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.

=	abale Identity Services I	Engine			Administra	tion / Syste	m			License Warning	0	Δ	ര		0
-	cisco la citat y contractor	Lingino									~	040	•	ΨI	\sim
Щ	Bookmarks	Deployment Licensing	Certifica	tes Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings					
5	Dashboard	Authentication	Δ.	ministrat	ors										
망	Context Visibility	Authorization	> ^	anninstrat	013						5	elected () Total 2	ø	٥
*	Operations	Administrators	~ /	dit + Add	Change Status	Delete D	Duplicate							u ~	∇
-0	Policy	Admin Users													
20	Administration	Admin Groups		Status	admin a	Descripti Default A	dmin User	Last Name Email Ac	ddress Admin Gr Super Ad	Imin					
nii.	Work Centers	Settings	<u> </u>	Enabled	a ApiAdmin				ERS Adm	in					
?	Interactive Help														

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.

≡	≡ dudio Identity Services Engine				Administration / System						🔺 License Warning			0	Q Q				
д	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings								
	Dashboard	Client Provisioni	ng																
명	Context Visibility	FIPS Mode Security Settings		API S	ettings	Services ADLO	Carling												
- X - 0	Operations Policy	Alarm Settings General MDM / U	JEM Settings	API Serv	ices Overvie														
80	Administration	Posture		> You can ma Starting Cit	anage Cisco ISE sco ISE Release	nodes through two s 3.1, new APIs are av	ets of API forma railable in the Op	its-External Restful Ser enAPI format.	rvices (ERS) and OpenAPI.										
di.	Work Centers	Profiling		The ERS ar Currently, I	nd OpenAPI sen ERS APIs also o	vices are HTTPS-only perate over port 9060	REST APIs that However, port	operate over port 443. 9060 might not be sup	opported for ERS APIs in late	r									
		Protocols		> Cisco ISE r Both the A	eleases. We rec PI services are o	commend that you on disabled by default. E	ly use port 443 nable the API se	for ERS APIs. rvices by clicking the c	corresponding toggle buttor	15									
?	Interactive Help	Endpoint Scripts		> To use eith	er API service,	you must have the ER	S-Admin or ERS	-Operator user group	assignment.										
	1	Proxy SMTP Server SMS Gateway System Time API Settings		For more in https://10. For openag ERS_V1 For more in https://10.	formation on IS 106.33.92:4424 pi documention i formation on IS 106.33.92:4424	E ERS API, please vis IO/ers/sdk for ERS, click below: E Open API, please x IO/api/swagger-ui/ind	iit: ieit: Jox.html												



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></ise-node-hostname></ise-pan-ip>
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.

	H Swagger. Select a definition Certifica	ates 🗸 🗸	
	Cisco ISE API - Certificates (IDD) (ADD) https://10.106.33.92.44249hp9V3api-docs?group=Centificates		
	Servers https://10.106.33.92.44240 - Inferred Urf v		
	certs-api-controller the certs API	~	
[Certificates	^	
	GET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	~ ≜	
	POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	~ ≞	
	GET /api/vl/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given ID	✓ ≜	
	DELETE /api/vl/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given ID	✓ ≜	
	OET /api/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	~ ≜	
	POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	~ ≜	
	POST /api/vl/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/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	✓ ≜	
	POST /api/vl/certs/signed-certificate/bind Bind CA Signed Centificate	~ ≞	
	GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular mode	^ ≜	
	This API supports filtering, sorting and pagination.		

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></id-of- </ise-node-hostname></ise-pan-ip>
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 (III) (IIII) (III) (IIII) (III) (III) (III) (III) (III) (III)	
Servers https://10.106.33.92:44240 - Inferred Url V	
certs-api-controller the certs API	~
Certificates	^
CET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	 ✓ ≜
POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	✓ ≜
CET /api/vl/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/vi/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	∨ ≜
POST /api/vi/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/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	✓ ≜
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Centificate	✓ ≜
GET /api/vl/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

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</ise-pan-ip>
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.

POST /api/vl/certs/ise-reat-carregenerate Regenerate entry internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for Internal CA service) vi POST /api/vl/certs/renew-certificate Renew certificate of OCSP responder and Cisco ISE Messaging Service vi POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate vi vi GET /api/vl/certs/system-certificate/bind Bind CA Signed Certificate vi vi GET /api/vl/certs/system-certificate/bind Bind CA Signed Certificate vi vi GET /api/vl/certs/system-certificate/(hostName)/(id) Get system certificate of a particular node vi vi PUT /api/vl/certs/system-certificate/(hostName)/(id) Update data for existing system certificate vi vi PUT /api/vl/certs/system-certificate/(hostName)/(id) Delets System Certificate ID vi vi PUST /api/vl/certs/system-certificate/seport Export a system certificate ID vi vi POST /api/vl/certs/system-certificate/seport Export a system certificate ID vi vi POST /api/vl/certs/system-certificate/seport Import system certificate ID vi vi GET /api/vl/certs/system-certificate/seport Import system certificate I	POST /api/vl/certs/certific	ste-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	\sim	e i	à
POST /api/vl/certs/renew-certificate Renew certificates Image: Service POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate Image: Service GET /api/vl/certs/system-certificate/(hostName) Get all system certificates of a particular node Image: Service GET /api/vl/certs/system-certificate/(hostName)/(id) Get system certificate Image: Service PUT /api/vl/certs/system-certificate/(hostName)/(id) Delete System certificate Image: Service PUT /api/vl/certs/system-certificate/(hostName)/(id) Delete System certificate Image: Service PUT /api/vl/certs/system-certificate/(hostName)/(id) Delete System Certificate by ID and hostname Image: Service POST /api/vl/certs/system-certificate/(hostName)/(id) Delete System Certificate in D Image: Service POST /api/vl/certs/system-certificate/(service selfsigned-certificate in D Image: Service Image: Service POST /api/vl/certs/system-certificate/import Import system certificate in Cloco ISE Image: Service POST /api/vl/certs/system-certificate/import Import system certificates in Cloco ISE Image: Service GET /api/vl/certs/system-certificate/import Import s	POST /api/vl/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)	~	e i	à
POST /api/v1/certs/signed-certificate/[hostName] Get al system certificate of a particular node in GET /api/v1/certs/system-certificate/[hostName]/[id] Get system certificate of a particular node in GET /api/v1/certs/system-certificate/[hostName]/[id] Get system certificate of a particular node in GET /api/v1/certs/system-certificate/[hostName]/[id] Get system certificate of a particular node by ID in PUT /api/v1/certs/system-certificate/[hostName]/[id] Update data for existing system certificate in OLLETE /api/v1/certs/system-certificate/[hostName]/[id] Delete System Certificate by ID and hostname in POST /api/v1/certs/system-certificate/export Export a system certificate by ID and hostname in POST /api/v1/certs/system-certificate/export Export a system certificate by ID and hostname in POST /api/v1/certs/system-certificate/export Export a system certificate by ID and hostname in POST /api/v1/certs/system-certificate/export Export a system certificate iD in POST /api/v1/certs/system-certificate/import Import system certificate iD in POST /api/v1/certs/system-certificate/ import system certificate in Cisco ISE <td>POST /api/vl/certs/renew-ce</td> <td>rtificate Renew certificates of OCSP responder and Cisco ISE Messaging Service</td> <td>~</td> <td>e i</td> <td>à</td>	POST /api/vl/certs/renew-ce	rtificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	~	e i	à
GET /api/vl/certs/system-certificate/{hostName}} Get all system certificates of a particular node in GET /api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID in GET /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate in PUT /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate in GELETE /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate in POST /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate ID in POST /api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE in POST /api/vl/certs/system-certificate/import Import system certificates in CET /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE in CET /api/vl/certs/trusted-certificate Cet is of all trusted certificates in This API supports Filtering. Sorting and Pagination. in in in	POST /api/vl/certs/signed-co	ertificate/bind Bind CA Signed Centificate	~	e i	à
GET /api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID PUT /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate OELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname OELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname POST /api/vl/certs/system-certificate/expert Expont a system certificate iD POST /api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Clico ISE POST /api/vl/certs/system-certificate/import Import system certificate in Clico ISE if POST /api/vl/certs/system-certificate Cell Int of all trusted certificates if POST /api/vl/certs/trusted-certificate Cell Int of all trusted certificates if This API supports Filtering. Sorting and Pagination. Filtering and Sorting are supported for the following attributes: if * Supported Supported Date Format: yyyAMA defH mm ss Supported Date Format: yyyAMA defH mm ss * Su	GET /api/vl/certs/system-ce	ertificate/{hostName} Get all system certificates of a particular node	\sim	e i	à
PUT /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate in DELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname in POST /api/vl/certs/system-certificate/knowth agiven a certificate D in POST /api/vl/certs/system-certificate/export Export a system certificate Centrate self-signed certificate in Cisco ISE in POST /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE in POST /api/vl/certs/system-certificate Cell for all trusted certificates in POST /api/vl/certs/system-certificate Cell for all trusted certificates in POST /api/vl/certs/system-certificate Cell for all trusted certificates in This API supports Fillering. Sorting and Pagination. Fillering and Sorting are supported for the following attributes: in • Supported Set	GET /api/vl/certs/system-co	<pre>prtificate/{hostName}/{id} Get system certificate of a particular node by ID</pre>	~	- 1	à
OELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname POST /api/vl/certs/system-certificate/export Export a system certificate bit a given a certificate ID POST /api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE POST /api/vl/certs/system-certificate/generate-selfsigned-certificate in Cisco ISE POST /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE GET /api/vl/certs/trusted-certificate Cell Int of all trusted certificates This API supports Filtering. Sorting and Pagination. Filtering and Sorting are supported for the following attributes: • Supported Date Format yyyAMA del Hum rss	PUT /api/v1/certs/system-co	<pre>artificate/{hostName}/{id} Update data for existing system certificate</pre>	\sim	e i	h
POST /api/vl/certs/system-certificate/export Export a system certificate ID POST /api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE POST /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE in POST /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE in CET /api/vl/certs/trusted-certificate Cet I del that de certificates in This API supports Filtering. Sorting and Pagination. Filtering and Sorting are supported for the following attributes: in • Supported Supported Date Format_tyywAM-dd H4 mm st in • Supported Cate Contents Cate Contents Cate Contents in • Supported Cate Contents Cate Contents Cate Contents in • Supported Cate Contents Cate Contents Cate Contents in • Supported Cate Contents Cate Contents Cate Contents in • Supported Cate Contents Cate Contents	DELETE /api/vl/certs/system-co	ertificate/{hostName}/{id} Delete System Certificate by ID and hostname	\sim	e i	h
POST /api/vl/certs/system-certificate/generate-selfsigned-certificate Centrals self-signed certificate in Cisco ISE integration POST /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE integration CET /api/vl/certs/trusted-certificate Get list of all trusted certificates integration This API supports Filtering. Sorting and Pagination. Filtering and Sorting are supported for the following attributes: integration • Integration Sorting and Sorting are supported for the following attributes: • Supported Date Format: typy-MA-dd HK mm tst • Support * Support • Support • Support • Support • Or Total T	POST /api/v1/certs/system-co	ertificate/export Export a system certificate with a given a certificate ID	~	e i	à
POST /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE Import System certificate Impo	POST /api/v1/certs/system-co	artificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE	~	e i	à
GET /spi/vl/certs/trusted-certificate Cet list of all trusted certificates A list This API supports Filtering, Sorting and Pagination. Filtering and Sorting are supported for the following attributes: Image: State of the following attributes:	POST /api/v1/certs/system-co	artificate/import Import system certificate in Cisco ISE	~	e i	à
This API supports Filtering, Sorting and Pagination. Filtering and Sorting are supported for the following attributes: testing/Name support support	GET /api/v1/certs/trusted-	zertificate Cet list of all trusted cartificates	^	. 1	à
Filtering and Sorting are supported for the following attributes: • transflyame • subject • issuedTo • issuedTo • subject Date Format: yyy=MM-dd HH mm:ss • Supported Date Format: ED, NED, 01 and L1 • environment: ED, NED, 01 and L1	This API supports Filtering, Sorting and Pag	ination.			
Supported Date Format; yvyv MM-dd HH rmm:ss Supported Qoratives: EQ, VEQ, Q, T and LT status o Allowed values: enabled, disabled o Supported Operators: EQ, NEQ	Filtering and Sorting are supported for the fo studyed studyed valid valid valid supported Operators: EQ. NEQ. of supported Operators: EQ. NEQ. of supported Operators: EQ. NEQ. of More values: Altered Operators: EQ. NEQ. of supported Operators: EQ. NEQ. of supported Operators: EQ. NEQ. of supported Operators: EQ. NEQ.	Howing attributes: d HR mm ss and LT and LT			

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></id-of-certificate></ise-pan-ip>
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	
Servers https://10.106.33.92:44240 - Inferred Url v	
certs-api-controller the certs API	~
Certificates	^
GET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	∨ ≜
POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	 ↓ ≜
GET /api/vl/certs/certificate-signing-request/{hostName}/{id} Get the certificate signing request for a given ID	∨ ≜
DELETE /api/vl/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/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	× 🗎
POST /api/vl/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/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	∨ ≜
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	∨ ≜
GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	~ ≜
GET /api/vl/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 Certification Content of the second seco

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.

≡	dentity Services I	Engine		Op	erations / Troub	leshoot		🔺 License Warning	Q	۵	0	Q	R
Щ	Bookmarks	Diagnostic Tools Download Lo	gs De	bug Wizard									
	Dashboard Context Visibility	Debug Profile Configuration Debug Log Configuration	Node List	sise-bgl-cfmeo1-pan.s	nfiguration								
0	Operations Policy Administration		0 Edit	Seset to Default	Log Filter Enable	Log Filter Disable					AI N	0 - 7	\$ 7
-file	Work Centers		0	Component Name	A Log Level INFO	Description RBAC resource access filter	Log file Name	Log Filter Disabled				Î	
?	Interactive Help		0	Active Directory	WARN	Active Directory client internal messages	ad_agent.log	Disabled					
			0	admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled					
			0	admin-license al-analytics	INFO	License admin messages Al Analytics	ise-psc.log ai-analytics.log	Disabled					
			0	anc api-gateway	INFO	Adaptive Network Control (ANC) debug API Gateway native objects logs	ise-psc.log api-gateway.log	Disabled Disabled					
			•	apiservice	DEBUG	ISE API Service logs Bootstrap wizard messages Save Can	api-service.log	Disabled					
			0	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.

≡	dentity Services	Engine	Ð		Operations / Troubleshoot						Q	۵ (D Q	A
Щ	Bookmarks	Diagr	nostic Tools	Download Logs	Debug Wiza	ird								
- 22	Dashboard		ISE-B	GL-CFME01-PAN										
15	Context Visibility		ISE-B	GL-CFME02-MNT	Delete	e ³ Expand All ≤>Col	lapse All			61-c				
*	Operations		ISE-D	CFME02-PSN	Debug	Log Type	Log File		pescription	Size				
0	Policy		ISE-R	TP-CFME01-PAN	✓ Applicatio	n Logs								-
20	Administration		ISE-R	TP-CFME02-MNT	> ad_	agent (1) (100 KB)								
đ	Work Centers		×.		> ai-a	analytics (11) (52 KB) -gateway (16) (124 KB)								1
					∨ api	-service (13) (208 KB)		_						
(?)	Interactive Help						api-service (all logs)	AP	9 Service debug messages	208 KB				
							api-service.log			12 KB				
							api-service.log.2024-	03-24-1		4.0 KB				
							api-service.log.2024-	04-07-1		4.0 KB				
			1		-									

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.