

FMC 6.6.1+ : アップグレードの前後のヒント

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[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](#)

[現在のFMCモデルとソフトウェアバージョンの確認](#)

[アップグレードパスの計画](#)

[アップグレードパッケージのアップロード](#)

[FMCバックアップの作成](#)

[NTP同期の確認](#)

[ディスク領域の確認](#)

[保留中のすべてのポリシー変更の展開](#)

[Firepowerソフトウェアの準備状況チェックの実行](#)

[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](#)

[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](#)

[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](#)

[位置情報の更新の現在のバージョンの確認](#)

[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](#)

[定期バックアップの設定](#)

[スマートライセンスが登録されていることを確認する](#)

[変数セットの設定の確認](#)

[クラウドサービスの有効化の確認](#)

[URLフィルタリング](#)

[AMP for Networks](#)

[シスコクラウド地域](#)

[Cisco Cloud Event Configuration](#)

[SecureX統合の有効化](#)

[SecureXリボンの統合](#)

[SecureXへの接続イベントの送信](#)

[セキュアエンドポイント\(AMP for Endpoint\)の統合](#)

[セキュアなマルウェア分析の統合\(Threat Grid\)](#)

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。

The screenshot shows the Cisco FMC 'About' page. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and 'admin'. The main content area displays system information in a table:

| | |
|----------------------------|--|
| Model | Cisco Firepower Management Center 1000 |
| Serial Number | WZP2326001X |
| Software Version | 7.0.0 (build 94) |
| OS | Cisco Firepower Extensible Operating System (FX-OS) 2.10.1 (build 174) |
| Snort Version | 2.9.18 (Build 174) |
| Snort3 Version | 3.1.0.1 (Build 174) |
| Rule Update Version | 2021-09-15-001-vrt |
| Rulepack Version | 2600 |
| Module Pack Version | 2961 |
| LSP Version | isp-rel-20210915-1507 |
| Geolocation Update Version | 2021-09-20-002 |
| VDB Version | build 338 (2020-09-24 12:58:48) |
| Hostname | KSEC-FMC-1600-2 |

On the right side, a help menu is open, listing various resources:

- Page-level Help
- How-Tos
- Documentation on Cisco.com
- What's New in This Release
- Software Download
- Secure Firewall YouTube
- Secure Firewall on Cisco.com
- Firepower Migration Tool
- Partner Ecosystem
- Ask a Question
- TAC Support Cases
- About

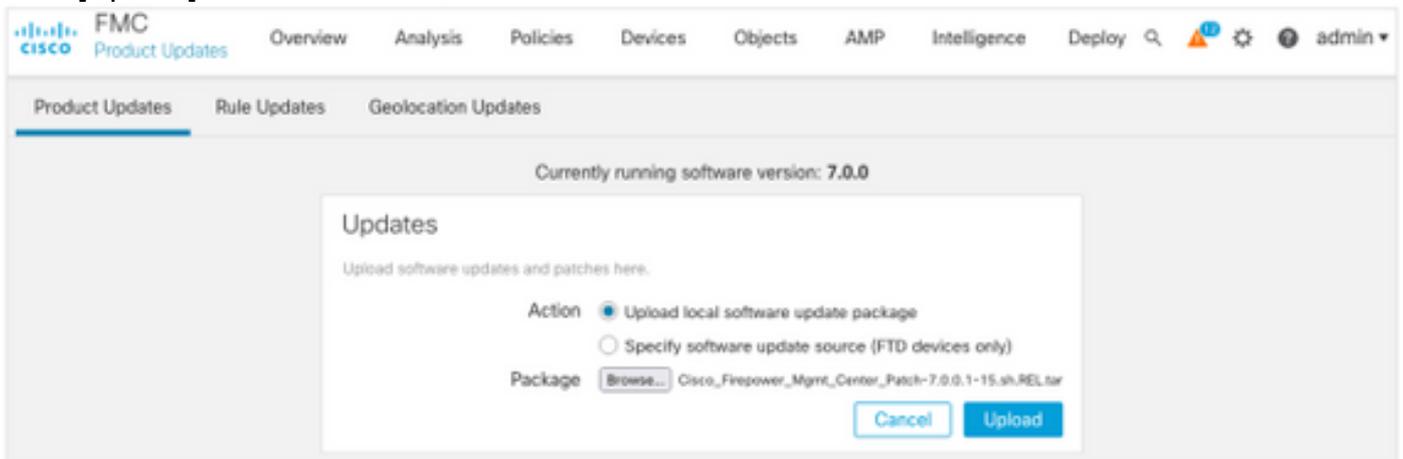
アップグレードパスの計画

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。

The screenshot shows the Cisco FMC interface for configuring a backup. The 'Create Backup' dialog is displayed with the following settings:

- Name: FMC_Backup
- Storage Location: /var/sf/backup/
- Back Up Configuration:
- Back Up Events:
- Back Up Threat Intelligence Director:
- Email when complete:
- Email Address: (empty field)
- Copy when complete:

Buttons at the bottom of the dialog include 'Cancel', 'Save As New', and 'Start Backup'.

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。

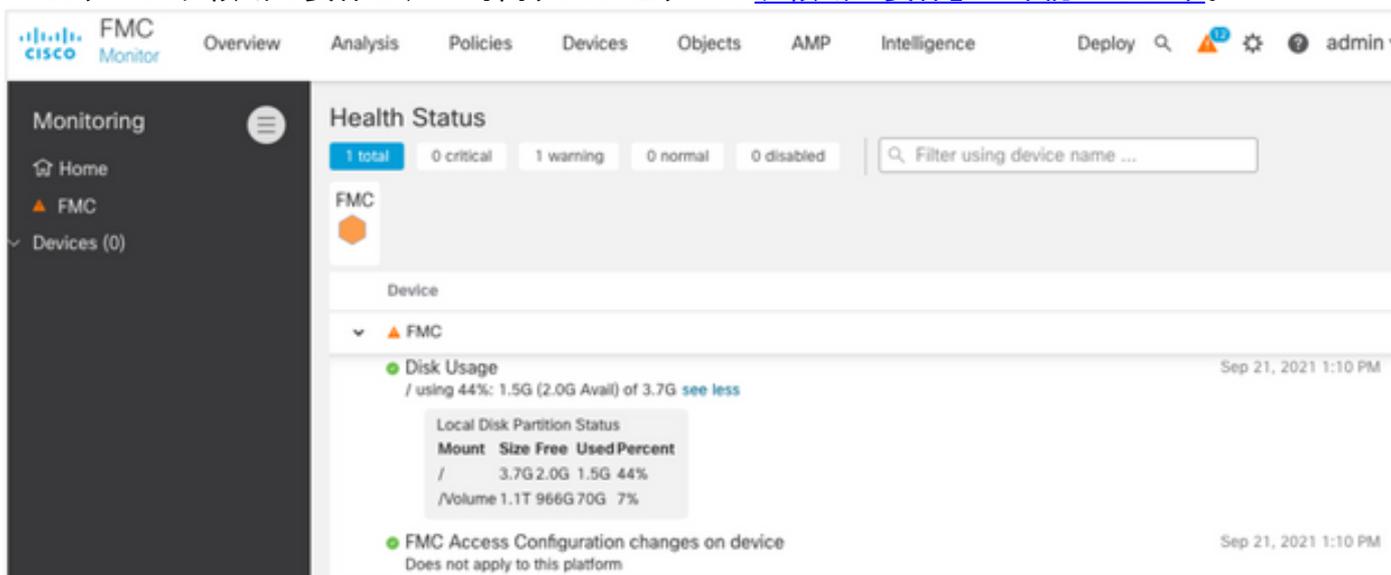
| Current Setting | | Via NTP (based on System Configuration Time Synchronization) | | |
|-----------------|------------------|---|----------------------|--------------|
| Current Time | 2021-09-21 13:50 | | | |
| NTP Server | Status | Authentication | Offset | Last Update |
| 173.38.201.115 | Being Used | none | +0.011(milliseconds) | 126(seconds) |
| 173.38.201.67 | Available | none | +0.042(milliseconds) | 223(seconds) |
| 127.127.1.1 | Unknown | none | +0.000(milliseconds) | 12d(seconds) |

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。

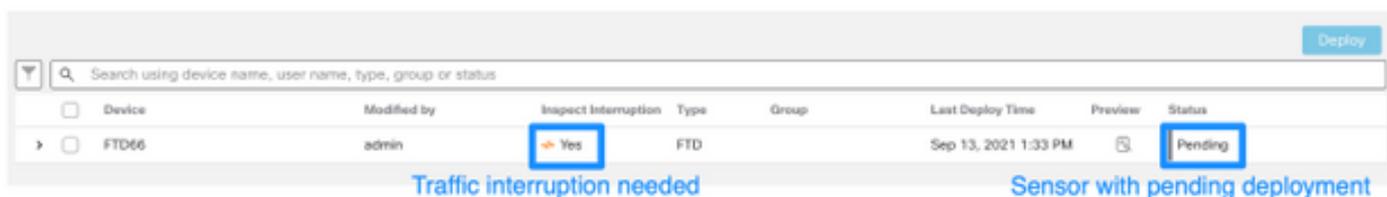


保留中のすべてのポリシー変更の展開

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。

The screenshot shows the Cisco FMC Upgrade interface. At the top, there are navigation tabs: Product Updates, Rule Updates, and Geolocation Updates. Below these, it states 'Currently running software version: 7.0.0'. A 'Selected Update' box contains the following information:

| | |
|---------|-----------------------------------|
| Type | Cisco Firepower Mgmt Center Patch |
| Version | 7.0.0.1-15 |
| Date | Tue Jul 6 19:27:03 UTC 2021 |
| Reboot | Yes |

Below this, there is a table with columns: Compatibility Check, Readiness Check Results, Readiness Check Completed, and Estimated Upgrade Time. A dropdown menu 'By Group' is visible. The table shows one entry for 'FTHC-NGFW-FMC1.proscloud.com' with a status of 'Compatibility check passed. Proceed' and an estimated upgrade time of 'N/A'. At the bottom, there are buttons for 'Back', 'Check Readiness', and 'Install'.

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

The screenshot shows the Cisco FMC Deployment interface. At the top right, there is a 'Deploy' button. Below it is a search bar: 'Search using device name, user name, type, group or status'. A table lists devices with the following columns: Device, Modified by, Inspect Interruption, Type, Group, Last Deploy Time, Preview, and Status. The table contains one entry for 'FTD66' with 'admin' as the modifier, 'Yes' in the 'Inspect Interruption' column, 'FTD' as the type, and 'Pending' in the 'Status' column. Below the table, there are two blue text labels: 'Traffic interruption needed' and 'Sensor with pending deployment'.

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。

New Task

Job Type: Download Latest Update

Schedule task to run: Once Recurring

Start On: September 13, 2021 Europe/Warsaw

Repeat Every: 1 Days (radio buttons for Hours, Days, Weeks, Months)

Run At: 3:00 Am

Job Name: Downloading Latest VDB

Update Items: Software Vulnerability Database

Comment: Daily task to download latest Vulnerability (VDB) database

Email Status To: admin@acme.com

Buttons: Cancel, Save

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нта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。

Recurring Rule Update Imports

The scheduled rule update has not yet run.
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site

Import Frequency: Weekly on Monc at 10:00 PM Europe/Warsaw

Policy Deploy Deploy updated policies to targeted devices after rule update completes

Cancel Save

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。

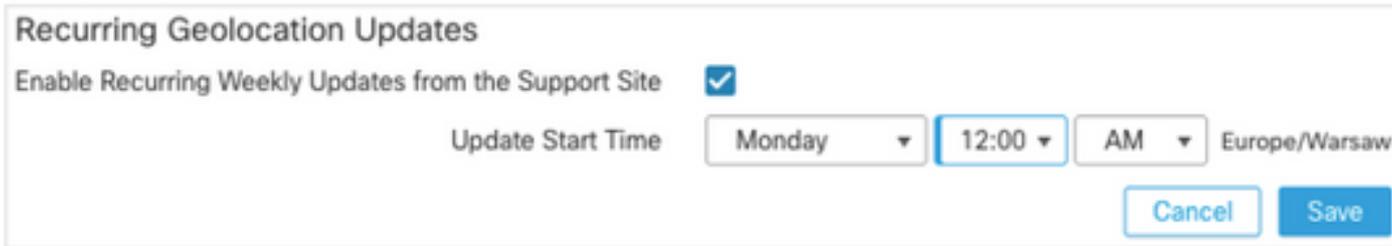
www.cisco.com から直接Geolocation Updatesをダウンロードするには、FMCから www.cisco.com への到達可能が必要です。

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。



Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site

Update Start Time Monday 12:00 AM Europe/Warsaw

Cancel Save

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。

New Task

Job Type

Schedule task to run Once Recurring

Start On Europe/Warsaw

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Comment

Email Status To

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。

New Task

Job Type

Schedule task to run Once Recurring

Start On UTC

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Backup Type Management Center Device

Backup Profile

Comment

Email Status To

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。

Smart Licensing Product Registration

Product Instance Registration Token:

MGI0ZGJhNTEtOTIxYy00ZGM2LWJjMTctNWE1ZTY5YWUxZGExLTE2NjQwMTUz%0AM
DQ00TZ8bTQxTWJDbmJJWlVld3hQMGS4bytHdU4wVzNvRWRZM1pjbk.J4Nkcr%0A!

If you do not have your ID token, you may copy it from your Smart Software manager under the assigned virtual account. [Cisco Smart Software Manager](#)

The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the device from the cloud.

Cisco Success Network

The Cisco Success Network provides usage information and statistics to Cisco. This information allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the [sample data](#) that will be sent to Cisco.

Enable Cisco Success Network

Cisco Support Diagnostics

The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your devices during the course of a TAC case. Additionally, Cisco will periodically collect configuration

Internet connection is required.

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ロ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。**

Cisco Cloud Event Configuration

Send high priority Connection Events to the cloud

Send File and Malware Events to the cloud

Send Intrusion Events to the cloud

Click [here](#) to view your Cisco Cloud configuration.
Click [here](#) to view your events in Cisco Threat Response.

Save

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。

Cisco Cloud Event Configuration

Send Intrusion Events to the cloud

Send File and Malware Events to the cloud

Send Connection Events to the cloud:

None Security Events All

Save

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サ]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。
。

Add New Client with 10 scopes ✕

Client Name*

Client Preset
 ✕ ▾

API Clients OAuth Code Clients

Scopes* Select All

🔍

| | |
|---|--|
| <input checked="" type="checkbox"/> Response | List and execute response actions using configured modules |
| <input type="checkbox"/> SSE | SSE Integration. Manage your Devices. |
| <input checked="" type="checkbox"/> Telemetry:write | collect application data for analytics - Write Only |
| <input type="checkbox"/> Users | Manage users of your organisation |
| <input type="checkbox"/> Webhook | Manage your Webhooks |

Redirect URL*

Redirect URL* Delete

Add another Redirect URL

Availability*
 ▾

Description

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。

SecureX Configuration

This feature allows FMC to integrate with other SecureX services via SecureX ribbon.

Follow these steps to configure SecureX

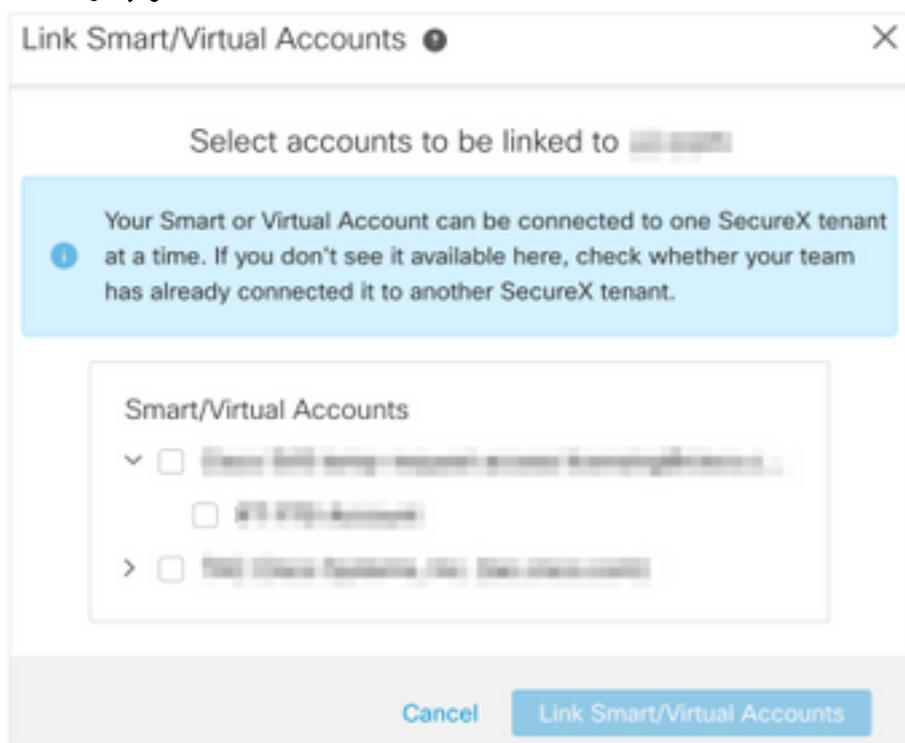
1. Confirm your cloud region
Currently selected region: `api-sse.cisco.com`
To change the cloud region, go to [System / Integration / Cloud Services](#).
2. Create a SecureX API client 
Copy and paste the URL below into the "Redirect URL" field:
[Copy to Clipboard](#)
`https://10.62.184.21/securex/oauth/callback`
Then click on "Add another Redirect URL" and copy and paste the URL below:
[Copied](#)
`https://10.62.184.21/securex/testcallback`
3. Enter the Client ID and password
Client ID
Client Password
 Show Password

5YVPsGdzrkX8q8q0yYI-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。