Firepower Management Center インストールおよび初期セットアップ

この章では、FMC をインストールして初期セットアッププロセスを実行する方法について説明します。

初期セットアップの概要

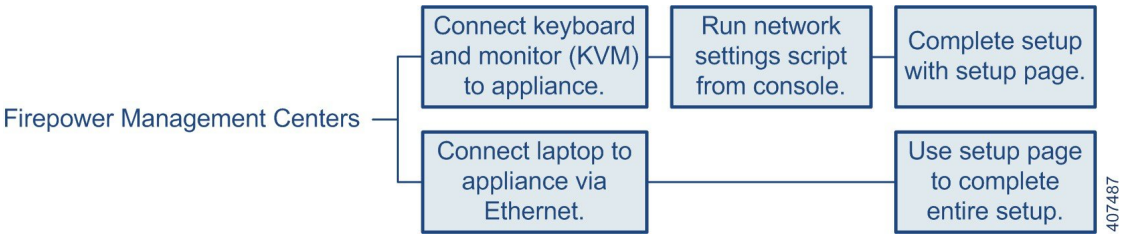
FMC をインストールしたら、初期セットアッププロセスを完了して、新しいアプライアンスを設定する必要があります。

FMC で Firepower バージョン6.3 - 6.4.x を実行している場合は、次のようになります。

FMC Web インターフェイスに初めてログインすると、初期管理ページを使用して、信頼できる管理ネットワーク上で通信するように新しいアプライアンスを設定できます。また、管理者パスワードの変更、エンドユーザライセンス契約書（EULA）への同意、時間の設定、および更新のスケジュールなどの初期管理レベル タスクも実行する必要があります。

この初期設定プロセスを実行するために FMC にアクセスする際は、アプライアンスに直接接続されたラップトップを使用することも、信頼できるローカル管理ネットワークを介したイーサネット接続を使用することもできます。次の図に、Firepower バージョン 6.3 - 6.4.x を実行している FMC の設定時に選択可能な選択肢を示します。

図 *1 : FMC* セットアップワークフロー、バージョン *6.3 - 6.4.x*



次のように、バージョン 6.3 - 6.4.x を実行している FMC をインストールしてセットアップします。

- 「アプライアンスの設置 （4ページ）」の説明に従って、アプライアンスを設置します。
- FMC をネットワークに接続する前に、FMC の eth0 の IP アドレスをネットワークに合わせて変更してから、初期設定を実行する必要があります。次の 2 つの選択肢があります。
  - 初期設定を実行する前に、VGA/キーボード接続を使用して FMC にアクセスし、eth0 の IP アドレスを設定します。「キーボードとモニタによる FMC へのアクセス（バージョン 6.3 - 6.4.x） （7 ページ）」を参照してください。

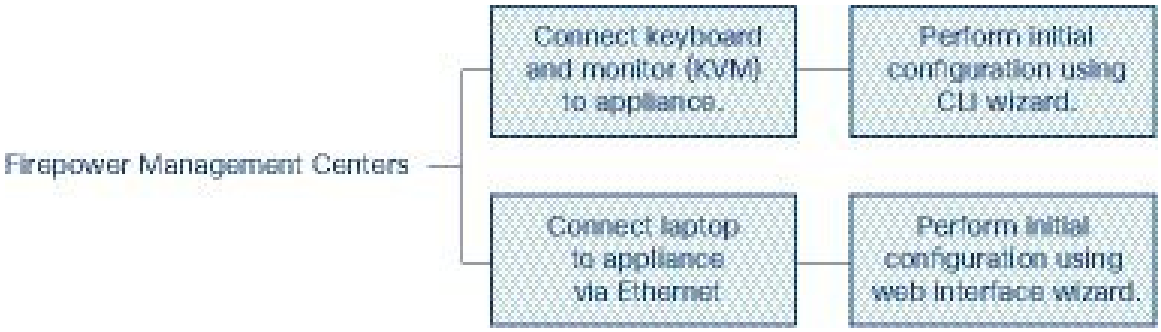
    次に、Web ブラウザを使用して FMC にアクセスし、初期設定プロセスを実行します。「初期設定FMCを実行します（バージョン6.3 - 6.4.x） （8 ページ）」参照してください。
  - 次に、Web ブラウザを使用して FMC にアクセスし、Web インターフェイスを使用して初期設定プロセスを実行して、そのプロセスの一部として eth0 の IP アドレスを設定します。「初期設定FMCを実行します（バージョン6.3 - 6.4.x） （8 ページ）」を参照してください。

FMC で Firepower バージョン 6.5 以降を実行している場合は、次のようになります。

FMC に初めてログインすると、初期設定ウィザードに従って、信頼できる管理ネットワーク上で通信するように新しいアプライアンスを設定できます。このウィザードのバージョンは、Web インターフェイスと CLI アクセスの両方に存在します。合理化された初期設定プロセスを提示し、システムを最新の状態に保ち、データをバックアップするために、毎週のメンテナンス作業が自動的に設定されます。

この初期設定ウィザードを実行するために FMC にアクセスする際は、アプライアンスに直接接続されたラップトップを使用することも、信頼できるローカル管理ネットワークを介したイーサネット接続を使用することもできます。次の図に、Firepower バージョン 6.5 以降を実行している FMC の設定時に選択可能な選択肢を示します。

図 *2 : FMC* セットアップワークフロー、バージョン *6.5* 以降



バージョン 6.5 以降を実行している FMC をインストールおよび設定するための手順

- 「アプライアンスの設置 （4 ページ）」の説明に従って、アプライアンスを設置します。
- FMC は DHCP によって割り当てられた IP4 アドレスが受け入れるように事前に設定されています。初期設定プロセス中にこれを変更でき、次の 2 つの選択肢があります。
  - CLI を使用して初期設定を実行するには、VGA/キーボード接続を使用して FMC にアクセスします。「CLI（バージョン 6.5 以降）を使用した初期設定 （16 ページ）」を参照してください。
  - Web ブラウザを使用して FMC にアクセスし、Web インターフェイスを使用して初期設定プロセスを実行します。「Web インターフェイスを使用した初期設定（バージョン 6.5 以降） （13 ページ）」を参照してください。

CLI または Linux シェルへのアクセス FMC

FMC CLI または Linux シェルにアクセスするには、FMC で実行している Firepower のバージョンに応じて、異なる手順が必要になります。

⚠

注意 Cisco TAC またはユーザ マニュアルの明示的な手順による指示がない限り、Linux シェルを使用しないことを強くお勧めします。

始める前に

キーボードとモニタを使用して FMC との物理的な直接接続を確立するか、FMC の管理インターフェイスとの SSH セッションを確立します。

手順

ステップ 1 CLI の **admin** ユーザのログイン情報を使用して FMC にログインします。

ステップ 2 使用している Firepower のバージョンに応じて、次に行う操作を決定します。

- FMC で Firepower バージョン 6.3.x または 6.4.x を実行しており、FMC CLI が有効になっていない場合、このステップにより、Linux シェルに直接アクセスできます。
- FMC で Firepower バージョン 6.3.x または 6.4.x を実行しており、FMC CLI が有効になっている場合、このステップにより、FMC CLI にアクセスできます。 Linux シェルにアクセスするには、ステップ 3 に進みます。
- FMC で Firepower バージョン 6.5 以降を実行している場合、このステップにより、FMC CLI にアクセスできます。Linux シェルにアクセスするには、ステップ 3 に進みます。

ステップ 3 FMC CLI から Linux シェルにアクセスするには、**expert** コマンドを入力します。

アプライアンスの設置

この手順は、FMC 1600、2600 および 4600 の背面パネルポートに関するものです。

AC 電源装置は内部アースがあるため、サポート対象の AC 電源コードを使用する場合は、それ以上シャーシのアース接続は必要ありません。対応するパワーコードの詳細については、『Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide』を参照してください。

始める前に

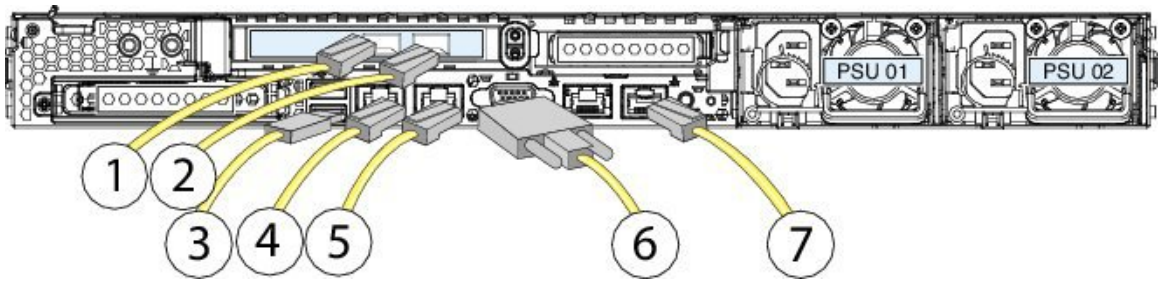
重要 FMC をインストールする前に、必ず『Regulatory Compliance and Safety Information』のドキュメントをお読みください。

- 『Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Intallation Guide』に記載されているようにアプライアンスをラックに設置します。
- 次のネットワーク設定を使用して、ローカル コンピュータを設定します。
  - IP アドレス：192.168.45.2
  - ネットマスク：255.255.255.0
  - デフォルト ゲートウェイ：192.168.45.1

  このコンピュータの他のネットワーク接続をすべて無効にします。

シャーシをラックに取り付けたら、次の手順に従ってケーブルの接続、電源の投入、接続の確認を行います。背面パネルのポートを識別するには、次の図を使用します。

図 *3 :* ケーブル接続



1	eth2 管理インターフェイス 10 ギガビット イーサネット SFP+ をサポート FMC 用に認定されている SFP+s（SFP-10G SR および SFP-10G-LR）のみがサポートされています。	**2**	eth3 管理インターフェイス 10 ギガビット イーサネット SFP+ をサポート FMC 用に認定されている SFP+s（SFP-10G SR および SFP-10G-LR）のみがサポートされています。
3	USB 3.0 タイプ A ポート X 2 キーボードを接続して、VGA ポートのモニタとともに、コンソールにアクセスすることができます。	**4**	eth0 管理インターフェイス（名前 1） ギガビット イーサネット 100/1000/10000 Mbps インターフェイス、RJ-45 eth0 はデフォルトの管理インターフェイスです。
5	eth1 管理インターフェイス（名前 2） ギガビット イーサネット 100/1000/10000 Mbps インターフェイス、RJ-45	**6**	VGA ビデオ ポート（DB-15 コネクタ） このポートはデフォルトで無効です。代わりに、VGA ポートとキーボード USB ポートを使用します。
7	シリアル コンソール ポート コンソール ケーブル（RJ45 から DB9）を使用して、コンピュータを FMC に接続します。		

手順

ステップ 1 （オプション）VGA ポートおよび USB ポート（ケーブル接続図の項目 3 および 6）：モニタを VGA ポートに、キーボードを USB ポートに接続します。

この設定を使用して、ご使用のバージョンに適した方法を使用して、CLI で初期設定を行うことができます。

- CLI（バージョン 6.5 以降）を使用した初期設定 （16 ページ）。
- キーボードとモニタによる FMC へのアクセス（バージョン 6.3 - 6.4.x） （7 ページ）。

または、eth0 でHTTPS を使用して初期設定を完了することができます（ステップ 2 を参照）。

ステップ 2 eth0 管理インターフェイス（背面パネルの「1」というラベルが付いたケーブル接続図の項目 4）：イーサネットケーブルを使用して、管理 PC から到達可能なデフォルトの管理ネットワークに eth0 インターフェイスを接続します。このインターフェイスはデフォルトの管理インターフェイスで、デフォルトで有効になっています。ネットワーク インターフェイス（ローカルコンピュータ上）と FMC 管理インターフェイスの両方のリンク LED が点灯していることを確認してください。

この設定を使用して、ご使用のバージョンに適した方法を使用して、HTTPS で初期設定を行うことができます。

- Web インターフェイスを使用した初期設定（バージョン 6.5 以降） （13 ページ）。
- 初期設定FMCを実行します（バージョン6.3 - 6.4.x） （8 ページ）。

この接続を使用して、ルーチン管理を実行したり、 FMC web インターフェイスからデバイスを管理したりすることもできます。

ステップ 3 （オプション）eth1 管理インターフェイス（ケーブル接続図の項目 5）：ネットワークの必要性に応じて、この管理インターフェイスをその他の管理インターフェイスと同じ、または異なるネットワークに接続します。管理インターフェイスおよびネットワークのトポロジの詳細については、ご使用のバージョンの『Firepower Management Center Configuration Guide』を参照してください。

ステップ 4 （オプション）eth2 および eth3 管理インターフェース（ケーブル接続図の項目 1 および）：ご使用のモデルに 10 ギガビットイーサネット SFP+インターフェースが含まれている場合、必要に応じて FMC 対応の SFP+ トランシーバおよびケーブルを取り付けます。ネットワークの必要に応じて、このインターフェイスをその他の管理インターフェイスと同じまたは異なるネットワークに接続します。管理インターフェイスおよびネットワークのトポロジの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

FMC 対応の各 SFP+ トランシーバ（SFP-10G-SR および SFP-10G-LR）には、セキュリティ情報が符号化された内部シリアル EEPROM が組み込まれています。このエンコーディングによって、SFP トランシーバが FMC シャーシの要件を満たしていることを識別して検証できます。

（注） FMC 対応の SFP+ トランシーバのみ、10-G インターフェイスと互換性があります。Cisco TAC は、テストされていないサードパーティ製の SFP トランシーバを使用したことに起因する相互運用性の問題についてはサポートを拒否することがあります。

ステップ 5 電源：サポート対象の電源コードの 1 つを使用して、シャーシの電源装置を電源に接続します。対応するパワーコードの詳細については、『Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide』を参照してください。

ステップ 6 確認：シャーシの前面にある電源ボタンを押し、電源ステータス LED がオンになっていることを確認します。

次のタスク

- FMC が Firepower バージョン 6.3x - 6.4.x を使用している場合、FMC をネットワークに接続する前に、ネットワークに合わせて FMC の eth0 IP アドレスを変更し、初期セットアップを実行する必要があります。次の 2 つの選択肢があります。
  - 初期設定を実行する前に、VGA/キーボード接続を使用して FMC にアクセスし、eth0 の IP アドレスを設定します。「キーボードとモニタによる FMC へのアクセス（バージョン 6.3 - 6.4.x） （7 ページ）」を参照してください。
  - 初期設定プロセスに直接進み、eth0 IP アドレスをそのプロセスの一部として設定します。初期設定FMCを実行します（バージョン6.3 - 6.4.x） （8 ページ） を参照してください。
- FMC が Firepower バージョン 6.5+ を使用している場合は、DHCP によって割り当てられた IP4 アドレスを受け入れるように事前に設定されています。初期設定プロセス中にこれを変更でき、次の 2 つの選択肢があります。
  - CLI を使用して初期設定を実行するには、VGA/キーボード接続を使用して FMC にアクセスします。「CLI（バージョン 6.5 以降）を使用した初期設定 （16 ページ）」を参照してください。
  - Web ブラウザを使用して FMC にアクセスし、Web インターフェイスを使用して初期設定プロセスを実行します。「Web インターフェイスを使用した初期設定（バージョン 6.5 以降） （13 ページ）」を参照してください。

キーボードとモニタによる FMC へのアクセス（バージョン 6.3 - 6.4.x）

アプライアンスに USB キーボードと VGA モニタを接続できます。これはキーボード、ビデオ、マウスの（KVM）スイッチに接続しているラックマウント型アプライアンスで便利です。

このタスクを実行する際は、物理インターフェイスの図を参照して背面パネルのポートを識別してください。

手順

ステップ 1 付属のイーサネットケーブルを使用して、シャーシの背面にある管理インターフェイス（eth0）を保護された管理ネットワークに接続します。

ステップ 2 モニタを VGA ポートに、キーボードをシャーシ背面の USB ポートの 1 つに接続します。

ステップ 3 ユーザ名として **admin** を、パスワードとして **Admin123** を使用して、FMC 上の Linux シェルにアクセスします（パスワードでは大文字と小文字が区別されます）。お使いの Firepower バージョンに適した手順を使用します。「CLI または Linux シェルへのアクセス FMC （3 ページ）」を参照してください。

ステップ 4 次のスクリプトを実行して、FMC のネットワーク設定を指定します。

```
sudo /usr/local/sf/bin/configure-network
```

ステップ 5 アプライアンスに IPv4 および IPv6（オプション）の設定情報を提供するためにプロンプトに応答します。

ステップ 6 最後のプロンプトで設定を確認することができます。

```
Are these settings correct: (y or n)?
```

入力した設定を確認してください。

- 設定が正しい場合は、**y** を入力して **Enter** を押し、設定を承認して続行します。
- 設定が間違っている場合は、 **n** を入力し **Enter** を押します。情報を再度入力するように求められます。

ステップ 7 設定を承認した後、**exit** と入力してシェルからログアウトします。

次のタスク

初期設定FMCを実行します（バージョン6.3 - 6.4.x） （8 ページ）の説明に従ってセットアップ プロセスを完了します。

初期設定FMCを実行します（バージョン6.3 - 6.4.x）

すべての FMC に対して、FMC の Web インターフェイスにログインして、セットアップページで初期設定オプションを選択することによって、セットアッププロセスを完了する必要があります。少なくとも、管理者のパスワード変更と、ネットワーク設定の指定をまだ行っていない場合はこれらの 2 つを実行し、EULA に同意する必要があります。

手順

ステップ 1 ブラウザで https://*mgmt_ip*/ にアクセスします。ここで、*mgmt_ip* は FMC の管理インターフェイスの IP アドレスです。

- イーサネット ケーブルを使用してコンピュータに接続された FMC の場合は、そのコンピュータ上のブラウザでデフォルトの管理インターフェイスの IPv4 アドレス（https://192.168.45.45/）にアクセスします。
- ネットワーク設定がすでに完了している FMC の場合は、管理ネットワーク上のコンピュータを使用して、その FMC の管理インターフェイスの IP アドレスを参照します。

ステップ 2 ユーザ名として **admin** を、パスワードとして **Admin123** を使用してログインします。

ステップ 3 [セットアップ（Setup）] ページの [パスワードの変更（Change Password）] セクションで、管理者アカウントのパスワードを変更します。Web インターフェイスの admin アカウントには管理者権限があり、アカウントを削除することはできません。大文字と小文字が混在する 8 文字以上の英数字で、1 つ以上の数字を含む強力なパスワードを使用することをお勧めします。辞書に掲載されている単語の使用は避けてください。

（注） シェルによる FMC へのアクセスと Web インターフェイスによる FMC へのアクセスのための admin アカウントは同じではないため、異なるパスワードを使用できます。この設定により、両方の管理者パスワードが同じ値に変更されます。

ステップ 4 FMC のネットワーク設定によって、管理ネットワーク上で通信できるようになります。[セットアップ（Setup）] ページの [ネットワーク設定（Network Settings）] セクションでこれらの設定を構成します。

- キーボードとモニタを使用してアプライアンスにアクセスするためのネットワーク設定がすでに完了している場合は、[セットアップ（Setup）]ページの[ネットワーク設定（Network Settings）] セクションが事前に入力されている可能性があります。
- [ネットワーク設定（Network Settings）] の値が事前に入力されていない場合、または事前に入力された値を変更する場合は、管理ネットワークプロトコルを選択する必要があります。Firepower システムは、IPv4 と IPv6 の両方の管理環境にデュアル スタック実装を提供します。IPv4、IPv6、または両方を指定できます。

  プロトコルの選択に応じて[セットアップ（Setup）]ページにフィールドが表示されます。ここで FMC の IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィックスの長さ、およびデフォルトのゲートウェイを入力する必要があります。また、デバイスに対してホスト名とドメインの他に、3 つまでの DNS サーバを指定することもできます。

  - IPv4 の場合は、アドレスとネットマスクをドット付き 10 進法の形式（255.255.0.0 のネットマスクなど）で入力する必要があります。
  - IPv6 ネットワークの場合は、[ルータ自動設定を使用してIPv6アドレスを割り当てる（Assign the IPv6 address using router autoconfiguration）] チェックボックスをオンにして IPv6 のネットワーク設定を自動的に割り当てます。このチェックボックスをオンにしない場合は、コロンで区切った 16 進形式のアドレスと、プレフィックスのビット数を設定する必要があります（プレフィックスの長さ 112 など）。

ステップ 5 （任意）[セットアップ（Setup）] ページの [時刻設定（Time Settings）] セクションで、2つの方法（手動または NTP サーバからの Network Time Protocol（NTP）を使用）のいずれかで FMC の時間を設定できます。

- Network Time Protocol（NTP）を使用して時間を設定するには、[次から NTP で（Via NTP from）] をオンにして、FMC がアクセスできる NTP サーバを指定します。
- 手動で時間を設定するには、[手動（Manually）] をオンにして、表示されているフィールドに現在の時間を入力します。

ローカル Web インターフェイスで admin アカウントに対して使用されるタイム ゾーンを選択し、現在のタイム ゾーンをクリックして、ポップアップ ウィンドウからタイム ゾーンを選択します。

（注） FMC とその管理対象デバイスの間で適切な時間同期を維持するために、ネットワークで NTP サーバを使用することをお勧めします。詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「Time and Time Synchronization」のセクションを参照してください。

ステップ 6 （任意）展開で侵入検知および防御を実行するよう計画している場合、[セットアップ（Setup）] ページの [定期的なルール更新のインポート（Recurring Rule Update Imports）] セクションで [サポート サイトからのルール更新の定期インポートを有効にする] チェックボックスをオンにすることをお勧めします。

それぞれのルール更新の後で、システムが侵入についての [ポリシーの展開（Policy Deploy）] を実行するよう設定するだけでなく、[インポート頻度（Import Frequency）] も指定することができます。初期設定プロセスの一部としてルールの更新を実行するには、[今すぐインストール（Install Now）] チェックボックスをオンにします。

新しい脆弱性が発見されると、脆弱性調査チーム（VRT）は侵入ルールの更新をリリースします。ルールの更新では、新規および更新された侵入ルールおよびプリプロセッサルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が提供されます。ルールの更新では、ルールを削除して、新しいルール カテゴリおよびシステム変数を提供する場合もあります。

ルールの更新には、新しいバイナリが含まれている場合があります。ルール更新のダウンロードおよびインストールのプロセスが、自身のセキュリティ ポリシーに適合していることを確認します。加えて、ルール更新のサイズが大きい場合があるため、ネットワーク使用率の低い時間帯にルールをインポートするようにしてください。

ステップ 7 （任意）展開で位置情報関連の分析を実行する予定の場合、[セットアップ（Setup）]ページの [定期的な位置情報の更新（Recurring Geolocation Updates）] セクションで [サポート サイトからの定期的な週次更新を有効にする（Enable Recurring Weekly Updates from the Support Site）] をオンにして、表示されるフィールドを使用して [開始時間の更新（Update Start Time）] を指定することをお勧めします。初期設定プロセスの一部として GeoDB の更新を実行するには、[今すぐインストール（Install Now）] チェックボックスをオンにします。

GeoDB の更新はサイズが大きくなることがあるため、ダウンロードの後のインストールに最大で 45 分かかることがあります。GeoDB は、ネットワークの使用量が少ないときに更新してください。

ほとんどの FMC を使用して、ダッシュボードおよび Context Explorer の地理情報統計を監視するだけでなく、システムで生成されたイベントに関連付けられているルーテッド IP アドレスの地理情報を表示することができます。FMC の地理情報データベース（GeoDB）には、この機能をサポートするための情報（IP アドレスに関連する ISP、接続タイプ、プロキシ情報、正確な位置情報など）が含まれています。定期的な GeoDB の更新を有効にすることで、システムが常に最新の地理情報を使用するようにすることができます。

ステップ 8 （任意）[セットアップ（Setup）] ページの [自動バックアップ（Automatic Backups）] セクションで、[自動バックアップを有効にする（Enable Automatic Backups）] をオンにして、失敗した場合に復元できる FMC の設定の週次バックアップを作成するスケジュール タスクを作成できます。

ステップ 9 FMC を使用して、管理対象のデバイスのライセンスを管理します。Firepower システムで提供されるライセンス タイプは、管理するデバイスのタイプによって異なります。

- 7000 および 8000 シリーズ、ASA with FirePOWER Services、および NGIPSv デバイスの場合は、従来のライセンスを使用する必要があります。従来のライセンスを使用するデバイスは、クラシック デバイスと呼ばれることもあります。

ライセンス付与された機能を使用する前に管理対象デバイスのクラシック ライセンスを有効にする必要があります。FMCの初期セットアップ中、FMCにデバイスを追加するとき、またはデバイスの追加後デバイスの一般的なプロパティを編集するときに、ライセンスを有効にすることができます。

FMC の初期セットアップ時にクラシック ライセンスを有効にするには、初期セットアップ時のクラシックライセンスの設定（バージョン6.3 - 6.4.x） （12 ページ）の手順に従ってください。

- FTD の物理デバイスと仮想デバイスの場合、スマート ライセンスを使用する必要があります。

  Cisco スマート ソフトウェア ライセンシングを使用するデバイスを管理する予定の場合、FMCにスマートライセンスを追加する方法の詳細については、そのデバイスの製品マニュアルを参照してください。

『Firepower Management Center コンフィギュレーション ガイド』は、クラシック ライセンスおよびスマート ライセンス、各クラスのライセンス タイプ、および展開全体でのライセンスの管理方法についての情報を提供します。

ステップ 10 **エンドユーザライセンス契約**をよくお読みください。条件を遵守することに同意する場合は、[エンドユーザライセンス契約を読んだうえで同意する（I have read and agree to the End User License Agreement）] チェックボックスをオンにします。

ステップ 11 指定した情報がすべて正しいことを確認して、[適用（Apply）] をクリックします。

FMC は、選択の内容に従って設定を適用してサマリ ダッシュボード ページを表示し、admin ユーザ（管理者ロールがあります）として Web インターフェイスにログインします。

（注） ネットワーク環境で NAT が使用されていると、ブラウザでの、初期セットアップ ページで設定されているアドレスによる FMC への到達の試みがタイムアウトする場合があります。この場合は、ブラウザのアドレス ウィンドウに正しいアドレスを入力して、再試行してください。

ステップ 12 イーサネット ケーブルを使用してアプライアンスの管理インターフェイスに直接接続している場合は、コンピュータの接続を切断して、FMC の管理インターフェイスを管理ネットワークに接続します。このガイドの残りの手順を完了するには、管理ネットワーク上のコンピュータのブラウザを使用して、先ほど設定した IP アドレスまたはホスト名で FMC GUI にアクセスします。

ステップ 13 Message Center の [タスク（Tasks）] タブのステータスをモニタすることによって、初期セットアップが成功したことを確認します。

次のタスク

- 必要に応じて、シリアル アクセスまたは Lights-Out Management（LOM）アクセス用に FMC を設定します。Firepower Management Center の代替アクセスのセットアップを参照してください。

- Firepower Management Center 初期管理および設定で説明されているアクティビティを実行します。

初期セットアップ時のクラシックライセンスの設定（バージョン6.3 - 6.4.x）

FMC を使用して 7000 および 8000 シリーズ、ASA with FirePOWER Services、および NGIPSvのクラシック ライセンスを管理します。

（注） ライセンス付与された機能を使用する前に管理対象デバイスのクラシック ライセンスを有効にする必要があります。FMC の初期セットアップ時の、FMC にデバイスを追加するとき、またはデバイスを追加した後にデバイスの一般的なプロパティを編集するときに、ライセンスを有効にすることができます（以下の手順を使用します）。

始める前に

クラシック ライセンスを FMC に追加する前に、ライセンスの購入時にシスコから製品認証キー（PAK）が提供されていることを確認してください。レガシーの、以前のシスコのライセンスの場合は、Cisco TAC に問い合わせてください。

手順

ステップ 1 初期セットアップ ページの [ライセンス設定（License Settings）] セクションから、シャーシのライセンス キーを取得します。

ライセンス キーは明確にラベル付けされます（たとえば、66:18:E7:6E:D9:93:35）。

ステップ 2 ライセンスを取得するには https://www.cisco.com/go/license/ に移動します。そこで、ライセンス キー（たとえば、66:18:E7:6E:D9:93:35）と PAK の入力が求められます。

（注） 追加のライセンスを発注したら、そのライセンスに対してカンマで区切った PAK を同時に入力することができます。

ステップ 3 画面の指示に従ってライセンスを生成します。ライセンスは電子メールで送信されます。

ステップ 4 検証ボックスのライセンスを貼り付けて、[追加/確認（Add/Verify）] をクリックします。

Web インターフェイスを使用した初期設定（バージョン 6.5 以降）

を展開した後、FMC への HTTPS アクセスがある場合、アプライアンスの FMC Web インターフェイスにアクセスして初期設定ができます。Web インターフェイスに初めてログインすると、FMC で初期設定ウィザードが表示され、アプライアンスの基本設定をすばやく簡単に設定できるようになります。このウィザードは、次の 3 つの画面と 1 つのポップアップ ダイアログ ボックスで構成されています。

- 最初の画面では、**admin** ユーザのパスワードをデフォルト値の **Admin123** から変更するよう求められます。
- 2 番目の画面では、シスコ エンドユーザ ライセンス契約（EULA）が表示されます。アプライアンスを使用するには、この内容に同意する必要があります。
- 3 番目の画面では、アプライアンス管理インターフェイスのネットワーク設定を変更できます。このページには現在の設定があらかじめ入力されており、必要に応じて変更できます。

  工場出荷時の初期状態に復元した後にアプライアンスを設定する場合（Firepower Management Center の工場出荷時の初期状態への復元 を参照）に、アプライアンスのライセンスおよびネットワーク設定を削除しなかった場合、プロンプトには保持されている値が事前に入力されます。
- この画面で入力した値については、ウィザードによる検証が実行されて、次の点が確認されます。
  - 構文の正確性
  - 入力値の互換性（たとえば、IP アドレスやゲートウェイに互換性があるか、また FQDN を使用して NTP サーバが指定されている場合は設定された DNS に互換性があるか）
  - FMC と DNS サーバおよび NTP サーバとの間のネットワーク接続

  これらのテストの結果はリアルタイムで画面上に表示されます。したがって、必要な修正を行い、設定の妥当性をテストしてから、画面の下部にある [終了（Finish）] をクリックできます。NTP および DNS 接続テストは非ブロッキングです。ウィザードが接続テストを完了する前に [終了（Finish）] をクリックすることもできます。[終了（Finish）] をクリックした後に接続の問題が見つかった場合は、このウィザードで設定を変更することはできませんが、初期設定の完了後に Web インターフェイスを使用してその接続を設定できます。

  FMC とブラウザとの間の既存の接続を切断することになる設定値を入力した場合、接続テストは実行されません。この場合、DNS または NTP の接続ステータス情報はウィザードに表示されません。
- 3 つのウィザード画面に続いて、ポップアップ ダイアログ ボックスが表示され、必要に応じてスマートライセンスをすばやく簡単に設定できます。

初期設定ウィザードと [スマートライセンス（Smart Licensing）] ダイアログの終了後、お使いのバージョンの『 Firepower Management Center Configuration Guide』の「Device Management Basics」に記載されているように、デバイス管理ページが表示されます。

始める前に

- アプライアンスの設置 （4 ページ） の説明に従って FMC をインストール
- FMC が管理ネットワーク上で通信するために必要な次の情報があることを確認してください。
  - IPv4 管理 IP アドレス

    FMC 管理インターフェイスは、DHCP によって割り当てられた IP4 アドレスを受け入れるように事前設定されています。DHCP が FMC MAC アドレスに割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP が使用できないシナリオでは、FMC 管理インターフェイスは IPv4 アドレス 192.168.45.45 を使用します。
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）。

手順

ステップ 1 Web ブラウザを使用して、FMC の IP アドレス：*https://<FMC-IP>* に移動します。

ログイン ページが表示されます。

ステップ 2 管理者アカウントのユーザ名に **admin** を、パスワードに **Admin123** を使用して FMC にログインします。（パスワードでは大文字と小文字が区別されます。）

ステップ 3 [パスワードの変更（Change Password）] 画面で、次のようにします。

a) （オプション）この画面の使用中にパスワードが表示されるようにするには、[パスワードの表示（Show password）] チェックボックスをオンにします。

b) （オプション）[パスワードの生成（Generate Password）] ボタンをクリックして、表示されている条件に準拠するパスワードを自動的に作成します。（生成されたパスワードは非ニーモニックです。このオプションを選択する場合は、パスワードをメモてください。）

c) 任意のパスワードを設定するには、[新しいパスワード（New Password）] テキストボックスと [パスワードの確認（Confirm Password）] テキストボックスに新しいパスワードを入力します。

パスワードは、ダイアログに示された条件を満たす必要があります。

（注） FMC では、パスワードをパスワード クラッキング ディクショナリと照合して、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列についてもチェックします。たとえば、「abcdefg」や「passw0rd」などのパスワードは初期設定スクリプトによって拒否される場合があります。

（注） 初期設定プロセスが完了すると、システムは 2 つの **admin** アカウント（1 つは Web アクセス用、もう 1 つは CLI アクセス用）のパスワードを同じ値に設定します。パスワードは、ご使用のバージョンの『Firepower Management Center Configuration Guide』に記載されている強力なパスワード要件に準拠している必要があります。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。

d) [Next] をクリックします。

[パスワードの変更（Change Password）] 画面で [次へ（Next）] をクリックし、**admin** の新しいパスワードが承認されると、残りのウィザードの手順が完了していなくても、Web インターフェイスと CLI の両方の **admin** アカウントでそのパスワードが有効になります。

ステップ 4 [ユーザ契約（User Agreement）] 画面では、EULA を読み、[同意する（Accept）] をクリックし続行します。

[同意しない（Decline）] をクリックすると、FMC からログアウトされます。

ステップ 5 [Next] をクリックします。

ステップ 6 [ネットワークの設定の変更（Change Network Settings）] 画面では次を実行します。

a) **完全修飾ドメイン名**を入力します。デフォルト値が表示されている場合は、デフォルト値を受け入れるか、完全修飾ドメイン名（構文<hostname><domain>）またはホスト名を入力します。

b) **DHCP を使用**するか、または **Static/Manual を使用**して、**[IPV4の設定（Configure IPV4）]** オプションのブートプロトコルを選択します。

c) **IPV4 アドレス**の表示されている値を使用するか（値が表示されている場合）、または新しい値を入力できます。ドット付き 10 進法形式を使用します（192.168.45.45 など）。

d) **ネットワークマスク**の表示されている値を使用するか（値が表示されている場合）、または新しい値を入力できます。ドット付き 10 進法形式を使用します（255.255.0.0 など）。

e) **ゲートウェイ**の表示されている値を使用するか（値が表示されている場合）、または新しいデフォルトゲートウェイを入力できます。 ドット付き 10 進法形式を使用します（192.168.0.1 など）。

f) （オプション）**DNS グループ**の場合は、デフォルト値の **Cisco Umbrella DNS** を使用します。

DNS 設定を変更するには、ドロップダウンリストから [カスタムDNSサーバ（Custom DNS Servers）] を選択し、[プライマリDNS（Primary DNS）] と [セカンダリDNS（Secondary DNS）] の IPv4 アドレスを入力します。ドロップダウンリストから [カスタムDNSサーバ（Custom DNS Servers）] を選択し、[プライマリDNS（Primary DNS）] フィールドと [セカンダリDNS（Secondary DNS）] フィールドを空白のままにして、DNS サーバを設定しません。

g) **NTP グループサーバ**の場合は、デフォルト値の**デフォルト NTP サーバ**を受け入れることができます。この場合は、システムでは **0.sourcefire.pool.ntp.org** がプライマリ NTP サーバとして使用され、**1.sourcefire.pool.ntp.org** がセカンダリ NTP サーバが使用されます。

他の NTP サーバを設定するには、ドロップダウンリストから [Custom NTP グループサーバ（Custom NTP Group Servers）] を選択し、ネットワークから到達可能な 1 台または 2 台の NTP サーバの FQDN または IP アドレスを入力します。

ステップ 7 [終了（Finish）] をクリックします。

ウィザードは、この画面で入力した値の検証を実行して、構文の正確性、入力した値の互換性、FMC と DNS および NTP サーバ間のネットワーク接続を確認します。[終了（Finish）] をクリックした後に接続の問題が見つかった場合は、このウィザードで設定を変更することはできませんが、初期設定の完了後に FMC Web インターフェイスを使用してその接続を設定できます。

次のタスク

- 新しく復元された FMC で初期設定を実行し、復元中にネットワーク設定を保持することを選択しましたが、初期設定時にネットワーク設定を変更した場合は、新しいネットワーク情報を使用して FMC に再接続する必要があります。
- システムには、スマートライセンシングを迅速かつ簡単にセットアップするための機会を提供するポップアップ ダイアログ ボックスが表示されます。このダイアログの使用は任意です。スマートライセンスについて十分な知識があり、FMC で Firepower Threat Defense デバイスを管理する場合は、このダイアログを使用してください。それ以外の場合は、このダイアログを閉じて、お使いのバージョンの『Firepower Management Center Configuration Guide』の「Licensing the Firepower System」を参照してください。
- FMC では、システムを最新の状態に維持し、データをバックアップするための週次メンテナンス作業が正常に設定されたことを確認します。自動初期設定（バージョン 6.5 以降）（20 ページ）を参照してください。
- 初期設定ウィザードと [スマートライセンス（Smart Licensing）] ダイアログの終了後、『*Firepower Management Center Configuration Guide*』の「Device Management Basics」に記載されているように、デバイス管理ページが表示されます。Firepower Management Center 初期管理および設定 の説明に従って FMC の基本設定を設立します。使用しているバージョンの『Firepower Management Center Configuration Guide』で説明されているように、Web インターフェイスを使用して初期設定を完了した後で、IPv6 アドレッシング用に FMC を設定できます。
- Firepower Management Center の代替アクセスのセットアップ で説明されているように、シリアルまたはシリアル経由の Lights-Out-Management アクセス用に FMC を任意で設定できます。

CLI（バージョン 6.5 以降）を使用した初期設定

このタスクを使用して、コンソールアクセス用の USB キーボードおよび VGA モニタに接続された FMC の初期設定を実行できます。初期構成ウィザードを完了させ、信頼できる管理ネッ

トワークで通信するように新しいアプライアンスを設定する必要があります。ウィザードでは、エンドユーザーライセンス契約（EULA）に同意し、管理者パスワードを変更する必要があります。

始める前に

- アプライアンスの設置 （4 ページ） の説明に従って FMC をインストール
- FMC が管理ネットワーク上で通信するために必要な次の情報があることを確認してください。
  - IPv4 管理 IP アドレス

    FMC 管理インターフェイスは、DHCP によって割り当てられた IP4 アドレスを受け入れるように事前設定されています。DHCP が FMC MAC アドレスに割り当てるように設定されている IP アドレスを確認するには、システム管理者に問い合わせてください。DHCP が使用できないシナリオでは、 FMC 管理インターフェイスは IPv4 アドレス 192.168.45.45 を使用します。
  - ネットワークマスクとデフォルトゲートウェイ（DHCP を使用しない場合）。

手順

ステップ 1 **admin** アカウントのユーザ名に **admin** を、パスワードに **Admin123** を使用しコンソールで FMC にログインします。パスワードでは、大文字と小文字が区別されることに注意してください。

ステップ 2 プロンプトが表示されたら、**enter**キーを押してエンドユーザライセンス契約（EULA）を表示します。

ステップ 3 EULA を確認します。プロンプトが表示されたら、**yes**、**YES** を入力し、**Enter** キーを押して EULA に同意します。

重要 EULA に同意せずに続行することはできません。**[はい（yes）]**、**[はい（YES）]**、または **[入力（Enter）]** 以外のもので応答すると、システムはユーザをログアウトします。

ステップ 4 システムのセキュリティやプライバシーを確保するために、FMC に初めてログインするときは、**admin** のパスワードを変更する必要があります。システムが新しいパスワードの入力を求めるプロンプトが表示されたら、表示された制限に従って新しいパスワードを入力し、確認のプロンプトが表示されたら同じパスワードを再度入力します。

（注） FMC では、パスワードをパスワード クラッキング ディクショナリと照合して、英語の辞書に載っている多くの単語だけでなく、一般的なパスワードハッキング技術で簡単に解読できるその他の文字列についてもチェックします。たとえば、「abcdefg」や「passw0rd」などのパスワードは初期設定スクリプトによって拒否される場合があります。

（注） 初期設定プロセスの完了時に、2 つの **admin** アカウント（Web アクセス用と CLI アクセス用）のパスワードは同じ値に設定されます。これは、お使いのバージョンの『*Firepower Management Center Configuration Guide*』に記載されている強力なパスワードの要件に準拠しています。その後、いずれかの **admin** アカウントのパスワードを変更すると、パスワードは同じではなくなり、Web インターフェイスの **admin** アカウントから強力なパスワード要件を削除できます。

ステップ 5 プロンプトに応答して、ネットワーク設定を行います。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が **(y/n)** のように括弧で囲まれて示されます。デフォルト値は、**[y]** のように大カッコ内に列挙されます。プロンプトに応答する場合は、次の点に注意してください。

- 工場出荷時の初期状態に復元した後にアプライアンスを設定Firepower Management Centerの工場出荷時の初期状態への復元する場合(を参照)、アプライアンスのライセンスおよびネットワーク設定を削除しなかった場合、プロンプトには保持されている値が事前に入力されます。
- Enter キーを押して、デフォルトを受け入れます。
- ホスト名に関しては、完全修飾ドメイン名（<hostname>.<domain>）またはホスト名を入力します。このフィールドは必須です。
- IPv4 を手動で設定することを選択した場合、システムは IPv4 アドレス、ネットマスク、およびデフォルトゲートウェイの入力を求めます。[DHCP] を選択した場合、システムは DHCP を使用してこれらの値を割り当てます。DHCP を使用しない場合は、これらのフィールドの値を指定する必要があります。標準のドット付き 10 進表記を使用します。
- DNS サーバの設定は任意です。DNS サーバを指定しない場合は [なし（none）] を入力します。それ以外の場合は、1 つまたは 2 つの DNS サーバに IPv4 アドレスを指定します。2 つのアドレスを指定する場合は、カンマで区切ります。
- ネットワークから到達可能な少なくとも 1 つの NTP サーバの完全修飾ドメイン名または IP アドレスを入力する必要があります。2 つのサーバ（プライマリとセカンダリ）を指定できます。情報はカンマで区切ります。

例：

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]:
208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org,
1.sourcefire.pool.ntp.org]:
```

ステップ 6 システムによって、設定の選択内容の概要が表示されます。入力した設定を確認してください。

例：

```
Hostname:                               fmc
IPv4 configured via:                    manual configuration
Management interface IPv4 address:     10.10.0.66
Management interface IPv4 netmask:      255.255.255.224
Management interface IPv4 gateway:      10.10.0.65
DNS servers:                            208.67.222.222,208.67.220.220
NTP servers:                           0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

ステップ 7 最後のプロンプトで設定を確認することができます。

- 設定が正しい場合は、**y** を入力して **Enter** を押し、設定を承認して続行します。
- 設定が間違っている場合は、**n** を入力し **Enter** を押します。システムは、ホスト名で始まる情報を再入力するようにプロンプトします。

例：

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

ステップ 8 設定を承認したら、**exit** と入力して FMC CLI を終了します。

次のタスク

- 新しく復元された FMC で初期設定を実行し、復元中にネットワーク設定を保持することを選択しましたが、初期設定時にネットワーク設定を変更した場合は、新しいネットワーク情報を使用して FMC に再接続する必要があります。
- FMC では、システムを最新の状態に維持し、データをバックアップするための週次メンテナンス作業が正常に設定されたことを確認します。自動初期設定（バージョン6.5以降）（20 ページ）を参照してください。
- 初期設定ウィザードと [スマートライセンス（Smart Licensing）] ダイアログの終了後、お使いのバージョンの『*Firepower Management Center Configuration Guide*』の「Device Management Basics」に記載されているように、デバイス管理ページが表示されます。Firepower Management Center 初期管理および設定 の説明に従って FMC の基本設定を設立します。使用しているバージョンの『*Firepower Management Center Configuration Guide*』で説明されているように、web インターフェイスを使用して初期設定を完了した後で、IPv6 アドレッシング用に FMC を設定できます。
- Firepower Management Center の代替アクセスのセットアップ で説明されているように、シリアルまたはシリアル経由の Lights-Out-Management アクセス用に FMC を任意で設定できます。

自動初期設定（バージョン 6.5 以降）

初期設定時（初期設定ウィザードまたはCLIを使用して実行されたとしても）は、FMCによって、データをバックアップするための毎週のメンテナンスタスクが自動的に設定され、システムが最新の状態に保たれます。

タスクはUTCでスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクはUTCでスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも1時間「遅れて」実行されることになります。

（注） 自動スケジュール設定を確認し、必要に応じて調整することを強くお勧めします。

- GeoDB の更新

  FMC では、毎週、ランダムに選択された時刻に行われるように、GeoDB の更新を自動的にスケジュールします。Web インターフェイスのメッセージ センターを使用して、この更新のステータスを確認できます。システムが更新プログラムを設定できず、FMC からインターネットに接続できる場合は、ご使用のバージョンの『Firepower Management Center Configuration Guide』で説明されているように、通常の GeoDB を設定することをお勧めします。

- FMC Software Updates

  FMC では、FMC およびその管理対象デバイスの最新ソフトウェアをダウンロードするための週次タスクを自動的にスケジュールします。 このタスクは、UTC で日曜日の午前 2 ～ 3 時の間に行われるようにスケジュールされます。したがって、日付と場所に応じて、現地時間では、土曜日の午後から日曜日の午後の範囲内のいずれかの時間帯に行われることになります。Web インターフェイスのメッセージ センターを使用して、このタスクのステータスを確認できます。FMCからインターネットにアクセスできるにもかかわらず、自動的にスケジュールされたタスクが失敗する場合は、お使いのバージョンの『Firepower Management Center Configuration Guide』の説明に従って、ソフトウェアの更新をダウンロードする定期タスクをスケジュールすることをお勧めします。

  このタスクでは、アプライアンスで現在実行されているバージョンに対するソフトウェアパッチおよびホットフィックスをダウンロードするだけです。このタスクでダウンロードされた更新プログラムのインストールは、別に行う必要があります。詳細については、『*Cisco Firepower Management Center Upgrade Guide*』を参照してください。

- 週次の FMC 設定バックアップ

  FMC では、ローカルに保存された設定のみのバックアップを実行するための週次タスクを自動的にスケジュールします。このタスクは、UTC で月曜日の午前2時に行われるようにスケジュールされます。したがって、日付と場所に応じて、現地時間では、日曜日の午後から月曜日の午後の範囲内のいずれかの時間帯に行われることになります。Web イン

ターフェイスのメッセージ センターを使用して、このタスクのステータスを確認できます。自動的にスケジュールされたタスクが失敗する場合は、お使いのバージョンの『Firepower Management Center Configuration Guide』の説明に従って、バックアップを実行する定期タスクをスケジュールすることをお勧めします。