



ASDM と Chassis Manager を使用した ASA プラットフォームモードでの展開

この章の対象読者

Firepower 2100 は、FXOS と呼ばれる基盤となるオペレーティングシステムを実行します。ASA 向け Firepower 2100 は、次のモードで実行できます。

- プラットフォームモード：プラットフォームモードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Chassis Manager Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティングシステムにセキュリティ ポリシーを設定できます。完全な FXOS の設定ガイドについては、『[FXOS ASA コンフィギュレーションガイド](#)』を参照してください。FXOS のトラブルシューティングコマンドについては、『[FXOS ASA configuration guide](#)』を参照してください。



(注) インターフェイスの **show** コマンドの多くでは ASA コマンドを使用できないか、またはコマンドに完全な統計情報がありません。FXOS コマンドを使用して、より詳細なインターフェイス情報を表示する必要があります。詳細については、『[FXOS troubleshooting guide](#)』を参照してください。

- アプライアンスモード（デフォルト）：アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。

この章では、ASA プラットフォームモードでネットワークに Firepower 2100 を展開する方法について説明します。デフォルトでは、Firepower 2100 はアプライアンスモードで実行されるため、この章ではモードをプラットフォームモードに設定する方法について説明します。この章では以下の展開については取り上げていませんので、『[ASA コンフィギュレーションガイド](#)』を参照してください。

- フェールオーバー

- CLI 設定

この章では、基本的なセキュリティポリシーの設定手順についても説明します。より高度な要件がある場合は設定ガイドを参照してください。

Firepower 2100 ハードウェアでは、ASA ソフトウェアまたは Threat Defense ソフトウェアを実行できます。ASA と Threat Defense との間で切り替えを行う際には、デバイスの再イメージ化が必要になります。「[Cisco ASA および Firepower Threat Defense 再イメージ化ガイド](#)」を参照してください。

プライバシー収集ステートメント：Firepower 2100 には個人識別情報は不要で、積極的に収集することはありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

- [ASA について \(2 ページ\)](#)
- [エンドツーエンドの手順 \(4 ページ\)](#)
- [ネットワーク配置とデフォルト設定の確認 \(7 ページ\)](#)
- [デバイスの配線 \(10 ページ\)](#)
- [ファイアウォールの電源投入 \(11 ページ\)](#)
- [プラットフォームモードを有効にする \(12 ページ\)](#)
- [\(任意\) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更 \(15 ページ\)](#)
- [\(任意\) Chassis Manager へのログイン \(21 ページ\)](#)
- [\(任意\) Chassis Manager で追加のインターフェイスを有効にする \(21 ページ\)](#)
- [ASDM へのログイン \(24 ページ\)](#)
- [ライセンスの設定 \(25 ページ\)](#)
- [ASA の設定 \(31 ページ\)](#)
- [\(任意\) データインターフェイスでの FXOS の管理アクセスの設定 \(33 ページ\)](#)
- [ASA および FXOS CLI へのアクセス \(34 ページ\)](#)
- [次のステップ \(37 ページ\)](#)
- [プラットフォームモードの Firepower 2100 の履歴 \(37 ページ\)](#)

ASA について

ASA は、高度なステートフルファイアウォールと VPN コンセントレータの機能を 1 つの装置に組み合わせたものです。

Firepower 2100 は ASA 用の単一アプリケーションアプライアンスです。ASA は、プラットフォームモードまたはアプライアンスモード（デフォルト）のいずれかで実行できます。Firepower 2100 は、FXOS と呼ばれる基盤となるオペレーティングシステムを実行します。プラットフォームモードの場合は、FXOS で、基本的な動作パラメータとハードウェアインターフェイスを設定する必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Chassis Manager Web インターフェイスまたは FXOS CLI を使用できます。その後、次のマネージャのいずれかを使用して、ASA オペレーティングシステムにセキュリティポリシーを設定できます。

- ASDM : デバイスに含まれるシンプルな単独のデバイス マネージャ。このガイドでは、ASDM を使用して ASA を管理する方法について説明します。
- CLI
- Cisco Security Manager : 別のサーバー上のマルチデバイス マネージャ。

アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。

ASA と FXOS の管理

ASA および FXOS のオペレーティングシステムは、管理 1/1 インターフェイスを共有します。このインターフェイスには、ASA および FXOS に接続するための個別の IP アドレスがありません。



- (注) このインターフェイスは ASA では管理 1/1 と呼ばれます。FXOS では、MGMT、management0、または同様の他の名前が表示されます。このガイドでは、一貫性と簡潔さのため、管理 1/1 としてこのインターフェイスを参照します。

FXOS および ASA で監視する必要がある機能は異なるため、継続的な保守で両方のオペレーティングシステムを使用する必要があります。FXOS の初期設定では、SSH またはブラウザ (<https://192.168.45.45>) を使用してデフォルトの 192.168.45.45 IP アドレスに接続できます。

ASA の初期設定では、ASDM を使用して <https://192.168.45.1/admin> に接続できます。ASDM では、後で任意のインターフェイスからの SSH アクセスを設定できます。

両方のオペレーティングシステムをコンソールポートから使用できます。初期接続では FXOS CLI にアクセスします。ASA CLI には **connect asa** コマンドを使用してアクセスできます。

ASA データインターフェイスから FXOS を管理できるようにすること、および SSH、HTTPS、および SNMP の各アクセスを設定することも可能です。この機能はリモート管理に役立ちます。

サポートされない機能

サポートしない ASA 機能

次の ASA 機能は、Firepower 2100 ではサポートされていません。

- 統合ルーティングおよびブリッジング
- 冗長インターフェイス
- クラスタ
- KCD を使用したクライアントレス SSL VPN

- ASA REST API
- ASA FirePOWER モジュール
- Botnet Traffic Filter
- 次のインスペクション：
 - SCTP インスペクションマップ（ACL を使用した SCTP ステートフルインスペクションはサポートされません）
 - Diameter
 - GTP/GPRS

サポートされない FXOS 機能

次の FXOS 機能は、Firepower 2100 ではサポートされていません。

- FXOS 設定のバックアップと復元

代わりに、**show configuration** コマンドを使用して、設定のすべてまたは一部を表示できます。



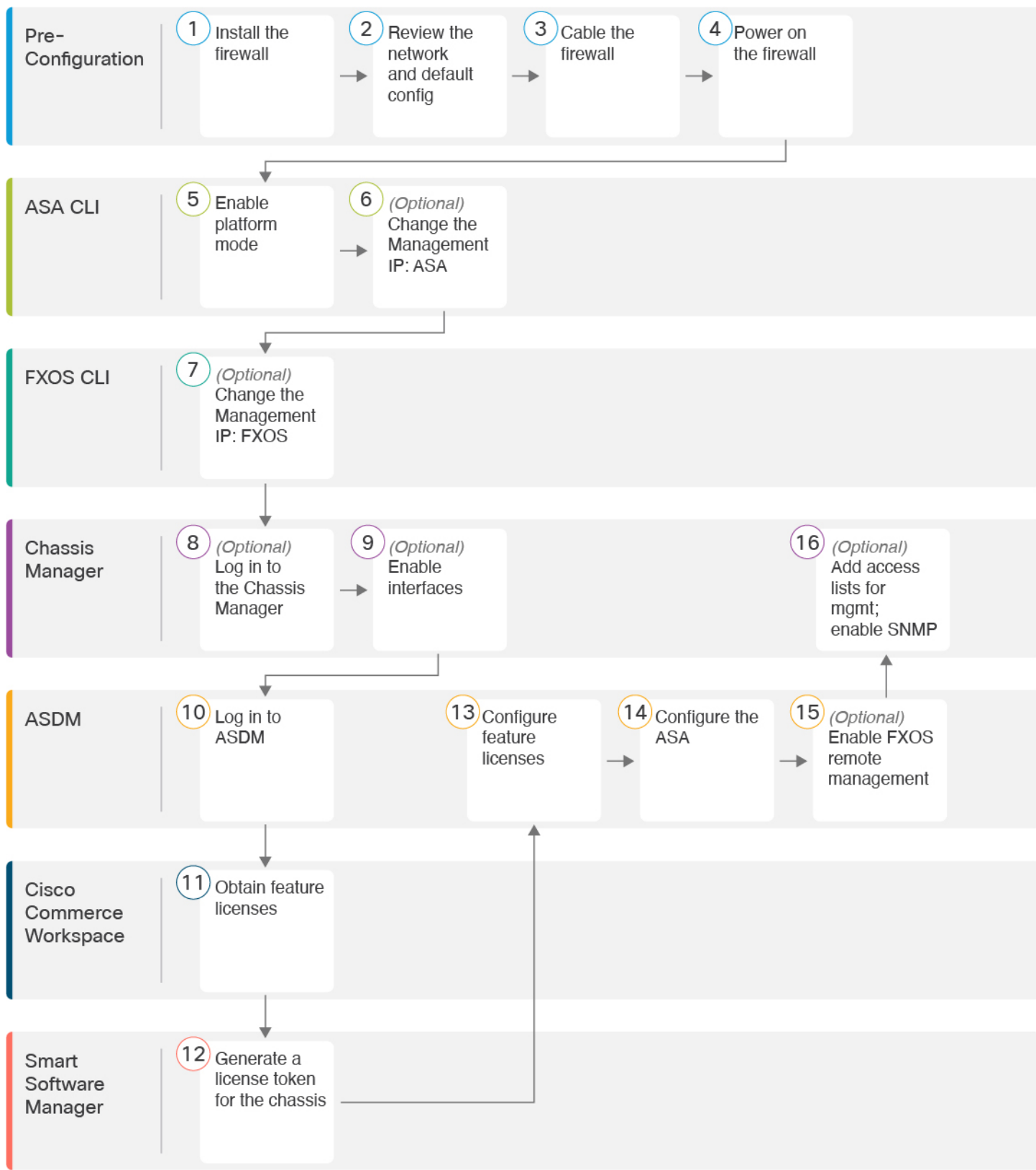
(注) **show** コマンドではシークレット（パスワードフィールド）が表示されないため、新しいデバイスに設定を貼り付ける場合は、実際のパスワードを含めるように **show** 出力を変更する必要があります。

- FXOS の外部 AAA 認証

FXOS (**connect asa**) から ASA コンソールに接続する場合、コンソールアクセス用の ASA AAA 設定が適用されることに注意してください (**aaa authentication serial console**)。

エンドツーエンドの手順

ASA を展開して設定するには、次のタスクを参照してください。



①	事前設定	ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。
②	事前設定	ネットワーク配置とデフォルト設定の確認 (7 ページ)。
③	事前設定	デバイスの配線 (10 ページ)。
④	事前設定	ファイアウォールの電源投入 (11 ページ)。
⑤	ASA CLI	プラットフォームモードを有効にする (12 ページ)。
⑥	ASA CLI	(任意) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更 (15 ページ) : 管理 IP の変更 : ASA。
⑦	FXOS CLI	(任意) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更 (15 ページ) : 管理 IP の変更 : FXOS。
⑧	Chassis Manager	(任意) Chassis Manager へのログイン (21 ページ)。
⑨	Chassis Manager	(任意) Chassis Manager で追加のインターフェイスを有効にする (21 ページ)。
⑩	ASDM	ASDM へのログイン (24 ページ)。
⑪	Cisco Commerce Workspace	ライセンスの設定 (25 ページ) : 機能ライセンスを取得します。
⑫	Smart Software Manager	ライセンスの設定 (25 ページ) : シャーシのライセンス トークンを生成します。
⑬	ASDM	ライセンスの設定 (25 ページ) : 機能ライセンスを設定します。
⑭	ASDM	ASA の設定 (31 ページ)。
⑮	ASDM	(任意) データインターフェイスでの FXOS の管理アクセスの設定 (33 ページ) : FXOS リモート管理を有効にし、FXOS が ASA インターフェイスから管理接続を開始できるようにします。
⑯	Chassis Manager	(任意) データインターフェイスでの FXOS の管理アクセスの設定 (33 ページ) : 管理アドレスを許可するようにアクセスリストを構成します。SNMP を有効にします (HTTPS および SSH はデフォルトで有効になっています)。

ネットワーク配置とデフォルト設定の確認

次の図に、Firepower2100でのデフォルトのネットワーク展開を示します（ASAプラットフォームモードでデフォルト設定を使用）。

外部インターフェイスをケーブルモデムまたはDSLモデムに直接接続する場合は、ASAが内部ネットワークのすべてのルーティングとNATを実行するように、モデムをブリッジモードにすることをお勧めします。外部インターフェイスがISPに接続するためにPPPoEを設定する必要がある場合は、その設定をASDMスタートアップウィザード内で行うことができます。

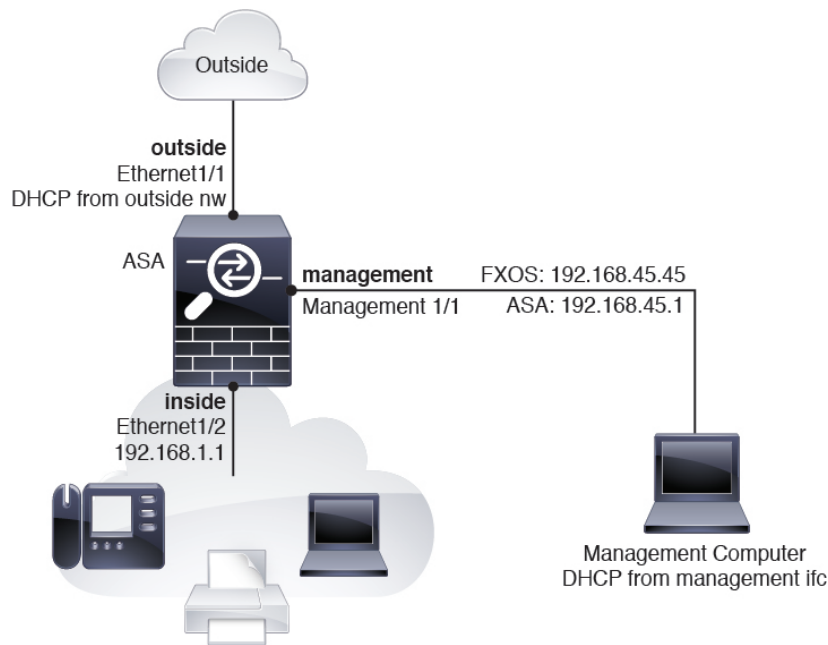


(注) デフォルトのFXOSおよびASA管理IPアドレスを使用できない場合は、[\(任意\) FXOSおよびASA管理IPアドレスまたはゲートウェイの変更 \(15 ページ\)](#) を参照してください。

内部IPアドレスを変更する必要がある場合は、ASDMスタートアップウィザードを使用して変更できます。たとえば、次のような状況において、内部IPアドレスの変更が必要になる場合があります。

- 外部インターフェイスが一般的なデフォルトネットワークである192.168.1.0ネットワーク上のIPアドレスの取得を試みる場合、DHCPリースが失敗し、外部インターフェイスがIPアドレスを取得しません。この問題は、ASAが同じネットワーク上に2つのインターフェイスを持つことができないために発生します。この場合、内部IPアドレスが新しいネットワーク上に存在するように変更する必要があります。
- ASAを既存の内部ネットワークに追加する場合は、内部IPアドレスが既存のネットワーク上に存在するように変更する必要があります。

図 1: ネットワーク内の Firepower 2100



Firepower 2100 プラットフォームモードのデフォルト設定

Firepower 2100 はプラットフォーム モードで実行するように設定できます。デフォルトはアプリケーション モードです。



(注) 9.13(1)以前のバージョンでは、プラットフォームモードがデフォルトであり、唯一のオプションでした。プラットフォームモードからアップグレードする場合、このモードが維持されます。

ASA の設定

Firepower 2100 上の ASA の工場出荷時のデフォルト設定は、次のとおりです。

- 内部から外部へのトラフィック フロー : Ethernet 1/1 (外部) 、 Ethernet 1/2 (内部)
- DHCP の外部 IP アドレス、内部 IP アドレス : 192.168.1.1
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP からのデフォルト ルート
- **管理** : 管理 1/1 (管理) 、 IP アドレス : 192.168.45.1
- **ASDM** アクセス : 管理ホストに許可されます。

- **NAT** : 内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **FXOS 管理** トラフィックの開始 : FXOS シャーシは、ASA 外部インターフェイス上で管理トラフィックを開始できます。
- **DNS** サーバー : OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address 192.168.45.1 255.255.255.0
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
```

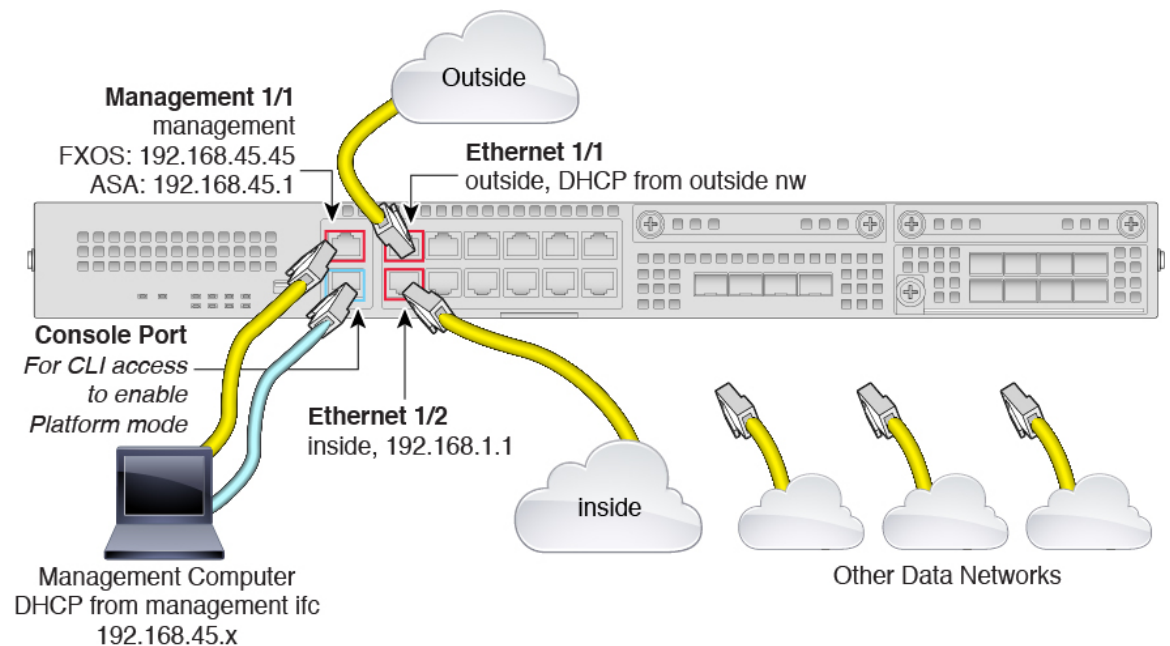
FXOS の設定

Firepower 2100 上の FXOS の工場出荷時のデフォルト設定は、次のとおりです。

- **管理 1/1** : IP アドレス 192.168.45.45
- **デフォルト ゲートウェイ** : ASA データ インターフェイス
- **Chassis Manager** および **SSH アクセス** : 管理ネットワークからのみ。
- **デフォルトのユーザー名** : **admin**、**デフォルトのパスワード** : **Admin123**
- **DHCP** サーバー : クライアント IP アドレス範囲 192.168.45.10 ~ 192.168.45.12

- **NTP** サーバー : Cisco NTP サーバー : 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org
- **DNS** サーバー : OpenDNS : 208.67.222.222、208.67.220.220
- **イーサネット 1/1** および **イーサネット 1/2** : 有効

デバイスの配線



Management 1/1 インターフェイスで Firepower 2100 を管理します。FXOS と ASA に同じ管理コンピュータを使用できます。デフォルト設定でも、Ethernet1/1 を外部として設定します。

手順

- ステップ 1** シャーシを取り付けます。[ハードウェア設置ガイド](#)を参照してください。
- ステップ 2** 管理コンピュータを Management 1/1 (ラベル「MGMT」) に直接接続するか、Management 1/1 を管理ネットワークに接続します。

管理ネットワーク上のクライアントだけが ASA または FXOS にアクセスできるため、管理コンピュータが管理ネットワーク上にあることを確認します。Management 1/1 には、デフォルトの FXOS IP アドレス (192.168.45.45) と ASA デフォルト IP アドレス (192.168.45.1) があります。FXOS ではクライアント (管理コンピュータを含む) に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の管理ネットワークの設定と競合しないようにしてください ([Firepower 2100 プラットフォームモードのデフォルト設定 \(8 ページ\)](#) を参照)。

FXOS および ASA 管理 IP アドレスをデフォルトから変更する必要がある場合は、[\(任意\) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更 \(15 ページ\)](#) を参照してください。

後で、データインターフェイスから FXOS および ASA 管理アクセスを設定できます。FXOS アクセスについては、[\(任意\) データインターフェイスでの FXOS の管理アクセスの設定 \(33 ページ\)](#) を参照してください。ASA アクセスについては、[ASA の一般的な操作の設定ガイド](#) を参照してください。

ステップ 3 管理コンピュータをコンソールポートに接続します。

アプライアンスモードからプラットフォームモードに変更するには、ASA CLI にアクセスする必要があります。Firepower 2100 には DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するためにはサードパーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティングシステムに必要な USB シリアル ドライバを必ずインストールしてください。

ステップ 4 外部ネットワークを Ethernet 1/1 インターフェイス (ラベル「WAN」) に接続します。

スマートソフトウェアライセンスの場合、ASA は License Authority にアクセスできるようにするためにインターネットアクセスを必要とします。

ステップ 5 内部ネットワークを Ethernet 1/2 に接続します。

ステップ 6 残りのインターフェイスに他のネットワークを接続します。

ファイアウォールの電源投入

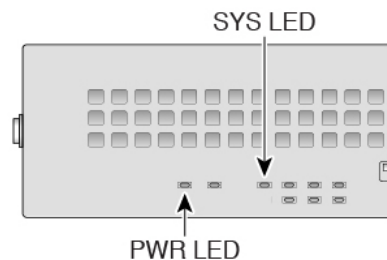
電源スイッチは、シャーシの背面の電源モジュール1の左にあります。これはシステムへの電源を制御するトグルスイッチです。電源スイッチがスタンバイの位置にある場合は、3.3 V のスタンバイ電源ユニットのみが電源モジュールから有効化され、12 V の主電源はオフになります。スイッチがオンの位置にある場合は、12 V の主電源がオンになり、システムが起動します。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

ステップ 2 デバイスの背面にある電源スイッチを押します。

ステップ 3 デバイスの前面にある PWR LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。



ステップ 4 デバイスの前面にある SYS LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

(注) 電源スイッチをオフの位置に動かす前に、システムがグレースフルシャットダウンを実行できるように `shutdown` コマンドを使用します。終了するまでに数分かかる場合があります。グレースフルシャットダウンが完了すると、コンソールにはすぐに電源オフすると安全ですと表示されます。前面パネルの青いロケータ ビーコン LED が点灯し、システムの電源をオフにする準備ができていていることを示します。これで、スイッチをオフの位置に移動できるようになりました。前面パネルの PWR LED が瞬間的に点滅し、消灯します。PWR LED が完全にオフになるまで電源を抜かないでください。

これらの `shutdown` コマンドの使用の詳細については、『[FXOS コンフィグレーションガイド](#)』を参照してください。

プラットフォームモードを有効にする

デフォルトでは、Firepower 2100 はアプライアンスモードで実行されます。この手順では、モードをプラットフォームモードに変更する方法と、必要に応じてアプライアンスモードに戻す方法について説明します。



注意 モードを変更する場合、システムをリロードする必要があり、設定がクリアされます。デフォルト設定は、リロード時に適用されます。

手順

ステップ 1 管理コンピュータをコンソールポートに接続します。Firepower 2100 には DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するためにはサードパーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット

- パリティなし
- 1 ストップ ビット

ASACLIに接続します。デフォルトでは、コンソールアクセスに必要なユーザークレデンシャルはありません。

(注) プラットフォームモードに変更すると、コンソール接続はASA CLIではなくFXOS CLIにアクセスします。ただし、プラットフォームモードのコンソールからASA CLIにアクセスできます。コンソールポートに接続してFXOSおよびASA CLIにアクセスする(35 ページ)を参照してください。

ステップ 2 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例 :

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

設定以外のすべてのコマンドは、特権EXECモードで使用できます。特権EXECモードからコンフィギュレーションモードに入ることもできます。

特権モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例 :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

ステップ 4 モードをプラットフォームモードに設定します。

no fxos mode appliance

write memory

reload

モードを設定したら、設定を保存してデバイスをリロードする必要があります。リロードする前に、中断することなく、モードを元の値に戻すことができます。

注意 リロードすると、設定はクリアされます。デフォルト設定は、リロード時に適用されません。

例 :

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system
has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

ステップ 5 再起動後、現在のモードを表示して変更を確認します。

show fxos mode

例 :

```
ciscoasa(config)# show fxos mode
Mode is currently set to platform
```

ステップ 6 (任意) モードをアプライアンスモードの設定に戻します。

fxos mode appliance

write memory

reload

モードを設定したら、設定を保存してデバイスをリロードする必要があります。リロードする前に、中断することなく、モードを元の値に戻すことができます。

注意 リロードすると、設定はクリアされます。デフォルト設定は、リロード時に適用されません。

例 :

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system
has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

(任意) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更

FXOS CLI から Firepower 2100 シャーシの FXOS 管理 IP アドレスを変更できます。デフォルトのアドレスは 192.168.45.45 です。FXOS 管理トラフィックのデフォルトゲートウェイを変更することもできます。デフォルトゲートウェイは 0.0.0.0 に設定されており、FXOS トラフィックはバックプレーン経由で送信され、ASA データインターフェイスを介してルーティングされます。代わりに管理 1/1 ネットワークでルータにトラフィックをルーティングする場合、ゲートウェイ IP アドレスを変更します。管理接続のアクセスリストを新しいネットワークに一致するように変更する必要もあります。ゲートウェイをデフォルトの 0.0.0.0 (ASA データインターフェイス) から変更すると、データインターフェイスで FXOS にアクセスできなくなり、FXOS はデータインターフェイスでトラフィックを開始できなくなります ([\(任意\) データインターフェイスでの FXOS の管理アクセスの設定 \(33 ページ\)](#) を参照)。

通常、FXOS 管理 1/1 IP アドレスは ASA 管理 1/1 IP アドレスと同じネットワーク上にあります。そのため、この手順では ASA の ASA IP アドレスを変更する方法も示します。

始める前に

- FXOS 管理 IP アドレスを変更した後で、新しいアドレスを使用して Chassis Manager および SSH 接続を再確立する必要があります。
- DHCP サーバーはデフォルトでは管理 1/1 で有効になっているため、管理 IP アドレスを変更する前に DHCP を無効にする必要があります。

手順

ステップ 1 コンソールポートに接続します ([コンソールポートに接続して FXOS および ASA CLI にアクセスする \(35 ページ\)](#) を参照)。接続が失われないようにするために、コンソールに接続することをお勧めします。

ステップ 2 DHCP サーバーを無効にします。

```
scope system
```

```
scope services
```

```
disable dhcp-server
```

```
commit-buffer
```

管理 IP アドレスを変更した後で、新しいクライアント IP アドレスを使用して DHCP を再び有効にすることができます。Chassis Manager で DHCP サーバーを有効および無効にすることもできます ([プラットフォーム設定 (Platform Settings)] > [DHCP])。

例：

```
firepower-2110# scope system
```

(任意) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更

```
firepower-2110 /system # scope services
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

ステップ 3 IPv4 管理 IP アドレス、および必要に応じてゲートウェイを設定します。

- a) fabric-interconnect a のスコープを設定します。

scope fabric-interconnect a

例 :

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
```

- b) 現在の管理 IP アドレスを表示します。

show

例 :

```
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
  ID      OOB IP Addr      OOB Gateway      OOB Netmask      OOB IPv6 Address OOB IPv6
Gateway Prefix Operability
-----
-----
  A      192.168.45.45    0.0.0.0          0.0.0.0          ::              ::
      64      Operable
```

- c) 新しい管理 IP アドレス、および必要に応じて新しいデフォルト ゲートウェイを設定します。

set out-of-band static ip ip_address netmask network_mask gw gateway_ip_address

現在設定されているゲートウェイを維持するには、**gw** キーワードを省略します。同様に、既存の管理 IP アドレスを維持したままゲートウェイを変更するには、**ip** キーワードと **netmask** キーワードを省略します。

ゲートウェイを ASA データインターフェイスに設定するには、**gw** を 0.0.0.0 に設定します。これがデフォルトの設定です。

例 :

```
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

ステップ 4 IPv6 管理 IP アドレスとゲートウェイを設定します。

- a) fabric-interconnect a のスコープ、次に IPv6 設定のスコープを設定します。

scope fabric-interconnect a

scope ipv6-config

例 :

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config #
```

- b) 現在の管理 IPv6 アドレスを表示します。

show ipv6-if

例 :

```
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
  IPv6 Address          Prefix      IPv6 Gateway
  -----
  ::                   ::         ::
```

- c) 新しい管理 IPv6 アドレスとゲートウェイを設定します。

Firepower-chassis /fabric-interconnect/ipv6-config # **set out-of-band static ipv6** *ipv6_address*
ipv6-prefix *prefix_length* **ipv6-gw** *gateway_address*

現在設定されているゲートウェイを維持するには、**ipv6-gw** キーワードを省略します。同様に、既存の管理 IP アドレスを維持したままゲートウェイを変更するには、**ipv6** キーワードと **ipv6-prefix** キーワードを省略します。

ゲートウェイを ASA データインターフェイスに設定するには、**gw** を :: に設定します。これがデフォルトの設定です。

例 :

```
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6
2001:DB8::34 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* #
```

ステップ 5 HTTPS、SSH、および SNMP のアクセス リストを削除して新しいアクセス リストを追加し、新しいネットワークからの管理接続を可能にします。

- a) システム/サービスの範囲を設定します。

scope system

scope services

例 :

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

- b) 現在のアクセス リストを表示します。

show ip-block

例 :

(任意) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
  IP Address      Prefix Length Protocol
  -----
  192.168.45.0    24 https
  192.168.45.0    24 ssh
firepower-2140 /system/services #
```

- c) 新しいアクセス リストを追加します。

IPv4 の場合 :

enter ip-block *ip_address prefix* [http | snmp | ssh]

IPv6 の場合 :

enter ipv6-block *ipv6_address prefix* [https | snmp | ssh]

IPv4 の場合、すべてのネットワークを許可するには **0.0.0.0** とプレフィックス **0** を入力します。IPv6 の場合、すべてのネットワークを許可するには **::** とプレフィックス **0** を入力します。Chassis Manager でアクセスリストを追加することもできます ([プラットフォーム設定 (Platform Settings)] > [アクセスリスト (Access List)])。

例 :

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

- a) 古いアクセス リストを削除します。

IPv4 の場合 :

delete ip-block *ip_address prefix* [http | snmp | ssh]

IPv6 の場合 :

delete ipv6-block *ipv6_address prefix* [https | snmp | ssh]

例 :

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

ステップ 6 (任意) IPv4 DHCP サーバーを再び有効にします。

scope system**scope services****enable dhcp-server start_ip_address end_ip_address**

Chassis Manager で DHCP サーバーを有効および無効にすることもできます ([プラットフォーム設定 (Platform Settings)]> [DHCP]) 。

例 :

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

ステップ 7 設定を保存します。

commit-buffer

例 :

```
firepower-2110 /system/services* # commit-buffer
```

ステップ 8 ASA アドレスを、正しいネットワーク上となるように変更します。デフォルトの ASA 管理 1/1 インターフェイス IP アドレスは 192.168.45.1 です。

- a) コンソールから、ASA CLI に接続して、グローバル コンフィギュレーション モードにアクセスします。

connect asa**enable****configure terminal**

ASA バージョン 9.12(1) 以降では、イネーブルパスワードを設定するよう求められます。以前のバージョンでは、デフォルトのイネーブルパスワードはブランクです。

例 :

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa# configure terminal
ciscoasa(config)#
```

- b) 管理 1/1 IP アドレスを変更します。

interface management1/1**ip address ip_address mask**

例 :

(任意) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更

```
ciscoasa(config)# interface management1/1
ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
```

- c) ASDM にアクセス可能なネットワークに変更します。

no http 192.168.45.0 255.255.255.0 management

http ip_address mask management

例 :

```
ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
```

- d) 設定を保存します。

write memory

- e) FXOS コンソールに戻るには、**Ctrl+a**、**d** と入力します。

例

次の例では、IPv4 管理インターフェイスとゲートウェイを設定します。

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
  ID   OOB IP Addr      OOB Gateway      OOB Netmask      OOB IPv6 Address OOB IPv6 Gateway
  Prefix Operability
  -----
  A    192.168.2.112    192.168.2.1      255.255.255.0    2001:DB8::2      2001:DB8::1
  64   Operable
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /fabric-interconnect #
```

次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
  IPv6 Address      Prefix      IPv6 Gateway
  -----
  2001:DB8::2       64         2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* # commit-buffer
```

```
firepower-2110 /fabric-interconnect/ipv6-config #
```

(任意) Chassis Manager へのログイン

Chassis Manager を使用して、インターフェイスの有効化や EtherChannel の作成など、シャーシの設定を行います。

始める前に

- サポートされるブラウザの詳細については、使用しているバージョンのリリースノートを参照してください
(<http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html> を参照)。
- FXOS および ASA 管理 IP アドレスを変更する必要がある場合は、(任意) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更 (15 ページ) を参照してください。

手順

-
- ステップ 1** Management 1/1 インターフェイスに接続している管理コンピュータで、次の URL にアクセスして Chassis Manager を起動します。
- https://192.168.45.45**
- ステップ 2** **admin** をデフォルトのユーザー名に入力します。パスワードの設定を求めるメッセージが表示されます。
-

(任意) Chassis Manager で追加のインターフェイスを有効にする

デフォルトでは、管理 1/1、イーサネット 1/1、およびイーサネット 1/2 の各インターフェイスは、シャーシでは物理的に有効、ASA 設定では論理的に有効になっています。追加のインターフェイスを使用するには、次の手順を使用してそのインターフェイスをシャーシで有効にし、その後 ASA 設定で有効にする必要があります。EtherChannel (ポートチャネルと呼ばれる) を追加することもできます。

(任意) Chassis Manager で追加のインターフェイスを有効にする



(注) フェールオーバーを有効にした後でFXOSのインターフェイスを変更する場合は(ネットワークモジュールを追加または削除する、あるいはEtherChannel設定を変更するなど)、スタンバイユニットのFXOSでインターフェイスを変更し、アクティブユニットで同じ変更を行います。

FXOSでインターフェイスを削除した場合(たとえば、ネットワークモジュールの削除、EtherChannelの削除、またはEtherChannelへのインターフェイスの再割り当てなど)、必要な調整を行うことができるように、ASA設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OSの古いインターフェイス設定は手動で削除できます。



(注) インターフェイスの **show** コマンドの多くではASAコマンドを使用できないか、またはコマンドに完全な統計情報がありません。FXOSコマンドを使用して、より詳細なインターフェイス情報を表示する必要があります。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**
- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

詳細については、『[FXOS troubleshooting guide](#)』を参照してください。



始める前に

- Chassis Manager にログインします。「[\(任意\) Chassis Manager へのログイン \(21 ページ\)](#)」を参照してください。
- Firepower 2100 は、Link Aggregation Control Protocol (LACP) のアクティブモードまたはオンモードで EtherChannel をサポートします。デフォルトでは、LACP モードはアクティブに設定されています。CLI でモードをオンに変更できます。最適な互換性を得るために、接続スイッチポートをアクティブモードに設定することを推奨します。
- 管理 IP アドレスをデフォルトから変更するには、[\(任意\) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更 \(15 ページ\)](#) を参照してください。

手順

ステップ 1 Chassis Manager で [インターフェイス (Interfaces)] をクリックします。

[すべてのインターフェイス (All Interfaces)] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

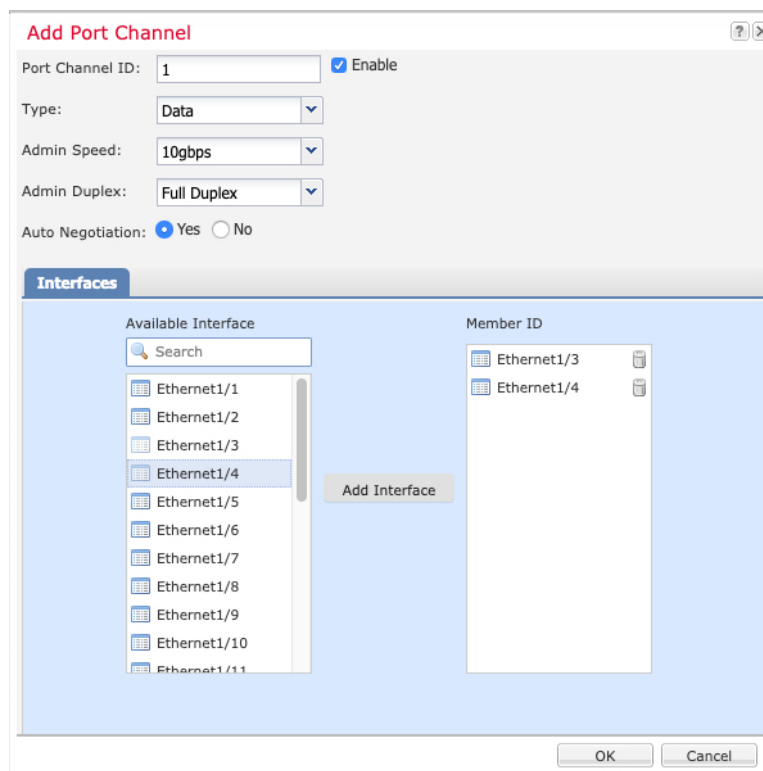
ステップ 2 インターフェイスを有効または無効にするには、[Enable] スライダ () または [無効 (Disable)] スライダ () をクリックします。

(注) Management 1/1 インターフェイスは、このテーブルで [MGMT] として表示されます。

ステップ 3 (任意) EtherChannel を追加します。

(注) EtherChannel メンバー ポートは ASA に表示されますが、EtherChannel およびポートメンバーシップは FXOS でのみ設定できます。

a) インターフェイス テーブルの上の [Add Port Channel] をクリックします。



b) [Port Channel ID] フィールドに、ポートチャネルの ID を入力します。有効な値は、1 ~ 47 です。

c) ポートチャネルを有効にするには、[Enable] チェックボックスをオンにします。

[Type] ドロップダウンリストは無視します。使用可能なタイプは [Data] のみです。

d) [Admin Speed] ドロップダウンリストで、すべてのメンバーインターフェイスの速度を選択します。

その速度 (および選択したその他の設定) に対応していないインターフェイスを選択すると、可能な範囲で最速の速度が自動的に適用されます。

- e) すべてのメンバー インターフェイスについて、[Auto Negotiation] で [Yes] または [No] のオプション ボタンをクリックします。
- f) [Admin Duplex] ドロップダウン リストで、すべてのメンバー インターフェイスのデュプレックスを選択します。
- g) [Available Interface] リストで、追加するインターフェイスを選択し、[Add Interface] をクリックします。

同じタイプと速度の最大 16 のインターフェイスを追加できます。チャンネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

ヒント 複数のインターフェイスを一度に追加できます。複数の個別インターフェイスを選択するには、Ctrl キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、Shift キーを押しながら最後のインターフェイスをクリックして選択します。

- h) [OK] をクリックします。

ASDM へのログイン

ASDM を起動して、ASA を設定できるようにします。

License Authority またはサテライト サーバーに接続する前に、高度暗号化 (3DES/AES) を管理接続に使用できるので、ASDM を起動できます。ASDM アクセスは、デフォルトの暗号化を適用する管理専用インターフェイスでのみ使用できることに注意してください。高度暗号化ライセンスに接続して取得するまで、through the box トラフィックは許可されません。

始める前に

ASDM を実行するための要件については、Cisco.com の『[ASDM リリース ノート](#)』を参照してください。

手順

ステップ 1 サポートされているブラウザを使用して、次の URL を入力します。

https://management_ip/admin

- *management_ip* : ASA 管理インターフェイスの IP アドレス (192.168.45.1) またはホスト名を指定します。

[Cisco ASDM] Web ページが表示されます。ASA に証明書がインストールされていないために、ブラウザのセキュリティ警告が表示されることがありますが、これらの警告は無視して、Web ページにアクセスすることができます。

- ステップ 2** 使用可能なオプション [Install ASDM Launcher] または [Run ASDM] のいずれかをクリックします。
- ステップ 3** 画面の指示に従ってオプションを選択し、ASDM を起動します。
[Cisco ASDM-IDMランチャー (Cisco ASDM-IDM Launcher)] が表示されます。
- ステップ 4** ユーザー名を空のままにして、ASA を展開したときに設定したイネーブル パスワードを入力し、[OK] をクリックします。
メイン ASDM ウィンドウが表示されます。

ライセンスの設定

ASA はスマート ライセンスを使用します。通常のスマートライセンシング (インターネット アクセスが必要) を使用できます。または、オフライン管理の場合、永続ライセンス予約または Smart Software Manager On-Prem (以前のサテライトサーバ) を設定できます。これらのオフラインライセンス方式の詳細については、「[Cisco ASA シリーズの機能ライセンス](#)」を参照してください。このガイドは通常のスマートライセンシングに適用されます。

シスコライセンスの概要については詳しくは、[cisco.com/go/licensingguide](https://www.cisco.com/go/licensingguide) を参照してください。

シャーンを登録すると、Smart Software Manager はファイアウォールと Smart Software Manager 間の通信用の ID 証明書を発行します。また、該当するバーチャルアカウントにファイアウォールが割り当てられます。Smart Software Manager に登録するまでは、設定変更を行うことはできず、特殊なライセンスを必要とする機能へ、操作はその他の点では影響を受けません。ライセンス付与される機能は次のとおりです。

- Essentials
- セキュリティ コンテキスト
- 高度な暗号化 (3DES/AES) : スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。
- Cisco Secure Client : Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ

License Authority またはサテライト サーバーに接続する前に、高度暗号化 (3DES/AES) を管理接続に使用できるので、ASDM を起動できます。ASDM アクセスは、デフォルトの暗号化を適用する管理専用インターフェイスでのみ使用できることに注意してください。高度暗号化ライセンスに接続して取得するまで、through the box トラフィックは許可されません。

Smart Software Manager から ASA の登録トークンを要求する場合、[このトークンを使用して登録した製品でエクスポート制御機能を許可 (Allow export-controlled functionality on the products registered with this token)] チェックボックスをオンにして、強力な暗号化の完全ライセンスが適用されるようにします (ご使用のアカウントでその使用が許可されている必要があります)。

強力な暗号化ライセンスは、シャーンで登録トークンを適用すると、対象となるお客様の場合自動的に有効化されるため追加の操作は不要です。スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。



(注) Firepower 4100/9300 シャーンの場合とは異なり、すべてのライセンス設定を FXOS 設定ではなく ASA で実行します。

始める前に

- [Smart Software Manager](#) にマスターアカウントを持ちます。
まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスターアカウントを作成できます。
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用の Smart Software Manager アカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

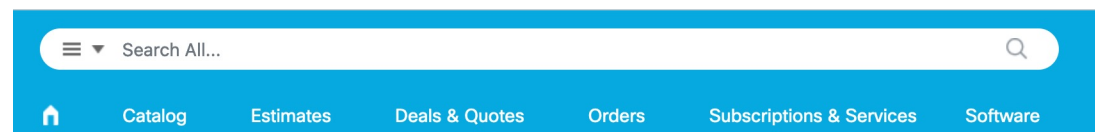
手順

ステップ 1

ご使用のスマート ライセンス アカウントに、必要なライセンスが含まれている (少なくとも Essentials ライセンスが含まれている) ことを確認してください。

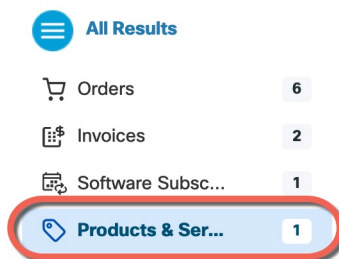
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェア ライセンシングアカウントにリンクされています。ただし、自身でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [すべて検索 (Search All)] フィールドを使用します。

図 2: ライセンス検索



結果から、[製品とサービス (Products and Services)] を選択します。

図 3: 結果



次のライセンス PID を検索します。

(注) PID が見つからない場合は、注文に手動で PID を追加できます。

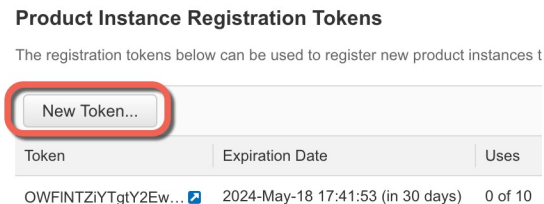
- Essentials ライセンス : L-FPR2100-ASA=。Essentials ライセンスは無料ですが、スマートソフトウェア ライセンシング アカウントに追加する必要があります。
- 5 コンテキストライセンス : L-FPR2K-ASASC-5=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 10 コンテキストライセンス : L-FPR2K-ASASC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 強力な暗号化(3DES/AES)のライセンス : L-FPR2K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。
- Cisco Secure Client : 『Cisco Secure Client 発注ガイド』を参照してください。ASA では、このライセンスを直接有効にしないでください。

ステップ 2 [Smart Software Manager](#) で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。



b) [General] タブで、[New Token] をクリックします。



- c) [登録トークンを作成 (Create Registration Token)] ダイアログボックスで、以下の設定値を入力してから [トークンを作成 (Create Token)] をクリックします。

Create Registration Token ? x

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description:

* Expire After: Days
Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

Allow export-controlled functionality on the products registered with this token i

- [説明 (Description)]
- [有効期限 (Expire After)] : 推奨値は 30 日です。
- 最大使用回数 (Max. Number of Uses)
- [このトークンに登録された製品で輸出管理機能を許可する (Allow export-controlled functionality on the products registered with this token)] : 輸出コンプライアンス フラグを有効にします。

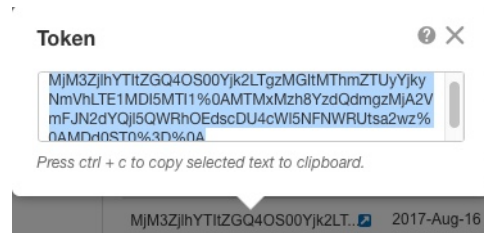
トークンはインベントリに追加されます。

- d) トークンの右側にある矢印アイコンをクリックして [トークン (Token)] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 4: トークンの表示

General			
Virtual Account			
Description:	Virtual Account		
Default Virtual Account:	No		
Product Instance Registration Tokens			
The registration tokens below can be used to register new product instances to this virtual account.			
New Token...			
Token	Expiration Date	Uses	Export-Controlled
OWFINTZiYtGtY2Ew.	2024-May-18 17:41:53 (in 30 days)	0 of 10	Allowed

図 5: トークンのコピー



ステップ 3 ASDM で、**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 4 **[Register]** をクリックします。

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for smart licensing, see the [Smart Call-Home](#) page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

Enable Smart license configuration

Feature Tier: -- None --

Throughput Level: -- None --

Privacy Host Name Version

Transport Call Home Smart Transport

Configure Transport URL

Default URL

Registration

Utility

Proxy URL

Proxy Port

Configure Utility Mode

Enable Standard Utility Mode

Custom ID

Customer Company Identifier

Customer Company Name

Customer Street

Customer City

Customer State

Customer Country

Customer Postal Code

Registration Status: UNREGISTERED

Effective Running Licenses

License Feature	License Value
Maximum VLANs	200
Inside Hosts	Unlimited
Failover	Active/Active
Encryption-DES	Enabled
Encryption-3DES-AES	Enabled
Security Contexts	2
Carrier	Disabled

ステップ 5 [ID Token] フィールドに登録トークンを入力します。

Smart License Registration

ID Token: :MzV8eHpYY05EMGg2aDRYak0ybmZNVnRaSW5sbm5XVXVIZkk2RTdGTwj6%0AZVBWWT0%3D%0A

Force registration

Help Cancel Register

必要に応じて、[登録を強制 (Force registration)] チェックボックスをオンにして、Smart Software Manager と同期されていない可能性がある登録済みの ASA を登録します。たとえば、ASA が誤って Smart Software Manager から削除された場合に [登録を強制 (Force registration)] を使用します。

ステップ 6 [Register] をクリックします。

ASA は、事前設定された外部インターフェイスを使用して Smart Software Manager に登録し、設定済みソフトウェア利用資格の認証を要求します。Smart Software Manager は、ご使用のアカウントが許可すれば高度暗号化 (3DES/AES) ライセンスも適用します。ライセンスステータスが更新されると、ASDMによってページが更新されます。また、登録が失敗した場合などには、[モニターリング (Monitoring)] > [プロパティ (Properties)] > [スマートライセンス (Smart License)] の順に選択して、ライセンスステータスを確認できます。

Registration Status: REGISTERED

Unregister Renew ID Certificate Renew Authorization

ステップ 7 次のパラメータを設定します。

To configure an HTTP proxy for smart licensing, see the [Smart Call-Home](#) page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

Enable Smart license configuration

Feature Tier: standard

Context: 3 (1-38)

Enable strong-encryption protocol

Registration Status: REGISTERED

Unregister Renew ID Certificate Renew Authorization

- [Enable Smart license configuration] をオンにします。
- [機能層 (Feature Tier)] ドロップダウンリストから **[Essentials]** を選択します。
使用できるのは Essentials 層だけです。

- (任意) [Context] ライセンスの場合、コンテキストの数を入力します。

2 コンテキストはライセンスなしで使用できます。コンテキストの最大数は、モデルによって異なります。

- Firepower 2110 : 25 コンテキスト
- Firepower 2120 : 25 コンテキスト

- Firepower 2130 : 30 コンテキスト
- Firepower 2140 : 40 コンテキスト

たとえば、Firepower 2110 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

ステップ 8 [Apply] をクリックします。

ステップ 9 ツールバーの [Save] アイコンをクリックします。

ステップ 10 ASDM を終了し、再起動します。

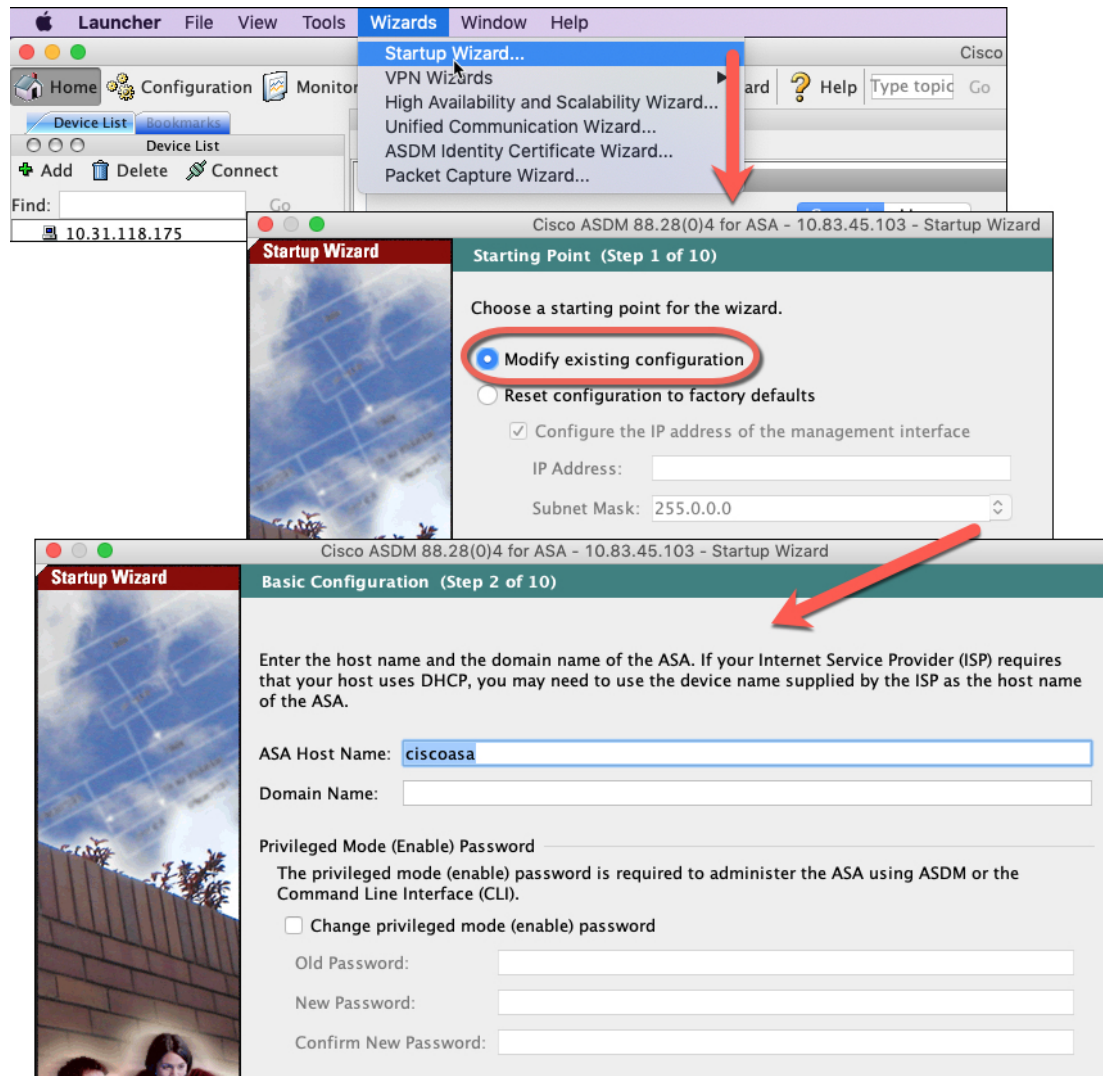
ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

ASA の設定

ASDM を使用する際、基本機能および拡張機能の設定にウィザードを使用できます。ウィザードに含まれていない機能を手動で設定することもできます。

手順

ステップ 1 [Wizards] > [Startup Wizard] の順に選択し、[Modify existing configuration] オプション ボタンをクリックします。



ステップ2 [Startup Wizard] では、手順を追って以下を設定できます。

- イネーブルパスワード
- インターフェイス（内部および外部のインターフェイスIPアドレスの設定やインターフェイスの有効化など）
- スタティックルート
- DHCP サーバー
- その他...

ステップ3（任意） [Wizards] メニューから、その他のウィザードを実行します。

ステップ 4 ASA の設定を続行するには、『[Navigating the Cisco ASA Series Documentation](#)』でソフトウェアバージョンに応じたマニュアルを参照してください。

(任意) データインターフェイスでの FXOS の管理アクセスの設定

データインターフェイスから Firepower 2100 の FXOS を管理する場合、SSH、HTTPS、および SNMP アクセスを設定できます。この機能は、デバイスをリモートで管理しつつ、管理 1/1 を隔離されたネットワークに維持する場合に役立ちます。これは、隔離されたネットワーク上の FXOS にアクセスするためのネイティブな方法です。この機能を有効にすると、ローカルアクセスに対してのみ管理 1/1 を使用し続けることができます。ただし、この機能を使用しながら FXOS の管理 1/1 からのリモートアクセスは許可することはできません。この機能には、バックプレーン（デフォルト）を経由した ASA データインターフェイスへのトラフィックの転送が必要で、FXOS 管理ゲートウェイを 1 つだけ指定できます。

ASA は、FXOS アクセスに非標準ポートを使用します。標準ポートは同じインタフェースで ASA が使用するため予約されています。ASA が FXOS にトラフィックを転送するときに、非標準の宛先ポートはプロトコルごとに FXOS ポートに変換されます（FXOS の HTTPS ポートは変更しません）。パケット宛先 IP アドレス（ASA インターフェイス IP アドレス）も、FXOS で使用する内部アドレスに変換されます。送信元アドレスは変更されません。トラフィックを返す場合、ASA は自身のデータルーティングテーブルを使用して正しい出力インターフェイスを決定します。管理アプリケーションの ASA データ IP アドレスにアクセスする場合、FXOS ユーザー名を使用してログインする必要があります。ASA ユーザー名は ASA 管理アクセスのみに適用されます。

ASA データインターフェイスで FXOS 管理トラフィック開始を有効にすることもできます。これは、たとえば、SNMP トラップ、NTP と DNS のサーバーアクセスなどに必要です。デフォルトでは、FXOS 管理トラフィック開始は、DNS および NTP のサーバー通信（スマートソフトウェアライセンス通信が必要）用の ASA 外部インターフェイスで有効になっています。

始める前に

- シングル コンテキスト モードのみ。
- ASA 管理専用インターフェイスは除外します。
- ASA データインターフェイスに VPN トンネルを使用して、FXOS に直接アクセスすることはできません。SSH の回避策として、ASA に VPN 接続し、ASA CLI にアクセスし、**connect fxos** コマンドを使用して FXOS CLI にアクセスします。SSH、HTTPS、および SNMPv3 は暗号化できるため、データインターフェイスへの直接接続は安全です。
- FXOS ゲートウェイが ASA データインターフェイス（デフォルト）にトラフィックを転送するように設定されていることを確認します。ゲートウェイを変更した場合は、(任

意) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更 (15 ページ) を参照してください。

手順

ステップ 1 ASDM で、[設定 (Configuration)] > [デバイス管理 (Device Management)] > [管理アクセス (Management Access)] > [FXOS リモート管理 (FXOS Remote Management)] を選択します。

ステップ 2 FXOS リモート管理を有効にします。

- a) ナビゲーション ウィンドウで、[HTTPS]、[SNMP]、または [SSH] を選択します。
- b) [Add] をクリックし、管理を許可する [Interface] を設定し、接続を許可する [IP Address] を設定し、[OK] をクリックします。

プロトコルタイプごとに複数のエントリを作成できます。以下のデフォルト値を使用しない場合は、[Port] を設定します。

- HTTPS デフォルト ポート : 3443
- SNMP デフォルト ポート : 3061
- SSH デフォルト ポート : 3022

ステップ 3 FXOS が ASA インターフェイスから管理接続を開始できるようにします。

- a) ナビゲーション ウィンドウで [FXOS Traffic Initiation] を選択します。
- b) [Add] をクリックし、FXOS 管理トラフィックを送信する必要がある ASA インターフェイスを有効にします。デフォルトでは、外部インターフェイスは有効になっています。

ステップ 4 [Apply] をクリックします。

ステップ 5 Chassis Manager に接続します (デフォルトでは、<https://192.168.45.45>、ユーザー名 : **admin**、パスワードは初回ログイン時に設定したものを使用)。

ステップ 6 [Platform Settings] タブをクリックし、[SSH]、[HTTPS]、または [SNMP] を有効にします。

SSH と HTTPS はデフォルトで有効になっています。

ステップ 7 [Platform Settings] タブで、管理アクセスを許可するように [Access List] を設定します。デフォルトでは、SSH および HTTPS は管理 1/1 192.168.45.0 ネットワークのみを許可します。ASA の [FXOS Remote Management] 設定で指定したアドレスを許可する必要があります。

ASA および FXOS CLI へのアクセス

ここでは、FXOS および ASA コンソールに接続する方法と、SSH を使用して FXOS に接続する方法について説明します。

コンソールポートに接続して FXOS および ASA CLI にアクセスする

Firepower 2100 コンソールポートで FXOS CLI に接続します。次に、FXOS CLI から ASA コンソールに接続し、再度戻ることができます。

一度に保持できるコンソール接続は 1 つだけです。FXOS コンソールから ASA のコンソールに接続する場合、Telnet または SSH 接続の場合とは異なり、この接続は永続的接続です。

手順

ステップ 1 管理コンピュータをコンソールポートに接続します。Firepower 2100 には DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するためにはサードパーティ製のシリアル to USB ケーブルが必要です。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

FXOS CLI に接続します。ユーザー クレデンシャルを入力します。デフォルトでは、**admin** ユーザーとデフォルトのパスワード **Admin123** を使用してログインできます。初めてログインすると、**admin** パスワードを変更するように求められます。

ステップ 2 ASA に接続します。

connect asa

例：

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

ステップ 3 FXOS コンソールに戻るには、**Ctrl+a**、**d** と入力します。

SSHで FXOS に接続

デフォルトの IP アドレス 192.168.45.45 を使用して管理 1/1 の FXOS に接続できます。リモート管理を設定する場合（[（任意）データインターフェイスでの FXOS の管理アクセスの設定（33 ページ）](#)）、非標準ポート（デフォルトでは 3022）でデータインターフェイス IP アドレスに接続することもできます。

SSH を使用して ASA に接続するには、まず、[ASA の一般的な操作の設定ガイド](#)に従って SSH アクセスを設定する必要があります。

ASA CLI から FXOS、およびその逆方向に接続することができます。

FXOS は最大 8 個の SSH 接続を許可します。

始める前に

管理 IP アドレスを変更するには、[\(任意\) FXOS および ASA 管理 IP アドレスまたはゲートウェイの変更 \(15 ページ\)](#) を参照してください。

手順

ステップ 1 管理 1/1 に接続している管理コンピュータで、管理 IP アドレスに SSH 接続します (デフォルトでは、<https://192.168.45.45>、ユーザー名：**admin**、パスワード：**Admin123**)。

FXOS でユーザーを追加した場合は、任意のユーザー名でログインできます。リモート管理を設定する場合、ASA データ インターフェイス IP にポート 3022 (デフォルトのポート) で SSH 接続します。

ステップ 2 ASA CLI に接続します。

connect asa

FXOS CLI に戻るには、**Ctrl+a, d** と入力します。

例：

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

ステップ 3 ASA に SSH 接続する場合 (ASA で SSH アクセスを設定した後)、FXOS CLI に接続します。

connect fxos

FXOS への認証を求められます。デフォルトのユーザー名：**admin** およびパスワード：**Admin123** を使用します。ASA CLI に戻るには、**exit** と入力するか、または **Ctrl-Shift-6, x** と入力します。

例：

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

firepower-2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
```

```

Cisco Firepower Extensible Operating System (FX-OS) Software

[...]

firepower-2110#
firepower-2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#

```

次のステップ

- ASA の設定を続行するには、「[Navigating the Cisco ASA Series Documentation](#)」でソフトウェアバージョンに応じたマニュアルを参照してください。
- FXOS シャーシの設定については、『[FXOS コンフィギュレーションガイド](#)』を参照してください。
- トラブルシューティングについては、『[FXOS トラブルシューティングガイド](#)』を参照してください。

プラットフォームモードの Firepower 2100 の履歴

機能名	バージョン	機能情報
デフォルトモードがアプライアンスモードに変更されました。	9.13(1)	アプライアンスモードの導入により、デフォルトモードがアプライアンスモードに変更されました。以前のリリースでは、プラットフォームモードのみが使用可能モードでした。9.13(1) にアップグレードしている場合、モードはプラットフォームモードのままになります。 新規/変更されたコマンド： fxos mode appliance 、 show fxos mode
管理者パスワードの設定を求めるプロンプトが表示されます。	9.13(1)	Chassis Manager に初めてログインすると、admin パスワードを変更するように求められます。以前のデフォルトパスワードは Admin123 でした。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。