

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

Contents

[Introdução](#)

[Background](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração no ISE](#)

[Exemplos Python](#)

[Obter Todos Os Certificados De Sistema De Um Nó Específico](#)

[Obter Certificado Do Sistema De Um Nó Específico Por ID](#)

[Obter Lista De Todos Os Certificados De Confiabilidade](#)

[Obter Certificado de Confiança por ID](#)

[Troubleshooting](#)

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

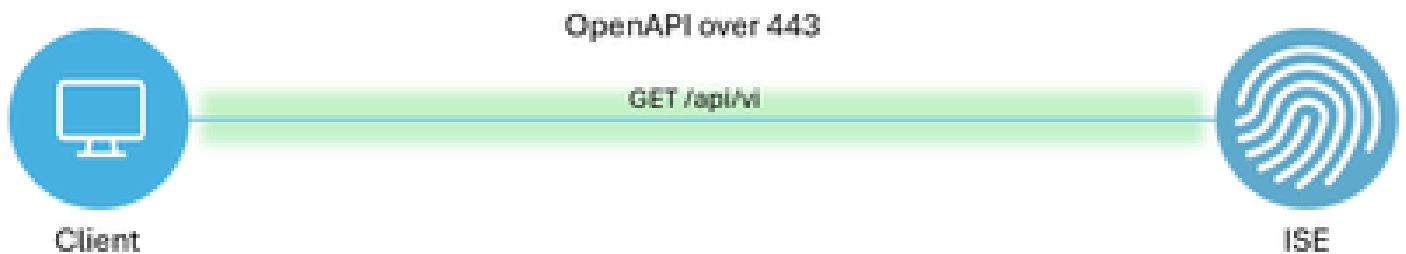
Componentes Utilizados

- 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.

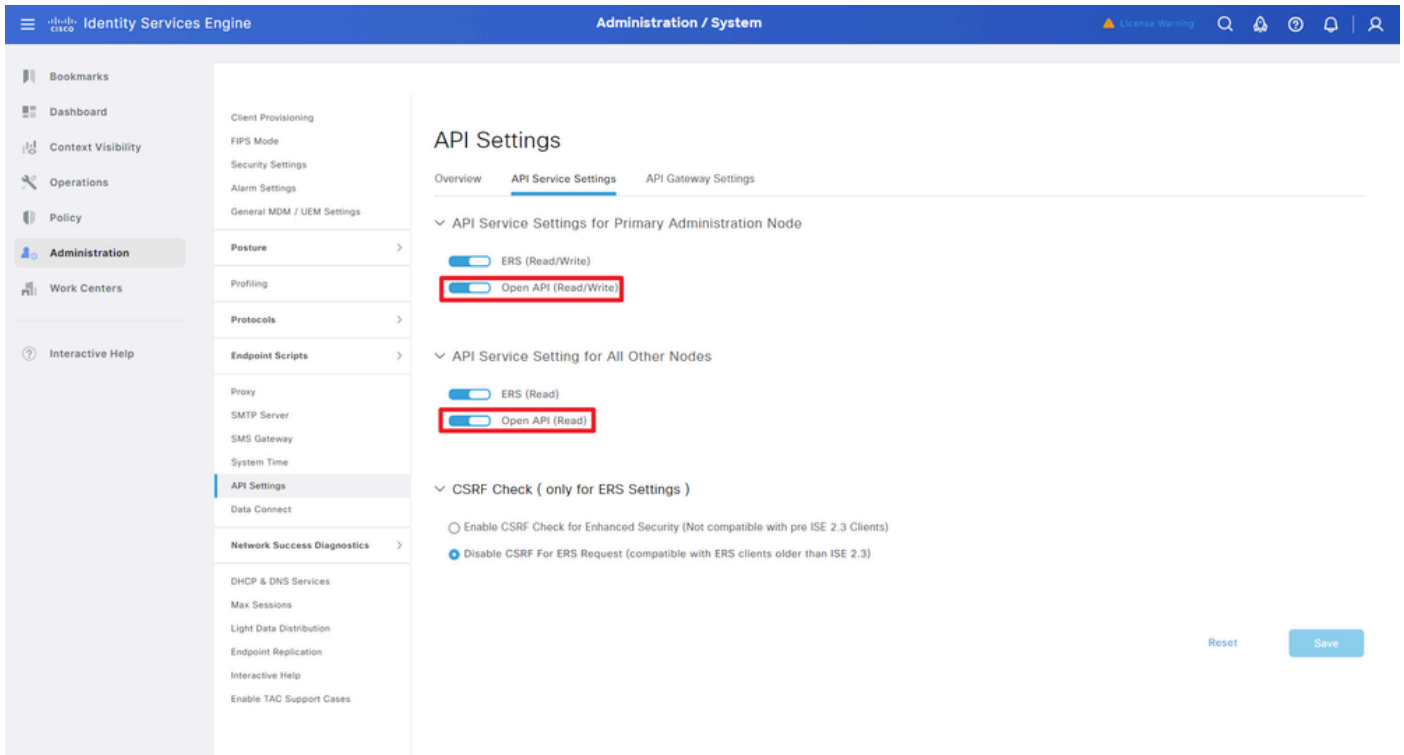
A captura de tela mostra a interface de administração do Identity Services Engine (ISE). O menu de navegação à esquerda tem 'Administration' selecionado. No topo, 'Administration / System' está destacado. O painel principal exibe a seção 'Administrators' com uma tabela de usuários administradores.

Status	Name	Description	First Name	Last Name	Email Address	Admin Groups
<input type="checkbox"/>	Enabled	admin				Super Admin
<input type="checkbox"/>	Enabled	ApiAdmin				ERS Admin

Administrador de API

Etapa 2: Habilitar API aberta no ISE

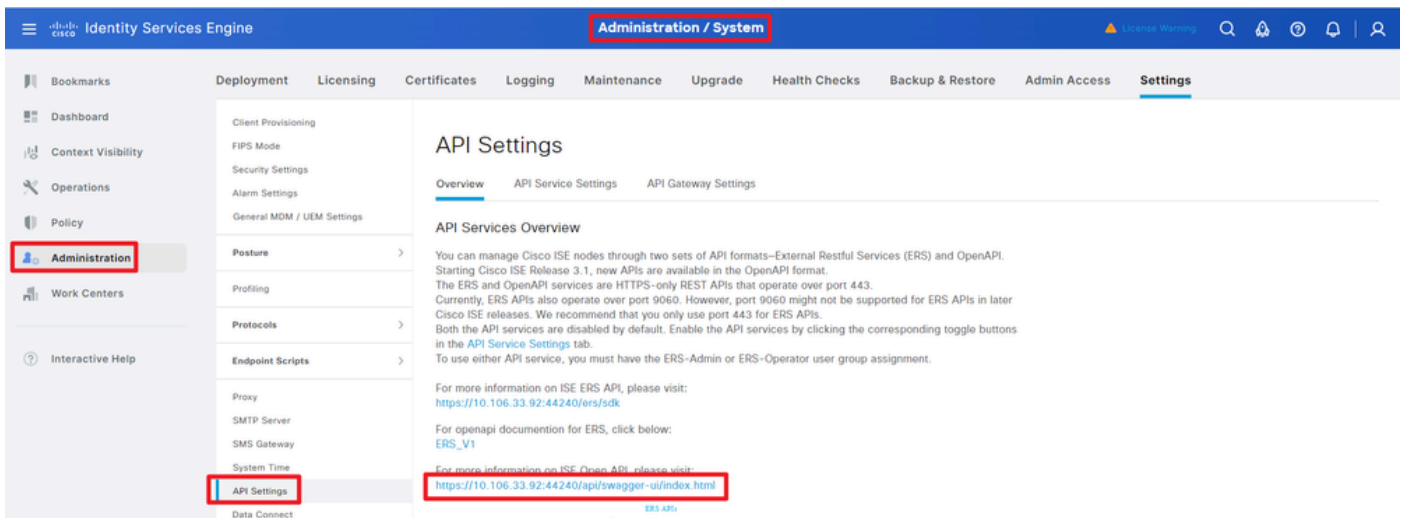
A API aberta é desabilitada por padrão no ISE. Para habilitá-la, navegue até Administração > Sistema > Configurações de API > Configurações de serviço de API. Alterne as opções da API aberta. Click Save.



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

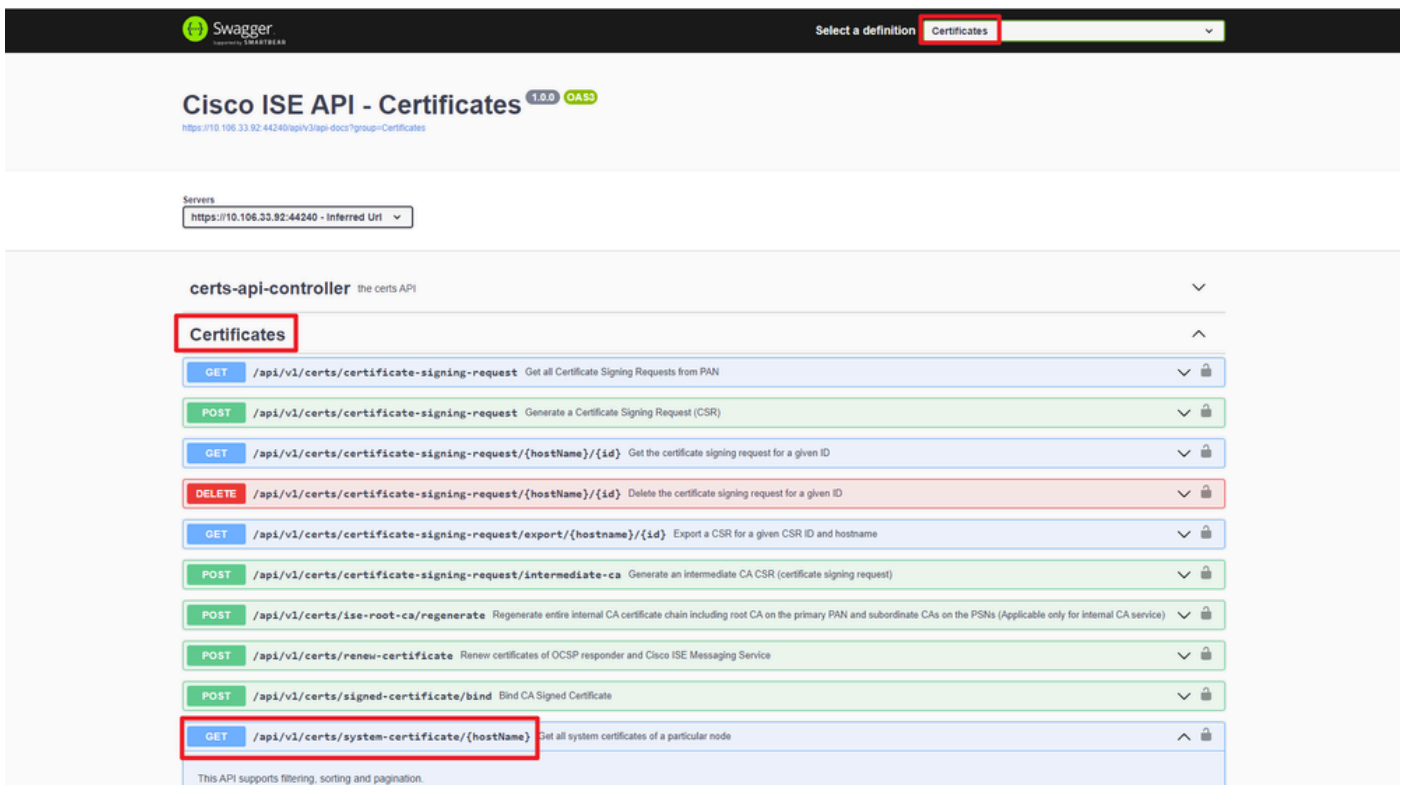
Obter Todos Os Certificados De Sistema De Um Nó Específico

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.

Cisco ISE API - Certificates 1.0.0 OAS3

<https://10.106.33.92:44240/api/v3/app-docs?group=Certificates>

Servers
<https://10.106.33.92:44240> - Inferred Url

certs-api-controller the certs API

Certificates

GET	/api/v1/certs/certificate-signing-request	Get all Certificate Signing Requests from PAN	🔒
POST	/api/v1/certs/certificate-signing-request	Generate a Certificate Signing Request (CSR)	🔒
GET	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Get the certificate signing request for a given ID	🔒
DELETE	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Delete the certificate signing request for a given ID	🔒
GET	/api/v1/certs/certificate-signing-request/export/{hostname}/{id}	Export a CSR for a given CSR ID and hostname	🔒
POST	/api/v1/certs/certificate-signing-request/intermediate-ca	Generate an intermediate CA CSR (certificate signing request)	🔒
POST	/api/v1/certs/ise-root-ca/regenerate	Regenerate entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)	🔒
POST	/api/v1/certs/renew-certificate	Renew certificates of OCSF responder and Cisco ISE Messaging Service	🔒
POST	/api/v1/certs/signed-certificate/bind	Bind CA Signed Certificate	🔒
GET	/api/v1/certs/system-certificate/{hostName}	Get all system certificates of a particular node	🔒
GET	/api/v1/certs/system-certificate/{hostName}/{id}	Get system certificate of a particular node by ID	🔒

This API provides details of a system certificate of a particular node based on given hostname and ID.

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-PSN.cisco.com'}}
```

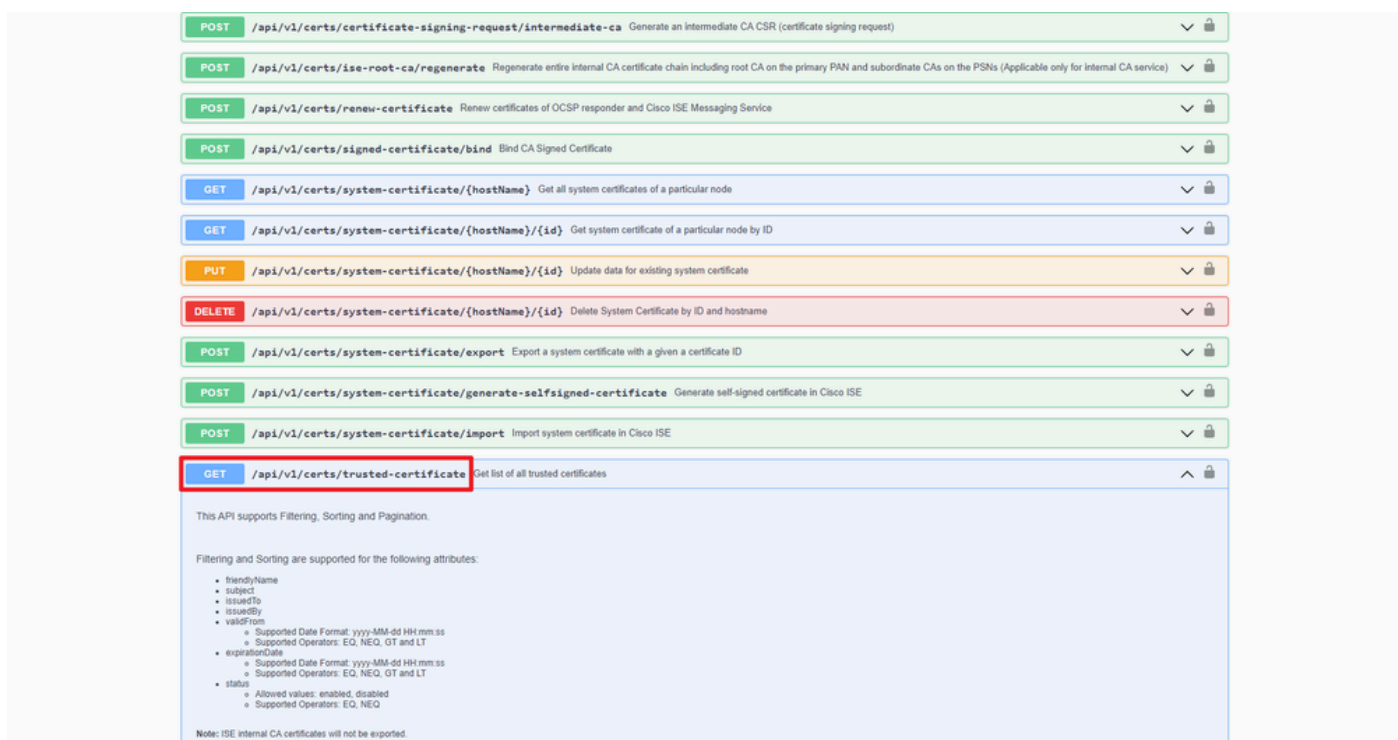
Obter Lista De Todos Os Certificados De Confiabilidade

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.



The screenshot displays the Cisco ISE API Explorer interface. It lists various API endpoints with their methods and descriptions. The endpoint `/api/v1/certs/trusted-certificate` is highlighted with a red box, indicating it is the target for the current step. Below the list, there is a section for filtering and sorting attributes, including `friendlyName`, `subject`, `issuedTo`, `issuedBy`, `validFrom`, `expirationDate`, and `status`. A note at the bottom states: "Note: ISE internal CA certificates will not be exported."

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.

Cisco ISE API - Certificates 1.0.0 OAS3

<https://10.106.33.92:44240/api/v1/certs/docs?group=Certificates>

Servers

certs-api-controller the certs API		⌵
Certificates ⌵		
GET	/api/v1/certs/certificate-signing-request	Get all Certificate Signing Requests from PAN
POST	/api/v1/certs/certificate-signing-request	Generate a Certificate Signing Request (CSR)
GET	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Get the certificate signing request for a given ID
DELETE	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Delete the certificate signing request for a given ID
GET	/api/v1/certs/certificate-signing-request/export/{hostname}/{id}	Export a CSR for a given CSR ID and hostname
POST	/api/v1/certs/certificate-signing-request/intermediate-ca	Generate an intermediate CA CSR (certificate signing request)
POST	/api/v1/certs/ise-root-ca/regenerate	Regenerate entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)
POST	/api/v1/certs/renew-certificate	Renew certificates of OCSF responder and Cisco ISE Messaging Service
POST	/api/v1/certs/signed-certificate/bind	Bind CA Signed Certificate
GET	/api/v1/certs/system-certificate/{hostName}	Get all system certificates of a particular node
GET	/api/v1/certs/system-certificate/{hostName}/{id}	Get system certificate of a particular node by ID
This API provides details of a system certificate of a particular node based on given hostname and ID.		

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 Certif

Troubleshooting

Para solucionar problemas relacionados às APIs abertas, defina o **Nível de Log** para theapiservicecomponent para **DEBUG** in the Debug Log janela de Configuração.

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

The screenshot shows the Identity Services Engine interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / Troubleshoot'. The left sidebar has 'Operations' highlighted. The main content area shows the 'Debug Wizard' section with 'Debug Log Configuration' selected. A table lists various components and their log levels. The 'apiservice' component is selected, and its log level is set to 'DEBUG'. The 'Save' button is highlighted.

Component Name	Log Level	Description	Log file Name	Log Filter
accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled
Active Directory	WARN	Active Directory client internal messages	ad_agent.log	Disabled
admin-ca	INFO	CA Service admin messages	ise-psc.log	Disabled
admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled
admin-license	INFO	License admin messages	ise-psc.log	Disabled
ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled
anc	INFO	Adaptive Network Control (ANC) debug...	ise-psc.log	Disabled
api-gateway	INFO	API Gateway native objects logs	api-gateway.log	Disabled
apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled
bootstrap-wizard	INFO	Bootstrap wizard messages	psc.log	Disabled
ca-service	INFO	CA Service messages	caservice.log	Disabled

Depuração do Serviço de API

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

The screenshot shows the Identity Services Engine interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / Troubleshoot'. The left sidebar has 'Operations' highlighted. The main content area shows the 'Download Logs' section with 'Debug Logs' selected. A table lists various debug log types and their sizes. The 'api-service' log type is selected, and the 'api-service.log' file is highlighted for download.

Debug Log Type	Log File	Description	Size
Application Logs			
>	ad_agent (1) (100 KB)		
>	ai-analytics (11) (52 KB)		
>	api-gateway (16) (124 KB)		
>	api-service (13) (208 KB)		
<input type="checkbox"/>	api-service (all logs)	API Service debug messages	208 KB
<input type="checkbox"/>	api-service.log		12 KB
<input type="checkbox"/>	api-service.log.2024-03-24-1		4.0 KB
<input type="checkbox"/>	api-service.log.2024-04-07-1		4.0 KB

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.