

# Gebruik OpenAPI om ISE-beleidsinformatie over ISE 3.3 op te halen

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie op ISE](#)

[Python-voorbeelden](#)

[Apparaatbeheer - lijst met beleidssets](#)

[Apparaatbeheer - Verificatieregels verkrijgen](#)

[Apparaatbeheer - autorisatieregels verkrijgen](#)

[Netwerktoegang - lijst van beleidssets](#)

[Netwerktoegang - Verificatieregels verkrijgen](#)

[Netwerktoegang - vergunningsregels verkrijgen](#)

[Problemen oplossen](#)

---

## Inleiding

Dit document beschrijft de procedure voor het gebruik van OpenAPI voor beheer Cisco Identity Services Engine (ISE) Beleid.

## 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

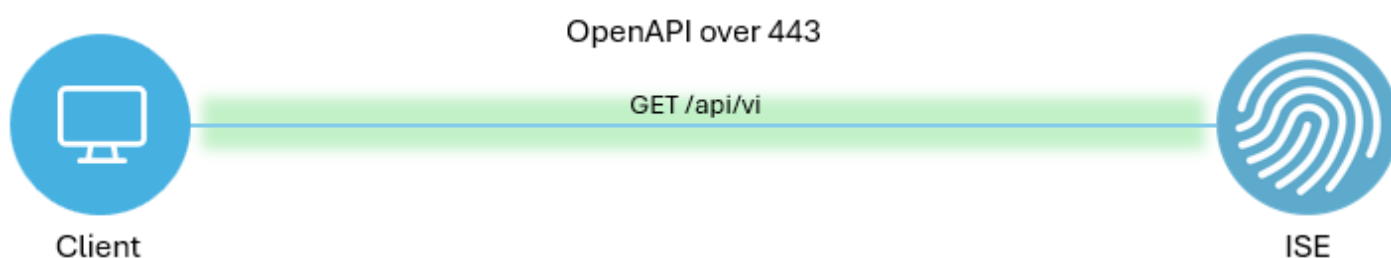
laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Vanaf Cisco ISE 3.1 zijn nieuwere API's beschikbaar in de OpenAPI-indeling. Het beheerbeleid optimaliseert de netwerkbeveiliging en het netwerkbeheer door de interoperabiliteit te verbeteren, de automatiseringsefficiëntie te verbeteren, de beveiliging te versterken, innovatie te bevorderen en de kosten te verlagen. Dit beleid zorgt ervoor dat ISE naadloos kan integreren met andere systemen, geautomatiseerde configuratie en beheer kan realiseren, granulaire toegangscontrole kan bieden, innovatie van derden kan aanmoedigen en beheerprocessen kan vereenvoudigen, waardoor de onderhoudskosten kunnen worden verlaagd en het totale rendement op investeringen kan worden verhoogd.

## Configureren

### Netwerkdigram



Topologie

### Configuratie op ISE

Stap 1. Voeg een OpenAPI-account toe.

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

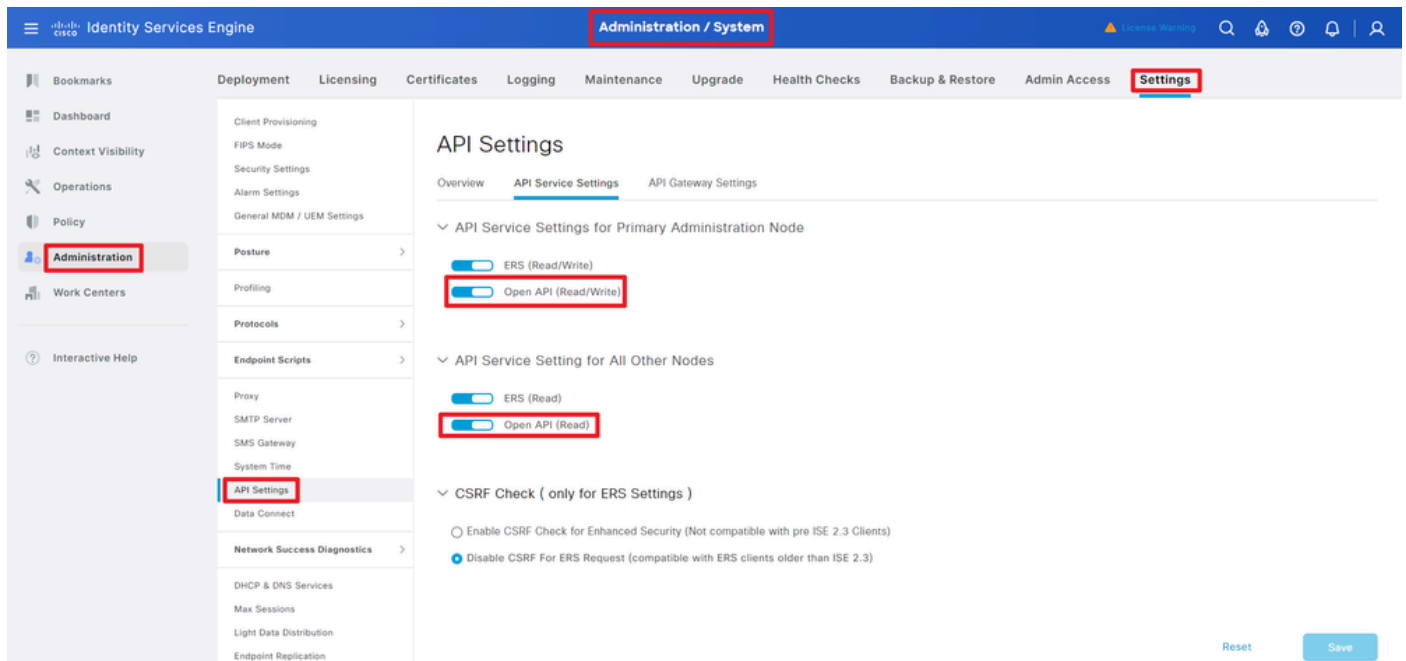
The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System interface. The navigation menu on the left includes 'Administration' and 'Admin Users'. The main content area displays the 'Administrators' table with the following data:

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

API-beheerder

## Stap 2. OpenAPI inschakelen op ISE.

Open API is standaard uitgeschakeld op ISE. Om dit in te schakelen, navigeert u naar Beheer > Systeem > Instellingen > API-instellingen > API-serviceinstellingen. Schakel de opties voor OpenAPI in. Klik op de knop Opslaan.

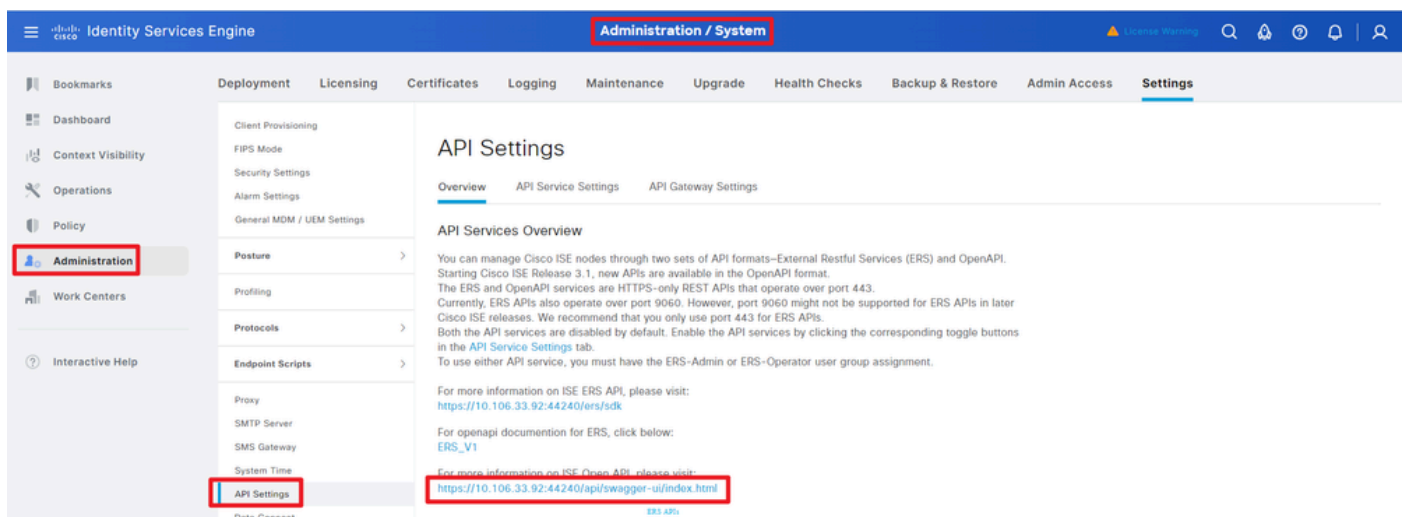


The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and 'Settings'. The left sidebar has 'Administration' highlighted. The main content area shows the 'API Settings' page with the 'API Service Settings' tab selected. The 'Open API (Read/Write)' and 'Open API (Read)' toggles are both turned on. The 'API Settings' menu item in the left sidebar is highlighted.

OpenAPI inschakelen

## Stap 3. Verken ISE OpenAPI.

Naar navigeren Beheer > Systeem > Instellingen > API-instellingen > Overzicht. Klik op OpenAPI om de link te bezoeken.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Administration / System' and 'Settings'. The left sidebar has 'Administration' highlighted. The main content area shows the 'API Settings' page with the 'API Services Overview' tab selected. The 'API Services Overview' section contains information about ERS and OpenAPI services. The 'API Settings' menu item in the left sidebar is highlighted.

Bezoek OpenAPI

## Python-voorbeelden

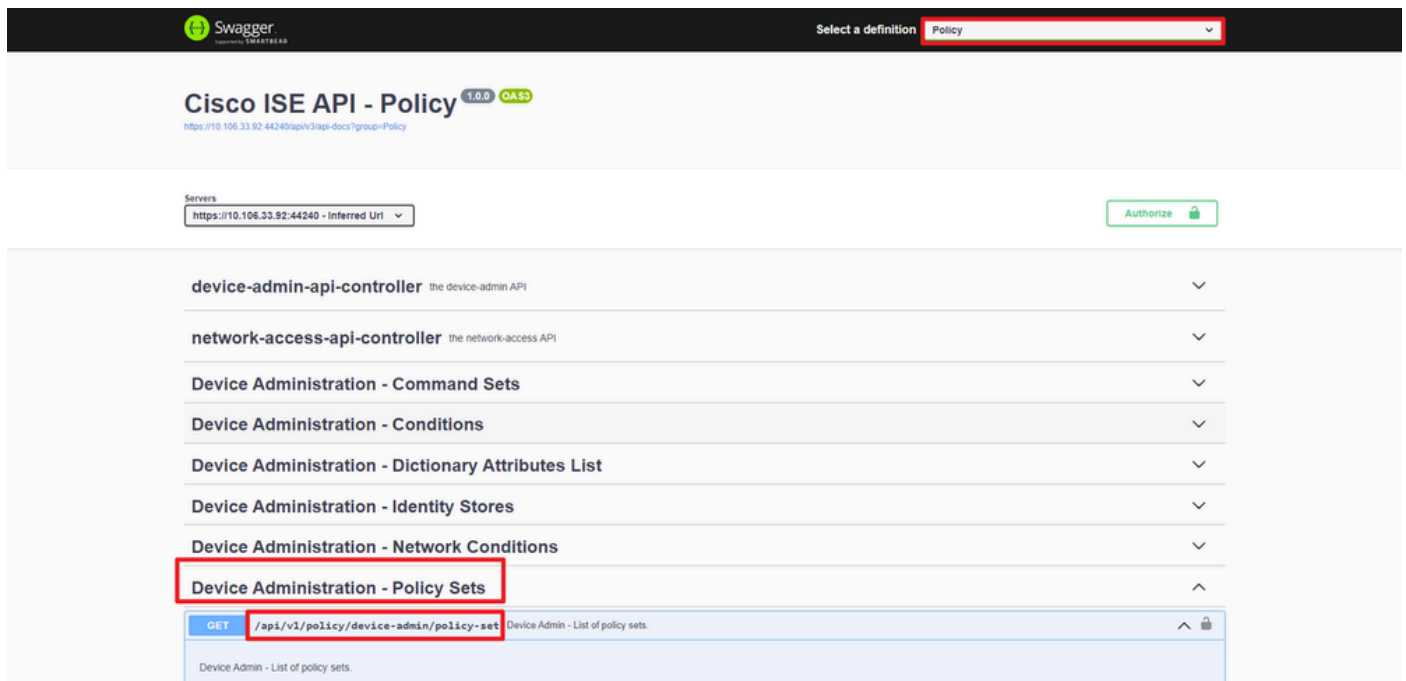
Apparaatbeheer - lijst met beleidssets

Deze API haalt informatie op over de beleidssets van de apparaatbeheerder.

Stap 1. Vereiste informatie voor een API-oproep.

Method	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set
referenties	Gebruik OpenAPI-accountreferenties.
Koppen	accepteren : application/json Content-Type : application/json

Stap 2. Zoek de URL die wordt gebruikt om informatie op te halen over de beleidssets van de apparaatbeheerder.



The screenshot shows the Swagger UI interface for the Cisco ISE API. At the top, the Swagger logo and 'Select a definition' dropdown are visible. The main title is 'Cisco ISE API - Policy' with version '1.0.0 OAS3'. Below this, the 'Servers' section shows the URL 'https://10.106.33.92:44240 - Inferred Url'. A list of API endpoints is shown, with 'Device Administration - Policy Sets' highlighted in a red box. Below this, the specific endpoint '/api/v1/policy/device-admin/policy-set' is also highlighted in a red box, with a 'GET' method and a description 'Device Admin - List of policy sets'.

API-URI

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

Zorg voor een goede verbinding tussen ISE en het apparaat met het python-codevoorbeeld.

<#root>

```
from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

    url = "
```

```

https://10.106.33.92/api/v1/policy/device-admin/policy-set
"
  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())

```

Dit is het voorbeeld van de verwachte output.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': True, 'id': '41ed8579-429b-42a8-879e-61861cb82bbf', 'name': 'Default', 'descr

## DApparaatbeheer - Verificatieregels verkrijgen

Deze API haalt verificatieregels van een bepaalde beleidsset op.

Stap 1. Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-of-Policy-Set>/verificatie
referenties	Gebruik OpenAPI-accountreferenties.
Koppen	accepteren : application/json Content-Type : application/json

Stap 2. Bepaal de plaats van de URL die wordt gebruikt om de informatie van de authenticatieregel terug te winnen.

API-URI

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

Zorg voor een goede verbinding tussen ISE en het apparaat met het python-codevoorbeeld.

<#root>

```

from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

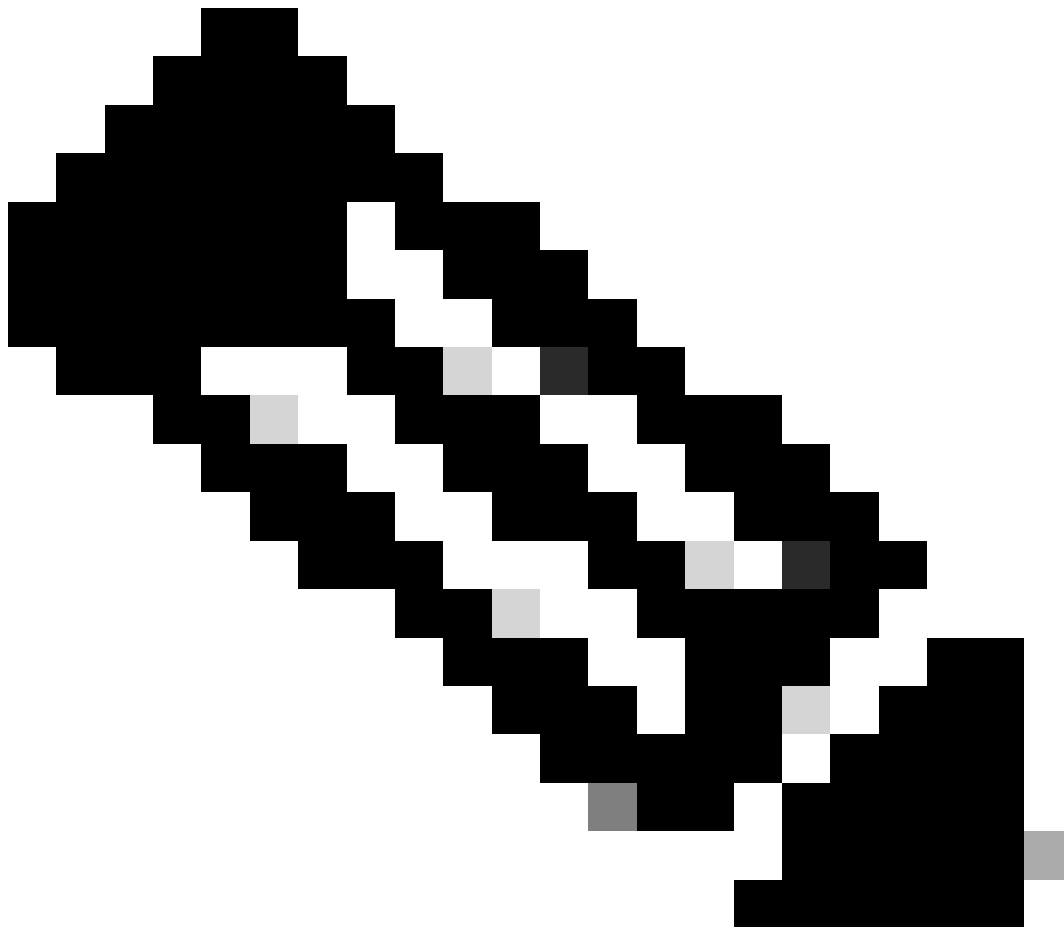
    url = "
https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authentication
"
    headers = {
"Accept": "application/json", "Content-Type": "application/json"
}
    basicAuth = HTTPBasicAuth(
"ApiAdmin", "Admin123"
)

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

```

```
print(response.json())
```

---



Opmerking: de ID is afkomstig van API-uitgangen in stap 3 van Apparaatbeheer - Lijst met beleidssets. Bijvoorbeeld, 41ed8579-429b-42a8-879e-61861cb82bbf is een standaard TACACS beleidsset.

---

Dit is het voorbeeld van de verwachte output.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '73461597-0133-45ce-b4cb-6511ce56f262', 'name': 'Default'}}

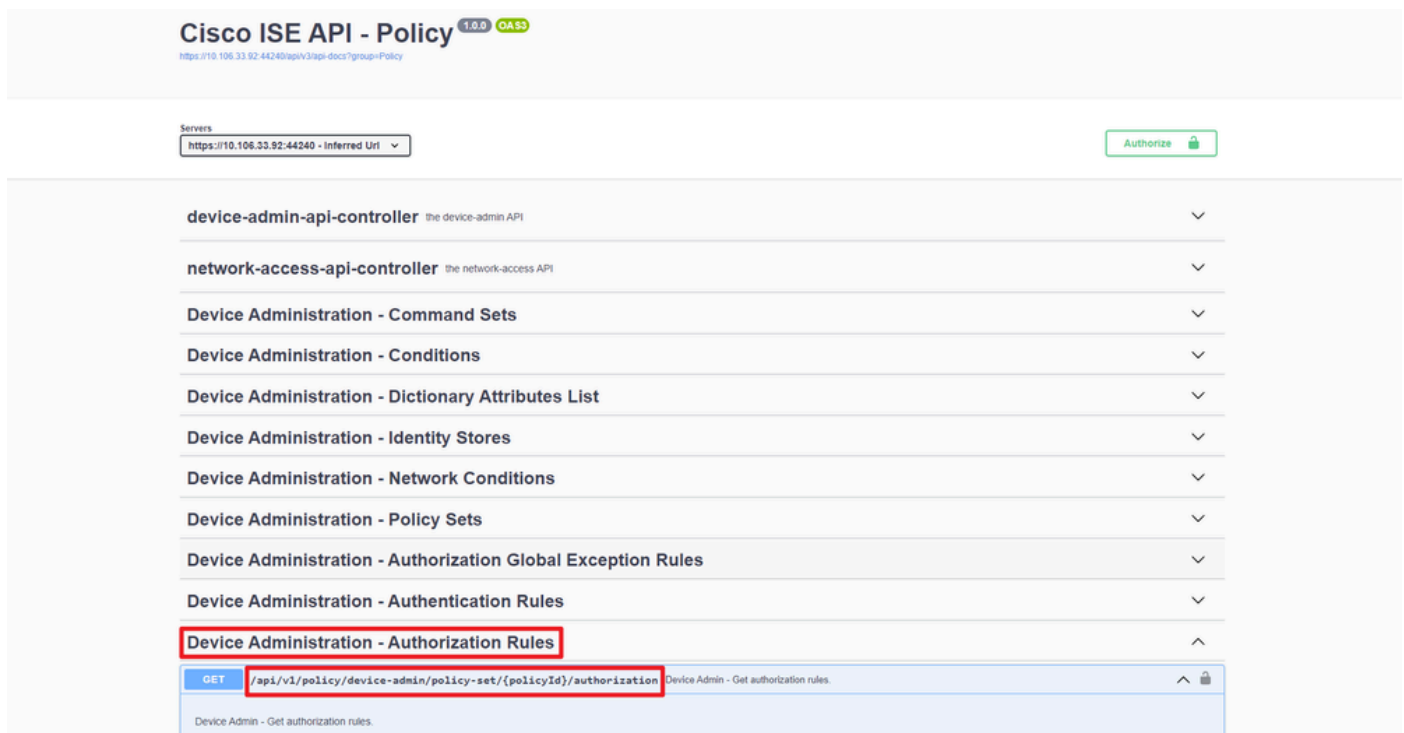
Apparaatbeheer - autorisatieregels verkrijgen

Deze API wint autorisatieregels van een bepaalde beleidsreeks terug.

## Stap 1. Vereiste informatie voor een API-oproep.

Method	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-of-Policy-Set>/autorisatie
referenties	Gebruik OpenAPI-accountreferenties.
Koppen	accepteren : application/json Content-Type : application/json

## Stap 2. Zoek de URL die wordt gebruikt om de informatie over de autorisatieregel op te halen.



API-URI

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

Zorg voor een goede verbinding tussen ISE en het apparaat met het python-codevoorbeeld.

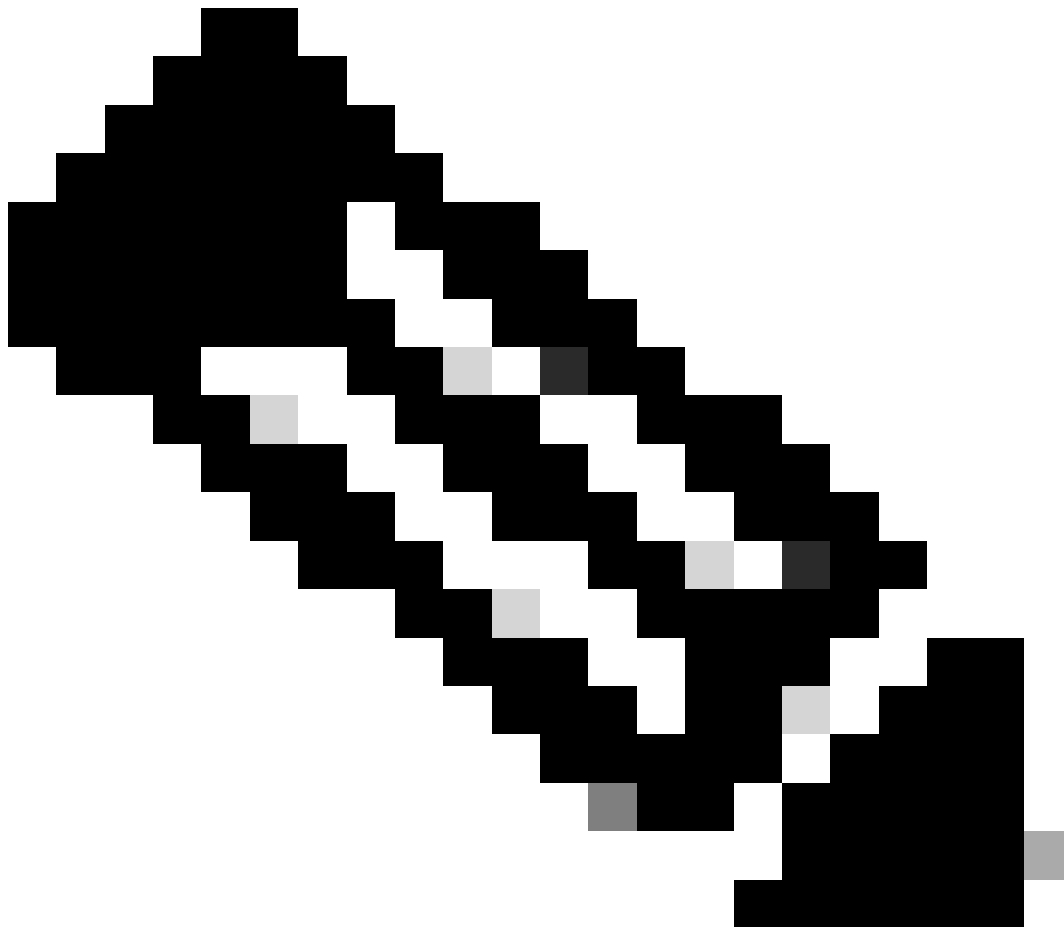
<#root>

```
from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "https://10.106.33.92/api/v1/policy/device-admin/policy-set/41ed8579-429b-42a8-879e-61861cb82bbf/authorization" 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 Apparaatbeheer - Lijst met beleidssets. Bijvoorbeeld, 41ed8579-429b-42a8-879e-61861cb82bbf is een standaard TACACS beleidsset.

---

Dit is het voorbeeld van de verwachte output.

Return Code:

200

Expected Outputs:

```
{'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '39d9f546-e58c-4f79-9856-c0a244b8a2ae', 'name': 'Default', 'hitCounts': 0, 'rank': 0, 'state': 'enable'}}
```

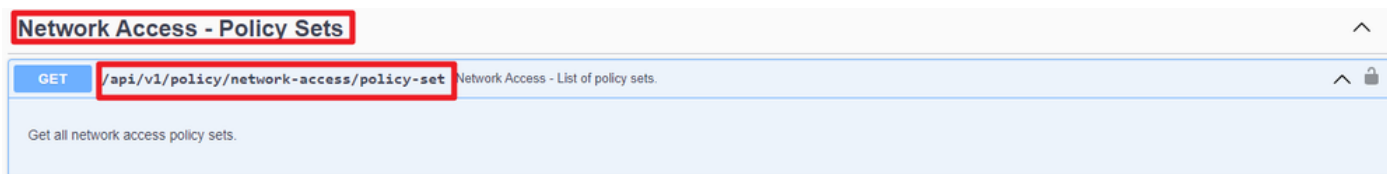
Netwerktogang - lijst van beleidssets

Deze API haalt beleidssets voor netwerktoegang van ISE-implementaties op.

Stap 1. Vereiste informatie voor een API-oproep.

Method	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set
referenties	Gebruik OpenAPI-accountreferenties.
Koppen	accepteren : application/json Content-Type : application/json

Stap 2. Bepaal de plaats van de URL die wordt gebruikt om de specifieke de knoopinformatie van ISE terug te winnen.



API-URI

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

Zorg voor een goede verbinding tussen ISE en het apparaat met het python-codevoorbeeld.

<#root>

```
from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

    url = "
https://10.106.33.92/api/v1/policy/network-access/policy-set
"
    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())
```

Dit is het voorbeeld van de verwachte output.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': False, 'id': 'ba71a417-4a48-4411-8bc3-d5df9b115769', 'name': 'BGL\_CFME0

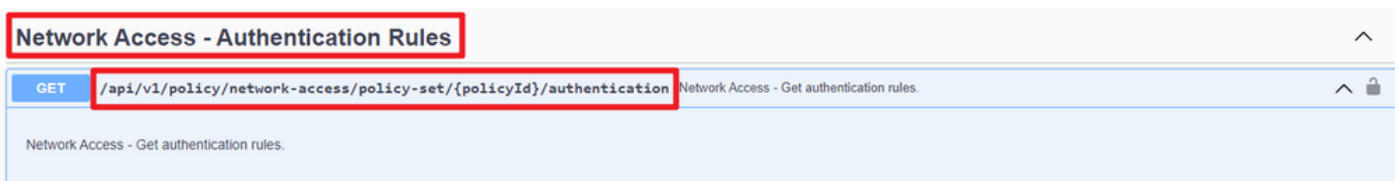
### Netwerktogang - Verificatieregels verkrijgen

Deze API haalt verificatieregels van een bepaalde beleidsset op.

Stap 1. Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-of-Policy-Set>/verificatie
referenties	Gebruik OpenAPI-accountreferenties.
Koppen	accepteren : application/json Content-Type : application/json

Stap 2. Zoek de URL die wordt gebruikt om de informatie over de verificatieregel op te halen.



API-URI

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

Zorg voor een goede verbinding tussen ISE en het apparaat met het python-codevoorbeeld.

<#root>

```
from requests.auth import HTTPBasicAuth
import requests

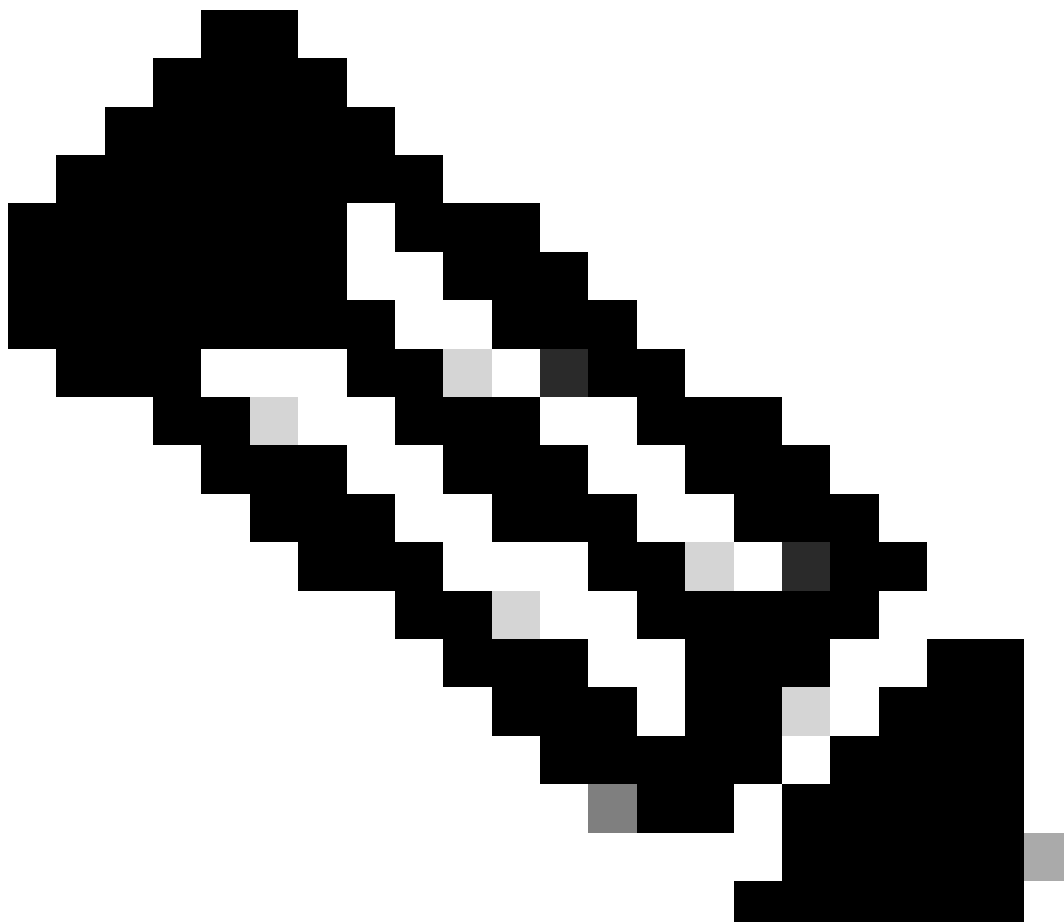
requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":
```

```
url = "
https://10.106.33.92/api/v1/policy/network-access/policy-set/ba71a417-4a48-4411-8bc3-d5df9b115769/authen
"
  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())
```

---



Opmerking: de ID is afkomstig van API-uitgangen in stap 3 van Network Access - List of Policy Sets. Dat ba71a417-4a48-4411-8bc3-d5df9b115769 is bijvoorbeeld BGL\_CFME02-FMCZO.

Dit is het voorbeeld van de verwachte output.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': True, 'id': '03875777-6c98-4114-a72e-a3e1651e533a', 'name': 'Default

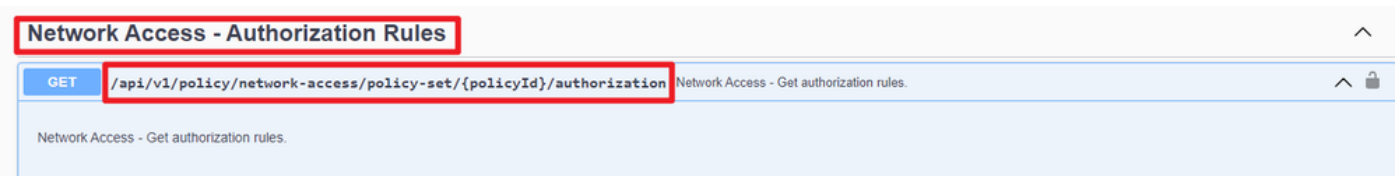
## Netwerktogang - vergunningsregels verkrijgen

Deze API wint autorisatieregels van een bepaalde beleidsreeks terug.

Stap 1. Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-of-Policy-Set>/authorisatie
referenties	Gebruik OpenAPI-accountreferenties.
Koppen	accepteren : application/json Content-Type : application/json

Stap 2. Zoek de URL die wordt gebruikt om de informatie over de autorisatieregel op te halen.



API-URI

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

Zorg voor een goede verbinding tussen ISE en het apparaat met het python-codevoorbeeld.

```
<#root>
```

```
from requests.auth import HTTPBasicAuth
import requests
```

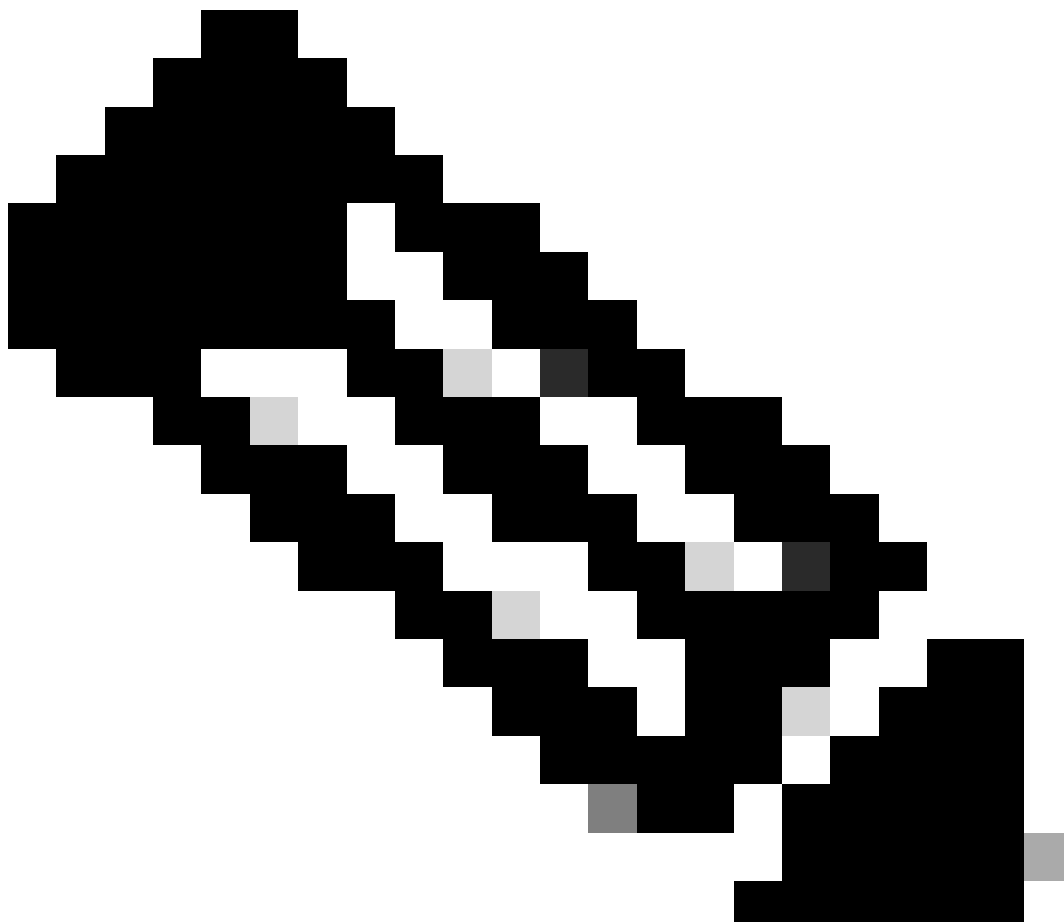
```
requests.packages.urllib3.disable_warnings()
```

```
if __name__ == "__main__":
```

```
url = "
https://10.106.33.92/api/v1/policy/network-access/policy-set/ba71a417-4a48-4411-8bc3-d5df9b115769/author
"
  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())
```

---



Opmerking: de ID is afkomstig van API-uitgangen in stap 3 van Network Access - List of Policy Sets. Bijvoorbeeld, ba71a417-4a48-441-8bc3-d5df9b115769 is BGL\_CFME02-FMC.

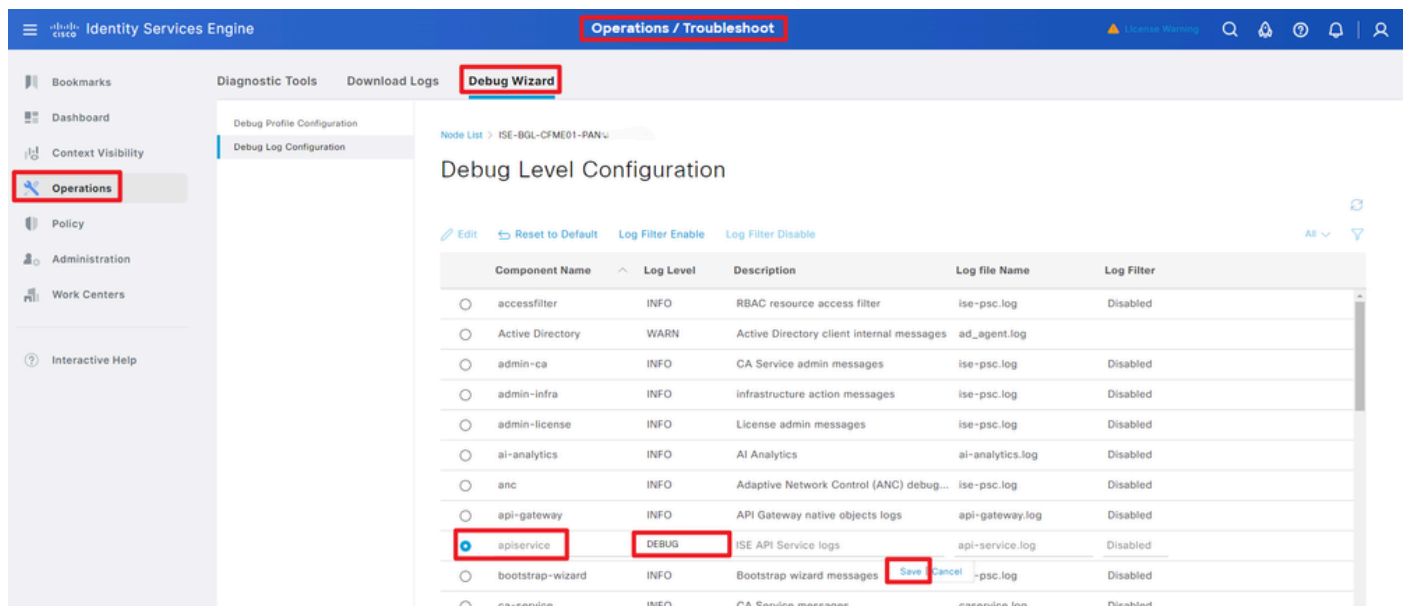
Dit is het voorbeeld van de verwachte output.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'rule': {'default': False, 'id': 'bc67a4e5-9000-4645-9d75-7c2403ca22ac', 'name': 'FMC A

## Problemen oplossen

Om problemen op te lossen die betrekking hebben op de OpenAPI's, stelt u het niveau Log voor de component OpenAPI 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.



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / Troubleshoot'. The left sidebar has 'Operations' highlighted. The main content area is titled 'Debug Wizard' and shows the 'Debug Level Configuration' for the 'api-service' component. The table below lists various components and their log levels.

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
apiservice	DEBUG	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

Debug van API-service

Als u het debug-logbestand wilt downloaden, gaat u naar Operations > Troubleshoot > Logbestanden downloaden > ISE PAN-knooppunt > Debug-logbestanden.

Identity Services Engine **Operations / Troubleshoot** License Warning

Bookmarks Diagnostic Tools **Download Logs** Debug Wizard

Dashboard  
Context Visibility  
**Operations**  
Policy  
Administration  
Work Centers  
Interactive Help

ISE-BGL-CFME01-PAN  
ISE-BGL-CFME02-MNT  
ISE-DLC-CFME01-PSN  
ISE-DLC-CFME02-PSN  
ISE-RTP-CFME01-PAN  
ISE-RTP-CFME02-MNT

Delete Expand All Collapse All

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

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.