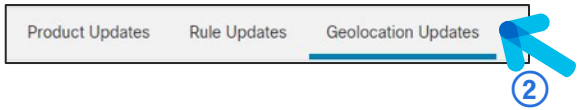


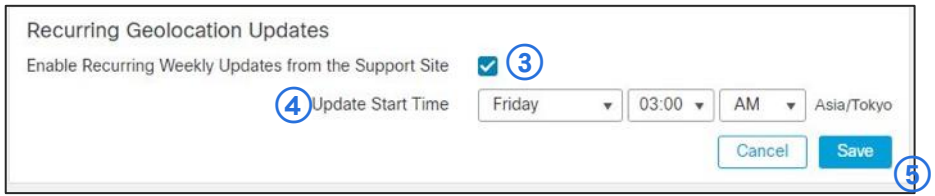


① System → Updates を選択
② Geolocation Updates を選択
③ いずれかを実施
   a. ローカル更新：[Upload and install geolocation update] を選択後、ファイルをアップロードして Import をクリック
   b. ダイレクト / Proxy 経由のクラウド更新：[Download and install geolocation update from the Support Site] を選択し、Import をクリック

GeoDB 定期更新

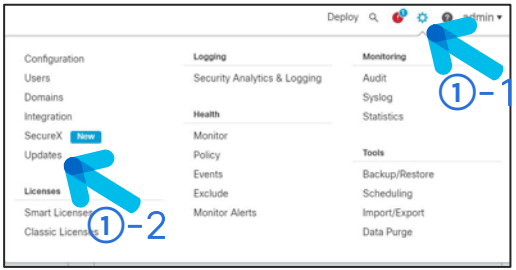


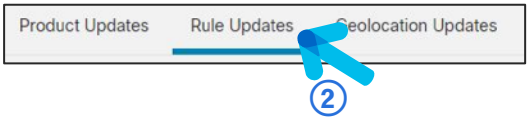




① System → Updates を選択
② Geolocation Updates を選択
③ [Enable Recurring Weekly Updates from the Support Site] へチェックを入れる
④ 更新タイミングを指定
⑤ Save をクリック

Snort Rules ワンタイム更新

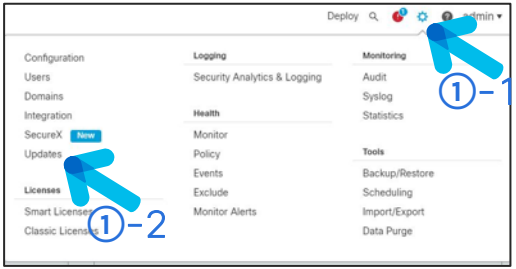


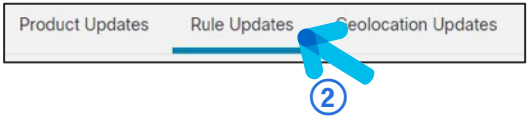


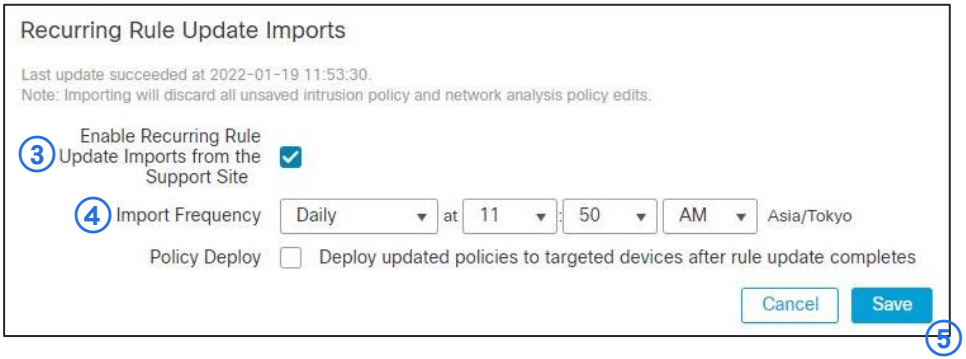
① System → Updates を選択
② Rule Updates を選択
③ いずれかを実施
   a. ローカル更新： Rule update or text rule file to upload and install を選択後、ファイルをアップロードして Import をクリック
   b. ダイレクト / Proxy 経由のクラウド更新：[Download and install geolocation update from the Support Site] を選択し、Import をクリック

- [Reapply all policies after the rule update import completes] にチェックを付けて Import を実行すると、Snort Rules 更新後に、ポリシーを設定された全ての FTD にしてルール配信 (deploy) を実行する
- 更新した Rule によっては、Deploy 時に Snort プロセスが再起動するため、FTD データ通信へ影響の発生する可能性がある

Snort Rules 定期更新



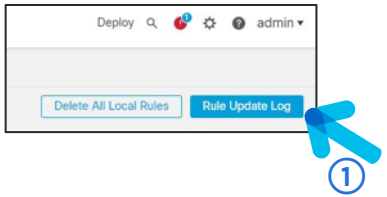


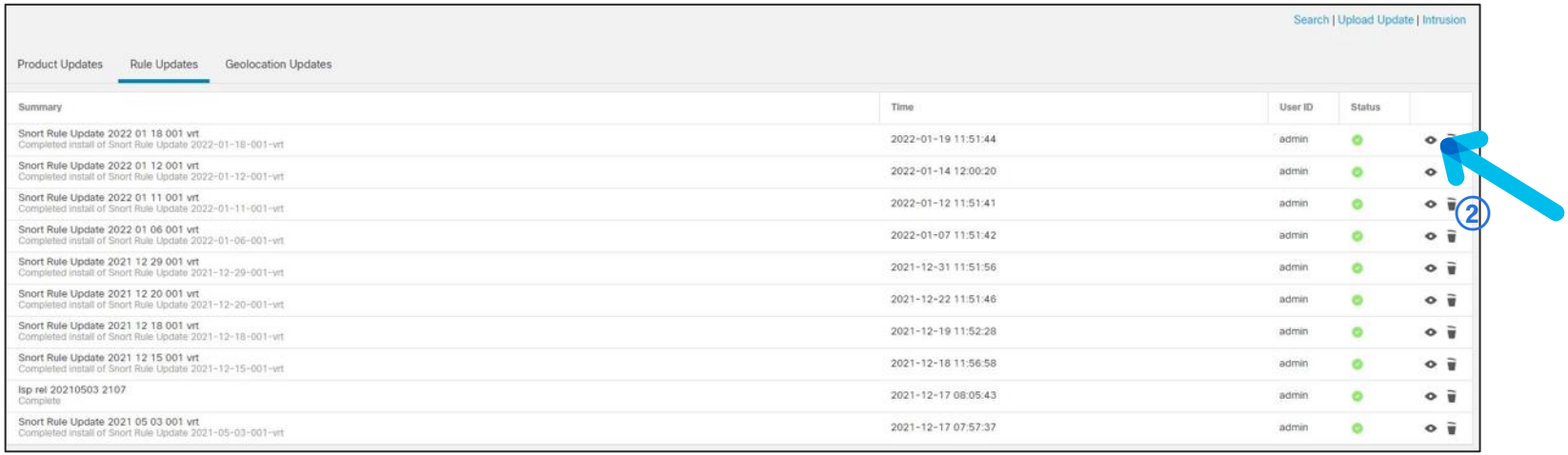


① System → Updates を選択
② Rule Updates を選択
③ [Enable Recurring Rule Update Imports from the Support Site] へチェックを付ける
④ Import Frequency にて更新頻度と実施時間帯を設定
⑤ Save をクリック

- [Deploy updated policies to targeted devices after rule update completes] にチェックを付けて Save すると、Snort Rules 更新後に、ポリシーを設定された全ての FTD にしてルール配信 (deploy) を実行する
- 更新した Rule によっては、Deploy 時に Snort プロセスが再起動するため、FTD データ通信へ影響の発生する可能性がある

Snort Rules 更新ログ





① Rule Update Log を選択。Rule Updates ログ一覧を参照できる
② インストールされたパッケージ (-vrt or lsp-) の View アイコンをクリックすると、更新パッケージ内の更新された Snort Rule を参照できる

Snort Rules 更新ログ

Product Updates | Rule Updates | Geolocation Updates

Rule Update Log

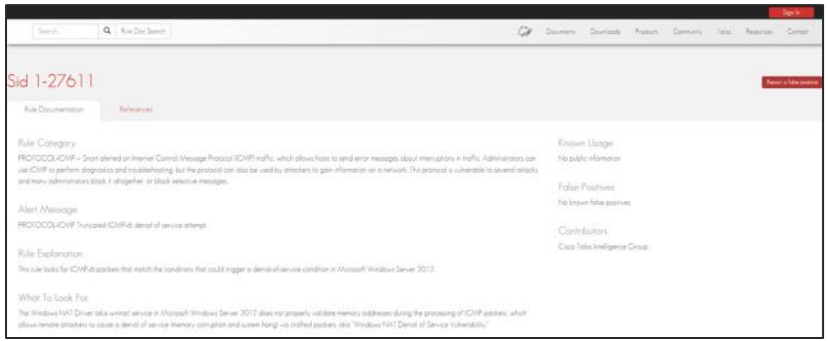
Search Constraints (Edit Search Save Search)

Table View of Rule Update Import Log

①-1

①-2

Time	Name	Type	Action	GID	SID	Rev	Policy	Details
2022-01-19 11:53:26	Sourcefire Rule Update	rule update component	changed					Upgrading Sourcefire Rule Update from 2022-01-12-001-vrt to 2022-01-18-001-vrt
2022-01-19 11:53:25	Sourcefire Decoder Rule Pack	rule update component	changed					Upgrading Sourcefire Decoder Rule Pack from 2047 to 2048
2022-01-19 11:53:12	Sourcefire Module Pack	rule update component	changed					Upgrading Sourcefire Module Pack from 3022 to 3023
2022-01-19 11:53:11	FILE-OTHER TRUFFLEHUNTER TALOS-2021-1435 attack attempt	rule	new	3	58881	1	All	New
2022-01-19 11:53:11	FILE-OTHER TRUFFLEHUNTER TALOS-2021-1436 attack attempt	rule	new	3	58882	1	All	New
2022-01-19 11:53:11	FILE-OTHER TRUFFLEHUNTER TALOS-2021-1436 attack attempt	rule	new	3	58883	1	All	New
2022-01-19 11:53:11	FILE-OTHER TRUFFLEHUNTER TALOS-2021-1437 attack attempt	rule	new	3	58895	1	All	New
2022-01-19 11:53:11	FILE-OTHER TRUFFLEHUNTER TALOS-2021-1437 attack attempt	rule	new	3	58896	1	All	New
2022-01-19 11:53:11	FILE-PDF TRUFFLEHUNTER TALOS-2022-1439 attack attempt	rule	new	3	58897	1	All	New
2022-01-19 11:53:11	FILE-PDF TRUFFLEHUNTER TALOS-2022-1439 attack attempt	rule	new	3	58898	1	All	New
2022-01-19 11:53:11	SERVER-WEBAPP TRUFFLEHUNTER TALOS-2022-1441 attack attempt	rule	new	3	58884	1	All	New
2022-01-19 11:53:11	SERVER-WEBAPP TRUFFLEHUNTER TALOS-2022-1441 attack attempt	rule	new	3	58885	1	All	New

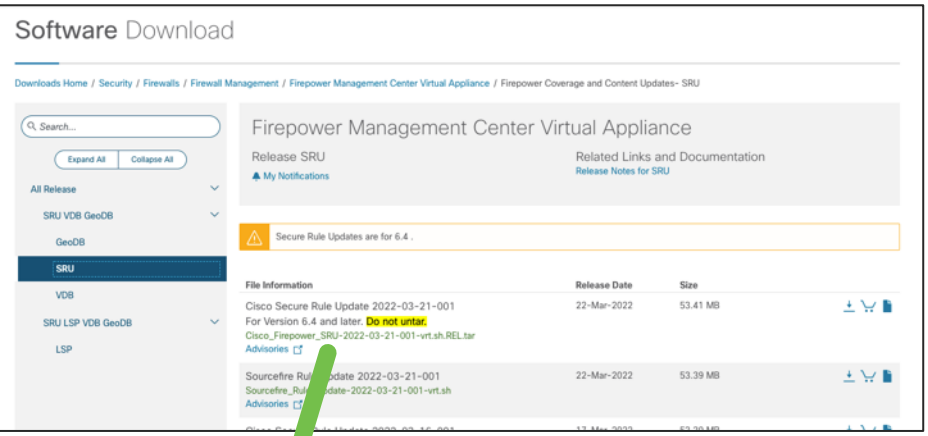


① Name、SID 列の表示内容は、オープンソース Snort コミュニティと同一

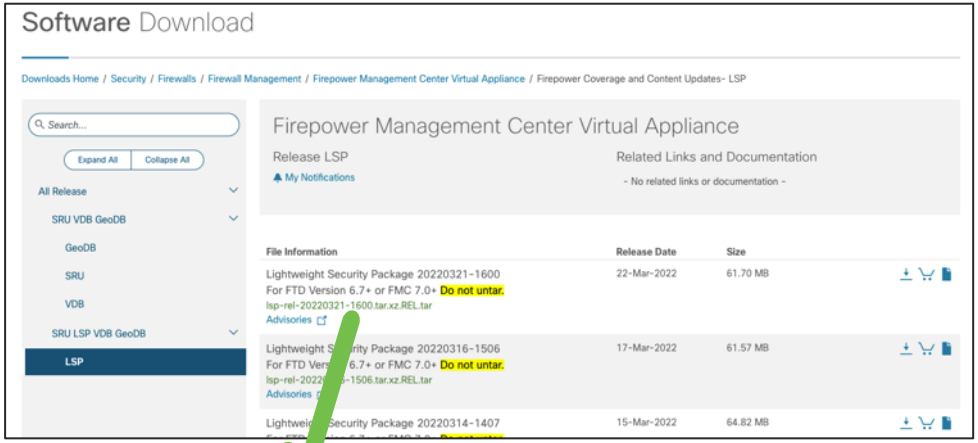
② snort.org にて SID 番号を検索すると、Snort Rule の詳細を参照できる

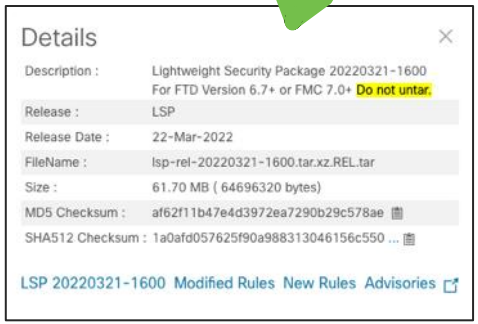
Snort Rules 更新ログ

- Cisco Software Download ページの Snort Rules ローカル更新用パッケージから、更新内容の確認が可能
- 対象の更新パッケージにカーソルを合わせて New Rules、Modified Rules をクリック



Snort 2 SRU





Snort 3 LSP

Snort Rules 更新ログ (Snort 2 SRU)

Cisco Talos Update for FireSIGHT Management Center

Date: 2022-03-22

This SRU number: 2022-03-21-001
Previous SRU number: 2022-03-16-001
Applies to:

- 3D Sensor versions: 5.4+ / 6.x
- Cisco FireSIGHT Management Center versions: 5.4+ / 6.x

Applies to:

- 3D Sensor Versions: 4.10
- Cisco FireSIGHT Management Center versions: 4.10

This is the complete list of rules added in SRU 2022-03-21-001.
The format of the file is:
GID - SID - Rule Group - Rule Message - Policy State
The Policy State refers to each default Cisco Talos policy, Connectivity, Balanced, Security, and Maximum Detection.
The default passive policy state is the same as the Balanced policy state with the exception of alert being used instead of drop.
Note: Unless stated explicitly, the rules are for the series of products listed above.

New Rules:

High Priority

GID	SID	Rule Group	Rule Message	Policy State			
				Con.	Bal.	Sec.	Max.
1	59280	SERVER-WEBAPP	Medical Center Portal Management System SQL injection attempt	off	off	off	off
1	59281	SERVER-WEBAPP	Trend Micro Deep Discovery Email Inspector Virtual Appliance network_dump command injection attempt	off	off	off	drop
1	59282	SERVER-WEBAPP	Trend Micro Smart Protection Server wcs_bwlists_handler command injection attempt	off	off	off	drop
1	59283	SERVER-WEBAPP	Trend Micro Smart Protection Server wcs_bwlists_handler command injection attempt	off	off	off	drop
1	59284	SERVER-WEBAPP	Trend Micro Smart Protection Server wcs_bwlists_handler command injection attempt	off	off	off	drop
1	59285	SERVER-WEBAPP	Trend Micro Smart Protection Server wcs_bwlists_handler command injection attempt	off	off	off	drop
1	59286	SERVER-WEBAPP	Trend Micro Control Manager Widget modDLPTemplateMatch_drildown directory traversal attempt	off	off	off	drop
3	59288	SERVER-OTHER	TRUFFLEHUNTER TALOS-2022-1478 attack attempt	off	off	drop	drop
3	59289	SERVER-OTHER	TRUFFLEHUNTER TALOS-2022-1483 attack attempt	off	off	drop	drop
3	59290	SERVER-OTHER	TRUFFLEHUNTER TALOS-2022-1484 attack attempt	off	off	drop	drop
3	59291	SERVER-OTHER	TRUFFLEHUNTER TALOS-2022-1482 attack attempt	off	off	drop	drop

Low Priority

GID	SID	Rule Group	Rule Message	Policy State			
				Con.	Bal.	Sec.	Max.
3	59287	SERVER-OTHER	TRUFFLEHUNTER TALOS-2022-1478 attack attempt	off	off	alert	alert

Cisco Talos Update for FireSIGHT Management Center

Date: 2022-03-22

This SRU number: 2022-03-21-001
Previous SRU number: 2022-03-16-001
Applies to:

- 3D Sensor versions: 5.4+ / 6.x
- Cisco FireSIGHT Management Center versions: 5.4+ / 6.x

Applies to:

- 3D Sensor Versions: 4.10
- Cisco FireSIGHT Management Center versions: 4.10

This is the complete list of rules modified in SRU 2022-03-21-001.
The format of the file is:
GID - SID - Rule Group - Rule Message - Policy State
The Policy State refers to each default Cisco Talos policy, Connectivity, Balanced, Security, and Maximum Detection.
The default passive policy state is the same as the Balanced policy state with the exception of alert being used instead of drop.
Note: Unless stated explicitly, the rules are for the series of products listed above.

Updated Rules:

High Priority

GID	SID	Rule Group	Rule Message	Policy State			
				Con.	Bal.	Sec.	Max.
1	45117	SERVER-WEBAPP	Huawei DeviceUpgrade command injection attempt	off	off	drop	drop
1	59070	SERVER-WEBAPP	Trend Micro SafeSync for Enterprise SQL injection attempt	off	off	off	drop
3	59275	POLICY-OTHER	TRUFFLEHUNTER TALOS-2022-1492 attack attempt	off	off	off	off
3	59276	POLICY-OTHER	TRUFFLEHUNTER TALOS-2022-1492 attack attempt	off	off	off	off

Snort Rules 更新ログ (Snort 3 LSP)

Cisco Talos Update for FireSIGHT Management Center

Date: 2022-03-22

This LSP: 20220321-1600 (LightSPD 2022-03-21-001)
Previous LSP: 20220316-1506 (LightSPD 2022-03-16-001)
Applies to:

- Cisco FireSIGHT Management Center versions: 6.7+

This is the complete list of rules added in LSP 20220321-1600 (LightSPD 2022-03-21-001).
The format of the file is:
GID - SID - Rule Group - Rule Message - Policy State - CVE(if any)
The Policy State refers to each default Cisco Talos policy, Connectivity, Balanced, Security, and Maximum Detection.
The default passive policy state is the same as the Balanced policy state with the exception of alert being used instead of drop.
Note: Unless stated explicitly, the rules are for the series of products listed above.

New Rules:

GID	SID	Rule Group	Rule Message	Policy State				CVE
				Con.	Bal.	Sec.	Max.	
1	59280	SERVER-WEBAPP	SERVER-WEBAPP Medical Center Portal Management System SQL injection attempt	off	off	off	off	
1	59281	SERVER-WEBAPP	SERVER-WEBAPP Trend Micro Deep Discovery Email Inspector Virtual Appliance network_dump command injection attempt	off	off	off	on	
1	59282	SERVER-WEBAPP	SERVER-WEBAPP Trend Micro Smart Protection Server wcs_bwlists_handler command injection attempt	off	off	off	on	
1	59283	SERVER-WEBAPP	SERVER-WEBAPP Trend Micro Smart Protection Server wcs_bwlists_handler command injection attempt	off	off	off	on	
1	59284	SERVER-WEBAPP	SERVER-WEBAPP Trend Micro Smart Protection Server wcs_bwlists_handler command injection attempt	off	off	off	on	
1	59285	SERVER-WEBAPP	SERVER-WEBAPP Trend Micro Smart Protection Server wcs_bwlists_handler command injection attempt	off	off	off	on	
1	59286	SERVER-WEBAPP	SERVER-WEBAPP Trend Micro Control Manager Widget modDLPTemplateMatch_drildown directory traversal attempt	off	off	off	on	
3	59287	SERVER-OTHER	SERVER-OTHER TRUFFLEHUNTER TALOS-2022-1478 attack attempt	off	off	on	on	CVE-2022-26042,
3	59288	SERVER-OTHER	SERVER-OTHER TRUFFLEHUNTER TALOS-2022-1478 attack attempt	off	off	on	on	CVE-2022-26042,
3	59289	SERVER-OTHER	SERVER-OTHER TRUFFLEHUNTER TALOS-2022-1483 attack attempt	off	off	on	on	CVE-2022-26009,
3	59290	SERVER-OTHER	SERVER-OTHER TRUFFLEHUNTER TALOS-2022-1484 attack attempt	off	off	on	on	CVE-2022-26342,
3	59291	SERVER-OTHER	SERVER-OTHER TRUFFLEHUNTER TALOS-2022-1482 attack attempt	off	off	on	on	CVE-2022-25996,

Cisco Talos Update for FireSIGHT Management Center

Date: 2022-03-22

This LSP: 20220321-1600 (LightSPD 2022-03-21-001)
Previous LSP: 20220316-1506 (LightSPD 2022-03-16-001)
Applies to:

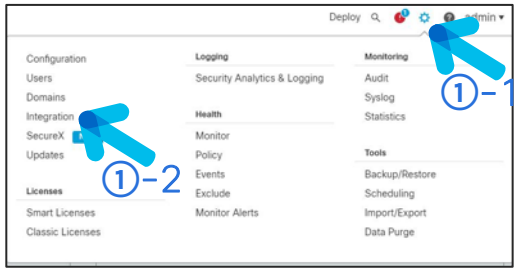
- Cisco FireSIGHT Management Center versions: 6.7+

This is the complete list of rules modified in LSP 20220321-1600 (LightSPD 2022-03-21-001).
The format of the file is:
GID - SID - Rule Group - Rule Message - Policy State - CVE (if any)
The Policy State refers to each default Cisco Talos policy, Connectivity, Balanced, Security, and Maximum Detection.
The default passive policy state is the same as the Balanced policy state with the exception of alert being used instead of drop.
Note: Unless stated explicitly, the rules are for the series of products listed above.

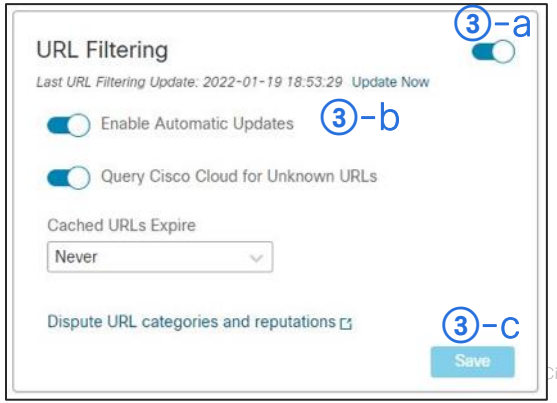
Updated Rules:

GID	SID	Rule Group	Rule Message	Policy State				CVE
				Con.	Bal.	Sec.	Max.	
1	45117	SERVER-WEBAPP	SERVER-WEBAPP Huawei DeviceUpgrade command injection attempt	off	off	on	on	CVE-2017-17215,
1	59070	SERVER-WEBAPP	SERVER-WEBAPP Trend Micro SafeSync for Enterprise SQL injection attempt	off	off	off	on	
3	59275	POLICY-OTHER	POLICY-OTHER TRUFFLEHUNTER TALOS-2022-1492 attack attempt	off	off	off	off	CVE-2022-26043,CVE-2022-26067,CVE-2022-26082,
3	59276	POLICY-OTHER	POLICY-OTHER TRUFFLEHUNTER TALOS-2022-1492 attack attempt	off	off	off	off	CVE-2022-26067,CVE-2022-26082,CVE-2022-26303,

URL Filtering ワンタイム・定期更新

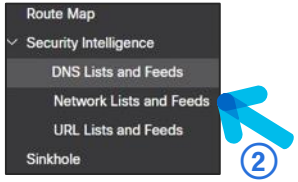


① System → Tools → Integration を選択
② Cloud Services を選択
③ URL Filtering より下記を設定
   a. URL Filtering 機能自体の有効化
   b. (定期更新を行う場合) Enable Automatic Update の有効化
   c. Save をクリック

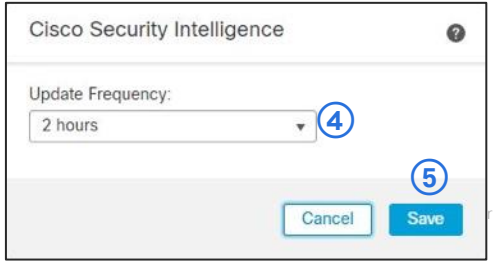


- Enable Automatic Update: 30分ごとにアップデートを確認する (定期更新・ダイレクトもしくは Proxy 経由更新のみ)
- Query Cisco Cloud for Unknown URLs: URL カテゴリやレピュテーションがローカルで確認できない場合に、クラウドへ照会する。プライバシーの問題等でこの機能を利用したくない場合は無効にする。
- 通信要件は Firepower Management Center Configuration Guide, Version 7.0 の Security Requirements に記載 (※使用しているソフトウェアバージョンのドキュメントを参照すること)

Security Intelligence ワンタイム・定期更新

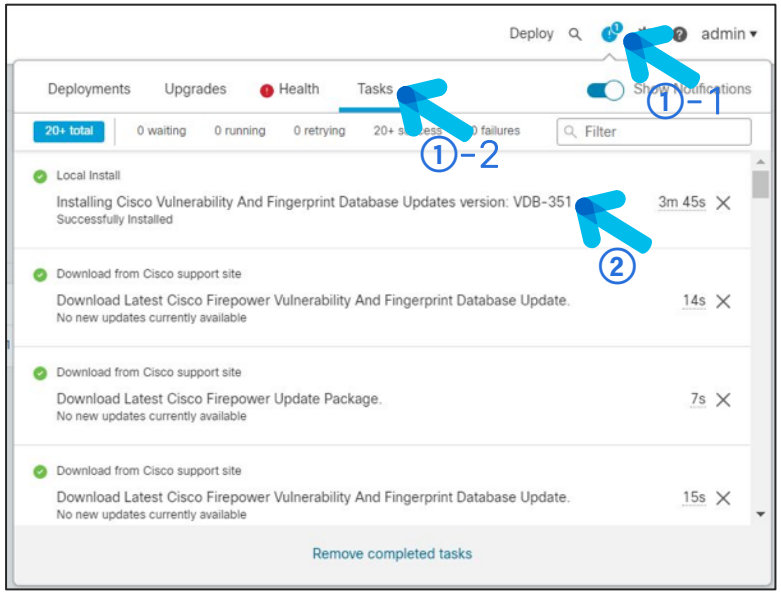


① Object → Object Management を選択
② 画面左側メニューより、Security Intelligence → 対象のオブジェクト種別 (DNS Lists and Feeds、Network Lusts and Feeds) を選択
③ 対象のオブジェクトの鉛筆アイコンをクリック
④ Update Frequency にて定期更新の頻度を変更
⑤ Save をクリック



- デフォルトの更新間隔
  - Cisco-DNS-and-URL-Intelligence-Feed：2 hours
  - Cisco-Intelligence-Feed：2 hours
  - Cisco-TID-Feed：5 minutes
- 画面上部→側の Update Feeds をクリックすると、ワンタイム更新を実行する

【参考情報】
Tasks による更新ファイルのインストール結果確認



① Notifications → Tasks を選択
② 対象のアップデートファイルのインストール完了を確認する。画面は Cisco Vulnerability And Fingerprint Database Updates version: VDB-351 の例

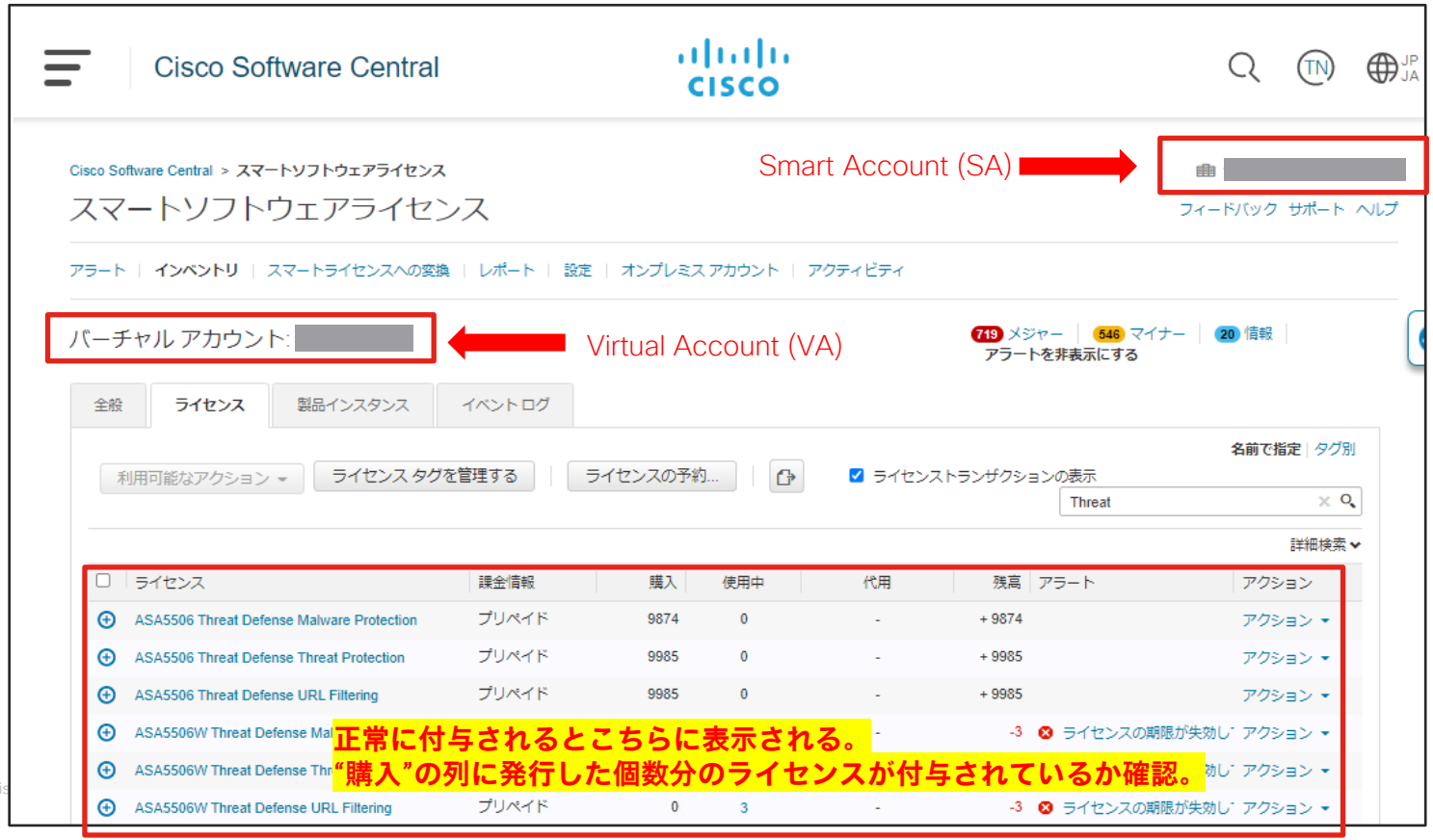
4. スマートライセンスの適用

CSSM にてライセンス確認

Cisco Smart Software Manager (CSSM)

https://www.cisco.com/c/ja_jp/buy/smart-accounts/software-manager.html

CSSM にてライセンス確認



トークン発行

機器登録の流れ：

① CSSM の、インベントリ > 全般 から “新しいトークン”発行
② 発行した トークン を機器に設定
③ トークンに記載されている SA (VA) に登録処理が行われる
④ VA に該当ライセンスがあれば”使用中”にカウントされる。なければ ”-1” となり機材側は ”out of compliance” となる

トークン発行

※ 最新の Token は一番上に表示される。

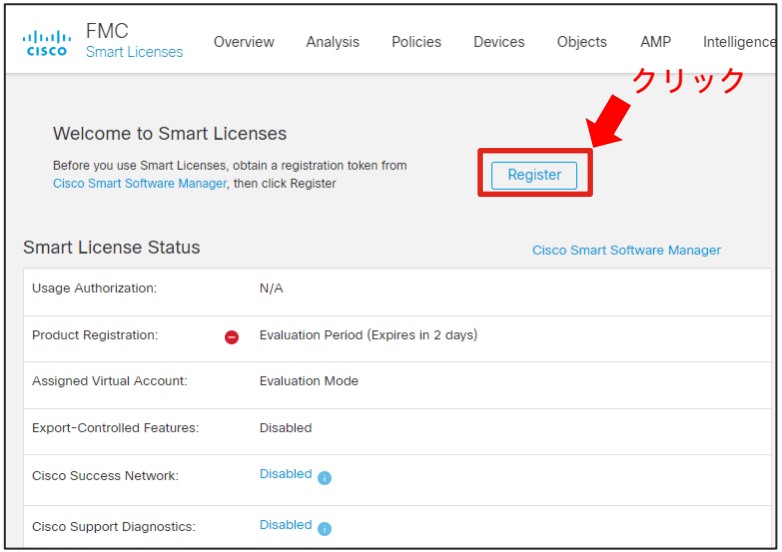
Actions のプルダウンから
Copy をクリック

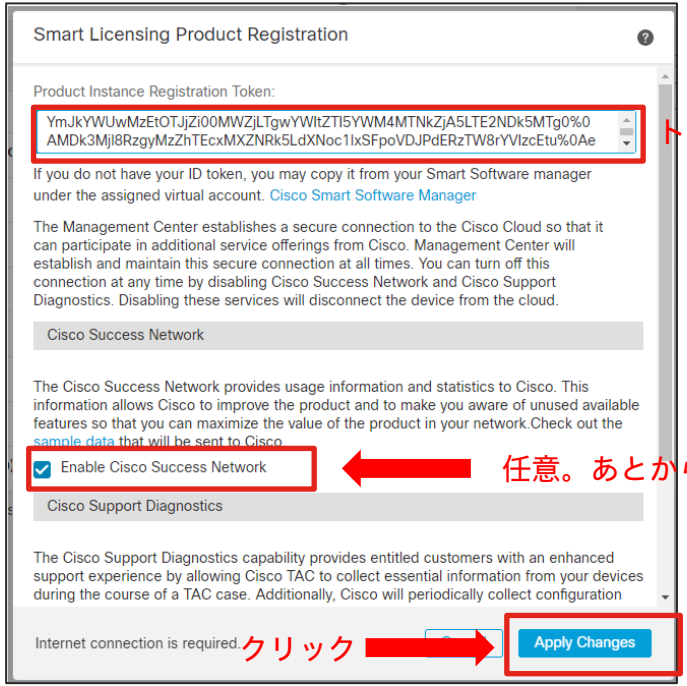
FMC のスマートライセンス登録

※ FTD を FMC 管理とする場合、FTD で利用するライセンスは FMC にて管理される。

※ Cisco Success Network: FMC の利用状況をシスコに共有する仕組み

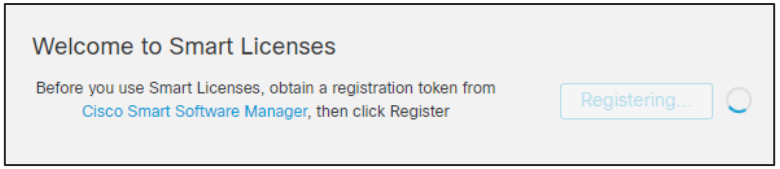
System > Licenses > Smart Licenses



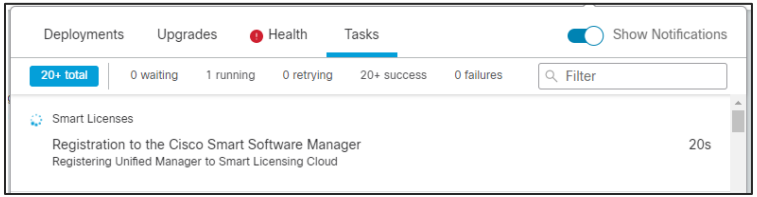


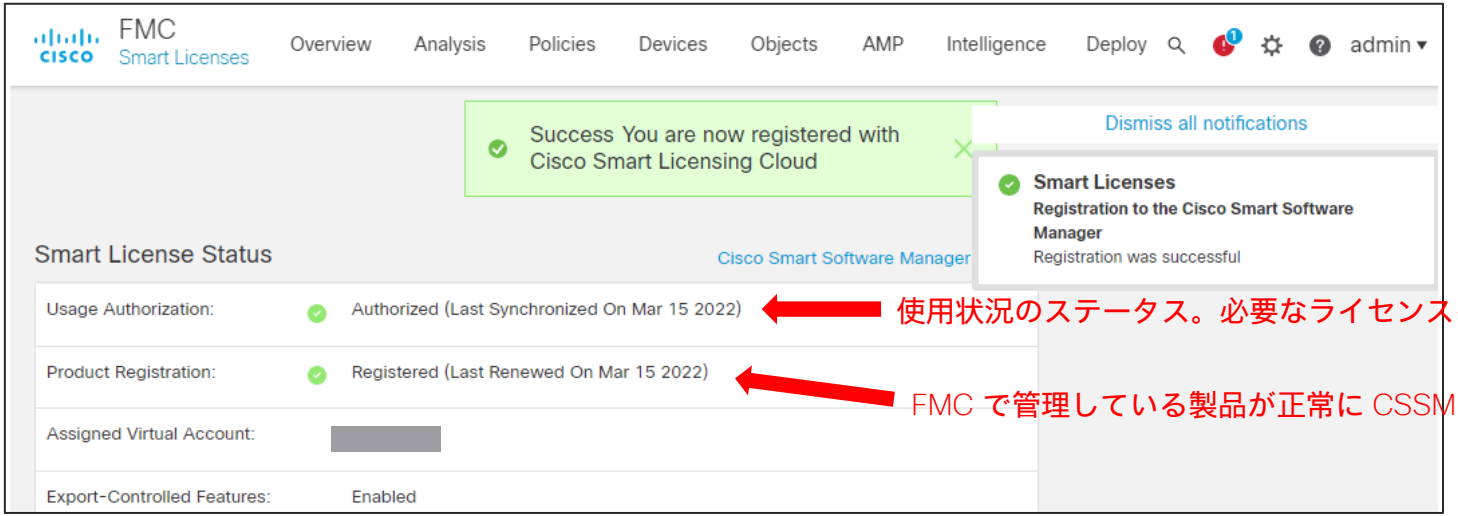
FMC の SL 登録

登録処理中の画面



Tasks でも状況確認が可能





使用状況のステータス。必要なライセンスを保有していれば Authorized

FMC で管理している製品が正常に CSSM 側に登録されると Registered

5. FMC と FTD の Upgrade / Patch インストール

Firewall ソフトウェアライフサイクルポリシー

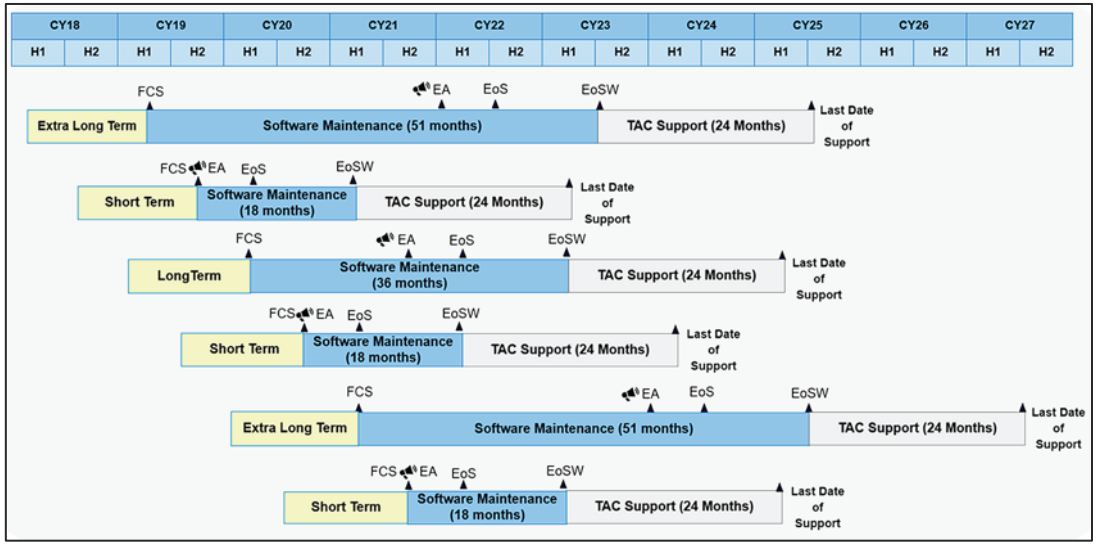
Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin
https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html

- 年の前半と後半にそれぞれ新しいソフトウェアをリリースする
- FTD (ASA も) のバージョンの数字の小数点1桁目が偶数ならロングタームサポート、奇数ならショートタームサポートとなる

  FTD 6.5 → ショートタームサポート

  FTD 6.6 → ロングタームサポート
- ロングタームサポートの中でも、奇数年にリリースされるものはエクストラロングタームサポートとなる

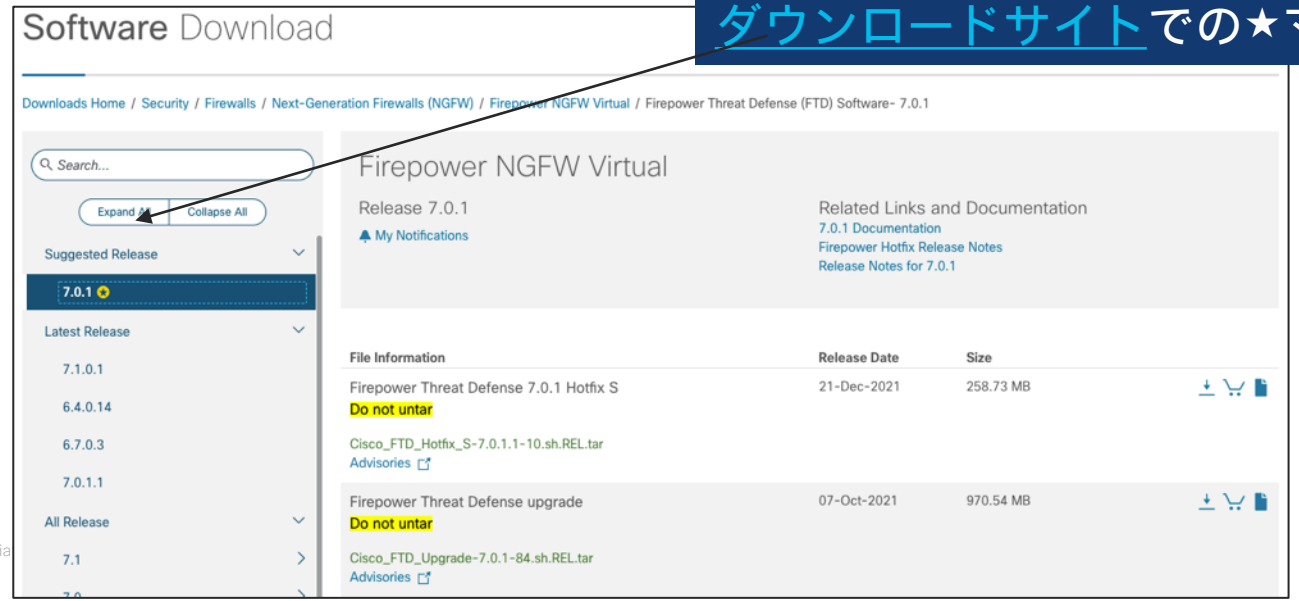
  FTD 7.0 → 2021年前半リリースなのでエクストラロングタームサポート



FMC / FTD 一般的な推奨ソフトウェアバージョン

- 2022年3月時点で一般的な推奨バージョンは 7.0.1
  - 本ガイドではバージョン 7.0.1.1-11 の Patch をインストールする
- 稼働実績と重大な障害の数、および重大な不具合の数を総合的に見て推奨バージョンを選定している

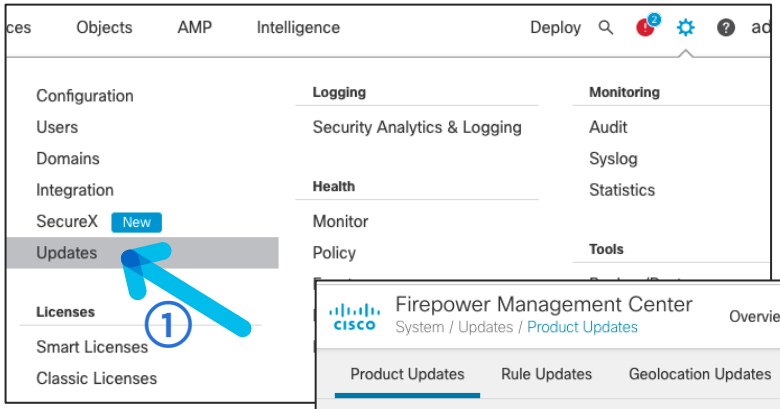
ダウンロードサイトでの★マークに注目



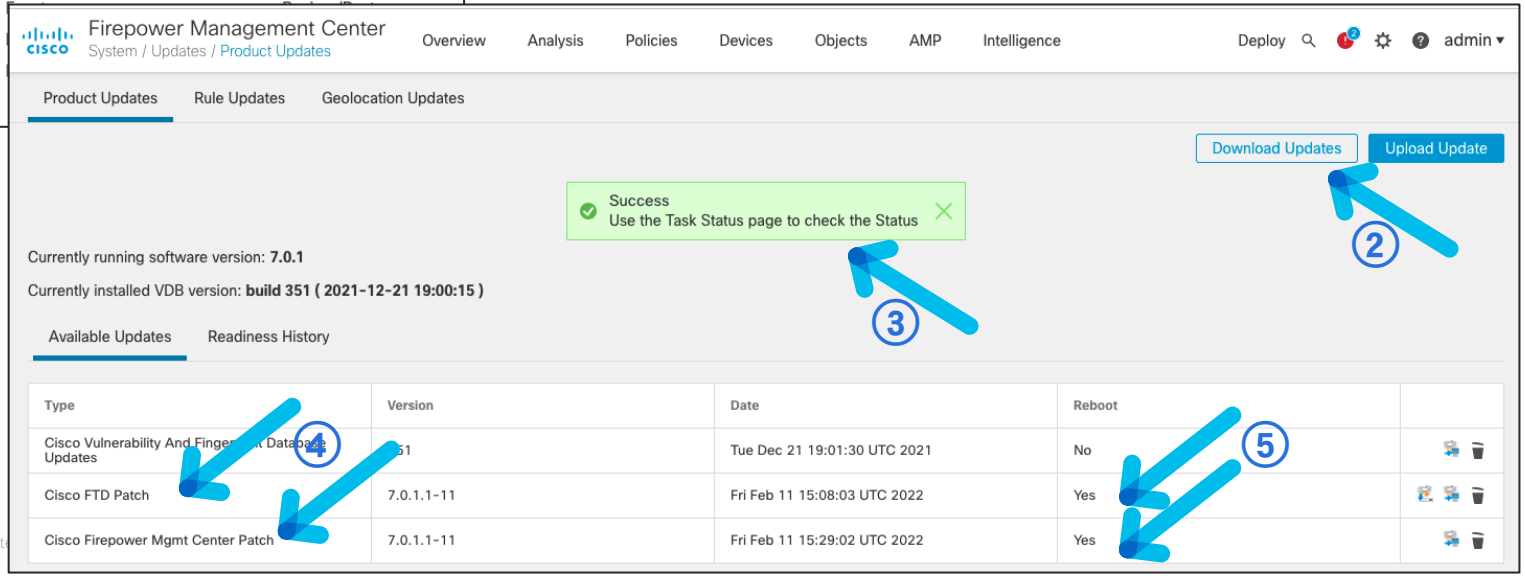
FMC と FTD Upgrade / Patch インストールの注意点

- 事前に FMC および FTD の backup を取得しておく (本章では割愛)
- できるだけ FMC と FTD のソフトウェアバージョンは合わせた方が良いが、異なるバージョンにする場合には、FMC 側が上位バージョンである必要があり、かつ、コンパチビリティを保つ必要がある。コンパチビリティガイド Table 18 参照。
- 作業は FMC の GUI で実施。Upgrade の順番は、FMC が先、FTD が後
- インストールファイルは FMC での自動ダウンロードもしくは cisco.com からの手動ダウンロードにて入手する
- Upgrade / Patch インストール前に、未適用の設定は deploy を実施しておく
- FP4100/9300 の FTD Upgrade / Patch インストールは、FXOS とのコンパチビリティを事前に調べ、必要に応じて FTD より先に FXOS 側の Upgrade を実施する。FTD の Upgrade / Patch インストールは FMC にて行う (FCM: Firepower Chassis Manager 側では行わない)。コンパチビリティガイド Table 11 参照。

FMC での upgrade / patch 自動ダウンロード



① System (歯車マーク) → Updates を選択
② Download Updates をクリック
③ ダウンロードタスクがキューイングされ、
④ その後、この環境に適用できる Upgrade / Patch ファイルイメージがダウンロードされる
⑤ インストール時の reboot の有無が表示される



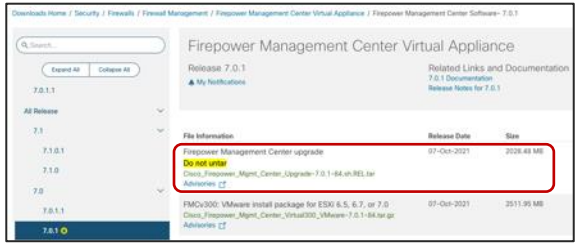
小数点1桁目の数字が変わる Major Upgrade はこの方法は使えず、Cisco.com からファイルを入手する必要がある

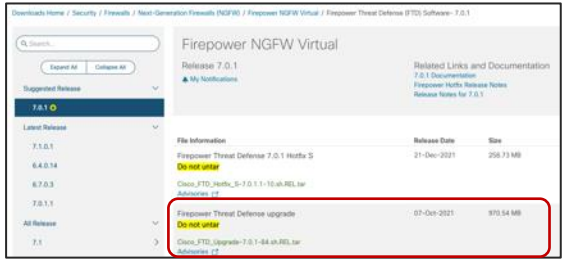
FMC での自動 DL 実施時にはスキップ

cisco.com からのイメージ入手

FMC での自動ダウンロードを使わない場合には、cisco.com からイメージファイルを入手今回は、7.0.1-84 から 7.0.1.1-11 への Patch インストールなので FMCv 用と FTDv 用のそれぞれの Patch イメージファイルをダウンロードする (アップグレードパスは Release Notes 参照)

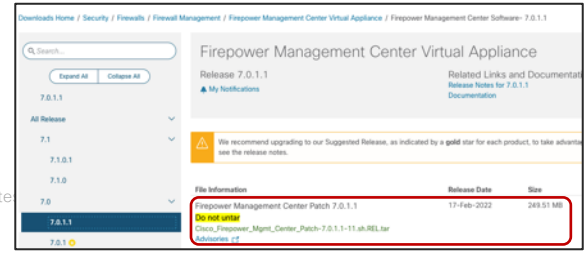
7.0.1-84 への Upgrade 用ファイル

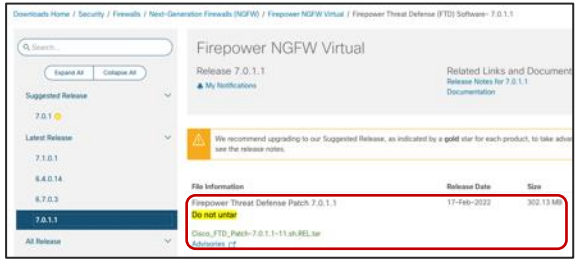




今回はこちら

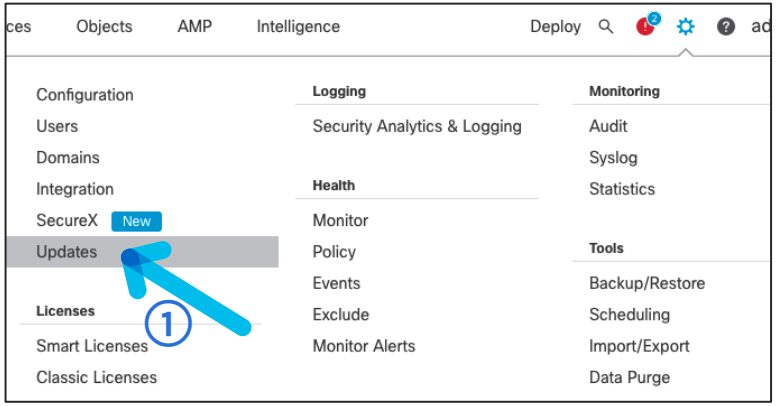
7.0.1.1-11 の Patch インストール 用ファイル



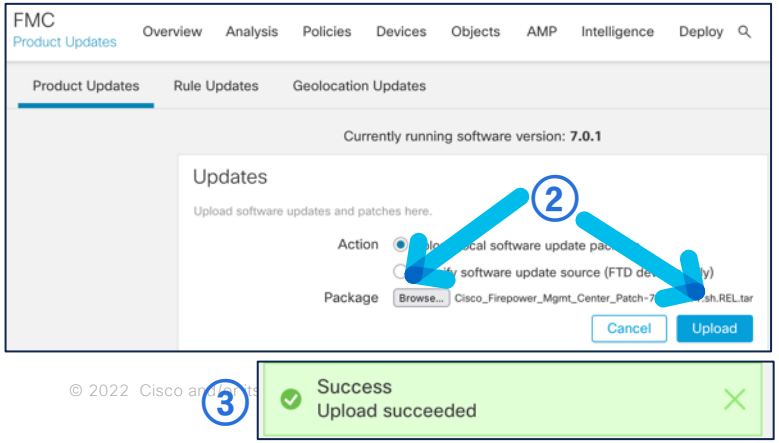


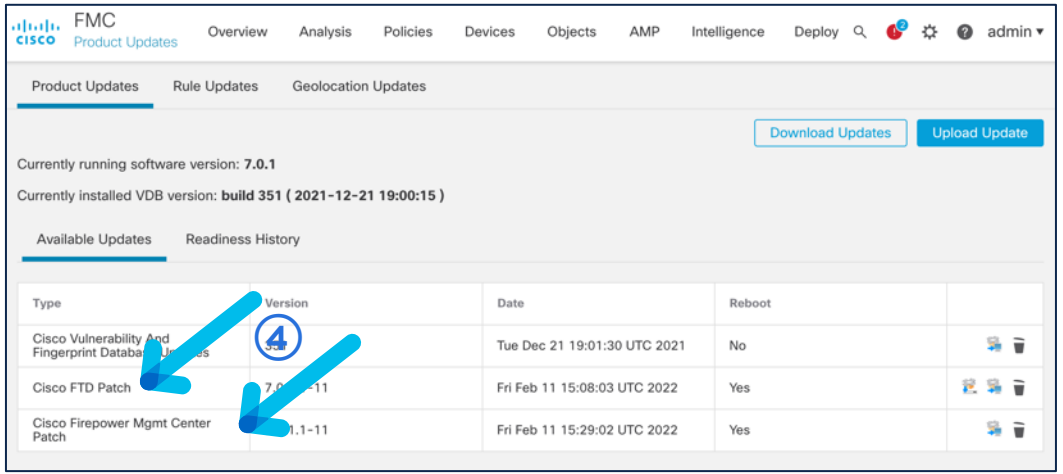
FMC での自動 DL 実施時にはスキップ

FMC への upgrade / patch ファイルアップロード



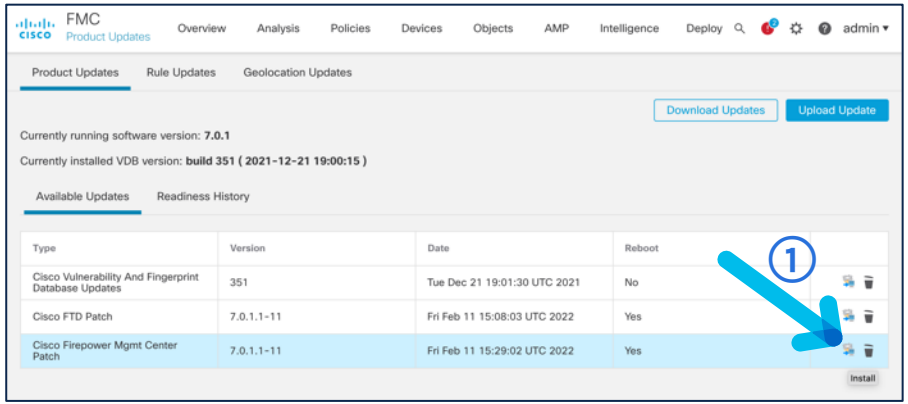
① System (歯車マーク) → Updates を選択
② Package → Browse からインストールするファイルを指定し、Upload をクリック
③ FMC へのアップロードが正しく終わったら表示される
④ アップロードした Upgrade / Patch インストール用ファイルが一覧に表示される

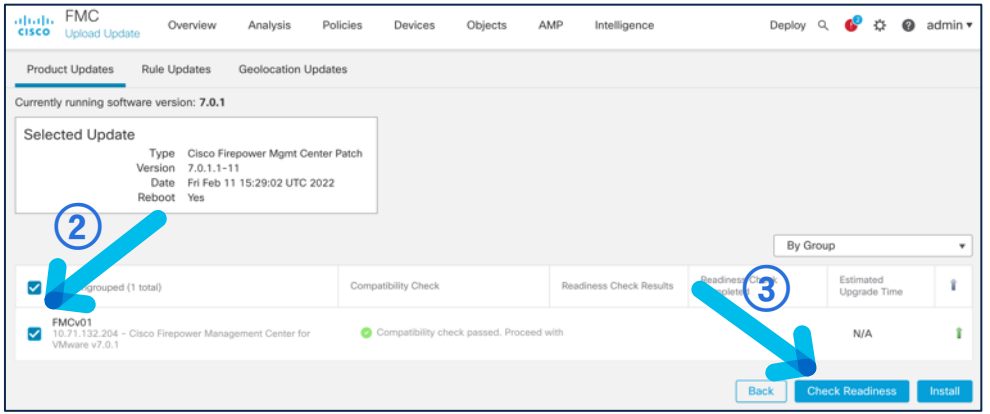




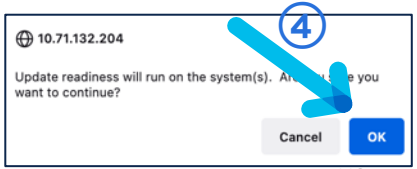
Readiness Check の実施

FMC と FTD を同時に Upgrade / Patch インストールする場合、FMC から先に実施すること
Upgrade / Patch インストールに指定のファイルを使って問題がないかを、実際に Upgrade / Patch インストールを行う前にチェックすること (Readiness Check) が可能



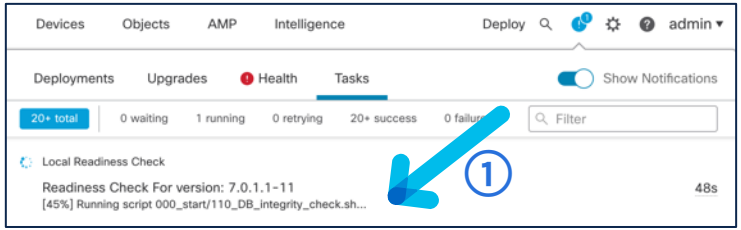


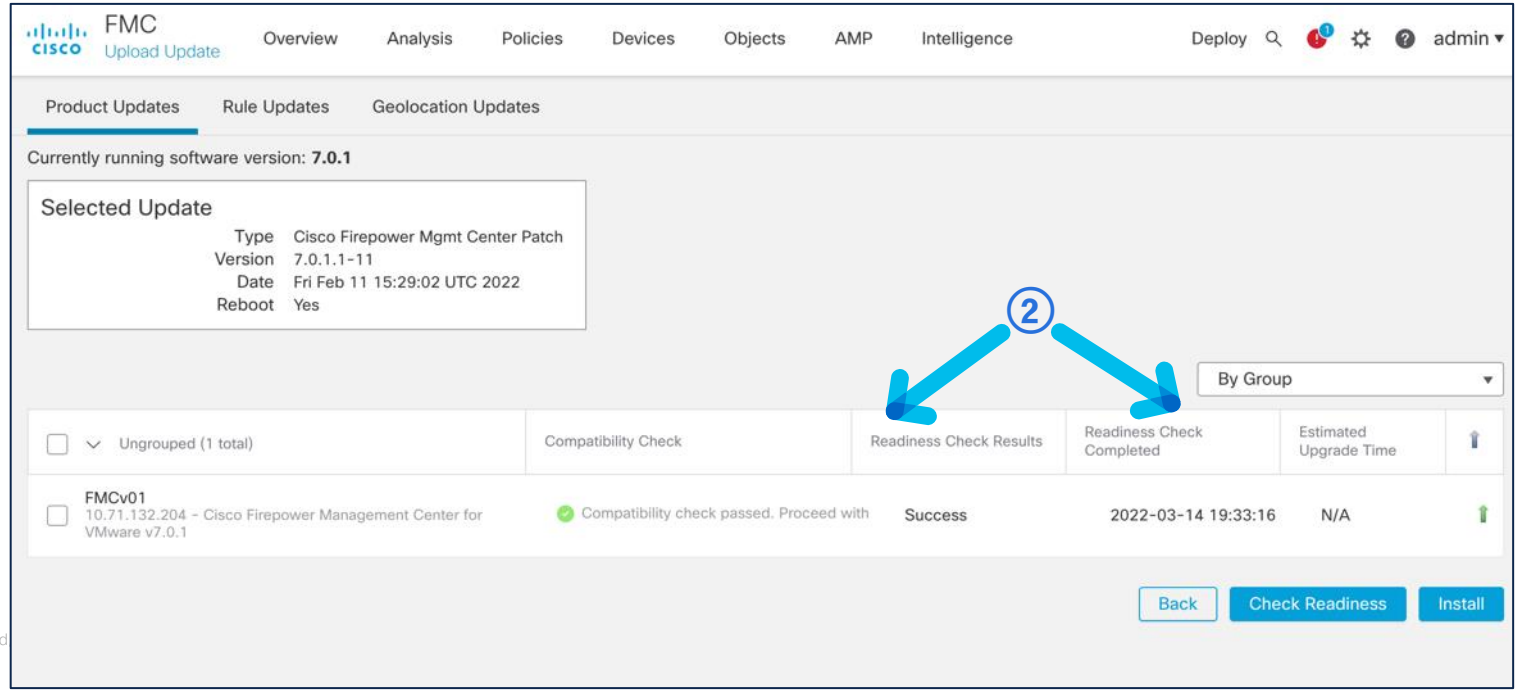
① Upgrade / Patch インストールしたいファイルを選択し、”Install” のアイコンをクリック
② そのファイルに対応したデバイス一覧 (この画面の場合は FMC) が表示されるので、Readiness Check をしたいデバイスを選択
③ Check Readiness をクリック
④ Readiness Check を本当に実施するかの確認が出るので、OK をクリックして実施



Readiness Check の実施

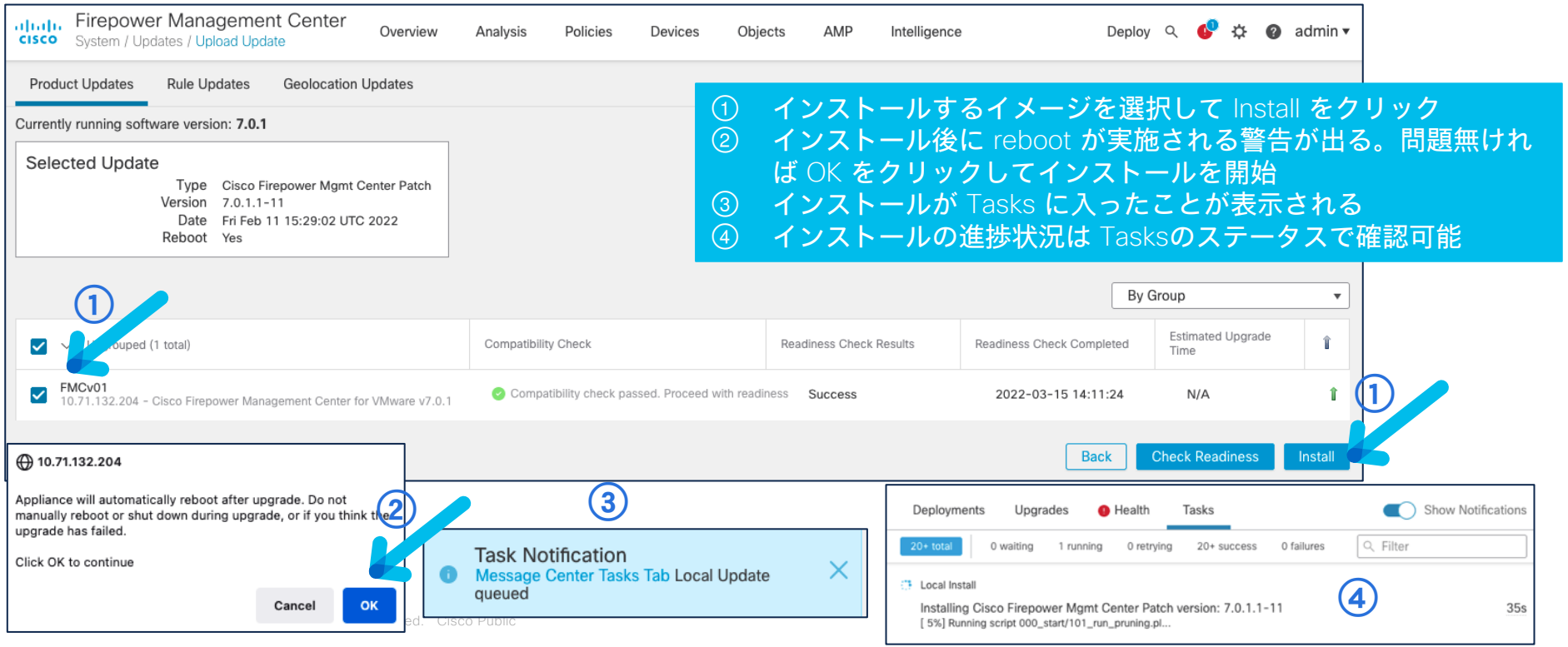
① Readiness Check の進捗具合は Tasks のステータスで確認可能
② Readiness Check が終わると Result と完了時刻が記録される。成功しなかった場合は、問題の原因を調べて解決させる





FMC Upgrade / Patch インストールの実施

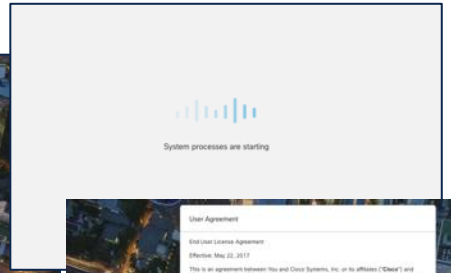
Readiness Check 成功後、実際に FMC へのインストールを実施



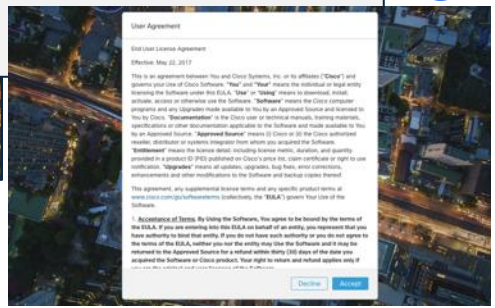
FMC Upgrade / Patch インストールの実施

①

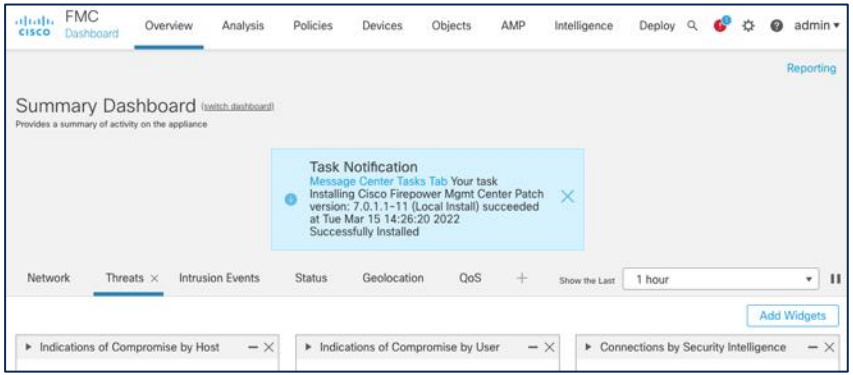
②

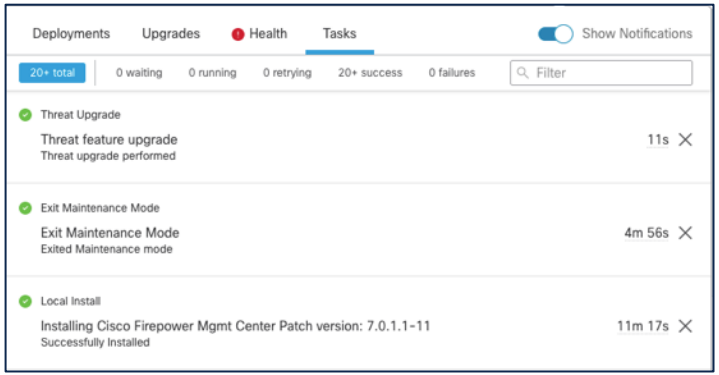


③



④



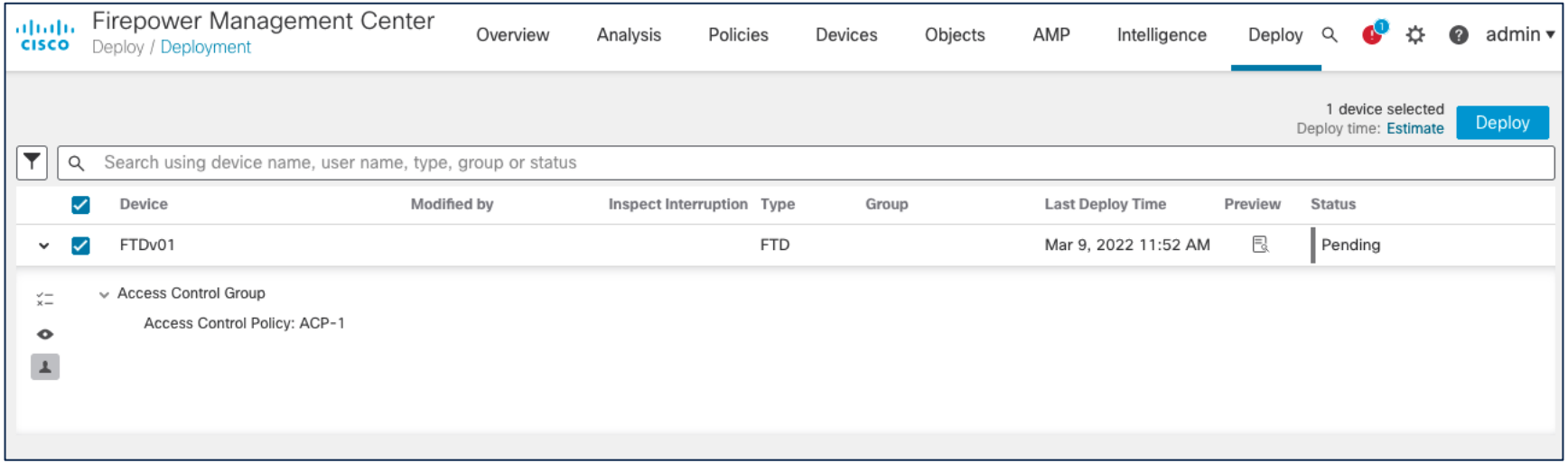


⑤

① インストール中に自動的にログアウトされ、FMC が再起動する
② 再起動後、FMC にアクセスした際、まだ起動プロセス中であればこの画面が出るので待つ
③ 再起動後、無事に管理者がログインできると、License Agreement 画面が出るので Accept する
④ ログイン完了、インストールの詳細が Tasks に入った旨の画面が残っている
⑤ Tasks スタータス画面にアクセスし、インストール作業の結果を確認

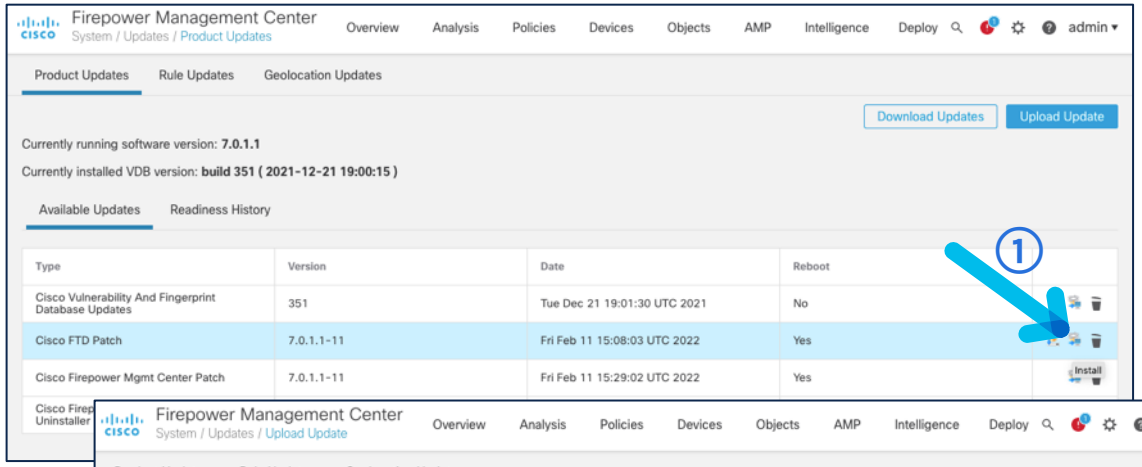
FMC Upgrade / Patch インストール後の Deploy

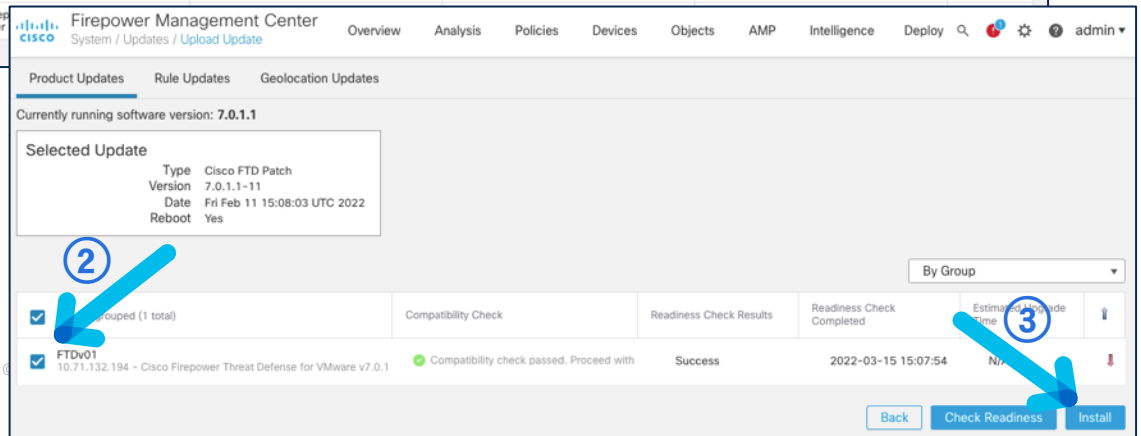
FMC Upgrade / Patch インストール後には、設定変更が無くても Deploy が必要



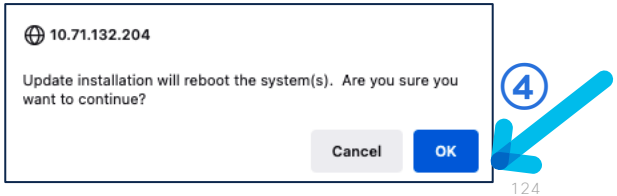
FTD Upgrade / Patch インストールの実施

FMC と同様に、FTD にも Readiness Check 実施後、Upgrade / Patch インストールを実施



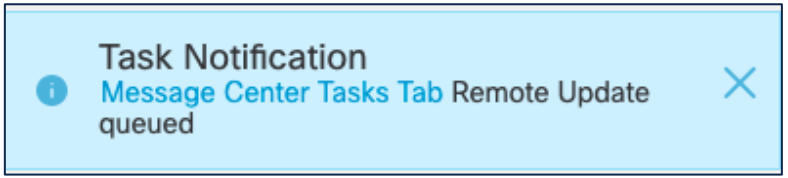


① インストールするイメージを選択し、Install のアイコンをクリック
② インストールするイメージを選択
③ Readiness Check が無事に完了していることを確認し、Install をクリック
④ インストール時に reboot が実施される警告が表示されるので OK をクリックし、インストールを開始

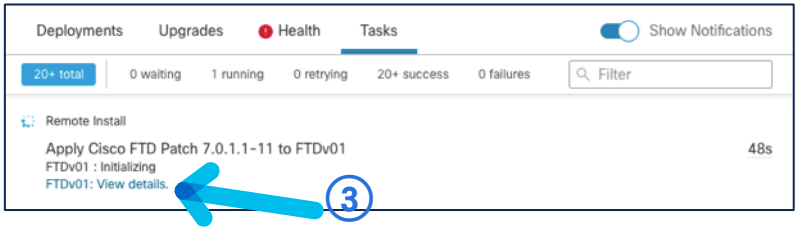


FTD Upgrade / Patch インストールの実施

①

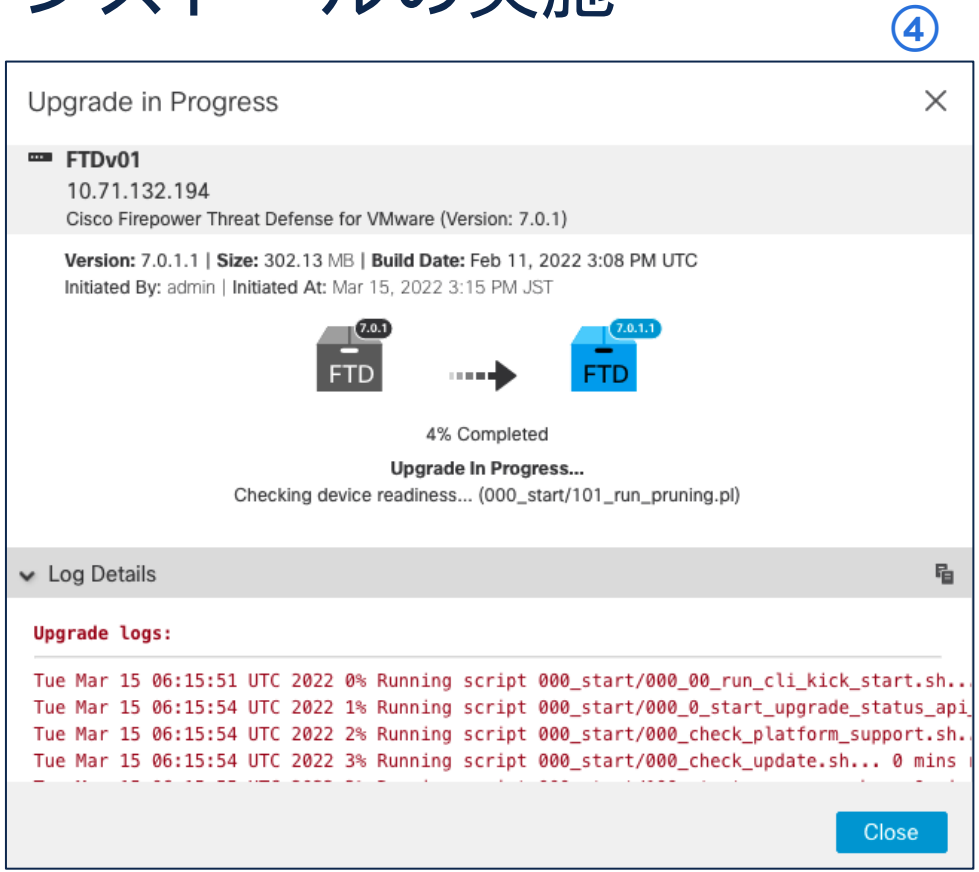


②



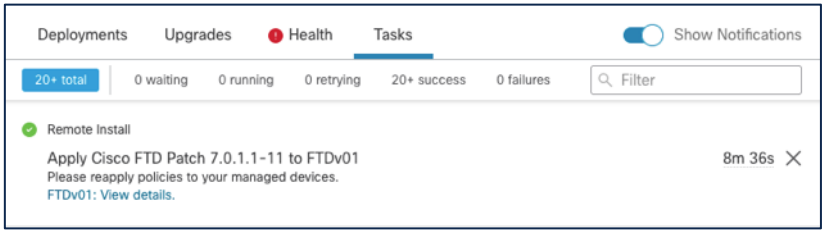
① インストールが Tasks に入ったことが表示される
② インストールの進捗状況は Tasks のステータスで確認可能
③ インストール中のデバイスの View Details をクリックすると、
④ インストール状況の詳細を確認できる

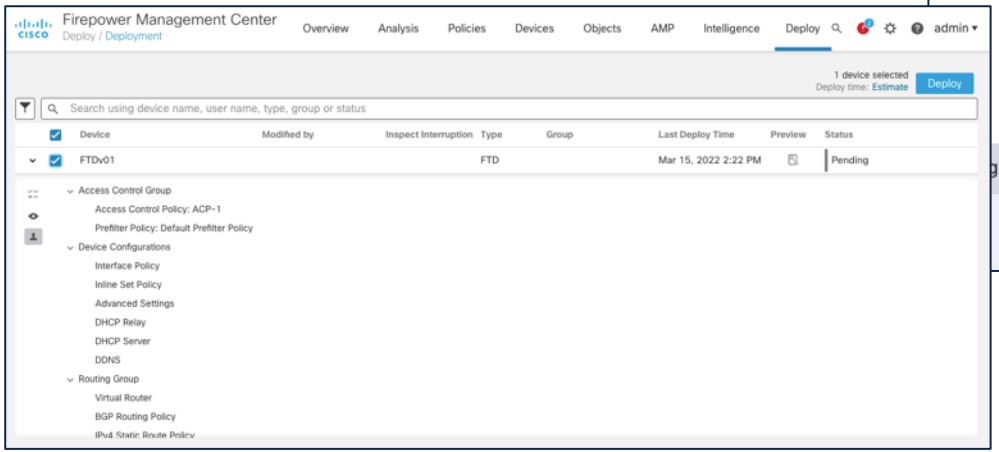
④

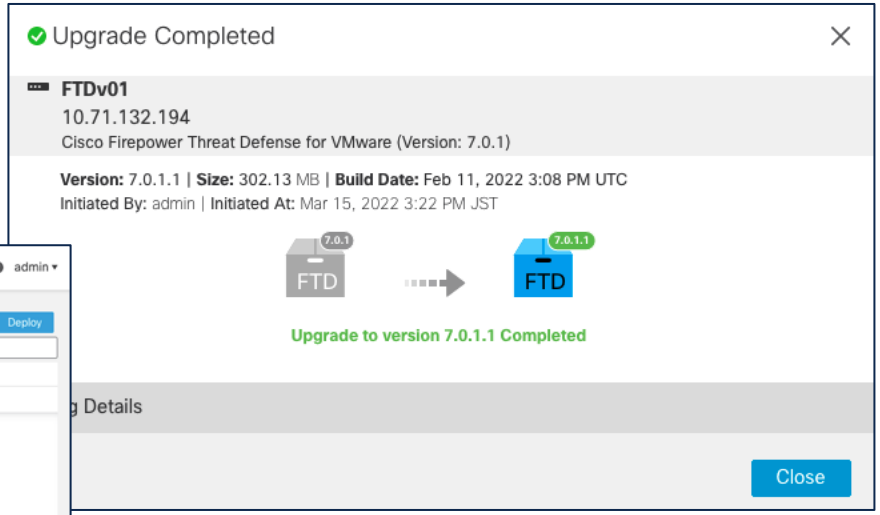


FTD Upgrade / Patch インストール結果確認と再 deploy の実施

FTD Upgrade / Patch インストール後に Task ステータスおよび View Details にて結果を確認
インストール完了後は、設定変更が無くても再 deploy が必要







Hotfix とは?

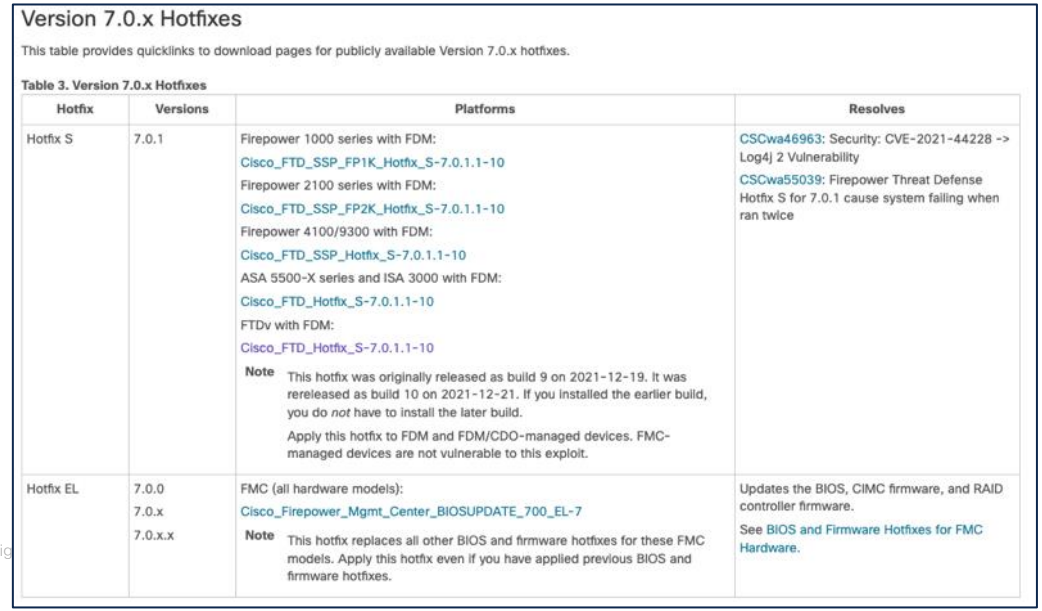
- Upgrade や Patch のリリースを待たずに緊急的に不具合等に対応する修正ファイルを Hotfix という

  https://www.cisco.com/c/en/us/td/docs/security/firepower/hotfix/Firepower_Hotfix_Release_Notes.html

- Hotfix にて緊急度の高い修正 (例: 危険度の高い脆弱性対策等) がスポット的に行われる
- Hotfix のイメージファイルの入手方法やインストール方法は、Upgrade / Patch インストール方法と同じ
- Hotfix が適用できるソフトウェアバージョンの判断は Hotfix のリリースノートを参照
- Hotfix インストール結果は FMC の GUI では確認できない。コンソールか ssh で実機に入り、expert mode で cat /etc/sf/patch_history の結果を見て判断する

Hotfix とは？

例えば、バージョン 7.0.x 用の Hotfix は以下の 2つがリリースされており、どの Hotfix のイメージが、どのモデル、バージョンに対応してどのような不具合に対応しているかが記載されている。
これらの Hotfix リリース以降に公開された Upgrade / Patch インストールファイルは、それまでの Hotfix での不具合対策を含んでいるため、個別に遡って Hotfix をインストールする必要は無い。
例: Patch 7.0.1.1-11 を FMC / FTD にインストールしていれば、以下の 2つの Hotfix はインストール不要



Version 7.0.x Hotfixes

This table provides quicklinks to download pages for publicly available Version 7.0.x hotfixes.

Table 3. Version 7.0.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix S	7.0.1	Firepower 1000 series with FDM: Cisco_FTD_SSP_FP1K_Hotfix_S-7.0.1.1-10 Firepower 2100 series with FDM: Cisco_FTD_SSP_FP2K_Hotfix_S-7.0.1.1-10 Firepower 4100/9300 with FDM: Cisco_FTD_SSP_Hotfix_S-7.0.1.1-10 ASA 5500-X series and ISA 3000 with FDM: Cisco_FTD_Hotfix_S-7.0.1.1-10 FTDv with FDM: Cisco_FTD_Hotfix_S-7.0.1.1-10 **Note** This hotfix was originally released as build 9 on 2021-12-19. It was rereleased as build 10 on 2021-12-21. If you installed the earlier build, you do *not* have to install the later build. Apply this hotfix to FDM and FDM/CDO-managed devices. FMC-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability CSCwa55039: Firepower Threat Defense Hotfix S for 7.0.1 cause system failing when ran twice
Hotfix EL	7.0.0 7.0.x 7.0.x.x	FMC (all hardware models): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EL-7 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these FMC models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and Firmware Hotfixes for FMC Hardware.

The bridge to possible