AMP虛擬私有雲和Threat Grid裝置的整合

目錄

本文檔介紹完成高級惡意軟體防護(AMP)虛擬私有雲與Threat Grid裝置整合的過程。本文檔還提供了與整合過程相關的問題的故障排除步驟。

作者：Armando Garcia，思科TAC工程師。

思科建議您瞭解以下主題：

- 運行和運行AMP虛擬私有雲
- 運行和操作Threat Grid裝置

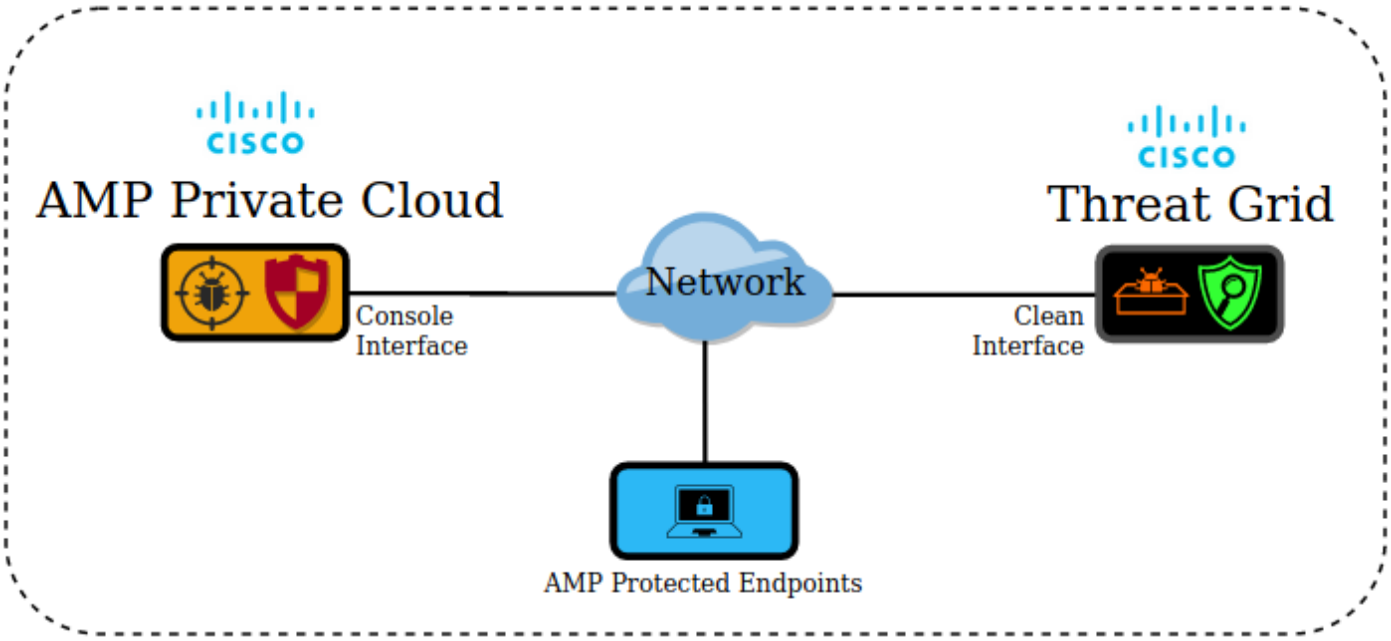
本文中的資訊係根據以下軟體和硬體版本：

- AMP私有雲3.2.0
- Threat Grid裝置2.12.0.1

附註：本文檔適用於裝置或虛擬版本中的Threat Grid裝置和AMP私有雲裝置。

背景資訊

整合架構



有關整合的基本資訊

- Threat Grid裝置會分析AMP私有雲裝置提交的樣本。
- 示例可以手動或自動提交到Threat Grid裝置。
- AMP私有雲裝置預設未啟用自動分析。
- Threat Grid裝置向AMP私有雲裝置提供來自樣本分析的報告和分數。
- Threat Grid裝置將分數大於或等於95的任何樣本通知（插入）AMP私有雲裝置。
- 如果分析中的得分大於或等於95，則AMP資料庫中的樣本將被標籤為惡意處置。
- AMP私有雲將追溯性檢測應用於分數大於或等於95的樣本。

程式

步驟1.設定和配置Threat Grid裝置（尚未整合）。 如有必要，檢查更新和安裝。

步驟2.設定和配置面向終端的AMP私有雲（尚未整合）。

步驟3.在Threat Grid管理UI中，選擇**Configuration**頁籤並選擇**SSL**。

步驟4.為Clean介面(PANDEM)產生或上傳新的SSL憑證。

重新生成SSL證書

如果clean介面的主機名與clean介面當前安裝在裝置中的證書中的主體替代名稱(SAN)不匹配，則可以生成新的自簽名證書。裝置為介面生成新證書，在自簽名證書的SAN欄位中配置當前介面主機名。

步驟4.1.從「操作」列中選擇**(...)，然後**從彈出選單中選擇「**生成新證書**」。

步驟4.2.在Threat Grid UI中，選擇**Operations**，在下一個螢幕中選擇**Activate**，然後選擇**Reconfigure**。

> **注意**：此生成的證書是自簽名證書。

上傳SSL證書

如果已經為Threat Grid裝置clean介面建立了證書，則可以將此證書上傳到裝置。

步驟4.1.從「操作」列中選擇**(...),**然後從彈出選單中選擇「**上傳新證書**」。

步驟4.2.在螢幕上顯示的文本框中以PEM格式複製證書和相應的私鑰，然後選擇**Add Certificate**。

步驟4.3.在Threat Grid UI中，選擇**Operations**，在下一個螢幕中選擇**Activate**，然後選擇**Reconfigure**。

步驟5.在AMP私有雲裝置管理UI中，選擇**Integrations**，然後選擇**Threat Grid**。

步驟6.在Threat Grid配置詳細資訊中，選擇**Edit**。

步驟7.在Threat Grid主機名中，輸入Threat Grid裝置的乾淨介面的FQDN。

步驟8.在Threat Grid SSL證書中，新增Threat Grid裝置安全介面的證書。（見下文附註）

Threat Grid裝置clean介面中的證書是自簽名的

步驟8.1.在Threat Grid管理UI中，選擇**Configuration**，然後選擇SSL。

步驟8.2.從「操作」列中選擇**(...),**然後從彈出選單中選擇「**Download Certificate**」。

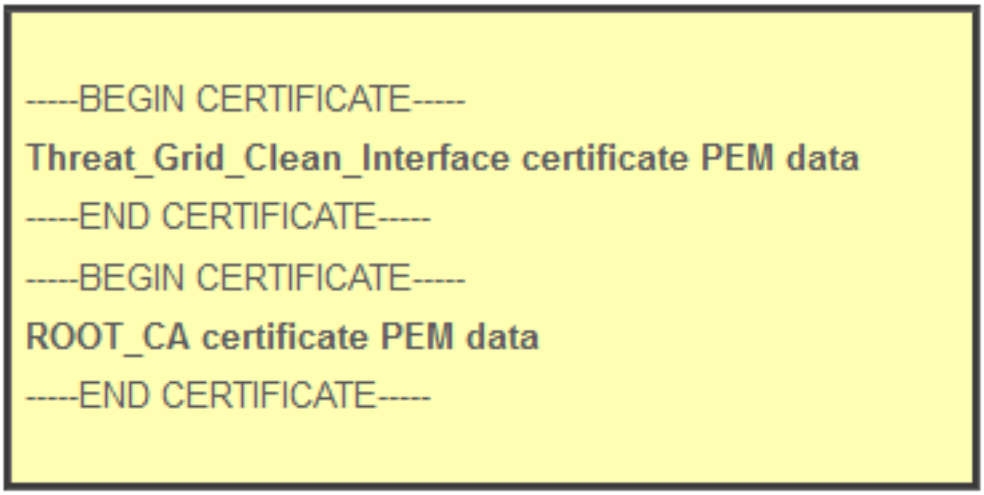
步驟8.3.繼續將下載的檔案新增到Threat Grid整合頁面中的AMP虛擬專用裝置。

Threat Grid裝置clean介面中的證書由企業證書頒發機構(CA)簽名

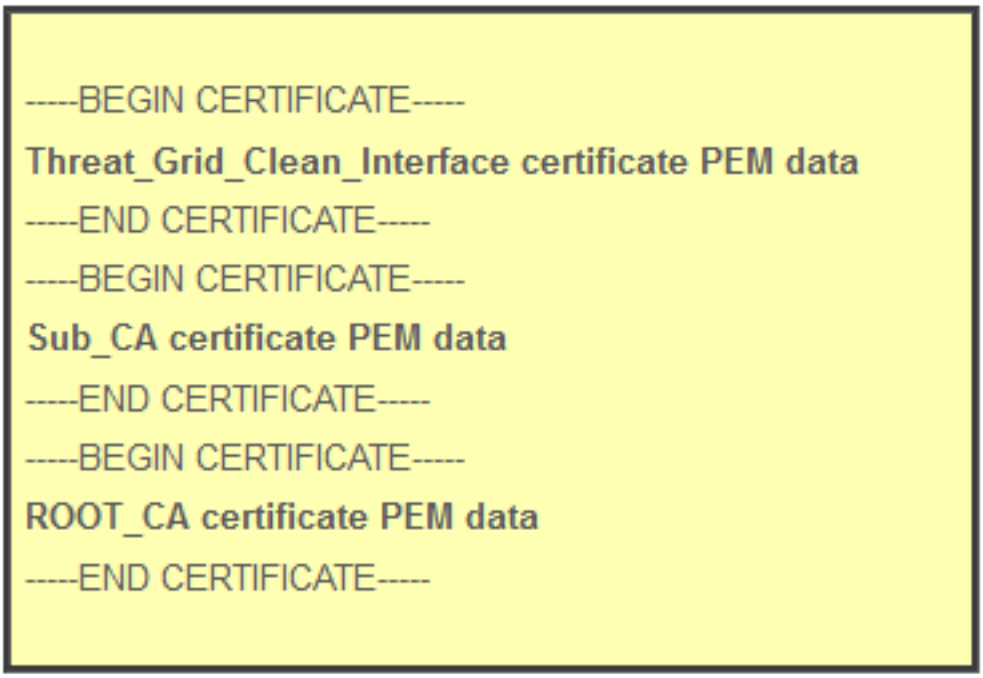
步驟8.1.將Threat Grid裝置clean介面的證書和完整的CA證書鏈複製到文本檔案中。

附註：文本檔案中的證書必須是PEM格式。

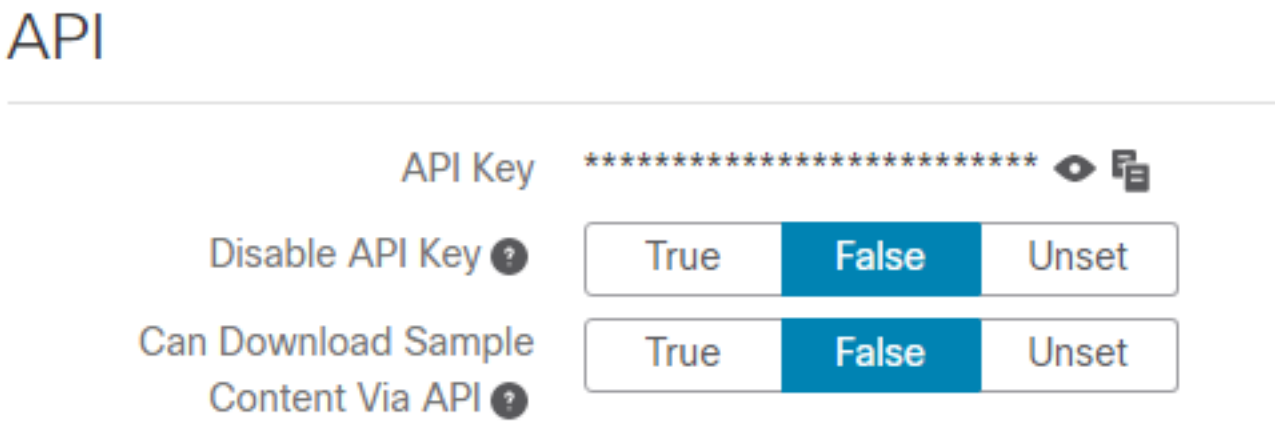
如果完整的憑證鏈結為：ROOT_CA證書> Threat_Grid_Clean_Interface證書；然後需要建立文本檔案，如圖所示。



如果完整的憑證鏈結為：ROOT_CA證書> Sub_CA證書> Threat_Grid_Clean_Interface證書；然後需要建立文本檔案，如圖所示。



9.Threat Grid APIThreat GridAPI



附註：在Threat Grid使用者的帳戶設定中，確認**Disable API Key**引數未設定為True。

步驟10.完成所有更改後，選擇**Save**。

步驟11.對AMP虛擬雲裝置應用重新配置。

步驟12.從AMP私有雲裝置管理UI中選擇**Integrations**，然後選擇**Threat Grid**。

步驟13.從**詳細資訊**複製處置更新服務URL、處置更新服務使用者和處置更新服務密碼的值。此資訊在步驟17中使用。

步驟14.在Threat Grid管理UI中，選擇**Configuration**，然後選擇**CA Certificates**。

步驟15.選擇**Add Certificate**，並以PEM格式複製簽署AMP私有雲部署更新服務證書的CA證書。

附註：如果簽署AMP私有雲部署更新證書的CA證書是子CA，請重複該過程，直到鏈中的所有CA都上傳到**CA證書**。

步驟16.在Threat Grid門戶中，選擇管理，然後選擇管理AMP私有雲整合。

步驟17.在「處置更新協同內容服務」頁中輸入在步驟13中收集的資訊。

- 服務URL:AMP私有雲裝置的處置更新服務的FQDN。
- 使用者：來自AMP私有雲裝置的處置更新服務的使用者。
- 密碼：AMP私有雲裝置的處置更新服務的密碼。

此時，如果所有步驟都應用正確，整合必須能夠成功運行。

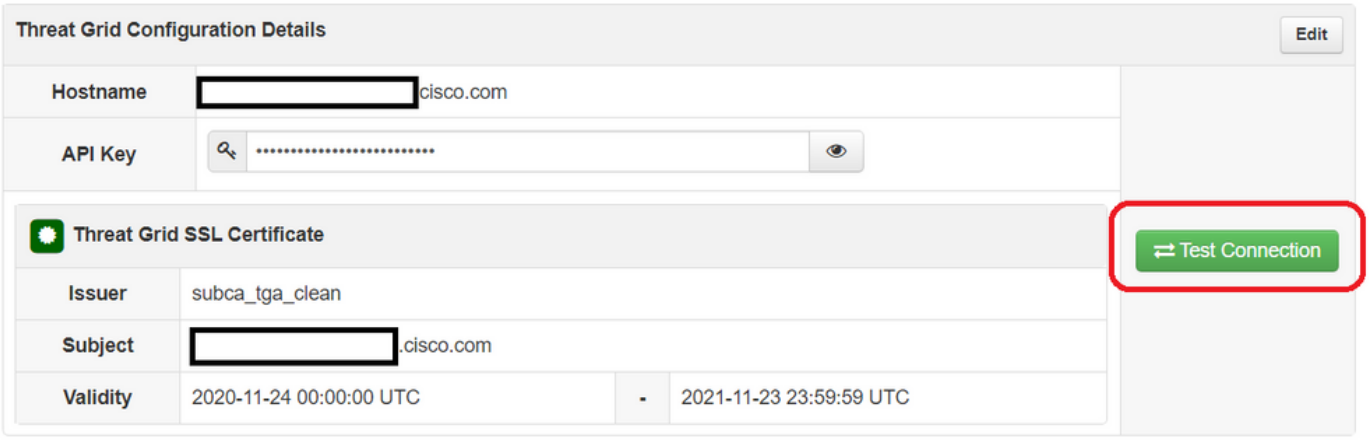
驗證

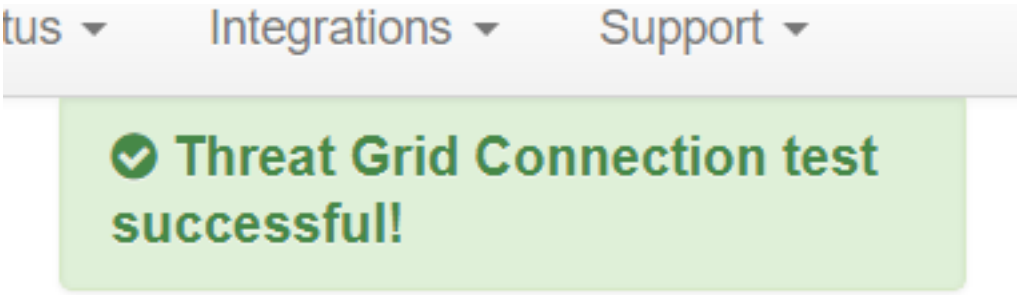
Threat Grid

註：只有步驟1、2、3和4才適合應用於生產環境以驗證整合。提供步驟5是為了瞭解有關整合

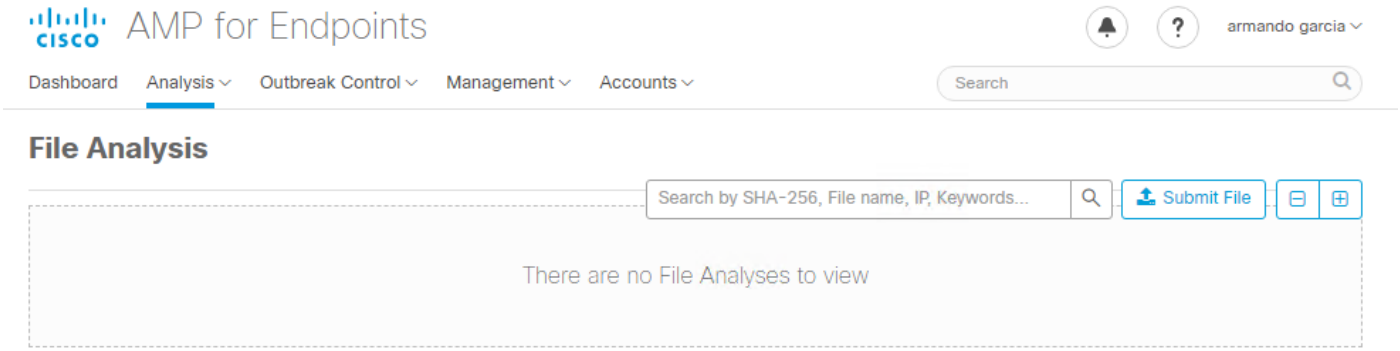
的更多資訊，建議不要將其應用於生產環境。

1.AMP Private Cloud Device Admin UI > Integrations > Threat GridTest ConnectionThreat Grid Connection test successful!

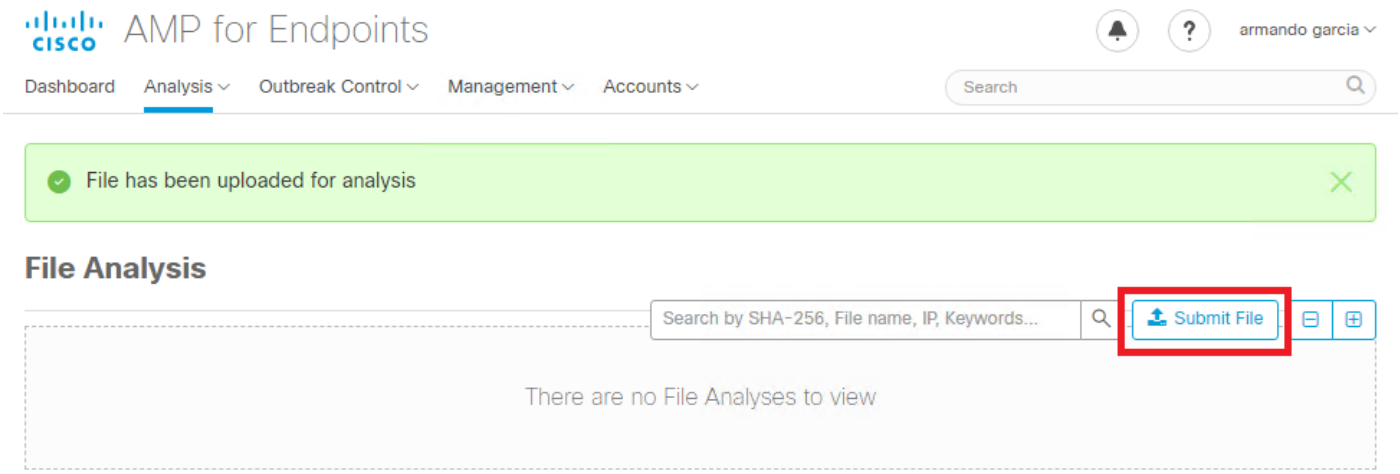


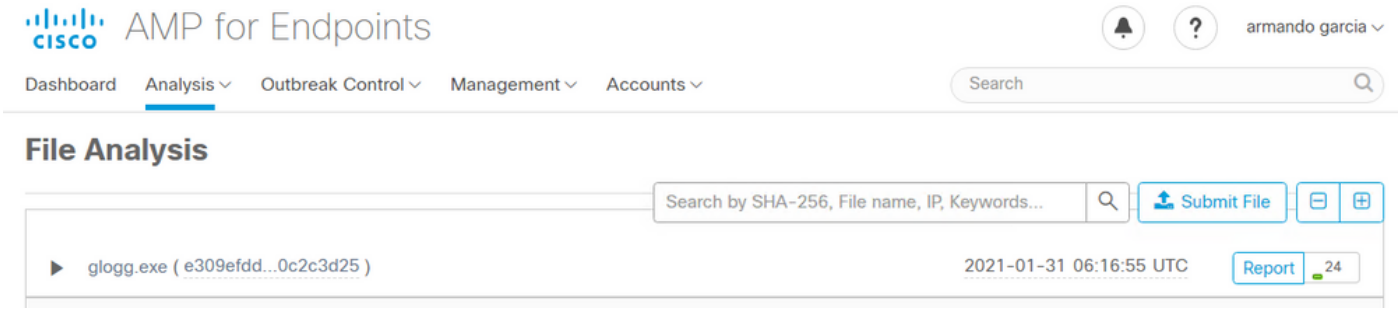


2.AMP



步驟3.確認在Threat Grid裝置中檢測到從AMP私有雲控制檯**Analysis > File Analysis**手動提交的檔案，並且Threat Grid裝置返回帶分數的報告。





步驟4.確認簽署AMP私有雲裝置的Disposition Update Service證書的CA已安裝在證書頒發機構的Threat Grid設**備中**。

步驟5.確認在報告和樣本分數由Threat Grid裝置提供後，由Threat Grid裝置標籤且分數高於95的任何樣本都記錄在AMP私有雲資料庫中，並且被處置為惡意。

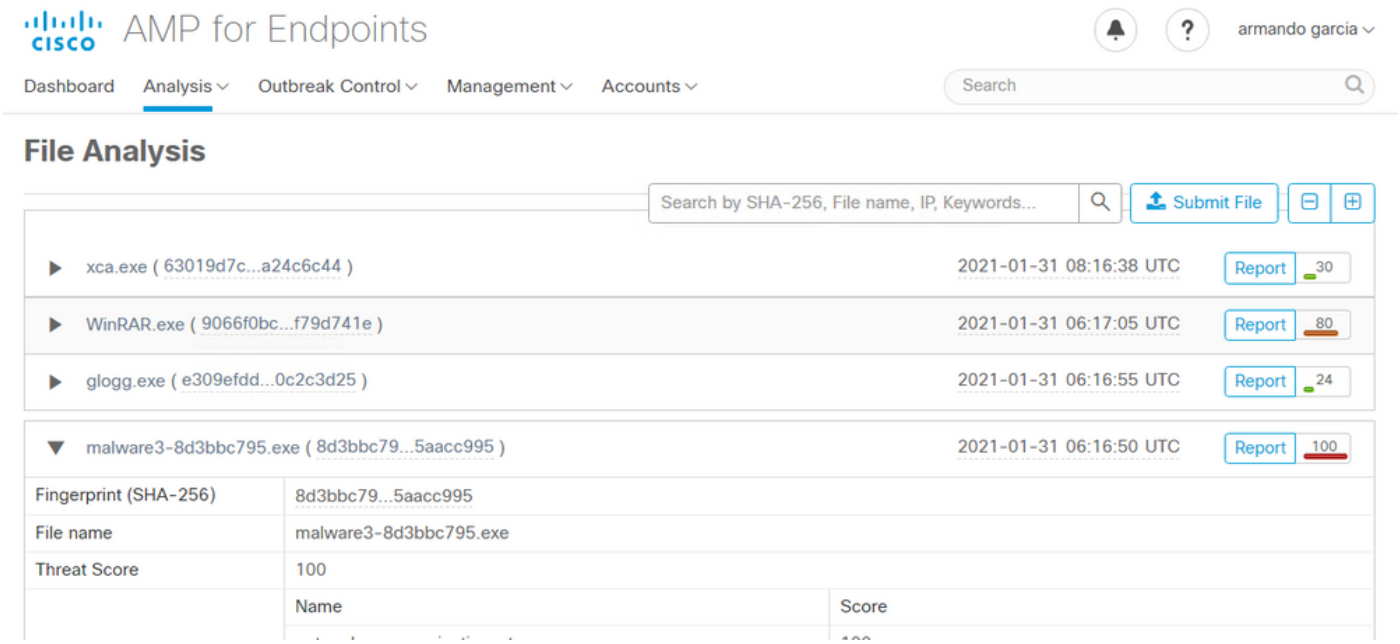
> **附註**：在AMP Private Cloud控制**檯File Analysis**頁籤中成功接收示例報告和>=95的示例分數，並不一定意味著在AMP資料庫中更改了檔案性質。如果簽署AMP私有雲裝置的Disposition Update Service證書的CA未安裝在**證書頒發機構**的Threat Grid裝置中，則AMP私有雲裝置會收到報告和分數，但不會從Threat Grid裝置收到任何標籤。

> **警告**：在Threat Grid裝置標籤了分數大於95的檔案後，已完成下一個測試，以觸發AMP資料庫中的示例處置更改。此測試的目的是在Threat Grid裝置提供>=95的樣本得分時提供有關AMP私有雲裝置內部操作的資訊。為了觸發處置更改過程，使用Cisco internal makemalware.exe應用程式建立了一個模仿惡意軟體的測試檔案。示例：malware3-419d23483.exeSHA256:8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995。

> **注意**：建議不要在生產環境中引爆任何模仿惡意軟體的測試檔案。

確認AMP私有雲資料庫中的樣本處置更新

AMPThreat GridThreat GridAMP100>=95AMPThreat Grid>=95AMP



如果：

- 已成功完成整合。
- 手動提交檔案後，在**File Analysis**中可感知示例報告和分數。

然後：

- 對於Threat Grid裝置以大於95的得分標籤的每個示例，將在AMP私有雲裝置中的檔案/data/poked/poked.log中新增一個條目。
- /data/poked/poked.log在Threat Grid裝置提供的第一個>=95的示例分數之後在AMP私有雲裝置中建立。
- AMP私有雲中的db_protect資料庫保留樣本的當前性質。此資訊可用於確認在Threat Grid裝置提供得分後，樣本的試樣狀態是否為3。

如果在AMP私有雲控制檯的**檔案分析**中觀察到示例報告和>=95分數，請應用以下步驟：

步驟1.通過SSH登入到AMP私有雲裝置。

步驟2.確認/data/poked/poked.log中有一個用於示例的條目。

列出從未從Threat Grid裝置收到>=95的示例分數的AMP私有雲裝置中的/data/poked/目錄，表明系統中尚未建立poked.log檔案。

如果AMP私有雲裝置從未從Threat Grid裝置收到過攻擊，則在目錄中找不到/data/poked/poked.log檔案，如圖所示。

```
[root@fireamp ~]# ls /data/poked/
poked_error.log
[root@fireamp ~]#
```

在接收到第一個>=95的示例分數後列出/data/poked/目錄，顯示檔案已建立。

收到分數大於95的第一個樣本後。

```
[root@fireamp ~]# ls /data/poked/
poked_error.log  poked.log
[root@fireamp ~]#
[root@fireamp ~]# cat /data/poked/poked.log
Jan 30 18:25:18 fireamp poked[9557]: [9557]  info @0.004940 127.0.0.1 --
{"disposition":"malicious","force":0,"state":"local","name":"W32.8D3BBC795B-100.SBX.TG","ok":1,"time":1612031118,"hash":"8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995","engine":"sha256"
,"user":"-","mode":"tg","score":100}
[root@fireamp ~]#
```

來自Threat Grid裝置提供的標籤的示例資訊可以在poked.log檔案中看到。

步驟3. **對示例SHA256運行此命令，以從AMP私有雲裝置的資料庫中檢索當前配置。**

```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

範例

在將樣本上傳到Threat Grid裝置之前獲取樣本處置情況的資料庫查詢未提供結果，如下圖所示。

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
[root@fireamp ~]#
```

從Threat Grid裝置收到報告和分數後，用於獲取樣本處置情況的資料庫查詢顯示了試樣狀態為3的樣本，該試樣狀態為3為惡意。

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
+------------------------------------------------------------------+----------------+
| hex(fingerprint)                                                 | disposition_id |
+------------------------------------------------------------------+----------------+
| 8D3BBC795BB47447984BF2842D3A0119BAC0D79A15A59686951E1F7C5AACC995 |              3 |
+------------------------------------------------------------------+----------------+
[root@fireamp ~]#
```

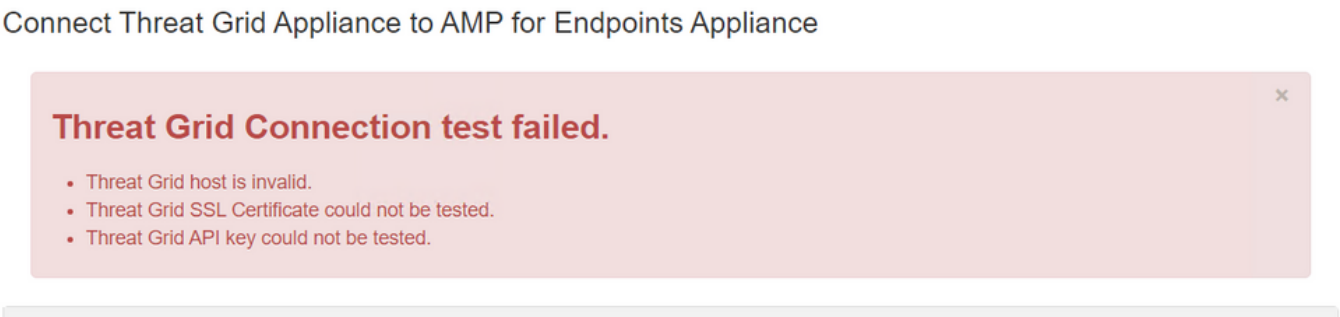
疑難排解

在整合過程中，可以發現可能的問題。檔案的這一部分涉及一些最常見的問題。

AMP私有雲裝置中的警告：主機無效、證書未測試、API金鑰未測試

症狀

警告消息：Threat Grid主機無效，無法測試Threat Grid SSL證書，無法測試Threat Grid API金鑰，在AMP私有雲裝置中選擇了**Integrations > Threat Grid**中的**Test Connection**按鈕後接收。



整合中的網路級別有問題。

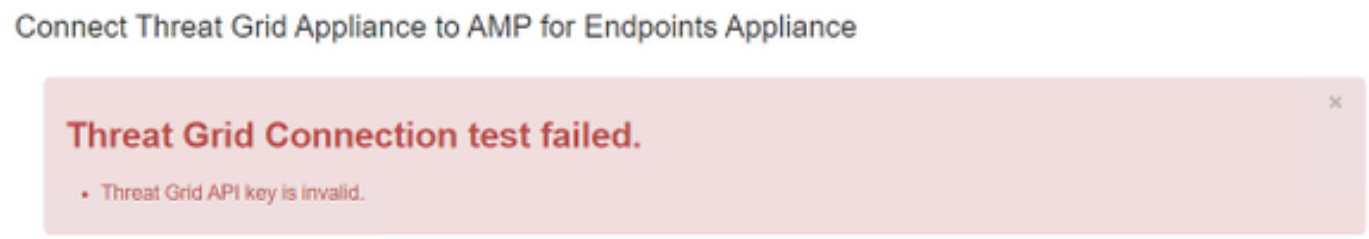
建議的步驟：

- 確認AMP Private Cloud裝置控制檯介面可以訪問Threat Grid裝置清潔介面。
- 確認AMP私有雲裝置可以解析Threat Grid裝置清理介面的FQDN。
- 確認AMP私有雲裝置和Threat Grid裝置的網路路徑中沒有過濾裝置。

AMPThreat Grid API

症狀

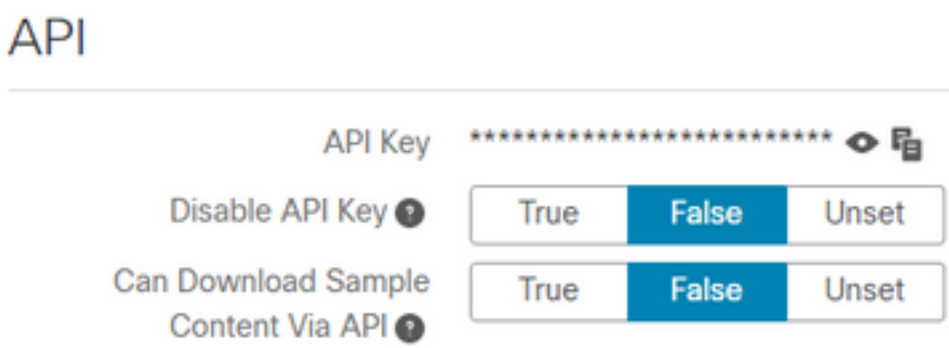
警告消息：Threat Grid連線測試失敗，Threat Grid API無效，在選擇了**整合> Threat Grid**中的**測試連線**按鈕後，在AMP私有雲裝置中接收。



AMPThreat GridAPI

建議的步驟：

- 在Threat Grid裝置使用者的帳戶設定中確認，Disable API Key引數未設定為True。
  — 必須將Disable API Key引數設定為：False或Unset。



- 確認AMP私有雲管理門戶**整合> Threat Grid**中配置的Threat Grid API金鑰與Threat Grid裝置中的使用者設定中的API金鑰相同。
- 確認是否在AMP私有雲裝置資料庫中儲存了正確的Threat Grid API金鑰。

從AMP私有雲裝置命令列中，可以確認在AMP裝置中配置的當前Threat Grid API金鑰。通過SSH登入到AMP私有雲裝置並運行此命令以檢索當前的Threat Grid使用者API金鑰：

```
mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
```

這是AMP私有雲裝置資料庫中針對Threat Grid裝置API金鑰的正確條目。

```
[root@fireamp ~]#  mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
+--------------------------+----------------------+----------------------+
| tg_api_key               | tg_login             | api_client_id        |
+--------------------------+----------------------+----------------------+
| mirt1if[redacted]nnjae7 | argarci2_samples-user | de4c23c64d3e36034bb7 |
+--------------------------+----------------------+----------------------+
[root@fireamp ~]#
```

即使未直接在整合的任何步驟中的AMP私有雲裝置中配置Threat Grid使用者名稱，但如果正確應用了Threat Grid API金鑰，則會在AMP資料庫的tg_login引數中感知Threat Grid使用者名稱。

這是Threat Grid API金鑰的AMP資料庫中的錯誤條目。

```
[root@fireamp ~]# mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
+-------------------------+----------+----------------------+
| tg_api_key              | tg_login | api_client_id        |
+-------------------------+----------+----------------------+
| thisisanwrongapikey     | NULL     | de4c23c64d3e36034bb7 |
+-------------------------+----------+----------------------+
[root@fireamp ~]#
```

tg_loginNULLAMPThreat GridThreat Grid

AMP私有雲裝置接收到樣本得分>=95，但樣本處置中並未發現任何變化

症狀

提交樣本後，從Threat Grid裝置成功接收了報告和>=95個樣本分數，但在AMP私有雲裝置中看不到樣本配置發生任何變化。

建議的步驟：

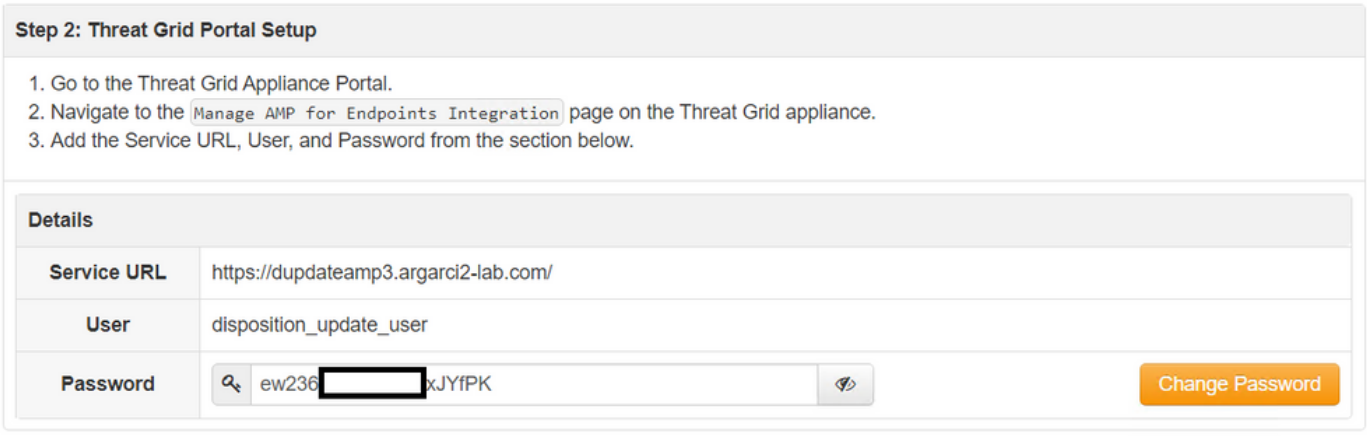
- 在AMP私有雲裝置中確認示例SHA256位於/data/poked/poked.log的內容中。

如果在/data/poked/poked.log中找到SHA256，則運行此命令以確認AMP資料庫中的當前樣本性質。

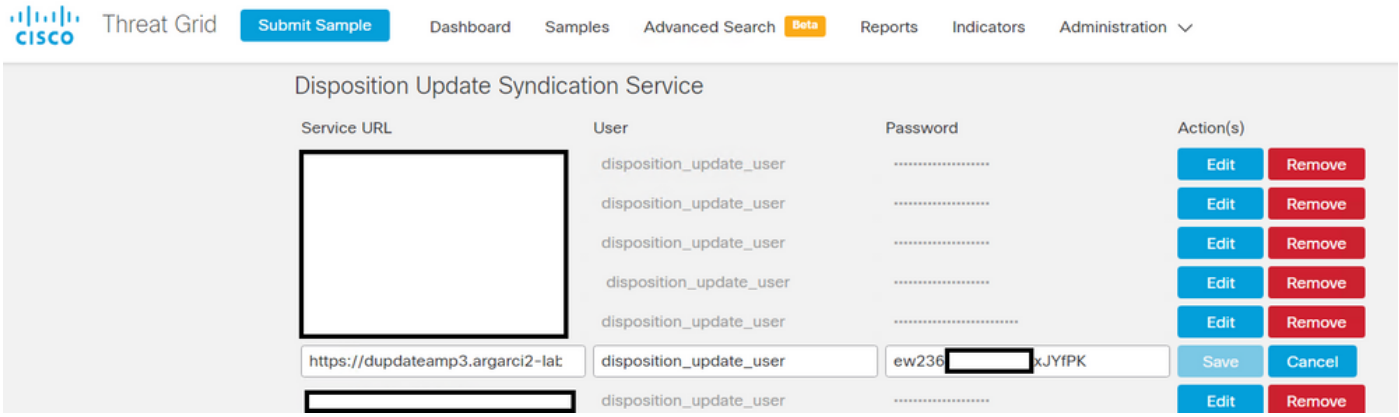
```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

- 在**管理>管理AMP私有雲整合**中，確認已將正確的AMP私有雲整合密碼新增到Threat Grid裝置管理門戶。

AMP私有雲管理門戶。



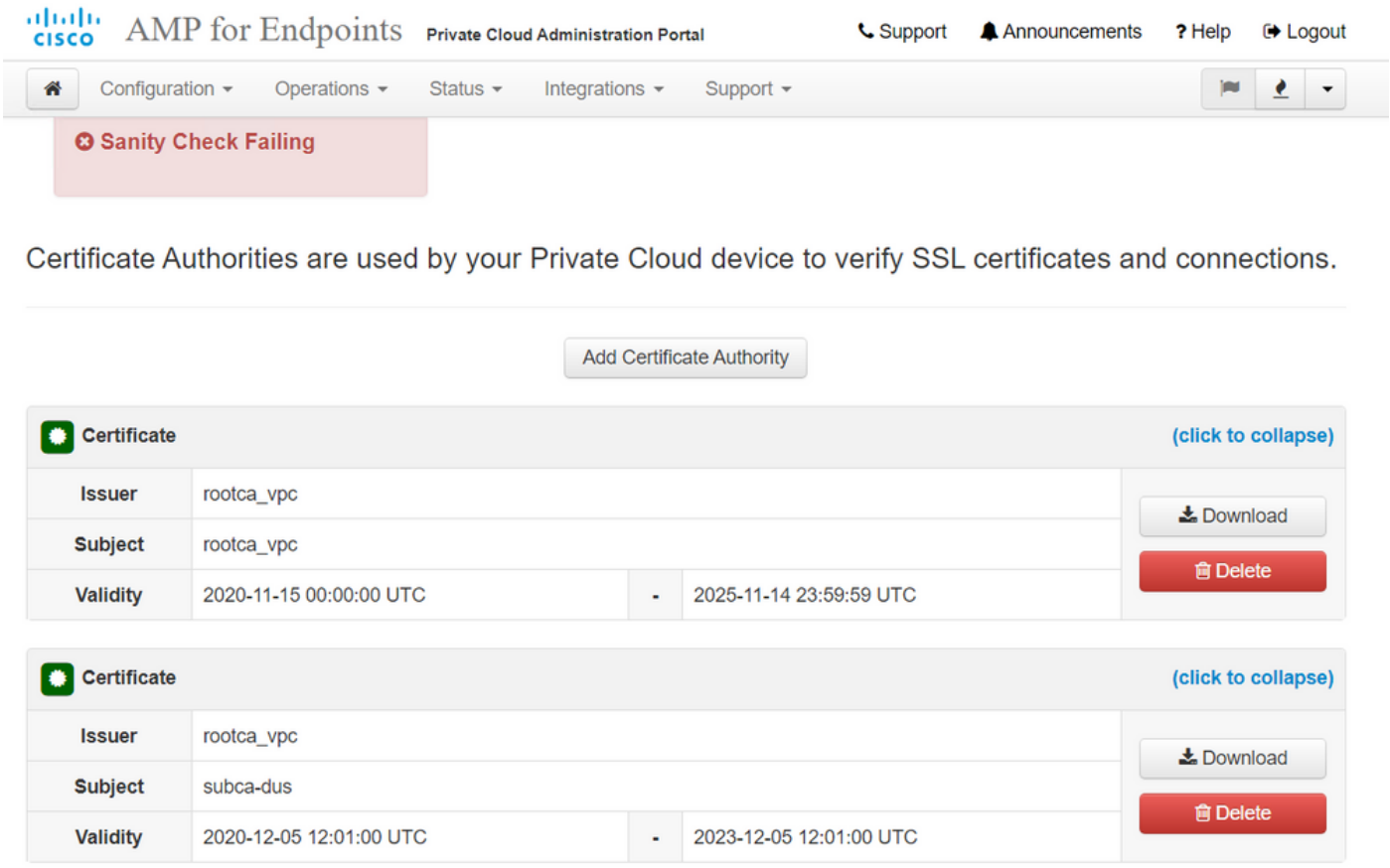
Threat Grid裝置控制檯門戶。



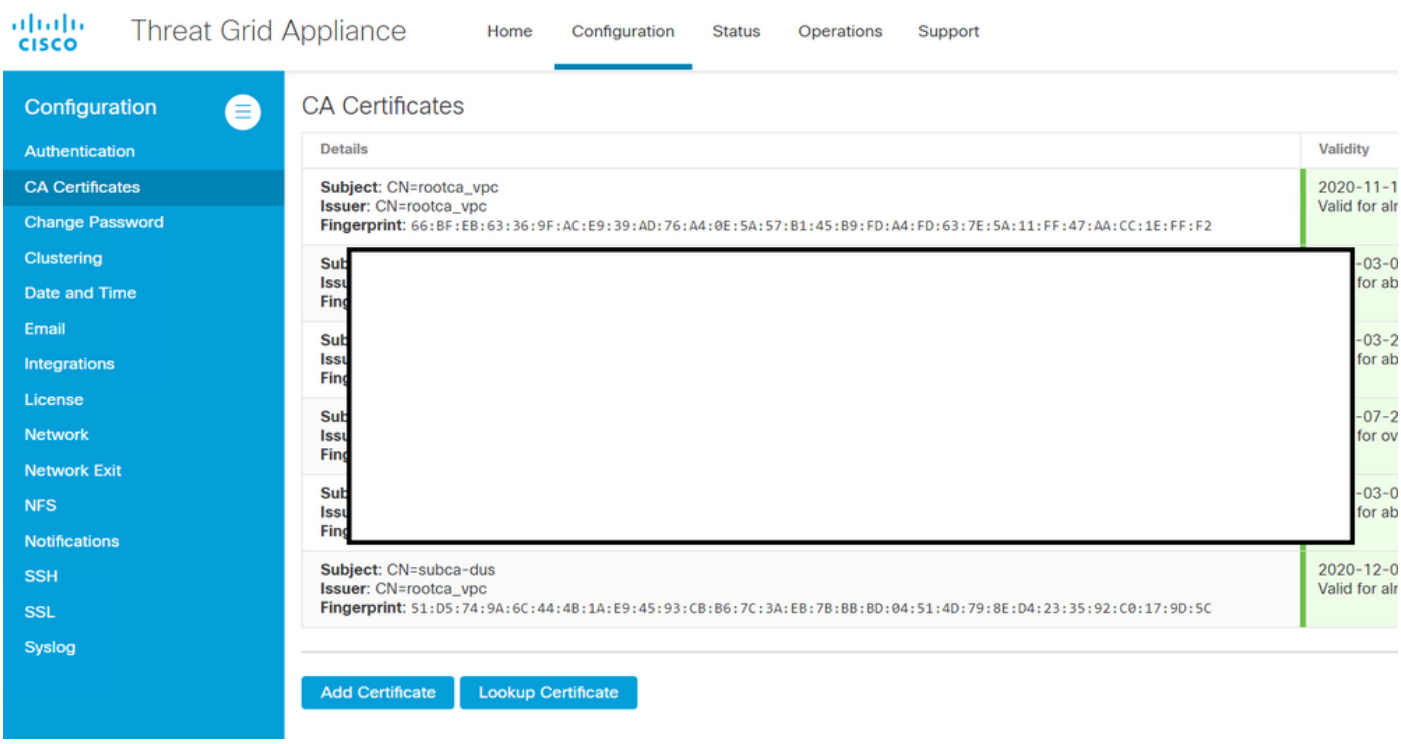
- 確認簽署AMP私有雲裝置處置更新服務證書的CA已安裝在CA證書中的Threat Grid裝置管理門戶中。

在以下示例中，AMP私有雲裝置處置更新服務證書的證書鏈為**Root_CA > Sub_CA > Disposition_Update_Service證書**;因此，必須在Threat Grid裝置的**CA證書**中安裝RootCA和Sub_CA。

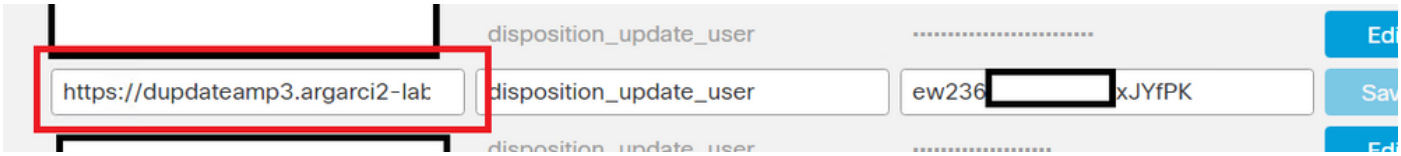
AMP私有雲管理門戶中的證書頒發機構。



Threat Grid



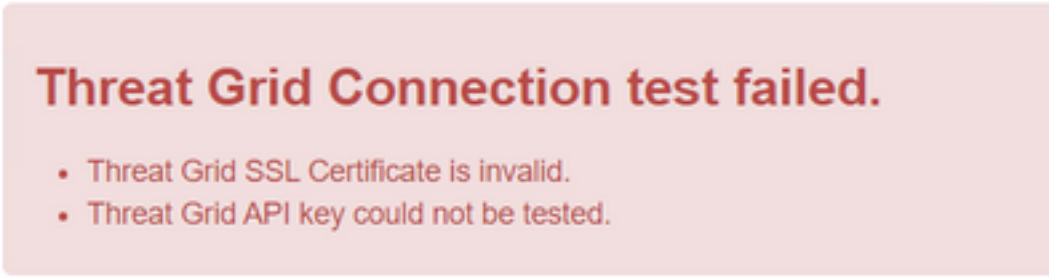
- **>AMP**AMPFQDNThreat GridAMPIPFQDN



AMP私有雲裝置中有關Threat Grid SSL證書無效的警告

症狀

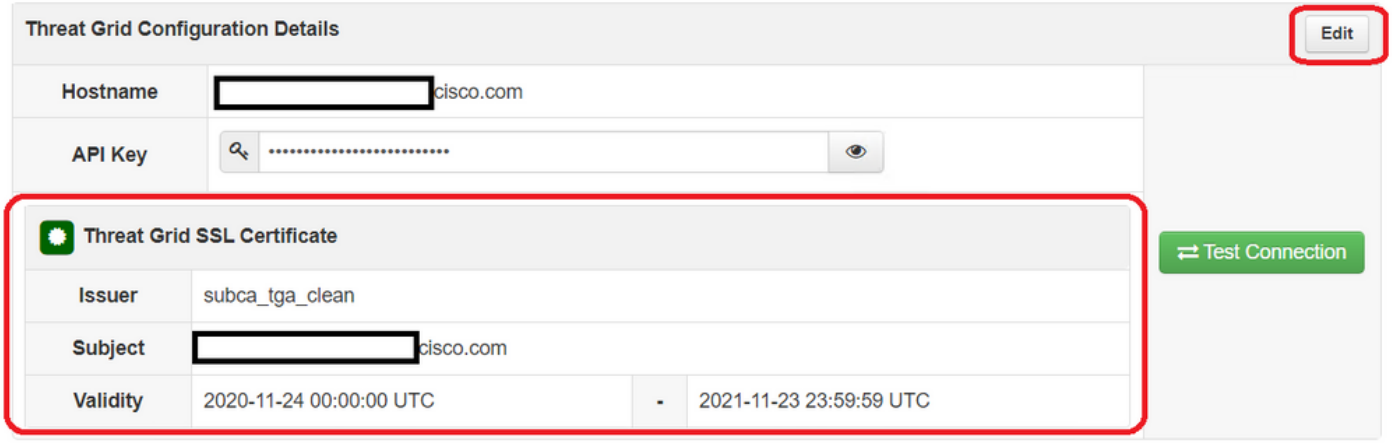
警告消息：在**Integrations > Threat Grid**中選擇**Test Connection**按鈕後，在AMP私有雲裝置中收到「Threat Grid SSL證書無效」。



建議的步驟：

- 確認Threat Grid裝置clean介面中安裝的證書是否由公司CA簽名。

如果由CA簽署，則必須在檔案內將完整的證書鏈新增到AMP私有雲裝置管理門戶**Integrations > Threat Grid(Threat Grid SSL證書)**中。



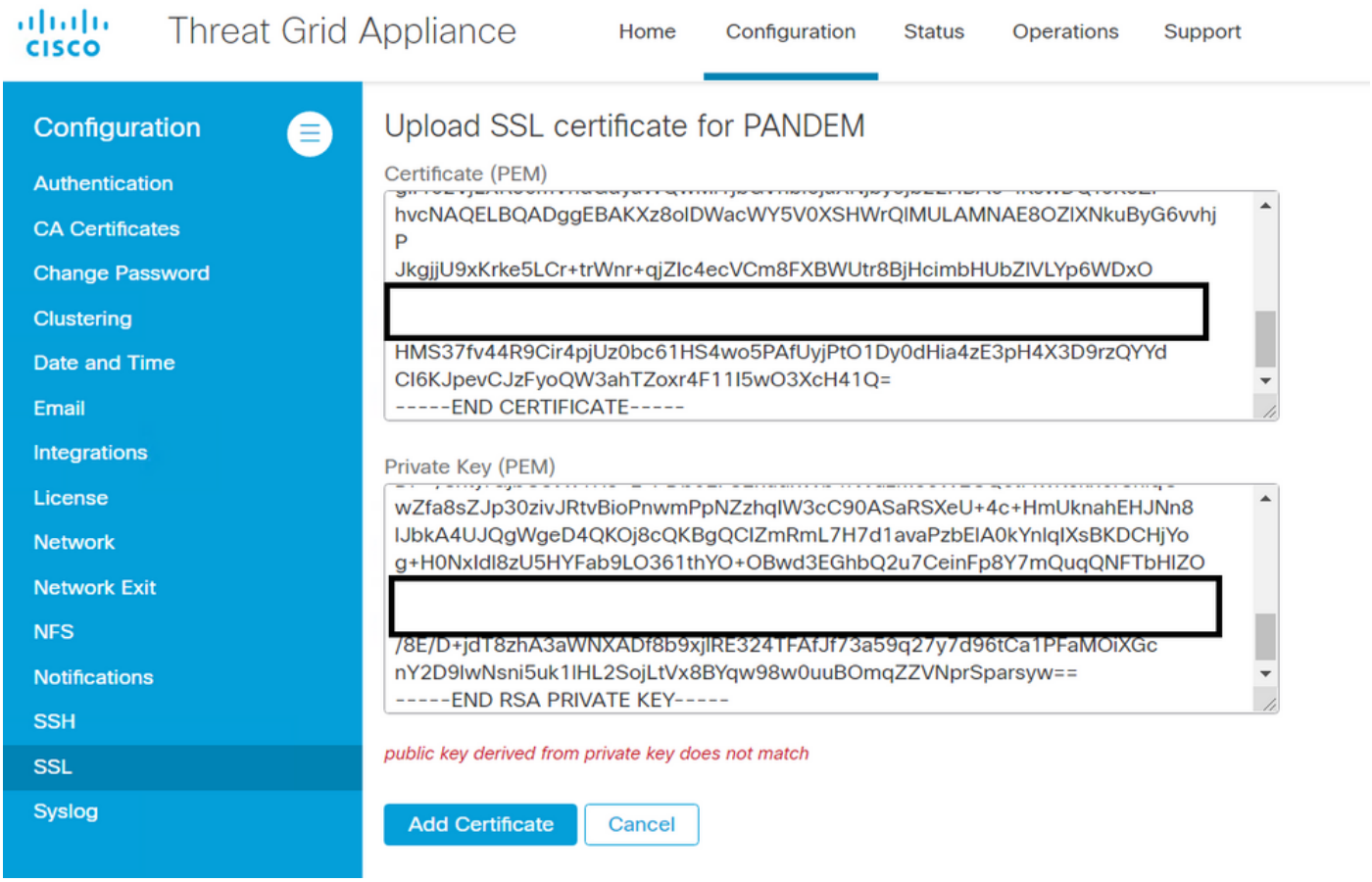
在AMP私有雲裝置中，可以在以下位置找到當前安裝的Threat Grid裝置證書：/opt/fire/etc/ssl/threat_grid.crt。

Threat Grid裝置中與證書相關的警告

警告消息 — 從私鑰派生的公鑰不匹配

症狀

警告消息：從私鑰派生的公鑰不匹配，在嘗試向介面新增證書後在Threat Grid裝置中接收。



從私鑰匯出的公鑰與證書中配置的公鑰不匹配。

建議的步驟：

- 確認私鑰是否與憑證中的公鑰相符。

如果私鑰與證書中的公鑰匹配，則模數和公鑰指數必須相同。對於此分析，僅確認模數在私鑰和證書中的公鑰中是否具有相同的值就足夠了。

步驟1.使用OpenSSL工具比較私鑰和憑證中設定的公鑰的模數。

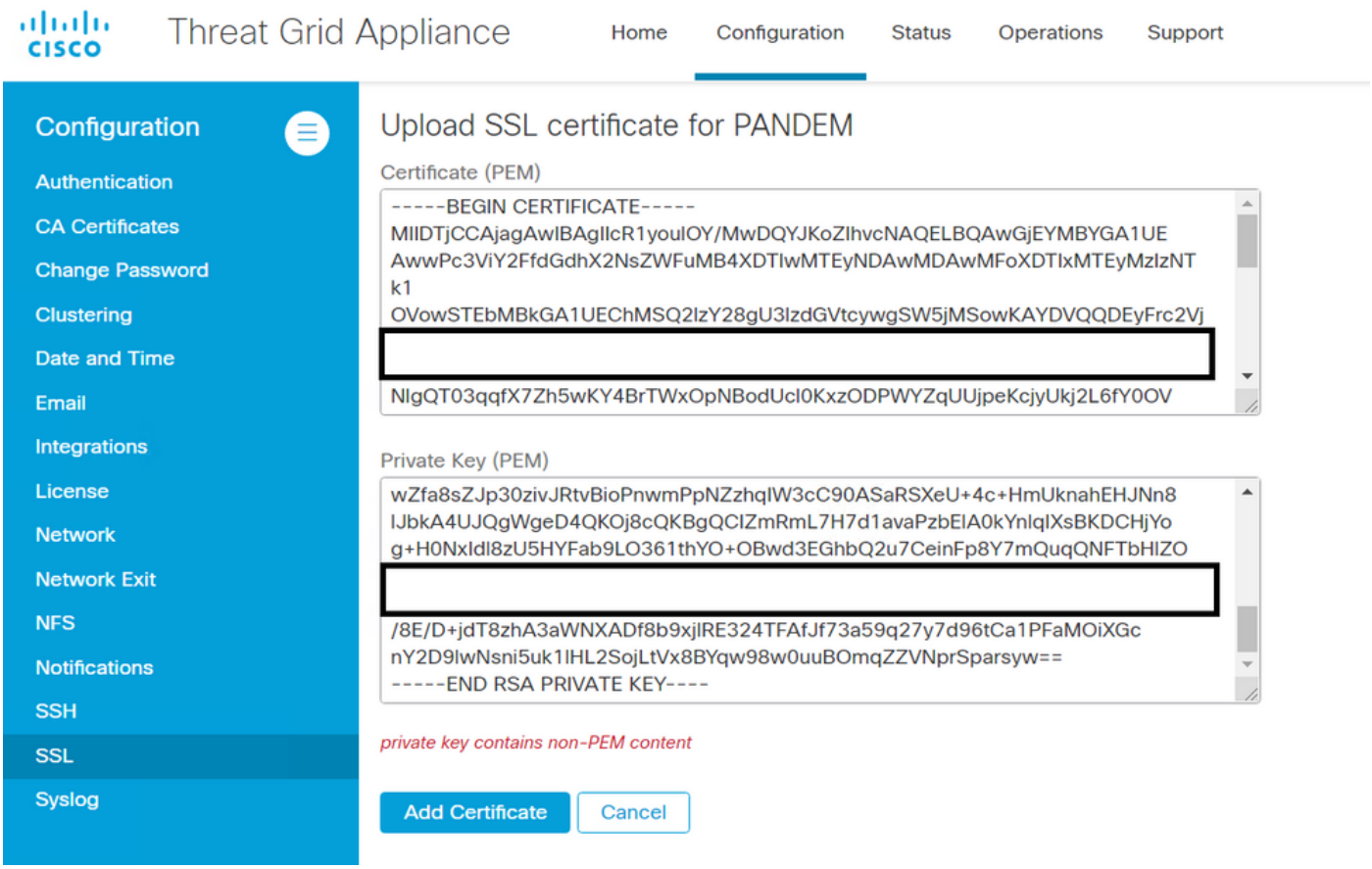
```
openssl x509 -noout -modulus -in
```

```
$ openssl x509 -noout -in certificate.cert | openssl md5
(stdin)= d41d8cd98f00b204e9800998ecf8427e
$
$
$ openssl rsa -noout -in private-key.key | openssl md5
(stdin)= d41d8cd98f00b204e9800998ecf8427e
```

警告消息 — 私鑰包含非PEM內容

症狀

警告消息：嘗試向介面新增證書後，Threat Grid裝置會收到包含非PEM內容的私鑰。



私鑰檔案中的PEM資料已損壞。

建議的步驟：

-

步驟1.使用OpenSSL工具驗證私鑰的完整性。

```
openssl rsa -check -noout -in
```

.PEMPEM

```
$ openssl rsa -check -noout -in wrong-private-key.key
unable to load Private Key
140333463315776:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:


$ openssl rsa -check -noout -in correct-private-key.key
RSA key ok
```

如果OpenSSL指令輸出不是**RSA Key ok**，這表示找到金鑰中的PEM資料有問題。

如果發現OpenSSL指令存在的問題，則：

- 確認私鑰中的PEM資料是否丟失。

私鑰檔案中的PEM資料以64個字元的行顯示。快速檢查檔案內的PEM資料可以顯示資料是否丟失。缺少資料的行未與檔案中的其他行對齊。

• 確認私鑰中的第一行以5個連字元開頭，單詞**BEGIN PRIVATE KEY**，以5個連字元結尾。
範例.

-----BEGIN PRIVATE KEY-----

• 確認私鑰中的最後一行以5個連字元開頭，即**END PRIVATE KEY**，以5個連字元結尾。
範例.

-----END PRIVATE KEY-----

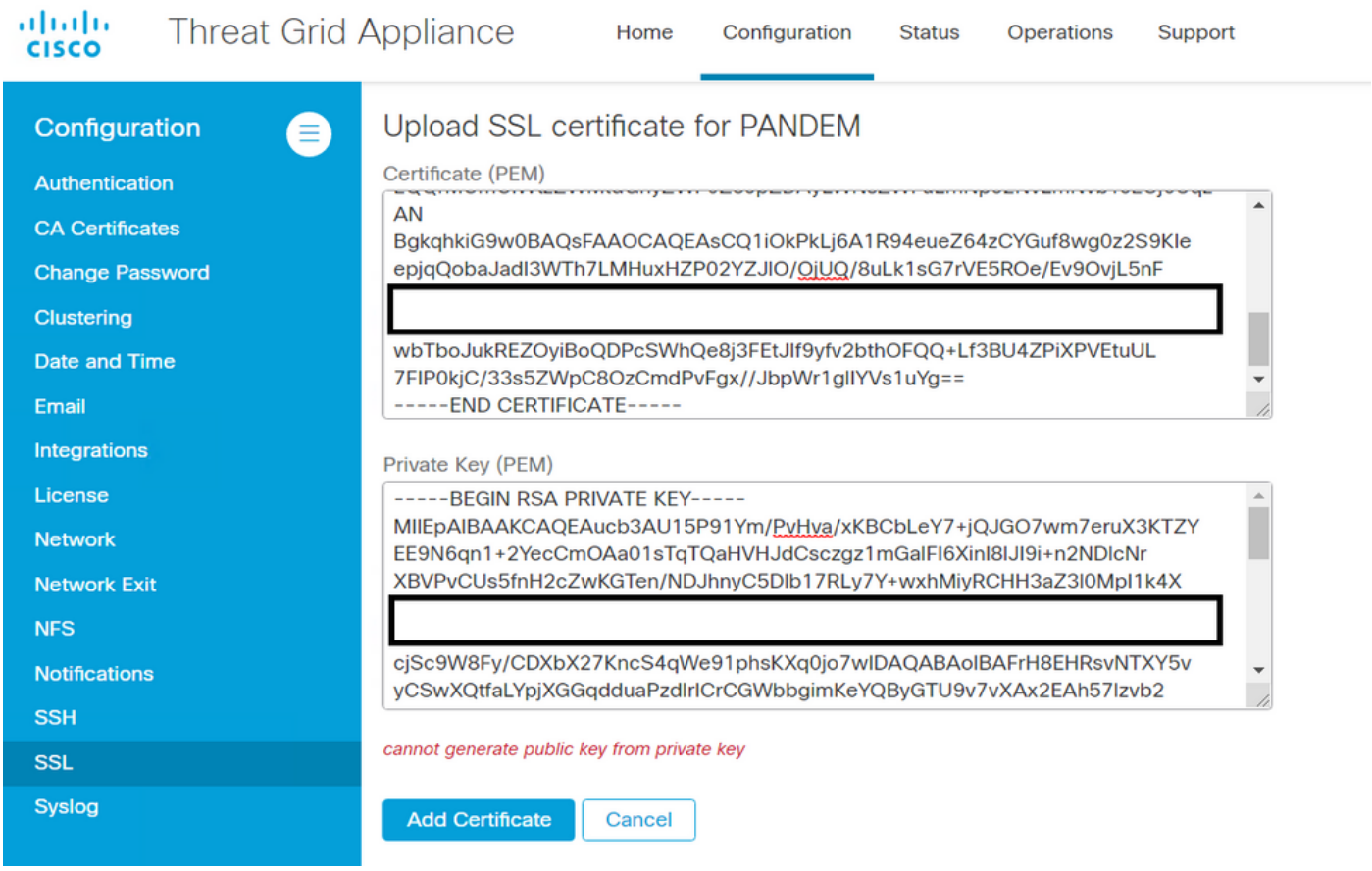
範例.私鑰中正確的PEM格式和資料。

```
$ cat correct-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCvfIytwkf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/PW4fE
/JNGbMIU/d1DDuzxfgGze0viztT9OrpCbZyQP2r+sGxaOKM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUXODeHLjTIcI2q/vH/iOWeIgAv10aGuBCOegVDU
NwOgPyY3XI8g7H                                          4HA6/VsM10NHKT4EhvSks
WXZW1XhNAgMBAA                                          tU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXfB                                          s7k0sCwmhKUaMAcTYAnrg
fINIJto/xOazhe                                          47ttvLvX3zweLCEXsDXK6
mdhzCQSTBfYbM4                                          R4M7HiocsbkLjijScTFYQ
JqSwA5BEgqeH3a                                          hgd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb9                                          BgQDePpxacxGRZLXfja3s
SU+TvjNWQGcUsX                                          a8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2xOCy51K5KsfDPa/SrbhDkxZty0SG
lCgVLEycQ5tlxtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRLPxeCS
CbcflDYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBgHFn/ZziDtrkSzJSN6fVGPhJHCUtI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUhOQvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDPlbP5LFkTMG27Brzr9oG95F45hrZOgWOD+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXzlOMn+A0
SxuwKWoARshnMsDvsTYWofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmblpAYS
DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IWaocGU8RQUJY5L6rmw+yls6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

警告消息 — 無法從私鑰生成公鑰

症狀

警告消息：嘗試向介面新增證書後，Threat Grid裝置會收到該私鑰無法生成公鑰。



無法從私鑰檔案內的當前PEM資料生成公鑰。

建議的步驟：

-

1.OpenSSL

```
openssl rsa -check -noout -in
```

如果OpenSSL指令輸出不是**RSA Key ok**，這表示找到金鑰中的PEM資料有問題。

步驟2.使用OpenSSL工具驗證是否可從私鑰中匯出公鑰。

```
openssl rsa -in
```

範例.公鑰匯出失敗，公鑰匯出成功。

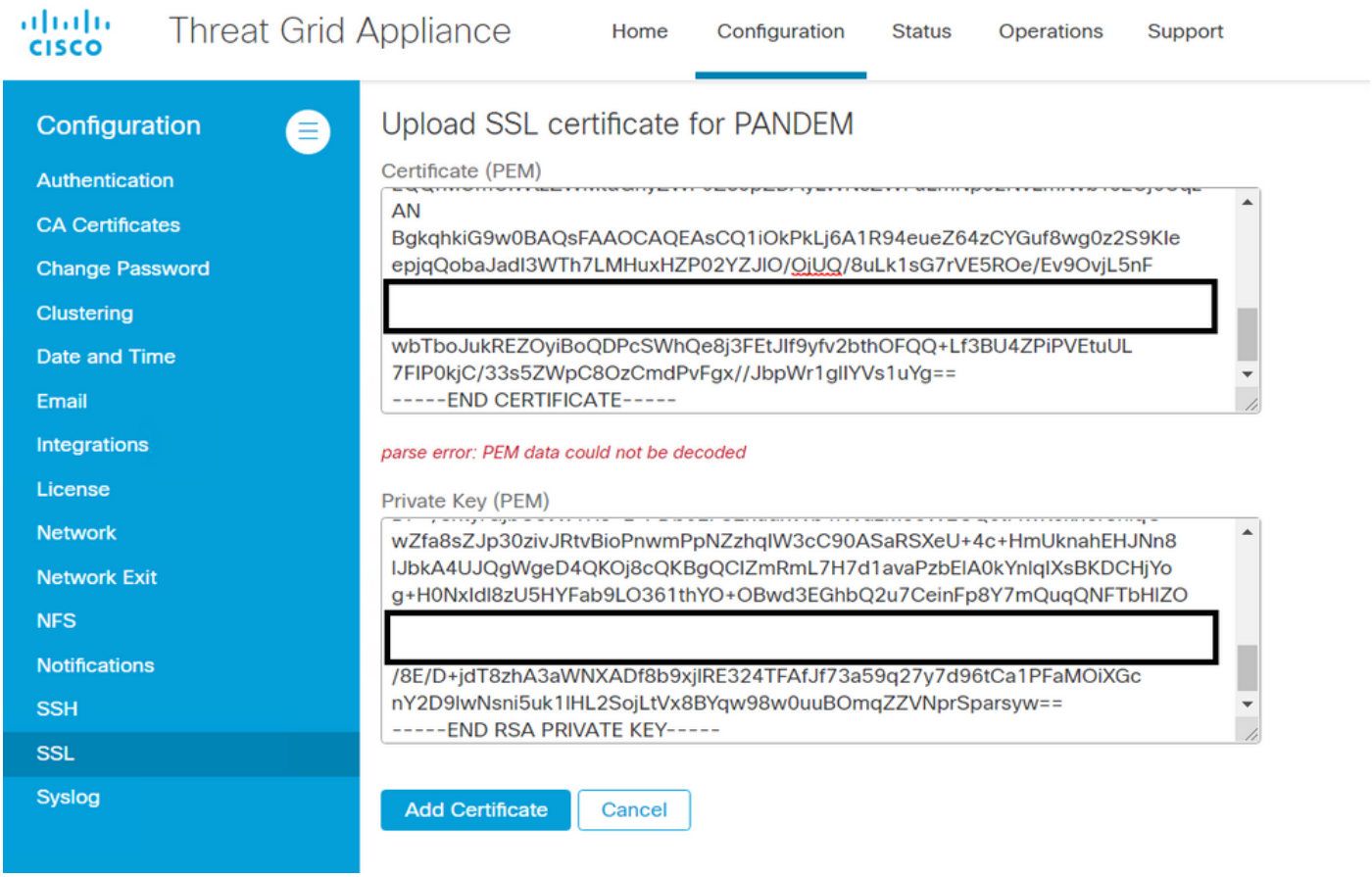
```
$ openssl rsa -in wrong-private-key.key -pubout
unable to load Private Key
140195161523520:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

$ openssl rsa -in correct-private-key.key -pubout
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr3yMrcJH/VCHOQ5bivT0
2yrw60oYJ/Pwnp/cFxFAyATWoZRYmb8GW/+RS/iNa8vz9FiiTIl0YS0OdmNKKIEL
Lg08O/TKGusV2CyqtT+UESFerUEAzYh1KBxTUi5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBsWjijNHNwBICv6WAO2gr/xj+qxpB3
P1YjNTU7llSFnSHC4E1Fzg3hy40yHCNqv7x/4jlniIAL9dGhrgQjnoFQ1DcDoD8m
N1yPIOx3C0lWeVForZmx+Dg6l+J4uIjytkVceBwOv1bDNdDRyk+BIb0pLFl2VtV4
TQIDAQAB
-----END PUBLIC KEY-----
```

警告消息 — 分析錯誤：無法解碼PEM資料

症狀

警告消息：分析錯誤：無法解碼PEM資料，在嘗試向介面新增證書後在Threat Grid裝置中接收。



無法從證書檔案中的當前PEM資料解碼證書。證書檔案中的PEM資料已損壞。

- 確認是否可以從證書檔案中的PEM資料檢索證書資訊。

步驟1.使用OpenSSL工具顯示PEM資料檔案中的憑證資訊。

```
openssl x509 -in
```

如果PEM資料已損壞，則會在OpenSSL工具嘗試載入證書資訊時發現錯誤。

範例.由於證書檔案中的PEM資料損壞，嘗試載入證書資訊失敗。

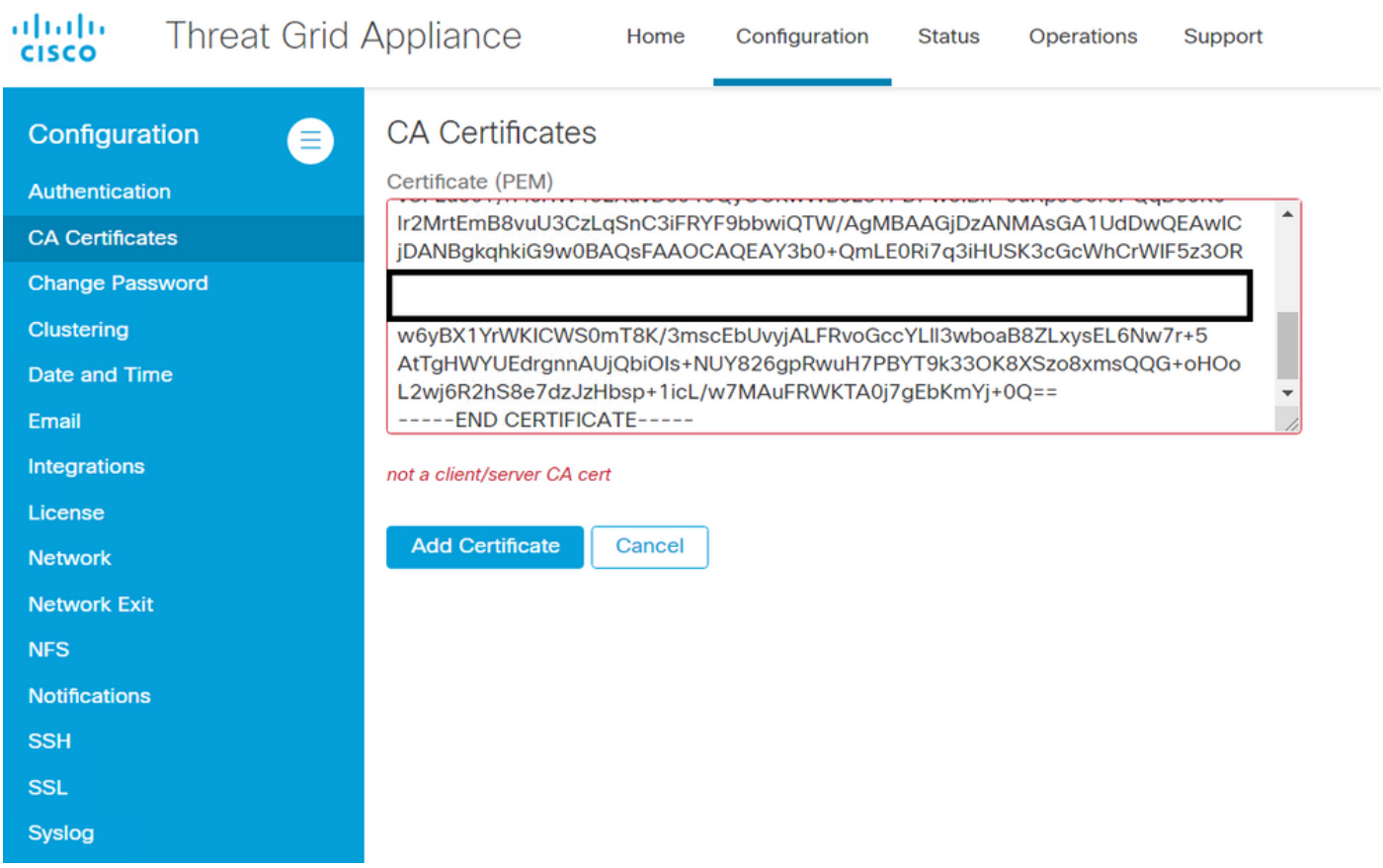
```
$ openssl x509 -in wrong-certificate.cert -text -noout
unable to load certificate
140159319831872:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:
```

警告消息 — 不是客戶端/伺服器CA證書

症狀

警告消息：分析錯誤：嘗試將CA證書新增到**Configuration > CA Certificates**後，會在Threat Grid裝

置中收到非客戶端/伺服器CA證書。



CA證書中的基本約束擴展值未定義為CA:沒錯。

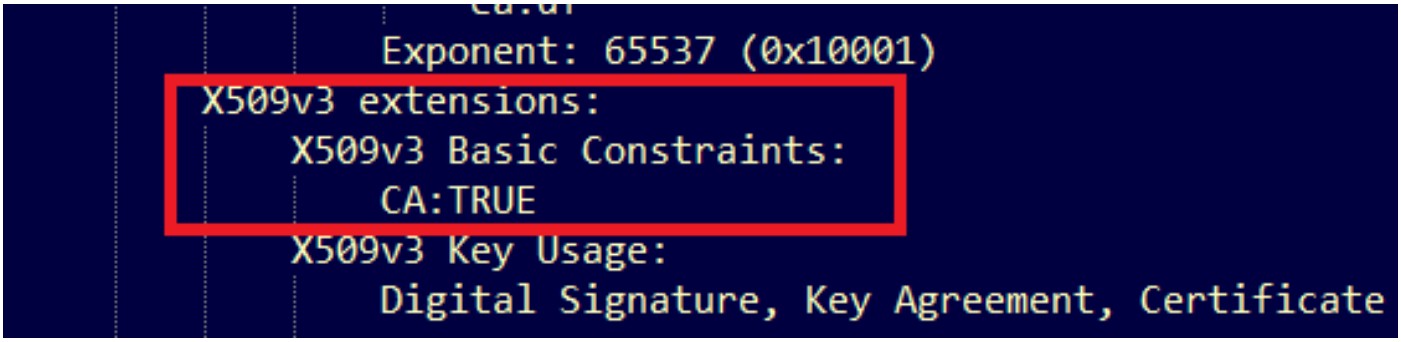
如果基本約束擴展值設定為CA，請用OpenSSL工具確認：CA憑證中為True。

步驟1.使用OpenSSL工具顯示PEM資料檔案中的憑證資訊。

```
openssl x509 -in
```

步驟2.在證書資訊中搜尋基本約束擴展**的當前**值。

範例.Threat Grid裝置接受的CA的基本約束值。



相關資訊

- Threat Grid裝置 — 配置指南

- Cisco AMP虛擬私有雲裝置 — 配置示例和技術說明
- 技術支援與文件 - Cisco Systems