



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、「[最適なアプリケーション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。

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 Secure Firewall ASA および Secure Firewall 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、[Cisco FXOS トラブルシューティングガイド \(Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け\)](#)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タスク \(3 ページ\)](#)
- [ネットワーク配置とデフォルト設定の確認 \(5 ページ\)](#)
- [ファイアウォールのケーブル接続 \(7 ページ\)](#)
- [ファイアウォールの電源投入 \(8 ページ\)](#)
- [\(任意\) IP アドレスの変更 \(9 ページ\)](#)
- [ASDM へのログイン \(10 ページ\)](#)
- [ライセンスの設定 \(11 ページ\)](#)
- [ASA の設定 \(18 ページ\)](#)

- [ASA および FXOS CLI へのアクセス \(19 ページ\)](#)
- [次のステップ \(21 ページ\)](#)

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 コンセントレータ機能を提供します。

ASA 5500-X 設定の移行

ASA 5500-X の設定をコピーして、Cisco Secure Firewall 4200 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. Cisco Secure Firewall 4200 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。

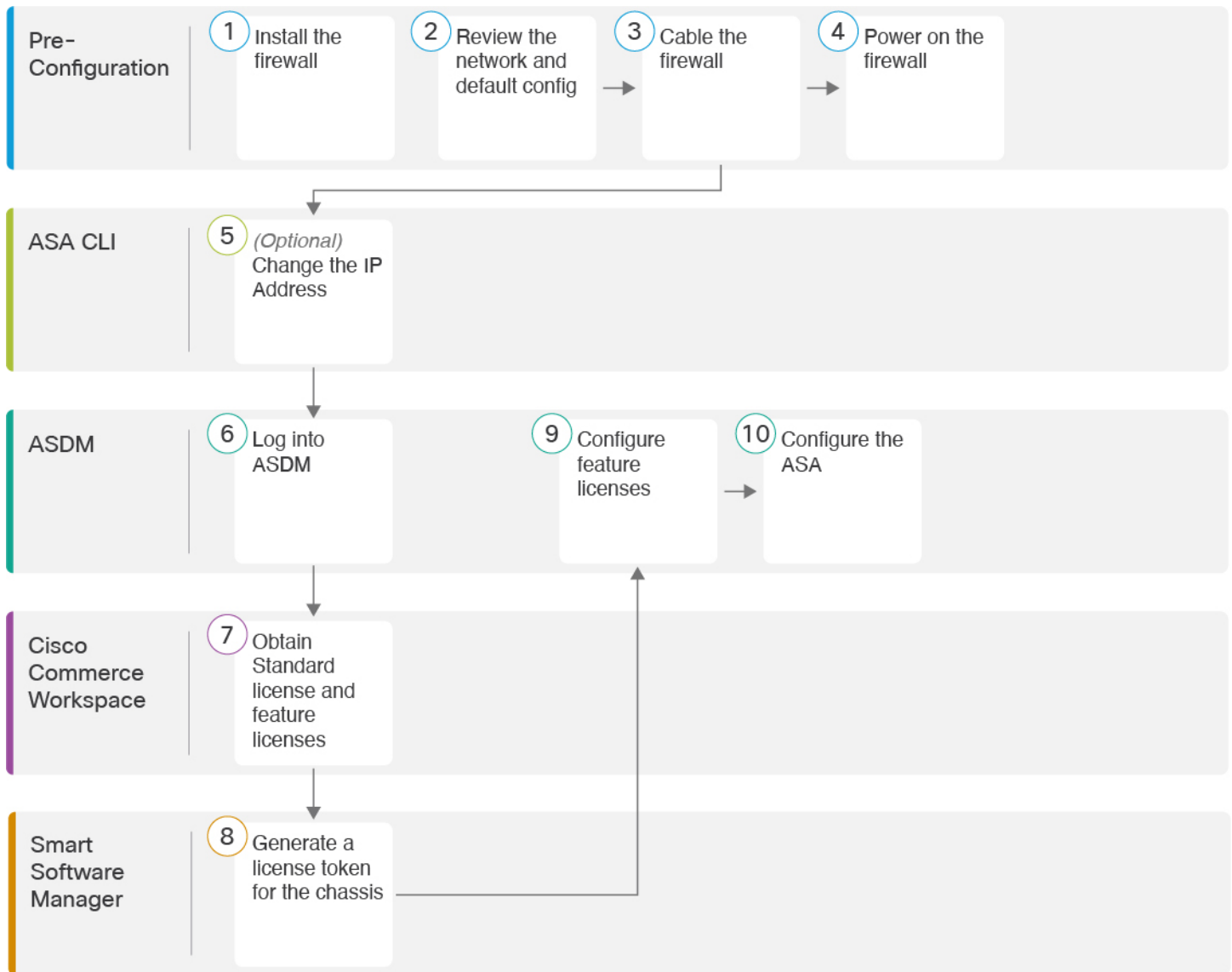
| ASA 5500-X 設定 | Cisco Secure Firewall 4200 の設定 |
|---------------|---|
| PAK ライセンス | スマートライセンス 設定をコピーして貼り付けると、PAK ライセンスは適用されません。デフォルトではライセンスはインストールされていません。スマートライセンシングでは、スマートライセンシングサーバーに接続してライセンスを取得する必要があります。スマートライセンシングは、ASDM または SSH アクセスにも影響します (以下を参照)。 |

| ASA 5500-X 設定 | Cisco Secure Firewall 4200 の設定 |
|--|---|
| 最初の ASDM アクセス | <p>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。</p> <p>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。</p> <p>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。</p> |
| インターフェイス ID | <p>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。</p> |
| <p>boot system コマンド</p> <p>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。</p> | <p>Cisco Secure Firewall 4200 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。</p> <p>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。</p> |

エンドツーエンドのタスク

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。

図 1: エンドツーエンドのタスク



| | | |
|---|---------|--|
| 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 (5 ページ)。 |
| ③ | 事前設定 | ファイアウォールのケーブル接続 (7 ページ)。 |
| ④ | 事前設定 | ファイアウォールの電源投入 (8 ページ)。 |
| ⑤ | ASA CLI | (任意) IP アドレスの変更 (9 ページ)。 |

| | | |
|---|--------------------------|--|
| ⑥ | ASDM | ASDM へのログイン (10 ページ)。 |
| ⑦ | Cisco Commerce Workspace | 基本ライセンスとオプションの機能ライセンスを取得します (「 ライセンスの設定 (11 ページ) 」)。 |
| ⑧ | Smart Software Manager | シャーシのライセンストークンを生成します (「 ライセンスの設定 (11 ページ) 」)。 |
| ⑨ | ASDM | 機能ライセンスを設定します (「 ライセンスの設定 (11 ページ) 」)。 |
| ⑩ | ASDM | ASA の設定 (18 ページ)。 |

ネットワーク配置とデフォルト設定の確認

次の図に、ASA でのデフォルトのネットワーク展開を示します (デフォルト設定を使用)。

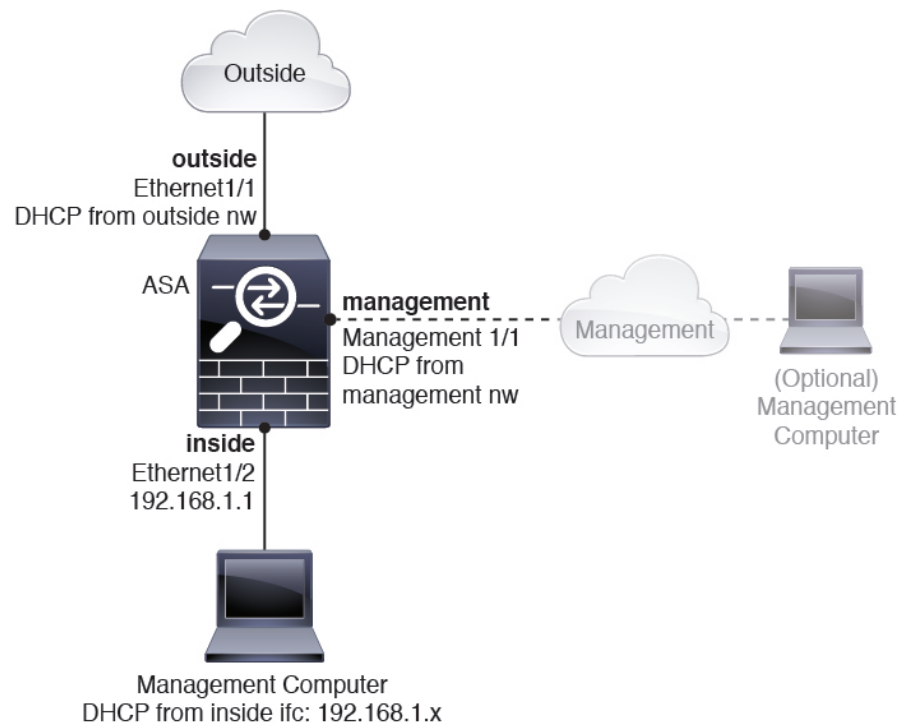
外部インターフェイスをケーブルモデムまたは DSL モデムに直接接続する場合は、ASA が内部ネットワークのすべてのルーティングと NAT を実行するように、モデムをブリッジモードにすることをお勧めします。外部インターフェイスが ISP に接続するために PPPoE を設定する必要がある場合は、その設定を ASDM スタートアップウィザード内で行うことができます。



(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 \(9 ページ\)](#)」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。



Cisco Secure Firewall 4200 のデフォルト設定

Cisco Secure Firewall 4200 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
- 管理：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 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。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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
```

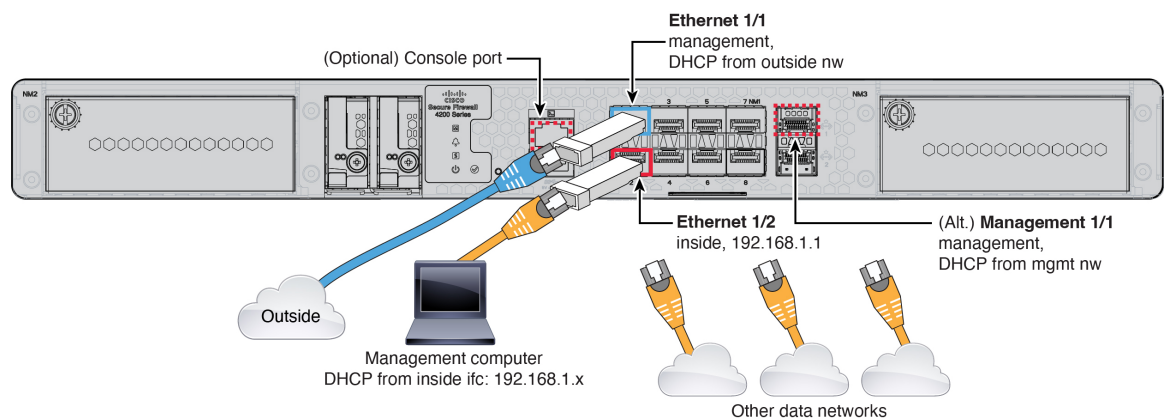
```

!
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 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!

```

ファイアウォールのケーブル接続

図 2: Cisco Secure Firewall 4200 のケーブル接続



Management 1/1 またはイーサネット 1/2 のいずれかで Cisco Secure Firewall 4200 を管理します。デフォルト設定でも、Ethernet1/1 を外部として設定します。

始める前に

- データインターフェイスおよびオプションの管理ポートに SFP を取り付けます。組み込みポートは、SFP モジュールを必要とする 1/10/25 Gb SFP ポートです。
- (オプション) コンソールケーブルを入手します。デフォルトではファイアウォールにコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。

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次のいずれかのインターフェイスに接続します。

- **Ethernet 1/2** : Ethernet 1/2 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 ([Cisco Secure Firewall 4200 のデフォルト設定 \(6 ページ\)](#) を参照)。192.168.1.0/24 上のクライアントのみが ASA にアクセスできます。

また、イーサネット 1/2 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 \(9 ページ\)](#) を参照してください)。

- **Management 1/1** : Management 1/1 は、管理ネットワーク上の DHCP サーバーから IP アドレスを取得します。このインターフェイスを使用する場合は、管理コンピュータから IP アドレスに接続できるように、ASA に割り当てられる IP アドレスを決定する必要があります。

別の管理インターフェイスが必要な場合は、後で Management 1/2 を設定できます。

後で他のインターフェイスから ASA 管理アクセスを設定できます。 [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 外部ネットワークを Ethernet1/1 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スの場合、ASA にはインターネットアクセスが必要です。

ステップ 4 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。

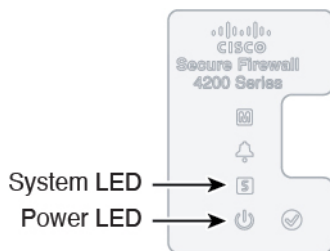
ファイアウォールの電源投入

システムの電源は、ファイアウォールの背面にあるロッカー電源スイッチによって制御されません。電源スイッチは、ソフト通知スイッチとして実装されています。これにより、システムのグレースフルシャットダウンがサポートされ、システム ソフトウェアおよびデータの破損のリスクが軽減されます。

手順

- ステップ1 電源コードをファイアウォールに接続し、電源コンセントに接続します。
- ステップ2 シャーシの背面で、電源コードに隣接する標準的なロッカータイプの電源オン/オフ スイッチを使用して電源をオンにします。
- ステップ3 ファイアウォールの背面にある電源 LED を確認します。緑色に点灯している場合は、ファイアウォールの電源が入っています。

図 3: システムおよび電源 LED



- ステップ4 ファイアウォールの背面にあるシステム LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

(注) スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの電源 LED が緑に点滅します。電源 LED が完全にオフになるまで電源を切らないでください。

(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 で内部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 \(19 ページ\)](#)」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 ethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 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。この規則の例外は、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 (Ethernet 1/2) インターフェイスの IP アドレス。
- **https://management_ip** : DHCP から割り当てられた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 [ASDMランチャーのインストール (**Install ASDM Launcher**)] をクリックします。

ステップ 3 画面の指示に従い、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

- セキュリティ コンテキスト
- キャリア (Diameter、GTP/GPRS、M3UA、SCTP)
- 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。この規則の例外は、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、シャージ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

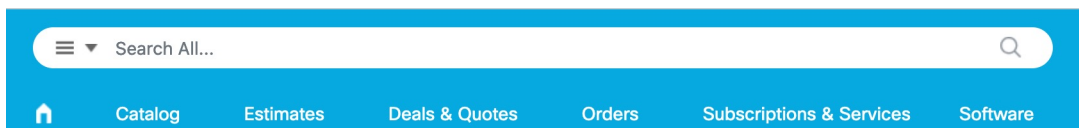
- [Smart Software Manager](#) にマスターアカウントを持ちます。
まだアカウントをお持ちでない場合は、リンクをクリックして[新しいアカウントを設定](#)してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用の Smart Software Manager アカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

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。

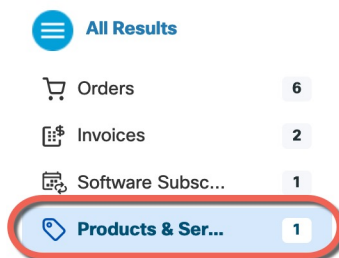
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェアライセンシングアカウントにリンクされています。ただし、自身でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [すべて検索 (Search All)] フィールドを使用します。

図 4: 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 5: 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-FPR4215-BSE=. Essentials ライセンスは必須ライセンスです。
- Essentials ライセンス : L-FPR4225-BSE=. Essentials ライセンスは必須ライセンスです。
- Essentials ライセンス : L-FPR4245-BSE=. Essentials ライセンスは必須ライセンスです。
- 5 コンテキストライセンス : L-FPR4200-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-FPR4200-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。
- キャリア (Diameter、GTP/GPRS、M3UA、SCTP) : L-FPR4200-ASA-CAR=
- 強力な暗号化 (3DES/AES) ライセンス : L-FPR4200-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。

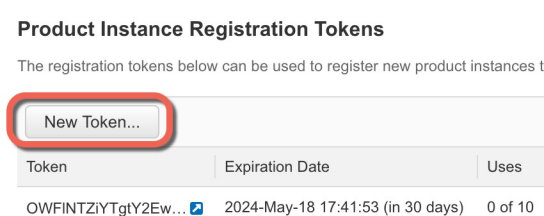
- Cisco Secure Client : 『Cisco Secure Client 発注ガイド』を参照してください。ASA では、このライセンスを直接有効にしないでください。

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

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 ⓘ

- [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 6: トークンの表示

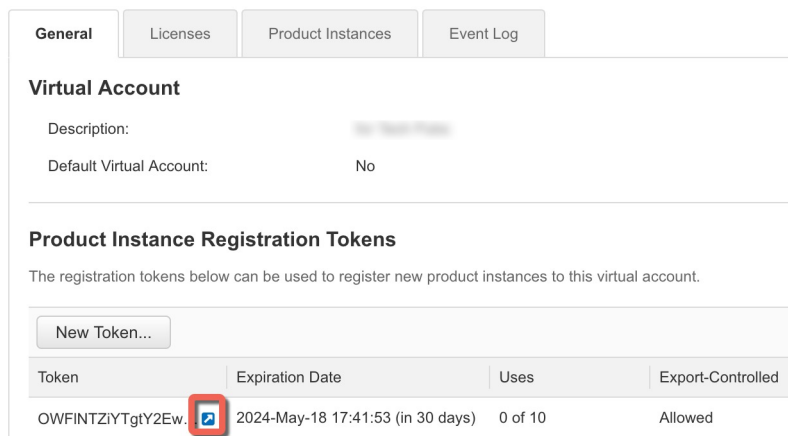
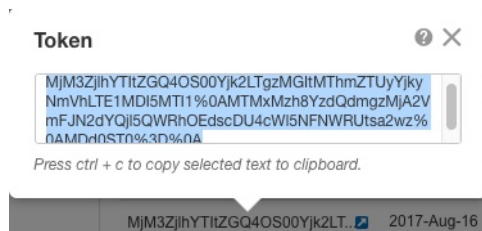


図 7: トークンのコピー



- 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:

Throughput Level:

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

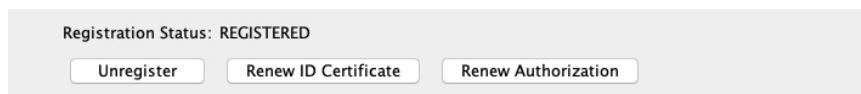
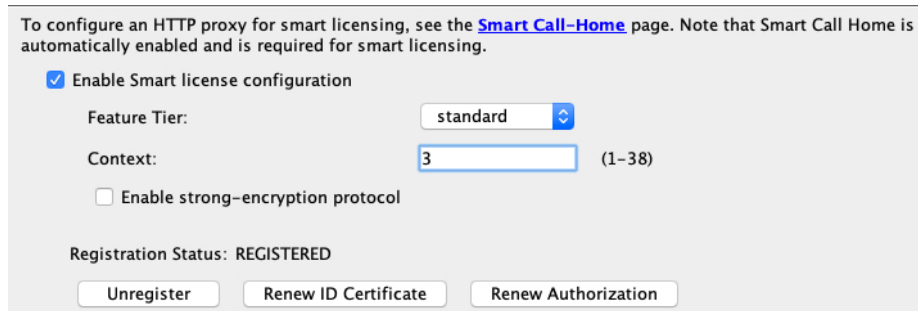
ID Token:

Force registration

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。

**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） [Context] ライセンスの場合、コンテキストの数を入力します。
 - Cisco Secure Firewall 4200 : 100 コンテキスト

たとえば、Cisco Secure Firewall 4215 で最大 100 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 98 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。

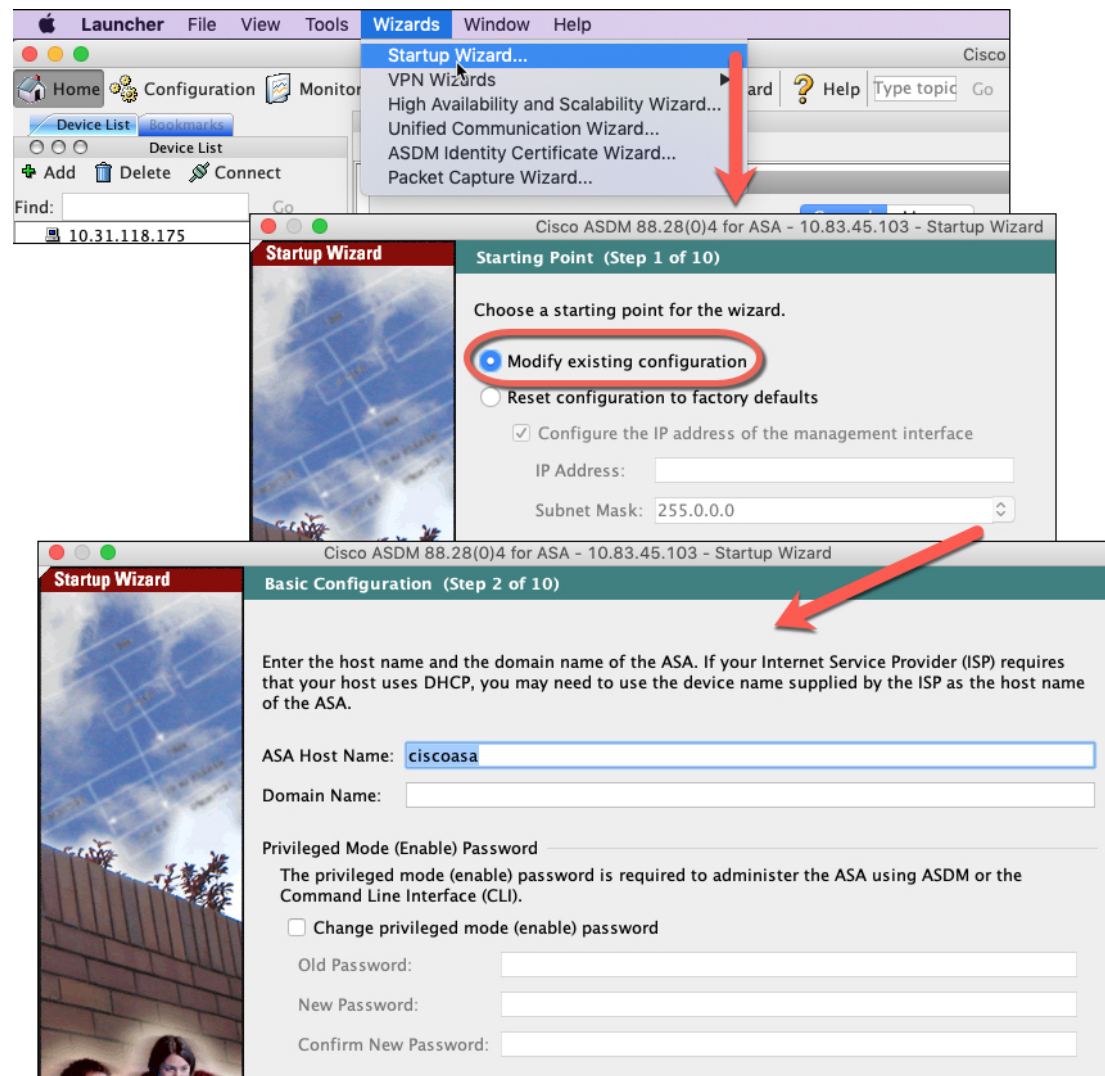
ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

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。

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 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。ご使用のオペレーティングシステムに必要な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

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。

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。