ASDM を使用した ASA の展開

この章の対象読者

使用可能なすべてのオペレーティングシステムとマネージャを確認するには、「最適なオペレーティングシステムとマネージャを見つける方法」を参照してください。この章の内容は、ASDM を使用する ASA に適用されます。

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。

ファイアウォールについて

ハードウェアでは、Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。Threat Defense と ASA 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。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。「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。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム（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。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイドを参照してください。

プライバシー収集ステートメント：ファイアウォール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

ASA は、1 つのデバイスで高度でステートフルなファイアウォール機能および VPN コンセントレーター機能を提供します。

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（このガイドで説明）：デバイスに含まれる単独のデバイスマネージャ。
- CLI
- CDO：シンプルなクラウドベースのマルチデバイスマネージャ。
- Cisco Security Manager：別のサーバー上のマルチデバイス マネージャ。

トラブルシューティングのために、FXOS CLI にアクセスすることもできます。

サポートされない機能

ASA のサポートされない汎用機能

次の ASA 機能は、Firepower 1010 ではサポートされていません。

- マルチ コンテキスト モード
- アクティブ/アクティブ フェールオーバー
- 冗長インターフェイス
- クラスタ
- ASA REST API
- ASA FirePOWER module
- 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す）
- Diameter
- GTP/GPRS

VLAN インターフェイスおよびスイッチ ポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- ポリシーベース ルーティング
- 等コストマルチパス（ECMP）ルーティング
- インラインセットまたはパッシブインターフェイス
- VXLAN
- EtherChannel
- フェールオーバーおよびステートリンク
- トラフィック ゾーン
- セキュリティグループタグ（SGT）

ASA 5500-X 設定の移行

ASA 5500-X の設定をコピーして、Firepower 1010 に貼り付けることができます。ただし、設定を変更する必要があります。また、プラットフォーム間の動作の相違点に注意してください。

1. 設定をコピーするには、ASA 5500-X で **more system:running-config** コマンドを入力します。
2. 必要に応じて設定を編集します（以下を参照）。
3. Firepower 1010 のコンソールポートに接続し、グローバル コンフィギュレーション モードを開始します。

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. **clear configure all** コマンドを使用して、現在の設定をクリアします。

5. ASA CLI で変更された設定を貼り付けます。

このガイドでは、工場出荷時のデフォルト設定を前提としているため、既存の設定に貼り付ける場合、このガイドの一部の手順は ASA に適用されません。

ASA 5500-X 設定	Firepower 1010 の設定

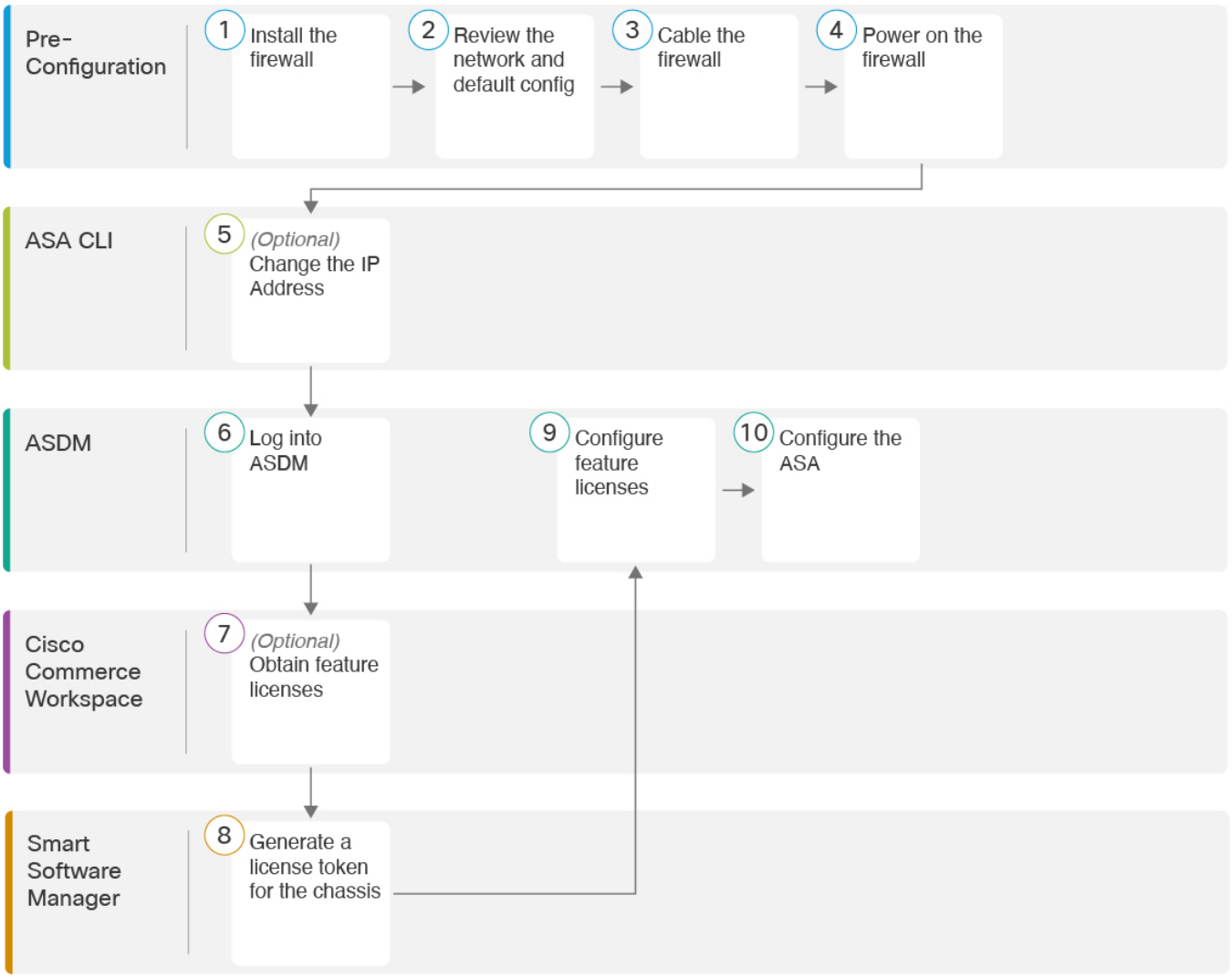
Ethernet 1/2 ～ 1/8 ファイアウォール インターフェイス	Ethernet 1/2 ～ 1/8 スイッチポート
	これらのイーサネットポートは、デフォルトではスイッチポートとして設定されています。設定内のインターフェイスごとに、通常のファイアウォール インターフェイスを作成するための **no switchport** コマンドを追加します。次に例を示します。
	`interface ethernet 1/2`
	`  no switchport`
	`  ip address 10.8.7.2 255.255.255.0`
	`  nameif inside`

PAK ライセンス	スマートライセンス 設定をコピーして貼り付けると、PAK ライセンスは適用されません。デフォルトではライセンスはインストールされていません。スマートライセンシングでは、スマートライセンシング サーバーに接続してライセンスを取得する必要があります。スマートライセンシングは、ASDM または SSH アクセスにも影響します（以下を参照）。
最初の ASDM アクセス	ASDM に接続できないか、スマート ライセンシング サーバーに登録できない場合は、弱い暗号化のみを設定した場合でも、VPN またはその他の強力な暗号化機能の設定を削除します。 強力な暗号化（3DES）ライセンスを取得した後に、これらの機能を再度有効にすることができます。 この問題の原因は、ASA には、管理アクセスに対してのみデフォルトで 3DES 機能が含まれていることです。強力な暗号化機能を有効にすると、ASDM および HTTPS トラフィック（スマートライセンシングサーバーとの間など）がブロックされます。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。

ASA 5500-X 設定	Firepower 1010 の設定
インターフェイス ID	新しいハードウェア ID と一致するようにインターフェイス ID を変更してください。たとえば、ASA 5525-X には、Management 0/0、GigabitEthernet 0/0 ～ 0/5 が含まれています。Firepower 1120 には、Management 1/1 および Ethernet 1/1 ～ 1/8 が含まれています。
boot system コマンド ASA 5500-X では、最大 4 つの **boot system** コマンドを使用して、使用するブートイメージを指定できます。	Firepower 1010 では 1 つの **boot system** コマンドのみが許可されるため、貼り付ける前に 1 つ以外のすべてのコマンドを削除する必要があります。ブートイメージを判別するために起動時に読み込まれないため、実際に任意のコマンドを設定に含める必要はありません。 **boot system** リロード時には、最後にロードされたブート イメージが常に実行されます。 **boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。

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	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 [英語] 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の投入
5	ASA CLI	（任意）IP アドレスの変更 （12 ページ）。
6	ASDM	ASDM へのログイン （13 ページ）。

7	Cisco Commerce Workspace	ライセンスの設定 （14 ページ）：機能ライセンスを取得します。
8	Smart Software Manager	ライセンスの設定 （14 ページ）：シャーシのライセンス トークンを生成します。
9	ASDM	ライセンスの設定 （14 ページ）：機能ライセンスを設定します。
10	ASDM	ASA の設定 （20 ページ）。

ネットワーク配置とデフォルト設定の確認

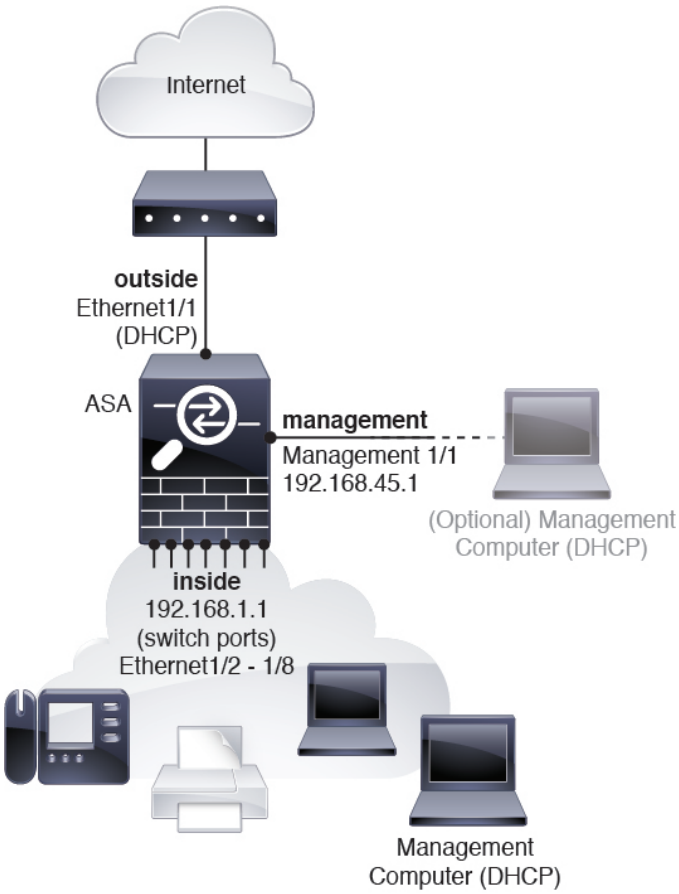
次の図は、Firepower 1010 でのデフォルトのネットワーク配置を示しています（デフォルト設定を使用）。

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） ASDM アクセスにデフォルト管理 IP アドレスを使用できない場合は、ASA CLI で管理 IP アドレスを設定できます。「（任意）IP アドレスの変更 （12 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。



Firepower 1010 のデフォルト設定

Firepower 1010 の工場出荷時のデフォルト設定は、次のとおりです。

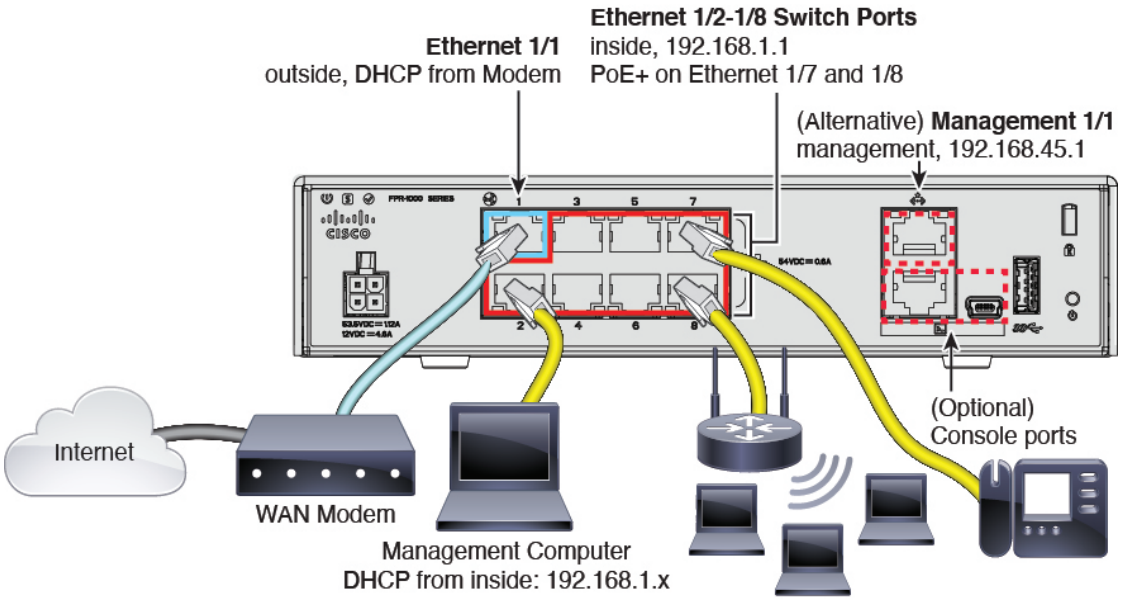
- **ハードウェア スイッチ**：イーサネット 1/2 ～ 1/8 は VLAN 1 に属しています。
- **内部から外部**へのトラフィック フロー：イーサネット 1/1（外部）、VLAN 1（内部）
- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- DHCP の**外部 IP アドレス**、内部 IP アドレス：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **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。
- **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 Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
```

```
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

デバイスの配線



管理 1/1、またはイーサネット 1/2 ～ 1/8（内部スイッチ ポート）のいずれかで Firepower 1010 を管理します。デフォルト設定でも、イーサネット 1/1 は外部として設定されています。

手順

ステップ 1 ハードウェア設置ガイドを使用してハードウェアを設置し、ハードウェアについてよく理解しておきます。

ステップ 2 管理コンピュータを次のいずれかのインターフェイスに接続します。

- イーサネット 1/2 ～ 1/8：管理コンピュータをいずれかの内部スイッチ ポート（イーサネット 1/2 ～ 1/8）に直接接続します。内部インターフェイスにはデフォルトの IP アドレス（192.168.1.1）があり、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内部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 1010 のデフォルト設定 （8 ページ）を参照）。
- 管理 1/1：管理コンピュータを管理 1/1 に直接接続します。または、管理 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 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。管理 1/1 にはデフォルトの IP アドレス（192.168.45.1）があり、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 1010 のデフォルト設定 （8 ページ）を参照）。

  Management 1/1 の 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、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）IP アドレスの変更 （12 ページ）」を参照してください。

ステップ 3 外部ネットワークを Ethernet 1/1 インターフェイスに接続します。

スマート ソフトウェア ライセンシングの場合、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 4 内部デバイスを残りの内部スイッチ ポート（イーサネット 1/2 ～ 1/8）に接続します。

イーサネット 1/7 および 1/8 は PoE+ ポートです。

（注） PoE は Firepower 1010E ではサポートされていません。

ファイアウォールの電源の投入

システムの電源は電源コードで制御されます。電源ボタンはありません。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

始める前に

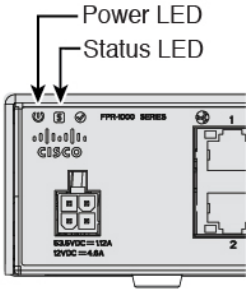
デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

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。

電源コードを差し込むと電源が自動的に入ります。

ステップ 2 デバイスの背面または上部にある電源 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 3 デバイスの背面または上部にあるステータス 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。

（任意）IP アドレスの変更

ASDM アクセスにデフォルトの IP アドレスを使用できない場合は、ASA CLI で管理インターフェイスの IP アドレスを設定できます。

（注） この手順では、デフォルト設定を復元し、選択した IP アドレスも設定します。このため、保持する ASA 設定に変更を加えた場合は、この手順を使用しないでください。

手順

ステップ 1 ASA コンソールポートに接続し、グローバル コンフィギュレーション モードに入ります。詳細については、「ASA および FXOS CLI へのアクセス （22 ページ）」を参照してください。

ステップ 2 選択した IP アドレスを使用してデフォルト設定を復元します。

configure factory-default [*ip_address* [*mask*]]

例：

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

ステップ 3 デフォルト コンフィギュレーションをフラッシュメモリに保存します。

write memory

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。

ASA には、管理アクセスのみを対象にした 3DES 機能がデフォルトで含まれているので、Smart Software Manager に接続でき、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に Smart Software Manager に登録する必要がある高度暗号化が有効になっている必要があります。

（注） 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソール ポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。

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 リリース ノート』を参照してください。

手順

ステップ 1 ブラウザに次の URL を入力します。

- **https://192.168.1.1**：内部インターフェイスの IP アドレス。内部スイッチ ポート（Ethernet1/2 ～ 1/8）の内部アドレスに接続できます。
- **https://192.168.45.1**：管理インターフェイスの IP アドレス。

（注） **http://** や IP アドレス（デフォルトは HTTP）ではなく、必ず **https://** を指定してください。ASA は、HTTP リクエストを HTTPS に自動的に転送しません。

[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 ユーザー名とパスワードのフィールドを空のままにして、[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 を参照してください。

シャーシを登録すると、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
- Security Plus：アクティブ/スタンバイ フェールオーバーの場合

- 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

ASA には、管理アクセスのみを対象にした 3DES 機能がデフォルトで含まれているので、Smart Software Manager に接続でき、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に Smart Software Manager に登録する必要がある高度暗号化が有効になっている必要があります。

（注） 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソール ポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。

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。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。

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。

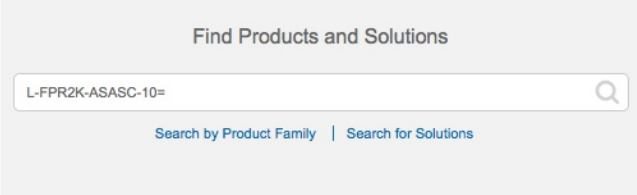
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用の Smart Software Manager アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

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、Smart Software Manager 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

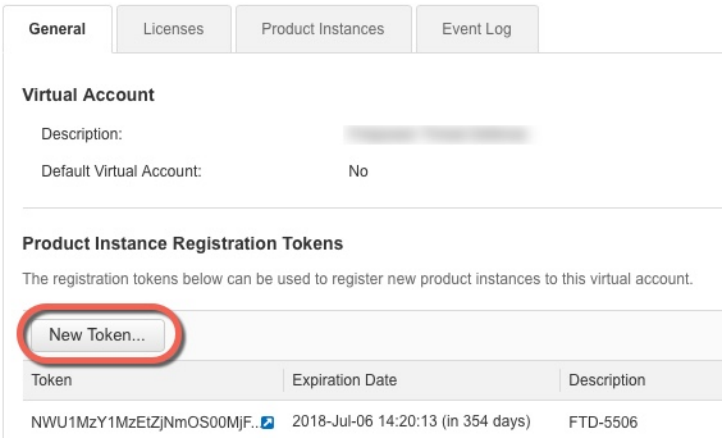


- Essentials ライセンス：L-FPR1000-ASA=。Essentials ライセンスは無料ですが、スマートソフトウェア ライセンシング アカウントに追加する必要があります。
- Security Plus ライセンス：L-FPR1010-SEC-PL=。Security Plus ライセンスによってフェールオーバーが有効になります。
- Strong Encryption（3DES/AES）license—L-FPR1K-ENC-K9=. アカウントに強力な暗号が承認されていない場合にのみ必要です。
- Cisco Secure Client：『Cisco Secure Client 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。

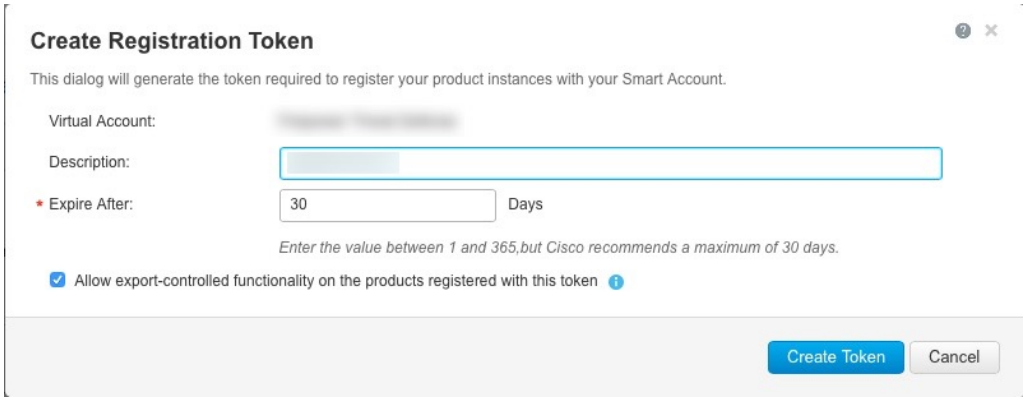
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

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。



- **[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 [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 *2:* トークンの表示

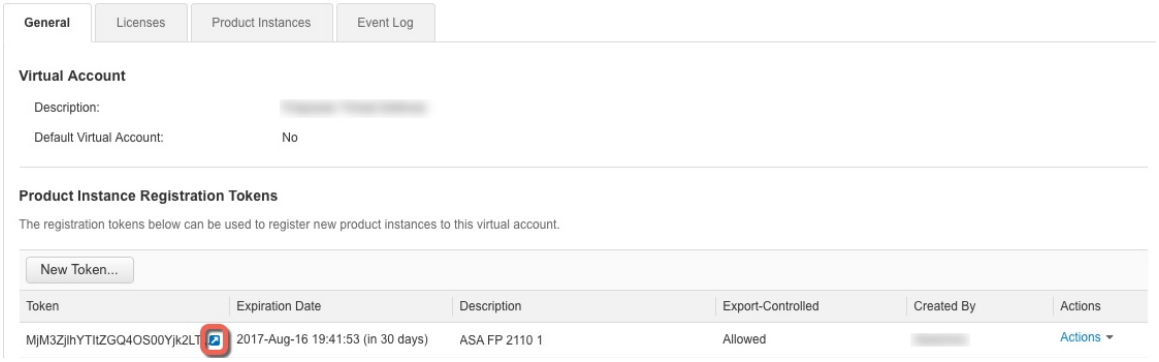
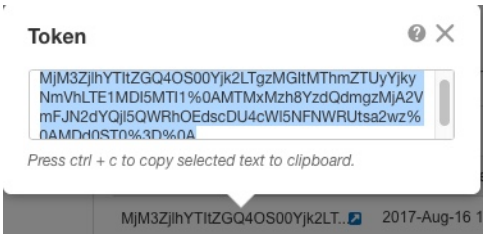
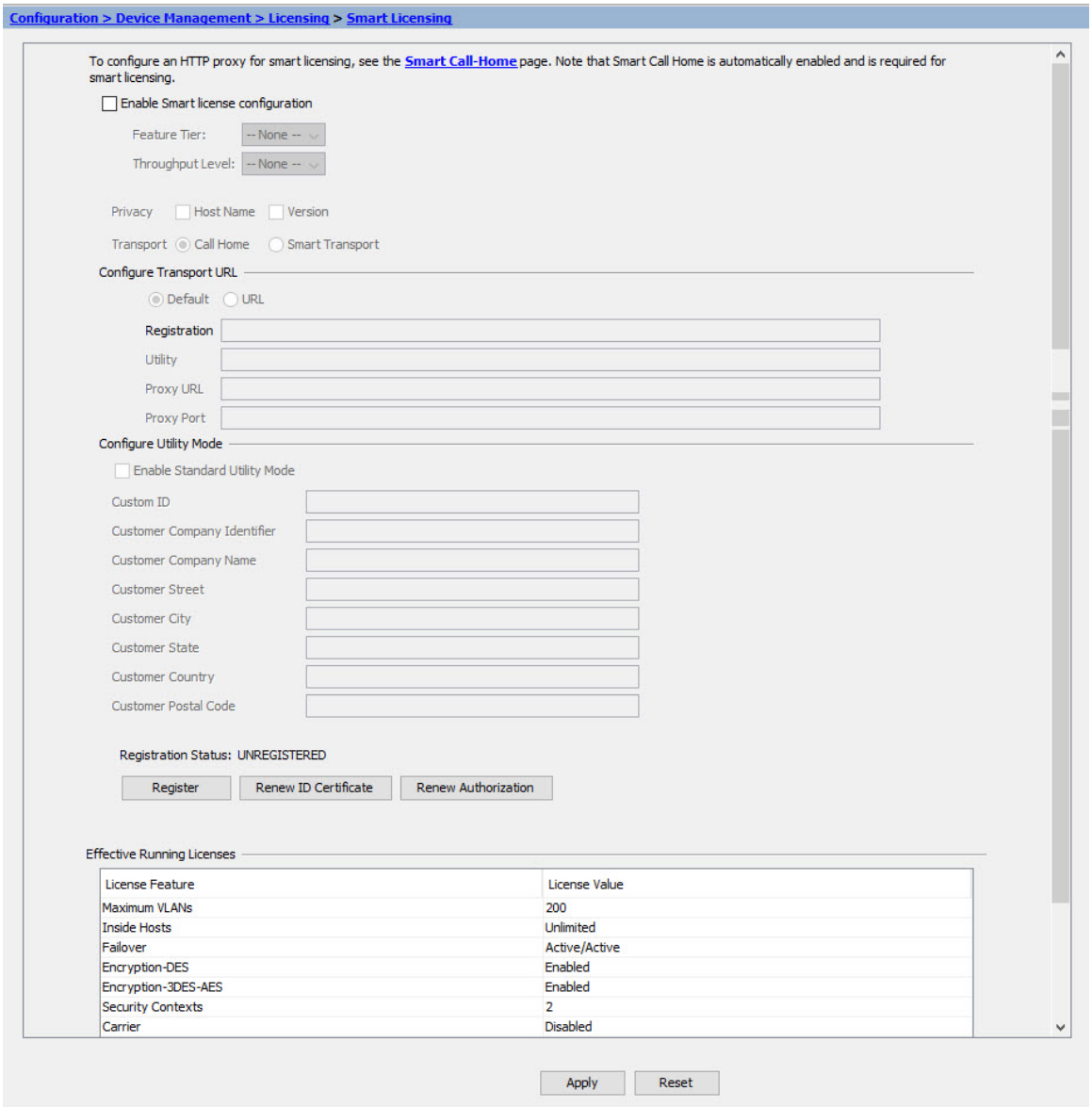


図 *3:* トークンのコピー

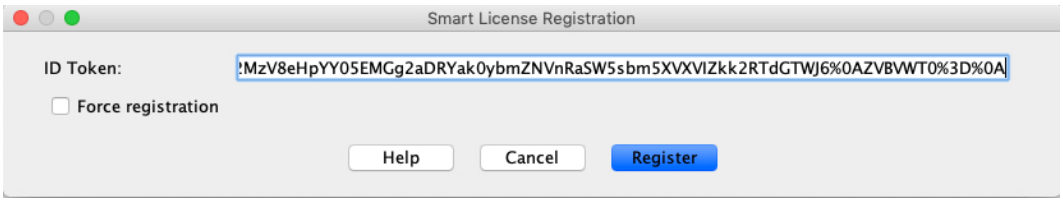


ステップ 3 ASDM で、**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 4 [Register] をクリックします。



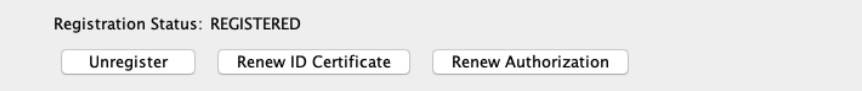
ステップ 5 [ID Token] フィールドに登録トークンを入力します。



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、ライセンススタータスを確認できます。



ステップ 7 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 **[Essentials]** を選択します。

使用できるのは Essentials 層だけです。

c) （任意） [Security Plus の有効化（Enable Security Plus）] をオンにします。

Security Plus 層では、アクティブ/スタンバイ フェールオーバーが有効になります。

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。

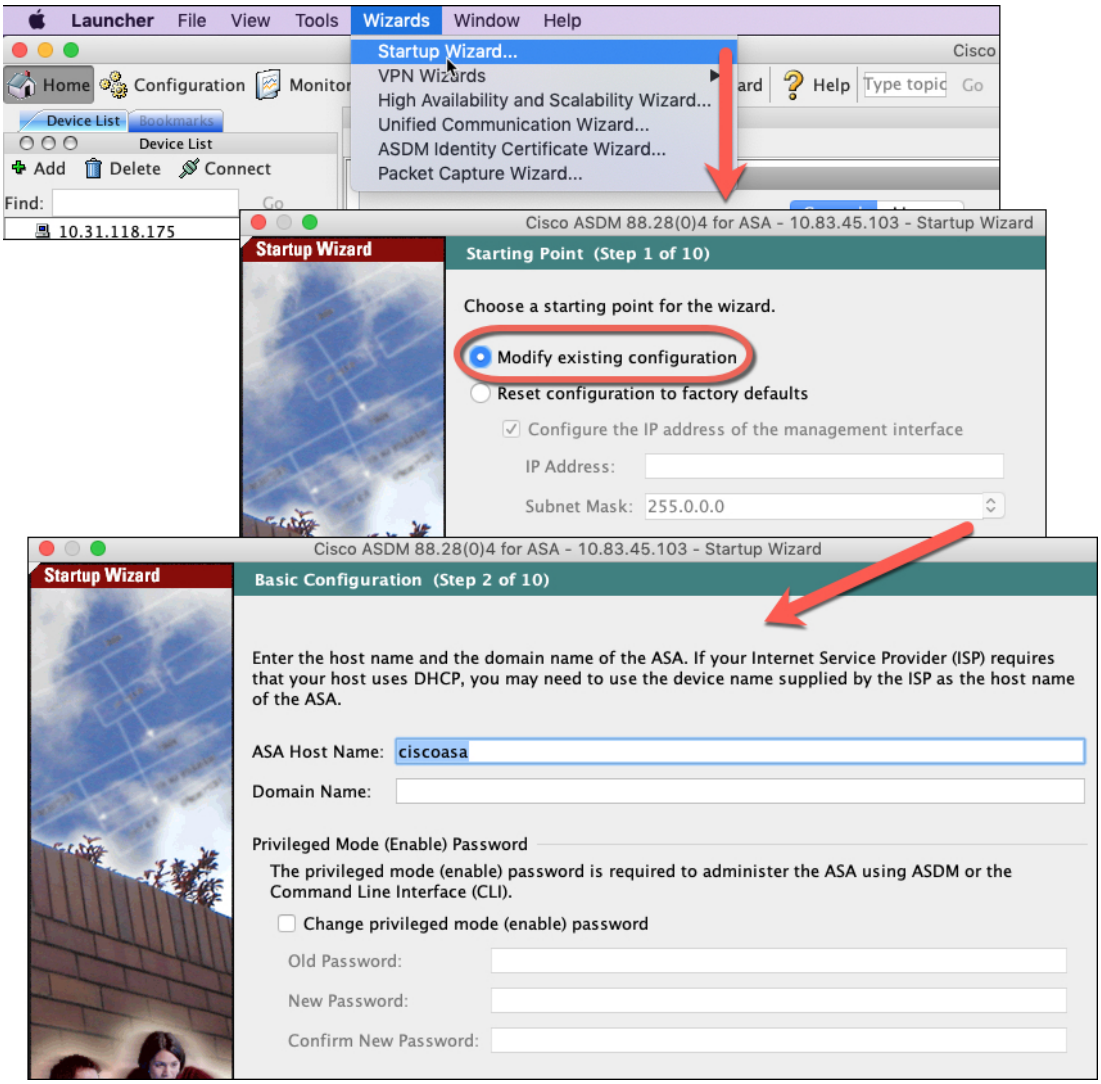
ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

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。

ASA および FXOS CLI へのアクセス

ASDM を使用する代わりに、ASA CLI を使用して 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 には、コンソール ポートに接続してアクセスできます。後で任意のインターフェイスで ASA への SSH アクセスを設定できます。SSH アクセスはデフォルトで無効になっています。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。

トラブルシューティングのために、ASA CLI からも FXOS CLI にアクセスできます。

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 1000 には、USB A to B シリアル ケーブルが付属しています。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（次を参照『Firepower 1010 hardware guide』）『。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

ASA CLI 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。

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#
```

ASA で設定したイネーブル パスワードは、FXOS **管理者**のユーザー パスワードでもあり、ASA の起動に失敗した場合は、FXOS フェールセーフ モードに移行します。

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 EXEC 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)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit**、**quit**、または **end** コマンドを入力します。

ステップ 4 （任意） FXOS CLI に接続します。

connect fxos [**admin**]

- **admin**：管理者レベルのアクセスを提供します。このオプションを指定しないと、ユーザーのアクセス権は読み取り専用アクセスになります。管理者モードであっても、コンフィギュレーション コマンドは使用できないことに注意してください。

ユーザーはクレデンシャルの入力を求められません。現在の ASA ユーザー名が FXOS に渡されるため、追加のログインは必要ありません。ASA CLI に戻るには、**exit** と入力するか、**Ctrl+Shift+6** を押し、**x** と入力します。

FXOS 内では、**scope security/show audit-logs** コマンドを使用してユーザーアクティビティを表示できます。

例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
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、Cisco ASA シリーズの操作マニュアルの中から、お使いの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。
- 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。

次のステップ

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。