使用OpenAPI检索ISE 3.3上的ISE证书信息

目录

简介

本文档介绍使用openAPI管理思科身份服务引擎(ISE)证书的步骤。

背景

面对企业网络安全和管理日益增加的复杂性，思科ISE 3.1引入了OpenAPI格式的API，可简化证书生命周期管理，提供标准化和自动化接口以实现高效安全的证书操作，帮助管理员实施强大的安全实践并保持网络合规性。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎(ISE)
- REST API
- Python

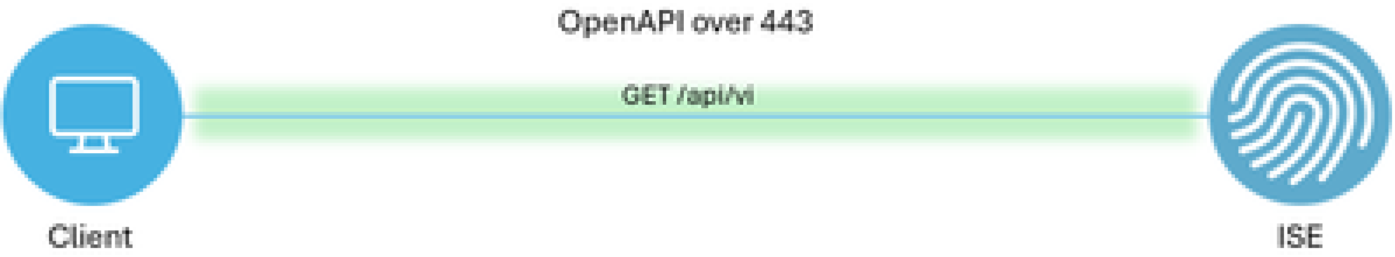
使用的组件

- ISE 3.3
- Python 3.10.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图

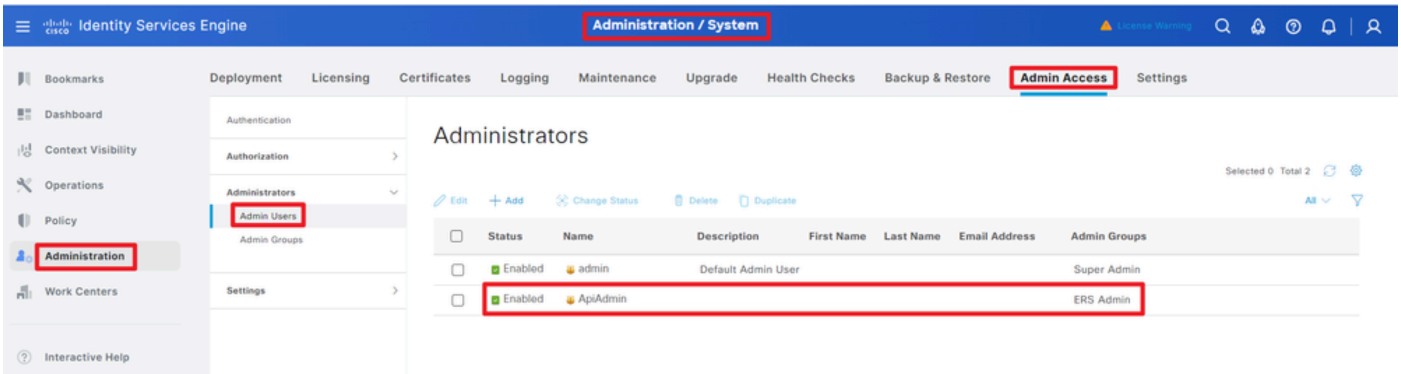


拓扑

ISE上的配置

第1步：添加Open API admin帐户

要添加API管理员，请导航到Administration > System > Admin Access > Administrators > Admin Users > Add。



Administrators

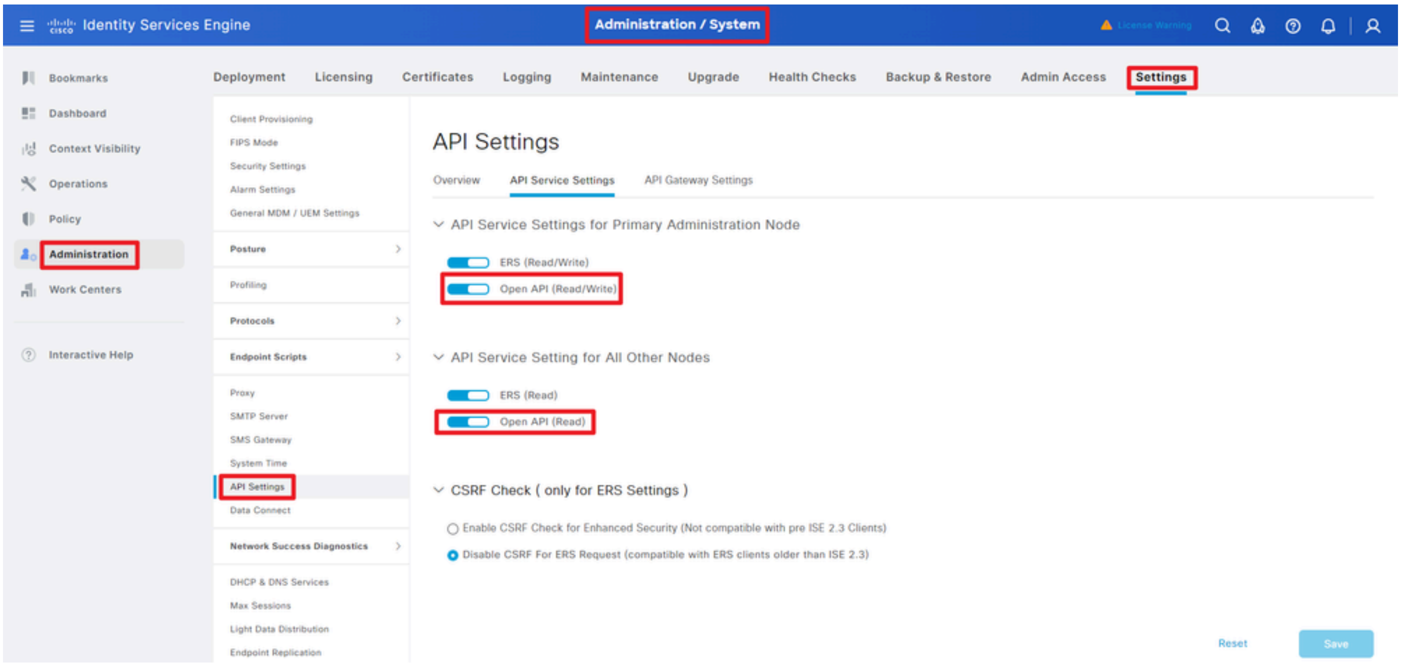
Selected 0 Total 2

□	Status	Name	Description	First Name	Last Name	Email Address	Admin Groups
□	Enabled	admin	Default Admin User				Super Admin
□	Enabled	ApiAdmin					ERS Admin

API管理员

第2步：在ISE上启用开放式API

默认情况下，在ISE上禁用开放式API。要启用它，请导航到管理>System >设置> API设置> API服务设置。切换Open API选项。Click Save.



API Settings

Overview | API Service Settings | API Gateway Settings

API Service Settings for Primary Administration Node

ERS (Read/Write)

Open API (Read/Write)

API Service Setting for All Other Nodes

ERS (Read)

Open API (Read)

CSRF Check (only for ERS Settings)

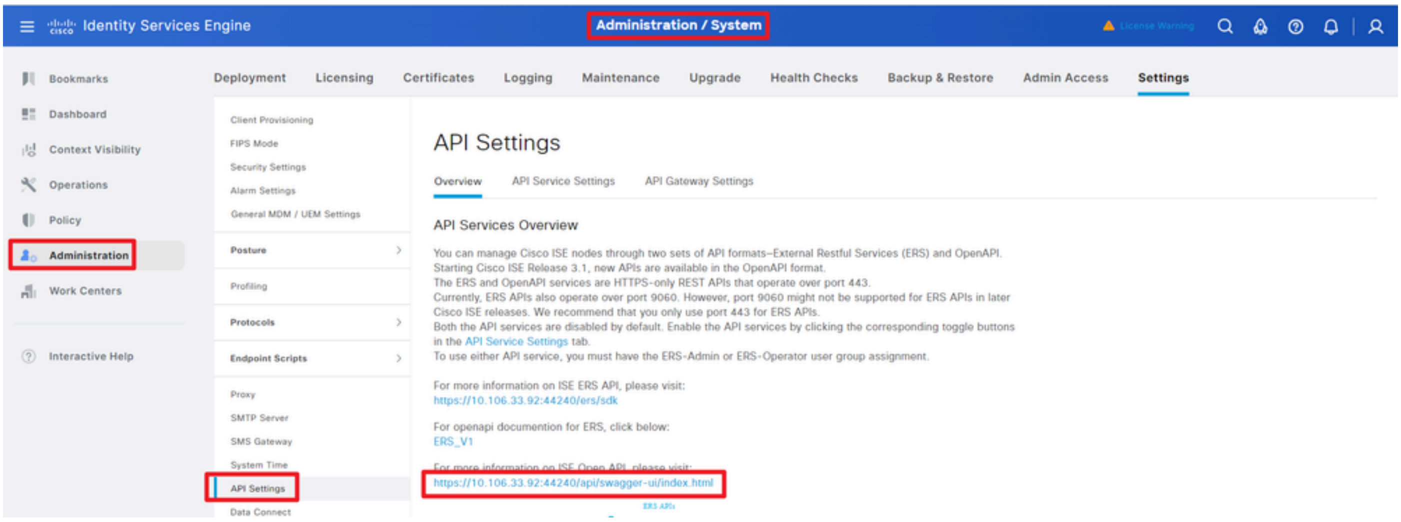
○ Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

● Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

启用OpenAPI

第3步：探索ISE开放式API

导航到管理>System >设置> API设置>概述。点击打开API访问链接。



API Settings

Overview | API Service Settings | API Gateway Settings

API Services Overview

You can manage Cisco ISE nodes through two sets of API formats–External Restful Services (ERS) and OpenAPI.
Starting Cisco ISE Release 3.1, new APIs are available in the OpenAPI format.
The ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443.
Currently, ERS APIs also operate over port 9060. However, port 9060 might not be supported for ERS APIs in later Cisco ISE releases. We recommend that you only use port 443 for ERS APIs.
Both the API services are disabled by default. Enable the API services by clicking the corresponding toggle buttons in the API Service Settings tab.
To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment.

For more information on ISE ERS API, please visit:
https://10.106.33.92:44240/ers/sdk

For openapi documention for ERS, click below:
ERS_V1

For more information on ISE Open API, please visit:
https://10.106.33.92:44240/api/swagger-ui/index.html

访问OpenAPI

Python示例

获取特定节点的所有系统证书

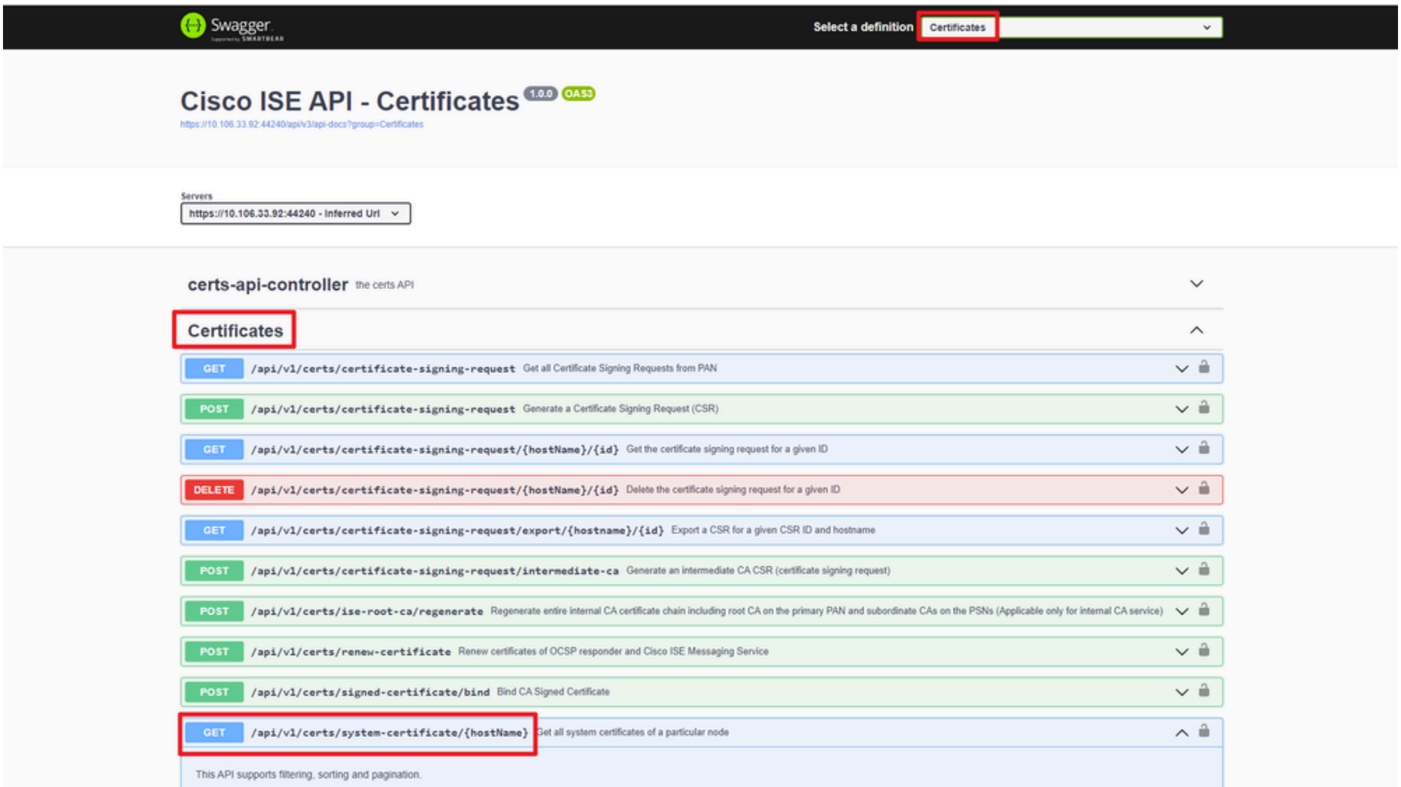
API列出特定ISE节点的所有证书。

第1步：API调用的必需信息。

方法	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>

凭证	使用Open API帐户凭证
信头	接受：application/json 内容类型：application/json

第2步：查找用于检索特定ISE节点的证书的URL。



Cisco ISE API - Certificates 1.0.0 OAS3

https://10.106.33.92:44240/api/v3/api-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 OCSP 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

This API supports filtering, sorting and pagination.

API URI

第3步：这是Python代码的示例。复制并粘贴内容。替换ISE IP、用户名和密码。另存为要执行的python文件。

确保ISE与运行python代码的设备之间保持良好的连接。

<#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())
```

以下是预期输出的示例。

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

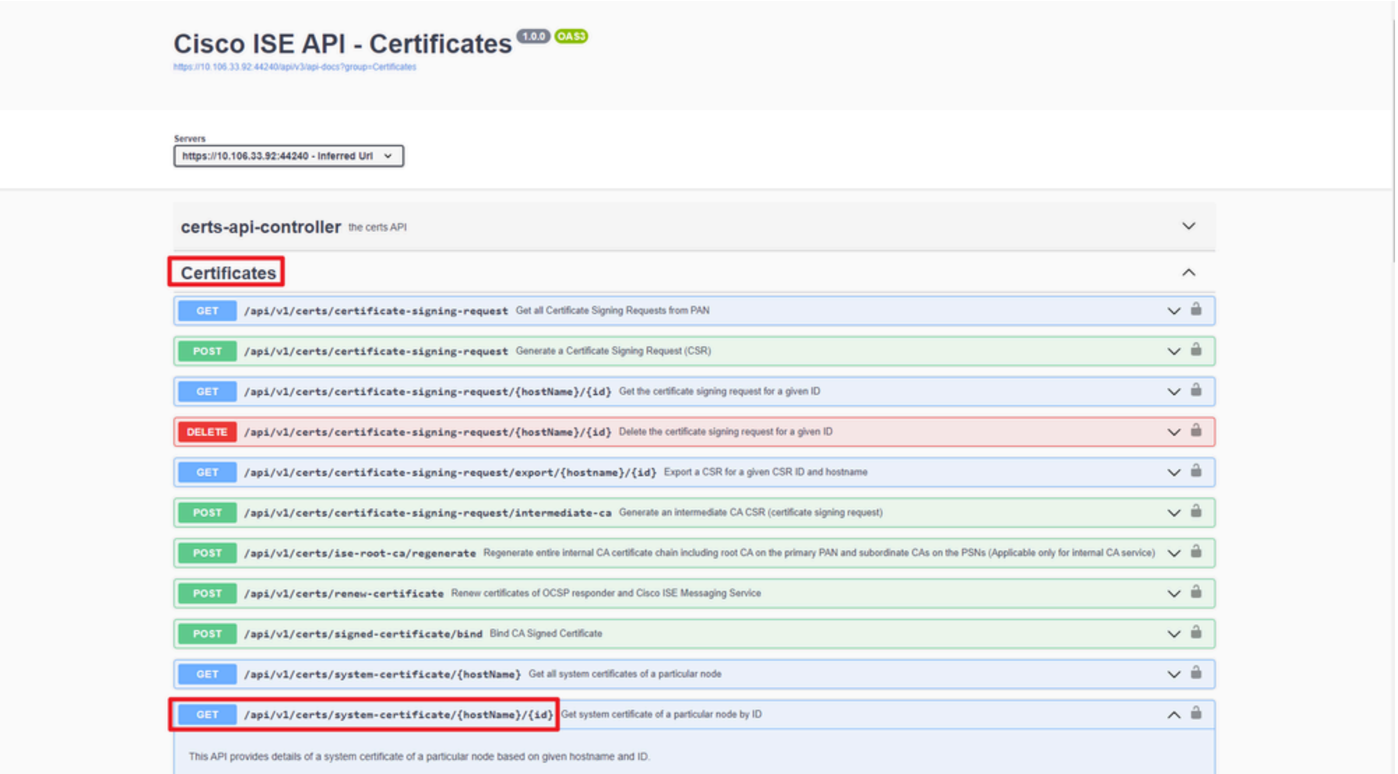
通过ID获取特定节点的系统证书

此API根据给定的主机名和ID提供特定节点的系统证书的详细信息。

第1步：API调用的必需信息。

方法	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-Of-Certificate>
凭证	使用Open API帐户凭证
信头	接受：application/json 内容类型：application/json

第2步：根据给定的主机名和ID查找用于检索特定节点证书的URL。



Cisco ISE API - Certificates 1.0.0 OAS3

https://10.106.33.92:44240/api/v3/api-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 OCSP 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.

API URI

第3步：以下是Python代码示例。复制并粘贴内容。替换ISE IP、用户名和密码。另存为要执行的python文件。

确保ISE与运行python代码的设备之间保持良好的连接。

<#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:")
```

注意：ID来自“获取特定节点的所有系统证书”第3步中的API输出，例如5b5b28e4-2a51-495c-8413-610190e1070b为“默认自签名saml服务器证书- CN=SAML_ISE-DLC-CFME02-PSN.cisco.com”。

以下是预期输出的示例。

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

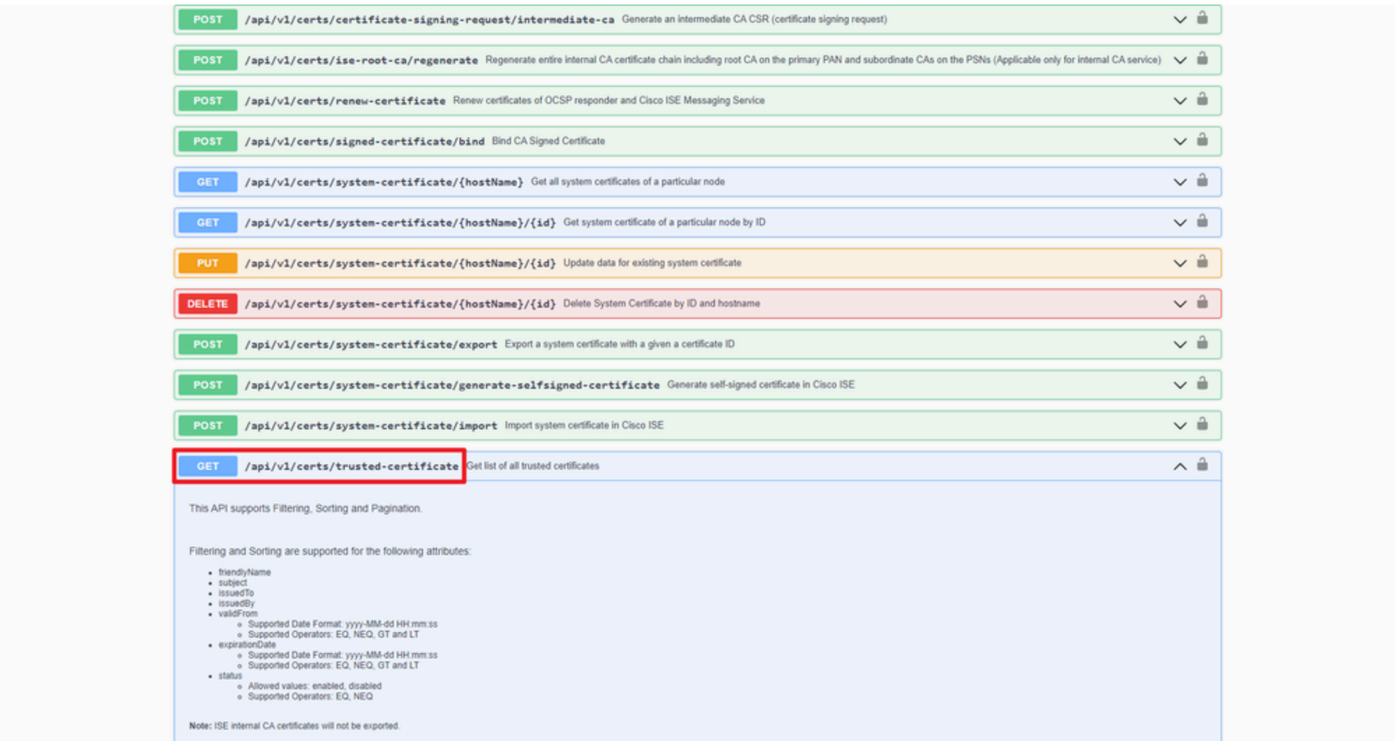
获取所有受信任证书的列表

API列出ISE集群的所有受信任证书。

第1步：API调用的必需信息。

方法	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate
凭证	使用Open API帐户凭证
信头	接受：application/json 内容类型：application/json

第2步：查找用于检索受信任证书的URL。



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 OCSP 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

PUT /api/v1/certs/system-certificate/{hostName}/{id} Update data for existing system certificate

DELETE /api/v1/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname

POST /api/v1/certs/system-certificate/export Export a system certificate with a given a certificate ID

POST /api/v1/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE

POST /api/v1/certs/system-certificate/import Import system certificate in Cisco ISE

GET /api/v1/certs/trusted-certificate Get list of all trusted certificates

This API supports Filtering, Sorting and Pagination.

Filtering and Sorting are supported for the following attributes:

- friendlyName
- subject
- issuedTo
- issuedBy
- validFrom
  - Supported Date Format: yyyy-MM-dd HH:mm:ss
  - Supported Operators: EQ, NEQ, GT and LT
- expirationDate
  - Supported Date Format: yyyy-MM-dd HH:mm:ss
  - Supported Operators: EQ, NEQ, GT and LT
- status
  - Allowed values: enabled, disabled
  - Supported Operators: EQ, NEQ

Note: ISE internal CA certificates will not be exported.

API URI

第3步：以下是Python代码示例。复制并粘贴内容。替换ISE IP、用户名和密码。另存为要执行的python文件。

确保ISE与运行python代码的设备之间保持良好的连接。

<#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:")
```

以下是预期输出的示例。（省略）

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

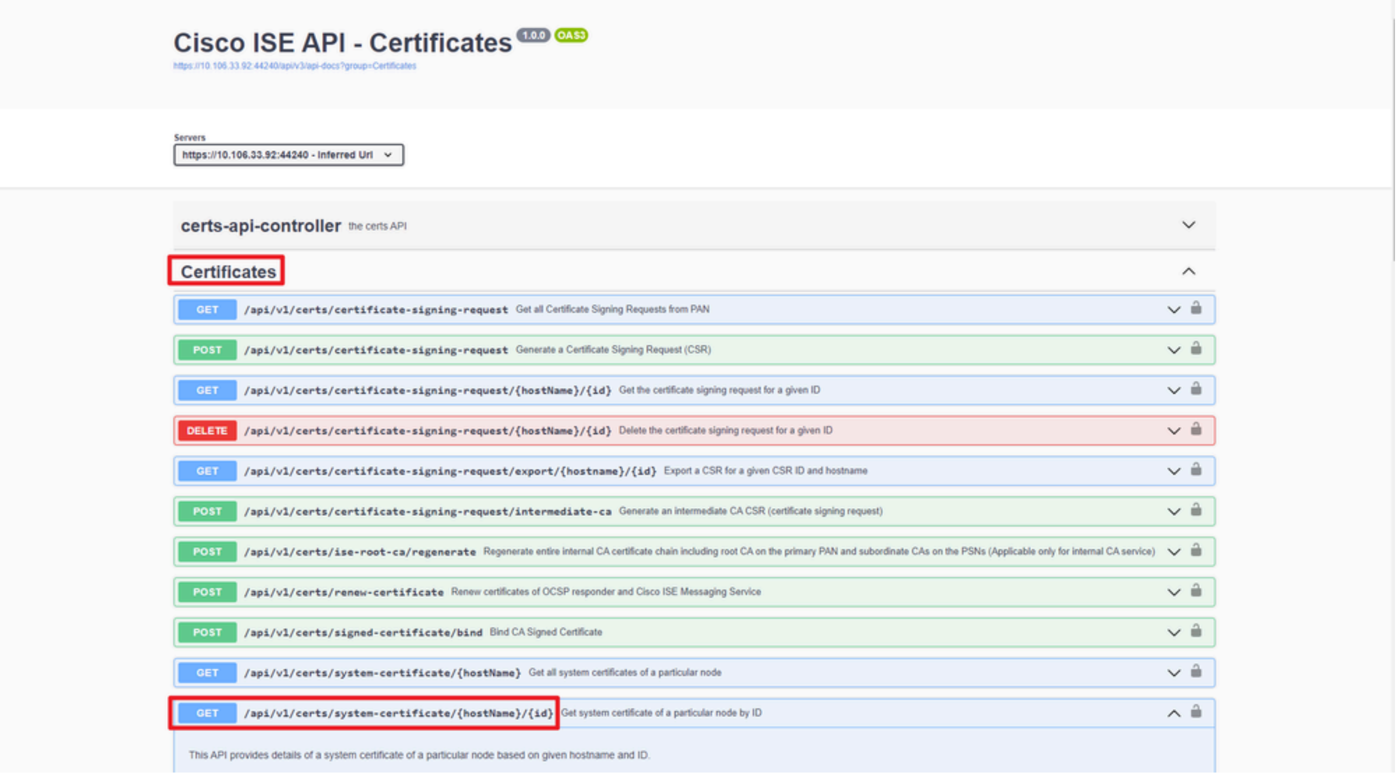
通过ID获取信任证书

此API可以根据给定ID显示信任证书的详细信息。

第1步：API调用的必需信息。

方法	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate/<ID-Of-Certificate>
凭证	使用Open API帐户凭证
信头	接受：application/json 内容类型：application/json

第2步：查找用于检索部署信息的URL。



Cisco ISE API - Certificates 1.0.0 OAS3
https://10.106.33.92:44240/api/v3/api-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 OCSP 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.

API URI

第3步：以下是Python代码示例。复制并粘贴内容。替换ISE IP、用户名和密码。另存为要执行的python文件。

确保ISE与运行python代码的设备之间保持良好的连接。

<#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:")
```

注意：ID来自“获取所有受信任证书列表”第3步中的API输出，例如，147d97cc-6ce9-43d7-9928-8cd0fa83e140是“VeriSign 3类公共主要证书颁发机构”。

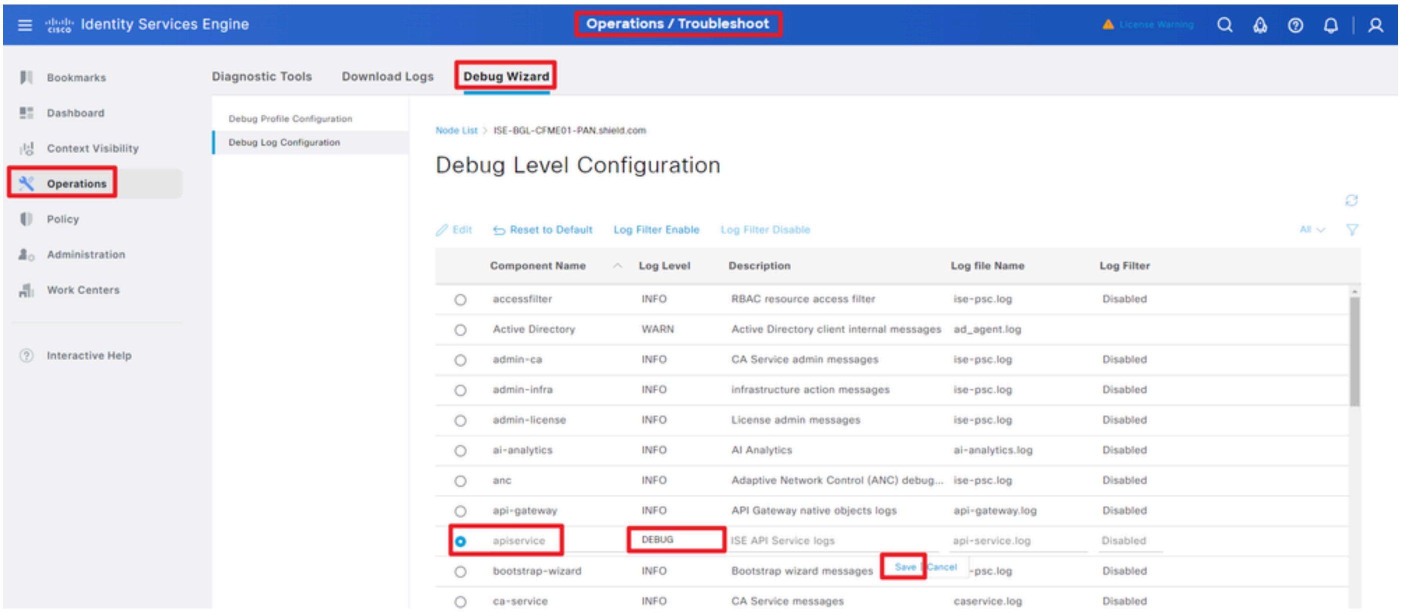
以下是预期输出的示例。

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

故障排除

要排除与开放式API相关的问题，请在调试日志配置窗口中将theapiservicecomponent 的日志级别设置为DEBUG。

要启用调试，请导航到**操作>故障排除**>调试向导>调试日志配置> **ISE**节点>设备。



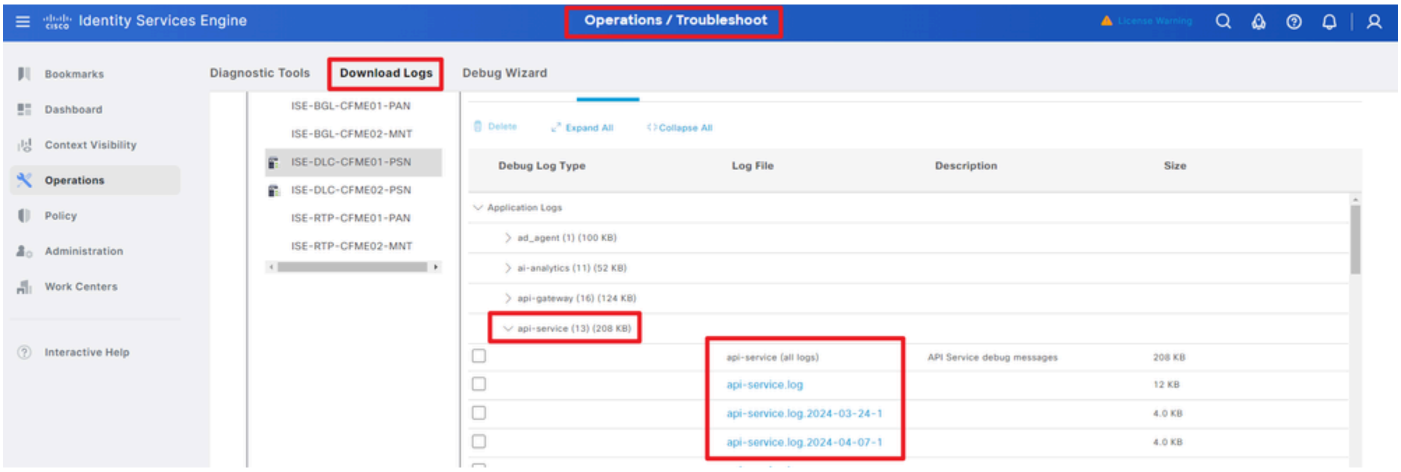
Node List > ISE-BGL-CFME01-PAN.shield.com

Debug Level Configuration

	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	
○	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

*API*服务调试

要下载调试日志，请导航到**操作>故障排除**>下载日志> **ISE PAN**节点>调试日志。



	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)			
□		api-service (all logs)	API 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

下载调试日志

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。