# Utiliser OpenAPI pour récupérer les informations de certificat ISE sur ISE 3.3

# Table des matières

Introduction
Fond
Conditions préalables
Exigences
Composants utilisés
Configurer
Diagramme du réseau
Configuration sur ISE
Exemples Python
Obtenir Tous Les Certificats Système D'Un Noeud Particulier
Obtenir le certificat système d'un noeud particulier par ID
Obtenir La Liste De Tous Les Certificats Approuvés
Obtenir le certificat de confiance par ID
Dépannage

# Introduction

Ce document décrit la procédure d'utilisation d'openAPI pour gérer le certificat Cisco Identity Services Engine (ISE).

# Fond

Face à la complexité croissante de la sécurité et de la gestion du réseau d'entreprise, Cisco ISE 3.1 introduit des API au format OpenAPI qui rationalisent la gestion du cycle de vie des certificats, offrant une interface standardisée et automatisée pour des opérations de certificats efficaces et sécurisées, aidant les administrateurs à appliquer des pratiques de sécurité strictes et à maintenir la conformité du réseau.

# Conditions préalables

# Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

# Composants utilisés

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Configurer

# Diagramme du réseau



Topologie

## Configuration sur ISE

## Étape 1 : Ajoutez un compte admin Open API

Pour ajouter un administrateur d'API, accédez à Administration -> Système -> Administration -> Administrateurs -> Admin Users -> Add.

≡	dials Identity Services I	Engine				Administra	tion / Syster	n		<b>▲</b> 0	cense Warning	Q	۵	0	<b>0</b>	۹
Щ	Bookmarks	Deployment Licensing	Cer	rtificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings					
	Dashboard	Authentication		Adm	Inlatrate											
명	Context Visibility	Authorization	>	Adm	inistrato	DIS						e	elected (	Total 2	a	a
*	Operations	Administrators	v	0 Edit	+ Add	🗘 Change Status	🗍 Delete 📋	Duplicate				9	CIEVIES V	100012	.~	7
0	Policy	Admin Users Admin Groups			Status	Name	Descriptio	n First Name	Last Name Email Ad	Idress Admin Gro	ups					
20	Administration				Enabled	admin 😛	Default Ac	Imin User		Super Adr	nin					
nii:	Work Centers	Settings	>		Enabled	a ApiAdmin				ERS Admir	n					
?	Interactive Help															

Administrateur API

Étape 2 : activez l'API ouverte sur ISE

L'API ouverte est désactivée par défaut sur ISE. Pour l'activer, accédez à Administration > System > API Settings > API Service Settings. Activez les options de l'API ouverte. Cliquez sur Save.



```
Activer OpenAPI
```

## Étape 3 : Explorez l'API ouverte ISE

accédez à Administration > System > API Settings > Overview. Cliquez sur le lien Open API visit.

=	dentity Services I	Engine				Administrat	tion / Systen	•				Q	۵	0	Q   Q
н	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings				
5	Dashboard	Client Provisionin	ng												
망	Context Visibility	FIPS Mode Security Settings		APIS	Settings										
×	Operations	Alarm Settings		Overview	API Service	e Settings API G	ateway Settings								
-0	Policy	General MDM / U	JEM Settings	API Ser	vices Overvie	w									
8.	Administration	Posture		> You can n	nanage Cisco ISE	nodes through two s	ets of API forma	ts-External Restful Ser	rvices (ERS) and OpenAPI.						
đ	Work Centers	Profiling		The ERS a Currently,	and 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	ported for ERS APIs in late	r					
		Protocols		> Gisco ISE 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 Scripte		> To use eit	in the API Service Settings tab. 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://10 For opena ERS_V1	information on IS 0.106.33.92:4424 pi documention	E ERS API, please vis to/ers/sdk for ERS, click below:	sit:								
		System Time API Settings Data Connect		For more https://10	information on IS 1.106.33.92:4424	E Onen API, niezse v 40/api/swagger-ui/ind ERS APA	isit: lex.html								

Visitez OpenAPI

## **Exemples** Python

Obtenir Tous Les Certificats Système D'Un Noeud Particulier

L'API répertorie tous les certificats d'un noeud ISE particulier.

Étape 1 : informations requises pour un appel API.

Méthode	GET

URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname></ise-node-hostname></ise-pan-ip>
Identifiants	Utiliser les informations d'identification du compte Open API
Header (En-tête)	Accepter : application/json Content-Type : application/json

Étape 2 : Localisez l'URL utilisée pour récupérer les certificats d'un noeud ISE particulier.

Swagger.	Select a	definition Certificates	~
Cisco ISE API - Certificates	9.9) (7A5)		
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/vl/certs/certificate-signing-request Ge	terate a Certificate Signing Request (CSR)		✓ ≜
GET /api/vl/certs/certificate-signing-request/{h	<pre>stName}/{id} Get the certificate signing request for a given ID</pre>		✓ ≜
DELETE /api/vl/certs/certificate-signing-request/{h	<pre>stName}/{id} Delete the certificate signing request for a given ID</pre>		✓ ≜
GET /api/vl/certs/certificate-signing-request/ex	<pre>port/{hostname}/{id} Export a CSR for a given CSR ID and hostna</pre>	ime	~ ≜
POST /api/vl/certs/certificate-signing-request/in	termediate-ca Generate an intermediate CA CSR (certificate signing r	equest)	~ ≜
POST /api/vl/certs/ise-root-ca/regenerate Regenerate	entire internal CA certificate chain including root CA on the primary PAN an	d subordinate CAs on the PSNs (Applicable only	y for internal CA service) 🗸 🔒
POST /api/v1/certs/renew-certificate Renew certificates	of OCSP responder and Cisco ISE Messaging Service		~ ≜
POST /api/vl/certs/signed-certificate/bind Bind CAS	Signed Certificate		~ ≜
CET /api/vl/certs/system-certificate/{hostName}	Set all system certificates of a particular node		^ ≜
This API supports filtering, sorting and pagination.			

#### URI API

Étape 3 : Voici l'exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer sous un fichier python à exécuter.

Assurez-vous de la bonne connectivité entre ISE et le périphérique exécutant l'exemple de code 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())
```

Voici l'exemple des résultats attendus.

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

Obtenir le certificat système d'un noeud particulier par ID

Cette API fournit les détails d'un certificat système d'un noeud particulier en fonction d'un nom d'hôte et d'un ID donnés.

Étape 1 : informations requises pour un appel API.

Méthode	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>
Identifiants	Utiliser les informations d'identification du compte Open API
Header (En-tête)	Accepter : application/json Content-Type : application/json

Étape 2 : Localisez l'URL utilisée pour récupérer le certificat d'un noeud particulier en fonction du nom d'hôte et de l'ID donnés.

Cisco ISE API - Certificates (ISO) (ASS) Inter 1710 100 33 02 44240raphy Steel-dect Tyroup-Continents	
Servers https://10.108.33.92:44240 - Inferred Url v	
certs-api-controller the certs API	~
Certificates	^
OET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	<ul> <li>↓ ≜</li> </ul>
POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	<ul> <li>✓ ≜</li> </ul>
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	<ul> <li>✓ ≜</li> </ul>
GET /api/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a CSR for a given CSR ID and hostname	<ul> <li>✓ ≜</li> </ul>
POST /api/v1/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	<ul> <li>✓ ≜</li> </ul>
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)	<ul> <li>✓ ≜</li> </ul>
POST /api/v1/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	<ul> <li>✓ ≜</li> </ul>
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	<ul> <li>✓ ≜</li> </ul>
GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	<ul> <li>↓ ≜</li> </ul>
GET /api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID	<b>^ ≜</b>
This API provides details of a system certificate of a particular node based on given hostname and ID.	

URI API

Étape 3 : Voici l'exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer sous un fichier python à exécuter.

Assurez-vous de la bonne connectivité entre ISE et le périphérique exécutant l'exemple de code 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:")
```



Remarque : l'ID provient des sorties d'API à l'étape 3 de « Get All System Certificates Of A Particular Node », par exemple, 5b5b28e4-2a51-495c-8413-610190e1070b is « Default self-signed saml server certificate - CN=SAML\_ISE-DLC-CFME02-PSN.cisco.com ».

Voici l'exemple des résultats attendus.

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

#### Obtenir La Liste De Tous Les Certificats Approuvés

L'API répertorie tous les certificats approuvés du cluster ISE.

Étape 1 : informations requises pour un appel API.

Méthode	GET
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate</ise-pan-ip>
Identifiants	Utiliser les informations d'identification du compte Open API
Header (En-tête)	Accepter : application/json Content-Type : application/json

Étape 2 : Localisez l'URL utilisée pour récupérer les certificats de confiance.

POST       /spi/vl/certs/ise-reod-cs/regenerate       Regenerate entry internal CA cartificate chain including root CA on the primary PNN and subordinate CAs on the PNNs (Applicable only for Internal CA service)         POST       /spi/vl/certs/remear-cartificate       Remove certificates of OCSP responder and Cisco ISE Messaging Service       Image: Comparison of Cisco ISE Messaging Service         POST       /spi/vl/certs/system-certificate/hand Bind CA Signed Certificate       Image: Comparison of Cisco ISE       Image: Comparison of Cisco ISE         GET       /spi/vl/certs/system-certificate/(hostName). Get all system certificate of a particular node by ID       Image: Comparison of Cisco ISE         PUT       /spi/vl/certs/system-certificate/(hostName)./(id)       Get all system certificate       Image: Comparison of Cisco ISE         PUT       /spi/vl/certs/system-certificate/(hostName)./(id)       Undets data for existing system certificate       Image: Comparison of Cisco ISE         PUT       /spi/vl/certs/system-certificate/(hostName)./(id)       Undets data for existing system certificate       Image: Comparison of Cisco ISE         POST       /spi/vl/certs/system-certificate/Lappert       Expont a system certificate ID       Image: Comparison of Cisco ISE       Image: Compare: Comparison of Cisco ISE	POST /api/vl/certs/certificate-signing-request/intermediate-ca Generate an intermediate CA CSR (certificate signing request)	~ ≜
POST       /api/vl/certs/signed-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Senice <ul> <li>POST</li> <li>/api/vl/certs/signed-certificate/bind</li> <li>End CA Signed Certificate</li> <li>QET</li> <li>/api/vl/certs/system-certificate/(hostName)/(id)</li> <li>Get Vapi/vl/certs/system-certificate/(hostName)/(id)</li> <li>Get Vapi/vl/certs/system-certificate/(hostName)/(id)</li> <li>Get Vapi/vl/certs/system-certificate/(hostName)/(id)</li> <li>Update data for existing system certificate</li> </ul> <li>POST /api/vl/certs/system-certificate/(hostName)/(id)</li> <li>Update data for existing system certificate</li> <li>Intel /api/vl/certs/system-certificate/sport Export a system certificate UD</li> <li>Intel /api/vl/certs/system-certificate/sport Export a system certificate Generate self-signed certificate in Cisco ISE</li> <li>Intel /api/vl/certs/system-certificate/import Import system certificate Generate self-signed certificate in Cisco ISE</li> <li>Intel /api/vl/certs/system-certificate/import system certificate</li> <li>Intel /api/vl/certs/system-certificate/import system certificate</li> <li>Intel /api/vl/certs/system-certificate/import system certificate</li> <li>Intel /api/vl/certs/system-certificate/import Import system certificate</li> <li>Intel /api/vl/certs/system-certificate/import</li> <li>Intel /api/vl/certs/system-certificate/import Import system certificate</li> <li>Intel</li>	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/system-certificate/bind Bind CA Signed Certificate         GBT       /api/vl/certs/system-certificate/(hostName) Get all system certificate of a particular node         GBT       /api/vl/certs/system-certificate/(hostName)/(id) Get system certificate of a particular node by ID         GBT       /api/vl/certs/system-certificate/(hostName)/(id) Update data for existing system certificate         PUT       /api/vl/certs/system-certificate/(hostName)/(id) Update data for existing system certificate         QBLETE       /api/vl/certs/system-certificate/(hostName)/(id) Delete System Certificate by ID and hostname         POST       /api/vl/certs/system-certificate/(appert Export a system certificate ID         POST       /api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cloco ISE         POST       /api/vl/certs/system-certificate/import Import system certificate in Cloco ISE         QBET       /api/vl/certs/trusted-certificate         The API supports Filtering, Sorting and Pagination.         Filtering and Sorting are supported for the following attributes:         * Second/Name       *         * Se	POST /api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	~ ≜
GET       /api/v1/certs/system-certificate/(hostName) Get all system certificate 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         PUT       /api/v1/certs/system-certificate/(hostName)/(id) Update data for existing system certificate         PUT       /api/v1/certs/system-certificate/(hostName)/(id) Delete System Certificate by ID and hostname         POST       /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 iD         POST       /api/v1/certs/system-certificate/generate-selfsigned-certificate ID         POST       /api/v1/certs/system-certificate/seport Import system certificate in Claco ISE         POST       /api/v1/certs/system-certificate/import Import system certificate in Claco ISE         CET       /api/v1/certs/trusted-certificate         Filtering and Sorting and Plagination.         Filtering and Sorting and Plagination.         * Supported for the following attributes:         * Supported Date Format yyy-MMA do Hit mm ss         * Supported Coreaters, EQ, NG, OT and LT         * Supported Date Format yyy-MMA do Hit mm ss         * Supported Coreaters, EQ, NG, OT and LT         *	POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	~ ≜
GET       /api/vl/certs/system-certificate/{hostName}/{id}       Get system certificate of a particular node by ID       Image: Certificate of the certificate of the certificate of the certificate         PUT       /api/vl/certs/system-certificate/{hostName}/{id}       Update data for existing system certificate       Image: Certificate of the certificate	GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	~ ≜
PUT       /api/vl/certs/system-certificate/{hostName}/{id}       Update data for existing system certificate         OELDTE       /api/vl/certs/system-certificate/{hostName}/{id}       Delete System Certificate by ID and hostname         POST       /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 by ID and hostname         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       Import system certificate         OELT       /api/vl/certs/system-certificate       Det ist of all husted certificates       Import system certificate         OELT       /api/vl/certs/system-certificate       Det ist of all husted certificates       Import system certificate         This API supports Filtering, Sorting and Pagination.       Import system certificate       Import system certificate         * isoported for the following attributes:       * isoported for the following attributes:       * isoported for the following attributes:         * supported for the following attributes:       * supported for the following attributes:       * isoported for paraters: EQ.NGO	GET /api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID	~ ≜
DELETE       /spi/vl/certs/system-certificate/(hostName)/{id}       Delete System Certificate by ID and hostname <ul> <li>POST</li> <li>/spi/vl/certs/system-certificate/export</li> <li>Export a system certificate with a given a certificate ID</li> <li>POST</li> <li>/api/vl/certs/system-certificate/export</li> <li>POST</li> <li>/api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Clico ISE</li> <li>POST</li> <li>/api/vl/certs/system-certificate/import</li> <li>(POST</li> <li>/api/vl/certs/system-certificate/import</li> <li>(POST</li> <li>/api/vl/certs/trusted-certificate</li> <li>Get fist of all trusted certificates</li> <li>POST</li> <li>/api/vl/certs/trusted-certificate</li> <li>Get fist of all trusted certificates</li> <li>POST</li> <li>/spond Sorting are supported for the following altributes:</li> <li>Support Sittering, Sorting are supported for the following altributes:</li> <li>Supported DiaF format: yyy-MM-dd Hit mm ss             <ul> <li>Supported DiaF format: yyyy-MM-dd Hit mm ss             <ul> <li>Supported DiaF</li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul></li></ul>	PUT /api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate	∨ ≜
POST       /api/vl/certs/system-certificate/export       Export a system certificate with a given a certificate ID <ul> <li>POST</li> <li>/api/vl/certs/system-certificate/generate-salfsigned-certificate Generate self-signed certificate In Cisco ISE</li> <li>POST</li> <li>/api/vl/certs/system-certificate/import</li> <li>Import system certificate in Cisco ISE</li> <li>Import /api/vl/certs/system-certificate/import</li> <li>Import system certificate in Cisco ISE</li> <li>Import /api/vl/certs/trusted-certificate</li> <li>OET</li> <li>/api/vl/certs/trusted-certificate</li> <li>Import System certificate</li> <li>Import System Certificate Certificate</li> <li>Import System Certificate<td>DELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname</td><td>~ ≜</td></li></ul>	DELETE /api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname	~ ≜
PDST       /api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE         PDST       /api/vl/certs/system-certificate/import       Import system certificate in Cisco ISE         QET       /api/vl/certs/trusted-certificate       Cet list of all trusted certificates         This API supports Filtering, Sorting and Pagination.         Filtering and Sorting are supported for the following attributes:         timedificate         * Support         * Supported Date Format: yyy-MMAd Hit mm ss         * Supported Date Format: yyy-MMAd Hit mm ss         * Supported Dot Format: yyy-MMAd Hit mm ss         * Supported Date Format: yyy-MMA di Hit mm ss         * Supported Date Format: yyy-MMA di Hit mm ss         * Supported Date Format: yyy-MMA di Hit mm ss         * Supported Date Format: yy-MMA di Hit mm ss         * Supported Date Format: yy-MMA di Hit mm ss         * Supported Date Format: yy-MMA di Hit mm ss         * Supported Date Format: yy-MMA di Hit mm ss         * Supported Date Format: yy-MMA di Hit mm ss         * Supported Date Format: yy-MMA di Hit mm ss         * Supported Date Format: yy-MMA di Hit mm ss         * Supported Date Format:	POST /api/v1/certs/system-certificate/export Export a system certificate with a given a certificate ID	~ ≜
POST       /api/v1/certs/system-certificate/import       Import system certificate in Clicco 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:         • finds/Name         • supports         • suppor	POST /api/vl/certs/system-certificate/generate-selfsigned-certificate Generate self-signed certificate in Cisco ISE	∨ ≜
OET       /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:         fining/Name         support         Suport         Suppor	POST /api/vl/certs/system-certificate/import Import system certificate in Cisco ISE	~ ≜
This API supports Filtering, Sorting and Pagination.  Filtering and Sorting are supported for the following attributes:  finandhykame subject stauedfe support Subject	GET /api/v1/certs/trusted-certificate Oet list of all trusted certificates	^ ≜
Filtering and Sorting are supported for the following attributes: transflytame subject subject subject Supported Date Format: yyy-MM-dd Hit mm:ss Supported Date Format: yyy-MM-dd Hit mm:ss Su	This API supports Filtering, Sorting and Pagination.	
Accelerative enabled, diskend     Supported Operators     Eo, NRO	Filtering and Sorting are supported for the following attributes: • tireds/Name • stated • statedTo • statedTo • statedTo • statedTo • supported Date Format: yyy-AM-dd Hit mm:ss • Supported Date Format: yyy-AM-dd Hit mm:ss • Supported Date Format: yyy-AM-dd Hit mm:ss • Supported Dates: ED, NEQ, OT and LT • states: • Supported Dates: ED, NEQ, OT and LT • states: • Supported Dates: enabled, disabled • Supported Operations: ED, NEQ • Supported Operations: ED, NEQ	

URI API

Étape 3 : Voici l'exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer sous un fichier python à exécuter.

Assurez-vous de la bonne connectivité entre ISE et le périphérique exécutant l'exemple de code 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:")

Voici l'exemple des résultats attendus.(Omis)

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

#### Obtenir le certificat de confiance par ID

Cette API peut afficher les détails d'un certificat de confiance basé sur un ID donné.

	Étap	be 1	:	information	tions	requises	pour	un	appel	API
--	------	------	---	-------------	-------	----------	------	----	-------	-----

Méthode	GET
URL	https:// <ise-pan-ip>/api/v1/certs/trusted- certificate/<id-of-certificate></id-of-certificate></ise-pan-ip>
Identifiants	Utiliser les informations d'identification du compte Open API
Header (En-tête)	Accepter : application/json Content-Type : application/json

Étape 2 : localisez l'URL utilisée pour récupérer les informations de déploiement.

Cisco ISE API - Certificates (ISO) (CISS) Integration 106.33.02.44280agev/3hgs-docs/forcuper-Centicates	
Servers https://10.106.33.92:44240 - Interred Url V	
certs-api-controller the certs API	~
Certificates	^
GET /api/vi/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	- 🛍
POST /api/vl/certs/certificate-signing-request Generate a Certificate Signing Request (CSR)	A matrix and a
CET /api/vl/certs/certificate-signing-request/{hostName}/{id} Get the certificate 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/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 /spi/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	
This API provides details of a system certificate of a particular node based on given hostname and ID.	

URI API

Étape 3 : Voici l'exemple de code Python. Copiez et collez le contenu. Remplacez l'adresse IP ISE, le nom d'utilisateur et le mot de passe. Enregistrer sous un fichier python à exécuter.

Assurez-vous de la bonne connectivité entre ISE et le périphérique exécutant l'exemple de code 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:")
```



**Remarque** : l'ID provient des sorties d'API à l'étape 3 de « Get List Of All Trusted Certificates », par exemple, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 est « VeriSign Class 3 Public Primary Certification Authority ».

Voici l'exemple des résultats attendus.

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

Pour résoudre les problèmes liés aux API ouvertes, définissez le niveau de journalisation pour theapiservicomponent sur DEBUGdans la

#### fenêtre de configuration du journal de débogage.

Pour activer le débogage, accédez à **Opérations -> Dépannage -> Assistant de débogage -> Configuration du journal de débogage ->** Noeud ISE -> apiservice.

≡	diada Identity Services	Engine	Operations / Troubleshoot				A License Warning	Q	۵	0	<b>Q</b>	A	
щ	Bookmarks	Diagnostic Tools Download Lo	ogs Del	bug Wizard									
≣ ≓ड <b>%</b>	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List > ISE-BOL-CFME01-PAN.shield.com Debug Level Configuration									6	3
-0	Policy		0 Edit	← Reset to Default	Log Filter Enable	Log Filter Disable					AL S	- 5	7
80	Administration			Component Name	A Log Level	Description	Log file Name	Log Filter					
-file	Work Centers		0	accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled				Ĩ	1
			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 Can	-psc.log	Disabled					
			0	ca-service	INFO	CA Service messages	caservice.log	Disabled					

Débogage du service API

Pour télécharger les journaux de débogage, accédez à **Opérations -> Dépannage -> Journaux de téléchargement -> Noeud PAN ISE -> Journaux de débogage.** 

≡	diale Identity Services	Engine		Operations / Trou	🔺 License Warning	Q	۵	0	Ф   А		
Ц	Bookmarks	Diagnostic Too	Download Logs	Debug Wizard							
- 55	Dashboard	15	SE-BGL-CFME01-PAN								
망	Context Visibility	15	SE-BGL-CFME02-MNT	Collapse A Collapse A	All Control of Control						
×	Operations		SE-DLC-CFME01-PSN	Debug Log Type	Log File	Description	Size				
0	Policy	15	SE-RTP-CFME01-PAN	✓ Application Logs							Î
8.	Administration	15	SE-RTP-CFME02-MNT	> ad_agent (1) (100 KB)							_
-fi	Work Centers	¢	,	> ai-analytics (11) (52 KB) > api-gateway (16) (124 KB)							
?	Interactive Help			✓ api-service (13) (208 KB)	sol, service (all lons)	ADI Sandra dahun massanas	208 8 8				
				0	api-service.log	Art Service debug messages	12 KB				
					api-service.log.2024-03-24-1		4.0 KB				
					api-service.log.2024-04-07-1		4.0 KB				

Télécharger les journaux de débogage

## À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.