# 使用OpenAPI检索ISE 3.3上的ISE证书信息

目录
<u>背景</u>
先决条件
<u>要求</u>
使用的组件
<u>网络图</u>
ISE上的配置
<u>Python示例</u>
<u>获取特定节点的所有系统证书</u>
通过ID获取特定节点的系统证书
<u>获取所有受信任证书的列表</u>
通过ID获取信任证书
<u>故障排除</u>

## 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



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。

=	dentity Services I	Engine				Administra	tion / Syst	em						Q (	0	φ	8
Ц	Bookmarks	Deployment Licensing	Cert	ificates	Logging	Maintenance	Upgrade	Health	Checks	Backup & Re	estore	Admin Access	Settings				
5	Dashboard	Authentication		Adm	inistrat	ore											
16	Context Visibility	Authorization	>	Aum	inistrat	015								Calcola	40 Tetel 2	a .	<b>b</b> .
*	Operations	Administrators	Ŷ	0 Edit	+ Add	🛞 Change Status	Delete	Duplicate						56/6016	A Notal 2	1 V 1	7
0	Policy	Admin Users			Status	Name	Descrip	tion	First Name	Last Name	Email Add	fress Admin G	roups				
80	Administration			0	Enabled	y admin	Default	Admin User				Super Ad	amin				
-fili	Work Centers	Settings	>		Enabled	a ApiAdmin						ERS Adm	nin				
?	Interactive Help																

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.

≡	dentity Services	Engine				Administrat	tion / Systen	n		<b>_</b>	License Warning	Q	۵	0	Ф   А
н	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
	Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help	Deployment Client Provision FIPS Mode Security Setting Alarm Settings General MDM / I Posture Profiling Protocols Endpoint Script Proxy SMTP Server SMS Gateway System Time API Settings Data Connect Network Succe DHCP & DNS Se	Licensing ing s UEM Settings is is ss Diagnostics tryices	> API S Overview > API S > API S > CSRF > CSRF > Diat	ettings API Service Service Settin ERS (Read/W Open API (Re Open API (Re Open API (Re Check ( only le CSRF Check	Maintenance Settings API G ags for Primary A frite) ad/Write) ag for All Other N ad) y for ERS Setting for Enhanced Securit IS Request (compatible)	Upgrade ateway Settings Administratio Nodes s ) y (Not compatible ye with ERS cile	n Node e with pre ISE 2.3 Clien nts older than ISE 2.3)	nts)	Admin Access	Settings				
		Max Sessions Light Data Distri Endpoint Replica	ibution ation									Rese	t		Save

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。

≡	dentity Services E	Engine				Administra	tion / Syster	n		A .	Joense Warning	Q	۞ ۿ	Q   Q							
Щ	Bookmarks	Deployment Licensi	ng Ce	ertificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings										
- 55	Dashboard	Client Provisioning																			
명	Context Visibility	FIPS Mode Security Settings		API S	Settings																
×	Operations	Alarm Settings		Overview	API Service	e Settings API C	Sateway Settings														
-0	Policy	General MDM / UEM Settings		API Serv	ices Overvie	w															
80	Administration	Posture	>	You can m	anage Cisco ISE	nodes through two	sets of API form	ats-External Restful Ser	rvices (ERS) and OpenAPI.												
đ	Work Centers	Profiling		The ERS at Currently,	nd OpenAPI sen ERS APIs also o	vices are HTTPS-onl perate over port 906	y REST APIs that 0. However, port	operate over port 443. 9060 might not be sup	ported for ERS APIs in later												
		Protocols	>	Cisco ISE Both the A	eleases. We ree PI services are	commend that you or disabled by default. I	hly use port 443 Enable the API se	for ERS APIs. arvices by clicking the c	corresponding toggle button	5											
?	Interactive Help	Endpoint Scripts	>	To use eith	er API service,	s tab. you must have the El	RS-Admin or ER	S-Operator user group a	assignment.												
	1	Proxy SMTP Server SMS Gateway System Time API Settings		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 Ext. more information on ISE Open API clease visit: https://10.106.33.92:44240/api/swagger-u/indox.html																	
		Data Connect				ERS AP	h														

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

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。

Swagger. Select a definition Certificates	×	
Cisco ISE API - Certificates (ISB) (753) https://10.108.33.02.44240/epi/v3/epi-decr/ty/usp-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/v1/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/vl/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given ID	✓ ≜	
GET /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/vi/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	A service) 🗸 🗎	
POST /api/vi/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	~ ≜	
POST /api/vi/certs/signed-certificate/bind Bind CA Signed Certificate	✓ ≜	
CET /api/vi/certs/system-certificate/{hostName} Bet 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&gt;</id-of- </ise-node-hostname></ise-pan-ip>
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 (IDD) (CTS) https://10.106.33.82.412404apt/v3/bpi-doct/prosp-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/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 Ranew certificates of OCSP responder and Cisco ISE Messaging Service	× 🛍
POST /api/vl/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/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.	

```
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-8413-610190e2

" 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samI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</ise-pan-ip>
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/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	~	r ii	i.
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 ii	
POST /api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	~	e i	
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	~	r ii	
GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	~	e ii	
GET /api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID	~	r ii	
PUT /api/v1/certs/system-certificate/{hostName}/{id} Update data for existing system certificate	~	e ii	
DELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname	~	r ii	1
POST /api/vl/certs/system-certificate/export Export a system certificate with a given a certificate ID	$\sim$	r ii	
POST /api/vl/certs/system-certificate/generate-selfsigned-certificate Generale self-signed certificate in Cisco ISE	~	e ii	
POST /api/v1/certs/system-certificate/import Import system certificate in Claco ISE	~	r ii	
GET /api/vi/certs/trusted-certificate Get list of all trusted certificates	^	, ii	
This API supports Filtering, Sorting and Pagination.			
Filtering and Sorting are supported for the following attributes:			

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=Veri

#### 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></id-of-certificate></ise-pan-ip>
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 (IDD) (ASS) https://10.106.33.82.442400apu/Japi-doc1/group-Centificates		
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/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/vl/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/vl/certs/ise-root-ca/regenerate Regenerate enline internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA set	nvice) 🗸 🗎	
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	∨ ≜	
OET /api/v1/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.		

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

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。

=	dentity Services	Engine			OF	erat	tions / Troub	leshoot		License Warning	Q	۵	0	۵	A
Щ	Bookmarks	Diagnostic Tools	Download Logs	Deb	oug Wizard										
≣  छ <b>火</b>	Dashboard Context Visibility Operations	Debug Profile Configuratio	ation	Node List > ISE-BOL-CFME01-PAN shield.com Debug Level Configuration											S
0	Policy			0 Edit	← Reset to Default	Log	Filter Enable	Log Filter Disable					All		7
8.	Administration				Component Name	$\sim$	Log Level	Description	Log file Name	Log Filter					
ń	Work Centers			0	accessfilter		INFO	RBAC resource access filter	ise-psc.log	Disabled					
				0	Active Directory		WARN	Active Directory client internal messages	ad_agent.log						
?	Interactive Help			0	admin-ca		INFO	CA Service admin messages	ise-psc.log	Disabled					
				0	admin-infra		INFO	infrastructure action messages	ise-psc.log	Disabled					
				0	admin-license		INFO	License admin messages	ise-psc.log	Disabled					
				0	ai-analytics		INFO	Al Analytics	ai-analytics.log	Disabled					
				0	anc		INFO	Adaptive Network Control (ANC) debug	ise-psc.log	Disabled					
				0	api-gateway		INFO	API Gateway native objects logs	api-gateway.log	Disabled					
				0	apiservice	_ [	DEBUG	ISE API Service logs	api-service.log	Disabled					
				0	bootstrap-wizard		INFO	Bootstrap wizard messages Save I Can	cel -psc.log	Disabled					
				0	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。

î.

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)。