# Gebruik OpenAPI om informatie over ISEcertificaten op te halen op ISE 3.3

# Inhoud

Inleiding
Achtergrond
Voorwaarden
Vereisten
Gebruikte componenten
Configureren
Netwerkdiagram
Configuratie op ISE
Python-voorbeelden
Ontvang alle systeemcertificaten van een bepaald knooppunt
Systeemcertificaat van een bepaald knooppunt verkrijgen via ID
Een lijst met alle vertrouwde certificaten opvragen
Vertrouwenscertificaat per ID verkrijgen
Problemen oplossen

# Inleiding

Dit document beschrijft de procedure voor het gebruik van openAPI om het Cisco Identity Services Engine (ISE)-certificaat te beheren.

# Achtergrond

Geconfronteerd met toenemende complexiteit op het gebied van netwerkbeveiliging en -beheer voor ondernemingen, introduceert Cisco ISE 3.1 OpenAPI-geformatteerde API's die het beheer van de levenscyclus van certificaten stroomlijnen, en een gestandaardiseerde en geautomatiseerde interface bieden voor efficiënte en veilige certificaatbewerkingen, waardoor beheerders sterke beveiligingsprocedures kunnen afdwingen en netwerknaleving kunnen handhaven.

# Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Identity Services Engine (ISE)
- REST API

Python

### Gebruikte componenten

- ISE-lijnkaart 3.3
- Python 3.10.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Configureren

### Netwerkdiagram



## Configuratie op ISE

Stap 1: Voeg een Open API Admin account toe

Om een API-beheerder toe te voegen, navigeer naar Beheer > Systeem > Admin Access > Beheerders > Admin Gebruikers > Add.

≡	diala Identity Services E	Engine				Administra	tion / Syste	m			🔺 Ue	ense Warning	Q	۵ ۵	٥	A
Щ	Bookmarks	Deployment Licensing	Certi	ficates	Logging	Maintenance	Upgrade	Health Checks	Backup & F	Restore	Admin Access	Settings				
53	Dashboard	Authentication		Adm	inistrat											
1d	Context Visibility	Authorization	>	Adm	inistrat	ors										
К	Operations	Administrators	U	/ Edit	+ Add	Change Status	Delete						Sele	cted 0 Total	2 (2) All V	\$ 7
U	Policy	Admin Users			Status	Name	Descript	tion First Nam	e Last Name	Email Add	Iress Admin Grou	uns				i.
80	Administration	Admin Groups		0	Enabled	admin a	Default	Admin User			Super Adm	in				
, fili	Work Centers	Settings	>	0	Enabled	a ApiAdmin					ERS Admin					
?	Interactive Help															

API-beheerder

Stap 2: Open API inschakelen op ISE

Open API is standaard uitgeschakeld op ISE. Om het in te schakelen, navigeer naar Beheer > Systeem > Instellingen > API-instellingen > API-serviceinstellingen. Schakel de opties voor Open

### API in. Klik op Save (Opslaan).

$\equiv$ $\frac{\mathrm{deals}}{\mathrm{casce}}$ Identity Services En	ngine	Administration / System	🔺 License Warning 🛛 🛕 🕐 📮 🛛 🗙
J Bookmarks D	Deployment Licensing (	ertificates Logging Maintenance Upgrade Health Checks Backup & Restor	e Admin Access Settings
<ul> <li>Dashboard</li> <li>Context Visibility</li> <li>Operations</li> <li>Policy</li> <li>Administration</li> <li>Work Centers</li> <li>Interactive Help</li> </ul>	Client Provisioning FIPS Mode Security Settings Altern Settings General MDM / UEM Settings Posture 2 Protocols 2 Protocols 2 Protocols 2 Proxy. SMTP Server 3 System Time Data Connect 2 DHCP & DNS Services Max Sessions Taxa Protocols 2 Proxy. System Time Deta Sonnect 2 DHCP & DNS Services Max Sessions	API Settings       API Gateway Settings         Overview       API Service Settings for Primary Administration Node	
	Light Data Distribution		Reset Save

OpenAPI inschakelen

#### Stap 3: Verken de open API van ISE

Ga naar Beheer > Systeem > Instellingen > API-instellingen > Overzicht. Klik op Open API bezoek link.

≡	dentity Services E	Engine				Administra	tion / Syste	m		<b>A</b>	License Warning	Q	۵ ۵	0   A
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings			
	Dashboard Context Visibility	Client Provisioning FIPS Mode		API S	Settings									
*	Operations	Alarm Settings		Overview	API Servic	e Settings API G	ateway Setting	1						
-0	Policy	General MDM / UE	M Settings	API Sen	vices Overvie	w								
80	Administration	Posture		> You can m Starting C	anage Cisco ISI isco ISE Release	E nodes through two : 3.1, new APIs are a	sets of API form vailable in the O	ats-External Restful Se penAPI format.	rvices (ERS) and OpenAPI.					
di	Work Centers	Profiling		The ERS a Currently,	nd OpenAPI ser ERS APIs also o	vices are HTTPS-only perate over port 906	y REST APIs tha 0. However, por	t operate over port 443 t 9060 might not be su	pported for ERS APIs in late	r				
		Protocols		> Both the AP	releases. We re PI services are	commend that you or disabled by default. E	ily use port 443 Enable the API s	for ERS APIs. ervices by clicking the o	corresponding toggle buttor	15				
?	Interactive Help	Endpoint Scripts		> To use eith	her API service,	you must have the Ef	RS-Admin or ER	S-Operator user group	assignment.					
		Proxy SMTP Server SMS Gateway		For more i https://10 For opena ERS_V1	nformation on IS 106.33.92:442 pi documention	SE ERS API, please vi 40/ers/sdk for ERS, click below:	sit:							
	I	System Time API Settings		For more https://10	nformation on 15 .106.33.92:442	SE Open APL please ( 40/api/swagger-ui/in	dex.html							



### Python-voorbeelden

Ontvang alle systeemcertificaten van een bepaald knooppunt

De API geeft een lijst van alle certificaten van een bepaald ISE-knooppunt.

Stap 1: Vereiste informatie voor een API-oproep.

Methode KRIJGEN
-----------------

URL	https:// <ise-pan-ip>/api/v1/certs/system- certificate/<ise-node-hostname></ise-node-hostname></ise-pan-ip>					
referenties	Open API-accountreferenties gebruiken					
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json					

Stap 2: Zoek de URL die wordt gebruikt om certificaten van een bepaalde ISE-knooppunt op te halen.

H Swagger. Select a definition Certificates	×
Cisco ISE API - Certificates (ISB) (ASS) http://10.106.33.82-447401epi/Valepi-docs/prouge-Certificates	
Servers https://10.106.33.92:44240 - Inferred Url V	
certs-api-controller the certs API	~
Certificates	^
CET /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/vi/certs/certificate-signing-request/{hostName}/{id} Delete the certificate signing request for a given ID	· 🛍
CET /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/vi/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	<b>a</b>
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	. <b>ii</b>
This API supports filtering, sorting and pagination.	

API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

<#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())
```

Hier is het voorbeeld van de verwachte 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
```

Systeemcertificaat van een bepaald knooppunt verkrijgen via ID

Deze API geeft details van een systeemcertificaat van een bepaald knooppunt op basis van een gegeven hostnaam en ID.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
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>
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om het certificaat van een bepaald knooppunt op te halen op basis van de gegeven hostnaam en ID.

Cisco ISE API - Certificates C C C C C C C C C C C C C C C C C C C	
Servers https://10.106.33.92.44240 - Inferred Url v	
certs-api-controller the corts API	~
Certificates	^
GET /api/vl/certs/certificate-signing-request Get all Certificate Signing Requests from PAN	✓ â
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	<ul><li>✓ â</li></ul>
GET /api/vl/certs/certificate-signing-request/export/{hostname}/{id} Export a GSR for a given CSR ID and hostname	✓ ≜
POST /api/vl/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)	✓ ≜
POST /api/vl/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	~ <b>a</b>
OET         /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	∧ ≜
This API provides details of a system certificate of a particular node based on given hostname and ID.	

#### API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

#### <#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:")
```



Opmerking: de ID is afkomstig van API-uitgangen in stap 3 van "Get All System Certificates Of A Particular Node", bijvoorbeeld, 5b5b28e4-2a51-495c-8413-610190e1070b is "Default self-signed saml server certificate - CN=SAML\_ISE-DLC-CFME02-PSN.cisco.com".

Hier is het voorbeeld van de verwachte 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

Een lijst met alle vertrouwde certificaten opvragen

De API maakt een lijst van alle vertrouwde certificaten van ISE-cluster.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN					
URL	https:// <ise-pan-ip>/api/v1/certs/Trusted- certificate</ise-pan-ip>					
referenties	Open API-accountreferenties gebruiken					
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json					

Stap 2: Zoek de URL die wordt gebruikt om vertrouwde certificaten op te halen.

POST	/api/vl/certs/certificate-signing-request/intermediate-ca Generate an Intermediate CA CSR (certificate signing request)	$\sim$	ú
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)	$\sim$	í
POST	/api/vl/certs/renew-certificate Renew certificates of OCSP responder and Cisco ISE Messaging Service	~	í
POST	/api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	~	é
GET	/api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular node	$\sim$	ú
GET	/api/vl/certs/system-certificate/{hostName}/{id} Get system certificate of a particular node by ID	$\sim$	ú
PUT	/api/vl/certs/system-certificate/{hostName}/{id} Update data for existing system certificate	$\sim$	i
DELETE	/api/vl/certs/system-certificate/{hostName}/{id} Delete System Certificate by ID and hostname	$\sim$	i
POST	/api/v1/certs/system-certificate/export Export a system certificate with a given a certificate ID	$\sim$	i
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 Claco ISE	~	
GET	/api/vl/certs/trusted-certificate Get list of all trusted certificates	^	
This API s	upports Filtering, Sorting and Pagination.		
Elitering a	of Postine we recented for the followine stickeday:		
<ul> <li>frier</li> </ul>	na sorung are supported for the following autoures. dyName		
<ul> <li>subj</li> <li>issu</li> </ul>	kđ Mil		
<ul> <li>valk</li> </ul>	Gey Form		
	s Supported Operations: EQ. NEG. Of and LT Supported Operations: EQ. NEG. Of and LT		
• exp	asonuane Supported Date Format: yyyy-MM-dd HH:mm ss		
<ul> <li>stati</li> </ul>	supported Operators: EQ, NEC, OI and LT		
	Autoved values, enboled, oldabled     Supported Cystanters, ED, NEO		
Note: ISE i	ternal CA certificates will not be exported.		

API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

#### <#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:")

Hier is het voorbeeld van de verwachte output.(weggelaten)

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

#### Vertrouwenscertificaat per ID verkrijgen

Deze API kan details van een vertrouwenscertificaat weergeven op basis van een gegeven ID.

Stap 1: Ve	reiste inforr	natie voor e	een API-o	proep.
------------	---------------	--------------	-----------	--------

Methode	KRIJGEN
URL	https:// <ise-pan-ip>/api/v1/certs/Trusted- certificate/<id-of-certificate></id-of-certificate></ise-pan-ip>
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om implementatieinformatie op te halen.

Cisco ISE API - 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)	<b>∨</b> ≜
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)	<b>∨ ≜</b>
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	<b>∨ ≜</b>
POST /api/vl/certs/signed-certificate/bind Bind CA Signed Certificate	~ ≜
GET /api/vl/certs/system-certificate/{hostName} Get all system certificates of a particular mode	~ ≜
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

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

#### <#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:")
```



**Opmerking**: De ID is afkomstig van API-uitgangen in stap 3 van "Get List Of All Trusted Certificates", bijvoorbeeld, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 is "VeriSign Class 3 Public Primary Certification Authority".

Hier is het voorbeeld van de verwachte outputs.

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

Om problemen op te lossen die betrekking hebben op de Open API's, stelt u het niveau Log voor deapiservice component in op DEBUG in het venster Debug Log Configuration.

Om debug in te schakelen, navigeer naar **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration > ISE Node > Appliance.** 

≡	dentity Services	Engine	Operations / Troubleshoot					A License Warning	Q	۵	0	٩	A
щ	Bookmarks	Diagnostic Tools Download Lo	gs Del	bug Wizard									
태 1년 <b>X</b>	Dashboard Context Visibility Operations	Debug Profile Configuration Debug Log Configuration	Node List	sise-bol-cfmeo1-pan.s	meld.com								8
0	Policy		0 Edit	← Reset to Default	Log Filter Enable	Log Filter Disable					AI	Ŷ	$\nabla$
8.	Administration			Component Name	∧ Log Level	Description	Log file Name	Log Filter					
nii:	Work Centers		0	accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled					1
			0	Active Directory	WARN	Active Directory client internal messages	ad_agent.log						1
?	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	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					

Debug van API-service

Als u debug-logbestanden wilt downloaden, navigeert u naar **Operations > Probleemoplossing > Downloadlogs > ISE PAN-knooppunt > Debug-logbestanden.** 

≡						Operations / Troubleshoot				Q	۵	0	$\varphi \mid \varphi$
н	Bookmarks	Diagn	iostic Tools	Download Logs	Debug Wiza	ard							
10	Dashboard		ISE-B	GL-CFME01-PAN									
110	Context Visibility		ISE-B	GL-CFME02-MNT	Delete	e <sup>®</sup> Expand All S≥Collapse A							
*	Operations		- ISE-D	C-CEME02-DSN	Debuş	g Log Type	Log File	Description	Size				
0	Policy		ISE-R	TP-CFME01-PAN	✓ Application	on Logs							1
8.	Administration		ISE-R	TP-CFME02-MNT	> ad	_agent (1) (100 KB)							_
ก็เ	Work Centers		×		> ai-	analytics (11) (52 KB) i-gateway (16) (124 KB)							
0	Interactive Help				\ > api	i-service (13) (208 KB)							
					1		api-service (all logs)	API Service debug messages	208 KB				
					<u> -</u>		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				

Debug logs downloaden

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.