ASA 展開

この章の対象読者

この章では、スマート ライセンシングの設定方法など、スタンドアロンの ASA 論理デバイスを展開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 configuration guide』を参照してください。

- クラスタリング
- 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。

（注） **プライバシー収集ステートメント**：Firepower 4100 には個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザ名などの設定では、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 （2 ページ）
- Firepower Chassis Manager：ライセンス サーバへのシャーシの登録 （3 ページ）
- Firepower Chassis Manager：ASA 論理デバイスの追加 （8 ページ）
- ASDM へのログイン （11 ページ）
- ASA でのライセンス権限付与の設定 （12 ページ）
- ASA の設定 （13 ページ）
- ASA CLI へのアクセス （15 ページ）
- 次のステップ （16 ページ）
- ASA の履歴 （17 ページ）

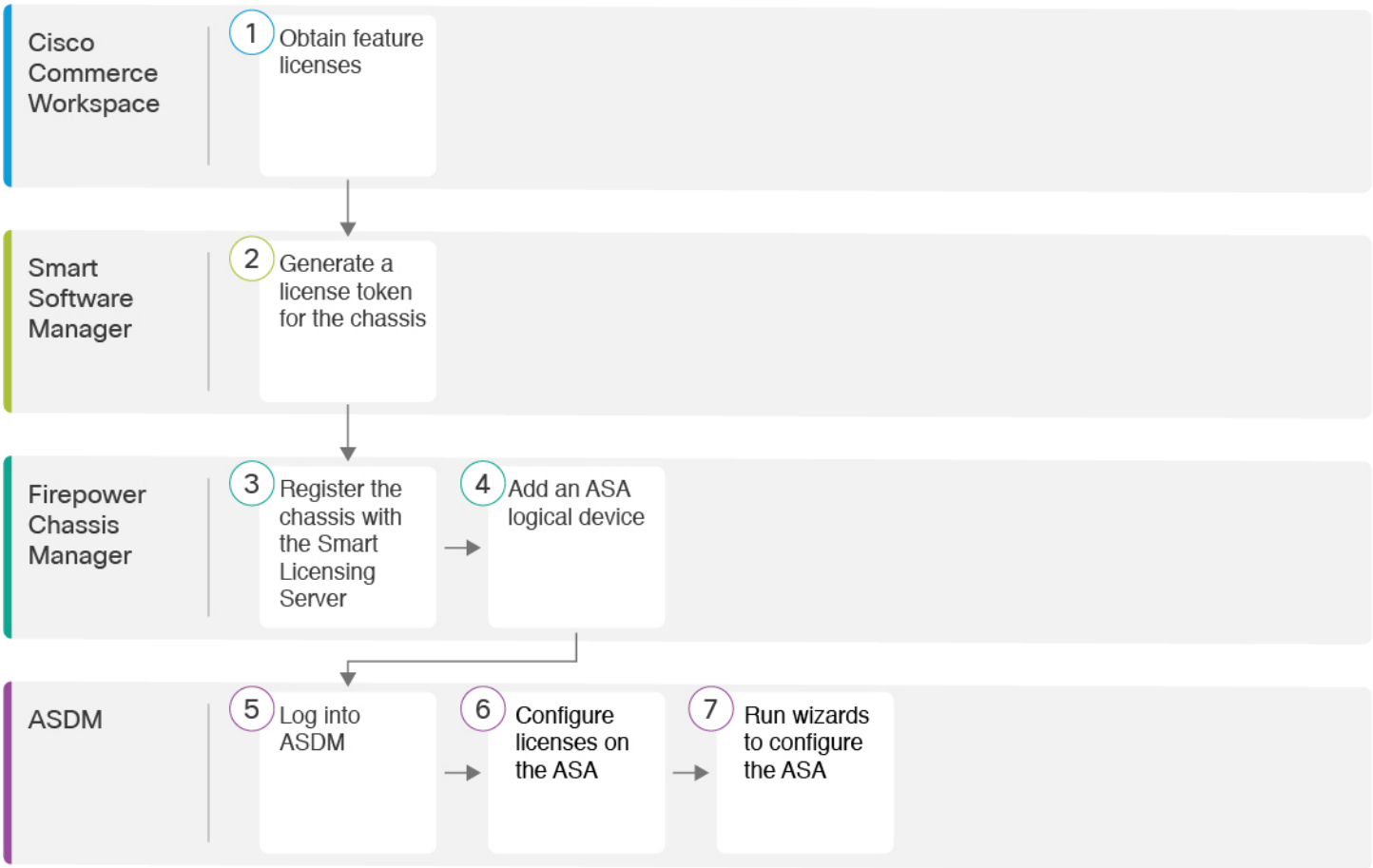
ASA について

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。次のいずれかのマネージャを使用して ASA を管理できます。

- 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：別のサーバ上のマルチデバイス マネージャ。

エンドツーエンドの手順

シャーシで 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	Cisco Commerce Workspace	Firepower Chassis Manager：ライセンス サーバへのシャーシの登録（3 ページ）：機能ライセンスを取得します。

2	Smart Software Manager	Firepower Chassis Manager：ライセンス サーバへのシャーシの登録（3 ページ）：シャーシのライセンス トークンを生成します。
3	Firepower Chassis Manager	Firepower Chassis Manager：ライセンス サーバへのシャーシの登録（3 ページ）：スマート ライセンシング サーバにシャーシを登録します。
4	Firepower Chassis Manager	Firepower Chassis Manager：ASA 論理デバイスの追加（8 ページ）。
5	ASDM	ASDM へのログイン（11 ページ）。
6	ASDM	ASA でのライセンス権限付与の設定（12 ページ）。
7	ASDM	ASA の設定（13 ページ）。

FirepowerChassisManager：ライセンスサーバへのシャーシの登録

ASA はシスコ スマート ソフトウェア ライセンシングを使用します。通常のスマート ソフトウェア 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 Series Feature Licenses」を参照してください。このガイドは通常のスマート ソフトウェア ライセンシングに適用されます。

Firepower 4100 上の ASA では、スマート ソフトウェア ライセンシングの設定は、シャーシ上の FXOS と ASA に分割されています。

- Firepower 4100：ライセンス認証局との通信を行うためのパラメータを含めて、FXOS にすべてのスマート ソフトウェア ライセンス インフラストラクチャを設定します。Firepower 4100 自体には動作のためのライセンスは必要ありません。
- ASA：ASA のすべてのライセンスの権限付与を設定します。

シャーシを登録すると、License Authority によって シャーシと License Authority 間の通信に使用される ID 証明書が発行されます。また、適切な仮想アカウントにシャーシが割り当てられます。License Authority に登録するまでは、特殊なライセンスを必要とする機能の設定変更を行うことはできませんが、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。

- Standard
- セキュリティ コンテキスト
- Carrier：Diameter、GTP/GPRS、SCTP

- 強力な暗号化（3DES/AES）
- AnyConnect：AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。

スマート ソフトウェア ライセンシング アカウントから ASA の登録トークンを要求する場合、[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、シャーシ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。

ASDM アクセスには強力な暗号化が必要です。

始める前に

- Cisco 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。

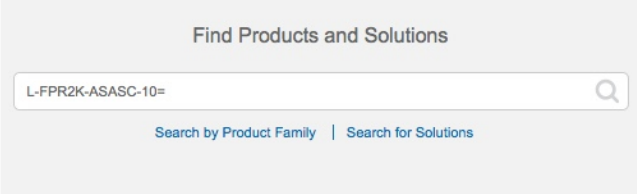
- （輸出コンプライアンス フラグを使用して有効化される）機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。
- まだ実行していない場合は、NTP の設定 を実行します。
- 初期設定時に DNS を設定しなかった場合は、**[プラットフォーム設定（Platform Settings）]**> **[DNS]** ページで DNS サーバを追加します。

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（少なくとも標準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、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *1*：ライセンス検索



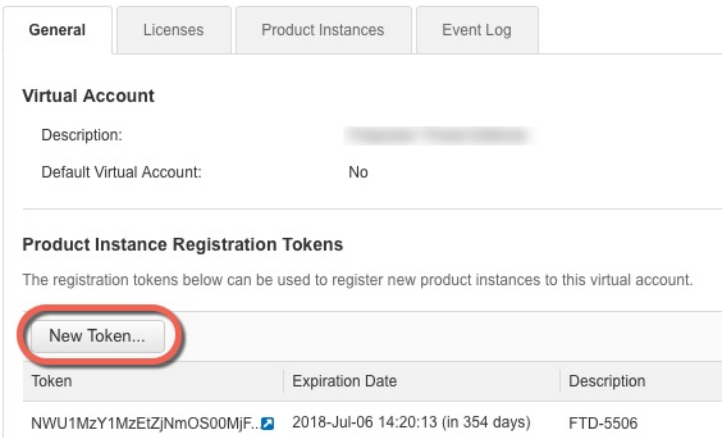
- 標準ライセンス：L-FPR4100-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。

- 10 コンテキストライセンス：L-FPR4K-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。
- 230 コンテキストライセンス：L-FPR4K-ASASC-230=。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。
- 250 コンテキストライセンス：L-FPR4K-ASASC-250=。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。
- キャリア（Diameter、GTP/GPRS、SCTP）：L-FPR4K-ASA-CAR=。
- 高度暗号化（3DES/AES）ライセンス：L-FPR4K-ENC-K9=。このライセンスは無料です。このライセンスは通常は必要ありませんが、トラッキングのために自分のアカウントに追加する必要があります。このライセンスは、古いサテライト サーバのバージョン（2.3.0 より前）を使用する ASA などには必要です。
- AnyConnect：『Cisco AnyConnect Ordering Guide』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。

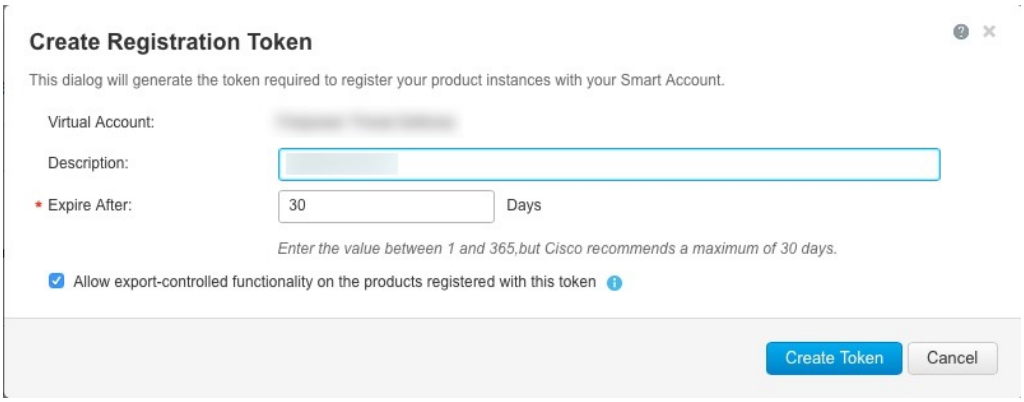
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [インベントリ（Inventory）] をクリックします。

b) [全般（General）] タブで、[新規トークン（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。



- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [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 [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 *2*: トークンの表示

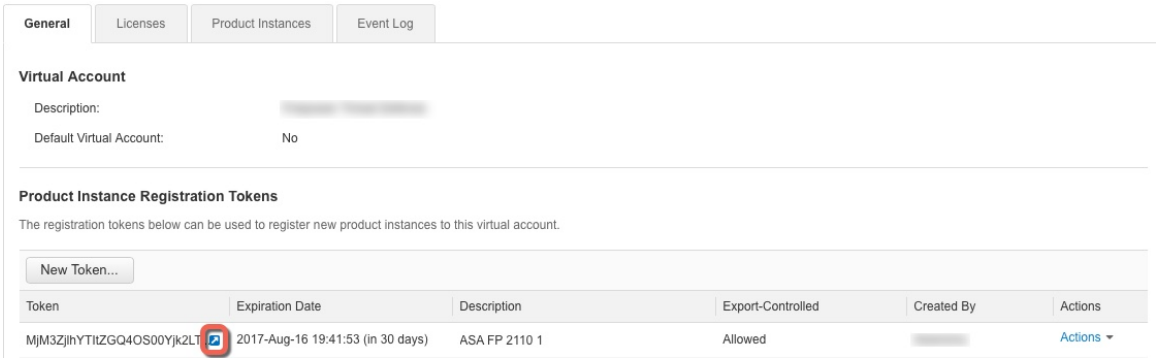
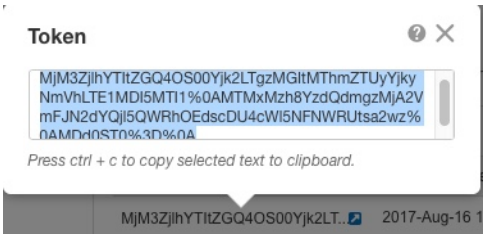
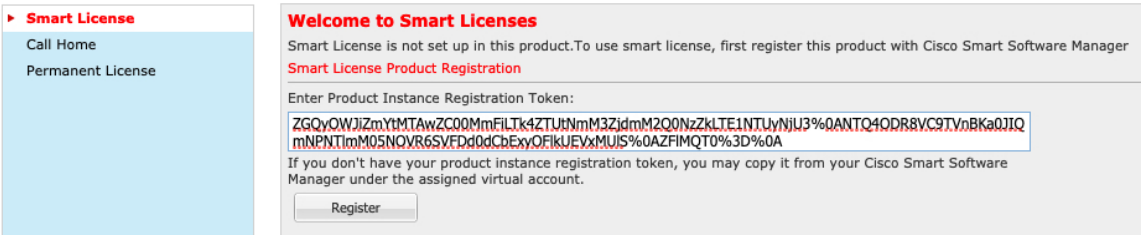


図 *3*: トークンのコピー



ステップ 3 Firepower Chassis Manager で、**[システム（System）] > [ライセンス（Licensing）] > [スマートライセンス（Smart License）]** の順に選択します。

ステップ 4 [Enter Product Instance Registration Token] フィールドに登録トークンを入力します。



ステップ 5 [Register] をクリックします。

Firepower 4100 がライセンス認証局に登録します。登録成功には数分かかることがあります。ページを更新してステータスを確認します。

図 *4*：登録が進行中

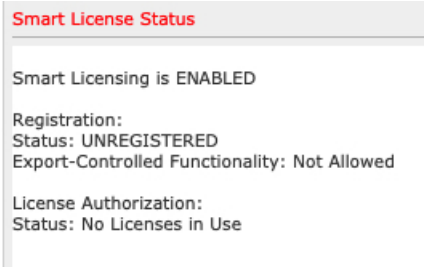
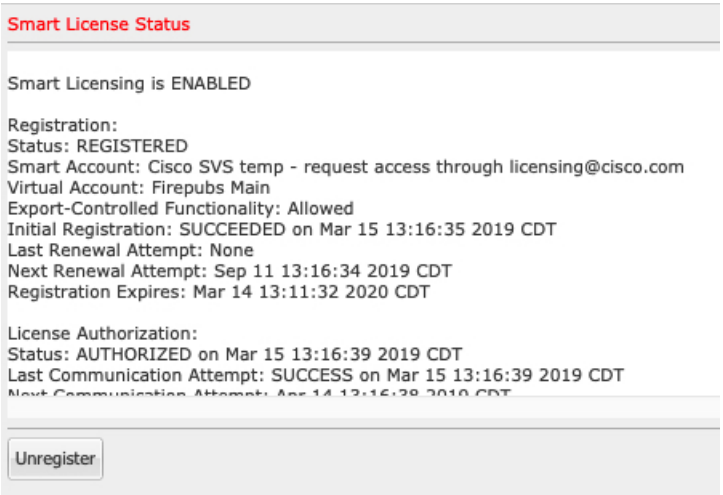


図 *5*：登録に成功しました



Firepower Chassis Manager：ASA 論理デバイスの追加

ASA をネイティブ インスタンスとして Firepower 4100 から展開できます。

フェールオーバー ペアまたはクラスタを追加するには、ASA の一般的な操作のコンフィギュレーション ガイドを参照してください。

この手順では、アプリケーションで使用されるブートストラップ設定を含む、論理デバイスの特性を設定できます。

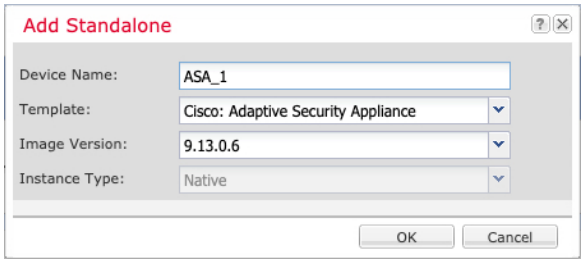
始める前に

- ASA と一緒に使用する管理インターフェイスを設定します。インターフェイスの設定 を参照してください。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用される（[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示される）シャーシ管理ポートと同じではありません。
- 次の情報を用意します。
  - このデバイスのインターフェイス ID
  - 管理インターフェイス IP アドレスとネットワーク マスク
  - ゲートウェイ IP アドレス
  - 新規管理者パスワード/イネーブル パスワード

手順

ステップ 1 Firepower Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）] > [スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシスーパバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

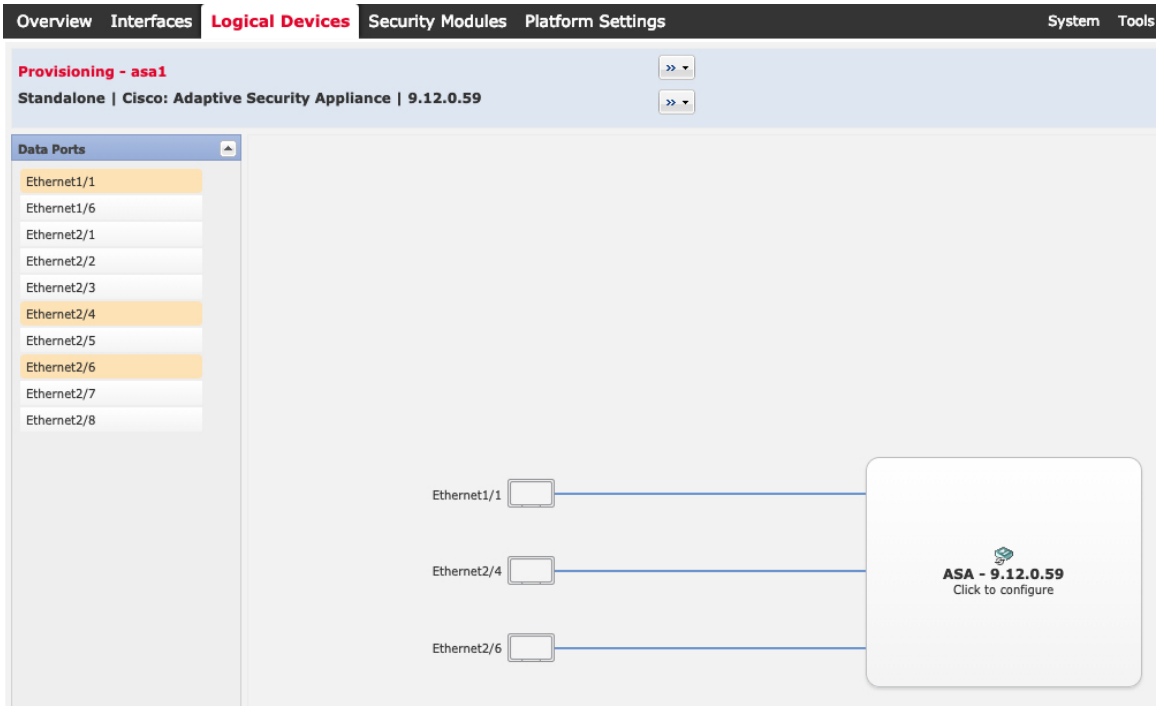
b) [Template] では、[Cisco Adaptive Security Appliance] を選択します。

c) [Image Version] を選択します。

d) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。

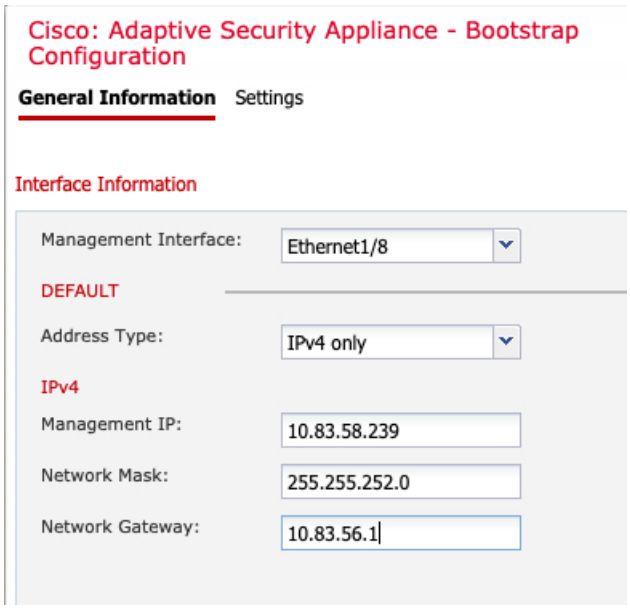


以前に [Interfaces] ページで有効にしたデータ インターフェイスのみを割り当てることができます。後ほど ASDM でこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [General Information] ページで、次の手順を実行します。



a) [Management Interface] を選択します。

このインターフェイスは、論理デバイスの管理に使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

b) 管理インターフェイスを選択します。[Address Type]、[IPv4 only]、[IPv6 only]、または [IPv4 and IPv6]。

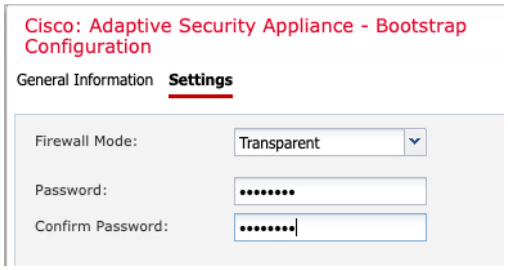
c) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

d) [Network Mask] または [Prefix Length] に入力します。

e) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] をクリックします。



a) [Firewall Mode] を [Routed] または [Transparent] に指定します。

ルーテッドモードでは、ASA は、ネットワークのルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォールモードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

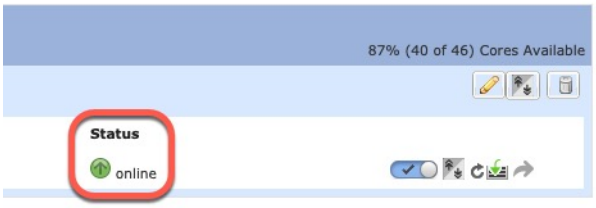
b) 管理者ユーザの [パスワード（Password）] を入力して確認し、パスワードを有効にします。

事前設定されている ASA 管理者ユーザ/パスワードおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスが可能な場合、パスワードを忘れたときに管理者ユーザ パスワードやイネーブル パスワードをリセットできます。

ステップ 7 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 8 **[保存（Save）]** をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



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。

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 release notes』を参照してください。
- Firepower Chassis Managerの [論理デバイス（Logical Devices）] ページで、ASA 論理デバイスの [ステータス（Status）] が [オンライン（online）] であることを確認します。

手順

ステップ 1 ブラウザに次の URL を入力します。

- **https://***management_ip*：ブートストラップ設定に入力した管理インターフェイスの IP アドレス。

[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。

ASA でのライセンス権限付与の設定

ASA にライセンスを割り当てます。少なくとも標準ライセンスを割り当てる必要があります。

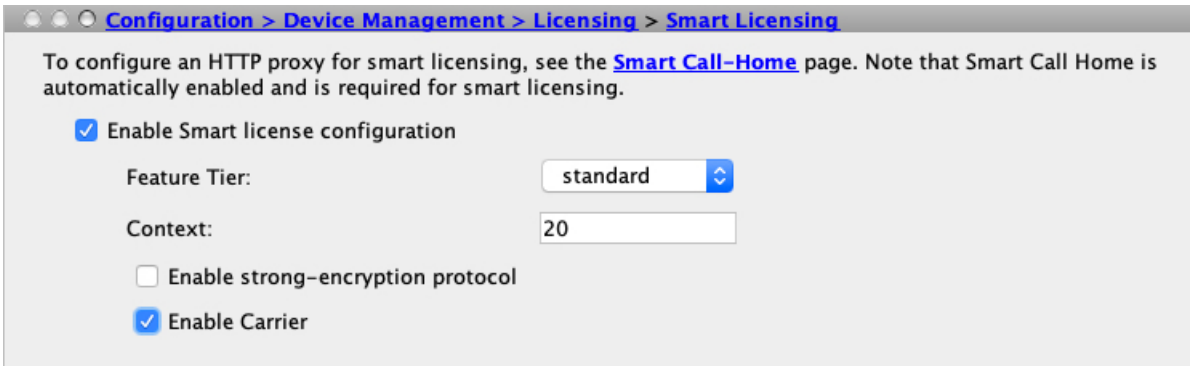
始める前に

- Firepower Chassis Manager：ライセンス サーバへのシャーシの登録 （3 ページ）。

手順

ステップ 1 ASDM で、**[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[ライセンシング（Licensing）]** > **[Smart Licensing]** の順に選択します。

ステップ 2 次のパラメータを設定します。



a) [Enable Smart license configuration] をオンにします。

b) [機能層（Feature Tier）] ドロップダウン リストから [標準（Standard）] を選択します。

使用できるのは標準層だけです。

c) （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。

10 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 250 です。たとえば、最大数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 240 を入力します。この値は、デフォルトの 10 に追加されます。

d) （任意） [キャリア（Carrier）] を確認します。

ステップ 3 （任意） 一般的に、[強力な暗号化プロトコルの有効化（Enable strong-encryption protocol）] をオンにする必要はありません。たとえば、古いサテライト サーバのバージョン（2.3.0 より前）を使用する ASA にはこのライセンスが必要ですが、このチェックボックスは、必要な場合、または自分のアカウントでのこのライセンスの使用状況を追跡する場合にはオンにできます。

ステップ 4 [Apply] をクリックします。

アカウントに適切なライセンスがない場合は、ライセンスの変更を適用できません。

ステップ 5 ツールバーの [保存（Save）] アイコンをクリックします。

ステップ 6 ASDM を終了し、再起動します。

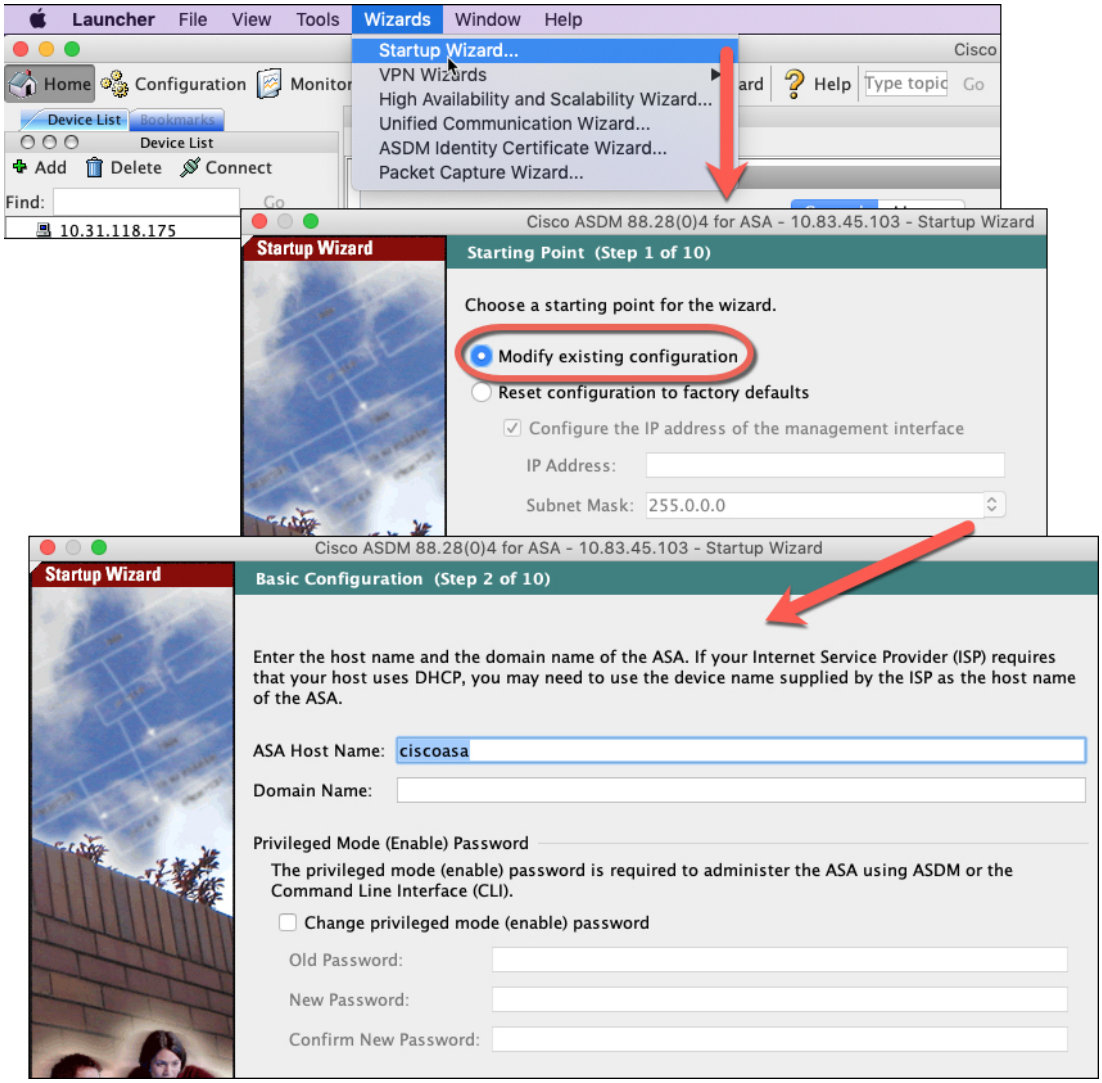
ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

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
- 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。

ASA CLI へのアクセス

ASA CLI を使用して、ASDM を使用する代わりに ASA のトラブルシューティングや設定を行うことができます。CLI にアクセスするには、FXOS CLI から接続します。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。詳細については、ASA の一般的な操作の設定ガイドを参照してください。

手順

ステップ 1 コンソール接続または Telnet 接続を使用して、FXOS からモジュール CLI に接続します。

connect module 1 {**console** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

ステップ 2 ASA コンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

ステップ 3 **Ctrl-a, d** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

例

次に、 ASA に接続してから、FXOS CLI のスーパバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

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。

ASA の履歴

機能	バージョン	詳細
ASA および FTD を同じ Firepower 9300 の別のモジュールでサポート	9.12(1)	ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1 が必要です。
ASA 論理デバイスのトランスペアレントモード展開のサポート	9.10(1)	ASA を展開するときに、トランスペアレントまたはルーテッド モードを指定できるようになりました。 （注） FXOS 2.4.1 が必要です。 新規/変更された [Firepower Chassis Manager] 画面： **[Logical Devices]** > **[Add Device]** > **[Settings]** > [Firewall Mode] ドロップダウン リスト
スマートエージェントの v1.6 へのアップグレード	9.6(2)	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンスアカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。
新しいキャリアライセンス	9.5(2)	新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インスペクションもサポートします。Firepower 9300 上の ASA の場合、**feature mobile-sp** コマンドは **feature carrier** コマンドに自動的に移行します。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**