

# AMP虛擬私有雲和Threat Grid裝置的整合

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[整合架構](#)

[有關整合的基本資訊](#)

[程式](#)

[重新生成SSL證書](#)

[上傳SSL證書](#)

[Threat Grid裝置clean介面中的證書是自簽名的](#)

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

[範例](#)

[驗證](#)

[確認AMP私有雲資料庫中的樣本處置更新](#)

[範例](#)

[疑難排解](#)

[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](#)

[AMP私有雲裝置中有關Threat Grid API金鑰無效的警告](#)

[AMP私有雲裝置接收到樣本得分 \$\geq 95\$ ，但樣本處置中並未發現任何變化](#)

[AMP私有雲裝置中有關Threat Grid SSL證書無效的警告](#)

[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](#)

[警告消息 — 私鑰包含非PEM內容](#)

[警告消息 — 無法從私鑰生成公鑰](#)

[警告消息 — 分析錯誤：無法解碼PEM資料](#)

[警告消息 — 不是客戶端/伺服器CA證書](#)

[相關資訊](#)

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

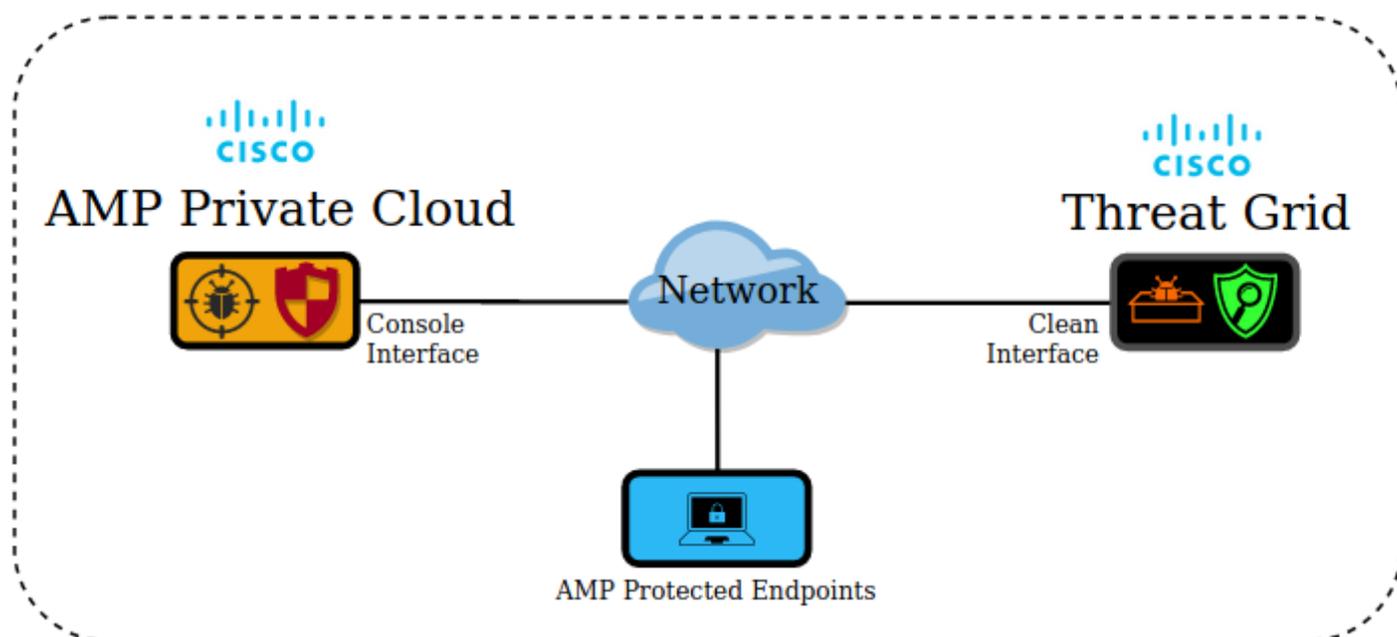
本文中的資訊係根據以下軟體和硬體版本：

- 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。

```
-----BEGIN CERTIFICATE-----  
Threat_Grid_Clean_Interface certificate PEM data  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
ROOT_CA certificate PEM data  
-----END CERTIFICATE-----
```

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。

```
-----BEGIN CERTIFICATE-----  
Threat_Grid_Clean_Interface certificate PEM data  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Sub_CA certificate PEM data  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
ROOT_CA certificate PEM data  
-----END CERTIFICATE-----
```

# API

API Key \*\*\*\*\*  

Disable API Key   True  False  Unset

Can Download Sample Content Via API   True  False  Unset

**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!

### Threat Grid Configuration Details Edit

Hostname	<input type="text" value="cisco.com"/>
API Key	<input type="password" value="....."/>
<b>Threat Grid SSL Certificate</b> <span>⇒ Test Connection</span>	
Issuer	subca_tga_clean
Subject	<input type="text" value="cisco.com"/>
Validity	2020-11-24 00:00:00 UTC - 2021-11-23 23:59:59 UTC

tus ▾ Integrations ▾ Support ▾

✔ Threat Grid Connection test successful!

2.AMP

AMP for Endpoints 🔔 ? armando garcia ▾

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

### File Analysis

Search by SHA-256, File name, IP, Keywords...

There are no File Analyses to view

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。

File has been uploaded for analysis

### File Analysis

Search by SHA-256, File name, IP, Keywords... Submit File

There are no File Analyses to view

### File Analysis

Search by SHA-256, File name, IP, Keywords... Submit File

glogg.exe ( e309efdd...0c2c3d25 )	2021-01-31 06:16:55 UTC	Report 24
-----------------------------------	-------------------------	-----------

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

## File Analysis

Search by SHA-256, File name, IP, Keywords...		Submit File	
▶ xca.exe ( 63019d7c...a24c6c44 )	2021-01-31 08:16:38 UTC	Report	30
▶ WinRAR.exe ( 9066f0bc...f79d741e )	2021-01-31 06:17:05 UTC	Report	80
▶ glogg.exe ( e309efdd...0c2c3d25 )	2021-01-31 06:16:55 UTC	Report	24
▼ malware3-8d3bbc795.exe ( 8d3bbc79...5aacc995 )	2021-01-31 06:16:50 UTC	Report	100
Fingerprint (SHA-256)	8d3bbc79...5aacc995		
File name	malware3-8d3bbc795.exe		
Threat Score	100		
	Name	Score	

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 $\geq 95$ 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 $\geq 95$ 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 $\geq 95$ 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 $\geq 95$ 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": "W32.80388C7958-100.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。

Connect Threat Grid Appliance to AMP for Endpoints Appliance

#### Threat Grid Connection test failed.

- Threat Grid host is invalid.
- Threat Grid SSL Certificate could not be tested.
- Threat Grid API key could not be tested.

整合中的網路級別有問題。

建議的步驟：

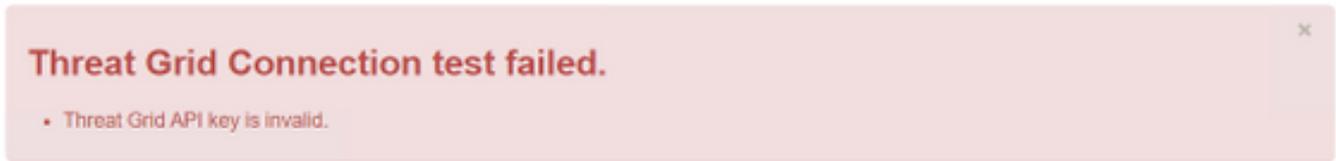
- 確認AMP Private Cloud裝置控制檯介面可以訪問Threat Grid裝置清潔介面。
- 確認AMP私有雲裝置可以解析Threat Grid裝置清理介面的FQDN。
- 確認AMP私有雲裝置和Threat Grid裝置的網路路徑中沒有過濾裝置。

## 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。

Connect Threat Grid Appliance to AMP for Endpoints Appliance



### 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。

## API

API Key	*****
Disable API Key ?	<input type="radio"/> True <input checked="" type="radio"/> False <input type="radio"/> Unset
Can Download Sample Content Via API ?	<input type="radio"/> True <input checked="" type="radio"/> False <input type="radio"/> 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      |
+-----+-----+-----+
| mirtlif: [REDACTED] | 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 $\geq 95$ ，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 $\geq 95$ 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。

**Step 2: Threat Grid Portal Setup**

- Go to the Threat Grid Appliance Portal.
- Navigate to the [Manage AMP for Endpoints Integration](#) page on the Threat Grid appliance.
- Add the Service URL, User, and Password from the section below.

Details	
Service URL	https://dupdateamp3.argarci2-lab.com/
User	disposition_update_user
Password	<input type="password" value="ew236[REDACTED]xJYfPK"/> <input type="button" value="Change Password"/>

Threat Grid裝置控制檯門戶。

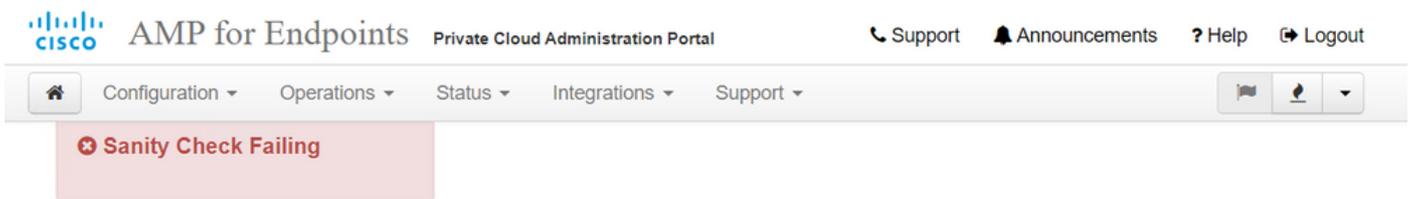
### Disposition Update Syndication Service

Service URL	User	Password	Action(s)
<div style="border: 2px solid black; width: 100%; height: 100%;"></div>	disposition_update_user	.....	<a href="#">Edit</a> <a href="#">Remove</a>
	disposition_update_user	.....	<a href="#">Edit</a> <a href="#">Remove</a>
	disposition_update_user	.....	<a href="#">Edit</a> <a href="#">Remove</a>
	disposition_update_user	.....	<a href="#">Edit</a> <a href="#">Remove</a>
	disposition_update_user	.....	<a href="#">Edit</a> <a href="#">Remove</a>
	disposition_update_user	.....	<a href="#">Edit</a> <a href="#">Remove</a>
<input type="text" value="https://dupdateamp3.argarci2-lat"/>	<input type="text" value="disposition_update_user"/>	<input type="text" value="ew236[redacted]xJYfPK"/>	<a href="#">Save</a> <a href="#">Cancel</a>
<input type="text" value=""/>	disposition_update_user	.....	<a href="#">Edit</a> <a href="#">Remove</a>

- 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。




 AMP for Endpoints
 [Private Cloud Administration Portal](#)
[Support](#)
[Announcements](#)
[Help](#)
[Logout](#)

[Home](#)
[Configuration](#)
[Operations](#)
[Status](#)
[Integrations](#)
[Support](#)

❌ **Sanity Check Failing**

Certificate Authorities are used by your Private Cloud device to verify SSL certificates and connections.

[Add Certificate Authority](#)

Certificate <span style="float: right;">(click to collapse)</span>			
Issuer	rootca_vpc		<a href="#">Download</a>  <a href="#">Delete</a>
Subject	rootca_vpc		
Validity	2020-11-15 00:00:00 UTC	- 2025-11-14 23:59:59 UTC	
Certificate <span style="float: right;">(click to collapse)</span>			
Issuer	rootca_vpc		<a href="#">Download</a>  <a href="#">Delete</a>
Subject	subca-dus		
Validity	2020-12-05 12:01:00 UTC	- 2023-12-05 12:01:00 UTC	

Configuration ☰

Authentication

**CA Certificates**

Change Password

Clustering

Date and Time

Email

Integrations

License

Network

Network Exit

NFS

Notifications

SSH

SSL

Syslog

### CA Certificates

Details	Validity
<b>Subject:</b> CN=rootca_vpc <b>Issuer:</b> CN=rootca_vpc <b>Fingerprint:</b> 66:BF:EB:63:36:9F:AC:E9:39:AD:76:A4:0E:5A:57:B1:45:B9:FD:A4:FD:63:7E:5A:11:FF:47:AA:CC:1E:FF:F2	2020-11-1 Valid for alr
Sub Issu Fing	-03-0 for ab
Sub Issu Fing	-03-2 for ab
Sub Issu Fing	-07-2 for ov
Sub Issu Fing	-03-0 for ab
<b>Subject:</b> CN=subca-dus <b>Issuer:</b> CN=rootca_vpc <b>Fingerprint:</b> 51:D5:74:9A:6C:44:4B:1A:E9:45:93:CB:B6:7C:3A:EB:7B:BB:BD:04:51:4D:79:8E:D4:23:35:92:C0:17:9D:5C	2020-12-0 Valid for alr

Add Certificate
Lookup Certificate

- >AMPAMPFQDNThreat GridAMPIPFQDN

<input type="text" value="https://dupdateamp3.argarci2-lab"/>	<input type="text" value="disposition_update_user"/>	<input type="text" value="ew236 [redacted] xJYfPK"/>	Ed
<input type="text" value="https://dupdateamp3.argarci2-lab"/>	<input type="text" value="disposition_update_user"/>	<input type="text" value="ew236 [redacted] xJYfPK"/>	Sav
<input type="text" value="https://dupdateamp3.argarci2-lab"/>	<input type="text" value="disposition_update_user"/>	<input type="text" value="ew236 [redacted] xJYfPK"/>	Ed

## 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」。

### Threat Grid Connection test failed.

- Threat Grid SSL Certificate is invalid.
- Threat Grid API key could not be tested.

### 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。

Threat Grid Configuration Details Edit

Hostname	<input type="text" value="cisco.com"/>
API Key	<input type="text" value="....."/>
<b>Threat Grid SSL Certificate</b>	
Issuer	subca_tga_clean
Subject	<input type="text" value="cisco.com"/>
Validity	2020-11-24 00:00:00 UTC - 2021-11-23 23:59:59 UTC

↔ Test Connection

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。

Threat Grid Appliance

Home
Configuration
Status
Operations
Support

**Configuration** ☰

Authentication

CA Certificates

Change Password

Clustering

Date and Time

Email

Integrations

License

Network

Network Exit

NFS

Notifications

SSH

**SSL**

Syslog

### Upload SSL certificate for PANDEM

Certificate (PEM)

```
-----BEGIN CERTIFICATE-----
hvcNAQELBQADggEBAKXz8oIDWacWY5V0XSHWrQIMULAMNAE8OZIXNkuByG6vvhj
P
JkgjjU9xKrke5LCr+trWnr+qjZlc4ecVCm8FXBWUtr8BjHcimbHUBZIVLYp6WDxO

HMS37fv44R9Cir4pjUz0bc61HS4wo5PAfUyjPtO1Dy0dHia4zE3pH4X3D9rzQYYd
Cl6KJpevCJzFyoQW3ahTZoxr4F11I5wO3XcH41Q=
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
wZfa8sZJp30zivJRtvBioPnwmPpNZzhqIW3cC90ASaRSXeU+4c+HmUknahEHJNn8
lJbkA4UJQgWgeD4QK0j8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqIXsBKDCHjYo
g+H0Nxldl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFTbHIZO

/8E/D+jd18zhA3aWNXADf8b9xjlRE3241FAfJf73a59q27y7d96tCa1PFaMOiXGc
nY2D9lwNsnl5uk11HL2SojLtVx8BYqw98w0uuBomqZZVNprSparsyw==
-----END RSA PRIVATE KEY-----
```

*public key derived from private key does not match*

Add Certificate
Cancel

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。

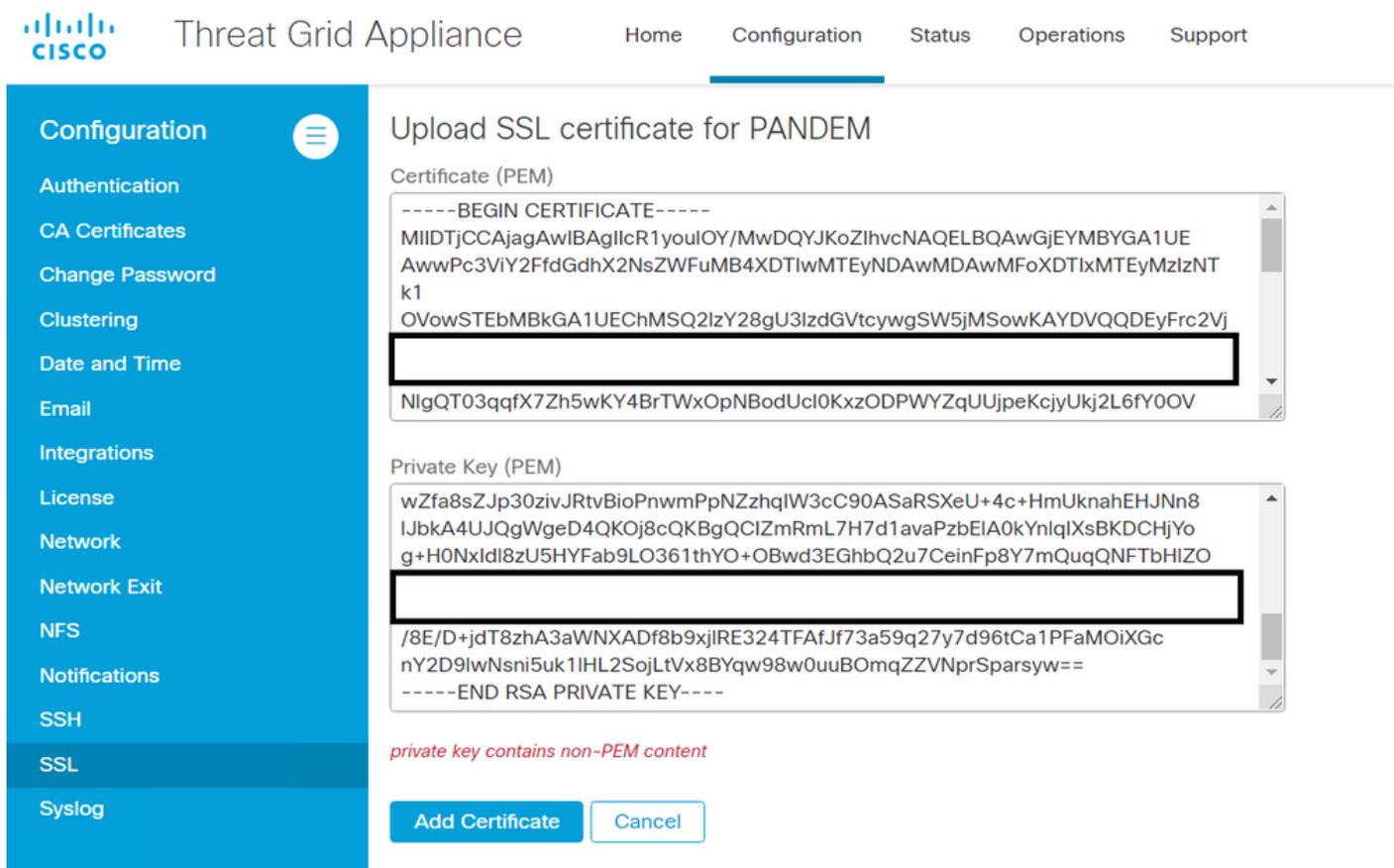
```
openssl x509 -noout -modulus -in
```

```
$ 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。

```

$ cat wrong-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYwggSiAgEAAoIBAQCvfIytwkf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNIHUoHFNSLkoo0H0ubkDtGo/PW4fE
/JNGbMIU/d1DDuzxfgGze0viztT90rpCbZyQP2r+sGxa0KM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTicI2q/vH/i0WeIgAv10aGuBCOeg      <-----
NwOgPyY3XI8g7l
WXZW1XhNAgMBA
Uh4/Vrdg1TYXfi
fINIJto/x0azh
mdhzCQSTBfYbM
JqSwA5BEgqeH3
WtVHzbVDqJ+rb
SU+TvjNWQGcUs:
4HA6/VsM10NHKT4EhvSks
tU9huSCL7t4BF7VpSeKXM
s7k0sCwmhKUaMacTYAnrg
47ttvLvX3zweLCEXsDXK6
R4M7HiocsbkLjijScTFYQ
rgd4kJ6ddAaSjQS7sJxaf
3gQDePpxacxGRZLXfja3s
a8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2xOCy51K5KsfDPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HFVnsq9+xbCU1fRlPxeCS
Cbcf1DYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBgHfn/ZziDtrkSzJSM6fVGPPhJHCuTI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTY1GD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdfQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofm1SMwT1MmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----

```

- 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-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCvfIytwfk9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/Pw4fE
/JNGbMIU/d1DDuzxfGze0viztT90rpCbZyQP2r+sGxa0KM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTicI2q/vH/i0WeIgAv10aGuBC0egVDU
NwOgPyY3XI8g7H 4HA6/VsM10NHKT4EhvSks
WXZW1XhNAgMBAAtU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXFBs7k0sCwmhKUaMAcTYAnrg
fINIJto/x0azhe47ttvLvX3zweLCEXsDXK6
mdhzCQSTBfYbM4R4M7HiocsbkLjijScTFYQ
JqSwA5BEgqeH3ahgd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb9BgQDePpxacxGRZLXfja3s
SU+TvjNWQGcUsXa8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2x0Cy51K5KsfdPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFp0AFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRlPxeCS
Cbcf1DYBwaMn8Ywp9PfZKpgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBGHFn/ZziDtrkSzJSN6fVGPhJHCutI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrlRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXzl0Mn+A0
SxuwKWoARshnMsDvsTYwofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHiErbltdVumF42Tax+fucqUrdB3LZo6FjagvPy+LBJA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+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。

Configuration

- Authentication
- CA Certificates
- Change Password
- Clustering
- Date and Time
- Email
- Integrations
- License
- Network
- Network Exit
- NFS
- Notifications
- SSH
- SSL**
- Syslog

### Upload SSL certificate for PANDEM

Certificate (PEM)

```
AN
BgkqhkiG9w0BAQsFAAOCAQEAsCQ1iOkPkLj6A1R94eueZ64zCYGuf8wg0z2S9Kle
epjqQobaJadl3WTh7LMHuxHZP02YZJIO/OjUQ/8uLk1sG7rVE5ROe/Ev9OvjL5nF
[Redacted]
wbTboJukREZOyiBoQDPcSWHqe8j3FEtJlf9yfv2bthOFQQ+Lf3BU4ZPiXPVEtuUL
7FIP0kjC/33s5ZWpC8OzCmdPvFgx//JbpWr1gllYVs1uYg==
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAACAQEAucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY
EE9N6qn1+2YecCmOAA01sTqTQaHVHJdCsczgz1mGalFI6Xinl8lJl9i+n2NDlcNr
XBVPvCUs5fnH2cZwKGTen/NDJhnyC5Dlb17RLy7Y+wxhMiyRCHH3aZ3l0Mpl1k4X
[Redacted]
cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAoIBAFrH8EHRsvNTXY5v
yCSwXQtfalYpjXGGqdduaPzdlrICrCGWbbgimKeYQByGTU9v7vXAx2EAh57Izvb2
```

cannot generate public key from private key

Add Certificate Cancel

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。

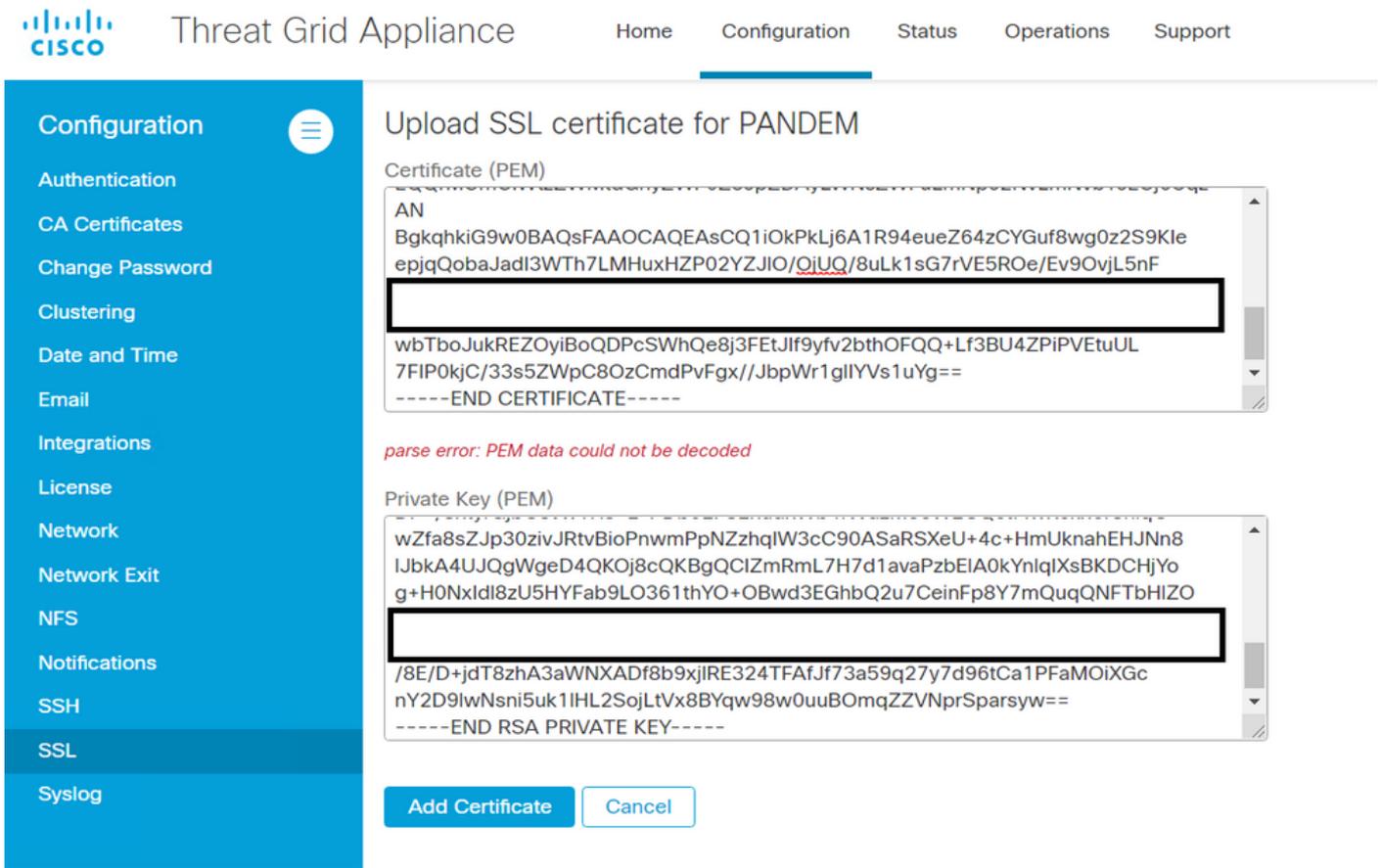
```
$ openssl rsa -in wrong-private-key.key -pubout
unable to load Private Key
140195161523520:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

$ openssl rsa -in correct-private-key.key -pubout
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr3yMrcJH/VCH0Q5bivT0
2yrw60oYJ/Pwnp/cFxFaYATWoZRYmb8GW/+RS/iNa8vz9FiiTII0YS0dmNKKIEL
Lg080/TKGusV2CyqtT+UESFerUEAzYh1KBxTUi5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBswjijNHNwBICv6WA02gr/xj+qxpB3
P1YjNTU7l1SFnSHC4E1Fzg3hy40yHCNqv7x/4jlniIAL9dGhrgQjnofQ1DcDoD8m
N1yPI0x3C0lWeVForZmx+Dg6l+J4uIjytkVceBw0v1bDNdDRyk+BIb0pLF12VtV4
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。



The screenshot shows the 'Upload SSL certificate for PANDEM' page in the Threat Grid Appliance configuration interface. The 'Certificate (PEM)' field contains a corrupted PEM certificate with a red error message: 'parse error: PEM data could not be decoded'. The 'Private Key (PEM)' field also contains a corrupted private key. The interface includes a navigation menu on the left with 'SSL' selected, and buttons for 'Add Certificate' and 'Cancel' at the bottom.

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。

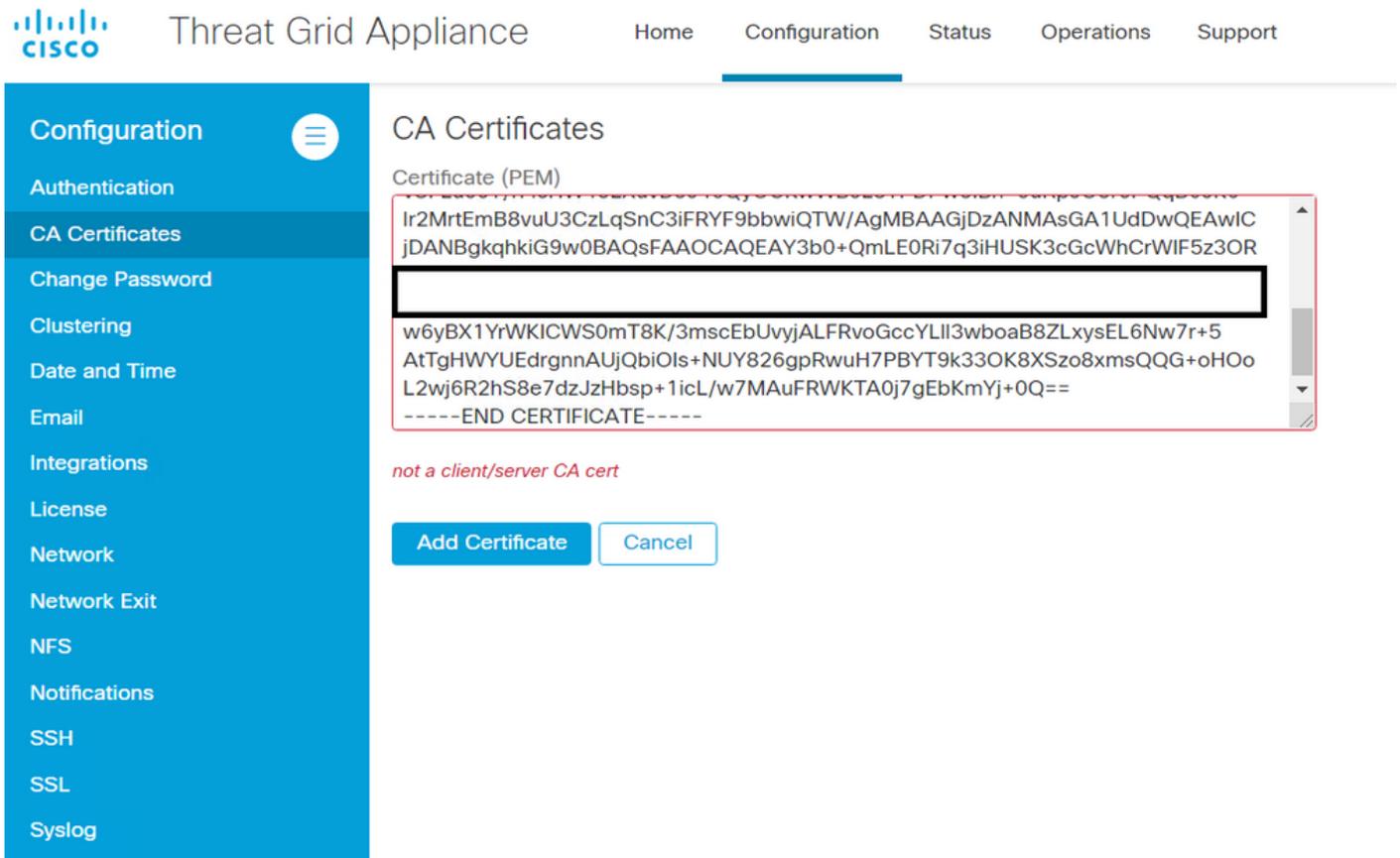
```
$ openssl x509 -in wrong-certificate.cert -text -noout
unable to load certificate
140159319831872:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:
```

## 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。

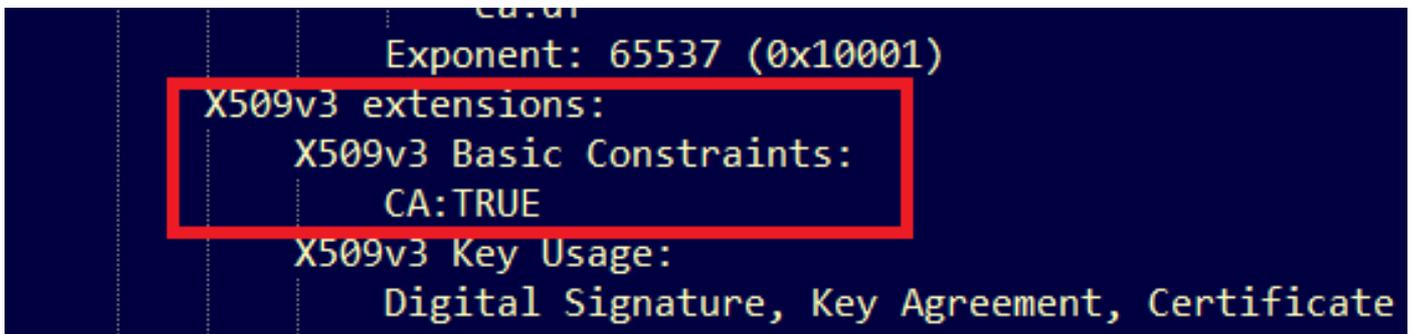
如果基本約束擴展值設定為CA，請用OpenSSL工具確認：CA憑證中為True。

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](#)