Cisco Secure Workload および Cisco Secure Firewall Management Center 統合ガイド

初版：2021 年 2 月 25 日

最終更新：2023 年 5 月 19 日

Cisco Secure Workload と Cisco Secure Firewall Management Center の統合

この統合について

Cisco Secure Workload（旧称 Cisco Tetration）と Cisco Secure Firewall（旧称 Cisco Firepower）のそれぞれの能力を組み合わせることで、特に次のような用途に役立つエージェントレスセキュリティ ソリューションを実現できます。

- ソフトウェアエージェントをインストールできないワークロードをセグメント化する。

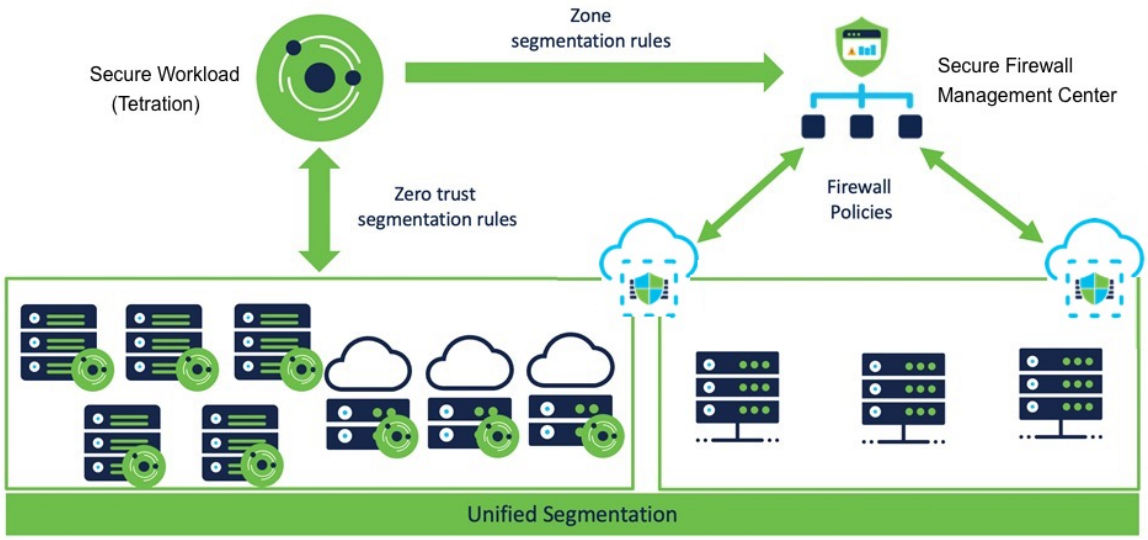
  たとえば、ワークロードのオペレーティングシステム（アプライアンスベースのソフトウェア）を制御できない場合や、エージェントではサポートされていないレガシー オペレーティング システムでワークロードを実行している場合は、この統合を使用します。

- データセンターやクラウド内のさまざまなゾーンのトラフィックをセグメント化する。

  たとえば、ネットワークに入るトラフィック、ネットワークから出るトラフィック、およびネットワーク内のワークロード間のトラフィックに対して、さまざまなポリシーセットを簡単かつ広く適用できます。

この統合により、Cisco Secure Workload は、Cisco Secure Firewall Management Center インスタンスによって管理される Cisco Secure Firewall Threat Defense（旧称 Firepower Threat Defense）ファイアウォールでセグメンテーションポリシーを自動的に適用および管理します。ポリシーは動的に更新され、アプリケーション環境の変更に応じて、ポリシーが適用する一連のワークロードは継続的に更新されます。

図 *1 : Cisco Secure Workload と Cisco Secure Firewall Management Center* の統合



Secure Workload バージョン 3.7 および 3.6 の場合： Secure Workload により適用されるセグメンテーションポリシーは、Cisco Secure Firewall Management Center でダイナミックオブジェクトに変換されたスコープ、インベントリフィルタ、およびクラスタから取得された IP アドレスに基づいてアクセス コントロール ポリシーに変換されます。詳細については、Cisco Secure Workload バージョン 3.7 および 3.6 に関する重要な情報 （6 ページ）を参照してください。

Tetration バージョン 3.5 の場合：Tetration セグメンテーションポリシーは、Firepower Management Center でプレフィルタポリシーに変換されます。

すべてのバージョン：

Cisco Secure Firewall Management Center 外部オーケストレータはユーザー注釈を生成しません。

このガイドを使用して、使用している製品バージョンに適したソリューションを展開してください。

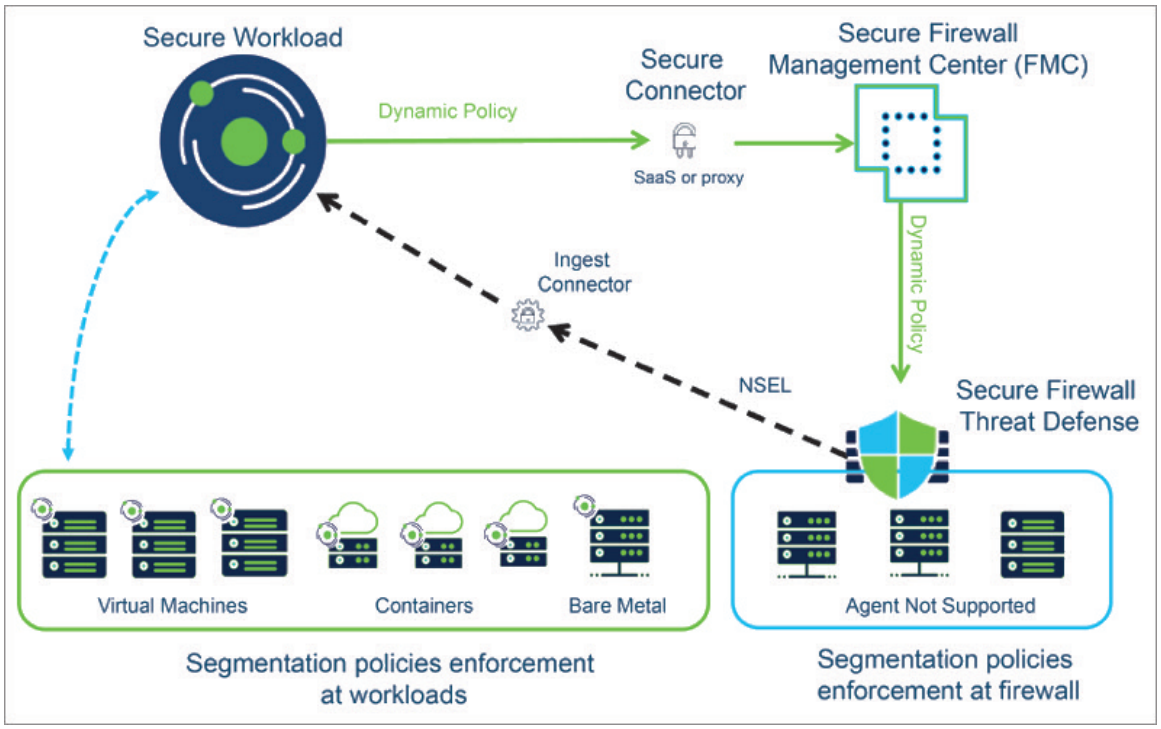
重要	この統合は、すべての Secure Workload/Tetration リリースのベータ機能です。

Cisco Secure Workload バージョン 3.8 に関する重要な情報

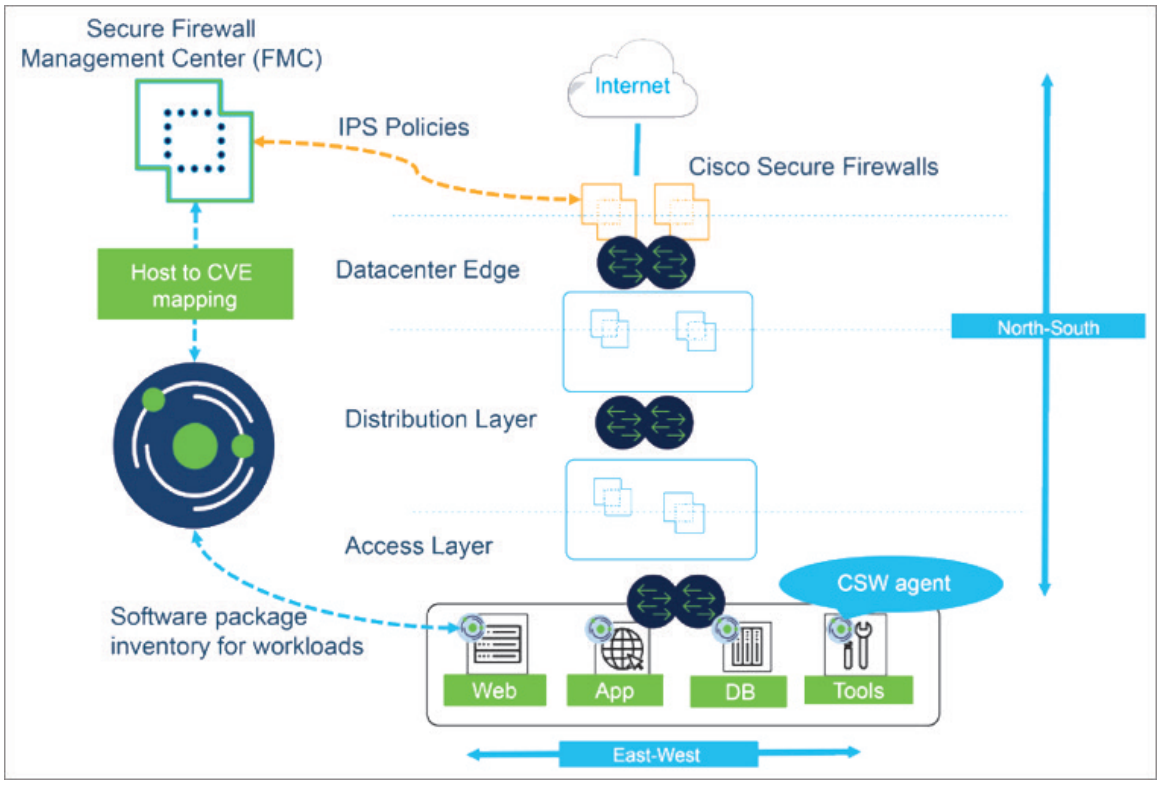
この統合には以下の機能および利点があります。

- エージェントレス ワークロードの完全な可視性と適用。
- Cisco Secure Workload は、Cisco Secure Firewall Management Center から NSEL レコードを取り込み、エージェントレス ワークロードのセグメンテーションポリシーを自動的に作成することができます。

- Cisco Secure Workload は、適用されたポリシーを Firewall Management Center に自動的にプッシュします。



- Cisco Secure Workload は、エージェントベースのワークロードからの CVE 情報を Cisco Secure Firewall Management Center にプッシュして、脆弱なワークロードの可視性を強化します。これにより、FMC はファイアウォールの推奨事項を実行し、関連する Snort シグネチャを使用して侵入防御ポリシーを調整することで、エクスプロイトから保護することができます。



ネットワークインベントリは、セグメンテーションポリシーのベースとなる Cisco Secure Workload スコープ、インベントリフィルタ、およびクラスタによって動的に更新されます。ネットワークでワークロードが追加、変更、または削除されると、Cisco Secure Firewall Management Center 内のダイナミックオブジェクトが Cisco Secure Workload により自動的に更新されます。対応するアクセスコントロールルールは、これらのダイナミックオブジェクトに基づきます。

プロセスの概要：

1. Cisco Secure Workload、Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense 製品を展開します。
2. FMC コネクタ Cisco Secure Workload を作成し、Cisco Secure Firewall Management Center との通信を確立します。
3. セグメンテーションポリシーで使用するコンシューマとプロバイダーを定義するスコープ、インベントリフィルタ、およびクラスタを Cisco Secure Workload で作成します。

   （Cisco Secure Workload の「コンシューマ」と「プロバイダー」は、Cisco Secure Firewall Management Center 上のトラフィックの「送信元」と「宛先」におおまかに対応します。）
4. アプリケーションの依存関係マッピングを使用してポリシーを自動的に検出するか、Cisco Secure Workload のアプリケーション ワークスペースでセグメンテーションポリシーを手動で作成します。
5. アプリケーション ワークスペースでポリシーを適用すると、Secure Workload はセグメンテーションポリシーをアクセスコントロールルールとして Cisco Secure Firewall Management

Center にプッシュします。これらのルールのコンシューマとプロバイダーは、Cisco Secure Firewall Management Center 内でスコープ、インベントリフィルタ、およびクラスタからダイナミックオブジェクトに変換されます。

6. 変更は、Cisco Secure Firewall Management Center によって管理される Cisco Secure Firewall Threat Defense デバイスに自動的に展開されます。

7. Secure Workload は継続的に変更をチェックし、5 秒ごとに更新を自動的にプッシュします。

   スコープ、インベントリフィルタ、クラスタなどがソースとなるダイナミックオブジェクトは、ネットワーク上のワークロードインベントリへの追加、削除、および変更を反映して自動的に更新されます。これらの変更、およびアプリケーションワークスペースで適用するポリシー変更（ポリシーの順序を含む）は、Cisco Secure Firewall Threat Defense 管理対象デバイスで自動的に更新されます。

変換されたアクセス コントロール ポリシー ルール

次のタイプのアクセスコントロールルールが追加されます。

- プレフィックスが Workload_golden_ のルール

  ゴールデンルールと呼ばれるこれらのルールは、Cisco Secure Firewall の背後にあるワークロードにインストールされているすべての Secure Workload エージェントと Secure Workload が通信できるようにします。

- プレフィックスが Workload_ のルール

  これらは、適用が有効になっているアプリケーションワークスペースのセグメンテーションポリシーから変換されたルールです。

- プレフィックスが Workload_ca_ のルール

  これらは、適用されたアプリケーションワークスペースごとに変換された catch-all ルールです。Cisco Secure Workload バージョン 3.7 以降、FMC コネクタの設定中に [Secure Workload キャッチオールを使用する（Use Secure Workload Catch All）] オプションを選択した場合にのみ、Cisco Secure Workload のキャッチオールルールを使用できます。

- ダイナミックオブジェクトは次のプレフィックス付きで作成されます。WorkloadObj_

ルールの順序は、Secure Workload のポリシーおよびワークスペースの標準ポリシー適用順序と一致します。

FMC でこれらのルールを削除または変更すると、次回 Secure Workload が更新を FMC にプッシュするときに変更内容が上書きされます。

FMC で、この統合から独立した追加のアクセスコントロールルールを作成し、既存のルールを上書きするのではなくマージするように統合を設定した場合、独立したルールは、上記のプレフィックスのいずれかを使用して名前が付けられていない限り、この統合によって変更されません。

Cisco Secure Workload バージョン 3.7 および 3.6 に関する重要な情報

この統合では、Secure Workload アプリケーション ワークスペースでセグメンテーションポリシーを作成します。適用されるポリシーが Secure Workload によって Cisco Secure Firewall Management Center 内のアクセスコントロールルールに変換されます。

ネットワークインベントリは、セグメンテーションポリシーのベースとなる Secure Workload スコープ、インベントリフィルタ、およびクラスタによって動的に管理されます。ネットワークでワークロードが追加、変更、または削除されると、Cisco Secure Firewall Management Center 内のダイナミックオブジェクトが Secure Workload により自動的に更新されます。 対応するアクセスコントロールルールは、これらのダイナミックオブジェクトに基づきます。

プロセスの概要：

1. Secure Workload、Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense 製品を展開します。
2. Secure Workload で FMC 外部オーケストレータを作成し、Cisco Secure Firewall Management Center との通信を確立します。
3. セグメンテーションポリシーで使用するコンシューマとプロバイダーを定義するスコープ、インベントリフィルタ、およびクラスタを Secure Workload で作成します。

   （Secure Workload の「コンシューマ」と「プロバイダー」は、Cisco Secure Firewall Management Center の「送信元」と「宛先」におおまかに対応します。）
4. Secure Workload のアプリケーション ワークスペースで、セグメンテーションポリシーを手動で作成します。
5. アプリケーション ワークスペースでポリシーを適用すると、Secure Workload はセグメンテーションポリシーをアクセスコントロールルールとして Cisco Secure Firewall Management Center にプッシュします。これらのルールのコンシューマとプロバイダーは、Cisco Secure Firewall Management Center 内でスコープ、インベントリフィルタ、およびクラスタからダイナミックオブジェクトに変換されます。
6. 変更は、Cisco Secure Firewall Management Center によって管理される Cisco Secure Firewall Threat Defense デバイスに自動的に展開されます。
7. Secure Workload は継続的に変更をチェックし、5 秒ごとに更新を自動的にプッシュします。

   スコープ、インベントリフィルタ、クラスタなどがソースとなるダイナミックオブジェクトは、ネットワーク上のワークロードインベントリへの追加、削除、および変更を反映して自動的に更新されます。これらの変更、およびアプリケーション ワークスペースで適用するポリシー変更（ポリシーの順序を含む）は、Cisco Secure Firewall Threat Defense 管理対象デバイスで自動的に更新されます。

変換されたアクセス コントロール ポリシー ルール：詳細

- Cisco Secure Workload バージョン 3.7 では、Cisco Secure Workload から変換されたセグメンテーションポリシーが、アクセス コントロール ポリシーの各セクションのルールとして Cisco Secure Firewall Management Center に追加されます。絶対ポリシーは [必須（Mandatory）] ルールセクションに追加され、デフォルトポリシーは [デフォルト（Default ）] セクションに追加されます。
- Cisco Secure Workload バージョン 3.6 では、Cisco Secure Workload から変換されたセグメンテーションポリシーが、アクセス コントロール ポリシーの [Default（デフォルト）] セクションにルールとして追加されます。

次のタイプのアクセスコントロールルールが追加されます。

- プレフィックスが Workload_golden_ のルール

  ゴールデンルールと呼ばれるこれらのルールは、Cisco Secure Firewall の背後にあるワークロードにインストールされているすべての Secure Workload エージェントと Secure Workload が通信できるようにします。

- プレフィックスが Workload_ のルール

  これらは、適用が有効になっているアプリケーションワークスペースのセグメンテーションポリシーから変換されたルールです。

- プレフィックスが Workload_ca_ のルール

  これらは、適用されたアプリケーションワークスペースごとに変換された catch-all ルールです。Cisco Secure Workload バージョン 3.7 以降、FMC 外部オーケストレータの設定中に [Cisco Secure Workload キャッチオールを使用する（Use Cisco Secure Workload Catch All）] オプションを選択した場合にのみ、Cisco Secure Workload のキャッチオールルールを使用できます。

ルールの順序は、Secure Workload のポリシーおよびワークスペースの標準ポリシー適用順序と一致します。

FMC でこれらのルールを削除または変更すると、次回 Secure Workload が更新を FMC にプッシュするときに変更内容が上書きされます。

FMC で、この統合から独立した追加のアクセスコントロールルールを作成し、既存のルールを上書きするのではなくマージするように統合を設定した場合、独立したルールは、上記のプレフィックスのいずれかを使用して名前が付けられていない限り、この統合によって変更されません。

変換されたダイナミックオブジェクト：詳細

ダイナミックオブジェクトを表示するには、FMC Web インターフェイスに移動し、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [外部属性（External Attributes）] > [ダイナミックオブジェクト（Dynamic Objects）] を選択します。

Secure Workload スコープ、インベントリフィルタ、およびクラスタから変換されたダイナミックオブジェクトと、この統合に必要な追加のダイナミックオブジェクトは、Cisco Secure Workload

のバージョンに応じて、次のフォーマットで FMC のダイナミックオブジェクトのリストに表示されます。

- Cisco Secure Workload 3.7 の場合：
  - [名前（Name）] 列に、*WorkloadObj_<Secure Workload inventory filter name>* フォーマットでダイナミックオブジェクトがリストされます。
  - [説明（Description）] 列には、UUID が表示されます。いずれかのオブジェクトの UUID が見つからない場合は、Cisco Secure Workload インベントリ フィルタ名が表示されます。
- Cisco Secure Workload 3.6 の場合：ダイナミックオブジェクトは *WorkloadObj_* プレフィックス付きでリストされます。

これらのオブジェクトを編集する必要がある場合は、Secure Workload でスコープ、インベントリフィルタ、およびクラスタを編集します。FMC で行った変更は、次回 Secure Workload による統合の更新時に上書きされます。

メンバーシップは変更される可能性があるため、この統合によって生成されたダイナミックオブジェクトを他の目的で使用する場合は注意が必要です。

この統合は、他のメカニズムを使用して作成および維持されるダイナミックオブジェクトには影響しません。

Cisco Secure Workload バージョン 3.7 および 3.6 の展開の考慮事項

すべての 3.7 バージョンの場合：

Cisco Secure Firewall Management Center（旧称 Firepower Management Center）ごとにサポートされる FMC オーケストレータは 1 つだけです。

（注） Cisco Secure Workload FMC 外部オーケストレータは、FMC が応答を停止した場合にフェールオーバーを識別できます。フェールオーバーの場合、システムはメモリ内のデータをクリアし、アクティブな FMC インスタンスとの再同期を開始します。FMC が現在の構成を Cisco Secure Workload に複製するのに時間がかかりすぎて、外部オーケストレータがタイムアウトして同期を再試行する状況が発生する可能性があります。この構成同期のタイムアウトは 10 分です。

また、FMC は、FMC 7.2 の時点で（それ以前も含め）、単一のエンドポイントが過剰な数のクエリを使用しないように自身を保護します。FMC が 1 分間に 120 を超える要求を検出した場合、120 の要求に達した後 1 分間、HTTP 429 「Too Many Requests」で応答します。ほとんどの FMC エンドポイントでは、一括挿入と一括読み取りを使用することで、このスロットリングが回避されます。ただし、すべてのダイナミックオブジェクトのコンテンツを収集すると、それぞれに対する要求が発生します。

適切に動作する統合の制限は、Cisco Secure Workload オーケストレーターがポリシーのすべてのコンポーネントを取得するために要する時間に基づいています（上限 10 分）。各オブジェクト要求は、FMC のネットワーク遅延、モデル、および負荷の影響を受けます。

たとえば、最初の 1 分は一般的な FMC 情報（FTDS、ACP、およびドメインの数）の収集に費やされ、残りはダイナミックオブジェクト/インベントリフィルタ（540）の収集に 4.5 分、ポリシールールの同期に次の 4.5 分というように分割されます（11,250）。

したがって、製品統合の現在のバージョンの妥当な負荷は、10 分 = 1 分（セットアップ用）+（0.024 秒 * SW ポリシーのルールの数）+（0.5 秒 * 使用中のインベントリフィルタの数）になります。この制限を超えると、部分的な負荷が発生します。これは、FMC で ACP が「同期していない」状態のままであるときに示されます。

すべての 3.6 バージョンの場合：

Firepower Management Center ごとにサポートされる FMC オーケストレータは 1 つだけです。

バージョン 3.6.1.36 以降を使用しており、展開でドメインを使用している場合：

すべての Secure Workload ワークスペースで適用されるすべてのポリシーは、FMC オーケストレータ構成で指定したドメイン内のすべてのアクセス コントロール ポリシーにプッシュされます（1 つ以上の FTD デバイスに割り当てられていないアクセス コントロール ポリシーを除く）。

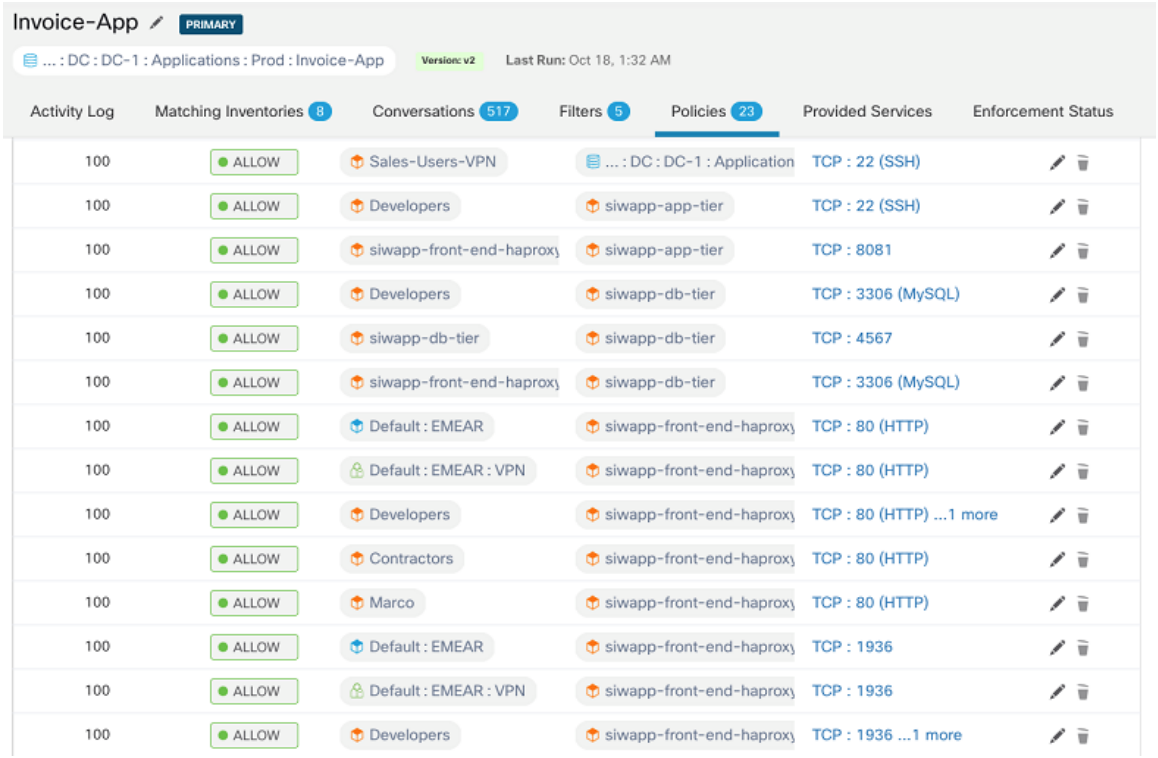
展開でドメインを使用していない場合、または 3.6.1.36 より前の 3.6 バージョンを使用している場合：

すべての Secure Workload ワークスペースで適用されたすべてのポリシーは、FTD デバイスに割り当てられているすべてのアクセス コントロール ポリシーにプッシュされます。

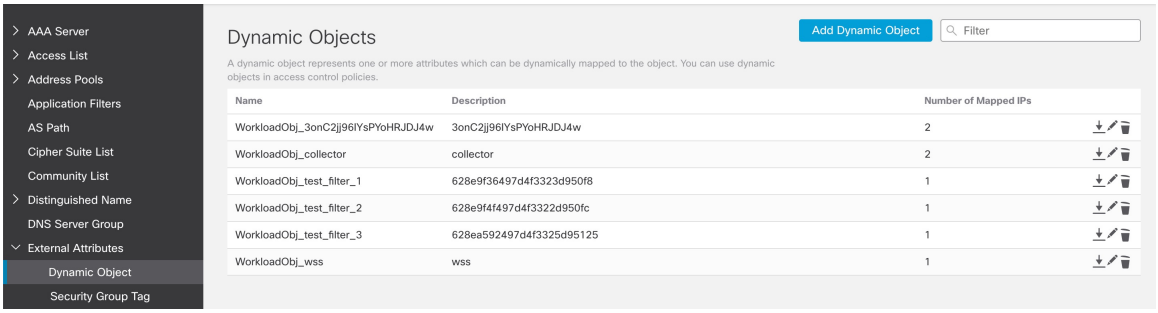
ダイナミックオブジェクトを使用した構成例

次の例は、Cisco Secure Workload バージョン 3.7 と Cisco Secure Firewall Management Center バージョン 7.0.1 の統合です。

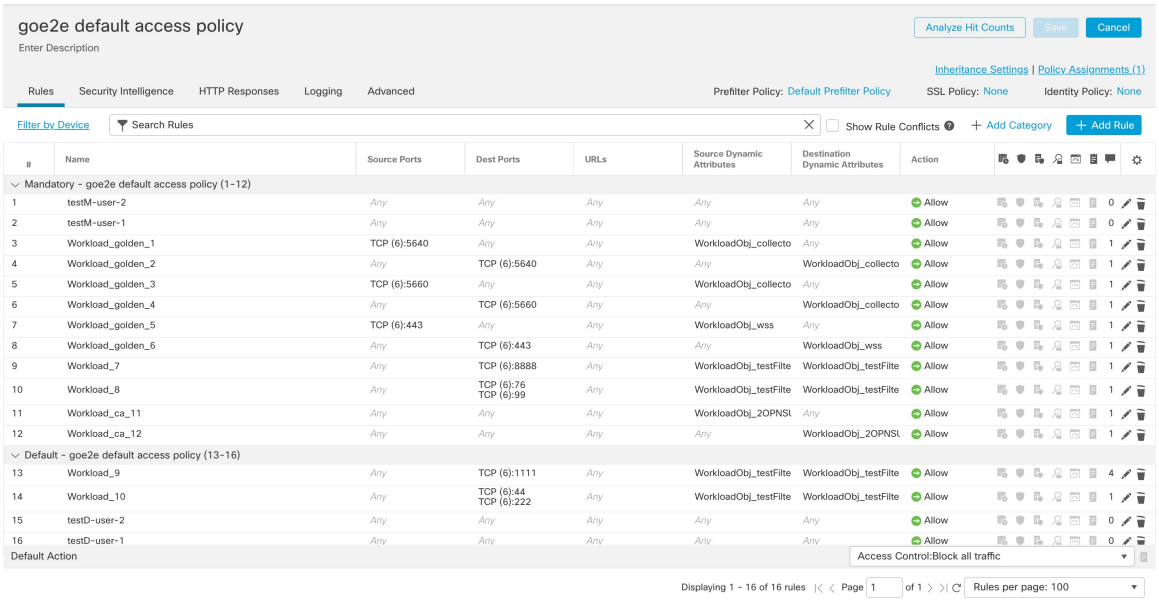
Cisco Secure Workload のセグメンテーションポリシー



FMC のダイナミックオブジェクト

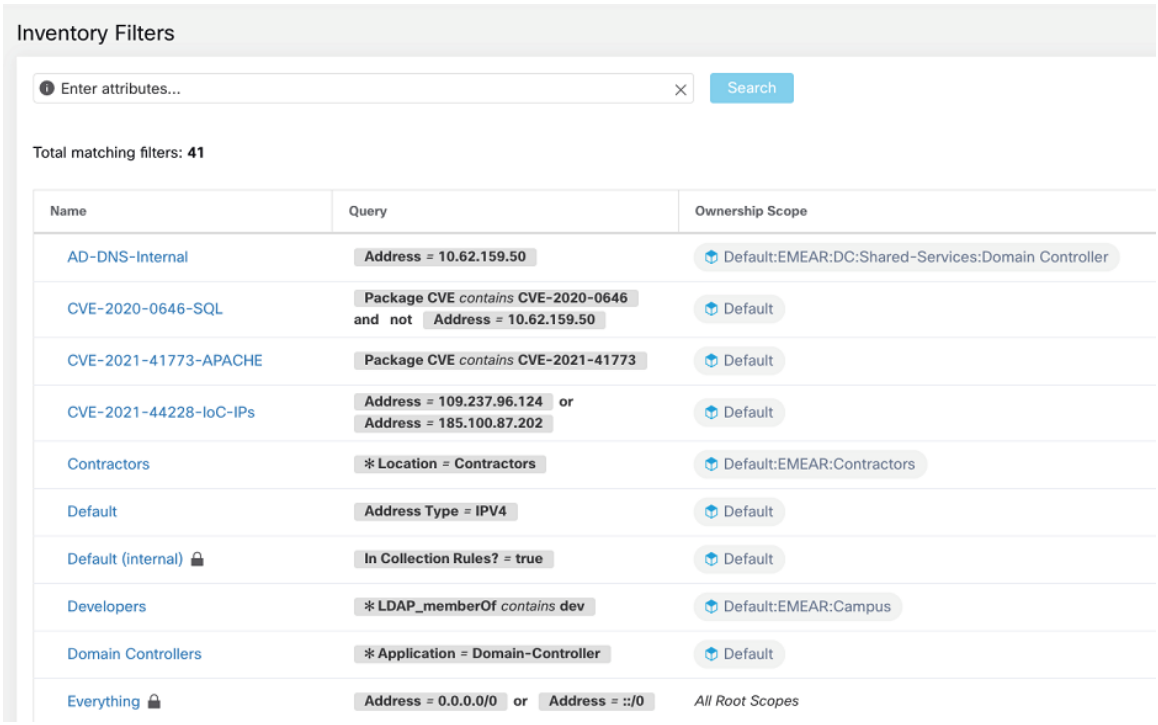


FMC のアクセス コントロール ポリシー



Cisco Secure Workload のスコープとインベントリ

Cisco Secure Workload のフィルタ



サポートされる展開

製品バージョン

主な機能	Cisco Secure Workload バージョン	Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense バージョン
• FMC オンボーディングを簡素化する FMC コネクタ。 • ACP からスコープへのマッピングを使用して、トポロジ認識型適用を実行する機能。 • ワークロードから CVE を公開するための仮想パッチ適用。	3.8.1.1	セグメンテーションと仮想パッチ適用のための 7.2 仮想パッチ適用のための 7.1.x セグメンテーションのための 7.0.1

主な機能	Cisco Secure Workload バージョン	Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense バージョン
• FMC のアクセス コントロール ポリシーの [必須（Mandatory）] セクションと [デフォルト（Default）] セクションにルールとして表示される Cisco Secure Workload セグメンテーションポリシーの優先順位を変更する機能。 • アクセス コントロール ポリシーのデフォルトアクションである、CSW キャッチオールルールまたはFMC の同等のルールのいずれかを使用する機能。	3.7.1.5	7.1 7.0.1
ダイナミックオブジェクトでアクセス コントロール ポリシーを使用する場合のFMC ドメインのサポート	3.6.1.36	7.1 7.0.1
ダイナミックオブジェクトによるアクセス コントロール ポリシー （注） プレフィルタポリシーは、Cisco Secure Workload バージョン 3.6 以降ではサポートされていません。	3.6	7.1 7.0.1
プレフィルタ ポリシー	3.5	7.0 6.7 6.6

サポートされている Cisco Secure Firewall プラットフォームと展開

- Cisco Secure Firewall Management Center によって管理される Cisco Secure Firewall Threat Defense デバイスのみがサポートされています。
- 設定されている場合は、FMC 高可用性がサポートされます。

  FMC 外部オーケストレータの設定時にスタンバイ/セカンダリ FMC のホスト名/IP アドレスを含めると、FMC が新しいアクティブ プライマリ アプライアンスに切り替わると、統合が自動的に切り替わり、新しいアクティブ FMC が使用されます。
- Cisco Secure Firewall Threat Defense（FTD）ルーテッドファイアウォールおよびトランスペアレント ファイアウォールの両方のモードがサポートされています。

  Cisco Secure Firewall Threat Defense モードの詳細については、該当するバージョンの『*Cisco Secure Firewall Management Center Configuration Guide*』の「Transparent or Routed Firewall Mode for Cisco Secure Firewall Threat Defense」の章を参照してください。

Secure Workload バージョン 3.7 および 3.6 の追加要件

この統合には専用の FMC を使用することが推奨されます。

Cisco Tetration バージョン 3.5 の追加要件

FTD は、Tetration との統合にのみ使用される専用ドメインに割り当てる必要があります。これは、割り当てられた FTD が Tetration ポリシーのプッシュ先となる唯一のデバイスとなるようにするためです。

新しいドメインの作成、ドメインの管理、およびドメイン間のデバイスの移動の詳細については、該当する Firepower のバージョンの『Firepower Management Center Configuration Guide』の、「Deployment Management」の章にある「Domain Management」セクションを参照してください。例：Firepower Management Center Configuration Guide, Version 6.7

.

Cisco Secure Workload バージョン 3.8.1.1 でのこの統合の導入

このセクションは、すべてのバージョン 3.8 ビルドに適用されます。

アップグレードについて

Cisco Secure Workload バージョン 3.8.1.1 へのアップグレード

- バージョン 3.7.1.5 からのアップグレード

  FMC 外部オーケストレータは Cisco Secure Firewall に移行されます。

  アップグレード前の構成は変更されません。

バージョン 3.8.1.1 にアップグレードした後、次を実行できます。

- エージェントベースのワークロードからの CVE 情報を Cisco Secure Firewall Management Center に公開し、ファイアウォールの推奨事項を実行して IPS ポリシーを微調整します。
- アクセス コントロール ポリシーの [必須（Mandatory）] または [デフォルト（Default）] セクションの下にリストするセグメンテーションポリシーの優先順位を設定します。
- Cisco Secure Workload キャッチオールルールを使用するオプションを有効または無効にするには、FMC コネクタを設定するときに、[Secure Workloadキャッチオールを使用する（Use Secure Workload Catch All）] オプションを選択またはクリアします。

統合の前提条件：Cisco Secure Workload バージョン 3.8.1.1

- サポートされている Firepower Management Center（FMC）と、サポートされている少なくとも 1 つの Cisco Secure Firewall Threat Defense（FTD）デバイスが設定されている。FTD デバイスを FMC に関連付け、各 FTD をアクセス コントロール ポリシーに割り当て、ポリシーを FMC から FTD に展開できること、およびシステムがネットワークトラフィックを予期したとおりに処理していることが確認済みである。

  詳細については、Cisco Secure Firewall Management Center ドキュメントロードマップを含め、製品の Cisco Secure Firewall Management Center ドキュメントを参照してください。
- Secure Workload アプライアンス（オンプレミス）またはアカウント（Software as a Service（SaaS））が設定され、予期したとおりに動作している。
- Secure Workload Software as a Service（SaaS）を使用している場合、またはオンプレミスの Secure Workload が FMC アプライアンスに直接到達できない場合は、セキュアコネクタトンネルを設定してソリューション コンポーネント間の接続を提供します。

  デフォルトでは、Secure Workload はポート 443 の HTTPS を使用して FMC REST API と通信します。

  セキュアコネクタの設定手順については、Secure Workload Web インターフェイスのオンラインヘルプとして利用できる Secure Workload ユーザーガイドを参照してください。

Cisco Secure Workload バージョン 3.8.1.1 でのこの統合の導入方法

次の表に、Cisco Secure Firewall Management Center を設定し、Secure Workload バージョン 3.8.1.1 リリースとの統合を設定するエンドツーエンドのワークフローを示します。

ステップ	説明	詳細情報
はじめる前に	この統合がどのように機能するか、統合を導入するための高レベルのプロセスの概要、および展開における考慮事項を理解します。	Cisco Secure Workload バージョン 3.8 に関する重要な情報 （2 ページ） のすべてのセクションとトピックを参照してください。

ステップ	説明	詳細情報
はじめる前に	要件および前提条件を満たします	以下のすべてのセクションを参照してください： サポートされる展開 （13 ページ） および 統合の前提条件：Cisco Secure Workload バージョン 3.8.1.1 （16 ページ）。
1	Secure Workload で、次の手順を実行します。 現在の環境のスコープ、インベントリフィルタ、クラスタ、ワークスペース、およびセグメンテーションポリシーを定義します。	アプリケーションの依存関係マッピングを使用してポリシーを自動的に検出するか、Cisco Secure Workload のアプリケーション ワークスペースでセグメンテーションポリシーを手動で作成します これについて質問がある場合は、Secure Workload Web インターフェイスからオンラインヘルプとして利用できる Secure Workload ユーザーガイドの「Segmentation」セクションを参照してください。 もう 1 つの方法としては、詳細設定：ADM を使用してセグメンテーションポリシーを生成する （48 ページ）を参照してください。
2	FMC の場合： Cisco Secure Firewall Threat Defense に割り当てられた各アクセス コントロール ポリシーの下部で、ポリシーの [デフォルトアクション（Default Action）] を設定します。	このアクションは、作成するセグメンテーションポリシーによって異なります。たとえば、セグメンテーションポリシーで明確に許可されているトラフィック以外のすべてのトラフィックをブロックする場合は、[すべてのトラフィックをブロック（Block all traffic）] を選択します。

ステップ	説明	詳細情報
3	FMC の場合： この統合専用のユーザーアカウントを作成します。	このユーザーアカウントの要件： • アカウントは、管理者ロールを持っている必要があります。 • （ドメインが FMC で設定されている場合）アカウントは [グローバル（Global）] ドメインにアクセスできる必要があります。 FMC でのユーザーアカウントの作成について質問がある場合は、Cisco Secure Firewall Management Center のオンラインヘルプで「Add an Internal User」のトピックを参照してください。
4	Secure Workload で、次の手順を実行します。 FMC コネクタを作成します。	Cisco Secure Firewall Management Center ごとに FMC コネクタを 1 つだけ作成します。 FMC コネクタを作成するには、バージョン 3.8.1.1 での FMC コネクタの設定 （19 ページ）セクションを参照してください。
5	Secure Workload で、次の手順を実行します。 アクセス コントロール ポリシーをスコープにマッピングします。	[管理（Manage）] > [ワークロード（Workloads）] > [コネクタ（Connectors）] > [セグメンテーション（Segmentation）] で、ACP マッピングを作成します。
6	Secure Workload で、次の手順を実行します。 仮想パッチ適用ルールを作成します。	[管理（Manage）] > [ワークロード（Workloads）] > [コネクタ（Connectors）] > [仮想パッチ適用（Virtual Patching）] で、仮想パッチ適用ルールを作成します。公開された CVE を持つワークロードが表示されます。
7	Secure Workload で、次の手順を実行します。 目的のワークスペースにポリシーを適用します。	ワークスペースで、[適用（Enforcement）] タブをクリックし、[ポリシーの適用（Enforce Policies）] ボタンをクリックしてウィザードを完了します。

ステップ	説明	詳細情報
8	アクセス コントロール ポリシーに新しいルールが表示されるまで待ちます。	これに要する時間は、転送されるデータの量、マシンの速度、ネットワーク帯域幅などに応じて異なります。 ルールを表示するには、次の手順を実行します。 FMC で、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して、表示するポリシーをクリックします。
9	新しいアクセス コントロール ポリシーは、関連する管理対象の Cisco Secure Firewall Threat Defense デバイスに自動的に展開されます。	将来の変更も、Cisco Secure Firewall Threat Defense デバイスに自動的に展開されます。 今後、新しい FTD を既存のアクセス コントロール ポリシーに関連付けると、新しい FTD は自動的に現在のルールを受信します。

バージョン 3.8.1.1 での FMC コネクタの設定

はじめる前に

「Implementing This Integration for Secure Workload Version 3.8.1.1」のここまでの手順を完了します。

設定

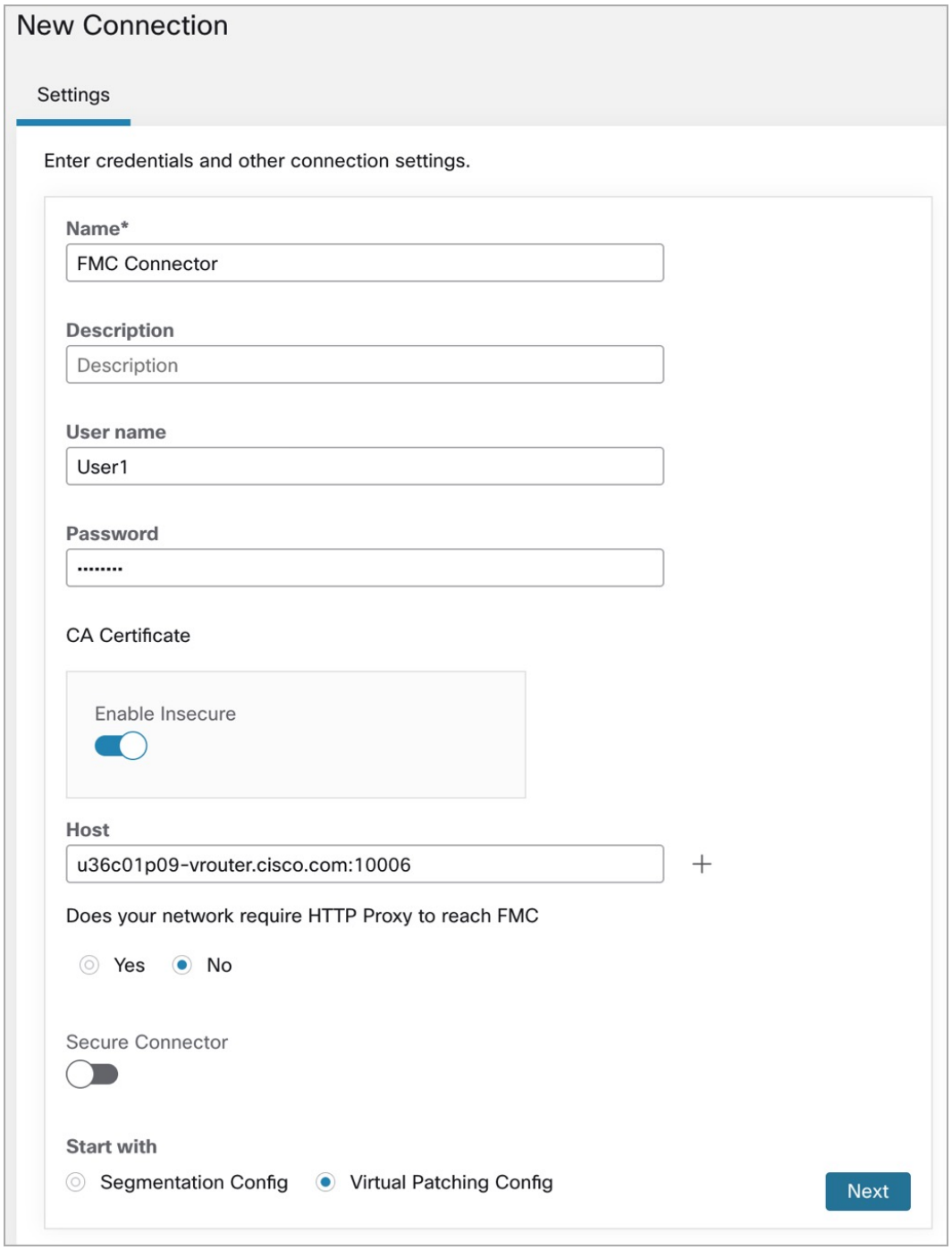
Cisco Secure Workload で FMC コネクタを作成し、Cisco Secure Firewall Management Center との通信を確立します。

1. [管理（Manage）] > [ワークロード（Workloads）] > [コネクタ（Connectors）] に移動します。
2. [ファイアウォール（Firewall）] で、[Cisco Secure Firewall] を選択します。
3. [ここに新しいコネクタを設定する（Configure your new connector here）] をクリックします。
4. [新しい接続（New Connection）] ページで、クレデンシャルとその他の接続設定を以下のように入力します。

フィールド	説明
名前	FMC コネクタの一意の名前を入力します。
説明（Description）	説明を入力します。

フィールド	説明
ユーザー名とパスワード	FMC との通信に使用するクレデンシャルを入力します。
[CA証明書（CA Certificate）]	Cisco Secure Workload がこの FMC の認証に使用する CA 証明書を入力するか、ネットワークが信頼されていて、Cisco Secure Workloadが証明書を検証しない場合は、[非セキュアを有効にする（Enable Insecure）] ことができます。 CA 証明書は、オブジェクト管理ワークフローを使用して FMC から取得できます。
ホスト（Host）	関連付けられているFMCのホスト名とポート番号は、<FQDN> : <Port> または <IP> : <Port> の形式で入力します ホスト名は、FMC の完全修飾ドメイン名または IP にする必要があります。
ネットワークは、FMC に到達するために HTTP プロキシを必要としますか	<proxy.host> : <proxy.port> の形式でプロキシ URL を入力します
[セキュアコネクタ（Secure Connector）]	セキュアコネクタを使用して Cisco Secure Workloadから FMC への接続をトンネリングする場合に有効にします。 このオプションを有効にする前に、セキュアコネクタを展開しておく必要があります。
から開始	まず、[セグメンテーション（Segmentation）] [設定（Config）] または [仮想パッチ適用設定（Virtual Patching Config）] のいずれかを選択します。 a）[セグメンテーション設定（Segmentation Config）] : アクセスコントロールポリシーをスコープに割り当て、追加のパラメータを設定します。 b）[仮想パッチ適用設定（Virtual Patching Config）] : FMC に公開する CVE のルールを設定します。

5. [次へ（Next）] をクリックします。



セグメンテーション

Cisco Secure Workload により適用されるセグメンテーションポリシーは、Cisco Secure Firewall Management Center でダイナミックオブジェクトに変換されたスコープ、インベントリフィルタ、およびクラスタから取得された IP アドレスに基づいてアクセス コントロール ポリシーに変換されます。

Cisco Secure Workload では、Cisco Secure Workload から変換されたセグメンテーションポリシーが、アクセス コントロール ポリシーの各セクションのルールとして Cisco Secure Firewall Management Center に追加されます。絶対ポリシーは [必須（Mandatory）] ルールセクションに追加され、デフォルトポリシーは [デフォルト（Default）] ルールセクションに追加されます。

次のタイプのアクセスコントロールルールが追加されます。

- プレフィックスが Workload_golden_ のルール：

  ゴールデンルールと呼ばれるこれらのルールは、Cisco Secure Firewall の背後にあるワークロードにインストールされているすべての Cisco Secure Workload エージェントと Cisco Secure Workload が通信できるようにします。

- プレフィックスが Workload_ のルール：

  これらは、適用が有効になっているアプリケーションワークスペースのセグメンテーションポリシーから変換されたルールです。

- プレフィックスが Workload_ca_ のルール：

  これらは、適用されたアプリケーションワークスペースごとに変換された catch-all ルールです。Cisco Secure Workload バージョン以降、FMC コネクタの設定中に [Secure Workload キャッチオールを使用する（Use Secure Workload Catch-All）] オプションを選択した場合にのみ、Cisco Secure Workload のキャッチオールルールを使用できます。

- ダイナミックオブジェクトは次のプレフィックス付きで作成されます。WorkloadObj_

（注）

- FMC でこれらのルールを削除または変更すると、次回 Cisco Secure Workload が更新を FMC にプッシュするときに変更内容が上書きされます。
- FMC で、この統合から独立した追加のアクセスコントロールルールを作成し、既存のルールを上書きするのではなくマージするように統合を設定した場合、独立したルールは、上記のプレフィックスのいずれかを使用して名前が付けられていない限り、この統合によって変更されません。

ACP マッピングの作成

1. [設定（Settings）] で [セグメンテーション設定（Segmentation Config）] が選択されている場合は、[ACPマッピングの作成（Create ACP Mapping）] ウィンドウに移動します。
2. ドロップダウンから [アクセスポリシー（Access Policy）] を選択し、[スコープ（Scope）] にマッピングします。 アクセスポリシーは、1 つのスコープにのみマッピングできます。
3. [Secure Workloadキャッチオールを使用する（Use Secure Workload Catch All）] チェックボックスをオンにして、Cisco Secure Workload からのキャッチオールルールを有効にします。キャッチオール Cisco Secure Workload ルールは、アクセス コントロール ポリシーの [デフォルト（Default）] セクションで、他のすべてのルール（Cisco Secure Workload ルールおよび FMC で直接作成されたルール（ある場合））の後にリストされます。Cisco Secure

Workload のキャッチオールルールを無効にする場合は、このオプションの選択を解除して、FMC アクセス コントロール ポリシーのデフォルトアクションを使用します。

4. [適用モード（Enforcement Mode）] でオプションを選択します。

   - [マージ（Merge）] : ユーザーが作成した既存のルールとともに、Cisco Secure Workload ポリシールールが追加されます。次のステップで説明するように、優先順位を設定できます。
   - [オーバーライド（Override）] : ユーザーが作成した既存のルールは、Cisco Secure Workload ポリシールールに置き換えられます。

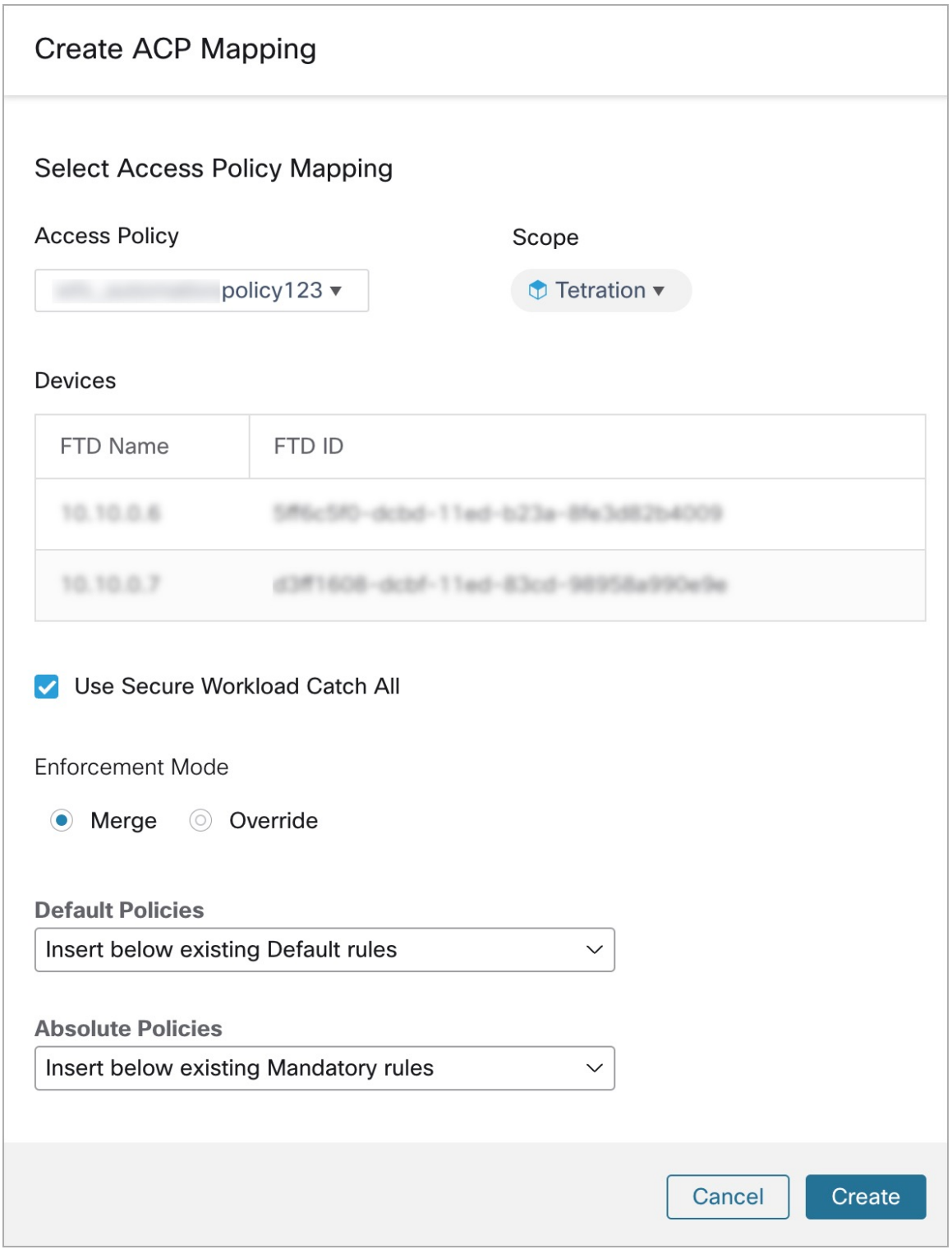
（注） 優先順位ドロップダウン メニュー オプションは、適用モードとして [マージ（Merge）] が選択されている場合にのみ使用できます。

5. [絶対値（Absolute）] および [デフォルトポリシー（Default Policies）] ドロップダウンメニューで、必要なオプションを選択して、FMC のアクセス コントロール ポリシーのそれぞれのセクションにある既存のルールの上または下に Cisco Secure Workload ポリシーの優先順位を設定します。

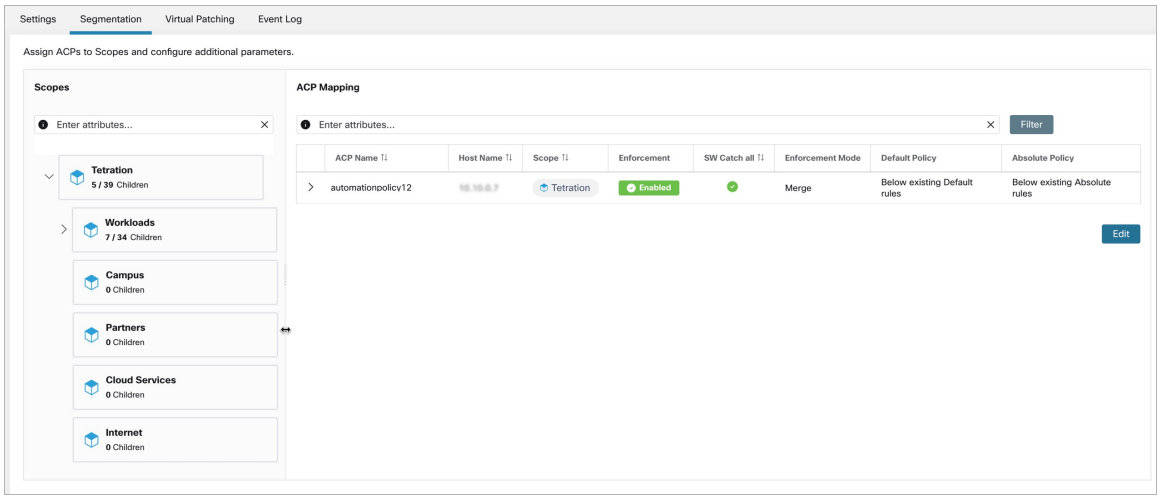
   - [既存の必須ルールの上に挿入（Insert above existing Mandatory rules）] を選択すると、Cisco Secure Workload ポリシーの優先順位が必須ルールより高くなります。
   - [既存の必須ルールの下に挿入（Insert below existing Mandatory rules）] を選択すると、Cisco Secure Workload ポリシーの優先順位が必須ルールより低くなります。

   たとえば、[絶対ポリシー（Absolute Policies）] ドロップダウンメニューで、[既存の必須ルールの上に挿入（Insert above existing Mandatory rules）] を選択すると、Cisco Secure Workload ルールが [必須（Mandatory）] セクションの先頭に設定され、続いて Cisco Secure Firewall Management Center の既存のアクセスコントロールルールが設定されます。新しいルールが作成されると、アクセス コントロール ポリシーのルールの順序は、Cisco Secure Workload のポリシーに対して選択された優先順位に基づいて更新されます。

図 *2:*

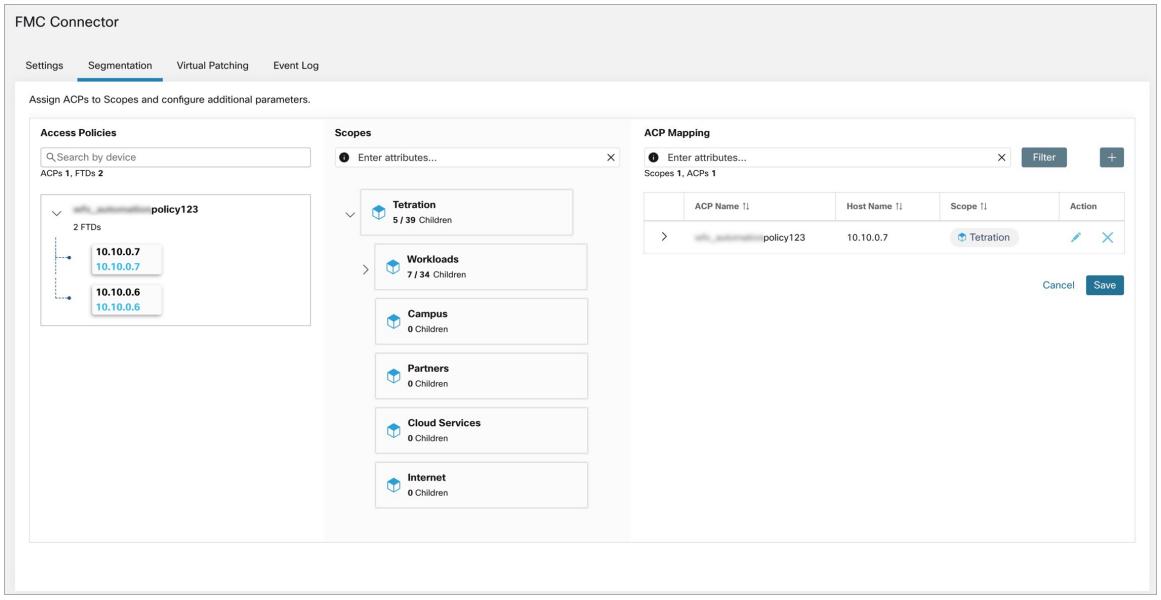


6. [作成（Create）] をクリックします。



ACP マッピングの編集

1. [セグメンテーション（Segmentation）] タブで、[編集（Edit）] をクリックします。
2. [アクション（Action）] で、編集アイコンをクリックします。



3. 必要な変更を行って、[保存（Save）] をクリックします。
4. [+] アイコンをクリックして、別の ACP をスコープにマップします。
5. [保存（Save）] をクリックして、すべての編集を保存します。

仮想パッチ適用

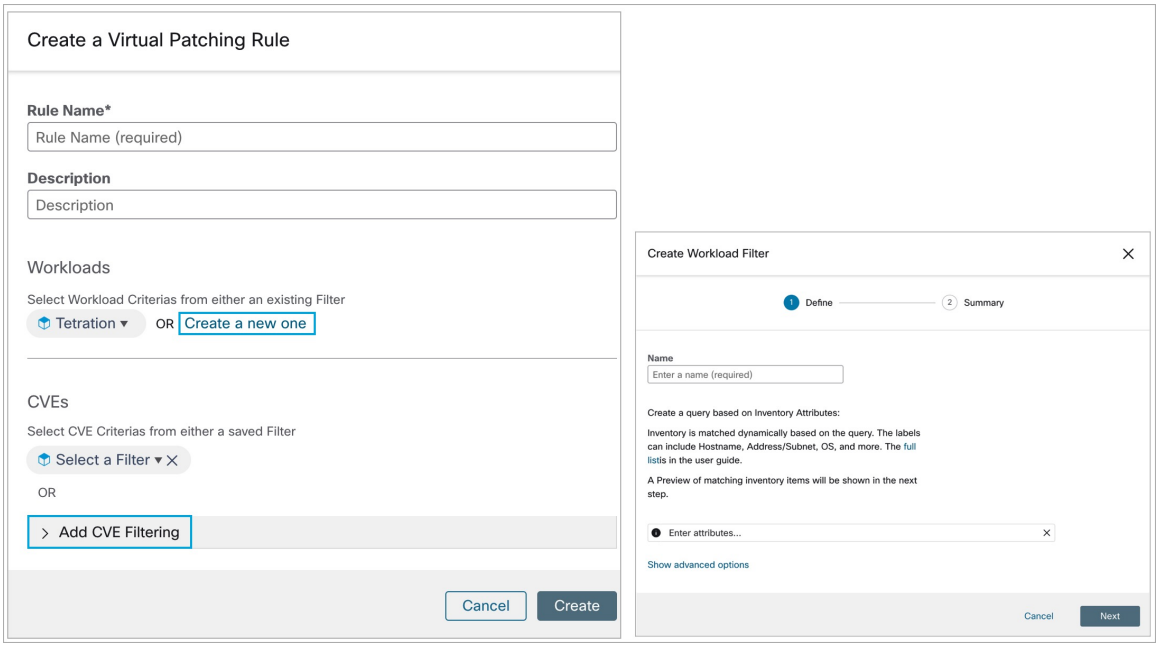
アプリケーションとコンピュータシステムを既知の脆弱性から保護するために、仮想パッチ適用と呼ばれるセキュリティ技術（外部パッチ、Web アプリケーション ファイアウォール

（WAF）、ジャストインタイムパッチ適用とも呼ばれます）が使用されます。もともと侵入防御システム（IPS）で使用されていた仮想パッチ適用は、永続的なパッチが開発および適用されるまで、脆弱性またはセキュリティ上の欠陥に対処するための一時的な修正または回避策を実装します。

たとえば、ソフトウェア開発ライフサイクルに従う組織は、アプリケーションの新しいバージョンを検出、修正、および開発するのに時間がかかります。ファイアウォールを導入し、IPS ルールを追加することで、アプリケーションの新しいバージョンが導入されるまでシステムを保護できます。Cisco Secure Workload は、IPS ポリシーの作成中に考慮すべき CVE をファイアウォールに公開します。

1. [設定（Settings）] で [仮想パッチ適用設定（Virtual Patching Config）] が選択されている場合、[仮想パッチ適用ルールの作成（Create a Virtual Patching Rule）] ウィンドウに移動します。
2. [ルール名（Rule Name）] と [説明（Description）] を入力します。
3. 既存のワークロードフィルタを選択することも、新しいワークロードフィルタを作成することもできます。
4. 既存の CVE フィルタを選択することも、CVE クエリを入力して CVE フィルタを追加することもできます。
5. [作成（Create）] をクリックします。
6. [仮想パッチ適用（Virtual Patching）] タブの [ルール（Rules）] で、[ルールの追加（Add Rule）] をクリックして 1 つ以上のルールを追加します。

   図 *3*:



7. 追加された仮想パッチ適用ルールは、[ルール（Rules）] の下に表示されます。

- [ルール名（Rule name）] と [説明（Description）] で検索できます。
- [フィルタ（filter）] アイコンをクリックして、表示する列を選択します。
- [アクション（Actions）] で、[編集（edit）] アイコンをクリックして、仮想パッチ適用ルールの詳細を変更します。
- [アクション（Actions）] で、[ゴミ箱（bin）] アイコンをクリックして、仮想パッチ適用ルールを削除します。

8. 公開された CVE を持つワークロードが右側に表示されます。
   - ルール名、インベントリフィルタ、ワークロード、最低スコアなどの属性を入力してフィルタリングできます。
   - メニューアイコンをクリックして、JSONおよび/またはCSV形式で詳細をダウンロードします。
   - 列ヘッダーをクリックしてエントリをソートします。
   - [エクスポート済み（Exported）] 列で、[CVEリスト（CVEs List）] をクリックして、ワークロードの公開されたすべての CVE のリストを表示します。
   - ハンバーガーメニューをクリックして、ワークロードの [監査ログ（Audit Log）] を表示します。過去 48 時間のログが保存され、表示されます。

イベント ログ

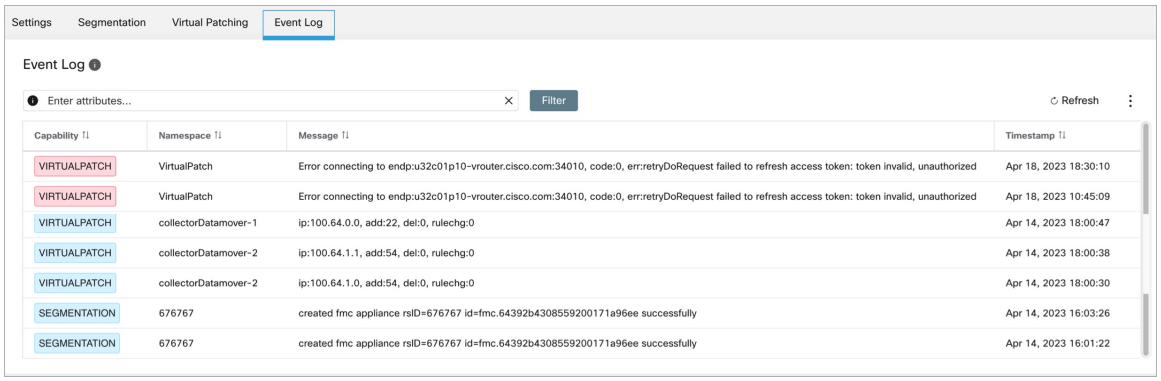
Cisco Secure Workload および Cisco Secure Firewall Management Center での重要なイベントまたはトランザクションは、[イベントログ（Event log）] タブに一覧表示されます。Cisco Secure Workload - Cisco Secure Firewall Management Center 統合に関連するメッセージも表示されます。

1. 属性を入力して、機能、イベントレベル、名前空間、およびメッセージに基づいてイベントをフィルタリングします。

（注） イベントレベルのカラーコードは、情報（青）、警告（オレンジ）、エラー（赤）です。

2. 列ヘッダーをクリックしてエントリをソートします。
3. 3 つのドットメニューアイコンをクリックして、JSON および/または CSV 形式で詳細をダウンロードします。
4. すべてのフィルタをリセットするには、[更新（Refresh）] をクリックします。

図 *4:* イベント ログ



Cisco Secure Workload バージョン 3.7.1.5 でのこの統合の導入

このセクションは、すべてのバージョン 3.7 ビルドに適用されます。

アップグレードについて

Cisco Secure Workload バージョン 3.7.1.5 へのアップグレード

- バージョン 3.6.1.36 からのアップグレード：

  アップグレード前の構成は変更されません。

- 3.6.1.36 より前の 3.6.x バージョンからのアップグレード：

  ドメインが Firepower Management Center で設定されており、オーケストレータで適用が有効になっている場合：

  デフォルトでは、すべてのドメインが適用対象として選択されています。

バージョン 3.7.1.5 にアップグレードした後、次を実行できます。

- アクセス コントロール ポリシーの [必須（Mandatory）] または [デフォルト（Default）] セクションの下にリストするセグメンテーションポリシーの優先順位を設定します。
- Cisco Secure Workload キャッチオールルールを使用するオプションを有効または無効にするには、FMC 外部オーケストレータを設定するときに、[Cisco Secure Workload キャッチオールを使用する（Use Secure Workload Catch All）] オプションを選択またはクリアします。

統合の前提条件：Cisco Secure Workload バージョン 3.7.1.5

- サポートされている Firepower Management Center（FMC）と、サポートされている少なくとも 1 つの Cisco Secure Firewall Threat Defense（FTD）デバイスが設定されている。FTD デバイスを FMC に関連付け、各 FTD をアクセス コントロール ポリシーに割り当て、ポ

リシーを FMC から FTD に展開できること、およびシステムがネットワークトラフィックを予期したとおりに処理していることが確認済みである。

詳細については、Cisco Secure Firewall Management Center ドキュメントロードマップを含め、製品の Cisco Secure Firewall Management Center ドキュメントを参照してください。

- Secure Workload アプライアンス（オンプレミス）またはアカウント（Software as a Service（SaaS））が設定され、予期したとおりに動作している。
- Secure Workload Software as a Service（SaaS）を使用している場合、またはオンプレミスの Secure Workload が FMC アプライアンスに直接到達できない場合は、セキュアコネクタトンネルを設定してソリューション コンポーネント間の接続を提供します。

  デフォルトでは、Secure Workload はポート 443 の HTTPS を使用して FMC REST API と通信します。

  セキュアコネクタの設定手順については、Secure Workload Web インターフェイスのオンラインヘルプとして利用できる Secure Workload ユーザーガイドを参照してください。

Cisco Secure Workload バージョン 3.7.1.5 でのこの統合の導入方法

次の表に、Cisco Secure Firewall Management Center を設定し、Secure Workload バージョン 3.7.1.5 リリースとの統合を設定するエンドツーエンドのワークフローを示します。

ステップ	説明	詳細情報
はじめる前に	この統合がどのように機能するか、統合を導入するための高レベルのプロセスの概要、および展開における考慮事項を理解します。	Cisco Secure Workload バージョン 3.7 および 3.6 に関する重要な情報 （6 ページ） のすべてのセクションとトピックを参照してください。
はじめる前に	要件および前提条件を満たします	以下のすべてのセクションを参照してください： サポートされる展開 （13 ページ） および 統合の前提条件：Cisco Secure Workload バージョン 3.7.1.5 （28 ページ）。

ステップ	説明	詳細情報
1	Secure Workload で、次の手順を実行します。 現在の環境のスコープ、インベントリフィルタ、クラスタ、ワークスペース、およびセグメンテーションポリシーを定義します。	Cisco Secure Firewall のダイナミックオブジェクトによって定義される一連のワークロードに適用するセグメンテーションポリシーを手動で作成します。 これについて質問がある場合は、Secure Workload Web インターフェイスからオンラインヘルプとして利用できる Secure Workload ユーザーガイドの「Segmentation」セクションを参照してください。 もう 1 つの方法としては、詳細設定：ADM を使用してセグメンテーションポリシーを生成する （48 ページ）を参照してください。
2	FMC の場合： Cisco Secure Firewall Threat Defense に割り当てられた各アクセス コントロール ポリシーの下部で、ポリシーの [デフォルトアクション（Default Action）] を設定します。	このアクションは、作成するセグメンテーションポリシーによって異なります。たとえば、セグメンテーションポリシーで明確に許可されているトラフィック以外のすべてのトラフィックをブロックする場合は、[すべてのトラフィックをブロック（Block all traffic）] を選択します。
3	FMC の場合： この統合専用のユーザーアカウントを作成します。	このユーザーアカウントの要件： • アカウントは、管理者ロールを持っている必要があります。 • （ドメインが FMC で設定されている場合）アカウントは [グローバル（Global）] ドメインにアクセスできる必要があります。 FMC でのユーザーアカウントの作成について質問がある場合は、Cisco Secure Firewall Management Center のオンラインヘルプで「Add an Internal User」のトピックを参照してください。

ステップ	説明	詳細情報
4	Secure Workload で、次の手順を実行します。 FMC オーケストレータを作成します。	Cisco Secure Firewall Management Center ごとに FMC オーケストレータを 1 つだけ作成します。 OpenAPI を使用して FMC オーケストレータを作成するには、Secure Workload Web ポータルのユーザーガイドの「バージョン 3.7.1.5 での FMC オーケストレータの設定 （32 ページ）」セクションを参照してください。
5	Secure Workload で、次の手順を実行します。 目的のワークスペースにポリシーを適用します。 （これは、FMC オーケストレータでの適用の有効化とは別の操作です）。	ワークスペースで、[適用（Enforcement）] タブをクリックし、[ポリシーの適用（Enforce Policies）] ボタンをクリックしてウィザードを完了します。
6	オーケストレータの適用を有効にします。 FMC オーケストレータでドメインをまだ選択していない場合は、ここで選択します。	FMC オーケストレータを編集してドメインを選択します。(FMC にドメインが設定されていない場合は、[グローバル（Global）] ドメインを選択する必要があります。) ドメインを選択した後に [更新（Update）] をクリックすると、オーケストレータの適用が有効になり、管理対象の FTD デバイスに Secure Workload ポリシーが展開されます。 詳細については、バージョン 3.7.1.5 での FMC オーケストレータの編集 （36 ページ）を参照してください。
7	アクセス コントロール ポリシーに新しいルールが表示されるまで待ちます。	これに要する時間は、転送されるデータの量、マシンの速度、ネットワーク帯域幅などに応じて異なります。 ルールを表示するには、次の手順を実行します。 FMC で、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して、表示するポリシーをクリックします。

ステップ	説明	詳細情報
8	新しいアクセス コントロール ポリシーは、関連する管理対象の Cisco Secure Firewall Threat Defense デバイスに自動的に展開されます。	将来の変更も、Cisco Secure Firewall Threat Defense デバイスに自動的に展開されます。 今後、新しい FTD を既存のアクセス コントロール ポリシーに関連付けると、新しい FTD は自動的に現在のルールを受信します。

バージョン 3.7.1.5 での FMC オーケストレータの設定

始める前に

Cisco Secure Workload バージョン 3.7.1.5 でのこの統合の導入 （28 ページ） の表の、ここまでの手順を完了します。

手順

ステップ 1 Secure Workload Web インターフェイスで、[管理（Manage）]>[外部オーケストレータ（External Orchestrators）] を選択します。

ステップ 2 [新規設定の作成（Create New Configuration）] をクリックします。

ステップ 3 [基本設定（Basic Config）] タブで、次のフィールドを設定します。

オプション	説明
タイプ（Type）	[FMC] を選択します。
名前（Name）	FMC オーケストレータの一意の名前を入力します。
説明（Description）	オーケストレータの説明を入力します。
フルスナップショット間隔（Full Snapshot Interval(s)）	フルスナップショットの間隔を秒単位で入力します。 [フルスナップショット間隔（Full Snapshot Interval(s)）] フィールドは、FMC 外部オーケストレータが FMC と Secure Workload の接続をテストする頻度を指定します。エラーが発生した場合（たとえば、ネットワークの問題により FMC に到達できない場合、または無効なエンドポイントやユーザー クレデンシャルが使用された場合）、FMC オーケストレータは [ステータス（Status）] フィールドにエラーを報告します。 デフォルト値：3600 秒

オプション	説明
ユーザー名（Username） **パスワード（Password）**	このドキュメントで前述した、FMC で作成した専用ユーザのユーザー名とパスワードを入力します。 これらのクレデンシャルは、FMC との通信に使用されます。
CA 証明書（CA Certificate）	Secure Workload がこの FMC の認証に使用する CA 証明書を入力します。この証明書は、オブジェクト管理ワークフローを使用して FMC から取得できます。 詳細については、該当する Firepower バージョンの『*Firepower Management Center Configuration Guide*』の「Reusable Objects」の章にある「Internal Certificate Authority Objects」のトピックを参照してください。
自己署名証明書の受け入れ（Accept Self-signed Cert）	自己署名証明書を信頼するように FMC オーケストレータを設定するには、このチェックボックスをオンにします。
セキュアコネクタトンネル（Secure Connector Tunnel）	Secure Workload SaaS を使用している場合は、このオプションを有効にする必要があります。 オンプレミスの Secure Workload アプライアンスを使用している場合は、このオプションを有効にする必要が生じる場合があります。 このオプションを有効にする前に、統合の前提条件：Cisco Secure Workload バージョン 3.7.1.5 （28 ページ） で説明されているように、セキュアコネクタを展開しておく必要があります。
Cisco Secure Workload キャッチオールを使用する（Use Cisco Secure Workload Catch All）	このチェックボックスをオンにして、Cisco Secure Workload のキャッチオールルールを有効にします。キャッチオール Cisco Secure Workload ルールは、アクセス コントロール ポリシーの [デフォルト（Default）] セクションで、他のすべてのルール（Cisco Secure Workload ルールおよび FMC で直接作成されたルール（ある場合））の後にリストされます。 Cisco Secure Workload のキャッチオールルールを無効にする場合は、このオプションの選択を解除して、FMC アクセス コントロール ポリシーのデフォルトアクションを使用します。

<table>
<tr><th colspan="2">オプション</th><th>説明</th></tr>
<tr><td rowspan="2">適用モード（Enforcement Mode）</td><td>マージ/オーバーライド（Merge/ Override）</td><td>ドロップダウンリストから [マージ（Merge）] または [オーバーライド（Override）] を選択します。
• [オーバーライド（Override）] を選択すると、既存の FMC アクセスコントロールルールが、適用された Secure Workload ポリシーに置き換わります。
重要 このオプションを選択すると、FTD（該当する場合は、選択したドメイン内）に関連付けられているすべてのアクセス コントロール ポリシーの既存のルールはすべて削除され、回復不能になります。
• 保持する必要があるルールが存在する場合は、この統合を続行する前にルールをエクスポートするか、[マージ（Merge）] オプション（以下で説明）を使用することをお勧めします。
（注） [適用モード（Enforcement Mode）] が [マージ（Merge）] に設定されている場合、次のようになります。
• 手動で FMC に入力するルールには、プレフィックスとして <code>Workload_</code> を使用しないことを推奨します。これは、これらのルールが自動的に削除されるためです。
• FMC UI による FTD 導入と Secure Workload を使用したポリシー適用を同時に実行しないでください。これらの非同期で長時間（最長 2 分）の操作は互いに競合し、FTD の展開が失敗する可能性があります。ポリシー適用が競合して FTD の展開が失敗した場合は、展開を繰り返す必要があります。</td></tr>
<tr><td>Absolute or Default Policy Priority（絶対またはデフォルトのポリシー優先順位）</td><td></td></tr>
</table>

オプション		説明
		優先順位ドロップダウンメニュー オプションは、適用モードとして [マージ（Merge）] が選択されている場合にのみ使用できます。 [絶対ポリシー（Absolute Policies）] または [デフォルトポリシー（Default Policies）] ドロップダウンメニューで、必要なオプションを選択して、FMC のアクセス コントロール ポリシーのそれぞれのセクションにある既存のルールの上または下に Cisco Secure Workload ポリシーを表示します。たとえば、[絶対ポリシー（Absolute Policies）] ドロップダウンメニューで、[既存の必須ルールの上に挿入（Insert above existing Mandatory rules）] を選択すると、Cisco Secure Workload ルールが [必須（Mandatory）] セクションの先頭に表示され、続いて Cisco Secure Firewall Management Center の既存のアクセス コントロール ルールが表示されます。 新しいルールが作成されると、アクセス コントロール ポリシーのルールの順序は、Cisco Secure Workload のポリシーに対して選択された優先順位に基づいて更新されます。

ステップ 4 左側の [ホストリスト（Host Lists）] リンクをクリックします。

ステップ 5 関連付けられている FMC のホスト名とポート番号を入力します。

ホスト名は、FMC の完全修飾ドメイン名または IP アドレスにする必要があります。

デフォルトのポート番号は 443 です。

FMC がサポート対象のハイアベイラビリティ構成で展開されている場合は、スタンバイ/セカンダリ FMC のホスト名とポートも入力します。

ステップ 6 [作成（Create）] をクリックします。

Secure Workload が Cisco Secure Firewall Management Center に正常に接続されたことを示す緑色のバナーが一時的に表示される場合があります。

接続が確立された後、Secure Workload は Cisco Secure Firewall Management Center で設定されたドメインを取得します。数分かかることがあります。

(ドメインが設定されていない場合、Secure Workload は [グローバル（Global）] ドメインを取得します。)

ドメインが正常に取得されると、ドメインを選択するオプションが表示されます。

ステップ 7 ここで管理対象の Cisco Secure Firewall Threat Defense デバイスにポリシーを展開しない場合は、次の手順を実行します。

ドメインを選択するオプションが表示されたら、[キャンセル（Cancel）] をクリックします。

ポリシーを展開する準備ができたら、[外部オーケストレータ（External Orchestrators）]ページに戻り、このオーケストレータを編集し、[ドメイン（Domains）] をクリックして、次の手順の説明に従ってドメインを選択します。

ステップ 8 セグメンテーションポリシーをプッシュするドメインを選択します。

Cisco Secure Firewall 展開にドメインが設定されていない場合は、[グローバル（Global）] ドメインを選択します。

ステップ 9 [更新（Update）]をクリックします。

セグメンテーションポリシーは、選択したドメインのアクセス コントロール ポリシーにプッシュされ、変更は関連する Cisco Secure Firewall Threat Defense デバイスに展開されます。

ルールをプッシュするのに必要な時間は通常数分ですが、ポリシールールの数と Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense のリソース構成によって異なります。

次のタスク

Cisco Secure Workload バージョン 3.7.1.5 でのこの統合の導入 （28 ページ） の手順概要表に戻り、残りの手順を続行します。

バージョン 3.7.1.5 での FMC オーケストレータの編集

- ポリシーを適用するドメインを指定せずに FMC オーケストレータを作成し、後からオーケストレータ構成を編集して、適用するドメインを指定できます。

  適用は、ドメインを選択した後に [更新（Update）] をクリックすると発生します。

- FMC 外部オーケストレータを編集する場合は、FMC アカウントのパスワードを再度入力する必要があります。

- ドメインが選択されている FMC オーケストレータを変更すると、Secure Workload がドメインを再度取得します。

  すでに選択したドメインは選択されたままです。

- オーケストレータを変更すると、[外部オーケストレータ（Exernal Orchestrators）] ページで最初は、接続と同期が行われている間、[接続ステータス（Connection Status）] が [失敗（Failure）]として表示される場合がありますが、しばらくするとこれが [成功（Success）] に変わります。その後、ドメインを編集できます。

Cisco Secure Workload バージョン 3.6 でのこの統合の導入

このセクションは、すべてのバージョン3.6.x ビルドに適用されます。ビルド固有の情報には、その旨のラベルが付けられています。

アップグレードについて

3.6.1.36 へのアップグレード

ドメインが Firepower Management Center で設定されていて、バージョン 3.6.1.36 にアップグレードする前に FMC オーケストレータで適用が有効になっている場合：

デフォルトでは、すべてのドメインが適用対象として選択されています。

3.5 から 3.6.1.5 へのアップグレード

バージョン 3.5 で FMC 統合を設定している場合、バージョン 3.6.1.5 にアップグレードするには、『*Cisco Secure Workload Upgrade Guide*』の重要な情報を参照してください。以下の手順を使用する必要はありません。

統合の前提条件：Cisco Secure Workload 3.6

- サポートされている Firepower Management Center（FMC）と、サポートされている少なくとも 1 つの Firepower Threat Defense（FTD）デバイスが設定されている。FTD を FMC に関連付け、各 FTD をアクセス コントロール ポリシーに割り当て、ポリシーを FMC から FTD に展開できること、およびシステムがネットワークトラフィックを予期したとおりに処理していることが確認済みである。

  詳細については、Cisco Secure Firewall ドキュメントロードマップを含め、製品の Cisco Secure Firewall Management Center ドキュメントを参照してください。

- Secure Workload アプライアンス（オンプレミス）またはアカウント（Software as a Service（SaaS））が設定され、予期したとおりに動作している。

- Secure Workload Software as a Service（SaaS）を使用している場合、またはオンプレミスの Secure Workload が FMC アプライアンスに直接到達できない場合は、セキュアコネクタトンネルを設定してソリューション コンポーネント間の接続を提供します。

  デフォルトでは、Secure Workload はポート 443 の HTTPS を使用して FMC REST API と通信します。

  セキュアコネクタの設定手順については、Secure Workload Web インターフェイスのオンラインヘルプとして利用できる Secure Workload ユーザーガイドを参照してください。

Secure Workload バージョン 3.6 でこの統合を実装する方法

次の表に、Firepower Management Center（FMC）を設定し、Secure Workload バージョン 3.6 リリースとの統合を設定するエンドツーエンドのワークフローを示します。

ステップ	説明	詳細情報
はじめる前に	この統合がどのように機能するか、統合を導入するための高レベルのプロセスの概要、および展開における考慮事項を理解します。	Cisco Secure Workload バージョン 3.7 および 3.6 に関する重要な情報 （6 ページ） のすべてのセクションとトピックを参照してください。
はじめる前に	要件および前提条件を満たします	以下のすべてのセクションを参照してください： サポートされる展開 （13 ページ） および 統合の前提条件：Cisco Secure Workload 3.6 （37 ページ）。
1	Secure Workload で、次の手順を実行します。 現在の環境のスコープ、インベントリフィルタ、クラスタ、ワークスペース、およびセグメンテーションポリシーを定義します。	Firepower のダイナミックオブジェクトによって定義される一連のワークロードに適用するセグメンテーションポリシーを手動で作成します。 これについて質問がある場合は、Secure Workload Web インターフェイスからオンラインヘルプとして利用できる Secure Workload ユーザーガイドの「Segmentation」セクションを参照してください。 もう 1 つの方法としては、詳細設定：ADM を使用してセグメンテーションポリシーを生成する （48 ページ）を参照してください。
2	FMC の場合： FTD に割り当てられた各アクセス コントロール ポリシーの下部で、ポリシーの [デフォルトアクション（Default Action）] を設定します。	このアクションは、作成するセグメンテーションポリシーによって異なります。たとえば、セグメンテーションポリシーで明確に許可されているトラフィック以外のすべてのトラフィックをブロックする場合は、[すべてのトラフィックをブロック（Block all traffic）] を選択します。

ステップ	説明	詳細情報
3	FMC の場合： この統合専用のユーザーアカウントを作成します。	このユーザーアカウントの要件： • アカウントは、管理者ロールを持っている必要があります。 • （ドメインが FMC で設定されている場合）アカウントは [グローバル（Global）] ドメインにアクセスできる必要があります。 FMC でのユーザーアカウントの作成について質問がある場合は、Firepower Management Center のオンラインヘルプで「Add an Internal User」のトピックを参照してください。
4	Secure Workload で、次の手順を実行します。 FMC オーケストレータを作成します。	Firepower Management Center ごとに FMC オーケストレータを 1 つだけ作成します。 • Secure Workload バージョン 3.6.1.36 の場合： バージョン 3.6.1.36 での FMC オーケストレータの設定 （41 ページ）を参照してください • Secure Workload バージョン 3.6.1.5 から 3.6.1.20 の場合： 以下の Secure Workload バージョン 3.6.1.5 から 3.6.1.20 での FMC オーケストレータの設定 （44 ページ） を参照。 OpenAPI を使用して FMC オーケストレータを作成するには、Secure Workload Web ポータルでオンラインヘルプとして利用できるユーザーガイドを参照してください。バージョン 3.6.1.36 では、ドメインに関するセクションを見逃さないでください。

ステップ	説明	詳細情報
5	Secure Workload で、次の手順を実行します。 目的のワークスペースにポリシーを適用します。 （これは、FMC オーケストレータでの適用の有効化とは別の操作です）。	ワークスペースで、[適用（Enforcement）] タブをクリックし、[ポリシーの適用（Enforce Policies）] ボタンをクリックしてウィザードを完了します。
6	Secure Workload バージョン 3.6.1.36 の場合： オーケストレータの適用を有効にします。 FMC オーケストレータでドメインをまだ選択していない場合は、ここで選択します。	FMC オーケストレータを編集してドメインを選択します。(FMC にドメインが設定されていない場合は、[グローバル（Global）] ドメインを選択する必要があります。) ドメインを選択した後に [更新（Update）] をクリックすると、オーケストレータの適用が有効になり、管理対象の FTD デバイスに Secure Workload ポリシーが展開されます。 詳細については、バージョン 3.6.1.36 での FMC オーケストレータの編集 （49 ページ）を参照してください。
	Secure Workload バージョン 3.6.1.5 から 3.6.1.20 の場合： FMC 外部オーケストレータで適用をまだ有効にしていない場合は、ここで有効にします。	上記で設定した FMC オーケストレータを編集し、[適用の有効化（Enable Enforcement）] を選択します。
7	アクセス コントロール ポリシーに新しいルールが表示されるまで待ちます。	これに要する時間は、転送されるデータの量、マシンの速度、ネットワーク帯域幅などに応じて異なります。 Firepower Management Center でルールを表示するには、次を実行します。 FMC で、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択して、表示するポリシーをクリックします。

ステップ	説明	詳細情報
8	新しいアクセスコントロールポリシーは、関連付けられた管理対象FTDに自動的に展開されます。	将来の変更もFTDデバイスに自動的に展開されます。 今後、新しい FTD を既存のアクセス コントロールポリシーに関連付けると、新しいFTDは自動的に現在のルールを受信します。

バージョン 3.6.1.36 での FMC オーケストレータの設定

始める前に

Secure Workload バージョン 3.6 でこの統合を実装する方法 （37 ページ） の表の、ここまでの手順を完了します。

3.6.1.36 より前の 3.6 バージョンを使用している場合は、この手順を使用しないでください。代わりに、Secure Workload バージョン 3.6.1.5 から 3.6.1.20 での FMC オーケストレータの設定（44 ページ）を参照してください。

手順

ステップ 1 Secure Workload Web インターフェイスで、[管理（Manage）]>[外部オーケストレータ（External Orchestrators）] を選択します。

ステップ 2 [新規設定の作成（Create New Configuration）] をクリックします。

ステップ 3 [基本設定（Basic Configs）] タブで、次のフィールドを設定します。

オプション	説明
タイプ（**Type**）	[FMC] を選択します。
名前（**Name**）	FMC オーケストレータの一意の名前を入力します。
説明（**Description**）	オーケストレータの説明を入力します。
フルスナップショット間隔（**Full Snapshot Interval(s)**）	フルスナップショットの間隔を秒単位で入力します。 [フルスナップショット間隔（Full Snapshot Interval(s)）] フィールドは、FMC 外部オーケストレータが FMC と Secure Workload の接続をテストする頻度を指定します。エラーが発生した場合（たとえば、ネットワークの問題により FMC に到達できない場合、または無効なエンドポイントやユーザークレデンシャルが使用された場合）、FMC オーケストレータは [ステータス（Status）] フィールドにエラーを報告します。 デフォルト値：3600 秒

オプション	説明
ユーザー名（Username）	このドキュメントで前述した、FMC で作成した専用ユーザのユーザー名とパスワードを入力します。 これらのクレデンシャルは、FMC との通信に使用されます。
パスワード（Password）	
CA 証明書（CA Certificate）	Secure Workload がこの FMC の認証に使用する CA 証明書を入力します。この証明書は、オブジェクト管理ワークフローを使用して FMC から取得できます。 詳細については、該当する Firepower バージョンの『*Firepower Management Center Configuration Guide*』の「Reusable Objects」の章にある「Internal Certificate Authority Objects」のトピックを参照してください。
自己署名証明書の受け入れ（Accept Self-signed Cert）	自己署名証明書を信頼するように FMC オーケストレータを設定するには、このチェックボックスをオンにします。
セキュアコネクタトンネル（Secure Connector Tunnel）	Secure Workload SaaS を使用している場合は、このオプションを有効にする必要があります。 オンプレミスの Secure Workload アプライアンスを使用している場合は、このオプションを有効にする必要が生じる場合があります。 このオプションを有効にする前に、統合の前提条件：Cisco Secure Workload 3.6 （37 ページ） で説明されているように、セキュアコネクタを展開しておく必要があります。

オプション	説明
適用モード（Enforcement Mode）	ドロップダウンリストから [マージ（Merge）] または [オーバーライド（Override）] を選択します。 • [オーバーライド（Override）] を選択すると、既存の FMC アクセスコントロールルールが、適用された Secure Workload ポリシーに置き換わります。 **重要** このオプションを選択すると、FTD（該当する場合は、選択したドメイン内）に関連付けられているすべてのアクセス コントロール ポリシーの既存のルールはすべて削除され、回復不能になります。 保持する必要があるルールが存在する場合は、この統合を続行する前にルールをエクスポートするか、[マージ（Merge）]オプション（以下で説明）を使用することをお勧めします。 • [マージ（Merge）] を選択すると、Secure Workload のルールがアクセスコントロールルールのリストの先頭に追加されます。 （注） [適用モード（Enforcement Mode）] が [マージ（Merge）] に設定されている場合、次のようになります。 • 手動で FMC に入力するルールには、プレフィックスとして `Workload_` を使用しないことを推奨します。これは、これらのルールが自動的に削除されるためです。 • FMC UI による FTD 導入と Secure Workload によるポリシー適用を同時に実行しないでください。これらの非同期で長時間（最長 2 分）の操作は互いに競合し、FTD の展開が失敗する可能性があります。ポリシー適用が競合して FTD の展開が失敗した場合は、展開を繰り返す必要があります。

ステップ 4 左側の [ホストリスト（Host Lists）] リンクをクリックします。

ステップ 5 関連付けられている FMC のホスト名とポート番号を入力します。

ホスト名は、FMC の完全修飾ドメイン名または IP アドレスにする必要があります。

デフォルトのポート番号は 443 です。

FMC がサポート対象のハイアベイラビリティ構成で展開されている場合は、スタンバイ/セカンダリ FMC のホスト名とポートも入力します。

ステップ 6 [作成（Create）] をクリックします。

Secure Workload が Firepower Management Center に正常に接続されたことを示す緑色のバナーが一時的に表示される場合があります。

接続が確立された後、Secure Workload は Firepower Management Center で設定されたドメインを取得します。数分かかることがあります。

(ドメインが設定されていない場合、Secure Workload は [グローバル（Global）] ドメインを取得します。)

ドメインが正常に取得されると、ドメインを選択するオプションが表示されます。

ステップ 7 ここで管理対象の FTD デバイスにポリシーを展開しない場合は、次の手順を実行します。

ドメインを選択するオプションが表示されたら、[キャンセル（Cancel）] をクリックします。

ポリシーを展開する準備ができたら、[外部オーケストレータ（External Orchestrators）] ページに戻り、このオーケストレータを編集し、[ドメイン（Domains）] をクリックして、次の手順の説明に従ってドメインを選択します。

ステップ 8 セグメンテーションポリシーをプッシュするドメインを選択します。

Firepower 展開にドメインが設定されていない場合は、[グローバル（Global）] ドメインを選択します。

ステップ 9 [更新（Update）]をクリックします。

セグメンテーションポリシーは、選択したドメインのアクセス コントロール ポリシーにプッシュされ、変更は関連する FTD デバイスに展開されます。

ルールをプッシュするのに必要な時間は通常数分ですが、ポリシールールの数と FMC および FTD のリソース構成によって異なります。

次のタスク

Secure Workload バージョン 3.6 でこの統合を実装する方法 （37 ページ） の手順概要表に戻り、残りの手順を続行します。

Secure Workload バージョン 3.6.1.5 から 3.6.1.20 での FMC オーケストレータの設定

次の手順に従い、Secure Workload Web インターフェイスを使用して、FMC 外部オーケストレータを作成します。

始める前に

Secure Workload バージョン 3.6 でこの統合を実装する方法 （37 ページ） の表の、ここまでの手順を完了します。

バージョン3.6.1.36を使用している場合は、この手順を使用しないでください。代わりに、バージョン 3.6.1.36 での FMC オーケストレータの設定 （41 ページ）を参照してください。

手順

ステップ 1 [管理（Manage）] > [外部オーケストレータ（External Orchestrators）] に移動します。

ステップ 2 [新規設定の作成（Create New Configuration）] をクリックします。

ステップ 3 [基本設定（Basic Configs）] タブで、次のフィールドを設定します。

オプション	説明
タイプ（**Type**）	[FMC] を選択します。
名前（**Name**）	FMC オーケストレータの一意の名前を入力します。
説明（**Description**）	オーケストレータの説明を入力します。
フルスナップショット間隔（**Full Snapshot Interval(s)**）	フルスナップショットの間隔を秒単位で入力します。 [フルスナップショット間隔（Full Snapshot Interval(s)）] フィールドは、FMC 外部オーケストレータが FMC と Secure Workload の接続をテストする頻度を指定します。エラーが発生した場合（たとえば、ネットワークの問題により FMC に到達できない場合、または無効なエンドポイントやユーザークレデンシャルが使用された場合）、FMC オーケストレータは [ステータス（Status）] フィールドにエラーを報告します。 デフォルト値：3600 秒
ユーザー名（**Username**）	このドキュメントで前述した、FMCで作成した専用ユーザのユーザー名とパスワードを入力します。 これらのクレデンシャルは、FMC との通信に使用されます。
パスワード（**Password**）	
CA 証明書（**CA Certificate**）	Secure Workload がこの FMC の認証に使用する CA 証明書を入力します。この証明書は、オブジェクト管理ワークフローを使用して FMC から取得できます。 詳細については、該当する Firepower バージョンの『*Firepower Management Center Configuration Guide*』の「Reusable Objects」の章にある「Internal Certificate Authority Objects」のトピックを参照してください。
自己署名証明書の受け入れ（**Accept Self-signed Cert**）	自己署名証明書を信頼するように FMC オーケストレータを設定するには、このチェックボックスをオンにします。

オプション	説明
セキュアコネクタトンネル（Secure Connector Tunnel）	Secure Workload SaaS を使用している場合は、このオプションを有効にする必要があります。 オンプレミスの Secure Workload アプライアンスを使用している場合は、このオプションを有効にする必要が生じる場合があります。 このオプションを有効にする前に、このドキュメントで前述したように、セキュアコネクタを展開しておく必要があります。 セキュアコネクタトンネルの詳細については、Secure Workload Webインターフェイスから入手できるユーザーガイドを参照してください。
適用の有効化（Enable Enforcement）	ポリシーを FMC およびその管理対象 FTD デバイスにプッシュするには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。 どのワークスペースにもポリシーを適用していない場合でも、このチェックボックスを選択できます。ワークスペースで適用を有効にすると、ポリシーが自動的に FMC とその管理対象 FTD にプッシュされます。 このボックスをオフにすると、ポリシーは FMC にプッシュされず、以前に FMC にプッシュされたすべてのルールがクリアされます。

オプション	説明
適用モード（Enforcement Mode）	ドロップダウンから [マージ（Merge）] または [オーバーライド（Override）] を選択します。 • [オーバーライド（Override）] を選択すると、既存の FMC アクセスコントロールルールが、適用された Secure Workload ポリシーに置き換わります。 **重要** このオプションを選択すると、FTD に関連付けられているすべてのアクセス コントロール ポリシーの既存のルールはすべて削除され、回復不能になります。 保持する必要があるルールが存在する場合は、この統合を続行する前にルールをエクスポートするか、[マージ（Merge）]オプション（以下で説明）を使用することをお勧めします。 • [マージ（Merge）] を選択すると、Secure Workload のルールがアクセスコントロールルールのリストの先頭に追加されます。 **（注）** [適用モード（Enforcement Mode）] が [マージ（Merge）] に設定されている場合、次のようになります。 • 手動で FMC に入力するルールには、プレフィックスとして `Workload_` を使用しないことを推奨します。これは、これらのルールが自動的に削除されるためです。 • FMC UI による FTD 導入と Secure Workload によるポリシー適用を同時に実行しないでください。これらの非同期で長時間（最長 2 分）の操作は互いに競合し、FTD の展開が失敗する可能性があります。ポリシー適用が競合して FTD の展開が失敗した場合は、展開を繰り返す必要があります。

ステップ 4 [ホストリスト（Hosts Lists）] タブをクリックします。

ステップ 5 関連付けられている FMC のホスト名とポート番号を入力します。

ホスト名は、FMC の完全修飾ドメイン名または IP アドレスにする必要があります。

デフォルトのポート番号は 443 です。

FMC がサポート対象のハイアベイラビリティ構成で展開されている場合は、スタンバイ/セカンダリ FMC のホスト名とポートも入力します。

ステップ 6 [作成（Create）] をクリックします。

ルールをプッシュするのに必要な時間は通常数分ですが、ポリシールールの数と FMC および FTD のリソース構成によって異なります。

数分後、統合のステータスを確認します。

a) [外部オーケストレータ（Exernal Orchestrators）] ページで、新しく作成した FMC オーケストレータの行をクリックします。
b) [設定の詳細（Configuration Details）] ダイアログボックスが表示されます。接続が成功すると、検出された FTD の数が [進捗ステータス（Progress Status）] フィールドに表示されます。

次のタスク

Secure Workload バージョン 3.6 でこの統合を実装する方法 （37 ページ） の手順概要表に戻り、残りの手順を続行します。

詳細設定：ADM を使用してセグメンテーションポリシーを生成する

手動で作成する代わりに、ADM がセグメンテーションポリシーを検出できるようにするには：

1. Secure Workload バージョン 3.6 でこの統合を実装する方法 （37 ページ） の手順に従いますが、ポリシーを手動で作成する代わりに、次の基本手順を実行します。
2. Firepower Management Center で、次の手順を実行します。
    1. flexconfig を使用して、NSEL レコード (フローデータ) をエクスポートするようにシステムを設定します。

        手順については、https://www.cisco.com/c/en/us/support/security/defense-center/series.html#~tab-documents にある Firepower 製品のドキュメントを参照してください。
    2. ポリシーに影響を与えるトラフィックが生成されていることを確認します。
3. Secure Workload で、次の手順を実行します。
    1. フローデータを保持するための取り込みアプライアンス（仮想アプライアンス）を展開します。
    2. Firepower システムからフローデータを収集するように ASA コネクタを設定します。

        （このコネクタは FTD デバイスからフローデータを収集します。）
    3. システムが適切なポリシーを生成するために十分なフローデータを収集するまでしばらく待ちます。
    4. 該当するすべてのアプリケーション ワークスペースで ADM を実行します

5. 提案されたセグメンテーションポリシーを適用する前に、分析、検証、および承認します。

Secure Workload 手順の詳細については、Secure Workload Web インターフェイスのユーザーガイドを参照してください。

バージョン 3.6.1.36 での FMC オーケストレータの編集

- ポリシーを適用するドメインを指定せずに FMC オーケストレータを作成し、後からオーケストレータ構成を編集して、適用するドメインを指定できます。

  適用は、ドメインを選択した後に [更新（Update）] をクリックすると発生します。

- FMC 外部オーケストレータを編集する場合は、FMC アカウントのパスワードを再度入力する必要があります。

- ドメインが選択されている FMC オーケストレータを変更すると、Secure Workload がドメインを再度取得します。

  すでに選択したドメインは選択されたままです。

- オーケストレータを変更すると、[外部オーケストレータ（Exernal Orchestrators）] ページで最初は、接続と同期が行われている間、[接続ステータス（Connection Status）] が [失敗（Failure）] として表示される場合がありますが、しばらくするとこれが [成功（Success）] に変わります。その後、ドメインを編集できます。

Tetration バージョン 3.5 でこの統合を実装する方法

次の表に、Firepower Management Center をセットアップし、Tetration との統合を設定するためのエンドツーエンドのワークフローを示します。

ステップ	説明	手順へのリンク
1	Tetration で次の操作を行います。 環境のスコープ、ワークスペース、セグメンテーションポリシーを定義します。	『Tetration User Guide』（https://<cluster>/documentation/ui/adm.html）の「Segmentation」の項を参照してください。
2	Tetration SaaS を使用している場合、または FMC アプライアンスに Tetration から直接到達できない場合は、セキュアコネクタトンネルを設定して接続を提供します。	デフォルトでは、Tetration はポート 443 の HTTPS を使用して FMC REST API と通信します。 『Tetration User Guide』（https://<cluster>/documentation/ui/software_agents/secure_connector.html）を参照してください。

ステップ	説明	手順へのリンク
3	仮想または物理 FMC を設定します。 使用しているデバイスに関連する『Getting Started Guide』を参照してください。	『Cisco Firepower Management Center Virtual Getting Started Guide』：https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcv/fpmc-virtual/fpmc-virtual-intro.html 『Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide』：https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1000-2500-4500/fmc-1000-2500-4500.html 『Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide』：https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1600-2600-4600/fmc-1600-2600-4600.html
4	FMC の場合： Tetration との統合のみに使用する専用ドメインを作成します。	該当する Firepower のバージョンの『Firepower Management Center Configuration Guide』の、「Deployment Management」の章にある「Creating New Domains」セクションを参照してください。次に例を示します。https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/domain_management.html#task_F3D21E5A48DF4F5FA0B3C1C4A86AA80D

ステップ	説明	手順へのリンク
5	FMC の場合： 上記で作成した専用ドメインの FMC に FTD を割り当てます。 （注） この手順は、プロセスの後半でも実行できます。Tetration/FMC 統合では、新しく割り当てられた FTD が検出されるためです。	管理対象デバイスを FMC に追加するには、FMC GUI の [デバイス（Devices）] > [デバイス管理（Device Management）] ページを使用します。 詳細については、現在の展開に対応する『Getting Started Guide』の「Add Managed Devices to the FMC」トピックを参照してください。次に例を示します。 • 『Cisco Firepower Management Center Virtual Getting Started Guide』：https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcv/fpmc-virtual/fpmc-virtual-initial-admin.html • 『Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide』：https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1000-2500-4500/fmc-1000-2500-4500.html#Cisco_Task.dita_009a8ec9-d320-4577-bcf5-9b09bfef3a2f • 『Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide』：https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1600-2600-4600/fmc-1600-2600-4600.html#Cisco_Task.dita_009a8ec9-d320-4577-bcf5-9b09bfef3a2f
6	FMC の場合： 上記で作成した専用ドメインで、FTD にアクセスコントロールおよびプレフィルタポリシーを割り当てます。FTD に割り当てられるプレフィルタポリシーは、読み取り専用の `Default Prefilter Policy` 以外である必要があります。FMC オーケストレータで、`Default Prefilter Policy` が割り当てられた FTD が検出されると、その FTD にポリシー適用がプッシュされません。	該当する Firepower バージョンの『Firepower Management Center Configuration Guide』の、「Prefiltering and Prefilter Policies」の章にある「Configure Prefiltering」トピックを参照してください。次に例を示します。 https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/prefiltering_and_prefilter_policies.html#id_17608

ステップ	説明	手順へのリンク
7	FMC の場合： Tetration と FMC の統合専用のカスタム内部ユーザーアカウントを作成します。 この内部ユーザーアカウントは次の条件があります。 • 管理者ロールが割り当てられていること。 • 関連付けられたFTD、アクセス、およびプレフィルタポリシーが属するドメインと同じドメイン内に存在すること。	該当する Firepower バージョンの『Firepower Management Center Configuration Guide』の「Add an Internal User」のトピックを参照してください。 次に例を示します。 https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/user_accounts_fmc.html#task_j5n_1cr_qcb
8	Tetration で次の操作を行います。 FMC オーケストレータを作成します。	Cisco Tetration バージョン 3.5 での FMC オーケストレータの設定 （53 ページ）
9	Tetration で次の操作を行います。 目的のワークスペースでポリシーの適用を実行します。	『Tetration User Guide』の「Policies」セクションを参照してください。 https://<cluster>/documentation/ui/adm/policies.html
10	FMCポリシーエンフォーサにより、関連付けられているすべてのFTDのプレフィルタポリシーにポリシーが展開されます。	Firepower Management Center で、[ポリシー（Policies）]>[アクセス制御（Access Control）]>[プレフィルタ（Prefilter）]を選択します。 Tetrationから FTD に適用されるルールを表示するには、関連するポリシーをクリックします。 詳細については、該当するFirepowerバージョンに関連する『Firepower Management Configuration Guide』の「Access Control」の章にある「Prefiltering」および「Prefilter Policies」トピックを参照してください。 次に例を示します。 https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/prefiltering_and_prefilter_policies.html#id_18072

Cisco Tetration バージョン 3.5 での FMC オーケストレータの設定

次の手順に従い、Tetration Web インターフェイスを使用して、FMC 外部オーケストレータを作成します。

手順

ステップ 1 [可視性（Visibility）] > [外部オーケストレータ（External Orchestrators）] に移動します

ステップ 2 [新規設定の作成（Create New Configuration）] をクリックします。

ステップ 3 [基本設定（Basic Configs）] タブで、次のフィールドを設定します。

オプション	説明
タイプ（**Type**）	[FMC] を選択します。
名前（**Name**）	FMC オーケストレータの一意の名前を入力します。
説明（**Description**）	オーケストレータの説明を入力します。
フルスナップショット間隔（**Full Snapshot Interval(s)**）	フルスナップショットの間隔を秒単位で入力します。 [フルスナップショット間隔（Full Snapshot Interval (s)）] フィールドは、FMC 外部オーケストレータが FMC と Tetration の接続をテストする頻度を指定します。エラーが発生した場合（たとえば、ネットワークの問題により FMC に到達できない場合、または無効なエンドポイントやユーザークレデンシャルが使用された場合）、FMC オーケストレータは [ステータス（Status）] フィールドにエラーを報告します。 デフォルト値：3600 秒
ユーザー名（**Username**）	このドキュメントで前述した、FMC で作成した専用ユーザのユーザー名とパスワードを入力します。 これらのクレデンシャルは、FMC との通信に使用されます。
パスワード（**Password**）	
CA 証明書（**CA Certificate**）	Tetration がこの FMC の認証に使用する CA 証明書を入力します。この証明書は、オブジェクト管理ワークフローを使用して FMC から取得できます。 詳細については、該当する Firepower バージョンの 『*Firepower Management Center Configuration Guide*』の「Reusable Objects」の章にある「Internal Certificate Authority Objects」のトピックを参照してください。
自己署名証明書の受け入れ（**Accept Self-signed Cert**）	自己署名証明書を信頼するように FMC オーケストレータを設定するには、このチェックボックスをオンにします。

オプション	説明
セキュアコネクタトンネル（Secure Connector Tunnel）	Tetration Software as a Service（SaaS）を使用している場合は、このオプションを有効にする必要があります。 オンプレミスの Tetration アプライアンスを使用している場合は、このオプションを有効にする必要が生じる場合があります。 このオプションを有効にする前に、このドキュメントで前述したように、セキュアコネクタを展開しておく必要があります。 セキュアコネクタトンネルの詳細については、Tetration の Web インターフェイスから入手できるユーザーガイドを参照してください。
適用の有効化（Enable Enforcement）	ポリシーを FMC およびその管理対象 FTD デバイスにプッシュするには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。 どのワークスペースにもポリシーを適用していない場合でも、このチェックボックスを選択できます。ワークスペースで適用を有効にすると、ポリシーが自動的に FMC とその管理対象 FTD にプッシュされます。 このボックスをオフにすると、ポリシーは FMC にプッシュされず、以前に FMC にプッシュされたすべてのプレフィルタルールがクリアされます。

オプション	説明
適用モード（Enforcement Mode）	ドロップダウンから [マージ（Merge）] または [オーバーライド（Override）] を選択します。 • [オーバーライド（Override）] を選択すると、既存のプレフィルタポリシールールが、適用された Tetration ポリシーに置き換わります。 **重要** このオプションを選択すると、既存のすべてのプレフィルタポリシールールが削除され、回復不能になります。 保持する必要があるルールが存在する場合は、この統合を続行する前にルールをエクスポートするか、[マージ（Merge）] オプション（以下で説明）を使用することをお勧めします。 • [マージ（Merge）] を選択すると、Tetration のルールがプレフィルタルールのリストの先頭に追加されます。 （注） [適用モード（Enforcement Mode）] が [マージ（Merge）] に設定されている場合、次のようになります。 • 手動で FMC に入力するルールには、プレフィックスとして `Tetrul_` を使用しないことを推奨します。これは、これらのルールが自動的に削除されるためです。 • FMC UI による FTD 導入と Tetration によるポリシー適用を同時に実行しないでください。これらの非同期で長時間（最長 2 分）の操作は互いに競合し、FTD の展開が失敗する可能性があります。ポリシー適用が競合して FTD の展開が失敗した場合は、展開を繰り返す必要があります。

ステップ 4 [ホストリスト（Hosts Lists）] タブをクリックします。

ステップ 5 関連付けられている FMC のホスト名とポート番号を入力します。

ホスト名は、FMC の完全修飾ドメイン名または IP アドレスにする必要があります。

デフォルトのポート番号は 443 です。

FMC がサポート対象のハイアベイラビリティ構成で展開されている場合は、スタンバイ/セカンダリ FMC のホスト名とポートも入力します。

ステップ 6 [作成（Create）] をクリックします。

ルールをプッシュするのに必要な時間は通常数分ですが、ポリシールールの数と FMC および FTD のリソース構成によって異なります。

数分後、統合のステータスを確認します。

a) [外部オーケストレータ（Exernal Orchestrators）] ページで、新しく作成した FMC オーケストレータの行をクリックします。
b) [設定の詳細（Configuration Details）] ダイアログボックスが表示されます。接続が成功すると、検出された FTD の数が [進捗ステータス（Progress Status）] フィールドに表示されます。

ドメインの適用ステータスの表示

リリース 3.6.1.36 以降の場合：[管理（Manage）] > [外部オーケストレータ（External Orchestrators）] ページのオーケストレータのリスト：

- リリース 3.6.1.36 の場合：

  [適用（Enforcement）] は常に [無効（Disabled）] と表示されます。

- リリース 3.7 の場合：

  少なくとも 1 つのドメインで適用が有効になっている場合、[適用（Enforcement）] は [有効（Enabled）] と表示されます。

上記のすべてのリリースで、どのドメインが適用されているかを確認するには、次を実行します。

1. 特定の FMC オーケストレータの構成を編集します。
2. [ドメイン（Domains）] をクリックします。
3. この [ドメイン（Domains）] ページにリストされているすべてのドメインに対して適用が有効になっています。

Secure Workload/Tetration と Cisco Secure Firewall Management Center 統合のトラブルシュート

Secure Workload/Tetration と Cisco Secure Firewall Management Center の統合における一般的な構成の問題をトラブルシュートするには、次の手順を使用します。

統合接続の問題のトラブルシューティング

[外部オーケストレータ（External Orchestrators）] ページを使用して、接続障害の背後にある一般的な問題を特定します。

1. [外部オーケストレータ（External Orchestrators）] ページに移動します。

   Secure Workload 3.6 の場合：[管理（Manage）] メニューにあります。

   Tetration 3.5 の場合：[可視性（Visibility）] メニューにあります。

2. [外部オーケストレータ（External Orchestrators）] ページで、使用している FMC オーケストレータの行を見つけます。

3. 統合接続ステータスが [接続ステータス（Connection Status）] 列に表示されます。この列に [失敗（Failure）] と表示されている場合は、行をクリックして詳細を表示します。

4. [設定の詳細（Configuration Details）] の表で、[認証失敗エラー（Authentication Failure Error）] 行を見つけます。

[認証失敗エラー（Authentication Failure Error）] フィールドに [接続の待機中（Waiting to connect）] と表示されている場合は、ページが更新されるまで 1 ー 2 分待ちます。

[認証失敗エラー（Authentication Failure Error）] 行に次のようなエラーが表示された場合：

```
fmc clusterUUID=602c4264755f0263ee16e5af failed to connect to appliance
172.28.171.193:10447
```

設定に関する次の問題を確認します。

問題	トラブルシューティングの手順
設定された IP ホスト名やポート番号が無効。	FMC 外部オーケストレータ設定に入力した FMC ホスト名とポート番号が正しいことを確認します。 設定された IP およびポートへの接続を確認します。
[ユーザー名（Username）] または [パスワード（Password）] が正しくない。	FMC オーケストレータ設定で入力した [ユーザー名（Username）] および [パスワード（Password）] フィールドが、FMC で作成した専用ユーザーと一致していること、また該当ユーザーがこのドキュメントで以前に指定している必要な権限を持っていることを確認します。 （注） 誤った Web インターフェイスのログイン情報を一定回数連続して入力すると、設定されている時間にわたって一時的にアカウントにアクセスできなくなります。この回数は、FMC のグローバルユーザー構成設定の [ログイン失敗の最大数（Max Number of Login Failures）] で指定します。詳細については、該当する Cisco Secure Firewall バージョンの Cisco Secure Firewall Management Center ガイドの「Appliance Platform Settings」の章にある「Global User Configuration Settings」のトピックを参照してください。

問題	トラブルシューティングの手順
FMC オーケストレータの基本設定で[セキュアコネクタトンネル（Secure Connector Tunnel）]チェックボックスがオンになっていても、セキュアコネクタが正しく展開されない。	セキュアコネクタが正しく展開されていることを確認します。詳細については、ユーザガイドの「Secure Connector」の項を参照してください。

（Secure Workload 3.6.1.36 以降）ステータスリストにドメインごとの適用ステータスが表示されない

ドメインの適用ステータスの表示 （56 ページ） を参照してください。

（Secure Workload 3.6）ポリシーの適用に関する問題の特定

- FMCで、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択し、FTD にアクセス コントロール ポリシーが割り当てられていることを確認します。
- FTD に関連付けられているアクセス コントロール ポリシーをクリックし、適切なルールがルールリストの[デフォルト（Default）]セクションに含まれていることを確認します。
- そうでない場合は、専用の FMC ユーザークレデンシャルに必要なアクセス権があることを確認します。

  ゴールデンルールのみが表示される場合は、アプリケーション ワークスペースでポリシーを適用していない可能性があります。

  ワークスペースで、ポリシーの適用が有効になっていることを確認します。
- FMC 外部オーケストレータの構成で、
  - Secure Workload が FMC に正常に接続できることを確認します。
  - 3.6 バージョンと、FMC 展開に複数のドメインが構成されているかどうかに応じて、

    [適用の有効化（Enable Enforcement）]チェックボックスがオンになっていることを確認します。

    または

    正しいドメインが選択されていることを確認します。

ヒント　このオーケストレータを介してポリシー更新を受信する管理対象FTDデバイスの数など、FMCオーケストレータに関する詳細を表示するには、[管理（Manage）] > [外部オーケストレータ（External Orchestrators）] に移動し、FMC オーケストレータの行をクリックします。FTD カウントは、表示されるテーブルの [進行状況（Progress Status）] 行に表示されます。

.

（Tetration 3.5）ポリシー適用の問題の特定

次の手順を使用して、関連付けられた FTD に Tetration のルールが適用されていることを確認します。

1. Cisco Secure Firewall Management Center で、[デバイス（Devices）]> [デバイス管理（Device Management）] を選択します。
2. 関連付けられている FTD の [アクセス コントロール ポリシー（Access Control Policy）] リンクをクリックします。
3. FTD アクセス コントロール ポリシーに割り当てられたプレフィルタポリシーが、デフォルトの読み取り専用 `Default Prefilter Policy` である場合、Tetration は FTD へのポリシーの展開をスキップします。FMC との統合で使用する Tetration のカスタム プレフィルタ ポリシーを作成する必要があります。（Tetration バージョン 3.5 でこの統合を実装する方法（49 ページ） の該当する手順を参照）。

カスタムルールがアクセス コントロール ポリシーのリストに表示されている場合は、これらのルールが適用されていることを確認します。

1. Cisco Secure Firewall Management Center で、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [プレフィルタ（Prefilter）] に移動します。
2. カスタム プレフィルタ ポリシーをクリックしてルールリストを表示します。

カスタム プレフィルタ ポリシーがアクセス コントロール リストに表示されていても、適用された Tetration ルールが表示されない場合は、次について確認します。

- FMC の接続を確認します。
- Tetration の [外部オーケストレータ（External Orchestrators）] の設定で、[適用の有効化（Enable Enforcement）] チェックボックスがオンになっていることを確認します。
- ポリシーの適用が実行されていることを確認します。

FMC ハイアベイラビリティ展開でポリシーの更新が失敗する

このスイッチオーバーが完了するまでに最大 4 分かかります。この間、非アクティブ FMC へのポリシーの適用は失敗します。

アクセス コントロール ポリシーに表示されない Secure Workload のルール

- ルールは、少なくとも 1 つの FTD が割り当てられているアクセス コントロール ポリシーにのみプッシュされます。
- [外部オーケストレータ（External Orchestrators）] ページで FMC オーケストレータの接続ステータスを確認します。
- Secure Workload バージョン 3.6.1.36 を使用している場合は、FMC オーケストレータで予期されるドメインが選択されていることを確認します。

Cisco TAC の連絡先

問題が解決しない場合は、お客様の展開に応じて適切なシスコサポートチームに連絡してください。

- Secure Workload/Tetration オンプレミス：TAC にお問い合わせください
- Secure Workload/Tetration SaaS：SaaS サポートチームが対応できるようにケースをオープンして ください

Secure Workload/FMC 統合の履歴

Cisco Secure Workload と FMC の統合の履歴、およびサポートされている製品バージョンの詳細については、「サポートされる展開 （13 ページ）」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。