Use OpenAPI to Retrieve ISE Certificate Information on ISE 3.3

Contents

Introduction
Background
Prerequisites
Requirements
Components Used
Configure
Network Diagram
Configuration on ISE
Python Examples
Get All System Certificates Of A Particular Node
Get System Certificate Of A Particular Node By ID
Get List Of All Trusted Certificates
Get Trust Certificate By ID
Troubleshoot

Introduction

This document describes the procedure for utilizing openAPI to manage Cisco Identity Services Engine (ISE) certificate.

Background

In the face of growing complexity in enterprise network security and management, Cisco ISE 3.1 introduces OpenAPI-formatted APIs that streamline certificate lifecycle management, offering a standardized and automated interface for efficient and secure certificate operations, helping administrators enforce strong security practices and maintain network compliance.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Identity Services Engine (ISE)
- REST API
- Python

Components Used

- ISE 3.3
- Python 3.10.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configuration on ISE

Step 1: Add an Open API admin account

To add an API admin, navigate to**Administration > System > Admin Access > Administrators > Admin** Users > Add.

≡	dentity Services E	Engine				Administra	tion / Syste	m		🛕 License Wa	mina Q	0 ه	Q	A
н	Bookmarks	Deployment Licensing	Cer	rtificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access Settin	ngs			
5	Dashboard	Authentication		Adm	inietrat	ore								
명	Context Visibility	Authorization	>	Aum	mstrat	015								-
*	Operations	Administrators	~	/ Edit	+ Add	🛞 Change Status	Delete	Duplicate			2	elected 0 Total	AL V	₩ V
.0	Policy	Admin Users			Status	Name	Descripti	on Eirst Name	Last Name Email A	ddrees Admin Groups				í.
80	Administration	Admin Groups		0	Enabled	a admin	Default A	udmin User	Last Halling Linding	Super Admin				
di.	Work Centers	Settings	×	0	Enabled	a ApiAdmin				ERS Admin				
?	Interactive Help													

API Admin

Step 2: Enable Open API on ISE

Open API is disabled by default on ISE. To enable it, navigate to **Administration > System > Settings > API Settings > API Service Settings**. Toggle the Open API options. Click *Save*.

$\equiv \frac{1}{casco}$ Identity Services Engine	Administration / System	🔺 License Warning 🔍 💩 😨 📮 🗙
Bookmarks Deployment	icensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
Dashboard Client Provisioning Id Context Visibility PDS Mode FIPS Mode Id Operations Alarm Settings General MDM / UEI Image: Policy General MDM / UEI Image: Policy Posture Image: Work Centers Profiling	Settings Overview API Service Settings API Gateway Settings Settings API Service Settings for Primary Administration Node ERS (Read/Write) Open API (Read/Write)	
Protocols ⑦ Interactive Help Endpoint Scripts Proxy SMTP Server SMTP Server SMS Gateway System Time System Time	API Service Setting for All Other Nodes ERS (Read) Open API (Read)	
API Settings Data Connect Network Success I DHCP & DNS Servi Max Sessions Light Data Distribut Endpoint Replicatio	CSRF Check (only for ERS Settings) CENTRY (Not compatible with pre ISE 2.3 Clients) Enable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3) Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)	Reset Save
Enable OpenAPI		

Step 3: Explore ISE open API

navigate to Administration > System > Settings > API Settings > Overview. Click open API visit link.

	dentity Services I				Administra	🔺 License Warning 🔍 💩 💿 📮 🛛								
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings			
- 55	Dashboard	Client Provisioni	ing											
명	Context Visibility	FIPS Mode Security Setting	5	API	Settings									
×	Operations	Alarm Settings		Overvier	API Service	e Settings API G	ateway Settings							
0	Policy	General MDM /	UEM Settings	API Se	vices Overvie	w								
80	Administration	Posture		> You can Starting	u can manage Cisco ISE nodes through two sets of API formats—External Restful Services (ERS) and OpenAPI. arting Cisco ISE Release 3.1, new APIs are available in the OpenAPI format. e ERS and OpenAPI services are HTTPS-only REST APIs that operate over port 443. reports ERS APIs elso nonext ore port 0604. Newware, nor 0606 micht not be supported for EPS APIs in later									
di.	Work Centers	Profiling		The ERS Currenth										
		Protocols		> Cisco IS Both the	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									
?	Interactive Help	Endpoint Script	ts	> To use e	To use either API service, you must have the ERS-Admin or ERS-Operator user group assignment.									
		Proxy SMTP Server SMS Gateway		For more https://1 For oper ERS_V1	information on IS 0.106.33.92:4424 api documention	E ERS API, please vis to/ers/sdk for ERS, click below:	it:							
		System Time		For more	information on IS	F Onen API, niesse v	icit-							
		API Settings Data Connect		https://	1.100.33.92:4424	ERS AND	A A A A A A A A A A A A A A A A A A A							

Visit OpenAPI

Python Examples

Get All System Certificates Of A Particular Node

The API lists all the certificates of a particular ISE node.

Step 1: Required information for an API call.

Method	GET
URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname></ise-node-hostname></ise-pan-ip>
Credentials	Use Open API account credentials

Headers	Accept : application/json Content-Type : application/json
---------	--

Step 2: Locate the URL that is utilized to retrieve certificates of a particular ISE node.

Select a definition Certificates	~	
Cisco ISE API - Certificates (ICO) (ICO) http://10.106.33.52-44240egiv/Jage-docr/group-Centicates		
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)	✓ ■	
CET /api/vl/certs/certificate-signing-request/{hostName}/{id} Get the contilicate signing request for a given ID	✓ ≜	
DELETE /api/vi/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	✓ ≜	
FOST /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 enfire 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/vi/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	~ ≞	
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	✓ ■	
GEY /api/vl/certs/system-certificate/{hostName} Det all system certificates of a particular node	^ ≞	
This API supports filtering, sorting and pagination.		

API URI

Step 3: Here is the example of Python Code. Copy and paste the content. Replace the ISE IP, username, password. Save as a python file to execute.

Ensure the good connectivity between ISE and the device running the python code example.

<#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())
```

Here is the example of expected outputs.

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

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.

Step 1: Required information for an API call.

Method	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>
Credentials	Use Open API account credentials
Headers	Accept : application/json Content-Type : application/json

Step 2: Locate the URL that is utilized to retrieve the certificate of a particular node based on given hostname and ID.

)

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)	> < > â
Certificates GET /api/v1/certs/certificate-signing-request Get /api/v1/certs/certificate-signing-request Get /api/v1/certs/certificate-signing-request Get /api/v1/certs/certificate-signing-request Get /api/v1/certs/certificate-signing-request Generate a Certificate Signing Requests (CSR)	× ^ × =
Certificates OET /api/vl/certs/certificate-signing-request GET /api/vl/certs/certificate-signing-request	^ ∨ ≜
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)	 ✓ ≜
POST /api/vl/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/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/vi/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/v1/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/v1/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID	^ ≜

```
API URI
```

Step 3: Here is the example of Python Code. Copy and paste the content. Replace the ISE IP, username, password. Save as a python file to execute.

Ensure the good connectivity between ISE and the device running the python code example.

<#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:")
    print(response.status_code)
    print("Expected Outputs:")
```



Note: The ID is from API outputs in step 3 of "Get All System Certificates Of A Particular Node", for example, 5b5b28e4-2a51-495c-8413-610190e1070b is "Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com".

Here is the example of expected outputs.

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

Get List Of All Trusted Certificates

The API lists all the trusted certificates of ISE cluster.

Step 1: Required information for an API call.

Method	GET
URL	https:// <ise-pan-ip>/api/v1/certs/trusted-certificate</ise-pan-ip>
Credentials	Use Open API account credentials
Headers	Accept : application/json Content-Type : application/json

Step 2: Locate the URL that is utilized to retrieve trusted certificates.

POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CACSR (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 node	∨ ≜	
GET /api/vl/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 Claco ISE	∨ ≜	
POST /api/v1/certs/system-certificate/import Import system certificate in Cisco ISE	∨ ≜	
GET /api/vl/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:		

API URI

Step 3: Here is the example of Python Code. Copy and paste the content. Replace the ISE IP, username, password. Save as a python file to execute.

Ensure the good connectivity between ISE and the device running the python code example.

<#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:")
    print(response.status_code)
    print("Expected Outputs:")
    print(response.json())
```

Here is the example of expected outputs.(Omitted)

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

Get Trust Certificate By ID

This API can displays details of a Trust Certificate based on a given ID.

Step 1: Required information for an API call.

Method	GET
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate/<id-of-certificate></id-of-certificate></ise-pan-ip>
Credentials	Use Open API account credentials
Headers	Accept : application/json Content-Type : application/json

Step 2: Locate the URL that is utilized to retrieve deployment information.

Cisco ISE API - Certificates (ISB) CASS https://10.106.33.92-44240apv/3rapi-docs/group-Certificates	
Servers https://10.106.33.92:44240 - Inferred Url v	
certs-api-controller the certs API	~
Certificates	^
OET /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)	 ✓ ≜
OET /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	∨ ≜
CEY /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 Certificate	✓ ≜
OET /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	^ ≜

```
API URI
```

Step 3: Here is the example of Python Code. Copy and paste the content. Replace the ISE IP, username, password. Save as a python file to execute.

Ensure the good connectivity between ISE and the device running the python code example.

<#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:")
    print(response.status_code)
    print("Expected Outputs:")
```



Note: The ID is from API outputs in step 3 of "Get List Of All Trusted Certificates", for example, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 is "VeriSign Class 3 Public Primary Certification Authority".

Here is the example of expected outputs.

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

Troubleshoot

To troubleshoot issues that are related to the Open APIs, set the**Log Level**for the**apiservice**component to**DEBUG**in the**Debug Log Configuration**window.

To enable debug, Navigate to **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration** > **ISE Node > apiservice.**

=	dentity Services	Engine	Operations / Troubleshoot					License Warning	Q	۵	0	٥	A
н	Bookmarks	Diagnostic Tools Download L	.ogs Del	bug Wizard									
ild N	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List Debt) ISE-BGL-CFME01-PAN:					6	3			
0	Policy		0 Edit	← Reset to Default	Log Filter Enable	Log Filter Disable					AI	~ 5	7
8	Administration			Component Name	∧ Log Level	Description	Log file Name	Log Filter					
ก็	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	AI 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	apl-service.log	Disabled					
			0	bootstrap-wizard	INFO	Bootstrap wizard messages Save Can	-psc.log	Disabled					
			0	ca-service	INFO	CA Service messages	caservice.log	Disabled					

API Service Debug

To download debug logs, Navigate to **Operations > Troubleshoot > Downlaod Logs > ISE PAN Node > Debug Logs.**

≡	dentity Services	Engine				Operations /	/ Trouble	eshoot		A License Warning	Q	۵	0	Q	۹
Щ	Bookmarks	Diagn	ostic Tools	Download Logs	Debug Wiz	ard									
10	Dashboard		ISE-BO	SL-CFME01-PAN											
15	Context Visibility		ISE-BO	SL-CFME02-MNT	Delete	2 ⁸ Expand All ⇔Co	ellapse All	Los Filo	Description	<u> e</u> lea					
*	Operations		ISE-DI	LC-CFME02-PSN	Debuş	g Log Type		Log File	Description	Size					
0	Policy		ISE-R1	FP-CFME01-PAN	✓ Application	on Logs									î.
8.	Administration		ISE-R1	FP-CFME02-MNT	> ad	_agent (1) (100 KB)									
di.	Work Centers		¢		> ai-	analytics (11) (52 KB) i-gateway (16) (124 KB)									1
					∨ ap	i-service (13) (208 KB)									
?	Interactive Help							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					
					-		_								

Download Debug Logs