

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

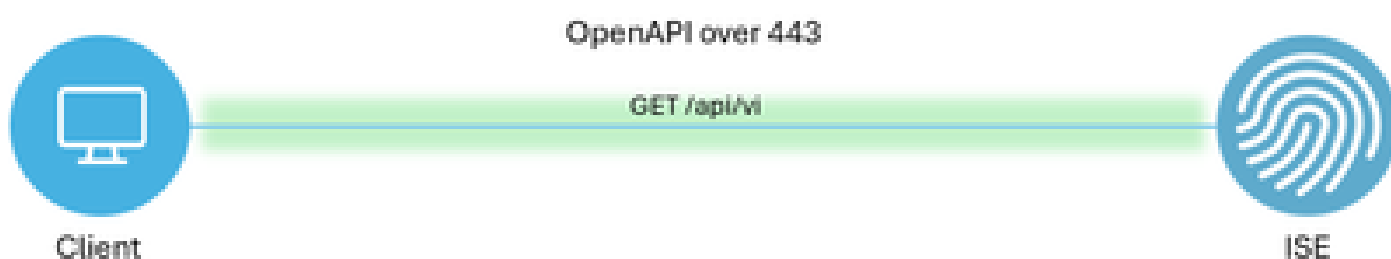
Composants utilisés

- 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 : Ajouter un compte admin API ouvert

Pour ajouter un administrateur d'API, accédez à Administration > System > Admin Access > Administrators > Admin Users > Add.

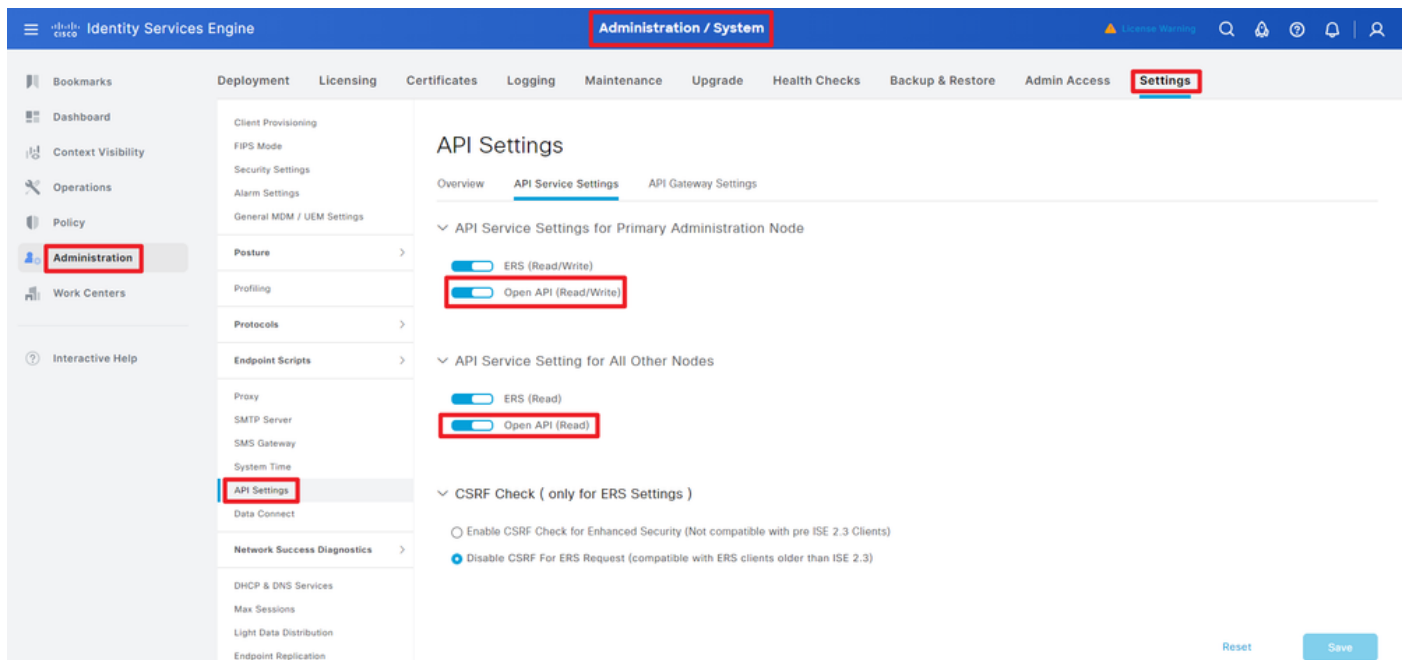
The screenshot shows the ISE Administration console. The 'Administration / System' tab is selected. In the left sidebar, 'Administration' is highlighted. In the main content area, the 'Admin Users' page is displayed, showing a table of administrators. The 'ApiAdmin' user is highlighted with a red box.

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

Administrateur API

Étape 2 : Activer l'API ouverte sur ISE

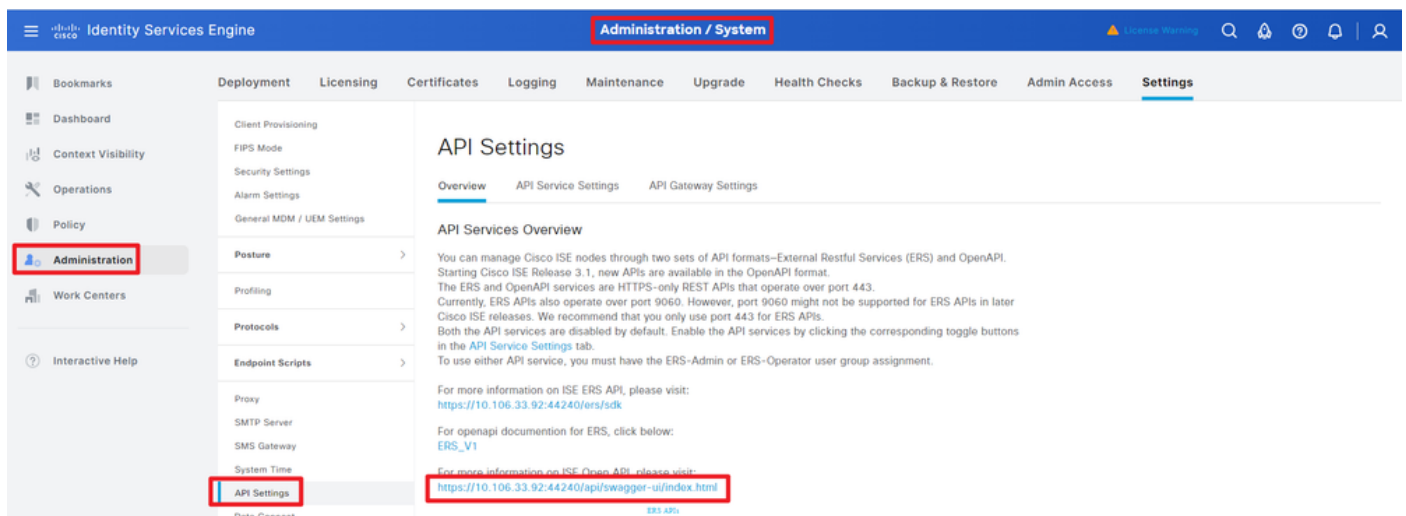
L'API ouverte est désactivée par défaut sur ISE. Pour l'activer, accédez à Administration > System > Settings > API Settings > API Service Settings. Activez les options de l'API ouverte. Cliquez sur Save.



Activer OpenAPI

Étape 3 : Explorez l'API ouverte ISE

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



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>
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.

The screenshot shows the Swagger UI for the Cisco ISE API - Certificates. The 'Certificates' section is expanded, showing a list of endpoints. The endpoint 'GET /api/v1/certs/system-certificate/{hostname}' is highlighted with a red box.

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>
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 1.0.0 QA55

<https://10.106.33.92:44240/api/v1/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 OSCP 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.	

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"
```

```
}
```

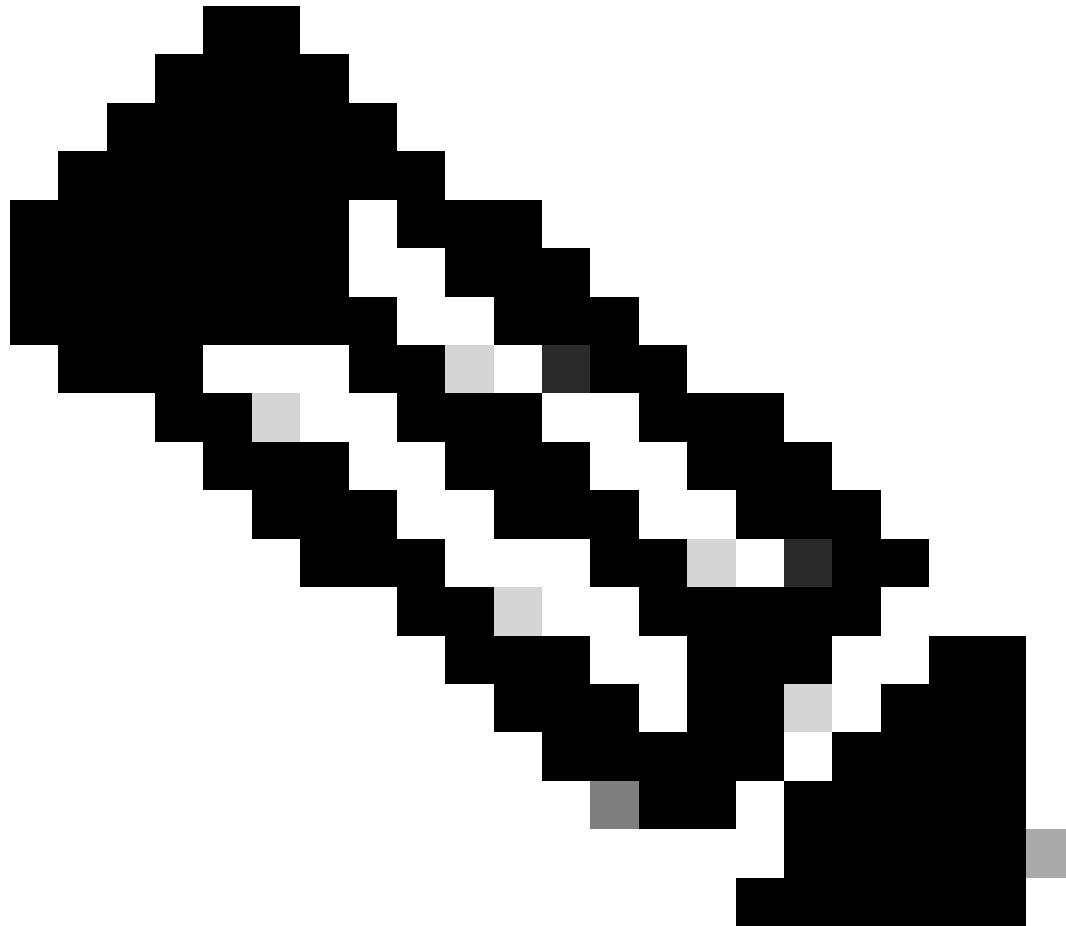
```
    basicAuth = HTTPBasicAuth(
```

```
"ApiAdmin", "Admin123"
```

```
)
```

```
    response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
    print("Return Code:")
```

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



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-PSN.cisco.com'}}

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
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.

The screenshot displays the Cisco ISE API Explorer interface. A list of API endpoints is shown, each with its method (POST, GET, PUT, DELETE), path, and description. The endpoint `GET /api/v1/certs/trusted-certificate` is highlighted with a red box. Below the list, the details for this endpoint are shown, including a note that the API supports filtering, sorting, and pagination. The supported attributes for filtering and sorting are listed:

- 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.

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:")
    print(response.status_code)
    print("Expected Outputs:")
    print(response.json())

```

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=VeriSign Class 3 Public Primary Certification Authority'}]}

Obtenir le certificat de confiance par ID

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

Étape 1 : Informations requises pour un appel API.

Méthode	GET
URL	https://<ISE-PAN-IP>/api/v1/certs/trusted-certificate/<ID-Of-Certificate>
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 1.0.0 OAS3

<https://10.106.33.92:44240/api/v1/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 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.			

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"

}

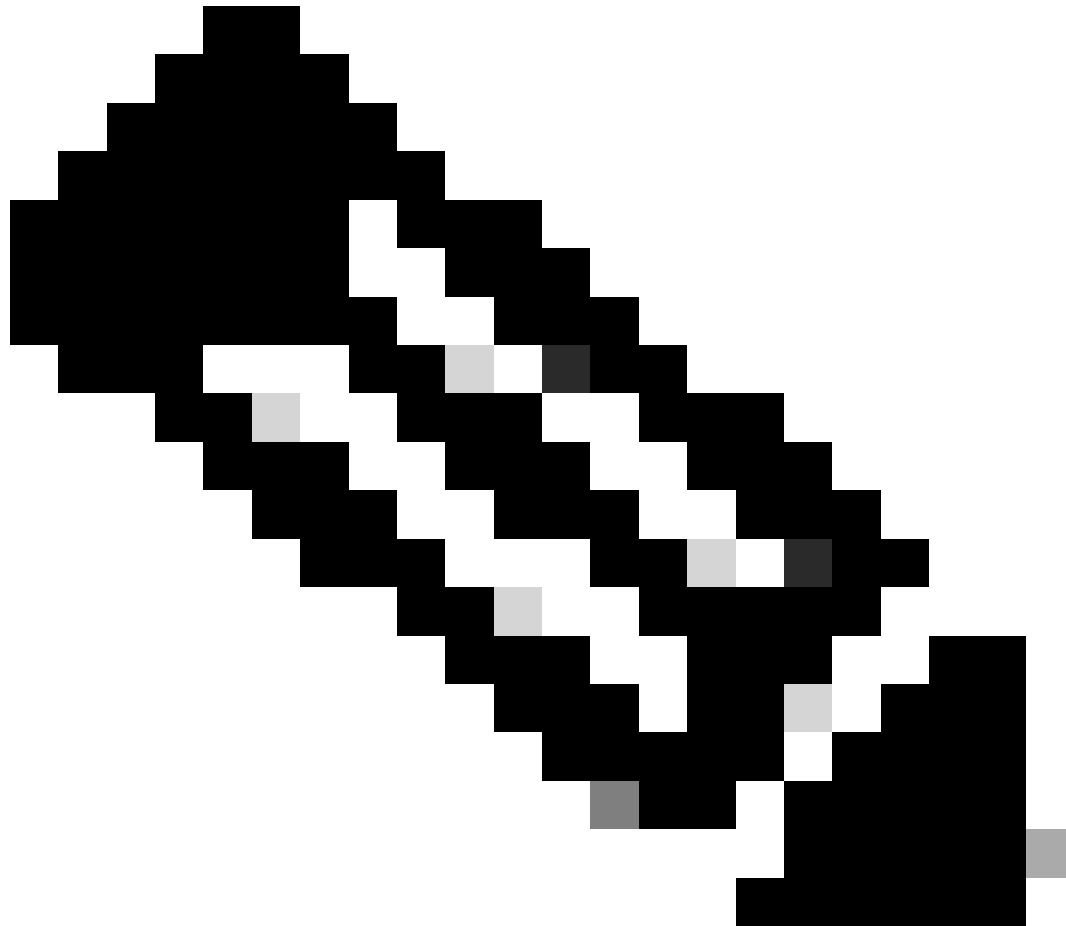
    basicAuth = HTTPBasicAuth(

"ApiAdmin", "Admin123"

)

    response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
    print("Return Code:")
```

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



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

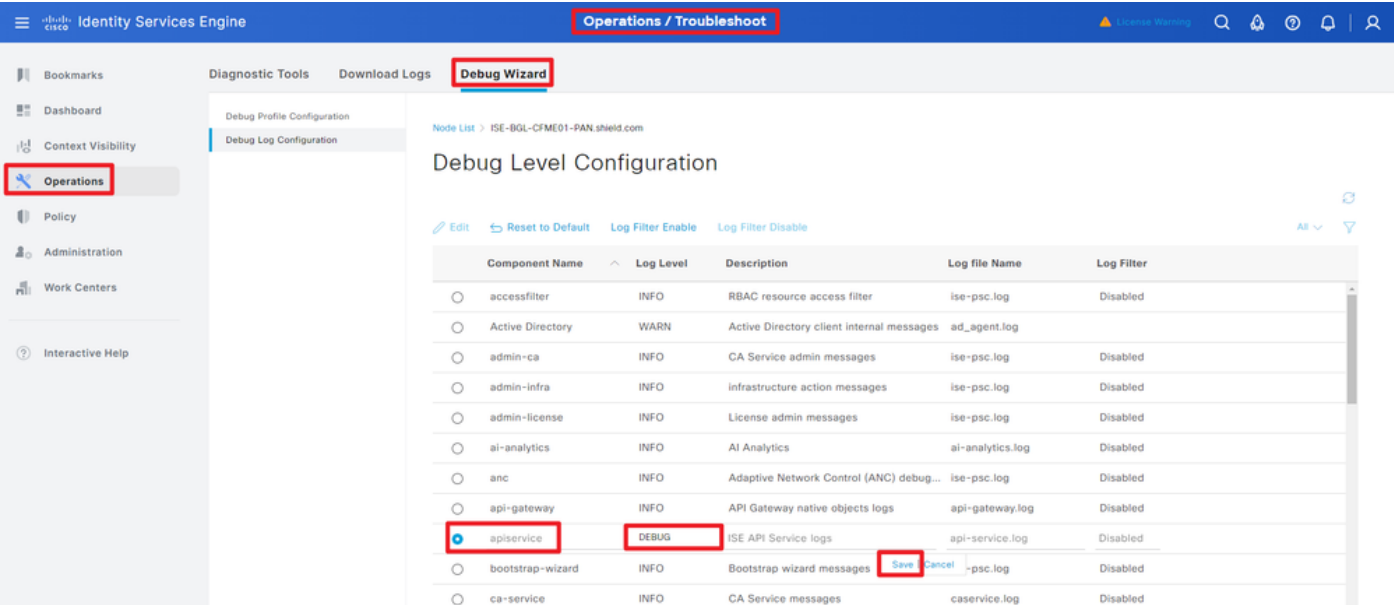
Expected Outputs:

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

Dépannage

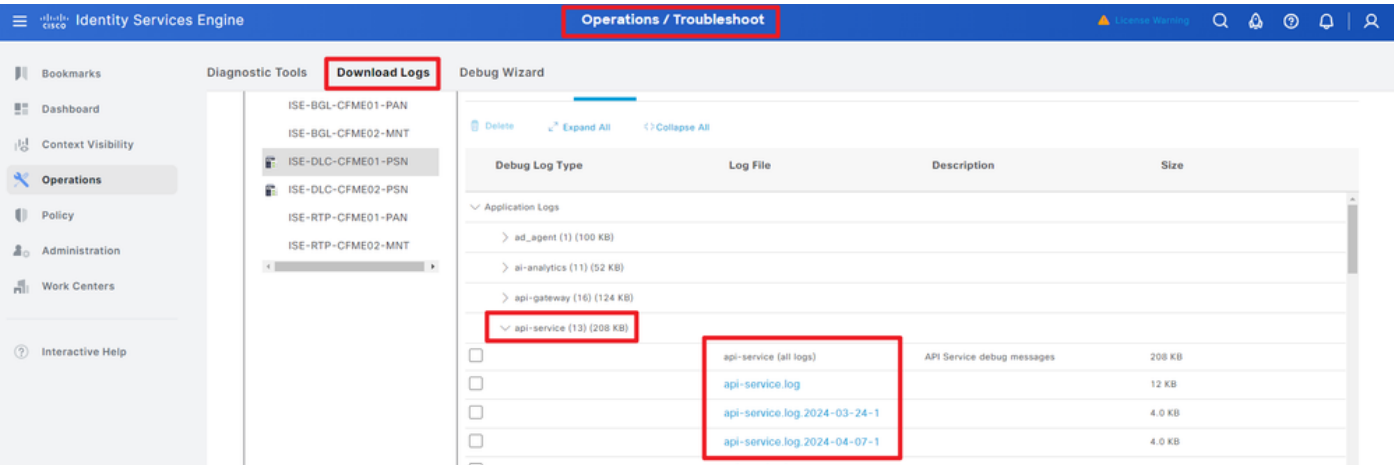
Pour résoudre les problèmes liés aux API ouvertes, définissez le niveau de journalisation pour theapiservicomponent sur DEBUG dans la fenêtre de configuration du journal de débogage.

Pour activer le débogage, accédez à Operations > Troubleshoot > Debug Wizard > Debug Log Configuration > ISE Node > apiservice.



Débogage du service API

Pour télécharger les journaux de débogage, accédez à Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs.



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.