Integração do dispositivo AMP Virtual Private Cloud e Threat Grid

Contents

Introduction

Este documento descreve o procedimento para concluir a integração da AMP (Advanced Malware Protection, Proteção avançada contra malware) na nuvem privada virtual e no dispositivo Threat Grid. O documento também fornece etapas de solução de problemas para problemas relacionados ao processo de integração.

Contribuído por Armando Garcia, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Trabalhe e opere a AMP Virtual Private Cloud
- Trabalhe e opere o Threat Grid Appliance

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

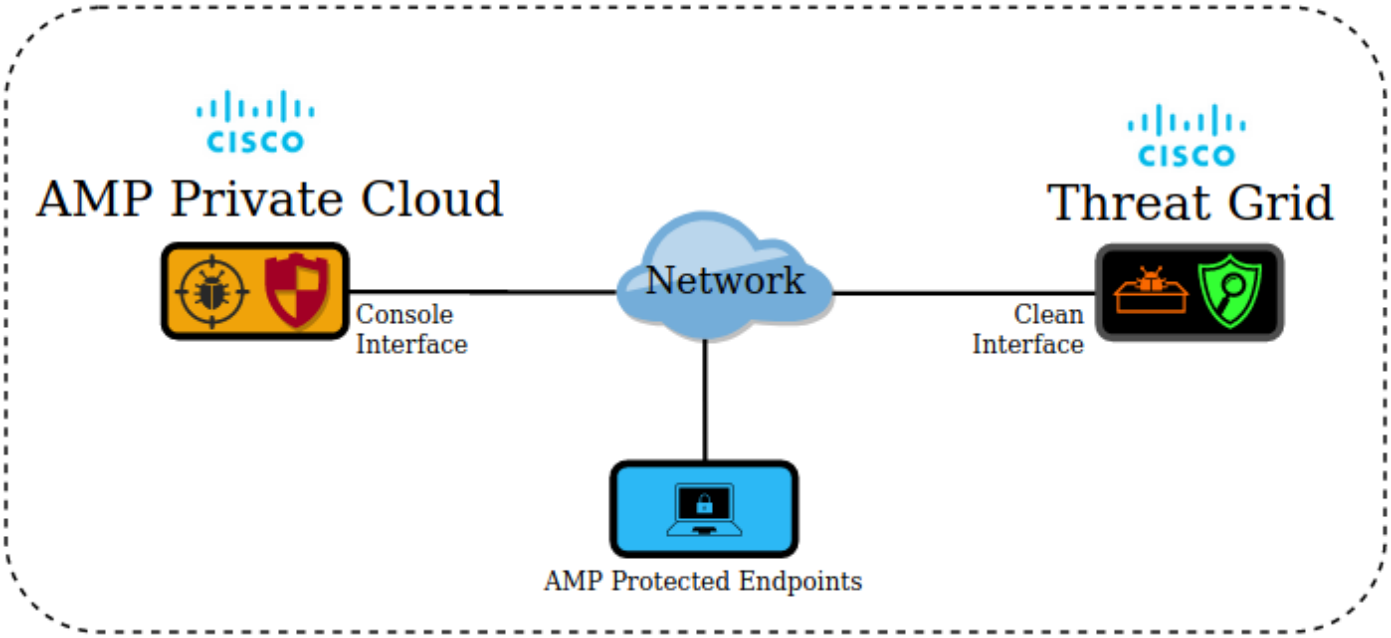
- AMP Private Cloud 3.2.0
- Threat Grid Appliance 2.12.0.1

> **Note**: A documentação é válida para dispositivos Threat Grid e dispositivos AMP Private Cloud no dispositivo ou na versão virtual.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Arquitetura da integração



Informações básicas sobre a integração

- O dispositivo Threat Grid analisa amostras enviadas pelo dispositivo AMP Private Cloud.
- As amostras podem ser enviadas manual ou automaticamente para o dispositivo Threat Grid.
- A análise automática não está habilitada por padrão no dispositivo AMP Private Cloud.
- O dispositivo Threat Grid fornece ao dispositivo AMP Private Cloud um relatório e uma

pontuação da análise da amostra.
- O dispositivo Threat Grid informa (cutuca) o dispositivo AMP Private Cloud sobre qualquer amostra com uma pontuação maior ou igual a 95.
- Se a pontuação da análise for maior ou igual a 95, a amostra no banco de dados da AMP será marcada com uma disposição de mal-intencionado.
- As detecções retrospectivas são aplicadas pela AMP Private Cloud a amostras com uma pontuação maior ou igual a 95.

Procedimento

Etapa 1.Configure e configure o Threat Grid Appliance (ainda não há integração). Verifique se há atualizações e instale, se necessário.

Etapa 2.Configurar e configurar a AMP para a nuvem privada de endpoints (ainda não há integração).

Etapa 3. Na interface do usuário do administrador do Threat Grid, selecione a guia **Configuration** e escolha **SSL**.

Etapa 4.Gerar ou carregar um novo certificado SSL para a interface Clean (PANDEM).

Regenerando certificados SSL

Um novo certificado autoassinado pode ser gerado se o nome do host da interface limpa não corresponder ao nome alternativo do assunto (SAN) no certificado atualmente instalado no dispositivo para a interface limpa. O dispositivo gera um novo certificado para a interface, configurando o nome de host da interface atual no campo SAN do certificado autoassinado.

Etapa 4.1. Na coluna Ações, selecione **(...)** e, no menu pop-up, selecione **Gerar novo certificado.**

Etapa 4.2. Na IU do Threat Grid, selecione **Operations**, na próxima tela, selecione **Ativate** e escolha **Reconfigure**.

> **Nota**: este certificado gerado é autoassinado.

Carregando certificados SSL

Se já houver um certificado criado para a interface de limpeza do dispositivo Threat Grid, esse certificado poderá ser carregado para o dispositivo.

Etapa 4.1. Na coluna Ações, selecione **(...)** e, no menu pop-up, selecione **Carregar novo certificado**.

Etapa 4.2. Copie o certificado e a chave privada correspondente no formato PEM nas caixas de texto que aparecem na tela e selecione **Adicionar certificado**.

Etapa 4.3. Na IU do Threat Grid, selecione **Operations**, na próxima tela, selecione **Ativate** e

escolha **Reconfigure**.

Etapa 5. Na IU de administração do dispositivo AMP Private Cloud, selecione **Integrations** e escolha **Threat Grid**.

Etapa 6. Em Detalhes da configuração do Threat Grid, selecione **Editar**.

Passo 7. No nome de host do Threat Grid, insira o FQDN da interface limpa do dispositivo Threat Grid.

Etapa 8. No certificado SSL do Threat Grid, adicione o certificado da interface limpa do dispositivo Threat Grid. (Consulte as notas abaixo)

O certificado na interface limpa do dispositivo Threat Grid é autoassinado

Etapa 8.1. Na interface do usuário do administrador do Threat Grid, selecione a **configuração** e **escolha** SSL.

Etapa 8.2. Na coluna Ações, selecione **(...)** e, no menu pop-up, selecione **Baixar certificado**.

Etapa 8.3. Continue para adicionar o arquivo baixado ao dispositivo virtual privado da AMP na página de integração do Threat Grid.

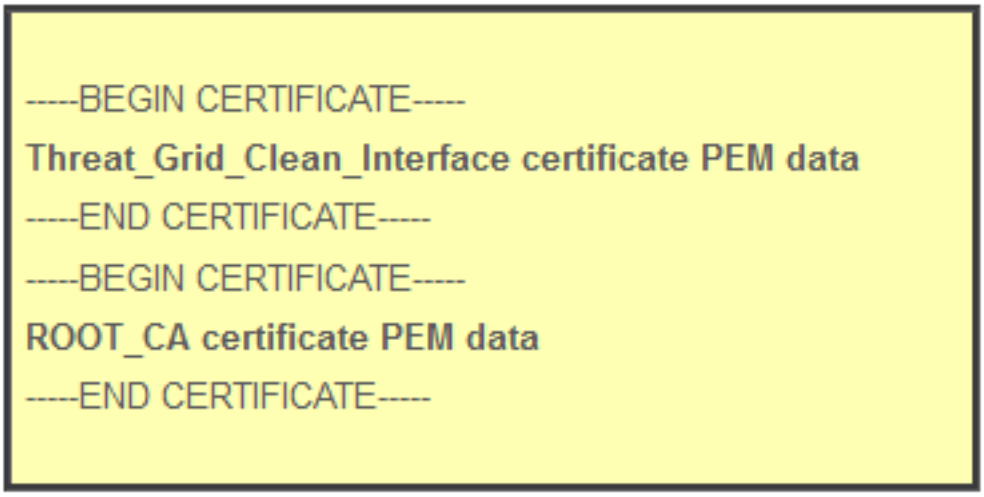
O certificado na interface de limpeza do dispositivo Threat Grid é assinado por uma autoridade de certificação (CA) corporativa

Etapa 8.1. Copie em um arquivo de texto o certificado da interface de limpeza do dispositivo Threat Grid e a cadeia completa de certificados CA.

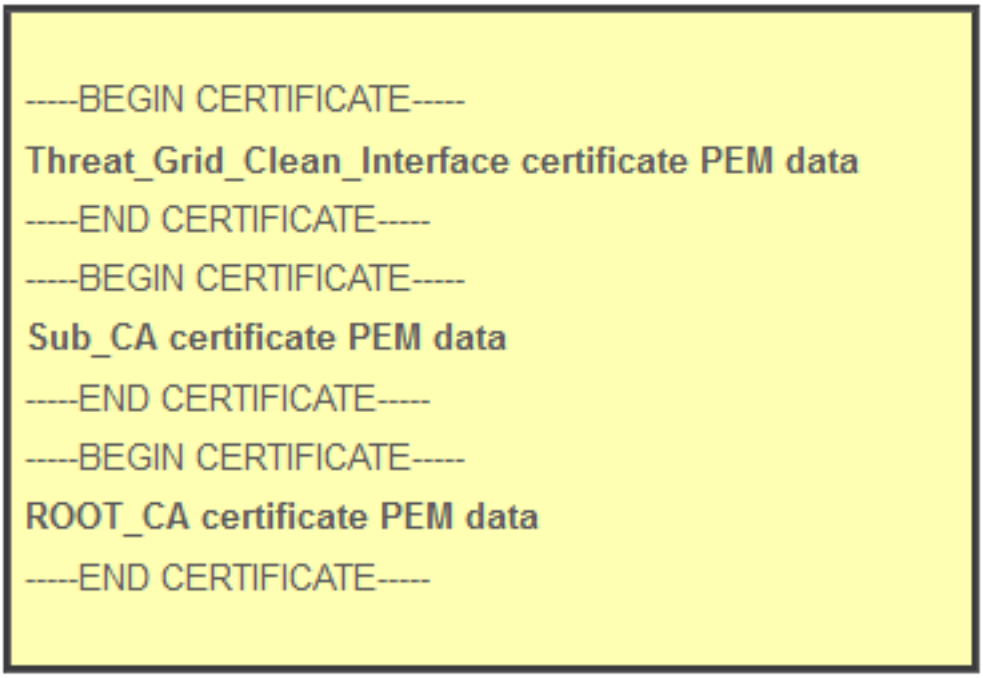
> **Note**: Os certificados no arquivo de texto devem estar no formato PEM.

Exemplo

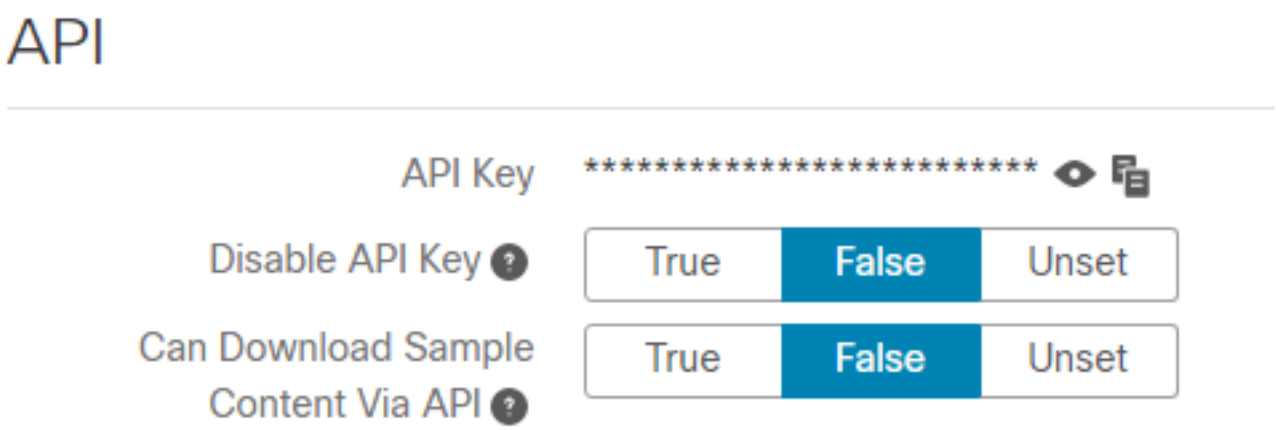
Se a cadeia de certificados completa for: Certificado ROOT_CA > certificado Threat_Grid_Clean_Interface; então o arquivo de texto precisa ser criado, como mostrado na imagem.



Se a cadeia de certificados completa for: Certificado ROOT_CA > Certificado Sub_CA > certificado Threat_Grid_Clean_Interface; então o arquivo de texto precisa ser criado, como mostrado na imagem.



Etapa 9. Na chave de API do Threat Grid, insira a chave de API do usuário do Threat Grid que será vinculado aos exemplos carregados.



Note: Nas configurações da conta do Threat Grid, confirme se o parâmetro **Disable API Key** não está definido como True.

Etapa 10. Depois que todas as alterações forem concluídas, selecione **Salvar**.

Etapa 11. Aplique uma reconfiguração ao dispositivo AMP Virtual Cloud.

Etapa 12. Na IU de administração do dispositivo AMP Private Cloud, selecione **Integrations** e escolha **Threat Grid**.

Etapa 13. Em **Detalhes**, copie os valores da URL do Serviço de Atualização de Disposição, do usuário do Serviço de Atualização de Disposição e da senha do Serviço de Atualização de

Disposição. Essas informações são usadas na Etapa 17.

Etapa 14. Na IU de administração do Threat Grid, selecione **Configuração** e escolha **Certificados CA**.

Etapa 15. Selecione **Adicionar certificado** e copie no formato PEM o certificado CA que assinou o certificado do serviço de atualização de disposição de nuvem privada da AMP.

> **Note**: Se o certificado CA que assinou o certificado AMP Private Cloud Disposition Update for um Sub-CA, repita o processo até que todas as CAs na cadeia sejam carregadas para **certificados CA**.

Etapa 16. No portal Threat Grid, selecione Administration (Administração) e selecione Manage AMP Private Cloud Integration (Gerenciar integração de nuvem privada da AMP).

Etapa 17. Na página Disposition Update Syndication Service, insira as informações coletadas na Etapa 13.

- URL do serviço: FQDN do serviço de atualização de disposição do dispositivo AMP Private Cloud.
- Usuário: usuário do Disposition Update Service do dispositivo AMP Private Cloud.
- Senha: senha para o serviço de atualização de disposição do dispositivo AMP Private Cloud.

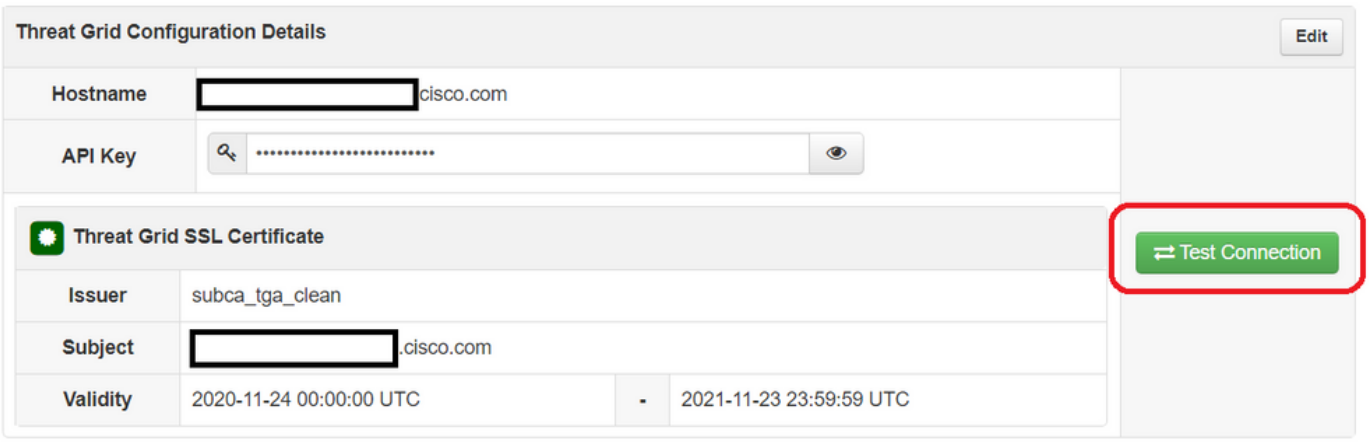
Nesse ponto, se todas as etapas foram aplicadas corretamente, a integração deve estar funcionando com êxito.

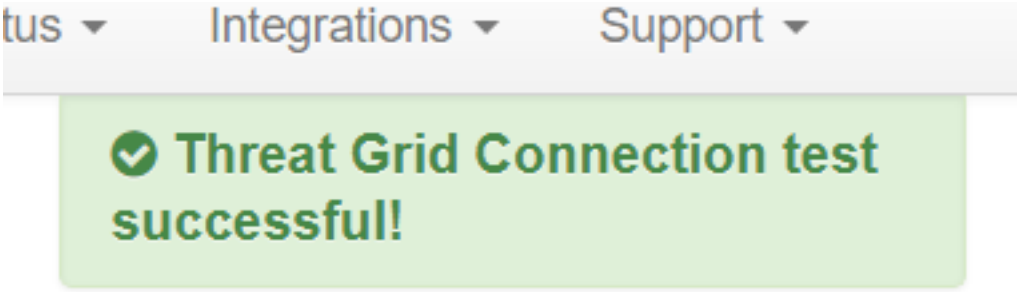
Verificação

Estas são as etapas para confirmar se o dispositivo Threat Grid foi integrado com êxito.

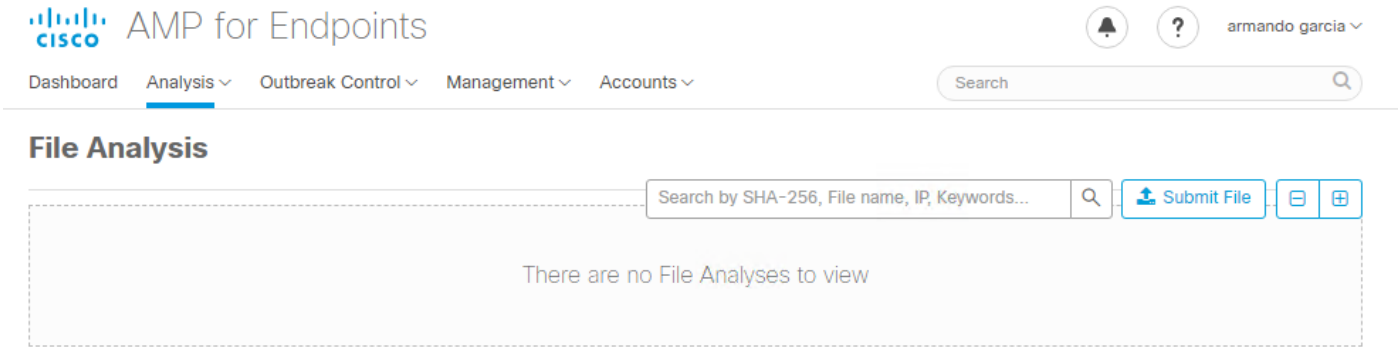
> **Observação**: somente as etapas 1, 2, 3 e 4 são adequadas para serem aplicadas em um ambiente de produção para verificar a integração. A etapa 5 é fornecida como informação para saber mais sobre a integração e não é aconselhável ser aplicada em um ambiente de produção.

Etapa 1. Selecione Testar conexão em Dispositivo de nuvem privada da AMP Interface do usuário > Integrações > Threat Grid e confirme a mensagem Teste de conexão do Threat Grid bem-sucedido! é recebido.

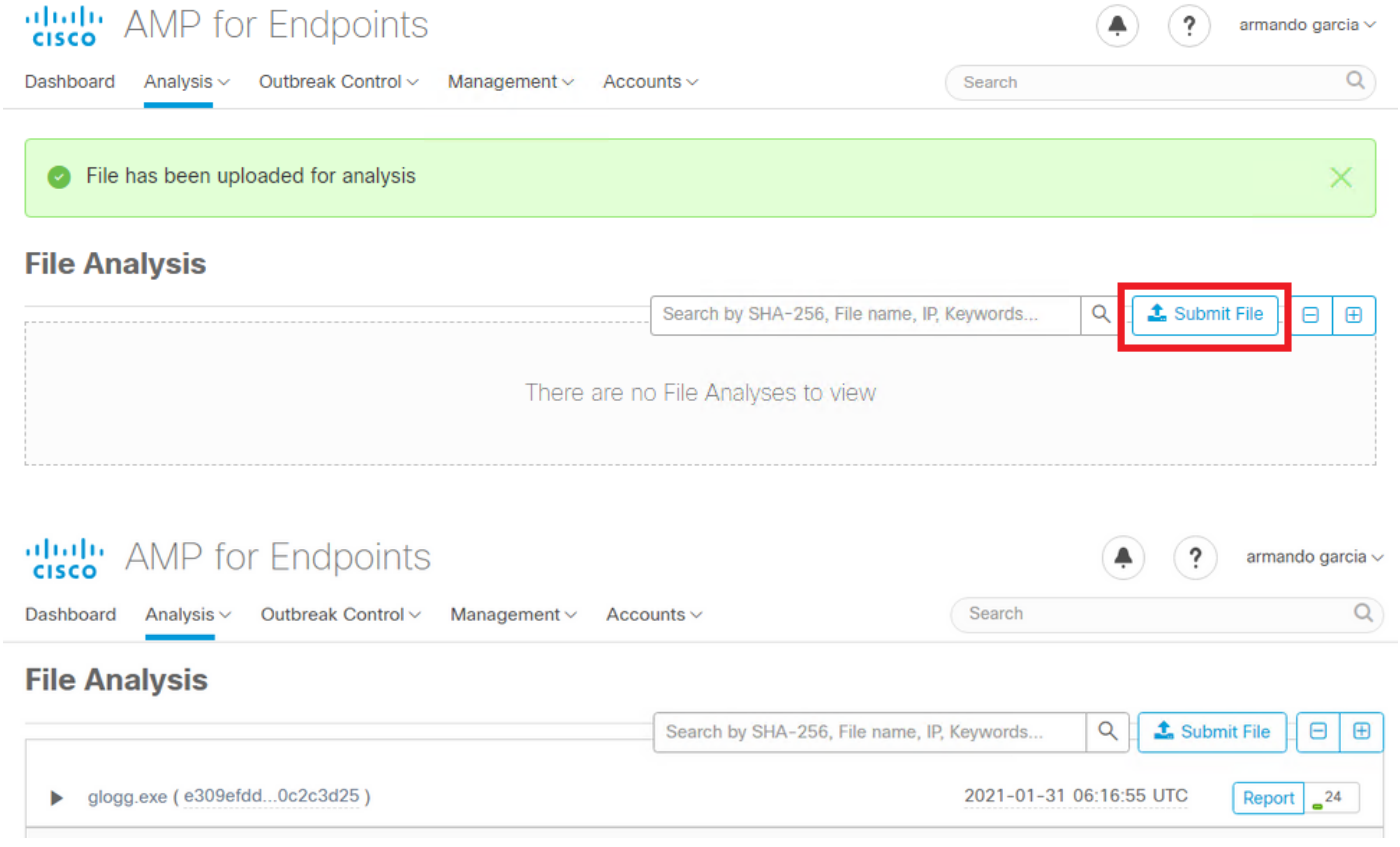




Etapa 2. Confirme se a página da Web Análise de arquivo no console AMP Private Cloud é carregada sem erros.



Etapa 3. Confirme se os arquivos enviados manualmente pelo console AMP Private Cloud **Analysis > File Analysis** são percebidos no dispositivo Threat Grid e um relatório com uma pontuação é retornado pelo dispositivo Threat Grid.



Etapa 4. Confirme se as CAs que assinaram o certificado do Disposition Update Service do

dispositivo AMP Private Cloud estão instaladas no dispositivo Threat Grid em **Certificate Authority**.

Etapa 5. Confirme se qualquer amostra marcada pelo dispositivo Threat Grid com uma pontuação >=95 é registrada no banco de dados AMP Private Cloud com a disposição de mal-intencionado após o relatório e a pontuação de amostra é fornecida pelo dispositivo Threat Grid.

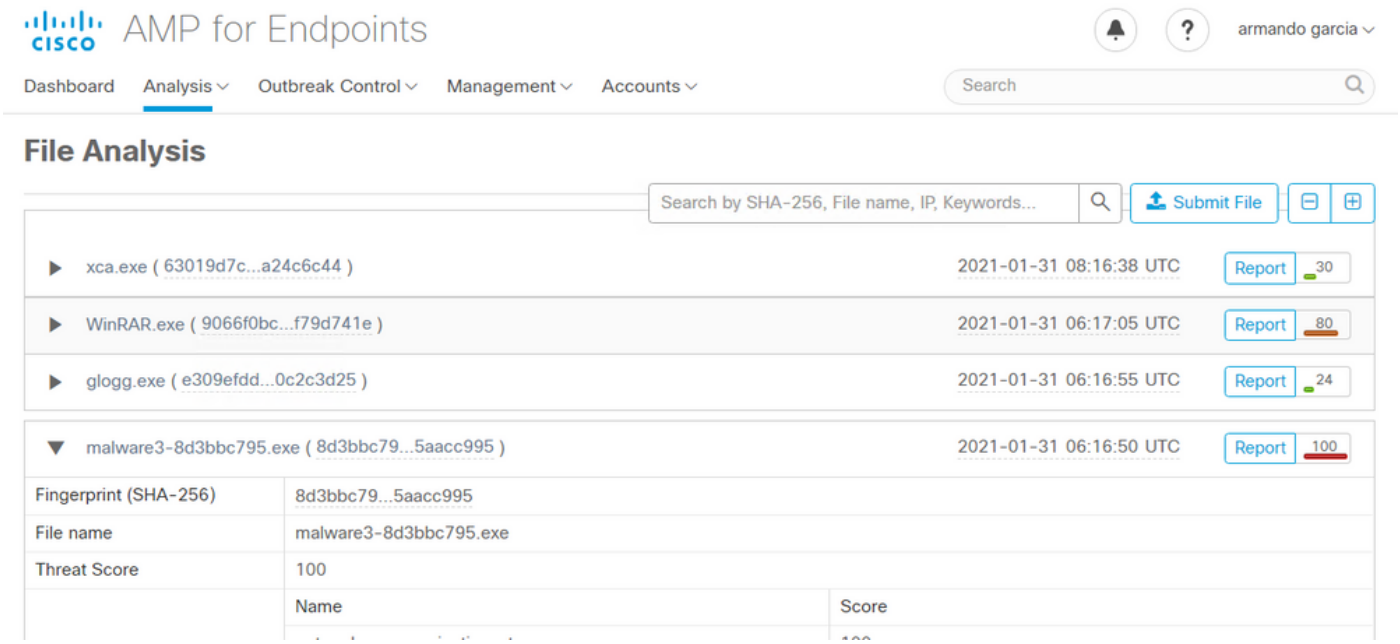
> **Note**: Uma recepção bem-sucedida de um relatório de exemplo e uma pontuação de amostra >=95 no console da AMP Private Cloud na guia **File Analysis**, não significa necessariamente que a disposição do arquivo foi alterada no banco de dados da AMP. Se as CAs que assinaram o certificado do Disposition Update Service do dispositivo AMP Private Cloud não estiverem instaladas no dispositivo Threat Grid em **Certificate Authority**, os relatórios e as pontuações serão recebidos pelo dispositivo AMP Private Cloud, mas nenhum pop-up será recebido do dispositivo Threat Grid.

> **aviso:** O próximo teste foi concluído para disparar uma alteração de disposição de exemplo no banco de dados do AMP depois que o dispositivo Threat Grid marcou um arquivo com uma pontuação >=95. O objetivo deste teste era fornecer informações sobre as operações internas no dispositivo de nuvem privada da AMP quando o dispositivo Threat Grid fornece uma pontuação de amostra de >=95. Para acionar o processo de alteração de disposição, um arquivo de teste de imitação de malware foi criado com o aplicativo interno makemalware.exe da Cisco. Exemplo: malware3-419d23483.exeSHA256: 8d3bbc795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995.

> **Caution**: Não é aconselhável destruir nenhum arquivo de teste de imitação de malware em um ambiente de produção.

Confirmação da atualização da disposição do exemplo no banco de dados de nuvem privada da AMP

O arquivo de malware de teste foi enviado manualmente para o dispositivo Threat Grid a partir da **análise de arquivo** no console AMP Private Cloud. Após a análise da amostra, um relatório de exemplo e uma pontuação de amostra de 100 foram fornecidos ao dispositivo AMP Private Cloud pelo dispositivo Threat Grid. Uma pontuação de exemplo >=95 aciona uma alteração de disposição para a amostra no banco de dados de dispositivos AMP Private Cloud. Essa alteração da disposição de exemplo no banco de dados da AMP com base em uma pontuação de amostra >=95 fornecida pelo Threat Grid é o que é conhecido como poke.



Se:

- A integração foi concluída com êxito.
- Exemplos de relatórios e pontuações são percebidos na **Análise de Arquivo** após o envio manual de arquivos.

Em seguida:

- Para cada exemplo que o dispositivo Threat Grid marca com uma pontuação >=95, uma entrada é adicionada ao arquivo /data/poked/poked.log no dispositivo AMP Private Cloud.
- O /data/poked/poked.log é criado no dispositivo AMP Private Cloud depois que a primeira pontuação de amostra >=95 é fornecida pelo dispositivo Threat Grid.
- O banco de dados db_protect na AMP Private Cloud mantém a disposição atual para a amostra. Essa informação pode ser usada para confirmar se a amostra tem uma disposição de 3 depois que o dispositivo Threat Grid forneceu a pontuação.

Se o relatório de exemplo e a pontuação >=95 forem percebidos na **Análise de arquivo** no console AMP Private Cloud, aplique estas etapas:

Etapa 1. Faça login via SSH no dispositivo AMP Private Cloud.

Etapa 2. Confirme se há uma entrada em /data/poked/poked.log para a amostra.

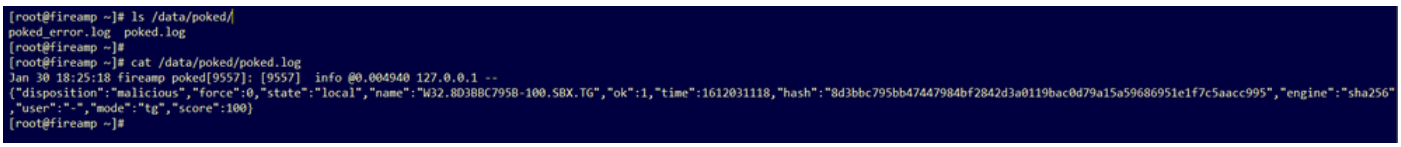
Listar o diretório /data/poked/ em um dispositivo AMP Private Cloud que nunca recebeu uma pontuação de amostra >=95 de um dispositivo Threat Grid mostra que o arquivo poked.log não foi criado no sistema.

Se o dispositivo AMP Private Cloud nunca recebeu um cupom de um dispositivo Threat Grid, o arquivo /data/poked/poked.log não é encontrado no diretório, como mostrado na imagem.

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

Listando o diretório /data/poked/ depois que a primeira pontuação de amostra >=95 foi recebida, mostra que o arquivo foi criado.

Depois de receber a primeira amostra com uma pontuação >=95.



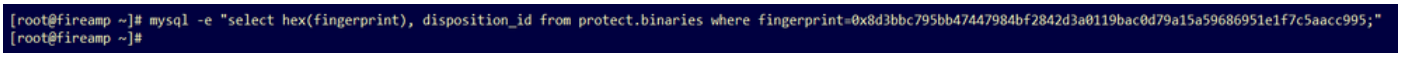
Informações de exemplo do cupom fornecido pelo dispositivo Threat Grid podem ser vistas no arquivo poked.log.

Etapa 3. **Execute** este comando com o exemplo SHA256 para recuperar a disposição atual do banco de dados do dispositivo AMP Private Cloud.

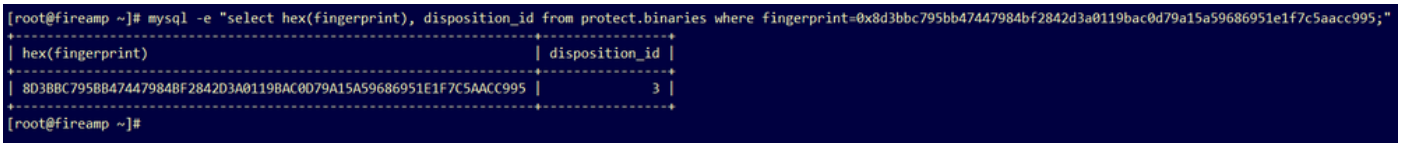
```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

Exemplo

Uma consulta de banco de dados para obter a disposição do exemplo antes que o exemplo seja carregado para o dispositivo Threat Grid não fornece resultados, como mostrado na imagem.



Uma consulta de banco de dados para obter a disposição de exemplo depois que o relatório e a pontuação foram recebidos do dispositivo Threat Grid, mostra a amostra com uma disposição de 3 que é considerada mal-intencionada.



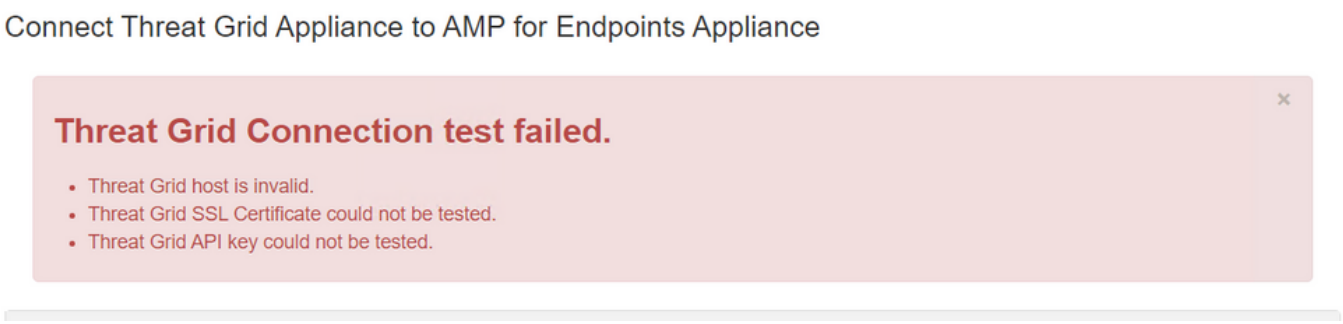
Troubleshooting

No processo de integração, podem ser percebidos possíveis problemas. Nesta parte do documento, algumas das questões mais comuns são abordadas.

Aviso no dispositivo AMP Private Cloud sobre host inválido, certificado não testado, chave API não testada

Sintoma

A mensagem de aviso: O host do Threat Grid é inválido, o certificado SSL do Threat Grid não pôde ser testado, a chave da API do Threat Grid não pôde ser testada, foi recebida no dispositivo AMP Private Cloud depois de selecionada a opção **Test Connection** no **Integrations > Threat Grid**.



Há um problema no nível da rede na integração.

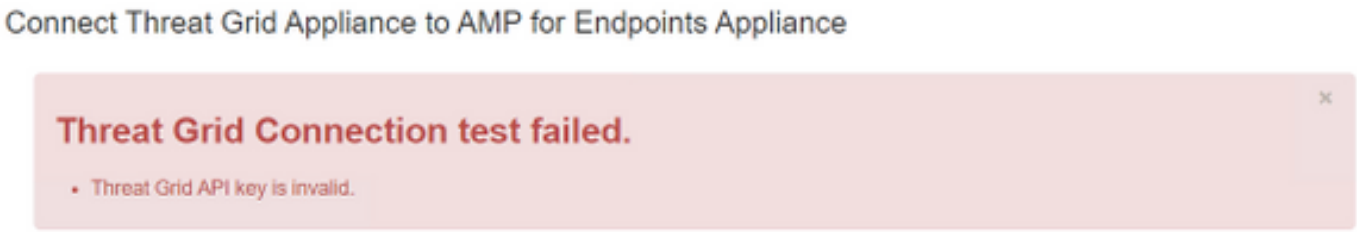
Etapas recomendadas:

- Confirme se a interface do console do dispositivo AMP Private Cloud pode acessar a interface limpa do dispositivo Threat Grid.
- Confirme se o dispositivo AMP Private Cloud pode resolver o FQDN da interface de limpeza do dispositivo Threat Grid.
- Confirme se não há um dispositivo de filtragem no caminho da rede do dispositivo AMP Private Cloud e do dispositivo Threat Grid.

Aviso no dispositivo AMP Private Cloud sobre chave inválida da API do Threat Grid

Sintoma

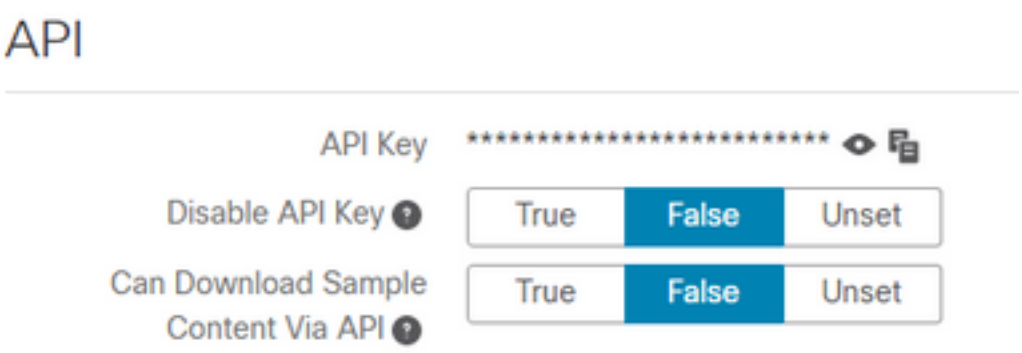
A mensagem de aviso: Falha no teste de conexão do Threat Grid, a API do Threat Grid é inválida, é recebida no dispositivo AMP Private Cloud após ser selecionado o botão **Test Connection** em **Integrations > Threat Grid**.



A chave da API do dispositivo Threat Grid configurada na nuvem privada da AMP.

Etapas recomendadas:

- Confirme nas configurações de conta do usuário do dispositivo Threat Grid, o parâmetro Disable API Key não está definido como True.
  - O parâmetro Disable API Key deve ser definido como: Falso ou indefinido.



- Confirme se a chave da API do Threat Grid configurada no portal de administração da nuvem privada da AMP **Integrations > Threat Grid**, é a mesma chave da API nas configurações do usuário no dispositivo Threat Grid.
- Confirme se a chave de API do Threat Grid correta foi salva no banco de dados de dispositivos da AMP Private Cloud.

Na linha de comando do dispositivo AMP Private Cloud, é possível confirmar a chave atual da API do Threat Grid configurada no dispositivo AMP. Faça login no dispositivo AMP Private Cloud via SSH e execute este comando para recuperar a chave de API do usuário do Threat Grid:

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

Esta é uma entrada correta no banco de dados do dispositivo AMP Private Cloud para a chave API do dispositivo Threat Grid.

```
[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 ~]#
```

Embora o nome de usuário do Threat Grid não tenha sido configurado diretamente no dispositivo de nuvem privada da AMP em qualquer etapa da integração, o nome de usuário do Threat Grid será percebido no parâmetro tg_login no banco de dados da AMP se a chave da API do Threat Grid tiver sido aplicada corretamente.

Esta é uma entrada incorreta no banco de dados do AMP para a chave da API do Threat Grid.

```
[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 ~]#
```

O parâmetro tg_login é NULL. O nome de usuário do Threat Grid não foi recuperado do dispositivo Threat Grid pelo dispositivo AMP Private Cloud após a aplicação da reconfiguração.

As pontuações de exemplo >=95 são recebidas pelo dispositivo AMP Private Cloud, mas nenhuma alteração percebida na disposição de exemplo

Sintoma

Os relatórios e as pontuações de exemplo >=95 são recebidos com êxito do dispositivo Threat Grid após o envio de uma amostra, mas nenhuma alteração na disposição da amostra é percebida no dispositivo AMP Private Cloud.

Etapas recomendadas:

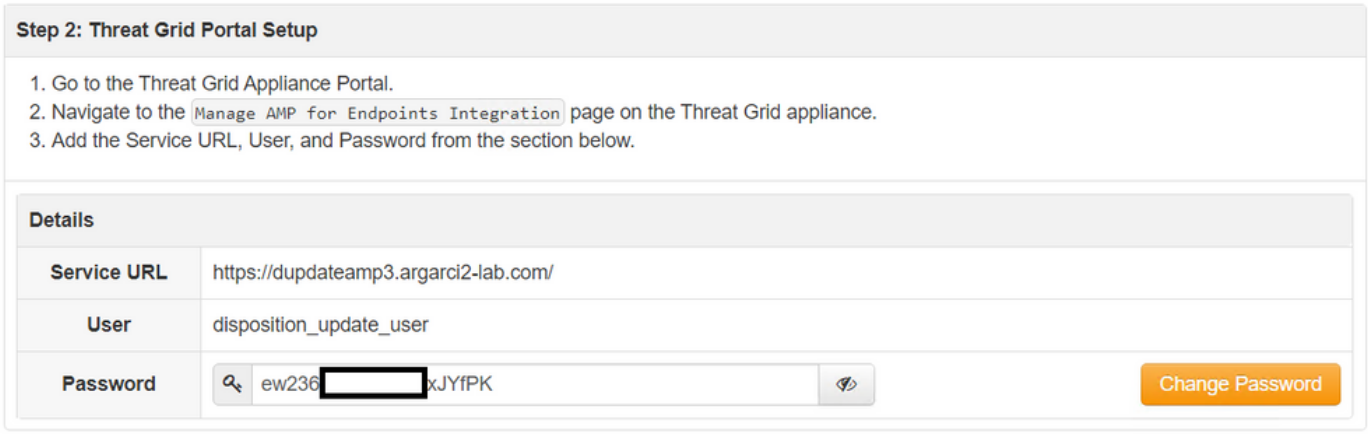
- Confirme no dispositivo AMP Private Cloud se a amostra SHA256 está no conteúdo de /data/poked/poked.log.

Se o SHA256 for encontrado em /data/poked/poked.log, execute esse comando para confirmar a disposição de exemplo atual no banco de dados do AMP.

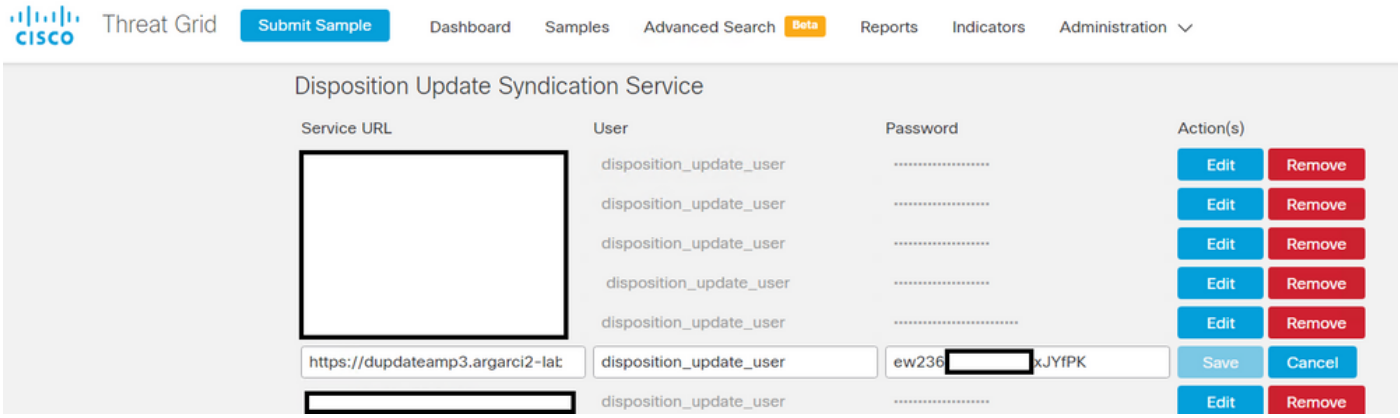
```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

- Confirme se a senha de integração da AMP Private Cloud correta foi adicionada ao portal de administração do dispositivo Threat Grid em **Administration > Manage AMP Private Cloud Integration**.

Portal de administração da AMP Private Cloud.



Portal do console do dispositivo Threat Grid.

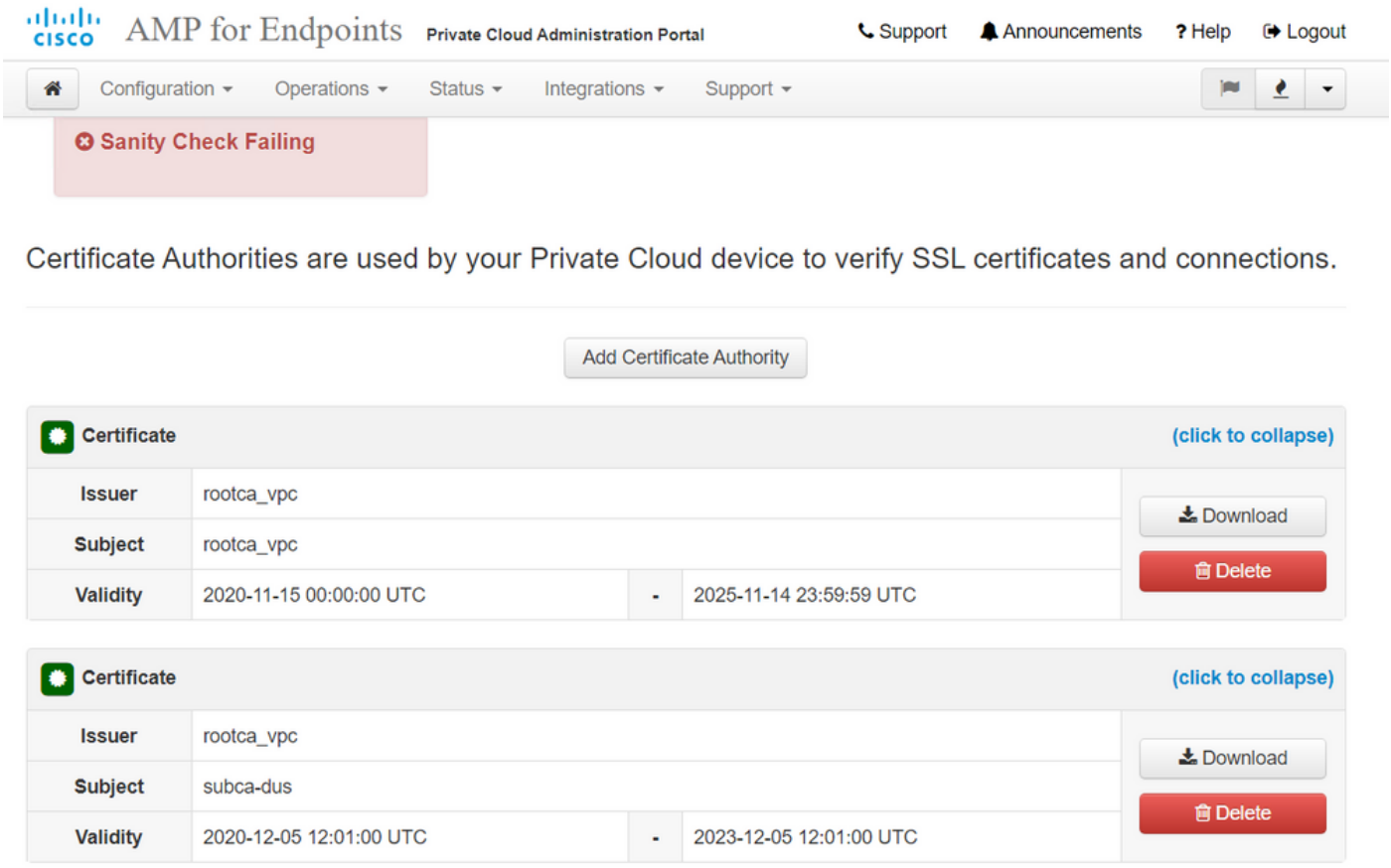


- Confirme se as CAs que assinaram o certificado do AMP Private Cloud Disposition Update Service foram instaladas no portal de administração do dispositivo Threat Grid em **Certificados CA**.

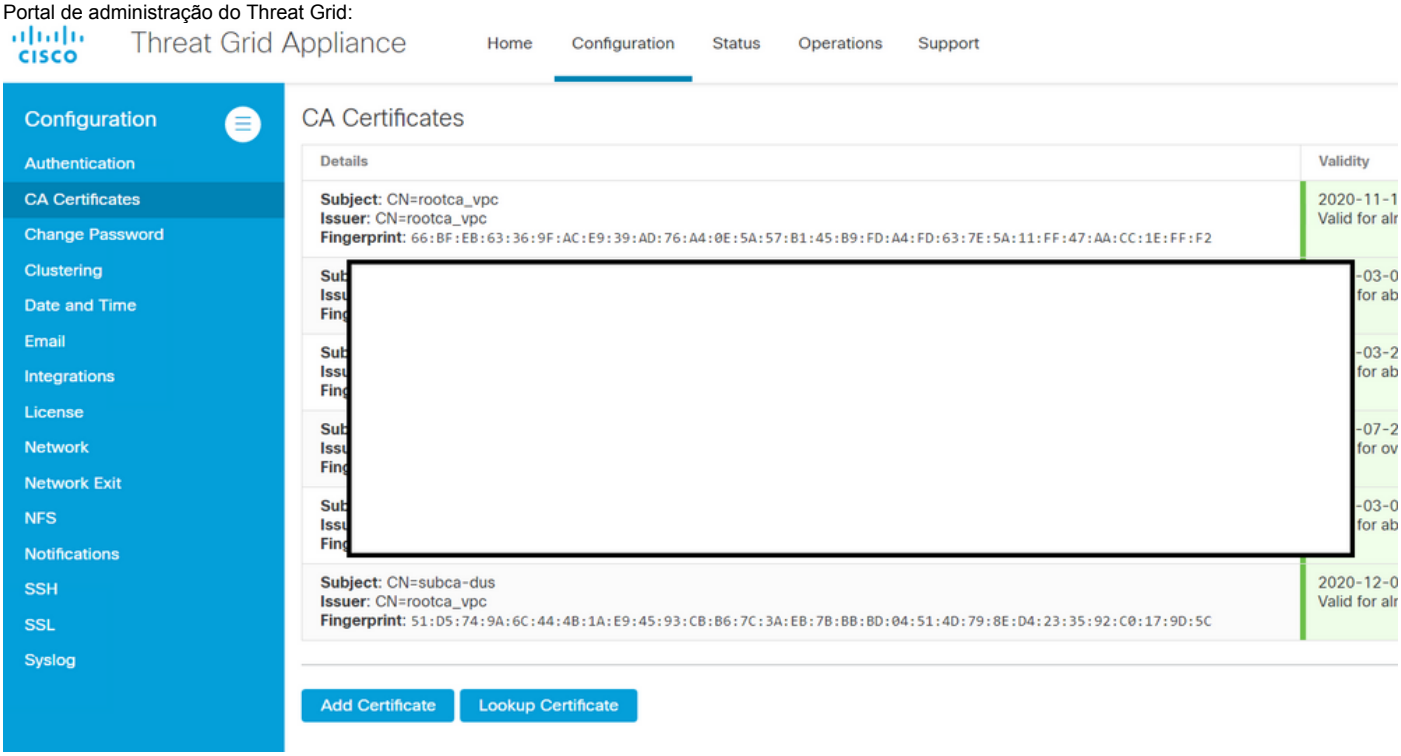
No exemplo abaixo, a cadeia de certificados do certificado do serviço de atualização de disposição do dispositivo AMP Private Cloud é **Root_CA > Sub_CA > Disposition_Update_Service certificate**; portanto, o RootCA e o Sub_CA devem ser instalados em **Certificados CA** no Threat

Grid Appliance.

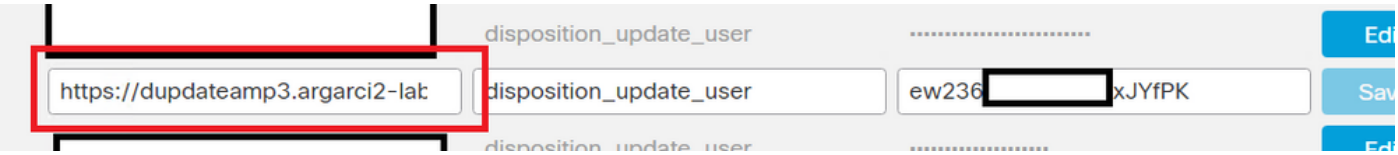
Autoridades de certificação no portal de administração de nuvem privada da AMP.



Portal de administração do Threat Grid:



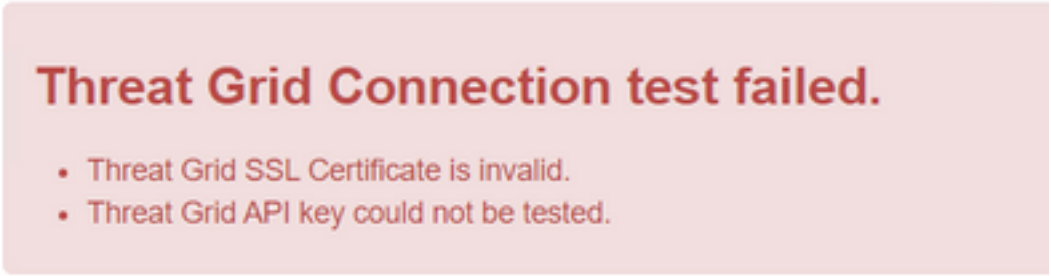
- Confirme se o FQDN do serviço de atualização de disposição do dispositivo AMP Private Cloud foi adicionado corretamente ao portal de administração do dispositivo Threat Grid em **Administration > Manage AMP Private Cloud Integration**. Confirme também se o endereço IP da interface do console do dispositivo AMP Private Cloud não foi adicionado em vez do FQDN.



Aviso no dispositivo AMP Private Cloud sobre certificado inválido de SSL do Threat Grid

Sintoma

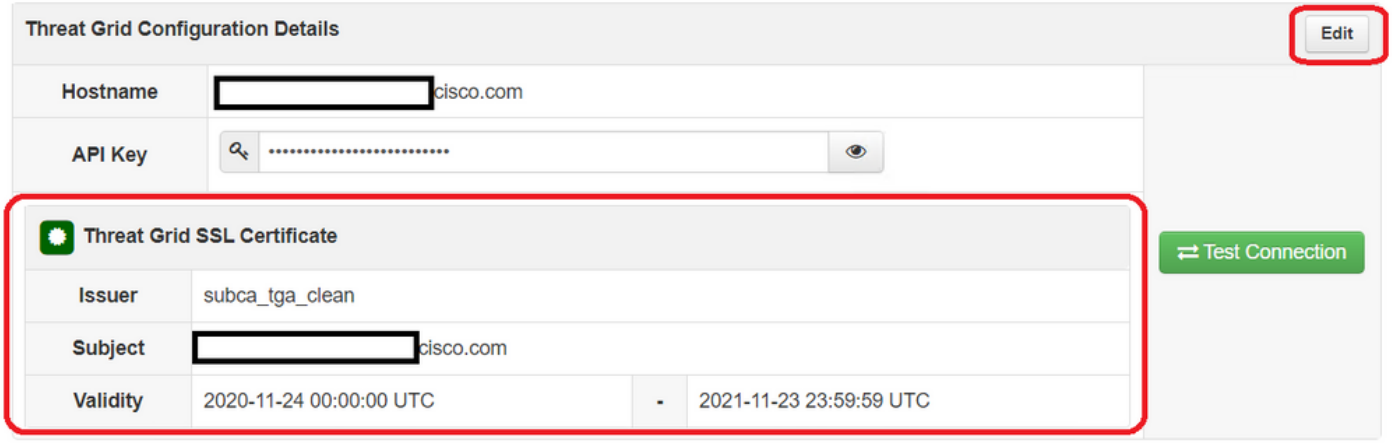
A mensagem de aviso: "O certificado SSL do Threat Grid é inválido", é recebido no dispositivo AMP Private Cloud depois de selecionado o botão **Test Connection** em **Integrations > Threat Grid**.



Etapas recomendadas:

- Confirme se o certificado instalado na interface de limpeza do dispositivo Threat Grid está assinado por uma CA corporativa.

Se for assinado por uma CA, a cadeia completa de certificados deve ser adicionada dentro de um arquivo ao portal de administração do dispositivo AMP Private Cloud **Integrations > Threat Grid** no **certificado SSL Threat Grid**.



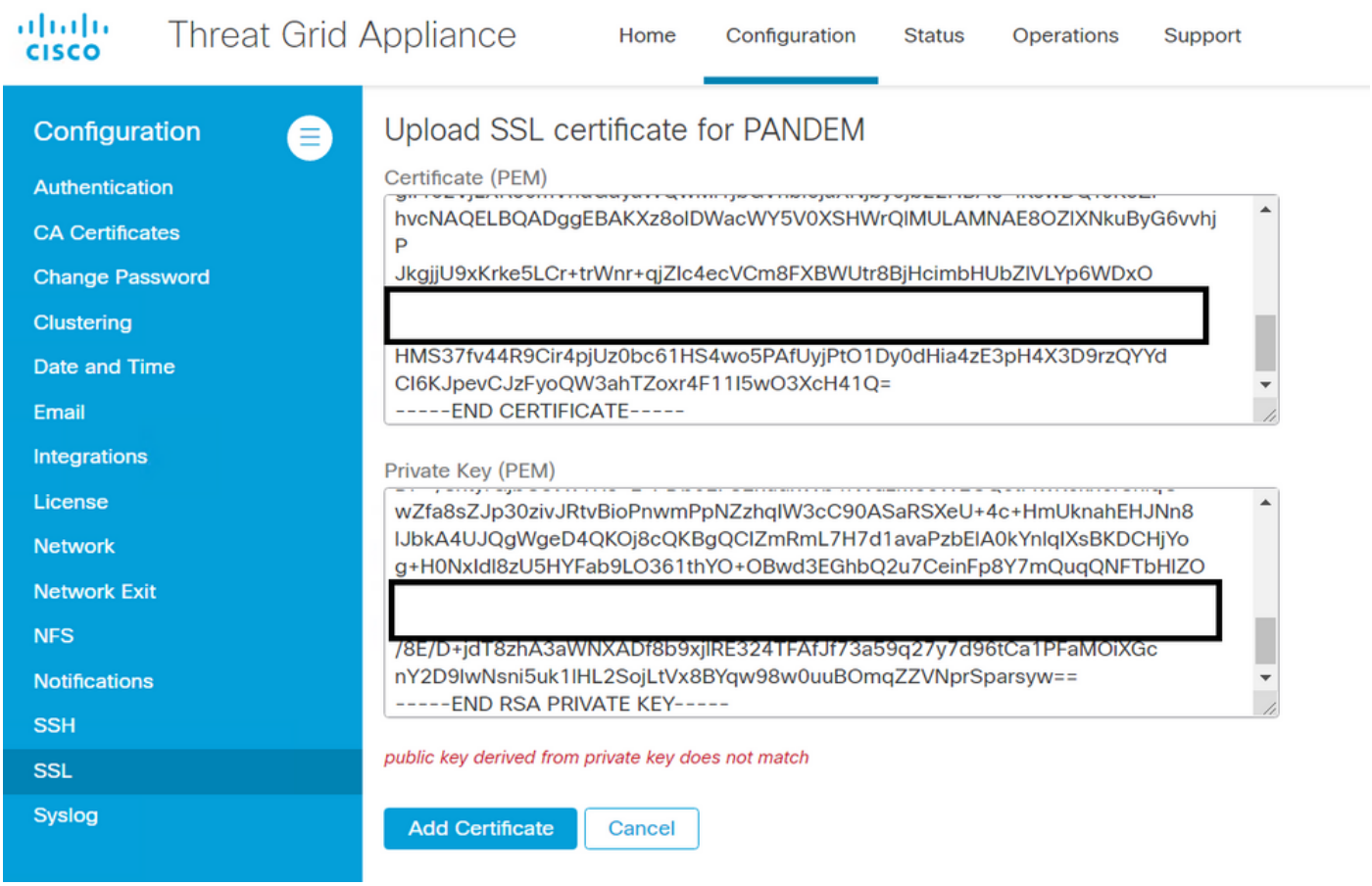
No dispositivo AMP Private Cloud, os certificados do dispositivo Threat Grid atualmente instalados podem ser encontrados em: /opt/fire/etc/ssl/threat_grid.crt.

Avisos no dispositivo Threat Grid relacionados a certificados

Mensagem de aviso - A chave pública derivada da chave privada não corresponde

Sintoma

A mensagem de aviso: a chave pública derivada da chave privada não corresponde, é recebida no dispositivo Threat Grid após uma tentativa de adicionar um certificado a uma interface.



A chave pública exportada da chave privada não corresponde à chave pública configurada no certificado.

Etapas recomendadas:

- Confirme se a chave privada corresponde à chave pública no certificado.

Se a chave privada corresponder à chave pública no certificado, o módulo e o expoente público deverão ser iguais. Para essa análise, basta confirmar se o módulo tem o mesmo valor na chave privada e na chave pública no certificado.

Etapa 1. Utilize a ferramenta OpenSSL para comparar o módulo na chave privada e na chave pública configuradas no certificado.

`openssl x509 -noout -modulus -in`

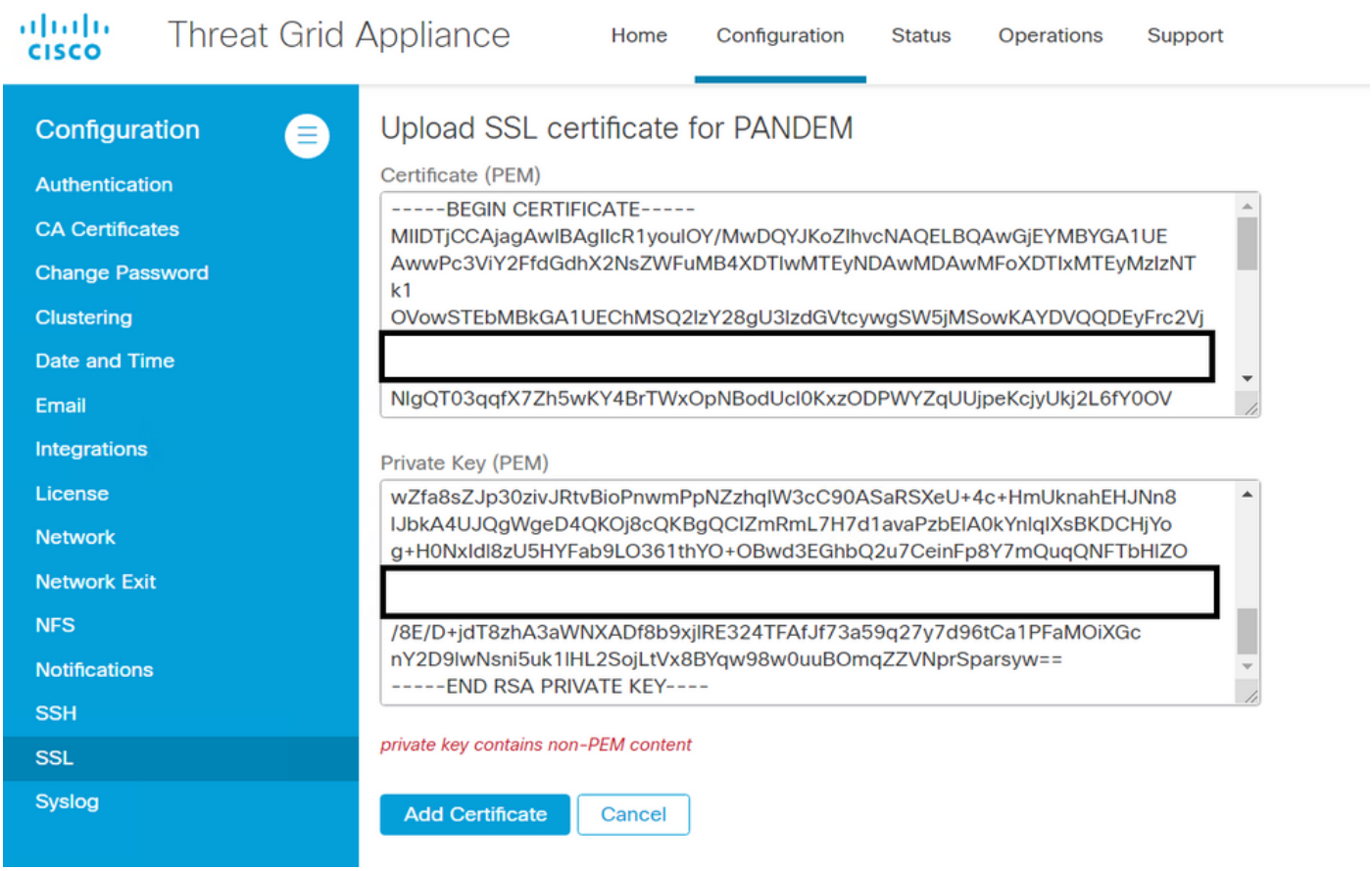
Exemplo. Correspondência bem-sucedida de uma chave privada e de uma chave pública configuradas em um certificado.

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

Mensagem de aviso - A chave privada contém conteúdo não PEM

Sintoma

A mensagem de aviso: A chave privada contém conteúdo não PEM, é recebida no dispositivo Threat Grid após uma tentativa de adicionar um certificado a uma interface.



Os dados PEM dentro do arquivo de chave privada estão corrompidos.

Etapas recomendadas:

- Confirme a integridade dos dados dentro da chave privada.

Etapa 1. Use a ferramenta OpenSSL para verificar a integridade da chave privada.

`openssl rsa -check -noout -in`

Exemplo. Saída de uma chave privada com erros nos dados PEM dentro do arquivo e de outra chave privada sem erros no conteúdo 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
```

Se a saída do comando OpenSSL não for **RSA Key ok**, isso significa que foram encontrados problemas com os dados PEM dentro da chave.

Se foram encontrados problemas com o comando OpenSSL, então:

- Confirme se os dados PEM dentro da chave privada estão ausentes.

Os dados PEM dentro do arquivo de chave privada são exibidos em linhas de 64 caracteres. Uma verificação rápida dos dados PEM dentro do arquivo pode mostrar se os dados estão faltando. A linha com dados ausentes não está alinhada com outras linhas no arquivo.

- Confirme se a primeira linha na chave privada começa com 5 hífens, as palavras **BEGIN PRIVATE KEY** e termina com 5 hífens.

Exemplo.

—INICIAR CHAVE PRIVADA—

- Confirme se a última linha na chave privada começa com 5 hífens, as palavras **END PRIVATE KEY** e termina com 5 hífens.

Exemplo.

—CHAVE PRIVADA FINAL—

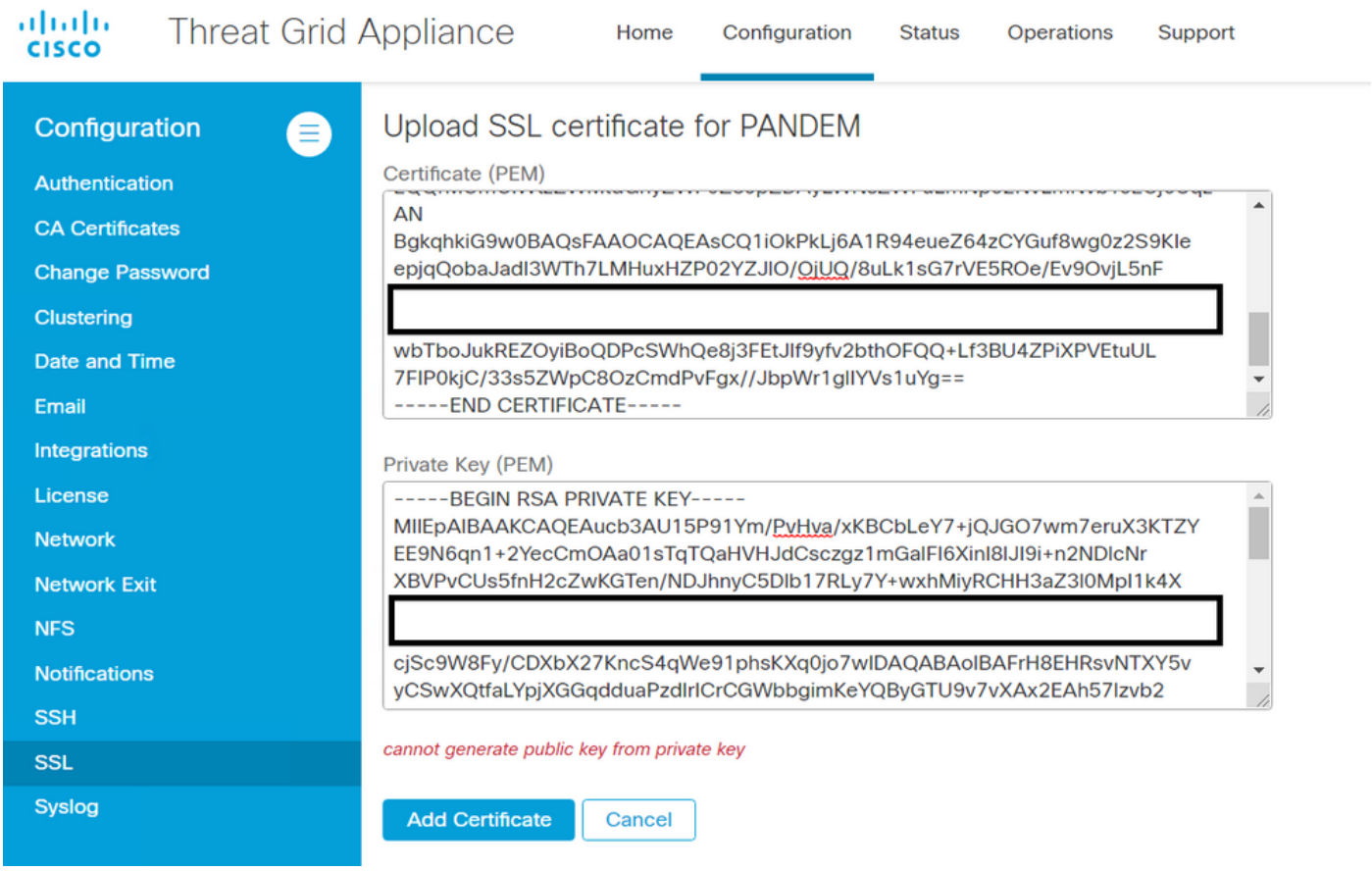
Exemplo. Corrija o formato PEM e os dados dentro de uma chave privada.

```
$ 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-----
```

Mensagem de aviso - Não é possível gerar a chave pública a partir da chave privada

Sintoma

A mensagem de aviso: não é possível gerar uma chave pública a partir da chave privada, é recebido no dispositivo Threat Grid após uma tentativa de adicionar um certificado a uma interface.



A chave pública não pode ser gerada a partir dos dados PEM atuais dentro do arquivo de chave privada.

Etapas recomendadas:

- Confirme a integridade dos dados dentro da chave privada.

Etapa 1. Use a ferramenta OpenSSL para verificar a integridade da chave privada.

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

Se a saída do comando OpenSSL não for **RSA Key ok**, isso significa que foram encontrados problemas com os dados PEM dentro da chave.

Etapa 2. Use a ferramenta OpenSSL para verificar se a chave pública pode ser exportada da chave privada.

```
openssl rsa -in
```

Exemplo. Falha na exportação de chave pública e uma exportação bem-sucedida de chave pública.

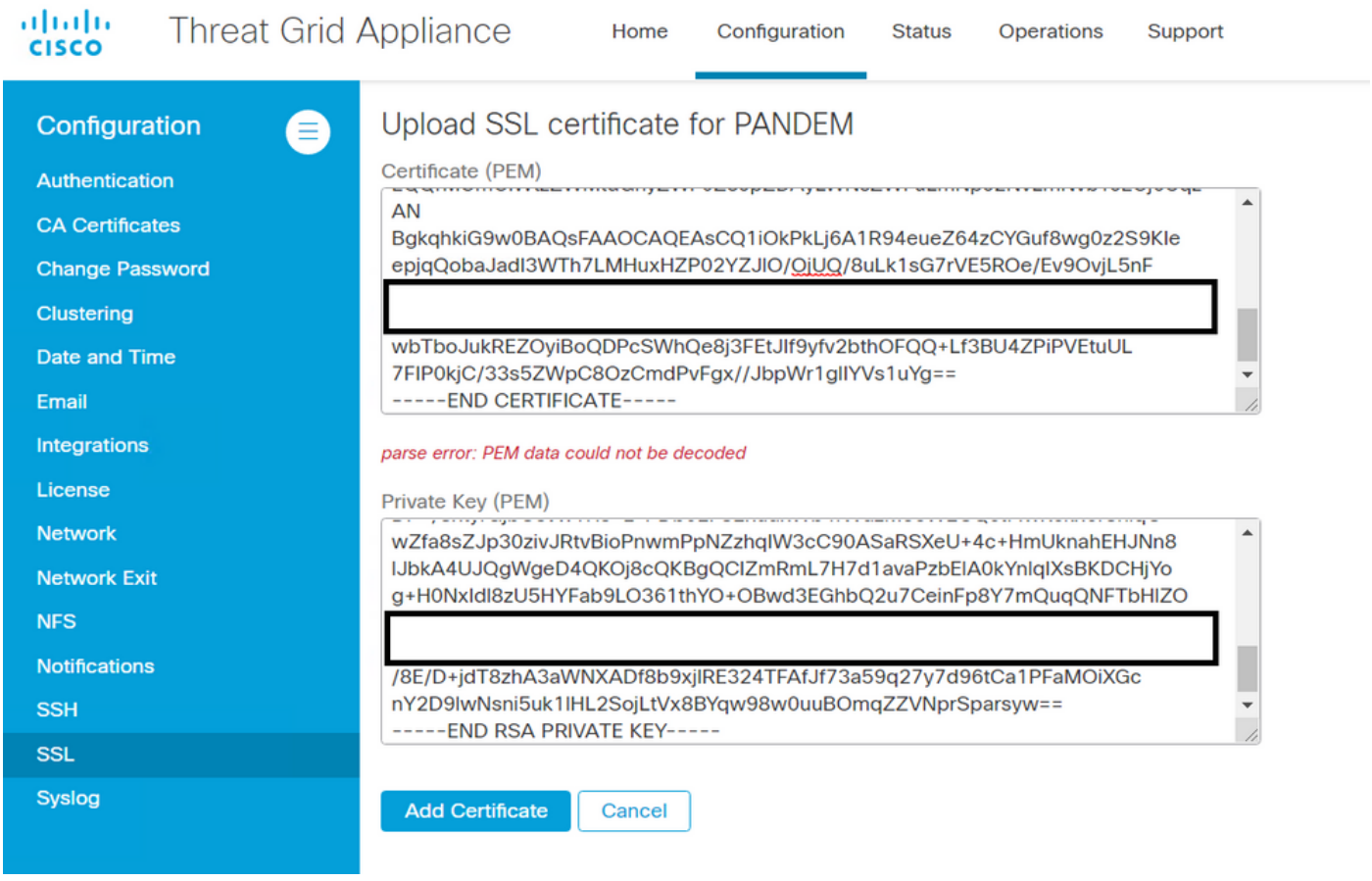
```
$ openssl rsa -in wrong-private-key.key -pubout
unable to load Private Key
140195161523520:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

$ 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-----
```

Mensagem de aviso - erro de análise: Não foi possível decodificar os dados PEM

Sintoma

A mensagem de aviso: erro de análise: Não foi possível decodificar os dados PEM, eles são recebidos no dispositivo Threat Grid após uma tentativa de adicionar um certificado a uma interface.



O certificado não pode ser decodificado dos dados PEM atuais dentro do arquivo de certificado. Os dados PEM dentro do arquivo de certificado estão corrompidos.

- Confirme se as informações do certificado podem ser recuperadas dos dados PEM dentro do arquivo do certificado.

Etapa 1. Use a ferramenta OpenSSL para exibir as informações do certificado do arquivo de

dados PEM.

`openssl x509 -in`

Se os dados PEM estiverem corrompidos, um erro será percebido quando a ferramenta OpenSSL tentar carregar as informações do certificado.

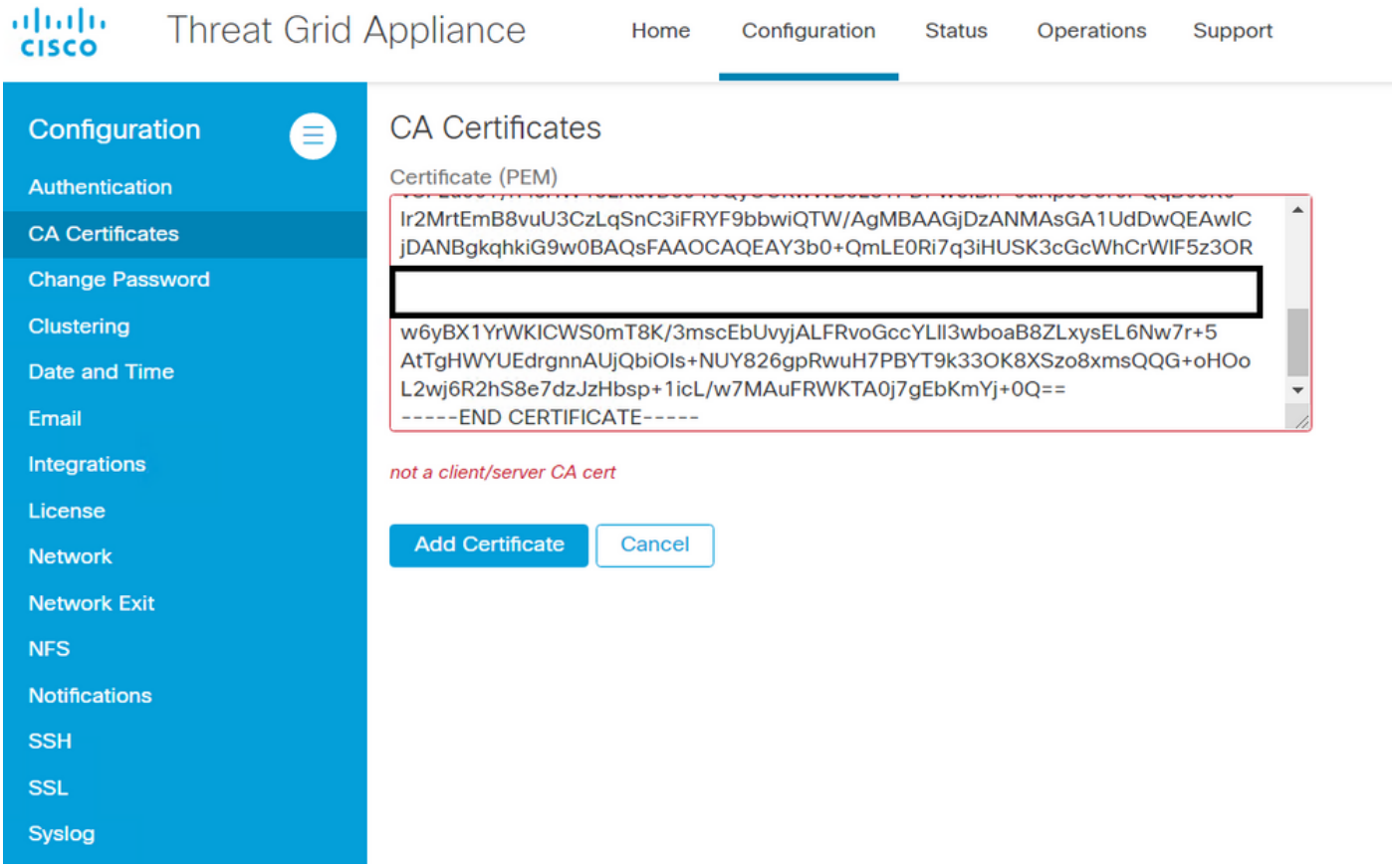
Exemplo. Falha ao tentar carregar as informações do certificado devido a dados PEM corrompidos no arquivo de certificado.

```
$ 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:
```

Mensagem de aviso - não um certificado CA cliente/servidor

Sintoma

A mensagem de aviso: erro de análise: não é um certificado CA cliente/servidor, é recebido no dispositivo Threat Grid após uma tentativa de adicionar um certificado CA a **Configuração > Certificados CA**.



O valor da extensão de Restrições Básicas no certificado CA não está definido como CA: Verdadeiro.

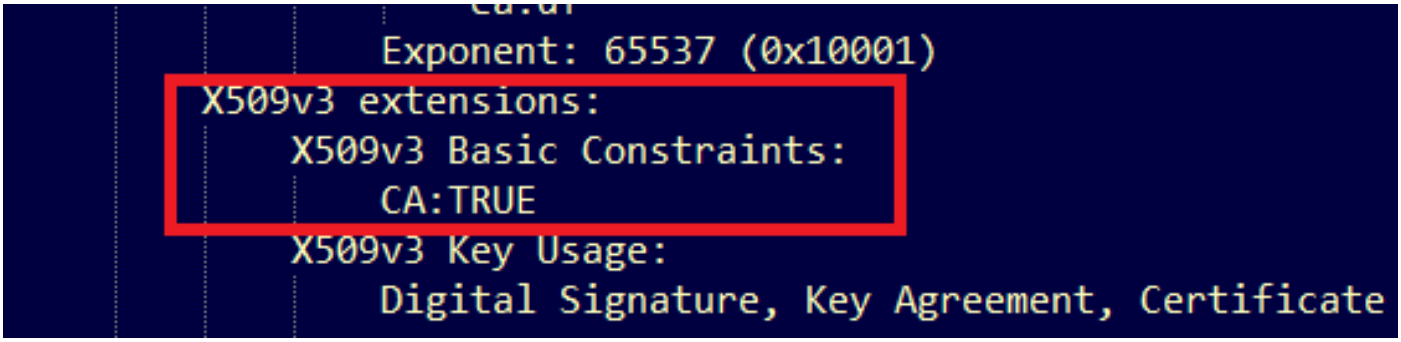
Confirme com a ferramenta OpenSSL se o valor da extensão de Restrições Básicas está definido como CA: Verdadeiro no certificado CA.

Etapa 1. Use a ferramenta OpenSSL para exibir as informações do certificado do arquivo de dados PEM.

```
openssl x509 -in
```

Etapa 2. Pesquise nas informações do certificado o valor atual da extensão **de Restrições Básicas**.

Exemplo. Valor de restrição básica para uma CA aceita pelo dispositivo Threat Grid.



Informações Relacionadas

- Dispositivo Threat Grid - Guias de configuração
- Cisco AMP Virtual Private Cloud Appliance - Exemplos de configuração e notas técnicas
- Suporte Técnico e Documentação - Cisco Systems