AMP Virtual Private Cloud 및 Threat Grid 어플라이언스의 통합

목차

이 문서에서는 AMP(Advanced Malware Protection) Virtual Private Cloud 및 Threat Grid Appliance의 통합을 완료하는 절차에 대해 설명합니다.이 문서에서는 통합 프로세스와 관련된 문제에 대한 트러블슈팅 단계를 제공합니다.

기고자: Armando Garcia, Cisco TAC 엔지니어

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AMP Virtual Private Cloud 작업 및 운영
- Threat Grid 어플라이언스 작업 및 운영

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

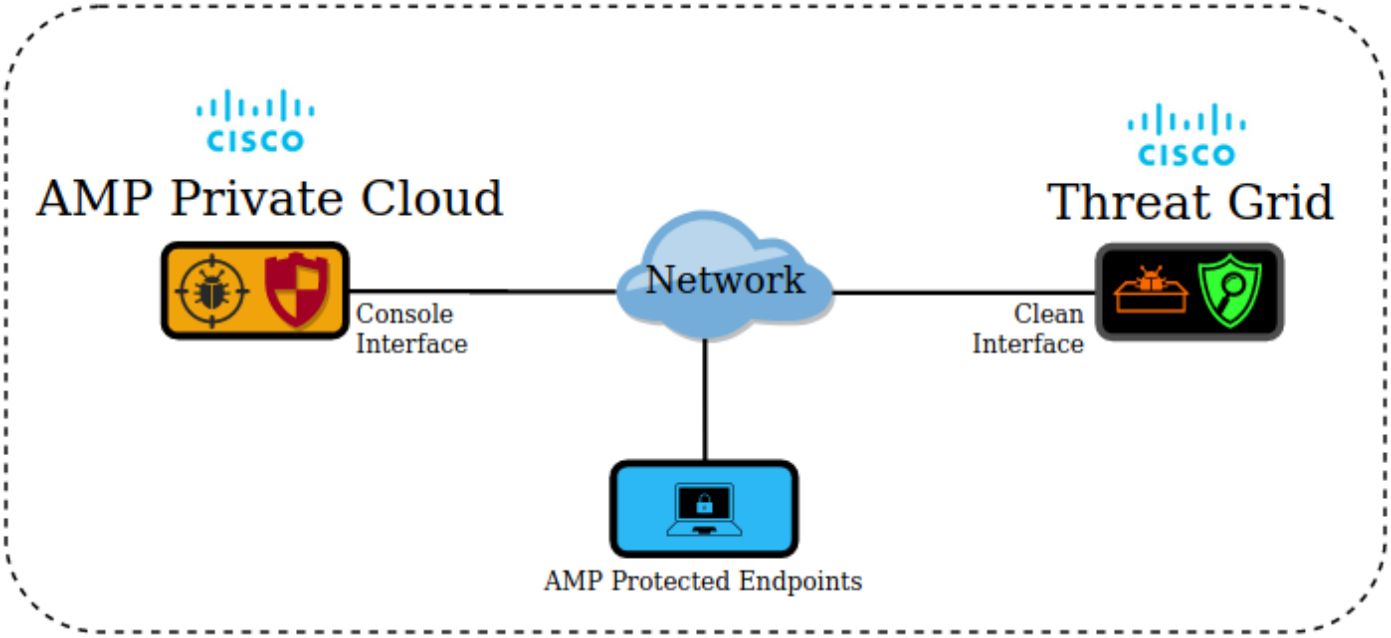
- AMP 프라이빗 클라우드 3.2.0
- Threat Grid Appliance 2.12.0.1

  참고:이 설명서는 어플라이언스 또는 가상 버전의 Threat Grid 어플라이언스 및 AMP Private Cloud 디바이스에 유효합니다.

. () . .

배경 정보

통합의 아키텍처



통합에 대한 기본 정보

- Threat Grid 어플라이언스는 AMP Private Cloud 디바이스에서 제출한 샘플을 분석합니다.
- 샘플은 수동으로 제출하거나 자동으로 Threat Grid 어플라이언스에 제출할 수 있습니다.
- AMP Private Cloud 디바이스에서는 자동 분석이 기본적으로 활성화되지 않습니다.
- Threat Grid 어플라이언스는 AMP Private Cloud 디바이스에 샘플 분석에서 얻은 보고서 및 점수를 제공합니다.
- Threat Grid 어플라이언스는 AMP Private Cloud 디바이스에 95점보다 크거나 같은 샘플에 대해 알림(포킹)합니다.
- 분석의 점수가 95보다 크거나 같으면 AMP 데이터베이스의 샘플에 악성 속성이 표시됩니다.

- 회귀적 탐지는 AMP Private Cloud에서 점수가 95보다 크거나 같은 샘플에 적용됩니다.

절차

1단계. Threat Grid Appliance를 설정 및 구성합니다(아직 통합되지 않음). 필요한 경우 업데이트를 확인하고 설치합니다.

2단계. AMP for Endpoints Private Cloud(아직 통합되지 않음)를 설정하고 구성합니다.

3단계. Threat Grid 관리 UI에서 Configuration(컨피그레이션) 탭**을** 선택하고 **SSL을** 선택합니다.

4단계. PANDEM(Clean interface)에 대한 새 SSL 인증서를 생성하거나 업로드합니다.

SSL 인증서 재생성

정상 인터페이스의 호스트 이름이 정상 인터페이스에 대해 현재 어플라이언스에 설치된 인증서의 SAN(Subject Alternative Name)과 일치하지 않을 경우 새 자체 서명 인증서를 생성할 수 있습니다 .어플라이언스는 인터페이스에 대한 새 인증서를 생성하여 자체 서명 인증서의 SAN 필드에 현재 인터페이스 호스트 이름을 구성합니다.

4.1단계. Actions(작업) 열에서 **(...)를** 선택하고 팝업 메뉴에서 Generate New Certificate(**새 인증서 생성)를 선택합니다.**

4.2단계. Threat Grid UI에서 **Operations**를 선택하고 다음 화면에서 Activate를 **선택하고 Reconfigure**를 **선택합니다**.

> **참고**: 이 생성된 인증서는 자체 서명됩니다.

SSL 인증서 업로드

Threat Grid 어플라이언스 정상 인터페이스에 대해 이미 생성된 인증서가 있는 경우 이 인증서를 어플라이언스에 업로드할 수 있습니다.

4.1단계. Actions(작업) 열에서 **(...)를** 선택하고 팝업 메뉴에서 Upload New Certificate(**새 인증서 업로드)를 선택합니다**.

4.2단계. 인증서 및 해당 개인 키를 화면에 나타나는 텍스트 상자에 PEM 형식으로 복사하고 **Add Certificate**(인증서 추가)를 선택합니다.

4.3단계. Threat Grid UI에서 **Operations**를 선택하고 다음 화면에서 Activate를 **선택하고 Reconfigure**를 **선택합니다**.

5단계. AMP Private Cloud 디바이스 관리 UI에서 Integrations(통합)를 선택하고 **Threat Grid**를 선택합니다.

6단계. Threat Grid Configuration Details에서 Edit를 **선택합니다**.

7단계. Threat Grid 호스트 이름에 Threat Grid 어플라이언스의 정상 인터페이스의 FQDN을 입력합

니다.

8단계. Threat Grid SSL Certificate에서 Threat Grid 어플라이언스의 정상 인터페이스의 인증서를 추가합니다.(아래 참고 사항 참조)

Threat Grid 어플라이언스 정상 인터페이스의 인증서가 자체 서명되었습니다.

8.1단계. Threat Grid 관리 UI에서 Configuration(컨피그레이션)을 선택하고 SSL을 **선택합니다**.

8.2단계. Actions(작업) 열에서 **(...)를** 선택하고 팝업 메뉴에서 Download Certificate(인증서 **다운로드)를** 선택합니다.

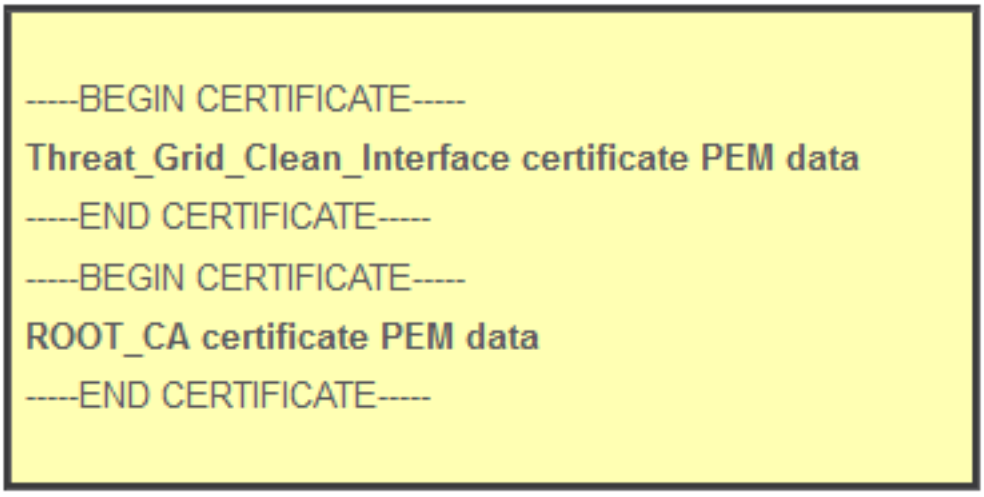
8.3단계. Threat Grid 통합 페이지에서 다운로드한 파일을 AMP Virtual Private 디바이스에 추가합니다.

Threat Grid 어플라이언스 정상 인터페이스의 인증서는 기업 CA(Certificate Authority)에 의해 서명됩니다.

8.1단계. 텍스트 파일에 Threat Grid 어플라이언스 정상 인터페이스의 인증서 및 전체 CA 인증서 체인을 복사합니다.

참고:텍스트 파일의 인증서는 PEM 형식이어야 합니다.

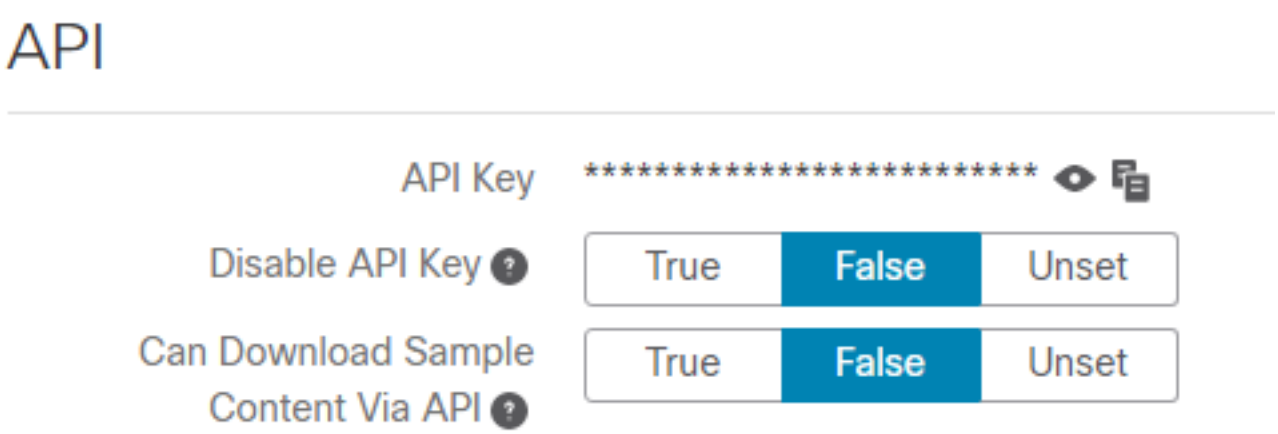
전체 인증서 체인이 다음과 같은 경우:ROOT_CA 인증서 > Threat_Grid_Clean_Interface 인증서;이미지에 표시된 대로 텍스트 파일을 만들어야 합니다.



전체 인증서 체인이 다음과 같은 경우:ROOT_CA 인증서 > Sub_CA Certificate > Threat_Grid_Clean_Interface certificate;이미지에 표시된 대로 텍스트 파일을 만들어야 합니다.

```
-----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-----
```

9. Threat Grid API Key Threat Grid API .



참고: Threat Grid 사용자의 계정 설정에서 Disable **API Key** 매개 변수가 True로 설정되지 않았는지 확인합니다.

10단계. 모든 변경 사항이 완료되면 저장을 **선택합니다**.

11단계. AMP 가상 클라우드 디바이스에 재구성을 적용합니다.

12단계. AMP Private Cloud 디바이스 관리 UI에서 Integrations(통합)를 선택하고 **Threat Grid**를 선택합니다.

13단계. **세부 정보에서** Disposition Update Service URL, Disposition Update Service 사용자 및 Disposition Update Service 비밀번호의 값을 복사합니다.이 정보는 17단계에서 사용됩니다.

14단계. Threat Grid 관리 UI에서 Configuration(컨피그레이션)을 선택하고 **CA Certificates(CA 인증서)**를 선택합니다.

15단계. **Add Certificate(인증서 추가)를** 선택하고 AMP Private Cloud Disposition Update Service

인증서에 서명한 CA 인증서를 PEM 형식으로 복사합니다.

> **참고:**AMP Private Cloud Disposition 업데이트 인증서에 서명한 CA 인증서가 하위 CA인 경우 체인의 모든 CA가 **CA 인증서**에 업로드될 때까지 프로세스를 반복합니다.

16단계. Threat Grid 포털에서 Administration(관리)을 선택하고 Manage AMP Private Cloud Integration(AMP 프라이빗 클라우드 통합 관리)을 선택합니다.

17단계. 분류 갱신 신디케이션 서비스 페이지에 단계 13에서 수집된 정보를 입력합니다.

- 서비스 URL: AMP Private Cloud 디바이스의 Disposition Update Service의 FQDN입니다.
- 사용자: AMP Private Cloud 디바이스의 Disposition Update Service의 사용자.
- Password(비밀번호): AMP Private Cloud 디바이스의 Disposition Update Service에 대한 비밀번호입니다.

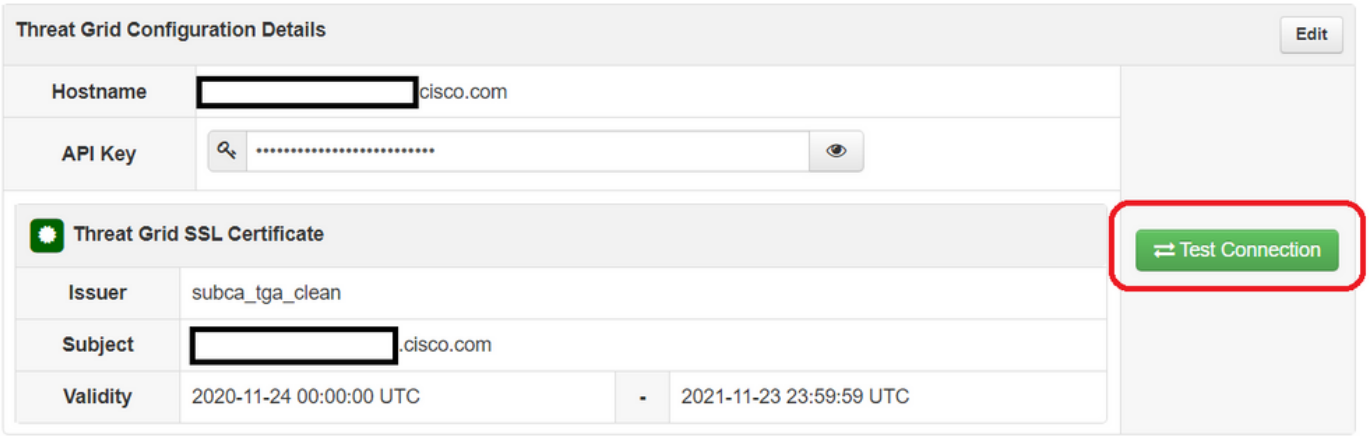
이 시점에서 모든 단계가 올바르게 적용된 경우 통합이 성공적으로 작동해야 합니다.

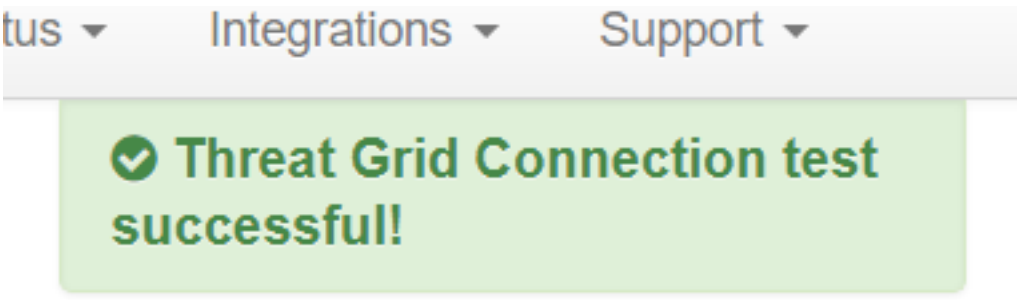
확인

Threat Grid .

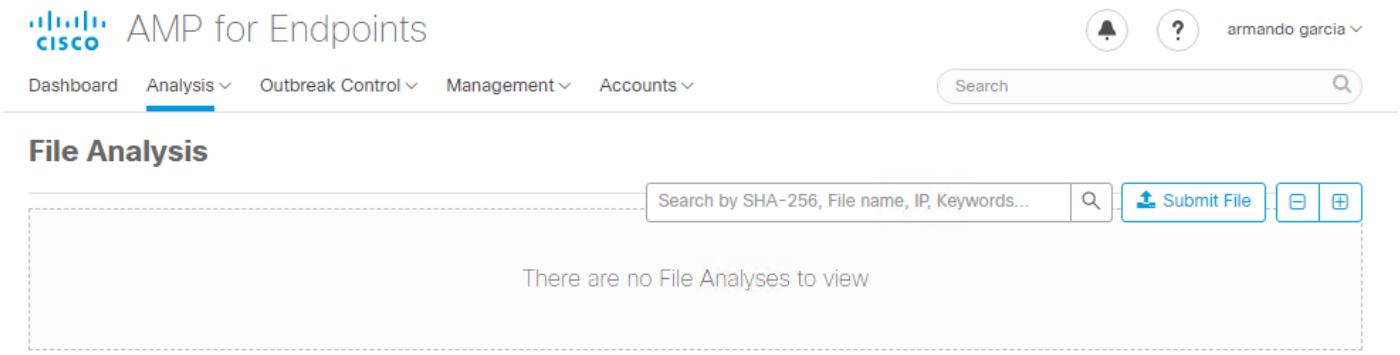
> **참고**: 1, 2, 3, 4단계만 프로덕션 환경에 적용하여 통합을 확인하는 것이 좋습니다.5단계는 통합에 대해 자세히 알아볼 수 있는 정보로 제공되며 프로덕션 환경에 적용하는 것은 권장되지 않습니다.

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

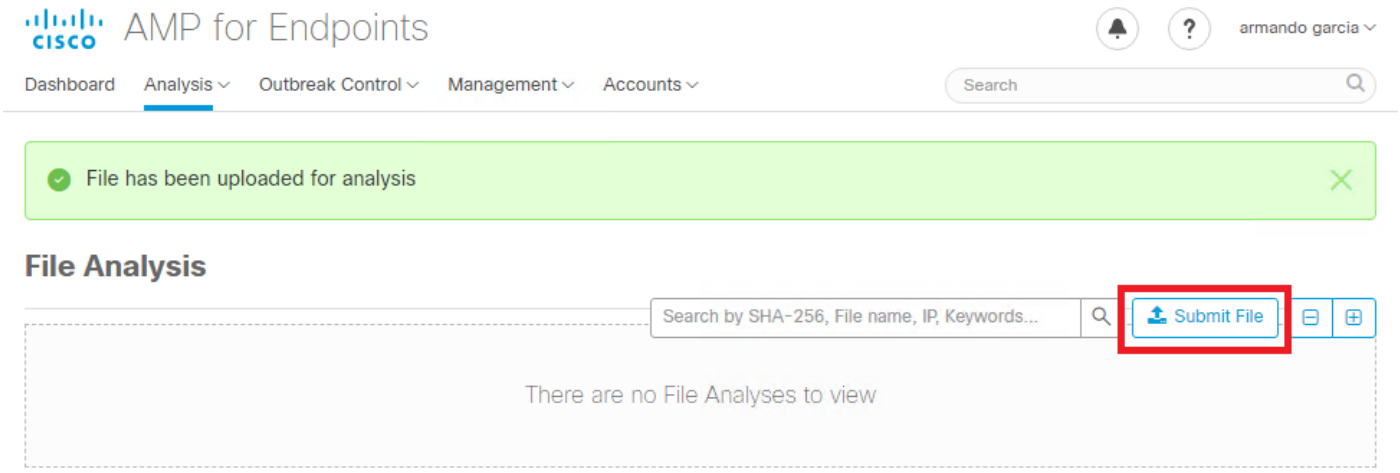


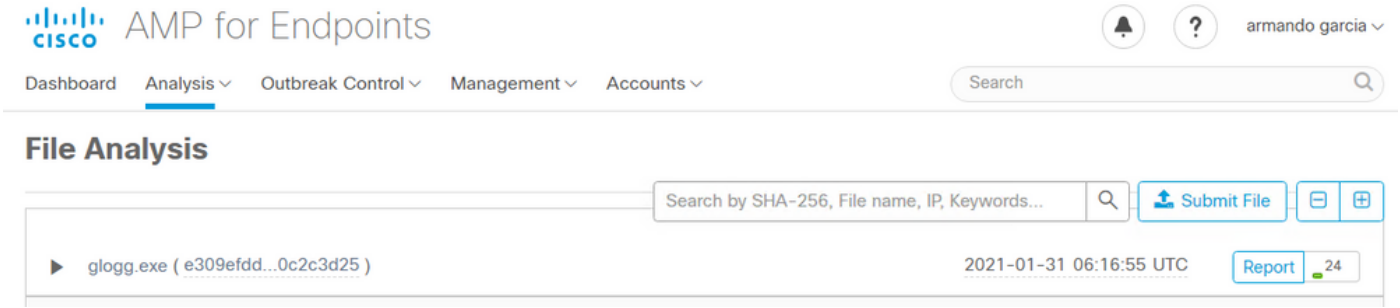


2. AMP Private Cloud File Analysis .



3단계. AMP Private Cloud 콘솔 **Analysis > File Analysis**에서 수동으로 제출된 파일이 Threat Grid 어플라이언스에서 인식되고 점수가 있는 보고서가 Threat Grid 어플라이언스에서 반환되는지 확인합니다.





4단계. AMP Private Cloud 디바이스의 Disposition Update Service 인증서에 서명한 CA가 Threat Grid 어플라이언스의 **Certificate Authorities**에 설치되어 있는지 **확인합니다**.

5단계. Threat Grid 어플라이언스에서 점수 >=95로 표시한 샘플이 보고서 후 악성으로 분류되고 샘플 점수가 Threat Grid Appliance에서 제공되는지 확인합니다.

참고:샘플 보고서를 성공적으로 수신하고 AMP Private Cloud 콘솔의 **File Analysis(파일 분석)** 탭에서 95점 이상의 샘플 점수를 받았을 경우 AMP 데이터베이스에서 파일 속성이 변경되었음을 의미하지는 않습니다.AMP Private Cloud 디바이스의 Disposition Update Service 인증

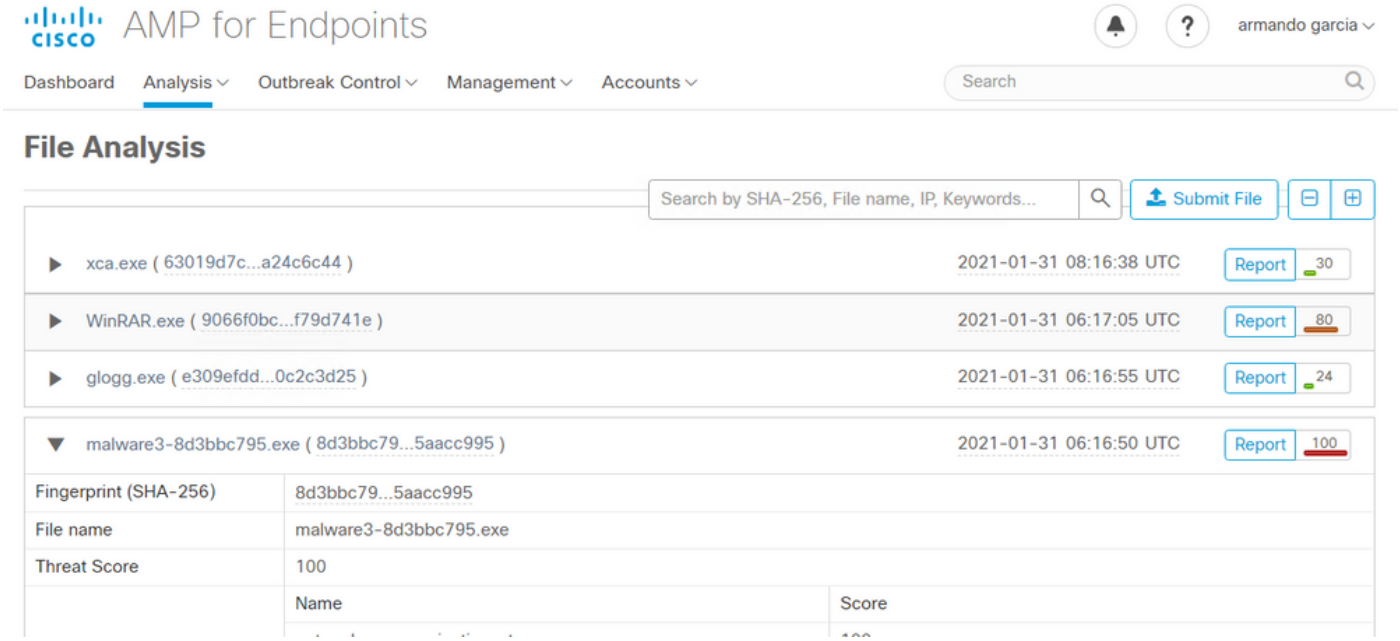
서에 서명한 CA가 **Certificate Authorities**의 Threat Grid 어플라이언스에 설치되지 않은 경우, AMP Private Cloud 디바이스에서 보고서 및 점수를 받지만 Threat Grid 어플라이언스에서 수신되는 포인트는 없습니다.

경고: Threat Grid 어플라이언스가 95점 이상의 파일을 표시한 후 AMP 데이터베이스에서 샘플 처리 변경을 트리거하기 위한 다음 테스트가 완료되었습니다.이 테스트의 목적은 Threat Grid Appliance에서 샘플 점수 >=95를 제공할 때 AMP Private Cloud 디바이스의 내부 작업에 대한 정보를 제공하는 것이었습니다. 속성 변경 프로세스를 트리거하기 위해 Cisco 내부 makemalware.exe 애플리케이션으로 악성코드 모조 테스트 파일이 생성되었습니다.샘플 :malware3-419d23483.exeSHA256:8d3bbc795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5acc995

주의:프로덕션 환경에서 악성코드 모방 테스트 파일을 폭발시키지 않는 것이 좋습니다.

AMP Private Cloud 데이터베이스의 샘플 처리 업데이트 확인

AMP Private Cloud **File Analysis** Threat Grid . Threat Grid 100 AMP Private Cloud . >=95 AMP Private Cloud .Threat Grid >=95 AMP poke .



다음과 같은 경우:

- 통합이 완료되었습니다.
- 샘플 보고서 및 점수는 파일을 수동으로 제출한 후 **파일 분석**에서 확인됩니다.

그 다음:

- Threat Grid 어플라이언스가 점수 >=95로 표시하는 각 샘플의 경우 AMP Private Cloud 디바이스의 /data/poked/poked.log 파일에 항목이 추가됩니다.
- /data/poked/poked.log은 Threat Grid 어플라이언스에서 첫 번째 >=95 샘플 점수를 제공한 후 AMP Private Cloud 디바이스에서 생성됩니다.
- AMP Private Cloud의 db_protect 데이터베이스에는 샘플에 대한 현재 속성이 포함됩니다.이 정보를 사용하여 Threat Grid 어플라이언스에서 점수를 제공한 후 샘플의 성향이 3인지 확인할

수 있습니다.

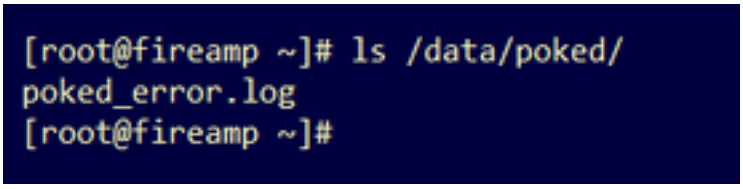
샘플 보고서 및 >=95 점수가 AMP Private Cloud 콘솔의 **File Analysis(파일 분석)**에서 인식되는 경우 다음 단계를 수행합니다.

1단계. SSH를 통해 AMP Private Cloud 디바이스에 로그인합니다.

2단계. 샘플에 대한 항목이 /data/poked/poked.log에 있는지 확인합니다.

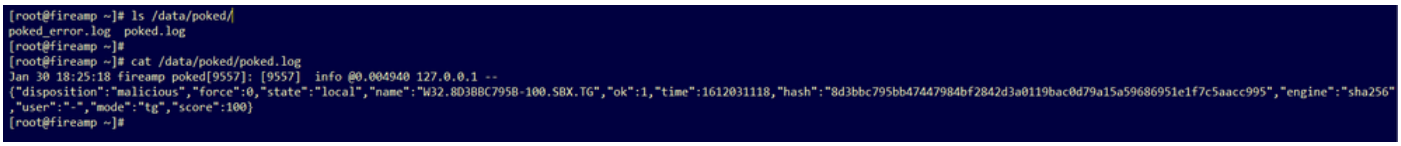
Threat Grid 어플라이언스에서 받은 적이 없는 AMP Private Cloud 디바이스에서 /data/focused/ 디렉토리를 나열하면 시스템에 focing.log 파일이 생성되지 않은 것으로 표시됩니다.

AMP Private Cloud 디바이스가 Threat Grid 어플라이언스에서 포크를 수신한 적이 없는 경우 /data/poked/poked.log 파일은 이미지에 표시된 대로 디렉토리에서 찾을 수 없습니다.



첫 번째 >=95 샘플 점수를 받은 후 /data/scucked/ 디렉터리를 나열하면 파일이 생성된 것입니다.

95점 이상의 첫 번째 샘플을 받은 후



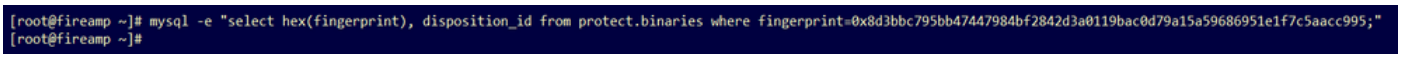
Threat Grid 어플라이언스에서 제공한 포크의 샘플 정보를 foke.log 파일 내에서 확인할 수 있습니다.

3단계. 샘플 SHA256과 함께 이 명령을 실행하여 AMP Private Cloud 디바이스의 데이터베이스에서 현재 성향을 검색합니다.

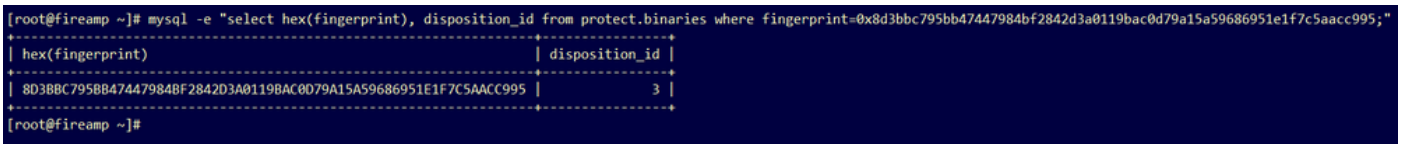
```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

예

샘플이 Threat Grid Appliance에 업로드되기 전에 샘플 처리를 가져오기 위한 데이터베이스 쿼리는 이미지에 표시된 것처럼 결과를 제공하지 않습니다.



Threat Grid 어플라이언스에서 보고서 및 점수를 받은 후 샘플 처리를 가져오기 위한 데이터베이스 쿼리에서는 3의 성향을 악성으로 간주하는 샘플을 보여줍니다.



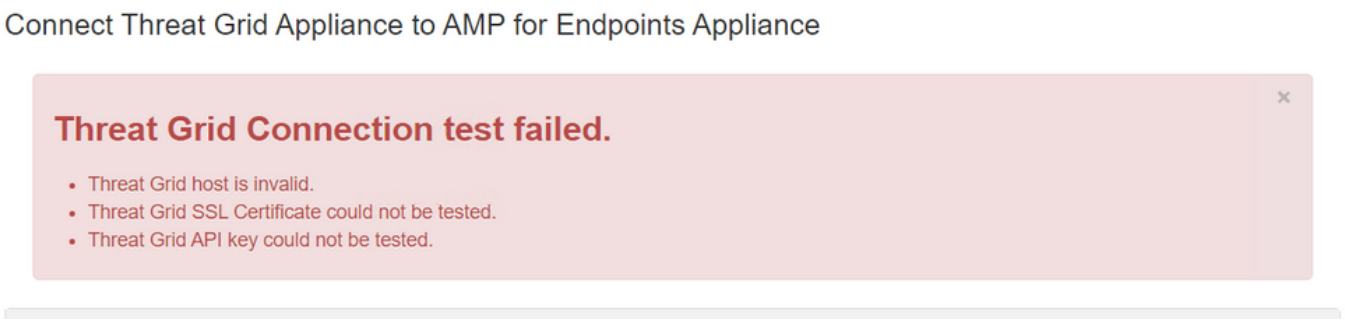
문제 해결

통합 프로세스에서 가능한 문제를 인지할 수 있습니다.문서의 이 부분에서는 가장 일반적인 몇 가지 문제를 다룹니다.

AMP Private Cloud 디바이스의 경고: 호스트가 잘못됨, 인증서가 테스트되지 않음, API 키가 테스트되지 않음

증상

경고 메시지:Threat Grid 호스트가 잘못되었거나, Threat Grid SSL 인증서를 테스트할 수 없습니다. Threat Grid API 키를 테스트할 수 없습니다. Integrations(통합) **> Threat Grid**에서 **Test Connection(연결 테스트)** 버튼을 선택한 후 AMP Private Cloud 디바이스에서 **수신됩니다**.



통합의 네트워크 레벨에서 문제가 있습니다.

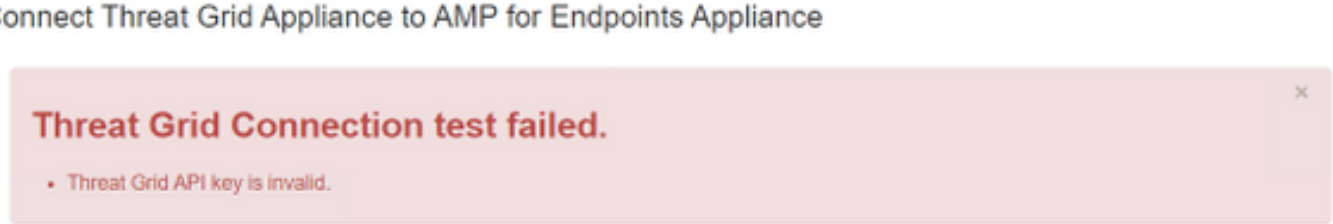
권장 단계:

- AMP Private Cloud 디바이스 콘솔 인터페이스가 Threat Grid 어플라이언스 정상 인터페이스에 도달할 수 있는지 확인합니다.
- AMP Private Cloud 디바이스가 Threat Grid 어플라이언스 정상 인터페이스의 FQDN을 확인할 수 있는지 확인합니다.
- AMP Private Cloud 디바이스 및 Threat Grid 어플라이언스의 네트워크 경로에 필터링 디바이스가 없는지 확인합니다.

Threat Grid API AMP Private Cloud

증상

경고 메시지:Threat Grid Connection 테스트에 실패했습니다. Threat Grid API는 유효하지 않으며, Integrations(통합) **> Threat Grid**에서 **Test Connection(연결 테스트)** 버튼을 선택한 후 AMP Private Cloud 디바이스**에서 수신됩니다**.

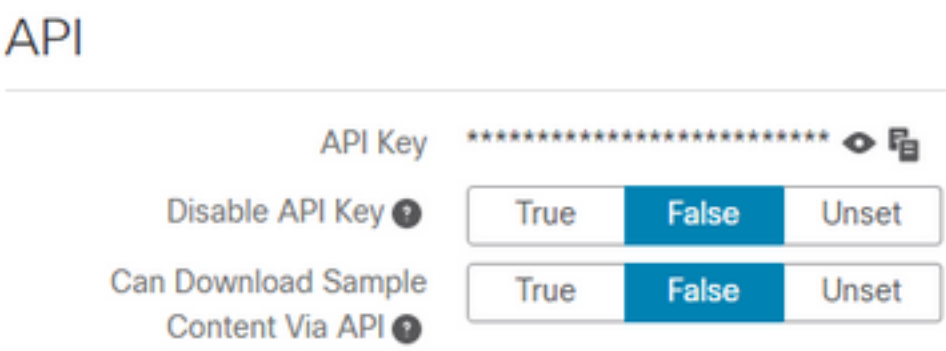


AMP Threat Grid API .

권장 단계:

- Threat Grid 어플라이언스 사용자의 계정 설정에서 Disable API Key 매개 변수가 True로 설정

되지 않았습니다.
- Disable API Key 매개 변수는 다음으로 설정해야 합니다.False 또는 Unset입니다.



- AMP Private Cloud 관리 포털 **Integrations > Threat Grid**에 구성된 Threat Grid API 키가 Threat Grid 어플라이언스의 사용자 설정에 있는 동일한 API 키인지 확인합니다.
- 올바른 Threat Grid API 키가 AMP Private Cloud 디바이스 데이터베이스에 저장되었는지 확인합니다.

AMP Private Cloud 디바이스 명령행에서 AMP 디바이스에 구성된 현재 Threat Grid API 키를 확인할 수 있습니다.SSH를 통해 AMP Private Cloud 디바이스에 로그인하고 이 명령을 실행하여 현재 Threat Grid 사용자 API 키를 검색합니다.

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

Threat Grid 어플라이언스 API 키에 대한 AMP Private Cloud 디바이스 데이터베이스의 올바른 항목입니다.

```
[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 ~]#
```

Threat Grid 사용자 이름이 통합의 어떤 단계에서도 AMP Private Cloud 디바이스에 직접 구성되지 않았지만 Threat Grid API 키가 올바르게 적용된 경우 AMP 데이터베이스의 tg_login 매개 변수에 Threat Grid 사용자 이름이 인식됩니다.

Threat Grid API 키에 대한 AMP 데이터베이스의 잘못된 항목입니다.

```
[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_login NULL. AMP Private Cloud Threat Grid Threat Grid .

샘플 점수가 95보다 높지만, 샘플 성향에는 변화가 없습니다.

증상

샘플이 제출되면 Threat Grid 어플라이언스에서 보고서 및 >=95개의 샘플 점수가 성공적으로 수신되지만 AMP Private Cloud 디바이스에서는 샘플 속성이 변경되지 않습니다.

권장 단계:

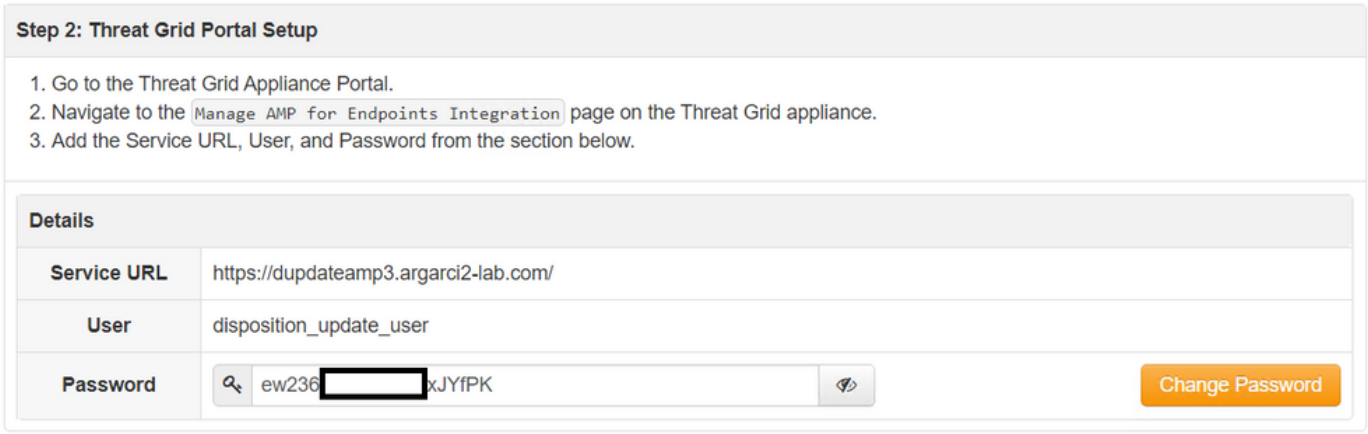
- 샘플 SHA256이 /data/poked/poked.log의 콘텐츠에 있는지 AMP Private Cloud 디바이스에서 확인합니다.

SHA256이 /data/poked/poked.log에 있는 경우 이 명령을 실행하여 AMP 데이터베이스의 현재 샘플 처리를 확인합니다.

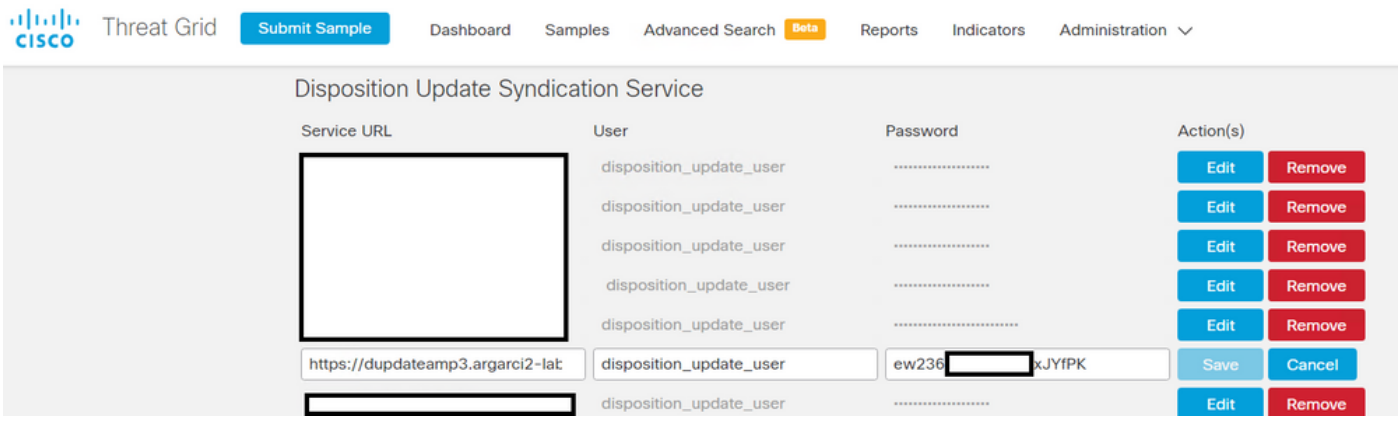
```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

- Administration(관리) > Manage AMP Private Cloud Integration(AMP 프라이빗 클라우드 통합 관리)의 Threat Grid 어플라이언스 관리 포털에 올바른 AMP Private Cloud 통합 비밀번호**가 추가되었는지 확인합니다**.

AMP Private Cloud 관리 포털



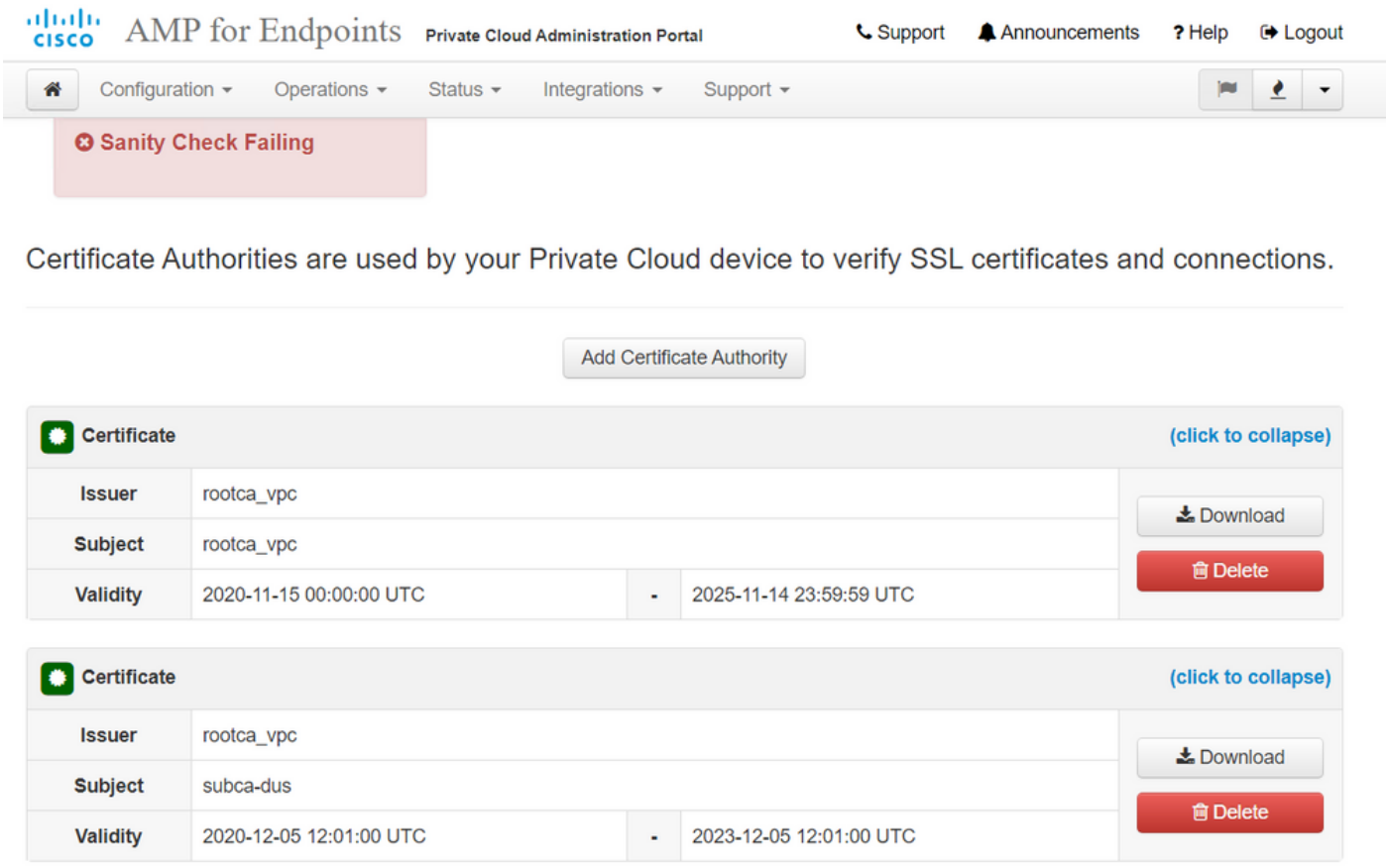
Threat Grid 어플라이언스 콘솔 포털입니다.



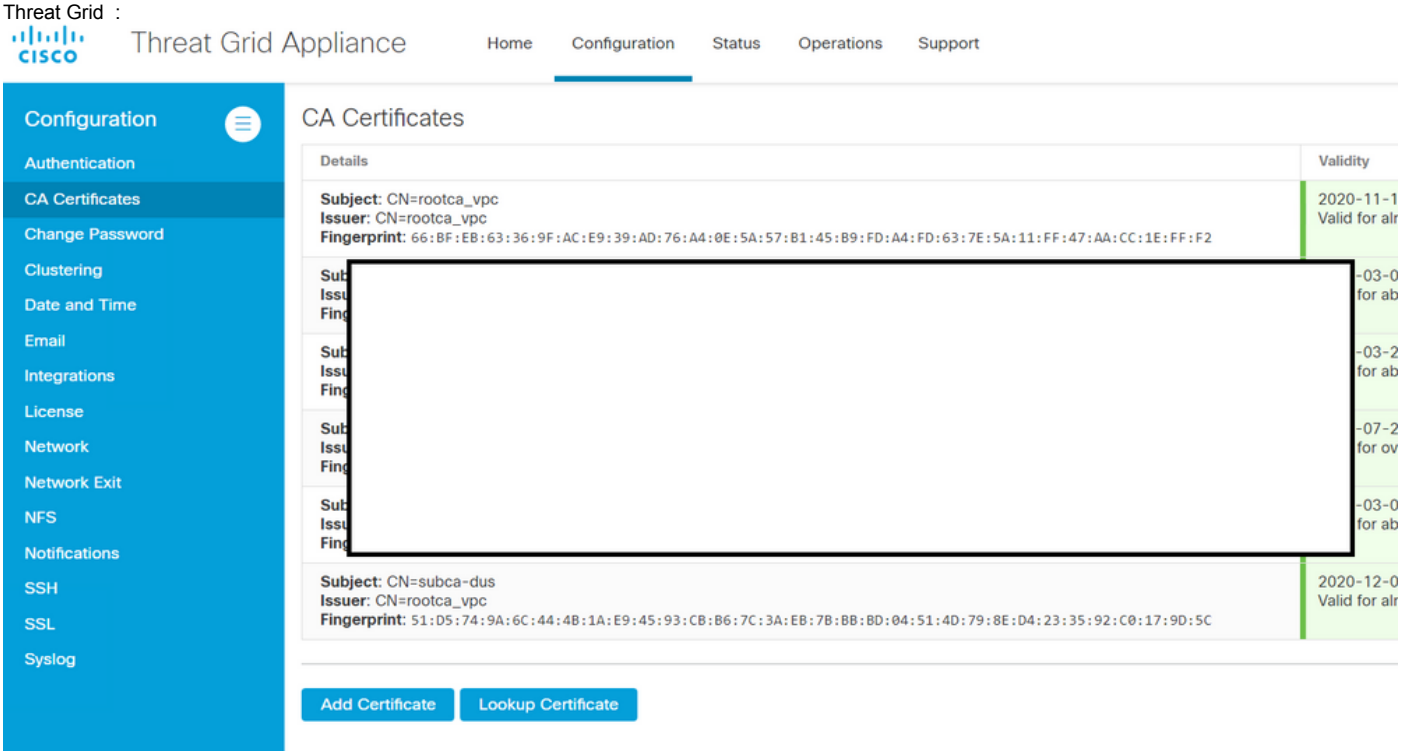
- AMP Private Cloud 디바이스 속성 업데이트 서비스 인증서에 서명한 CA가 **CA 인증서**의 Threat Grid 어플라이언스 관리 포털에 설치되었는지 **확인합니다**.

아래 예에서 AMP Private Cloud 디바이스 속성 업데이트 서비스 인증서의 인증서 체인은 **Root_CA > Sub_CA > Disposition_Update_Service 인증서입니다**.따라서 RootCA 및 Sub_CA는 Threat Grid Appliance의 **CA 인증서**에 설치해야 합니다.

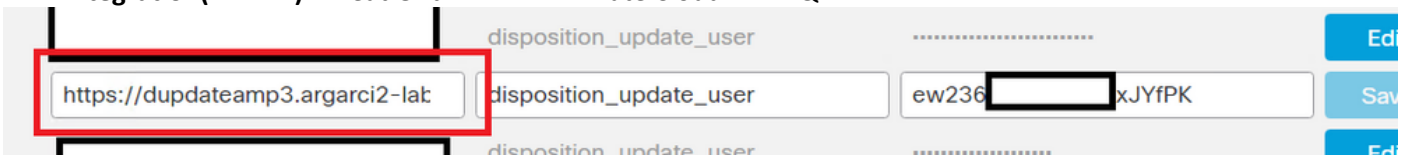
AMP Private Cloud 관리 포털의 인증 기관



Threat Grid :



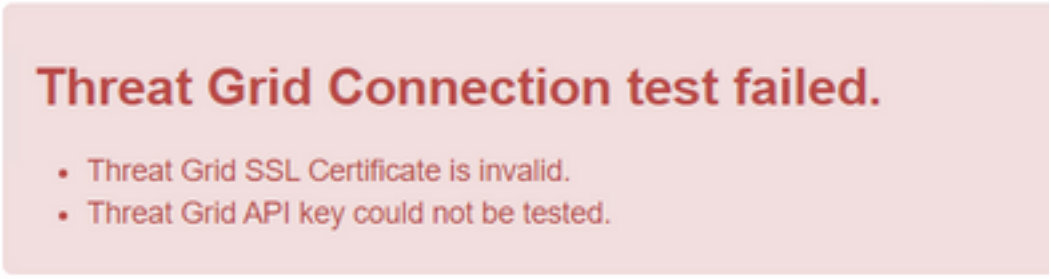
- AMP Private Cloud Disposition Update Service FQDN Administration() **> Manage AMP Private Cloud Integration(AMP)** Threat Grid . AMP Private Cloud IP FQDN .



AMP Private Cloud 디바이스의 잘못된 Threat Grid SSL 인증서에 대한 경고

증상

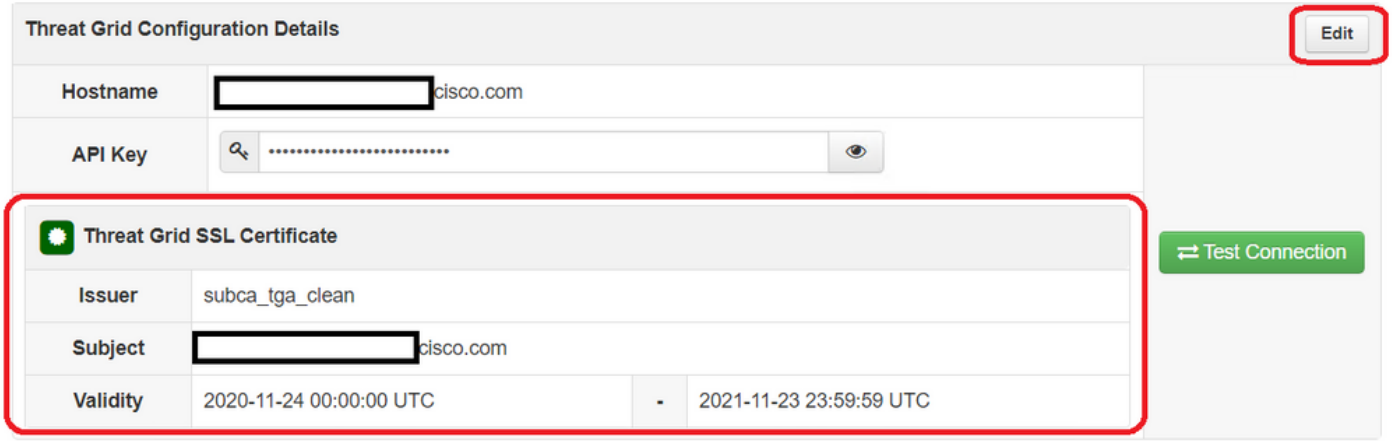
경고 메시지:"Threat Grid SSL 인증서가 유효하지 않습니다."라는 메시지가 Integrations(통합) **> Threat Grid**에서 **Test Connection(연결 테스트)** 버튼을 선택한 후 AMP Private Cloud 디바이스**에서 수신됩니다**.



권장 단계:

- Threat Grid 어플라이언스 정상 인터페이스에 설치된 인증서가 기업 CA에 의해 서명되었는지 확인합니다.

CA에서 서명한 경우 전체 인증서 체인을 파일 내에 추가해야 합니다. AMP Private Cloud 디바이스 관리 포털인 Integrations(통합) **> Threat Grid(Threat Grid SSL 인증서)**의 **Threat Grid(Threat Grid)에 추가해야 합니다**.



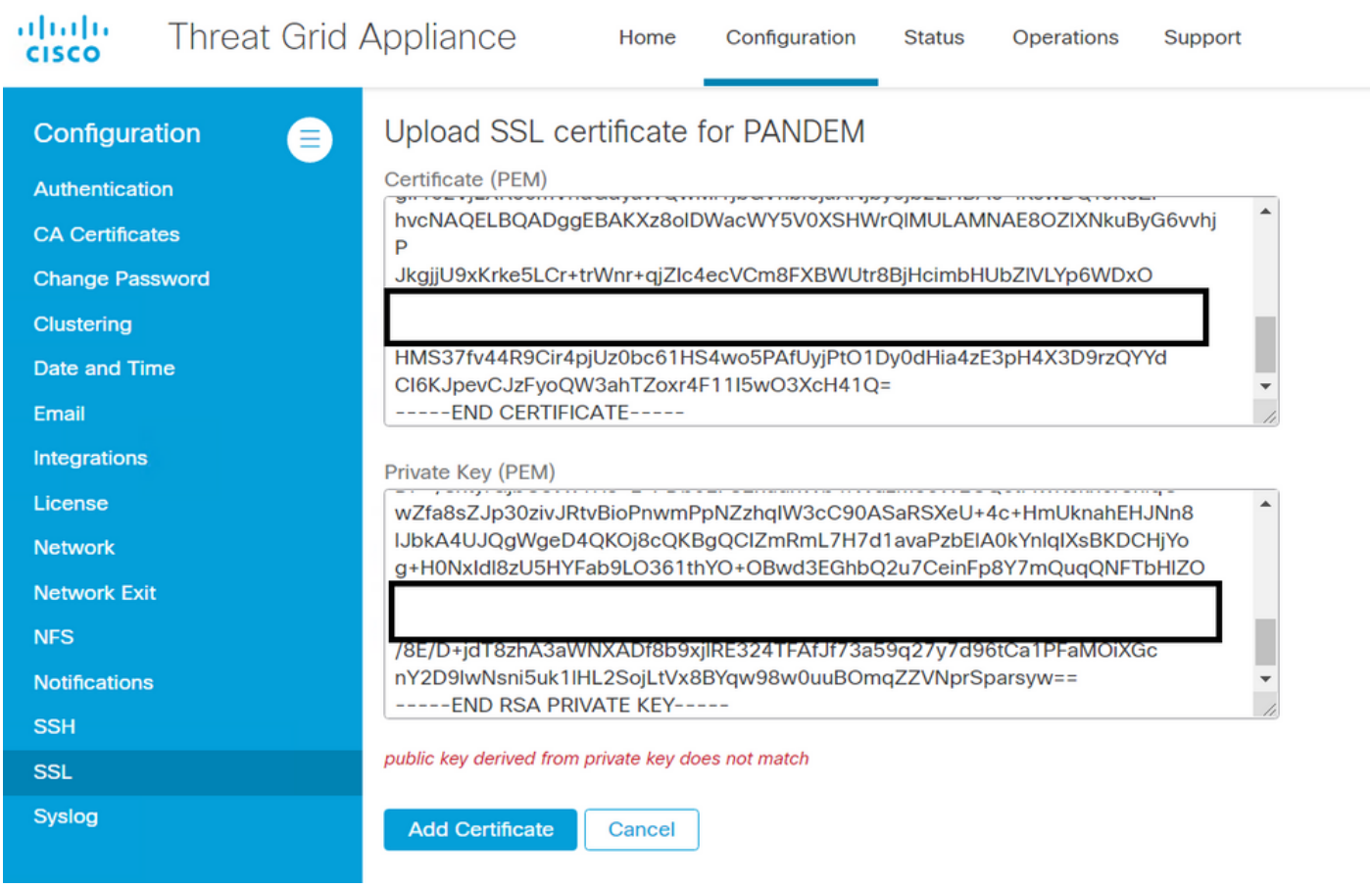
AMP Private Cloud 디바이스에서 현재 설치된 Threat Grid 어플라이언스 인증서는 다음에서 확인할 수 있습니다./opt/fire/etc/ssl/threat_grid.crt

인증서와 관련된 Threat Grid 어플라이언스의 경고

경고 메시지 - 개인 키에서 파생된 공개 키가 일치하지 않습니다.

증상

경고 메시지:개인 키에서 파생된 공개 키가 일치하지 않습니다. 인터페이스에 인증서를 추가하려고 시도한 후 Threat Grid 어플라이언스에서 수신됩니다.



개인 키에서 내보낸 공개 키가 인증서에 구성된 공개 키와 일치하지 않습니다.

권장 단계:

- 개인 키가 인증서의 공개 키와 일치하는지 확인합니다.

개인 키가 인증서의 공개 키와 일치하면 모듈러스 및 공개 지수가 동일해야 합니다.이 분석에서는 모듈러스가 인증서의 개인 키와 공개 키에 동일한 값을 가지고 있는지 확인하기에 충분합니다.

1단계. OpenSSL 툴을 사용하여 개인 키의 모듈과 인증서에 구성된 공개 키를 비교합니다.

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

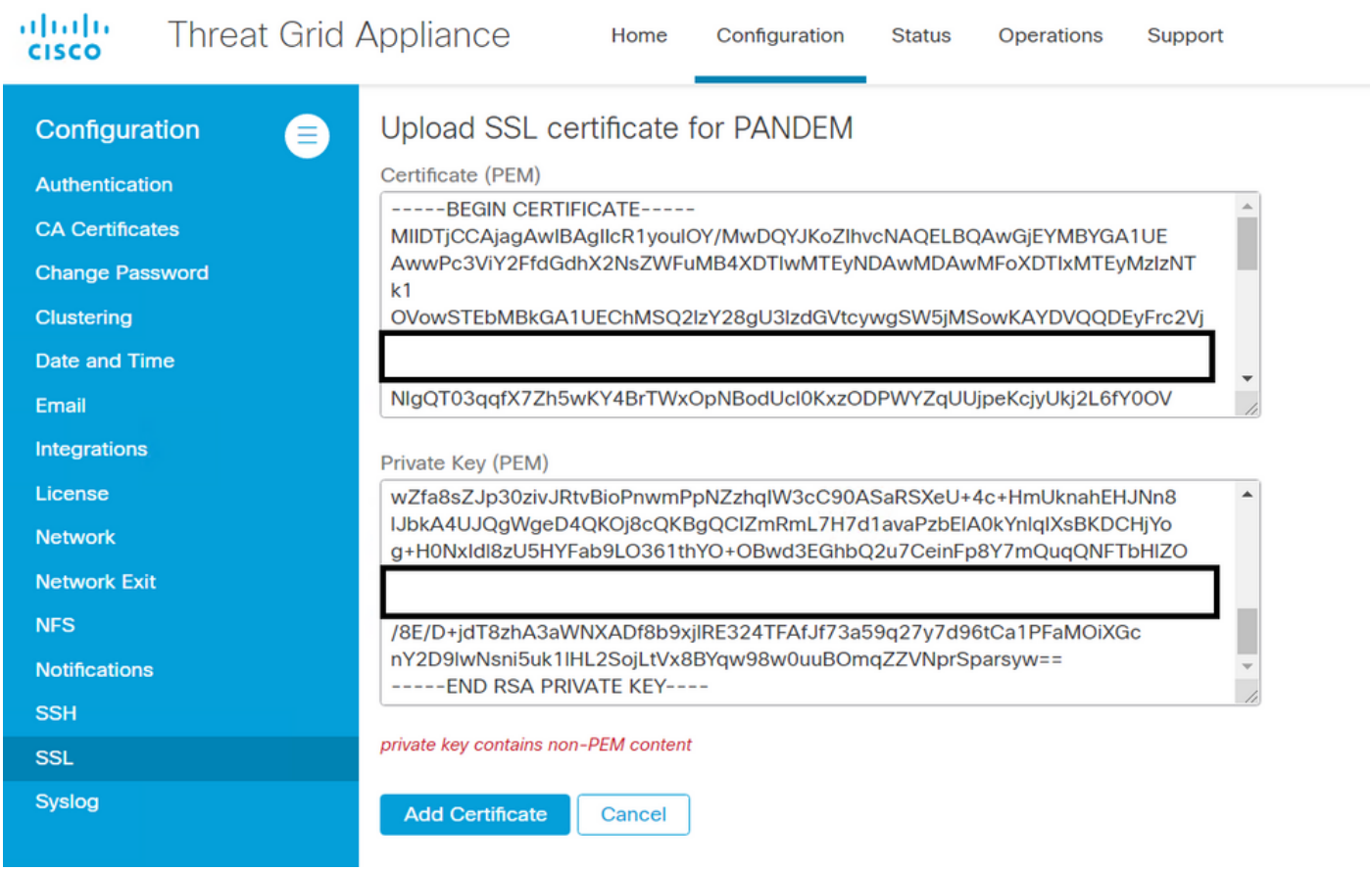
.

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

경고 메시지 - 개인 키에 비 PEM 콘텐츠가 포함되어 있습니다.

증상

경고 메시지:개인 키는 비 PEM 콘텐츠를 포함하며, 인터페이스에 인증서를 추가하려고 시도한 후 Threat Grid 어플라이언스에서 수신됩니다.



개인 키 파일 내의 PEM 데이터가 손상되었습니다.

권장 단계:

- .

1단계. OpenSSL 툴을 사용하여 개인 키의 무결성을 확인합니다.

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

. PEM PEM .

```
$ 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
```

OpenSSL 명령 출력이 **RSA Key**가 아닌 경우 이는 키 내의 PEM 데이터에 문제가 있음을 의미합니다.

OpenSSL 명령으로 문제가 발견된 경우 다음을 수행합니다.

- 개인 키 내의 PEM 데이터가 누락되었는지 확인합니다.

개인 키 파일 내의 PEM 데이터는 64자 줄로 표시됩니다.파일 내의 PEM 데이터를 빠르게 검사하면 데이터가 누락되었는지 확인할 수 있습니다.데이터가 누락된 행이 파일의 다른 행과 정렬되지 않았습니다.

- 개인 키의 첫 번째 줄은 하이픈 5개, BEGIN PRIVATE KEY 단어**로** 시작하고 5개의 하이픈으로 끝나는지 확인합니다.

예.

—개인 키 시작—

- 개인 키의 마지막 줄은 5개의 하이픈으로 시작하고 **END PRIVATE KEY**라는 단어**로 시작하고** 5개의 하이픈으로 끝납니다.

예.

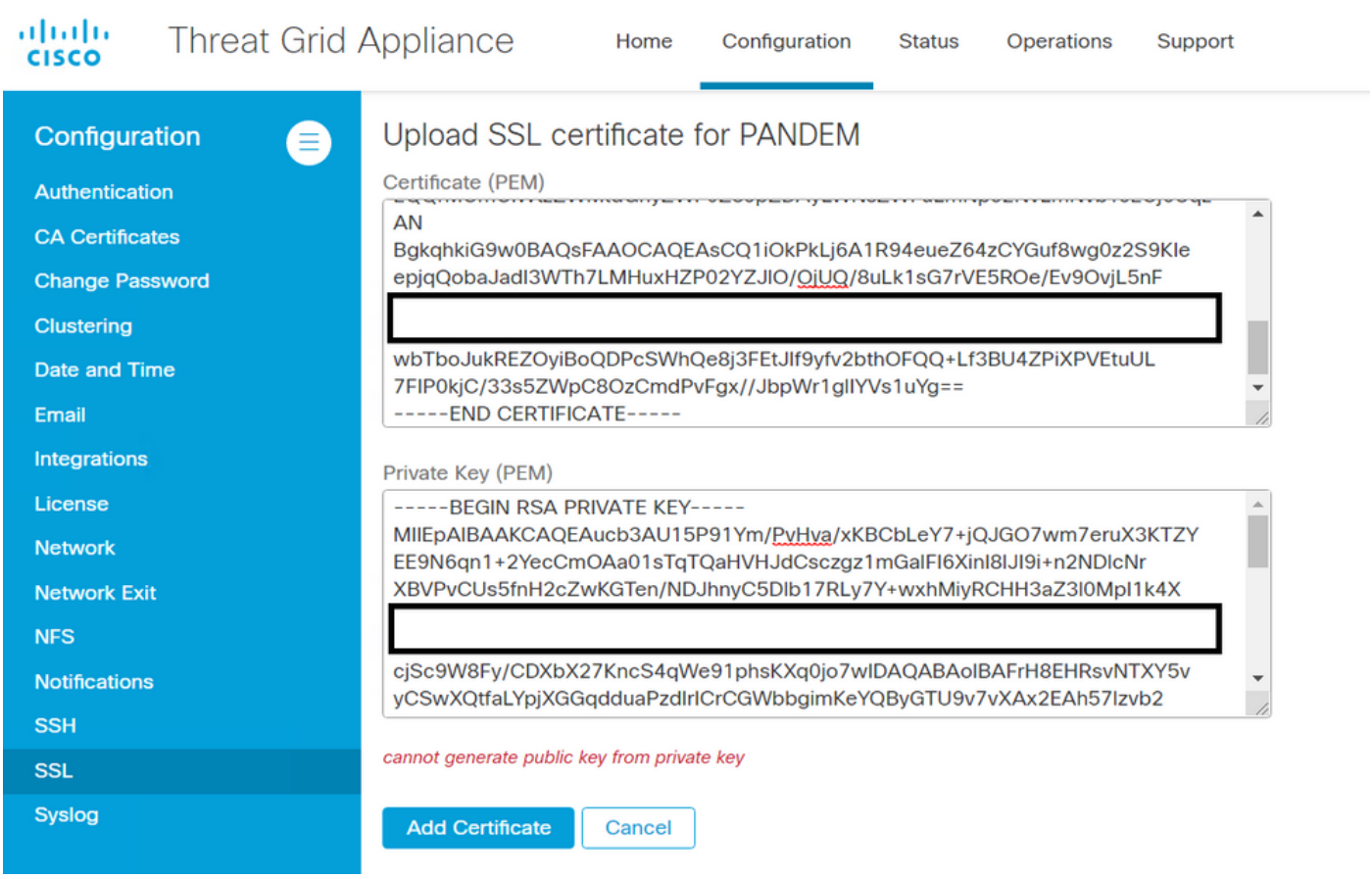
—개인 키 종료—

예.개인 키 내의 PEM 형식 및 데이터를 수정하십시오.

경고 메시지 - 개인 키에서 공개 키를 생성할 수 없습니다.

증상

경고 메시지:개인 키에서 공개 키를 생성할 수 없습니다. 이(가) 인터페이스에 인증서를 추가하려고 시도한 후 Threat Grid 어플라이언스에서 수신됩니다.



개인 키 파일 내의 현재 PEM 데이터에서 공개 키를 생성할 수 없습니다.

권장 단계:

- .

1. OpenSSL .

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

OpenSSL 명령 출력이 **RSA Key**가 아닌 경우 이는 키 내의 PEM 데이터에 문제가 있음을 의미합니다.

2단계. OpenSSL 툴을 사용하여 개인 키에서 공개 키를 내보낼 수 있는지 확인합니다.

```
openssl rsa -in
```

예.공개 키 내보내기에 실패했으며 공개 키를 성공적으로 내보냈습니다.

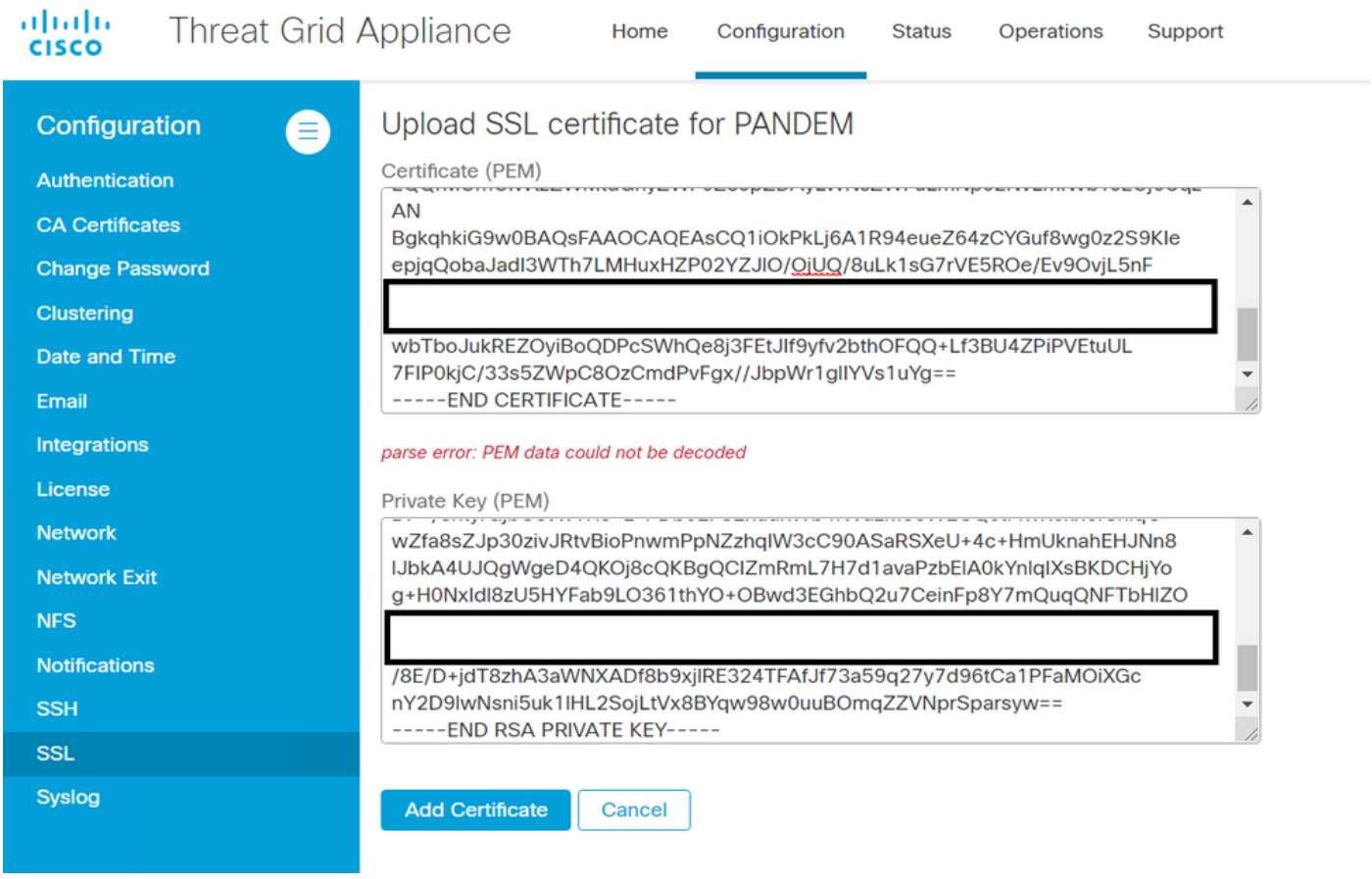
```
$ openssl rsa -in wrong-private-key.key -pubout
unable to load Private Key
140195161523520:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

$ 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-----
```

경고 메시지 - 구문 분석 오류:PEM 데이터를 디코딩할 수 없습니다.

증상

경고 메시지:구문 분석 오류:PEM 데이터를 디코딩할 수 없습니다. 인터페이스에 인증서를 추가하려고 시도한 후 Threat Grid 어플라이언스에서 수신됩니다.



인증서 파일 내의 현재 PEM 데이터에서 인증서를 디코딩할 수 없습니다.인증서 파일 내의 PEM 데이터가 손상되었습니다.

- 인증서 파일 내의 PEM 데이터에서 인증서 정보를 검색할 수 있는지 확인합니다.

1단계. OpenSSL 툴을 사용하여 PEM 데이터 파일의 인증서 정보를 표시합니다.

```
openssl x509 -in
```

PEM 데이터가 손상된 경우 OpenSSL 툴이 인증서 정보를 로드하려고 시도할 때 오류가 발생합니다.

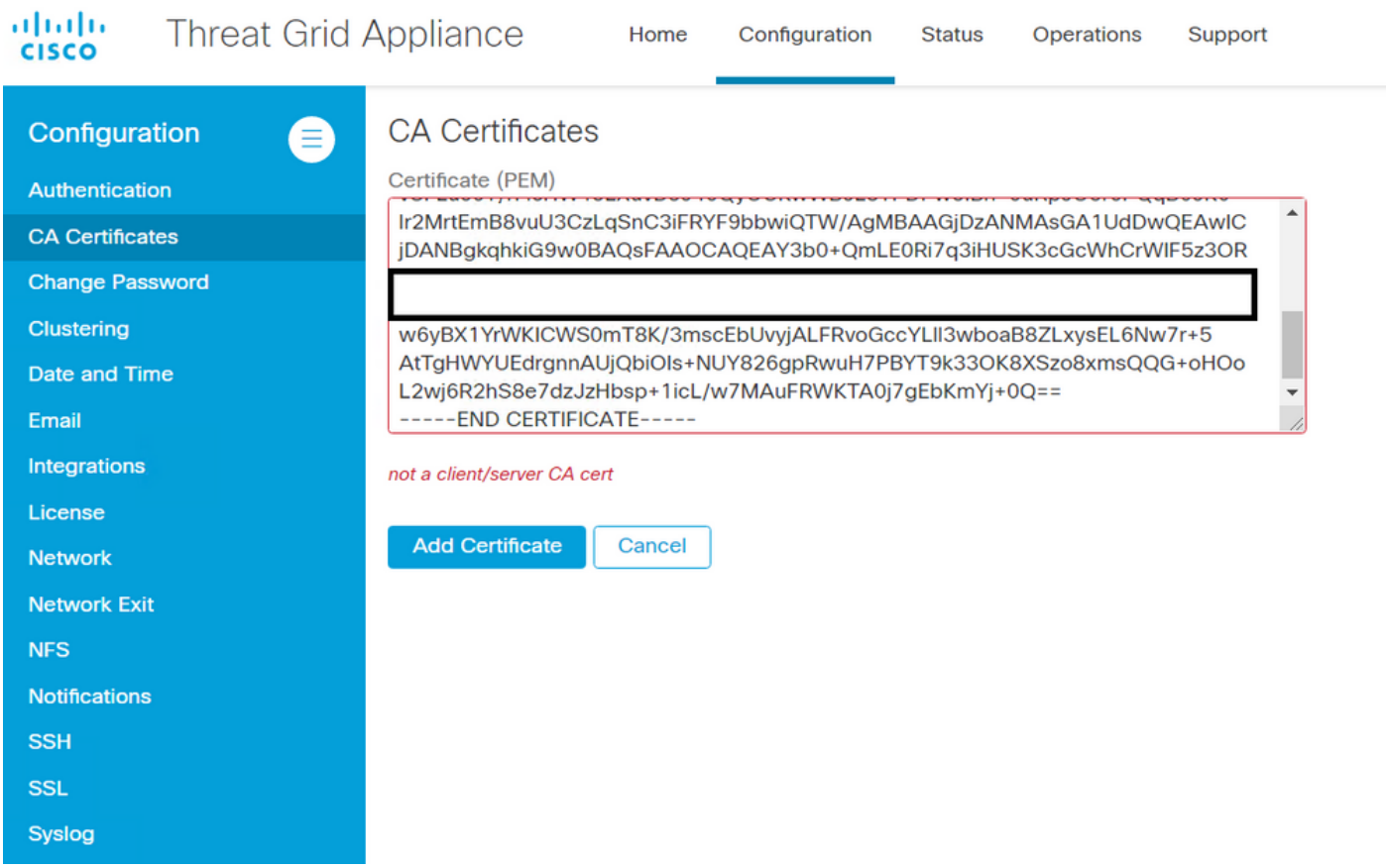
예.인증서 파일의 PEM 데이터가 손상되어 인증서 정보를 로드하지 못했습니다.

```
$ 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:
```

경고 메시지 - 클라이언트/서버 CA 인증서가 아님

증상

경고 메시지:구문 분석 오류:클라이언트/서버 CA 인증서가 아니라 Threat Grid 어플라이언스에서 수신됩니다. 이는 Configuration(컨피그레이션) > **CA Certificates(CA 인증서)**에 CA 인증서를 추가하려고 시도한 후에**는 것입니다**.



CA 인증서의 기본 제약 조건 확장 값이 CA로 정의되지 않았습니다.그렇습니다.

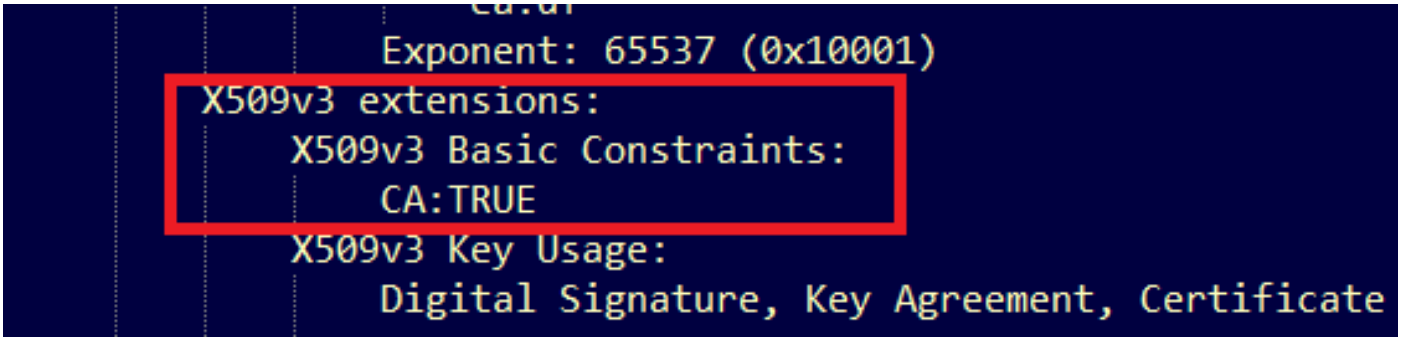
Basic Constraints 확장 값이 CA로 설정된 경우 OpenSSL 툴로 확인합니다.CA 인증서에서 True입니다.

1단계. OpenSSL 툴을 사용하여 PEM 데이터 파일의 인증서 정보를 표시합니다.

```
openssl x509 -in
```

2단계. 인증서 정보에서 **기본 제약 조건** 확장의 현재 값을 검색합니다.

예.Threat Grid 어플라이언스에서 허용하는 CA의 기본 제약 조건 값입니다.



관련 정보

- Threat Grid Appliance - 컨피그레이션 가이드
- Cisco AMP Virtual Private Cloud Appliance - 컨피그레이션 예 및 TechNotes
- 기술 지원 및 문서 – Cisco Systems