# Talos接続ステータスのトラブルシューティング

## 内容



## はじめに

このドキュメントでは、Secure Firewall FMCおよびFDMでTALOSの接続の問題をトラブルシューティング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。

- Cisco Secure Firewall Management Center(FMC)
- Cisco Secure Firewall Device Manager(FDM)

- Cisco Secure Firewall Threat Defense(FTD)

### 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。

FMCバージョン7.6.0または7.7.0
FDMバージョン7.6.0または7.7.0
FTDバージョン7.6.0または7.7.0

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たものです。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。

## バックグラウンド情報

Cisco Secure Firewall Management Center(FMC)は、クライアント側の証明書を使用して、Cisco Talos脅威インテリジェンスサービスとのセキュアな接続を確立します。この認証は、URLレピュテーションデータベース(URLDB)、Lightweight Security Package(LSP)、およびその他のエンリッチメントデータを含む重要なアップデートをFMCが正常にダウンロードするために不可欠です。

通常の動作状況では、この証明書はソフトウェアのインストール時に事前にプロビジョニングされ、有効期限が近づくと自動的に更新されるように設計されています。ただし、Cisco Secure Firewall FMCソフトウェアの特定のバージョンに存在する既知の問題により、2025年3月30日以降は自動更新プロセスが正常に完了しません。これが発生すると、FMCがTalosで認証を行えなくなり、接続に障害が発生し、最新の脅威インテリジェンスを取得できなくなります。

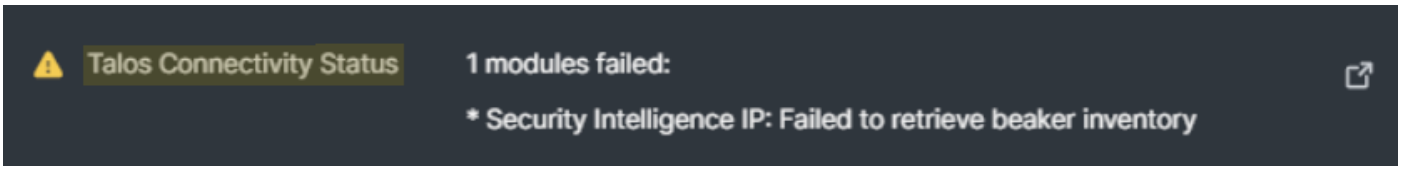
**証明書ステータスの確認**

### FMCのGUI

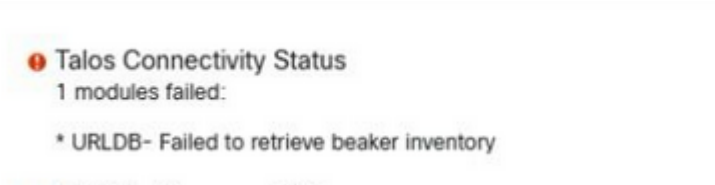
クライアント側の証明書の更新が失敗すると、Cisco FMCがヘルスアラートをトリガーし、Cisco Talosとの通信の中断を管理者に通知します。これらのアラートをモニタするには、System > Healthに移動して、Talos Connectivity Statusセクションを調べます。

システムが証明書の期限切れの問題の影響を受けている場合、通常は次のいずれかのエラーメッセージが表示されます。

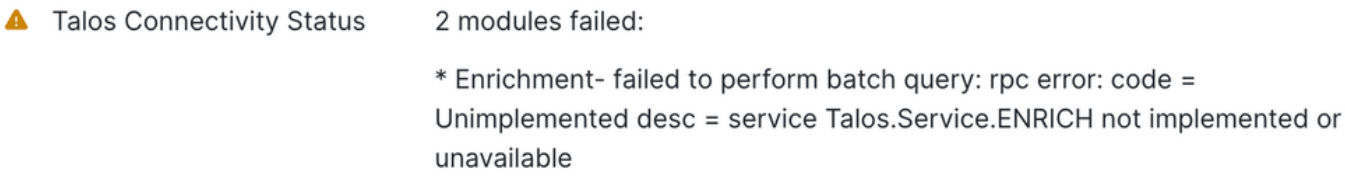
- 「LSP - Failed to retrieve beaker inventory」:




- 「URLDB - Failed to retrieve beaker inventory（URLDB – ビーカインベントリを取得できませんでした）」:




- “エンリッチメント – バッチクエリの実行に失敗しました":




## FMC の CLI

使用しているFMCアプライアンスがこの問題の影響を受けているかどうかを確認するには、expertモードにアクセスし、次のコマンドを実行してクライアント側証明書の現在の有効期限を確認します。

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'
```

**sudo openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text**

コマンド出力で、Validityセクションを探します。[次の日付以降]フィールドは、証明書の現在の有効期限を示します。この日付がすでに過ぎているか、近づいている場合、更新プロセスは失敗しており、証明書の更新を開始するには、手動によるサービスの再起動が必要です。

例：

<#root>

```
> expert
>sudo su
//type the 'FMC CLI admin password'
openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 46240369 (0x2c19271)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Cisco Systems Inc., OU = Security, CN = Keym
```

**Validity**

Not Before: Jan 30 22:32:39 2024 GMT

**Not After :**

```
 Mar 30 22:32:39 2025 GMT
        Subject: CN = SFW76EVAL-prod-01, C = US, ST = California, L = San Jose, O = Cisco, OU = Securit
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

# トラブルシュート

## 1. シナリオの特定

| [Software Version] | 関連するバグID | 主な原因 |
|---|---|---|
| 7.6.0 または 7.7.0 | Cisco Bug ID CSCwo63951 | 証明書の有効期限/接続の失敗 |
| 7.6.1+または7.7.10+ | Cisco Bug ID CSCwr23982 | 登録/ライセンス設定（エアギャップなど） |

## 2. バージョン7.6.0および7.7.0のトラブルシューティング

症状

前述のヘルスアラート以外にも、次の動作が見られます。

- FDMタスク・マネージャ・エラー：「Snort 3 cloud update failed: No response from the update server or connection timeout」

- ログエントリ： /ngfw/var/log/messages内の次のエラーが表示されます：トンネル(UUID)への接続に失敗しました。エラー：接続されていません。

- ステータス： UIのスタントアップデート： URLフィルタリングの設定画面に「Not updated yet」と表示されます。

一時的な回避策

サービスをすぐに復元するには、エキスパートモードで必要なプロセスを再起動します。

ステップ 1：CLIにアクセスし、エキスパートモードに入ります。

ステップ 2次のコマンドを実行します。

```
expert
sudo su
//type the 'FMC CLI admin password'
pmtool restartbyid talosAgent
pmtool restartbyid beaker3
```

---

注：この回避策は、5日間だけ有効な証明書をトリガーします。永続的な修正が適用されるまで、5日ごとにこのプロセスを繰り返す必要があります。

---

永続的な解決策

この問題を永続的に解決するには、次の条件が満たされていることを確認します。

ステップ 1：接続の確認：アプライアンスがhttps://api-sse.cisco.comへのアウトバウンドアクセスを持っていることを確認します。これを行うには、FMC CLIにアクセスし、expertモードに入り、次のコマンドを実行します。

ステップ 1.1：テストDNS解決：

<#root>

```
expert
sudo su
```

```
//type the 'FMC CLI admin password'
```

**nslookup api-sse.cisco.com**

ステップ 1.2：テストTCPポートアクセス：

<#root>

```
 expert
sudo su
//type the 'FMC CLI admin password'
```

**telnet api-sse.cisco.com 443**

---

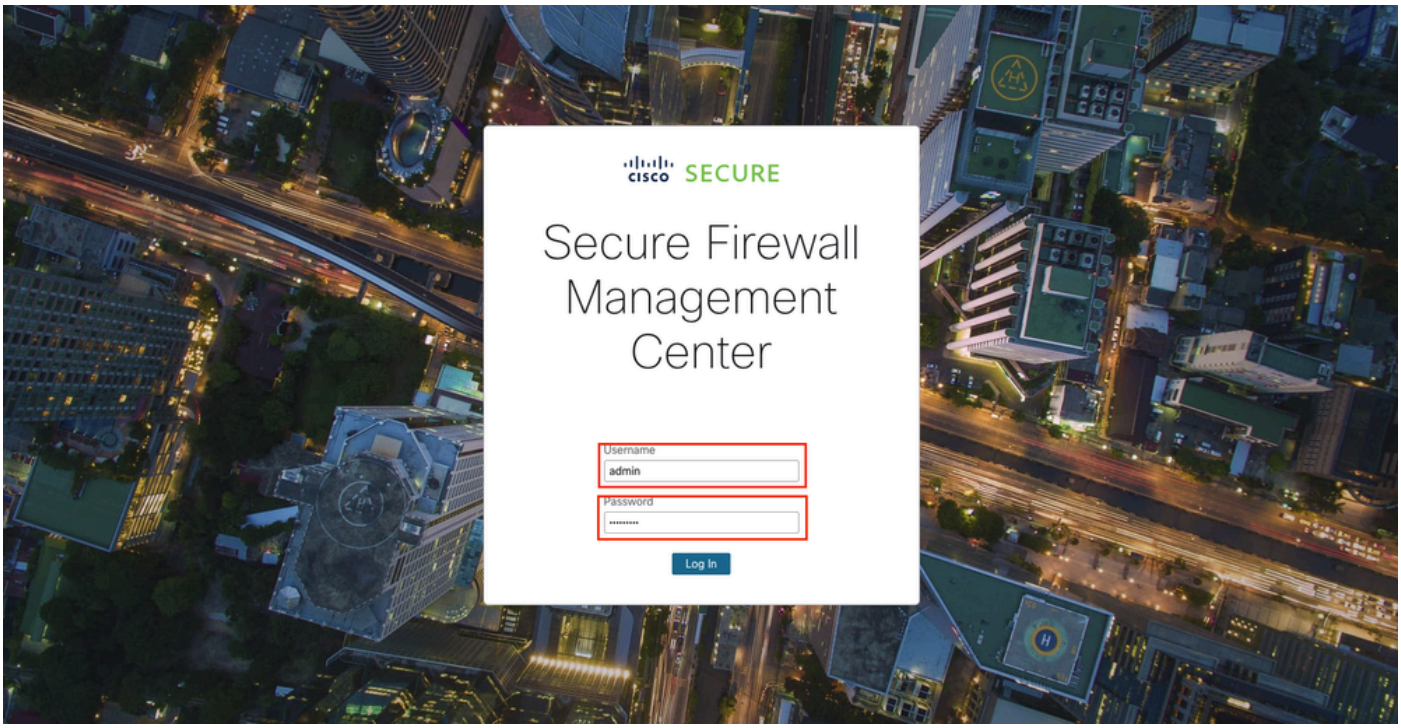
注:https://api-sse.cisco.comへの発信HTTPS(TCP 443)アクセスが、すべてのアップストリームファイアウォール、プロキシ、またはセキュリティデバイスを介して許可されていることを確認します。

---

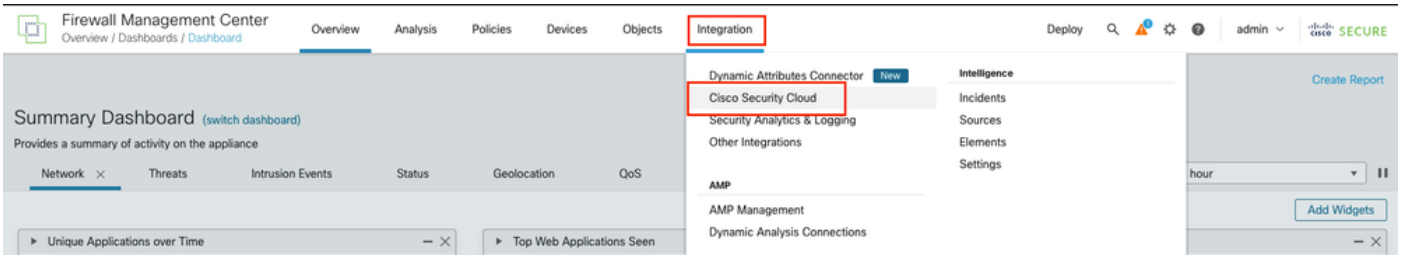
ステップ 2テレメトリを有効にする：SSEConnectorが新しい証明書を取得できるように、カスタマーサクセスネットワーク(CSN)テレメトリが有効になっていることを確認します。FMCでCSNを有効にするには、次の手順を実行します。

ステップ 2.1：Webブラウザを開いてFMC URL(https://<FMC_IP_or_Hostname>など)に移動し、FMC GUIにログインします。 ユーザ名とパスワードを入力して、

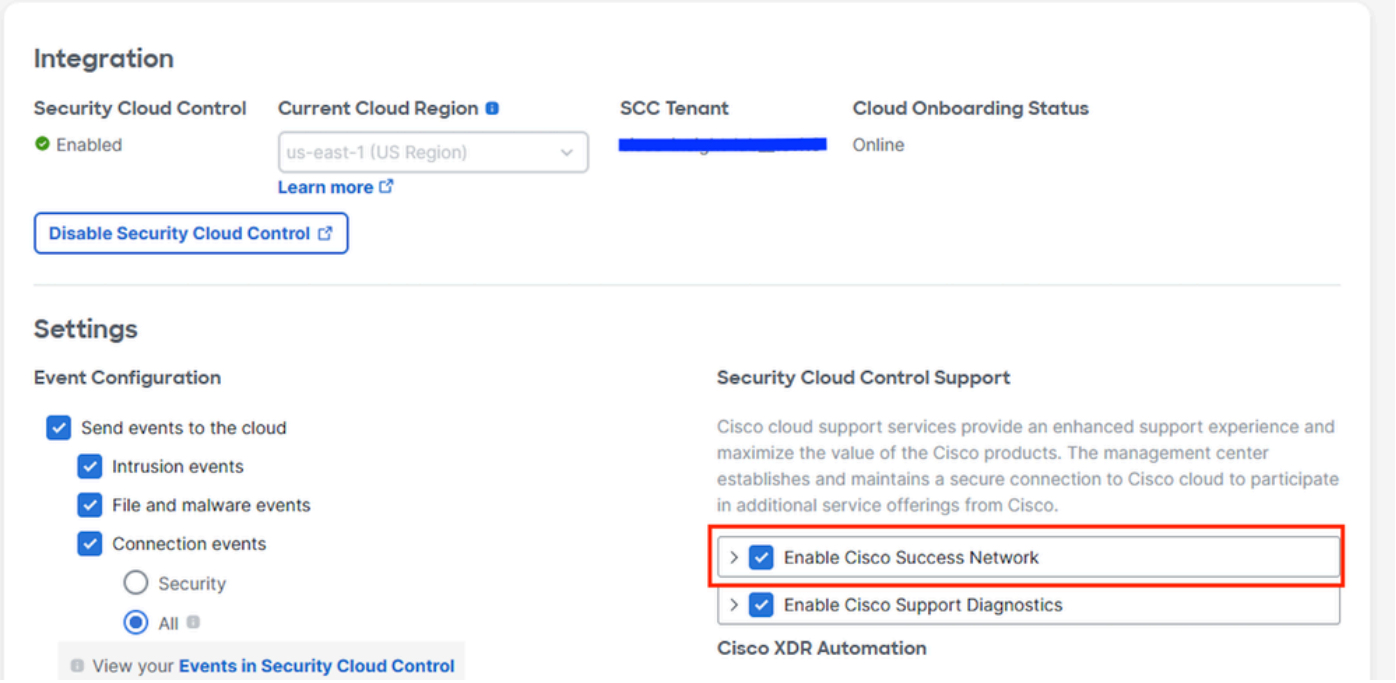
FMCのGUIインターフェイス




ステップ 2.2： Cisco Success Network Settingsに移動します。メインメニューから、Integration > Cisco Security Cloudの順に選択します。




ステップ 2.3： Cisco Success Networkというラベルが付いたオプションを見つけて有効にします。そのためには、Enable Cisco Success Networkのボックスをチェックして、テレメトリをアクティブにします。




ステップ 3更新プログラムのインストール： GeoDB 2025-04-03-094またはVDB 406 （ 以降 ）をインストールします。 これにより、新しい365日間証明書のインストールがトリガーされます。

---

注：高可用性(HA)。　HAペアでは、SSEConnectorプロセスはスタンバイユニットでは実行されません。スタンバイFMCをアップデートするには、ロールスイッチを実行してスタンバイをアクティブにし、必要なVDBまたはGeoDBのアップデートをインストールします。

---

## 3. バージョン7.6.1+および7.7.10+のトラブルシューティング

この問題は、通常、評価ライセンス、SSMオンプレミス、PLR、またはSLRを使用している環境など、標準のCisco Security Cloud(CSC)登録がない環境で発生します。

影響を受ける機能

- Lightweight Security Package(LSP)の自動/手動アップデート
- URLフィルタリングデータベースコンテンツの更新とクラウド検索。
- 接続イベントのターロスエンリッチメント。

推奨される対処法

1. 標準環境：FMCの登録は、Integration > Cisco Security Cloudから行います。登録すると、30分以内に新しい証明書のダウンロードが自動的にトリガーされます。

2.　手動アップデート：自動アップデートが失敗した場合、software.cisco.comから手動で最新のLSPをダウンロードし、FMCに直接インストールします。

3.　エアギャップ環境：ネットワークにインターネットアクセスがない場合、Talos　Connectivity Statusヘルスモジュールは無関係になります。このシナリオでは、適用された正常性ポリシー内で、この特定のモジュールを無効にします。

## 関連情報

- 詳細については、Cisco Technical Assistance Center(TAC)にお問い合わせください。 有効なサポート契約が必要です。シスコワールドワイドサポートの連絡先です。

- Cisco Support & Downloads:Cisco Technical Support & Downloads

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。