

OpenAPI zum Abrufen von ISE-Richtlinieninformationen zu ISE 3.3 verwenden

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration auf der ISE](#)

[Python-Beispiele](#)

[Device Admin - Liste der Richtlinienätze](#)

[Geräteadministrator - Authentifizierungsregeln abrufen](#)

[Geräteadministrator - Autorisierungsregeln abrufen](#)

[Netzwerkzugriff - Liste von Richtlinienätzen](#)

[Netzwerkzugriff - Authentifizierungsregeln abrufen](#)

[Netzwerkzugriff - Autorisierungsregeln abrufen](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird das Verfahren zur Verwendung von OpenAPI zur Verwaltung Cisco Identity Services Engine (ISE) Richtlinie.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

- ISE 3.3
- Python 3.10.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Ab Cisco ISE 3.1 sind neuere APIs im OpenAPI-Format verfügbar. Die Managementrichtlinien optimieren die Netzwerksicherheit und das Netzwerkmanagement, indem sie die Interoperabilität verbessern, die Effizienz der Automatisierung verbessern, die Sicherheit stärken, Innovationen fördern und die Kosten senken. Diese Richtlinie ermöglicht der ISE die nahtlose Integration in andere Systeme, eine automatisierte Konfiguration und Verwaltung, eine präzise Zugriffskontrolle, die Förderung von Innovationen von Drittanbietern und die Vereinfachung von Managementprozessen. Auf diese Weise werden Wartungskosten gesenkt und die Investitionsrendite insgesamt gesteigert.

Konfigurieren

Netzwerkdiagramm



Topologie

Konfiguration auf der ISE

Schritt 1: Fügen Sie ein OpenAPI-Administratorkonto hinzu.

Um einen API-Administrator hinzuzufügen, navigieren Sie zu Administration > System > Admin Access > Administrators > Admin Users > Add.

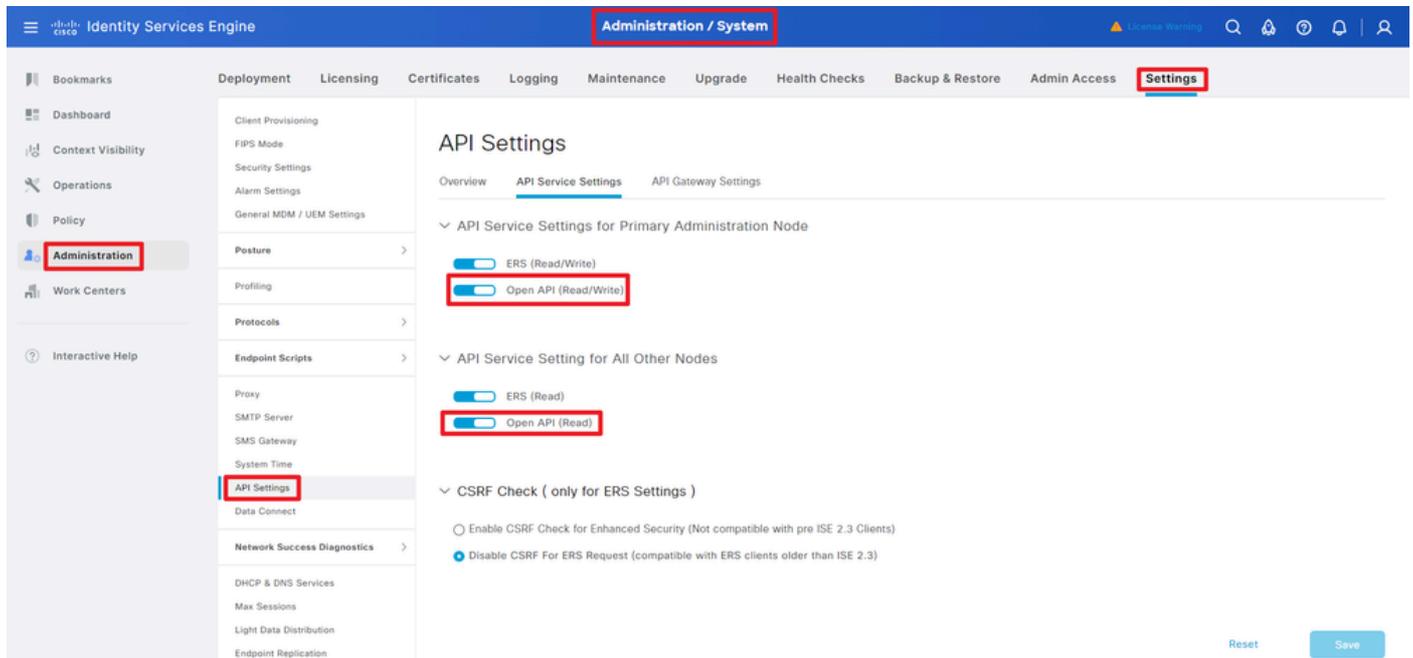
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu on the left includes 'Administration', which is highlighted. The main content area displays the 'Administrators' page, where the 'Admin Users' sub-menu is selected. A table lists the existing administrators:

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

API-Administrator

Schritt 2: Aktivieren Sie OpenAPI auf der ISE.

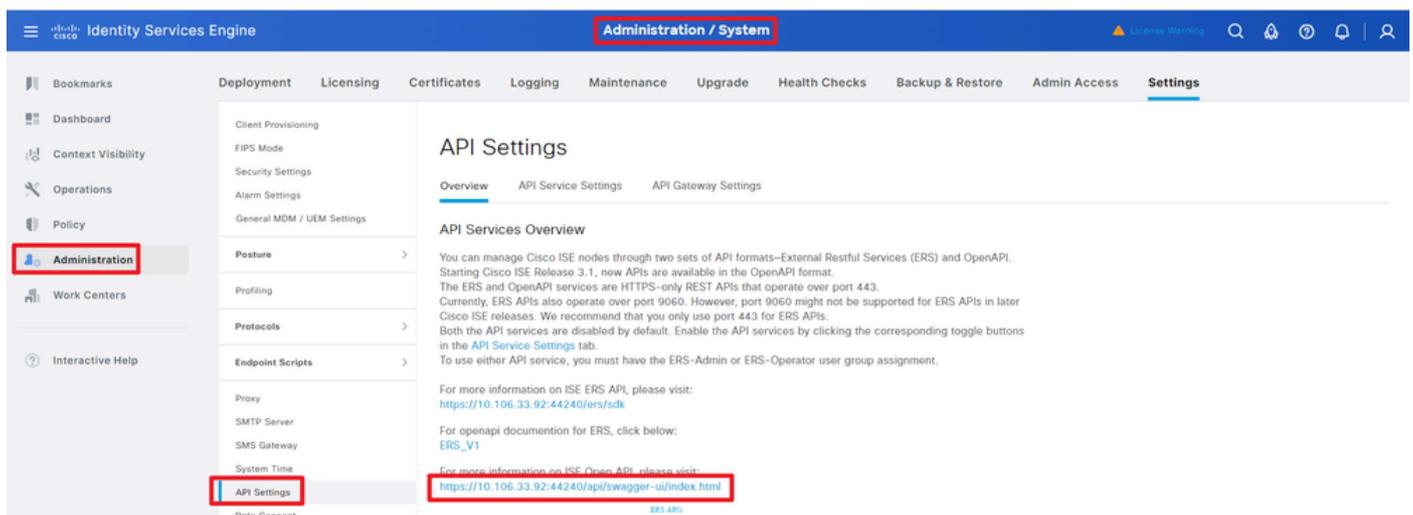
Die offene API ist auf der ISE standardmäßig deaktiviert. Navigieren Sie zu Administration > System > Settings > API Settings > API Service Settings. Schalten Sie die OpenAPI-Optionen um. Klicken Sie auf Speichern.



OpenAPI aktivieren

Schritt 3: Erkunden der ISE OpenAPI

Navigieren Sie zu Administration > System > Settings > API Settings > Overview. Klicken Sie auf OpenAPI, um den Link aufzurufen.



OpenAPI aufrufen

Python-Beispiele

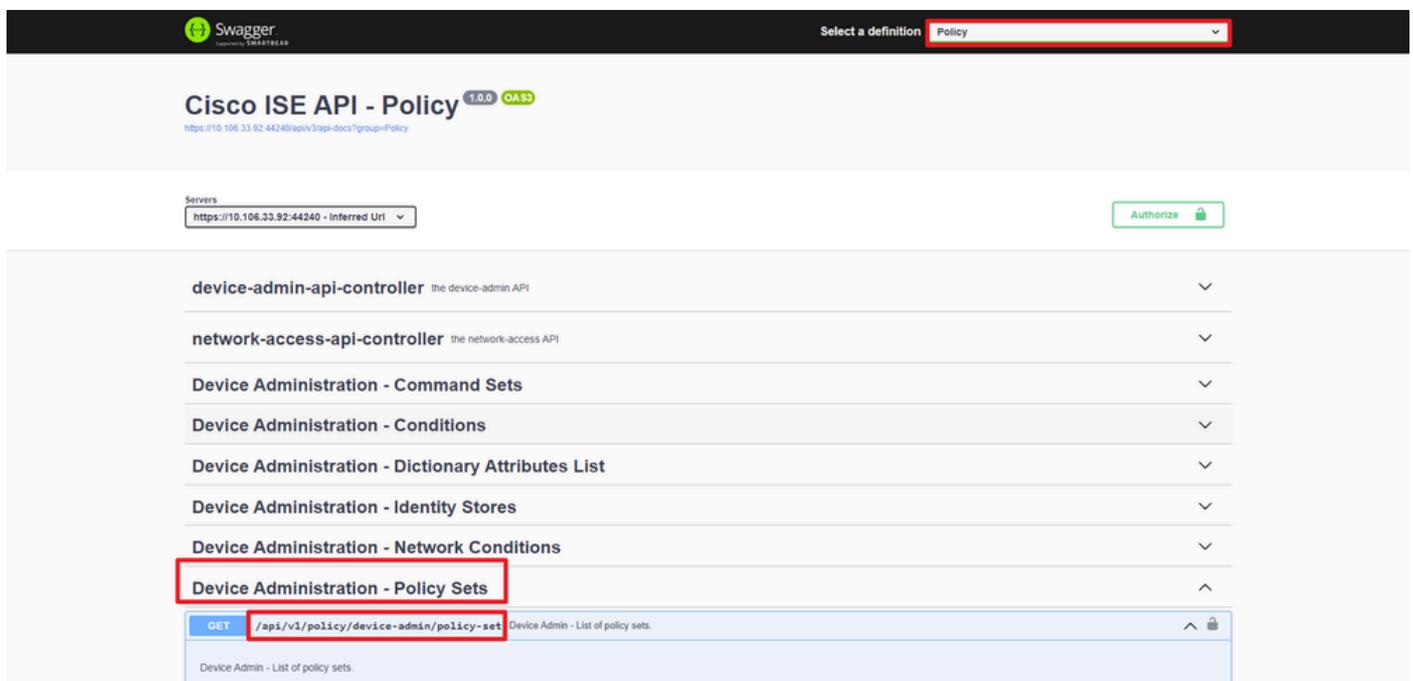
Device Admin - Liste der Richtlinienätze

Diese API ruft Informationen zu den Admin-Richtliniensätzen des Geräts ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen von Informationen zu den Admin-Richtlinien für Geräte verwendet wird.



API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#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())

```

Dies ist das Beispiel der erwarteten Ergebnisse.

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

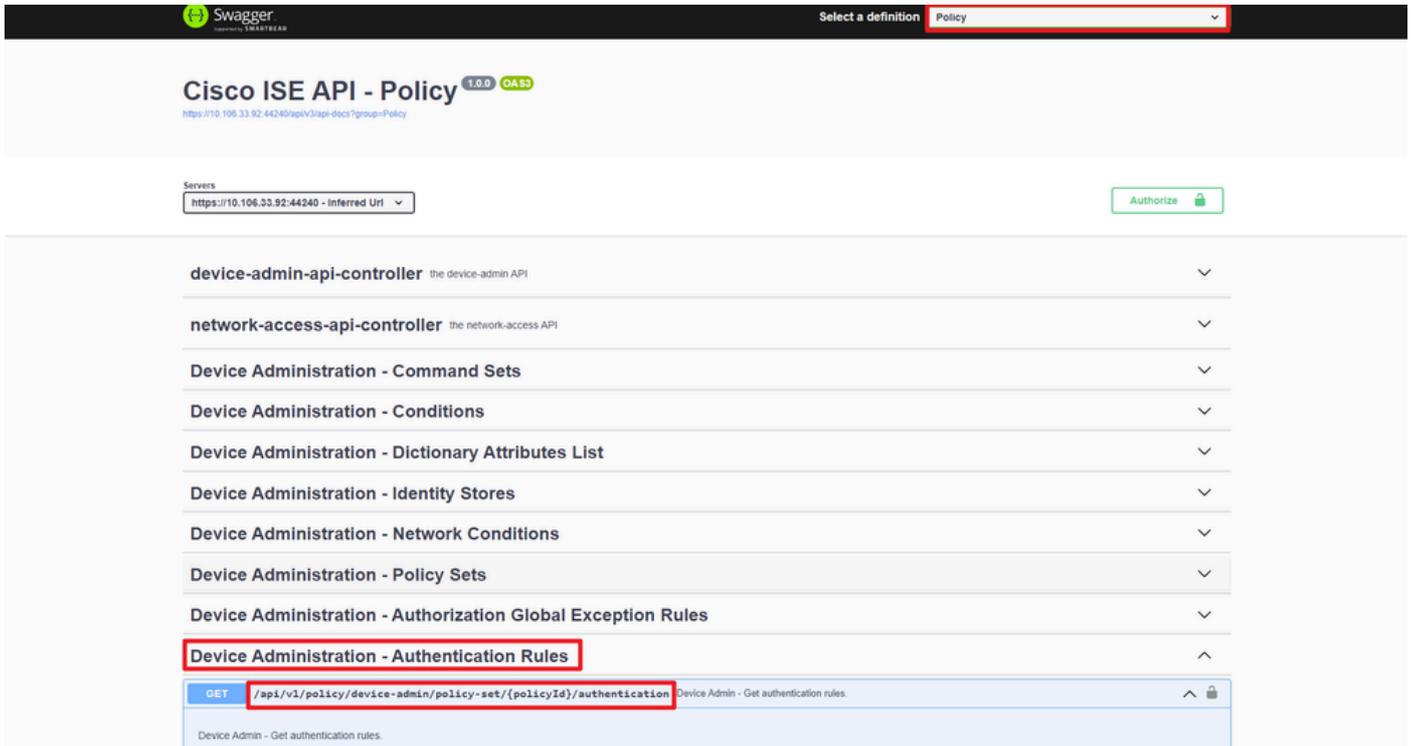
GGeräteadministrator - Authentifizierungsregeln abrufen

Diese API ruft Authentifizierungsregeln eines bestimmten Richtlinienatzes ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authentication
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen von Authentifizierungsregelinformationen verwendet wird.



API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#root>

```
from requests.auth import HTTPBasicAuth
import requests

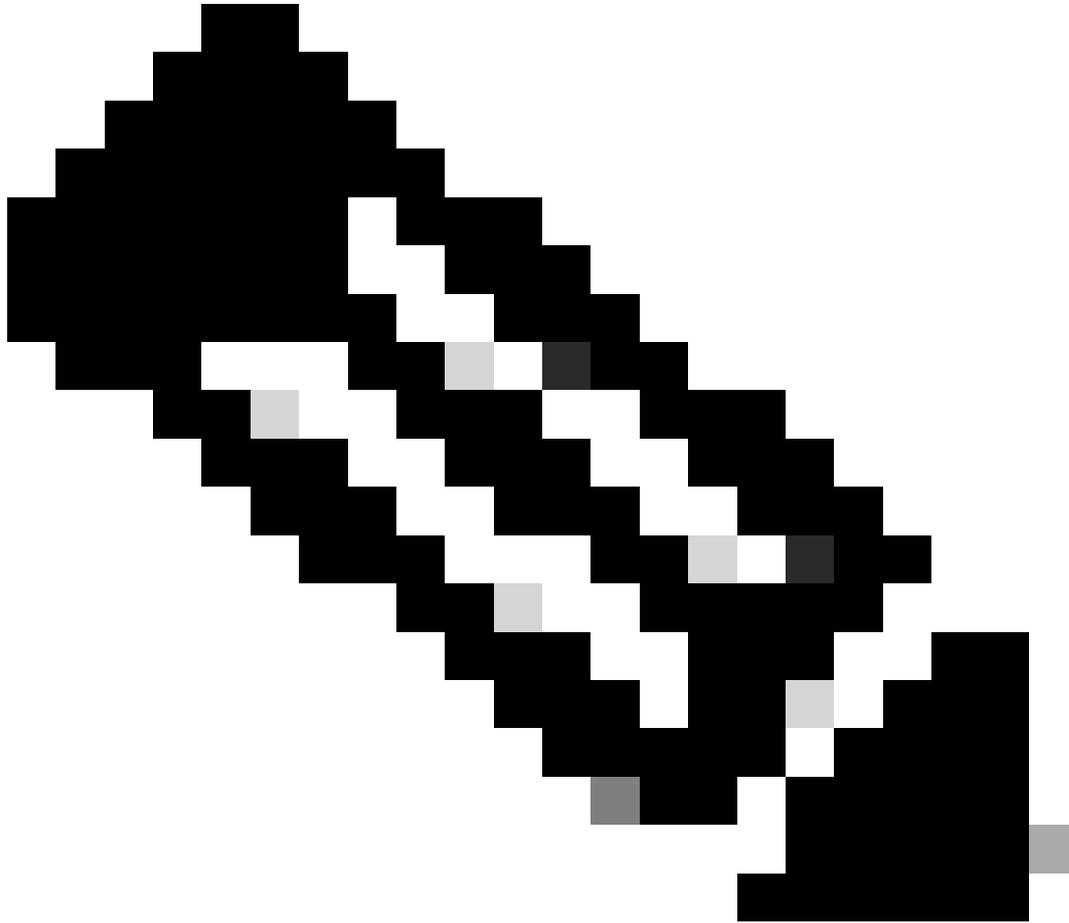
requests.packages.urllib3.disable_warnings()

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())
```



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von Device Admin - List Of Policy Sets. 41ed8579-429b-42a8-879e-61861cb82bbf ist beispielsweise der TACACS-Standardrichtliniensatz.

Dies ist das Beispiel der erwarteten Ergebnisse.

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

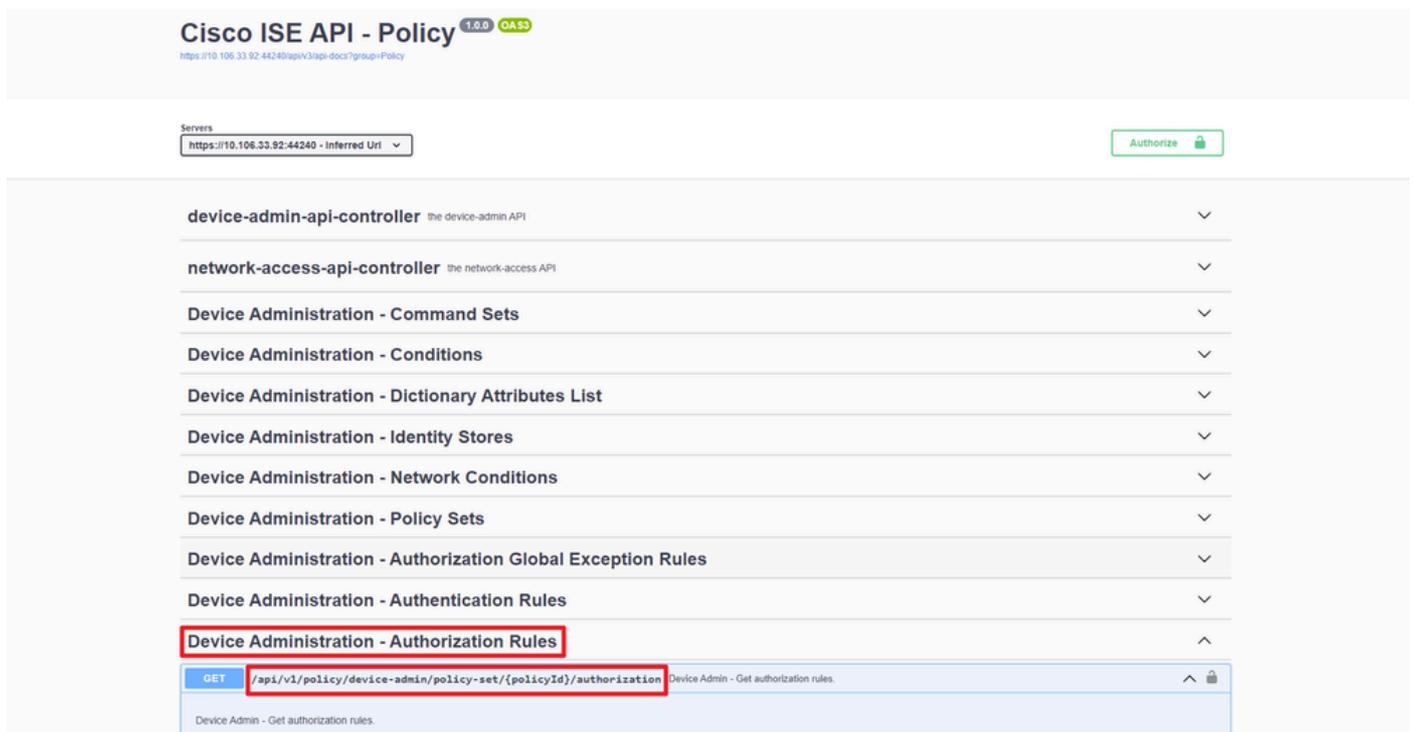
Geräteadministrator - Autorisierungsregeln abrufen

Diese API ruft Autorisierungsregeln eines bestimmten Richtlinienatzes ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https://<ISE-PAN-IP>/api/v1/policy/device-admin/policy-set/<ID-Of-Policy-Set>/authorization
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen der Autorisierungsregelinformationen verwendet wird.



API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

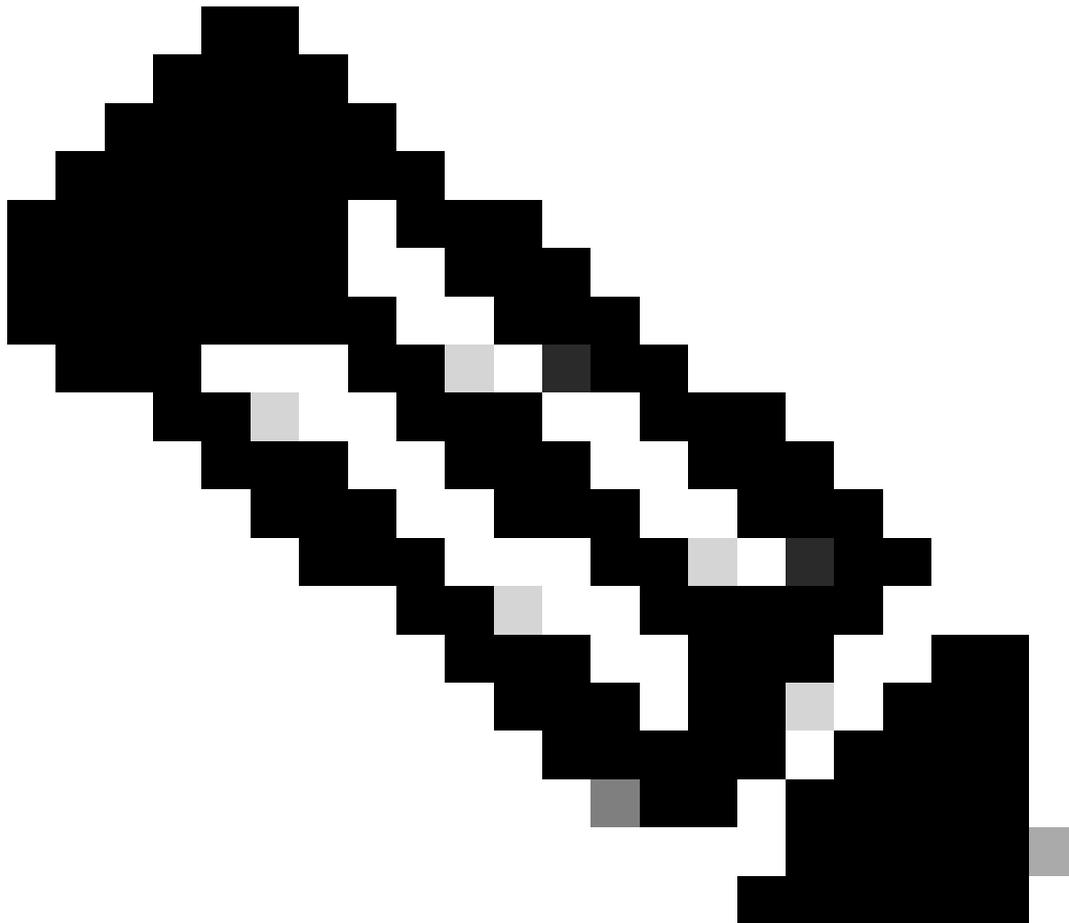
Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#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/authoriz
```

```
" 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:")
```



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von Device Admin - List Of Policy Sets. 41ed8579-429b-42a8-879e-61861cb82bbf ist beispielsweise der TACACS-Standardrichtliniensatz.

Dies ist das Beispiel der erwarteten Ergebnisse.

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'}
```

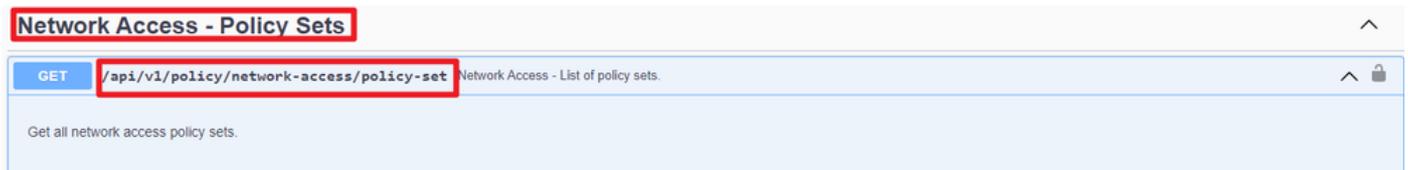
Netzwerkzugriff - Liste von Richtlinienansätzen

Diese API ruft Netzwerkzugriffsrichtliniensätze von ISE-Bereitstellungen ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Geben Sie die URL an, die zum Abrufen der spezifischen ISE-Knoteninformationen verwendet wird.



API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

```
<#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())

```

Dies ist das Beispiel der erwarteten Ergebnisse.

Return Code: 200 Expected Outputs: {'version': '1.0.0', 'response': [{'default': False, 'id': 'ba71a417-4a48-4411-8bc3-d5df9b115769', 'name': 'BGL_CFME0

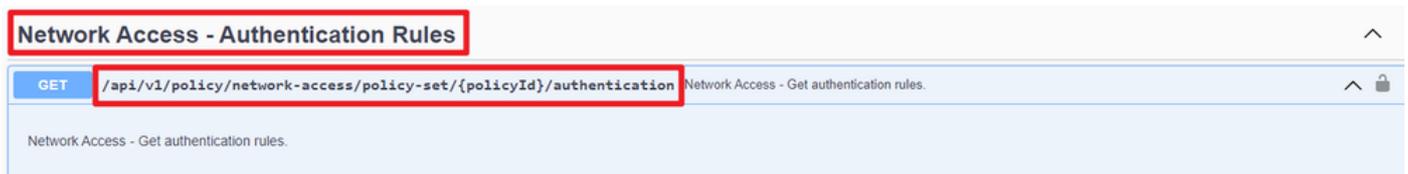
Netzwerkzugriff - Authentifizierungsregeln abrufen

Diese API ruft Authentifizierungsregeln eines bestimmten Richtlinienansatzes ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	https://<ISE-PAN-IP>/api/v1/policy/network-access/policy-set/<ID-Of-Policy-Set>/authentication
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen der Authentifizierungsregelninformationen verwendet wird.



API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

```
<#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())
```



Hinweis: Die ID stammt aus API-Ausgaben in Schritt 3 von Network Access - List Of Policy Sets. Zum Beispiel `ba71a417-4a48-4411-8bc3-d5df9b115769` ist `BGL_CFME02-FMC`.

Dies ist das Beispiel der erwarteten Ergebnisse.

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

Netzwerkzugriff - Autorisierungsregeln abrufen

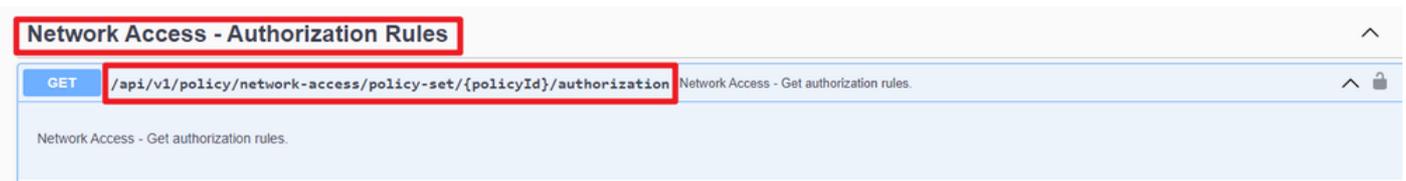
Diese API ruft Autorisierungsregeln eines bestimmten Richtlinienatzes ab.

Schritt 1: Erforderliche Informationen für einen API-Aufruf.

Methode	HOLEN
URL	<code>https://<ISE-PAN-IP>/api/v1/policy/network-</code>

	access/policy-set/<ID-Of-Policy-Set>/authorization
Anmeldeinformationen	OpenAPI-Kontoinformationen verwenden.
Header	Akzeptieren : application/json Inhaltstyp : application/json

Schritt 2: Suchen Sie nach der URL, die zum Abrufen der Autorisierungsregelinformationen verwendet wird.



API-URI

Schritt 3: Dies ist ein Beispiel für Python-Code. Kopieren Sie den Inhalt, und fügen Sie ihn ein. Ersetzen Sie die ISE-IP, den Benutzernamen und das Kennwort. Speichern Sie die Datei als Python, um sie auszuführen.

Stellen Sie eine gute Verbindung zwischen der ISE und dem Gerät sicher, auf dem das Python-Codebeispiel ausgeführt wird.

<#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())

```



Hinweis: Die ID stammt aus den API-Ausgaben in Schritt 3 von "Network Access - List Of Policy Sets". Beispiel: ba71a417-4a48-4411-8bc3-d5df9b115769 lautet BGL_CFME02-FMC.

Dies ist das Beispiel der erwarteten Ergebnisse.

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

Fehlerbehebung

Um Probleme im Zusammenhang mit den OpenAPIs zu beheben, legen Sie die Protokollstufe für die APIs-Komponente im Fenster Konfiguration des Debug-Protokolls auf DEBUG fest.

Um das Debuggen zu aktivieren, navigieren Sie zu Operations > Troubleshoot > Debug Wizard >

Debug Log Configuration > ISE Node > apiservice.

Operations / Troubleshoot

Debug Wizard

Node List > ISE-BGL-CFME01-PAN

Debug Level Configuration

Edit Reset to Default Log Filter Enable Log Filter Disable

Component Name	Log Level	Description	Log File Name	Log Filter
<input type="radio"/> accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled
<input type="radio"/> Active Directory	WARN	Active Directory client internal messages	ad_agent.log	Disabled
<input type="radio"/> admin-ca	INFO	CA Service admin messages	ise-psc.log	Disabled
<input type="radio"/> admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled
<input type="radio"/> admin-license	INFO	License admin messages	ise-psc.log	Disabled
<input type="radio"/> ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled
<input type="radio"/> anc	INFO	Adaptive Network Control (ANC) debug...	ise-psc.log	Disabled
<input type="radio"/> api-gateway	INFO	API Gateway native objects logs	api-gateway.log	Disabled
<input checked="" type="radio"/> apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled
<input type="radio"/> bootstrap-wizard	INFO	Bootstrap wizard messages	-psc.log	Disabled
<input type="radio"/> ca-service	INFO	CA Service messages	caservice.log	Disabled

Save Cancel

Debuggen von API-Diensten

Um die Debug-Protokolldatei herunterzuladen, navigieren Sie zu Operations > Troubleshoot > Download Logs > ISE PAN Node > Debug Logs.

Operations / Troubleshoot

Download Logs

Debug Wizard

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

Deletes 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-Protokolle herunterladen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.