

使用OpenAPI檢索ISE 3.3上的ISE證書資訊

目錄

[簡介](#)

[背景](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[ISE上的配置](#)

[Python示例](#)

[取得特定節點的所有系統憑證](#)

[按ID取得特定節點的系統憑證](#)

[取得所有信任憑證的清單](#)

[透過ID獲取信任證書](#)

[疑難排解](#)

簡介

本檔案介紹使用openAPI管理思科身分辨識服務引擎(ISE)憑證的程式。

背景

面對企業網路安全和管理日益成長的複雜性，思科ISE 3.1引入了OpenAPI格式的API，簡化了證書生命週期管理，提供標準化和自動化介面以實現高效安全的證書操作，幫助管理員實施強大的安全實踐並保持網路合規性。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身分辨識服務引擎(ISE)
- REST API
- Python

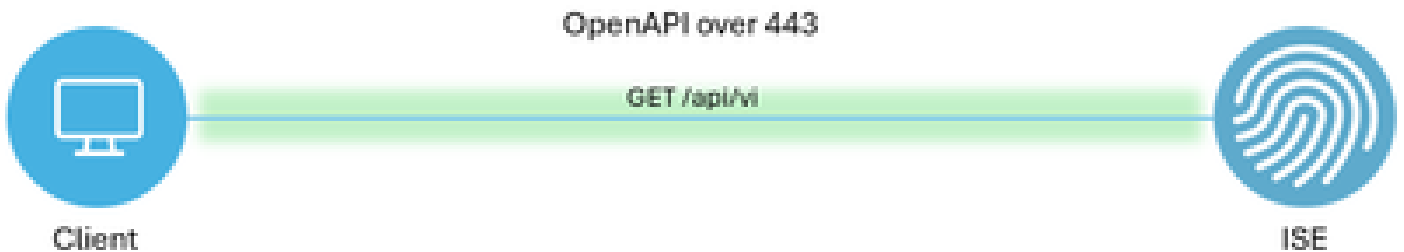
採用元件

- ISE 3.3
- Python 3.10.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表

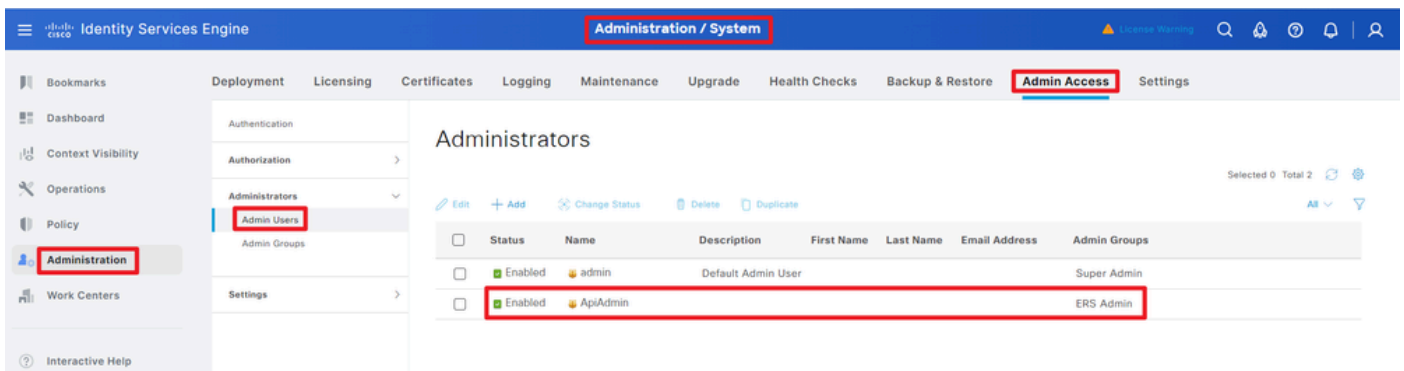


拓撲

ISE上的配置

第1步：增加打開API admin帳戶

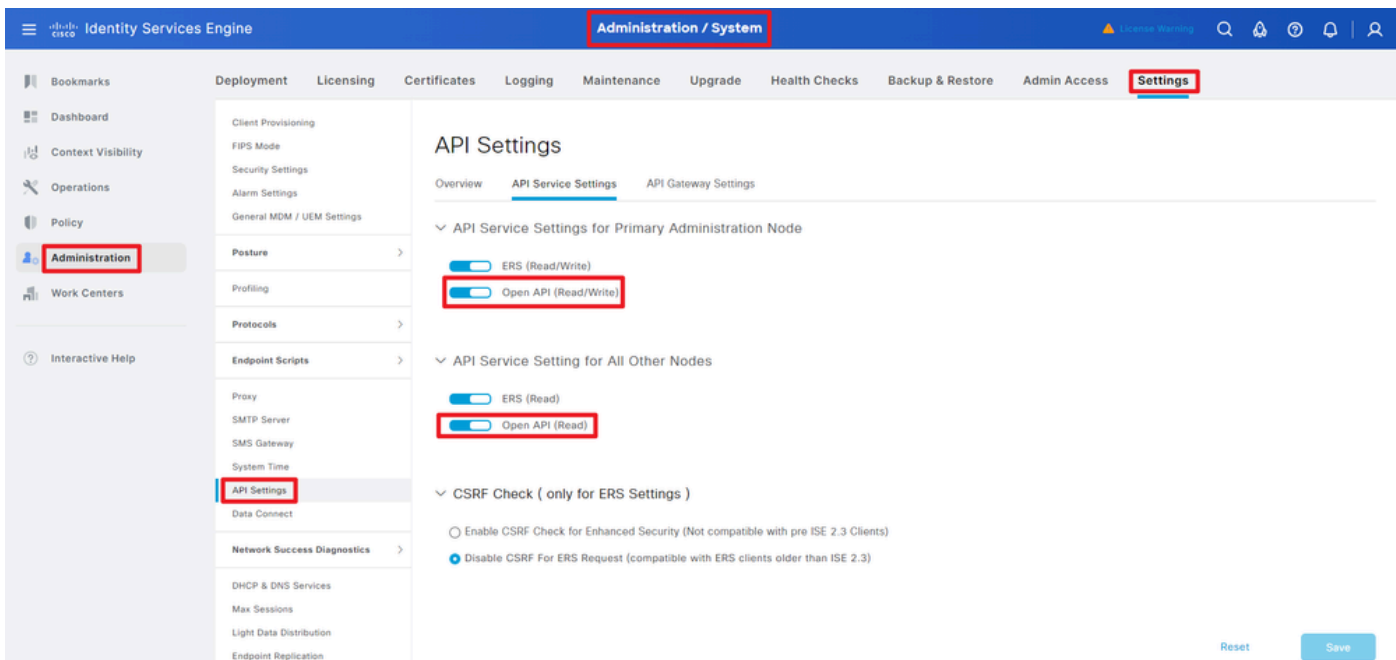
要增加API管理員，請導航到管理>系統>管理員訪問許可權>管理員>管理員使用者>增加。



API管理

第2步：在ISE上啟用開放式API

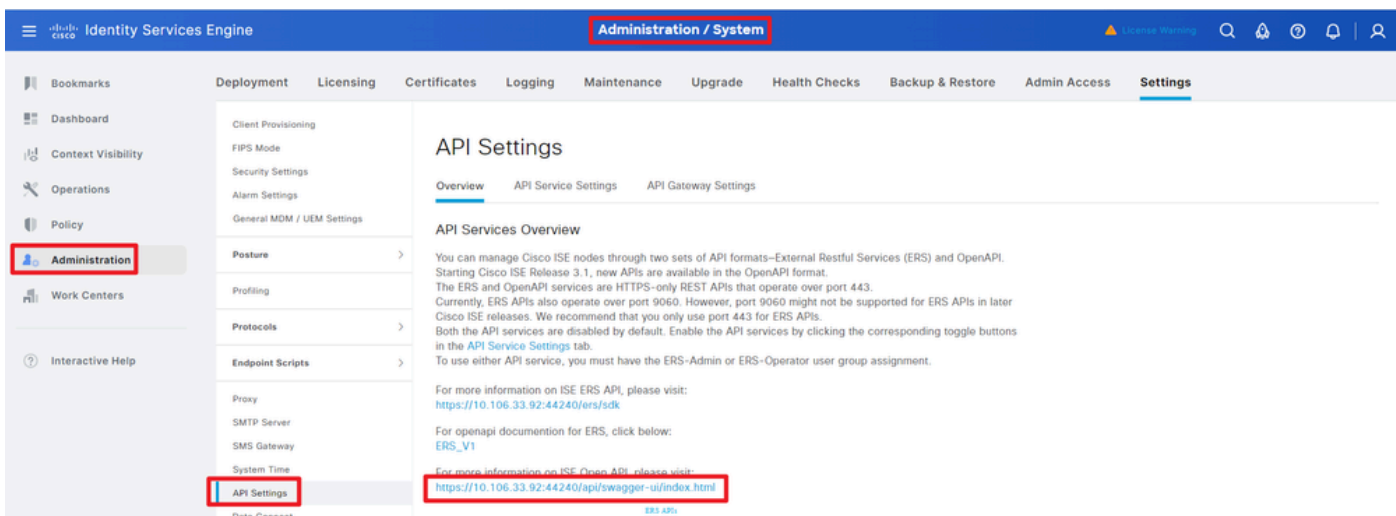
預設情況下，在ISE上停用開放式API。要啟用該功能，請導航到管理>系統>設定> API設定> API服務設定。切換「開啟API」選項。按一下Save。



啟用OpenAPI

第3步：探索ISE開放式API

導航到管理>系統>設定> API設定>概述。點選打開API訪問連結。



訪問OpenAPI

Python示例

取得特定節點的所有系統憑證

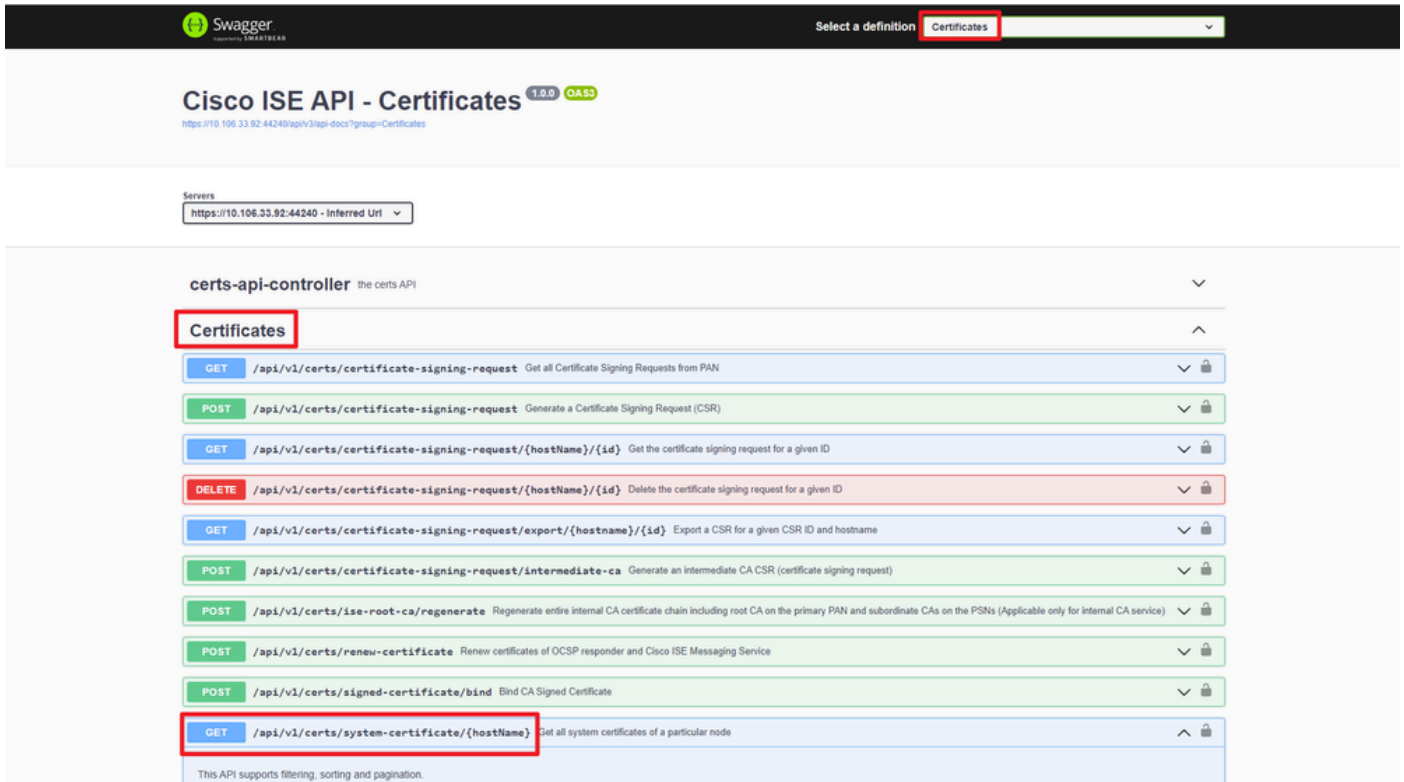
API列出特定ISE節點的所有證書。

第1步：API呼叫的必要資訊。

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

憑證	使用Open API帳戶憑據
標頭	接受 : application/json Content-Type : application/json

第2步：查詢用於檢索特定ISE節點證書的URL。



API URI

第3步：以下是Python代碼的示例。複製並貼上內容。替換ISE IP、使用者名稱和密碼。另存為要執行的python檔案。

確保ISE與運行python代碼示例的裝置之間保持良好的連線。

```
<#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())

```

以下是預期輸出的範例。

Return Code:

200

Expected Outputs:

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

按ID取得特定節點的系統憑證

此API根據給定的主機名和ID提供特定節點的系統證書的詳細資訊。

第1步：API呼叫的必要資訊。

方法	取得
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-Of-Certificate>
憑證	使用Open API帳戶憑據
標頭	接受：application/json Content-Type：application/json

第2步：根據給定的主機名和ID查詢用於檢索特定節點證書的URL。

Cisco ISE API - Certificates 1.0.0 OAS3

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

Servers

<https://10.106.33.92:44240> - Inferred Uri

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.

API URI

第3步：以下是Python代碼的示例。複製並貼上內容。替換ISE IP、使用者名稱和密碼。另存為要執行的python檔案。

確保ISE與運行python代碼示例的裝置之間保持良好的連線。

<#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:")
```



註：ID來自「獲取特定節點的所有系統證書」步驟3中的API輸出，例如，5b5b28e4-2a51-495c-8413-610190e1070b為「預設自簽名saml伺服器證書- CN=SAML_ISE-DLC-CFME02-PSN.cisco.com」。

以下是預期輸出的範例。

Return Code:

200

Expected Outputs:

```
{'response': {'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com'}}
```

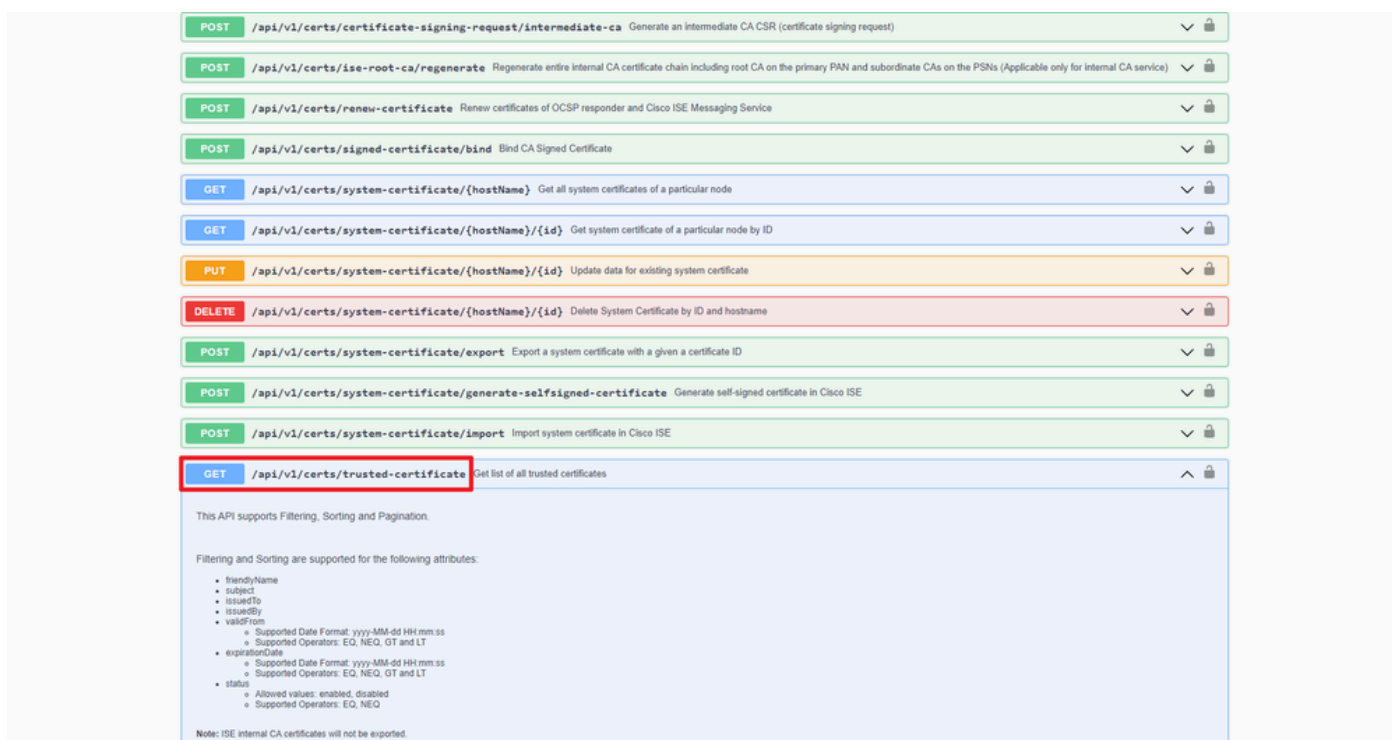
取得所有信任憑證的清單

API列出ISE集群的所有受信任證書。

第1步：API呼叫的必要資訊。

方法	取得
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate
憑證	使用Open API帳戶憑據
標頭	接受：application/json Content-Type：application/json

第2步：查詢用於檢索受信任證書的URL。



API URI

第3步：以下是Python代碼的示例。複製並貼上內容。替換ISE IP、使用者名稱和密碼。另存為要執行的python檔案。

確保ISE與運行python代碼示例的裝置之間保持良好的連線。

```
<#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:")
```

以下是預期輸出的範例。(省略)

Return Code:

200

Expected Outputs:

```
{'response': [{'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Authority', 'subject': 'CN=VeriSign Class 3 Public Primary Certification Authority'}]}
```

透過ID獲取信任證書

此API可根據給定ID顯示信任證書的詳細資訊。

第1步：API呼叫的必要資訊。

方法	取得
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate/<ID-Of-Certificate>
憑證	使用Open API帳戶憑據
標頭	接受：application/json Content-Type：application/json

第2步：查詢用於檢索部署資訊的URL。

The screenshot shows the Cisco ISE API - Certificates page. The page title is "Cisco ISE API - Certificates" with version "1.0.0" and "OAS3" tags. The URL is "https://10.106.33.92:44240/api/v3/api-docs?group=Certificates". The page displays a list of API endpoints for certificates. The endpoint `/api/v1/certs/system-certificate/{hostname}/{id}` is highlighted with a red box. Below the list, there is a note: "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代碼的示例。複製並貼上內容。替換ISE IP、使用者名稱和密碼。另存為要執行的python檔案。

確保ISE與運行python代碼示例的裝置之間保持良好的連線。

<#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:")
```



註：ID來自「獲取所有受信任證書清單」第3步中的API輸出，例如，147d97cc-6ce9-43d7-9928-8cd0fa83e140是「VeriSign 3類公共主要證書頒發機構」。

以下是預期輸出的範例。

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

疑難排解

若要疑難排解與開放式API相關的問題，請在偵錯日誌組態視窗中將theapiservicecomponent 的日誌層級設定為DEBUG。

要啟用調試，請導航到操作>故障排除>調試嚮導>調試日誌配置> ISE節點>裝置服務。

Identity Services Engine Operations / Troubleshoot

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration
Debug Log Configuration

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

Debug Level Configuration

Edit Reset to Default Log Filter Enable Log Filter Disable All

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

Save Cancel

API服務調試

要下載調試日誌，請導航到操作>故障排除>下載日誌> ISE PAN節點>調試日誌。

Identity Services Engine Operations / Troubleshoot

Diagnostic Tools **Download Logs** Debug Wizard

ISE-BGL-CFME01-PAN
ISE-BGL-CFME02-MNT
ISE-DLC-CFME01-PSN
ISE-DLC-CFME02-PSN
ISE-RTP-CFME01-PAN
ISE-RTP-CFME02-MNT

Delete Expand All Collapse All

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

下載調試日誌

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。