# FDMによるAMPファイルポリシーの設定およびテスト

## 内容



## はじめに

このドキュメントでは、Firepower Device Manager(FDM)を使用して高度なマルウェア防御(AMP)ファイルポリシーを設定およびテストする方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Firepower Device Manager（FDM）
- Firepower Threat Defense（FTD）

### 使用するコンポーネント

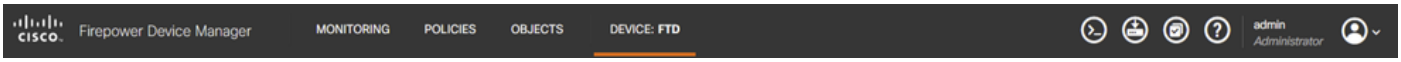
- FDMで管理されるCisco仮想FTDバージョン7.0
- 評価ライセンス(評価ライセンスはデモ目的で使用されます。有効なライセンスを取得して使用することを推奨します)

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、クリアな（デフォルト）設定で作業を開始しています。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。

## 手順

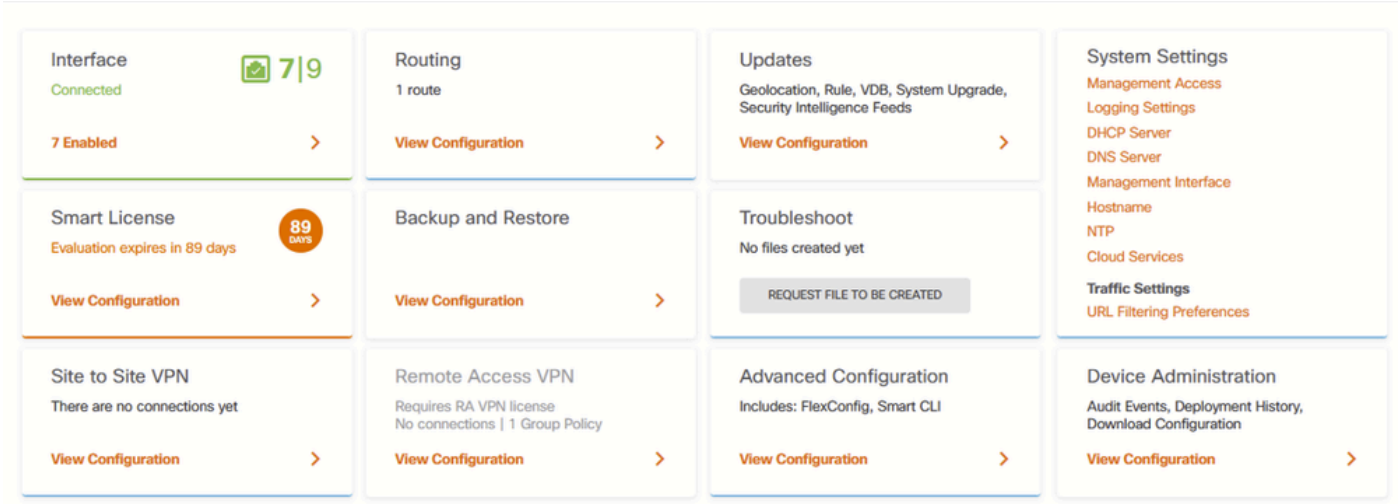
## ライセンス

1. マルウェアライセンスを有効にするには、FDM GUIのDEVICEページに移動します。



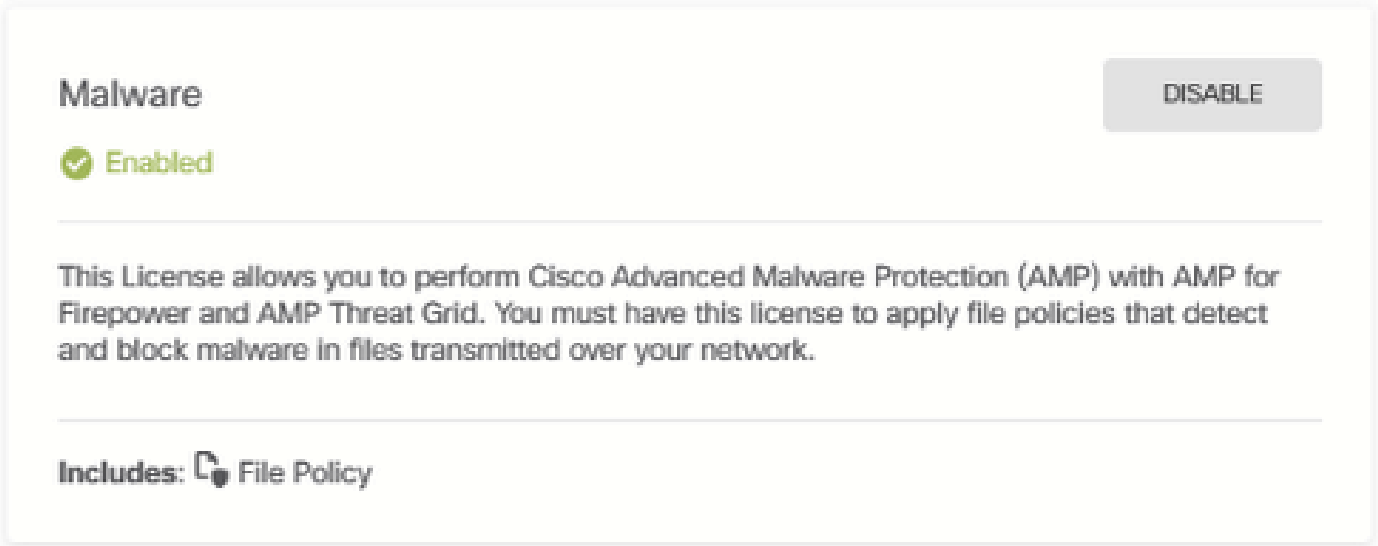

FDMデバイス・タブ

2. Smart Licenseというラベルの付いたボックスを見つけ、View Configurationをクリックします。




FDMデバイス・ページ

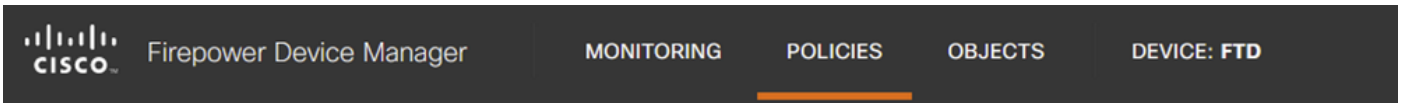
3. Malwareというラベルの付いたライセンスを有効にします。




マルウェアライセンス

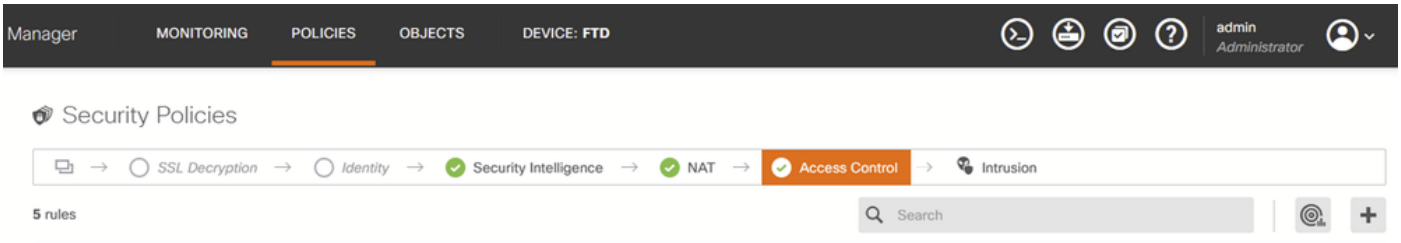
## コンフィギュレーション

1. FDMで「ポリシー」ページにナビゲートします。



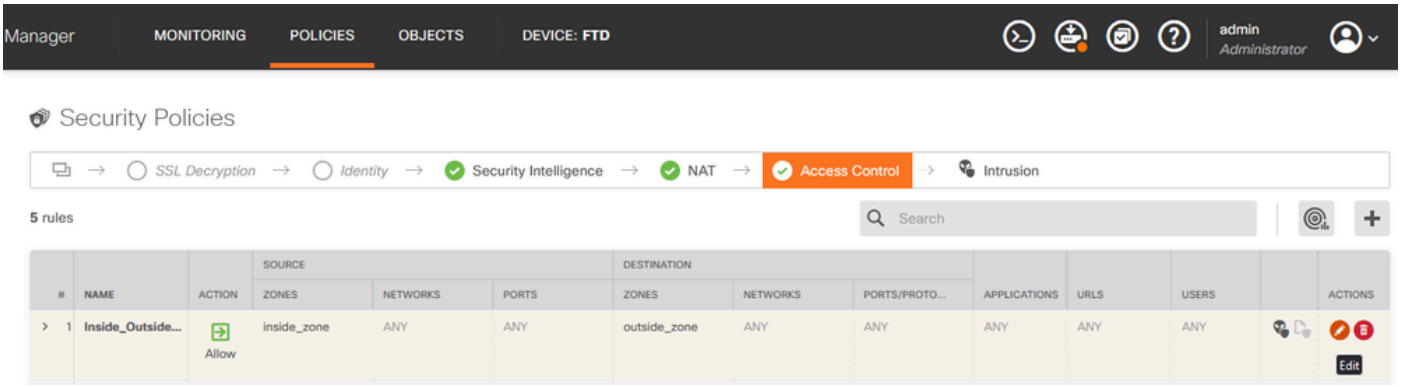

FDMポリシー・タブ

2. セキュリティポリシーで、アクセスコントロールセクションに移動します。



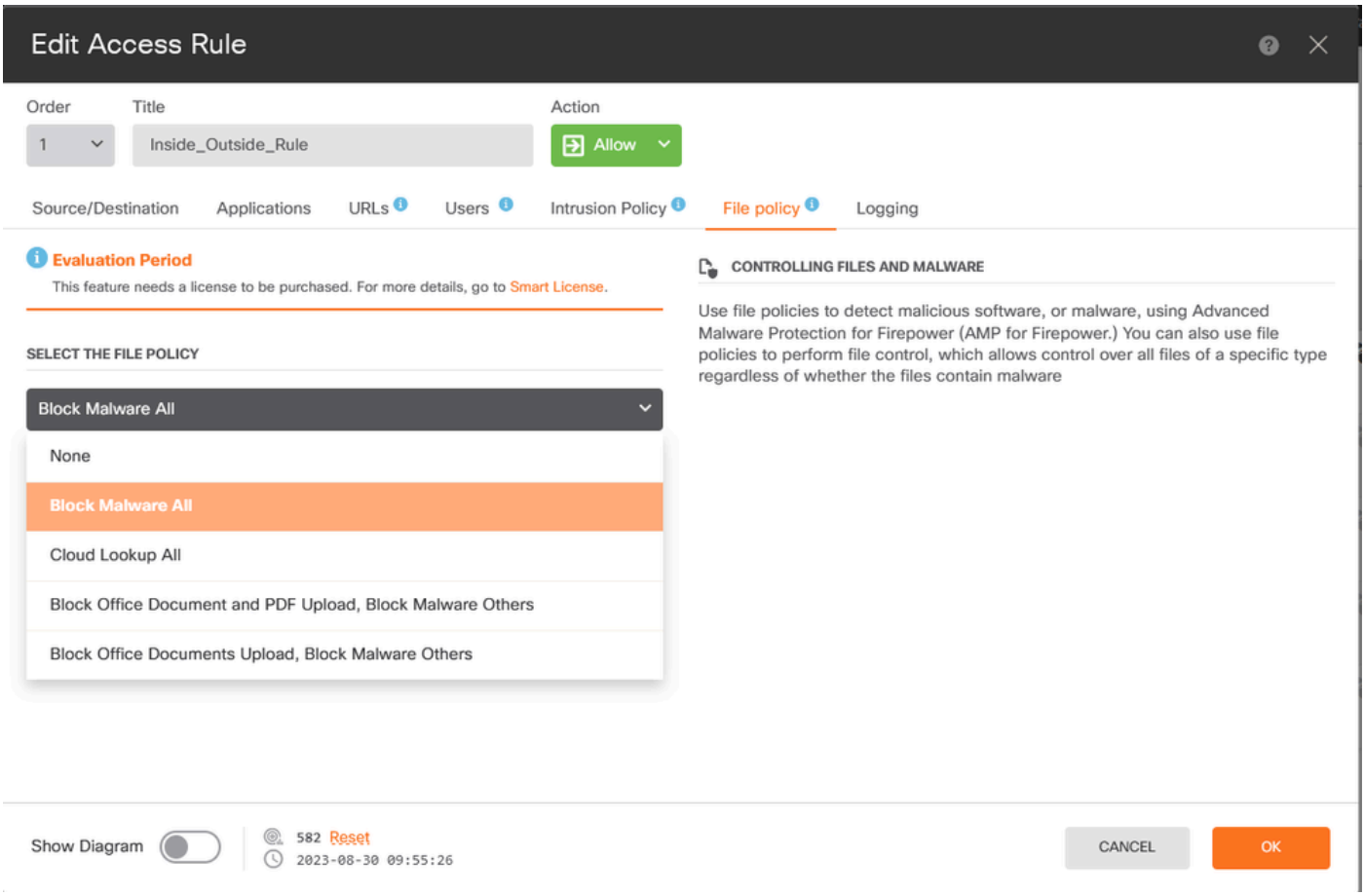

FDMの「アクセス制御」タブ

3. ファイルポリシーを設定するアクセスルールを検索または作成します。Access Ruleエディタをクリックします。アクセスルールの作成方法については、このリンクを参照してください。




FDMアクセス制御規則

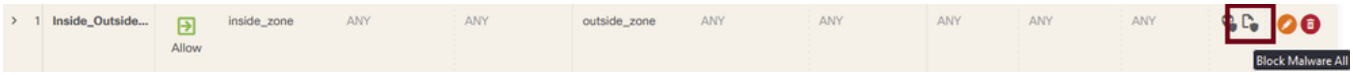
4. Access RuleにあるFile Policyセクションをクリックして、ドロップダウンから必要なFile Policyオプションを選択します。OKをクリックして、ルールの変更を保存します。




FDMの「アクセス制御規則ファイル・ポリシー」タブ

5. ファイルポリシーアイコンが有効になっているかどうかをチェックして、ファイルポリシーがアクセスルールに適用されていることを確認します。

ファイル



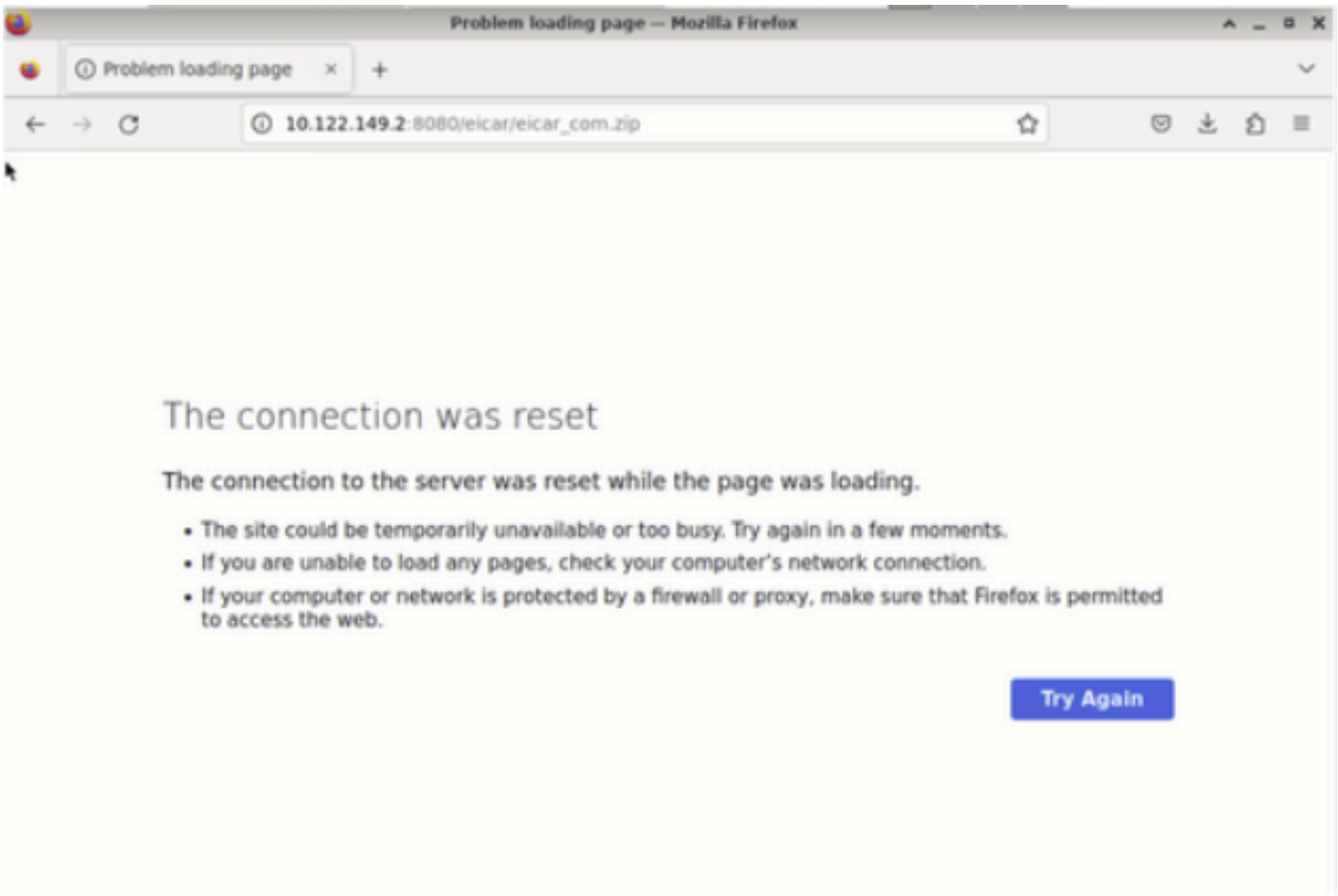

ファイルポリシーアイコンが有効

6.変更内容を保存して管理対象デバイスに展開します。

## テスト

マルウェア防御のために設定されたファイルポリシーが機能していることを確認するには、次のテストシナリオを使用して、エンドホストのWebブラウザからマルウェアテストファイルをダウンロードします。

次のスクリーンショットに示されているように、Webブラウザからマルウェアテストファイルをダウンロードしようとしても失敗します。




ブラウザのダウンロードテスト

FTD CLIのシステムサポートトレースに、ファイルのダウンロードがファイルプロセスによってブロックされたことが示されます。FTD CLIを使用してシステムサポートトレースを実行する方法については、このリンクを参照してください。

```
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File signature verdict Reject and flags 0x00005A00 for 2546d
cffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad of instance 0
192.168.0.10-40016 > 10.122.149.2-8080 6 File Process: drop /eicar/eicar_com.zip
192.168.0.10-40016 > 10.122.149.2-8080 6 IPS Event: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File malware event for 2546dcffc5ad854d4ddc64fbf056871cd5a00
f2471cb7a5bfd4ac23b6e9eedad named eicar_com.zip with disposition Malware and action Block Malware
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 Archive childs been processed No
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort detect_drop: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 deleting firewall session
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST
192.168.0.10-40016 > 10.122.149.2-8080 6 ===> Blocked by File Process
Verdict reason is sent to DAQ
```

システムサポートトレーステスト

これにより、ファイルポリシー設定がマルウェアのブロックに成功したことが確認されます。

# トラブルシューティング

上記の設定を使用したときにマルウェアが正常にブロックされない場合は、次のトラブルシューティングの提案を参照してください。

1. マルウェアライセンスが期限切れでないことを確認します。

2. アクセスコントロールルールが正しいトラフィックを対象としていることを確認します。

3. 選択したファイルポリシーオプションがターゲットトラフィックに対して正しいこと、およびマルウェア防御を希望していることを確認します。

それでも問題を解決できない場合は、Cisco TACにサポートを依頼してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。