Usar OpenAPI para recuperar informações de certificado do ISE no ISE 3.3

Contents

Introdução

Este documento descreve o procedimento para utilizar o openAPI para gerenciar o certificado do Cisco Identity Services Engine (ISE).

Background

Diante da crescente complexidade no gerenciamento e na segurança da rede corporativa, o Cisco ISE 3.1 apresenta APIs formatadas com OpenAPI que otimizam o gerenciamento do ciclo de vida dos certificados, oferecendo uma interface padronizada e automatizada para operações de certificação eficientes e seguras, ajudando os administradores a aplicar práticas de segurança sólidas e manter a conformidade da rede.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Identity Services Engine (ISE)
- API REST
- Python

Componentes Utilizados

- ISE 3.3
- Python 3. 10. 0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

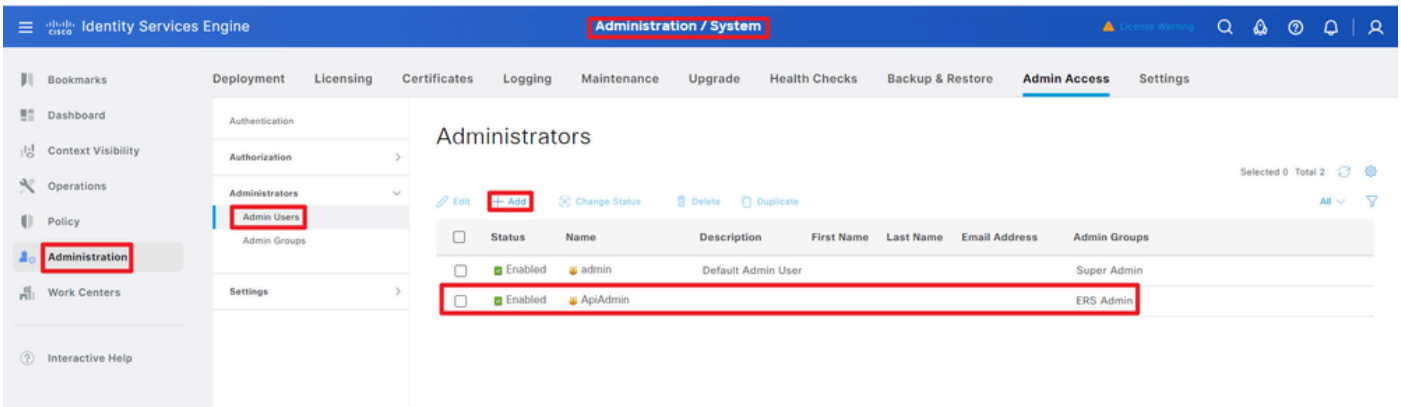
Diagrama de Rede

Topologia

Configuração no ISE

Etapa 1: Adicione uma conta de administrador da API aberta

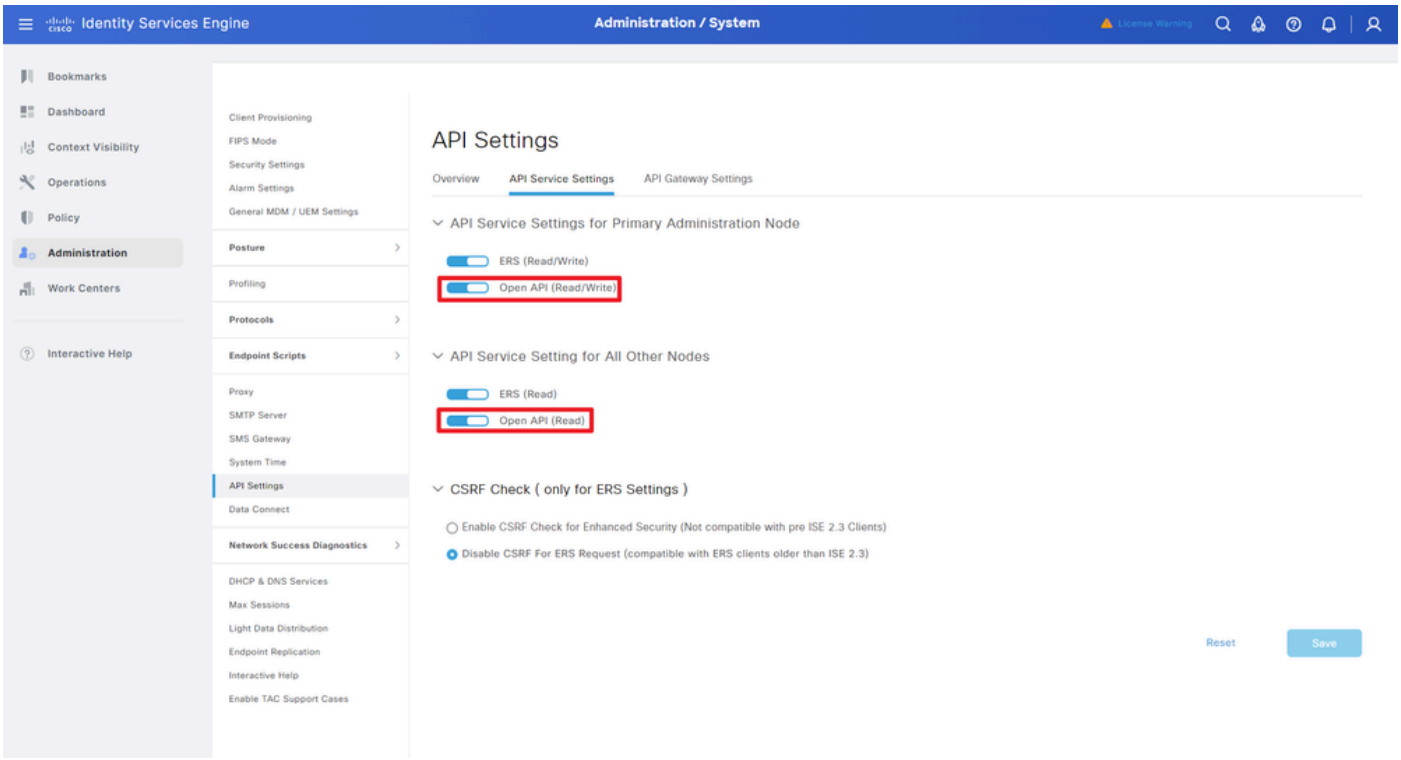
Para adicionar um administrador de API, navegue para Administração -> Sistema -> Administração -> Administradores -> Usuários Admin -> Adicionar.



Administrador de API

Etapa 2: Habilitar API aberta no ISE

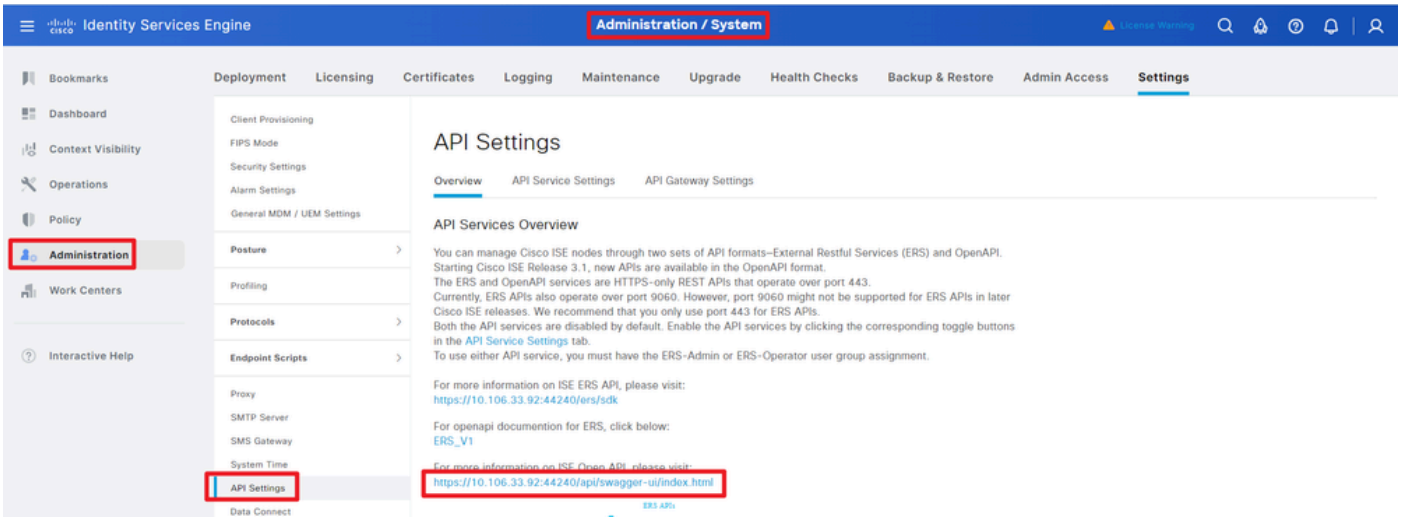
A API aberta é desabilitada por padrão no ISE. Para habilitá-la, navegue até Administração > Sistema > Configurações de API > Configurações de serviço de API. Alterne as opções da API aberta. Click Save.



Habilitar OpenAPI

Etapa 3: Explorar a API aberta do ISE

navegue até Administração > Sistema > Configurações de API > Visão geral. Clique no link de visita à API aberta.



Visite o OpenAPI

Exemplos Python

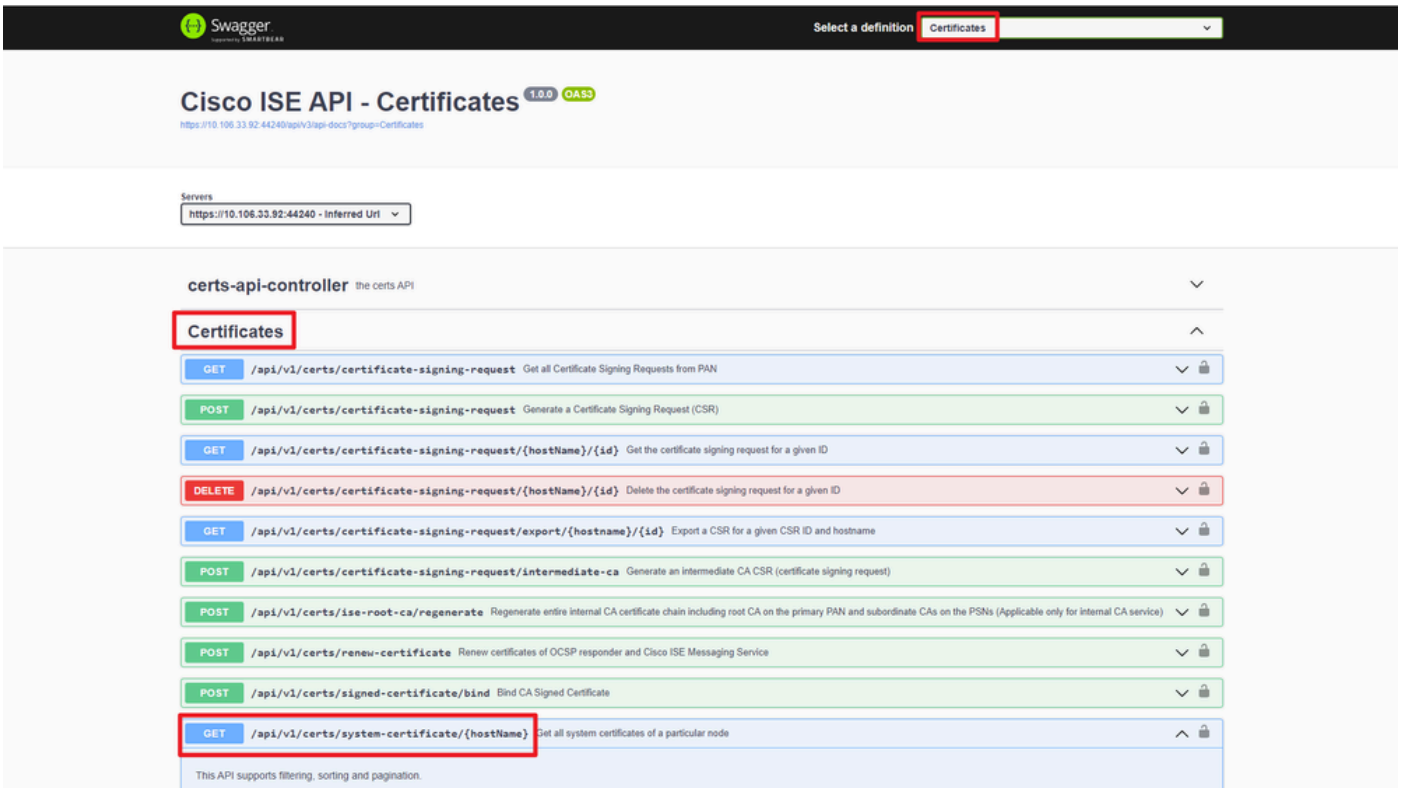
Obter Todos Os Certificados De Sistema De Um Nó Específico

A API lista todos os certificados de um determinado nó do ISE.

Etapa 1: Informações necessárias para uma chamada à API.

Método	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>
Credenciais	Usar credenciais de conta da API aberta
Cabeçalhos	Aceitar: application/json Tipo de conteúdo: application/json

Etapa 2: Localize o URL que é utilizado para recuperar certificados de um nó ISE específico.



URI de API

Etapa 3: Aqui está o exemplo do código Python. Copie e cole o conteúdo. Substitua o IP, o nome de usuário e a senha do ISE. Salve como um arquivo python para executar.

Verifique a boa conectividade entre o ISE e o dispositivo que está executando o exemplo de código python.

<#root>

```
from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

    url = "
https://10.106.33.92/api/v1/certs/system-certificate/ISE-DLC-CFME02-PSN
```

```
"
    headers = {
"Accept": "application/json", "Content-Type": "application/json"
}
    basicAuth = HTTPBasicAuth(
"ApiAdmin", "Admin123"
)

    response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
    print("Return Code:")
    print(response.status_code)
    print("Expected Outputs:")
    print(response.json())
```

Aqui está o exemplo de saídas esperadas.

```
Return Code:
200
Expected Outputs:
{'response': [{'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME0
```

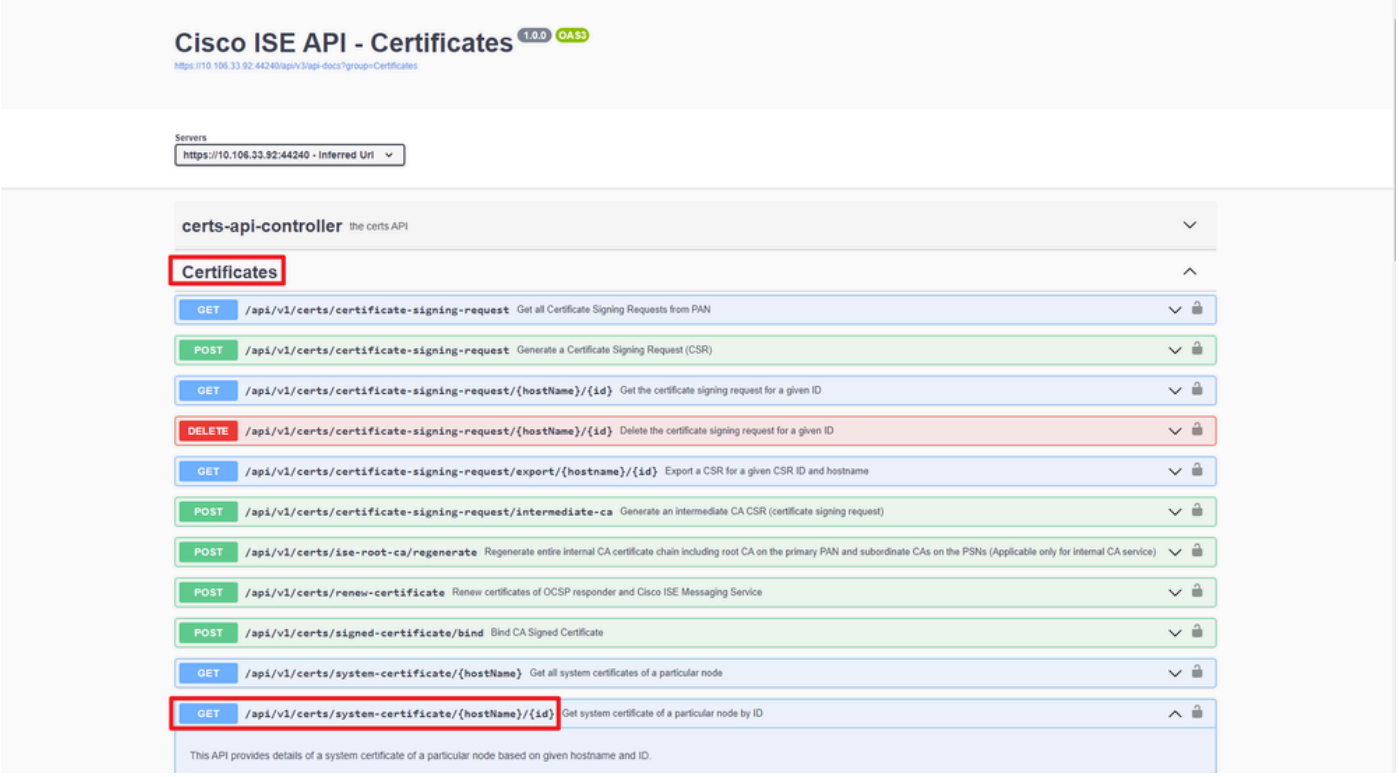
Obter Certificado Do Sistema De Um Nó Específico Por ID

Esta API fornece detalhes de um certificado de sistema de um nó específico com base em um nome de host e ID fornecidos.

Etapa 1: Informações necessárias para uma chamada à API.

Método	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-Of-Certificate>
Credenciais	Usar credenciais de conta da API aberta
Cabeçalhos	Aceitar: application/json Tipo de conteúdo: application/json

Etapa 2: Localize o URL que é utilizado para recuperar o certificado de um nó específico com base no nome do host e ID fornecidos.



URI de API

Etapa 3: Aqui está o exemplo do código Python. Copie e cole o conteúdo. Substitua o IP, o nome de usuário e a senha do ISE. Salve como um arquivo python para executar.

Verifique a boa conectividade entre o ISE e o dispositivo que está executando o exemplo de código python.

<#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/system-certificate/ISE-DLC-CFME02-PSN/5b5b28e4-2a51-495c-8413-610190e1

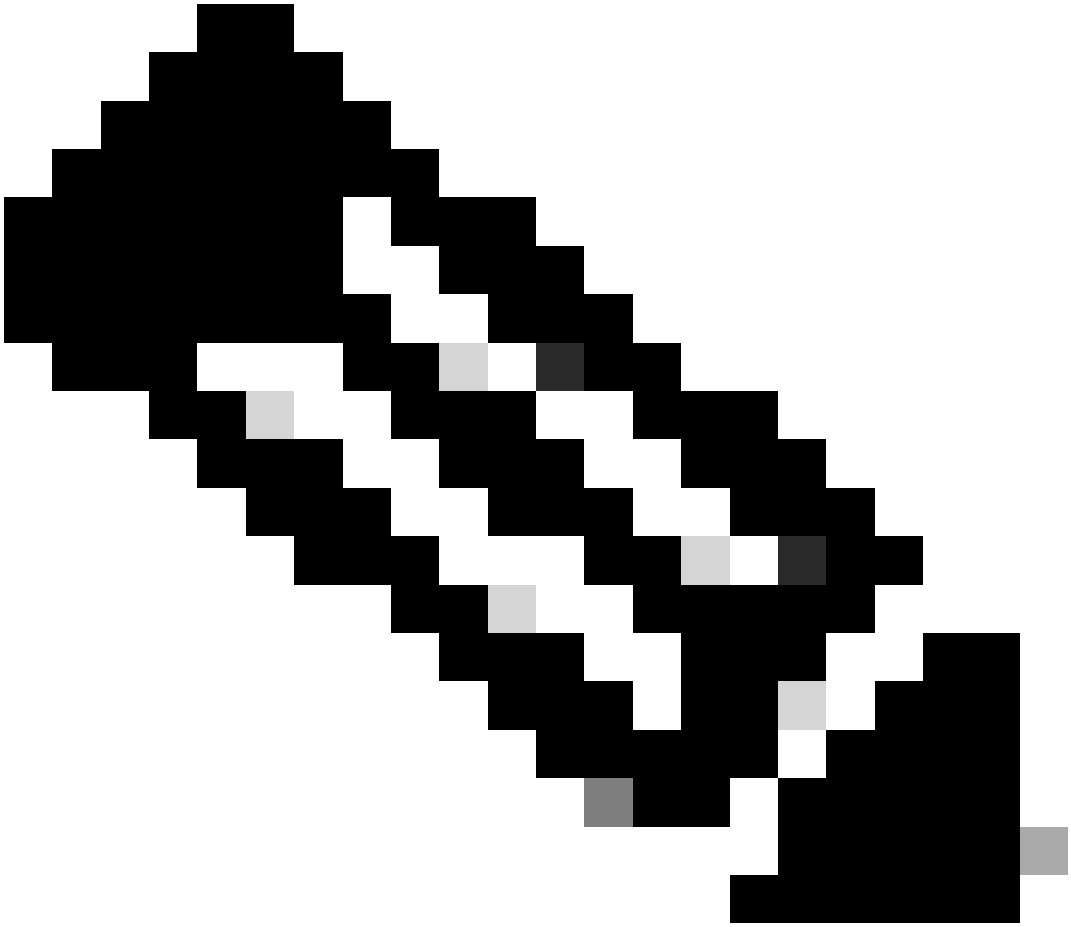
" headers = {

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")



Observação: o ID é das saídas de API na etapa 3 de "Obter todos os certificados de sistema de um nó específico", por exemplo, 5b5b28e4-2a51-495c-8413-610190e1070b é "Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com".

Aqui está o exemplo de saídas esperadas.

Return Code:
200
Expected Outputs:
{'response': {'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02

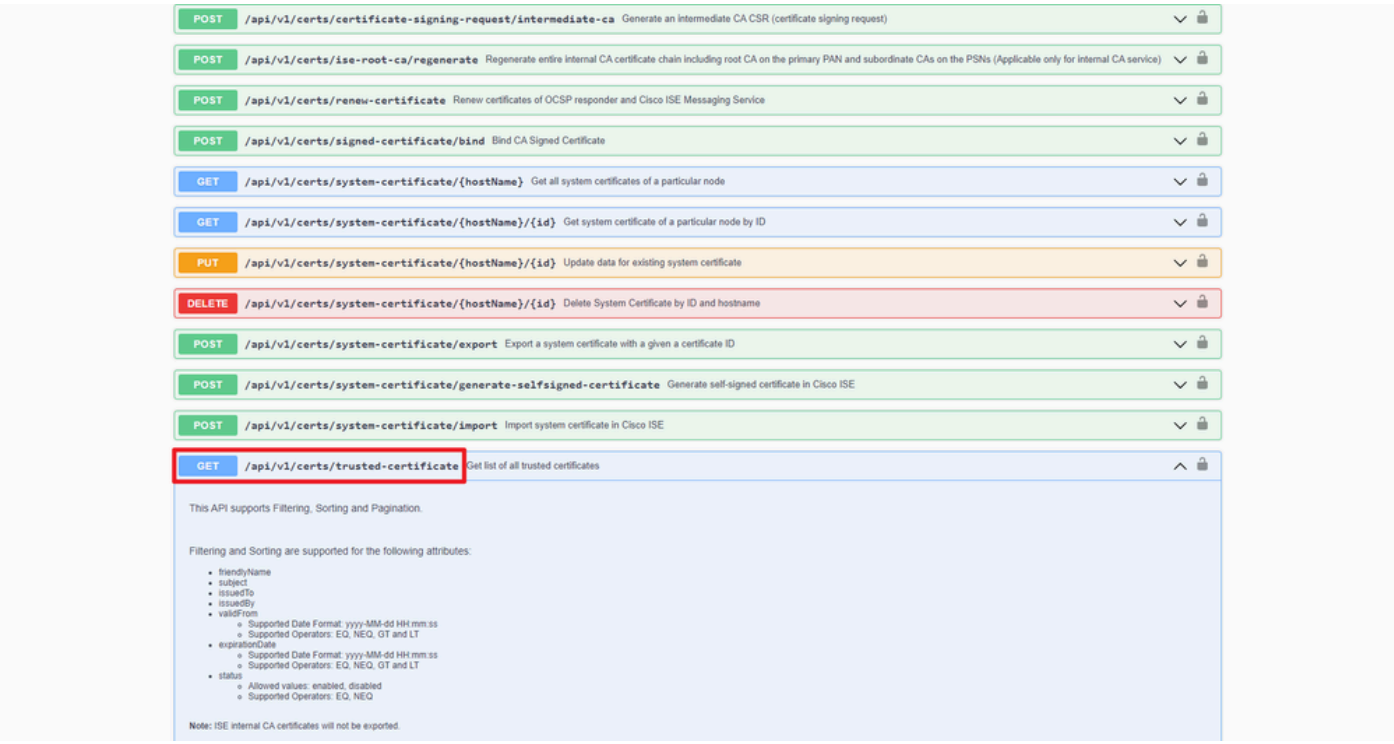
Obter Lista De Todos Os Certificados De Confiabilidade

A API lista todos os certificados confiáveis do cluster do ISE.

Etapa 1: Informações necessárias para uma chamada à API.

Método	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate
Credenciais	Usar credenciais de conta da API aberta
Cabeçalhos	Aceitar: application/json Tipo de conteúdo: application/json

Etapa 2: Localize o URL utilizado para recuperar certificados confiáveis.



URI de API

Etapa 3: Aqui está o exemplo do código Python. Copie e cole o conteúdo. Substitua o IP, o nome de usuário e a senha do ISE. Salve como um arquivo python para executar.

Verifique a boa conectividade entre o ISE e o dispositivo que está executando o exemplo de código python.

<#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/trusted-certificate

" headers = {

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

```
"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")
```

Aqui está o exemplo de saídas esperadas.(Omitido)

```
Return Code:
200
Expected Outputs:
{'response': [{'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Authority', 'subject': 'CN=Ver
```

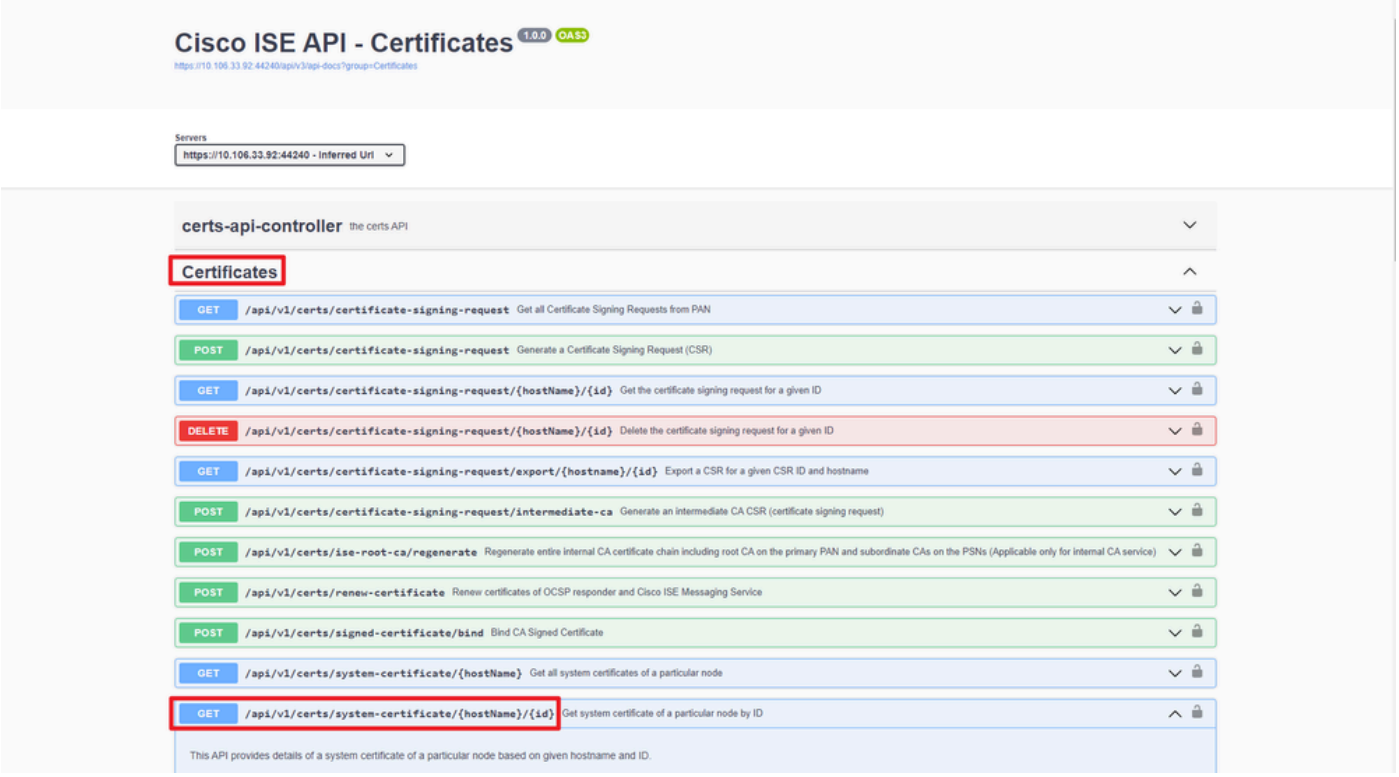
Obter Certificado de Confiança por ID

Esta API pode exibir detalhes de um Certificado de Confiança com base em uma determinada ID.

Etapa 1: Informações necessárias para uma chamada à API.

Método	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate/<ID-Of-Certificate>
Credenciais	Usar credenciais de conta da API aberta
Cabeçalhos	Aceitar: application/json Tipo de conteúdo: application/json

Etapa 2: Localize o URL que é utilizado para recuperar informações de implantação.



URI de API

Etapa 3: Aqui está o exemplo do código Python. Copie e cole o conteúdo. Substitua o IP, o nome de usuário e a senha do ISE. Salve como um arquivo python para executar.

Verifique a boa conectividade entre o ISE e o dispositivo que está executando o exemplo de código python.

<#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/trusted-certificate/147d97cc-6ce9-43d7-9928-8cd0fa83e140

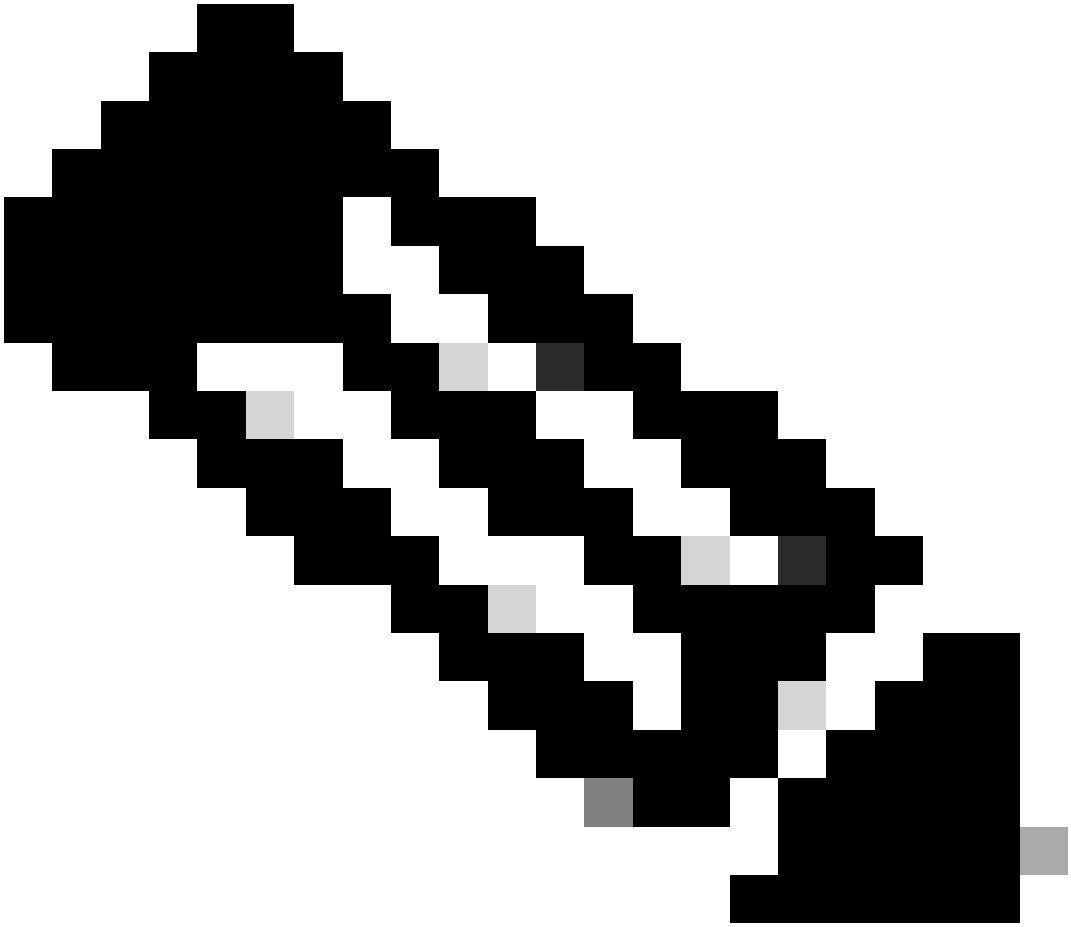
" headers = {

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")



Observação: a ID é de saídas de API na etapa 3 de "Obter lista de todos os certificados confiáveis", por exemplo, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 é "VeriSign Class 3 Public Primary Certification Authority".

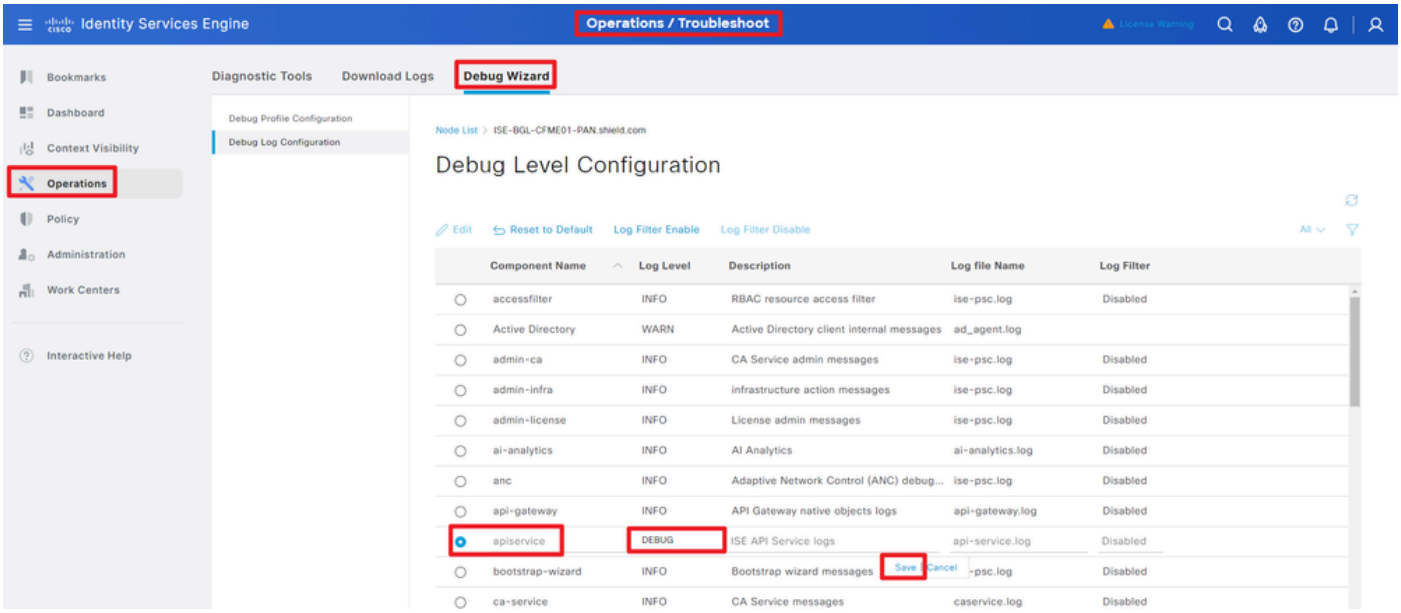
Aqui está o exemplo de saídas esperadas.

Return Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certifi

Troubleshooting

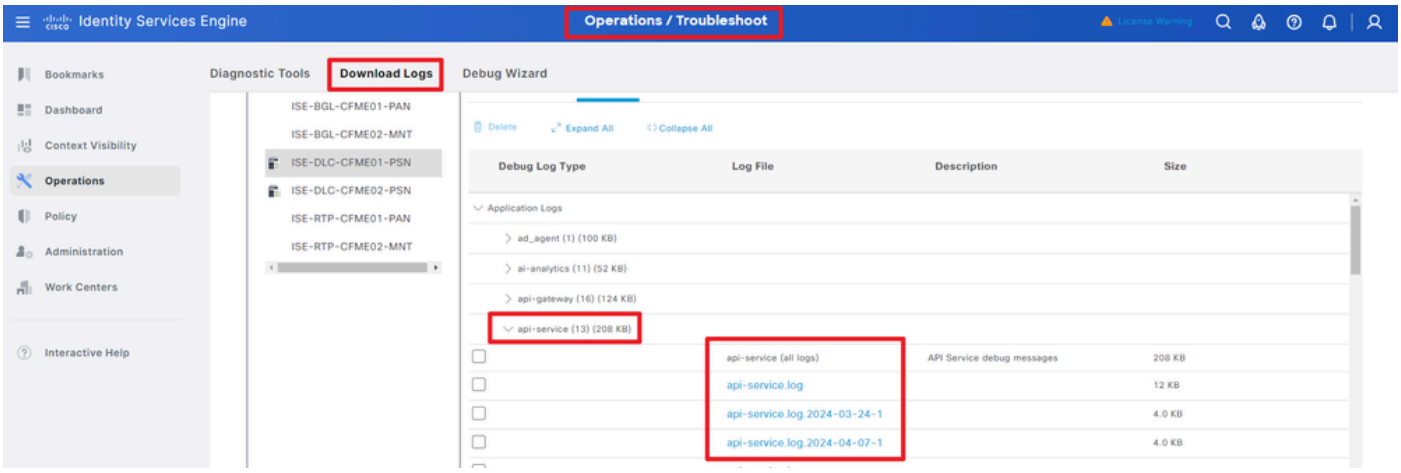
Para solucionar problemas relacionados às APIs abertas, defina **oNível de Log** para theapiservicecomponent paraDEBUGin theDebug Log janela de Configuração.

Para habilitar a depuração, navegue até **Operations -> Troubleshoot -> Debug Wizard -> Debug Log Configuration -> ISE Node -> apiservice.**



Depuração do Serviço de API

Para fazer o download de logs de depuração, navegue até **Operations -> Troubleshoot -> Download Logs -> ISE PAN Node -> Debug Logs.**



Logs de depuração de download

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.