

# FTD接続用FMC Sftunnel CA証明書の更新

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[問題](#)

[有効期限の後に何が起こりますか？](#)

[証明書の有効期限が切れているかどうか、または有効期限が切れているかどうかを簡単に確認する方法](#)

[証明書の有効期限が近づいていることが将来どのように通知されますか。](#)

[解決策1：証明書の有効期限がまだ切れていない（理想的なシナリオ）](#)

[推奨されるアプローチ](#)

[解決策2 – 証明書はすでに期限切れです](#)

[FTDはsftunnel経由で接続されたままです。](#)

[FTDがsftunnel経由で接続されなくなりました。](#)

[推奨されるアプローチ](#)

[手動アプローチ](#)

---

## はじめに

このドキュメントでは、Firepower Threat Defense(FTD)の接続に関連したFirepower Management Center(FMC)sftunnel(CTL)認証局(CA)証明書の更新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 Threat Defense ( 脅威対策 )
- Firepower Management Center
- 公開キー インフラストラクチャ ( PKI )

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

## 背景説明

FMCとFTDは、sftunnel ( Sourcefireトンネル ) を介して相互に通信します。この通信では、証明書を使用して、TLSセッションで通信を安全にします。sftunnelの詳細と、確立方法については、[このリンク](#)を参照してください。

パケットキャプチャから、FMC ( この例では10.48.79.232 ) とFTD(10.48.79.23)が互いに証明書を交換していることがわかります。これは、正しいデバイスと通信し、傍受や中間者攻撃 (MITM)がないことを検証するためです。これらの証明書を使用して通信が暗号化され、その証明書に関連付けられた秘密キーを持つユーザだけが再度復号化できます。

The screenshot displays a network traffic capture analysis tool interface. The top section shows a list of captured packets with columns for No., Time, Source, Src Port, Destination, Dst Port, VLAN, Protocol, Length, Checksum, and Info. Packet 97 is selected, showing a TLSv2 record. The bottom section shows the detailed protocol tree for this packet, including the Certificate and Certificate Request layers. The Certificate layer is expanded, showing its structure, including the issuer and subject fields. A red arrow points from the 'Certificate' entry in the packet list to the corresponding entry in the protocol tree.

証明書\_exchange\_server\_cert

The screenshot shows a network traffic capture tool displaying a list of packets. Packet 100 is highlighted, showing a TLSv2 record. The detailed view of this record shows a Certificate field with a truncated rdnSequence containing organizational names like 'Cisco Systems, Inc.' and 'Intrusion Management System'.

証明書\_交換\_クライアント\_証明書

証明書が、FMCシステムで設定されているものと同じ内部CA ( 発行者 ) 認証局(CA)によって署名されていることがわかります。この設定は、FMCの/etc/sf/sftunnel.confファイルで定義されています。このファイルには、次のものが含まれています。

```

proxysl {
  proxy_cert /etc/sf/keys/sftunnel-cert.pem; ---> Certificate provided by FMC to FTD
  proxy_key /etc/sf/keys/sftunnel-key.pem;
  proxy_cacert /etc/sf/ca_root/cacert.pem; ---> CA certificate (InternalCA)
  proxy_cr1 /etc/sf/ca_root/cr1.pem;
  proxy_cipher 1;
  proxy_tls_version TLSv1.2;
};

```

これは、sftunnelのすべての証明書 ( FTDとFMCの両方 ) の署名に使用されるCAと、すべてのFTDに送信するためにFMCによって使用される証明書を示します。この証明書は内部CAによって署名されています。

FTDがFMCに登録されると、FMCは、sftunnelでの以降の通信に使用されるFTDデバイスにプッシュするための証明書も作成します。この証明書は、同じ内部CA証明書でも署名されます。FMCでは、/var/sf/peers/<UUID-FTD-device>の下、場合によってはcerts\_pushedフォルダの下に、証明書 ( および秘密キー ) が見つかります。この名前はsftunnel-cert.pem(秘密キーの場合はsftunnel-key.pem)と呼ばれます。FTDでは、/var/sf/peers/<UUID-FMC-device>の下に、同じ命名規則を持つものを見つけることができます。

ただし、セキュリティ上の理由から、各証明書には有効期間も設定されています。内部CA証明書を検査すると、パケットキャプチャから示されているように、FMC内部CAの有効期間 ( 10年 ) も確認できます。

The screenshot shows a network traffic capture tool displaying a list of packets and a detailed view of a TLSv1.2 Record Layer: Handshake Protocol: Certificate. The certificate details include issuer information, validity dates (2023-03-14 02:09:59 UTC), and subject information.

FMC内部CAの有効性(⌵)

## 問題

FMC内部CA証明書の有効期間は10年です。有効期限が切れると、リモートシステムはこの証明書（および証明書によって署名された証明書）を信頼しなくなり、FTDとFMCデバイス間のsftunnel通信の問題が発生します。これは、接続イベント、マルウェア検索、IDベースのルール、ポリシーの導入など、いくつかの重要な機能が動作していないことを意味します。

sftunnelが接続されていない場合、FMCのUIのDevices > Device Managementタブにデバイスがdisabledと表示されます。この期限切れに関連する問題は、Cisco Bug ID [CSCwd08098](#)で追跡されています。不具合の修正済みリリースを実行している場合でも、すべてのシステムが影響を受けることに注意してください。この修正の詳細については、「ソリューション」セクションを参照してください。

The screenshot shows the Firewall Management Center (FMC) UI. The 'Devices' tab is selected, and the 'Ungrouped' section shows two devices: 'BSNS-1120-3' (Snort 3) and 'EMEA-FPR3105-10' (Snort 3). Both devices are marked as 'Snort 3' and 'Disabled'.

無効なデバイス

FMCは、CAを自動的に更新して、証明書をFTDデバイスに再発行しません。また、証明書の有効期限を示すFMCヘルスアラートもありません。Cisco Bug ID [CSCwd08448](#)は、将来的にFMC UIのヘルスアラートを提供するためにこの点に関して追跡されています。

## 有効期限の後に何が起こりますか？

最初は何も起こらず、sftunnel通信チャネルは以前と同様に動作し続けます。ただし、FMCとFTDデバイス間のsftunnel通信が切断され、接続を再確立しようとする、接続に失敗し、証明書有効期限切れを示すメッセージログファイルのログ行で確認できます。

/ngfw/var/log/messagesからのFTDデバイスからのログ行：

```
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Initiating IPv4 connection
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Wait to connect to 8305 (IP
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Connected to 10.10.200.31 f
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] -Error with certificate at
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] issuer = /title=Intern
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] subject = /title=Intern
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] err 10:certificate has e
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] SSL_renegotiate error: 1:
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] Connect:SSL handshake fail
Sep 20 04:10:47 FTD-hostname SF-IMS[50792]: [51982] sftunnel:sf_ssl [WARN] SSL Verification status: ce
```

/var/log/messagesからのFMCデバイスからのログ行：

```
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [INFO] VERIFY ssl_verify_callback_in
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [ERROR] SSL_renegotiate error: 1: er
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [WARN] establishConnectionUtil: SSL
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [INFO] establishConnectionUtil: Fail
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [ERROR] establishSSLConnection: Unab
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [ERROR] establishSSLConnection: ret_
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [ERROR] establishSSLConnection: ired
Sep 20 03:14:23 FMC-hostname SF-IMS[1504]: [4171] sftunnel:sf_ssl [ERROR] establishSSLConnection: Fail
```

sftunnelの通信は、さまざまな理由で切断される可能性があります。

- ネットワーク接続の喪失による通信損失（一時的な可能性のみ）
- FTDまたはFMCのリポート
  - 予期される問題：手動リポート、アップグレード、FMCまたはFTDでのsftunnelプロセスの手動再起動（pmtool restartbyid sftunnelなどによる）
  - 想定外のもの：トレースバック、停電

sftunnelの通信を切断する可能性は非常に多いため、証明書が期限切れであるにもかかわらず現在すべてのFTDデバイスが正しく接続されている場合でも、状況をできるだけ迅速に修正することを強くお勧めします。

証明書の有効期限が切れているかどうか、または有効期限が切れているかどうかを簡単に確認する方法

最も簡単な方法は、FMCのSSHセッションで次のコマンドを実行することです。

```
expert
sudo su
cd /etc/sf/ca_root
openssl x509 -dates -noout -in cacert.pem
```

証明書の有効期間の要素が表示されます。ここで関連する主な部分は「notAfter」であり、この証明書が2034年10月5日まで有効であることを示します。

```
root@firepower:/Volume/home/admin# openssl x509 -dates -in /etc/sf/ca_root/cacert.pem
notBefore=Oct  7 12:16:56 2024 GMT
notAfter=Oct  5 12:16:56 2034 GMT
```

次の日付以降

証明書がまだ有効な日数を即時に示す単一のコマンドを実行する場合は、次のコマンドを使用できます。

```
CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -enddate -noout -in "$CERT_PATH" | cut -d= -f2)
```

証明書が複数年有効なセットアップの例を示します。

```
root@fmcv72-stejanss:/Volume/home/admin# CERT_PATH="/etc/sf/ca_root/cacert.pem"; EXPIRY_DATE=$(openssl x509 -enddate -noout -in "$CERT_PATH" | cut -d= -f2); EXPIRY_DATE_SECONDS=$(date -d "$EXPIRY_DATE" +%s); CURRENT_DATE_SECONDS=$(date +%s); THIRTY_DAYS_SECONDS=$((30*24*60*60)); EXPIRY_THRESHOLD=$((CURRENT_DATE_SECONDS + THIRTY_DAYS_SECONDS)); DAYS_LEFT=$(( (EXPIRY_DATE_SECONDS - CURRENT_DATE_SECONDS) / (24*60*60) )); if [ "$EXPIRY_DATE_SECONDS" -le "$CURRENT_DATE_SECONDS" ]; then DAYS_EXPIRED=$(( (CURRENT_DATE_SECONDS - EXPIRY_DATE_SECONDS) / (24*60*60) )); echo -e "\n\nThe certificate has expired $DAYS_EXPIRED days ago.\n\nIn case the sftunnel communication with the FTD is not yet lost, you need to take action immediately in renewing the certificate.\n\n"; elif [ "$EXPIRY_DATE_SECONDS" -le "$EXPIRY_THRESHOLD" ]; then echo -e "\n\nThe certificate will expire within the next 30 days!\n\nIt is ONLY valid for $DAYS_LEFT more days.\n\nIt is recommended to take action in renewing the certificate as quickly as possible.\n\n"; else echo -e "\n\nThe certificate is valid for more than 30 days.\n\nIt is valid for $DAYS_LEFT more days.\n\nThere is no immediate need to perform action but this depends on how far the expiry date is in the future.\n\n"; fi

The certificate is valid for more than 30 days.
It is valid for 3649 more days.
There is no immediate need to perform action but this depends on how far the expiry date is in the future.

root@fmcv72-stejanss:/Volume/home/admin#
```

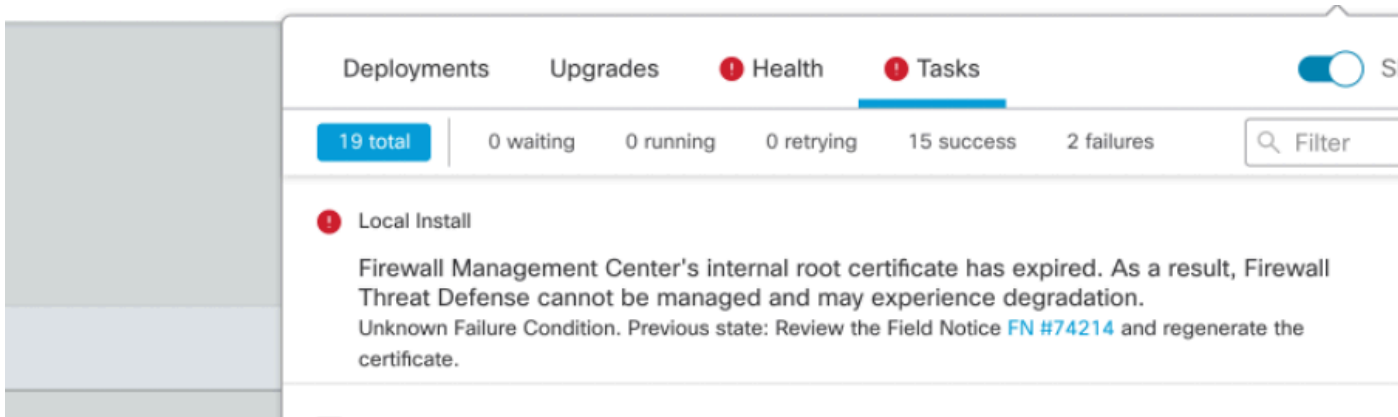
Certificate\_expiry\_validation\_command ( 証明書の有効期限の検証コマンド )

証明書の有効期限が近づいていることが将来どのように通知されますか。

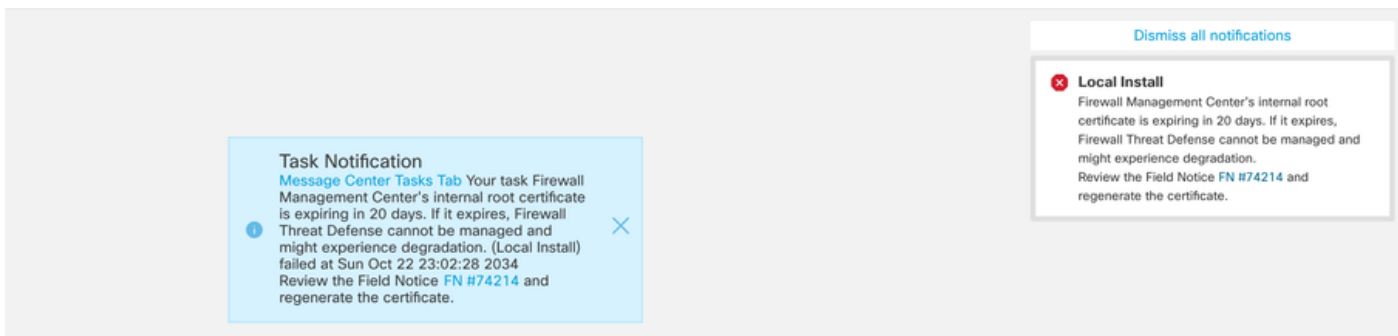
最近のVDBアップデート ( 399以降 ) では、証明書の有効期限が90日以内に切れると、自動的にアラートが通知されます。そのため、有効期限が近づいたときにアラートが通知されるので、手動で追跡する必要はありません。この結果、FMCのWebページに2つの形式で表示されます。ど

こちらの方法も[Field Noticeページ](#)を参照しています。

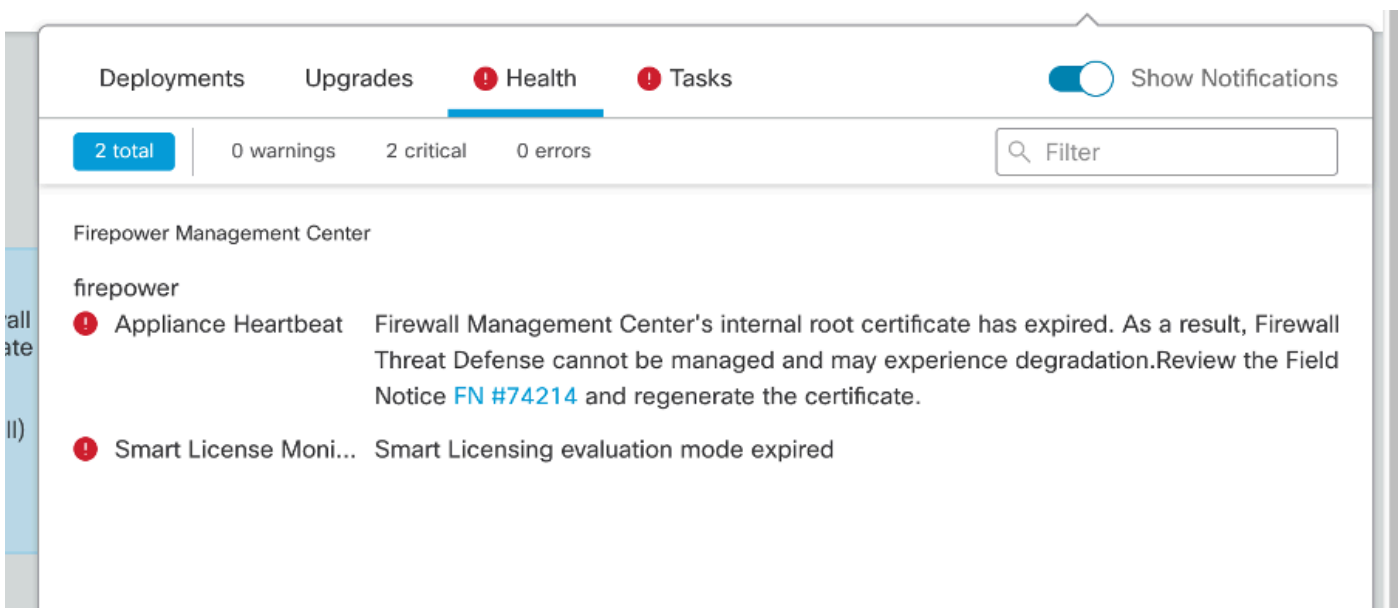
最初の方法は、Task Tabを使用する方法です。このメッセージは固定されているため、明示的に閉じていない限り、ユーザが使用できます。通知ポップアップも表示され、ユーザが明示的に閉じるまで使用できます。これは常にエラーとして表示されます。

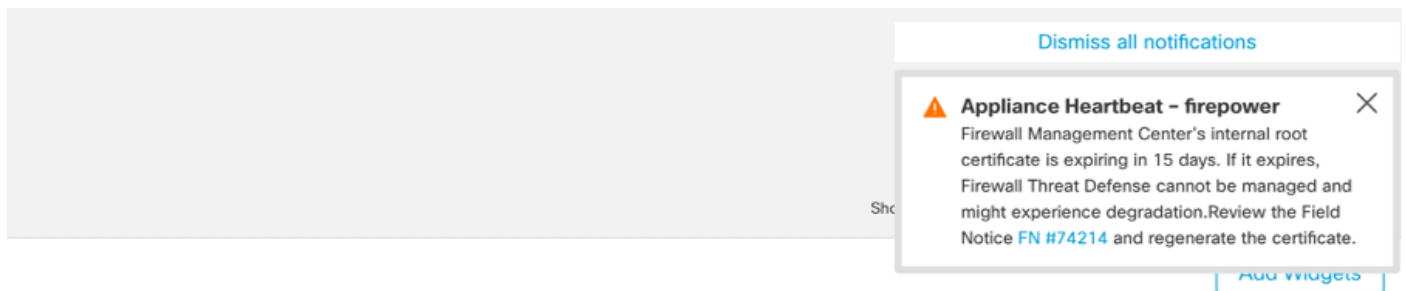


「タスク」タブの「期限切れ通知」

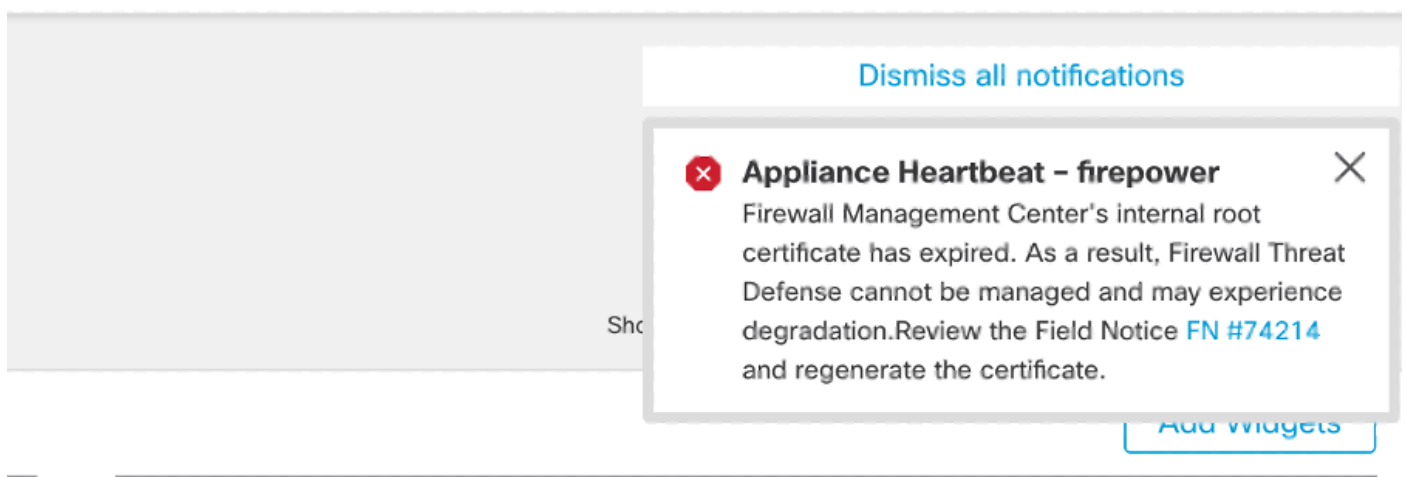


2番目の方法は、ヘルスアラートを使用する方法です。これは[正常性]タブに表示されますが、これはスティッキーではなく、既定では5分ごとに実行されるヘルスマニタの実行時に置換または削除されます。また、ユーザが明示的に閉じる必要がある通知ポップアップも表示されます。この場合、両方がエラー（期限切れ時）として表示され、警告（期限切れ時）として表示されます。





ヘルスアラートポップアップに関する警告通知



ヘルスアラートポップアップのエラー通知

## 解決策1：証明書の有効期限がまだ切れていない（理想的なシナリオ）

証明書の期限切れに応じて、まだ時間がある場合は、これが最善の状況です。FMCバージョンに依存する完全自動アプローチ（推奨）を採用するか、TACの介入を必要とする、より手動のアプローチを採用します。

### 推奨されるアプローチ

これは、通常の状況ではダウンタイムがなく、手動操作の量が最小限であると予想される状況です。

続行する前に、次に示す特定のバージョンの[ホットフィックス](#)をインストールする必要があります。このホットフィックスの利点は、これらのホットフィックスではFMCをリブートする必要がないため、証明書がすでに期限切れになっている場合にsftunnel通信が切断される可能性があることです。使用可能なホットフィックスは次のとおりです。

- [7.0.0 ~ 7.0.6](#)：ホットフィックスFK - 7.0.6.99-9
- 7.1.x：ソフトウェアメンテナンス終了による修正済みリリースなし
- [7.2.0 ~ 7.2.9](#)：ホットフィックスFZ - 7.2.9.99-4
- [7.3.x](#)：ホットフィックスAE - 7.3.1.99-4



- [7.4.0 ~ 7.4.2](#) : ホットフィックスAO - 7.4.2.99-5
- [7.6.0](#) : ホットフィックスB - 7.6.0.99-5

ホットフィックスをインストールすると、次のgenerate\_certs.plスクリプトがFMCに含まれるようになります。

1. 内部CAを再生成します
2. この新しい内部CAによって署名されたsftunnel証明書を再作成します
3. 新しいsftunnel証明書と秘密キーをそれぞれのFTDデバイスにプッシュします ( sftunnelが動作可能な場合 )。

したがって、可能であれば次のことを行うことを推奨します。

1. 上記の適切なホットフィックスをインストールします
2. FMCでバックアップを作成します。
3. (expertモードで)FMC上でsftunnel\_status.plスクリプトを使用して、現在のすべてのsftunnel接続を検証します。
4. generate\_certs.plを使用して、エキスパートモードからスクリプトを実行します。
5. 結果を検査して、手動操作が必要かどうかを検証します ( デバイスがFMCに接続されていない場合 ) [詳細は以下で説明]
6. FMCからsftunnel\_status.plを実行して、すべてのsftunnel接続が正常に動作していることを確認します

```

root@fmcv72-stejanss:/Volume/home/admin# generate_certs.pl
setting log file to /var/log/sf/sfca_generation.log

You are about to generate new certificates for FMC and devices.
After successful cert generation, device specific certs will be pushed automatically
If the connection between FMC and a device is down, user needs to copy the certificates onto the device manually
For more details on disconnected devices, use sftunnel_status.pl
Do you want to continue? [yes/no]:yes

Current ca_root expires in 3646 days - at Oct  9 10:12:50 2034 GMT
Do you want to continue? [yes/no]:yes

Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
Failed to push to BSNS-1120-1 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
Failed to push to EMEA-FPR3110-08 = /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem

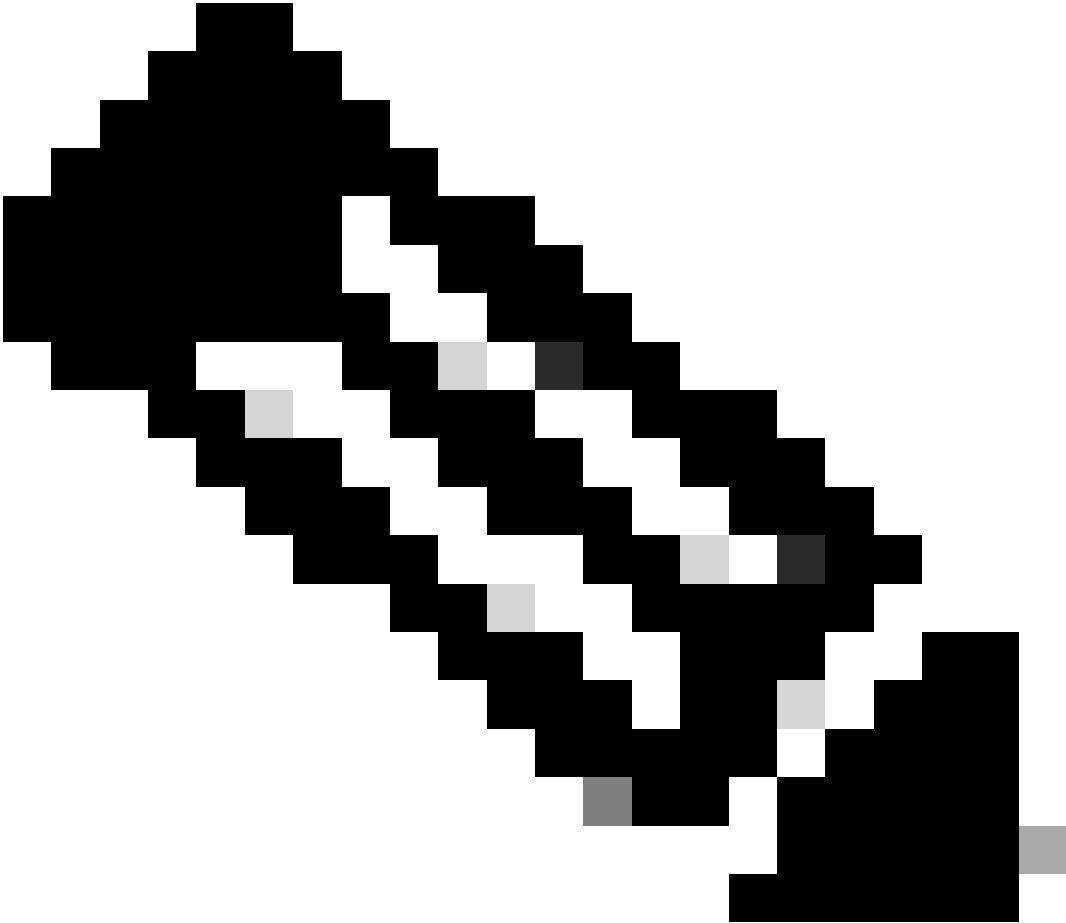
Some files were failed to be pushed to remote peers. For more details check /var/tmp/certs/1728915794/FAILED_PUSH

Scalars leaked: 1
root@fmcv72-stejanss:/Volume/home/admin# █

```

Generate\_certs.plスクリプト

---



注:FMCをハイアベイラビリティ(HA)で実行している場合は、最初にプライマリノードで操作を実行し、次にセカンダリノードで操作を実行する必要があります。これは、FMCノード間の通信にこれらの証明書が使用されるためです。両方のFMCノードのInternalCAが異なります。

---

この例では、/var/log/sf/sfca\_generation.logでログファイルが作成され、sftunnel\_status.plの使用が示され、InternalCAの有効期限が示され、そのCAでの障害が示されています。この例では、デバイスBSNS-1120-1およびEMEA-FPR3110-08デバイスに証明書をプッシュできませんでした。これらのデバイスのsftunnelがダウンしていたために、この処理が行われることが予想されます。

失敗した接続のsftunnelを修正するには、次の手順を実行します。

1. FMC CLIで、`cat /var/tmp/certs/1728303362/FAILED_PUSH` ( 数値はUNIX時間を表すので、システム内の前のコマンドの出力を確認してください ) を使用して、次の形式のFAILED\_PUSHファイルを開きます。FTD\_UUID FTD\_NAME FTD\_IP

## SOURCE\_PATH\_ON\_FMC DESTINATION\_PATH\_ON\_FTD

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/tmp/certs/1728915794/FAILED_PUSH
c8d5d5c6-87c9-11ef-a993-b9831565bc4e BSNS-1120-1 10.48.67.54 /etc/sf/ca_root/cacert.pem /var/sf/peers/cdb123c8-4
347-11ef-aca1-f3aa241412a1/cacert.pem
c8d5d5c6-87c9-11ef-a993-b9831565bc4e BSNS-1120-1 10.48.67.54 /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/c
erts_pushed//sftunnel-key.pem /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
c8d5d5c6-87c9-11ef-a993-b9831565bc4e BSNS-1120-1 10.48.67.54 /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/c
erts_pushed//sftunnel-cert.pem /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-cert.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77 EMEA-FPR3110-08 10.48.189.37 /etc/sf/ca_root/cacert.pem /var/sf/peers/cdb12
3c8-4347-11ef-aca1-f3aa241412a1/cacert.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77 EMEA-FPR3110-08 10.48.189.37 /var/sf/peers/6bf1143a-8a2e-11ef-92d8-fd927e807
d77/certs_pushed//sftunnel-key.pem /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/sftunnel-key.pem
6bf1143a-8a2e-11ef-92d8-fd927e807d77 EMEA-FPR3110-08 10.48.189.37 /var/sf/peers/6bf1143a-8a2e-11ef-92d8-fd927e807
root@fmcv72-stejanss:/Volume/home/admin#
```

失敗\_プッシュ

- これらの新しい証明書(cacert.pem / sftunnel-key.pem / sftunnel-cert.pem)をFMCからFTDデバイスに転送します。


===自動アプローチ===

ホットフィックスのインストールでは、copy\_sftunnel\_certs.pyおよびcopy\_sftunnel\_certs\_jumpserver.pyスクリプトも提供されます。これらのスクリプトは、証明書の再生中にsftunnelがアップ状態ではなかったシステムへの各種証明書の転送を自動化します。これは、証明書がすでに期限切れになったためにsftunnel接続が切断されたシステムでも使用できます。

copy\_sftunnel\_certs.py スクリプトは、FMC自体がさまざまなFTDシステムにSSHアクセスできる場合に使用できます。アクセスできない場合は、FMCから、FMCとFTDの両方のデバイスにSSHアクセスできるジャンプサーバにスクリプト (/usr/local/sf/bin/copy\_sftunnel\_certs\_jumpserver.py)をダウンロードし、そこからPythonスクリプトを実行できます。それも不可能な場合は、次に示す手動アプローチを実行することを推奨します。次の例は、使用されているcopy\_sftunnel\_certs.pyスクリプトを示していますが、手順はcopy\_sftunnel\_certs\_jumpserver.pyスクリプトと同じです。

A. SSH接続の確立に使用されるデバイス情報(device\_name、IP address、admin\_username、admin\_password)を含むCSVファイルをFMC (またはジャンプサーバ)に作成します。

プライマリFMCのジャンプサーバのようにリモートサーバからこのコマンドを実行する場合は、プライマリFMCの詳細を最初のエントリとして追加し、その後すべての管理対象FTDとセカンダリFMCを追加してください。セカンダリFMCのジャンプサーバのようにリモートサーバからこのコマンドを実行する場合は、セカンダリFMCの詳細を、最初のエントリとして追加し、その後すべての管理対象FTDを追加してください。

- vi devices.csvを使用してファイルを作成します。 

viデバイス.csv





```
root@firepower:/Volume/home/admin#
root@firepower:/Volume/home/admin#
root@firepower:/Volume/home/admin# vi devices.csv
root@firepower:/Volume/home/admin#
root@firepower:/Volume/home/admin# copy_sftunnel_certs.py devices.csv

=====

2024-11-12 14:07:36 - Attempting connection to FMCpri
2024-11-12 14:07:40 - Connected to FMCpri
2024-11-12 14:07:41 - FMCpri is not an HA-peer. Certificates will not be copied
2024-11-12 14:07:41 - Closing connection with FMCpri

=====

2024-11-12 14:07:41 - Attempting connection to FTDv
2024-11-12 14:07:43 - Connected to FTDv
2024-11-12 14:07:44 - Copying certificates to peer
2024-11-12 14:07:44 - Successfully copied certificates to FTDv
2024-11-12 14:07:44 - Restarting sftunnel for FTDv
2024-11-12 14:07:44 - Closing connection with FTDv

=====

2024-11-12 14:07:44 - Attempting connection to BSNS-1120-1
2024-11-12 14:08:04 - Could not connect to BSNS-1120-1

=====

root@firepower:/Volume/home/admin# █
```

copy\_sftunnel\_certs.pyデバイス.csv

### ===手動によるアプローチ===

1. 前の出力 ( FAILED\_PUSHファイル ) からファイルの場所をコピーして、FMC CLIに影響を受ける各FTDの各ファイル(cacert.pem / sftunnel-key.pem ( セキュリティ目的で完全には表示されていません ) / sftunnel-cert.pem)を出力(cat)します。

```
root@fmcv72-stejanss:/Volume/home/admin# cat /etc/sf/ca_root/cacert.pem
-----BEGIN CERTIFICATE-----
MIIDhDCCAmwCAQAwDQYJKoZIhvcNAQELBQAwYcxEzARBgNVBAMwMk1udGVybMFS
Q0ExJDAiBgNVBAsMG0ludHJ1c2lubiBNYW5hZ2VtZW50IFN5c3R1bTEtMCsGA1UE
AwwkY2RiMTIzYzgtNDM0Ny0xMwVmlWFjYTEtZjNhYTI0MTQxMmExMRswGQYDVQK
DBJDaXNjbyBTeXN0ZW1zLk1uZmMwHhcNMjQxMDE0MTQyMzI4WhcNMzQxMDEyMTQy
MzI4WjCBhZETMBEGA1UEDAwKSW50ZXJ1eWwxDQTEkMCIGA1UECwwbSW50cnVzaW9u
IE1hbmFnZW11bnQGU3lzdGVtMS0wKwYDVQDDCRjZGIxMjNjOC00MzQ3LTEXZWYt
YWNhMS1mM2FhMjQxNDEyYTEXGzAZBgNVBAoMEkNpc2NvIFN5c3R1bXMsIEluYzCC
ASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANhWuapG1tBJXMmUav8kVukF
xiV917W4d7/CYBb4pd1KiM0iJAep3wqxdpDUQ4KBDWnC5+p8dg+XK7Asp0W36CD
mdpRwRfqM7J51tXEUyCJEmiRYFEhE0eccsUWXG5LcLI8CHGjHMx6VlQl+aRlAPCF
7UYpMgFPh3Wp+T9tgx1HqbE28JktD1Nu/iism5lvxtZRqdEXnL6Jn3rfoKbF0M77
xUtMeC0504buhfzSl+Am5J0bFuXMcPYq1N+t137r1/1etwHzmjVke7g/rfNv0y0
N+4m8i5QRN0BoghtZ0+Y/PudToSX0VmKh5Sq/i1MvOYBZEIM3Dx+Gb/DQYBWLUC
AwEAATANBgkqhkiG9w0BAQsFAAOCQAQEAy2EVhEoylDdlWSu2ewdehtBtI6Q5x7e
UD187bbowmTJsd100LVGgYoU5qUFDh3NAqSxrDHEu/NsLUbrRiA30RI8WEA1o/S6
J3Q1F3hJJF0qSrIx/ST72jgL2o87ixhRIzreB/+26rHo5nns2r2tFss61KBltWN
nRZnSIYAwYhqGCjH9quiZpFDJ3N83oREGX+xfLYqFim5h3rFwk0J2q6YtaBJAuwg
0blDXGnrnWuIIV/xb0cwKbrALmtanhgGXyqT/pMYrjwLI1xVL16/PrMTV29WcQcA
IVBnyzhS4ER9sYIKB5V6MK4r2gJDG1t47E3RYnstyGx8hlzRvzHz2w==
-----END CERTIFICATE-----
root@fmcv72-stejanss:/Volume/home/admin#
```

cacert.pem ( 推奨 )

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/certs_pushed/sftunn
el-key.pem
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQCyc5A0xZ5N22qD
```

sftunnel-key.pem ( トンネルキー.pem )

```
root@fmcv72-stejanss:/Volume/home/admin# cat /var/sf/peers/c8d5d5c6-87c9-11ef-a993-b9831565bc4e/certs_pushed/sftunn
el-cert.pem
-----BEGIN CERTIFICATE-----
MIID3zCCAsegAwIBAgIBD0TANBgkqhkiG9w0BAQsFADCBhZETMBEGA1UEDAwKSW50
ZXJ1eWwxDQTEkMCIGA1UECwwbSW50cnVzaW9uIE1hbmFnZW11bnQGU3lzdGVtMS0w
KwYDVQDDCRjZGIxMjNjOC00MzQ3LTEXZWYtYWNhMS1mM2FhMjQxNDEyYTEXGzAZ
BgNVBAoMEkNpc2NvIFN5c3R1bXMsIEluYzAeFw0yNDEwMTQyMzI4WhcNMzQxMDEy
MTQyMzI4WjCBhZETMBEGA1UECwwbSW50cnVzaW9uIE1hbmFnZW11bnQGU3lzdGVt
cYwSWSjMS0wKwYDVQDDCRjZGIxMjNjOC00MzQ3LTEXZWYtYTk5My1iOTgzMTU2NWJj
NGUxETAPBgNVBwMCHmVubmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCQAQ8AMIIB
CgKCAQEAE3MuQNMWetdtqg2k52FKHY2dQJEHc0mdUc/Y0KniUUA45iAdLbv0X819y
lQFPFdlurv4mYxgDoBDcZozLLiRBeaXcZnowoqmatv0MtMyL0TINTL+5G/KiyCr
gsz2ub03avXW/cbC2WZQGat0kQ/4Fb+LC5dnX2KA5H7m1rs0WNWEKFSpn/Y2UYGb
Zdi3bZz5wy5YHGFGQ8KK04v4mksSu02b+AWfIgoe1EaSwv5K+Wa0ssj6keaCkYfA
TP1sEiYkytFdE0F2s8mXFSfLbK+8hI+jWqAN/Q0a3D9gHD8gErrPHgLD8m30TqP8s
kRF5JEI5UHhwlVt0FKbhWEW06906QIDAQABo0IwQDAJBgNVHRMEAjAAMBQGA1Ud
EQQNMAuCCWxvY2FsaG9zdDAAdBgNVHSUEFjAUBgggrBgEFBQcDAgYIKwYBBQUHAWew
DQYJKoZIhvcNAQELBQADggEBAHHAjwZHXG1nA+jAxGIaL6T/L2oYCDxuB3tcNKW
ZViILv110cUNYIvC/w7JbK1LUTLbit0aH01ff4Lcv0q6uk+SL7cAuAICXodP1EQo
ERz4E13a0MNNv5dt/a2fhIxzimhIq7P3zTMuKknVyblg0RqG7q8SxyEL5AT8Iy
beuhcg6+7LzCiw29/pTzCnycIrzBhBVK2ZcQ9vYtBXdCaZGK17lnYiEpk4Qi fne
9A2tQqecypKRRASd60uttEmVvpHCgMtGrC60Kb5h5SP00Ze1rGWD0V9eTj1Njis0
+J+WXE06VApI17aYKWXHHLGF7n+esy1GaZ3Djn44mMkn8I=
-----END CERTIFICATE-----
root@fmcv72-stejanss:/Volume/home/admin#
```

sftunnel-cert.pem ( 推奨 )

2. sudo suでルート権限を使用して、expertモードで各FTDのFTD CLIを開き、次の手順で証明書を書き換えます。

1. FAILED\_PUSHの出力の水色の強調表示で示されている場所を参照します(たとえば、cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1。ただし、これはFTDごとに異なります)。
2. 既存のファイルのバックアップを作成します。

```
cp cacert.pem cacert.pem.backup
cp sftunnel-cert.pem sftunnel-cert.pem.backup
cp sftunnel-key.pem sftunnel-key.pem.backup
```

```
> expert
admin@BSNS-1120-1:~$ sudo su
Password:
root@BSNS-1120-1:/home/admin# cd /var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1/
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp cacert.pem cacert.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp sftunnel-cert.pem sftunnel-cert.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# cp sftunnel-key.pem sftunnel-key.pem.backup
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal sftunnel*
-rw-r--r-- 1 root root 1.5K Oct 14 12:41 sftunnel-cert.pem
-rw-r--r-- 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-r--r-- 1 root root 1 Oct 14 14:21 sftunnel-heartbeat
-rw-r--r-- 1 root root 1.7K Oct 14 12:41 sftunnel-key.pem
-rw-r--r-- 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-r--r-- 1 root root 521 Oct 14 12:41 sftunnel.json
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal cacert.pem
-rw-r--r-- 1 root root 1.3K Oct 14 12:41 cacert.pem
```

現在の証明書のバックアップを作成する

3. ファイルを空にして、新しいコンテンツを書き込めるようにします。

```
> cacert.pem
> sftunnel-cert.pem
> sftunnel-key.pem
```

```
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > cacert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > sftunnel-cert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# > sftunnel-key.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal sftunnel*
-rw-r--r-- 1 root root 0 Oct 14 14:50 sftunnel-cert.pem
-rw-r--r-- 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-r--r-- 1 root root 1 Oct 14 14:21 sftunnel-heartbeat
-rw-r--r-- 1 root root 1.7K Oct 14 12:41 sftunnel-key.pem
-rw-r--r-- 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-r--r-- 1 root root 0 Oct 14 14:50 sftunnel-key.pem???
-rw-r--r-- 1 root root 521 Oct 14 12:41 sftunnel.json
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal cacert.pem
-rw-r--r-- 1 root root 0 Oct 14 14:50 cacert.pem
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1#
```

既存の証明書ファイルの内容が空です

4. vi cacert.pem / vi sftunnel-cert.pem / vi sftunnel-key.pem ( ファイルごとに個別のコマンド : スクリーンショットではcacert.pemについてのみこれが表示されますが、sftunnel-cert.pemとsftunnel-key.pemについては繰り返す必要があります ) を使用して、新しいコンテンツ ( FMCの出力から ) を各ファイルに個別に書





```

root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# ls -hal
total 68K
drwxr-xr-x 4 root root 4.0K Oct 14 15:01 .
drwxr-xr-x 3 root root 4.0K Oct 14 15:01 ..
-rw-r--r-- 1 root root 0 Oct 14 12:42 LIGHT_REGISTRATION
-rw-r--r-- 1 root root 0 Oct 14 12:42 LIGHT_UNREGISTRATION
-rw-r--r-- 1 root root 2.0K Oct 14 12:45 LL-caCert.pem
-rw-r--r-- 1 root root 2.2K Oct 14 12:45 LL-cert.pem
-rw-r--r-- 1 root root 3.2K Oct 14 12:45 LL-key.pem
-rw-r--r-- 1 root root 1.3K Oct 14 14:55 cacert.pem
-rw-r--r-- 1 root root 1.3K Oct 14 14:49 cacert.pem.backup
-rw-r--r-- 1 root root 2.3K Oct 14 12:41 ims.conf
-rw-r--r-- 1 root root 221 Oct 14 12:41 peer_flags.json
drwxr-xr-x 3 root root 19 Oct 14 12:42 proxy_config
-rw-r--r-- 1 root root 1.2K Oct 14 12:42 sfiproxy.conf.json
-rw-r--r-- 1 root root 1.4K Oct 14 14:59 sftunnel-cert.pem
-rw-r--r-- 1 root root 1.5K Oct 14 14:49 sftunnel-cert.pem.backup
-rw-r--r-- 1 root root 1 Oct 14 14:21 sftunnel-heartbeat
-rw-r--r-- 1 root root 1.7K Oct 14 15:01 sftunnel-key.pem
-rw-r--r-- 1 root root 1.7K Oct 14 14:49 sftunnel-key.pem.backup???
-rw-r--r-- 1 root root 0 Oct 14 14:50 sftunnel-key.pem???
-rw-r--r-- 1 root root 521 Oct 14 12:41 sftunnel.json
-rw-r--r-- 1 root root 5 Oct 14 12:48 sw_version
drwxr-xr-x 6 root root 90 Oct 14 12:42 sync2
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1#

```

権利の所有者とアクセス許可で更新されたすべての証明書ファイル

3. sftunnelが動作していなかった各FTDでsftunnelを再起動し、証明書の変更をコマンドを使用して有効にします `pmtool restartbyid sftunnel`

```

root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1# pmtool restartbyid sftunnel
root@BSNS-1120-1:/var/sf/peers/cdb123c8-4347-11ef-aca1-f3aa241412a1#

```

`pmtool restartbyid sftunnel`

3. `sftunnel_status.pl`の出力を使用して、すべてのFTDが正しく接続されていることを確認します

## 解決策2 – 証明書はすでに期限切れです

この状況では、2つの異なるシナリオがあります。sftunnel接続のすべてが引き続き動作しているか、または部分的に動作していません。

FTDはsftunnel経由で接続されたままです。

「[証明書はまだ期限切れになっていない \(理想的なシナリオ\) – 推奨されるアプローチ](#)」セクションで示したのと同じ手順を適用できます。

ただし、この状況ではFMC（または任意のFTD）のアップグレードやリポートは行わないでください。すべてのsftunnel接続が切断されるため、各FTDですべての証明書の更新を手動で実行する必要があります。唯一の例外は、リストされているホットフィックスリリースです。これは、FMCをリポートする必要がないためです。

トンネルは接続されたままになり、証明書は各FTDで置き換えられます。一部の証明書の入力に失敗した場合は、失敗した証明書を使用するように求められます。そのため、前のセクションで前述したように、[手動によるアプローチ](#)を使用する必要があります。

FTDがsftunnel経由で接続されなくなりました。

### 推奨されるアプローチ

「[証明書はまだ期限切れになっていない（理想的なシナリオ） - 推奨されるアプローチ](#)」セクションで示したのと同じ手順を適用できます。このシナリオでは、新しい証明書がFMCで生成されますが、トンネルがすでにダウンしているため、デバイスにコピーできません。このプロセスは、[copy\\_sftunnel\\_certs.py / copy\\_sftunnel\\_certs\\_jumpserver.py](#)スクリプトで自動化できます

すべてのFTDデバイスがFMCから切断されている場合は、sftunnel接続に影響しないため、この状況でFMCをアップグレードできます。sftunnelを介して接続されているデバイスがまだある場合は、FMCのアップグレードによってsftunnel接続がすべて閉じられ、証明書の期限切れが原因で接続が再開されないことに注意してください。ここでのアップグレードの利点は、各FTDに転送する必要がある証明書ファイルに関する優れたガイダンスを提供することです。

### 手動アプローチ

この場合、新しい証明書を生成するFMCからgenerate\_certs.plスクリプトを実行できますが、これらの証明書をそれぞれのFTDデバイス([手動](#))にプッシュする必要があります。デバイスの量によっては、これは可能であるか、面倒な作業になる可能性があります。ただし、[copy\\_sftunnel\\_certs.py / copy\\_sftunnel\\_certs\\_jumpserver.py](#)スクリプトを使用すると、高度に自動化されます。

## 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。