

# 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

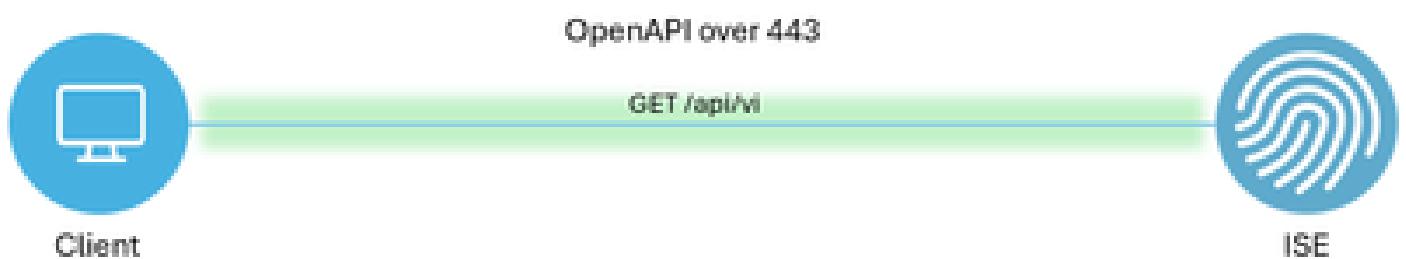
## Composants utilisés

- 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.

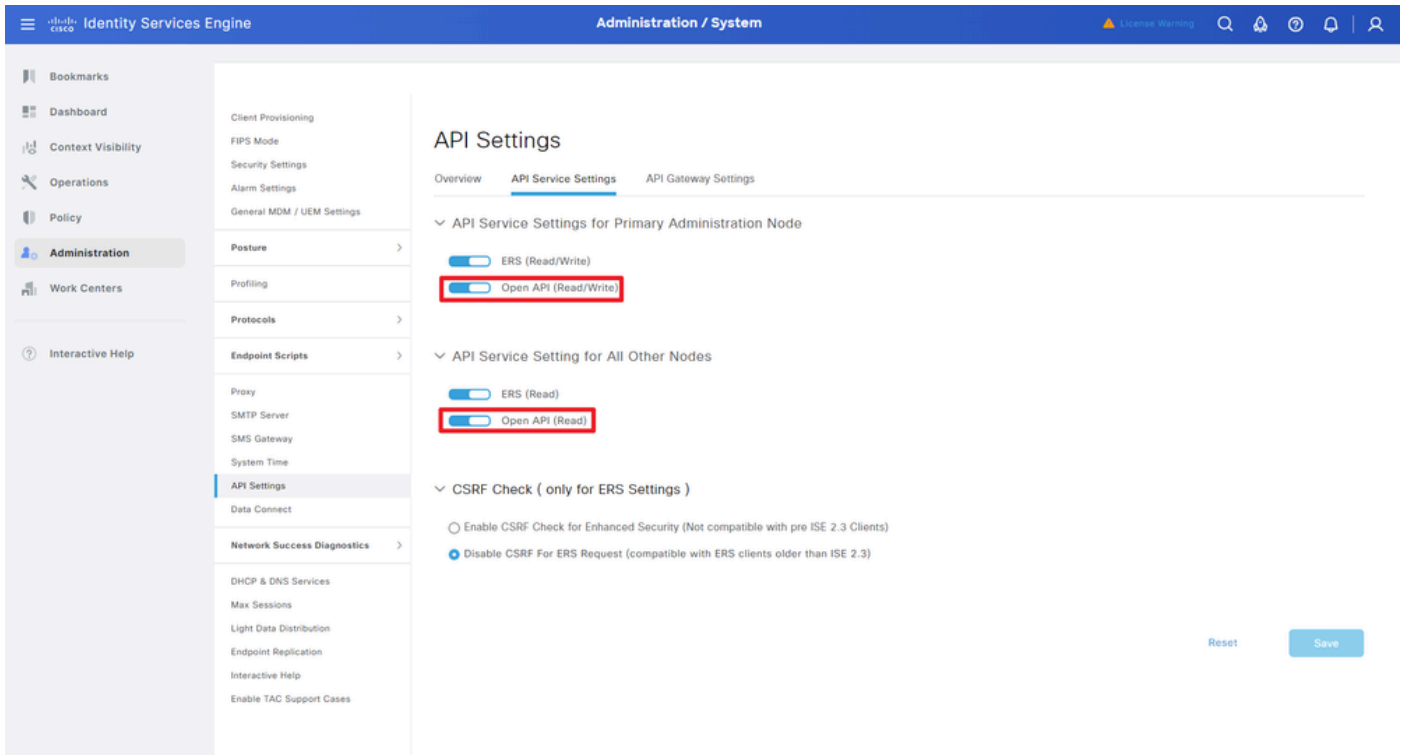
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The 'Administration / System' tab is selected. The 'Admin Users' section is highlighted in the left sidebar. The main content area displays a table of administrators:

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 : activez l'API ouverte sur ISE

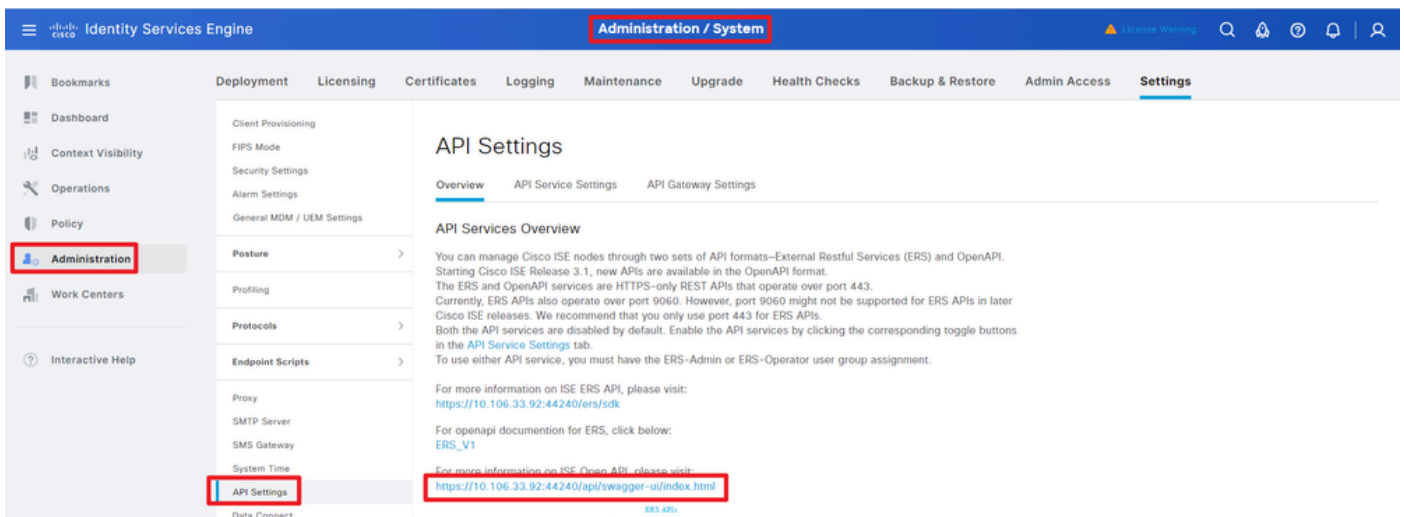
L'API ouverte est désactivée par défaut sur ISE. Pour l'activer, accédez à Administration > System > API Settings > API Service Settings. Activez les options de l'API ouverte. Cliquez sur Save.



Activer OpenAPI

### Étape 3 : Explorez l'API ouverte ISE

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



Visitez OpenAPI

### Exemples Python

Obtenir Tous Les Certificats Système D'Un Noeud Particulier

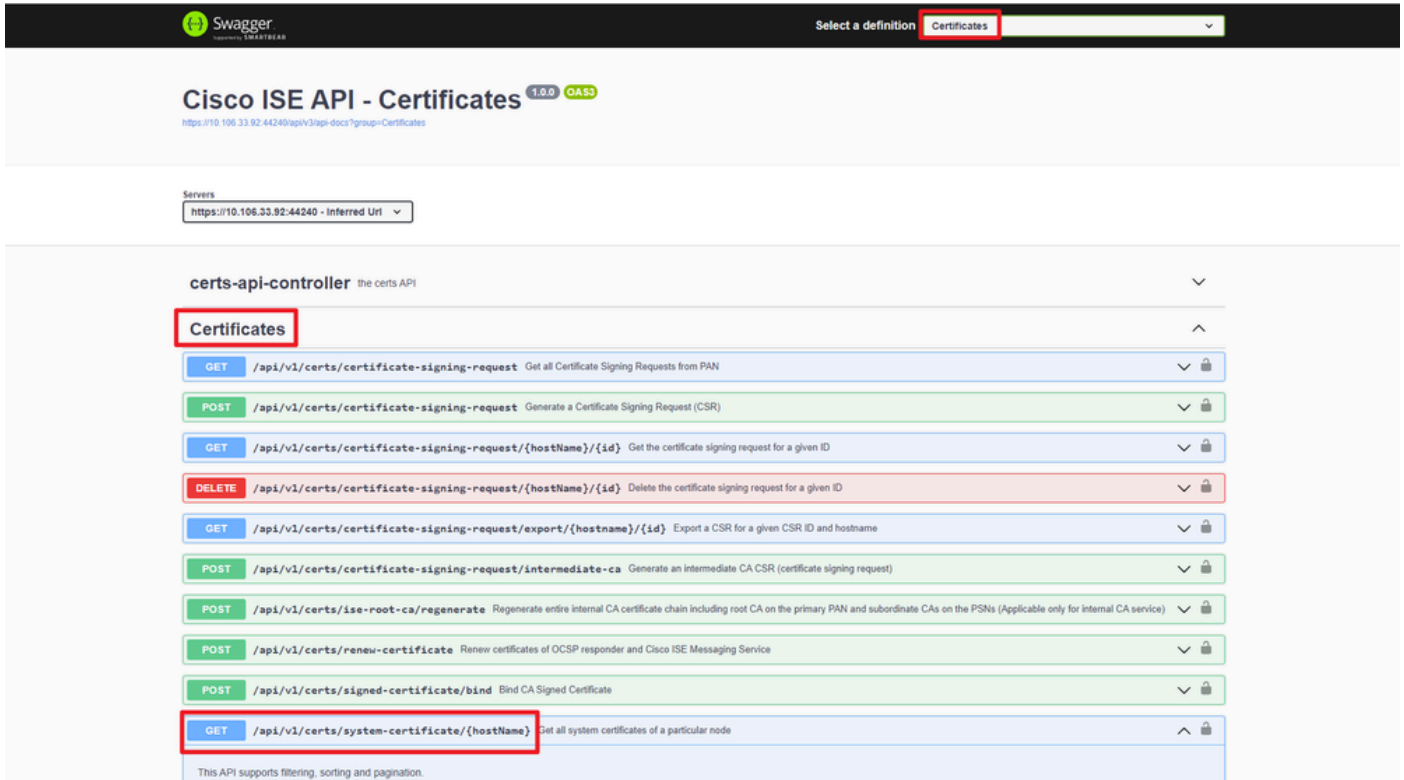
L'API répertorie tous les certificats d'un noeud ISE particulier.

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.



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 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		⌵
<b>Certificates</b>		⌴
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/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-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 shows the Cisco ISE API Explorer interface. A list of API endpoints is displayed, each with its method (POST, GET, PUT, DELETE), path, and description. The endpoint `/api/v1/certs/trusted-certificate` is highlighted with a red box. Below the list, there is a section titled "This API supports Filtering, Sorting and Pagination." followed by a list of supported attributes for filtering and sorting, including `friendlyName`, `subject`, `issuedTo`, `issuedBy`, `validFrom`, `expirationDate`, and `status`. A note at the bottom states: "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:")
```

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.

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/certs/docs?group=Certificates>

Servers

certs-api-controller the certs API	
<b>Certificates</b>	
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:")
```



**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 Certif

Dépannage

Pour résoudre les problèmes liés aux API ouvertes, définissez le niveau de **journalisation** pour theapiservicecomponent sur DEBUG dans 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**.

The screenshot shows the 'Debug Wizard' interface in the Cisco Identity Services Engine. The 'Debug Level Configuration' table is displayed, listing various components and their log levels. The 'apiservice' component is selected, and its log level is set to 'DEBUG'. The 'Save' button is highlighted.

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	Disabled
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
<b>apiservice</b>	<b>DEBUG</b>	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

### Débogage du service API

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

The screenshot shows the 'Download Logs' interface in the Cisco Identity Services Engine. The 'api-service (13) (208 KB)' log file is selected. The 'api-service (all logs)' entry is highlighted.

Debug Log Type	Log File	Description	Size
Application Logs			
>	ad_agent (1) (100 KB)		
>	ai-analytics (11) (52 KB)		
>	api-gateway (16) (124 KB)		
>	<b>api-service (13) (208 KB)</b>		
<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

### 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.