FMC 6.6.1+：アップグレードの前後のヒント

内容

概要

このドキュメントでは、Cisco Secure Firewall Management Center(FMC)をバージョン6.6.1+にアップグレードする前とアップグレード後に実行する検証と設定のベストプラクティスについて説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Hardware:Cisco FMC 1000
- ソフトウェア：リリース7.0.0（ビルド94）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

FMCのアップグレード前に行うべき重要事項

FMCターゲットソフトウェアバージョンの選択

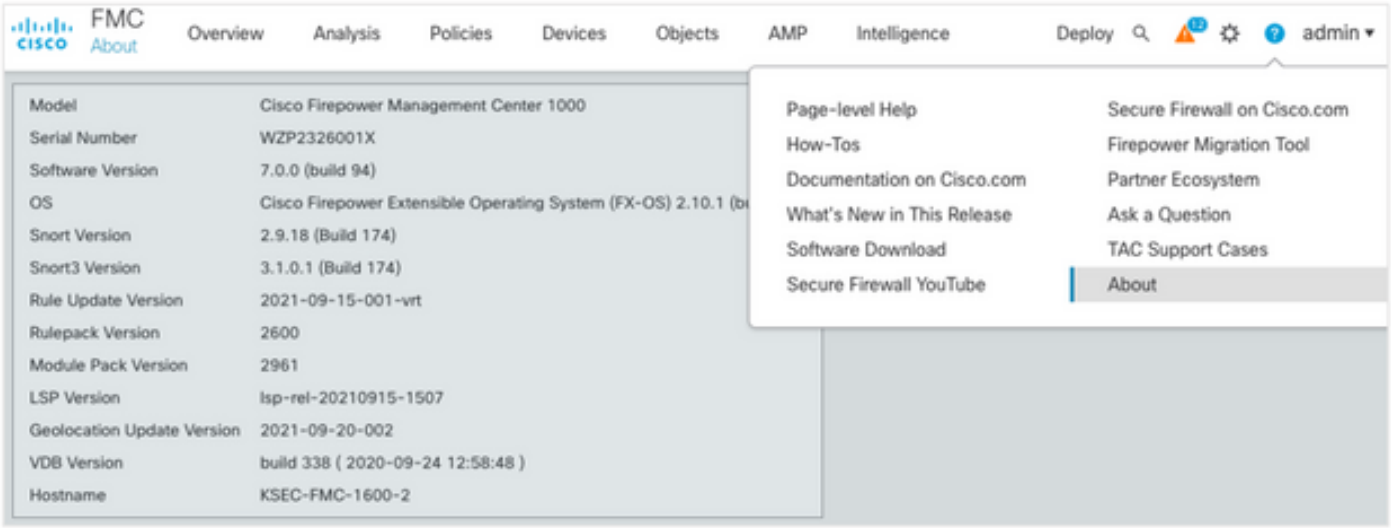
ターゲットバージョンのFirepowerリリースノートを確認し、次のことに精通してください。

- 互換性
- 機能
- 解決済みの問題
- 既知の問題

現在のFMCモデルとソフトウェアバージョンの確認

現在のFMCモデルとソフトウェアバージョンを確認します。

1. [ヘルプ] > [**バージョン情報]に移動します。**
2. モデルとソフ**トウェア**のバージョン**を確認します。**



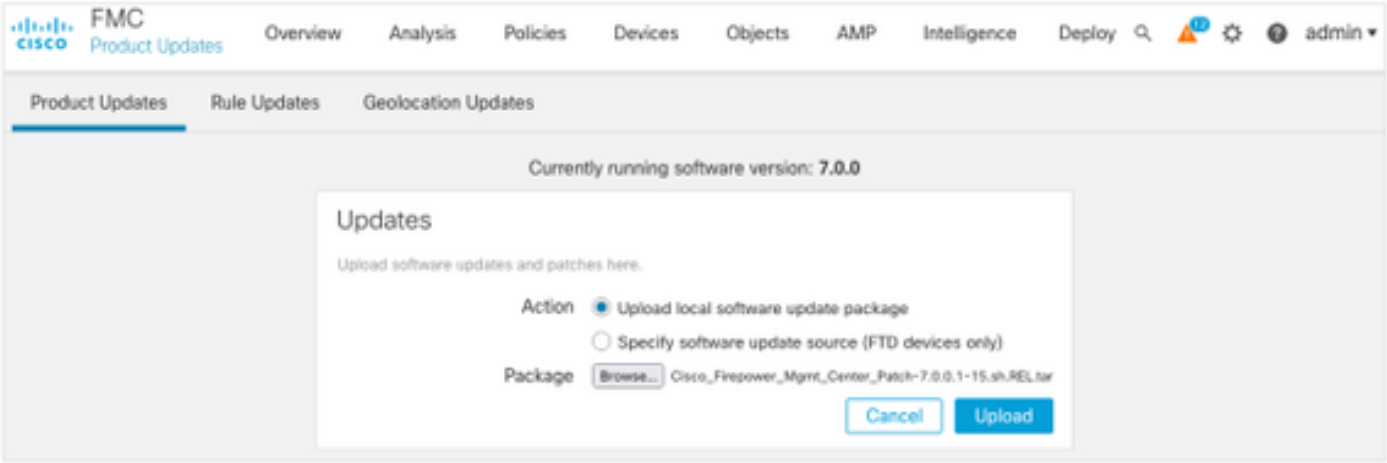
アップグレードパスの計画

現在および対象のFMCソフトウェアバージョンによっては、暫定アップグレードが必要になる場合があります。Cisco Firepower Management Centerアップグレード・ガイドで、アップグレード・パスを**確認します。Firepower Management Centerセクション**を参照し、アップグレードパスを計画します。

アップグレードパッケージのアップロード

アップグレードパッケージをデバイスにアップロードするには、次の手順を実行します。

1. ソフトウェアダウンロードページからアップグレードパッケージをダウンロードします。
2. FMCで、[System] > [**Updates**]に**移動します。**
3. [**Upload Update**]を**選択します。**
4. [Upload local software update package]**オプションボタンをクリ**ックします。
5. [**参照]をク**リックし、パッケージを選択します。
6. [Upload] をクリックします。

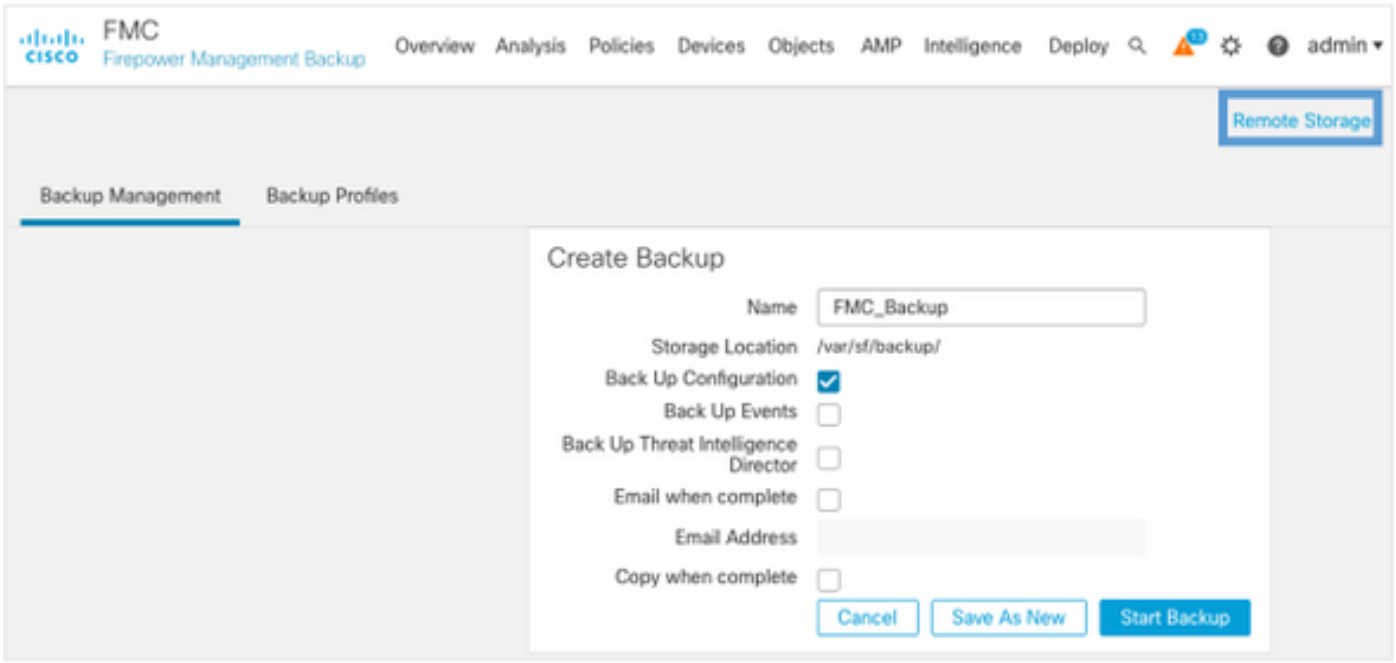


FMCバックアップの作成

バックアップは重要なディザスタリカバリ手順であり、アップグレードが大失敗した場合に設定を復元できます。

1. [**System**] > [**Tools**] > [**Backup/Restore]に移動します。**
2. [**Firepower Management Backup]を選択します。**
3. [名前]フ**ィールド**に、バックアップ名を入力します。
4. バックアップに含めるストレージの場所と情報を選択します。
5. [Start Backup] をクリックします。
6. [通知]**> [タスク]から**、バックアップの作成の進行状況を監視します。

ヒント：安全なリモートロケーションにバックアップし、転送が成功したことを確認することを強く推奨します。リモート記憶域は、[バックアップ管理]ページから構成できます。



詳細については、次を参照してください。

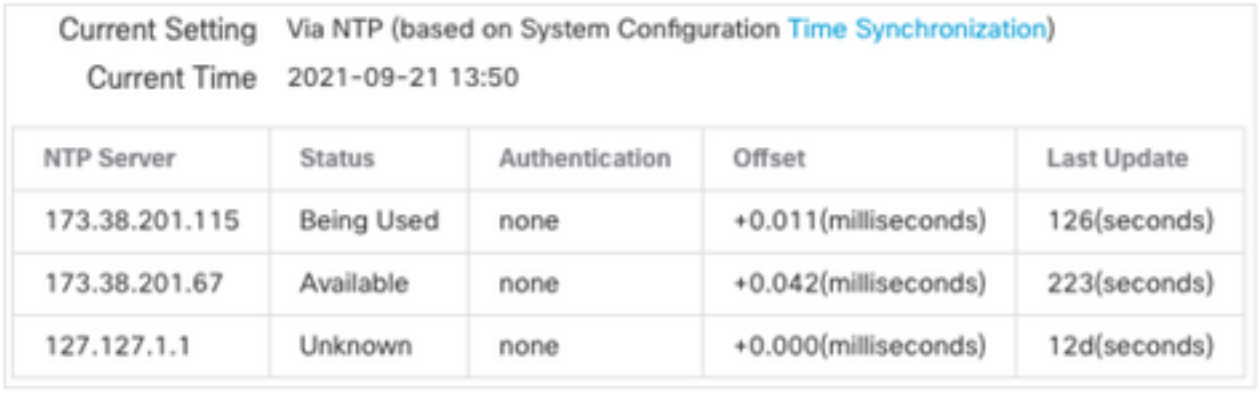
- Firepower Management Centerコンフィギュレーションガイド、バージョン7.0 – 章：バックアップと復元
- Firepower Management Centerコンフィギュレーションガイドバージョン7.0 – リモートストレージ管理

NTP同期の確認

FMCのアップグレードを成功させるには、NTP同期が必要です。NTP同期を確認するには、次の手順を実行します。

1. [システム(System)] > [設定(Configuration)] > [時間(Time)]に移動します。
2. NTPステータスを確認します。

注：ステータス：「使用中」は、アプライアンスがNTPサーバと同期されていることを示します。

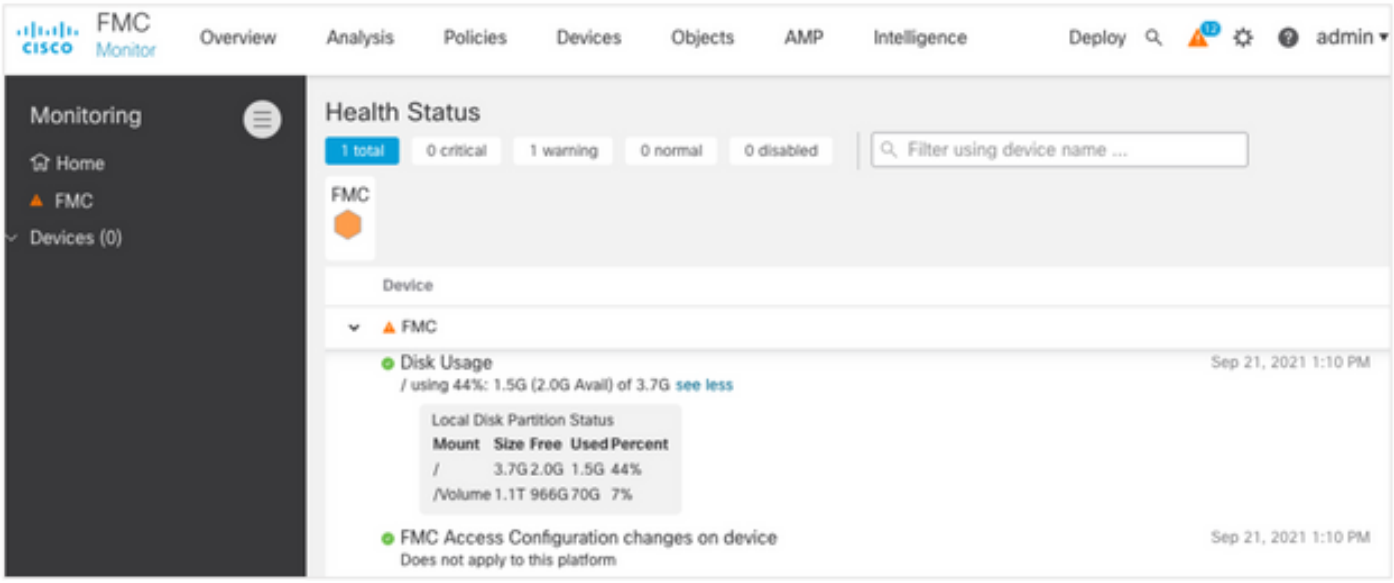


詳細については、『Firepower Management Centerコンフィギュレーションガイド、バージョン7.0 – 時刻と時刻の同期』を参照してください。

ディスク領域の確認

FMCのモデルとターゲットバージョンに応じて、使用可能な空きディスク領域が十分にあることを確認します。十分でない場合は、アップグレードが失敗します。使用可能なFMCディスク領域を確認するには、次の手順を実行します。

1. [System] > [Health] > [Monitor]に移動します。
2. FMCを選択します。
3. メニューを展開し、[ディスクの使い方]を検索します。
4. ディスク領域の要件は、「時間テストとディスク領域の要件」で確認できます。

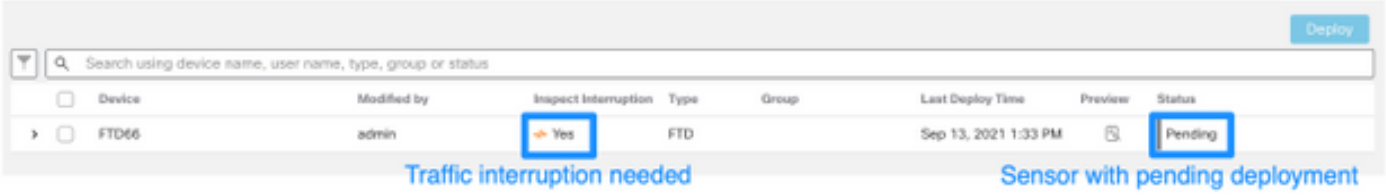


保留中のすべてのポリシー変更の展開

アップデートまたはパッチをインストールする前に、センサーに変更を導入する必要があります。保留中のすべての変更が展開されていることを確認するには、次の手順を実行します。

1. [Deploy] > [Deployment]に移動します。
2. リスト内のすべてのデバイスを選択し、展開します。

   注意：[Inspect Interrupt]列は、トラフィックの中断を示します



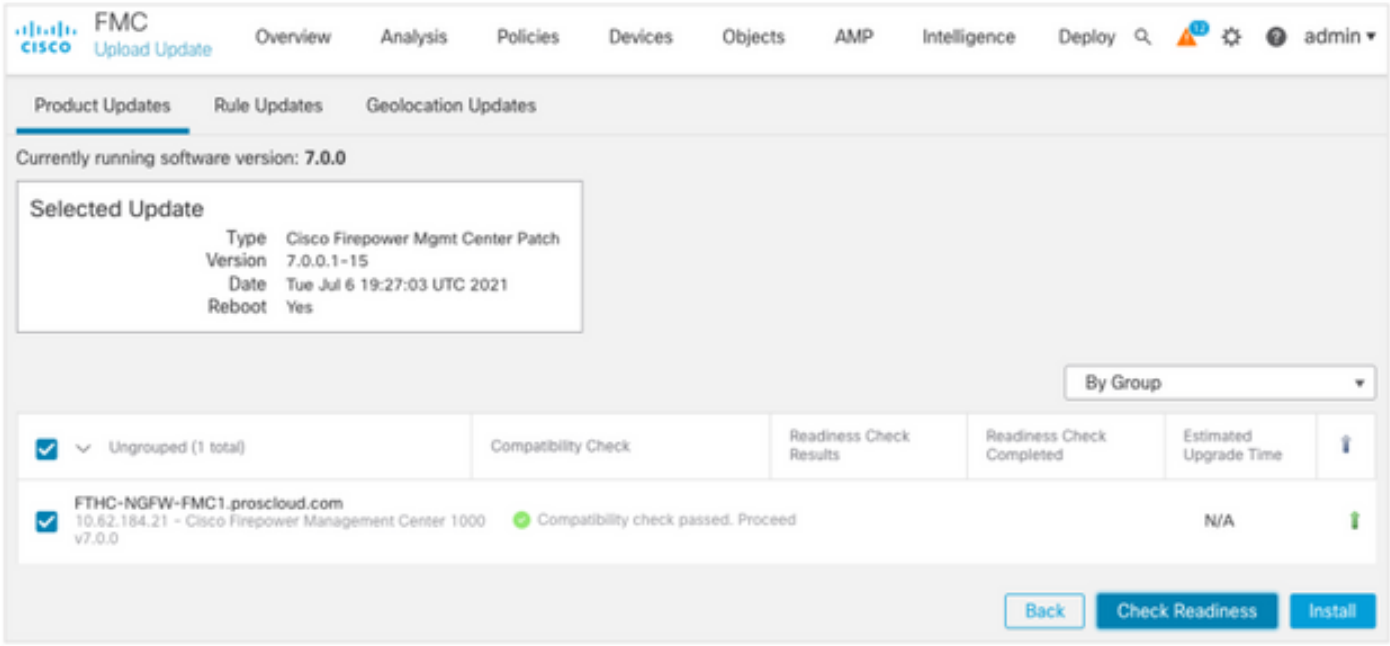
Firepowerソフトウェアの準備状況チェックの実行

レディネスチェックでは、Firepowerアプライアンスのソフトウェアアップグレードに対する準備状況を評価します。

ソフトウェアの準備状況チェックを実行するには、次の手順を実行します。

1. [システム(System)] > [更新(Updates)]に移動します。
2. ターゲットバージョンの横にある[インストール]アイコンを選択します。
3. FMCを選択し、[Check Readiness]をクリックします。

4. ポップアップウィンドウで、[OK]をクリックします。
5. [Notifications] > [Tasks]から[Readiness Check]プロセスを監視します。



詳細については、『Cisco Firepower Management Center Upgrade Guide - Firepower Software Readiness Checks』を参照してください。

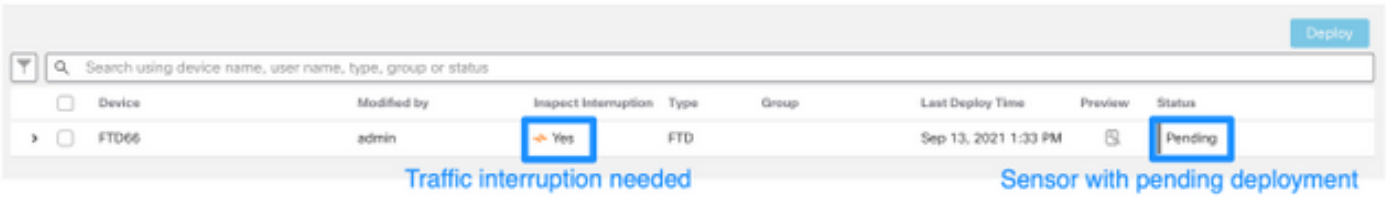
FMCアップグレード後の主な作業

保留中のすべてのポリシー変更の展開

アップデートまたはパッチのインストールが完了するたびに、センサーに変更を導入する必要があります。保留中のすべての変更が展開されていることを確認するには、次の手順を実行します。

1. [Deploy] > [Deployment]に移動します。
2. リスト内のすべてのデバイスを選択し、[Deploy]をクリックします。

   注意：[Inspect Interrupt]列は、トラフィックの中断を示します



最新の脆弱性とフィンガープリントのデータベースがインストールされているかどうかを確認する

現在のフィンガープリント(VDB)バージョンを確認するには、次の手順を実行します。

1. [ヘルプ] > [バージョン情報]に移動します。
2. VDBのバージョンを確認します。

cisco.comからVDBアップデートを直接ダウンロードするには、FMCからcisco.comへの到達可能

性が必要です。

1. [システム(System)] > [更新(Updates)] > [製品の更新(Product Updates)]に移動します。
2. [更新プログラムのダウンロード]を選択します。
3. 利用可能な最新バージョンをインストールします。
4. 後でセンサーを再配備する必要があります。

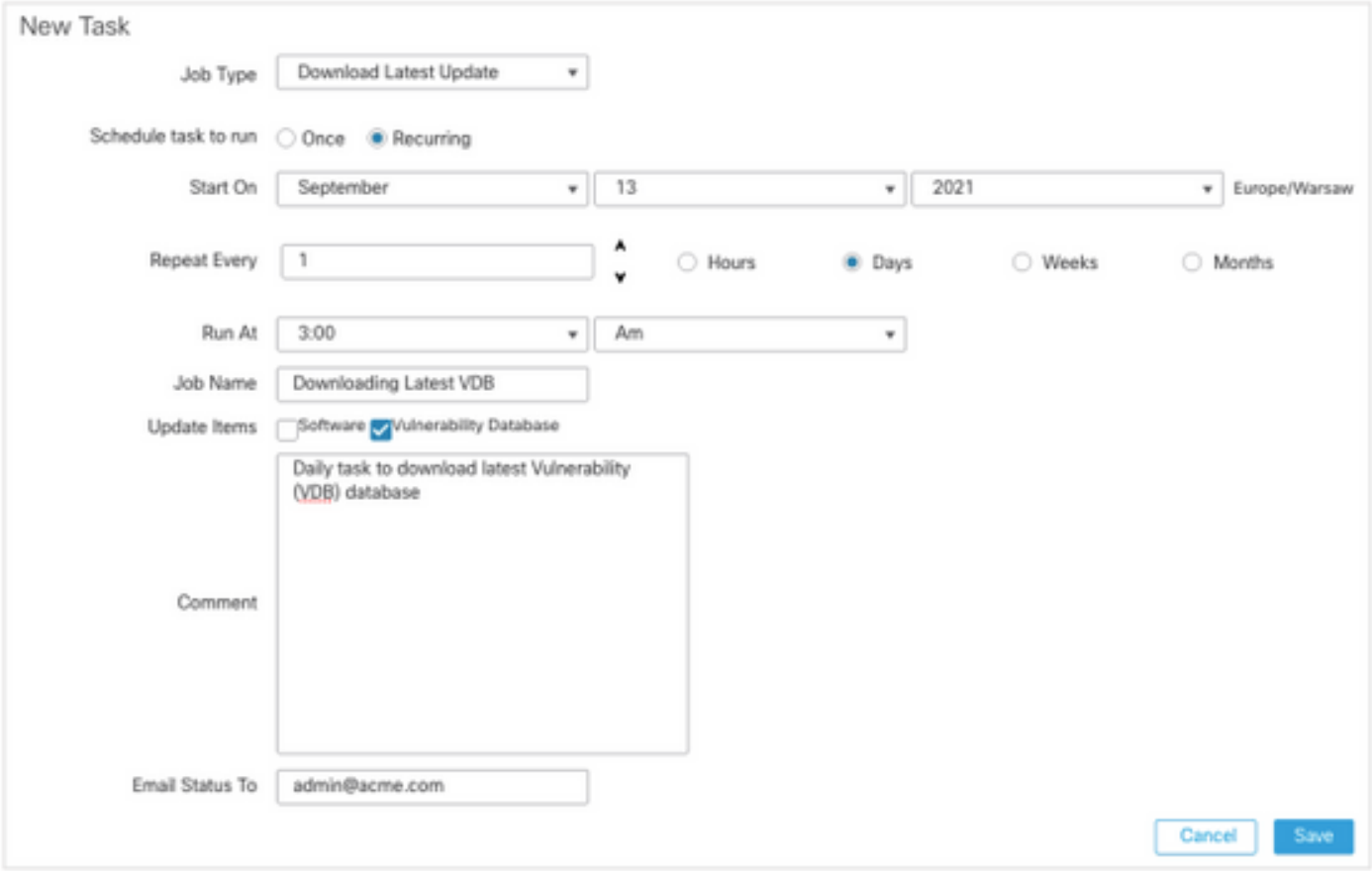
注：FMCがインターネットにアクセスできない場合、VDBパッケージは software.cisco.comから直接ダウンロードできます。

VDBパッケージの自動ダウンロードとインストールを実行するタスクをスケジュールすることをお勧めします。

ベストプラクティスとして、VDBアップデートを毎日確認し、週末にFMCにインストールしてください。

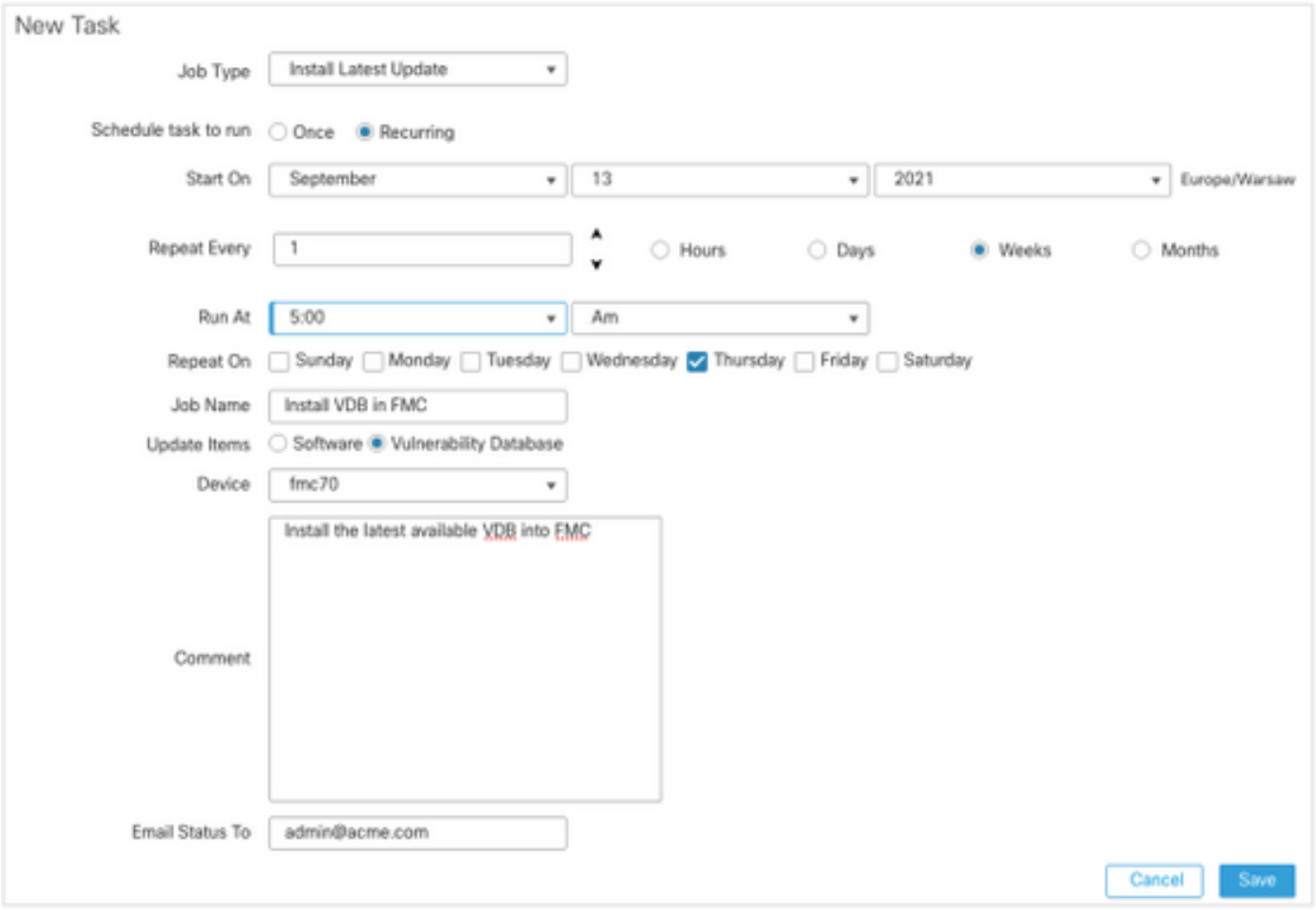
www.cisco.comから毎日VDBを確認するには、次の手順を実行します。

1. [システム(System)] > [ツール(Tools)] > [スケジュール(Scheduling)]に移動します。
2. [タスクの追加]をクリックします。
3. [ジョブの種類]ドロップダウンリストから、[最新の更新をダウンロード]を選択します。
4. タスクを実行するスケジュールを設定するには、[定期的な作業]ラジオボタンをクリックします.
5. 毎日タスクを繰り返し、午前3時または営業時間外に実行します。
6. [Update Items]で[Vulnerability Database]チェックボックスをオンにします.



最新のVDBをFMCにインストールするには、定期的なタスクを毎週設定します。

1. [システム(System)] > [ツール(Tools)] > [スケジュール(Scheduling)]に移動します。
2. [タスクの追加]をクリックします。
3. [ジョブの種類]ドロップダウンリストから、[最新の更新プログラムのインストール]を選択します。
4. [タスクの実行をスケジュールする]で、[定期的なタスク]ラジオボタンをクリックします。
5. 1週間ごとにタスクを繰り返し、午前5時または営業時間外に実行します。
6. [Update Items]には、[Vulnerability Database]チェックボックスをオンにします。



詳細については、『Firepower Management Center Configuration Guide, Version 7.0 - Update the Vulnerability Database (VDB)』を参照してください

SnortルールとLightweightセキュリティパッケージの現在のバージョンの確認

現在のSnort Rule(SRU)、Lightweight Security Package(LSP)、および位置情報のバージョンを確認するには、次の手順を実行します。

1. [ヘルプ] > [バージョン情報]に移動します。
2. ルール更新バージョンとLSPバージョンを確認してください。

SRUとLSPをwww.cisco.comから直接ダウンロードするには、FMCからwww.cisco.comへの到達可能が必要です。

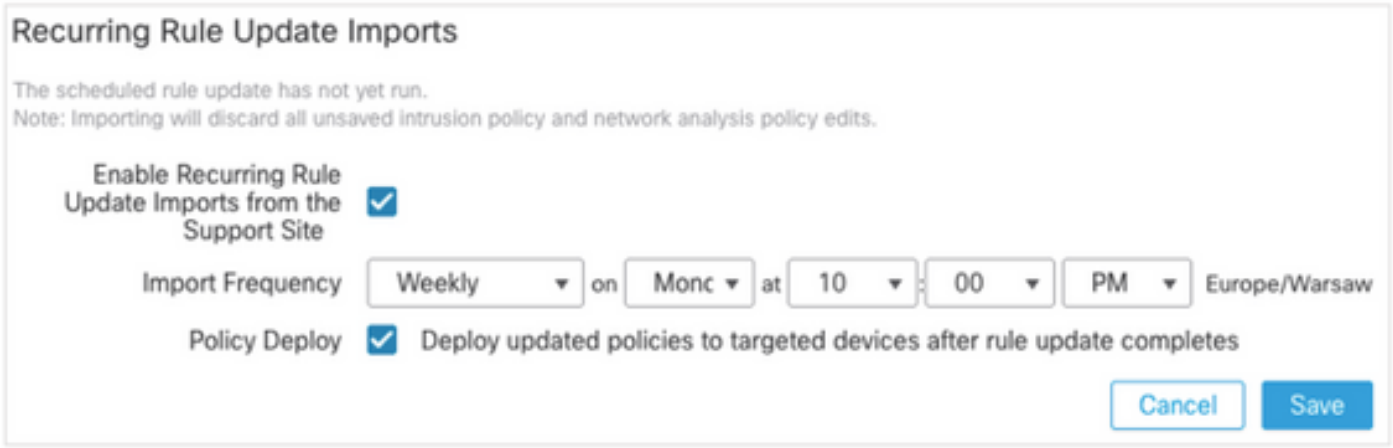
1. [システム(System)] > [更新(Updates)] > [ルールの更新(Rule Updates)]に移動します。
2. [ワンタイムルールの更新/ルールのインポート]タブで、[サポートサイトから新しいルールの更新をダウンロード]を選択します。
3. 「インポート」を選択します。
4. その後、センサーに設定を展開します。

注：FMCがインターネットにアクセスできない場合、SRUおよびLSPパッケージはsoftware.cisco.comから直接ダウンロードできます。

侵入ルールの更新は累積されるため、常に最新の更新をインポートすることをお勧めします。

Snortルールアップデート(SRU/LSP)の毎週のダウンロードと展開を有効にするには、次の手順を実行します。

1. [システム(**System**)] > **[更新(Updates)] > [ルールの更新(Rule Updates)]に移動します。**
2. [定期的なルールの更新**のインポート]タブで**、[サポートサイトから定期的なルールの更新**のインポートを有効にする]チェックボックスを**オンにします。
3. インポート頻度として[weekly]を選択し、ダウンロードとポリシーの導入に関して、週の1日と午後の遅れを選択します。
4. [Save] をクリックします。



詳細については、『Firepower Management Center Configuration Guide, Version 7.0 - Update Intrusion Rules』を参照してください。

位置情報の更新の現在のバージョンの確認

現在の位置情報バージョンを確認するには、次の手順を実行します。

1. [ヘルプ] > [**バージョン情報]に移動します。**
2. 位置情報の更新**バージョンを確認します。**

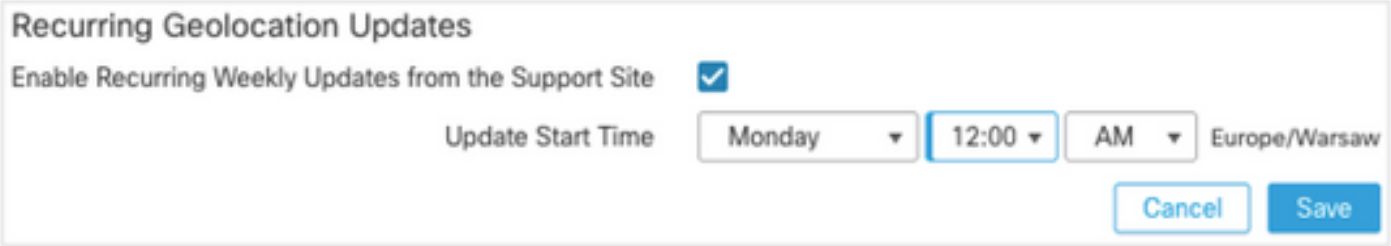
www.cisco.comから直接Geolocation Updatesをダウンロードするには、FMCからwww.cisco.comへの到達可能が必要です。

1. [システム(**System**)] > **[更新(Updates)] > [位置情報の更新(Geolocation Updates)]に移動します。**
2. [ワンタイム**位置情報の更新(One-Time Geolocation Update)]タブで**、[サポートサイト**から位置情報の更新をダウンロードしてインストールします。**
3. [Import] をクリックします。

注：FMCがインターネットにアクセスできない場合、Geolocation Updatesパッケージはsoftware.cisco.comから直接ダウンロードできます。

自動位置情報アップデートをオンにするには、次の手順を実行します。

1. [システム(System)] > **[更新(Updates)] > [位置情報の更新(Geolocation Updates)]に移動します。**
2. [定期的な位置情報の更新]セクションで、[サポートサイトから定期的な**毎週の更新を有効にする]チェックボックスを**オンにします。
3. インポート頻度として[weekly]を選択し、[Monday at midnight]を選択します。
4. [Save] をクリックします。

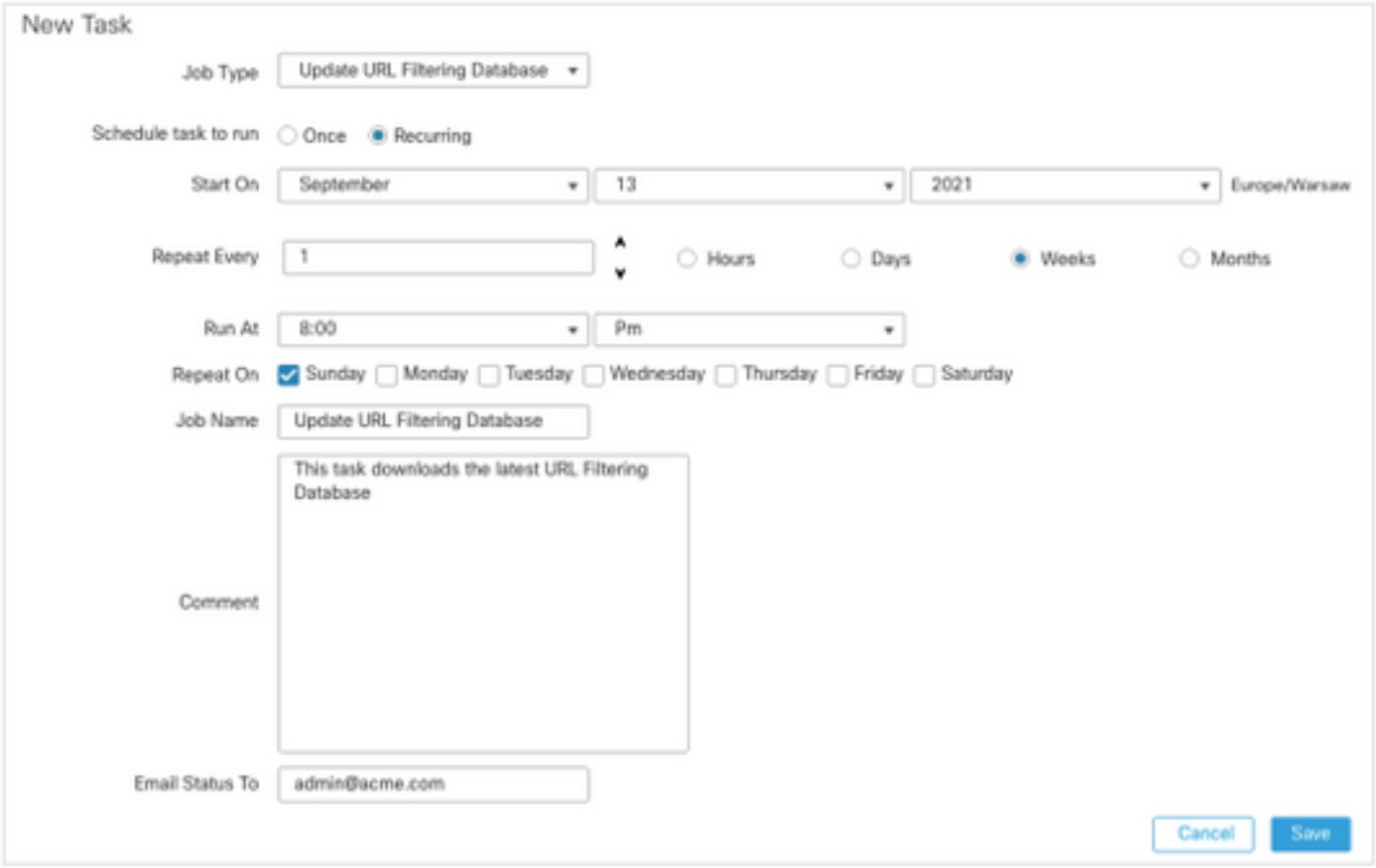


詳細については、『Firepower Management Center Configuration Guide, Version 7.0 - Update the Geolocation Database (GeoDB)』を参照してください。

スケジュールされたタスクによるURLフィルタリングデータベース更新の自動化

URLフィルタリングの脅威データが最新であることを確認するには、Cisco Collective Security Intelligence(CSI)クラウドからデータ更新を取得する必要があります。このプロセスを自動化するには、次の手順を実行します。

1. [システム(System)] > **[ツール(Tools)] > [スケジュール(Scheduling)]に移動します。**
2. [タスクの追**加]をクリックします。**
3. [ジョブの種類]**ドロップダウン**リストから、[URLフィルタリングデータベ**ースの更新]を選択します。**
4. [タスクを**実行するスケジュール]で、**[定期的なスケジュール]**オプションボタン**をクリックします。
5. 毎週タスクを繰り返し、日曜または営業時間外の午後8時に実行します。
6. [Save] をクリックします。

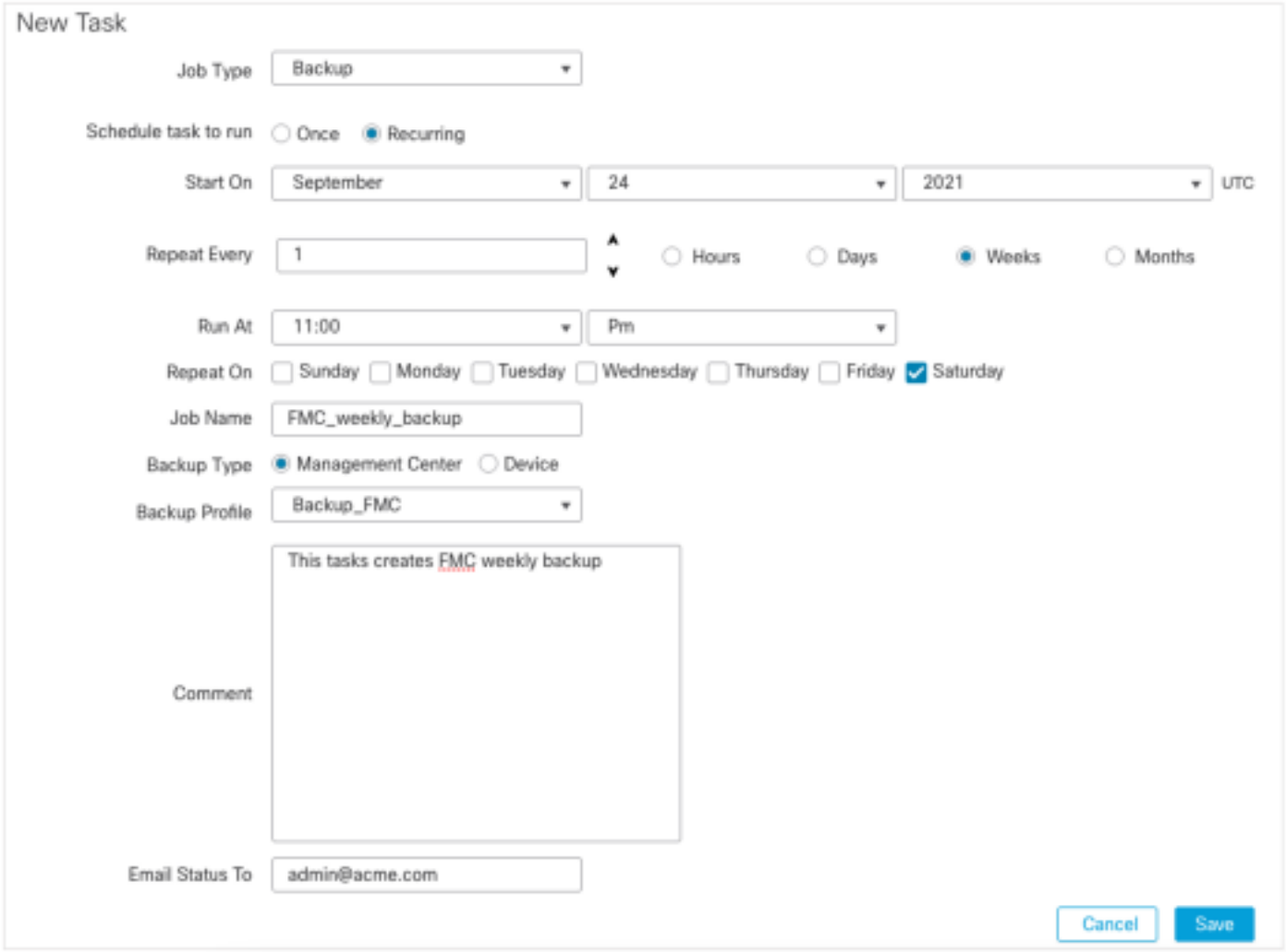


詳細については、『Firepower Management Center Configuration Guide, Version 7.0 - Automating URL Filtering Updates Using a Scheduled Task』を参照してください。

定期バックアップの設定

ディザスタリカバリ計画の一環として、定期的なバックアップを実行することをお勧めします。

1. グローバルドメインに属していることを**確認します**。
2. FMCバックアッププロファイルを作成します。詳細については、「FMCバックアップの**作成」セクションを参照して**ください。
3. [システム(System)] > **[ツール(Tools)] > [スケジュール(Scheduling)]に移動します**。
4. [タスクの追**加]をクリックします**。
5. [ジョブの種類]**ドロップダウン**リストから、[バックアップ]を選択**します。**
6. [タスクを**実行するスケジュール]で、**[定期的なスケジュール]**オプションボタン**をクリックします。
   バックアップの頻度は、組織のニーズに合わせて調整する必要があります。メンテナンス時間帯や使用率の低い時間帯にバックアップを作成することをお勧めします。
7. [バックアッ**プの種類]で、**[Management Center]ラジオ・ **ボタンをク**リックします。
8. [バックアッ**ププロファイル**]ドロップダウンリストから、[バックアッププロファイル]を選択します。
9. [Save] をクリックします。

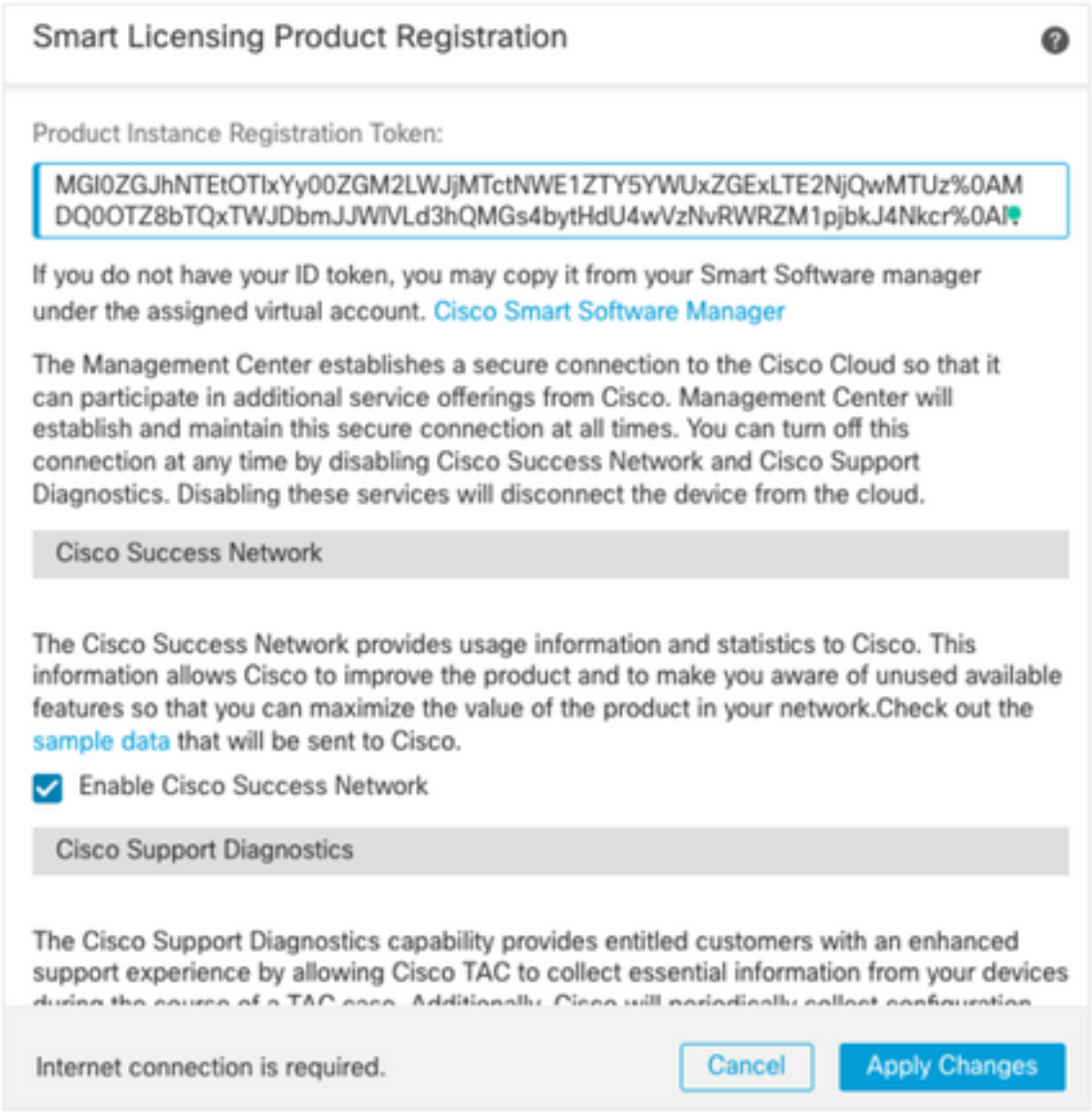


詳細については、『Firepower Management Center Configuration Guide, Version 7.0 - Chapter:バックアップと復元.

スマートライセンスが登録されていることを確認する

Cisco Firewall Management CenterをCisco Smart Software Managerに登録するには、次の手順を実行します。

1. https://software.cisco.comで、[**Smart Software Manager**] > [**Manage licenses**]**に移動します**。
2. [Inventory] > [**General**]**タブに移動**し、新しいトークンを**作成します**。
3. FMC UIで、[**System**] > [**Licenses**] > [Smart Licenses]**に移動します**。
4. [Register] をクリックします。
5. Cisco Smart Software Licensingポータルで生成されたトークンを挿入します。
6. [The **Cisco Success Network**]**が有効になっていることを確認します**。
7. [Apply Changes] をクリックします。
8. スマートライセンスのステータスを確認します。



詳細については、『Firepower Management Center Configuration Guide, Version 7.0 - Register Smart Licenses』を参照してください。

変数セットの設定の確認

HOME_NET変数に組織内の内部ネットワーク/サブネットだけが含まれていることを確認します。不適切な変数セット定義は、ファイアウォールのパフォーマンスに悪影響を及ぼします。

1. 「オブジェクト」>「変数セット」に移動します。
2. 侵入ポリシーで使用する変数セットを編集します。異なる設定の侵入ポリシーごとに1つの変数を設定できます。
3. 環境に応じて変数を調整し、[保存]をクリックします。

対象となる他の変数は、DNS_SERVERSまたはHTTP_SERVERSです。

詳細については、『Firepower Management Centerコンフィギュレーションガイド、バージョン7.0 – 変数セット』を参照してください。

クラウドサービスの有効化の確認

さまざまなクラウドサービスを利用するには、[システム(System)] > [統合(Integration)] > [クラウ

ドサービス(Cloud Services)]に移動します。

URL フィルタリング

1. URLフィルタリングを有効にして、自動更新を許可し、[Query Cisco Cloud for Unknown URLs]をオンにします。
   キャッシュURLの有効期限が頻繁に発生すると、クラウドに対するクエリが増えるため、Web口ードが遅くなります。
2. **変更を保存します。**

ヒント：キャッシュURLの有効期限の場合は、デフォルトの[Never]**のままにします。**より厳密なWeb再分類が必要な場合は、この設定を適宜変更できます。

AMP for Networks

1. 両方の設定がオンになっていることを確認します。**自動ローカルマルウェア検出の更新を有効**にし、**マルウェアイベントからのURIをシスコと共有します。**
2. FMC 6.6.Xでは、ネットワーク用AMPのレガシーポート32137の使用を無効にして、代わりに使用されるTCPポートが443になるようにします。
3. **変更を保存します。**

注：この設定はFMC 7.0+では使用できなくなり、ポートは常に443になります。

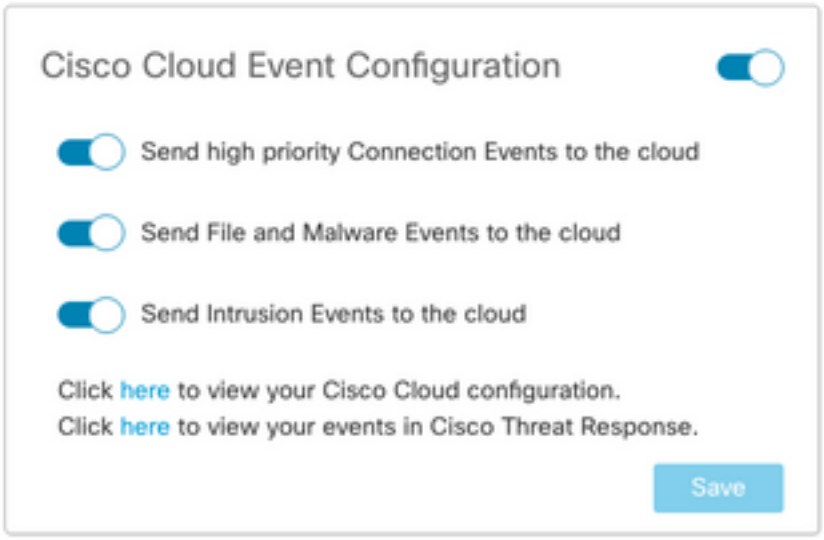
シスコクラウド地域

1. クラウド領域は、SecureX組織領域と一致する必要があります。SecureX組織が作成されていない場合は、FMCのインストールに近い地域を選択します。 APJ地域、EU地域、または米国地域。
2. **変更を保存します。**

Cisco Cloud Event Configuration

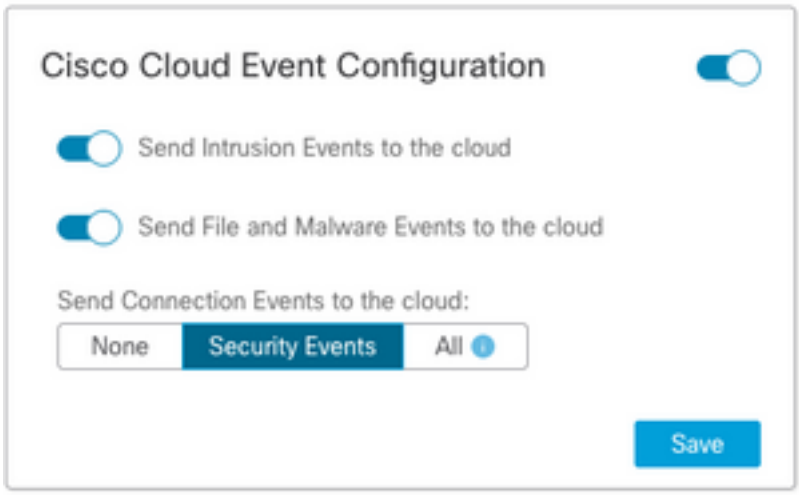
FMC 6.6.xの場合

1. 次の3つのオプションすべてを確認します。**クラウドへの優先度の高い接続イベントの送信**、クラウドへのファイ**ルおよびマルウェアイベントの送信、およびクラウドへの侵入イ**ベントの**送信が選択**されます。
2. **変更を保存します。**



FMC 7.0以降

1. 両方のオプションが選択されていることを確認します。**侵入イベントをクラウドに送信**し、**ファイルとマルウェアイベントをクラウドに送信します**。
2. 接続イベントのタイプとして、[Security Analytics and Logging]ソリューションが使用されている場合は**[All]** を選択します。SecureXの場合は、[セキュリティイベント]**のみを選択します**。
3. **変更を保存します。**



SecureX統合の有効化

SecureXの統合により、シスコのセキュリティ製品全体にわたる脅威の状況を瞬時に可視化できます。SecureXを接続してリボンを有効にするには、次の手順を実行します。

SecureXリボンの統合

注：このオプションは、FMCバージョン7.0以降で使用できます。

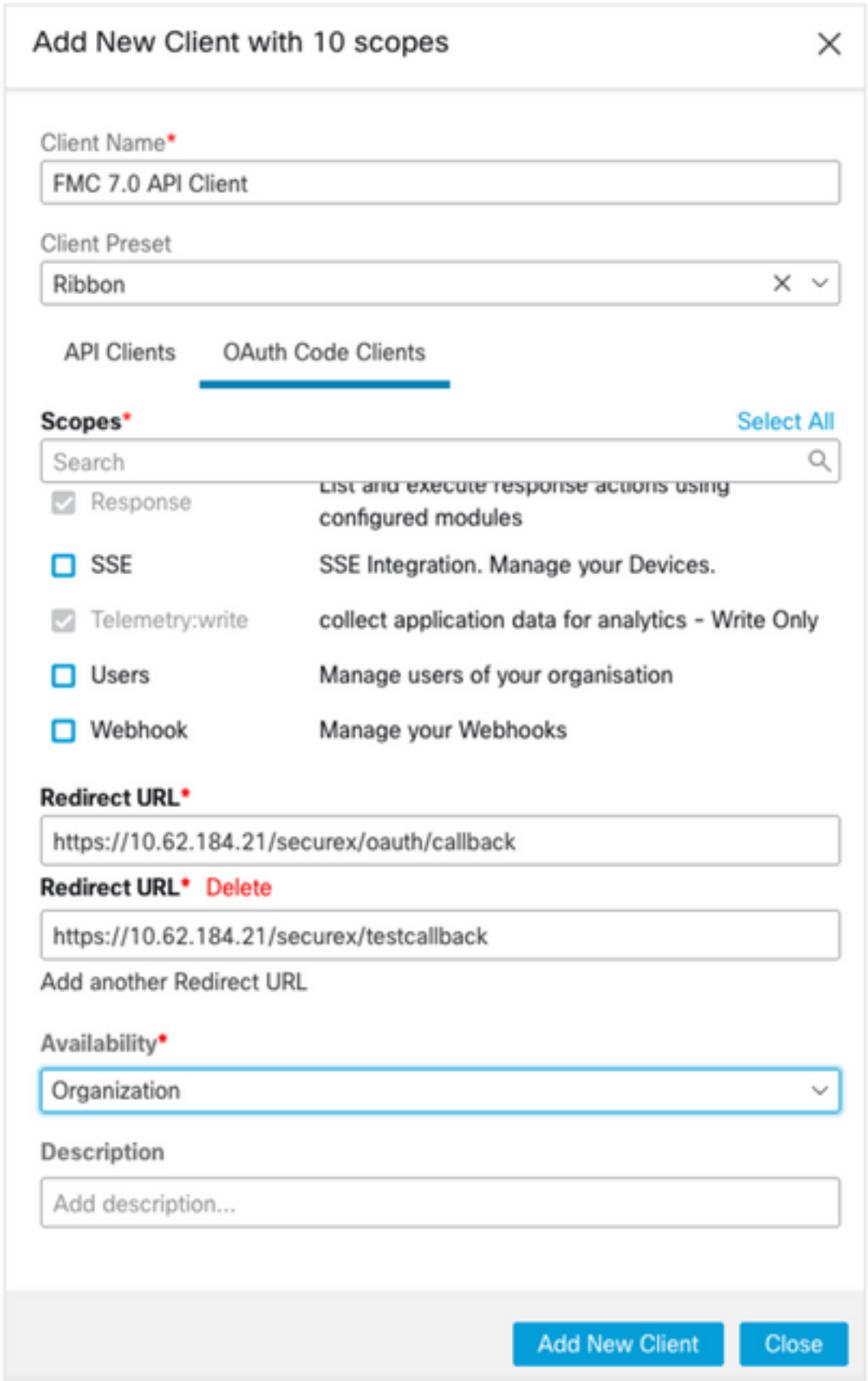
1. SecureXにログインし、APIクライアントを作成します。 [クライ**アント名**]フィールドに、FMCのわかりやすい名前を入力します。たとえば、FMC 7.0 API Clientなどです。[Oauth Code Clients]タブ**をクリック**します。[クライアントプ**ロセット**]ドロップダウンリストで、[リボン]を**選択します**。スコープを選択します。Casebook, Enrich:read, Global Intel:read,

Inspect:read, Notification, Orbital, Private Intel, Profile, Response, Telemetry:write.FMCに表示される2つのリダイレクトURLを追加します。

リダイレクトURL:<FMC_URL>/securex/oauth/callback

2番目のリダイレクトURL:<FMC_URL>/securex/testcallback

1. [可用性]ドロップダウンリストで、[組織]を選択します。[Add New Client]をクリックします。



2. FMCから、[System] > [SecureX]に移動します。

3.右上隅の切り替えをオンにし、表示されている領域がSecureX組織と一致することを確認します。

4.クライアントIDとクライアントパスワードをコピーし、FMCに貼り付けます。

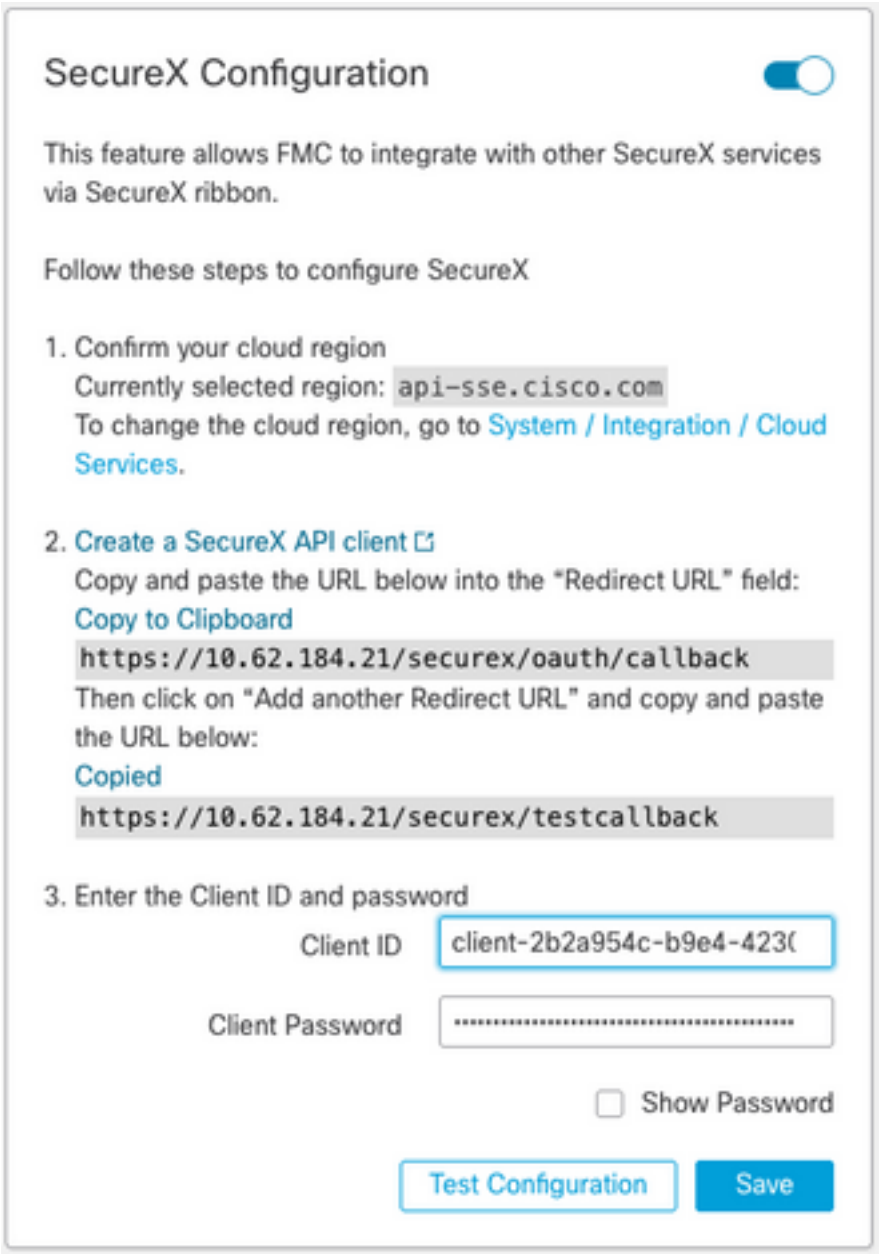
5. 「**test the configuration**」を選択します。

6. SecureXにログインして、APIクライアントを承認します。

7.変更を保存し、ブラウザを更新して、下部にリボンが表示されるようにします。

8.リボンを展開し、[**SecureX**]を選択します。プロンプトが表示されたら、SecureXクレデンシャルを入力します。

9. SecureXリボンがFMCユーザに対して完全に機能するようになりました。

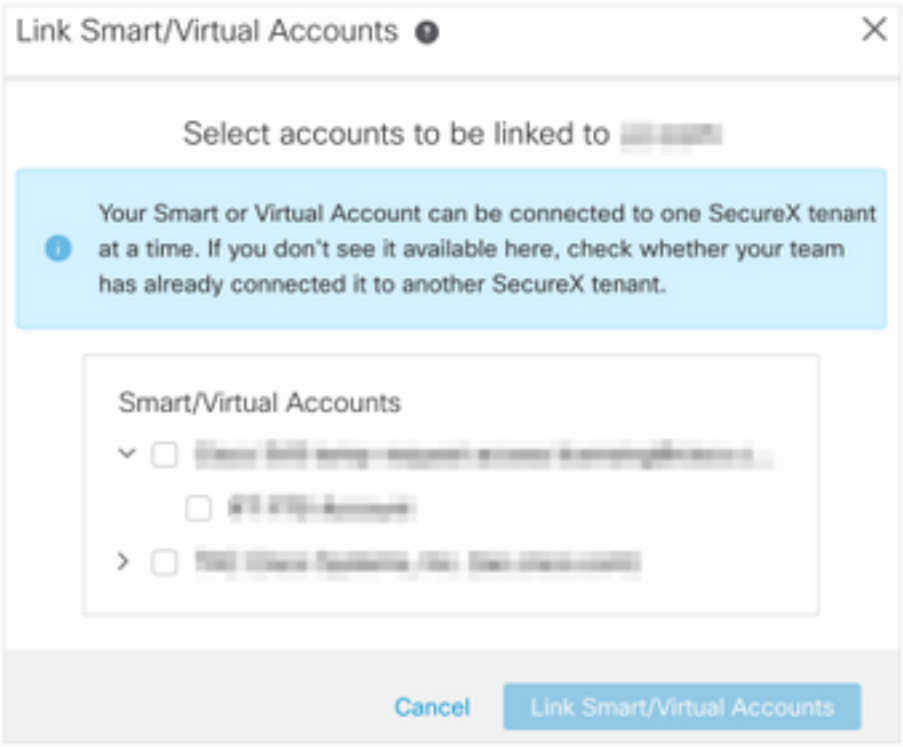


5YVPsGdzrkX8q8q0yYl-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

> **注**：他のFMCユーザがリボンへのアクセスを必要とする場合、そのユーザはSecureXクレデンシャルを使用してリボンにログインする必要があります。

SecureXへの接続イベントの送信

1. FMCで、[System] > [Integration] > [Cloud Services]に移動し、[Cisco Cloud Event Configuration]で[Turn on Cloud Services]セクションで説明されているように、侵入、ファイル、およびマルウェアイベントが送信されることを確認します。
2. 「スマートライセンスの登録」セクションの説明に従って、FMCがスマートライセンスに登録されていることを確認します。
3. FMCの[システム(System)] > [ライセンス(Licenses)] > [スマートライセンス(Smart Licenses)]に表示される[割り当て済み仮想アカウント(Assigned virtual Account)]名をメモします。
4. FMCをSecureXに登録します。 SecureXで、[Administration] > [Devices]に移動します。「デバイスの管理」を選択します。ブラウザでポップアップウィンドウが許可されていることを確認します。セキュリティサービス交換(SSE)にログインします。[Tools]メニュー> [Link Smart/Virtual Accounts]に移動します。[Link more accounts]を選択します。FMCに割り当てられた仮想アカウントを選択します（ステップ3）。[Link Smart/Virtual Accounts]を選択します。



- FMCデバイスが[Devices]にリストされていることを確認します。
- [クラウドサービス]タブに移動し、Cisco SecureXの脅威に対する応答とイベント機能をオンにしてください。
- イベント機能の横にある追加サービス設定（歯車アイコン）を選択します。
- [全般]タブで、[Share event data with Talos]を選択します。
- [イベントの自動昇格]タブの[イベントタイプ別]セクションで、使用可能なすべてのイベントタイプと[保存]を選択します。

5.メインのSecureXポータルで、[統合モジュール(Integration Modules)] > [Firepower]に移動し、Firepower統合モジュールを追加します。

6.新しいダッシュボードを作成します。

7. Firepower関連タイルを追加します。

セキュアエンドポイント(AMP for Endpoint)の統合

Firepowerの導入でセキュアエンドポイント（エンドポイント用AMP）の統合を有効にするには、次の手順を実行します。

1. [AMP] > [AMP Management]に移動します。
2. [Add AMP Cloud Connection]を選択します。
3. クラウドと登録を選択します。

   注：ステータス[有効]は、クラウドへの接続が確立されたことを意味します。

統合 Secure Malware Analytics(Threat Grid)

デフォルトでは、Firepower Management CenterはパブリックCisco Threat Gridクラウドに接続して、ファイルの送信とレポートの取得を行うことができます。この接続を削除することはできません。ただし、導入クラウドに最も近いものを選択することをお勧めします。

1. [AMP] > [動的分析接続]に移動します。
2. [Action]セクションの[Edit]（鉛筆アイコン）をクリックします。
3. 正しいクラウド名を選択します。
4. Threat Gridアカウントを関連付けて、詳細なレポート機能と高度なサンドボックス機能を使用するには、[関連付け(Associate)]アイコンをクリックします。

詳細については、『Firepower Management Center Configuration Guide, Version 7.0 - Enabling Access to Dynamic Analysis Results in the Public Cloud』を参照してください。

オンプレミスのスレッドグリッドアプライアンスの統合については、Firepower Management Centerコンフィギュレーションガイド、バージョン7.0 - Dynamic Analysis On-Premises Appliance(Cisco Threat Grid)を参照してください。