従来型デバイス用のプラットフォーム設定

次のトピックでは、Firepower プラットフォーム設定について、および従来型デバイスでそれを設定する方法について説明します。

従来型デバイス用のプラットフォーム設定について

管理対象デバイスのプラットフォーム設定はポリシーベースであるため、複数のデバイスに同じ設定を適用できます。次の従来型デバイスでは *Firepower* プラットフォーム設定ポリシーを使用します。

- 7000/8000 シリーズ デバイス
- ASA FirePOWER モジュール
- NGIPSv

FMC の場合、これらの設定の多くはシステム設定で処理されることに注意してください。システム設定（System Configuration）を参照してください。

表 *1*：従来型デバイス用の *Firepower* プラットフォーム設定

プラットフォーム設定	説明	参照先
アクセス リスト（Access List）	どのコンピュータが特定のポートでシステムにアクセスできるかを制御します。	従来型デバイス用のアクセス リストの設定 （4 ページ）
監査ログ（Audit Log）	外部ホストに監査ログを送信するようにシステムを設定します。	従来型デバイスからの監査ログのストリーミング （4 ページ）

プラットフォーム設定	説明	参照先
監査ログ証明書	監査ログのセキュアなストリーミングの一部として、従来型デバイスと監査ログ サーバ間の相互認証が必要です。	従来型デバイス用の有効な監査ログ サーバ証明書の要求 （6 ページ）
外部認証	外部 RADIUS、LDAP、または Microsoft Active Directory のリポジトリによって認証される 7000/8000 シリーズ デバイス ユーザのデフォルト ユーザ ロールを設定します。	7000/8000 シリーズ デバイスへの外部認証の有効化 （8 ページ）
[言語（Language）]	7000/8000 シリーズ デバイスの Web インターフェイスに別の言語を指定します。	7000/8000 シリーズ Web インターフェイスの言語の設定 （10 ページ）
ログイン バナー	ユーザがログインすると表示されるカスタム ログイン バナーを作成します。	従来型デバイス用のログイン バナーのカスタマイズ （10 ページ）
シェル タイムアウト	ユーザのログイン セッションが非アクティブになったためにタイムアウトするまでのアイドル時間の長さを分単位で設定します。	従来型デバイスのセッション タイムアウトの設定 （12 ページ）
SNMP	Simple Network Management Protocol （SNMP）のポーリングを有効にします。	従来型デバイスでの SNMP ポーリングの設定 （12 ページ）
時刻の同期	システムの時刻の同期を管理します。	従来型デバイスの時刻を NTP サーバに同期 （11 ページ）
UCAPL/CC コンプライアンス	米国国防総省によって設定される特定の要件の順守を有効にします。	セキュリティ認定コンプライアンスの有効化

従来型デバイス用のプラットフォーム設定の要件

ライセンス要件

なし。

モデルの要件

Firepower プラットフォーム設定ポリシーを従来型デバイスに適用できます。

一部のプラットフォーム設定は、7000/8000 シリーズ デバイスのみに適用されます。これらのデバイスには、外部認証設定、表示言語、セッション タイムアウトなどの Web インターフェイスがあるためです。これらの設定を ASA FirePOWER または NGIPSv に適用しても効果はありません。

7000/8000 シリーズ デバイスのローカル Web インターフェイスにログインして、非ポリシーベースのシステム設定を行うこともできます。7000/8000 シリーズ デバイスのローカル システム設定 （14 ページ）を参照してください。

ドメインの要件

なし。

Firepower プラットフォーム設定ポリシーは、任意のドメイン レベルで適用できます。

従来型デバイス用のプラットフォーム設定の構成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	従来型	任意（Any）	Admin

管理対象デバイスのプラットフォーム設定はポリシーベースであるため、複数のデバイスに同じ設定を適用できます。従来型デバイスでは Firepower プラットフォーム設定ポリシーを使用します。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]**を選択します。

ステップ 2 新しい Firepower ポリシーを作成するか、既存のポリシーを編集します。

プラットフォーム設定ポリシーの作成および従来型デバイス用のプラットフォーム設定について （1 ページ）を参照してください。

ステップ 3 [ポリシー割り当て（Policy Assignment）] をクリックして、ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択します。

ステップ 4 [ポリシーに追加（Add to Policy）] をクリックして（またはドラッグ アンド ドロップして）、選択したデバイスを追加します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

従来型デバイス用のアクセス リストの設定

デフォルトでは、Firepower デバイスへのアクセスは制限されていません。ポート 22（SSH）は、CLI アクセス用に開かれています。 7000/8000 シリーズ デバイスでは、Web インターフェイス アクセス用にポート 443（HTTPS）も開いています。

よりセキュアな環境で運用するために、特定の IP アドレスに対するアクセスを追加することを検討してください。さらに、ポート 161 で SNMP 情報をポーリングするためのアクセスも追加できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**[デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。	
ステップ 2	[アクセス リスト（Access List）] をクリックします。	
ステップ 3	1 つ以上の IP アドレスへのアクセスを追加するには、[ルールの追加（Add Rules）] をクリックします。	
ステップ 4	[IP アドレス（IP Address）] フィールドに、IP アドレスまたはアドレスの範囲を入力するか、`any` を入力します。	
ステップ 5	[SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。	
ステップ 6	[追加（Add）] をクリックします。	
ステップ 7	[保存（Save）] をクリックします。	

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

従来型デバイスからの監査ログのストリーミング

Firepower アプライアンスは、ユーザ インタラクションのレコード（または監査ログ）を生成します。これらの監査ログは、syslog または HTTP サーバにストリーミングできます。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

ヒント　7000/8000 シリーズデバイスでは、デバイスの Web インターフェイスで監査ログを確認することもできます。システムの監査

オプションで、Transport Layer Security（TLS）証明書を使用して、Firepower デバイスと信頼できる監査ログサーバ間の通信を保護することができます。各デバイス（クライアント証明書は一意）については、証明書署名要求（CSR）を生成して、署名のために認証局（CA）に送信してから、署名付き証明書をデバイスにインポートする必要があります。FMC を使用して、管理対象デバイスに監査ログ証明書をインポートすることはできません。これらの証明書は各デバイスに固有のものであり、各デバイスにログインして証明書をインポートする必要があります。

セキュリティを確保するには、グローバルに認識された信頼できる CA を使用します。同じ CA が次の証明書に署名する必要があります。

- クライアント証明書とサーバ証明書の両方（デバイスと監査ログサーバ間で相互認証が必要になる場合）。
- 証明書チェーンの中間証明書。署名 CA から中間 CA を信頼するように要求された場合は、必要な証明書チェーン（証明書パスとも呼ばれる）を提供する必要があります。

監査ログの形式は次のとおりです。

```
timestamp host [tag] appliance_name: username@ip_address, subsystem, action
```

次に例を示します。

```
Mar 01 14:45:24 localhost [FIREPOWER] MyFirepowerAppliance: admin@10.1.1.2, System >
Configuration, Page View
```

タグはオプションであり、ユーザ設定可能であることに注意してください。syslog イベントには、オプションのファシリティと重大度もあります。。

始める前に

デバイスが、監査ログをストリーミングする予定のサーバと通信できることを確認します。syslog のストリーミングの場合、システムはポート 7/UDP を使用して、設定を保存した際に syslog サーバが到達可能であることを確認します。次に、システムはポート 514/UDP を使用して監査ログをストリーミングします。 チャネルを保護している場合、システムは 6514/TCP を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	（オプション）監査ログ サーバとのセキュアな通信を設定します。	ASA FirePOWER および NGIPSv の場合は、OpenSSL などのツールを使用して CSR を生成してから、CLI を使用して署名付き証明書をインポートすることができます。**configure audit_cert import**。

	コマンドまたはアクション	目的
		7000/8000 シリーズデバイスの場合は、デバイスの Web インターフェイスでシステム設定（**[System]** > **[Configuration]**）を使用します。7000/8000 シリーズデバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得 （15 ページ）。 証明書が正しくインポートされたことを確認するには、7000/8000 シリーズデバイスの Web インターフェイスを使用するか、CLI で **show audit_cert** を使用します。
ステップ 2	FMC で、**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。	
ステップ 3	監査ログのストリーミングを設定するには、[監査ログ（Audit Log）] をクリックします。	syslog のストリーミング： HTTP のストリーミング：
ステップ 4	（オプション）各メッセージに含める [タグ（Tag）] を入力します。たとえば、Firepower 監査ログに **`Firepower`** をタグ付けする必要がある場合があります。	
ステップ 5	[Save] をクリックします。	syslog のストリーミングを設定した場合、システムは syslog サーバが到達可能であることを確認します。

次のタスク

- （オプション）セキュアな通信を設定した場合は、デバイスと監査ログ サーバ間の相互認証を要求することもお勧めします。従来型デバイス用の有効な監査ログ サーバ証明書の要求 （6 ページ）
- 設定変更を展開します。設定変更の展開を参照してください。

従来型デバイス用の有効な監査ログ サーバ証明書の要求

セキュリティを強化するために、Firepower アプライアンスと監査ログ サーバ間の相互認証を要求することを推奨します。相互認証を実現するには、1 つ以上の証明書失効リスト（CRL）

をロードします。これらの CRL にリストされている失効した証明書を使用して、サーバに監査ログをストリーミングすることはできません。

Firepower は、識別符号化規則（DER）形式でエンコードされた CRL をサポートしています。これらの CRL は、システムが FMC Web インターフェイスの HTTPS クライアント証明書を検証するために使用する CRL と同じであることに注意してください。

始める前に

署名付きクライアント証明書を入手し、各デバイスにインポートします。

- ASA FirePOWER および NGIPSv の場合は、OpenSSL などのツールを使用して CSR を生成してから、CLI を使用して署名付き証明書をインポートすることができます。**configure audit_cert import**。
- 7000/8000 シリーズ デバイスの場合は、デバイスの Web インターフェイスでシステム設定（**[System]** > **[Configuration]**）を使用します。7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得 （15 ページ）。

グローバルに認識された信頼できる CA を使用します。同じ CA が、インポートしたクライアント証明書と、この手順で必要になるサーバ証明書に署名する必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 [TLSの有効化（Enable TLS）]、[相互認証の有効化（Enable Mutual Authentication）] の順に選択します。

相互認証を有効にすることをお勧めします。そうしないと、デバイスは検証せずにサーバ証明書を受け入れます。

ステップ 4 [CRLの取得の有効化（Enable Fetching of CRL）] を選択し、CRL ファイルに URL を入力して、[CRLの追加（Add CRL）] をクリックします。

最大 25 個の CRL を追加できます。展開すると、システムは CRL の更新をスケジュールします。更新頻度を設定する場合は、証明書失効リストのダウンロードの設定を参照してください。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

7000/8000 シリーズ デバイスへの外部認証の有効化

LDAP または RADIUS サーバに対して 7000/8000 シリーズ デバイスのユーザを認証できるようにするには、ローカル データベースを使用するのではなく、デバイス プラットフォーム設定を使用します。

始める前に

外部認証オブジェクトを設定します。外部認証の設定を参照してください。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [外部認証（External Authentication）] をクリックします。

ステップ 3 [ステータス（Status）] ドロップダウン リストから [有効（Enabled）] を選択します。

ステップ 4 [デフォルト ユーザ ロール（Default User Role）] ドロップダウン リストから、ユーザ ロールを選択して、外部認証済みユーザに付与するデフォルト権限を定義します。

ステップ 5 外部サーバを使用して CLI またはシェル アクセス アカウントを認証する場合、[シェル認証（Shell Authentication）] ドロップダウン リストから [有効（Enabled）] を選択します。

ステップ 6 CAC 認証および認可を有効にする場合は、[CAC 認証（CAC Authentication）] ドロップダウン リストから使用可能な CAC 認証オブジェクトを選択します。

詳細については、LDAP を使用した共通アクセス カード認証の設定を参照してください。

ステップ 7 使用する外部認証オブジェクトそれぞれの横にあるチェック ボックスをクリックします。複数のオブジェクトを有効にすると、ユーザは指定された順序でサーバと照合されます。サーバの順序を変更する場合は、次の手順を参照してください。

シェル認証を有効にする場合は、[シェルアクセスフィルタ（Shell Access Filter）] を含む外部認証オブジェクトを有効にする必要があります。CLI/シェル アクセスのユーザは、認証オブジェクトがリストの順序で最も高いサーバに対してのみ認証できることに注意してください。

CLI と CAC の両方の認証が必要な場合は、各目的のため個別の認証オブジェクトを使用する必要があります。

ステップ 8 （オプション）上矢印および下矢印を使用して、認証要求が行われたときに認証サーバがアクセスされる順序を変更できます。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

7000/8000 シリーズ デバイスの外部認証について

外部認証サーバを参照する認証オブジェクトを作成する場合、外部認証を有効にすることにより、ローカルデータベースを使用せずに、管理対象デバイスにログインしているユーザをそのサーバに認証させることができます。

外部認証を有効にすると、システムでは LDAP または RADIUS サーバのユーザのユーザ クレデンシャルが確認されます。さらに、ユーザがローカルの内部認証を有効にしており、ユーザクレデンシャルが内部データベースにない場合、システムは一致するクレデンシャルのセットがないか外部サーバを検査します。ユーザが複数のシステムで同じユーザ名を持っている場合、すべてのサーバですべてのパスワードが動作します。ただし、使用可能な外部認証サーバで認証が失敗した場合、システムはローカルデータベースの検査に戻らないので注意してください。

外部認証を有効にすると、アカウントが外部で認証されている任意のユーザのデフォルトのユーザ ロールを設定できます。これらのロールを組み合わせることができる場合は、複数のロールを選択できます。たとえば、自社の [ネットワーク セキュリティ（Network Security）] グループのユーザのみを取得する外部認証を有効化した場合、デフォルトのユーザ ロールを設定して [セキュリティ アナリスト（Security Analyst）] ロールを組み込み、ユーザが自分で追加のユーザ設定を行わなくても収集されたイベントデータにアクセスできるようにすることが可能です。ただし、外部認証がセキュリティ グループに加えて他のユーザのレコードを取得する場合、デフォルトのロールを未選択のままにしておきたい場合もあります。

アクセス ロールが選択されていない場合、ユーザはログインできますが、どの機能にもアクセスできません。ユーザがログインを試行すると、アカウントがユーザ管理ページ（**[System]** > **[Users]**）に表示されます。ここで、追加の権限を付与するアカウント設定を編集できます。

ヒント 1 つのユーザ ロールを使用するようにシステムを設定してそのポリシーを適用し、後で設定を変更して別のデフォルトのユーザ ロールを使用する場合、アカウントを変更するか、削除して再作成するまで、変更前に作成されたユーザ アカウントはすべて、最初のユーザ ロールを保持します。

CLI/シェル アクセスまたは CAC 認証および承認のために LDAP サーバに対して認証できる一連のユーザを指定する場合は、それぞれに個別の認証オブジェクトを作成し、オブジェクトを個別に有効にする必要があります。

内部認証によってユーザがログインしようとすると、システムは最初にそのユーザがローカル ユーザ データベースに存在するかどうか検査します。ユーザが存在する場合、システムは次にユーザ名とパスワードをローカル データベースに対して検査します。一致が検出されると、ユーザは正常にログインします。ただし、ログインが失敗し、外部認証が有効になっている場合、システムはそれぞれの外部認証サーバに対して、ユーザを設定に表示される認証順序で検査します。ユーザ名およびパスワードが外部サーバからの結果と一致した場合、システムはユーザを、その認証オブジェクトに対してデフォルトの権限を持つ外部ユーザに変更します。

外部ユーザがログインしようとすると、システムは外部認証サーバに対してユーザ名およびパスワードを検査します。一致が検出されると、ユーザは正常にログインします。ログインが失敗した場合、ユーザのログイン試行は拒否されます。外部ユーザは、ローカルデータベース内

のユーザ リストに対して認証できません。ユーザが新しい外部ユーザの場合、外部認証オブジェクトのデフォルト権限を持つ外部ユーザ アカウントがローカル データベースに作成されます。

7000/8000 シリーズ Web インターフェイスの言語の設定

ここで指定した言語は、ログインしたすべてのユーザの Web インターフェイスに使用されます。次の言語を選択できます。

- 英語
- 中国語（簡体字）
- 中国語（繁体字）
- 日本語
- 韓国語

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [言語（Language）] をクリックします。

ステップ 3 使用する言語を選択します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

従来型デバイス用のログイン バナーのカスタマイズ

従来型デバイス用の CLI ログイン バナーをカスタマイズできます。 7000/8000 シリーズ デバイスの場合、ログイン バナーも Web インターフェイスに表示されます。ログイン バナーが大きすぎる場合や、エラーの原因となる場合、システムがバナーを表示しようとすると、CLI セッションが失敗することがあります。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [ログイン バナー（Login Banner）] を選択します。

ステップ 3 [カスタム ログイン バナー（Custom Login Banner）] フィールドに、使用するログイン バナー テキストを入力します。

タブによるスペース設定は維持されません。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

従来型デバイスの時刻を NTP サーバに同期

正常に動作させるには、Firepower Management Center とその管理対象デバイスのシステム時刻を同期させることが不可欠です。展開に FTD デバイスが含まれている場合は、脅威に対する防御のための NTP 時刻同期の設定を参照してください。

⚠

注意 FMC と管理対象デバイスの時刻が同期していないと、意図しない結果になることがあります。

展開後、設定された NTP サーバと管理対象デバイスを同期するには、数分かかる場合があります。NTP サーバとして設定されている FMC とデバイスを同期する場合、FMC 自体が NTP サーバを使用するように設定されていると、時刻の同期にさらに時間がかかることがあります。

始める前に

デバイスが、使用予定の NTP サーバと通信できることを確認します。次のいずれかの操作を実行できます。

- FMC と同じ NTP サーバを使用します。FMC の時刻を NTP サーバに同期。
- FMC を NTP サーバとして設定します。ネットワーク NTP サーバにアクセスせずに時刻を同期。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [時刻の同期（Time Synchronization）] をクリックします。

ステップ 3 時刻の同期方法を指定します。

- [NTPの接続元（Via NTP from）]：ネットワーク上の NTP サーバから時刻を受信します。

- [Management CenterのNTPを使用（Via NTP from Management Center）]：FMC が NTP サーバとして機能するように設定されています。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

従来型デバイスのセッション タイムアウトの設定

無人ログインセッションは、セキュリティ上のリスクを生じさせる場合があります。ユーザのログインセッションが非アクティブになったためにタイムアウトするまでのアイドル時間を設定できます。最大値は 24 時間（1440 分）です。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [シェル タイムアウト（Shell Timeout）] をクリックします。

ステップ 3 セッション タイムアウトの設定

- Web インターフェイス（7000/8000 シリーズのみ）：[ブラウザセッションタイムアウト（分）（Browser Session Timeout (Minutes)）] を入力します。

  システムを長期間にわたってパッシブかつセキュアにモニタする予定のシナリオでは、特定の Web インターフェイスのユーザがタイムアウトしないように設定できます。詳細については、Web インターフェイスでの内部ユーザの追加 を参照してください。

- CLI：[シェルタイムアウト（分）（Shell Timeout (Minutes)）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

従来型デバイスでの SNMP ポーリングの設定

Simple Network Management Protocol（SNMP）を使用すると、Firepower デバイスの標準 Management Information Base（MIB）にアクセスできます。MIB には、連絡先、管理、場所、サービス情報、IP アドレッシングやルーティングの情報、トランスミッション プロトコルの使用状況の統計などのシステムの詳細が含まれます。 7000/8000 シリーズ デバイスの追加の

MIB には、物理インターフェイス、論理インターフェイス、仮想インターフェイス、ARP、NDP、仮想ブリッジ、仮想ルータを通して渡されるトラフィックの統計が含まれます。SNMP ポーリングを有効にすると、システムで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングのみで使用可能になることに注意してください。

システムは、SNMPv1、v2、および v3 をサポートしています。SNMPv2 は読み取り専用コミュニティのみをサポートし、SNMPv3 は読み取り専用ユーザのみをサポートしています。SNMPv3 は、AES128 での暗号化をサポートします。

始める前に

使用するコンピュータごとに SNMP アクセスを追加し、システムをポーリングします。従来型デバイス用のアクセス リストの設定 （4 ページ）を参照してください。

（注） SNMP MIB には展開の攻撃に使用される可能性がある情報が含まれています。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することを推奨します。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することも推奨します。

手順

ステップ 1 **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** を選択し、Firepower ポリシーを作成または編集します。

ステップ 2 [SNMP] をクリックします。

ステップ 3 [SNMPバージョン（SNMP Version）] ドロップダウン リストから、使用する SNMP バージョンを選択します。

- [バージョン1（Version 1）] または [バージョン2（Version 2）] : [コミュニティストリング（Community String）] フィールドに読み取り専用の SNMP コミュニティ名を入力します。手順の最後にスキップします。
- [バージョン3（Version 3）] : [ユーザを追加（Add User）] をクリックすると、ユーザ定義ページが表示されます。SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

ステップ 4 ユーザ名を入力します。

ステップ 5 [認証プロトコル（Authentication Protocol）] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 6 [認証パスワード（Authentication Password）] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 7 [パスワードの確認（Verify Password）] フィールドに、認証パスワードを再度入力します。

ステップ 8 使用するプライバシー プロトコルを [プライバシー プロトコル（Privacy Protocol）] リストから選択するか、プライバシー プロトコルを使用しない場合は [なし（None）] を選択します。

ステップ 9 [プライバシー パスワード（Privacy Password）] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 10 [パスワードの確認（Verify Password）] フィールドに、プライバシー パスワードを再度入力します。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

7000/8000 シリーズ デバイスのローカル システム設定

7000/8000 シリーズ デバイスのローカル Web インターフェイスにログインして、非ポリシーベースのシステム設定を行うことができます。これらの設定の多くは FMC システム設定とパラレルです。詳細は、FMC システム設定の章「システム設定（System Configuration）」に記載されています。

表 *2: 7000/8000* シリーズ デバイスのローカル システム設定

システム設定	説明	参照先
監査ログ証明書	監査ログのセキュアなストリーミングの一部として、7000/8000 シリーズ デバイスの署名付きクライアント証明書を取得およびインポートします。	7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得（15 ページ）
調整の変更	過去 24 時間にわたるシステムへの変更の詳細なレポートを送信します。	変更調整
コンソール設定	VGA またはシリアル ポート経由、または Lights-Out Management（LOM）経由のコンソール アクセスを設定します。	リモート コンソールのアクセス管理
HTTPS Certificate	必要に応じて、信頼できる認証局の HTTPS サーバ証明書を要求し、システムに証明書をアップロードします。	HTTPS 証明書
情報	アプライアンスに関する最新情報を表示し、表示名を編集します。	アプライアンス情報（Appliance Information）

システム設定	説明	参照先
管理インターフェイス	アプライアンスの IP アドレス、ホスト名、プロキシ設定などのオプションを変更します。	7000/8000 シリーズ デバイスでの管理インターフェイスの設定（17 ページ）
プロセス	Firepower のプロセスをシャットダウン、リブート、または再起動します。	7000/8000 シリーズ デバイスのシャットダウンまたは再起動 （21 ページ）
パケット転送の禁止	低帯域幅の展開で、7000/8000 シリーズ デバイスから FMC へのパケット データの送信を無効にします。	FMC へのパケット転送の禁止 （16 ページ）
時刻（Time）	現在の時刻設定を表示します。	7000/8000 シリーズ デバイスのシステム時刻の表示 （22 ページ）

7000/8000 シリーズ デバイスでのセキュアな監査ログ ストリーミング用の署名付きクライアント証明書の取得

オプションで、Transport Layer Security（TLS）証明書を使用して、Firepower デバイスと信頼できる監査ログ サーバ間の通信を保護することができます。各デバイス（クライアント証明書は一意）については、証明書署名要求（CSR）を生成して、署名のために認証局（CA）に送信してから、署名付き証明書をデバイスにインポートする必要があります。FMC を使用して、管理対象デバイスに監査ログ証明書をインポートすることはできません。これらの証明書は各デバイスに固有のものであり、各デバイスにログインして証明書をインポートする必要があります。

セキュリティを確保するには、グローバルに認識された信頼できる CA を使用します。同じ CA が次の証明書に署名する必要があります。

- クライアント証明書とサーバ証明書の両方（デバイスと監査ログ サーバ間で相互認証が必要になる場合）。
- 証明書チェーンの中間証明書。署名 CA から中間 CA を信頼するように要求された場合は、必要な証明書チェーン（証明書パスとも呼ばれる）を提供する必要があります。

システムは、ベース 64 エンコードの PEM 形式で証明書要求のキーを生成します。

手順

ステップ 1 デバイスの Web インターフェイスにログインし、**[System]** > **[Configuration]** を選択します。

ステップ 2 [監査ログ証明書（Audit Log Certificate）] をクリックします。

ステップ 3 CSR を作成します。

a) [新規 CSR の生成（Generate New CSR）] をクリックします。

b) 必要な場所と組織の情報を入力します。

c) [共通名（Common Name）] フィールドに、証明書を要求するサーバの完全修飾ドメイン名を入力します。共通名と DNS ホスト名が一致しないと、監査ログのストリーミングは失敗します。

d) [生成（Generate）] をクリックします。

ステップ 4 CSR のテキスト ファイルを作成します。

a) 証明書要求のテキスト ブロック全体（`BEGIN CERTIFICATE REQUEST` 行と `END CERTIFICATE REQUEST` 行を含む）をコピーして貼り付けます。

b) このファイルを *clientname*`.csr` として保存します。*clientname* は、証明書を使用する予定のデバイスの名前にします。

ステップ 5 CSR を CA に送信して、署名付き証明書の受信を待機します。

ステップ 6 デバイスに署名付き証明書をインポートします。

ページを離れた場合は、**[[System] > [Configuration]] > [監査ログ証明書（Audit Log Certificate）]** に戻り、[監査クライアント証明書のインポート（Import Audit Client Certificate）] をクリックします。以下をコピーして貼り付けます。

- [クライアント証明書（Client Certificate）]：署名付き証明書のすべてのテキスト（`BEGIN CERTIFICATE` 行と `END CERTIFICATE` 行を含む）。
- [秘密キー（Private Key）]：秘密キー ファイルのすべてのテキスト（`BEGIN RSA PRIVATE KEY` 行と `END RSA PRIVATE KEY` 行を含む）。
- [証明書チェーン（Certificate Chain）]：必要な各中間証明書のすべてのテキスト。

正しい証明書をインポートしていることを確認します。クライアント証明書は一意です。

ステップ 7 [Save] をクリックします。

次のタスク

まだ設定していない場合は、FMC のデバイス プラットフォーム設定を使用して監査ログのストリーミングを設定します。従来型デバイスからの監査ログのストリーミング （4ページ）。

FMC へのパケット転送の禁止

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	7000 & 8000 シリーズ	該当なし	管理者

侵入ポリシー違反をトリガーしたパケットの具体的な内容について気にする必要がない場合、低帯域幅の展開で 7000 または 8000 シリーズ デバイスから Firepower Management Center デバイスにパケットを送信することを無効にするとができます。

手順

ステップ 1 7000 または 8000 シリーズ デバイスのローカル web インターフェイスで、**[System]** > **[Configuration]** を選択します。

ステップ 2 [情報（Information）] をクリックします。

ステップ 3 [管理センターへのパケット転送を禁止する（Prohibit Packet Transfer to the Management Center）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

7000/8000 シリーズ デバイスでの管理インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
該当なし	任意（Any）	7000 & 8000 シリーズ	グローバルだけ	Admin

Webインターフェイスを使用して、管理対象デバイスの管理インターフェイスの設定を変更します。モデルでサポートされている場合に、オプションでイベントインターフェイスを有効にすることができます。管理インターフェイスの詳細については、管理インターフェイスを参照してください。

⚠

注意 慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソール ポートへのアクセスおよび CLI での再設定が必要になります。

手順

ステップ 1 **[System]** > **[Configuration]** を選択して、[管理インターフェイス（Management Interfaces）] を選択します。

ステップ 2 [インターフェイス（Interfaces）]エリアで、設定するインターフェイスの横にある [編集（Edit）] をクリックします。

このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする（Enabled）]：管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効にしないでください。eth0 インターフェイスを必要とするプロセスもあります。
- [チャネル（Channels）]：（8000 シリーズのみ）イベント オンリーのインターフェイスを設定します。8000 シリーズのデバイスで eth1 管理インターフェイスを有効にして、イベント インターフェイスとして機能させることができます。これを設定するには、[管理トラフィック（Management Traffic）] チェックボックスをオフにして、[イベント トラフィック（Event Traffic）] チェックボックスをオンのままにしておきます。eth0 管理インターフェイスを入力するには、両方のチェックボックスをオンのままにしておきます。

  Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

  必要に応じて、管理インターフェイスの [イベント トラフィック（Event Traffic）] を無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベント チャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

  インターフェイス上でイベント チャネルと管理チャンネルの両方を無効にすることはできません。
- [モード（Mode）]：リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MTU]：最大伝送ユニット（MTU）を設定します。デフォルトは 1500 です。設定可能な MTU の範囲は、モデルとインターフェイスのタイプによって異なる場合があります。

  システムは、設定された MTU 値から自動的に 18 バイトを削減するため、IPv6 の場合、1298 未満の値は MTU の最小値である 1280 に準拠しません。IPv4 の場合は、594 未満の値は MTU の最小値 576 に準拠しません。たとえば、構成値 576 は自動的に 558 に削減されます。
- [MDI/MDIX]：[自動-MDIX（Auto-MDIX）] を設定します。
- [IPv4 設定（IPv4 Configuration）]：IPv4 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv4 の管理 IP アドレス** と**ネットマスク**を手動で入力します。
  - [DHCP]：DHCP を使用するインターフェイスを設定します（eth0 のみ）。
  - [無効（Disabled）]：無効 IPv4。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 設定（IPv6 Configuration）]：IPv6 IP アドレスを設定します。次のどちらかを選択します。
  - [スタティック（Static）]：**IPv6 の管理 IP アドレス**と **IPv6 のプレフィックス長**を手動で入力します。

- [DHCP]：DHCPv6 を使用するインターフェイスを設定します（eth0 のみ）。
- [ルータ割当て（Router Assigned）]：ステートレス自動設定を有効にします。
- [無効（Disabled）]：IPv6 を無効にします。IPv4 と IPv6 の両方を無効に**しないでください**。

ステップ 3 [ルート（Routes）]エリアで、スタティック ルートを編集アイコン（）をクリックして編集するか、またはルートを追加アイコン（）をクリックして追加します。表示アイコン（  ）をクリックして、ルートの統計を表示します。

（注） Firepower Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加する必要があります。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。出力インターフェイスは、指定したゲートウェイをインターフェイスのネットワークに照合することで自動的に選択されます。ルーティングの詳細については、管理インターフェイス上のネットワーク ルートを参照してください。

次の設定をスタティック ルートに対して設定できます。

- [宛先（Destination）]：ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク（Netmask）] または [プレフィックス長（Prefix Length）]：ネットワークのネットマスク（IPv4）またはプレフィックス長（IPv6）を設定します。
- [インターフェイス（Interface）]：出力管理インターフェイスを設定します。
- [ゲートウェイ（Gateway）]：ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定（Shared Settings）] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

（注） eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定することができなくなります。

以下の共有設定を行うことができます。

- [ホスト名（Hostname）]：デバイスのホスト名を設定します。ホスト名を変更する場合、Syslog メッセージに新しいホスト名を反映させるには、デバイスをリブートします。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン（Domains）]：カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。
- [プライマリ DNS サーバ（Primary DNS Server）]、[セカンダリ DNS サーバ（Secondary DNS Server）]、[テリタリ DNS サーバ（Tertiary DNS Server）]：DNS サーバが優先順で使用されるよう設定します。

- [リモート管理ポート（Remote Management Port）]：FMC で通信のリモート管理ポートを設定します。FMCおよび管理対象デバイスは、双方向のSSL暗号化通信チャネル（デフォルトではポート 8305）を使用して通信します。

  （注） シスコは、リモート管理ポートをデフォルト設定のままにしておくことを**強く**推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、導入内の相互に通信する必要がある**すべての**デバイスの管理ポートを変更する必要があります。

ステップ 5 [LCDパネル（LCD Panel）]エリアで、[ネットワーク設定の再設定を許可（Allow reconfiguration of network settings）] チェックボックスをオンにして、デバイスの LCD パネルを使用したネットワーク設定の変更を有効にします。

LCD パネルを使用して、デバイスの IP アドレスを編集できます。変更が管理 Firepower Management Centerに反映されていることを確認します。状況によっては、Firepower Management Center でデータを手動で更新することが必要になります。

注意 LCD パネルを使用した再構成を許可すると、セキュリティ リスクが発生する可能性があります。LCDパネルを使用してネットワーク設定を構成する場合は、物理アクセスだけが必要で、認証は必要ありません。このオプションを有効にするとセキュリティ上の問題が発生する可能性があることを示す警告が Web インターフェイスに表示されます。

ステップ 6 [プロキシ（Proxy）] エリアで、HTTP プロキシ設定をします。

デバイスは、ポート TCP/443（HTTPS）および TCP/80（HTTP）でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。

（注） NT LAN Manager（NTLM）認証を使用するプロキシはサポートされません。

a) [有効（Enabled）] チェックボックスをオンにします。
b) [HTTP プロキシ（HTTP Proxy）] フィールドに、プロキシ サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
c) [ポート（Port）] フィールドに、ポート番号を入力します。
d) [プロキシ認証の使用（Use Proxy Authentication）] を選択してから [ユーザ名（User Name）] と [パスワード（Password）] を入力して、認証資格情報を設定します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 管理 IP アドレスを変更すると、FMC と管理対象デバイスの間の通信に影響を与える可能性があります。

IP アドレスを変更しても、現在の接続には影響を与えません。ただし、デバイスまたは FMC をリロードした場合は、接続を再確立する必要があります。ピアの正しい IP アドレスを持つために、少なくとも 1 つのデバイス（FMC または管理対象デバイス）が必要です。たとえば、デバイス設定中に（IP アドレスの代わりに）FMC の NAT ID を指定した場合は、デバイスを追加したときに FMC で定義したデバイス IP アドレスが正しくなくなるため、FMC は通信を

再確立できなくなります。この場合は、FMC でデバイスの管理 IP アドレスを変更する必要があります。デバイス管理設定の編集を参照してください。

7000/8000 シリーズ デバイスのシャットダウンまたは再起動

手順

ステップ 1 デバイスの Web インターフェイスで、**[System]** > **[Configuration]** を選択します。

ステップ 2 [プロセス（Process）] を選択します。

ステップ 3 次のいずれかを実行します。

シャットダウン	[アプライアンスのシャットダウン（Shutdown Appliance）] の横にある [コマンドの実行（Run Command）] をクリックします。 **注意** 電源ボタンを使用して Firepower アプライアンスを停止しないでください。データが失われる可能性があります。Web インターフェイス（または CLI）を使用すると、設定データを失うことなく、安全にシステムの電源を切って再起動する準備が整います。
再起動	[アプライアンスの再起動（Reboot Appliance）] の横にある [コマンドの実行（Run Command）] をクリックします。 （注） 再起動するとログアウトします。システムはデータベースチェックを実行しますが、これは完了するのに 1 時間かかります。
コンソールの再起動	[アプライアンスコンソールの再起動（Restart Appliance Console）] の横にある [コマンドの実行（Run Command）] をクリックします。
Snort プロセスの再起動	[Snortの再起動（Restart Snort）] の横にある [コマンドの実行（Run Command）] をクリックします。 **注意** Snort プロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中にトラフィックがドロップするか、検査なしで通過するかどうかは、デバイスの設定方法によって異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

7000/8000 シリーズ デバイスのシステム時刻の表示

[ユーザ設定（User Preferences）] の [タイムゾーン（Time Zone）] ページで設定したタイムゾーンを使用すると、ほとんどのページでローカル時刻で時刻設定が表示されますが、アプライアンスには UTC 時間を使用して格納されます。さらに、現在の時刻は [時刻の同期（Time Synchronization）] ページの上部に UTC で表示されます（ローカル時刻は手動時計設定オプションで表示されます（有効になっている場合））。

制約事項

タイムゾーン機能（[ユーザ設定（User Preferences）]）は、デフォルトのシステム クロックが UTC 時間に設定されていることを前提としています。**これは変更しないでください。**システム時刻を UTC から変更することはサポートされていないため、デバイスを再イメージ化する必要があります。

次の手順を使用して、7000 および 8000 シリーズ デバイスでシステム時刻情報を確認します。

手順

ステップ 1 デバイスの Web インターフェイスにログインし、**[System]** > **[Configuration]** を選択します。

ステップ 2 [時間（Time）] をクリックします。

NTP を使用している場合は、NTP サーバのステータスを参照してください。