



Management Center Virtual 初期管理および設定

Management Center Virtual の初期セットアッププロセスが完了し、正常にセットアップされたことを確認したら、展開の管理を容易にするさまざまな管理タスクを実行することを推奨します。また、ライセンスの取得など、初期設定で省略したタスクも完了する必要があります。以下のセクションで説明するタスクの詳細、および展開の設定を開始する方法の詳細については、ご使用のバージョンに対応する『[Firepower Management Center Configuration Guide](#)』を参照してください。

- [個別のユーザー アカウント \(1 ページ\)](#)
- [デバイス登録 \(2 ページ\)](#)
- [ヘルス ポリシーとシステム ポリシー \(2 ページ\)](#)
- [ソフトウェアとデータベースの更新 \(3 ページ\)](#)

個別のユーザー アカウント

初期設定が完了した時点で、システム上の唯一の Web インターフェイスのユーザーは、管理者ロールとアクセス権を持つ **admin** ユーザーです。その役割を持つユーザーはシステムへのすべてのメニューと設定にアクセスできます。セキュリティおよび監査上の理由から、**admin** アカウント（および Administrator ロール）の使用を制限することをお勧めします。ユーザーアカウントは、Management Center Virtual GUI の [システム (System)] > [ユーザー (Users)] > [ユーザー (User)] ページで管理します。



- (注) シェルを使用した Management Center Virtual へのアクセスと Web インターフェイスを使用した Management Center Virtual へのアクセスのための **admin** アカウントは異なるため、別のパスワードを使用できます。

システムを使用する各ユーザーに対して個別のアカウントを作成すると、各ユーザーによって行われたアクションと変更を組織で監査できるほか、各ユーザーに関連付けられたユーザーアクセスロールを制限することができます。これは、ほとんどの設定および分析タスクを実行す

る Management Center Virtual で特に重要です。たとえば、アナリストはネットワークのセキュリティを分析するためにイベントデータにアクセスする必要がありますが、展開の管理機能にアクセスする必要はありません。

システムには、Web インターフェイスを使用してさまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザー ロールが用意されています。また、特別なアクセス権限を持つカスタム ユーザー ロールを作成することもできます。

デバイス登録

Management Center は、現在システムでサポートされているすべてのデバイス（物理または仮想）を管理できます。

- **Threat Defense** : 統合した次世代ファイアウォールと次世代 IPS デバイスを提供します。
- **Threat Defense Virtual** : 複数のハイパーバイザ環境で作業し、管理オーバーヘッドを削減し、運用効率を向上させるために設計された 64 ビットのバーチャルデバイス。
- **Cisco ASA with FirePOWER Services** (または ASA FirePOWER モジュール) : 最も重要なシステムポリシーを提供し、検出とアクセス制御のために、システムにトラフィックを渡します。ただし、Management Center の Web インターフェイスを使用して ASA FirePOWER のインターフェイスを設定することはできません。Cisco ASA with FirePOWER Services には、ASA プラットフォームに一意的なソフトウェアと CLI があり、これらを使用してシステムをインストールし、他のプラットフォーム固有の管理タスクを実行することができます。
- **7000 および 8000 シリーズ アプライアンス** : システム用に特別に設計された物理デバイス。7000 および 8000 シリーズ デバイスのスループットはさまざまですが、多くの同じ機能が共有されます。一般に、8000 シリーズ デバイスは 7000 シリーズ デバイスよりも高性能で、8000 シリーズ 高速パス ルール、リンク集約、およびスタックなどの追加機能もサポートします。デバイスを Management Center に登録する前に、そのデバイス上でリモート管理を設定する必要があります。
- **NGIPSv** : VMware vSphere 環境で展開する 64 ビットのバーチャルデバイス。NGIPSv のデバイスは、冗長性とリソースの共有、スイッチ、およびルーティングのようなシステムのハードウェアベースの機能のどちらもサポートしていません。

Management Center に管理対象デバイスを登録するには、Management Center GUI の **[デバイス (Device)] > [デバイス管理 (Device Management)]** ページを使用します。ご使用のバージョンの [Firepower Management Center コンフィギュレーション ガイド](#) でデバイス管理情報を参照してください。

ヘルス ポリシーとシステム ポリシー

デフォルトでは、すべてのアプライアンスにシステムの初期ポリシーが適用されます。システム ポリシーは、メール リレー ホストのプリファレンスや時間同期の設定など、展開内の複数

のアプライアンスで共通している可能性が高い設定を管理します。シスコでは、Management Center を使用して、それ自体およびその管理対象デバイスすべてに同じシステムポリシーを適用することを推奨しています。

デフォルトで、Management Center にはヘルス ポリシーも適用されます。ヘルスポリシーは、ヘルスマニターリング機能の一部として、システムが展開環境内でアプライアンスのパフォーマンスを継続して監視するための基準を提供します。シスコでは、Management Center を使用して、その管理対象デバイスすべてにヘルス ポリシーを適用することを推奨しています。

ソフトウェアとデータベースの更新

展開を開始する前に、アプライアンス上でシステムソフトウェアを更新する必要があります。展開環境内のすべてのアプライアンスでシステムの最新のバージョンを実行することを推奨します。展開環境でこれらのアプライアンスを使用する場合は、最新の侵入ルール更新、VDB、および GeoDB もインストールする必要があります。



注意 システムの一部を更新する前に、その更新に関するリリースノートまたはアドバイザリテキストを読んでおく必要があります。リリースノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

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

Management Center は設定の一環として次のアクティビティを確立し、システムを最新の状態に保ち、データをバックアップします。

- 週次自動 GeoDB 更新
- Management Center とその管理対象デバイスにおける最新ソフトウェアをダウンロードする週次タスク。



重要 このタスクは、Management Center にソフトウェアの更新のみをダウンロードします。ユーザーは、このタスクがダウンロードした更新をインストールする必要があります。詳細については、『Cisco Firepower Management Center Upgrade Guide』を参照してください。

- ローカルに保存された設定のみの Management Center バックアップを実行する週次タスク。

Management Center でバージョン 6.6 以降を実行している場合、初期設定の一環として、Management Center はシスコのサポートサイトから最新の脆弱性データベース（VDB）の更新をダウンロードしてインストールします。これは 1 回限りの操作です。

Web インターフェイスのメッセージセンターを使用して、これらのアクティビティのステータスを確認できます。システムがこれらのアクティビティのいずれかを設定できず、Management

Centerがインターネットにアクセスできる場合は、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、これらのアクティビティを自分で設定することをお勧めします。

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。